

Defensa de la red

Objetivos

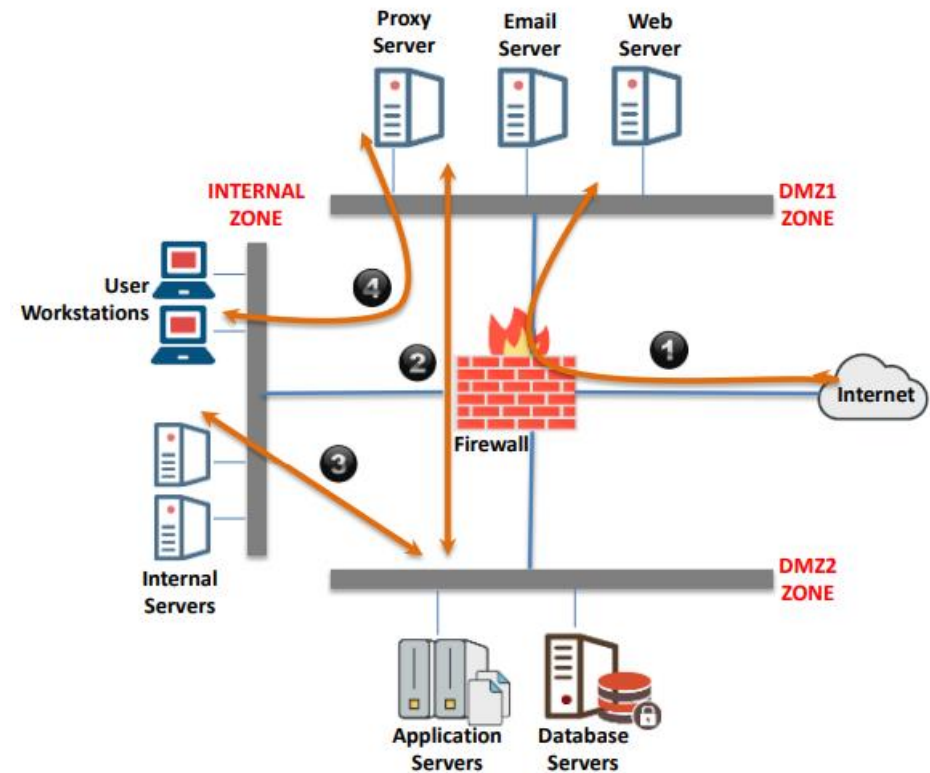
- ❑ Comprensión de la segmentación de red y sus tipos
- ❑ Comprensión de los distintos tipos de cortafuegos y sus funciones
- ❑ Comprensión de los distintos tipos de IDS/IPS y sus funciones Descripción general de los distintos tipos de Honeypots
- ❑ Diferentes tipos de servidores proxy y sus ventajas
- ❑ Comprender los fundamentos de las redes privadas virtuales (VPN) y su importancia en Seguridad de las redes
- ❑ Descripción general de la gestión de incidentes y eventos de seguridad (SIEM) y del análisis del comportamiento de los usuarios (UBA) Descripción general de diversos programas antivirus y antimalware

Comprender los distintos tipos de segmentación de la red

- La segmentación de la red mejora la seguridad de la red creando capas de la red y separando los servidores que contienen información sensible del resto de servidores.
- El objetivo de esta sección es explicar el papel de la segmentación de la red en la seguridad de la misma.

¿Qué es la segmentación de redes?

- La segmentación de red es la práctica de dividir una red en segmentos de red más pequeños y separar grupos de sistemas o aplicaciones entre sí
- En una red segmentada, los grupos de sistemas o aplicaciones que no interactúan entre sí se colocarán en un segmento de red diferente
- Ventajas de seguridad de la segmentación de redes
 - ✓ Seguridad mejorada
 - ✓ Mejor control de acceso
 - ✓ Mejora de la supervisión
 - ✓ Mejora del rendimiento



Ventajas de seguridad de la segmentación de la red

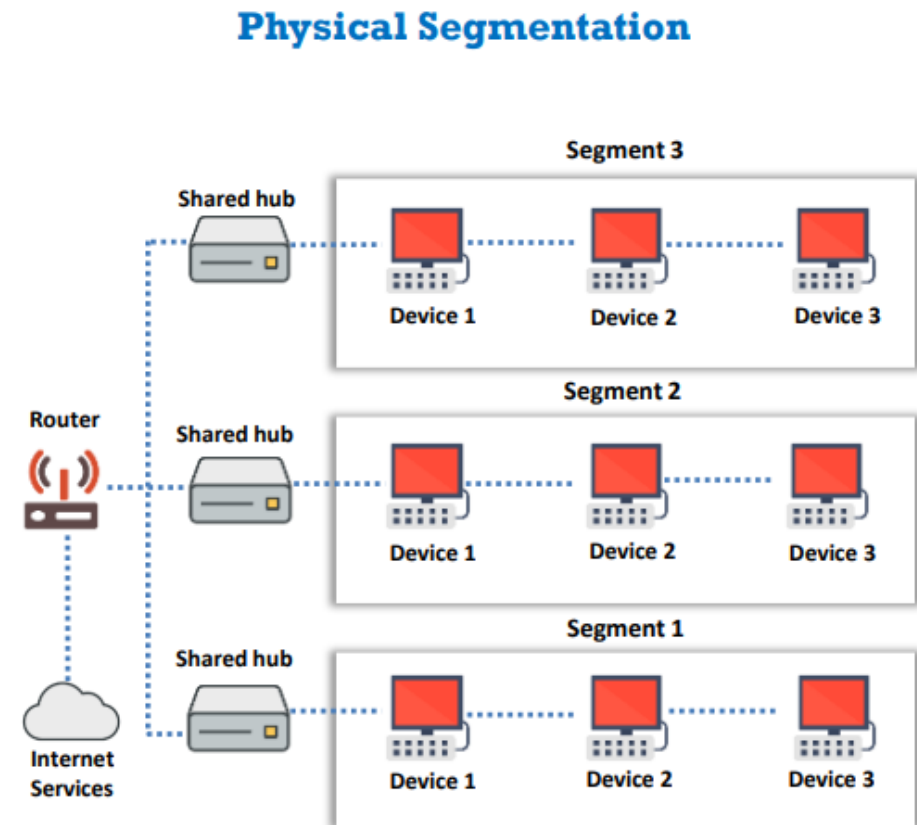
- **Mayor seguridad:** Aísla el tráfico de red para impedir el acceso entre segmentos de red.
- **Mejor control de acceso:** Permite acceder a recursos específicos de la red.
- **Monitorización mejorada:** Proporciona registro de eventos, monitorización y denegación de conexiones internas y detección de acciones maliciosas.
- **Mejora del rendimiento:** Reduce el tráfico local, con menos hosts por subred, y aísla el tráfico de difusión a la subred local.
- **Mejor contención:** Limita los problemas de red que puedan producirse a la subred local.

Tipos de segmentación de la red

La segmentación física es un proceso de división de una red de mayor tamaño en componentes

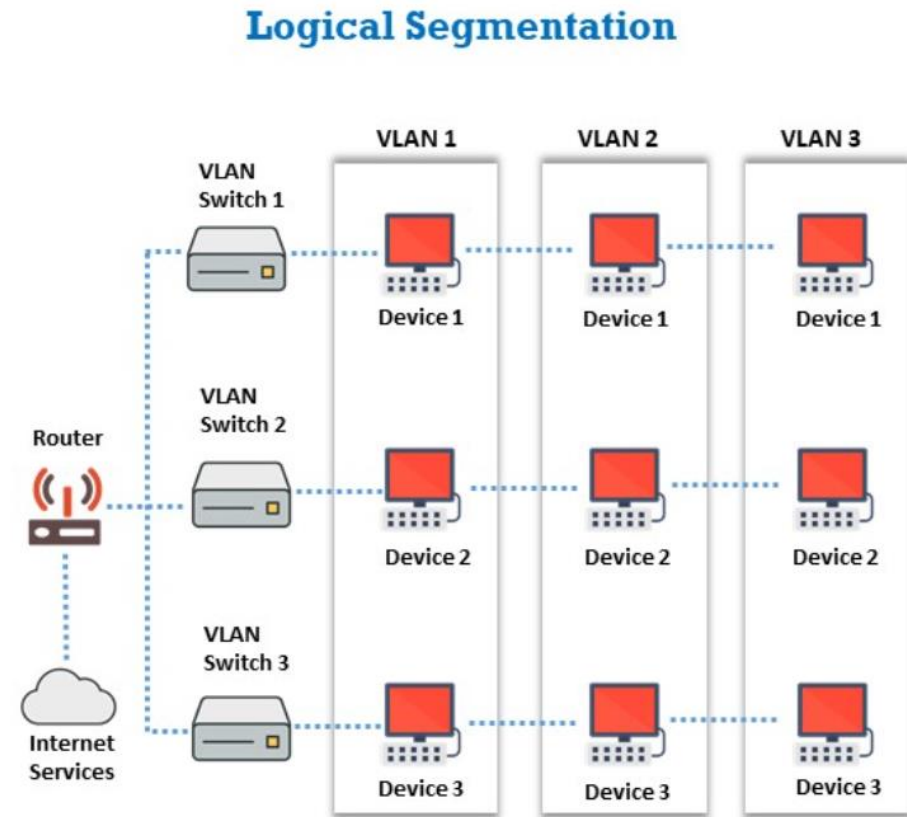
Estos segmentos pueden comunicarse a través de dispositivos intermediarios como conmutadores, concentradores, o enrutadores

La segmentación física de la red puede ser el enfoque para dividir una red, pero es caro porque ocupa más espacio



Tipos de segmentación de la red

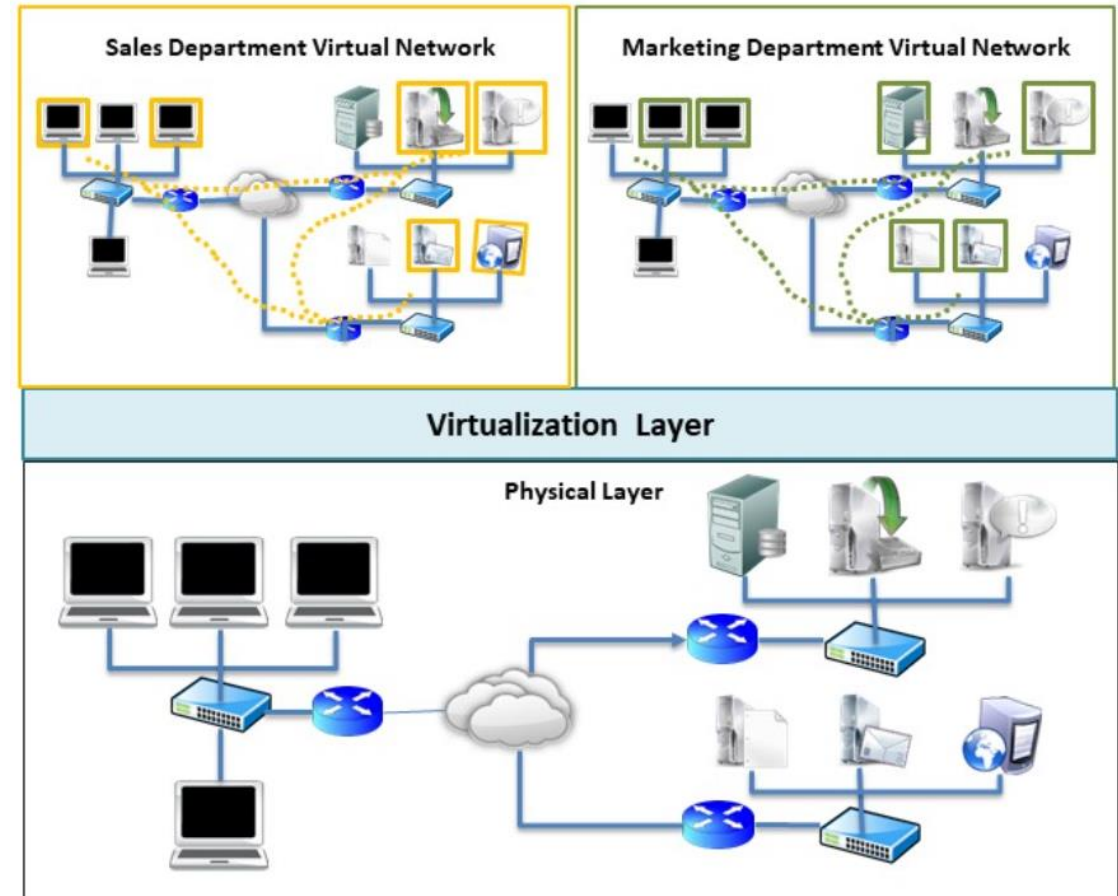
- ❑ La segmentación lógica utiliza VLAN, que son aislada lógicamente sin tener en cuenta la ubicación de los dispositivos
- ❑ Cada VLAN se considera una red lógica independiente y los dispositivos dentro de una VLAN se comunican como si estuvieran en su propia red aislada
- ❑ En este enfoque, los cortafuegos son compartidos y Los conmutadores gestionan la infraestructura VLAN
- ❑ Es más fácil de aplicar y flexible



Tipos de segmentación de la red

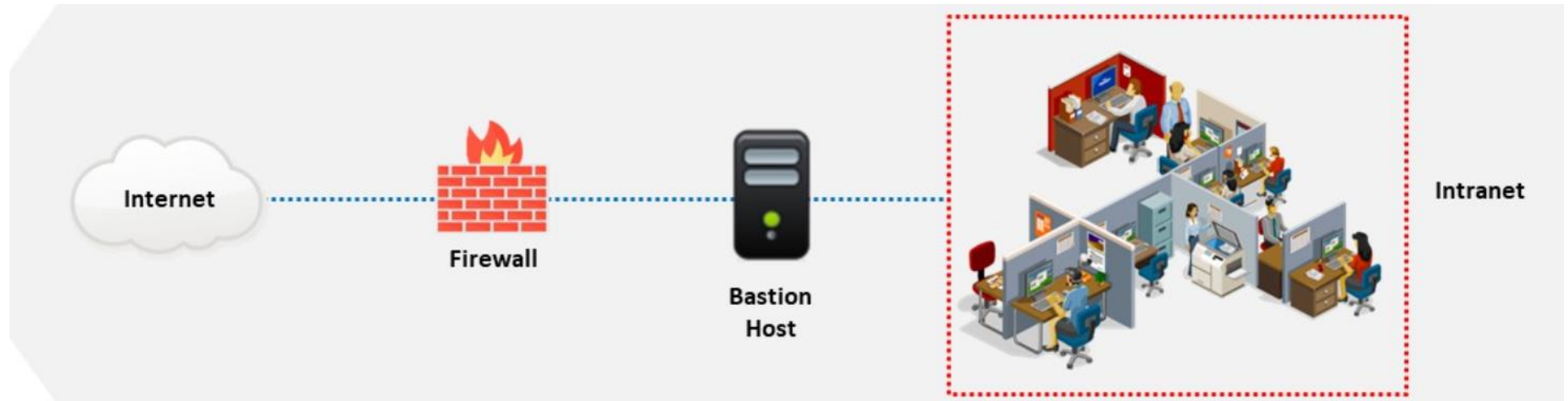
Virtualización de redes

- La virtualización de la red es un proceso que combina todos los recursos de red disponibles y permite a los profesionales de la seguridad compartir estos recursos entre los usuarios de la red mediante una **única unidad administrativa**.
- La virtualización de redes permite a cada usuario acceder desde su sistema a los recursos de red disponibles, como archivos, carpetas, ordenadores, impresoras, discos duros, etc.



Introducción a Bastionado de Host

1. Un host bastión es un sistema informático diseñado y configurado para **proteger los recursos de la red** de los ataques
2. Un host bastión es el único ordenador host de Internet **al que se puede acceder directamente** desde la red pública.
3. Ofrece una **gama limitada de servicios**, como alojamiento de sitios web y correo para garantizar la seguridad.



Necesidad de un Bastionado de Host

1. **Minimizar las posibilidades de penetración** de intrusos
2. **Crear todos los registros**, que pueden utilizarse para identificar ataques o intentos de ataque.
3. En caso de ataque, el anfitrión del bastión actúa como **chivo expiatorio**
4. **Proporcionar un nivel adicional de seguridad**

Colocación del host Bastión

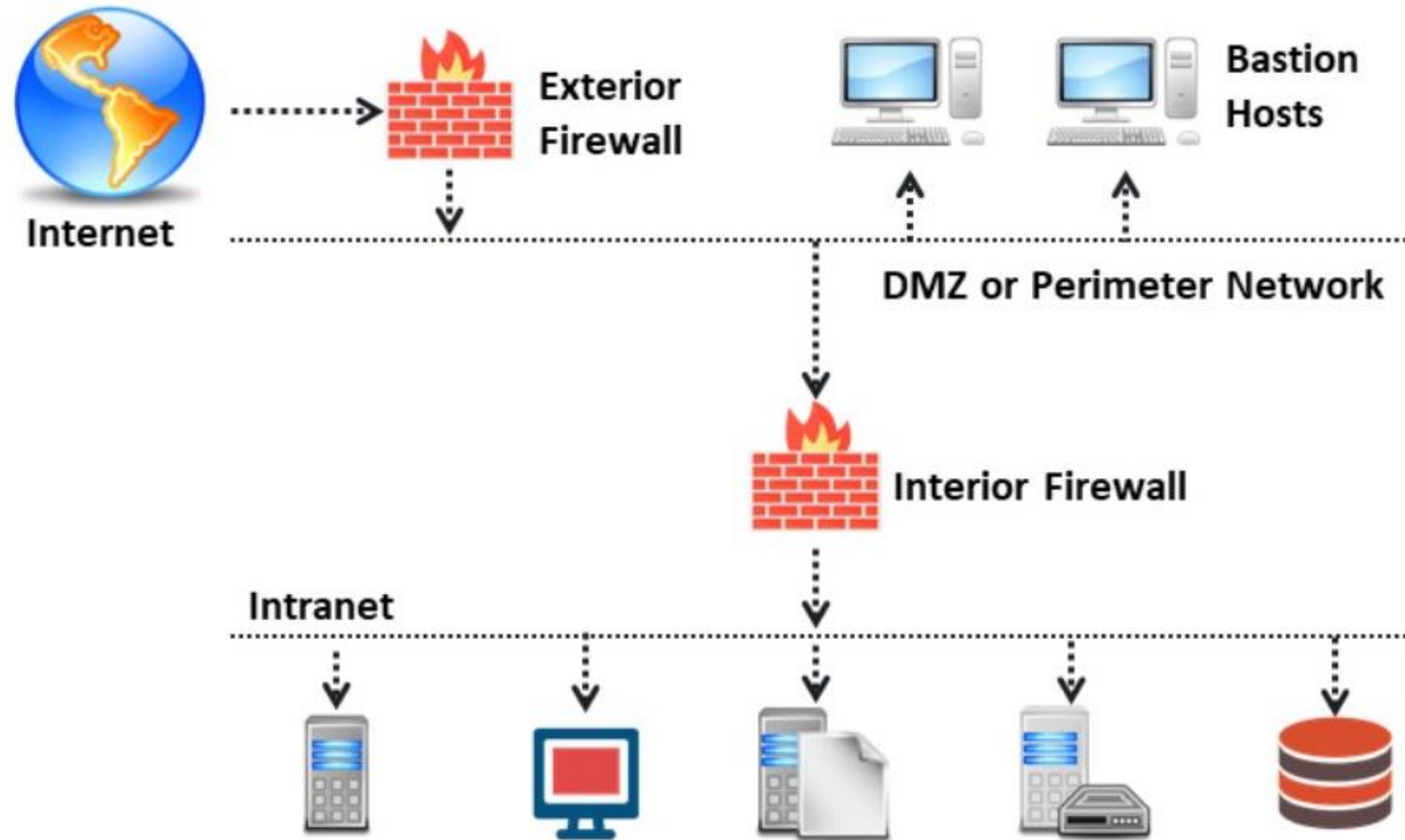
UBICACIÓN FÍSICA

- Situado en una sala de servidores especialmente seleccionada con controles ambientales adecuados
- Debe instalarse en un armario de servidores cerrado con ventilación, refrigeración y alimentación de reserva

UBICACIÓN EN LA RED

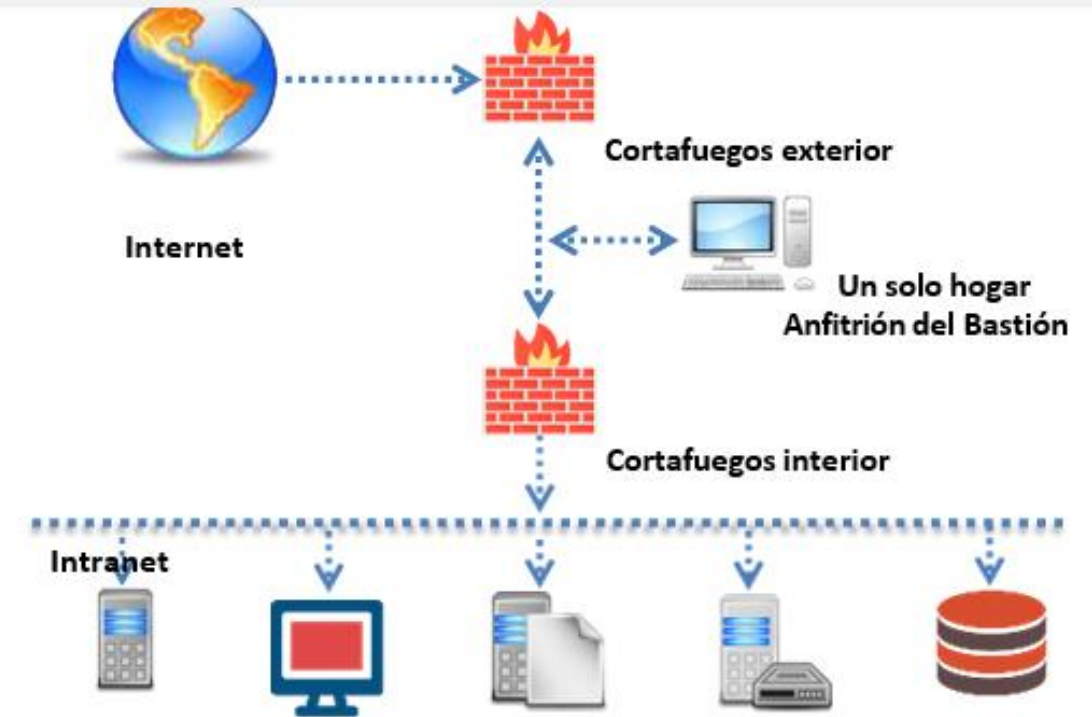
- Colocar en una red especial también conocida como zona desmilitarizada (DMZ) que no lleve datos sensibles
- Evite colocar el bastión en redes internas
- Debe ubicarse en una capa adicional conocida como red perimetral
- Adjuntar un router de filtrado de paquetes

Colocación del host Bastión



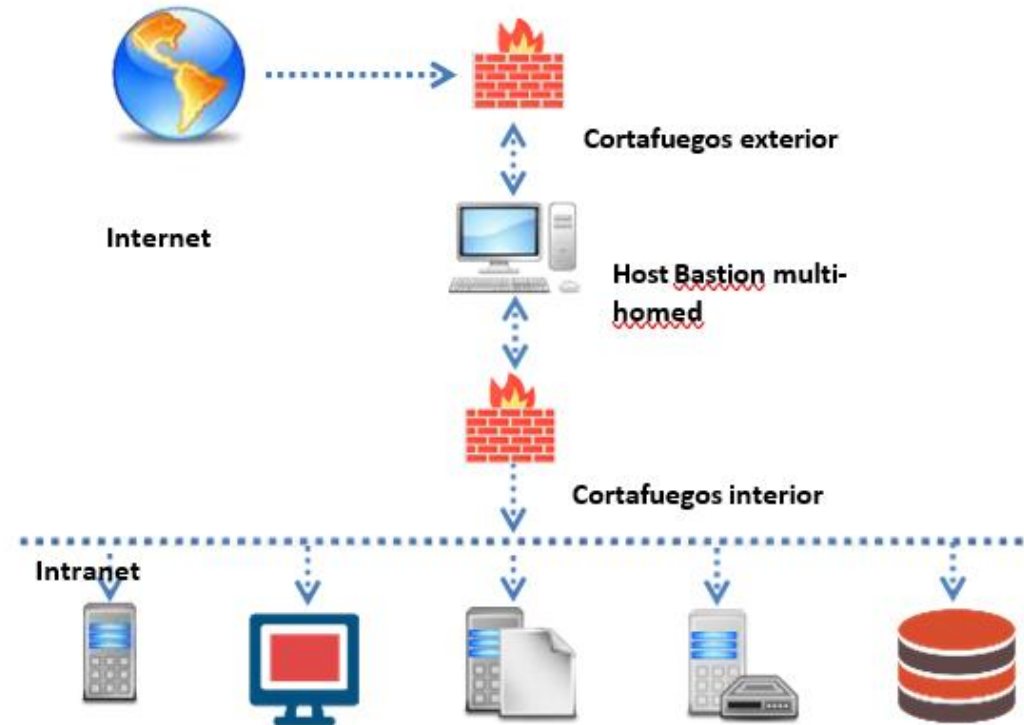
Tipos de hosts Bastion: Single-homed

- Un dispositivo cortafuegos con **una sola interfaz de red**
- Todo el tráfico, tanto entrante como saliente, se **encamina a través de** el anfitrión del bastión
- Comprueba los datos en función de las directrices de seguridad y actúa en consecuencia



Tipos de hosts Bastion: Multi-homed

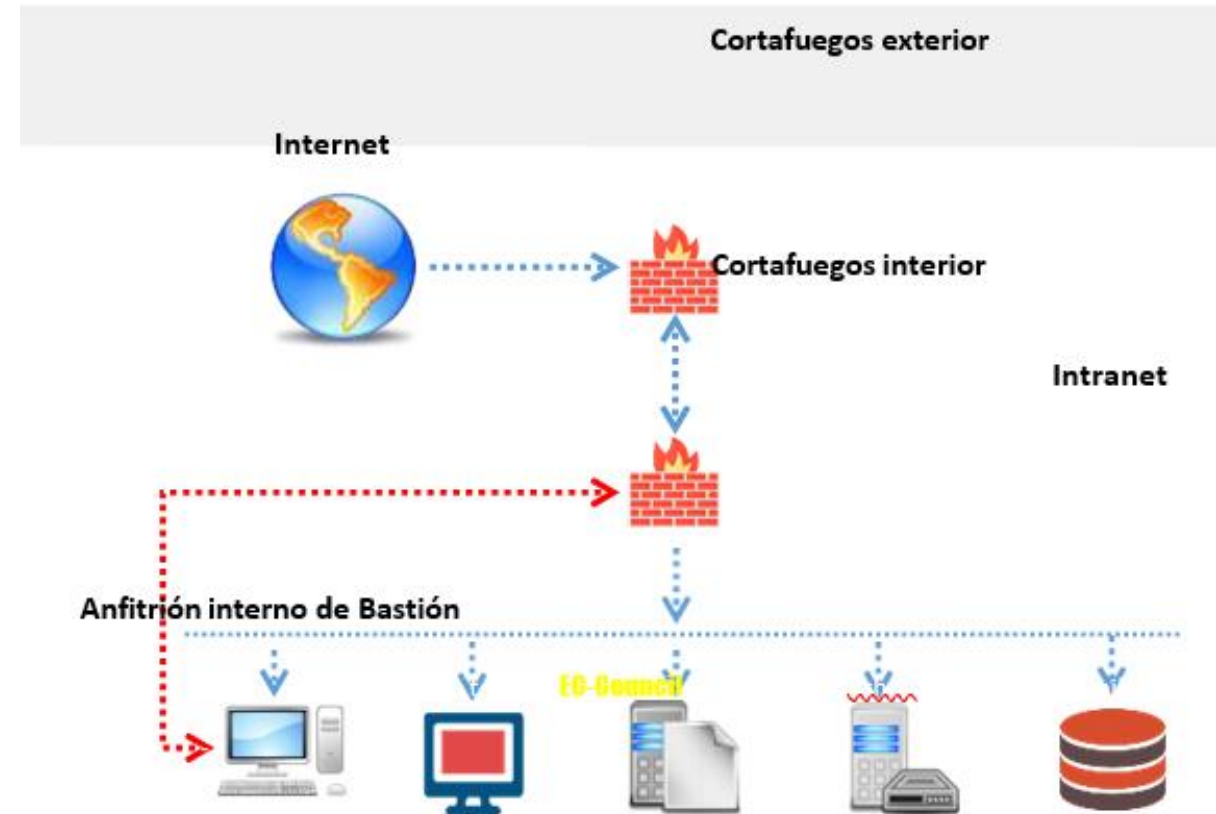
- ❑ Un dispositivo cortafuegos con al menos **dos interfaces de red**
- ❑ Este tipo de host bastión es capaz de separar las redes internas de las externas, por lo que mejora la seguridad



Tipos de anfitriones del Bastión:

Anfitrión interno de Bastión

- Residen **dentro de** la red interna de una organización
- Puede ser **individual** o **múltiple**.
- Los dispositivos de la red interna **se comunican** con el host bastión interno



Tipos de anfitriones del Bastión:

HOSTS DUAL-HOMED SIN ENRUTAMIENTO

- ✓ Operan con **múltiples conexiones de redes**, **pero** las conexiones de red **no interactúan entre sí**

Hosts de servicios externos

- ✓ Los hosts Bastion son visibles para todo el mundo lo que los hace vulnerables a los ataques
- ✓ Sólo requieren **unos privilegios de acceso mínimos** a la red interna, proporcionando sólo unos pocos servicios

MÁQUINAS VÍCTIMAS

- Las máquinas víctimas permiten **iniciar sesión** a cualquier usuario
- Son útiles para probar nuevas aplicaciones cuyos fallos de seguridad aún no se conocen y ejecutan servicios que no son seguros

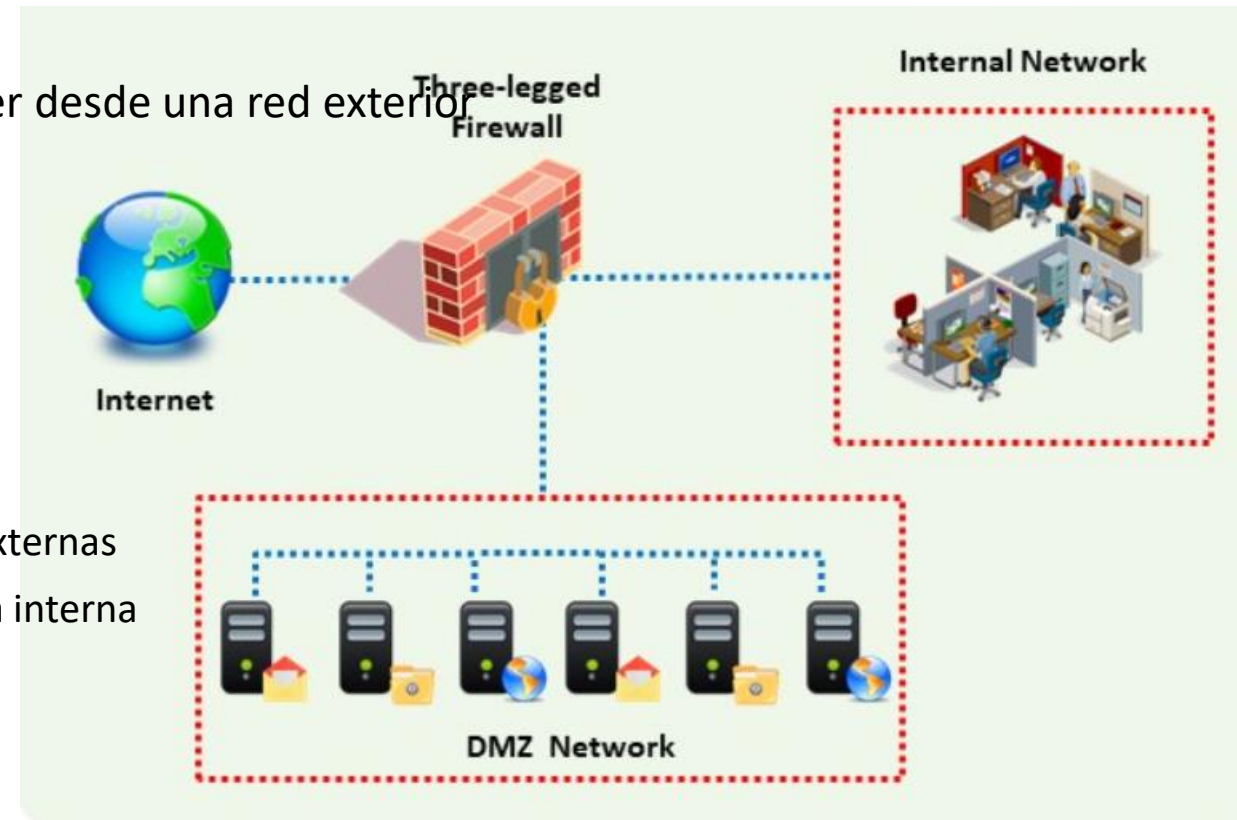
Cortafuegos de caja única

Si una máquina se construye como un cortafuegos, es propensa a más **ataques**.
La seguridad de todo el sitio depende de esta única máquina por lo que es necesario garantizar que esta máquina es absolutamente segura

¿Qué es la Zona Desmilitarizada (DMZ)?

Una subred informática se sitúa entre la red privada de la organización, como una **LAN**, y una red externa. red pública como **Internet**, y actúa como una capa de seguridad adicional

- ❑ Contiene los servidores a los que hay que acceder desde una red exterior
 - Servidores web
 - Servidores de correo electrónico
 - Servidores DNS
- ❑ Configuraciones DMZ
 - Tanto las redes **internas** como las **externas** pueden conectarse al DMZ
 - **Los hosts** de la DMZ pueden conectarse a redes externas
 - Pero los hosts en la DMZ no puede conectarse a la interna



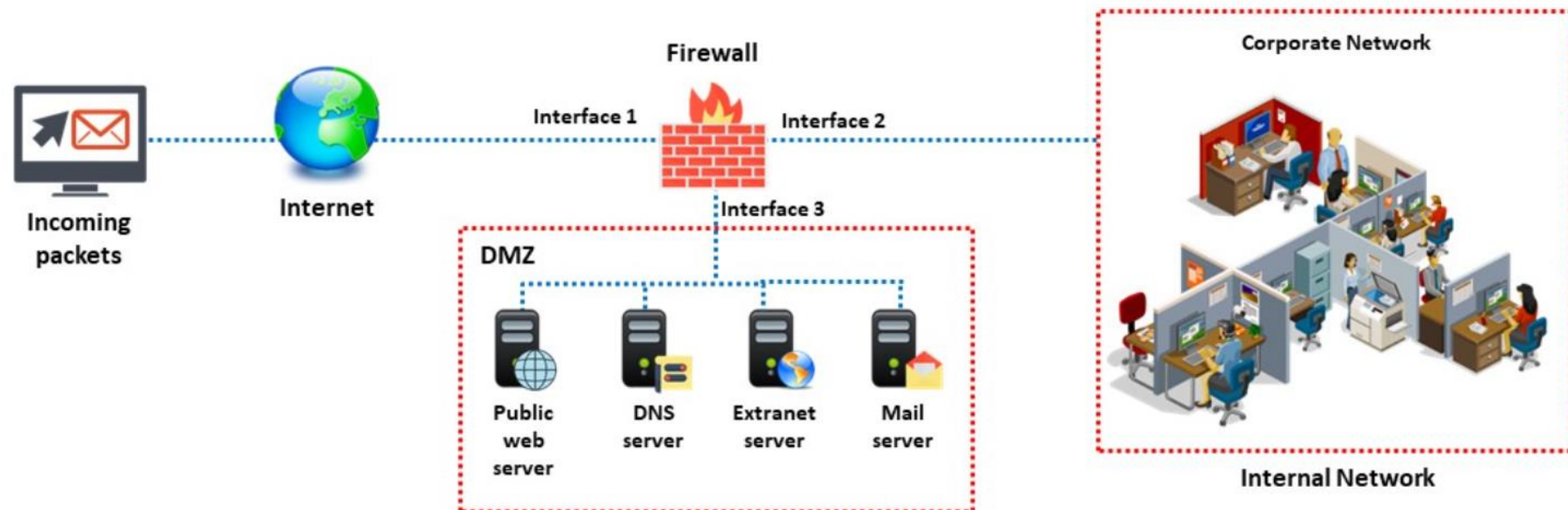
Ventajas de la DMZ

- La separación de la DMZ de la LAN permite una protección de alto nivel de la LAN.
- Proporciona un mayor control de los recursos.
- Utiliza múltiples productos basados en software y hardware de diferentes plataformas para proporcionar una capa adicional de protección.
- Ofrece un alto nivel de flexibilidad para aplicaciones basadas en Internet, como correo electrónico, servicios web, etc.

Diferentes formas de crear una DMZ

Un único Cortafuegos DMZ

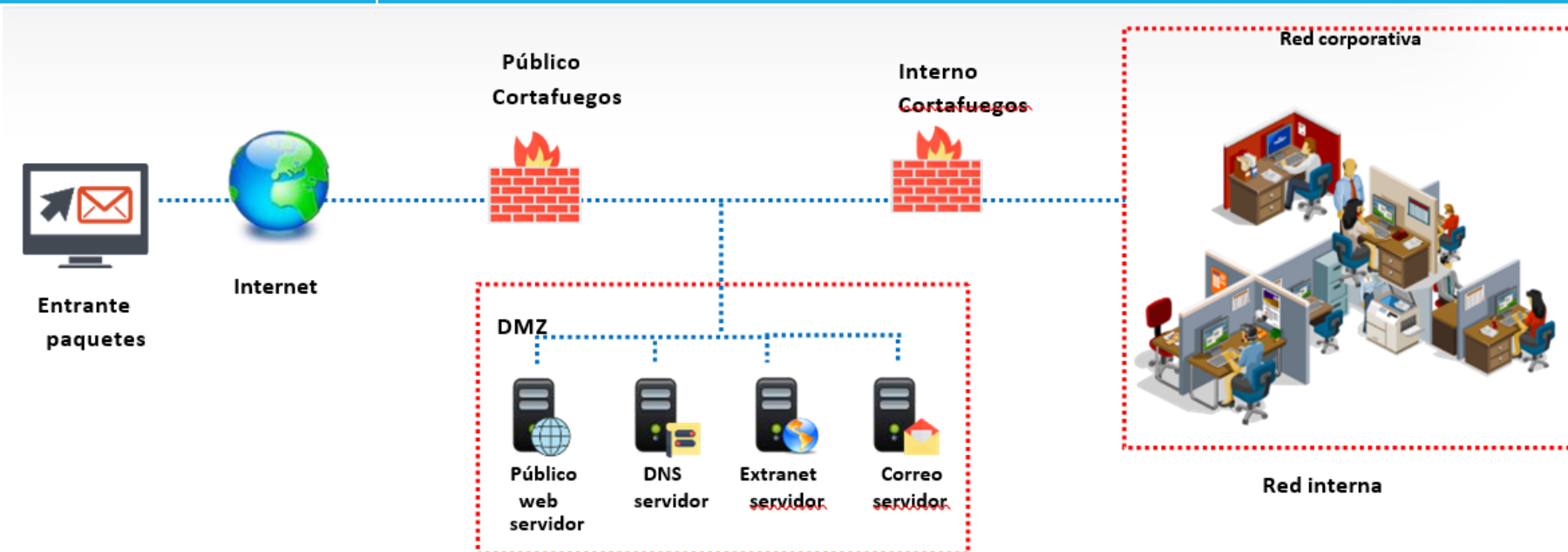
- En este modelo, la arquitectura de red que contiene la DMZ consta de tres interfaces de red
- La primera interfaz de red conecta el ISP con el cortafuegos, formando el externo mientras que la segunda interfaz forma la red interna
- La tercera interfaz forma la DMZ



Diferentes formas de crear una DMZ

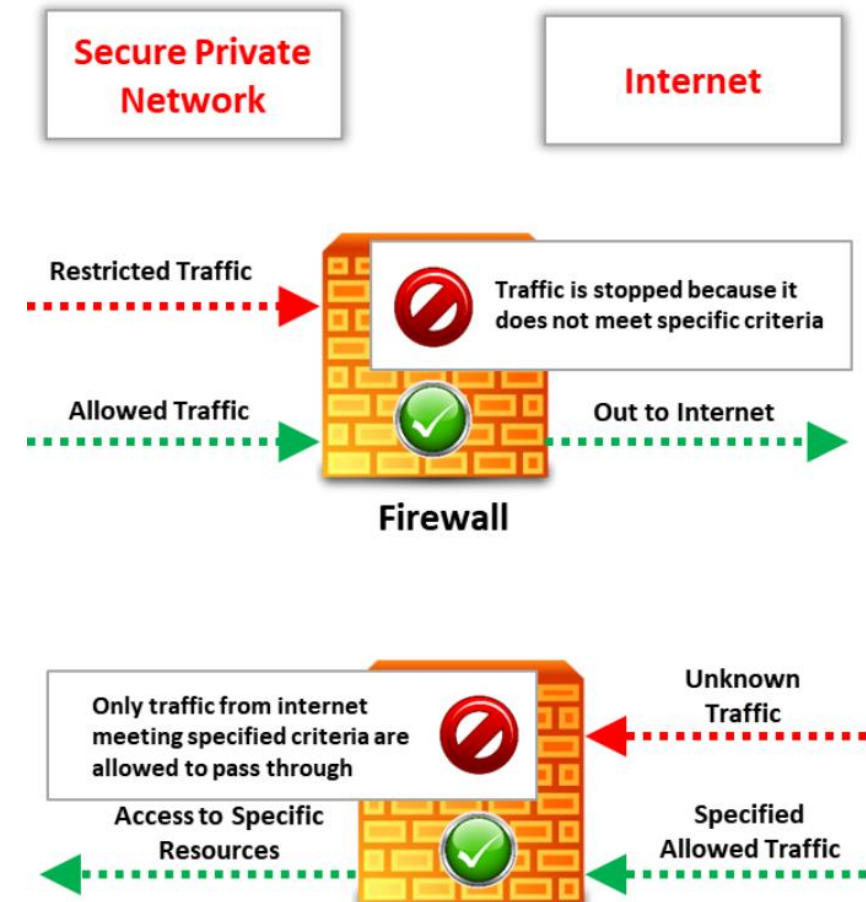
Doble cortafuegos DMZ

- Este enfoque utiliza dos cortafuegos para crear una DMZ
- El primer cortafuegos sólo permite que el tráfico desinfectado entre en la DMZ, mientras que el segundo cortafuegos realiza una doble comprobación
- Es el enfoque más seguro a la hora de implantar una DM



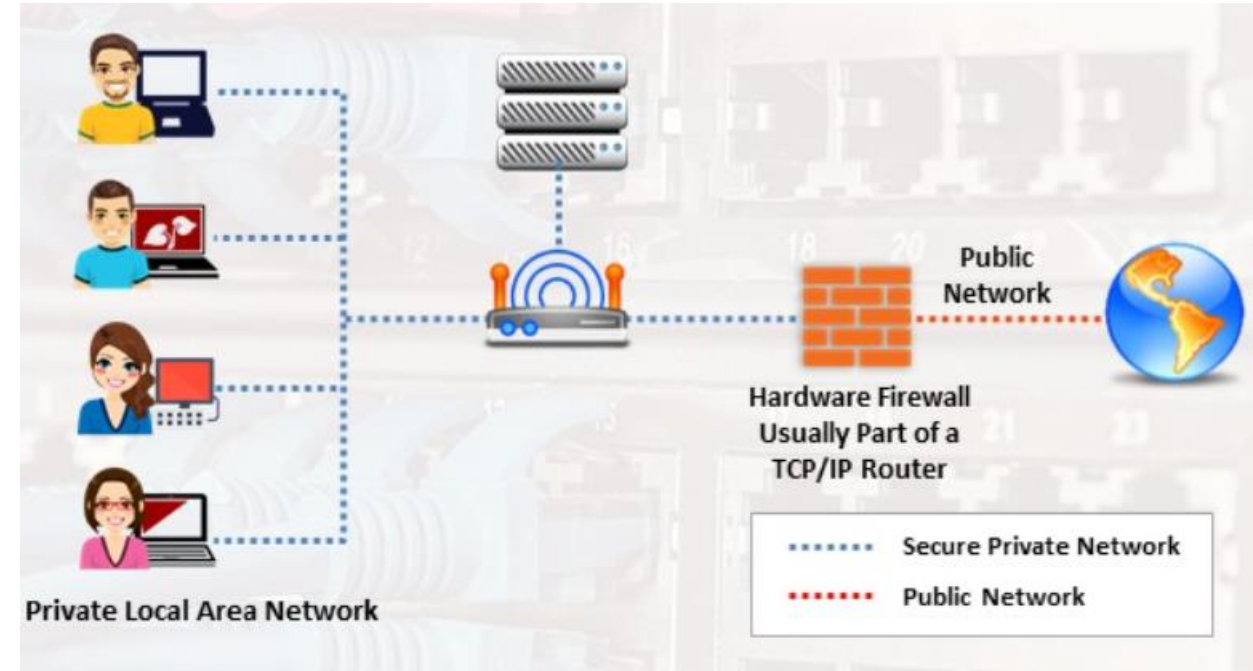
¿Qué es un cortafuegos?

- Un cortafuegos es un software o hardware, o una combinación de ambos, que se utiliza generalmente para separar una red protegida de una red pública desprotegida.
- Supervisa y filtra el tráfico entrante y saliente de la red e impide el acceso no autorizado a las redes privadas.

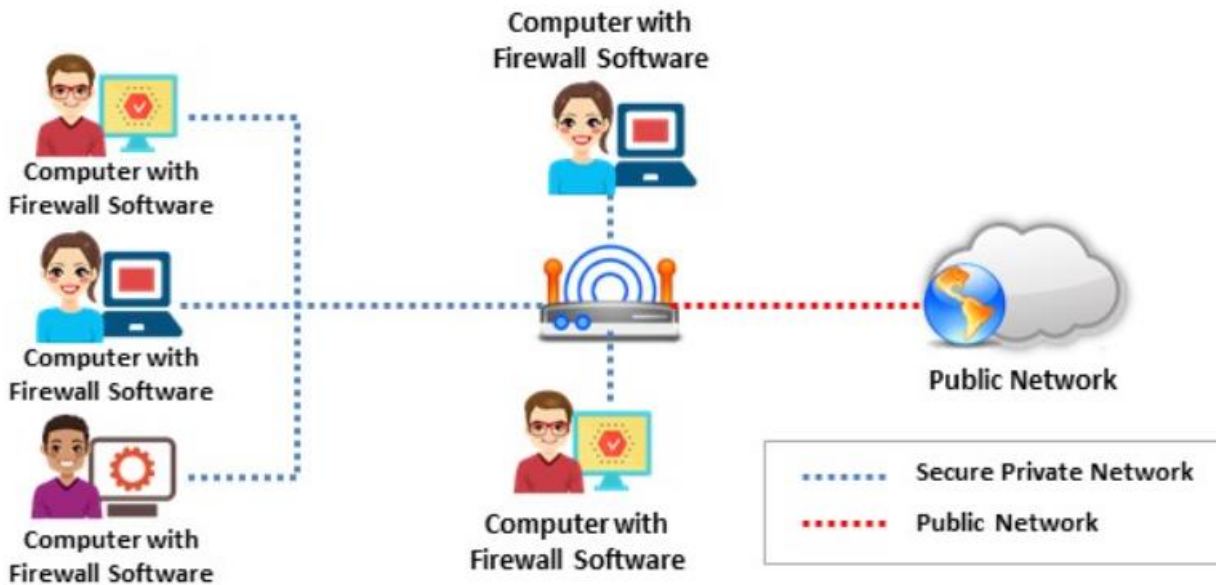


Tipos de cortafuegos: Cortafuegos de hardware

- Un cortafuegos de hardware es un dispositivo cortafuegos dedicado que se coloca en el perímetro de la red.
- Forma parte integrante de la configuración de la red y también está integrado en los routers de banda ancha o se utiliza como producto independiente
- Emplea la técnica del filtrado de paquetes. Lee la cabecera de un paquete para averiguar las direcciones de origen y destino y las compara con un conjunto de reglas predefinidas y/o creadas por el usuario que determinan si debe reenviar o descartar el paquete.
- Un cortafuegos de hardware funciona en un sistema individual o en una red concreta conectada mediante una única interfaz.



Tipos de cortafuegos: Cortafuegos de software



- ❑ Un cortafuegos de software es un programa informático que se instala en un ordenador, al igual que un software normal.
- ❑ Generalmente se utiliza para filtrar el tráfico de usuarios domésticos individuales
- ❑ Sólo filtra el tráfico del ordenador en el que está instalado, no el de toda la red

Tipos de cortafuegos: Basados en host y basados en red

CORTAFUEGOS BASADOS EN HOST

- El cortafuegos basado en host se utiliza para filtrar el tráfico entrante/saliente de un ordenador individual en el que está instalado
- Es un cortafuegos basado en software
- Este software cortafuegos forma parte de OS
- Ejemplo: Firewall de Windows, Iptables, UFW, etc.

CORTAFUEGOS BASADOS EN RED

- El cortafuegos basado en red se utiliza para filtrar el tráfico entrante/saliente desde la LAN interna
- Es un cortafuegos basado en hardware
- Ejemplo: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link, etc.

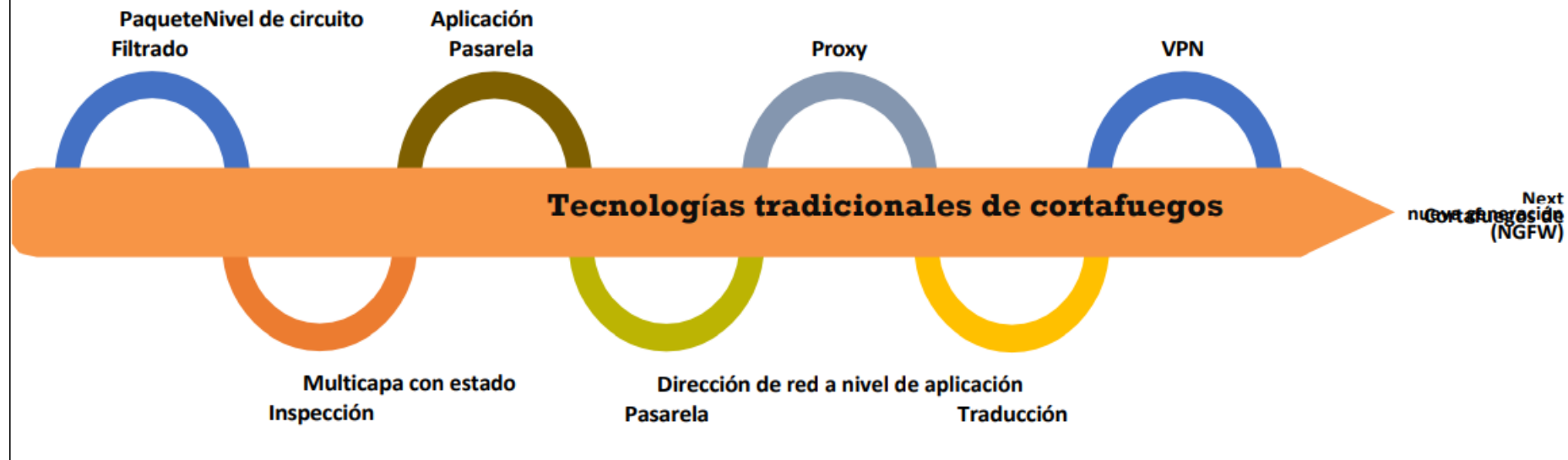
Tecnologías de cortafuegos



Los **cortafuegos** se diseñan y desarrollan con la ayuda de diferentes **servicios de cortafuegos**



Cada servicio de cortafuegos proporciona seguridad en función de su **eficacia** y **sofisticación**



Tecnologías de cortafuegos

Tecnologías de cortafuegos que funcionan en cada capa OSI

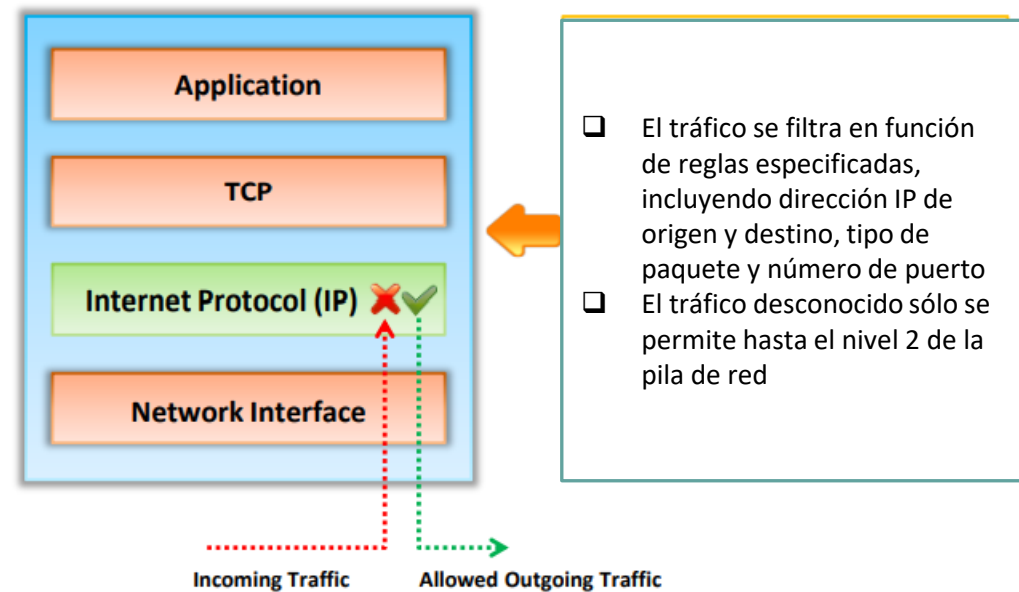
Capa OSI	Tecnología cortafuegos
Aplicación	✓ Red privada virtual (VPN) ✓ Proxies de aplicación
Presentación	✓ Red privada virtual (VPN)
Sesión	✓ Red privada virtual (VPN) ✓ Pasarelas a nivel de circuito
Transporte	✓ Red privada virtual (VPN) ✓ Filtrado de paquetes
Red	✓ Red privada virtual (VPN) ✓ Traducción de direcciones de red (NAT) ✓ Filtrado de paquetes ✓ Inspección multicapa con estado
Enlace de datos	✓ Red privada virtual (VPN) ✓ Filtrado de paquetes
Físico	✓ No aplicable

Filtrado de paquetes Cortafuegos

Los cortafuegos de filtrado de paquetes funcionan en el nivel de **red** del modelo OSI (o la capa **IP** de TCP/IP)

Suelen formar parte de un router. La mayoría de los routers admiten el filtrado de paquetes

En un cortafuegos de filtrado de paquetes, cada paquete se compara con un conjunto de criterios antes de reenviarse



Pasarela a nivel de circuito



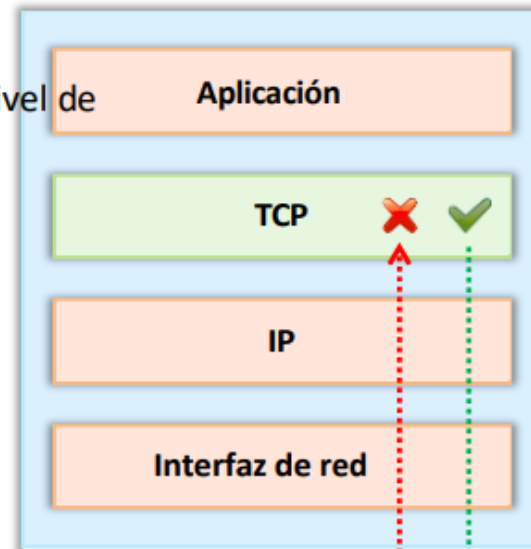
Las pasarelas a nivel de circuito funcionan a nivel de **capa de sesión** del modelo OSI, o el capa TCP de TCP/IP



Monitorizan el handshake TCP entre paquetes para determinar si una sesión solicitada es **legítima o no**



Información transmitida a un ordenador a través de una pasarela a nivel de circuito parece haberse originado en la **pasarela**



Tráfico entrante

Tráfico saliente permitido

- El tráfico se filtra en función de **reglas de sesión especificadas**, como cuando una sesión es iniciada por un ordenador reconocido
- Sólo se permite el tráfico desconocido hasta **el nivel 3 de la red pila**

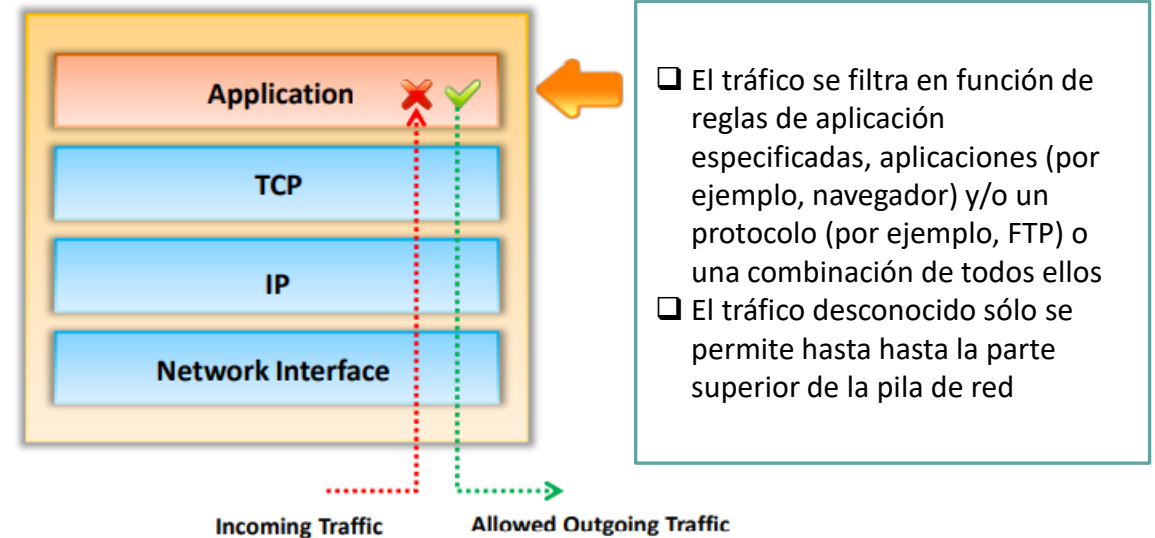
No autorizado

Permitido



Pasarelas a nivel de aplicación

- Las pasarelas de nivel de aplicación pueden filtrar paquetes en la capa de aplicación del modelo OSI
- Como examinan los paquetes en la capa de aplicación, pueden filtrar comandos específicos de la aplicación como específicos de la aplicación, como http:post y get
- En términos sencillos, una pasarela de nivel de aplicación puede configurarse para que sea un proxy web que no permita ningún tráfico FTP, Gopher, Telnet u otros a través de ella.



Cortafuegos de inspección multicapa con estado



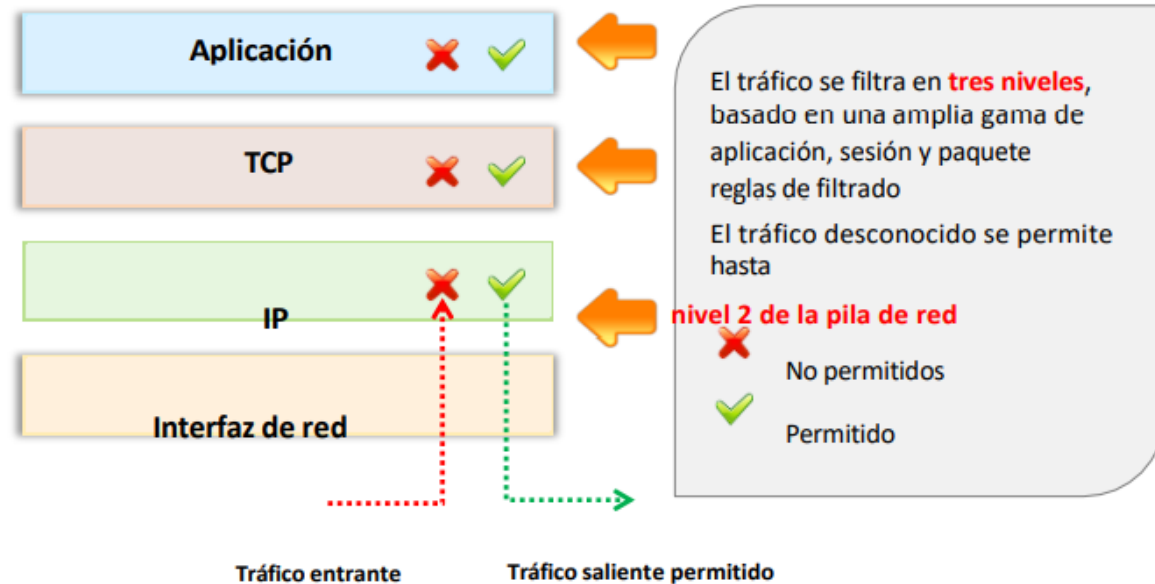
Una inspección multicapa con estado **combina** los **aspectos** del cortafuegos otros tres tipos



Filtran los paquetes en la red determinar si la **sesión** **paquetes** son **legítimos** y evalúan el contenido de los paquetes en el **capa de aplicación**



Son **caros** y requieren personal competente para administrar el dispositivo

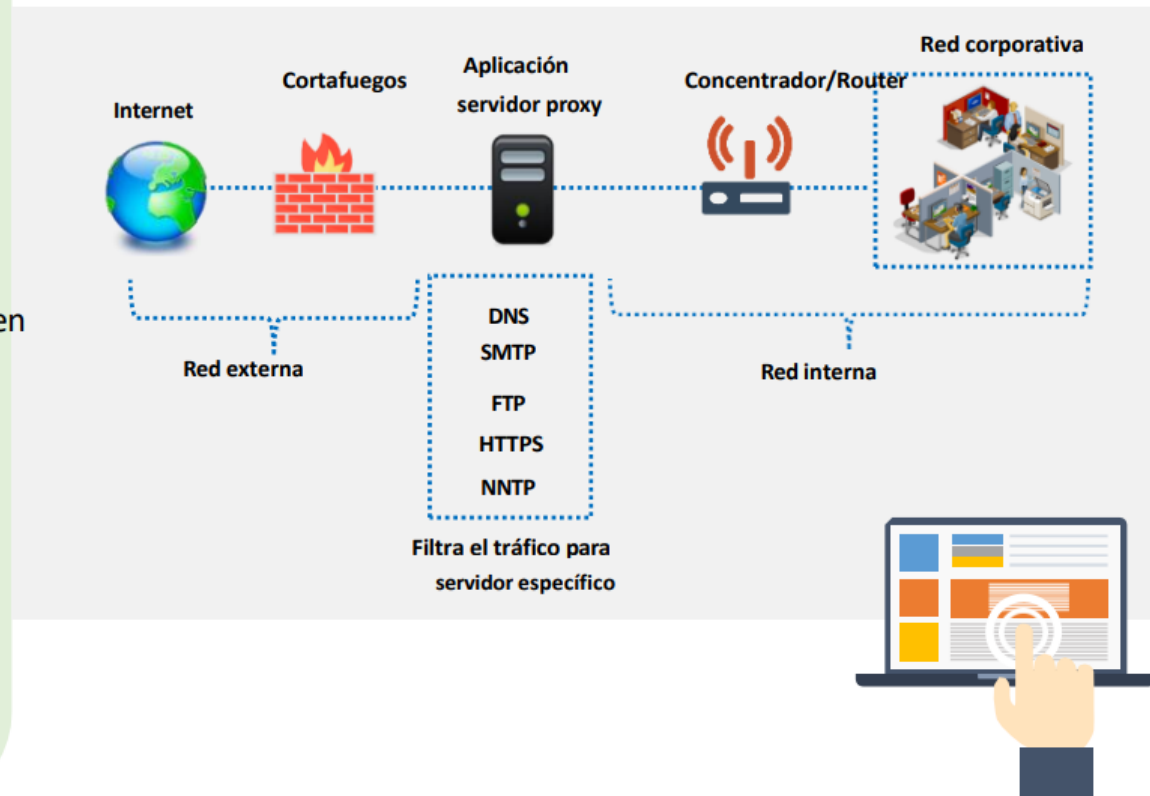


Proxy de aplicación



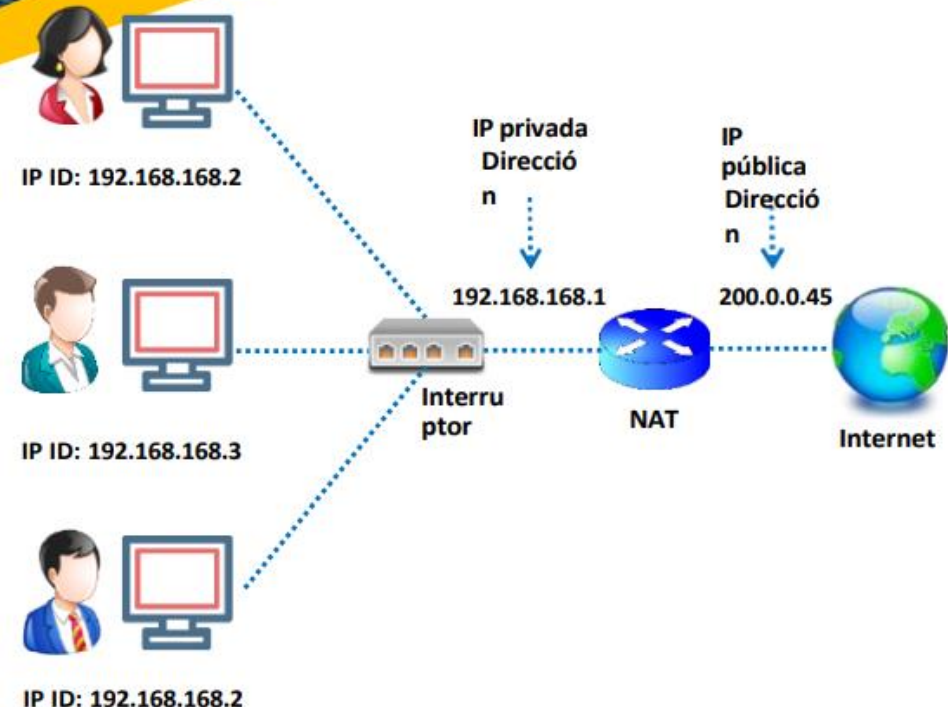
- ❑ Un proxy a nivel de aplicación funciona como un servidor proxy y **filtra las conexiones** para servicios específicos
- ❑ Filtra las conexiones basándose en sobre los **servicios** y **protocolos**
- ❑ **Por ejemplo**, un proxy FTP sólo permitirá el tráfico FTP a pasan, mientras que todos los se bloquearán otros servicios y protocolos

Proxy de aplicación



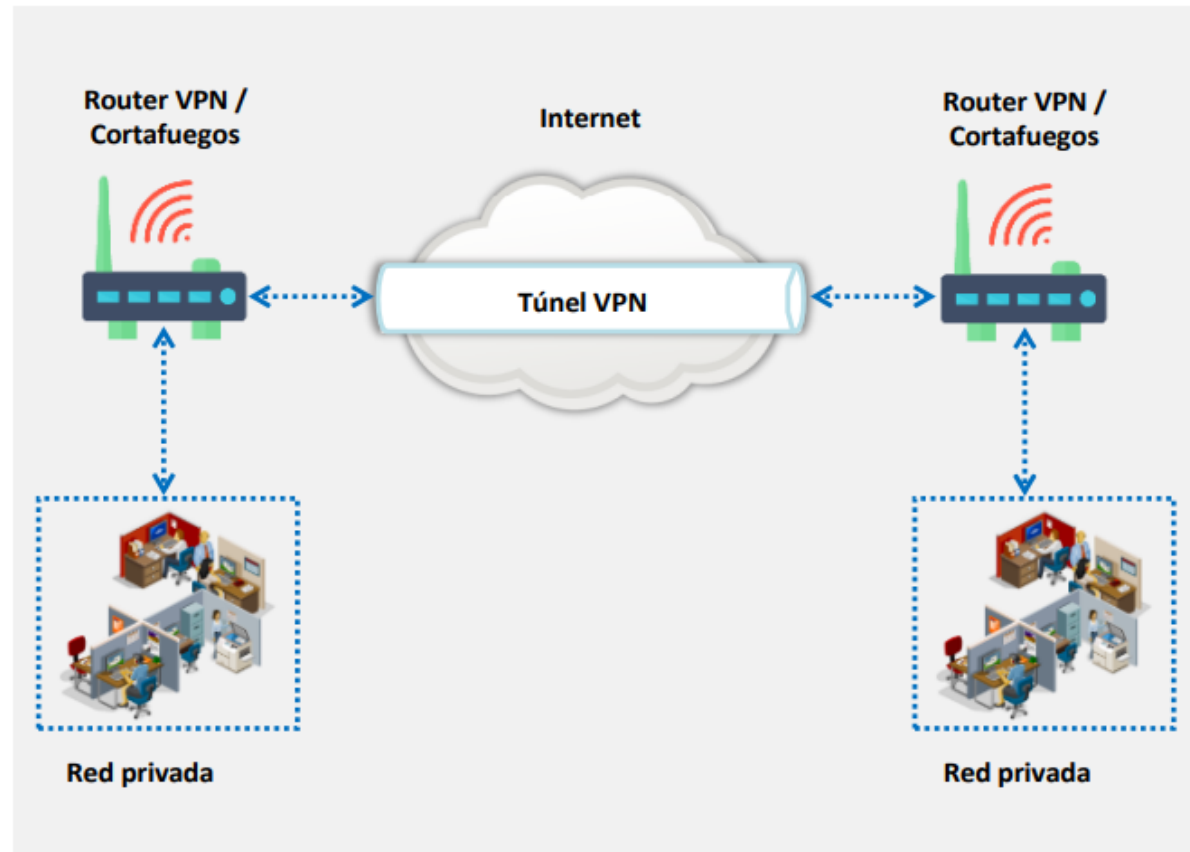
Traducción de direcciones de red (NAT)

- ❑ La traducción de direcciones de red separa las direcciones IP en dos conjuntos y permite a la LAN utilizar estas direcciones para el **tráfico interno** y **externo** respectivamente.
- ❑ También funciona con un router, al igual que el filtrado de paquetes; NAT también **modificará** los paquetes que envía el router al mismo tiempo.
- ❑ Tiene la capacidad de **cambiar** la **dirección** del paquete y hacer que parezca que ha llegado de una dirección válida
- ❑ Limita el número de **direcciones IP públicas** que puede utilizar una organización.



Red privada virtual (VPN)

- ❑ Una VPN es una **red privada** construida utilizando redes públicas, como Internet
- ❑ Se utiliza para la **transmisión segura** de información sensible a través de una red no fiable, mediante **encapsulación** y cifrado.
- ❑ Establece una conexión virtual punto a punto mediante el uso de **conexiones dedicadas**
- ❑ El **dispositivo informático que** ejecuta el software VPN sólo puede acceder a la VPN



Cortafuegos de nueva generación

- ❑ La tecnología de cortafuegos de nueva generación (NGFW) es **de tercera generación. tecnología de cortafuegos** que va más allá de la inspección de puertos y protocolos.
- ❑ Además de las funciones tradicionales de cortafuegos, la tecnología de cortafuegos NGFW puede inspeccionar el tráfico en función **del contenido de los paquetes.**
- ❑ Capacidades típicas de NGFW:
 - ✓ Inspección profunda de paquetes (DPI)
 - ✓ Inspección de tráfico cifrado
 - ✓ Gestión de la calidad del servicio y del ancho de banda
 - ✓ Integración de inteligencia sobre amenazas
 - ✓ Sistema integrado de prevención de intrusiones
 - ✓ Protección avanzada contra amenazas
 - ✓ Control de aplicaciones
 - ✓ Inspección antivirus



Funciones de cortafuegos

Evitar la exploración de la red

Controla el tráfico

Realiza la autenticación del usuario

Filtra paquetes, servicios y protocolos

Realiza el registro del tráfico

Realiza la traducción de direcciones de red NAT

Evita los ataques de malware

Limitaciones del cortafuegos

1

Un cortafuegos no impide que la red **sufra ataques de puerta trasera**

2

Un cortafuegos no protege la red de los **ataques internos**

3

Un cortafuegos no puede hacer nada si el diseño y la **configuración de la red son defectuosos.**

4

Un cortafuegos no es una alternativa a un **antivirus o antimalware**

5

Un cortafuegos no impide la **aparición de nuevos virus**

6

Un cortafuegos no puede evitar **las amenazas de ingeniería social**

7

Un cortafuegos no impide **el uso indebido de contraseñas**

8

Un cortafuegos no bloquea los ataques procedentes de un nivel superior de la **pila de protocolos**

Pasos de la implantación y despliegue de cortafuegos

Planificación: Al implantar un cortafuegos para la red, las organizaciones deben planificar su posicionamiento con antelación. Es fundamental realizar una evaluación de los riesgos de seguridad para saber dónde es más probable que se origine una amenaza para la red y las razones que la motivan.

Configuración: Configurar un cortafuegos implica configurar varios componentes y características como el hardware, el software, la configuración de políticas, la implementación de mecanismos de registro y alerta.

Pruebas: Probar un cortafuegos implica examinarlo para detectar cualquier fallo.

Despliegue: Es necesario asegurarse de que el cortafuegos se despliega de acuerdo con las políticas de seguridad de la organización.

Gestión y mantenimiento: La gestión de un cortafuegos incluye el mantenimiento de la arquitectura del cortafuegos, las políticas, el software y otros componentes desplegados en la red.

Protección de cortafuegos basada en host con Iptables

- ❑ Iptables es un cortafuegos integrado para sistemas operativos Linux.
- ❑ Iptables viene preinstalado en cualquier distribución de Linux. Sin embargo, puede actualizarlo/instalarlo con el comando: `sudo apt-get install iptables`

Tarea	Comandos Iptable
Filtrado de paquetes no TCP	<code>iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP</code>
Bloqueo del ataque del escáner XMAS	<code>iptables -A INPUT -p tcp --tcp-flags ALL -j DROP</code>
Descarta cualquier paquete NULL	<code>iptables -A INPUT -f -j DROP</code>
Descarta los paquetes fragmentados	<code>iptables -A INPUT -f -j DROP</code>

Protección de cortafuegos basada en host con Iptables

- ❑ Hay tres tipos diferentes de cadenas:
- ❑ **Entrada:** La cadena de entrada verifica las conexiones entrantes y su comportamiento. Iptables compara la dirección IP y el puerto de la conexión entrante con una regla de la cadena.
- ❑ **Reenvío:** La cadena de reenvío reenvía principalmente las conexiones entrantes a su destino. El comando iptables -L -v verifica si una conexión entrante necesita una cadena de reenvío.
- ❑ **Salida:** La cadena de salida se utiliza para las conexiones de salida, en las que la cadena comprueba la cadena de salida y decide si permite o deniega la solicitud de salida.

Protección de cortafuegos basada en host con Iptables

□ Ejemplo de reglas de firewall iptables:

- Compruebe las reglas existentes mediante el comando `sudo iptables -L -n -v`
- Compruebe las reglas de una tabla específica mediante el comando `iptables -t nat -L -v -n`.
- Bloquee la dirección IP especificada mediante el cortafuegos iptables. `iptables -A INPUT -s 10.10.10.55 -j DROP`
- Bloquee un puerto específico en el cortafuegos iptables utilizando el comando `iptables -A OUTPUT -p tcp --dport xxx -j DROP`.
- Bloquear Facebook en el cortafuegos Iptables utilizando el comando `iptables -A OUTPUT -p tcp -d 66.220.144.0/20 -j DROP`

Protección de cortafuegos basada en host con Iptables

Tarea	Comandos Iptables
Filtrado de paquetes no TCP	<code>iptables -A INPUT -p tcp ! --syn -m estado --state NEW -j DROP</code>
Bloqueo del ataque XMAS	<code>iptables -A INPUT -p tcp --tcp-flags ALL -j DROP</code>
Descarta cualquier paquete NULL	<code>iptables -A INPUT -f -j DROP</code>
Descarta los paquetes fragmentados	<code>iptables -A INPUT -f -j DROP</code>
Bloquear inundaciones de red en el puerto Apache	<code>iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/minuto --limit-burst 200 -j ACCEPT</code>
Bloquear las peticiones de ping entrantes	<code>iptables -A INPUT -p icmp -i eth0 -j DROP</code>
Bloquear el acceso a una dirección MAC específica	<code>iptables -A INPUT -m mac --mac-fuente 00:00:00:00:00:00 -j DROP</code>
Bloquear la conexión en la interfaz de red	<code>iptables -A INPUT -i eth0 -s xxx.xxx.xxx.xxx -j DROP</code>
Desactivar los correos salientes	<code>iptables -A OUTPUT -p tcp --dports 25,465,587 -j REJECT</code>

Implantación de cortafuegos seguros:

Mejores prácticas

Filtrar puertos vulnerables comunes y no utilizados	Para mejorar el rendimiento del cortafuegos, limite las aplicaciones que se están ejecutando
Si es posible, cree un ID de usuario único para ejecutar el programa servicios de cortafuegos. En lugar de ejecutar los servicios utilizando los ID de administrador o root	Configurar un servidor de syslog remoto y aplicar un estricto medidas para protegerla de usuarios malintencionados
Configure el conjunto de reglas del cortafuegos para denegar todo el tráfico y activar sólo los servicios necesarios	Supervise los registros del cortafuegos a intervalos regulares. Incluya en su política de conservación de datos
Cambia todas las contraseñas por defecto y crea una fuerte contraseña que no se encuentre en ningún diccionario. Una contraseña fuerte para garantizar que los ataques de fuerza bruta también fallen	Investigar inmediatamente todas las entradas de registro sospechosas que se encuentren

Utilizar el Script Firewalk (NSE) de Nmap para Intentar Descubrir las Reglas de un Firewall

- Firewalk es una herramienta de seguridad de red de reconocimiento activo para enumerar reglas de cortafuegos.
- Firewalk envía paquetes TCP o UDP con un TTL superior al de la puerta de enlace/cortafuegos objetivo.
- Si la puerta de enlace/cortafuegos permite el tráfico, reenviará los paquetes al siguiente salto donde expirarán y provocarán un mensaje ICMP_TIME_EXCEEDED.
- Si el host de la pasarela no permite el tráfico, probablemente descartará los paquetes y no habrá respuesta.
- Para obtener el TTL IP correcto que resultará en paquetes caducados, es necesario aumentar el número de saltos.

Utilizar el Script Firewalk (NSE) de Nmap para Intentar Descubrir las Reglas de un Firewall

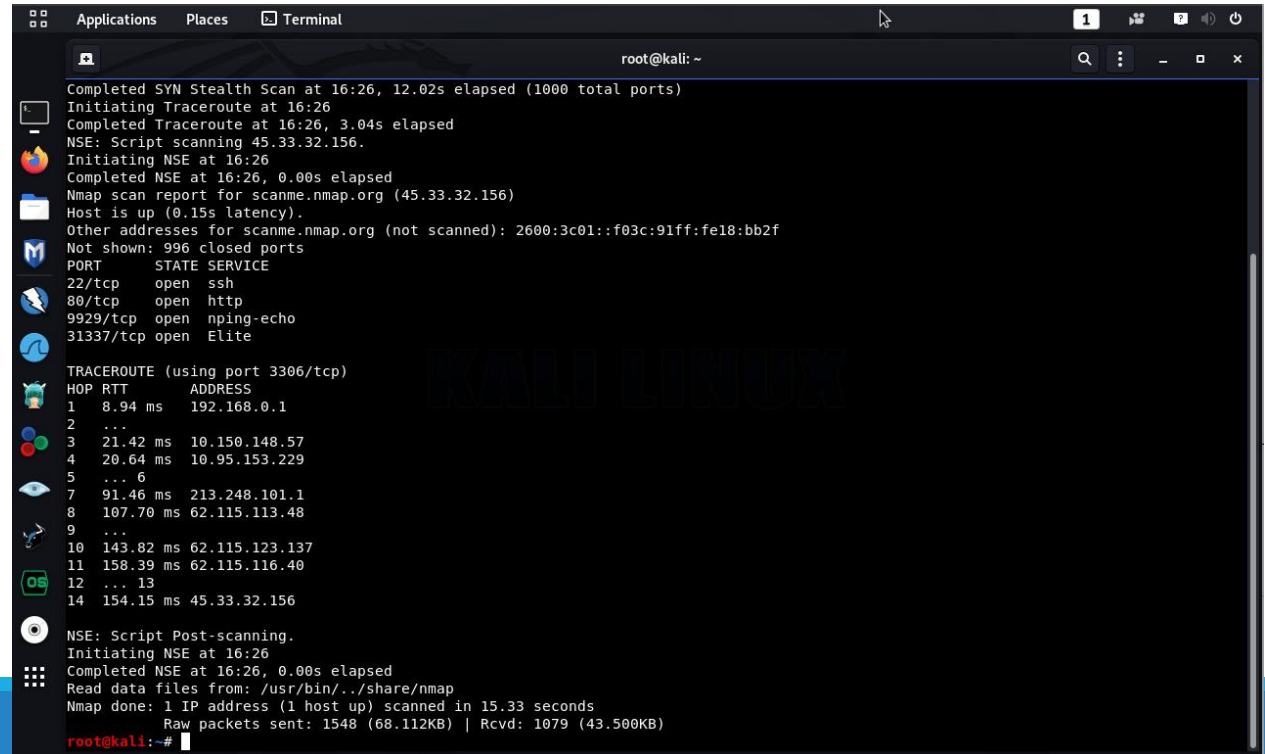
- Entre los argumentos del script se enumeran:
 - **firewalk.max-probed-ports:** Máximo número de puertos a probar por protocolo. Definirlo a -1 para escanear cada puerto filtrado.
 - **firewalk.max-retries:** Máximo número de retransmisiones permitidas.
 - **firewalk.recv-timeout:** La duración de los paquetes capturados en bucle (en milisegundos)
 - **firewalk.max-active-probes:** Máximo número de pruebas activas en paralelo.
 - **firewalk.probe-timeout:** Periodo válido de una prueba (en milisegundos)
 - Ejemplos:
 - `nmap --script=firewalk --traceroute <host>`
 - `nmap --script=firewalk --traceroute --script-args=firewalk.max-retries=1 <host>`
 - `nmap --script=firewalk --traceroute --script-args=firewalk.probe-timeout=400ms <host>`
 - `nmap --script=firewalk --traceroute --script-args=firewalk.max-probed-ports=7 <host>`

Utilizar el Script Firewalk (NSE) de Nmap para Intentar Descubrir las Reglas de un Firewall

Para el siguiente ejemplo se utiliza el host scanme.nmap.org (El cual es parte del proyecto Nmap, y puede ser utilizado para realizar escaneos).

```
# nmap -n -Pn -v --script=firewalk --script-args=firewalk.max-probed-ports=5 --traceroute scanme.nmap.org
```

Los resultados de este primer escaneo no exponen resultados obtenidos por el script NSE de nombre "firewalk".



```
root@kali: ~  
Completed SYN Stealth Scan at 16:26, 12.02s elapsed (1000 total ports)  
Initiating Traceroute at 16:26  
Completed Traceroute at 16:26, 3.04s elapsed  
NSE: Script scanning 45.33.32.156.  
Initiating NSE at 16:26  
Completed NSE at 16:26, 0.00s elapsed  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.15s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
9929/tcp   open  nping-echo  
31337/tcp  open  Elite  
  
TRACEROUTE (using port 3306/tcp)  
HOP RTT      ADDRESS  
1  8.94 ms   192.168.0.1  
2  ...  
3  21.42 ms  10.150.148.57  
4  20.64 ms  10.95.153.229  
5  ... 6  
7  91.46 ms  213.248.101.1  
8  107.70 ms 62.115.113.48  
9  ...  
10 143.82 ms 62.115.123.137  
11 158.39 ms 62.115.116.40  
12 ... 13  
14 154.15 ms 45.33.32.156  
  
NSE: Script Post-scanning.  
Initiating NSE at 16:26  
Completed NSE at 16:26, 0.00s elapsed  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds  
Raw packets sent: 1548 (68.112KB) | Rcvd: 1079 (43.500KB)  
root@kali:~#
```

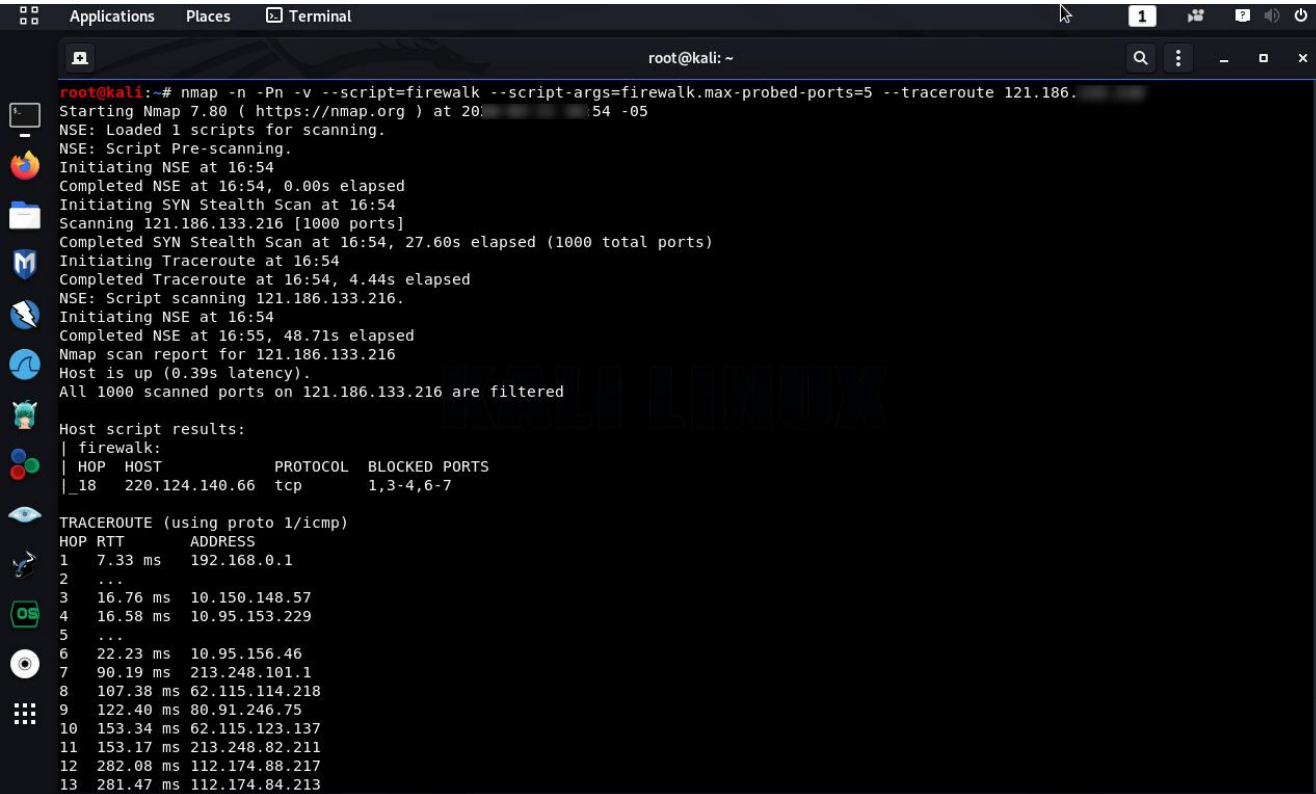
Utilizar el Script Firewalk (NSE) de Nmap para Intentar Descubrir las Reglas de un Firewall

Se procede realizar un segundo escaneo.

```
# nmap -n -Pn -v --script=firewalk --script-args=firewalk.max-probed-ports=5 --traceroute 121.186. X. Y
```

Los resultados obtenidos por este segundo escaneo, y puntualmente por el script NSE de nombre “firewalk”, muestran en el salto número 18 los puertos TCP bloqueados 1,3,4, 6 y 7.

Mencionar también la utilización de la opción “--traceroute” de Nmap, lo cual realiza y muestra un trazado de la ruta hacia el host escaneado.



```
root@kali: ~  
root@kali:~# nmap -n -Pn -v --script=firewalk --script-args=firewalk.max-probed-ports=5 --traceroute 121.186.133.216  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-14 16:54:05  
NSE: Loaded 1 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 16:54  
Completed NSE at 16:54, 0.00s elapsed  
Initiating SYN Stealth Scan at 16:54  
Scanning 121.186.133.216 [1000 ports]  
Completed SYN Stealth Scan at 16:54, 27.60s elapsed (1000 total ports)  
Initiating Traceroute at 16:54  
Completed Traceroute at 16:54, 4.44s elapsed  
NSE: Script scanning 121.186.133.216.  
Initiating NSE at 16:54  
Completed NSE at 16:55, 48.71s elapsed  
Nmap scan report for 121.186.133.216  
Host is up (0.39s latency).  
All 1000 scanned ports on 121.186.133.216 are filtered  
  
Host script results:  
|_ firewalk:  
|_ HOP  HOST          PROTOCOL  BLOCKED PORTS  
|_ 18   220.124.140.66  tcp      1,3-4,6-7  
  
TRACEROUTE (using proto 1/icmp)  
HOP RTT      ADDRESS  
1   7.33 ms   192.168.0.1  
2   ...  
3   16.76 ms  10.150.148.57  
4   16.58 ms  10.95.153.229  
5   ...  
6   22.23 ms  10.95.156.46  
7   90.19 ms  213.248.101.1  
8   107.38 ms 62.115.114.218  
9   122.40 ms 80.91.246.75  
10  153.34 ms 62.115.123.137  
11  153.17 ms 213.248.82.211  
12  282.08 ms 112.174.88.217  
13  281.47 ms 112.174.84.213
```

Implementación y despliegue de cortafuegos:

Gestión y mantenimiento

- ☐ Aplique los últimos parches y actualizaciones al dispositivo cortafuegos, si los publica el proveedor del cortafuegos
- ☐ Mantener la arquitectura del cortafuegos, las políticas, el software y otros componentes de acuerdo con la configuración y el despliegue del cortafuegos
- ☐ Actualizar la política del cortafuegos en función de las nuevas amenazas detectadas.
- ☐ Revisar periódicamente la política de cortafuegos
- ☐ Supervise y registre continuamente todas las alertas que se produzcan cuando el cortafuegos identifique amenazas.
- ☐ Realice periódicamente copias de seguridad de las reglas y políticas del cortafuegos
- ☐ Actualizar los conjuntos de reglas del cortafuegos en función de los requisitos de seguridad
- ☐ Realizar un análisis del registro del cortafuegos para detectar incidentes de seguridad

Sistema de detección y prevención de intrusiones (IDS/IPS)

01

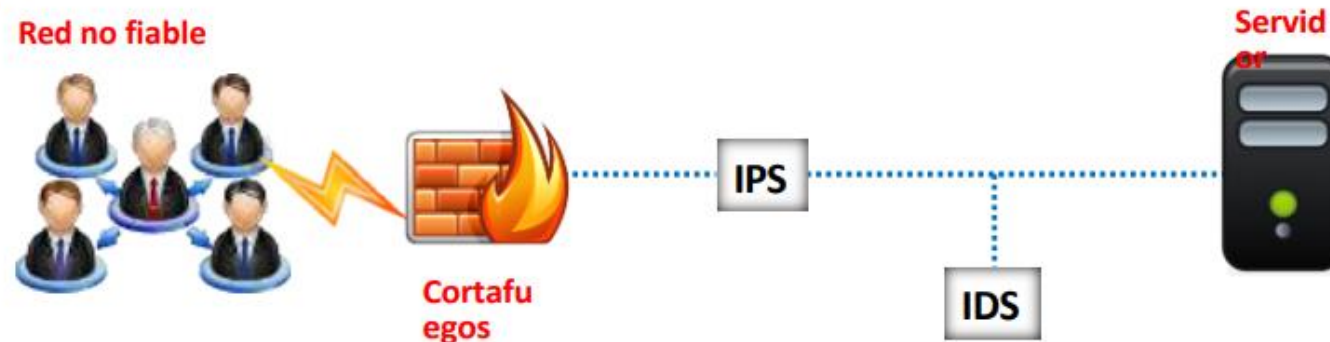
Un sistema de detección y prevención de intrusiones (IDS/IPS) es un dispositivo de seguridad de red que **inspecciona todo el tráfico de red entrante y saliente** en busca de patrones sospechosos que puedan indicar una violación de la seguridad de la red o del sistema.

02

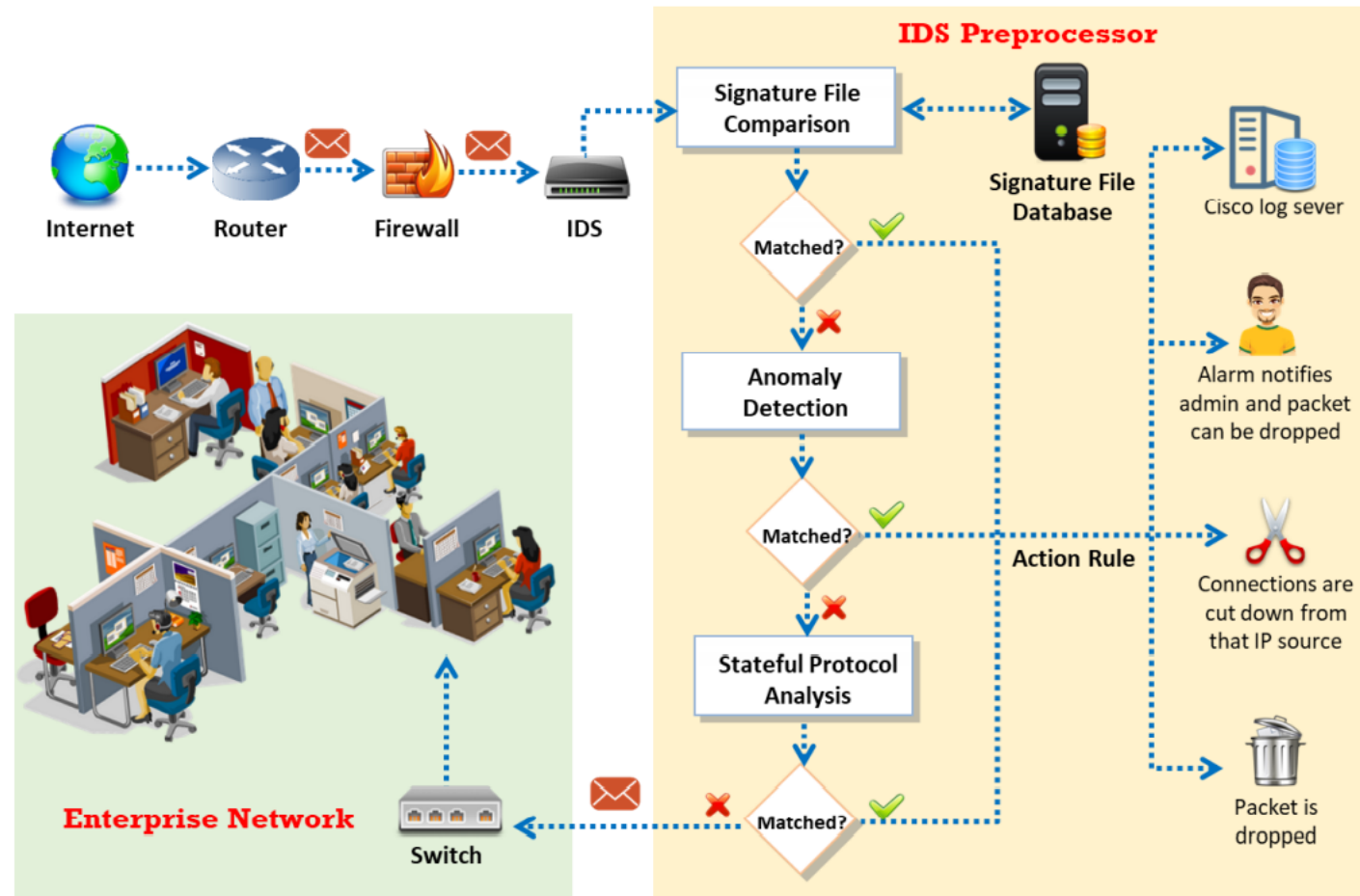
Si se encuentra, el IDS alertará al administrador sobre las **actividades sospechosas**

03

El IDS comprueba el tráfico de la red en busca de **firmas** que coincidan con patrones de intrusión conocidos y activa una alarma cuando encuentra una coincidencia.



¿Cómo funciona un IDS?



Papel de un IDS en la defensa de la red

Un IDS funciona desde dentro de la red, a diferencia de un cortafuegos, que sólo busca intrusiones fuera de la red.

Un IDS se coloca detrás del cortafuegos, inspeccionando todo el tráfico, buscando heurísticas y un patrón que coincida con las intrusiones

Enfoque de IDS basado en

Detección basada en firmas: Conocida como detección de uso indebido

Supervisa patrones de paquetes de datos en la red y los compara con patrones de ataque de red preconfigurados, conocidos como firmas

Este método utiliza operaciones de comparación de cadenas para comparar la actividad en curso, como un paquete o una entrada de registro, con una lista de firmas.

Ventajas

- Detecta ataques con un mínimo de falsas alarmas
- Puede identificar rápidamente el uso de una herramienta o técnica específica
- Ayuda a los administradores a rastrear rápidamente cualquier posible problema de seguridad e iniciar procedimientos de gestión de incidentes.

Desventajas

- Este enfoque sólo detecta amenazas conocidas, la base de datos debe actualizarse constantemente con nuevas firmas de ataques
- Utiliza firmas muy definidas que impiden detectar variantes comunes de los ataques

Enfoque de IDS basado en

Detección basada en anomalías: En este enfoque, las alarmas por actividades anómalas se generan evaluando patrones de red como qué tipo de ancho de banda se utiliza, qué protocolos se utilizan y qué puertos y qué dispositivos están conectados entre sí

Un IDS supervisa la actividad típica durante un intervalo de tiempo determinado y, a continuación, elabora las estadísticas del tráfico de red

Por ejemplo: los IDS basados en anomalías supervisan las actividades para detectar el uso normal del ancho de banda de Internet, los intentos fallidos de inicio de sesión, los niveles de utilización del procesador, etc.

Ventajas

- Un IDS basado en anomalías identifica comportamientos anómalos en la red y detecta los síntomas de ataques sin detalles claros
- La información adquirida por los detectores de anomalías se utiliza además para definir las firmas de los detectores de uso indebido.

Desventajas

- La tasa de generación de falsas alarmas es elevada debido al comportamiento impredecible de los usuarios y las redes
- La necesidad de crear un amplio conjunto de eventos del sistema para caracterizar los patrones de comportamiento normales.

Enfoque de IDS basado en

Análisis de protocolos con seguimiento de estado:

Este método compara los eventos observados con perfiles predeterminados basados en definiciones aceptadas de actividad benigna para cada protocolo con el fin de identificar cualquier desviación del estado del protocolo

Puede identificar secuencias impredecibles de comandos. Por ejemplo, puede identificar actividades como la emisión repetida de los mismos comandos o el uso de comandos arbitrarios

También detecta variaciones en la longitud de los comandos, valores mínimos/máximos de atributos y otras anomalías potenciales

Para cualquier protocolo que realice autenticación, el IDS/IPS realizará un seguimiento del autenticador que se utiliza para cada sesión y registrará el autenticador implicado en la actividad sospechosa

Componentes de IDS

Un IDS está formado por diferentes componentes. Estos componentes se utilizan para recopilar información de una variedad de sistemas y fuentes de red, y luego analizar la información para detectar cualquier anomalía.

A continuación se enumeran los principales componentes de un IDS.

- **Sensores de red:** Estos agentes analizan e informan de cualquier actividad sospechosa.
- **Analizador:** Analiza los datos recogidos por los sensores.
- **Sistemas de alerta:** Estos sistemas activan alertas al detectar actividad maliciosa.
- **Consola de mando:** Actúa como interfaz entre el usuario y el IDS.
- **Sistema de respuesta:** Un IDS utiliza este sistema para iniciar contramedidas sobre las actividades detectadas.
- **Base de datos de firmas o comportamientos de ataque:** Lista de firmas detectadas previamente y almacenadas en una base de datos que ayudan al IDS en la detección de intrusiones.

Soluciones IDS basadas en red: Snort

Snort es un sistema de detección de intrusiones en la red (NIDS) para Linux y Windows que detecta amenazas emergentes.

The screenshot displays the Snort web interface. On the left, a text editor window titled '*downloaded.rules [Read-Only]' shows several Snort rules. One rule is highlighted with a red box:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET SCAN Suspicious inbound to MySQL port 3306"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/2010937; classtype:bad-unknown; sid:2010937; rev:3; metadata:created_at 2010_07_30, updated_at 2018_03_27;)
```

Below this, a caption reads: "Snort rule for TCP scan attempt detection".

The main interface shows a table of 'RealTime Events' with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, and Event Message. The table contains several entries, with one highlighted in red:

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
ET	2	bob-virtua...	394	2019-08-22 13:44:29	10.10.10.50	50254	10.10.10.16	3306	ET SCAN Suspicious inbound to ...
ET	1	bob-virtua...	396	2019-08-22 13:44:29	10.10.10.50	47824	10.10.10.16	5907	ET SCAN Potential VNC Scan 5...
			97	2019-08-22 13:44:30	10.10.10.50	46220	10.10.10.16	5432	ET SCAN Suspicious inbound to ...
			99	2019-08-22 13:44:30	10.10.10.50	43738	10.10.10.16	1433	ET SCAN Suspicious inbound to ...
			101	2019-08-22 13:44:30	10.10.10.50	36150	10.10.10.16	5800	ET SCAN Potential VNC Scan 5...
			102	2019-08-22 13:44:31	10.10.10.50	43824	10.10.10.16	1521	ET SCAN Suspicious inbound to ...
			995	2019-08-22 14:32:39	0.0.0.0		0.0.0.0		[OSSEC] Listened ports status (...)

Below the table, a 'System Message' section shows a detailed alert for the highlighted event:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET SCAN Suspicious inbound to MySQL port 3306"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/2010937; classtype:bad-unknown; sid:2010937; rev:3; metadata:created_at 2010_07_30, updated_at 2018_03_27;)
```

Below this, a packet capture table shows the details of the detected scan attempt:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	Win	Seq
TCP	10.10.10.50	10.10.10.16	4	5	0	60	25570	2	0	64	4467	

Below the packet capture table, a 'Reverse DNS' section is visible.

A caption at the bottom reads: "Snort sends an alert when TCP scan attempt is detected".

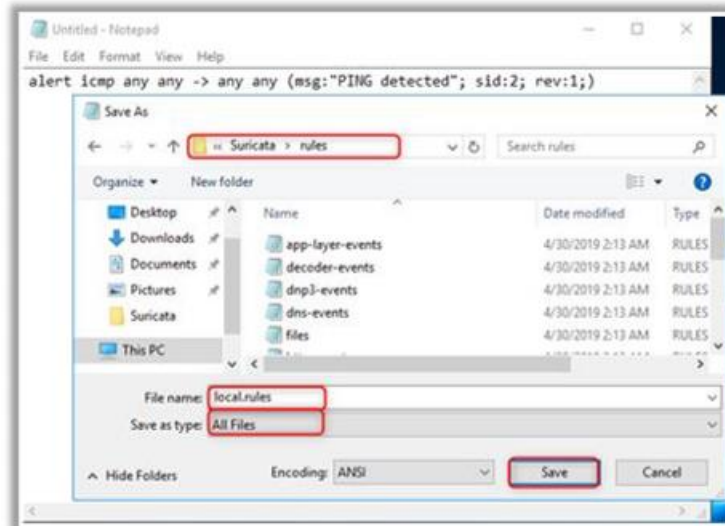
Soluciones IDS basadas en red: Zeek (Bro)

Zeek (anteriormente, Bro) es un IDS basado en el comportamiento y un marco de análisis de red que detecta anomalías en una red con fines de ciberseguridad.

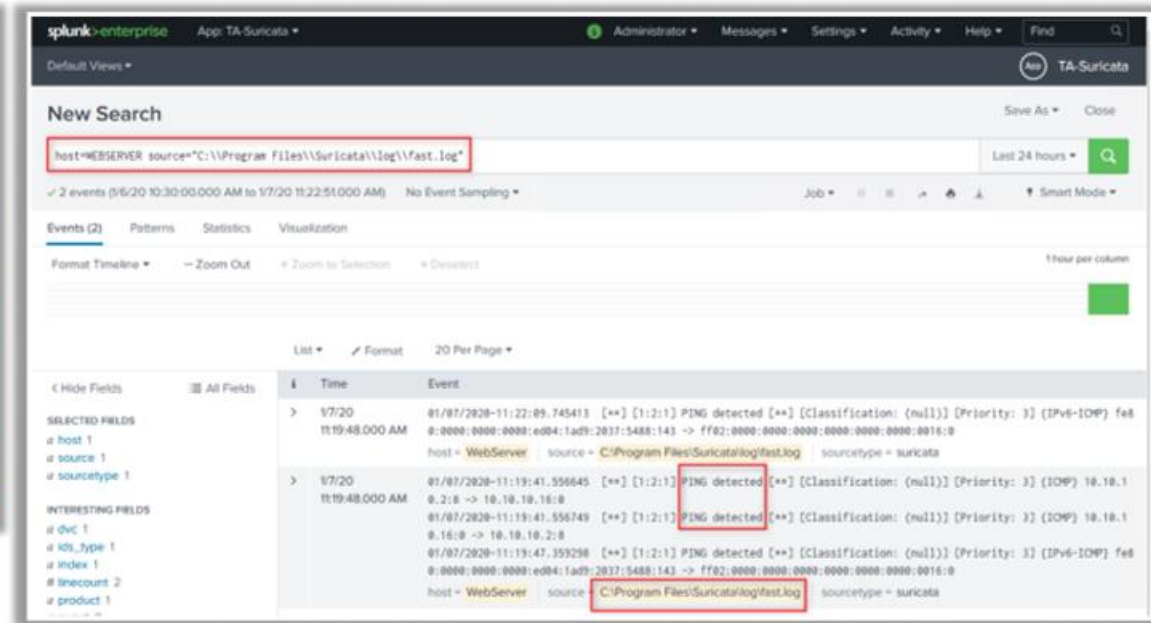


Soluciones IDS basadas en red: Suricata

Suricata es un IDS/IPS de código abierto



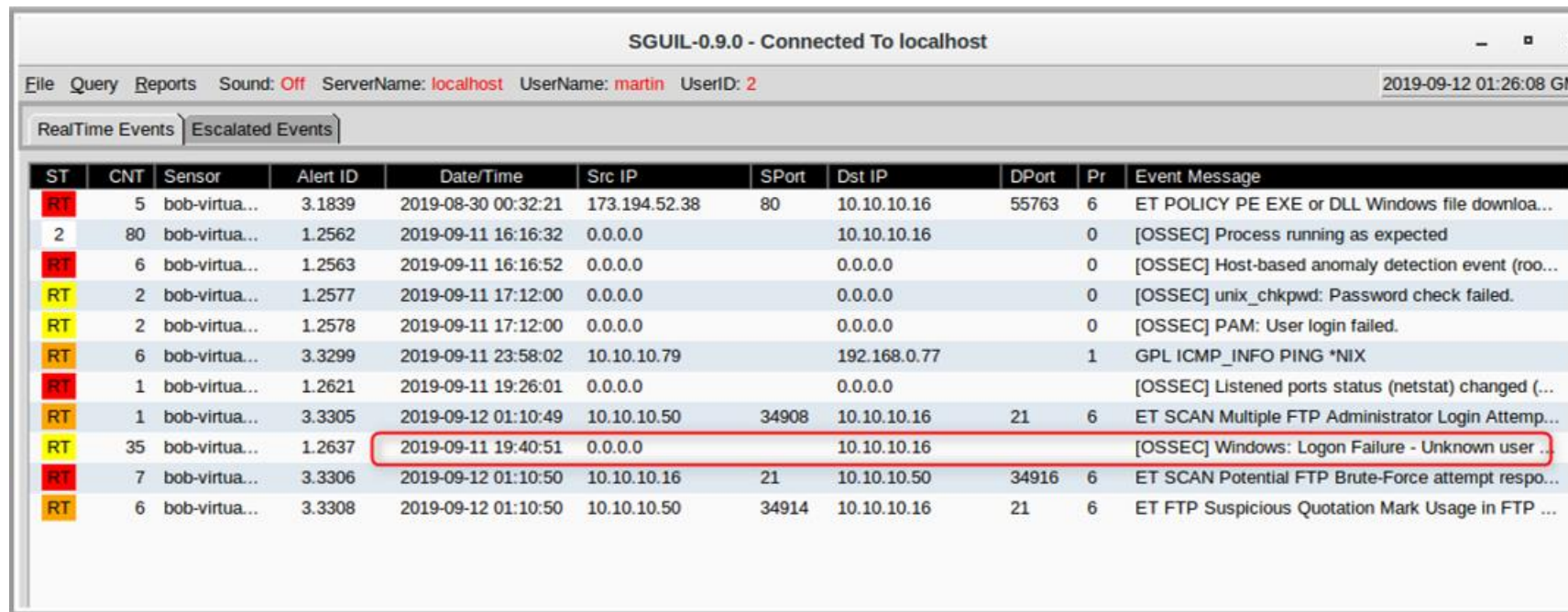
Suricata rule for PING attempt detection



PING attempt detection with Suricata

Soluciones IDS basadas en host: OSSEC

OSSEC (Open Source HIDS SECurity) es un HIDS que puede utilizarse para realizar análisis de registros, comprobaciones de integridad, supervisión del registro de Windows, detección de rootkits, alertas temporales y respuesta activa.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	bob-virtua...	3.1839	2019-08-30 00:32:21	173.194.52.38	80	10.10.10.16	55763	6	ET POLICY PE EXE or DLL Windows file downloa...
2	80	bob-virtua...	1.2562	2019-09-11 16:16:32	0.0.0.0		10.10.10.16		0	[OSSEC] Process running as expected
RT	6	bob-virtua...	1.2563	2019-09-11 16:16:52	0.0.0.0		0.0.0.0		0	[OSSEC] Host-based anomaly detection event (roo...
RT	2	bob-virtua...	1.2577	2019-09-11 17:12:00	0.0.0.0		0.0.0.0		0	[OSSEC] unix_chkpwd: Password check failed.
RT	2	bob-virtua...	1.2578	2019-09-11 17:12:00	0.0.0.0		0.0.0.0		0	[OSSEC] PAM: User login failed.
RT	6	bob-virtua...	3.3299	2019-09-11 23:58:02	10.10.10.79		192.168.0.77		1	GPL ICMP_INFO PING *NIX
RT	1	bob-virtua...	1.2621	2019-09-11 19:26:01	0.0.0.0		0.0.0.0			[OSSEC] Listened ports status (netstat) changed (...)
RT	1	bob-virtua...	3.3305	2019-09-12 01:10:49	10.10.10.50	34908	10.10.10.16	21	6	ET SCAN Multiple FTP Administrator Login Attemp...
RT	35	bob-virtua...	1.2637	2019-09-11 19:40:51	0.0.0.0		10.10.10.16			[OSSEC] Windows: Logon Failure - Unknown user ...
RT	7	bob-virtua...	3.3306	2019-09-12 01:10:50	10.10.10.16	21	10.10.10.50	34916	6	ET SCAN Potential FTP Brute-Force attempt respo...
RT	6	bob-virtua...	3.3308	2019-09-12 01:10:50	10.10.10.50	34914	10.10.10.16	21	6	ET FTP Suspicious Quotation Mark Usage in FTP ...

Soluciones IDS basadas en host: Wazuh

Wazuh es un sistema de detección de intrusiones basado en host.

Realiza análisis de registros, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa

Wazuh nació como una bifurcación de OSSEC HIDS

