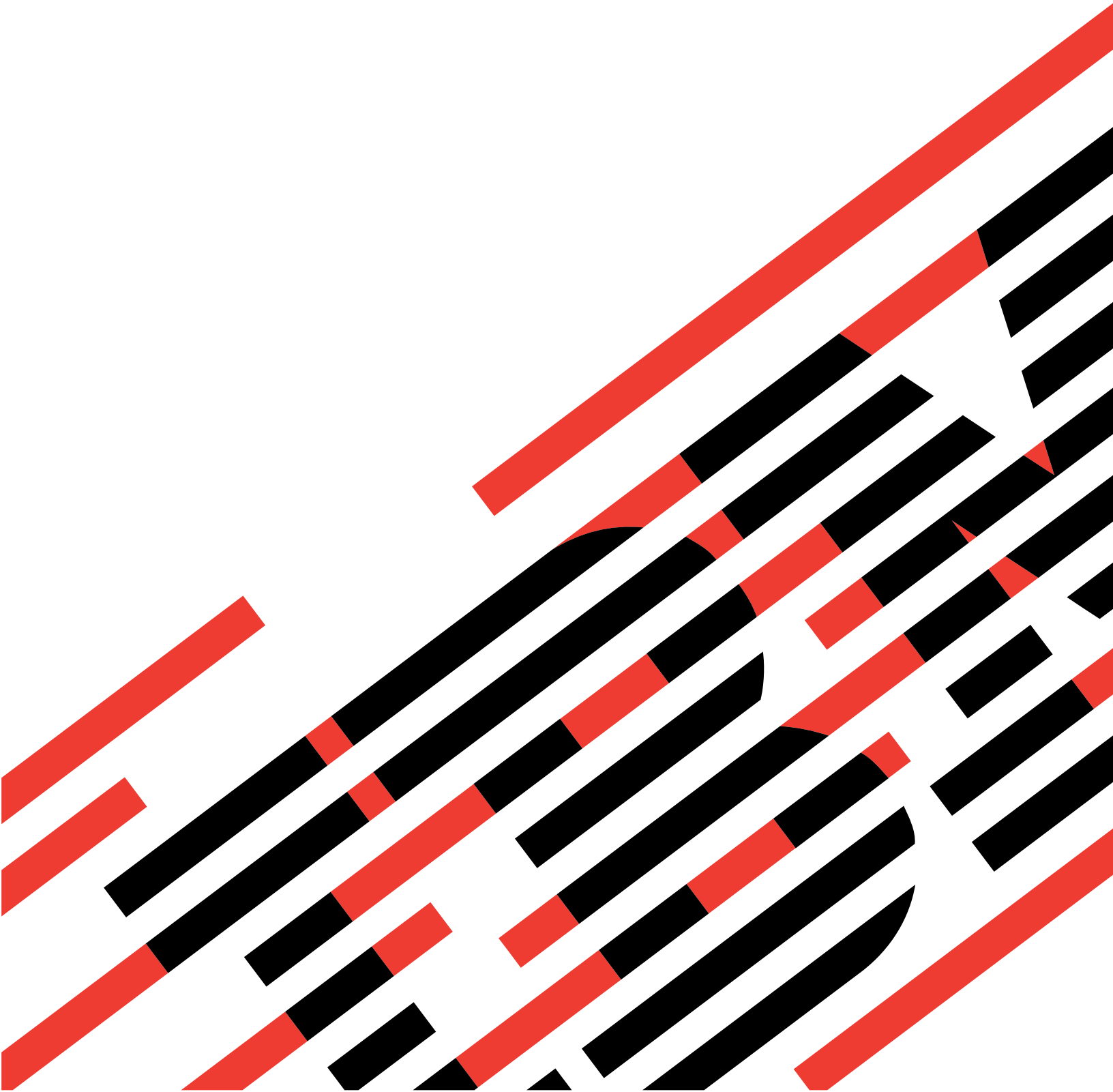
IBM

eserver

iSeries

Seguridad de la red
Filtrado IP y conversión de direcciones de red (NAT)



IBM

@server

iSeries

Seguridad de la red
Filtrado IP y conversión de direcciones de red (NAT)

Contenido

Parte 1. Filtrado IP y conversión de direcciones de red (NAT)

El filtrado IP y la conversión de direcciones de red (NAT) actúan como un cortafuegos para proteger la red interna de los intrusos. El filtrado IP permite controlar qué tráfico IP se debe dejar entrar y salir de la red. Básicamente, protege la red filtrando paquetes en función de las reglas que usted defina. NAT, por otra parte, permite ocultar las direcciones IP privadas que no están registradas detrás de un conjunto de direcciones IP registradas. Esto ayuda a proteger la red interna de las redes externas. NAT también ayuda a aliviar el problema de escasez de direcciones IP, ya que se pueden representar muchas direcciones privadas con un conjunto pequeño de direcciones registradas.

Nota: Las **reglas de paquetes** son la combinación del filtrado IP y de NAT. El término reglas de paquetes, utilizado en este tema, se aplica a ambos componentes.

Si desea comprender los por qué, los qué y los cómo de las reglas de paquetes, repase los temas que figuran a continuación.

Novedades de la versión V5R2
Destaca las modificaciones y mejoras efectuadas en las reglas de paquetes para la versión V5R2.

Imprimir este tema
Si prefiere una versión en copia impresa de esta información, venga hasta aquí para imprimir el PDF.

Casos prácticos de reglas de paquetes
Repase estos casos prácticos para familiarizarse con algunos de los usos más frecuentes de las reglas de paquetes. Cada caso práctico proporciona una ilustración y una configuración de ejemplo.

Conceptos de reglas de paquetes
Antes de comenzar, es necesario tener al menos conocimientos básicos de las tecnologías y conceptos de las reglas de paquetes. Este tema proporciona información acerca del filtrado IP y de NAT. Se incluyen temas tales como la correlación y la ocultación de direcciones. También incluye una lista de terminología específica de iSeries.

Planificar reglas de paquetes
La planificación es sumamente importante para determinar cuales son los recursos que es necesario proteger y contra quién. Este tema proporciona una hoja de trabajo de planificación y otra información a fin de ayudarle a tomar una decisión, partiendo de una base sólida, sobre lo que es más conveniente para sus necesidades de seguridad concretas.

Configurar reglas de paquetes
Este tema proporciona información sobre lo que se puede hacer con las reglas de paquetes y cómo hacerlo.

Gestionar reglas de paquetes
Este tema describe algunas tareas que se pueden realizar para gestionar las reglas de paquetes. Entre otras funciones se incluye el registro por diario, la edición y la visualización de los archivos de reglas.

Resolver problemas de las reglas de paquetes
Consulte este tema cuando se produzcan errores y para cerciorarse de que se está ocupando de áreas de posibles problemas.

Información afín para las reglas de paquetes
Venga hasta aquí para obtener enlaces con otras fuentes de información de reglas de paquetes y temas afines.

Además de la información incluida en este tema, puede consultar la ayuda en línea disponible en el Editor de reglas de paquetes de iSeries Navigator. La ayuda en línea de iSeries Navigator le ofrece consejos y técnicas para obtener el máximo rendimiento de las reglas de paquetes. Esta ayuda incluye asesoramiento acerca de **¿Cómo puedo...?** , **Desearía saber...**, y amplia ayuda contextual.

Capítulo 1. Novedades de la versión V5R2

Entre las mejoras de la función de reglas de paquetes de la versión V5R2 se incluyen:

- **Editor de reglas de paquetes**
  El Editor de reglas de paquetes, nuevo y fácil de utilizar, permite crear y modificar reglas de paquetes utilizando asistentes y páginas de propiedad.
- **Asistentes nuevos**
  Tres asistentes nuevos que, dependiendo del tipo de reglas que desee configurar, crean automáticamente todas las sentencias de filtro y NAT necesarias. Estos asistentes son los siguientes:
  - Asistente **Permitir un servicio**
  - Asistente **Conversión de direcciones**
  - Asistente **Protección contra la usurpación**
- **Una nueva manera de visualizar las reglas de paquetes**
  La nueva manera de visualizar en iSeries Navigator permite seleccionar una interfaz y ver sus reglas de paquetes activas y asociadas, incluyendo las sentencias de filtro.
- **Soporte para crear archivos de reglas de paquetes**
  Soporte para crear archivos de reglas de paquetes en función de una definición de tipo de datos XML encontrada en el archivo,
  `/QIBM/XML/DTD/QtofPacketRules.dtd`
- **Archivo de reglas de paquetes de ejemplo**
  Este archivo puede verse en formato tradicional .i3p o en formato .xml. Puede utilizarse el archivo de ejemplo a fin de aprender la sintaxis apropiada para crear reglas de paquetes en iSeries y para ver cómo funcionan juntas en un archivo las distintas sentencias.

Si desea obtener más información de las novedades o modificaciones de este release, consulte el Enlace con PDF Memorándum de los usuarios  .

Capítulo 2. Imprimir este tema

Para ver o bajar la versión en PDF, seleccione Reglas de paquete (aproximadamente 245 KB o 42 páginas).

Para salvar un archivo PDF en la estación de trabajo para poder verlo o imprimirlo:

1. Pulse con el botón derecho del ratón en el PDF del navegador (pulse con el botón derecho del ratón en el enlace superior).
2. Pulse en **Guardar destino como...**.
3. Sitúese en el directorio en el que desea salvar el archivo PDF.
4. Pulse en **Salvar**.

Bajar Adobe Acrobat Reader

Si necesita Adobe Acrobat Reader para ver o imprimir estos PDF, puede bajar una copia desde el sitio web de Adobe (http://www.adobe.com/products/acrobat/readstep.html)  .

Capítulo 3. Casos prácticos de reglas de paquetes

Consulte los casos prácticos presentados a continuación si precisa una explicación sobre cómo utilizar NAT y el filtrado IP para proteger la red. Cada uno de los casos prácticos incluye un diagrama y una configuración de ejemplo.

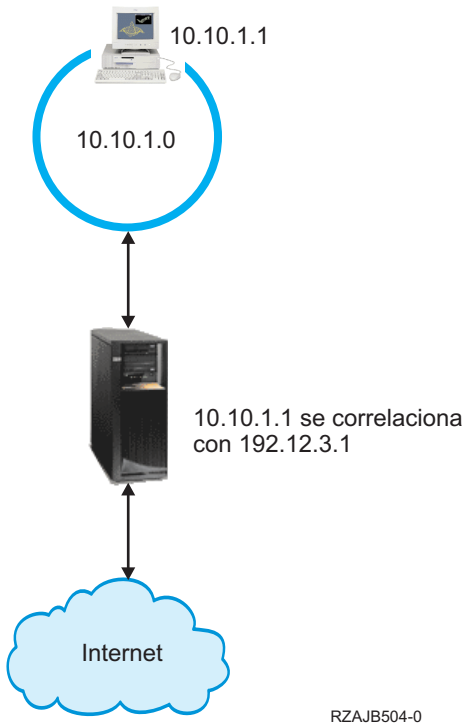
- **Caso práctico de reglas de paquetes: correlacionar las direcciones IP (NAT estática)**
  En este caso práctico, su empresa utiliza NAT estática para correlacionar sus direcciones IP privadas con direcciones públicas.
- **Caso práctico de reglas de paquetes: crear reglas de filtro para permitir HTTP, Telnet y FTP**
  En este caso práctico, su empresa utiliza el filtrado IP para restringir el tráfico IP que puede acceder a su servidor Web en HTTP, Telnet y FTP.
- **Caso practico de reglas de paquetes: combinar NAT y el filtrado IP**
  En este caso práctico, su empresa utiliza NAT y el filtrado IP para ocultar el servidor de los PC y de la web detrás de una dirección IP única y pública y para permitir que otras empresas puedan acceder al servidor Web.
- **Caso práctico de reglas de paquetes: ocultar las direcciones IP (NAT de enmascaramiento)**
  En este caso práctico, su empresa utiliza NAT de enmascaramiento para ocultar las direcciones privadas de los PC, permitiendo al mismo tiempo que los empleados puedan acceder a Internet

Nota: En cada uno de los casos prácticos, las direcciones IP `192.x.x.x` representan direcciones IP públicas. Todas las direcciones se utilizan únicamente a título de ejemplo.

Caso práctico de reglas de paquetes: correlacionar direcciones IP (NAT estática)

Situación

Usted es propietario de una empresa y decide montar una red privada. Sin embargo, nunca ha registrado ninguna dirección IP pública ni ha adquirido un permiso para utilizarla. Todo va bien hasta que desea acceder a Internet. Resulta que el rango de direcciones de la empresa está registrado a nombre de otro, y por ello piensa que la configuración actual que tiene está obsoleta. La necesidad de permitir a los usuarios públicos el acceso al servidor Web es imperiosa. ¿Qué debe hacer?



Solución

Podría utilizar la función de NAT estática. Esta asigna una dirección (privada) original a una dirección (pública) registrada. El iSeries correlaciona esta dirección registrada con la dirección privada. La dirección registrada permite que la dirección privada se comunique con Internet. Básicamente, constituye un puente entre ambas redes. Las comunicaciones pueden iniciarse desde cualquiera de las dos.

La utilización de NAT estática permite conservar todas las direcciones IP internas actuales y acceder igualmente a Internet. Será necesario tener una dirección IP registrada por cada dirección privada que acceda a Internet. Por ejemplo, si tiene 12 usuarios, necesita 12 direcciones IP públicas para correlacionar las 12 direcciones privadas.

En la ilustración anterior, la dirección de NAT 192.12.3.1 espera el regreso de información y mientras tanto resulta inservible, como si de un shell se tratase. Cuando la información vuelve, NAT correlaciona a la inversa la dirección con el PC. Si la función de NAT estática está activa, el tráfico de entrada que vaya destinado de forma directa a la dirección 192.12.3.1 no llegará nunca a esa interfaz porque tal dirección es únicamente una representación de la dirección interna. El destino real es la dirección privada 10.10.1.1, aunque (para el mundo que está fuera del iSeries) parezca que la dirección IP deseada es 192.12.3.1.

Configuración

Para configurar las reglas de paquetes descritas en este caso práctico es preciso utilizar el asistente **Conversión de direcciones** en iSeries Navigator. El asistente requiere la información siguiente:

- La dirección privada que desea correlacionar: 10.10.1.1
- La dirección pública con la que desea correlacionar la dirección privada: 192.12.3.1
- El nombre de línea en que tiene lugar la correlación de direcciones: TRNLINE

Para utilizar el asistente **Conversión de direcciones**, siga estos pasos:

1. En iSeries Navigator, seleccione **su servidor –>red –> políticas IP.**
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.
3. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Crear un archivo nuevo de reglas de paquetes** y pulse **Aceptar**.
4. En el menú **Asistentes**, seleccione **Conversión de direcciones** y siga las instrucciones del asistente para configurar las reglas de paquetes de conversión de direcciones para correlacionar.

Sus reglas de paquetes deben quedar definidas de la manera siguiente:

```
-----------------------------------------------------
Sentencias para correlacionar 10.1.1.1 con 192.12.3.1 sobre TRNLINE
-----------------------------------------------------
ADDRESS MAPPRIVATE1   IP = 10.1.1.1
ADDRESS MAPPUBLIC1   IP = 192.12.3.1
MAP MAPPRIVATE1   TO MAPPUBLIC1   LINE = TRNLINE
-----------------------------------------------------
```

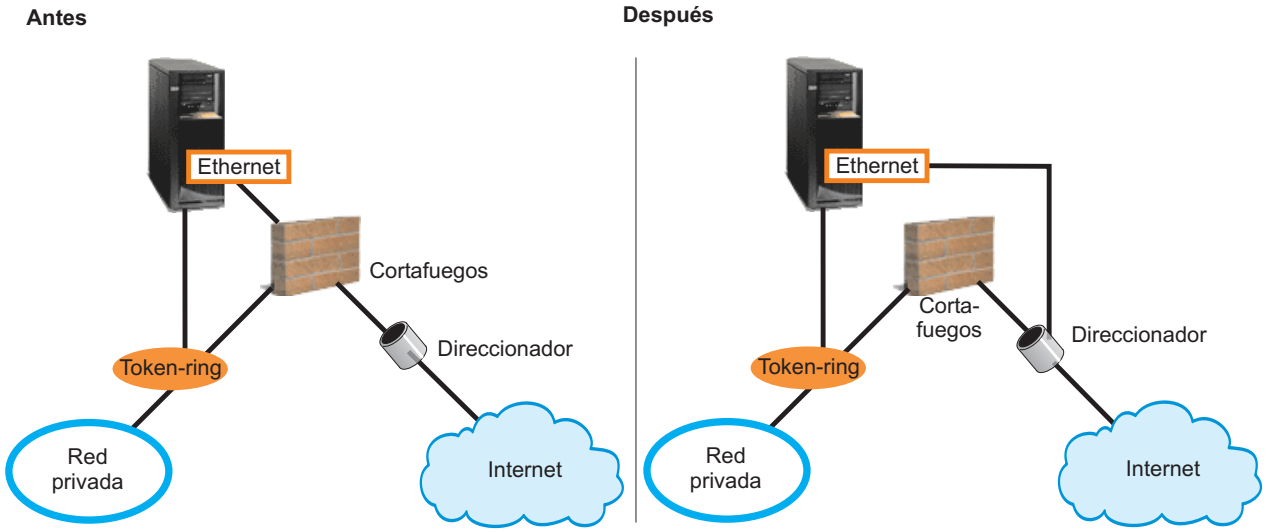
Cuando termine de crear estas reglas y otras que considere necesarias, deberá verificarlas para asegurarse de que se activarán sin errores. Después de hacer eso, podrá activarlas.

Nota: la línea de token-ring definida en la configuración anterior (LINE=TRNLINE) debe ser la línea utilizada por 192.12.3.1. La función de NAT estática no tendrá efecto si 10.10.1.1 utiliza la línea de token-ring definida en la configuración anterior. Siempre que utilice NAT, también debe habilitar el reenvío IP. En el apartado Resolución de problemas de las reglas de paquetes hallará información detallada al respecto.

Caso práctico de reglas de paquetes: crear reglas de filtro para permitir HTTP, Telnet y FTP

Situación

Desea proporcionar aplicaciones Web a sus clientes, pero el cortafuegos actual hace horas extraordinarias y no desea añadirle más carga. Un colega le sugiere que ejecute las aplicaciones fuera del cortafuegos. Sin embargo, le interesa que desde Internet sólo pueda acceder al servidor Web iSeries el tráfico HTTP, FTP y Telnet. ¿Qué debe hacer?



Solución

Los filtros IP permiten establecer reglas que expliquen cuál es la información que desea permitir. Escriba en este escenario reglas de paquetes que permitan al tráfico HTTP, FTP y Telnet (de entrada y de salida) llegar al servidor Web, que es el iSeries en este caso. La dirección pública del servidor es 192.54.5.1 y la dirección IP privada es 10.1.2.3.

Configuración

Para configurar las reglas de paquetes descritas en este caso práctico es preciso utilizar el asistente **Permitir un servicio** en iSeries Navigator. El asistente requiere la información siguiente:

- El tipo de servicio que desea permitir: HTTP
- La dirección pública del servidor iSeries: 192.54.5.1
- La dirección del cliente: una dirección IP
- La interfaz sobre la que se ejecutará el servicio: TRNLINE
- La dirección en la que se ejecutará el servicio: INBOUND
- El nombre que desea utilizar para identificar este conjunto de filtros: external_files

Para utilizar el asistente **Permitir servicio**, siga estos pasos:

1. En iSeries Navigator, seleccione **su servidor –> red –> políticas IP**.
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.
3. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Crear un archivo nuevo de reglas de paquetes** y pulse **Aceptar**.
4. En el menú **Asistentes**, seleccione **Permitir un servicio** y siga las instrucciones del asistente para crear las reglas de filtro.

Estas reglas de paquetes permiten al tráfico HTTP entrar y salir del sistema. Sus reglas de paquetes deben quedar definidas de la manera siguiente:

```
-------------------------------------------
Sentencias para permitir HTTP de entrada sobre TRNLINE
-------------------------------------------
INCLUDE   FILE = /QIBM/UserData/OS400/TCPIP/PacketRules/Services.i3p
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.54.5.1   DSTADDR = *
  SERVICE = HTTP_80_FS   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.54.5.1
   SERVICE = HTTP_80_FC   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.54.5.1   DSTADDR = *
   SERVICE = HTTP_443_FS   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.54.5.1
   SERVICE = HTTP_443_FC   JRN = OFF
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
-------------------------------------------
```

Utilice el asistente **Permitir un servicio** dos veces más para crear reglas de filtro que permitan al tráfico FTP y al tráfico Telnet entrar y salir del sistema.

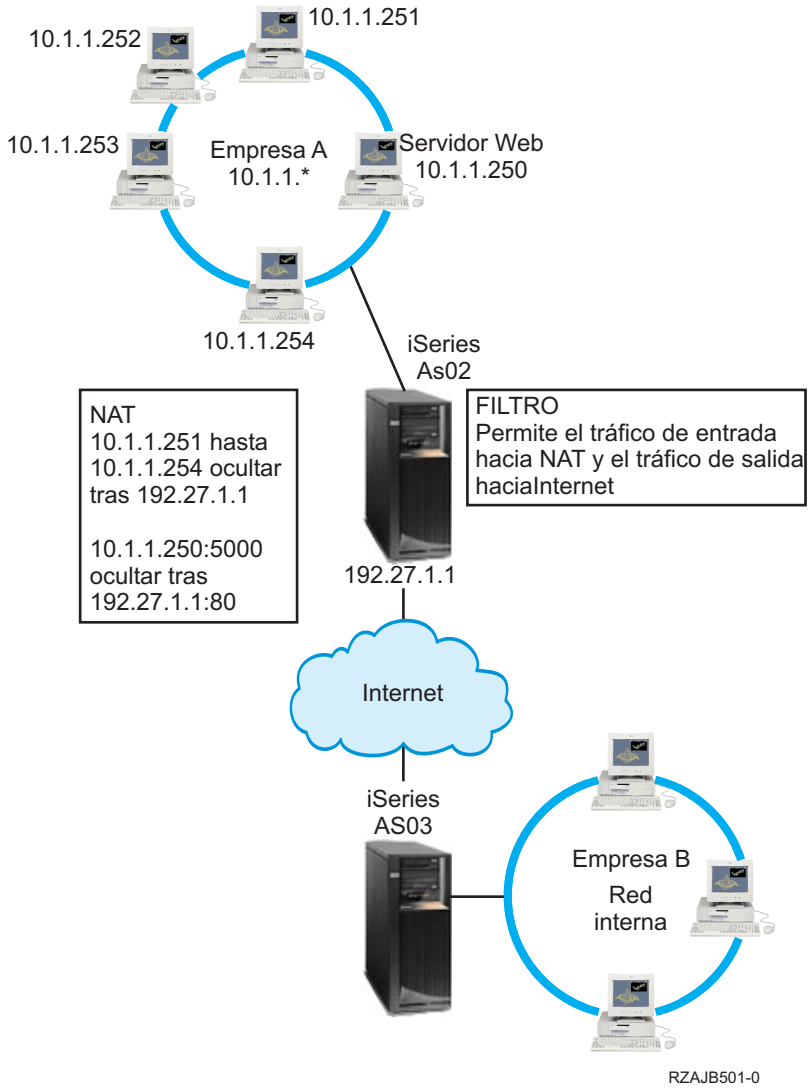
Cuando termine de crear estas reglas de filtro, deberá verificarlas para asegurarse de que se activarán sin errores. Después de hacer eso, podrá activarlas.

Caso practico de reglas de paquetes: combinar NAT y el filtrado IP

Situación

Su empresa cuenta con una red interna de tamaño moderado que utiliza un iSeries como pasarela. Usted desea transferir la totalidad del tráfico Web del iSeries pasarela a un servidor Web dedicado, situado detrás de la pasarela. El servidor Web se ejecuta en el puerto 5000. Usted desea ocultar todos los PC

privados y el servidor Web detrás de una dirección de la interfaz del iSeries pasarela; AS02 en el diagrama de más abajo. También desea permitir a otras empresas el acceso al servidor Web. ¿Qué debe hacer?



Solución

Podría utilizar juntos el filtrado IP y NAT para configurar:

1. Ocultar NAT a fin de ocultar los PC detrás de una dirección pública, 192.27.1.1, para que así puedan acceder a Internet.
2. NAT con correlación de puerto para ocultar la dirección del servidor Web, 10.1.1.250, y el número de puerto ,5000, detrás de una dirección pública, 192.27.1.1 y el número de puerto 80. Observe que ambas reglas de NAT están escondidas detrás de 192.27.1.1. Esto es aceptable siempre y cuando las direcciones que vaya a ocultar no se solapen. La regla de NAT con correlación de puerto sólo permitirá que acceda al sistema el tráfico iniciado externamente en el puerto 80. Si el tráfico iniciado externamente no coincide exactamente con la dirección y el número de puerto, NAT no lo convertirá y el paquete quedará descartado.
3. Reglas que filtran todo el tráfico de entrada que vaya destinado a la red privada hasta llegar a NAT y el tráfico de salida hasta llegar a Internet.

Configuración

Para configurar las reglas de paquetes para ocultar NAT, descritas en este caso práctico, deberá utilizar el asistente **Conversión de direcciones** en iSeries Navigator. El asistente requiere la información siguiente:

- El conjunto de direcciones que desea ocultar: 10.1.1.251 mediante 10.1.1.254
- La dirección de interfaz detrás de la cual desea ocultar el conjunto de direcciones: 192.27.1.1

Para utilizar el asistente **Conversión de direcciones**, siga estos pasos:

1. En iSeries Navigator, seleccione **su servidor –> red –> políticas IP**.
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.
3. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Crear un archivo nuevo de reglas de paquetes** y pulse **Aceptar**.
4. En el menú **Asistentes**, seleccione **Conversión de direcciones** y siga las instrucciones del asistente para configurar las reglas de paquetes de conversión de direcciones para ocultar.

Esta regla de paquetes ocultará los cuatro PC detrás de una dirección pública para que así puedan acceder a Internet. La regla de paquetes Ocultar NAT debe quedar definida de la manera siguiente:

```
------------------------------------------------------------
Sentencias a ocultar 10.1.1.251 - 10.1.1.254 detrás de 192.27.1.1
------------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.251 THROUGH 10.1.1.254
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE HIDE1   BEHIND BEHIND1
------------------------------------------------------------
```

Para configurar el NAT con correlación de puerto, siga estos pasos:

1. Acceda al Editor de reglas de paquetes de iSeries Navigator.
2. Cree una dirección definida para la dirección de servidor Web y el puerto 5000:
   a. En el menú **Insertar**, seleccione **Dirección...**.
   b. En la página **General**, entre **Web250** en el campo **Nombre de dirección**.
   c. Seleccione **Direcciones IP** en la lista desplegable **Dirección definida**. A continuación, pulse en **Añadir** y entre la dirección IP del servidor Web `10.1.1.250` en el campo de edición.
   d. Pulse en **Aceptar**.
3. Cree una dirección definida para representar la dirección pública 192.27.1.1:
   Nota: como ya ha creado una dirección definida para representar la dirección pública 192.27.1.1 cuando configuró las reglas de paquetes para ocultar NAT, puede omitir este paso en este caso práctico específico y continuar en el paso 4. Sin embargo, si utiliza estas instrucciones para configurar el NAT con correlación de puerto a fin de utilizarlo en su red, y no ha configurado las reglas de paquetes para ocultar NAT, deberá seguir las instrucciones que contiene este paso.
   a. En el menú **Insertar**, seleccione **Dirección...** .
   b. En la página **General**, entre o seleccione **BEHIND1** en el campo **Nombre de dirección**.
   c. Seleccione **Direcciones IP** en la lista desplegable **Dirección definida**. A continuación, pulse en **Añadir** y entre `192.27.1.1` en el campo de edición **Direcciones IP**.
   d. Pulse en **Aceptar**.
4. Cree la regla de NAT con correlación de puerto:
   a. En el menú **Insertar** seleccione **Ocultar...**.
   b. En la página **General**, seleccione `Web250` en la lista desplegable **Ocultar nombre de dirección**.
   c. Seleccione **BEHIND1** en la lista desplegable **Detrás de nombre de dirección**.
   d. Seleccione **Permitir conexiones de entrada**, y entre `5000` en el campo **Ocultar puerto**.
   e. Entre `80` en el campo **Detrás de puerto**.

f. Entre 16 y seleccione **segundos** en los campos **Tiempo de espera excedido**.
g. Entre 64 en el campo **Conversaciones máximas**.
h. Seleccione **OFF** en la lista desplegable **Registrar por diario**.
i. Pulse en **Aceptar**.

La regla de NAT con correlación de puerto ocultará la dirección y el número de puerto del servidor Web detrás de una dirección y un número de puerto públicos. Observará que ambas reglas de NAT están ocultas detrás de una dirección IP común. Esto es aceptable siempre y cuando las direcciones que vaya a ocultar no se solapen. Esta regla de NAT con correlación de puerto sólo permitirá que acceda al sistema el tráfico iniciado externamente en el puerto 80.

La regla de NAT con correlación de puerto debe quedar definida de la manera siguiente:

```
ADDRESS Web250   IP = 10.1.1.250
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE Web250:5000   BEHIND BEHIND1:80   TIMEOUT = 16   MAXCON = 64   JRN = OFF
```

Para crear las reglas de filtro descritas en este caso práctico, siga estos pasos:

1. Acceda al Editor de reglas de paquetes de iSeries Navigator.
2. Cree una regla de filtro para permitir que el tráfico de entrada llegue a la red privada.
   a. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Crear un archivo nuevo de reglas de paquetes** y pulse **Aceptar**.
   b. En el menú **Insertar**, seleccione **Filtrar...**.
   c. En la página **General**, entre external_rules en el campo **Establecer nombre**.
   d. Seleccione **PERMIT** en la lista desplegable **Acción**.
   e. Seleccione **INBOUND** en la lista desplegable **Dirección** .
   f. Seleccione = y * en las listas desplegables **Nombre de dirección origen**.
   g. Seleccione = y entre 192.27.1.1 en los campos **Nombre de dirección de destino**.
   h. Seleccione **OFF** en la lista desplegable **Registrar por diario** .
   i. En la página **Servicios**, seleccione **Servicio**,
   j. Seleccione **TCP** en la lista desplegable **Protocolo**.
   k. Seleccione = y * en las listas desplegables **Puerto origen**.
   l. Seleccione = y * en las listas desplegables **Puerto de destino**.
   m. Pulse en **Aceptar**.
3. Cree una regla de filtro para permitir que el tráfico de salida procedente de la red privada llegue a Internet.
   a. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Abrir un archivo de reglas de paquetes existente** y pulse **Aceptar**.
   b. En el diálogo **Abrir archivo**, seleccione el archivo **external_rules** y pulse **Abrir**.
   c. En el menú **Insertar**, seleccione **Filtrar...** .
   d. En la página **General**, seleccione external_rules en la lista desplegable **Establecer nombre**.
   e. Seleccione **PERMIT** en la lista desplegable **Acción**.
   f. Seleccione **OUTBOUND** en la lista desplegable **Dirección**.
   g. Seleccione = y entre 192.27.1.1 en los campos **Nombre de dirección origen**.
   h. Seleccione = y * en las listas desplegables **Nombre de dirección destino**.
   i. Seleccione **OFF** en la lista desplegable **Registrar por diario**.
   j. En la página **Servicios**, seleccione **Servicio** ,
   k. Seleccione **TCP** en la lista desplegable **Protocolo**.
   l. Seleccione = y * en las listas desplegables **Puerto origen**.

m. Seleccione = y * en las listas desplegables **Puerto de destino**.

n. Pulse en **Aceptar**.

4. Defina una interfaz de filtro para el conjunto de filtros que ha creado:
   a. En el menú **Insertar**, seleccione **Interfaz de filtro...**.
   b. Seleccione **Nombre de línea** y después seleccione **TRNLINE** en la lista desplegable **Nombre de línea**.
   c. En la página **Conjuntos de filtros**, seleccione **external_rules** en la lista desplegable **Conjunto de filtros**. A continuación, pulse en **Añadir**.
   d. Pulse en **Aceptar**.

Estos filtros, junto con la sentencia HIDE, permitirán que el tráfico de entrada que vaya destinado a la red privada llegue hasta NAT y que el tráfico de salida llegue a Internet. No obstante, NAT sólo permitirá que entre en el servidor el tráfico iniciado externamente en el puerto 80. NAT no convertirá el tráfico iniciado externamente que no coincida con la regla de NAT con correlación de puerto. Las reglas de filtro deberán quedar definidas de la manera siguiente:

```
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.27.1.1
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.27.1.1   DSTADDR = *
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
```

La sentencia siguiente enlaza (asocia) el conjunto de filtros 'external_rules' con la interfaz física correcta.

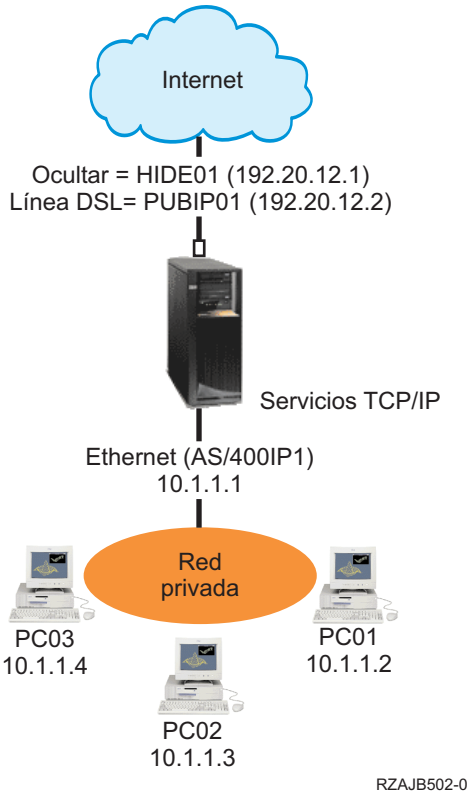
```
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
```

Cuando termine de crear estas reglas de filtro, deberá verificarlas para asegurarse de que se activarán sin errores. Después de hacer eso, podrá activarlas.

Caso práctico de reglas de paquetes: ocultar las direcciones IP (NAT de enmascaramiento)

Situación

Usted tiene una pequeña empresa y desea permitir el servicio HTTP en el iSeries. Tiene un modelo 170e con una tarjeta Ethernet y tres PC. El suministrador de servicios Internet (ISP) le proporciona una conexión DSL y un modem DSL. También le asigna las direcciones IP públicas siguientes: 192.20.12.1 y 192.20.12.2. Todos los PC tienen una dirección 10.1.1.x en la red interna. Desea asegurarse de que las direcciones privadas de los PC permanecen ocultas para evitar que usuarios externos inicien comunicaciones con la red interna, permitiendo al mismo tiempo que los empleados puedan acceder a Internet. ¿Qué debe hacer?



Solución

Oculte las direcciones de los PC, 10.1.1.1 hasta 10.1.1.4, detrás de la dirección pública 192.20.12.1. A partir de ese momento podrá ejecutar los servicios TCP/IP desde la dirección 10.1.1.1. La función de NAT de rango (que oculta un rango de direcciones internas) protegerá los PC contra las comunicaciones que se inicien desde fuera de la red, porque para que comience la función NAT de rango, el tráfico debe iniciarse internamente. Sin embargo, la función de NAT de rango no protegerá la interfaz de iSeries. Será necesario filtrar el tráfico para proteger el iSeries contra la recepción de información sin convertir.

Configuración

Para configurar las reglas de paquetes descritas en este caso práctico es preciso utilizar el asistente **Conversión de direcciones** en iSeries Navigator. El asistente requiere la información siguiente:

- El conjunto de direcciones que desea ocultar: 10.1.1.1 hasta 10.1.1.4
- La dirección de interfaz detrás de la cual desea ocultar el conjunto: 192.20.12.1

Para utilizar el asistente **Conversión de direcciones**, siga estos pasos:

1. En iSeries Navigator, seleccione **su servidor –> red –> políticas IP**.
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.
3. En el diálogo **Bienvenido a la configuración de reglas de paquetes**, seleccione **Crear un archivo nuevo de reglas de paquetes** y pulse **Aceptar**.
4. En el menú **Asistentes**, seleccione **Conversión de direcciones** y siga las instrucciones del asistente para configurar las reglas de paquetes de conversión de direcciones para ocultar.

Sus reglas de paquetes deben quedar definidas de la manera siguiente:

```
-----------------------------------------------------
Sentencias a ocultar 10.1.1.1 - 10.1.1.4 detrás de 192.20.12.1
-----------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.1 THROUGH 10.1.1.4
ADDRESS BEHIND1   IP = 192.20.12.1
HIDE HIDE1   BEHIND BEHIND1
-----------------------------------------------------
```

Cuando termine de crear estas reglas de filtro, deberá verificarlas para asegurarse de que se activarán sin errores. Después de hacer eso, podrá activarlas.

Capítulo 4. Conceptos de reglas de paquetes

Las reglas de paquetes constan de reglas de conversión de direcciones de red (NAT) y de reglas de filtrado IP. Estos dos componentes se ejecutan en la capa IP de la pila TCP/IP y ayudan a proteger el sistema contra los riesgos potenciales asociados normalmente al tráfico TCP/IP.

Para comprender mejor cómo funcionan las reglas de paquetes, deberá estar familiarizado con los conceptos siguientes y saber cómo se aplican en el iSeries:

- **Terminología de las reglas de paquetes**
  Proporciona una lista de terminología específica de iSeries con la que deberá estar familiarizado.
- **Las reglas de paquetes frente a otras soluciones de seguridad de iSeries**
  ¿Qué diferencias hay entre las reglas de paquetes y otras soluciones de seguridad de iSeries? Venga hasta aquí para averiguarlo.
- **Conversión de direcciones de red (NAT)**
  Hay varios tipos diferentes de conversión de direcciones. Este tema proporciona la información necesaria para determinar cuál es el adecuado para cada red.
- **Filtrado IP**
  Consulte este tema si desea obtener más información sobre cómo funciona el componente de filtrado IP de las reglas de paquetes.
- **Organizar las reglas de NAT con las reglas de filtro IP**
  Se pueden utilizar reglas de NAT y reglas de filtro IP separadamente o juntas. Este tema describe la manera en que estos dos componentes funcionan juntos.
- **Organizar varias reglas de filtro IP**
  Cuando se crean las reglas de filtro, el sistema las procesa siguiendo un orden determinado. Este tema explica cómo se procesan múltiples reglas de filtro, y proporciona un ejemplo.
- **Protección contra la usurpación**
  Esta página define la protección contra la usurpación y explica por qué es necesario utilizarla.

Terminología de las reglas de paquetes

La lista que figura a continuación contiene algunos términos específicos de iSeries que se utilizan en este tema de Information Center.

Marco Es una dirección pública que hace de frontera entre una red de confianza y otra que no lo es. Describe la dirección IP como si se tratase de una interfaz real en el iSeries. El sistema necesita saber cuál es el ″tipo″ de dirección que se define. Por ejemplo, la dirección IP del PC es de confianza, pero la dirección IP pública del servidor es la frontera.

Cortafuegos
Es una barrera lógica que rodea a los sistemas de una red. Consta de hardware, de software y de una política de seguridad que controla el acceso y el flujo de información entre los sistemas seguros o de confianza y los que no lo son.

maxcon
Es el número máximo de conversaciones que pueden estar activas a la vez. El sistema pide que se defina este número cuando se configuran las reglas de enmascaramiento de NAT. El valor por omisión es 128. Maxcon sólo es pertinente para las reglas de NAT de enmascaramiento.

Conversación de NAT
Es una relación existente entre cualquiera de las direcciones IP y los números de puerto siguientes:

- Dirección IP de origen y número de puerto de origen privados (sin NAT)
- Dirección IP de origen (NAT) pública y número de puerto de origen (NAT) público
- Dirección IP y número de puerto de destino (una red externa)

Identificador de filtro PPP
Un identificador de filtro PPP permite aplicar reglas de filtro a una interfaz que ha sido definida en un perfil de punto a punto. El identificador de filtro PPP también enlaza las reglas de filtro con grupos de usuarios en un perfil de punto a punto. Como el perfil de punto a punto se asocia con una dirección IP específica, el identificador de filtros define implícitamente la interfaz a la que se aplican las reglas. Si desea más información, consulte el caso práctico Gestionar el acceso de usuarios remotos a recursos utilizando políticas de grupo y filtrado IP en el tema *Servicios de acceso remoto: conexiones PPP*.

Tiempo de espera excedido
Controla el tiempo que puede durar una conversación. Si se establece un tiempo de espera demasiado corto, la conversación se detiene con excesiva rapidez. El valor por omisión es 16.

Las reglas de paquetes frente a otras soluciones de seguridad de iSeries

El iSeries tiene integrados diversos componentes de seguridad que pueden proteger el sistema contra varios tipos de riesgos. Las reglas de paquetes permiten, por ejemplo, proteger el sistema de forma económica. En algunos casos, las reglas de paquetes pueden proporcionar todo lo necesario sin tener que efectuar desembolsos adicionales. Sin embargo, la seguridad del sistema debe ser más importante que los costes.

En situaciones de alto riesgo, tales como asegurar un sistema de producción o asegurar las comunicaciones entre el iSeries y otros sistemas en una red, se deberían investigar otras soluciones de seguridad de iSeries con objeto de ampliar la protección.

Consulte los temas de Information Center, que figuran a continuación, para obtener información que le ayudará a asegurar que su estrategia de seguridad incluye múltiples líneas de defensa:

- **IBM SecureWay®: iSeries e Internet**
  Este tema proporciona amplia información sobre los riesgos y las soluciones que deben tenerse en cuenta a la hora de utilizar Internet.
- **Capa de sockets segura (SSL)**
  SSL proporciona conexiones seguras entre las aplicaciones de servidor y sus clientes. Este tema incluye información acerca de cómo habilitar SSL en las aplicaciones iSeries.
- **Conexión en red privada virtual (VPN)**
  VPN permite a las empresas extender de manera segura sus intranets privadas en la infraestructura existente de una red pública, como es Internet. Este tema describe VPN y define cómo utilizarla en iSeries.
- **Consejos y herramientas para asegurar su iSeries** 
  Este libro en PDF proporciona información de alto nivel acerca de la manera de ampliar la seguridad del iSeries.

Conversión de direcciones de red (NAT)

Las direcciones IP se están agotando con rapidez debido al amplio crecimiento de Internet. Las empresas utilizan redes privadas, lo que les permite seleccionar las direcciones IP que deseen. Sin embargo, si dos empresas tienen direcciones IP duplicadas e intentan comunicarse entre sí, tendrán problemas. Para poder comunicarse en Internet, es necesario tener una dirección exclusiva y registrada. La conversión de direcciones de red (NAT) permite acceder a Internet de una forma segura y sin tener que cambiar las direcciones IP de la red privada. Como su nombre indica, NAT es un mecanismo que convierte una dirección IP en otra.

Las reglas de paquetes contienen tres métodos de NAT. Normalmente se utiliza NAT para correlacionar direcciones (NAT estática) u ocultar direcciones (NAT de enmascaramiento). En los enlaces siguientes hallará información más detallada sobre las diversas formas de NAT:

- Función de NAT estática (de correlación)
- Función de NAT de enmascaramiento (de ocultación)
- Función de NAT de enmascaramiento u ocultación (de correlación de puerto)

Gracias a la ocultación o a la correlación de las direcciones, NAT resuelve los diversos problemas que estas plantean. En los ejemplos que se dan a continuación se explican varios problemas que puede resolver NAT.

Ejemplo 1: ocultar las direcciones IP internas a la vista de los demás

Va a configurar un iSeries como servidor Web público. Sin embargo, no desea que las redes externas sepan cuáles son las direcciones IP internas reales del servidor. Puede crear reglas de NAT que conviertan las direcciones privadas en direcciones públicas que tengan acceso a Internet. En este caso, la dirección ″verdadera″ del servidor queda oculta, lo que hace que el servidor resulte menos vulnerable a un ataque.

Ejemplo 2: convertir una dirección IP de un sistema principal interno en una dirección IP diferente

Desea que las direcciones IP privadas de la red interna se comuniquen con sistemas principales de Internet. Para disponerlo así, puede convertir la dirección IP de un sistema principal interno en una dirección IP diferente. Para comunicarse con los sistemas principales de Internet, debe utilizar direcciones IP públicas. Por lo tanto, utilizará NAT para convertir las direcciones IP privadas en direcciones públicas. Con ello se asegura de que el tráfico IP procedente del sistema principal interno se direcciona por Internet.

Ejemplo 3: compatibilizar las direcciones IP de dos redes distintas

Desea permitir que un sistema principal de otra red, como por ejemplo la de una empresa suministradora, se comunique con un sistema principal concreto de la red interna. Sin embargo, ambas redes utilizan direcciones privadas (10.x.x.x), lo que plantea un posible conflicto de direcciones a la hora de direccionar el tráfico entre ambos sistemas principales. Para evitarlo, puede utilizar NAT para convertir la dirección del sistema principal interno en una dirección IP distinta.

Función de NAT estática (de correlación)

NAT estática, o de correlación, proporciona una correspondencia biunívoca entre direcciones IP privadas y direcciones IP públicas. Permite correlacionar una dirección IP de la red interna con una dirección IP que se desea hacer pública.

La función de NAT estática permite que las comunicaciones se inicien desde la red interna o desde una red externa, como por ejemplo Internet. Resulta especialmente útil si dentro de la red interna hay un servidor al que desea permitir el acceso de usuarios públicos. En este caso, deberá crear una regla de NAT que correlacione la dirección real del servidor con una dirección pública. Ésta pasará a ser información externa. Con ello se garantiza que la información interna permanece fuera del alcance de alguien cuyas intenciones pudieran ser atacar los sistemas.

En la lista siguiente se destacan las características de NAT estática:

- Correlación biunívoca
- El inicio puede tener lugar en la red interna y en la externa
- La dirección con la que se establece asociación o correlación puede ser cualquiera
- La dirección con la que se establece asociación o correlación ya no puede utilizarse como interfaz IP

- No utiliza NAT con correlación de puerto

Atención

Proceda con cautela si decide correlacionar un PC con la dirección ″conocida públicamente″ del iSeries. Esta dirección es la dirección IP que está reservada para la mayor parte del tráfico de Internet e intranet. Si realiza la correlación con esta dirección IP, NAT convertirá todo el tráfico y lo enviará a la dirección privada interna. Dado que esta interfaz estará reservada para NAT, el iSeries y la interfaz quedarán inutilizados.

En Caso práctico de reglas de paquetes: correlacionar direcciones IP, hallará un caso práctico y una ilustración de la función de NAT estática.

Función de NAT de enmascaramiento (de ocultación)

La función de NAT de enmascaramiento u ocultación permite impedir que el mundo exterior (el que está fuera del iSeries) sepa cuál es la dirección real del PC. NAT direcciona el tráfico del PC al iSeries, lo que básicamente convierte al iSeries en la pasarela del PC. He aquí como funciona.

La función de NAT de enmascaramiento permite convertir varias direcciones IP en una sola dirección IP. Sirve para *ocultar* una o varias direcciones IP de la red interna detrás de una dirección IP que se desea hacer pública. Ésta es la dirección pública a la que se convierten las direcciones privadas y debe ser una interfaz definida del servidor iSeries. Para ser una interfaz definida, debe definirse la dirección pública como dirección `BORDER` .

Ocultar varias direcciones

Para ocultar varias direcciones, hay que especificar un rango de direcciones que NAT debe convertir por medio del servidor iSeries. El proceso general es el siguiente:

1. La dirección IP convertida sustituye a la dirección IP de origen. Esto sucede en la cabecera IP del paquete IP.
2. El número de puerto de origen IP (si lo hay) que figura en una cabecera TCP o UDP es sustituido por un número de puerto temporal.
3. Una conversación existente es la relación que hay entre la nueva dirección de origen IP y el nuevo número de puerto.
4. La conversación existente permite al servidor de NAT deshacer la conversión de los datagramas IP desde la máquina externa.

Para ver cómo es una cabecera de datagrama IP, vaya a Cabecera de paquete IP.

Cuando se utiliza la función de NAT de enmascaramiento, el tráfico lo inicia un sistema interno. Cuando esto sucede, NAT convierte el paquete IP a medida que pasa por el servidor de NAT de iSeries. La función de NAT de enmascaramiento es una magnífica opción porque los sistemas principales externos no pueden iniciar tráfico hacia la red. Como resultado, la red gana en protección contra un ataque del exterior. Asimismo, sólo es necesario comprar una única dirección IP pública para varios usuarios internos.

En la lista siguiente se destacan las características de NAT de enmascaramiento:

- La dirección IP privada o el rango de direcciones IP están vinculados detrás de una dirección IP pública en la máquina de NAT
- El inicio sólo puede tener lugar en la red interna
- Los números de puerto se asocian con números de puerto aleatorios. Esto significa que tanto la dirección como el número de puerto están ocultos a la vista de Internet.
- La dirección registrada que consta en la máquina de NAT puede utilizarse como interfaz fuera de NAT

Atención

- El valor de MAXCON debe ser lo suficientemente alto para dar cabida al número de conversaciones que se desea utilizar. Por ejemplo, si se utiliza FTP, el PC tendrá dos conversaciones activas. En este caso, será necesario establecer MAXCON de manera que dé cabida a varias conversaciones para cada PC. Habrá que decidir cuántas conversaciones concurrentes interesa permitir en la red. El valor por omisión es 128.
- El valor de TIMEOUT (una sentencia de regla HIDE) debe ser lo suficientemente alto para dar tiempo a que finalicen las conversaciones entre los PC. Para que la función de NAT de ocultación funcione correctamente, debe haber una conversación interna en curso. El valor de TIMEOUT indica al código cuánto debe esperar a que se produzca una respuesta a esta conversación interna. El valor por omisión es 16.
- La función de NAT de enmascaramiento sólo da soporte a los protocolos siguientes: TCP, UDP e ICMP.
- Siempre que utilice NAT, debe habilitar el reenvío IP. Utilice el mandato CHGTCPA (Cambiar atributos TCP/IP) para verificar que el reenvío de datagramas IP está establecido en YES.

Consulte el caso práctico y la ilustración presentados en Ocultar las direcciones IP (NAT de enmascaramiento), donde hallará un ejemplo de NAT de enmascaramiento u ocultación.

Función de NAT de enmascaramiento (de correlación de puerto)

La función de NAT con correlación de puerto es una variante de NAT de enmascaramiento. ¿En qué se diferencian? En la primera se puede especificar tanto la dirección IP como el número de puerto que se ha de convertir. Esto permite al PC interno y a la máquina externa iniciar el tráfico IP. Esto sirve en el caso de que la máquina externa (o cliente) desee acceder a máquinas o servidores dentro de la red. Sólo tendrá acceso el tráfico IP que coincida con la dirección IP y el número de puerto. He aquí como funciona:

Inicio interno

En el momento en que el PC interno que tiene la *Dirección 1: Puerto 1* inicia el tráfico hacia una máquina externa, el código de conversión comprobará si en el archivo de reglas de NAT figura la *Dirección 1: Puerto 1*. Si la dirección IP de origen (Dirección 1) y el número de puerto de origen (Puerto 1) coinciden con la regla de NAT, NAT da comienzo a la conversación y lleva a cabo la conversión. Los valores especificados en la regla de NAT sustituyen a la dirección IP de origen y al número de puerto de origen. La *Dirección 1: Puerto 1* es sustituida por la *Dirección 2: Puerto 2*.

Inicio externo

Una máquina externa inicia el tráfico IP utilizando la *Dirección 2* como dirección IP de destino. El número de puerto de destino es el *Puerto 2*. El servidor de NAT deshará la conversión del datagrama con o sin una ″conversación existente″. Dicho de otra manera, NAT creará de forma automática una conversación si no existe una todavía. La *Dirección 2: Puerto 2* pasa a ser la *Dirección 1: Puerto 1*.

En la lista siguiente se destacan las características de NAT de enmascaramiento con correlación de puerto:

- Relación biunívoca.
- El inicio puede tener lugar en la red interna y en la externa.
- La dirección registrada tras la que se oculta la dirección privada debe estar definida en el iSeries que realiza las operaciones de NAT.
- El tráfico IP que está fuera de las operaciones de NAT no puede utilizar la dirección registrada. No obstante, si esta dirección intenta utilizar un número de puerto que coincide con el puerto oculto de la regla de NAT, el tráfico se convertirá. La interfaz quedará inutilizada.
- Normalmente los números de puerto se correlacionan con números de puerto conocidos públicamente, por lo que no se necesita información adicional. Por ejemplo, podría ejecutar un servidor HTTP

enlazado al puerto 5123 y, a continuación, correlacionar éste con la dirección IP pública y el puerto 80. Si desea ocultar un número de puerto interno detrás de otro número de puerto (no común), es necesario indicar físicamente al cliente cuál es el valor del número de puerto de destino. Si no, es difícil que la comunicación tenga lugar.

Atención

- El valor de MAXCON debe ser lo suficientemente alto para dar cabida al número de conversaciones que se desea utilizar. Por ejemplo, si se utiliza FTP, el PC tendrá dos conversaciones activas. Será necesario establecer MAXCON de manera que dé cabida a varias conversaciones para cada PC. El valor por omisión es 128.
- La función de NAT de enmascaramiento sólo da soporte a los protocolos siguientes: TCP, UDP e ICMP.
- Siempre que utilice NAT, debe habilitar el reenvío IP. Utilice el mandato CHGTCPA (Cambiar atributos TCP/IP) para verificar que el reenvío de datagramas IP está establecido en YES.

Filtros IP

Aunque las reglas de paquetes en sí no son un cortafuegos totalmente funcional, proporcionan un sólido componente que puede filtrar los paquetes para el iSeries. Específicamente, el componente de filtros IP de las reglas de paquetes le permite controlar el tráfico IP que desee dejar entrar y salir de la red de su empresa. El filtrado IP le ayudará a proteger su sistema mediante el filtrado de paquetes en función de las reglas que usted especifique. Estas reglas están basadas en la información hallada en la cabecera del paquete IP.

Se pueden aplicar reglas de filtro a varias líneas; también se pueden aplicar varias reglas a una misma línea. Las reglas de filtro están asociadas con líneas, por ejemplo de token-ring (trnline), y no con interfaces lógicas ni direcciones IP. El sistema coteja cada paquete con cada una de las reglas asociadas con una línea. El proceso de cotejo con las reglas es secuencial. Una vez que el sistema encuentra una coincidencia del paquete con una regla, detiene el proceso y aplica la regla coincidente.

Cuando el sistema aplica una regla coincidente, en realidad lleva a cabo la acción que especifica esa regla. El iSeries da soporte a 3 acciones (V4R4 y siguientes):

1. PERMIT — permite que el paquete procese como de costumbre
2. DENY — descarta inmediatamente el paquete
3. IPSEC — envía el paquete mediante una conexión VPN, que usted especifica en la regla de filtro

Nota: en este caso, IPSEC es una acción que se puede definir en las reglas de filtro. Aunque este tema no trata específicamente de IPSec, es importante destacar que los filtros y la red privada virtual (VPN) están estrechamente relacionados. Si desea obtener más información sobre VPN, consulte el tema Red privada virtual (VPN).

Después de aplicar una regla, el sistema reanuda la comparación secuencial de reglas y paquetes y asigna acciones a todas las reglas correspondientes. Si no encuentra una regla coincidente para un paquete concreto, el sistema lo descarta de forma automática. La regla de denegación por omisión del sistema garantiza que el sistema descartará de manera automática cualquier paquete que no coincida con una regla de filtro. Recuerde que si se designa una regla de filtro para permitir el tráfico en sólo una dirección, como la de entrada o salida, el sistema implementa la regla de denegación por omisión en ambas direcciones; es decir, se descartan tanto el paquete de entrada como el de salida.

Sentencias de filtro de ejemplo

El propósito de esta sentencia de filtro de ejemplo es demostrar la sintaxis apropiada para crear reglas de filtro en el iSeries y para ver cómo funcionan juntas en un archivo las distintas sentencias. Utilícelas solo como ejemplo.

Una sentencia de filtro común puede definirse de la manera siguiente:

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = 162.56.39.100
DSTADDR = *   PROTOCOL = *   DSTPORT >= 1024   SRCPORT = 80
```

Este filtro permitirá que entre en la interfaz el tráfico (INBOUND) que tenga una dirección origen de 162.56.39.100, un puerto origen de 80 y un puerto de destino mayor o igual a 1024.

Dado que el tráfico IP generalmente circula tanto INBOUND como OUTBOUND en una conexión, es normal tener dos sentencias relacionadas para permitir el tráfico en ambas direcciones. Estas dos sentencias son duplicados entre sí y figuran en el ejemplo siguiente:

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = 162.56.39.100
DSTADDR = *   PROTOCOL = *   DSTPORT >= 1024   SRCPORT = 80
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = *   DSTADDR =
162.56.39.100   PROTOCOL = *   DSTPORT = 80   SRCPORT >= 1024
```

Observará que ambas sentencias de filtro tienen el mismo nombre de conjunto, TestFilter. Se considera que forman parte del mismo conjunto los filtros que tienen el mismo nombre de conjunto. En un conjunto puede tener tantos filtros como desee. Cuando se activan los filtros de un conjunto dado, se procesan en el orden en que aparecen en el archivo.

Una sentencia de filtro por sí sola no producirá efecto cuando se activen las reglas. Es necesario aplicar el conjunto de filtros a una interfaz de filtros. A continuación figura un ejemplo de cómo aplicar el conjunto, TestFilter, a una interfaz de líneas Ethernet:

```
FILTER_INTERFACE   LINE = ETH237   SET = TestFilter
```

Una vez que active estas reglas, sólo se permitirá en ETH237 el tráfico IP que permita el conjunto TestFilter.

Nota: el sistema añade la regla por omisión DENEGAR TODO EL TRÁFICO al final de los filtros activados de una interfaz. Por lo tanto, cuando aplique reglas a la interfaz mediante la que está configurando el iSeries, es muy importante que habilite su estación de trabajo o la de la persona que esté configurando el iSeries. En caso contrario, se suspenderá la comunicación con el iSeries.

También puede aplicar varios conjuntos a una sentencia de interfaz de filtro de la manera siguiente:

```
FILTER_INTERFACE   LINE = ETH237   SET = set1, set2, set3
```

Estos conjuntos se procesarán en el mismo orden en que los vaya poniendo en la sentencia de interfaz de filtro (set1, set2, y finalmente, set3). Recuerde que los filtros contenidos en cada conjunto se procesan en el orden en que aparecen en el archivo. Esto significa que el orden de los filtros entre conjuntos diferentes es irrelevante. El orden de los filtros sólo es importante cuando los filtros están en el mismo conjunto.

Cabecera de paquete IP

Se pueden crear reglas de filtro que hagan referencia a las diversas partes de las cabeceras IP, TCP, UDP e ICMP. En la lista siguiente se incluyen los campos a los que se hace referencia en una regla de filtro que compone la cabecera de paquete IP:

- Dirección IP de origen
- Protocolo (por ejemplo, TCP, UDP)
- Dirección IP de destino
- Puerto origen
- Puerto de destino
- Sentido del datagrama IP (de entrada, de salida o ambos)
- Bit SYN TCP

Por ejemplo, puede crear y activar una regla que filtre un paquete tomando como base la dirección IP de destino, la de origen y el sentido (de entrada). En este caso, el sistema empareja todos los paquetes de entrada (en función de las direcciones de origen y de destino) con las reglas correspondientes. A continuación, emprende la acción especificada en la regla. Descartará cualquier paquete que *no* esté permitido en las reglas de filtro. Esta actuación recibe el nombre de regla de denegación por omisión.

Nota: el sistema aplica la regla de denegación por omisión a los programas sólo si la interfaz física tiene activa por lo menos una regla. Esta regla puede ser definida por el cliente o generada por iSeries Navigator. Sin tener en cuenta si la regla de filtro permite el tráfico de entrada o el de salida, el sistema implementa la regla de denegación por omisión en ambas direcciones. Si en la interfaz física no existe una regla de filtro activa, la regla de denegación por omisión no funcionará.

Organizar las reglas de NAT con las reglas de filtro IP

NAT y los filtros IP funcionan de manera independiente. A pesar de ello, es posible utilizar NAT junto con filtros IP. Si opta por aplicar sólo reglas de NAT, el sistema efectuará únicamente la conversión de direcciones. De modo parecido, si opta por aplicar sólo reglas de filtro IP, el sistema sólo filtrará el tráfico IP. No obstante, si aplica ambos tipos de reglas, el sistema convertirá y filtrará las direcciones. Cuando se utiliza NAT y filtros juntos, las reglas actúan siguiendo un orden concreto. En el caso del tráfico de entrada, primero se procesan las reglas de NAT. En el caso del tráfico de salida, primero se procesan las reglas de filtro.

Tal vez le interese estudiar la posibilidad de utilizar archivos aparte para crear las reglas de NAT y las de filtro. Aunque no sea necesario, con ello se simplifica la lectura y la resolución de problemas de las reglas de filtro. De cualquier manera (tanto si las reglas están en un mismo archivo como en archivos aparte), se reciben los mismos errores. Si decide utilizar archivos aparte para las reglas de NAT y las de filtro, igualmente podrá activar ambos conjuntos de reglas. Sin embargo, deberá asegurarse de que las reglas no se estorban entre sí.

Para activar a la vez las reglas de NAT y las de filtro, es necesario utilizar la función de *inclusión*. Supongamos, por ejemplo, que ha creado el Archivo A para las reglas de filtro y el Archivo B para las reglas de NAT. Puede incluir el contenido del Archivo B en el Archivo A sin reescribir todas las reglas. En Incluir archivos en las reglas de paquetes hallará más información sobre cómo hacerlo.

Organizar varias reglas de filtro IP

Al crear reglas de filtro, un filtro hace referencia a una sentencia de regla. Un conjunto hace referencia a un grupo de filtros. Los filtros, dentro de un conjunto, se procesan en orden físico de arriba abajo. De igual modo, varios conjuntos se procesan en orden físico dentro de una sentencia FILTER_INTERFACE.

A continuación figura un ejemplo en el que un conjunto contiene tres sentencias de filtro. Cada vez que se haga referencia a este conjunto, se incluirán las tres reglas. Normalmente es más sencillo incluir todas las reglas de filtro en un conjunto.

```
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = * FRAGMENTS  %
        = HEADERS JRN = FULL
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP DSTPORT = * SRCPORT = * FRAGMENTS = NONE  %
        JRN = OFF
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS = NONE JRN  %
        = OFF
FILTER_INTERFACE LINE = ETHLINE SET = all
###Línea Ethernet ETHLINE
```

Protección contra la usurpación

La usurpación se produce cuando alguien intenta acceder a su sistema pretendiendo ser un sistema de confianza de su propia red. Es una buena idea proteger contra este tipo de ataque a las interfaces que estén enlazadas con una red pública. Puede protegerse contra la usurpación completando el asistente Protección contra la usurpación, que está disponible en el Editor de reglas de paquetes de iSeries Navigator. Este asistente le ayudará a asignar reglas a las interfaces vulnerables. Una vez que las reglas estén activas, cualquier sistema de la red pública (que no es de confianza) no podrá actuar como una máquina de confianza desde una red privada (de confianza).

Capítulo 5. Planificar reglas de paquetes

Para conectar a Internet alguno de sus recursos de red, debería elaborar un plan de seguridad y comprender los riesgos potenciales de seguridad que implica. En general, es necesario que reúna información detallada sobre cómo tiene previsto utilizar Internet, así como un documento que describa su configuración de red interna. En base a los resultados obtenidos, podrá evaluar correctamente sus necesidades de seguridad. El tema IBM SecureWay: iSeries e Internet le proporcionará los detalles que necesita para crear un plan total de seguridad de red. Si parte de su plan incluye la utilización de reglas de paquetes, le recomendamos que consulte los temas que figuran a continuación a fin de reunir toda la información necesaria para empezar a configurarlas:

- **Reglas de paquete: requisitos de autorización de usuario**
  Asegúrese de que tiene las autorizaciones apropiadas para administrar las reglas de paquetes.
- **Reglas de paquete: requisitos del sistema**
  Asegúrese de que su iSeries satisface los requisitos mínimos del sistema para trabajar con reglas de paquetes.
- **Reglas de paquete: planificación de hoja de trabajo**
  Esta hoja de trabajo le ayudará a reunir la información que necesita para empezar a configurar las reglas de paquetes.

Después de elaborar un plan, podrá empezar a configurar las reglas de paquetes.

Reglas de paquete: requisitos de autorización de usuario

Para poder administrar reglas de paquetes en iSeries, es preciso que se asegure de que tiene las autorizaciones apropiadas. Debe tener la autorización especial *IOSYSCFG en su perfil de usuario. Si tiene previsto administrar reglas de paquetes desde el ID de usuario QSECOFR, o desde un ID de usuario de tipo *SECOFR, o tiene la autorización *ALLOBJ, esto será suficiente. Si no es así, necesitará autorización sobre los directorios, archivos e ID de usuario QSYS que figuran a continuación:

1. Añadir la autorización sobre objeto, `*RXW`, y la autorización sobre datos, `OBJMGT`, en estos tres archivos:
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.i3p`
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.txt`
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.tcpipml`
2. Añadir la autorización sobre objeto, `*RWX`, en los directorios siguientes:
   `/QIBM/UserData/OS400/TCPIP/PacketRules`
   `/QIBM/UserData/OS400/TCPIP/OpNavRules`
3. Añadir la autorización sobre objeto, `*RWX`, en los archivos siguientes:
   `/QIBM/UserData/OS400/TCPIP/OpNavRules/VPNPolicyFilters.i3p`
   `/QIBM/UserData/OS400/TCPIP/OpNavRulesPPPFilters.i3p`
4. También necesitará la autorización `ADD` sobre el perfil QSYS, ya que QSYS posee los archivos de reglas que se acaban de crear.

Estos son los directorios y archivos por omisión que utiliza el editor de reglas de paquetes. Si opta por almacenar sus archivos en directorios distintos a los que figuran más arriba, necesitará una autorización sobre esos directorios.

Reglas de paquete: requisitos del sistema

Para que las reglas de paquetes funcionen adecuadamente en iSeries, es necesario contar con los elementos siguientes:

1. OS/400 Versión 5 Release 2 (5722-SS1), o una versión más reciente.
2. iSeries Access para Windows (5722-XE1) e iSeries Navigator
   - Componente de red de iSeries Navigator

3. TCP/IP (5722-TC1) tiene que estar configurado, incluyendo las interfaces IP, las rutas, el nombre de sistema principal local y el nombre de dominio local.

Nota: Si no entiende algún concepto sobre TCP/IP, redes o direcciones IP, consulte TCP/IP Tutorial and Technical Overview y V4 TCP/IP for AS/400: More Cool Things Than Ever .

Reglas de paquete: planificación de hoja de trabajo

La hoja de trabajo de planificación de reglas de paquetes le ayudará a reunir información detallada acerca de su plan de utilización de reglas de paquetes. Esta información es necesaria para poder concretar las necesidades de seguridad. También puede utilizarse esta información para configurar las reglas de paquetes. Para configurar reglas de paquetes en su sistema, deberá primero contestar las preguntas que figuran a continuación.

Esta información es necesaria para crear un plan de utilización de reglas de paquetes	**Respuestas**
¿Cuál es el diseño de su red y de sus conexiones? Muéstrelo en un plano.	
¿Qué direccionadores y direcciones IP va a utilizar?	
¿Qué reglas va a utilizar para controlar el tráfico TCP/IP que pasa por los sistemas? Para cada regla que liste, especifique los aspectos de flujo de tráfico TCP/IP que figuran a continuación: • el tipo de servicio que desea permitir o denegar (por ejemplo, HTTP, FTP, etc.) • el número de puerto conocido públicamente correspondiente a dicho servicio • el sentido en el que circula el tráfico • si el tráfico es de respuesta o de inicio • las direcciones IP del tráfico (origen y destino)	
¿Qué direcciones IP desea correlacionar con otras direcciones o bien ocultar detrás de otras direcciones? (Esta lista es necesaria sólo si se está utilizando la conversión de direcciones de red).	

Capítulo 6. Configurar reglas de paquetes

Cuando haya creado un plan para configurar las reglas de paquetes en el sistema, estará en disposición de empezar realmente a crearlas y aplicarlas. Hallará información específica, paso a paso, en el Editor de reglas de paquetes de la ayuda en línea. Sin embargo, la lista de comprobación que aparece a continuación, proporciona una visión general de las tareas que es preciso realizar a fin de garantizar que las reglas funcionen apropiadamente al activarlas:

__ 1. Acceda al Editor de reglas de paquetes.
Siga estas instrucciones para acceder al Editor de reglas de paquetes en iSeries Navigator.

__ 2. Utilice los asistentes que forman parte del Editor de reglas de paquetes (V5R2 y versiones más recientes) para crear los archivos de reglas:

- Asistente **Permitir un servicio**
  Este asistente genera e inserta un conjunto de sentencias de reglas de paquetes que permitirán el tráfico necesario para un servicio TCP o UDP determinado.
- Asistente **Protección contra la usurpación**
  Este asistente genera e inserta un conjunto de sentencias de reglas de paquetes que denegarán cualquier tráfico en una interfaz que sólo debiera entrar a este servidor a través de otra interfaz.
- Asistente **Conversión de direcciones**
  Este asistente genera e inserta un conjunto de sentencias de reglas de paquetes para correlacionar o para ocultar.

Dependiendo del tipo de reglas que desee configurar, estos asistentes crean automáticamente todas las sentencias de filtro y de NAT necesarias. Puede acceder a los asistentes desde el menú **Asistentes** del Editor de reglas de paquetes. Si prefiere escribir las reglas usted, continúe hasta llegar al próximo elemento de la lista de comprobación.

__ 3. Definir direcciones y servicios
Cree los alias de las direcciones y los servicios para los que tiene previsto crear varias reglas.

Nota: *deberá* definir direcciones si desea crear reglas de NAT.

__ 4. Crear reglas de NAT.
Realice esta tarea *sólo* si tiene previsto utilizar NAT.

__ 5. Crear reglas de filtro.
Defina qué filtros desea aplicar a la red que administra este sistema.

__ 6. Incluir archivos
Especifique los archivos adicionales que desee incluir en el archivo de reglas ″original″. Realice esta tarea *sólo* si tiene archivos de reglas que desee reutilizar en un archivo de reglas nuevo.

__ 7. Definir las interfaces
Aplique las reglas a una interfaz.

__ 8. Hacer comentarios
Describa qué función realiza cada archivo de reglas.

__ 9. Verificar los archivos de reglas
Asegúrese de que las reglas se activarán sin errores ni problemas.

__ 10. Activar el archivo de reglas.
Las reglas de paquetes deben activarse para que puedan funcionar.

__ 11. Gestionar reglas de paquetes
Una vez que haya activado las reglas de paquetes, deberá gestionarlas periódicamente a fin de mantener la seguridad del sistema. Este tema incluye información acerca de cómo editar reglas de paquetes, registrar por diario y auditar acciones de reglas de paquetes, y consejos y técnicas para las copias de seguridad y la recuperación.

Acceder a las reglas de paquetes

Al Editor de reglas de paquetes se accede mediante iSeries Navigator, la interfaz gráfica que permite trabajar con los recursos de iSeries. Utilice el Editor de reglas de paquetes para empezar a crear reglas de paquetes en el sistema. Puede crear un archivo nuevo, editar un archivo existente, o trabajar con los archivos de ejemplo que se facilitan en el sistema.

Para acceder al Editor de reglas de paquetes, siga estos pasos:
1. En iSeries Navigator, expanda su servidor -->**Red -->Políticas IP**.
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.

Utilice la ayuda en línea para obtener instrucciones paso a paso sobre cómo realizar las tareas descritas en la sección Configurar reglas de paquetes, incluida en este tema.

Definir direcciones y servicios

Cuando se crean reglas de paquetes, es preciso especificar las direcciones IP y los servicios a los que desea aplicar las reglas. Las **direcciones definidas** son especificaciones de interfaz a las que se han dado nombres simbólicos. Las direcciones deben definirse cuando la dirección que se desea representar es un rango de direcciones, una subnet, una lista de identificadores punto a punto, o una lista de direcciones que no sean contiguas. Una sentencia de dirección definida es necesaria cuando se tiene previsto crear reglas de conversión de direcciones para correlacionar. Si la dirección que desea representar es una dirección IP única en una sentencia de filtro, no será necesaria la sentencia de dirección definida. Los **alias de servicios** permiten definir servicios y después reutilizarlos en tantos filtros como desee. Los alias de servicios también mantienen un seguimiento de las finalidades de las distintas definiciones de servicios.

La definición de direcciones y de alias de servicios simplifica la creación de reglas de paquetes. Cuando cree las reglas, haga referencia al apodo de las direcciones o al alias de los servicios en lugar de a los detalles concretos de las direcciones o los servicios. La utilización de apodos y alias en las reglas de filtro ofrece dos ventajas:

1. Minimiza el riesgo de cometer errores tipográficos.
2. Minimiza el número de reglas de filtro que es necesario crear.

Supongamos, por ejemplo, que en la red hay 31 usuarios que necesitan tener acceso a Internet. Sin embargo, desea que estos usuarios tengan únicamente acceso Web. En esta situación, tiene dos opciones en cuanto a la manera de crear las reglas de filtro necesarias:

1. Definir una regla de filtro para la dirección IP de cada uno de los usuarios.
2. Crear, definiendo una dirección, un apodo para todo el conjunto de direcciones que representa a los usuarios.

Con la primera opción, aumentan las probabilidades de cometer errores tipográficos, así como el grado de mantenimiento que se debe efectuar en el archivo de reglas. Si se utiliza la segunda opción, tan sólo es necesario crear dos reglas de filtro. Basta con utilizar un apodo en cada regla para hacer referencia a la totalidad del conjunto de direcciones al que se aplica la regla.

También se pueden crear apodos para los servicios y utilizarlos de la misma forma que los apodos de las direcciones. Los alias de los servicios definen los criterios TCP, UDP e ICMP que se desea seleccionar. Se selecciona el puerto de origen y el de destino que se desea utilizar.

Nota: recuerde que *debe* definir direcciones si tiene previsto utilizar reglas de NAT. Las reglas de NAT señalan únicamente a una dirección definida.

Para obtener instrucciones paso a paso sobre cómo definir direcciones, alias de servicios y servicios ICMP, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Si tiene previsto utilizar la conversión de direcciones de red, prosiga hasta crear reglas de NAT. De lo contrario, vaya a crear reglas de filtro IP para filtrar el tráfico IP que entra y sale de la red.

Crear reglas de NAT

Si llega a la conclusión de que es necesario utilizar NAT, *deberá* definir apodos para las direcciones IP que tiene previsto utilizar. No puede crear reglas de NAT con la notación estándar de direcciones de 32 bits. En lugar de especificar una dirección real como 193.112.14.90, debe hacer referencia a 193.112.14.90 por medio de un *nombre*. El sistema asociará el nombre que usted defina con las direcciones correspondientes y lo convertirá según convenga. Por lo tanto, debe definir las direcciones para que el sistema pueda aplicarles reglas de NAT.

El Editor de reglas de paquetes permite crear dos tipos de reglas de NAT. Uno de ellos permite ocultar las direcciones, mientras que el otro permite correlacionarlas.

Ocultar direcciones
Se debe optar por esta posibilidad si se desea que las direcciones privadas queden ocultas para los demás. Las reglas de direcciones ocultas permiten ocultar varias direcciones internas detrás de una única dirección IP pública. Este tipo de NAT también se conoce como NAT de *enmascaramiento*.

Correlacionar direcciones

Se recomienda correlacionar direcciones cuando se desee direccionar el tráfico procedente de una única dirección IP pública a una única dirección interna. Este tipo de NAT también se conoce como NAT *estática*.

Para obtener instrucciones paso a paso sobre cómo ocultar o correlacionar direcciones, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Si tiene previsto filtrar el tráfico que circula hacia dentro y hacia afuera de la red, vaya a Crear reglas de filtro IP. De lo contrario, continúe hasta Hacer comentarios en reglas de paquetes.

Crear reglas de filtro IP

Cuando se crea un filtro, se especifica una regla que rige el tráfico IP que circula hacia dentro y hacia afuera del sistema. Las reglas que se definen especifican si el sistema debe permitir o denegar el acceso a los paquetes que intentan acceder al sistema. El sistema dirige los paquetes IP tomando como base el tipo de información que figura en las cabeceras de los mismos. También los dirige a la acción que tenga especificado que se debe aplicar. Asimismo, descarta cualquier paquete que no coincida con una regla concreta. Esta regla de descartar automáticamente se denomina *regla de denegación por omisión*. La regla de denegación por omisión, que se encuentra al final del archivo, se activa automáticamente cada vez que un paquete no coincide con el criterio de las reglas anteriores. Para que la regla de denegación por omisión esté activa, debe haber como mínimo una regla de filtro activada.

Nota: cuando aplique reglas a una interfaz mediante la que está configurando el iSeries, es muy importante que habilite su estación de trabajo o la de la persona que esté configurando el iSeries. En caso contrario, se suspenderá la comunicación con el iSeries. Si ocurre esto, deberá iniciar la sesión en iSeries utilizando una interfaz que todavía tenga conectividad, como es la consola de operadores. Utilice el mandato RMVTCPTBL para eliminar todos los filtros del sistema.

Para poder crear las reglas de filtro, debe determinar si es necesario utilizar la conversión de direcciones de red (NAT). Si utiliza reglas de NAT, *debe* definir direcciones y servicios. NAT es la única función que

requiere una dirección definida, pero puede utilizarse también para otras funciones. Si define las direcciones y los servicios, puede reducir el número de reglas que deben definirse, así como la posibilidad de cometer errores tipográficos.

He aquí otras maneras de minimizar los errores y maximizar el grado de eficiencia a la hora de crear reglas de filtro:

- **Defina las reglas de filtro de una en una**. Por ejemplo, cree todos los permisos para Telnet a la vez. Así podrá agrupar las reglas cada vez que haga referencia a ellas.
- **Las reglas de filtro se procesan en el mismo orden en que figuran en el archivo**. A medida que cree las reglas, colóquelas en el orden en que tenga pensado que se apliquen. Si el orden es incorrecto, el sistema será vulnerable a un ataque ya que los paquetes no se procesarán de la manera que tenía prevista. Para simplificar la cuestión, tome en consideración las siguientes acciones voluntarias:
  1. Coloque los nombres de los conjuntos de filtro dentro de la sentencia FILTER_INTERFACE en el mismo orden exacto en el que están definidos físicamente en el archivo.
  2. Coloque todas las reglas de filtro en un solo conjunto para evitar problemas con el orden de los conjuntos.
- **Verifique la sintaxis de cada una de las reglas a medida que avance**. Es más fácil y rápido que depurarlas todas a la vez.
- **Cree nombres de conjunto para los grupos de archivos que estén asociados lógicamente entre sí**. Esto es importante porque sólo puede haber activo un archivo de reglas en todo momento. Vea el ejemplo dado más abajo.
- **Escriba reglas de filtro sólo para los datagramas que desee permitir**. Todo lo demás quedará descartado por la regla de denegación automática.
- **Escriba primero las reglas que correspondan al tráfico intenso**.

Ejemplo: lea el consejo *Cree nombres de conjunto* anterior. Tal vez le interese dar acceso Telnet a varios usuarios internos, pero no a todos ellos. Para gestionar con mayor facilidad estas reglas, puede asignar a cada una de ellas `TelnetOK` como nombre de conjunto. Un segundo criterio puede permitir Telnet a través de una interfaz concreta y bloquear el tráfico Telnet procedente de las demás. En este caso, es necesario crear un segundo conjunto de reglas que bloqueen por completo el acceso Telnet. Puede asignar a estas reglas `TelnetNever` como nombre de conjunto. La creación de nombres de conjunto hace que resulte más fácil reconocer la finalidad de la regla. También es más sencillo determinar cuáles son las interfaces a las que desea que se apliquen los conjuntos en concreto. Siga todos los consejos anteriores para simplificar el proceso de creación de filtros.

Para obtener instrucciones paso a paso sobre cómo crear reglas de filtro IP, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Cuando haya creado los filtros, es posible que desee considerar la inclusión de un archivo o de varios archivos en la sentencia de filtro. Si no es así, el paso siguiente consistirá en definir las interfaces a las que se aplican las reglas.

Definir interfaces de filtro IP

Se *deben* definir interfaces de filtro para establecer cuáles son las reglas de filtro que se desea que aplique el sistema y a qué interfaces. Para poder definir interfaces de filtro, primero es necesario crear los filtros que se tiene pensado que el sistema aplique a las diversas interfaces. Si se opta por definir las direcciones (cuando se definen las interfaces), se hará referencia a las mismas por su nombre. Si se opta por *no* definir las direcciones (cuando se definen las interfaces), se hará referencia a las mismas por la dirección IP.

Al crear filtros, puede incluir varios filtros en un conjunto. A continuación, añade el conjunto a una sentencia FILTER_INTERFACE. El nombre de conjunto utilizado en la sentencia debe ser uno que haya usted definido en una sentencia de filtro. Por ejemplo, si tiene el nombre de conjunto `ALL`, y todos sus filtros están en ese conjunto, debe incluir el nombre de conjunto `ALL` en la sentencia de interfaz de filtros para que los filtros funcionen adecuadamente. No sólo puede tener varios filtros en un conjunto, sino que también puede tener varios conjuntos en una sentencia FILTER_INTERFACE.

Para definir las interfaces, debe incluir los archivos adicionales que desee utilizar. A continuación, ya puede definir las interfaces. Recuerde que los conjuntos de filtros se aplican en el mismo orden en que están especificados en la sentencia FILTER_INTERFACE. Así pues, las reglas de filtro deben figurar en la sentencia FILTER_INTERFACE en el mismo orden exacto en el que los conjuntos están definidos físicamente en el archivo.

Para obtener instrucciones paso a paso sobre cómo definir una interfaz de filtro, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Una vez definidas las interfaces de filtro, el paso siguiente es hacer comentarios en las reglas de paquetes.

Incluir archivos en reglas de paquetes

Se puede activar más de un archivo de reglas de paquetes en el sistema utilizando la función *Incluir* del Editor de reglas de paquetes. La utilización de varios archivos hace que resulte mucho más fácil trabajar con las reglas, sobre todo si se precisa un número elevado de ellas para controlar el tráfico en varias interfaces. Por ejemplo, podría interesarle utilizar un grupo de reglas en varias interfaces.

Puede crear este grupo dentro de un archivo individual. En lugar de volver a escribir las reglas cada vez que desee utilizarlas en otros archivos, puede incluirlas en el archivo maestro. El archivo maestro es el único archivo que puede haber activo en todo momento. Basta con utilizar la función de inclusión para añadirlas al archivo maestro.

A la hora de crear archivos de inclusión, quizás le interese tener separadas las reglas de NAT correspondientes a una interfaz de las reglas de filtro de dicha interfaz. Sin embargo, sólo puede haber un único archivo activo en todo momento.

Cuando vaya a crear un archivo nuevo de reglas, puede incluir como parte del mismo cualquier archivo ya existente. Para ello, primero debe crear las nuevas reglas de filtro que desea utilizar. Siempre que cree reglas, debe archivarlas (agruparlas) por tipo. Así no tendrá que volver a crear reglas que haya utilizado con anterioridad. Bastará con que las incluya o elimine según convenga.

Para obtener instrucciones paso a paso sobre cómo incluir un archivo en las reglas, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Una vez incluidos todos los archivos adicionales de reglas que desee utilizar, el paso siguiente es definir las interfaces de filtro IP.

Hacer comentarios en reglas de paquetes

Poner comentarios en los archivos de reglas es muy importante. Interesa dejar constancia de cómo se espera que funcionen las reglas. Por ejemplo, interesa dejar constancia de qué es lo que una determinada regla permite o deniega. Este tipo de información le ahorrará mucho tiempo en el futuro. Si alguna vez ha de reparar con rapidez una filtración de información confidencial, necesitará los comentarios para refrescar su memoria. Tal vez no disponga de tiempo para desentrañar el significado de las reglas, así que ponga comentarios en abundancia.

En cada uno de los diálogos asociados con la creación y la activación de las reglas de paquetes hay un campo **Descripción**. Éste es el campo que está reservado para los comentarios. El sistema hace caso omiso de lo que se escriba en este campo. Puede interesarle el utilizar el campo de comentarios en cada uno de los pasos del proceso de creación de reglas. Con ello puede reducir las probabilidades de olvidarse de poner un comentario significativo. Es mejor poner comentarios cuando aún se tiene fresco en la memoria el proceso al que se refieren. No obstante, también se puede esperar hasta que se haya acabado de crear todas las reglas.

Para obtener instrucciones paso a paso sobre cómo hacer comentarios en un archivo de reglas, utilice el Editor de reglas de paquetes de la ayuda en línea.

Paso siguiente
Una vez realizados los pasos (anteriores a este) para la configuración de reglas de paquetes, el paso siguiente será salvar y verificar las reglas de paquetes. .

Verificar reglas de paquetes

Las reglas deben verificarse siempre antes de activarlas. Esto ayuda a garantizar que las reglas se activarán sin problemas. Cuando se verifican las reglas de paquetes, el sistema las comprueba para ver si existen errores sintácticos y semánticos e informa de los resultados mediante una ventana de mensaje situada en la parte inferior del Editor de reglas de paquetes. Para los mensajes de error que estén asociados con un archivo y un número de línea específicos, puede pulsar con el botón derecho del ratón sobre el error y seleccionar **Ir a línea** para resaltar el error en el archivo que esté editando.

Para utilizar la función de verificación, es probable que desee visualizar las reglas de paquetes para comprobar si existen errores visibles. No pueden activarse las reglas que contengan errores sintácticos. La función de verificación comprueba si existen errores de naturaleza sintáctica. El sistema no puede verificar si las reglas están ordenadas correctamente. Debe comprobarse manualmente si el orden de las reglas es correcto. Las reglas de paquetes dependen de un orden, lo que significa que debe poner las reglas en el orden en que desee que se apliquen. Si las ordena de forma incorrecta, no obtendrá el resultado previsto. Antes de activar las reglas, asegúrese de que son correctas y de que están colocadas en el orden en que desea que se apliquen.

Para obtener instrucciones paso a paso sobre cómo verificar reglas de paquetes, utilice el Editor de reglas de paquetes de la ayuda en línea.

Mensajes de aviso: cada vez que active las reglas de filtro, el sistema las verificará de manera automática. Pueden generarse diversos mensajes de error y de aviso. Los mensajes de aviso son simplemente informativos y no detienen el proceso de verificación. Lea detenidamente todos los mensajes. Aparecerá uno en el que se dice que la verificación o la activación ha sido satisfactoria. Este último mensaje también podría indicar que la regla no se ha cargado satisfactoriamente si hay errores graves.

Paso siguiente
Cuando se hayan verificado satisfactoriamente las reglas, el paso siguiente será activarlas.

Activar reglas de paquetes

Activar las reglas de paquetes creadas es el último paso en la configuración de las reglas de paquetes. Para que funcionen las reglas que ha creado, debe activarlas o cargarlas. Sin embargo, antes de activar las reglas es necesario verificar que son correctas. Intente siempre resolver los problemas que haya antes de activar las reglas de paquetes. Si activa reglas que tienen errores o que no están colocadas en el orden correcto, el sistema estará en una situación de riesgo. El sistema cuenta con una función de verificación a la que se llama de manera automática cada vez que se activan las reglas. Dado que esta función automática comprueba únicamente si existen errores sintácticos de envergadura, no debe fiarse solamente de ella. Compruebe siempre manualmente si también existen errores en los archivos de reglas.

Si las reglas de filtro no se aplican a una interfaz (por ejemplo, si sólo se utilizan reglas de NAT y no de filtro), aparecerá un aviso (TCP5AFC). No se trata de un error. Tan sólo verifica que utilizar una interfaz es necesario y que es lo que usted tiene previsto. Fíjese siempre en el último mensaje. Si en él se dice que la activación es satisfactoria, entonces los mensajes que le preceden son todos ellos avisos.

Nota: si se activan reglas nuevas en todas las interfaces, estas sustituirán a todas las reglas anteriores en todas las interfaces físicas. Aunque una interfaz física no se mencione en las reglas nuevas, será sustituida. Sin embargo, si se elige activar las reglas nuevas en una interfaz específica, las reglas sólo sustituirán a las reglas de esa interfaz en concreto. Las reglas existentes en las demás interfaces no se tocarán.

Último paso

Una vez que se han configurado las reglas de paquetes y se han activado satisfactoriamente, es posible que necesite gestionarlas periódicamente a fin de garantizar la seguridad del sistema. Consulte la sección Gestionar reglas de paquetes incluida en este tema, si desea examinar una lista de tareas que puede realizar para mantener y gestionar adecuadamente las reglas de paquetes.

Capítulo 7. Gestionar reglas de paquetes

Para mantener la seguridad de su sistema y la integridad de sus reglas de paquetes, es recomendable realizar periódicamente las tareas de gestión siguientes:

Nota: hallará las instrucciones específicas, paso a paso, para realizar estas tareas en el Editor de reglas de paquetes de la ayuda en línea, a menos que se especifique otra cosa.

- Crear una copia de seguridad de las reglas de paquetes para estar a cubierto de una pérdida de archivos.
- Desactivar las reglas de paquetes cuando sea necesario detener las reglas de NAT y las de filtro por cualquier motivo. Recuerde, no obstante, que si desactiva las reglas, la red quedará desprotegida.
- Editar las reglas de paquetes cuando sea necesario cambiar la manera en que el tráfico IP circula hacia dentro y hacia afuera del sistema.
- Registrar por diario y auditar las acciones de reglas de paquetes para anotar las reglas de paquetes. Esto sirve de ayuda para depurar las reglas, en caso de que sea necesario.
- Ver las reglas de paquetes cuando sea necesario resolver errores.

Debe emplear todos los medios a su alcance para gestionar con eficiencia y eficacia las reglas de paquetes. La seguridad del sistema depende de que las reglas sean precisas y estén actualizadas. Si necesita ayuda en la resolución de problemas, consulte Resolver problemas de las reglas de paquetes.

Desactivar reglas de paquetes

Si tiene que modificar las reglas de paquetes activas, o desea activar reglas nuevas, primero debe desactivar las reglas que estén activas actualmente. Puede optar por desactivar reglas de una interfaz específica, en un identificador punto a punto, o en todas las interfaces y todos los identificadores punto a punto.

Para obtener instrucciones paso a paso sobre cómo desactivar reglas de paquetes, utilice el Editor de reglas de paquetes de la ayuda en línea.

Ver las reglas de paquetes

Es necesario ver las reglas de filtro antes de activarlas, a fin de verificar que son correctas. Ver las reglas de filtro creadas permite comprobar si existen errores visibles. Puede interesarle ver las reglas de filtro no sólo antes de proceder a activarlas y a probarlas sino antes de imprimirlas y crear una copia de seguridad de ellas. El ver las reglas no es la única manera que existe de comprobar si hay errores. No obstante, es una forma útil de minimizar o eliminar los errores antes de realizar pruebas.

Para poder revisar las reglas de filtro, imprima el archivo de reglas que ha creado. Esto le permitirá detectar las equivocaciones visibles y verificar que ha incluido todos los archivos de reglas creados con anterioridad que deseaba añadir.

El sistema cuenta también con una función de verificación, pero no debe basarse exclusivamente en ella. Debe tomar las medidas oportunas para corregir todos los errores manualmente. Con ello ahorrará tiempo y recursos.

Para ver las reglas inactivas, es necesario abrir el archivo de reglas del Editor de reglas de paquetes.

Si desea editar las reglas de filtro activas, primero debe verlas para determinar cómo desea modificarlas.

Para ver las reglas activas actualmente, siga estos pasos:

1. En iSeries Navigator, seleccione **su servidor ––> red ––> políticas IP ––> reglas de paquetes**.

2. Seleccione la interfaz de las reglas de paquetes activas que desea ver.
3. Visualice la lista de reglas de paquetes activas en el panel derecho.

Nota: no se pueden editar las reglas desde este diálogo. Debe desactivar el archivo de reglas y después utilizar el Editor de reglas de paquetes para editar las reglas.

Vuelva a Administración de NAT y de filtros IP.

Editar las reglas de paquetes

A medida que vayan cambiando las necesidades de seguridad de la red, *debe* editar las reglas para garantizar que responden a la nueva estrategia de seguridad. Sin embargo, para poder editar las reglas de paquetes activas, primero es necesario desactivarlas. Una vez desactivadas, utilice el Editor de reglas de paquetes de iSeries Navigator para realizar las modificaciones necesarias en las reglas. Recuerde que debe verificar y luego reactivar las reglas cuando haya terminado de editarlas.

Para obtener instrucciones paso a paso sobre cómo editar reglas de paquetes, utilice el Editor de reglas de paquetes de la ayuda en línea.

Crear una copia de seguridad de las reglas de paquetes

En principio puede parecer que no resulta necesario, pero crear una copia de seguridad de las reglas de paquetes siempre es una buena idea. En caso de producirse una pérdida, las copias de seguridad ahorran el tiempo y el esfuerzo que sería necesario invertir para volver a crear los archivos partiendo de cero.

Estos consejos de carácter general pueden servirle para asegurarse de que cuenta con una forma fácil de reemplazar los archivos perdidos:

Imprima las reglas de filtro
Podrá guardar los impresos allí donde estén más seguros y volver a entrar la información según convenga. Los impresos resultan también útiles si es necesario buscar un error en una regla de filtro.

Para obtener instrucciones paso a paso sobre imprimir reglas de paquetes, utilice el Editor de reglas de paquetes de la ayuda en línea.

Copie la información en un disco
La copia en disco ofrece una ventaja sobre los impresos: en lugar de tener que volver a entrar la información manualmente, ésta existe en formato electrónico. Constituye un método directo de transportar información de una fuente en línea a otra.

Nota: El iSeries copia la información en el disco del sistema, no en un disquete. Los archivos de reglas se almacenan en el sistema de archivos IFS dentro del iSeries, no en un PC. Tal vez le interese emplear un método de protección de disco como medio de proteger los datos almacenados en el disco del sistema.

Si se utiliza un iSeries, debe planificarse una estrategia de copia de seguridad y recuperación. En Copia de seguridad y recuperación hallará más información sobre la recuperación y las copias de seguridad de los archivos.

Registrar por diario y auditar las acciones de las reglas de paquetes

Las reglas de paquetes incluyen una función de registro por diario. El registro por diario permite resolver problemas de NAT y de filtros. Puede utilizarlo para crear un archivo de anotaciones de las acciones de las reglas. Esto le permitirá depurar y revisar las reglas con más facilidad. Consultando estos diarios o anotaciones del sistema, también podrá auditar el tráfico que circula hacia dentro y hacia afuera del sistema.

La función de registro por diario se utiliza de manera individualizada para cada regla. A la hora de crear una regla de NAT o de filtro, las opciones de registro por diario son las siguientes: FULL y OFF. En la tabla que figura a continuación hallará información más detallada.

OPCIÓN	DEFINICIÓN
FULL	Se anotan todos y cada uno de los paquetes convertidos.
OFF	No se realiza registro por diario alguno.

Si el registro por diario está activo, se generará una entrada de diario para cada regla que se aplique a un datagrama (de NAT o de filtro). Las únicas reglas para las que no se crea una entrada de diario son las de denegación por omisión. Estas no quedan nunca registradas por diario porque las crea el sistema.

Al utilizar estos diarios, se crea un archivo general en el iSeries. La información que consta en los diarios del sistema sirve para determinar cómo se utiliza el sistema. Esto puede servir de ayuda a la hora de decidirse a cambiar los diversos aspectos del plan de seguridad.

Si la función de registro por diario está establecida en OFF, el sistema no creará una entrada de diario para la regla. Aunque se puede elegir esta opción, puede que no resulte ser la mejor. Si no tiene experiencia en la creación de reglas de NAT y de filtro, le interesa utilizar FULL (anotaciones) según convenga. De este modo, podrá utilizar los archivos de anotaciones como herramientas de resolución de problemas. No obstante, debe ser selectivo con lo que decide registrar por diario. El registro por diario supone una carga pesada para los recursos del sistema. Procure concentrase en las reglas que controlan el tráfico intenso.

Para ver los diarios, siga estos pasos:
1. En una solicitud de mandatos del iSeries, entre: DSPJRN JRN(QIPNAT), si se trata de diarios de NAT, o DSPJRN JRN(QIPFILTER), si se trata de diarios de filtros IP.

Capítulo 8. Resolver problemas de las reglas de paquetes

En este apartado se dan una serie de consejos para resolver algunos de los problemas frecuentes planteados por las reglas de paquetes.

- La función de **rastreo de comunicaciones de iSeries** permite ver la totalidad del tráfico de datagramas de una interfaz especificada. Para reunir la información e imprimirla, utilice los mandatos Arrancar rastreo de comunicaciones (STRCMNTRC) e Imprimir rastreo de comunicaciones (PRTCMNTRC).
- El **orden de las reglas de NAT y de filtro IP** determina el modo en que se procesan las reglas. Estas se procesan en el mismo orden en que figuran en el archivo. Si el orden no es correcto, los paquetes no se procesarán de la manera prevista. Con esto, el sistema será vulnerable a los ataques. Coloque los nombres de los conjuntos de filtro dentro de la sentencia FILTER_INTERFACE en el mismo orden exacto en el que están definidos físicamente en el archivo.

  Consulte el apartado Crear reglas de filtro IP de este tema si necesita más ayuda para escribir reglas de filtro correctas. Recuerde el proceso que se muestra en la tabla siguiente:

Proceso del tráfico de entrada	Proceso del tráfico de salida
1. Reglas de NAT	1. Reglas de filtro IP
2. Reglas de filtro IP	2. Reglas de NAT

- **Eliminar todas las reglas** es la mejor manera de restablecer el sistema y borrar todos los errores. En el iSeries, emita el mandato siguiente: RMVTCPTBL (Eliminar tabla TCP/IP). Si se queda bloqueado fuera de las aplicación iSeries Navigator, este mandato sirve también para volver y reparar las reglas.

  Nota: el mandato ″Eliminar tabla TCP/IP″ también inicia los servidores VPN— sólo si los servidores VPN (IKE y ConMgr) estaban ejecutándose antes.
- **Permitir el reenvío de datagramas IP** en la configuración TCP/IP del iSeries es esencial si se utiliza NAT. Utilice el mandato CHGTCPA (Cambiar atributos TCP/IP) para verificar que el reenvío de datagramas IP está establecido en YES.
- **Verificar las rutas de retorno por omisión** es la manera de asegurarse de que la dirección con la que se realiza la correlación o tras la que se efectúa la ocultación es correcta. Para que NAT pueda deshacer la conversión, esta dirección debe ser direccionable en la ruta de retorno al iSeries y debe pasar por la línea correcta.

  Nota: si el iSeries tiene más de una red, o línea, conectada a él, debe tener especial cuidado con el direccionamiento del tráfico de entrada. Éste se maneja en cualquier línea en la que entre, que puede no ser la línea correcta que está a la espera de deshacer la conversión.
- **Ver los mensajes de error y de aviso** del archivo `EXPANDED.OUT` para asegurarse de que las reglas están en el orden deseado. Al verificar y activar un conjunto de filtros, estos filtros se fusionan con las reglas generadas por iSeries Navigator. El proceso de combinación genera las reglas fusionadas en un archivo nuevo denominado `EXPANDED.OUT`, que se coloca en el mismo directorio que contiene sus reglas (normalmente /QIBM). Los mensajes de aviso y de error hacen referencia a este archivo. Para ver este archivo, debe abrirlo desde el Editor de reglas de paquetes.
  1. Acceda al Editor de reglas de paquetes de iSeries Navigator.
  2. En el menú **Archivar**, seleccione **Abrir** .
  3. Vaya al directorio `QIBM/UserData/OS400/TCPIP/PacketRules/` o al directorio en que ha guardado sus reglas de paquetes, si es distinto del de por omisión.
  4. En la ventana **Abrir archivo**, seleccione el archivo **EXPANDED.OUT**. Aparecerá el archivo `EXPANDED.OUT`.
  5. Seleccione este archivo y pulse en **Abrir**.

  El archivo EXPANDED.OUT sólo le facilitará información. No es posible editarlo.

Capítulo 9. Información afín para las reglas de paquetes

A continuación figura una lista de manuales y libros rojos de IBM (en formato PDF) que proporcionan información adicional acerca del filtrado IP y de NAT.

Manuales

- **Consejos y herramientas para asegurar su iSeries**  (aproximadamente 254 páginas)
  Este libro en PDF proporciona información de alto nivel acerca de la manera de ampliar la seguridad del iSeries.

Libros rojos

- **Visión general técnica y de guía de aprendizaje de TCP/IP** 
  En esta sección encontrará información sobre temas de seguridad relacionados con redes TCP/IP.

- **TCP/IP for AS/400: More Cool Things Than Ever** 
  En esta sección encontrará algunos casos prácticos que muestran el uso de NAT y del filtrado IP de paquetes.

Para salvar un archivo PDF en la estación de trabajo para poder verlo o imprimirlo:

1. Pulse con el botón derecho del ratón sobre el PDF en el navegador (pulse con el botón derecho del ratón en el enlace superior).
2. Pulse en **Guardar destino como...**.
3. Sitúese en el directorio en el que desea salvar el archivo PDF.
4. Pulse en **Salvar**.

Si necesita Adobe Acrobat Reader para ver o imprimir estos PDF, puede bajar una copia desde el sitio web de Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Impreso en España