Guía Académica
Fundamentos de Ciberseguridad

Elaborado por:

Santiago Aguilar Cárdenas

Facultad de Ingeniería Electrónica

Universidad Santo Tomás

Seccional Tunja

GA-2

Información Académica

Guía Académica

Fundamentos de Ciberseguridad

Elaborado por:

Santiago Aguilar Cárdenas

Director del Trabajo de Grado:
Ph.D. William Fabián Chaparro Becerra

Codirectores del Trabajo de Grado:
M.Sc. Angélica María Salazar Madrigal
M.Sc. Cristian David Parra Camacho

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

Información del Documento

Asignatura:	Transmisión de Datos
Nivel:	Pregrado – Ingeniería Electrónica
Duración estimada:	Estudio autónomo
Modalidad:	Estudio teórico previo a prácticas de laboratorio

PREÁMBULO

Resumen

Esta guía académica reúne los fundamentos esenciales de ciberseguridad que el estudiante requiere para comprender e implementar estrategias de protección en infraestructuras de red. Se desarrollan conceptos sobre los principios de seguridad de la información (tríada CIA), tipología de amenazas y vulnerabilidades, mecanismos de control de acceso mediante ACLs, tecnologías de encriptación con VPN IPsec, y arquitecturas de defensa implementadas en dispositivos Cisco ASA, articulándolos con escenarios reales de protección de redes corporativas.

Presentación

El presente documento ha sido diseñado para proporcionar los fundamentos teóricos de ciberseguridad necesarios para comprender e implementar configuraciones de seguridad en dispositivos Cisco, y posteriormente, aplicar estos controles en escenarios reales y simulados de infraestructuras de red.

Con el fin de favorecer una progresión **de lo conceptual a lo aplicado**, esta guía académica desagrega el Syllabus en **seis unidades** específicas: comienza con los principios fundamentales (tríada CIA), continúa con la identificación de amenazas, avanza hacia mecanismos técnicos de control (ACLs), implementación de confidencialidad mediante VPN, administración de perímetros con Firewalls, y finaliza con estrategias integradas de defensa en profundidad. Esta decisión facilita que cada tema se construya sobre el anterior y que el estudiante cuente con prerrequisitos claros para las prácticas de laboratorio y ejercicios evaluativos.

Estructura de la Guía (alineación con el Syllabus)

La presente guía se organiza en cuatro unidades temáticas que desarrollan de manera progresiva competencias en ciberseguridad aplicada a redes. Cada unidad integra contenidos conceptuales con referencias a casos de aplicación práctica en dispositivos Cisco, lo que facilita la transición de la teoría a entornos reales.

Unidades de la guía:

Unidad 1: **Principios de Seguridad de la Información** – Tríada CIA y fundamentos de protección de información en redes.

Unidad 2: **Access Control Lists (ACLs)** – Control de tráfico en routers mediante reglas de filtrado y políticas de acceso.

Unidad 3: **VPN IPsec** – Cifrado de comunicaciones para asegurar confidencialidad e integridad en redes públicas.

Unidad 4: **Firewalls Cisco ASA** – Protección del perímetro de red y control de accesos no autorizados.

Competencias

Competencias:

- Explicar los principios fundamentales de seguridad de la información y su aplicación en infraestructuras de comunicaciones.
- Identificar y clasificar amenazas y vulnerabilidades específicas en ambientes de red, evaluando su impacto potencial en los objetivos de confidencialidad, integridad y disponibilidad.

Objetivos

Objetivos de aprendizaje de la guía:

1. **Comprender** los fundamentos de seguridad de la información (tríada CIA, amenazas y vulnerabilidades) como base para el análisis técnico en redes.
2. **Comprender** mecanismos de control de acceso mediante ACLs para filtrar tráfico y hacer cumplir políticas de seguridad en dispositivos de red.
3. **Conocer** VPN IPsec para proteger la confidencialidad e integridad de las comunicaciones sobre redes públicas.

Resultados de Aprendizaje

Resultados de aprendizaje esperados:

- Describe la tríada CIA y su importancia en el diseño de arquitecturas de seguridad.
- Clasifica tipos de amenazas (malware, phishing, ataques DDoS, etc.) y sus mecanismos de operación.
- Explica el funcionamiento de ACLs estándar y extendidas como mecanismo de control de tráfico.
- Fundamenta los algoritmos criptográficos utilizados en VPN IPsec y su rol en la protección de comunicaciones.
- Describe las funciones de los firewalls en la defensa del perímetro y la inspección de tráfico.

Índice

1 Principios de Seguridad de la Información: Tríada CIA

Competencias

- Explicar los tres pilares fundamentales de la seguridad de la información y su interdependencia.
- Analizar cómo cada principio de la tríada CIA se aplica en contextos de infraestructuras de red.
- Relacionar controles técnicos específicos con cada componente de la tríada CIA en dispositivos Cisco.

Objetivos

- Definir y explicar los conceptos de confidencialidad, integridad y disponibilidad en el contexto de seguridad de la información.
- Identificar cómo los principios de la tríada CIA se aplican en escenarios reales de protección de datos empresariales.
- Reconocer la importancia del balance entre los tres principios y sus posibles conflictos en la práctica.
- Asociar mecanismos de control (encriptación, firmas digitales, redundancia) con cada elemento de la tríada.

Resultados de Aprendizaje

- Explica, con ejemplos concretos, cómo cada principio de la tríada CIA protege los activos de información de una organización.
- Analiza escenarios de incidentes de seguridad identificando qué principio(s) fue(ron) comprometido(s).
- Propone controles técnicos y organizacionales para garantizar cada uno de los tres principios.

1.1 Concepto de Seguridad de la Información

La seguridad de la información es la disciplina que busca proteger los activos informáticos de una organización contra amenazas internas y externas. En el contexto de redes de datos, los activos incluyen no solo la información transmitida, sino también los dispositivos de infraestructura (routers, switches, firewalls) y los servicios que dependen de ellos. Un enfoque efectivo de seguridad requiere un entendimiento profundo de cuáles son los objetivos que se pretende lograr: la protección simultánea de la **confidencialidad**, la **integridad** y la **disponibilidad**, conocidos colectivamente como la **tríada CIA**.

Tríada CIA

Modelo fundamental que define los tres objetivos principales de cualquier sistema de seguridad de la información: Confidencialidad, Integridad y Disponibilidad. Estos tres principios son interdependientes y deben trabajar en conjunto para crear un entorno seguro y confiable.

1.2 Confidencialidad

La **confidencialidad** se refiere a la protección de la información contra el acceso no autorizado. Solo las personas o entidades con permisos específicos deben acceder a datos sensibles. Una violación de confidencialidad ocurre cuando alguien sin autorización logra leer, ver o escuchar información protegida.

Aspecto	Descripción
Objetivo	Asegurar que solo usuarios autorizados accedan a datos sensibles.
Mecanismos Técnicos	Cifrado (encriptación), control de acceso, autenticación, VPN, firewalls.
Ejemplos de Violación	Acceso no autorizado a emails, robo de datos personales, escucha de conversaciones.
En Redes Cisco	ACLs, VPN IPsec, cifrado de contraseñas, protocolos seguros (SSH en lugar de Telnet).

Cuadro 1: Dimensión de Confidencialidad en la Seguridad

Ejemplo

Un atacante utiliza *packet sniffing* (análisis de paquetes) para capturar datos en la red sin encriptación. Si la comunicación hubiera estado protegida con VPN IPsec, el atacante solo habría visto datos cifrados, ilegibles. En este caso, VPN protege la confidencialidad de la comunicación.

1.3 Integridad

La **integridad** se refiere a la garantía de que la información no ha sido modificada, alterada o corrompida de manera no autorizada, ya sea en tránsito o en almacenamiento. Una violación de integridad significa que los datos han sido cambiad sin autorización, pero no necesariamente que alguien no autorizado pudo leerlos.

Aspecto	Descripción
Objetivo	Asegurar que los datos no sean alterados sin autorización.
Mecanismos Técnicos	Funciones hash, firmas digitales, checksums, certificados digitales.
Ejemplos de Violación	Modificación de transacciones, alteración de configuraciones, cambio de registros.
En Redes Cisco	IPsec (protocolo de integridad), checksums en paquetes, firmas en configuraciones.

Cuadro 2: Dimensión de Integridad en la Seguridad

Ejemplo

Un atacante accede a una transacción bancaria en tránsito. Aunque no pueda ver los datos (confidencialidad está protegida por cifrado), podría intentar modificar el monto transferido. Los protocolos de integridad como HMAC (Hash-based Message Authentication Code) detectan estos cambios no autorizados, impidiendo que la transacción falsa se procese.

1.4 Disponibilidad

La **disponibilidad** se refiere a la garantía de que los servicios, datos y recursos de red estén accesibles cuando se requieran por usuarios autorizados. Una violación de disponibilidad ocurre cuando los servicios o datos no están accesibles, ya sea por ataque (como un DDoS) o por falla técnica (como una caída de servidor).

Aspecto	Descripción
Objetivo	Asegurar que servicios y datos estén disponibles cuando se necesiten.
Mecanismos Técnicos	Redundancia, balanceo de carga, respaldo, topologías tolerantes a fallos.
Ejemplos de Violación	Ataques DDoS, fallos de equipos, caída de links, pérdida de datos.
En Redes Cisco	Redundancia de routers, switches stacking, link redundancy, QoS.

Cuadro 3: Dimensión de Disponibilidad en la Seguridad

Ejemplo

Un ataque DDoS (Distributed Denial of Service) sobrecarga un servidor web empresarial con millones de solicitudes, impidiendo que clientes legítimos accedan al sitio. Aunque los datos están seguros (confidencialidad) y no han sido modificados (integridad), la disponibilidad ha sido comprometida. Implementar protecciones contra DDoS (filtrado, limitación de tasa) es esencial para mantener disponibilidad.

1.5 Interrelación de la Tríada CIA

Los tres elementos de la tríada CIA no son independientes. A menudo, implementar un control que fortalece un aspecto puede afectar a otros. Por ejemplo, implementar encriptación muy fuerte (mejora de confidencialidad) puede afectar el rendimiento (disponibilidad). Un firewall muy restrictivo (mejora de confidencialidad e integridad) podría negar acceso a usuarios legítimos (afecta disponibilidad).

Relación	Descripción
C-I Compatibles	El cifrado protege confidencialidad; los hash protegen integridad. Ambos pueden trabajar juntos sin conflicto directo.
A-C Posible Conflicto	Un firewall muy restrictivo (confidencialidad) puede bloquear servicios legítimos (disponibilidad).
A-I Posible Conflicto	Sistemas muy redundados para disponibilidad pueden ser más complejos, aumentando superficies de ataque (integridad).

Cuadro 4: Interrelaciones entre elementos de la tríada CIA

1.6 Aplicación de la Tríada CIA en Infraestructuras de Red

En el contexto de redes Cisco, cada componente de la tríada se implementa mediante tecnologías y configuraciones específicas:

Confidencialidad en Cisco

VPN IPsec: Encripta tráfico entre routers. **SSH:** Reemplaza Telnet con comunicación cifrada. **ACLs:** Limitan acceso a interfaces y recursos. **MPLS:** Encapsula tráfico en túneles. **Firewall ASA:** Aplica políticas basadas en aplicación.

Integridad en Cisco

IPsec HMAC: Verifica que los datos no sean modificados en tránsito. **Firmas digitales:** Autentican origen de configuraciones. **Checksums:** Detectan errores de transmisión. **Logging:** Registra cambios para auditoría.

Disponibilidad en Cisco

Redundancia de routers: HSRP/VRRP para failover. **Link Aggregation:** Combina múltiples enlaces para mayor ancho de banda. **QoS:** Prioriza tráfico crítico. **DDoS Protection:** Limita tasas de conexión. **Backups:** Respaldos de configuraciones.

Relevancia para Ciberseguridad

La tríada CIA es fundamental para la defensa de redes. Un atacante puede violar uno o más principios. Por ejemplo, un malware que cifra archivos (ransomware) viola confidencialidad (datos ilegibles) e integridad (modificación destructiva), impactando también disponibilidad. Proteger

todos los tres aspectos simultáneamente es la base de una arquitectura segura.

1.7 Equilibrio Estratégico

Las organizaciones deben encontrar el equilibrio correcto entre seguridad y funcionalidad. Excesivo énfasis en confidencialidad mediante restricciones severas puede afectar disponibilidad. Por el contrario, maximizar disponibilidad sin controles adecuados compromete confidencialidad e integridad. La clave es una evaluación de riesgo que guíe la implementación de controles proporcionales a la importancia de los activos.

Nota Importante

El balance de la tríada CIA es específico de cada organización. Una institución financiera puede priorizar integridad (exactitud de transacciones), mientras que una plataforma de streaming puede priorizar disponibilidad. La evaluación de riesgos debe informar esta priorización.

Referencias de la unidad

ISO/IEC 27001 - Information Security Management System (2022). International Organization for Standardization.

Kurose, James F. y Keith W. Ross (2020). *Computer Networking*. 8th. Pearson Education.

Stallings, William (2017). *Cryptography and Network Security: Principles and Practice*. 7th. Pearson Education.

Standards, National Institute of y Technology (NIST) (2018). *Cybersecurity Framework*. U.S. Department of Commerce.

2 Access Control Lists (ACLs): Control de Tráfico en Routers

Competencias

- **Comprender:** Explicar cómo funcionan las ACLs en dispositivos Cisco y su rol en seguridad de redes.
- **Comprender:** Diferenciar entre ACLs estándar, extendidas y nombradas, reconociendo casos de uso para cada una.
- **Hacer:** Diseñar e implementar ACLs que cumplan con políticas de seguridad específicas en routers Cisco.

Objetivos

- Explicar qué son las ACLs y cómo operan en diferentes capas del modelo OSI.
- Identificar los componentes de una regla de ACL (permission, protocol, source, destination, port).
- Diseñar ACLs que implementan políticas de control de tráfico específicas.
- Aplicar ACLs en interfaces de routers Cisco (inbound/outbound).
- Validar el funcionamiento de ACLs mediante pruebas de conectividad y análisis de tráfico.

Resultados de Aprendizaje

- Explica el funcionamiento de ACLs en Cisco IOS con referencia a protocolos específicos (TCP, UDP, ICMP).
- Diseña ACLs estándar y extendidas que cumplen con requisitos de seguridad documentados.
- Aplica ACLs en routers, identificando direcciones (inbound/outbound) y números de línea (standard/extended).
- Documenta políticas de ACL y justifica decisiones de permitir/denegar tráfico específico.

2.1 ¿Qué es una ACL?

Una **Access Control List (ACL)** es un conjunto ordenado de reglas que un router o firewall utiliza para filtrar tráfico de red. Cada regla (denominada ACE - Access Control Entry) especifica si el tráfico que cumple ciertos criterios debe ser permitido o denegado. Las ACLs operan típicamente en la capa 3 (IP) o capa 4 (TCP/UDP) del modelo OSI.

Access Control Entry (ACE)

Regla individual dentro de una ACL que define una acción (permitir o denegar) para tráfico que coincida con criterios específicos como dirección IP origen, dirección IP destino, protocolo y puerto.

Ejemplo

Una ACL puede contener la regla: "Permitir todo tráfico TCP desde la red 192.168.1.0/24 hacia la red 10.0.0.0/8 en puerto 443 (HTTPS)". Cualquier paquete que coincida con estos criterios será permitido; cualquier otro será denegado (por defecto).

2.2 Tipos de ACLs en Cisco

Cisco soporta varios tipos de ACLs, cada uno con características y casos de uso específicos:

Tipo	Descripción	Rango de Números
Estándar	Filtra solo por dirección IP origen. Útil para control básico pero limitado.	1-99, 1300-1999
Extendida	Filtra por dirección origen, destino, protocolo, puerto. Máxima flexibilidad.	100-199, 2000-2699
Nombrada	Versión moderna de estándar o extendida con nombres descriptivos en lugar de números.	Nombres textuales

Cuadro 5: Tipos de ACLs en Cisco

2.2.1 ACLs Estándar

Las ACLs estándar (números 1-99, 1300-1999) evalúan solo la dirección IP origen. Son simples pero limitadas en precisión.

Sintaxis ACL Estándar

```
access-list <número> <permit|deny> <dirección-origen> [wildcard-mask]
```

Ejemplo

`access-list 10 permit 192.168.1.0 0.0.0.255`
Esta regla permite todo tráfico que se origina en la red 192.168.1.0/24. La máscara 0.0.0.255 es una wildcard mask que especifica qué bits de la dirección son significativos.

2.2.2 ACLs Extendidas

Las ACLs extendidas (números 100-199, 2000-2699) son más poderosas, permitiendo especificación de origen, destino, protocolo y puertos.

Sintaxis ACL Extendida

```
access-list <número> <permit|deny> <protocol> <src-ip> [src-port] <dst-ip>
[dst-port]
```

Ejemplo

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 80
```

Permite tráfico TCP desde 192.168.1.0/24 hacia 10.0.0.0/8 en puerto 80 (HTTP).

2.2.3 ACLs Nombradas

Las ACLs nombradas son la versión moderna, usando nombres descriptivos en lugar de números, facilitando gestión y documentación.

Sintaxis ACL Nombrada

```
ip access-list standard|extended <nombre>
permit|deny <criterios>
```

Ejemplo

```
ip access-list extended PERMITIR-HTTPS
permit tcp any 10.0.0.0 0.0.0.255 eq 443
```

Define una ACL nombrada que permite HTTPS (puerto 443) a la red 10.0.0.0/8 desde cualquier origen.

2.3 Estructura y Procesamiento de ACLs

Las ACLs se procesan secuencialmente, línea por línea. Una vez que un paquete coincide con una regla, se aplica la acción (permitir o denegar) y el procesamiento se detiene. Si ninguna regla coincide, se aplica la acción implícita por defecto: denegar.

Aspecto	Descripción
Orden de Evaluación	Las reglas se evalúan de arriba hacia abajo. La primera que coincida se aplica.
Acción Implícita	Si ninguna regla coincide explícitamente, se deniega el tráfico (deny any implícito).
Direccion de Aplicación	Inbound: filtra tráfico que entra a la interfaz. Outbound: filtra tráfico que sale de la interfaz.
Wildcards	Máscaras de comodín especifican qué bits de IP son significativos. 0.0.0.255 = todos los últimos 8 bits importan.

Cuadro 6: Características de procesamiento de ACLs

Ejemplo

Una ACL con tres reglas:

1. Denegar TCP desde 203.0.113.5 a puerto 22 (SSH)
2. Permitir TCP desde cualquier origen a puerto 443 (HTTPS)
3. Negar todo lo demás (implícito)

Un paquete SSH desde 203.0.113.5 será denegado por la regla 1. Un paquete HTTPS desde 192.168.1.1 pasará la regla 1, coincidirá con la regla 2 y será permitido. Un paquete Telnet desde cualquier origen pasará las primeras dos reglas, alcanzará el denegar implícito y será denegado.

2.4 Aplicación de ACLs en Interfaces

Las ACLs deben ser aplicadas a una interfaz específica en una dirección específica:

Aplicar ACL a Interfaz

```
interface <tipo> <número>
ip access-group <número|nombre> in|out
```

Relevancia para Ciberseguridad

Las ACLs son una defensa crítica contra acceso no autorizado. Una ACL mal configurada es peor que ninguna, ya que crea falsa sensación de seguridad.

Referencias de la unidad

Cisco Systems, Inc. (2023). *Access Control Lists (ACLs) Configuration Guide*. Documentación técnica de Cisco.

Kurose, James F. y Keith W. Ross (2020). *Computer Networking*. 8th. Pearson Education.

Tanenbaum, Andrew S. y David J. Wetherall (2011). *Computer Networks*. 5th. Pearson Education.

3 Virtual Private Networks (VPN) IPsec: Encriptación de Comunicaciones

Competencias

- **Comprender:** Explicar el concepto de VPN y su rol en proteger comunicaciones sobre redes públicas o no confiables.
- **Comprender:** Analizar la arquitectura de IPsec, identificando sus componentes y protocolos constituyentes.
- **Hacer:** Diseñar e implementar túneles VPN IPsec entre dispositivos Cisco, garantizando confidencialidad e integridad.

Objetivos

- Definir Virtual Private Network (VPN) y sus ventajas en comunicaciones empresariales.
- Explicar cómo IPsec proporciona confidencialidad, integridad y autenticación en comunicaciones IP.
- Identificar componentes de IPsec: IKE (Internet Key Exchange) y protocolos ESP/AH.
- Diseñar topologías de VPN Site-to-Site y Remote-Access.
- Configurar y validar túneles VPN IPsec en routers Cisco.

Resultados de Aprendizaje

- Explica, con diagramas, cómo IPsec encripta y autentica tráfico en un túnel VPN.
- Diseña políticas de IPsec incluyendo algoritmos de encriptación, integridad y autenticación.
- Configura y valida túneles VPN entre routers Cisco en topologías Site-to-Site.
- Diagnostica problemas en VPN mediante análisis de logs y pruebas de conectividad.

3.1 ¿Qué es una VPN?

Una **Virtual Private Network (VPN)** es una red privada que se crea sobre una red pública (como Internet), utilizando encriptación para proteger la confidencialidad e integridad de los datos transmitidos. Las VPN permiten comunicaciones seguras entre sitios remotos o trabajadores remotos y la sede corporativa, como si estuvieran en una red privada dedicada, pero sin los costos de arrendamiento de líneas privadas.

VPN

Tecnología que crea un túnel cifrado sobre una red pública, permitiendo comunicación privada y segura entre dos puntos, como si existiera un enlace dedicado privado entre ellos.

3.1.1 Tipos de VPN

Tipo	Descripción	Caso de Uso
Site-to-Site	Conecta dos o más sitios completos (redes LAN). El túnel se establece entre routers fronterizos.	Conectar oficinas remotas a sede corporativa.
Remote-Access	Conecta individuos (usuarios remotos o trabajadores en casa) a la red corporativa. Requiere cliente VPN.	Trabajadores remotos, nómadas, teletrabajo.

Cuadro 7: Tipos de VPN

Ejemplo

Una empresa con sedes en Bogotá y Tunja establece una VPN Site-to-Site IPsec entre los routers fronterizos. Los servidores en Tunja (red privada 10.2.0.0/16) pueden comunicarse de forma segura con las workstations en Bogotá (red privada 10.1.0.0/16) como si estuvieran en una red local, aunque el tráfico viaja encriptado a través de Internet.

3.2 IPsec: Protocolo de Seguridad IP

IPsec (Internet Protocol Security) es un framework de protocolos y estándares que proporciona seguridad a nivel de capa de red (IP). IPsec no es un único protocolo sino una suite que integra múltiples componentes:

IPsec

Suite de protocolos de seguridad que proporciona autenticación, encriptación e integridad para comunicaciones IP, operando en la capa 3 (red) del modelo OSI.

3.2.1 Componentes de IPsec

Componente	Función
IKE v1/v2	Internet Key Exchange: protocolo para negociación de parámetros de seguridad y distribución de claves.
ESP	Encapsulating Security Payload: proporciona confidencialidad, autenticidad e integridad.
AH	Authentication Header: proporciona autenticación e integridad (menos común, a menudo reemplazado por ESP).
SA	Security Association: parámetros (direcciones, algoritmos, claves) que define cómo se protege tráfico específico.

Cuadro 8: Componentes de IPsec

3.2.2 Algoritmos de Encriptación

Transforman datos en formato ilegible. Ejemplos comunes:

Algoritmo	Tamaño Clave	Nota
DES	56 bits	Obsoleto, nunca usar.
3DES	168 bits	Seguro pero lento.
AES	128, 192, 256 bits	Estándar moderno, recomendado.

Cuadro 9: Algoritmos de encriptación en IPsec

3.3 Configuración de VPN IPsec en Cisco

La configuración de VPN en routers Cisco sigue pasos ordenados:

Pasos de Configuración

1. Definir políticas IKE (Fase 1) 2. Definir políticas IPsec (Fase 2) 3. Crear crypto maps 4. Aplicar a interfaz 5. Probar y validar

Nota Importante

[Configuración Completa] Aunque la configuración detallada está fuera del alcance de esta guía teórica, el estudiante debe entender que cada paso define aspectos de la negociación y protección de tráfico. Las prácticas de laboratorio cubrirán configuración paso a paso con ejemplos concretos.

3.4 Ventajas y Limitaciones de VPN IPsec

Aspecto	Descripción
Ventajas	Encriptación de extremo a extremo, autenticación mutua, perfecta para Site-to-Site, bien soportada en equipos Cisco.
Limitaciones	Configuración compleja, no inspecciona contenido de aplicación, requiere sincronización de relojes para correcta validación.

Cuadro 10: Características de IPsec

Relevancia para Ciberseguridad

IPsec es fundamental para seguridad de WAN en infraestructuras empresariales. Sin VPN, datos entre sitios viajarían sin protección por Internet, expuestos a ataques MITM. IPsec proporciona confianza en que comunicaciones son privadas e íntegras.

Referencias de la unidad

Cisco Systems, Inc. (2023). *IPsec Configuration Guide*. Documentación técnica de Cisco.

Kaufman, C., P. Hoffman, Y. Nir y P. Eronen (2014). *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 7296.

Kent, S. y K. Seo (2005). *Security Architecture for the Internet Protocol*. RFC 4301.

Stallings, William (2017). *Cryptography and Network Security: Principles and Practice*. 7th. Pearson Education.

4 Firewalls Cisco ASA: Protección del Perímetro de Red

Competencias

- **Comprender:** Explicar la función de un firewall en la protección del perímetro de red y sus componentes arquitectónicos.
- **Comprender:** Analizar características avanzadas de firewalls de nueva generación como inspección stateful y control de aplicaciones.
- **Hacer:** Diseñar e implementar políticas de firewall en Cisco ASA para protección de infraestructuras de red.

Objetivos

- Explicar qué es un firewall y cómo opera en la protección del perímetro de una red corporativa.
- Diferenciar entre firewalls de inspección de estado (stateful) y sin estado (stateless).
- Identificar características de firewalls de nueva generación (NGFW): inspección profunda, control de aplicaciones, prevención de intrusiones.
- Diseñar zonas de seguridad en el Cisco ASA (inside, outside, DMZ).
- Configurar y validar políticas de acceso en Cisco ASA.

Resultados de Aprendizaje

- Explica la diferencia entre ACLs en routers y políticas de firewall en ASA en términos de visibilidad y control.
- Diseña arquitecturas de red que incluyen zonas de seguridad (DMZ, inside, outside) con políticas apropiadas.
- Configura reglas de acceso en Cisco ASA basadas en requerimientos de seguridad documentados.
- Valida el funcionamiento de políticas de firewall mediante pruebas de conectividad cruzada entre zonas.

4.1 ¿Qué es un Firewall?

Un **firewall** es un dispositivo o software que monitorea y controla el tráfico de red que entra y sale de una red, aplicando políticas de seguridad definidas. Actúa como un guardián en el perímetro de la red, tomando decisiones de permitir o denegar tráfico basándose en un conjunto de reglas.

Firewall

Dispositivo o software que protege una red controlando acceso entre la red protegida y redes externas (como Internet), implementando políticas de seguridad basadas en protocolos, direcciones, puertos y contenido.

4.1.1 Funciones Principales de un Firewall

Funciones

1. Filtrado de tráfico: Permite o deniega tráfico basándose en reglas. **2. Inspección de estado:** Mantiene registro de conexiones activas, permitiendo tráfico de respuesta sin requerer reglas explícitas. **3. Traducción de direcciones:** NAT (Network Address Translation) oculta direcciones internas. **4. Prevención de intrusiones:** Detecta y bloquea patrones de ataque. **5. Control de aplicaciones:** Permite/deniega aplicaciones específicas.

4.2 Generaciones de Firewalls

La tecnología de firewall ha evolucionado significativamente:

Generación	Características	Ejemplo
Primera	Filtra por puerto y protocolo (stateless).	Filtrado básico.
Segunda	Inspección stateful, mantiene registro de conexiones.	Cisco ASA tradicional.
Tercera+	Inspección profunda (DPI), control de aplicaciones, prevención de intrusiones integrada (NGFW).	Cisco ASA con FirePOWER.

Cuadro 11: Generaciones de firewalls

4.3 Cisco ASA (Adaptive Security Appliance)

El **Cisco ASA** es un firewall de nueva generación que combina inspección stateful, prevención de intrusiones, control de aplicaciones y otras tecnologías en un único dispositivo. Es fundamental en infraestructuras empresariales para protección del perímetro.

Cisco ASA

Firewall de seguridad adaptativa que proporciona inspección de tráfico con estado, prevención de intrusiones integrada, control de aplicaciones, NAT y VPN, operando como punto central de protección en el perímetro de red.

4.4 Arquitectura de Zonas de Seguridad

El ASA organiza interfaces en zonas de seguridad, cada una con nivel de confianza diferente:

Zona	Descripción	Ejemplo
Inside	Zona confiable con usuarios internos. Máximo nivel de confianza.	Red LAN corporativa.
Outside	Zona no confiable, conexiones externas. Mínimo nivel de confianza.	Internet pública.
DMZ	Zona intermedia para servidores de cara al público. Confianza parcial.	Servidores web, email públicos.

Cuadro 12: Zonas de seguridad en Cisco ASA

Ejemplo

Arquitectura típica:

- **Inside:** Red LAN 192.168.1.0/24 con usuarios y servidores internos.
- **DMZ:** Red 10.0.0.0/24 con servidor web accesible desde Internet.
- **Outside:** Internet pública.

Políticas:

- Inside puede iniciar conexiones a Outside y DMZ (tráfico saliente).
- Outside puede iniciar conexiones a DMZ (para acceder servidor web) pero no a Inside.
- DMZ puede responder a conexiones desde Outside pero no puede iniciar hacia Inside sin autorización explícita.

4.5 Políticas de Acceso en ASA

Las políticas de acceso en ASA definemás allá de simple permitir/denegar; especifican direcciones, puertos, protocolos y acciones más sofisticadas:

Componente	Descripción
Origen	Dirección IP o red que inicia la conexión. Puede ser específica o any (cualquiera).
Destino	Dirección IP o red hacia donde va la conexión.
Protocolo	TCP, UDP, ICMP, u otros. Define tipo de comunicación.
Puerto	Puerto específico o rango de puertos. Ejemplo: 80 para HTTP, 443 para HTTPS.
Acción	Permit (permitir), Deny (denegar), Inspect (inspección profunda), Log (registrar).

Cuadro 13: Componentes de una política de acceso en ASA

4.6 Inspección Profunda de Paquetes (DPI)

Un avance importante en firewalls moderno es la **inspección profunda de paquetes (Deep Packet Inspection - DPI)**, que analiza contenido de aplicación, no solo encabezados de protocolo.

DPI

Tecnología que analiza payload (contenido) de paquetes de red, permitiendo inspeccionar y controlar aplicaciones específicas, protocolos cifrados y contenido potencialmente malicioso.

Ejemplo

DPI en Cisco ASA:

- Sin DPI: Firewall ve "tráfico TCP puerto 443" y lo permite si la política lo autoriza. No sabe qué aplicación es.
- Con DPI: Firewall inspecciona contenido, identifica que es tráfico BitTorrent, y puede bloquearlo aunque use puerto 443 (típicamente HTTPS). Proporciona control granular por aplicación, no solo por puerto.

4.7 Función NAT en Firewall

El ASA realiza **Network Address Translation (NAT)**, traduciendo direcciones IP privadas internas a públicas para Internet, proporcionando seguridad por oscurecimiento.

NAT

PAT (Port Address Translation): Traduce múltiples direcciones internas a una sola pública usando puertos diferentes. Típica configuración donde todos los usuarios internos aparecen como una dirección pública.

4.8 Mejores Prácticas en Firewalls

Nota Importante

[Principios] **1. Denegar por Defecto:** Solo permitir tráfico específicamente necesario. **2. Minimalismo:** Mantener políticas simples y documentadas. **3. Auditoría Regular:** Revisar logs y políticas periódicamente. **4. Defensa en Profundidad:** No confiar únicamente en firewall; combinar con ACLs, VPN, IDS. **5. Teste Cambios:** Validar políticas nuevas en laboratorio antes de producción.

Relevancia para Ciberseguridad

Un firewall ASA bien configurado es defensa crítica contra amenazas externas. Sin embargo, no es suficiente solo. Debe combinarse con otras tecnologías: VPN para datos en tránsito, encriptación para datos en reposo, IDS/IPS para detección de ataques, y seguridad de endpoint en hosts individuales.

Referencias de la unidad

Cheswick, William R., Steven M. Bellovin y Aviel D. Rubin (2003). *Firewalls and Internet Security: Repelling the Wily Hacker*. 2nd. Addison-Wesley Professional.

Cisco Systems, Inc. (2023). *Cisco ASA 5500-X Series Firewalls: Next-Generation Security Appliances*. Disponible en línea: https://www.cisco.com/.

Stallings, William (2017). *Cryptography and Network Security: Principles and Practice*. 7th. Pearson Education.

Glosario de Términos

Glosario

Término	Definición
ACL	Access Control List. Lista de reglas para controlar acceso a recursos de red.
ARP	Address Resolution Protocol. Mapea direcciones IP a direcciones MAC.
Broadcast	Transmisión enviada a todos los dispositivos del segmento de red.
CIDR	Classless Inter-Domain Routing. Notación dirección/prefijo para representar redes.
DMZ	Demilitarized Zone. Zona semi-protegida para servidores públicos.
FCS	Frame Check Sequence. Campo de detección de errores en tramas Ethernet.
Firewall	Dispositivo que controla el tráfico entre redes según políticas de seguridad.
IPsec	Internet Protocol Security. Suite de protocolos para comunicaciones seguras.
LAN	Local Area Network. Red de área local.
LLC	Logical Link Control. Subcapa de enlace de datos (IEEE 802.2).
MAC	Media Access Control. Dirección física de 48 bits / Subcapa de enlace de datos.
Máscara	Valor de 32 bits que define la porción de red y host en una dirección IPv4.
NAT	Network Address Translation. Traducción de direcciones IP públicas/privadas.
Next Hop	Siguiente salto: dirección IP del próximo router en la ruta al destino.
OSPF	Open Shortest Path First. Protocolo de enrutamiento de estado de enlace.
PDU	Protocol Data Unit. Forma que toma un bloque de datos en cada capa del modelo.
QoS	Quality of Service. Calidad de servicio para administrar congestión en la red.
Subred	División lógica de una red IP más grande.
VLAN	Virtual LAN. Segmentación lógica de redes en un switch.
VLSM	Variable Length Subnet Mask. Máscaras de subred de longitud variable.
VPN	Virtual Private Network. Red privada virtual sobre infraestructura pública.
WAN	Wide Area Network. Red de área amplia.