

Contenido

Apuntes Tema 5: Cortafuegos	3
Capítulo 1	3
Funciones Fundamentales de un Cortafuegos	3
Cortafuegos de Red vs. Basados en Host	4
Tres Pilares de la Protección Moderna	5
Cortafuegos de Hardware y Software.....	6
Cortafuegos en la Nube	7
Cortafuegos de red: Soluciones Comunes	8
Cortafuegos Basados en Host: Soluciones Comunes	9
Capítulo 2	10
Clasificación según Niveles de Filtrado de Tráfico	10
Protección en Múltiples Niveles	10
Filtrado a Nivel de Paquetes.....	11
Ejemplos de Filtrado a Nivel de Paquetes.....	12
Filtrado a Nivel de Estado	13
Ejemplos de Funcionamiento del Filtrado a Nivel de Estado	14
Filtrado a Nivel de Aplicación	15
Ejemplos de Inspección Profunda de Contenido (Capa 7)	16
Firewalls de Nueva Generación (NGFW)	17
Ejemplos de Capacidades de un NGFW.....	18
Capítulo 3	19
Estrategias para Limitar Accesos en la Red	19
Ejemplo Práctico: Red Corporativa Segmentada.....	20
Tema 6 Proxy.....	21
Características Principales de un Proxy.....	22
Ejemplos Prácticos de Funcionalidades de un Proxy	23
Forward Proxy (Proxy de Reenvío).....	24
Proxy Transparente	25

Reverse Proxy (Proxy Inverso).....	26
Diferencias Clave entre Tipos de Proxy	27
Casos de Uso y Ejemplos Reales	28

Apuntes Tema 5: Cortafuegos

Capítulo 1

Cortafuegos: Características, Tipos y Funciones Esenciales para la Seguridad de Redes

Una guía completa sobre la primera línea de defensa en ciberseguridad moderna

Funciones Fundamentales de un Cortafuegos

Supervisión y Filtrado

Inspecciona y filtra meticulosamente cada paquete de datos que intenta atravesar la red, analizando contenido, origen, destino y comportamiento para evitar intrusiones, malware y amenazas avanzadas persistentes.

Registro y Auditoría

Documenta todas las actividades sospechosas y eventos de seguridad en registros detallados, facilitando análisis forenses, cumplimiento normativo y la identificación de patrones de ataque para mejorar las defensas.

Aplicación de Políticas

Implementa políticas de seguridad personalizadas y granulares según las necesidades específicas de cada organización, departamento o usuario, garantizando un equilibrio entre protección y productividad.

Estas funciones trabajan en conjunto para crear un ecosistema de seguridad robusto y adaptable que evoluciona con las amenazas emergentes.

Cortafuegos de Red vs. Basados en Host

Cortafuegos de Red

Estos sistemas de protección perimetral se posicionan estratégicamente en puntos clave entre redes internas y externas, actuando como guardianes centralizados que filtran todo el tráfico antes de que alcance la infraestructura corporativa.

- Protegen toda la infraestructura simultáneamente
- Ubicados en gateways y puntos de entrada principales
- Proporcionan visibilidad completa del tráfico organizacional
- Ideales para políticas de seguridad centralizadas
- Reducen la carga administrativa al gestionar protección desde un punto único

Cortafuegos Basados en Host

Software especializado instalado directamente en dispositivos individuales, proporcionando una capa adicional de protección personalizada que complementa las defensas perimetrales y protege contra amenazas internas.

- Protección específica a nivel de dispositivo
- Control granular sobre aplicaciones y procesos individuales
- Defensa contra amenazas internas y movimiento lateral
- Protección continua incluso fuera de la red corporativa
- Políticas adaptadas a roles y necesidades específicas del usuario

Tres Pilares de la Protección Moderna

Hardware

Rendimiento y protección perimetral robusta

Software

Flexibilidad y control granular individual

Cloud

Escalabilidad y protección distribuida global

La seguridad óptima a menudo requiere una combinación estratégica de estos tres enfoques, aprovechando las fortalezas únicas de cada tipo para crear una defensa en profundidad que proteja todos los vectores de ataque posibles.

Cortafuegos de Hardware y Software

Cortafuegos de Hardware

Dispositivos físicos dedicados exclusivamente a la seguridad de red, diseñados para manejar grandes volúmenes de tráfico con mínima latencia. Estos aparatos especializados ofrecen rendimiento superior y son ideales para redes corporativas con múltiples usuarios y dispositivos conectados simultáneamente.

Características distintivas:

- Procesamiento optimizado para filtrado de tráfico
- Protección para múltiples equipos y segmentos de red
- Alto rendimiento sin impacto en recursos del sistema
- Interfaces físicas dedicadas para diferentes zonas de seguridad
- Resistencia a ataques de denegación de servicio

Cortafuegos de Software

Programas especializados instalados en dispositivos individuales que proporcionan protección flexible y personalizable. Estos cortafuegos complementan la seguridad a nivel de usuario, permitiendo control granular sobre aplicaciones específicas y adaptándose a las necesidades cambiantes de cada dispositivo.

Ventajas principales:

- Instalación flexible en múltiples plataformas
- Actualizaciones frecuentes y rápidas
- Control detallado de aplicaciones individuales
- Menor inversión inicial comparado con hardware
- Protección portátil que viaja con el dispositivo

Cortafuegos en la Nube

Alojamiento en la Nube

Solución completamente alojada en infraestructura cloud que protege activos distribuidos, usuarios remotos y aplicaciones SaaS sin necesidad de hardware físico en las instalaciones.

Escalabilidad Dinámica

Capacidad de escalar recursos de seguridad instantáneamente según demanda, adaptándose a picos de tráfico y crecimiento organizacional sin inversiones significativas en infraestructura.

Flexibilidad Total

Gestión centralizada de políticas de seguridad para entornos híbridos, multi-nube y trabajo remoto, proporcionando protección consistente independientemente de la ubicación de usuarios y recursos.

Los cortafuegos en la nube representan la evolución natural de la seguridad perimetral, adaptándose perfectamente a la realidad de las organizaciones modernas donde los límites tradicionales de red han desaparecido. Esta tecnología elimina la complejidad de gestionar hardware físico, reduce costos operativos y proporciona acceso a capacidades avanzadas de seguridad que se actualizan automáticamente.

"El futuro de la seguridad de red reside en soluciones cloud-native que protegen datos y usuarios independientemente de su ubicación física."

Cortafuegos de red: Soluciones Comunes

Fortinet FortiGate	Hardware	Líder en appliances físicos, aunque también tiene versiones virtuales.
Cisco Secure Firewall	Hardware	Anteriormente conocido como ASA/Firepower. El estándar en muchas grandes empresas.
Palo Alto Networks	Hardware	Pioneros en cortafuegos de próxima generación (NGFW).
Sophos Firewall	Hardware	Popular por su facilidad de gestión; también disponible como software/virtual.
Check Point Quantum	Hardware	Soluciones de alta seguridad para grandes perímetros corporativos.
pfSense	Software	Código abierto. Se instala en un ordenador/servidor para convertirlo en un router/firewall de red.
AWS Network Firewall	Nube	Servicio gestionado nativo para proteger entornos dentro de Amazon Web Services.
Azure Firewall	Nube	Servicio nativo de Microsoft para proteger redes virtuales en Azure.

Cortafuegos Basados en Host: Soluciones Comunes

Microsoft Defender	Software	Viene integrado en Windows. Protege el dispositivo individual.
iptables / nftables	Software	El estándar integrado en la mayoría de sistemas Linux para filtrar tráfico en el propio servidor.
ZoneAlarm	Software	Solución clásica de terceros para protección personal en PCs.
Little Snitch	Software	Muy popular en macOS para controlar conexiones salientes de aplicaciones.

Capítulo 2

Clasificación según Niveles de Filtrado de Tráfico

Los cortafuegos han evolucionado desde simples filtros de paquetes hasta sistemas sofisticados capaces de inspeccionar profundamente el contenido y contexto del tráfico. Esta evolución responde a amenazas cada vez más complejas que requieren análisis multicapa para su detección y neutralización efectiva.

Protección en Múltiples Niveles

Nivel 1: Filtrado de Paquetes

Inspección básica de direcciones IP, puertos y protocolos. Primera barrera de defensa rápida y eficiente.

Nivel 2: Inspección de Estado

Análisis contextual de conexiones y sesiones. Prevención de ataques que explotan protocolos legítimos.

Nivel 3: Inspección de Aplicación

Análisis profundo de contenido y comportamiento. Detección de amenazas sofisticadas ocultas en tráfico normal.

Nivel 4: NGFW con IA

Inteligencia artificial y prevención unificada. Protección predictiva contra amenazas emergentes y desconocidas.

La arquitectura de seguridad moderna implementa estos niveles de forma combinada y superpuesta, creando una defensa en profundidad donde cada capa compensa las limitaciones de las anteriores y proporciona redundancia crítica contra amenazas multivectoriales.

Filtrado a Nivel de Paquetes

La Primera Generación de Protección

El filtrado a nivel de paquetes representa el enfoque más básico y fundamental de los cortafuegos, **operando en las capas de red** y transporte del modelo OSI. Esta técnica examina cada paquete de datos de forma aislada, sin mantener información sobre el estado de las conexiones o el contexto de las comunicaciones.

Características del filtrado de paquetes:

- Inspección de **direcciones IP de origen y destino**
- Análisis de números de **puerto TCP/UDP**
- Verificación de **protocolos** de capa de transporte
- Decisiones basadas en **reglas estáticas predefinidas**
- Alto rendimiento con mínima latencia
- Bloqueo o permiso según coincidencias exactas

Aunque limitado en capacidades de detección avanzada, este método sigue siendo extremadamente eficiente para filtrado básico y forma la base sobre la cual se construyen técnicas más sofisticadas.

Ejemplos de Filtrado a Nivel de Paquetes

Escenario	Regla de Filtrado de Paquetes (Estática)	Efecto
Bloqueo de Tráfico Malicioso	Denegar todo el tráfico entrante al puerto TCP 23 (Telnet) y puerto TCP 20/21 (FTP).	Impide que cualquier conexión externa intente usar estos protocolos no seguros o innecesarios para acceder a la red interna.
Control de Acceso Geográfico	Denegar todo el tráfico de la dirección IP de origen 103.20.100.0/24.	Bloquea inmediatamente a toda una subred, impidiendo que sus paquetes crucen el firewall.
Permitir Conexiones de Servidores Específicos	Permitir tráfico entrante al puerto TCP 443 (HTTPS) solo si la dirección IP de destino es la IP pública de nuestro servidor web 203.0.113.10.	Garantiza que solo el tráfico de navegación seguro llegue a nuestro servidor web, ignorando cualquier otro destino en la red.
Bloqueo de Protocolos de Red Específicos	Denegar todo el tráfico del Protocolo ICMP.	Impide el uso de comandos como ping y traceroute, evitando que atacantes potenciales realicen un reconocimiento de la red.

Filtrado a Nivel de Estado

El filtrado con estado representa un salto cualitativo significativo en la evolución de los cortafuegos, introduciendo la capacidad de **mantener contexto sobre las conexiones activas** y tomar decisiones inteligentes basadas en el historial de comunicaciones.

Seguimiento de Conexiones

Mantiene tablas dinámicas que **registran el estado de cada conexión** TCP, UDP e ICMP, recordando qué comunicaciones han sido iniciadas legítimamente y cuáles son respuestas esperadas.

Análisis Contextual

Evalúa cada paquete considerando su **relación con paquetes anteriores y posteriores** en la misma sesión, detectando anomalías que podrían indicar intentos de ataque o comportamiento malicioso.

Decisiones Dinámicas

Permite o bloquea tráfico basándose no solo en reglas estáticas, sino en el estado actual de las comunicaciones, adaptándose a flujos legítimos mientras rechaza intentos de conexión sospechosos.

Esta tecnología proporciona protección significativamente superior contra ataques sofisticados como secuestro de sesiones, falsificación de paquetes y exploits que intentan aprovecharse de conexiones legítimas establecidas.

Ejemplos de Funcionamiento del Filtrado a Nivel de Estado

Navegación Web

El firewall registra peticiones salientes y permite automáticamente que los datos de respuesta web regresen, sin necesidad de reglas entrantes explícitas.

Bloqueo de Falsificación de Sesión

Si un atacante envía un paquete de "respuesta" sin que haya habido una solicitud inicial desde la red interna, el firewall lo descarta. El paquete no coincide con ninguna conexión activa o esperada en la Tabla de Estado.

Protección FTP Activo

Al detectar el protocolo FTP, el firewall inspecciona el canal de control para ver qué puerto de datos se negoció. Dinámicamente abre ese puerto específico solo para la transferencia de archivos y solo entre esas dos direcciones IP por un tiempo limitado.

Prevención de Ataques de Denegación de Servicio

El firewall rastrea la cantidad de intentos de conexión y conexiones incompletas por origen. Si detecta un número excesivamente alto y rápido desde una única fuente, puede bloquear o limitar el tráfico de esa IP para evitar la saturación.

Estos ejemplos demuestran cómo el filtrado de estado proporciona una capa de seguridad inteligente y proactiva, esencial para proteger las redes modernas contra amenazas avanzadas y mantener la integridad de las comunicaciones.

Filtrado a Nivel de Aplicación

Inspección Profunda de Contenido

Los cortafuegos de nivel de aplicación operan en la capa 7 del modelo OSI, proporcionando la capacidad de inspeccionar el contenido real de las comunicaciones y comprender el comportamiento de aplicaciones específicas.

Capacidades avanzadas incluyen:

- Análisis detallado de protocolos HTTP, HTTPS, FTP, SMTP
- Detección de amenazas ocultas en tráfico cifrado
- Identificación de aplicaciones independientemente del puerto
- Prevención de fugas de datos sensibles
- Control granular por usuario y aplicación
- Bloqueo de malware embebido en tráfico legítimo

Protección contra amenazas avanzadas:

Este nivel de inspección es crucial para detectar ataques sofisticados que explotan vulnerabilidades en aplicaciones web, intentos de exfiltración de datos, malware polimórfico y amenazas persistentes avanzadas (APT) que operan dentro del tráfico aparentemente legítimo.

La inspección a nivel de aplicación puede reducir el rendimiento entre un 10-30%, pero la protección adicional justifica ampliamente este compromiso en entornos de alta seguridad.

Ejemplos de Inspección Profunda de Contenido (Capa 7)

Control de Uso de Aplicaciones

El firewall detecta el patrón de tráfico del protocolo de aplicaciones como Facebook, Netflix o WhatsApp, independientemente del puerto que utilicen, permitiendo un control granular de su uso en la red corporativa.

Prevención de Fuga de Datos

El firewall inspecciona el contenido de correos salientes (SMTP) o subidas de archivos (HTTPS), identificando y bloqueando información sensible que no debería abandonar la red.

Detección de Amenazas en Tráfico Cifrado

Mediante la inspección SSL/TLS, el firewall "descifra" y vuelve a cifrar el tráfico HTTPS entrante, permitiendo la detección de malware o exploits ocultos en comunicaciones cifradas.

Bloqueo de Archivos por Tipo Específico

El firewall analiza los encabezados y metadatos de los archivos que intentan descargarse (vía HTTP o FTP), bloqueando aquellos que no cumplen con las políticas de seguridad, como ejecutables o archivos comprimidos sospechosos.

Identificación de Uso Ilegítimo de Puertos

Detecta cuando el tráfico en un puerto estándar (ej. 80 para HTTP) no corresponde a su protocolo habitual, sino a patrones de túnel VPN o tráfico P2P (BitTorrent), señalando un posible uso no autorizado.

Estos ejemplos ilustran cómo los firewalls de capa 7 son esenciales para una seguridad avanzada, permitiendo a las organizaciones protegerse contra amenazas complejas y asegurar el cumplimiento de políticas de uso de aplicaciones y datos.

Firewalls de Nueva Generación (NGFW)

Los NGFW representan la **convergencia de múltiples tecnologías de seguridad** en una plataforma unificada, combinando capacidades tradicionales de cortafuegos con funciones avanzadas de prevención de amenazas, inspección profunda y inteligencia contextual.

Inteligencia Artificial Integrada

Algoritmos de machine learning que analizan patrones de comportamiento, detectan anomalías y predicen amenazas emergentes antes de que causen daño, aprendiendo continuamente de nuevos vectores de ataque.

Análisis en Tiempo Real

Procesamiento de millones de eventos de seguridad por segundo, correlacionando información de múltiples fuentes para identificar ataques coordinados y proporcionar respuesta automatizada inmediata.

Prevención Unificada de Amenazas

Integración de antivirus, anti-malware, IPS/IDS, filtrado web, control de aplicaciones y prevención de pérdida de datos en una única solución cohesiva con gestión centralizada.

"Los NGFW no solo detectan y bloquean amenazas conocidas; anticipan y neutralizan ataques emergentes mediante análisis predictivo y respuesta automatizada inteligente."

Ejemplos de Capacidades de un NGFW

Detección de Día Cero

Un archivo nunca antes visto ingresa a la red. El NGFW usa **Inteligencia Artificial** para analizar su comportamiento, identificándolo como malicioso y bloqueándolo de inmediato, sin depender de firmas.

Identificación de Túneles Maliciosos

Detecta el tráfico malicioso que se esconde en puertos legítimos (ej. 443 HTTPS), como túneles VPN o protocolos de Comando y Control (C&C), gracias a su **Inspección Profunda de Contenido**.

Respuesta Automatizada

Cuando un servidor interno muestra un tráfico saliente anómalo, el NGFW lo detecta en **Tiempo Real** a través de la correlación de eventos (IPS y análisis de comportamiento) y responde automáticamente.

Control de Riesgo por Usuario

Permite un **Control Granular por Usuario** y aplicación. Si un usuario autorizado a YouTube intenta descargar un video HD, el NGFW puede limitar o bloquear la acción para evitar el consumo excesivo de ancho de banda.

Estos escenarios resaltan la capacidad de los NGFW para ir más allá de la seguridad tradicional, ofreciendo una defensa proactiva y contextualizada contra las amenazas cibernéticas modernas.

Capítulo 3

Planificación de la Instalación de Cortafuegos

La implementación efectiva de cortafuegos requiere una planificación estratégica meticulosa que considere la topología de red, requisitos de seguridad, flujos de trabajo organizacionales y objetivos de cumplimiento normativo. Una instalación bien diseñada equilibra protección máxima con mínima fricción operacional.

Estrategias para Limitar Accesos en la Red

Identificación de Zonas Críticas

Mapear todos los activos de red, clasificándolos según criticidad, sensibilidad de datos y requisitos de acceso. Identificar sistemas que requieren aislamiento estricto y aquellos que necesitan mayor conectividad.

Segmentación de Red

Dividir la infraestructura en segmentos lógicos aislados (DMZ, red corporativa, servidores, IoT, invitados) con cortafuegos controlando el tráfico entre cada zona según el principio de menor privilegio.

Definición de Políticas de Acceso

Establecer reglas granulares y estrictas basadas en roles, necesidades del negocio y perfiles de riesgo. Documentar excepciones y revisar periódicamente para eliminar permisos obsoletos.

Implementación de Defensa en Capas

Desplegar cortafuegos perimetrales para protección externa e internos para controlar movimiento lateral, creando múltiples puntos de control que un atacante debe superar.

Monitorización y Ajuste Continuo

Implementar sistemas de registro, alertas y análisis de tráfico para identificar patrones anormales, ajustar políticas según amenazas emergentes y optimizar rendimiento.

Una planificación cuidadosa en la fase inicial previene configuraciones débiles que podrían dejar brechas de seguridad explotables y reduce significativamente el esfuerzo de remediación posterior.

Ejemplo Práctico: Red Corporativa Segmentada

Perímetro Externo

Cortafuegos NGFW de hardware en el borde de red bloqueando ataques externos, escaneando tráfico entrante y aplicando políticas de acceso remoto seguro.

DMZ Protegida

Zona desmilitarizada con servidores web y email públicos, aislada mediante cortafuegos dedicados que permiten tráfico específico mientras previenen acceso a la red interna.

Segmentación Interna

Cortafuegos internos separando departamentos sensibles (finanzas, RRHH, desarrollo) controlando tráfico lateral y previniendo propagación de amenazas entre segmentos.

Protección de Endpoint

Software de cortafuegos en dispositivos individuales proporcionando última línea de defensa contra amenazas que evaden controles perimetrales e internos.

Componentes de Hardware

- Cortafuegos perimetral de alto rendimiento (10-40 Gbps)
- Dispositivos internos para segmentación de VLANs
- Appliances dedicados para DMZ y zonas críticas
- Sistemas de prevención de intrusiones integrados

Componentes de Software

- Agentes en estaciones de trabajo corporativas
- Protección para dispositivos móviles y remotos
- Cortafuegos virtuales en entornos cloud híbridos
- Consolas centralizadas de gestión y monitorización

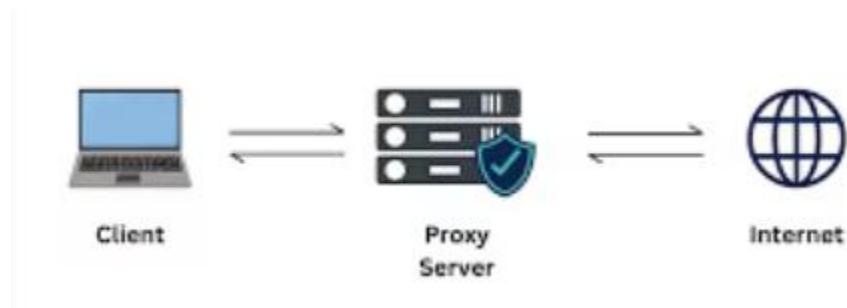
Este enfoque de defensa en profundidad multinivel garantiza que incluso si un atacante compromete una capa, múltiples barreras adicionales dificultan significativamente el movimiento lateral y la exfiltración de datos, proporcionando tiempo crítico para detección y respuesta.

Tema 6 Proxy

¿Qué es un Proxy?

- Un servidor proxy actúa como **intermediario inteligente** entre un usuario y el Internet.
- Recibe todas las solicitudes del usuario y las reenvía a los recursos web solicitados, ocultando la identidad real del solicitante.
- En una conexión normal, tú le pides información directamente a una página web. Con un proxy, el proceso cambia:

- 1.- Tú le haces la petición al proxy.
- 2.- El proxy solicita la información a la página web por ti.
- 3.- El proxy recibe la información y te la envía de vuelta



Características Principales de un Proxy

Privacidad Mejorada

Oculta la dirección IP real del usuario, protegiendo su identidad digital y ubicación geográfica.

Caché Inteligente

Almacena contenido frecuentemente solicitado para acelerar la carga de páginas web.

Control de Acceso

Filtrá y regula el acceso a sitios específicos o servicios según políticas establecidas.

Seguridad Reforzada

Bloquea proactivamente tráfico malicioso, ataques y contenido potencialmente peligroso.

Acceso a contenido restringido

Permite entrar a sitios que están bloqueados en tu país o región.

Ejemplos Prácticos de Funcionalidades de un Proxy

Privacidad Mejorada

Un periodista usa un proxy para ocultar su ubicación al investigar un tema delicado, evitando ser rastreado por su dirección IP real.

Caché Inteligente

En una oficina, el proxy guarda las páginas web más visitadas. La segunda vez que un empleado accede a la intranet o a un portal de noticias, la carga es casi instantánea.

Control de Acceso

Una escuela configura un proxy para bloquear el acceso a redes sociales y sitios de juegos durante el horario lectivo, asegurando la concentración de los alumnos.

Seguridad Reforzada

Un proxy empresarial detecta y bloquea un intento de phishing, impidiendo que un empleado acceda a un sitio web malicioso que podría robar credenciales.

Acceso a Contenido Restringido

Un usuario en un país con censura utiliza un proxy para acceder a noticias internacionales y plataformas de streaming que no están disponibles directamente en su región.

Forward Proxy (Proxy de Reenvío)

El Forward Proxy **actúa en nombre del cliente** para acceder a Internet, funcionando como su representante digital.

- Oculta completamente la IP del usuario final
- Puede evadir restricciones geográficas impuestas
- Utilizado en redes internas para controlar y monitorizar
- Filtra contenido según políticas organizacionales

Ejemplo práctico: Una empresa que bloquea el acceso a redes sociales durante el horario laboral y usa un forward proxy para filtrar y registrar intentos de acceso.

Proxy Transparente

Invisibilidad Total

- La diferencia con el anterior es que el usuario **no sabe que está usando un proxy**, funcionando de manera completamente transparente.
- No modifica solicitudes ni respuestas.
- La configuración se realiza en infraestructura de red. No en la computadora del cliente.

Sin Anonimato

La dirección IP original del usuario permanece visible, por lo que no ofrece protección de identidad.

Optimización Silenciosa

Se utiliza principalmente para **almacenamiento en caché y filtrado**.

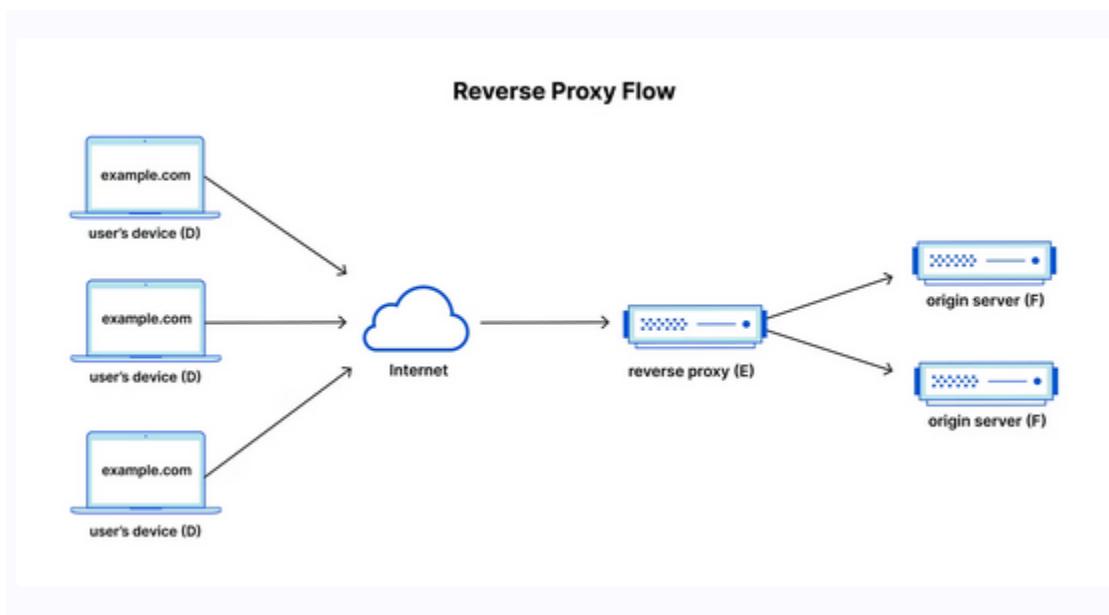
Implementación Común

Muy usado en redes corporativas y educativas para controlar el tráfico sin complicaciones técnicas ni configuración del cliente.

Reverse Proxy (Proxy Inverso)

A diferencia del forward proxy, el reverse proxy **actúa en nombre del servidor**, no del cliente.

- Recibe solicitudes externas de Internet
- Las dirige inteligentemente a servidores internos
- **FUNCIONALIDADES**
 - Oculta la IP real de los servidores
 - Bloquea ataques antes de llegar al servidor
 - Balanceo de Carga, Enrutamiento de Microservicios
 - Cifrar y descifrar el tráfico HTTPS
 - Caché de Contenido



Diferencias Clave entre Tipos de Proxy

Forward Proxy

Protege al cliente y controla su acceso a Internet. Actúa como escudo del usuario.

Proxy Transparente

Controla tráfico sin ocultar identidad ni intervención visible. Operación silenciosa.

Reverse Proxy

Protege y optimiza servidores, gestionando solicitudes entrantes. Portero del servidor.

Casos de Uso y Ejemplos Reales

Forward Proxy en Empresas

Empleados accediendo a Internet con restricciones corporativas, anonimato controlado y monitorización de actividad.

Proxy Transparente Educativo

Escuelas que filtran contenido inapropiado automáticamente sin que los alumnos noten su presencia.

Reverse Proxy en Grandes Plataformas

Sitios como Netflix o Amazon que balancean millones de solicitudes, protegen servidores y aceleran contenido globalmente.