SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.9.0. Capítulo 9

Implantación y configuración de cortafuegos

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Para reducir el riesgo de las amenazas lógicas al sistema de información, se deben robustecer los puntos de acceso al sistema.

El punto de interconexión de la red privada de la empresa con internet, es el primer punto que se debe proteger, ya que es la entrada desde el exterior al sistema de información.

Los cortafuegos permiten la separación física de la red en diferentes tramos o zonas, para lo cual dispondrán normalmente de al menos dos tomas de red que les permitan interrumpir la misma, desempeñando la función de punto de interconexión único.

Los cortafuegos no solo protegen de una amenaza externa, sino que permiten definir subredes internas protegidas de ellas mismas.

2. TIPOS DE CORTAFUEGOS

La norma ISO 17799:2005 establece explícitamente controles relacionados con la implantación y uso de sistemas que separen las redes de comunicaciones.

En concreto, el objetivo de control "11.4 Control de acceso a la red", persigue evitar el acceso no autorizado a la red, para lo cual establece, entre otras medidas, que deben existir sistemas apropiados para la interconexión entre la red de la empresa, y las redes de otras empresas o las redes públicas.

También el Esquema Nacional de Seguridad, dispone en la medida técnica "5.4.1 Perímetro seguro", que se dispondrá 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.

2.1. TIPOS DE ATAQUES

Los tipos de amenazas lógicas se dividen tradicionalmente en cuatro tipos:

- **Ataque de interrupción,** consistente en que un objeto del sistema no esté disponible.
- **Ataque de interceptación,** consistente en que una persona o programa consiga tener un acceso no autorizado a un objeto del sistema.
- **Ataque de modificación,** consistente en que, además de lograr interceptar un objeto, se logre modificarlo; lo que puede incluir la destrucción completa y por tanto la interrupción.
- **Ataque de fabricación,** consistente en que se realice una modificación para conseguir un objeto similar al atacado, de forma que sea difícil distinguir entre el objeto original y el fabricado.

2.2. TIPOS DE CORTAFUEGOS

Cortafuegos o firewall: Dispositivo que se intercala entre dos redes para filtrar el tráfico entre ellas.

Se pueden definir subredes dentro de la empresa, y se pueden aislar mediante firewalls; por ejemplo, puede haber una subred para aquellos equipos que contienen información confidencial, y otra subred para el resto de equipos.

Los cortafuegos permiten implementar determinados aspectos de la política de seguridad de la empresa, y son un sistema fundamental para la seguridad lógica.

2.2. TIPOS DE CORTAFUEGOS

En función de la capa OSI donde actúa, existen:

Firewalls a nivel de red, que actúan exclusivamente a este nivel, y por lo tanto están constituidos por encaminadores o router.

Firewall a nivel de aplicación, denominados **proxy,** permite acceso controlado a las aplicaciones.

2.2. TIPOS DE CORTAFUEGOS

Según el método de protección que se aplique:

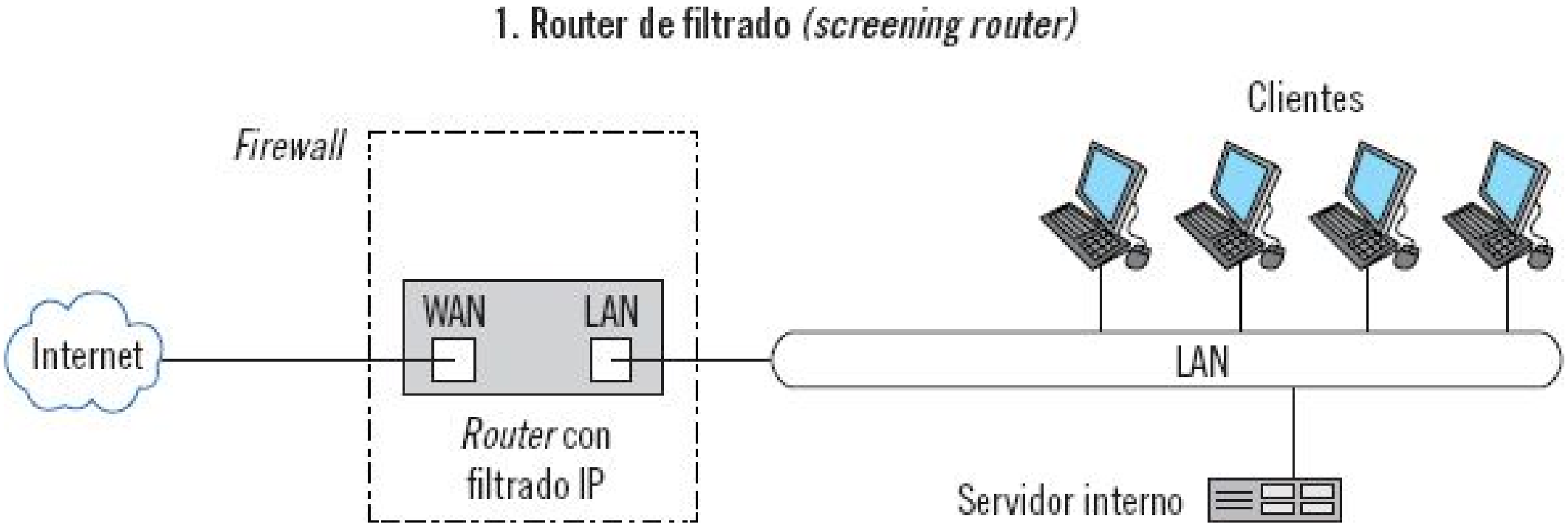
- **Protección mediante filtrado de paquetes (este es el único método de protección que pueden aplicar los firewall de red), que puede realizarse de dos maneras:**
  - **Filtrado estático de paquetes.**
  - **Filtrado dinámico de paquetes.**
- **Protección mediante servidores proxy:**
  - **Proxy de aplicación, que permiten o no la conexión a una aplicación (HTTP, FTP, SMTP).**
  - **Proxy a nivel de circuito, que crean un canal de comunicación entre el cliente y el servidor.**

- ***Definición de Proxy: elemento que se interpone entre dos segmentos de redes de computadores, para filtrar los servicios que se pueden pedir de un segmento a otro, y convertir en su caso direcciones identificativas de red.***
- ***Definición de Servidor proxy: elemento cortafuegos que gestiona el tráfico con internet entrante y saliente de una red de área local, y que puede proporcionar otras funciones, como el almacenamiento en caché de las URL más visitadas.***

2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Router de filtrado (screening router)

Los encaminadores o router habitualmente permiten definir reglas para bloquear el tráfico entrante o saliente según las direcciones, por lo tanto, son el mecanismo más sencillo y económico.



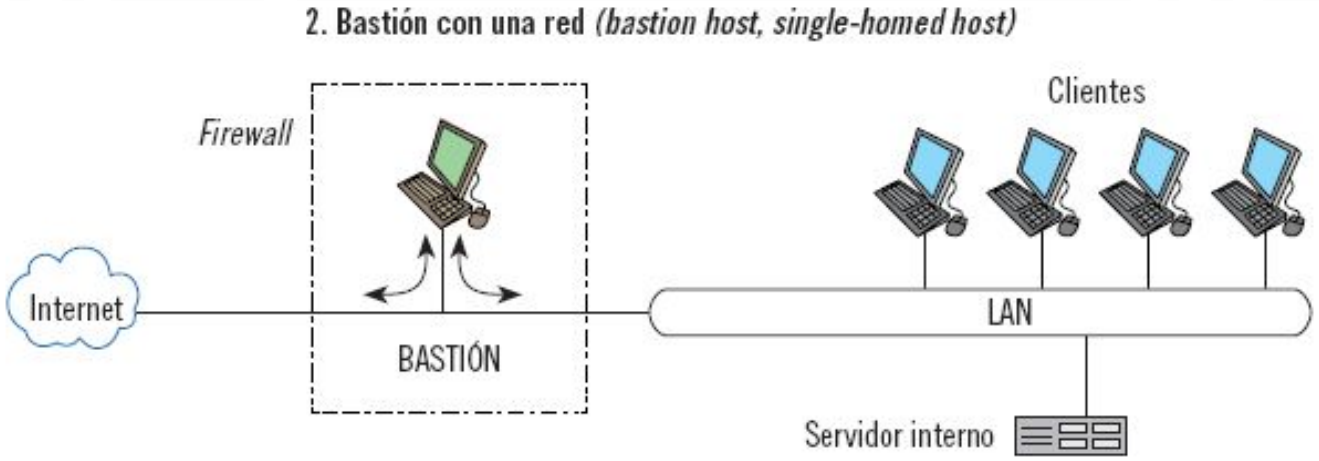
2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Bastión con una red (bastion host o single-homed host)

En esta ocasión, se emplea una estación de trabajo robustecida o bastionada, para proteger toda la red, filtrando el tráfico al funcionar como una pasarela o puerta de enlace de aplicación.

Debe deshabilitarse el envío directo del tráfico IP interno al externo (IP forwarding), bloqueándose por defecto que pase todo el tráfico.

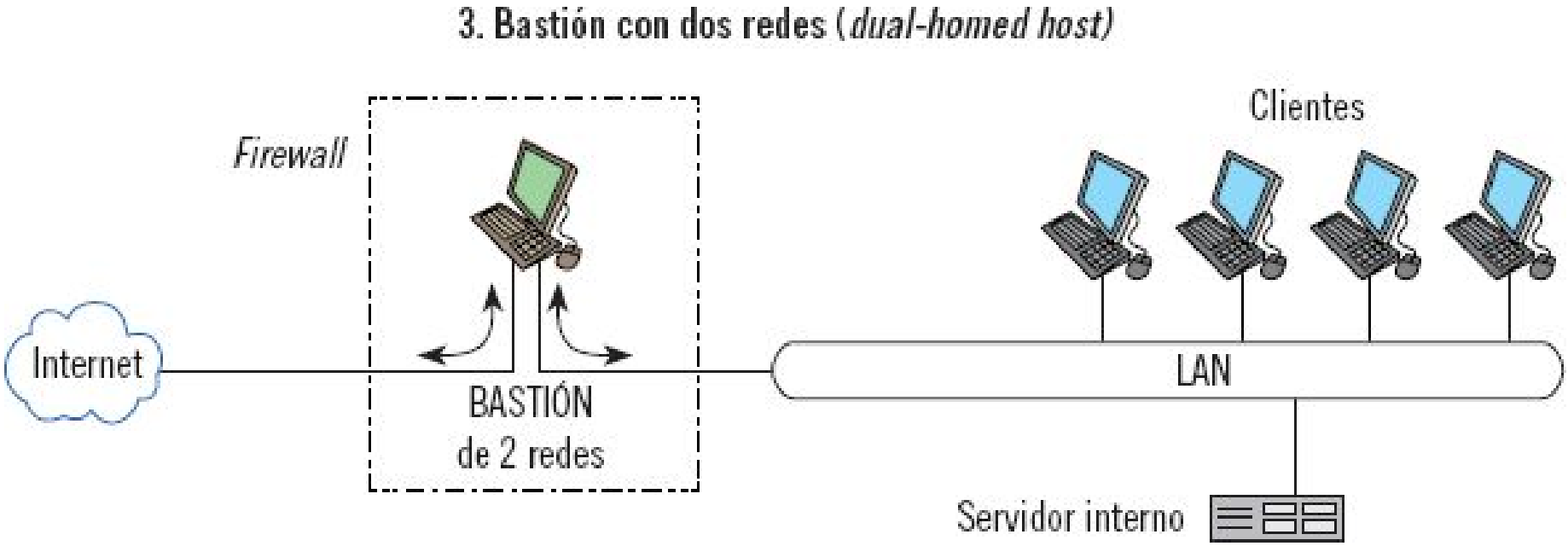
Entre las desventajas, cabe señalar que al compartir la única tarjeta de red, no hay separación física entre la red sin proteger y la red protegida.



2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Bastión con dos redes (dual-homed host)

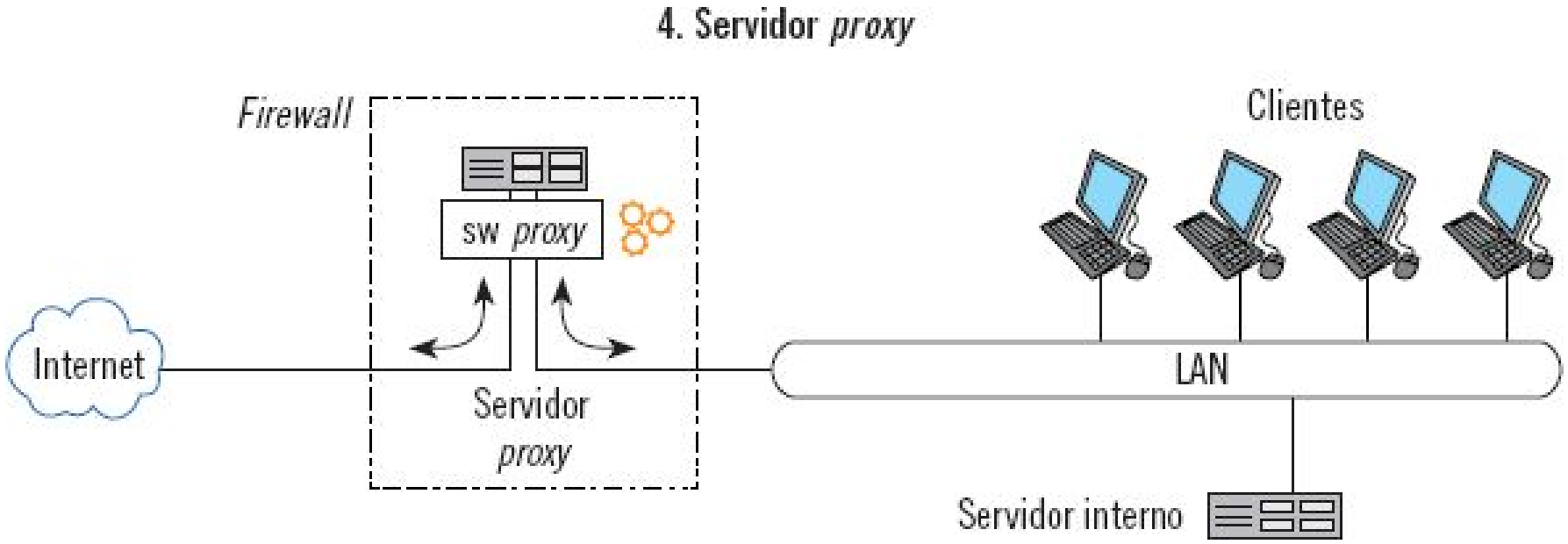
Se hace que el bastión incorpore 2 tarjetas de red: la externa, conectada a internet, y la interna, conectada a la LAN.



2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Servidor proxy

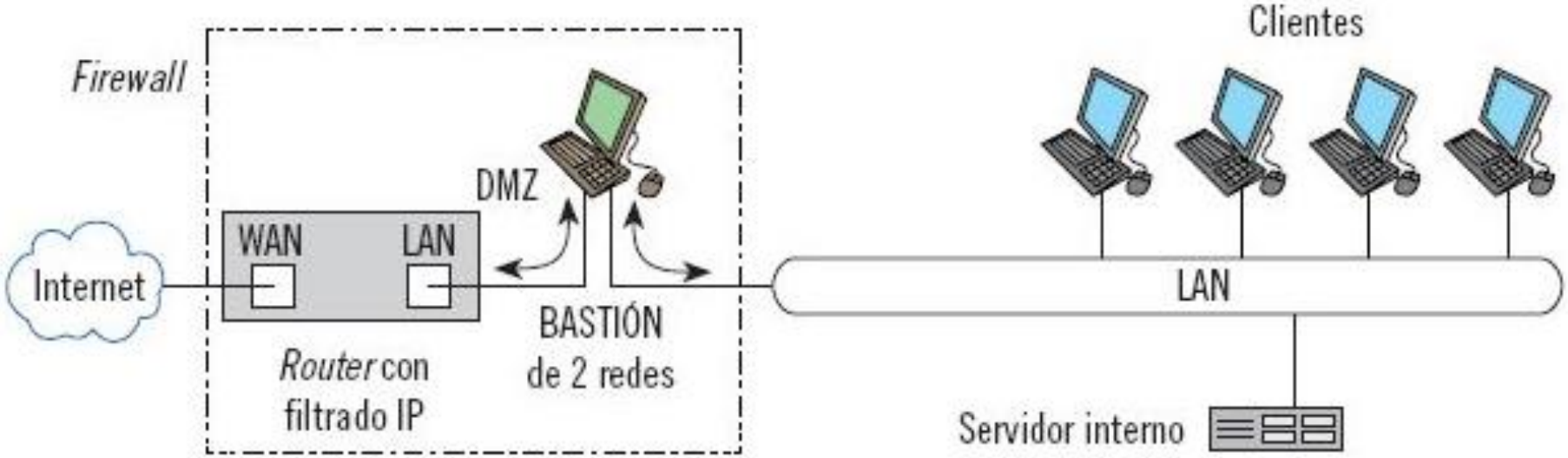
Una petición web dirigida a un cortafuegos no es reencaminada directamente hacia el servidor final, sino que es atendida por el servidor proxy que incorpora el firewall, y a la vez el servidor proxy del firewall dirige la petición al servidor real.



2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Bastión filtrado (screened host)

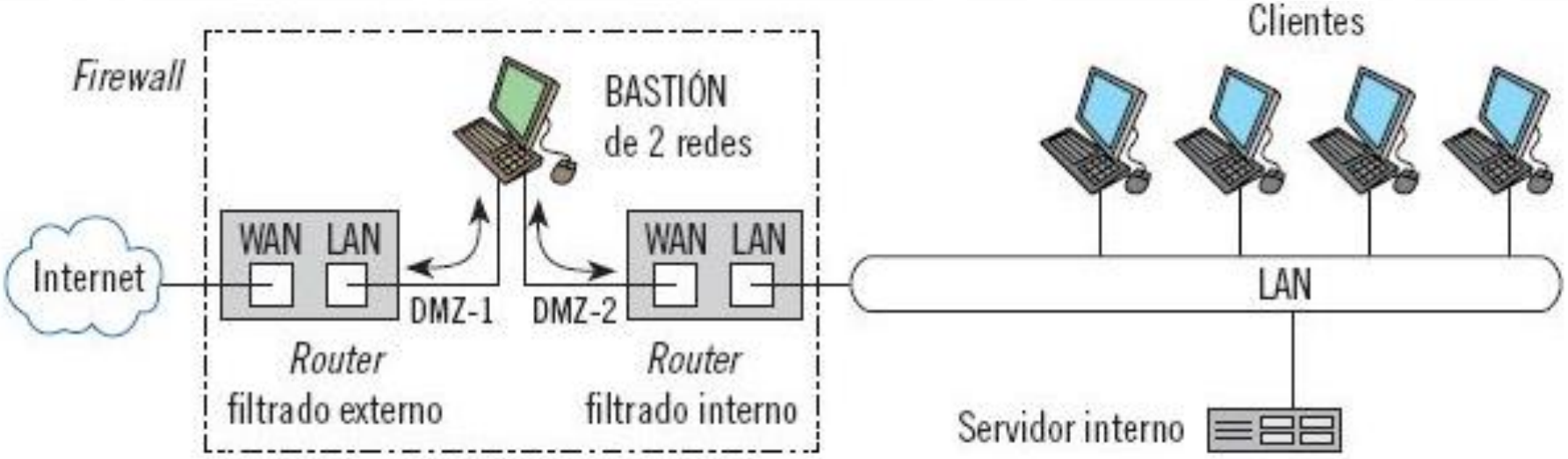
Se emplea un bastión al que se le antepone un equipo que realice el filtrado de paquetes de red, normalmente un router. El router se configura ahora para que solo admita ciertas conexiones o tipos de tráfico hacia el bastión, de manera que solo envíe el tráfico de internet, una vez filtrado, hacia el bastión. También se configura para que solo admita conexiones internas desde el bastión.



2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Subred filtrada (screened subnet)

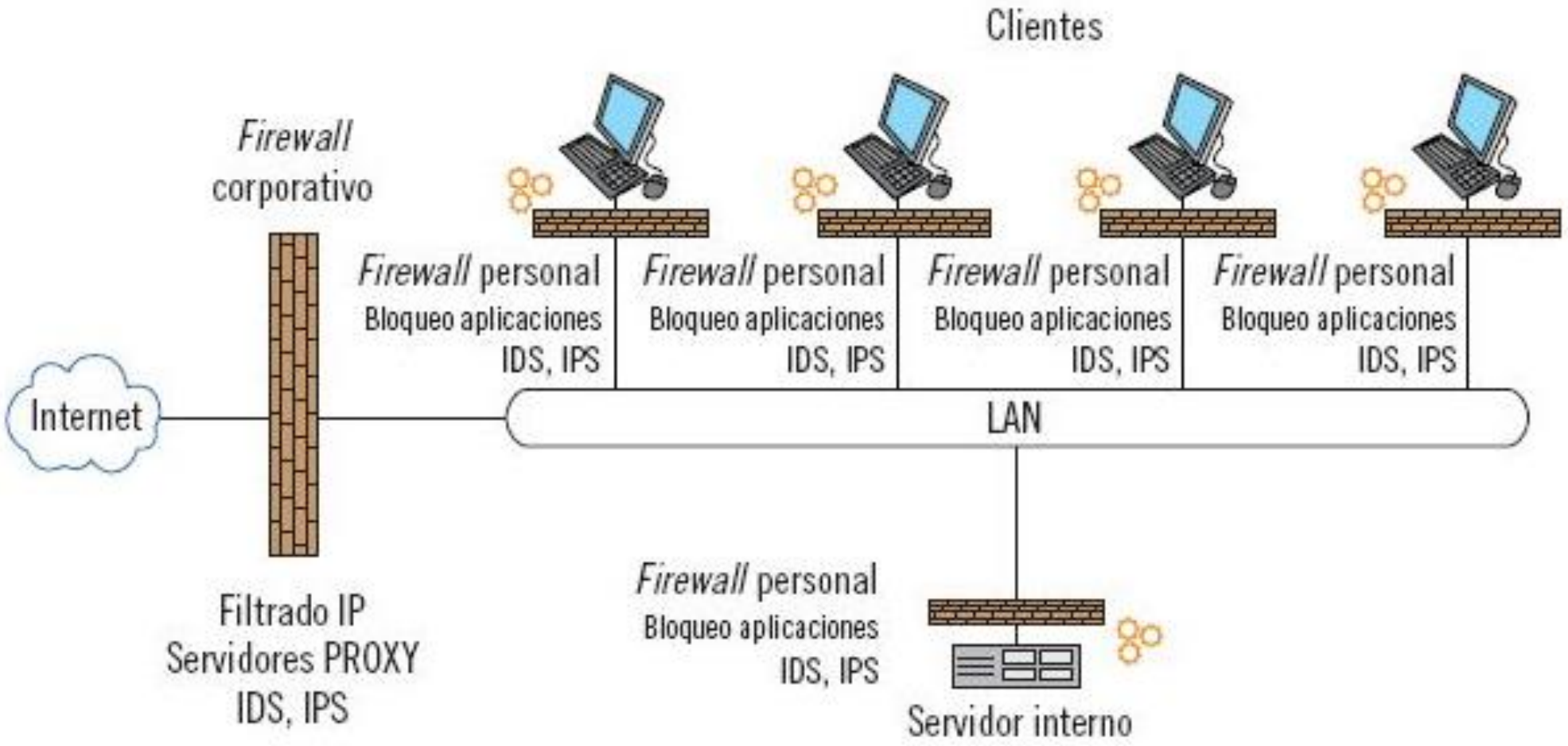
Esta es la configuración más segura, porque el bastión se separa de la red interna mediante un segundo equipo de filtrado de paquetes (generalmente un router de filtrado interno, o un firewall que solo emplee filtrado de red).

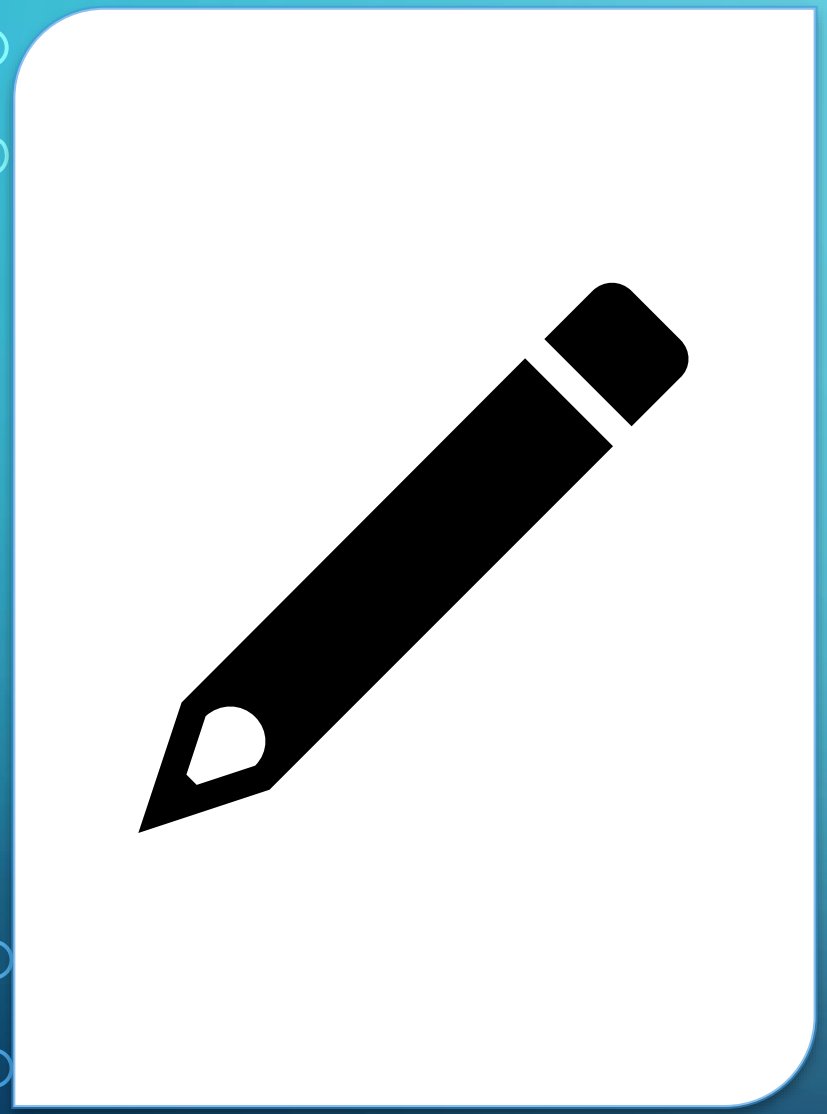


2.3. CONSTRUCCIÓN DE CORTAFUEGOS

Firewalls personales

7. Cortafuegos personal

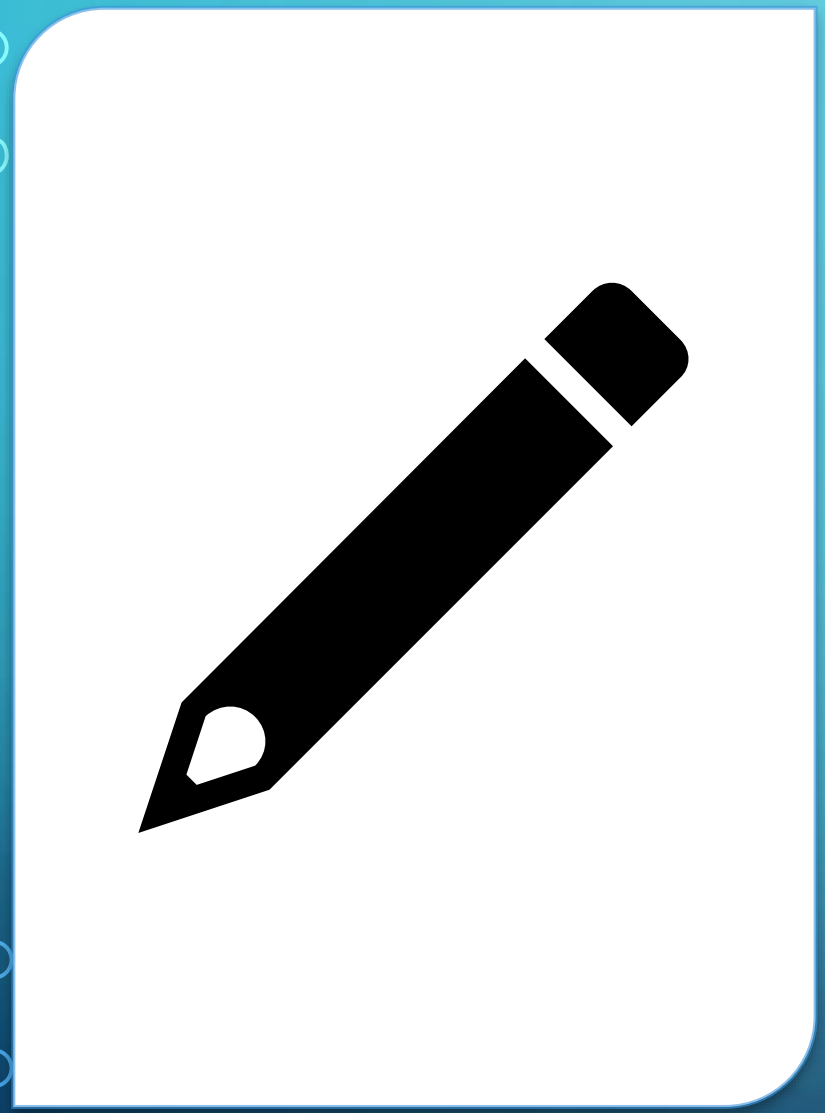


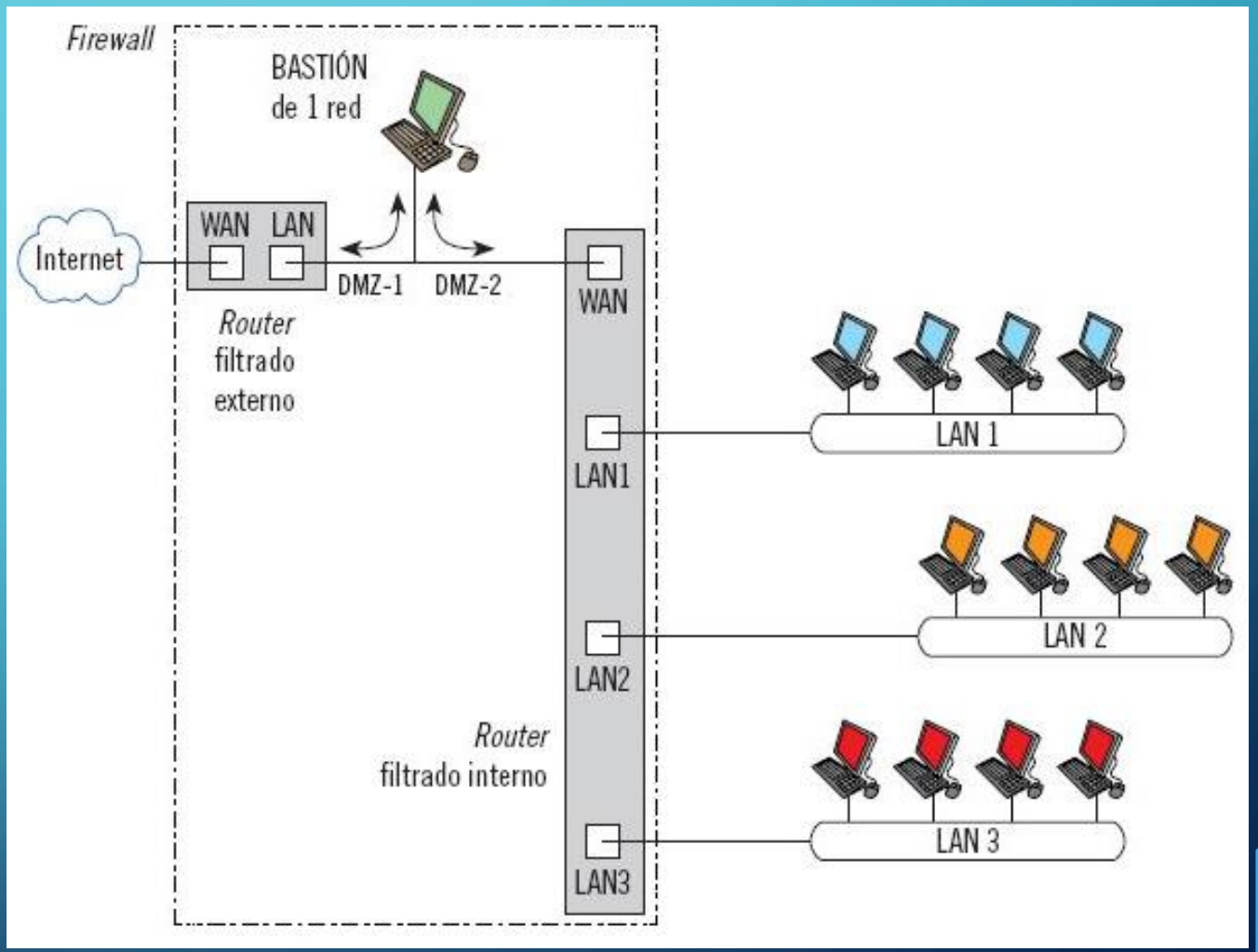


Actividades

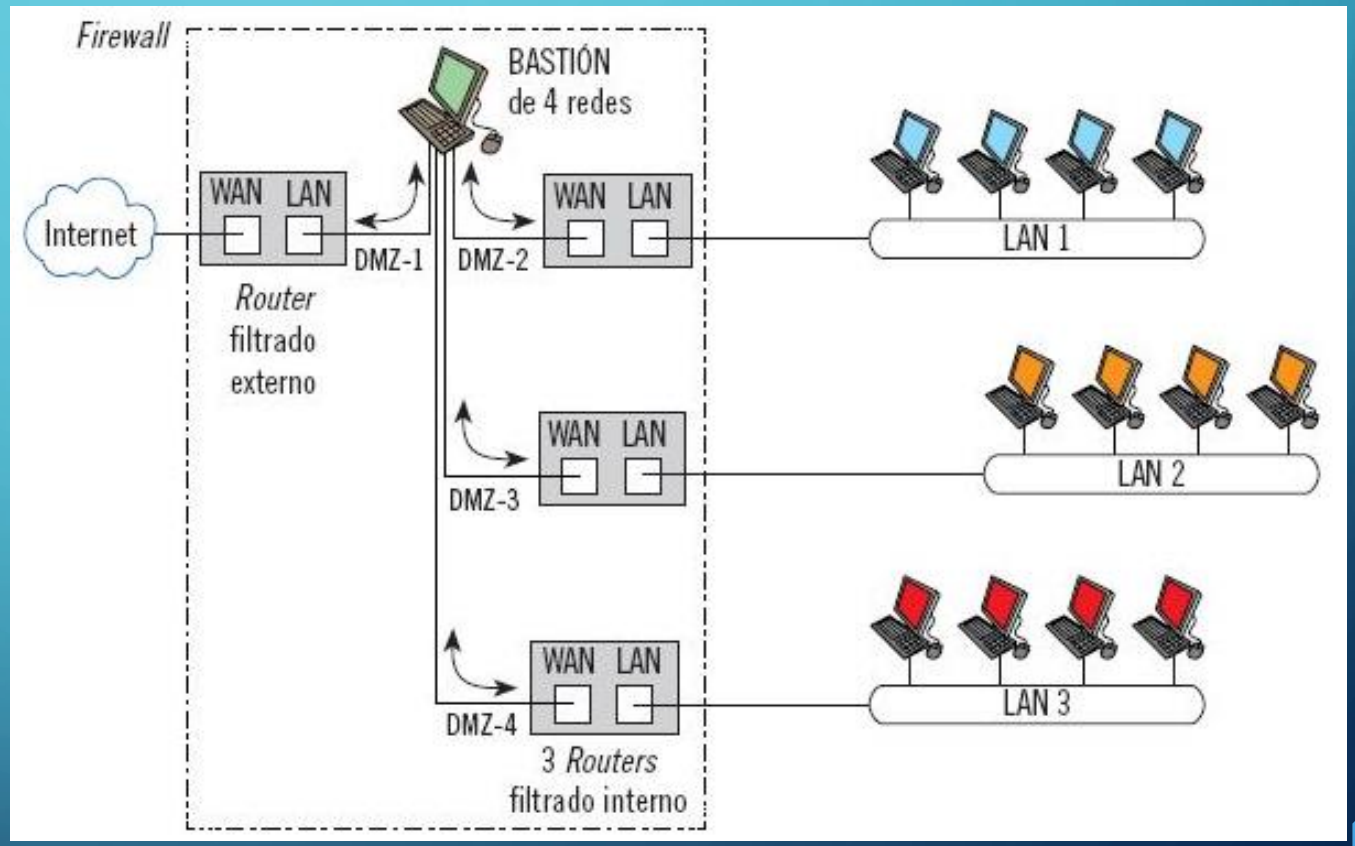
DIBUJAR EL DIAGRAMA DE RED DE UN FIREWALL CONSTRUIDO CON SUBRED FILTRADA, EN EL QUE SE NECESITAN PROTEGER TRES SUBREDES PRIVADAS DIFERENTES, QUE DEBEN MANTENERSE FÍSICAMENTE SEPARADAS.

Actividades





Actividades



3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES

La norma ISO 17799:2005 establece en el control "11.4.5 segregación en redes", que los grupos de servicios de información, usuarios, y sistemas de información debieran ser segregados en subredes.

Para ello, se recomienda dividir la red en dominios de red lógicos:

- **La política de control de accesos.**
- **El coste de estas medidas, en términos materiales y de horas de trabajo necesarios para la necesaria monitorización de estos dispositivos.**
- **El valor y clasificación de la información almacenada o procesada.**
- **Separar diferentes áreas de negocio, o diferentes líneas comerciales, reduciendo el impacto que un incidente en una subred tendría en otra subred. Por ejemplo, separar sistemas de producción, separar compras y ventas, separar redes de oficina, separar redes de control industrial, separar las redes de datos confidenciales, etc.**
- **Debe tenerse en cuenta la separación de redes inalámbricas.**

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES

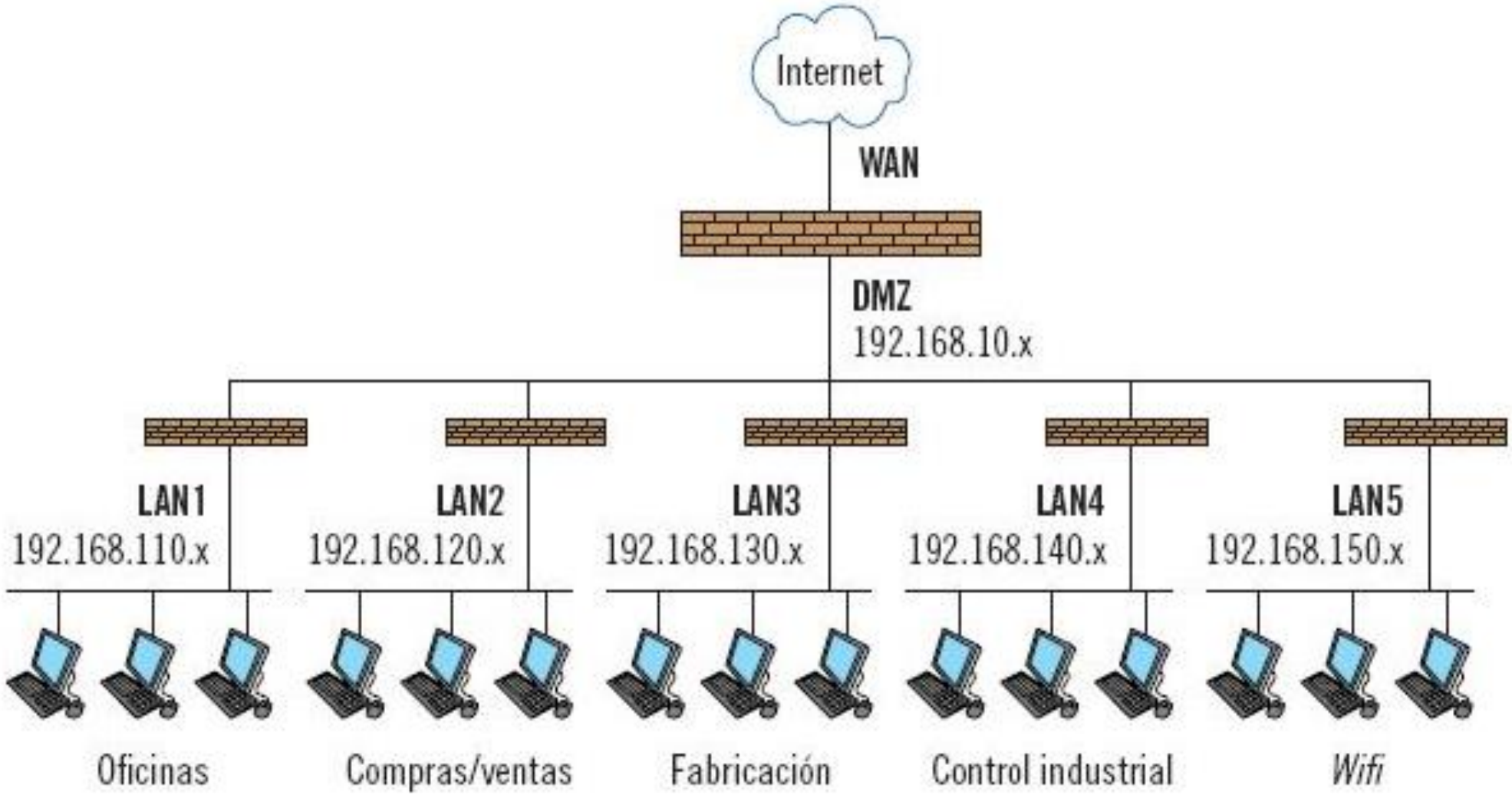
El Esquema Nacional de Seguridad, dispone la medida 5.4.4, referente a la segregación de redes, para acotar el acceso a la información, y por lo tanto la propagación de incidentes de seguridad.

Indica además que debe segregarse empleando medidas que garanticen:

- **El control de entrada de los usuarios que llegan a cada segmento**
- **El control de salida de la información disponible en cada segmento**
- **Los medios físicos y lógicos que se empleen para segmentar la red deben estar particularmente asegurados, mantenidos y monitorizados, como en el caso de los firewalls de acceso a internet.**

3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES

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



3.1. USO DE ZONAS DESMILITARIZADAS

Las zonas DMZ añaden seguridad, porque aumentan la separación entre redes.

Por ejemplo, el rango de direcciones IP, empleado en la zona DMZ será diferente al rango de direcciones de la red privada, lo que aumenta la dificultad para acceder a la red privada.

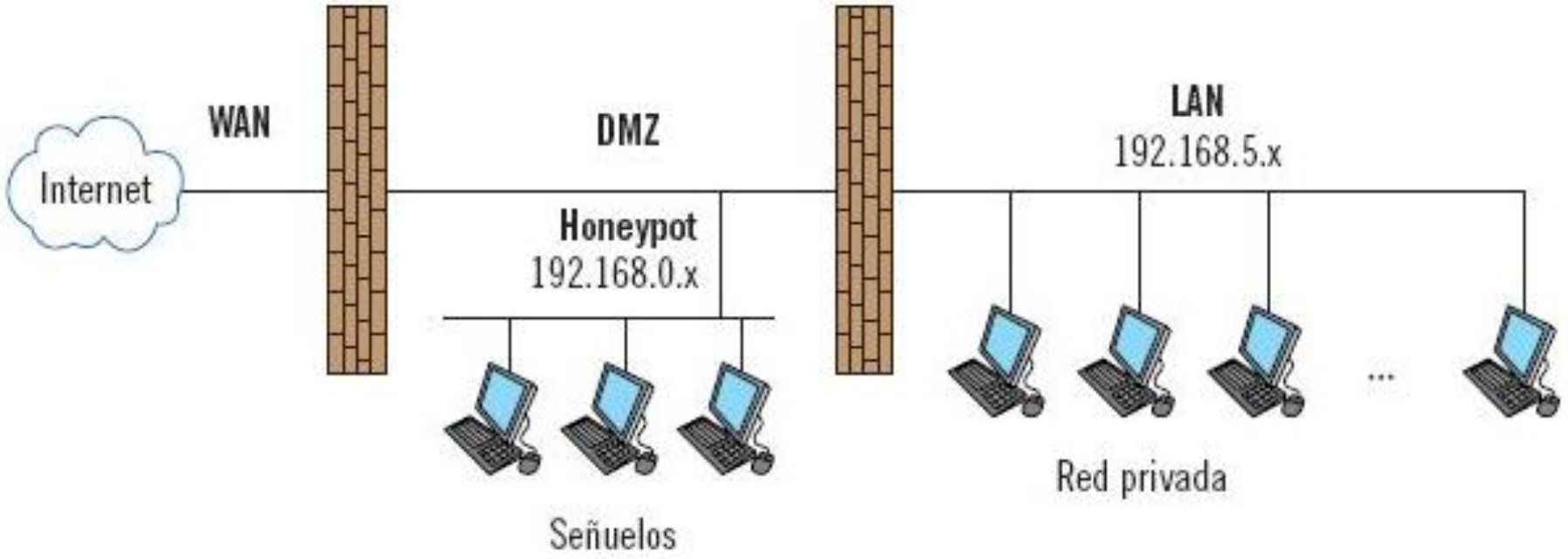
Habitualmente, se pueden obtener más beneficios de las zonas DMZ, empleándolas para diferentes servicios.

3.1. USO DE ZONAS DESMILITARIZADAS

Redes falsas o honeypots

Consisten en un conjunto de máquinas intencionadamente vulnerables que simulan una red privada normal, de manera que un atacante que ganara acceso a la DMZ, pensaría que ya está en la red privada.

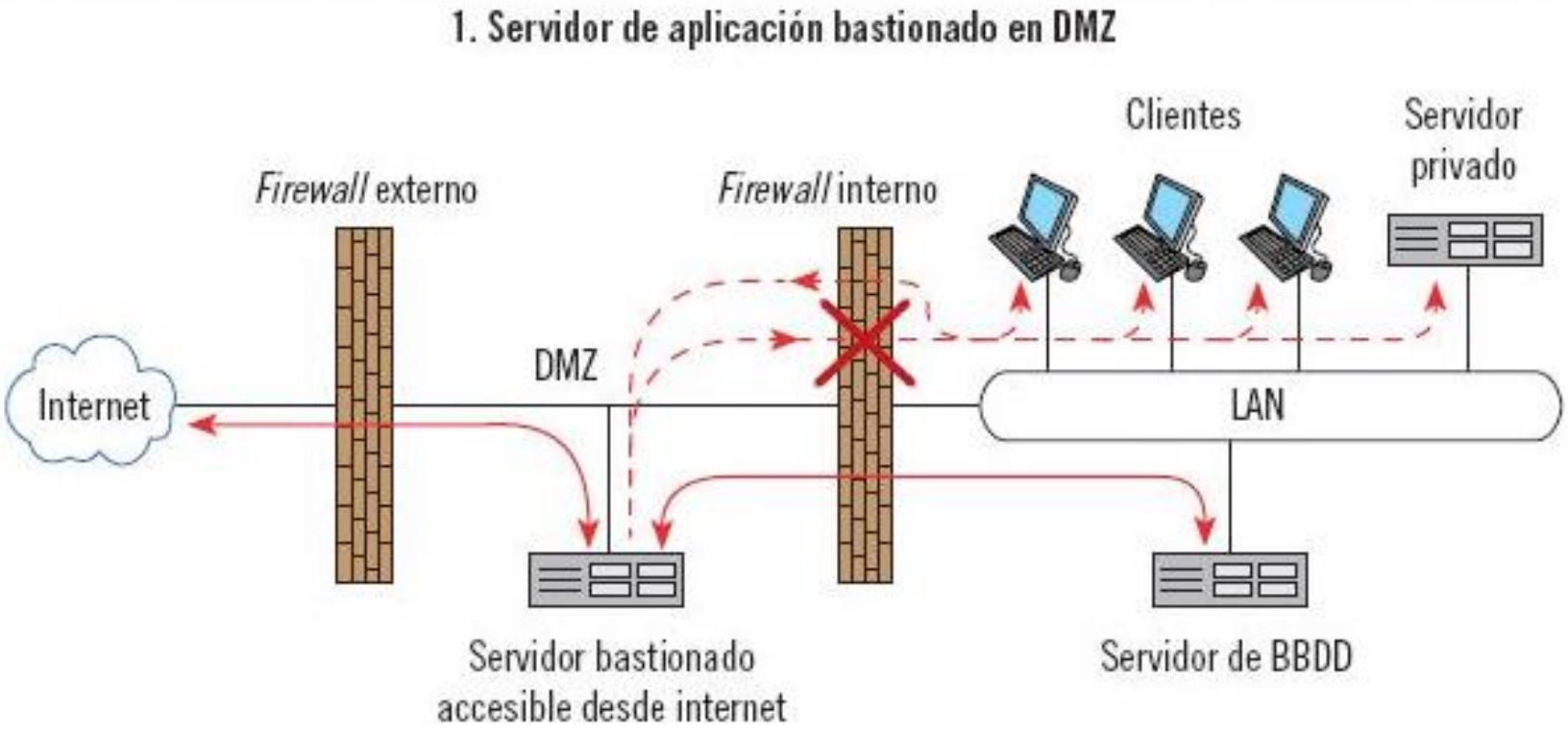
Redes falsas, redes señuelo o *honeypots*



3.1. USO DE ZONAS DESMILITARIZADAS

Ubicación de servidores accesibles desde el exterior

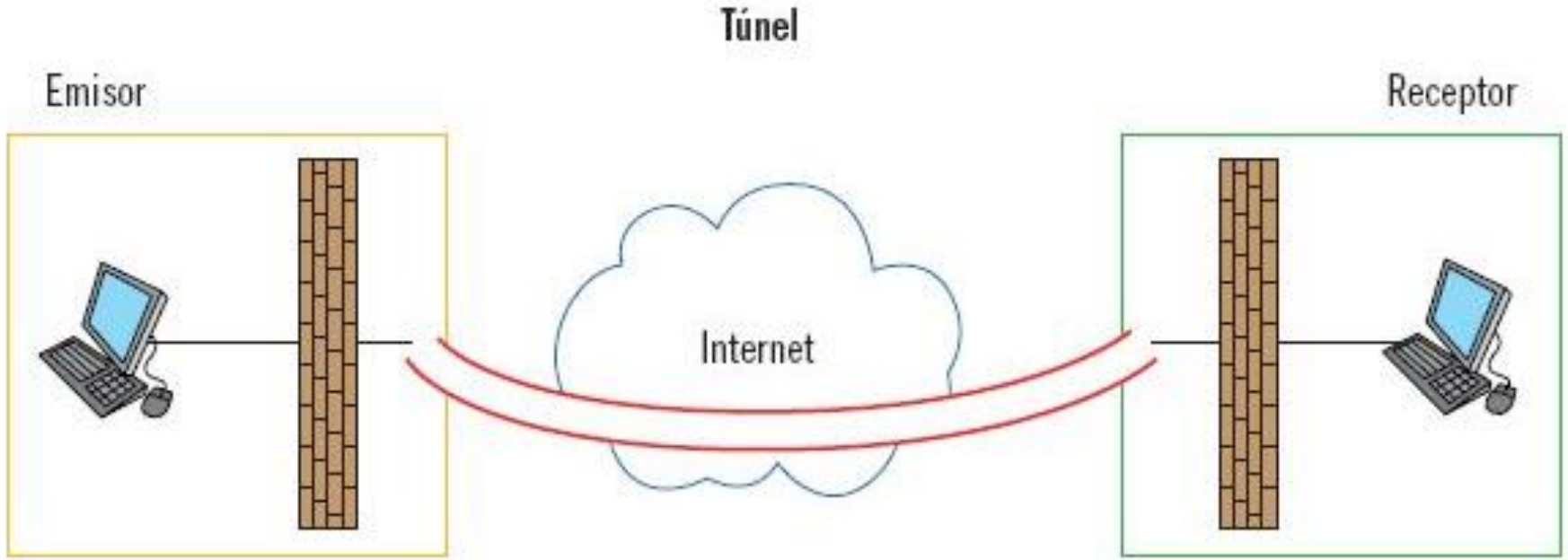
Los servidores accesibles desde internet se deben ubicar en zona DMZ siempre que sea posible.



4. CANALES SEGUROS DE COMUNICACIONES

Si se quiere que las comunicaciones entre dos sucursales distintas de la empresa sean seguras, se pueden emplear diversas soluciones:

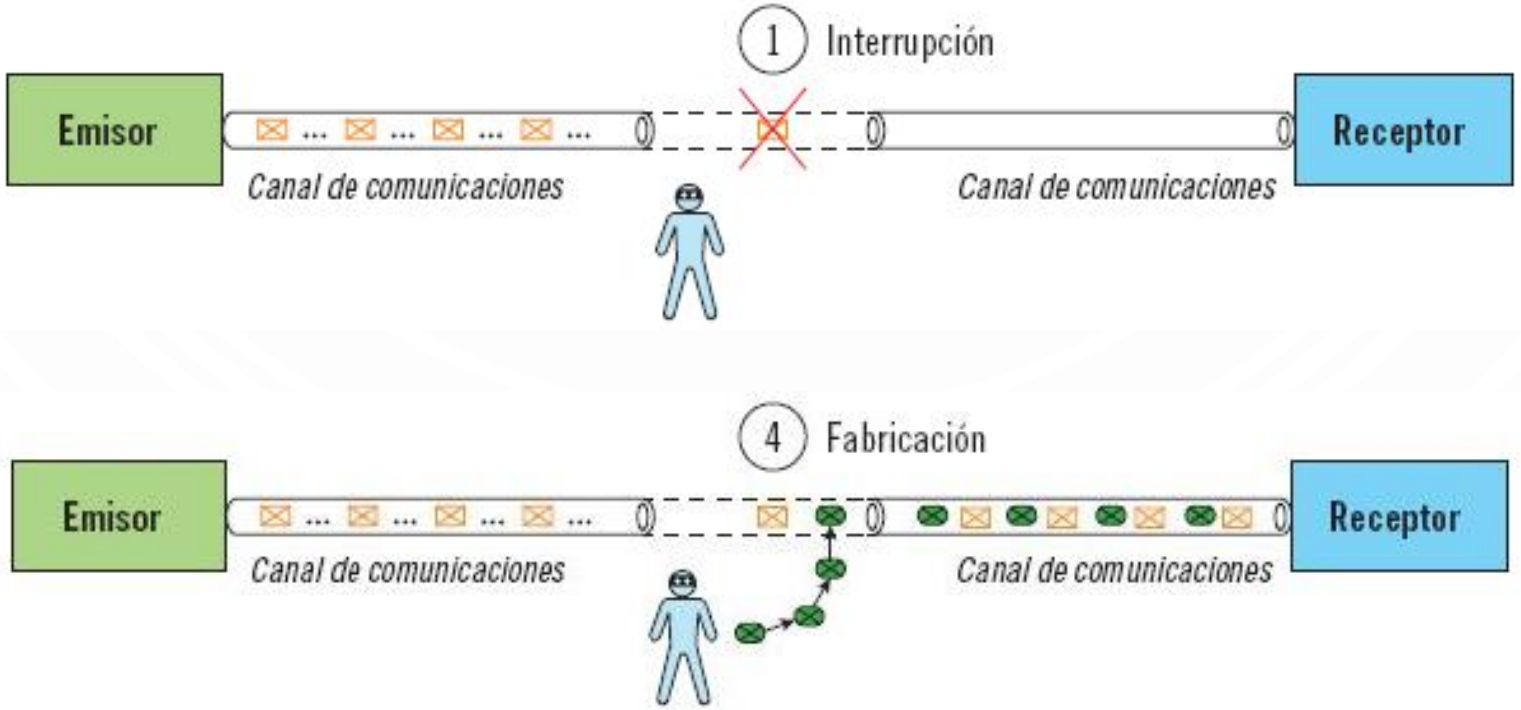
- Emplear líneas de comunicaciones propias de la empresa.
- Alquilar enlaces a operadores de telecomunicaciones.
- Utilizar una red privada virtual (VPN) a través de medios inseguros (Internet).



4.1. ATAQUES DE INTERRUPCIÓN Y ATAQUES DE FABRICACIÓN

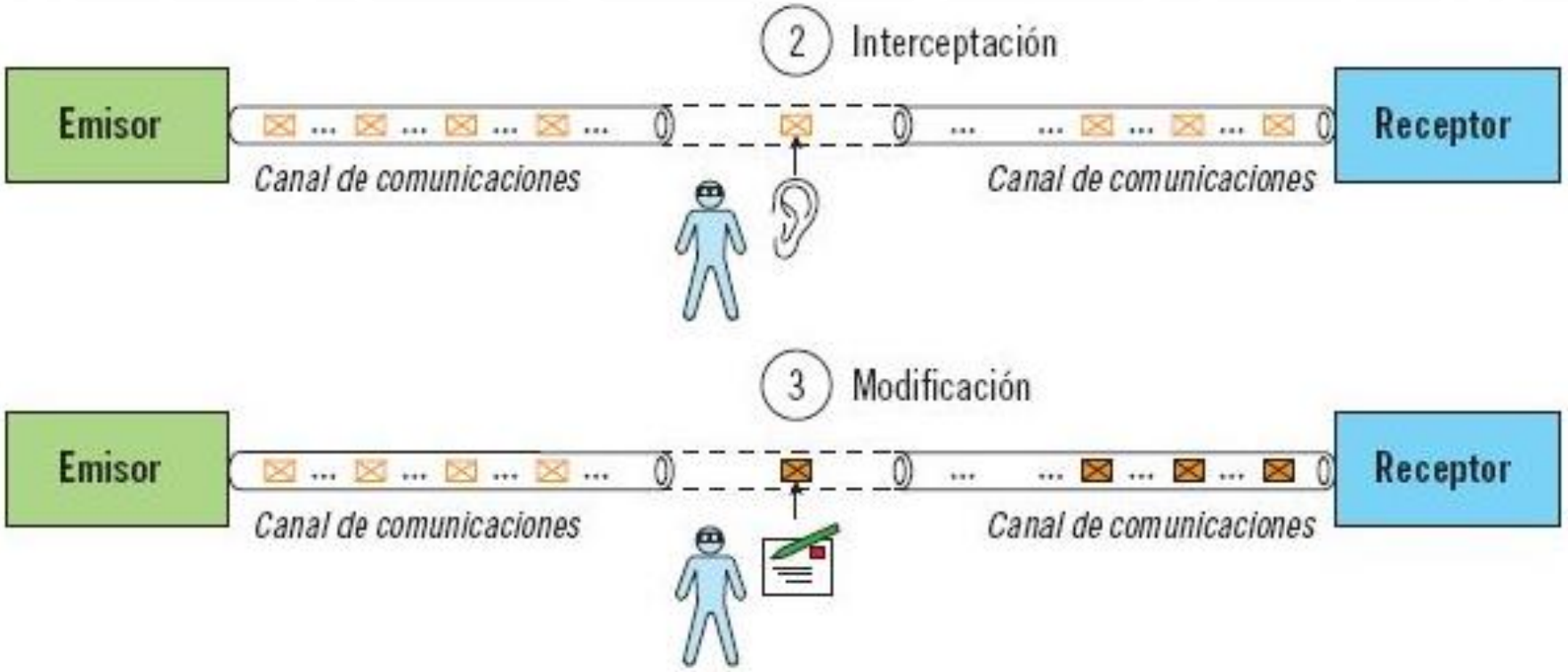
Ante un ataque de interrupción, se busca asegurar la disponibilidad de las comunicaciones principalmente mediante redundancia de servicios.

Ante un ataque de fabricación, mediante equipos intermedios con capacidad de detección.



4.2. ATAQUES DE INTERCEPTACIÓN Y ATAQUE DE MODIFICACIÓN

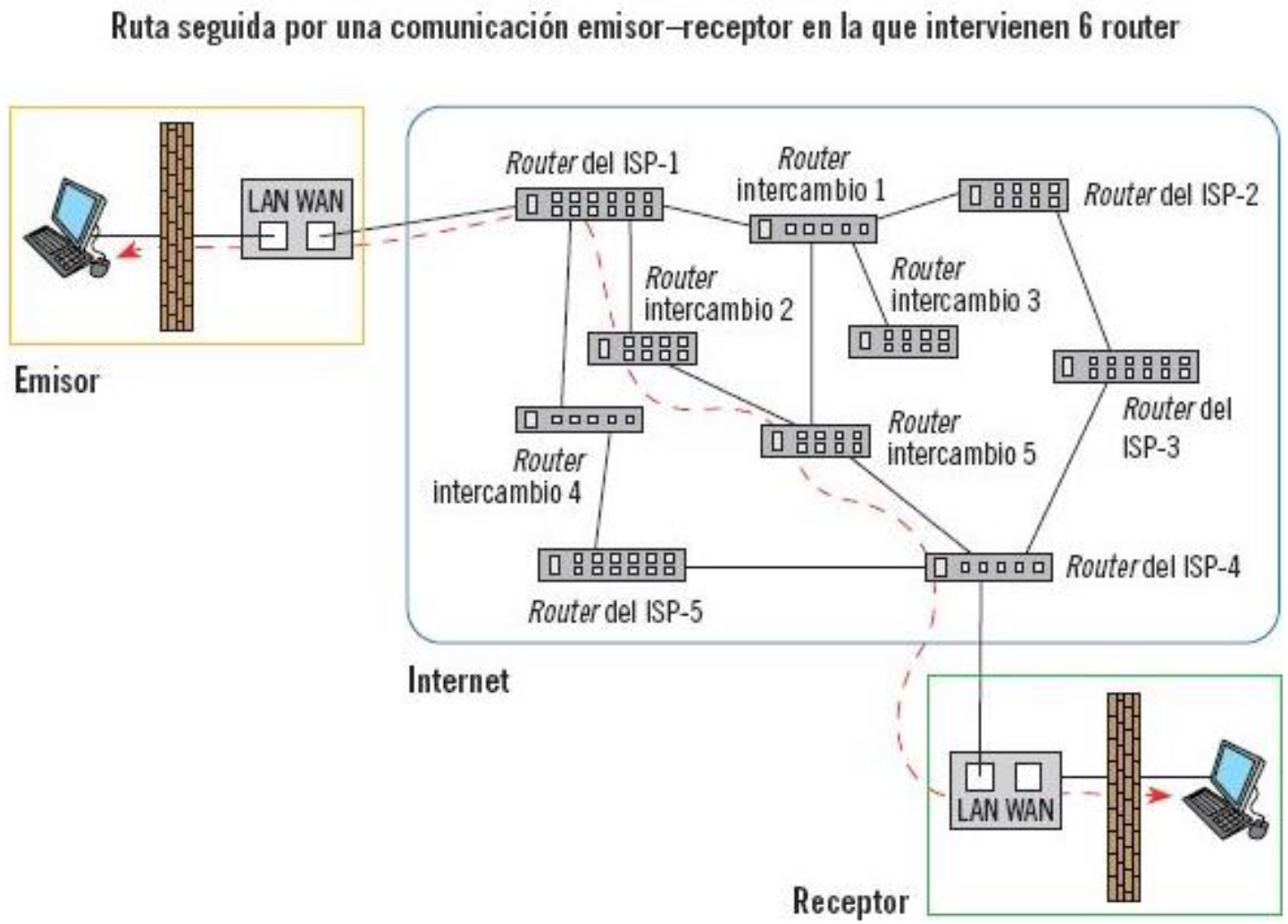
Se busca asegurar la confidencialidad e integridad de las comunicaciones, de manera que, aunque se disponga de acceso al canal de comunicaciones, la información no sea legible para un destinatario no autorizado, y la modificación de los mensajes en tránsito sea convenientemente detectada por el destinatario: criptografía y firmas digitales.



4.3. CRIPTOGRAFÍA EN COMUNICACIONES TCP/IP

Las comunicaciones TCP/IP a través de internet precisan de una serie de saltos entre nodos de comunicaciones, para encaminar los paquetes desde el emisor hasta el receptor.

Estos nodos intermedios son encaminadores o router, es decir, elementos de la capa de red que necesitan saber la dirección IP destino de cada paquete, para encaminarlo y que logre alcanzar su destino.

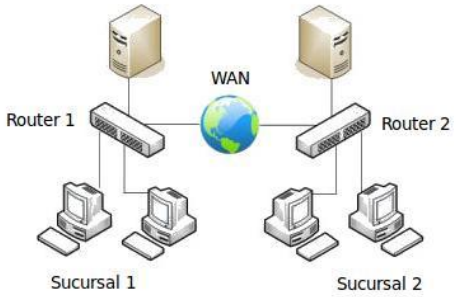


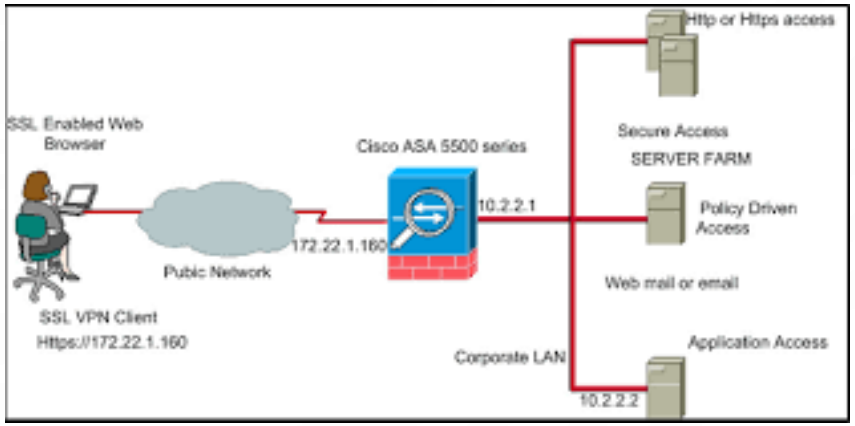
4.4. PROTOCOLOS VPN

Las redes privadas virtuales (VPN) proporcionan una conexión segura a través de redes públicas no seguras, aunando el uso de criptografía, mecanismos de autenticación, y la encapsulación de protocolos.

El resultado final es que se logra extender la red privada sobre una red pública sin problemas de seguridad, de manera que un usuario que emplee VPN para conectarse a la red privada de su empresa, logra operar a todos los efectos, como si su estación de trabajo estuviera en la red privada de la empresa.

- VPN punto a punto, para conectar diferentes oficinas de una misma empresa.
- VPN de acceso remoto, para permitir el teletrabajo sin comprometer la seguridad.





4.4. PROTOCOLOS VPN

Para constituir una red privada virtual, ambos extremos deben emplear el mismo protocolo:

- **PPTP (Point to Point Tunneling Protocol)**
- **L2TP (Layer 2 Tunneling Protocol)**
- **IPsec (IP Security)**

4.4. PROTOCOLOS VPN.

PPTP (Point to Point Tunneling Protocol)

Antiguo

Opera en el nivel de enlace (capa 2 del modelo OSI), de manera que se emplea cifrado nodo a nodo.

Se apoya en el protocolo PPP (Point to Point Protocol)

La autenticación se realiza mediante el protocolo CHAP (Microsoft Challenge Handshake Authentication Protocol), que emplea el algoritmo MD4 para asegurar la integridad de la información, y el algoritmo RCA para asegurar la confidencialidad. El algoritmo de encriptación empleado se considera débil, por lo que está prácticamente en desuso, y no es recomendable usar VPN con PPTP si los requisitos de seguridad son altos.

4.4. PROTOCOLOS VPN

L2TP (Layer 2 Tunneling Protocol)

Este protocolo tiene como base PPTP, de manera que también opera en capa 2, y está orientado a comunicaciones nodo a nodo, por lo que se precisa que todos los elementos intermedios cumplan con el protocolo L2TP, que sí es un estándar reconocido por IETF.

Emplea autenticación PPP que se realiza entre los puntos finales del túnel, lo que permite una suplantación de identidad por el camino. No encripta los datos de usuario, lo que supone una falta de confidencialidad, y tampoco se asegura la integridad de cada paquete.

Por todo lo anterior, el protocolo L2TP se mejora con las prestaciones de cifrado de IPsec que se verán a continuación, conformando la pareja L2TP/IPsec, que está estandarizado en la RFC 3193.

4.4. PROTOCOLOS VPN

IPsec (IP Security)

Es un conjunto de protocolos estándar, recogidos en varias normas de internet (RFC 4301 y RFC 4309), y son el conjunto de protocolos de uso más extendido.

Consta del protocolo AH, que aporta autenticación e integridad, del protocolo ESP, que aporta confidencialidad, y de una asociación de seguridad (SA) con la configuración VPN, que permite el intercambio de claves.

Actividades

UNA EMPRESA DISPONE DE DOS DELEGACIONES, UNA EN EL NORTE Y OTRA EN EL SUR. LA DELEGACIÓN DEL NORTE TIENE 20 TÉCNICOS, Y LA DELEGACIÓN DEL SUR TIENE 15 TÉCNICOS DE CAMPO.

ENTRE AMBAS DELEGACIONES SOLO SE CONECTAN 2 PAREJAS DE SERVIDORES, Y EL RESTO DE ORDENADORES DE LA RED NO TIENE VISIBILIDAD SOBRE LA RED DE LA OTRA DELEGACIÓN.

LOS TÉCNICOS DE CAMPO TRABAJAN EN LAS INSTALACIONES DEL CLIENTE, Y EMPLEAN PORTÁTILES QUE CONECTAN A LA RED DEL CLIENTE PARA, VÍA INTERNET, PODER CONECTARSE A LA RED PRIVADA DE SU EMPRESA, CON OBJETO DE USAR LA APLICACIÓN DE TRABAJO, EL SERVIDOR DE CORREO, EL SERVIDOR PROXY WEB, Y OTROS SERVICIOS QUE SE VAYAN AÑADIENDO.

DISEÑAR LA INFRAESTRUCTURA PARA QUE TODAS LAS COMUNICACIONES SEAN SEGURAS.

Actividades

SOLUCIÓN 1/2

PARA LAS COMUNICACIONES ENTRE LOS SERVIDORES DE LAS DELEGACIONES SE PUEDE EMPLEAR UN PROTOCOLO EXTREMO A EXTREMO, YA QUE SOLO SE TRATA DE CONECTAR 4 SERVIDORES. SE RECOMIENDA EMPLEAR UNA VPN DE ACCESO REMOTO, EMPLEANDO IPSEC EN MODO TRANSPORTE, O CON CIFRADO EXTREMO A EXTREMO, PARA HABILITAR EXCLUSIVAMENTE ESOS DOS TÚNELES ENTRE LAS PAREJAS DE SERVIDORES.

Actividades

SOLUCIÓN 1/2

LA CONEXIÓN DE LOS TÉCNICOS A LA RED DE LOS CLIENTES NO ES SEGURA, Y SUPONE UNA IMPORTANTE AMENAZA. RESULTA OBLIGATORIO EL EMPLEO DE REDES PRIVADAS VIRTUALES PARA PROTEGER LOS PORTÁTILES, Y LA INFORMACIÓN QUE LOS TÉCNICOS INTERCAMBIAN CON SU EMPRESA (APLICACIÓN DE TRABAJO, CORREO ELECTRÓNICO, ETC.). SE RECOMIENDA EMPLEAR UNA VPN DE ACCESO REMOTO, POR EJEMPLO, CON IPSEC. PARA ELLO, CADA PORTÁTIL INCORPORARÁ UNA APLICACIÓN CLIENTE DE VPN Y EL FIREWALL DE CADA DELEGACIÓN EJECUTARÁ EL SERVIDOR VPN (EL CORTAFUEGOS DE LA DELEGACIÓN NORTE DEBE PODER GESTIONAR 20 CLIENTES VPN, Y EL FIREWALL DE LA DELEGACIÓN SUR AL MENOS 15 CLIENTES VPN). PUEDE SER NECESARIO QUE LOS FIREWALL DE LAS LAN REMOTAS DONDE TRABAJAN LOS TÉCNICOS DE CAMPO SE AJUSTEN, PARA PERMITIR EL ESTABLECIMIENTO DE LAS VPN IPSEC.

5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS

Se parte de todo prohibido e ir abriendo exclusivamente los flujos permitidos.

- **Reglas de tráfico entrante (incoming) para filtrar el tráfico que procede de internet y va destinado a la red privada.**
- **Reglas de tráfico saliente (outcoming) para filtrar el tráfico que procede de la red privada y va destinado a internet.**

El firewall dispondrá al menos de dos interfaces de red, uno para la conexión a internet o red WAN, y otro para la conexión a la red privada o red LAN.

- **Protocolo de transporte: TCP o UDP.**
- **Puerto de comunicaciones: sirve para identificar la aplicación.**
- **Dirección IP origen: quién origina el paquete.**
- **Dirección IP destino: a quién va destinado el paquete.**
- **Acción: permitido o prohibido.**

Actividades

UNA EMPRESA DISPONE DE UN SERVIDOR WEB Y DE UN SERVIDOR DE CORREO ELECTRÓNICO, Y AMBOS COMPARTEN LA IP PÚBLICA 15.15.15.15.

EL SERVIDOR WEB DEBE SER ACCESIBLE DESDE EL EXTERIOR, EMPLEANDO EL PROTOCOLO HTTPS.

EL SERVIDOR DE CORREO DEBE PODER RECIBIR EL CORREO QUE LE ENVÍAN OTROS SERVIDORES EXTERNOS, ASÍ COMO ENVIAR CORREO (TIENE LA DIRECCIÓN IP PRIVADA 192.168.100.20).

ADEMÁS, SE PERMITE QUE LOS USUARIOS DE LA RED PRIVADA (CON RANGO DE RED 192.168.100.0/24) PUEDAN NAVEGAR LIBREMENTE POR INTERNET.

CONFIGURE LAS REGLAS DE ACCESO EN EL FIREWALL PERIMETRAL.

Actividades

SOLUCIÓN

DEBE EXISTIR UNA REGLA QUE PROHÍBA TODO EL TRÁFICO, Y ADEMÁS:

UNA REGLA QUE PERMITA EL TRÁFICO ENTRANTE DE INTERNET A LA IP PÚBLICA DE LA EMPRESA EN EL PUERTO TCP 443 (PROTOCOLO HTTPS).

UNA REGLA QUE PERMITA EL TRÁFICO ENTRANTE DE INTERNET A LA IP PÚBLICA EN EL PUERTO 25, PARA RECIBIR CORREO DESDE SERVIDORES EXTERNOS.

UNA REGLA QUE PERMITA EL TRÁFICO SALIENTE DE LA IP PRIVADA DEL SERVIDOR DE CORREO A INTERNET EN EL PUERTO 25, PARA PODER ENVIAR CORREO.

DEBEN EXISTIR REGLAS PARA PERMITIR TRÁFICO SALIENTE DESDE EL RANGO DE RED PRIVADO DE LA EMPRESA A INTERNET, EN LOS PUERTOS WEB (80 Y 443).

Actividades

PROTOCOLO	PUERTO	IP ORIGEN	IP DESTINO	ACCIÓN
TCP	443	*	15.15.15.15	PERMITIR
TCP	25	*	15.15.15.15	PERMITIR
TCP	25	192.168.100.20	*	PERMITIR
TCP	80	192.168.100.0/24	*	PERMITIR
TCP	443	192.168.100.0/24	*	PERMITIR
TCP, UDP	*	*	*	PROHIBIR