System i

Networking
Filtrado IP y conversión de direcciones de red

Versión 6 Release 1

System i

Networking
Filtrado IP y conversión de direcciones de red

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos”, en la página 35.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761–SS1) y a todos los releases y modificaciones ulteriores hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecutan en los modelos CISC.

Contenido

Filtrado IP y conversión de direcciones de red

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 también 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: *Regla de paquetes* es la combinación de filtrado IP y NAT. El término reglas de paquetes, utilizado en este temario, se aplica a ambos componentes.

Además de la información de este tema, utilice la ayuda en línea disponible en el editor de reglas de paquetes, de System i Navigator. La ayuda en línea de System i Navigator ofrece consejos y técnicas para obtener el máximo partido de las reglas de paquetes, incluida la ayuda de tipo ¿Cómo puedo...? e Indíqueme, así como una amplia ayuda contextual.

Nota: Por el hecho de utilizar los ejemplos de código, indica que acepta los términos de la información sobre licencia de código y exención de responsabilidad.

Archivo PDF de Filtrado IP y conversión de direcciones de red

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF, seleccione Filtrado IP y conversión de direcciones de red (alrededor de 621 KB).

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse la opción que guarda el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Para poder ver o imprimir estos archivos PDF, debe instalar Adobe en su sistema. Puede descargar una copia gratuita desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Referencia relacionada

"Información relacionada con Filtrado IP y conversión de direcciones de red" en la página 32
En las publicaciones IBM Redbooks encontrará información relacionada con el temario Filtrado IP y conversión de direcciones de red. Puede ver o imprimir cualquiera de los archivos PDF.

Casos prácticos: reglas de paquetes

Puede utilizar la conversión de direcciones de red (NAT) y el filtrado IP para proteger la red.

Cada uno de los casos prácticos incluye un diagrama y una configuración de ejemplo.

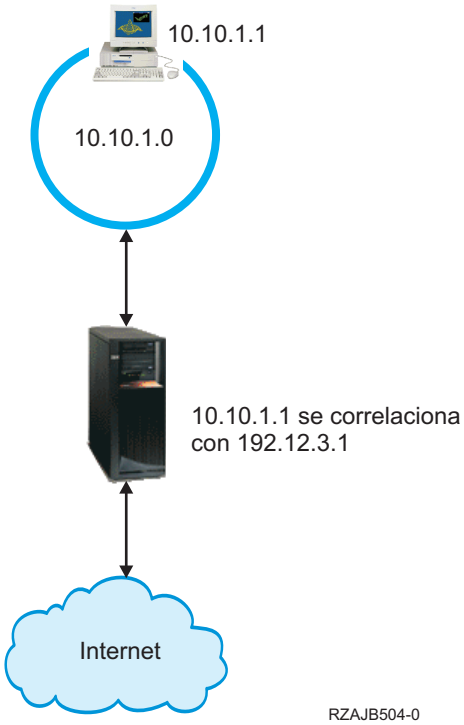
Consejo: En cada uno de los casos prácticos, las direcciones IP 192.*x*.*x*.*x* representan direcciones IP públicas. Todas las direcciones se utilizan únicamente a título de ejemplo.

Caso practico: correlacionar direcciones IP utilizando NAT

En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) estática para correlacionar sus direcciones IP privadas con direcciones públicas.

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. Cuando accede a Internet, descubre 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. Sin embargo, necesita permitir a los usuarios públicos el acceso a su servidor Web. ¿Qué debe hacer?



Solución

Puede utilizar la NAT estática. Esta asigna una dirección (privada) original a una dirección (pública) registrada. El sistema 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. La comunicación se puede iniciar desde cualquiera de las dos redes.

La utilización de NAT estática permite conservar todas las direcciones IP internas actuales y acceder igualmente a Internet. Debe 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 este ejemplo, 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 sistema personal. Si la NAT estática está activa, el tráfico de entrada destinado directamente a la dirección 192.12.3.1 no llega nunca a esa interfaz, porque esa dirección solo representa la dirección interna. El destino real es la dirección privada 10.10.1.1, aunque (para el mundo que está fuera del sistema) parezca que la dirección IP necesaria sea 192.12.3.1.

Configuración

Para configurar las reglas de paquetes descritas en este caso práctico, utilice el asistente **Conversión de direcciones** de System i 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 la línea en la que tiene lugar la correlación de direcciones: TRNLINE

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

1. En System i Navigator, seleccione ***su sistema*** → **Red** → **Políticas IP**.
2. Pulse **Reglas de paquetes** con el botón derecho del ratón 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.

Las reglas de paquetes quedan definidas como en el siguiente ejemplo.

```
Declaraciones para mapear de 10.1.1.1 a 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
```

RZAJB507-0

Cuando haya terminado de crear estas reglas, tendrá que verificarlas para asegurarse de que se activarán sin errores.

Nota: la línea de token-ring definida en la configuración anterior (LINE=TRNLINE) debe ser la línea utilizada por 192.12.3.1. La 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.

Conceptos relacionados

"Función NAT estática (de correlación)" en la página 13
La conversión de direcciones de red (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.

Tareas relacionadas

"Verificar reglas de paquetes" en la página 27
Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar sin problemas.

"Activar reglas de paquetes" en la página 27
Activar las reglas de paquetes que se crean es el último paso en la configuración de las reglas de paquetes.

Referencia relacionada

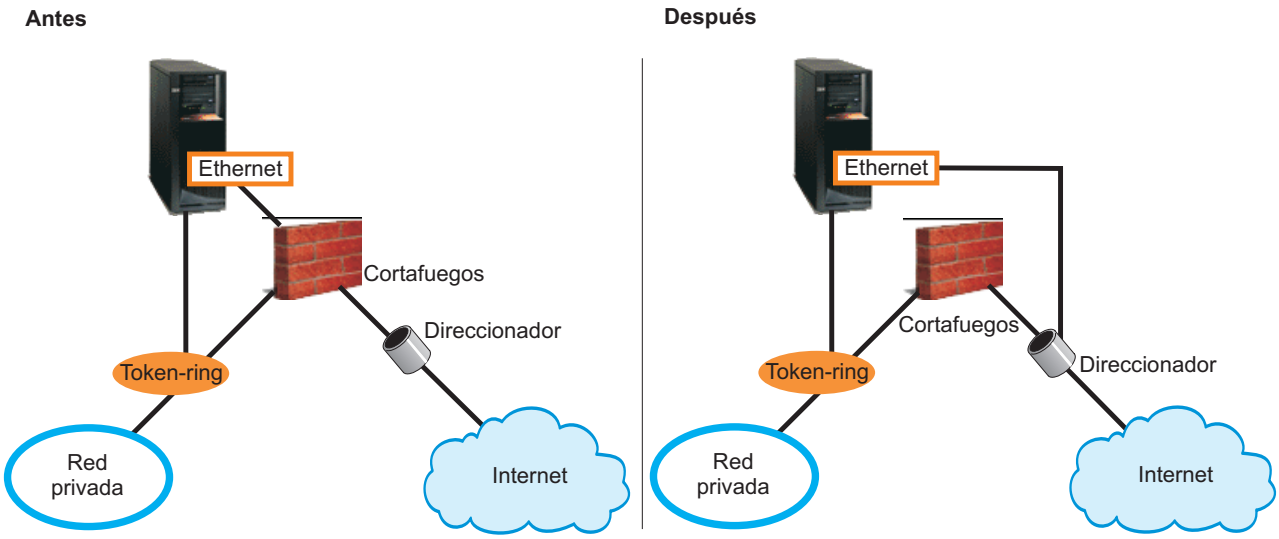
"Resolución de problemas relacionados con las reglas de paquetes" en la página 31
En este tema se dan una serie de consejos para resolver algunos de los problemas frecuentes planteados por las reglas de paquetes.

Caso práctico: crear reglas de filtro para permitir tráfico 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, que solo podrá ser tráfico HTTP, Telnet y de protocolo de transferencia de archivos (FTP).

Situación

Desea proporcionar aplicaciones Web a sus clientes, pero el cortafuegos actual funciona a plena capacidad y usted y no quiere añadirle más tráfico. Un colega le sugiere que ejecute las aplicaciones fuera del cortafuegos. Sin embargo, le interesa que desde Internet solo pueda acceder al servidor Web de System i el tráfico HTTP, FTP y Telnet. ¿Qué debe hacer?



Solución

El filtrado IP le permite establecer reglas que definan qué información puede fluir a través del servidor Web. En este caso práctico, puede escribir reglas de filtro que permitan tráfico HTTP, FTP y Telnet (de entrada y de salida). 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, utilice el asistente **Permitir un servicio** de System i Navigator. El asistente requiere la información siguiente:

- El tipo de servicio que desea permitir: HTTP.
- La dirección pública del servidor Web: 192.54.5.1.
- La dirección del cliente: cualquier dirección IP.
- La interfaz por la que se ejecutará el servicio: TRNLINE.
- El sentido en 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 System i Navigator, seleccione ***su sistema*** → **Red** → **Políticas IP**.
2. Pulse **Reglas de paquetes** con el botón derecho del ratón 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 que el tráfico HTTP entre y salga del sistema. Las reglas de paquetes quedan definidas como en el siguiente ejemplo.

```
Declaraciones 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
```

RZAJB508-0

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 haya terminado de crear estas reglas, tendrá que verificarlas para asegurarse de que se pueden activar sin errores.

Tareas relacionadas

"Verificar reglas de paquetes" en la página 27
Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar sin problemas.

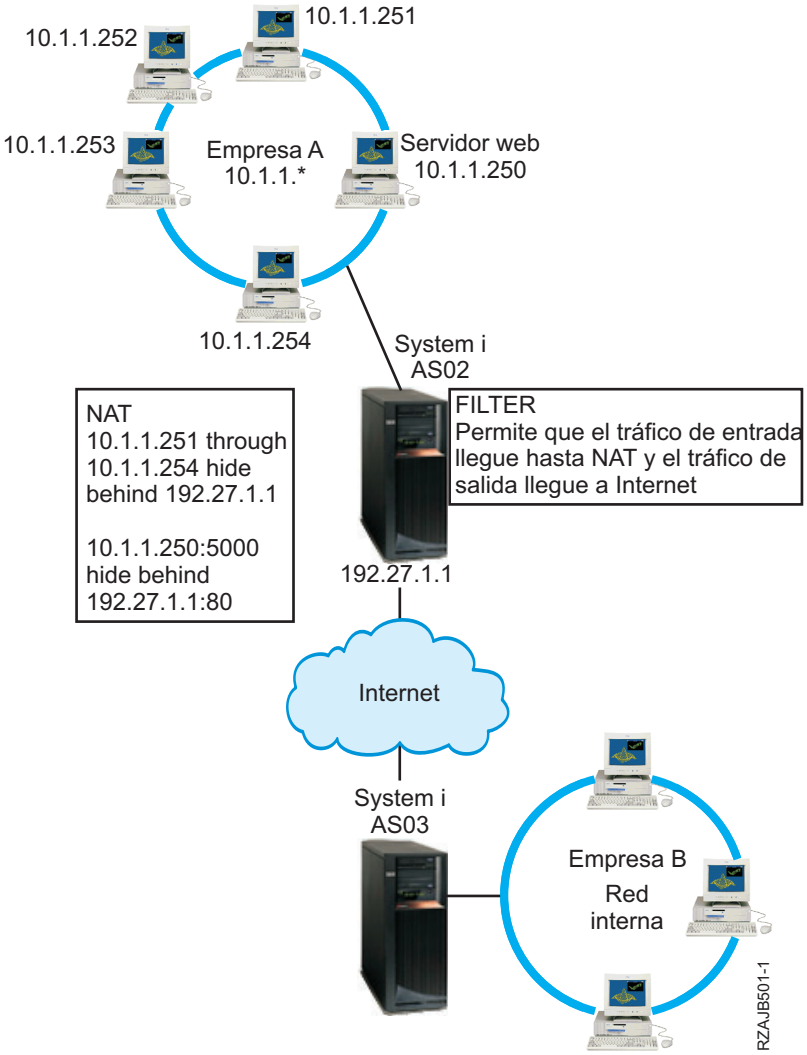
"Activar reglas de paquetes" en la página 27
Activar las reglas de paquetes que se crean es el último paso en la configuración de las reglas de paquetes.

Caso practico: combinar NAT y el filtrado IP

En este caso práctico, su empresa combina la conversión de direcciones de red (NAT) y el filtrado IP entre sí. La empresa desea ocultar los sistemas personales y el servidor Web detrás de una sola dirección IP pública y desea permitir que las otras empresas puedan acceder al servidor Web.

Situación

Su empresa cuenta con una red interna de tamaño moderado que utiliza un modelo System i como pasarela. Desea transferir todo el tráfico Web del sistema pasarela a un servidor Web dedicado, situado detrás de la pasarela. El servidor Web se ejecuta en el puerto 5000. Desea ocultar todos los sistemas personales privados y el servidor Web detrás de la interfaz del System i, AS02 en la siguiente figura. También desea permitir que otras empresas accedan al servidor Web. ¿Qué debe hacer?



Solución

Puede utilizar el filtrado IP y NAT conjuntamente para configurar los sistemas personales y el servidor Web:

- Ocultar NAT a fin de ocultar los sistemas personales detrás de una dirección pública, 192.27.1.1, para que así puedan acceder a Internet.
- 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 solo 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.
- 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, utilice el asistente de conversión de direcciones, de System i Navigator. El asistente requiere la información siguiente:

- El conjunto de direcciones que desea ocultar: de 10.1.1.251 a 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 de conversión de direcciones, siga estos pasos:

1. En System i Navigator, seleccione ***su sistema*** → **Red** → **Políticas IP**.
2. Pulse **Reglas de paquetes** con el botón derecho del ratón 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 oculta los cuatro sistemas personales detrás de una dirección pública para que puedan acceder a Internet. La regla de paquetes Ocultar NAT se parece a la del siguiente ejemplo.

```
Declaraciones para ocultar 10.1.1.251 - 10.1.1.254 detrás 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
```

RZAJB509-0

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

1. Acceda al editor de reglas de paquetes desde System i 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 **Direcciones definidas**. Luego pulse **Añadir** y entre la dirección IP del servidor Web `10.1.1.250` en el campo.
   d. Pulse **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 concreto y continuar en el paso 4. Sin embargo, si utiliza estas instrucciones para configurar NAT con correlación de puerto a fin de utilizarlo en su propia red, y no ha configurado las reglas de paquetes para ocultar NAT, deberá seguir las instrucciones de 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 **Direcciones definidas**. A continuación, pulse **Añadir** y entre `192.27.1.1` en el campo de edición **Direcciones IP**.
   d. Pulse **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 **Ocultar nombre de dirección**.
   c. Seleccione **BEHIND1** en la lista **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 **Máximo de conversaciones**.
h. Seleccione **OFF** en la lista **Registro por diario**.
i. Pulse **Aceptar**.

La regla de NAT con correlación de puerto oculta 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 solo permitirá que acceda al sistema el tráfico iniciado externamente en el puerto 80.

La regla de NAT con correlación de puerto queda definida como en el siguiente ejemplo:

```
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 desde System i 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 **Filtro**.
   c. En la página General, entre external_rules en el campo **Establecer nombre**.
   d. Seleccione **PERMIT** en la lista **Acción**.
   e. Seleccione **INBOUND** en la lista **Sentido**.
   f. Seleccione = y * en las listas **Nombre de dirección origen**.
   g. Seleccione = y entre 192.27.1.1 en los campos **Nombre de dirección destino**.
   h. Seleccione **OFF** en la lista **Registro por diario**.
   i. En la página Servicios, seleccione **Servicio**.
   j. Seleccione **TCP** en la lista **Protocolo**.
   k. Seleccione = y * en las listas **Puerto origen**.
   l. Seleccione = y * en las listas **Puerto destino**.
   m. Pulse **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 **Filtro**.
   d. En la página General, seleccione **external_rules** en la lista **Establecer nombre**.
   e. Seleccione **PERMIT** en la lista **Acción**.
   f. Seleccione **OUTBOUND** en la lista **Sentido**.
   g. Seleccione = y entre 192.27.1.1 en los campos **Nombre de dirección origen**.
   h. Seleccione = y * en las listas **Nombre de dirección destino**.
   i. Seleccione **OFF** en la lista **Registro por diario**.
   j. En la página Servicios, seleccione **Servicio**.
   k. Seleccione **TCP** en la lista **Protocolo**.

l. Seleccione **=** y ***** en las listas **Puerto origen**.
m. Seleccione **=** y ***** en las listas **Puerto destino**.
n. Pulse **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, **TRNLINE** en la lista **Nombre de línea**.
   c. En la página Conjuntos de filtros, seleccione **external_rules** en la lista **Conjunto de filtros** y pulse **Añadir**.
   d. Pulse **Aceptar**.

Estos filtros, junto con la sentencia HIDE, permiten 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 solo permite que entre en el sistema el tráfico iniciado externamente en el puerto 80. NAT no convierte el tráfico iniciado externamente que no coincida con la regla de NAT con correlación de puerto. Las reglas de filtro quedan definidas como en el siguiente ejemplo:

```
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 haya terminado de crear estas reglas de filtro, deberá verificarlas para asegurarse de que se activarán sin errores. Después ya podrá activarlas.

Tareas relacionadas

"Verificar reglas de paquetes" en la página 27
Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar sin problemas.

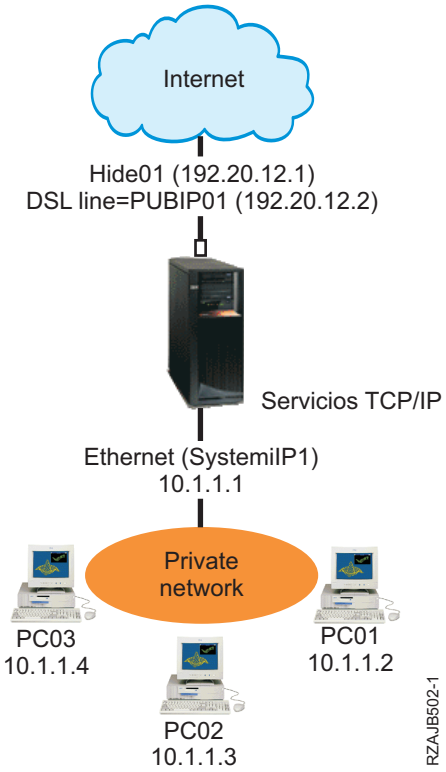
"Activar reglas de paquetes" en la página 27
Activar las reglas de paquetes que se crean es el último paso en la configuración de las reglas de paquetes.

Caso practico: ocultar direcciones IP utilizando NAT de enmascaramiento

En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) de enmascaramiento para ocultar las direcciones privadas de los sistemas personales. Al mismo tiempo, la empresa permite que los empleados accedan a Internet.

Situación

Supongamos que tiene una pequeña empresa y desea permitir el servicio HTTP en la plataforma System i. Su sistema tiene una tarjeta Ethernet y tres sistemas personales. Su proveedor de servicios de Internet (ISP) le proporciona una conexión de línea de abonado digital (DSL) y un módem DSL. También le asigna las direcciones IP públicas siguientes: 192.20.12.1 y 192.20.12.2. Todos los sistemas personales tienen las direcciones 10.1.1.*x* en la red interna. Quiere asegurarse de que las direcciones privadas de los sistemas personales permanecen ocultas para impedir que los usuarios externos puedan iniciar 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 sistemas personales, de 10.1.1.1 a 10.1.1.4, detrás de la dirección pública 192.20.12.1. Puede ejecutar servicios TCP/IP desde la dirección 10.1.1.1. La NAT de rango (que oculta un rango de direcciones internas) protege los sistemas personales 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 NAT de rango no protege la interfaz de System i. Tendrá que filtrar tráfico para proteger el sistema contra la recepción de información no deseada.

Configuración

Para configurar las reglas de paquetes descritas en este caso práctico, utilice el asistente de conversión de direcciones, de System i Navigator. El asistente requiere la información siguiente:

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

Para utilizar el asistente de conversión de direcciones, siga estos pasos:

1. En System i Navigator, seleccione ***su sistema*** → **Red** → **Políticas IP**.
2. Pulse **Reglas de paquetes** con el botón derecho del ratón 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.

Las reglas de paquetes quedan definidas como en el siguiente ejemplo.

```
Declaraciones para ocultar 10.1.1.1 - 10.1.1.4 detrás 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
```

RZAJB510-0

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

Conceptos relacionados

"Función NAT de enmascaramiento (ocultación)" en la página 14
La conversión de direcciones de red (NAT) de enmascaramiento (ocultación) le permite ocultar la dirección real de un sistema personal privado. NAT hace que el tráfico del sistema personal se direccione a su sistema, lo que básicamente convierte al sistema en la pasarela del sistema personal.

Tareas relacionadas

"Verificar reglas de paquetes" en la página 27
Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar sin problemas.

"Activar reglas de paquetes" en la página 27
Activar las reglas de paquetes que se crean es el último paso en la configuración de las reglas de paquetes.

Conceptos relacionados con las 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 tipos de reglas 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, debe familiarizarse con los conceptos siguientes y entender cómo atañen a su sistema:

- Las reglas de paquetes comparadas con otras soluciones de i5/OS
- NAT

Nota: Por el hecho de utilizar los ejemplos de código, indica que acepta los términos de la información sobre licencia de código y exención de responsabilidad.

Terminología de las reglas de paquetes

A continuación se proporcionan algunos términos útiles relacionados con las reglas de paquetes.

dirección limítrofe
La dirección limítrofe es una dirección pública que hace de frontera entre una red de confianza y otra que no lo es. Describe la dirección IP como una interfaz real del sistema. El sistema debe saber cuál es el tipo de dirección que se define en cada caso. Por ejemplo, la dirección IP del sistema personal es de confianza, pero la dirección IP pública del sistema es una dirección limítrofe.

cortafuegos
Es una barrera lógica que rodea a los sistemas de una red. Consta de hardware, 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
Maxcon es un parámetro que forma parte de la regla de filtro de la conversión de direcciones de red (NAT) de enmascaramiento. Es el número máximo de conversaciones que pueden estar

activas en un momento dado. Debe definir este número cuando configure las reglas de enmascaramiento de NAT. El valor por omisión es 128. Maxcon solo 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 origen y número de puerto origen privados (sin NAT).
- Dirección IP origen (NAT) pública y número de puerto origen (NAT) público.
- Dirección IP y número de puerto destino (una red externa).

Identificador de filtro PPP
El identificador de filtro PPP le permite aplicar reglas de filtro a una interfaz que ha sido definida en un perfil punto a punto. El identificador de filtro PPP también enlaza las reglas de filtro con grupos de usuarios en un perfil punto a punto. Como el perfil punto a punto se asocia a una dirección IP específica, el identificador de filtro define implícitamente la interfaz a la que se aplican las reglas.

Tiempo de espera
El tiempo de espera 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.

Información relacionada

Caso práctico: gestionar el acceso de usuarios remotos a recursos utilizando políticas de grupo y filtrado IP

Las reglas de paquetes comparadas con otras soluciones de i5/OS

En situaciones de alto riesgo, como al proteger un sistema de producción o al proteger las comunicaciones entre la plataforma System i y los otros sistemas de una red, es posible que tenga que investigar otras soluciones de seguridad con objeto de su protección.

El sistema tiene componentes de seguridad integrados que pueden protegerlo contra varios tipos de riesgos. Las reglas de paquetes proporcionan un medio económico de proteger el sistema. En algunos casos, las reglas de paquetes pueden proporcionar todo lo necesario sin tener que efectuar desembolsos adicionales.

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

- **System i y la seguridad en Internet**

  Este temario proporciona 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 sobre cómo habilitar SSL en las aplicaciones de i5/OS.
- **Redes privadas virtuales (VPN)**

  VPN permite a las empresas extender de manera segura sus intranets privadas por la infraestructura existente de una red pública, como es Internet. En este tema se describe la VPN y se indica cómo utilizarla en el sistema.

Conversión de direcciones de red (NAT)

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.

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. 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). Gracias a la ocultación o a la correlación de las direcciones, NAT resuelve los diversos problemas que estas plantean.

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

Se propone configurar una plataforma System i como servidor Web público. Sin embargo, no quiere que las redes externas sepan cuáles son las direcciones IP internas reales del sistema. 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 sistema queda oculta, lo que hace que el sistema resulte menos vulnerable ante un ataque.

Ejemplo: convertir una dirección IP de un host interno en una dirección IP diferente

Desea que las direcciones IP privadas de la red interna se comuniquen con hosts de Internet. Para disponerlo así, puede convertir la dirección IP de un host interno en una dirección IP diferente. Para comunicarse con los hosts 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 host interno se direcciona por Internet.

Ejemplo: compatibilizar las direcciones IP de dos redes distintas

Desea permitir que un host de otra red, como por ejemplo la de una empresa suministradora, se comunique con un host 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 hosts. Para evitarlo, puede utilizar NAT para convertir la dirección del host interno en una dirección IP distinta.

Referencia relacionada

"Crear reglas de filtro IP" en la página 24
Cuando se crea un filtro, se especifica una regla que rige el tráfico IP que circula hacia dentro y hacia afuera del sistema.

Función NAT estática (de correlación)

La conversión de direcciones de red (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 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 sistema al que desea permitir el acceso de usuarios públicos. En este caso, debe crear una regla de NAT que correlacione la dirección real del sistema con una dirección pública. La dirección pública pasa a ser información externa. Con ello se garantiza que la información interna permanezca fuera del alcance de alguien cuyas intenciones pudieran ser atacar los sistemas.

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

- Es una correlación biunívoca.
- Se puede iniciar mediante una red externa y una red interna.
- La dirección con la que se establece asociación o correlación puede ser cualquier dirección.

- La dirección con la que se establece asociación o correlación ya no se puede utiliza como interfaz IP.
- No utilice NAT con correlación de puerto.

Atención: Utilice la NAT estática con precaución si decide correlacionar un sistema personal con la dirección públicamente conocida de la plataforma System i. La *dirección conocida públicamente* es la dirección IP que está reservada para la mayor parte del tráfico de Internet y de intranet. Si correlaciona con esta dirección IP, NAT convertirá todo el tráfico y lo enviará a la dirección privada interna. Dado que esta interfaz está reservada para NAT, el sistema y la interfaz quedarán inservibles.

Conceptos relacionados

"Caso practico: correlacionar direcciones IP utilizando NAT" en la página 2
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) estática para correlacionar sus direcciones IP privadas con direcciones públicas.

Función NAT de enmascaramiento (ocultación)

La conversión de direcciones de red (NAT) de enmascaramiento (ocultación) le permite ocultar la dirección real de un sistema personal privado. NAT hace que el tráfico del sistema personal se direccione a su sistema, lo que básicamente convierte al sistema en la pasarela del sistema personal.

La función NAT de enmascaramiento permite convertir varias direcciones IP en una sola dirección IP. Puede utilizar la NAT de enmascaramiento para ocultar una o varias direcciones IP de la red interna detrás de una dirección IP que desee hacer pública. La dirección pública es aquella a la que se convierten las direcciones privadas y debe ser una interfaz definida en el sistema. Para ser una interfaz definida, hay que definir la dirección pública como dirección BORDER.

Ocultar múltiples direcciones

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

1. La dirección IP convertida sustituye a la dirección IP origen. Esto sucede en la cabecera IP del paquete IP.
2. El número de puerto 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 origen IP y el nuevo número de puerto.
4. La conversación existente permite que el servidor NAT deshaga la conversión de los datagramas IP desde el servidor externo.

Cuando se utiliza la función 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 NAT. La función NAT de enmascaramiento es una magnífica opción porque los hosts externos no pueden iniciar tráfico hacia la red. Como resultado, la red gana en protección contra un ataque del exterior. Asimismo, solo 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 enlazados detrás de una dirección IP pública en la estación de trabajo NAT.
- La NAT de enmascaramiento solo la puede iniciar la red interna.
- Los números de puerto se asocian a 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 estación de trabajo NAT se puede usar como interfaz externa de NAT.

Nota:

Si los parámetros no se establecen para adaptarlos a su entorno, la conversión de direcciones podría no funcionar como cabría esperar. Por ejemplo, las direcciones IP de los paquetes no se convierten o los paquetes se podrían descartar. No obstante, esto no provocará ningún daño en el hardware o el sistema. Si desea ajustar los valores de los parámetros, tenga en cuenta los siguientes elementos:

- El valor de MAXCON debe ser lo suficientemente alto como para dar cabida al número de conversaciones que se desea utilizar. Por ejemplo, si se utiliza el protocolo de transferencia de archivos (FTP), el sistema personal tendrá dos conversaciones activas. En este caso, será necesario establecer MAXCON de manera que dé cabida a múltiples conversaciones para cada sistema personal. Habrá que decidir cuántas conversaciones concurrentes interesa permitir en la red. El valor predeterminado es 128.
- El valor de TIMEOUT (una sentencia de regla HIDE) debe ser lo suficientemente alto como para dar tiempo a que finalicen las conversaciones entre los sistemas personales y el servidor. Para que la función 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 predeterminado es 16.
- La NAT de enmascaramiento solo soporta estos protocol: TCP, protocolo de datagramas de usuario (UDP) y protocolo Internet de mensajes de control (ICMP).
- Siempre que utilice NAT, debe habilitar el reenvío IP. Utilice el mandato Cambiar atributos de TCP/IP (CHGTCPA) para verificar que el valor de reenvío de datagramas IP es YES.

Conceptos relacionados

"Cabecera de paquete IP" en la página 18
Se pueden crear reglas de filtro que hagan referencia a las diversas partes de las cabeceras IP, TCP, UDP e ICMP.

"Caso practico: ocultar direcciones IP utilizando NAT de enmascaramiento" en la página 9
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) de enmascaramiento para ocultar las direcciones privadas de los sistemas personales. Al mismo tiempo, la empresa permite que los empleados accedan a Internet.

Función NAT de enmascaramiento (con correlación de puerto)

La conversión de direcciones de red (NAT) con correlación de puerto es una variante de la NAT de enmascaramiento.

En la NAT con correlación de puerto, puede especificar la dirección IP y el número de puerto que hay que convertir. Esto permite al sistema personal interno y a la estación de trabajo externa iniciar el tráfico IP. Puede utilizar la NAT con correlación de puerto si la estación de trabajo externa (o el cliente externo) tiene que acceder a estaciones de trabajo o sistemas dentro de la red. Solo tendrá acceso el tráfico IP que coincida con la dirección IP y el número de puerto.

Inicio interno

Cuando el sistema personal interno que tiene la *Dirección 1: Puerto 1* inicia el tráfico hacia una estación de trabajo externa, el código de conversión comprobará si en el archivo de reglas de NAT figura la *Dirección 1: Puerto 1*. Si la dirección IP origen (Dirección 1) y el número de puerto 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 origen y al número de puerto origen. La *Dirección 1: Puerto 1* es sustituida por la *Dirección 2: Puerto 2*.

Inicio externo

Una estación de trabajo externa inicia el tráfico IP utilizando la *Dirección 2* como dirección IP destino. El número de puerto destino es el *Puerto 2*. El servidor NAT deshace la conversión del datagrama con o sin una conversación existente. Dicho de otra manera, NAT creará automáticamente una conversación si todavía no existe una. 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:

- La NAT de enmascaramiento con correlación de puerto tiene una relación biunívoca.
- La NAT de enmascaramiento con correlación de puerto se puede iniciar mediante ambas redes, la externa y la interna.
- La dirección registrada tras la que se oculta la dirección privada debe estar definida en la plataforma System i 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, puede ejecutar un servidor HTTP enlazado al puerto 5123 y luego correlacionarlo 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 destino. Si no, es difícil que la comunicación tenga lugar.

Notas:

- El valor de MAXCON debe ser lo suficientemente alto como para dar cabida al número de conversaciones que se desea utilizar. Por ejemplo, si se utiliza el protocolo de transferencia de archivos (FTP), el sistema personal tendrá dos conversaciones activas. Debe establecer MAXCON de manera que dé cabida a múltiples conversaciones para cada sistema personal. El valor por omisión es 128.
- La NAT de enmascaramiento solo soporta estos protocol: TCP, protocolo de datagramas de usuario (UDP) y protocolo Internet de mensajes de control (ICMP).
- Siempre que utilice NAT, debe habilitar el reenvío IP. Utilice el mandato Cambiar atributos de TCP/IP (CHGTCPA) para verificar que el reenvío de datagramas IP está establecido en YES.

Filtrado IP

El componente de filtrado IP de las reglas de paquetes le permite controlar qué tráfico IP desea permitir que entre y salga de la red de su empresa.

Utilice el filtrado IP como ayuda para proteger el sistema, filtrando paquetes en función de las reglas que especifique.

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 a líneas (por ejemplo, token-ring (trnline)) no a interfaces lógicas ni a direcciones IP. El sistema coteja cada paquete con cada una de las reglas asociadas a 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.

- PERMIT — permite que el paquete procese como de costumbre
- DENY — descarta inmediatamente el paquete
- IPSEC — envía el paquete mediante una conexión de red privada virtual (VPN), que usted especifica en la regla de filtro

Nota: En este caso, el protocolo de seguridad IP (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.

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 solo 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.

Información relacionada

Redes privadas virtuales (VPN)

Sentencias de filtro de ejemplo

La finalidad de esta sentencia de filtro de ejemplo es hacer una demostración de la sintaxis apropiada para crear reglas de filtro en el sistema y enseñarle cómo funcionan juntas las diversas sentencias de un archivo.

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 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 produce efecto al activar 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, solo 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. Cuando aplique reglas a una interfaz mediante la que está configurando la plataforma System i, es muy importante que permita que su estación de trabajo (o la de la persona que esté configurando el sistema) se conecte a la plataforma System i. En caso contrario, se perderá la comunicación con el sistema.

También puede aplicar varios conjuntos a una sentencia de interfaz de filtro como se muestra en el siguiente ejemplo:

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

Estos conjuntos (set) se procesan en el mismo orden en que los vaya poniendo en la sentencia de interfaz de filtro (set1, set2 y set3). Los filtros de 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 solo 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 origen
- Protocolo (por ejemplo, TCP, UDP)
- Dirección IP destino
- Puerto origen
- Puerto 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 destino, la origen y el sentido (de entrada). En este caso, el sistema empareja todos los paquetes de entrada (en función de las direcciones origen y destino) con las reglas correspondientes. A continuación, emprende la acción especificada en la regla. El sistema descarta los paquetes que no estén permitidos en las reglas de filtro. A esto se le llama *regla de denegación predeterminada*.

Nota: El sistema aplica la regla de denegación predeterminada a los paquetes solo si la interfaz física tiene activa por lo menos una regla. Esta regla puede haberla definido el cliente o puede haberse generado mediante System i 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 predeterminada en ambos sentidos. Si en la interfaz física no existe una regla de filtro activa, la regla de denegación predeterminada no funciona.

Conceptos relacionados

"Función NAT de enmascaramiento (ocultación)" en la página 14
La conversión de direcciones de red (NAT) de enmascaramiento (ocultación) le permite ocultar la dirección real de un sistema personal privado. NAT hace que el tráfico del sistema personal se direccione a su sistema, lo que básicamente convierte al sistema en la pasarela del sistema personal.

Organizar las reglas de NAT con las reglas de filtro IP

Aunque la conversión de direcciones de red (NAT) y el filtrado de IP funcionan de forma independiente, puede utilizar NAT conjuntamente con el filtrado de IP.

Si opta por aplicar solo reglas de NAT, el sistema efectuará únicamente la conversión de direcciones. De modo parecido, si opta por aplicar solo reglas de filtro IP, el sistema solo 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 crea 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 tener que reescribir todas las reglas.

Tareas relacionadas

"Incluir archivos en reglas de paquetes" en la página 26
Mediante la característica **Incluir** del editor de reglas de paquetes, puede activar más de un archivo de reglas de paquetes en el sistema.

Organizar múltiples reglas de filtro IP

Cuando crea una regla de filtro, la regla hace referencia a una sentencia de una sola regla. Un grupo de reglas de filtro se denomina un *conjunto*. Los filtros que hay dentro de un conjunto se procesan en orden físico de arriba abajo. Varios conjuntos se procesan en orden físico dentro de una sentencia FILTER_INTERFACE.

El ejemplo siguiente muestra dónde contiene un conjunto 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.

Nota: Por el hecho de utilizar los ejemplos de código, indica que acepta los términos de la información sobre licencia de código y exención de responsabilidad.

```
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 estar en un sistema de confianza de su propia red. Debe proteger contra este tipo de ataque las interfaces que estén enlazadas con una red pública.

Puede protegerse contra la usurpación siguiendo los pasos del asistente Protección contra la usurpación, que está disponible en el editor de reglas de paquetes de System i 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 estación de trabajo de confianza desde una red privada (de confianza).

Planificar reglas de paquetes

Antes de conectar recursos de red a Internet, debe elaborar un plan de seguridad y comprender los riesgos potenciales que ello implica para la seguridad.

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. System i y la seguridad en Internet le proporcionará los detalles que necesita para crear un plan total de seguridad de red.

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

Tareas relacionadas

"Configurar reglas de paquetes" en la página 21
En esta lista de comprobación se proporciona una visión general de las tareas que debe realizar para asegurarse de que las reglas funcionan como es debido al activarlas.

Reglas de paquetes: requisitos de autorización de usuario

Para poder administrar reglas de paquetes en la plataforma System i, asegúrese de que tiene las autorizaciones de acceso necesarias. 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, esta es la autorización correcta. Si no tiene el ID de usuario correcto o la autorización *ALLOBJ, necesita una autorización en los siguientes directorios, archivos e ID de usuario QSYS:

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 necesita la autorización ADD sobre el perfil QSYS, ya que QSYS es propietario de los archivos de reglas recién creados.

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 de los de la lista anterior, necesita una autorización sobre esos directorios.

Reglas de paquetes: requisitos del sistema

Debe asegurarse de que el sistema satisface los requisitos mínimos del sistema para trabajar con reglas de paquetes.

Para que las reglas de paquetes funcionen como es debido en el sistema, se necesitan los siguientes productos:

- OS/400 V5R2, i5/OS V5R3 o posterior.
- IBM System i Access para Windows (5761-XE1) y System i Navigator.
  - Componente de red de System i Navigator.
- IBM TCP/IP Connectivity Utilities para i5/OS (5761-TC1) tiene que estar configurado, incluidas las interfaces IP, las rutas, el nombre de host local y el nombre de dominio local.

Información relacionada

TCP/IP Tutorial and Technical Overview

V4 TCP/IP for AS/400: More Cool Things Than Ever

Reglas de paquetes: hoja de trabajo de planificación

Puede utilizar la hoja de trabajo de planificación de reglas de paquetes para 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 de la lista, especifique los aspectos del flujo de tráfico TCP/IP que figuran a continuación: • El tipo de servicio que desea permitir o denegar (por ejemplo, HTTP, protocolo de transferencia de archivos (FTP), etc.). • El número del puerto conocido públicamente correspondiente a dicho servicio. • El sentido de circulación del 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 solo es necesaria si se está utilizando la conversión de direcciones de red).	

Configurar reglas de paquetes

En esta lista de comprobación se proporciona una visión general de las tareas que debe realizar para asegurarse de que las reglas funcionan como es debido al activarlas.

Encontrará información específica en la ayuda en línea del editor de reglas de paquetes.

Cuando haya creado un plan para las reglas de paquetes en el sistema, estará listo para empezar realmente a crearlas y aplicarlas.

__ Acceda al editor de reglas de paquetes. Para acceder al editor de reglas de paquetes de System i Navigator, siga estas instrucciones.

__ 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 permite el tráfico necesario para un determinado servicio TCP o de protocolo de datagramas de usuario (UDP).

- Asistente **Protección contra la usurpación**

  Este asistente genera e inserta un conjunto de sentencias de reglas de paquetes que deniega en una interfaz todo el tráfico que solo deba entrar en 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.

En función del tipo de reglas que desee configurar, estos asistentes crean automáticamente todas las sentencias de filtro y de conversión de direcciones de red (NAT) necesarias. Puede acceder a los asistentes desde el menú Asistentes del editor de reglas de paquetes. Si prefiere escribir las reglas usted mismo, continúe en el próximo punto de la lista de comprobación.

__ Defina direcciones y servicios, creando alias de las direcciones y servicios para los que piense crear múltiples reglas.

Nota: Debe definir direcciones si desea crear reglas de NAT.

__ Cree reglas de NAT. Solo debe realizar esta tarea si se propone utilizar NAT.

__ Cree reglas de filtro para definir qué filtros hay que aplicar a la red administrada por este sistema.

__ Especifique los archivos adicionales que desee incluir en el archivo de reglas maestro. Solo debe realizar esta tarea si ya tiene archivos de reglas que quiere reutilizar en un nuevo archivo de reglas.

__ Defina las interfaces aplicando las reglas.

__ Haga comentarios para describir qué hace cada archivo de reglas.
__ Verifique los archivos de reglas para asegurarse de que las reglas se activarán sin errores ni problemas.
__ Active el archivo de reglas. Las reglas de paquetes deben activarse para que puedan funcionar.
__ Gestione las reglas de paquetes. Una vez que haya activado las reglas de paquetes, deberá gestionarlas periódicamente a fin de mantener la seguridad del sistema.

Tareas relacionadas

"Planificar reglas de paquetes" en la página 19
Antes de conectar recursos de red a Internet, debe elaborar un plan de seguridad y comprender los riesgos potenciales que ello implica para la seguridad.

"Gestionar reglas de paquetes" en la página 28
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 exactas y estén actualizadas.

Acceder al editor de reglas de paquetes

Puede utilizar 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 proporcionados en el sistema.

Debe acceder al editor de reglas de paquetes mediante System i Navigator.

Para acceder al editor de reglas de paquetes, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Políticas IP**.
2. Pulse **Reglas de paquetes** con el botón derecho del ratón y seleccione **Editor de reglas**.

Utilice la ayuda en línea para obtener instrucciones sobre cómo realizar cada una de estas tareas.

Referencia relacionada

"Resolución de problemas relacionados con las reglas de paquetes" en la página 31
En este tema se dan una serie de consejos para resolver algunos de los problemas frecuentes planteados por las reglas de paquetes.

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 las siguientes ventajas:

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

Supongamos, por ejemplo, que tiene usuarios en la red que necesitan 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:

- Definir una regla de filtro para la dirección IP de cada uno de los usuarios.
- 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 solo 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. El alias de servicio define qué criterios de TCP, protocolo de datagramas de usuario (UDP) y protocolo Internet de mensajes de control (ICMP) desea seleccionar. Se selecciona el puerto origen y el destino que se desea utilizar.

Recuerde: Debe definir direcciones si piensa utilizar la conversión de direcciones de red (NAT). Las reglas de NAT solo pueden señalar hacia una dirección definida.

Para obtener instrucciones sobre cómo definir direcciones, alias de servicios y servicios ICMP, utilice la ayuda en línea del editor de reglas de paquetes.

Si se propone utilizar la conversión de direcciones de red (NAT), vaya a: Crear reglas de NAT. De lo contrario, vaya a: “Crear reglas de filtro IP” en la página 24 para filtrar el tráfico IP que entra y sale de la red.

Tareas relacionadas

“Añadir comentarios en las reglas de paquetes” en la página 26
Puede anotar cómo desea que funcionen las reglas añadiendo comentarios sobre los archivos de reglas.

Crear reglas de NAT

Si quiere emplear la conversión de direcciones de red (NAT), debe definir apodos para las direcciones IP que piense 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 a 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 le permite crear dos tipos de reglas de NAT. Uno de ellos le permite ocultar las direcciones, mientras que el otro le permite correlacionarlas.

Ocultar direcciones

Oculte las direcciones si se desea que las direcciones privadas no estén visibles para los demás. La regla para ocultar direcciones le permite ocultar múltiples direcciones internas detrás de una sola dirección IP pública. Este tipo de NAT también se conoce como NAT de enmascaramiento.

Correlacionar direcciones

Correlacione las direcciones cuando 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 sobre cómo ocultar o correlacionar direcciones, utilice la ayuda en línea del editor de reglas de paquetes.

Próximo tema

Si tiene previsto filtrar el tráfico que circula hacia dentro y hacia fuera de la red, vaya a: Crear reglas de filtro IP. De lo contrario, continúe en: "Añadir comentarios en las reglas de paquetes" en la página 26.

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.

Importante: Cuando aplique reglas a una interfaz mediante la que esté configurando la plataforma System i, es muy importante que dé permiso a su propia estación de trabajo o la de la persona que esté configurando el sistema. En caso contrario, se perdería la comunicación con el sistema. En ese caso, debe iniciar sesión en el sistema utilizando una interfaz que todavía tenga conectividad, como la consola de los 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. Cuando 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 opcionales:
  - Coloque los nombres de los conjuntos de filtro dentro de la sentencia FILTER_INTERFACE en el mismo orden en que están definidos físicamente en el archivo.
  - 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 solo puede haber activo un archivo de reglas en todo momento. Vea el siguiente ejemplo.
- Escriba reglas de filtro solo 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 Crear nombres de conjunto. 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 habilitar 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 sobre cómo crear reglas de filtro IP, utilice la ayuda en línea del editor de reglas de paquetes.

Cuando haya creado los filtros, es posible que le interese incluir archivos en reglas de paquetes en la sentencia de filtro. Si no es así, el paso siguiente es "Definir interfaces de filtro IP" a las que se aplican las reglas.

Conceptos relacionados

"Conversión de direcciones de red (NAT)" en la página 12
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.

Referencia relacionada

"Resolución de problemas relacionados con las reglas de paquetes" en la página 31
En este tema se dan una serie de consejos para resolver algunos de los problemas frecuentes planteados por las reglas de paquetes.

Definir interfaces de filtro IP

Puede definir interfaces de filtro para establecer las reglas de filtro que se desea que el sistema aplique a cada interfaz.

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 solo 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 sobre cómo definir una interfaz de filtro, utilice la ayuda en línea del editor de reglas de paquetes.

Incluir archivos en reglas de paquetes

Mediante la característica **Incluir** del editor de reglas de paquetes, puede activar más de un archivo de reglas de paquetes en el sistema.

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 múltiples 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 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, solo 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 sobre cómo incluir un archivo en las reglas, utilice la ayuda en línea del editor de reglas de paquetes.

Conceptos relacionados

"Organizar las reglas de NAT con las reglas de filtro IP" en la página 18
Aunque la conversión de direcciones de red (NAT) y el filtrado de IP funcionan de forma independiente, puede utilizar NAT conjuntamente con el filtrado de IP.

Añadir comentarios en las reglas de paquetes

Puede anotar cómo desea que funcionen las reglas añadiendo comentarios sobre los archivos de reglas.

Por ejemplo, le podría interesar dejar constancia de qué es lo que una determinada regla permite o deniega. Este tipo de información puede ahorrarle mucho tiempo en el futuro. Si alguna vez debe arreglar un problema de seguridad, podría necesitar estos comentarios para explicar cómo funcionan las reglas. Tal vez no disponga de tiempo para desentrañar el significado de las reglas en un momento posterior, 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**. Este 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 sobre cómo hacer comentarios en un archivo de reglas, utilice la ayuda en línea del editor de reglas de paquetes.

Tareas relacionadas

"Definir direcciones y servicios" en la página 22
Cuando se crean reglas de paquetes, es preciso especificar las direcciones IP y los servicios a los que desea aplicar las reglas.

Verificar reglas de paquetes

Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar 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, puede visualizar las reglas de paquetes para comprobar si existen errores visibles. No puede activar 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 del 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.

Para obtener instrucciones sobre cómo verificar reglas de paquetes, utilice la ayuda en línea del editor de reglas de paquetes.

Conceptos relacionados

"Caso practico: correlacionar direcciones IP utilizando NAT" en la página 2
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) estática para correlacionar sus direcciones IP privadas con direcciones públicas.

"Caso práctico: crear reglas de filtro para permitir tráfico HTTP, Telnet y FTP" en la página 4
En este caso práctico, su empresa utiliza el filtrado IP para restringir el tráfico IP que puede acceder a su servidor Web, que solo podrá ser tráfico HTTP, Telnet y de protocolo de transferencia de archivos (FTP).

"Caso practico: combinar NAT y el filtrado IP" en la página 5
En este caso práctico, su empresa combina la conversión de direcciones de red (NAT) y el filtrado IP entre sí. La empresa desea ocultar los sistemas personales y el servidor Web detrás de una sola dirección IP pública y desea permitir que las otras empresas puedan acceder al servidor Web.

"Caso practico: ocultar direcciones IP utilizando NAT de enmascaramiento" en la página 9
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) de enmascaramiento para ocultar las direcciones privadas de los sistemas personales. Al mismo tiempo, la empresa permite que los empleados accedan a Internet.

Tareas relacionadas

"Ver reglas de paquetes" en la página 29
Antes de activar las reglas de filtro, debe verificar que son correctas.

Activar reglas de paquetes

Activar las reglas de paquetes que se crean 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, debe verificar que son correctas. Intente siempre resolver los problemas que haya antes de activar las reglas de paquetes. Si activa las 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 solo se utilizan reglas de NAT y no de filtro), aparecerá un aviso (TCP5AFC). No se trata de un error. Solo verifica si su intención es utilizar una interfaz. Fíjese siempre en el último mensaje. Si en él se dice que la activación es satisfactoria, los mensajes que le preceden son todos ellos avisos.

Nota: Si activa 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 solo sustituirán a las reglas de esa interfaz en concreto. Las reglas existentes en las demás interfaces no se tocarán.

Una vez configuradas y activadas las reglas de paquetes, deberá gestionarlas periódicamente a fin de garantizar la seguridad del sistema.

Conceptos relacionados

"Caso practico: correlacionar direcciones IP utilizando NAT" en la página 2
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) estática para correlacionar sus direcciones IP privadas con direcciones públicas.

"Caso práctico: crear reglas de filtro para permitir tráfico HTTP, Telnet y FTP" en la página 4
En este caso práctico, su empresa utiliza el filtrado IP para restringir el tráfico IP que puede acceder a su servidor Web, que solo podrá ser tráfico HTTP, Telnet y de protocolo de transferencia de archivos (FTP).

"Caso practico: combinar NAT y el filtrado IP" en la página 5
En este caso práctico, su empresa combina la conversión de direcciones de red (NAT) y el filtrado IP entre sí. La empresa desea ocultar los sistemas personales y el servidor Web detrás de una sola dirección IP pública y desea permitir que las otras empresas puedan acceder al servidor Web.

"Caso practico: ocultar direcciones IP utilizando NAT de enmascaramiento" en la página 9
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) de enmascaramiento para ocultar las direcciones privadas de los sistemas personales. Al mismo tiempo, la empresa permite que los empleados accedan a Internet.

Tareas relacionadas

"Gestionar reglas de paquetes"
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 exactas y estén actualizadas.

Gestionar reglas de paquetes

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 exactas y estén actualizadas.

Nota: Las instrucciones específicas para realizar estas tareas están en la ayuda en línea del editor de reglas de paquetes, a menos que se indique otra cosa.

Tareas relacionadas

"Configurar reglas de paquetes" en la página 21
En esta lista de comprobación se proporciona una visión general de las tareas que debe realizar para asegurarse de que las reglas funcionan como es debido al activarlas.

"Activar reglas de paquetes" en la página 27
Activar las reglas de paquetes que se crean es el último paso en la configuración 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 las 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 sobre cómo desactivar reglas de paquetes, utilice la ayuda en línea del editor de reglas de paquetes.

Ver reglas de paquetes

Antes de activar las reglas de filtro, debe verificar que son correctas.

Conviene que vea las reglas de filtro que haya creado para poder comprobar si existen errores visibles. Es posible que en algún momento le interese ver las reglas de filtro, no solo antes de activarlas y probarlas, sino también antes de imprimirlas y hacer copia de seguridad de ellas. La acción de 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 revisarlas, imprima las reglas de filtro que haya creado. Esto le permite detectar las equivocaciones visibles y verificar que ha incluido todos los archivos de reglas de filtro 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. Así se ahorrará tiempo y recursos valiosos.

Para ver las reglas inactivas, debe abrir el archivo de reglas en el 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 System i Navigator, seleccione ***su sistema*** → **Red** → **Políticas IP** → **Reglas de paquetes**.
2. Seleccione la interfaz de las reglas de paquetes activas que desea ver.
3. Vea la lista de reglas de paquetes activas en el panel derecho.

Nota: No puede 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.

Tareas relacionadas

"Verificar reglas de paquetes" en la página 27
Debe verificar siempre las reglas de paquetes antes de activarlas. Así se asegura de que las reglas se pueden activar sin problemas.

"Editar 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.

Editar 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. Luego utilice el editor de reglas de paquetes de System i Navigator para hacer los cambios necesarios en las reglas. Recuerde que debe verificar y luego reactivar las reglas cuando haya terminado de editarlas.

Para obtener instrucciones sobre cómo editar reglas de paquetes, utilice la ayuda en línea del editor de reglas de paquetes.

Tareas relacionadas

"Ver reglas de paquetes" en la página 29
Antes de activar las reglas de filtro, debe verificar que son correctas.

Hacer copia de seguridad de las reglas de paquetes

Al hacer copia de seguridad de los archivos de reglas de paquetes, puede ahorrarse el tiempo y el trabajo que le supondría crearlos de nuevo en el caso de una pérdida.

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

Imprima las reglas de filtro

Podrá guardar las salidas impresas en un lugar seguro y volver a entrar la información según convenga. Las salidas impresas resultan también útiles si tiene que buscar un error en una regla de filtro.

Para obtener instrucciones sobre imprimir reglas de paquetes, utilice la ayuda en línea del editor de reglas de paquetes.

Copie la información en un disco

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

Nota: El sistema copia la información en el disco del sistema, no en un disquete. Los archivos de reglas se almacenan en el sistema de archivos integrado de la plataforma System i, no en un sistema personal. Puede emplear un método de protección de disco como medio de proteger los datos almacenados en el disco del sistema.

Si se propone utilizar una plataforma System i, debe planificar una estrategia de copia de seguridad y recuperación.

Información relacionada

Hacer copia de seguridad del sistema

Registrar por diario y auditar acciones de reglas de paquetes por cada regla de paquete

Las reglas de paquetes incluyen una característica de registro por diario. El registro por diario le permite resolver problemas relacionados con NAT y con el filtrado.

Puede utilizar el diario para crear un archivo de anotaciones de las acciones de reglas que se produjeron para cada regla de paquete. Esto le permite depurar y revisar las reglas. Consultando estos diarios o anotaciones del sistema, también podrá auditar el tráfico que circula hacia dentro y hacia fuera del sistema.

La característica 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 siguiente tabla 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 sistema. 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 este paso:

1. En una línea de mandatos, teclee `DSPJRN JRN(QIPNAT)`, si son diarios de NAT, o `DSPJRN JRN(QIPFILTER)`, si son diarios de filtros IP.

Resolución de problemas relacionados con las reglas de paquetes

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

- La prestación **Rastreo de comunicaciones de i5/OS** le permite ver todo el 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. Esto hace que el sistema sea vulnerable a los ataques. Coloque los nombres de los conjuntos de filtro dentro de la sentencia FILTER_INTERFACE en el mismo orden en que están definidos físicamente en el archivo.

  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 caso de i5/OS, emita el mandato Eliminar tabla TCP/IP (RMVTCPTBL). Si se queda bloqueado fuera de la aplicación System i Navigator, este mandato sirve también para volver y reparar las reglas.

  Nota: El mandato Eliminar tabla TCP/IP también inicia los servidores de redes privadas virtuales (VPN), pero solo si los servidores VPN (IKE y ConMgr) ya se estaban ejecutando antes.
- Si se propone utilizar NAT, es muy importante **permitir el reenvío de datagramas IP** en la configuración TCP/IP del sistema. Utilice el mandato Cambiar atributos de TCP/IP (CHGTCPA) para verificar que el valor del reenvío de datagramas IP es 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 la conversión de direcciones de red (NAT) pueda deshacer la conversión, esta dirección debe ser direccionable en la ruta de retorno al sistema y debe pasar por la línea correcta.

  Nota: Si la plataforma System i tiene conectada más de una red o más de una línea, debe tomar medidas de precaución especiales al direccionar el tráfico de entrada. El tráfico de entrada se maneja en cualquier línea en la que entre, que podría no ser la línea correcta que está a la espera de deshacer la conversión.
- Hay que **ver los mensajes de error y de aviso** del archivo `EXPANDED.OUT` para asegurarse de que las reglas están colocadas en el orden deseado. Cuando verifica y activa un conjunto de filtros, estos se

fusionan con las reglas que System i Navigator haya generado. 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, siga estos pasos para abrirlo desde el editor de reglas de paquetes:

1. Acceda al editor de reglas de paquetes de System i Navigator.
2. En el menú Archivo, seleccione **Abrir**.
3. Vaya al directorio QIBM/UserData/OS400/TCPIP/PacketRules/ o al directorio en el que ha guardado las reglas de paquetes, si es distinto del predeterminado.
4. En la ventana Abrir archivo, seleccione el archivo **EXPANDED.OUT**. Aparecerá el archivo EXPANDED.OUT.
5. Seleccione el archivo EXPANDED.OUT y pulse **Abrir**.

El archivo EXPANDED.OUT es solamente informativo. No puede editarlo.

Conceptos relacionados

"Caso practico: correlacionar direcciones IP utilizando NAT" en la página 2
En este caso práctico, su empresa utiliza la conversión de direcciones de red (NAT) estática para correlacionar sus direcciones IP privadas con direcciones públicas.

Tareas relacionadas

"Acceder al editor de reglas de paquetes" en la página 22
Puede utilizar 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 proporcionados en el sistema.

Referencia relacionada

"Crear reglas de filtro IP" en la página 24
Cuando se crea un filtro, se especifica una regla que rige el tráfico IP que circula hacia dentro y hacia afuera del sistema.

Información relacionada con Filtrado IP y conversión de direcciones de red

En las publicaciones IBM Redbooks encontrará información relacionada con el temario Filtrado IP y conversión de direcciones de red. Puede ver o imprimir cualquiera de los archivos PDF.

IBM Redbooks

- **TCP/IP Tutorial and Technical Overview** 
  Aquí puede encontrar información sobre temas de seguridad relacionados con redes TCP/IP.
- **V4 TCP/IP for AS/400: More Cool Things Than Ever** 
  Aquí puede encontrar algunos casos prácticos que muestran el uso de NAT y del filtrado IP de paquetes.

  Referencia relacionada

  "Archivo PDF de Filtrado IP y conversión de direcciones de red" en la página 1
  Puede ver e imprimir un archivo PDF de esta información.

Información sobre licencia de código y exención de responsabilidad

IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación, a partir de los que puede generar funciones similares adaptadas a sus necesidades específicas.

SUJETO A LAS GARANTÍAS ESTATUTARIAS QUE NO PUEDAN EXCLUIRSE, IBM Y LOS DESARROLLADORES Y SUMINISTRADORES DE PROGRAMAS DE IBM NO OFRECEN NINGUNA GARANTÍA NI CONDICIÓN, YA SEA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO DETERMINADO Y NO VULNERACIÓN CON RESPECTO AL PROGRAMA O AL SOPORTE TÉCNICO, SI EXISTE.

BAJO NINGUNA CIRCUNSTANCIA, IBM Y LOS DESARROLLADORES O SUMINISTRADORES DE PROGRAMAS DE IBM SE HACEN RESPONSABLES DE NINGUNA DE LAS SIGUIENTES SITUACIONES, NI SIQUIERA EN CASO DE HABER SIDO INFORMADOS DE TAL POSIBILIDAD:

1. PÉRDIDA DE DATOS O DAÑOS CAUSADOS EN ELLOS;
2. DAÑOS ESPECIALES, ACCIDENTALES, DIRECTOS O INDIRECTOS, O DAÑOS ECONÓMICOS DERIVADOS;
3. PÉRDIDAS DE BENEFICIOS, COMERCIALES, DE INGRESOS, CLIENTELA O AHORROS ANTICIPADOS.

ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LA LIMITACIÓN DE LOS DAÑOS DIRECTOS, ACCIDENTALES O DERIVADOS, POR LO QUE PARTE DE LAS LIMITACIONES O EXCLUSIONES ANTERIORES, O TODAS ELLAS, PUEDE NO SER PROCEDENTE EN SU CASO.

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en los EE.UU.

Es posible que en otros países IBM no ofrezca los productos, los servicios o los dispositivos que se describen en este documento. Póngase en contacto con el representante local de IBM que le informará sobre los productos y servicios disponibles actualmente en su área. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar puede utilizarse cualquier otro producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran alguno de los temas tratados en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo siguiente no puede aplicarse en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciatarios de este programa que deseen obtener información acerca de él para: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código de Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Cualquier información de rendimiento que aparezca en este documento ha sido determinada en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos podrían ser distintos. Algunas mediciones se han realizado en sistemas en fase de desarrollo y, por lo tanto, no hay ninguna garantía que estas mediciones sean las mismas en los sistemas normalmente disponibles. Además, algunas mediciones podrían haberse estimado mediante extrapolación. Los resultados reales podrían ser diferentes. Los usuarios de este documento deberían verificar los datos aplicables para su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, compatibilidad ni de ninguna otra afirmación relacionada con productos no IBM. Las cuestiones relativas a las capacidades de productos no IBM deben dirigirse a los proveedores de dichos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para que los ejemplos sean lo más completos posible, incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por alguna empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en el lenguaje fuente, que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de la forma deseada sin tener que efectuar ningún pago a IBM, con el objetivo de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

Cada copia o parte de estos programas de ejemplo o trabajos derivados de los mismos, deben incluir el siguiente aviso de copyright:

© (el nombre de su empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de la interfaz de programación

Esta publicación de Filtrado de IP y conversión de direcciones de red documenta interfaces de programación que permiten al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

AS/400
i5/OS
IBM
IBM (logotipo)
OS/400
Redbooks
System i

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Microsoft, Windows y el logotipo Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN ″TAL CUAL″, SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA

UN FIN DETERMINADO.

Impreso en España