CDA. Redes y seguridad en centros de datos

Cortafuegos/Firewalls
Redes privadas virtuales
Detección de intrusiones

Centros de datos
3º Grado en Ingeniería Informática
ESEI

Octubre-2022

Contenido

Conceptos básicos I

Cortafuegos/Firewalls
Mecanismos de control de acceso a la red y los recursos informáticos de una organización

- Formado por componentes hardware y software
- Separa red interna (*equipos de confianza*) de equipos externos (*potencialmente hostiles*) mediante el control del tráfico
- Deniega intentos de conexión no autorizados (en ambos sentidos)
- **Finalidad:** prevención de ataques desde el exterior hacia equipos internos
  - Opcionalmente: control del uso de la red por parte de los equipos internos
  - Protección del propio equipo: *"firewalls personales"*

Conceptos básicos II

Principios básicos de funcionamiento

1. **Todo** el tráfico desde interior a exterior y viceversa debe pasar por el Cortafuegos/Firewall.
   - bloqueo de todos los accesos físicos a red interna excepto el del Cortafuegos
   - diferentes topologías $\Rightarrow$ diferentes niveles de aislamiento
2. Cortafuegos permite sólo tráfico autorizado (entrante o saliente)
   - definido por las políticas de seguridad de la organización
   - cada tipo de Cortafuegos permite distintos tipos de control
3. Corfafuegos debe ser inmune a intrusiones
   - Sistema Operativo y software fiable y actualizado

Tipos de controles realizados

Control de Servicios

Determinar tipos de servicios de red accesibles desde interior y exterior
Alternativas:

1. Cortafuegos filtra tráfico a los servicios basándose en la dirección IP + núms. de puerto
2. Cortafuegos proporciona un software intermediario (Proxy) para cada servicio concreto a controlar.

   Proxy recibe e interpreta las solicitudes a nivel de aplicación, permitiendo o no su paso

Control de Direcciones

Determinar qué direcciones pueden iniciar las solicitudes de servicios y hacia cuáles se permite su paso a través del Cortafuegos

Control de Usuarios

Control de acceso en base al usuario concreto que pretende acceder

Control de Comportamiento

Control de cómo se usan los servicios (limitaciones a determinados servicios Web, filtrado de SPAM, etc)

Utilidad de los Cortafuegos

- Definen un punto único de resistencia frente a ataques
  - mantiene usuarios no autorizados fuera de la red protegida
  - prohibe entrada o salida de servicios potencialmente vulnerables
  - protección frente a ciertos ataques de suplantación de IP (*IP spoofing*)
  - simplifica la administración (punto único de entrada)
- Ofrece ubicación donde realizar supervisión de eventos de seguridad
  - registro de accesos, intentos de intrusión, gestión de alarmas de seguridad, auditorias, etc
- Ofrece ubicación ”cómoda” para situar otros elementos de gestión de red (no exclusivamente relacionados con la seguridad)
  - traducción de direcciones, NAT(*network address translation*)

    direcciones locales (privadas) $\Leftrightarrow$ direcciones públicas de Internet
  - software de auditoria y registro del uso de la red
  - plataforma para implantar pasarelas IPSec o similares (enlaces de redes virtuales privadas [VPN])
  - plataforma donde centralizar sistemas de detección de intrusiones (ej.: SNORT)

Limitaciones

- No protegen contra ataques que no pasen a través del Cortafuegos
  - conexiones alternativas que ofrecen un punto de entrada alternativo fuera de su control
- No protegen contra amenazas internas
- Pueden proporcionar una sensación de falsa seguridad
  - Cortafuegos no basta por si sólo
  - Seguridad en redes afecta a muchos aspectos
  - **Idea:** *defensa en profundidad*
    - implementar diversas capas de mecanismos de defensa complementarios y coordinados
    - no confiar la defensa de la red a un único mecanismo (cortafuegos)

NOTA: NAT *(network address translation)* en Cortafuegos

- Ventajas del NAT (enmascaramiento, SNAT: *Source NAT*)
  - Permite ”ahorrar” direcciones públicas de Internet

    Todos los equipos de la red interna usarán/compartirán un conjunto reducido de direcciones IP válidas en la red externa
  - Ofrecen un nivel adicional de seguridad
    - Se ocultan (hacia el exterior) las características de la red interna
    - Desde el exterior sólo son visibles las direcciones IP externas
    - Suele ser recomendable implantar NAT
  - Uso de NAT sopone imponer un ”Cortafuegos implícito”
    - En principio, sólo permite conexiones salientes originadas en la red interna (direcciones privadas)
    - Las conexiones entrantes requieren configuración específica, por lo que están muy controladas
- Los Cortafuegos suelen ofrecer funciones de NAT

Esquema usual (SNAT): traducción de direcciones mediante ”reparto” de puertos

- Traduce direcciones IP privadas a 1 (ó más) IP públicas, mediante el uso de distintos núm. de puerto
- Puerto origen (de la máquina cliente) no suele ser relevante (se asigna al azar al establecer la conexión)
- SNAT (enmascaramiento) se implementa usando una tabla que mapea direcciones internas a puertos

Ejemplo: Compartición de la dir. IP pública 193.147.87.47 desde la red privada 10.0.2.0/24

origen interno		origen ”NAT”		destino exte	
dir.origen	puerto origen	dir. NAT	puerto NAT	dir.destino	pu
10.0.2.16	20122	193.147.87.47	37012	193.144.51.100	
10.0.2.45	12856	193.147.87.47	6734	87.123.56.120	
10.0.2.16	5378	193.147.87.47	11003	200.132.50.27	
...	...	...	...	...	

Tipos de Cortafuegos I

Filtros de paquetes

- Inspeccionan paquetes recibidos/enviados y comprueban si encajan con las reglas de filtrado
- Filtrado basado en la informacióemcontenida en cada paquete recibido/enviado
  - cada paquete se inspecciona de forma aislada y la decisión se toma de forma aislada
  - filtro ”sin estado”: no tiene en cuenta si los paquetes son parte de una conexión
- Filtrado de puertos estándar para bloquear servicios concretos

Filtros ”con estado”

- Mantiene registro de las conexiones que pasan a través del Cortafuegos
- Estudian y reconocen paquetes $\left\{ \begin{array}{l} \text{de inicio/fin de conexión} \\ \text{parte de conexiones ya abiertas} \end{array} \right.$

Tipos de Cortafuegos II

Filtros a nivel de aplicación (Proxies)

- Cortafuegos basados en el uso de Proxies del nivel de aplicación
  - interceptan los mensajes entre aplicaciones
  - bloqueo de aplicaciones no permitidas (las que no cuenten con Proxy)
  - control del tráfico de las aplicaciones permitidas
- Proxy ”comprende” el protocolo de una aplicación concreta
  - previene abusos
  - permite limitar porciones concretas del protocolo
  - pueden detectar uso de protocolos no permitidos en puertos estándar
- Mayor ”conocimiento” sobre el tráfico
  - pueden realizar análisis en profundidad de los mensajes

Filtrado de paquetes

Dispositivos que encaminan tráfico entre red externa e interna

- Trabajan en capas de red (IP) y/o transporte (TCP,UDP)
- Suelen implementarse como un elemento añadido a un router o como un equipo dedicado

Analizan cada paquete (antes de la decisión de enrutado) y aplican un conjunto de reglas para decidir si se retransmite o descarta

- inspecciona las cabeceras del paquete y comprueba si encajan en la lista de reglas aceptación/rechazo
- filtrado basado en la información de cada paquete concreto (en filtros "sin estado")
  - cada paquete se analizan de forma aislada sin considerar el contexto
  - no tiene en cuenta si son parte de una conexión

Reglas de filtrado emplean info. contenida en cada paquete analizado

```
- IP origen (info. capa de red)  - puerto origen (info. capa transporte)
- IP destino (info. capa de red) - puerto destino (info. capa transporte)

- tipo de protocolo (flags en los paquetes IP): TCP, UDP, IMCP,...
- interfaz de entrada o salida (en Cortafuegos con 3 o más conexiones)
- otra información: tamaño del paquete, tiempo del vida del paquete,
                    flags de protocolos de transporte, ...
```

El control de servicios se basa en el filtrado de los puertos estándar

Funcionamiento general

El filtrado de paquetes se configura como una lista de reglas estáticas

- **condiciones:** basadas en los campos de la cabecera IP y/o TCP
- **acciones:** descartar, rechazar, retransmitir

Funcionamiento

1. Reglas comprobadas secuencialmente una a una (orden es relevante)
2. Cuando hay una correspondencia, se invoca la regla (aceptar o denegar el paquete)
3. Si ninguna regla encaja, se aplica la acción predeterminada

denegar por defecto

Lo que no está expresamente permitido, está prohibido

- política más conservadora, todo está bloqueado
- los servicios permitidos deben añadirse explícitamente
  $\rightarrow$ indicar explicitamente qué paquetes se dejan pasar
- mayor dificultad de administración (muy perceptible por el usuario)
- mayor nivel de protección

aceptar por defecto (no recomendado)

Lo que no está expresamente prohibido, está permitido

- política más permisible, todo está permitido
- servicios vulnerables/peligrosos deben bloquearse explícitamente
- mayor facilidad de administración (puesta en marcha sencilla)
- nivel de protección más bajo (incrementa el riesgo)

NOTA: Rechazar *vs.* denegar paquetes

- **descartar**: se bloquea el paquete sin informar al origen de que no se procesó
- **rechazar**: se notifica al origen (mediante mensaje ICMP) la razón del rechazo del paquete

  → `https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol`

Suele ser preferible descartar

- responder aumenta el tráfico de red
- respuestas ofrecen información potencialmente útil sobre la red
- denegación es más robusta ante ataques DOS (*denial of service*) (cualquier paquete al que se responda se podría usar en DOS)

Filtros ”con estado”

Evolución de filtros de paquetes ”clásicos” (*Stateful packet inspection*)

Tienen en cuenta contexto del paquete para decidir acción a realizar.

- Mantienen registro de las conexiones que pasan por el Cortafuegos
- Estudian y reconocen los paquetes
  - que inician/finalizan las conexiones
  - que forman parte de conexiones establecidas
  - que están relacionados con conexiones previas
- Permiten control más ”fino” que los filtros sin estado
- Ejemplo en GNU/Linux: NETFILTER/iptables con módulos de seguimiento de conexiones *(connection tracking)*

Evolucionan hacia *Deep Packet Inspection* (DPI)

- ”entienden” protocolos de capa de aplicación (al menos para clasificar tráfico y reconstruir mensajes)
- capaces de evaluar contenido de los paquetes
- Ejemplo: L7-Filter (`https://l7-filter.sourceforge.net/`), módulo NETFILTER/iptables

Ventajas y limitaciones del Filtrado de Paquetes I

Ventajas.

- **Simplicidad**
  - Maneja una información mínima (cabeceras de paquetes)
  - Especificación de reglas es simple

  $\Rightarrow$ permite establecer filtrado en casi cualquier red
- **Rapidez/eficiencia:** mínimo proceso a realizar sobre los paquetes para la toma de decisiones (coste y retardos reducidos)
- Son transparentes al usuario (no requieren participación por su parte)

Ventajas y limitaciones del Filtrado de Paquetes II

Limitaciones.

- Usan info. de ”bajo nivel” $\rightarrow$ no examinan datos de niveles superiores (capa aplicación)
  - no puede evitar ataques que aprovechen vulnerabilidades o funcionalidades específicas de las aplicaciones
  - no pueden bloquear comandos específicos del protocolo de aplicación
- Posibilidades de registro (log) reducidas
  - manejan info. limitada (sólo capas IP y/o TCP/UDP)
- No admiten esquemas de autenticación/control de usuarios (requieren info. de niveles más altos)
- Reglas de filtrado muy complejas pueden ser difíciles de definir/gestionar
- Identificación basada en direcciones IP $\Rightarrow$ vulnerables a la falsificación de direcciones (*IP spoofing*)

Pasarelas de nivel aplicación *(Proxies)* I

También *Application Firewalls* o *Proxy Firewalls*

Dispositivos repetidores de tráfico a nivel de aplicación.

- Proxy separa completamente red interna de red externa,
- Actúa como servidor intermediario, ofreciendo un núm. limitado de servicios a nivel de aplicación
- Hace posible un control a más alto nivel
  - permite analizar las conexiones a nivel de cada aplicación concreta
  - permite la autentificación de usuarios
- Para cada protocolo de nivel aplicación permitido se debe ejecutar el correspondiente Proxy en el equipo Cortafuegos.
  - Cortafuegos sólo permite tráfico de aplicaciones que cuenten con Proxy
- Ejemplo: proxy-cache WEB SQUID.

Pasarelas de nivel aplicación *(Proxies)* II

Funcionamiento

- Cliente interno que desee conectar con exterior establece conexión con Proxy
- Proxy establece conexión con servidor externo en nombre de ese cliente
- Proxy gestiona 2 conexiones
  - **cliente_interno – Proxy**
    (Proxy actúa como servidor)
  - **Proxy – servidor_externo**
    (Proxy actúa como cliente)

  Para ambas aplicaciones son conexiones transparentes: cliente y servidor las tratan como una conexión directa
- Proxy recibe, examina y retransmite el tráfico bidireccionalmente entre cliente (interno) y servidor (externo)
  - analiza cada mensaje (petición o respuesta) y toma la decisión de reenviarlo o no
  - puede realizar otras tareas: cache de datos/recursos recibidos, estadísticas, etc

Ventajas y limitaciones I

Ventajas

- Mayor control que con filtros de paquetes $\Rightarrow$ mayor flexibilidad
  - Proxy especializado en analizar/controlar una aplicación concreta
  - "Entiende" mensajes del protocolo de aplicación $\Rightarrow$ Control "fino" para cada aplicación concreta
    - limitar comandos de subida a servidor FTP
    - bloqueo de contenidos WEB por tipo MIME
- Centralización de la información de cada protocolo del nivel de aplicación
- Evitan comunicación directa con servidor destino
- Autentificación de usuario a nivel de aplicación
- Posibilita registro de eventos a nivel de aplicación
- Posibilidad servicios añadidos: caché, gestión/compartición conexiones

Ventajas y limitaciones II

Limitaciones

- Exige instalar Proxy para cada aplicación que se pretenda controlar
- Alto coste de procesamiento
  - mantener e inspeccionar mensajes de 2 conexiones
  - menor rendimiento que filtros de paquetes
  - cantidad de servicios con Proxy está limitada por recursos del equipo cortafuegos.
- No totalmente transparentes al usuario (requieren cierta intervención)

Pasarelas de nivel de circuitos

Mecanismo de control híbrido ($\approx$ proxy en la capa de transporte)

- Puede ser un sistema autónomo o una función complementaria realizada por un Proxy para ciertas aplicaciones concretas
- Funciona como intermediaro (Proxy) de conexiones en la capa de transporte
  - No permiten conexión TCP directa de extremo a extremo
  - Pasarela gestiona 2 conexiones TCP $\begin{cases} \textbf{pasarela–equipo\_interno} \\ \textbf{pasarela–equipo\_externo} \end{cases}$
  - Pasarela de circuitos retransmite paquetes TCP desde una conexión a la otra sin analizar sus contenidos
  - La seguridad que aporta consiste en determinar qué conexiones se permiten o no
- Diferencia con Proxies de aplicación
  - no analiza el tráfico (no maneja info. del protocolo de aplicación)
  - menor necesidad de procesamiento (sólo retransmite paquetes TCP entre 2 conexiones ya abiertas)
  - una vez establecidas las 2 conexiones, las pasarelas de circuitos tienen un funcionamiento análogo al de un filtro de paquetes con estado
- Ejemplo: SOCKS (servidor + librería cliente)

Topologías de cortafuegos I

Decisiones clave: ubicación de { reglas de filtrado / servicios públicos

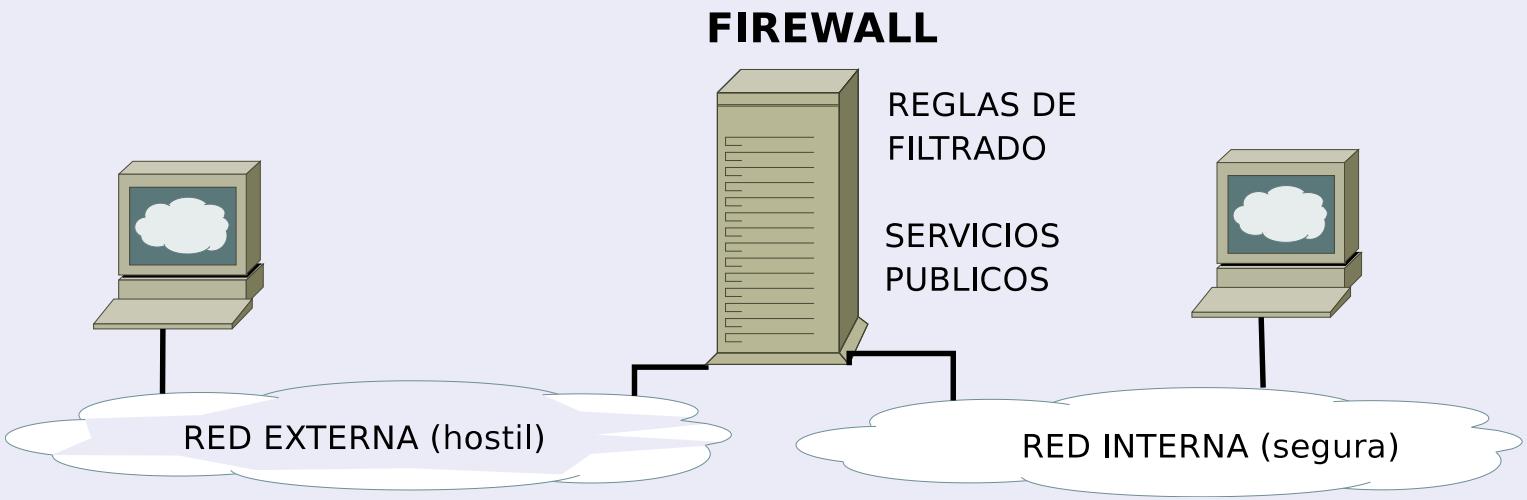
(a) Cortafuegos básico de borde

- Un equipo actúa como cortafuegos, conectando red interna con la externa
  - Ofrece todas las funcionalidades de Cortafuegos + (opcionalmente) todos los servicios adicionales
  - Si se ve comprometido, todo el sistema se compromete
- **Opción 1:** router con filtrado de paquetes
  - Opción más simple, pero menos potente
  - Escasas posibilidades de monitorización
- **Opción 2:** equipo dedicado (*dual homed host*)
  - Sistema estándar con 2 interfaces de red con la posibilidad de encaminamiento activada y regulada por las reglas de filtrado
  - Todas las conexiones pasan a través de él
  - Puede integrar los Proxies precisos

Topologías de cortafuegos II

(a) Cortafuegos básico de borde (cont.)

- Organizacion típica *dual homed host*
  - Los equipos de la red externa sólo pueden comunicarse con el *dual homed host*
  - Idealmente, lodos los servicios al exterior se ofrecerán únicamente desde el *dual homed host*
  - Equipos de red interna y externa no deberían poder entrar en contacto directamente, sino a través de un intermediario (Proxy)

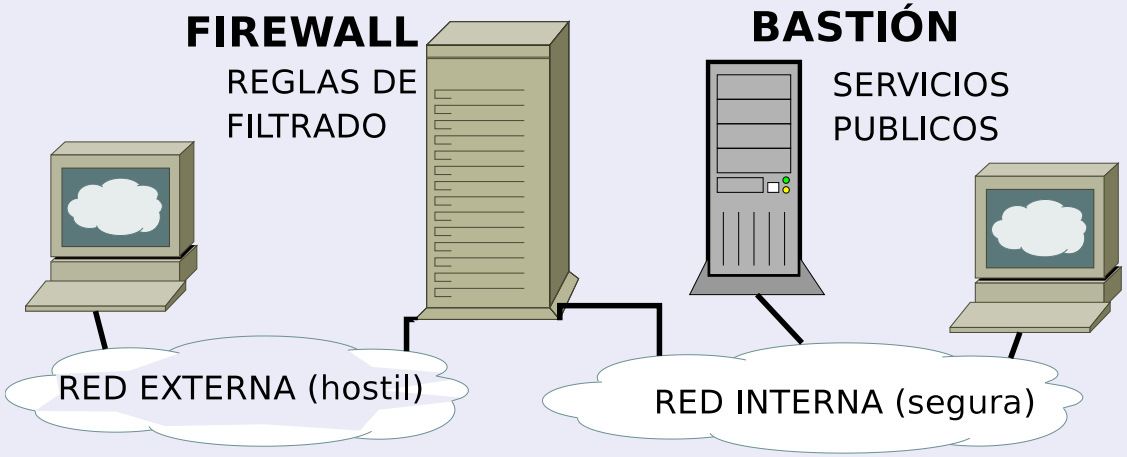


Topologías de cortafuegos III

(b) Host oculto (*screened host*)

Ofrecer los servicios (internos y externos) en una única máquina ubicada en el interior (red protegida)

- alojará a los Proxies de aplicación usados por la red interna
- alojará los servicios ofrecidos al exterior
  - en esquema anterior estaban en el Cortafuegos o repartidos en la LAN interna



Topologías de cortafuegos IV

(b) Host oculto (*screened host*)

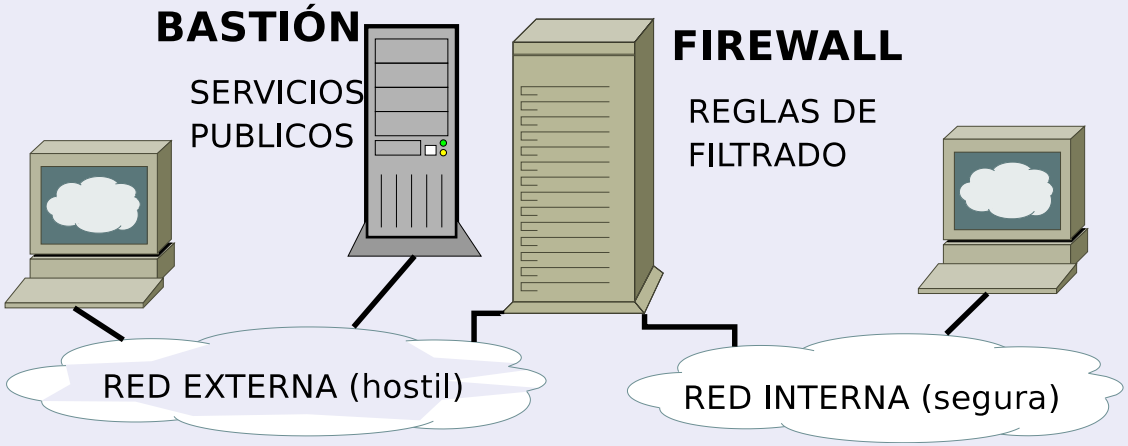
Única/s máquina/s accesible/s desde exterior (*host/s bastion*)

- Elemento potencialmente vulnerable por ser el único accesible desde exterior
  - atacantes externos pueden aprovechar vulnerabilidades no corregidas que permiten ejecución de *exploits*
  - una vez conseguido el control del *host bastión* posible extender ataque a otros equipos de la red interna
- Administración delicada (base de la seguridad de este esquema)
  - mínimos servicios software instalados (sólo los imprescindibles)
  - actualizaciones de seguridad del S.O. + servidores
  - monitorización de ficheros de log

Topologías de cortafuegos V

(c) Host inseguro (*untrusted host*)

- Variante del anterior
- El *host bastión* con los servicios hacia el exterior se ubica fuera de la red protegida
  - Cortafuegos no tiene efecto sobre él
- Características:
  - ofrece los servicios públicos sin debilitar la red interna
  - configuración y administración delicada



Topologías de cortafuegos VI

(d) Red de Perímetro/Zona Desmilitarizada(DMZ)

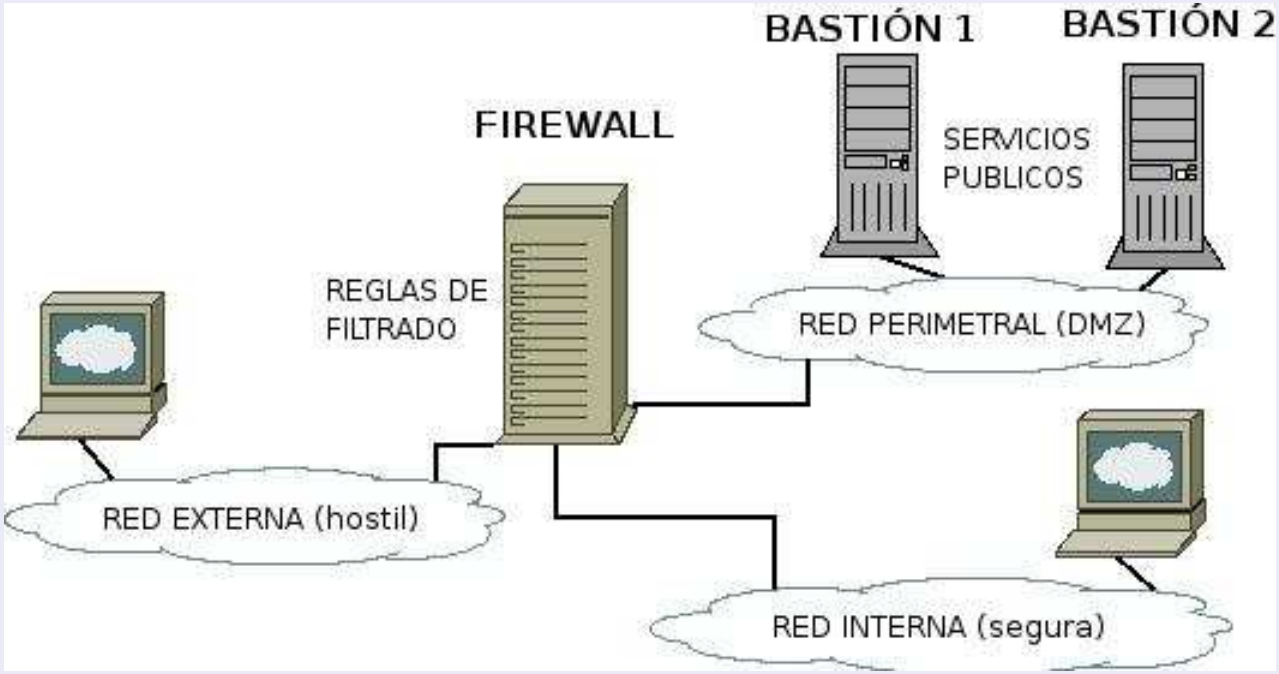
Objetivo: aislar servicios al exterior en una red separada para evitar acceso a la red protegida

- *Host inseguro* se sitúa detrás del Cortafuegos en una red aislada propia (red DMZ)
- Incrementa seguridad, fiabilidad y disponibilidad del *host inseguro*
- Equipos internos siguen sin poder confiar en ese host
  - Idealmente Cortafuegos evita (o limita al máximo) conexiones desde DMZ a red interna
- Dentro de DMZ puede ubicarse más de 1 *host bastión*
  - DMZ define una red de servicios públicos
  - DMZ suele incluir { proxies de aplicación para red interna; servicios que requieran acceso desde exterior }

Topologías de cortafuegos VII

(d) Red de Perímetro/Zona Desmilitarizada(DMZ) (cont.)

Implementación: Cortafuegos con 3 interfaces



Topologías de cortafuegos VIII

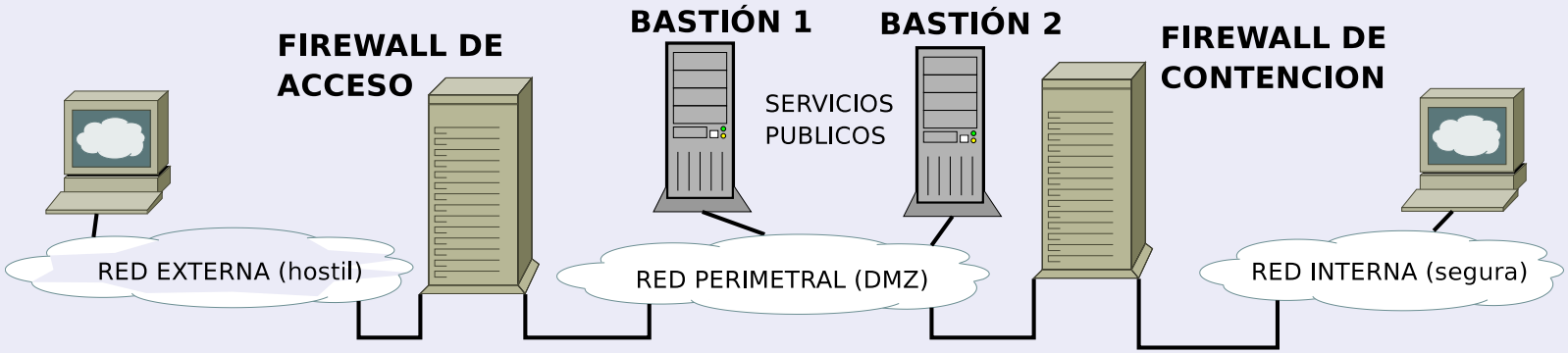
(e) DMZ con doble firewall (*screened subnet*)

Mejora del esquema anterior: añade un segundo cortafuegos

- cortafuegos externo (de acceso): bloquea tráfico no deseado externo → DMZ
- cortafuegos interno (de contención): bloquea tráfico no deseado DMZ → interno

Idea: aumentar la separación entre la red de servicios externos(DMZ) y la red interna

- DMZ se sitúa entre cortafuegos externo e interno
- Se crean 2 niveles de seguridad (red DMZ + red interna)
- Tráfico de exterior a red interna debe atravesar 2 cortafuegos



(e) DMZ con doble firewall (cont.)

Mejora tolerancia a fallos: evita puntos únicos de fallo

- Superando cortafuegos externo (acceso), sólo quedaría desprotegida DMZ
- Aún comprometiendo un equipo de la DMZ, se contaría con el cortafuegos de contención (no hay acceso directo desde DMZ a red interna)

Ventajas.

- Mejora seguridad y tolerancia a fallos
- Mayor flexibilidad: pueden definirse tantas DMZ como sea preciso, con distintos niveles de seguridad

Limitaciones.

- Dificultad de administración (gestionar 2 conjuntos de reglas de filtrado funcionando en conjunto)
- Sensación de falsa seguridad

Redes Virtuales Privadas

VPN *(Virtual Private Network)*: Conjunto de tecnologías que permiten extender el alcance de una red local (privada) sobre la infraestructura de una red pública no controlada, manteniendo la confidencialidad del tráfico.

- Suelen basarse en el concepto de *tunneling*
  - Se crea/mantiene una conexión lógica entre dos extremos
  - Encapsulado de tráfico de un protocolo dentro de paquetes de otro protocolo distinto
- Hacen uso de enlaces cifrados para definir conexiones protegidas entre porciones ”separadas” de la propia red
- Ejemplos típicos:
  - Interconexión ”segura” entre 2 delegaciones de una misma organización usando una red pública no segura (Internet) [VPN punto a punto]
  - Conexión segura de un usuario a la red interna desde equipos fuera de la red de la organización [VPN de acceso remoto]
- Evitan el uso de lineas dedicadas
  - menor coste (red pública *vs.* enlace de pago)
  - mayor flexibilidad

Tecnologías de VPNs (I)

IPsec: *Internet Protocol Security*

Familia de protocolos que protegen el tráfico a nivel IP (capa 3 [red])

- Forma parte de IPv6, pero existe la especificación permite usarlo sobre redes IPv4
  - define nuevos formatos de paquetes (cabeceras) compatibles con IPv4
- Ofrece autenticación e integridad de los paquetes y, opcionalmente, confidencialidad (cifrado)
- Incluye protocolos para la negociación de claves entre los extremos
- Contempla la protección del tráfico:
  - entre un par de hosts *(host-to-host)*
  - entre un par de redes *(network-to-network)*
  - entre un host y una red *(host-to-network)*
- Concepto clave: asociaciones de seguridad *(SA, Security Association)*
  - ”Enlace lógico” unidireccional entre los 2 extremos de una conexión IPsec
  - Se corresponde con el conjunto de parámetros de seguridad (claves, etc) que caracterizan la conexión IPsec
  - Identificada por un SPI (*Security parameters index*) único

Protocolos IPsec

Protocolo **AH** (*Authentication Headers*)

- proporciona integridad y autenticidad del origen
- emplea funciones HMAC (*Hash based Message Authentication Code*) con claves secretas

Protocolo **ESP** (*Encapsulating Security Payloads*)

- proporciona integridad y autenticidad (con HMAC)
- proporciona confidencialidad (con cifrado simétrico [clave secreta])

Protocolo **ISAKMP** (*Internet Security Association and Key Management Protocol*)

- Esquema/framework para el intercambio de claves
- Fija/acuerda los parámetros de las SAs
- Claves ”precompartidas”, protocolo IKE (*Internet Key Exchange*), ...

Modos de funcionamiento IPsec

- **Modo transporte**
  - Las cabeceras IPsec protegen la carga útil (datos de la capa de transporte)
  - Esquema habitual en comunicaciones IPsec entre equipos finales *host-to-host*
- **Modo túnel**
  - Las cabeceras IPsec protegen la totalidad del paquete IP ”original”
  - Se encapsula un paquete IP completo (cabecera+carga útil) dentro de un paquete IPsec
  - Esquema habitual en comunicaciones IPsec entre pasarelas IPsec *network-to-network*
  - Es el modo habitual de conformar VPN sobre IPsec

Tecnologías de VPNs (II)

PPTP: *Point to Point Tunneling Protocol*

Protocolo de capa 2 desarrollado por Microsoft, 3Com y otros (RFC 2637). Encapsula paquetes PPP (*Point-to-Point Protocol*) dentro de datagramas IP tunel

- PPP es un protocolo de capa 2 (enlace) para establecer una comunicación directa entre 2 equipos (punto a punto)
- Usado frecuentemente en las conexiones de acceso a internet
- PPP soporta opcionalmente cifrado, autenticación y compresión de los paquetes enviados

Los datagramas IP que encapsulan paquetes PPP circulan por una red TCP/IP pública (”internet”)

- Se inicia el tunel con una conexión al puerto TCP 1723 del destino
- El tunel en sí encapsula los paquetes PPP dentro de paquetes del protocolo GRE *(Generic Routing Encapsulation)*

PPTP no soporta por sí mismo confidencialidad (cifrado) o autenticación

- Delega esas tareas en el protocolo PPP
- Actualmente se considera que su seguridad es deficiente

Tecnologías de VPNs (III)

L2TP: Layer 2 Tunneling Protocol

Protocolo genérico para *tunneling*

- Evolución/mejora de PPTP
- Habitualmente en VPNs ”porta” (encapsula) paquetes PPP

Paquetes L2TP encasulan el tráfico sobre paquetes UDP
L2TP no proporciona condifencialidad ni autenticación por sí mismo.

- Suele combinarse con IPsec (L2TP/IPsec)

Otros: VPNs de nivel de transporte/aplicación

Posibilidad de establecer conexiones cifradas en nivel de transporte o de aplicación sobre las cuales encapsular tráfico.

- **Túneles SSH**

  El protocolo de capa de aplicación SSH (*Secure Shell*) permite la redirección de puertos (locales o remotos) sobre la conexión SSH establecida entre el cliente y el servidor

- **OpenVPN**

  OpenVPN permite encapsular tráfico IP sobre una conexión SSL/TLS *Secure Socket Layer/Transport Layer Secure* [capa de transporte] establecida entre los dos extremos del túnel cifrado.

OpenVPN (I)

OpenVPN es una implementacion de VPN que usa el protocolo SSL/TLS *(Secure Socket Layer/Transport Layer Security)* para crear enlaces de red cifrados.

- Usualmente emplea la implementación OpenSSL
- Web: http://www.openvpn.net

Permite 3 modos de operación:

Host a Host: crea un enlace cifrado entre dos máquinas independientes

Road Warrior: permite que un usuario se conecte al servidor OpenVPN desde fuera de la red propia y pueda acceder a sus recursos

Red a Red: permite que 2 redes separadas pueden comunicarse para formar una sóla red

- Se crea la sensación de que están unidas por un enlace virtual
- Tráfico de comunicación enviado sobre la red pública va cifrado

OpenVPN (II)

Funcionamiento:

- Se establece una conexión SSL cifrada entre los 2 extremos usando la red pública (por defecto usa el puerto 1194 UDP)
- En los equipos conectados se crearán interfaces de red virtuales (*tun0, tun1, ...*) para acceder a esa conexión
  - Funcionarán como un interfaz de red convencional (*ethX*)
  - Tendrán dir. IP asignada, participan en las reglas de enrutado, su tráfico puede ser filtrado por el firewall, etc
- El tráfico IP que reciban/envíen se encapsulará sobre la conexión SSL y se envía cifrado

OpenVPN (III)

OpenVPN soporta 2 modos de autenticación/cifrado

Clave estática: se genera una clave secreta estática que será compartida por los 2 extremos

- Esquema sencillo de configurar e implantar
- Exige un mecanismo seguro para el intercambio previo de la clave y la protección de esa clave en ambos extremos

Modo SSL: hace uso del mecanismo de establecimiento de sesiones SSL (basado en certificados digitales) para acordar una clave de sesión temporal que se usará para cifrar cada conexión concreta

- Exige que ambos extremos tengan certificados digitales firmados por una autoridad reconocida por ambos

Funcionamiento SSL/TLS

SSL: *Secure Socket Layer*

- Desarrollo inicial por Netscape
- Inicalmente para proteger tráfico HTTP, aplicable en otros protocolos.
- Actualmente es el estándar TLS (*Transport Later Security*)

Protege el tráfico empleando cifrado asimétrico, cifrado simétrico y HMAC (autenticación de mensajes con HASH + clave secreta), garantizando:

1. **Autenticación de las entidades (servidor y/o cliente):** empleando certificados digitales
2. **Confidencialidad de los mensajes:** empleando cifrado simétrico con claves de cifrado negociadas/acordadas en cada conexión
3. **Integridad y atenticidad de los mensajes:** uso de HMAC con claves de autenticación negociadas/acordadas en cada conexión

Establecimiento de conexión

- Intercambio de certificados servidor y cliente (opcional)
- Si son reconocidos: intercambio seguro de clave secreta maestra (mediante cifrado asimétrico)

Tráfico de mensajes

Cifrados + autenticados con claves de sesión generadas a partir de la clave

Sistemas de detección de intrusiones (IDS)

Intrusión: Conjunto de acciones que pretenden comprometar la confidencialidad, integridad o disponibilidad de un recurso (red o equipo)

- Origen: atacantes externos, usuarios internos, software malicioso (*malware*)

Sistemas de detección de intrusiones

IDS (*Intrusion Detection Systems*): Monitorizan redes o sistemas para detectar e informar actividades o accesos no autorizados.

- Generan alertas y registran los eventos detectados
- Opcionalmente, correlacionan eventos detectados con info. adicional (alertas de cortafuegos, BD de vulnerabilidades, etc)

Pasivos $\rightarrow$ detectan + generan alertas

Sistemas de prevención de intrusiones

IPS (*Intrusion Prevention Systems*): Monitorizan redes o sistemas para detectar e intentar impedir actividades o accesos no autorizados.

- Funcionamiento "*en-linea*" (analizan y actúan "sobre la marcha")
- Bloquean/descartan los paquetes o las acciones sospechosas o no permitidas

Activos $\rightarrow$ detectan + bloquean la intrusión

IDS e IPS complementan a otros mecanismos de seguridad (cortafuegos, cifrado, etc)

Tipos de IDS/IPS (I)

NDIS: detectores de intrusiones en red

Capturan el tráfico de la red (ubicados en ”zonas estratégicas”: DMZ, routers de acceso, etc) y lo evaluan para determinar si se corresponde con una intrusión

- Análisis de intrusiones a nivel de paquetes de red
- Monitoriza todo el tráfico de una porción de la red (on-line [captura y análisis simultáneto] u off-line [captura y análisis posterior])
  - Suelen hacer uso de sniffers conectados a hubs, puertos de administración de switches (*span ports*), bridges (dispositivos TAP)
- Sensores accesibles a través de la red de la organización o mediante una ”red de gestión” separada
- Suelen centrarse en detectar ataques DOS (*Denial Of Service*), escaneo de puertos, paquetes malformados, explotación de vulnerabilidades (en servicios o aplicaciones), etc
- Ejemplos: SNORT (`http://www.snort.org`), Suricata (`http://www.openinfosecfoundation.org`)

Tipos de IDS/IPS (II)

HDIS: detectores de intrusiones en host

Analizan los eventos que se producen en un equipo (host) determinado para determinar si está sufiendo un ataque

- Sensores (agentes) monitorizan un equipo concreto
- Aspectos monitorizados:
  - Logs del sistema y de las aplicaciones
  - Llamadas al sistema
  - Modificaciones sobre el sistema de ficheros (BD con hashes de ficheros/directorios sensibles)
- Suelen centrarse en detectar el ”abuso” de privilegios (escalada de privilegios)
- Ejemplos: OSSEC (`http://www.ossec.net`), SAGAN (`http://sagan.quadrantsec.com`), TRIPWIRE(`http://www.tripwire.com`)