Capítulo 7.
SEGURIDAD PERIMETRAL

Autor: Jesús Costas Santos

SEGURIDAD PERIMETRAL

Índice de contenidos

SEGURIDAD PERIMETRAL

7.1.CORTAFUEGOS

- Red corporativa interconectada a Red pública, los peligros de ataque a sus servidores, *routers* y sistemas internos se multiplican.
- Seguridad perimetral: 1ª línea de defensa entre las redes públicas y redes corporativas o privadas.
- **Cortafuegos** o *firewall*: bloquear las conexiones no autorizadas,
- **Proxy:** intermediario entre clientes y servidores finales, filtrado y monitorización de servicios.

SEGURIDAD PERIMETRAL

7.1.CORTAFUEGOS

- Un cortafuegos o *firewall*: aplicación o dispositivo bloquear comunicaciones no autorizadas, permitiendo las que si lo están.
- Configuración para permitir y limitar el tráfico entre diferentes redes o ámbitos de una red: conjunto de normas y reglas.
- Las características fundamentales de los cortafuegos son:
  - Filtrado de paquetes inspección de direcciones de red: MAC, IP o puerto origen y destino, con este último filtrado según las aplicaciones asociadas a dicho puerto.
  - Filtrado por aplicación.
  - Reglas de filtrado sobre el tráfico de salida o de entrada en un determinado interfaz de red.
  - Registro o logs del filtrado de paquetes.

SEGURIDAD PERIMETRAL

7.1.CORTAFUEGOS

- Ejemplo práctico:
  - GNU/Linux: cortafuegos por excelencia: Iptables. Integra funciones de NAT en enrutamiento.
  - Contiene serie de cadenas de reglas de filtrado en 3 tablas.
  - Orden importante: lee de manera secuencial las cadenas de reglas.
  - iptables -t [tabla] - -[tipo_operación] -- [cadena]-- [regla_con_parámetros] - - [acción].
    - Tablas: filter, NAT y mangle (no muy usada).
    - Operación: A (añadir), L (listar), F (borrar)
    - Cadena: -i (interfaz), -s (origen), -p (protocolo), -d (puerto)
    - -j: ACCEPT, DROP, MASQUERADE (NAT), LOG
    - LOG: *cat /var/log/iptables.log*. Añadir previamente en /etc/rsyslog.d/50-default.conf:
    - kern.warning /var/log/iptables.log

SEGURIDAD PERIMETRAL

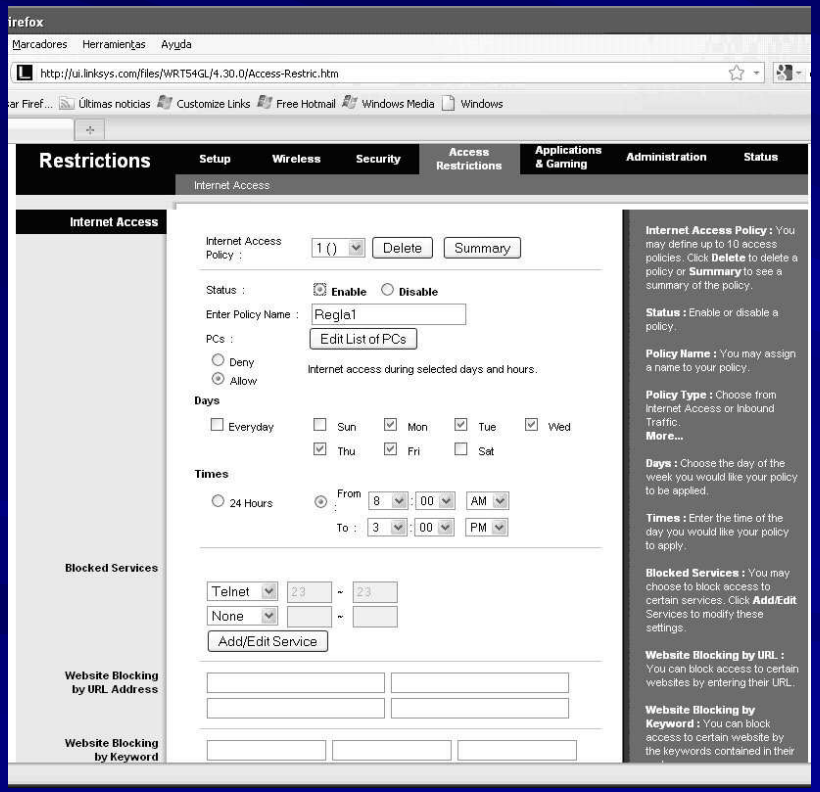
7.1.3. TIPOS DE CORTAFUEGOS

- Una clasificación posible es por la **ubicación** en la que se encuentre el *firewall*:
  - **Firewalls basados en servidores**: aplicación de *firewall* instala y ejecuta en un sistema operativo de red (NOS), junto a otra serie de servicios como enrutamiento, proxy, DNS, DHCP, etc.
  - **Firewalls dedicados**: equipos que tienen instalado una aplicación específica de cortafuegos, trabajan de forma autónoma como cortafuegos.
  - **Firewalls integrados**: se integran en un dispositivo hardware para ofrecer la funcionalidad de *firewall*. Como ejemplos encontramos *switches* o *routers* que integran funciones de cortafuegos.
  - **Firewalls personales**: se instalan en los distintos equipos de la red de forma que los proteja individualmente de amenazas externas. Por ejemplo en un equipo doméstico el cortafuegos preinstalado en sistema operativo Windows.

SEGURIDAD PERIMETRAL

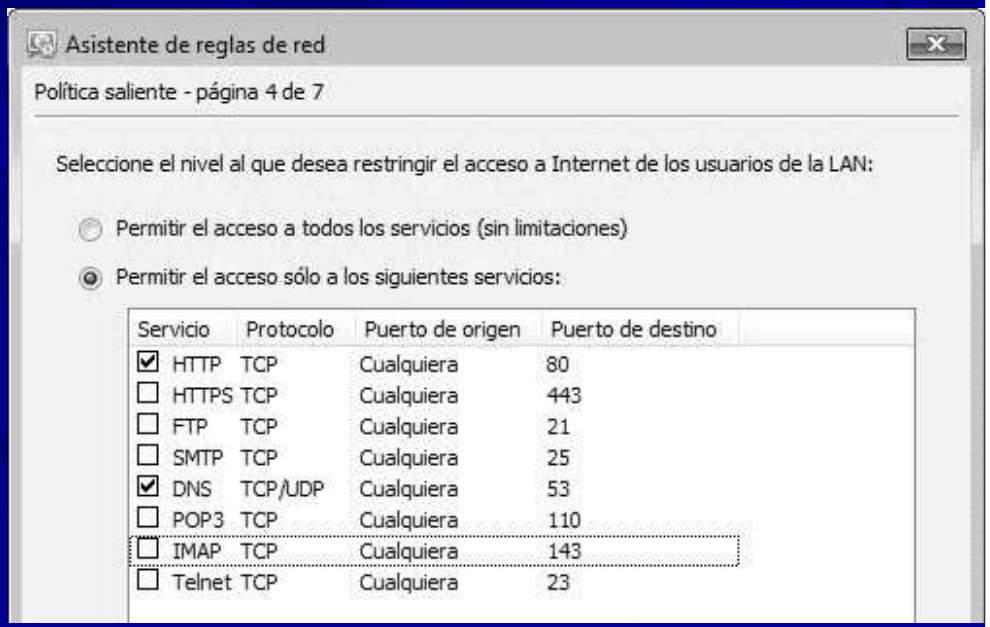
7.1.3. TIPOS DE CORTAFUEGOS

Cortafuegos integrado en router



Cortafuegos de escritorio:

Kerio Winroute Firewall



SEGURIDAD PERIMETRAL

7.1.3. TIPOS DE CORTAFUEGOS

- Para el caso de los *routers* CISCO de gama media y alta, es posible configurar listas de control de acceso o ACL.
- ACL: listas de condiciones aplican al tráfico que viaja a través de una interfaz del *router*, y se crean según el protocolo, la dirección o el puerto a filtrar.
- Existen dos tipos de ACL:
  - ACL estándar, solo especificar una dirección de origen.
  - ACL extendida, aparece el protocolo y una dirección de origen y de destino, ofrecen un mayor control.

SEGURIDAD PERIMETRAL

7.1.4. DMZ

- Las arquitecturas de cortafuegos más implementadas son:
  - **Screening router**: frontera entre la red privada y la red pública un *router* que realiza tareas de filtrado.
  - **Dual Homed-Host**: frontera un equipo servidor tareas de filtrado y enrutamiento mediante al menos 2 tarjetas de red.
  - **Screened Host**: *router* fronterizo exterior + servidor proxy filtrará y permitirá añadir reglas de filtrado en las aplicaciones más empleadas.
  - **Screened-subnet**: creación de una subred intermedia, denominada **DMZ** o **zona desmilitarizada**, entre red externa y red privada interna, 2 niveles de seguridad, uno algo menor en el cortafuegos más externo y uno de mayor nivel de seguridad en el cortafuegos de acceso a la red interna.
- En DMZ: se ubican los servidores HTTP, DNS, FTP y otros que sean de carácter público.

SEGURIDAD PERIMETRAL

7.2. PROXY

- Un servidor proxy: aplicación o sistema que gestiona las conexiones de red, sirviendo de intermediario entre las peticiones de servicios que requieren los clientes, como http, FTP, irc, telnet, ssh, etc., creando así una memoria caché de dichas peticiones y respuestas por parte de los servidores externos.
- La finalidad: poder servir más rápidamente conexiones siguientes que hayan sido solicitadas.
- Añaden **funciones** de control y autenticación de usuarios, y reglas de filtrado de los contenidos solicitados, así como registro de logs.
- Ventajas: mejora de velocidad de respuesta a peticiones y proporciona seguridad en acceso a contenidos.

SEGURIDAD PERIMETRAL

7.2.1. Tipos, características y funciones principales

- **Proxy caché Web:** aplicación específica acceso a la web. Mantienen copias locales de los archivos mas solicitados.
- **Proxy NAT**: integración de los servicios de traducción de direcciones de red y proxy.
- **Proxy transparente**: normalmente, configurar cada cliente manualmente. En este caso no es necesario configurar el cliente. Combina un servidor proxy con NAT las conexiones al puerto 80, son redirigidas hacía el puerto del servicio proxy.
- **Proxy anónimo**: aumentar la privacidad y el anonimato de los clientes proxy, mediante una activa eliminación de características identificativas (dirección IP del cliente, cabeceras From y Referer, *cookies*, identificadores de sesion...).
- **Proxy inverso:** servidor proxy instalado en una red con varios servidores web, intermediario a las peticiones externas, capa de seguridad previa, gestión y distribución de carga de las distintas peticiones externas, gestión de SSL o como caché de contenidos estáticos.
- **Proxy abierto**: acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

SEGURIDAD PERIMETRAL

7.2.1. Tipos, características y funciones principales

- GNU/Linux: Proxy por excelencia Squid y Dansguardians.
- Squid: Archivo de configuración: /etc/squid3/squid.conf.
  - Puerto de escucha: http_port 3128
  - Dirección de la caché y el tamaño:
    - cache_dir ufs /var/spool/squid3 2000 16 256
    - cache_mem 32 MB
    - maximum_object_size_in_memory 256 MB
  - Direcciones logs de acceso al proxy y de caché
    - access_log /var/log/squid/access.log
    - cache_log /var/log/squid/cache.log

SEGURIDAD PERIMETRAL

7.2.1. Tipos, características y funciones principales

- Autenticación de usuarios:
  - *auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/claves*
  - *acl passwd proxy_auth REQUIRED*
- Añadir usuarios a /etc/squid3/claves:
  - *htpasswd –c /etc/squid3/claves pepe*

SEGURIDAD PERIMETRAL

7.2.1. Tipos, características y funciones principales

- Filtrado:
  - *acl nopermitidas url_regex "/etc/squid/nopermitidas"*
  - *acl nowebs dstdomain "/etc/squid/nowebs"*
  - *http_access deny nopermitidas*
  - *http_access deny nowebs*
- Proxy transparente: redirección peticiones puerto 80 al 3128 (proxy-squid):
  - *iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128*
- Otras funciones: Añadir blacklist descargada o gestión web mediante módulo squid en webmin.

SEGURIDAD PERIMETRAL

DIRECCIONES DE INTERÉS

- Completa información práctica sobre iptables:
  - http://www.kriptopolis.org/iptables-0
- Listado de cortafuegos personales:
  - http://www.infospyware.com/cortafuegos/
- Configuraciones prácticas de cortafuegos:
  - http://www.pello.info/filez/firewall/iptables.html
- Configuraciones de enrutamiento, Proxy y cortafuegos para GNU/Linux:
  - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/frames/frameset_14.html
- Configuraciones de enrutamiento para Windows:
  - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_enrutamiento.htm
- Configuraciones de funciones de cortafuegos, proxy-caché y servidor VPN para Windows, mediante ISA Server:
  - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_isa.htm
- Blacklist o listado de URL y dominios maliciosos, categorizados, para ser intergados en servidores Proxy como Dansguardians y Squid.
  - http://urlblacklist.com
- Manual práctico Iptables:
  - http://lucas.hispalinux.es/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/

SEGURIDAD PERIMETRAL

SOFTWARE-SIMULADORES

- Simuladores de configuración de dispositivos como router-punto de acceso inalámbrico TP-LINK.
  - http://www.tp-link.com/support/simulator.asp
  - http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm
- Simulador del router inalámbrico Linksys WRT54GL:
  - http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm
- Simuladores de routers inalámbricos D-Link:
  - http://support.dlink.com/emulators/dwlg820/HomeWizard.html
  - http://support.dlink.com/emulators/dsl2640b/306041/vpivci.html
  - http://support.dlink.com/emulators/dwl2100ap
  - http://support.dlink.com/emulators/di604_reve

SEGURIDAD PERIMETRAL

SOFTWARE

- ISA Server: Microsoft Internet Security and Acceleration Server, gestión integral de seguridad para entornos Windows Server.
  - http://www.microsoft.com/spain/isaserver/default.mspx
- Forefront TMG: Microsoft Forefront Threat Management Gateway, Nuevo entorno de gestión integral de seguridad para entornos Windows Server.
  - http://www.microsoft.com/forefront/en/us/default.aspx
- Iptables: cortafuegos de sistemas GNU/Linux.
  - http://www.netfilter.org/
- Squid: servidor Proxy, entornos GNU/Linux.
  - http://www.squid-cache.org/
- Dansguardians: servidor Proxy, entornos GNU/Linux.
  - http://dansguardian.org/
- WinGate: software Proxy Server para sistemas Windows.
  - http://www.wingate.com/
- Webmin: gestión intergal de servicios como Proxy en sistemas operativos GNU/Linux, desde entorno web.
  - http://www.webmin.com/
- Kerio Winroute firewall: gestión integral bajo Windows, con funciones de enrutamiento y cortafuegos.
  - http://www.kerio.com/
- Zone Alarm: Software cortafuegos - firewall
  - http://www.zonealarm.com/security/es/zonealarm-pc-security-free-firewall.htm?lid=es

SEGURIDAD PERIMETRAL

NOTICIAS

- Chinos aprenden a evitar el "Gran Firewall" de internet
  - Fuente: http://www.bbc.co.uk/mundo/ciencia_tecnologia/2010/03/100320_china_internet_control_censura_firewall_jp.shtml