Capítulo 1

Riesgos de Seguridad en Redes Modernas

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#1

1.0 Introducción

- La Seguridad de Redes
  - Involucra:
    - Protocolos, Tecnologías, Dispositivos, Herramientas, Técnicas
  - Consiste en prevenir futuros ataques al minimizar efectos de ataques reales.
  - Complejidad alta
    - Subdivisión en diferentes dominios de especialización.
  - Políticas de Seguridad enmarcan rangos de acción de los empleados en una organización.
  - Los ataques de red se clasifican para atacarlos adecuadamente en:
    - Virus, gusanos, caballos de troya, etc.
  - De manera general se clasifican como: ataques de reconocimiento, acceso, o denegación de servicio (DoS).

1.1 Aseguramiento de Redes

- Las Redes son Objetivos.
  - Los ataques a las redes son comunes.
  - Norse Dark Intelligence muestra ataques a servidores HoneySpot.
    - Estudian mecanismos sobre como los hackers buscan comprometer los sistemas.

1.1 Aseguramiento de Redes

- Razones para Asegurar Redes:
  - Las violaciones de la seguridad de la red pueden causar:
    - Pérdida de datos
    - Poner en peligro la privacidad
    - poner en peligro la integridad de la información.
    - Pérdida de ingresos
    - Robo de propiedad intelectual,
    - Litigios,
    - Poner en peligro la seguridad pública.
  - Necesario vigilar constantemente evolución de los riesgos de seguridad.
    - Cisco Security Intelligence Operations (SIO) Provee:
      - Alertas sobre posibles ataques.
      - Objetivo:
        - Identificar y detener posibles ataques

1.1 Aseguramiento de Redes

- Términos utilizados en alertas sobre seguridad de redes:

Vulnerabilidad: Debilidad en la red que puede ser utilizada para causar impactos negativos. (Configuraciones débiles o inseguras)

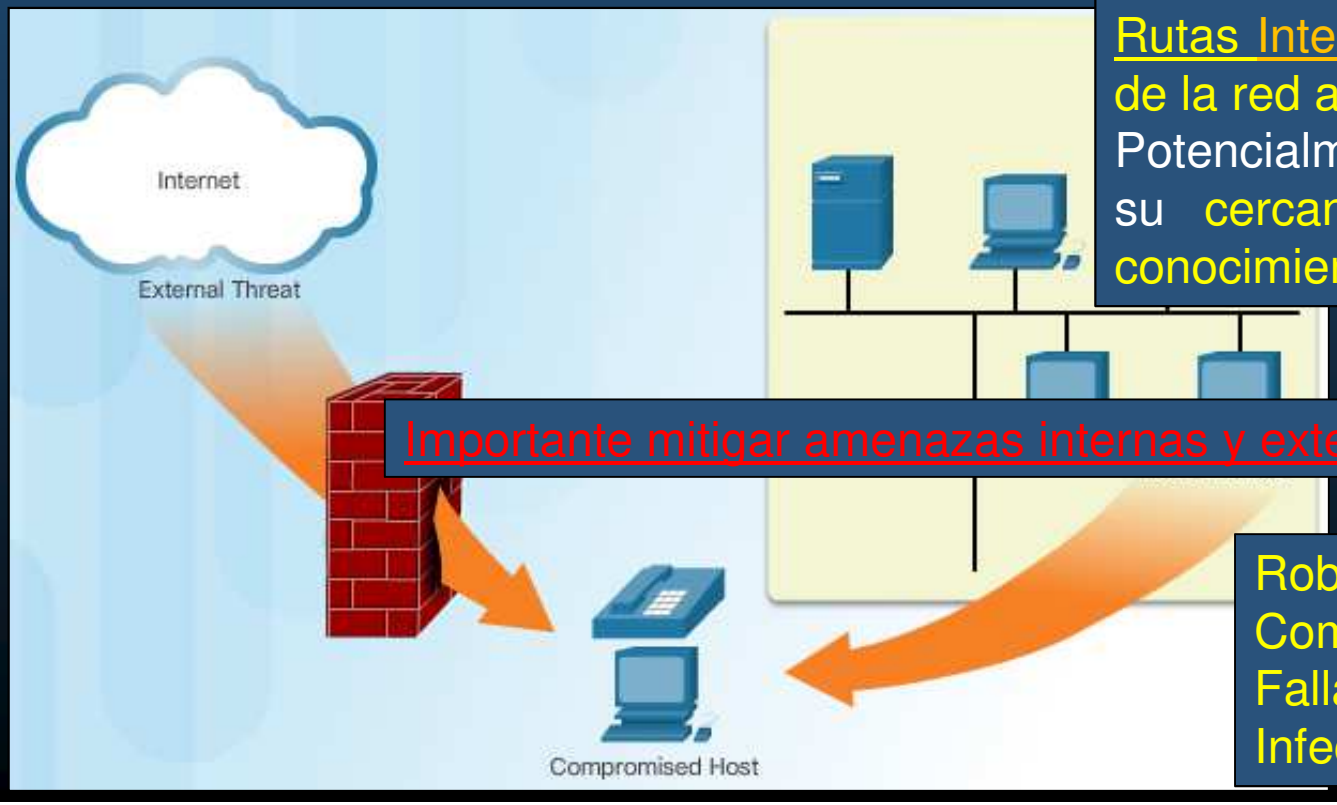
Amenaza: Vulnerabilidad potencial que puede explotarse. (Malware, Exploits, y mas)

Riezgo: Potencial de una Amenaza potencial para explotarse de forma negativa. (Probabilidad de que un ataque ocurra)

Mitigación: Acción de reducir la severidad de una vulnerabilidad.

1.1 Aseguramiento de Redes

- Vectores de Ataques de Red:
  - Ruta por la que se gana acceso a un objetivo de ataque.
    - Objetivos comunes: Servidor, Host, Red, etc…
    - Ataque común: DoS (Incapacidad de Atender solicitudes legítimas)



Rutas Internas: Se generan dentro de la red atacada.
Potencialmente mas dañinas por su cercanía a infraestructura y conocimiento de la empresa.

Importante mitigar amenazas internas y externas.

Robo de información.
Comprometer dispositivos.
Fallas de red.
Infección de equipos de red.

1.1 Aseguramiento de Redes

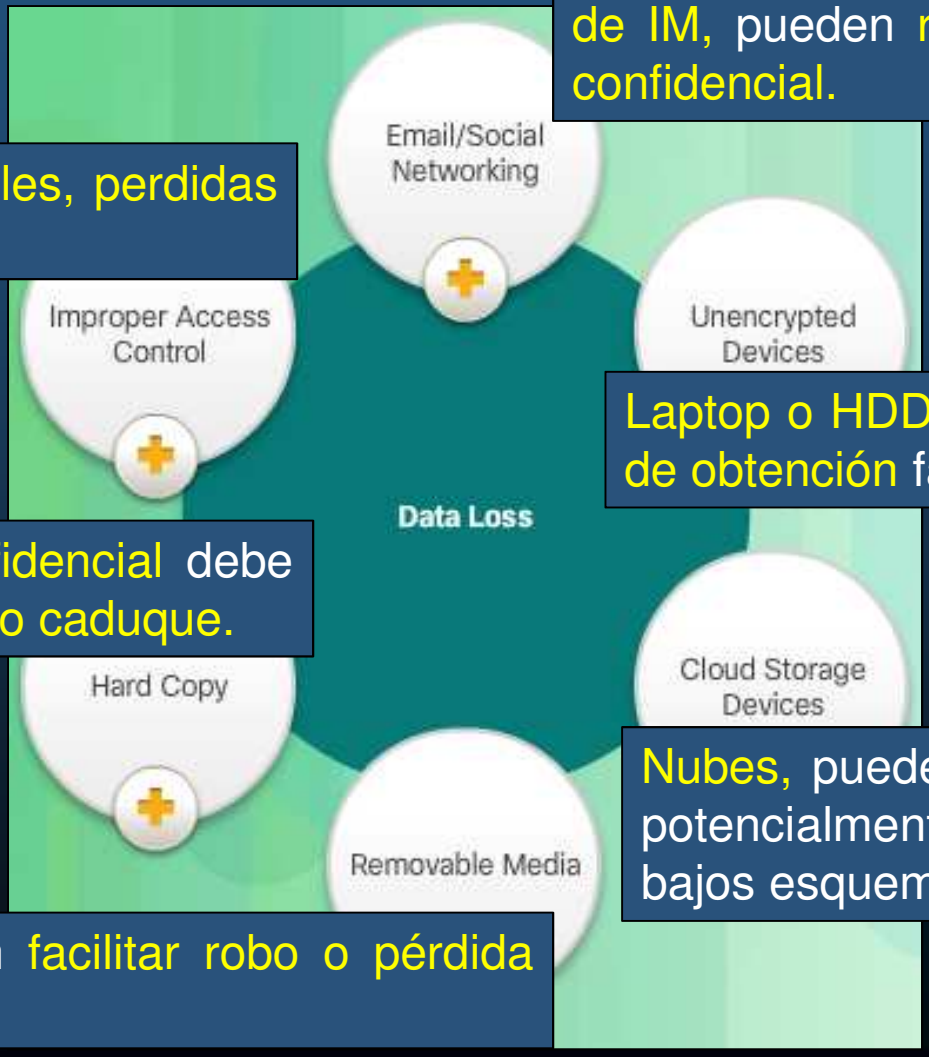
- Perdida de Datos (Exfiltración de datos):
  - Datos valiosos
    - Investigación, desarrollo, ventas, finanzas, recursos humanos y legales, empleados, contratos, clientes.
  - Da como resultado:
    - Pérdida de reputación
    - Pérdida de competitividad
    - Pérdida de clientes
    - Pérdida de ingresos
    - Acciones legales
    - Costos notificaciones a los afectados y recuperarse de incumplimientos
  - Imprescindible implementar “Data Loss Prevention (DLP)”

1.1 Aseguramiento de Redes

- Vectores de Perdida de Datos:

Intercepción de emails o mensajes de IM, pueden revelar información confidencial.

Contraseñas débiles, perdidas o comprometidas.



Laptop o HDD robados, son fuente de obtención fácil de información.

La información confidencial debe ser destruida, cuando caduque.

Nubes, pueden ser prácticas, pero potencialmente riesgosas ante bajos esquemas de seguridad.

Drives USB, pueden facilitar robo o pérdida de información.

1.1 Aseguramiento de Redes

- Redes de Área de Campus (CAN):
  - LANs Interconectadas delimitadas por un área geográfica.
  - Diferentes técnicas para asegurar ame

Servidor Authentication, Authorization, & Accounting (AAA): Autentica, Autoriza (matriz de permisos), Registra Actividades de Cuentas.

Adaptive Security Appliance (ASA): Realiza filtrado de tráfico de retorno a la red.

VPN: integrida extremos.

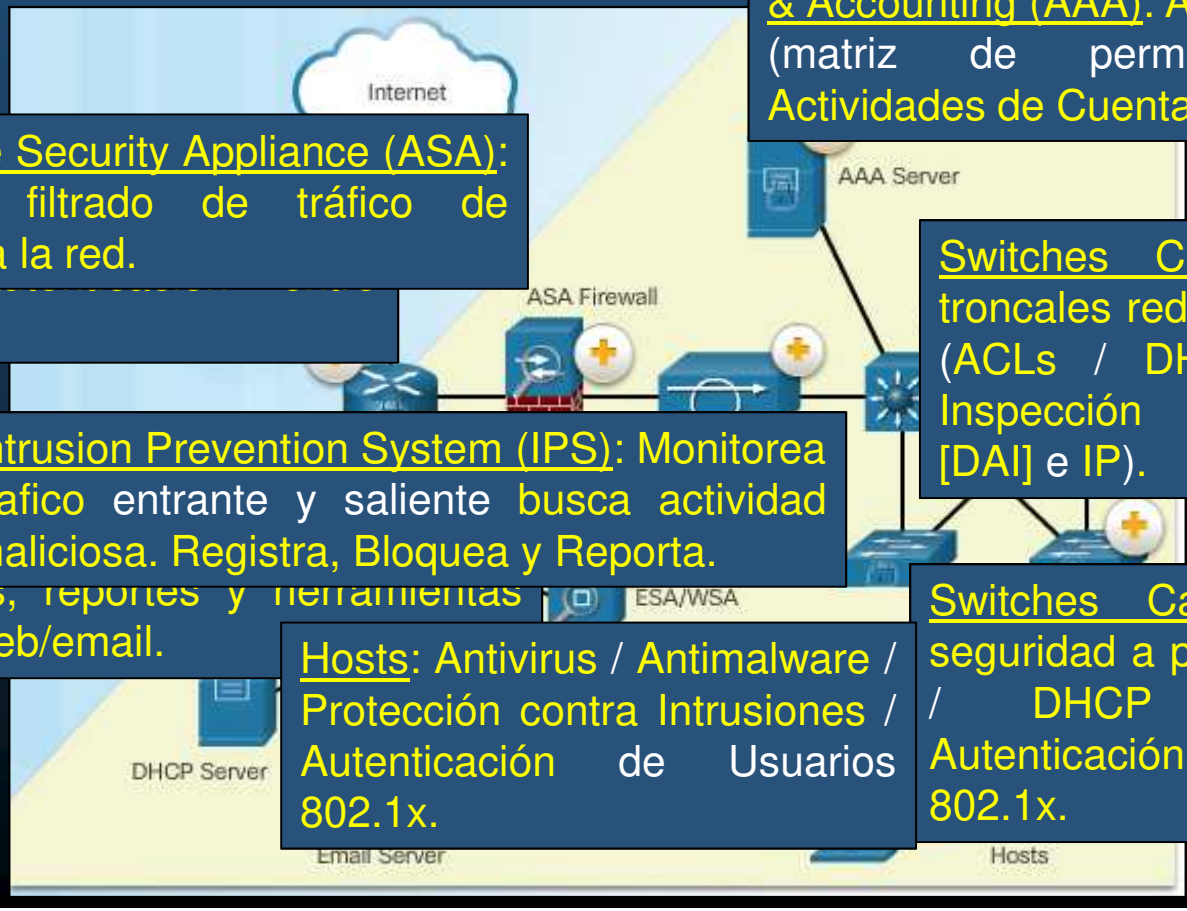
Switches Capa 3: Brindan troncales redundantes seguros (ACLs / DHCP Snooping / Inspección ARP Dinámica [DAI] e IP).

Intrusion Prevention System (IPS): Monitorea trafico entrante y saliente busca actividad maliciosa. Registra, Bloquea y Reporta.

Email Security Appliance (ES contra amenazas, reportes y herramientas de control para web/email.

Switches Capa 2: Brindan seguridad a puertos de acceso / DHCP Snooping / Autenticación de Usuarios 802.1x.

Hosts: Antivirus / Antimalware / Protección contra Intrusiones / Autenticación de Usuarios 802.1x.



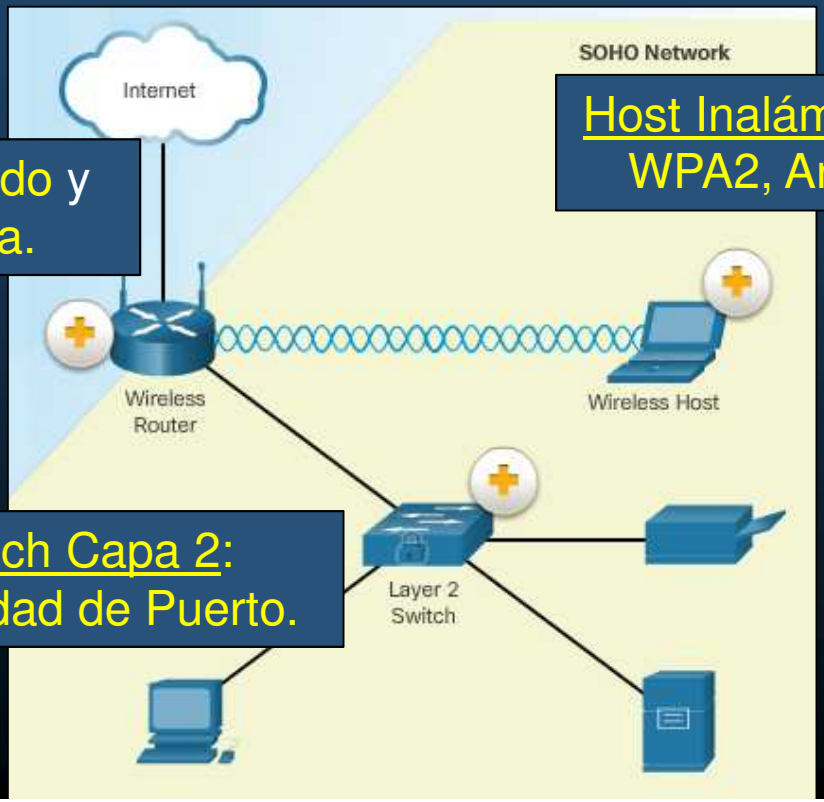
1.1 Aseguramiento de Redes

- Redes Small Office and Home Office (SOHO):
  - Amenazas comunes:
    - Búsqueda de internet gratis.
    - Uso de internet para fines ilegales.
    - Típicamente protegidas con dispositivos de grado de consumidor.

Todas las redes sin importar el tipo, deben asegurarse

Router: Firewall Integrado y seguridad inalámbrica.

Host Inalámbrico con: Conexiones WPA2, Antivirus, Antimalware.



Switch Capa 2: Seguridad de Puerto.

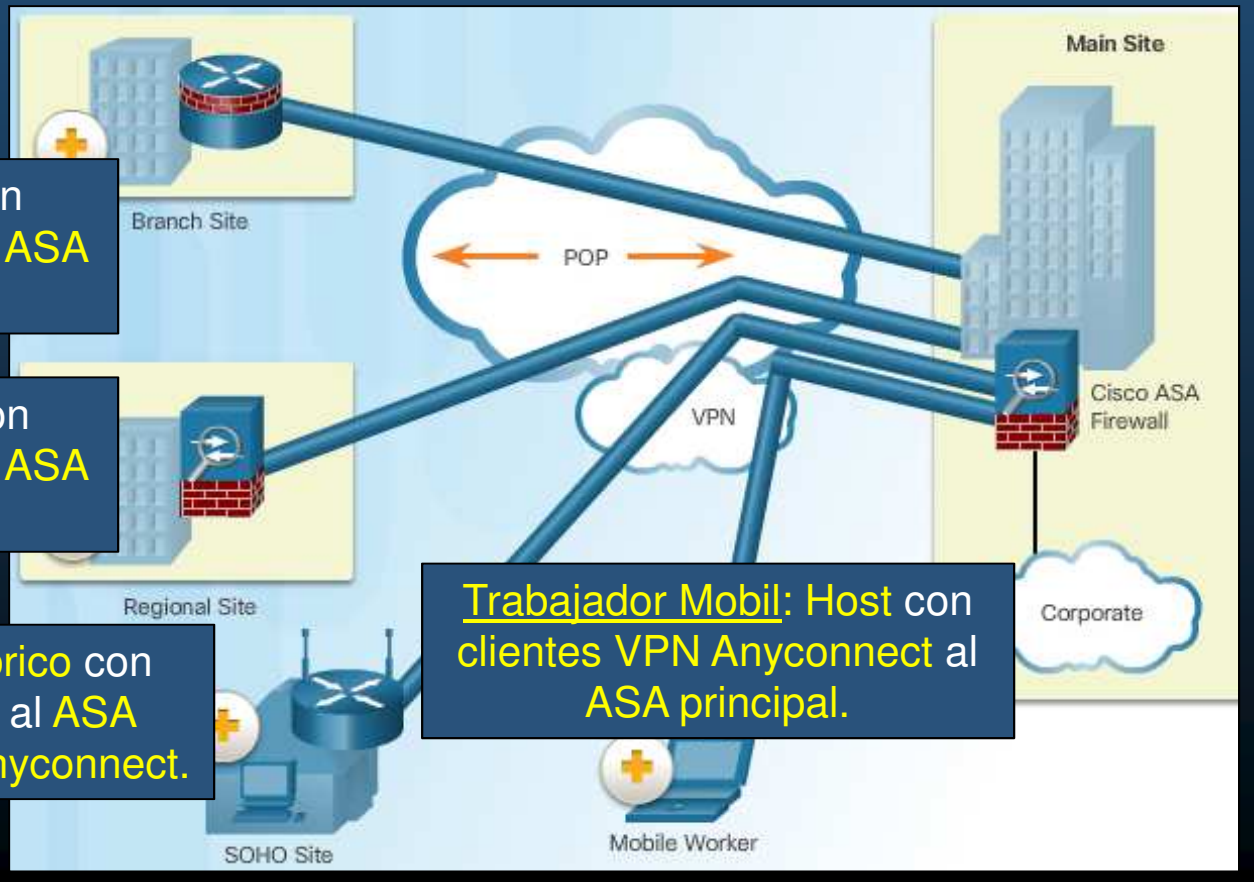
1.1 Aseguramiento de Redes

- Redes de Área Amplia (WAN):
  - Asegurar transporte de datos entre sitios.
    - Dispositivos en los extremos.
    - Uso de ASA y VPNs.

Sucursal Local: Router ISR con Conexiones VPN permanentes al ASA principal.

Rama Regional: Router ISR con Conexiones VPN permanentes al ASA principal.

Rama Regional: Router Inalámbrico con Conexiones VPN permanentes al ASA principal ó uso de clientes VPN Anyconnect.



Trabajador Mobil: Host con clientes VPN Anyconnect al ASA principal.

1.1 Aseguramiento de Redes

- Redes de Centros de Datos:
  - Usualmente localizados en instalaciones diferentes al sitio.
    - Dispositivos en los extremos.
    - Uso de ASA, VPNs, Switches de centro de datos integrados.
  - Almacenan información critica y sensible.
    - Requieren seguridad física para proteger a las personas y equipos.
      - Alarmas contra incendio,
      - Rociadores,
      - Bastidores de servidor arriostrados sísmicamente
      - Calefacción redundante,
      - Ventilación
      - Aire acondicionado (HVAC)
      - Sistemas UPS
    - Perímetro exterior: agentes de seguridad, cercas, puertas, video vigilancia y alarmas.
    - Perímetro interior: video vigilancia, detectores de movimiento, equipos de trampas de seguridad y sensores biométricos de acceso y salida.

1.1 Aseguramiento de Redes

- Redes de Centros de Datos:

1.1 Aseguramiento de Redes

- Redes Virtuales y de Nube:
  - Almacenamiento/Cómputo en la nube, extiende capacidades sin añadir infraestructura.
    - Fuera del perímetro de la red.
  - Nube separa aplicaciones del hardware.
  - Virtualización separa S.O. del hardware.
  - Red de Nube: Servidores físicos y virtuales para centros de datos.
  - Virtualización es susceptible a ataques:
    - Secuestro de Hypervisores.
    - Vulnerabilidades en software desactualizado en VMs.
    - Tormentas de actualización de antivirus al mismo tiempo (VMs).

1.1 Aseguramiento de Redes

- Redes Virtuales y de Nube:
  - Cisco Secure Data Center.

ASA y Cisco Security Gateway (Switching Capa 3): Seguridad Inter-VM granular.

Software Cisco Security Manager : Seguridad Inter-VM granular.

ASA e IPS: Inteligencia de amenazas, genera huellas de S.O. reputación y análisis contra amenazas.

1.1 Aseguramiento de Redes

- Frontera de Red en Evolución:
  - Actualmente dispositivos móviles sustituyen PCs al acceder información empresarial (BYOD).
    - Cisco define esquema de Red Sin Fronteras.
      - Mobile Device Management (MDM) para dispositivos de la empresa y de los empleados. (Desktop, Laps, Tablets, Handhelds)
        - Asegura
        - Monitorea
        - Administra

Encripta datos: Solo dispositivos encriptados acceden empresa.

Solicitud de PIN: o contraseñas para que dispositivos accedan empresa.

Limpieza de Datos: de manera remota, para dispositivos robados.

Prevención de Pérdida de Datos: Evita que usuarios válidos hagan uso descuidado de los datos.

Detección de Jailbreak/Root: Evita que dispositivos no administrados tengan acceso a la empresa.

1.2 Amenazas de Red

- El Hacker:
  - Programador inteligente capaz de crear nuevos programas o mejorar los existentes.
  - Profesional de redes con capacidades de programación para probar seguridad de redes.
  - Persona que intenta ganar acceso no autorizado a dispositivos o internet.
  - Individuo que corre programas para evitar o ralentizar acceso a redes, o corromper datos.

Sombrero Blanco: Hacker ético. Busca explotar vulnerabilidades para mejorar seguridad.

Sombrero Gris: No éticos, pero no para beneficio personal sino exponer al público. No buscan causar daños

Sombrero Negro: Criminales no éticos, buscan beneficio personal o malicioso.

1.2 Amenazas de Red

- Evolución de los Hackers:
  - 1960s Phone Freaking. Silbatos/Tonos para hacer llamadas telefónicas gratis.
  - 1980s War Dialing. Software de marcación telefónica para buscar servidores que acceder.

    .

    .

    .
  - Actualidad:

Script Kiddies: Gente sin experiencia que usa herramientas para causar daños.

Vulnerability Broker: Buscan exploits, reportan a las empresas, usualmente por recompensas.

Patrocinados por el Estado: Roban secretos a otros gobiernos / empresas información de inteligencia. ¿Corregir un error percibido?

Hacktivist: Protestan contra ideales político-sociales exponiendo vulnerabilidades o evitando accesos.

Cyber Criminal: Criminales u organizaciones responsables de robos de millones de dolares.

1.2 Amenazas de Red

- Cyber Criminales:
  - Sombrero Negro, que buscan hacerse de dinero ilícitamente.
    - Solitarios o en organizaciones criminales.
  - Operan economía underground,
    - Compran / venden herramientas de ataque, información de propiedad intelectual.
  - Atacan medianas y grandes empresas / industrias.

1.2 Amenazas de Red

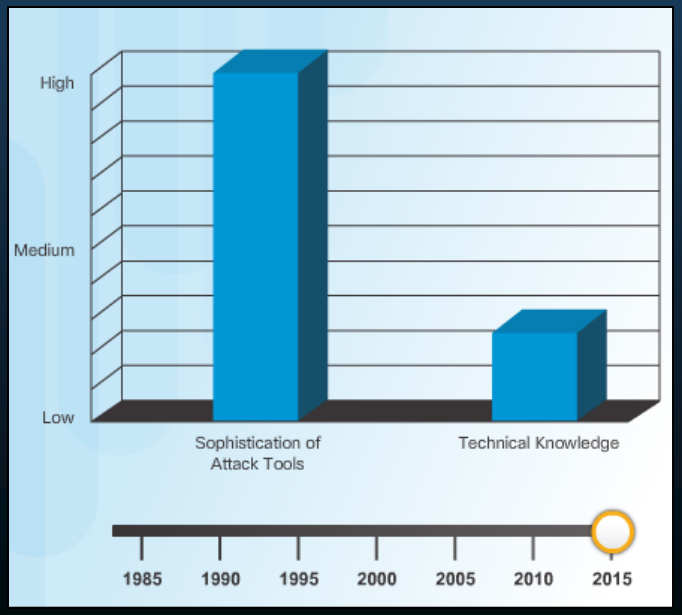
- Hacktivistas:
  - No buscan beneficio propio.
    - Motivados por cuestiones político / sociales, para promover mensajes.
      - Vgr; Anonymous / Syrian Electronic Army
  - Usualmente no muy organizados,
    - Causan problemas significativos a gobiernos o negocios.
    - Uso de herramientas gratuitas.

1.2 Amenazas de Red

- Patrocinados por Gobiernos:
  - De los hackers mas recientes.
    - Usualmente realizan cyberespionaje o robo de propiedad intelectual.
    - Usualmente las naciones niegan su existencia.
  - Crean herramientas avanzadas a la medida, a partir de vulnerabilidades no antes descubiertas.
  - Vgr; Malware Stuxnet.
    - Creado para dañar capacidades de enriquecimiento nuclear de Iran.
  - ¿Corregir un error percibido?

1.2 Amenazas de Red

- Introducción a las Herramientas de Ataque:
  - Para explotar vulnerabilidades un atacante debe utilizas técnicas o herramientas.
    - Al paso de los años las herramientas:
      - Se vuelven mas sofisticadas y automatizadas.
      - Requieren menos conocimiento técnico para su uso.



1.2 Amenazas de Red

- Evolución de las Herramientas de Seguridad:
  - Herramientas de Hacking Ético: permiten probar y mantener segura una red.
    - También utilizadas por los Sombrero Negro + las suyas propias.
  - Herramientas de prueba de penetración:

Password cracker: Remover, sustituir ó descubrir contraseñas (John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, Medusa).

Wireless Hacking: Acceder a redes inalámbricas o detectar vulnerabilidades (Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, NetStumbler).

Network Scanning: Buscan puertos TCP/UDP abiertos (Nmap, SuperScan, Angry IP Scanner, NetScanTools).

Packet Crafting: Probar seguridad de firewalls con paquetes especialmente diseñados (Hping, Scapy, Socat, Yersinia, Netcat, Nping, Nemesis).

Packet Sniffer: Analizar paquetes de redes tradicionales (Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip).

Rootkit Detector: Verifican directorios en integridad buscando Root (AIDE, Netfilter, OpenBSD Packet Filter).

Fuzzers: Buscan vulnerabilidades (Skipfish, Wapiti, W3af).

1.2 Amenazas de Red

- Evolución de las Herramientas de Seguridad:
  - Herramientas de Hacking Ético: permiten probar y mantener segura una red.
    - También utilizadas por los Sombrero Negro + las suyas propias.
  - Herramientas de prueba de penetración:

Forensic: Buscan rastros de evidencias (Sleuth Kit, Helix, Maltego, Encase).	Encryption Tools: Previenen accesos no autorizados (VeraCrypt, CipherShed, OpenSHH, OpenSSL, Tor, OpenVPN, and Stunnel).
Debuggers: Ingeniería inversa para escribir exploits (GDB, WinDbg, IDA Pro, and Immunity Debugger).	Exploitation Tools: verifican vulnerabilidad de hosts (Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, Netsparker).
Debuggers: Ingeniería inversa para escribir exploits (GDB, WinDbg, IDA Pro, and Immunity Debugger).	Vulnerability Scanners: verifican dispositivos vulnerables en redes (Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, Open VAS).
Hacking OS: OS con hacking tools (Kali, SELinux, Knoppix, BackBox).	

1.2 Amenazas de Red

- Categorías de las Herramientas de Ataque:
  - Combinaciones de herramientas pueden generar diversos ataques:

Eavesdropping: Escucha de tráfico, también conocido como Sniffing/Snooping.	DoS: Ganado acceso, comprometer disponibilidad / bloquear servicios mediante inundaciones, sobrecargas, bloqueos, etc.
Data Modification: Alteración de tráfico capturado.	Man-in-the-Middle: Atacante entre el origen y el destino, monitorean, capturan y manipulan comunicaciones.
Address Spoofing: Creación de tráfico falso que parezca verídico.	Compromised-key: Obtenida una llave, puede utilizarse para ganar acceso a una comunicación segura.
Password-Based: Obtenida una contraseña, buscar conseguir listas de usuarios/contraseñas, o cambiar configuraciones.	Sniffer: Monitoreo y captura de datos sensibles no encriptados.

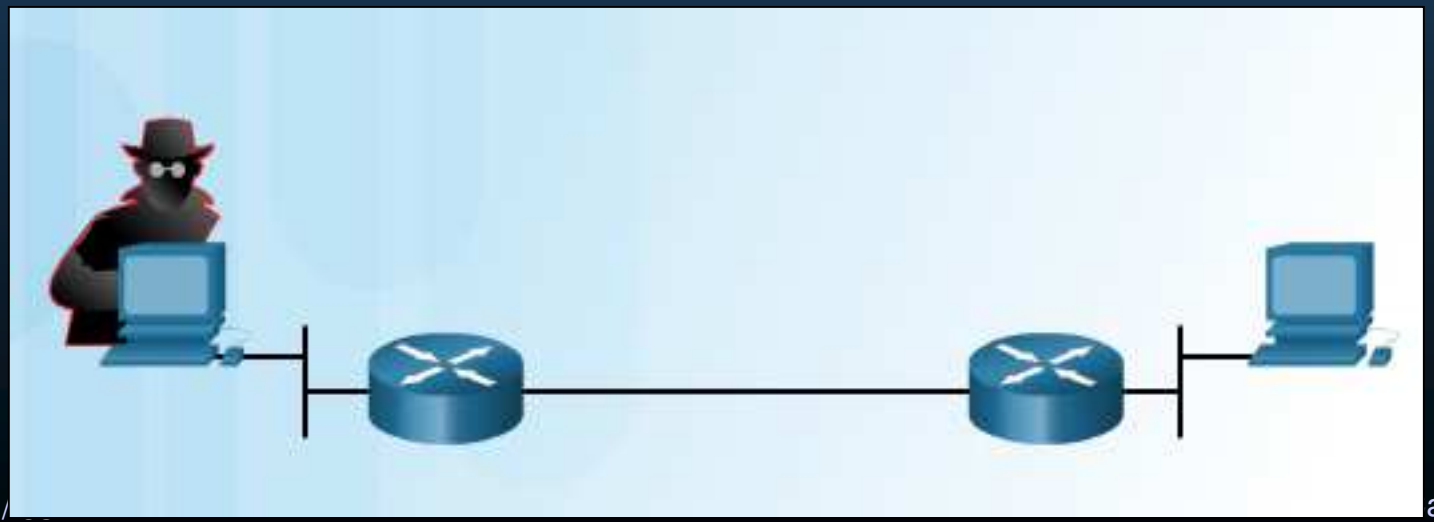
1.2 Amenazas de Red

- Varios Tipos de Malware:
  - Atacantes solicitan al usuario, instalar malware en dispositivos finales para explotar sus vulnerabilidades mediante:

Virus: Software que ejecuta funciones maliciosas en un equipo.

Gusanos: Software que se replica, instalando copias de si mismo en memoria y cualquier dispositivo de la red.

Caballos de troya: Código malicioso que aparenta ser algo legítimo, para atacar desde dentro.



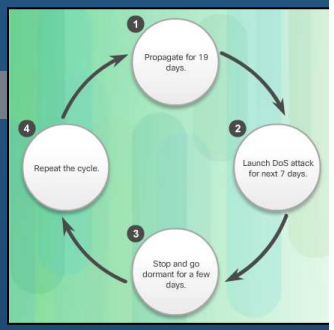
1.2 Amenazas de Red

- Virus:
  - Código malicioso añadido a un archivo ejecutable.
    - Suele requerir activación por el usuario.
    - Puede permanecer inactivo durante un tiempo.
    - Puede buscar otros ejecutables para infectarlos.
    - Pueden realizar acciones desde mostrar una imagen hasta destruir información.
    - Pueden mutar o evitar su detección.
    - Se propagan por:
      - Memorias USB
      - CDs/DVDs
      - E-mail
      - Etc…

1.2 Amenazas de Red

- Caballos de Troya:
  - Malware que contiene funciones maliciosas disfrazadas de funciones legítimas.
  - Clasificaciones según sus acciones:
    - Habilitan acceso remoto.
    - Envían datos sensibles.
    - Destruyen datos/ archivos.
    - Proxy, establece equipo como intermediario para enviar ataques.
    - FTP, habilita transferencias no autorizadas.
    - Deshabilita seguridad como antivirus,
    - Firewall, etc.
    - DoS.
  - Suelen ser difíciles de detectar.

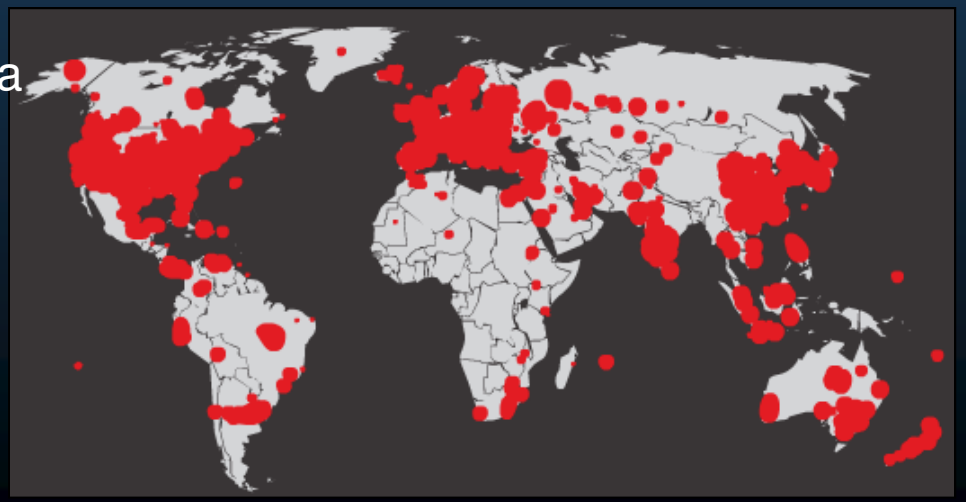
1.2 Amenazas de Red



- Gusanos:
  - Software que se auto-replica, explotando vulnerabilidades.
    - Responsables de los ataques mas devastadores de Internet.
      - Code Red worm (2001).
      - SQL Slammer. DoS (2003) Buffer Overflow en SQL Server.
      - MyDoom worm (2004) robo de contactos para envío de spam.
      - Conficker worm (2008)

Se ejecuta de manera independiente.

- En general:
  - Habilitan vulnerabilidad. Se instalan explotando una vulnerabilidad.
  - Se propagan: se replica a si mismo.
  - Contienen carga útil: código malicioso.



1.2 Amenazas de Red

- Otros Malwares:
  - Ransomware: Deniega el acceso a un equipo y solicita un pago para remover la restricción.
  - Spyware: recolecta y envía información sobre un usuario.
    - Adware: Despliega molestos anuncios, para generar ingresos al autor, analizar intereses.
    - Tracking cookies.
    - Key loggers.
  - Scareware: Scam software (estafas), para generar ansiedad en el usuario y forzarlo a realizar acciones desesperadas.
  - Phishing: Convence a la gente de que divulgue información sensible. Engaña mediante interfaces similares a las reales para obtener información.
  - Rootkits: Se instala en un equipo con privilegios root y brinda acceso externo con dichos privilegios.

1.2 Amenazas de Red

- Tipos de Ataques de Red:
  - Gran cantidad de posibles ataques.
    - Para mitigarlos, es útil categorizarlos
      - Ataques de reconocimiento.
      - Ataques de Acceso
      - Ataques DoS

1.2 Amenazas de Red

- Ataques de Reconocimiento (Recon):
  - Recolección de información.
    - Ladrón que ronda el vecindario pretendiendo vender algo.
    - Busca vulnerabilidades.
  - Técnicas:
    - Búsqueda de información de un objetivo (Google search, website, whois).
      - Sniffing en busca de información útil. (dirección de red, contraseñas).
    - Barrido de ping. Busca Ips activas en una red.
    - Escaneo de puertos. Conociendo una IP activa se buscan puertos habiertos (Nmap, SuperScan, Angry IP Scanner, NetScanTools).
    - Escaners de Vulnerabilidades. Identificar tipo y versión de servicio por cada puerto abierto (Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, Open VAS).
    - Herramientas de Explotación. Intenta explotar vulnerabilidades (Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, Netsparker)

1.2 Amenazas de Red

- Ataques de Acceso:
  - Explotan vulnerabilidades conocidas en servicios:
    - Autenticación, FTP, Web, Bases de Datos, etc.
  - Objetivos:
    - Obtener datos, Ganar acceso, Escalar privilegios.
  - Tipos:
    - Ataque a Passwords: Ingeiería social, por diccionario, fuerza bruta (Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, Medusa).
    - Trust Exploitation: Ganar acceso a equipos, comprometiendo otros considerados de confianza (por transitividad).
    - Redirección de puertos: Uso de puertos en un sistema comprometido para atacar otros sistemas por otros puertos.
    - Man-in-the-midle: Lectura, modificación de comunicaciones entre dos entidades.
    - Desbordamiento de buffer: escribir en memoria mas datos del espacio reservado / disponible (¿ejecutar código malicioso?).
    - IP, MAC, DHCP Spoofing: Hacerse pasar por otro equipo, falsificar datos.

1.2 Amenazas de Red

- Ataques de Ingeniería Social:
  - Manipular individuos para que divulguen información.
    - Manipulación por vanidad, autoridad, codicia.

Social Engineering Toolkit (SET)

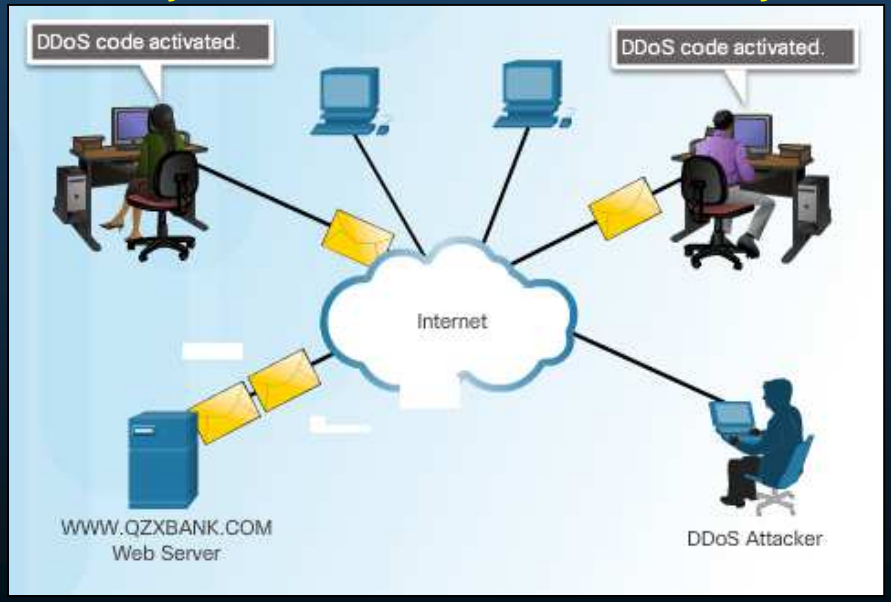
  - Algunos tipos:
    - Pretexting: Mentir para obtener información (Pedir información bancaria para comprobar identidad)
    - Phishing: e-mail fraudulento disfrazado de fuente legítima, pidiendo instalar malware o revelar información.
    - Spear phishing: Phishing a la medida para un individuo u organización.
    - Spam: email, para engañar al usuario a que haga clic en una liga / descargue archivo infectado.
    - Tailgating: Meterse rápidamente por la puerta que abre un usuario autorizado antes de que se cierre.
    - Quid pro quo: Ofrecer algo a cambio de información sensible (regalo x confirmar información personal)
    - Baiting: Atacante deja un cebo (USB infectada), esperando que alguien la encuentre y use en algún equipo, para comprometerlo.

1.2 Amenazas de Red

- Ataques de Denegación de Servicios:
  - Interrupción de servicio a usuarios, equipos o aplicaciones (comprometer disponibilidad).
  - Dos grandes fuentes:
    - Paquetes maliciosamente formados: el receptor es incapaz de manejarlos y entra en alguna excepción no contemplada y el dispositivo colapsa.
    - Cantidad abrumadora de Tráfico: imposible de ser atendida por una red, host, o aplicación, causando colapso.
  - 3 Tipos pioneros:
    - Ping de la muerte: Echo request en un paquete ip mayor a la longitud máxima de 65535bytes.
    - Ataque Pitufo: Gran numero de ICMPs a Broadcasts de varios orígenes a varios destinos, con IPs origen falsas.
    - TCP SYN Flood: Envio de TCP SYN con IP origen falsas, respuesta SYN, ACK, ACK nunca es recibido. Se satura de conexiones semi-abiertas.

1.2 Amenazas de Red

- Ataque DoS Distribuido:
  - Se origina de múltiples fuentes coordinadas.
    - Un atacante infecta una red (Botnet).
    - Los equipos comprometidos (zombies) buscan e infectan mas equipos, controlados por un sistema manejador.
    - El Sistema manejador indica a los zombies ejecutar DoS.



  - El mercado negro vende servicios DDoS para atacar determinado objetivo.

1.2 Amenazas de Red

- Ataque mas común DDoS:
  - Explota HTTP incluso con SSL.
  - Envíar mucha información rápido puede ser detectada fácilmente.
    - Sloworis genera ataques lentos, con mucha información que procesar.
      - Indica al servidor que tiene problemas de hashing y requiere recomputar hashes.

1.2 Amenazas de Red

Network Attack Type	Reconnaissance	Access	DoS	Social Engineering
Buffer Overflow		✓		
Tailgating				✓
Password		✓		
Port Scanning	✓			
Smurf			✓	
Man-in-the-Middle		✓		
Baiting				✓
IP, MAC, DHCP Spoofing		✓		
TCP SYN Flood			✓	
Ping Sweep	✓			
Port Redirection		✓		

1.3 Mitigación de Amenazas

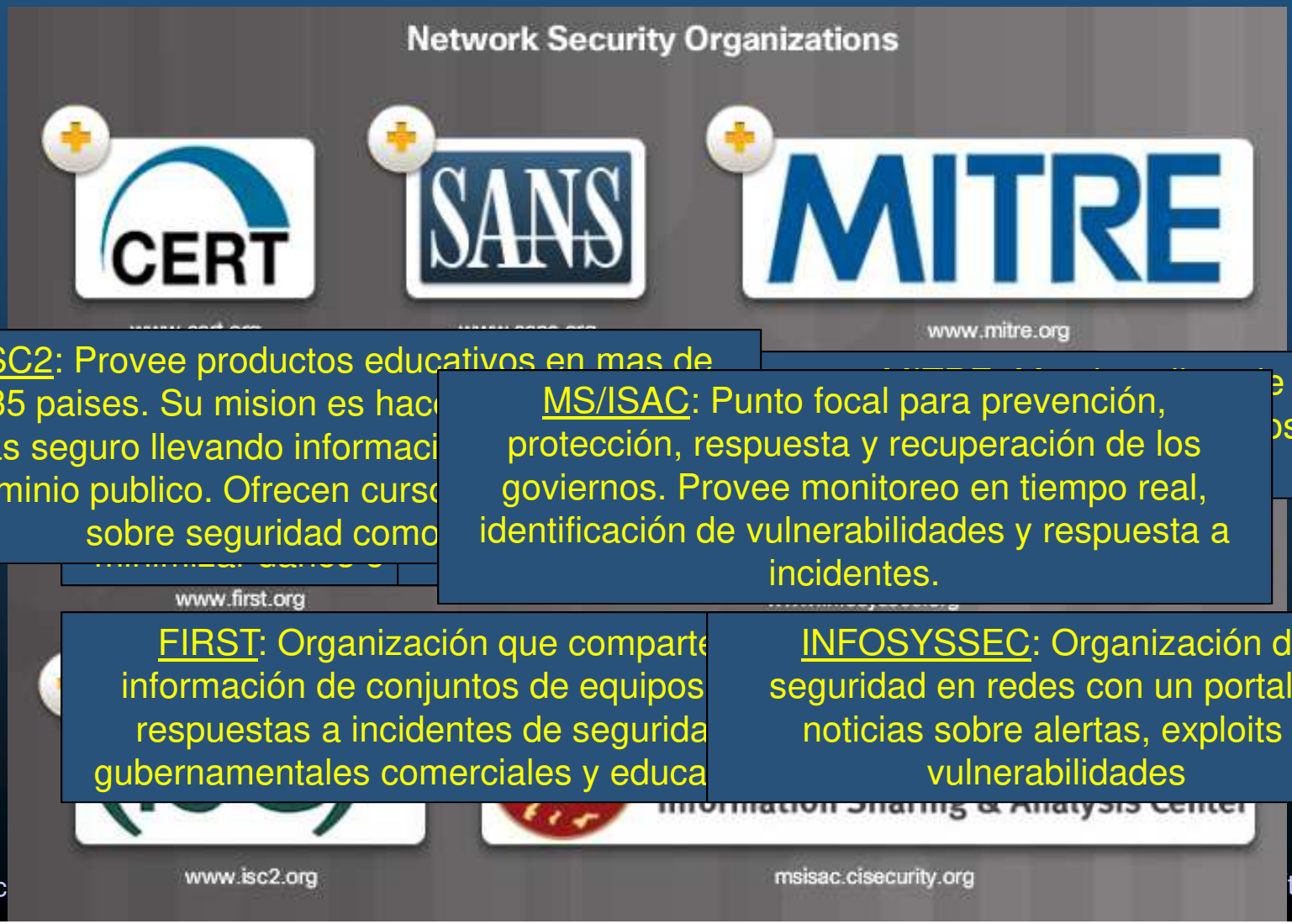
- Profesionistas en Seguridad de Redes:
  - Responsables de mantener la seguridad, integridad y confidencialidad de los datos.
    - Campo laboral creado por los hackers.

    - Estar en constante actualización de nuevas amenazas.
    - Deben asistir a entrenamientos y capacitaciones.
    - Estar suscritos a noticias en tiempo real sobre amenazas.
    - Examinar detenidamente sitios sobre seguridad.
    - Mantener contacto con empresas de seguridad

Chief Information Officer (CIO)	Chief Security Officer (CSO)
Chief Information Security Officer (CISO)	Security Manager
Security Operations (SecOp) Manager	Network Security Engineer

1.3 Mitigación de Amenazas

- Organizaciones de Seguridad de Redes:



ISC2: Provee productos educativos en mas de 135 paises. Su mision es hac mas seguro llevando informaci dominio publico. Ofrecen curs sobre seguridad como

MS/ISAC: Punto focal para prevención, protección, respuesta y recuperación de los goviernos. Provee monitoreo en tiempo real, identificación de vulnerabilidades y respuesta a incidentes.

FIRST: Organización que comparte información de conjuntos de equipos respuestas a incidentes de seguridad gubernamentales comerciales y educa

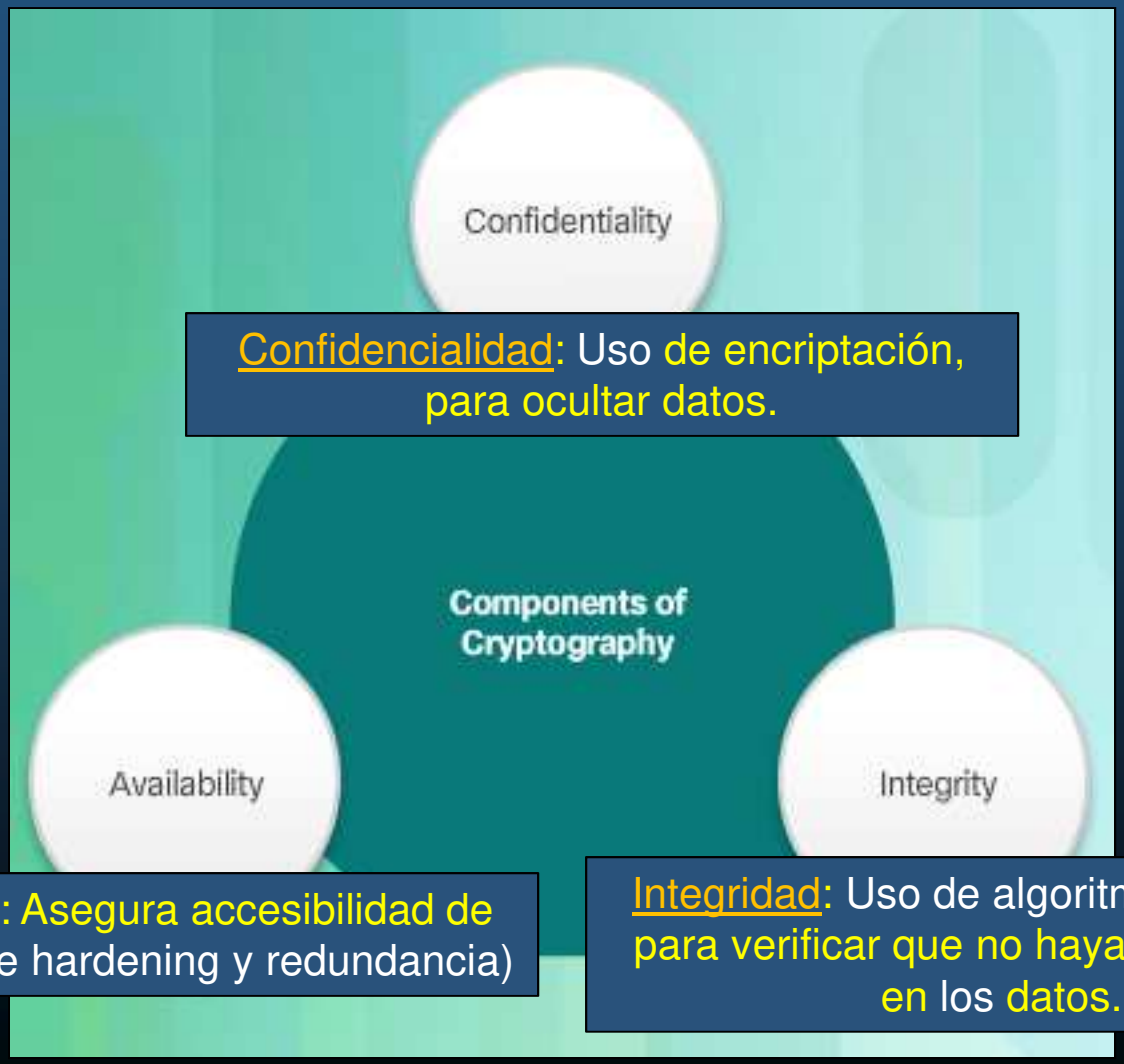
INFOSYSSEC: Organización de seguridad en redes con un portal de noticias sobre alertas, exploits y vulnerabilidades

1.3 Mitigación de Amenazas

- Criptografía
  - Es el estudio y práctica de esconder información.
  - Cada tipo de red de comunicaciones utiliza su propio mecanismo para proteger información de acceso no autorizados.
  - Usos comunes:
    - Comunicaciones en redes de datos.
    - Las conversaciones de voz.
    - Datos de un equipo .
  - La tendencia es cifrar todo lo que sea posible.

1.3 Mitigación de Amenazas

- Componentes de Criptografía



Confidencialidad: Uso de encriptación, para ocultar datos.

Disponibilidad: Asegura accesibilidad de datos (Mediante hardening y redundancia)

Integridad: Uso de algoritmos de Hash, para verificar que no haya alteraciones en los datos.

1.3 Mitigación de Amenazas

- Dominios de seguridad de redes.
  - Marco de referencia para la discusión de seguridad en redes (ISO/IEC 27002)
    - Brinda separación de 12 elementos:

1. Evaluación de Riezgos: Calificar cualitativa y cuantitativamente situaciones / amenazas.
2. Políticas de Seguridad: Documento con restricciones y comportamientos de los miembros de una organización, así como para acceso a datos.
3. Organización de la Seguridad de Información: modelo para la seguridad de la información.
4. Gestión de Activos: Inventario y Clasificación de los bienes de información.
5. Seguridad de Recursos Humanos: Procedimientos relacionados a empleados en una organización.
6. Seguridad Ambiental y Física: Protección de instalaciones de la organización.
7. Administración de Operaciones y Comunicaciones: Control de seguridad técnica en sistemas y redes.
8. Desarrollo, Mantenimiento y Adquisición de Sistemas de Información: Integración de seguridad en diferentes aplicaciones.

1.3 Mitigación de Amenazas

- Dominios de seguridad de redes (cont.).
  - Marco de referencia para la discusión de seguridad en redes (ISO/IEC 27002)
    - Brinda separación de 12 elementos:

9. Control de Acceso: Restricciones de acceso y permisos a redes, sistemas, aplicaciones, funciones y datos.
10. Administración de Incidentes en Seguridad de Información: Describe cómo anticipar y responder ante brechas en seguridad de Información.
11. Administración Continua de Negocios: Describe, protección, administración y recuperación de procesos críticos para el negocio.
12. Conformidad: Aseguramiento de conformidad con las políticas de seguridad de información, estándares y regulaciones.

1.3 Mitigación de Amenazas

- Políticas de Seguridad (Dominio 2).
  - Reglas por las que se da acceso a las personas, a tecnologías y bienes de e información en una organización.
    - Críticas para mantener una organización segura.
    - Responsabilidad de los profesionales de seguridad en redes.
    - Importante cubrir todos los aspectos de operaciones de negocio.

1.3 Mitigación de Amenazas

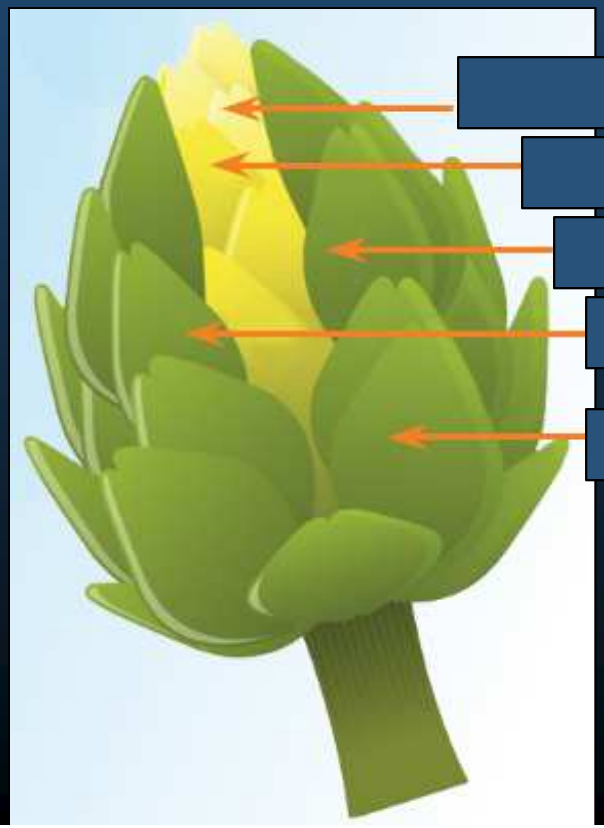
- Políticas de Seguridad de Redes.
  - Documento para ayudar a describir el diseño de red, plasmar los principios de seguridad, y facilitar desarrollos de red y establecer reglas de acceso a redes.
  - Compilada usualmente por un comité.
  - Gobierna (según la Arquitectura Cisco SecureX):
    - Acceso a datos.
    - Navegación web.
    - Uso de contraseñas.
    - Encriptación.
    - Adjuntos de Mails.
    - Servicios por usuario.
    - Jerarquía de acceso y permisos para que cada empleado trabaje.
    - Bienes protegidos
    - Dispositivos de seguridad.
    - Estrategias de mitigación

1.3 Mitigación de Amenazas

- Objetivos de las Políticas de Seguridad de Redes.
  - Asegurar la seguridad de cualquier red y sistemas de cómputo de una organización.
  - Mantener políticas en constante revisión y actualización.
  - EL desarrollo de políticas de seguridad debe considerar:
    - ¿Qué bienes hay que otros deseen?
    - ¿Qué procesos, datos, o sistemas de información son críticos para cada persona u organización?
    - ¿Qué detendría a una persona u organización de llevar a cabo su trabajo o misión?

1.3 Mitigación de Amenazas

- Alcachofa de la Seguridad.
  - Cuando un hacker lanza un ataque deberá remover hojas que revelaran información sensible solo de esa hoja.
    - Deberá continuar removiendo hojas para llegar al centro, donde se encuentre la información mas sensible.
      - (No es necesario remover todas las hojas).



Contraseñas.

Ataques del lado del cliente.

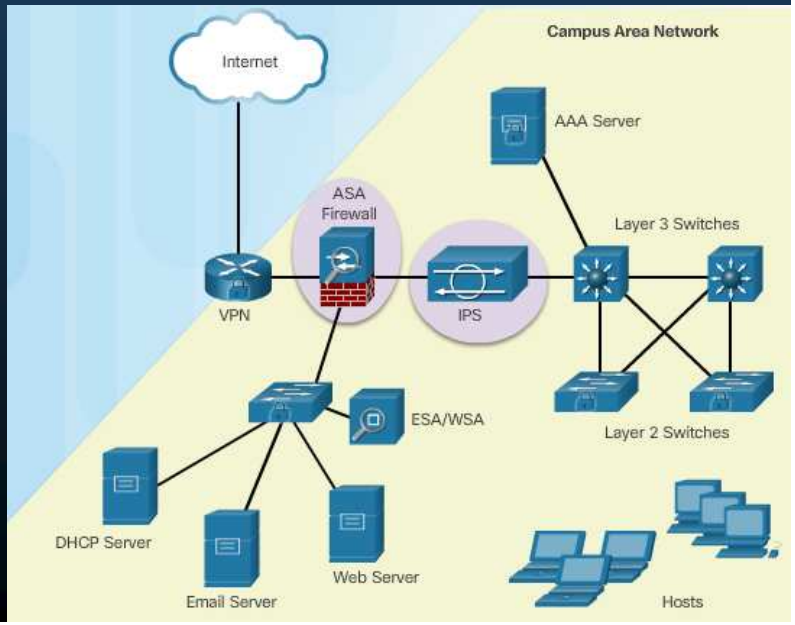
Bases de Datos.

Aplicaciones web.

Desbordamiento de buffers.

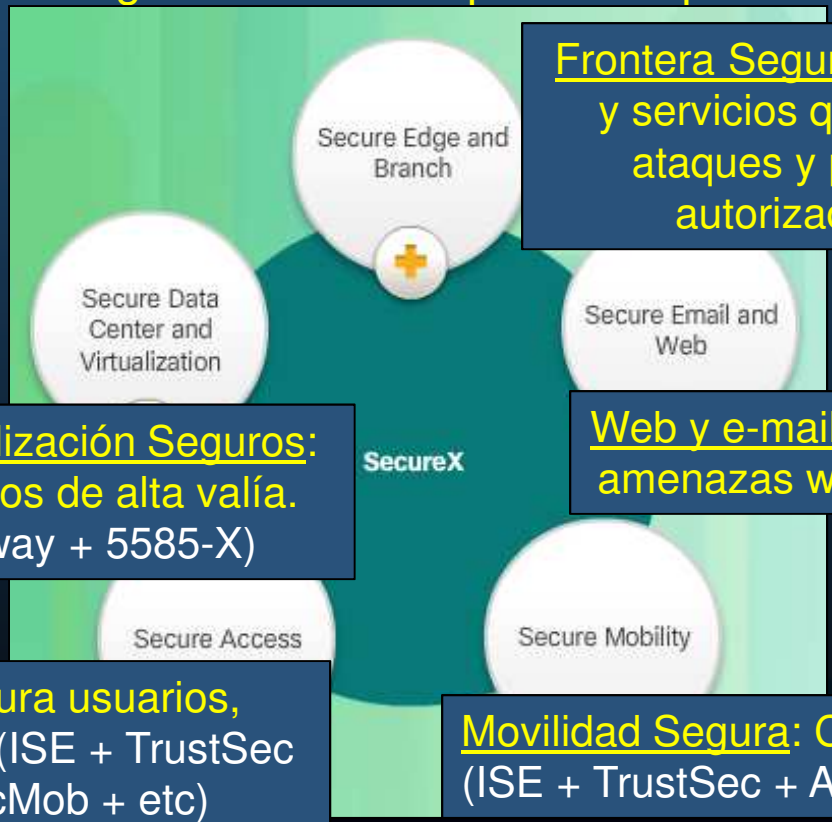
1.3 Mitigación de Amenazas

- Evolución de las herramientas de seguridad.
  - 1990s. Seguridad como parte integral de operaciones diarias.
    - Herramientas dedicadas a cada función de red.
  - IDSs. Detección en tiempo real de ciertos ataques.
  - IPSs. Detección y bloqueo en tiempo real de ciertos tipos de ataques.
  - Firewall. Evita tráfico indeseable, establece perímetros de seguridad.
  - ASA. Dispositivos Firewall dedicados y autónomos.
  - Cisco SecureX. Linea de tecnologías de seguridad (identificar y detener tráfico malicioso).



1.3 Mitigación de Amenazas

- Productos SecureX.
  - Movilidad de usuarios y localización de datos en lugares no tradicionales incrementan la complejidad de la seguridad.
  - SecureX proveen seguridad efectiva para cualquier usuario.



Frontera Segura y Sucursales: Sistemas y servicios que detectan y bloquean ataques y previenen accesos no autorizados (Firewall + IPS)

Centro de Datos y Virtualización Seguros: Protegen datos y recursos de alta valía. (ASAv + Virtual Gateway + 5585-X)

Web y e-mail Seguros: Evitan evolucionar amenazas web y de e-mail (ESA + WSA)

Acceso Seguro: Asegura usuarios, controla acceso a hosts (ISE + TrustSec + AnyConnect + SecMob + etc)

Movilidad Segura: Conectividad móvil por VPNs (ISE + TrustSec + AnyConnect + SecMob + etc)

1.3 Mitigación de Amenazas

- Tecnologías SecureX.
  - Utiliza lenguaje de politicas de alto nivel para establecer contexto de una situación mediante:
    - Quién, qué, donde, cuando y como.
  - 5 Componentes principales:
    - Motores de búsqueda: Proxys o dispositivos de red que examinan contenidos en múltiples capas, identifican aplicaciones, autentican usuarios (Firewall / IPS / Proxy).
    - Mecanismos de Entrega: Mecanismos por los que elementos escaneados son introducidos a la red.
    - Operaciones de Inteligencia de Seguridad: Distinguen trafico bueno del malo (Cisco SIO monitorea Bases de Tráfico)
    - Consolas de Administración de Políticas: Separan la creación y administración de políticas de los puntos de aseguramiento.
    - Puntos Finales de Siguiente-Generación: Todas las conexiones entrantes o salientes, deben enrutarse a través de un dispositivo que escanee sus elementos.

1.3 Mitigación de Amenazas

- Elemento de Escaneo de Redes Consiente de Contexto Centralizado.
  - SecureX genera complejidad en la infraestructura de T.I.s.
    - Para escalar dicho modelo se requiere Elemento de Escaneo de Redes Consiente de Contexto.
  - Dispositivo de Seguridad de Red que examina paquetes que busca ¿quién, qué, donde, cuando y como? de dicho paquete.
    - Hay como dispositivos autónomos y como módulos de software.
    - Administrados por consola de políticas, mediante lenguaje de alto nivel:
      - Identidad de la persona
      - Aplicación en uso
      - Tipo de dispositivo siendo accedido
      - Ubicación
      - Tiempo de acceso
    - Aplicación distribuida que asegura seguridad por zonas, sucursales, trabajadores remotos, dispositivos virtualizados, servicios en la nube.

1.3 Mitigación de Amenazas

- Operaciones de Inteligencia de Seguridad de Cisco (SIO).
  - Servicio basado en la nube que conecta información de amenazas globales, servicios basados en reputación, análisis sofisticados a dispositivos Cisco.

Fuentes:

- Listas negras y filtros de reputación
- Trampas spam, honeypots, rastreadores
- Registros de dominios web
- Bases de datos de firmas de ataques
- Inspección de contenidos
- Información de terceros (asociaciones).
- Equipo de investigación (white hats).

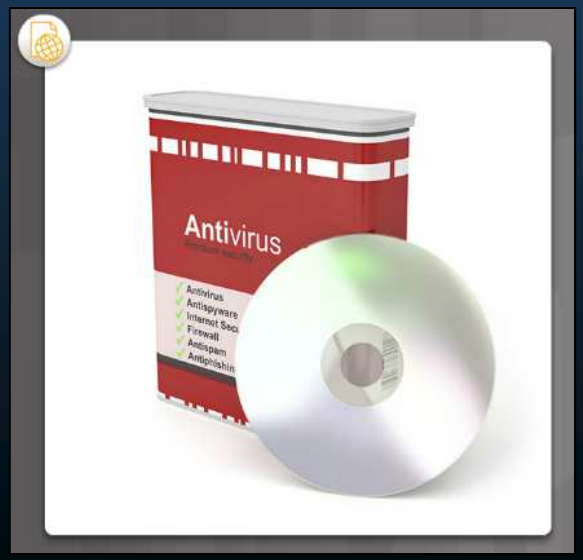
1.3 Mitigación de Amenazas

- Defensa de la Red.
  - Vigilancia y educación constante.

  - Mejores Prácticas :
    - Desarrollar política de seguridad.
    - Educar a los empleados (riezgos, ing. Social, Validación de identidades).
    - Controlar acceso físico.
    - Uso de contraseñas fuertes y cambio constante.
    - Encriptación de datos sensibles.
    - Uso de hardware y software de seguridad (Firewall, IPS, VPN, Antivirus)
    - Realizar Respaldos y comprobar su estado.
    - Apagar dispositivos innecesarios y cerrar puertos.
    - Actualizar parches de seguridad de sistemas constantemente.
    - Realizar auditorías de seguridad.

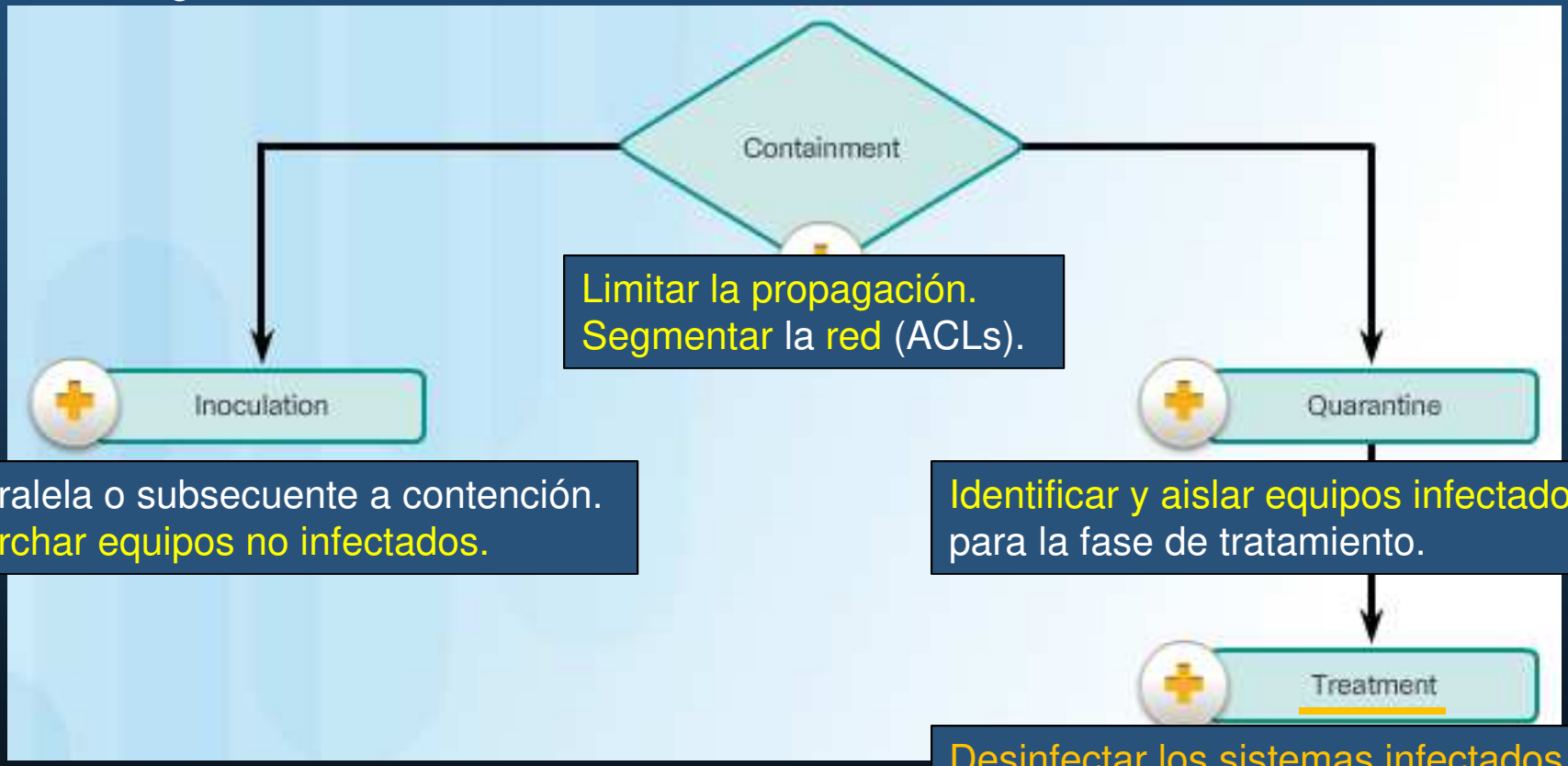
1.3 Mitigación de Amenazas

- Mitigar Malware.
  - Contramedidas basadas en hosts :
    - Antivirus (Symantec, McAfee, and Trend Micro).
      - Licencias por volumen.
      - Opciones de actualización automática
  - Contramedidas para redes.
    - Actualizaciones de seguridad de dispositivos de red.



1.3 Mitigación de Amenazas

- Mitigación de Gusanos.
  - Los gusanos se basan mas en las redes.



1.3 Mitigación de Amenazas

- Mitigación de Ataques de Reconocimiento.
  - Precursor a otros ataques.
  - Monitorear actividad.
  - Pre-configurar alarmas, para cuando se excedan ciertos límites (ASA, IOSSec).
    - Herramientas Anti-Sniffer (cambian tiempo de respuesta)
    - Encriptación.
    - Anti escaneo de puertos (IPS limita tiempo de respuesta)
    - Deshabilitar ICMP en routers de frontera

1.3 Mitigación de Amenazas

- Mitigación de Ataques de Acceso.
  - La mayoría de estos ataques son por adivinación de contraseña ó fuerza bruta ó diccionario.
  - Prevención:
    - Contraseñas fuertes: al menos 8 caracteres entre mayúsculas, minúsculas, números y otros caracteres.
    - Deshabilitar cuentas tras determinado número de intentos fallidos: retrasa ataques.
    - Un dispositivo confiable no debe confiar en otros dispositivos incondicionalmente.
    - Uso de protocolos encriptados o con autenticación por hashes.
    - Educar a los empleados de los riesgos de ing. Social.
  - Detección
    - Revisión de logs, uso de ancho de banda, cargas de procesos.

1.3 Mitigación de Amenazas

- Mitigación de Ataques DoS.
  - Identificado por quejas de recursos no disponibles.
  - Software de monitoreo de uso de red con actividad inusual.

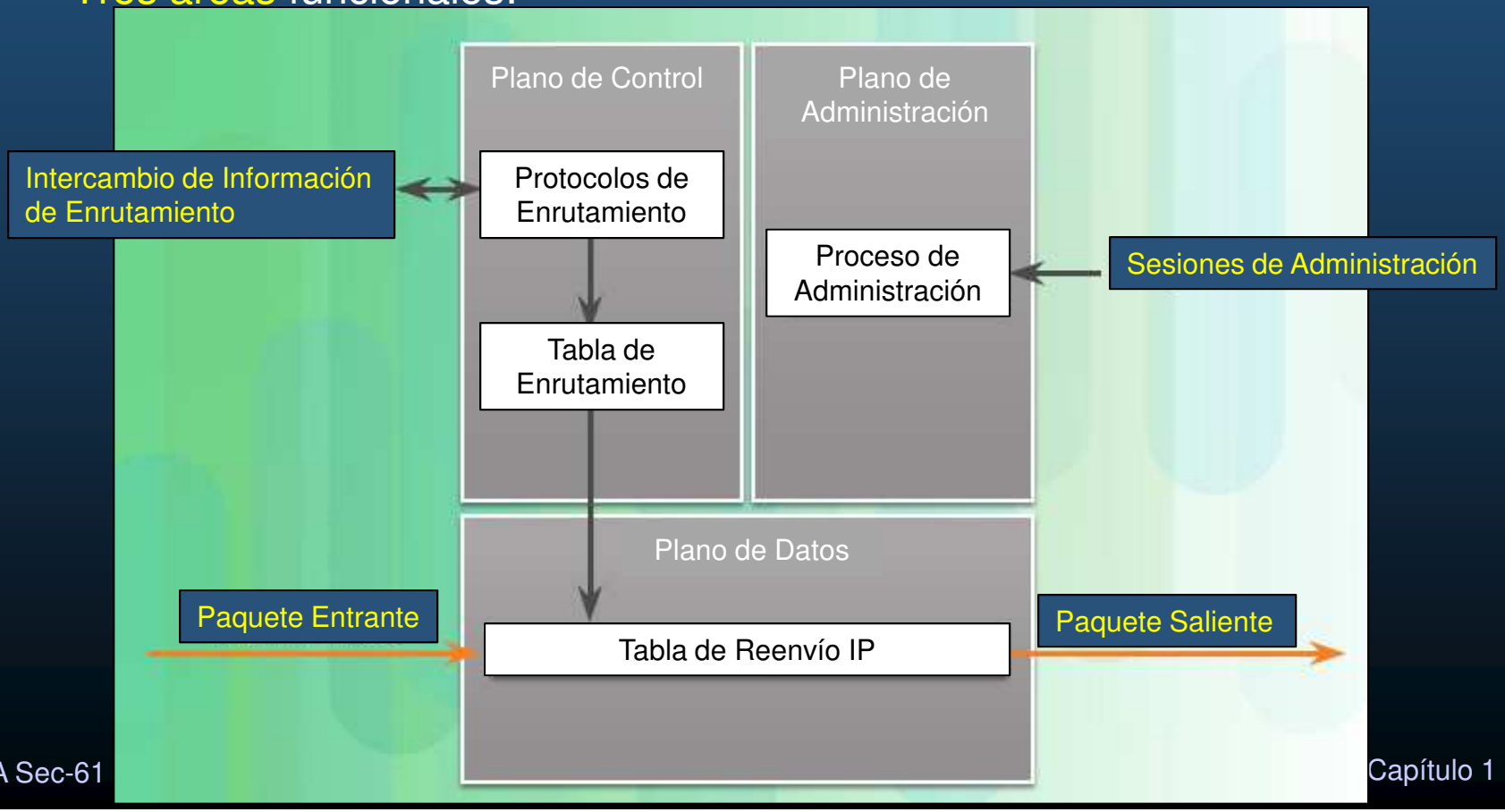
  - Mitigación:
    - Detección y bloqueo de direcciones falseadas.
    - Habilitar seguridad de puerto en switches.
    - Anti DHCP Snoop.
    - Inspección ARP.
    - ACLs

1.3 Mitigación de Amenazas

- Cisco Network Foundation Protection (NFP).
  - Guías para proteger la infraestructura de red (servicio de entrega).
  - Tres áreas funcionales:
    - Plano de Control: Responsable del enrutamiento correcto. Genera paquetes para la correcta operación de la red (Paquetes de control generados por dispositivos: ARP, Enrutamiento).
    - Plano de Administración: Responsable de administrar elementos de red. Genera paquetes de administración (Telnet, SSH, TFTP NTP, AAA,SNMP, SYSLOG, TACACS, RADIUS, NetFlow)
    - Plano de Datos: Responsable del re-envío de datos. Paquetes de usuario reenviados entre dispositivos.

1.3 Mitigación de Amenazas

- Cisco Network Foundation Protection (NFP).
  - Guías para proteger la infraestructura de red (servicio de entrega).
  - Tres áreas funcionales:



1.3 Mitigación de Amenazas

- Seguridad del Plano de Control.
  - Autenticación de protocolos de enrutamiento: previene a un router aceptar actualizaciones de enrutamiento fraudulentas.
  - Supervisión del Plano de Control (CoPP): Característica del IOS de Cisco para controlar el tráfico en un router.
    - Diseñado para prevenir que tráfico innecesario sobrecargue el router.
    - Conjunto de reglas para asociar entradas y salidas del plano de control.
  - AutoSecure: Puede bloquear funciones del plano de administración y servicios del plano de datos.

1.3 Mitigación de Amenazas

- Seguridad del Plano de Administración.
  - El tráfico entre hosts de administración y equipo administrado se prefiere fuera de banda (OOB), fuera de ambiente producción, aunque pueda ser en banda.
  - Políticas de Contraseñas de Logueo: Restringe los métodos de acceso mediante "quién" y "como".
  - Presentación de notificaciones legales: Banners indicando implicaciones legales.
  - Confidencialidad de Datos: Uso de protocolos de administración con autenticación fuerte.
  - Control de Acceso Basado en Roles (RBAC): solo acceso a usuarios, grupos y servicios en conjunto con Cuentas de Autenticación y Autorización (AAA).
    - Crea vistas de comandos en CLI para usuarios en un servidor repositorio
  - Acciones Autorizadas: Restringe acciones permitidas por RBAC.
  - Reportes de Acceso a Administración: Registro de acciones para todos los accesos (usuario, dispositivo, acción, momento).

1.3 Mitigación de Amenazas

- Seguridad del Plano

  - Uso de ACLs, Mecanis

En Capa 2:

- Seguridad de Puerto
- DHCP Snooping
- Inspección Dinámica de ARP (DAI)
- Guardia de IP Origen para prevención de spooffing.

    - Bloqueo de Tráfico o Usuarios no deseados: ACLs para filtrar interfaces, basadas en direcciones o autenticación de usuarios.

    - Reducción de posibilidades de ataque DoS: ACLs que definan hosts o redes de confianza. Característica de intercepción TCP, para evitar inundación de servidores.

    - Mitigación de ataques apócrifos (spoofs): ACLs para descartar tráfico con direcciones inválidas. Ruta de Reenvío Reversa a Unicast (uRPF).

    - Control de Ancho de Banda: ACLs en enlaces lentos pueden prevenir bloqueos.

    - Clasificación de Tráfico para Proteger Planos de Administración y Control: ACLs para lineas VTYs.

Actividad Práctica

- Ataques de Red / Herramientas de Auditoría de Seguridad de Redes y Herramientas de Ataque.

1. Investigue un ataque de red y describa lo siguiente:
   - Nombre del Ataque:
   - Tipo de Ataque:
   - Fechas de Ataques:
   - Equipos/Organizaciones afectadas:
   - ¿Como funciona o que hace?:
   - Opciones de Mitigación:
2. Investigue una herramienta de auditoría de seguridad de redes / herramienta de ataque. Y describa:
   - Nombre de la herramienta:
   - Desarrollador:
   - Tipo (Comandos/GUI):
   - Plataforma para su uso:
   - Costo:
   - Características y capacidades:

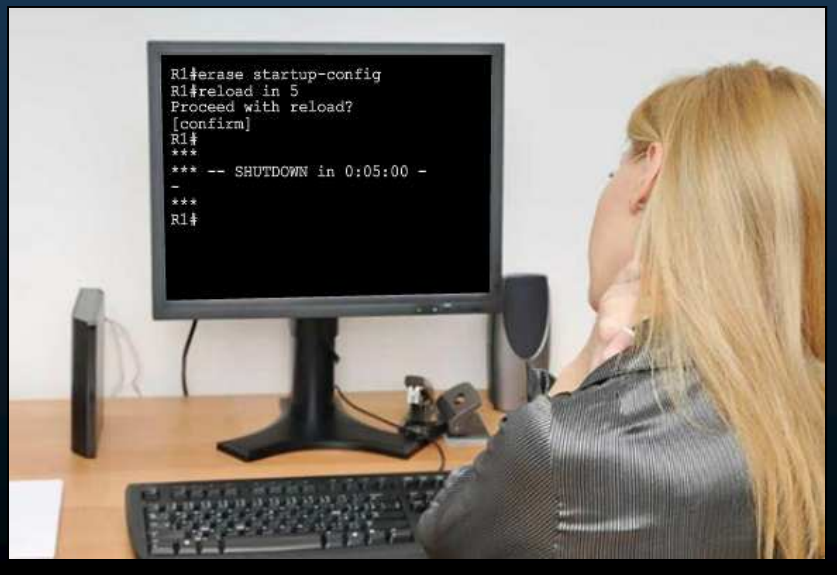
Capítulo 2

Asegurado de Dispositivos de Red

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#2.1.1.1

2.1 Asegurado de Dispositivos de Acceso

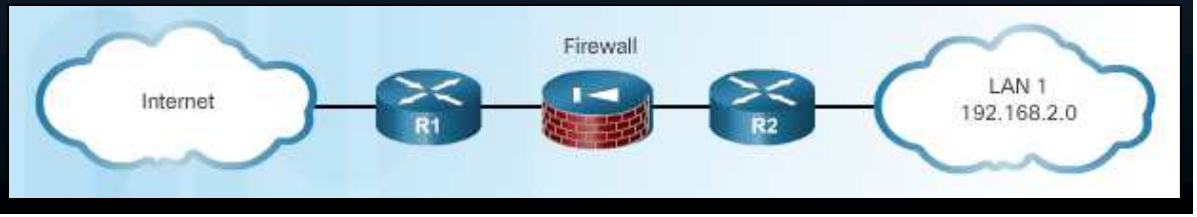
- Asegurado de la Infraestructura de Red.
  - Infraestructura de red: Routers, Switches, Servidores, Puntos Finales, etc.
  - Un usuario descontento puede ser un atacante.
  - Importante establecer Políticas de Seguridad.
  - Los routers son objetivos principales, bloqueo de comunicaciones.
    - Mas aún los routers de frontera.
  - Asegurar dispositivos es imperativo.



2.1 Asegurado de Dispositivos de Acceso

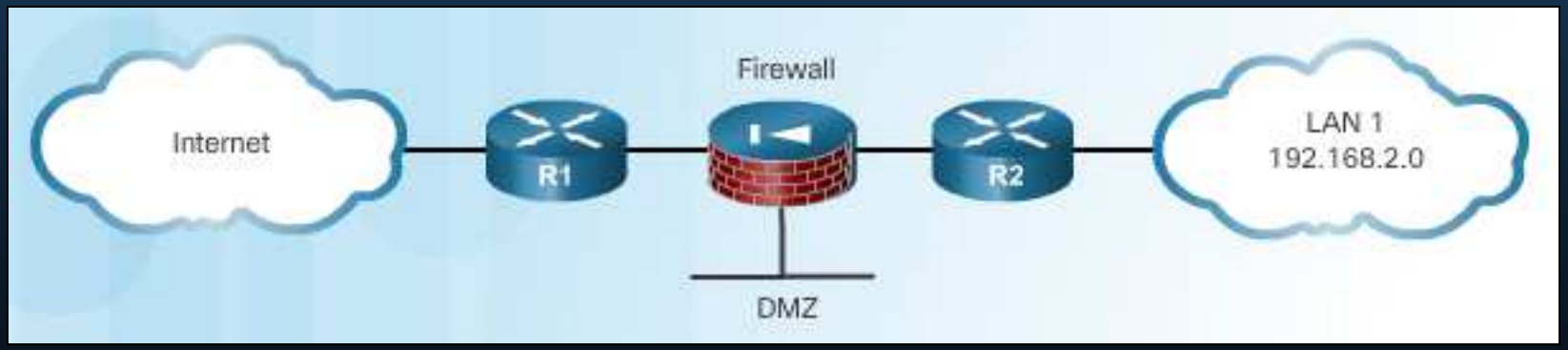
- Asegurado de Routers de Frontera.

  - Escenarios principales:
    - Router solitario: Un router protege la red interna.
      - Las políticas de seguridad se implementan en dicho router.
      - Común en pequeños sitios, sucursales, SOHO.
      - Recomendado utilizar ISR.
    - Defensa a Profundidad: Múltiples capas de seguridad para proteger la red interna.
      - Router de Frontera, router de pantalla, filtrado de tráfico inicial.
      - Firewall, Filtrado adicional, seguimiento de conexiones, evita conexiones del exterior, autentica usuarios, etc.
      - IPSs, WSA, ESA (opcionales)
      - Router Interno, .



2.1 Asegurado de Dispositivos de Acceso

- Asegurado de Routers de Frontera.
  - Escenarios principales:
    - DMZ: Variación de Defensa a Profundidad con Zona Desmilitarizada conectada al Firewall.
      - Zona Desmilitarizada: Red accesible desde el exterior (solo ciertos servicios)



2.1 Asegurado de Dispositivos de Acceso

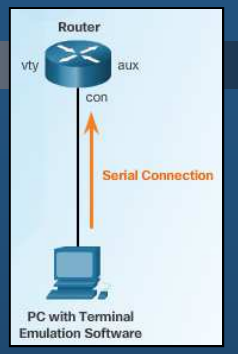
- Tres Áreas de Seguridad de un Router.

  - Seguridad Física:
    - Colocar en un cuarto asegurado, a solo personal autorizado, libre de electromagnetismos, con supresión de incendios, control de humedad.
    - Instalaciones con energía ininterrumpida, mediante UPSs y/o generadores de energía
  - Seguridad de Sistema Operativo:
    - Instalar máxima cantidad de memoria, previene DoSs.
    - Usar la última versión estable, asegura las últimas características de seguridad y encriptación.
    - Mantener copia de seguridad de las imágenes del S.O.
  - Hardening:
    - Asegurar accesos administrativos, usuarios y niveles de acceso.
    - Deshabilitar puertos, interfaces y servicios no utilizados.

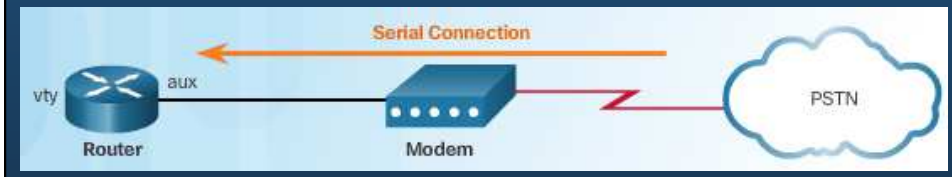
2.1 Asegurado de Dispositivos de Acceso

- Asegurar Acceso Administrativo.
  - Restringir acceso al dispositivo: Limitar puertos accesibles, Restringir comunicaciones permitidas, y métodos de acceso.
  - Registrar actividad de todos los accesos: Guardar registro de cada acceso, quién, que y cuando se realizó cada acción.
  - Autenticar accesos: permitir solo acceso a usuarios, grupos y servicios autenticados. Limitar el número de logins fallidos.
  - Autorizar acciones: restringir acciones, vistas por: usuarios, grupos y servicios.
  - Presentar Notificaciones Legales: Desplegar notificaciones para sesiones interactivas.
  - Asegurar confidencialidad de datos: proteger datos almacenados, de ser vistos y /o copiados.

2.1 Asegurado de Dispositivos de Acceso



- Asegurar Acceso Local y Remoto.
  - Local: conexión al puerto de consola. Requiere acceso físico.
  - Remoto: Conexiones a puerto auxiliar, vtys (telnet/SSH/HTTP/HTTPS/SNMP)



  - Precauciones a tomar cuando se accede remotamente:
    - Encriptar el tráfico.
    - Establecer red de administración independiente.
    - Configurar filtros de paquetes, para permitir solo hosts y protocolos autorizados.
    - Configurar VPN para acceso a la red local antes de acceder a red de administración.

2.1 Asegurado de Dispositivos de Acceso

- Contraseñas Fuertes.
  - Hay muchas herramientas para crackear passwords.
  - Usar contraseñas de mas de 10 caracteres.
  - Mezclar mayúsculas, minúsculas, números, símbolos, espacios (no al principio).
  - Evitar contraseñas con información identificable.
  - Incluya errores de deletreo (Smith -> 5myth)
  - Cambie contraseñas regularmente
  - No escriba las contraseñas o las deje en lugares inseguros.
  - Use frases, suelen ser mas fáciles de recordar que contraseñas seguras.

Contraseñas Débiles
secret
smith
toyota
bob1967
Blueleaf23

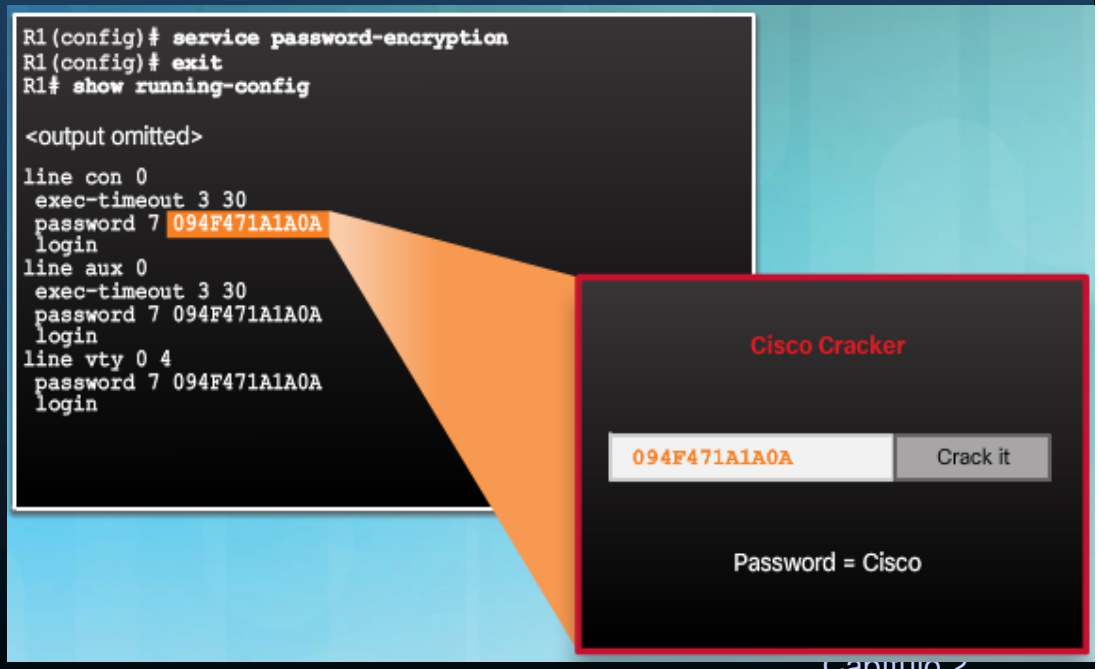
Contraseñas Fuertes
b67n42d39c
12^h u4@1p7

2.1 Asegurado de Dispositivos de Acceso

- Incremento de la Seguridad de Acceso.
  - Configuraciones recomendables:

```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```

  - Notas:
    - Longitud de password 6 por defecto.
    - Passwords (excepto secret) almacenados en texto plano y aún con `password-encryption`, pueden ser recuperados con las herramientas adecuadas.
    - Interface administrativa permanece activa por 10 min. (default)
    - Es posible inhabilitar EXEC en líneas no utilizadas con: `R(conf-line)# no exec`



2.1 Asegurado de Dispositivos de Acceso

- Algoritmos de Passwords Secretos.
  - Los Hashes MD5 pueden actualmente ser reconstruidos:
  - Sin embargo, Cisco usa MD5 por defecto.
  - Recomendable usar tipos 8 y 9.

    Sin embargo, se requiere conocer el hash del password deseado:

```
R2(config)# enable secret cisco12345
R2(config)# do show run | include enable
enable secret 5 $1$cam7$99EfzkvmJ5h1gEbryLVRy.
R1(config)# enable secret ?
  0       Specifies an UNENCRYPTED password will follow
  5       Specifies a MD5 HASHED secret will follow
  8       Specifies a PBKDF2 HASHED secret will follow
  9       Specifies a SCRYPT HASHED secret will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' secret
  level   Set exec level password

R1(config)# line con 0
R1(config-line)# pas
  0     Specifies  NCRYPTED password will follow
  7     Specif  DDEN password will follow
  LINE  The  PTED (cleartext) line password
R1(conf  )#
```

Disponibles desde Cisco IOS 15.3(3)M

```
R1(config)# enable secret 9 cis
ERROR: The secret you entere  a valid encrypted secret.
To enter an UNENCRYPTED  do not specify type 9 encryption.
When you properly ent NCRYPTED secret, it will be encrypted.

R1(config)# enable s ret 9
$9$HZWdzLHwhPtZ3U$D9OlUDSGvBy.m8Tf9vCGDJRcYy8zIMbyRJgtxgRkwzY
R1(config)#
```

2.1 Asegurado de Dispositivos de Acceso

- Algoritmos de Passwords Secretos.
  - Para ingresar un password sin encriptar, es necesario el comando:

```
enable algorithm-type {md5 | scrypt | sha256} secret unencrypted-password
```

  - Donde:
    - scrypt → tipo 9
    - sha256 → tipo 8

```
R1(config)# enable algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm
R1(config)# enable algorithm-type scrypt ?
  secret  Assign the privileged level secret (MAX of 25 characters)

R1(config)# enable algorithm-type scrypt secret cisco12345
R1(config)# do show run | include enable
enable secret 9 $9$Gyk9x3Ve4c0n5k$8.cR3yReBduzHymEyCOcErgPKW8MSKokRN 9KjEg4WQA
R1(config)#
```

2.1 Asegurado de Dispositivos de Acceso

- Algoritmos de Passwords Secretos.
  - Similar para el comando `username`:

```
username name algorithm-type {md5 | scrypt | sha256} secret unencrypted-password
```

```
R1(config)# username Bob secret cisco54321
R1(config)# do show run | include username
username Bob privilege 15 secret 5 $1$1mBB$UjOC6JA4f1WgI3/La8wGz/
R1(config)#
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# do show run | include username
username Bob privilege 15 secret 9 $9$9FkS.zTuLs89pk$v5P2y.M6reR181S
92moKHdFauk8joK0xHICXxGDuurs
R1(config)#
```

  - Hacia atrás, solo hay compatibilidad hasta nivel 7:

```
R1(config)# enable password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' password
  level   Set exec level password

R1(config)# username Bob password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) user password

R1(config)# line con 0
R1(config-line)# password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) line password
```

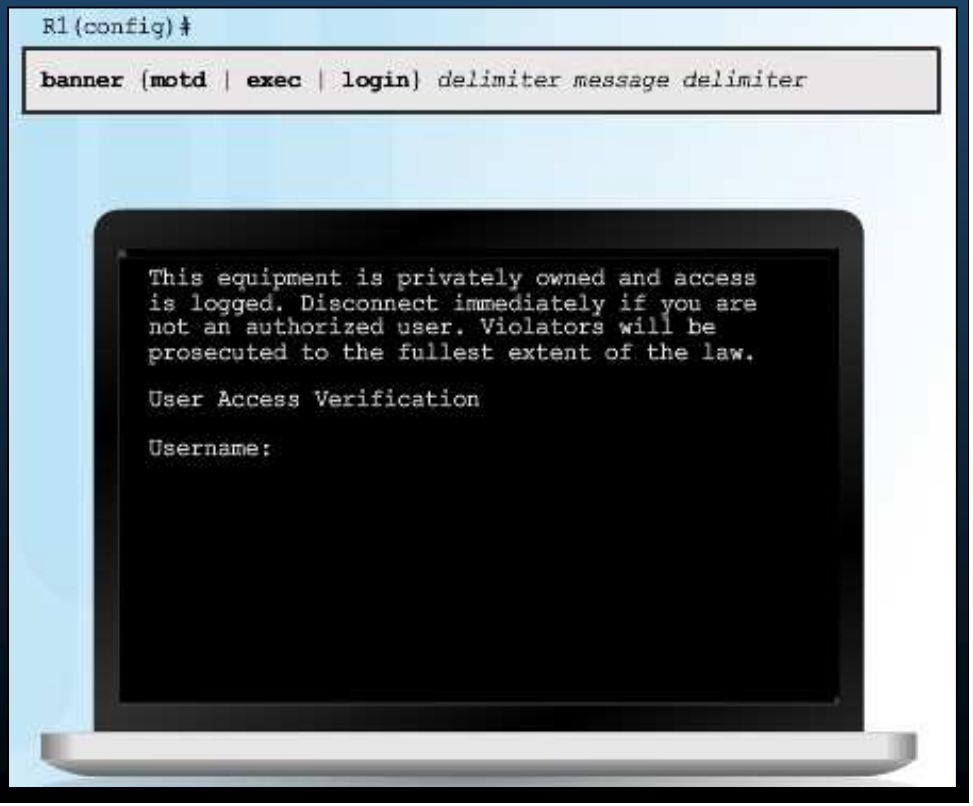
2.1 Asegurado de Dispositivos de Acceso

- Asegurando Lineas de Acceso.
  - Por default AUX y Console no piden contraseña
  - Se puede configurar un password
  - Las líneas solo soportan contraseñas tipo 7.
  - Puede configurarse ingreso por usuarios con `login local`.
  - Habilitar SSH es recomendado siempre para VTYs.

```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

2.1 Asegurado de Dispositivos de Acceso

- Mejora del Proceso de Logueo.
  - Mejoras de seguridad mediante Logueo virtual:
    - Retrasos entre intentos de logueo consecutivos.
    - Deshabilita logueo de host específicos ante sospecha de ataque DoS.
    - Genera syslogs para detección de logueos.
  - Consideraciones adicionales:
    - Configurar ACLs para permitir conexiones de fuentes confiables.
    - Habilitar Banners para proteger desde punto de vista legal.



2.1 Asegurado de Dispositivos de Acceso

- Configuración de Mejoras del Proceso de Logueo.
  - Bloquea el logueo (modo quieto) ciertos segundos cada cantidad de intentos fallidos en un lapso de segundos.

```
R1(config)#
login block-for seconds attempts tries within seconds
```

  - Mapea hacia un a ACL con los hosts permitidos (incluso en modo quieto).

```
R1(config)#
login quiet-mode access-class {acl-name|acl-number}
```

  - Define tiempo de espera entre accesos fallidos:

```
R1(config)#
login delay seconds
```

  - Indica registrar accesos tanto efectivos:

```
R1(config)#
login on-success log [every login]
```

  como fallidos:

```
R1(config)#
login on-failure log [every login]
```

  - Requieren:
    - Uso de base de datos local para autenticar.
  - No aplica para configuración de líneas con solo password.
  - No aplica a conexiones de consola (se asume solo personal autorizado tiene acceso).

2.1 Asegurado de Dispositivos de Acceso

- Habilitación de Mejoras del Proceso de Logueo.
  - Deshabilitadas por default hasta ingresar el comando: `login block-for`.

```
R1(config)# login block-for 120 attempts 5 within 60
```

  - Monitorea logueos y opera en dos modos:
    - Normal: Observación, cuenta cantidad de intentos fallidos en un tiempo.
    - Tranquilo: Si el número de intentos fallidos sobrepasó el límite; bloquea accesos Telnet, SSH y HTTP (incluso válidos).
      - Solo los que cumplan con ACL podrán ingresar.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
```

  - `R(conf)# login block-for` implementa un retraso de 1s entre logueos.
    - Puede alterarse con: `R1(config)# login delay 3`

2.1 Asegurado de Dispositivos de Acceso

- Registrar Intentos Fallidos de Logueo.
  - Tres opciones:

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

Intentos antes de enviar al log
1 - 65535

Generan mensajes syslog

Genera log al superar la razón-umbral

  - Verificación:

```
R1# show login
    A login delay for 10 sec is applied.
    Quiet-Mode access list PERMIT-ADMIN is applied.

    Router enabled to watch for login Attacks.
    If more than 5 login failures occur in 60 sec or less,
    login will be disabled for 120 secs.
```

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username     SourceIPAddr     lPort Count TimeStamp
admin        1.1.2.1          23    5     15:38:54 UTC Wed Dec 10 2008
Admin        10.10.10.10      23    13    15:58:43 UTC Wed Dec 10 2008
admin        10.10.10.10      23    3     15:57:14 UTC Wed Dec 10 2008
cisco        10.10.10.10      23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

```
R1# show login
3 seconds is applied.
list PERMIT-ADMIN is applied.

watch for login Attacks.
ogin failures occur in 60 seconds or
be disabled for 120 seconds.

in Quiet-Mode.
uiet-Mode for  105 seconds.
filtered by applied ACL PERMIT-ADMIN.
```

2.1 Asegurado de Dispositivos de Acceso

- Configuración de SSH.
  - Requisitos:
    - IOS con soporte para SSH
    - Nombre de host único.
    - Dominio de red correctamente configurado.
    - Autenticación local configurada o mediante AAA.

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

2.1 Asegurado de Dispositivos de Acceso

```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.span.com
Key type: RSA KEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB
  A58A1BDB F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620
  ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13
  74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21
  176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301 0001
% Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.span.com.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE
  DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3
  1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE
  9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto key zeroize rsa
% All 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
R1(config)#
```

2.1 Asegurado de Dispositivos de Acceso

- Modificar Configuración de SSH.
  - Verificación y modificación de parámetros configurados:

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
<output omitted>

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
<output omitted>
```

Defaults

2.1 Asegurado de Dispositivos de Acceso

- Conexión a un router por SSH.
  - Verificar que efectivamente el router corra SSH:

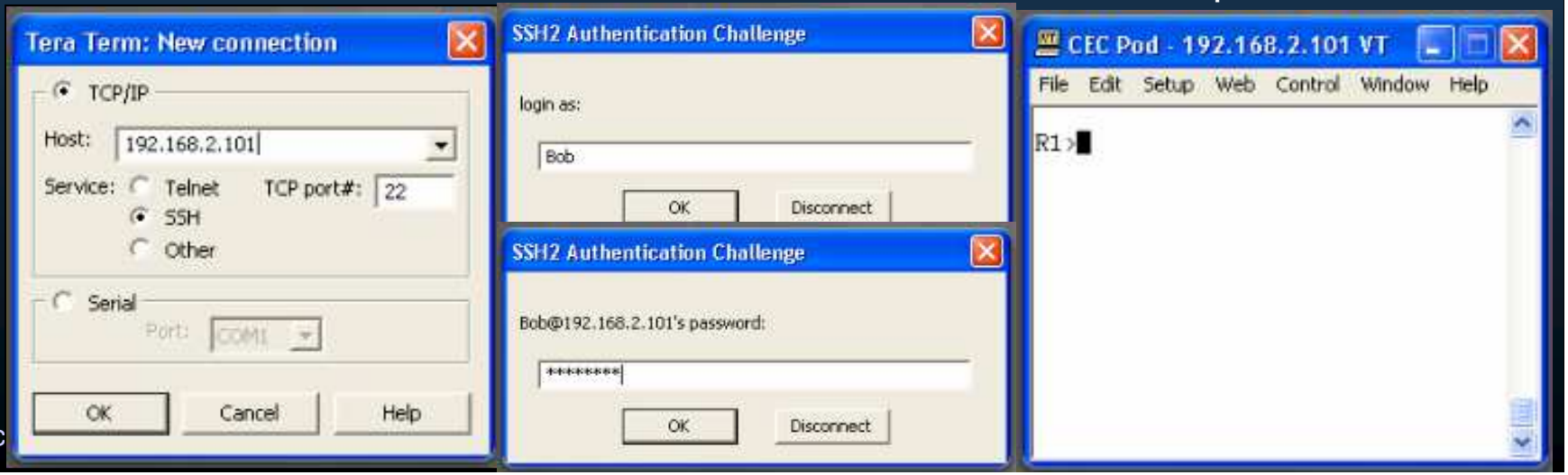
```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```

  - Un router puede fungir como cliente o servidor SSH:

```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

```
R1# show ssh
Connection Version Mode Encryption  Hmac      State              Username
0          2.0     IN   aes128-cbc  hmac-sha1 Session started    Bob
0          2.0     OUT  aes128-cbc  hmac-sha1 Session started    Bob
%No SSHv1 server connections running.
R1#
```

  - Para conectarse a un router servidor ssh desde un host se requiere cliente.



2.2 Asignación de Roles Administrativos

- Limitar Disponibilidad de Comandos.
  - En grandes empresas no todos tienen las mismas tareas o responsabilidades.
  - Niveles para la CLI (quien accede y a que tiene acceso):
    - Nivel 0: privilegios de acceso a nivel de usuario, solo 5 comandos: `disable, enable, exit, help, y logout.`
    - Nivel 1, Modo Usuario: modo por defecto con `prompt>` no permite cambios ni ver el running-config.
    - Niveles 2-14: Privilegios configurables para roles de usuarios, es posible
      ol.
      : se accede mediante el comando `enable`,
      or defecto para `prompt#`.
      ior, se encuentran disponibles en todos los
      superi
  - Para
    el comando `privilege`

Modo se refiere al nivel del prompt

```
configure   Global configuration mode
exec        Exec mode
interface   Interface configuration mode
line        Line configuration mode
router      Router configuration mode
```

Level, es el nivel al que se asignará el privilegio, de 0 a 15

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

2.2 Asignación de Roles Administrativos

- Configuración y Asignación de Niveles de Privilegios.

```
R1# conf t
R1(config)# !Level 5 and SUPPORT user configuration
R1(config)# privilege exec level 5 ping
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt secret cisco5
R1(config)# !Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt secret cisco10
R1(config)# !Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret cisco123
```

Nivel 5: privilegios nivel 1 + ping

Nivel 10: privilegios nivel 5 + reload

Nivel 15: todos los privilegios

Contraseña por nivel (todos los usuarios)

Contraseña por usuario con nivel

- Verificación:

```
R1> enable 5
Password: <cisco5>
R1# show privilege
Current privilege level is 5
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos
!!!!!
Success rate is 100 percent (5/
R1# reload
Translating "reload"

% Bad IP address or host name
Translating "reload"

% Unknown command or computer n
R1#
```

```
R1# enable 10
Password: <cisco10>
R1# show privilege
Current privilege level is 10
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
!!!!!
Success rate is 100 percent (5/5)
R1# reload

System configuration has been mod

R1# show running-config
                ^
% Invalid input detected at '^' m
R1#
```

```
R1# enable 15
Password:
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1979 bytes
!
! Last configuration change at 15:30:07 UTC Tue Feb 17 2015
!
version 15.4
<output omitted>
R1#
```

2.2 Asignación de Roles Administrativos

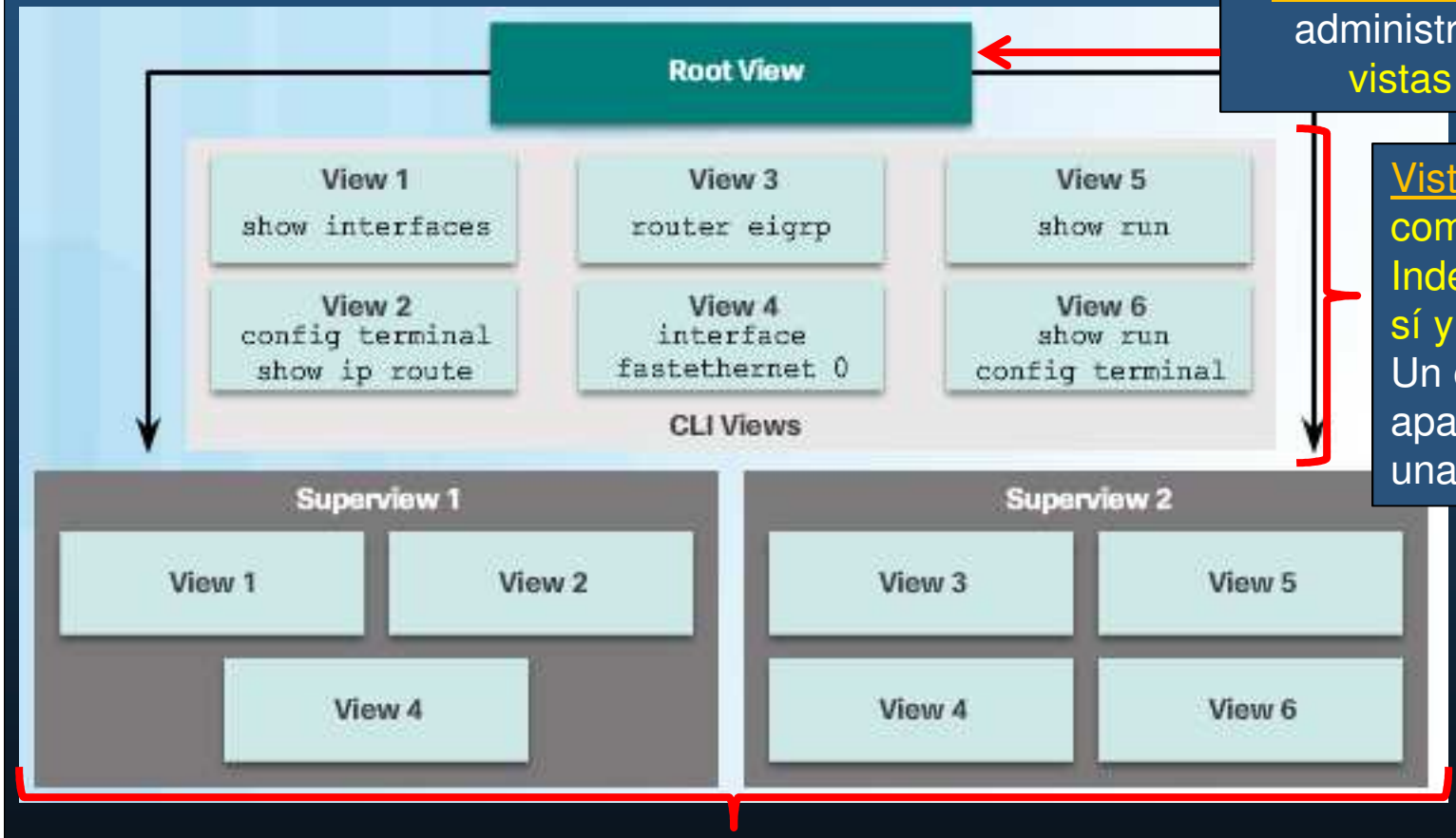
- Limitaciones de los Niveles de Privilegios.
  - No es posible controlar el acceso a interfaces, puertos, ó ranuras de un router.
  - Los privilegios en niveles inferiores siempre se heredan a los superiores.
  - Los comandos colocados a un nivel superior, no están disponibles en los inferiores.
  - Asignar comandos con palabras clave, permite el acceso de todos los comandos con dichas palabras clave.
    - Vgr; Permitir `show ip route` permite todos los comandos `show` y `show ip`.
  - Tedioso crear nivel que tenga casi todos los comandos, pero no todos.

2.2 Asignación de Roles Administrativos

- Acceso a CLI Basado en Roles.
  - Mejora flexibilidad de niveles, disponible desde Cisco IOS Release 12.3(11)T
  - Controla que comandos están disponibles para roles específicos.
  - Permite al administrador crear vistas de la configuración de un router.
    - Cada vista define los comandos disponibles
  - Seguridad: conjunto de comandos accesibles por usuario.
    - Acceso a usuarios solo por determinados puertos/interfaces.
    - Evita que usuarios colecten información de configuraciones a las que no tienen acceso.
  - Disponibilidad: Previene ejecución no deseada de comandos no autorizados.
  - Eficiencia Operacional: Configuración aparentemente sencilla (solo a lo que tienen acceso). La ayuda solo muestra lo permitido.

2.2 Asignación de Roles Administrativos

- Vistas Basadas en Roles.



Vista Raíz: Requerida por el administrador para definir vistas y supervistas

Vistas: Conjunto de comandos disponibles. Independientes entre sí y sin jerarquía. Un comando puede aparecer en mas de una vista

SuperVistas: Conjunto de vistas (no de comandos) usadas por administradores para no asignar a usuarios, vistas una por una.

2.2 Asignación de Roles Administrativos

- Características de las Supervistas.
  - Una Supervista puede ser compartida por multiples supervisores
  - No se pueden especificar comandos para Supervistas.
  - Usuarios logueados a una supervista pueden utilizar todos los comandos definidos para cada una de las vistas que conforman la supervista.
  - Cada supervista tiene una contraseña utilizada para switchear entre supervistas.
  - Eliminar una supervista, no elimina las vistas asociadas.

2.2 Asignación de Roles Administrativos

- Configuración de Vistas Basadas en Roles.
  - Habilitar AAA: `R(config)#aaa new-model`
  - Loguearse como administrador a la vista raíz: `R# enable view [view-name]`
    - `view-name` indica la vista a acceder, si se omite se considera la vista `root`

enable.

rser view <*view-name*> Max. 15 vistas.

```
R2(config)# aaa new-model
R2(config)#
R2(config)# parser view SHOWVIEW
R2(config-view)# secret cisco
R2(config-view)# commands exec include show
R2(config-view)# exit
R2(config)#
R2(config)# parser view VERIFYVIEW
R2(config-view)# secret cisco5
R2(config-view)# commands exec include ping
R2(config-view)# exit
R2(config)#
R2(config)# parser view REBOOTVIEW
R2(config-view)# secret cisco10
R2(config-view)# commands exec include reload
R2(config-view)# end
R2#
```

```
R2# show running-config | section parser
parser view SHOWVIEW
 secret 5 $1$4c8S$8ayWlp1brumavcCek7OUz.
 commands exec include show
parser view VERIFYVIEW
 secret 5 $1$mV.n$W199F.nQQQvuP7QiEzE.40
 commands exec include ping
parser view REBOOTVIEW
 secret 5 $1$BBYq$L6prAiM.wrcuGbst/9JY51
 commands exec include reload
R2#
```

`R(conf-view)# exit`

2.2 Asignación de Roles Administrativos

- Configuración de Supervistas.
  - El administrador debe estar en la vista raiz:
    `R# enable view root`

```
R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIE
% Invalid view name SHOWVIE

R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view JR-ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view REBOOTVIEW
R1(config-view)# exit
R1(config)#
```

```
R1# show running-config
<output omitted>

!
parser view SUPPORT superview
 secret 5 $1$Vp1O$BBB1N68Z2ekr/aLHledts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
!
```

2.2 Asignación de Roles Administrativos

- Verificación de Vistas Basadas en Roles.

```
R1# enable view USER
Password: <cisco>

R1# ?
Exec commands:
  <0-0>/<0-4>   Enter card slot/s
  do-exec       Mode-independent
  enable        Turn on privilege
  exit          Exit from the EXE
  show          Show running syst

R1# show ?
  banner      Display banner ini
  flash0:     display informatic
  flash1:     display informatic
  flash:      display informatic
  parser      Display parser ini
  usbflash0:  display informatic

R1# show
```

```
R1# show parser view
Current view is 'JR-ADMIN'

R1# enable view
Password:

R1# show parser view
Current view is 'root'

R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------
R1#
```

```
R1# enable view SUPPORT
Password: <cisco1>

r card slot/sublot number
-independent "do-exec" prefix support
 on privileged commands
 from the EXEC
 echo messages
 running system information
```

```
ADMIN

r card slot/sublot number
-independent "do-exec" prefix support
 on privileged commands
 from the EXEC
 echo messages
 and perform a cold restart
 running system information

R1#
```

2.3 Monitoreo y Administración de Dispositivos

- Característica de Configuración Elástica (Resiliente).
  - Creación de imagen de running-config y asegurada en almacenamiento persistente.
    - Permite una rápida recuperación, si se formatea la flash o nvram.
      - Respaldo del IOS y startup_config
      - No es accesibles por el usuario.
      - Primer conjunto de búsqueda al arranque.
      - Identifica discrepancias
      - Solo se puede deshabilitar mediante acceso por consola.
      - Solo disponible para tecnología Flash PCMCIA ATA.

2.3 Monitoreo y Administración de Dispositivos

- Habilitación de la Característica de Configuración Resiliente.

```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:.runcfg-20150218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2015
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2015
Secure archive flash0:.runcfg-20150218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

Habilita Característica Resiliente para IOS

Habilita/Actualiza Característica Resiliente para `startup-config`

Para deshabilita característica resilientes se usa la forma `no` de los comandos previos.
Los archivos asegurados no se muestran en la salida del comando `dir`.

2.3 Monitoreo y Administración de Dispositivos

- Restaurar Imagen del Conjunto de Arranque Primario.

Reiniciar y entrar en modo ROMmon

```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4       75551300  -rw-     c1900-universalk9-mz.SPA.154-3.M2.bin
<output omitted>
```

Localizar el IOS asegurado.

Iniciar con el IOS asegurado.

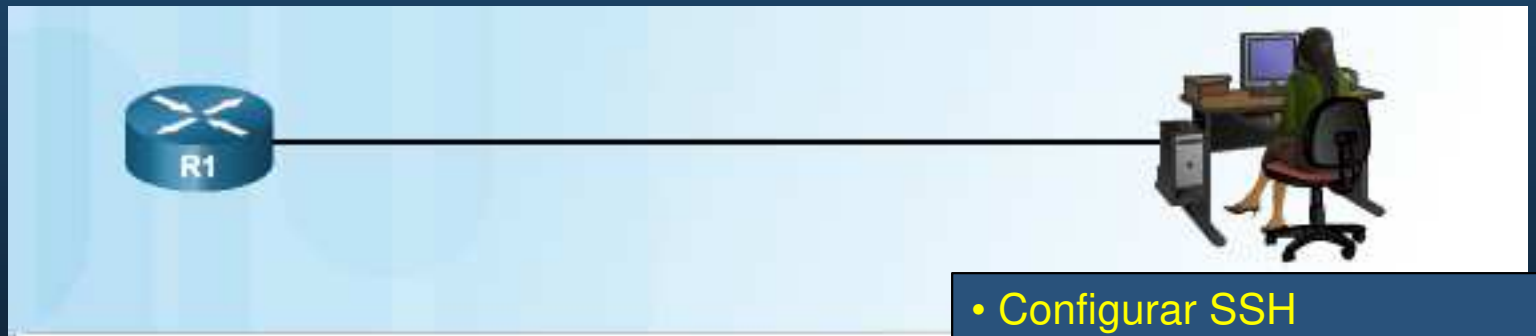
```
rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin
<Router reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#
```

Generar un archivo con el `starup-config` asegurado.

Copiar el archivo generado a la RAM.

2.3 Monitoreo y Administración de Dispositivos

- Configuración de Copia Segura.
  - Uso de SCP para copiar archivos de la imagen de arranque resiliente.
  - Configuración del servidor SCP en el router:

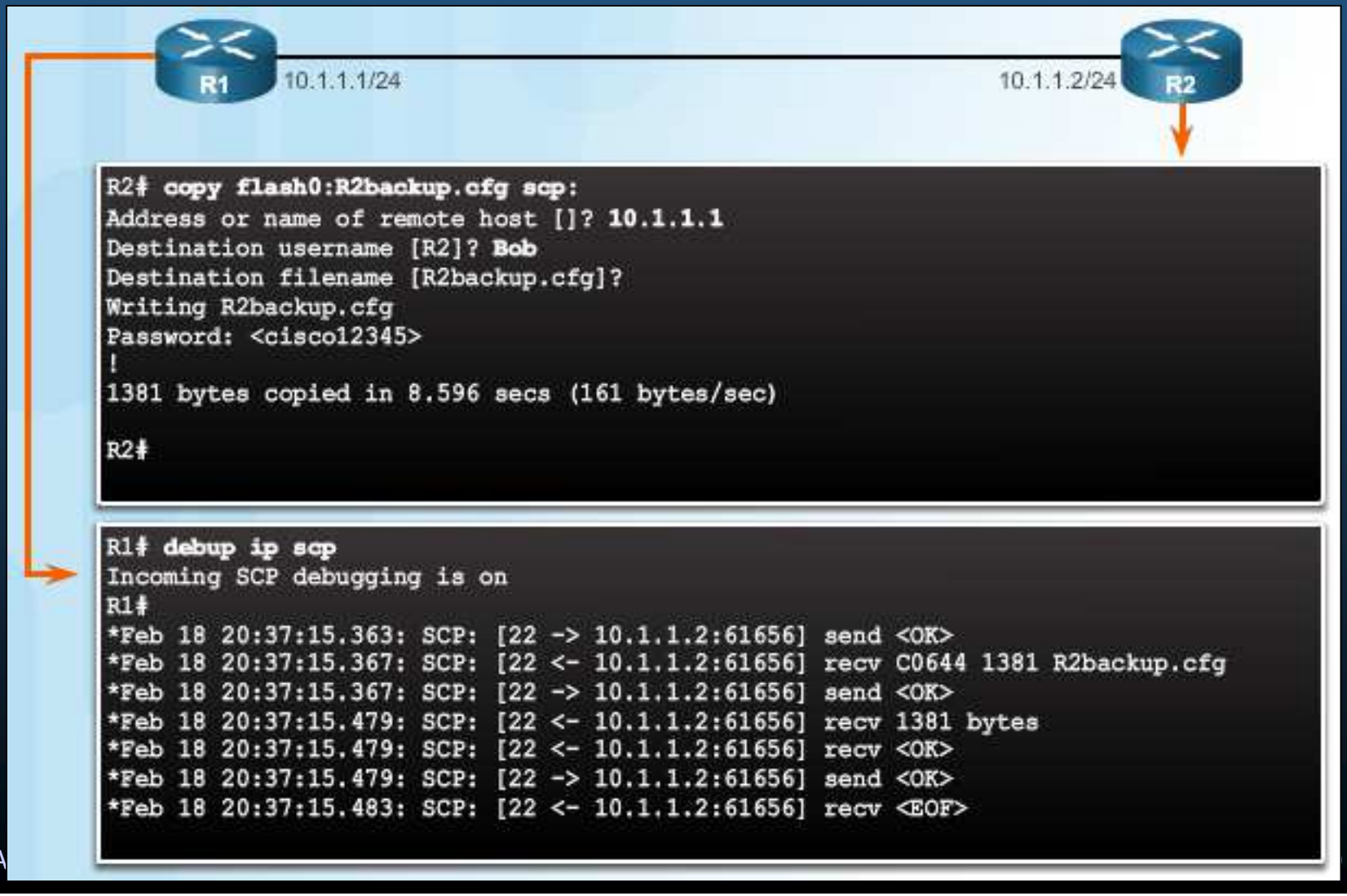



```
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Bob privilege 15 algorithm-type scrypt secret cisco12345
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# aaa authorization exec default local
R1(config)# ip scp server enable
```

- Configurar SSH
- Habilitar AAA.
- Especificar uso de base local para autenticar.
- Autorizar uso de comandos.
- Habilitar servidor SCP.

2.3 Monitoreo y Administración de Dispositivos

- Uso de SCP.



2.3 Monitoreo y Administración de Dispositivos

- Recuperación de Contraseñas en un Router.
  1. Conectarse al Router mediante el Puerto de Consola.
  2. Registrar el valor actual del registro.
  3. Ingresar al modo ROMmon (`Break` al arranque).
  4. Establecer registro para ignorar startup-config (**`0x2142`**).
  5. Reiniciar sin entrar a configuración inicial (`Ctrl+C`).
  6. Copiar `startup-config` a `running-config`.
  7. Cambiar contraseñas (`enable secret`).
  8. Habilitar interfaces.
  9. Regresar el valor del registro original (`0x2102`)
  10. Guardar la configuración.

Ligeras variaciones por modelo :
http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/6130-index.html

2.3 Monitoreo y Administración de Dispositivos

- Deshabilitar Recuperación de Contraseñas.
  - Deshabilitar acceso a ROMmon para evitar riesgos por acceso físico no autorizado al dispositivo.

```
R1(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
R1(config)#
```

  - Una vez deshabilitado, se muestra en el `running-config`. Así como al iniciar el dispositivo.

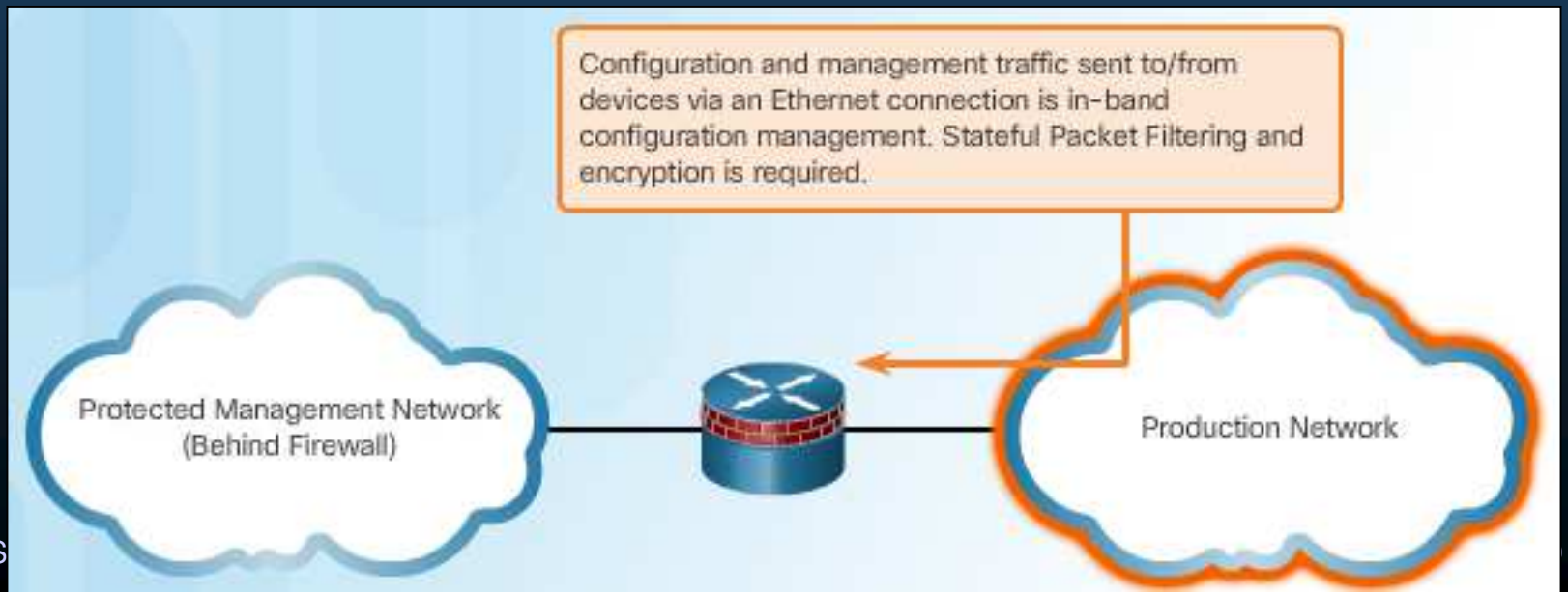
```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size:0xcb80
```

```
R1# show running-config
Building configuration...

Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```

PRECAUCIÓN: Sin ROMmon, no podrá utilizarse Xmodem, para restaurar el IOS
Alternativa: Controlar acceso: solo personal autorizado.

2.3 Monitoreo y Administración de Dispositivos

- Determinar el Tipo de Acceso de Administración.
  - En empresas grandes, la administración puede se caótica.
    - Datos pueden verse en tiempo real, por demanda o reportes programados.
  - Dispositivos generan logs constantemente al host de administración.
    - En Banda: Por redes públicas (solo cuando OOB no disponible).
    - Fuera de Banda (OOB): Por enlaces dedicados y asegurados al máximo(preferible).

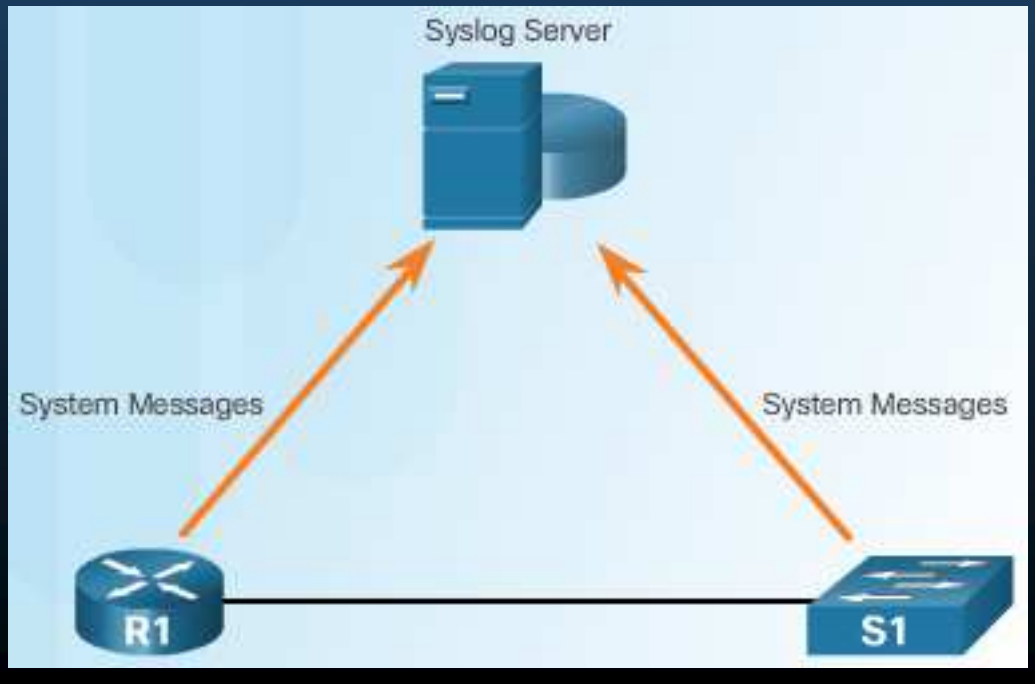


2.3 Monitoreo y Administración de Dispositivos

- Accesos en Banda y fuera de Banda.
  - Fuera de Banda
    - Provee el mas alto nivel de seguridad.
    - Mitiga el riesgo del paso de protocolos de administración en redes de producción.
  - En Banda:
    - Aplicar solo a dispositivos que deben ser monitoreados/administrados.
    - Utilice IPSec, SSH o SSL.
    - Decida si el canal de administración debe estar abierto todo el tiempo.

2.3 Monitoreo y Administración de Dispositivos

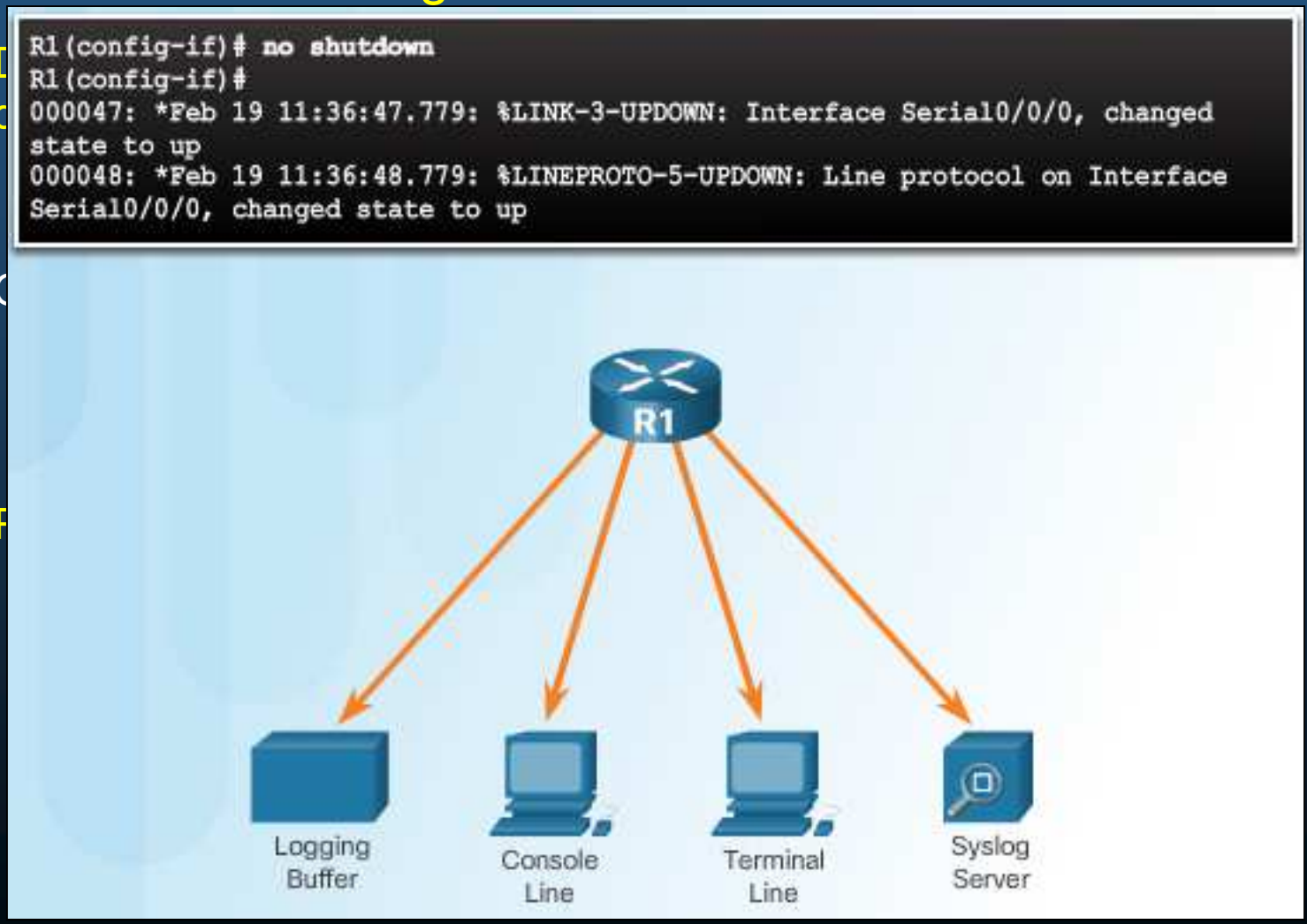
- Introducción a SYSLog (RFC 5424).
  - Envía notificaciones UDP al puerto 514.
  - Tres principales funciones:
    - Recolectar logs.
    - Seleccionar tipos de logs a capturar y a ignorar.
    - Especificar almacenamiento de logs capturados.



2.3 Monitoreo y Administración de Dispositivos

- Operación de SYSLog.
  - D eso local
  - C aces,
  - F

```
R1(config-if)# no shutdown
R1(config-if)#
000047: *Feb 19 11:36:47.779: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```



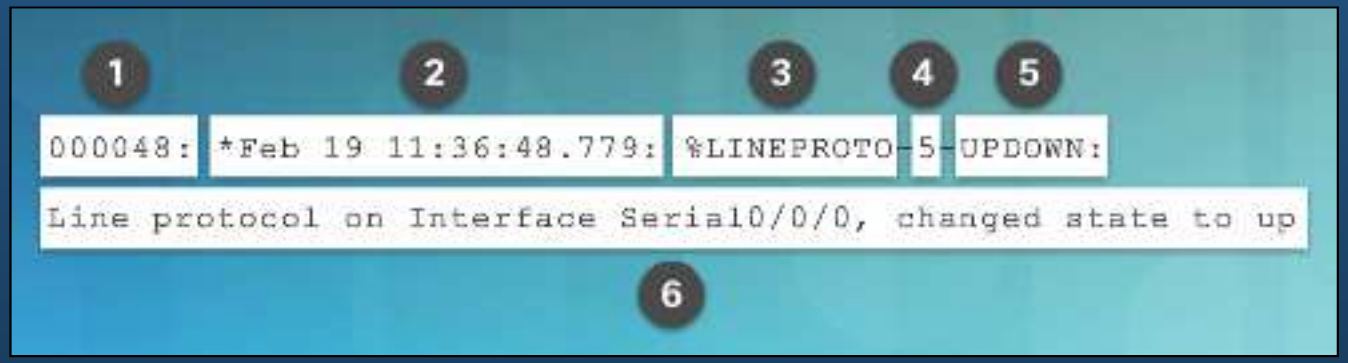
2.3 Monitoreo y Administración de Dispositivos

- Mensajes SYSLog.

Nivel	Palabra Clave	Descripción	Definición
0	Emergencias	Sistema Inestable, condición de pánico	LOG_EMERG
1	Alertas	Acción Inmediata / Corrección Necesaria	LOG_ALERT
2	Crítico	Existen condiciones críticas requieren atención	LOG_CRIT
3	Errores	Existen condiciones de error en dispositivo	LOG_ERR
4	Advertencia	Existen condiciones advertencia a ser evaluadas	LOG_CRIT
5	Notificaciones	Condiciones requieren ser manejadas (no errores)	LOG_NOTICE
6	Informativo	Solo mensajes informativos de eventos normales	LOG_INFO
7	Debugueo	Mensajes de debugueo	LOG_DEBUG

2.3 Monitoreo y Administración de Dispositivos

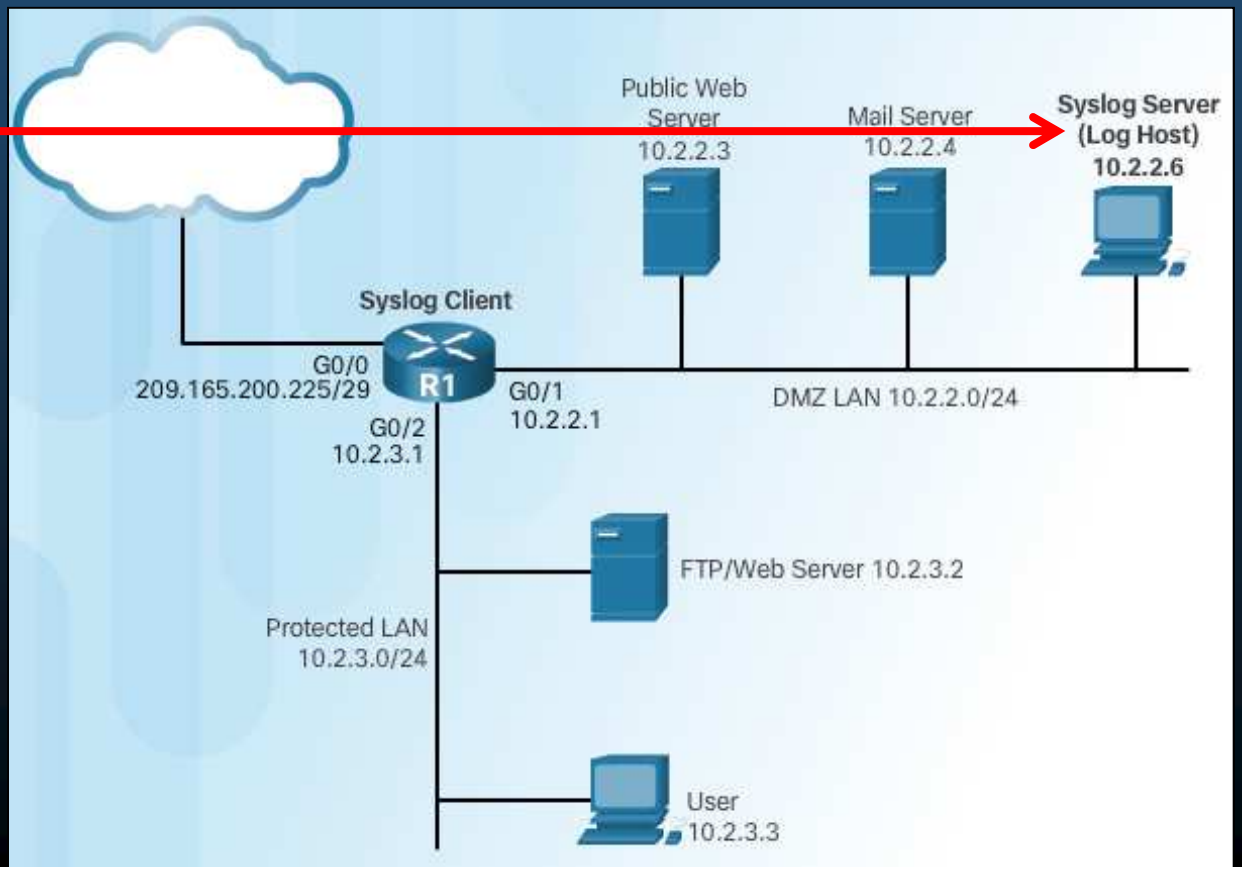
- Elementos de Mensajes SYSLog.



	Columna 1	Columna 2
1	`seq no`	Estampa logs con número secuencial `service sequence-numbre`
2	`timestamp`	Despliega Fecha/Hora si `service timestamp` está configurado
3	`facility`	Indica el origen o causa del mensaje del sistema.
4	`severity`	Niveles del 0 al 7
5	`MNEMONIC`	Cadena de texto que identifica el mensaje brevemente
6	`description`	Cadena de texto que detalla el reporte

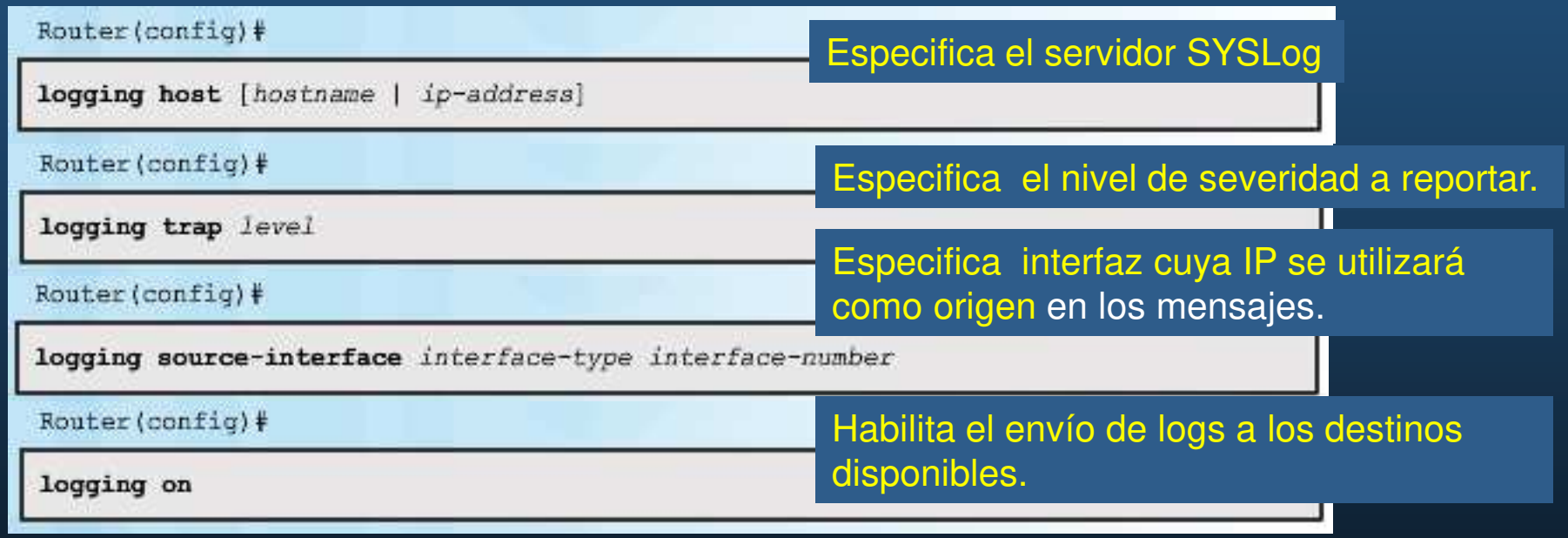
2.3 Monitoreo y Administración de Dispositivos

- Sistemas SYSLog.
  - Contienen dos tipos de sistemas.
    - Servidores SYSLog: Registran logs de hosts.
    - Clientes SYSLog: equipos que generan o reenvían mensajes log a servidores.



2.3 Monitoreo y Administración de Dispositivos

- Configuración de un Sistema de Logueo.



2.3 Monitoreo y Administración de Dispositivos

- Ej

```
R1(config)# logging host 10.2.2.6
000051: *Feb 19 12:45:32.491: %SYS-6-LOGGINGHOST_STARTSTOP:
Logging to host 10.2.2.6 port 514 started - CLI initiated
R1(config)# logging trap informational
R1(config)# logging source-interface gigabitethernet0/1
R1(config)# logging on
R1(config)# exit
000052: *Feb 19 12:46:07.151: %SYS-5-CONFIG_I: Configured from console by console
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns,
xml disabled, filtering disabled)
<output omitted>
     Trap logging: level informational, 55 message lines logged
        Logging to 10.2.2.6  (udp port 514, audit disabled,
              link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
        GigabitEthernet0/1

Log Buffer (8192 bytes):
<output omitted>
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial0/0/0, changed state to up
000049: *Feb 19 11:43:25.043: %SYS-5-CONFIG_I: Configured from console by console
000050: *Feb 19 12:45:31.491: %SYS-6-LOGGINGHOST_STARTSTOP:
Logging to host 10.2.2.6 port 0 CLI Request Triggered
000051: *Feb 19 12:45:32.491: %SYS-6-LOGGINGHOST_STARTSTOP:
Logging to host 10.2.2.6 port 514 started - CLI initiated
000052: *Feb 19 12:46:07.151: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

2.3 Monitoreo y Administración de Dispositivos

- Introducción a SNMP.
  - Herramienta de administración y monitoreo en redes IP.
  - Tres elementos relevantes sobre NMS (Network Management System)
    - Administrador SNMP
    - Agentes SNMP (nodo administrado)
    - Base de Información de Administración (MIB)
  - Utiliza UDP
  - Agentes escuchan puerto 161
    - Pueden ser administrados / enviar notificaciones.
  - Administradores escuchan puerto 162
    - Pueden solicitar información, cambio de configuraciones.

2.3 Monitoreo y Administración de Dispositivos

- Base de Información de Administración (MIB).
  - Mer
    -

Tools & Resources

SNMP Object Navigator

HOME
SUPPORT
TOOLS & RESOURCES
SNMP Object Navigator

TRANSLATE/BROWSE | SEARCH | DOWNLOAD MIBS | MIB SUPPORT - SW

Translate | Browse The Object Tree

Translate OID into object name or object name into OID to receive object details

Enter OID or object name: 1.3.6.1.2.1.4.21 (examples - OID: 1.3.6.1.4.1.9.9.27 Object Name: ifIndex)

Translate

Object Information

Specific Object Information

Object	ipRouteTable
OID	1.3.6.1.2.1.4.21
Type	SEQUENCE
Permission	not-accessible
Status	mandatory
MIB	RFC1213-MIB - View Supporting Images
Description	This entity's IP Routing table.

OID Tree

You are currently viewing your object with 2 levels of hierarchy above your object.

iso (1) . org (3) . dod (6) . internet (1) . mgmt (2)

- mib-2 (1)
  - system (1)
  - interfaces (2)
  - at (3)

estándares

Cisco OID
https://ss

o mgmt (9)

ash group (10)

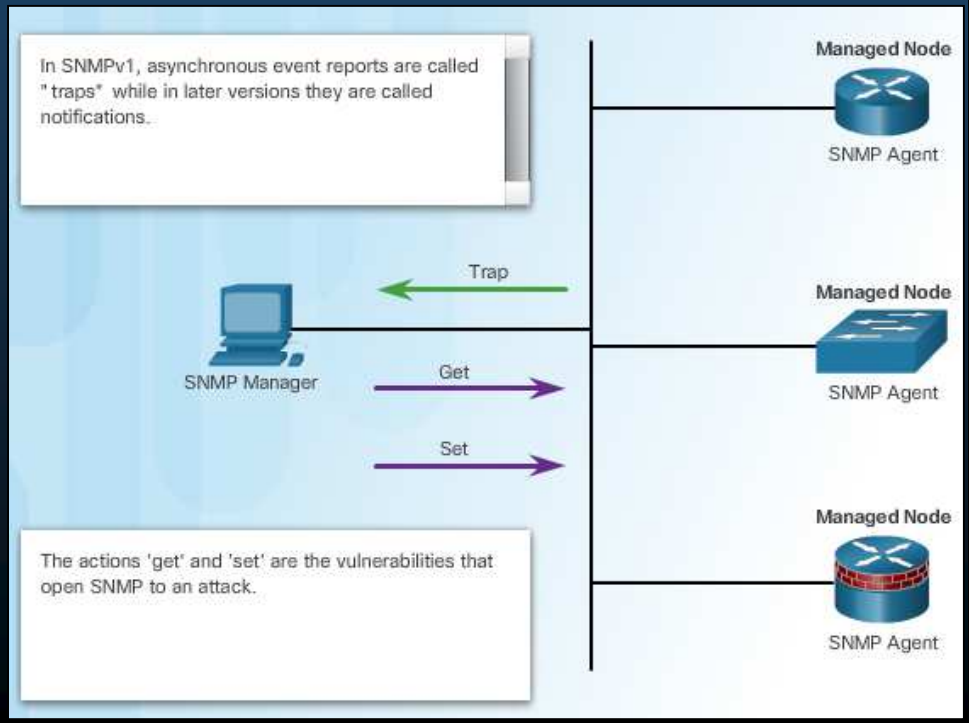
2.3 Monitoreo y Administración de Dispositivos

- Versiones SNMP.

Modelo	Nivel	Autenticación	Encriptación	Resultado
SNMPv1	NoAuthNoPriv	Cadena de la Comunidad	No	Utiliza cadena de la comunidad para autenticar.
SNMPv2c	NoAuthNoPriv	Cadena de la Comunidad	No	Utiliza cadena de la comunidad para autenticar.
SNMPv3	NoAuthNoPriv	Nombre de Usuario	No	Utiliza comparación de nombres de usuario para autenticar.
SNMPv3	AuthNoPriv	MD5 o SHA	No	Provee autenticación basada en HMAC-MD5 o HMAC-SHA.
SNMPv3	AuthPriv	MD5 o SHA	DES o AES	Provee autenticación basada en HMAC-MD5 o HMAC-SHA. Modelo de Seguridad Basado en Usuario (USM)mediante: DES 56bits, 3DES de 168bits, AES 128-256bits.

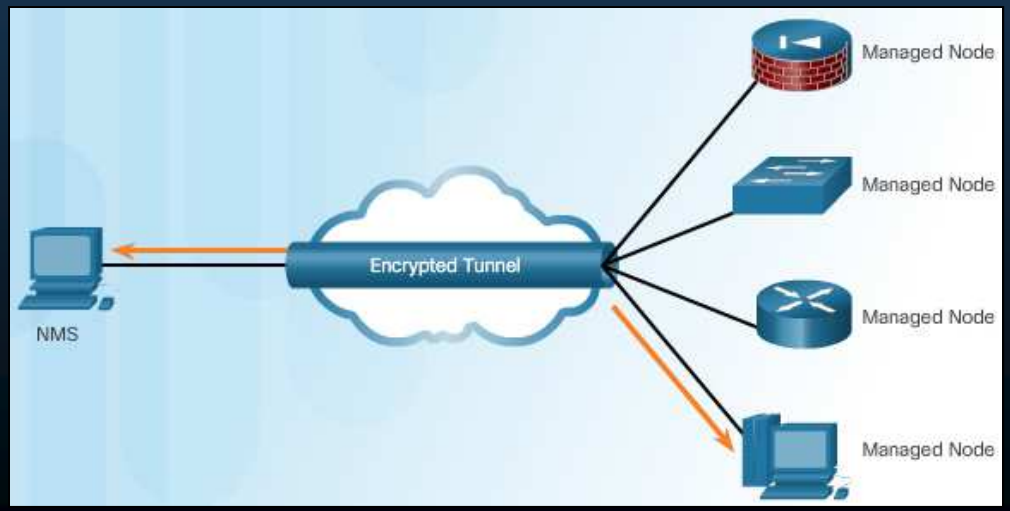
2.3 Monitoreo y Administración de Dispositivos

- Vulnerabilidades SNMP.
  - Al menos un nodo debe correr el software de administración SNMP.
  - Los dispositivos a ser administrados corren el agente SNMP.
    - Pueden ser encuestados mediante comandos `get`.
    - Pueden ser manipulados mediante comandos `set`.
    - Pueden ser instruidos para enviar notificaciones o `traps`.
    - SNMPv1 y SNMPv2c no autentican ni cifran.



2.3 Monitoreo y Administración de Dispositivos

- SNMPv3.
  - Autentica y Cifra.
  - Tres características de seguridad:
    - Autenticación e integridad de mensajes: verifica que un paquete provenga de una fuente confiable y no haya sido alterado.
    - Encriptación: Busca prevenir que los paqueteas sean vistos por equipos no autorizados.
    - Control de acceso: restringe acceso a ciertas porciones o datos.



2.3 Monitoreo y Administración de Dispositivos

- Configuración de SNMPv3.

Paso 1: Configurar una ACL para permitir la red de administración protegida.

```
Router(config)# ip access-list standard acl-name
Router(config-std-nacl)# permit source_net
```

Paso 2: Configurar una vista SNMP (para especificar lo que SNMP podrá ver).

```
Router(config)# snmp-server view view-name oid-tree
```

Paso 3: Configurar un grupo SNMP
(nombre, versión3, autenticar&encriptar = priv, vista Paso2, ACL Paso1).

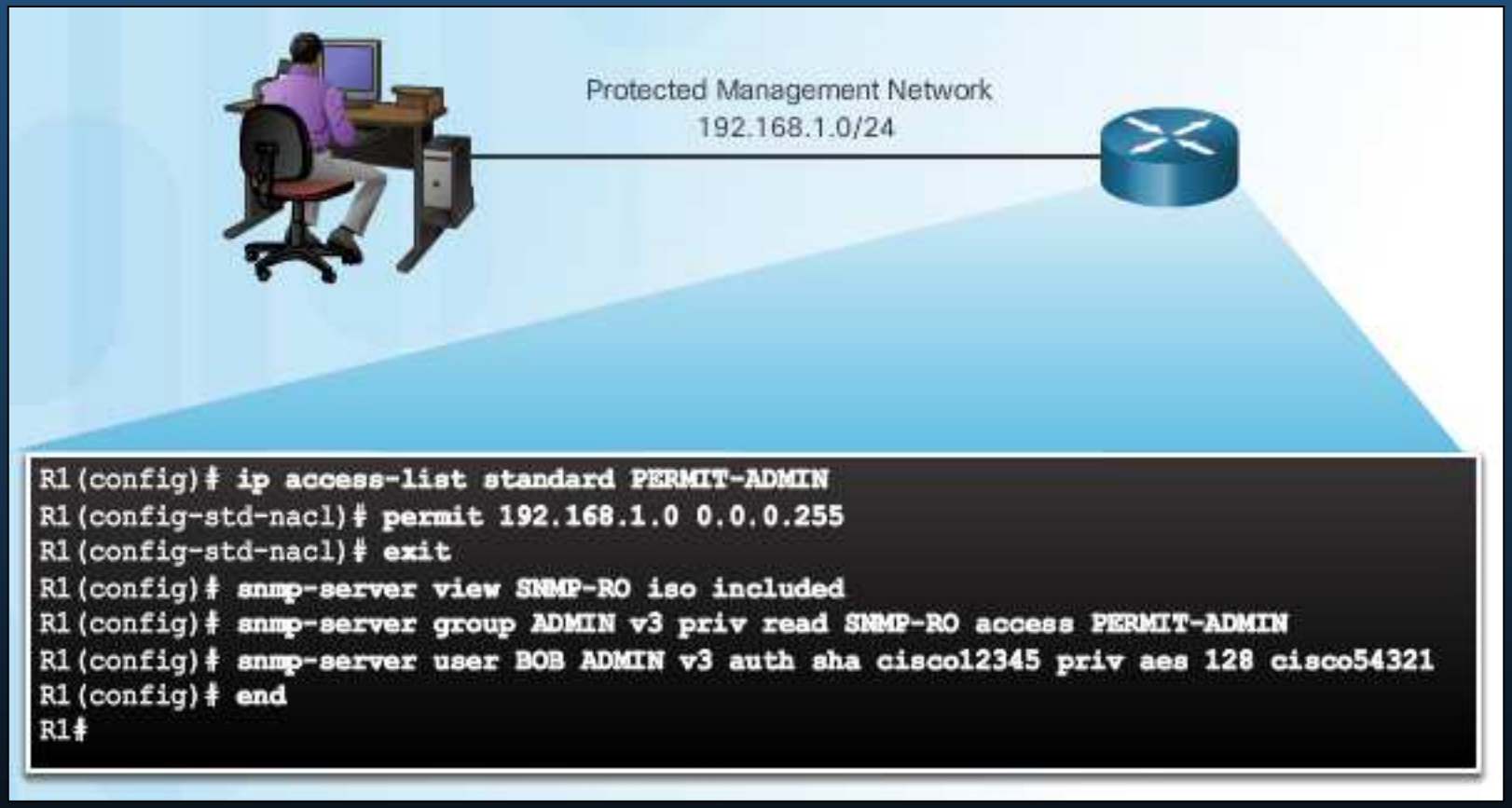
```
Router(config)# snmp-server group group-name v3
priv read view-name access [acl-number | acl-name]
```

Paso 4: Configurar un usuario como miembro del grupo SNMP
(nombre usuario, versión3, autenticar md5/sha, encriptar = priv + tipo, pass).

```
Router(config)# snmp-server user username group-name v3
auth {md5 | sha} auth-password priv {des | 3des | aes
{128 | 192 | 256}} privpassword
```

2.3 Monitoreo y Administración de Dispositivos

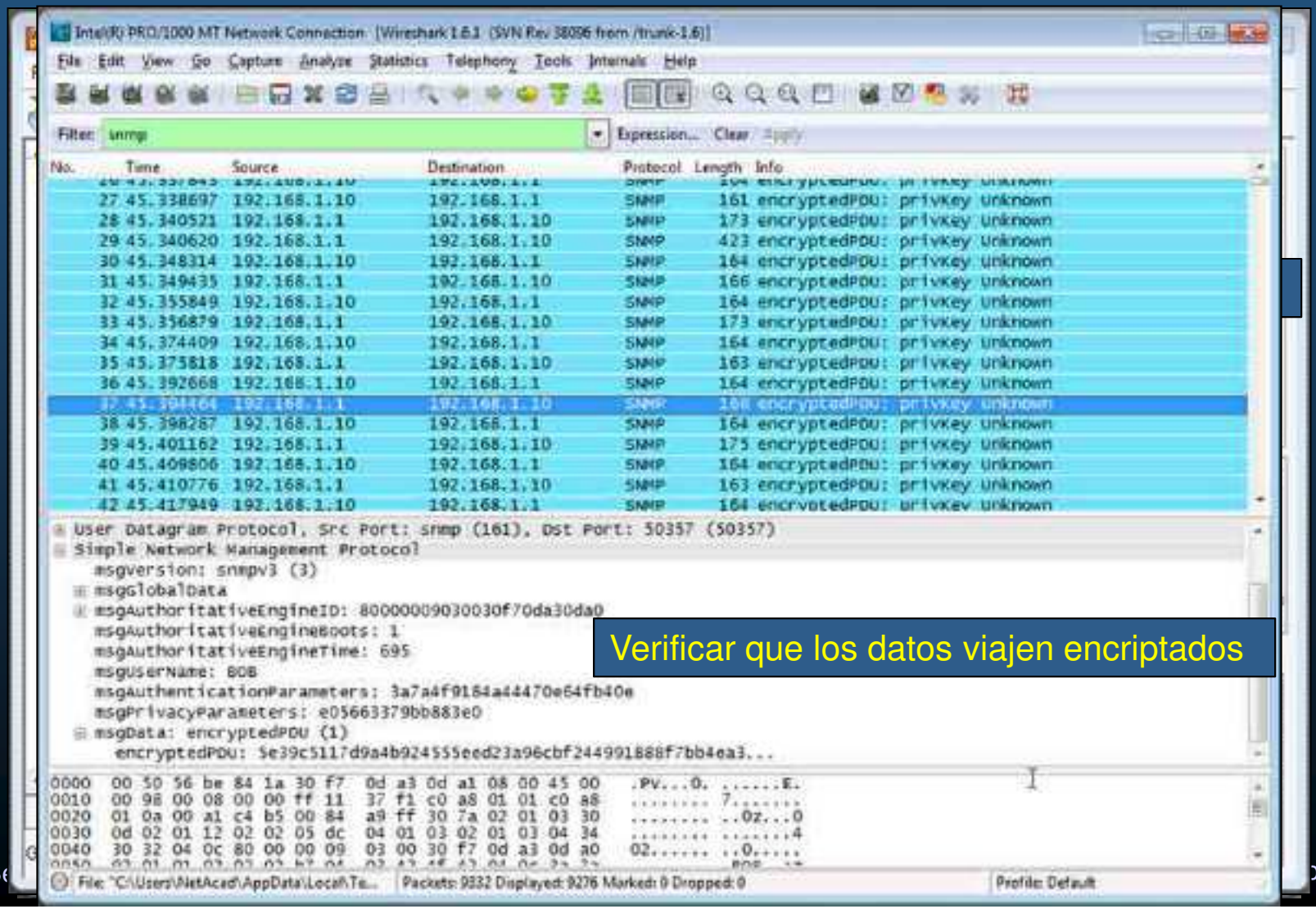
- Ejemplo de SNMPv3.




```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
R1(config)# end
R1#
```

2.3 Monitoreo y Administración de Dispositivos

- Verificación de SNMPv3.



2.3 Monitoreo y Administración de Dispositivos

- Network Time Protocol (NTP).
  - Cuestiones relacionadas con seguridad de red requieren timestamps.
  - NTP sincroniza relojes de dispositivos.
    - Configuración Manual de fecha y hora:

```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

    - Configuración mediante NTP: permite a clientes actualizar fecha y hora desde un servidor público o privado.
      - NTP utiliza UDPs por en puerto 123 (RFC 1305)

2.3 Monitoreo y Administración de Dispositivos

- Servidor NTP.
  - Implementando un servidor privado:
    - Fuente confiable y segura.
    - Suceptible a DoS, mediante solicitudes de cambio de hora.
  - Implementación de un servidor público:
    - Implica permitir paquetes inseguros en el firewall.
    - Puede no requerir autenticación (no confiable).
  - El servidor (denominado maestro), del que los clientes escuchan mensajes.

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

  - Los clientes pueden realizar solicitudes de información al master:

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

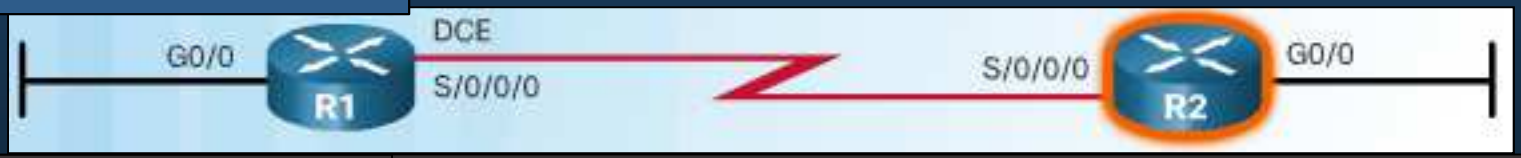
2.3 Monitoreo y Administración de Dispositivos

- Servidor NTP (continuación).
  - En una LAN se puede indicar a los dispositivos enviar broadcasts NTP:

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

    - Reduce la complejidad de configuración.
    - Decrementa la precisión de la sincronización de la hora.

Ejemplo:
NTP Master: 10.10.10.1




```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^Z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```

```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^Z
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.0000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCF2253E.5DC2A53B (13:01:50.366 UTC Tue Dec 16 2008) clock
offset is 0.3072 msec, root delay is 23.41 msec
root dispersion is 0.38 msec, peer dispersion is 0.05 msec
R2#
```

2.3 Monitoreo y Administración de Dispositivos

- Autenticación NTP (NTPv3 y posteriores).

```
R2# show ntp associations detail
10.10.10.1 configured, our_master, sane, valid, stratum 2
ref ID 127.127.7.1, time CCF29760.A8F4DB7D (21:08:48.659 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 17, sync dist 1886.810
delay 23.41 msec, offset 0.9618 msec, dispersion 1875.08
precision 2**18, version 3
org time CCF2979B.8E2195E9 (21:09:47.555 UTC Tue Dec 16 2008)
rcv time CCF2979B.90E1A99D (21:09:47.565 UTC Tue Dec 16 2008)
xmt time CCF2979B.8AE1EA33 (21:09:47.542 UTC Tue Dec 16 2008)
filtdelay =    23.41   23.47   23.61   23.41    0.00    0.00    0.00    0.00
filtoffset =    0.96    0.94    0.94    0.66    0.00    0.00    0.00    0.00
filterror =     0.02    0.99    1.97    2.94 16000.0 16000.0 16000.0 16000.0

R2# conf t
R2(config)# ntp authenticate
R2(config)# ntp authentication-key 1 md5 cisco123
R2(config)# ntp trusted-key 1
R2(config)# ^Z
R2# show ntp associations detail | include 10.10.10.1
10.10.10.1 configured, our_master, sane, valid, stratum 16
R2#


R2# show ntp associations detail | include 10.10.10.1
10.10.10.1 configured, authenticated, our_master, sane, valid, stratum 2
R2#
```

2.4 Características de Seguridad Automáticas

- Cisco Discovery Protocol (CDP) Y Link Layer Discovery Protocol (LLP).
  - Servicios de Cisco para simplificar configuraciones.
    - CDP Habilitado por defecto.
  - Pueden volver vulnerable a un equipo (Usar con Precaución).

2.4 Características de Seguridad Automáticas

Feature	Default	
Cisco Discovery Protocol (CDP)	Enabled	Deshabilitar si no se usa.
Link Layer Discovery Protocol (LLDP)	Disabled	
Configuration autoloading	Disabled	
FTP server	Disabled	
TFTP server	Disabled	
Network Time Protocol (NTP) service	Disabled	
Packet assembler/disassembler (PAD) service	Enabled	Deshabilitar si no se usa.
TCP and User Datagram Protocol (UDP) minor services	Enabled in versions 11	Deshabilitar si no se usa.
Maintenance Operation Protocol (MOP) service	Enabled on most Ethernet interfaces	Deshabilitar si no se usa.
Simple Network Management Protocol (SNMP)	Enabled	Deshabilitar si no se usa / Restringir.
HTTP or HTTPS configuration and monitoring	Setting is	Deshabilitar si no se usa / Restringir.
Domain Name System (DNS)	Enabled	Deshabilitar si no se usa / Configurar.
Internet Control Message Protocol (ICMP) redirects	Enabled	Deshabilitar si no se usa.
IP source routing	Enabled	Deshabilitar si no se usa.
Finger service	Enabled	Deshabilitar si no se usa.
ICMP unreachable notifications	Enabled	Deshabilitar en interfaces públicas.
ICMP mask reply	Disabled	
IP identification service	Enabled	Deshabilitar si no se usa.
TCP keepalives	Disabled	Habilitar para prevenir DoS.
Gratuitous ARP (GARP)	Enabled	Deshabilitar si no se usa.
Proxy ARP	Enabled	Deshabilitar si no se usa.

nerarse.

2.4 Características de Seguridad Automáticas

- Cisco AutoSecure (IOS v12.3+).
  - Script de CLI.
    - Hace recomendaciones para corregir vulnerabilidades y asegurar.
    - Modifica la configuración de un router.
    - Puede bloquear funciones del
      - BootP Seguro, CDP, FTP, TF
        source routing, Finger, passw
        ARP, redirect broadcasts.
      - Notificaciones Legales media
      - Asegurar contraseñas (secre
      - Asegurar NTP.
      - Asegurar accesos SSH.
      - Servicios de Intercepción TC
    - Puede bloquear funciones y se
      - Cisco Express Forwarding (C
      - Filtrado de tráfico con ACLs
      - Firewall de inspección para protocolos comunes.

```
R1# auto secure
  --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
 of the router but it will not make router
 absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.

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]:yes
```

2.4 Características de Seguridad Automáticas

- Uso de Cisco AutoSecure.
  - Comando del modo privilegiado.

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

```
R1# auto secure ?
  firewall        AutoSecure Firewall
  forwarding      Secure Forwarding
  full            Interactive full
  login           AutoSecure Login
  management      Secure Management
  no-interact     Non-interactive
  ntp             AutoSecure NTP
  ssh             AutoSecure SSH
  tcp-intercept   AutoSecure TCP
  <cr>

R1#
```

    - Modo interactivo:
      - Pregunta que servicios/funciones habilitar/deshabilitar (por defecto).
    - Modo no interactivo:
      - Implementa recomendaciones de Cisco.
    - Modo por planos:
      - Puede asegurar solo uno u otro plano (`management` / `forwarding`).
    - Modo por servicios/funciones.
      - Puede indicarse el servicio/función a asegurar.

2.4 Características de Seguridad Automáticas

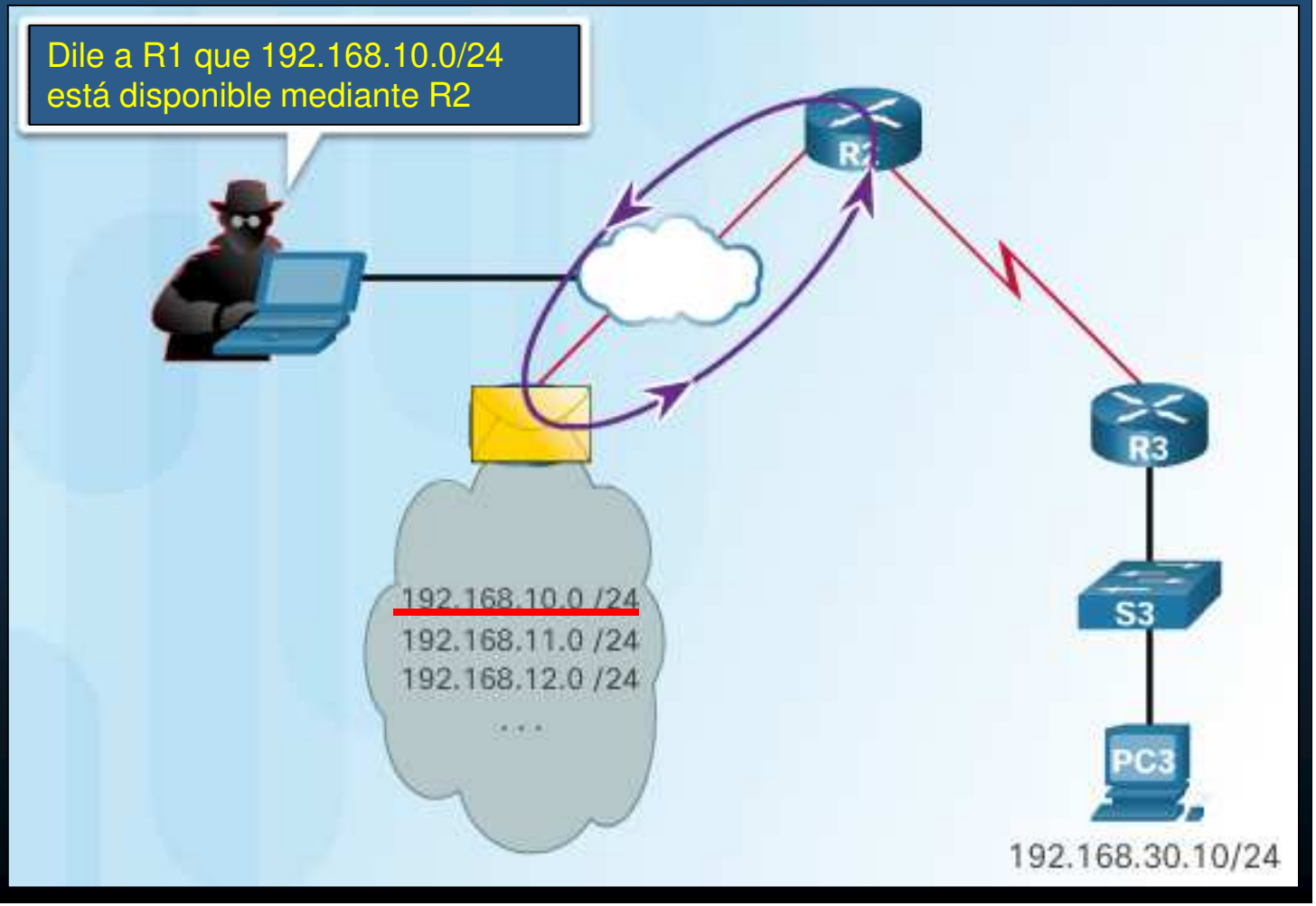
- Ejemplo de uso de AutoSecure.

```
Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]: yes
```

Se asegura el plano de reenvío.

2.5 Seguridad en el Plano de Control

- Engaño de Protocolos de Enrutamiento (spoofing).
  - Falseo de información de enrutamiento puede usarse para manipular tráfico:
    - Descartar.
    - Monitorear.
    - Crear Bucles.
    - DoS.



2.5 Seguridad en el Plano de Control

- Autenticación OSPF con MD5.


```
R1# show ru
router ospf
 passive-in
 network 10
 network 19
!
<output omitte
!----------
R2# show ru
router ospf
 passive-in
 network 10
 network 19
!
<output omitte
```

```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
LOADING to FULL, Loading Done
----------------------------
```

Posible configurar Autenticación OSPF global con MD5 en todas las interfaces.

```
R(conf-if)# ip ospf message-digest-key key md5 password
R(conf-router)# area area-id authentication message-digest
```

La configuración por interfáz, tiene prioridad.

```
from LOADING to FULL, Loading Done
R2(config-if)#
```

2.5 Seguridad en el Plano de Control


```
R1(config)# key chain SHA256
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string ospfSHA256
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA256
R1(config-if)#
000218: Feb 20 15:06:07.607 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000219: Feb 20 15:07:22.635 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0
from LOADING to FULL, Loading Done
R1(config-if)#
```

```
R2(config)# key chain SHA256
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string ospfSHA256
R2(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)# interface s0/0/0
R2(config-if)# ip ospf authentication key-chain SHA256
R2(config-if)#
000142: Feb 20 15:07:22.631: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
R2(config-if)#
```

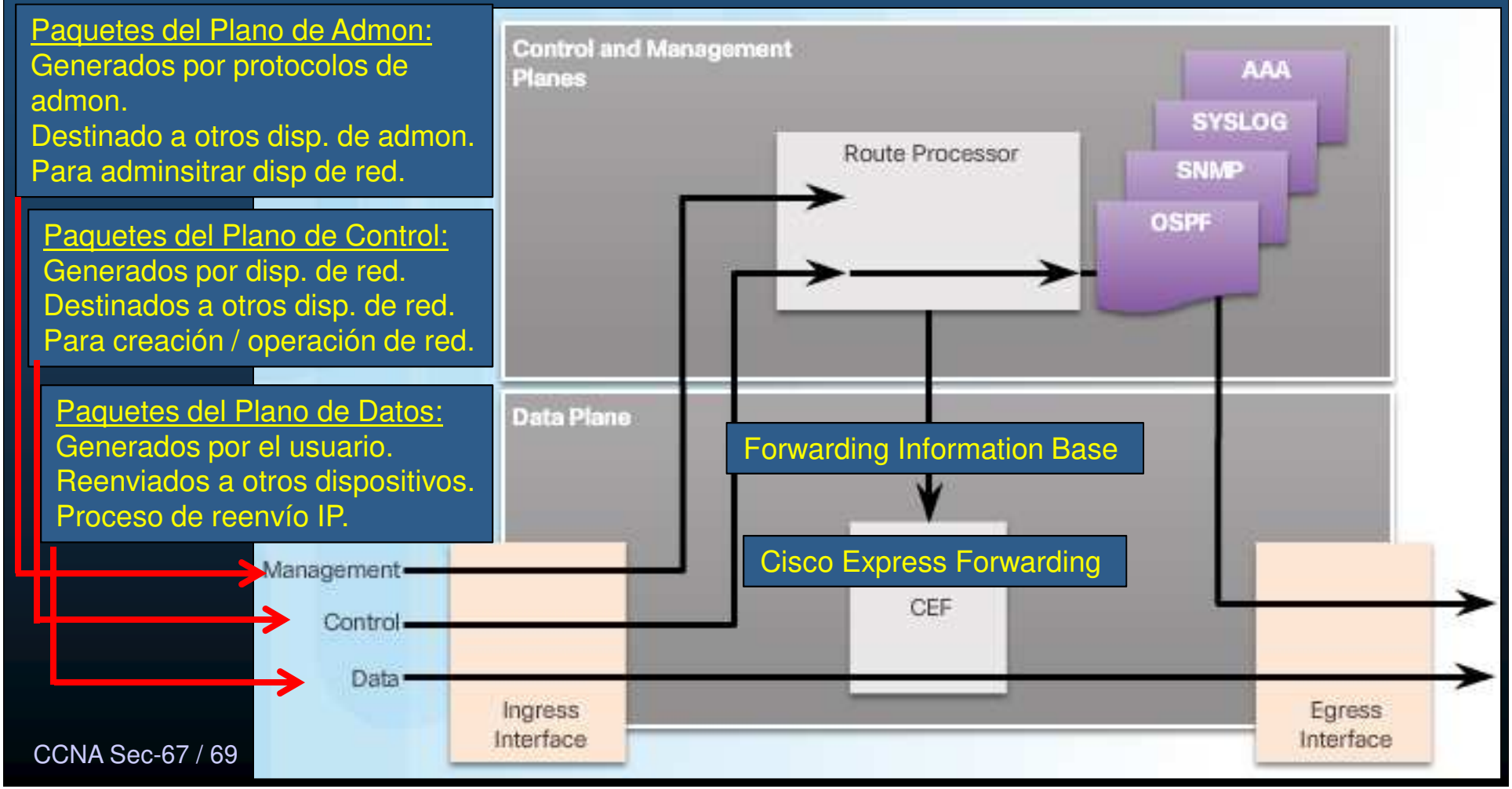
2.5 Seguridad en el Plano de Control

- Operaciones de Dispositivos de Red.
  - Un router debe diferenciar tráfico para planos Datos, Control y Administración.

Paquetes del Plano de Admon:
Generados por protocolos de admon.
Destinado a otros disp. de admon.
Para adminsitrar disp de red.

Paquetes del Plano de Control:
Generados por disp. de red.
Destinados a otros disp. de red.
Para creación / operación de red.

Paquetes del Plano de Datos:
Generados por el usuario.
Reenviados a otros dispositivos.
Proceso de reenvío IP.



2.5 Seguridad en el Plano de Control

- Vulnerabilidades de los planos de Control y Administración.
  - CPU del plano de control, es menos capaz de manejar tráfico que CEF.
    - Fácilmente sobrecargable ante mucho tráfico.
    - DoS.
      - Por ataques o malas configuraciones.
    - Mitigación mediante implementación de ACLs por interfaces.
      - Acorde a políticas de seguridad.

2.5 Seguridad en el Plano de Control

- Operación CoPP (Control Plane Policing).
  - Herramienta admiva para flujo de tráfico "punteado" al CPU del router.
    - Previene que tráfico innecesario llegue al CPU.
  - Punteado → Acción que toma una interface cuando envía paquetes al procesador del router.
  - Su implementación requiere menos esfuerzo que la implementación de ACLs.
  - Su puesta en marcha está mas allá del ámbito de este curso.

Capítulo 3

Autenticación, Autorización y Auditoría de Cuentas

```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

Habilita funciones de seguridad en PT (router 29xx)

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#3.1.1.1

3.1 Propósito de AAA

- Autenticación sin AAA.
  - Varios tipos de Autenticación en routers Cisco.
    - Configurar líneas con `login` y `password`: sencillo, débil, e inseguro.

```
R1(config)# line vty 0 4
R1(config-line)# password cis5cio
R1(config-line)# login
```

    - Habilitar SSH: comunicaciones cifradas, accounting básico (nombre de usuario y contraseña en base local por equipo), hay que configurar usuarios en todos y cada uno de los equipos individualmente.

```
R1(config)# ip domain-name cisco-academy.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Requiere haber cambiado nombre al Router

No disponible en P.T. 8.
Solo en modelos 829 (LTE 4G)

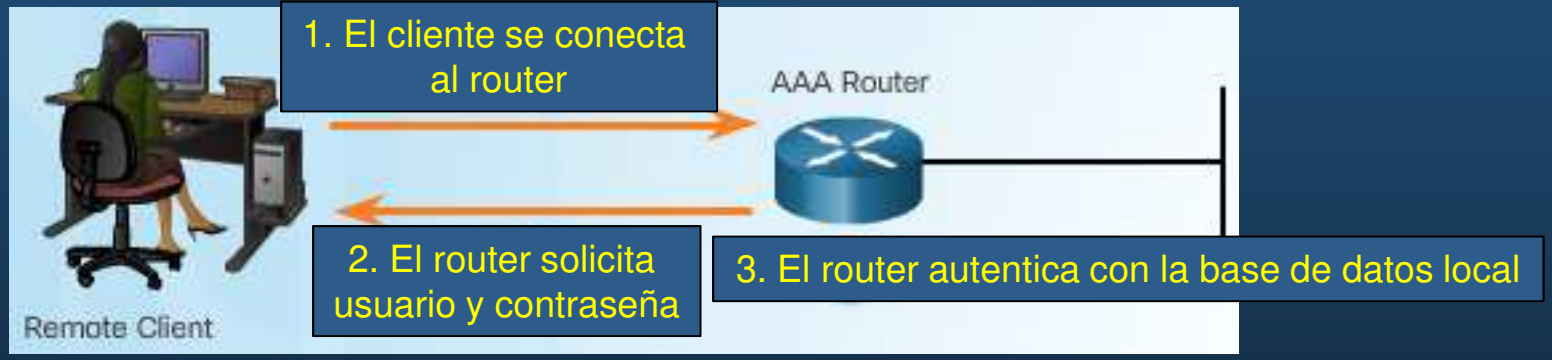
    - Servidor AAA: almacena nombres de usuario y contraseñas en un servidor, que puede ser consultado por todos los dispositivos.
      - Autenticación contingente si Admin olvida un nombre de usuario y/o contraseña

3.1 Propósito de AAA

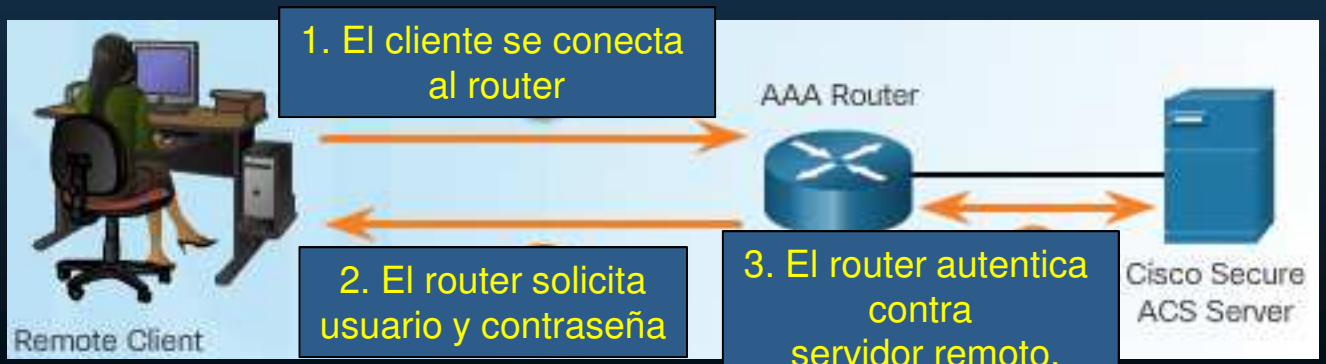
- Componentes de AAA.
  - Controla quién tiene acceso en una red, lo que pueden hacer, y auditar sus acciones.
    - Autenticación: Probar ser quién se dice ser.
      - Contraseñas, preguntas secretas, tokens, etc.
    - Autorización: Determinar recursos a los que se tiene acceso y las acciones permitidas sobre ellos.
    - Auditoria: Mantener registro de acciones realizadas por los usuarios.
      - Que fue accedido, cuanto tiempo, cambios realizados.

3.1 Propósito de AAA

- Modos de Autenticación.
  - Dos métodos principales mediante AAA:
    - Local: Autenticación auto-contenida, ideal para redes pequeñas.

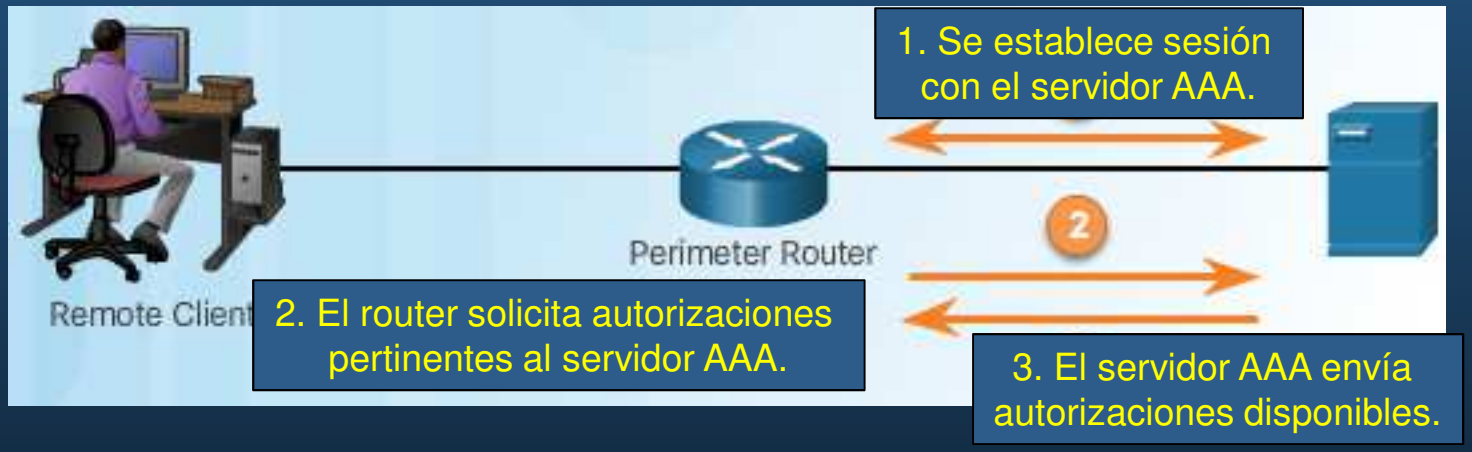


    - Basado en Servidor: Ideal para desarrollos medianos/grandes



3.1 Propósito de AAA

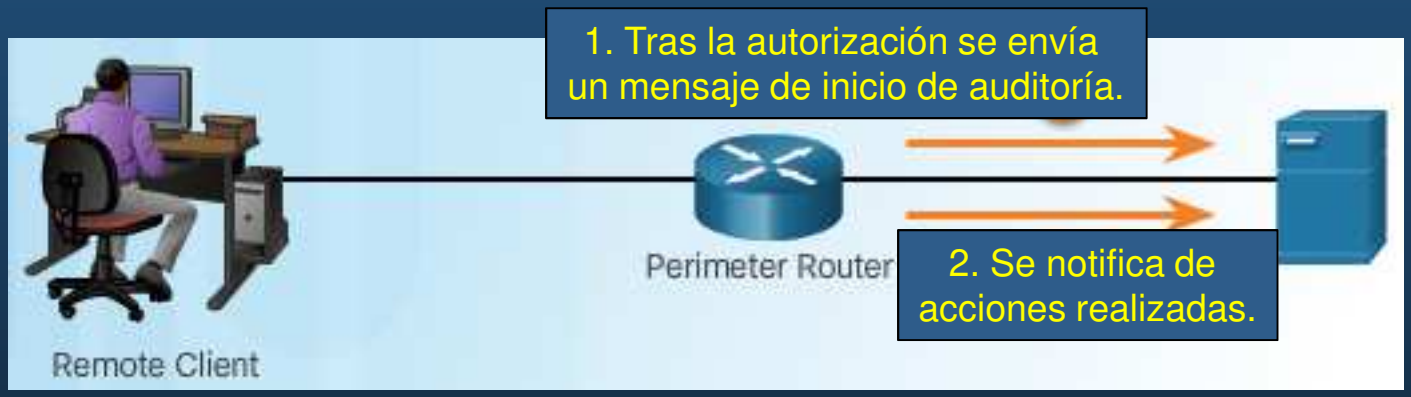
- Autorización.
  - Una vez autenticado se determinan las acciones y recursos autorizados.



  - Este proceso es automático e inmediato a la autenticación y no requiere intervención del usuario.

3.1 Propósito de AAA

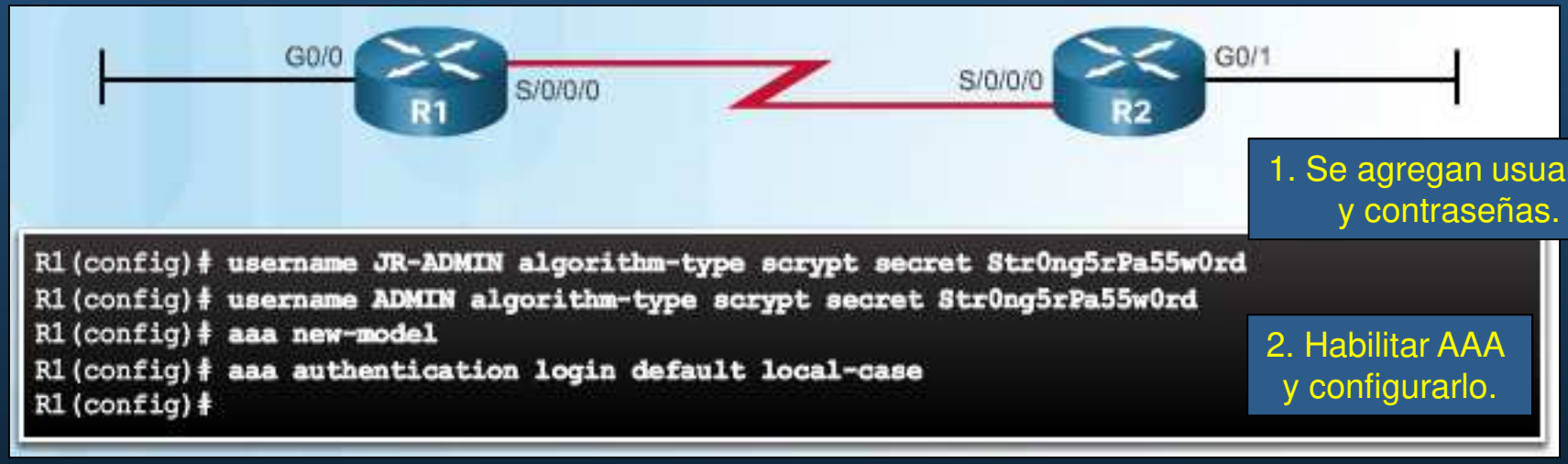
- Auditoría de Cuentas.
  - Colecta y reporta uso de datos.



  - Brinda mayor seguridad que solo Autenticar y Autorizar.
  - Genera logs de:
    - PPP, Telnet, SSH, EXEC, reboots, comandos, intentos de autenticación, autorización, etc.

3.2 Autenticación AAA Local

- Autenticación de Acceso Administrativo.
  - Para redes pequeñas (uno o dos routers).
  - Similar al uso de `login local` + Autenticación de respaldo.

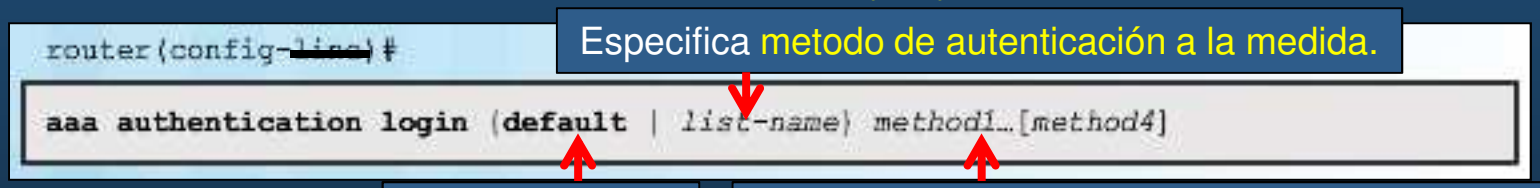


  - Tanto nombre de usuario como contraseña son sensibles a mayúsculas.

  - Desbloquear usuario que fué marcado por errores de ingreso:
    - `R# clear aaa local user lockout username "usn"`

3.2 Autenticación AAA Local

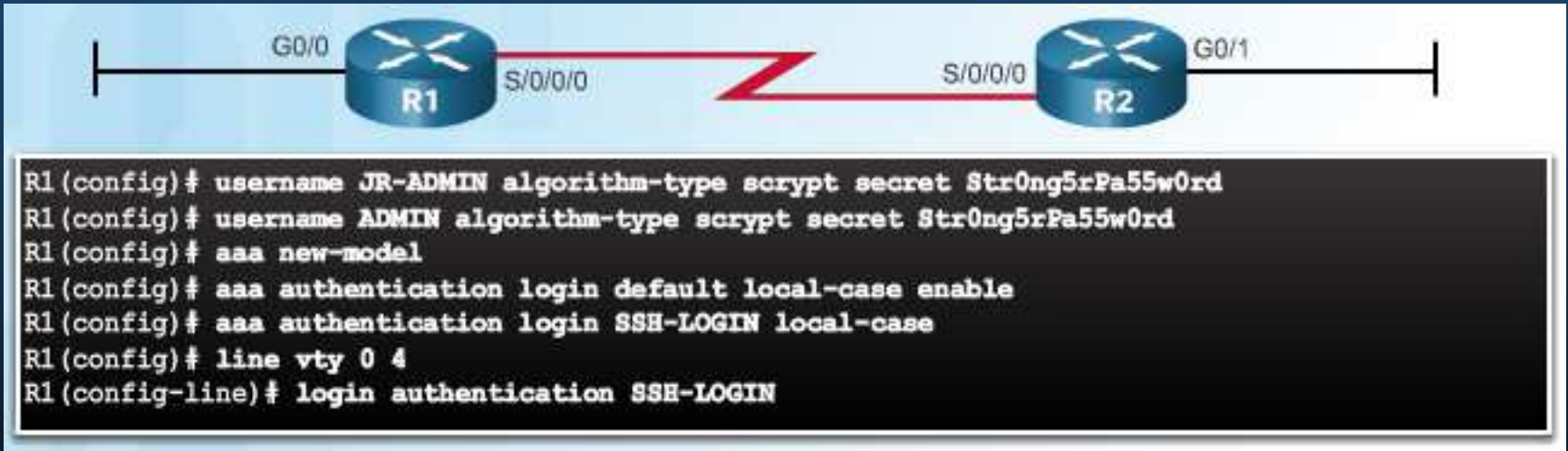
- Métodos de Autenticación.
  - **`R(config)# aaa new-model`**
    - Implica `login-local` (excepto consola) → Configurar usuarios/contraseñas previo.
  - **`R(config)# aaa authentication login`**
    - Habilita Autenticación a consola, aux y vtys



Método	Descripción
`enable`	Usa enable password para autenticar.
`local`	Usa base local para autenticar (insensible mayúsculas).
`local-case`	Usa base de datos local sensible a mayúsculas para autenticar.
`none`	Sin autenticación (solo debe usarse en pruebas).
`group radius`	Usa servidor radius para autenticar.
`group tacacs+`	Usa servidor tacacs+ para autenticar.
`group` *`nombre`*	Usa subconjunto de radius/tacacs para autenticar. Definido por aaa group server

3.2 Autenticación AAA Local

- Métodos Default y Nombrados.
  - Diferentes métodos pueden aplicarse a diferentes líneas/interfaces.
  - En el ejemplo, consola y auxiliar autentican mediante base local y `enalbe password`, mientras que vtys solo admiten la base local.



  - Note que las listas de métodos nombradas deben especificarse en las líneas a aplicarse.
  - Cada línea puede tener **solo una** lista nombrada asignada.

3.2 Autenticación AAA Local

- Refinamiento en la Configuración de Autenticación.
  - Seguridad adicional puede ser implementada mediante:

No disponible en P.T. 8

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

Cierra conexión y bloquea cuenta

```
R1# show aaa local user lockout
                Local-user          Lock time
                JR-ADMIN            04:28:49 UTC Sat Dec 27 2015
```

Desbloqueo manual:
`R# clear aaa local user lockout`

  - Cada sesión de usuario AAA, se identifica con un número único, y sus detalles pueden ser consultados mediante:

```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
    Unique Id: 175
    User Name: ADMIN
    IP Address: 192.168.1.10
    Idle Time: 0
    CT Call Handle: 0
```

  - Usuarios bloqueados permanecerán así, hasta que se desbloqueen manualmente.
  - `R(Config)#login delay seconds` establece tiempo de espera entre intentos de logueo fallidos.

No disponible en P.T. 8

3.2 Autenticación AAA Local

- Opciones de Debug AAA.
  - Existen múltiples opciones para debuguear AAA.
  - De particular interés:
    - `authentication`

      Ayuda a identificar problemas de autenticación.
  - Debe usarse con precaución pues sobrecarga al plano de control.

Sólo esa opción disponible en P.T. 8

```
R1# debug aaa ?
  accounting          Accounting
  administrative      Administrative
  api                 AAA api events
  attr                AAA Attr Manager
  authentication      Authentication
  authorization       Authorization
  cache               Cache activities
  coa                 AAA CoA processing
  db                  AAA DB Manager
  dead-criteria       AAA Dead-Criteria Info
  id                  AAA Unique Id
  ipc                 AAA IPC
  mlist-ref-count     Method list reference counts
  mlist-state         Information about AAA method
                      list state change and notification
  per-user            Per-user attributes
  pod                 AAA POD processing
  protocol            AAA protocol processing
  server-ref-count    Server handle reference counts
  sg-ref-count        Server group handle reference counts
  sg-server-selection Server Group Server Selection
  subsys              AAA Subsystem
  testing             Info. about AAA generated test packets
```

3.2 Autenticación AAA Local

- Debug de Autenticación AAA.

```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''ruser=''
        port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
        action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

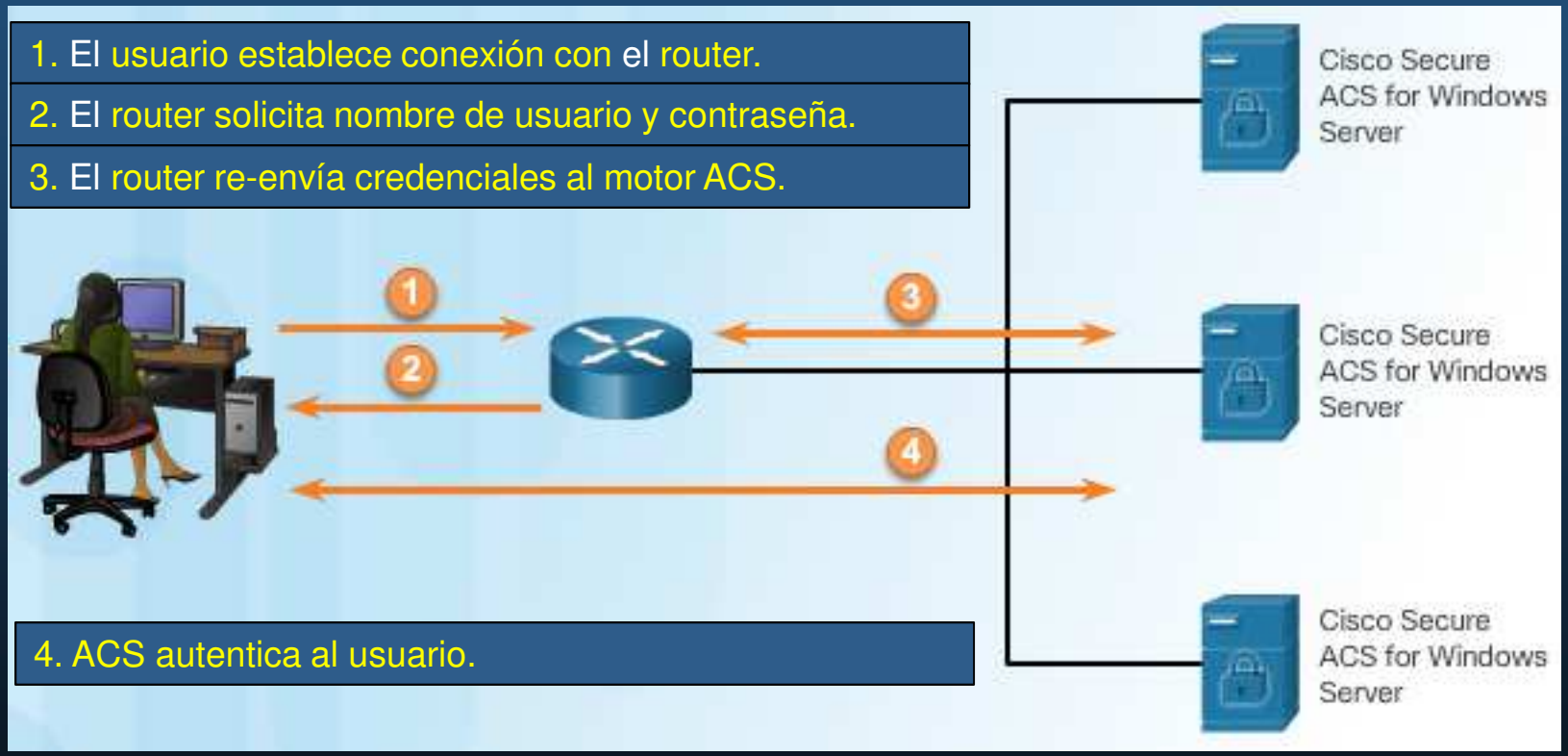
- Ejemplo de uso de la base local y login correcto.

3.3 AAA basada en Servidor

- Auntenticación AAA Local vs Basada en Servidor.
  - Local.
    - Problemas de escalabilidad.
    - Para usarse en redes pequeñas.
  - Basada en Servidor.
    - Fácilmente escalable.
    - Vgr; Cisco Secure ACS (Access Control System):
      - Crea un acceso centralizado a la base de usuarios y accesos.
      - Interconectividad con bases de datos externas como LDAP/Active Dir.
      - Soporte para RADIUS / TACACS+
    - Puede implementarse medianate múltiples servidores

3.3 AAA basada en Servidor

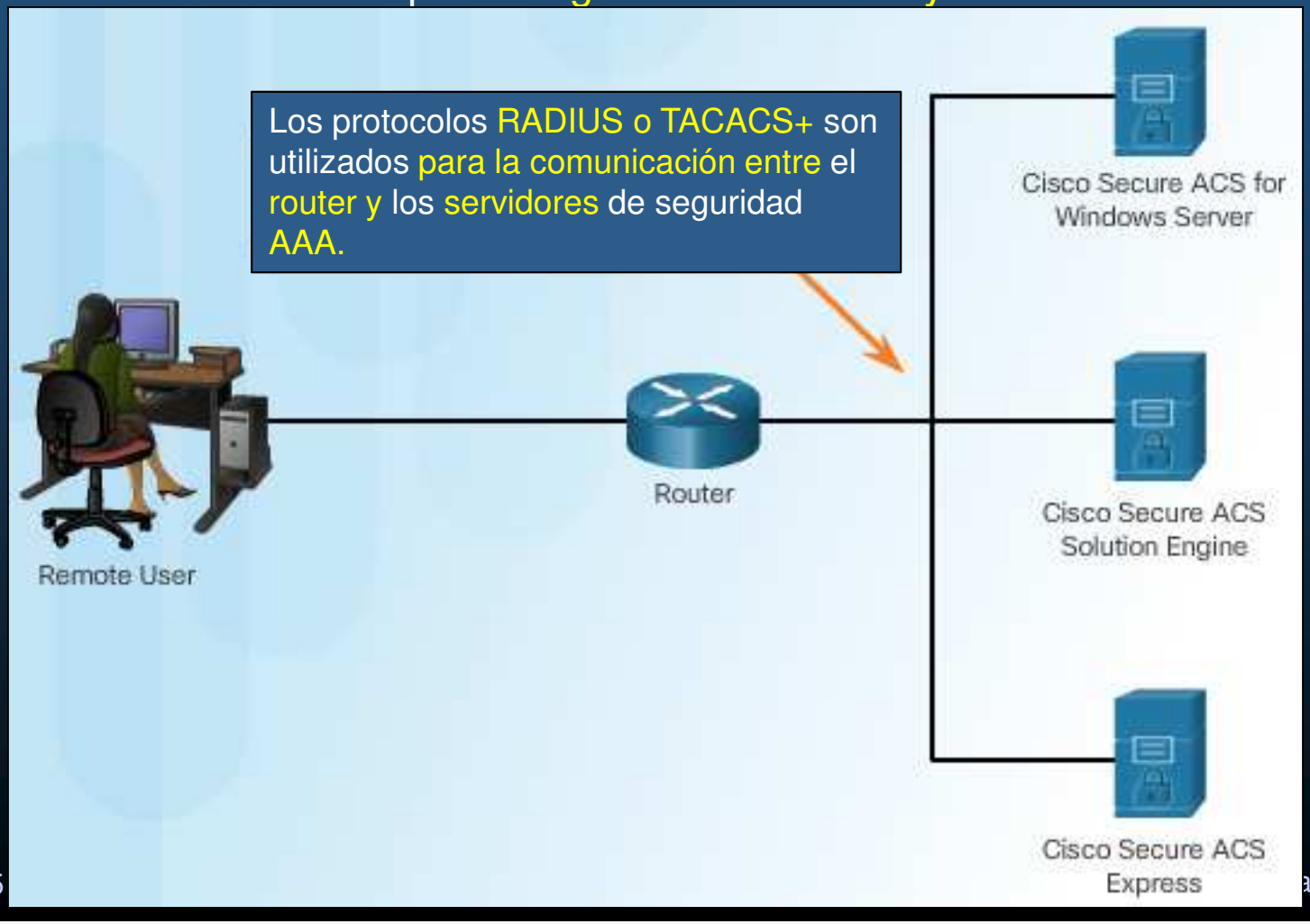
- Auntenticación AAA Basada en Servidor.
  - Puede implementarse mediante múltiples servidores.



Fin de vida para ACS: 30 de Agosto de 2017
Reemplazado por Cisco ISE

3.3 AAA basada en Servidor

- Introducción al Sistema de Control de Acceso (ACS) de Cisco.
  - Solución centralizada que amalgama identidades y accesos de red.



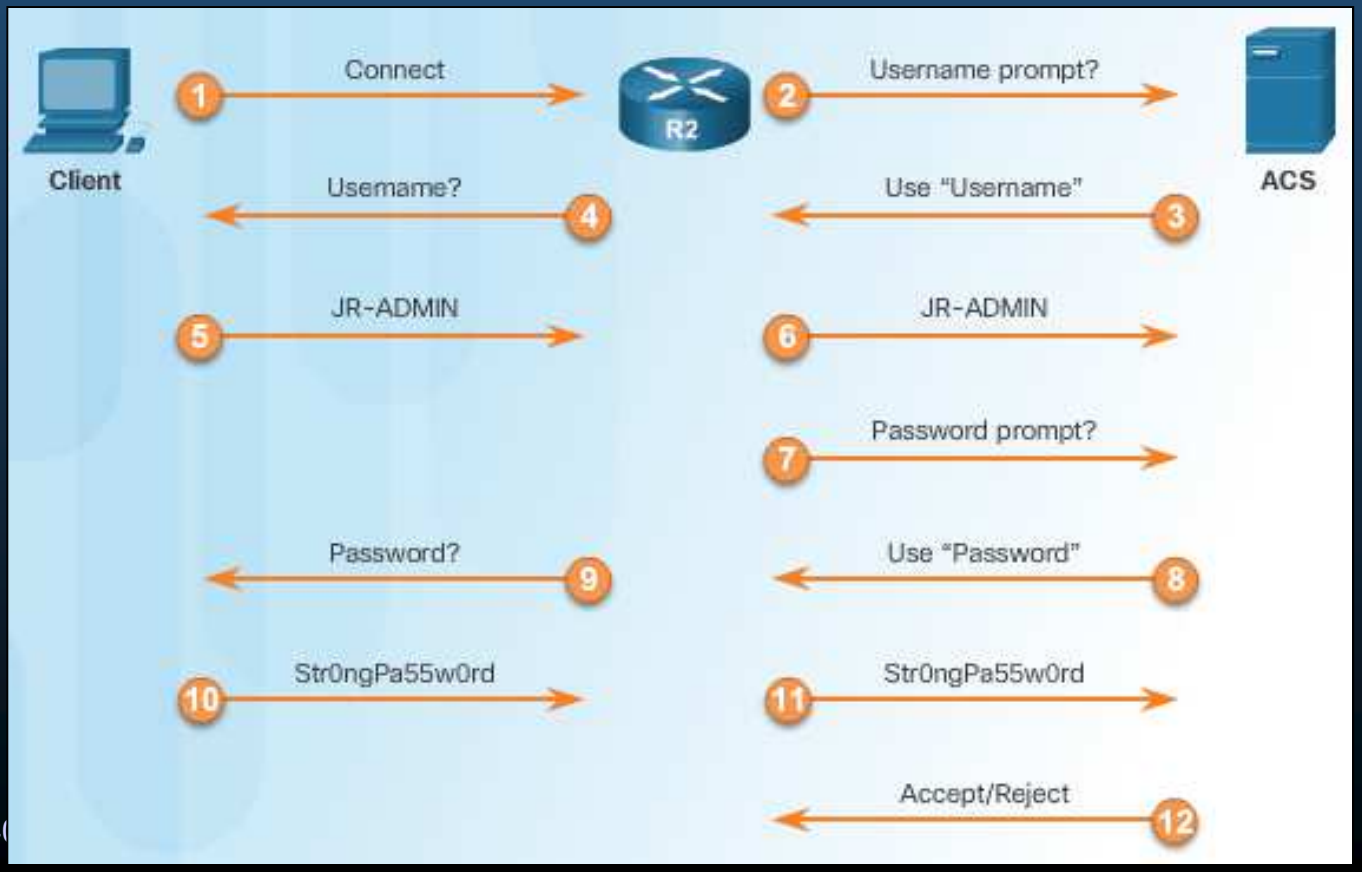
3.3 AAA basada en Servidor

- Introducción a RADIUS y TACACS+.

	TACACS+	RADIUS
Funcionalidad	Modularidad acorde a arquitectura AAA.	Combina Autenticación y Autorización, pero separa Auditoría. Menor flexibilidad.
Estándar	Soportado en su mayoría por Cisco.	Abierto, estándar RFC.
Protocolo de Transporte	TCP (49)	UDP (1645-1646/1812-1813)
CHAP	Desafío bidireccional cliente/servidor.	Desafío unidireccional cliente/servidor.
Confidencialidad	Paquetes encriptados.	Contraseña encriptadas.
Personalización	Provee autorización de comandos del router basado en grupos o usuarios.	No soporta autorización de comandos del router basado en grupos o usuarios.
Auditoría de Cuentas	Limitado.	Extenso

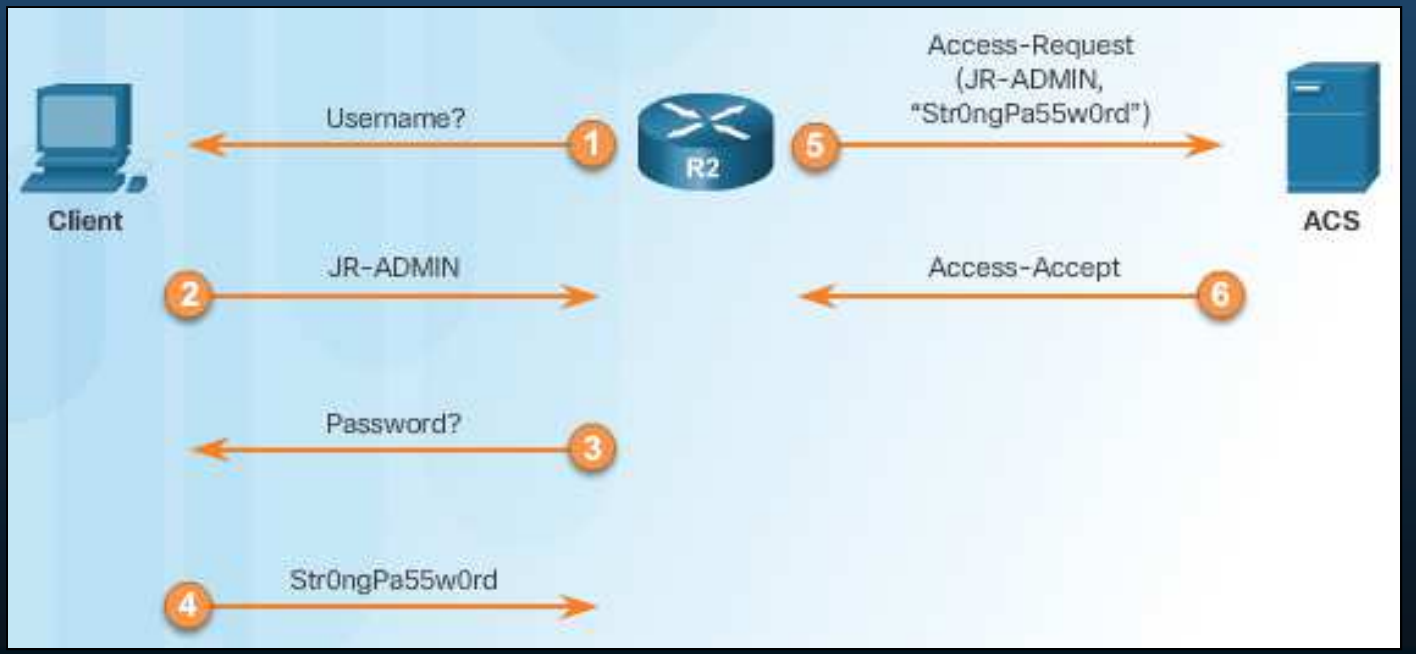
3.3 AAA basada en Servidor

- Autenticación TACACS+.
  - TACACS+: versión Cisco de TACACS (incompatibles).
  - Separa servicios de autenticación, autorización y auditoria de cuentas.
  - Soporte multiprotocolo en Capa 3.



3.3 AAA basada en Servidor

- Autenticación RADIUS.
  - Desarrollado por Livingston Enterprises, estándar IETF para AAA.
  - Soporte Local/Roaming.
  - RFCs 2865, 2866, 2867, 2868, 3162 and 6911.
  - Oculta contraseñas usando mecanismos con MD5, incluso en PAP.
  - Utilizado en:
    - VoIP/SIP
    - 802.1X



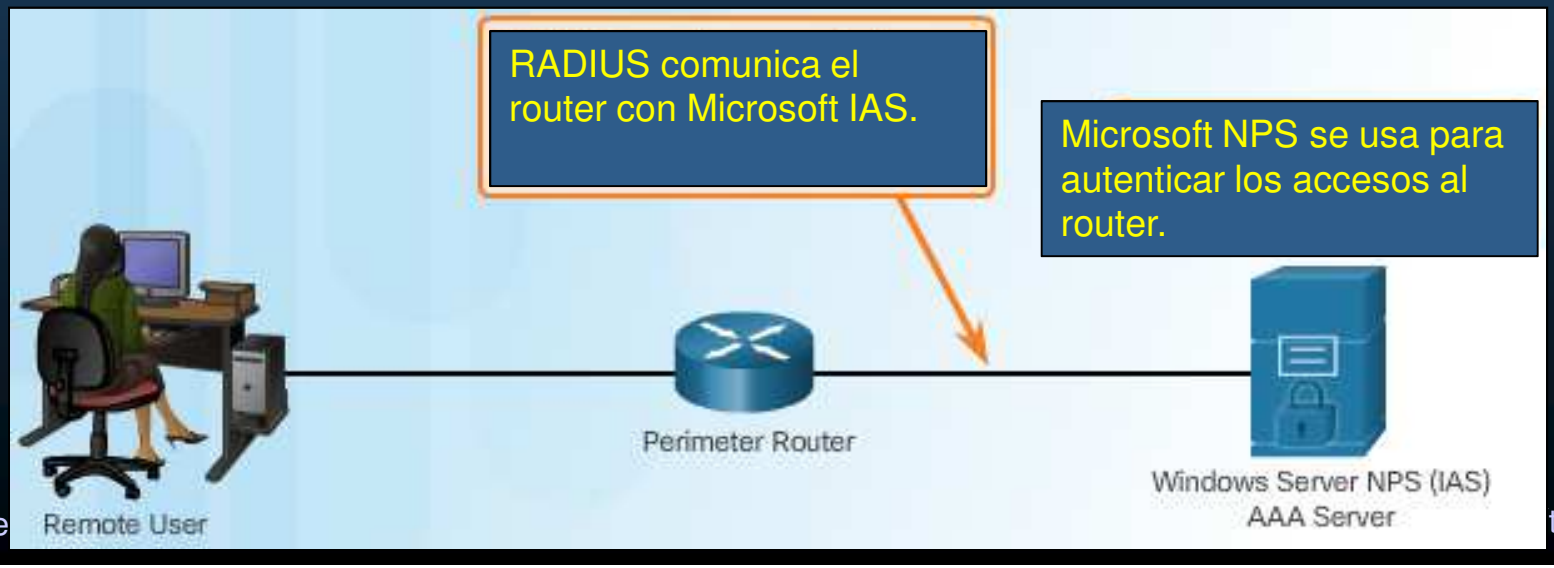
  - Una alternativa de siguiente generación es: DIAMETER AAA

3.3 AAA basada en Servidor

- Integración de TACACS+ y ACS.
  - ACS 5.6 incluye:
    - Arquitectura distribuida para desarrollos a mediana y gran escala.
    - GUI web intuitiva para clientes IPv4 e IPv6.
    - Autenticación mediante Active Directory y LDAP.
    - Reportes programados a e-mail.
    - Monitoreo avanzado mediante SNMP.
    - Logs encriptados.
    - Reportes de auditorías detallados y flexibles.

3.3 AAA basada en Servidor

- Integración de AAA con Microsoft Active Directory (AD).
  - AD es utilizado autenticar/autorizar usuarios al entrar en un dominio Windows.
    - Puede ser utilizado para autenticar/autorizar en dispositivos Cisco.
  - Aunque es posible unir ACS con AD, AD puede fungir como servidor AAA.
  - Microsoft AAA con RADIUS se conoció como Servicio de Autenticación de Internet (IAS) hasta Windows 2008 → Servidor de Políticas de Red (NPS).
  - La configuración en el IOS es similar a la usada para un servidor RADIUS.
    - Solo que se usa AD para Autenticar/Autorizar.



3.3 AAA basada en Servidor

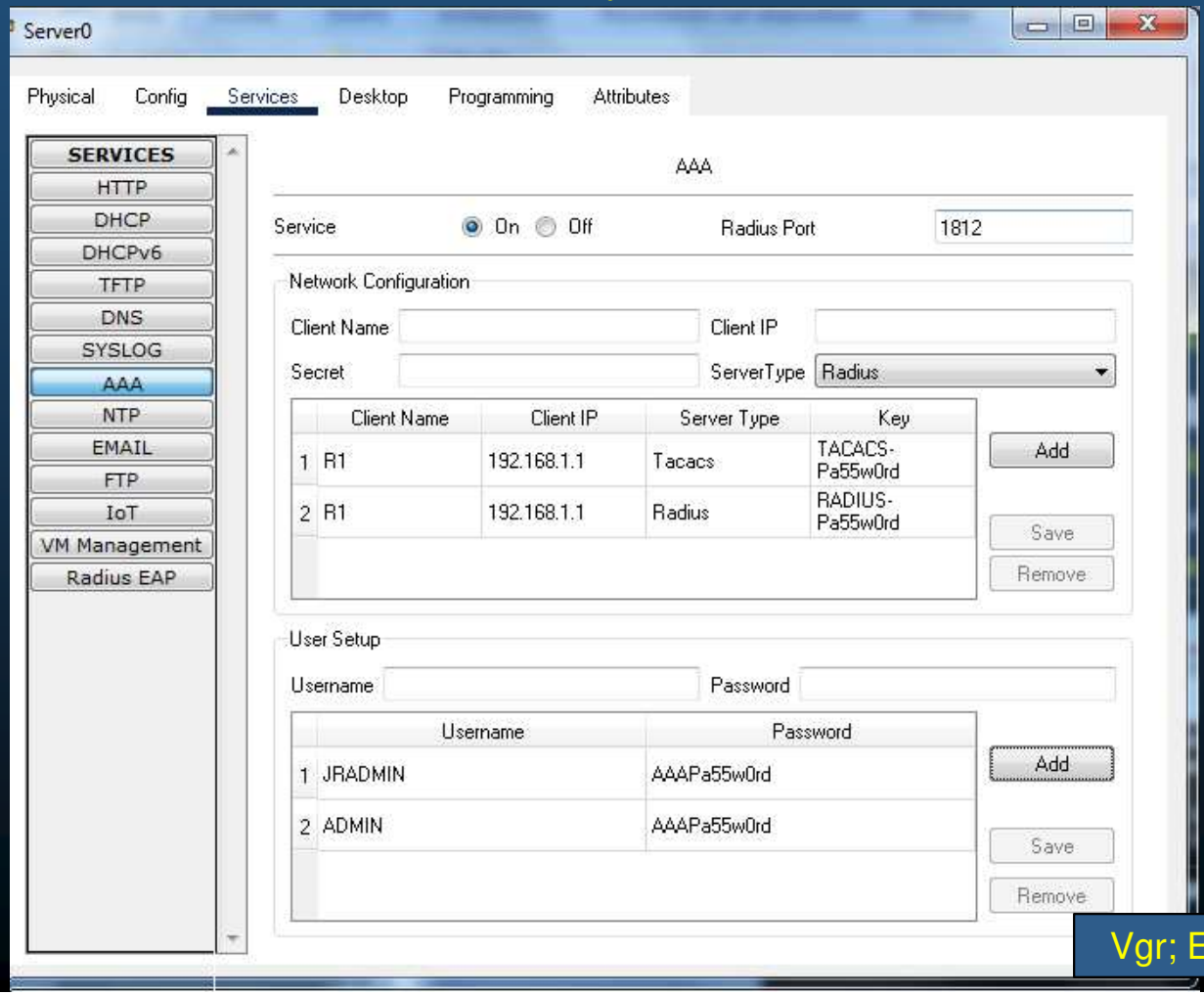
- Integración de AAA con Motor de Servicio de Identidad (ISE).
  - Motor de Servicio de Identidad de Cisco:
    - Plataforma de políticas de control de identidad y acceso.
    - Mejorar seguridad de infraestructura, y simplificar operaciones de servicio.
    - Define políticas, controla y reporta accesos justos para cualquier dispositivo, incluso BYOD.
    - Componente principal de Cisco TrustSec.
      - Protege bienes como: datos, aplicaciones, y dispositivos móviles de accesos no autorizados.
    - Características ISE:
      - Perfilado de Dispositivos: Personales ó Empresariales.
      - Evaluación de postura: Verifica si el dispositivo está libre de virus o alteraciones antes de ingresar a la red.
      - Administración de Invitados: Permite y asegura accesos temporales de invitados.
      - AAA: Combinadas en una aplicación que además realiza las 3 características anteriores.

3.3 AAA basada en Servidor

- Integración de AAA con Motor Servicio de Identidad (ISE).
  - Motor Servicio de Identidad de Cisco:
    - Administración de identidades consciente de contexto.
      - Determina que usuarios acceden a la red.
      - Establece la identidad del usuario, ubicación e historial de accesos.
      - Asigna servicios según el rol o grupo y políticas asociadas.
      - Brinda acceso a usuarios autenticados, a segmentos específicos de una red, aplicaciones específicas o ambos.
    - Mas Información.
      - Video.
      - Transcripción.

3.4 Autenticación AAA basada en Servidor

- Pasos para configurar autenticación AAA basada en Servidor.
  0. Habilitar Servidor Radius/Tacacs+ y Usuarios.



Vgr; En Packet Tracer 8

3.4 Autenticación AAA basada en Servidor

- Pasos para configurar autenticación AAA basada en Servidor.
  1. Habilitar AAA.
  2. Especificar la dirección del servidor ACS.
  3. Configurar la llave secreta.
  4. Configurar autenticación para utilizar el servidor TACACS+ ó RADIUS.

3.4 Autenticación AAA basada en Servidor

- Configurar servidor(es) TACACS+.
  - Habilitar AAA globalmente con el comando:
    `R(Config)# aaa new-model`
  - Configurar cada servidor TACACS+:
    `R(Config)# tacacs server` *`nombre`*
    - Configurar la dirección IP del servidor TACACS+:
      `R(Config-srv- tacacs)# address ipv4` *`Dir_IP`*
      - Opcionalmente puede cambiar el puerto de autenticación y auditoría de cuentas.
    - Mantener una sola conexión TCP p' todas las sesiones de autenticación.
      `R(Config-srv- tacacs)# single-connection`
    - Especificar la llave a utilizar para cifrar transferencias de datos:
      `R(Config-srv- tacacs)# key` *`llave`*

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.101
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
```

No disponible en P.T. 8

3.4 Autenticación AAA basada en Servidor

- Configurar Servidores RADIUS.
  - Habilitar AAA globalmente con el comando:
    `R(Config)# aaa new-model`
  - Configurar cada servidor RADIUS:
    `R(Config)# radius server` *nombre*
    - Configurar la dirección IP del servidor RADIUS:
      `R(Config-radius-srvr)# address ipv4` *Dir_IP*
      - Opcionalmente puede cambiar el puerto de autenticación y auditoría de cuentas (Cisco 1645/1646 vs IANA 1812/1813).
    - Con UDP, no existe equivalente a `single-connection` en RADIUS.
    - Especificar la llave a utilizar para cifrar contraseñas:
      `R(Config-radius-srvr)# key` *llave*

```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
```

No disponible en P.T. 8

3.4 Autenticación AAA basada en Servidor

- Configurar Autenticación para Utilizar un Servidor AAA.
  - Identificados los servidores, deben incluirse a la lista de método de autenticación.

```
R1(config)# aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

  - Ejemplo que Autentica con TACACS+, o RADIUS si no disponible, ó Base local si tampoco disponible (como respaldo).

```
R1(config)# aaa new-model
```

Alternativa para Packet Tracer 8

```
R(config)#tacacs host 10.20.30.1
R(config)#tacacs host 10.20.30.1 single-connection
R(config)#tacacs host 10.20.30.1 key TACACS-Pa55w0rd

R(config)#radius host 10.20.30.1
R(config)#tacacs host 10.20.30.1 auth-port 1812 key RADIUS-Pa55w0rd
```

```
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

3.4 Autenticación AAA basada en Servidor

- Monitoreo del Tráfico de Autenticación.
  - Permite resolver problemas de configuración.

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

    - Mensaje PASS → Autenticación válida para el intento por TACACS+.
    - Si fuese inválida diría FAIL en vez de PASS.

3.4 Autenticación AAA basada en Servidor

- Debug de RADIUS y TACACS+.

No disponible en P.T. 8

```
R1# debug radius ?
  accounting      RADIUS accounting packets only
  authentication  RADIUS authentication packets only
  brief           Only I/O transactions are recorded
  elog            RADIUS event logging
  failover        Packets sent upon fail-over
  local-server    Local RADIUS server
  retransmit      Retransmission of packets
  verbose         Include non essential RADIUS debugs
  <cr>
```

```
R1# debug tacacs ?
  accounting      TACACS+ protocol accounting
  authentication  TACACS+ protocol authentication
  authorization   TACACS+ protocol authorization
  events          TACACS+ protocol events
  packet          TACACS+ packets
  <cr>
```

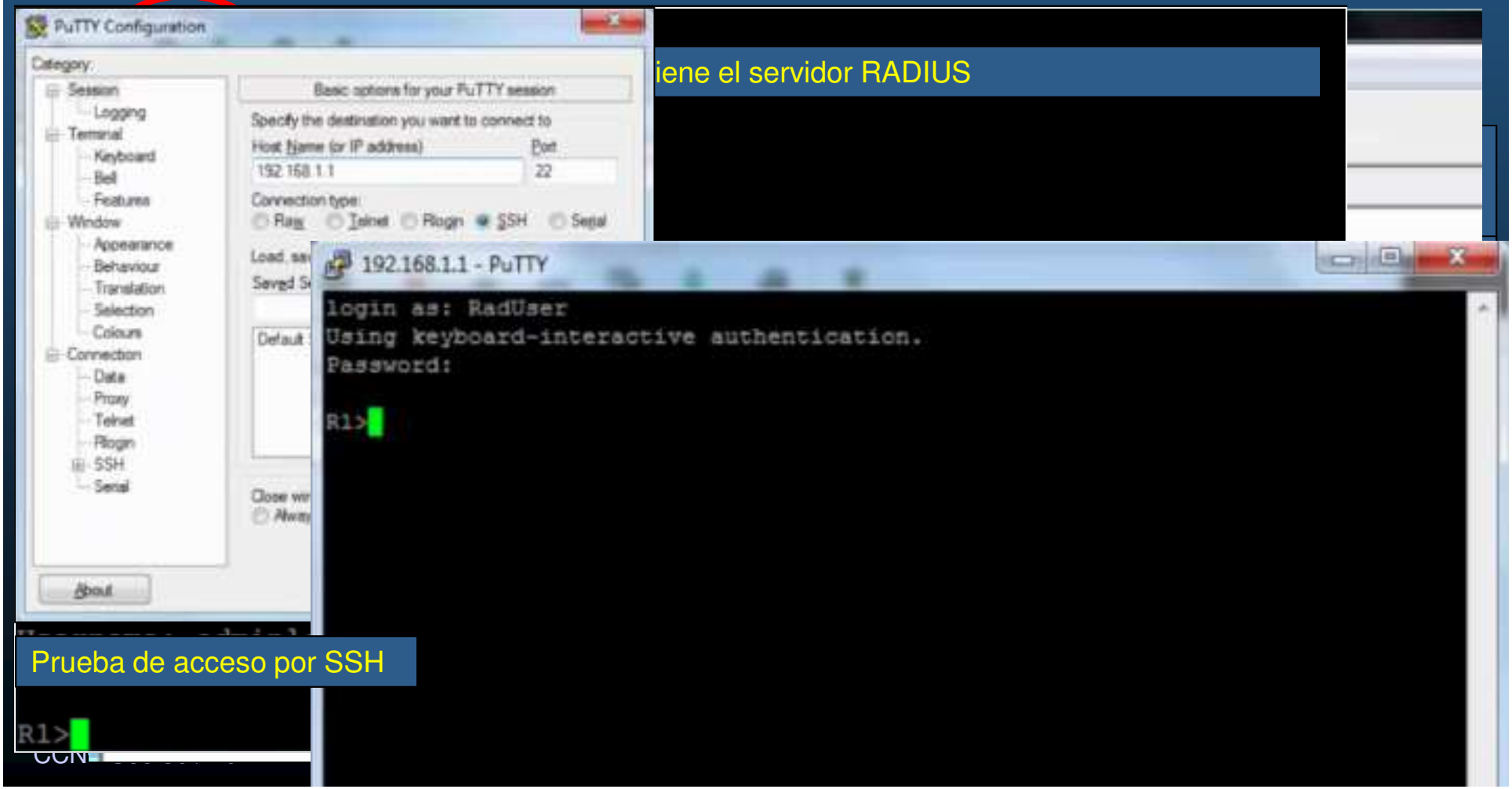
- Ofrecen información mas detallada que `debug aaa authentication`.

Precaución, puede generar grandes cantidades de información y saturar CPU.

```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

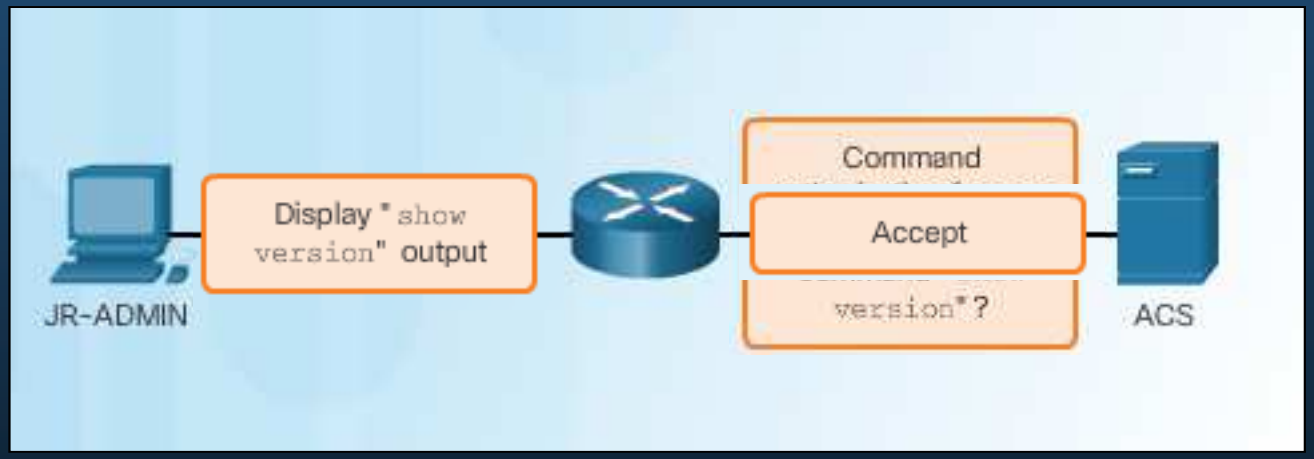
3.4 Autenticación AAA basada en Servidor

- Configuración de Router Cisco para Acceder un Servidor RADIUS (WinRadius).



3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Introducción a la Autorización basada en Servidor AAA.
  - Permisos para accesar ciertas áreas, servicios/programas, comandos.
  - TACACS+ puede restringir solo ciertas funciones por usuario.
  - Permisos por usuario en Cisco ACS simplifica la configuración.



  - Por defecto, TACACS+ establece una nueva sesión TCP con cada solicitud.
    - Para mantener una sola conexión por sesión use:

```
R(Config-srv- tacacs)# single-connection
```

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

No disponible en P.T. 8

- Configuración de Autorización AAA.
  - Utilice:

Para Servicios de red. | Para iniciar shell de exec. | Para comandos del shell.

```
R1(config)# aaa authorization (network | exec | commands level)
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec ?
  WORD      Named authorization list.
  default   The default authorization list.
```

```
R1(config)# aaa authorization exec default ?
  cache              Use Cached-group
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD      Server-group name
  ldap      Use list of all LDAP hosts.
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

  - Cuando la Autorización AAA no está habilitada, todos tienen acceso total.
  - Cuando se inicia la Autorización, cambia a no permitir accesos.
    - Importante crear usuario con acceso total previamente.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Introducción a Auditoría de Cuentas basada en Servidor AAA.
  - Permite mantener registro del uso de recursos por los usuarios.
  - Permite establecer patrones de uso de recursos por usuarios
    - Tomar acciones ante comportamientos sospechosos.
  - Ayuda a la resolución de problemas.
  - Cisco ACS permite almacenar dicha información en el servidor.
  - Permite establecer listas sobre como llevar a cabo los registros.

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Configuración de Auditoría de Cuentas.
  - Utilize:

No disponible en P.T. 8

Para Servicios de red.

Para iniciar shell de exec.

Para conexiones SSH/Telnet.

Disparadores.

```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]
```

Solicita inicio de registro al inicio del proceso, y de detenerse al finalizar.

Solicita detener el proceso de registro.

Deshabilita el registro en una línea o interface.

```
R1(config)# aaa accounting exec?
  WORD        Named Accounting list.
  default     The default accounting list.
```

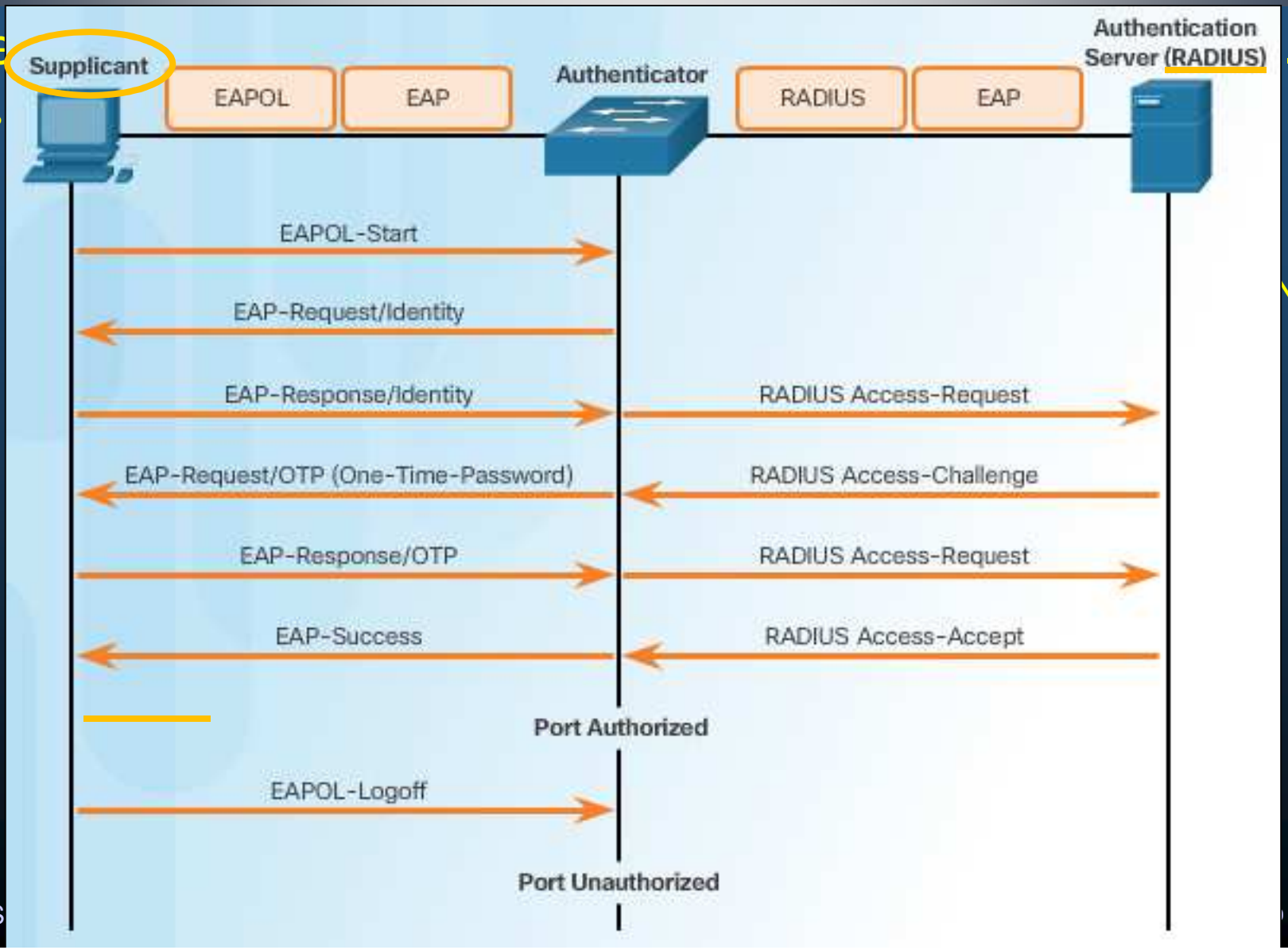
```
R1(config)# aaa accounting exec default start-stop?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

R1(config)# aaa accounting exec default start-stop group?
  WORD       Server-group name
  radius     Use list of all Radius hosts.
  tacacs+    Use list of all Tacacs+ hosts.
```

  - Ejemplo:

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Se
  - .



N.

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Estado de Autorización de Puertos 802.1x.
  - Cuando el cliente recibe un "accept", el puerto del switch cambia a "authorized", y los marcos del cliente pueden viajar por el switch.
  - Si la autenticación falla, el puerto permanece "unauthorized".
  - Cuando un cliente autenticado envía "EAPOL logout" el puerto cambia a "unauthorized".
  - El comando: **`authentication port-control`** controla la autorización de puertos:

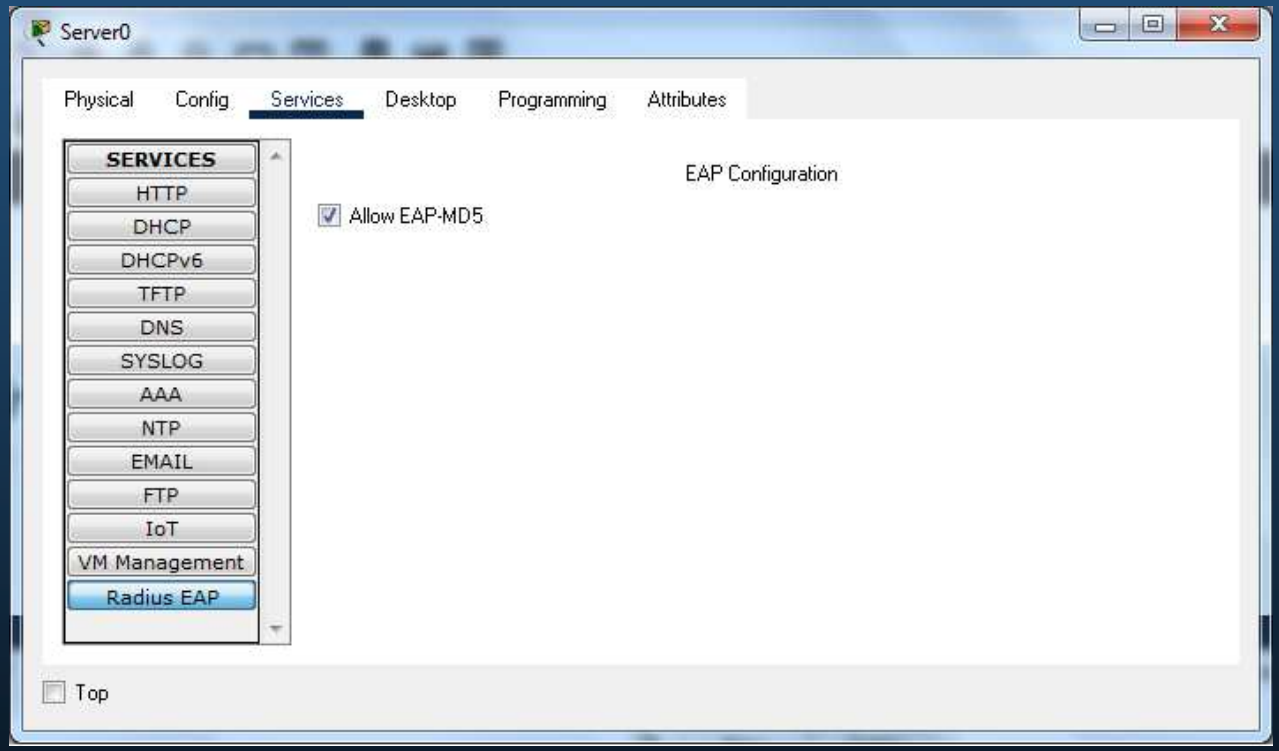
No disponible en P.T. 8

```
S1(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}
```

Parámetro	Descripción
`auto`	Habilita autenticación 802.1X y pone puerto como "unauthorized" (Solo tráfico EAPOL)
`forze-authorized`	El puerto envía y recibe tráfico sin haber sido autenticado el cliente 802.1X.
`forze-unauthorized`	Causa que el puerto permanezca siempre como "unauthorized" Ignora intentos de autenticar

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Configuración 802.1X.
  - Habilitar Servidor RADIUS EAP
    - Vgr; En P.T. 8



  - Agregar al Switch cómo cliente válido para el servidor RADIUS
    - Vgr; En P.T. 8 (Servicio AAA)

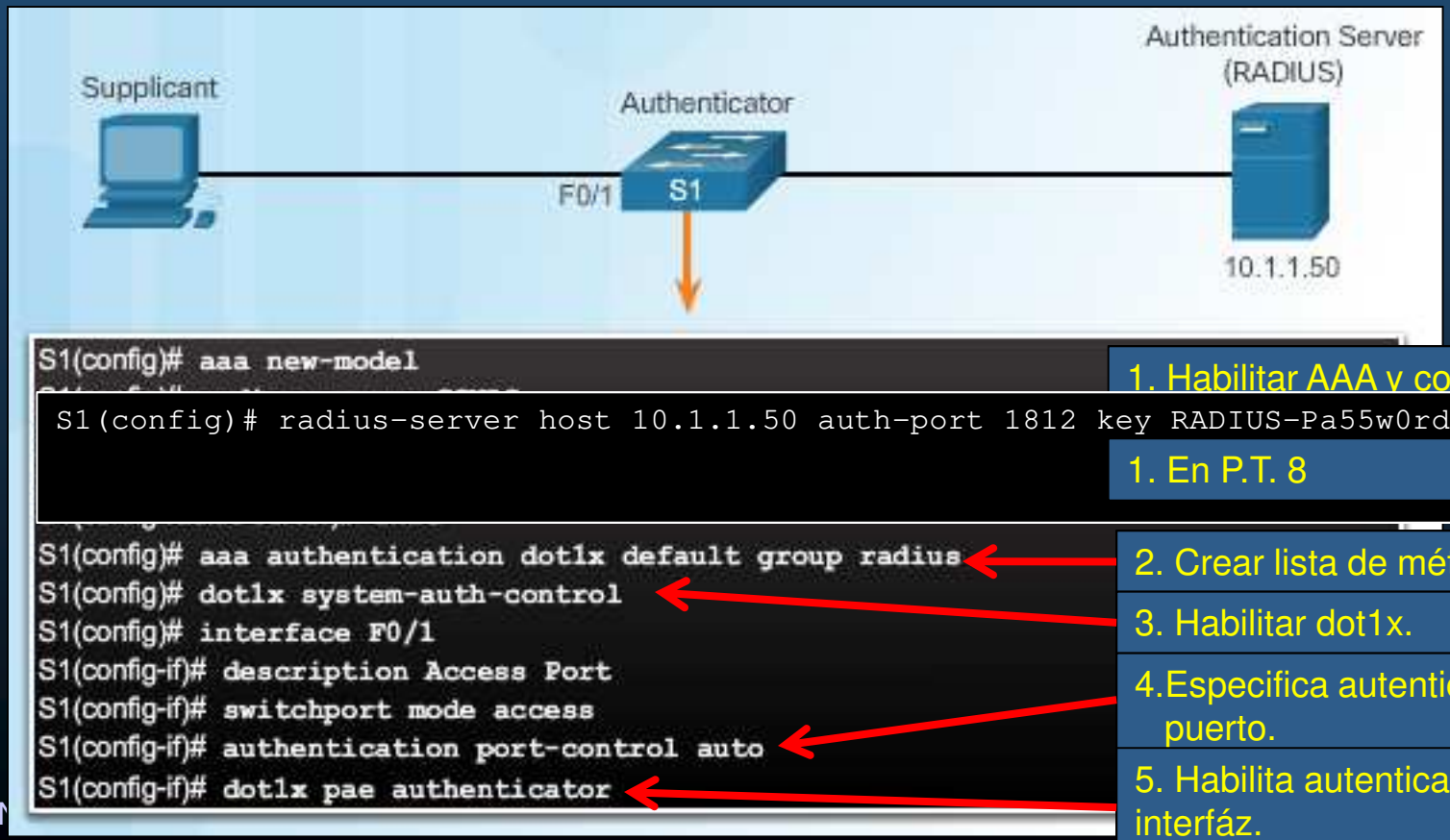
3	Switch0	192.168.1.253	Radius	RADIUS-Pa55w0rd

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

- Configuración 802.1X.

```
S1(config)# interface Vlan1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shut

S1(config)# ip default-gateway 192.168.1.254
```

0. Habilitar SVI y Default Gateway



1. Habilitar AAA y configurar RADIUS

1. En P.T. 8

2. Crear lista de métodos con dot1x.

3. Habilitar dot1x.

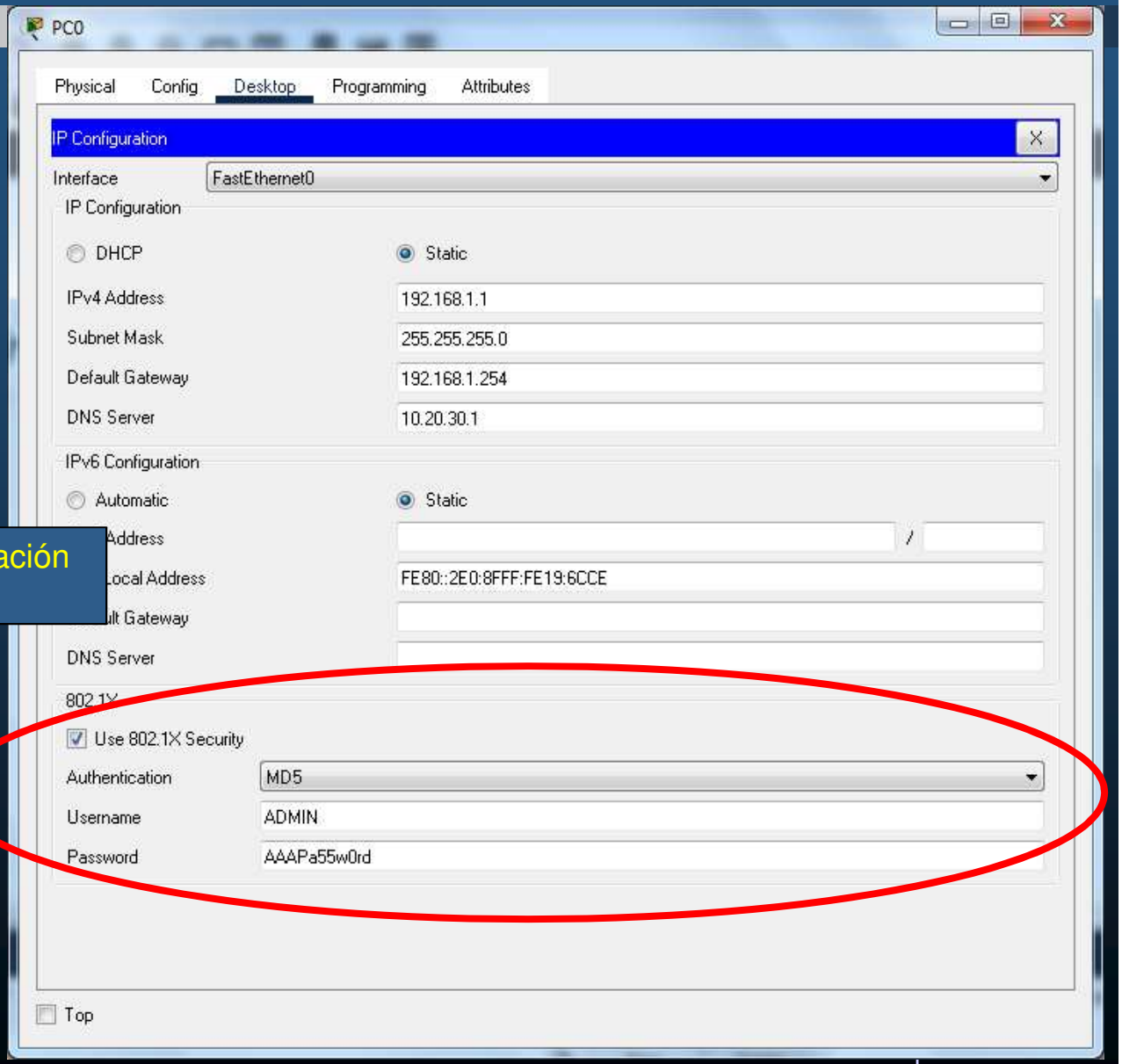
4. Especifica autenticación basada en puerto.

5. Habilita autenticación 802.1X en la interfáz.

3.5 Autorización y Auditoría de Cuentas basadas en Servidor AAA

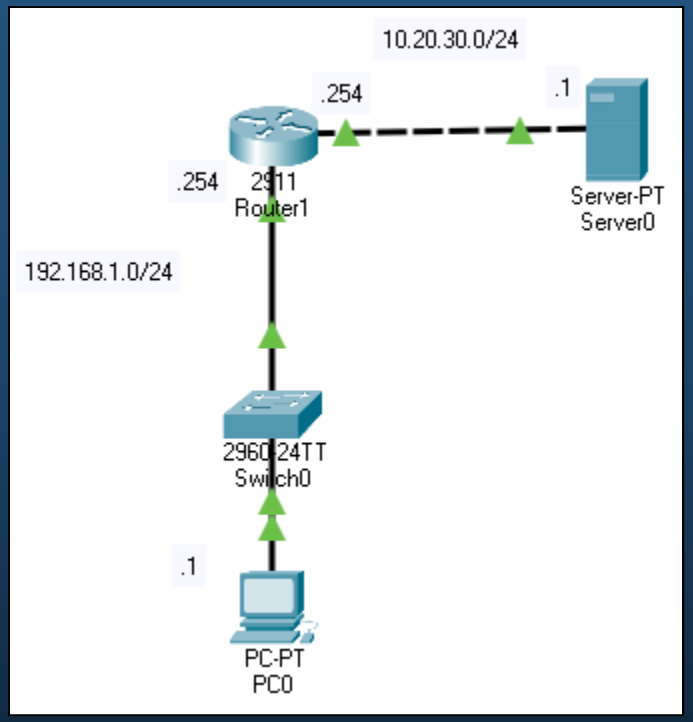
- Configuración 802.1X.

6. Habilitar software de autenticación 802.1X en el cliente.



Integración Capítulo 3

- Actividad Práctica.
  - Realice la configuración IP de los dispositivos mostrados en la topología.
  - Configure:
    - Autenticación sin AAA por Telnet
      - password cis5cio
    - Autenticación sin AAA por SSH
      - Dominio cisco-academy.com
      - Usuario: Admin / Str0ng3rPa55w0rd
    - Server 0 para autenticar a ADMIN / AAAPa55w0rd
      - AAA TACACS+
      - AAA RADIUS
      - 802.1x EAP
    - Autenticación de Acceso Administrativo
      - Usuario JR-ADMIN / Str0ng3rPa55w0rd
      - Habilitar AAA
    - Cree las autenticaciones nombradas:
      - SSH-LOGIN
      - SSH-TACACS
      - SSH-RADIUS



- Habilite AAA para todas las lineas por:
  - tacacs+, radius y base local
  - Autorización y Auditoría para exec.
- Autenticación dot1x en Switch 0
  - Para PC0

Capítulo 4

Implementando Tecnologías de Firewall

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#4.1.1.1

4.1 Listas de Control de Acceso

- Introducción a ACLs.
  - Permiten controlar tipos de tráfico de red.
  - Pueden ser definidas para capas 2, 3, 4 y 7 (OSI).
  - Históricamente el número de la ACL define el tipo.

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
DECnet and Extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Ethernet address	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Extended transparent bridging	1100-1199

Pueden ser nombradas para IPv4.
Deben ser nombradas para IPv6.

4.1 Listas de Control de Acceso

- Configuración de ACLs Estándar Numeradas.
  - Lista secuencial de sentencias `permit` ó `deny`, conocidas como ACEs (Entidades de Control de Acceso).
  - Las ACLs estándar numeradas filtran paquetes basándose en la dirección IP de origen.

```
access-list (acl-#) (permit | deny | remark) source-addr [source-wildcard][log]
```

Parámetro	Descripción
acl-#	Número decimal (1 – 99 ó 1300 - 19999)
`deny`	Niega el acceso si se cumplen las condiciones.
`permit`	Permite el acceso si se cumplen las condiciones.
`remark`	Agrega una nota/comentario entre ACEs.
source-addr	IP de origen / any (0.0.0.0 255.255.255.255)
source-wildcard	(Opcional) Mascara que puede aplicarse a la IP para buscar coincidencias.
`log`	(Opcional) Genera logs de los paquetes que coinciden con la ACE, que son enviados a la consola.

4.1 Listas de Control de Acceso

- Configuración de ACLs Extendidas Numeradas.
  - Permiten filtrar paquetes basadas en la información de capas 3 y 4 origen y destino:

```
access-list acl-# (permit | deny | remark) protocol source-addr [source-wildcard]
dest-addr [dest-wildcard][operator port][established]
```

Parámetro	Descripción
acl-#	Número decimal (1 – 99 ó 1300 - 19999)
deny	Niega el acceso si se cumplen las condiciones.
permit	Permite el acceso si se cumplen las condiciones.
remark	Agrega una nota/comentario entre ACEs.
protocol	Nombre o número de un protocolo de internet (icmp, ip, tcp, udp)
source-addr	Ip de origen / any (0.0.0.0 255.255.255.255)
source-wildcard	Mascara wildcard que se aplica a la IP para buscar coincidencias.
destination-addr	Ip destino / any (0.0.0.0 255.255.255.255)
destination-wildcard	Mascara wildcard que se aplica a la IP para buscar coincidencias.
operator	(Opcional) operador condicional para buscar coincidencias (lt, gt, eq, neq, range)
port	(Opcional) Numero decimal para un puerto TCP/UDP
established	(Opcional) Para TCPs, indica solo tráfico de una conexión establecida.

4.1 Listas de Control de Acceso

- Configuración de ACLs Nombradas.
  - En lugar de utilizar un número, es posible asignar un nombre:
  - Creación de la ACL:

```
Router(config)# ip access-list [standard | extended] name_of_ACL
```

  - Ingreso de ACEs:

Standard ACE Syntax

```
Router(config-std-nacl)# (permit | deny | remark) (source [source-wildcard] | any)
```

Extended ACE Syntax

```
Router(config-ext-nacl)# (permit | deny | remark) protocol source-addr [source-wildcard]
dest-address [dest-wildcard] [operator port]
```

4.1 Listas de Control de Acceso

- Aplicación de una ACL.
  - Tras crear una ACL, puede aplicarse ya sea de entrada/salida, de varias maneras:
    - A una Interface:
    - A una VTY:

```
Router(config-if)# ip access-group {acl-#|name} {in|out}
Router(config-line)# access-class {acl-#|name} {in|out}
```

```
R1(config)# ip access-list standard VTY_ACCESS
R1(config-std-nacl)# permit 192.168.10.10 log
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class VTY_ACCESS in
R1(config-line)# end
R1#
R1#!The administrator accesses the vty lines from 192.168.10.10
R1#
*Feb 26 18:58:30.579: %SEC-6-IPACCESSLOGNP: list VTY_ACCESS permitted 0
192.168.10.10 -> 0.0.0.0, 5 packets
R1# show access-lists
Standard IP access list VTY_ACCESS
    10 permit 192.168.10.10 log (6 matches)
    20 deny any
```

4.1 Listas de Control de Acceso

- Guías de Configuración de ACLs.
  - Crear una ACL globalmente y después aplicarla.
  - Asegurarse de que la última ACE sea `deny any` o `deny any any`.
  - Recuerde que las ACEs se procesan en orden descendente, tan pronto una coincida se deja de revisar el resto de ACEs.
  - Coloque las ACEs mas específicas al inicio.
  - Recuerde: solo se admite una ACL por interface, por protocolo, por dirección.
  - Recuerde: nuevas ACEs se incluyen al final de la ACL.
  - Recuerde: los paquetes generados por un router no se filtran por las ACLs.
  - Coloque ACLs estándar lo mas cerca del destino.
  - Coloque ACLs extendidas lo mas cerca del origen.

4.1 Listas de Control de Acceso

- Edición de ACLs.
  - Por defecto las ACEs se numeran de 10 en 10.
    - Use esos números para eliminar o añadir ACEs.
    - Nota: Si no se especifica número se agrega al final de la ACL.

ACL Existente

```
Router# show access-lists
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Edición de la ACL

```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# 5 deny tcp any any eq telnet
Router(config-ext-nacl)# 20 deny udp any any
```

ACL Resultante:

```
Router# show access-lists
Extended IP access list 101
     5 deny tcp any any eq telnet
    10 permit tcp any any
    20 deny udp any any
    30 permit icmp any any
```

  - Recuerde: Las ACEs más específicas, deberían incluirse al inicio.

4.1 Listas de Control de Acceso

- Números de Secuencia y ACLs Estándar.
  - Para las ACLs Estándar, el IOS coloca las ACEs en un orden distinto al que fueron introducidas.
    - Primero van las ACEs de host acorde a un hash para optimizar búsquedas.
    - El número de secuencia solo sirve como referencia para eliminar ACEs.

ACL Existente

```
router# show access-lists
Standard IP access list 19
    10 permit 192.168.100.1
    20 permit 10.10.10.0, wildcard bits 0.0.0.255
    30 permit 201.101.110.0, wildcard bits 0.0.0.255
    40 deny any
```

Edición de la ACL

```
router(config)# ip access-list standard 19
router(config-std-nacl)# 25 permit 172.22.1.1
```

ACL Resultante:

```
router# show access-lists
Standard IP access list 19
    10 permit 192.168.100.1
    25 permit 172.22.1.1
    20 permit 10.10.10.0, wildcard bits 0.0.0.255
    30 permit 201.101.110.0, wildcard bits 0.0.0.255
    40 deny any
```

4.1 Listas de Control de Acceso

- Antispoof con ACLs.
  - Existen rangos de IPs que nunca deben ser consideradas como orígenes:

```
R1(config)# access-list 150 deny ip host 0.0.0.0 any
R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
R1(config)# access-list 150 deny ip host 255.255.255.255 any
```

1. Todos ceros
2. Broadcasts
3. Localhost
3. Privadas
4. Multicast

  - En interfaces locales, permitir solo IPs origen de la red directamente conectada:

```
R1(config)# access-list 105 permit ip 192.168.1.0 0.0.0.255 any
```

4.1 Listas de Control de Acceso

- Permitir Solo el Tráfico Necesario por el Firewall.
  - Trafico usualmente necesario:
    - DSN, SMTP, FTP. Probablemente: SSH, SNMP

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap
```

4.1 Listas de Control de Acceso

- Mitigar el abuso de ICMPs.
  - Los hackers pueden usar ping para descubrir posibles objetivos.
  - Sin embargo, algunos mensajes son requeridos para una correcta operación.
    - Entrantes:
      - Echo reply: permite a hosts externos contestar un Echo-request.
      - Source quench: solicita decrementar el tráfico al emisor.
      - Unreachable: generado por ACL que bloquea.

```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

La resolución de problemas, puede requerir habilitar respuestas desde el exterior.

    - Salientes:
      - Echo-request: permite hacer ping a hosts externos.
      - Parameter Problem: Informa sobre errores en la cabecera.
      - Packet too big: permite MTU discovery.
      - Source quench: decrementar el tráfico cuando se requiere.

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
R1(config)# access-list 114 deny icmp any any
R1(config)# access-list 114 permit ip any any
```

4.1 Listas de Control de Acceso

- Mitigación de Exploits SNMP.
  - Establecer una ACL para permitir tráfico administrativo solo de IPs confiables.
    - Advertencia: La IP puede ser clonada y ser aún susceptible.
  - Deshabilitar SNMP en router de frontera, y donde no sea requerido.

```
Router(config)# no snmp-server
```

4.1 Listas de Control de Acceso

- Introducción a ACLs IPv6.
  - IPv4 presenta algunas carencias que han llevado a evolucionar a IPv6:
    - Seguridad. (IPSec)
    - Roaming. IP móviles.
    - QoS, Protocolo de Reserva de Recursos (RSVP)
    - Escalabilidad de direccionamiento: (DHCP, NAT, CIDR, VLSM)
  - Riesgos actuales:
    - Aprovecharse de IPv4 para atacar IPv6 en dual stack.
    - Uso de NDP y túneles (Teredo) para obtener acceso IPv6 mas allá del NAT IPv4.
  - Mitigación:
    - Filtrar tráfico en router de frontera.
      - ACLs IPv6.

4.1 Listas de Control de Acceso

- Sintaxis para ACLs IPv6.
  - Las ACLs en IPv6 son siempre nombradas:

Aplique ACLs IPv6 a interfaces con el comando `ipv6 traffic filter`

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any |
host destination-ipv6-address} [operator [port-number]]
```

Parámetro	Descripción
`Deny`	Niega el acceso si se cumplen las condiciones.
`Permit`	Permite el acceso si se cumplen las condiciones.
`protocol`	Nombre o número de un protocolo de internet ó número de protocolo IPv6
`source-ipv6-prefix / prefix length`	Ipv6 de origen y su longitud de prefijo
`destination-ipv6-prefix / prefix length`	Ipv6 de destino y su longitud de prefijo
`Any`	Abreviación para ::/0 (Cualquier dirección)
`host`	Indica un solo host definido por *`source-ipv6-addr / destination-ipv6-addr`*
`operator`	(Opcional) operador condicional para buscar coincidencias (lt, gt, eq, neq, range)
`port`	(Opcional) Numero decimal para un puerto TCP/UDP

4.1 Listas de Control de Acceso

- Configuración de ACLs IPv6.
  - Las ACLs IPv6 contienen un `deny ipv6 any` implícito y varios `permit` para habilitar descubrimiento de vecinos por NDP.
  - Si se especifica `deny ipv6 any`, explícitamente, se boqueará NDP.

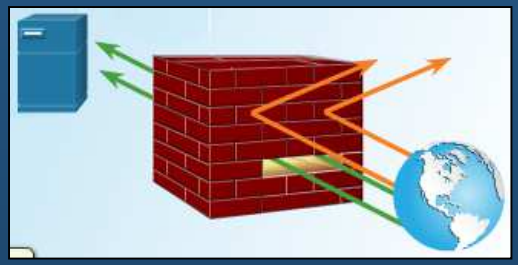

```
R1(config)# ipv6 access-list LAN_ONLY
R1(config-ipv6-acl)# permit 2001:db8:1:1::/64 any
R1(config-ipv6-acl)# permit icmp any any nd-na
R1(config-ipv6-acl)# permit icmp any any nd-ns
R1(config-ipv6-acl)# deny ipv6 any any
R1(config-ipv6-acl)# end
R1# show ipv6 access-list
IPv6 access list LAN_ONLY
    permit ipv6 2001:DB8:1:1::/64 any sequence 10
    permit icmp any any nd-na sequence 20
    permit icmp any any nd-ns sequence 30
    deny ipv6 any any sequence 40
R1#
```

4.2 Tecnologías de Firewall

- Definición de Firewall.
  - Originalmente: muro a prueba de fuego.
  - Redes: prevención de que tráfico no deseado entre a ciertas áreas de la red.
    - Resistencia a ataques.
    - Único punto de interconexión de redes.
    - Implementa las políticas de control de acceso.
  - 1988: DEC crea el primer filtro de tráfico sin estado, se realiza paquete a paquete, sin considerar flujos similar a las ACLs.
  - 1989: AT&T Bell desarrollan el primer firewall de estado completo. Evalúa estado de conexiones en flujos de datos. Reglas estáticas y dinámicas.
  - No eran dispositivos separados, sino un router con software añadido (ISR).
  - Con el tiempo surgieron los dispositivos separados, descargando de procesos a los routers.
  - Definición: Sistema o conjunto de ellos, que hace cumplir las políticas de control de acceso entre redes.

4.2 Tecnologías de Firewall

- Beneficios y Limitaciones de los Firewalls.



  - Beneficios:
    - Prevé la exposición de hosts y recursos sensibles.
    - Sanitiza el flujo de protocolos, prevee su explotación de fallas.
    - Bloquea datos maliciosos.
    - Reduce la complejidad de administración de seguridad.
  - Limitaciones:
    - Malas configuraciones, pueden volver vulnerable la red.
    - Los datos de muchas aplicaciones no pueden atravesar firewalls seguros.
    - Los usuarios puede buscar formas de que su tráfico atraviese el firewall, exponiendo la red a ataques.
    - El desempeño de la red se puede ver afectado.
    - Tráfico no autorizado puede entunelarse, o esconderse como tráfico legítimo.

4.2 Tecnologías de Firewall

- Tipos de Firewalls.
  - De filtrado de paquetes: Típicamente un router con capacidades de filtrado de tráfico en capas 3 y 4.
  - De estado completo (Clásicos): Monitorea el estado de las conexiones (inicio, transferencia, terminación), involucra capas 3 y 4 mas 5 (sesión).
  - De puerta de enlace de aplicaciones: Filtra información de capas 3,4,5 y 7 mediante un proxy o intermediario.

  - Basado en host: Pc/Servidor corriendo firewall de software.
  - Transparente: Filtra tráfico IP entre un par de interfaces puenteadas.
  - Hibrido: Una combinación de varios tipos de firewalls.

4.2 Tecnologías de Firewall

- Beneficios y Limitaciones de Firewall de Filtrado de Paquetes.
  - Ventajas del Filtrado de paquetes:
    - Implementados mediante sencillas sentencias `permit` o `deny`.
    - Bajo impacto en el desempeño de la red.
    - Fáciles de implementar, y soportados por muchos routers.
    - Grado inicial de seguridad a nivel de red.
    - Realizan la mayoría de las tareas de firewalls dedicados a bajo costo.
  - Desventajas:
    - Susceptibles a suplantación de IPs.
    - Solo revisan la cabecera TCP y admiten todos los fragmentos.
    - ACLs complejas pueden resultar difíciles de mantener.
    - No pueden filtrar dinámicamente algunos servicios (Dynamic Port Negotiations)
    - Sin estado, examinan cada paquete individualmente, sin conciencia del contexto.

4.2 Tecnologías de Firewall

- Firewall de estado completo (Clásico).
  - Mas versátiles y comunes.
  - Aunque considerados de capa 3, analizan información de capas 4 y 5.
  - Filtran paquetes consientes del estado de una conexión.
    - Mantiene registro (tabla de estado) de las conexiones en una interfaz y sentido.
      - Verifica que sean válidas.

10.1.1.1 Solicita una página web a 209.165.201.3

El router en base a la información de estado, agrega una ACE dinámica para permitir el tráfico de regreso

Inside ACL (Outgoing Traffic)	Outside ACL (Incoming Traffic)
permit 10.1.1.0.0.0.0.255 any	Dynamic: permit tcp host 209.165.201.3 eq 80 host 10.1.1.1 eq 1500

4.2 Tecnologías de Firewall

- Beneficios y Limitaciones de Firewalls de Estado Completo.
  - Beneficios:
    - Medio principal de defensa.
    - Filtrado de paquetes robusto.
    - Desempeño mejorado sobre filtrado de paquetes.
    - Defensa contra ataques de spoofing y DoS.
    - Registros (logs) mas detallados.
    - Mejor rendimiento (menos procesamiento requerido) que un proxy.
  - Limitaciones:
    - No realizan inspección en capa 7 (de aplicación).
    - Seguimiento limitado para protocolos sin estado (UDP, ICMP).
    - Difícil defender aplicaciones que usen negociación dinámica de puerto.
    - No soporta autenticación.

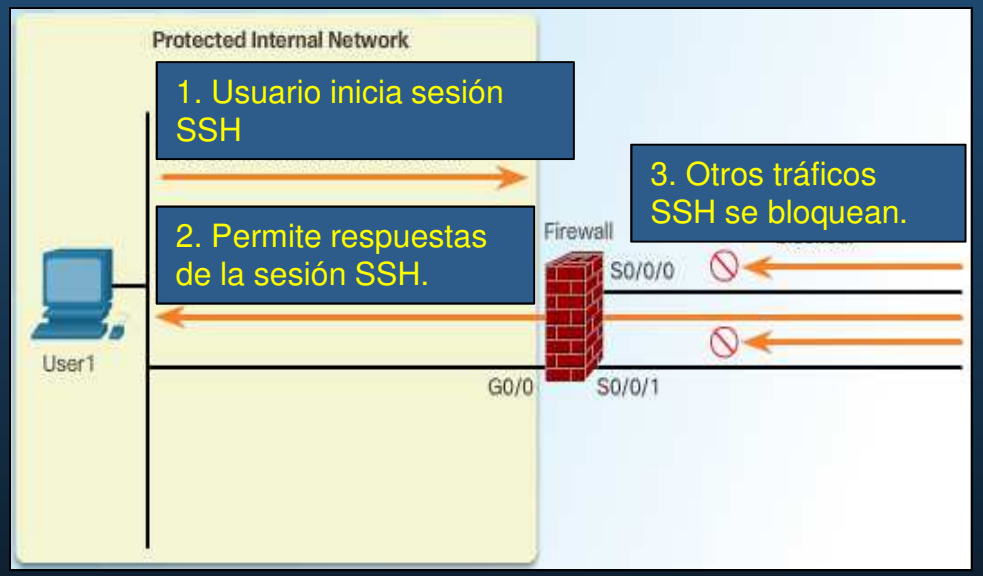
4.2 Tecnologías de Firewall

- Firewalls de Siguiente Generación.
  - Identificación Granular, visibilidad y control de comportamientos en aplicaciones
  - Restricción de aplicaciones web basados en la reputación del sitio.
  - Protección proactiva contra riesgos de Internet.
  - Cumplimiento de políticas de seguridad basadas en usuario, dispositivo, rol, aplicación, y perfil de amenazas.
  - Desempeño compatible con NAT, VPN, e Protocolo de Inspección de Estado Completo (SPI).
  - Uso de sistemas de prevención de intrusiones (IPS).

  - Servcios Cisco Sourcefire's FirePOWER en Cisco Adaptive Security Appliance (ASA).
    - Diseñado para proteger antes, durante y despues de un ataque.

4.2 Tecnologías de Firewall

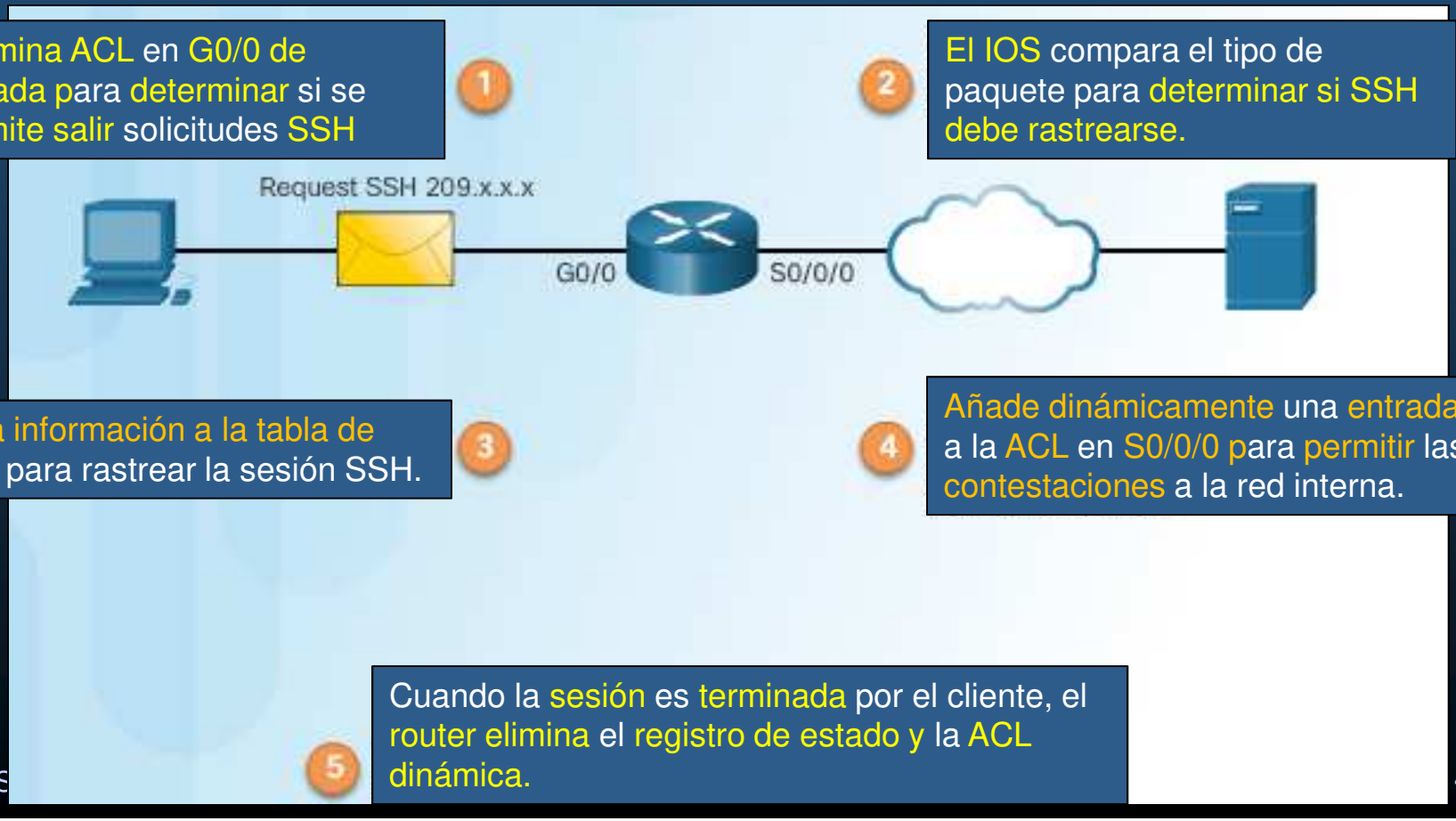
- Introducción a Firewalls Clásicos.
  - Denominados Firewall de Control de Acceso Basado en Contexto (CBAC).
    - Firewall de estado completo disponible en IOS 12.0 y posteriores.
    - Soporta examinar NAT/PAT.
    - Bloquea P2P.
    - Cuatro principales funciones:
      - Filtrado de tráfico.
      - Inspección de tráfico.
      - Detección de intrusiones.
      - Generación de alertas y registros.



    - Solo filtra protocolos especificados por administrador.
    - Solo detecta/protege ataques que atraviesen el firewall (no internos).

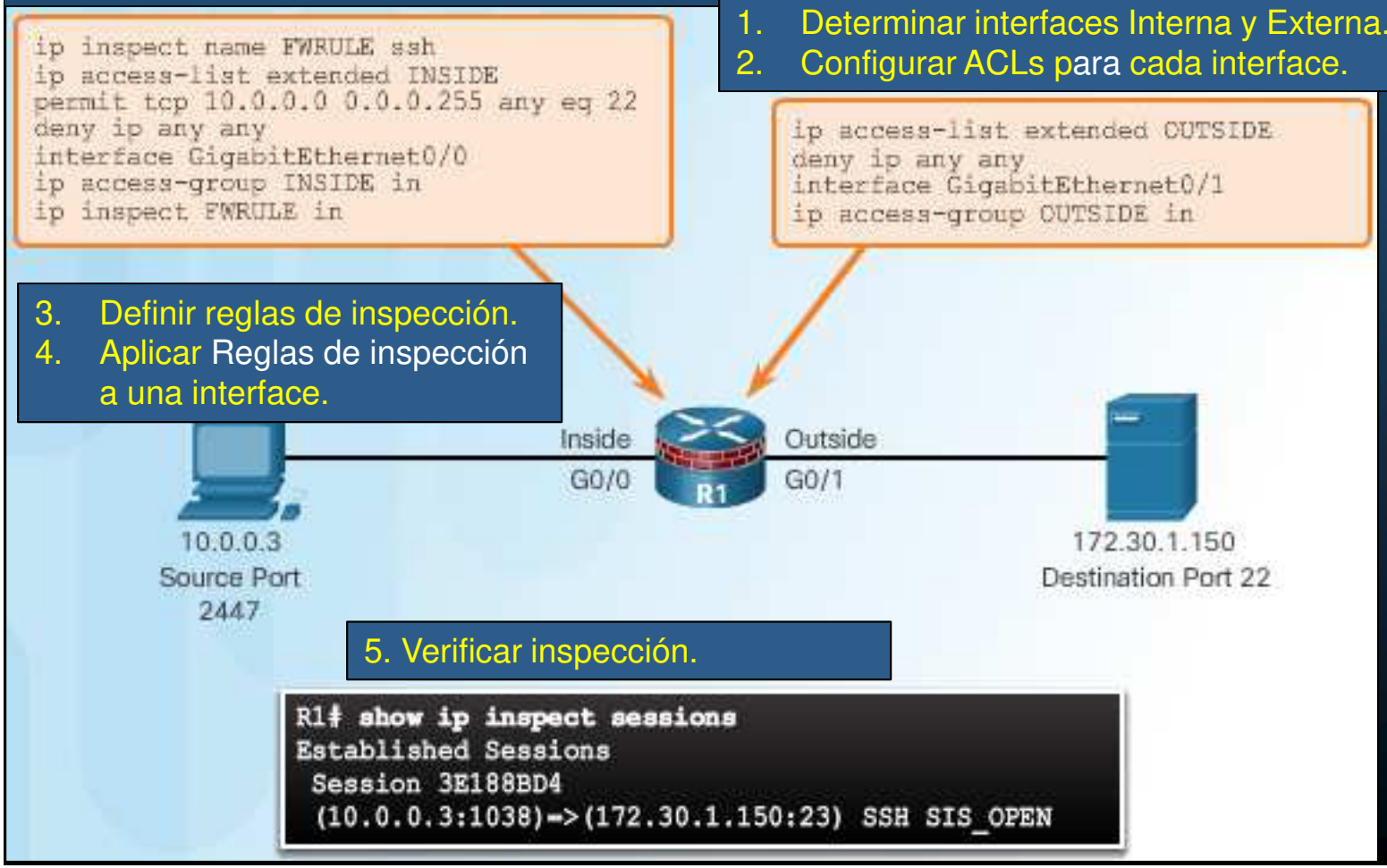
4.2 Tecnologías de Firewall

- Operación de un Firewall Clásico.
  - Un firewall clásico crea una ACL temporal para permitir el tráfico de regreso.
    - Da de baja la ACL cuando la conexión termina o permanece inactiva.



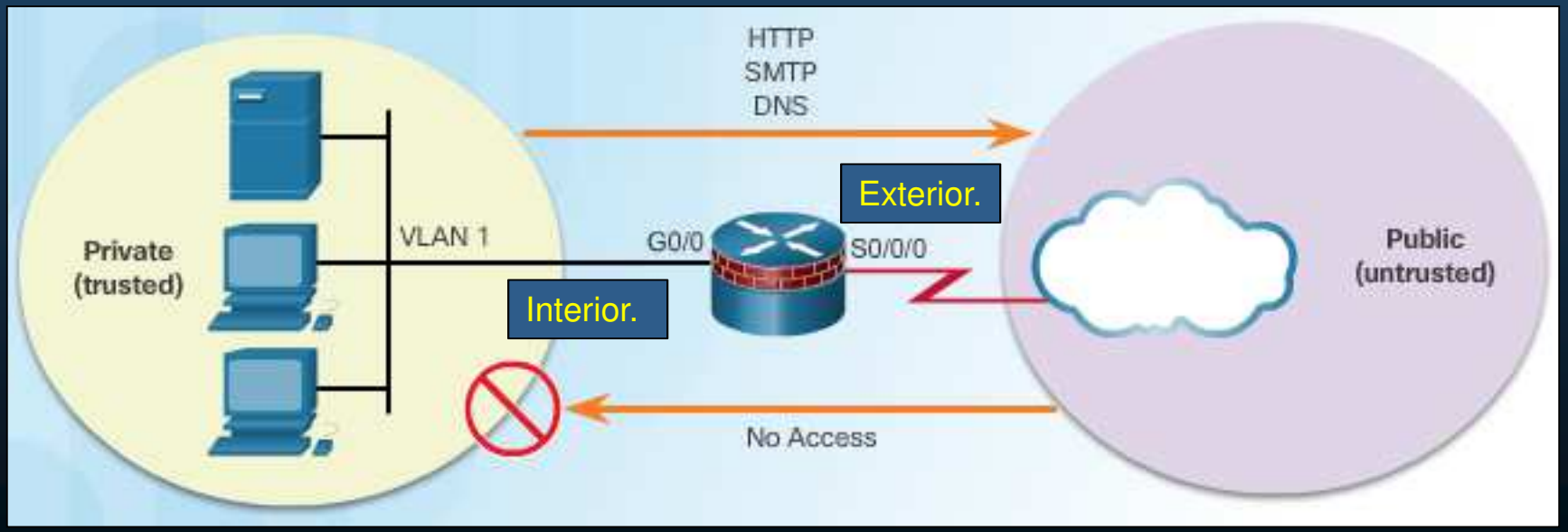
4.2 Tecnologías de Firewall

- Configuración de un FireWall Clásico.
  - Permitir SSH de 10.0.0.0 a 172.30.0.0 (Solo conexiones en ese sentido)



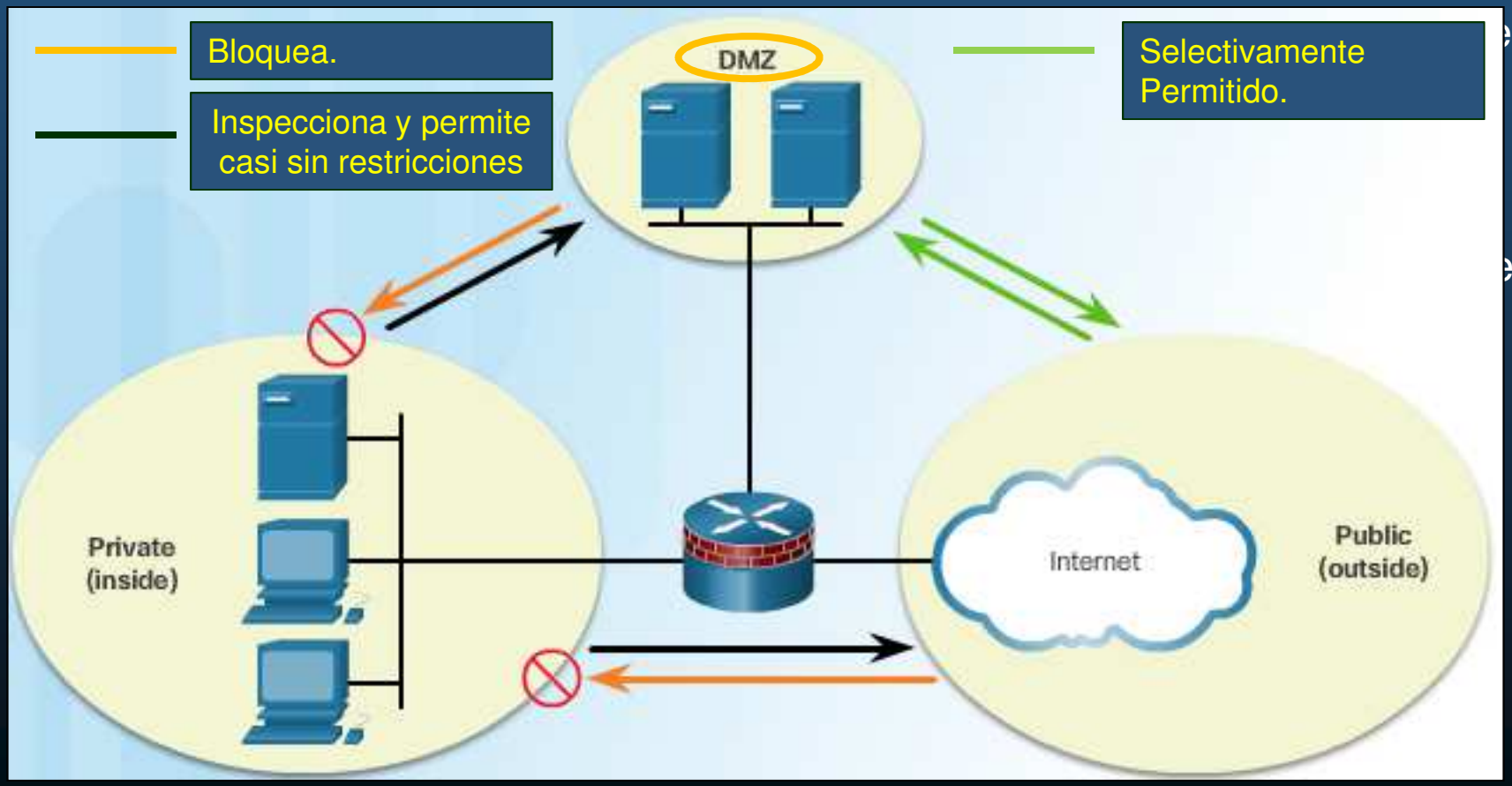
4.2 Tecnologías de Firewall

- Redes Interior y Exterior.
  - Determinadas por dos interfaces de un router.
    - Trafico saliente de la red interna a la externa, se permite e inspecciona.
      - Tráfico inspeccionado de regreso, se permite.
    - Tráfico entrante, originado en la red externa hacia la red interna, generalmente se bloquea.



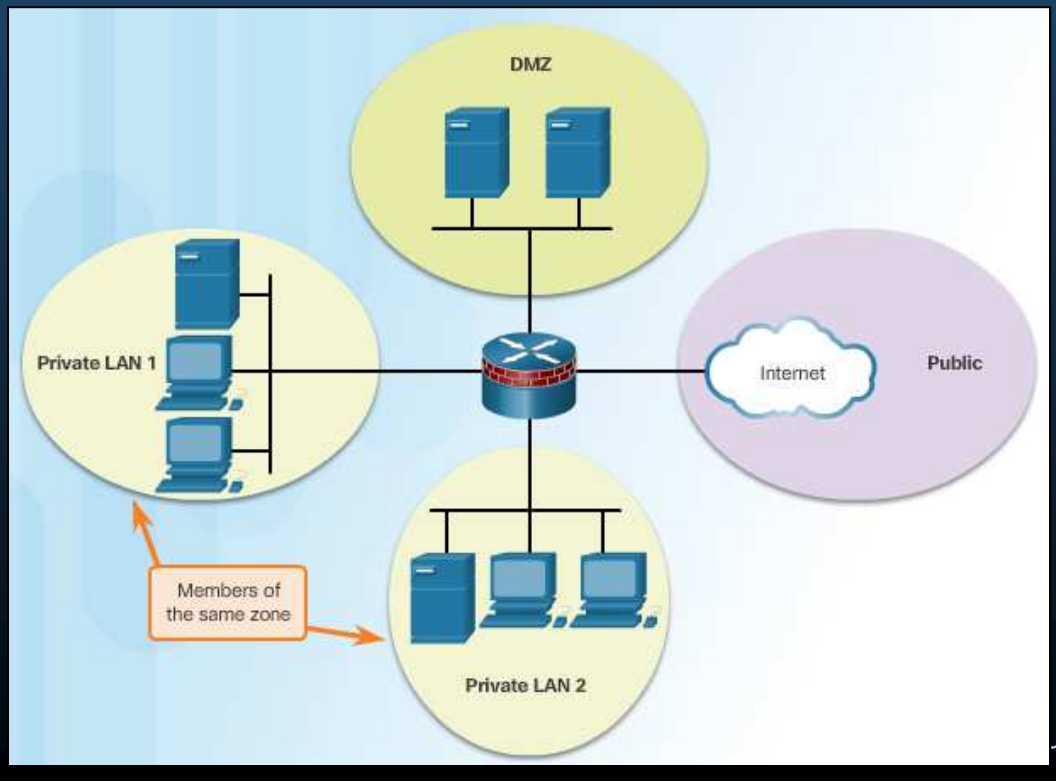
4.2 Tecnologías de Firewall

- Zonas Desmilitarizadas (DMZ).
  - Diseño, un firewall 3 interfaces, pública, privada y desmilitarizada.



4.2 Tecnologías de Firewall

- Firewall con Politicas basadas en Zonas ZPFs.
  - Zona: conjunto de interfaces con funciones y características similares.
  - El tráfico entre interfaces de una misma zona debe viajar libremente.
  - El tráfico entre zonas se bloquea a menos que se configure alguna política.
    - Excepto tráfico generado por el router (plano de control: SSH, SNMP, Enrutamiento).



4.2 Tecnologías de Firewall

- Defensa por Capas.
  - Uso de diferentes tipos de firewalls por capas en diferentes niveles y dispositivos(zonas, routers, hosts) denominada: Configuración de Subred Filtrada.

Seguridad de Punto Final: Cumplimiento de políticas de seguridad de dispositivo e identidades

Seguridad de Comunicaciones.

Seguridad de Perímetro: fronteras entre zonas.

Seguridad de Núcleo de Red: Protección contra software malicioso y anomalías de tráfico.

4.2 Tecnologías de Firewall

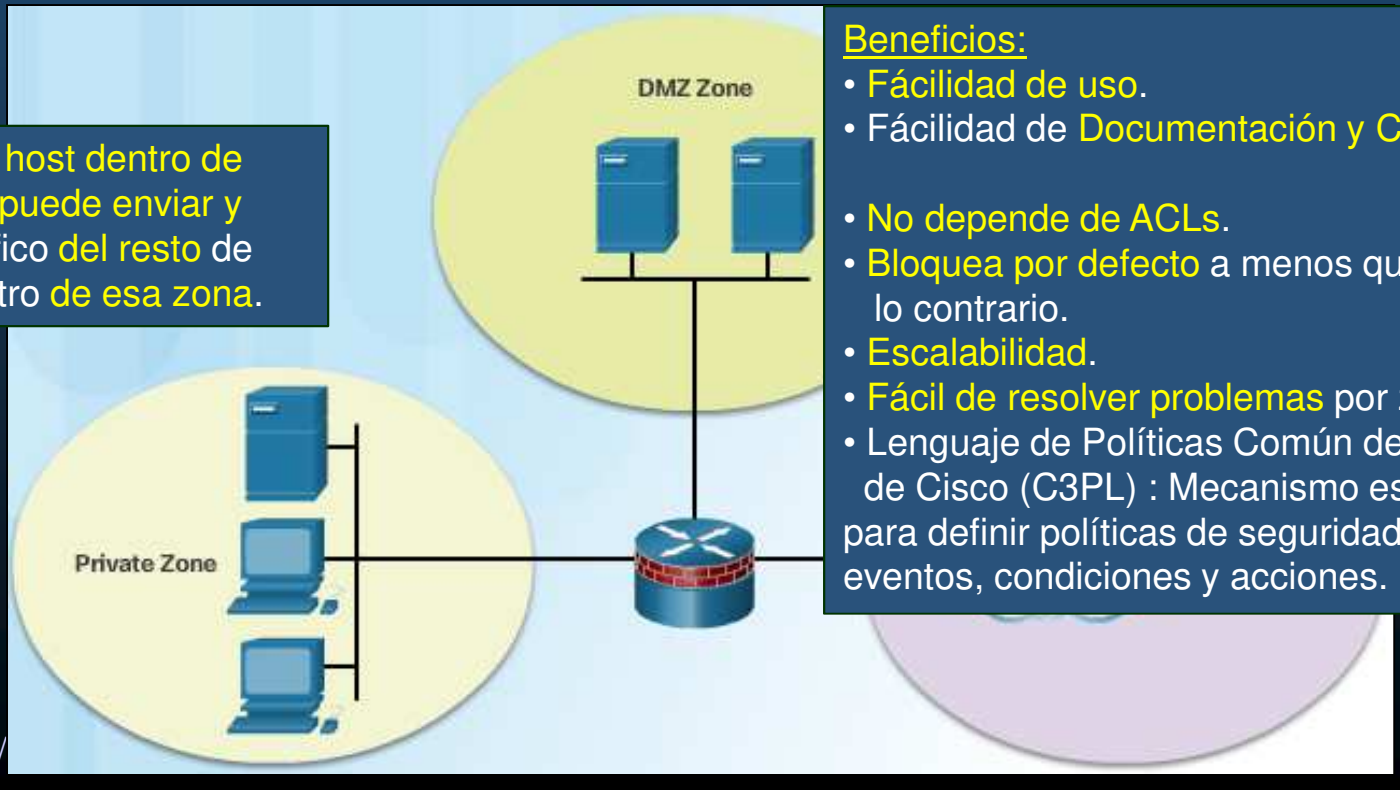
- Consideraciones para Implementación de una Defensa Completa.
  - Colocar Firewalls en fronteras de seguridad.
  - No confiar exclusivamente a los Firewalls la seguridad de la red.
  - Denegar todo el tráfico por defecto, permitir solo lo necesario.
  - Asegurarse de controlar accesos.
  - Los Firewalls no sustituyen a usuarios informados.
  - Monitorear regularmente los registros (logs) del Firewall.
  - Practicar cambios administrativos para cambios de configuración.

  - Los Firewalls no detienen intrusos internos.
  - Los Firewalls no protegen contra instalación de A.P.s no autorizados en redes seguras.
  - Los Firewalls no suplen backups, para recuperarse de ataques.
  - Los Firewalls no sustituyen a usuarios informados.

4.3 Firewall con Políticas Basadas en Zonas

- Seguridad por Zonas y Politicas de Firewall: ZPF
  - Dos configuraciones para el IOS de un Firewall.
    - Clásico: Las políticas de firewall se aplican por interfaces.
    - ZPF: Se asignan zonas de seguridad a las interfaces; Las políticas del firewall se aplican al tráfico que viaja entre zonas.

Cualquier host dentro de una zona puede enviar y recibir tráfico del resto de hosts dentro de esa zona.

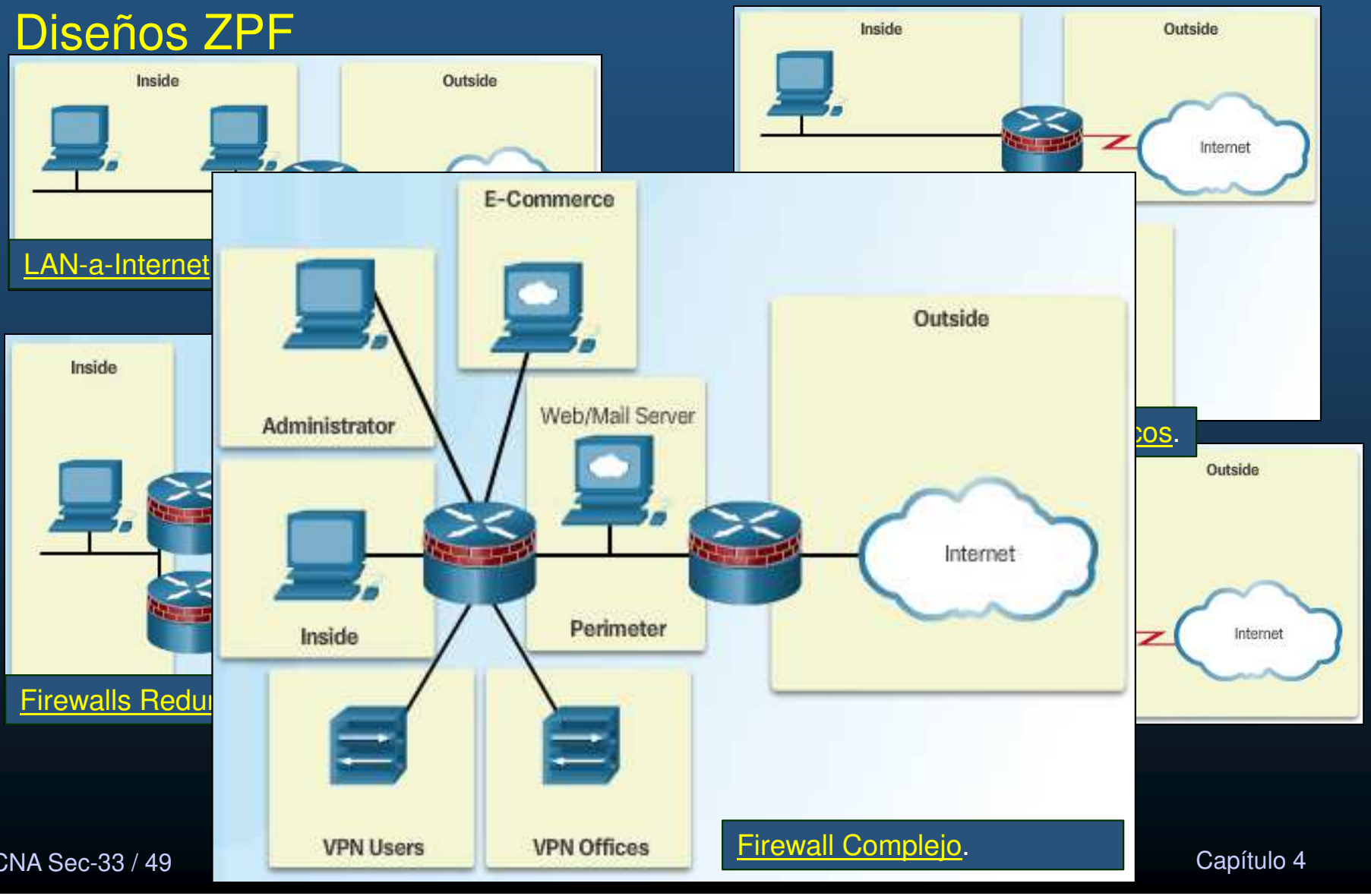


Beneficios:
- Fácilidad de uso.
- Fácilidad de Documentación y Comunicación.

- No depende de ACLs.
- Bloquea por defecto a menos que se indique lo contrario.
- Escalabilidad.
- Fácil de resolver problemas por zonas.
- Lenguaje de Políticas Común de Clasificación de Cisco (C3PL) : Mecanismo estructurado para definir políticas de seguridad, basado en eventos, condiciones y acciones.

4.3 Firewall con Políticas Basadas en Zonas

- Diseños ZPF



4.3 Firewall con Políticas Basadas en Zonas

- Pasos para definir un Diseño ZPF

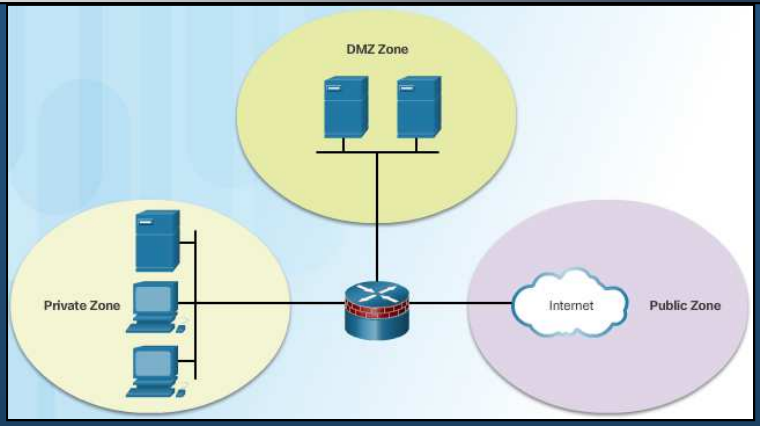
1. Determinar las Zonas: Separar la red en zonas.
2. Establecer políticas entre zonas: Definir por pares de zonas los servicios cliente-servidor requeridos (TCP/UDP/ICMP/etc).
3. Diseñar la infraestructura física: Tomar en cuenta requisitos de disponibilidad, numero de dispositivos por zona, zonas mas y menos seguras, así como zonas intermedias, y dispositivos redundantes.
4. Identificar subconjuntos dentro de las zonas y mezclar requerimientos de tráfico: Las subzonas se configuran por interface, y se mezclan sus requisitos de tráfico. (Su configuración queda fuera del alcance de este curso).

4.3 Firewall con Políticas Basadas en Zonas

- Operación y Acciones ZPF
  - Inspeccionar (`inspect`): Inspección de paquetes de estado completo.
  - Desechar (`drop`): Similar a la sentencia `deny` de una ACL, se recomienda incluir en los logs.
  - Admitir (`pass`): Análogo a la sentencia `permit` de una ACL (no rastrea el estado de las conexiones o sesiones).

4.3 Firewall con Políticas Basadas en Zonas

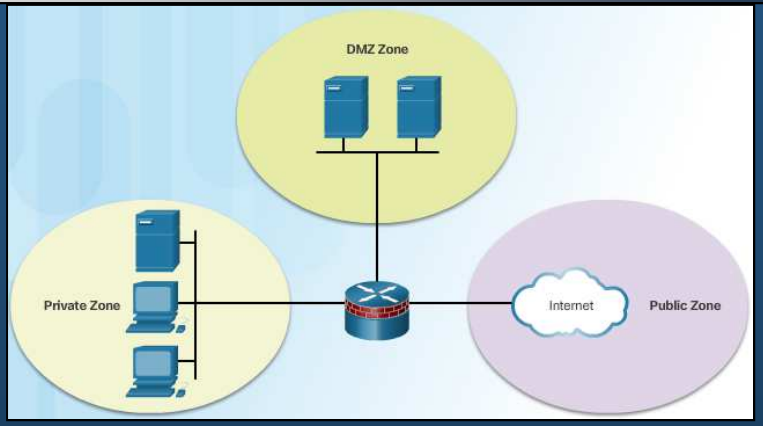
- Reglas para el Tránsito de Tráfico
  - Las transiciones de tráfico entre interfaces de un router dependen en si las interfaces de ingreso y egreso pertenecen o no a la misma zona.



Interfaz origen ¿miembro de una zona?	Interfaz destino ¿miembro de una zona?	¿Existe Par de Zonas?	¿Existe Política?	Resultado
NO	NO	N/A	N/A	ADMITE
SI	NO	N/A	N/A	DESECHA
NO	SI	N/A	N/A	DESECHA
SI (Privada)	SI (Privada)	N/A	N/A	ADMITE
SI (Privada)	SI (Pública)	NO	N/A	DESECHA
SI (Privada)	SI (Pública)	SI	NO	ADMITE
SI (Privada)	SI (Pública)	SI	SI	INSPECCIONA

4.3 Firewall con Políticas Basadas en Zonas

- Reglas para el Tránsito de Tráfico hacia la Zona Propia
  - Zona propia se refiere al router mismo.
  - Las reglas dependen en si el router es el origen o el destino del tráfico y si existe par de zona y política.

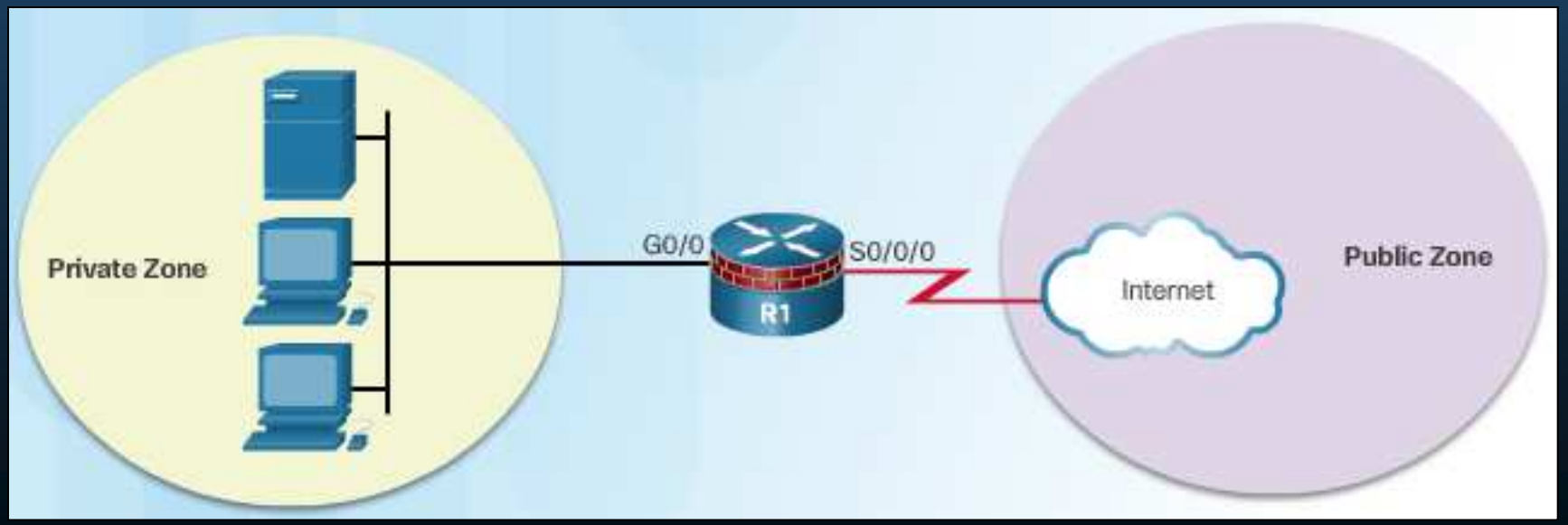


Interfaz origen ¿miembro de una zona?	Interfaz destino ¿miembro de una zona?	¿Existe Par de Zonas?	¿Existe Política?	Resultado
SI (Zona Propia)	SI	NO	N/A	ADMITE
SI (Zona Propia)	SI	SI	NO	ADMITE
SI (Zona Propia)	SI	SI	SI	INSPECCIONA
SI	SI (Zona Propia)	NO	N/A	ADMITE
SI	SI (Zona Propia)	SI	NO	ADMITE
SI	SI (Zona Propia)	SI	SI	INSPECCIONA

4.3 Firewall con Políticas Basadas en Zonas

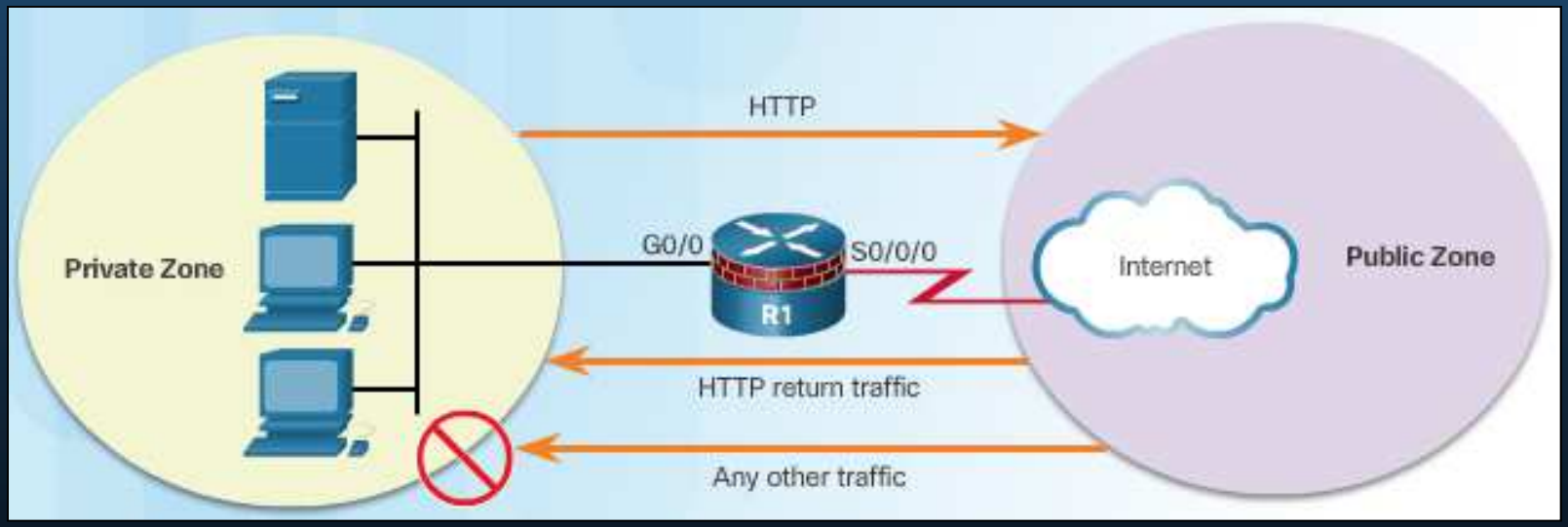
- Configuración de un ZPF

1. Crear las zonas.
2. Identificar tráfico con un mapa de clases.
3. Definir acciones con un mapa de políticas.
4. Identificar pares de zonas y alinear a un mapa de políticas.
5. Asignar zonas a las interfaces adecuadas.



4.3 Firewall con Políticas Basadas en Zonas

- Creación de Zonas
  - Determinar:
    - Que interfaces deben incluirse en cada zona.
    - Cual será el nombre de cada zona.
    - Que tráfico se requerirá entre zonas y en que dirección.

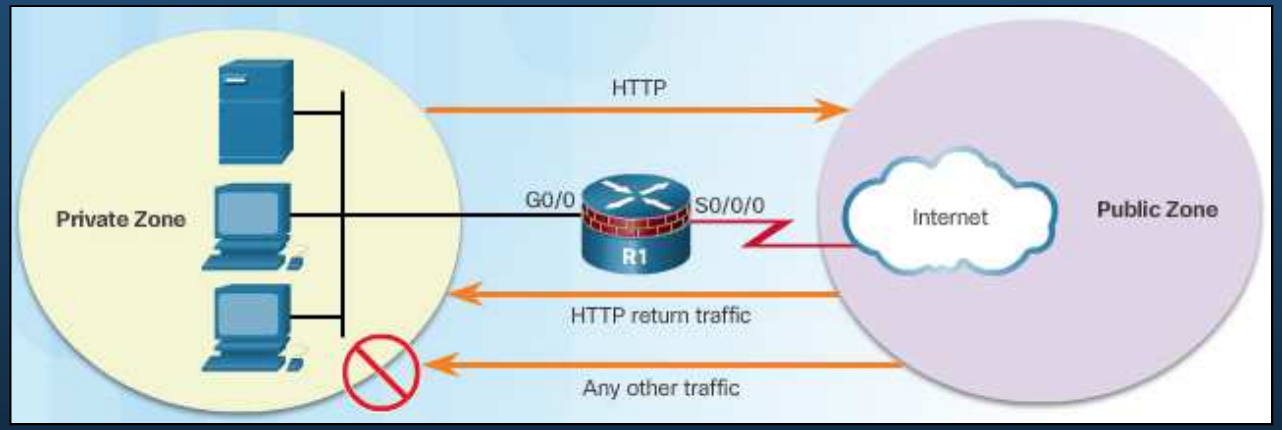



```
Router(config)# zone security zone-name
```

```
R1(config)# zone security PRIVATE
R1(config-sec-zone)# exit
R1(config)# zone security PUBLIC
```

4.3 Firewall con Políticas Basadas en Zonas

- Identificar Tráfico
  - Una clase, identifica un conjunto de paquetes en base a sus contenidos.
  - Típicamente se definen clases para aplicarles políticas de seguridad.

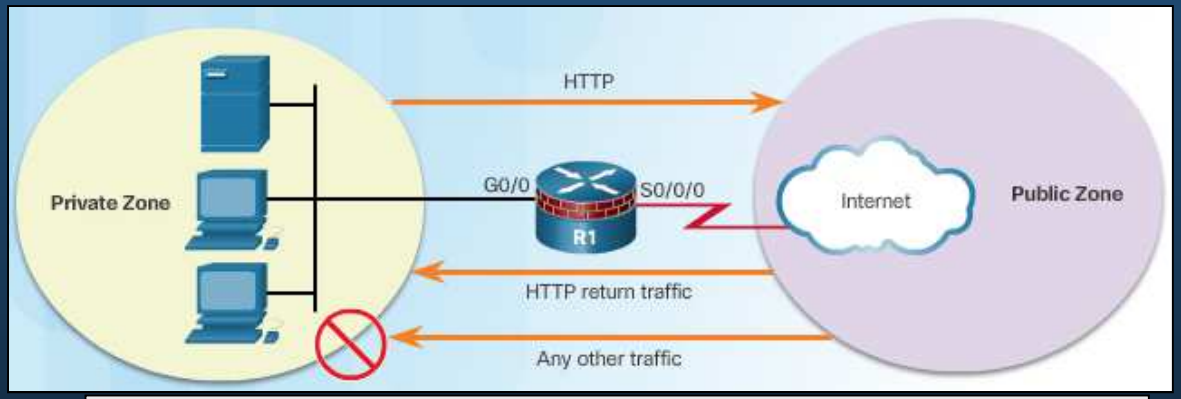



```
Router(config)# class-map type inspect [match-any | match-all] class-map-name
```

Parámetro	Descripción
match-any	Los paquetes deben cumplir al menos con un criterio para ser considerados miembros de la clase.
match-all	Los paquetes deben cumplir todos los criterios para ser considerados miembros de la clase.
class-map-name	Nombre del mapa de clase.

4.3 Firewall con Políticas Basadas en Zonas

- Identificar Tráfico
  - Una clase, identifica un conjunto de paquetes en base a sus contenidos.
  - Típicamente se definen clases para aplicarles políticas de seguridad.

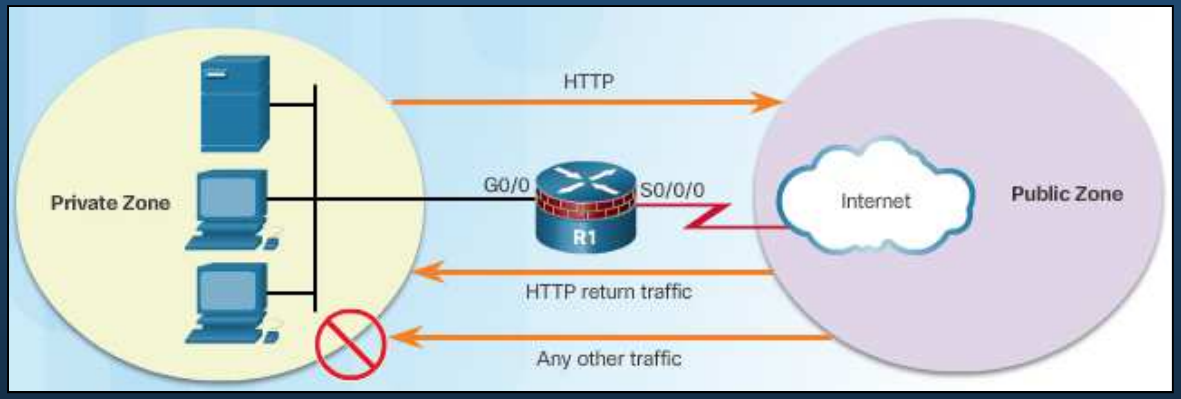



```
Router(config-cmap)# match access-group {acl-# | acl-name }
Router(config-cmap)# match protocol protocol-name
Router(config-cmap)# match class-map class-map-name
```

Parámetro	Descripción
`match access-group`	Configura los criterios de match, por los de una ACL.
`match protocol`	Configura los criterios de match para un protocolo específico.
`match class-map`	Usa otro `class-map`, para identificar el tráfico.

4.3 Firewall con Políticas Basadas en Zonas

- Identificar Tráfico
  - Una clase, identifica un conjunto de paquetes en base a sus contenidos.
  - Típicamente se definen clases para aplicarles políticas de seguridad.

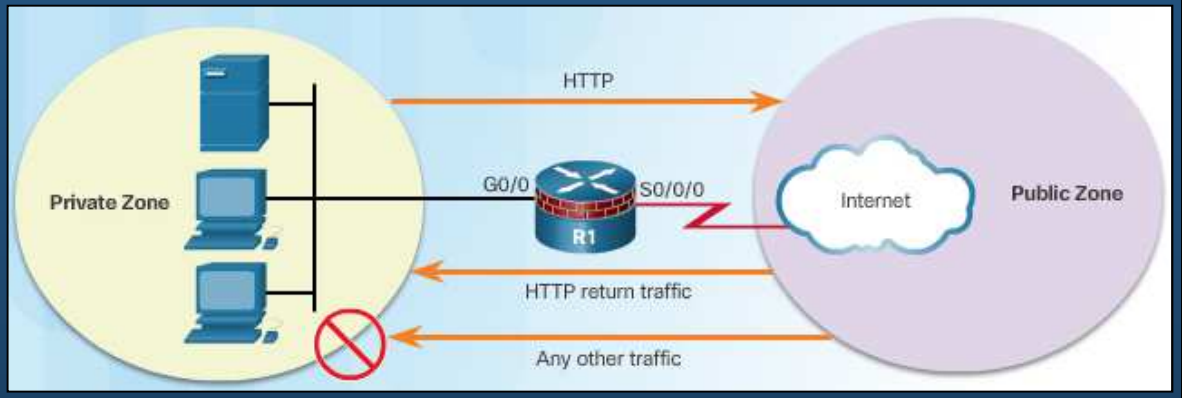


  - Ejemplo:

```
R1(config)# class-map type inspect match-any HTTP-TRAFFIC
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# match protocol dns
```

4.3 Firewall con Políticas Basadas en Zonas

- Definir una Acción
  - Utilizar un policy-map para definir acciones ante tráfico de alguna clase.




```
Router(config)# policy-map type inspect policy-map-name
Router(config-pmap)# class type inspect class-map-name
Router(config-pmap-c)# { inspect | drop | pass }
```

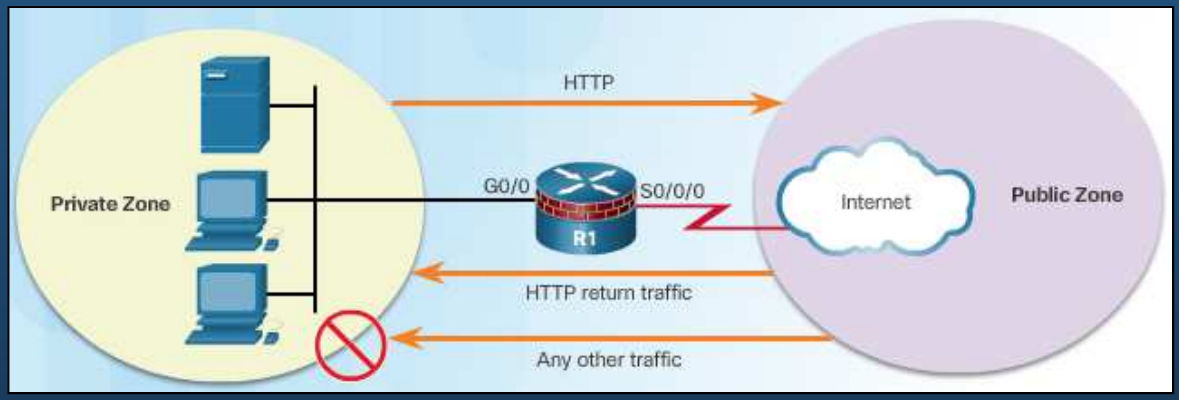
Parámetro	Descripción
inspect	Inspecciona: Ofrece control de tráfico basado en estado (mantiene información de conexiones y permite tráfico de retorno)
drop	Desecha: Descarta el tráfico.
pass	Admite: Acción sin estado, permite al router reenviar el tráfico de una zona a otra.

- Ejemplo:

```
R1(config)# policy-map type inspect PRIV-TO-PUB-POLICY
R1(config-pmap)# class type inspect HTTP-TRAFFIC
R1(config-pmap-c)# inspect
```

4.3 Firewall con Políticas Basadas en Zonas

- Identificar Pares de Zonas y Asignar Políticas



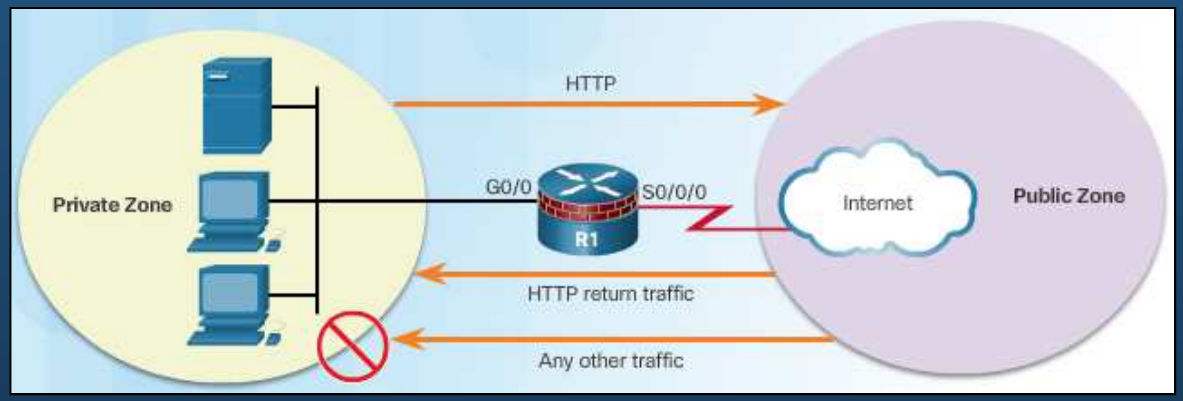

```
Router(config)# zone-pair security zone-pair-name source {source-zone-name | self
} destination {destination-zone-name | self }
Router(config-sec-zone-pair)# service-policy type inspect policy-map-name
```

Parámetro	Descripción
`source source-zone-name`	Especifica el nombre de la zona donde se origina el tráfico.
`Destination dest-zone-name`	Especifica el nombre de la zona a donde se destina el tráfico.
`self`	Indica que el tráfico se genera o destina en el mismo router.

```
R1(config)# zone-pair security PRIV-PUB source PRIVATE destination PUBLIC
R1(config-sec-zone-pair)# service-policy type inspect PRIV-TO-PUB-POLICY
```

4.3 Firewall con Políticas Basadas en Zonas

- Asignar Zonas a Interfaces




```
Router(config-if)# zone-member security zone-name
```

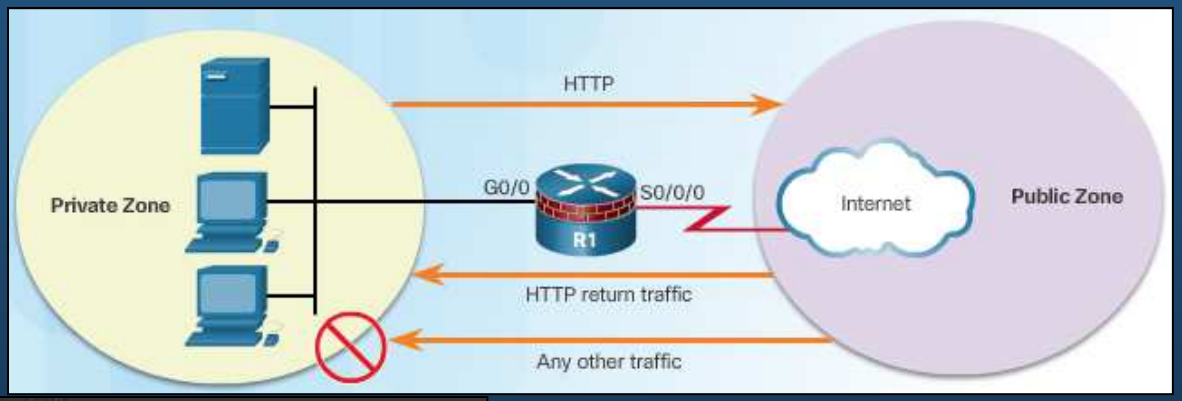
- Ejemplo:

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# zone-member security PRIVATE
R1(config-if)# interface Serial 0/0/0
R1(config-if)# zone-member security PUBLIC
```

- Nota:
  - Asignar zonas a interfaces sin haber definido políticas de seguridad causará que todo el tráfico sea descartado.

4.3 Firewall con Políticas Basadas en Zonas

- Verificar Configuración ZPF (`show run`)



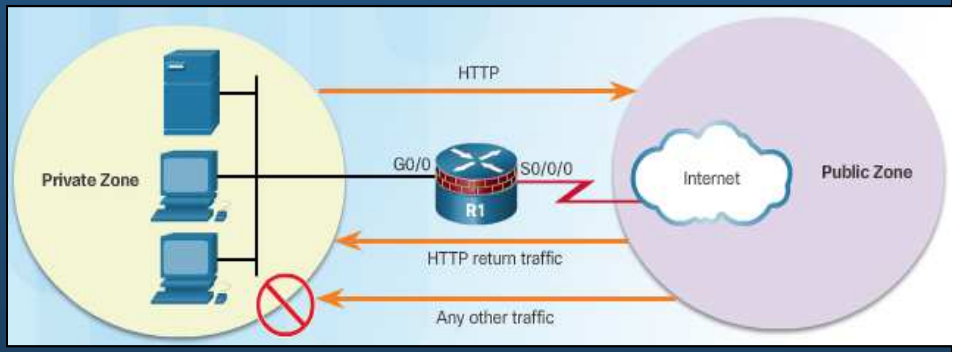

```
R1# show run | begin class-map
!
<some output omitted>
!
class-map type inspect match-any HTTP-TRAFFIC
 match protocol http
 match protocol https
 match protocol dns
!
policy-map type inspect PRIV-TO-PUB-POLICY
 class type inspect HTTP-TRAFFIC
  inspect
 class class-default
  drop
!
```

Note, que `class-default`, no es miembro de la clase `HTTP-TRAFFIC`

```
zone security PRIVATE
zone security PUBLIC
zone-pair security PRIV-PUB source PRIVATE destination PUBLIC
 service-policy type inspect PRIV-TO-PUB-POLICY
!
interface GigabitEthernet0/0
 zone-member security PRIVATE
!
interface Serial0/0/0
 zone-member security PUBLIC
!
```

4.3 Firewall con Políticas Basadas en Zonas

- Verificar Configuración ZPF (`show policy-map ...`)




```
R1# show policy-map type inspect zone-pair sessions

policy exists on zp PRIV-PUB
  Zone-pair: PRIV-PUB

  Service-policy inspect : PRIV-TO-PUB-POLICY

    Class-map: HTTP-TRAFFIC (match-any)
      Match: protocol http
        12 packets, 384 bytes
        30 second rate 0 bps
      Match: protocol https
        5 packets, 160 bytes
        30 second rate 0 bps
      Match: protocol dns
        0 packets, 0 bytes
        30 second rate 0 bps

    Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session 2204E220 (192.168.1.3:1049)=>(10.1.1.2:443) https:tcp
SIS_OPEN/TCP_CLOSEWAIT
          Created 00:00:14, Last heard 00:00:11
          Bytes sent (initiator:responder) [821:1431]

    Class-map: class-default (match-any)
      Match: any
      Drop
        4 packets, 160 bytes
R1#
```

1.

2.

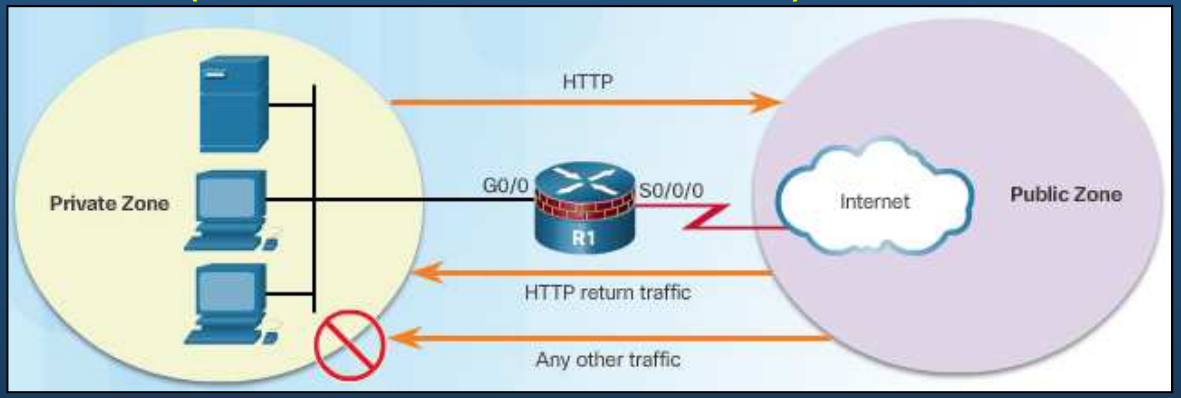
3.

C:> `ping 10.1.1.2` (servidor web)

4.3 Firewall con Políticas Basadas en Zonas

- Verificar Configuración ZPF (verificación adicional)

```
Router# show class-map type inspect
Router# show zone security
Router# show zone-pair security
Router# show policy-map type inspect
```




```
R1# show class-map type inspect
 Class Map type inspect match-any HTTP-TRAFFIC (id 1)
   Match protocol http
   Match protocol https
   Match protocol dns

R1# show zone security
zone self
Description: System Defined Zone

zone PRIVATE
 Member Interfaces:
 GigabitEthernet0/0

zone PUBLIC
 Member Interfaces:
 Serial0/0/0
```

```
R1# show zone-pair security
Zone-pair name PRIV-PUB
    Source-Zone PRIVATE  Destination-Zone PUBLIC
    service-policy PRIV-TO-PUB-POLICY
```

```
R1# show policy-map type inspect
  Policy Map type inspect PRIV-TO-PUB-POLICY
    Class HTTP-TRAFFIC
      Inspect
    Class class-default
      Drop
```

4.3 Firewall con Políticas Basadas en Zonas

- Consideraciones sobre ZPF.
  - No hay filtros para el tráfico intrazona.
  - Solo se admite una zona por interfaz.
  - No es posible configurar Firewall Clásico y ZPF en una misma interfaz.
  - Si solo se configura membrecía a una zona todo el tráfico se desecha.
  - Solo el tráfico explícitamente permitido entre zonas es reenviado.
  - Tráfico a la zona propia no es filtrado.

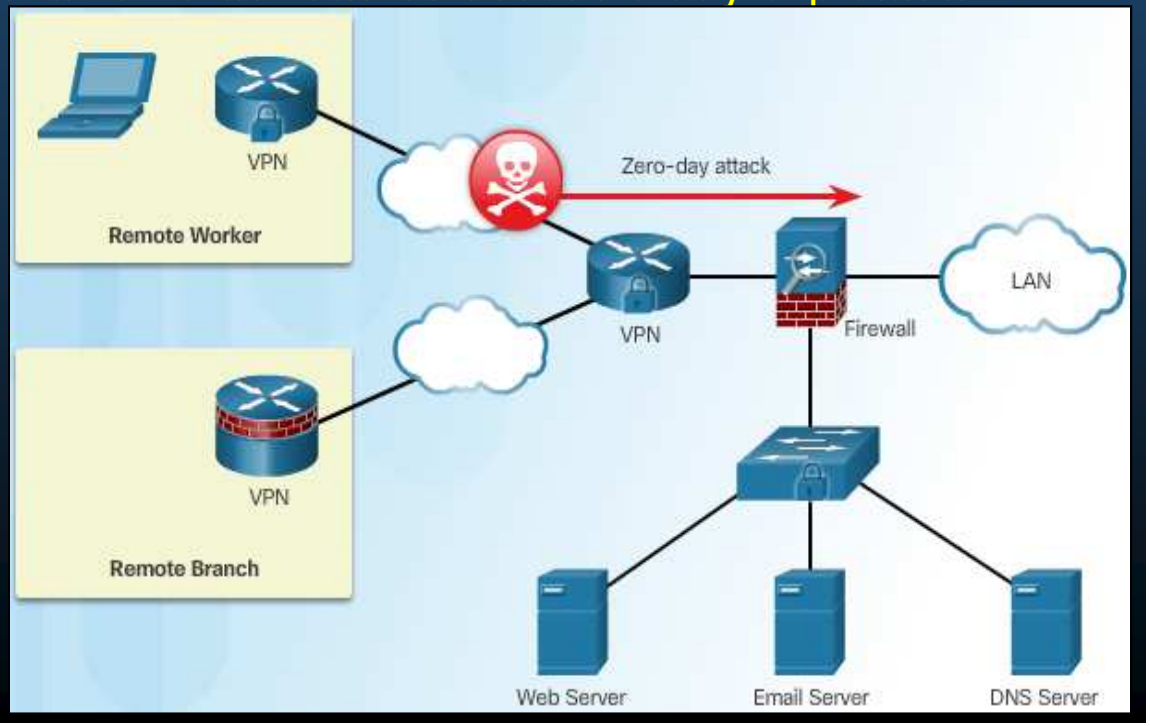
Capítulo 5

Implementando Sistemas de Prevención de Intrusos (IPS)

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#5.1.1.1

5.1 Tecnologías IPS

- Ataque de Día Cero.
  - Una red debe reconocer y mitigar amenazas.
  - Un firewall no puede proteger contra ataques de día cero.
  - Ataque de día cero: ataque que busca explotar vulnerabilidades desconocidas.
  - Hora cero: Momento en que la vulnerabilidad es descubierta y explotada.
    - Toma tiempo desarrollar un parche de seguridad: *tiempo vulnerable*.
      - Defensa contra estos ataques requiere medidas mas sofisticadas.

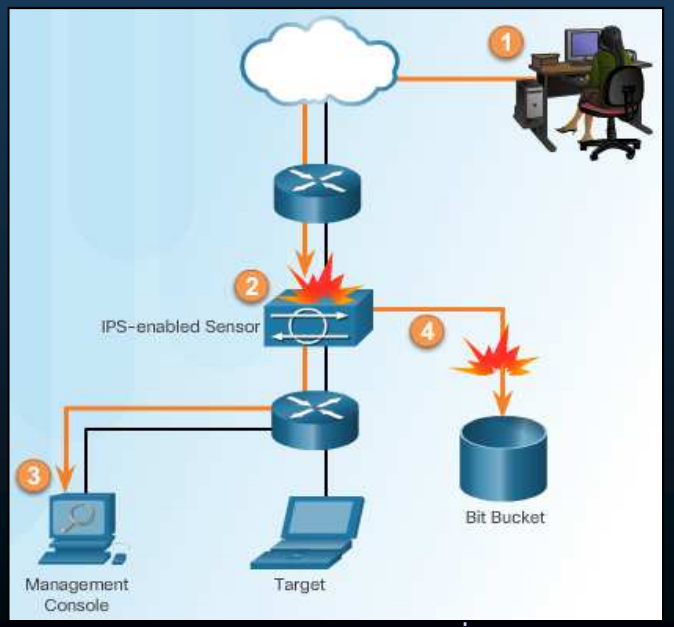


5.1 Tecnologías IPS

- Monitoreo contra Ataques.
  - Monitorear y analizar logs. (solución poco escalable)
  - Sistema de Detección de Intrusos (IDS):
    - Copia el flujo de tráfico (modo promiscuo).
    - Analiza la copia offline.
    - Busca firmas maliciosas.
      - Trabaja de forma pasiva.
      - IDS en posición estratégica, solo trafico duplicado pasa por IDS.
      - No afecta de forma negativa el flujo real.
    - No detiene ataque.
    - Requiere de routers o firewalls para detener ataques.

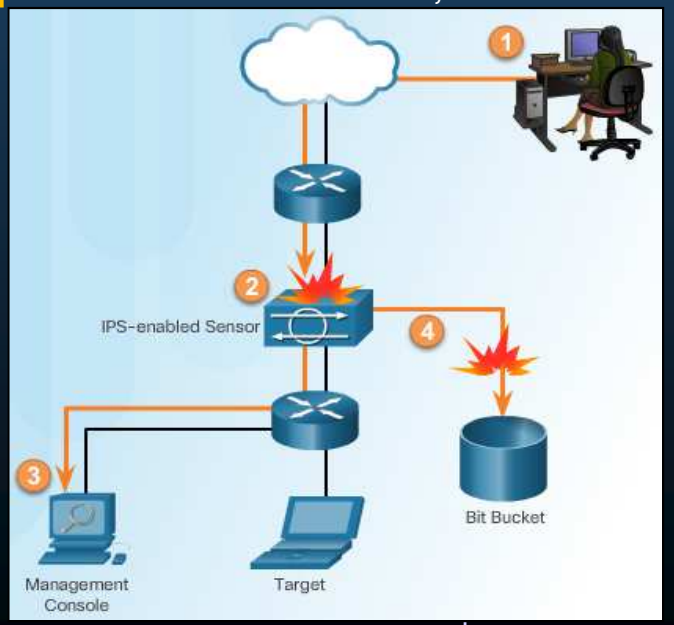
5.1 Tecnologías IPS

- Detección y Detención de Ataques.
  - Un IPS se basa en tecnologías IDS para identificar, detener y bloquear ataques.
  - Se implementa en línea (el tráfico entrante y saliente debe atravesarlo).
    - No permite ingreso de tráfico sin analizarlo.
    - Monitorea tráfico en capas 3 y 4.
    - Analiza la carga útil, buscando ataques mas sofisticados que incluyan datos maliciosas en las capas 2 a 7.
    - 3 Tecnologías de detección Cisco:
      - Basado en Firmas.
      - Basado en Perfiles.
      - Basado en Análisis de Protocolos.
    - Mal configurados, pueden afectar considerablemente el flujo de tráfico.



5.1 Tecnologías IPS

- Similitudes entre Tecnologías IDS e IPS.
  - Ambas se catalogan como sensores.
    - Router con IOS con Software IPS.
    - IDS/IPS dedicado.
    - Modulo de red con ASA, router o switch.
  - Ambas tecnologías utilizan firmas para detectar patrones de mal uso, en el tráfico de red.
  - Ambas pueden detectar patrones atómicos (de un solo paquete).
  - Ambas pueden detectar patrones compuestos (de multi-paquete).



5.1 Tecnologías IPS

- Ventajas y Desventajas entre Tecnologías IDS e IPS.

	Ventajas	Desventajas
IDS	• No impacta la Red. • No impacta el fallo de sensores. • No impacta la sobrecarga de sensores.	• Acciones de respuesta no detienen packetes trigger (maliciosos). • Requiere de otros dispositivos para responder a ataques. • Afinamiento en configuración requerido para establecer acciones de respuesta. • Más vulnerable a técnicas de evasión de seguridad de red.
IPS	• Detiene paquetes trigger. • Puede emplear técnicas de normalización de flujo	• Problemas en el sensor pueden afectar el flujo de tráfico. • Sobrecarga del sensor impacta la red. • Impacto en la red: Latencia y Jitter.

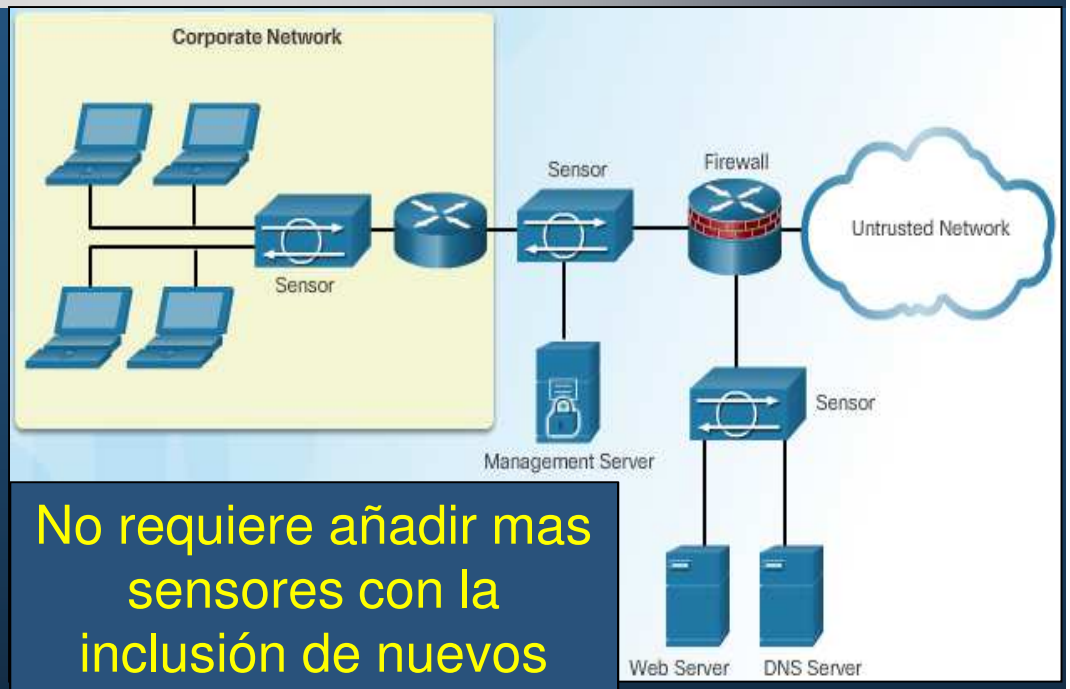
5.1 Tecnologías IPS

- IPS basado en host.
  - Los IPS pueden ser de red, o basados en host (HIPS).
  - Un HIPS es un host con software de monitoreo instalado.
    - Puede considerarse como la combinación de un antivirus, antimalware y un firewall.

	Ventajas	Desventajas
HIPS	• Provee protección específica a un sistema operativo de host. • Provee protección a aplicaciones y al sistema operativo • Protege al host después de desencriptar un mensaje (IPS no descifra).	• Dependiente del sistema operativo. • Debe instalarse en todos los hosts. • Difícil obtener un panorama completo de lo que ocurre en la red entera.

5.1 Tecnologías IPS

- Sensores Basados en IPS de Red.
  - Puede implementarse con dispositivos de red dedicados o no dedicados con hardening.
    - Router ISR + AIM | NME
    - ASA con o sim AIP-SSM
    - Catalyst 6500 + IDSM-2
    - IPS 4300



No requiere añadir mas sensores con la inclusión de nuevos hosts

  - Los sensores detectan actividad maliciosa en tiempo real y desencadenan acciones.
  - Deben tener al menos:
    - NIC: para interconexión de redes.
    - Procesador: para la ejecución de los procesos de análisis.
    - Memoria: para almacenar datos temporales del análisis (intensivo)

5.1 Tecnologías IPS

- Soluciones IPS de Cisco.
  - Router ISR (1900, 2900, y 3900 ISR G2s)
    - Requiere Cisco IOS IPS parte del Cisco IOS Security Technology Package.
    - No requiere módulos adicionales.
    - Requiere descarga de archivos de firmas y abundante memoria.
    - Limitado a ciertos patrones de tráfico (redes pequeñas).
  - Basadas en Módulos ISR:
    - Módulos de Integración Avanzada (AIM)
    - Modulo de Red Mejorado (NME)
    - Soporte para redes medianas.

  - Basadas en Módulos ASA (Para Cisco ASA 5500):
    - Módulos de Prevención e Inspección Avanzada (AIP)
    - Módulos de Servicios de Seguridad y Prevención (PSSM)
    - Soporte para redes medianas así como sucursal y corporativo.

5.1 Tecnologías IPS

- Soluciones IPS de Cisco Basadas en Aparatos.
  - **Cisco ASA 5500-X, ASA 5585-X + IPS Security Services Processor**:
    - No requiere Hardware Adicional para un desempeño IPS óptimo.
    - Soporte para pequeñas sucursales / oficinas.
  - **Sensores de las Series Cisco IPS 4300 y 4500**
    - Servicios IPS en línea. +
    - Tecnología Innovadora para detección, clasificación y detención de amenazas.

    - Detiene mas amenazas sin mermar el tráfico de red legítimo.
    - Enfocado a proteger dispositivos, servicios y aplicaciones de red.
  - **Cisco Catalyst 6500 + Módulo de Servicio IDS.**
    - Solución IPS que trabaja en conjunto con otras tecnologías.
    - Soporta ilimitado número de VLANs.
    - Utiliza el mismo software que otros Aparatos Sensores.

5.1 Tecnologías IPS

- Otras Soluciones IPS de Cisco.
  - **Cisco ASA 5500-X (Firewall de Próxima Generación).**
    - Incluye visibilidad y control de aplicaciones (AVC) y Esenciales de Seguridad Web (WSE) de Cisco, aparte del IPS tradicional.
    - Constituye un Firewall de inspección de estado completo.
    - Cuenta con controles de seguridad inteligentes de extremo a extremo y para operaciones de flujos seguros.
  - **Cisco ASA con Servicios FirePOWER (**ASA 5500-X y 5585-X**).**
    - Da servicios de próxima generación enfocados a amenazas adaptables.
    - Brinda defenza, antes, durante y después de un ataque.
    - Combina Firewall con protección contra malware.

5.1 Tecnologías IPS

- Elección de un IPS.
  - Factores a Considerar:
    - Cantidad de Tráfico de Red.
    - Topología de Red.
    - Presupuesto para Seguridad.
    - Personal disponible para administración de Seguridad.
  - Pequeñas implementaciones, pueden bastarse con un Router ISR con IOS habilitado para IPS.
  - Conforme se incremente el tráfico se pueden añadir módulos IPS NME o IPS AIM.
  - Instalaciones mas grandes pueden requerir aparatos ASA 5500-X.
  - Empresas y proovedores de servicios pueden requerir soluciones dedicadas o incluso Switches Catalyst 6500 con módulos IDSM-2.

5.1 Tecnologías IPS

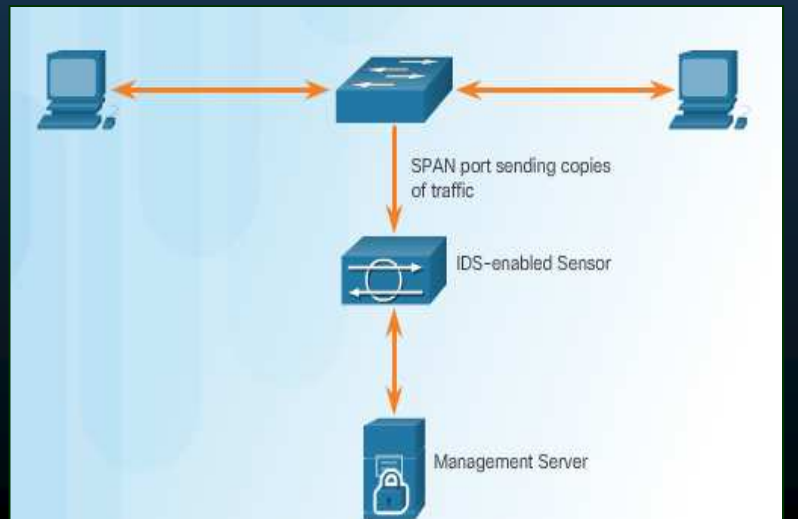
- Redes Basadas en IPS.

	Ventajas	Desventajas
Red IPS	• Puede identificar ataques en cualquier parte de la red. • Es costo efectiva. • No es visible a otros hosts de la red. • Independiente de los sistemas operativos de los hosts. • Muestra eventos de bajo nivel de red.	• No puede examinar el tráfico encriptado. • No puede determinar si un ataque se realizó con éxito. • Con el crecimiento de la red se torna difícil identificar el lugar idóneo para colocar un solo IPS.

5.1 Tecnologías IPS

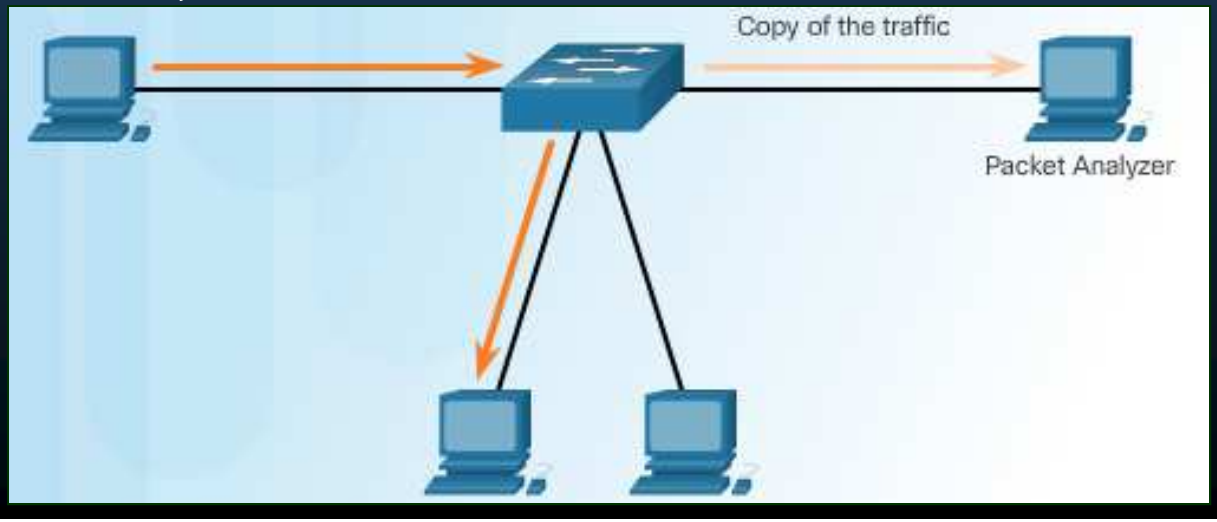
- Modos de Implementación de un IPS.
  - Modo en Línea (modo de par de interfaces en línea) :
    - Sensor intermedio, analiza los paquetes en la red.
    - Añade latencia.
    - Permite eliminar paquetes indeseados.
    - Capaz de analizar capas de la 3 a la 7.

  - Modo promiscuo (modo pasivo):
    - Los paquetes no fluyen a través del sensor.
    - El sensor analiza una copia del tráfico.
    - No afecta el flujo de paquetes.
    - Puede no evitar que paquetes maliciosos alcancen su destino.
    - Acciones post-eventos.
    - Usualmente requiere de otros dispositivos.



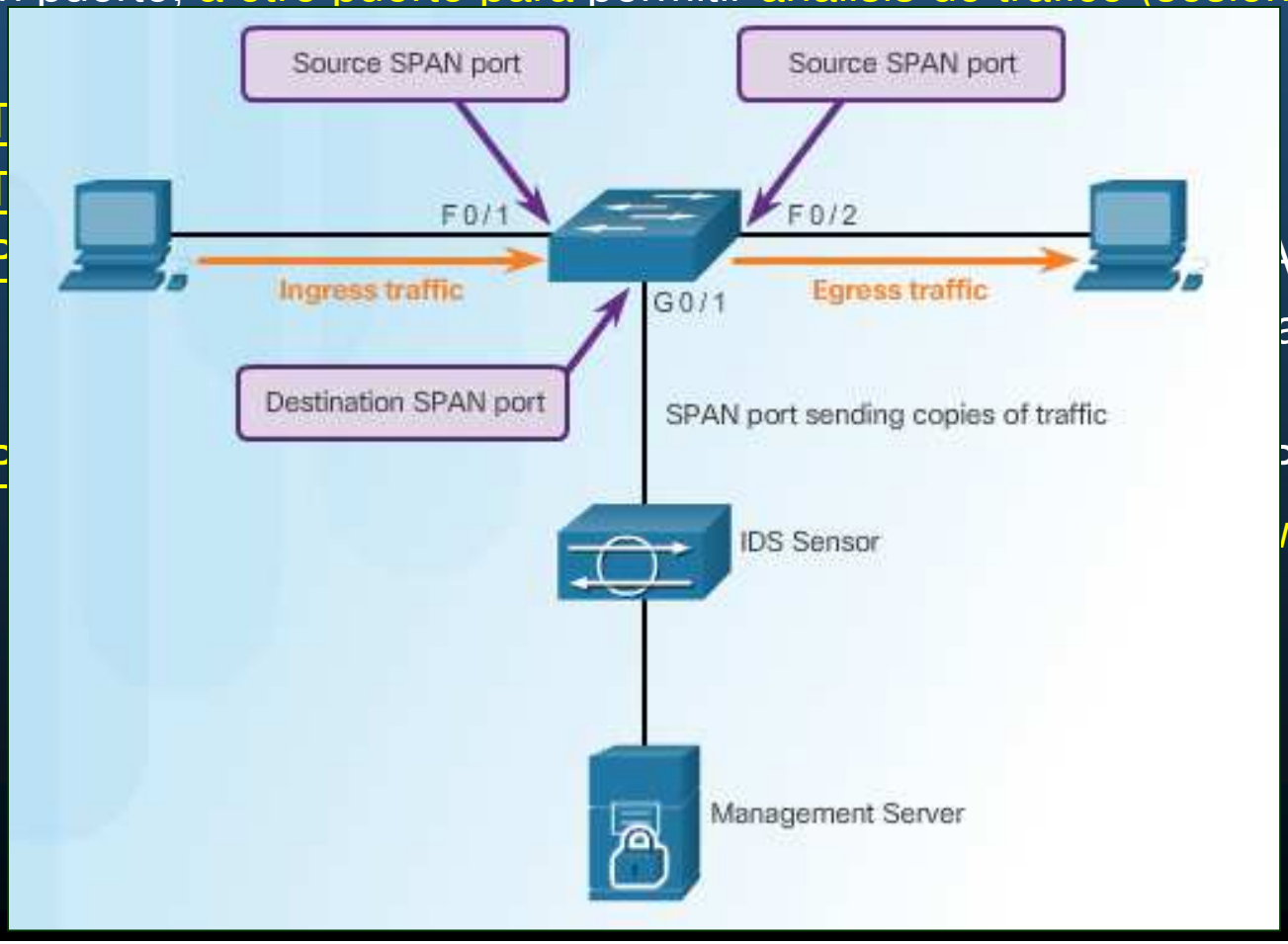
5.1 Tecnologías IPS

- Puertos Espejo.
  - Un analizador de paquetes (sniffer) puede ayudar a monitorear la red.
  - Un HUB facilitaba la implementación de un sniffer.
    - Cualquier host podía ser una sniffer → No deseable.
  - Redes switcheadas utilizan tablas MAC para redirigir tráfico solo a su destinatario.
  - Un puerto espejo, permite a un switch enviar por él una copia de cualquier tráfico entrante, además de a su destinatario.



5.1 Tecnologías IPS

- Analizador de Red con Puertos Switcheados (SPAN).
  - Característica de los switches Cisco para enviar copia de un frame que entra por un puerto, a otro puerto para permitir análisis de tráfico (sesión SPAN).
    - T
    - T
    - F
    - F



AN
a VLAN.
PAN).
witch.

5.1 Tecnologías IPS

- Configuración de SPAN para Detección de Intrusiones.
  - Establecer orígenes con:

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

    - *number* : identifica una sesión SPAN (relación de orígenes / destino)

  - Establecer destinos con:

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

    - *number* : identifica una sesión SPAN (relación de orígenes / destino)

```
S1# show monitor
Session 1
---------
Type                      : Local Session
Source Ports              :
    Both                  : Fa0/1
Destination Ports         : Fa0/2
    Encapsulation         : Native
          Ingress         : Disabled
```


```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```

5.2 Firmas IPS

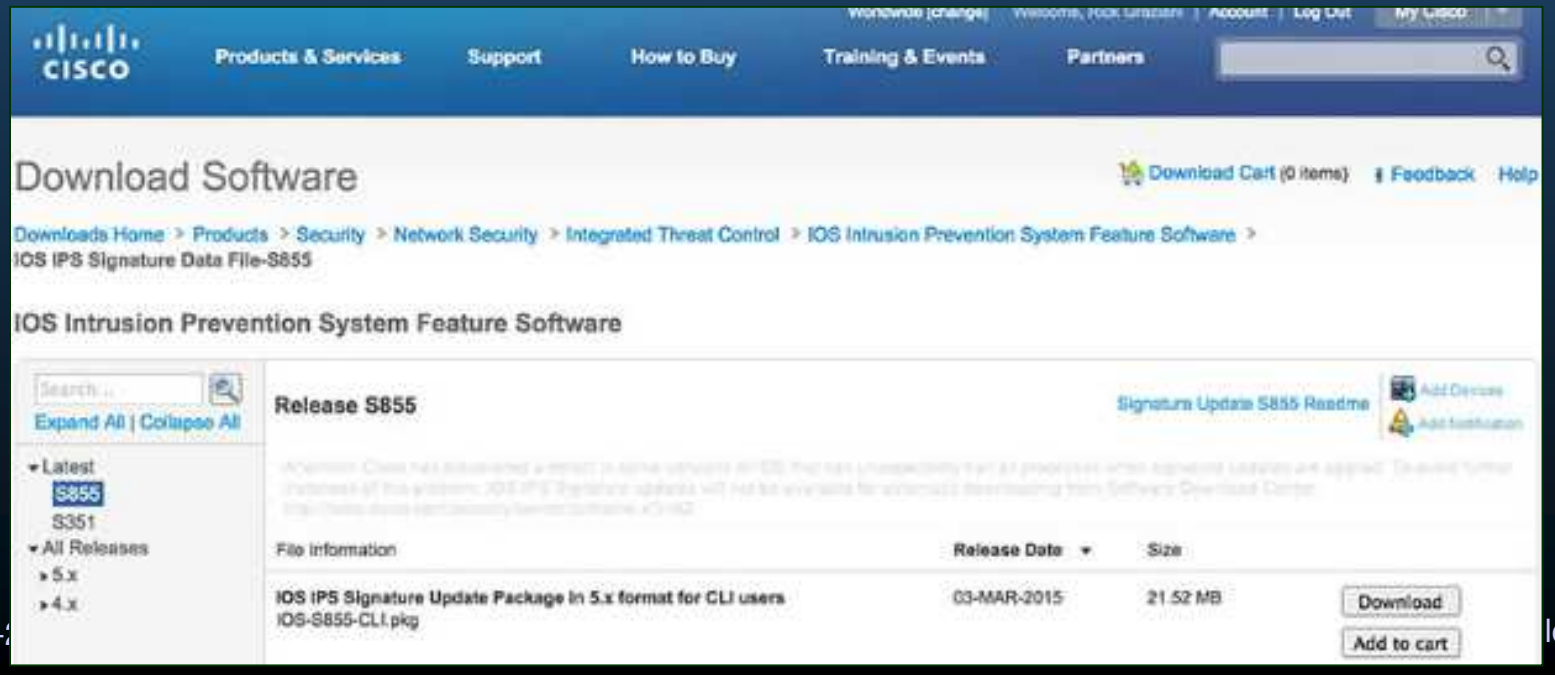
- Atributos de Firmas.
  - Identificar tráfico malicioso.
    - Diferentes características (firmas).
  - Firma: conjunto de reglas (IDS/IPS) para detectar intrusiones.
    - Identifican de manera univoca: gusanos, virus, anomalías en protocolos o tráfico malicioso.
  - Los sensores usan las firmas para buscar ataques y responder con acciones.
  - Atributos de las Firmas:
    - Tipo.
    - Disparador (alarma).
    - Acción.

5.2 Firmas IPS

- Tipos de Firmas.
  - Atómicas.
    - Consiste en un simple paquete, actividad o evento a verificar.
      - Si concuerda, se dispara una alarma y se realiza una acción.
    - No mantienen información de estado (actividades futuras o pasadas).
    - Consume mínimos recursos.
  - Compuestas (de estado completo).
    - Analiza múltiples paquetes de una sesión TCP.
    - Rastrea el estado de los paquetes relacionados a un ataque.
    - Identifica una secuencia de operaciones distribuidas (múltiples hosts), en un tiempo determinado (horizonte de eventos).
    - El horizonte de eventos varía de una firma a otra (consume recursos).

5.2 Firmas IPS

- Archivos de Firmas.
  - Contienen Firmas que se pueden distribuir y subir fácilmente a un IPS.
  - Fungen como actualizaciones para IPSs.
  - Recuperación periódica y automática de actualizaciones para IPS desde cisco.com, pueden configurarse en dispositivos ISR G2, tras instalar certificados VeriSign SSL en los dispositivos.



5.2 Firmas IPS

- Micro-Motores de Firmas (SME).
  - Brindan eficiencia al escaneo de firmas.
  - Categorizan firmas comunes en grupos.
  - El IOS puede buscar por grupos de características en lugar de una a una.

  - IDS/IPS → Carga SME
  - SME → Compila Expresiones Regulares de las Firmas
    - Para buscar patrones en series de bytes.
  - SME busca por protocolo.
  - Cada motor define un conjunto de parámetros permitidos por protocolo.
  - Las firmas se definen en base a los parámetros ofrecidos por los motores.
  - Cada SME extrae valores de un paquete y envía porciones a cada E.R.
    - Múltiples búsquedas a la vez.

  - Los SMEs disponibles varían dependiendo de la versión de IOS.

5.2 Firmas IPS

- Micro-Motores de Firmas (SME).
  - Atómicos: Examinan paquetes simples (UDP, ICMP, etc.)
  - De Servicio: Busca ataques a servicios (DNS, RPC, SMTP, HTTP, FTP,etc.)
  - De Cadena: Firmas basadas en expresiones regulares (TCP, UDP, ICMP)
  - De Multicadena: Soportan combinaciones de patrones flexibles.
  - Otros: Motor para varias y múltiples firmas.

  - Diferentes versiones para antes y después de IOS 12.4(11)T y 5.x
    - 5.x incluye algunas firmas cifradas y clasificaciones de riesgo.

  - Analizar expresiones regulares requiere memoria
    - Importante contar con la mayor cantidad posible de memoria.

5.2 Firmas IPS

- Adquirir Archivos de Firmas (SME).
  - Cisco investiga, crea y publica firmas para nuevas amenazas descubiertas.
    - Cada 2 semanas, las de mas baja importancia.
    - En unas horas, si se trata de una amenaza severa.
  - Las actualizaciones son acumulativas (incluyen las firmas previas).
  - Importante mantener actualizadas (requiere cuenta de cisco.com).

5.2 Firmas IPS

- Alarmas de Firmas.
  - El Disparador de una firma es cualquier cosa que señale de manera confiable a una intrusión.
  - Cuatro tipos (Cisco IPS 4300)

Decodificar protocolos: mecanismo alternativo para descomponer paquetes en campos y buscar anomalías o malformaciones por protocolo. Ayuda a reducir falsos positivos.

Tipo de Detección	Ventajas	Desventajas
Basada en Patrones	• Fácil configuración. • Pocos Falsos Positivos. • Buen diseño de firmas.	• No detecta firmas desconocidas. • Inicialmente muchos falsos positivos. • Necesario crear, actualizar y tunear firmas.
Basada en Anomalías	• Simple y confiable. • Políticas a la medida.	• Salida genérica. • Deben crearse las políticas.
Basada en Políticas	• Fácil configuración. • Puede detener ataques desconocidos	• Difícil perfilar actividad típica en redes grandes. • El tráfico debe ser constante por perfil.
Basada en Miel	• Ventana para visualizar ataques. • Distrae y confunde a los atacantes. • Ralentiza y advierte de un ataque. • Colecta información de un ataque.	• Requiere un servidor de miel dedicado. • El servidor de miel no debe ser confiable.

5.2 Firmas IPS

- Detección Basada en Patrones.
  - Busca patrones predefinidos y dispara alarma si encuentra coincidencias.

	Firma Atómica	Firma Compleja
Detección Basada en Patrones	No requiere estado para examinar patrones para determinar si realizar una acción.	Debe analizar múltiple información para determinar si la acción de la firma se realiza.
Ejemplo	Detectar solicitud ARP requiere detectar MAC origen FF:FF:FF:FF:FF:FF	Buscar la cadena `"confidencial"`, entre múltiples paquetes TCP.

  - Los patrones deben ser secuencias binarias o de texto.
  - Usualmente se limitan a paquetes destinados a un cierto servicio.
    - Difícil para protocolos sin puertos predefinidos.
  - Una configuración temprana provocará muchos falsos positivos.
    - Tras tunear presentará menos que otros enfoques.

5.2 Firmas IPS

- Detección Basada en Anomalías.
  - Consiste en crear un perfil de lo que se considera normal para una red o host.
    - Por monitoreo o basado en especificaciones.
  - Tras definir el perfil, la firma dispara una acción si se detecta tráfico excesivo o mas allá de cierto umbral.

	Firma Atómica	Firma Compleja
Detección Basada en Anomalías	No requiere estado para identificar actividad que se desvía del perfil.	Estado requerido para identificar actividad que se desvía del perfil.
Ejemplo	Detectar tráfico a un puerto destino, que no se encuentra en el perfil.	Verificar cumplimiento de protocolo para tráfico HTTP.

  - Reacciona ante ataques nuevos y conocidos.
  - Una alerta no necesariamente significa un ataque.
    - La definición de normalidad debe actualizarse con el tiempo.
  - Asegurarse de no estar bajo ataque al definir normalidad.
  - Los ataques se pueden disfrazar de tráfico normal.

5.2 Firmas IPS

- Detección Basada en Políticas y Tarros de Miel.
  - Detección Basada en Políticas:
    - Requiere, definir comportamientos sospechosos basado en análisis históricos.

	Firma Atómica	Firma Compleja
Detección Basada en Políticas	No requiere estado para identificar comportamiento indeseable.	Estado requerido para identificar comportamiento indeseado.
Ejemplo	Detectar paquetes anormalmente largos y fragmentados, examinando solamente el último fragmento.	Host Unix enviando solicitudes RPC a hosts remotos sin consultar previamente un PortMapper.

    - Una firma para cubrir toda una clase de actividades.
  - Detección Basada en Tarros de Miel.
    - Utiliza un servidor falso, para distraer la atención de ataques a dispositivos reales.
    - El tarro de miel, pude utilizarse para analizar ataques ante diferentes configuraciones y actualizar firmas en sus sensores.
    - Utilizado principalmente para investigación.

5.2 Firmas IPS

- Beneficios del uso de IPSs de Cisco.
  - Cisco IPS 4300 / Cisco Catalyst 6500 + Modulo IDS

  - Uso de infraestructura de enrutamiento como capa de seguridad.
  - En línea, y soportado por múltiples plataformas de enrutamiento.
  - Mitiga ataques tanto internos como externos.
  - Provee protección de amenazas en combinación con soluciones Cisco IDS, Firewall, VPN, y Control de Admisión de Red (NAC).
  - El tamaño de la base de datos de firmas, puede adecuarse a la cantidad de RAM disponible.

5.2 Firmas IPS

- Mecanismos Disparadores de Alarmas.
  - Los mecanismos disparadores pueden generar alarmas que sean falsos positivos o falsos negativos.
    - A tener en cuenta al implementar un IPS

Tipo de Alarma	Actividad de Red	Actividad IPS	Recomendación
Falso Positivo	Trafico normal de usuario	Alarma Generada	Tunear Alarma
Falso Negativo	Tráfico de Ataque	Alarma No Generada	Tunear Alarma
Verdadero Positivo	Tráfico de Ataque	Alarma Generada	Configuración Idónea
Verdadero Negativo	Trafico normal de usuario	Alarma No Generada	Configuración Idónea

5.2 Firmas IPS

- Acciones de Firmas.
  - Cuando una firma detecta la actividad para la que fue configurada, dispara una o mas acciones:

Categoría de Acciones	Alerta Específica
Generar una Alerta	Producir una alerta
	Producir una alerta verbosa
Registrar la Actividad	Registrara paquetes del atacante
	Registrar pares de paquetes
	Registrar ataques de la victima
Desechar o Prevenir la Actividad	Denegar al atacante en línea
	Denegar la conexión en línea
	Denegar paquete en línea
Reiniciar Conexión TCP	Reiniciar la conexión TCP
Bloquear Actividad Futura	Solicitar bloquear la conexión
	Solicitar bloquear al host
	Enviar una trampa SNMP

5.2 Firmas IPS

- Administrar Alertas Generadas.

* Los eventos se almacenan en una base de datos local llamada Tienda de Eventos

  - Monitorear las Alertas Generadas es vital para entender un ataque.

Alerta Específica	Descripción
Producir una alerta	Escribe el evento en la Tienda de Eventos* como una alerta
Producir una alerta verbosa	Esta acción incluye un volcado codificado del paquete que desató la alerta. Se escribe una alerta en la Tienda de Eventos* incluso si no se ha seleccionado una acción a producir por la alerta.

  - Analizar una avalancha de alertas falsas, puede abrumar a los analistas.
    - Dos tipos de alertas para facilitar la tarea:
      - Atómicas: Generadas cada vez que se dispara una firma.
        - Útil para indicar la ocurrencia de un ataque en particular.
        - Inundan la base de datos.
      - De Resumen: Una alerta con la cantidad de ocurrencias de una firma.
        - Sumariza eventos de una misma fuente en un periodo de tiempo.
        - Envía una Alerta cada que vence el tiempo definido.
        - Evita consumir recursos excesivamente.
    - Algunos IPS resumen automáticamente tras detectar recursos consumidos..

5.2 Firmas IPS

- Registro de Actividades para Análisis Posterior.
  - No contar con información para detener una actividad no impide registrarla.

Alerta Específica	Descripción
Registrar paquetes del atacante	Inicia registro de paquetes IP con la dirección del atacante y envía Alerta a la Tienda de Eventos, aunque no se haya seleccionado Producir Alerta.
Registrar pares de paquetes	Inicia registro de paquetes IP con el par de direcciones del atacante y la víctima; envía Alerta a la Tienda de Eventos, aunque no se haya seleccionado Producir Alerta.
Registrar ataques de la victima	Inicia registro de paquetes IP con la dirección de la víctima y envía Alerta a la Tienda de Eventos, aunque no se haya seleccionado Producir Alerta.

  - Permite analizar la información de la actividad realizada por el atacante tras dispararse la alarma.

5.2 Firmas IPS

- Actividad de Denegación.
  - Permite prevenir que ocurra una actividad.

Alerta Específica	Descripción
Denegar al atacante en línea	• Desecha el paquete actual y futuros de la dirección del atacante por un periodo de tiempo. • El sensor mantiene una lista de atacantes siendo denegados. • Las entradas pueden ser eliminadas manualmente o por timer. • Timer independiente por cada entrada, se reinicia ante nuevos ataques. • Si la lista llega a su límite por almacenamiento, sigue bloqueando lo contenido.
Denegar la conexión en línea	Desecha el paquete actual y futuros del flujo TCP.
Denegar paquete en línea	Desecha el paquete actual.

  - Actividades propias de un IPS (un IDS no deniega tráfico).
  - El motor de análisis determina los paquetes a ser reenviados y desechados.
  - Desechar permite salvar recursos al no tener que analizar esos paquetes.

5.2 Firmas IPS

- Actividad de Bloqueo y Admisión de Tráfico.

Alerta Específica	Descripción
Reiniciar la conexión TCP	Envía un TCP RST (reset) para secuestrar y terminar un flujo TCP. Se usa en combinación con acciones de denegación de paquete o conexión.
Solicitar bloquear la conexión	Envía una solicitud a un dispositivo para que bloquee la conexión. Vgr; Indicar a un router actualizar sus ACLs.
Solicitar bloquear al host	Envía una solicitud a un dispositivo para que bloquee al host atacante. Vgr; Indicar a un router actualizar sus ACLs.
Enviar una trampa SNMP	Envía una solicitud al componente de notificación de aplicaciones del sensor, para realizar una notificación SNMP. Escribe una alerta en la Tienda de Eventos, aunque no se haya seleccionado Producir Alerta.

- Actividad de Admitir.
  - Permite definir excepciones a las firmas configuradas.
  - Facilita administración, primero denegar todo, luego definir excepciones.
  - Algunos IPS las denominan filtros de firmas.

5.2 Firmas IPS

- Monitoreo de Actividad de IPSs.
  - Crucial para proteger contra ataques.
  - Factores a considerar para implementar estrategias de monitoreo:
    - Método de Administración.
    - Correlación de Eventos.
    - Personal de Seguridad.
    - Plan de Respuesta a Incidentes.

5.2 Firmas IPS

- Consideraciones de Monitoreo.
  - Método de Administración.
    - Individual : Por sensor.
      - Fácil y rápida con pocos sensores.
    - Centralizada: Para implementaciones con muchos sensores.
      - Reduce tiempo y personal requerido.
      - Concentra mayor visibilidad de eventos.
  - Correlación de Eventos que suceden al mismo tiempo en distintos puntos.
    - Sincronizar hora en dispositivos mediante NTP.
    - Permite evaluar cuando sucedió un evento con respecto de otro.
      - Independientemente del dispositivo donde hayan sucedido.
    - Monitorear de forma centralizada.

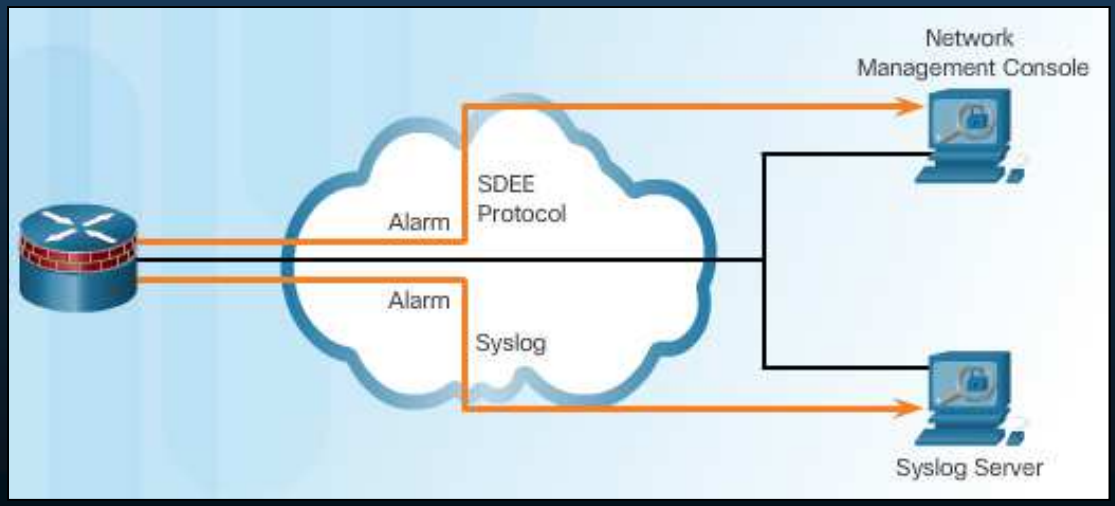
5.2 Firmas IPS

- Consideraciones de Monitoreo (continuación).
  - Personal de Seguridad.
    - A mas sensores, mayor personal puede ser necesario para monitorear, evaluar, afinar y optimizar su desempeño.
  - Plan de Respuesta a Incidentes.
    - ¿Que hacer si algún sistema se ve comprometido?.
      - Restaurarlo a su estado previo al ataque.
      - Identificar pérdidas (propiedad intelectual, datos sensibles, etc)
      - Identificar posibles daños secundarios (a otros sistemas).
  - Nota: Aunque puede usarse la CLI para configurar un IPS, es preferible un Administrador con GUI. Cisco ofrece:
    - Cisco Configuration Professional
    - Cisco IPS Manager Express (IME)
    - Cisco Security Manager

5.2 Firmas IPS

- Intercambio de Eventos en Dispositivos Seguros.
  - Cuando una firma es disparada, se generan alarmas que pueden ser almacenadas y consultadas localmente en el sensor o mediante una aplicación de administración.
  - Cuando se detecta un ataque, el IPS puede enviar mensajes syslog o alarmas en el formato de Intercambio de Eventos en Dispositivos Seguros (SDEE - Secure Device Event Exchange).

Protocolo SDEE: desarrollado para comunicar eventos IDS y ser Extensible a otros eventos.



5.2 Firmas IPS

- Mejores Prácticas para Configuración de IPS.
  - Balancear la necesidad de actualizar sensores a las últimas firmas contra el tiempo requerido (vulnerable).
  - Actualizar paquetes de firmas en automático para grandes implementaciones.
  - Descargue los nuevos paquetes de firmas a un servidor seguro (protegido por otro IPS) de la red de administración.
  - Coloque paquetes de firmas en un SFTP (red de administración).
  - Configure el SFTP como solo-lectura para el directorio de firmas.
  - Configure sensores para buscar regularmente nuevas firmas en el SFTP.
  - Mantenga los niveles de sensor soportados por la consola de administración, sincronizados con los paquetes de firmas en los sensores.

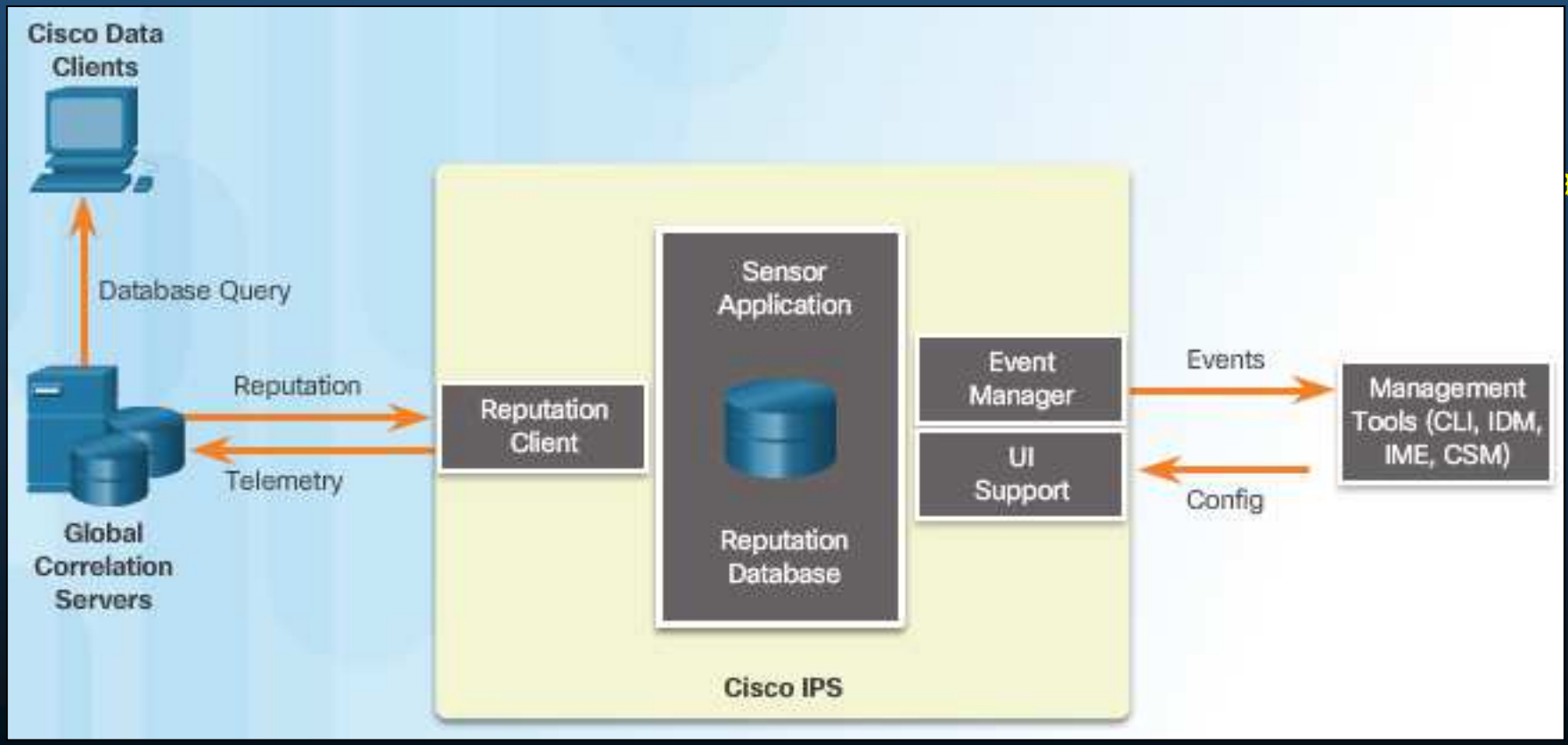
  - Nota: La descarga automática de definiciones de firmas puede configurarse en routers ISR G2 y es una alternativa al SFTP.

5.2 Firmas IPS

- Correlación Global de Cisco.
  - Servicio mediante el cual, los IPSs Cisco reciben actualizaciones de amenazas de la llamada Red de Base de Sensores Cisco.
  - Objetivos:
    - Lidiar inteligentemente con alertas para mejorar efectividad.
    - Mejorar protección contra sitios maliciosos conocidos.
    - Compartir datos de telemetría para mejorar visibilidad de alertas y acciones de sensores a una escala global.
    - Simplificar la configuración de ajustes.
    - Manejo automático de carga/descarga de información de seguridad.
  - Brinda actualizaciones globales sobre dispositivos con actividad de reputación maliciosa.
  - Disponible para Cisco IPS 4300 y 4500 / Cisco ASA 5500 / Módulos ISR G2

5.2 Firmas IPS

- Red de Base de Sensores Cisco.
  - Dos servicios a habilitar/deshabilitar en un IPS:



5.2 Firmas IPS

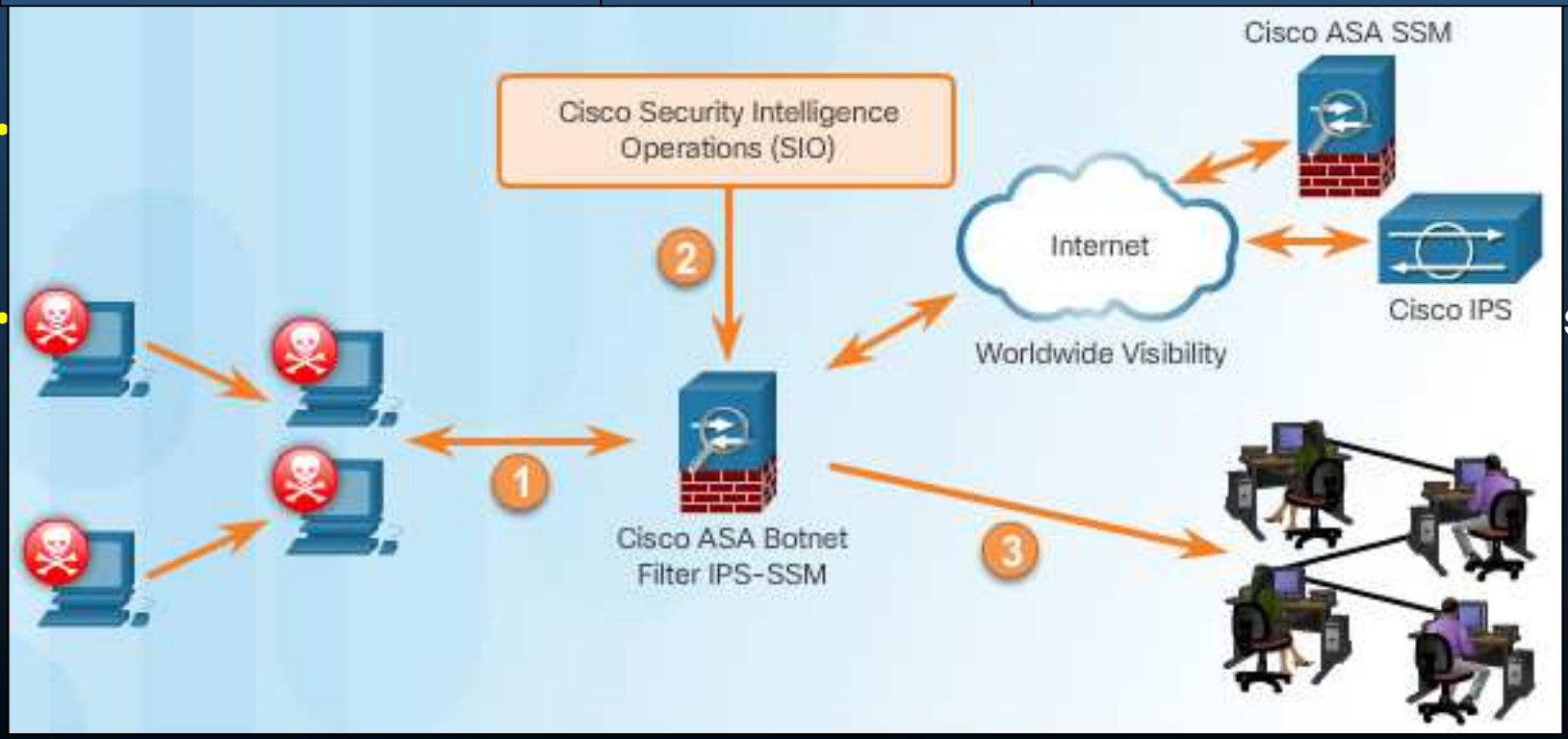
- Operación de la Inteligencia de Seguridad de Cisco.
  - La Red de Base de Sensores Cisco, colecta información bajo el siguiente

  - Brinda Información para detectar, prevenir y reaccionar a amenazas.

5.2 Firmas IPS

- Reputaciones, Listas Negras y Filtros de Tráfico.

1. Clientes infectados buscan comunicarse con un host de comando y control en Internet.	2.ASA actualiza su lista de filtros desde Cisco SIO.	3. ASA envía alertas al equipo de seguridad para prevenir, mitigar y remediar.



5.2 Firmas IPS

- Reputaciones, Listas Negras y Filtros de Tráfico (Cont.).
  - Es posible complementar la base de datos dinámica, añadiendo direcciones a una lista negra y/o lista blanca estáticas.
  - Coincidencias, generarán mensajes syslog.
  - Las compañías deben considerar el impacto de sus prácticas de seguridad.
    - Podrían ganarse una mala reputación.
    - Ser bloqueadas sus IPs.
    - Bloquear re-envíos de correo electrónico.
  - Es muy difícil que una compañía que aparece en listas negras, vuelva a ser considerada confiable.

5.3 Implementaciones IPS

- Implementar IPS en IOS.
  - IOS IPS permite administrar prevención de intrusos en routers Cisco.
  - Requerirá Firmas IOS IPS en formatos 5.x / 12.4(10) / 4.x
  - Pasos:
    - Descargar los archivos de IOS IPS.
    - Crear un directorio de configuraciones en Flash.
    - Crear una llave de criptografía.
    - Habilitar el IOS IPS.
    - Cargar los paquetes de firmas al router.

Requiere IOS con licencia de Paquete de Tecnologías: `securityk9`
verifique su disponibilidad con: `show version`
Para habilitar en Packet Tracer: routers 19xx y 29xx

```
R1# erase startup-config
R1# conf t
R1(config)# license boot module <c1900 | c2900> technology-package securityk9
...
ACCEPT? [yes/no]: yes
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

Los routers 29xx, requieren que esta sea la primera configuración que se realice.

5.3 Implementaciones IPS

- Descargar Archivos IPS en IOS.
  - IOS 12.4(10)T y previos contienen firmas incluidas, así como la capacidad de importar nuevas.
    - Seleccionar firmas involucra cargar un archivo XML (Signature Definition File - SDF) al router.
      - Contiene descripción de firmas en formato IPS 4.x
  - IOS 12.4(15)T4 y posteriores no incluyen firmas incluidas deben importarse.
    - Utilizan firmas en versión 5.x
    - Pueden descargarse de cisco.com (requiere cuenta de usuario).
  - Paso 1: Descargar Archivos IPS (paquetes de firmas y llave pública)
    - `IOS-Sxxx-CLI.pkg` – Paquete de Firmas.
    - `realm-cisco.pub.key.txt`

En Packet Tracer, los routers cuentan con archivos de firmas importados (xmls en la flash). No es necesario importar archivos.

5.3 Implementaciones IPS

- Descargar Archivos IPS en IOS (Cont.).
  - Paso 2: Crear directorio de configuración en Flash.
    - Comandos para manejo de directorios:

```
Router# mkdir directory-name
Router# rename current-name new-name
Router# dir [/all] [filesystem: ][file-url]
```

```
R1# mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash0:/IPSDIR
R1# dir flash:
Directory of flash0:/

   14  -rw-        1381  Feb 18 2015 20:37:14 +00:00  R2backup.cfg
   15  drw-           0  Feb 28 2015 01:14:12 +00:00  IPSDIR

256487424 bytes total (175632384 bytes free)
R1#
```

    - Cualquier ubicación es válida mientras tenga permisos de escritura.
      - Una memoria USB es válida si el router la soporta.

5.3 Implementaciones IPS

- Llaves para criptografía IPS.
  - Paso 3: Configurar llave para criptografía IPS.
    - Abrir el archivo `realm-cisco.pub.key.txt` obtenido en el Paso 1.

```
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
 exit
 exit
```

    - Verifica el archivo de firmas maestro (`sigdef-default.xml`) firmado con una llave privada de Cisco.
    - Copiar y pegar contenido en confi
      - Si fuese inválida:
        - **`%IPS-3-INVALID_DIGI`**
          `Signature found (key not found)`
      - Remover con: **`no crypto key pubkey-chain rsa.`**

En Packet Tracer, los routers cuentan con archivos de firmas importados. No es necesario importar archivos ni configurar `crypto key pubkey-chain rsa`

5.3 Implementaciones IPS

- Paso 4: Habilitar IOS IPS.
  - a. Identificar el nombre de reglas IPS y especificar su ubicación.
    - Crear un nombre de reglas.

```
Router(config)# ip ips name [rule-name]
```

    - Crear ACL para filtrar el tráfico escaneado (Opcional).
      - Todo tráfico admitido será escaneado.
    - Configurar ubiación de firmas.

```
Router(config)# ip ips config location flash:<directory-name>
```

```
R1(config)# ip ips name IOSIPS
R1(config)# ip ips name IOSIPS list ?
  <1-199>  Numbered access list
  WORD     Named access list

R1(config)#
R1(config)# ip ips config location flash:IPS
R1(config)#
```

En Packet Tracer, los comandos subrallados en rojo no están implementados.

  - b. Habilitar SDEE y registrar notificaciones de eventos.
    - Habilitar HTTP o HTTPS para que SDEE vea solicitudes.
      - #R(config) ip http[s] server
    - Habilitar notificaciones de eventos SDEE
      - #R(config) ip ips notify [sdee | log]

```
R1(config)# ip http server
R1(config)# ip ips notify ?
  SDEE  Send events to SDEE
  log   Send events as syslog messages

R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#
```

[sdee | log] Formato de notificación, syslog por default. Requiere configurar adicionalmente un servidor SysLog.

5.3 Implementaciones IPS

- Paso 4: Habilitar IOS IPS.
  - c. Configurar la categoría de firmas.
    - Todas las firmas se clasifican en categorías jerárquicas.
      - Las 3 más conocidas son: `all`, `basic`, y `advanced`.
    - Las firmas con las que se escanea tráfico pueden ser: `retired` o `unretired`
      - Retirar una firma (o no), de la compilación (de utilizarla para escanear tráfico).
    - Al iniciar una configuración, todas las firmas deberían retirarse (No saturar RAM).
    - Posteriormente, habilitar (des-retirar) las firmas deseadas (Compilar consume RAM).

En Packet Tracer, solo se admite categoría `basic`.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips ?
  advanced  Advanced
  basic     Basic
  <cr>
```

```
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# end
Do you want to accept these changes? [confirm]
R1#
*Dec 9 04:29:39.119: Applying Category configuration to
signatures ...
R1#
```

  - d. Aplicar la regla IPS a la interface deseada y especificar dirección.

```
Router(config)# ip ips ips-name ( in | out )
```

    - Vgr; Aplicar Regla IOSIPS a G0/0 para el tráfico de entrada:

```
R1(config)# interface g0/0
R1(config-if)# ip ips IOSIPS in
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ip ips IOSIPS in
R1(config-if)# ip ips IOSIPS out
R1(config-if)# end
```

5.3 Implementaciones IPS

- Paso 5: Cargar Paquetes de Firmas IOS IPS al Router.
  - Mediante FTP / TFTP.
  - FTP

`idconf`
Especifica que el destino es una configuración.

```
Router# copy ftp://ftp_user: password @ Server_IP_address/signature_package idconf
```

  - Vgr;

```
R1# copy tftp://192.168.1
Loading IOS-S416-CLI.pkg
!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9553609 bytes]

Feb 27 18:17:42.507: %IPS
Feb 27 18:17:42.515: %IPS
Feb 27 18:17:45.975: %IPS
engine will be scanned
<output omitted>
Feb 27 18:17:51.483: %I
engines
Feb 27 18:17:51.519: %IP
this engine will be scann
Feb 27 18:17:51.519: %IPS
R1#
```

Verificación.

```
R1# show ip ips signature count

Cisco SDF release version S416.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 342
      atomic-ip enabled signatures: 90
      atomic-ip retired signatures: 321
      atomic-ip compiled signatures: 21
      atomic-ip obsoleted signatures: 3

<output omitted>

Total Signatures: 3027
   Total Enabled Signatures: 1048
   Total Retired Signatures: 2726
   Total Compiled Signatures: 301
   Total Obsoleted Signatures: 9

R1#
```

5.3 Implementaciones IPS

- Retirar y Des-Retirar Firmas.
  - Ejemplos de Retirar la firma individual 6130 con sub-firma 10 Y Des-retirar categoría IOSIPS Basic.

```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

  - Des-retirar pueden no ser compiladas por insuficiencia de memoria, parámetros inválidos o si la firma está obsoleta.
  - Un grupo de firmas implica, todas las firmas en esa categoría.

5.3 Implementaciones IPS

- Cambiar Acciones de Firmas.

En Packet Tracer, las aciones subralladas en rojo no están implementadas.

- `Router(config-sigdef-sig)# event-action action`

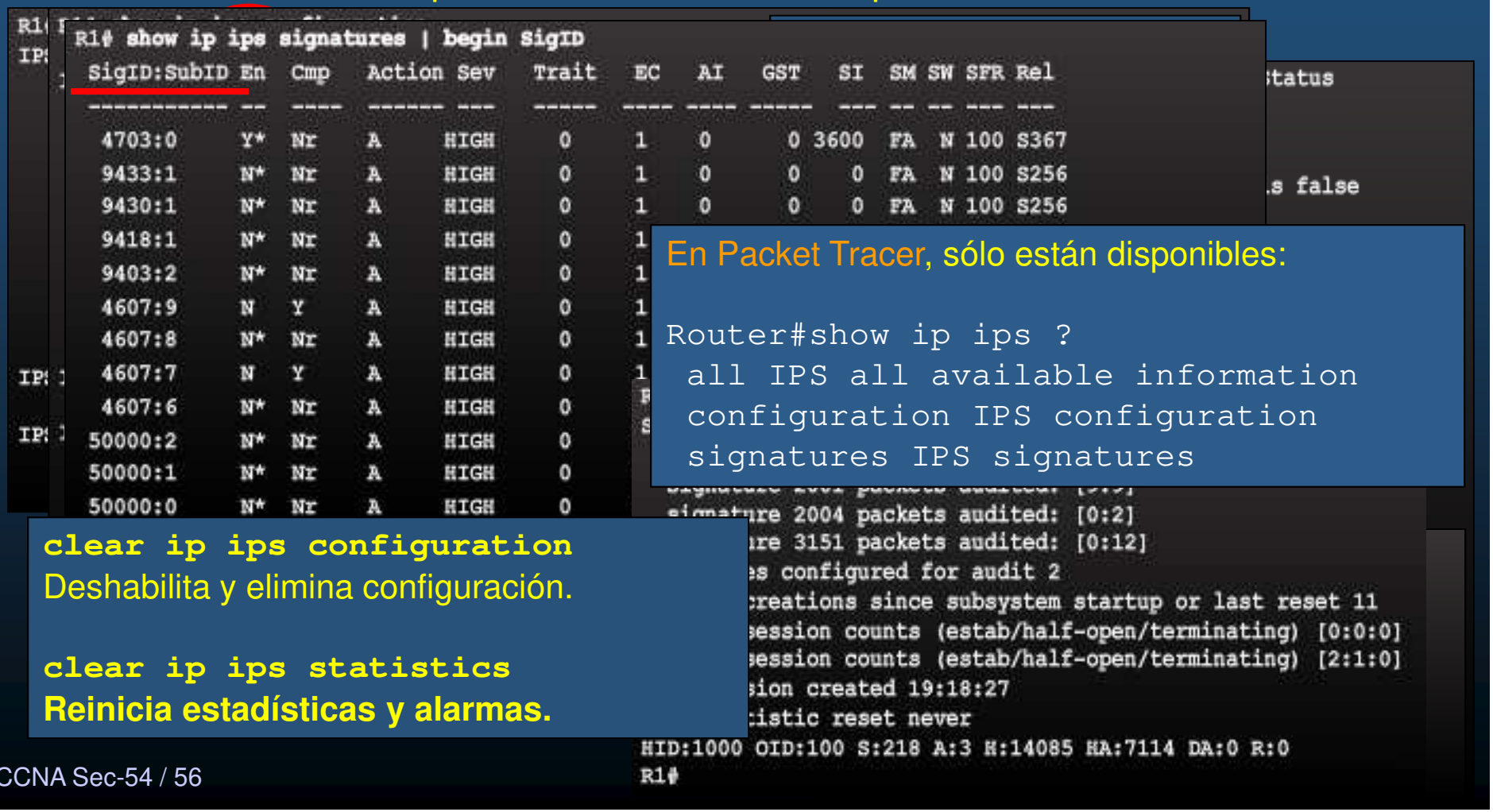
Action	Descripción
deny-attacker-inline	Extermina paquetes de la dirección del atacante por un periodo de tiempo.
deny-connection-inline	Extermina paquetes del flujo tcp.
deny-packet-inline	Extermina el paquete.
produce-alert	Escribe el evento en la Tienda de Eventos como una alerta.
reset-tcp-connection	Envía un TCP Reset, para secuestrar y terminar el flujo TCP.

- Ejemplos:

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# event-action produce-alert
R1(config-ips-category-action)# event-action deny-packet-inline
R1(config-ips-category-action)# event-action reset-tcp-connection
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit

Do you want to accept these changes? [confirm] y
R1(config)#
```

5.3 Implementaciones IPS

- Verificación de IOS IPS.
  - Comandos `show` para verificar la correcta operación de IOS IPS.



5.3 Implementaciones IPS

- Reportar Alertas IPS.
  - Para especificar el método de notificar eventos:
    - **`R(Config)# ip ips notify < log | sdee >`**
  - **Ejemplo syslog:**

```
R1# config t
R1(config)# logging 192.168.10.100
R1(config)# ip ips notify log
R1(config)# logging on
R1(config)#
```

Packet Tracer, sólo soporta SysLog

5.3 Implementaciones IPS

- Habilitar SDEE.

No disponible en Packet Tracer.

  - SDEE se prefiere sobre syslog para reportar eventos.
    - `R(config)# ip ips notify sdee`
  - Requiere habilitar HTTP(s)
    - Ejemplo:

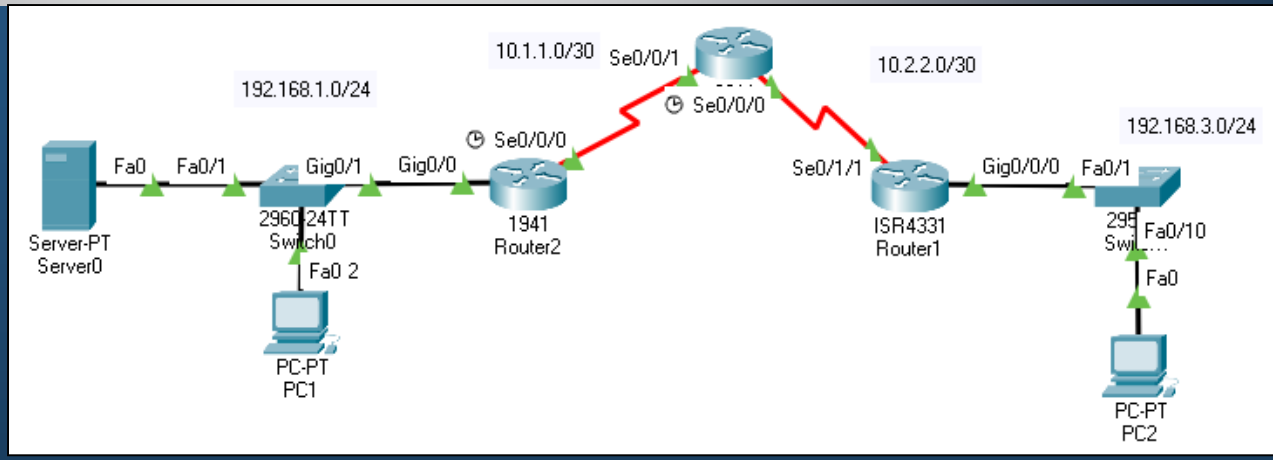
```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip ips notify sdee
R1(config)# ip sdee events 500
R1(config)#
```

  - Todos los eventos se pierden al deshabilitar SDEE.
  - SDEE utiliza un mecanismo de extracción.
    - La Aplicación de Administración solicita y el IOS IPS responde.
    - Provisionalmente almacena hasta 200 eventos en buffer.
      - Para cambiar tamaño del buffer: `Router(config)# ip sdee events events`
      - Al cambiar a un tamaño menor se pierde el contenido de los buffers.
    - Para limpiar los eventos o suscripciones: `Router# clear ip ips sdee {events| subscription}`

- `R(config) ip audit notify` se interpreta como: `R(config) ip ips notify`

Integración

- Actividad Práctica.
  - Monte la topología mostrada:
  - Habilite el paquete de tecnologías de seguridad en Router2.
  - Configure la topología.



  - Verifique conectividad de PC2 a PC1 mediante un ping.
  - Cree un directorio de configuración IOS IPS en la flash llamado `ipsdir`.
  - Configure la localización de la configuración de IPS.
  - Cree una regla IPS llamada `IOSIPS`.
  - Habilite SysLog en `Server 0` y habilite IOSIPS para que le envíe notificaciones.
  - Configure IOSIPS para que utilice las categorías `basic`.
  - Aplique la regla IPS a G0/0/0 de salida.
  - Des-retire el echo request (firma 2004 ID 0), y habilite la firma, para producir una alerta y denegar el tráfico en línea.
  - Verifique la configuración
    - El ping de PC2 a PC1 debería fallar ahora y registrar eventos en el servidor SysLog.