REDES CISCO

Guía de estudio para la certificación CCNA Security

Ernesto Ariganello

Ra-Ma®

REDES CISCO

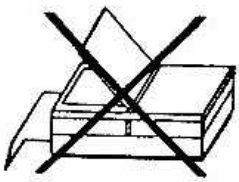
Guía de estudio para la certificación CCNA Security

REDES CISCO

Guía de estudio para la certificación CCNA Security

Ernesto Ariganello

Ra-Ma®



La ley prohíbe
copiar o imprimir este libro

REDES CISCO: GUÍA DE ESTUDIO PARA LA CERTIFICACIÓN CCNA SECURITY
© Ernesto Ariganello

ISBN de Edición en Papel: 978-84-9964-214-7

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco
Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-428-8

E-Book desarrollado en España en septiembre de 2014.

COPYRIGHT

ÍNDICE

INTRODUCCIÓN **15**

CAPÍTULO 1. FUNDAMENTOS DE SEGURIDAD EN LAS REDES **23**

1.1 PRINCIPIOS DE UNA RED SEGURA 23

1.1.1 Evolución de la seguridad en redes 24

1.1.2 Claves para la protección de datos 26

1.1.3 Hacking 27

1.1.4 Organizaciones de seguridad en redes 29

1.1.5 Dominios de la seguridad en redes 30

1.1.6 Políticas de seguridad en redes 32

1.1.7 Cisco SecureX Architecture 32

1.2 VULNERABILIDADES 33

1.2.1 Virus 34

1.2.2 Gusanos 34

1.2.3 Troyanos 35

1.2.4 Mitigación de virus, gusanos y troyanos 36

1.3 METODOLOGÍAS DE ATAQUE 37

1.3.1 Ataques de reconocimiento 37

1.3.2 Ataques de acceso 38

1.3.3 Ataques de denegación de servicio 38

1.3.4 Mitigación de ataques de red 39

1.3.5 Cisco Network Foundation Protection 41

1.4 FUNDAMENTOS PARA EL EXAMEN 45

CAPÍTULO 2. SEGURIDAD EN LOS ROUTERS 47
2.1 SEGURIDAD EN EL ROUTER 47
2.1.1 Modelos de defensa 47
2.1.2 Complementos de seguridad 49
2.1.3 Acceso administrativo seguro 50
2.2 CONFIGURACIÓN DE CONTRASEÑAS 51
2.2.1 Contraseña enable secret 52
2.2.2 Contraseña de consola 53
2.2.3 Contraseña de telnet 53
2.2.4 Contraseña de auxiliar 53
2.2.5 Seguridad mejorada para conexiones virtuales 54
2.2.6 Banners 57
2.2.7 Configuración de SSH 58
2.2.8 Configuración de SSH con CCP 63
2.3 ASIGNACIÓN DE ROLES 64
2.3.1 Configuración de niveles de privilegios 64
2.3.2 Configuración de acceso a la CLI basado en roles 66
2.4 PROTECCIÓN DE ARCHIVOS Y CONTRASEÑAS 70
2.4.1 Resguardo de la configuración e imagen IOS 70
2.4.2 Recuperación de contraseñas 73
2.5 FUNDAMENTOS PARA EL EXAMEN 75

CAPÍTULO 3. MONITORIZACIÓN Y ADMINISTRACIÓN DE LA RED 77
3.1 ADMINISTRACIÓN Y REPORTES 77
3.1.1 Syslog como herramienta de registro 78
3.1.2 Configuración de Syslog 79
3.2 SNMP 82
3.3 NTP 85
3.4 AUDITORÍAS DE SEGURIDAD 89
3.4.1 Asistente de Auditoría de Seguridad 92
3.4.2 Cisco AutoSecure 94
3.4.3 One-Step Lockdown 97
3.5 FUNDAMENTOS PARA EL EXAMEN 100

CAPÍTULO 4. AAA 101
4.1 INTRODUCCIÓN A AAA 101
4.1.1 Modos de acceso AAA 102
4.1.2 Autenticación AAA 103

4.1.3 Autorización AAA 103
4.1.4 Auditoría AAA 104
4.2 CONFIGURACIÓN LOCAL DE AAA 104
4.2.1 Configuración de AAA con CLI 104
4.2.2 Configuración de AAA con CCP 105
4.3 AUTENTICACIÓN AAA BASADA EN SERVIDOR 109
4.3.1 Protocolos de autenticación AAA 109
4.3.2 Cisco Secure ACS 111
4.3.3 Instalación de ACS 112
4.3.4 Configuración de ACS 114
4.4 CONFIGURACIÓN DE AUTENTICACIÓN BASADA EN SERVIDOR 121
4.4.1 Configuración de RADIUS y TACACS+ con CLI 122
4.5 CONFIGURACIÓN DE TACACS+ CON CCP 124
4.6 RESOLUCIÓN DE FALLOS EN AAA 128
4.7 CONFIGURACIÓN DE AUTORIZACIÓN BASADA EN SERVIDOR 130
4.7.1 Configuración de autorización con CCP 132
4.8 REGISTRO DE AUDITORÍA AAA BASADA EN SERVIDOR 134
4.8.1 Configuración del registro de auditoría 134
4.9 FUNDAMENTOS PARA EL EXAMEN 136

CAPÍTULO 5. SEGURIDAD DE CAPA 2 137
5.1 SEGURIDAD DE LAN 137
5.1.1 Seguridad en los dispositivos finales 138
5.1.2 Dispositivos Cisco de seguridad para terminales 138
5.2 SEGURIDAD EN CAPA 2 140
5.2.1 Ataques comunes de capa 2 140
5.3 SEGURIDAD DE PUERTOS DE CAPA 2 142
5.3.1 Configuración de seguridad de puertos 142
5.3.2 Verificación de la seguridad de puertos 145
5.4 CONTROL DE TORMENTAS 147
5.4.1 Configuración de control de tormentas 147
5.5 PROTECCIÓN DE LAS TOPOLOGÍAS STP 148
5.5.1 Configuración de BPDU Guard 149
5.5.2 Configuración de BPDU Filter 150
5.5.3 Configuración de Root Guard 150
5.6 SEGURIDAD EN VLAN 151
5.6.1 Seguridad del enlace troncal 151
5.6.2 Configuración de un enlace troncal seguro 152

5.6.3 VLAN Access Lists 152
5.6.4 Private VLAN 153
5.6.5 Private VLAN Edge 155
5.6.6 Switched Port Analyzer 156
5.7 FUNDAMENTOS PARA EL EXAMEN 157

CAPÍTULO 6. LISTAS DE CONTROL DE ACCESO 159
6.1 INTRODUCCIÓN A ACL 159
6.1.1 Funcionamiento de las ACL 159
6.1.2 Mitigación de ataques con ACL 161
6.1.3 Tipos de lista de acceso 161
6.2 UBICACIÓN DE LAS ACL 162
6.2.1 Lista de acceso entrante 163
6.2.2 Lista de acceso saliente 163
6.3 RECOMENDACIONES EN EL DISEÑO DE LAS ACL 164
6.4 CONFIGURACIÓN DE ACL NUMERADA 165
6.4.1 Configuración de ACL estándar 166
6.4.2 Configuración de ACL extendida 167
6.4.3 Asociación de las ACL a una interfaz 168
6.4.4 Aplicación de una ACL a la línea de telnet 169
6.5 LISTAS DE ACCESO CON NOMBRE 169
6.5.1 Configuración de ACL nombrada 170
6.6 MENSAJES DE REGISTRO EN LAS ACL 170
6.7 CONFIGURACIÓN DE ACL CON CCP 171
6.8 LISTAS DE ACCESO REFLEXIVAS 175
6.9 LISTAS DE ACCESO DINÁMICAS 178
6.10 LISTAS DE ACCESO BASADAS EN TIEMPO 180
6.11 VERIFICACIÓN DE LISTAS DE ACCESO 182
6.12 LISTAS DE ACCESO IPV6 184
6.13 OBJECT GROUP 185
6.13.1 Características de los object group 186
6.13.2 Configuración de los object group 186
6.14 FUNDAMENTOS PARA EL EXAMEN 190

CAPÍTULO 7. FIREWALLS 191
7.1 REDES SEGURAS CON FIREWALLS 191
7.1.1 Características de los firewalls 192
7.1.2 Tipos de firewall 193

7.1.3 Diseño de redes con firewalls 195
7.2 CONTROL DE ACCESO BASADO EN EL CONTEXTO 197
7.2.1 Funcionamiento de CBAC 199
7.2.2 Configuración de CBAC 200
7.2.3 Verificación de CBAC 204
7.3 FIREWALL BASADO EN ZONAS 207
7.3.1 Funcionamiento del firewall basado en zonas 208
7.3.2 Configuración del firewall basado en zonas 212
7.3.3 Configuración del firewall basado en zonas con CCP 214
7.3.4 Configuración manual del firewall basado en zonas con CCP 218
7.4 RESOLUCIÓN DE PROBLEMAS EN EL FIREWALL BASADO EN ZONAS 226
7.5 CISCO ADAPTIVE SECURITY APPLIANCE 228
7.5.1 Características del Cisco ASA 231
7.5.2 Configuración básica del firewall Cisco ASA 232
7.5.3 Configuración del firewall Cisco ASA con ASDM 238
7.6 CONFIGURACIÓN AVANZADA DEL FIREWALL CISCO ASA 245
7.6.1 Configuración de object groups 245
7.6.2 Configuración de ACL 251
7.6.3 Configuración de NAT 255
7.6.4 Configuración de control de acceso 261
7.6.5 Configuración de políticas 264
7.6.6 Configuración de acceso remoto y VPN 266
7.7 FUNDAMENTOS PARA EL EXAMEN 276

CAPÍTULO 8. CISCO IPS 277
8.1 CARACTERÍSTICAS DE LOS IDS E IPS 277
8.1.1 Implementaciones IPS basadas en red 279
8.2 FIRMAS IPS 282
8.2.1 Tipos de firmas 282
8.2.2 Alarmas de firmas 283
8.2.3 Acciones de firmas 286
8.2.4 Administración y monitorización IPS 287
8.3 CONFIGURACIÓN DE CISCO IOS IPS 288
8.3.1 Configuración de IPS con CLI 288
8.3.2 Configuración de IPS con CCP 294
8.3.3 Modificación de las firmas 299
8.3.4 Verificación y monitorización de Cisco IOS IPS 300
8.4 FUNDAMENTOS PARA EL EXAMEN 303

CAPÍTULO 9. TECNOLOGÍAS VPN 305
9.1 REDES PRIVADAS VIRTUALES 305
9.2 TÚNELES GRE 306
9.2.1 Configuración básica de túneles GRE 307
9.3 IPSEC 309
9.3.1 Características de IPsec 309
9.3.2 Modos de IPsec 311
9.3.3 Cabeceras IPsec 312
9.4 PROTOCOLOS DE IPSEC 312
9.4.1 IKE 312
9.4.2 ESP 312
9.4.3 AH 313
9.4.4 Autenticación de vecinos 314
9.5 INTERNET KEY EXCHANGE 314
9.5.1 Protocolos IKE 315
9.5.2 Fases IKE 315
9.5.3 Modos IKE 315
9.5.4 Funciones adicionales IKE 316
9.6 ALGORITMOS DE ENCRIPTACIÓN 317
9.6.1 Encriptación simétrica 317
9.6.2 Encriptación asimétrica 318
9.7 PUBLIC KEY INFRASTRUCTURE 319
9.8 CONFIGURACIÓN DE VPN SITE-TO-SITE 320
9.8.1 Configuración de la política ISAKMP 321
9.8.2 Configuración de los IPsec transform sets 322
9.8.3 Configuración de la Crypto ACL 325
9.8.4 Configuración del Crypto Map 325
9.8.5 Aplicación del Crypto Map a una interfaz 326
9.8.6 Configuración de ACL en una interfaz 327
9.9 VERIFICACIÓN 328
9.10 CONFIGURACIÓN DE IPSEC CON CCP 330
9.11 VPN DE ACCESO REMOTO 339
9.11.1 SSL VPN 339
9.11.2 Cisco Easy VPN 342
9.11.3 Servidor Cisco Easy VPN 344
9.12 FUNDAMENTOS PARA EL EXAMEN 351

ANEXO 1. INTRODUCCIÓN A IPV6 353
DIRECCIONAMIENTO IPV6 353
Formato del direccionamiento IPv6 355
Tipos de comunicación IPv6 356

ANEXO 2. CUESTIONARIO 357
PREPARATIVOS PARA EL EXAMEN 357
Recomendaciones para la presentación al examen 357
CUESTIONARIO TEMÁTICO 358

ÍNDICE ALFABÉTICO 397

INTRODUCCIÓN

El crecimiento exponencial de Internet y la constante evolución de sus vulnerabilidades hace que los especialistas en seguridad y gestión de riesgos en las redes se encuentren entre los más buscados por las organizaciones de todo el mundo y la demanda sigue en aumento. La escasez de candidatos cualificados con el conocimiento especializado y habilidades necesarias para administrar dispositivos y aplicaciones en una infraestructura segura, hace de la certificación CCNA Security una de las más reconocidas en la actualidad.

El CCNA Security (*Cisco Certified Network Associate Security*) valida a nivel de asociado los conocimientos y habilidades necesarios para asegurar las redes de Cisco, reconocer las vulnerabilidades de la red y mitigar las amenazas de seguridad. El examen 640-554 IINS (*Implementing Cisco IOS Network Security*) permite la obtención de la certificación CCNA Security.

Este examen evalúa los conocimientos del candidato para asegurar routers y switches Cisco y sus redes asociadas. Pone a prueba las habilidades para la instalación, reparación y supervisión de dispositivos de red, para mantener la integridad, confidencialidad y disponibilidad de datos y dispositivos y desarrolla la competencia en las tecnologías que Cisco utiliza en su infraestructura de seguridad.

Las características de este libro ayudan a facilitar la comprensión de los temas, presentados de manera resumida pero detallada, con explicaciones, notas y llamadas para permitir que el lector recuerde lo fundamental y concreto a la hora de presentarse al examen de certificación. Los ejemplos de configuraciones de cada tema fueron realizados con dispositivos reales por el autor, siendo muy

recomendable que el lector los realice en equipos reales o en simuladores para su completa comprensión y análisis.

Debido a la idea práctica y concreta de esta guía de estudio es recomendable poseer conocimientos previos a la lectura de estas páginas sobre TCP/IP, modelo OSI, enrutamiento, conmutación, ACL, etc.

Las preguntas finales son ejemplos similares a los que aparecen en el examen de certificación CCNA 640-554 IINS; por lo tanto, es importante para lograr el éxito deseado leerlas y analizarlas detenidamente hasta tener un completo dominio de cada tema. Todas las respuestas están contenidas en esta guía de estudio.

Los puntos siguientes son pautas generales que pueden ser incluidos en el contenido del examen 640-554 IINS. Sin embargo, otros temas relacionados también pueden aparecer en cualquier entrega específica de la prueba.

- **Las amenazas de seguridad comunes**.
  - Describir las amenazas comunes a la seguridad.

- **Seguridad y routers Cisco**.
  - Implementación de seguridad en routers Cisco.
  - Describir y asegurar el plano control, el plano datos y el plano de gestión.
  - Describir Cisco Security Manager.
  - Describir la transición de IPv4 a IPv6.

- **AAA en dispositivos Cisco**.
  - Describir AAA.
  - Implementar AAA.
  - Describir TACACS+.
  - Describir RADIUS.
  - Verificar la funcionalidad AAA.

- **Listas de acceso**.
  - Describir las ACL IP estándar, extendidas y nombradas.
  - Describir las consideraciones en la construcción de las ACL.
  - Aplicar las ACL IP para mitigar las amenazas en la red.

- **Gestión y administración de una red segura.**
  - Describir la administración de red segura.
  - Implementar la administración de red segura.

- **Ataques comunes de Capa 2.**
  - Describir la seguridad en un switch de capa 2.
  - Describir la seguridad con VLAN.
  - Implementación de VLAN y enlaces troncales.
  - Implementar spanning tree.

- **Tecnologías Cisco Firewall.**
  - Ventajas y desventajas operativas de las diferentes tecnologías de firewall.
  - Describir los firewalls stateful.
  - Implementar zona de seguridad basado en la política de uso de CCP.
  - Implementar el Cisco Adaptive Security Appliance (ASA).
  - Implementar NAT y PAT.

- **Cisco IPS.**
  - Describir la implementación de Cisco System Prevención (IPS).
  - Describir las tecnologías IPS.
  - Configurar el Cisco IOS IPS utilizando CCP.

- **Tecnologías VPN.**
  - Describir los diferentes métodos utilizados en criptografía.
  - Describir las tecnologías VPN.
  - Describir los componentes básicos de IPsec.
  - Implementar un IOS IPsec de sitio a sitio VPN con autenticación de clave previamente compartida.
  - Verificar las operaciones VPN.
  - Implementar Secure Sockets Layer (SSL) VPN utilizando el administrador de dispositivos ASA.

Con el fin de reflejar mejor el contenido del examen, idiomas, tiempo de evaluación, etc., puede ver toda la información disponible en:

https://learningnetwork.cisco.com/community/certifications/security_ccna/iins?tab=1

https://learningnetwork.cisco.com/docs/DOC-13753

Para lograr la certificación CCNA Security es necesario como requisito previo estar en posesión de la certificación CCNA o de alguna de las especialidades del CCIE. La certificación tiene un período de validez de tres años, puede recertificarse con el mismo examen o con cualquier examen superior.

Los exámenes constan de diferentes tipos y modalidades de preguntas:

- Respuesta única a partir de opciones múltiples.
- Respuestas múltiples a partir de opciones múltiples.
- Respuestas tipo *drag and drop*.
- Completar los espacios en blanco.
- Configuración de dispositivos con simulador.

Para mayor información sobre localización de centros de certificación autorizados, requisitos, horarios, precios u otro tipo de información puede consultarse la web de Pearson-Vue en *http://www.vue.com*.

Los estudiantes que deseen presentarse al examen de certificación 640-554 IINS deben cumplir las políticas de privacidad de Cisco Systems:

- Las personas de entre 13 y 17 años pueden presentarse al examen de certificación con el consentimiento de los padres o tutores.
- Las personas mayores de 18 años pueden presentase sin ningún tipo de restricción.
- Los menores de 13 años no pueden presentarse al examen.

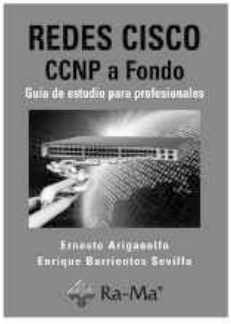
Los candidatos deben asumir el compromiso de integridad y confidencialidad de Cisco prohibiendo acciones que describan cualquier información acerca del examen de certificación. Más información en:

http://www.cisco.com/web/learning/downloads/Cisco-Career-Certifications-and-Confidentiality-Agreement_v13.pdf

Los libros de la serie REDES CISCO son un complemento a esta guía de estudio. Para aquellos que persiguen la certificación CCNA 640-802 o la certificación profesional CCNP serán sin duda un material de consulta necesario y permanente.

Editorial Ra-Ma
ISBN: 978-84-9964-094-5

Editorial Ra-Ma
ISBN: 978-84-9964-049-5



Editorial Ra-Ma
ISBN: 978-84-7897-966-0

Bibliografía de referencia:

- *www.cisco.com*
- Curricula 1.1 CCNA Security
- CCNP a fondo, editorial RA-MA

Convenciones sobre sintaxis de comandos

Las convenciones que se utilizan para representar la sintaxis de comandos en este libro son las mismas que se utilizan en *Cisco IOS Command Reference*. El autor ha preferido conservar los argumentos en idioma inglés tal como aparecerían tras ejecutar un comando de ayuda.

- La **negrita** representa comandos y palabras clave que se escriben tal y como se muestra.
- La *cursiva* indica argumentos para los que hay que suministrar valores.
- Los corchetes [ ] indican elementos opcionales.

- Las llaves { } contienen una elección de palabras clave necesarias.
- Las barras verticales | separan elementos alternativos y exclusivos entre sí.
- Las llaves y las barras verticales entre corchetes, por ejemplo [x {y | z}], indican una opción necesaria en un elemento opcional. No es necesario introducir lo que hay entre los corchetes, pero si lo hace, tendrá algunas opciones necesarias en los corchetes.

Advertencia

Se ha realizado el máximo esfuerzo para hacer de este libro una obra tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". Los autores no serán responsables ante cualquier persona o entidad con respecto a cualquier pérdida, daño o perjuicio que pudieran resultar emergentes de la información contenida en este libro.

Todos los términos mencionados en este libro que, según consta, pertenecen a marcas comerciales o marcas de servicios, se utilizan únicamente con fines educativos. No debe considerarse que la utilización de un término en este libro afecte la validez de cualquier marca comercial o de servicio.

Los conceptos, opiniones y gráficos expresados en este libro por los autores no son necesariamente los mismos que los de Cisco Systems, Inc.

Los iconos y topologías mostradas en este libro se ofrecen con fines de ejemplo y no representan necesariamente un modelo de diseño para redes.

Las configuraciones y salidas de los routers, switches y/o cualquier otro dispositivo se han tomado de equipos reales y se ha verificado su correcto funcionamiento. No obstante, cualquier error en la transcripción es absolutamente involuntario.

Acerca del autor

Ernesto Ariganello es ingeniero en telecomunicaciones y especialista en electrónica de hardware de alta complejidad. Es CCNP e instructor certificado de la Cisco Networking Academy, imparte cursos relacionado con redes y comunicaciones. Trabaja, además, como consultor para varias empresas de la Unión Europea. Su labor en educación y formación es sumamente valorada en Europa y Latinoamérica, fundamentada en clases claras, dinámicas y muy prácticas, por donde han pasado más de 1.000 alumnos por diferentes centros de formación y empresas.

Ha editado varios libros de la serie REDES CISCO, de los cuales su primera obra, *Guía de estudio para la certificación CCNA*, y la *Guía de estudio para la certificación CCNP* han sido reconocidas como las pioneras con contenidos escritos íntegramente en español.

Agradecimientos

Nuevamente y en primer lugar agradezco al lector por confiar en mi trabajo y por honrarme con su interés en aprender con este libro.

A Sergio Matías Mujica, por haber dedicado muchas horas de esfuerzo personal colaborando en la realización de las configuraciones con los dispositivos y por investigar para las prácticas con simuladores.

A Diego Romero García, por su constante paciencia, siempre dispuesto a echarme una mano en los diseños de este y los anteriores libros.

A mi amigo Pablo Roberto García, por enseñarme la fortaleza de la constancia. Por ser un ejemplo de entereza ante los momentos más difíciles de la vida. A su familia por ser como es.

A mis editores, una vez más, por confiar en mí, dándome la posibilidad de otra nueva publicación.

Como siempre, a mi familia, a mi mujer y a mi hijo, a mis compañeros de trabajo y a los amigos de Argentina y España por su apoyo constante.

Ernesto Ariganello

Capítulo 1

FUNDAMENTOS DE SEGURIDAD EN LAS REDES

1.1 PRINCIPIOS DE UNA RED SEGURA

Mantener una red segura garantiza la seguridad de la red y de los usuarios y protege los intereses comerciales. Esto requiere vigilancia de parte de los profesionales de seguridad en redes, quienes deberán estar constantemente al tanto de las nuevas y evolucionadas amenazas y ataques a las redes, así como también de las vulnerabilidades de los dispositivos y aplicaciones. La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más adelante de los hackers malintencionados.

La complejidad de la seguridad en redes dificulta dominar todo lo que esta abarca. Varias organizaciones han creado dominios que subdividen el mundo de la seguridad en redes en segmentos más fácilmente manejables. Estas organizaciones establecen estándares, fomentan la colaboración y proveen oportunidades de desarrollo para los profesionales de la seguridad.

Tal como la seguridad en redes está compuesta de dominios, los ataques a las redes son clasificados para hacer más fácil el aprender de ellos y abordarlos apropiadamente. Los virus, los gusanos y los troyanos son tipos específicos de ataques a las redes. Generalmente, los ataques a las redes se clasifican como ataques de reconocimiento, de acceso o de denegación de servicio. Los profesionales de la seguridad en redes son responsables de crear y mantener la política de seguridad de red. Todas las prácticas de seguridad en redes están relacionadas con y guiadas por la política de seguridad en redes.

1.1.1 Evolución de la seguridad en redes

Hoy en día, Internet es una red muy diferente a la que era en sus comienzos en los años sesenta. El trabajo de un profesional de redes incluye asegurarse de que el personal apropiado esté muy versado en herramientas, procesos, técnicas, protocolos y tecnologías de seguridad en redes. Es crítico que los profesionales de seguridad en redes mantengan una paranoia saludable para manejar la colección de amenazas a las redes en constante evolución.

Una de las primeras herramientas de seguridad de redes fue el sistema de detección de intrusos **IDS**, desarrollado por SRI International en 1984. Un IDS provee detección en tiempo real de ciertos tipos de ataques mientras están en progreso. Esta detección permite a los profesionales de redes mitigar más rápidamente el impacto negativo de dichos ataques en los dispositivos de red y los usuarios. A fines de los años noventa, el sistema de prevención de intrusos **IPS** comenzó a reemplazar a la solución IDS. Los dispositivos IPS permiten detectar actividad maliciosa y tienen la habilidad de bloquear el ataque automáticamente en tiempo real.

Además de las soluciones IPS e IDS, se desarrollaron los firewalls para prevenir que tráfico no deseado ingresara a ciertas áreas señaladas dentro de una red, proporcionando seguridad de perímetro. En 1988, Digital Equipment Corporation (**DEC**) creó el primer firewall de red en la forma de un filtro de paquetes. Estos primeros firewalls inspeccionaban los paquetes para verificar que se correspondieran con conjuntos de reglas predefinidas, con la opción de permitirlos o descartarlos. Los firewalls de filtrado de paquetes inspeccionan cada paquete aisladamente sin examinar si es parte de una conexión existente. En 1989, AT&T Bell Laboratories desarrolló el primer *firewall stateful*. Como los firewalls de filtrado de paquetes, los firewalls de estados utilizan reglas predefinidas para permitir o denegar tráfico. A diferencia de los firewalls de filtrado de paquetes, los firewalls stateful hacen seguimiento de las conexiones establecidas y determinan si un paquete pertenece a un flujo de datos existente, ofreciendo mayor seguridad y procesamiento más rápido.

Los firewalls originales eran prestaciones de software agregadas a dispositivos de red existentes, como routers. Con el tiempo, varias empresas desarrollaron firewalls dedicados o autónomos, que permiten a los routers y switches liberar la memoria y el procesador de la intensiva actividad de filtrar paquetes. Para las organizaciones que no requieren un firewall dedicado, los routers modernos, como el *Router de Servicios Integrados Cisco* (**ISR**), pueden ser utilizados como sofisticados firewalls stateful.

Además de encargarse de las amenazas que provienen de afuera de la red, los profesionales de redes deben también estar preparados para amenazas que provengan desde dentro de la misma. Las amenazas internas, ya sean intencionales o accidentales, pueden causar aún más daño que las amenazas externas, por el acceso directo y conocimiento de la red y datos corporativos. A pesar de este hecho, el desarrollo de herramientas y técnicas para mitigar amenazas internas ha tardado varias décadas luego de la introducción de herramientas y técnicas para mitigar amenazas externas.

La mayoría de las amenazas desde dentro de la red revelan los protocolos y tecnologías utilizados en la red de área local o la infraestructura conmutada. Estas amenazas internas caen, básicamente, en dos categorías: falsificación y DoS.

- **Ataques de falsificación**: son ataques en los que un dispositivo intenta hacerse pasar por otro falsificando datos. Por ejemplo, la falsificación de direcciones MAC ocurre cuando un ordenador envía paquetes de datos cuya dirección MAC corresponde a otro ordenador. Como este, existen otros tipos de ataques de falsificación.

- **Ataques de DoS**: hacen que los recursos de un ordenador no estén disponibles para los usuarios a los que estaban destinados. Los hackers usan varios métodos para lanzar ataques de DoS.

NOTA:

Evolución de las tecnologías de seguridad:

- ✓ *1988, DEC Packet Filter Firewall.*
- ✓ *1989, AT&T Bell Labs Stateful Firewall.*
- ✓ *1991, DEC SEAL Application Layer Firewall.*
- ✓ *1994, Check Point Firewall.*
- ✓ *1995, NetRanger IDS.*
- ✓ *1997, RealSecure IDS.*
- ✓ *1998, Snort IDS.*
- ✓ *1999, Primer IPS.*
- ✓ *2006, Cisco Zone-Based Policy Firewall.*
- ✓ *2010, Cisco Security Intelligence Operations.*

1.1.2 Claves para la protección de datos

Además de prevenir y denegar tráfico malicioso, la seguridad en redes también requiere que los datos se mantengan protegidos. La criptografía, el estudio y práctica de ocultar información, es ampliamente utilizada en la seguridad de las redes modernas. Hoy en día, cada tipo de comunicación de red tiene un protocolo o tecnología correspondiente, diseñado para ocultar esa comunicación de cualquier otro que no sea el usuario al que está destinada.

Los datos inalámbricos pueden ser cifrados utilizando varias aplicaciones de criptografía. Se puede cifrar una conversación entre dos usuarios de teléfonos IP y también pueden ocultarse con criptografía los archivos de un ordenador. La criptografía puede ser utilizada en casi cualquier comunicación de datos. De hecho, la tendencia apunta a que todas las comunicaciones sean cifradas.

Los tres objetivos principales de la seguridad de la red son:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

La criptografía asegura la confidencialidad de los datos. La seguridad de la información comprende la protección de la información y de los sistemas de información de acceso, uso, revelación, interrupción, modificación o destrucción no autorizados. El cifrado provee confidencialidad al ocultar los datos que van en texto plano.

Algunos ejemplos para proporcionar confidencialidad a la red pueden ser:

- Utilizar los mecanismos de seguridad de red como por ejemplo, los firewalls y las listas de control de acceso.
- Exigir credenciales apropiadas por ejemplo, nombres de usuario y contraseñas, para acceder a los recursos de red específicos.
- Cifrar todo el tráfico de manera que un atacante no pueda descifrar el tráfico que se apropio de la red.

La integridad de datos asegura que estos no han sido modificados en tránsito. La integridad de datos podría realizar la autenticación de origen para verificar que el tráfico se origina en la fuente que realmente lo envió. Algunos ejemplos de violaciones de integridad incluyen:

- Modificar la apariencia de una página web corporativa.
- Interceptar y alterar una transacción de comercio electrónico.
- Modificación de los registros financieros almacenados electrónicamente.

La disponibilidad de datos es una forma de medición de la accesibilidad a los datos o recursos. Por ejemplo, si un servidor no está disponible cinco minutos al año, tendría una disponibilidad del 99,999 %. Algunos ejemplos de cómo un atacante podría intentar poner en peligro la disponibilidad de una red son:

- Enviar incorrectamente datos formateados a un dispositivo conectado en red, dando como resultado un error de excepción no controlada.
- Inundar un sistema de red con una cantidad excesiva de tráfico o de solicitudes. Esto consumiría los recursos del sistema de procesamiento y evitaría que el sistema respondiese a las solicitudes legítimas (ataque de denegación de servicio DoS).

NOTA:

Evolución de las tecnologías de protección de datos:

- ✓ *1993, Túneles Cisco GRE.*
- ✓ *1996, VPN Site-to-Site IPsec.*
- ✓ *1999, SSH.*
- ✓ *2000, MPLS.*
- ✓ *2001, Acceso remoto VPN IPsec.*
- ✓ *2002, Dynamic Multipoint VPN.*
- ✓ *2005, SSL VPN.*
- ✓ *2009, GET VPN.*

1.1.3 Hacking

La palabra *hackers* tiene una variedad de significados. Generalmente son programadores que intentan ganar acceso no autorizado a dispositivos en Internet. También se utiliza para referirse a individuos que ejecutan programas para impedir o reducir la velocidad del acceso a las redes por parte de un gran número de

usuarios, o corromper o eliminar los datos de los servidores. Pero para otros, el término hacker tiene una interpretación positiva como un profesional de redes que utiliza habilidades de programación sofisticadas para asegurarse de que las redes no sean vulnerables a ataques. Bueno o malo, el **hacking** es una fuerza impulsora de la seguridad en redes.

El trabajo del profesional de seguridad en redes es el de estar siempre un paso más adelante que los hackers capacitándose y participando en organizaciones de seguridad. El profesional de seguridad en redes también debe tener acceso a herramientas de seguridad, protocolos, técnicas y tecnologías de última generación. Al mismo tiempo debe mantenerse al tanto de actividades maliciosas y tener las habilidades y herramientas para minimizar o eliminar las amenazas asociadas con esas actividades. En relación con otras profesiones tecnológicas, la seguridad en redes tiene la curva de aprendizaje más empinada y la mayor demanda de participación constante en el desarrollo profesional.

El hacking comenzó en la década de 1960 con el phone freaking, o phreaking, que se refiere al hecho de usar varias frecuencias de radio para manipular los sistemas de telefonía. El phreaking empezó cuando AT&T comenzó a incluir conmutadores automáticos en sus sistemas telefónicos. Los conmutadores telefónicos utilizaban tonos, o marcación por tonos, para indicar diferentes funciones, como el marcado y la terminación de una llamada. Algunos clientes se percataron de que, imitando un tono usando un silbato, podían explotar los conmutadores telefónicos para efectuar llamadas a larga distancia gratuitas.

A medida que los sistemas de comunicación evolucionaron, los métodos de hacking los fueron siguiendo.

NOTA:

Cronología de los ataques más conocidos:

- ✓ *1978, primer* spam *en ARPAnet.*
- ✓ *1988, virus Morris en Internet.*
- ✓ *1999, virus Melissa de correo electrónico.*
- ✓ *2000, ataque DoS Mafiaboy, gusano Love Bug.*
- ✓ *2001, ataque de DoS Code Red.*
- ✓ *2004, Botnet ataca los sistemas militares de EE.UU.*
- ✓ *2007, Storm botnet, filtrado de datos de tarjeta de crédito TJX.*
- ✓ *2008, fraude de acciones Société Générale.*
- ✓ *2011, ataque a Sony PlayStation.*

1.1.4 Organizaciones de seguridad en redes

Los profesionales de la seguridad en redes deben colaborar con colegas profesionales más frecuentemente que en la mayoría de las otras profesiones. Esto incluye asistir a workshops y conferencias que generalmente están asociadas, patrocinadas u organizadas por organizaciones tecnológicas locales, nacionales o internacionales.

Tres de las organizaciones de seguridad en redes mejor establecidas son:

- **SANS** (*SysAdmin, Audit, Network, Security Institute*). SANS se estableció en 1989 como una organización cooperativa de investigación y educación. El objetivo de SANS es la capacitación y certificación en seguridad de la información. SANS desarrolla documentos de investigación sobre varios aspectos de la seguridad de la información.

- **CERT** (*Computer Emergency Response Team*). Fue creado para trabajar con la comunidad de Internet para detectar y resolver incidentes de seguridad. El CERT responde a acontecimientos de seguridad serios y analiza las vulnerabilidades de los productos. El CERT trabaja para administrar los cambios relacionados con técnicas progresivas de intrusión y con las dificultades en detectar ataques y atrapar a los atacantes.

- El CERT se ocupa de cinco áreas:

    - Aseguramiento del software.
    - Sistemas seguros.
    - Seguridad en las organizaciones.
    - Respuesta coordinada.
    - Educación y capacitación

- **(ISC)^2** *International Information Systems Security Certification Consortium*. Provee productos y servicios educativos independientes del proveedor en más de 135 países. (ISC)^2 es reconocido universalmente por sus cuatro certificaciones de seguridad de la información, incluyendo una de las certificaciones más populares en la profesión de seguridad en redes, el *Certified Information Systems Security Professional* (**CISSP**).

Existen otras organizaciones de seguridad en redes que también son importantes para los profesionales de la seguridad en redes. **InfoSysSec** es una organización de seguridad en redes que aloja un portal de novedades de seguridad, proporcionando las últimas novedades en cuanto a alertas, *exploits* y vulnerabilidades. La **Mitre Corporation** mantiene una lista de las vulnerabilidades y exposiciones comunes, utilizadas por organizaciones de seguridad de redes de gran prestigio. **FIRST** es una organización de seguridad que reúne una variedad de equipos de respuesta a incidentes de seguridad de organizaciones gubernamentales, comerciales y educativas, para fomentar la cooperación y coordinación en el intercambio de información, la prevención de incidentes y la rápida reacción. Finalmente, el Center for Internet Security (**CIS**) es un emprendimiento sin fines de lucro que desarrolla puntos de referencia en la configuración de la seguridad a través de consensos globales para reducir el riesgo de interrupciones en los negocios y el comercio electrónico.

Además de los sitios web de las organizaciones de seguridad, una de las herramientas más útiles para los profesionales de la seguridad en redes es la de los *feeds Really Simple Syndication* (**RSS**). RSS es una familia de formatos basados en XML utilizados para publicar información actualizada, permitiendo que las actualizaciones lleguen en tiempo y forma desde sitios web particulares o agregar canales de varios sitios a un solo lugar.

1.1.5 Dominios de la seguridad en redes

Los dominios proveen un marco organizado para facilitar el aprendizaje sobre la seguridad en redes. Es importante entender el funcionamiento de cada uno de los dominios de la seguridad en redes.

Existen 12 dominios de seguridad en redes descriptos por **ISO/IEC 27002**, que sirven para organizar a alto nivel la información dentro de la seguridad en redes. Estos dominios tienen algunos paralelismos significativos con los dominios definidos por la certificación **CISSP**. Los 12 dominios están diseñados para servir como base común para desarrollar los estándares de seguridad en las organizaciones y las prácticas de administración de seguridad efectiva, así como también para ayudar a construir confianza en las actividades que tienen lugar dentro de la organización.

Los dominios de la seguridad en redes proveen una separación conveniente para los elementos de la seguridad en redes. Estos 12 dominios sirven como referencia útil para avanzar en el trabajo como profesional de la seguridad en redes.

1. **Evaluación de riesgos**: es el primer paso en el proceso de administración de riesgos. Determina el valor cuantitativo y cualitativo del riesgo relacionado con una amenaza reconocida o situación determinada.

2. **Política de seguridad**: es un documento que trata las restricciones y comportamientos de los miembros de una organización y generalmente especifica cómo se puede acceder a los datos y quién puede hacerlo.

3. **Organización de la seguridad de la información**: es el modelo de gobierno establecido por una organización para la seguridad de la información.

4. **Administración de los bienes**: es un inventario y esquema de clasificación para los bienes de información.

5. **Seguridad de los recursos humanos**: trata sobre los procedimientos de seguridad que guardan relación con los empleados de una organización que entran, se mueven o se van de ella.

6. **Seguridad física y ambiental**: describe la protección de las instalaciones reales de los ordenadores dentro de una organización.

7. **Administración de las comunicaciones y las operaciones**: describe la administración de los controles técnicos de seguridad en sistemas y redes.

8. **Control de acceso**: describe la restricción de derechos a redes, sistemas, aplicaciones, funciones y datos.

9. **Adquisición, desarrollo y mantenimiento de los sistemas de información**: describe la integración de la seguridad a las aplicaciones.

10. **Administración de incidentes de seguridad de la información**: describe cómo anticipar y responder a las fisuras de seguridad de la información.

11. **Administración de la continuidad de los negocios**: describe la protección, mantenimiento y recuperación de procesos y sistemas críticos para los negocios.

12. **Conformidad**: describe el proceso de asegurar conformidad con las regulaciones, los estándares y las políticas de la seguridad de la información.

1.1.6 Políticas de seguridad en redes

Uno de los dominios más importantes es el de las políticas de seguridad. Una política de seguridad es una declaración formal de las reglas a las cuales deberán atender las personas que tienen acceso a los bienes tecnológicos y de información de una organización. La conceptualización, el desarrollo y la aplicación de una política de seguridad tienen un rol significativo en mantener a la organización segura. Es responsabilidad del profesional de la seguridad en redes hacer cumplir las políticas de seguridad en todos los aspectos de las operaciones de negocios en la organización.

La política de seguridad en redes es un documento amplio diseñado para ser claramente aplicable a las operaciones de una organización. Por su amplitud de cobertura e impacto, generalmente es un comité el que lo compila. Es un documento complejo que está diseñado para gobernar temas como acceso a los datos, navegación en la Web, uso de las contraseñas, criptografía y adjuntos de correo electrónico.

La política de seguridad en redes traza las reglas de acceso a la red, determina cómo se harán cumplir las políticas y describe la arquitectura básica del ambiente básico de seguridad de la información de la empresa.

Antes de crear una política debe entenderse qué servicios están disponibles para qué usuarios. La política de seguridad de red establece una jerarquía de permisos de acceso y da a los empleados solo el acceso mínimo necesario para realizar sus tareas.

La política de seguridad de la red establece qué bienes deben ser protegidos y da pautas sobre cómo deben ser protegidos. Esto será luego usado para determinar los dispositivos de seguridad y las estrategias y procedimientos de mitigación que deberán ser implementados en la red. Una posible orientación que los administradores pueden utilizar en el desarrollo de la política de seguridad y la determinación de distintas estrategias de mitigación es la arquitectura de **Cisco SecureX**.

1.1.7 Cisco SecureX Architecture

Cisco SecureX permite a las grandes organizaciones y a las pequeñas empresas colaborar fácilmente. Al utilizar una amplia gama de parámetros en su aplicación de las políticas proporciona una seguridad más eficaz y sensible al contexto de la situación en que se produce el acceso a la red.

Además generaliza el lenguaje de políticas de seguridad en toda la red pudiendo así ser desplegadas a nivel mundial y estar disponibles donde y cuando los usuarios lo necesiten.

Con su aplicación de políticas de seguridad sensibles al contexto, la arquitectura de seguridad de red Cisco SecureX proporciona:

1. **Seguridad de red a un nivel superior**: basada en un lenguaje de políticas de seguridad que comprenden la totalidad del contexto del acceso a la red: el qué, quién, dónde, cuándo y cómo se accede a la red.

2. **Un acceso a la red de alta seguridad en los diferentes entornos**: en entornos virtuales, físicos, en las instalaciones y en entornos de nube para permitir y garantizar una aplicación coherente de las políticas de seguridad de red.

3. **Simplificar las políticas de seguridad de red**: para corresponderse directamente con las necesidades y normas de negocio.

4. **Protección contra las amenazas a medida que van siendo identificadas**: mediante el uso del conocimiento global de *Cisco Security Intelligence Operations* (**SIO**), para proporcionar correlación y protección en tiempo real.

5. **Soportar todo tipo de terminales**: Incluyendo todos los nuevos terminales que son utilizados en el acceso a la red, desde PC portátiles a dispositivos móviles de siguiente generación como Cisco Cius, iPads, iPhones y otros teléfonos inteligentes.

Uno de los pasos más importantes al crear una política es el de identificar los bienes críticos. Estos pueden incluir bases de datos, aplicaciones vitales, información de clientes y empleados, información comercial clasificada, discos compartidos, servidores de correo electrónico y servidores web.

1.2 VULNERABILIDADES

Las principales vulnerabilidades de los dispositivos finales son los ataques de virus, gusanos y troyanos.

1.2.1 Virus

Un virus informático es un programa que tiene por objeto alterar el normal funcionamiento del ordenador sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones por desconocimiento del usuario. El código del virus queda alojado en el ordenador, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente, se añade el código del virus al programa infectado y se graba en el disco duro, con lo cual el proceso de replicado se completa.

1.2.2 Gusanos

Un gusano (*Worm*) es un programa que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos del ordenador que atacan. Mientras que los virus requieren un programa huésped para ejecutarse, los gusanos pueden ejecutarse solos.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de ordenadores para enviar copias de sí mismos a otros terminales en la red y son capaces de llevar esto a cabo sin intervención del usuario, propagándose utilizando Internet, basándose en diversos métodos, como SMTP, IRC o P2P, entre otros.

1.2.3 Troyanos

En informática se denomina troyano a un programa malicioso que se presenta al usuario como un software aparentemente legítimo e inofensivo, pero que al ejecutarlo ocasiona daños.

Los troyanos pueden realizar diferentes tareas, pero en la mayoría de los casos crean una puerta trasera que permite la administración remota a un usuario no autorizado. Un troyano no es estrictamente un virus informático y la principal diferencia es que los troyanos no propagan la infección a otros sistemas por sí mismos.

Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, el individuo puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso. Las acciones que el individuo puede realizar en el equipo remoto dependen de los privilegios que tenga el usuario en el ordenador remoto y de las características del troyano.

Los troyanos generalmente se clasifican de acuerdo al daño que causan o a la manera en que violan el sistema:

1. **Troyanos de acceso remoto**: permiten el acceso remoto no autorizado.
2. **Troyano de envío de datos**: provee al atacante de datos sensibles, como contraseñas.
3. **Troyano destructivo**: corrompe o elimina archivos.
4. **Troyano proxy**: el ordenador del usuario funciona como un servidor proxy.
5. **Troyano FTP**: abre el puerto 21.
6. **Troyano inhabilitador de software de seguridad**: detiene el funcionamiento de programas antivirus y/o firewalls.
7. **Troyano de denegación de servicio**: reduce la velocidad o detiene la actividad en la red.

1.2.4 Mitigación de virus, gusanos y troyanos

El principal recurso para la mitigación de ataques de virus y troyanos es el software antivirus. El software antivirus ayuda a prevenir a los hosts de ser infectados y diseminar código malicioso. Requiere mucho más tiempo limpiar ordenadores infectados que mantener al software antivirus actualizado en las mismas máquinas.

La mayoría de las vulnerabilidades descubiertas en el software tienen relación con el desbordamiento del buffer. Un buffer es un área de la memoria utilizada por los procesos para almacenar datos temporariamente. Un desbordamiento en el buffer ocurre cuando un buffer de longitud fija llena su capacidad y un proceso intenta almacenar datos más allá de ese límite máximo. Esto puede dar por resultado que los datos extra sobreescriban localizaciones de memoria adyacentes o causen otros comportamientos inesperados. Los desbordamientos de buffer son generalmente el conducto principal a través del cual los virus, gusanos y troyanos hacen daño.

Los gusanos dependen más de la red que los virus. La mitigación de gusanos requiere diligencia y coordinación por parte de los profesionales de la seguridad en redes. La respuesta a una infección de un gusano puede separarse en cuatro fases:

- **Fase de contención**: consiste en limitar la difusión de la infección del gusano de áreas de la red que ya están infectadas. La contención requiere el uso de ACL y firewalls.

- **Fase de inoculación**: durante la fase de inoculación todos los sistemas no infectados reciben un parche del vendedor apropiado para la vulnerabilidad.

- **Fase de cuarentena**: incluye el rastreo y la identificación de máquinas infectadas dentro de las áreas contenidas y su desconexión, bloqueo o eliminación.

- **Fase de tratamiento**: consiste en terminar el proceso del gusano, eliminar archivos modificados o configuraciones del sistema que el gusano haya introducido e instalar un parche para la vulnerabilidad que el gusano usaba para explotar el sistema.

Los virus, gusanos y troyanos pueden hacer lentas a las redes o detenerlas completamente y corromper o destruir datos. Hay opciones de hardware y software disponibles para mitigar estas amenazas.

1.3 METODOLOGÍAS DE ATAQUE

Hay varios tipos diferentes de ataques de red que no son virus, gusanos o troyanos. Para mitigar los ataques es útil tener a los diferentes tipos de ataques categorizados. Al categorizarlos es posible abordar tipos de ataques en lugar de ataques individuales. No hay un estándar sobre cómo categorizar los ataques de red. El método utilizado en este caso clasifica los ataques en tres categorías principales.

1.3.1 Ataques de reconocimiento

Los ataques de reconocimiento consisten en el descubrimiento y mapeo de sistemas, servicios o vulnerabilidades sin autorización. Los ataques de reconocimiento muchas veces emplean el uso de sniffers de paquetes y escáneres de puertos, los cuales están ampliamente disponibles para su descarga gratuita en Internet. El reconocimiento es análogo a un ladrón vigilando un vecindario en busca de casas vulnerables para robar, como una residencia sin ocupantes o una casa con puertas o ventanas fáciles de abrir.

Los ataques de reconocimiento son generalmente precursores de ataques posteriores con la intención de ganar acceso no autorizado a una red o interrumpir el funcionamiento de la misma.

Los ataques de reconocimiento utilizan varias herramientas para ganar acceso a una red:

- **Sniffers de paquetes**: es una aplicación de software que utiliza una tarjeta de red en modo promiscuo para capturar todos los paquetes de red que se transmitan a través de una LAN.
- **Barridos de ping**: es una técnica de escaneo de redes básica que determina qué rango de direcciones IP corresponde a los hosts activos.
- **Escaneo de puertos**: escaneo de un rango de números de puerto TCP o UDP en un host para detectar servicios abiertos.
- **Búsquedas de información en Internet**: pueden revelar información sobre quién es el dueño de un dominio particular y qué direcciones han sido asignadas a ese dominio.

1.3.2 Ataques de acceso

Los ataques de acceso explotan vulnerabilidades conocidas en servicios de autenticación, FTP y web, para ganar acceso a cuentas web, bases de datos confidenciales y otra información sensible. Un ataque de acceso puede efectuarse de varias maneras. Un ataque de acceso generalmente emplea un ataque de diccionario para adivinar las contraseñas del sistema. También hay diccionarios especializados para diferentes idiomas.

Hay cinco tipos de ataques de acceso:

1. **Ataques de contraseña**: el atacante intenta adivinar las contraseñas del sistema. Un ejemplo común es un ataque de diccionario.

2. **Explotación de la confianza**: el atacante usa privilegios otorgados a un sistema en una forma no autorizada, posiblemente causando que el objetivo se vea comprometido.

3. **Redirección de puerto**: se usa un sistema ya comprometido como punto de partida para ataques contra otros objetivos. Se instala una herramienta de intrusión en el sistema comprometido para la redirección de sesiones.

4. **Ataque *Man in the Middle***: el atacante se ubica en medio de una comunicación entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes.

5. **Desbordamiento de buffer**: el programa escribe datos más allá de la memoria de buffer. Un resultado del desbordamiento es que los datos válidos se sobreescriben o explotan para permitir la ejecución de código malicioso.

1.3.3 Ataques de denegación de servicio

Los ataques de denegación de servicio (**DoS**) envían un número extremadamente grande de solicitudes en una red o Internet. Estas solicitudes excesivas hacen que la calidad de funcionamiento del dispositivo víctima sea inferior. Como consecuencia, el dispositivo atacado no está disponible para acceso y uso legítimo. Al ejecutar explotaciones o combinaciones de explotaciones, los ataques de DoS desaceleran o colapsan aplicaciones y procesos. Un ataque distribuido de denegación de servicio (**DDoS**) es similar en intención al ataque de DoS, excepto en que el ataque DDoS se origina en varias fuentes coordinadas.

Los ataques de DoS más comunes son:

- **Ping de la muerte**: se trata de una solicitud de eco en un paquete IP más grande que el tamaño de paquete máximo de 65.535 bytes. Enviar un ping de este tamaño puede colapsar el nodo objetivo. Una variante de este ataque es colapsar el sistema enviando fragmentos ICMP, que llenen los buffers de reensamblado de paquetes en el objetivo.

- **Ataque Smurf**: el atacante envía un gran número de solicitudes ICMP a direcciones broadcast, todos con direcciones de origen falsificadas de la misma red que la víctima. Si el dispositivo de enrutamiento que envía el tráfico a esas direcciones de broadcast reenvía los broadcast, todos los host de la red destino enviarán respuestas ICMP, multiplicando el tráfico por el número de hosts en las redes. En una red broadcast multiacceso cientos de máquinas podrían responder a cada paquete.

- **Inundación TCP/SYN**: se envía una inundación de paquetes SYN TCP, generalmente con una dirección de origen falsa. Cada paquete se maneja como una solicitud de conexión, causando que el servidor genere una conexión a medio abrir devolviendo un paquete SYN-ACK TCP y esperando un paquete de respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente es falsa, la respuesta nunca llega. Estas conexiones a medio abrir saturan el número de conexiones disponibles que el servidor puede atender, haciendo que no pueda responder a solicitudes legítimas hasta después de que el ataque haya finalizado.

1.3.4 Mitigación de ataques de red

Los ataques de inundación reconocimiento pueden ser mitigados de varias maneras. Utilizar una autenticación fuerte es una primera opción para la defensa contra sniffers de paquetes. El cifrado también es efectivo en la mitigación de estos. Si el tráfico está cifrado, es prácticamente irrelevante si un sniffer de paquetes está siendo utilizado, ya que los datos capturados no son legibles.

El software anti-sniffer y las herramientas de hardware detectan cambios en el tiempo de respuesta de los hosts para determinar si los hosts están procesando más tráfico del que sus propias cargas de tráfico indicarían. Una infraestructura conmutada es la norma hoy en día, lo cual dificulta la captura de datos que no sean los del dominio de colisión inmediato, que probablemente contenga solo un host.

Es imposible mitigar el escaneo de puertos. Sin embargo, el uso de un **IPS** y un firewall puede limitar la información que puede ser descubierta con un escáner de puerto, y los barridos de ping pueden ser detenidos si se deshabilitan el eco y la respuesta al eco ICMP en los routers de borde. Los IPS basados en red y los basados en host pueden notificar al administrador cuando está tomando lugar un ataque de reconocimiento. Esta advertencia permite al administrador prepararse mejor para el ataque o notificar al ISP sobre el lugar desde donde se está lanzando el reconocimiento.

Un número sorprendente de ataques de acceso se lleva a cabo a través de simples averiguaciones de contraseñas o ataques de diccionario de fuerza bruta contra las contraseñas. El uso de protocolos de autenticación cifrados o de hash, en conjunción con una política de contraseñas fuerte, reduce enormemente la probabilidad de ataques de acceso exitosos.

Hay prácticas específicas que ayudan a asegurar una política de contraseñas fuerte:

- Deshabilitar cuentas luego de un número específico de autenticaciones fallidas.
- Usar una contraseña de una sola vez (**OTP**) o una contraseña cifrada.
- Usar contraseñas fuertes. Las contraseñas fuertes tienen por lo menos seis caracteres y contienen letras mayúsculas y minúsculas, números y caracteres especiales.

La criptografía es un componente crítico de una red segura. Se recomienda utilizar cifrado para el acceso remoto a una red. Además, el tráfico del protocolo de enrutamiento también debería estar cifrado. Cuanto más cifrado esté el tráfico, menos oportunidad tendrán los hackers de interceptar datos con ataques *Man in the Middle*.

Un ataque de DoS puede ser truncado usando tecnologías antifalsificación (anti-spoofing) en routers y firewalls de perímetro. Hoy en día, muchos ataques de DoS son ataques distribuidos de DoS llevados a cabo por hosts comprometidos en varias redes. Mitigar los ataques DDoS requiere diagnóstico y planeamiento cuidadoso, así como también cooperación de los **ISP**.

Los elementos más importantes para mitigar los ataques de DoS son los firewalls y los IPS (**Cisco ASAs** e **ISR**). Se recomiendan fuertemente los IPS tanto basados en host como basados en red. Los routers y switches Cisco soportan

algunas tecnologías antifalsificación como seguridad de puerto, snooping de DHCP, IP Source Guard, inspección de ARP dinámico y ACL.

Por último, aunque la calidad de servicio (**QoS**) no ha sido diseñada como una tecnología de seguridad, una de sus aplicaciones, la implementación de políticas de tráfico (traffic policing), puede ser utilizada para limitar el tráfico ingresante de cualquier cliente dado en un router borde.

Recuerde:

1. Mantener parches actualizados, instalándolos cada semana o día si fuera posible, para prevenir los ataques de desbordamiento de buffer y la escalada de privilegios.

2. Cerrar los puertos innecesarios y deshabilitar los servicios no utilizados.

3. Utilizar contraseñas fuertes y cambiarlas seguido.

4. Controlar el acceso físico a los sistemas.

5. Evitar ingresos innecesarios en páginas web.

6. Realizar copias de resguardo y probar los archivos resguardados regularmente.

7. Educar a los empleados en cuanto a los riesgos de la ingeniería social y desarrollar estrategias para validar las entidades a través del teléfono, del correo electrónico y en persona.

8. Cifrar y poner una contraseña a datos sensibles.

9. Implementar hardware y software de seguridad como firewalls, IPS, dispositivos de red privada virtual, software antivirus y filtrado de contenidos y UPS para suministro eléctrico.

10. Desarrollar una política de seguridad escrita para la compañía.

1.3.5 Cisco Network Foundation Protection

Cisco **NFP** (*Network Foundation Protection*) proporciona directrices generales para la protección de la infraestructura de red. Estas directrices constituyen la base para garantizar el funcionamiento continuo del servicio.

NFP divide lógicamente a los routers y switches en tres áreas funcionales:

- **Plano de control**: responsable del correcto enrutamiento de los datos. El plano de control de tráfico consiste en paquetes generados por los dispositivos para el propio funcionamiento de la red, tales como anuncios OSPF o mensajes ARP.

- **Plano de gestión**: responsable de la gestión de elementos de la red. El plano de gestión de tráfico o de administración genera, a través de los dispositivos de red, procesos y protocolos como telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS y NetFlow.

- **Plano de datos**: responsable del envío de datos. El tráfico del plano de datos consiste sobre todo en tráfico generado por usuarios que es reenviado por el router. La mayoría del tráfico viaja a través del router o un switch a través del plano de datos.

La seguridad del plano de control se puede implementar utilizando las siguientes características:

- **Cisco AutoSecure**: proporciona en un solo paso protección sobre el plano de control, así como sobre los planos de gestión y de datos. Se trata de un script que se inicia desde la línea de comandos para configurar el nivel de seguridad de los routers. El guión desactiva los procesos no esenciales del sistema y los servicios. En primer lugar, hace recomendaciones para tratar las vulnerabilidades de seguridad y modifica la configuración del router.

- **Routing protocol authentication**: protocolo de autenticación o autenticación de vecinos, impide que un router acepte actualizaciones de enrutamiento fraudulentas. La mayoría de los protocolos de enrutamiento admite la autenticación de vecino.

- **CoPP** (*Control Plane Policing*): es una característica del Cisco IOS diseñado para permitir a los usuarios controlar el flujo de tráfico que maneja el procesador. CoPP está diseñado para evitar el tráfico innecesario en la ruta que pueda abrumar el procesador. La función de CoPP trata del plano de control como una entidad separada con sus propios puertos de entrada (*input*) y salida (*output*).

CoPP consta de las siguientes características:

- **CoPP** (*Control Plane Policing*): permite a los usuarios configurar un filtro de calidad de servicio que gestiona el flujo de tráfico de paquetes del plano control protegiéndolo contra los ataques de reconocimiento y de denegación de servicio.

- **CPPr** (*Control Plane Protection*): una extensión de CoPP, pero permite la vigilancia de granularidad. Por ejemplo, CPPr puede filtrar y limitar la velocidad de los paquetes que se van al plano de control del router y descartar los paquetes maliciosos y/o erróneos.

- **Control Plane Logging**: permite el registro de los paquetes que CoPP o CPPr permite o deniega. Se proporciona el mecanismo de registro necesario para implementar, supervisar y solucionar problemas de manera eficiente sobre las funciones de CoPP.

El tráfico del plano de gestión se genera por los dispositivos de red a través de procesos y protocolos como telnet, SSH, TFTP y FTP, etc. El plano de gestión es un objetivo muy atractivo para los hackers. Por esta razón, el módulo de gestión se construyó con varias tecnologías diseñadas para mitigar dichos riesgos.

La seguridad del plano de gestión se puede implementar utilizando las siguientes características:

- **Inicio de sesión y política de contraseñas**: restringir el acceso a los dispositivos. Limitar los puertos accesibles y los métodos de de acceso.

- **Notificación legal**: mostrar avisos legales según las leyes locales.

- **Garantizar la confidencialidad de los datos**: proteger los datos confidenciales almacenados localmente que puedan ser vistos o copiados. Utilizar protocolos de gestión con una autenticación fuerte para mitigar los ataques de confidencialidad destinados a exponer las contraseñas y configuraciones del dispositivo.

RBAC (*Role-based access control*): función de control de acceso basado en roles, concede el acceso solo a los usuarios autenticados, grupos y servicios. **RBAC** y **AAA** proporcionan mecanismos para gestionar con eficacia el control de acceso.

- **Autorizar las acciones**: restringir las acciones y opiniones que están permitidas por algún usuario en particular del grupo, o un servicio.

- **Informe de gestión de acceso**: tener registros y las cuentas de todos los accesos (lo que ocurrió y cuándo ocurrió).

El tráfico del plano de datos consiste sobre todo en el tráfico generado por los usuarios y los paquetes que se reenvían a través del router a través del plano de datos. La seguridad del plano de datos se puede implementar con el uso de ACL, mecanismos antispoofing y funciones de seguridad de nivel 2.

Las ACL permiten realizar el filtrado de paquetes para controlar qué paquetes se mueven a través de la red y a dónde se les permite ir, clasificar el tráfico, controlar el ancho de banda, etc.

Las ACL también se pueden utilizar como un mecanismo antispoofing descartando a quien no tiene una dirección de origen válido. Características tales como *Unicast Reverse Path Forwarding* (**uRPF**) se pueden utilizar para complementar la estrategia de antispoofing.

Los switches Cisco Catalyst pueden utilizar las funciones integradas para proteger a nivel de la capa 2. Las siguientes son las herramientas de seguridad de nivel 2 integradas en los switches Cisco Catalyst:

- **Port security**: evita la suplantación de direcciones MAC y los ataques de inundaciones de direcciones MAC.

- **DHCP snooping**: previene los ataques de cliente en el servidor DHCP y en el router.

- **Dynamic ARP Inspection** (**DAI**): añade seguridad a ARP mediante el uso de la tabla DHCP snooping para minimizar el impacto del envenenamiento ARP y los ataques de suplantación.

- **IP Source Guard**: evita la suplantación de direcciones IP mediante el uso de la tabla DHCP snooping.

1.4 FUNDAMENTOS PARA EL EXAMEN

- Analice cuáles son los factores a tener en cuenta en el proceso de asegurar una red.
- Estudie los tres objetivos principales de la seguridad de la red.
- Recuerde cuáles son y cómo funcionan los mecanismos de cifrado y criptografía.
- Tenga en cuenta los posibles significados de la palabra hackers.
- Recuerde cuáles son las organizaciones encargadas de establecer normas para la seguridad en las redes.
- Estudie cada uno de los dominios de la seguridad, especialmente el de políticas de seguridad.
- Estudie y analice el funcionamiento de Cisco SecureX.
- Recuerde cada una de las vulnerabilidades y ataques que puede sufrir una red, y las herramientas y recursos para mitigarlos.
- Estudie en detalle el funcionamiento de Cisco Network Foundation Protection.

Capítulo 2

SEGURIDAD EN LOS ROUTERS

2.1 SEGURIDAD EN EL ROUTER

El router borde es el último router entre la red interna y una red de confianza como Internet. Todo el tráfico a Internet de una organización pasa por este router borde; por lo tanto, generalmente funciona como la primera y última línea de defensa de una red. A través del filtrado inicial y final, el router borde ayuda a asegurar el perímetro de una red protegida. También es responsable de implementar las acciones que están basadas en las políticas de seguridad de la organización. Por estas razones, es importante asegurar los routers de la red.

2.1.1 Modelos de defensa

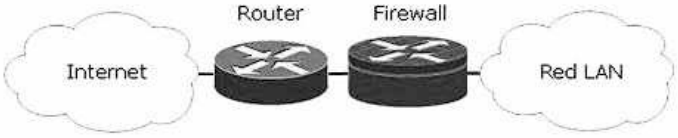
Las implementaciones de seguridad en los routers de la red pueden incluir un solo router protegiendo una red interna o un router como la primera línea de defensa en un enfoque de defensa profunda.

- **Defensa de un solo router**: un solo router conecta la red protegida, o LAN interna a Internet. Todas las políticas de seguridad están configuradas en este dispositivo. Generalmente se utiliza este esquema en implementaciones de sitios pequeños como sucursales y SOHO. En las redes más pequeñas, las funciones de seguridad requeridas pueden ser soportadas por ISR sin comprometer el rendimiento del router.

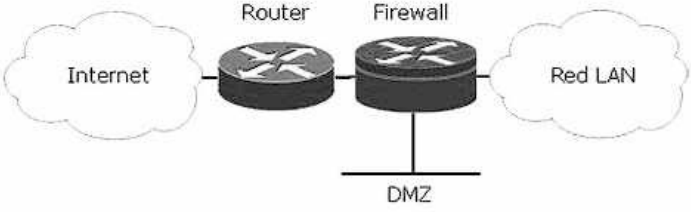
- **Defensa profunda**: es más segura que la de un solo router. En este enfoque, el router borde actúa como la primera línea de defensa y se le conoce como *screening router*. Envía al firewall todas las conexiones dirigidas a la LAN interna. La segunda línea de defensa es el firewall que provee control de acceso adicional ya que monitoriza el estado de las conexiones, actuando como un dispositivo de control. El router borde tiene un conjunto de reglas que especifican qué tráfico permitir y qué tráfico denegar. Por defecto, el firewall deniega la iniciación de conexiones desde las redes externas no confiables para la red interna. Sin embargo, permite a los usuarios internos conectarse a las redes no confiables y permite que las respuestas vuelvan a través del firewall. También puede realizar autenticación de usuario (proxy de autenticación) de manera que los usuarios tengan que estar autenticados para ganar acceso a los recursos de la red.

- **Zona desmilitarizada**: una variante del enfoque de defensa profunda es ofrecer un área intermedia llamada zona desmilitarizada **DMZ** (*demilitarized zone* [DMZ]). La DMZ puede ser utilizada para los servidores que tienen que ser accesibles desde Internet o alguna otra red externa. La DMZ puede ser establecida entre dos routers, con un router interno conectado a la red protegida y un router externo conectado a la red no protegida, o ser simplemente un puerto adicional de un solo router. El firewall, ubicado entre las redes protegida y no protegida, se instala para permitir las conexiones requeridas (por ejemplo, HTTP) de las redes externas no confiables a los servidores públicos en la DMZ. EL firewall sirve como protección primaria para todos los dispositivos en la DMZ. En el enfoque DMZ, el router provee protección filtrando algún tráfico, pero deja la mayoría de la protección a cargo del firewall.

Enfoque de un solo router



Enfoque de defensa profunda



Enfoque DMZ

NOTA:

*El **hardening** del router hace referencia a la robustez en el proceso y los mecanismos para asegurar el router. Por ejemplo, restricciones de puertos y servicios no utilizados, acceso controlado y solo a personal autorizado, etc.*

2.1.2 Complementos de seguridad

El router y los dispositivos físicos que se conectan a él deben estar ubicados en un cuarto bajo llave que sea accesible solo para personal autorizado, libre de interferencia magnética o electrostática, con un sistema contraincendios y controles de temperatura y humedad. Se debe instalar un sistema de alimentación ininterrumpida **UPS** (*Uninterruptible Power Supply*). Esto reduce la posibilidad de un ataques de DoS a causa de pérdida de electricidad en el edificio.

Hay que asegurar las funciones y el rendimiento de los sistemas operativos del router con la máxima cantidad de memoria posible. La disponibilidad de la memoria puede ayudar a proteger la red de ataques de DoS, mientras que soporta el máximo rango de dispositivos de seguridad. Debemos usar la última versión estable del sistema operativo que cumpla los requerimientos de la red. Las funciones de seguridad de un sistema operativo evolucionan con el tiempo, aunque la última versión de un sistema operativo puede no ser la versión más estable

disponible. Mantenga una copia segura de resguardo de la imagen del sistema operativo y el archivo de configuración del router.

Asegúrese de que solo personal autorizado tenga acceso y de que su nivel de acceso sea controlado. Deshabilite puertos e interfaces no utilizadas. Reduzca la cantidad de maneras por las que puede accederse a un dispositivo. Deshabilite servicios innecesarios o habilitados por defecto.

NOTA:

Añadidos que aumentan la seguridad de los dispositivos:

- ✓ *Restringir la accesibilidad de los dispositivos.*
- ✓ *Registrar y justificar todos los accesos.*
- ✓ *Limitar los puertos administrativos.*
- ✓ *Restringir los administradores permitidos.*
- ✓ *Restringir los métodos de acceso permitidos.*
- ✓ *Autenticar los accesos y limitar el número de intentos fallidos.*
- ✓ *Autorizar las acciones.*
- ✓ *Presentar notificaciones legales.*
- ✓ *Asegurar la confidencialidad de los datos.*

2.1.3 Acceso administrativo seguro

Los administradores deben asegurarse de que se usen contraseñas fuertes en toda la red. Los atacantes utilizan varios métodos de descubrimiento de contraseñas administrativas. Pueden intentar adivinar las contraseñas basándose en la información personal del usuario o hacer sniffing de los paquetes TFTP que contienen archivos de configuración en texto plano. Los atacantes también pueden usar herramientas como *L0phtCrack* y *Cain & Abel* para efectuar ataques de fuerza bruta para adivinar las contraseñas.

Para aumentar la seguridad de las contraseñas deben configurarse según lo siguiente:

- Establecer longitudes mínimas de contraseñas.
- Deshabilitar conexiones no utilizadas.
- Cifrar todas las contraseñas en el archivo de configuración.

El uso de una contraseña segura, junto con la asignación de niveles de privilegios son maneras simples de proporcionar control de acceso terminal en una red. Deben establecerse contraseñas diferentes para el modo de acceso EXEC privilegiado y líneas individuales, como las líneas de consola y auxiliar.

2.2 CONFIGURACIÓN DE CONTRASEÑAS

La administración de las contraseñas en una red grande debería mantenerse por medio de un servidor de autenticación central **TACACS+** o **RADIUS** como el Servidor de Control de Acceso Seguro de Cisco (Cisco Secure **ACS**). Todos los routers deben ser configurados con las contraseñas de usuario y de EXEC privilegiado. También se recomienda el uso de una base de datos de nombres de usuario local como copia de resguardo si el acceso a un servidor de autenticación, autorización y registro de auditoría (**AAA**) se encuentra comprometido. El uso de una contraseña y la asignación de niveles de privilegios son maneras simples de proporcionar control de acceso terminal en una red.

A partir de la *release* 12.3(1) del IOS de Cisco, los administradores pueden especificar la longitud de caracteres mínima para todas las contraseñas de routers con un valor de 0 a 16 caracteres usando el siguiente comando de configuración global, **security passwords minlength**. Este comando afecta las contraseñas de usuario, las EXEC privilegiado y las de línea que se creen después de que el comando sea ejecutado. Las contraseñas de router ya existentes no son afectadas.

```
Router(config)#security passwords min-length length
```

Por defecto, la interfaz administrativa permanece activa y autenticada por 10 minutos luego de la última actividad de la sesión. Se recomienda que estos tiempos sean ajustados para limitar a un máximo de dos a tres minutos. Estos relojes pueden ser ajustados usando el comando **exec-timeout** en modo de configuración de línea para cada uno de los tipos de línea utilizado.

```
Router(config-line)# exec-timeout minutes [seconds]
```

También es posible deshabilitar el proceso **exec** para una línea específica, como el puerto auxiliar, usando el comando **no exec** dentro del modo de configuración del línea. Este comando permite solo conexiones salientes en la línea. El comando **no exec** permite deshabilitar el proceso EXEC para conexiones que pueden intentar enviar datos no solicitados al router.

El comando **service password-encryption** es útil principalmente para evitar que individuos no autorizados puedan ver contraseñas en el archivo de configuración ya que por defecto, algunas se muestran en texto plano, sin cifrar. El

algoritmo utilizado por el comando **service password encryption** es simple y fácilmente reversible por alguien que tenga acceso al texto cifrado y una aplicación de cracking de contraseñas. Por esta razón, el comando no deberá ser utilizado con la intención de proteger los archivos de configuración contra ataques serios.

```
Router(config)# service password encryption
```

El comando **enable secret** es mucho más seguro, ya que cifra la contraseña utilizando **MD5** (*Message Digest* 5), un algoritmo mucho más fuerte.

Otra función de seguridad disponible es la autenticación. Hay dos métodos para configurar nombres de usuario de cuentas locales: **username password** y **username secret**.

```
Router(config)# username name password password
Router(config)# username name secret {[0] password | 5 encrypted-
secret}
```

El comando **username secret** es más seguro porque usa el algoritmo **MD5**, (*Message Digest* 5) para crear las claves. MD5 es un algoritmo mucho mejor que el tipo 7 estándar utilizado por el comando **service password-encryption**. La capa agregada de protección que proporciona MD5 es útil en ambientes en los que la contraseña atraviesa la red o es almacenada en un servidor TFTP. Al configurar una combinación de nombre de usuario y contraseña deben seguirse las restricciones de longitud de contraseña. El comando **login local** en la configuración de línea habilita la base de datos local para autenticación.

Por defecto, con excepción de la contraseña **enable secret**, todas las contraseñas de router de Cisco están almacenadas en texto plano dentro de la configuración del router.

Estas contraseñas pueden ser visualizadas con el comando **show running-config**. Los sniffers también pueden ver estas contraseñas si los archivos de configuración de servidor TFTP atraviesan una conexión no asegurada de intranet o Internet. Si un intruso gana acceso al servidor TFTP donde están almacenados los archivos de configuración del router, podrá obtener estas contraseñas.

2.2.1 Contraseña enable secret

El comando de configuración **enable secret** restringe el acceso al modo EXEC privilegiado. Esta contraseña aparece cifrada dentro de la configuración del router usando un algoritmo *Message Digest* 5. Si la contraseña **enable secret** se

pierde o se olvida, debe ser reemplazada utilizando el procedimiento de recuperación de contraseñas de los routers Cisco.

```
Router(config)# enable secret password
```

2.2.2 Contraseña de consola

Por defecto, el puerto de línea de consola no requiere una contraseña para el acceso administrativo de la consola; sin embargo, siempre debe ser configurado con una contraseña. Se utiliza el comando **line console 0** seguido de los subcomandos **login** y **password** para solicitar el ingreso y establecer una contraseña de ingreso en la línea de consola.

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password password
```

2.2.3 Contraseña de telnet

Por defecto, los routers de Cisco soportan hasta cinco sesiones simultáneas de terminal virtual vty (telnet o SSH). En el router, los puertos vty se numeran del 0 al 4. Se utiliza el comando **line vty 0 4** seguido por los subcomandos **login** y **password** para solicitar ingreso y establecer una contraseña de ingreso a las sesiones telnet entrantes.

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
```

2.2.4 Contraseña de auxiliar

Por defecto, los puertos auxiliares del router no requieren una contraseña para acceso administrativo remoto. Los administradores algunas veces usan este puerto para configurar y monitorizar remotamente el router usando una conexión de módem *dialup*. Para acceder a la línea auxiliar, se utiliza el comando **line aux 0** y los subcomandos **login** y **password** para solicitar ingreso y establecer una contraseña de ingreso a las conexiones entrantes.

```
Router(config)# line aux 0
Router(config-line)# password password
Router(config-line)# login
```

2.2.5 Seguridad mejorada para conexiones virtuales

La función de identificación mejorada del IOS Cisco proporciona mayor seguridad para los dispositivos al crear una conexión virtual como telnet, SSH o HTTP, debido a que hace más lentos los ataques de diccionario y detiene los ataques de DoS. Para configurar mejor la seguridad de las conexiones de ingreso virtuales, el proceso de autenticación deberá ser configurado con parámetros específicos:

- Retardos entre intentos de ingreso sucesivos.
- Cierre de sesión si se sospechan ataques de DoS.
- Generación de mensajes de registro del sistema para detección de sesiones.

Habilitando un perfil de detección, el dispositivo de red puede ser configurado para reaccionar a repetidos intentos de ingreso fallidos con un rechazo a las solicitudes de conexión subsiguientes (**login blocking**). Este bloqueo puede ser configurado para un período de tiempo que se denomina "período silencioso" (**quiet period**). Durante un período silencioso se permiten los intentos de conexión legítimos por medio de la configuración de una lista de control de acceso con las direcciones asociadas con los administradores de sistemas.

```
Router# configure terminal
Router(config)# login block-for seconds attempts tries within
seconds
Router(config)# login quiet-mode access-class {acl-name | acl-
number}
Router(config)# login delay seconds
Router(config)# login on-failure log [every login]
Router(config)# login on-success log [every login]
```

El comando **login block-for** habilita las funciones de ingreso mejoradas. La actividad de inicio de sesión en el dispositivo se monitoriza y opera en dos modos:

- **Modo de vigilancia**: es el modo normal, el router cuenta la cantidad de intentos de ingreso fallidos dentro de una cantidad de tiempo determinada.

- **Modo silencioso**: cuando el número de ingresos fallidos sobrepasa el umbral configurado, todos los intentos de ingreso de telnet, SSH y HTTP serán denegados.

Para proporcionar acceso a los hosts críticos en todo momento debe ser creada una ACL e identificada usando el comando **login quiet-mode access-class**.

El comando **login block-for** genera un retraso de un segundo entre intentos de ingreso, tanto fallidos como exitosos. El atacante tendrá que esperar un segundo antes de probar con otra contraseña. Este tiempo de retraso puede modificarse mediante el comando **login delay**, que introducirá un retraso uniforme entre intentos sucesivos de ingreso.

El comando **auto secure** habilita el registro de mensajes para intentos fallidos de ingreso. El registro de intentos de ingreso exitosos no está habilitado por defecto. Estos comandos pueden ser utilizados para mantener un registro del número de intentos de ingreso exitosos y fallidos.

Para generar registros para las solicitudes de ingreso fallidas:

```
login on-failure log [every login]
```

Para generar mensajes en el registro para las solicitudes de ingreso exitosas:

```
login on-success log [every login]
```

El número de intentos de ingreso antes de que se genere un mensaje puede especificarse mediante el parámetro **every login**. El valor por defecto es 1. El rángo válido va de 1 a 65.535.

El siguiente comando genera un mensaje en el registro cuando se excede la tasa de fallos de inicio de sesión.

```
security authentication failure rate threshold-rate log
```

Para verificar que el comando **login block-for** esté configurado y el modo en el que está el router, use el comando **show login**. El router puede estar en modo normal o silencioso, dependiendo de si se ha excedido el umbral de intentos de ingreso.

El comando **show login failures** muestra más información en relación a los intentos fallidos, como la dirección IP de la que se originó el intento de ingreso fallido.

EJEMPLO:

```
Router# configure terminal
Router(config)#username CCNA secret Security
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#exit
Router(config)# login block-for 20 attempts 5 within 60
Router(config)#ip access-list standard INGRESOS
Router(config-std-nacl)#remark Permitir solo al administrador
Router(config-std-nacl)#permit 172.16.0.55
Router(config)# login quiet-mode access-class INGRESOS
Router(config)# login delay 10
Router(config)# login on-failure log
Router(config)# login on-success log
Router(config)#exit

Router# show login

A login delay of 3 seconds is applied.
Quiet-Mode access list INGRESOS is applied.
All successful login is logged.
All failed login is logged.

Router enabled to watch for login Attacks.
If more than 5 login failures occur in 10 seconds or less,
logins will be disabled for 30 seconds.
Router presently in Normal-Mode.

Current Watch Window
Time remaining: 9 seconds.
Login failures for current window: 0.
Total login failures: 0.

Router# show login failures

Total failed logins:30
Detailed information about last 50 failures

Username      SourceIPAddr 1Port  Count  TimeStammp
Admin         10.0.0.28    23     12     10:45:22 UTC Wed Jan 15 2012
Hack          10.1.1.15    23     15     10:47:15 UTC Wed Jan 15 2012
.....................................................................
```

2.2.6 Banners

Los banners son muy importantes para la red desde una perspectiva legal. Además de advertir a intrusos potenciales, los banners también pueden ser utilizados para informar a administradores remotos de las restricciones de uso.

La elección del contenido de los mensajes banner es importante y debe ser revisada por un asesor legal antes de colocarse en routers de red. Nunca use la palabra "bienvenido" o algún otro saludo familiar que pueda ser sacado de contexto o entendido como una invitación para usar la red.

Los banners están deshabilitados por defecto y deben ser habilitados explícitamente. Use el comando **banner** desde el modo de configuración global para especificar mensajes apropiados.

```
banner {exec | incoming | login | motd | slip-ppp} # message #
```

El **banner motd** de es de poco uso en entornos de producción y se utiliza raramente. El **banner exec**, por el contrario, es útil para mostrar mensajes de administrador, ya que se presenta solo para los usuarios autenticados.

Existen parámetros opcionales y pueden ser utilizados en la sección del mensaje del comando **banner**:

$(hostname) muestra el nombre de host del router.

$(domain) muestra el nombre de dominio del router.

$(line) muestra los números de línea vty o tty.

$(line-desc) muestra la descripción de la línea.

EJEMPLO:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# bannerlogin #
Enter TEXT message. End with the character '#'.
+------------------------------------------------------------------+
| WARNING                                                          |
| -------                                                          |
| This system is solely for the use of authorized users for        |
| official purposes. You have no expectation of privacy in         |
| its use and to ensure that the system is functioning             |
| properly, individuals using this computer system are subject     |
```

```
| to having all of their activities monitored and recorded by |
| system personnel. Use of this system evidences an express   |
| consent to such monitoring and agreement that if such       |
| monitoring reveals evidence of possible abuse or criminal   |
| activity, system personnel may provide the results of such  |
| monitoring to appropriate officials.                        |
+-------------------------------------------------------------+
#
```

2.2.7 Configuración de SSH

SSH (*Secure Shell*) ha reemplazado a telnet como práctica recomendada para proveer administración de router remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.

Los siguientes pasos configuran SSH usando la **CLI** (línea de comandos) para configurar un router Cisco:

1. Si el router tiene un nombre de host único, configure el nombre de dominio IP de la red usando el comando **ip domain-name** *domain-name* en el modo de configuración global. Hay que asegurarse de que cada router destino esté usando el nombre de dominio correcto para la red.

2. Deben generarse las claves secretas de una sola vía para que un router cifre el tráfico SSH. Estas claves se denominan claves asimétricas. Para crear la clave **RSA** (*Rivest, Shamir and Adleman*), use el comando **crypto key generate rsa general-keys modulus** *modulus-size* en el modo de configuración global. La longitud mínima de clave módulo recomendada es de 1.024 bits (desde 360 bits a 2.048 bits).

3. Asegúrese de que haya una entrada de nombre de usuario válida en la base de datos local. Si no la hay, cree una usando el comando **username** *name* **secret** *password.*

4. El intervalo de tiempo que el router espera para que responda el cliente SSH durante la fase de negociación SSH puede ser configurado usando el comando **ip ssh timeout** *seconds* en el modo de configuración global. El intervalo por defecto es de 120 segundos.

5. Por defecto, el usuario tiene tres intentos para ingresar antes de ser desconectado. Para configurar un número diferente de intentos consecutivos SSH, use el comando **ip ssh authentication-retries** *number* en el modo de configuración global.

6. Habilite sesiones SSH vty de entrada usando los comandos de línea vty **login local** y **transport input ssh**. Para prevenir sesiones de telnet configure el comando **no transport input telnet** para todas las líneas vty.

Para verificar el SSH y mostrar las claves generadas, use el comando **show crypto key mypubkey rsa** en modo EXEC privilegiado. Si hay pares de claves existentes, se recomienda que sean sobreescritos usando el **comando crypto key zeroize rsa**.

SSH se habilita automáticamente luego de que se generan las claves RSA. Puede accederse al servicio SSH del router usando software de cliente SSH. Hay dos maneras de conectarse a un router con SSH habilitado:

- Conectarse mediante un router Cisco con SSH habilitado usando el comando de modo privilegiado **EXEC ssh**.

- Conectarse usando un cliente SSH público y disponible comercialmente ejecutándose en un host. Algunos ejemplos de estos clientes son PuTTY, OpenSSH, y TeraTerm.

EJEMPLO:

```
Router# conf term

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# username ernesto secret CCNAsecurity
Router(config)# ip domain-name Aprenderedes.com
Router(config)# crypto key zeroize rsa

% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes

Router(config)#
```

```
*Mar 1 01:33:35.455: %SSH-5-DISABLED: SSH 1.99 has been disabled
Router(config)# crypto key generate rsa modulus 1024

The name for the keys will be: R1. Aprenderedes.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router(config)#

*Mar 1 01:34:20.235: %SSH-5-ENABLED: SSH 1.99 has been enabled

Router(config)# ip ssh time-out 120
Router(config)# ip ssh authentication-retries 4
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# transport input ssh
Router(config-line)# end

Router# show crypto key mypubkey rsa
% Key pair was generated at: 01:34:20 UTC Mar 1 2012
Key name: R1.Aprenderedes.com
Usage: General Purpose Key
Key is not exportable.

Key Data:
      30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181
      009C3542 26FDD40C C0CEA5DE 8D4AEC7E 2AB70ECB 1F5EAC60 1459AA16
      0EE4059B FD95C548 29126EC0 522501E3 6AEF0581 BDFF46FC 1C145B94
      6590C7BB 931C1734 0BC90ACE 57A726ED 5E233A92 02F2B5A6 DE10BA2A
      99D7EC00 2646FC20 39BB4298 55B4DED1 ED6F7D3F 289FFB3F 8F1F014B
      2252BC49 45D27160 0C50AC02 E51B1C1A 9F020301 0001

% Key pair was generated at: 01:34:21 UTC Mar 1 2012
Key name: R1.Aprenderedes.com.server
Usage: Encryption Key
Key is not exportable.

Key Data:
      307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D811FD
      3CF9D04F 33A7D951 93ED5C01 90E3515B B9C23EF6 268E638F 868D2AD2
      3A7722BC 52DF0CAF DC33C7F8 54208F5B 147CAB1E 9B634B69 4D44F556
      43482BB5 7B3A447B 397F6E7E 5C423F7C 903A391A B8970A32 51F7D9EB
      91FBE954 D7AEC02D 31020301 0001
```

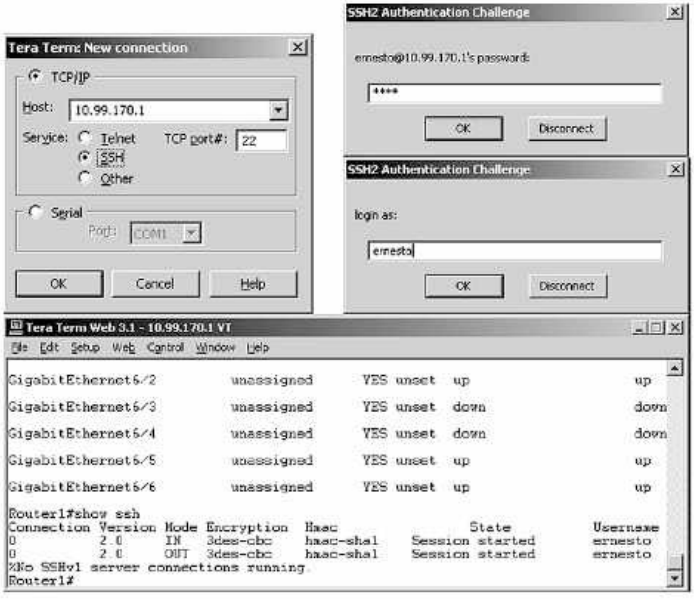
NOTA:

Asegúrese de que los routers destino estén ejecutando una imagen IOS de Cisco versión 12.1(1)T o posterior, para que soporten SSH. Solo las imágenes criptográficas IOS que contienen el grupo de funciones IPsec soportan SSH. Específicamente, las imágenes criptográficas de IOS 12.1 o la posterior IPsec DES o el Triple Data Encryption Standard (3DES) soportan SSH. Estas imágenes generalmente tienen el identificador k8 o k9 en su nombre de imagen. Por ejemplo, ***c1841-advipservicesk9-mz.124-10b.bin*** *es una imagen que soporta SSH.*

EJEMPLO:

En el siguiente caso se muestra como un cliente Windows se conecta al Router1 utilizando el programa **Tera Term**, el comando **show ssh** no muestra conexiones activas hasta que el cliente se conecta:

Desde el cliente Windows:



```
Router1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.

Router1#show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN 3des-cbc hmac-sha1 Session started ernesto
0 2.0 OUT 3des-cbc hmac-sha1 Session started ernesto
%No SSHv1 server connections running.
```

Desde un router como cliente el comando para establecer una conexión a Router1:

```
Router2#ssh ?
 -c Select encryption algorithm
 -l Log in using this user name
 -o Specify options
 -p Connect to this port
 WORD IP address or hostname of a remote system

Router2#ssh -l ernesto 10.99.170.1
```

NOTA:

CCP *(Cisco Configuration Professional) se utilizará como ejemplo a lo largo de todo este libro. Está disponible en el CD-ROM incluido en los nuevos routers o puede descargarse desde cisco.com. Por defecto viene configurado en algunos modelos de routers, sin embargo, si el router es antiguo y no está configurado con la configuración por defecto de CCP, configure los siguientes servicios para acceder al mismo correctamente:*

Usuario y contraseña con un nivel de privilegio 15:

```
username name privilege 15 secret password
```

Habilitar el HTTP Server:

```
ip http server
ip http authentication local
ip http secure-server
```

Definir el protocolo a utilizar para conectarse:

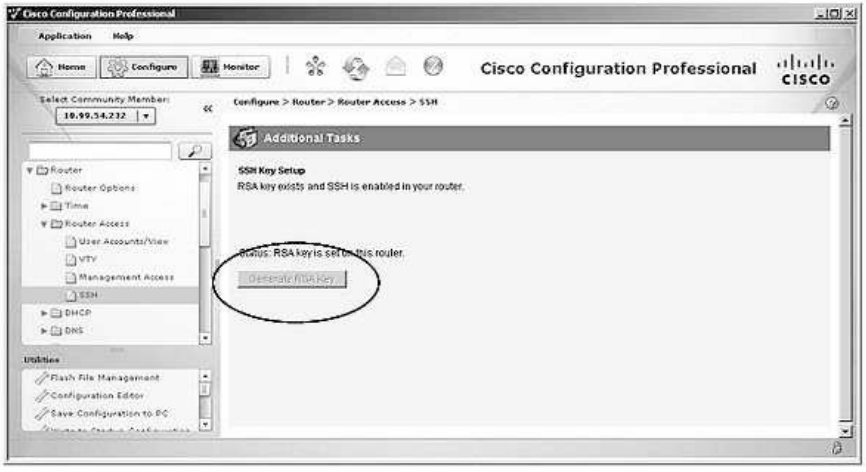
```
line vty 0 4
privilege level 15
login local
transport input telnet ssh
```

2.2.8 Configuración de SSH con CCP

CCP (*Cisco Configuration Professional*) se puede utilizar para configurar SSH en un router. Para ver la configuración actual de claves SSH, seleccione **Configure** / **Router** / **Router Access** / **SSH**. La configuración de clave SSH tiene dos opciones de estatus.

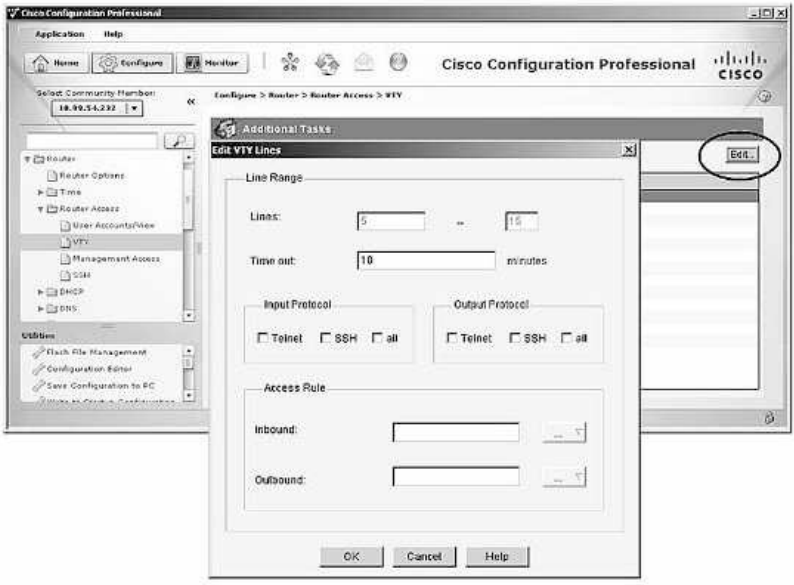
- **RSA key is not set on this router**: este aviso aparece si no hay clave de cifrado configurada para el dispositivo.

- **RSA key is set on this router**: este aviso aparece si se ha generado una clave criptográfica, en cuyo caso SSH está activado en el router.



El botón **Generate RSA Key** configurará una clave criptográfica, el tamaño del módulo aparecerá en el cuadro de diálogo. El valor del recomendado del módulo debe estar entre 512 y 1.024 (valor entero múltiplo de 64), desde 360 bits a 2.048 bits.

Después de que SSH esté activado en el router, será necesario configurar las líneas vty de apoyo a SSH. Seleccione **Configure** / **Router** / **Router Access** / **VTY**. La ventana de líneas vty muestra la configuración vty del router. Haga clic en el botón **Edit** para configurar los parámetros correspondientes.



2.3 ASIGNACIÓN DE ROLES

No todos los administradores requieren los mismos roles y privilegios de acceso a los dispositivos de la infraestructura de red. Aunque es importante que el administrador principal pueda conectarse a un dispositivo y administrarlo con seguridad, deben agregarse más configuraciones para permitir el acceso a otros administradores con distintos niveles y mantener segura la red.

2.3.1 Configuración de niveles de privilegios

El siguiente paso para el administrador que quiere asegurar la red es configurar niveles de privilegio. Los niveles de privilegio determinan a quién le será permitido conectarse al dispositivo y qué podrá hacer una vez que se conecte. La CLI del software IOS de Cisco tiene dos niveles de acceso a los comandos.

El modo de EXEC usuario (nivel 1 de privilegios) proporciona los privilegios más básicos al usuario del modo EXEC y le permite solo comandos de nivel de usuario con el *prompt* **router>**.

El modo EXEC privilegiado (nivel 15 de privilegios) incluye todos los comandos de nivel enable con el *prompt* **router#**.

Aunque estos dos niveles proporcionan control, algunas veces se necesita un nivel de control más preciso. Hay 16 niveles de privilegios en total. Los niveles 0, 1 y 15 tienen configuración predeterminada y cada nivel de privilegios incluye los privilegios de todos los otros niveles inferiores.

Para asignar comandos a un nivel de privilegios personalizado, utilice el comando **privilege** del modo de configuración global.

```
Router(config)# privilege mode {level level command | reset} command
```

Deben configurarse niveles de privilegios para autenticación. Hay dos métodos para asignar contraseñas a los diferentes niveles:

Para el nivel privilegiado, usando el comando de configuración global:

```
enable secret level level password
```

Para un usuario que tiene acceso a un nivel de privilegios específico, usando el comando de configuración global:

```
username name privilege level secret password
```

EJEMPLO:

Las siguientes sintaxis muestran un ejemplo de configuración de diferentes niveles de privilegios y la manera de acceder y moverse entre cada uno de ellos.

```
Router# config term
Router(config)# username ADM privilege 1 secret CCNA
Router(config)# privilege exec level 5 debug
Router(config)# enable secret level 5 secret Uy56s
Router(config)# username Soporte privilege 1 secret SecuR
Router(config)# privilege exec level 10 ping
Router(config)# enable secret level 10 secret GtY67
Router(config)# username Jefatura privilege 10 secret CisCo
Router(config)# end

User Access Verification
Username: ADM
Password: ***** (CCNA)

Router> show privilege
Current privilege level is 1

Router# enable 10
Password: ***** (GtY67)
Router# show privilege
```

```
Current privilege level is 10

Router# ping 192.168.0.95
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.95, timeout is 2
seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
```

Cuando un comando no está disponible en un determinado nivel aparecerá un mensaje del tipo:

```
% Invalid input detected at `^` marker.
```

El comando "?" muestra los comandos disponibles en cada nivel de privilegio:

```
Router(config)# ?
Configure commands:

default Set a command to its defaults
end Exit from configure mode
exit Exit from configure mode
help Description of the interactive help system
no Negate a command or set its defaults
rtr RTR base configuration
```

2.3.2 Configuración de acceso a la CLI basado en roles

Esta función provee acceso más granular, ya que controla específicamente qué comandos están disponibles para roles específicos. El acceso a la CLI basado en roles permite al administrador de la red crear diferentes vistas de las configuraciones del router para diferentes usuarios. Cada vista define los comandos CLI a los que cada usuario tiene acceso.

La CLI basada en roles proporciona tres tipos de vistas, cada una dictamina qué comandos están disponibles:

- **Vista de root**: tiene los mismos privilegios de acceso que un usuario con nivel 15 de privilegios. Sin embargo, una vista de root no es lo mismo que un usuario de nivel 15. Solo un usuario de vista de root puede configurar una nueva vista y agregar o remover comandos de las vistas existentes.

- **Vista CLI**: no tiene jerarquías de comandos y, por lo tanto, no hay vistas superiores o inferiores. Deben asignarse todos los comandos asociados con cada vista, y las vistas no heredan comandos de otras vistas.

- **Supervista**: permite al administrador de redes asignar a los usuarios y grupos de usuarios múltiples vistas CLI de una sola vez, en lugar de tener que asignar una por usuario con todos los comandos asociados a esa única vista CLI.

Las supervistas tienen las siguientes características:

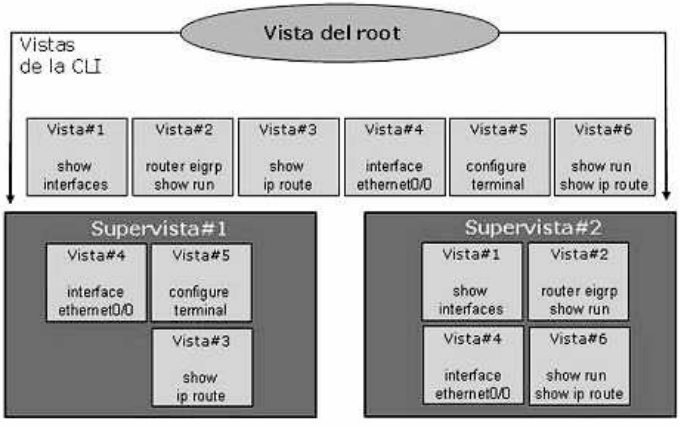
- Una sola vista CLI puede ser compartida entre varias supervistas.

- No pueden configurarse comandos para una supervista. El administrador debe agregar comandos a la vista CLI y luego agregar esa vista CLI a la supervista.

- Los usuarios que están autenticados en una supervista pueden acceder a todos los comandos que están configurados para cualquiera de las vistas CLI que son parte de la supervista.

- Cada supervista tiene una contraseña que se usa para moverse entre ellas o de una vista CLI a una supervista.

- Eliminar una supervista no elimina las vistas CLI asociadas. Las vistas CLI permanecen disponibles para ser asignadas a otra supervista.



Para configurar y editar las vistas, el administrador debe ingresar a la vista de root usando el comando de EXEC privilegiado **enable view**. También puede usarse el comando **enable view root**. Ingrese la contraseña **enable secret** cuando se la pida.

1. Habilite AAA con el comando de configuración global **aaa new-model**. Salga e ingrese a la vista de root con el comando **enable view**.

2. Cree una vista usando el comando **parser view** *view-name*. Esto habilita el modo de configuración de la vista. Excluyendo la vista de root, hay un límite máximo de 15 vistas en total.

3. Asigne una contraseña **secret** a la vista usando el comando **secret** *encrypted-password.*

4. Asigne comandos a la vista seleccionada usando el comando **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] en el modo de configuración de vista. Finalmente salga del modo de configuración de la vista con el comando **exit**.

Para configurar una supervista el administrador debe estar en la vista de root y debe usarse el comando **view** *view-name* para asignar vistas. Para confirmar que se está usando la vista de root, se utiliza el comando **enable view** o el comando **enable view root**. Ingrese la contraseña **enable secret** cuando se la solicite.

1. Ingrese al modo de configuración de supervista usando el comando **parser view** *view-name* **superview**.

2. Asigne una contraseña **secret** a la vista usando el comando **secret** *encrypted-password.*

3. Asigne una vista existente usando el comando **view** *view-name* en el modo de configuración de vista. Salga del modo de configuración de supervista con el comando **exit**.

Puede asignarse más de una vista a una supervista, y las vistas pueden ser compartidas por más de una supervista.

El comando **enable view** *view-name* en el modo de usuario permite acceder a las vistas existentes. Ingrese la contraseña que se asignó a la vista personalizada. Use el mismo comando para moverse de una vista a la otra.

Para verificar una vista, use el comando **enable view**. Desde la vista de root, use el comando **show parser view all** para ver un resumen de todas las vistas.

EJEMPLO:

El siguiente caso muestra la configuración de dos vistas CLI (**first** y **second**) y los comandos para su verificación:

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip
interface
Router(config-view)# command exec include logout
Router(config-view)# exit
!
!
Router(config-view)# do show run | beg view
parser view first
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout

Router# enable view first
Password:*****
00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
 configure Enter configuration mode
 enable Turn on privileged commands
 exit Exit from the EXEC
 show Show running system information
```

```
Router# show ?

 ip IP information
 parser Display parser information
 version System hardware and software status
```

2.4 PROTECCIÓN DE ARCHIVOS Y CONTRASEÑAS

Cuando se asegura una imagen IOS, la función de configuración resistente deniega todas las solicitudes para copiarla, modificarla o eliminarla. De la misma forma, si alguien ganara acceso físico al router, podría tomar control del dispositivo a través del procedimiento de recuperación de contraseña.

2.4.1 Resguardo de la configuración e imagen IOS

Si la configuración o la imagen del IOS se borran, el operador quizás nunca recupere una copia archivada para restaurar el router. El proceso de recuperación debe, entonces, tomar lugar en cada router afectado, agregándose al período de inactividad total de la red.

La función de configuración **Resilient Configuration** del IOS de Cisco permite una recuperación más rápida si alguien reformatea la memoria flash o borra el archivo de configuración de inicio en la NVRAM. La copia segura de la configuración de inicio se almacena en la flash junto con la imagen segura del IOS. Este conjunto de los archivos de configuración actual y la imagen del IOS de Cisco se conoce como el conjunto de arranque (*bootset*). Algunas características de la configuración resistente son:

- El archivo de configuración en el grupo de arranque primario es una copia de la configuración actual que estaba en el router cuando se habilitó la función.
- Asegura el grupo de archivos más pequeño posible para preservar el espacio de almacenamiento. No se requiere espacio extra para asegurar el archivo primario de la imagen IOS.
- Detecta automáticamente diferencias de versiones de imagen o de configuración.
- Utiliza almacenamiento local para asegurar los archivos.
- La función solo puede deshabilitarse desde una sesión de consola.

Hay dos comandos de configuración global disponibles para configurar las funciones de configuración resistente del IOS de Cisco: **secure boot-image** y **secure boot-config**.

El comando **secure boot-image** habilita la resistencia de la imagen del IOS. Cuando se habilita por primera vez, se asegura la imagen actual, al mismo tiempo que se crea una entrada en el registro. Esta función puede ser deshabilitada solo por medio de una sesión de consola anteponiendo un **no** antes del comando.

```
Router(config)# secure boot-image
```

Si se detecta una versión diferente del software IOS de Cisco, se muestra un mensaje como el siguiente:

```
ios resilience: Archived image and configuration version 12.2
differs from running version 12.3
```

Para registrar la configuración actual del router y archivarla de manera segura en el dispositivo de almacenamiento permanente se utiliza el comando **secure bootconfig** en el modo de configuración global. Se mostrará un mensaje del registro en la consola notificando al usuario que la función de adaptabilidad de la configuración ha sido activada. El archivo de configuración está oculto y no puede ser visto o eliminado directamente desde el *prompt* de la CLI.

```
Router(config)# secure boot-config
```

Los archivos de configuración actuales no son visibles a través del comando **dir**, para verificar la existencia del archivo se utiliza el comando **show secure bootset**.

NOTA:

La función de configuración resistente de IOS solo está disponible para sistemas que soporten una interfaz flash Advanced Technology Attachment (ATA) PCMCIA.

El modo **ROMmon** no tiene tales restricciones y puede listar los archivos asegurados y arrancar desde ellos. Hay cinco pasos para restaurar un conjunto de arranque primario de un archivo seguro luego de que el router ha sido manipulado:

1. Reiniciar el router usando el comando **reload**.

2. Desde el modo **ROMmon**, ingrese el comando **dir** para listar los contenidos del dispositivo que contiene el archivo asegurado de conjunto de arranque. Desde la CLI, el nombre del dispositivo puede hallarse en la salida del comando **show secure bootset**.

3. Arranque el router con la imagen del conjunto de arranque asegurada usando el comando **boot** con el nombre de archivo encontrado en el paso 2. Cuando el router comprometido arranque, cambie al modo EXEC privilegiado y restaure la configuración.

4. Ingrese al modo de configuración global usando el comando **conf t**. Restaure la configuración segura al nombre de archivo proporcionado usando el comando **secure boot-config restore** con el nombre de archivo correspondiente.

EJEMPLO:

```
Router# reload
rommon 1 > dir slot0:
rommon 2 > boot slot0:c3745-js2-mz

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
no

Router> enable
Router# configure terminal
Router(config)# secure boot-config restore slot0:rescue-cfg
Router(config)# end
Router# copy slot0:rescue-cfg running-config

Router# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun
16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
 file size is 25469248 bytes, run size is 25634900 bytes
 Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC
Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

2.4.2 Recuperación de contraseñas

Por razones de seguridad, la recuperación de contraseñas requiere que administrador tenga acceso físico al router a través de un cable de consola. Siga los siguientes pasos:

1. Conecte un terminal o PC con software de emulación de terminal al puerto de consola del router. Acceda físicamente al router, apague y encienda el router.

2. Pulse la tecla de interrupción del terminal durante los primeros sesenta segundos del encendido del router. En el caso de Hyperterminal la combinación del **control+pausa** dará la señal de interrupción en el router. Aparecerá el símbolo **rommon>**. Si no aparece, el terminal no está enviando la señal de interrupción correcta. En este caso, compruebe la configuración del terminal o del emulador de terminal.

3. Introduzca el comando **confreg 0x2142** en el símbolo **rommon>** para arrancar desde la memoria flash e ignorar la NVRAM.

4. En el símbolo **rommon>** introduzca el comando **reset** para reiniciar el router. Esto hace que el router se reinicie pero ignore la configuración grabada en la NVRAM.

5. Siga los pasos de arranque normales. Aparecerá el símbolo **router>**.

6. La memoria RAM estará vacía, copie el contenido de la NVRAN a la RAM. De esta manera recuperará la configuración y también la contraseña no deseada. El nombre de router volverá a ser el original.

```
Router# copy startup-config running-config

MADRID#
```

7. Cambie la contraseña no deseada por la conocida:

```
MADRID# configure terminal

MADRID(config)# enable secret password
```

8. Guarde su nueva contraseña en la NVRAM, y si fuera necesario levante administrativamente las interfaces con el comando **no shutdown**:

```
MADRID# copy running-config startup-config
```

9. Introduzca desde el modo global el comando **config-register 0x2102**.

10. Introduzca el comando **reload** en el símbolo del nivel EXEC privilegiado. Responda **yes** a la pregunta para guardar el registro de configuración y confirme el reinicio:

```
MADRID# reload
System configuration has been modified. Save? [yes/no]:
yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

El comando **no service password-recovery** es un comando oculto de IOS y no tiene argumentos o palabras clave. Si se configura un router con este comando, se deshabilita el acceso al modo **ROMmon**. El comando **show running configuration** muestra una sentencia **no service password-recovery**.

```
router1#show running-config
Building configuration...
.....
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-recovery
! Enable Secure ROMMON
! Hidden command
hostname router1
!
```

Cuando se ingresa el comando **no service password-recovery**, se muestra un mensaje de advertencia que debe ser aceptado para que la función se habilite.

```
router1(config)#no service password-recovery

 WARNING:
 Executing this command will disable password recovery mechanism.
 Do not execute this command without another plan for
 password recovery.

Are you sure you want to continue? [yes/no]: yes
```

Cuando el router arranca, la secuencia de arranque inicial muestra el siguiente mensaje:

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
```

```
Copyright (c) 1998 by cisco Systems, Inc.
C3600 processor with 65536 Kbytes of main memory
Main memory is configured to 64 bit mode with parity enabled
```

Para recuperar un dispositivo luego de que se ingresa el comando **no service password-recovery**, se debe emitir la secuencia **break** dentro de los cinco segundos luego de que la imagen se descomprima durante el arranque.

2.5 FUNDAMENTOS PARA EL EXAMEN

- Recuerde cuáles son los modelos de defensa y cómo funcionan.
- Analice de qué manera se puede incrementar la seguridad de las contraseñas.
- Recuerde los comandos de configuración de las contraseñas y cómo funciona la seguridad mejorada, realice prácticas.
- Sepa para qué sirve la función *resilience* y cómo se configura.
- Recuerde la forma de configuración de SSH tanto por CLI como por CCP.
- Estudie qué son y cómo funcionan los roles y privilegios.
- Analice paso a paso la forma de recuperación de archivos de configuración, IOS y de las contraseñas. Realice prácticas.

Capítulo 3

MONITORIZACIÓN Y ADMINISTRACIÓN DE LA RED

3.1 ADMINISTRACIÓN Y REPORTES

Deben considerarse muchos factores al implementar una administración segura. Esto incluye, por ejemplo, administración de cambios en la configuración. Cuando una red está bajo ataque es importante conocer el estado de dispositivos críticos de la red y cuándo ocurrieron las últimas modificaciones conocidas.

Muchas aplicaciones y protocolos, como **SNMP** (*Simple Network Management Protocol*), están disponibles para su uso en sistemas de administración de redes, con el propósito de monitorizar y efectuar cambios en la configuración de los dispositivos de manera remota.

Cuando se registra y se administra información, el flujo de información entre los hosts de administración y los dispositivos administrados puede tomar uno de dos caminos:

- **Out-of-band, OOB** (fuera de banda): flujos de información en una red de administración dedicada en los cuales no reside tráfico de producción. Es recomendable evitar utilizar protocolos de administración por la red de producción.

- **In-band** (en banda): flujos de información que atraviesan la red de producción de la empresa, Internet o ambos a través de canales de datos comunes. Es recomendable, cuando sea posible, el uso de IPsec, SSH o SSL.

3.1.1 Syslog como herramienta de registro

Los routers Cisco pueden registrar información en relación a los cambios de configuración, violaciones de las ACL, el estado de las interfaces y muchos otros tipos de eventos. Además, pueden enviar mensajes de registro a numerosos destinos diferentes. El router debería estar configurado para enviar mensajes de registro a uno o más de los siguientes destinos:

- **Consola**: los mensajes se registran en la consola y pueden ser visualizados cuando se modifica o se prueba el router usando software de emulación de terminal. El registro de consola está habilitado por defecto. Este tipo de registro no se almacena en el router.

- **Líneas de terminal**: las sesiones pueden ser configuradas para recibir mensajes de registro en cualquiera de las líneas de terminal. Este tipo de registro no se almacena en el router.

- **Registro de buffer**: el registro de buffer es un poco más útil como herramienta de seguridad porque los mensajes quedan almacenados en la memoria del router por un cierto tiempo.

- **SNMP traps**: los eventos de los routers, como la superación de un umbral, pueden ser procesados por el router y reenviados como traps SNMP a un servidor SNMP externo. Las traps SNMP son una herramienta de registro de seguridad viable, pero requieren la configuración y mantenimiento de un sistema SNMP.

- **Syslog**: los routers Cisco pueden ser configurados para reenviar mensajes de registro a un servicio syslog externo. Este servicio puede residir en uno o muchos servidores o estaciones de trabajo.

Syslog es el estándar para registrar eventos del sistema. Syslog es la herramienta de registro de mensajes más popular, ya que proporciona capacidades de almacenamiento de registro de largo plazo y una ubicación central para todos los mensajes del router.

Las implementaciones syslog contienen dos tipos de sistemas:

- **Servidores syslog**: también conocidos como hosts de registro, estos sistemas aceptan y procesan mensajes de registro de clientes syslog.
- **Clientes syslog**: routers u otros tipos de dispositivos que generan y reenvían mensajes de registro a servidores syslog.

Nivel	Aviso	Descripción	Definición
0	emergencies	El sistema es inoperable.	LOG_EMERG
1	alerts	Se requiere una acción inmediata.	LOG_ALERT
2	critical	Existen condiciones críticas.	LOG_CRIT
3	errors	Existen condiciones de error.	LOG_ERR
4	warnings	Existen condicciones de advertencia.	LOG_WARNING
5	notification	Notificaciones significativas.	LOG_NOTICE
6	informational	Mensajes informativos.	LOG_INFO
7	debugging	Mensajes de debugg.	LOG_DEBUG

3.1.2 Configuración de Syslog

Los siguientes pasos configuran el registro del sistema:

1. Configuración del host de registro de destino utilizando el comando **logging host**.
2. Establecer el nivel de severidad del *trap* con el comando **logging trap** *level* (este paso es opcional).

3. Configurar la interfaz de origen con el comando **logging source-interface**. Esto especifica que los paquetes syslog contengan la dirección IPv4 o IPv6 de una interfaz particular, sin importar qué interfaz usa el paquete para salir del router.

4. Habilitar el registro utilizando el comando **logging on**. Puede habilitar o deshabilitar el registro para estos destinos individualmente usando los comandos **logging buffered**, **logging monitor** y **logging** de configuración global. Sin embargo, si el comando **logging on** está deshabilitado, no se envían mensajes a estos destinos. Solo la consola recibe mensajes.

```
Router(config)# logging host 192.168.1.23
Router(config)# logging trap critical
Router(config)# logging source-interface fastethernet0/2
Router(config)# logging on
```

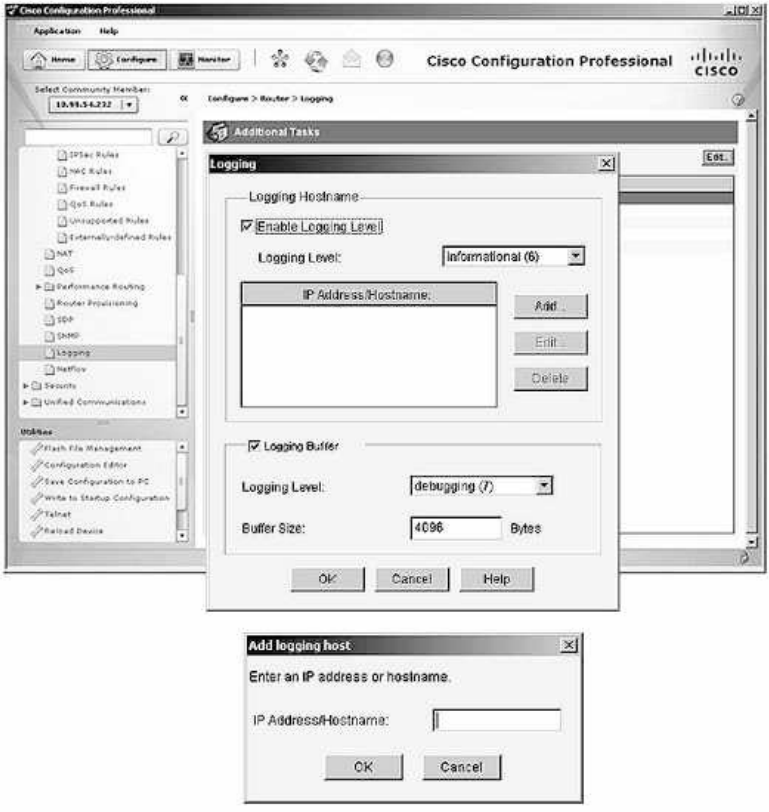
Los mensajes emergentes de loggin aparecen a medida que los eventos ocurren, también es posible visualizarlos con el comando **show logging**. Los mensajes llevan implícitos los datos correspondientes a la fecha, nivel de severidad y un mensaje de texto que indica detalles del mensaje.

```
00:00:46:%LINK-3-UPDOWN:Interface Port-channel1, changed state to up
00:00:47:%LINK-3-UPDOWN:Interface Ethernet0/1, changed state to up
00:00:47:%LINK-3-UPDOWN:Interface Ethernet0/2, changed state to up

Router> show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
 Console logging:disabled
 Monitor logging:level debugging, 0 messages logged
 Buffer logging:level debugging, 4104 messages logged
 Trap logging:level debugging, 4119 message lines logged
 Logging to 216.231.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from
209.165.200.225 (afi 0)
reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from
tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down
BGP
```

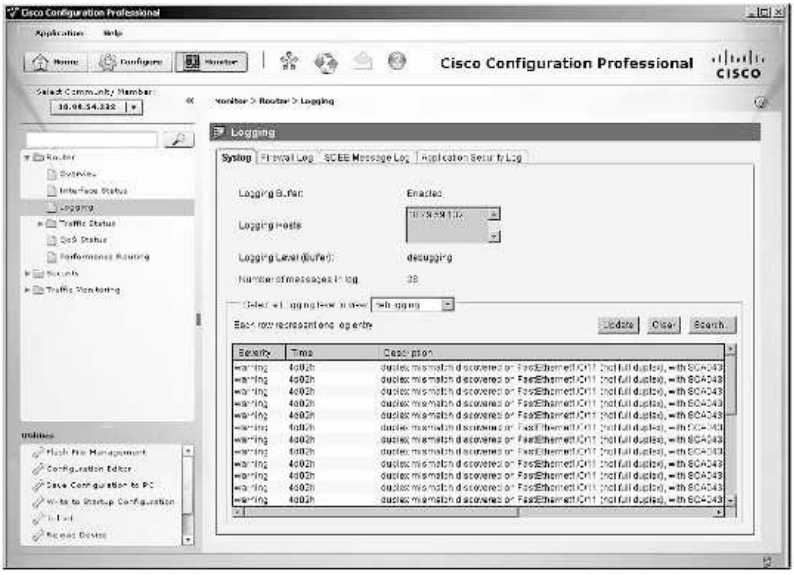
```
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor
209.165.200.226 3/1 (update
malformed) 0 bytes
```

La configuración del registro del sistema con CCP es muy simple:

- Desde **Configure** / **Router** / **Logging** y luego **Edit**.
- En la siguiente ventana seleccione el nivel desde **Logging Level**.
- Seleccione **add** para configurar la dirección IP del host.
- Acepte en **OK** para regresar a la ventana anterior y **OK** para salir.



CCP permite también ser utilizado como monitor de registros, para esto seleccione **Monitor** y luego **Logging**.



3.2 SNMP

SNMP (*Simple Network Management Protocol*) fue desarrollado para administrar nodos, servidores, estaciones de trabajo, routers, switches y dispositivos de seguridad, en una red IP. SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP es parte de la suite del protocolo TCP/IP.

SNMPv1, SNMPv2 y SNMPv3 están basados en administradores **NMS** (*Network Management Systems*), agentes (nodos administrados) y bases de información de administración ([**MIB**] *Management Information Bases*).

El administrador SNMP puede obtener información del agente y cambiar información en el agente (*get* y *set*). Los sets pueden cambiar variables de configuración en el dispositivo agente o iniciar acciones en los dispositivos.

Los agentes SNMP aceptan comandos y solicitudes de los sistemas de administración SNMP solo si esos sistemas tienen una community string configurada.

Hay dos tipos de *community strings*:

- **Community strings de solo lectura**: proporcionan acceso de solo lectura a todos los objetos en la MIB, excepto a las community strings.

- **Community strings de lectura-escritura**: proporcionan acceso de lectura-escritura a todos los objetos en la MIB, excepto a las community strings.

Por defecto, la mayoría de los sistemas SNMP utiliza *public* como community string, por lo tanto, cualquiera que tenga un sistema SNMP podrá leer la MIB del router.

SNMPv3 es un protocolo interoperable basado en estándares para administración de redes. La versión actual de SNMPv3 resuelve las vulnerabilidades de las versiones anteriores, incluyendo:

- **Integridad del mensaje**: asegura que el paquete no ha sido manipulado en su tránsito por la red.

- **Autenticación**: determina que el mensaje proviene de un origen válido.

- **Cifrado**: encripta los contenidos de un paquete para evitar que pueda ser visualizado por una fuente no autorizada.

- **Control de acceso**: limita a determinadas acciones la entrada a partes específicas de los datos.

SNMPv3 incluye tres niveles de seguridad:

- **noAuth**: autentica el paquete por medio de una comparación de *strings* en el nombre de usuario o community string.

- **Auth**: autentica el paquete usando HMAC (*Hashed Message Authentication Code*) con MD5 o SHA (*Secure Hash Algorithms*).

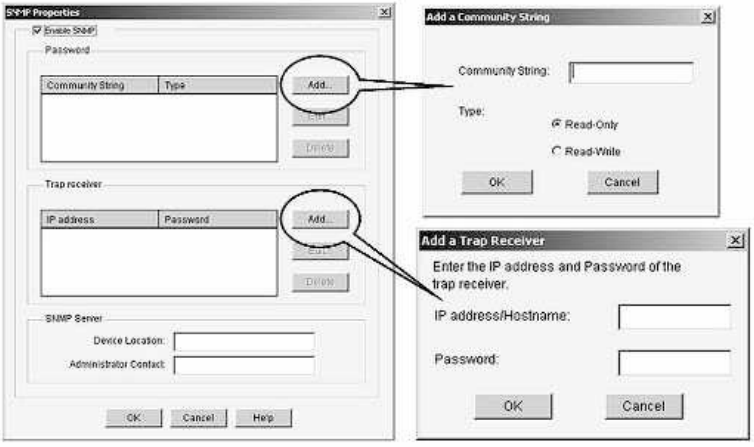
- **Priv**: autentica el paquete usando los algoritmos HMAC MD5 o HMAC SHA y cifra el paquete usando los algoritmos DES (*Data Encryption Standard*), 3DES o AES (*Advanced Encryption Standard*).

Para configurar SNMP por CLI se utiliza el siguiente comando:

```
Router(config)# snmp-server community string [view view-name]
[ro | rw] [number]
```

La configuración de SNMP con CCP solo soporta las versiones 1 y 2, SNMPv3 no está soportado por CCP. Para habilitar SNMPv1 y SNMPv2 siga los siguientes pasos:

- Elija la opción **Configure / Router / SNMP** y luego **Edit**.
- Desde la ventana de **SNMP Properties** marque la casilla **Enable SNMP**.
- Marque **Add** para agregar una nueva community string. Si ya existe una, puede editarla o borrarla desde **Edit** o **Delete**. En este punto también debe seleccionar si es de solo lectura o de lectura y escritura. Acepte desde **OK**.
- Para agregar un nuevo trap, desde la ventana de Trap Receiver seleccione **Add**. Configure la dirección IP o el nombre del host y finalmente la contraseña. Si ya existe uno, puede editarlo o eliminarlo desde **Edit** o **Delete**. Acepte desde **OK**.



3.3 NTP

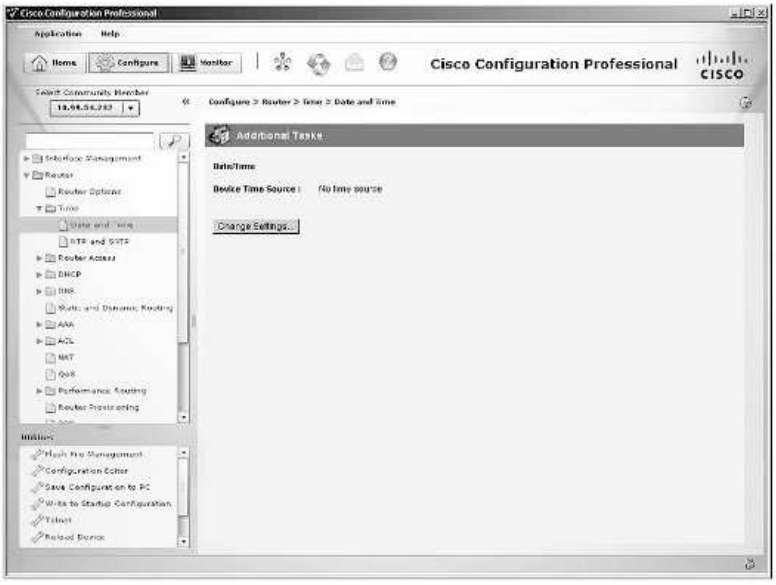
Para asegurarse de que los mensajes del registro estén sincronizados entre sí deben mantenerse los relojes de los hosts y los dispositivos de red sincronizados entre sí. Aunque la configuración manual funciona en un ambiente de una red pequeña, a medida que la red crece se vuelve difícil asegurarse de que todos los dispositivos de la infraestructura estén operando con la fecha sincronizada.

NTP (*Network Time Protocol*) permite a los routers de la red sincronizar sus configuraciones de tiempo con un servidor NTP (puerto UDP 123). Un grupo de clientes NTP puede obtener información de fecha y hora de una sola fuente y tener configuraciones más consistentes. Cuando se implementa NTP en la red, puede configurarse para que se sincronice con un reloj privado o puede sincronizarse con un servidor NTP disponible públicamente en Internet. Muchos servidores NTP en Internet no solicitan ninguna autenticación de sus pares; por lo tanto, el administrador de la red debe confiar en que el reloj mismo es confiable, válido y seguro.

La configuración manual de la fecha y hora se realiza con el comando:

```
Router# clock set hh:mm:ss day month year

Router# clock set 14:38:00 feb 10 2012

Router# show clock

14:38:11.292 PST Tue Feb 10 2012
```

La configuración horaria con CCP lleva los siguientes pasos, seleccione **Configure / Router / Time / Date and Time**:



En la ventana emergente seleccione **Change Settings** y a continuación configure los datos correspondientes a la fecha y hora para finalizar con **Apply**:

En una red configurada con NTP, se designan uno o más routers como *master* NTP, que serán los encargados de mantener el reloj. El siguiente comando habilita un NTP *master*.

```
Router(config)# ntp master [stratum]
```

El valor de estrato es el número de saltos desde una fuente externa, como puede ser un reloj atómico.

NOTA:

La configuración del master NTP debe incluir la configuración previa del reloj o algún mecanismo de ajuste horario como Internet, vía satélite o radio.

Las asociaciones entre máquinas que ejecutan NTP generalmente tienen una configuración estática. Se da a cada dispositivo la dirección IP de los *masters* NTP. Es posible obtener una fecha y hora precisas intercambiando mensajes NTP entre cada par de máquinas con una asociación.

Para que el reloj de un cliente NTP sincronice con un servidor NTP se utiliza el siguiente comando:

```
Router(config)# ntp server ip-address [version number] [key keyid]
[source interface] [prefer]
```

Configure el dispositivo para recibir mensajes broadcast NTP en una determinada interfaz:

```
Router(config-if)# ntp broadcast client
```

NTPv3 (NTP versión 3) y posteriores soportan un mecanismo de autenticación criptográfico entre pares NTP. Este mecanismo de autenticación, en conjunto con las ACL que especifican a qué dispositivos de red se les permite sincronizarse con otros dispositivos de red, puede ser usado para ayudar a mitigar posibles ataques. La autenticación es para el beneficio del cliente para asegurar que esté obteniendo la hora de un servidor autenticado.

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key number md5 value
Router(config)# ntp trusted-key key-number
```

EJEMPLO:

```
ServerNTP# configure terminal
ServerNTP(config)# ntp master 1
ServerNTP(config)# exit

ServerNTP# show clock

14:38:11.292 PST Tue Feb 10 2012

ClienteNTP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ClienteNTP(config)# ntp server 172.25.1.1
ClienteNTP(config)# ntp server 172.25.1.2
ClienteNTP(config)# interface FastEthernet0/0
ClienteNTP(config-if)# ntp broadcast client
ClienteNTP(config-if)#exit
ClienteNTP(config)#ntp authenticate
ClienteNTP(config)# ntp authentication-key 1 md5 CCNA35
ClienteNTP(config)#exit

ClienteNTP# show ntp status

Clock is synchronized, stratum 4, reference is 172.25.1.1 nominal
freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (14:38:11.292 PST Tue Feb 10
2012) clock offset is 7.33 msec, root delay is 133.36 msec root
dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

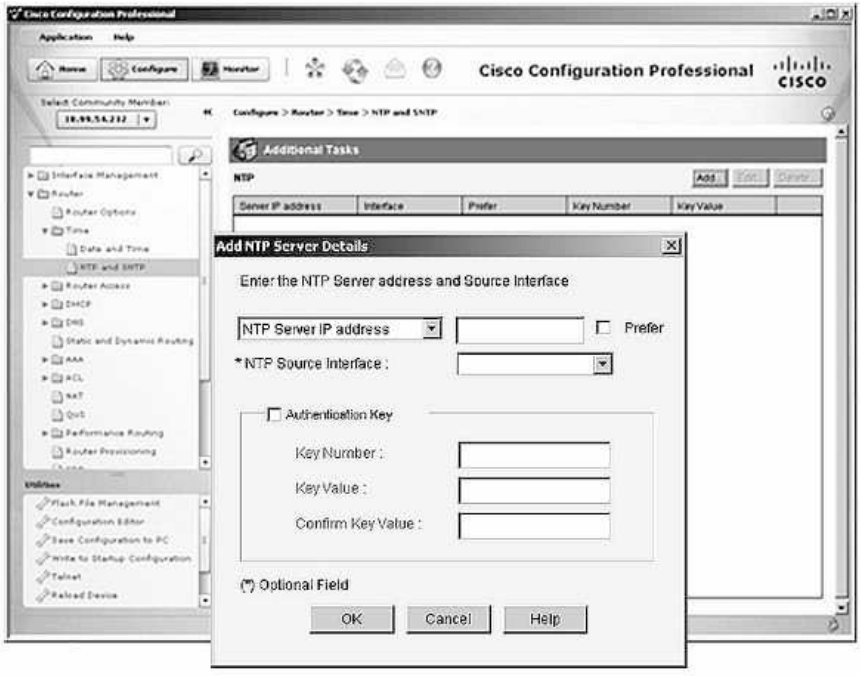
Pueden verse las asociaciones NTP a través de los siguientes comandos:

```
show ntp associations

show ntp associations detail
```

Para configurar NTP con CCP siga los siguientes pasos:

- Desde **Configure / Router / Time / NTP and SNTP**, seleccione **Add**.
- Desde la siguiente ventana agregue el nombre del servidor o la IP correspondiente. El parámetro **NTP Source Interface** es opcional.
- Si el servidor NTP utiliza autenticación, configure los parámetros desde **Authentication Key**.

- Finalice con **OK**.

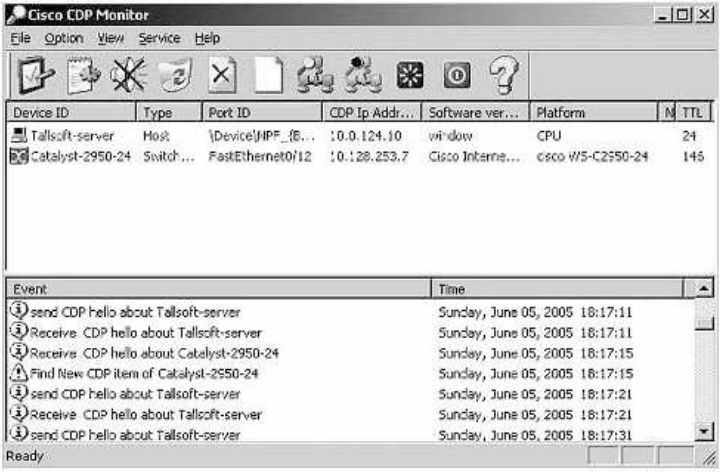


3.4 AUDITORÍAS DE SEGURIDAD

Los dispositivos Cisco traen inicialmente muchos servicios habilitados por defecto. Estos servicios pueden hacer que el dispositivo se vuelva vulnerable a ataques si no se habilita seguridad. Los administradores pueden, además, habilitar otros servicios que pueden exponer el dispositivo a riesgos significativos. Ambas situaciones deben tomarse en cuenta al asegurar la red.

CDP (*Cisco Discovery Protocol*) es un ejemplo de un servicio habilitado por defecto en los routers de Cisco. Se usa principalmente para obtener direcciones de protocolo de los dispositivos de Cisco circundantes y para descubrir las plataformas de esos dispositivos. Desafortunadamente, un atacante en la red puede usar CDP para descubrir dispositivos en la red local. Los atacantes no necesitan tener dispositivos habilitados para CDP, simplemente el software como el CDP

Monitor de Cisco, permite obtener la información buscada. Aunque es una herramienta extremadamente útil, el uso de CDP debe restringirse. Los dispositivos de borde son un ejemplo de un dispositivo que no debe tener esta función habilitada.



Dependiendo de las necesidades de seguridad de la organización, muchos servicios deberían estar deshabilitados o mínimamente restringidos en sus capacidades.

Muchas prácticas ayudan a certificar que un dispositivo sea seguro.

- Deshabilitar los servicios e interfaces innecesarios.
- Deshabilitar y restringir los servicios de administración comúnmente configurados, como SNMP.
- Deshabilitar servicios de sonda y escaneo, como ICMP.
- Asegurar la seguridad del acceso terminal.
- Deshabilitar el Protocolo ARP gratuito y proxy.
- Deshabilitar broadcasts dirigidos por IP.

La siguiente tabla muestra algunas recomendaciones más:

Función	Por defecto	Acción
CDP	Habilitado	Deshabilitarlo globalmente o por interfaz.
FTP	Deshabilitado	Habilitarlo solo cuando se necesite.
TFTP	Deshabilitado	Habilitarlo solo cuando se necesite.
NTP	Deshabilitado	Habilitarlo solo cuando se necesite.
SNMP	Habilitado	Deshabilitarlo cuando no se necesite.
HTTP, HTTPS	Habilitado	Deshabilitarlo cuando no se necesite o restrinja el acceso con ACL.
DNS	Habilitado	Deshabilitarlo cuando no se necesite. Si es necesario el servicio, asegúrese de que el servidor DNS sea confiable.
ICMP	Habilitado	Deshabilitarlo cuando no se necesite.
ARP gratuito	Habilitado	Deshabilitarlo según las interfaces cuando no se necesite.
ARP proxy	Habilitado	Deshabilitarlo en todas las interfaces salvo cuando el router funcione como puente en una LAN.

Los administradores deben determinar primero las vulnerabilidades existentes en la configuración para asegurar los dispositivos de la red. La mejor manera de lograrlo es a través de alguna herramienta de auditoría de seguridad. Esta efectúa revisiones en el nivel de seguridad de las configuraciones comparándolas con configuraciones recomendadas y recolectando discrepancias.

Cisco recomienda las siguientes herramientas de auditoría de seguridad:

- **Asistente de Auditoría de Seguridad**: es una función de auditoría de seguridad presente en el CCP de Cisco. Proporciona una lista de vulnerabilidades y luego permite al administrador elegir qué cambios realizar en la configuración.

- **Cisco AutoSecure**: una función de auditoría de seguridad disponible a través de la CLI del IOS. El comando **autosecure** inicia una auditoría de seguridad y luego permite cambios de configuración. Basándose en el modo seleccionado, los cambios de configuración pueden ser automáticos o requerir participación del administrador de la red.

- **One-Step Lockdown**: es una función de auditoría de seguridad proporcionada por el CCP de Cisco. La función One-Step Lockdown proporciona una lista de vulnerabilidades y luego efectúa automáticamente los cambios de configuración recomendados para la seguridad.

Tanto el Asistente de Auditoría de Seguridad como One-Step Lockdown están basadas en la función Autosecure del Cisco IOS.

3.4.1 Asistente de Auditoría de Seguridad

El Asistente de Auditoría de Seguridad compara la configuración del router contra las configuraciones recomendadas y hace lo siguiente:

- Deshabilita los servidores y los servicios innecesarios.

- Deshabilita o hace hardening en SNMP.

- Apaga las interfaces no utilizadas y aplica el firewall a las interfaces externas.

- Verifica lo fuertes que pueden ser las contraseñas.

- Establece el uso de ACL.

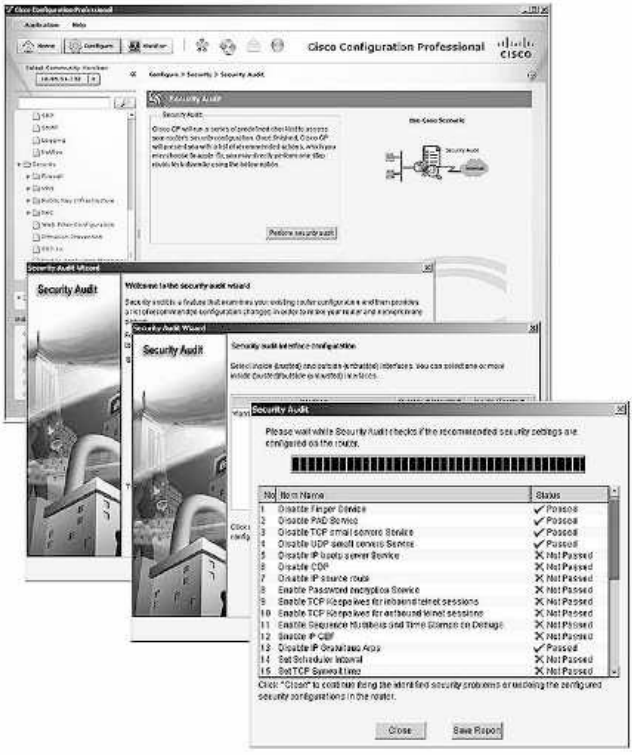
Para la configuración del Asistente de Auditoría de Seguridad desde CCP siga los siguientes pasos:

- Desde **Configure** / **Security** / **Security Audit**, seleccione el botón **Perform security audit**.

- Prosiga con **Next** y en la siguiente ventana seleccione el tipo de interfaz y luego **Next**.

- Espere hasta que termine el proceso y guarde el reporte desde **Save Report**.

- Efectúe las acciones pertinentes.



3.4.2 Cisco AutoSecure

AutoSecure puede asegurar las funciones del plano de administración y las funciones y servicios del plano de reenvíos de un router; es una función que se inicia desde la CLI y ejecuta un script.

El plano de administración hace referencia a la ruta lógica del tráfico de administración de una plataforma de enrutamiento. Este puede ser:

- Servicios como BOOTP, CDP, FTP, TFTP, PAD, UDP y TCP, MOP, ICMP, enrutamiento de origen IP, Finger, cifrado de contraseñas, keepalives de TCP, ARP gratuito, ARP proxy y broadcast dirigidos seguros.
- Notificación legal a través de un banner.
- Contraseñas y funciones de autenticación seguras.
- NTP seguro.
- Acceso SSH seguro.
- Servicios de interceptación de TCP.

El plano de reenvíos es responsable del reenvío de paquetes. Hay tres servicios y funciones:

- Habilita CEF (*Cisco Express Forwarding*).
- Habilita filtrado de tráfico con ACL.
- Implementa inspección del firewall de IOS para protocolos comunes.

Generalmente se usa AutoSecure para proporcionar una política de seguridad básica en un router nuevo. Las funciones pueden ser alteradas posteriormente para soportar la política de seguridad de la organización.

El comando **autosecure** inicia la configuración en el router:

```
Router# auto secure [management | forwarding] [no-interact | full]
[ntp | login | ssh | firewall | tcp-intercept]
```

Por defecto el modo es interactivo, el router presenta opciones para habilitar o deshabilitar servicios y otras funciones de seguridad.

Los siguientes parámetros son opcionales:

- **no-interact**: no mostrará ninguna configuración interactiva al usuario, como nombres de usuarios o contraseñas.
- **full**: se mostrarán preguntas interactivas (viene por defecto).
- **forwarding**: solo se asegura el plano de reenvío.
- **management**: solo se asegura el plano de administración.
- **ntp**: especifica la configuración de NTP en la CLI de AutoSecure.
- **login**: especifica la configuración de la función *login* en la CLI de AutoSecure.
- **ssh**: especifica la configuración de la función *login* en la CLI de AutoSecure.
- **firewall**: especifica la configuración de la función firewall en la CLI de AutoSecure.
- **tcp-intercept**: especifica la configuración de la función *tcp-intercept* en la CLI de AutoSecure.

NOTA:

Si está utilizando CCP, debe habilitar manualmente el servidor HTTP a través del comando ***ip http server****, o HTTPS utilizando el comando* ***ip http secure-server*** *después de completar la configuración de AutoSecure.*

EJEMPLO:

La siguiente sintaxis muestra cuándo se inicia el comando **auto secure**, un asistente lleva al administrador a través de toda la configuración del dispositivo.

```
Router#auto secure
 --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:
.....................................................

Router#show auto secure config
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no snmp-server community public
no snmp-server community private
banner ^C Test ^C
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 00071A1507545B54
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
```

```
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 6
 login authentication local_auth
 transport input telnet
login block-for 5 attempts 5 within 6

crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 6
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
!
interface Serial0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
!
ip cef
Router#
```

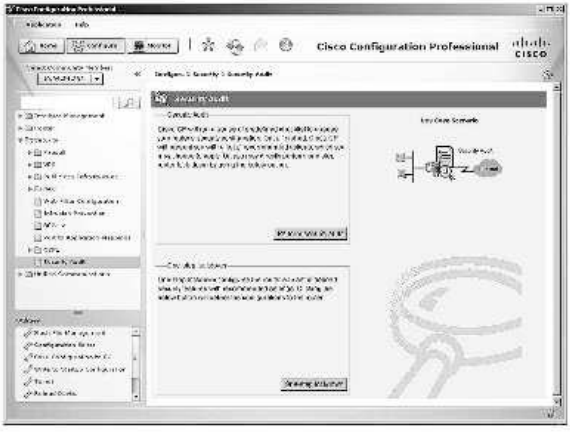
3.4.3 One-Step Lockdown

One-step lockdown examina la configuración del router buscando problemas de seguridad potenciales y efectúa automáticamente los cambios necesarios de la configuración para corregirlos.

One-Step Lockdown produce las siguientes acciones:

Deshabilita	Habilita	Configura
Servicio de Finger Servicio de PAD Servicio de pequeños servidores TCP INK icio de pequeños servidores UDP Servicio de servidores BOOTP IP Servicio de identificación de IP Cisco Discovery Protocol Ruta de origen IP GARP IP SNMP Redirecciones IP ARP proxy IP Broadcast dirigido por IP Servicio MOP IP inalcanzables Respuesta de solicitud de máscara IP IP inalcanzables en interfaz nula	Servicio de cifrado de contraseñas Keepalives TCP para sesiones telnet entrantes y salientes Números de secuencia y marcas de tiempo en los debugs Conmutación de IP Cisco Express Forwarding Enable NetFlow Reverse Path Forwarding (RPF) Unicast en interfaces externas Firewall en todas las interfaces externas SSH para acceso al router AAA	Longitud de contraseña mínima en seis caracteres Tasa de fallos de autenticación a menos de tres intentos Tiempo synwait TCP Banner de notificaciones Parámetros de inicio de sesión Contraseña enable secret password Scheduler interval Scheduler allocate Usuarios telnet Clase de acceso al servicio de servidor HTTP Clase de acceso en líneas vty

- Desde **Configure** / **Security** / **Security Audit**, seleccione el botón **One-step lockdown**.



- Continúe aceptando desde el botón **Yes**. Las siguientes pantallas lo guiarán durante todo el proceso de configuración.

3.5 FUNDAMENTOS PARA EL EXAMEN

- Tenga una idea clara de la diferencia entre *in-band* y *out-of-band*.
- Memorice el nivel y la definición de los mensajes de registro y cuáles son las formas de enviar los eventos.
- Practique con equipos reales o simuladores las configuraciones de SNMP y NTP.
- Recuerde la función de sincronización que realiza NTP.
- Estudie y analice para qué sirven las auditorías de seguridad.
- Estudie las funciones y configuraciones de Cisco AutoSecure y One-step lockdown.

Capítulo 4

AAA

4.1 INTRODUCCIÓN A AAA

Se pueden utilizar diferentes tipos de métodos de autenticación en un dispositivo Cisco y cada uno ofrece varios niveles de seguridad. La forma más simple de autenticación son las contraseñas. Los inicios de sesión de solo contraseña son muy vulnerables a ataques de fuerza bruta.

Adicionalmente, este método no ofrece registros de auditoría de ningún tipo. Cualquiera que tenga la contraseña puede ganar acceso al dispositivo y alterar la configuración.

Utilizando una combinación de usuario y contraseña en la consola, líneas vty y aux ayudará a proporcionar registros de auditoría. La autenticación de base de datos local puede implementarse usando uno de los siguientes comandos:

```
username username password password
```

```
username username secret password
```

AAA (*Authentication*, *Authorization*, *Accounting*) provee una mejor solución al hacer que todos los dispositivos accedan a la misma base de datos de usuarios y contraseñas en un servidor central. Cada una de las partes se detalla a continuación:

- **Authentication**. El proceso de autenticación se encarga de verificar que el usuario es quien dice ser, por ejemplo mediante el uso de un nombre de usuario y contraseña.
- **Authorization**. El proceso de autorización determina a qué recursos tiene acceso el usuario una vez que se ha autenticado.
- **Accounting**. El proceso de auditoría se encarga de registrar la actividad realizada por el usuario una vez que haya sido autenticado.

NOTA:

El proceso AAA puede resumirse en estas tres preguntas:

✓ *¿Quién es usted?*
Autenticación

✓ *¿Qué se le permite hacer al usuario?*
Autorización

✓ *¿Qué han estado haciendo los usuarios en la red?*
Auditoría

4.1.1 Modos de acceso AAA

Puede utilizarse AAA para autenticar usuarios para acceso administrativo o para acceso remoto a una red. Estos dos métodos de acceso usan diferentes modos para solicitar los servicios de AAA.

AAA tiene dos modos de acceso (carácter y paquete), que se resumen en la siguiente lista:

Interfaz	Modo	Descripción
AUX	Carácter	Puerto auxiliar DTE
Consola	Carácter	Puerto de consola
TTY	Carácter	Puerto asíncrono

VTY	Carácter	Terminales virtuales
PPP	Paquete	Interfaces PPP, serial o ISDN
Arap	Paquete	AppleTalk Remote Access (ARA)
NASI	Paquete	NetWare Access Server Interface o intefaz serie

4.1.2 Autenticación AAA

La autenticación AAA local utiliza una base de datos local para la autenticación. Este método almacena los nombres de usuario y sus correspondientes contraseñas localmente en el router Cisco, y los usuarios se autentican en la base de datos local. Este método no es muy seguro y puede mejorarse con la autenticación basada en servidor.

El método basado en servidor utiliza un recurso externo de servidor de base de datos a través de los protocolos **RADIUS** (*Remote Dial-in User Services*) o **TACACS+** (*Terminal Access Control Access Control Server Plus*). La familia de productos de **ACS** (*Access Control Server*) de Cisco soporta tanto TACACS+ como RADIUS, que son los dos protocolos predominantes usados por los dispositivos de seguridad para la implementación de AAA.

4.1.3 Autorización AAA

Una vez que los usuarios han sido autenticados exitosamente contra la fuente de datos AAA seleccionada (ya sea local o basada en servidor), se les autoriza el acceso a recursos específicos en la red. La autorización consiste básicamente en lo que un usuario puede y no puede hacer en la red luego de que es autenticado, parecido a cómo los niveles de privilegios y la CLI basada en roles les dan a los usuarios derechos y privilegios específicos a ciertos comandos en el router.

En general, la autorización se implementa usando una solución de AAA basada en servidor y utiliza un grupo de atributos creado que describe el acceso del usuario a la red. Estos atributos se comparan con la información contenida dentro de la base de datos AAA y se determinan las restricciones para ese usuario, que son enviadas al router local donde el usuario está conectado.

La autorización, que se implementa inmediatamente después de que el usuario se autentica, es automática: no se requiere participación de parte del usuario luego de la autenticación.

4.1.4 Auditoría AAA

El registro de auditoría recolecta y reporta datos de uso para que puedan ser empleados para auditorías o emisión de facturas. Los datos recolectados pueden incluir el inicio y fin de conexiones, comandos ejecutados, números de paquetes y número de bytes. El registro de auditoría se implementa usando una solución AAA basada en servidor. Estas estadísticas pueden ser extraídas para crear reportes detallados sobre la configuración de la red.

Un uso popular de los registros de auditoría es su combinación con la autenticación AAA para la administración de dispositivos de redes por parte de los administradores. El registro de auditoría proporciona una mejor rendición que la que ofrece la autenticación. Los servidores AAA mantienen un registro detallado de absolutamente todo lo que hace el usuario una vez autenticado en el dispositivo. Esto incluye todos los comandos de configuración y EXEC emitidos por el usuario. El registro contiene varios campos de datos, incluyendo el nombre de usuario, la fecha y hora y el comando ingresado por el usuario. Esta información es útil, al solucionar problemas en los dispositivos. También proporciona protección contra individuos malintencionados.

4.2 CONFIGURACIÓN LOCAL DE AAA

4.2.1 Configuración de AAA con CLI

El comando **aaa new-model** sirve para habilitar AAA en el router. Si se utiliza la forma **no** delante quedará deshabilitado. Defina una lista nombrada de los métodos de autenticación y luego aplíquela a las interfaces con el comando **aaa authentication login**.

```
Router(config)# aaa new-model
Router(config)# aaa authentication login {default | list-name}
method1 [method2...]
```

Para habilitar un nombre de lista específico, use el comando **aaa login authentication** *list-name* en el modo de configuración de línea correspondiente. Cuando se habilita por primera vez AAA, se aplica una lista por defecto llamada **default** a todas las interfaces y líneas, pero no tiene métodos de

autenticación definidos, estos pueden definirse con el comando **aaa authentication login default** *method1*[*method2*...].

Es posible obtener información de todos los usuarios bloqueados, como así también poder desbloquear a un usuario específico:

```
Router# show aaa local user lockout
Router# clear aaa local user lockout {username username | all}
```

Los siguientes comandos permiten manejar los intentos fallidos antes de bloquear la cuenta de un usuario. El primero, tras un número excesivo de intentos fallidos de ingreso, bloquea el usuario hasta que un administrador lo desbloquee. El segundo comando realiza un retraso entre intentos de ingreso fallidos sin bloquear la cuenta.

```
Router(config)# aaa local authentication attempts max-fail number-
of-unsuccessful-attempts

Router(config)# login delay
```

Para ver los atributos recolectados en una sesión AAA, utilice el siguiente comando:

```
Router# show aaa user {all | unique id}
```

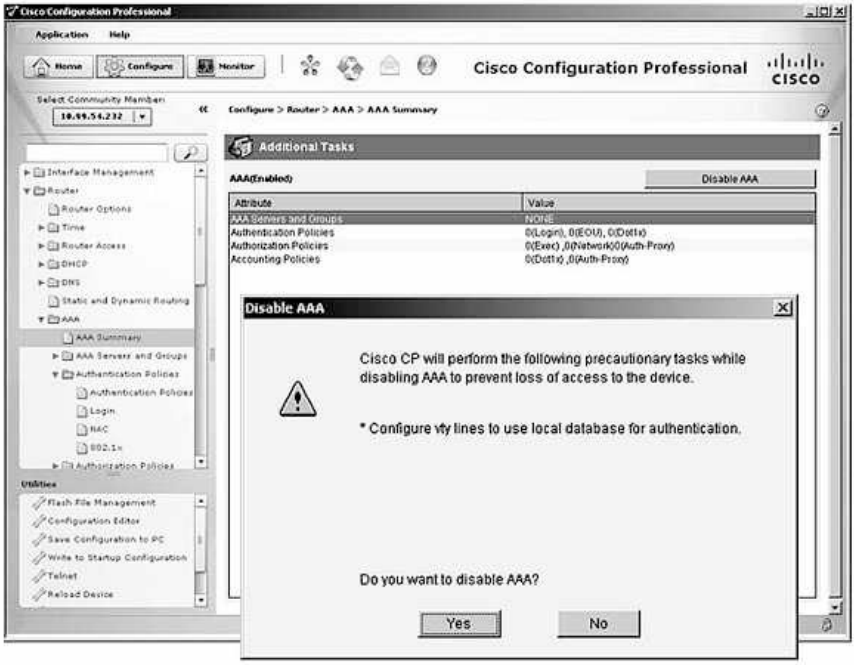
Este último comando no proporciona información sobre todos los usuarios que ingresan a un dispositivo, sino sobre aquellos que han sido autenticados o autorizados usando AAA o cuyas sesiones están siendo monitorizadas por el módulo de registro de auditoría de AAA.

Puede usarse el comando **show aaa sessions** para visualizar el ID único de una sesión.

4.2.2 Configuración de AAA con CCP

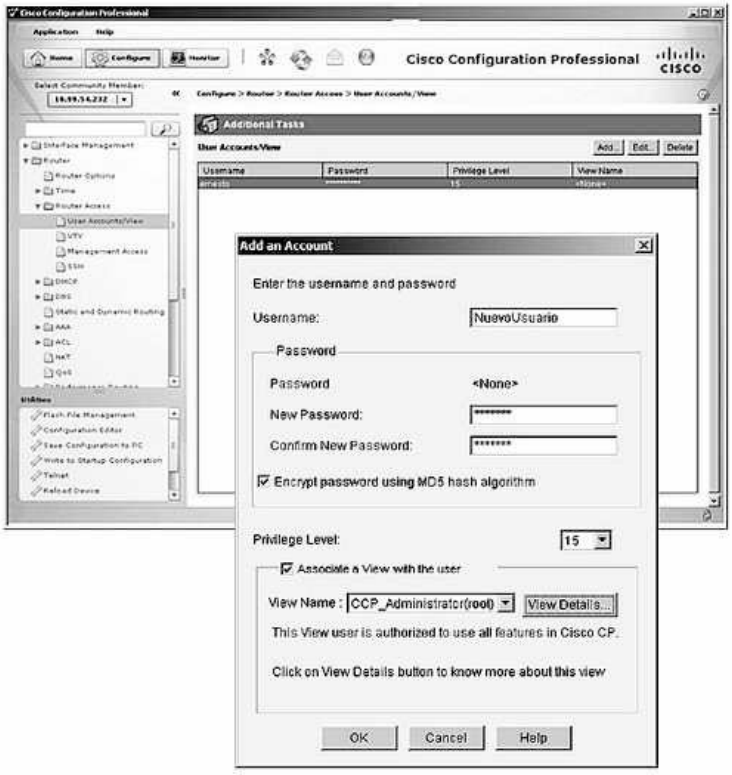
AAA puede configurarse a través de CCP. Para verificar la configuración y poder habilitar o deshabilitar AAA, seleccione **Configure** / **Router** / **AAA** / **AAA Summary**. Se mostrará el estado dependiendo de las configuraciones. Cuando AAA está deshabilitada, hay que habilitarla desde el botón **enable**. Seleccione **Yes** para continuar.

Desde el botón **Disable AAA**, CCP muestra un mensaje informativo indicando que hará cambios en la configuración para asegurarse de que se podrá acceder al router después de la activación de AAA.



La primera tarea cuando se utiliza CCP para configurar los servicios de AAA para autenticación local es la creación de los usuarios:

- Seleccione **Configure** / **Router** / **Router Access** / **User Accounts** / **View**.
- Desde **Add** puede añadir un nuevo usuario.
- En la ventana emergente defina la cuenta de usuario con el nombre y la contraseña apropiada.
- Defina el nivel de privilegio.
- Si se han definido vistas, marque la casilla **Associate a View with the user** y verifique la vista asociada con el usuario.
- Finalice con **OK**, **Deliver** y **OK** en las ventanas subsiguientes.


Cisco Configuration Professional
Add an Account
Enter the username and password
Username:
NuevoUsuario
Password
Password
<None>
New Password:
Confirm New Password:
Encrypt password using MD5 hash algorithm
Privilege Level:
15
Associate a View with the user
View Name :
CCP_Administrator(root)
View Details...
This View user is authorized to use all features in Cisco CP.
Click on View Details button to know more about this view
OK
Cancel
Help


Deliver Configuration to Device
Commands Delivery Status
Command Delivery Status:
Preparing commands for delivery...
Submitting 2 commands, please wait...
Configuration delivered to device.
OK
Deliver
Cancel
Save to file
Help

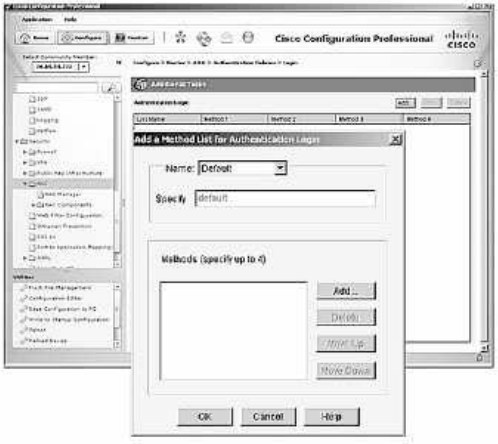
Para configurar la autenticación AAA, se debe primero definir una lista de métodos de autenticación. Las listas de métodos deben ser aplicadas a las diferentes interfaces o líneas. Configure la lista de métodos por defecto para la autenticación de inicio de sesión utilizando la base de datos local:

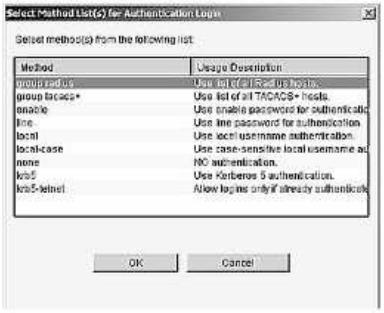
- Seleccione **Configure** / **Router** / **AAA** / **Authentication Policies** / **Login**. Para ver las opciones de una lista de métodos, elija el nombre de la lista y pulse **Edit**, para agregar una nueva seleccione **Add**.

- Desde el menú de edición de listas de métodos de autenticación de inicio de sesión pulse **Add**.

- Si no estuviera seleccionado, desde la lista de seleccionar método de autenticación de inicio de sesión, seleccione **local**.

- Finalice con **OK**.





Desde la CLI se podrá observar:

```
username nuevo_usuario privilege 15 secret 5
$1$f16u$uKOO6J/UnojZ0bCEzgnQi1 view root.
aaa authentication login default local.
```

4.3 AUTENTICACIÓN AAA BASADA EN SERVIDOR

Mantener bases de datos locales de autenticación para cada router en una red de cierto tamaño no es fiable. Como solución a este problema pueden usarse uno o más servidores AAA, para crear una base de datos de usuario y administrativa central a la que accedan todos los dispositivos de la red. También puede trabajar con bases de datos externas, incluyendo Active Directory y **LDAP** (*Lightweight Directory Access Protocol*). Estas bases de datos almacenan información de cuentas de usuario y contraseñas, permitiendo una administración centralizada de las cuentas de usuario.

El método basado en servidor utiliza un recurso externo de servidor de base de datos a través de los protocolos RADIUS (*Remote Dial-in User Services*) o TACACS+ (*Terminal Access Control Access Control Server Plus*). Aunque ambos protocolos pueden ser usados para la comunicación entre clientes y servidores AAA, TACACS+ es considerado el más seguro entre ambos. TACACS+ es una mejora de Cisco sobre el protocolo TACACS original. A pesar de su nombre, TACACS+ es un protocolo enteramente nuevo que es incompatible con todas las versiones anteriores de TACACS.

4.3.1 Protocolos de autenticación AAA

RADIUS está definido en la RFC 2865 y TACACS+ en la RFC 1492. Ambos protocolos se encargan de proporcionar servicios AAA, pero existen diferencias sustanciales entre ellos.

RADIUS utiliza UDP, puerto 1645 o el 1812 para la autenticación y el puerto UDP 1646 o el 1813 para los registros de auditoría, mientras que TACACS+ utiliza TCP puerto 49, lo que conlleva una serie de diferencias en el comportamiento de ambos protocolos:

- TCP proporciona dos mecanismos para saber que el servidor ha fallado: uno a través de las banderas RST y el otro a través de los keepalives. En el caso de UDP son las aplicaciones las que deben realizar estas funciones.

- TCP escala mejor que UDP en grandes redes, especialmente si la red tiende a estar congestionada.

- TCP permite múltiples conexiones simultáneas a múltiples servidores enviando automáticamente solo a aquellos que estén activos. UDP necesitaría programación extra en las aplicaciones.

Tanto TACACS+ como RADIUS son protocolos de administración, pero cada uno soporta diferentes capacidades y funcionalidades. La elección de uno sobre otro depende de las necesidades de la organización. Las diferencias entre ambos se enumeran a continuación:

1. RADIUS fue desarrollado por Livingston Enterprises; es un protocolo AAA abierto de estándar IETF con aplicaciones en acceso a las redes y movilidad IP.

2. TACACS+ es una mejora de Cisco del protocolo TACACS original, es un protocolo enteramente nuevo que es incompatible con todas las versiones anteriores de TACACS.

3. El protocolo RADIUS esconde las contraseñas durante la transmisión, el resto del paquete se envía en texto plano.

4. RADIUS combina autenticación y autorización en un solo proceso.

5. RADIUS es muy popular entre los proveedores de servicio VoIP.

6. RADIUS no permite especificar qué comandos puede utilizar el usuario después de iniciar una sesión en el router, simplemente permite o deniega el acceso al equipo.

7. TACACS+ tiene dos métodos de autorizar el uso de comandos en el router:

    - Especificando en el servidor TACACS+ los comandos que se permite usar a un determinado usuario o grupo.

    - Confiando en los niveles de privilegio. Se lanza una consulta al servidor TACACS+ para ver si el usuario o grupo puede usar un determinado comando en un determinado nivel de privilegio.

8. El protocolo DIAMETER es el reemplazo programado para RADIUS. DIAMETER usa un nuevo protocolo de transporte llamado **SCTP** (*Stream Control Transmission Protocol*) y TCP en lugar de UDP.

9. RADIUS no soporta los siguientes protocolos:

   - AppleTalk Remote Access (ARA) protocol.
   - NetBIOS Frames Protocol Control protocol.
   - Novell Asynchronous Services Interface (NASI).
   - X.25 PAD connection.

10. TACACS+ ofrece soporte multiprotocolo, como IP y AppleTalk.

11. TACACS+ proporciona servicios AAA separados.

12. Las extensiones al protocolo TACACS+ proporcionan más tipos de códigos de solicitud y respuesta de autenticación que los que estaban en la especificación TACACS original.

13. TACACS+ separa completamente los procesos de autenticación y autorización y soporta más protocolos que RADIUS, mientras que RADIUS los unifica.

4.3.2 Cisco Secure ACS

Cisco Secure ACS (*Access Control Server*) es un servidor de control de acceso altamente escalable y de alto rendimiento que puede ser usado para controlar el acceso y la configuración administrativos para todos los dispositivos de red en una red que soporta RADIUS, TACACS+ o ambos. Cisco Secure ACS ofrece varios beneficios:

- Extiende la seguridad de acceso al combinar la autenticación, el acceso del usuario y el acceso del administrador con control de políticas.
- Permite mayor flexibilidad y movilidad, seguridad mejorada y ganancias en la productividad del usuario.
- Aplica una política de seguridad uniforme para todos los usuarios, sin importar cómo acceden a la red.

- Reduce la carga administrativa, ya que escala el acceso administrativo y de usuario a la red.

Cisco Secure ACS soporta una gran variedad de conexiones de acceso, incluyendo redes LAN cableadas e inalámbricas, dialup, banda ancha, contenido, almacenamiento, VoIP, firewalls y VPN, y proporciona una variedad de funciones avanzadas:

- Monitorización automática de servicio.
- Sincronización de la base de datos e importación de herramientas de despliegues de gran escala.
- Soporte de autenticación de usuario LDAP.
- Reporte de acceso administrativo y de usuario.
- Restricciones al acceso a la red basadas en criterios como la hora y el día de la semana.
- Perfiles de grupo de dispositivos y usuario.

NOTA:

Cisco Secure ACS está disponible como software instalable en un Windows Server o en un servidor 1U montable en rack, este último puede dar soporte a más de 350 usuarios.

4.3.3 Instalación de ACS

La opción de Cisco Secure ACS para Windows habilita los servicios AAA en un router para contactar un ACS externo instalado en un sistema de servidor Windows para autenticación de usuario y administrador.

Antes de la instalación de Cisco Secure ACS en el Servidor Windows se deben tener en cuenta los siguientes requisitos:

- Para un soporte completo de TACACS+ y RADIUS en IOS, los clientes AAA deben estar utilizando la versión 11.2 de IOS o posterior.

- Los dispositivos Cisco que no son clientes AAA de IOS deben ser configurados con TACACS+, RADIUS o ambos.

- Los clientes dial-in, VPN o inalámbricos deben poder conectarse a los clientes AAA aplicables.

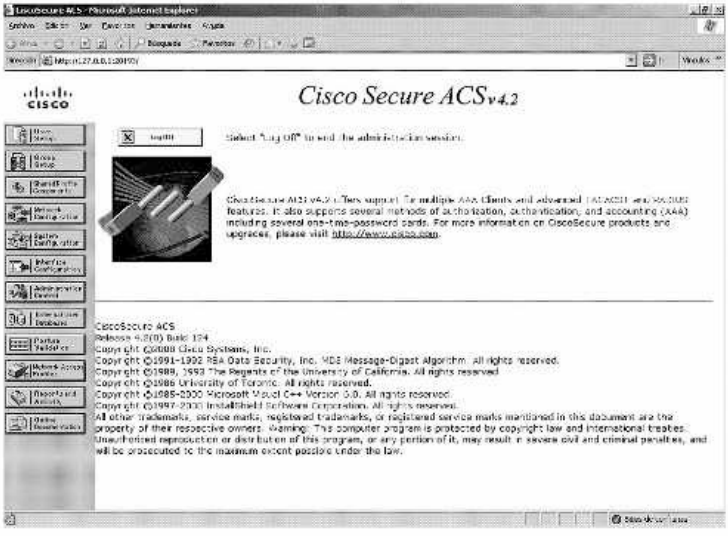
- El ordenador que ejecuta ACS debe poder alcanzar a todos los clientes AAA a través del ping.

- Los dispositivos gateway entre el ACS y otros dispositivos en la red deben permitir la comunicación a través de los puertos necesarios para soportar la función o el protocolo aplicable.

- Debe instalarse un navegador web soportado en el ordenador que ejecuta el ACS.

- Deben habilitarse todas las NIC en el ordenador que ejecuta el ACS. Si hay una tarjeta de red deshabilitada, la instalación puede resultar lenta por retrasos causados por la Microsoft CryptoAPI.

Luego de haber instalado el ACS exitosamente, debe realizarse una configuración inicial. La única manera de configurar un servidor ACS es a través de una interfaz HTML. La página de inicio del Cisco Secure ACS es la siguiente:



4.3.4 Configuración de ACS

La página de inicio de Cisco Secure ACS está dividida en marcos. Los botones de la barra de navegación representan áreas o funciones particulares que pueden ser configuradas:

- Configuración de usuario.
- Configuración de grupo.
- Componentes de perfil compartido.
- Configuración de red.
- Configuración del sistema.
- Configuración de la interfaz.
- Control de administración.
- Bases de datos de usuarios externas.
- Validación de postura.
- Perfiles de acceso a la red.
- Reportes y actividad.
- Documentación en línea.

Si no se muestran las opciones de RADIUS, debe añadirse el cliente AAA que usa el protocolo RADIUS.

El cliente AAA debe ser agregado al servidor y se deben especificar la dirección IP y la clave de cifrado. Según la versión de ACS los pasos para la configuración del cliente AAA pueden variar:

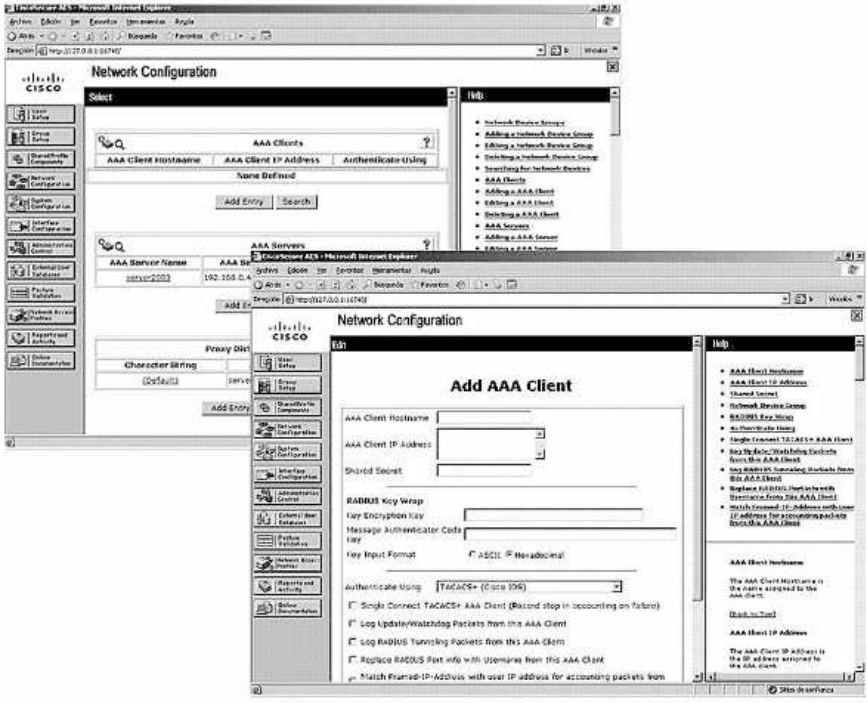
- Desde **Network Configuration** para versiones 4.x o desde **Network Resources** para versiones 5.x seleccione **Add Entry**.

- Ingrese el nombre de host del cliente y la dirección IP en los campos **AAA Client Hostname** y **Client IP Address** respectivamente.

- Ingrese la clave secreta que el cliente utiliza para el cifrado en el campo **Shared Secret**.

- Elija el protocolo AAA apropiado de la lista desplegable **Authenticate Using**.

- Complete los otros parámetros según se requiera y finalice con **Submit and Apply**.

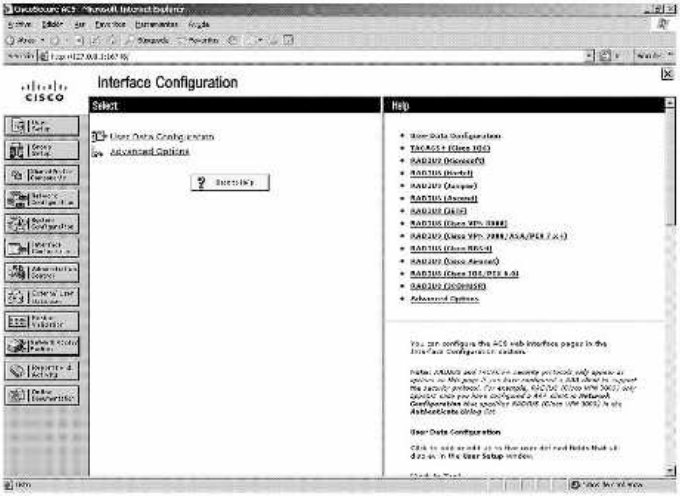


Las opciones disponibles en el botón **Interface configuration** permiten al administrador controlar el despliegue de las opciones en la interfaz del usuario. Las opciones específicas desplegadas dependen de si se han agregado clientes TACACS+ o RADIUS al servidor y pueden ser:

- User Data Configuration.

- TACACS+ (Cisco IOS).

- RADIUS (Microsoft).
- RADIUS (Ascend).
- RADIUS (IETF).
- RADIUS (IOS/PIX).
- Advanced Options.



El ACS puede ser configurado para reenviar la autenticación de los usuarios a una o más bases de datos externas. Si se configura el ACS para que utilice múltiples bases de datos de usuarios con nombres de usuario comunes almacenados en cada una, preste especial atención a las configuraciones de las bases de datos. La primera base de datos que coincida con las credenciales de autenticación del usuario será la única que el ACS utilizará para ese usuario. Por esta razón, es aconsejable que solo exista una instancia de un nombre de usuario en todas las bases de datos externas.

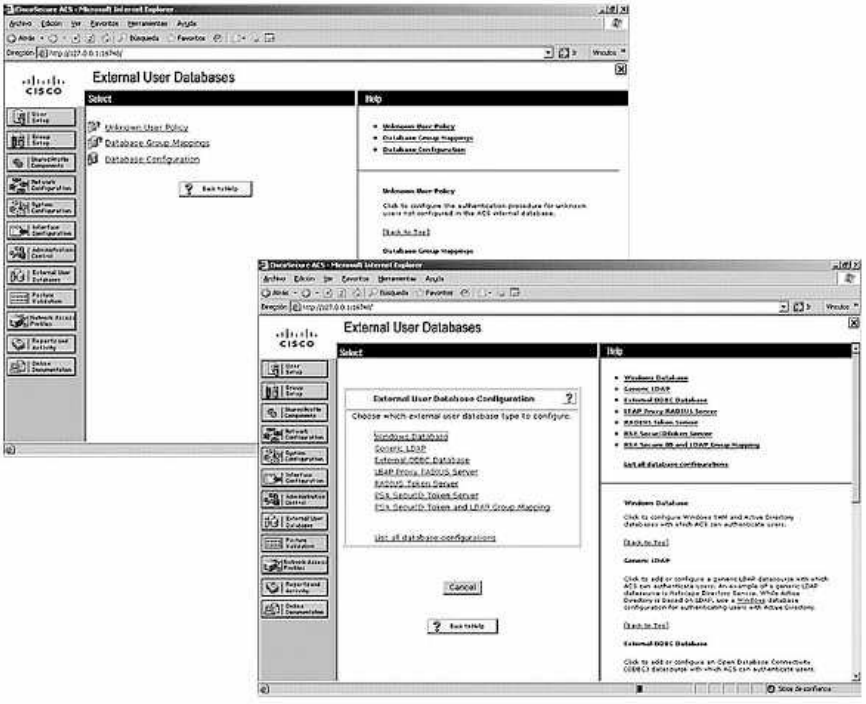
Desde el botón **External User Databases** pueden configurarse las bases de datos externas. Donde:

- **Unknown User Policy**: configura el procedimiento de autenticación para usuarios que no están en la base de datos del ACS.

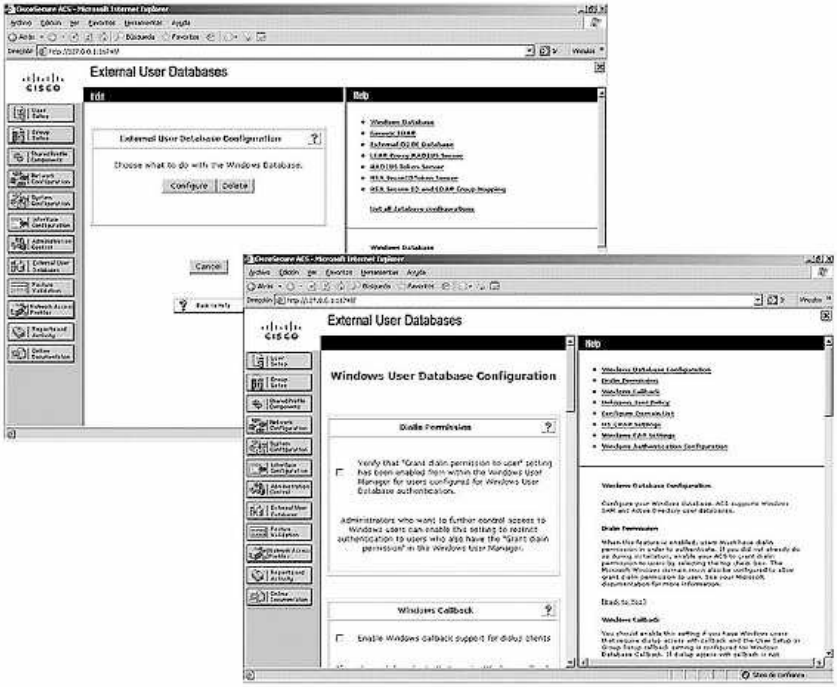
- **Database Group Mappings**: configura qué privilegios de usuario heredan los usuarios de bases de datos externas cuando el ACS los autentica.

- **Database Configuration**: define los servidores externos con los que trabajará el ACS.

Para utilizar la base de datos de Windows como base de datos externa, seleccione **Database Configuration** y luego **Windows Database**. Aparecerá el panel **Windows External User Database Configuration**.



Si se requiere mayor control sobre quién puede autenticarse a la red, se puede configurar la opción de permiso de **Dialin**.

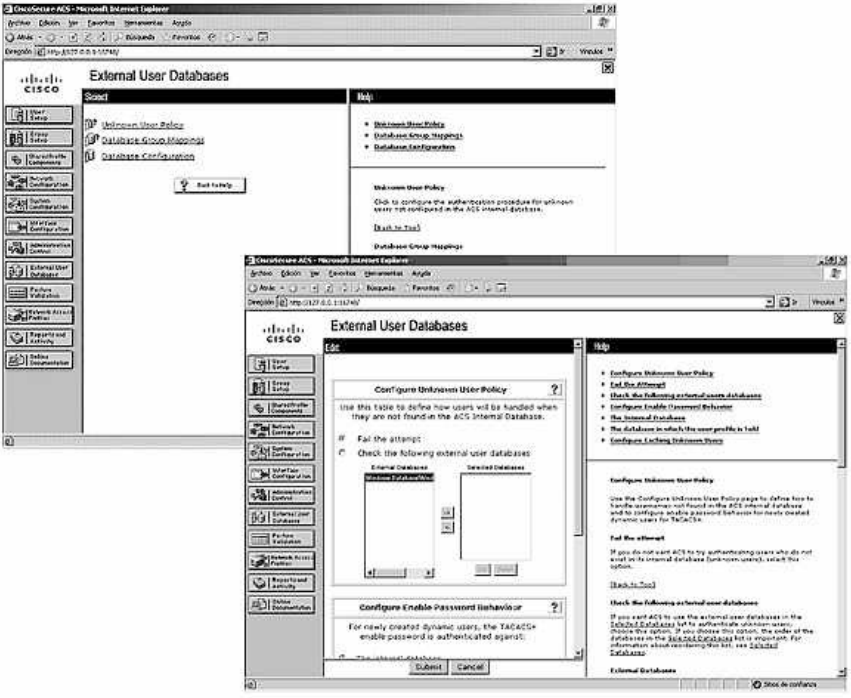


A partir de que el ACS se ha configurado para comunicarse con una base de datos de usuarios externa, puede configurarse para autenticar usuarios con dicha base de datos de usuarios externa de dos maneras:

- Por medio de la asignación específica de usuarios, autenticando a usuarios específicos con una base de datos externa.

- Por medio de una política de usuarios desconocidos, utilizando una base de datos externa para autenticar a los usuarios que no se hallan en la base de datos de usuario del ACS. Este método no requiere que los administradores definan usuarios en la base de datos del ACS.

Desde **External User Databases / Unknown User Policy** habilite la política de usuarios desconocidos desde la casilla correspondiente en la sección **Unknown User Policy**. Complete los datos requeridos y finalice con **Submit**.



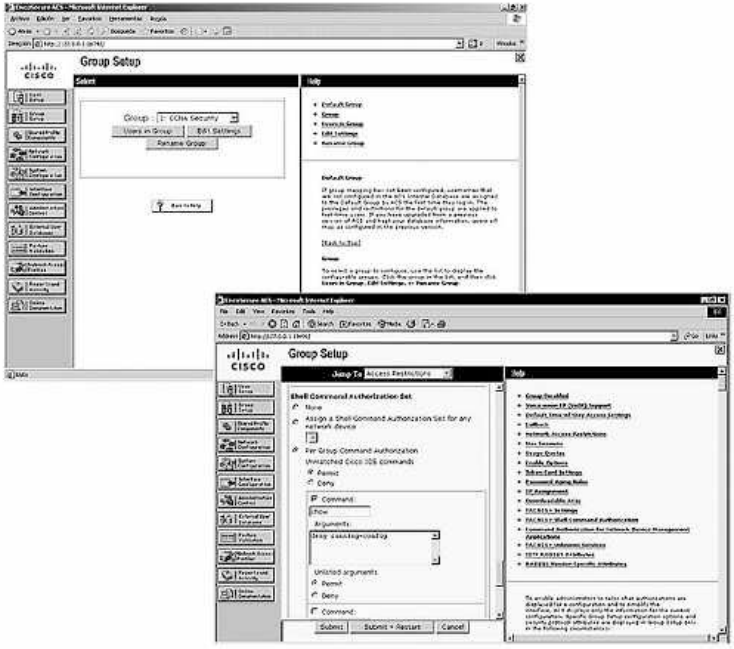
Cuando un usuario es autenticado por medio de una base de datos externa, la autorización que toma lugar la determina el ACS. Este mecanismo debe tener en cuenta que los usuarios que son autenticados por un servidor Windows pueden requerir una autorización diferente a la de los usuarios autenticados por un servidor LDAP.

La necesidad de autorizaciones diferentes hace necesario ubicar a los usuarios autenticados por el servidor Windows en un grupo y a los usuarios autenticados por el servidor LDAP en otro grupo. Para hacer esto se utiliza el mapeo de grupos de bases de datos.

Una de las opciones que puede configurarse en un grupo es la autorización de comandos por grupo, de tal manera que puede permitirse al grupo ejecutar o no algún comando determinado.

- Seleccione **Group Setup**.
- En la casilla **Group** seleccione el grupo a editar y luego **Edit Settings**.

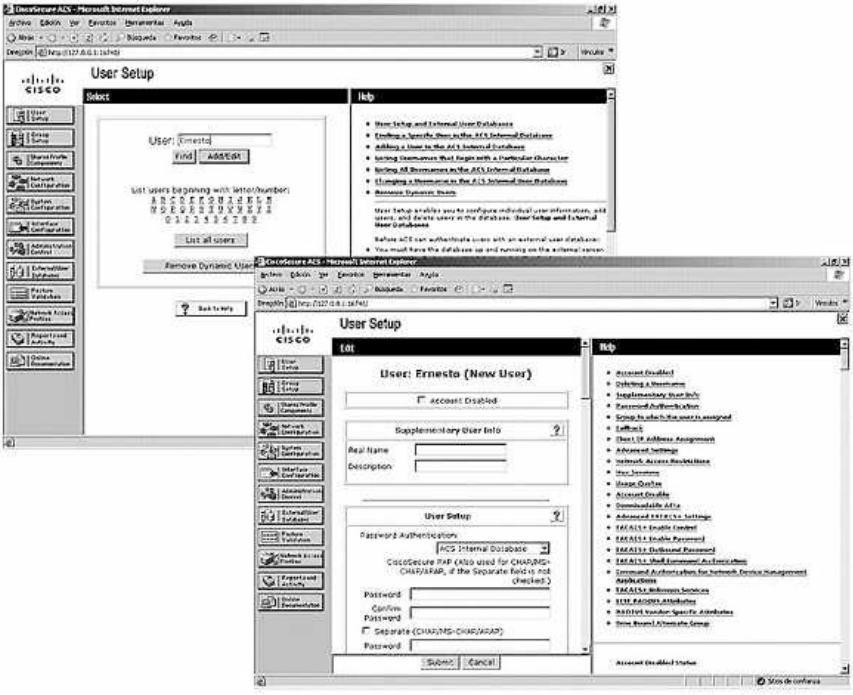
- Marque **Permit** en la opción **Unmatched Cisco IOS commands**.
- En la casilla de texto **Command** ingrese el comando.
- En la opción **Unlisted Arguments**, marque en **Permit**.



Para agregar una cuenta de usuario y configurar el acceso del usuario:

- Seleccione **User Setup** en la página de inicio.
- Ingrese un nombre de usuario en el campo **User** y luego **Add/Edit**.
- Añada los datos en los campos para definir la cuenta del usuario. Los campos necesarios son los campos de contraseña del usuario, **TACACS+ enable control**, **TACACS+ enable password** y comandos autorizados de shell de TACACS+.
- Finalice con **Submit**.

Si hay propiedades del usuario que son necesarias y no puede ver, verifique la configuración de interfaz desde **Interface Configuration / User Data Configuration**.



4.4 CONFIGURACIÓN DE AUTENTICACIÓN BASADA EN SERVIDOR

AAA basado en servidor debe identificar los servidores TACACS+ y RADIUS que el servicio AAA debe consultar al autenticar y autorizar usuarios.

Habilite AAA globalmente para permitir el uso de todos los elementos AAA. Este paso es un prerrequisito de todos los otros comandos AAA.

```
Router(config)# aaa authentication type {default | list-name}
method1 [method2...]
```

4.4.1 Configuración de RADIUS y TACACS+ con CLI

El comando **radius-server host** se utiliza para indicar el servidor RADIUS. El comando tiene varias opciones; la sintaxis completa es la siguiente:

```
Router(config)# radius-server host {hostname | ip-address} [auth-
port port-number] [acct-port port-number] [timeout seconds]
[retransmit retries] [key string] [alias{hostname | ip-address}]
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
hostname	Especifica un nombre para el servidor RADIUS.
ip-address	Especifica una dirección IP para el servidor RADIUS.
auth-port	Especifica el puerto UDP para las solicitudes de autenticación.
port-number	Número de puerto para las autenticaciones (0 no se utiliza; por defecto 1645).
acct-port	Especifica el puerto UDP para las solicitudes de auditoría.
port-number	Número de puerto para las auditorías (0 no se utiliza; por defecto 1646).
timeout	Especifica el valor en segundos que el router espera por la respuesta del servidor RADIUS antes de reenviar una petición.
seconds	Especifica el valor del timeout.
retransmit	Especifica el número de veces que una petición al servidor RADIUS es retransmitida.
retries	Especifica el valor de la retransmisión.
key	Especifica que una clave para autenticar y encriptar será utilizada entre el router y el servidor RADIUS.
string	Especifica el valor de la clave.
alias	Especifica hasta 8 alias que se pueden dar a un servidor RADIUS.

El comando **tacacs-server host** se utiliza para indicar el servidor TACACS. El comando tiene varias opciones, vemos a continuación la sintaxis completa:

```
Router(config)# tacacs-server host {hostname | ip-address} [key
string] [nat] [port [integer]] [single-connection] [timeout
[integer]]

Router(config)# no tacacs-server host {host-name | host-ip-address}
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
hostname	Nombre del servidor TACACS+.
ip-address	Dirección IP del servidor TACACS+.
key	Especifica que una clave para autenticar y encriptar será utilizada entre el router y el servidor TACACS+.
string	Especifica el valor de la clave.
nat	Dirección NAT del cliente que es enviada al servidor TACACS+.
port	Especifica el número de puerto TACACS+ (por defecto = 49).
integer	Especifica el valor del número de puerto TACACS+.
single-connection	Mantiene una sola conexión abierta.
timeout	Especifica un valor de timeout.
integer	Especifica en segundos el valor del timeout.

Los comandos **radius-server key** y **tacacs-server key** cumplen la misma función de configuración de la clave de autenticación para la comunicación entre el router y el servidor.

```
Router(config)# [no] radius-server key {0 string | 7 string |
string}

Router(config)# [no] tacacs-server key {0 string | 7 string |
string}
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
`0 string`	La clave se introduce sin encriptación.
`7 string`	La clave se introduce con encriptación.
`string`	La clave se introduce sin encriptación.

4.5 CONFIGURACIÓN DE TACACS+ CON CCP

Para la configuración de TACACS+ con CCP será necesario especificar una lista de servidores Cisco Secure ACS disponibles:

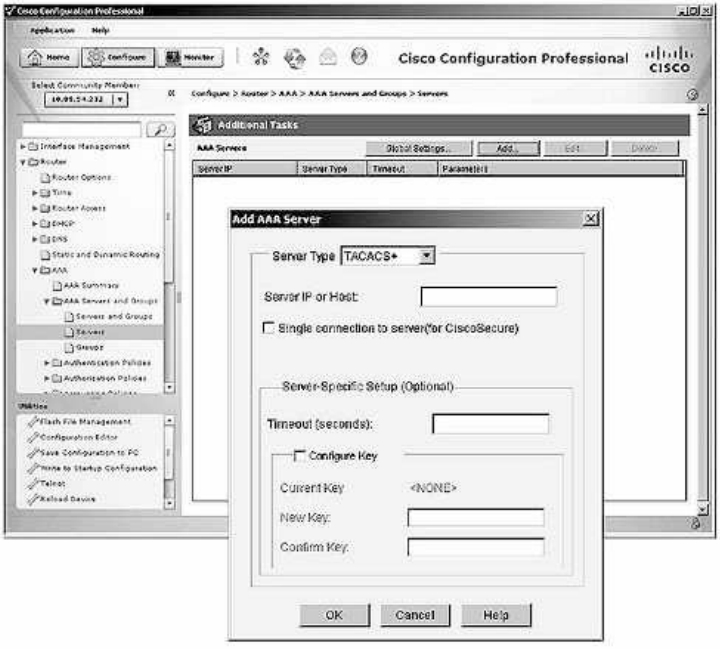
- Desde la página principal de CCP seleccione **Configure** / **Router** / **AAA** / **AAA Servers and Groups** / **Servers** y luego **Add**.

- En la siguiente ventana, en **Server Type**, elija **TACACS+**, complete los datos del nombre o dirección IP del servidor. Marque la casilla **Single connection to server** para que el router mantenga una única conexión abierta con el servidor TACACS+ en lugar de abrir y cerrar una conexión TCP cada vez que se comunica con el servidor.

- El valor opcional en el campo **Timeout** determina el tiempo que el router espera una respuesta de este servidor antes de continuar con el siguiente servidor de la lista de grupos. Por defecto es de 5 segundos.

- Active la casilla **Configure Key** e introduzca la clave que se utilizará para cifrar el tráfico entre el router y el servidor. Si esta opción no está activada, el router usa el valor que se ha configurado en la ventana de servidores AAA en la configuración global.

- Finalice con **Ok**.



Después de habilitar AAA y configurar los servidores TACACS+, el router puede ser configurado para usar el servidor Cisco Secure ACS para autenticar el acceso de usuarios al router. La lista de métodos por defecto se aplica automáticamente a todas las interfaces y las líneas, excepto aquellos que tienen una lista de métodos definidos explícitamente por el usuario.

- Desde la página de inicio de CCP seleccione **Configure** / **Router** / **AAA** / **Authentication Policies** / **Login** y luego **Add**.

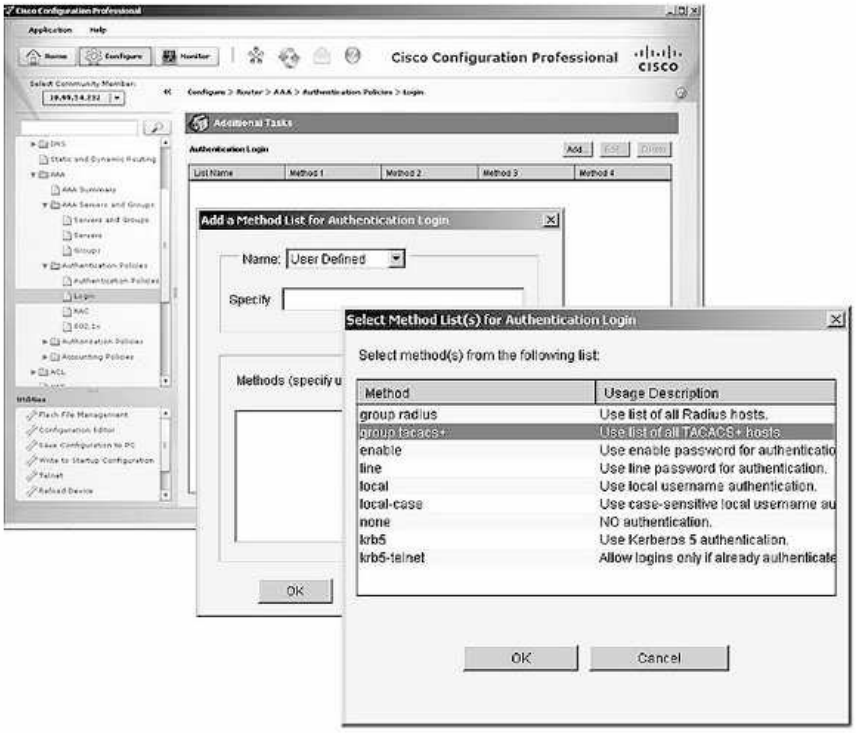
- Para crear un nuevo método de autenticación elija **User Defined** desde la lista.

- Introduzca el método de autenticación de inicio de sesión en el campo **Specify**.

- Desde **Add**, defina los métodos que utilizarán esta política. Elija **TACACS+** desde el grupo de listas de métodos.

- Acepte con **OK** para agregar TACACS+.

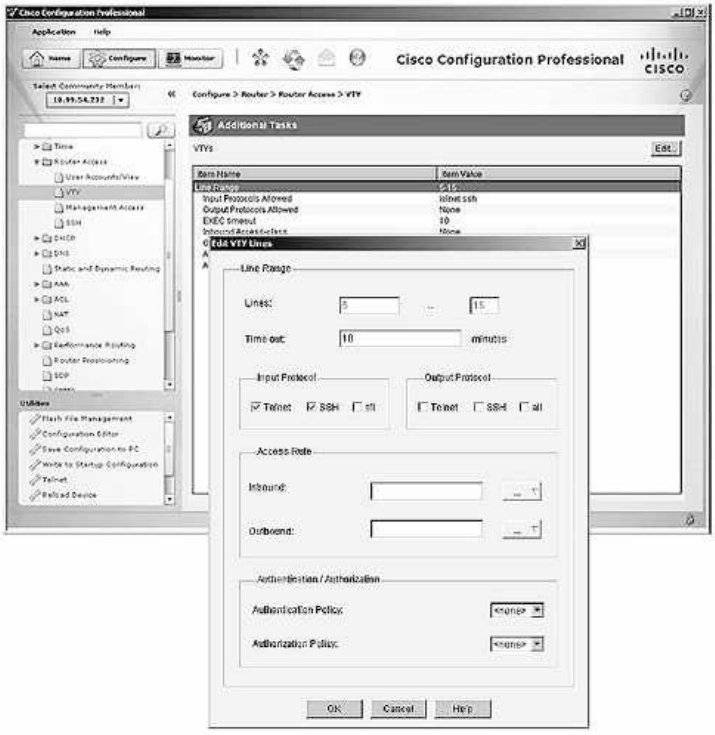
- Para agregar un método de respaldo a esta política seleccione **Add**.
- Elija **enable** desde el grupo de listas de métodos. De esta forma, la enable password será la contraseña de inicio de sesión para la autenticación de backup.
- Acepte desde **OK** para volver a la lista de métodos.
- Finalice con **Deliver**.



Finalmente se aplicarán las listas a las líneas y las interfaces en el router.

- Seleccione **Configure / Router / Router Access / VTY**.
- Desde la ventana de líneas vty seleccione **Edit** para realizar cambios.

- Seleccione la línea y desde la casilla **Authentication Policy** elija las políticas de autenticación que se aplican.



EJEMPLO:

En la siguiente sintaxis se muestra una configuración de AAA utilizando RADIUS:

```
Router(config)# aaa new-model
Router(config)# radius-server host 10.10.1.5
Router(config)# radius-server key TheRADIUSServerKey
Router(config)# username root password MySecretPassword
Router(config)# aaa authentication ppp mydiallist radius local
Router(config)# aaa authorization network radius local
Router(config)# aaa accounting network mynetwork start-stop group
radius
```

En la siguiente sintaxis se muestra una configuración de AAA utilizando TACACS+:

```
Router(config)# aaa new-model
Router(config)# tacacs-server host 10.10.1.5
Router(config)# tacacs-server key TheTacacsServerKey
Router(config)# username root password MySecretPassword
Router(config)# aaa authentication ppp mydiallist tacacs+ local
Router(config)# aaa authorization commands 15 tacacs+ if-
authenticated none
Router(config)# aaa accounting network start-stop tacacs+
```

4.6 RESOLUCIÓN DE FALLOS EN AAA

Existen varios comandos **debug** que se pueden usar para este propósito, que, recuerde que siempre que se utilicen con comandos **debug**, ha de hacerse con cuidado y con la plena seguridad de no saturar el router. La siguiente tabla muestra los principales comandos **debug**:

Comando	Descripción
`debug aaa authentication`	Muestra información sobre los eventos de autenticación.
`debug aaa authorization`	Muestra información sobre los eventos de autorización.
`debug aaa accounting`	Muestra información sobre los eventos de auditoría.
`debug radius`	Muestra información relativa a RADIUS.
`debug tacacs`	Muestra información relativa a TACACS+.

Los siguientes son ejemplos de algunos de los comandos **debug** más utilizados:

```
Router#debug aaa authentication
4:50:12: AAA/AUTHEN: create_user user='' ruser='' port='tty19'
rem_addr='10.10.1.1'
authen_type=1 service=1 priv=1
4:32:10: AAA/AUTHEN/START (0): port='tty19' list='' action=LOGIN
service=LOGIN
4:32:10: AAA/AUTHEN/START (0): using "default" list
4:32:10: AAA/AUTHEN/START (42987541): Method=TACACS+
4:32:10: TAC+ (42987541): received authen response status = GETUSER
```

```
4:32:10: AAA/AUTHEN (42987541): status = GETUSER
4:32:13: AAA/AUTHEN/CONT (42987541): continue_login
4:32:13: AAA/AUTHEN (42987541): status = GETUSER
4:32:13: AAA/AUTHEN (42987541): Method=TACACS+
4:32:13: TAC+: send AUTHEN/CONT packet
4:32:13: TAC+ (42987541): received authen response status = GETPASS
4:32:13: AAA/AUTHEN (42987541): status = GETPASS
4:32:18: AAA/AUTHEN/CONT (42987541): continue_login
4:32:18: AAA/AUTHEN (42987541): status = GETPASS
4:32:18: AAA/AUTHEN (42987541): Method=TACACS+
4:32:18: TAC+: send AUTHEN/CONT packet
4:32:18: TAC+ (42987541): received authen response status = PASS
4:32:18: AAA/AUTHEN (42987541): status = PASS
Router#debug aaa authorization
5:18:43: AAA/AUTHOR (0): user='carrel'
5:18:43: AAA/AUTHOR (0): send AV service=shell
5:18:43: AAA/AUTHOR (0): send AV cmd*
5:18:43: AAA/AUTHOR (754913891): Method=TACACS+
5:18:43: AAA/AUTHOR/TAC+ (754913891): user=carrel
5:18:43: AAA/AUTHOR/TAC+ (754913891): send AV service=shell
5:18:43: AAA/AUTHOR/TAC+ (754913891): send AV cmd*
5:18:43: AAA/AUTHOR (754913891): Post authorization status = FAIL
Router#debug radius brief
RADIUS protocol debugging is on
RADIUS packet hex dump debugging is off
RADIUS protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 6 10.10.10.1:1824,
Accounting-Request,
len 358
10:05:21: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to
5555551212
10:05:26: RADIUS: Retransmit id 6
10:05:31: RADIUS: Tried all servers.
10:05:31: RADIUS: No valid server found. Trying any viable server
10:05:31: RADIUS: Tried all servers.
10:05:31: RADIUS: No response for id 7
10:05:31: RADIUS: Initial Transmit ISDN 0:D:23 id 8 10.0.0.0:1823,
Access-Request, len 171
10:05:36: RADIUS: Retransmit id 8
10:05:36: RADIUS: Received from id 8 1.7.157.1:1823, Access-Accept,
len 115
10:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from
5555551212, call
lasted 26 seconds
10:05:47: RADIUS: Initial Transmit ISDN 0:D:23 id 9 10.0.0.1:1824,
Accounting-Request, len
775
10:05:47: RADIUS: Received from id 9 1.7.157.1:1824, Accounting-
response, len 20
```

4.7 CONFIGURACIÓN DE AUTORIZACIÓN BASADA EN SERVIDOR

La autorización se ocupa de permitir o prohibir el acceso a ciertas áreas y programas de la red a los usuarios autenticados. Puede configurarse el router para no permitir al usuario realizar ciertas funciones luego de una autenticación exitosa. La autorización puede configurarse tanto para el modo carácter como para el modo paquete. Tenga en consideración que RADIUS no separa los procesos de autenticación y autorización mientras que TACACS+ sí lo hace.

El comando **aaa authorization** permite definir el grado de acceso de los usuarios. Cuando la autorización AAA no está habilitada, se permite acceso sin restricciones a todos los usuarios. Luego de que inicia la autenticación, por defecto, no se permite acceso a nadie. El comando completo para su configuración es el siguiente:

```
Router(config)# [no] aaa authorization {network | exec | commands
level | reverse-access} {default | listname}[method1 [method2...]]
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
`network`	Ejecuta autorización para todos los servicios de red que lo pidan.
`exec`	Ejecuta autorización para ver si a un usuario le está permitido usar una *Shell exec*.
`commands`	Ejecuta autorización para todos los comandos al nivel especificado.
`level`	Nivel del comando específico que ha de ser autorizado.
`reverse-access`	Ejecuta autorización para conexiones de acceso reverso como por ejemplo telnet reverso.
`default`	Utiliza los métodos de autenticación por defecto cuando un usuario inicia sesión.
`list-name`	Nombre para una lista de métodos de autenticación.

method1 [method2...]	Al menos uno de los siguientes métodos es usado: • **If-needed**: no autentica si el usuario ya está autenticado. • **Krb5**: usa Kerberos 5. • **Local**: usa la base de datos local. • **None**: no hay autenticación. • **Radius**: usa un servidor RADIUS. • **Tacacs+**: usa un servidor TACACS+.

El comando **aaa authentication PPP** especifica los métodos de autenticación para usar en interfaces seriales PPP. La siguiente sintaxis describe el comando completo:

```
Router(config)# [no] aaa authentication ppp {default | list-name}
method1 [method2...]
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
`default`	Utiliza los métodos de autenticación por defecto cuando un usuario inicia sesión.
`list-name`	Nombre para una lista de métodos de autenticación.
`method1 [method2...]`	Al menos uno de los siguientes métodos es utilizado: • **If-needed**: no autentica si el usuario ya está autenticado. • **Krb5**: usa Kerberos 5. • **Local**: usa la base de datos local. • **None**: no hay autenticación. • **Radius**: usa un servidor RADIUS. • **Tacacs+**: usa un servidor TACACS+

4.7.1 Configuración de autorización con CCP

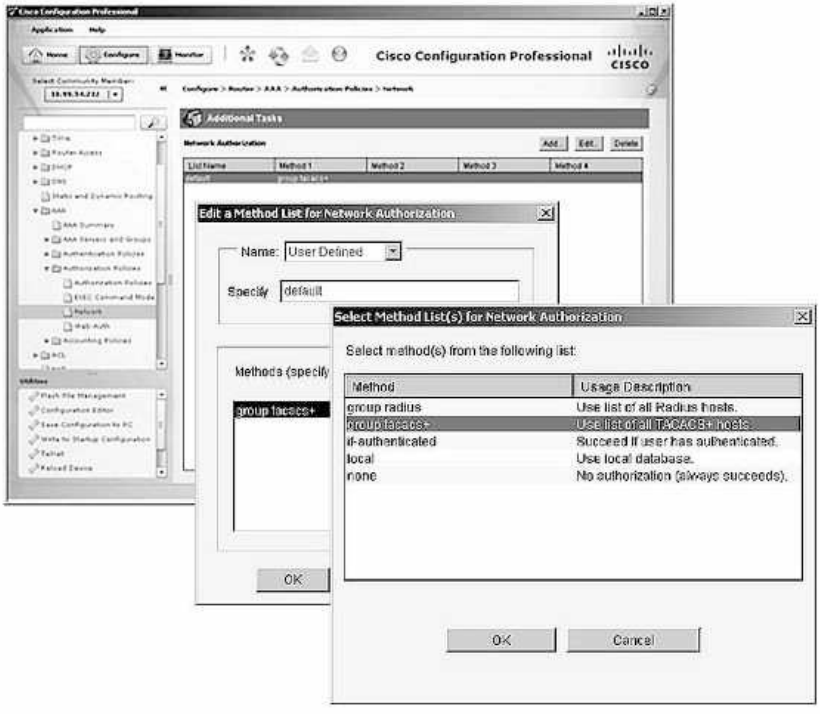
El router puede configurarse para que utilice un servidor Cisco Secure ACS para la autorización, debe crearse una lista de métodos de autorización definida por el usuario o editarse la lista de métodos de autorización por defecto. La lista de métodos de autorización por defecto se aplica automáticamente a todas las interfaces excepto a aquellas que tengan una lista de métodos de autorización definida por el usuario aplicada explícitamente. Esta lista invalida la lista de métodos de autorización por defecto.

CCP puede ser utilizarse para configurar la lista de métodos de autorización por defecto para el acceso de modo carácter (*exec*):

- Desde la página de inicio de CCP seleccione **Configure** / **Router** / **AAA** / **Authorization Policies** / **EXEC Command Mode** y luego **Edit**.
- Desde **Add** defina el método que esta política utilizará.
- Desde la ventana de **Select Method List(s)** seleccione de la lista **group tacacs+**.
- Confirme con **OK**, regresa a la ventana anterior.
- Finalice con **OK**.

También se puede utilizar CCP para configurar la lista de métodos de autorización por defecto para el modo paquete (*network*):

- Desde la página de inicio de CCP, seleccione **Configure** / **Router** / **AAA** / **Authorization Policies** / **Network** y luego **Add**.
- Desde la ventana **Add a Method List for Network Authorization** seleccione **Default**.
- Desde **Add** defina el método que esta política utilizará.
- Desde la ventana de **Select Method List(s)** seleccione de la lista **group tacacs+**.
- Confirme con **OK**, regresa a la ventana anterior.
- Finalice con **OK**.



En ambos casos lo que se verá en la CLI será:

```
aaa authorization exec default group tacacs+
aaa authorization network default group tacacs+
```

4.8 REGISTRO DE AUDITORÍA AAA BASADA EN SERVIDOR

El Cisco Secure ACS sirve como repositorio central de la información de registros de auditoría, esencialmente monitorizando los eventos que toman lugar en la red. Muchas empresas deben mantener un registro de los recursos que los individuos o grupos utilizan.

El registro de auditoría de AAA proporciona mecanismos para registrar los datos obtenidos en una base de datos y producir reportes sobre los mismos.

Cada sesión establecida a través del Cisco Secure ACS puede ser monitorizada y almacenada en el servidor. Esta información recopilada puede resultar de gran ayuda en la administración, las auditorías de seguridad, el planeamiento de la capacidad y el cobro de servicios por uso de la red.

De manera semejante a las listas de métodos de autenticación y autorización, las listas de métodos de registros de auditoría definen la manera en que se realizan los registros y la secuencia que deben seguir los métodos que se utilizan. Una vez habilitados, la lista de métodos del registro de auditoría por defecto se aplica automáticamente a todas las interfaces, excepto aquellas que tienen una lista nombrada de métodos de registro de auditoría explícitamente definida.

4.8.1 Configuración del registro de auditoría

El **comando aaa accounting**, permite guardar un registro con los comandos que ha utilizado cada usuario.

El comando completo es el siguiente:

```
Router(config)# [no] aaa accounting {auth-proxy | system | network |
exec | connection | commands level} {default | list-name} [vrf vrf-
name] {start-stop | stop-only | none} [broadcast] group group-name
```

La siguiente tabla describe los parámetros:

Parámetro	Descripción
`auth-proxy`	Lleva a cabo auditoría de todos los eventos de autenticación de proxy.
`system`	Lleva a cabo auditoría de todos los eventos del sistema no asociados con usuarios.
`network`	Lleva a cabo auditoría de todas las peticiones relativas a la red.
`exec`	Lleva a cabo auditoría de todas las sesiones de *Shell exec*.
`connection`	Lleva a cabo auditoría de todas las conexiones de salida desde el servidor de acceso de la red.
`commands level`	Lleva a cabo auditoría de todos los comandos al nivel especificado.
`default`	Utiliza los métodos de auditoría que vienen a continuación.
`Option`	Descripción.
`list-name`	Cadena de caracteres usada para nombrar la lista, las opciones son: • **Group radius**: lista de servidores RADIUS. • **Group tacacs**: lista de servidores TACACS+. • **Group group-name**: un subconjunto de servidores RADIUS o TACACS+.
`vrf vrf-name`	Especifica una configuración para VRF.
`start-stop`	Envía un evento **start** cuando el proceso inicia y envía un evento stop cuando el proceso finaliza.
`stop-only`	Envía un evento **stop** cuando el proceso finaliza.
`broadcast`	Habilita el envío de registros de auditoría a múltiples servidores AAA.
`group group-name`	Cadena de caracteres usada para nombrar la lista, las opciones son: • **Group radius**: lista de servidores RADIUS. • **Group tacacs**: lista de servidores TACACS+. • **Group group-name**: un subconjunto de servidores RADIUS o TACACS+.

4.9 FUNDAMENTOS PARA EL EXAMEN

- Estudie con detenimiento la función de AAA, que significa "autenticación, autorización y auditoría".
- Practique las configuraciones de AAA con CCP y con la CLI.
- Tenga presente el funcionamiento y las diferencias entre la autenticación local y la autenticación basada en servidor.
- Estudie con detenimiento la funcionalidad y las configuraciones de los protocolos RADIUS y TACACS+.
- Instale y pruebe las funcionalidades de Cisco Secure ACS.
- Realice prácticas de configuración de AAA basada en servidor con CLI y con CCP.
- Estudie las configuraciones de registro de auditoría.

Capítulo 5

SEGURIDAD DE CAPA 2

5.1 SEGURIDAD DE LAN

La infraestructura de una red corporativa es un área importante para enfocar la seguridad de la LAN. La mitigación de ataques es parte de la seguridad de una LAN. Estos ataques incluyen la falsificación de direcciones MAC (spoofing), manipulación de STP, desbordamiento de la tabla de direcciones MAC, tormentas de LAN y ataques de VLAN. La seguridad de terminales incluye asegurar tanto los dispositivos de infraestructura de red de la LAN como los dispositivos finales, las estaciones de trabajo, servidores, teléfonos IP, puntos de acceso, dispositivos de la red de área de almacenamiento, etc.

Otro elemento a asegurar en la infraestructura de red son los dispositivos no terminales de la LAN, como pueden ser los switches, dispositivos inalámbricos, dispositivos de telefonía IP y dispositivos de almacenamiento.

Las configuraciones de seguridad de capa 2 incluyen habilitar entre otras cosas la seguridad de puertos, BPDU Guard, Root Guard, control de tormentas y PVLAN.

5.1.1 Seguridad en los dispositivos finales

La seguridad en los dispositivos finales comienza con la protección contra virus, troyanos, gusanos y otras amenazas. Los sistemas operativos proporcionan solo servicios básicos de seguridad. Los sistemas operativos proveen a cada proceso una identidad y ciertos privilegios. Cuando un atacante tiene la opción de comunicarse directamente con la aplicación objetivo, dicha aplicación debe estar protegida de forma adecuada. Es posible modificar maliciosamente los privilegios durante la operación de un programa o durante una misma sesión de usuario.

Los nuevos dispositivos de red tales como los iPhones, BlackBerrys o netbooks no son buenos candidatos para la instalación de los antivirus tradicionales. Se han diseñado para ser rápidos, ligeros y portátiles. Además, crean fronteras indefinidas de la red, con constantes entradas y salidas, es decir, que no existe un perímetro definido de la red. El desafío es cómo permitir que estos dispositivos heterogéneos puedan conectarse a recursos de la empresa de forma segura. Para abordar estas mismas cuestiones, Cisco creó **SecureX architecture**.

5.1.2 Dispositivos Cisco de seguridad para terminales

Cisco Systems ha diseñado soluciones robustas para asegurar los dispositivos terminales de la red:

- **IronPort**: son dispositivos perimetrales de seguridad que dan protección contra las dos principales amenazas de Internet para los terminales: la seguridad del correo electrónico y la seguridad en sitios web. En este caso, los terminales son asegurados por dispositivos que funcionan en el perímetro de la red.
    - **C-Series**: es un dispositivo de seguridad de correo electrónico para el control de virus y spam.
    - **S-Series**: es un dispositivo de seguridad web para el filtrado de spyware, filtrado de URL y antimalware.
    - **M-Series**: es un dispositivo de administración de seguridad, complementa los dispositivos de seguridad de correo electrónico y servidores web mediante la administración y monitorización de las políticas de la organización, configurando y auditando información.

- **NAC** (*Network Admission Control*): utiliza la infraestructura de la red para implementar la política de seguridad en todos los dispositivos que requieran acceso a recursos de red. Con NAC se pueden autenticar, autorizar, evaluar y corregir a usuarios y máquinas previo a su acceso a la red. NAC identifica si los dispositivos de red cumplen o no con las políticas de seguridad, y repara cualquier vulnerabilidad antes de permitir su acceso a la red. NAC provee cuatro características importantes para mantener la estabilidad de la red:

  - Autenticación y autorización.
  - Evaluación del cumplimiento de las políticas de red en los dispositivos entrantes (evaluación de posturas).
  - Cuarentena de sistemas que no cumplan con las políticas.
  - Resolución de los problemas en los sistemas que no cumplan con las políticas de la red.

Los productos Cisco NAC se dividen en dos categorías:

- **NAC Framework**: utiliza la infraestructura de red Cisco existente y software de terceros para implementar el cumplimiento de la política de seguridad en todos los terminales. Es apropiado para cuando se requiere una solución consistente de LAN, WAN, wireless, extranet y acceso remoto, que se integre en la seguridad existente y repare software, herramientas y procesos. Las cuatro funciones de NAC pueden ser provistas por diferentes dispositivos o por uno solo.

- **Cisco NAC Appliance**: concentra las cuatro funciones NAC en un mismo dispositivo y provee una solución completa para el control del acceso a la red. Esta solución resulta apropiada para redes de mediana escala que requieran una solución completa e independiente y necesiten un rastreo simple e integrado de las actualizaciones del sistema operativo, del antivirus y de las vulnerabilidades. No es necesaria una red Cisco para su funcionamiento. El dispositivo Cisco NAC Appliance consolida todas las funciones del framework NAC en un mismo dispositivo de red, cumpliendo con todos los mismos roles.

Los siguientes componentes principales de Cisco NAC Appliance ejecutan estas tareas:

- **Cisco NAC Appliance Server** (NAS): dispositivo utilizado para realizar el control de acceso a la red implementado en capa 2 o 3, como un gateway virtual o como un gateway IP real, y puede ser instalado en forma central o distribuida.

- **Cisco NAC Appliance Manager** (NAM): interfaz centralizada de administración, utilizada por el personal de soporte técnico. Los administradores pueden utilizarlo para establecer roles de usuarios, verificaciones de conformidad y requisitos de solución de problemas. Provee una interfaz basada en web para la creación de políticas de seguridad y administración de usuarios online. Puede actuar como un proxy de autenticación para autenticar servidores internos.

- **Cisco NAC Appliance Agent** (NAA): software cliente que facilita la administración de la red. Este agente simple de solo lectura se ejecuta en una terminal. Realiza una inspección profunda del perfil de seguridad de la máquina local, analizando sus configuraciones de registro, servicios y archivos. Permite corregir algún problema forzando la actualización de seguridad en el host.

5.2 SEGURIDAD EN CAPA 2

La capa 2 es el eslabón más débil para las capas superiores del modelo OSI, ya que si se ve comprometida, los hackers pueden trabajar luego hacia niveles superiores. Es importante recordar que los ataques de capa 2 suelen requerir acceso desde el interior, ya sea de un empleado o un visitante. Desde la perspectiva de la seguridad, la independencia de la capa 2 crea un desafío, ya que si la capa se ve comprometida, las otras capas no se enteran de este hecho, por lo que también quedan expuestas.

5.2.1 Ataques comunes de capa 2

Los siguientes son los ataques más comunes a nivel de capa 2.

- **Ataques de falsificación de direcciones MAC**: estos ocurren cuando un atacante altera la dirección MAC de su host de forma tal que coincida con la dirección MAC de otro host conocido. El host atacante envía entonces una trama a través de la red con la nueva dirección MAC configurada. Cuando el switch recibe la trama, examina su

dirección MAC de origen. El switch sobrescribe la entrada correspondiente a dicha dirección MAC, asignándole un nuevo puerto. A partir de ese momento, las tramas destinadas al host original son redirigidas inadvertidamente al host atacante.

- **Ataques por desbordamiento de la tabla de direcciones MAC**: las tablas de direcciones MAC tienen un tamaño limitado. La inundación MAC se aprovecha de esta limitación bombardeando al switch con direcciones MAC falsas, hasta llenar por completo la tabla de direcciones MAC en la CAM. Si se ingresan las suficientes entradas en dicha tabla antes de que expiren las más antiguas, la tabla se llena al punto en que no pueden aceptarse nuevas direcciones MAC. Cuando esto ocurre, el switch comienza a inundar todos sus puertos con todo el tráfico entrante, ya que no puede aprender más direcciones MAC legítimas. El switch funcionará como un hub dentro de la misma VLAN. Como resultado, el atacante podrá ver todas las tramas enviadas.

- **Ataques de manipulación STP**: para llevar adelante este ataque, el host atacante realiza un broadcast de BPDU con cambios en la topología y configuración del STP, forzando un nuevo cálculo a partir de una menor prioridad. Todo el tráfico del dominio conmutado inmediato atraviesa entonces el puente raíz falso, obteniendo información de una variedad de tramas que le resultarían inaccesibles de otra forma.

- **Ataques de tormenta de LAN**: sucede cuando los paquetes inundan la LAN, creando un exceso de tráfico y degradando el desempeño de la red. Estas tormentas pueden ser causadas por errores en la implementación de la pila de protocolos, errores en la configuración de la red, por tormentas de broadcast o por usuarios realizando ataques DoS.

- **Ataques de VLAN**: el **VLAN hopping** permite que el tráfico de una VLAN sea visto desde otra VLAN, con ayuda del router. En un ataque básico de VLAN hopping, el atacante aprovecha la configuración automática por defecto de los enlaces troncales de la mayor parte de los switches. Entonces configura un sistema para que simule ser un switch. Esta falsificación puede efectuarse de dos maneras: emulando las encapsulaciones ISL o 802.1Q a través de un switch intruso o falsificando las señales del protocolo **DTP** (*Dynamic Trunking Protocol*). Engañando al switch para que asuma que se trata de otro

switch con un enlace troncal, el atacante puede obtener acceso a todas las VLAN permitidas en dicho enlace. Para tener éxito, este ataque requiere que el puerto se encuentre configurado con trunking automático o dinámico.

5.3 SEGURIDAD DE PUERTOS DE CAPA 2

La seguridad de puertos permite a los administradores especificar en forma estática las direcciones MAC permitidas en un puerto determinado, o permitir al switch aprender en forma dinámica un número limitado de direcciones MAC. Limitando a uno el número de direcciones MAC permitidas en un puerto, la seguridad de puerto puede ser utilizada para controlar la falsificación de MAC y el desbordamiento de la tabla de direcciones MAC.

5.3.1 Configuración de seguridad de puertos

El proceso para habilitar un puerto seguro se inicia una vez que la interfaz se ha configurado como puerto de acceso:

```
Switch(config-if)# switchport mode access
```

Hay que verificar que la interfaz no se encuentre configurada en modo **dynamic-auto** y habilitar la seguridad del puerto con el comando **switchport port-security**. Debido a que el comando completo incluye muchos parámetros opcionales que en algunos casos dependerán del tipo de IOS y del modelo del switch es recomendable la configuración paso a paso.

```
Switch(config-if)# switchport port-security [mac-address mac-address
[vlan {vlan-id | {access | voice}}]] | [mac-address sticky [mac-
address | vlan {vlan-id | {access | voice}}]] [maximum value [vlan
{vlan-list| {access | voice}}]]
```

Una vez habilitado **port-security** se debe identificar un conjunto de direcciones MAC permitidas en ese puerto configuradas explícitamente o de forma dinámica y especificar un número máximo de direcciones MAC que serán permitidas:

```
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address mac-address
Switch(config-if)#switchport port-security maximum value
```

El comando **port-security mac-address** *mac-address* puede repetirse cuantas veces sea necesario para cada dirección MAC que deba incorporarse. Si no se configura cada interfaz, aprenderá dinámicamente las direcciones MAC. El rango de MAC permitidas va desde 1 a 1.024. Las direcciones aprendidas son eliminadas si los host conectados no transmiten en un período determinado.

El rango del parámetro **maximum** *value* va desde 1 a 132. El valor por defecto es 1. Cuando este valor es mayor que el número máximo de direcciones MAC configuradas, el resto de las direcciones se aprenderán dinámicamente. Por lo tanto, se debe tener un control apropiado sobre cuántas direcciones se deben permitir.

Cuando se encuentra habilitado el modo **mac-address sticky** la interfaz agregará todas las direcciones MAC seguras que aprenda en forma dinámica hasta el máximo permitido configurado.

```
Switch(config-if)# switchport port-security mac-address sticky
```

Finalmente se debe definir cómo debe reaccionar una interfaz con seguridad de puerto habilitado si ocurre un intento de violación, para eso se utiliza el siguiente comando:

```
Switch(config-if)# switchport port-security violation {shutdown |
restrict |protect}
```

Cuando se supera el número máximo de direcciones MAC permitidas o se detecta una dirección MAC desconocida, se interpretará como una violación. El puerto del switch toma algunas de las siguientes acciones cuando ocurre una violación:

- **Shutdown**: acción por defecto, el puerto automáticamente se pone en el estado **errdisable**, dejándolo inoperable y tendrá que ser habilitado manualmente desde el modo interfaz con los comandos de interfaz **shutdown** y **no shutdown**, o utilizando el comando de recuperación **errdisable recovery cause psecure-violation** desde el modo global.

- **Restrict**: el puerto permanece activo pero los paquetes desde las direcciones MAC que están violando la restricción son eliminados. El switch continúa ejecutando el temporizador de los paquetes que están violando la condición y puede enviar un *trap* de SNMP a un servidor syslog para alertar de lo que está ocurriendo.

- **Protect**: el puerto sigue habilitado pero los paquetes de las direcciones que están violando la condición son eliminados, no queda ninguna constancia de lo que está aconteciendo en el puerto.

El envejecimiento de la seguridad de puertos puede ser utilizado para configurar los temporizadores para remover las direcciones seguras estáticas y dinámicas de un puerto.

```
Switch(config-if)# switchport port-security aging {static | time
time| type {absolute | inactivity}}
```

Es posible configurar dos tipos de envejecimiento por puerto:

- **Absolute**: las direcciones seguras del puerto son eliminadas una vez concluido el tiempo de envejecimiento.

- **Inactivity**: las direcciones seguras del puerto son eliminadas solo si se encuentran inactivas por el tiempo de envejecimiento especificado.

El resto de los parámetros son opcionales y se describen en la siguiente tabla.

Parámetro	Descripción
`vlan vlan-id`	Se utiliza solo para puertos troncales para especificar el ID de VLAN, si no se configura se utiliza la VLAN nativa.
`vlan voice`	Especifica una VLAN como VLAN de voz.
`vlan [vlan-list]`	Configura un número máximo de direcciones MAC permitidas en una VLAN para un enlace troncal.

Todos los comandos **port-security** pueden eliminarse anteponiendo un **no** al propio comando.

EJEMPLO:

La siguiente sintaxis muestra un ejemplo de configuración de seguridad de puerto en un switch Catalyst 3750 para 5 direcciones MAC:

```
Switch(config)# interface GigabitEthernet0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximun 5
```

```
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security aging time 60
```

Cuando el número máximo de direcciones MAC se excede se guarda un *log* cuya sintaxis se muestra a continuación:

```
Jun 3 17:18:41.888 EDT: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address 0000.5e00.0101 on port
GigabitEthernet0/11.
```

En el modo **shutdown**, cuando el número máximo de direcciones MAC se sobrepasa se muestra el siguiente mensaje *log* que indica que el puerto ha sido puesto en modo **errdisable**:

```
Jun 3 17:14:19.018 EDT: %PM-4-ERR_DISABLE: psecure-violation error
detected on Gi0/11, putting Gi0/11 in err-disable state

Jun 3 17:14:19.022 EDT: %PORT_SECURITY-2-PSECURE_VIOLATION: Security
violation occurred, caused by MAC address 0003.a089.efc5 on port
GigabitEthernet0/11.

Jun 3 17:14:20.022 EDT: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Gigabit Ethernet0/11, changed state to down

Jun 3 17:14:21.023 EDT: %LINK-3-UPDOWN: Interface
GigabitEthernet0/11, changed state to down
```

5.3.2 Verificación de la seguridad de puertos

El estado de un puerto puede verse con el comando **show port-security interface**:

```
Switch#show port-security interface gigabitethernet 0/11
Port Security :                  Enabled
Port Status :                    Secure-shutdown
Violation Mode :                 Shutdown
Aging Time :                     0 mins
Aging Type :                     Absolute
SecureStatic Address Aging :     Disabled
Maximum MAC Addresses :          1
Total MAC Addresses :            0
Configured MAC Addresses :       0
Sticky MAC Addresses :           0
Last Source Address :            0003.a089.efc5
Security Violation Count :       1
```

Para ver un resumen rápido del estado de los puertos puede utilizarse el siguiente comando:

```
Switch#show interfaces status err-disabled

Port          Name          Status              Reason
Gi0/11        Test port     err-disabled        psecure-violation
```

Hay que recordar que cuando un puerto está en el estado **errdisable** se debe recuperar manualmente o de manera automática. La secuencia de comandos para la recuperación manual es la siguiente:

```
Switch(config)#interface type mod/num
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

Se puede ver un resumen del estado de **port-security** con el siguiente comando:

```
Switch#show port-security

Secure  Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
(Count)  (Count)  (Count)
--------------------------------------------------------------------
Gi0/11              5            1            0             Restrict
Gi0/12              1            0            0             Shutdown
--------------------------------------------------------------------
Total Addresses in System (excluding one mac per port): 0
Max Addresses limit in System (excluding one mac per port): 6176
```

Los administradores pueden monitorizar quiénes están utilizando la red y dónde se encuentran. La funcionalidad de notificaciones de direcciones MAC envía *traps* SNMP a una estación de administración de la red cada vez que una dirección MAC se incorpora o se elimina de las tablas de reenvío.

Las notificaciones de direcciones MAC son generadas solo para las direcciones MAC dinámicas y seguras.

El comando de configuración global **mac address-table notification** habilita las notificaciones de direcciones MAC en el switch.

5.4 CONTROL DE TORMENTAS

Los ataques de tormenta de LAN pueden ser mitigados utilizando el control de tormentas para monitorizar umbrales de supresión predefinidos. Al habilitar el control de tormentas, es posible configurar un umbral superior y un umbral inferior. El control de tormentas utiliza uno de los siguientes métodos para medir la actividad del tráfico:

- Ancho de banda como un porcentaje del total de ancho de banda disponible en el puerto, y que puede utilizarse para tráfico de broadcast, multicast o unicast.
- Tasa de tráfico en paquetes por segundo recibidos como broadcast, multicast o unicast.
- Tasa de tráfico en bits por segundo recibidos como broadcast, multicast o unicast.
- Tasa de tráfico en paquetes por segundo y por pequeñas tramas. Esta funcionalidad se habilita en forma global. El umbral para pequeñas tramas debe configurarse para cada interfaz.

5.4.1 Configuración de control de tormentas

Cuando se desata una tormenta, la acción será filtrar el tráfico según alguno de los métodos anteriores; entonces, el puerto bloqueará el tráfico una vez alcanzado el umbral superior. El puerto permanece bloqueado hasta que la tasa de tráfico cae por debajo del umbral inferior, si fue especificado, y luego reanuda el reenvío normal. Si el umbral inferior no ha sido especificado, el switch bloquea todo el tráfico hasta que el mismo cae por debajo del umbral superior. El umbral, o nivel de supresión, se refiere al número de paquetes permitidos antes de tomar una acción. En general, mientras más alto sea el nivel de supresión, menos efectiva será la protección contra las tormentas de broadcast.

```
Switch(config-if)# storm-control {{broadcast | multicast | unicast}
level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}} |
{action {shutdown | trap}}
```

La siguiente tabla describe los parámetros.

Parámetro	Descripción
broadcast	Habilita el control de tormentas de broadcast en la interfaz.
multicast	Habilita el control de tormentas de multicast en la interfaz.
unicast	Habilita el control de tormentas de unicast en la interfaz.
level *level* [*level-low*]	Configura los niveles de supresión inferior y superior como un porcentaje del ancho de banda del puerto.
level bps *bps* [*bps-low*]	Configura los niveles de supresión inferior y superior en la tasa de bits por segundos sobre el tráfico que recibe el puerto.
Level pps *pps* [*pps-low*]	Configura los niveles de supresión inferior y superior en la tasa de paquetes por segundos sobre el tráfico que recibe el puerto.
action {**shutdown** | **trap**}	Determina la acción a realizar cuando ocurre algún tipo de tormenta. En el caso de **shutdown** deshabilita el puerto, y para **trap**, se envía una notificación SNMP.

Para verificar la configuración del control de tormentas se utiliza el siguiente comando:

```
Switch# show storm-control [interface] [{broadcast | multicast |
unicast | history}]
```

5.5 PROTECCIÓN DE LAS TOPOLOGÍAS STP

El objetivo **STP** (*Spanning Tree Protocol*) es mantener la red libre de bucles de capa 2. STP explora constantemente la red, de forma que cualquier fallo o adición en un enlace, switch o bridge es detectado al instante. Cuando cambia la topología de red, el algoritmo de Spanning Tree reconfigura los puertos del switch o el bridge para evitar una pérdida total de la conectividad.

En un dominio STP se lleva a cabo la elección de un switch raíz o root bridge. La elección del switch raíz la determina el switch que posea la menor prioridad. Este valor es la suma de la prioridad por defecto dentro de un rango del 1 al 65.536 (20 a 216) y el ID del switch equivalente a la dirección MAC. Por defecto, la prioridad es $2^{15} = 32.768$ y es un valor configurable.

Una red ejecutando STP utiliza las BPDU para la comunicación entre los switches. De esta manera reconocen la existencia de los demás switches de la topología. Una vez que el root bridge es elegido, envía las BPDU hacia los demás que confían en él. Se debe tener en cuenta qué ocurriría si otro switch se conecta a la red de manera que intente ser el nuevo root bridge y cuál es la manera de evitarlo.

Para mitigar manipulaciones de STP, será necesario en primera instancia habilitar PortFast en el switch. Las siguientes sintaxis configuran PortFast para todos los puertos no troncales o para una interfaz específica respectivamente.

```
Switch(config)# spanning-tree portfast default
```

```
Switch(config-if)# spanning-tree portfast
```

PortFast se utiliza en puertos de acceso de capa 2 para conectar una única estación de trabajo o servidor, para permitir a dichos dispositivos conectarse a la red en forma inmediata, en lugar de esperar a que finalice la convergencia de STP.

Para verificar la configuración de PortFast se utiliza el siguiente comando:

```
Switch# show running-config interface type slot/port
```

5.5.1 Configuración de BPDU Guard

La característica BPDU Guard fue creada para garantizar la integridad de los puertos del switch configurados con PortFast para que si se recibe alguna BPDU, el puerto se ponga inmediatamente en estado **errdisable**. El puerto pasa a una condición de error y es desactivado, teniendo que ser manualmente rehabilitado o automáticamente recuperado a través de la función de un temporizador.

Por defecto, BPDU Guard está deshabilitado en todos los puertos del switch pudiendo configurarse con el siguiente comando:

```
Switch(config)# spanning-tree portfast bpduguard default
```

```
Switch(config-if)# spanning-tree bpduguard enable
```

Los puertos que tienen PortFast habilitado también tendrán BPDU Guard habilitado. El siguiente comando muestra información del estado de STP.

```
Switch# show spanning-tree summary
```

5.5.2 Configuración de BPDU Filter

Normalmente STP opera en todos los puertos del switch en un esfuerzo para tratar de que no se formen bucles de capa 2. Las BPDU se envían a todos los puertos del switch, incluso a aquellos en los que PortFast se ha habilitado. Las BPDU también pueden ser recibidas y procesadas por un switch de un dominio STP diferente. Aunque STP debería estar siempre ejecutándose, en ciertos casos habrá que prevenir el envío de las BPDU o su proceso en uno o más puertos del switch. Para conseguir este objetivo se puede utilizar filtrado de las BPDU, que por defecto está deshabilitado en todos los puertos del switch.

La configuración puede hacerse de manera global afectando de esta manera a todos los puertos utilizando el siguiente comando:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

Todos los puertos que tienen PortFast habilitado también tendrán los filtros BPDU habilitados. De la misma forma puede configurarse por puertos:

```
Switch(config-if)# spanning-tree bpdufilter {enable | disable}
```

5.5.3 Configuración de Root Guard

La característica **Root Guard** fue desarrollada para controlar cuándo los candidatos a ser root bridge se conectan en la red. Básicamente un switch aprende e identifica el bridge ID del root si otro switch anuncia una mejor. Cuando Root Guard está habilitado, el switch local no permitirá al nuevo switch que se convierta en root, mientras que BPDU superiores están llegando a ese puerto, este mantendrá un estado inconsistente STP. En este estado no se podrán enviar ni recibir datos, pero se pueden recibir BPDU para detectar un nuevo anuncio del root. Básicamente, lo que hace Root Guard es que un puerto solamente pueda enviar BPDU pero no recibirlas. Previene que un puerto se convierta en puerto raíz donde normalmente las BPDU podrían ser recibidas desde el root bridge.

Esta característica está deshabilitada por defecto y se habilita únicamente por puerto utilizando el siguiente comando:

```
Switch(config-if)# spanning-tree guard root
```

Cuando las BPDU superiores no son recibidas, el puerto vuelve a pasar por los estados STP y regresa a su estado normal. La utilización de Root Guard afecta a todas las VLAN asociadas al puerto, es recomendable configurarlo en los puertos donde nunca se espera un root bridge para alguna de esas VLAN.

Para ver el estado inconsistente de un puerto puede usarse el siguiente comando:

```
Switch# show spanning-tree inconsistentports
```

5.6 SEGURIDAD EN VLAN

Las **VLAN** (LAN Virtuales) proveen seguridad, segmentación y flexibilidad; permiten agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden concentrar lógicamente los puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común.

Muchas veces es necesario agrupar usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas. Para conseguir esta comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las VLAN que tienen configuradas a través de enlaces troncales es necesario que las tramas sean identificadas con el propósito de saber a qué VLAN pertenecen.

Asegurar las VLAN y los enlaces troncales es una tarea primordial.

5.6.1 Seguridad del enlace troncal

Los switches pueden negociar dinámicamente un enlace troncal mediante el intercambio de mensajes **DTP** (*Dynamic Trunking Protocol*). Si bien esto puede facilitar la administración del switch, se expone a que los puertos del switch queden comprometidos. Si un puerto mantiene su configuración por defecto, donde el trunk está en modo **auto**, podría ser indagado por un puerto de otro switch también en **auto** o en modo **on** enlazando entonces un troncal. El atacante puede recibir cualquier tipo de tráfico enviado por cualquiera de las VLAN del troncal y enviar tráfico por cualquiera de ellas.

Cuando se está asegurando un troncal se debe tener en cuenta el mecanismo de ataque **VLAN hopping**. Consiste en que un atacante posicionado en una VLAN de acceso puede enviar tramas con etiquetas 802.1Q falsas, sin la necesidad de un router, de tal manera que los paquetes parecerán de una VLAN completamente diferente.

La mitigación de los ataques de VLAN hopping con doble encapsulación 802.1Q requiere varias modificaciones en la configuración de VLAN. Uno de los elementos más importantes es utilizar una VLAN nativa dedicada en todos los enlaces troncales. Este ataque puede evitarse fácilmente siguiendo la práctica

recomendada de no utilizar VLAN nativas para enlaces troncales en ningún otro puerto del switch. Además, deben deshabilitarse todos los puertos no utilizados del switch y colocarse en una VLAN sin uso.

5.6.2 Configuración de un enlace troncal seguro

La primera práctica consiste en configurar los enlaces que no deban ser troncales en puertos de acceso con el comando de configuración de interfaz **switchport mode access** para deshabilitar el trunking en dichas interfaces.

La configuración básica de un enlace troncal conlleva los siguientes pasos:

- Convertir una interfaz a un enlace troncal con el comando:

```
Switch(config-if)# switchport mode trunk
```

- Evitar la generación de tramas DTP con el comando:

```
Switch(config-if)# switchport nonegotiate
```

- Asignar una VLAN sin uso como la VLAN nativa del trunk. La VLAN nativa por defecto es la VLAN 1.

```
Switch(config-if)# switchport trunk native vlan vlan_number
```

5.6.3 VLAN Access Lists

El tráfico dentro de la misma VLAN se permite sin ningún tipo de restricción. Cuando un host envía un paquete de broadcast, todos los demás host dentro de la misma VLAN lo recibirán. Una **VACL** (VLAN *Access Lists*) puede filtrar los paquetes entre un origen y los destinos en la misma VLAN si ambos están conectados al mismo switch. Es muy útil poder segmentar tráfico en una VLAN sin tener que utilizar múltiples VLAN y un router.

En principio se debe crear una lista de acceso de la manera tradicional y asociarla a la VACL con el siguiente comando.

```
Switch(config)# access-list {100-199} {permit | deny} protocol
source-addr destination-addr [destination-wildcard]

Switch(config)# vlan access-map map-name [sequence-number]
```

Posteriormente, se definen las condiciones para que el tráfico pueda ser filtrado.

```
Switch(config-access-map)# match ip address {acl-number | acl-name}
Switch(config-access-map)# match ipx address {acl-number | acl-name}
Switch(config-access-map)# match mac address acl-name
```

El siguiente comando define la acción a seguir por el access map:

```
Switch(config-access-map)# action {drop | forward [capture] |
redirect type mod/num}
```

Por último, la VACL se debe aplicar a una VLAN con el siguiente comando.

```
Switch(config)# vlan filter map-name vlan-list vlan-list
```

5.6.4 Private VLAN

Las **PVLAN** (*Private* VLAN) hacen que una VLAN normal pueda estar lógicamente asociada con una VLAN secundaria, los host asociados con la VLAN secundaria podrán comunicarse con la VLAN primaria (por ejemplo, con un router) pero no con otros de la VLAN secundaria. Una VLAN secundaria se configura como uno de los siguientes tipos:

- **Isolated**: los host asociados con la misma VLAN están aislados entre sí pero no de la VLAN primaria.

- **Community**: cualquier puerto asociado puede comunicarse con otros y además con la VLAN primaria, pero no podrá comunicarse con cualquier otra VLAN secundaria.

El primer paso en la configuración de la PVLAN es definir alguna VLAN secundaria, para ello se utiliza el siguiente comando.

```
Switch(config)# vlan vlan-id
Switch(config-vlan)# private-vlan {isolated | community}
```

La VLAN secundaria puede ser **isolated** o **community**, lo siguiente es definir la VLAN primaria.

```
Switch(config)# vlan vlan-id
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association {secondary-vlan-list |
add secondary-vlan-list | remove secondary-vlan-list}
```

Una vez definida la función del puerto que participará en la PVLAN puede configurarse con el siguiente comando.

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous}
```

Donde:

- **Promiscuo**: el puerto del switch se conecta a un router, firewall o algún dispositivo que hace las veces de gateway.
- **Host**: el puerto del switch está conectado a un host normal, que reside en una VLAN aislada o *community*.

A través del siguiente comando, el puerto del switch sabrá cómo interactuar con los diferentes tipos de VLAN.

```
Switch(config-if)# switchport private-vlan host-association primary-
vlan-id secondary-vlan-id
```

El siguiente comando asocia puertos en modo promiscuo a VLAN primarias y secundarias.

```
Switch(config-if)# switchport private-vlan mapping primary-vlan-id
secondary-vlan-list | {add secondary-vlan-list} | {remove secondary-
vlan-list}
```

EJEMPLO:

En la siguiente sintaxis, el switch está configurado para que los PC en los puertos Fast 1/1 y 1/2 funcionen en una comunidad VLAN 10 y los puertos Fast 1/4 y 1/5 en la comunidad VLAN 20, y el host en Fast 1/3 esté aislado en la VLAN 30. El router está en el modo promiscuo en la VLAN primaria. Cada VLAN tiene asignado un rol y la primaria está asociada con la secundaria. Cada puerto está asociado a una VLAN determinada.

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan community
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan community
Switch(config)# vlan 30
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 100
```

```
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 10,20,30
Switch(config-vlan)# exit
Switch(config)# interface range fastethernet 1/1 - 1/2
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 10
Switch(config)# interface range fastethernet 1/4 - 1/5
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 20
Switch(config)# interface fastethernet 1/3
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 30
Switch(config)# interface fastethernet 2/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 10,20,30
```

5.6.5 Private VLAN Edge

Algunas aplicaciones requieren que el tráfico de capa 2 no se transmita entre los puertos del mismo switch, es decir, que un host no detecte el tráfico generado por otro. En tal ambiente, el uso de la característica Private VLAN Edge, también conocida como "puertos protegidos", asegura que no haya intercambio de tráfico unicast, broadcast o multicast entre estos puertos del switch.

Las PVLAN Edge poseen las siguientes características:

- Un puerto protegido no enviará tráfico unicast, multicast o broadcast a otro puerto que sea también un puerto protegido. Todo el tráfico de datos entre los puertos protegidos debe ser enviado a través de un dispositivo de capa 3.

- El tráfico entre un puerto protegido y un puerto no protegido se envía de la manera habitual.

- Los puertos por defecto no son puertos protegidos.

La configuración de la característica PVLAN Edge puede realizarse en una interfaz física o en un grupo EtherChannel a través del siguiente comando en el modo de la interfaz específica.

```
Switch(config-if)# switchport protected
```

Para deshabilitar un puerto protegido anteponga un **no** al comando **switchport protected**.

Para verificar la funcionalidad de las PVLAN Edge se utiliza el siguiente comando.

```
Switch# show interfaces interface-id switchport
```

5.6.6 Switched Port Analyzer

Un switch al dividir dos segmentos separa los dominios de colisión, por lo tanto no enviará las tramas donde se encuentre conectado el terminal que debe analizar los paquetes si se encuentra en el otro segmento.

Para resolver este problema Cisco ha creado una funcionalidad llamada **SPAN** (*Switched Port Analyzer*), cuyo funcionamiento básico es copiar todas las tramas que pasan por un puerto determinado a otro donde estará conectado el capturador de paquetes.

En entornos de grandes redes puede darse el caso de que un dispositivo de captura de paquetes esté conectado a un switch y sea necesario capturar paquetes desde otros switches. Para estos casos existe la herramienta **RSPAN** (*Remote* SPAN). El funcionamiento se basa en una VLAN especial que se encarga de transportar ese tráfico entre los switches.

Una sesión de SPAN se puede configurar para controlar el tráfico desde un puerto de origen a un puerto de destino. El comando **monitor session** habilita SPAN en el switch. Las siguientes sintaxis muestran los comandos completos para la configuración de SPAN en origen y en destino respectivamente.

```
Switch(config)# [no] monitor session session_number source {
{interface type/num} | {vlan vlan-ID}} [, | - | rx | tx | both] |
{remote vlan vlan-ID}
```

```
Switch(config)# [no] monitor session session_number destination
{{interface type/num} [, | - ] [encapsulation {dot1q
|replicate}] [ingress {dot1q vlan vlan-ID | untagged vlan vlan-ID |
vlan vlan-ID }]} | {remote vlan vlan-ID}
```

Los comandos completos pueden resultar largos y complicados, una configuración básica puede ser la siguiente.

```
Switch(config)# [no] monitor session session_number source
{interface type/num}
```

```
Switch(config)# [no] monitor session {session_number} destination
{interface type/num} [encapsulation {dot1q |replicate}
```

Para verificar la configuración de SPAN se utiliza el siguiente comando.

```
Switch# show monitor session session-number
```

EJEMPLO:

La siguiente sintaxis muestra un ejemplo de configuración de SPAN en un Catalyst 3550:

```
Switch# conf term

Enter configuration commands, one per line. End with CNTL/Z.

Cat3550(config)# monitor session 1 source interface gig 0/1
Cat3550(config)# monitor session 1 destination interface gig 0/3
encapsulation replicate
Cat3550(config)# end

Switch# show monitor session 1

Session 1
------------
Type                    : Local Session
Source Ports            :
Both                    : Gi0/1
Destination Ports       : Gi0/3
Encapsulation           : Native
Ingress                 : Disabled
```

5.7 FUNDAMENTOS PARA EL EXAMEN

- En este capítulo se deben tener presentes muchos conceptos sobre el funcionamiento de las VLAN, enlaces troncales y STP aprendidos en el CCNA. Un repaso sobre estos temas es fundamental.

- Recuerde cuáles son las soluciones que Cisco dispone para asegurar terminales.

- Memorice y analice cuáles son los ataques comunes de capa 2, qué efectos tienen y cómo mitigarlos.

- Tenga presente cómo funciona la seguridad en los puertos de un switch.

- Estudie cómo proteger y mejorar el funcionamiento de topologías STP, enlaces troncales y VLAN.

- Recuerde qué son y cómo se configuran las PVLAN, las PVLAN Edge y las VACL.

- Diseñe topologías con equipos reales o simuladores, haga pruebas y ensaye soluciones.

Capítulo 6

LISTAS DE CONTROL DE ACCESO

6.1 INTRODUCCIÓN A ACL

Desde la primera vez que se conectaron varios sistemas para formar una red, ha existido la necesidad de restringir el acceso a determinados sistemas o partes de la red por motivos de seguridad, privacidad y otros. Mediante la utilización de las funciones de filtrado de paquetes del software IOS, un administrador de red puede restringir el acceso a determinados sistemas, segmentos de red, rangos de direcciones y servicios, basándose en una serie de criterios. La capacidad de restringir el acceso cobra mayor importancia cuando la red de una empresa se conecta con otras redes externas, como otras empresas asociadas o Internet.

6.1.1 Funcionamiento de las ACL

Los dispositivos de red se sirven de las **ACL** (*Access Control Lists*) para identificar el tráfico. Esta identificación puede usarse después para filtrarlo y conseguir una mejor administración del tráfico global de la red. Las listas de acceso constituyen una eficaz herramienta para el control de la red, añaden la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las diferentes interfaces.

Las ACL trabajan utilizando entradas de control de acceso, **ACE** (*Access Control Entries*), en un listado secuencial de condiciones de permiso o prohibición que se aplican a direcciones IP o a protocolos IP de capa superior.

Las listas de acceso identifican el tráfico que ha de ser filtrado en su tránsito por el dispositivo, pero no pueden filtrar el tráfico originado por el mismo. Pueden aplicarse también a los puertos de líneas de terminal virtual para permitir y denegar tráfico telnet entrante o saliente.

Las listas de acceso son mecanismos opcionales del software Cisco IOS que pueden ser configurados para filtrar o verificar paquetes con el fin de determinar si deben ser retransmitidos hacia su destino o descartados. Se pueden usar listas de acceso IP para establecer un control más fino a la hora de separar el tráfico en diferentes colas de prioridades y personalizadas.

Cuando un paquete llega a una interfaz, el dispositivo comprueba si el paquete puede ser retransmitido verificando su tabla de enrutamiento. Si no existe ninguna ruta hasta la dirección de destino, el paquete es descartado. A continuación, se comprueba si la interfaz de destino está agrupada en alguna lista de acceso. De no ser así, el paquete puede ser enviado al buffer de salida. Si el paquete de salida está destinado a un puerto que no ha sido agrupado a ninguna lista de acceso de salida, dicho paquete será enviado directamente al puerto destinado. Si el paquete de salida está destinado a un puerto que ha sido agrupado en una lista de acceso saliente, antes de que el paquete pueda ser enviado al puerto destinado será verificado por una serie de instrucciones de la lista de acceso asociada con dicha interfaz. Dependiendo del resultado de estas pruebas, el paquete será admitido o denegado.

Las instrucciones de una lista de acceso operan en un orden lógico secuencial. Evalúan los paquetes de principio a fin, instrucción a instrucción. Si la cabecera de un paquete se ajusta a una instrucción de la lista de acceso, el resto de las instrucciones de la lista serán omitidas y el paquete será permitido o denegado según se especifique en la instrucción competente.

Si la cabecera de un paquete no se ajusta a una instrucción de la lista de acceso, la prueba continúa con la siguiente instrucción de la lista.

El proceso de comparación sigue hasta llegar al final de la lista, cuando el paquete será denegado implícitamente. Esta instrucción final se conoce como la denegación implícita de todo, al final de cada lista de acceso. Aunque esta instrucción no aparece en la configuración, siempre está activa. Debido a dicha condición, es necesario que en toda lista de acceso exista al menos una instrucción **permit**, en caso contrario la lista de acceso bloquearía todo el tráfico.

6.1.2 Mitigación de ataques con ACL

Las listas de control de acceso son herramientas eficaces para mitigar muchas amenazas de red como las falsificaciones de direcciones IP, ataques de DoS SYN TCP o ataques de DoS *smurf*.

El IOS de Cisco soporta varias tecnologías diseñadas para minimizar el daño causado por los ataques de DoS. La mayoría de los ataques usan algún tipo de falsificación. Hay muchas clases de direcciones IP bien conocidas que nunca deben tomarse como direcciones IP de origen del tráfico que ingresa a la red de una organización. Hay ACL específicas que son fáciles de implementar y previenen que los ataques se originen en los siguientes tipos de direcciones.

- Local host 127.0.0.0/8.
- Direcciones privadas especificadas en la RFC 1918.
- Direcciones Multicast del tipo 224.0.0.0/4.

También es muy común que un firewall requiera una configuración para permitir protocolos necesarios para la administración del router.

Los hackers pueden usar mensajes de redirección ICMP para alterar las tablas de enrutamiento de los hosts. Las entradas de mensajes eco y de redirección ICMP deben ser bloqueadas.

6.1.3 Tipos de lista de acceso

Las listas de acceso se utilizan en las redes para ampliar la seguridad, mitigar los ataques de red y controlar el tráfico de la red. Según el tipo y clase de tráfico, los administradores deben definir qué tipo de lista de acceso es la adecuada para administrar el tráfico.

- **Listas de acceso estándar**: comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.
- **Listas de acceso extendidas**: comprueban tanto la dirección de origen como la de destino de cada paquete. También pueden verificar protocolos especificados, números de puerto y otros parámetros.

- **Listas de acceso con nombre**: permiten asignar nombres en lugar de un rango numérico en las listas de acceso estándar y extendidas.

- **Listas de acceso dinámicas**: este tipo de ACL depende de telnet a partir de la autenticación de los usuarios que quieran atravesar el router y que han sido previamente bloqueados por una ACL extendida. Una ACL dinámica añadida a la ACL extendida existente permitirá tráfico a los usuarios que son autenticados en una sesión de telnet por un período de tiempo en particular.

- **Listas de acceso reflexivas**: permiten el filtrado de paquetes IP en función de la información de la sesión de capa superior. Mayormente se utilizan para permitir el tráfico saliente y para limitar el entrante en respuesta a las sesiones originadas dentro del router.

- **Listas de acceso basadas en tiempo**: son similares a las ACL extendidas en función, salvo que además restringen el tráfico en base a la hora del día, el día de la semana o el día del mes. Las entradas ACL pueden registrar el tráfico en ciertos momentos del día, pero no constantemente.

6.2 UBICACIÓN DE LAS ACL

Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido en los dispositivos de red para los paquetes que entran en interfaces de entrada y paquetes que salen de las interfaces de salida.

Una vez creada, una ACL debe asociarse a una o varias interfaces de forma que analice todos los paquetes que pasen por estas ya sea de manera entrante o saliente según corresponda el caso. La manera de determinar cuál de los casos es el que corresponde es pensar si los paquetes van hacia la red en cuestión (saliente) o si vienen de ella (entrante).

Las ACL deben ubicarse donde más repercutan sobre la eficacia. Las reglas básicas son:

- Ubicar las ACL extendidas lo más cerca posible del origen del tráfico denegado. De esta manera, el tráfico no deseado se filtra sin atravesar la infraestructura de red.

- Como las ACL estándar no especifican las direcciones de destino, se recomienda configurarlas lo más cerca del posible destino.

6.2.1 Lista de acceso entrante

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento (evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado). Para las listas entrantes un **permit** significa continuar el procesamiento del paquete tras su recepción en una interfaz, mientras que **deny** significa descartar el paquete.

6.2.2 Lista de acceso saliente

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión. Para las listas salientes un **permit** significa enviar al búfer de salida, mientras que **deny** se traduce en descartar el paquete.

6.3 RECOMENDACIONES EN EL DISEÑO DE LAS ACL

El orden en el que aparecen las instrucciones en la lista de acceso es fundamental para un filtrado correcto. La práctica recomendada consiste en crear las listas de acceso usando un editor de texto y descargarlas después en un router vía TFTP o copiando y pegando el texto. Las listas de acceso se procesan de arriba abajo. Si coloca las pruebas más específicas y las que se verificarán con más frecuencia al comienzo de la lista de acceso, se reducirá la carga de procesamiento. Solo las listas de acceso con nombre permiten la supresión, aunque no la alteración del orden de instrucciones individuales en la lista. Si desea reordenar las instrucciones de una lista de acceso, deberá eliminar la lista completa y volver a crearla en el orden apropiado o con las instrucciones correctas.

La siguiente lista enumera consideraciones importantes a la hora de diseñar una ACL.

1. Una lista de acceso puede ser aplicada a múltiples interfaces.

2. Solo puede haber una lista de acceso por protocolo, por dirección y por interfaz.

3. Es posible tener varias listas para una interfaz, pero cada una debe pertenecer a un protocolo diferente.

4. Organice las listas de acceso de modo que las referencias más específicas a una red o subred aparezcan delante de las más generales.

5. Coloque las condiciones de cumplimiento más frecuente antes de las menos habituales.

6. Las adiciones a las listas se agregan siempre al final de estas, pero siempre delante de la condición de denegación implícita.

7. No es posible agregar ni eliminar selectivamente instrucciones de una lista cuando se usan listas de acceso numeradas, pero sí cuando se usan listas de acceso IP con nombre.

8. A menos que termine una lista de acceso con una condición de permiso implícito de todo, se denegará todo el tráfico que no cumpla ninguna de las condiciones establecidas en la lista al existir un **deny** implícito al final de cada lista.

9. Toda lista de acceso debe incluir al menos una instrucción **permit**. En caso contrario, todo el tráfico será denegado.

10. Cree una lista de acceso antes de aplicarla a la interfaz. Una interfaz con una lista de acceso inexistente o indefinida aplicada permitirá todo el tráfico.

11. Las listas de acceso permiten filtrar solo el tráfico que pasa por el router. No pueden hacer de filtro para el tráfico originado por el propio router.

NOTA:

Recuerde antes de comenzar la configuración:

Un bit de máscara wildcard 0 significa "comprobar el valor correspondiente".
Un bit de máscara wildcard 1 significa "No comprobar (ignorar) el valor del bit correspondiente".

6.4 CONFIGURACIÓN DE ACL NUMERADA

Prácticamente cualquier tipo de tráfico puede ser definido explícitamente usando apropiadamente una ACL numerada. La siguiente tabla describe el tipo de ACL y el rango que le corresponde.

ACL	Rango	Rango extendido
IP estándar	1-99	1.300-1.999
IP extendida	100-199	2.000-2.699
Prot, type code	200-299	
DECnet	300-399	
XNS estándar	400-499	
XNS extendida	500-599	

Apple Talk	600-699	
Ethernet	700-799	
IPX estándar	800-899	
IPX extendida	900-999	
Filtros Sap	1.000-1.099	

El proceso de creación de una ACL se lleva a cabo creando la lista y posteriormente asociándola a una interfaz entrante o saliente.

6.4.1 Configuración de ACL estándar

Las listas de acceso IP estándar verifican solo la dirección de origen en la cabecera del paquete IP. Las ACL estándar llevan un número que las identifica según sus características. El rango numérico de las listas de acceso estándar es de 1 a 99 y el rango extendido es de 1.300 a 1.999.

```
Router(config)# access-list {1-99} {permit | deny} source-address
[source-wildcard]
```

Donde:

- **1-99**: identifica el rango y número de lista.
- **Permit | deny**: indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección origen.
- **source-address**: identifica la dirección IP de origen.
- **source-wildcard**: identifica los bits del campo de la dirección que serán comprobados.

La lista de acceso estándar puede eliminarse anteponiendo un **no** al comando.

```
Router(config)# no access-list {1-99}
```

6.4.2 Configuración de ACL extendida

Las listas de acceso IP extendidas pueden verificar otros muchos elementos, incluidas opciones de la cabecera del segmento de capa 4, como los números de puerto. Las ACL extendidas llevan un número que las identifica según sus características. El rango numérico de las listas de acceso extendidas es de 100 a 199 y el rango extendido es de 2.000 a 2.699.

```
Router(config)# access-list {100-199} {permit | deny} protocol
source-address [source-wildcard] [operator port] destination-address
[destination-wildcard] [operator port | icmp_type] [established]
```

Donde:

- **100-199**: identifica el rango y número de lista.
- **Permit | deny**: indica si la entrada permitirá o bloqueará el tráfico desde la dirección origen hacia el destino.
- **Protocol**: como por ejemplo IP, TCP, UDP, ICMP.
- **source-address**: identifica direcciones IP de origen.
- **source-wildcard**: identifica los bits del campo de la dirección de origen que serán comprobados.
- **destination-address**: identifica direcciones IP de destino.
- **destination -wildcard**: identifica los bits del campo de la dirección de destino que serán comprobados.
- **operator port**: compara los puertos de origen o de destino. Operandos posibles son **lt** (menor que), **gt** (mayor que), **eq** (igual), **neq** (no igual), y **range** (rango).
- **established**: se usa solo para TCP de entrada. Esto permite que el tráfico TCP pase si el paquete utiliza una conexión ya establecida (si, por ejemplo, posee un conjunto de bits ACK).

La lista de acceso extendida puede eliminarse anteponiendo un **no** al comando.

```
Router(config)# no access-list {100-199}
```

6.4.3 Asociación de las ACL a una interfaz

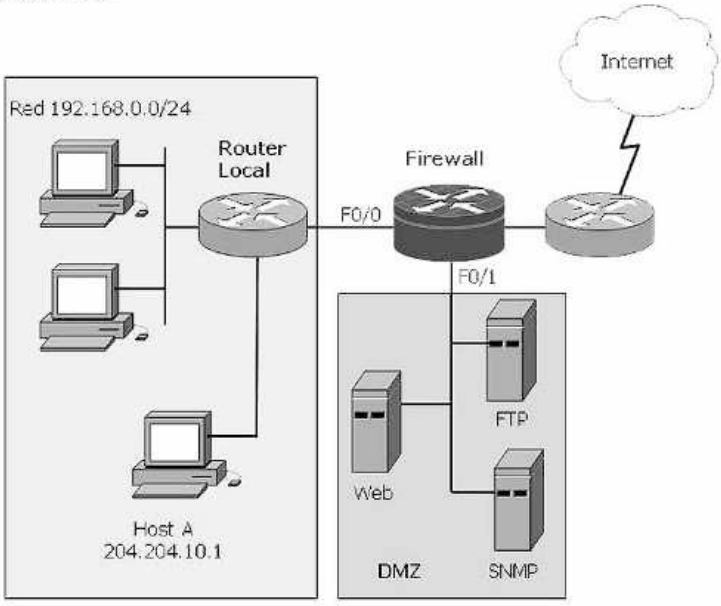
La asociación de las ACL a una interfaz en particular se realiza en el modo de interfaz correspondiente aplicando el siguiente comando.

```
Router(config-if)# ip access-group access-list-number {in | out}
```

Donde:

- **access-list-number** indica el número de lista de acceso que será aplicado a esa interfaz.
- **in | out** selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.

EJEMPLO:



En el siguiente ejemplo se ha configurado una ACL estándar denegado en el firewall la red 192.168.1.0 y luego se ha permitido a cualquier origen; posteriormente se asoció la ACL a la interfaz FastEthernet 0/0 como entrante.

```
Router#configure terminal
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.0
Router(config)#access-list 10 permit any
Router(config)#interface Fast 0/0
Router(config-if)#ip access-group 10 in
```

En el siguiente caso se ha denegado al host A, 204.204.10.1, hacia el puerto 80 hacia la red de servidores configurando una ACL extendida. Posteriormente se permite todo tráfico IP. Esta ACL se asoció a la interfaz Fastethernet 0/1 como saliente.

```
Router(config)#access-list 120 deny tcp host 204.204.10.1 any eq 80
Router(config)#access-list 120 permit ip any any
Router(config)#interface Fastethernet 0/1
Router(config-if)#ip access-group 120 out
```

6.4.4 Aplicación de una ACL a la línea de telnet

Para evitar intrusiones no deseadas en las conexiones de telnet se puede crear una lista de acceso estándar y asociarla a la Line VTY. El proceso de creación se lleva a cabo como una ACL estándar denegando o permitiendo un origen hacia esa interfaz. El modo de asociar la ACL a la línea de telnet es el siguiente:

```
Router(config)#line vty 0 4
Router(config-line)# access-class access-list-number {in | out}
```

NOTA:

La dirección 0.0.0.0 y una máscara wildcard 255.255.255 que identifican a toda la red, puede abreviarse con el parámetro ***any****. La máscara wildcard de un host específico puede abreviarse con el parámetro host.*

6.5 LISTAS DE ACCESO CON NOMBRE

Con listas de acceso IP numeradas, para modificar una lista tendría que borrar primero la lista de acceso completa y volver a introducirla de nuevo con las correcciones necesarias.

En una lista de acceso numerada no es posible borrar instrucciones individuales. Las listas de acceso IP con nombre permiten eliminar entradas individuales de una lista específica. El borrado de entradas individuales permite

modificar las listas de acceso sin tener que eliminarlas y volver a configurarlas desde el principio. Sin embargo, no es posible insertar elementos selectivamente en una lista.

6.5.1 Configuración de ACL nombrada

Básicamente, la configuración de una ACL nombrada es igual a la de las extendidas o estándar numeradas. Si se agrega un elemento a la lista, este se coloca al final de la misma. No es posible usar el mismo nombre para varias listas de acceso. Las listas de acceso de diferentes tipos tampoco pueden compartir nombre.

```
Router(config)# ip access-list [standard | extended] name_of_ACL
```

Para el caso de una ACL nombrada estándar el proceso continúa con el siguiente comando:

```
Router(config-std-nacl)# deny {source [source-wildcard] | any}

Router(config-std-nacl)# permit {source [source-wildcard] | any}
```

Para el caso de una ACL nombrada extendida, el proceso continúa con el siguiente comando:

```
Router(config-ext-nacl)# {permit | deny} protocol source-addr
[source-wildcard] [operator port] destination-addr [destination-
mask] [operator port] [established]
```

Para eliminar una instrucción individual, anteponga **no** a la condición de prueba.

```
Router(config[std|ext]nacl)#no[permit|deny] ..........
```

El proceso termina asociando la ACL nombrada a una interfaz de entrada o salida.

```
Router(config-if)# ip access-group access-list-name {in | out}
```

6.6 MENSAJES DE REGISTRO EN LAS ACL

Al final de una sentencia ACL, el administrador tiene la opción de configurar el parámetro **log**. Cuando este parámetro se configura, se comparan los paquetes en búsqueda de una coincidencia con la sentencia. El dispositivo registra en una función de registro habilitada, como la consola, el buffer interno del router o

un servidor syslog. Los mensajes de registro se generan en la primera coincidencia de paquete y luego en intervalos de cinco minutos.

La habilitación del parámetro **log** en una ACL puede afectar seriamente al rendimiento del dispositivo. Cuando se habilita el registro, los paquetes son transmitidos por conmutación de proceso o por conmutación rápida. El parámetro **log** debe ser usado solamente si la red está bajo ataque y el administrador está intentando determinar quién es el atacante. En este punto, el administrador debe habilitar el registro por el tiempo que sea necesario para reunir la información suficiente y luego deshabilitarlo.

```
Router(config)# access-list {100-199} {permit | deny} protocol
source-address [source-wildcard] destination-address [destination-
wildcard] [established] [log]
```

6.7 CONFIGURACIÓN DE ACL CON CCP

La configuración de las listas de control de acceso con CCP se inicia desde **Configure** / **Router** / **ACL**. Pueden definirse ciertos tipos de roles o reglas de tal forma que el dispositivo responda a un determinado tipo de tráfico. CCP proporciona reglas predeterminadas que un administrador puede utilizar al crear listas de acceso.

Para acceder a los roles predeterminados siga la siguiente ruta **Configure** / **Router** / **ACL** / **ACL** Summary.

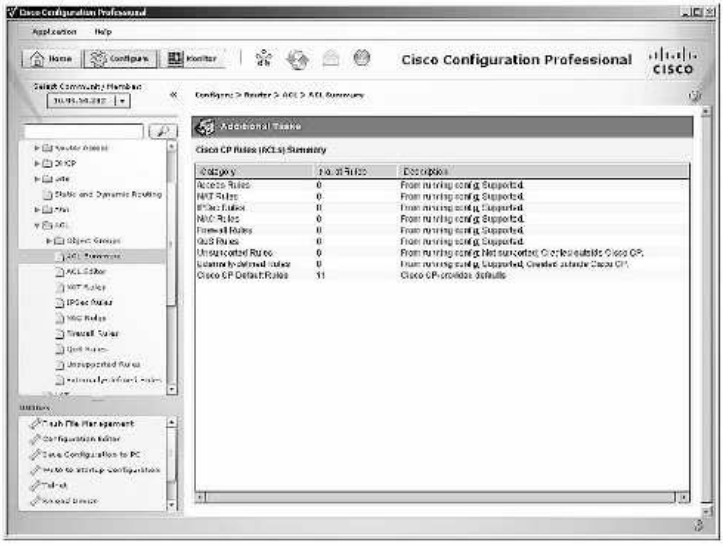
- **Access rules**: regulará el tráfico que puede entrar y salir de la red. Un administrador puede aplicar reglas de acceso a las interfaces del router y las líneas vty.
- **NAT rules**: determina qué direcciones IP privadas se convierten en direcciones IP válidas de Internet.
- **IPsec rules**: determina que el tráfico está cifrado en las conexiones seguras.
- **NAC rules**: especifica las direcciones IP que son admitidas a la red o bloqueadas desde la red.
- **Firewall rules**: especifica el origen y destino del tráfico y si está permitido o denegado.

- **QoS rules**: especifica la calidad de servicio (QoS) del tráfico a la que está asociada la regla.

- **Unsupported rules**: reglas de solo lectura y que no se pueden modificar mediante CCP.

- **Externally defined rules**: no fueron creadas con CCP, pero están soportadas por CCP. Estas reglas no se pueden asociar en cualquier interfaz.

- **Cisco CP default rules**: reglas predefinidas por el asistente de CCP.



Para configurar una ACL estándar o extendida con CCP siga los siguientes pasos:

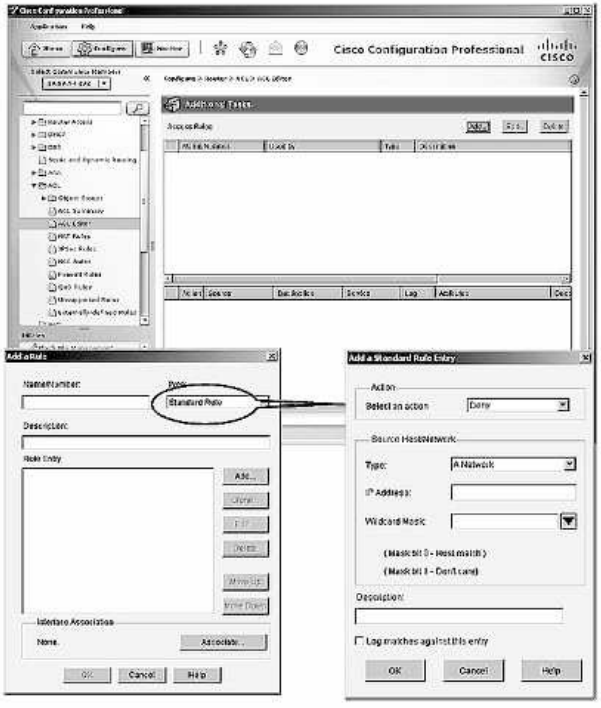
- Seleccione **Configure** / **Router** / **ACL** / **ACL Editor** y luego **Add**.

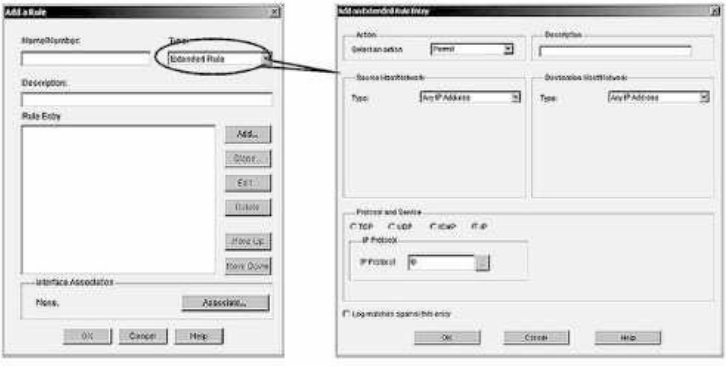
- En la ventana **Add a Rule** numere o nombre el tipo de ACL con **Name/Number**.

- Desde la casilla **Type** seleccione **estándar** o **extendida**. Opcionalmente puede completar una descripción desde la casilla **Description**. Siga con **Add**.

- Según el tipo de lista de acceso seleccionada en la casilla **Type** complete los datos necesarios y finalice con **OK**.

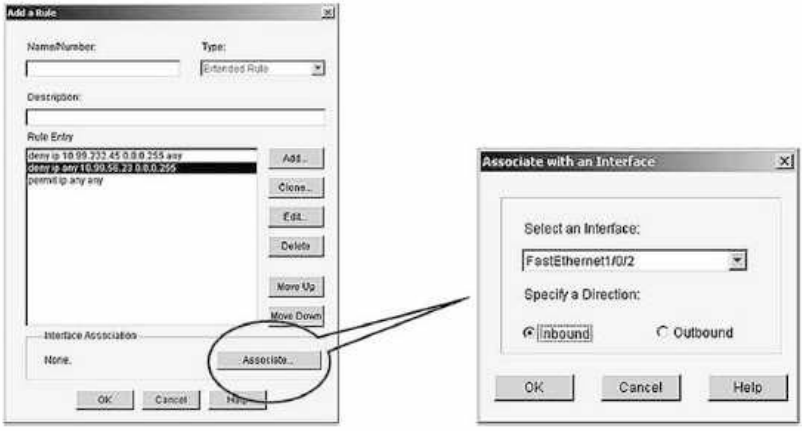
- Opcionalmente puede marcar la casilla **Log matches** para tener registro de syslog.





Continúe añadiendo o editando entradas hasta que la regla esté completa. Si en algún momento el orden de las entradas debe cambiarse en la lista, use los botones **Move Up** y **Move Down**.

El siguiente paso es asociar la ACL a una o varias interfaces. Seleccione el botón **Associate** y luego seleccione el tipo y número de interfaz. En las casillas **Inbound** u **Outbound** marque si es de entrada o de salida.

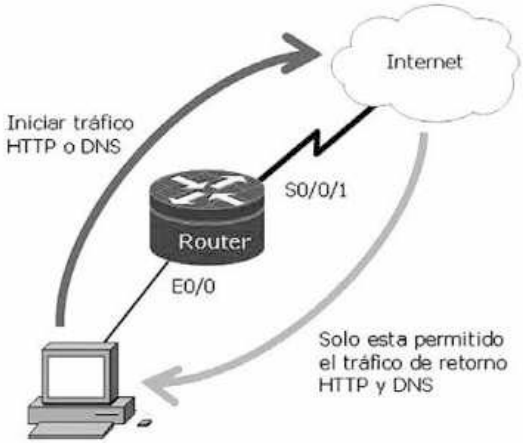


Verifique la asociación en **Interface Association** y luego pulse **OK**.

Finalice con el botón **Deliver**.

6.8 LISTAS DE ACCESO REFLEXIVAS

En las listas de control de acceso extendidas, el uso del comando **established** permite el filtrado de sesiones de los paquetes TCP siempre y cuando estén establecidos los bits ACK o RTS. La idea básica es que se bloquee el acceso al tráfico del exterior salvo que se permita explícitamente por medio de una ACL, o, si se trata de tráfico de retorno, que el mismo se corresponda con tráfico que se inició dentro de la red interna. Sin embargo, para el resto de protocolos como UDP o ICMP esto no es posible, debiendo permitirse todo el tráfico o direcciones puntuales origen/destino.



Las ACL reflexivas permiten el verdadero filtrado de las sesiones independientemente del protocolo utilizado. Una ACL reflexiva se activa cuando una sesión de la capa superior IP se inicia desde el interior de la red hacia la red exterior, permitiendo solo el tráfico de paquetes que formen parte de la sesión. El criterio del filtrado se basa en los bits ACK y RTS, además de las direcciones de origen y destino y los números de puerto.

```
Router(config)# access-list {100-199} {permit | deny} protocol
source-address [source-wildcard] destination-address [destination-
wildcard] [established]
```

El filtrado de sesiones de las ACL reflexivas usa filtros temporales que se eliminan una vez que la sesión finaliza. Las ACL reflexivas trabajan utilizando entradas de control de acceso ([**ACE**] *Access Control Entries*) temporales insertadas en una ACL extendida, que se aplica en la interfaz externa del router de perímetro. Una vez que la sesión finaliza o la entrada temporal vence, es eliminada de la configuración de la ACL en la interfaz externa. Esto reduce la exposición de la red a ataques de DoS.

Las ACE que se añaden examinan el tráfico asociado con nuevas sesiones usando el parámetro **reflect**. Las ACE de conexión se crean dinámicamente basándose en estas sentencias para permitir el tráfico de retorno. A medida que el tráfico deja la red, si coincide con una sentencia de permiso con un parámetro **reflect**, se agrega una entrada temporal a la ACL reflexiva. Por cada sentencia **permit-reflect**, el router crea una ACL reflexiva aparte.

El proceso de configuración se inicia creando una ACL interna que busque nuevas sesiones de salida y cree ACE reflexivas temporales y una ACL externa que

use las ACL reflexivas para examinar el tráfico de retorno, asociándolas a las interfaces correspondientes.

La siguiente sintaxis muestra los parámetros de configuración de una ACL nombrada interna.

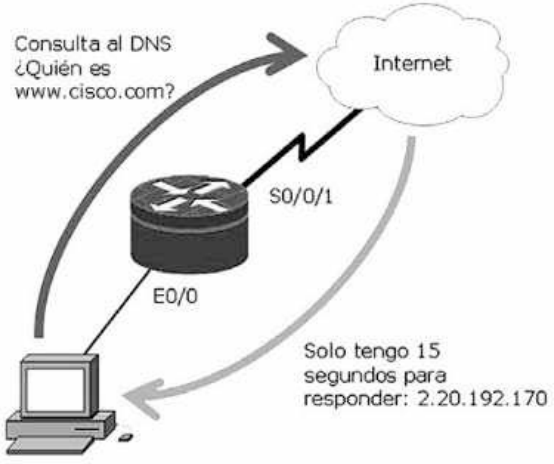
```
Router(config)# ip access-list extended internal_ACL_name

Router(config-ext-nacl)# permit protocol source-addr [source-mask]
[operator port] destination-addr [destination-mask] [operator port]
[established] reflect reflexive_ACL_name [timeout seconds]
```

La ACL nombrada interna extendida creada origina las ACE reflexivas, ahora debe hacerse referencia a las entradas temporales a medida que el tráfico fluye de vuelta a la red. Para esto debe crearse una segunda ACL nombrada extendida. En esta ACL nombrada se usa la sentencia **evaluate** para hacer referencia a las ACE reflexivas que fueron creadas por la ACL interna.

```
Router(config)# ip access-list extended external_ACL_name
Router(config-ext-nacl)#evaluate reflexive_ACL_name
```

EJEMPLO:

Un escenario típico para las ACL reflexivas es el uso de navegadores web que utilizan DNS para navegar en Internet. La siguiente sintaxis muestra la configuración básica de una ACL reflexiva en un período de funcionamiento de 15 segundos.



```
Router(config)#ip access-list extended Lista_interna
Router(config-ext-nacl)#permit tcp any any eq 80 reflect trafico_web
Router(config-ext-nacl)#permit udp any any eq 53 reflect trafico_DNS
timeout 15
Router(config-ext-nacl)#exit
Router(config)#ip access-list extended Lista_externa
Router(config-ext-nacl)#evaluate trafico_web
Router(config-ext-nacl)#evaluate trafico_DNS
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#interface s0/0/1
Router(config-if)#description salida al ISP
Router(config-if)#ip access-group Lista_interna out
Router(config-if)#ip access-group Lista_externa in
Router(config-if)#exit
```

6.9 LISTAS DE ACCESO DINÁMICAS

La configuración básica de las ACL dinámicas, *lock-and-key*, comienza con la aplicación de una ACL extendida bloqueando el tráfico que pasa por el router y la configuración de telnet con autenticación local. Cuando el usuario hace telnet y se autentica, una ACL dinámica se agrega a la ACL extendida permitiendo el tráfico durante un período de tiempo particular. Es posible, además, la configuración de interrupciones por inactividad.

Las ACL dinámicas ofrecen beneficios extra de seguridad sobre las ACL estándar y extendidas:

- Mecanismo de desafío para autenticar usuarios individuales.
- Administración simplificada en grandes redes.
- Procesamiento reducido para ACL.
- Menores oportunidades para los hackers de forzar una entrada a la red.
- Creación de acceso dinámico de usuarios a través de un firewall, sin comprometer otras restricciones de seguridad configuradas.

El mecanismo de una ACL dinámica permite a un usuario abrir una conexión por telnet o SSH permitida por una ACL externa, entonces el usuario puede autenticarse a través de una base de datos local o a través de un servidor AAA que use los protocolos RADIUS o TACACS+.

Una vez que el usuario ha sido autenticado exitosamente, el IOS agrega una entrada a la ACL dinámica que ofrece acceso al usuario a los recursos internos configurados. No es posible establecer políticas de acceso por usuario. En su lugar, el administrador define una política para todos los usuarios de ACL dinámicas y esta política se aplica a todos los usuarios autenticados.

El primer paso en la configuración es crear o verificar que ya existan un usuario y contraseña.

```
Router(config)# username name password password
```

La siguiente sintaxis muestra el comando para la configuración de la lista de acceso dinámica. Posteriormente se debe aplicar a la interfaz correspondiente.

```
Router(config)# access-list {100-199} dynamic dynamic_ACL_name
[timeout minutes] {permit | deny} protocol source-addr [source-
wildcard] [operator port] destination-addr [destination-wildcard]
[operator port] [established]
```

Existen dos tipos de vencimiento, por inactividad y absoluto. El parámetro **timeout** es opcional y especifica un vencimiento absoluto en un rango posible de 1 a 9.999 minutos. El valor de vencimiento por inactividad se especifica por medio del comando **autocommand**, el cual habilita la autenticación *lock and key* en las líneas vty. Si no se especifican los tiempos de vencimiento, por defecto, la entrada nunca vencerá.

```
Router(config)# line vty 0 4
Router(config-line)# autocommand access-enable host [timeout
minutes]
```

EJEMPLO:

El host 10.20.20.3 con el nombre de usuario *ernesto* y contraseña *s3cury7i* realiza una conexión telnet al router 10.20.20.1, esto pone en funcionamiento la ACL dinámica. Posteriormente, la sesión se cierra haciendo posible que el usuario pueda acceder a la red 172.16.0.0. La interrupción por inactividad y la absoluta se configurarán a 10 y 15 minutos respectivamente.

```
Router(config)#username ernesto password 0 s3cury7i
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 10.20.20.1 255.255.255.0
Router(config-if)#ip access-group 100 in
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)#access-list 100 permit tcp any host 10.20.20.1 eq 23
Router(config)#access-list 100 dynamic ListaDinamica timeout 15
permit ip 10.20.20.0 0.0.0.255 172.16.0.0 0.0.0.255
Router(config)# line vty 0 4
Router(config-line)# autocommand access-enable host timeout 10
Router(config-line)# login local
```

6.10 LISTAS DE ACCESO BASADAS EN TIEMPO

Las ACL basadas en tiempo son básicamente ACL extendidas numeradas o nombradas. Las entradas basadas en tiempo pueden especificar el período de tiempo durante el que la sentencia ACL será válida. El período de tiempo especificado puede ser recurrente o una instancia específica que ocurra una sola vez.

El comando **time-range** permite habilitar el tiempo de validez de la sentencia. El nombre del rango permite asociar una sentencia específica de la ACL, dicho nombre debe comenzar con una letra y no puede contener espacios.

El comando **absolute** especifica un único período de tiempo para el cual el rango de tiempo es válido. Las sentencias de la ACL que hacen referencia a este rango de tiempo no son utilizadas luego de este período.

El comando **periodic** especifica un período de tiempo recurrente para el cual el rango de tiempo es válido. Se permiten múltiples comandos **periodic** dentro del mismo rango de tiempo.

La sintaxis de los comandos completos es la siguiente.

```
Router(config)# time-range time_range_name
Router(config-time-range)# absolute [start_time start_date]
[end_time end_date]
Router(config-time-range)# periodic day_of_the_week hh:mm to
[day_of_the_week] hh:mm
```

Donde:

- **start_time** / **end_time**: es el tiempo de inicio y finalización, especificado en formato 24 horas (hh:mm), donde las horas pueden ir desde 0 hasta 23 y los minutos, desde 0 hasta 59.

- **start_date / end_date**: es la fecha de inicio y finalización, donde el día se especifica como un número que puede ir de 1 a 31, el mes es el nombre del mes en inglés (puede utilizar el comando ayuda "?") y el año es un valor de cuatro dígitos.

- **day_of_the_week hh:mm**: es el día de inicio en inglés (puede utilizar el comando ayuda "?") y el tiempo de inicio, especificado como hh:mm.

- **to [day_of_the_week] hh:mm**: indica el día y la hora de finalización, si se omite este parámetro se utiliza el día configurado en el inicio.

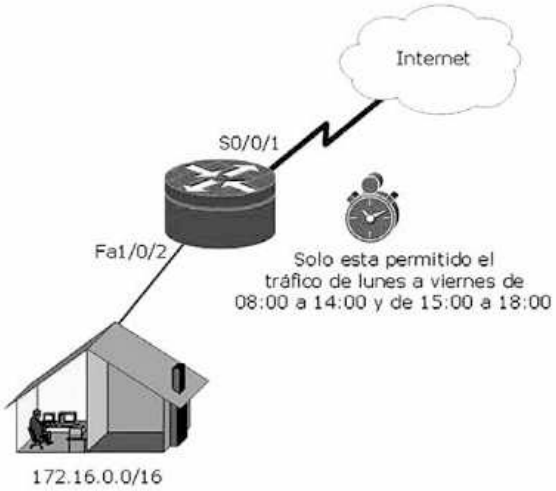
Una vez configurado el comando **time-range** se debe configurar una lista de acceso extendida con el añadido del parámetro **time-range**.

```
Router(config)# access-list {100-199} {permit | deny} protocol
source-addr [source-mask] [operator port] destination-addr
[destination-mask] [operator port] [established] [log | log-input]
[established] [time-range name_of_time_range]
```

EJEMPLO:

En el siguiente ejemplo una empresa necesita aplicar una política de seguridad para una pequeña oficina remota, de tal forma que solo durante el período de trabajo los empleados puedan conectarse a los servidores de la oficina central. De esta forma, durante los períodos de inactividad la entrada a dicha red permanece restringida.

```
Soho(config)# time-range red-servidores
Soho(config-time-range)# periodic weekdays 08:00 to 14:00
Soho(config-time-range)# periodic weekdays 15:00 to 18:00
Soho(config-time-range)# exit
Soho(config)# access-list 120 permit ip 172.16.0.0 0.0.255.255 any
time-range red-servidores
Soho(config)# access-list 120 deny ip any any
Soho(config)# interface FastEthernet 1/0/2
Soho(config-if)# ip access-group 120 in
Soho(config-if)# exit
```



NOTA:

En la configuración del parámetro del día de finalización, el comando ayuda mostrará la siguiente lista:

- ✓ *monday*
- ✓ *tuesday*
- ✓ *wednesday*
- ✓ *thursday*
- ✓ *friday*
- ✓ *saturday*
- ✓ *sunday*
- ✓ *daily (todos los días)*
- ✓ *weekdays (de lunes a viernes)*
- ✓ *weekend (sábado y domingo)*

6.11 VERIFICACIÓN DE LISTAS DE ACCESO

La primera y fundamental ayuda para verificar el funcionamiento de las ACL es el comando **show access-lists**. La salida del comando muestra cuántos paquetes coinciden con cada entrada de las ACL, lo cual permite monitorizar los paquetes específicos que han sido permitidos o denegados.

```
Switch# show access-lists 101
Extended IP access list 101
 permit tcp host 198.92.32.30 any established (4304 matches)
 permit udp host 198.92.32.30 any eq domain (129 matches)
 permit icmp host 198.92.32.30 any
 permit tcp host 198.92.32.30 host 171.9.2.41 gt 1023
 permit tcp host 198.92.32.30 host 171.9.2.35 eq smtp (2 matches)
 permit tcp host 198.92.32.30 host 198.92.30.32 eq smtp
 permit tcp host 198.92.32.30 host 171.69.108.33 eq smtp
 permit udp host 198.92.32.30 host 171.68.225.190 eq syslog
 permit udp host 198.92.32.30 host 171.68.225.126 eq syslog
 deny ip 50.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
 deny ip 71.6.0.0 0.0.0.255 224.0.0.0 0.255.255.255 (2 matches)
 deny ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
 deny ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
 deny ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
 deny ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
 deny ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
 deny ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
 deny ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
 deny ip 192.150.42.0 0.0.0.255 224.0.0.0 15.255.255.255
```

El comando **debug ip packet** es útil para analizar los mensajes que viajan entre los hosts locales y remotos. Tenga en consideración un uso prudencial de los comandos **debug** en redes en producción, ya que su ejecución genera una cantidad importante de información y usa considerablemente los recursos del sistema.

```
Router#debug ip packet detail 105
IP packet debugging is on (detailed) for access list 105

Router#
00:10:01: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-
Access1), g=10.10.10.2, len 100, forward
00:10:01: ICMP type=0, code=0
00:10:01: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-
Access1), g=10.10.10.2, len 100, forward
00:10:01: ICMP type=0, code=0
00:10:01: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-
Access1), g=10.10.10.2, len 100, forward
00:10:01: ICMP type=0, code=0
```

La opción **detail** muestra información de los códigos y tipos de paquetes, como los números de puerto de origen y destino. La "**g**" en la salida del comando indica el gateway del siguiente salto.

6.12 LISTAS DE ACCESO IPV6

El desempeño de las ACL estándar IPv6 es idéntico a las ACL IPv4. A partir de las IOS versión 12.0 (23) S y 12.2 (13) T o versiones posteriores esto se amplía también a las ACL extendidas. Para configurar una ACL IPv6, en primer lugar se debe entrar en el modo de configuración de ACL IPv6.

```
Router(config)# ipv6 access-list access-list-name
```

A continuación, configurar cada entrada de la lista de acceso para permitir o denegar tráfico específico.

```
Router(config-ipv6-acl)# {permit | deny} protocol {source-ipv6-
prefix/prefix-length | any | host source-ipv6-address | auth}
[operator port] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address | auth} [operator port]
```

Una vez creada la ACL se debe aplicar a una interfaz específica de entrada o salida.

```
Router(config-if)# ipv6 traffic-filter access-list-name {in | out}
```

La denegación implícita al final de cada ACL también está presente en las ACL IPv6, pero además hay algunos hechos adicionales a tener en cuenta.

- Cada ACL IPv6 contiene normas implícitas para permitir el descubrimiento de vecinos de IPv6. El proceso de descubrimiento de vecinos se sirve de la capa de red IPv6.
- Las ACL IPv6, por defecto, permiten enviar y recibir paquetes IPv6 en una interfaz.
- Las listas de acceso IPv6 niegan implícitamente todos los servicios que no estén específicamente permitidos.

Las reglas sobre el descubrimiento de vecinos IPv6 funcionan de manera similar a como lo hace ARP en IPv4. Estas reglas no se modifican aun cuando se aplica una ACL a una interfaz.

Las sentencias implícitas que se agregan al final de cada ACL IPv6 son las siguientes:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

donde:

- **nd-na** (*Neighbor Discovery-Neighbor Advertisement*): esta instrucción permite enviar los mensajes **na** que sirven para descubrir las direcciones de capa 2 de otros nodos.

- **nd-ns** (*Neighbor Discovery-Neighbor Solicitation*): esta instrucción permite recibir los mensajes **ns** que llegan como respuesta al mensaje **na** enviado previamente.

Estas reglas de descubrimiento de vecinos pueden ser modificadas anteponiendo la instrucción explícita **deny ipv6 any any**. En el caso de añadir una denegación explicita como esta, tendrá prioridad sobre los permisos implícitos sobre el descubrimiento de vecinos.

EJEMPLO:

La siguiente sintaxis es un ejemplo de una configuración básica de una ACL IPv6 nombrada "**CCNA**". En letras grises se detallan las sentencias implícitas.

```
Switch(comfit)# ipv6 access-list CCNA
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# permit icmp any any nd-na
Switch(config-ipv6-acl)# permit icmp any any nd-ns
Switch(config-ipv6-acl)# deny ipv6 any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface gigabitethernet 1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CCNA out
```

6.13 OBJECT GROUP

En las grandes redes corporativas, las ACL pueden contener cientos de líneas, siendo difíciles de configurar y administrar.

Las ACL basadas en **object group** son más pequeñas, más legibles y más fáciles de configurar y administrar que las ACL convencionales. Los object group permiten a un administrador clasificar a los usuarios, dispositivos y protocolos en

grupos, tanto para IPv4 como para IPv6. De esta forma se pueden aplicar a las ACL para crear políticas de control de acceso para un grupo determinado. Esta característica permite utilizar grupos en lugar de direcciones IP individuales, protocolos y puertos, que se utilizan en las ACL convencionales. Esto se traduce en un menor número de **ACE** (*Access Control Entries*), más manejable.

6.13.1 Características de los object group

Después de que un grupo se crea, será posible agregar objetos adicionales al mismo, simplemente siguiendo igual procedimiento al que se utiliza para la creación de un nuevo object group, en este caso, especificando el nombre del grupo ya existente y, a continuación, especificando los objetos adicionales.

Se pueden agrupar objetos tales como equipos o servicios. Después de agrupar los objetos, el comando se aplicará a todos los elementos del grupo.

No se puede eliminar un object group ni crear un object group vacío si se está utilizando en una ACE.

Al agrupar objetos similares, se puede utilizar una ACE para todo el object group en lugar de tener que introducir una ACE para cada objeto por separado.

6.13.2 Configuración de los object group

Un object group puede crearse con el comando **object-group**, este comando se aplica a cada elemento de ese grupo. Esta característica puede reducir significativamente el tamaño de su configuración.

Existen dos tipos de **object-group**:

- **Red**: pueden agruparse objetos como nombres de host, direcciones IP, subredes, rangos de direcciones IP o grupos de red ya existentes.
- **Servicio**: pueden agruparse objetos como protocolos de capa superior, protocolos que requieren puertos específicos (telnet o SNMP) protocolo ICMP y grupos de servicio ya existentes.

Los object group deben tener nombres únicos etiquetados debidamente para que se diferencien entre los dos tipos existentes.

La siguiente sintaxis muestra los comandos para la configuración de un network object group.

```
Router(config)# object-group network nw_grp_id

Router(config-network-group)# description description-text | host
{host-address | host-name} | network-address {/prefix-length |
network-mask} | range host-address1 host-address2 | any | group-
object nested-object-group-name
```

La siguiente sintaxis muestra los comandos para la configuración de un service object group.

```
Router(config)# object-group service svc_grp_id

Router(config-service-group)# protocol | [tcp | udp | tcp-udp
[source {{[eq]| lt | gt} port1 | range port1 port2}] [{[eq]| lt |
gt} port1 | range port1 port2]] | icmp icmp-type
```

En una ACL IPv4, los object group se aplican mediante la inclusión del parámetro **object-group** seguido por el nombre del grupo apropiado creado anteriormente. Tenga en cuenta que una ACE puede contener una mezcla de grupos y objetos individuales, como protocolos específicos, redes o servicios.

```
Router(config)# ip access-list extended name_of_ACL

Router(config-ext-nacl)# [line line_number] {permit | deny}
{protocol | object-group protocol_obj_grp_id} {source-
prefix/wildcard-mask | any | host source-address | object-group
network_obj_grp_id} [operator port} | object-group
service_obj_grp_id}] {destination-prefix/wildcard mask | any | host
destination-address | object-group network_obj_grp_id} [operator
port] | object-group service_obj_grp_id}] {[log [level]]}
```

Para el caso de las ACL IPv6 la sintaxis es la siguiente:

```
Router(config)# ipv6 access-list access-list-name

Router(config-ipv6-acl)# {permit | deny} {protocol | object-group
protocol_obj_grp_id} {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address | object-group network_obj_grp_id}[operator
port] | object-group service_obj_grp_id}] {destination-ipv6-
prefix/prefix-length | any | host destination-ipv6-address | object-
group network_obj_grp_id} [{operator port | object-group
service_obj_grp_id}]
```

Después de que un grupo de objetos se aplica a un ACE, el grupo de objetos no se puede borrar. Si los objetos adicionales se añaden al grupo después

de que se ha aplicado a la ACE, no hay necesidad de volver a aplicar el grupo con la ACE. La ACE se ajusta automáticamente para incluir los nuevos objetos que se adjuntan.

EJEMPLO:

El siguiente ejemplo muestra la configuración de un network object group llamado **grupo_de_red**, que contiene como objetos a dos host, un rango de direcciones IP y una subred.

```
Router> enable
Router# configure terminal
Router(config)# object-group network grupo_de_red
Router(config-network-group)# host 10.99.20.52
Router(config-network-group)# host 10.99.20.54
Router(config-network-group)# range 10.99.20.23 10.99.20.28
Router(config-network-group)# 10.99.50.243 255.255.255.224
```

La siguiente sintaxis muestra la configuración de un network object group llamado **red_de_servidores** que contiene como objetos dos host, una subred y un *object group* ya existente llamado **Servidores_FTP**.

```
Router> enable
Router# configure terminal
Router(config)#object-group network red_de_servidores
Router(config-network-group)# host sjc.eng.ftp
Router(config-network-group)# host 10.99.20.242
Router(config-network-group)# 10.99.20.225 255.255.255.224
Router(config-network-group)# group-object Servidores_FTP
```

El siguiente ejemplo muestra la configuración de un service object group llamado **grupo_de_servicio** que contiene varios protocolos como ICMP, TCP, UDP y TCP-UDP además un object group existente llamado **ingenieria_de_servicio**.

```
Router> enable
Router# configure terminal
Router(config)# object-group service grupo_de_servicio
Router(config-service-group)# icmp echo
Router(config-service-group)# tcp smtp
Router(config-service-group)# tcp telnet
Router(config-service-group)# tcp source range 1 65535 telnet
Router(config-service-group)# udp domain
Router(config-service-group)# tcp-udp range 2000 2005
Router(config-service-group)# group- ingenieria_de_servicio
```

A continuación se crea una ACL basada en object group llamada **ACL_de_grupos** que permitirá enviar paquetes a los usuarios del object group llamado **grupo_de_red**, siempre y cuando los puertos de los protocolos coincidan con los especificados en el object group llamado **grupo_de_servicio**.

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended ACL_de_grupos
Router(config-ext-nacl)# permit object-group grupo_de_servicio
object-group grupo_de_red any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Finalmente, la ACL basada en grupos se aplica a una interfaz.

```
Router> enable
Router# configure terminal
Router(config)# interface vlan 200
Router(config-if)# ip access-group ACL_de_grupos in
Router(config-if)# end

Router# show ip access-list ACL_de_grupos
```

La siguiente sintaxis es un ejemplo de verificación de los object group.

```
Router# show object-group

Network object group auth_proxy_acl_deny_dest
 host 209.165.200.235

Service object group auth_proxy_acl_deny_services
 tcp eq www
 tcp eq 443

Network object group auth_proxy_acl_permit_dest
 209.165.200.226 255.255.255.224
 209.165.200.227 255.255.255.224
 209.165.200.228 255.255.255.224
 209.165.200.229 255.255.255.224
 209.165.200.246 255.255.255.224
 209.165.200.230 255.255.255.224
 209.165.200.231 255.255.255.224
 209.165.200.232 255.255.255.224
 209.165.200.233 255.255.255.224
 209.165.200.234 255.255.255.224

Service object group auth_proxy_acl_permit_services
 tcp eq www
 tcp eq 443
```

6.14 FUNDAMENTOS PARA EL EXAMEN

- Este capítulo puede convertirse en complicado si no se tienen los conceptos claros. Es fundamental entender el diseño de las ACL. Si es necesario, realice un repaso del temario del CCNA.
- Practique el funcionamiento y el cálculo de las wilcard.
- Aprenda claramente la diferencia entre ACL saliente y ACL entrante.
- Lea detenidamente las consideraciones para el diseño de una ACL.
- Estudie el rango de cada una de las ACL, sepa para qué sirve cada tipo y en qué casos se utilizan.
- Realice configuraciones de todos los tipos de ACL, analice su funcionamiento, saque conclusiones.
- Estudie el funcionamiento de los object group, realice configuraciones.

Capítulo 7

FIREWALLS

7.1 REDES SEGURAS CON FIREWALLS

El firewall es un dispositivo, sistema o grupo de sistemas que aplica una política restrictiva en el control de acceso en las redes.

Al principio, los firewalls inspeccionaban los paquetes para ver si coincidían con grupos de reglas preestablecidas, con la opción de reenviar o descartar paquetes. Este tipo de filtrado de paquetes, llamado *stateless*, funciona sin importar si el paquete es parte de un flujo de datos existente. Cada paquete se filtra de manera similar a una ACL, basándose exclusivamente en los valores de los parámetros contenidos en el encabezado del paquete.

Los firewalls sin estados no son dispositivos autónomos, la funcionalidad de firewall es proporcionada por los routers o servidores de la red.

Los firewalls con estados filtran los paquetes basándose en la información extraída de los datos que fluyen y se almacenan en él. Este tipo de firewall stateful es capaz de determinar si un paquete pertenece a un flujo de datos existente. Las reglas estáticas, como las de los firewalls stateless, son suplementadas por reglas dinámicas creadas en tiempo real para definir estos flujos activos. Los firewalls con estados ayudan a mitigar ataques de DoS que explotan conexiones activas a través de dispositivos de red.

NOTA:

El primer firewall data de 1988, cuando DEC creó el primer dispositivo de red destinado al filtrado de paquetes. Al año siguiente, en 1989, AT&T Bell Laboratories desarrolló el primer firewall con estados.

7.1.1 Características de los firewalls

Algunos de los beneficios del uso de los firewall en una red pueden ser:

- Previenen la exposición de los hosts y las aplicaciones sensibles a usuarios no confiables.
- Examinan el flujo de datos de los protocolos, previniendo la explotación de fallos en los mismos.
- Puede bloquearse el acceso de datos maliciosos a servidores y clientes.
- Hace que la aplicación de una política de seguridad se torne simple, escalable y robusta.
- Mejora la administración de la seguridad de la red al reducir el control de acceso a la misma.

Los firewalls también tienen limitaciones:

- Si está mal configurado, el firewall puede tener consecuencias serias.
- Muchas aplicaciones no pueden pasar a través del firewall en forma segura.
- Los usuarios pueden intentar buscar maneras de sortear el firewall para recibir material bloqueado, exponiendo la red a potenciales ataques.
- El rendimiento de la red puede disminuir.
- Puede hacerse tunneling de tráfico no autorizado o puede disfrazárselo como tráfico legítimo.

7.1.2 Tipos de firewall

Antes de adoptar alguna de las varias opciones de solución de firewall, es importante llevar a cabo un análisis de coste contra los posibles riesgos. No siempre la solución más costosa es la más adecuada.

Cualquiera que sea la decisión que se tome en la adquisición de una solución de firewall, es crítico contar con un diseño de red apropiado para el desarrollo exitoso del firewall. Hay varios tipos de firewalls de filtrado, incluyendo los siguientes.

- **Firewall de filtrado de paquetes**: trabajan principalmente en la capa de Red del modelo OSI y generalmente se los considera dispositivos de capa 3. Sin embargo, analizan tráfico basándose en información de capa 4 como protocolo y números de puerto de origen y destino. El filtrado de paquetes utiliza las ACL para determinar si permite o deniega tráfico basándose en direcciones IP de origen y destino, protocolo, tipo de paquete y números de puerto origen y destino. Los firewalls de filtrado de paquetes generalmente son parte de un router con funcionalidad de firewall.

- **Stateful firewall**: los firewalls con estados son la tecnología de firewall más versátil y común en uso actualmente, están clasificados como de capa de red. Proporcionan filtrado de paquetes con estados utilizando la información de conexiones establecidas, almacenadas en una tabla de estados. Los firewalls con estados usan dicha tabla para monitorizar el proceso de comunicación. El dispositivo examina la información en los encabezados de paquetes de capa 3, aunque, para algunas aplicaciones, también puede analizar tráfico de capas 4 y 5. Cada vez que se accede a un servicio externo, el firewall stateful retiene ciertos detalles de la solicitud y guarda el estado de la solicitud en la tabla de estados. Dicha tabla contiene las direcciones de origen y destino, los números de puertos, información de secuencias TCP y etiquetas adicionales por cada conexión TCP o UDP asociada con esa sesión particular. Cuando el sistema externo responde a una solicitud, el firewall compara los paquetes recibidos con el estado previamente almacenado para permitir o denegar el acceso a la red. El firewall permite la entrada de datos solo si existe una conexión apropiada que justifique su paso.

- **Proxy firewall**: filtra según información de las capas 3, 4, 5 y 7 del modelo de referencia OSI. La mayoría del control y filtrado del firewall se hace por software.

- **Firewall de traducción de direcciones** (NAT): aunque la inspección con estados proporciona velocidad y transparencia, los paquetes dentro de la red deben poder salir de la red. Esto puede exponer las direcciones IP internas a potenciales atacantes. El **NAT firewall** aumenta el número de direcciones IP disponibles y oculta el diseño del direccionamiento interno de la red. La mayoría de los firewalls y servidores proxy llevan incorporada, para mayor seguridad, la traducción de direcciones de red.

- **Host-based firewall**: el firewall basado en hosts ejecuta un software de firewall tanto para un servidor como para un ordenador personal.

- **Transparent firewall**: el firewall transparente filtra el tráfico IP entre dos interfaces conmutadas.

- **Hybrid firewall**: es una combinación de varios tipos diferentes de firewalls. Un firewall híbrido puede funcionar combinando un firewall con estados y un firewall de gateway de aplicación.

NOTA:

Cisco Systems lanzó al mercado tres soluciones firewalls:

- ✓ ***Firewall IOS**: es una función especializada del IOS que se ejecuta en los routers Cisco. Es un firewall de calidad profesional que soporta pequeñas y medianas empresas y oficinas sucursales.*

- ✓ ***Cisco PIX Security Appliance**: es un dispositivo autónomo que asegura una robusta ejecución de las políticas de usuario y aplicación contra ataques y servicios de conectividad segura.*

- ✓ ***ASA** (Adaptive Security Appliances): es una solución de fácil despliegue que integra capacidades de software, seguridad en comunicaciones unificadas de voz y vídeo, SSL y VPN IPsec, IPS y servicios de seguridad de contenidos. Los ASA fueron diseñados para proteger redes de todos los tamaños y bajar los costos generales de despliegue y operación para la empresa al proporcionar una seguridad global multicapa.*

7.1.3 Diseño de redes con firewalls

La seguridad en redes consiste en crear y mantener una política de seguridad, incluyendo una política de seguridad de firewall. Las siguientes recomendaciones sirven como punto de inicio para implementar una política de seguridad con firewall.

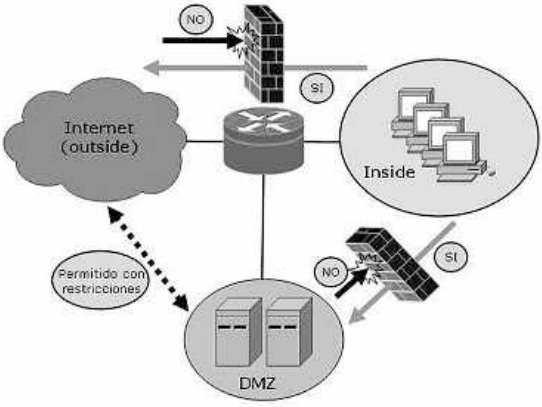
- Instalar los firewalls en las fronteras de seguridad claves.
- Los firewalls son el principal dispositivo de seguridad, pero no es aconsejable depender exclusivamente de ellos para la seguridad de una red.
- Denegar todo el tráfico por defecto y permitir solo los servicios necesarios.
- Asegurar que el acceso físico al firewall esté controlado.
- Monitorizar regularmente los registros del firewall.
- Administrar y controlar regularmente la configuración en el firewall.
- Los firewalls protegen principalmente contra ataques técnicos que se originan fuera de la red. Los ataques internos tienden a no ser de naturaleza técnica.

Algunos diseños son tan simples como la designación de una red externa y una interna, determinadas por dos interfaces en un firewall. La red externa no es confiable, mientras que la interna sí lo es. El tráfico proveniente de la red interna, pasa a través del firewall hacia afuera con pocas o ninguna restricción. El tráfico que se origina fuera generalmente es bloqueado o permitido muy selectivamente. Al tráfico de retorno que proviene de la red externa, asociado con tráfico de origen interno, se le permite pasar de la interfaz no confiable a la confiable.

Un diseño más complicado puede involucrar tres o más interfaces en el firewall. En este caso, generalmente se trata de una interfaz externa, una interna y una **DMZ** (*Demilitarized Zone*). En la seguridad de las redes, a menudo se hace referencia a una zona desmilitarizada como una porción de red conectada con un firewall donde es común permitir tipos específicos de tráfico desde fuera.

Las características de este diseño se resumen en:

- El flujo de tráfico circula libremente de la interfaz interna a la externa y la DMZ.
- Se permite libremente el paso del tráfico que proviene de la DMZ por la interfaz externa.
- El tráfico de la interfaz externa generalmente se bloquea salvo que esté asociado con tráfico de origen interno o de la DMZ.
- En interfaz DMZ es común permitir tráfico desde fuera, siempre que sea el tipo de tráfico correcto y que su destino sea la DMZ (por ejemplo correo electrónico, DNS, HTTP o HTTPS).



En un escenario de defensa por capas, los firewalls proporcionan seguridad perimetral de toda la red y de los segmentos de red internos en el núcleo.

La defensa por capas usa diferentes tipos de firewalls que se combinan para agregar profundidad a la seguridad de la organización. El tráfico sigue la siguiente secuencia:

1. El tráfico que ingresa de la red no confiable se topa con un filtro de paquetes inicial en el router más externo.
2. El tráfico se dirige a un potente firewall dentro de la DMZ donde se aplican más reglas al tráfico y se descartan paquetes sospechosos.

3. El tráfico apunta ahora al router interior, donde se moverá al host de destino interno solo si ha superado con éxito el filtrado entre el router externo y la red interna.

Las recomendaciones finales en el diseño de una red con firewalls pueden ser las siguientes.

- Un número importante de las intrusiones proviene de hosts dentro de la red.
- Los firewalls no ofrecen protección contra instalaciones de módems no autorizadas.
- El firewall no puede reemplazar a los administradores y usuarios informados.
- Una defensa profunda debe incluir almacenamiento externo para resguardo y recuperación de desastres y una topología de hardware redundante.

7.2 CONTROL DE ACCESO BASADO EN EL CONTEXTO

CBAC (*Context-Based Access Control*) es una solución disponible dentro del firewall Cisco IOS. CBAC filtra inteligentemente los paquetes TCP y UDP en base a la información obtenida de la sesión de protocolo de capa de aplicación. CBAC detecta y previene contra la mayoría de los ataques más populares de las redes. CBAC solo ofrece filtrado para los protocolos especificados si el tráfico pasa a través de un router. Si el protocolo no está especificado, las ACL existentes determinarán el filtrado del protocolo.

Las principales características de CBAC son las siguientes.

- Examina las conexiones soportadas para ejecutar las traducciones de direcciones necesarias basándose en la información de NAT y PAT contenida en el paquete. Cuando NAT o PAT está habilitado cambia las direcciones IP y números de puerto basándose en la información de la tabla de traducción de direcciones.
- Puede bloquear conexiones peer-to-peer (P2P) así como también el tráfico de mensajería instantánea.

- Filtra el tráfico para permitir el paso de retorno en conexiones TCP y UDP específico a través del firewall cuando la conexión se inicia dentro de la red. Logra esto al crear entradas temporales en una ACL que de otra manera denegaría el tráfico. Si una conexión TCP no se establece dentro de los 30 segundos luego de la recepción del primer segmento SYN, o no se detecta actividad por más de 60 minutos se elimina la entrada de la tabla de estados y de la ACL.

- Inspecciona paquetes de capa de aplicación y mantiene información de sesiones TCP y UDP, puede detectar y prevenir ciertos tipos de ataques de red como inundación SYN. También contribuye a la protección contra ataques de DoS inspeccionando los números de secuencia de los paquetes de las conexiones TCP para ver si están dentro de los rangos esperados y los descarta si le resultan sospechosos.

- Inspecciona las consultas y respuestas DNS. Cuando un dispositivo interno genera una consulta DNS, CBAC espera que el servidor DNS envíe una respuesta dentro de un período de 5 segundos, si no lo hace la entrada ACL dinámica se elimina para evitar un posible ataque de falsificación. Los tiempos de conexión UDP si no se detecta tráfico tienen como límite 30 segundos, luego la entrada de la tabla de estados se elimina.

- Proporciona una cantidad limitada de conexiones ofreciendo protección contra ataques SMTP específicos. Con la detección de intrusos, los mensajes syslog son inspeccionados en búsqueda de determinados ataques. Cuando CBAC detecta un ataque basado en estas características, reinicia las conexiones en cuestión y envía información al servidor syslog.

- Inspecciona tráfico ICMP como solicitud de eco, respuesta eco, destino inalcanzable, tiempo excedido, solicitud y respuesta de marca de tiempo. CBAC espera respuesta de los mensajes soportados por un lapso de 10 segundos, transcurrido ese tiempo la conexión ICMP se elimina de la tabla de estados y la entrada ACL dinámica se descarta.

- Genera alertas en tiempo real y registros de auditorías. Las funciones de registros de auditoría monitorizan todas las transacciones de red y registran las marcas de tiempo, hosts de origen y destino, puertos utilizados y el número total de bytes transmitidos. Las alertas en tiempo real envían mensajes syslog cuando detectan actividad sospechosa.

7.2.1 Funcionamiento de CBAC

CBAC crea entradas en las ACL de las interfaces del firewall agregando una entrada temporal en la ACL para una sesión específica. Estas entradas son creadas cuando cierto tráfico específico sale de la red interna protegida a través del firewall.

Con CBAC, los protocolos que serán inspeccionados se especifican en una regla de inspección. La regla de inspección se aplica a una interfaz en una dirección (de entrada o de salida) cuando se aplica la inspección. El motor del firewall inspecciona solo los paquetes de los protocolos especificados si ya han pasado por la ACL de entrada que se aplica a la interfaz interna. Si la ACL deniega un paquete, el paquete se descarta y no es inspeccionado por el firewall.

Las entradas temporales permiten el ingreso del tráfico de retorno que normalmente sería bloqueado si no fuesen parte de la misma sesión y con las mismas propiedades esperadas que el tráfico original que disparó al CBAC cuando salió por el firewall. Sin esta entrada temporal en la ACL, este tráfico sería denegado por la propia ACL existente. La tabla de estados cambia dinámicamente y se adapta con el flujo de tráfico.

Sin CBAC, el filtrado de tráfico se limita a implementaciones básicas de una ACL que examina paquetes en la capa de red o, a lo sumo, la capa de transporte. CBAC usa un filtro de paquetes con estados que es sensible a las aplicaciones. Esto significa que el filtro es capaz de reconocer todas las sesiones de una aplicación dinámica. CBAC examina no solo la información de las capas de red y de transporte, sino también la información de protocolo de capa de aplicación para conocer el estado de la sesión.

Cuando un paquete TCP sale de la red interna a través de una interfaz externa del firewall donde TCP se ha configurado para la inspección CBAC ocurre lo siguiente.

1. El paquete llega a la interfaz externa del firewall.

2. El paquete es evaluado con la lista de acceso existente en la interfaz de salida, si el paquete es denegado simplemente se elimina, si el paquete es permitido continúa el proceso de inspección CBAC.

3. El paquete es inspeccionado por CBAC para determinar y registrar la información sobre el estado de la conexión del paquete. Esta información se registra en una entrada en la nueva tabla de estado creada para la nueva conexión.

4. Basándose en la información de estado obtenida, CBAC crea una entrada temporal en lista de acceso que se inserta en el principio de la ACL aplicada la interfaz externa. Esta entrada temporal en la lista de acceso está diseñada para permitir paquetes entrantes que forman parte de la misma conexión que el paquete saliente que acaba de ser inspeccionado.

5. El paquete saliente se reenvía a la interfaz.

6. Más tarde, un paquete entrante llega a la interfaz. Este paquete es parte de la conexión establecida previamente con el paquete de salida. El paquete de entrada se evalúa en la lista de acceso de entrada, y se permite debido a la entrada de la lista de acceso temporal creada anteriormente.

7. El paquete entrante permitido es inspeccionado por CBAC, la entrada de la conexión en la tabla de estado se actualizará. Basándose en la información de estado actualizada, las entradas temporales en la ACL entrante podrían ser modificadas con el fin de permitir solo los paquetes que son válidos para el estado actual de la conexión.

8. Todos los paquetes entrantes o salientes adicionales que pertenecen a la conexión son inspeccionados para actualizar la entrada en la tabla de estado y modificar las entradas temporales de la lista de acceso entrante según sea necesario, y se envían a través de la interfaz.

9. Cuando termina la conexión o el tiempo de espera supera el máximo permitido, la entrada en la tabla de estado y las entradas temporales de la lista de acceso entrante se eliminan.

7.2.2 Configuración de CBAC

El primer paso en la configuración de CBAC es la elección de las interfaces internas y externas donde se aplicará la inspección. Las interfaces donde las sesiones se inicien se considerarán como interfaces internas.

- Un escenario típico es el de dos interfaces en el que una se conecta con la red externa y la otra con la red interna protegida. CBAC evitará que el tráfico de ciertos protocolos ingrese al firewall y a la red interna, salvo que sea parte de una sesión iniciada en la red interna.

- En un contexto más complejo de tres interfaces en el que la primera se conecta con la red externa, la segunda con una red en la DMZ y la tercera con la red protegida interna, el firewall puede permitir el paso de tráfico externo a recursos dentro de la DMZ y a su vez evitar que el tráfico de protocolos específicos ingrese a la red interna, salvo que sea parte de una sesión iniciada en la red interna.

El siguiente paso consiste en configurar ACLs en una interfaz para filtrar el tráfico de entrada, de salida o ambos. Cuando las redes de ambos lados del firewall requieran protección, como en configuraciones extranet e intranet, y para la protección contra ataques de DoS, configure el firewall en dos direcciones. Las ACL deben estar definidas para cada protocolo habilitado en la interfaz para controlar el flujo de tráfico de ese protocolo.

Inicie el proceso de configuración teniendo en cuenta las siguientes recomendaciones.

1. Siguiendo las reglas básicas de configuración de las ACL, determine qué tipo de tráfico reenviar o bloquear en las interfaces del router. Para que el firewall Cisco IOS cree dinámicamente las entradas temporales, la ACL del tráfico de retorno debe ser extendida.

2. Permita el tráfico que deberá inspeccionar el firewall Cisco IOS.

3. Configure protección antifalsificación denegando todo el tráfico de entrada en una interfaz externa cuya dirección de origen coincida con una dirección de red protegida. La protección antifalsificación evita que el tráfico de la red no protegida asuma la identidad de un dispositivo de la red protegida.

4. Configure una entrada para prevenir ataques de broadcast denegando la dirección de origen 255.255.255.255.

5. Por defecto, la última entrada en las ACL es una denegación implícita de todo el tráfico IP que no está permitido específicamente en las otras entradas de la ACL.

6. Deniegue el tráfico IP con cualquier dirección de origen o destino, explicitando así la regla de denegación.

7. Recuerde que, por defecto, la última entrada en las ACL es una denegación implícita de todo el tráfico IP.

8. Si el firewall solo tiene dos conexiones, una a la red interna y otra a la red externa, la aplicación de ACL debe ser de entrada en ambas interfaces porque los paquetes serán detenidos antes de tener oportunidad de afectar al router.

El siguiente paso es definir las reglas de inspección para especificar qué protocolos de capa de aplicación inspeccionar en una interfaz. Cuando sea necesario habilitar el motor del firewall en dos direcciones en una sola interfaz pueden configurarse dos reglas, una por cada dirección.

La regla de inspección consiste en una serie de sentencias, cada una especificando el protocolo y el mismo nombre de regla de inspección. La inspección de TCP genérico y UDP permite dinámicamente el tráfico de retorno de las sesiones activas. La inspección de ICMP permite que los paquetes de respuesta de eco se reenvíen como una respuesta a mensajes eco ICMP previamente enviados. Las reglas de inspección incluyen opciones para el control de mensajes de alerta y registro de auditoría.

La siguiente sintaxis muestra cómo se configuran las reglas de inspección:

```
Router(config)# ip inspect name inspection_name protocol [alert {on
| off}] [audit-trail {on | off}] [timeout seconds]
```

Donde:

- **inspection_name**: identifica un grupo de reglas de inspección, pueden agregarse más protocolos a una regla existente utilizando el mismo nombre de inspección.
- **protocol**: determina el protocolo a inspeccionar.
- **alert** {**on** | **off**}: es un parámetro opcional que sirve para generar mensajes de alerta para cada protocolo inspeccionado. Cuando esta opción no está configurada, las alertas se generan basándose en el comando **ip inspect alert-off**.
- **audit-trail** {**on** | **off**}: es un parámetro opcional que genera auditorías. Cuando esta opción no está configurada, las auditorías se generan basándose en el comando **ip inspect audit-trail**.
- **timeout seconds**: los vencimientos por inactividad TCP o UDP pueden establecerse opcionalmente para un determinado protocolo. Este parámetro invalida los tiempos de vencimiento por inactividad globales de TCP y UDP, pero no invalida dichos tiempos para DNS.

El último paso en el proceso de configuración de CBAC consiste en aplicar la regla de inspección a la interfaz elegida. Tome en cuenta estas dos sencillas recomendaciones:

- En la interfaz en la que se inicia el tráfico, aplique una ACL en la dirección de entrada para permitir solo el tráfico solicitado y aplique la regla en la dirección de entrada para inspeccionar el tráfico solicitado.

- En las otras interfaces, aplique una ACL en la dirección de entrada para denegar todo el tráfico, excepto el tráfico que no ha sido inspeccionado por el firewall, como GRE o ICMP, que no está relacionado con mensajes de solicitud de eco y su respuesta.

La siguiente sintaxis muestra el comando para activar la inspección en la interfaz.

```
Router(config-if)# ip inspect inspection_name {in | out}
```

EJEMPLO:

La siguiente sintaxis muestra cómo se ha habilitado CBAC en un router. Para el nombre de la inspección se ha utilizado **Security**.

```
ip inspect name Security icmp router-traffic
ip inspect name Security tcp router-traffic
ip inspect name Security udp router-traffic

access-list 151 deny ip any any

interface FastEthernet0/0
description *Conexion_WAN*
ip address 1.1.1.1 255.255.255.0
ip access-group 151 in
ip nat outside
no shut

interface FastEthernet0/1
description *Conexion_LAN*
ip address 192.168.10.1 255.255.255.0
ip nat inside
ip inspect Security in
no shut

CBAC(config)#ip inspect audit-trail
CBAC(config)#logging buffered debugging
```

```
CBAC(config)#logging on
CBAC#
*Mar 1 00:38:30.851: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp
session: initiator (192.168.10.2:56162) -- responder (2.2.2.2:23)

CBAC#sh ip inspect sessions
Established Sessions
Session 669F632C (192.168.10.2:56162)=>(2.2.2.2:23) tcp SIS_OPEN


CBAC#sh ip inspect sessions detail
Established Sessions
 Session 669F632C (192.168.10.2:56162)=>(2.2.2.2:23) tcp SIS_OPEN
 Created 00:00:11, Last heard 00:00:05
 Bytes sent (initiator:responder) [42:90]
 In SID 2.2.2.2[23:23]=>1.1.1.4[56162:56162] on ACL INBOUND (18
matches)
```

7.2.3 Verificación de CBAC

CBAC soporta muchos comandos **show** que pueden ser utilizados para ver las entradas temporales creadas en una ACL, la tabla de estados y la operación de CBAC. El siguiente comando muestra información sobre las inspecciones CBAC.

```
Router# show ip inspect parameter
```

Parámetro	Descripción
`name inspection_name`	Limita lo que se muestra a las reglas de inspección especificadas.
`config`	Muestra toda la configuración de la inspección CBAC del router.
`interfaces`	Muestra las reglas activadas en las interfaces del router.
`sessions`	Muestra un resumen de las conexiones en la tabla de estados CBAC.
`sessions [detail]`	Muestra al detalle las conexiones en la tabla de estados CBAC.
`all`	Muestra toda la información de las opciones de la lista de esa tabla.

El comando **debug ip inspect** puede inspeccionar varias aplicaciones y otros detalles de operación. Estos comandos permiten ver en tiempo real cómo opera CBAC en el router.

```
Router# debug ip inspect protocol parameter
```

Parámetro	Descripción
`tcp`	Muestra eventos de inspección TCP.
`udp`	Muestra eventos de inspección UDP.
`icmp`	Muestra eventos de inspección ICMP.
`application_name`	Muestra eventos de inspección de la aplicación especificada.
`events`	Muestra eventos CBAC, incluye el procesamiento de paquetes.
`object-creation`	Muestra información sobre la adición de una entrada a la tabla de estados.
`object-deletion`	Muestra información sobre la eliminación de una entrada en la tabla de estados.
`function-trace`	Muestra información sobre las funciones de software que CBAC llama.
`timers`	Muestra información relacionada con los temporizadores.
`detailed`	Muestra información relacionada con los procesos CBAC en el router.

NOTA:

A partir de la versión 12.4(20)T del IOS de Cisco, el comando **debug policy-firewall** *reemplaza al comando* **debug ip inspect**.

EJEMPLO:

La siguiente sintaxis muestra la salida del comando **show ip inspect all**.

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
 tcp timeout 3600
 udp timeout 30
 ftp timeout 3600
Interface Configuration
 Interface Ethernet0
 Inbound inspection rule is all
 tcp timeout 3600
 udp timeout 30
 ftp timeout 3600
 Outgoing inspection rule is not set
 Inbound access list is not set
 Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (30.0.0.1:46065)=>(40.0.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (40.0.0.1:20)=>(30.0.0.1:46072) ftp-data SIS_OPEN
```

Las siguientes son las dos formas de registro que soporta la inspección CBAC.

- **Las alertas** muestran mensajes relacionados con la operación de CBAC, como recursos insuficientes del router, ataques de DoS y otras amenazas.

- **Las auditorías** monitorizan las conexiones que CBAC inspecciona, incluyendo intentos de acceso válidos y no válidos.

Las alertas están habilitadas por defecto y se muestran automáticamente en la consola del router. Pueden ser habilitadas y deshabilitadas globalmente y por reglas de inspección, aunque es altamente recomendable que las alertas permanezcan habilitadas. La siguiente sintaxis muestra el comando para habilitar las alertas.

```
Router(config)# ip inspect alert-off
```

El registro de auditoría proporciona información estadística básica sobre la conexión. La auditoría está deshabilitada por defecto, pero puede ser habilitada con el siguiente comando.

```
Router(config)# ip inspect audit-trail
```

Por defecto, tanto las alertas como las auditorías se muestran en la línea de consola. Esta información puede ser registrada en otros dispositivos, incluyendo el buffer interno del router o un servidor syslog externo.

EJEMPLO:

En el ejemplo se muestra cómo después de configurar el **comando ip inspect audit-trail**, aparecen los mensajes de auditoría.

```
Router(config)# ip inspect audit-trail

%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192)
sent 22 bytes -- responder (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194)
sent 336 bytes -- responder (192.168.129.11:21) sent 325 bytes
```

7.3 FIREWALL BASADO EN ZONAS

El firewall basado en zonas permite la aplicación de diferentes políticas de inspección a múltiples grupos de hosts conectados a la misma interfaz del router. De esta forma, las interfaces son asignadas a zonas y luego se aplica una política de inspección al tráfico que se mueve entre dichas zonas.

El ZPF (*Zone-based Policy Firewall* [ZBF o ZFW]) se implementó a partir de la versión 12.4(6)T de Cisco IOS, soporta las funciones de firewalls anteriores, incluyendo inspección de paquetes con estados, inspección de aplicaciones, filtrado de URL y mitigación de ataques de DoS.

Con CBAC el proceso de inspección depende excesivamente de las ACL. Todo el tráfico que pasa por una interfaz está sujeto a la misma inspección, no pueden aplicarse políticas a un grupo de hosts o subredes. Otro cambio significativo es la introducción del Cisco Common Classification Policy Language (C3PL). Este nuevo lenguaje de configuración de políticas facilita una visión modular sobre la implementación de firewalls.

ZPF proporciona un enfoque estructurado basado en zonas útil para la documentación y la comunicación. La zona en sí define una frontera en la que el tráfico está sujeto a restricciones de políticas cuando cruza a otra región de la red. La política por defecto entre las zonas es la de denegar todo.

NOTA:

En CBAC, el tráfico está permitido implícitamente hasta que es explícitamente bloqueado con una ACL. Por el contrario en ZPF, todo el tráfico que intente moverse entre las zonas será denegado.

Algunas de las diferencias entre CBAC y ZPF pueden resumirse en las siguientes.

- ZPF no depende exclusivamente de las ACL mientras que CBAC sí.
- La postura de seguridad del router es la de bloquear salvo que sea explícitamente permitido.
- Con ZPF las políticas son de fácil lectura y C3PL permite una rápida resolución de problemas. En CBAC las múltiples políticas de inspección en varias interfaces del router dificultan la correlación de las políticas del tráfico entre diferentes interfaces.
- Una política afecta a cualquier tráfico dado, en lugar de necesitar múltiples ACL y acciones de inspección.
- ZPF y CBAC pueden implementarse al mismo tiempo en el router; sin embargo, los modelos no pueden ser combinados en la misma interfaz.

7.3.1 Funcionamiento del firewall basado en zonas

La infraestructura de la red debe estar dividida en zonas con diferentes niveles de seguridad.

Debe considerarse la división lógica en zonas jerárquicas independientemente del número de dispositivos, profundidad de la defensa, redundancia, etc.

Se deben establecer políticas entre cada par de zonas origen-destino para el tráfico que no está basado en el concepto de sesiones, y definir flujos de tráfico unidireccionales desde el origen al destino y viceversa.

Luego de identificar las zonas y documentar los requerimientos de tráfico, el siguiente paso consiste en diseñar la infraestructura física tomando en cuenta los requerimientos de seguridad y disponibilidad. Esto incluye la estimación del número de dispositivos entre las zonas más seguras y las menos seguras y la determinación de dispositivos redundantes. En cada dispositivo firewall del diseño se deben identificar subconjuntos en las zonas conectadas a sus interfaces y enlazar los requerimientos de tráfico en esas zonas.

Una vez concebido, este modelo el firewall puede llevar a cabo tres funciones específicas.

- **Inspect**: esta acción es equivalente al comando **ip inspect** en CBAC. El tráfico de retorno y potenciales mensajes ICMP son permitidos. Maneja el correcto establecimiento de las sesiones para los protocolos que requieren múltiples sesiones paralelas de señalización y de datos.

- **Drop**: semejante a una sentencia **deny** en una ACL. Puede configurarse la opción **log** para registrar los paquetes rechazados.

- **Pass**: semejante a una sentencia **permit** en una ACL, no se monitorizan el estado de las conexiones o sesiones dentro del tráfico. El tráfico se permite en una sola dirección. Debe aplicarse una política correspondiente para permitir el paso del tráfico de retorno en la dirección opuesta.

Las interfaces del router que pertenecen a zonas están sujetas a reglas que rigen el comportamiento de las interfaces, de la misma forma lo está el tráfico que se mueve entre interfaces que pertenecen a una zona.

- La zona debe configurarse antes de que se asignen interfaces a ella.

- Si el tráfico debe fluir entre todas las interfaces de un router, cada interfaz debe ser miembro de una zona.

- Se puede asignar una interfaz a solo una zona de seguridad.

- El flujo del tráfico se permite implícitamente entre las interfaces que pertenecen a la misma zona.

- Para permitir el tráfico desde y hacia una interfaz que pertenece a una zona, debe configurarse una política que permita o inspeccione el tráfico entre esa zona y cualquier otra.

- El tráfico no puede fluir entre una interfaz perteneciente a una zona y cualquier otra interfaz que no pertenezca a esa zona.

- Las interfaces que no han sido asignadas a una zona pueden usar la configuración CBAC de inspección de paquetes con estados.

- Cuando una interfaz en el router no es parte de la política de firewall basado en zonas, puede ser necesario colocar esa interfaz en una zona y configurar una política que deje pasar todo, conocida como "política falsa", entre esa zona y cualquier otra zona a la que se desee que fluya el tráfico.

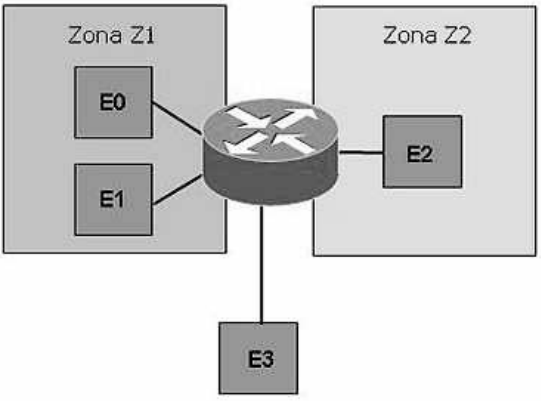
Cuando el router está involucrado en el flujo de tráfico, algunas reglas adicionales para firewalls basados en zonas gobiernan el comportamiento de la interfaz.

- Todo el tráfico desde y hacia una interfaz es bloqueado implícitamente cuando se asigna la interfaz a una zona, excepto el tráfico desde o hacia otras interfaces en la misma zona y el tráfico hacia cualquier interfaz en el router.

- Todas las interfaces IP del router son automáticamente parte de la self zone cuando se configura ZPF. La self zone es la única excepción a la política de denegación por defecto. Todo el tráfico que se dirija a cualquier interfaz del router será permitido hasta que el tráfico sea explícitamente denegado.

La única excepción a denegar todo por defecto es el tráfico que fluye desde y hacia el router en sí. Este tráfico se permite por defecto; si es necesario, debe configurarse una política explícita para restringirlo.

EJEMPLO:



Las siguientes son las restricciones de seguridad correspondientes a la figura:

- Las interfaces E1 y E0 son miembros de la zona de seguridad Z1.
- La interfaz de E2 es miembro de la zona de seguridad Z2.
- La interfaz E3 no es miembro de ninguna zona de seguridad.

Las situaciones generadas son las siguientes:

- El tráfico fluye libremente entre las interfaces E0 y E1, ya que son miembros de la misma zona de seguridad (Z1).
- Si no se configuran las políticas, el tráfico no fluirá entre las otras interfaces (por ejemplo, E0 y E2; E1 y E2; E3 y E1 y E3 y E2).
- El tráfico puede fluir entre E0 o E1 y E2 solo cuando una política explícita que lo permita se configura entre las zonas Z1 y Z2.
- El tráfico no puede fluir entre E3 y E3 E0/E1/E2 porque no es parte de ninguna zona de seguridad.

7.3.2 Configuración del firewall basado en zonas

El primer paso consiste en la creación de las zonas para el firewall con el comando **zone security**. El parámetro **description** no afecta al funcionamiento de la zona pero ayuda a administrar mejor el firewall. Las interfaces que tienen necesidades de seguridad similares deberían agruparse en la misma zona.

```
Router(config)# zone security zone-name
Router(config-sec-zone)# description line-of-description
```

Las clases de tráfico ZPF permiten definir los flujos de tráfico de una manera tan granular como se necesite.

La siguiente sintaxis muestra el comando para crear clases de tráfico ZPF.

```
Router(config)# class-map type inspect [match-any | match-all]
class-map-name
```

Para mapas de clases de nivel superior a capas 3 y 4, la opción **match-any** es el comportamiento por defecto.

```
Router(config)# class-map type inspect protocol-name [match-any |
match-all] class-map-name
```

La sintaxis para hacer referencia a listas de acceso dentro del mapa de clases es la siguiente.

```
Router(config-cmap)# match access-group {access-group | name access-
group-name}
```

Los protocolos son comparados dentro del mapa de clases a través del siguiente comando.

```
Router(config-cmap)# match protocol protocol-name
```

La característica de crear una jerarquía de clases y políticas anidando es una de las razones por las que ZPF constituye un enfoque tan potente para la creación de firewalls. Se pueden configurar mapas de clases anidados utilizando la siguiente sintaxis.

```
Router(config-cmap)# match class-map class-map-name
```

Los nombres no pueden repetirse en los tipos de mapas de clases o de políticas.

A continuación se debe especificar qué hacer con el tráfico que coincide con la clase de tráfico deseada.

```
Router(config)# policy-map type inspect policy-map-name
```

Las clases de tráfico sobre las cuales debe realizarse una acción se especifican en el mapa de políticas.

```
Router(config-pmap)# class type inspect class-name
```

La clase por defecto con la que coincide el resto del tráfico se especifica por medio del siguiente comando.

```
Router(config-pmap)# class class-default
```

Por último, se especifica la acción que debe realizarse sobre el tráfico. Las opciones son **pass** (dejar pasar), **inspect** (inspeccionar), **drop** (descartar) y **police** (aplicar una política).

```
Router(config-pmap-c)# pass | inspect | drop [log] | police
```

Luego de configurar la política de firewall, se debe aplicar entre un par de zonas. Para aplicar esta política, primero deben crearse estas dos zonas especificando la zona de origen, la zona de destino y la política de manejo del tráfico que fluye entre ellas.

```
Router(config)# zone-pair security zone-pair-name [source source-
zone-name | self] destination [self | destination-zone-name]
```

Para asociar un mapa de políticas y sus acciones asociadas a un par de zonas utilice el siguiente comando.

```
Router(config)# service-policy type inspect policy-map-name
```

La siguiente sintaxis se utiliza con la versión 12.4(20)T de IOS. De esta manera puede configurarse la inspección profunda de paquetes con la asociación de un mapa de políticas de capa 7.

```
Router(config-pmap-c)# service-policy {h323 | http | im | imap | p2p
| pop3 | sip | smtp | sunrpc | urlfilter} policy-map
```

El mapa de política es el nombre del mapa de políticas de capa 7 que se aplica al mapa de políticas de nivel superior de las capas 3 y 4.

Por último, se deben asignar interfaces a las zonas de seguridad apropiadas con el siguiente comando.

```
Router(config-if)# zone-member security zone-name
```

El comando aplicado coloca a la interfaz en una zona de seguridad, lo cual hace que todo el tráfico que se dirige desde y hacia la interfaz se descarte por defecto. Este mecanismo no se aplica para el tráfico que proviene del router o se dirige hacia él. Para permitir que el tráfico atraviese una interfaz que está en una zona de seguridad, la zona debe ser parte de un par de zonas que tenga una política aplicada. Si la política permite el tráfico con las acciones de paso o inspección, este podrá fluir a través de la interfaz.

EJEMPLO:

La siguiente sintaxis muestra la configuración de un mapa de clase llamado **class1** con los criterios de coincidencia de la ACL 120 y el protocolo HTTP, y un mapa de la política de inspección llamado **policy1** para especificar que el tráfico de paquetes en **class1** será descartado.

```
Router(config)# class-map type inspect match-all class1

Router(config-cmap)# match access-group 120
Router(config-cmap)# match protocol http

Router(config)# policy-map type inspect policy1

Router(config-pmap)# class type inspect class1

Router(config-pmap-c)# drop
```

7.3.3 Configuración del firewall basado en zonas con CCP

El asistente básico de CCP permite implementar un firewall con dos zonas, una zona interna y una zona externa. CCP crea el firewall solicitando información sobre las interfaces en el router, así como qué normas han de utilizarse en el

firewall. CCP permite también la configuración avanzada de un firewall donde es posible definir una zona de seguridad DMZ que puede ser utilizada para servicios accesibles desde Internet. El asistente avanzado permite, además, al usuario seleccionar el nivel de seguridad por defecto que se aplicará inicialmente.

Los pasos para acceder al asistente de configuración avanzado del Firewall con CCP son los siguientes.

- Desde la página de inicio, seleccione **Configure / Security / Firewall / Firewall**. Escoja la opción **Advanced Firewall** y luego pulse el botón **Launch the selected task**.

- Aparecerá la ventana del asistente avanzado. Seleccione **Siguiente** para iniciar la configuración.

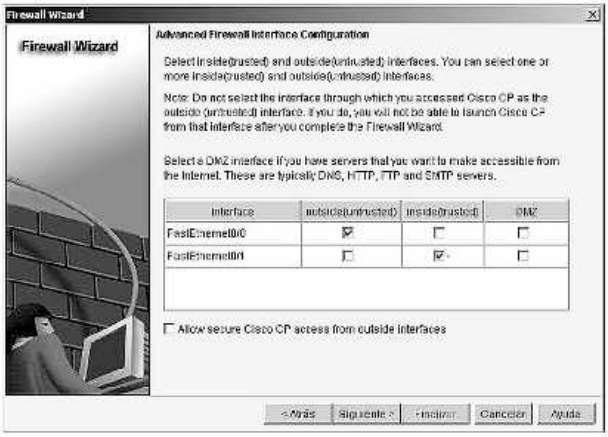
Lo siguiente es definir las interfaces internas y externas. Una interfaz externa suele ser la interfaz del router que está conectada a Internet o a una WAN. Una interfaz interna es típicamente una interfaz física o lógica que conecta a la LAN. Es posible seleccionar múltiples interfaces internas y externas.

- Desde la ventana de configuración avanzada marque las casillas correspondientes para seleccionar las interfaces internas en **inside (trusted)** o externas en **outside (untrusted)**. Estas interfaces se asociarán con una de las dos zonas creadas por defecto por CCP, la zona interior y la zona exterior.

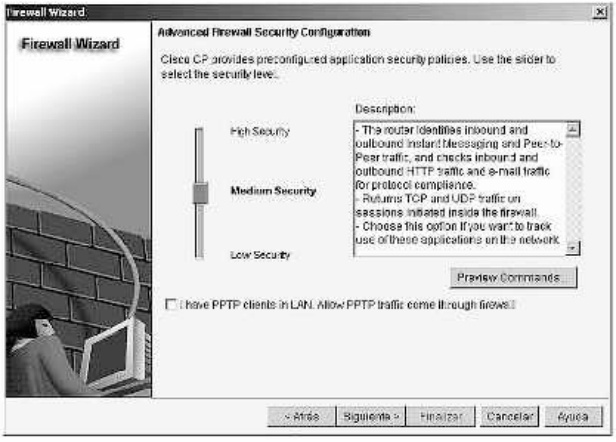
- Si fuese necesario configurar una zona DMZ utilice el menú desplegable para seleccionar la interfaz conectada a la DMZ.

- Opcionalmente puede marcar la casilla **Allow secure Cisco CP access from the outside interfaces** para permitir que usuarios externos puedan conectarse al firewall a través de CCP. Al elegir esta opción lo que se está haciendo en realidad es permitir el acceso HTTP seguro a la interfaz externa. Continúe con **Siguiente**. Especifique el host de origen o de la red a la que CCP le permite administrar de forma remota el router, complete el resto de los campos correspondientes. El firewall se modifica para permitir el acceso a la dirección especificada.

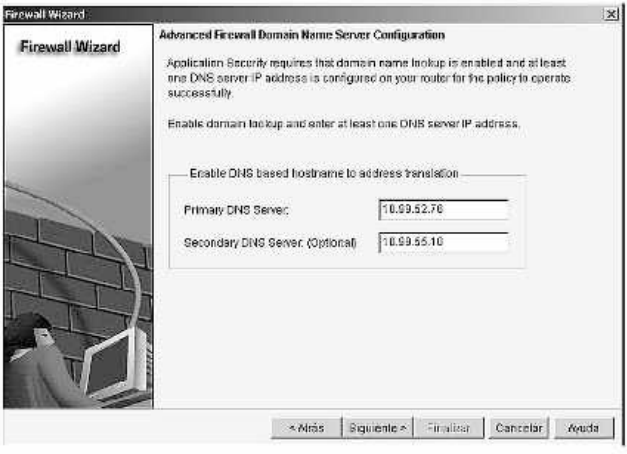
- Por el contrario, si esta casilla no está activada, aparecerá una advertencia para informarle de que el acceso a CCP en la interfaz externa no estará permitido al finalizar la configuración. Acepte con **OK**.



Después de la configuración de la interfaz, aparecerá la ventana **Advanced Firewall Security Configuration**. Utilice la barra deslizante para ver una descripción de la seguridad que cada nivel ofrece y seleccione el deseado. Los niveles de seguridad son bajo, medio y alto. Al utilizar el asistente de seguridad básico, esta opción no está disponible. Una vez que el nivel de seguridad adecuado es seleccionado, continúe con **Siguiente**.



En la ventana de **Advanced Firewall Security Configuration**, seleccione **Preview Commands** para ver los comandos IOS que conforman la política seleccionada. El router debe estar configurado con la dirección IP de al menos un servidor DNS para que las aplicaciones puedan funcionar.

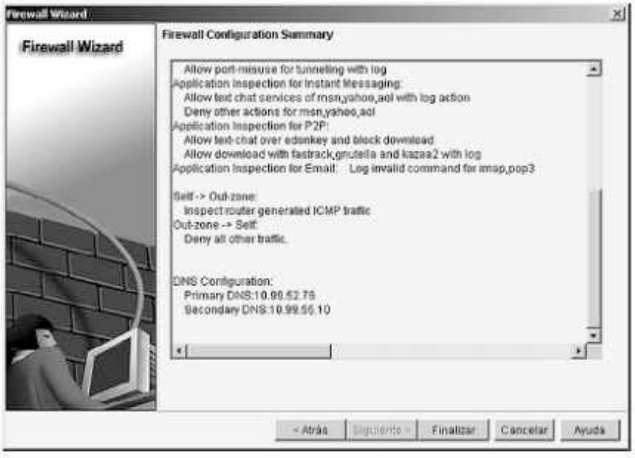


La ventana **Firewall Configuration Summary** muestra el nombre de la política elegida y los estados de configuración de la política.

- Seleccione **Finish** para completar la configuración.

- Si hay protocolos de enrutamiento configurados en el router, aparecerá una ventana de configuración de tráfico de enrutamiento. Desde este cuadro se permitirá que las actualizaciones de enrutamiento pasen a través del firewall.

- En la ventana **Deliver Configuration to Device** pulse el botón **Deliver** para habilitar los comandos de firewall de políticas basadas en zonas.



Los comandos ejecutados por los asistentes de seguridad básico y avanzado son a menudo muy largos. Las configuraciones creadas por los asistentes suelen ser más amplias que las creadas por una configuración manual.

7.3.4 Configuración manual del firewall basado en zonas con CCP

La configuración del firewall de política basada en zona también puede realizarse manualmente.

En primer lugar deben definirse las zonas, que pueden contener una interfaz o múltiples interfaces, sin embargo, una interfaz no puede ser un miembro de más de una zona. Recuerde que una zona de seguridad es un grupo de interfaces

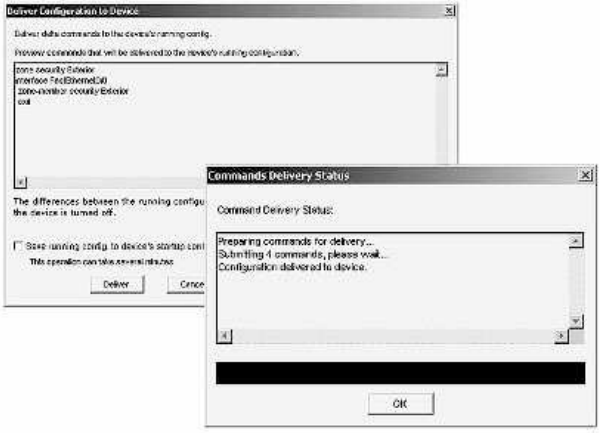
a las que se las puede aplicar una política de seguridad. Las interfaces deben agruparse teniendo en cuenta funciones comunes, características o requisitos de seguridad. Para que el tráfico fluya entre las interfaces en un router, deben pertenecer a una zona de seguridad. Sin embargo, no es necesario que todas las interfaces del router sean miembros de alguna zona de seguridad.

- Seleccione **Configure / Security / Firewall / Firewall Components / Zones**. Para crear una nueva zona marque **Add**. Elija **Edit** para seleccionar las interfaces en zonas existentes. Seleccione **Delete** para eliminar una zona determinada, antes de la eliminación la zona debe desasociarse de la interfaz.

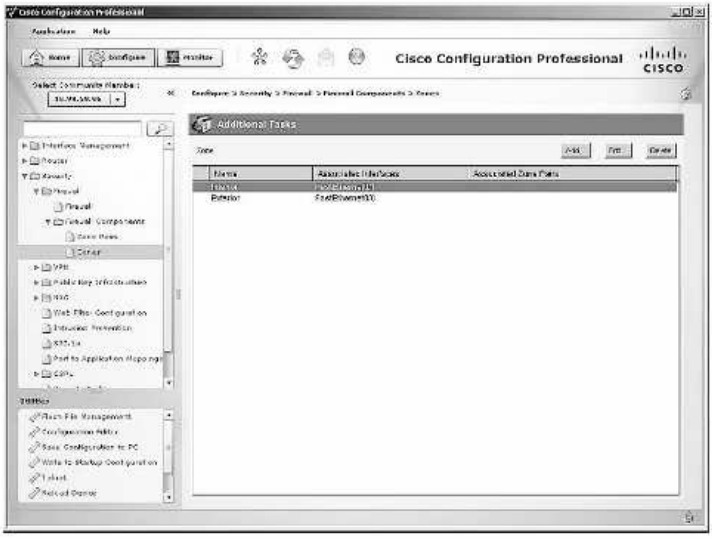
- Cuando la ventana de la zona aparece, ingrese el nombre de la zona.

- Elija las interfaces para esta zona, marcando la casilla de verificación situada delante del nombre de la interfaz. Debido a que las interfaces físicas no se pueden asociar a más de una zona, no aparecen en la lista las que ya han sido asignadas a una zona. Repita la operación para crear más zonas.

- Finalice con **OK** para crear la zona y pulse **Deliver** en la siguiente ventana. Opcionalmente puede marcar la casilla para guardar la configuración en la **startup config**. Termine con **OK** en la ventana de **Commands Delivery Status**.



Las zonas ya han sido creadas.

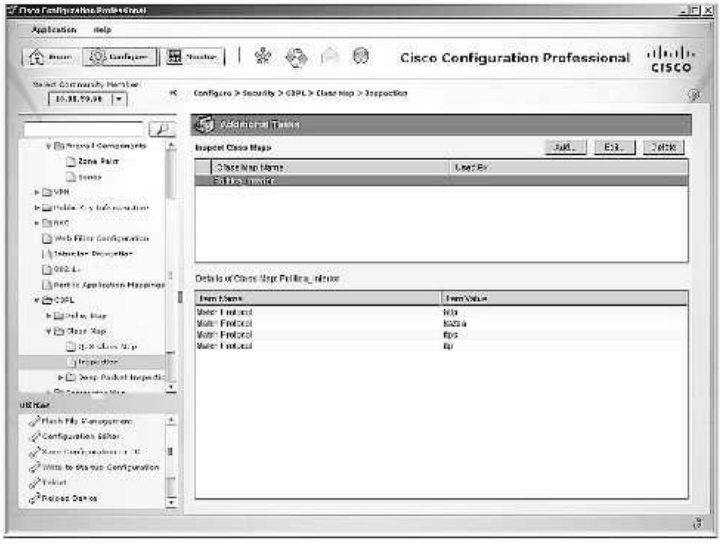


Después de crear una zona y de aplicar las interfaces, el siguiente paso es configurar los mapas de clase para identificar el tráfico y los parámetros de tráfico para la posterior aplicación de la política.

- Seleccione **Configure / Security / C3PL / Class Map / Inspection** y luego **Add**.

- Asigne un nombre en la casilla **Class Map**, opcionalmente puede añadir una descripción en la casilla **Descripción**. Si es necesario editar un mapa de clase existente o ver más detalles, selecciónelo en la lista y luego pulse **Edit**.

- Seleccione los protocolos que desee de la lista y agréguelos con **Add>>** a la lista de inspección para este mapa de clase. Finalice con **OK**.



A partir de la creación de los mapas de clase se deben aplicar ciertas políticas a los mismos. Los mapas de políticas especifican qué acciones tomar cuando el tráfico coincide con el criterio especificado.

Los mapas de política especifican la acción que el router tomará para el tráfico que coincida con los criterios establecidos en los mapas de clase asociados. Recuerde cuáles son estas acciones:

- **Pass**: se permite el paso de tráfico de una zona a otra solo en una dirección. El router no controla el estado de las conexiones o de sesión.

- **Drop**: el router descarta el tráfico no deseado y, opcionalmente, puede registrar el evento.

- **Inspect**: el router mantiene el estado basado en sesiones y la información de conexión para que sea permitido el tráfico que regresa de una zona de destino a una zona de origen.

Para crear un mapa de políticas siga los siguientes pasos.

- Seleccione **Configure** / **Security** / **C3PL** / **Policy Map** / **Protocol Inspection**.

- Desde la ventana de **Protocol Inspection Policy Maps**, pulse **Add**.

- Complete el nombre de la política en el campo **Policy Name field** y opcionalmente añada una descripción en el campo **Description**.

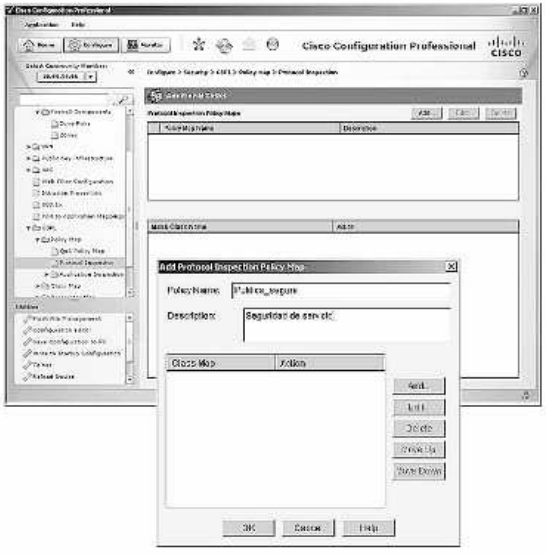
- Las columnas **Class Map** y **Action** muestran las clases de mapas que son asociados con las políticas y qué acción tomará el router con el tráfico que se describió en el mapa de clase. Continúe con **Add**.

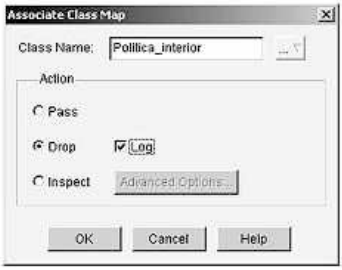
- En el campo **Class Name**, escriba el nombre de la clase a aplicar.

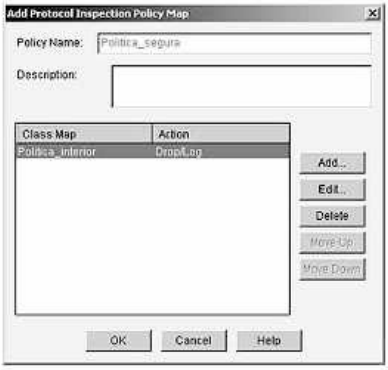
- Después de seleccionar el mapa de clase, defina la acción que el mapa de política tendrá para el tráfico que coincide con el mapa de clases. En la sección **Action**, seleccione **Pass**, **Drop** o **Inspect**, sobre la base de las necesidades particulares de este mapa de la clase. Termine con **OK**.

- Para agregar otro mapa de clase a la política, elija **Add**. Para modificar las acciones de un mapa de clase existente, seleccione el mapa de clase de la lista y luego **Edit**. Para eliminar una asignación, seleccione el mapa de clases de la lista y luego pulse **Delete**. Utilice los botones **Subir** y **Bajar** para cambiar el orden en que aparecen los mapas de clase.

- Termine con **OK**. En la ventana **Command Delivery Status**, finalice con **OK**.







La llamada **zone-pair** es un par de zonas donde se permite una política de firewall unidireccional. La dirección del tráfico se determina mediante la especificación de un origen y un destino en la zona de seguridad. La misma zona no puede ser definida como el origen y el destino. Si la intención es que el tráfico fluya libremente entre todas las interfaces, cada interfaz debe configurarse en una zona.

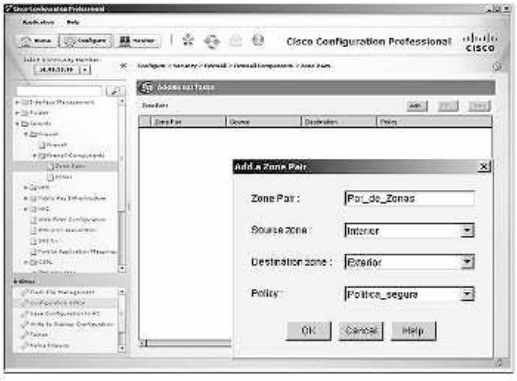
El proceso para configurar un nuevo par de zonas es el siguiente:

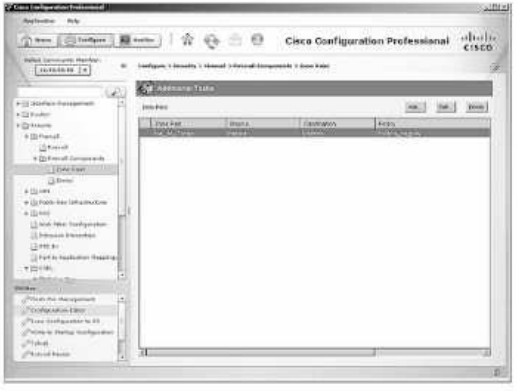
- Seleccione **Configure** / **Security** / **Firewall** / **Firewall Components** / **Zone Pairs** y luego **Add**.

- En el campo **Zone Pair**, escriba el nombre para el nuevo par de zona. Elija una zona de origen y una zona de destino, de donde se originará y recibirá el tráfico respectivamente, y la política que determina qué tipo de tráfico puede ser enviado a través de estas zonas. Confirme con **OK**.

- Las listas **Source** y **Destination** contienen las zonas que se han configurado en el router y la zona libre. Esta última se puede utilizar para configurar pares de zonas para el tráfico originado desde el propio router o destinado a él. La lista **Policy** contiene el nombre de cada mapa de política que está configurado en el router. Termine con **OK** en la ventana **Command Delivery Status**.

- Para editar un par de zona, elija una desde el panel **Zone Pairs** y luego **Edit**. Es posible editar el mapa de política, pero el nombre de las zonas de origen y destino no podrá modificarse.





7.4 RESOLUCIÓN DE PROBLEMAS EN EL FIREWALL BASADO EN ZONAS

Se puede obtener información sobre las conexiones activas en la tabla ZPF con el comando:

```
Router# show policy-map type inspect zone-pair session
```

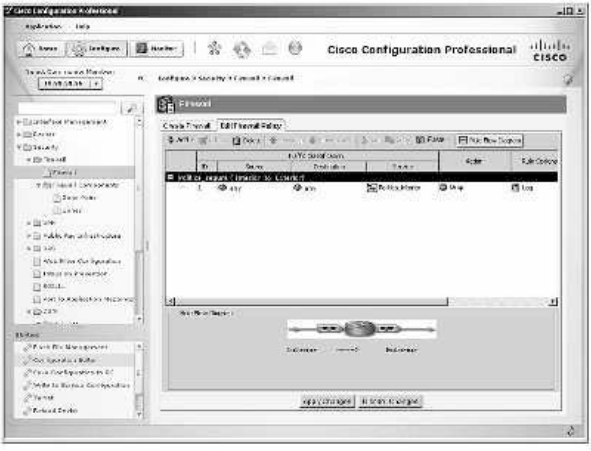
EJEMPLO:

La siguiente sintaxis muestra un ejemplo del comando **show policy-map type**.

```
Router# show policy-map type inspect zone-pair session

policy exists on zp zp
 Zone-pair: zp

 Service-policy inspect : fw

 Class-map: x (match-any)
 Match: class-map match-any y
 2 packets, 48 bytes
 30 second rate 0 bps
 Match: protocol tcp
 0 packets, 0 bytes
 30 second rate 0 bps
 Match: protocol icmp
 0 packets, 0 bytes
 30 second rate 0 bps

 Inspect

 Number of Established Sessions = 1
 Established Sessions
 Session 53105C0 (1.1.1.2:19180)=>(2.1.1.2:23) tacacs:tcp SIS_OPEN
 Created 00:00:02, Last heard 00:00:02
 Bytes sent (initiator:responder) [30:69]

 Class-map: class-default (match-any)
 Match: any
 Drop
 0 packets, 0 bytes
```

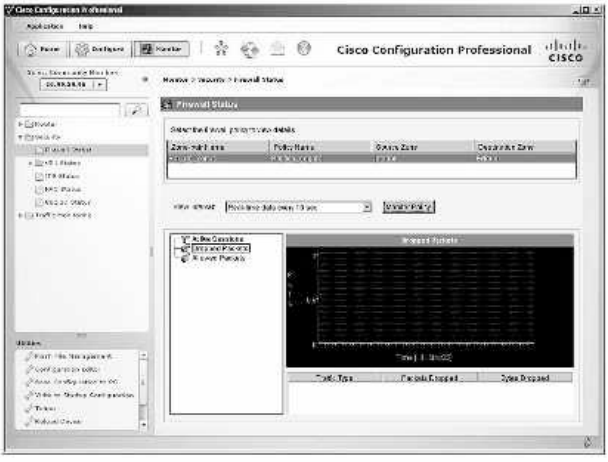
También puede examinarse el estado de las conexiones con CCP. Además es posible efectuar modificaciones desde la misma ventana.

- Seleccione **Configure / Security / Firewall / Firewall** y luego **Edit Firewall Policy**.



CCP se puede utilizar para mostrar el estado de actividad del firewall, las sesiones activas o para ver las estadísticas de paquetes perdidos y paquetes permitidos relacionados con la política implementada para cada par de zonas configuradas en el router.

- Desde **Monitor / Security / Firewall Status**.



7.5 CISCO ADAPTIVE SECURITY APPLIANCE

El Cisco **ASA** (*Cisco Adaptive Security Appliance*) es un dispositivo de seguridad autónomo y un componente principal de la arquitectura Cisco SecureX. Todos los modelos ofrecen características avanzadas de firewall y funcionalidad de VPN. Los dispositivos Cisco ASA son escalables para satisfacer los requisitos y diferentes tamaños de red. La elección del modelo de ASA dependerá de las necesidades de la organización, tales como el rendimiento, número máximo de conexiones y presupuesto.

El software ASA combina firewall, concentrador VPN y la funcionalidad de prevención de intrusiones en un mismo dispositivo. Anteriormente, estas funciones estaban disponibles en tres dispositivos separados, cada uno con su propio software y hardware. La combinación de estas funcionalidades en una sola imagen de software ofrece mejoras significativas en las características disponibles.

Los dispositivos ASA ofrecen características avanzadas como:

- **Virtualización**: un ASA puede dividirse en múltiples dispositivos virtuales.

- **Alta disponibilidad**: dos ASA idénticos se pueden combinar en una configuración de conmutación para proporcionar redundancia ante errores.

- **Servidor de seguridad de identidad**: el ASA ofrece control de acceso granular basado en una asociación de direcciones IP sobre la información de registro de Windows Active Directory.

- **Control de amenazas y contención de servicios**: todos los modelos ASA son compatibles con las funciones básicas de IPS. Sin embargo, las características avanzadas de IPS solo pueden ser proporcionadas por la integración de módulos especiales de hardware dentro de la arquitectura de ASA.

Un firewall stateful, como el ASA, facilita el seguimiento del estado de las conexiones de red TCP o UDP que lo atraviesan. El firewall está programado para detectar los paquetes legítimos entre diferentes tipos de conexiones. Solo los paquetes que coincidan con una conexión conocida activa serán permitidos por el firewall, mientras que los otros serán rechazados.

Todo el tráfico enviado a través de un ASA es inspeccionado mediante un algoritmo de seguridad (*Adaptive Security Algorithm*), ya sea permitiendo o

denegando los paquetes. El algoritmo tiene en cuenta el estado de la conexión asociada con dicho paquete.

Si el paquete pertenece a una nueva conexión, el ASA tiene que comprobarlo a través de las listas de acceso configuradas para determinar si el paquete se permite o se deniega. Para realizar esta comprobación, el primer paquete de la sesión pasa a través de la ruta de la administración de sesiones en el plano de gestión, y dependiendo del tipo de tráfico, también podría pasar a través del plano de control.

La ruta de la administración de sesiones es responsable de las siguientes tareas.

- Realización de los controles de lista de acceso.
- Realización de búsquedas de rutas.
- Asignación de NAT.
- Establecimiento de sesiones en el modo fast path.

Si la conexión ya está establecida, el ASA no vuelve a revisar los paquetes. En este caso, los paquetes que coinciden pueden ir a través del modo fast path en ambas direcciones. La vía rápida es responsable de las siguientes tareas:

- Verificación de IP checksum.
- Sesión de búsqueda.
- Comprobación de la secuencia TCP.
- Traducciones NAT basadas en las sesiones existentes.
- Ajustes de cabecera de las capas 3 y 4.

Para UDP u otros protocolos sin conexión, el ASA mantiene información de conexión de estado para que también puedan utilizar la vía rápida.

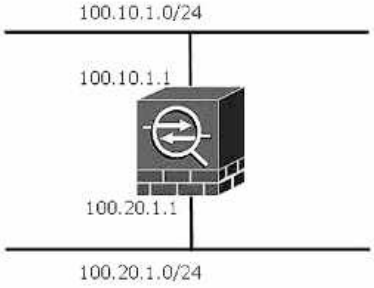
Los dispositivos ASA poseen dos modos de funcionamiento:

- **Modo enrutado**: es el modo tradicional para la implementación de un servidor de seguridad, donde hay dos o más interfaces que separan las

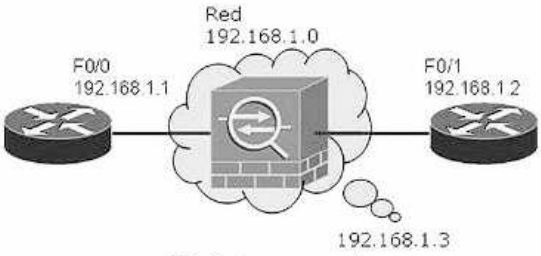
redes de capa 3. Dentro de la red, el ASA es considerado como un salto de router y puede realizar NAT entre las redes conectadas. El modo enrutado admite varias interfaces. Cada interfaz está en una subred diferente y requiere una dirección IP en la subred.

- **Modo transparente**: el ASA se considera como un dispositivo de capa 2, llamado firewall stealth. En el modo transparente, el ASA no se considera un salto de router, funciona como un switch de capa 2, por lo tanto solo necesita una dirección IP de administración y se requiere antes de que el dispositivo comience a reenviar tráfico. Una vez que la dirección se asigna, todas las interfaces se inician "escuchando" en la dirección de red establecida.

Un firewall transparente puede ser usado para simplificar la configuración de la red o ser desplegado en un período de investigación en un escenario que no puede ser alterado. El modo transparente también es útil para hacer que el servidor de seguridad sea invisible para los atacantes. Sin embargo, las desventajas de utilizar el modo transparente son que no incluye soporte para protocolos de enrutamiento dinámico, VPN, QoS o DHCP.



Modo enrutado



Modo transparente

7.5.1 Características del Cisco ASA

El Cisco ASA 5505 es un dispositivo de seguridad con todas las funciones necesarias para las pequeñas empresas, sucursales, teletrabajadores y entornos empresariales. Ofrece servicios como firewall de alto rendimiento, SSL, VPN y VPN IPsec en un sistema modular plug-and-play.

El ASA asigna niveles de seguridad para distinguir entre las redes internas y externas determinando el nivel de confiabilidad de una interfaz. Cuanto más alto sea el nivel, mayor confianza de la interfaz. Los números de nivel de seguridad oscilan entre 0 (no confiable) a 100 (muy fiable). Cada operación de interfaz debe tener un nombre y un nivel de seguridad asignado.

Cuando el tráfico se mueve de una interfaz con un nivel de seguridad superior a una interfaz con un nivel de protección inferior, se considera tráfico de salida. Por el contrario, el movimiento del tráfico de una interfaz con un nivel de protección inferior a una interfaz con un mayor nivel de seguridad se considera como tráfico de entrada.

Múltiples interfaces se pueden asignar al mismo nivel de seguridad. Cuando las interfaces tienen el mismo nivel de seguridad, el ASA inspecciona el tráfico en ambas direcciones. El filtrado se aplica solo para las conexiones salientes desde un nivel superior a un nivel inferior.

El ASA 5505 es comúnmente utilizado como un dispositivo frontera que conecta una pequeña empresa a un dispositivo del ISP. Puede ser desplegado para la interconexión y protección de varias estaciones de trabajo, impresoras de red y teléfonos IP. En ese escenario, el ASA 5505 puede implementarse con dos segmentos diferentes de red protegidos: la red interior (VLAN 1) para conectar las estaciones de trabajo y los teléfonos IP; y la DMZ (VLAN 3) para conectar a un servidor web de la compañía. La interfaz externa (VLAN 2) se utiliza para conectarse a Internet.

En una implementación más amplia, el ASA 5505 puede ser utilizado por los teletrabajadores y usuarios remotos para conectarse a una ubicación centralizada mediante una VPN.

Los modelos de alta gama, como el ASA 5510 están diseñados para ofrecer servicios avanzados de seguridad para pequeñas y medianas empresas y sucursales.

El ASA 5510 soporta 300 Mb/s de rendimiento de firewall y de 9.000 conexiones por segundo de capacidad. Esto hace que el ASA 5510 sea muy adecuado para la mayoría de las implementaciones de oficina.

La serie Cisco ASA 5510, 5520, 5540 y 5550 viene en formato de una unidad de rack y cada uno de ellos tiene una ranura de expansión para módulos de servicios de seguridad.

7.5.2 Configuración básica del firewall Cisco ASA

Los dispositivos ASA pueden ser configurados y administrados a través de la línea de comandos o por el asistente ASDM (*Adaptive Security Device Manager*).

El ASA contiene comandos con estructura similar a la de Cisco IOS. Pueden utilizarse abreviaturas, completar los comandos con el tabulador y utilizar la ayuda (?). Los siguientes son los modos de acceso:

- Modo EXEC usuario:

```
ciscoasa> en
```

- Modo EXEC privilegiado:

```
ciscoasa# config t
```

- Modo de configuración global:

```
ciscoasa(config)#
```

- Subcomando:

```
ciscoasa(config-if)#
```

- Modo ROMMON:

```
ROMMON>
```

Es posible ejecutar cualquier comando en cualquier modo de configuración sin necesidad de interponer el parámetro **do** como en IOS. La interrupción en IOS es **Ctrl+C (^C)**, mientras que en ASA se utiliza la tecla **Q**.

Comandos IOS	Comandos ASA
`show ip interfaces brief`	`show interfaces ip brief`
`show ip route`	`show route`
`show ip nat translations`	`show xlate`
`show vlan`	`show switch vlan`
`erase startup-config`	`write erase`
`enable secret`	`enable password`
`ip route`	`route outside`
`Ctrl+C`	`Q`

`line console 0`
`password password`
`login`
	`passwd password`

El ASA 5505 viene con una configuración predeterminada que, en la mayoría de los casos, es suficiente para una implementación básica de SOHO. La configuración incluye dos redes VLAN preconfiguradas: VLAN1 para la red interior y VLAN2 es para la red exterior.

La interfaz en el interior también ofrece direccionamiento DHCP y NAT. Los clientes de la red interior pueden obtener una dirección IP dinámica del ASA para que puedan comunicarse entre sí y con los dispositivos en Internet.

La configuración predeterminada de fábrica del ASA 5505 es la siguiente:

- El nombre de host por defecto es "ciscoasa".
- Las contraseñas están en blanco.
- Una VLAN 1 interior, que incluye los puertos Ethernet 0/1 hasta el 0/7. La VLAN1 lleva una dirección IP y máscara 192.168.1.1 y 255.255.255.0 respectivamente.
- Un VLAN 2 exterior, que incluye el puerto Ethernet 0/0. La VLAN 2 obtiene su dirección IP desde el ISP mediante DHCP.

- La ruta por defecto que se deriva de DHCP.
- Todas las direcciones IP interiores se traducen al exterior a través de PAT.
- El servidor HTTP brinda soporte de acceso al asistente ASDM.
- Un servidor DHCP interno proporciona direcciones entre 192.168.1.5 y 192.168.1.36 para los hosts que se conectan la interfaz VLAN 1.

Esta configuración se puede cambiar manualmente mediante la CLI o de forma interactiva utilizando el asistente ASDM. El ASA puede ser restaurado a su configuración predeterminada de fábrica mediante el comando **configure factory-default**.

Una vez reiniciado, el ASA muestra el siguiente mensaje: "**Pre-configure Firewall now through interactive prompts [yes]?**". Si se responde [**no**], se cancela el asistente de inicialización de la instalación y el ASA mostrará el valor predeterminado del sistema. Al pulsar enter, se acepta el valor por defecto [**yes**] y el ASA de forma interactiva le guiará a un administrador para configurar lo siguiente:

- Modo firewall.
- Habilitar contraseña.
- Habilitar recuperación de la contraseña.
- Fecha y hora.
- Dirección IP y máscara interna.
- Nombre de host.
- Nombre de dominio.

La siguiente lista muestra la sintaxis de los comandos para la configuración básica y de acceso.

Comando	Descripción
hostname *name*	Configura el nombre del dispositivo. Por defecto es **ciscoasa**.
domain-name *name*	Configura el nombre del dominio.
enable password *password*	Configura la contraseña EXEC. Las contraseñas por defecto están en blanco.
passwd *password*	Configura la contraseña de telnet/SSH. Las contraseñas por defecto están en blanco.
key config-key password-encryption [*new-passphrase* [*old-passphrase*]]	Crea o cambia una contraseña maestra existente. La contraseña debe ser de 8 a 128 caracteres de longitud, excepto la tecla enter, y las comillas son aceptadas.
password encryption aes	Configura el cifrado de las contraseñas. Habilita la encriptación para las contraseñas de todos los usuarios.
show password encryption	Muestra si la encriptación de las contraseñas está habilitada.
telnet	Identifica qué host interno puede hacer telnet al ASA.
telnet timeout *minutes*	Configura el tiempo de expiración de una sesión de telnet. Por defecto el valor es de 5 minutos.
aaa authentication ssh console LOCAL	Configura la autenticación SSH en una base de datos local.
crypto key generate rsa modulus 1024	Genera la clave RSA requerida para la autenticación SSH. Es sensible a mayúsculas y minúsculas.
ssh *ip-addresssubnet-maskinterface-name*	Identifica qué host interno puede hacer SSH al ASA.
ssh timeout *minutes*	Configura el tiempo de expiración de una sesión de SSH. Por defecto el valor es de 5 minutos.
show ssh	Muestra la configuración SSH.
show interface	Verifica la configuración de las interfaces.

show int ip brief	Verifica la configuración de las interfaces.
route *interface-name* **0.0.0.0 0.0.0.0** *next-hop-ip-address*	Configura una ruta por defecto.
show route	Verifica las rutas configuradas.

La siguiente lista muestra la sintaxis de los comandos para la configuración de VLAN.

Comando	Descripción
interface vlan *vlan-number*	Crea una interfaz virtual SVI.
nameif *name*	Configura un nombre para la interfaz SVI.
security-level *value*	Asigna un nivel de seguridad en un rango de 0 a 100 para la interfaz SVI.
ip address *ip-address netmask*	Configura un direccionamiento para la interfaz SVI. La dirección IP puede configurarse por tres medios: o Manualmente. o A través de DHCP. o A través de PPPoE.
no forward interface vlan *number*	Limita la interfaz al inicializarse para que no tome contacto con otra VLAN.
switchport access vlan *vlan-id*	Configura un puerto a una VLAN determinada. Por defecto, los puertos están asignados a la VLAN1.
no shutdown	Habilita un puerto de capa 2.
show switch vlan	Verifica la configuración de VLAN.
show interface	Muestra la configuración de las interfaces.
show int ip brief	Muestra un listado de las interfaces.

La siguiente lista muestra la sintaxis de los comandos para la configuración de DHCP.

Comando	Descripción
ip address dhcp	Habilita el cliente DHCP en la interfaz interna. La dirección IP es solicitada mediante DHCP. La opción **[setroute]** se puede añadir para crear una ruta predeterminada.
ip address dhcp setroute	Habilita el cliente DHCP en la interfaz interna. La dirección IP y la ruta por defecto son solicitadas mediante DHCP.
ip address pppoe	Habilita el cliente DHCP en la interfaz DCL. La dirección IP es solicitada mediante DHCP.
ip address pppoe setroute	Habilita el cliente DHCP en la interfaz DCL. La dirección IP y la ruta por defecto son solicitadas mediante DHCP.
dhcpd enable inside	Configura un servidor DHCP en la interfaz interna.
dhcpd address [*start-of-pool*] - [***end-of-pool***] **inside**	Define un almacén de direcciones IP para el servidor DHCP.
dhcpd domain *domain-name*	Configura el nombre del dominio DHCP.
dhcpd dns *dns-ip-address*	Configura la dirección IP del servidor DNS que entregará el DHCP.
dhcpd wins *wins-ip-address*	Configura la dirección IP del servidor WINS que entregará el DHCP.
dhcpd lease *seconds*	Configura el tiempo de arrendamiento. Por defecto es de 1 hora.
dhcpd option *value*	Configura el código de opción de DHCP. El código de opción se encuentra en el rango de 0-250.
dhcpd auto_config outside	Permite intercambiar información del dominio DNS desde la interfaz externa a la interfaz interna.
show dhcpd binding	Muestra el estado de las conexiones DHCP.

`show dhcpd statistics`	Muestra estadísticas DHCP.
`show dhcpd state`	Muestra el estado de las interfaces DHCP.
`clear dhcpd binding or`	Borra los enlaces DHCP.
`clear dhcpd statistics`	Borra las estadísticas DHCP.

La siguiente lista muestra la sintaxis de los comandos para la configuración de NTP.

Comando	Descripción
`ntp server` *ip-address*	Configura la dirección IP del servidor NTP.
`ntp authentication-key`	Configura la clave y contraseña de autenticación.
`ntp trusted-key` *value*	Identifica el valor de una clave de confianza.
`ntp authenticate`	Habilita la autenticación en NTP.
`show ntp status`	Verifica la configuración NTP.
`show ntp associations`	Verifica la configuración NTP.

7.5.3 Configuración del firewall Cisco ASA con ASDM

Cisco **ASDM** (*Cisco Adaptive Security Device Manager*) es un asistente que facilita la instalación, configuración, monitorización y solución de problemas en los dispositivos Cisco ASA. La aplicación reduce la complejidad de los comandos y permite configuraciones ágiles sin necesidad de un amplio conocimiento de la CLI del ASA. Funciona con SSL para proteger las comunicaciones y se puede utilizar para supervisar y configurar varios ASA que ejecutan la misma versión de ASDM.

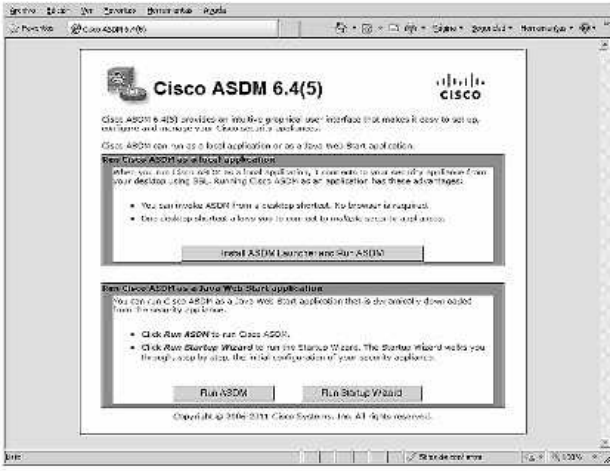
El ASDM viene preinstalado en la memoria flash de los ASA a partir de la versión 7.0, de lo contrario debe instalarse desde un servidor TFTP.

```
CCNAS-ASA# show flash:
--#-- --length-- -----date/time------ path
124 15390720 Oct 19 2011 15:49:48 asa842-k8.bin
125 16280544 Oct 19 2011 18:22:24 asdm-645.bin
3 4096 Jan 01 2003 00:03:32 log
10 4096 Jan 01 2003 00:04:00 crypto_archive
11 4096 Jan 01 2003 00:04:04 coredumpinfo
```

```
12 43 Jan 01 2003 00:04:04 coredumpinfo/coredump.cfg
127 12105313 Oct 19 2011 18:07:50 csd_3.5.841-k9.pkg
128 4096 Oct 19 2011 18:07:52 sdesktop
135 1462 Oct 19 2011 18:07:52 sdesktop/data.xml
129 2857568 Oct 19 2011 18:07:54 anyconnect-wince-ARMv4I-2
k9.pkg
130 3203909 Oct 19 2011 18:07:54 anyconnect-win-2.4.1012-k
131 4832344 Oct 19 2011 18:07:58 anyconnect-macosx-i386-2.
k9.pkg
132 5209423 Oct 19 2011 18:08:00 anyconnect-linux-2.4.1012
260034560 bytes total (198070272 bytes free)
```

Los requisitos mínimos para la utilización del asistente AS siguientes:

- Habilitar el HTTP Server en el ASA con el comando **enable**.
- Especificar la red, la dirección IP o el nombre del host o están permitidos para hacer uso del ASDM en el ASA con **http ip-address subnet-mask interface-name**.
- El host remoto debe tener acceso al dispositivo por red, u web instalado y Java versión 6 o superior.



Las capturas de pantalla utilizadas para la elaboración d corresponden a un dispositivo Cisco ASA 5520 con una versión de sof y ASDM versión 6.4(5) según los requisitos necesarios para el

```
.4.1012-

9.pkg
4.1012-

-k9.pkg
```

DM son los

http server

los host que
el comando

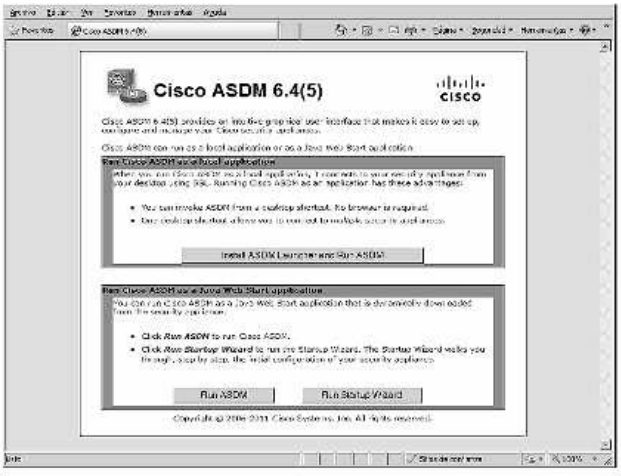
n navegador

e este libro
ftware 8.4(2)
examen de

```
12 43 Jan 01 2003 00:04:04 coredumpinfo/coredump.cfg
127 12105313 Oct 19 2011 18:07:50 csd_3.5.841-k9.pkg
128 4096 Oct 19 2011 18:07:52 sdesktop
135 1462 Oct 19 2011 18:07:52 sdesktop/data.xml
129 2857568 Oct 19 2011 18:07:54 anyconnect-wince-ARMv4I-2.4.1012-
k9.pkg
130 3203909 Oct 19 2011 18:07:54 anyconnect-win-2.4.1012-k9.pkg
131 4832344 Oct 19 2011 18:07:58 anyconnect-macosx-i386-2.4.1012-
k9.pkg
132 5209423 Oct 19 2011 18:08:00 anyconnect-linux-2.4.1012-k9.pkg
260034560 bytes total (198070272 bytes free)
```

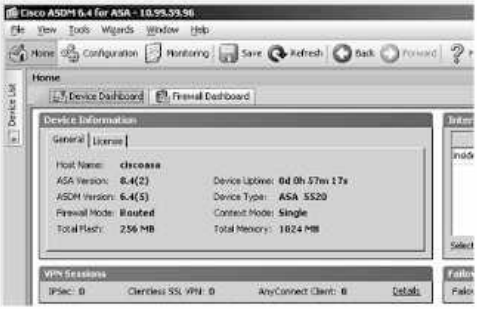
Los requisitos mínimos para la utilización del asistente ASDM son los siguientes:

- Habilitar el HTTP Server en el ASA con el comando **http server enable**.
- Especificar la red, la dirección IP o el nombre del host o los host que están permitidos para hacer uso del ASDM en el ASA con el comando **http ip-address subnet-mask interface-name**.
- El host remoto debe tener acceso al dispositivo por red, un navegador web instalado y Java versión 6 o superior.



Las capturas de pantalla utilizadas para la elaboración de este libro corresponden a un dispositivo Cisco ASA 5520 con una versión de software 8.4(2) y ASDM versión 6.4(5) según los requisitos necesarios para el examen de

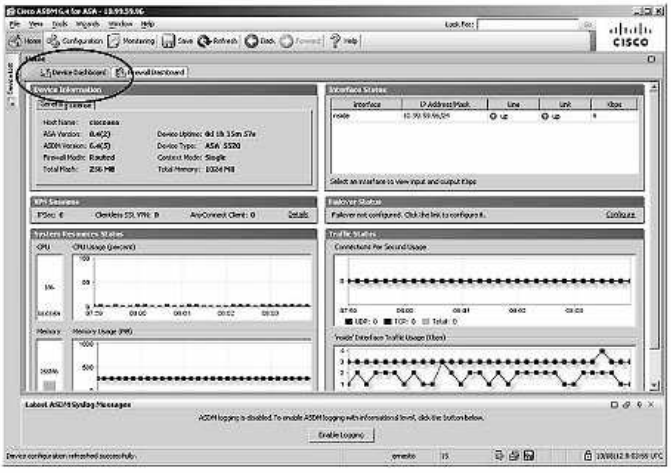
certificación. Alguna variante sobre estas características podría modificar el asistente y algunos menús del ASDM.

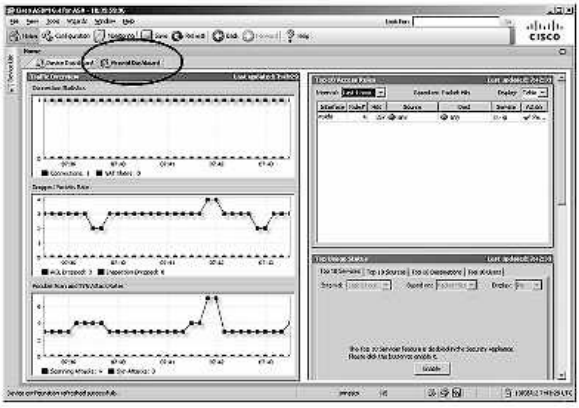


La página principal del ASDM ofrece información importante acerca del ASA. Por defecto, la página principal muestra dos solapas:

- **Device Dashboard**: proporciona una vista general acerca del ASA, como el estado de las interfaces, la versión del sistema operativo e información de licencias, así como información relacionada con el rendimiento.

- **Firewall Dashboard**: proporciona información relacionada con la seguridad sobre el tráfico que pasa a través del ASA, como por ejemplo las estadísticas de conexión, paquetes perdidos, escaneo y detección de ataques SYN.

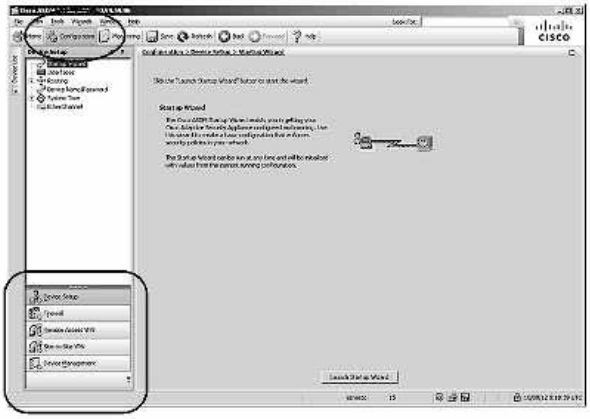




La interfaz de usuario del ASDM está diseñada para proporcionar un fácil acceso a las muchas características del ASA.

Desde el modo de configuración se puede acceder a las siguientes características:

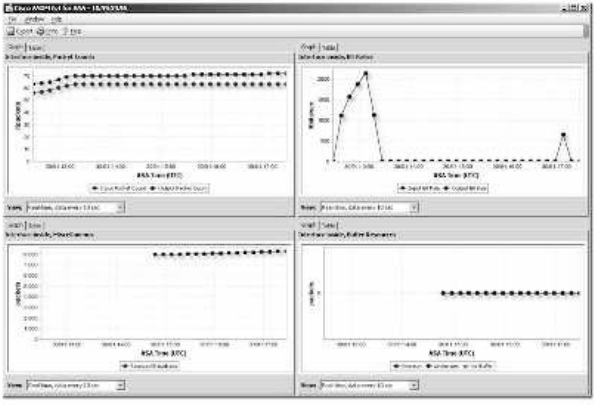
- Configuración del dispositivo.
- Firewall.
- VPN de acceso remoto.
- Site-to-site VPN.
- Administración de dispositivos.



Desde el modo de monitorización se puede acceder a las siguientes características:

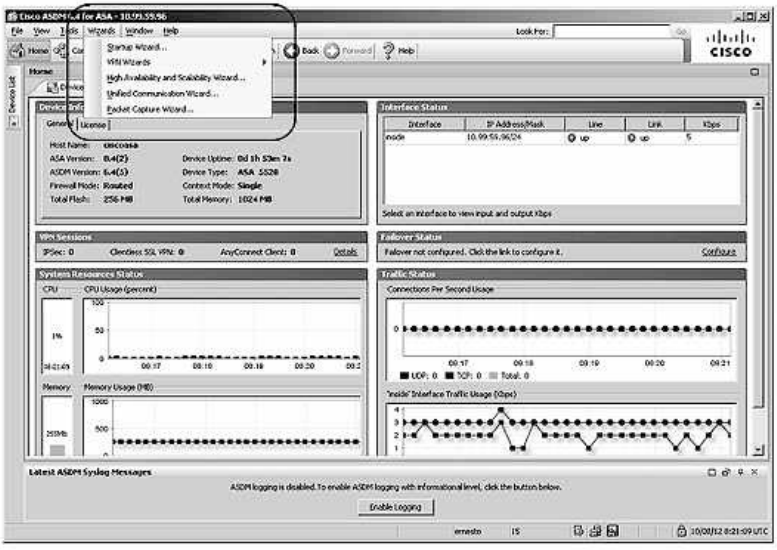
- Interfaces.
- VPN.
- Routing.
- Propiedades.
- Logging.

ASDM permite la monitorización de las interfaces en tiempo real.

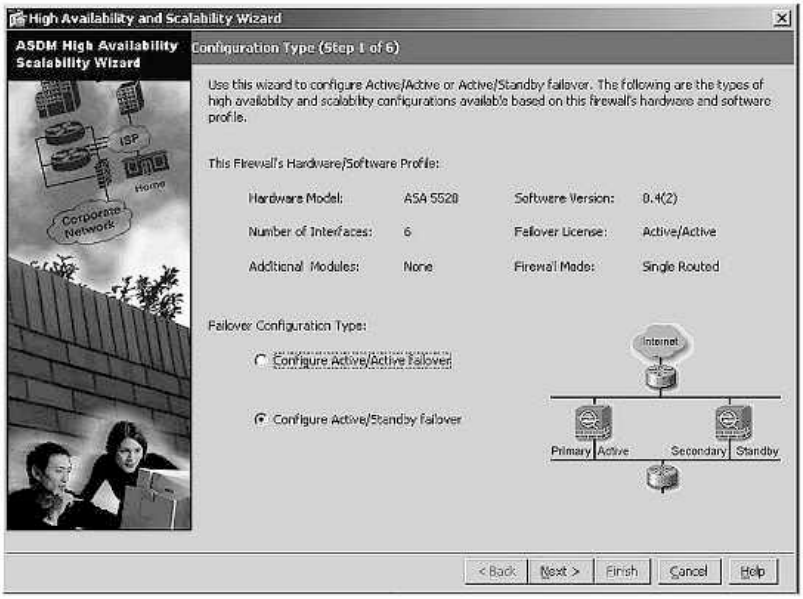


Cisco ASDM ofrece varios asistentes que ayudan a simplificar la configuración del dispositivo. Los asistentes guían al administrador indicando paso a paso el estado de la configuración.

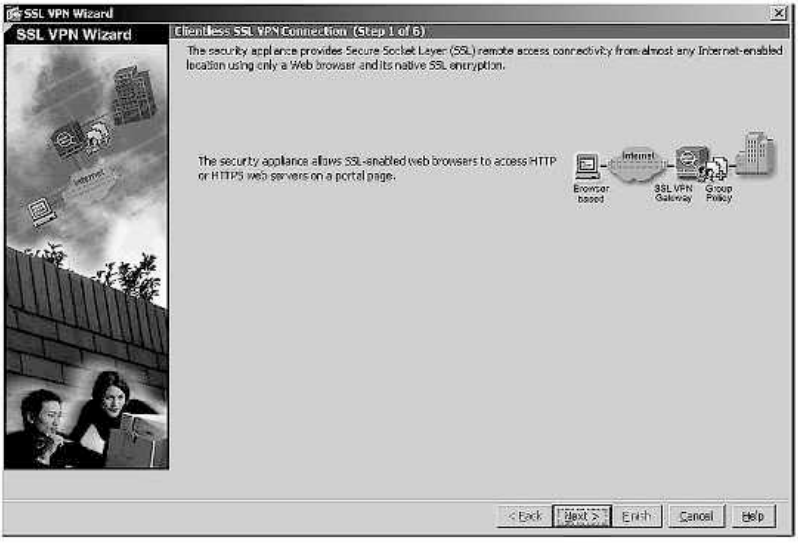
- Asistente inicial.
- Asistente VPN.
- Asistente para alta disponibilidad y escalabilidad.
- Asistente para comunicaciones unificadas.
- Asistente para captura de paquetes.



La siguiente captura de pantalla muestra el asistente para la configuración de alta disponibilidad y escalabilidad.



La siguiente captura de pantalla muestra el asistente para la configuración de Clientless SSL VPN.



7.6 CONFIGURACIÓN AVANZADA DEL FIREWALL CISCO ASA

7.6.1 Configuración de object groups

Los ASA soportan objetos y object groups. Los objetos son creados y utilizados por el ASA en lugar de una dirección IP para una configuración determinada. Un objeto puede ser definido con una dirección IP en particular o con un protocolo y, opcionalmente, un puerto, y puede volver a utilizarse en varias configuraciones. La ventaja es que cuando un objeto se modifica, el cambio se aplica automáticamente a todas las reglas que utilizan el objeto especificado.

Los objetos pueden acoplarse o desacoplarse de uno o más object groups cuando sea necesario. Estos objetos se pueden utilizar en NAT, listas de acceso y object groups. En concreto, los objetos de la red son una parte vital de la configuración de NAT.

Hay dos tipos de objetos que se pueden configurar:

- **Network object**: contiene una única dirección y máscara IP. Los objetos de red pueden ser de tres tipos: de host, subred o rango.
- **Service object**: contiene una fuente de protocolo y opcionalmente puerto de destino.

NOTA:

El network object se utiliza para configurar NAT en las versiones de imagen ASA 8.3 y superior.

Para crear un *network object* se utiliza el comando siguiente.

```
Ciscoasa(config)# object network object-name
Ciscoasa(config-network)#
```

Los *network objects* pueden ser definidos utilizando alguno de los tres métodos siguientes.

- Asignando una IP al nombre del objeto.

  host *ip-addr*

- Asignando una subred al nombre del objeto.

  subnet *net-address net-mask*

- Asignando un rango de direcciones.

  range *ip-addr-1 ip-addr-n*

Para crear un *service object* utilice el siguiente comando.

```
Ciscoasa(config)# object service object-name
Ciscoasa(config-service)#
```

El nombre del *service object* solo se puede asociar con un protocolo y puerto. Si un *service object* existe y está configurado con un protocolo y puerto diferente, la nueva configuración reemplazará el protocolo y el puerto existentes con los nuevos.

Existen cinco opciones de configuración.

- Especificando un nombre de protocolo IP o el número.

  service *protocol* [**source** [*operator port*]] [**destination** [*operator port*]]

- Especificando qué *service object* es para el protocolo TCP.

  service tcp [**source** [*operator port*]] [**destination** [*operator port*]]

- Especificando qué *service object* es para el protocolo UDP.

  service udp [**source** [*operator port*]] [**destination** [*operator port*]]

- Especificando qué *service object* es para el protocolo ICMP.

  service icmp *icmp-type*

- Especificando qué *service object* es para el protocolo IPv6.

  service icmp6 *icmp6-type*

Los parámetros opcionales sirven para identificar los puertos de origen o destino o ambos, por defecto el operador es **eq**.

Los objetos pueden ser agrupados juntos para crear un object group. Al agrupar, los object groups se pueden utilizar en una entrada de control de acceso

(ACE) en una ACL en lugar de tener que introducir una ACE para cada objeto por separado.

Las siguientes directrices y limitaciones se aplican a grupos de objetos.

- Los objetos y los object groups comparten el mismo espacio de nombres.
- Los object groups deben tener nombres únicos.
- Un object group no puede ser eliminado si está siendo utilizado en un comando.
- El ASA no es compatible con object groups IPv6 anidados.

El ASA soporta los siguientes tipos de object groups:

- Network.
- Protocol.
- ICMP-type.
- Service.

Para configurar un *network object group* se utiliza el siguiente comando.

```
Ciscoasa(config)# object-group network grp-name
```

Después de introducir el comando, agregue los objetos con los siguientes comandos.

```
Ciscoasa(config-network)# network-object
Ciscoasa(config-network)# group-object
```

Para configurar un *protocol object group* se utiliza el siguiente comando.

```
Ciscoasa(config)# object-group protocol grp-name
```

Después de introducir el comando, hay que definir un grupo de protocolos como TCP y UDP. Agregaremos objetos de red con los siguientes comandos:

```
Ciscoasa(config-protocol)# protocol-object
Ciscoasa(config-protocol)# group-object
```

NOTA:

Un network object group no se puede utilizar para implementar NAT.

Para configurar un ICMP *object group* se utiliza el siguiente comando.

```
Ciscoasa(config)# object-group icmp-type grp-name
```

Después de introducir el comando hay que agregar los objetos ICMP con los siguientes comandos.

```
Ciscoasa(config-icmp)# icmp-object
Ciscoasa(config-icmp)# group-object
```

Para configurar un *service object group* se utiliza el siguiente comando.

```
Ciscoasa(config)# object-group service grp-name
```

El *service object group* puede definirse utilizando servicios TCP, UDP, ICMP-type y otros protocolos. Continúe con los siguientes comandos para agregar los servicios.

```
Ciscoasa(config-icmp)# service-object
Ciscoasa(config-icmp)# group-object
```

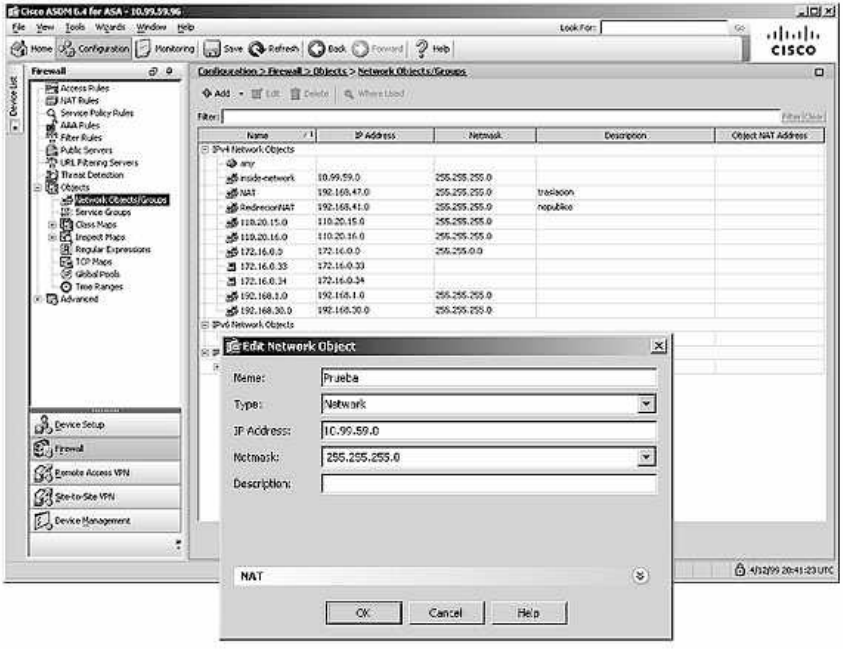
Para configurar un *service object group* para TCP, UDP o ambos especifique la opción en el comando, luego agregue los puertos correspondientes.

```
Ciscoasa(config)# object-group service grp-name [tcp|udp|tcp-udp]
Ciscoasa(config-service)# port-object
Ciscoasa(config-service)# group-object
```

La siguiente tabla muestra algunos comandos adicionales para la configuración de los *object group*.

Comando	Descripción
`clear config object network`	Elimina los *network objects*.
`clear config object service`	Elimina los *service objects*.
`clear configure object-group`	Elimina todos los *object group*.
`show running-config object`	Muestra los objetos.
`show running-config object-group`	Muestra los todos *object group*.

Los network object, network object group, service objects, service object groups, ICMP object groups o protocol object groups pueden configurarse también a través del asistente ASDM siguiendo las indicaciones desde **Configuration / Firewall / Objects**.



EJEMPLO:

Las siguientes sintaxis muestran la configuración de algunos *object group*.

```
Ciscoasa(config)#object-group icmp-type icmp-allowed
Ciscoasa(config-icmp-type)#icmp-object echo
Ciscoasa(config-icmp-type)#icmp-object time-exceeded
Ciscoasa(config-icmp-type)#exit

Ciscoasa(config)#object-group network ftp_servers
Ciscoasa(config-network)#network-object host 10.1.1.14
Ciscoasa(config-network)#network-object host myFTPserver
Ciscoasa(config-network)#network-object 10.1.1.32 255.255.255.224
Ciscoasa(config-network)#exit

Ciscoasa(config)#object-group protocol proto_grp_1
Ciscoasa(config-protocol)#protocol-object udp
Ciscoasa(config-protocol)#protocol-object tcp
Ciscoasa(config-protocol)#protocol-object esp
Ciscoasa(config-protocol)#exit

Ciscoasa(config)#object-group service allowed_prots tcp
Ciscoasa(config-service)#port-object eq ftp
Ciscoasa(config-service)#port-object range 2020 2021
Ciscoasa(config-service)#exit

Ciscoasa(config)#object-group service high_ports tcp-udp
Ciscoasa(config-service)#port-object range 1024 65535
Ciscoasa(config-service)#exit

Ciscoasa(config)#object-group service RTPUsers
Ciscoasa(config-service)#service-object icmp echo-reply
Ciscoasa(config-service)#service-object icmp echo
Ciscoasa(config-service)#service-object tcp http
Ciscoasa(config-service)#service-object tcp https
Ciscoasa(config-service)#service-object tcp http
Ciscoasa(config-service)#service-object tcp pptp
Ciscoasa(config-service)#service-object udp domain
Ciscoasa(config-service)#service-object udp isakmp
Ciscoasa(config-service)#service-object esp
Ciscoasa(config-service)#service-object gre
Ciscoasa(config-service)#exit

Ciscoasa# show object-group
object-group network ftp_servers
 description: This is a group of FTP servers
 network-object host 209.165.201.3
 network-object host 209.165.201.4
object-group network TrustedHosts
 network-object host 209.165.201.1
 network-object 192.168.1.0 255.255.255.0
 group-object ftp_servers
```

7.6.2 Configuración de ACL

Los dispositivos ASA de la serie 5500 ofrecen capacidades de filtrado de tráfico básico a través de las ACL. Existen muchas similitudes con las ACL en IOS y las ACL en ASA como por ejemplo las siguientes:

- Ambos procesan las ACL de manera secuencial.
- Siempre existe una denegación implícita al final de cada ACL.
- Únicamente se permite una sola ACL por interfaz, por protocolo y por dirección.
- Las ACL están compuestas por una o más ACE.
- Las ACL pueden ser configuradas basándose en tiempos o rangos.

Las ACL en IOS utilizan la máscara *wildcard* en lugar de la máscara de subred como lo hacen los ASA. Los dispositivos ASA permiten además configurar niveles de seguridad en las interfaces desde 0, como el nivel más bajo, a 100 como el más alto. Al tráfico de una interfaz más segura se le permite acceder a las interfaces menos seguras. El tráfico de una interfaz menos segura a las interfaces más seguras está bloqueado.

Por lo tanto, en una ACL será necesario permitir explícitamente el tráfico a partir de un nivel de protección inferior a un nivel de seguridad mayor.

Una ACL puede utilizarse no solo para filtrar los paquetes que pasan a través del dispositivo, sino también para filtrar los paquetes destinados al mismo.

Para el caso del tráfico que pasa a través del dispositivo desde una interfaz a otra la configuración se realiza creando una ACL y aplicándola a una determinada interfaz. Sin embargo, para el tráfico que termina en el ASA destinado al plano de control requerirá un conjunto adicional de reglas para la aplicación del filtrado.

Los dispositivos ASA soportan cinco tipos de listas de acceso:

- **Listas de acceso estándar**: a diferencia de IOS, donde se identifica el origen, en el ASA se identifica el destino. Se suelen utilizar para rutas OSPF y se pueden utilizar en un mapa de rutas para la redistribución de dicho protocolo. Las listas de acceso estándar no pueden ser aplicadas a las interfaces para controlar el tráfico.

- **Listas de acceso extendidas**: contienen una o más entradas de control para especificar las direcciones de origen y de destino, protocolo y puertos.

- **Listas de acceso EtherType**: solo pueden configurarse si el dispositivo de seguridad se ejecuta en modo transparente.

- **Listas de acceso Webtype**: se utilizan en una configuración que admite el filtrado clientless SSL VPN.

- **Listas de acceso IPv6**: se utilizan para permitir o denegar el tráfico IPv6.

Las opciones de configuración de una ACL en un ASA son bastante similares a las ACL en IOS.

- **Nombre**: puede ser cualquier nombre alfanumérico de hasta 241 caracteres.

- **Tipo**: pueden ser extendidas, estándar o webtype.

- **Acción**: se puede permitir o denegar.

- **Protocolo**: puede ser para todo el tráfico IP o para un protocolo determinado.

- **Origen**: identifica el origen y puede ser un host, una red o un network object group.

- **Puerto de origen**: (opcional) puede ser el actual número de puerto TCP o UDP, un nombre de puerto o service object group.

- **Destino**: identifica el destino y puede ser cualquier host, una red o un network object group.

- **Operando** (opcional): el operando se utiliza en conjunción con el puerto de origen y destino. Los operandos válidos son **lt** (menor que), **gt** (mayor que), **eq** (igual), **neq** (no igual) y **range** para un rango determinado.

- **Puerto de destino**: (opcional) puede ser el actual número de puerto TCP o UDP, un nombre de puerto o un service object group.

- **Registro**: puede establecer elementos para registro de eventos. Las opciones incluyen establecer el nivel de gravedad, el nombre y el intervalo de registro (por defecto, 300 segundos).

- **Rango**: (opcional) especifica un intervalo de tiempo para una ACE.

Hay diversas opciones que se pueden utilizar en la configuración de una ACL, muchas de las cuales están fuera del alcance de este libro. Sin embargo, para la mayoría de las necesidades, una versión más útil y resumida de la sintaxis es la que sigue:

```
Ciscoasa(config)#access-list id extended {deny | permit} protocol
{source-addr source-mask} | any | host src-host interface src-if-
name [operator port [port]] {dest-addr dest-mask} | any | host dst-
host | interface dst-if-name [operator port [port]]
```

Una vez creada la ACL se debe aplicar a una interfaz como entrante o saliente.

```
Ciscoasa(comfit-if)#access-group access-list {in | out} interface
interface-name [per-user-override | control-plane]
```

La siguiente sintaxis muestra una versión resumida de la configuración de una ACL basándose en los parámetros de los *object group*.

```
Ciscoasa(config)#access-list id [line line-num] [extended] {deny |
permit} object-group protocol-obj-grp-id object-group network-obj-
grp-id object-group service-obj-grp-id] object-group network-obj-
grp-id object-group service-obj-grp-id] [log level] [interval secs]
[[disable | default] | [time-range time-range-ID]] | [inactive]
```

NOTA:

El firewall sigue la regla de factor de multiplicación cuando se definen las ACE. Por ejemplo, dos hosts que deben acceder a dos servidores para obtener dos servicios requieren la configuración de 8 ACE.

2 hosts × 2 servidores × 2 servicios = 8 ACE

La siguiente tabla muestra comandos adicionales para la configuración y verificación de las ACL en los dispositivos ASA.

Comando	Descripción
`same-security-traffic permit inter-interface`	Permite la conectividad entre interfaces del mismo nivel de seguridad.
`same-security-traffic permit intra-interface`	Habilita el tráfico entre una interfaz cifrada y otra sin cifrar.
`help access-list`	Muestra la ayuda para la configuración de las ACL.
`clear configure access-list id`	Borra la configuración de una ACL.
`remark`	Añade un comentario en la ACL.
`show running-config access-list`	Muestra la configuración de las ACL.
`show access-list`	Muestra la configuración de las ACL.

EJEMPLO:

La lista de acceso **ACL_IN** impide que las máquinas de la red 192.168.1.0/24 accedan a la red a la red 209.165.201.0/27 por TCP. Todas las otras direcciones están permitidas.

```
Firewall_ASA(config)# access-list ACL_IN extended deny tcp
192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
Firewall_ASA(config)# access-list ACL_IN extended permit ip any any
```

Si desea restringir el acceso solo a determinados hosts, escriba una ACE con permisos limitados. Por defecto, el resto del tráfico se deniega a menos que sea explícitamente permitido.

```
Firewall_ASA(config)# access-list ACL_IN extended permit ip
192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
```

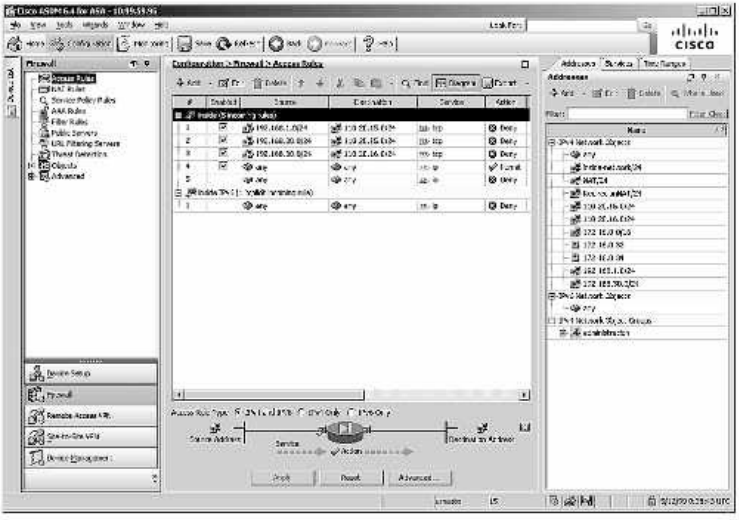
La siguiente ACL restringe todos los host en la interfaz donde se aplica la lista de acceso para acceder a una página web en la dirección 209.165.201.29. El resto del tráfico está permitido.

```
Firewall_ASA(config)# access-list ACL_IN extended deny tcp any host
209.165.201.29 eq www
Firewall_ASA(config)# access-list ACL_IN extended permit ip any any
```

Para definir un *object group* en una ACL solo es necesario especificar el *object group* en la ACE de la siguiente manera:

```
Firewall_ASA(config)# object-group network administracion
Firewall_ASA(config-network)# group-object ingenieria
Firewall_ASA(config-network)# group-object recursos
Firewall_ASA(config-network)# group-object contaduria

Firewall_ASA(config)# access-list ACL_IN extended permit ip object-
group administracion host 209.165.201.29
```

Las listas de acceso pueden configurarse también a través del asistente ASDM siguiendo las indicaciones desde **Configuration / Firewall / Access Rules**.



7.6.3 Configuración de NAT

Los dispositivos ASA soportan **NAT** (*Network Address Translation*) y **PAT** (*Port Address Translation*) y se pueden implementar mediante alguno de estos métodos:

- **Inside NAT**: el método de implementación de NAT más común, trabaja cuando un host de una interfaz de alta seguridad envía el tráfico a una interfaz de menor seguridad donde se traduce la dirección del host interno a una dirección global. El ASA a continuación restaura la dirección IP interna original para el tráfico de retorno.

- **Outside NAT**: este método se utiliza cuando el tráfico de una interfaz de menor seguridad está destinado a un host en una interfaz de mayor seguridad. Este método puede ser útil para hacer que un host externo aparezca como uno de una dirección IP interna conocida.

- **Bidirectional NAT**: hace referencia a la utilización de los dos métodos anteriores a la vez.

A partir de la versión 8.3 de software de ASA los comandos para la configuración de NAT serán reemplazados por una nueva característica llamada Auto-NAT. Auto-NAT ha simplificado considerablemente la configuración y solución de problemas de NAT. Auto-NAT se aprovecha de la utilización de los network objects para configurar todas las variantes de NAT. Hay que recordar que los network objects se pueden utilizar para identificar un host, subred o rango de direcciones IP.

Los parámetros de los comandos NAT se deben especificar en el objeto con el siguiente comando, la elección de los parámetros está relacionada con el tipo de NAT requerido.

```
Ciscoasa(config)#nat [(real-ifc,mapped-ifc)] dynamic {mapped-inline-
host-ip [interface] | [mapped-obj] [pat-pool mapped-obj [round-
robin]] [interface]} [dns]
```

El ASA divide la configuración de NAT en dos secciones. La primera parte define la red que se traduce utilizando un network objects. La segunda define los parámetros reales del comando **nat**. Estos aparecen en dos lugares diferentes en el running-config.

Cisco ASA soporta los siguientes tipos de traducción de direcciones de red:

- **NAT dinámica**: es una traducción de direcciones de muchos a muchos.

- **PAT o NAT sobrecargado**: es una traducción de direcciones de muchos a una dirección.

- **NAT estática**: es una traducción de uno a uno.

Para configurar NAT dinámica se requieren dos network objects. El network objects identifica en primer lugar el conjunto de direcciones IP públicas en que las direcciones internas se traducirán. El objeto de la segunda red une a los dos objetos. Utilice los siguientes comandos:

- Para nombrar el *network object* que identifica el *pool* de direcciones públicas:

```
object network mapped-obj
```

- Asigna un rango de direcciones IP:

```
range ip-addr-1 ip-addr-n
```

- Nombra el NAT *object*:

```
object network nat-object-name
```

- Asigna una subred al nombre del objeto. Alternativamente puede utilizarse el parámetro *range*:

```
subnet net-address net-mask
```

- Mapea una dirección estática a un host o red interna:

```
nat (real-ifc,mapped-ifc) dynamic mapped-obj
```

Para configurar PAT utilice los siguientes comandos.

- Nombra el PAT object:

```
object network nat-object-name
```

- Asigna una subred al nombre del objeto. Alternativamente puede utilizarse el parámetro *range*:

```
subnet net-address net-mask
```

- Provee a los host internos de la sobrecarga a la red externa:

```
nat (real-ifc,mapped-ifc) dynamic interface
```

Para configurar NAT estático se asigna una dirección interior a una dirección exterior, utilice los siguientes comandos:

- Para nombrar el NAT object:

```
object network nat-object-name
```

- Para identificar la dirección IP interior del host:

```
host ip-addr
```

- Mapea estáticamente una dirección interna a una externa:

```
nat (real-ifc,mapped-ifc) static mapped-inline-host-ip
```

NOTA:

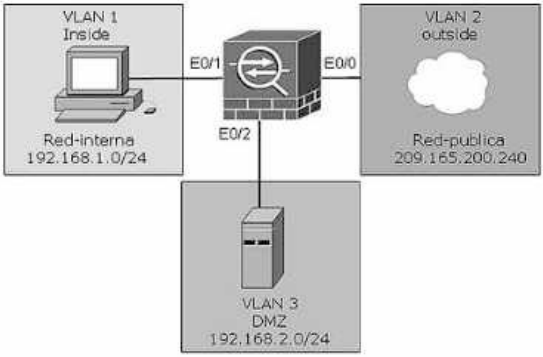
*La palabra clave **any** se podría utilizar en lugar del parámetro mapped-ifc. Esto permite la traducción de un objeto entre varias interfaces con solo un comando.*

La siguiente tabla muestra comandos adicionales para la configuración y verificación de NAT en los dispositivos ASA.

Comando	Descripción
`show run object`	Muestra la configuración de los network object.
`show run nat`	Muestra la configuración de NAT.
`show nat`	Muestra las traducciones realizadas a través de NAT.
`show xlate`	Muestra las traducciones realizadas a través de NAT.
`clear nat counters`	Borra los contadores de NAT.

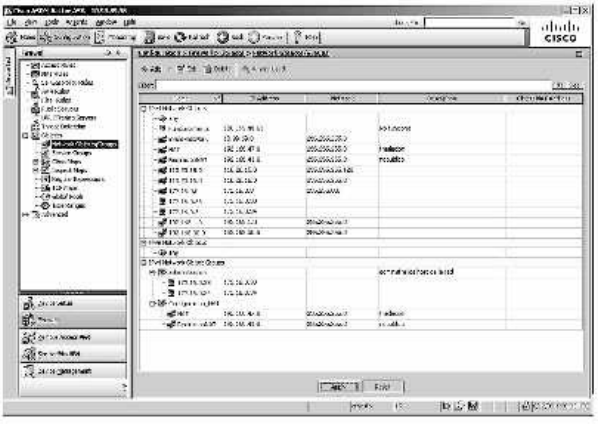
EJEMPLO:

La siguiente sintaxis muestra la configuración de los object network basados en la topología de la figura.

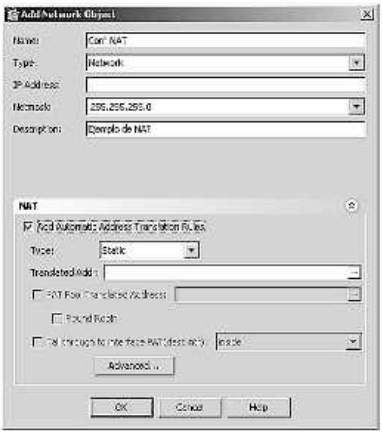


```
ciscoasa(config)# object network Red-publica
ciscoasa(config-network-object)# range 209.165.200.240
255.255.255.240
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network Red-interna
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic Red-
publica
ciscoasa(config-network-object)# end

ciscoasa(config)# object network Red-interna
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.224
ciscoasa(config-network-object)# nat (inside,outside) dynamic
interface
ciscoasa(config-network-object)# end

ciscoasa(config)# object network DMZ
ciscoasa(config-network-object)# host 192.168.2.3
ciscoasa(config-network-object)# nat (dmz,outside) static
209.165.200.227
ciscoasa(config-network-object)# end
ciscoasa(config)#access-list DMZ-SALIENTE permit ip any host
192.168.2.3

ciscoasa(config)#access-group DMZ-SALIENTE in interface outside

ciscoasa# show nat
Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ 209.165.200.227
translate_hits = 4, untranslate_hits = 4
```

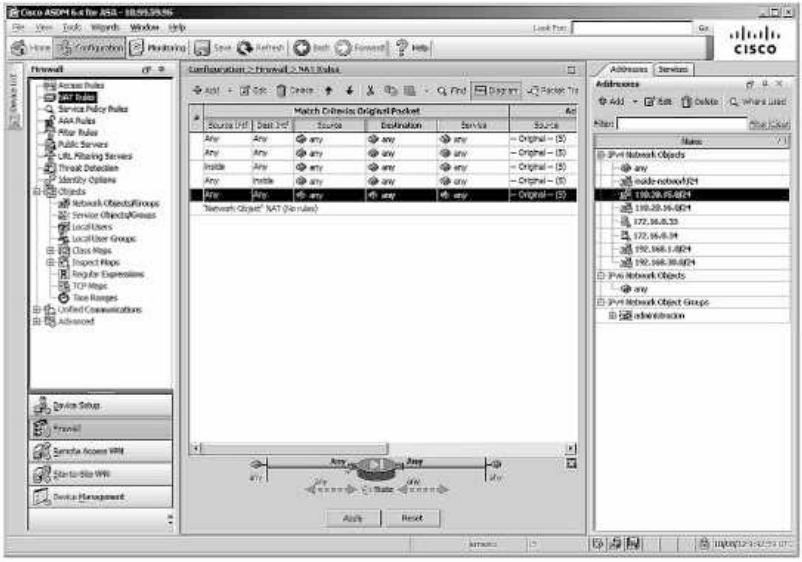
La configuración de NAT puede hacerse también a través del asistente ASDM, en primer lugar se debe crear el network object seleccionando **Configurations / Firewall / Objects / Network Objects/Groups** luego elija **Add / Network Object**.



Una vez completados los datos requeridos para la creación del network object despliegue la solapa para la configuración de NAT. Marque la casilla **Add Automatic Address Translation Rules**, en **Type** seleccione el tipo de NAT que quiera configurar.



Desde **Configurations / Firewall / NAT Rules** se pueden verificar las configuraciones de NAT.



7.6.4 Configuración de control de acceso

Los dispositivos cisco ASA pueden ser configurados para la autenticación de usuarios utilizando una base de datos local o un servidor de autenticación. AAA puede utilizar una base de datos local para la autenticación. Este método almacena nombres de usuarios y contraseñas de forma local en el ASA, y los usuarios se autentican contra dicha base de datos. En este caso no se necesita un servidor de autenticación AAA dedicado y es ideal para redes pequeñas.

La sintaxis del comando para la autenticación local es la siguiente:

```
ciscoasa(config)#username name password password [privilege priv-
level]
```

La autenticación AAA basada en servidor es un método mucho más escalable que la autenticación AAA local. Este método utiliza un servidor de base de datos externo a través de los protocolos RADIUS o TACACS+.

La configuración de la autenticación basada en servidor comienza creando un grupo de servidores AAA y definiendo el protocolo de autenticación. Posteriormente se deben configurar los parámetros específicos del servidor. Las sintaxis de los comandos para la autenticación basada en servidor son las siguientes:

```
ciscoasa(config)#aaa-server server-tag protocol protocol
```

```
ciscoasa(config)#aaa-server server-tag [(interface-name)] host
{server-ip | name} [key]
```

Para autenticar a los usuarios que acceden a la línea de comandos a través de una consola, SSH, HTTPS (ASDM, o telnet, o para autenticar a los usuarios que acceden al modo EXEC privilegiado utilizando el comando **enable**, se utiliza la siguiente sintaxis.

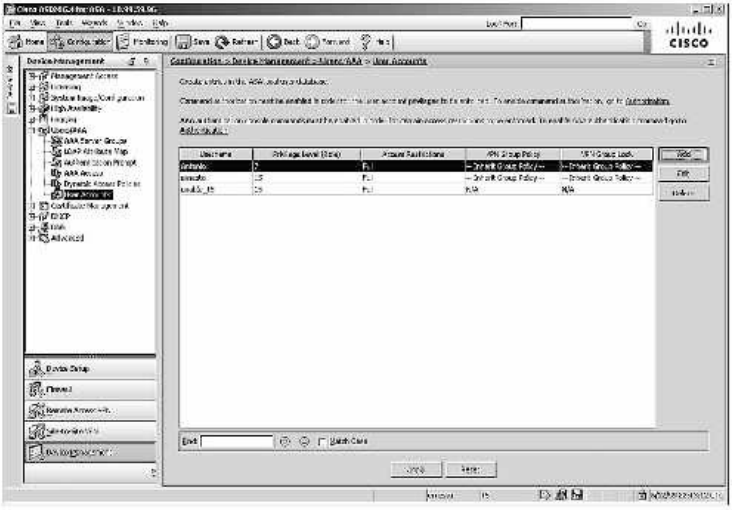
```
ciscoasa(config)#aaa authentication {serial | enable | telnet | ssh
| http} console {LOCAL | server-group [LOCAL]}
```

La siguiente tabla muestra comandos adicionales para la configuración y verificación de AAA en los dispositivos ASA.

Comando	Descripción
`clear config username [name]`	Elimina un usuario de la base de datos local.
`show running-conf username`	Muestra una lista de los usuarios que pueden autenticarse.
`clear config aaa-server`	Elimina la configuración del servidor de autenticación.
`show running-conf aaa-server`	Muestra una lista de los servidores de autenticación.
`clear config aaa`	Borra todos los parámetros de la configuración AAA.

Para habilitar AAA en un ASA a través del asistente ASDM se requieren los siguientes pasos:

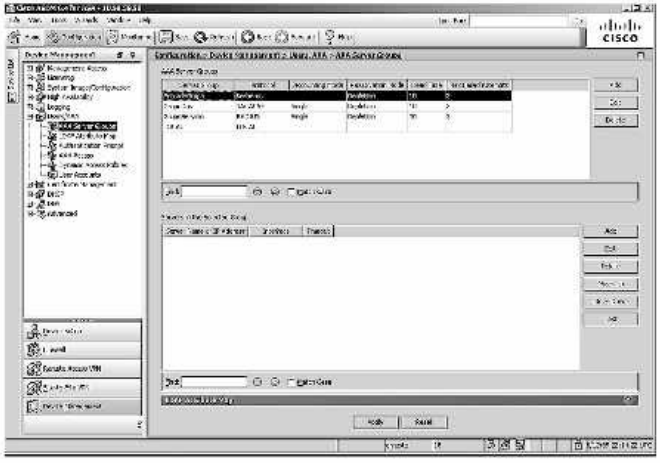
- Crear una base de datos local: elija **Configuration** / **Device Management** / **Users/AAA** / **User Accounts** y luego **Add**, complete los datos solicitados.



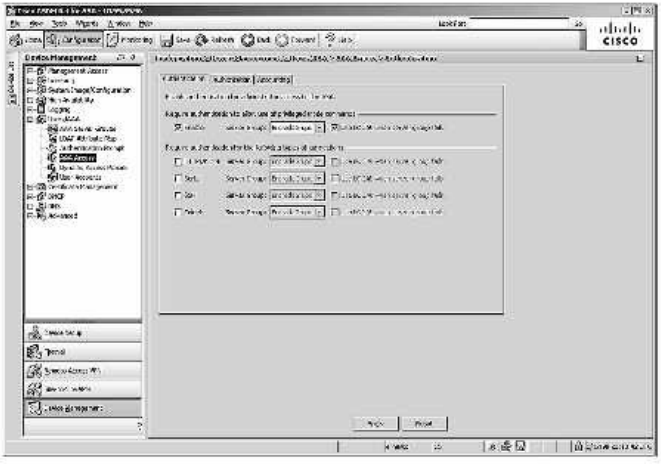
- Crear un grupo de servidores: seleccione **Configuration** / **Device Management** / **Users/AAA** / **AAA Server Groups**, luego **Add** en la parte superior, complete los datos solicitados.

- Agregar los servidores AAA en el grupo de servidores específicos: seleccione **Configuration / Device Management / Users/AAA / AAA Server Groups** y luego **Add** en la parte inferior, complete los datos solicitados.

- Termine el proceso con **Apply**.



Para forzar la autenticación con los grupos de servidores AAA y la base de datos local, seleccione **Configuration / Device Management / Users/AAA / AAA Access**.



7.6.5 Configuración de políticas

MPF (*Modular Policy Framework*) define un conjunto de reglas para la aplicación de funciones del firewall, como la inspección del tráfico que pasa por el ASA y la calidad de servicio. MPF permite la clasificación granular de los flujos de tráfico, para aplicar las distintas políticas avanzadas para los diferentes flujos. MPF se utiliza junto con módulos de hardware para redirigir el tráfico y puede ser utilizado para la inspección avanzada de tráfico de las capas superiores.

Cisco MPF tiene tres puntos clave en su configuración:

- **Clasificar tráfico**: se identifica el tráfico y se crean los criterios que se utilizarán en la configuración del comando **class-map** para clasificar el tráfico de las capas 3 y 4.

```
ciscoasa(config)#class-map class-map-name
ciscoasa(config-cmap)#description description-text
```

Para clasificar todo el tráfico:

```
ciscoasa(config-cmap)#match any
```

Para clasificar solo el tráfico que coincida con las sentencias de una ACL extendida:

```
ciscoasa(config-cmap)#match access-list access-list-name
```

- **Definir acciones**: define y crea una política para el tráfico a través del comando **policy-map**.

```
ciscoasa(config)#policy-map policy-map-name
ciscoasa(config-pmap)#description description-text
```

Especifica un *class map* para realizar las acciones:

```
ciscoasa(config-pmap)#class class-map-name
```

Existe una gran variedad de subcomandos en este modo de configuración, utilice el comando **ayuda** para verlos en su totalidad:

```
ciscoasa(config-pmap-c)# ?
MPF policy-map class configuration commands:
csc Content Security and Control service module
```

```
exit Exit from MPF class action configuration mode
help Help for MPF policy-map class/match submode commands
inspect Protocol inspection services
ips Intrusion prevention services
no Negate or set default values of a command
police Rate limit traffic for this class
priority Strict scheduling priority for this class
quit Exit from MPF class action configuration mode
set Set connection values
```

- **Activar una política**: ejecutar una política en las interfaces donde se aplicara el punto anterior.

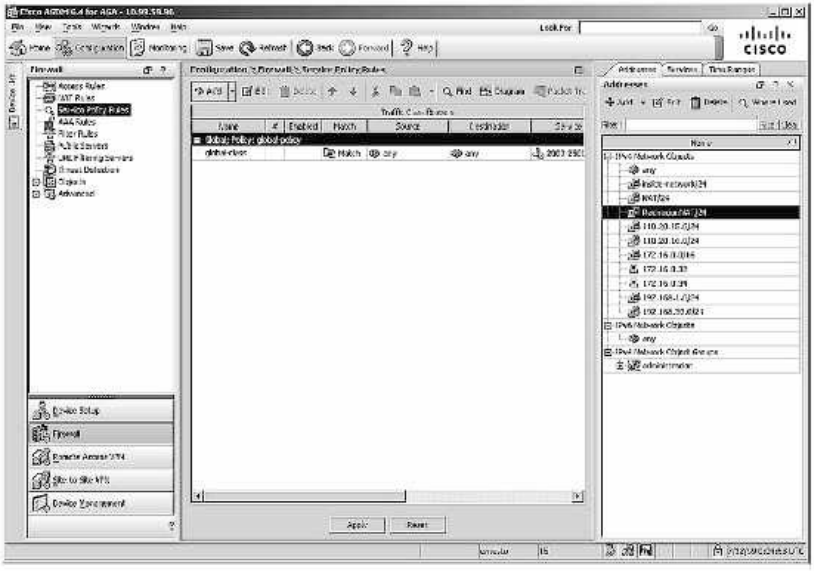
```
ciscoasa(config)#service-policy policy-map-name [global |
interface intf]
```

EJEMPLO:

La siguiente sintaxis es un ejemplo de configuración del comando **policy-map**, en este caso para limitar el número de conexiones al servidor web 10.1.1.1.

```
ciscoasa(config)# access-list http-server permit tcp any host
10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description control de conexiones al servidor
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
32-17
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout idle 0:10:0
```

Para configurar un service policy a traves del asistente ASDM, seleccione **Configuration / Firewall / Service Policy Rules**, y luego **Add**.



7.6.6 Configuración de acceso remoto y VPN

La mejor opción para obtener acceso remoto es la implementación de **SSL VPN** (*Secure Sockets Layer Virtual Private Network*) debido a que proporciona la flexibilidad necesaria para permitir el acceso seguro a todos los usuarios, independientemente de la manera en que se vaya a establecer la conexión.

Los dispositivos ASA soportan tres tipos de accesos remotos VPN:

- **Clientless SSL VPN Remote Access**, a través de un navegador web.
- **SSL o IPsec (IKEv2) VPN Remote Access**, utilizando el cliente Cisco AnyConnect.
- **IPsec (IKEv1) VPN Remote Access**, a través del cliente Cisco VPN.

El ASA soporta IKEv1 para las conexiones desde el cliente CiscoVPN. Para el cliente AnyConnect VPN se requiere IKEv2. Para IKEv2, es posible configurar diferentes tipos de cifrados y autenticación, y múltiples algoritmos de integridad de una única política. Con IKEv1 para cada parámetro, se puede establecer solo un valor.

Cuando la seguridad es el problema, IPsec es la mejor opción, ya que en ese sentido supera ampliamente a SSL.

SSL es un sistema de cifrado que fue creado por Netscape a mediados de la década de 1990 y fue diseñado para permitir comunicaciones seguras en una red insegura como Internet. Proporciona cifrado e integridad de las comunicaciones, así como también autenticación mediante certificados digitales. Los beneficios de SSL son su facilidad de uso y de implementación.

El usuario convencional que requiere acceso remoto VPN IPsec necesita un cliente VPN instalado en el host. Una ventaja de SSL es que no requiere ningún preinstalado de software del cliente. SSL VPN permite a los usuarios acceder a páginas web, servicios de acceso y archivos; permite además enviar y recibir correo electrónico y ejecutar aplicaciones basadas en TCP mediante un navegador.

En muchos casos, IPsec y SSL VPN son complementarios, ya que pueden resolver diferentes problemas. Este enfoque complementario permite a un solo dispositivo hacer frente a todas las necesidades de los usuarios de acceso remoto.

El ASA ofrece dos modos principales de despliegue que se encuentran en las soluciones Cisco SSL VPN:

- **Clientless SSL VPN**: permite a los usuarios establecer una conexión segura, de acceso remoto a través de un túnel VPN al ASA mediante un navegador web. Después de la autenticación, los usuarios acceden a una página del portal y pueden acceder a recursos internos específicos. Aunque resulta más fácil de implementar y más flexible que las basadas en el cliente SSL VPN (Client-Based SSL VPN), SSL VPN sin cliente solo proporciona acceso limitado a los recursos y aplicaciones y puede incluir riesgos de seguridad adicionales cuando se utilizan clientes no corporativos.

- **Client-Based SSL VPN**: requiere una aplicación de cliente VPN que se instala en la máquina remota. Proporciona a los usuarios autenticados el acceso completo a la red y a los recursos corporativos. Sin embargo, los dispositivos remotos requieren una aplicación cliente como el cliente Cisco VPN o el nuevo cliente AnyConnect para ser instalado en el dispositivo del usuario final.

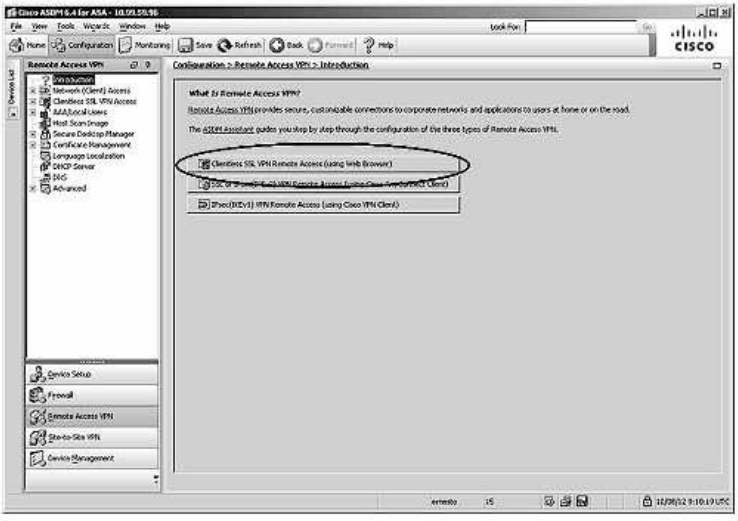
El cliente AnyConnect se puede instalar manualmente en el host, o descargarlo a petición a través de un navegador.

Cuando el cliente AnyConnect está instalado en el host, la conexión VPN puede ser iniciada por la aplicación. Una vez que el usuario se autentica, el ASA examina la revisión del cliente y la actualiza según sea necesario. El cliente AnyConnect, a continuación, finaliza la instalación y se configura, y, finalmente, establece una conexión SSL VPN.

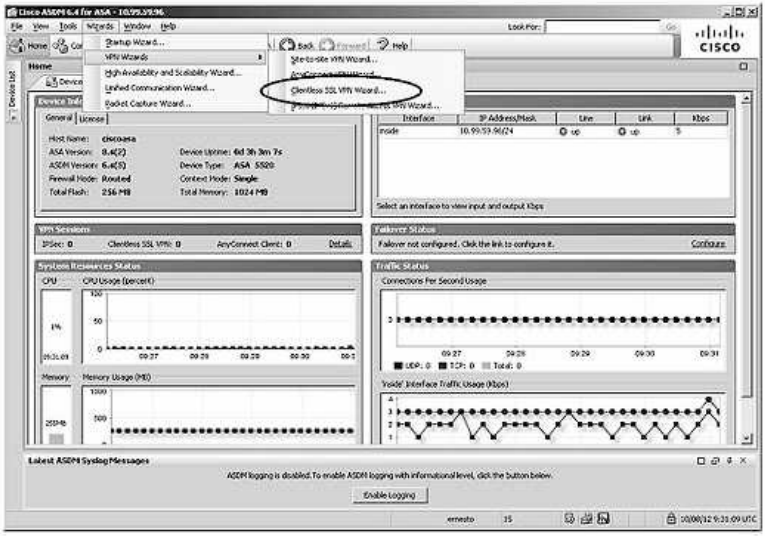
Dependiendo de la política SSL VPN configurada en el ASA, cuando la conexión termina, la aplicación cliente AnyConnect permanecerá instalada en el host o de lo contrario se desinstalará.

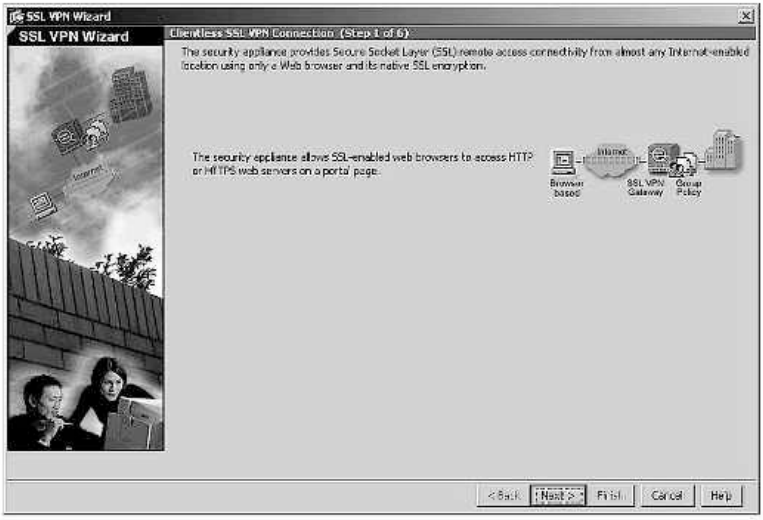
La aplicación puede ser controlada desde el icono situado a la derecha en la barra de tareas.

Para la configuración de Clientless SSL VPN con ASDM elija **Configurations / Remote Access VPN / Introduction** y luego **Clientless SSL VPN Remote Access** (utilizando un navegador web).

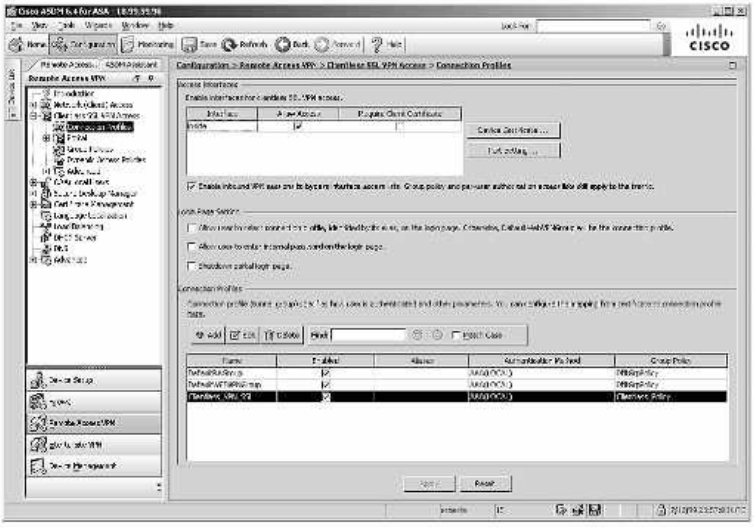


También puede configurarse a través del asistente VPN: desde la barra de menú seleccione **Wizards / VPN Wizards / Clientless SSL VPN Wizard**. Es un proceso de configuración de 6 pasos, complete los datos requeridos en cada uno de ellos.

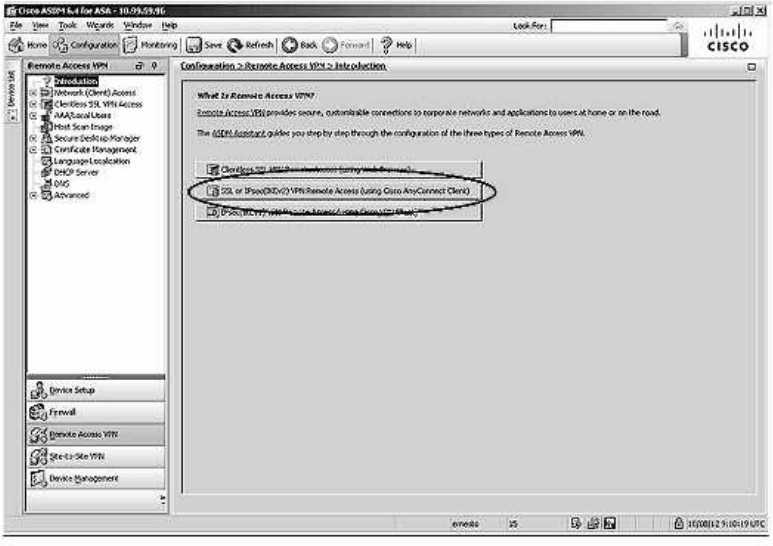




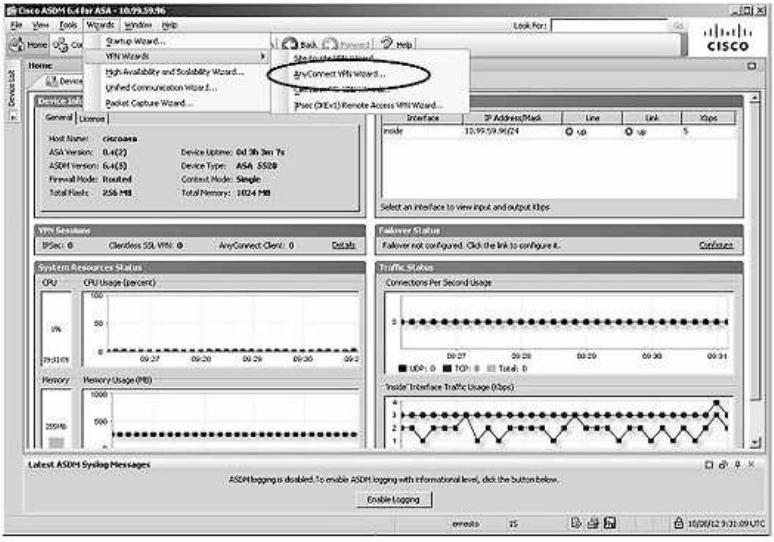
Para verificar la configuración de Clientless SSL VPN elija **Configurations / Remote Access VPN / Clientless SSL VPN Access / Connection Profiles**. Desde esta ventana puede verificarse y editarse la configuración.

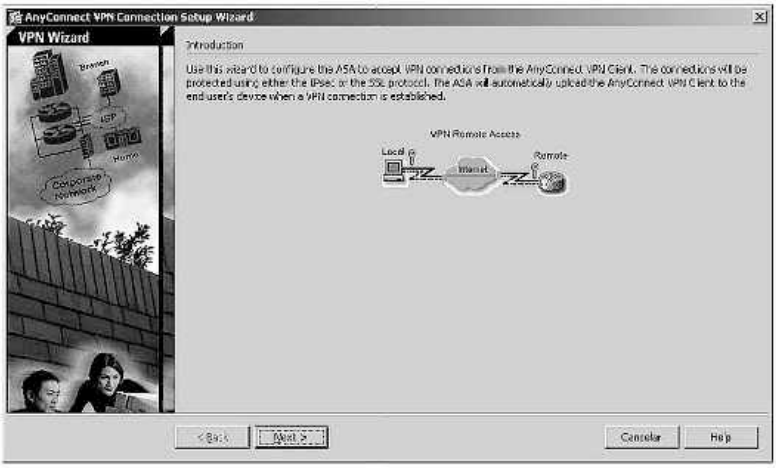


Para la configuración de AnyConnect SSL VPN con ASDM elija **Configurations / Remote Access VPN / Introduction** y luego **SSL or IPsec(IKEv2) VPN Remote Access** (utilizando el cliente Cisco AnyConnect).

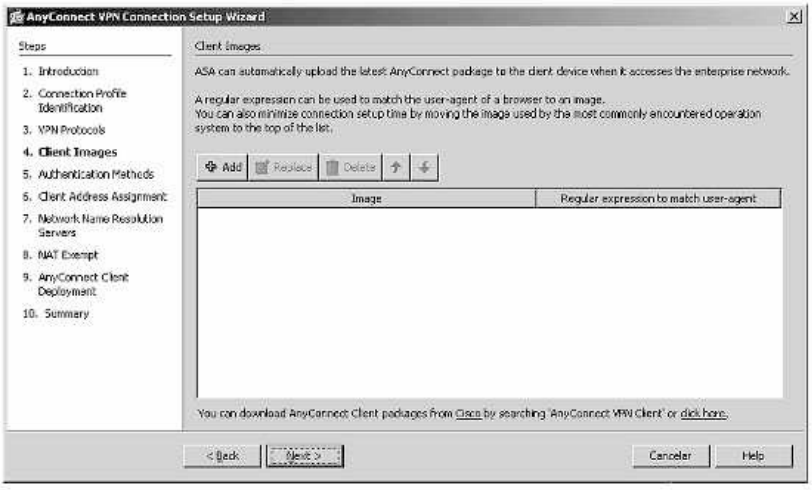


También puede configurarse a través del asistente VPN: desde la barra de menú seleccione **Wizards / VPN Wizards / AnyConnect VPN Wizard**. Es un proceso de configuración de 10 pasos, recuerde que el asistente lo guiará para completar los datos en cada uno de ellos.

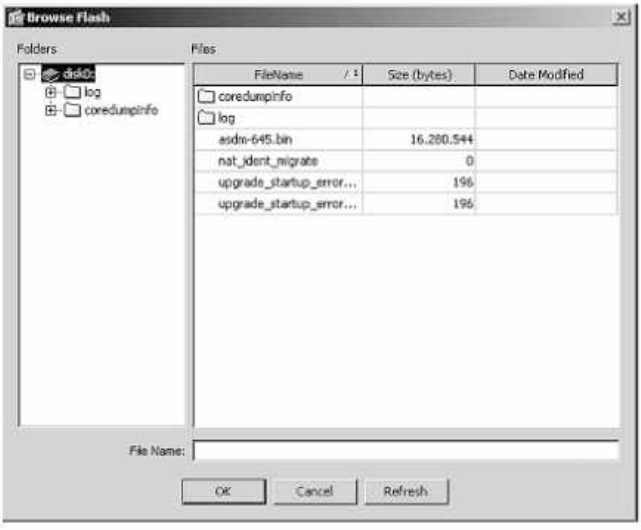




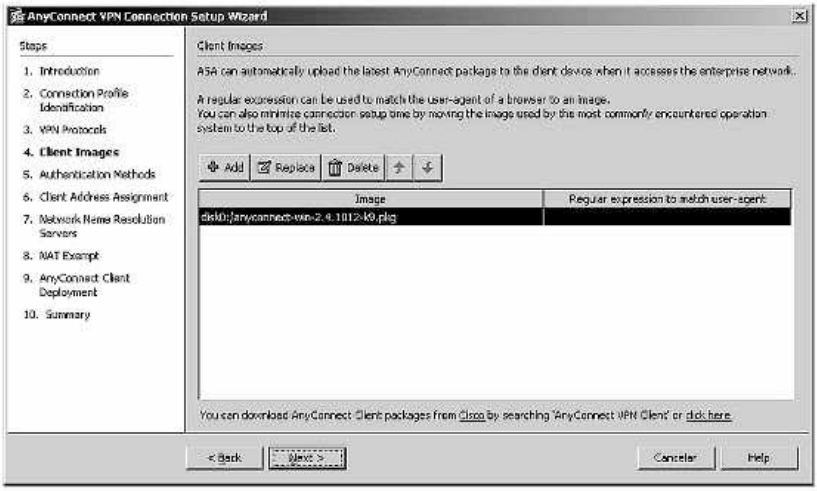
Para agregar las imágenes del cliente AnyConnect en el paso 4, verifique si el archivo **.pkg** existe en la memoria flash. Seleccione **Add** y luego **Browse Flash**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Client Images
ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.
A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.
Add
Replace
Delete
Image
Regular expression to match user-agent
You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.
< Back
Next >
Cancel
Help


Add AnyConnect Client Image
AnyConnect Image:
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help


Browse Flash
Folders
Files
disk0:
log
coredumpinfo
FileName
Size (bytes)
Date Modified
coredumpinfo
log
asdm-645.bin
16,280,544
nat_ident_migrate
0
upgrade_startup_error...
196
upgrade_startup_error...
196
File Name:
OK
Cancel
Refresh

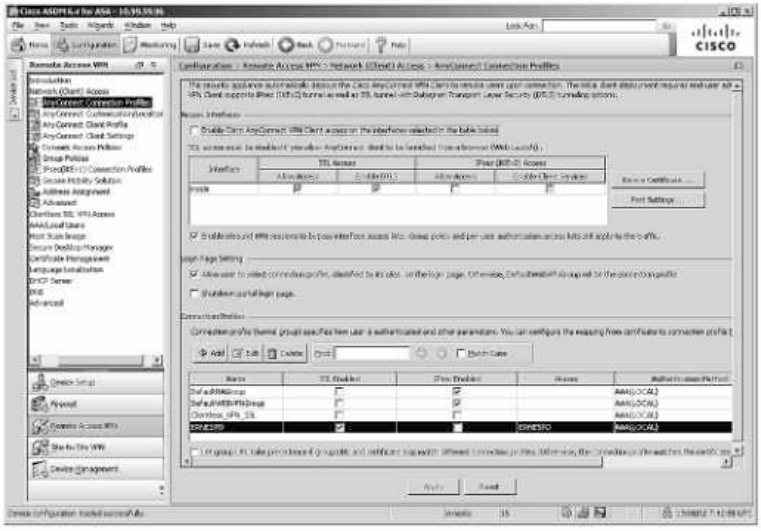
Para agregar el archivo de la imagen seleccione **Upload** y en la siguiente ventana ubique el archivo en el host local desde **Browse Local Files** y luego **Upload File**, el archivo se instalará entonces en la memoria flash.



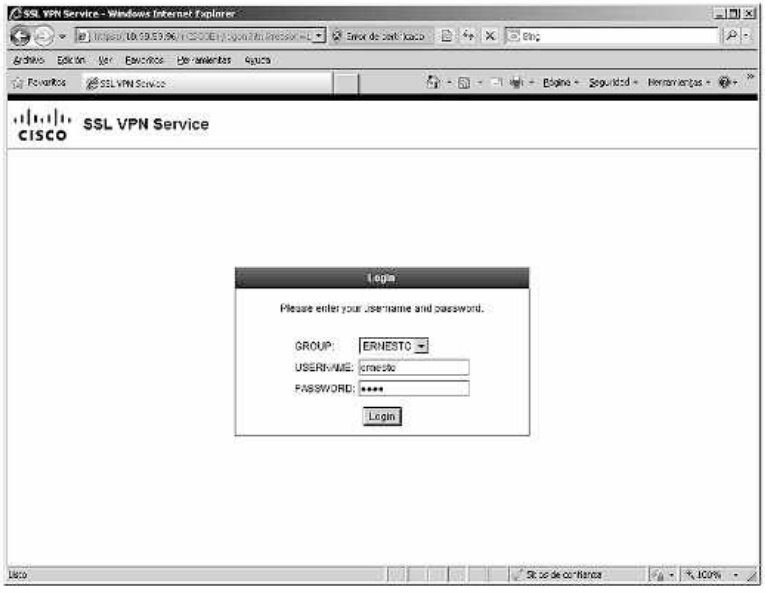
NOTA:

Tenga en cuenta que hay imágenes para host de Linux, Mac OS, Windows y dispositivos móviles.

La configuración de VPN puede ser verificada y modificada desde **Configurations / Remote Access VPN / Network (Client) Access / AnyConnect Connection Profiles**.



Terminada la configuración desde el asistente ASDM, verifique el funcionamiento desde el navegador web.



7.7 FUNDAMENTOS PARA EL EXAMEN

- Estudie las características de cada tipo de firewall.
- Entienda el concepto de DMZ.
- Recuerde qué es CBAC, en qué dispositivos funciona, características y comandos.
- Analice el funcionamiento de un firewall basado en zonas y cómo responden las interfaces en cada una de las zonas.
- Realice todas las configuraciones que le sea posible por CLI y con CCP de firewalls, repítalas.
- Estudie las características del dispositivo Cisco ASA.
- Instale y practique la configuración del Cisco ASA con ASDM. Si no dispone de dispositivos reales, puede hacerlo perfectamente con simuladores.
- Aprenda los comandos y configuraciones de los object groups, ACL, AAA y NAT.
- Estudie las configuraciones y funcionamiento de las VPN con los Cisco ASA.
- Realice topologías en simuladores o en equipos reales.

Capítulo 8

CISCO IPS

8.1 CARACTERÍSTICAS DE LOS IDS E IPS

Los sistemas de detección de intrusiones **IDS** (*Intrusion Detection Systems*) fueron implementados para monitorizar de manera pasiva el tráfico de la red. Un IDS copia el tráfico de red y lo analiza en lugar de reenviar los paquetes reales. Compara el tráfico capturado con firmas maliciosas conocidas de manera offline del mismo modo que el software que busca virus. Esta implementación offline de IDS se conoce como "modo promiscuo".

Al operar con una copia del tráfico el IDS no tiene efectos negativos sobre el flujo real de paquetes del tráfico reenviado; sin embargo, no puede evitar que el tráfico malicioso de ataques de un solo paquete alcance el sistema objetivo antes de aplicar una respuesta para detener el ataque. El IDS generalmente requiere asistencia de otros dispositivos de red, como routers y firewalls, para responder a un ataque.

El sistema de prevención de intrusiones **IPS** (*Intrusion Prevention System*) se apoya en la tecnología IDS ya existente. A diferencia del IDS, un dispositivo IPS se implementa en modo en línea y no permite el paso de tráfico malicioso respondiendo inmediatamente. Esto significa que todo el tráfico de entrada y de salida debe fluir a través de él para ser procesado. El IPS no permite que los paquetes ingresen al lado confiable de la red sin ser analizados primero. Puede detectar, calificar y tratar inmediatamente un problema según corresponda.

El IPS monitoriza el tráfico de capas 3 y 4 y analiza los contenidos y la carga de los paquetes en búsqueda de ataques sofisticados insertos en ellos, que pueden incluir datos maliciosos pertenecientes a las capas 2 a 7. Las plataformas IPS de Cisco utilizan una mezcla de tecnologías de detección, incluyendo detecciones de intrusiones basadas en firma, basadas en perfil y de análisis de protocolo. Este análisis, más profundo, permite al IPS identificar, detener y bloquear ataques que pasarían a través de un dispositivo firewall tradicional. Cuando un paquete pasa a través de una interfaz en un IPS, no es enviado a la interfaz de salida o confiable hasta haber sido analizado.

Las tecnologías IDS e IPS pueden complementarse entre sí basándose en las soluciones de cada una de ellas y en los objetivos de seguridad de la organización. Las tecnologías IDS e IPS se despliegan como sensores, que pueden ser cualquiera de los siguientes dispositivos:

- Un router configurado con software IPS Cisco IOS.
- Un dispositivo diseñado específicamente para proporcionar servicios IDS o IPS dedicados.
- Un módulo de red instalado en un dispositivo de seguridad adaptable, switch o router.

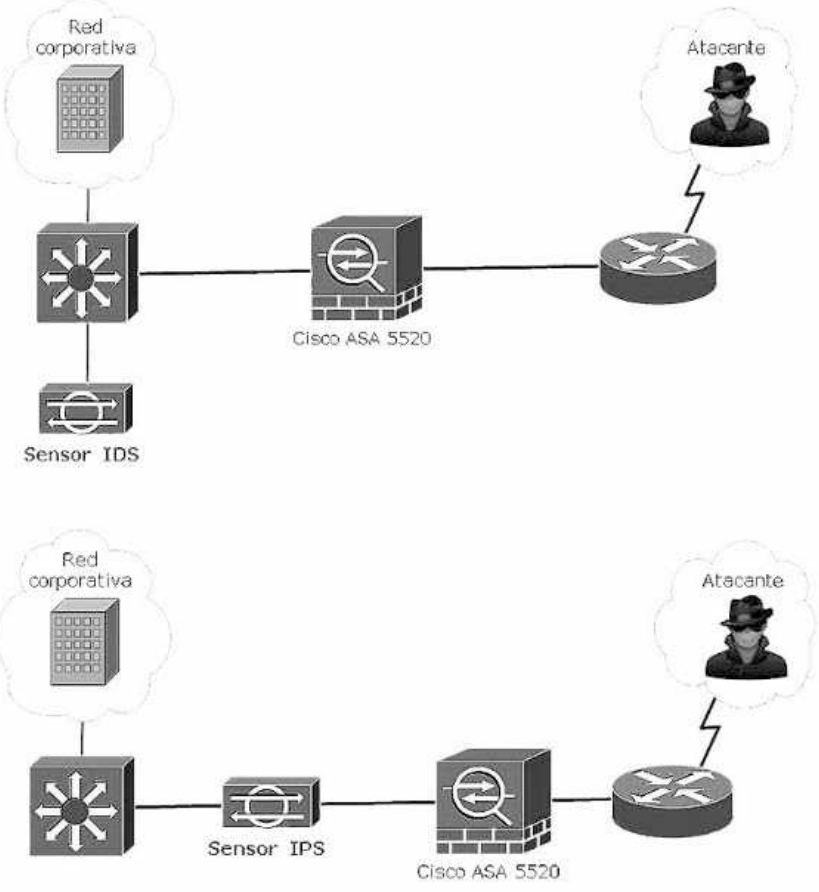
Las características del IDS en modo promiscuo son las siguientes:

- No tiene impacto sobre la red, no crea latencia ni genera jitter.
- La acción de respuestas no puede detectar los paquetes disparadores.
- No tiene impacto sobre la red si el sensor falla o se sobrecarga.
- Se requieren ajustes correctos para las acciones de respuesta.
- Se necesita una política de seguridad bien definida.
- Son más vulnerables a técnicas de evasión.

Las características del IPS en modo en línea son las siguientes:

- Detiene los paquetes disparadores.
- Puede tener algún impacto sobre la red, al crear latencia o jitter.

- Los posibles problemas de los sensores afectan al tráfico de la red.
- Puede utilizar técnicas de normalización de flujo.
- Se necesita una política de seguridad bien definida.



8.1.1 Implementaciones IPS basadas en red

Un IPS de red puede ser implementado utilizando un dispositivo IPS dedicado, como la serie IPS 4200 o puede ser agregado a un router ISR, un dispositivo firewall ASA o un switch Catalyst 6500.

El sistema de monitorización basado en red puede ver fácilmente los ataques que están tomando lugar en toda la red. Sin embargo, los datos cifrados pueden cegar al IPS de red, impidiendo la detección de los ataques.

Los sensores se despliegan en puntos clave de la red para detectar actividad maliciosa y no autorizada en tiempo real y pueden realizar acciones cuando sea necesario. Pueden ser agregados a un router, a un switch Catalyst 6500 o a un firewall ASA con un módulo adecuado.

Los sensores IPS de red generalmente se ajustan para el análisis de prevención de intrusiones. En el sistema operativo subyacente de la plataforma sobre la que se monta el IPS se quitan los servicios de red innecesarios y se aseguran los servicios esenciales.

El hardware debe incluir tres características importantes:

- **Placa de red**: el IPS de red debe poder conectarse a cualquier red ya sea Ethernet, Fast Ethernet o Gigabit Ethernet.

- **Procesador**: la prevención de intrusiones requiere ciclos de CPU para realizar análisis de detección de intrusiones y búsqueda de coincidencias en los patrones.

- **Memoria**: el análisis de detección de intrusiones hace un uso intensivo de la memoria, que afecta directamente a la habilidad de un IPS de red de detectar un ataque eficientemente y de manera precisa.

Pueden agregarse hosts adicionales a las redes protegidas sin requerir más sensores. Solo se requerirán sensores adicionales cuando su tasa de capacidad de tráfico se exceda, cuando su rendimiento no satisfaga las necesidades actuales o cuando una revisión en la política de seguridad o diseño de la red solicite sensores adicionales para ayudar a aplicar fronteras de seguridad. Cuando se agregan nuevas redes remotas o locales, los sensores adicionales son fáciles de desplegar.

Los ISR 1841, 2800 y 3800 de Cisco pueden ser configurados para soportar funciones IPS usando IPS IOS de Cisco, lo cual es parte del grupo de funciones del firewall Cisco IOS. Esto no necesita la instalación de un módulo IPS pero sí requiere la descarga de archivos de firmas y una memoria adecuada para cargarlas.

Además de los IPS IOS de Cisco, Cisco ofrece una variedad de soluciones de IPS basadas en dispositivos y módulos que se detallan en la siguiente tabla:

Dispositivo	Solución	Características
Advanced Integration Module (AIM) IPS de Cisco y Network Module Enhanced (IPS NME)	Recomendado para las pequeñas y medianas empresas y sucursales. Proporciona funciones IPS avanzadas y mantiene el bajo costo de la solución. Se debe revisar el software y hardware del IOS de Cisco para asegurar la compatibilidad.	Integra IPS a los routers Cisco 1841, 2800 y 3800. IPS AIM ocupa una ranura AIM interna del router, integra su propia CPU y memoria. Proporciona protección de intrusiones con todas las funciones. Puede inspeccionar tráfico GRE e IPsec. El IPS IOS de Cisco y el AIM IPS / NME IPS no pueden ser usados en conjunto.
Cisco Adaptive Security Appliance Advanced Inspection y Prevention Security Services Module (ASA AIP-SSM)	Utiliza tecnología de inspección y prevención avanzada para proporcionar servicios de seguridad de alto rendimiento como servicios de prevención de intrusiones y anti-X avanzados.	Módulo de alto rendimiento para la serie ASA 5500. No utiliza disco para mejorar la confiabilidad. Incluye módulos con diferente capacidad de memoria.
Sensores de la serie IPS 4200 de Cisco	Combinan servicios de prevención de intrusiones en línea con tecnologías innovadoras que mejoran la exactitud en la detección, clasificación y detención de amenazas, incluyendo gusanos, *spyware*, *adware* y virus de red. Como resultado, pueden detenerse más amenazas sin el riesgo de descartar tráfico de red legítimo.	Proporciona una detección de ataques sofisticada para los dispositivos, servicios y aplicaciones de la red. El software de sensor IPS de Cisco versión 5.1 incluye habilidades de detección aumentadas y funciones de escalabilidad, adaptabilidad y rendimiento mejoradas.
Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2)	Como parte de la solución IPS de Cisco, trabaja en conjunto con otros componentes para proteger eficientemente la estructura de datos.	Módulo de protección de intrusiones integrado al switch. Soporta un número ilimitado de VLAN. Capacidad de prevenir intrusiones. Ejecuta la imagen Cisco IPS Sensor Appliances.

8.2 FIRMAS IPS

Cuando los sensores escanean los paquetes de la red, utilizan las firmas para detectar algún tipo de actividad intrusiva, como ataques de DoS, y responder con acciones predefinidas. Estas firmas identifican puntualmente gusanos, virus, anomalías en los protocolos o tráfico malicioso específico.

Cuando un sensor encuentra una coincidencia entre una firma y un flujo de datos, realiza una acción, como dejar constancia del evento en el registro o enviar una alarma al software de administración del IDS o IPS.

Las firmas se dividen en tres partes bien definidas:

- **Tipo**
- **Alarma**
- **Acción**

Basándose en la severidad percibida de la firma puede ajustarse a uno de estos cuatro niveles de severidad:

- **Alto**: se detectan los tipos de ataques usados para ganar acceso o causar un ataque de DoS y es extremadamente probable una amenaza inmediata.
- **Medio**: se detecta la actividad de red anormal que puede ser considerada maliciosa y es probable una amenaza inmediata.
- **Bajo**: la actividad de red anormal que puede ser considerada maliciosa es detectada, pero es poco probable una amenaza inmediata.
- **Informativo**: la actividad que dispara la firma no es considerada una amenaza inmediata, pero muestra información útil.

Así como los antivirus deben actualizar constantemente sus bases de datos de virus, los administradores de red deben vigilar y descargar las actualizaciones al archivo de firmas IPS. Las nuevas firmas están disponibles en *cisco.com*.

8.2.1 Tipos de firmas

Los tipos de firma se categorizan en dos grupos:

- **Atómicos**: es la forma más simple. Consiste en un solo paquete, actividad o evento examinado para determinar si coincide con una

forma configurada. Si lo hace, se dispara una alarma y se realiza una acción de firma. La detección de firmas atómicas consume un mínimo de recursos y son fáciles de identificar y entender gracias a que se las compara con un evento o paquete específico. El análisis de tráfico de estas firmas atómicas generalmente puede ser llevado a cabo muy rápida y eficientemente. Los IDS son particularmente vulnerables a los ataques atómicos, porque hasta el momento que encuentran el ataque, los paquetes únicos maliciosos han sido permitidos dentro de la red. Los IPS, en cambio, evitan la entrada de estos paquetes a la red.

- **Compuestos**: también se conocen como firmas stateful (con estados). Este tipo de firma identifica una secuencia de operaciones distribuidas en múltiples hosts durante un período de tiempo arbitrario. A diferencia de las firmas atómicas, las firmas compuestas, al ser firmas con estados, generalmente requieren varios datos para asociar una firma de ataque, por lo que el dispositivo IPS debe mantener información de estados. La cantidad de tiempo que las firmas deben mantener la información de estados se conoce como "horizonte de eventos". La longitud de un horizonte de eventos varía de una firma a la otra. El IPS no puede mantener la información de estados por un período indeterminado sin eventualmente quedarse sin recursos. Por lo tanto, un IPS usa un horizonte de eventos configurado para determinar cuánto tiempo debe buscar una firma de ataque específica cuando se detecta un componente inicial de firma. Configurar la longitud del horizonte de eventos es un balance entre el consumo de los recursos del sistema y la capacidad de detectar un ataque que toma lugar durante un período extenso de tiempo.

NOTA:

Las firmas IPS son conceptualmente similares al archivo virus.dat utilizado por los escáneres de virus.

8.2.2 Alarmas de firmas

La alarma de firma, también conocida como disparador de firma es el fundamento de una firma IPS. El disparador de la firma de un sensor IPS puede ser cualquier cosa que pueda señalar a un intruso o una violación a las políticas de

seguridad. Un IPS de red puede disparar una acción de firma si detecta un paquete cuya carga contiene una cadena específica que se dirige a un puerto específico.

Estos mecanismos disparadores pueden ser aplicados tanto a firmas atómicas como a firmas compuestas; a su vez, los disparadores pueden ser simples o complejos.

Los sensores IDS e IPS de Cisco (sensores IPS 4200 Series de Cisco y Catalyst 6500 - IDSM) pueden usar cuatro tipos de disparadores de firma:

- **Detección basada en patrones**: también conocida como detección basada en firmas, es el mecanismo disparador más simple, ya que busca un patrón predefinido específico. Un sensor IDS o IPS basado en firmas compara el tráfico de la red con una base de datos de ataques conocidos y dispara una alarma o detiene las comunicaciones si se encuentra una coincidencia.

- **Detección basada en anomalías**: se conoce también como detección basada en perfiles, involucra primero la definición de un perfil de lo que se considera normal para la red o el host. Este perfil normal puede ser determinado monitorizando la actividad de la red o aplicaciones específicas en el host durante un período de tiempo. También puede basarse en una especificación definida, como una RFC. Luego de definir la actividad normal, la firma dispara una acción si ocurre actividad que excede un umbral específico que no está incluido en el perfil normal. La ventaja de la detección basada en anomalías es que pueden detectarse ataques nuevos y previamente no publicados.

- **Detección basada en políticas**: también conocida como detección basada en comportamiento, es similar a la detección basada en patrones, pero en lugar de tratar de definir patrones específicos, el administrador define comportamientos sospechosos basándose en un análisis histórico.

- **Detección basada en señuelo**: también conocida como detección basada honeypots utiliza un servidor ficticio para atraer a los atacantes. El propósito del honeypots es distraer a los atacantes de los dispositivos de red reales como una especie de señuelo. Al montar diferentes tipos de vulnerabilidades en el servidor honeypot, los administradores pueden analizar los tipos de ataques y patrones de tráfico malicioso entrantes. Los sistemas honeypot raramente se usan en ambientes de producción. Los antivirus y otros proveedores tienden a usarlos para investigación.

Otro mecanismo disparador común es la llamada decodificación de protocolos. En lugar de solo buscar un protocolo en cualquier parte del paquete, las decodificaciones de protocolos fragmentan el paquete según los campos del protocolo y luego buscan patrones específicos u otros aspectos malformados en los campos específicos del protocolo. La ventaja de la decodificación de protocolos es que permite una inspección más granular del tráfico y reduce el número de falsos positivos.

Las alarmas se disparan cuando se cumplen parámetros específicos. El administrador debe equilibrar el número de alarmas incorrectas que pueden ser toleradas y la habilidad de la firma de detectar intrusos reales. Si hay pocas alarmas, puede ser que se esté permitiendo la entrada a la red de paquetes sospechosos, pero el tráfico de red fluirá más rápidamente. Sin embargo, si los sistemas IPS usan firmas sin ajustar, producirán muchas alarmas de falso positivo.

Una alarma de falso positivo es un resultado esperado pero no deseable. Ocurre cuando el sistema de intrusos genera una alarma luego de procesar tráfico normal que no debería disparar una alarma. El análisis de falsos positivos limita el tiempo del que dispone el analista de seguridad para examinar actividad de intrusos real en la red. Si esto ocurre, el administrador debe asegurarse de ajustar el IPS para cambiar estos tipos de alarma a negativos reales. Un negativo real describe una situación en la que el tráfico de red normal no genera una alarma.

Un falso negativo ocurre cuando el sistema de intrusos falla en la generación de una alarma luego de procesar tráfico de un tipo de ataque que está configurado para detectar.

Deben considerarse varios factores en la implementación de las alarmas utilizadas por la firma:

- El nivel asignado a la firma determina el nivel de severidad de la alarma.
- Al ajustar una alarma de firma, el nivel de severidad de la firma debe ser el mismo que el de la alarma.
- Para minimizar la cantidad de falsos positivos, se deben estudiar los patrones de tráfico existentes y luego ajustar las firmas para reconocer patrones de intrusos atípicos.
- El ajuste de las firmas debe basarse en los patrones de tráfico reales de la red.

8.2.3 Acciones de firmas

Cada vez que una firma detecta actividad para la cual está configurada, dispara una o más acciones. Las acciones que pueden llevarse a cabo son las siguientes:

1. **Generar una alerta**
   - **Producir una alerta**: esta acción ingresa el evento al Event Store como una alerta.
   - **Producir una alerta detallada**: esta acción incluye una transcripción codificada en la alerta del paquete ofensivo.
2. **Ingresar la actividad en el registro**
   - **Registrar paquetes atacantes**: esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta.
   - **Registrar paquetes pares**: esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y de la víctima.
   - **Registrar paquetes de la víctima**: esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta.
3. **Descartar o detener la actividad**
   - **Denegar al atacante en línea**: esta acción detiene el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo determinado. El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. El temporizador se actualiza en cada nuevo ataque. Si la lista de paquetes denegados está llena, el paquete será denegado de todas formas.
   - **Denegar conexión en línea**: esta acción termina el paquete actual y los futuros en este flujo TCP.
   - **Denegar paquetes en línea**: esta acción termina el paquete.
4. **Reiniciar una conexión TCP**: esta acción envía un TCP resets para tomar el control del flujo y terminarlo.

5. **Bloquear actividad futura**.

   - **Solicitar bloqueo de conexión**: esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
   - **Solicitar bloqueo del host**: esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
   - **Solicitar SNMP trap**: esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP.

6. **Permitir la actividad**: la acción de permiso es necesaria para que el administrador pueda definir las excepciones de las firmas configuradas ya que pueden primero denegar todo y luego permitir solo la actividad necesaria.

8.2.4 Administración y monitorización IPS

La monitorización de los eventos de seguridad de la red permite identificar con precisión los ataques y las violaciones a la política de seguridad que toman lugar en la red. Existen cuatro factores a considerar en el planteamiento de la monitorización:

- **Administración**: los sensores IPS pueden ser administrados individual o centralmente acorde al tamaño de la red. La administración individual de varios routers y sensores IPS se vuelve difícil y toma mucho tiempo.
- **Correlación de eventos**: es el proceso por el cual se correlacionan ataques y otros eventos que toman lugar simultáneamente en diferentes puntos de una red. Posteriormente, una herramienta de correlación podrá luego ordenar las alertas basándose en las marcas de tiempo sin importar qué dispositivo detectó el evento. Otorgar marcas de tiempo a los eventos con un sistema de tiempo común como un servidor NTP (*Network Time Protocol*) permite una mayor precisión en las marcas de tiempo de todas las alertas generadas por los IPS.
- **Personal de seguridad**: las grandes empresas requieren personal apropiado para analizar esta actividad y determinar cómo el IPS está protegiendo la red. Examinar estas alertas también permite ajustar y optimizar la operación del IPS en relación con los requisitos únicos de la red.

- **Plan de respuesta a incidentes**: cuando un sistema de la red se halla comprometido, debe implementarse un plan de respuesta. El sistema comprometido debe ser devuelto al estado en que estaba antes del ataque y determinar las consecuencias de lo acontecido.

Cuando se detecta una firma de ataque, la función IPS del IOS puede enviar un mensaje syslog o una alarma en formato SDEE (*Secure Device Event Exchange*). Este formato fue desarrollado para mejorar la comunicación de eventos generados por dispositivos de seguridad. Un mensaje de alarma de sistema SDEE tiene este tipo de formato:

```
%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address
[192.168.121.1:137 - >192.168.121.255:137]
```

NOTA:

Aunque la CLI puede ser utilizada para configurar un despliegue de IPS, es más simple utilizar un administrador de dispositivos como CCP. Múltiples sensores IPS pueden ser administrados también con el Cisco IPS Manager Express (IME) o el Cisco Security Manager (CSM).

8.3 CONFIGURACIÓN DE CISCO IOS IPS

8.3.1 Configuración de IPS con CLI

Configurar la CLI de IOS de Cisco con las firmas de formato IPS IOS 5.x conlleva varios pasos. El IOS de Cisco versión 12.4(10) y los anteriores utilizaban firmas de formato IPS 4.x y algunos de los comandos actuales se han modificado.

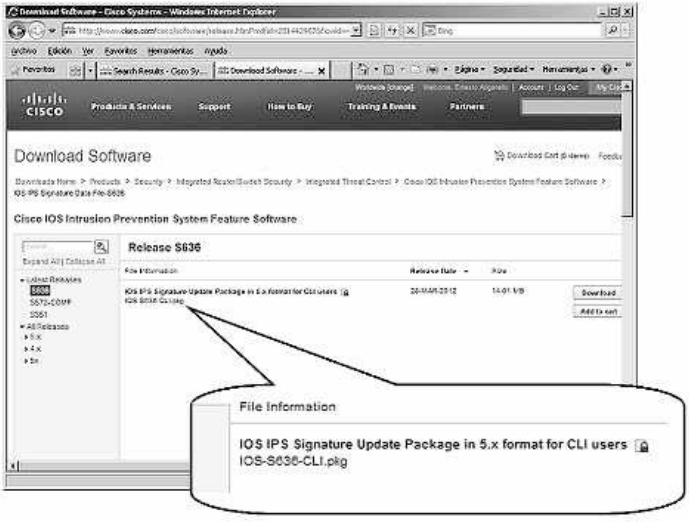
Antes de configurar IPS, es necesario descargar los archivos del paquete de firmas del IPS IOS y la clave criptográfica pública de *cisco.com*. Los archivos IPS específicos que se descargarán varían en relación con la versión en uso. Solo los clientes registrados pueden descargar los archivos de paquete y clave.

El formato del paquete de firmas es el siguiente:

- **IOS-Sxxx-CLI.pkg**

El formato de la clave criptográfica pública utilizada por el IPS IOS es el siguiente.

- **realm-cisco.pub.key**



Los siguientes comandos crean o modifican un directorio existente en la memoria flash para almacenar los archivos de firmas y configuraciones.

```
Router#mkdir directory-name
Router#rename current-name new-name
```

```
Router# mkdir security

Mkdir file name [security]?
Created dir flash: security
```

Para verificar los contenidos de la flash, ingrese el comando **dir flash:**

```
Router#dir flash:

Router# dir flash:
Directory of flash:

2 drwx 0 Mar 13 1993 13:16:21 security
8128000 bytes total (8126976 bytes free)
```

La clave criptográfica descargada anteriormente (*realm-cisco.pub.key.txt*) verifica la firma digital del archivo de configuración principal (*sigdef-default.xml*). El contenido del archivo está firmado con una clave privada de Cisco para garantizar su autenticidad e integridad.

Si la clave no es válida o está configurada incorrectamente se genera un mensaje de error, debe ser eliminada y reconfigurada.

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found
(key not found
```

Utilice los comandos **no crypto key pubkey-chain rsa** y **no named-key realm-cisco.pub signature** para reconfigurar la clave.

Para confirmar que la clave criptográfica está configurada utilice el comando **show run**.

```
Router# show run
.....................................
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
Quit
```

A partir de ahora se inicia el proceso de configuración del IPS. Se debe identificar el nombre de la regla IPS y especificar la ubicación.

```
Router(config)#ip ips name [rule name] [optional ACL]
```

El último parámetro de este comando añade una ACL para filtrar el tráfico escaneado, todo el tráfico que la ACL permite está sujeto a inspección por el IPS, de lo contrario no será inspeccionado por el IPS.

Para configurar la ubicación del almacenamiento de la firma IPS en las versiones actuales de IOS se utiliza el comando:

```
Router(config)# ip ips config location flash:directory-name
```

Para versiones anteriores a la IOS 12.4(11)T, se utiliza el comando:

```
Router(config)# ip ips sdf location
```

Hay que habilitar la notificación de eventos de registro y **SDEE** (*Security Device Event Exchange*) configurando el servidor http y posteriormente la notificación de eventos SDEE IPS. Las notificaciones SDEE están deshabilitadas por defecto y deben ser habilitadas explícitamente.

```
Router(config)# ip http server
Router(config)# ip ips notify sdee
```

El registro de notificaciones mostrará los mensajes de registro IPS en la consola. Está habilitado por defecto, pero puede configurarse con el siguiente comando.

```
Router(config)# ip ips notify log
```

Para mostrar nuevas alertas SDEE en la consola del router, ejecute el comando **debug ip sdee**.

Como ayuda a la recuperación de errores puede borrar la memoria de eventos SDEE; desde el router ejecute el comando **clear ip sdee**.

Las firmas se agrupan en categorías jerárquicas, lo que permite clasificarlas para agruparlas y ajustarlas más fácilmente. Las tres categorías más comunes son:

- **all**
- **basic**
- **advanced**

Las firmas pueden ser dadas de baja para que el IPS IOS no las compile en la memoria para escanear o reincorporarlas para instruir al IPS IOS a compilarlas en la memoria y usarlas luego para escanear el tráfico.

Cuando se configura por primera vez el IPS IOS, todas las firmas de la categoría **all** deben ser dadas de baja y luego algunas selectas deben ser reincorporadas a una categoría para que se haga menos uso de la memoria.

Para dar de baja y reincorporar las firmas, se utilizan los siguientes comandos respectivamente:

Comando	Descripción
`ip ips signature-category`	Ingresa al modo de categoría de IPS.
`category` *category-name*	Determina el modo de acción de categoría.
`retired true`	Para dar de baja una categoría.
`retired false`	Para reincorporar una categoría.

EJEMPLO:

En la siguiente sintaxis se han retirado todas las firmas en la categoría **all**, y se ha reincorporado la categoría **ios ips basic**.

```
Cisco_IPS(config)#ip ips signature-category
Cisco_IPS(config-ips-category)# category all
Cisco_IPS(config-ips-category-action)# retired true
Cisco_IPS(config-ips-category-action)# exit
Cisco_IPS(config-ips-category)# category ios_ips basic
Cisco_IPS(config-ips-category-action)# retired false
Cisco_IPS(config-ips-category-action)# exit
Cisco_IPS(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
Cisco_IPS(config)#
```

NOTA:

IPS IOS procesa los comandos de categoría en el orden listado en la configuración. Si se configuran varias categorías y una firma pertenece a más de una de ellas, las propiedades de la firma en la categoría serán las que se configuraron al final.

La regla IPS debe aplicarse a una interfaz determinada.

```
router(config-if)#ip ips rule-name [in | out]
```

El tráfico será inspeccionado según sea de entrada o de salida, dependiendo de los argumentos in-out configurados.

Finalmente, el paquete de firmas debe copiarse en el router. El método más común es un servidor TFTP. Verifique la conectividad hacia el servidor y utilice el siguiente comando.

```
copy ftp://ftp_user: Server_IP_address/signature_package idconf
```

```
router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
*Feb 10 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Feb
14 2008
*Feb 10 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8
signatures - 1 of 13 engines
*Feb 10 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time
4 ms - packets for this engine will be scanned
*Feb 10 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622
signatures - 2 of 13 engines
*Feb 10 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time
6024 ms - packets for this engine will be scanned
*Feb 10 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced -
35 signatures - 12 of 13 engines
*Feb 10 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced -
build time 16 ms - packets for this engine will be scanned
*Feb 10 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25
signatures - 13 of 13 engines
*Feb 10 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build
time 32 ms - packets for this engine will be scanned
*Feb 10 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed
time 31628 ms
```

Para verificar que el paquete de firmas esté compilado apropiadamente utilice el siguiente comando:

```
show ip ips signature count
```

```
router#show ip ips signature count
Cisco SDF release version S310.0 ß signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8
Signature Micro-Engine: service-msrpc: Total Signatures 25
```

```
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures: 351 ß total compiled signatures for the
IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
router#
```

NOTA:

No reincorpore la categoría all. Esta categoría de firma contiene todas las firmas de la versión de firmas. El IPS IOS no puede compilar y usar todas las firmas de una vez, porque esto agotaría su memoria.

8.3.2 Configuración de IPS con CCP

CCP proporciona controles para la aplicación de Cisco IOS IPS en las interfaces, la importación y edición de archivos de firmas de *cisco.com* y la configuración de la acción que el IPS tomará si se detecta una amenaza. Las tareas de gestión de routers y dispositivos de seguridad se muestran en un panel de tareas en la parte izquierda de la página principal del CCP.

Seleccione **Configure** / **Security** / **Intrusion Prevention** para mostrar las opciones de prevención de intrusos en CCP.

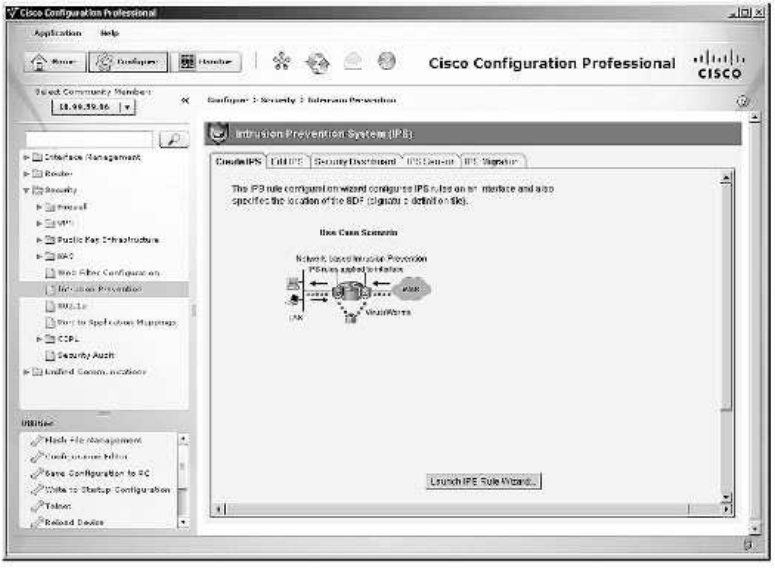
Las pestañas en la parte superior de la ventana del IPS sirven para configurar o supervisar al IPS.

- **Create IPS**: inicia el asistente para crear algunas reglas nuevas IP en una interfaz y especificar la ubicación del archivo de definición de firma.
- **Edit IPS**: se pueden editar las reglas o eliminarlas de interfaces.
- **Seguridad Dashboard**: muestra una tabla de las principales amenazas e implementa firmas asociadas a esas amenazas.

- **Sensor IPS**: gestiona el sensor IPS, realiza los ajustes de conmutación por error y configura las ACL para las interfaces supervisadas.

- **IPS Migration**: las configuraciones de Cisco IOS IPS que se crearon con versiones anteriores del software Cisco IOS pueden migrarse a versiones superiores. La migración no está disponible en las versiones anteriores de Cisco IOS versión 12.4 (11) T.

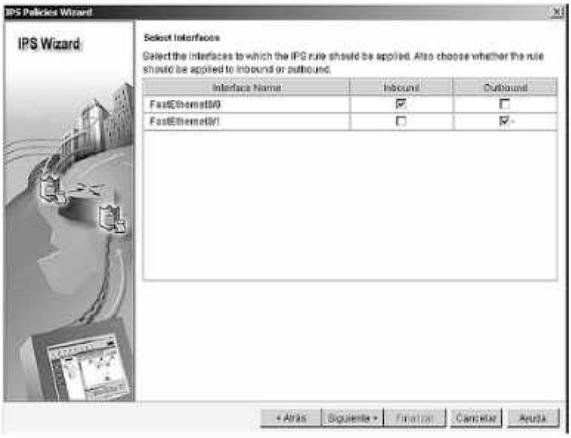
Se puede utilizar CCP para crear una nueva regla en un router Cisco de forma manual a través de la pestaña **Edit IPS**, o automáticamente mediante el asistente para reglas de IPS desde el botón **Launch IPS Rule wizard**. El asistente lleva a cabo todos los pasos de configuración de Cisco IOS IPS.



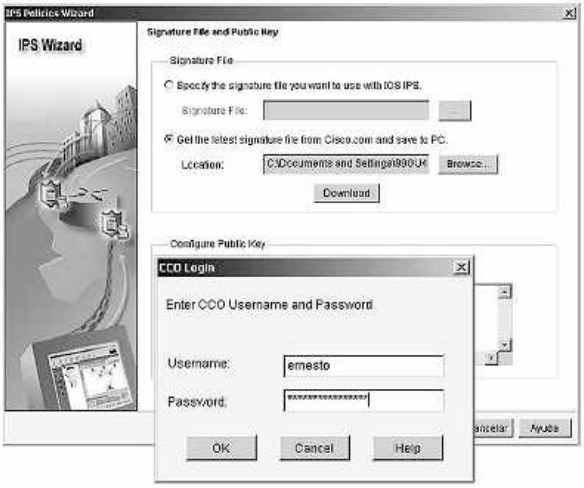
La configuración de Cisco IOS IPS en un dispositivo de seguridad o router con CCP implica los siguientes pasos:

- Seleccione **Configure** / **Security** / **Intrusion Prevention** / **Create IPS**. Pulse el botón **Launch IPS Rule wizard**. Si la notificación SDEE no está activada en el router, aparecerá un aviso indicando que CCP abrirá una suscripción con el router para obtener los eventos SDEE. Acepte con **OK**. La ventana muestra la bienvenida al asistente para políticas de IPS, continúe con **Siguiente**.

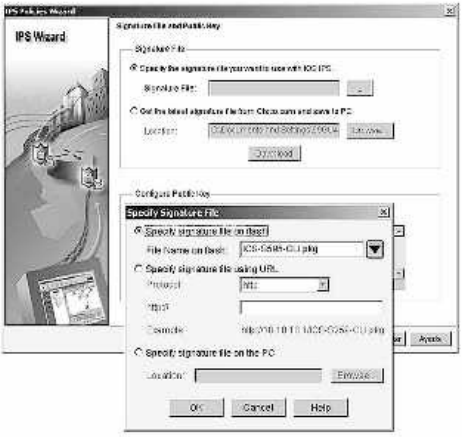
- En la ventana **Select Interfaces** hay que elegir las interfaces a las que aplicar la regla de IPS y el sentido del tráfico marcando una o ambas casillas. Continúe con **Siguiente**.



- En la ventana **Signature File and Public Key** especifique el archivo de firma que desea utilizar con IPS IOS o descargue el último archivo de firma desde *cisco.com* e indique en el cuadro de texto la ruta para guardar la firma en el PC.



- Si ya posee una copia del archivo de la firma y no es necesario que lo descargue especifique que desea utilizarlo con la opción IOS IPS. Puede acceder al archivo de definición de firma (SDF) utilizando un archivo flash en el propio router, a través de TFTP, o por medio de un archivo guardado en el PC. Continúe con **Siguiente**.



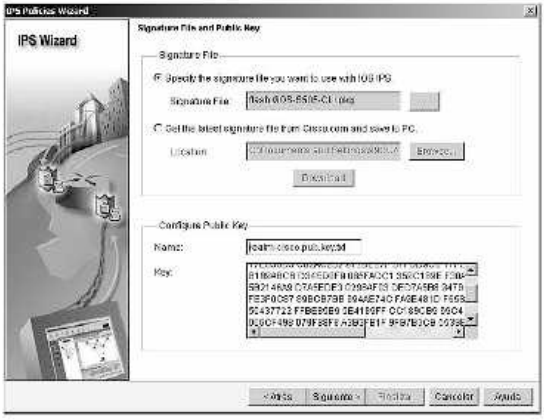
NOTA:

Recuerde que el archivo de firma es un paquete de actualización de IOS IPS con la convención de nombres de IOS-Snnn-CLI.pkg, donde nnn es el número del conjunto de firmas.

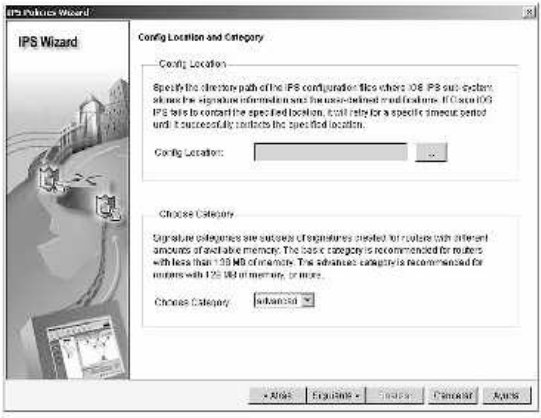
Si la clave pública no se ha descargado previamente y guardado en el PC, descárguela desde *cisco.com*. Abra el archivo de clave pública en un editor de texto y copie el nombre en la casilla **Name** (será del tipo realm-cisco.pub signature). Copie el texto entre la frase "key-string" y la palabra "quit" en el campo **Key**, observe la sintaxis:

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
```

```
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
Quit
```



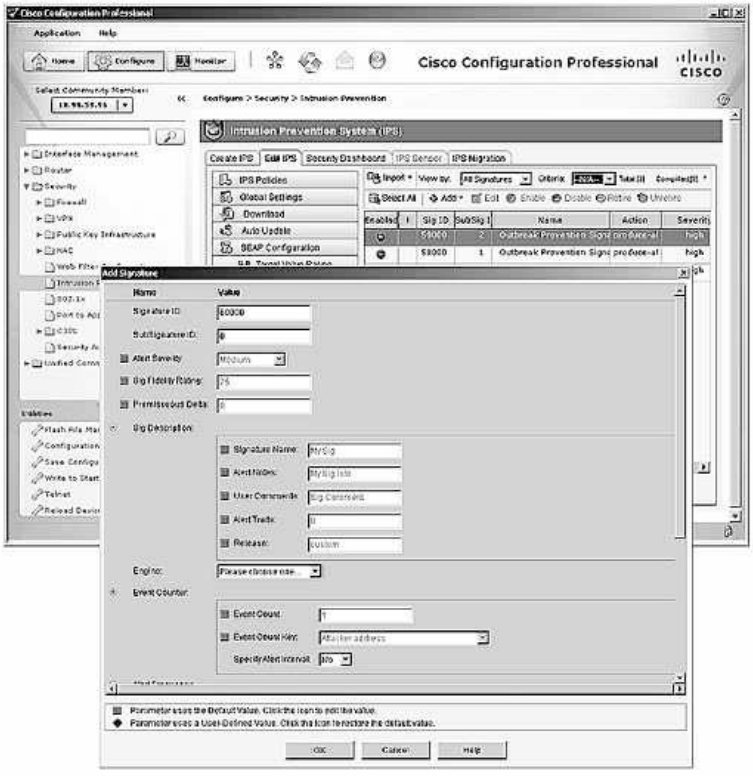
Si utiliza Cisco IOS versión 12.4 (11) o superior, la información sobre la ubicación del almacenamiento de la firma y el tipo de categoría firma pueden ser especificados. Termine con el botón **Finalizar**.



8.3.3 Modificación de las firmas

CCP también puede ser utilizado para modificar una configuración de firma. Para modificar una firma, seleccione **Configure** / **Security** / **Intrusion Prevention** / **Edit IPS** / **Signatures** para acceder a la lista de firmas disponibles.

Para modificar una acción de firma, pulse el botón derecho sobre la firma y seleccione **Actions** en el menú contextual. Las acciones disponibles dependen de la firma. Las firmas pueden tener diferentes parámetros, para modificarlos seleccione la firma correspondiente y pulse el botón **Edit**.



La CLI de IOS puede utilizarse para modificar firmas individuales o un grupo de firmas que pertenecen a una categoría de la firma con el comando **ip ips signature-definition**.

También se puede utilizar para cambiar las acciones de la firma para una firma o un grupo de firmas basado en categorías de firmas. Para cambiar una acción, el comando **event-acción** se debe utilizar en el modo de Categoría IPS.

EJEMPLO:

El siguiente ejemplo muestra cómo retirar una firma individual (6130) con la identificación subsig 10. El ejemplo también muestra cómo cambiar la acción para alertar a la firma de una caída y restablecerla.

```
Cisco_IPS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco_IPS(config)#ip ips signature-definition
Cisco_IPS(config-sigdef)#signature 6130 10
Cisco_IPS(config-sigdef-sig)#status
Cisco_IPS(config-sigdef-sig-status)#retired true
Cisco_IPS(config-sigdef-sig-status)#exit
Cisco_IPS(config-sigdef-sig)#exit
Cisco_IPS(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
Cisco_IPS(config)#exit

Cisco_IPS #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco_IPS(config)#ip ips signature-definition
Cisco_IPS(config-sigdef)#signature 6130 10
Cisco_IPS(config-sigdef-sig)#engine
Cisco_IPS(config-sigdef-sig-engine)#event-action produce-alert
Cisco_IPS(config-sigdef-sig-engine)#event-action deny-packet-inline
Cisco_IPS(config-sigdef-sig-engine)#event-action reset-tcp-
connection
Cisco_IPS(config-sigdef-sig-engine)#exit
Cisco_IPS(config-sigdef-sig)#exit
Cisco_IPS(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
Cisco_IPS(config)#
```

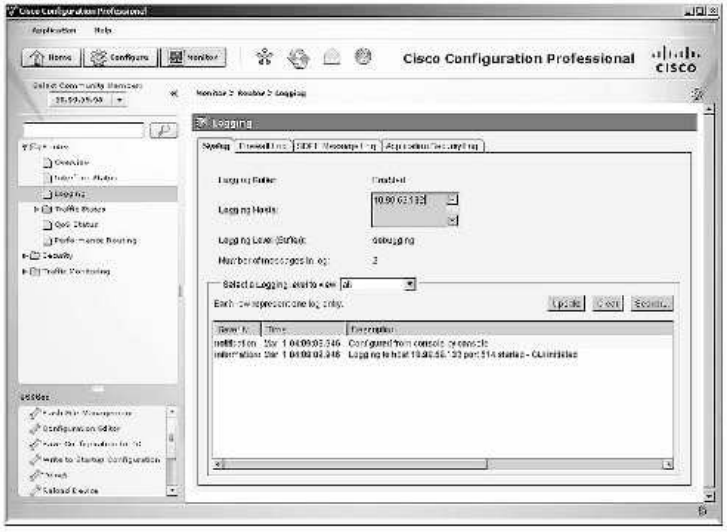
8.3.4 Verificación y monitorización de Cisco IOS IPS

La siguiente tabla muestra una lista de comandos para la verificación y monitorización de los dispositivos Cisco IOS IPS.

Comando	Descripción
`show ip ips`	Se puede utilizar con otros parámetros para proporcionar información específica.
`show ip ips all`	Muestra todos los datos de configuración de IPS.
`show ip ips configuration`	Muestra los datos de configuración adicionales que no se muestran con el **show running-config**.
`show ip ips interfaces`	Muestra los datos de configuración de interfaz y las reglas de entrada y de salida aplicadas.
`show ip ips signatures`	Comprueba la configuración de la firma.
`show ip ips statistics`	Muestra el número de paquetes auditados y el número de alarmas enviadas.
`clear ip ips configuration`	Deshabilita todas las configuraciones IPS.
`clear ip ips statistics`	Resetea todas las estadísticas.
`ip ips notify [log | sdee]`	Envía mensajes de log. El parámetro **[log | sdee]** determina el formato del mensaje.

Para verificar la configuración de Cisco IOS IPS con CCP seleccione **Configure / Security / Intrusion Prevention / Edit IPS** y luego **IPS Policies**.

CCP o Cisco IPS Manager Express pueden ser utilizados para ver los mensajes SDEE. Seleccione en la página de inicio de CCP **Monitor** / **Router** / **Logging**.



8.4 FUNDAMENTOS PARA EL EXAMEN

- Estudie y analice las diferencias entre un IDS y un IPS.
- Aprenda qué es una firma, qué tipos existen y cómo se obtienen.
- Analice y memorice cómo funciona y qué desencadena una alarma de firma.
- Estudie los mecanismos de configuración de un IPS, desde descargar una firma hasta poder reincorporarla.
- Realice prácticas de configuración con CLI y con CCP. Puede utilizar simuladores.

Capítulo 9

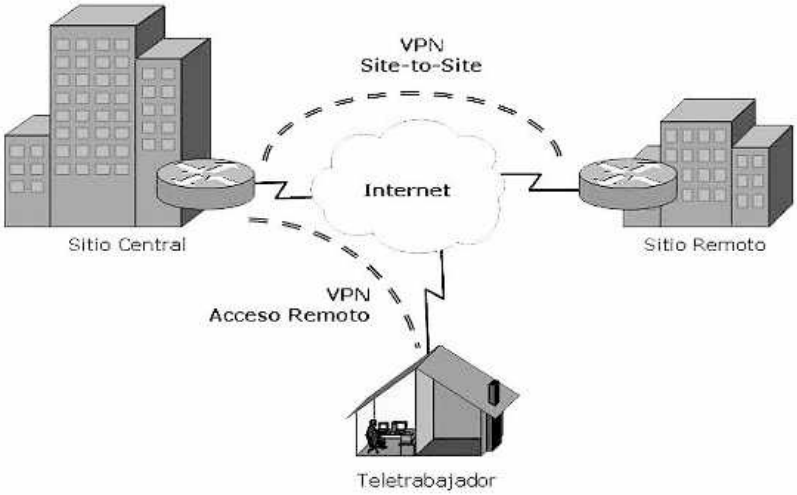
TECNOLOGÍAS VPN

9.1 REDES PRIVADAS VIRTUALES

Una VPN es una red privada que se crea mediante el uso de túneles sobre una red pública, usualmente Internet. En lugar de utilizar conexiones físicas dedicadas, una VPN utiliza conexiones virtuales enrutadas a través de Internet, desde la organización hasta el sitio remoto. En el sentido más simple, una VPN conecta dos extremos sobre una red pública para formar una conexión lógica.

Una VPN de sitio a sitio se crea cuando los dispositivos de conexión en ambos extremos de la conexión VPN conocen la configuración VPN de antemano. La VPN permanece estática y los hosts internos no tienen conocimiento de la existencia de la VPN. Las redes Frame Relay, ATM, GRE y MPLS son ejemplos de VPN de sitio a sitio.

Una VPN de acceso remoto se crea cuando la información de la VPN no se configura en forma estática, sino que se permite que la información cambie en forma dinámica y puede ser habilitada o deshabilitada. Considere un trabajador a distancia que necesita acceder a datos corporativos a través de Internet. Su conexión VPN puede no estar activa en todo momento. El PC del trabajador es responsable de establecer la VPN. La información requerida para establecer la conexión VPN, como puede ser la dirección IP del trabajador a distancia, cambia dinámicamente de acuerdo a la ubicación del mismo.



9.2 TÚNELES GRE

Los túneles **GRE** (*Generic Routing Encapsulation*) permiten encapsular cualquier tipo de tráfico. En un principio se utilizaban para encapsular tráfico no IP dentro de las redes IP, pero también permiten la encapsulación de tráfico IP. Funcionan encapsulando la cabecera IP original dentro de la cabecera GRE.

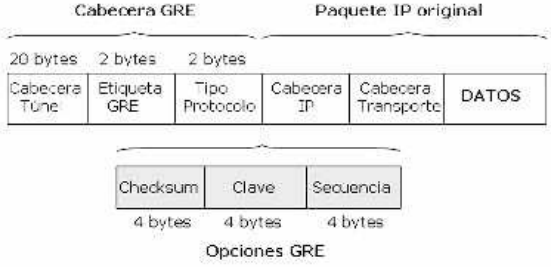
Las características generales de los túneles GRE son las siguientes:

- Es similar a un túnel IPsec en el sentido de que ambos encapsulan la cabecera original IP.
- No ofrece mecanismos de control de flujo.
- GRE añade un mínimo de 24 bytes a la cabecera, en los que incluimos la nueva cabecera IP.
- Permiten tunelizar cualquier protocolo de capa 3.
- Permite que los protocolos de enrutamiento viajen a través del túnel.
- Era la única opción para transportar tráfico multicast a través de un túnel, hasta la versión de IOS 12.4(4)T.
- La seguridad es limitada.

GRE es una herramienta sencilla y potente, permite de una manera sencilla establecer una conexión punto a punto sobre la cual encapsular cualquier protocolo de capa 3.

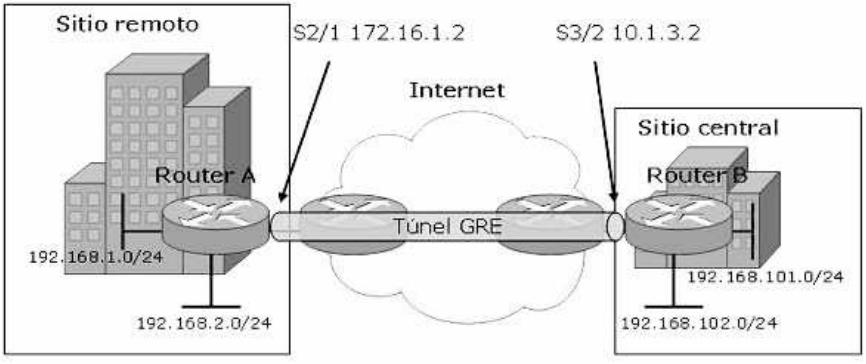
A diferencia de IPsec los túneles GRE permiten que el tráfico de los protocolos de enrutamiento viaje a través de ellos. Con IPsec se limita al uso de rutas estáticas, haciendo que la escalabilidad sea un problema.

GRE utiliza un campo de tipo de protocolo en el encabezado GRE para soportar la encapsulación de cualquier protocolo de capa 3 del modelo OSI. El encabezado GRE, junto con el encabezado de tunneling IP, agrega al menos 24 bytes de sobrecarga adicional a los paquetes enviados a través del túnel.



9.2.1 Configuración básica de túneles GRE

En la actualidad, los túneles GRE se utilizan normalmente para transportar tráfico IP en una red IP o sobre un túnel IPsec. La figura muestra una configuración básica de un túnel GRE.



Router A:

```
RouterA(config)#interface serial 2/1
RouterA(config-if)#ip address 172.16.1.2 255.255.255.0
RouterA(config-if)#interface tunnel 0
RouterA(config-if)#ip address 192.168.200.1 255.255.255.0
RouterA(config-if)#tunnel source serial 2/1
RouterA(config-if)#tunnel destination 10.1.3.2
RouterA(config-if)#tunnel mode gre ip
```

Router B:

```
RouterB(config)#interface serial 3/2
RouterB(config-if)#ip address 10.1.3.2 255.255.255.0
RouterB(config-if)#interface tunnel 2
RouterB(config-if)#ip addr 192.168.200.2 255.255.255.0
RouterB(config-if)#tunnel source serial 3/2
RouterB(config-if)#tunnel destination 172.16.1.2
RouterB(config-if)#tunnel mode gre ip
```

Esta configuración incluye:

- Crear una interfaz túnel con el comando **interface tunnel 0**.
- Asignar una dirección IP a la interfaz túnel.
- Identificar la interfaz del origen del túnel con el comando **tunnel source**.
- Identificar el destino del túnel con el comando **tunnel destination**.
- Configurar el protocolo GRE utilizando el comando **tunnel mode**, por defecto GRE/IP.

En la figura anterior se muestra la configuración de un túnel GRE entre dos extremos. Dicho túnel es definido como una interfaz en cada router, permitiendo de esta manera la opción multiprotocolo.

El origen del túnel GRE en un extremo ha de ser el final del túnel en el otro y viceversa. Esta validación es llevada a cabo inicialmente cuando se establece el túnel. Es necesario configurar una subred apropiada y común para el túnel.

GRE no provee cifrado. Si fuera necesario, debe configurarse IPsec.

9.3 IPsec

IPsec es un conjunto de características que protegen los datos IP cuando estos viajan desde una entidad a otra. Las localizaciones involucradas en la VPN definen el tipo de VPN. Una localización podría ser un cliente final tal como un PC, una pequeña oficina remota o una oficina remota más grande o datacenter, etc., la combinación de cualquiera de estas localizaciones determinará el tipo de VPN en uso, por ejemplo una pequeña oficina **SOHO** (*Small Office Home Office*) conectándose a la oficina principal podría ser una VPN site-to-site. Es importante recordar que solamente IPsec puede proteger la capa de red, la capa IP y superiores, transporte y usuario.

IPsec no puede brindar servicio a la capa de enlace. Si fuese necesaria la protección de dicha capa, habrá que buscar entonces otro tipo de encriptación para el enlace.

Las características o servicios de IPsec están implementados por una serie de protocolos estándar. Es importante que la implementación de IPsec esté fundamentada sobre estándares abiertos para que de esta manera permita interoperabilidad entre diferentes fabricantes. Los protocolos procedentes de IPsec no especifican una autenticación o encriptación en particular ni tampoco técnicas de generación de claves o SA.

IPsec se basa en protocolos primarios que ayudan a implementar su arquitectura global, como IKE, ESP y AH, los cuales se detallarán más adelante.

Es importante comprender que estos protocolos están basados en estándares abiertos, IPsec los utiliza para autenticación, encriptación, generación de llaves y establecimiento de asociaciones de seguridad. IPsec es utilizado para proteger el flujo de los datos a través de una VPN, pero una VPN no necesariamente tiene que requerir que estos contenidos estén protegidos. Una VPN puede ser simplemente un túnel o un enlace entre dos puntos finales; por lo tanto, la cabecera o etiqueta es identificada como tal, pero el contenido interno está disponible para cualquiera que lo quiera inspeccionar entre dichos extremos finales. Entonces una VPN IPsec puede ser considerada segura y protegida mientras que otro tipo de VPN no comparte este tipo de características.

9.3.1 Características de IPsec

Las características de IPsec consisten en cuatro características específicas. Es importante comprender el significado de cada una de estas características y los protocolos que las implementan.

- Confidencialidad de los datos.
- Integridad de los datos.
- Autenticación del origen de los datos.
- Anti-replay

La confidencialidad involucra los datos dentro de la VPN privada de IPsec y entre los participantes de la VPN. Muchas de las VPN se realizan a través de Internet, es decir, que muchos de los datos podrían ser interceptados y examinados. Cualquier tipo de tráfico corre siempre el riesgo de ser examinado, por lo tanto, no solamente debe verse a Internet con esa vulnerabilidad, sino también cualquier otra ruta posible.

La confidencialidad de los datos abarca la encriptación de los datos para hacerlos ilegibles, los paquetes que son encriptados al ser interceptados por otras personas no podrán ser leídos, solamente los podrá interpretar el receptor. El uso de la encriptación implica la selección de un algoritmo de encriptación y de un medio para distribuir las llaves de encriptación involucradas.

La confidencialidad de los datos no es requerida en las VPN IPsec.

A menudo los paquetes viajan encriptados cuando pasan por una VPN pero la confidencialidad es una característica opcional en IPsec.

La integridad de los datos es una garantía de que los datos no han sido modificados o alterados durante el tránsito a través de la VPN IPsec.

La integridad de los datos en sí misma no proporciona la protección de los datos. Típicamente utiliza un algoritmo hash para verificar si los datos dentro de un paquete han sido modificados entre dos puntos finales. Los paquetes que han sido identificados como dudosos no son aceptados.

La autenticación del origen de los datos valida el origen en la VPN IPsec. Esta característica se realiza por cada uno de los extremos de la VPN para asegurar que el otro extremo es exactamente quien debe ser, el que está conectado. Esta característica es dependiente del servicio de integridad de datos, la autenticación del origen de los datos no podría existir por sí sola.

Anti-replay asegura que los paquetes no están duplicados dentro de una VPN, esto se lleva a cabo a través del número de secuencia de los paquetes y de un sistema de ventanas deslizantes en el receptor. El número de secuencias es

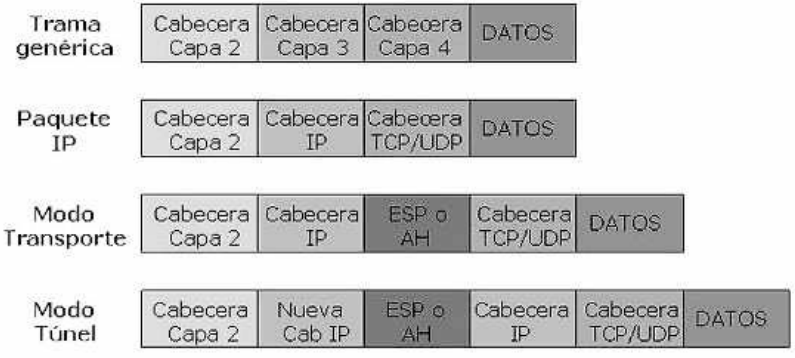
comparado con la ventana deslizante para detectar paquetes que llegan más tarde, dichos paquetes se consideran como duplicados y son eliminados. Como ocurre con la confidencialidad de los datos, Anti-replay se considera como una característica opcional.

9.3.2 Modos de IPsec

IPsec ofrece dos modos de configuración diferentes dependiendo de hasta dónde se quieran proteger los datos.

- **Modo transporte**: la cabecera IPsec es insertada justo después de la cabecera IP, de manera que la cabecera IP original está expuesta y no es protegida. Los datos en la capa de transporte y superiores son los que se benefician de IPsec.

- **Modo túnel**: en este caso tanto la cabecera IP original como el resto de datos del paquete son protegidos. Este modo genera una nueva cabecera IP que contiene las direcciones IP de los terminadores IPsec (por ejemplo concentradores VPN, firewall o router). De esta manera, las direcciones IP expuestas son las de los terminadores pero no las de los host que están detrás de ellos.



9.3.3 Cabeceras IPsec

Tanto AH, reconocido con el número de protocolo IP 51, como ESP, protocolo IP número 50, son implementados mediante la adición de cabeceras al paquete IP original. La VPN puede usar uno de los dos o ambos, aunque hay que recordar que si se utiliza ESP, el uso adicional de AH no conlleva un mayor beneficio ya que ESP implementa por sí mismo todas las funcionalidades de IPsec.

9.4 PROTOCOLOS DE IPsec

Los tres protocolos principales utilizados por IPsec son los siguientes:

- **IKE** (*Internet Key Exchange*)
- **ESP** (*Encapsulating Security Payload*)
- **AH** (*Authentication Header*)

Juntos, estos tres protocolos ayudan a implementar su arquitectura global y ofrecen las características mencionadas anteriormente. Cada VPN IPsec utiliza una combinación de estos protocolos para proporcionar las características requeridas por la VPN.

9.4.1 IKE

IKE (*Internet Key Exchange*) ofrece un marco para el intercambio de la negociación de seguridad y llaves de autenticación. Existe una variedad de opciones entre dos extremos IPsec. La negociación segura de estos parámetros utilizada para establecer la VPN IPsec se lleva a cabo por IKE.

IKE también intercambia llaves utilizadas para los algoritmos de encriptación simétrica dentro de VPN IPsec. Comparados con otros algoritmos de encriptación, los algoritmos simétricos tienden a ser más eficientes y fáciles de implementar por hardware. La utilización de tales algoritmos requiere un material de llaves apropiadas, IKE proporciona los mecanismos de intercambio de dichas llaves.

9.4.2 ESP

ESP (*Encapsulating Security Payload*) proporciona el marco para la confidencialidad de los datos, integridad de los datos, autenticación del origen de los datos y opcionalmente características como Anti-replay.

ESP es el único protocolo de IPsec que proporciona encriptación de los datos, pero también puede proporcionar todas las otras características de IPsec.

Debido a esto último, ESP es mayoritariamente utilizado en VPN IPsec hoy en día. Los siguientes procesos de encriptación están disponibles en ESP:

- **DES** (*Data Encryption Standard*) es un método de autenticación muy antiguo que está bastante extendido.
- **3DES** (*Triple Data Encryption Standard*) es un bloque encriptado que utiliza tres veces DES.
- **AES** (*Advanced Encryption Standard*) es uno de los algoritmos de llaves simétricas más populares actualmente.

9.4.3 AH

AH (*Authentication Header*) proporciona el marco para la integridad de los datos, autenticación del origen de los datos y características opcionales como Anti-replay. La confidencialidad de los datos no es proporcionada por AH.

AH se asegura de que los datos no han sido modificados o interferidos pero no esconde estos datos cuando están transitando. La utilización de AH de manera solitaria ha caído en desuso en favor de ESP.

Ambos, AH y ESP utilizan HMAC (*Hash-based Message Authentication Code*) como chequeo para la autenticación e integridad. La siguiente tabla muestra los algoritmos de hash de HMAC:

Algoritmo Hash	Entrada	Salida	Utilizado por IPsec
MD5 (*Message Digest*)	Variable	128 bits	128 bits
SHA-1 (*Secure Hash Algorithm*)	Variable	160 bits	Primeros 96 bits

Ambos, MD5 y SHA-1, utilizan una llave secreta compartida para el cálculo de los valores de autenticación del mensaje. La fuerza criptográfica de HMAC depende de las propiedades de la función de hash subyacente. MD5 y SHA-1 toman datos de entradas de longitud variable y crean un hash de longitud fija, la diferencia es el tamaño y la fuerza del *hash* que ha sido creado. Aunque IPsec utiliza solamente los primeros 96 bits de los 160 del hash de SHA-1, es considerado más seguro que MD5.

9.4.4 Autenticación de vecinos

Con la autenticación del vecino se garantiza que el extremo IPsec es quien realmente se supone que ha de ser. Existen cinco métodos para autenticar al vecino:

- **Usuario y contraseña**: donde un usuario y su respectiva contraseña son definidos en ambos extremos. No es una solución muy segura ya que esos datos son almacenados localmente y son susceptibles de robo.

- **Contraseña de un solo uso** (OTP): este método es bueno para establecer sesiones de una en una, si alguien descubre una contraseña utilizada previamente, no le servirá de nada.

- **Sistemas biométricos**: analizan una parte de las características del ser humano, por ejemplo, las huellas digitales, la retina, etc. Es un método muy seguro ya que duplicar dichas características sería prácticamente imposible.

- **Claves precompartidas**: similar al método de usuario y contraseña, pero en este caso se utiliza un valor configurable en ambos extremos.

- **Certificados digitales**: este método es muy común y cada vez gana más terreno de utilización. Un certificado digital es emitido para cada dispositivo por parte de una CA y será válido solamente en el aquel para el que ha sido emitido.

9.5 INTERNET KEY EXCHANGE

Una conexión IPsec entre dos dispositivos puede ser establecida configurando manualmente llaves de encriptación en ambos extremos, pero esto no es óptimo ni escalable. La solución es usar una arquitectura IKE (*Internet Key Exchange*).

9.5.1 Protocolos IKE

IKE es un método para intercambiar de manera dinámica parámetros y claves IPsec para que se puedan establecer las **SA**. Las SA o asociaciones de seguridad son acuerdos de parámetros IPsec entre dos *peers*. IKE utiliza los siguientes protocolos:

- **ISAKMP** (*Internet Security Association and Key Management Protocol*): define cómo establecer, negociar, modificar y borrar las SA.
- **Oakley**: utiliza el algoritmo **DH** (*Diffie-Hellman*) para gestionar el intercambio de claves sobre SA.

9.5.2 Fases IKE

El protocolo IKEpuede dividirse en dos partes que crean una comunicación segura entre los dos extremos IPsec. Aunque son dos fases primarias y obligatorias, existe también una tercera opcional:

- **Fase 1**. Es obligatoria. Una SA bidireccional es establecida entre los dos *peers*. Puede ser establecida usando dos modos, modo **main** o modo agresivo, los cuales serán vistos posteriormente.
- **Fase 1.5**. Es opcional. Proporciona una capa adicional de autenticación llamada **Xauth** o autenticación extendida, cuya finalidad es validar al usuario que va a hacer uso de la conexión segura.
- **Fase 2**. Es obligatoria. Se establecen SA unidireccionales entre los *peers* usando los parámetros acordados en la fase 1. Durante esta fase se utiliza el modo **quick**.

9.5.3 Modos IKE

El modo **main** consiste en el intercambio de seis mensajes entre los peers, que pueden simplificarse en estos tres conceptos:

- Parámetros IPsec y políticas de seguridad. El iniciador envía una o más propuestas y el vecino selecciona la apropiada.
- Intercambio de llaves públicas Diffie-Hellman. Son enviadas entre los dos peers.

- Autenticación de la sesión ISAKMP. Cada extremo es autenticado por el otro.

El modo agresivo consiste en el intercambio de tres mensajes entre los *peers*:

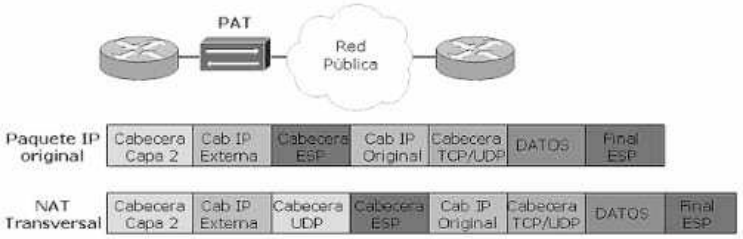
- El iniciador envía todos los datos, incluyendo parámetros IPsec, políticas de seguridad y llaves públicas DH.
- El vecino autentica el paquete y envía una propuesta de parámetros, material clave y una identificación.
- El iniciador autentica el paquete.

El modo rápido se utiliza durante la fase 2 y su negociación está protegida por la SA estipulada en la fase 1. Negocia las SA utilizadas para encriptar datos a través de la conexión IPsec. También gestiona el intercambio de llaves para esas SA.

9.5.4 Funciones adicionales IKE

Además de intercambiar llaves y parámetros IPsec, IKE puede realizar las siguientes funciones:

- **Dead Peer Detection** (DPD): es un mecanismo que envía hello de manera periódica entre los peers para detectar fallos.
- **Modo Configuration**: centraliza las configuraciones que han de ser enviadas a los clientes. Cisco Easy VPN es un claro ejemplo de gestión centralizada.
- **Xauth** (IKE *extended authentication*): autentica al usuario, que hará uso del túnel seguro para verificar que es quien dice ser.
- **NAT transversal**: para que PAT pueda funcionar necesita obtener información de puertos que de otro modo no podría leer al estar encriptados cuando se utiliza IPsec. Insertando una cabecera UDP antes de la cabecera ESP se permite que el router pueda mantener la tabla PAT, como aparece en la siguiente figura:



9.6 ALGORITMOS DE ENCRIPTACIÓN

La encriptación no es más que la aplicación de un algoritmo matemático y una llave a una serie de datos para hacerlos ilegibles a todos excepto a quien pueda desencriptarlos.

Existen dos enfoques para asegurar la seguridad de los datos cuando se utilizan varios métodos de cifrado. El primero consiste en proteger los algoritmos. Si la seguridad de un sistema de cifrado se basa en mantener en secreto a los algoritmos en sí, debe custodiarse en extremo el código del algoritmo. Si se revela el algoritmo, cada una de las partes involucradas debe cambiar de algoritmo. El segundo enfoque indica proteger las claves. Con la criptografía moderna, todos los algoritmos son públicos: las claves criptográficas son las que aseguran el secreto de los datos. Estas son secuencias de bits, las cuales se ingresan en el algoritmo de cifrado junto con los datos a cifrar.

9.6.1 Encriptación simétrica

Estos algoritmos se basan en el uso de una sola llave tanto para encriptar como para desencriptar los datos. La llave ha de estar muy bien protegida porque si fuera robada, los datos podrían ser desencriptados. Tienden a ser fáciles de implementar y son útiles cuando es necesario encriptar grandes cantidades de datos.

Las llaves se intercambian antes de enviar cualquier mensaje secreto. El mensaje se guarda y se envía de manera segura a través de la red. Cuando el mensaje llega al destino se utilizan las mismas llaves para descifrarlo. La misma clave puede volver a utilizarse en el mensaje de respuesta.

DES, 3DES, AES, SEAL y las series RC (*Rivest Ciphers*), incluyendo RC2, RC4, RC5 y RC6, son algoritmos bien conocidos de cifrado con clave simétrica.

Diffie-Hellman no es un mecanismo de cifrado y no es utilizado para cifrar datos sino que es un método para intercambiar de forma segura las claves para cifrar datos. En un sistema de claves simétricas, ambos extremos de la comunicación deben tener claves idénticas. El intercambio seguro de dichas claves siempre se ha presentado como un desafío. Los sistemas de claves asimétricas resuelven este desafío porque utilizan dos claves. Una clave es llamada clave privada, mientras que la otra se llama clave pública.

La clave privada es secreta y sólo conocida por el usuario. La clave pública se comparte en forma abierta y se distribuye con facilidad.

9.6.2 Encriptación asimétrica

Estos algoritmos utilizan diferentes llaves para encriptar y para desencriptar. La llave utilizada para encriptar recibe el nombre de llave pública, mientras que la usada para desencriptar recibe el nombre de llave privada. La llave pública puede ser distribuida para que cualquiera pueda encriptar los datos, pero solamente el poseedor de la llave privada podrá leerlos.

Para el caso de las firmas digitales hay que invertir la lógica, la llave privada se usa para firmar y encriptar el mensaje, mientras que la llave pública desencripta y valida la firma digital.

Las llaves no son intercambiadas previamente. El emisor y el receptor poseen claves diferentes con sus respectivas llaves cada uno. Antes de enviar un mensaje se le debe solicitar al destino la clave abierta. El origen coloca el mensaje y su propia clave en la que el destino envió y la cierra. El mensaje es enviado. Como solo el destino posee la llave puede desencriptarlo y leer el mensaje. A su vez, como el origen también envió su propia clave abierta el proceso de respuesta podrá repetirse continuamente.

Existen varios protocolos que utilizan algoritmos de clave asimétrica:

- **IKE** (*Internet Key Exchange*): un componente fundamental de las VPN IPsec.
- **SSL** (*Secure Socket Layer*): ahora implementado como el estándar IETF TLS.
- **PGP** (SSH *Pretty Good Privacy*): provee privacidad y autenticación criptográficas y se utiliza con frecuencia para incrementar la seguridad de las comunicaciones de correo electrónico.

- **RSA** (Rivest, Shamir and Adleman): algoritmo de encriptación cuya longitud de llave empieza en 1.024 bits.

9.7 PUBLIC KEY INFRASTRUCTURE

PKI (*Public Key Infrastructure*) involucra el proceso de intercambio y mantenimiento de llaves necesario para soportar tecnologías basadas en clave pública de gran escala. PKI soporta soluciones muy escalables y se está volviendo una solución de autenticación muy importante para las VPN.

PKI consiste en un conjunto de componentes técnicos, organizativos y legales, necesarios para establecer un sistema que permita la utilización a gran escala de criptografía de clave pública, con el fin de proveer servicios de autenticación, confidencialidad, integridad y no repudio. El framework PKI está conformado por el hardware, el software, las personas, las políticas y los procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar los certificados digitales.

Existe una serie de elementos que intervienen y son los siguientes:

- **Peers**: dispositivos que necesitan comunicarse de manera segura.
- **CA** (Autoridad Certificadora): otorga y mantiene certificados digitales.
- **Certificado digital**: identifica a un peer de manera unívoca. Actualmente se utiliza la versión X.509v3.
- **RA** (*Registration Authority*): es una entidad opcional que puede gestionar el proceso de petición de certificados.
- **Mecanismo de distribución**: medio para distribuir CRL (*Certificate Revocation Lists*) en la red, por ejemplo vía Web.

La siguiente secuencia describe los pasos de un intercambio de mensajes PKI:

- Un host genera un par de llaves RSA (pública y privada) y pide la llave pública de su CA.
- El CA envía su llave pública al host.

- El host genera una petición de certificado que, dependiendo de la arquitectura de la red, será enviada al CA o RA.

- Una vez aprobado, el CA firma el certificado con su llave privada y se lo envía al host.

- El host guarda ese certificado en memoria no volátil.

El host utiliza el certificado para establecer comunicaciones seguras con otros hosts que hayan también llevado a cabo estos pasos.

9.8 CONFIGURACIÓN DE VPN SITE-TO-SITE

Antes de comenzar la configuración de una VPN se deben verificar las políticas restrictivas que puedan bloquear el tráfico IPsec. Los routers perimetrales en general implementan políticas de seguridad restrictivas con ACL, donde solo se permite tráfico específico y se deniega todo el otro tráfico.

Para optimizar las interfaces IPsec, deben agregarse sentencias específicas de permiso en las ACL.

- Para permitir el tráfico AH se utiliza el siguiente comando:

```
access-list acl permit ahp source wildcard destination
wildcard
```

- Para permitir el tráfico ESP se utiliza el siguiente comando:

```
access-list acl permit esp source wildcard destination
wildcard
```

- Para permitir el tráfico ISAKMP se utiliza el siguiente comando:

```
access-list acl permit udp source wildcard destination
wildcard eq isakmp
```

NOTA:

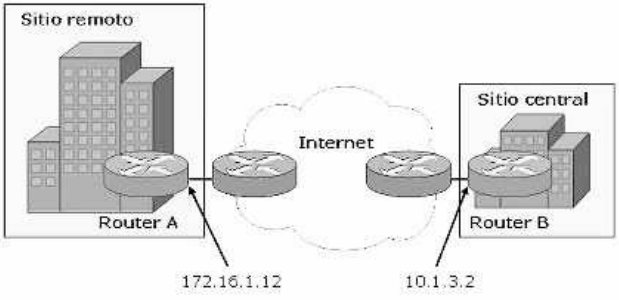
ESP tiene asignado el número de protocolo IP 50.
AH tiene asignado el número de protocolo IP 51.
ISAKMP utiliza el puerto UDP 500.

Para la configuración de una VPN *site-to-site* utilizando Cisco IOS son necesarios los siguientes 6 pasos:

1. Configuración de la política ISAKMP (IKE fase 1).
2. Configuración de los IPsec transform sets (IKE fase 2, terminación del túnel).
3. Configuración de la crypto ACL (tráfico interesante, transferencia segura de datos).
4. Configuración del crypto map (IKE fase 2).
5. Aplicación del crypto map a la interfaz (IKE fase 2).
6. Configuración de la ACL para la interfaz.

9.8.1 Configuración de la política ISAKMP

Este paso está unido con la fase 1 de IKE, la cual se encarga de establecer un túnel bidireccional seguro usado para intercambiar claves IPsec para las SA.



Router A:

```
RouterA(config)#crypto isakmp policy 10
RouterA(config-isakmp)#encryption des
RouterA(config-isakmp)#hash md5
RouterA(config-isakmp)#authentication pre-shared
RouterA(config-isakmp)#group 1
RouterA(config-isakmp)#lifetime 3600
RouterA(config)#crypto isakmp policy 20
RouterA(config-isakmp)#encryption d3es
RouterA(config-isakmp)#hash sha
RouterA(config-isakmp)#authentication pre-shared
```

```
RouterA(config-isakmp)#group 1
RouterA(config-isakmp)#lifetime 3600

RouterA(config)#crypto isakmp key 0 TOPsecret address 10.1.3.2

RouterA(config)#crypto isakmp key 0 Secret address 10.10.4.3
```

Router B:

```
RouterB(config)#crypto isakmp policy 15
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#authentication pre-shared
RouterB(config-isakmp)#group 2
RouterB(config-isakmp)#lifetime 1800

RouterB(config)#crypto isakmp policy 25
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#authentication pre-shared
RouterB(config-isakmp)#group 1
RouterB(config-isakmp)#lifetime 3600

RouterB(config)#crypto isakmp key 0 TOPsecret address 172.16.1.12

RouterB(config)#crypto isakmp key 0 SECret address 10.10.4.3
```

Los parámetros de configuración que se muestran en la sintaxis exhiben dos políticas ISAKMP configuradas. Debido a que se utilizan claves precompartidas, las claves ISAKMP han de estar definidas. Estas políticas son intercambiadas durante IKE fase 1. La política 10 en el router A encaja con la política 25 en el router B, así como la clave entre ambos (TOPsecret). El túnel IKE es creado usando esos atributos.

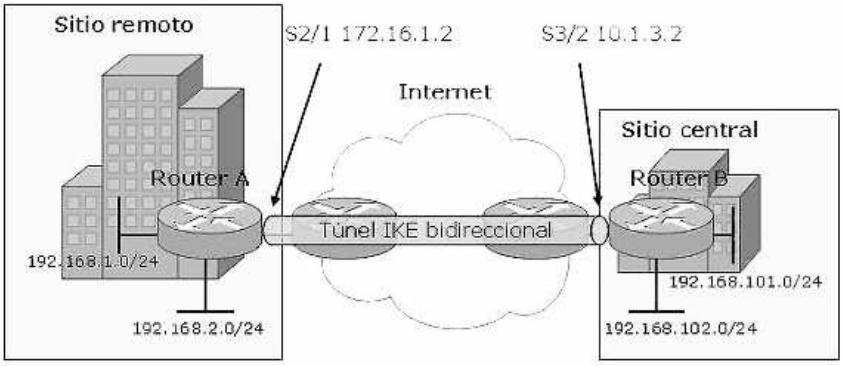
Las políticas siguen un orden secuencial, por lo tanto es beneficioso siempre configurarlas más fuertes con los números más bajos, para que tengan mayores posibilidades de ser elegidas primero.

9.8.2 Configuración de los IPsec transform sets

La configuración de los transform sets cubre en realidad tres de los pasos de la configuración de IPsec:

- IPsec transform sets
- Crypto ACL
- Crypto map

La siguiente sintaxis muestra la configuración de los transform sets en Cisco IOS.



Router A:

```
RouterA#show run
!
crypto ipsec transform-set set-60
esp-des esp-sha-hmac
mode tunnel
!
crypto ipsec transform-set set-70
esp-3des esp-sha-hmac
mode tunnel
!
crypto ipsec security-association
lifetime seconds 1800
!
access-list 170 permit 192.168.1.0
0.0.0.255 192.168.101.0 0.0.0.255
!
crypto map Sitio-central 70 ipsec-isakmp
set peer 10.1.3.2
match address 170
set transform-set set-70
```

Router B:

```
RouterB#show run
!
crypto ipsec transform-set set-55
esp-3des esp-sha-hmac
mode tunnel
!
crypto ipsec transform-set set-65
esp-3des esp-md5-hmac
mode tunnel
!
crypto ipsec security-association
lifetime seconds 1800
!
access-list 155 permit 192.168.101.0
0.0.0.255 192.168.1.0 0.0.0.255
!
crypto map to-remote 55 ipsec-isakmp
set peer 172.16.1.2
match address 155
set transform-set set-55
```

Cada dispositivo IPsec define uno o más transform sets. En este caso set-60, set-70, set-55 y set-65, estos nombres son de significado local. Los términos esp-3des y esp-sha-hmac definen ESP como el protocolo de IPsec.

El comando **crypto ipsec transform-set** se utiliza para seleccionar un *transform* AH, un transform de encriptación ESP o un transform de autenticación ESP. Solamente se puede seleccionar un IOS transform de cada tipo. La figura muestra el uso de un transform DES encriptación ESP y un transform de autenticación ESP. No es necesario utilizar los tres tipos de transform al configurar el túnel IPsec.

En la sintaxis, el parámetro **esp-3des** define el algoritmo de encriptación, mientras que **esp-sha-hmac** define el algoritmo de autenticación. También se muestra cómo está configurado el modo **tunnel**. Al ser este último el modo por defecto existe la posibilidad de que en un **sh run** esta configuración no apareciera en pantalla.

A su vez, el comando **crypto ipsec security-association** permite que el tiempo de vida de las **SA** sea configurado, en este caso ha sido configurado con un valor de 30 minutos.

La siguiente tabla muestra una lista de transform sets:

Tipo de transform	IOS transform	Descripción
AH transform	Ah-md5-hmac	AH con autenticación MD5
	Ah-sha-hmac	AH con autenticación SHA
ESP encryption transform	Esp-aes	ESP con autenticación AES de 128 bits
	Esp-aes 192	ESP con autenticación AES de 192 bits
	Esp-aes 256	ESP con autenticación AES de 256 bits
	Esp-des	ESP con autenticación DES de 56 bits
	Esp-3des	ESP con autenticación DES de 168 bits
ESP authentication transform	Esp-md5-hmac	ESP con autenticación MD5
	Esp-sha-hmac	ESP con autenticación SHA

9.8.3 Configuración de la Crypto ACL

La utilización de una ACL extendida permite categorizar el tráfico interesante. Dicha ACL es mostrada también en la sintaxis anterior. En el sitio remoto, la ACL es la 170 mientras que en la oficina central es la 155. Cada una de ellas define el origen y destino del tráfico que será enviado a través de los túneles.

Es importante que estas ACL sean espejos la una de la otra: la dirección de origen en una ha de ser la dirección de destino en la otra y viceversa. Aunque también es común en los sitios remotos enviar todo el tráfico a través del túnel y crear en el sitio central configuraciones más complejas.

En la figura anterior, una subred de cada sitio es categorizada como interesante gracias a las ACL y será protegida por el túnel IPsec, el resto del tráfico no será tunelizado.

9.8.4 Configuración del Crypto Map

En este paso se configura el crypto map, que se basa en unir el transform set junto con la ACL y hacer que apunten hacia el peer remoto. Los números 70 y 55 en cada uno de los crypto maps son números de línea, pudiendo tener múltiples líneas, las cuales son referenciadas de menor a mayor número.

En caso de tener una sola interfaz con múltiples clientes VPN remotos, será necesario un solo crypto *map* con entradas únicas por cada peer.

En la oficina remota, el crypto map Sitio-central crea una SA hacia el *peer* 10.1.3.2 y protege cualquier tráfico que coincida con la ACL 170 usando los parámetros de seguridad definidos en el transform set-70. Se aplica la misma lógica para el crypto *map* en la oficina central.

9.8.5 Aplicación del Crypto Map a una interfaz

Una vez que el crypto map es creado es necesario aplicarlo a la interfaz para que sea operacional. La siguiente sintaxis se aplica a la figura anterior donde se asocia el crypto map a la interfaz:

Router A:

```
RouterA#show run
!
crypto map to-central 10 ipsec-isakmp
set peer 10.1.3.2
match address 170
set transform-set set-70
!
interface serial 2/1
ip address 172.16.1.2 255.255.255.0
crypto map to-central
!
ip route 192.168.101.0 255.255.255.0
10.1.3.2
```

Router B:

```
RouterB#show run
!
crypto map to-remote 10 ipsec-isakmp
set peer 172.16.1.2
match address 155
set transform-set set-55
!
interface serial 3/2
ip address 10.1.3.2 255.255.255.0
crypto map to-remote
!
ip route 192.168.1.0 255.255.255.0
172.16.1.2
```

En la sintaxis del comando **crypto map** se muestra cómo se utiliza de manera global y cómo aplicarlo de manera local en el modo de interfaz. Normalmente son asociados en interfaces de salida, como muestra el ejemplo; esa interfaz es el origen de la VPN IPsec.

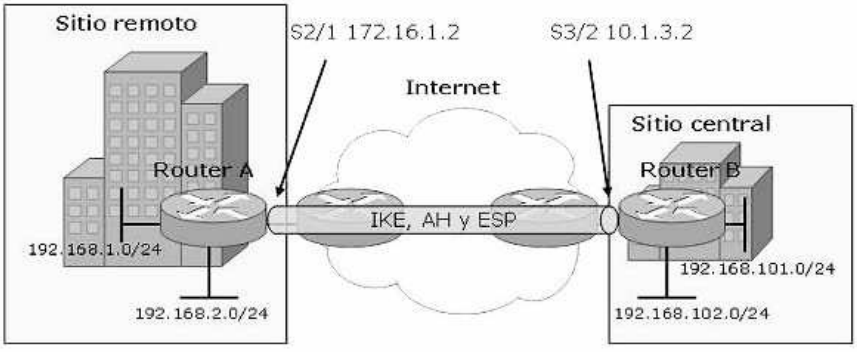
Será necesario modificar la tabla de enrutamiento. Desde la oficina remota la idea es que los dispositivos en la red 192.168.1.0/24 se comuniquen a través del túnel con la red remota 192.168.101.0/24, pero la tabla de rutas de A no contiene esa información, ya que no está siendo anunciada desde B. Son necesarias las configuraciones de rutas estáticas en los router A y B para lograr conectividad usando como puertas de enlace las interfaces contrarias que tienen el crypto map aplicado.

9.8.6 Configuración de ACL en una interfaz

En los ejemplos mostrados hasta ahora, el router conectado a Internet también hace la función de peer IPsec. Teniendo en cuenta que este router debería estar bloqueando gran cantidad de tráfico, se deben permitir los paquetes adecuados para que las SA de IKE e IPsec sean permitidas.

En este caso, la IP de origen de los paquetes IPsec es conocida. Cuando permitimos paquetes IPsec desde Internet es posible utilizar una ACL extendida, por ejemplo si se conoce el rango de direccionamiento desde el que se recibirán las conexiones.

La figura muestra parte de una ACL empleada para permitir paquetes IPsec en la interfaz.



Router A:

```
RouterA#show run
!
access-list 110 permit ahp host
10.1.3.2 host 172.16.1.2
access-list 110 permit esp host
10.1.3.2 host 172.16.1.2
access-list 110 permit udp host
10.1.3.2 host 172.16.1.2 eq isakmp
!
interface serial 2/1
ip address 172.16.1.2 255.255.255.0
crypto map to-central
ip access-group 110 in
```

Router B:

```
RouterB#show run
!
access-list 120 permit ahp host
172.16.1.2 host 10.1.3.2
access-list 120 permit esp host
172.16.1.2 host 10.1.3.2
access-list 120 permit udp host
172.16.1.2 host 10.1.3.2 eq isakmp
!
interface serial 3/2
ip address 10.1.3.2 255.255.255.0
crypto map to-remote
ip access-group 120 in
```

Las ACL en las interfaces que conectan hacia Internet podrían ser enormes, por lo tanto es necesario asegurar que el tráfico IPsec será correctamente permitido para poder establecer las VPN. En el ejemplo se conoce exactamente el origen de las conexiones pero se podrían utilizar ACL extendidas con rangos determinados en lugar de orígenes específicos.

9.9 VERIFICACIÓN

La siguiente tabla muestra comandos para la verificación y monitorización de la configuración de IPsec.

Comando	Descripción
`Show crypto map`	Muestra los crypto maps configurados.
`show crypto isakmp policy`	Muestra las políticas IKE configuradas.
`show crypto ipsec as`	Muestra los túneles IPsec establecidos.
`show crypto ipsec transform-set`	Muestra los conjuntos de **transform-set** IPsec configurados.
`debug crypto isakmp`	Muestra los eventos IKE.
`debug crypto ipsec`	Muestra los eventos IPsec.

Para ver todos los crypto maps configurados hay que utilizar el comando **show crypto map**. Este comando verifica las configuraciones y muestra el tiempo de vida de las SA.

```
Router#show crypto map
Crypto Map: "router-time" idb: Ethernet0 local address:
172.21.114.123
Crypto Map "router-time" 10 ipsec-isakmp
 Peer = 172.21.114.67
 Extended IP access list 141
 access-list 141 permit ip
 source: addr = 172.21.114.123/0.0.0.0
 dest: addr = 172.21.114.67/0.0.0.0
 Current peer: 172.21.114.67
 Security-association lifetime: 4608000 kilobytes/120 seconds
 PFS (Y/N): N
 Transform sets={ t1, }
```

Se utiliza el comando **show crypto ipsec transform-set** para mostrar todos los conjuntos de transformación configurados. Dado que los conjuntos de transformación determinan el nivel de protección con el que los datos son transmitidos a través del túnel, es importante verificar la fortaleza de la política de protección IPsec.

```
Router#show crypto ipsec transform-set
Transform set combined-des-sha: { esp-des esp-sha-hmac }
 will negotiate = { Tunnel, },
Transform set combined-des-md5: { esp-des esp-md5-hmac }
 will negotiate = { Tunnel, },
Transform set t1: { esp-des esp-md5-hmac }
 will negotiate = { Tunnel, },
```

```
Transform set t100: { ah-sha-hmac }
 will negotiate = { Transport, },
Transform set t2: { ah-sha-hmac }
 will negotiate = { Tunnel, },
 { esp-des }
 will negotiate = { Tunnel, },
```

Uno de los comandos más útiles es **show crypto ipsec sa**. Si la salida indica que existe una SA establecida, se asume que el resto de la configuración está funcionando. Entre los datos presentados, los valores **pkts encrypt** y **pkts decrypt** indican que el tráfico está siendo transmitido a través del túnel.

```
Router# show crypto ipsec sa

interface: FastEthernet0
 Crypto map tag: test, local addr. 12.1.1.1
 local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
 current_peer: 12.1.1.2
 PERMIT, flags={origin_is_acl,}
 #pkts encaps:7767918,#pkts encrypt: 7767918,#pkts digest 7767918
 #pkts decaps:7760382,#pkts decrypt: 7760382,#pkts verify 7760382
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0,
 #pkts decompress failed: 0, #send errors 1, #recv errors 0
 local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
 path mtu 1500, media mtu 1500
 current outbound spi: 3D3
 inbound esp sas:
        .....................................
```

9.10 CONFIGURACIÓN DE IPsec CON CCP

Además de configurar IPsec VPN a través de CLI, es posible configurarlos mediante el asistente CCP.

- Desde **Configure** / **Security** / **VPN** elija un asistente de la lista contenida en la carpeta VPN, en este caso **Site-to-Site VPN**.
- Marque la casilla correspondiente al subtipo de aplicación VPN **Create a Site-to-Site VPN**.
- Ingrese al asistente desde el botón **Launch the selected task** ubicado en la parte inferior de la ventana.

CCP permite la configuración de VPN a partir de dos formas, el asistente paso a paso y una configuración rápida preestablecida.

Algunos de los componentes durante el proceso de configuración deben estar configurados antes de iniciar el asistente, como es el caso de PKI.

La carpeta principal de VPN contiene una guía de diseño para crear VPN, asistentes para crear **VPN Site-to-Site**, **Easy VPN Remote**, **Easy VPN Server** y **Dynamic multipoint VPN**.

También hay tres subcarpetas:

- **The SSL VPN**: se utiliza para configurar los parámetros de VPN SSL.
- **The GET VPN**: se utiliza para configurar los parámetros GET VPN.

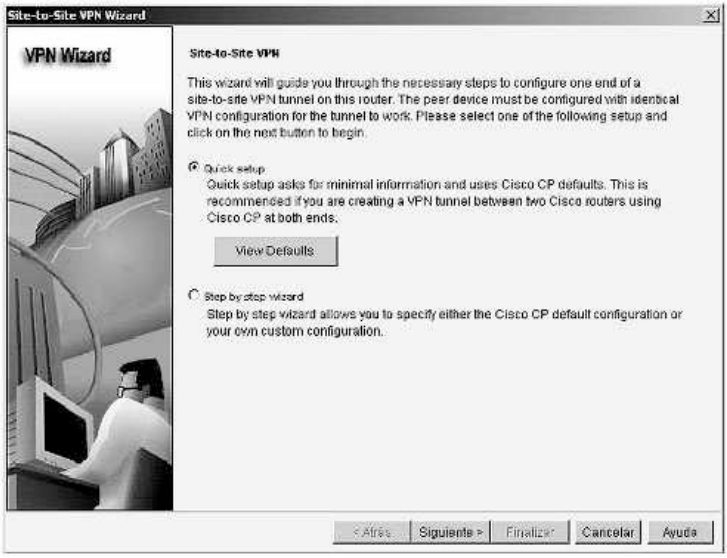
- **VPN components**: se utilizan para configurar los componentes de VPN tales como IPsec, IKE, Easy VPN Server, políticas de grupo y la configuración de proxy del explorador, y encriptación VPN. La opción de cifrado aparece si la imagen del software Cisco IOS en el router es compatible con el cifrado de tipo 6, también conocido como el cifrado VPN Key.

Desde el asistente pueden verse dos opciones de configuración:

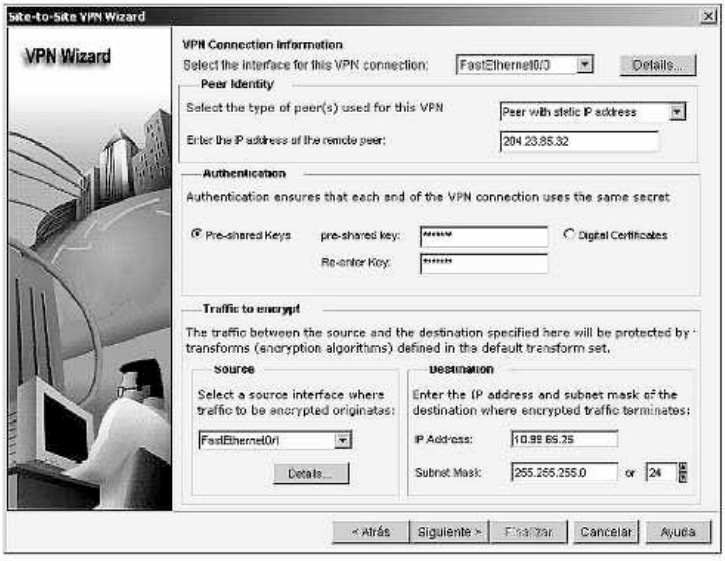
- **Quick setup**: utiliza las políticas por defecto IKE y los IPsec transform sets por defecto. Esta opción es recomendable para una rápida configuración utilizando los mejores parámetros de seguridad.

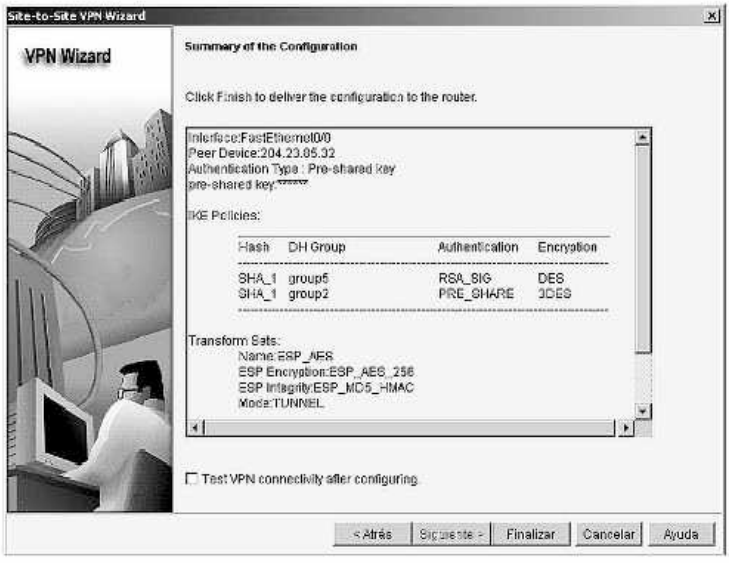
- **Step by step**: permite al administrador especificar las opciones de configuración según su propio criterio.

Para la configuración rápida seleccione **Quick setup** y luego **Siguiente**.



Complete todos los datos requeridos y continúe con **Finalizar**. La última ventana mostrará el resumen de la configuración, termine con el botón **Finalizar**.



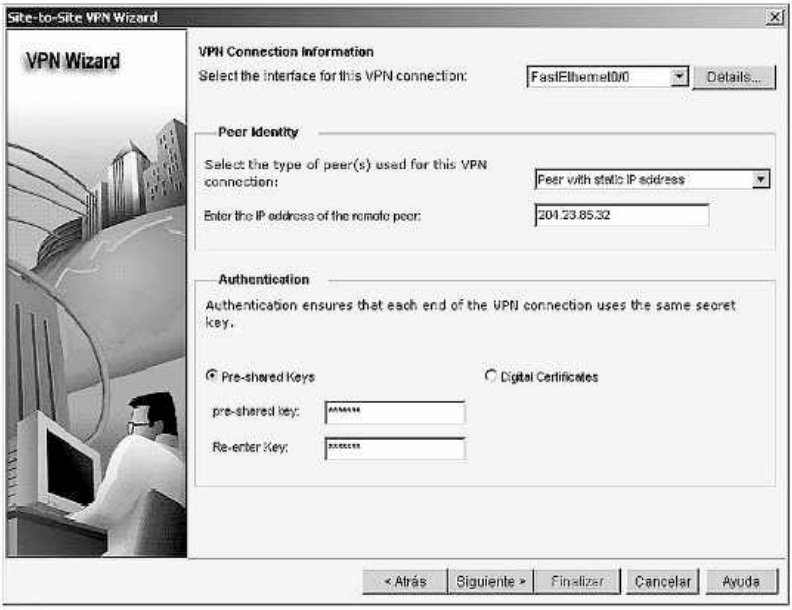


Para la configuración paso a paso, marque la casilla **Step by step** desde el asistente de configuración de VPN y luego **Siguiente**.

El asistente paso a paso requiere múltiples pasos para configurar una conexión VPN e incluye los siguientes parámetros:

- Configuración de conexión, incluyendo la interfaz externa, identidad del par y credenciales de autenticación.
- Propuestas IKE, tales como prioridad, cifrado, el algoritmo HMAC (*Hashed Message Authentication Code*), el método de autenticación IKE, el grupo DH (*Diffie-Hellman*) y el tiempo de vida IKE.
- Información del conjunto de transformación IPsec, incluyendo nombre, algoritmo de integridad, algoritmo de cifrado, modo de operación (túnel o transporte) y compresión.
- Tráfico a proteger, identificando las subredes únicas de origen y destino o definiendo una ACL para su uso en VPN más complejas.

La primera tarea en el asistente paso a paso es configurar las opciones de conexión. Complete todos los datos requeridos y continúe con **Siguiente**.



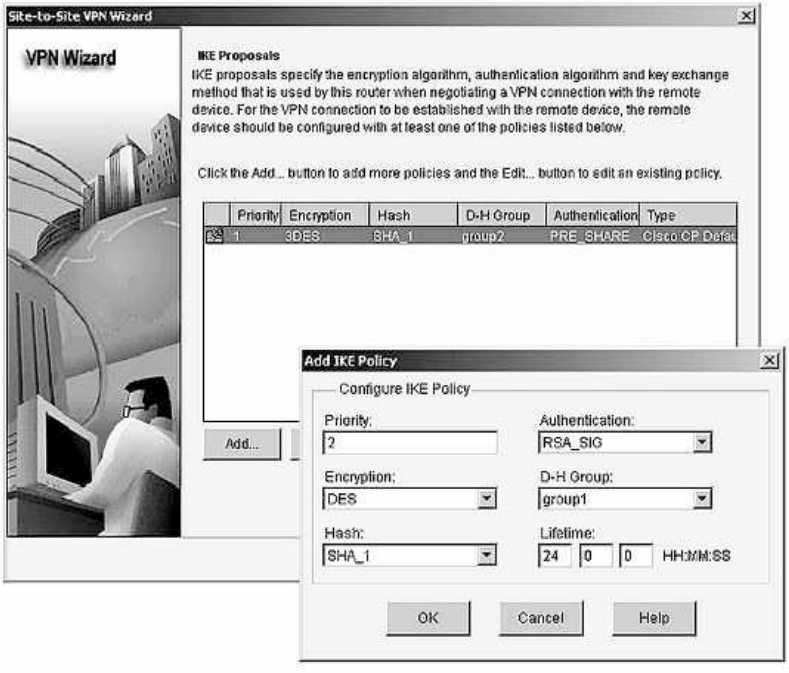
La segunda tarea del asistente paso a paso es configurar las propuestas IKE. Es posible crear una propuesta IKE personalizada o utilizar la propuesta IKE por defecto.

Para crear una propuesta IKE personalizada, debe agregar un nuevo IKE.

- Desde el botón **Add** puede definir una propuesta y especificar su prioridad, algoritmo de cifrado, algoritmo de hashing, método de autenticación IKE, grupo DH y tiempo de vida IKE. Cuando la propuesta IKE esté completa pulse **OK**.

- Una vez agregadas las políticas IKE, seleccione la propuesta a utilizar y continúe con **Siguiente** para seguir con la siguiente tarea.

Para utilizar la propuesta IKE predefinida, seleccione **Siguiente** en la página **IKE Proposal**. De esta forma, selecciona la propuesta IKE por defecto.



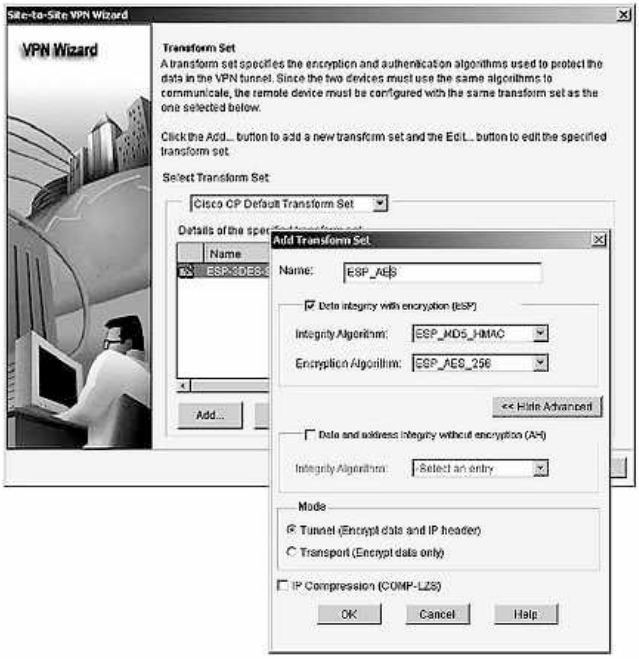
La tercera tarea del asistente paso a paso consiste en configurar el IPsec transform set. Es posible crear un conjunto de transformación IPsec personalizado o utilizar un conjunto predefinido.

Para crear un IPsec transform set personalizado, es necesario agregar un nuevo conjunto.

- Desde el botón **Add** puede definir el transform set y especificar su nombre, algoritmo de integridad, algoritmo de cifrado, modo de operación y compresión opcional. Cuando el transform set esté completo continúe con **OK**.

- Una vez agregados los nuevos transform set, seleccione cuál de ellos será utilizado y continúe con **Siguiente** para proceder a la siguiente tarea.

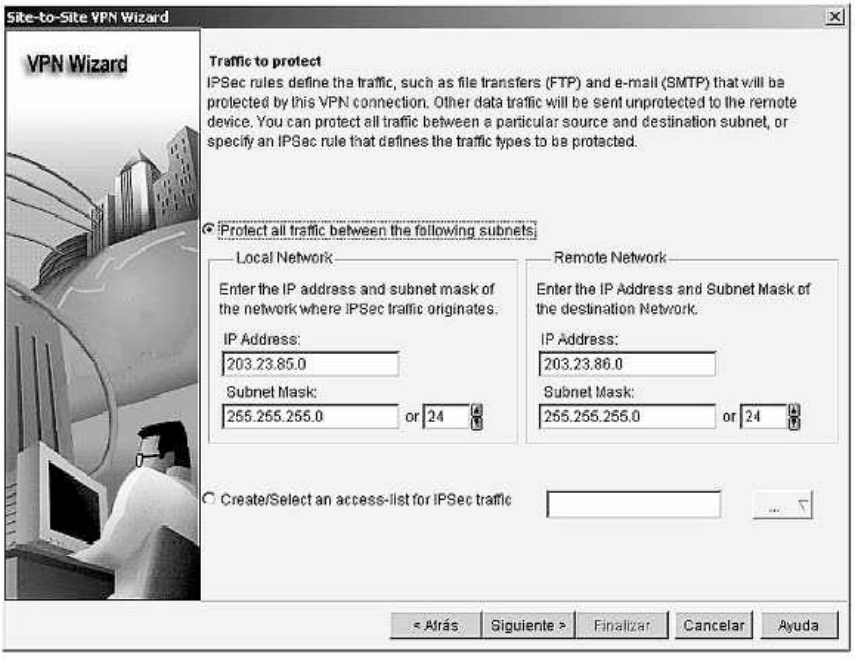
Para utilizar el IPsec transform set por defecto, pulse **Siguiente** en la página **Transform Set**.



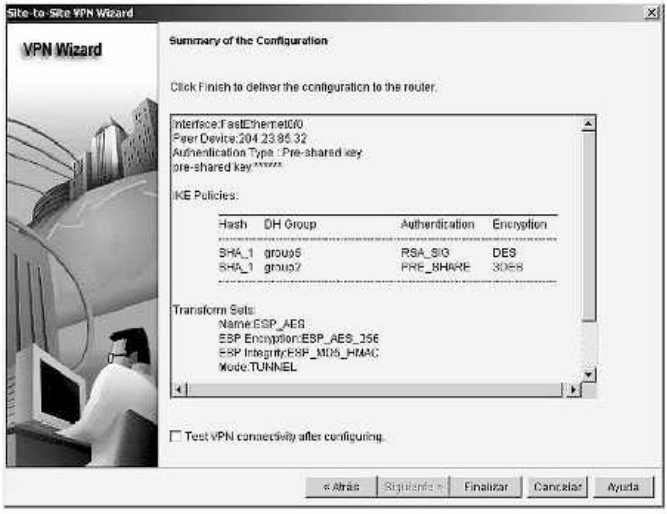
La cuarta tarea del asistente paso a paso consiste en configurar el tráfico que requiere protección. Marque la casilla **Protect all traffic between the following subnets** y defina la dirección IP y la máscara de subred de la red local donde se origina el tráfico IPsec y la de la red remota hacia donde se envía el tráfico IPsec.

Para especificar una ACL personalizada que defina el tipo de tráfico a proteger marque la casilla **Create/Select an access-list for IPsec traffic**.

Podrá seleccionar una ACL existente o crear una nueva siguiendo las opciones **Select an existing rule** o **Create a new rule**.

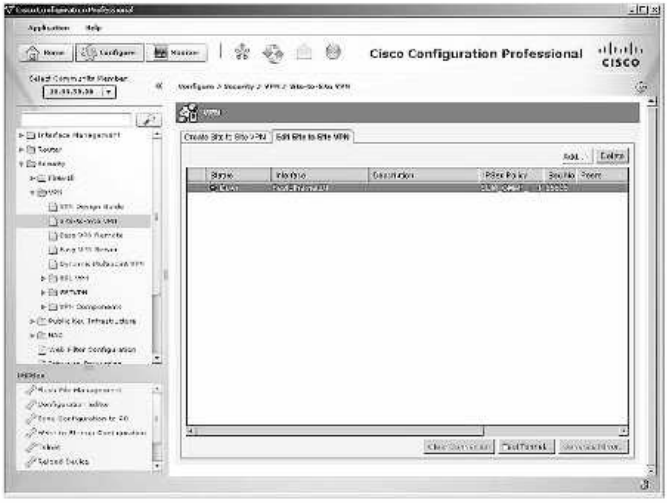


Una vez completos todos los datos requeridos, continúe con **Finalizar**. La última ventana mostrará el resumen de la configuración, termine con el botón **Finalizar**.



Para ver todos los parámetros y el estado de túneles IPsec, seleccione **Monitor / Security / VPN Status / IPsec Tunnels**.

Para probar la configuración del túnel VPN seleccione **Configure / Security / VPN / Site-to-Site VPN / Edit Site to Site VPN** y luego el botón **Test Tunnel**.



9.11 VPN DE ACCESO REMOTO

Las VPN proveen comunicaciones seguras con permisos de acceso ajustados a usuarios individuales, tales como empleados, contratistas y socios. También mejoran la productividad, extendiendo la red y aplicaciones corporativas en forma segura, al mismo tiempo que se reducen los costes y se aumenta la flexibilidad.

Existen dos métodos principales para implementar VPN de acceso remoto:

- **Secure Sockets Layer** (SSL).
- **IP Security** (IPsec).

Dependiendo de sus necesidades, VPN IPsec y VPN SSL son complementarias, ya que resuelven diferentes problemas.

Tanto la tecnología IPsec como VPN SSL ofrecen acceso a virtualmente cualquier aplicación o recurso de la red, sin embargo, IPsec supera a SSL de muchas formas significativas.

- Número de aplicaciones soportadas.
- Fortaleza de su cifrado.
- Fortaleza de su autenticación.
- Seguridad general.

9.11.1 SSL VPN

Una VPN SSL no requiere un cliente de software instalado previamente en el host remoto. Proporciona conectividad de acceso remoto a los recursos corporativos a cualquier usuario autorizado, desde cualquier ubicación en Internet.

El acceso basado en Web sin clientes y el acceso completo a la red, sin software instalado previamente en el equipo, facilita el acceso remoto personalizado para cada tipo de usuario.

La protección contra virus, gusanos, spyware y hackers, integrando la seguridad en la red y en la plataforma Cisco SSL VPN, reduce los costos y la complejidad de la administración, eliminando la necesidad de equipos e infraestructura adicionales de seguridad.

SSL VPN provee tres modos de acceso remoto en los routers con Cisco IOS: clientless, thin client y full client. Los dispositivos ASA tienen dos modos: *clientless* y el cliente AnyConnect.

- **Modo clientless**: el usuario remoto accede a la red interna o corporativa utilizando un navegador web estándar en la máquina cliente sin necesidad de un software VPN especializado instalado. No todas las aplicaciones cliente-servidor son accesibles mediante clientless SSL por lo tanto no funciona para empleados que requieren acceso completo a la red. Sin embargo, este acceso limitado es muchas veces una solución perfecta para quienes deben acceder solo a un conjunto limitado de recursos en la red de la organización.

- **Modo thin client**: llamado también TCP port forwarding, asume que la aplicación cliente utiliza TCP para conectarse a un puerto de un servidor bien conocido. En este modo, el usuario remoto descarga un componente Java utilizando un enlace provisto en la página del portal. El componente Java actúa como un proxy TCP en la máquina cliente para los servicios configurados en el gateway de la SSL VPN. El componente Java inicia una nueva conexión SSL para cada conexión del cliente. El componente Java inicia una petición HTTP desde el cliente del usuario remoto hacia el gateway de la SSL VPN. El nombre y número de puerto del servidor interno de correo electrónico está incluido en la petición. El gateway VPN crea una conexión TCP para dicho servidor y puerto de correo electrónico interno. El modo *thin client* es también conocido como un tipo de modo *clientless* y puede ser utilizado en cualquier equipo que soporte VPN sin cliente. Extiende la capacidad de las funciones criptográficas del navegador web para permitir el acceso remoto a aplicaciones basadas en TCP, tales como POP3, SMTP, IMAP, telnet y SSH.

- **Modo full client**: permite el acceso completo a la red corporativa utilizando un túnel VPN SSL, el cual es utilizado para transportar datos al nivel de capa de red. Este modo soporta la mayor parte de las aplicaciones basadas en IP, tales como Microsoft Outlook, Microsoft Exchange, Lotus Notes Email y Telnet. El ser parte de la SSL VPN resulta transparente para las aplicaciones que se ejecutan en el cliente. Se descarga un componente Java para manipular el túnel entre el host cliente y el gateway de la SSL VPN. El usuario puede utilizar cualquier aplicación como si el host cliente se encontrara dentro de la red interna. Este cliente VPN, debido a que es descargado en forma dinámica y actualizado sin ninguna distribución manual de software o interacción

con el usuario final, requiere poco soporte por parte de las organizaciones, minimizando así los costos de implementación y operación. Al igual que con el acceso clientless, el modo de acceso completo ofrece un acceso total y personalizado en base a los privilegios de acceso del usuario final. El modo de acceso completo es una opción natural para los empleados que necesitan acceso remoto a las mismas aplicaciones y recursos de red que utilizan dentro de la oficina.

Establecer una sesión SSL involucra los siguientes pasos:

1. El usuario ejecuta una conexión saliente con el puerto TCP 443.

2. El router responde con un certificado digital que contiene una clave pública firmada digitalmente por una CA (*Certificate Authority*) confiable.

3. El host del usuario genera una clave secreta compartida que usan ambos participantes.

4. La clave compartida es cifrada con la clave pública del router y es transmitida hacia el router. El software del router es capaz de descifrar el paquete utilizando su clave privada. Ahora, ambos participantes de la sesión conocen la clave secreta compartida.

5. La clave es utilizada para cifrar la sesión SSL.

SSL utiliza algoritmos de cifrado con tecnologías de hash con claves de longitud de entre 40 y 256 bits.

NOTA:

La funcionalidad de VPN SSL puede agregar una carga de procesamiento importante si el router ya se encuentra ejecutando varias de estas otras funciones. El proceso SSL VPN consume recursos de CPU y memoria en forma intensiva.

9.11.2 Cisco Easy VPN

Mientras que las SSL VPN resultan útiles en muchos casos, numerosas aplicaciones requieren la seguridad de una conexión VPN IPsec para su autenticación y para cifrar datos. Establecer una conexión entre dos sitios puede ser complicado y en general requiere coordinación entre los administradores de red en cada extremo para configurar los parámetros de la VPN.

La solución Cisco Easy VPN ofrece flexibilidad, escalabilidad y facilidad de uso para VPN de sitio a sitio y de acceso remoto. Consiste de tres componentes:

- **Cisco Easy VPN Server**: un router Cisco IOS o un equipo Cisco ASA Firewall, funcionando como el dispositivo cabecera de la VPN de acceso remoto o sitio a sitio.
- **Cisco Easy VPN Remote**: un router Cisco IOS o un equipo Cisco ASA Firewall, funcionando como cliente VPN remoto.
- **Cisco Easy VPN Client**: una aplicación soportada por un PC, utilizada para acceder al servidor Cisco VPN.

La mayor parte de los parámetros de la VPN se definen en el Cisco IOS Easy VPN Server para simplificar la implementación. Cuando un cliente remoto inicia una conexión de túnel VPN, el Cisco Easy VPN Server envía las políticas IPsec al cliente y crea la conexión de túnel VPN IPsec correspondiente.

Los dispositivos remotos pueden ser trabajadores móviles ejecutando el cliente Cisco Easy VPN en host remotos para establecer fácilmente conexiones VPN con el dispositivo Cisco Easy VPN Server a través de Internet. También puede ser un dispositivo Cisco ejecutando la funcionalidad Cisco Easy VPN Remote, la cual le permite ser un cliente del Easy VPN Server. Esto quiere decir que los individuos en pequeñas sucursales no necesitan ejecutar el software cliente de la VPN en sus ordenadores.

El Cisco Easy VPN Server hace posible que los trabajadores remotos que utilizan clientes VPN en sus ordenadores puedan crear túneles IPsec seguros para acceder a la intranet de sus oficinas centrales, donde se almacenan datos y aplicaciones críticas. Permite a los routers Cisco IOS y firewalls Cisco PIX y ASA funcionar como cabeceras VPN en VPN de acceso remoto y de sitio a sitio. Los dispositivos de las oficinas remotas utilizan la funcionalidad **Cisco Easy VPN Remote** o la aplicación **Cisco VPN Client** para conectarse al servidor, el cual luego envía las políticas de seguridad definidas hacia los dispositivos VPN

remotos. Esto asegura que dichas conexiones utilicen políticas actualizadas desde el momento en que se establecen las conexiones.

Cisco Easy VPN Remote permite que los routers Cisco IOS, firewalls Cisco PIX, clientes Cisco VPN 3002 o clientes de software, actúen como clientes remotos VPN.

Estos dispositivos pueden recibir políticas de seguridad desde un Cisco Easy VPN Server, minimizando los requisitos de configuración en los dispositivos remotos. Esta solución de bajo costo es ideal para oficinas remotas con poco soporte IT o para grandes instalaciones con equipamiento local de clientes, donde no resulta práctico configurar los dispositivos remotos en forma individual.

Cuando un cliente se conecta a un servidor, toma lugar la negociación para asegurar la VPN:

1. El cliente VPN inicia el proceso de fase 1 IKE. Si se utiliza una clave precompartida para la autenticación, el cliente VPN inicia el modo agresivo. Si se utilizan certificados digitales para la autenticación, el cliente VPN inicia el modo principal.

2. El cliente VPN establece una SA ISAKMP. Para reducir la configuración manual en el cliente VPN, las propuestas ISAKMP de Easy VPN incluyen todas las combinaciones de algoritmos de cifrado y hash, métodos de autenticación y tamaños de grupos DH.

3. Easy VPN Server acepta la propuesta de SA. La política ISAKMP puede consistir de diferentes propuestas, pero el Easy VPN Server utiliza la primera coincidencia; por lo tanto, siempre deben configurarse primero las políticas más seguras. En este punto finaliza la autenticación de los dispositivos y comienza la autenticación del usuario.

4. Easy VPN Server inicia el desafío de nombre de usuario y contraseña. La información ingresada se verifica contra las entidades de autenticación utilizando protocolos AAA tales como RADIUS y TACACS+. También pueden utilizarse tokens a través del proxy AAA. Los dispositivos VPN configurados para controlar a los clientes VPN remotos siempre deben asegurar la autenticación de los usuarios.

5. Se inicia el proceso de configuración de modo. Los restantes parámetros del sistema (dirección IP, DNS, atributos de división de túnel y demás) son enviados al cliente VPN en este punto.

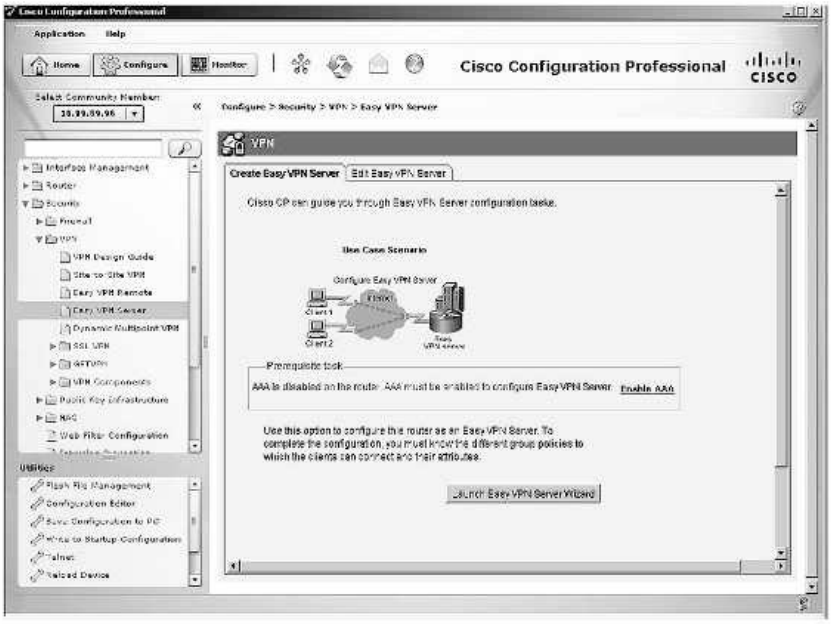
6. Se inicia el proceso *Reverse Route Injection* (RRI). RRI asegura la creación de una ruta estática en el Cisco Easy VPN Server para el direccionamiento IP interno de cada cliente VPN.

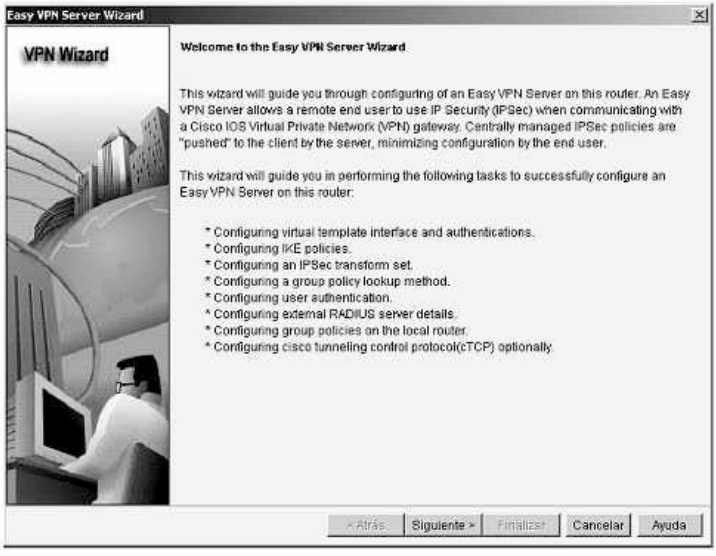
7. El modo rápido IPsec completa la conexión. La conexión se completa una vez que se crearon las SA IPsec.

9.11.3 Servidor Cisco Easy VPN

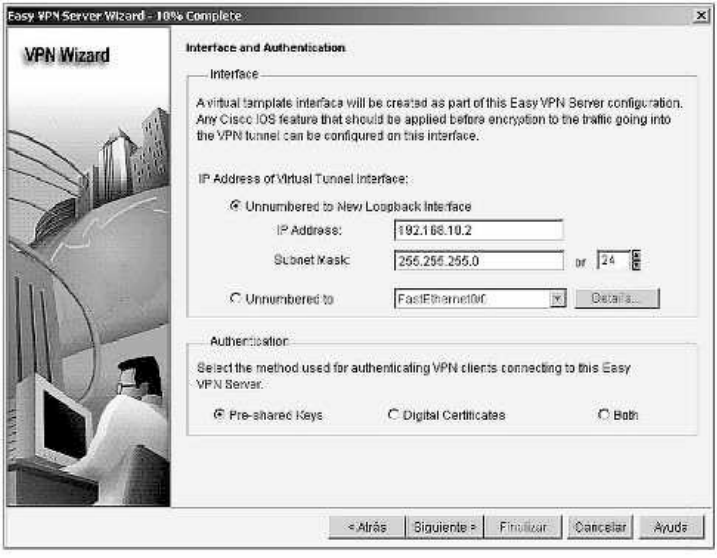
La configuración de Cisco Easy VPN Server utilizando el asistente CCP necesita algunos requisitos previos, como que los privilegios de los usuarios, AAA, y la contraseña **enable secret** estén configurados de antemano.

Desde la página principal del CCP, seleccione **Configure**, luego **Security** / **VPN**, y luego escoja la opción **Easy VPN Server**. Si AAA no ha sido configurado previamente, el asistente le pide que lo configure. Si se encuentra desactivado en el router, debe ser configurado antes de comenzar la configuración del servidor Easy VPN y crear al menos un usuario administrativo.

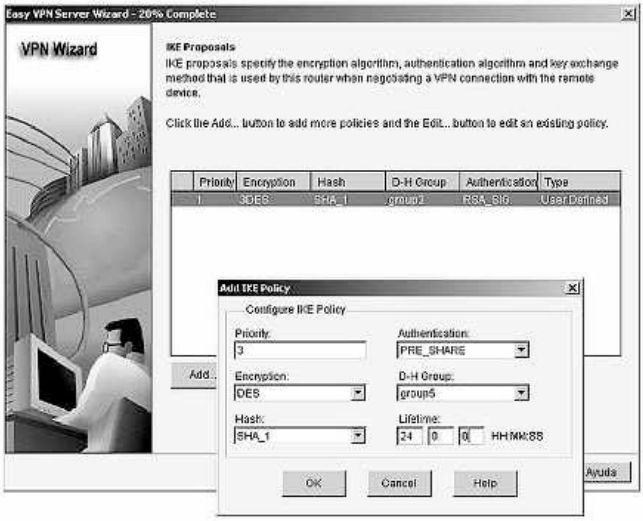


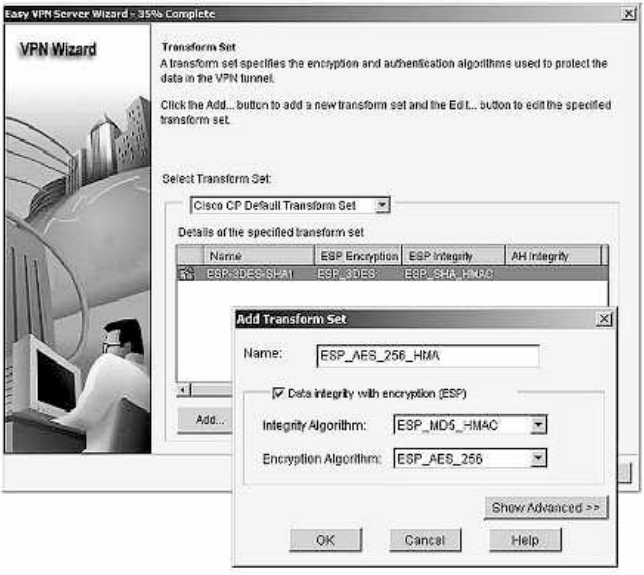


Cuando el asistente de Easy VPN Server se inicia, aparecerán las ventanas para la configuración de interfaz y de autenticación. Especifique la interfaz del router donde la conexión VPN se terminará, y el método de autenticación.



Continúe con **Siguiente** para ver la ventana de propuestas IKE. Puede agregar o editar las propuestas con los botones **Edit** y **Add**. Continúe con **Siguiente**. CCP proporciona transform set por defecto, puede agregar o editarlos con los botones **Edit** y **Add**. Continúe con **Siguiente**.

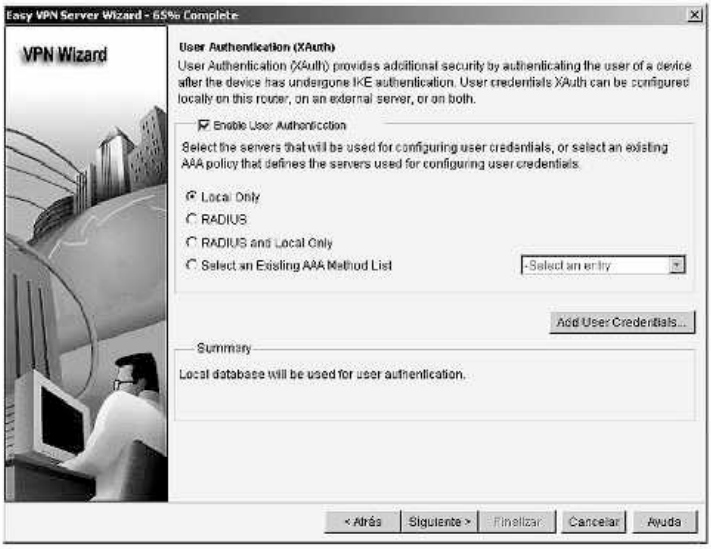




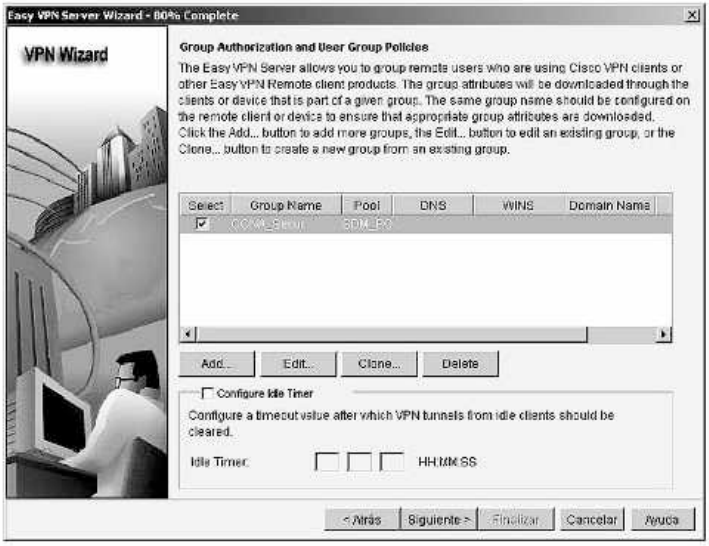
Aparece a continuación la ventana de autorización y directiva del grupo. Hay tres opciones para elegir la ubicación donde se pueden almacenar las directivas de grupo:

- **Local**: todos los grupos están en la configuración del router en la NVRAM.
- **RADIUS**: el router utiliza el servidor RADIUS para la autorización de grupo.
- **RADIUS y Local**: el router puede buscar políticas almacenadas en una base de datos del servidor AAA al que se puede llegar a través de RADIUS.

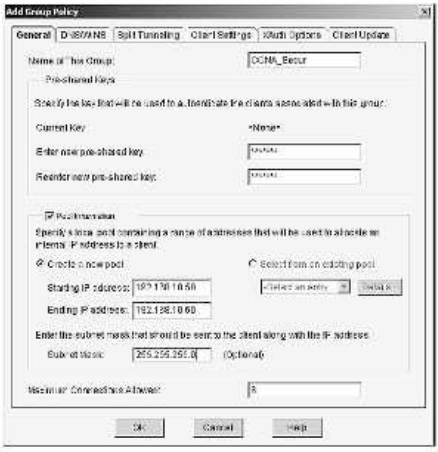
Seleccione **Siguiente** para configurar la autenticación de usuario opcional (XAuth).



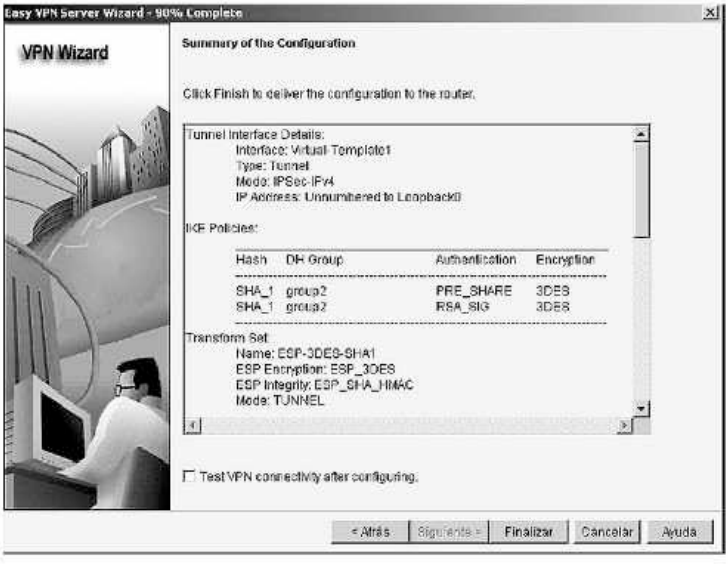
Continúe con **Siguiente** para configurar los parámetros de autorización de grupo.



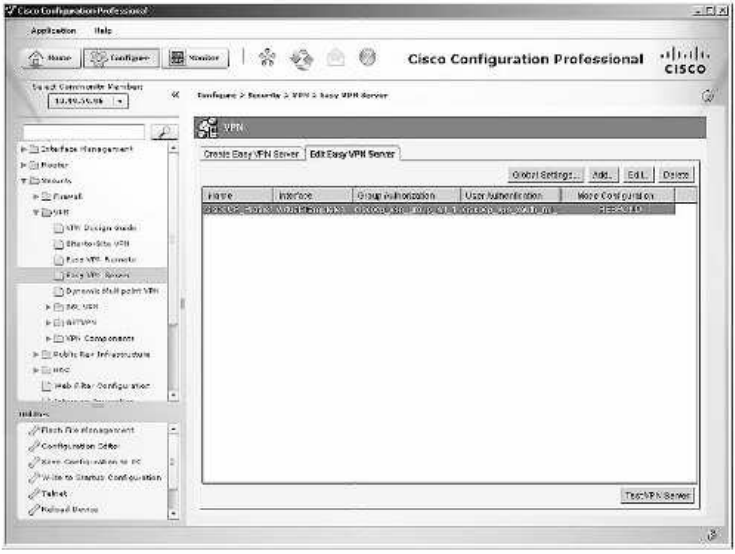
Puede agregar una nueva directiva de grupo desde el botón **Add**; complete los datos requeridos, como nombre del grupo o claves previamente compartidas.

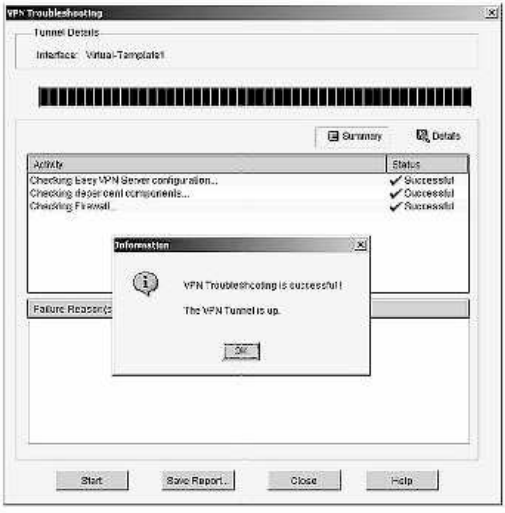


Después de todos los pasos, el asistente Easy VPN Server presenta un resumen de los parámetros configurados. Haga clic en **Atrás** para corregir los posibles errores en la configuración. De lo contrario, haga clic en **Finalizar** para aplicar la configuración al router.



Desde la solapa Edit Easy VPN Server es posible ejecutar una prueba para confirmar la configuración del túnel con el botón **Test VPN Server**, esto realiza un chequeo mostrando una posible solución de problemas.





9.12 FUNDAMENTOS PARA EL EXAMEN

- Estudie y analice los diferentes tipos de VPN, cuáles son y en qué caso los aplicaría.
- Tenga en cuenta las ventajas y desventajas de un túnel GRE.
- Recuerde claramente qué es IPsec, cuáles son sus protocolos y para qué se utilizan.
- Analice los algoritmos de encriptación, sepa la diferencia entre simétricos y asimétricos.
- Estudie el protocolo IKE y sus fases.
- Estudie y practique las configuraciones de los diferentes tipos de VPN, tanto desde la CLI como con CCP.
- Recuerde qué es una VPN SSL, sus modos y cómo funciona cada uno de ellos.
- Estudie la solución Cisco Easy VPN, sus componentes y configuración.
- Si no dispone de dispositivos reales, todas las prácticas de VPN pueden realizarse con simuladores.

Anexo 1

INTRODUCCIÓN A IPV6

DIRECCIONAMIENTO IPv6

IPv6 ha estado en desarrollo desde mediados de los 90 y durante varios años. Se había anunciado al principio como el protocolo que podría expandir el direccionamiento IP, llevar IP mobile a la madurez y finalmente ser capaz de incorporar seguridad a nivel de capa 3. Esas afirmaciones son correctas pero hay que tener en cuenta que a nivel de capa 3 esas capacidades de IPv6 han sido aportadas a IPv4 en los pasados años. Actualmente, las direcciones IPv4 son escasas y la mayor razón en Internet para evolucionar a IPv6 es la necesidad de un mayor direccionamiento.

Una de las razones de que el direccionamiento IPv4 sea demasiado escaso es que no ha sido asignado eficientemente. Las direcciones de clase A son excesivamente grandes para la mayoría de las organizaciones, ya que soportan unas 16.777.214 direcciones de host, mientras que las direcciones de clase C soportan solo 254 direcciones de host. Como resultado de esto, muchas organizaciones hacen peticiones de clase B que soportan 65.534 direcciones de host, pero hacen solo un uso parcial de dicho rango.

Inicialmente, un dispositivo IP requería una dirección pública. Para prevenir el agotamiento de las direcciones IPv4, la IETF (*Internet Engineering Task Force*) adoptó el uso de CIDR (*Classless Interdomain Routing*), VLSM (*Variable-Length Subnet Mask*) y NAT (*Network Address Translation*). CIDR y VLSM trabajan juntas a la hora de mejorar el direccionamiento, mientras que NAT

oculta clientes y minimiza la necesidad de direcciones públicas. Otra de las razones de escasez de direcciones públicas es que no han sido asignadas equitativamente a lo largo del mundo. Una gran cantidad de direccionamiento es ocupada por EE.UU., mientras que Europa es el siguiente en la lista con una larga porción de direcciones. Asia, en cambio, tiene un número insuficiente de direcciones en comparación con su población; aunque la percepción desde EE.UU. es que todavía existe espacio libre en el direccionamiento IPv4 en Asia, se reconoce la necesidad de implementar IPv6 y así obtener más direccionamiento.

Otra razón para considerar la necesidad de un mayor direccionamiento es el crecimiento exponencial de la población mundial, con el persistente crecimiento de consumibles electrónicos que requieren el uso de direcciones IP.

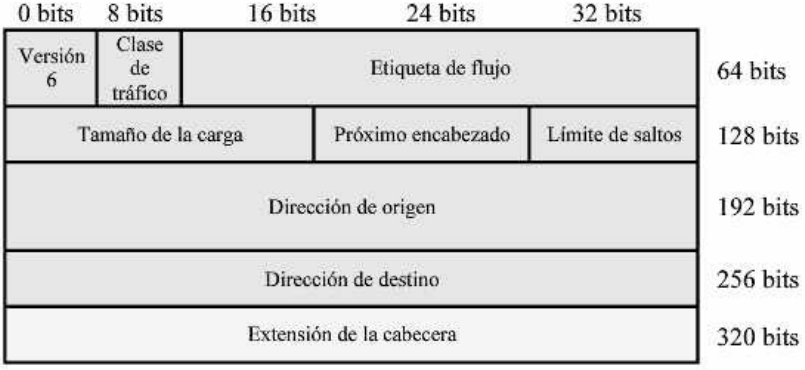
Esta necesidad de direccionamiento IP podría ser atenuada intentando utilizar NAT y asignaciones temporales a través de DHCP, pero tener sistemas intermedios manipulando los paquetes complica el diseño y la resolución de problemas. El concepto del diseño de Internet con innumerables sistemas intermedios no hace que NAT trabaje adecuadamente; sin embargo, es un mal necesario.

La longitud de una dirección IPv6 es lo primero que sale a relucir, son 128 bits, lo que hace 2.128 direcciones IPv6 disponibles. Varias de estas direcciones dan funciones especiales y están reservadas pero aun así quedarían disponibles aproximadamente 5 × 1.028 direcciones IP por cada habitante del planeta. Lo que permitiría que el direccionamiento pueda crecer sin preocupaciones, en contraposición al direccionamiento, IPv4 cuya cantidad está limitada a $\mathbf{2^{32}}$.

En IPv6 se utiliza una cabecera más simplificada que en IPv4, haciendo que el procesamiento sea más eficiente, permitiendo un mecanismo más flexible y a su vez extensible a otras características. Una de esas características es la movilidad, mobile IP es un estándar de la IETF que permite a los usuarios con dispositivos wireless estar conectados de manera transparente y moverse a cualquier sitio sin restricciones.

La cabecera IPv6 es optimizada para procesadores de 32 a 64 bits y las extensiones de cabecera permiten la expansión sin tener que forzar a que los campos que no se usan se estén transmitiendo constantemente.

Las principales diferencias entre las cabeceras de las dos versiones es la longitud de los campos de origen y destino. También hay otros campos que son aparentes como *checksum*, fragmentación y la etiqueta de flujo. A diferencia de IPv4 móvil, IPv6 móvil (MIPv6) evita el ruteo triangular y por lo tanto es tan eficiente como el IPv6 normal. IPv& también incorpora características de IPsec.



Formato del direccionamiento IPv6

La primera diferencia respecto a IPv4 es que las direcciones IPv6 son de 128 bits y están representadas en un formato hexadecimal (en lugar de la notación decimal tradicional) y separada cada parte por dos puntos en lugar de uno. Teniendo de esta forma 8 partes de 16 bits cada una. Como cada dígito hexadecimal se asocia con 4 bits, cada campo de 16 bits será de 4 dígitos hexadecimales.

Un ejemplo de dirección IPv6 puede ser el siguiente:

2001:0000:0001:0002:0000:0000:0000:ABCD

Este formato se puede reducir hasta optimizar la lectura para su comprensión. Hay dos formas para conseguir simplificar tanta cantidad de números:

- Todos los ceros a la izquierda de cada uno de los campos pueden ser omitidos.

  2001:0:1:2:0:0:0:ABCD

- Se pueden omitir los campos consecutivos de 0 con "**::**", independientemente de la cantidad de campos que se abrevie. Este mecanismo solo puede hacerse una vez, debido a que luego no se podría reestructurar la cantidad de campos exactamente como era.

  2001:0:1:2::ABCD

Tipos de comunicación IPv6

De la misma manera que su antecesor en IPv6 se soportan estas clases de direcciones:

- **Unicast**: para enviar tráfico a una sola interfaz.
- **Multicast**: para enviar a todas las interfaces del mismo grupo. Una dirección IPv6 del mismo grupo multicast identifica un conjunto de interfaces en diferentes dispositivos.
- **Anycast**: para enviar tráfico a la interfaz más cercana dentro de un grupo. Una dirección IPv6 de anycast también identifica un conjunto de interfaces en diferentes dispositivos, pero la diferencia de un paquete enviado a una dirección anycast es que dicho paquete está destinado al dispositivo más cercano. Esto será determinado por el protocolo de enrutamiento que se esté utilizando. Todos los nodos con la misma dirección de anycast deberán proporcionar el mismo servicio.

Una interfaz puede tener varias direcciones y de diferentes tipos. Los routers tienen que reconocer estas direcciones incluyendo las de anycast y multicast.

Anexo 2

CUESTIONARIO

PREPARATIVOS PARA EL EXAMEN

Aprobar un examen de certificación no es una tarea fácil, pero tampoco imposible. Existen diferentes maneras de preparación, que van desde cursos bajo la plataforma de Cisco, cursos intensivos o preparación libre a través de diferentes bibliografías y prácticas. Lo único y fundamental, aunque parezca una obviedad, es estudiar.

En lo personal y después de varios años de experiencia docente y recabando información de los propios alumnos debo decir que ningún método es perfecto y que hacer recomendaciones es una tarea delicada. Si se es alumno de una academia, una vez finalizado el curso completo se debe centrar la atención en el examen, no es lo mismo prepararse para el examen de certificación que para un curso. Si la intención es presentarse por cuenta propia, se deben estudiar a fondo todos los conceptos contenidos en el examen, incluso los más insignificantes, no sirve de nada la experiencia laboral, son ideas diferentes. Un ejemplo: son típicos los casos de alumnos avanzados, con amplia experiencia laboral con routers y switches pero que no sabían crear subredes (una de las cuestiones mínimas indispensables de las que hablaba), el fracaso es rotundo.

Recomendaciones para la presentación al examen

No hay truco ni magia. Hay que realizar test de preguntas, estudiar en grupo, consultar toda la bibliografía disponible e Internet. Muchas veces un aluvión de nuevos conocimientos puede ser contra producente. Cuando un alumno

desaprueba reiteradas veces, seguramente no será porque le falten conocimientos, sino porque le falte exactitud, rapidez y confianza.

Previo a comenzar el examen se podrán hacer las anotaciones necesarias como ayuda a la memoria. Se debe controlar el tiempo cada cierto período. Si estando en la pregunta 30, por ejemplo, quedan 20 minutos es un mal pronóstico.

Debemos tener siempre en cuenta que no es posible volver atrás en el cuestionario, y que no se puede avanzar sin responder. Es necesario probar el correcto funcionamiento de las topologías de los simuladores y guardar las configuraciones con el comando respectivo. Los comandos de ayuda no funcionan por lo que hay que estudiar los comandos completos.

Las preguntas que siguen a continuación son una base de ayuda para el examen, de ninguna manera son garantía de aprobación sin el conocimiento adecuado. Se han realizado cuidadosamente, intentando que se parezcan lo más posible al examen.

CUESTIONARIO TEMÁTICO

1. ¿Qué opción es la diferencia clave entre el modo de configuración de ACL con Cisco IOS y el modo de configuración Cisco ASA?

A. El modo de configuración ACL en Cisco IOS tiene un permiso implícito al final de toda regla.
B. El modo de configuración en Cisco IOS soporta la configuración de ACL global, que se aplica a todas las interfaces.
C. El modo de configuración de ACL con Cisco ASA utiliza máscaras de red en lugar de máscaras comodín.
D. El modo de configuración de ACL en Cisco ASA se aplica al tráfico dirigido a las direcciones IP de las interfaces de dispositivos Cisco ASA.
E. El Cisco ASA no es compatible con las ACL estándar. El dispositivo Cisco ASA solo soporta ACL extendidas.

Respuesta: C

2. Cuando el inicio de sesión de autenticación AAA está configurada en los routers Cisco, ¿qué dos métodos de autenticación deben utilizarse como método final para asegurarse de que el administrador puede iniciar sesión en el router en caso de que el servidor externo AAA falle?

   A. group RADIUS
   B. group TACACS+
   C. local
   D. krb5
   E. enable secet
   F. if-authenticated

Respuesta: CE

3. ¿Qué comando habilita la característica Cisco IOS image resilience?

   A. secure boot-<IOS image filename>
   B. secure boot-running-config
   C. secure boot-start
   D. secure boot-image

Respuesta: D

4. Usted es el administrador de seguridad de una red de una gran empresa con muchos lugares remotos. Se le ha dado la tarea de implementar una solución Cisco IPS. ¿Qué lugar de la red sería el mejor lugar para desplegar Cisco IOS IPS?

   A. El firewall de la conexión a Internet en la sede corporativa.
   B. El punto de entrada en el centro de datos.
   C. Fuera del firewall de la conexión a Internet sede corporativa.
   D. Los routers de las sucursales remotas.

Respuesta: D

5. ¿Cuáles de los siguientes IPsec transform set provee mayor protección?

A. crypto ipsec transform-set 1 esp-3des esp-sha-hmac
B. crypto ipsec transform-set 2 esp-3des esp-md5-hmac
C. crypto ipsec transform-set 3 esp-aes 256 esp-sha-hmac
D. crypto ipsec transform-set 4 esp-aes esp-md5-hmac
E. crypto ipsec transform-set 5 esp-des esp-sha-hmac
F. crypto ipsec transform-set 6 esp-des esp-md5-hmac

Respuesta: C

6. ¿Cuáles son las dos opciones que representan una amenaza para la instalación física de una red empresarial?

A. Vigilancia con cámaras.
B. Guardias de seguridad.
C. Suministro eléctrico.
D. Acceso físico a la sala de ordenadores.
E. Cambio de control.

Respuesta: CD

7. ¿Qué afirmación describe cómo el remitente del mensaje verifica el cifrado asimétrico emitido?

A. El emisor encripta el mensaje utilizando la clave pública del remitente, y el receptor descifra el mensaje utilizando la clave privada del remitente.
B. El emisor encripta el mensaje utilizando la clave privada del remitente y el receptor descifra el mensaje utilizando la clave pública del remitente.
C. El emisor encripta el mensaje utilizando la clave pública del receptor, y el receptor descifra el mensaje utilizando la clave privada del receptor.
D. El emisor encripta el mensaje utilizando la clave privada del receptor, y el receptor descifra el mensaje utilizando la clave pública del receptor.
E. El emisor encripta el mensaje utilizando la clave pública del receptor, y el receptor descifra el mensaje utilizando la clave pública del remitente.

Respuesta: B

8. ¿Qué tipo de NAT se utiliza cuando se traducen varias direcciones IP internas a una única dirección global IP externa?

A. Política de NAT.
B. PAT dinámico.
C. NAT estático.
D. NAT dinámico.
E. Política de PAT.

Respuesta: B

9. ¿Cuáles son dos características soportadas por Cisco IronPort Security Gateway?

A. Protección spam.
B. Outbreak intelligence.
C. Escaneo HTTP y HTTPS.
D. Encriptación de e-mail.
E. DDoS.

Respuesta: AD

10. Se sospecha que un atacante en su red ha configurado un dispositivo de capa 2 clandestino para interceptar el tráfico de varias VLAN, lo que permite al atacante obtener datos potencialmente sensibles.

¿Qué dos métodos le ayudarán a mitigar este tipo de actividad?

A. Desactivar todos los puertos troncales y configurar manualmente cada VLAN según se requiera en cada puerto.
B. Colocar los puertos activos no utilizados en una VLAN no utilizada.
C. Asegurar con encriptación la VLAN nativa.
D. Establecer la VLAN nativa en los puertos troncales a alguna de VLAN no utilizada.
E. Desactivar DTP en los puertos que requieren trunking.

Respuesta: DE

11. ¿Cuál de las siguientes opciones determina que se dispare una alarma falso negativo?

A. Se activa una alarma por el tráfico normal o por una acción benigna.
B. La firma no se activa cuando se detecta tráfico ofensivo.
C. Genera una alarma cuando se detecta tráfico ofensivo.
D. Una firma no se dispara cuando el tráfico capturado y analizado no es ofensivo.

Respuesta: B

12. Usted utiliza Cisco IOS IPS. ¿Qué estado tiene que tener una firma antes de que cualquier acción pueda ser tomada cuando un ataque coincide con dicha firma?

A. Habilitada.
B. Reincorporada.
C. Compilada exitosamente.
D. Compilada exitosamente y unretired.
E. Compilada exitosamente y habilitada.
F. Reincorporada y habilitada.
G. Habilitada, reincorporada y compilada exitosamente.

Respuesta: G

13. Cuáles son dos opciones características del asistente Cisco Configuration Professional Security Audit?

A. Muestra una pantalla con casillas de verificación para que pueda elegir las opciones relacionadas con la seguridad para implementar cambios de configuración.
B. Tiene dos modos de funcionamiento: interactivas y no interactivas.
C. Habilita automáticamente el firewall de Cisco IOS y Cisco IOS IPS para asegurar el router.
D. Utiliza diálogos interactivos y le indica a la aplicación basada en roles CLI.
E. Obliga a los usuarios a identificar primero cuáles son las interfaces del router que se conectan a la red en el interior y con la red exterior.

Respuesta: AE

14. Respecto a la siguiente sintaxis:

```
access-list 10 permit 10.10.0.10
access-list 10 deny 10.10.0.0 0.0.0.255.255
access-list 10 permit 10.0.0.0 0.0.0.255.255

interface FastEthernet0/0
ip access-group 10 in
```

¿Qué afirmación acerca de esta configuración de una lista de control de acceso es verdadera?

- **A.** La lista de acceso permite todo el tráfico en la subred 10.0.0.0.
- **B.** Todo el tráfico de las subredes 10.10.0.0 se deniega.
- **C.** Solo el tráfico desde 10.10.0.10 está permitido.
- **D.** Esta configuración no es válida. Se debe configurar como una ACL extendida para permitir la máscara comodín asociada.
- **E.** Desde la subred 10.10.0.0, solo el tráfico procedente de 10.10.0.10 está permitido, el tráfico procedente de la subred 10.0.0.0 también está permitido.
- **F.** La lista de acceso permite el tráfico destinado al servidor 10.10.0.10 en FastEthernet0 / 0 de cualquier origen.
- **G.** Ninguna de las anteriores es correcta.

Respuesta: E

15. ¿Qué dos características del protocolo TACACS+ son verdaderas?

- **A.** Utiliza UDP puertos 1645 o 1812.
- **B.** Separa las funciones AAA.
- **C.** Encripta el cuerpo de cada paquete.
- **D.** Ofrece amplias capacidades de contabilidad.
- **E.** Es un protocolo estándar abierto RFC.

Respuesta: BC

16. Respecto a la siguiente sintaxis:

```
Jan12        20:31:05.150:AAA/MEMORY:create_user          (0x4C5E1F60)
user=tectearruser=`NULL´

ds0=port=`tty´rem_addr=`192.0.52.14´authen_type_ASCII
service=ENABLEpriv=15

initial_task_id_=`0´, vrf=(id=0)

Jan12 20:31:05.150:AAA/AUTHEN/STAR (2600878790):port=`tty515´list="

action=LOGINservice=ENABLE

Jan12  20:31:05.150:AAA/AUTHEN/STAR  (2600878790):CONSOLE  ENABLE-de
enable password (if any)

Jan12 20:31:07.190:AAA/AUTHEN/STAR (2600878790):Method=ENABLE

Jan12 20:31:07.190:AAA/AUTHEN (2600878790): status=GETPASS

Jan12   20:31:07.190:AAA/AUTHEN/CONT   (2600878790):   continue_login
(user=`(undef)´)

Jan12 20:31:07.190:AAA/AUTHEN/STAR (2600878790): status=GETPASS

Jan12 20:31:05.190:AAA/AUTHEN/CONT (2600878790):Method=ENABLE

Jan12 20:31:07.190:AAA/AUTHEN (2600878790):password incorrect

Jan12 20:31:07.190:AAA/AUTHEN (2600878790): status=FAIL

Jan12 20:31:07.190:AAA/MEMORY:free_user (0x4C5E1F60) user=`NULL´
```

¿Qué afirmación acerca de esta salida es verdadera?

- **A.** El usuario ha iniciado sesión en el router con el nombre de usuario y contraseña correctos.
- **B.** El inicio de sesión falló porque no estaba la password por defecto.
- **C.** El inicio de sesión ha fallado porque la contraseña introducida es incorrecta.
- **D.** Al usuario registrado se le dio el nivel de privilegio 15.

Respuesta: C

17. ¿Qué característica de gestión del router prevé la posibilidad de configurar múltiples vistas administrativas?

A. role-based CLI
B. virtual routing and forwarding
C. secure config privilege {level}
D. parser view view name

Respuesta: A

18. ¿Qué dos afirmaciones sobre SSL-based VPN son verdaderas?

A. Los algoritmos asimétricos se utilizan para la autenticación y el intercambio de claves.
B. SSL VPN y VPN IPsec no se pueden configurar al mismo tiempo en el mismo router.
C. La interfaz de programación de aplicaciones se puede utilizar para modificar extensamente el software de cliente SSL para su uso en aplicaciones especiales.
D. El proceso de autenticación utiliza las tecnologías de hash.
E. El cliente y el clientless SSL VPN requieren software de cliente para ser instalado en la máquina cliente.
F. Ninguna de las anteriores es correcta.

Respuesta: AD

19. ¿Qué protocolo de capa 2 proporciona solución a los bucles mediante la gestión de las rutas físicas de los segmentos de red?

A. root guard
B. port fast
C. HSRP
D. STP

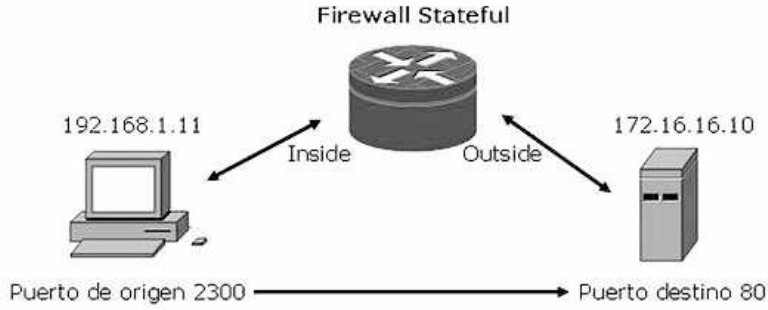
Respuesta: D

20. ¿Cuáles de las opciones son dos ventajas de un firewall de capa de aplicación?

A. Proporciona un alto rendimiento de filtrado.
B. Hace difícil que se produzcan ataques DoS.
C. Soporta un gran número de aplicaciones.
D. Autentica los dispositivos.
E. Autentica individuos.

Respuesta: BE

21. Respecto al siguiente gráfico:



Un firewall stateful tiene configurada una ACL interior donde se creó la entrada: permit ip 192.16.1.0 0.0.0.255 any. ¿Cuál sería la configuración dinámica resultante de la ACL para el tráfico de retorno en la ACL exterior?

A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300
B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
C. permit tcp any eq 80 host 192.168.1.11 eq 2300
D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Respuesta: A

22. ¿Qué opción representa un paso que se debe tomar cuando se desarrolla una política de seguridad?

A. Realizar pruebas de intrusión.
B. Determinar las puntuaciones de riesgo del dispositivo.
C. Implementar un sistema de monitorización de seguridad.
D. Realizar un análisis de riesgo cuantitativo.

Respuesta: D

23. ¿Qué enunciado describe el resultado de asegurar la imagen de IOS de Cisco con la característica Cisco IOS image resilience?

A. El comando **show version** no muestra la ubicación del archivo de la imagen de Cisco IOS.
B. El archivo de la imagen de Cisco IOS no es visible en el resultado del comando **show flash**.
C. Cuando se arranca el router, la imagen de Cisco IOS se carga desde una ubicación FTP segura.
D. La ejecución de la imagen de Cisco IOS está codificada y automáticamente se hace copia de seguridad en la NVRAM.
E. La ejecución de la imagen de Cisco IOS está codificada y automáticamente se hace copia de seguridad un servidor TFTP.

Respuesta: B

24. ¿Qué tipo de máscara de red se utiliza cuando se configuran listas de control de acceso Cisco IOS?

A. Máscara de subred extendida.
B. Máscara de subred estándar.
C. Máscara de subred.
D. Máscara wildcard.

Respuesta: D

25. ¿Qué producto Cisco IPS ofrece la característica de inspección profunda de paquetes disponible en los routers de servicios integrados?

A. Cisco iSDM
B. Cisco AIM
C. Cisco IOS IPS
D. Cisco AIP-SSM

Respuesta: C

26. ¿Cuáles son los tres modos de acceso que puede ser proporcionado por SSL VPN?

A. Cliente de túnel completo.
B. IPsec SSL.
C. TLS modo de transporte.
D. Thin client.
E. Clientless.
F. Modo de túnel TLS.

Respuesta: ADE

27. ¿Cuál de las siguientes opciones es la acción resultante de la configuración de un firewall Cisco IOS de zonas basado en política configurado según las siguientes condiciones?

```
Source: Zone 1
Destination: Zone 2
Zone pair exists?: Yes
Policy exists?: No
```

A. No afecta a la zona ni a la política.
B. pass
C. drop
D. Se aplican las políticas por defecto.

Respuesta: C

28. ¿Qué tipo de control de seguridad es una defensa en profundidad?

A. Mitigación de amenazas.
B. Análisis de riesgo.
C. Mitigación botnet.
D. Canales secretos.

Respuesta: A

29. ¿Qué lista de acceso permite el tráfico HTTP procedente del host 10.1.129.100 puerto 3030 destinado al host 192.168.1.10?

A. access-list 101 permit tcp any eq 3030
B. access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 3030 192.168.1.0 0.0.0.15 eq www
C. access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.1.10 0.0.0.0 eq www
D. access-list 101 permit tcp host 192.168.1.10 eq 80 10.1.0.0 0.0.255.255 eq 3030
E. access-list 101 permit tcp 192.168.1.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255
F. access-list 101 permit ip host 10.1.129.100 eq 3030 host 192.168.1.100 eq 80

Respuesta: B

30. Cuando las características de mitigación de STP están configuradas, ¿dónde se puede implementar root guard?

A. En los puertos que se conectan a switches que no deberían estar en el puente raíz.
B. En todos los puertos del switch.
C. Hacia los puertos de usuario.
D. Root guard debe configurarse globalmente en el switch.

Respuesta: A

31. ¿Qué técnica IPS se utiliza comúnmente para mejorar la precisión y la sensibilidad del contexto, con el objetivo de detectar y responder solo a los incidentes relevantes de tal manera de, reducir las alertas?

A. Relevancia del ataque.
B. Valor de los activos.
C. Precisión de la firma.
D. Calificación de riesgo

Respuesta: D

32. Un Cisco ASA appliance tiene tres interfaces configuradas. La primera interfaz es de entrada, con un nivel de seguridad 100. La segunda interfaz es la DMZ, con un nivel de seguridad 50. La tercera interfaz es de salida y tiene un nivel de seguridad 0. De forma predeterminada, sin ningún tipo de lista de acceso configurada…

¿Qué cinco tipos de tráfico están permitidos?

A. Tráfico saliente iniciado desde el interior hacia la DMZ.
B. Tráfico saliente iniciado desde de la DMZ hacia el exterior.
C. Tráfico saliente iniciado desde el interior hacia el exterior.
D. Tráfico entrante iniciado desde el exterior a la DMZ.
E. Tráfico entrante iniciado desde el exterior hacia el interior.
F. Tráfico entrante iniciado desde la DMZ hacia el interior.
G. Tráfico de retorno HTTP procedente de la red interior que regresa a través de la interfaz externa.
H. Tráfico de retorno HTTP procedente de la red interior que regresa a través de la interfaz DMZ.
I. Tráfico de retorno HTTP procedente de la red DMZ que regresa a través de la interfaz interna.
J. Tráfico de retorno HTTP procedente de la red exterior que regresa a través de la interfaz interna.

Respuesta: ABCGH

33. ¿Qué dos características representan una amenaza combinada?

A. Ataque man-in-the-middle.
B. Troyano.
C. Pharming.
D. Ataque de denegación de servicio.
E. Ataque día cero.

Respuesta: BE

34. ¿Qué afirmación describe la mejor práctica en la configuración de enlaces troncales en un puerto de switch?

A. Deshabilitar doble etiquetado, permitiendo DTP en el puerto de enlace troncal.
B. Habilitar el cifrado en el puerto de enlace troncal.
C. Habilitar la autenticación y cifrado en el puerto de enlace troncal.
D. Limitar las VLAN en el enlace troncal a la VLAN nativa solamente.
E. Configurar una VLAN no utilizada como la VLAN nativa.

Respuesta: E

35. Cuando se configura un firewall Cisco IOS de zonas basado en política, por defecto, ¿qué tres tipos de tráfico están permitidos por el router cuando algunas de las interfaces del router se asignan a una zona?

A. El tráfico enviado entre una interfaz miembro de una zona y cualquier interfaz que no es un miembro de la misma zona.
B. El tráfico enviado hacia y desde las interfaces del router (zona libre).
C. El tráfico enviado entre las interfaces que son miembros de la misma zona.
D. El tráfico enviado entre las interfaces que no están asignadas a ninguna zona.
E. El tráfico enviado entre una interfaz miembro de una zona y otra interfaz que pertenece a una zona diferente.
F. El tráfico enviado a una interfaz miembro de una zona que es tráfico de regreso.

Respuesta: BCD

36. ¿Qué opción es una característica de un firewall stateful?

- **A.** Puede analizar el tráfico en la capa de aplicación.
- **B.** Permite la modificación de las reglas de seguridad en tiempo real para permitir el tráfico de retorno.
- **C.** Permitirá la comunicación de salida, pero el tráfico de retorno se debe permitir explícitamente.
- **D.** Admite la autenticación de usuario.

Respuesta: B

37. ¿Qué tipo de política puede ser clasificada como una política VPN?

- **A.** Política de aplicación.
- **B.** Política DLP.
- **C.** Política de acceso remoto.
- **D.** Política de compromiso.
- **E.** Política WAN corporativa.

Respuesta: C

38. ¿Qué opciones representan tres ejemplos comunes de implementación AAA en los routers Cisco?

- **A.** La autenticación de usuarios remotos que acceden a la LAN corporativa a través de conexiones VPN IPsec.
- **B.** Autenticar el acceso administrativo en el puerto de consola, puerto auxiliar y puertos vty del router.
- **C.** Implementación de PKI para autenticar y autorizar IPsec VPN peers mediante certificados digitales.
- **D.** Seguimiento de estadísticas de auditorías Cisco NetFlow.
- **E.** Asegurar el router mediante el bloqueo de todos los servicios no utilizados.
- **F.** Mejoras de los comandos de autorización mediante TACACS+.

Respuesta: ABF

39. ¿Qué opción describe el propósito de Diffie-Hellman?

A. Utilizado entre el iniciador y el que responde para establecer una política de seguridad básica.
B. Utilizado para verificar la identidad del peer.
C. Utilizado para el cifrado de clave asimétrica pública.
D. Utilizado para establecer una clave simétrica compartida a través de un proceso de intercambio de clave pública.

Respuesta: D

40. ¿Qué tipo de ataque de capa 2 provoca que un switch inunde el tráfico entrante a todos los puertos?

A. Ataque de suplantación MAC.
B. Ataque de desbordamiento CAM.
C. VLAN hopping.
D. Ataque STP.

Respuesta: B

41. ¿Qué definición del protocolo Diffie-Hellman es verdadera?

A. Se utiliza el cifrado simétrico para garantizar la confidencialidad de datos a través de un canal de comunicaciones sin garantía.
B. Se utiliza el cifrado asimétrico para proporcionar autenticación a través de un canal de comunicaciones sin garantía.
C. Se utiliza en la de IKE Fase 1 para proporcionar autenticación del mismo.
D. Proporciona una forma para que dos vecinos establezcan una clave secreta compartida, que solo ellos sabrán, a pesar de que se están comunicando a través de un canal no seguro.
E. Se trata de un algoritmo de integridad de los datos que se utiliza dentro de los intercambios IKE para garantizar la integridad del mensaje de los intercambios IKE.

Respuesta: D

42. ¿Qué opción es la correcta representación de la siguiente dirección IPv6?

2001:0000:150C:0000:0000:41B1:45A3:041D

- **A.** 2001::150c::41b1:45a3:041d
- **B.** 2001:0:150c:0::41b1:45a3:04d1
- **C.** 2001:150c::41b1:45a3::41d
- **D.** 2001:0:150c::41b1:45a3:41d

Respuesta: D

43. Respecto a la siguiente sintaxis:

```
access-list 100 permit tcp 172.16.16.16 0.0.0.7 host 192.168.1.2
eq 443
access-list 100 permit tcp 172.16.16.16 0.0.0.7 host 192.168.1.2
eq 80
access-list 100 deny tcp any host 192.168.1.2 eq telnet
access-list 100 deny tcp any host 192.168.1.2 eq www
access-list 100 permit ip any any
```

¿Qué tráfico es permitido por esta lista de acceso?

- **A.** Tráfico TCP procedente de cualquier host y puerto en la subred 172.16.16.8/29 hacia el host 192.168.1.2 puerto 80 o 443.
- **B.** Tráfico TCP de origen en el host 172.16.16.21 en el puerto 80 o 443 con destino al host 192.168.1.2 en cualquier puerto.
- **C.** Cualquier tráfico TCP originado en el host 172.16.16.30 destinado al host 192.168.1.2.
- **D.** Cualquier tráfico TCP originado en el host 172.16.16.20 destinado al host 192.168.1.2.

Respuesta: D

44. ¿Cuál de las siguientes opciones sobre los algoritmos de encriptación es falsa?

A. 3DES-Symmetric.
B. AES- Symmetric.
C. DES- Symmetric.
D. 3DES- Asymmetric.
E. RCA-Asymmetric.

Respuesta: D

45. ¿Qué tipo de NAT se configura si un host en la red externa requiere el acceso a un host interno?

A. PAT.
B. NAT sobrecargado.
C. NAT dinámico.
D. NAT estático.

Respuesta: D

46. Respecto a la siguiente sintaxis:

```
Router#show run | include username
Username administrador secret 5 $1$knm.$GHKLKGDRJHI7HVMnhjHFG0
```

¿Qué indica **level 5** en el comando de configuración global **enable secret**?

A. router#enable secret level 5 password.
B. La contraseña enable secret utiliza un hash MD5.
C. La contraseña enable secret utiliza un hash SHA.
D. La contraseña enable secret está encriptada con un nivel 5 por el algoritmo propietario de Cisco.
E. La contraseña enable secret ha sido establecida con un nivel de privilegio 5.
F. La contraseña enable secret permite el acceso directamente al nivel 5 del modo EXEC.

Respuesta: E

47. ¿Cuáles de las siguientes opciones ofrece una variedad de soluciones de seguridad, incluyendo firewall, IPS, VPN, antispyware y antivirus?

A. Cisco 4200 series IPS appliance.
B. Cisco ASA 5500 series security appliance.
C. Cisco IOS router.
D. Cisco PIX 500 series security appliance.

Respuesta: B

48. ¿Cuáles son las cuatro tareas necesarias cuando se configura Cisco IOS IPS utilizando el asistente IPS Cisco Configuration Profesional?

A. Seleccione la interfaz para aplicar la regla IPS.
B. Seleccione la dirección del flujo de tráfico en que se debe aplicar la regla IPS.
C. Agregar o quitar alertas y acciones IPS basadas en la valoración del riesgo.
D. Especifique el archivo de la firma y la clave pública de Cisco.
E. Seleccione el modo de derivación IPS (fail-open o fail-close).
F. Especifique la ubicación de configuración y seleccione la categoría de firmas para ser aplicada a la interfaz seleccionada.

Respuesta: ABDF

49. ¿Qué comando AAA de auditoría se utiliza para habilitar el registro de inicio y finalización para sesiones de terminal de usuario en el router?

A. aaa accounting network start-stop tacacs+
B. aaa accounting system start-stop tacacs+
C. aaa accounting exec start-stop tacacs+
D. aaa accounting connection start-stop tacacs+
E. aaa accounting commands 15 start-stop tacacs+

Respuesta: C

50. ¿Cómo se procesan en el router las listas de control de acceso Cisco IOS?

A. ACL estándar se procesan primero.
B. La mejor concurrencia ACL se procesa primero.
C. Las entradas de ACL permitidas se procesan antes que las entradas de ACL denegadas.
D. Las ACL se procesan desde arriba hacia abajo.
E. La ACL se procesa antes que la ACL en la interfaz.

Respuesta: D

51. ¿Qué tres afirmaciones sobre la configuración de listas de control de acceso a un router Cisco son verdaderas?

A. Coloque las entradas de ACL más específicas en la parte superior de la ACL.
B. Coloque las entradas menos específicas de ACL en la parte superior de la ACL para filtrar el tráfico general y por lo tanto reducir el "ruido" en la red.
C. Una ACL siempre busca la entrada más específica antes de tomar cualquier acción filtrante.
D. Los paquetes generados por el router no se pueden filtrar con ACL en el propio router.
E. Si una lista de acceso se aplica, pero no está configurada, todo el tráfico se filtra.

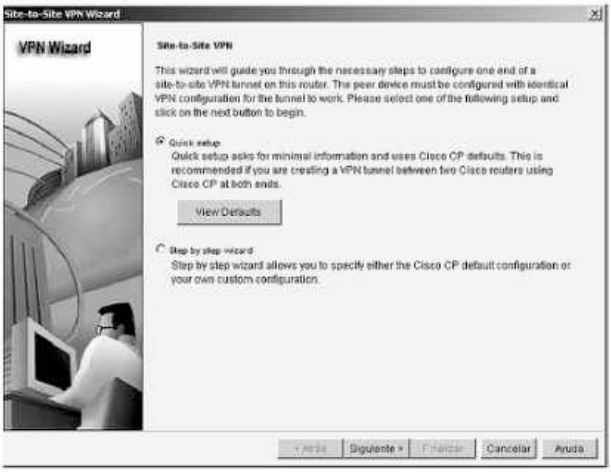
Respuesta: ADE

52. ¿Qué tipo de informe de administración está definido por la separación del tráfico de gestión y el tráfico de producción?

A. IPsec encrypted
B. in-band
C. out-of-band
D. SSH

Respuesta: C

53. Según la siguiente imagen:



Usted se encuentra configurando una VPN Site-to-Site, al tener poca experiencia ha elegido el modo **Quick setup**. ¿Qué afirmación respecto a su elección es verdadera?

A. Le ayuda en la configuración paso a paso.
B. Configura todo por defecto con las características mínimas
C. Configura todo por defecto con las mejores características.
D. La elección es incorrecta, seleccionar **Step by step wizard** es mejor.

Respuesta: A

54. ¿Qué tipo de entrada en una lista de acceso Cisco ASA se puede configurar para que coincida con múltiples entradas en una sola declaración?

A. Object-class anidados.
B. Class-map.
C. Wildcard extendida.
D. Object groups.

Respuesta: D

55. Durante la configuración de role-based CLI, ¿qué se debe activar antes de crear las vistas de usuario?

A. Múltiples niveles de privilegios.
B. Nombres de usuario y contraseñas.
C. Comando aaa new-model.
D. La contraseña para el usuario root.
E. HTTP o HTTPS Server.
F. Servidor TACACS.

Respuesta: C

56. ¿Cuáles son dos opciones de las características incorporadas en IPv6?

A. VLSM.
B. IPsec nativo.
C. Broadcast controlados.
D. IP móvil.
E. NAT.

Respuesta: BD

57. Ha sido encargado por su gerente de implementar syslog en su red. ¿Qué opción es un factor importante a considerar en la implementación?

A. Usar SSH para acceder a la información de syslog.
B. Permitir el nivel más alto disponible de la función syslog para asegurar que todos los mensajes de eventos se registran.
C. Registrar todos los mensajes en la memoria intermedia del sistema de manera que se pueden mostrar al acceder al router.
D. Sincronizar los relojes en la red con un protocolo como NTP.

Respuesta: D

58. ¿Qué afirmación acerca de deshabilitar las firmas al utilizar Cisco IOS IPS es verdadera?

A. No toman ninguna acción, pero sí producen alertas.
B. No analizan ni procesan.
C. Evitar seguir consumiendo recursos del router.
D. Ellos consideran como "retiradas" las firmas.

Respuesta: C

59. Respecto a la siguiente sintaxis:

```
Router#show run | include username
Username ernesto secret 5 $1$knm.$GHKLKGDRJHI7HVMnhjHFG0
```

¿Qué significa la opción **secret 5** en el comando de configuración global **username** acerca de la contraseña de usuario?

A. Es un hash utilizado pos SHA.
B. Es una encriptación utilizada por DH group 5.
C. Es un hash utilizado por MD5.
D. Es una encriptación generada por el comando **service password-encryption**.
E. Es un algoritmo de hash propietario de Cisco.
F. Es una encriptación utilizada por el algoritmo de hash propietario de cisco.

Respuesta: C

60. ¿Cuál es la mejor manera de prevenir un ataque VLAN hopping?

A. Encapsular puertos troncales con IEEE 802.1Q.
B. Asegurar físicamente armarios de datos.
C. Desactivar las negociaciones DTP.
D. Activar BDPU guard.

Respuesta: C

61. ¿Qué paso es importante en la aplicación de una gestión de red segura?

A. Implementar la administración in-band siempre que sea posible.
B. Implementar acceso telnet encriptado para la administración de dispositivos.
C. La implementación SNMP de lectura/escritura para solucionar problemas.
D. Sincronizar los relojes de los hosts y dispositivos.
E. Implementar la protección del plano de gestión usando protocolos de autenticación.

Respuesta: D

62. ¿Qué afirmación sobre PVLAN Edge es verdadera?

A. PVLAN Edge puede ser configurado para restringir el número de direcciones MAC que aparecen en un único puerto.
B. El switch no reenvía el tráfico de un puerto protegido a otro puerto protegido.
C. Por defecto, cuando se detecta un error en la política de puertos, los puertos del switch se deshabilitan.
D. El switch solo reenvía el tráfico a los puertos de la misma VLAN Edge.

Respuesta: B

63. ¿Cuáles son dos consideraciones importantes sobre la gestión de redes seguras?

A. Manejo de los log.
B. Fuerza en el algoritmo de cifrado.
C. Impresión exacta del tiempo horario.
D. Almacenamiento off-site.
E. Usar RADIUS para los comandos de autorización en el router.
F. No utilizar una interfaz loopback para el acceso de administración de dispositivos.

Respuesta: AC

64. ¿Qué afirmación acerca de una lista de control de acceso que se aplica a una interfaz del router es verdadera?

A. Solo se filtra el tráfico que pasa a través del router.
B. Se filtra el tráfico de paso y el generado a través del router.
C. Una denegación ACL bloquea todo el tráfico.
D. Se filtra el tráfico en las direcciones entrantes y salientes.

Respuesta: A

65. ¿Qué tres afirmaciones sobre Cisco ASA appliance son verdaderas?

A. La interfaz DMZ en el Cisco ASA típicamente utiliza un nivel de seguridad entre 1 y 99.
B. El dispositivo Cisco ASA soporta tolerancia ante fallos de estado.
C. El Cisco ASA no tiene configuraciones predeterminadas MPF.
D. El Cisco ASA utiliza contextos de seguridad virtuales particionando el ASA en múltiples firewalls virtuales.
E. El Cisco ASA soporta el control de acceso de usuario basado en 802.1x.
F. Un SSM se requiere en el aparato Cisco ASA para soportar el tráfico Botnet Filtering.

Respuesta: ABD

66. En los routers Cisco ISR, ¿cuál es el fin de la clave pública de cifrado realm-cisco.pub?

A. Se utiliza para la autenticación y encriptación SSH servidor-cliente.
B. Se utiliza para verificar la firma digital del archivo de firmas IPS.
C. Se utiliza para generar un certificado de identidad para el ISR para que los administradores puedan autenticar al ISR, al acceder mediante Cisco Configuration Professional.
D. Se utiliza para habilitar el cifrado asimétrico sobre IPsec y SSL VPN.
E. Se utiliza durante los intercambios en VPN IPsec DH.

Respuesta: B

67. ¿Qué herramienta de administración de Cisco centraliza todos los aspectos de configuración y provisión del dispositivo a través de la familia de productos de seguridad de Cisco?

A. Cisco Configuration Professional.
B. Security Device Manager.
C. Cisco Security Manager.
D. Cisco Secure Management Server.

Respuesta: C

68. ¿Cuál es el propósito del navegador web SSL VPN en el Cisco ASA appliance?

A. Permitir la división del túnel cuando se utiliza clientless SSL VPN.
B. Que los usuarios puedan acceder a un portal web para descargar y ejecutar el cliente AnyConnect.
C. Permitir el acceso del túnel a las aplicaciones que no están basadas en Web.
D. Optimizar las conexiones VPN SSL utilizando DTLS
E. Permitir inicio de sesión único en lo que los usuarios de VPN SSL solo necesitan iniciar sesión una vez.

Respuesta: B

69. Si va a implementar VLAN trunking, ¿qué parámetro de configuración adicional se debe agregar a la configuración del enlace troncal?

A. no switchport mode access
B. no switchport trunk native VLAN 1
C. switchport mode DTP
D. switchport nonnegotiate

Respuesta: D

70. Cuando se configura un firewall Cisco IOS de zonas basado en política, ¿qué tres acciones se pueden aplicar a una clase de tráfico?

A. pass
B. police
C. inspect
D. drop
E. queue
F. shape

Respuesta: ACD

71. ¿Qué dos protocolos habilita Cisco Configuration Professional para enviar alertas IPS desde un router Cisco ISR?

A. syslog
B. SDEE
C. FTP
D. TFTP
E. SSH
F. HTTPS

Respuesta: BF

72. ¿Qué dos funciones son requeridas para la operación IPsec?

A. Utilizar SHA para el cifrado.
B. Utilizar PKI para la preautenticación de clave compartida.
C. Utilizar IKE para negociar la SA.
D. Utilizar protocolos AH para el cifrado y la autenticación.
E. Utilizar Diffie-Hellman para establecer una clave secreta compartida.

Respuesta: CE

73. Según la siguiente sintaxis:

```
Current configuration : 156 bytes
!
interface FastEthernet0/0
ip address 192.168.32.13 255.255.255.0
ip access-group IOS in
ip flow ingress
ip flow egress
duplex auto
speed auto
!
End

Router(config-ext-nacl)#do show access-list IOS
Extended IP access list IOS

 10 permit tcp host 10.1.1.1 ep 1030 host 192.168.15.80 eq telnet
 20 permit tcp host 10.1.1.1 ep 1030 host 192.168.15.66 eq 8080
 30 permit tcp host 10.1.1.1 ep 1030 host 192.168.15.36 eq www
 40 permit tcp host 10.1.1.1 ep 1030 host 192.168.15.63 eq www

Router(config-ext-nacl)#exit
Router(config)#
```

Esta lista de acceso Cisco IOS ha sido configurada en la interfaz Fa0/0 en dirección entrante.

¿Cuáles son los cuatro paquetes TCP de origen de 10.1.1.1 puerto 1030 y enviados a la interfaz Fa0/0 que se permiten?

A. Dirección IP de destino: 192.168.15.37 puerto de destino: 22.
B. Dirección IP de destino: 192.168.15.80 puerto de destino: 23.
C. Dirección IP de destino: 192.168.15.66 puerto de destino: 8080.
D. Dirección IP de destino: 192.168.15.36 puerto de destino: 80.
E. Dirección IP de destino: 192.168.15.63 puerto de destino: 80.
F. Dirección IP de destino: 192.168.15.40 puerto de destino: 21.

Respuesta: BCDE

74. ¿Qué afirmación es una ventaja de la utilización de Cisco IOS IPS?

- **A.** Se utiliza la infraestructura de enrutamiento subyacente para proporcionar una capa adicional de seguridad.
- **B.** Funciona en modo pasivo a fin de no afectar el flujo de tráfico.
- **C.** Es compatible con la base de firmas como un sensor Cisco IPS.
- **D.** La base de firmas está estrechamente relacionada con la imagen de Cisco IOS.

Respuesta: A

75. ¿Qué afirmación describe cómo el tráfico VPN es cifrado para garantizar la confidencialidad cuando se utiliza el cifrado asimétrico?

- **A.** El remitente cifra los datos utilizando la clave privada del remitente y el receptor descifra los datos usando la clave pública del remitente.
- **B.** El remitente cifra los datos utilizando la clave pública del remitente, y el receptor descifra los datos usando la clave privada del remitente.
- **C.** El remitente cifra los datos utilizando la clave pública del remitente, y el receptor descifra los datos usando la clave pública del receptor.
- **D.** El remitente cifra los datos utilizando la clave privada del receptor, y el receptor descifra los datos usando la clave pública del receptor.
- **E.** El remitente cifra los datos utilizando la clave pública del receptor, y el receptor descifra los datos usando la clave privada del receptor.
- **F.** El remitente cifra los datos utilizando la clave privada del receptor, y el receptor descifra los datos usando la clave pública del remitente.

Respuesta: E

76. ¿Qué protocolo asegura el tráfico de una sesión de administración en un router?

- **A.** SSTP
- **B.** POP
- **C.** Telnet
- **D.** SSH

Respuesta: D

77. Al configurar SSL VPN en el dispositivo Cisco ASA, ¿qué paso de configuración se requiere solo para un túnel de acceso completo SSL VPN Cisco AnyConnect y no se requiere para clientless SSL VPN?

A. Autenticación de usuario.
B. Grupo de políticas.
C. Conjunto de direcciones IP.
D. Interfaz SSL VPN.
E. Perfil de conexión.

Respuesta: C

78. ¿Cuáles son cuatro tipos de VPN compatibles con Cisco ISR y Cisco ASA appliances?

A. SSL clientless remote-access VPN.
B. SSL full-tunnel client remote-access VPN.
C. SSL site-to-site VPN.
D. IPsec site-to-site VPN.
E. IPsec client remote-access VPN.
F. IPsec clientless remote-access VPN.

Respuesta: ABDE

79. ¿Qué ubicación es recomendable para las ACL extendidas nombradas o numeradas?

A. Una ubicación intermedia para filtrar el tráfico tanto como sea posible.
B. Una ubicación tan cerca del destino del tráfico como sea posible.
C. Cuando se utiliza la palabra clave "established", un lugar cercano al destino para asegurarse de que el tráfico de retorno se permita.
D. Una ubicación tan cerca del origen del tráfico como sea posible.

Respuesta: D

80. ¿Qué afirmación acerca de los algoritmos de cifrado asimétrico es verdadera?

A. Se utiliza la misma clave para el cifrado y descifrado de datos.
B. Se utiliza la misma clave para descifrar pero diferentes claves para el cifrado de datos.
C. Se utilizan diferentes claves para el cifrado y descifrado de datos.
D. Se utilizan claves distintas para el descifrado pero la misma clave para el cifrado de datos.

Respuesta: C

81. ¿Qué opción puede ser utilizada para autenticar vecinos IPsec durante IKE fase 1?

A. Diffie-Hellman
B. pre-shared key
C. XAUTH
D. integrity check value
E. ACS
F. AH

Respuesta: A

82. ¿Qué entrada de una ACL Cisco IOS permite el rango IP desde 172.16.80.0 a 172.16.87.255?

A. permit 172.16.80.0 0.0.3.255
B. permit 172.16.80.0 0.0.7.255
C. permit 172.16.80.0 0.0.248.255
D. permit 176.16.80.0 255.255.252.0
E. permit 172.16.80.0 255.255.248.0
F. permit 172.16.80.0 255.255.240.0

Respuesta: B

83. Desea utilizar el asistente site-to-site VPN de Cisco Configuration Professional para implementar site-to-site VPN IPsec mediante la clave pre-shared. ¿Cuáles son las cuatro configuraciones que no sean por defecto que se requieren?

A. La interfaz para la conexión VPN.
B. La dirección IP del vecino VPN.
C. El IPsec transform-set.
D. La política IKE.
E. El tráfico interesante (a proteger).
F. La clave pre-shared.

Respuesta: ABEF

84. ¿Qué nivel de syslog se asocia con el mensaje LOG_WARNING?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6

Respuesta: D

85. ¿Qué medidas de seguridad debe tomar para la VLAN nativa en un puerto troncal?

A. La VLAN nativa para los puertos troncales nunca debe ser usada en otro lugar en el switch.
B. La VLAN nativa para los puertos de enlace troncal debe ser la VLAN 1.
C. La VLAN nativa para los puertos troncales debe coincidir con la VLAN de acceso para garantizar que el tráfico transversal de múltiples switches pueda ser entregado a los switches físicamente dispares.
D. La VLAN nativa para los puertos troncales debe estar etiquetada con 802.1Q.

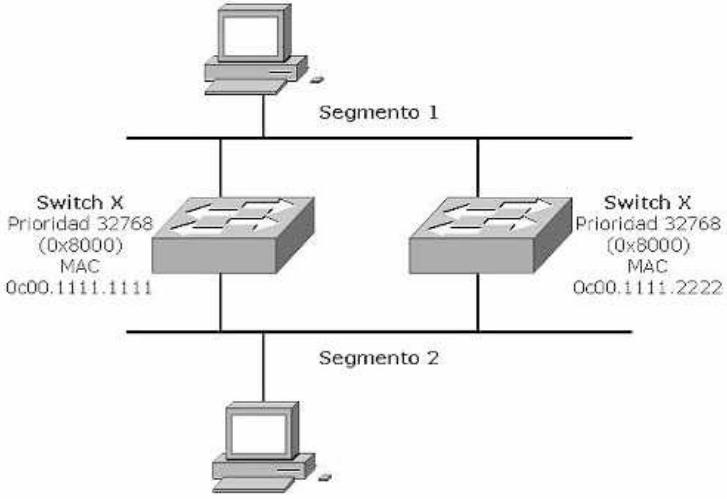
Respuesta: A

86. ¿En qué tipo de ataque de capa 2 un atacante transmite broadcast BDPU con una prioridad menor que la del switch?

A. Ataque por inundación MAC.
B. Desbordamiento de CAM.
C. Ataque VLAN hopping.
D. Ataque STP.

Respuesta: D

87. Respecto al siguiente gráfico:



¿Cuál de los switches será designado como el root bridge en esta topología?

A. Depende de qué switch se conectó primero.
B. Ningún switch asumiría el papel de root bridge, porque tienen la misma prioridad por defecto.
C. Switch X.
D. Switch Y.

Respuesta: C

88. ¿Qué tipo de tecnología de firewall se considera como una tecnología de firewall versátil y de uso común?

A. Firewall de filtrado estático.
B. Firewall de capa de aplicación.
C. Firewall stateful.
D. Proxy firewall.
E. Firewall de capa adaptable.

Respuesta: C

89. ¿Cuáles son dos servicios proporcionados por IPsec?

A. Confidencialidad.
B. Carga útil encapsulada.
C. Integridad de los datos.
D. Encabezado de autenticación.
E. Internet Key Exchange.

Respuesta: AC

90. ¿Cuáles son dos servicios proporcionados por IPsec? Cuando port security está habilitado en un switch Cisco Catalyst, ¿cuál es la acción por defecto cuando el número máximo de direcciones MAC permitidas es excedido?

A. El puerto permanece activado, pero el ancho de banda es reducido hasta que las antiguas direcciones MAC caduquen.
B. El puerto se deshabilita.
C. La tabla de direcciones MAC se borra y la nueva dirección MAC se introduce en la tabla.
D. El modo de violación del puerto está configurado para restringir tráfico.

Respuesta: B

91. Respecto a la siguiente sintaxis:

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using
source 10.116.0.79

14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to
192.168.60.15 (AUTHEN/START)

14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from
192.168.60.15

14:00:09: TAC+ (383258052): received authen response status =
GETUSER

14:00:10: TAC+: send AUTHEN/CONT packet

14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to
192.168.60.15 (AUTHEN/CONT)

14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from
192.168.60.15

14:00:10: TAC+ (383258052): received authen response status =
GETPASS

14:00:14: TAC+: send AUTHEN/CONT packet

14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to
192.168.60.15 (AUTHEN/CONT)

14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from
192.168.60.15

14:00:14: TAC+ (383258052): received authen response status = PASS

14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

¿Qué afirmación acerca del comando **debug** es verdadera?

- **A.** La solicitud de autenticación solicitada proviene del nombre de usuario GETUSER.
- **B.** La petición de autenticación TACACS+ proviene de un usuario válido.
- **C.** La solicitud de autenticación TACACS+ ha validado, pero por alguna razón la conexión del usuario se cerrará inmediatamente.
- **D.** La solicitud de conexión se estaba iniciando suplantada por una dirección de origen diferente.

Respuesta: B

92. ¿Qué afirmación representa mejor las características de una VLAN?

A. Los puertos en una VLAN no comparten broadcasts entre switches físicamente separados.
B. Una VLAN solo se puede conectar a través de una red LAN en el mismo edificio.
C. Una VLAN es un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos.
D. Una VLAN proporciona seguridad de puertos individual.

Respuesta: C

93. ¿Qué prioridad es más importante cuando usted planea crear listas de control de acceso?

A. Construir la ACL en base a su política de seguridad.
B. Siempre coloque la ACL más cercana a la fuente de origen.
C. Colocar las declaraciones de denegación en la parte superior de la ACL para evitar que el tráfico no deseado pase a través del router.
D. Se deben comprobar siempre las ACL en un entorno pequeño antes que en la red de producción.

Respuesta: A

94. ¿Qué tipo de tecnología de prevención de intrusiones es el principal tipo usado por los dispositivos de Cisco IPS de seguridad?

A. Basado en perfil.
B. Basado en reglas.
C. Basado en protocolos.
D. Basado en firmas.
E. Basado en NetFlow.

Respuesta: D

95. ¿Qué dos afirmaciones son ciertas acerca de las diferencias entre IDS e IPS?

A. IPS funciona en modo promiscuo.
B. IPS recibe una copia del tráfico a analizar.
C. IPS funciona en el modo en línea.
D. IDS recibe una copia del tráfico a analizar.

Respuesta: CD

96. Qué opción es una característica del protocolo RADIUS?

A. Utiliza TCP.
B. Ofrece soporte multiprotocolo.
C. Combina autenticación y autorización en un solo proceso.
D. Soporta el desafío bidireccional.

Respuesta: C

97. ¿Qué tipo de lista de control de acceso Cisco IOS se identifica por el rango 2.000 a 2.699?

A. Estándar.
B. Extendido.
C. Nombrado.
D. IPv4 para 100 a 199 e IPv6 para 2.000 a 2.699.

Respuesta: B

98. ¿Cuál de las siguientes afirmaciones es verdadera respecto al plano de administración?

A. Asegura el acceso al router.
B. Asegura el tráfico que pasa a través del router.
C. Asegura el tráfico que esta destinado al router.
D. Es responsable del enrutamiento del tráfico.

Respuesta: A

99. ¿Qué tres afirmaciones acerca de los modos de funcionamiento de IPsec ESP son verdaderas?

A. El modo túnel se utiliza entre un host y un firewall.
B. El modo túnel se utiliza entre dos firewall.
C. El modo túnel solo encripta y autentica los datos.
D. El modo transporte autentica la cabecera IP.
E. En el modo transporte la cabecera IP original está expuesta.

Respuesta: ABE

100. ¿Cuál de las siguientes opciones determina que se dispare una alarma falso positivo?

A. Se activa una alarma por el tráfico normal o una acción benigna.
B. La firma no se activa cuando se detecta tráfico ofensivo.
C. Genera una alarma cuando se detecta tráfico ofensivo.
D. Una firma no se dispara cuando el tráfico capturado y analizado no es ofensivo.

Respuesta: A

ÍNDICE ALFABÉTICO

SÍMBOLOS

3DES 313

A

AAA 101
  auditoría 104
  autenticación 103
  autorización 103
  configuración 104
  modos de acceso 102
  Radius 109
  Tacacs+ 109
Access Control Server 111
Accounting 102
ACL 159
  basadas en tiempo 180
  condiciones 160
  de entrada 163
  de salida 163
  dinámicas 178
  estándar 166
  extendida 167
  IPv6 184
  mitigación de ataques 161
  nombradas 169
  numeradas 165
  object group 185
  reflexivas 175
  tipos 161
  ubicación 162
  verificación 182
Adaptive Security Appliance 228
AES 313
AH 313
AnyConnect 267
ASA
  AAA 261
  AnyConnect 267
  ASDM 232
  características 231
  filtrado de paquetes 251
  funcionalidad 228
  modos 229
  MPF 264
  NAT y PAT 255
  object groups 245
  VPN 266
ASDM 232, 238
Ataques
  de acceso 38
  de capa 2 140
  de denegación de servicio 38
  de DoS 25
  de falsificación 25
  de paquetes SYN TCP 39
  de reconocimiento 37
  mitigación 39
Auditorías 89
Authentication 102
Authorization 102

B

Banners....57
BPDU Filter....150
BPDU Guard....149

C

CBAC....197
CCP....63
CDP....89
CERT....29
Cisco AutoSecure....42, 94
Cisco Configuration Professional....63
Cisco Easy VPN....342
Cisco Secure ACS....111
Cisco SecureX....32
Confidencialidad....26
Contraseña
de auxiliar....53
de consola....53
de telnet....53
modo EXEC....52
recuperación....73
Control de tormentas....147
CoPP....42
CPPr....43
Criptografía....26
Crypto ACL....325
Crypto Map....325

D

Defensa
de un solo router....47
DMZ....48
modelos....47
profunda....48
DES....313
Disponibilidad....26
de datos....27
DMZ....195
Dominios de seguridad....30
DTP....151

E

Encriptación asimétrica....318
Encriptación simétrica....317
Enlace troncal....151
ESP....312
Establisehed....167

F

Firewall
ASA....228
basado en zonas....207
características....192
diseño de redes....195
stateful....193
tipos....193

G

GRE
configuración....307
túneles....306

H

Hacking....27

I

IDS
características....277
IKE....312, 314
fases....315
modos....315
protocolos....315
Integridad....26
de datos....26
IPS
acciones....286
administración....287
alarmas....283
configuración....288
firmas....282
implementación....Véase IPsec
autenticación....314
cabeceras....312
características....309
configuración con CCP....330
introducción....309
modos....311
protocolos....312
Transform sets....322
verificación....328
IPv6, características....354
IPv6, formato....355

IPv6, introducción 353
IPv6, tipos 356
IronPort 138
ISAKMP 315, 322
ISC² 29

L

Lan Virtuales 151
Listas de acceso 159
lock-and-key 178

M

MPF 264

N

NAC 139
NAT
  bidirectional 256
  inside 255
  outside 256
NFP 41
NTP 85

O

Oakley 315
Object group 185
One-step lockdown 97

P

PKI 319
Plano
  de control 42
  de datos 42
Políticas de seguridad 32
Private VLAN Edge 155
PVLAN 153

R

RADIUS 109
RBAC 43
Resguardo
  de configuración 70
  de IOS 70
Roles y privilegios 64
Rommon 73
Root Guard 150
RSA 319
RSPAN 156

S

SANS 29
SNMP 77, 82
SPAN 156
SSH 58
STP
  PortFast 149
  protección 149
Syslog 78

T

TACACS+ 109
Transform sets 322
Trunking 151

U

uRPF 44

V

VACL 152
VLAN hopping 151
VPN
  acceso remoto 339
  Cisco Easy 342
  introducción 305
  site-to-site 320
  SSL 339
Vulnerabilidades
  gusanos 34
  mitigación 36
  troyanos 35
  virus 34

Z

ZPF 207

REDES CISCO

Guía de estudio para la certificación CCNA Security

La certificación **CCNA Security** (*Cisco Certified Network Associate Security*) valida los conocimientos y prácticas para asegurar las redes de Cisco. Con la certificación CCNA Security se obtienen las habilidades necesarias para desarrollar una infraestructura de seguridad, reconocer las amenazas y vulnerabilidades en las redes y mitigar las amenazas de seguridad. Siguiendo estos conceptos, esta guía de estudio fue diseñada para preparar el examen **640-554 IINS** (*Implementing Cisco IOS Network Security*) para la obtención de la certificación CCNA Security.

Este libro abarca temas como la instalación, la configuración, monitorización y mantenimiento de los dispositivos **Cisco IOS Firewall** y **ASA** (*Adaptive Security Appliances*) utilizando la interfaz de línea de comandos (CLI) y los administradores de dispositivos web como **CCP** (*Cisco Configuration Professional*) y **ASDM** (*Adaptive Security Device Manager*). El temario está basado en el *blueprint* de Cisco para este examen y cubre temas como:

- Configurar la conversión de direcciones de red, listas de acceso, la inspección dinámica del tráfico y el filtrado de aplicaciones.
- Implementar la detección de intrusiones basándose en la firma.
- Configurar la administración de la identidad utilizando AAA.
- Configurar redes privadas virtuales mediante IPsec para la conectividad sitio a sitio y de acceso remoto.

Como en toda la serie de libros Redes Cisco, esta guía fue creada para ser amigable con el lector, dejando de lado lo innecesario y centrándose fundamentalmente en el examen de certificación. Contiene ejemplos de configuraciones y capturas de dispositivos reales, notas aclaratorias y recomendaciones para el examen. También está destinada para quien quiera aprender sobre la seguridad en las redes y los procesos globales de seguridad.

Otros títulos de esta serie:

Redes CISCO. Guía de estudio para la certificación CCNA 640-802. Ariganello, E.
482 páginas. ISBN: 9788499640945

Redes CISCO. Guía de estudio para la certificación CCNP. Ariganello, E. y Barrientos, E.
718 páginas. ISBN: 9788499640358

Redes CISCO. CCNP a Fondo. Guía de estudio para profesionales. Ariganello, E. y Barrientos, E.
922 páginas. ISBN: 9788478979660

Técnicas de configuración de Routers CISCO. Ariganello, E.
276 páginas. ISBN: 9788478978489

9 788499 642147

Ra-Ma®

ra-ma.es