



iSeries

Networking Security

IP filtering and network address translation (NAT)

Version 5 Release 3





@server

iSeries

Networking Security

IP filtering and network address translation (NAT)

Version 5 Release 3

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 43.

Sixth Edition (August 2005)

This edition applies to version 5, release 3, modification 0 of OS/400 Operating System (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 2000,2005. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Part 1. IP filtering and network address translation 1

Chapter 1. Print this topic 3

Chapter 2. Packet rules scenarios 5

Packet rules scenario: Map IP addresses (static NAT)	5
Packet rules scenario: Create filter rules to allow HTTP, Telnet, and FTP	7
Packet rules scenario: Combine NAT and IP filtering	9
Packet rules scenario: Hide IP addresses (masquerade NAT)	13

Chapter 3. Packet rules concepts 17

Packet rules terminology	17
Packet rules versus other iSeries security solutions	18
Network address translation (NAT)	18
Static (map) NAT	19
Masquerade (hide) NAT	20
Masquerade (port-mapped) NAT	21
IP filtering.	21
Sample filter statements	22
IP packet header.	23
Organize NAT rules with IP filter rules	23
Organize multiple IP filter rules	24
Spoof protection.	24

Chapter 4. Plan for packet rules 25

Packet rules: User authority requirements	25
Packet rules: System requirements	25
Packet rules: Planning worksheet	26

Chapter 5. Configure packet rules 27

Access packet rules	28
Define addresses and services	28
Create NAT rules	29
Create IP filter rules	29
Define IP filter interfaces	30
Include files in packet rules	31
Make comments in packet rules	31
Verify packet rules	31
Activate packet rules	32

Chapter 6. Manage packet rules 33

Deactivate packet rules	33
View packet rules	33
Edit packet rules	34
Backup packet rules	34
Journal and audit packet rules actions	34

Chapter 7. Troubleshoot packet rules 37

Chapter 8. Related information for packet rules 39

Part 2. Appendixes. 41

Appendix. Notices 43

Trademarks	44
Terms and conditions for downloading and printing publications	44

Part 1. IP filtering and network address translation

IP filtering and network address translation (NAT) act like a firewall to protect your internal network from intruders. IP filtering lets you control what IP traffic to allow into and out of your network. Basically, it protects your network by filtering packets according to rules that you define. NAT, on the other hand, allows you to hide your unregistered private IP addresses behind a set of registered IP addresses. This helps to protect your internal network from outside networks. NAT also helps to alleviate the IP address depletion problem, since many private addresses can be represented by a small set of registered addresses.

Note: **Packet rules** is the combination of IP filtering and NAT. When you see the term, packet rules, used in this topic it means that the subject applies to both of those components.

Review the topics below to help you understand the whys, whats, and hows of packet rules.

Print this topic

If you prefer a hardcopy version of this information, go here to print the PDF.

Packet rules scenarios

Review these scenarios to become familiar with some of the more common uses of packet rules. Each scenario provides you with an illustration and a sample configuration.

Packet rules concepts

You should have at least a basic knowledge of packet rules technologies and concepts before you begin. This topic provides you with information about IP filtering and NAT. It includes topics such as mapping and hiding addresses. It also includes a list of iSeries™ specific terminology.

Plan for packet rules

Planning is extremely important to determining what resources you need to protect and from whom you need to protect them. This topic provides you with a planning worksheet and other information to help you make an informed decision about what is best for your particular security needs.

Configure packet rules

This topic provides you with information about what you can do with packet rules and how to do it.

Manage packet rules

This topic describes various tasks you can perform to manage your packet rules. Some of the features include journaling, editing, and viewing your rules files.

Troubleshoot packet rules

Refer to this topic when you experience errors and to make sure you are addressing potential problem areas.

Related information for packet rules

Go here for links to other sources of packet rules information and related topics.

In addition to the information contained in this topic, use the online help available from the Packet Rules Editor in iSeries Navigator. The iSeries Navigator online help offers tips and techniques for making the most of packet rules, including **How do I...** help, **Tell me about...** help, and extensive contextual help.


Chapter 1. Print this topic

To view or download the PDF version, select Packet rules (about 245 KB).

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...**
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site (<http://www.adobe.com/products/acrobat/readstep.html>) .

Chapter 2. Packet rules scenarios

Use the following scenarios to help explain how you can use NAT and IP filtering to protect your network. Each scenario includes a diagram and sample configuration.

- **Packet rules scenario: Map your IP addresses (static NAT)**

In this scenario, your company uses static NAT to map its private IP addresses to public addresses.

- **Packet rules scenario: Create filter rules to allow HTTP, Telnet, and FTP**

In this scenario, your company uses IP filtering to restrict the IP traffic that can access its Web server to HTTP, Telnet, and FTP.

- **Packet rules scenario: Combine NAT and IP filtering**

In this scenario, your company uses both NAT and IP filtering to hide its PCs and Web server behind a single, public, IP address and to allow other companies to access the Web server.

- **Packet rules scenario: Hide your IP addresses (masquerade NAT)**

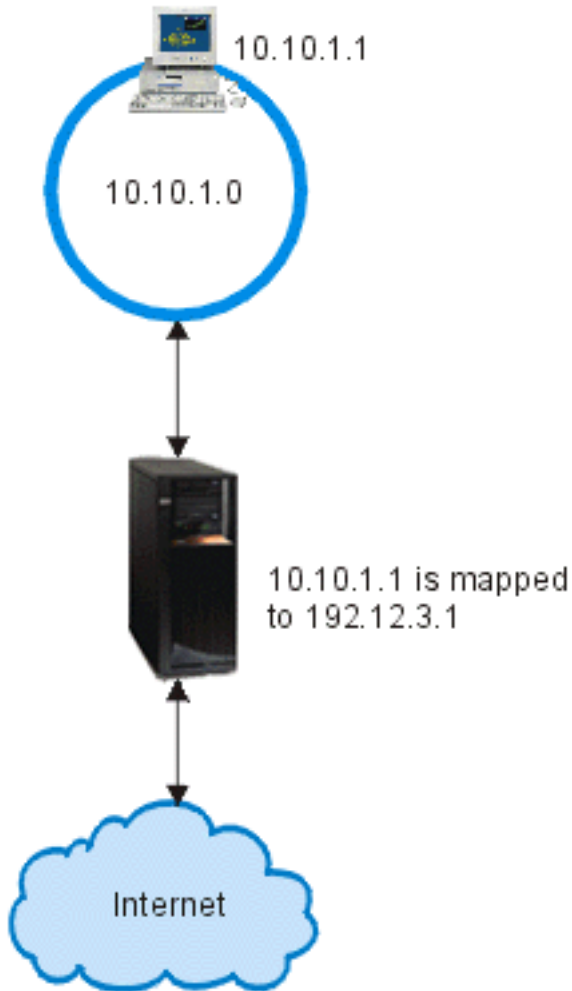
In this scenario, your company uses masquerade NAT to hide the private addresses of your PCs, while at the same time, allowing your employees to access the Internet

Note: In each scenario, the 192.x.x.x IP addresses represent public IP addresses. All addresses are for example purposes only.

Packet rules scenario: Map IP addresses (static NAT)

Situation

You own your own company, and you decide to start a private network. However, you have never registered or acquired permission to use public IP addresses. Everything was fine until you wanted to access the Internet. It turns out that your company's address range is registered to someone else, so you think your current setup is obsolete. You really need to allow public users access to your Web server. What should you do?



Solution

You could use static NAT. Static NAT assigns one original (private) address to one registered (public) address. Your iSeries maps this registered address to your private address. The registered address allows your private address to communicate with the Internet. Essentially, it forms a bridge between the two networks. Communication can then be initiated from either network.

By using static NAT, you can keep all of your current internal IP addresses and still access the Internet. You will need to have one registered IP address for each private address that accesses the Internet. For example, if you have 12 users, you need 12 public IP addresses to map to your 12 private addresses.

In the illustration above, the NAT address, 192.12.3.1, sits unusable, like a shell, waiting for information to come back. When the information returns, NAT maps the address back to the PC. When static NAT is active, any inbound traffic destined directly to the address 192.12.3.1 will never get to that interface because it is only representing your internal address. The real private address 10.10.1.1 is the actual destination, even though (to the world outside the iSeries) it appears that 192.12.3.1 is the desired IP address.

Configuration

To configure the packet rules described in this scenario, you should use the **Address Translation** wizard in iSeries Navigator. The wizard requires the following information:

- Private address you want to map: 10.10.1.1
- Public address to which you want to map the private address: 192.12.3.1
- The name of line over which the address mapping takes place: TRNLINE

To use the **Address Translation** wizard, follow these steps:

1. In iSeries Navigator, select **your server** → **Network** → **IP policies**.
2. Right-click **Packet Rules**, and select **Rules Editor**.
3. From the **Welcome Packet Rules Configuration** dialog, select **Create a new packet rules file**, and click **OK**.
4. From the **Wizards** menu, select **Address Translation**, and follow the wizard's instructions to configure the map address translation packet rules.

Your packet rules should look like this:

```
-----  
Statements to map 10.1.1.1 to 192.12.3.1 over TRNLINE  
-----  
ADDRESS MAPPRIVATE1  IP = 10.1.1.1  
ADDRESS MAPPUBLIC1  IP = 192.12.3.1  
MAP MAPPRIVATE1  TO MAPPUBLIC1  LINE = TRNLINE  
-----
```

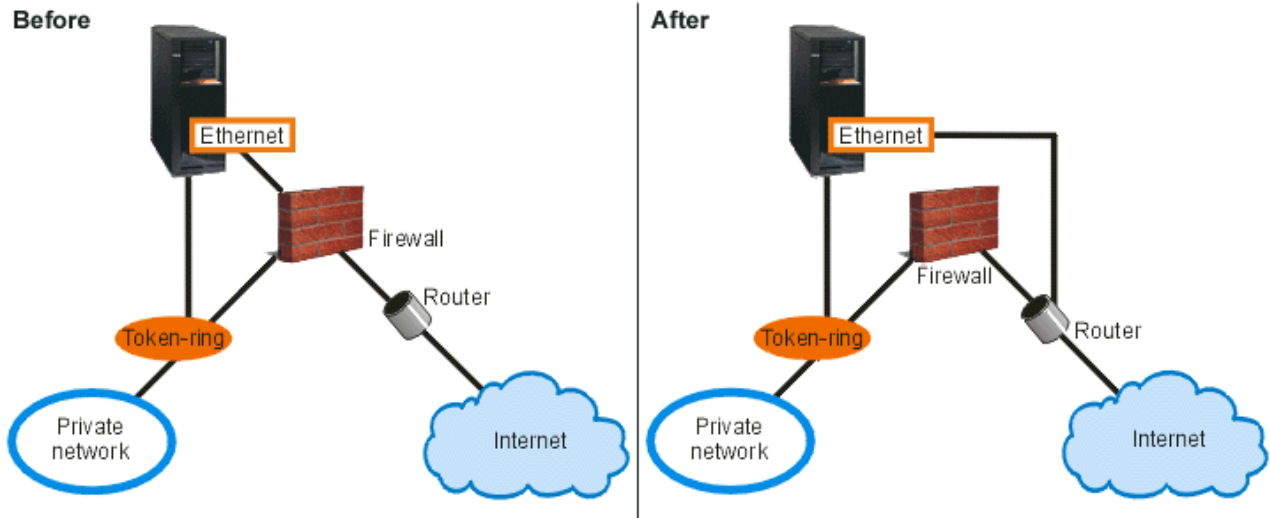
After you finish creating these rules and any others you determine you need, you should verify them to ensure they will activate without errors. After that, you can activate them.

Note: The token ring line that is defined above (LINE=TRNLINE) must be the line that 192.12.3.1 uses. This static NAT will not work if 10.10.1.1 uses the defined token ring line above. Whenever you use NAT, you should also enable IP forwarding. See the Troubleshoot packet rules section for details.

Packet rules scenario: Create filter rules to allow HTTP, Telnet, and FTP

Situation

You want to provide Web applications to your customers, but your current firewall is working overtime and you do not want to add additional stress to it. Your colleague suggests running the applications outside of the firewall. However, from the Internet, you only want HTTP, FTP, and Telnet traffic to have access to your iSeries Web server. What should you do?



Solution

IP filtering allows you to set rules which define what information you want to permit. In this scenario you will write filter rules that permit HTTP, FTP, and Telnet traffic (inbound and outbound) to the Web server, which is your iSeries in this case. The public address of the server is 192.54.5.1, and the private IP address is 10.1.2.3.

Configuration

To configure the packet rules described in this scenario, you should use the **Permit A Service** wizard in iSeries Navigator. The wizard requires the following information:

- The type of service you want to permit: HTTP
- The public address of the iSeries server: 192.54.5.1
- The address of the client: Any IP address
- The interface over which the service will run: TRNLINE
- The direction the service will run: INBOUND
- The name you want to use to identify this filter set: external_files

To use the **Permit Service** wizard, follow these steps:

1. In iSeries Navigator, select **your server** -> **Network** -> **IP policies**.
2. Right-click **Packet Rules**, and select **Rules Editor**.
3. From the **Welcome Packet Rules Configuration** dialog, select **Create a new packet rules file**, and click **OK**.
4. From the **Wizards** menu, select **Permit A Service**, and follow the wizard's instructions to create the filter rules.

These packet rules permit HTTP traffic in and out of the system. Your packet rules should look like this:

```
-----
Statements to permit inbound HTTP over 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
-----
```

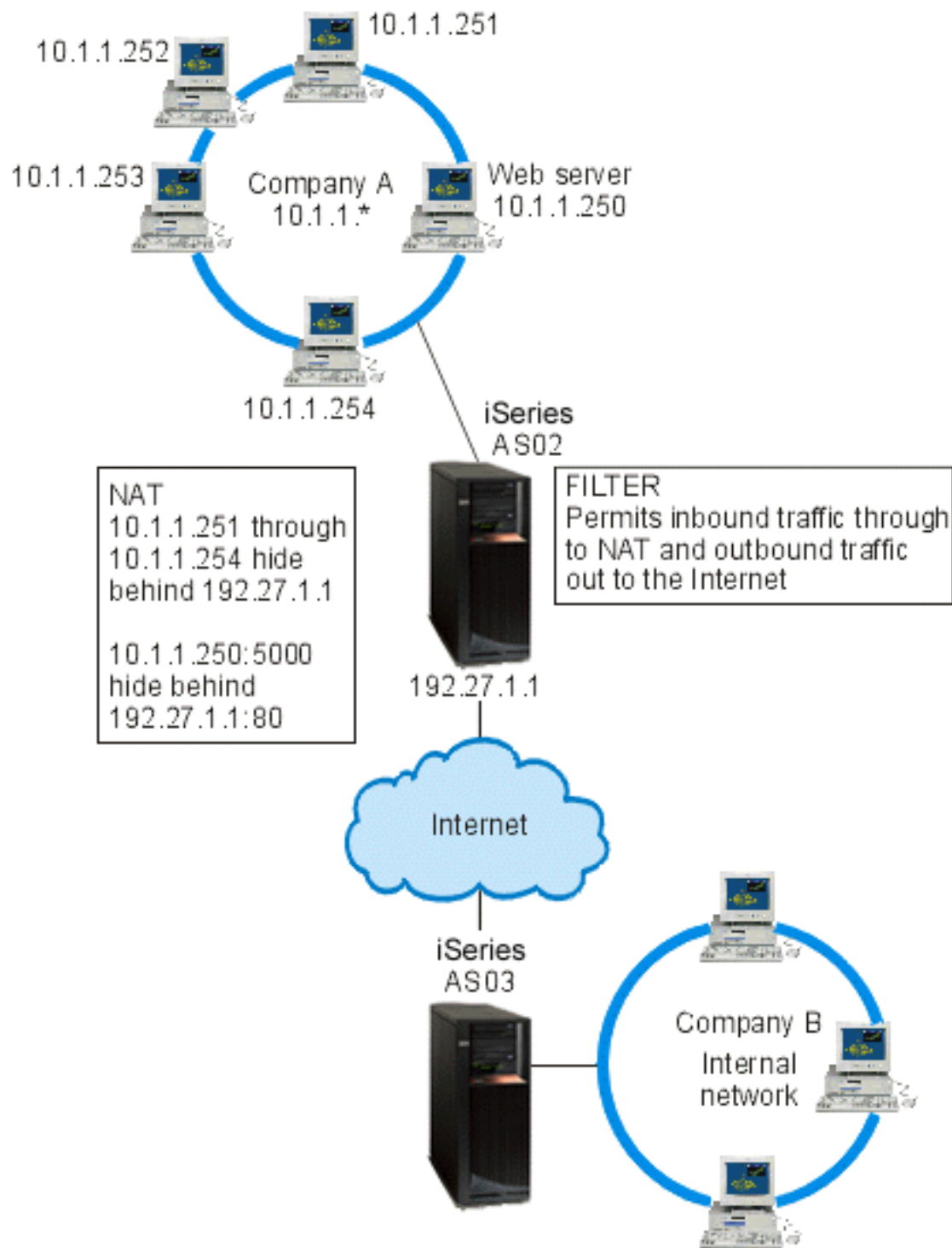
Use the **Permit a Service** wizard two more times to create filter rules that permit FTP traffic and Telnet traffic in and out of the system.

After you finish creating these filter rules, you should verify them to ensure they will activate without errors. After that, you can activate them.

Packet rules scenario: Combine NAT and IP filtering

Situation

Your business has a moderately sized internal network that uses an iSeries as its gateway. You want to transfer all Web traffic from the gateway iSeries to a dedicated Web server, behind the gateway. The Web server runs on port 5000. You want to hide all of your private PCs and the Web server behind an address on the gateway iSeries interface; AS02 in the diagram below. You also want to allow other companies to access the Web server. What should you do?



Solution

You could use IP filtering and NAT together to configure:

1. Hide NAT to hide your PCs behind a public address, 192.27.1.1, so they can access the Internet.
2. Port-mapped NAT to hide your Web server address, 10.1.1.250, and port number, 5000, behind a public address, 192.27.1.1, and port number, 80. Notice that both NAT rules are hidden behind

192.27.1.1. This is acceptable as long as the addresses you are hiding do not overlap. The port-mapped NAT rule will only allow externally initiated traffic on port 80 to access your system. If the externally initiated traffic does not match the exact address and port number, NAT will not translate it and the packet will be discarded

3. Rules that filter all inbound traffic destined for your private network through to NAT and any outbound traffic out to the Internet.

Configuration

To configure the hide NAT packet rules described in this scenario, you should use the **Address Translation** wizard in iSeries Navigator. The wizard requires the following information:

- The set of addresses you want to hide: 10.1.1.251 through 10.1.1.254
- The interface address behind which you want to hide the set of addresses: 192.27.1.1

To use the **Address Translation** wizard, follow these steps:

1. In iSeries Navigator, select **your server** -> **Network** -> **IP policies**.
2. Right-click **Packet Rules**, and select **Rules Editor**.
3. From the **Welcome Packet Rules Configuration** dialog, select **Create a new packet rules file**, and click **OK**.
4. From the **Wizards** menu, select **Address Translation**, and follow the wizard's instructions to configure the hide address translation packet rules.

This packet rule will hide your four PCs behind a public address, so they can access the Internet. Your Hide NAT packet rule should look like this:

```
-----  
Statements to hide 10.1.1.251 - 10.1.1.254 behind 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  
-----
```

To configure the port-mapped NAT, follow these steps:

1. Access the Packet Rules Editor from iSeries Navigator.
2. Create a defined address for the Web server address and port 5000:
 - a. From the **Insert** menu, select **Address...**
 - b. On the **General** page, enter **Web250** in the **Address name** field.
 - c. Select **IP addresses** in the **Defined address** drop-down list. Then click **Add** and enter the IP address of the Web server 10.1.1.250 in the edit field.
 - d. Click **OK**.
3. Create a defined address to represent the public address 192.27.1.1:

Note: Since you already created a defined address to represent the public address 192.27.1.1 when you configured the hide NAT packet rules, you can omit this step for this particular scenario and skip to Step 4. However, if you use these instructions to configure the port-mapped NAT for your own network and you did not configure the hide NAT packet rules, then continue with the instructions for this step.

 - a. From the **Insert** menu, select **Address...**
 - b. On the **General** page, enter or select **BEHIND1** in the **Address name** field.
 - c. Select **IP addresses** in the **Defined address** drop-down list. Then click **Add** and enter 192.27.1.1 in the **IP addresses** edit field.
 - d. Click **OK**.

4. Create the port-mapped NAT rule:
 - a. From the **Insert** menu, select **Hide...**
 - b. On the **General** page, select Web250 from the **Hide address name** drop-down list.
 - c. Select **BEHIND1** from the **Behind address name** drop-down list.
 - d. Select **Allow inbound connections**, and enter 5000 in the **Hide port** field.
 - e. Enter 80 in the **Behind port** field.
 - f. Enter 16 and select **seconds** in the **Timeout** fields.
 - g. Enter 64 in the **Maximum conversations** field.
 - h. Select **OFF** from the **Journaling** drop-down list.
 - i. Click **OK**.

This port mapped NAT will hide your Web server address and port number behind a public address and port number. Notice that both NAT rules are hidden behind one common IP address. This is acceptable as long as the addresses you are hiding do not overlap. This port mapped NAT rule will only allow externally initiated traffic on port 80 to access your system.

Your port mapped NAT rule should look like this:

```
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
```

To create the filter rules described in this scenario, follow these steps:

1. Access the Packet Rules Editor from iSeries Navigator.
2. Create a filter rule to permit inbound traffic destined for your private network.
 - a. From the **Welcome Packet Rules Configuration** dialog, select **Create a new packet rules file**, and click **OK**.
 - b. From the **Insert** menu, select **Filter...**
 - c. On the **General** page, enter external_rules in the **Set name** field.
 - d. Select **PERMIT** from the **Action** drop-down list.
 - e. Select **INBOUND** from the **Direction** drop-down list.
 - f. Select = and * from the **Source address name** drop-down lists.
 - g. Select = and enter 192.27.1.1 in the **Destination address name** fields.
 - h. Select **OFF** from the **Journaling** drop-down list.
 - i. On the **Services** page, select **Service**,
 - j. Select **TCP** from the **Protocol** drop-down list.
 - k. Select = and * from the **Source port** drop-down lists.
 - l. Select = and * from the **Destination port** drop-down lists.
 - m. Click **OK**.
3. Create a filter rule to permit outbound traffic from your private network to the Internet.
 - a. From the **Welcome Packet Rules Configuration** dialog, select **Open an existing packet rules file**, and click **OK**.
 - b. From the **Open file** dialog, select the external_rules file, and click **Open**.
 - c. From the **Insert** menu, select **Filter...**
 - d. On the **General** page, select external_rules from the **Set name** drop-down list.
 - e. Select **PERMIT** from the **Action** drop-down list.
 - f. Select **OUTBOUND** from the **Direction** drop-down list.
 - g. Select = and enter 192.27.1.1 in the **Source address name** fields.
 - h. Select = and * from the **Destination address name** drop-down lists.

- i. Select **OFF** from the **Journaling** drop-down list.
 - j. On the **Services** page, select **Service**,
 - k. Select **TCP** from the **Protocol** drop-down list.
 - l. Select = and * from the **Source port** drop-down lists.
 - m. Select = and * from the **Destination port** drop-down lists.
 - n. Click **OK**.
4. Define a filter interface for the filter set that you created:
 - a. From the **Insert** menu, select **Filter interface...**
 - b. Select **Line name** and select **TRNLINE** from the **Line name** drop-down list.
 - c. On the **Filter sets** page, select **external_rules** from the **Filter set** drop-down list. Then, click **Add**.
 - d. Click **OK**.

These filters, in conjunction with the HIDE statement, will permit any inbound traffic destined for your private network through to NAT and any outbound traffic out to the Internet. However, NAT will only allow externally initiated traffic on port 80 to enter the server. NAT will not translate externally initiated traffic that does not match the port mapped NAT rule. Your filter rules should look like this:

```
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
```

This statement binds (associates) the 'external_rules' filter set with the correct physical interface.

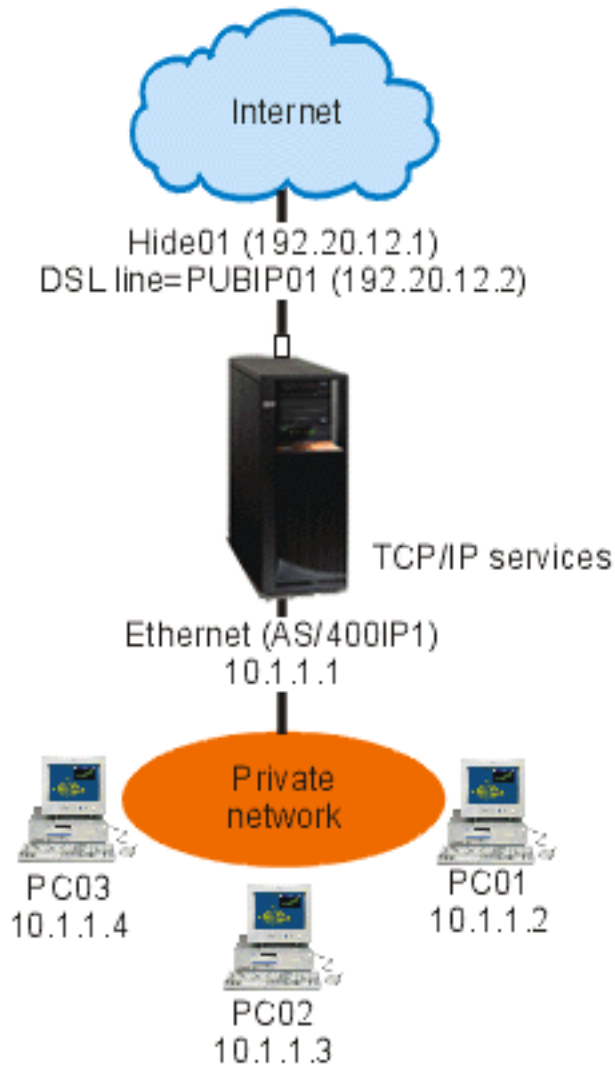
```
FILTER_INTERFACE LINE = TRNLINE SET = external_files
```

After you finish creating these filter rules, you should verify them to ensure they will activate without errors. After that, you can activate them.

Packet rules scenario: Hide IP addresses (masquerade NAT)

Situation

You have a small company and you want to allow HTTP service on your iSeries. You have a model 170e with one Ethernet card and three PCs. Your Internet Service Provider (ISP) provides you with a DSL connection and a DSL modem. The ISP also assigns you the following public IP addresses: 192.20.12.1 and 192.20.12.2. All of your PCs have 10.1.1.x addresses on the internal network. You want to ensure that the private addresses of your PCs remain hidden to prevent external users from initiating communications with your internal network, while at the same time, allowing your employees to access the Internet. What should you do?



Solution

Hide your PC addresses, 10.1.1.1 through 10.1.1.4, behind the public address, 192.20.12.1. You will then be able to run TCP/IP services from the 10.1.1.1 address. Range NAT (hiding a range of internal addresses) will protect your PCs from communication that is initiated outside your network because for range NAT to start, traffic must be initiated internally. However, range NAT will not protect the iSeries interface. You will need to filter traffic to protect your iSeries from receiving untranslated information.

Configuration

To configure the packet rules described in this scenario, you should use the **Address Translation** wizard in iSeries Navigator. The wizard requires the following information:

- The set of addresses you want to hide: 10.1.1.1 through 10.1.1.4
- The interface address behind which you want to hide the set: 192.20.12.1

To use the **Address Translation** wizard, follow these steps:

1. In iSeries Navigator, select **your server** → **Network** → **IP policies**.
2. Right-click **Packet Rules**, and select **Rules Editor**.

3. From the **Welcome Packet Rules Configuration** dialog, select **Create a new packet rules file**, and click **OK**.
4. From the **Wizards** menu, select **Address Translation**, and follow the wizard's instructions to configure the hide address translation packet rules.

Your packet rules should look like this:

```
-----  
Statements to hide 10.1.1.1 - 10.1.1.4 behind 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  
-----
```

After you finish creating these filter rules, you should verify them to ensure they will activate without errors. After that, you can activate them.

Chapter 3. Packet rules concepts

Packet rules comprise both network address translation (NAT) rules and IP filtering rules. These two components run at the IP layer of the TCP/IP stack and help protect your system against potential risks that are commonly associated with TCP/IP traffic.

To better understand how packet rules work, you should be familiar with these concepts and how they apply to your iSeries:

- **Packet rules terminology**
Provides you with a list of iSeries specific terminology with which you should be familiar.
- **Packet rules versus other iSeries security solutions**
How do packet rules compare to other iSeries security solutions? Go here to find out.
- **Network address translation (NAT)**
There are several different types of address translation. This topic provides you with the information you need to determine which is right for your network.
- **IP filtering**
Refer to this topic for more information about how the IP filtering component of packet rules works.
- **Organize NAT rules with IP filter rules**
You can use NAT rules and IP filter rules separately or together. This topic describes how the two components work together.
- **Organize multiple IP filter rules**
When you create your filter rules, the system processes them in a certain order. This topic explains how multiple filter rules are processed and provides an example.
- **Spoof protection**
This page defines spoof protection and tells you why you should use it.

Packet rules terminology

The following list contains some iSeries specific terms that are used throughout this Information Center topic.

border

Border is a public address that forms a border between a trusted and an untrusted network. It describes the IP address as an actual interface on the iSeries. The system needs to know the "type" of address you are defining. For example, your PCs IP address is trusted, but your server's public IP address is border.

firewall

A logical barrier around systems in a network. A firewall consists of hardware, software, and a security policy that controls the access and flow of information between secure (trusted) systems and nonsecure (untrusted) systems.

maxcon

Maxcon is the number of conversations that can be active at one time. The system asks you to define this number when you set up NAT masquerade rules. The default value is 128. Maxcon only pertains to Masquerade NAT rules.

NAT conversation

A NAT conversation is a relationship between any of the following IP addresses and port numbers:

- Private source IP address and source port number (without NAT)
- Public (NAT) source IP address and public (NAT) source port number

- Destination IP address and port number (an external network)

PPP filter identifier

A PPP filter identifier allows you to apply filter rules to an interface that has been defined in a point-to-point profile. The PPP filter identifier also links the filter rules to groups of users in a point-to-point profile. Because the point-to-point profile is associated with a specific IP address, the filter identifier implicitly defines the interface to which the rules apply. To learn more, refer to this scenario, *Manage remote user access to resources using Group Policies and IP filtering in the Remote Access Services: PPP connections* topic.

timeout


Timeout controls the amount of time a conversation is allowed to last. If you have Timeout set too short, the conversation is stopped too quickly. The default value is 16.

Packet rules versus other iSeries security solutions

Your iSeries has integrated security components that can protect your system from several types of risks. Packet rules, for one, provide an economical way for you to secure your system. In some cases, packet rules can provide everything you need without any additional purchases. However, the security of your system should take precedence over cost.

In high risk situations, such as securing a production system or securing communications between your iSeries and other systems in a network, you should investigate other iSeries security solutions to broaden your protection.

Refer to these Information Center topics for information that will help to ensure that your security strategy includes multiple lines of defense:

- **IBM® SecureWay®: iSeries and the Internet**
This topic provides a wealth of information about the risks and solutions you should consider before using the Internet.
- **Secure Sockets Layer (SSL)**
SSL provides secure connections between server applications and their clients. This topic includes information about how you can enable SSL on your iSeries applications.
- **Virtual private networking (VPN)**
VPN allows your company to securely extend its private intranet over the existing framework of a public network, such as the Internet. This topic describes VPN and tells you how to use it on your iSeries.
- **Tips and Tools for Securing your iSeries** 
This PDF book provides you with high-level information about how you can enhance security on your iSeries.

Network address translation (NAT)

IP addresses are depleting rapidly due to widespread Internet growth. Organizations use private networks, which allows them to select any IP addresses they want. However, if two companies have duplicate IP addresses and they attempt to communicate with each other, they will have problems. In order to communicate on the Internet, you must have a unique, registered address. Network address translation (NAT) allows you to access the Internet safely without having to change your private network IP addresses. Just as the name implies, NAT is a mechanism that translates one Internet Protocol (IP) address into another.

Packet rules contains three methods of NAT. You commonly use NAT to map addresses (static NAT) or hide addresses (masquerade NAT). Review the links below for more detailed information about the various forms of NAT:

- Static (map) NAT

- Masquerade (hide) NAT
- Masquerade, or hide (port-mapped) NAT

By hiding or mapping addresses, NAT solves various addressing problems. The examples below explain some problems that NAT can resolve.

Example 1: Hiding internal IP addresses from public knowledge

You are configuring an iSeries as a public Web server. However, you do not want external networks to know your server's real internal IP addresses. You can create NAT rules that translate your private addresses to public addresses that can access the Internet. In this instance, the "true" address of the server remains hidden, making the server less vulnerable to attack.

Example 2: Converting an IP address for an internal host into a different IP address

You want private IP addresses on your internal network to communicate with Internet hosts. To arrange this, you can convert an IP address for an internal host into a different IP address. You must use public IP addresses to communicate with Internet hosts. Therefore, you use NAT to convert your private IP addresses to public addresses. This ensures that IP traffic from your internal host is routed through the Internet.

Example 3: Making the IP addresses of two different networks compatible

You want to allow a host system in another network, such as a vendor company, to communicate with a specific host in your internal network. However, both networks use private addresses (10.x.x.x), which creates a possible address conflict for routing the traffic between the two hosts. To avoid conflict, you can use NAT to convert the address of your internal host to a different IP address.

Static (map) NAT

Static (map) NAT provides a one-to-one mapping of private IP addresses to public IP addresses. It allows you to map an IP address on your internal network to an IP address that you want to make public.

Static NAT allows communication to be initiated from your internal network or an external network, like the Internet. It is especially useful if you have a server within your internal network that you want to allow public users to access. In this case, you need to create a NAT rule that maps the actual server address to a public address. The public address will become external information. This ensures that private information remains out of the hands of someone who might attack your systems.

The following list highlights the features of static NAT:

- One-to-one mapping
- External and internal network initiation
- The address you associate or map to, can be any address
- The address you associate or map to becomes un-usable as an IP interface
- Does not use port-mapped NAT

Attention

Use caution if you decide to map a PC to the "well-known" address of the iSeries. The well-known address is the IP address reserved for most Internet and intranet traffic. If you do map to this IP address, NAT will translate all traffic and send it to the internal private address. Since this interface will be reserved for NAT, your iSeries and the interface become unusable.

Review Packet rules scenario: Map IP addresses for a scenario and illustration of static NAT.

Masquerade (hide) NAT

Masquerade (hide) NAT allows you to keep the outside world (outside the iSeries) from knowing your PC's actual address. NAT routes traffic from your PC to your iSeries, which essentially makes the iSeries the gateway for your PC. Here is how it works.

Masquerade NAT allows you to translate multiple IP addresses to another single IP address. You can use masquerade NAT to *hide* one or more IP addresses on your internal network behind an IP address that you want to make public. This public address is the address to which the private addresses are translated and has to be a defined interface on your iSeries server. To be a defined interface, you must define the public address as a BORDER address.

Hiding multiple addresses

To hide multiple addresses, you specify a range of addresses that NAT should translate through the iSeries server. Here is the general process:

1. The translated IP address replaces the source IP address. This occurs in the IP header of the IP packet.
2. The IP source port number (if there is one) in a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header is replaced with a temporary port number.
3. An existing conversation is the relationship between the new IP source address and port number.
4. This existing conversation allows your NAT server to untranslate IP datagrams from the outside machine.

To view an IP datagram header, visit [IP packet header](#).

When you use masquerade NAT, an internal system initiates traffic. When this happens, NAT translates the IP packet as it passes through the iSeries NAT server. Masquerade NAT is a great choice because external hosts cannot initiate traffic into your network. As a result, your network gains additional protection from an outside attack. Also, you only need to purchase a single public IP address for multiple internal users.

The following list highlights the features of masquerade NAT:

- Private IP address or range of IP addresses are bound behind a public IP address on the NAT machine
- Internal network initiation only
- Port numbers are associated with random port numbers. This means that both the address and the port number are hidden from the Internet.
- The registered address on the NAT machine is a usable interface outside of NAT

Attention

- You must set MAXCON high enough to accommodate the number of conversations you want to use. For example, if you are using FTP, your PC will have two conversations active. In this case, you will need to set MAXCON high enough to accommodate multiple conversations for each PC. You need to decide how many concurrent conversations you want to allow in your network. The default value is 128.
- You must have TIMEOUT (a HIDE rule statement) set high enough to allow enough time for conversations between PCs to end. For Hide NAT to occur properly, there must be an internal conversation in progress. The timeout value tells the code how long to wait for a reply to this internal conversation. The default value is 16.
- Masquerade NAT only supports the following protocols: TCP, UDP, and ICMP.
- Whenever you use NAT, you must enable IP forwarding. Use the CHGTCPA (Change TCP/IP Attributes) command to verify that you set IP datagram forwarding to YES.

Remember to view the scenario and illustration in [Hide your IP addresses \(masquerade NAT\)](#) to show you an example of Masquerade or Hide NAT.

Masquerade (port-mapped) NAT

Port-mapped NAT is a variation of masquerade NAT. How do they differ? In port-mapped NAT you can specify both the IP address and the port number to translate. This allows both your internal PC and the external machine to initiate IP traffic. You can use this if the external machine (or client) wants to access machines or servers inside your network. Only IP traffic that matches both the IP address and the port number is allowed access. Here is how it works:

Internal initiation

As the internal PC with *Address 1: Port 1* initiates traffic to an outside machine, the translating code will check the NAT rule file for *Address 1: Port 1*. If both the source IP address (Address 1) and the source port number (Port 1) match the NAT rule, then NAT starts the conversation and performs the translation. The specified values from the NAT rule replace the IP source address and source port number. *Address 1: Port 1* is replaced with *Address 2: Port 2*.

External initiation

An external machine initiates IP traffic with the destination IP address of *Address 2*. The destination port number is *Port 2*. The NAT server will untranslate the datagram with or without an "existing conversation." In other words, NAT will automatically create a conversation if one does not already exist. *Address 2: Port 2* is untranslated to *Address 1: Port 1*.

The following list highlights the features of masquerade port-mapped NAT:

- One-to-one relationship.
- External and internal network initiation.
- The registered address the private address hides behind must be defined on the iSeries performing the NAT operations.
- IP traffic outside of NAT operations cannot use the registered address. However, if this address attempts to use a port number that matches the hidden port in the NAT rule, then the traffic will be translated. The interface will be unusable.
- Usually the port numbers are mapped to well-known port numbers, so extra information is not necessary. For example, you could run an HTTP server bound to port 5123, then map this to the public IP and port 80. If you want to hide an internal port number behind another (uncommon) port number, the client needs to be physically told the value of the destination port number. If not, it is difficult for communication to occur.

Attention

- You must set MAXCON high enough to accommodate the number of conversations you want to use. For example, if you are using FTP, your PC will have two conversations active. You will need to set MAXCON high enough to accommodate multiple conversations for each PC. The default value is 128.
- Masquerade NAT only supports the following protocols: TCP, UDP, and ICMP.
- Whenever you use NAT, you must enable IP forwarding. Use the CHGTCPA (Change TCP/IP Attributes) command to verify that IP datagram forwarding is set to YES.

IP filtering

Though not a fully-functional firewall in itself, packet rules provide a solid component that can filter packets for your iSeries. Specifically, the IP filtering component of packet rules allows you to control what IP traffic you want to allow into and out of your company's network. Use IP filtering to help protect your system by filtering packets according to rules that you specify. These rules are based on information found in the IP packet header.

You can apply filter rules to multiple lines or you can apply different rules to each line. Filter rules are associated with lines, e.g. token ring (trnline), not logical interfaces or IP addresses. The system checks each packet against each rule that you associate with a line. The rules are checked in a sequential process. Once the system matches the packet to a rule, it stops the process and applies the matching rule.

When your system applies a matching rule, it actually performs the action that is specified by that rule. The iSeries supports 3 actions (V4R4 and beyond):

1. PERMIT — allows the packet to process as usual
2. DENY — immediately discards the packet
3. IPSEC — sends the packet through a VPN connection, which you specify in the filter rule

Note: In this case, IPSEC is an action that you can define in your filter rules. Even though this topic does not cover IPsec specifically, it is important to note that filtering and virtual private networking (VPN) are closely related. For more information about VPN, review the Virtual private networking (VPN) topic.

After you apply a rule, the system continues its sequential comparison of rules and packets and assigns actions to all corresponding rules. If the system is unable to find a matching rule for a particular packet, the system automatically discards that packet. The system's default deny rule ensures that the system automatically discards any packet that is not matched to a filter rule. Note that if a filter rule is designed to permit traffic in only one direction, such as inbound or outbound, the system implements the default deny rule in both directions; that is, both inbound and outbound packets are discarded.

Sample filter statements

The purpose of this sample filter statement is to demonstrate the proper syntax for creating filter rules on your iSeries and to show you how the various statements work together in a file. Use them as examples only.

A common filter statement may look like this:

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

This filter will permit all traffic entering the interface (INBOUND) that has a source address of 162.56.39.100, a source port of 80, and destination port greater or equal to 1024.

Since IP traffic typically flows both INBOUND and OUTBOUND over a connection it is common to have two related statements to permit traffic in both directions. These two statements are called mirrors of each other and can be seen in the example that follows:

```
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
```

You may notice that both of these filter statements have the same set name, TestFilter. All filters with the same set name are considered to be in the same set. You can have any number of filters in a set. When you activate filters within a given set they are processed in the order in which they appear in the file.

A filter statement alone will not have any effect when you activate rules. You must apply the filter set to a filter interface. An example of applying the set, TestFilter, to an Ethernet line interface is as follows:

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

After you activate these rules, only IP traffic permitted by the TestFilter set will be permitted over ETH237.

Note: The system adds a default DENY ALL TRAFFIC rule to the end of any activated filters on an interface. So, when you apply rules to the interface through which you are configuring the iSeries, it is very important that you permit your own workstation or that of anyone else who may be configuring the iSeries. Failure to do so will result in a loss of communication with the iSeries. You can also apply multiple sets to a filter interface statement like this:

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

These sets will be processed in the same order as you list them in the filter interface statement (set1, set2, and finally, set3). Remember for each set, the filters within it are processed in the order in which they appear in the file. This means that the ordering of filters between different sets is irrelevant. Filter order only matters when filters are in the same set.

IP packet header

You can create filter rules to refer to various portions of IP, TCP, UDP, and ICMP headers. The following list includes the fields you refer to in a filter rule that make up the IP packet header:

- Source IP address
- Protocol (for example, TCP, UDP)
- Destination IP address
- Source port
- Destination port
- IP datagram direction (inbound, outbound, or both)
- TCP SYN bit

For example, you may create and activate a rule that filters a packet based on the destination IP address, source IP address, and direction (inbound). In this case, the system matches all incoming packets (according to their origin and destination addresses) with corresponding rules. Then the system takes the action that you specified in the rule. The system discards any packets that are *not* permitted in your filter rules. This is called the default deny rule.

Note: The system applies the default deny rule to packets only if the physical interface has at least one active rule. This rule can be customer-defined or generated by iSeries Navigator. Regardless of whether the filter rule permits inbound traffic or outbound traffic, the system implements the default deny rule in both directions. If there isn't a filter rule active on the physical interface, then the default deny rule will not work.

Organize NAT rules with IP filter rules

NAT and IP filtering work independent of each other. Even so, you can still use NAT in conjunction with IP filtering. If you choose to apply only NAT rules, your system will only perform address translation. Similarly, if you choose to apply only IP filter rules, your system will only filter IP traffic. However, if you apply both types of rules, your system will translate and filter addresses. When you use NAT and filtering together, the rules occur in a specific order. For inbound traffic, NAT rules process first. For outbound traffic, filter rules process first.

You may want to consider using separate files to create your NAT and filter rules. Although this is not necessary, it will make your filter rules easier to read and troubleshoot. Either way (separate or together), you will receive the same errors. If you decide to use separate files for your NAT and filter rules, you can still activate both sets of rules. However, you should make sure your rules do not interfere with one another.

To activate both NAT and filtering rules at the same time, you need to use the *include* feature. For example, you created File A for filter rules and File B for NAT rules. You can include the contents of File B into File A without rewriting all of your rules. See Include files in packet rules for more information about how to do this.

Organize multiple IP filter rules

When you create filter rules, a filter refers to one rule statement. A set refers to a group of filters. The filters, within a set, are processed top-to-bottom in physical order. Likewise, multiple sets are also processed in physical order within a `FILTER_INTERFACE` statement.

Here is an example where one set contains three filter statements. Whenever you refer to this set, all three rules will be included. It is usually easiest to include all of your filter rules in one set.

```
FILTER SET a11 ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR %
    = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = * FRAGMENTS %
    = HEADERS JRN = FULL
FILTER SET a11 ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR %
    = * PROTOCOL = TCP DSTPORT = * SRCPORT = * FRAGMENTS = NONE %
    JRN = OFF
FILTER SET a11 ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR %
    = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS = NONE JRN %
    = OFF
FILTER_INTERFACE LINE = ETHLINE SET = a11
###Ethernet line ETHLINE
```

Spoof protection

Spoofing occurs when someone attempts to access your system by pretending to be a system that you normally trust within your own network. It is a good idea to protect any interfaces that are linked to a public network from this type of attack. You can protect against spoofing by completing the Spoof Protection wizard which is available from the Packet Rules Editor in iSeries Navigator. This wizard helps you to assign rules to your vulnerable interfaces. Once the rules are active, a system from the public (untrusted) network will not be able to act as a trusted machine from a private (trusted) network.

Chapter 4. Plan for packet rules

Before you connect any of your network resources to the Internet, you should develop a security plan and have an understanding of the potential security risks involved. In general, you must gather detailed information about how you plan to use the Internet as well as a document that describes your internal network configuration. Based on the results of gathering this information, you can accurately evaluate your security needs. The topic, IBM SecureWay: iSeries and the Internet will provide you with the details you need to create a total network security plan. If part of your plan includes using packet rules, you should refer to the following topics to gather all the information you need to begin configuring them:

- **Packet rules: User authority requirements**
Make sure you have the proper authorities to administer your packet rules.
- **Packet rules: System requirements**
Make sure your iSeries meets the minimum system requirements to work with packet rules.
- **Packet rules: Planning worksheet**
Use this worksheet to help you gather the information you need to begin configuring packet rules.

After you develop a plan, you can begin configuring your packet rules.

Packet rules: User authority requirements

Before you can administer packet rules on your iSeries, you need to ensure that you have the proper authorities. You need to have *IOSYSCFG special authority in your user profile. If you plan to administer packet rules from the QSECOFR userid, or from a userid of type, *SECOFR, or you have *ALLOBJ authority, this will be sufficient. If not, you need authority to the following directories, files and QSYS userid:



1. Add object authority, *RXW, and data authority, OBJMGT, to these three files:
/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.i3p
/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.txt
/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.tcpipl
2. Add Object authority, *RWX, to the following directories:
/QIBM/UserData/OS400/TCPIP/PacketRules
/QIBM/UserData/OS400/TCPIP/OpNavRules
3. Add Object authority, *RWX, to the following files:
/QIBM/UserData/OS400/TCPIP/OpNavRules/VPNPolicyFilters.i3p
/QIBM/UserData/OS400/TCPIP/OpNavRulesPPPFilters.i3p
4. You will also need ADD authority to the QSYS profile, since QSYS owns the newly created rules files.

These are the default directories and files that the Packet Rules Editor uses. If you choose to store your files in directories other than those listed above, you will need authority to those directories.

Packet rules: System requirements

To function properly on your iSeries, packet rules requires the following:

1. OS/400® Version 5 Release 2 (5722-SS1), or later.
2. iSeries Access for Windows® (5722-XE1) and iSeries Navigator
 - Network component of iSeries Navigator
3. TCP/IP (5722-TC1) must be configured, including IP interfaces, routes, local host name, and local domain name.

Note: If you do not understand TCP/IP, networking, or IP addresses, see TCP/IP Tutorial and Technical Overview  and V4 TCP/IP for AS/400®: More Cool Things Than Ever .

Packet rules: Planning worksheet

Use the packet rules planning worksheet to gather detailed information about your packet rules usage plan. You need this information to pinpoint your security needs. You can also use this information to configure your packet rules. You should answer each question before you proceed with configuring packet rules on your system.

You need this information to create a plan for using packet rules	Answers
What is the layout of your network and connections? Create a drawing to show this.	
What routers and IP addresses will you use?	
What rules will you use to control TCP/IP traffic that passes through your systems? For each rule that you list, specify these aspects of TCP/IP traffic flow: <ul style="list-style-type: none">• the type of service that you want to permit or deny (for example, HTTP, FTP, and so forth)• the well-known port number for that service• the direction of the traffic• whether the traffic is reply or initiating traffic• the IP addresses for the traffic (source and destination)	
What IP addresses do you want to map to other addresses or hide behind other addresses? (You need this list only if you are using network address translation.)	

Chapter 5. Configure packet rules

After you have created a plan for configuring packet rules on your system, you should be ready to begin actually creating and applying them. You will find the specific, step-by-step, information in the Packet Rules Editor online help. However, the following checklist provides you with an overview of the tasks you must complete to ensure that your rules will work properly when you activate them:

- ___ 1. Access the Packet Rules Editor.
Follow these instructions to access the Packet Rules Editor in iSeries Navigator.
- ___ 2. Use the wizards provided as part of the Packet Rules Editor (V5R2 and later) to create your rules files:
 - **Permit a Service Wizard**
This wizard will generate and insert a set of packet rule statements that will permit the necessary traffic for a given TCP or UDP service.
 - **Spoof Protection Wizard**
This wizard will generate and insert a set of packet rule statements that will deny any traffic on an interface that should only be entering this server through a different interface.
 - **Address Translation Wizard**
This wizard will generate and insert a set of either map or hide packet rules statements.

Depending on what type of rules you want to configure, these wizard create all of the required filter and NAT statements for you. You can access the wizards from the **Wizards** menu in the Packet Rules Editor. If you prefer to write the rules yourself, continue on to the next item in the checklist.

- ___ 3. Define addresses and services
Create aliases for the addresses and services for which you plan to create multiple rules.

Note: You *must* define addresses if you want to create NAT rules.
- ___ 4. Create NAT rules.
Perform this task *only* if you plan to use NAT.
- ___ 5. Create filter rules.
Define what filters to apply to the network that this system administrates.
- ___ 6. Include files
Specify any additional files that you want to include in your "master" rules file. Complete this task *only* if you have existing rules files that you want to reuse in a new rules file.
- ___ 7. Define the interfaces
Apply your rules to an interface.
- ___ 8. Make comments
Describe what each rules file does.
- ___ 9. Verify your rules files
Ensure that your rules will activate error free and without problems.
- ___ 10. Activate your rules file.
Packet rules must be activated in order for them to work.
- ___ 11. Manage packet rules
After you have activated your packet rules, you must manage them periodically to maintain the security of your system. This topic includes information about editing your rules files, journaling and auditing packet rules actions, and backup and recovery tips and techniques.

Access packet rules

You must access the Packet Rules Editor through iSeries Navigator, the graphical interface that enables you to work with your iSeries resources. Use the Packet Rules Editor to get started creating packet rules on your system. You can create a new file, edit an existing one, or you can work with the sample files provided on the system.

To access the Packet Rules Editor, follow these steps:

1. In iSeries Navigator, expand your server -->**Network** -->**IP Policies**.
2. Right-click **Packet Rules** and select **Rules Editor**.

Use the online help for step-by-step instructions on how to complete each of the tasks described in the Configure packet rules section of this topic.

Define addresses and services

When you create packet rules, you must specify the IP addresses and services to which you want the rules to apply. **Defined addresses** are interface specifications that have been given symbolic names. You should define addresses when the address you want to represent is a range of addresses, a subnet, a list of point-to-point identifiers, or a list of non-contiguous addresses. A defined address statement is required when you plan to create map address translation rules. If the address you want to represent is a single IP address in a filter statement, then a defined address statement is not required. **Service aliases** allow you to define services and then to reuse them in any number of filters. Service aliases also keep track of the purposes of different service definitions.

Defining addresses and service aliases, makes it easier to create your packet rules. When you create the rules, you refer to the address nickname or service alias rather than the specific address or service details. Using nicknames and aliases in your filter rules has two advantages:

1. Minimizes the risks of typographical errors.
2. Minimizes the number of filter rules that you need to create.

For example, you have 31 users on your network who need Internet access. However, you want to restrict these users to Web access only. You have two choices about how to create the filter rules that you need in this situation.

1. Define a filter rule for each user's IP address.
2. Create a nickname for the entire address set that represents your users by defining an address.

The first choice increases your chances of making typographical errors, as well as increases the amount of maintenance that you must perform for your rules file. Using the second choice, you only need to create two filter rules. Use a nickname in each rule to refer to the entire set of addresses to which the rule applies.

You can also create nicknames for services and use them in the same manner as address nicknames. The service alias defines what TCP, UDP, and ICMP criteria you want to select. You select the source and destination port that you want to use.

Note: Remember you *must* define addresses if you plan to use NAT. NAT rules can only point to a defined address.

For step-by-step instructions on how to define addresses, service aliases, and ICMP services, use the Packet Rules Editor online help.

Next step

If you plan to use network addresses translation, continue on to create NAT rules. Otherwise, go to create IP filter rules to filter IP traffic coming into and going out of your network.

Create NAT rules

If you determine that you need to use NAT, you *must* define nicknames for the IP addresses you intend to use. You cannot create NAT rules with the standard 32-bit address notation. Rather than specifying a real address such as 193.112.14.90, you must refer to 193.112.14.90 by *aname*. The system associates the name you defined with the corresponding addresses and translates them accordingly. Therefore, you must define your addresses before your system can apply NAT rules to them.

The Packet Rules Editor allows you to create two types of NAT rules. One type allows you to hide addresses, while the other type allows you to map addresses.

Hiding Addresses

You should hide addresses when you want to keep your private addresses hidden from public view. A hidden address rule allows you to hide multiple internal addresses behind a single public IP address. This type of NAT is also known as *masquerade* NAT.

Mapping Addresses

You should map addresses when you want to route traffic from a single public IP address into a single internal address. This type of NAT is also known as *static* NAT.

For step-by-step instructions on how to hide or map addresses, use the Packet Rules Editor online help.

Next Step

If you plan to filter traffic flowing into and out of your network, go to Create IP filter rules. Otherwise, proceed to Make comments in packet rules.

Create IP filter rules

When you create a filter, you specify a rule that governs the IP traffic flow into and out of your system. The rules you define specify whether the system should permit or deny packets attempting to access your system. The system directs IP packets based on the type of information in the IP packet headers. It also directs the IP packet to the action that you have specified the system to apply. The system discards any packets that do not match a specific rule. This automatic discard rule is called the *default deny rule*. Located at the end of the file, the default deny rule automatically activates any time a packet does not match the criteria in any of the preceding rules. You must have at least one filter rule activated for the default deny rule to be active.

Note: When you apply rules to an interface through which you are configuring the iSeries, it is very important that you permit your own workstation or that of anyone else who may be configuring the iSeries. Failure to do so will result in a loss of communication with the iSeries. If this happens, you will have to log on to the iSeries using an interface that still has connectivity, such as the operators console. Use the RMVTCPTBL command to remove all filters on the system.

Before you create your filter rules, you should determine whether you need to use network address translation (NAT). If you use NAT rules, you *must* define addresses and services. NAT is the only function that requires a defined address, but you can use it for other functions as well. If you define addresses and services, you can reduce the number of rules that you must create as well as minimize the possibility of typographical errors.

Here are some other ways you can minimize error and maximize efficiency when creating filter rules:

- **Define one filter rule at a time.** For example, create all the permits for telnet at the same time. This way you can group associate the rules whenever you refer to them.

- **Filter rules are processed in the order that they appear in the file.** Be sure to order the rules the way you intend them to be applied as you create them. If the order is incorrect, your system is vulnerable to attack because the packets will not process as you intend them to process. To make things easier, consider the following voluntary actions:
 1. Place your filter set names in the `FILTER_INTERFACE` statement in the exact same order in which the sets are physically defined in the file.
 2. Place all filter rules in one set to avoid problems with set order.
- **Verify the syntax of each rule as you go along.** This is easier and faster than debugging them all at once.
- **Create set names for groups of files that are logically associated with each other.** This is important because only one rule file can be active at a time. See example below.
- **Only write filter rules for the datagrams you want to permit.** Everything else will be discarded by the automatic deny rule.
- **Write rules for high traffic volume first.**

Example: Look at the *Create set names* tip above. You may want to allow telnet access to a number of internal users, but not to all. To manage these rules easier, you can assign each of them the set name `TelnetOK`. A second criteria may allow telnet through a specific interface and block telnet traffic from all others. In this case, you need to create a second set of rules that block telnet access entirely. You can assign these rules the set name `TelnetNever`. By creating set names, you make it easier to distinguish the purpose of the rule. It is also easier to determine which interfaces you intended to apply to particular sets. Use all of the tips above to ease the process of creating filters.

For step-by-step instructions on how to create IP filter rules, use the Packet Rules Editor online help.

Next Step

After you create your filters, you may want to consider including a file or multiple files in the filter statement. If not, the next step is to define the interfaces to which the rules apply.

Define IP filter interfaces

You *must* define filter interfaces to establish which filter rules you want the system to apply to which interfaces. Before you can define your filter interfaces, you need to create the filters that you intend the system to apply to various interfaces. If you chose to define your addresses (when you define your interfaces), you will refer to them by name. If you chose *not* to define your addresses (when you define your interfaces), you will refer to them by IP addresses.

When you create your filters, you can include multiple filters in one set. You then add the set to a `FILTER_INTERFACE` statement. The set name used in the statement needs to be a set name that you defined in a filter statement. For example, if you have a set name, `ALL`, and all of your filters are in that set, you must include the set name, `ALL`, in the filter interface statement for the filters to work properly. Not only can you have multiple filters in a set, but you can also have multiple sets in a `FILTER_INTERFACE` statement.

Before you define your interfaces, you should include any additional files you want to use. Then, you can define your interfaces. Remember that the filter sets are applied in the order that they are specified in the filter interface statement. So, the filter rules should appear in the `FILTER_INTERFACE` statement in the same order in which the sets are physically defined in the file.

For step-by-step instructions on how to define a filter interface, use the Packet Rules Editor online help.

Next Step

After you define the filter interfaces, the next step is to make comments in your packet rules.

Include files in packet rules

You can activate more than one packet rules file on your system by using the *Include* feature of the Packet Rules Editor. Using multiple files makes it much easier for you to work with your rules. Especially, if you need a large number of rules to control traffic on multiple interfaces. For example, you may want to use a group of rules on multiple interfaces.

You can create this group within an individual file. Instead of rewriting the rules every time you wish to use them in other files, you can include them in the master file. The master file is the one file that can be active at any given time. You only need to use the include feature to add the rules to your master file.

When creating include files, you may want to keep your NAT rules for an interface separate from your filter rules for that interface. However, only one file can be active at any given time.

When you create a new rules file, you can include any existing files as part of the new file. Before you do this, you should create the new filter rules you want to use. Whenever you create a rule, you should file (group) them by type. This way you do not have to recreate rules that you have used before. You can just include or remove them as needed.

For step-by-step instructions on how to include a file in your rules, use the Packet Rules Editor online help.

Next Step

After you include all of the additional rules files you want to use, the next step is to define IP filter interfaces.

Make comments in packet rules

Making comments about your rules files is very important. You want to record how you intend your rules to work. For instance, you may want to record what a particular rule permits or denies. This type of information will save you hours of time in the future. If you ever need to fix a security leak quickly, you will need these comments to jog your memory. You may not have the time to figure out what your rules meant, so use comments generously.

Each of the dialogs associated with creating and activating packet rules has a **Description** field. This is the field that is reserved for your comments. The system ignores anything you put in this field. You may want to use the comment field at each step of the rule creation process. This can reduce your chance of forgetting to make a significant comment. It is best to make your comments while the process on which you are commenting is still fresh in your mind. However, you can wait until you finish creating all your rules.

For step-by-step instructions on how to make comments in a rules file, use the Packet Rules Editor online help.

Next step

After you complete each of the configuring packet rules steps prior to this one, the next step is to save and verify your packet rules.

Verify packet rules

You should always verify your rules before you activate them. This helps ensure that the rules will activate without problems. When you verify your packet rules, the system checks them for syntax and semantic errors and reports the results in a message window at the bottom of the Packet Rules Editor. For error messages that are associated with a specific file and line number, you can right-click the error and select **Go To Line** to highlight the error in the file you are editing.

Before using the verify function you may want to consider viewing your packet rules to check for visible errors. You can not activate rules that have syntactical errors. The verify function checks for errors of a syntactical nature. The system can not verify whether you have ordered your rules correctly. You must check for rule order manually. Packet rules are order dependent, which means, you must order the rules the way that you want them applied. If you order them incorrectly, you will not get the intended result. Ensure that your rules are correct and ordered the way you want them applied before you activate them.

For step-by-step instructions on how to verify packet rules, use the Packet Rules Editor online help.

Warning messages: Whenever you activate your filter rules, the system automatically verifies them. Various warning and error messages may be produced. A warning message is simply for informational purposes and will not stop the verification process. Read all messages carefully. One message will appear saying that your verification or activation was successful. This last sentence could also state that the rule load was unsuccessful if there are severe errors.

Next step

After your rules verify successfully, the next step is to activate them.

Activate packet rules

Activating the packet rules you create is the final step in configuring packet rules. You must activate, or load, the rules that you create in order for them to work. However, before you activate your rules you should verify that they are correct. Always attempt to resolve any problems before activating your packet rules. If you activate rules that have errors or that are ordered incorrectly, your system will be at risk. Your system has a verify function that is automatically invoked any time you activate your rules. Because this automatic feature only checks for major syntactical errors, you should not rely solely on it. Make sure you always manually check for errors in your rules files as well.

When filter rules are not applied to an interface (for example, you are only using NAT rules, not filtering rules), a warning (TCP5AFC) appears. This is not an error. It only verifies that using one interface is indeed, your intention. Always look at the last message. If it says the activation is successful, then the messages above it are all warnings.

Note: When you activate new rules on all interfaces, they replace all previous rules on all physical interfaces. Even if a physical interface is not mentioned in the new rules, it will be replaced. However, if you choose to activate new rules on a specific interface, the rules will only replace the rules on that specific interface. Existing rules on other interfaces will be untouched.

Final step

Once your packet rules have been configured and successfully activated, you may need to periodically manage them to ensure the security of your system. Refer to the Manage packet rules section of this topic for a list of tasks you can perform to properly maintain and monitor your packet rules.

Chapter 6. Manage packet rules

To maintain the security of your system and the integrity of your packet rules, you should periodically perform these management tasks:

Note: You will find the specific, step-by-step, instructions for these tasks in the Packet Rules Editor online help, unless otherwise noted.

- Backup packet rules to protect yourself against losing files.
- Deactivate packet rules when you need to stop your NAT and filter rules for any reason. Remember, however, when you deactivate your rules, your network will be unprotected.
- Edit packet rules when you need to change how IP traffic flows into and out of your system.
- Journal and audit packet rule actions to log your packet rules. This helps to debug your rules if you need to.
- View packet rules when you need to troubleshoot errors.

You should use every possible means to effectively and efficiently manage your packet rules. The security of your system depends on accurate and current rules. If you need troubleshooting assistance, refer to [Troubleshoot packet rules](#).

Deactivate packet rules

If you need to make changes to your active packet rules, or you want to activate new rules, you must first deactivate the currently active rules. You can choose to deactivate rules on a specific interface, on a point-to-point identifier, or on all interfaces and all point-to-point identifiers.

For step-by-step instructions on how to deactivate your packet rules, use the Packet Rules Editor online help.

View packet rules

You should view your filter rules before you activate them to verify that they are correct. By viewing the filter rules you create, you can check for any visible errors. You may want to view your filter rules not only before activating and testing, but also before printing and backing up. Viewing your rules is not your only way of checking for errors. It is, however, a useful way to minimize or remove the errors before testing.

You should print out the filter rules you create so you can look over them. This allows you to catch any visible mistakes and verify that you included any previously created filter rules files you wanted to add.

Your system also has a verify function, but do not solely rely on it. You should take the necessary measures to ensure that you correct all errors manually. This will save you valuable time and resources.

To view inactive rules you need to open the rule file in the Packet Rules Editor.

If you want to edit your active filter rules, you should first view them to determine how you want to change them.

To view your currently active rules, follow these steps:

1. In iSeries Navigator, select **your server** —> **Network** —> **IP policies** —> **Packet rules**.
2. Select the interface for those active packet rules you want to view.
3. View the list of active packet rules in the right pane.

Note: You can not edit the rules from within this dialog. You must deactivate your rules file and then use the Packet Rules Editor to edit your rules.

Return to NAT and IP filter administration.

Edit packet rules

As your network security requirements change, you *must* edit your rules to ensure that they compliment your new security strategy. However, before you can edit your active packet rules, you must first deactivate them. Then, use the Packet Rules Editor in iSeries Navigator to make the necessary changes to your rules. Make sure you verify and then reactivate the rules when you finish editing them.

For step-by-step instructions on how to edit your packet rules, use the Packet Rules Editor online help.

Backup packet rules

It may not seem necessary at first, but backing up your packet rules is always a good idea. In the event of a loss, your backups can save you the time and work it would take to recreate your files from scratch.

These are general tips you can use to ensure that you have an easy way to replace lost files:

Print out the filter rules

You can store the printouts wherever they are most likely to be secure and reenter the information as necessary. Printouts are also useful if you need to search for an error in a filter rule.

For step-by-step instructions on how to print your packet rules, use the Packet Rules Editor online help.

Copy the information to a disk

Copying has an advantage over printouts: rather than reentering manually, the information exists electronically. It provides you a straightforward method for transporting information from one on-line source to another.

Note: Your iSeries copies information to the system disk, not to a floppy disk. The rules files are stored in the IFS file system on the iSeries, not on a PC. You may want to use a disk protection method as a backup means for protecting the data that is stored on the system disk.

When using an iSeries, you must plan a backup and recovery strategy. Review Back up and Recovery for more information about recovering and backing up your files.

Journal and audit packet rules actions

Your packet rules includes a journaling feature. Journaling allows you to troubleshoot NAT and filtering problems. You can use the journal to create a log of rule actions. This allows you to debug and spot check your rules easier. You can also audit the traffic that flows into and out of your system by reviewing these system logs or journals.

The journaling feature is used on a per-rule basis. When you create a NAT or filter rule, you have the following journaling options: full or off. See the table below for more detail.

OPTION	DEFINITION
FULL	Every packet that is translated is logged.
OFF	No journaling occurs.

If journaling is turned on, a journal entry is generated for each rule applied to a datagram (NAT or filter). The only rules for which a journal entry is not created are the default deny rules. They are never journaled because they are created by the system.

By using these journals, you create a general file on the iSeries. You can then use the information recorded in your system's journals to determine how your system is being used. This can help you decide to change various aspects of your security plan.

If you set the journaling feature to OFF, your system will not create a journal entry for that rule. Although you can choose to do this, it may not be your best option. If you are not experienced in creating filter and NAT rules, you may want to use FULL (logging) as necessary. You can then use the logs as troubleshooting tools. However, be selective in what you choose to journal. Journaling is a heavy burden on your system's resources. Try to focus on the rules that control heavy traffic.

To view these journals do the following:

1. At a command prompt on the iSeries enter: DSPJRN JRN(QIPNAT) for NAT journals or DSPJRN JRN(QIPFILTER) for IP filter journals.

Chapter 7. Troubleshoot packet rules

This section provides some troubleshooting advice for some common packet rules problems.

- **iSeries communications trace** capability allows you to see all datagram traffic for a specified interface. Use the start communications trace (STRCMNTRC) and print communications trace (PRTCMNTRC) commands to collect and print the information.
- **NAT and IP filtering rule order** determines how your rules are processed. They are processed in the order which they appear in the file. If the order is not correct, the packets will not process as you intend. This will leave your system vulnerable to attack. Place your filter set names in the FILTER_INTERFACE statement in the exact same order in which the sets are physically defined in the file.

Review the Create IP filter rules section of this topic for more help on writing syntactically correct filter rules. Remember the process shown in the table below:

Inbound Traffic Process	Outbound Traffic Process
1. NAT rules	1. IP filter rules
2. IP filter rules	2. NAT rules

- **Removing all rules** is the best way to reset your system and clear out errors. On the iSeries, issue the following command: RMVTCPTBL (Remove TCP/IP Table). If you lock yourself out of the iSeries Navigator application, you can also use this command to go back and repair any rules.

Note: The "Remove TCP/IP Table" command also starts the VPN servers— only if the VPN servers (IKE and ConMgr) were running before.

- **Allowing IP datagram forwarding** in your TCP/IP configuration on the iSeries is essential if you are using NAT. Use the CHGTCPA (Change TCP/IP Attributes) command to verify that IP datagram forwarding is set to YES.
- **Verifying default return routes** ensures that the address that you map to or hide behind is correct. This address must be routable on the return route back to the iSeries and pass through the correct line to be untranslated by NAT.

Note: If your iSeries has more than one network, or line, connected to it, you should be especially careful about routing inbound traffic. Inbound traffic is handled on any line that it enters on, which may not be the correct line waiting to untranslate it.


- **Viewing error and warning messages** in the EXPANDED.OUT file to ensure the rules are ordered as you intend. When you verify and activate a set of filters, these filters are merged with any iSeries Navigator-generated rules. The combination produces the merged rules in a new file called EXPANDED.OUT, which is placed in the same directory that contains your rules (usually /QIBM). Warning and error messages refer to this file. To view this file, you must open it from the Packet Rules Editor.
 1. Access the Packet Rules Editor in iSeries Navigator.
 2. From the **File** menu, select **Open**.
 3. Go to the directory, QIBM/UserData/OS400/TCPIP/PacketRules/ or to the directory where you have saved your packet rules, if its different than the default.
 4. From the **Open file** window, select **EXPANDED.OUT file**. The EXPANDED.OUT file should appear.
 5. Select this file and click **Open**.

The EXPANDED.OUT file is for your information only. You can not edit it.



Chapter 8. Related information for packet rules

Listed below are the IBM Manuals and Redbooks™ (in PDF format) that provide additional information about IP filtering and NAT.

Manuals


- **Tips and Tools for Securing your iSeries**  (about 254 pages)
This PDF book provides you with high-level information about how you can enhance security on your iSeries.

Redbooks

- **TCP/IP Tutorial and Technical Overview** 
Find information on security issues related to TCP/IP networks.
- **TCP/IP for AS/400: More Cool Things Than Ever** 
Find several scenarios that demonstrate NAT and IP packet filtering.

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...**
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site (www.adobe.com/prodindex/acrobat/readstep.html) .

Part 2. Appendixes

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AS/400
IBM
iSeries
OS/400
SecureWay

Microsoft[®], Windows, Windows NT[®], and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java[™] and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for downloading and printing publications

Permissions for the use of the publications you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

Personal Use: You may reproduce these Publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these Publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these Publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these Publications, or reproduce, distribute or display these Publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the Publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

All material copyrighted by IBM Corporation.

By downloading or printing a publication from this site, you have indicated your agreement with these terms and conditions.



Printed in USA