

Introducción al funcionamiento y configuración de Firewalls

Las computadoras ejecutan aplicaciones como (e. email, web browsers) y usan servicios (e. DNS, RIP, Identificación) como soporte de esas operaciones.

Una aplicación o servicio en la computadora local, pretende comunicarse con otra aplicación o servicio en otro sistema o red. Con TCP/IP y UDP/IP, la comunicación utiliza direcciones IP de las computadoras y numeros de puerto.

Sin un firewall, las comunicaciones desde y hacia el equipo se realizan sin supervisión.

No todos los puertos están siendo usados y eventualmente, una aplicación o servicio puede aceptar o no un intento de conexión.

En cambio, cuando se usa un firewall, este decide que sistemas pueden comunicarse y que puertos pueden usarse para tal fin.

Puede por ejemplo, bloquearse el intento de conexión entrante a un determinado port TCP/IP, y permitir que el mismo port se use para intentos de conexión salientes.

Se pueden bloquear intentos de comunicación mediante un firewall, pero este no realiza un análisis de los paquetes, para esto debe utilizarse un antivirus.

Se destina un rango de puertos locales para aplicaciones que se comunican con servicios de otros sistemas.

En general los ports destinados a servicios van desde el 1 hasta el 1023. Los puertos para uso temporal van desde el 1024 hasta el 5000.

De esta manera los puertos destinados a aplicaciones o servicios no superponen los ports asignados a servicios propios del sistema como compartir archivos, identificación, etc.

Convencionalmente, se acepta que determinados servicios tienen asignados puertos específicos.

Por ejemplo, servidores Web en el port 80, DNS en port 53 etc.

De esta manera, las aplicaciones locales saben como buscar servicios en otros sistemas.

En los firewalls mas eficaces, se puede establecer una regla de comunicación aplicable en ciertas condiciones, por ejemplo, cuando se está ejecutando una determinada aplicación, o cuando está activa la conexión dialup.

Se pueden establecer también prioridades de unas reglas sobre otras, para establecer el orden de aplicación de cada una.

Cuando la computadora local está en la misma red con otros equipos, es necesaria la dirección Ethernet para establecer comunicación, (mediante el protocolo ARP).

A menos que se la use frecuentemente, la computadora local pierde esta información, por lo tanto pregunta a los demás equipos acerca de su dirección Ethernet a intervalos regulares.

Si se bloquea ARP, los sistemas no pueden hablar entre si. (Algo similar se aplica en las conexiones dialup).

En el ambiente de chatgroups (IRC) se está expuesto a la interferencia debida a usuarios maliciosos que envían por ejemplo nukes ICMP y otros datagramas que confunden al sistema local haciendo que no puedan encontrar al servidor IRC..

(Se debe tener en cuenta que no todos los firewalls pueden bloquear ICMP).

GLOSARIO DE TÉRMINOS

Address - Es el campo de datos en la cabecera de un paquete que especifica quien envia o a quien se destina dicho paquete.

Address Mask - El valor que explica como interpretar el address. Las máscaras se usan a menudo para ayudar a identificar un rango de addresses.

Allow/Block (reglas) - La acción a tomar respecto de un paquete de acuerdo a la regla. Block significa que el paquete no será enviado o recibido. Allow significa que será recibido o enviado.

All Addresses (reglas) - Significa que la regla se aplicará a todas las direcciones.

ARP - Address Resolution Protocol, un protocolo Ethernet para aparear las direcciones IP con las direcciones Ethernet.

ARP es una herramienta esencial para indicarle a su sistema como encontrar otras computadoras. Si se bloquea, no será posible buscar otros equipos ni ser buscado por los mismos. Tampoco otros equipos pueden averiguar si el suyo se encuentra o no en la red. No se puede creer, sin embargo que el protocolo ARP alcanza para proteger. Es solamente un paso.

Recomendación: Permitir (Allow) desde todas las direcciones hacia todas las direcciones, a menos que se encuentre en un entorno particularmente inseguro, si así fuera, permita acceso desde sistemas o subsistemas seguros.

Autenticacion - La propiedad que permite conocer que una persona o sistema, es quien dice ser.

Broadcast (en redes) - Mensaje que se direcciona a todas las computadoras en una subred especificada.

cc:mail - Sistema de correo Lotus. Usa TCP en port 3264.

Intento de conexión (Connection Attempt)- Transferencia de datos que solicita la apertura de una conexión. Los Firewalls a menudo bloquean intentos entrantes de conexión, ya que usualmente es el equipo local quien debe solicitarlos.

FTP es una excepción.

En modo activo, el equipo remoto hará un intento de conexión para enviar un archivo. En modo pasivo, solamente el equipo local realiza intentos de conexión.

Default (rulesets, set de reglas) - La acción a tomar cuando no hay una regla anterior aplicable.

DNS - Domain Name Service, Es un servicio que permite la asignación del nombre de un equipo a una dirección IP. DNS usualmente usa UDP port 53, pero puede usar TCP. Si no permite DNS, no será posible buscar cualquier sistema por su nombre.

Fileshare - Compartir archivos. Recurso accesible a partir de una conexión a redes. Usa UDP ports 137 y 138 y TCP port 139.

Su sistema usa UDP broadcast (dirigido a todos los equipos de una subred) para anunciar su presencia y se alista para ver a los demás equipos. Esto es correcto en un ambiente seguro de oficina, pero inapropiado para una conexión a Internet.

Permita inbound, (entrante) si quiere recibir avisos de todos los equipos de su entorno. Bloquee outbound hacia Internet. Si no lo permite para la red interna, no verá ni será visto por su entorno.

El sistema operativo, permite cierta protección para este tipo de acceso. Si bloquea TCP port 139, no se permitirá compartir archivos.

Recomendación: Bloquear durante conexiones dialup. Compartir archivos e impresoras durante el acceso a Internet, no es una buena idea. Cuando elija permitir, bloquee intentos de conexión desde afuera (incoming) a menos que quiera compartir sus propios recursos. Permita conexiones salientes (outgoing), si quiere compartir los recursos de equipos externos.

Filter (firewalls) - Herramienta usada para interceptar todas las conexiones entrantes y salientes, el tráfico de una red, y bloquear todo aquello no deseado.

Finger - Servicio que busca información acerca de un usuario. Usa port 79.

Recomendación: Permita tráfico entrante si en su sistema corre un finger daemon (probablemente no). Permita tráfico saliente si lo necesita.

Firewall - Servicio que controla la transferencia de datos entre una computadora o red y las redes adyacentes. El firewall es responsable del filtrado de todos los paquetes y a menudo proporciona servicios de proxy para proteger equipos dentro del sistema.

FTP - File Transfer Protocol. Es un protocolo de alto nivel para la transferencia de archivos. FTP usa TCP/IP, ports 20-21.

Proveer servicio ftp invita a intentos de hacking. Use la seguridad de su Sistema Operativo para controlar el acceso (e.g. nombres de usuario, passwords, control de acceso a archivos). En el firewall, decida si puede filtrar las IP remotas y permitir solo las IP locales en su servidor ftp.

Recomendación: Bloquee conexiones entrantes a menos que esté usando un servidor ftp. Si está accediendo a un servidor ftp, intente usar modo pasivo.

Ftp es generalmente seguro desde el lado cliente. El riesgo existe principalmente para los archivos que transfiere: pueden tener virus. Con ftp activo se estará permitiendo que otro sistema inicie conexiones TCP hacia usted, sin su control explícito. En 'Passive mode' ftp no trabaja de esta forma, lo que significa que pueden bloquearse intentos entrantes de conexión ftp.

Recomendación: Permita ftp si lo utiliza. Use modo pasivo (bloqueando conexiones entrantes). Verifique con antivirus todos los archivos recibidos.

Gopher - Programa usado para acceder a información que se usa habitualmente en internet. Usa port 70.

Recomendación: Permitir si va a ser usado.

HTTP - Hypertext Transfer Protocol, Es la herramienta mas usada para navegación WWW. Usa TCP port 80.

Los sitios Web a menudo envían cookies por diferentes canales.

Recomendación: Si se bloquea se impedirá la navegación. Permitir, verificando archivos por posibles virus. Usar las características de seguridad del navegador. Utilizar Java con precaución y desactivar ActiveX.

HTTPS - Secure HTTP. Es una variación de HTTP que usa encriptación para aumentar la privacidad. Usa TCP port 443.

Identificación - Servicio que envía información del usuario hacia otro sistema, de modo que este intente verificar la identidad. Si se bloquea, otros equipos pueden rechazar las peticiones de servicio, como por ejemplo e-mail. Usa TCP port 113.

Conexión entrante, (Incoming Connection) - Conexión establecida por un equipo remoto hacia el equipo local. Es fácilmente identificable en el protocolo TCP.

ICMP - Internet Control Message Protocol, Protocolo de mantenimiento que maneja mensajes de error y ayuda a despejar el ambiente de red. ICMP se transporta sobre paquetes IP.

El abuso de ICMP puede provocar inconvenientes serios, por ejemplo en los grupos IRC. Debido a que otros pueden obtener información acerca del equipo, como la dirección IP, se pueden enviar falsos mensajes ICMP a nuestro equipo provocando la caída de la conexión IRC.

Tipos de ICMP:

- 0 - Echo Reply (ping reply)
- 3 - Destination Unreachable
- 4 - Source Quench
- 5 - Redirect
- 8 - Echo Request (ping request)
- 9 - Router Advertisement
- 10 - Router Solicitation
- 11 - Time Exceeded (usada por Traceroute)
- 12 - Parameter Problem
- 13 - Timestamp Request
- 14 - Timestamp Reply
- 15 - Information Request
- 16 - Information Reply
- 17 - Address Mask Request
- 18 - Address Mask Reply

Recomendación: Bloquear ICMP entrante tipo 3 (destino no alcanzable).

ICQ - Usa UDP port 4000. ICQ es difícil de filtrar para un firewall debido al uso de puerto UDP en el rango temporal (temporary range). La información se puede falsificar.

Recomendación: Permitir si usa ICQ, recordando que la información que recibe puede haber sido enviada falsamente por una tercera persona.

Paquete entrante (Inbound packet) - Paquete de información que llega desde otro equipo o red.

IP - Protocolo esencial en internet. Soporta TCP, UDP, ICMP y muchos otros.

IPX - Protocolo de red más comúnmente usado en Novell. Soporta SPX. También puede ser tunelizado sobre IP.

IRC - Internet Relay Chat. Servicio que permite compartir una conversación tipeada. IRC usa generalmente TCP ports en el rango 6660-6669.

El riesgo más grande aquí es la posibilidad de ataque o nuke.

Recomendación: Permitir conexiones entrantes solo si está usando un server IRC. Permitir conexiones salientes si usa IRC, pero bloqueando ICMP entrantes.

Learning Mode (firewalls) - Configuración que ayuda al usuario a establecer nuevas reglas en el grupo de reglas de filtrado.

Local (Address or Port) - Se refiere al equipo propio en oposición a equipo remoto.

Log File - Grabación de la actividad del firewall. Una entrada se puede ver aproximadamente como sigue:

Dial-Up Adapter [0000][Ref# 4] Blocking incoming TCP: src=154.11.111.155, dst=192.134.5.124, sport=1029, dport=139.

Este mensaje especifica:

- El nombre del dispositivo en el cual se intercepta el tráfico
- El número del dispositivo [0000],
- La regla del firewall relacionada con la interceptación, en este caso la número 4,
- Se avisa que el tráfico de entrada ha sido bloqueado,
- El IP del equipo remoto era 154.11.111.155,
- El destino local (dirección IP) era 192.134.5.124 es decir el IP dinámico del equipo local,
- el port de origen en el equipo remoto 1029,
- el puerto local de destino 139 (NetBIOS: fileshares)

Match (firewall rules) Aplicación de una regla - Un paquete coincide con una regla cuando los valores en su campo de datos, están dentro del rango especificado por la regla de filtrado. Los campos de datos especificados en las reglas son: protocolo, dirección y número de port.

NetBEUI - NetBIOS Extended User Interface. Protocolo de área local que opera bajo la interfaz NetBIOS.

Recomendación: Bloquear a menos que sea necesario.

NetBIOS - Protocolo para compartir archivos e impresoras. Este protocolo puede transportarse sobre TCP y UDP o IPX.

Si se bloquea NetBIOS, no se podrá acceder a recursos compartidos. Se recomienda bloquear NetBIOS (UDP ports 137-138, TCP port 139) cuando se esté conectado a Internet.

Netware-IP - Este protocolo envía información sobre IP. Se le asigna el port 396.

News (NNTP) - Servicio prestado por muchos ISP's

El mayor riesgo ocurre cuando se envían mensajes con la verdadera dirección de mail, porque se recibirá una cantidad interminable de spam. Usa TCP port 119.

Recomendación: Permitir conexiones entrantes solo si se tiene un server de news.

Si se bloquea, no se podrá acceder a los grupos de News.

Modificar la dirección de email antes de enviar posting.

El servidor de news puede requerir autenticación antes de permitir el acceso.

NeWS - Network Window System. Usa port 144.

Recomendación: Mantener bloqueado.

NTP - Network Time Protocol, Servicio que proporciona la hora. Usa port 123.

Es un riesgo si su sistema posee servicios que dependen de la fecha u hora o aplicaciones que usen la fecha u hora suministrados.

Recomendación: Mantener bloqueado a menos que sea necesario.

Options - Información y configuración de una regla de firewall:

- * - Nueva regla que no ha sido editada aún por el usuario.
- B - Bloqueo de intento de conexión entrante.
- F - Bloqueo de fragmentos entrantes
- L - Escribir log de seguimiento cuando el tráfico se ajuste a la regla
- I - Idem anterior, pero no mas de dos veces por segundo (util contra ataques de saturación flooding)
- C - Grabar intentos de conexión.
- W - Avisar al usuario cuando el tráfico se ajusta a esta regla
- w - Idem anterior pero no mas de dos veces por segundo.
- T - Regla temporalmente válida, solo durante esta sesión.

Outbound packet - Paquete de salida, que deja el propio equipo con destino a una red o equipo remoto.

Packet - Bloque de datos sobre un medio de comunicación, como internet.

Packet Filter - Filtrado de paquetes, una función del firewall que verifica paquetes entrantes y salientes, y permite o bloquea su transporte, dependiendo de las reglas en el set de reglas.

Ping - Es un servicio basado en ICMP- usado para verificar la accesibilidad de las computadoras de una red.

POP2 - Post Office Protocol, version 2. Usado para transferir email. Usa TCP port 109.

Es una versión antigua de servicio de mail. No se considera un riesgo.

Recomendación: Permitir conexiones entrantes solo si se tiene un server de mail POP2. Permitir conexiones de salida al servidor POP2 que corresponda.

POP3 - Post Office Protocol, version 3. Usado para transferir email. Usa TCP port 110. Es uno de los mas populares servicios de mail. No se considera un riesgo.

Recomendación: Permitir conexiones entrantes solo si está usando un servidor de mail POP3. Permitir conexiones salientes hacia el servidor de mail correspondiente.

Port - Número usado para identificar una instancia de comunicación.

Printshare - Recurso de impresora compartida accesible a través de una conexión en red. Usa TCP port 139.

Recomendación: Bloquear durante la conexión dialup.

Priority - Prioridad, una parte de la regla que configura el orden de prioridad en el uso.

Una regla de bajo número de prioridad, se ejecuta antes que las reglas con números mas altos. De esta forma, se establece la precedencia de una regla sobre otra. Cuando las reglas tienen la misma prioridad, el orden de uso se considerará arbitrario.

Protocol - Método estándar de comunicación

Hay dos tipos principales de protocolos, protocolos sin conexión y basados en conexión. Un protocolo sin conexión, orientado a datagrama envía paquetes sin un método de verificar su recepción. Los paquetes pueden perderse durante el tránsito. Ejemplos de protocolos sin conexión son IP, UDP e IPX.

Un protocolo basado en conexión proporciona un mecanismo de comprobar los envíos. De esta manera, se comprueban los paquetes recibidos en buen estado y se reenvían los paquetes perdidos o corruptos. TCP y SPX son protocolos basados en conexión.

RARP - Reverse Address Resolution Protocol, Protocolo Ethernet usado para resolver direcciones IP.

RARP no se aplica en general bajo un entorno Windows, sino en redes de computadoras y dispositivos que aprovechan la red internet. Si se bloquea RARP, su sistema no será capaz de buscar otros sistemas usando ningún otro protocolo, excepto broadcasts.

Recomendación: No construir reglas para RARP (puede permanecer bloqueado a menos que lo necesite).

RAS - Remote Access Service, Servicio que soporta conexiones dialup.

Reference Number - Número de ID para una regla del firewall, se usa para identificación en los mensajes grabado en log.

Los mensajes que mencionan 'Ref #0' tienen un significado especial. Aparecen cuando un paquete no está incluido en regla alguna, y es bloqueado por default.

Remote (Address or Port) - Se refiere a otro equipo con el cual se quiere comunicar el equipo local.

RIP - Routing Information Protocol, Protocolo basado en UDP-based utilizado para enviar información de enrutamiento a los sistemas en una red. Usa UDP port 520.

Puede falsificarse la información con el protocolo RIP, interfiriendo con las conexiones.

Recomendación: Bloquear mensajes entrantes a menos que el propio sistema se vuelva no alcanzable. Permitir paquetes salientes, limitadamente.

Rule (firewalls) - Set de parámetros que definen un tipo de paquetes de datos a verificar, y que hacer cuando son encontrados, permitir el tráfico o bloquearlo.

Ruleset (firewalls) - El conjunto de reglas que juntas describen como filtrar todos los paquetes.

Service - Una aplicación o función considerada parte del sistema operativo.

SMTP - Simple Mail Transfer Protocol. Uses TCP/IP port 25.

Uno de los servicios de mail mas populares. No es considerado riesgoso en PCs. Salvo los ya mencionados, virus y spam, que no dependen del protocolo sino del contenido de los mensajes de email.

Recomendación: Permitir conexiones entrantes solo si está usando un servidor de correo. Permitir conexiones salientes hacia su servidor SMTP.

SNMP - Simple Network Management Protocol. Protocolo utilizado para manejar redes y enrutamientos. Se debe permitir solo si es necesario. Usa UDP port 161.

Recomendación: Bloquear.

TCP - Protocolo de Internet basado en conexión transportado en paquetes IP. Por ejemplo aplicaciones basadas en TCP y servicios, SMTP, navegación, email e IRC.

TCPMUX - TCP Port Service Multiplexer (usa port 1), Muy raro en PCs.

Este servicio es peligroso, porque puede asignar puertos en forma aleatoria para el uso de aplicaciones.

Esto significa que es necesario abrir todos los puertos en el sistema, provocando absoluta desprotección.

Recomendación: Bloquear.

Telnet - Servicio basado en TCP que soporta accesos remotos (usualmente a sistemas UNIX. Telnet usa el port 23.

Un riesgo con Telnet es que se está enviando el nombre de usuario y password a la red, y pueden ser robados y usados posteriormente.

Recomendación: Permitir solo si es necesario, pero debe considerarse el uso de una VPN.

Temporary Range: Es el rango de puertos locales usado por las aplicaciones, para servicios basados en TCP o UDP. Se los denomina también puertos temporales o efímeros. Las aplicaciones como ICQ (UDP port 4000) son difíciles de filtrar para un firewall debido a que usa puertos dentro de este rango (1024 a 5000).

Recomendación: Tratar con cierta sospecha la información proveniente de aplicaciones basadas en transporte UDP que usen puertos temporales.

TFTP - trivial file transfer protocol, protocolo de transferencia basado en UDP, usa port 69. tftp es un riesgo de seguridad porque actúa sin intervención del usuario.

Recomendación: Bloquear.

Tunnel - Encapsulamiento de un protocolo o corriente de datos dentro de otro. Por ejemplo una Virtual Private Network (VPN) tuneliza datos encriptando y luego encapsulando dentro de un protocolo como TCP (mejor) o UDP (peor).

UDP - Protocolo de Internet sin conexión (datagramas) con transporte sobre paquetes IP. Es más difícil para un firewall bloquear ataques basados en UDP que los ataques basados en TCP.

Algunos ejemplos de aplicaciones que usan UDP son: ICQ, DNS, RIP, NetBIOS (para broadcasts etc.), RIP.

VPN - Virtual Private Network. Conexión privada segura generalmente a través de una red insegura. Con una VPN se puede, por ejemplo, conectar LAN's de dos oficinas a través de Internet de manera que cada una puede acceder a la otra como si estuvieran en la misma LAN. El enrutamiento a través de Internet se torna invisible. Visto desde Internet, el tráfico se ve encriptado.

Otra posible configuración de un VPN es "cliente/servidor", donde las computadoras, por ejemplo una laptop, se conecta a un servidor VPN que proporciona acceso a una red protegida. Un equipo portátil u hogareño puede así conectarse a la oficina mediante un acceso seguro, y acceder a los recursos también en forma segura.

WINS - Windows Internet Name Service, Protocolo similar a DNS. Usa port 1512.
Si el sistema está configurado para usar WINS, al bloquearlo no será posible conectarse a otros sistemas.

Recomendación: Permitir solamente al servidor WINS propio.

Winsock - Forma parte del SO Windows y maneja la mayoría de las conexiones a redes (no maneja archivos o impresoras compartidas, ni ICMP).