Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Implantación y configuración de cortafuegos

Introducción
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
Criterios de seguridad para la segregación de redes en el cortafuegos mediante zonas desmilitarizadas / DMZ
Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones
Definición de reglas de corte en los cortafuegos
Relación de los registros de auditoría del cortafuegos, necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
Establecimiento de la monitorización y pruebas del cortafuegos
Resumen

Introducción

Para minimizar el riesgo de amenazas lógicas, es crucial fortalecer los puntos de acceso al sistema. El primer punto que debe protegerse es el punto de interconexión de la red privada de la empresa con Internet.

Los cortafuegos permiten la separación física de la red en diferentes segmentos o zonas, lo que ayuda a proteger contra amenazas externas y permite definir subredes internas protegidas entre sí.

Cuando los requisitos de seguridad son altos, se deben proteger las comunicaciones con redes privadas virtuales (VPN). Esto asegura que, incluso si las contramedidas de las pasarelas de seguridad son vulneradas, las comunicaciones no serán legibles para un externo.

El Esquema Nacional de Seguridad establece que el sistema debe proteger sus perímetros, especialmente cuando hay interconexión a redes públicas como Internet. Se deben analizar los riesgos de la interconexión y controlar el punto de unión.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

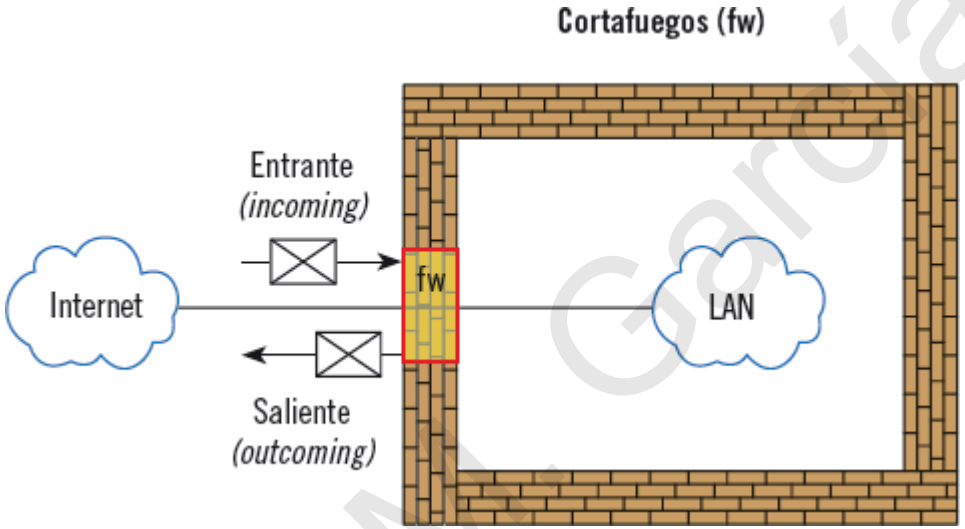
- La norma ISO 27002 establece controles para la implantación y uso de sistemas que separen las redes de comunicaciones. El objetivo es evitar el acceso no autorizado a la red, por lo que deben existir sistemas apropiados para la interconexión entre la red de la empresa y las redes de otras empresas o las redes públicas.

- Normas de seguridad. La serie ISO 27000 es un estándar de facto en seguridad de la información. La norma ISO 27002, que procede de la norma ISO 17799 del año 2005, define las contramedidas que deben aplicarse para cumplir la norma.

- Necesidad de una pasarela de seguridad Si se dispone de muchos usuarios externos, podría necesitarse una pasarela de seguridad que permita un control más granular, diferenciando servicios, con mecanismos de autenticación, que permita la definición de horarios, con sistemas de detección y prevención de intrusiones u otras funcionalidades.

- Esquema Nacional de Seguridad establece que se debe disponer de un sistema cortafuegos que separe la red interna del exterior, de forma que todo el tráfico pase por este punto, y que solo se deje progresar los flujos de tráfico previamente autorizados.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de ataques

- Los ataques de seguridad pueden parecer aleatorios, pero a menudo son el resultado del desconocimiento o la falta de concienciación sobre la seguridad de la información.
- Un atacante potencial puede observar los hábitos de los usuarios para planificar un ataque.

Recopilación de información

- Para explotar las vulnerabilidades de un sistema, el atacante necesita recopilar información sobre el sistema y sus usuarios.
- Esta información puede incluir horarios de trabajo, nombres de usuario, cambios en la empresa, aplicaciones y sistemas operativos utilizados, problemas frecuentes, proveedores, clientes, servicios externos, tipo de correo electrónico, y las claves.

Técnicas de ataque

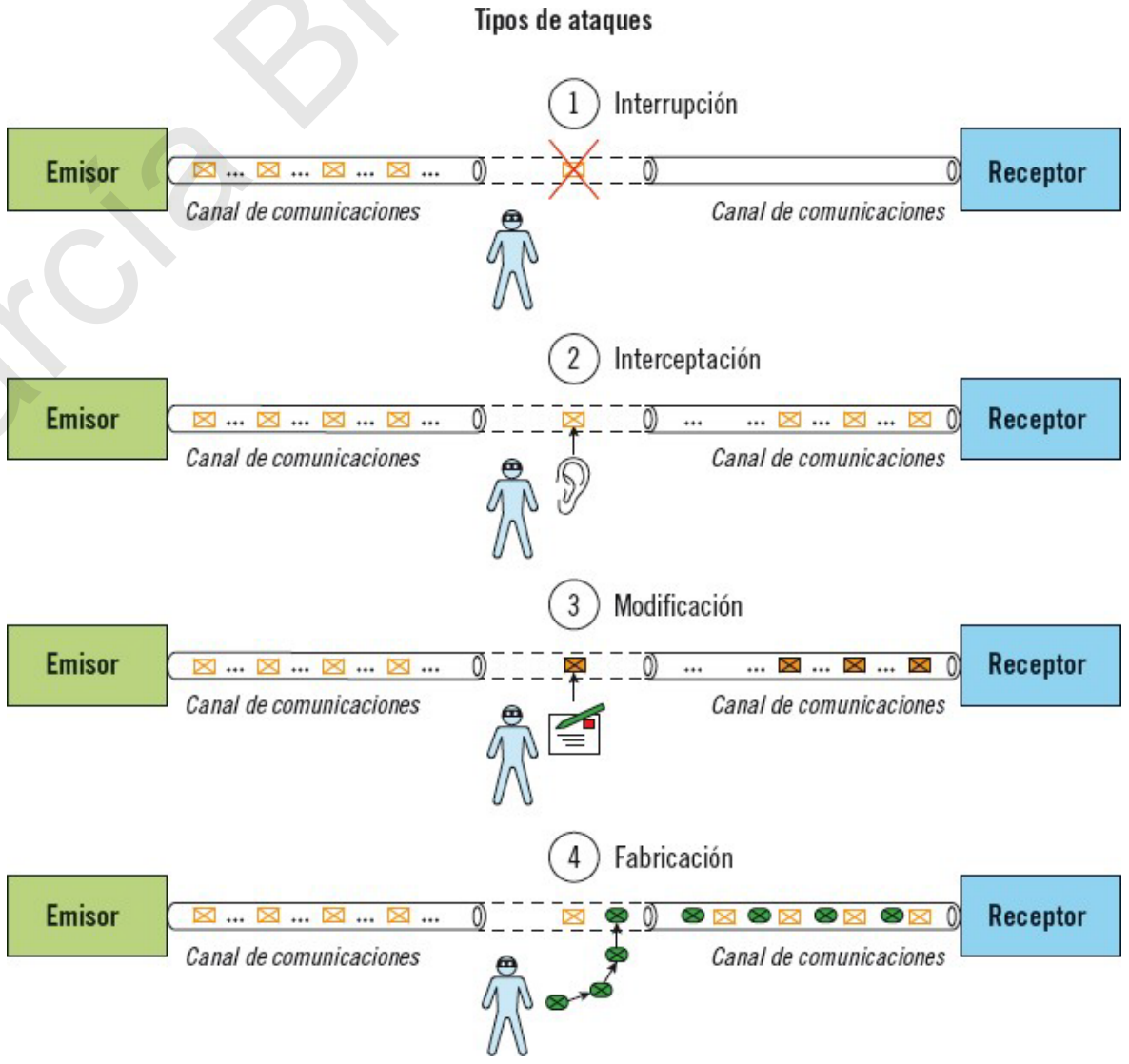
- Los atacantes pueden utilizar material físico, como correspondencia y documentos desechados, para obtener información.
- También pueden emplear técnicas de ingeniería social, como conversaciones, llamadas telefónicas y correos electrónicos, para engañar a los usuarios y obtener información.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de ataques

Tipos de amenazas lógicas

- Ataque de interrupción: un objeto del sistema no está disponible.
- Ataque de interceptación: acceso no autorizado a un objeto del sistema.
- Ataque de modificación: interceptación y modificación de un objeto del sistema.
- Ataque de fabricación: creación de un objeto similar al atacado.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de cortafuegos

- Los cortafuegos son equipos diseñados para restringir y filtrar el flujo de información entre redes.
- Se suelen emplear para separar la red interna de una empresa de Internet.
- También pueden utilizarse para definir subredes dentro de la empresa y aislarlas según la sensibilidad de la información que contienen.
- Los cortafuegos son esenciales para implementar la política de seguridad de la empresa y son un componente fundamental de la seguridad lógica.

Firewalls a Nivel de Red

- Actúan exclusivamente a nivel de red y se componen principalmente de routers.
- Ubicados entre la red interna y externa, filtran los paquetes de red según reglas predefinidas.
- Permiten aceptar, rechazar o no responder a paquetes según su origen o destino.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de cortafuegos

Firewalls a Nivel de Aplicación

- Conocidos normalmente como proxys, se sitúan entre clientes internos y servidores externos.
- No hay comunicación directa entre los clientes y los servidores externos.
- El proxy actúa como intermediario, conectándose al servidor externo si el acceso está autorizado.

Métodos de Protección

- Filtrado de Paquetes:
  - Filtrado estático: se aplican reglas fijas para autorizar o rechazar paquetes.
  - Filtrado dinámico: las reglas son dinámicas, basadas en el estado de la comunicación. (p.e.- permitir la entrada de paquetes en respuesta a las peticiones salientes)
- Protección Mediante Servidores Proxy:
  - Definen reglas para filtrar servicios entre segmentos de redes.
  - Pueden gestionar el tráfico de Internet y proporcionar funciones como el almacenamiento en caché de URL.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de cortafuegos

Un proxy es un servidor intermedio que actúa como intermediario entre los usuarios de una red y los servidores a los que solicitan recursos.

Básicamente, un proxy recibe las solicitudes de los clientes y las reenvía al servidor correspondiente, actuando como una barrera entre la red local y la red externa, como internet. Los proxies se utilizan principalmente para mejorar el rendimiento, la seguridad y el control de acceso a internet.

Un servidor proxy es un tipo específico de proxy que se utiliza para gestionar las solicitudes y respuestas entre los clientes y los servidores externos. Este servidor intercepta las solicitudes de los clientes y las procesa según las reglas definidas antes de reenviarlas al servidor final.

Los servidores proxy pueden realizar diversas funciones, como caché de datos, filtrado de contenido, anonimización de direcciones IP y control de acceso.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de cortafuegos

Proxys de aplicación, circuito y transmisión

Proxy de Aplicación:

- Funcionamiento: Actúa a nivel de aplicación del modelo OSI y puede filtrar y controlar el tráfico de aplicaciones específicas, como HTTP, FTP o SMTP.
- Funciones: Realiza inspección profunda de paquetes, control de acceso y filtrado de contenido en función de las reglas de seguridad definidas.
- Ejemplo: Proxy HTTP, proxy FTP, proxy SMTP.

Proxy a Nivel de Circuito:

- Funcionamiento: Opera a nivel de transporte del modelo OSI y proporciona una conexión segura y transparente entre el cliente y el servidor, sin inspeccionar los datos de la aplicación.
- Funciones: Ofrece anonimato al ocultar la dirección IP del cliente al servidor final y puede cifrar el tráfico para mayor seguridad.
- Ejemplo: VPN (Virtual Private Network), SOCKS proxy.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Tipos de cortafuegos

Proxy de Transmisión o de Red:

- Funcionamiento: Opera a nivel de red y proporciona una capa de intermediación entre los clientes y los servidores, permitiendo el enrutamiento selectivo del tráfico.
- Funciones: Puede realizar funciones de enrutamiento, filtrado de direcciones IP, balanceo de carga y gestión de ancho de banda.
- Ejemplo: Proxy transparente, proxy de enrutamiento.

¿Y que es un proxy Inverso?

Funcionamiento: El proxy inverso se encuentra en el lado del servidor y actúa como intermediario entre los clientes externos y los servidores internos. Intercepta las solicitudes de los clientes y las reenvía al servidor adecuado, y luego reenvía las respuestas del servidor de nuevo al cliente. Opera a nivel aplicación y maneja las solicitudes entrantes.

Funciones: Proporciona funciones como el equilibrio de carga, la terminación SSL, la caché de contenido y la protección de servidores internos al ocultar su ubicación y dirección IP.

Ejemplo: Un proxy inverso se puede utilizar para enrutar el tráfico web hacia varios servidores web internos, equilibrando la carga entre ellos y mejorando el rendimiento y la disponibilidad del servicio.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

- No hay una única forma de implementar un cortafuegos.
- Depende de los requisitos de seguridad, las redes internas, los servicios accesibles y el presupuesto.
- Ejemplos habituales para entornos de pequeñas y medianas empresas:
  - Utilizar un simple router doméstico.
  - Implementar redes complejas con servidores proxy y routers intercalados.
- Ventajas e inconvenientes dependen del contexto específico de cada caso.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Router de Filtrado (Screening Router)

Dispositivo de red utilizado para controlar y filtrar el tráfico entre dos redes separadas. Actúa como una barrera de seguridad entre la red interna y externa, protegiendo los recursos internos de posibles amenazas externas.

Ventajas:

- Seguridad de Red: Protege contra ataques externos, como intrusiones no autorizadas o ataques de malware.
- Control de Acceso: Permite definir políticas de acceso para regular qué tipo de tráfico se permite o se bloquea.
- Filtrado de Paquetes: Examina cada paquete de datos entrante y saliente para prevenir ataques de denegación de servicio (DoS) o intrusiones.
- NAT (Traducción de Direcciones de Red): Oculta las direcciones IP internas de los dispositivos hacia el exterior, proporcionando una capa adicional de seguridad.
- Monitoreo y Registro: Puede llevar un registro de eventos de red para facilitar la detección y análisis de posibles amenazas o problemas de seguridad.

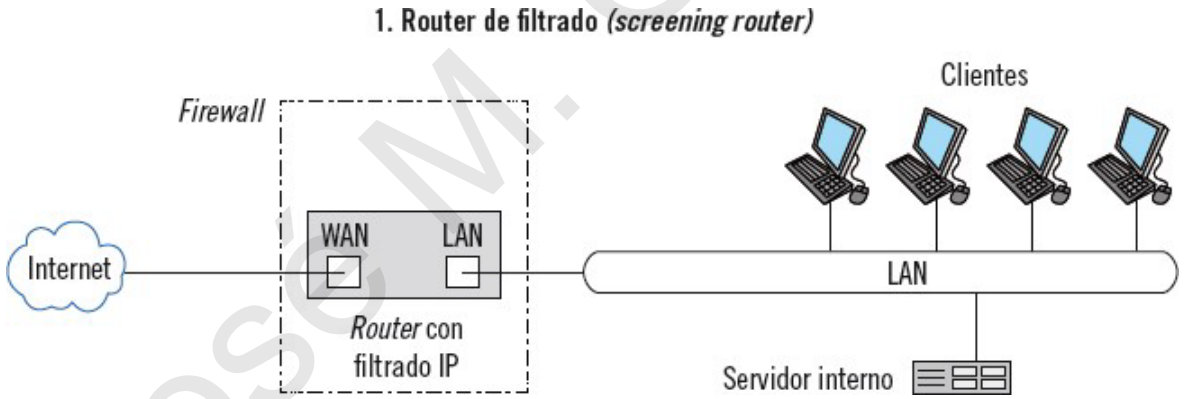
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Router de Filtrado (Screening Router)

Inconvenientes del Router de Filtrado

- Configuración Compleja
- El proceso de filtrado puede afectar el rendimiento del router, especialmente en redes con alto tráfico.
- Posibilidad de Falsos Positivos/Negativos: Configuraciones incorrectas pueden resultar en bloqueo de tráfico legítimo o permitir el paso de tráfico malicioso.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión con una Red

El Bastión con una Red, también conocido como "Bastion Host" o "Single-Homed Host", es un servidor especialmente configurado y reforzado que actúa como punto de entrada seguro a una red desde Internet.

¿Qué es un Bastión Host?

- Un Bastión Host es un servidor que se coloca en una posición estratégica dentro de la infraestructura de red para protegerla de amenazas externas. El punto de entrada y salida es una tarjeta de red
- Actúa como una puerta de enlace entre la red interna y el mundo exterior, filtrando y controlando el tráfico de red entrante y saliente. Se deshabilita el envío directo de tráfico IP interno al externo, y se bloquea por defecto todo el tráfico.

Ventajas del Bastión Host

- Seguridad Reforzada: Al concentrar y controlar todo el tráfico de red, proporciona un punto único de control y vigilancia para proteger la red interna.
- Acceso Controlado: Permite configurar políticas de acceso estrictas para determinar quién puede acceder a la red y qué servicios están disponibles.
- Auditoría y Registro: Facilita la monitorización y el registro detallado de todas las actividades de red, lo que ayuda en la detección y respuesta a posibles amenazas.

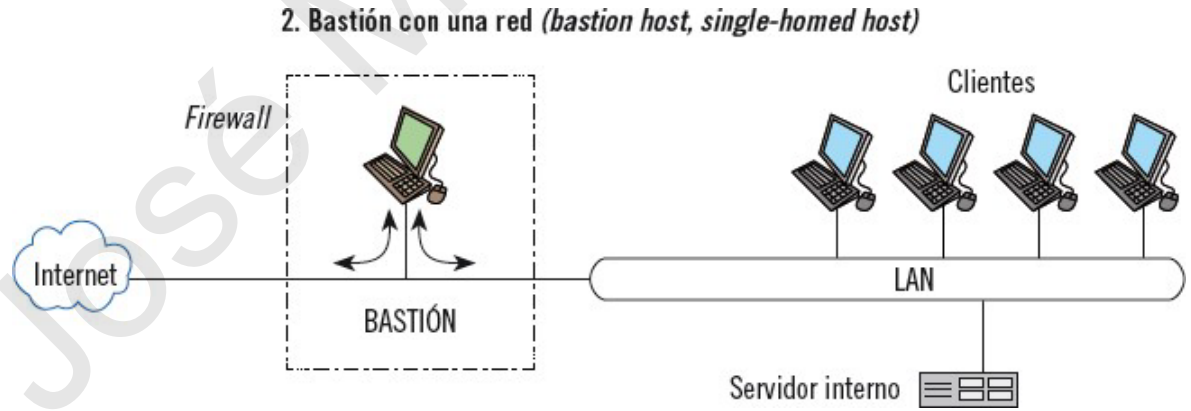
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión con una Red

Inconvenientes del Bastión Host

- Punto Único de Fallo: Si el Bastión Host se ve comprometido, toda la red puede quedar expuesta a riesgos de seguridad. Falta separación física entre la red sin proteger y la red protegida debido a que comparten la misma tarjeta de red.
- Configuración y Mantenimiento Complejo: Requiere conocimientos técnicos avanzados para configurar y mantener adecuadamente las políticas de seguridad.
- Costos Adicionales: Implementar y mantener un Bastión Host puede implicar costos adicionales de hardware, software y recursos humanos.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión con dos redes

En el diseño del Bastión con Dos Redes, también conocido como "Dual-Homed Host", el bastión incorpora dos tarjetas de red: una conectada a Internet y otra conectada a la LAN interna.

Esta configuración permite tener redes físicamente separadas, proporcionando mayor seguridad a la infraestructura de red.

Características

- El bastión actúa como una estación de doble domicilio al estar presente en ambas redes simultáneamente.
- No se recomienda que el bastión funcione como router, y se debe deshabilitar el acceso directo del tráfico IP entre interfaces para bloquear por defecto todo el tráfico.

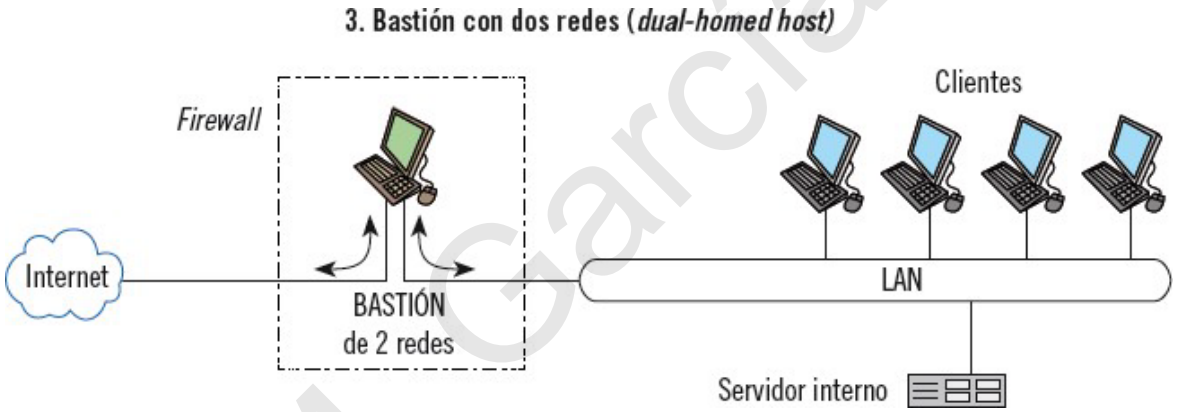
Ventajas

- Ofrece las mismas ventajas que el Bastión con una Red, pero elimina la desventaja de tener una sola interfaz de red.
- Proporciona mayor seguridad al tener redes físicamente separadas, lo que reduce el riesgo de comprometer toda la red en caso de un ataque.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión con dos redes



Bastión Multired (Multi-Homed Host)

El bastión puede tener más de dos tarjetas de red para atender a diferentes subredes privadas internas. Esta configuración se conoce como "Bastión Multired" o "Multi-Homed Host", y permite segmentar aún más la red interna para mejorar la seguridad y el control del tráfico.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Servidor proxy

El servidor proxy actúa como intermediario entre el cliente y el servidor real, sustituyendo al servidor real en la comunicación.

En el contexto de los cortafuegos, un proxy es una aplicación que se ejecuta en lugar de otra, gestionando las solicitudes de recursos en nombre del cliente.

Funcionamiento del Servidor Proxy

- Cuando un cliente realiza una solicitud de recurso, esta se dirige primero al servidor proxy en lugar del servidor real.
- El servidor proxy, ubicado en el bastión de dos redes, procesa la solicitud y la reenvía al servidor real, actuando como un filtro y controlando el acceso a la aplicación.

Tipos de Servidores Proxy

- Los servidores proxy más comunes son los utilizados para aplicaciones web, aunque también existen servidores proxy para otros protocolos como SMTP y FTP.
- Se configuran con un control de acceso para implementar el filtrado por aplicación, garantizando un acceso controlado a los recursos.

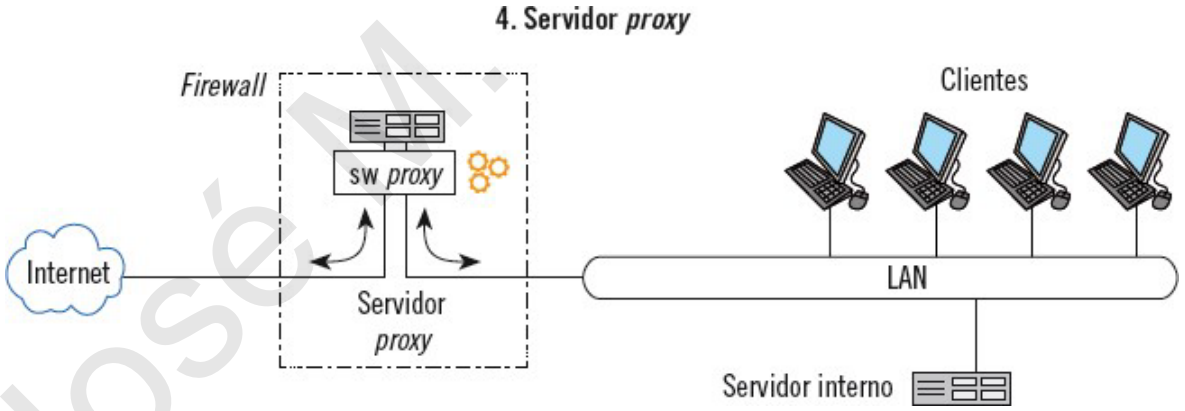
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Servidor proxy

Ubicación y Configuración del Servidor Proxy

- El servidor proxy se instala típicamente en un bastión de dos redes, donde se deshabilita el acceso directo del tráfico IP entre interfaces, bloqueando por defecto todo el tráfico.
- Aunque el servidor proxy aporta seguridad en el acceso a las aplicaciones, la protección frente a ataques la proporciona el bastión, minimizando las vulnerabilidades del sistema.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión Filtrado (Screened Host)

El bastión filtrado utiliza un equipo, generalmente un router, para filtrar los paquetes de red antes de llegar al bastión.

El router se configura para permitir solo ciertos tipos de tráfico hacia el bastión desde internet y conexiones internas desde el bastión hacia la red interna.

Zona Desmilitarizada (DMZ)

- La zona entre el router y el bastión se conoce como Zona Desmilitarizada (DMZ), actuando como una capa de seguridad adicional entre la red externa e interna.
- La DMZ proporciona una separación lógica o física entre las dos redes, dependiendo de si se emplea un bastión de una o dos redes.

Configuración y Ventajas

- La configuración con un bastión filtrado ofrece la ventaja de tener el bastión como la única parte del cortafuegos conectada a la red interna.
- Aunque tanto el router como el bastión representan puntos únicos de fallo, el diseño mejora al incluir dos etapas de protección, lo que lo hace más robusto en general.

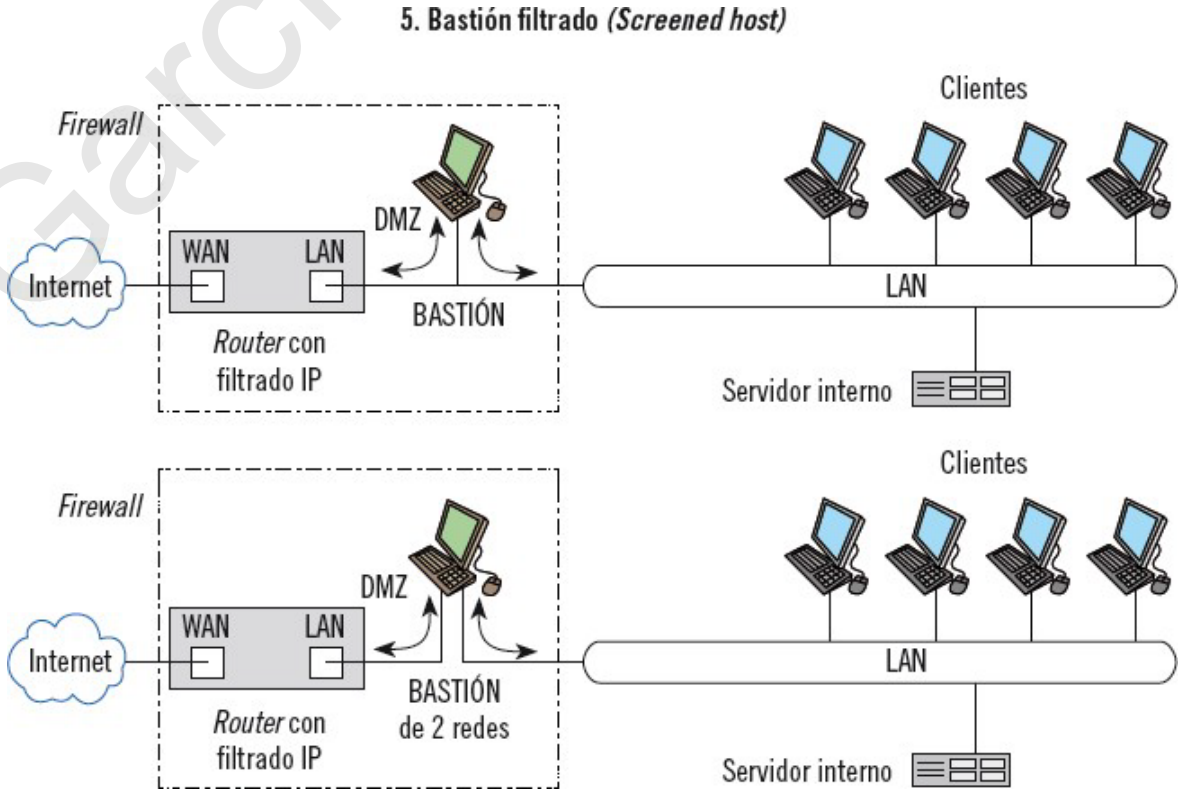
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Bastión Filtrado (Screened Host)

Zona Desmilitarizada (DMZ)

- La zona entre el router y el bastión se conoce como Zona Desmilitarizada (DMZ), actuando como una capa de seguridad adicional entre la red externa e interna.
- La DMZ proporciona una separación lógica o física entre las dos redes, dependiendo de si se emplea un bastión de una o dos redes.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Subred Filtrada (Screened Subnet)

La configuración de subred filtrada es la más segura, ya que separa el bastión de la red interna mediante un segundo equipo de filtrado de paquetes, como un router interno o un firewall dedicado.

Protección Adicional con Doble Filtrado

- En este diseño, el bastión se encuentra protegido por dos routers: uno externo y uno interno, creando zonas desmilitarizadas (DMZ) que pueden estar separadas lógica o físicamente.
- Esta configuración añade una capa adicional de seguridad, ya que incluso si un atacante compromete el bastión, aún necesitaría vulnerar el segundo router interno para obtener acceso completo a la red interna.

Configuración de los Routers

- El router exterior, generalmente proporcionado por el proveedor de servicios de internet (ISP), se configura para comunicarse solo con internet y el bastión.
- El router interior se configura para comunicarse únicamente con la red interna y el bastión, y ambos routers nunca deben comunicarse entre sí para mantener la seguridad del sistema.

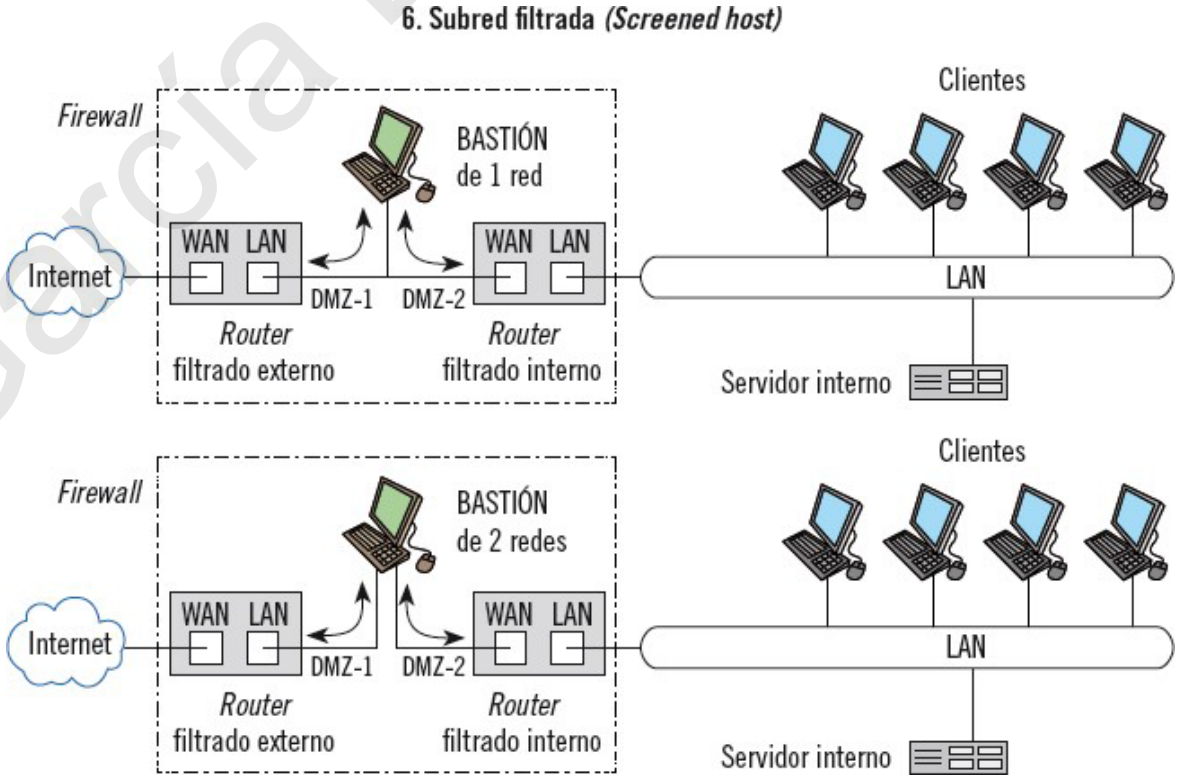
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Subred Filtrada (Screened Subnet)

Funciones del Bastión

- Tanto el router exterior como el interior proporcionan filtrado de paquetes IP, mientras que el bastión desactiva el enrutamiento directo de tráfico y puede ejecutar servicios de proxy según sea necesario para controlar el acceso a las aplicaciones.
- Esta configuración garantiza un control exhaustivo sobre el tráfico entrante y saliente, ofreciendo una sólida defensa contra posibles ataques externos.



Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

Implementar cortafuegos

Firewalls personales

- Los firewalls personales son aplicaciones de cortafuegos instaladas en cada ordenador conectado a la red, ya sea cliente o servidor.
- Aunque no tienen una función corporativa de protección, son esenciales para la seguridad individual de cada equipo y la red en su conjunto.

Importancia y Función

Activar los firewalls personales es fundamental, ya que dificultan la propagación de incidentes y proporcionan el primer nivel de defensa para cada dispositivo.

Las capacidades de procesamiento de los equipos modernos permiten que estos firewalls personales sean cada vez más potentes, incluyendo funciones avanzadas como prevención de intrusiones (IPS) y detección de intrusiones (IDS).

Funcionalidades Avanzadas

Los firewalls personales pueden integrar características de prevención de intrusiones (IPS), que bloquean activamente intentos de acceso no autorizados, y de detección de intrusiones (IDS), que monitorean y alertan sobre actividades sospechosas.

Estas funcionalidades mejoran significativamente la seguridad del sistema al proporcionar una defensa proactiva contra amenazas conocidas y desconocidas.

Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

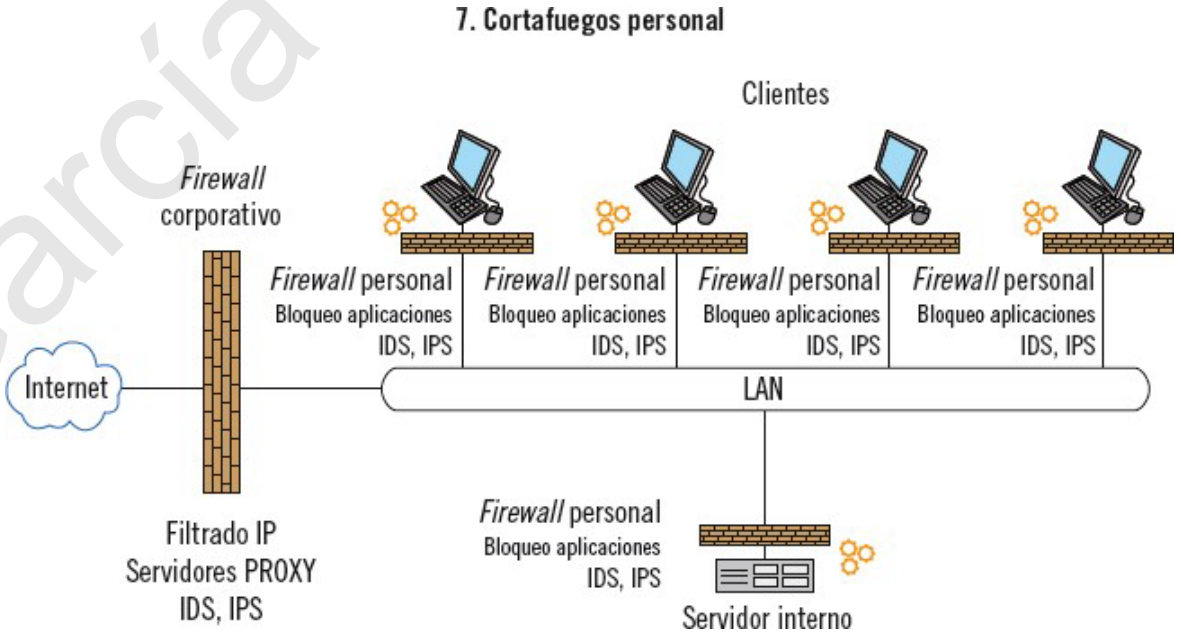
Implementar cortafuegos

Firewalls personales

Mejoras en la Seguridad

La implementación de firewalls personales ayuda a fortalecer la seguridad de la red en su conjunto al proteger cada dispositivo individualmente.

Es esencial educar a los usuarios sobre la importancia de mantener activos y actualizados los firewalls personales para garantizar una protección óptima contra las amenazas cibernéticas.



Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

Introducción

El uso de firewalls con dos dispositivos permite crear una subred entre ellos, llamada Zona Desmilitarizada (DMZ), que no pertenece ni a la red externa ni a la interna.

La norma ISO 27002 y el Esquema Nacional de Seguridad establecen la necesidad de segregar redes en subredes para proteger los servicios de información, usuarios y sistemas.

Implementación de la Segregación de Redes

- La segregación de redes se basa en una evaluación del riesgo y los requisitos de seguridad de cada dominio.
- Se recomienda dividir la red en dominios de red lógicos, protegidos por firewalls que controlan el acceso y flujo de información.

Criterios de Segregación de Redes

- Los criterios de segregación incluyen la política de control de accesos, el valor de la información, y la separación de diferentes áreas de negocio para reducir el impacto de incidentes.
- También se considera la separación de redes inalámbricas y el costo en términos materiales y de horas de trabajo para la monitorización de dispositivos.

Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

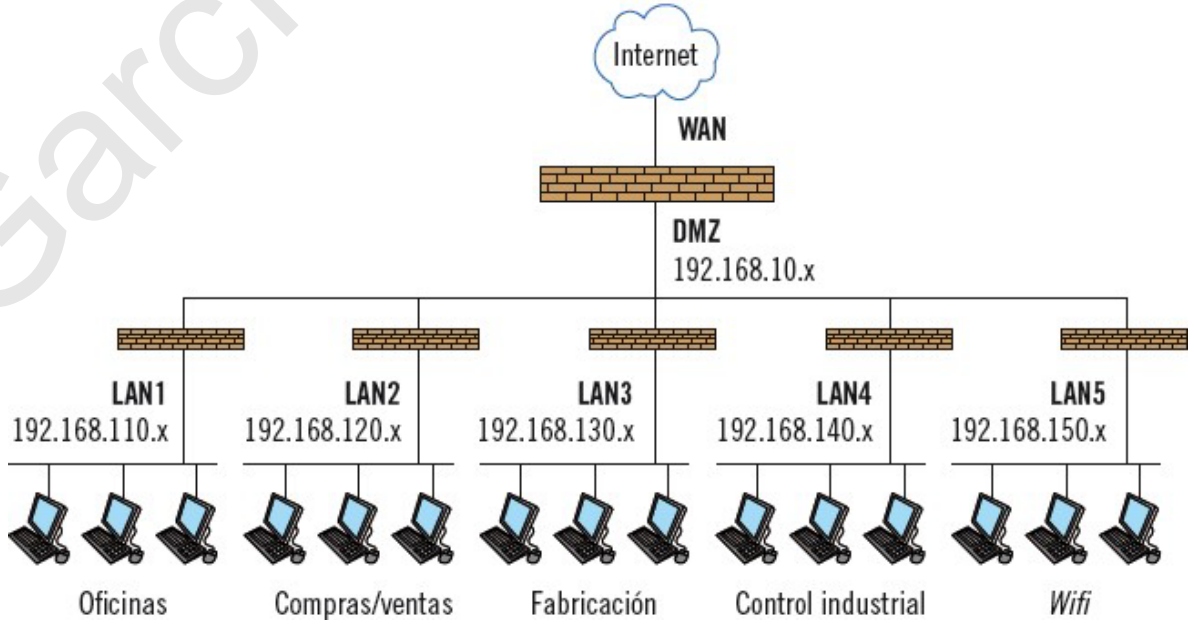
Introducción

Medidas de Seguridad

Además, se deben emplear medidas que garanticen el control de entrada y salida de usuarios y datos en cada segmento de red.

Los medios físicos y lógicos utilizados para la segmentación deben estar adecuadamente asegurados, mantenidos y monitorizados, como en el caso de los firewalls de acceso a internet.

Diferentes subredes separadas entre sí por cortafuegos, con diferentes rangos de direcciones IP



Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

Zonas desmilitarizadas

Uso de Zonas Desmilitarizadas (DMZ)

Las zonas DMZ aumentan la seguridad al aumentar la separación entre redes.

Emplean rangos de direcciones IP diferentes al de la red privada, lo que dificulta el acceso no autorizado a la red interna.

Se pueden obtener más beneficios de las zonas DMZ al emplearlas para diferentes servicios, aumentando así su utilidad y eficacia.

Redes Falsas o Honeypots

Las redes falsas, también conocidas como honeypots o redes señuelo, consisten en un conjunto de máquinas intencionadamente vulnerables que simulan una red privada normal.

Su propósito es engañar a los atacantes para que crean que han accedido a la red privada cuando en realidad están en una red controlada.

Es crucial construir estas redes con cuidado para evitar revelar su verdadera naturaleza al atacante.

Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

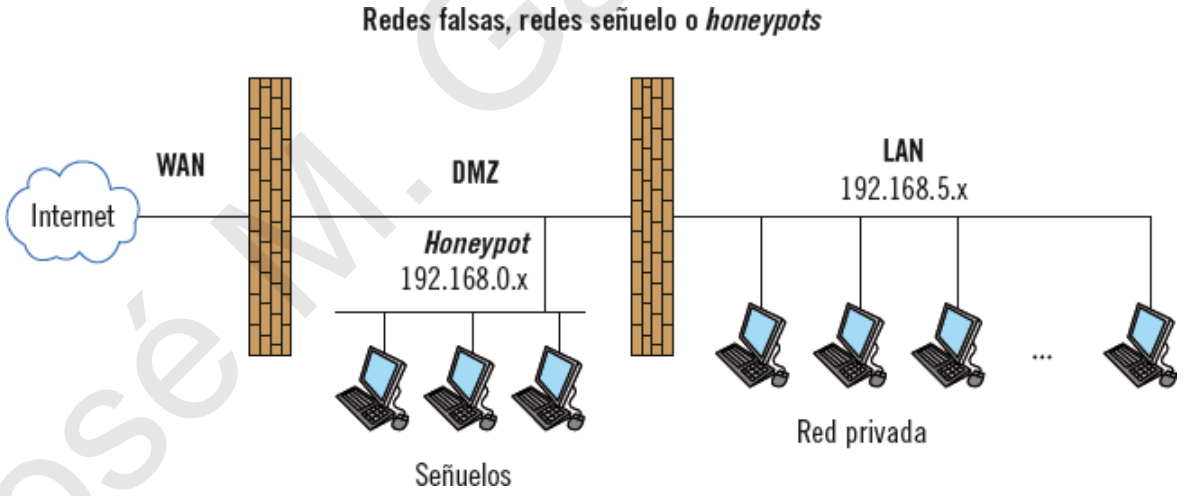
Zonas desmilitarizadas

Consideraciones sobre Honeypots

Para construir honeypots, a menudo se emplean máquinas obsoletas que simulen estar en producción.

El coste de mantenimiento es alto, ya que deben simular actividad diaria y apariencia realista para engañar a los atacantes.

Esta medida es más común en entornos de alta seguridad debido a su costo y complejidad.



Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

Zonas desmilitarizadas

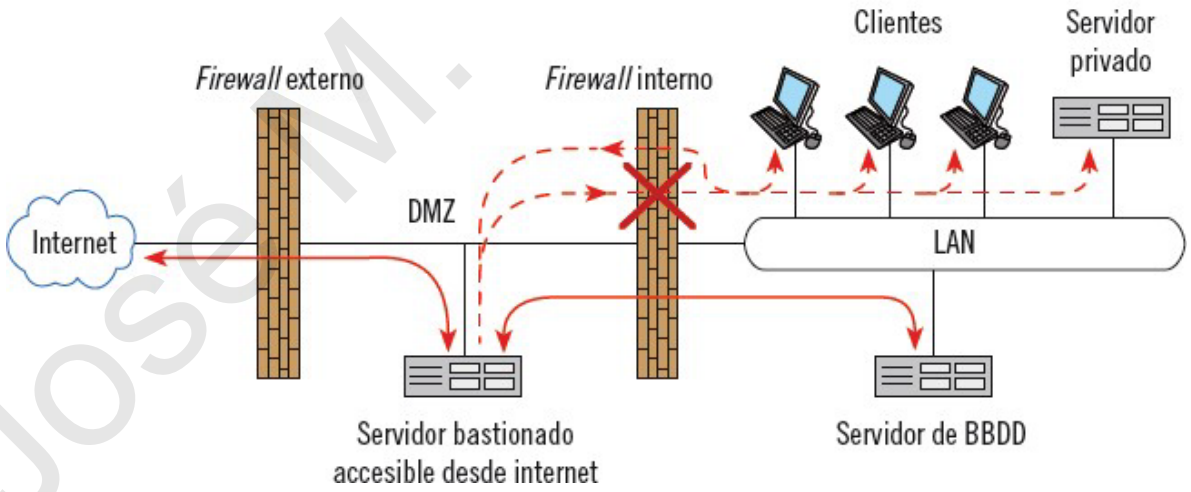
Ubicación de Servidores Accesibles desde el Exterior

Es crucial robustecer los servidores de aplicaciones accesibles desde el exterior para prevenir intrusiones.

Ubicar estos servidores en la red privada puede exponer toda la red a riesgos de seguridad si son comprometidos.

La mejor práctica es alojar los servidores accesibles desde internet en una zona DMZ para minimizar los riesgos y permitir un acceso controlado.

1. Servidor de aplicación bastionado en DMZ



Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ

Zonas desmilitarizadas

Ubicación de Servidores Accesibles desde el Exterior

Ventajas de la Zona DMZ

- La zona DMZ proporciona un entorno intermedio entre la red interna y el internet, permitiendo un acceso seguro a los servidores desde el exterior.
- El firewall externo se configura para dirigir los accesos a la aplicación exclusivamente al servidor correspondiente en la DMZ.
- El firewall interno se configura para permitir el acceso desde la red privada solo a los recursos necesarios en la DMZ, minimizando así los riesgos de seguridad.

Consideraciones Adicionales

- Aunque el servidor de la aplicación en la DMZ esté robustecido, persiste el riesgo de compromiso.
- En casos donde no sea posible ubicar el servidor en la DMZ, se puede emplear un proxy como sustituto para la aplicación.
- El uso de servidores proxy sigue el mismo principio de diseño que los bastiones host, proporcionando un acceso controlado desde internet a las aplicaciones.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Introducción

Utilización de Redes Privadas Virtuales (VPN)

- Las comunicaciones seguras entre sucursales pueden lograrse mediante diversas soluciones.
- Una opción costosa implica el uso de líneas de comunicación propiedad de la empresa o alquiladas a operadores de telecomunicaciones.
- La popularización de la banda ancha ha llevado al uso de VPN, que establecen conexiones seguras extremo a extremo a través de internet.

Beneficios de las VPN

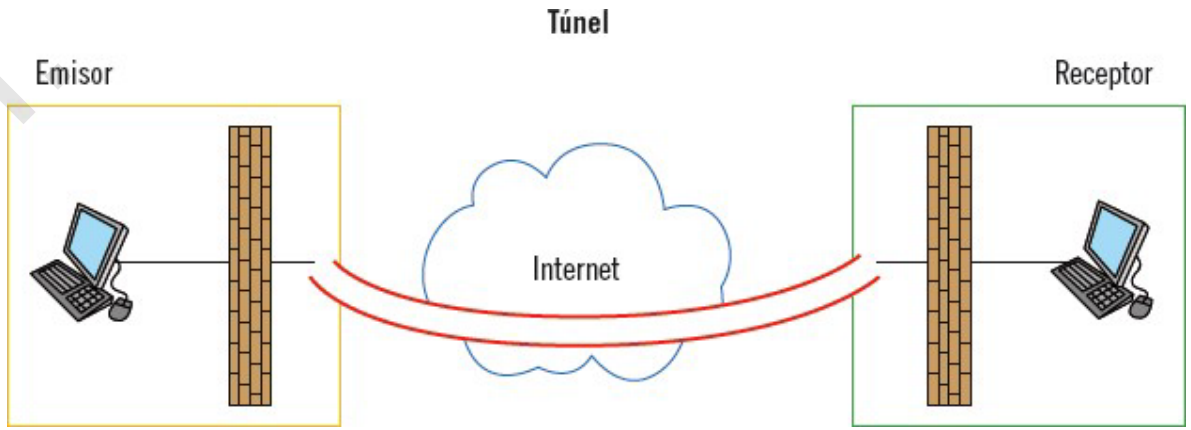
- Las VPN proporcionan conexiones seguras y rápidas, construyendo una red privada virtual sobre internet.
- Esto permite que las comunicaciones viajen protegidas como si estuvieran en un túnel aislado del resto de usuarios de internet.
- Las VPN pueden operar de manera transparente desde el cortafuegos de un extremo al cortafuegos del otro extremo, incluso dentro de la red interna o entre subredes.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Introducción

Protección de la Información en VPN

- Es crucial añadir medidas para proteger la información transmitida, especialmente en redes públicas como internet.
- Se deben considerar las salvaguardas una vez que el firewall entrega la información al proveedor de acceso a internet (ISP) para reducir el riesgo en el transporte por redes públicas.
- Las VPN pueden ofrecer comunicaciones protegidas mediante túneles, aunque es importante entender las diferencias entre túneles completos y divididos para una protección óptima (¿Cuáles son?)



Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Ataques de introducción y de fabricación

Los ataques de interrupción y los ataques de fabricación son dos tipos de ataques que tienen como objetivo afectar la disponibilidad y la integridad de los sistemas de información y las redes.

Ataques de Interrupción:

Objetivo: o bloquear el acceso a los recursos de una red o sistema, impidiendo que los usuarios legítimos utilicen los servicios.

Métodos: Estos ataques suelen lograrse mediante el envío masivo de tráfico malicioso a los servidores o dispositivos objetivo, lo que puede saturar los recursos de red, agotar el ancho de banda disponible o sobrecargar los sistemas hasta el punto de que dejen de funcionar correctamente.

Ejemplos: Algunos ejemplos de ataques de interrupción incluyen ataques de denegación de servicio (DoS), en los que se envían grandes volúmenes de tráfico falso a un servidor o red para sobrecargarlos, y ataques de denegación de servicio distribuido (DDoS), en los que múltiples dispositivos comprometidos se utilizan para lanzar un ataque coordinado.

Frente a ataques de interrupción, se emplea redundancia en el servicio, con al menos dos conexiones a internet por medios físicos diferentes para evitar aislamientos.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Ataques de introducción y de fabricación

Los ataques de interrupción y los ataques de fabricación son dos tipos de ataques que tienen como objetivo afectar la disponibilidad y la integridad de los sistemas de información y las redes.

Ataques de Fabricación:

Objetivo: manipular o alterar los datos que fluyen a través de una red, introduciendo información falsa o maliciosa en los paquetes de datos normales.

Métodos: Estos ataques suelen lograrse mediante la inserción de paquetes de datos manipulados en el flujo de tráfico normal de la red. Estos paquetes pueden estar diseñados para explotar vulnerabilidades en los sistemas receptores, causar mal funcionamiento en los dispositivos de red o comprometer la integridad de los datos transmitidos.

Ejemplos: Algunos ejemplos de ataques de fabricación incluyen ataques de inyección de paquetes, en los que se insertan paquetes maliciosos en la comunicación entre dos sistemas para comprometer la seguridad o el funcionamiento de uno o ambos sistemas, y ataques de suplantación de identidad, en los que se falsifica la información de origen de los paquetes para hacer que parezcan legítimos y confiables.

Ante ataques de fabricación, se refuerzan los elementos de red intermedios y equipos de seguridad perimetral para detectar intentos de denegación de servicio.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Ataques de introducción y de fabricación

Medidas de Seguridad

- Redundancia en el servicio: Al menos dos conexiones a internet de proveedores diferentes.
- Refuerzo de la seguridad perimetral: Capacidades para detectar envíos masivos de paquetes idénticos o ligeramente modificados.
- Funciones de balanceo de carga: Cortafuegos perimetrales permiten la conexión de múltiples redes WAN con balanceo de carga para distribuir el tráfico de manera equilibrada.

Beneficios del Balanceo de Carga

- Mejora la disponibilidad y el rendimiento de las conexiones a internet.
- En condiciones normales, equilibra el tráfico entre las diferentes salidas WAN, aprovechando las velocidades de conexión de cada proveedor.
- Detecta automáticamente fallos y redistribuye el tráfico entre las salidas WAN disponibles para garantizar la continuidad del servicio.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Ataques de interceptación y ataque de modificación

Son dos tipos de ataques cibernéticos que tienen como objetivo comprometer la confidencialidad e integridad de la información transmitida a través de redes.

Ataques de Interceptación:

- Objetivo: El objetivo principal de los ataques de interceptación es obtener acceso no autorizado a la información confidencial que se transmite a través de una red.
- Métodos: Estos ataques se llevan a cabo mediante la captura y el monitoreo del tráfico de red, con el fin de obtener datos sensibles, como contraseñas, información financiera, correos electrónicos o cualquier otra información confidencial transmitida sin cifrar.
- Técnicas: Los atacantes pueden utilizar diversas técnicas para interceptar el tráfico de red, como el uso de programas de sniffing (captura de paquetes), el acceso a puntos de acceso Wi-Fi no seguros, la explotación de vulnerabilidades en dispositivos de red, o incluso la instalación de dispositivos de escucha físicos en la infraestructura de red.
- Ejemplos: Algunos ejemplos de ataques de interceptación incluyen el espionaje de redes Wi-Fi no seguras para capturar datos transmitidos por usuarios desprevenidos, la captura de contraseñas mediante programas de sniffing instalados en redes corporativas, y el uso de malware para interceptar datos confidenciales transmitidos a través de Internet.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Ataques de interceptación y ataque de modificación

Ataques de Modificación:

- Objetivo: Los ataques de modificación tienen como objetivo alterar o modificar la información transmitida a través de una red, con el fin de manipular su contenido o comprometer la integridad de los datos.
- Métodos: Estos ataques se llevan a cabo mediante la manipulación de los paquetes de datos mientras viajan a través de la red, con el fin de cambiar su contenido, insertar información falsa o eliminar datos importantes.
- Técnicas: Los atacantes pueden utilizar técnicas como la inyección de código malicioso en el tráfico de red, la alteración de los parámetros de las solicitudes HTTP, la modificación de archivos descargados en tránsito, o incluso la suplantación de identidad para modificar el origen o destino de los datos transmitidos.
- Ejemplos: Algunos ejemplos de ataques de modificación incluyen la modificación de páginas web para incluir contenido malicioso o engañoso, la alteración de archivos descargados para incluir malware, y la manipulación de datos en tránsito para cambiar las transacciones financieras o comprometer la integridad de los datos sensibles.

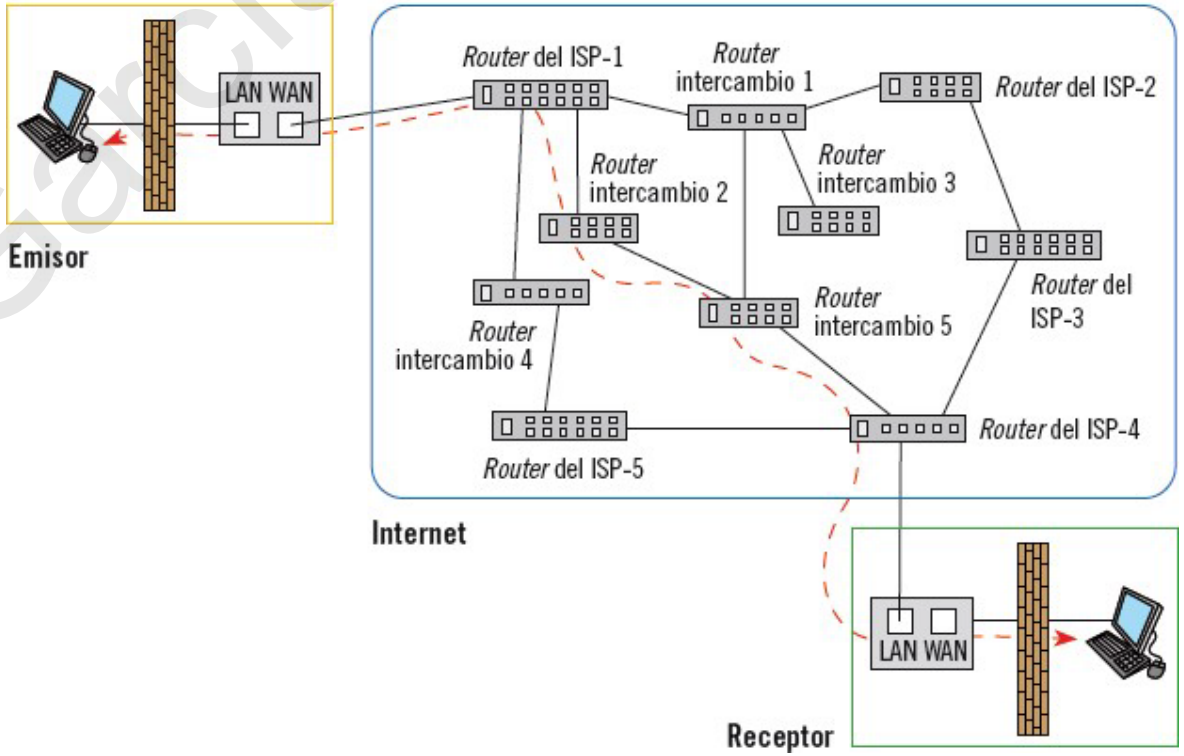
Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Criptografía en comunicaciones TCP/IP

En las comunicaciones TCP/IP, los datos se transmiten a través de una serie de nodos intermedios, como encaminadores o routers, que dirigen los paquetes hacia su destino final basándose en las direcciones IP.

La criptografía desempeña un papel crucial en la protección de la confidencialidad y la integridad de los datos durante su transmisión a través de Internet.

Ruta seguida por una comunicación emisor–receptor en la que intervienen 6 *router*



Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Criptografía en comunicaciones TCP/IP

Cuando se emplean métodos criptográficos para cifrar los paquetes IP, pueden surgir dos escenarios diferentes dependiendo de cómo se manejen las direcciones IP:

- Direcciones IP no encriptadas: En este caso, las direcciones IP no están cifradas y son legibles para los nodos intermedios a lo largo del camino de transmisión. Cifrado extremo a extreno
- Direcciones IP encriptadas: Aquí, las direcciones IP están cifradas, lo que plantea desafíos adicionales para los nodos intermedios en términos de enrutamiento de los paquetes. Cifrado nodo a nodo

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

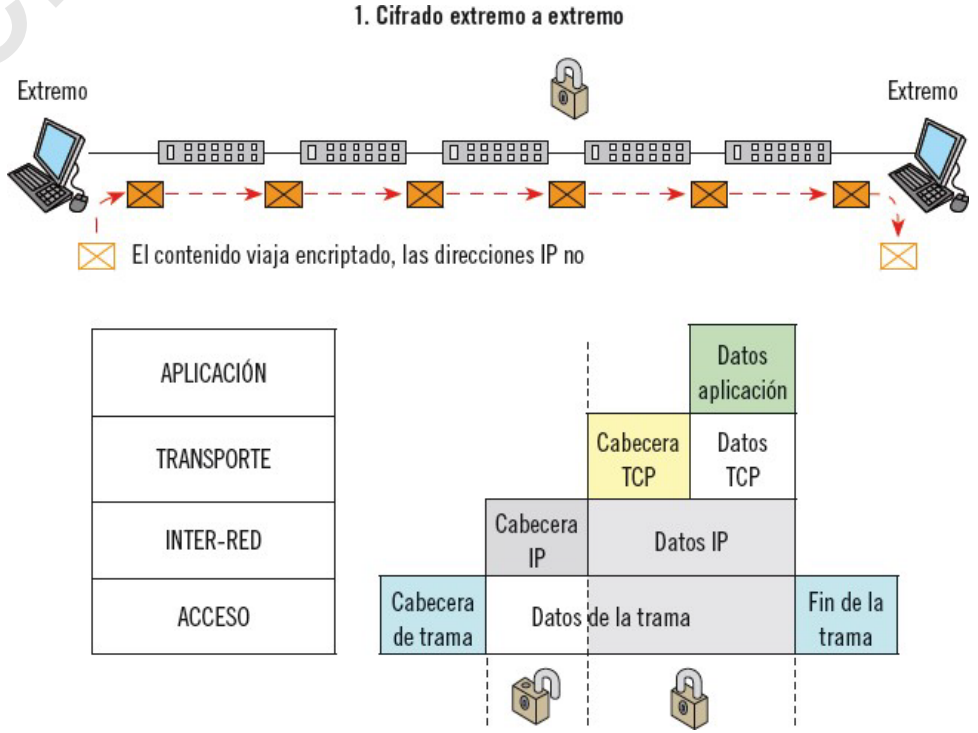
Criptografía en comunicaciones TCP/IP

Direcciones IP no encriptadas: En este caso, las direcciones IP no están cifradas y son legibles para los nodos intermedios a lo largo del camino de transmisión. Cifrado extremo a extreno

En el cifrado extremo a extremo, se protege únicamente la parte de datos del paquete en el nivel 3 del modelo OSI.

Las direcciones IP del emisor y del receptor no se cifran, lo que significa que son accesibles para cualquier nodo intermedio en la ruta de transmisión.

Aunque la información de los datos del paquete esté protegida, la revelación de las direcciones IP puede proporcionar información valiosa a un atacante sobre las partes involucradas en la comunicación y sus hábitos de uso.



Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

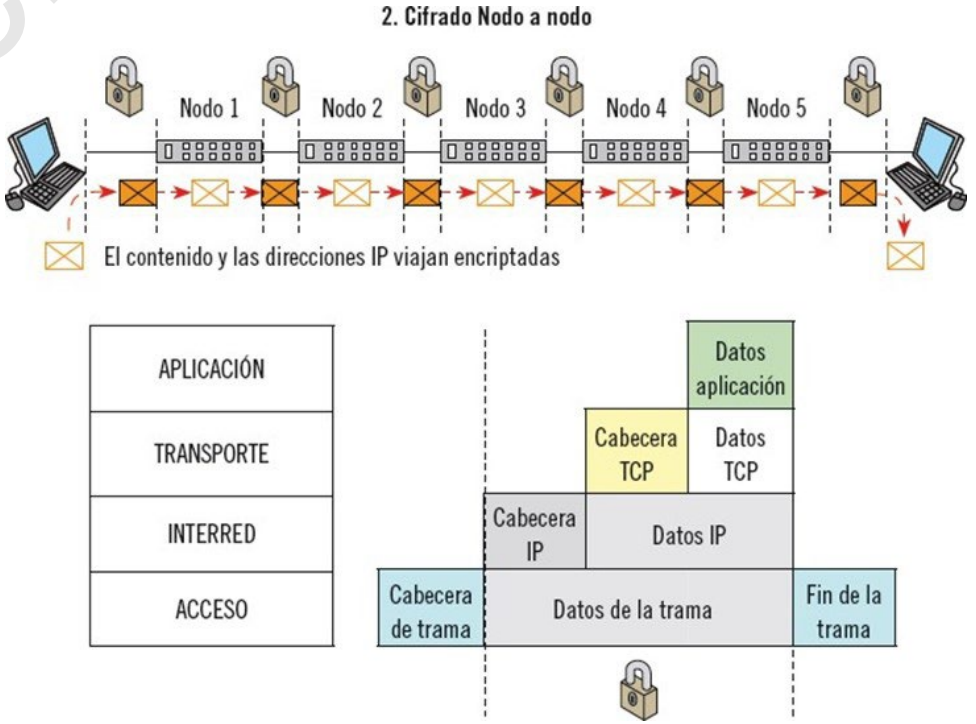
Criptografía en comunicaciones TCP/IP

Direcciones IP encriptadas: Aquí, las direcciones IP están cifradas, lo que plantea desafíos adicionales para los nodos intermedios en términos de enrutamiento de los paquetes. Cifrado nodo a nodo

En el cifrado nodo a nodo, todas las direcciones IP, así como los datos del paquete, se cifran antes de ser transmitidos.

Esto significa que cada nodo intermedio debe ser capaz de desencriptar y volver a encriptar los paquetes para poder enrutarlos correctamente.

Sin embargo, esto puede ser un desafío, ya que todos los nodos intermedios deben ser compatibles con el mismo método de cifrado para garantizar la transmisión adecuada de los datos.



Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

Las redes privadas virtuales (VPN) son herramientas fundamentales para garantizar conexiones seguras a través de redes públicas, como internet. Funcionan mediante la combinación de técnicas de cifrado, autenticación y encapsulación de datos para crear un túnel seguro entre el cliente y el servidor VPN, permitiendo así la transmisión segura de información.

Los componentes básicos de una VPN son el cliente VPN y el servidor VPN, los cuales deben utilizar el mismo protocolo VPN para establecer la conexión segura.

Existen dos tipos principales de VPN:

- las VPN sitio a sitio, que conectan diferentes ubicaciones de una misma empresa
- VPN de acceso remoto, que permiten a los usuarios acceder a la red privada desde ubicaciones externas.

Sin embargo, el uso de VPN también presenta algunas desventajas, como la posible pérdida de rendimiento debido al cifrado de datos y la encapsulación de protocolos, así como la introducción de nuevas vulnerabilidades. Por ejemplo, en el caso de las VPN de acceso remoto, el traslado de equipos a ubicaciones externas puede exponerlos a riesgos adicionales.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

Para establecer una VPN, es fundamental utilizar un protocolo VPN compatible en ambos extremos de la conexión.

Los protocolos más comunes son IPsec (Internet Protocol Security) y SSL/TLS (Secure Sockets Layer/Transport Layer Security), que operan en las capas 3 y 4 del modelo OSI, respectivamente.

También existen otros protocolos, como OpenVPN y SOCKS, que actúan en capas superiores, pero podrían dejar cierta información sin protección en caso de interceptación.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

IPsec (Protocolo de seguridad de Internet)

- Estándar para VPNs seguras.
- Proporciona autenticación, integridad de datos y confidencialidad.
- Opera en la capa de red (capa 3) del modelo OSI.
- Utiliza dos protocolos principales: AH (Authentication Header) y ESP (Encapsulating Security Payload).

SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- Originalmente diseñado para seguridad en navegadores web.
- Opera en la capa de aplicación (capa 7) del modelo OSI.
- Proporciona autenticación, integridad y confidencialidad de datos.
- Comúnmente utilizado en VPNs de acceso remoto y VPNs basadas en navegador.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

PPTP (Point-to-Point Tunneling Protocol):

- Uno de los primeros protocolos VPN desarrollados.
- Fácil de configurar y ampliamente compatible.
- Sin embargo, su seguridad se considera relativamente débil y puede ser vulnerable a ataques.

L2TP/IPsec (Layer 2 Tunneling Protocol/IPsec):

- Combina la simplicidad de PPTP con la seguridad de IPsec.
- Proporciona cifrado y autenticación de alto nivel.
- Utilizado principalmente en conexiones de sitio a sitio y en entornos corporativos.

OpenVPN:

- Un protocolo de VPN de código abierto y altamente configurable.
- Utiliza tecnologías SSL/TLS para asegurar las conexiones.
- Compatible con una variedad de sistemas operativos y dispositivos.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

SSTP (Secure Socket Tunneling Protocol):

- Desarrollado por Microsoft y compatible con Windows Vista y versiones posteriores.
- Utiliza SSL/TLS para cifrar los datos transmitidos.
- Es una opción popular para conexiones de VPN en entornos Windows.

WireGuard:

- Un protocolo VPN de última generación diseñado para ser más rápido, más simple y más eficiente que otros protocolos.
- Utiliza tecnologías modernas y está integrado en el núcleo del sistema operativo en algunos casos, lo que lo hace muy rápido y ligero.
- Aunque relativamente nuevo, está ganando popularidad debido a su rendimiento y facilidad de configuración.

IKEv2 (Internet Key Exchange version 2):

- Un protocolo de VPN seguro y robusto que se utiliza ampliamente en dispositivos móviles.
- Proporciona una conexión estable y rápida, especialmente en redes móviles, y es capaz de recuperarse rápidamente de interrupciones de conexión.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Protocolos VPN

SoftEther VPN:

- Una solución VPN multi-protocolo y de código abierto que admite múltiples protocolos, incluidos SSL, IPsec, L2TP, y OpenVPN.
- Ofrece flexibilidad y escalabilidad, lo que lo hace adecuado para una variedad de aplicaciones, desde el uso doméstico hasta entornos empresariales.

Utilización de redes privadas virtuales / VPN para establecer canales seguros de comunicaciones

Recomendaciones uso VPN

- La Norma ISO 27002 recomienda el uso de redes privadas virtuales como medida técnica.
- Los protocolos VPN ofrecen autenticación del usuario o de la máquina, lo que aumenta la seguridad.

Control "13.1.3 Segregación en redes"

- Sugiere emplear VPN para segregar en dominios lógicos separados la red.
- Se puede restringir el acceso a la red utilizando VPN para grupos de usuarios dentro de la organización.

Esquema Nacional de Seguridad

- Promueve el uso de redes privadas virtuales para proteger la confidencialidad de las comunicaciones.
- Especialmente cuando las comunicaciones discurren por redes externas al dominio de seguridad de la organización.

Definición de reglas de corte en los cortafuegos

Introducción

Las reglas de corte se definen desde una perspectiva de "todo prohibido", donde se habilitan exclusivamente los flujos de tráfico permitidos.

Es un diseño habitual para un control de acceso lógico adecuado, similar a otros contextos donde se requiere un control de acceso.

Tipos de reglas de tráfico

- Reglas de tráfico entrante (incoming): Filtran el tráfico que viene desde internet hacia la red privada.
- Reglas de tráfico saliente (outgoing): Filtran el tráfico que va desde la red privada hacia internet.

Funcionamiento del firewall

- El firewall tiene al menos dos interfaces de red: una para la conexión a internet (WAN) y otra para la red privada (LAN).
- Aplica reglas de tráfico entrante cuando recibe un paquete desde internet hacia la red privada, y reglas de tráfico saliente cuando recibe un paquete desde la red privada hacia internet.
- Identifica origen y destino del paquete observando las direcciones IP del mismo.

Definición de reglas de corte en los cortafuegos

Introducción

Componentes de una regla

- Protocolo de transporte: TCP o UDP.
- Puerto de comunicaciones: Identifica la aplicación.
- Dirección IP origen y destino: Quién origina y a quién va destinado el paquete.
- Acción: Permitido o prohibido.

Protocolo	Puerto	IP Origen	IP Destino	Acción
TCP, UDP	*	*	*	prohibir
TCP	80	*	84.122.10.15	permitir

Ejemplo: reglas entrantes para permitir exclusivamente el acceso a un servidor web interno, cuya dirección IP pública accesible es 84.122.10.15

Definición de reglas de corte en los cortafuegos

Introducción

Protocolo	Puerto	IP Origen	IP Destino	Acción
TCP, UDP	*	*	*	prohibir
TCP	25	192.168.10.23	*	permitir

Ejemplo: reglas salientes para permitir exclusivamente que un servidor de correo con dirección IP 192.168.10.23 pueda enviar correo al exterior

Definición de reglas de corte en los cortafuegos

Introducción

Para gestionar diferentes subredes, se pueden definir reglas de acceso entre ellas utilizando direcciones origen y destino adecuadas.

Las direcciones deben ser del rango de direcciones al que pertenece el interfaz de red de cada una de esas subredes.

Acciones para prohibir el tráfico

Dependiendo del firewall, puede haber dos opciones al rechazar un paquete:

- Informar al remitente de que ha sido rechazado.
- Simplemente no responder al paquete.

Definición de reglas de corte en los cortafuegos

Introducción

Desde el punto de vista de la seguridad, esta distinción es relevante (informar o no responder) y tiene implicaciones en la protección contra ataques de denegación de servicio (DoS):

- Informar puede revelar información sobre la configuración y la topología de la red interna, lo que podría ser aprovechado por un atacante para planificar futuros ataques.
- Prevención de ataques: Si el firewall informa al remitente de que sus paquetes son rechazados, un atacante podría utilizar esta información para lanzar un ataque de denegación de servicio (DoS) inundando el firewall con un gran número de paquetes, lo que podría saturar la conexión a internet.
- Eficiencia: No responder a los paquetes prohibidos puede ayudar a evitar el desperdicio de recursos del firewall en el procesamiento de paquetes maliciosos. Si el firewall simplemente desprecia los paquetes prohibidos, puede enfocarse en gestionar el tráfico legítimo de manera más eficiente.

Definición de reglas de corte en los cortafuegos

Introducción

Ataques de denegación de servicio (DoS)

- Un ataque de denegación de servicio busca eliminar la disponibilidad de un servicio o recurso para los usuarios autorizados.
- Conlleva la ocupación total de recursos de procesamiento, almacenamiento y capacidad de comunicaciones.

Informar / no responder

Ataque DoS dirigido al firewall:

- Si el firewall informa al remitente de paquetes rechazados, un atacante podría inundar el firewall con peticiones para saturar su conexión a internet.
- Si el firewall simplemente desprecia los paquetes entrantes prohibidos, el atacante tendría más dificultades para progresar en el sistema.

Relación de los registros de auditoría del cortafuegos, necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Definición de reglas de corte en los cortafuegos

- Las reglas de corte se establecen desde una perspectiva de "todo prohibido" para luego habilitar exclusivamente los flujos de tráfico permitidos.
- Existen reglas de tráfico entrante (incoming) y reglas de tráfico saliente (outgoing).
- Se deben tener al menos dos interfaces de red: una para la conexión a internet o red WAN, y otra para la conexión a la red privada o red LAN.
- Las reglas incluyen varias condiciones como el protocolo de transporte (TCP o UDP), el puerto de comunicaciones, la dirección IP origen y destino, y la acción (permitido o prohibido).
- Es relevante decidir si el firewall debe informar al remitente de paquetes rechazados o simplemente no responder.
- Las acciones de prohibición pueden implicar informar al remitente o no responder, y esta distinción es relevante desde el punto de vista de la seguridad y la prevención de ataques de denegación de servicio (DoS).

Relación de los registros de auditoría del cortafuegos, necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Recomendaciones para la gestión de registros en el cortafuegos

- La norma ISO 27002 establece la necesidad de registrar y monitorizar el funcionamiento de los equipos de seguridad perimetral, como los cortafuegos.
- Se deben mantener registros de eventos clave como el inicio y fin de conexiones, cambios en la configuración del cortafuegos, activación o desactivación de funcionalidades de seguridad, entre otros.
- También es importante registrar las actividades de usuarios con privilegios, los fallos del equipo, y proteger los registros para mantener su confidencialidad e integridad.
- Es fundamental controlar las alteraciones en los archivos de registros, garantizar la disponibilidad de espacio de almacenamiento, y considerar la conservación de copias de seguridad de los registros.
- La sincronización de los relojes es esencial para garantizar la precisión de los registros y su trazabilidad en eventos. Todos los equipos de la red privada deben sincronizar su hora con una misma referencia, como un servidor de tiempo en internet mediante el protocolo NTP o PTP.

Establecimiento de la monitorización y pruebas del cortafuegos

El proceso de aseguramiento de la red mediante la monitorización y pruebas del cortafuegos es esencial para protegerla de las amenazas de internet. Este enfoque se apoya en directrices del Esquema Nacional de Seguridad y la norma ISO 27002, que subrayan la necesidad de medidas de vigilancia efectivas.

Es crucial contar con un procedimiento formal de monitorización del cortafuegos, que se integre dentro de las políticas de seguridad de la empresa y se adapte a los riesgos en constante cambio. Asignar recursos adecuados basados en una evaluación exhaustiva de riesgos es esencial, considerando aspectos como la criticidad de los procesos y el valor de la información.

La monitorización debe abarcar varios aspectos, incluidos accesos autorizados y no autorizados, operaciones privilegiadas, cambios de configuración y fallos del equipo. Se recomienda el uso de herramientas de código libre para realizar pruebas de intrusión controlada y complementar la monitorización en tiempo real con análisis de red y escaneo de puertos.

Es importante destacar la posibilidad de errores en la configuración del cortafuegos o accesos no autorizados desconocidos, lo que subraya la necesidad de verificaciones regulares y exhaustivas. Herramientas como ftester pueden ser utilizadas para realizar pruebas de inyección de paquetes y confirmar el correcto funcionamiento del cortafuegos, garantizando así una respuesta adecuada ante situaciones de ataque.

Resumen

Para proteger la red de una empresa de las amenazas de internet, se emplean cortafuegos o fírewalls en los puntos de interconexión. Estos pueden ser de filtrado de paquetes o de aplicación, como servidores proxy.

Los diseños varían desde simples routers hasta subredes filtradas con zonas desmilitarizadas (DMZ).

Los cortafuegos controlan el acceso entre la red privada e internet, pero surgen problemas de acceso a la información desde internet o desde la propia red privada.

Las redes privadas virtuales (VPN) se utilizan para establecer conexiones seguras entre emisor y receptor mediante autenticación y encriptación. Los protocolos VPN más comunes son PPTP, L2TP e IPsec.

La combinación de cortafuegos y VPN ayuda a separar la LAN de internet o subredes internas, asegurando los activos de la empresa.

Es crucial monitorear su eficacia y rendimiento mediante registros de auditoría y verificaciones regulares.