FIREWALLS

Mónica Ribes
Junio 2.000

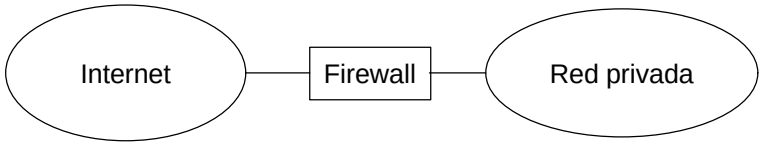
1

ÍNDICE

2

¿QUÉ ES UN FIREWALL?

Sistema que protege una red de otra en la que no se tiene confianza.



3

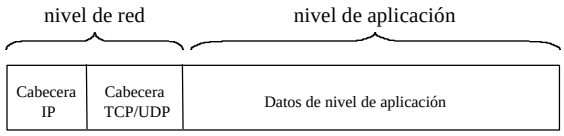
DECISIONES DE DISEÑO

- Aquello que no esté expresamente permitido está prohibido
- Aquello que no esté expresamente prohibido está permitido

4

TIPOS DE FIREWALL

- Firewall a nivel de red
- Firewall a nivel de aplicación



5

FIREWALL A NIVEL DE RED

Filtrado de paquetes según:

- La dirección IP origen
- La dirección IP destino
- Campo de opciones IP
- El protocolo a nivel de transporte

Cabecera IP

- El puerto origen y destino
- Banderas SYN/ACK (sólo TCP)

Cabecera TCP/UDP

6

FIREWALL A NIVEL DE RED

Software gratuito:

⇨ Para PC: **ftp://ftp.net.ohio-state.edu/pub/kbridge**

⇨ Para Unix: **ftp://ftp.cisco.com/pub/acl-example.tar.gz**

7

FIREWALL A NIVEL DE APLICACIÓN

Ordenador que ejecuta un software de servidor proxy.

CARACTERÍSTICAS:

- Conexión a nivel de aplicación
- Depende del servicio
- Requiere modificaciones de clientes
- Suministran informes

8

FIREWALL A NIVEL DE APLICACIÓN

Los servidores proxy más populares son:

- Para Unix y Linux:
  - **TIS Internet Firewall Toolkit**
    http://www.tis.com/docs/products/fwtk/index.html
  - **SOCKS**
    http://www.socks.ben.com
- Para Windows NT
  - **Microsoft Internet Information Server**
  - **Netscape Commerce Server**

9

ARQUITECTURAS MÁS POPULARES DE FIREWALL

Firewall a nivel de red:

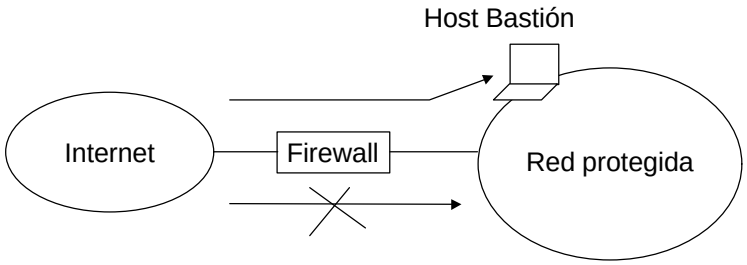
- **"Screened host Firewall"** (Firewall mediante filtrado de host)
- **"Screened subnet Firewall"** (Firewall mediante filtrado de subred)

Firewall a nivel de aplicación:

- **"Dual homed gateway"** (Firewall mediante host de doble conexión o gateway de dos dominios)

10

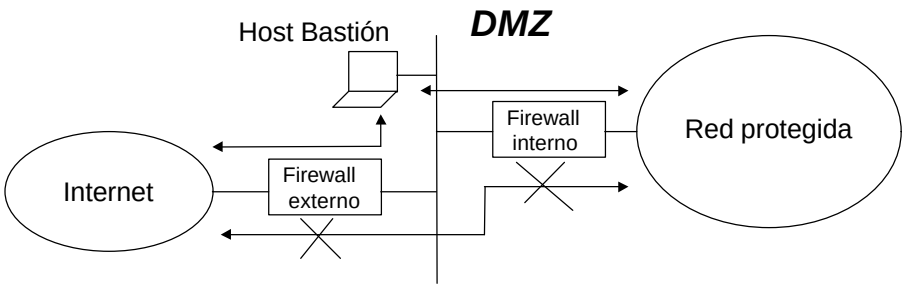
“SCREENED HOST FIREWALL”



El router sólo permite tráfico desde/hacia el host bastión

11

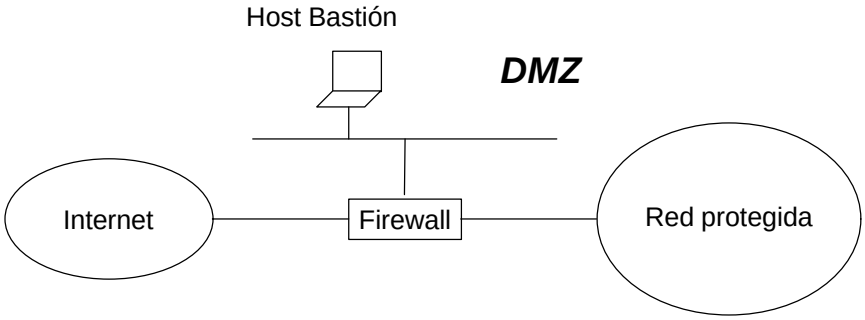
“SCREENED SUBNET FIREWALL”



El firewall sólo permite tráfico desde/hacia la DMZ (demilitarized zone) de la red.

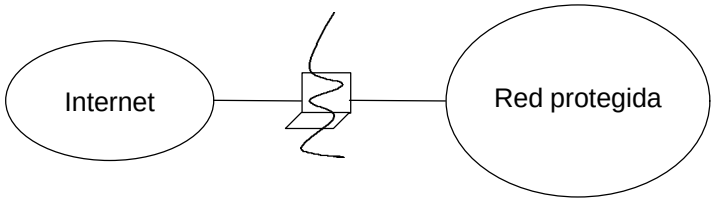
12

“COLLAPSED DMZ TOPOLOGY”



13

“DUAL HOMED GATEWAY”



Deshabilitado el encaminamiento IP.

14

LIMITACIONES DE LOS FIREWALLS

- No protege frente a desastres
- No protege frente a los virus
- “No autentifica el origen de los datos”
- “No garantiza confidencialidad de los datos”

15

CASO PRÁCTICO

Estudio realizado por la Universidad de Southampton en Gran Bretaña.

Objetivos:

- Mejorar la seguridad de la red sin limitar la libertad académica
- Suministrar un metodología para la configuración del firewall
- Suministrar unas pautas para evaluar los distintos firewalls comerciales
- Dar una visión de los productos actuales

16

FASES DEL PROYECTO

1. Evaluación de las distintas soluciones firewalls y elección de una de ellas
2. Configurar el firewall con todo permitido para analizar y clasificar el tráfico. Consultar a los usuarios por sus requerimientos futuros
3. Añadir filtros para bloquear servicios.
   Realizar seminarios para mentalizar a los usuarios
4. Refinamiento de los filtros
5. Un firewall basado en prohibición por defecto
6. Evaluación del funcionamiento del firewall

17

1.EVALUACIÓN DE UN FIREWALL

COSTE: hardware, software, extras (p.e. VPN), instalación, formación, administración, mantenimiento y actualizaciones.

FUNCIONALIDAD:

- *INTERFACES:* máximo número, medios soportados (10/100Mbps Ethernet, Gigabit Ethernet ATM, FDDI, Token Ring)
- *FILTRADO:* ¿a nivel de red o a nivel de aplicación? Si tiene un proxy, ¿qué protocolos cubre? ¿Puede filtrar por hora del día?
- *CONTROL DE CONTENIDO:* p.e. exploración de virus, “applets” de Java

18

1.EVALUACIÓN DE UN FIREWALL (II)

- *AUTENTIFICACIÓN:* ¿Soporta passwords, S/Key, Radius, TACACS o SecurID?
- *DETECCIÓN DEL ATAQUE NEGACIÓN DE SERVICIO (DoS):* Los sistemas de detección de intrusos, ¿eliminan la conexión manualmente?, ¿se pueden modificar las reglas en tiempo real para reaccionar contra DoS?
- *¿SOPORTA VPN?*
- *¿SOPORTA NAT?*
- *INFORMES:* ¿cuál es el nivel de detalle?, si el firewall es atacado ¿los logs pueden ser alterados o borrados?, ¿puede el producto alertar de los ataques?, ¿incluye herramientas de análisis de logs?, ¿son fáciles de leer estos informes?

19

1.EVALUACIÓN DE UN FIREWALL(III)

- *INTERFACE DE USUARIO:* ¿está basado en un browser, tipo consola?, ¿hay alguna herramienta de configuración remota?, si es así ¿es segura?, ¿es el interface fácil de usar? ¿soporta SNMP?
- *SEGURIDAD DEL FIREWALL:* ¿cómo de segura es la plataforma del firewall?
- *TOLERANCIA A FALLOS*
- *ARQUITECTURA DEL FIREWALL:* ¿el hardware es propietario o no?, ¿funciona sobre Win NT, sobre Unix o sobre otra plataforma? ¿el S.O. utilizado tiene futuro?
- *RENDIMIENTO:* ¿por hardware o software?, ¿cuál es la velocidad de transmisión de paquetes?, ¿cuál es el “overhead” de la encriptación VPN?

20

1.EVALUACIÓN DE UN FIREWALL(IV)

DOCUMENTACIÓN, MANTENIMIENTO Y SOPORTE TÉCNICO

VARIOS: ¿existe una versión de demostración para la evaluación durante un período adecuado?, ¿cuáles son las credenciales del fabricante del firewall, nº de años en el negocio, tamaño de la base instalada,...?, ¿hay artículos en revistas acreditadas que corroboren la fiabilidad del firewall?

21

1. ELECCIÓN DE HARDWARE Y SOFTWARE

- HARDWARE

Opciones:

-PC: no ofrece ni fiabilidad ni escalabilidad

-Unix: sólo soporta el software de Gauntlet, y hay otros software más interesantes

-Equipo de Fore System: muy caro

-Equipo de Nokia: plataforma propietaria y escalable a un alto precio

-Sun: ventajas: -flexible para escoger el software de firewall
-buen precio
-futuro S.O. asegurado
-sencillo de mantener y actualizar

22

1. ELECCIÓN DE HARDWARE Y SOFTWARE

- SOFTWARE

Opciones:

-SunScreen EFS 3.0 de Sun

-Firewall-1 de Check Point

Ventajas:-producto maduro

-fácil de usar

-bien documentado

-módulos opcionales de VPN

-soporta una amplia variedad de métodos de autentificación

-amplia base instalada

23

3.FILTROS FIREWALL-1

RULE	SOURCE	DESTINATION	SERVICES	ACTION
1	Any	ECS	BackOrifice	
			Netbus	reject
2	ECS	Any	BackOrifice	
			Netbus	reject
3	Any	ECS	finger	reject
4	Any	ECS	SNMP	reject
5	Any	ECS	TFTP	reject
6	Any	ECS	lpd	reject
7	Any	ECS	nbname	
			nbsession	
			nbdatagram	reject
8	Any	dns-servers	DNS-TCP	accept

24

3.FILTROS FIREWALL-1(II)

RULE	SOURCE	DESTINATION	SERVICES	ACTION
9	Any	ECS	DNS-TCP	reject
10	sucs-nis-servers	nis-servers	NIS	accept
11	Any	ECS	NIS	reject
12	Any	mail-access-servers	pop-2 pop-3 imap	accept
13	Any	incoming-smtp-servers	smtp	accept
14	Any	ECS	pop-2 pop-3 imap	reject
15	Any	ECS	smtp	reject
16	Any	www-servers	http https	accept
17	ecml-clients	ecml-server	https	accept

25

3.FILTROS FIREWALL-1(III)

RULE	SOURCE	DESTINATION	SERVICES	ACTION
18	honours-clients	honours-server	https	accept
19	Any	ECS	http/https	reject
20	NatGallery	iip-server	telnet/ftp	accept
21	Any	iip-server	telnet/ftp	reject
22	Any	ftp-servers	ftp	accept
23	Any	ECS	ftp/tftp	reject
24	Any	login-servers	shell/login/telnet exec/ssh	accept
25	SUCS-CLUSTERS	ug-login-servers	telnet/ssh	accept
26	Any	ECS	shell/login/telnet exec/ssh	reject

26

3.FILTROS FIREWALL-1(IV)

RULE	SOURCE	DESTINATION	SERVICES	ACTION
27	SUCS-CLUSTERS	UG-VLAN	X11	accept
28	cardlock-mmc-server	cardlock	Cardlocks	accept
29	Any	cardlock	Any	reject
30	cvs-clients	cvs-server	cvs	accept
31	SUCS-CLUSTERS	cad-licence-server	cad-licence	accept
32	sucs-mbone-relay	mbone-relay	mbone	accept
33	SUCS-CLUSTERS	ug-nfs-servers	NFS-SGI	accept
34	Any	ECS	NFS-SGI	reject
35	sucs-webcache	ecs-webcache	squid-3130	accept
36	Any	news-server	nntp	accept
37	Any	ECS	nntp	reject
38	Any	Any	Any	accept

27

6. EVALUACIÓN DEL FUNCIONAMIENTO DEL FIREWALL

Productos:

- *Internet Security Systems* (IIS)
- *SAINT* (Security Administrator Integrated Network Tool) de World Wide Digital Security Inc. Última versión de SATAN. Gratis.

28

FIREWALLS FUTUROS

- Mejorar el rendimiento
- Procesado de nuevas aplicaciones (p.e. aplicaciones multimedia en tiempo real)
- Firewalls cooperativos
- IPv6

29

BIBLIOGRAFÍA

- ***The Use of Firewalls in an Academic Enviroment*****,** http://www.jtap.ac.uk/reports/htm/jtap-049.htm
- William R. Cheswick, Steven M. Bellovin.***Firewalls and Internet Security****.* Addison-Wesley.
- ***8 Cortafuegos en el banco de pruebas***, Comunicaciones World. Julio/Agosto 1.998
- John Vacca. ***Seguridad en Internet.*** Anaya Multimedia.
- Marcus Goncalves. ***Protecting your Web Site with Firewalls.*** Prentice Hall.

30