Unidad 4

El cortafuegos

Seguridad y alta disponibilidad

4

Índice

Introducción

Se denomina cortafuegos o firewall son las soluciones diseñadas para proteger su computadora y que pueden complementarse o combinarse con software antivirus. Estos son los tipos de protección que podría haber usado sin darse cuenta, pero eso no significa que no tenga que preocuparse por saber qué hacen y qué no.

Las reglas se van a agrupar en cadenas y a su vez las cadenas las vamos a encontrar en tablas.

Los programas de aplicación se distribuyen en unidades llamadas paquetes. Un paquete es un conjunto de archivos y carpetas necesarios para un producto de software. Un desarrollador de aplicaciones generalmente diseña y construye un paquete, una vez que se completa el desarrollo del código de la aplicación.

Para llevar a cabo el seguimiento de conexiones, también conocido como connection tracking es la propiedad del cortafuegos para controlar la conexión a la que está asociada cada paquete. El protocolo NAT no puede darse sin producirse el connection tracking.

El firewall de Windows está orientado a las aplicaciones y servicios que presentan acceso a la red, para lo que se realizará una clasificación en redes públicas, privadas y en redes de dominio. Además, las reglas del firewall de Windows embién ofrece reglas de seguridad a conexiones.

Cuando el cortafuegos permite una conexión determinada ya no habrá manera de controlar los ataques que se produzcan.

Al finalizar esta unidad

- Estudiaremos la relevancia del cortafuegos como medida fundamental de seguridad.
- Estudiaremos las componentes y el funcionamiento del cortafuegos de Linux.
- Conocer la base de gran cantidad de las reglas de los cortafuegos.
- Aprenderemos las diferencias entre el funcionamiento del cortafuegos de Linux con el de Windows.
- Aprenderemos a distinguir las propiedades del cortafuegos genérico del cortafuegos de aplicaciones web.

4.1. Introducción

Se conoce como cortafuegos o *firewall* son las soluciones diseñadas para proteger su computadora y que pueden complementarse o combinarse con software antivirus. Estos son los tipos de protección que podría haber usado sin darse cuenta, pero eso no significa que no tenga que preocuparse por saber qué hacen y qué no.

Un cortafuegos o *firewall* en inglés, en el mundo informático es un sistema de seguridad que impide el acceso no autorizado a tu ordenador a la vez que permite que tu ordenador se comunique con otros servicios autorizados. También se utilizan en redes informáticas, especialmente redes internas o redes de área local. Esta es una de las primeras medidas de seguridad que se empezaron a implementar en los ordenadores tras la llegada de Internet.

Imagen 1. Router Cisco

Imagen 2. Router Mikrotik

Estos cortafuegos presentan una serie de reglas que hay que tener en cuenta:

1. Van a permitir la salida de la red interna LAN hacia la red de internet WAN.
2. Van a impedir que un paquete derivado de la red de internet WAN, excepto en los que se hayan solicitado con anterioridad.

Si bien esto ofrece una gran protección para los usuarios domésticos, no responde necesidades del entorno profesional. En este tema, nos centramos en lo que conocemos como cortafuegos profesionales que serán los routers que tienen entre 4 y 24 interfaces de red. Por lo general, 4 serán suficientes en el caso de estar hablando de una pequeña empresa, además de presentar un firmware que le permite especificar de forma concreta las reglas de firewall detalladas. Estos se denominan cortafuegos de hardware entre los que podemos destacar pfSense, Mikrotik, WatchGuard, entre otros. Cabe hacer especial mención a Cisco, en el caso de estar refiriéndonos a una gran empresa.

Pero cualquier computadora que tenga dos o más interfaces de red que transporten tráfico de red pueden llevar a cabo las funciones de cortafuegos utilizando el software adecuado.

Las marcas de cortafuegos de hardware hacen que su sistema operativo interno esté disponible públicamente para que pueda instalarse en la PC, como lo hace Mikrotik con su RouterOS. Además, también existen firewalls, conocidos como cortafuegos *open source* como OPNSense y pfSense, este último también disponible en versiones de hardware (comerciales).

La mayor parte de los cortafuegos hardware están fundamentados en el reparto UNIX/Linux, ya que su kernel está fundamentalmente planteado para el enrutamiento, así como para el filtrado de paquetes.

Para distinguir unos cortafuegos de otros, podemos fijarnos en la dificultad o facilidad que presenta un usuario para establecer las reglas.

En el momento en el que comprendamos cómo funciona un cortafuego Linux, no nos costará apenas trabajo aprender el funcionamiento del resto de tipos.

En conclusión, un cortafuegos nos va a ayudar a proteger el sistema y lo hacen disminuyendo la superficie ante un posible ataque.

4.2. Conceptos previos

4.2.1. Paquetes

Los programas de aplicación se distribuyen en unidades llamadas paquetes. Un paquete es un conjunto de archivos y carpetas necesarios para un producto de software. Un desarrollador de aplicaciones generalmente diseña y construye un paquete, una vez que se completa el desarrollo del código de la aplicación. El producto de software debe combinarse en uno o más paquetes de software para que pueda conectarse fácilmente a un medio de distribución. Los productos de software pueden ser producidos e instalados en masa por los administradores.

Un paquete es una colección de archivos y directorios en un formato específico. Este formato sigue la interfaz binaria de la aplicación (ABI), así como la definición de la interfaz del sistema V.

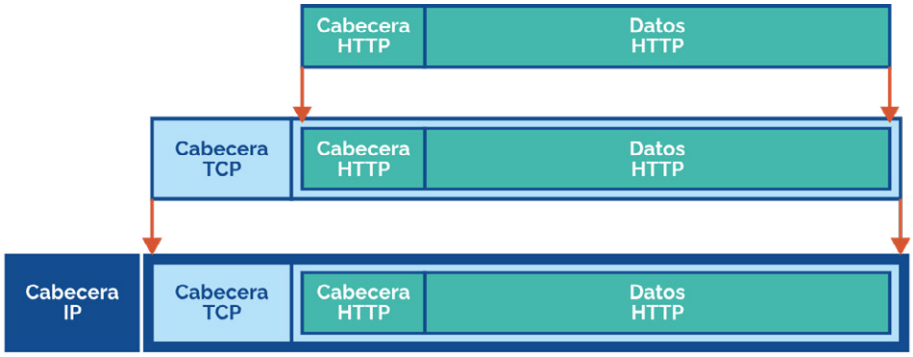


Imagen 3. Un paquete IP contiene un paquete TCP, el cual contiene un paquete HTTP

Como se muestra en la figura que se muestra a continuación, el protocolo IPv4 define varios campos en el encabezado del paquete. Estos campos contienen valores binarios que el servicio IPv4 indica al enviar paquetes por la red.

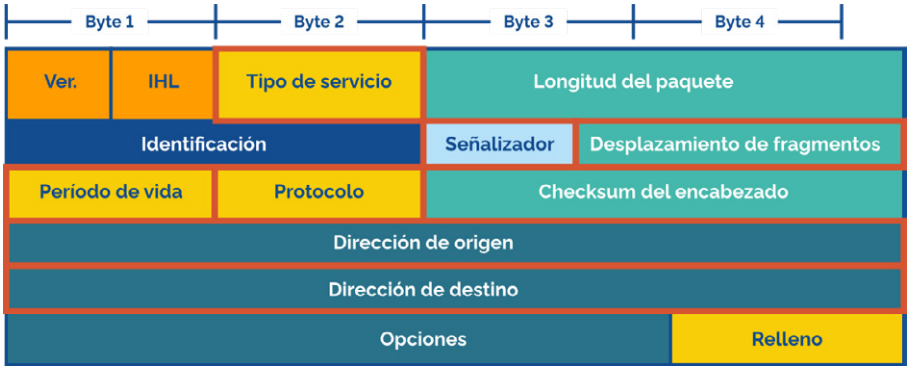


Imagen 4. Campos que contiene la cabecera de un paquete IP

4.2.2. Reglas y acciones

Para cada uno de los paquetes se establecen una serie de reglas que determinará qué acción o qué objeto será el que tiene que elegirse en función de una serie de factores.

Las crisis psicológicas que podemos encontrar en situaciones de emergencias:

Cuando estos eventos ocurren dentro del ámbito de emergencias se ofrece una respuesta inmediata e intensa de las personas., que se distingue por:

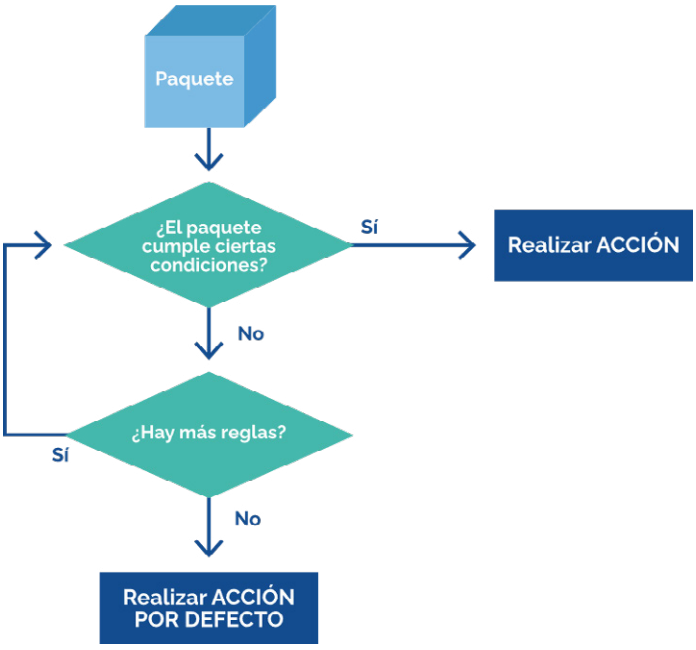


Imagen 5. Aplicación de las reglas del cortafuegos a todos los paquetes

Podemos destacar una serie de acciones:

- **ACCEPT:** sería la acción de aceptar el paquete.
- **REJECT:** sería la acción de rechazar el paquete. En este caso el emisor recibe un mensaje informándole.
- **DROP:** sería la acción de descartar el paquete. En este caso el emisor no va a recibir ningún tipo de mensaje informándole.

Para que una regla determinada tome una decisión, se tienen en cuenta una serie de condiciones:

- El contenido de uno o más campos de la parte de la cabecera del paquete, donde se destacan el origen, el destino, el protocolo llevado a cabo...
- La interfaz de la red por la que va a entrar o por la que va a salir el paquete.
- La dirección MAC del origen
- El estado de la conexión
- En el caso de que la dirección de origen corresponda a una determinada lista de direcciones

Se podrán generar reglas sin tener en cuenta las condiciones, simplemente con una determinada acción. La regla que se establezca, se va a aplicar a todos los paquetes y en el caso de que la regla presente una serie de condiciones, será fundamental que se cumplan con todas ellas.

En ocasiones, aunque parezca que no tiene sentido, se pueden establecer reglas que presenten condición pero que no presenten acción y se usarán para temas estadísticos.

4.2.3. Cadenas y tablas

Las reglas de un cortafuegos las vamos a encontrar de forma agrupada en cadenas, conocidas como *chains*.

En cualquier cortafuegos siempre encontraremos 3 cadenas predefinidas:

- **INPUT:** este tipo de reglas van a ir ligadas a los paquetes de entrada que tienen como destino el router.
- **OUTPUT:** este tipo de reglas van a ir ligadas a los paquetes de salida que tienen como origen el router.
- **FORWARD:** este tipo de reglas van a ir ligadas a los paquetes de entrada que tienen como destino no es el router.

Estas cadenas las vamos a encontrar agrupadas en tablas. Podemos diferenciar entre distintos tipos de tablas:

- **Filter:** tablas que se emplean para la filtración de paquetes.
- **Nat:** las cadenas presentes en este tipo de tablas se utilizan para determinar a qué paquetes se les va a aplicar cada uno de los protocolos.
- **Mangle:** las cadenas presentes en este tipo de tablas nos ayudan a realizar ciertas modificaciones en los paquetes.
- **Raw:** las cadenas presentes en esta tabla son las primeras que se aplican, cuando aún no hay ninguna clasificación, ni ningún cambio en los paquetes.

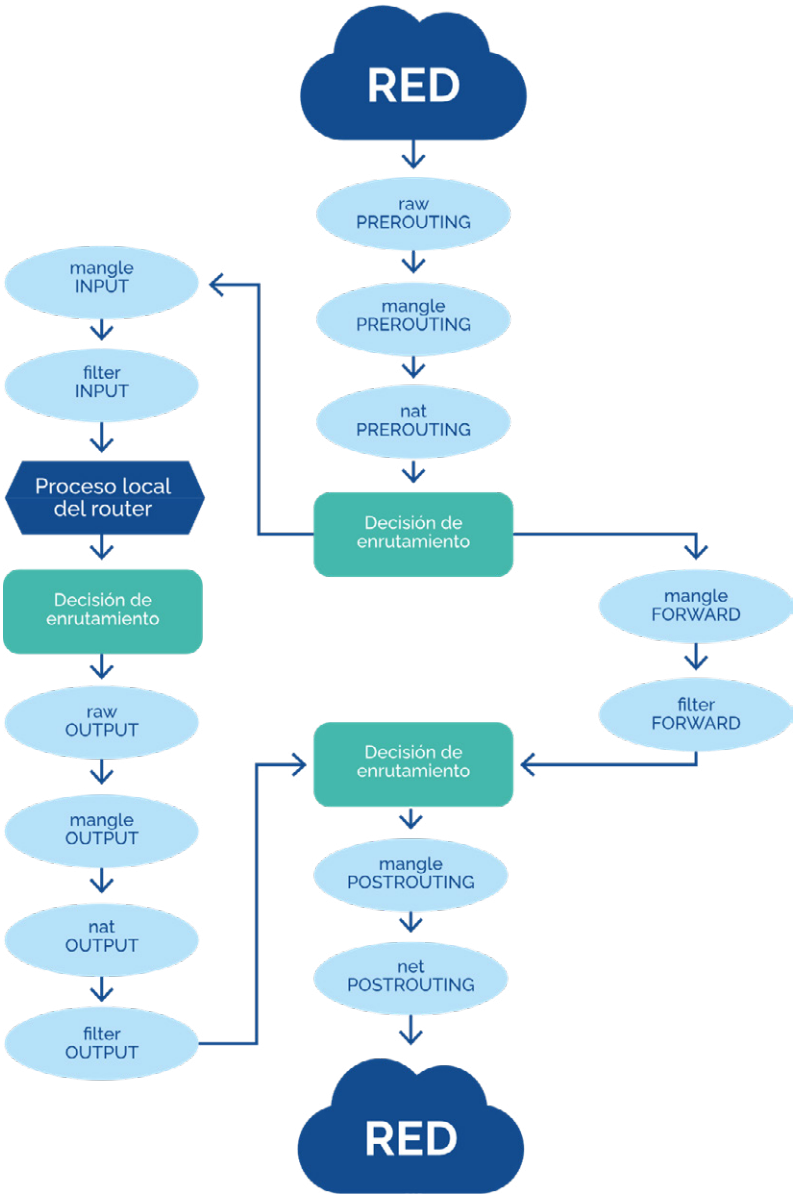


Imagen 6. Camino de un paquete por las distintas tablas y cadenas del cortafuegos

4.2.4. Cadenas definidas por el usuario

Será sencillo que una cadena como FORWARD presente numerosas reglas que haga que sea muy difícil conocer el contenido de éstas.

Para facilitar esto, se van a establecer una serie de subrutas. Siempre se podrá volver a la cadena principal haciendo uso de la acción RETURN.

4.2.5. Seguimiento de conexiones

El seguimiento de conexiones, también denominadas *Connection Tracking* es la propiedad que tienen los cortafuegos para detectar las conexiones que hay entre dos equipos, así como la capacidad de recordarlas y memorizarlas en el kernel.

Las conexiones van a venir definidas por:

- Protocolo utilizado
- IP: puerto origen ←→ IP: puerto destino

Los paquetes pueden tener valores idénticos en los cinco campos que pueden formar parte o forman parte de la misma conexión.

El cortafuegos debe recordar los distintos valores de los paquetes que entran para así poder verificar si corresponden con conexiones abiertas o son conexiones nuevas. El kernel va a designar un estado a todos los paquetes:

- **INVALID:** por alguna causa el paquete no va a ser considerado válido.
- **NEW:** el paquete va a establecer una conexión nueva.
- **ESTABLISHED:** el paquete corresponde a una conexión abierta.
- **RELATED:** a partir de una conexión previa, se va a producir la creación de una nueva conexión.

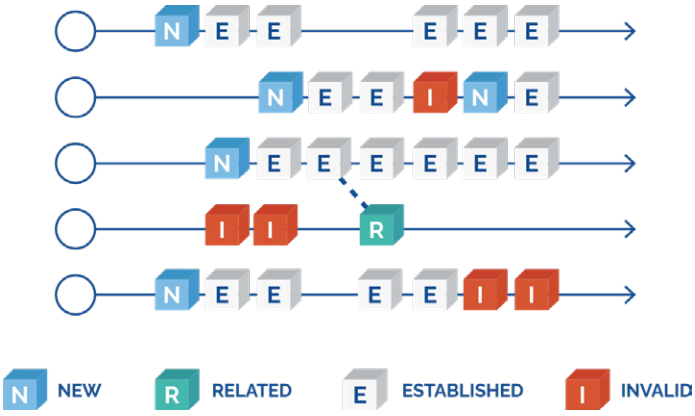


Imagen 7. Estado de los paquetes de diferentes conexiones

Un cortafuegos va a tener la capacidad de distinguir y aprender las conexiones abiertas que van a llamarse *statefull firewall.* En el caso contrario, se denominará *stateless firewall.*

Va a ser fundamental a la hora de determinar las reglas de un cortafuegos considerar el estado de un paquete, ya que a través del estado del paquete podemos detectar los paquetes que presenten estado NEW para poder decidir nosotros mismos, evitándole a la CPU del router que tenga que realizar un procesamiento del resto de paquetes. Las cadenas INPUT y FORWARD deberán tener DROP por defecto como política y así comentar con dos reglas:

- En el caso de que el estado del paquete sea **INVALID → DROP**
- En el caso de que el estado del paquete sea **ESTABLISHED o RELATED → ACCEPT**

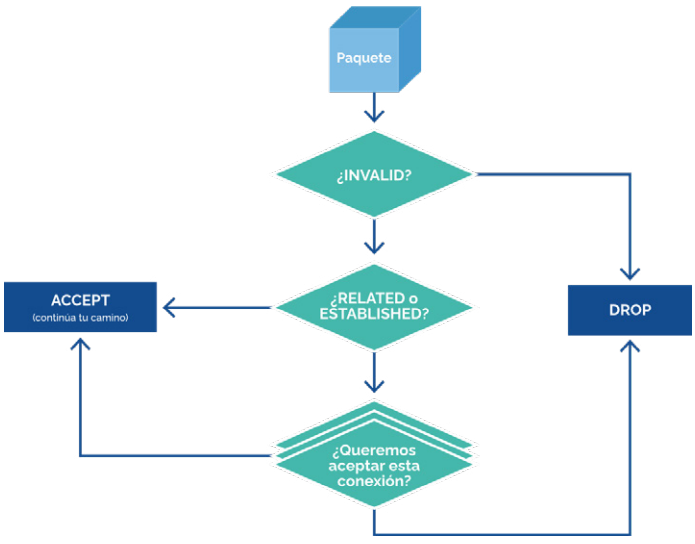


Imagen 8. Reglas habituales en un cortafuegos con seguimiento de conexiones -Cadenas INPUT/FORWARD

4.2.6. NAT y MANGLE

Internet en sus inicios no se consideraba una gran red, por lo que tan sólo se reservaban 32 bits para las direcciones, lo que equivale a 4.294.967.296 direcciones únicas, de hecho, la cantidad de dispositivos conectados a Internet ha crecido exponencialmente a medida que IP Las direcciones están agotadas. Esta es la razón del **nacimiento de NAT** o Network Address Translation (en español se traduciría como Traducción de Direcciones de Red).

La idea es simple, hacer que las redes de computadoras usen una serie de direcciones privadas (direcciones IP privadas) y conectarse a Internet usando una sola dirección IP (direcciones IP públicas). Gracias a este parche, las grandes empresas solo utilizarán una dirección IP y no la cantidad de empresas con dispositivos. También se utiliza para conectar su red doméstica a Internet.

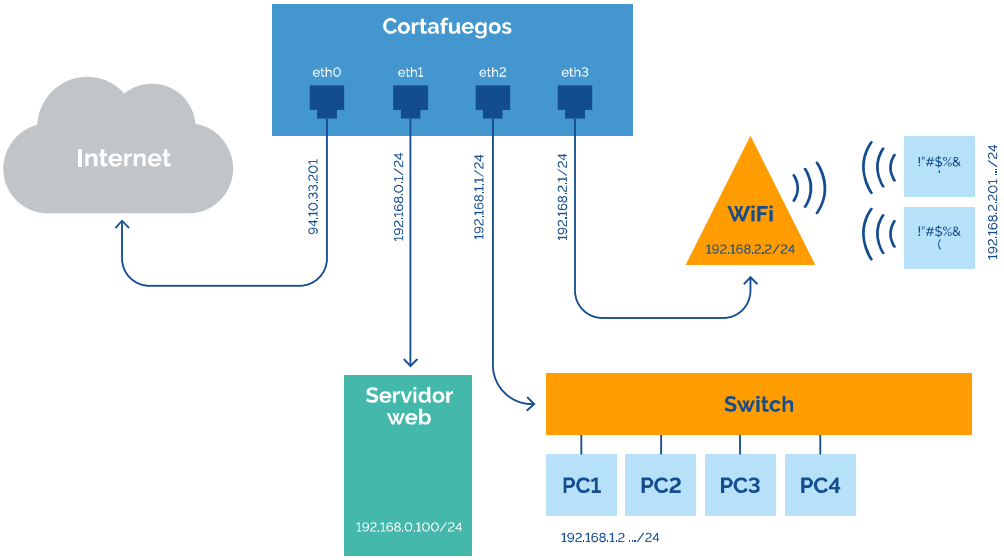


Imagen 9. Ejemplo de red de una pequeña empresa

En cuanto a la **tabla mangle** debe usarse principalmente para modificar paquetes, como dijimos. En otras palabras, aquí puede usar comparaciones de modificación para modificar el campo TOS (*Type Of Service*).

La tabla mangle se destina para los siguientes objetivos:

1. TOS
2. TTL
3. MARK

4.3. Iptables

Iptables es una utilidad de línea de comandos para configurar el firewall del kernel de Linux que se implementó como parte del proyecto Netfilter. El término iptables también se usa comúnmente para referirse a un firewall de kernel.

Se puede configurar directamente con iptables o usando uno de los muchos paneles de control y GUI que existen. El término iptables se usa para referirse a IPv4 y el término ip6tables se usa para referirse a IPv6. iptables e ip6tables tienen la misma sintaxis, pero algunas opciones son específicas de IPv4 o IPv6.

Todos los núcleos nativos de Arch Linux admiten iptables. Solo necesita instalar las herramientas de espacio de usuario proporcionadas por el paquete iptables. El paquete iproute2 incluido en el ensamblaje base se basa en iptables, por lo que el paquete iptables debe instalarse en su sistema de manera predeterminada.

4.3.1. Añadir reglas

Filtrado de paquetes de red basado en reglas - "reglas" - denotadas por diferentes coincidencias - "coincidencias" - (condiciones que debe cumplir un paquete de red para que se aplique la regla) y objetivo - "objetivo" -

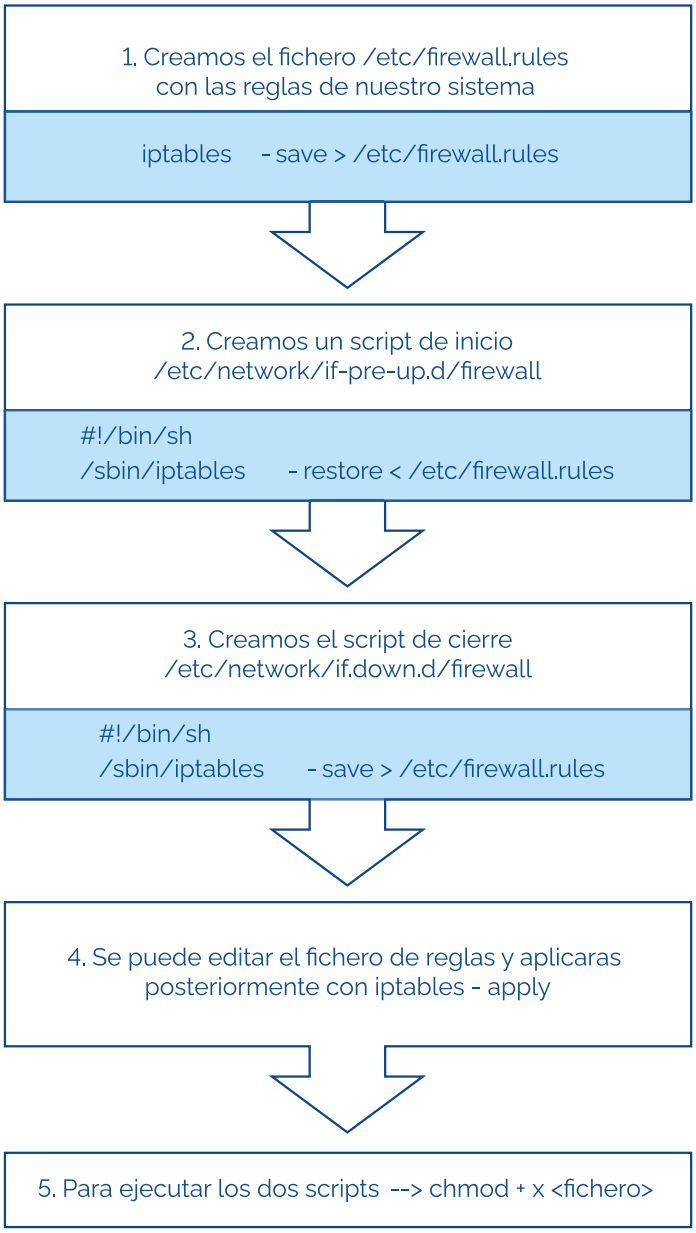
Los targets se especifican mediante la opción -j o --jump —«salto»—. Los targets pueden ser bien cadenas definidas por el usuario, bien uno de los targets integrados especiales, o bien una extensión de target. Los targets integrados son ACCEPT, DROP, QUEUE y RETURN; las extensiones de target son, por ejemplo, REJECT y LOG.

En el caso de que el objetivo sea un target integrado, el destino del paquete es decidido inmediatamente y el procesamiento del paquete de red en la tabla actual se detiene. Si el objetivo («target») es una cadena definida por el usuario y el paquete supera con éxito esta segunda.

4.3.2. Persistencia de las reglas

Para prevenir cualquier problema que pueda producirse contamos con dos comandos que nos van a dar la capacidad de conservar las reglas establecidas de iptables en un documento de texto. Se denomina iptables-save o iptables-restore.

Para lograr de forma completa la persistencia de nuestras reglas seguiremos los siguientes pasos:



4.3.3. Parámetros de iptables más utilizados

Parámetros de iptables	
Parámetro	**Significado**
!	Se puede poner delante de prácticamente todos los parámetros para de esa manera revertir la condición.
-p	Protocolo del nivel de transporte del paquete
-s	Dirección IP de origen
-d	Dirección IP de destino
-j	Concreta la acción de la regla.
-i	Interfaz de red de entrada.
-o	Interfaz de la red de salida

4.3.4. Un cortafuegos mínimo

Hay una serie de reglas mínimas que hay que tener en cuenta en un equipo de escritorio de Linux. Son una serie de reglas, que en ocasiones no van a ser suficientes en el caso de que estemos hablando de un cortafuegos empresarial.

4.3.5. Un cortafuegos empresarial mínimo

Un cortafuegos empresarial mínimo va a tener dos funciones principales, hacer NAT para que de esa forma los equipos presentes en la red internet puedan salir a internet y así poder repeler todo tipo de entrada a la red interna desde la zona exterior, salvo las conexiones a los distintos servicios que deben ser observables desde internet.

4.4. Variante de iptables

IPTABLES, como ya sabrá, está integrado en el kernel de Linux y forma parte del proyecto netfilter, que, además de iptables, consta de ip6tables, ebtables, arptables e ipset. Es un firewall altamente configurable y flexible como la mayoría de las herramientas de Linux y, a pesar de algunas fallas, sigue siendo excepcionalmente poderoso. Dentro del kernel, comienza con el sistema y siempre está activo y, a nivel del kernel, recibirá paquetes y esos paquetes serán aceptados o rechazados al observar las reglas de iptables.

Gran parte de las variantes de iptables se utilizan para favorecer el uso de cortafuegos por lo que serán incapaces de entrar en uso con iptables. Entre todos los tipos podemos destacar Firewall Builder ya que está dirigido a la gestión profesional de sistemas.

Firewall Builder es una herramienta de administración de firewall multiplataforma que le permite agrupar y administrar firewalls para diferentes sistemas operativos, brindando la opción de control remoto.

El hecho de que funcione multiplataforma ya es una ventaja, ya que desde un PC con Windows XP podemos gestionar y configurar un cortafuegos independiente para Linux o Mac OS, por ejemplo.

Algunas de las características que podemos destacar de Firewall Builder son:

- **Objetos:** con él, puede especificar las direcciones de los dispositivos en los que desea aplicar el firewall y también administrarlos a través de este software. Además del rango de direcciones, también puede especificar nombres de DNS, grupos, hosts, redes, direcciones y más desde esta sección de audiencia.
- **Nuevo Objeto:** menú a través del cual se pueden crear nuevos clusters, hosts, redes, nuevo rango de direcciones, servicios IP, servicios ICMP, etc.
- **Crear un nuevo cortafuegos:** puede crear un nuevo firewall después de seleccionar el dispositivo y el enrutador al que desea aplicar el firewall.
- **Reglas:** puede crear reglas de firewall personalizadas para cada dispositivo al que desee aplicar el firewall.

4.5. El firewall de Windows

Un firewall es una herramienta de seguridad que evita el acceso no autorizado a una red. De esta manera, evita que otros tomen el control de su dispositivo para implantar virus informáticos o robar sus datos personales.

Si tiene un negocio, encontrará que los firewalls son muy útiles para proteger su negocio de amenazas externas o internas. Por ejemplo, si sabes cómo activar el Firewall de Windows 10 o nunca lo has desactivado en tu escritorio, te habrás dado cuenta de que una de sus funciones es filtrar el tráfico y advertirte sobre amenazas maliciosas. Direcciones IP estáticas.

Al mismo tiempo, un firewall activo ejecutará sistemas de filtrado de forma continua para proteger todo el hardware de su empresa e incluso el software instalado en su computadora. Algunos de estos métodos se utilizan para:

- Filtrar paquetes
- Examinar el tráfico de red para establecer si un paquete presenta o no relación con otro
- Examinar la conexión entre sistemas abiertos

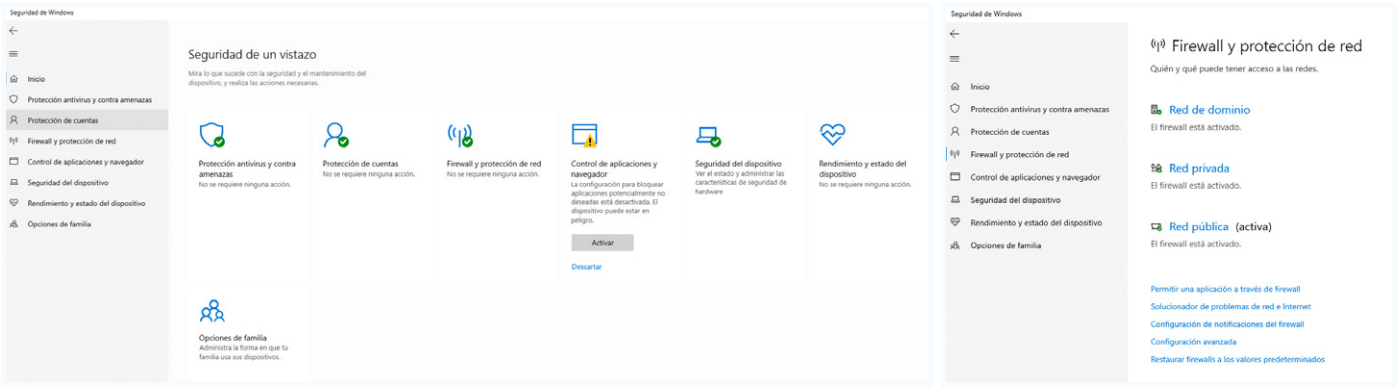


Imagen 3. Firewall y protección de red en el Centro de seguridad de Windows Defender

Red de dominio	En el caso de que el equipo esté asociado a un dominio de Actibe Directory y la persona que se conecte a él, este será el firewall para configurar.
Red privada	En el caso de que el equipo no esté asociado a un dominio, Windows entiende que estará asociado a una red privada.
Red pública	Windows deduce como red pública toda red que tenga que presenta una mayor protección al tener acceso personas desconocidas y que pueden producir un ataque.

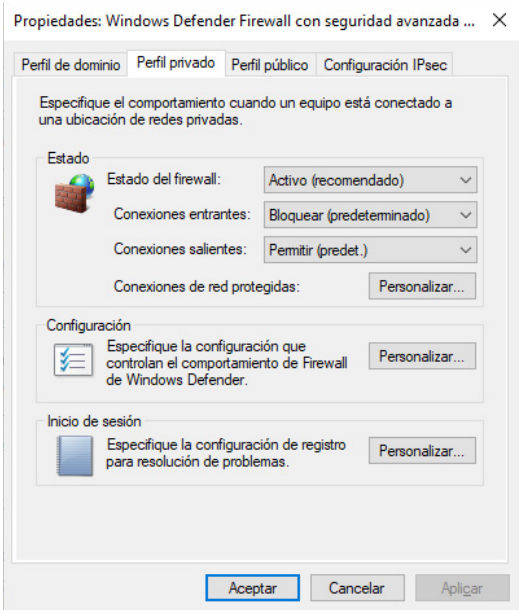


Imagen 4. Propiedades del perfil privado

En la imagen anterior podemos ver como los tres tipos de redes de las que hemos hablado antes van a venir representados como "perfiles".

En el caso de que el *firewall esté activado* para un perfil concreto, se protegerá, como consecuencia el resto de las conexiones de red que se localizan en ese perfil. En el caso de querer establecer alguna excepción, se realizará mediante la opción de "Conexiones de red protegidas".

4.5.1. Creación de reglas

Windows Defender Firewall con seguridad avanzada admite poder elegir las reglas tanto de entrada como de salida. Lo podemos observar en la siguiente imagen:

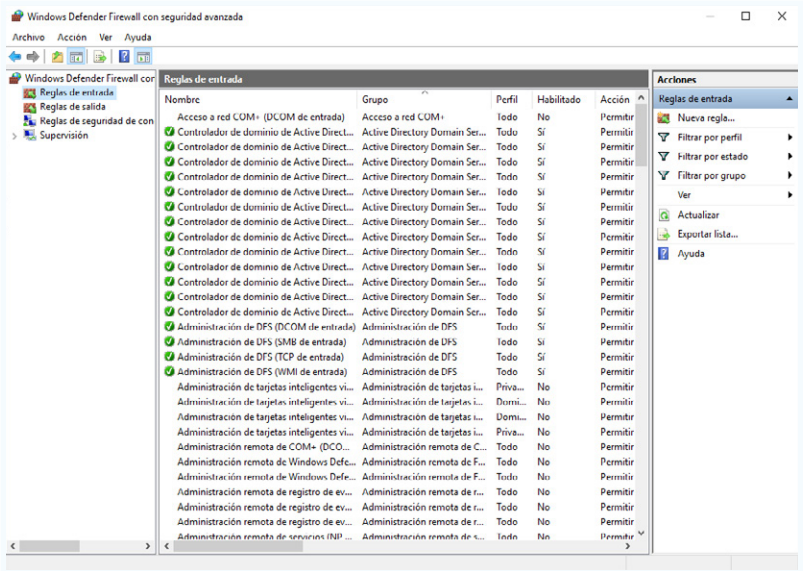


Imagen 5. Listado de reglas de entrada.

4.5.2. Reglas de seguridad de conexión

Al establecer una regla de seguridad de conexión se nos muestra otro asistente con las opciones que se muestran a continuación:

- **Aislamiento:** supone una limitación en la conexión en función del criterio usado para la autenticación.
- **Exención de autenticación:** determina una serie de equipos que no tienen que autenticarse para poder establecer la conexión.
- **Túnel:** es parecida a la explicada antes, sin embargo, en este caso se establece un túnel de cifrado entre ambos equipos.
- **Personalizada:** será una mezcla de todas las anteriores.

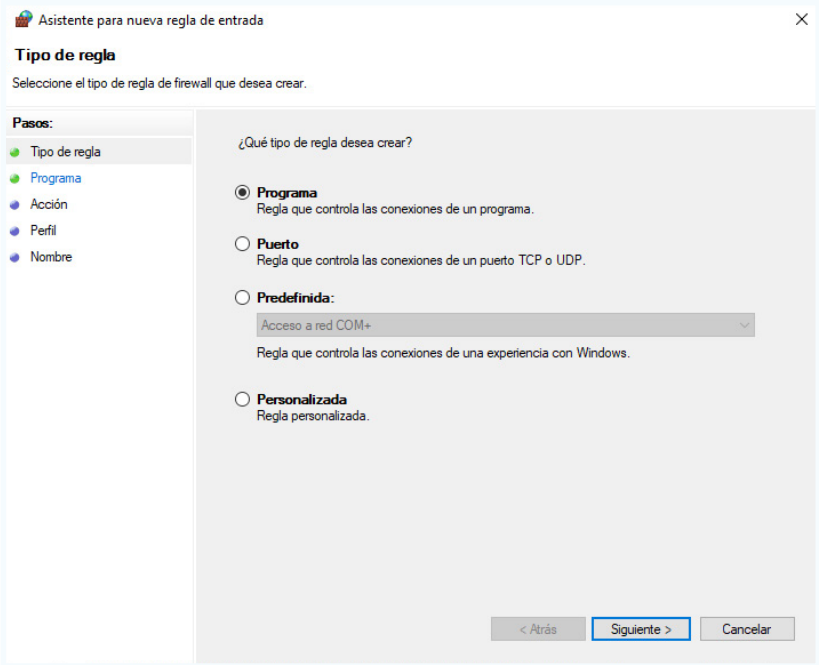


Imagen 6. Asistente para crear una regla de seguridad de conexión

4.6. Registro de sucesos

El cortafuegos es incapaz de acumular en un fichero log las actuaciones que va a desarrollar sobre los paquetes sobre los que tiene algún efecto. El administrador será el que decida qué reglas le parecen adecuadas para de ese modo registrarlas.

En iptables esto se va a lograr con LOG. Es un objetivo no terminal por lo que el kernel no termina el estudio en cadena.

En el caso de que un paquete satisfaga, el kernel volcará los datos más importantes del proceso log (syslogd) con cierto nivel de importancia, concretamente los del nivel 4 = warning, generalmente poniendo delante el prefijo ACCESO A SSH.

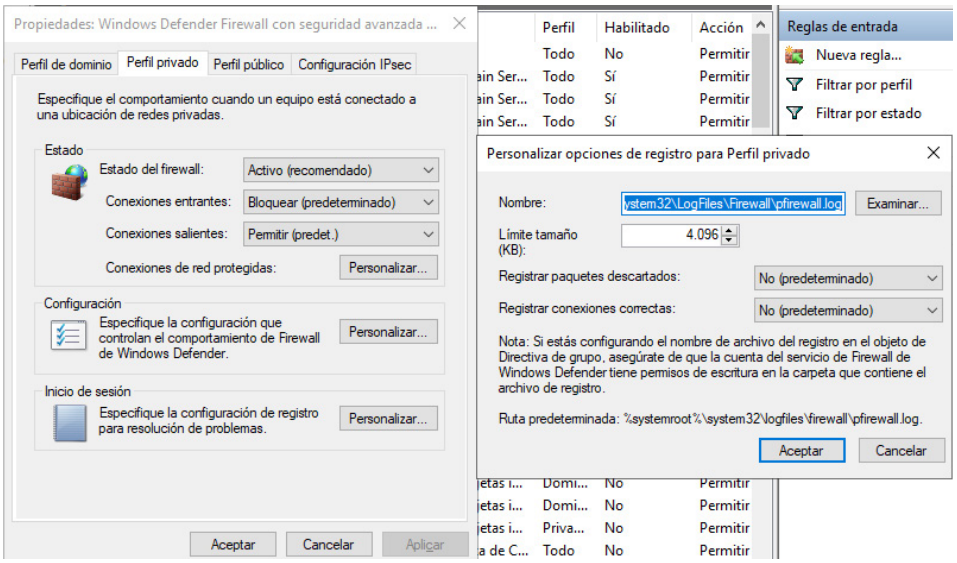


Imagen 7. Activando el registro de paquetes descartados en el firewall de Windows.

El administrador podrá seleccionar otro nombre, así como otra ruta para el fichero de log. Cuando se haya producido una activación del registro, el fichero log se creará y comenzará posteriormente a llenarse con los distintos paquetes de una de las dos condiciones que podemos encontrar, o bien paquetes descartados o bien correctas.

www.universae.com