Firewalls – Proxys - AntiSpam

Filtro de información

José Juan Cerpa Ortega

Firewalls

- Dispositivo hardware o software
- Filtra tráfico TCP/UDP/IP/ICMP...
- Protege una red de otra expuesta
- Inútil si el sistema donde se instala es vulnerable
- Necesario desactivar servicios innecesarios
- Se suele ubicar en el nivel más exterior

Firewalls

- Los Firewalls NO proporcionan seguridad absoluta. Son un mecanismo más, y deben combinarse con otras medias de seguridad, tanto en redes como en sistemas operativos, para hacer el sistema lo más seguro posible.
- La única seguridad absoluta es aislar la máquina.

Firewalls

- Un firewall no detecta...
  - Ataques internos
  - Formas de ataques desconocidas
  - Virus
- Los firewalls se construyen a partir de...
  - Filtros : bloquear selectivamente los paquetes
  - Nodos bastion : Ordenadores altamente seguros expuestos directamente a internet.

Firewalls

- ¿Cómo crear una política de seguridad?
  - Describa para que es el servicio
  - Describa el grupo de personas a las que va dirigido el servicio
  - Describa a que servicio necesita acceder cada grupo
  - Describa para cada grupo de servicio como se puede mantener seguro el servicio
  - Redacte un informe en el que se considere violación cualquier otro tipo de acceso

Firewalls

- Política por defecto ACEPTAR
- Todo lo que venga de la red local al firewall ACEPTAR
- Todo lo que venga al puerto TCP 80 ACEPTAR
- Todo lo que venga al puerto TCP 25 ACEPTAR
- Todo lo que venga al puerto TCP 110 ACEPTAR
- Todo lo que venga al puerto UDP 53 ACEPTAR
- Todo lo que venga de la red local al exterior ENMASCARAR
- Todo lo que venga del puerto TCP 1 al 1024 DENEGAR
- Todo lo que venga del puerto UDP 1 al 1024 DENEGAR

Firewalls

- Hay 2 formas de implementar un firewall
  - Aceptar todo por defecto. Fácil de implementar pero “peligrosa”.
  - Denegar todo por defecto. El firewall es un muro aunque más difícil de configurar.
- IMPORTANTE : El orden en que se introducen las reglas es fundamental ya que las reglas se chequean por orden.

Firewalls

- Ipchains e Iptables son los firewalls implementados en los núcleos de los sistemas Linux.
- Ipchains está en desuso y la que se implementa en versiones desde la 2.4 como un servicio es iptables.
- Ejecutando iptables en la linea de comandos introducimos reglas que indicarán acciones a tomar ante recepción de paquetes

Firewalls

- Tres tipos de reglas:
  - Filtrado : INPUT, OUTPUT, FORWARD
  - Redirección : PREROUTING, POSTROUTING
  - Modificación de paquetes : MANGLE
- Opciones para las reglas
  - -A → añadir una regla
  - - I → inserta en una posición determinada
  - -R → reemplazar en una posición determinada
  - -D → eliminar una regla determinada
- Acciones
  - Reject → Aceptar
  - Drop → Denegar

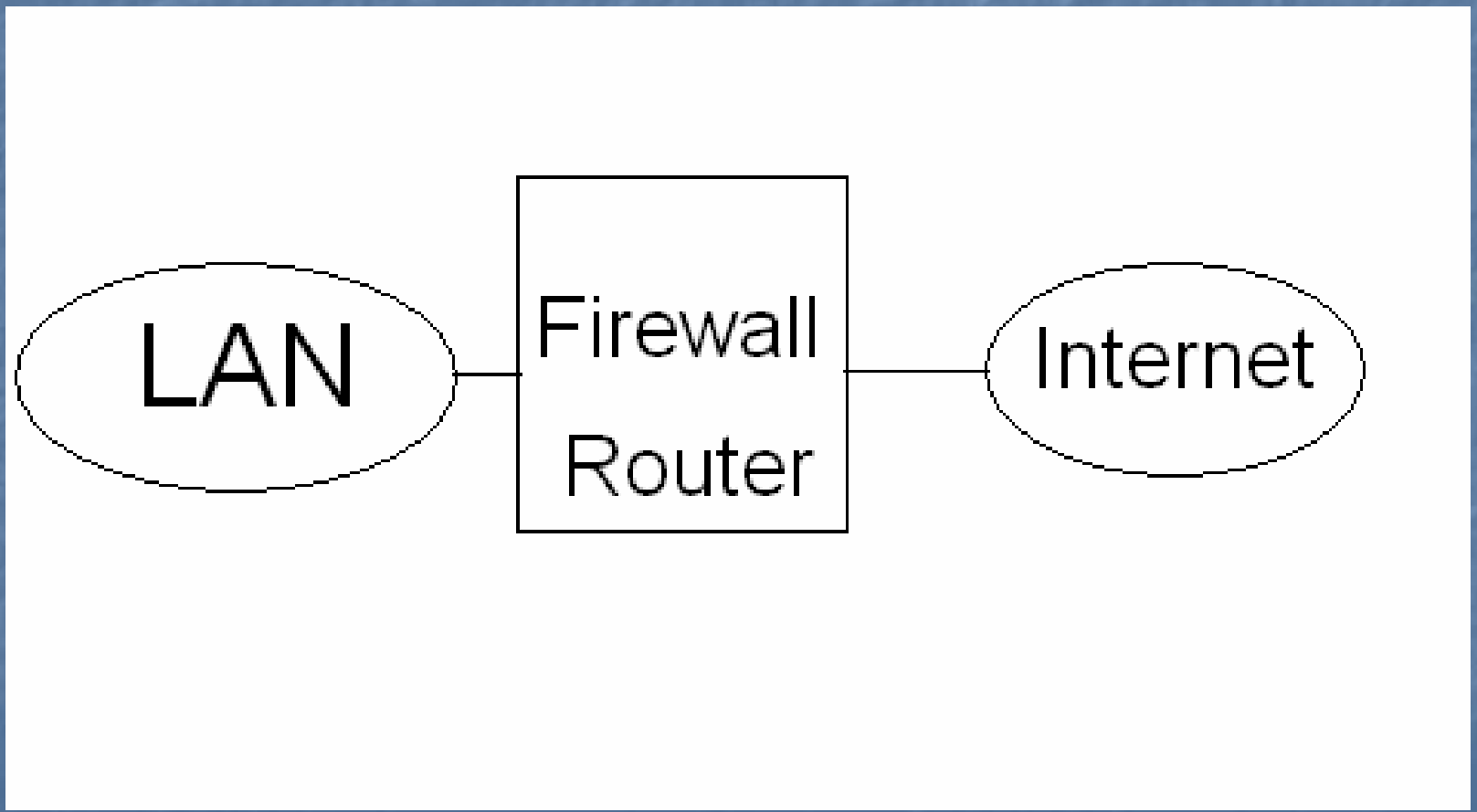
Firewalls

- Filtrado de paquetes
  - Nº regla
  - Dirección
  - Tipo : TCP/UDP...
  - IP Fuente
  - Puerto Fuente
  - IP Destino
  - Puerto Destino
  - Acción

Firewalls

- Netstat –an : Ver los servicios activos en el sistema para empezar a planificar el firewall. También se puede usar nmap.
- Iptables –L –n : verificar las reglas aplicadas.
- IPtraf : programa práctico para chequear el firewall mostrando el tráfico que atraviesa la máquina.

Firewalls



Firewalls

- #!/bin/sh
- #Flush de reglas
- iptables –F
- iptables –t nat –F

- #politica por defecto
- iptables –P INPUT ACCEPT
- iptables –P OUTPUT ACCEPT
- iptables –P FORWARD ACCEPT
- iptables –t nat –P PREROUTING ACCEPT
- iptables –t nat –P POSTROUTING ACCEPT

Firewalls

- #Redirigir a una ip por ejemplo para usar radmin
- iptables –t nat –A PREROUTING –s 1.2.3.4 –i eth0 –p tcp –dport 4899 –j DNAT –to 192.168.0.5:4899
- #El localhost lo dejamos como esta
- /Sbin/iptables –A INPUT –i –lo –j ACCEPT
- #A nuestra ip le permitimos todo eth0 va al router y eth1 a la LAN
- iptables –A INPUT –s 192.168.0.0/24 –i eth1 –j ACCEPT
- #Filtrar el acceso a la red con FORWARD
- #Aceptamos accesos a la web
- iptables –A FORWARD –s 192.168.0.0/24 –i eth1 –p tcp –dport 80 –j ACCEPT
- iptables –A FORWARD –s 192.168.0.0/24 –i eth1 –p tcp –dport 443 –j ACCEPT

Firewalls

- #Abrir el Puerto SMPT y POP3
- iptables –A INPUT –s 0.0.0.0/0 –p tcp –dport 25 –j ACCEPT
- iptables –A INPUT –s 0.0.0.0/0 –p tcp –dport 110 –j ACCEPT
- #Permitimos red privada virtual
- iptables –A INPUT –s 1.2.3.4 –p tcp –dport 1723 –j ACCEPT
- #Aceptar consultas al DNS
- iptables –A FORWARD –s 192.168.0.0/24 –i eth1 –p tcp –dport 53 –j ACCEPT
- iptables –A FORWARD –s 192.168.0.0/24 –i eth1 –p udp –dport 53 –j ACCEPT
- #Se deniega el resto
- iptables –A FORWARD –s 192.168.0.0/24 –i eth1 –j DROP

Firewalls

- #Enmascarar y activar bit forwarding
- iptables –t nat –A POSTROUTING –s 192.168.0.0/24 –o eth0 –j MASQUERADE
- echo 1 > /proc/sys/net/ipv4/ip_forward
- #El resto se cierra rango bien conocidos 0.0.0.0 significa cualquier red
- iptables –A INPUT –s 0.0.0.0/0 –p tcp –dport 1:1024 –j DROP
- iptables –A INPUT –s 0.0.0.0/0 –p udp –dport 1:1024 –j DROP
- #cerrar el Puerto de gestion webmin
- iptables –A INPUT –s 0.0.0.0/0 -p tcp –dport 10000 –j DROP
- # Cerrar la red virtual
- iptables –A INPUT –s 0.0.0.0/0 –i eth0 –p tcp –dport 1723 –j DROP

Proxys

- Actúa en nombre de los clientes
- Caché para optimizar el ancho de banda
- Controla el tráfico hacia el exterior
- Permite registrar todo lo que hagan los usuarios
- El más usado es el proxy http.
- SQUID es el paquete usado como proxy en sistemas Linux.

Proxys

- Configuración Básica
  - Fichero /etc/squid/squid.conf
  - http_port ip:puerto : Dirección y puerto por el que escuchará el proxy.
  - Cache_dir : tamaño de la caché.
  - Reference_age : tiempo que se mantendrán en caché los objetos almacenados. (1 mes lo más razonable).

Proxys

- Listas de control de acceso
  - acl nombre src componentes. Ej.
  - Acl mired src 192.168.0.0/24
- Reglas de control de acceso
  - http_access allow/deny nombre_lista
  - http_access allow mired

AntiSpam

- Filtrado de cabeceras:
  - Colocar en un fichero ej. Check_cabeceras
    /^Subject: Re: Your password!/
  - Header_checks = regexp:/ruta/check_cabeceras
- Filtrado de contenido:
  - Colocar en un fichero

    /Accept credit cards/ REJECTS

    /Nude Celebrities/ REJECTS
  - Body_checks = regexp:/ruta/check_body

AntiSpam

- Amavisd-new : (A mail virus scanner). Postfix entrega el correo a amavisd por un puerto para chequearlo y este lo devuelve a postfix por otro puerto. Preparado para actuar con spamassassin.
- El fichero de configuración es el /etc/amavisd/amavisd.conf y apenas es necesario modificarlo.

AntiSpam

- Spamassassin : aplicación que puntúa a los correos.
- Si superan una serie de pruebas se le añade puntos
- Si supera un umbral de puntos se le considerará Spam.
- Incluye filtros bayesianos para aprender de los correos recibidos. (falsos/positivos y viceversa)
- Puede ser preconfigurado con /etc/mail/spammassassin/local.cf

AntiSpam

- /etc/postfix/master.cf
- smtp-amavis
- amavis-smtp unix - - y - 2 smtp
- -o smtp_data_done_timeout=1200s
- -o smtp_never_send_ehlo=yes
- -o disable_dns_lookups=yes
- localhost:10025 inet n - y - - smtpd
- -o content_filter=
- -o local_recipient_maps=
- -o smtpd_helo_restrictions=
- -o smtpd_client_restrictions=
- -o smtpd_sender_restrictions=
- -o smtpd_recipient_restrictions=permit_mynetworks,reject
- -o mynetworks=127.0.0.1/24
- -o strict_rfc821_envelopes=yes

AntiSpam

- /etc/postfix/main.cf
- content_filter = smtp-amavis:(127.0.0.1):10024
- smtpd_recipient_restrictions =
- reject_non_fqdn_sender,
- reject_non_fqdn_recipient,
- reject_unknown_sender_domain,
- reject_unauth_pipeling
- check_client_access hash:/etc/postfix/mynetworks,
- permit_mynetworks,
- reject_unauth_destination

AntiSpam

- Para que amavisd-new haga uso de spamassassin debemos cerciorarnos de que no existe esta línea en el fichero de configuración de amavisd-new
  - @bypass_spam_checks_acl = qw(.);)

AntiSpam

- $daemon_user =’amavis’;
- $daemon_group=’amavis’;
- $mydomain = ‘pepe-informatica.com’;
- $forward_method= ‘smtp:127.0.0.1:10025’
- $notify_method = $forward_method;
- $final_spam_destiny = D_PASS;
- $sa_tag_level_deflt = 4.0;
- $sa_Tag2_level_deflt = 5.0;
- $sa_kill_level_deflt = $sa_tag2_level_deftl;
- [‘clam antivirus-clamd’,
- \&ask_daemon, [“CONTSCAN {}\n, ‘/var/run/clamav/clamd.ctl’],
- qr/\bOK$/, qr/\bFOUND$/,
- qr/^.*?: (?!Infected Archive)(.*) FOUND$/],