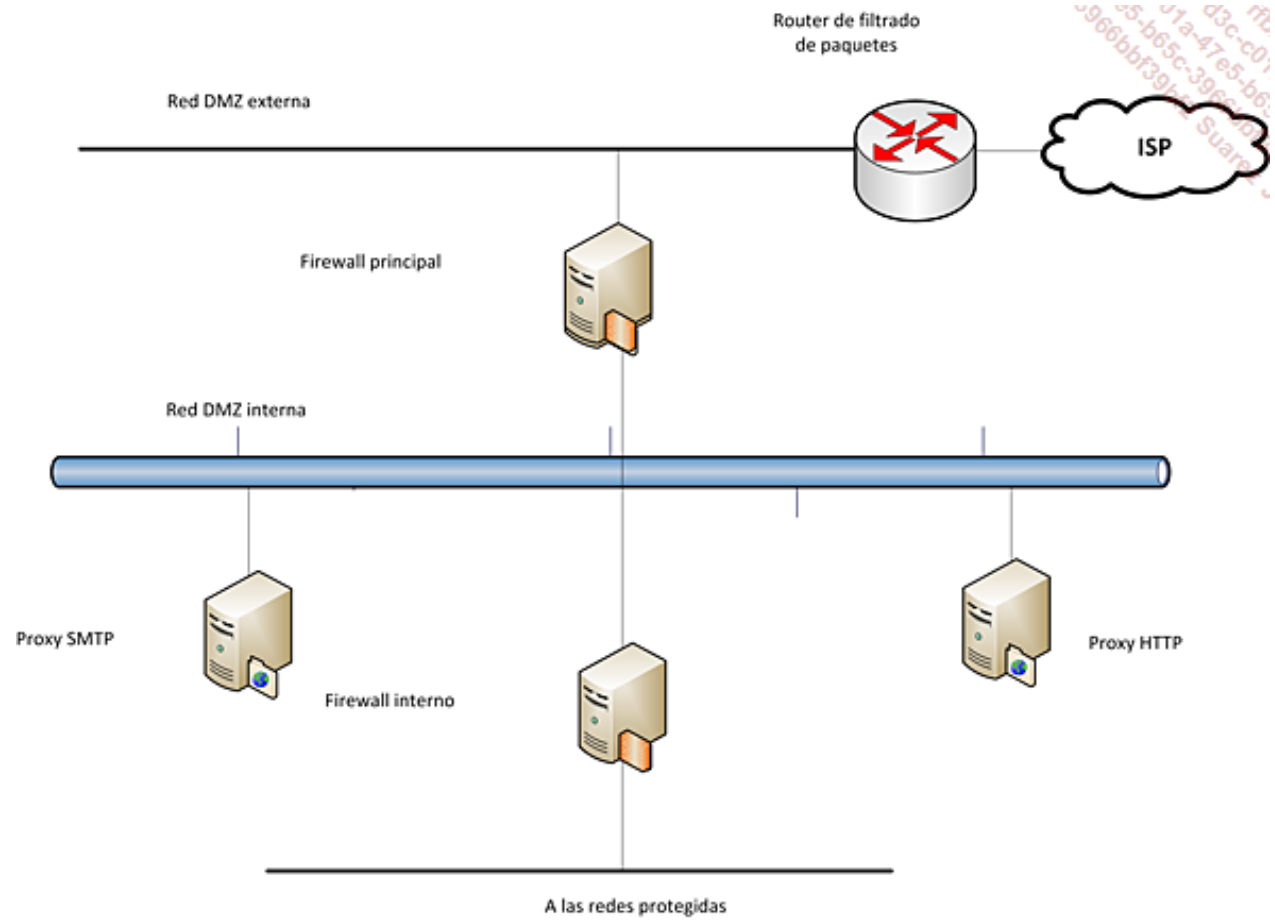
IMPLANTACIÓN Y CONFIGURACIÓN CORTAFUEGOS

Introducción a la tecnología firewall

- Consiste en proteger la red empresarial de intrusiones externas. Estos dispositivos filtran las tramas (que contengan datos) de diferentes capas del modelo TCP/IP para controlar el flujo y el bloqueo en caso de ataques, que pueden adoptar diversas formas.
- El filtrado realizado por el cortafuegos (firewall) es el primer baluarte de la protección del sistema de información.

Propósito

- Se trata de controlar los flujos de datos entrantes en la red. Se ofrecen varios tipos de filtrado:
- Aplicación para el control de las aplicaciones en función del puerto utilizado.
- Usuario: para el control de acceso en función de los usuarios identificados.
- Adaptativo: para la emisión de un registro de las transmisiones de paquetes IP.
- Los métodos de filtrado más corrientes son prohibir por defecto cualquier conexión entrante a excepción de las destinadas al servidor web, o cualquier conexión de una dirección IP a partir de la cual se detecten acciones de scanning sobre la red de la empresa


Router de filtrado
de paquetes
Red DMZ externa
ISP
Firewall principal
Red DMZ interna
Proxy SMTP
Proxy HTTP
Firewall interno
A las redes protegidas

La traducción de direcciones (Network Address Translation o NAT)

- Su principio consiste en cambiar la dirección IP de origen o destino, en la cabecera de un datagrama IP, cuando el paquete pasa por el cortafuegos en función de la dirección fuente o destino y el puerto origen o destino.

Traducción	Mapeo	Utilización
NAT estático	Permanente - 1:1	Correspondencia permanente de una dirección pública con una dirección IP privada interna encaminable asociada.
NAT dinámico	Temporal - 1:1	Conjunto de direcciones públicas asignadas dinámicamente a los clientes internos durante el tiempo de una conexión.
PAT	Temporal - N:1	Se comparte una dirección pública entre varios clientes internos.

Las funcionalidades del firewall

- Las funcionalidades básicas
- Análisis del tráfico a nivel de paquete, circuito o aplicación.
- Verificación del tráfico en su contexto.
- Limitación del riesgo de accesos no autorizados.
- Análisis y modificación del contenido a partir de filtros de aplicación.
- Detección de intrusos.
- Protección de los servidores accesibles desde la red externa (Internet...).

Las funcionalidades del firewall

- Las funcionalidades del firewall multicapa
- Este tipo de firewall permite aumentar la seguridad de los flujos mediante diversos procesos de filtrado:
- A nivel de **paquete**:
- Filtros estáticos y dinámicos.
- Detección de intrusos.
- Filtrado a partir del análisis de datos.
- Posibilidad de eliminar paquetes.
- Protocolo PPTP (*Point-to-Point Tunneling Protocol*) autorizado.

Las funcionalidades del firewall

- A nivel **circuito** (protocolo):
- Filtrado basado en las sesiones.
- Control y análisis de la conexión del cliente al servidor.
- Asociación de conexión.

- A nivel de **aplicación**:
- Inspección de datos.
- Análisis del contenido (acción de bloqueo/modificación/redirección).
- Filtro para los protocolos HTTP (*Hypertext Transfer Protocol*), SMTP (S*imple Mail Transfer Protocol*)...

Los diferentes tipos de cortafuegos

- Los firewall personales o los appliances de firewall personal
- El firewall integrado en un servidor o en el sistema operativo

- Se deben retirar todos los protocolos de red no utilizados.
- En efecto, pueden utilizarse para eludir o dañar el entorno del firewall.
- Todos los servicios de red y aplicativos deben suprimirse o desactivarse.
- En efecto, los servicios no utilizados a menudo se convierten en potenciales blancos de ataque. En realidad, muchos administradores se olvidan de implementar los controles de acceso para restringir el acceso al firewall. Las aplicaciones o servicios de red no utilizados, y ejecutados con sus configuraciones por defecto, se convierten en vulnerabilidades críticas.

- Todas las cuentas de usuario o sistemas no utilizados deberán eliminarse o desactivarse.
- Todos los parches (patches y hotfixes) deberán instalarse antes que los componentes del firewall y haber sido probados previamente en una máquina de prueba para verificar su eficacia. Por supuesto, las actualizaciones de parches del sistema deben por fuerza realizarse con periodicidad para garantizar un buen estado de seguridad.
- Todas las conexiones físicas a las interfaces de red no utilizadas deben ser desactivadas o desconectadas.
- El equipo que alberga el firewall debe ser respaldado (copia de seguridad) como cualquier otro servidor importante, aunque de forma externa a la arquitectura de respaldo clásica, es decir, fuera de la red interna de la empresa. En principio, se debe utilizar la unidad de respaldo local. Los soportes (cartuchos o cintas) se deben almacenar por supuesto en un lugar seguro.

Eleccion Firewall

- pasos necesarios se describen a continuación:
- Identificación de las aplicaciones de red y las vulnerabilidades asociadas a cada una de ellas.
- Creación de una matriz de tráfico de aplicaciones mostrando los métodos de protección utilizados.
- Creación de un conjunto de reglas basadas en una matriz de las aplicaciones que utilizan la red.

verificación de la política de seguridad definida en un firewall

- Debemos verificar al menos una vez o más por trimestre las reglas del firewall.
- Para esto, existen dos métodos. El primero y más sencillo consiste en imprimir la configuración de cada firewall operativo y compararla con la versión definida de origen, teniendo en cuenta los posibles ajustes. Las modificaciones realizadas en el tiempo deben describirse en la documentación relacionada con el firewall para conocer las razones de los cambios.
- El segundo, más riguroso, implica comprobar la configuración existente

Revista periódica (auditoría) de seguridad de los firewall

- Esta auditoría deberá ajustarse a la política global de seguridad, que en sí misma debe seguir siendo coherente.
- Las mejores prácticas aconsejan que las políticas de seguridad del sistema de información sean revisadas y actualizadas periódicamente, al menos dos veces al año

6. Estrategia de implementación de firewall

Las reglas en un firewall

- elementos:
- La dirección fuente del paquete (la dirección de nivel de red del modelo TCP/IP de la máquina o del dispositivo de red de origen), ej.: 192.168.1.1.
- La dirección de destino del paquete (la dirección de nivel de red del modelo TCP/IP de la máquina o del dispositivo de red de destino), ej.: 192.168.1.2.
- El tipo de tráfico, protocolo de red específico utilizado para la comunicación entre los sistemas o dispositivos de origen y de destino, ej.: Ethernet a nivel de la capa de acceso a la red e IP a nivel de la capa de red.
- Los parámetros a nivel de la capa de transporte, ej.: TCP: 80 puerto de destino de un servidor web o información sobre las interfaces del router mediante las cuales transitan los paquetes.
- Una acción que actuará sobre los paquetes de entrada: Deny (Impedir), Permit (Permitir), Drop (Eliminar).

- La gestión de las reglas del firewall puede consolidarse después de haber realizado la matriz de las aplicaciones que utilizan la red. Las reglas deben ser simples y tan específicas como sea posible, en correspondencia con el tráfico de red que controlan.

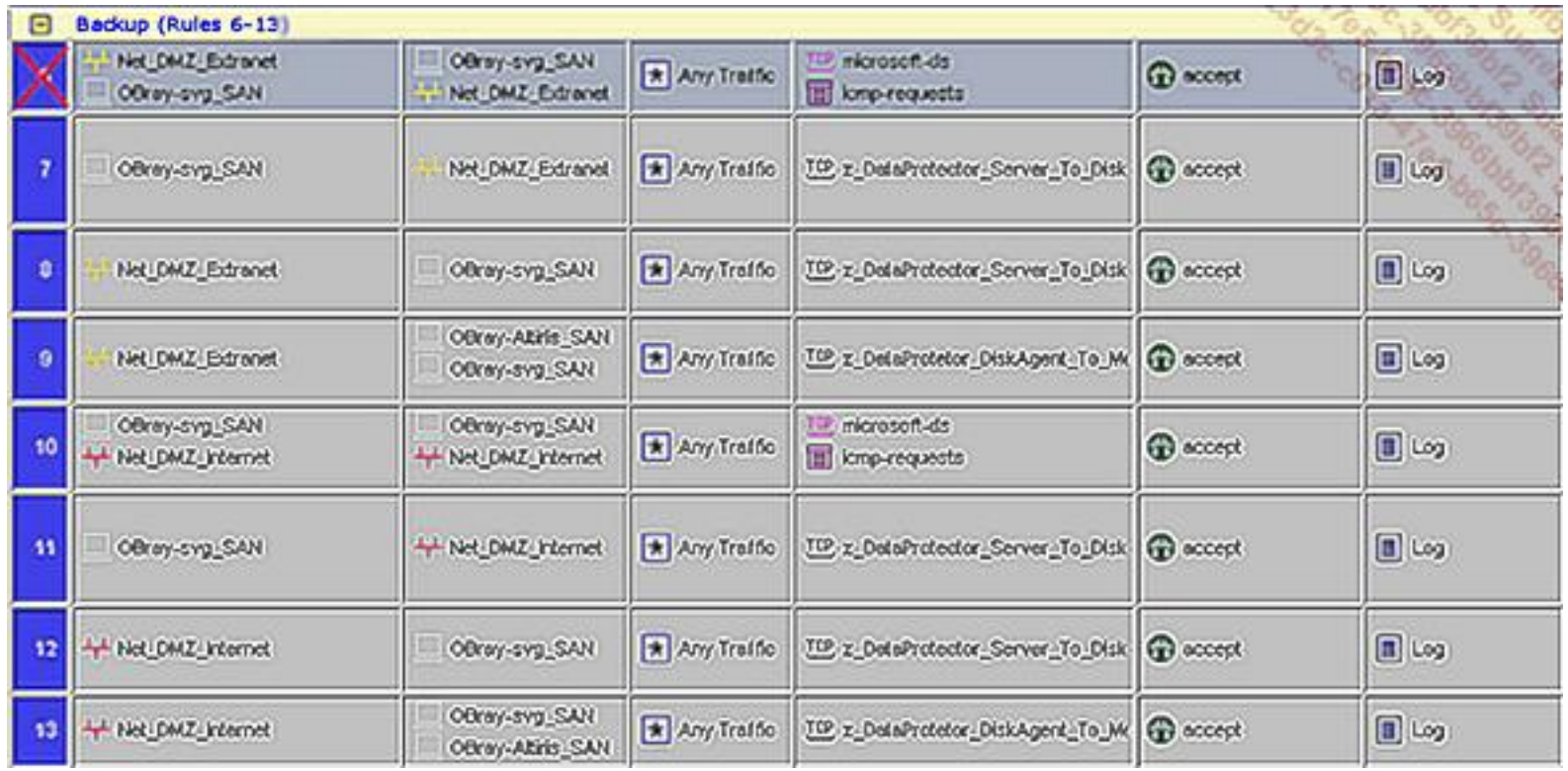
- Por razones de seguridad, el mejor método de configuración consiste en bloquear primero todos los flujos entrantes para luego permitir uno a uno de forma selectiva según los tipos de tráfico previstos. La otra solución consiste en permitir todas las conexiones y el tráfico por defecto para luego bloquear según los tipos de protocolo no recomendados e incluso prohibirlos.

Las reglas estrictas

- El conjunto de reglas de un firewall deben por fuerza bloquear los siguientes tipos:
- Tráfico entrante, cuyo origen es un sistema fuente no autenticado con una dirección de destino del mismo firewall. Este tipo de paquete es un ataque o una prueba de dirección del firewall. Hay una excepción a esta regla. Se refiere al caso en que el firewall acepta la transferencia de un mail que entra por el puerto 25. En este caso, debe permitir las conexiones entrantes hacia sí mismo, solo en este puerto.
- Tráfico entrante con una dirección fuente que indica que el paquete tiene su origen en la red protegida detrás del firewall. Este tipo de paquete representa probablemente un tipo de intento de usurpación (spoofing attempt).
- Tráfico entrante que contenga paquetes ICMP (*Internet Control Message Protocol*), correspondiente al comando ping. Ya que ICMP puede ser utilizado para acceder a las redes detrás de algunos tipos de firewall, este protocolo no debe poder transitar desde Internet o de cualquier red externa no aprobada.

- Tráfico entrante y saliente a partir de una dirección fuente que pertenezca a un rango de direcciones reservadas a redes privadas (RFC 1918). La RFC 1918 reserva los siguientes ámbitos de direcciones para redes privadas IPv4.
- 10.0.0.0 a 10.255.255.255 (clase A, o ./8. en notación CIDR)
- 172.16.0.0 a 172.31.255.255 (clase B, o ./12. en notación CIDR)
- 192.168.0.0 a 192.168.255.255 (clase C, o ./16. en notación CIDR)
- Tráfico entrante para que el origen de la dirección forme parte de estos rangos de direcciones privadas. Este tráfico es el comienzo de un ataque del tipo denegación de servicio. Sin embargo, este tipo particular de tráfico de red debe ser bloqueado con conjuntos de reglas, salvo si el firewall cuenta con una funcionalidad de protección.

- Tráfico entrante proveniente de una fuente no identificada que contenga tráfico SNMP (*Simple Network Management Protocol*). La presencia de estos paquetes puede indicar que un intruso está probando (scanner) la red. Hay en general pocos motivos para que una empresa permita este tipo de tráfico. Por tanto, debe ser bloqueado.
- Tráfico entrante que contenga información sobre IP Source Routing. Se trata de un mecanismo que permite a un sistema especificar las rutas tomadas por este paquete en la red. A nivel de la seguridad, el source routing puede permitir que un intruso acceda a una red privada utilizando una máquina conectada a la vez a Internet y a la red interna como pasarela.
- El tráfico de red entrante o saliente con una dirección de origen o destino equivalente a 127.0.0.1 (localhost). Este tipo de tráfico corresponde normalmente a un ataque sobre el mismo firewall.
- El tráfico de red entrante o saliente con una dirección de origen o destino equivalente a 0.0.0.0 (localhost). Algunos sistemas operativos interpretan esta dirección como una dirección local (localhost) o como una dirección de difusión. Estos paquetes pueden ser utilizados en caso de ataque a la red.
- El tráfico de red entrante o saliente que contenga direcciones de difusión. Este caso puede ser una fuente de ataque cuyo objetivo es inundar la red o subred con tramas.


Backup (Rules 6-13)
Net_DMZ_Extranet
OBray-svg_SAN
Any Traffic
microsoft-ds
icmp-requests
accept
Log
7
OBray-svg_SAN
Net_DMZ_Extranet
Any Traffic
z_DataProtector_Server_To_Disk
accept
Log
8
Net_DMZ_Extranet
OBray-svg_SAN
Any Traffic
z_DataProtector_Server_To_Disk
accept
Log
9
Net_DMZ_Extranet
OBray-Altiris_SAN
OBray-svg_SAN
Any Traffic
z_DataProtector_DiskAgent_To_M
accept
Log
10
OBray-svg_SAN
Net_DMZ_Internet
OBray-svg_SAN
Net_DMZ_Internet
Any Traffic
microsoft-ds
icmp-requests
accept
Log
11
OBray-svg_SAN
Net_DMZ_Internet
Any Traffic
z_DataProtector_Server_To_Disk
accept
Log
12
Net_DMZ_Internet
OBray-svg_SAN
Any Traffic
z_DataProtector_Server_To_Disk
accept
Log
13
Net_DMZ_Internet
OBray-svg_SAN
OBray-Altiris_SAN
Any Traffic
z_DataProtector_DiskAgent_To_M
accept
Log

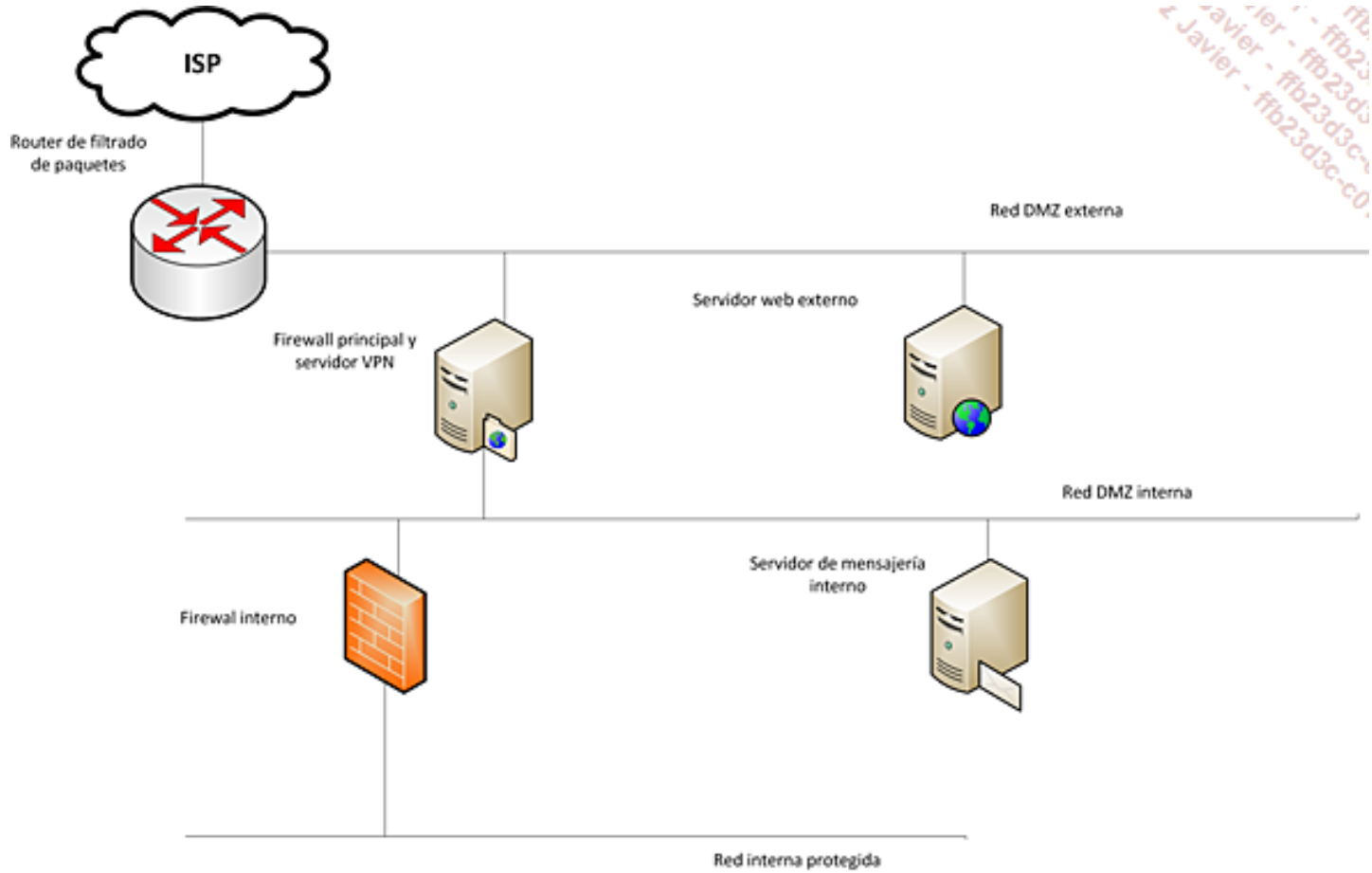
Guía de mejores prácticas para implementar entornos de firewall

- Hacerlo simple; cuanto más simple sea la solución implementada, más sencillo será securizar el cortafuegos y administrarlo.
- Utilizar los dispositivos mejor adaptados al entorno y a su función principal. En la mayoría de los casos, los cortafuegos híbridos o los appliances son las mejores opciones porque están destinados a esta función.
- Crear una defensa en profundidad en diferentes capas del modelo TCP/IP, en lugar de una sola. Si es necesario, utilizar varios cortafuegos, routers que puedan efectuar controles de acceso o de filtrado, varios servidores equipados con firewall, según las necesidades de protección.
- También hay que pensar en las posibles amenazas internas. Un intruso que haya podido tener acceso de una forma u otra a la red interna protegida detrás del firewall tendrá todas las facilidades para introducirse en toda la red. Los sistemas críticos deben ser colocados y protegidos detrás de firewall específicos o múltiples.
-

- La funcionalidad de **grabación de eventos en un registro**
- La mayoría de los sistemas de firewall presentan una funcionalidad de grabación de eventos en un registro. En general se cuenta en todos los tipos de sistemas operativos con un programa de recuperación de la información, lo que permite visualizarlos y evaluarlos posteriormente.
- La **copia de seguridad** de los datos del firewall
- La gestión y el mantenimiento de las copias de seguridad son puntos esenciales en la estrategia para la administración de los firewalls. Por principio, cada operación de respaldo debe ser completada. No es necesario ni recomendable realizar copias incrementales.
-

Las redes DMZ (Zona DesMilitarizada)

- El entorno más común de implementación de firewall es conocido como DMZ (*Zona DesMilitarizada*).
- Este tipo de red incluirá al menos dos firewalls.


ISP
Router de filtrado de paquetes
Red DMZ externa
Servidor web externo
Firewall principal y servidor VPN
Red DMZ interna
Servidor de mensajería interno
Firewall interno
Red interna protegida

- La DMZ es un entorno de subred ubicado entre una red interna de confianza y una red externa no segura.
- Los servidores instalados en la parte externa de la DMZ permiten proporcionar servicios a la red externa. Puede tratarse de:
- Servidores web, de archivos (FTP: *File Transfer Protocol*), de correo (SMTP) y servidores de nombres (DNS: *Domain Name System*).
- Servidores de relevo que permiten garantizar una comunicación indirecta entre la red local y la red Internet (proxys, relay SMTP, antivirus...).

Ubicación de los servidores en entornos con DMZ

- Podemos emplear varias recomendaciones para definir la implementación:
- Proteger los servidores externos con un filtro router/paquete perimetral.
- No configurar servidores accesibles por una red externa en la red protegida.
- Ubicar los servidores internos detrás de los cortafuegos según su criticidad y sus accesos.
- Aislar los servidores de tal manera que un ataque externo no pueda propagarse a la red interna.

configuraciones para implementar los servidores o sistemas específicos a fin de definir protecciones adecuadas.

- Servidores accesibles desde el exterior (Web, DNS...):
- Pueden colocarse en la parte externa de la DMZ entre un router perimetral y el firewall principal. Este router puede facilitar los controles de acceso y filtrado para los servidores. El firewall principal tiene la posibilidad de restringir las conexiones entre estos servidores y sistemas internos en el caso de que aparezcan intrusos.

- Servidores VPN:
- Es preferible colocar estos servidores en la parte externa de la DMZ para que el tráfico pueda pasar a través del firewall. Esto significa que el servidor VPN se coloca en la plataforma del cortafuegos de tal forma que el tráfico saliente pueda ser cifrado después de haber sido filtrado (ej.: para un proxy HTTP) y que el tráfico entrante pueda ser descifrado y filtrado también por el cortafuegos.

- Servidores internos o accesibles desde el interior.
- Estos servidores (Web, de datos...) pueden ser ubicados en la parte interna de la DMZ, entre dos cortafuegos dedicados (principal e interna) con el firewall interno separando la DMZ de la red que se quiere proteger. El hecho de colocar estos sistemas en la parte interna de la DMZ proporciona una defensa en profundidad contra amenazas externas y una protección contra las amenazas internas.

- Servidores de correo:
- Algunos firewalls pueden usarse para aceptar los correos electrónicos, es decir, una conexión SMTP. Una configuración típica incluye la utilización de un cortafuegos principal para aceptar conexiones SMTP y hacerlas pasar luego a un servidor dedicado proxy/email localizado en la parte interna de la DMZ. Esta solución elimina la necesidad de que el firewall procese el contenido activo y las carpetas anexadas a cada mail.

VPN

- Para efectuar una conexión remota a una red interna de una pyme debemos utilizar una red privada virtual o VPN (*Virtual Private Network*). Esta funcionalidad cifra el tráfico de red y requiere una autenticación fuerte, proporcionando un acceso remoto seguro.

- Existen tres tipos de soluciones VPN asociadas a un firewall:
- Integrada como servicio del firewall.
- Sistemas autónomos ubicados delante del firewall.
- Sistemas autónomos ubicados detrás del firewall (soluciones de software).

El servidor VPN

- Es el equipo que actúa como punto de control en la empresa. Deberá estar situado en la red empresarial, puede también servir como firewall o router perimetral. Autónomo, este dispositivo debe ser colocado en la DMZ dedicada.
- La tecnología VPN utilizada en el entorno DMZ permite estar protegido por las reglas del firewall y autorizar solo el tráfico VPN.
- Existen tres protocolos para el tunneling a través de Internet: *Internet Protocol Security* (IPSec), *Layer 2 Tunneling Protocol* (L2TP) y *Point-to-Point Tunneling Protocol* (PPTP).

categorías de VPN

- **Las VPN usuario-sitio**
- **Las VPN sitio-sitio**

Los protocolos vinculados a la seguridad

- Los protocolos IPSec (*Internet Protocol Security*) y SSL/TLS (*Secure Sockets Layer/Transport Layer Security*)

- El protocolo IPSec, definido por la RFC 2401 y el más utilizado, tiene por objeto asegurar el intercambio de datos a nivel de la capa de red.
- Otros protocolos asociados incluyen PPTP (*Point-to-Point Tunneling Protocol*) utilizado por Microsoft y L2TP (*Layer 2 Tunneling Protocol*).

Los sistemas de detección y prevención de intrusión

La detección de intrusión o Intrusion Detection System (IDS)

- Los sistemas de detección están diseñados para informar de los accesos no autorizados o intrusos en las redes.

- Los firewalls que operan con sistemas de detección de intrusos son capaces de detectar automáticamente las amenazas procedentes del exterior, más rápidamente que una verificación por un operador.

Las herramientas de detección de intrusión (IDS) o escáneres de intrusión

- Estas herramientas, que pueden asociarse con otras herramientas de detección de vulnerabilidades, permiten escanear cada servidor verificando a partir de un catálogo de acontecimientos.

- Una de las más conocidas se llama Nessus. Es una herramienta gratuita de detección de vulnerabilidades para redes. www.nessus.org

La prevención de intrusión o IPS (Intrusion Prevention System)

- Un sistema IDS (*Intrusion Detection System*) tiene la funcionalidad de detección de una intrusión.

- Un sistema IPS (*Intrusion Prevention System*), además de la detección, cuenta con la posibilidad de detener a los intrusos.
-

- Las principales soluciones IPS que podemos encontrar actualmente en el mercado son:
- IBM ISS (Proventia)
- Juniper Networks Sondas IDP (*Intrusion Detection and Prevention*)
- 3Com TippingPoint UnityOne IPS 400
- Cisco Services for Intrusion Prevention System (IPS)

Los servidores DNS (Domain Name Service)