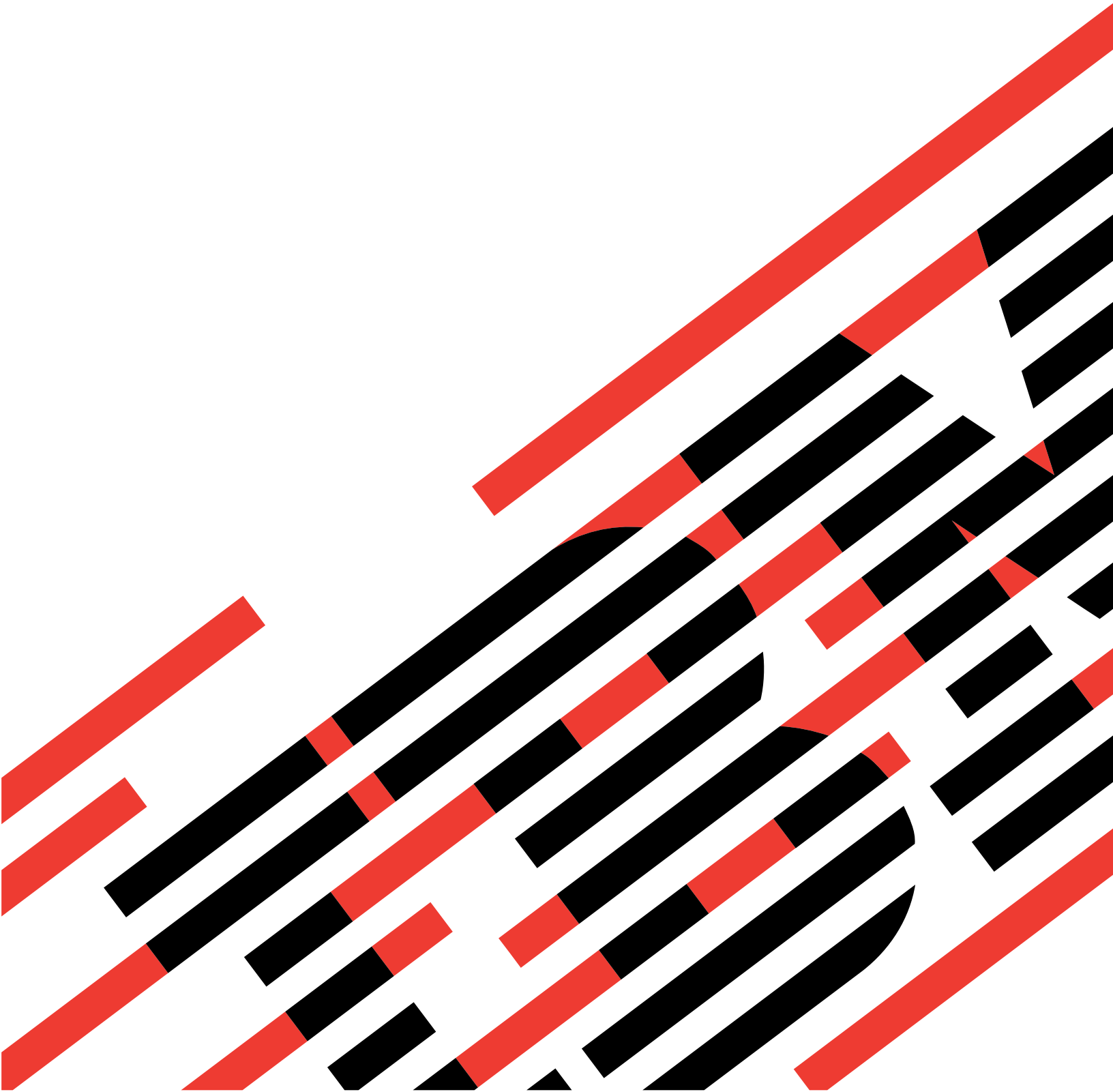
IBM

eserver

iSeries

Virtual private networking

Version 5 Release 3



IBM

@server

iSeries

Virtual private networking

Version 5 Release 3

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 69.

Sixth Edition (August 2005)

This edition applies to version 5, release 3, modification 2 of IBM i5/OS (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.

Contents

Virtual private networking 1
What's new for V5R3 2
Print this topic. 3
VPN scenarios 3
VPN scenario: Basic branch office connection . . 4
Configuration details 6
VPN scenario: Basic business to business connection 9
Configuration details 11
VPN scenario: Protect an L2TP voluntary tunnel with IPSec 13
Configuration details 15
VPN scenario: Use network address translation for VPN 20
VPN concepts 21
IP Security (IPSec) protocols 22
Authentication Header 23
Encapsulating Security Payload 24
AH and ESP combined 25
Key management 25
Layer 2 Tunnel Protocol (L2TP) 26
Network address translation for VPN. 27
NAT compatible IPSec 28
IP Compression (IPComp) 29
VPN and IP filtering 30
Migrate policy filters to the current release . . 30
VPN connections with no policy filters . . . 31
Implicit IKE 32
Plan for VPN 32
VPN setup requirements 32
Determine what type of VPN to create 33
Complete the VPN planning worksheets. . . . 33
Planning worksheet for dynamic connections 34
Planning worksheet for manual connections 35
Configure VPN 36
Configure VPN connections with the New Connection wizard 38
Configure VPN security policies 38
Configure an Internet Key Exchange (IKE) policy 39
Configure a data policy 39
Configure the VPN secure connection 40
Configure a manual connection. 41
Configure VPN packet rules 41
Configuring the pre-IPSec filter rule 42
Configure a policy filter rule. 43
Define an interface for the VPN filter rules . . 44
Activate the VPN packet rules 44
Start a VPN connection 45
Manage VPN 45
Set default attributes for your connections . . . 45
Reset connections in error state 46
View error information 46
View the attributes of active connections . . . 46
Use the VPN server trace 46
View the VPN server job logs 47
View the attributes of Security Associations (SA) 47
Stop a VPN connection 47
Delete VPN configuration objects 47
Troubleshoot VPN 48
Get started with troubleshooting VPN 48
Common VPN configuration errors and how to fix them 49
VPN error message: TCP5B28 50
VPN error message: Item not found 51
VPN error message: PARAMETER PINBUF IS NOT VALID 51
VPN error message: Item not found, Remote key server... 52
VPN error message: Unable to update the object 52
VPN error message: Unable to encrypt key... 53
VPN error message: CPF9821 53
VPN error: All keys are blank 53
VPN error: Sign-on for a different system appears when using Packet Rules 54
VPN error: Blank connection status in iSeries Navigator window 54
VPN error: Connection has enabled status after you stop it 54
VPN error: 3DES not a choice for encryption 54
VPN error: Unexpected columns display in the iSeries Navigator window 54
VPN error: Active filter rules fail to deactivate 54
VPN error: The key connection group for a connection changes 55
Troubleshoot VPN with the QIPFILTER journal 55
QIPFILTER journal fields 56
Troubleshoot VPN with the QVPN journal . . . 57
QVPN journal fields 58
Troubleshoot VPN with the VPN job logs . . . 59
Common VPN Connection Manager error messages 60
Troubleshoot VPN with the OS/400 communications trace 65
Related information for VPN 67

Appendix. Notices 69
Trademarks 70
Terms and conditions for downloading and printing publications 71

Virtual private networking

A virtual private network (VPN) allows your company to securely extend its private intranet over the existing framework of a public network, such as the Internet. With VPN, your company can control network traffic while providing important security features such as authentication and data privacy.

OS/400(R) VPN is an optionally-installable component of iSeries(TM) Navigator, the graphical user interface (GUI) for OS/400. It allows you to create a secure end-to-end path between any combination of host and gateway. OS/400 VPN uses authentication methods, encryption algorithms, and other precautions to ensure that data sent between the two endpoints of its connection remains secure.

VPN runs on the network layer of the TCP/IP layered communications stack model. Specifically, VPN uses the IP Security Architecture (IPSec) open framework. IPSec provides base security functions for the Internet, as well as furnishes flexible building blocks from which you can create robust, secure virtual private networks.

VPN also supports Layer 2 Tunnel Protocol (L2TP) VPN solutions. L2TP connections, which are also called virtual lines, provide cost-effective access for remote users by allowing a corporate network server to manage the IP addresses assigned to its remote users. Further, L2TP connections provide secure access to your system or network when you protect them with IPSec.

It is important that you understand the effect a VPN will have on your entire network. Correct planning and implementation are essential to your success. Review these topics to ensure that you know how VPNs work and how you might use them:

“What’s new for V5R3” on page 2
This topic describes what information is new or significantly changed in this release.

“Print this topic” on page 3
If you prefer a hardcopy version of this information, go here to print the PDF.

“VPN scenarios” on page 3
Review these scenarios to become familiar with the basic VPN types and the steps involved in configuring them.

“VPN concepts” on page 21
It is important that you have at least a basic knowledge of standard VPN technologies. This topic provides you with conceptual information about the protocols VPN uses in its implementation.

“Plan for VPN” on page 32
The first step to successfully using VPN is planning. This topic provides information about migrating from prior releases, setup requirements, and links to a planning advisor that will generate a planning worksheet that is customized to your specifications.

“Configure VPN” on page 36
After planning for your VPN, you can begin configuring it. This topic provides you with an overview of what you can do with VPN and how to do it.

“Manage VPN” on page 45
This topic describes various tasks you can perform to manage your active VPN connections, including how to make changes to, monitor, or delete them.

"Troubleshoot VPN" on page 48
Refer to this topic when you experience problems with your VPN connections.

"Related information for VPN" on page 67
Go here for links to other sources of VPN information and related topics.

What's new for V5R3

Function enhancements
Enhancements to the Version 5 Release 3 (V5R3) virtual private networking (VPN) function include two new identifier types. There are two new identifier types that can be selected when defining VPN key exchange policies and connection data endpoints. The identifier types include local IP address and IPv4 host name. For additional information, see the online help within iSeries(TM) Navigator.

- **My local IP address**
  The identifier type, My Local IP Address, can be selected to define the local key server type for an Internet Key Exchange Policy or the local data endpoint in a connection definition. When selected, VPN uses an available IPv4 address. VPN connections which use this identifier type must not use a policy filter. In addition, the local system must be the initiator of the connection.
- **IPv4 host name**
  The identifier IPv4 host name can be selected to define a few different parameters:
  - The remote key server identifier type in an Internet Key Exchange Policy
  - The remote address identifier in the connection's properties
  - The policy filter definition for a connection group's properties

  The IPv4 host name resolves to the IP address of the host name specified as the identifier type.

VPN Security Notice:
It is recommended that you use main mode negotiation whenever a preshared key is used for authentication. They provide a more secure exchange. If you must use preshared keys and aggressive mode negotiation, select obscure words that are unlikely to be cracked in attacks that scan the dictionary for possible passwords. For instructions on how to force a key exchange to use main mode negotiation, see Security exposure with preshared key authentication. When you create or edit an Internet key exchange policy, you can also use the iSeries Navigator online help for detailed information.

Information enhancements
Changes to the V5R3 VPN Information Center topic include a visual presentation explaining the Layer 2 Tunnel Protocol (L2TP) voluntary tunnel concept. Use the following link to view a visual presentation about L2TP voluntary tunnels protected by IPSec. This requires the Flash plug-in

. Alternatively, you can use the HTML version of this presentation.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The

  image to mark where new or changed information begins.
- The

  image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to Users.

Print this topic

To view or download the PDF version of this document, select Virtual private networking (VPN) (about 509 KB).

Saving PDF files

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...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

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

.

VPN scenarios

Review the following scenarios to become familiar with the technical and configuration details involved with each of these basic connection types:

- **"VPN scenario: Basic branch office connection" on page 4**
  In this scenario, your company wants to establish a VPN between the subnets of two remote departments through a pair of iSeries(TM) computers acting as VPN gateways.
- **"VPN scenario: Basic business to business connection" on page 9**
  In this scenario, your company wants to establish a VPN between a client workstation in your manufacturing division and a client workstation in the supply department of your business partner.
- **"VPN scenario: Protect an L2TP voluntary tunnel with IPSec" on page 13**
  This scenario illustrates a connection between a branch office host and a corporate office that uses L2TP protected by IPSec. The branch office has a dynamically assigned IP address, while the corporate office has a static, globally routable IP address.
- **"VPN scenario: Use network address translation for VPN" on page 20**
  In this scenario your company wants to exchange sensitive data with one of it's business partners by using OS/400(R) VPN. To further protect the privacy of your company's network structure, your company will also use VPN NAT to hide the private IP address of the iSeries it uses to host the applications to which your business partner has access.

More VPN scenarios

For more VPN configuration scenarios, see these other sources of VPN information:

- **QoS scenario: Secure and predictable results (VPN and QoS)**
  You can create quality of service (QoS) policies with your VPN. This example shows the two being used together.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153**

This IBM Redpaper provides a step-by-step process for configuring the VPN tunnel using V5R1 VPN and the Windows 2000 integrated L2TP and IPSec support.

- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

This redbook explores VPN concepts and describes its implementation using IP security (IPSec) and Layer 2 Tunneling Protocol (L2TP) on OS/400.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

This redbook explores all the integrated network security features available on the OS/400 system such as IP filters, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, auditing, and logging. It describes their use through practical examples.

VPN scenario: Basic branch office connection

Suppose your company wants to minimize the costs incurred from communicating to and among its own branches. Today, your company uses frame relay or leased lines, but you want to explore other options for transmitting internal confidential data that are less expensive, more secure, and globally accessible. By exploiting the Internet, you can easily establish a virtual private network (VPN) to meet the needs of your company.

Your company and its branch office both require VPN protection across the Internet, but not within their respective intranets. Because you consider the intranets trusted, the best solution is to create a gateway-to-gateway VPN. In this case, both gateways are connected directly to the intervening network. In other words, they are *border* or *edge* systems, which are not protected by firewalls. This example serves as a useful introduction to the steps involved in setting up a basic VPN configuration. When this scenario refers to the term, *Internet*, it refers to the intervening network between the two VPN gateways, which might be the company's own private network or the public Internet.

> **Important note:**
> This scenario shows the iSeries(TM) security gateways attached directly to the Internet. The absence of a firewall is intended to simplify the scenario. It does not imply that the use of a firewall is not necessary. In fact, consider the security risks involved any time you connect to the Internet. Review this redbook, AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> , for a detailed description of various methods for reducing these risks.

Advantages

This scenario has the following advantages:

- Using the Internet or an existing intranet reduces the cost of private lines between remote subnets.
- Using the Internet or an existing intranet reduces the complexity of installing and maintaining private lines and associated equipment.
- Using the Internet allows remote locations to connect to almost anywhere in the world.
- Using VPN provides users access to all servers and resources on either side of the connection just as though they were connected using a leased line or wide area network (WAN) connection.
- Using industry standard encryption and authentication methods ensures the security of sensitive information passed from one location to another.

- Exchanging your encryption keys dynamically and regularly simplifies setup and minimizes the risk of your keys being decoded and security being breached.
- Using private IP addresses in each remote subnet makes it unnecessary to allocate valuable public IP addresses to each client.

Objectives

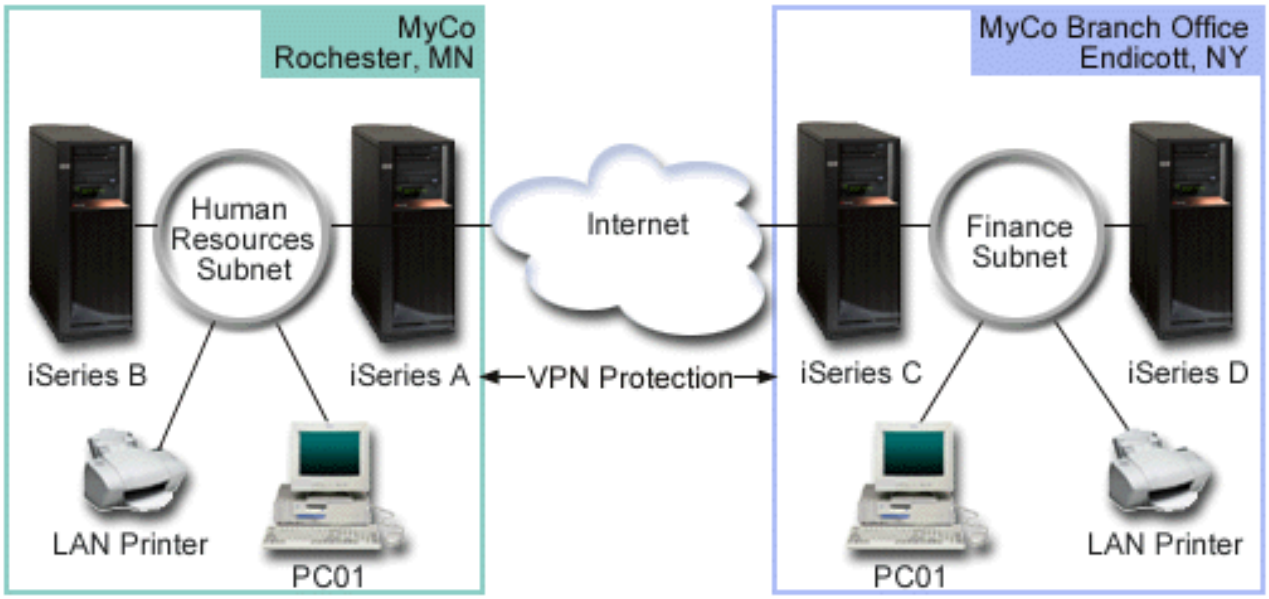
In this scenario, MyCo, Inc. wants to establish a VPN between the subnets of its Human Resources and Finance departments through a pair of iSeries servers. Both servers will act as VPN gateways. In terms of VPN configurations, a gateway performs key management and applies IPSec to the data that flows through the tunnel. The gateways are not the data endpoints of the connection.

The objectives of this scenario are as follows:

- The VPN must protect all data traffic between the Human Resources department's subnet and the Finance department's subnet.
- Data traffic does not require VPN protection once it reaches either of the department's subnets.
- All clients and hosts on each network have full access to the other's network, including all applications.
- The gateway servers can communicate with each other and access each other's applications.

Details

The following figure illustrates the network characteristics of MyCo.



Human Resources Department

- iSeries-A runs on OS/400(R) Version 5 Release 2 (V5R2) and acts as the Human Resources Department's VPN gateway.
- Subnet is 10.6.0.0 with mask 255.255.0.0. This subnet represents the data endpoint of the VPN tunnel at the MyCo Rochester site.
- iSeries-A connects to the Internet with IP address 204.146.18.227. This is the connection endpoint. That is, iSeries-A performs key management and applies IPSec to incoming and outgoing IP datagrams.
- iSeries-A connects to its subnet with IP address 10.6.11.1.
- iSeries-B is a production server in the Human Resources subnet that runs standard TCP/IP applications.

Finance Department

- iSeries-C runs on OS/400 Version 5 Release 2 (V5R2) and acts as the Finance Department's VPN gateway.
- Subnet is 10.196.8.0 with mask 255.255.255.0. This subnet represents the data endpoint of the VPN tunnel at the MyCo Endicott site.
- iSeries-C connects to the Internet with IP address 208.222.150.250. This is the connection endpoint. That is, iSeries-C performs key management and applies IPSec to incoming and outgoing IP datagrams.
- iSeries-C connects to its subnet with IP address 10.196.8.5.

Configuration tasks

You must complete each of these tasks to configure the branch office connection described in this scenario:

1. Verify TCP/IP routing to ensure that the two gateway servers can communicate with each other across the Internet. This allows ensures that hosts on each subnet route properly to their respective gateway for access to the remote subnet.
   Note: Routing is beyond the scope of this topic. If you have questions, see TCP/IP routing and workload balancing in the Information Center.
2. Complete (page 6) the planning worksheets and checklists for both systems.
3. Configure (page 7) VPN on the Human Resources VPN gateway (iSeries-A).
4. Configure (page 8) VPN on the Finance VPN gateway (iSeries-C).
5. Make sure the VPN servers are started (page 8).
6. Test (page 8) communications between the two remote subnets.

Configuration details

After you complete the first step, verifying that TCP/IP routing is working properly and your gateway servers can communicate, you are ready to begin configuring the VPN.

Step 2: Complete the planning worksheets

The following planning checklists illustrate the type of information you need before you begin configuring the VPN. All answers on the prerequisite checklist must be YES before you proceed with VPN setup.

Note: These worksheets apply to iSeries-A, repeat the process for iSeries-C, reversing IP addresses as necessary.

Prerequisite checklist	Answers
Is your OS/400(R) V5R2 (5722-SS1) or later?	Yes
Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?	Yes
Is Cryptographic Access Provider (5722-AC2 or AC3) installed?	Yes
Is iSeries(TM) Access for Windows(R) (5722-XE1) installed?	Yes
Is iSeries Navigator installed?	Yes
Is the Network subcomponent of iSeries Navigator installed?	Yes
Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?	Yes
Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?	Yes
Is TCP/IP configured on your iSeries (including IP interfaces, routes, local host name, and local domain name)?	Yes
Is normal TCP/IP communication established between the required endpoints?	Yes

Prerequisite checklist	Answers
Have you applied the latest program temporary fixes (PTFs)?	Yes
If the VPN tunnel traverses firewalls or routers that use IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?	Yes
Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?	Yes
Are the firewalls configured to enable IP forwarding?	Yes

You need this information to configure the VPN	Answers
What type of connection are you creating?	gateway-to-gateway
What will you name the dynamic-key group?	HRgw2FINgw
What type of security and system performance do you require to protect your keys?	balanced
Are you using certificates to authenticate the connection? If no, what is the preshared key?	No topsecretstuff
What is the identifier of the local key server?	IP address: 204.146.18.227
What is the identifier of the local data endpoint?	Subnet: 10.6.0.0 Mask: 255.255.0.0
What is the identifier of the remote key server?	IP address: 208.222.150.250
What is the identifier of the remote data endpoint?	Subnet: 10.196.8.0 Mask: 255.255.255.0
What ports and protocols do you want to allow to flow through the connection?	Any
What type of security and system performance do you require to protect your data?	balanced
To which interfaces does the connection apply?	TRLINE

Step 3: Configure VPN on iSeries-A

Use the the information from your worksheets to configure VPN on iSeries-A as follows:

1. In iSeries Navigator, expand iSeries-A **—>Network —>IP Policies**.
2. Right-click **Virtual Private Networking** and select **New Connection** to start the New Connection wizard.
3. Review the **Welcome** page for information about what objects the wizard creates.
4. Click **Next** to go to the **Connection Name** page.
5. In the **Name** field, enter `HRgw2FINgw`.
6. (optional) Specify a description for this connection group.
7. Click **Next** to go to the **Connection Scenario** page.
8. Select **Connect your gateway to another gateway**.
9. Click **Next** to go to the **Internet Key Exchange Policy** page.
10. Select **Create a new policy** and then select **Balance security and performance**.
11. Click **Next** to go to the **Certificate for Local Connection Endpoint** page.
12. Select **No** to indicate that you will not be using certificates to authenticate the connection.
13. Click **Next** to go to the **Local Key Server** page.
14. Select **Version 4 IP address** from the **Identifier type** field.
15. Select `204.146.18.227` from the **IP address** field.
16. Click **Next** to go to the **Remote Key Server** page.
17. Select **Version 4 IP address** in the **Identifier type** field.
18. Enter `208.222.150.250` in the **Identifier** field.

19. Enter `topsecretstuff` in the **Pre-shared key** field.
20. Click **Next** to go to the **Local Data Endpoint** page.
21. Select **IP version 4 subnet** from the **Identifier type** field.
22. Enter `10.6.0.0` in the **Identifier** field.
23. Enter `255.255.0.0` in the **Subnet mask** field.
24. Click **Next** to go to the **Remote Data Endpoint** page.
25. Select **IP version 4 subnet** from the **Identifier type** field.
26. Enter `10.196.8.0` in the **Identifier** field.
27. Enter `255.255.255.0` in the **Subnet mask** field.
28. Click **Next** to go to the **Data Services** page.
29. Accept the default values, and then click **Next** to go to the **Data Policy** page.
30. Select **Create a new policy** and then select **Balance security and performance**. Select **Use the RC4 encryption algorithm**.
31. Click **Next** to go to the **Applicable Interfaces** page.
32. Select **TRLINE** from the **Line** table.
33. Click **Next** to go to the **Summary** page. Review the objects that the wizard will create to ensure they are correct.
34. Click **Finish** to complete the configuration.
35. When the **Activate Policy Filters** dialog box appears, select **Yes, activate the generated policy filters** then select **Permit all other traffic**. Click **OK** to complete the configuration. When prompted, specify that you want to activate the rules on all interfaces.

You are now finished configuring VPN on iSeries-A. The next step is to configure VPN on the Finance Department VPN gateway (iSeries-C).

Step 4: Configure VPN on iSeries-C

Follow the same steps you used to configure iSeries-A, reversing IP addresses as necessary. Use the planning worksheets for guidance. When you finish configuring the Finance Department VPN gateway, your connections will be in an *on-demand* state, which means the connection starts when IP datagrams that this VPN connection must protect are sent. The next step is to start the VPN servers, if they are not already started.

Step 6: Start the VPN servers

Follow these steps to start the VPN servers:

1. In iSeries Navigator, expand **the server —>Network —>IP Policies**.
2. Right-click **Virtual Private Networking** and select **Start**.

Step 7: Test connection

After you finish configuring both servers and you have successfully started the VPN servers, test the connectivity to ensure that the remote subnets can communicate with each other. To do this, follow these steps:

1. In iSeries Navigator, expand **iSeries-A —>Network**.
2. Right-click **TCP/IP Configuration** and select **Utilities** and then select **Ping**.
3. From the **Ping from** dialog box, enter `iSeries-C` in the **Ping** field.
4. Click **Ping Now** to verify connectivity from iSeries-A to iSeries-C.
5. Click **OK** when you are finished.

VPN scenario: Basic business to business connection

Many companies use frame relay or leased lines to provide secure communications with their business partners, subsidiaries, and vendors. Unfortunately, these solutions are often expensive and geographically limiting. VPN offers an alternative for companies who want private, cost-effective communications.

Suppose you are a major parts supplier to a manufacturer. Since it is critical that you have the specific parts and quantities at the exact time required by the manufacturing firm, you always need to be aware of the manufacturer's inventory status and production schedules. Perhaps you handle this interaction manually today, and find it time consuming, expensive and even inaccurate at times. You want to find an easier, faster, and more effective way to communicate with your manufacturing company. However, given the confidentiality and time-sensitive nature of the information you exchange, the manufacturer does not want to publish it on its corporate Web site or distribute it monthly in an external report. By exploiting the public Internet, you can easily establish a virtual private network (VPN) to meet the needs of both companies.

Objectives

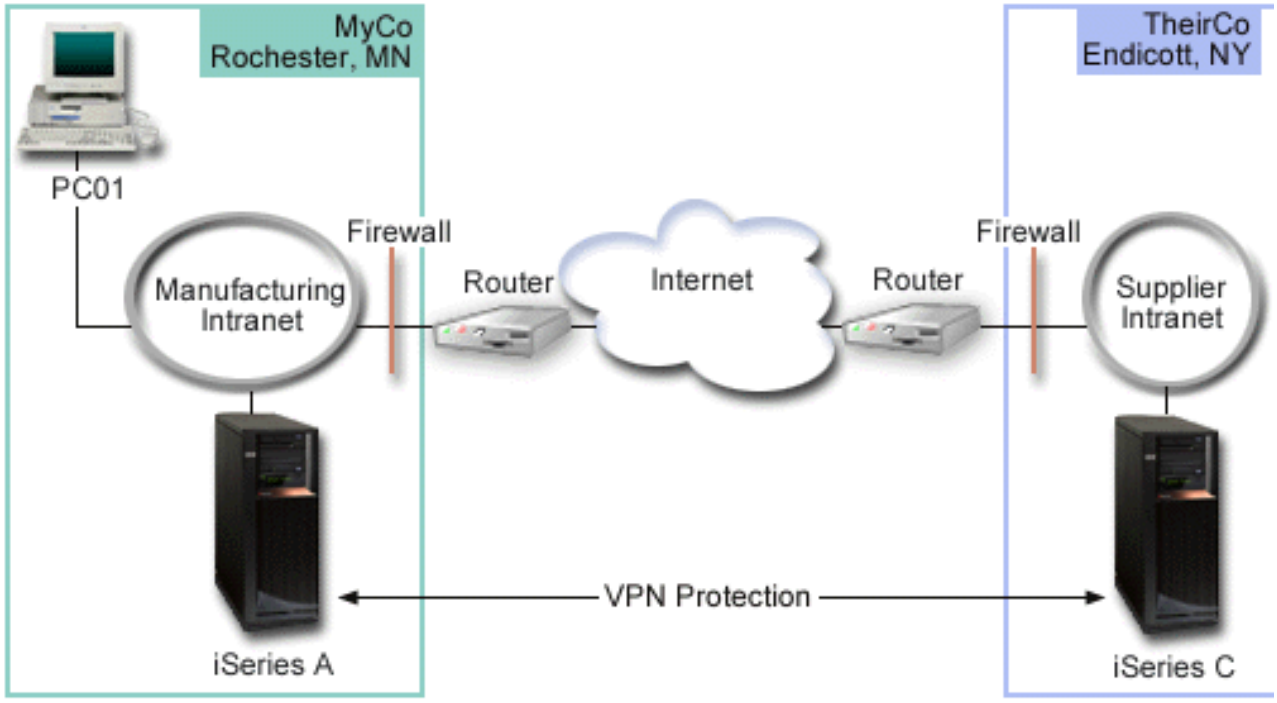
In this scenario, MyCo wants to establish a VPN between a host in its parts division and a host in the manufacturing department of one their business partners,TheirCo.

Because the information these two companies share is highly confidential, it must be protected while it travels across the Internet. In addition, data must not flow in the clear within either company's networks because each network considers the other untrusted. In other words, both companies require end-to-end authentication, integrity, and encryption.

Important note:
The intent of this scenario is to introduce, by example, a simple host-to-host VPN configuration. In a typical network environment, you will also need to consider firewall configuration, IP addressing requirements, and routing, among others.

Details

The following figure illustrates the network characteristics of MyCo and TheirCo:



MyCo Supply Network

- iSeries-A runs on OS/400(R) Version 5 Release 2 (V5R2).
- iSeries-A has an IP address of 10.6.1.1. This is the connection endpoint, as well as the data endpoint. That is, iSeries-A performs IKE negotiations and applies IPSec to incoming and outgoing IP datagrams and is also the source and destination for data that flows through the VPN.
- iSeries-A is in subnet 10.6.0.0 with mask 255.255.0.0
- Only iSeries-A can initiate the connection with iSeries-C.

TheirCo Manufacturing Network

- iSeries-C runs on OS/400 Version 5 Release 2 (V5R2).
- iSeries-C has an IP address of 10.196.8.6. This is the connection endpoint, as well as the data endpoint. That is, iSeries-A performs IKE negotiations and applies IPSec to incoming and outgoing IP datagrams and is also the source and destination for data that flows through the VPN.
- iSeries-C is in subnet 10.196.8.0 with mask 255.255.255.0

Configuration tasks

You must complete each of these tasks to configure the business to business connection described in this scenario:

1. Verify TCP/IP routing to ensure that iSeries-A and iSeries-C can communicate with each other across the Internet. This ensures that hosts on each subnet route properly to their respective gateway for access to the remote subnet. Be aware that for this scenario, you will need to consider the routing of private addresses that you may not have before.

   Note: Routing is beyond the scope of this topic. If you have questions, see TCP/IP routing and workload balancing topic in the Information Center.
2. Complete (page 11) the planning worksheets and checklists for both systems.
3. Configure (page 12) VPN on iSeries-A in MyCo's Supply network.
4. Configure (page 13) VPN on iSeries-C in TheirCo's Manufacturing network.

5. Activate (page 13) filter rules on both servers.
6. Start (page 13) the connection from iSeries-A.
7. Test (page 13) communications between the two remote subnets.

Configuration details

After you complete the first step, verifying that TCP/IP routing is working properly and your servers can communicate, you are ready to begin configuring the VPN.

Step 2: Complete the planning worksheets

The following planning checklists illustrate the type of information you need before you begin configuring the VPN. All answers on the prerequisite checklist must be YES before you proceed with VPN setup.

Note: These worksheets apply to iSeries-A, repeat the process for iSeries-C, reversing IP addresses as necessary.

Prerequisite checklist	**Answers**
Is your OS/400(R) V5R2 (5722-SS1) or later?	Yes
Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?	Yes
Is Cryptographic Access Provider (5722-AC2 or AC3) installed?	Yes
Is iSeries(TM) Access for Windows(R) (5722-XE1) installed?	Yes
Is iSeries Navigator installed?	Yes
Is the Network subcomponent of iSeries Navigator installed?	Yes
Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?	Yes
Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?	Yes
Is TCP/IP configured on your iSeries (including IP interfaces, routes, local host name, and local domain name)?	Yes
Is normal TCP/IP communication established between the required endpoints?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
If the VPN tunnel traverses firewalls or routers that use IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?	Yes
Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?	Yes
Are the firewalls configured to enable IP forwarding?	Yes

You need this information to configure the VPN	**Answers**
What type of connection are you creating?	host-to-host
What will you name the dynamic-key group?	MyCo2TheirCo
What type of security and system performance do you require to protect your keys?	highest
Are you using certificates to authenticate the connection? If no, what is the preshared key?	Yes
What is the identifier of the local key server?	IP address: 10.6.1.1
What is the identifier of the local data endpoint?	IP address: 10.6.1.1
What is the identifier of the remote key server?	IP address: 10.196.8.6
What is the identifier of the remote data endpoint?	IP address: 10.196.8.6
What ports and protocols do you want to allow to flow through the connection?	Any
What type of security and system performance do you require to protect your data?	highest

To which interfaces does the connection apply?	TRLINE

Step 3: Configure VPN on iSeries-A

Use the the information from your worksheets to configure VPN on iSeries-A as follows:

1. In iSeries Navigator, expand your server **—>Network —>IP Policies**.
2. Right-click **Virtual Private Networking** and select **New Connection** to start the Connection wizard.
3. Review the **Welcome** page for information about what objects the wizard creates.
4. Click **Next** to go to the **Connection Name** page.
5. In the **Name** field, enter `MyCo2TheirCo`.
6. (optional) Specify a description for this connection group.
7. Click **Next** to go to the **Connection Scenario** page.
8. Select **Connect your host to another host**.
9. Click **Next** to go to the **Internet Key Exchange Policy** page.
10. Select **Create a new policy** and then select **Highest security, lowest performance**.
11. Click **Next** to go to the **Certificate for Local Connection Endpoint** page.
12. Select **Yes** to indicate that you will be using certificates to authenticate the connection. Then, select the certificate that represents iSeries-A.
    Note: If you want to use a certificate to authenticate the local connection endpoint, you must first create the certificate in the Digital Certificate Manger (DCM).
13. Click **Next** to go to the **Local Connection Endpoint Identifier** page.
14. Select **Version 4 IP address** as the identifier type. The associated IP address must be 10.6.1.1. Again, this information is defined in the certificate that you create in DCM.
15. Click **Next** to go to the **Remote Key Server** page.
16. Select **Version 4 IP address** in the **Identifier type** field.
17. Enter `10.196.8.6` in the **Identifier** field.
18. Click **Next** to go to the **Data Services** page.
19. Accept the default values, and then click **Next** to go to the **Data Policy** page.
20. Select **Create a new policy** and then select **Highest security, lowest performance**. Select **Use the RC4 encryption algorithm**.
21. Click **Next** to go to the **Applicable Interfaces** page.
22. Select **TRLINE**.
23. Click **Next** to go to the **Summary** page. Review the objects that the wizard will create to ensure they are correct.
24. Click **Finish** to complete the configuration.
25. When the **Activate Policy Filters** dialog box appears, select **No, packet rules will be activated at a later time** and then click **OK**.

The next step is to specify that only iSeries-A can initiate this connection. Do this by customizing the properties of the dynamic-key group, MyCo2TheirCo, that the wizard created:

1. Click **By Group** in the left pane of the VPN interface, the new dynamic-key group, MyCo2TheirCo, displays in the right pane. Right-click it and select **Properties**.
2. Go to the **Policy** page and select the **Local system initiates connection** option.
3. Click **OK** to save your changes.

You are now finished configuring VPN on iSeries-A. The next step is to configure VPN on the iSeries-C in TheirCo's Manufacturing network.

Step 4: Configure VPN on iSeries-C

Follow the same steps you used to configure iSeries-A, reversing IP addresses as necessary. Use the planning worksheets for guidance. When you finish configuring iSeries-C, you must activate the filter rules that the Connection wizard created on each server.

Step 5: Activate packet rules

The wizard automatically creates the packet rules that this connection requires to work properly. However, you must activate them on both systems before you can start the VPN connection. To do this on iSeries-A, follow these steps:

1. In iSeries Navigator, expand **iSeries-A —>Network —>IP Policies**.
2. Right-click **Packet Rules** and select **Activate**. This opens the **Activate Packet Rules** dialog box.
3. Select whether you want to activate only the VPN generated rules, only a selected file, or both the VPN generated rules and a selected file. You might choose the latter, for instance, if you have miscellaneous PERMIT and DENY rules that you want to enforce on the interface in addition to the VPN generated rules.
4. Select the interface on which you want the rules activated. In this case, select **All interfaces**.
5. Click **OK** on the dialog box to confirm that you want to verify and activate the rules on the interface or interfaces you specified. After you click OK, the system checks the rules for syntax and semantic errors and reports the results in a message window at the bottom of the 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.
6. Repeat these steps to activate packet rules on iSeries-C.

Step 6: Start connection

Follow these steps to start the MyCo2TheirCo connection from iSeries-A:

1. In iSeries Navigator, expand **iSeries-A —>Network —>IP Policies**.
2. If the VPN server is not started, right-click **Virtual Private Networking** and select **Start**. This starts the VPN server.
3. Expand **Virtual Private Networking —>Secure Connections**.
4. Click **All Connections** to display a list of connections in the right pane.
5. Right-click **MyCo2TheirCo** and select **Start**.
6. From the **View** menu, select **Refresh**. If the connection starts successfully, the status will change from *Idle* to *Enabled*. The connection may take a few minutes to start, so periodically refresh until the status changes to *Enabled*.

Step 7: Test connection

After you finish configuring both servers and have successfully started the connection, test the connectivity to ensure that the remote hosts can communicate with each other. To do this, follow these steps:

1. In iSeries Navigator, expand **iSeries-A —>Network**.
2. Right-click **TCP/IP Configuration** and select **Utilities** and then select **Ping**.
3. From the **Ping from** dialog box, enter `iSeries-C` in the **Ping** field.
4. Click **Ping Now** to verify connectivity from iSeries-A to iSeries-C.
5. Click **OK** when you are finished.

VPN scenario: Protect an L2TP voluntary tunnel with IPSec

Suppose your company has a small branch office in another state. Throughout any given workday the branch office may require access to confidential information about an iSeries(TM) within your corporate intranet. Your company currently uses an expensive leased line to provide the branch office access to the

corporate network. Although your company wants to continue providing secure access to your intranet, you ultimately want to reduce the expense associated with the leased line. This can be done by creating a Layer 2 Tunnel Protocol (L2TP) voluntary tunnel that extends your corporate network, such that the branch office appears to be part of your corporate subnet. VPN protects the data traffic over the L2TP tunnel.

With an L2TP voluntary tunnel, the remote branch office establishes a tunnel directly to the L2TP network server (LNS) of the corporate network. The functionality of the L2TP access concentrator (LAC) resides at the client. The tunnel is transparent to the remote client's Internet Service Provider (ISP), so the ISP is not required to support L2TP. If you want to read more about L2TP concepts, see "Layer 2 Tunnel Protocol (L2TP)" on page 26.

> **Important note:**
> This scenario shows the iSeries security gateways attached directly to the Internet. The absence of a firewall is intended to simplify the scenario. It does not imply that the use of a firewall is not necessary. Consider the security risks involved any time you connect to the Internet. Review this redbook, AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> , for a detailed description of various methods for reducing these risks.

Objectives

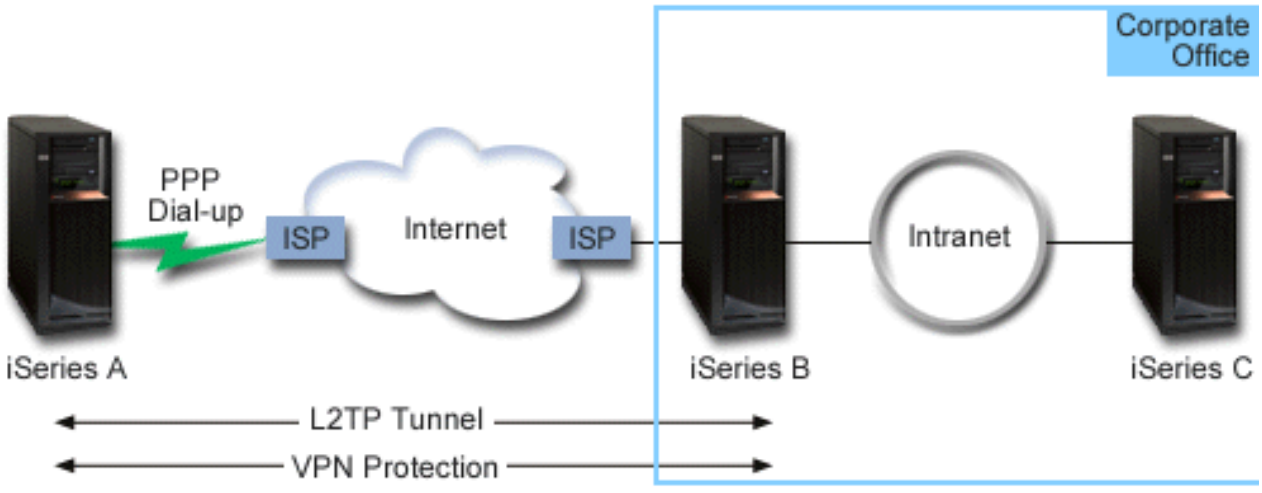
In this scenario, a branch office iSeries connects to its corporate network through a gateway iSeries with an L2TP tunnel protected by VPN.

The main objectives of this scenario are:

- The branch office system always initiates the connection to the corporate office.
- The branch office system is the only system at the branch office network that needs access to the corporate network. In other words, its role is that of a host, not a gateway, in the branch office network.
- The corporate system a host computer in the corporate office network.

Details

The following figure illustrates the network characteristics for this scenario:



iSeries-A

- Must have access to TCP/IP applications on all systmes in the corporate network.
- Receives dynamically assigned IP addresses from its ISP.
- Must be configured to provide L2TP support.

iSeries-B

- Must have access to TCP/IP applications on iSeries-A.
- Subnet is 10.6.0.0 with mask 255.255.0.0. This subnet represents the data endpoint of the VPN tunnel at the corporate site.
- Connects to the Internet with IP address 205.13.237.6. This is the connection endpoint. That is, iSeries-B performs key management and applies IPSec to incoming and outgoing IP datagrams. iSeries-B connects to its subnet with IP address 10.6.11.1.

In L2TP terms, *iSeries-A* acts as the L2TP initiator, while *iSeries-B* acts as the L2TP terminator.

Configuration tasks

Assuming that TCP/IP configuration already exists and works, you must complete the following tasks:

1. Configure VPN (page 15) on iSeries-A.
2. Configure a PPP (page 17) connection profile and virtual line for iSeries-A.
3. Apply (page 18)the dynamic-key group to the PPP profile.
4. Configure VPN (page 18) on iSeries-B.
5. Configure a PPP (page 18) connection profile and virtual line for iSeries-B.
6. Activate (page 19) packet rules on iSeries-A and iSeries-B.
7. Start (page 19) the connection from iSeries-A.

Configuration details

After you verify that TCP/IP is working properly and your iSeries(TM) servers can communicate, you are ready to begin configuring the connection described in this scenario.

Step 1: Configure VPN on iSeries-A

Follow these steps to configure VPN on iSeries-A:

1. **Configure the Internet Key Exchange policy**
   a. In iSeries Navigator, expand iSeries-A **—> Network—> IP Policies—> Virtual Private Networking—> IP Security Policies**.
   b. Right-click **Internet Key Exchange Policies** and select **New Internet Key Exchange Policy**
   c. On the **Remote Server** page, select **Version 4 IP address** as the identifier type and then enter `205.13.237.6` in the **IP address** field.
   d. On the **Associations** page, select **Preshared key** to indicate that this connection uses a preshared key to authenticate this policy.
   e. Enter the preshared key in the **Key** field. Treat your preshared key like a password.
   f. Select **Key Identifier** for the local key server identifier type, and then enter the key identifier in the **Identifier** field. For example, `thisisthekeyid`. Remember that the local key server has a dynamically assigned IP address which is impossible to know in advance. iSeries-B uses this identifier to identify the iSeries-A when iSeries-A initiates a connection.
   g. On the **Transforms** page, click **Add** to add the transforms that iSeries-A proposes to iSeries-B for key protection and to specify whether the IKE policy uses identity protection when initiating phase 1 negotiations.
   h. On the **IKE Policy Transform** page, select **Preshared key** for your authentication method, **SHA** for your hash algorithm, and **3DES-CBC** for your encryption algorithm. Accept the default values for Diffie-Hellman group and Expire IKE keys after.
   i. Click **OK** to return to the **Transforms** page.

j. Select **IKE aggressive mode negotiation (no identity protection).**

Note: If you use preshared keys and aggressive mode negotiation together in your configuration, select obscure passwords that are unlikely to be cracked in attacks that scan the dictionary. It is also recommended you periodically change your passwords.

k. Click **OK** to save your configurations.

2. **Configure the data policy**
   a. From the VPN interface, right-click **Data policies** and select **New Data Policy**.
   b. On the **General** page, specify the name of the data policy. For example, `l2tpremoteuser`.
   c. Go to the **Proposals** page. A proposal is a collection of protocols that the initiating and responding key servers use to establish a dynamic connection between two endpoints. You can use a single data policy in several connection objects. However, not all remote VPN key servers necessarily have the same data policy properties. Therefore, you can add several proposals to one data policy. When establishing a VPN connection to a remote key server, there must be at least one matching proposal in the data policy of the initiator and the responder.
   d. Click **Add** to add a data policy transform.
   e. Select **Transport** for the encapsulation mode.
   f. Specify a key expiration value.
   g. Click **OK** to return to the **Transforms** page.
   h. Click **OK** to save your new data policy.
3. **Configure the dynamic-key group**
4.
   a. From the VPN interface, expand **Secure Connections**.
   b. Right-click **By Group** and select **New Dynamic-Key Group**.
   c. On the **General** page, specify a name for the group. For example, `l2tptocorp`.
   d. Select **Protects a locally initiated L2TP tunnel**.
   e. For system role, select **Both systems are hosts**.
   f. Go to the **Policy** page. Select the data policy you created in step two, `l2tpremoteuser`, from the **Data policy** drop-down list.
   g. Select **Local system initiates connection** to indicate that only iSeries-A can initiate connections with iSeries-B.
   h. Go to the **Connections** page. Select **Generate the following policy filter rule for this group**. Click **Edit** to define the parameters of the policy filter.
   i. On the **Policy Filter- Local Addresses** page, select **Key Identifier** for the identifier type.
   j. For the identifier, select the key identifier, `thisisthekeyid`, that you defined in the IKE policy.
   k. Go the the **Policy Filter - Remote Addresses** page. Select **IP version 4 address** from the **Identifier type** drop-down list.
   l. Enter `205.13.237.6` in the **Identifier** field.
   m. Go to the **Policy Filter - Services** page. Enter `1701` in the **Local Port** and **Remote Port** fields. Port 1701 is the well-known port for L2TP.
   n. Select **UDP** from the **Protocol** drop-down list.
   o. Click **OK** to return to the **Connections** page.
   p. Go to the **Interfaces** page. Select any line or PPP profile to which this group will apply. You have not created the PPP profile for this group yet. After you do so, you will need to edit the properties of this group so that the group applies to the PPP profile you create in the next step.
   q. Click **OK** to create the dynamic-key group, l2tptocorp.

You now need to add a connection to the group you just created.

5. **Configure the dynamic-key connection**
   a. From the VPN interface, expand **By Group**. This displays a list of all dynamic-key groups you have configured on iSeries-A.
   b. Right-click **l2tptocorp** and select **New Dynamic-Key Connection**.
   c. On the **General** page, specify an optional description for the connection.
   d. For the remote key server, select **Version 4 IP address** for the identifier type.
   e. Select `205.13.237.6` from the **IP address** drop-down list.
   f. Deselect **Start on-demand**.
   g. Go to the **Local Addresses** page. Select **Key identifier** for the identifier type and then select `thisisthekeyid` from the **Identifier** drop-down list.
   h. Go to the **Remote Addresses** page. Select **IP version 4 address** for the identifier type.
   i. Enter `205.13.237.6` in the **Identifier** field.
   j. Go to the **Services** page. Enter `1701` in the **Local Port** and **Remote Port** fields. Port 1701 is the well-known port for L2TP.
   k. Select **UDP** from the **Protocol** drop-down list.
   l. Click **OK** to create the dynamic-key connection.

You are now finished configuring VPN on iSeries-A. The next step is to configure a PPP profile for iSeries-A.

Step 2: Configure a PPP connection profile and virtual line on iSeries-A

This section describes the steps you must take to create the PPP profile for iSeries-A. The PPP profile has no physical line associated with it; instead, it uses a virtual line. This is because the PPP traffic tunnels through the L2TP tunnel, while VPN protects the L2TP tunnel.

Follow these steps to create a PPP connection profile for iSeries-A:

1. In iSeries Navigator, expand iSeries-A **—>Network—>Remote Access Services**.
2. Right-click **Originator Connection Profiles** and select **New Profile**.
3. On the **Setup** page, select **PPP** for the protocol type.
4. For Mode selections, select **L2TP (virtual line)**.
5. Select **Initiator on-demand (voluntary tunnel)** from the **Operating mode** drop-down list.
6. Click **OK** to go to the PPP profiles properties pages.
7. On the **General** page, enter a name that identifies the type and the destination of the connection. In this case, enter `toCORP`. The name you specify must be 10 characters, or less.
8. (optional) Specify a description for the profile.
9. Go to the **Connection** page.
10. In the **Virtual line name** field, select **tocorp** from the drop-down list. Remember that this line has no associated physical interface. The virtual line describes various characteristics of this PPP profile; for example, the maximum frame size, authentication information, the local host name, and so on. The **L2TP Line Properties** dialog box opens.
11. On the **General** page, enter a description for the virtual line.
12. Go to the **Authentication** page.
13. In the **Local host name** field, enter the host name of the local key server, `iSeriesA`.
14. Click **OK** to save the new virtual line description and return to the **Connection** page.
15. Enter the remote tunnel endpoint address, `205.13.237.6`, in the **Remote tunnel endpoint address** field.

16. Select **Requires IPSec Protection** and select the dynamic-key group you created in step one, `l2tptocorp` from the **Connection group name** drop-down list.
17. Go to the **TCP/IP Settings** page.
18. In the **Local IP address** section, select **Assigned by remote system**.
19. In the **Remote IP address** section, select **Use fixed IP address**. Enter `10.6.11.1`, which is the remote system's IP address in its subnet.
20. In the routing section, select **Define additional static routes** and click **Routes**. If there is no routing information provided in the PPP profile, then iSeries-A is only able to reach the remote tunnel endpoint but not any other system on the 10.6.0.0 subnet.
21. Click **Add** to add a static route entry.
22. Enter the subnet, `10.6.0.0`, and the subnet mask, `255.255.0.0` to route all 10.6.*.* traffic through the L2TP tunnel.
23. Click **OK** to add the static route.
24. Click **OK** to close the Routing dialog box.
25. Go to the **Authentication** page to set the user name and password for this PPP profile.
26. In the Local system identification section, select **Allow the remote system to verify the identity of this system**.
27. Under **Authentication protocol to use** select **Require encrypted password (CHAP-MD5)**
28. Enter the user name, `iSeriesA`, and a password.
29. Click **OK** to save the PPP profile.

Step 3: Apply the l2tptocorp dynamic-key group to the toCorp PPP profile

After you have your PPP connection profile configured, you need to go back to the dynamic-key group, `l2tptocorp`, you created and associate it with the PPP profile. To do this, follow these steps:

1. Navigate to the VPN interface, then expand **Secure Connections—>By Group**.
2. Right-click the dynamic-key group, `l2tptocorp`, and select **Properties**.
3. Go to the **Interfaces** page and select **Apply this group** for the PPP profile you created in step two, `toCorp`.
4. Click **OK** to apply `l2tptocorp` to the PPP profile, `toCorp`.

Step 4: Configure VPN on iSeries-B

Follow the same steps you used to configure iSeries-A, reversing IP addresses and identifiers as necessary. Take these other points into consideration before you begin:

- The identify the remote key server by the key identifier you specified for the local key server on iSeries-A. For example, `thisisthekeyid`.
- Use the *exact* same preshared key.
- Make sure your transforms match the ones you configured on iSeries-A, or connections will fail.
- Do not specify **Protects a locally initiated L2TP tunnel** on the **General** page of the dynamic-key group.
- Remote system initiates the connection.
- Specify that the connection should start on-demand.

Step 5: Configure a PPP connection profile and virtual line on iSeries-B

Follow these steps to create a PPP connection profile for iSeries-B:

1. In iSeries Navigator, expand iSeries-B **—>Network—> Remote Access Services**.
2. Right-click **Responder Connection Profiles** and select **New Profile**.
3. On the **Setup** page, select **PPP** for the protocol type.
4. For Mode selections, select **L2TP (virtual line)**.

5. Select **Terminator (network server)** from the **Operating mode** drop-down list.
6. Click **OK** to PPP profiles properties pages.
7. On the **General** page, enter a name that identifies the type and the destination of the connection. In this case, enter `tobranch`. The name you specify must be 10 characters, or less.
8. (optional) Specify a description for the profile.
9. Go to the **Connection** page.
10. Select the IP address of the local tunnel endpoint, 205.13.237.6.
11. In the **Virtual line name** field, select **tobranch** from the drop-down list. Remember that this line has no associated physical interface. The virtual line describes various characteristics of this PPP profile; for example, the maximum frame size, authentication information, the local host name, and so on. The **L2TP Line Properties** dialog box opens.
12. On the **General** page, enter a description for the virtual line.
13. Go to the **Authentication** page.
14. In the **Local host name** field, enter the host name of the local key server, `iSeriesB`.
15. Click **OK** to save the new virtual line description and return to the **Connection** page.
16. Go to the **TCP/IP Settings** page.
17. In the **Local IP address** section, select the fixed IP address of the local system, 10.6.11.1.
18. In the **Remote IP address** section, select **Address pool** as the address assignment method . Enter a starting address, and then specify the number of addresses that can be assigned to the remote system.
19. Select **Allow remote system to access other networks (IP forwarding)**.
20. Go to the **Authentication** page to set the user name and password for this PPP profile.
21. In the Local system identification section, select **Allow the remote system to verify the identity of this system**. This opens the **Local System Identification** dialog box.
22. Under **Authentication protocol to use** select **Require encrypted password (CHAP-MD5)**
23. Enter the user name, `iSeriesB`, and a password.
24. Click **OK** to save the PPP profile.

Step 6: Activate packet rules

VPN automatically creates the packet rules that this connection requires to work properly. However, you must activate them on both systems before you can start the VPN connection. To do this on iSeries-A, follow these steps:

1. In iSeries Navigator, expand **iSeries-A —>Network —>IP Policies**.
2. Right-click **Packet Rules** and select **Activate**. This opens the **Activate Packet Rules** dialog box.
3. Select whether you want to activate only the VPN generated rules, only a selected file, or both the VPN generated rules and a selected file. You might choose the latter, for instance, if you have miscellaneous PERMIT and DENY rules that you want to enforce on the interface in addition to the VPN generated rules.
4. Select the interface on which you want the rules activated. In this case, select **All interfaces**.
5. Click **OK** on the dialog box to confirm that you want to verify and activate the rules on the interface or interfaces you specified. After you click OK, the system checks the rules for syntax and semantic errors and reports the results in a message window at the bottom of the 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.
6. Repeat these steps to activate packet rules on iSeries-B.

Step 7: Start connection

The final step is to start the connection. Before you can initiate an L2TP connection, you must enable the

L2TP terminator to respond to initiator requests. After you ensure that all the required services are started, start the PPP connection on the terminator side. The following steps describe how to start the PPP connection on iSeries-B:

1. In iSeries Navigator, expand iSeries-B **—> Network—> Remote Access Services**.
2. Click **Responder Connection Profiles** to display a list of responder profiles in the right-pane.
3. Right-click `tobranch` and select **Start**. After the connection profile starts, the window refreshes and shows the connection as `Waiting for connection requests`. iSeries-A can now respond to L2TP connection requests from iSeries-B.

Follow these steps to start the L2TP connection on iSeries-A:

1. In iSeries Navigator, expand iSeries-A **—> Network—> Remote Access Services**.
2. Click **Originator Connection Profiles** to display a list of responder profiles in the right-pane.
3. Right-click **toCORP**, and select **Start**. After the connection profile starts, the window refreshes and shows the connection as `Establishing L2TP tunnel`.
4. Press F5 to refresh the screen. If the L2TP tunnel started successfully, the connection status will now say `Active connections`.

VPN scenario: Use network address translation for VPN

Suppose you are the network administrator for a small manufacturing company in Minneapolis. One of your business partners, a parts supplier in Chicago, wants to starting doing more of their business with your company over the Internet. It is critical that your company have the specific parts and quantities at the exact time it needs them, so the supplier needs to be aware of your company's inventory status and production schedules. Currently you handle this interaction manually, but you find it time consuming, expensive and even inaccurate at times, so you are more than willing to investigate your options.

Given the confidentiality and time-sensitive nature of the information you exchange, you decide to create a VPN between your supplier's network and your company's network. To further protect the privacy of your company's network structure, you decide you will need to hide the private IP address of the iSeries(TM) that hosts the applications to which the supplier has access. The question is: How do you make this work?

The answer: OS/400(R) VPN. Use it to not only create the connection definitions on the VPN gateway in your company's network, but also to provide the address translation you need to hide your local private addresses. Unlike conventional network address translation (NAT), which changes the IP addresses in the security associations (SAs) that VPN requires to function, VPN NAT performs address translation before the SA validation by assigning an address to the connection when the connection starts.

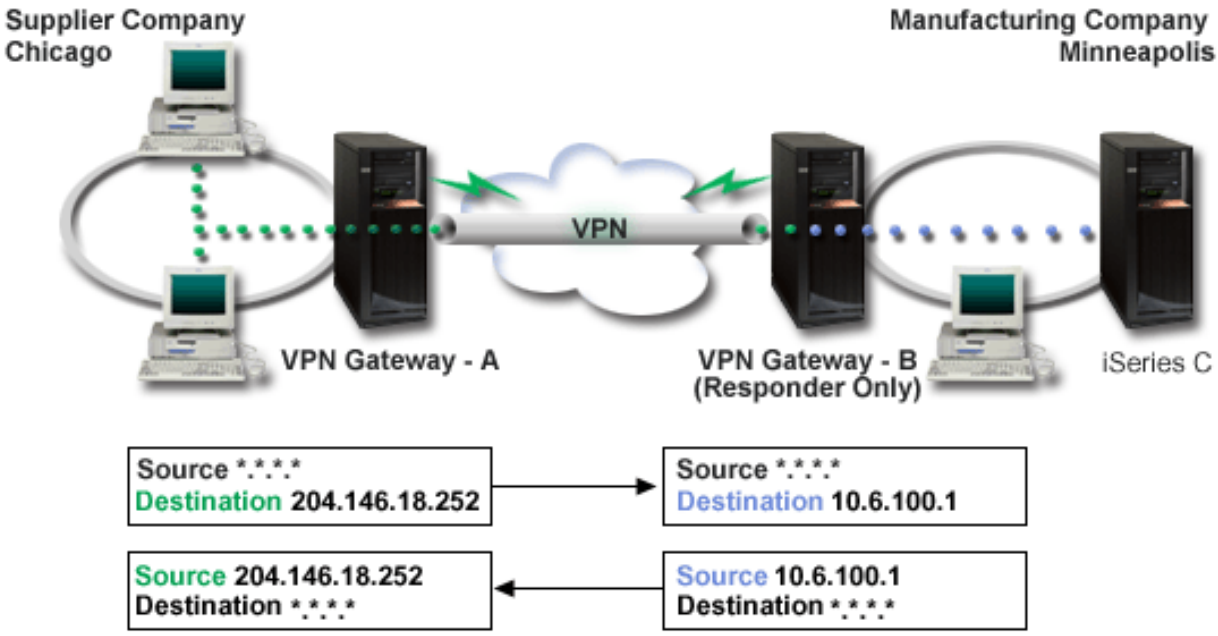
Objectives

The objectives of this scenario are to:

- allow all clients in the supplier network to access a single host iSeries in the manufacturer's network over a gateway-to-gateway VPN connection.
- hide the private IP address of the host iSeries in the manufacturer's network, by translating it to a public IP address by using network address translation for VPN (VPN NAT).

Details

The following diagram illustrates the network characteristics of both the supplier network and the manufacturing network:



- VPN gateway-A is configured to always initiate connections to VPN gateway-B.
- VPN gateway-A defines the destination endpoint for the connection as 204.146.18.252 (the public address assigned to iSeries-C).
- iSeries-C has a private IP address in the manufacturer's network of 10.6.100.1.
- A public address of 204.146.18.252 has been defined in the local service pool on VPN gateway-B for iSeries-C's private address, 10.6.100.1.
- VPN gateway-B translates iSeries-C's public address to its private address, 10.6.100.1, for inbound datagrams. VPN gateway-B translates returning, outbound, datagrams from 10.6.100.1 back to iSeries-C's public address, 204.146.18.252. As far as clients in the supplier network are concerned, iSeries-C has an IP address of 204.146.18.252. They will never be aware that address translation has occured.

Configuration Tasks

You must complete each of the following tasks to configure the connection described in this scenario:

1. Configure a basic gateway-to-gateway VPN between **VPN gateway-A** and **VPN gateway-B**.
2. Define a local service pool on **VPN gateway-B** to hide **iSeries-C**'s private address behind the public identifier, 204.146.18.252.
3. Configure **VPN gateway-B** to translate local addresses using local service pool addresses.

VPN concepts

Virtual private networking (VPN) uses several important TCP/IP protocols to protect data traffic. To better understand how any VPN connection works, familiarize yourself with these protocols and concepts and how OS/400(R) VPN uses them:

- "IP Security (IPSec) protocols" on page 22
  IPSec provides a stable, long lasting base for providing network layer security.
- "Key management" on page 25
  A dynamic VPN provides additional security for your communications by using the Internet Key Exchange (IKE) protocol for key management. IKE allows the VPN servers on each end of the connection to negotiate new keys at specified intervals.

- “Layer 2 Tunnel Protocol (L2TP)” on page 26
  If you plan to use a VPN connection to secure communications between your network and remote clients, you must also be familiar with L2TP.
- “Network address translation for VPN” on page 27
  OS/400 VPN provides a means for performing network address translation, called VPN NAT. VPN NAT differs from traditional NAT in that it translates addresses before applying the IKE and IPSec protocols. Refer to this topic to learn more.
- “NAT compatible IPSec” on page 28
  UDP encapsulation allows IPSec traffic to pass through a conventional NAT device. Review this topic for more information about what it is and why you should use it for your VPN connections.
- “IP Compression (IPComp)” on page 29
  IPComp reduces the size of IP datagrams by compressing the datagrams to increase the communication performance between two VPN partners.
- “VPN and IP filtering” on page 30
  IP filtering and VPN are closely related. In fact, most VPN connections require filter rules to work properly. This topic provides you information about what filters VPN requires, as well as other filtering concepts related to VPN.

IP Security (IPSec) protocols

IPSec provides a stable, long lasting base for providing network layer security. It supports all of the cryptographic algorithms in use today, and can also accommodate newer, more powerful algorithms as they become available. IPSec protocols address these major security issues:

Data origin authentication
Verifies that each datagram was originated by the claimed sender.
Data integrity
Verifies that the contents of a datagram were not changed in transit, either deliberately or due to random errors.
Data confidentiality
Conceals the content of a message, typically by using encryption.
Replay protection
Ensures that an attacker cannot intercept a datagram and play it back at some later time.
Automated management of cryptographic keys and security associations
Ensures that your VPN policy can be used throughout the extended network with little or no manual configuration.

VPN uses two IPSec protocols to protect data as it flows through the VPN: Authentication Header (AH) and Encapsulating Security Payload (ESP). The other part of IPSec enablement is the Internet Key Exchange (IKE) protocol, or key management. While IPSec encrypts your data, IKE supports automated negotiation of security associations (SAs), and automated generation and refreshing of cryptographic keys.

The principal IPSec protocols are listed below:

- “Authentication Header” on page 23
- “Encapsulating Security Payload” on page 24
- “AH and ESP combined” on page 25
- “Key management” on page 25

The Internet Engineering Task Force (IETF) formally defines IPSec in Request for Comment (RFC) 2401, *Security Architecture for the Internet Protocol*. You can view this RFC on the Internet at the following Web site: http://www.rfc-editor.org

.

Authentication Header

The Authentication Header (AH) protocol provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality, which means that all of your data is sent in the clear.

AH ensures data integrity with the checksum that a message authentication code, like MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the AH header. It is worth noting here, that these three distinct functions are often lumped together and referred to as **authentication**. In the simplest terms, AH ensures that your data has not been tampered with enroute to its final destination.

Although AH authenticates as much of the IP datagram as possible, the values of certain fields in the IP header cannot be predicted by the receiver. AH does not protect these fields, known as **mutable** fields. However, AH always protects the payload of the IP packet.

The Internet Engineering Task Force (IETF) formally defines AH in Request for Comment (RFC) 2402, *IP Authentication Header*. You can view this RFC on the Internet at the following Web site: http://www.rfc-editor.org

.

Ways of using AH

You can apply AH in two ways: transport mode or tunnel mode. In transport mode, the IP header of the datagram is the outermost IP header, followed by the AH header and then the payload of the datagram. AH authenticates the entire datagram, except the mutable fields. However, the information contained in the datagram is transported in the clear and is, therefore, subject to eavesdropping. Transport mode requires less processing overhead than tunnel mode, but does not provide as much security.

Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram. The AH header follows the new IP header. The original datagram (both the IP header and the original payload) comes last. AH authenticates the entire datagram, which means that the responding system can detect whether the datagram changed while in transit.

When either end of a security association is a gateway, use tunnel mode. In tunnel mode the source and destination addresses in the outermost IP header do not need to be the same as those in the original IP header. For example, two security gateways may operate an AH tunnel to authenticate all traffic between the networks they connect together. In fact, this is a very typical configuration.

The main advantage to using tunnel mode, is that tunnel mode totally protects the encapsulated IP datagram. In addition, tunnel mode makes it possible to use private addresses.

Why AH?

In many cases, your data only requires authentication. While the “Encapsulating Security Payload” on page 24 protocol can perform authentication, AH does not affect your system performance as does ESP. Another advantage of using AH, is that AH authenticates the entire datagram. ESP, however, does not authenticate the leading IP header or any other information that comes before the ESP header.

In addition, ESP requires strong cryptographic algorithms in order to be put into effect. Strong cryptography is restricted in some countries, while AH is not regulated and can be used freely around the world.

What algorithms does AH use to protect my information?

AH uses algorithms known as **hashed message authentication codes (HMAC)**. Specifically, VPN uses

either HMAC-MD5 or HMAC-SHA. Both MD5 and SHA take variable-length input data and a secret key to produce fixed-length output data (called a hash value). If the hashes of two messages match, then it is very likely that the messages are the same. Both MD5 and SHA encode the message length in their output, but SHA is regarded as more secure because it produces larger hashes.

The Internet Engineering Task Force (IETF) formally defines HMAC-MD5 in Request for Comments (RFC) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. The Internet Engineering Task Force (IETF) formally defines HMAC-SHA in Request for Comments (RFC) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. You can view these RFCs on the Internet at the following Web site: http://www.rfc-editor.org

.

Encapsulating Security Payload

The Encapsulating Security Payload (ESP) protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection. The difference between ESP and the "Authentication Header" on page 23 protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

If you decide to use both encryption and authentication, then the responding system first authenticates the packet and then, if the first step succeeds, the system proceeds with decryption. This type of configuration reduces processing overhead, as well as reduces your vulnerability to denial-of-service attacks.

Two ways of using ESP

You can apply ESP in two ways: transport mode or tunnel mode. In transport mode, the ESP header follows the IP header of the original IP datagram. If the datagram already has an IPSec header, then the ESP header goes before it. The ESP trailer and the optional authentication data follow the payload.

Transport mode does not authenticate or encrypt the IP header, which might expose your addressing information to potential attackers while the datagram is in transit. Transport mode requires less processing overhead than tunnel mode, but does not provide as much security. In most cases, hosts use ESP in transport mode.

Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram, followed by the ESP header and then the original datagram (both the IP header and the original payload). The ESP trailer and the optional authentication data are appended to the payload. When you use both encryption and authentication, ESP completely protects the original datagram because it is now the payload data for the new ESP packet. ESP, however, does not protect the new IP header. Gateways must use ESP in tunnel mode.

What algorithms does ESP use to protect my information?

ESP uses a symmetric key that both communicating parties use to encrypt and decrypt the data they exchange. The sender and the receiver must agree on the key before secure communication takes place between them. OS/400(R) VPN uses Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4, or Advanced Encryption Standard (AES) for encryption.

The Internet Engineering Task Force (IETF) formally defines DES in Request for Comment (RFC) 1829, *The ESP DES-CBC Transform*. The Internet Engineering Task Force (IETF) formally defines 3DES in RFC 1851, *The ESP Triple DES Transform*. You can view these and other RFCs on the Internet at the following Web address: http://www.rfc-editor.org

.

ESP uses HMAC-MD5 and HMAC-SHA algorithms to provide authentication functions. Both MD5 and SHA take variable-length input data and a secret key to produce fixed-length output data (called a hash value). If the hashes of two messages match, then it is very likely that the messages are the same. Both MD5 and SHA encode the message length in their output, but SHA is regarded as more secure because it produces larger hashes.

The Internet Engineering Task Force (IETF) formally defines HMAC-MD5 in Request for Comments (RFC) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. The Internet Engineering Task Force (IETF) formally defines HMAC-SHA in Request for Comments (RFC) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. You can view these and other RFCs on the Internet at the following Web address: http://www.rfc-editor.org

.

AH and ESP combined

VPN allows you to combine AH and ESP for host-to-host connections in transport mode. Combining these protocols protects the entire IP datagram. Although combining the two protocols offers more security, the processing overhead involved may outweigh the benefit.

Key management

With each successful negotiation, the VPN servers regenerate the keys that protect a connection, thus making it more difficult for an attacker to capture information from the connection. Additionally, if you use perfect forward secrecy, attackers cannot derive future keys based on past keying information.

The VPN key manager is IBM(TM)s implementation of the Internet Key Exchange (IKE) protocol. The key manager supports the automatic negotiation of security associations (SAs), as well as the automatic generation and refresh of cryptographic keys.

A **security association (SA)** contains information that is necessary to use the IPSec protocols. For example, an SA identifies algorithm types, key lengths and lifetimes, participating parties, and encapsulation modes.

Cryptographic keys, as the name implies, lock, or protect, your information until it safely reaches its final destination.

Note: Securely generating your keys is the most important factor in establishing a secure and private connection. If your keys are compromised, then your authentication and encryption efforts, no matter how strong, become worthless.

Phases of key management

The VPN key manager uses two distinct phases in its implementation.

Phase 1

Phase 1 establishes a master secret from which subsequent cryptographic keys are derived in order to protect user data traffic. This is true even if no security protection yet exists between the two endpoints. VPN uses either RSA signature mode or preshared keys to authenticate phase 1 negotiations, as well as to establish the keys that protect the IKE messages that flow during the subsequent phase 2 negotiations.

A *preshared key* is a nontrivial string up to 128 characters long. Both ends of a connection must agree on the preshared key. The advantage of using preshared keys is their simplicity, the disadvantage is

that a shared secret must be distributed out-of-band, for example over the telephone or through registered mail, before IKE negotiations. Treat your preshared key like a password.

RSA Signature authentication provides more security than preshared keys because this mode uses digital certificates to provide authentication. You must configure your digital certificates by using Digital Certificate Manager (5722-SS1 Option 34). In addition, some VPN solutions require RSA Signature for interoperability. For example, Windows(R) 2000 VPN uses RSA Signature as its default authentication method. Finally, RSA Signature provides more scalability than preshared keys. The certificates that you use must come from certificate authorities that both key servers trust.

Phase 2
Phase 2, however, negotiates the security associations and keys that protect the actual application data exchanges. Remember, up to this point, no application data has actually been sent. Phase 1 protects the phase 2 IKE messages.

Once phase 2 negotiations are complete, your VPN establishes a secure, dynamic connection over the network and between the endpoints that you defined for your connection. All data that flows across the VPN is delivered with the degree of security and efficiency that was agreed on by the key servers during the phase 1 and phase 2 negotiation processes.

In general, phase 1 negotiations are negotiated once a day, while phase 2 negotiations are refreshed every 60 minutes or as often as every five minutes. Higher refresh rates increase your data security, but decrease system performance. Use short key lifetimes to protect your most sensitive data.

When you create a dynamic VPN by using iSeries(TM) Navigator, you must "Configure an Internet Key Exchange (IKE) policy" on page 39 to enable phase 1 negotiations and a "Configure a data policy" on page 39 to govern phase 2 negotiations. Optionally, you can use the New Connection wizard. The wizard automatically creates each of the configuration objects VPN requires to work properly, including an IKE policy, data policy.

Suggested reading
If you want to read more about the Internet Key Exchange (IKE) protocol and key management, review these Internet Engineering Task Force (IETF) Request for Comments (RFC):

- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*

You can view these RFCs on the Internet at the following Web site: http://www.rfc-editor.org

.

Layer 2 Tunnel Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) connections, which are also called virtual lines, provide cost-effective access for remote users by allowing a corporate network server to manage the IP addresses assigned to its remote users. Further, L2TP connections provide secure access to your system or network when you use them in conjunction with IP Security (IPSec).

L2TP supports two tunnel modes: the voluntary tunnel and the compulsory tunnel. The major difference between these two tunnel modes is the endpoint. On the voluntary tunnel, the tunnel ends at the remote client whereas the compulsory tunnel ends at the ISP.

With an L2TP **compulsory tunnel**, a remote host initiates a connection to its Internet Service Provider (ISP). The ISP then establishes an L2TP connection between the remote user and the corporate network. Although the ISP establishes the connection, you decide how to protect the traffic by using VPN. With a compulsory tunnel, the ISP must support LT2P.

With an L2TP **voluntary tunnel**, the connection is created by the remote user, typically by using an L2TP tunneling client. As a result, the remote user sends L2TP packets to its ISP which forwards them on to the corporate network. With a voluntary tunnel, the ISP does not need to support L2TP. The scenario, *"VPN scenario: Protect an L2TP voluntary tunnel with IPSec" on page 13* provides you with an example of how to configure a branch office iSeries(TM) to connect to its corporate network through a gateway iSeries with an L2TP tunnel protected by VPN.

You can view a visual presentation about the concept of L2TP voluntary tunnels protected by IPSec. This requires the Flash plug-in

. Alternatively, you can use the HTML version of this presentation.

L2TP is actually a variation of an IP encapsulation protocol. The L2TP tunnel is created by encapsulating an L2TP frame inside a User Datagram Protocol (UDP) packet, which in turn is encapsulated inside an IP packet. The source and destination addresses of this IP packet define the endpoints of the connection. Because the outer encapsulating protocol is IP, you can apply IPSec protocols to the composite IP packet. This protects the data that flows within the L2TP tunnel. You can then apply Authentication Header (AH), Encapsulated Security Payload (ESP), and the Internet Key Exchange (IKE) protocol in a straightforward way.

See Scenario: Configure a remote PPP dial-up connection for an example of how L2TP is used when connecting to IBM (R), via Universal Connection.

Network address translation for VPN

Network address translation (NAT) takes your private IP addresses and translates them into public IP addresses. This helps conserve valuable public addresses while at the same time allows hosts in your network to access services and remote hosts across the Internet (or other public network).

In addition, if you use private IP addresses, they can collide with similar, incoming IP addresses. For example, you may want to communicate with another network but both networks use 10.*.*.* addresses, causing the addresses to collide and all packets to be dropped. Applying NAT to your outbound addresses might appear to be the answer to this problem. However, if the data traffic is protected by a VPN, conventional NAT will not work because it changes the IP addresses in the security associations (SAs) that VPN requires to function. To avoid this problem, VPN provides its own version of network address translation called VPN NAT. VPN NAT performs address translation before the SA validation by assigning an address to the connection when the connection starts. The address remains associated with the connection until you delete the connection.

Note: FTP does not support VPN NAT at this time.

How should I use VPN NAT?
There are two different types of VPN NAT that you need to consider before you begin. They are:

VPN NAT for preventing IP address conflicts
This type of VPN NAT allows you to avoid possible IP address conflicts when you configure a VPN

connection between networks or systems with similar addressing schemes. A typical scenario is one where both companies want to create VPN connections by using one of the designated private IP address ranges. For example, 10.*.*.*. How you configure this type of VPN NAT depends on whether your server is the initiator or the responder for the VPN connection. When your server is the connection initiator, you can translate your local addresses into ones that are compatible with your VPN connection partner's address. When your server is the connection responder, you can translate your VPN partner's remote addresses into ones that are compatible with your local addressing scheme. Configure this type of address translation only for your dynamic connections.

VPN NAT for hiding local addresses
This type of VPN NAT is used primarily to hide the real IP address of your local system by translating its address to another address that you make publicly available. When you configure VPN NAT, you can specify that each publicly known IP address be translated to one of a pool of hidden addresses. This also allows you to balance the traffic load for an individual address across multiple addresses. VPN NAT for local addresses requires that your server act as the responder for its connections.

Use VPN NAT for hiding local addresses if you answer yes to these questions:

1. Do you have one or more servers that you want people to access by using a VPN?
2. Do you need to be flexible about the actual IP addresses of your systems?
3. Do you have one or more globally routable IP addresses?

The scenario, *"VPN scenario: Use network address translation for VPN" on page 20* provides you with an example of how to configure VPN NAT to hide local addresses on your iSeries(TM).

For step-by-step instructions on how to set up VPN NAT on your iSeries, use the online help available from the VPN interface in iSeries Navigator.

NAT compatible IPSec

The problem: Conventional NAT breaks VPN

Network address translation (NAT) 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.

Unfortunately, conventional NAT does not work on IPSec packets because when the packet goes through a NAT device, the source address in the packet changes, thereby invalidating the packet. When this happens, the receiving end of the VPN connection discards the packet and the VPN connection negotiations fail.

The solution: UDP encapsulation
In a nutshell, UDP encapsulation wraps an IPSec packet inside a new, but duplicate, IP/UDP header. The address in the new IP header gets translated when it goes through the NAT device. Then, when the packet reaches its destination, the receiving end strips off the additional header, leaving the original IPSec packet, which will now pass all other validations.

You can only apply UDP encapsulation to VPNs that will use IPSec ESP in either tunnel mode or transport mode. In addition, at v5r2, the iSeries(TM) server can only act as a client for UDP encapsulation. That is, it can only *initiate* UDP encapsulated traffic.

The graphics below illustrate the format of a UDP encapsulated ESP packet in tunnel mode:

Original IPv4 datagram:

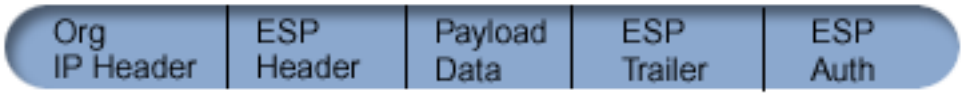
After applying IPSec ESP in tunnel mode:

After applying UDP Encapsulation:

The graphics below illustrate the format of a UDP encapsulated ESP packet in transport mode:

Original IPv4 datagram:

After applying IPSec ESP in transport mode:



After applying UDP Encapsulation:

Once the packet is encapsulated, the iSeries sends the packet to it's VPN partner over UDP port 4500. Typically, VPN partners perform IKE negotiations over UDP port 500. However, when IKE detects NAT during key negotiation, subsequent IKE packets are sent over source port 4500, destination port 4500. This also means that port 4500 must be unrestricted in any applicable filter rules. The receiving end of the connection can determine whether the packet is an IKE packet or a UDP encapsulated packet because the first 4 bytes of the UDP payload are set to zero on an IKE packet. For it to work properly, both ends of the connection must support UDP encapsulation.

IP Compression (IPComp)

The IP Payload Compression protocol (IPComp) reduces the size of IP datagrams by compressing the datagrams to increase the communication performance between two partners. The intent is to increase overall communication performance when the communication is over slow or congested links. IPComp does not provide any security and must be used along with either an AH or an ESP transform when the communication occurs over a VPN connection.

The Internet Engineering Task Force (IETF) formally defines IPComp in Request for Comments (RFC) 2393, *IP Payload compression Protocol (IPComp)*. You can view this RFC on the Internet at the following Web site: http://www.rfc-editor.org

.

VPN and IP filtering

Most VPN connections require filter rules to work properly. The filter rules required depend on the type of VPN connection that you are configuring as well as what type of traffic you want to control. In general, each connection will have a policy filter. The policy filter defines which addresses, protocols, and ports can use the VPN. In addition, connections that support the Internet Key Exchange (IKE) protocol typically have rules that are written explicitly to allow IKE processing over the connection.

Starting with V5R1 of the operating system, VPN can generate these rules automatically. Whenever possible, allow VPN to generate your policy filters for you. Not only will this help to eliminate errors, but it also eliminates the need for you to configure the rules as a separate step by using the Packet Rules editor in iSeries(TM) Navigator.

There are, of course, exceptions. Review these topics to learn more about other, less common, VPN and filtering concepts and techniques that may apply to your particular situation:

- **"Migrate policy filters to the current release"**
  In V4R4 and V4R5 of the operating system, you had to configure the VPN packet rules as a separate step. They were not generated automatically as part of your VPN configurations. This topic details special considerations for migrating V4R4 and V4R5 policy filters to the current release and tells you how to do it.
- **"VPN connections with no policy filters" on page 31**
  If the connection endpoints of your VPN are single, specific, IP addresses and you want to start the VPN without having to write or activate filter rules on the system, you can configure a dynamic policy filter. This topic explains why you might want to consider this and outlines how to do it.
- **"Implicit IKE" on page 32**
  In order for IKE negotiations to occur for your VPN, you need to allow UDP datagrams over port 500 for this type of IP traffic. However, if there are no filter rules on the system specifically written to permit IKE traffic, then the system will implicitly allow IKE traffic to flow. Read this topic for more information about how this works on iSeries.

Migrate policy filters to the current release

In V4R4 and V4R5 of the operating system, you had to configure the VPN packet rules as a separate step in the Packet Rules interface of iSeries(TM) Navigator. They were not generated automatically as part of your VPN configurations. Starting with V5R1 of the operating system, the VPN GUI can create these packet rules automatically.

There are several items you need to consider if you created policy filter rules (rules where action=IPSEC) in V4R4 or V4R5, and you want to use those same rules with the current release. Or, perhaps VPN *will* generate your policy filter rules, but you need to add additional rules that allow other IP traffic; for example, telnet, across the connection. Follow these recommendations to help you avoid potential configuration errors.

To clarify: When this topic refers to the *customer* rules file, it is referring to any rules file that you have created by using the Packet Rules editor in iSeries Navigator. Contrast this with the *VPNPOLICYFILTERS.I3P* rules file, which is the rules file that VPN automatically generates as part of VPN configurations.

- If you have VPN connections from either V4R4 or V4R5 and you do not plan to configure other VPN connections in the current release, you can activate your filter rules and start the connections, as usual.

- If you have VPN connections from either V4R4 or V4R5 and you plan to configure new VPN connections in the current release, use the **Migrate Policy Filters** wizard. The wizard removes the policy filters from the packet rules files that you created and inserts equivalent policy filters into VPNPOLICYFILTERS.I3P, that VPN generates. To access the wizard, follow these steps:
  1. In iSeries Navigator, expand your server **—>Network —>IP Policies**.
  2. Right-click **Virtual Private Networking** and select **Migrate Policy Filters**.
  3. When you complete the wizard, click **Finish**.
  4. Click **Help** if you have questions about how complete a page or any of its fields.
- If VPN generated your policy filter rules, but you need to add some non-VPN filter rules, you must configure these rules by using the Packet Rules Editor in iSeries Navigator. If any of these non-VPN filter rules need to come before the VPN filters, then begin their set names with `PREIPSEC`.For example, `PREIPSECMYRULES`. This helps the system determine the order in which it will process your filter rules. The set names of all other non-VPN rules must not have the `PREIPSEC` prefix. For example, `MORERULES`.
- Always allow VPN to create your policy filter rules. However, your non-VPN filter rules must remain in your customer rules file. Remember, if any of these non-VPN filters need to come before the policy filters in the VPNPOLICYFILTERS.I3P rules file, you will need to add `PREIPSEC` to the front of the set name. This ensures that your customer rules and the VPN rules work together as you intend. For example, VPN generated your policy filter rules (VPN sets), but you added additional rules (Your sets) to allow other IP traffic across the connection. When you load the rules on your system, they will be ordered as follows:
  1. Your sets whose names begin with PREIPSEC
  2. VPN sets whose name begins with PREIPSEC
  3. VPN sets with ACTION=IPSEC (policy filters)
  4. Your sets with ACTION=IPSEC (policy filters)
  5. Your sets with anything else.
  6. VPN sets with anything else.

  Check the EXPANDED.OUT file to view the order of the merged output file. EXPANDED.OUT is written to the directory where your customer rules file is located.
- Using iSeries Navigator, you can choose to activate:
  – only the VPN generated rules file, VPNPOLICYFILTERS.I3P
  – only your customer rules file
  – both the VPN generated rules and your customer rules file
- Activate your filter rules on all interfaces rather than by an individual interface. This helps to guarantee that the filters will activate and will also set the correct order of the policy filters.
- Always verify your filter rules before you attempt to activate them. If the verify runs without errors, check EXPANDED.OUT to ensure the rules are ordered as you intend. After you complete this step, then you can activate the rules.

VPN connections with no policy filters

A policy filter rule defines which addresses, protocols, and ports can use a VPN and directs the appropriate traffic through the connection. In some cases, you may want to configure a connection that does not require a policy filter rule. For example, you may have non-VPN packet rules loaded on the interface that your VPN connection will use, so rather than deactivating the active rules on that interface, you decide to configure the VPN so that your system manages all filters dynamically for the connection. The policy filter for this type of connection is referred to as a **dynamic policy filter**. Before you can use a dynamic policy filter for your VPN connection, all of the following must be true:

- The connection can only be initiated by the local server.
- The data endpoints of the connection must be single systems. That is, they cannot be a subnet or a range of addresses.
- No policy filter rule can be loaded for the connection.

If your connection meets this criteria, then you can configure the connection so that it does not require a policy filter. When the connection starts, traffic between the data endpoints will flow across the it regardless of what other packet rules are loaded on your system.

For step-by-step instructions on how to configure a connection so that is does not require a policy filter, use the online help for VPN.

Implicit IKE

To establish a connection, most VPNs require Internet Key Exchange (IKE) negotiations to occur before IPSec processing can happen. IKE uses the well-known port 500, so for IKE to work properly, you need to allow UDP datagrams over port 500 for this type of IP traffic. If there are no filter rules on the system specifically written to permit IKE traffic, then IKE traffic is implicitly allowed. However, rules written specifically for UDP port 500 traffic are handled based on what is defined in the active filter rules.

Plan for VPN

Planning is an essential part of your total VPN solution. There are many complex decisions you need to make to ensure that your connection works properly. Use these resources to gather all the information that you need to ensure that your VPN is a success:

- "VPN setup requirements"
  Before you begin, ensure that you meet the minimum requirements for creating a VPN.
- "Determine what type of VPN to create" on page 33
  Determining how you will use your VPN is one of the first steps in successful planning. This topic describes the various connection types you can configure.
- **Use the VPN planning advisor**
  The planning advisor asks you questions about your network and based on your answers, it provides you with suggestions for creating your VPN.
  Note: Use the VPN planning advisor only for connections that support the Internet Key Exchange (IKE) protocol. Use the planning worksheet for manual connections for your manual connection types.
- "Complete the VPN planning worksheets" on page 33
  If you prefer, you can print and complete the planning worksheets to gather detailed information about your VPN usage plans.

After you come up with a plan for your VPN, you can begin "Configure VPN" on page 36 it.

VPN setup requirements

To function properly on iSeries(TM) and with network clients, ensure your iSeries and client PC meet the following requirements:

V5R2 iSeries requirements

- OS/400(R) Version 5 Release 2 (5722-SS1) or later
- Digital Certificate Manager (5722-SS1 Option 34)
- Cryptographic Access Provider (5722-AC2 or AC3)
- iSeries Access for Windows(R)(5722-XE1) and iSeries Navigator
  - Network component of iSeries Navigator
- Set the retain server security data (QRETSVRSEC *SEC) system value to 1
- TCP/IP must be configured, including IP interfaces, routes, local host name, and local domain name

Client requirements

- A workstation with a Windows(R) 32-bit operating system properly connected to your iSeries, and configured for TCP/IP
- A 233 Mhz processing unit
- 32 MB RAM for Windows 95/98 clients
- 64 MB RAM for Windows NT(R) and 2000 clients
- iSeries Access for Windows and iSeries Navigator installed on the client PC
- Software that supports the IP Security (IPSec) protocol
- Software that supports L2TP, if remote users will use L2TP to establish a connection with your system

Determine what type of VPN to create

Determining how you will use your VPN is one of the first steps in successful planning. To do this, you need to understand the role that both the local key server and the remote key server play in the connection. For example, are the *connection* endpoints different from the *data* endpoints. Are they the same or some combination of both? Connection endpoints authenticate and encrypt (or decrypt) data traffic for the connection, and optionally provide key management with the Internet Key Exchange (IKE) protocol. Data endpoints, however, define the connection between two systems for IP traffic that flows across the VPN; for example, all TCP/IP traffic between 123.4.5.6 and 123.7.8.9. Typically, when the connection and data endpoints are different, the VPN server is a gateway. When they are the same, the VPN server is a host.

Various types of VPN implementations that are well suited to most business needs follow:

Gateway-to-gateway
The connection endpoints of both systems are different from the data endpoints. The IP Security (IPSec) protocol protects traffic as it travels between the gateways. However, IPSec does not protect data traffic on either side of the gateways within the internal networks. This is a common setup for connections between branch offices because traffic that is routed beyond the branch office gateways, into the internal networks, is often considered trusted.

Gateway-to-host
IPSec protects data traffic as it travels between your gateway and a host in a remote network. VPN does not protect data traffic in the local network because you consider it trusted.

Host-to-gateway
VPN protects data traffic as it travels between a host in the local network and a remote gateway. VPN does not protect data traffic in the remote network.

Host-to-host
The connection endpoints are the same as the data endpoints on both the local and the remote systems. VPN protects data traffic as it travels between a host in the local network and a host in the remote network. This type of VPN provides end-to-end IPSec protection.

Complete the VPN planning worksheets

Use the VPN planning worksheets to gather detailed information about your VPN usage plans. You need this information to adequately plan your VPN strategy. You can also use this information to configure your VPN. Choose the worksheet for the type of connection you want to create.

- "Planning worksheet for dynamic connections" on page 34
  Complete this worksheet before you configure a dynamic connection.
- "Planning worksheet for manual connections" on page 35
  Complete this worksheet before you configure a manual connection.
- **VPN planning advisor**
  Or, if you prefer, use the advisor for interactive planning and configuration guidance. The planning advisor asks you questions about your network and based on your answers, it provides you with suggestions for creating your VPN.

Note: Use the VPN planning advisor only for your dynamic connections. Use the planning worksheet for manual connections for your manual connection types.

If you will create multiple connections with similar properties, you may want to set the VPN defaults. The default values you configure seed the VPN property sheets. This means that you are not required to configure the same properties multiple times. To set the VPN defaults, select **Edit** from the VPN main menu, and then select **Defaults**.

Planning worksheet for dynamic connections

Before you create your dynamic VPN connections, complete this worksheet. The worksheet assumes you will use the New Connection Wizard. The wizard allows you to set up a VPN based on your basic security requirements. In some cases, you may need to refine the properties that the wizard configures for a connection. For example, you may decide that you require journaling or that you want the VPN server to start each time TCP/IP starts. If this is the case, right-click the dynamic-key group or connection that the wizard created and select **Properties**.

Answer each question before you proceed with your VPN setup.

Prerequisite checklist	**Answers**
Is your OS/400(R) V5R2 (5722-SS1) or later?	
Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?	
Is Cryptographic Access Provider (5722-AC2 or AC3) installed?	
Is iSeries(TM) Access(5722-XE1) installed?	
Is iSeries Navigator installed?	
Is the Network subcomponent of iSeries Navigator installed?	
Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?	
Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?	
Is TCP/IP configured on your iSeries (including IP interfaces, routes, local host name, and local domain name)?	
Is normal TCP/IP communication established between the required endpoints?	
Have you applied the latest program temporary fixes (PTFs)?	
If the VPN tunnel traverses firewalls or routers that use IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?	
Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?	
Are the firewalls configured to enable IP forwarding?	

You need this information to configure a dynamic VPN connection	**Answers**
What type of connection are you creating? • Gateway-to-gateway • Host-to-gateway • Gateway-to-host • Host-to-host	
What will you name the dynamic-key group?	
What type of security and system performance do you require to protect your keys? • Highest security, lowest performance • Balance security and performance • Lowest security and highest performance	

You need this information to configure a dynamic VPN connection	Answers
Are you using certificates to authenticate the connection? If no, what is the preshared key?	
What is the identifier of the local key server?	
What is the identifier of the local data endpoint?	
What is the identifier of the remote key server?	
What is the identifier of the remote data endpoint?	
What type of security and system performance do you require to protect your data? • Highest security, lowest performance • Balance security and performance • Lowest security and highest performance	

Planning worksheet for manual connections

Complete this worksheet to assist you in creating your virtual private network (VPN) connections that do not use IKE for key management.

Answer each of these questions before you proceed with your VPN setup:

Prerequisite checklist	Answers
Is your OS/400(R) V5R2(5722-SS1) or later?	
Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?	
Is Cryptographic Access Provider (5722-AC2 or AC3) installed?	
Is iSeries(TM) Access(5722-XE1) installed?	
Is iSeries Navigator installed?	
Is the Network subcomponent of iSeries Navigator installed?	
Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?	
Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?	
Is TCP/IP configured on your iSeries (including IP interfaces, routes, local host name, and local domain name)?	
Is normal TCP/IP communication established between the required endpoints?	
Have you applied the latest program temporary fixes (PTFs)?	
If the VPN tunnel traverses firewalls or routers that use IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?	
Are the firewalls or routers configured to permit the AH and ESP protocols?	
Are the firewalls configured to enable IP forwarding?	

You need this information to configure a manual VPN	Answers
What type of connection are you creating? • Host-to-host • Host-to-gateway • Gateway-to-host • Gateway-to-gateway	
What will you name the connection?	
What is the identifier of the local connection endpoint?	
What is the identifier of the remote connection endpoint?	

You need this information to configure a manual VPN	Answers
What is the identifier of the local data endpoint?	
What is the identifier of the remote data endpoint?	
What type of traffic will you allow for this connection (local port, remote port, and protocol)?	
Do you require address translation for this connection? See “Network address translation for VPN” on page 27 for more information.	
Will you use tunnel mode or transport mode?	
Which IPSec protocol will the connection use (AH, ESP, or AH with ESP)? See “IP Security (IPSec) protocols” on page 22 for more information.	
Which authentication algorithm will the connection use (HMAC-MD5 or HMAC-SHA)?	
Which encryption algorithm will the connection use (DES-CBC or 3DES-CBC)? **Note:** You specify an ecryption algorithm only if you selected ESP as your IPSec protocol.	
What is the AH inbound key? If you use MD5, the key is a 16-byte hexadecimal string. If you use SHA, the key is a 20-byte hexadecimal string. Your inbound key must match the outbound key of the remote server exactly.	
What is the AH outbound key? If you will use MD5, the key is a 16-byte hexadecimal string. If you will use SHA, the key is a 20-byte hexadecimal string. Your outbound key must match the inbound key of the remote server exactly.	
What is the ESP inbound key? If you use DES, the key is an 8-byte hexadecimal string. If you will use 3DES, the key is a 24-byte hexadecimal string. Your inbound key must match the outbound key of the remote server exactly.	
What is the ESP outbound key? If you use DES, the key is an 8-byte hexadecimal string. If you will use 3DES, the key is a 24-byte hexadecimal string. Your outbound key must match the inbound key of the remote server exactly.	
What is the inbound Security Policy Index (SPI)? The inbound SPI is a 4-byte hexadecimal string, where the first byte is set to 00. Your inbound SPI must match the outbound SPI of the remote server exactly.	
What is the outbound SPI? The outbound SPI is a 4-byte hexadecimal string. Your outbound SPI must match the inbound SPI of the remote server exactly.	

Configure VPN

The VPN interface provides you with several different ways to configure your VPN connections. Keep reading to help you decide which type of connection to configure and how to do it.

What type of connection should I configure?
A **dynamic** connection is one that dynamically generates and negotiates the keys that secure your connection, while it is active, by using the Internet Key Exchange (IKE) protocol. Dynamic connections provide an extra level of security for the data that flows across it because the keys change, automatically, at regular intervals. Consequently, an attacker is less likely to capture a key, have time to break it, and use it to divert or capture the traffic the key protects.

A **manual (page 38)** connection, however, does not provide support for IKE negotiations, and consequently, automatic key management. Further, both ends of the connection require you to configure several attributes that must match exactly. Manual connections use static keys that do not refresh or change while the connection is active. You must stop a manual connection to change its associated key. If you consider this a security risk, you may want to create a dynamic connection instead.

How do I configure a dynamic VPN connection?
VPN is actually a group of configuration objects that define the characteristics of a connection. A dynamic VPN connection requires each of these objects to work properly. Follow the links below for specific information about how to configure each of the VPN configuration objects:

> **Tip:**
> "Configure VPN connections with the New Connection wizard" on page 38
> In general, you can use the Connection wizard to create all of your dynamic connections. The wizard automatically creates each of the configuration objects VPN requires to work properly, including the packet rules. If you specify that you want the wizard to activate the VPN packet rules for you, you can skip to step six below, *Start the connection*. Otherwise, after the wizard finishes configuring your VPN, you must activate the packet rules and then you can start the connection.

If you choose not to use the wizard to configure your dynamic VPN connections, follow these steps to complete the configuration:

1. "Configure VPN security policies" on page 38
   You must define VPN security policies for all of your dynamic connections. The Internet Key Exchange policy and data policy dictate how IKE protects its phase 1 and phase 2 negotiations.
2. "Configure the VPN secure connection" on page 40
   Once you have defined the security policies for a connection, you must then configure the secure connection. For dynamic connections, the secure connection object includes a dynamic-key group and a dynamic-key connection. The **dynamic-key group** defines the common characteristics of one or more VPN connections, while the **dynamic-key connection** defines the characteristics of individual data connections between pairs of endpoints. The dynamic-key connection exists within the dynamic-key group.

   Note: You only need to complete the next two steps, *Configure packet rules* and *Define an interface for the rules*, if you select **The policy filter rule will be defined in Packet Rules** option on the **Dynamic-Key Group - Connections** page in the VPN interface. Otherwise, these rules are created as part of your VPN configurations and are applied to the interface you specify.

   It is recommended that you always allow the VPN interface to create your policy filter rules for you. Do this by selecting the **Generate the following policy filter for this group** option on the **Dynamic-Key Group - Connections** page.
3. "Configure VPN packet rules" on page 41
   After you complete your VPN configurations, you must create and apply filter rules that allow data traffic to flow through the connection. The VPN **pre-IPSec** rules permit all IKE traffic on the specified interfaces so that IKE can negotiate connections. The **policy filter** rule defines which addresses, protocols, and ports can use the associated new dynamic-key group.

   If you are migrating from either V4R4 or V4R5 and have VPN connections and policy filters you want to continue using with the current release, review the topic, "Migrate policy filters to the current release" on page 30 to ensure that your old policy filters and new policy filters will work together as you intend.
4. "Define an interface for the VPN filter rules" on page 44
   After you configure the packet rules and any other rules that you need to enable your VPN connection, you must define an interface to which to apply them.
5. "Activate the VPN packet rules" on page 44
   After you define an interface for your packet rules, you must activate them before you can start the connection.

6. “Start a VPN connection” on page 45
   Complete this task to start your connections.

How do I configure a manual VPN connection?
Just as the name suggests, a manual connection is one where you must configure all of your VPN properties by hand, including inbound and outbound keys. Follow the links below for specific information about how to configure a manual connection:

1. “Configure a manual connection” on page 41
   Manual connections define the characteristics of a connection including what security protocols and the connection and data endpoints.

   Note: You only need to complete the next two steps, *Configure policy filter rule* and *Define an interface for the rules*, if you select **The policy filter rule will be defined in Packet Rules** option on the **Manual Connection - Connection** page in the VPN interface. Otherwise, these rules are created as part of your VPN configurations.

   It is recommended that you always allow the VPN interface to create your policy filter rules for you. Do this by selecting the **Generate a policy filter that matches the data endpoints** option on the **Manual Connection - Connection** page.
2. “Configure a policy filter rule” on page 43
   After you configure the attributes of the manual connection, you must create and apply a policy filter rule that allows data traffic to flow through the connection. The **policy filter** rule defines which addresses, protocols, and ports can use the associated connection.
3. “Define an interface for the VPN filter rules” on page 44
   After you configure the packet rules and any other rules that you need to enable your VPN connection, you must define an interface to which to apply them.
4. “Activate the VPN packet rules” on page 44
   After you define an interface for your packet rules, you must activate them before you can start the connection.
5. “Start a VPN connection” on page 45
   Complete this task to start connections that are initiated locally.

Configure VPN connections with the New Connection wizard

The New Connection wizard allows you to create a virtual private network (VPN) between any combination of hosts and gateways. For example, host-to-host, gateway-to-host, host-to-gateway, or gateway-to-gateway.

The wizard automatically creates each of the configuration objects VPN requires to work properly, including the packet rules. However, if you need to add function to your VPN; for example, journaling or network address translation for VPN (VPN NAT), you may want further refine your VPN through the property sheets of the appropriate dynamic-key group or connection. To do this, you must first stop the connection if it is active. Then, right-click the dynamic-key group or connection, and select **Properties**.

Complete the VPN planning advisor before you begin. The advisor provides you with a means for gathering important information that you will need to create your VPN.

To create a VPN with the Connection wizard, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Virtual Private Networking** and select **New Connection**to start the wizard.
3. Complete the wizard to create a basic VPN connection. Click **Help** if you need assistance.

Configure VPN security policies

After you determine how you will use your VPN you must define your VPN security policies. Specifically, you will need to:

- "Configure an Internet Key Exchange (IKE) policy"
  The IKE policy defines what level of authentication and encryption protection IKE uses during phase 1 negotiations. IKE phase 1 establishes the keys that protect the messages that flow in the subsequent phase 2 negotiations. You do not need to define an IKE policy when you create a manual connection. In addition, if you create your VPN with the New Connection wizard, the wizard can create your IKE policy for you.
- "Configure a data policy"
  A data policy defines what level of authentication or encryption protects data as it flows through the VPN. The communicating systems agree on these attributes during the Internet Key Exchange (IKE) protocol phase 2 negotiations. You do not need to define a data policy when you create a manual connection. In addition, if you create your VPN with the New Connection wizard, the wizard can create a data policy for you.

After you configure your VPN security policies, you must then configure the "Configure the VPN secure connection" on page 40.

Configure an Internet Key Exchange (IKE) policy

An IKE policy defines what level of authentication or encryption protection "Key management" on page 25 uses during phase 1 negotiations. IKE phase 1 establishes the keys that protect the messages that flow in the subsequent phase 2 negotiations. VPN uses either RSA signature mode or preshared keys to authenticate phase 1 negotiations. If you plan to use digital certificates for authenticating the key servers, you must first configure them by using the Digital Certificate Manager (5722-SS1 Option 34). The IKE policy also identifies which remote key server will use this policy.

To define an IKE policy or make changes to an existing one, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> IP Security Policies**.
2. To create a new policy, right-click **Internet Key Exchange Policies** and select **New Internet Key Exchange Policy**. To make changes to an existing policy, click **Internet Key Exchange Policies** in the left pane then right-click the policy you want to change in the right pane, and select **Properties**.
3. Complete each of the property sheets. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** to save your changes.

Note: It is recommended that you use main mode negotiation whenever a preshared key is used for authentication. They provide a more secure exchange. If you must use preshared keys and aggressive mode negotiation, select obscure passwords that are unlikely to be cracked in attacks that scan the dictionary. It is also recommended you periodically change your passwords. Use the iSeries Navigator online help for more detailed information.

Configure a data policy

A data policy defines what level of authentication or encryption protects data as it flows through the VPN. The communicating systems agree on these attributes during the "Key management" on page 25 phase 2 negotiations.

To define a data policy or make changes to an existing one, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> IP Security Policies**.
2. To create a new data policy, right-click **Data Policies** and select **New Data Policy**. To make changes to an existing data policy, click **Data Policies** (in the left pane) then right-click the data policy you want to change (in the right pane) and select **Properties**.

3. Complete each of the property sheets. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** to save your changes.

Configure the VPN secure connection

After you have configured the security policies for your connection, you must then configure the secure connection. For dynamic connections, the secure connection object includes a dynamic-key group and a dynamic-key connection.

The **dynamic-key group** defines the common characteristics of one or more VPN connections. Configuring a dynamic-key group allows you to use the same policies, but different data endpoints for each connection within the group. Dynamic-key groups also allow you to successfully negotiate with remote initiators when the data endpoints proposed by the remote system are not specifically known ahead of time. It does this by associating the policy information in the dynamic-key group with a policy filter rule with an IPSEC action type. If the specific data endpoints offered by the remote initiator fall within the range specified in the IPSEC filter rule, they can be subjected to the policy defined in the dynamic-key group.

The **dynamic-key connection** defines the characteristics of individual data connections between pairs of endpoints. The dynamic-key connection exists within the dynamic-key group. After you configure a dynamic-key group to describe what policies connections in the group use, you need to create individual dynamic-key connections for connections that you initiate locally.

To configure the secure connection object, complete these tasks:

Part 1: Configure a dynamic-key group:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**.
2. Right-click **By Group** and select **New Dynamic-Key Group**.
3. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** to save your changes.

Part 2: Configure a dynamic-key connection:

1. In iSeries Navigator, expand your server **—> Network —> IP Policies—> Virtual Private Networking—> Secure Connections—> By Group**.
2. In the left-pane of the iSeries Navigator window, right-click the dynamic-key group you created in part one and select **New Dynamic-Key Connection**.
3. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** to save your changes.

After you complete these steps, you need to “Activate the VPN packet rules” on page 44 the packet rules that the connection requires to work properly.

Note: In most cases, allow the VPN interface to generate your VPN packet rules automatically by selecting the **Generate the following policy filter for this group** option on the **Dynamic-Key Group - Connections** page. However, if you select the **The policy filter rule will be defined in Packet Rules** option, you must then “Configure VPN packet rules” on page 41 by using the Packet Rules editor and then activate them.

Configure a manual connection

Just as the name suggests, a manual connection is one where you must configure all of your VPN properties by hand. Further, both ends of the connection require you to configure several elements that must match *exactly*. For example, your inbound keys must match the remote system's outbound keys or the connection will fail.

Manual connections use static keys that are not refreshed or changed while the connection is active. You must stop a manual connection in order to change its associated key. If you consider this a security risk, and both ends of the connection support the Internet Key Exchange (IKE) protocol, you may want to consider setting up a dynamic connection instead.

To define the properties for your manual connection, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**.
2. Right-click **All Connections** and select **New Manual Connection**.
3. Complete each of the property sheets. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** to save your changes.

Note: In most cases, allow the VPN interface to generate your VPN packet rules automatically by selecting the **Generate a policy filter that matches the data endpoints** option on the **Manual Connection - Connection** page. However, if you select the **The policy filter rule will be defined in Packet Rules** option, you must then "Configure a policy filter rule" on page 43 by hand and then activate them.

Configure VPN packet rules

If you are creating a connection for the first time, allow VPN to automatically generate the VPN packet rules for you. You can do this by either using the New Connection wizard or the VPN properties pages to configure your connection.

If you decide to create your VPN packet rules by using the Packet Rules editor in iSeries(TM) Navigator, create any additional rules this way as well. Conversely, if you have VPN generate your policy filter rules, create all additional policy filter rules this way.

In general, VPNs require two types of filter rules: Pre-IPSec filter rules and policy filter rules. Review the topics below to learn how to configure these rules by using the Packet Rules editor in iSeries Navigator. If you want to read about other VPN and filtering options, see the "VPN and IP filtering" on page 30 section of the VPN concepts topic.

- "Configuring the pre-IPSec filter rule" on page 42
  The pre-IPSec rules are any rules on your system that come before rules with an IPSEC action type. This topic only discusses the pre-IPSec rules that VPN requires to work properly. In this case, the pre-IPSec rules are a pair of rules that allow IKE processing over the connection. IKE allows dynamic key generation and negotiations to occur for your connection. You may need to add other pre-IPSec rules depending on your particular network environment and security policy.

  Note: You only need to configure this type of pre-IPSec rule if you already have other rules that permit IKE for specific systems. If there are no filter rules on the system specifically written to permit IKE traffic, then IKE traffic is implicitly allowed.
- "Configure a policy filter rule" on page 43
  The policy filter rule defines the traffic that can use the VPN and what data protection policy to apply to that traffic.

Things to consider before you begin

When you add filter rules to an interface, the system automatically adds a default DENY rule for that interface. This means that any traffic not explicitly permitted is denied. You cannot see or change this

rule. As a result, you may find that traffic that previously worked mysteriously fails after you activate your VPN filter rules. If you want to allow traffic other than VPN on the interface, you must add explicit PERMIT rules to do so.

After you configure the appropriate filter rules, you must "Define an interface for the VPN filter rules" on page 44 to which they apply, and then "Activate the VPN packet rules" on page 44 them.

It is essential that you configure your filter rules properly. If you do not, the filter rules can block all IP traffic coming into and going out of your iSeries. This includes your connection to iSeries Navigator, which you use to configure the filter rules.

If the filter rules do not permit iSeries Navigator traffic, iSeries Navigator cannot communicate with your iSeries. If you find yourself in this situation, you must log on to your iSeries using an interface that still has connectivity, such as the operations console. Use the RMVTCPTBL command to remove all filters on this system. This command also ends the *VPN servers and then restarts them. Then, configure your filters and reactivate them.

Configuring the pre-IPSec filter rule

Attention: Complete this task only if you have specified that you do not want VPN to generate your policy filter rules automatically.

A pair of Internet Key Exchange (IKE) servers dynamically negotiate and refresh keys. IKE uses the well-known port, 500. For IKE to work properly, you need to allow UDP datagrams over port 500 for this IP traffic. To do this, you will create a pair of filter rules; one for inbound traffic and one for outbound traffic, so that your connection can dynamically negotiate keys to protect the connection:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Packet Rules** and select **Rules Editor**. This opens the Packet Rules editor, which allows you to create or edit filter and NAT rules for your iSeries.
3. On the Welcome window, select **Create a new packet rules file** and click **OK**.
4. From the Packet Rules editor select **Insert —> Filter**.
5. On the **General** page, specify a set name for your VPN filter rules. It is recommended that you create at least three different sets: one for your pre-IPSec filter rules, one for your policy filter rules, and one for miscellaneous PERMIT and DENY filter rules. Name the set that contains your pre-IPSec filter rules with a prefix of *preipsec*. For example, preipsecfilters.
6. In the **Action** field, select **PERMIT** from the drop-down list.
7. In the **Direction** field, select **OUTBOUND** from the drop-down list.
8. In the **Source address name** field, select **=** from the first drop-down list and then enter the IP address of the local key server in the second field. You specified the IP address of the local key server in the IKE policy.
9. In the **Destination address name** field, select **=** from the first drop-down list and then enter the IP address of the remote key server in the second field. You also specified the IP address of the remote key server in the IKE policy.
10. On the **Services** page, select **Service** . This enables the **Protocol**, **Source port**, and **Destination port** fields.
11. In the **Protocol** field, select **UDP** from the drop-down list.
12. For **Source port**, select **=** in the first field, then enter `500` in the second field.
13. Repeat the previous step for **Destination port**.
14. Click **OK**.
15. Repeat these steps to configure the INBOUND filter. Use the same set name and reverse addresses as necessary.

Note: A less secure, but easier option for permitting IKE traffic through the connection, is to configure only one pre-IPSec filter, and use wildcard values (*) in the **Direction**, **Source address name**, and **Destination address name** fields.

The next step is to "Configure a policy filter rule" to define what IP traffic the VPN connection protects.

Configure a policy filter rule

Attention: Complete this task only if you have specified that you do not want VPN to generate your policy filter rule automatically.

The policy filter rule (a rule where action=IPSEC)defines which addresses, protocols, and ports can use the VPN. It also identifies the policy that will be applied to traffic in the VPN connection. To configure a policy filter rule, follow these steps:

Note: If you just configured the pre-IPSec rule (for dynamic connections, only) the Packet Rules editor will still be open; go to step four.

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Packet Rules** and select **Rules Editor**. This opens the Packet Rules editor, which allows you to create or edit filter and NAT rules for your iSeries.
3. On the Welcome window, select **Create a new packet rules file** and click **OK**.
4. From the Packet Rules editor select **Insert —> Filter**.
5. On the **General** page, specify a set name for your VPN filter rules. It is recommended that you create at least three different sets: one for your pre-IPSec filter rules, one for your policy filter rules, and one for miscellaneous PERMIT and DENY filter rules. For example, `policyfilters`
6. In the **Action** field, select **IPSEC** from the drop-down list. The **Direction** field defaults to OUTBOUND and you cannot change it. Although this field defaults to OUTBOUND, it is actually bi-directional. OUTBOUND displays to clarify the semantics of the input values. For example, source values are local values, and destination values are remote values.
7. For **Source address name**, select **=** in the first field, and then enter the IP address of the local data endpoint in the second field. You can also specify a range of IP addresses or an IP address plus a subnet mask after you define them by using the **Define Addresses** function.
8. For **Destination address name**, select **=** in the first field, and then enter the IP address of the remote data endpoint in the second field. You can also specify a range of IP addresses or an IP address plus a subnet mask after you define them by using the **Define Addresses** function.
9. In the **Journaling** field, specify what level of journaling you require.
10. In the **Connection name** field, select the connection definition to which these filter rules apply.
11. (optional) Enter a description.
12. On the **Services** page, select **Service**. This enables the **Protocol**, **Source port**, and **Destination port** fields.
13. In the **Protocol** field, **Source port**, and **Destination port** fields, select the appropriate value for the traffic. Or, you can select the asterisk (*) from the drop-down list. This allows any protocol using any port to use the VPN.
14. Click **OK**.

The next step is to "Define an interface for the VPN filter rules" on page 44 to which these filter rules apply.

Note: When you add filter rules for an interface, the system automatically adds a default DENY rule for that interface. This means that any traffic not explicitly permitted is denied. You cannot see or change this rule. As a result, you may find that connections that previously worked mysteriously fail after you activate your VPN packet rules. If you want to allow traffic other than VPN on the interface, you must add explicit PERMIT rules to do so.

Define an interface for the VPN filter rules

After you configure your VPN packet rules and any other rules that you need to enable your VPN connection, you must define the interface to which to they apply.

To define an interface to which to apply your VPN filter rules, follow these steps:

Note: If you just configured the VPN packet rules, the Packet Rules interface will still be open; go to step four.

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Packet Rules** and select **Rules Editor**. This opens the Packet Rules editor, which allows you to create or edit filter and NAT rules for your iSeries.
3. On the Welcome window, select **Create a new packet rules file** and click **OK**.
4. From the Packet Rules editor select **Insert —> Filter Interface**.
5. On the **General** page, select **Line name**, and then select the line description to which your VPN packet rules apply from the drop-down list.
6. (optional) Enter a description.
7. On the **Filter Sets** page, click **Add** to add each set name for the filters you just configured.
8. Click **OK**.
9. Save your rules file. The file is saved into the integrated file system on your iSeries with an extension of .i3p.
   Note: Do not save your file into the following directory:
   `/QIBM/UserData/OS400/TCPIP/RULEGEN`
   This directory is for system use only. If you ever need to use the RMVTCPTBL *ALL command to deactivate packet rules, the command will delete all files within this directory.

After you define an interface for your filter rules, you must "Activate the VPN packet rules" them before you can start the VPN.

Activate the VPN packet rules

You must activate the VPN packet rules before you can start your VPN connections. You cannot activate (or deactivate) packet rules when you have VPN connections running on your system. So, before you activate your VPN filter rules, ensure that there are no active connections associated with them.

If you created your VPN connections with the New Connection wizard, you can choose to have the associated rules activated, automatically, for you. Be aware that, if there are other packet rules active on any of the interfaces you specify, the VPN policy filter rules will replace them.

If you choose to activate your VPN generated rules by using the Packet Rules Editor, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Packet Rules** and select **Activate**. This opens the **Activate Packet Rules** dialog box.
3. Select whether you want to activate only the VPN generated rules, only a selected file, or both the VPN generated rules and a selected file. You might choose the latter, for instance, if you have miscellaneous PERMIT and DENY rules that you want to enforce on the interface in addition to the VPN generated rules.
4. Select the interface on which you want the rules activated. You can choose to activate on a specific interface, on a point-to-point identifier, or on all interfaces and all point-to-point identifiers.
5. Click **OK** on the dialog box to confirm that you want to verify and activate the rules on the interface or interfaces you specified. After you click OK, the system checks the rules for syntax and semantic errors and reports the results in a message window at the bottom of the 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.

After you activate your filter rules, you can “Start a VPN connection.”

Start a VPN connection

These instructions assume you have properly configured your VPN connection. Follow these steps to start your VPN connection:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. If the VPN server is not started, right-click **Virtual Private Networking** and select **Start**. This starts the VPN server.
3. Ensure your packet rules are “Activate the VPN packet rules” on page 44.
4. Expand **Virtual Private Networking—> Secure Connections**.
5. Click **All Connections** to display a list of connections in the right pane.
6. Right-click the connection you want to start and select **Start**. To start multiple connections, select each connection you want to start, right-click and select **Start**.

Manage VPN

Use the VPN interface in iSeries(TM) Navigator to handle all of your management tasks, including:

- “Start a VPN connection”
  Complete this task to start connections you will initiate locally.
- “Set default attributes for your connections”
  The default values seed the panels that you use to create new policies and connections. You can set defaults for security levels, key session management, key lifetimes, and connection lifetimes.
- “Reset connections in error state” on page 46
  Resetting connections in error returns them to the idle state.
- “View error information” on page 46
  Complete this task to help you determine why your connection is in error.
- “View the attributes of active connections” on page 46
  Complete this task to check the status and other attributes of your active connections.
- “Use the VPN server trace” on page 46
  The VPN server trace allows you to configure, start, stop, and view the VPN Connection Manager and VPN Key Manager server traces. This is similar to using the TRCTCPAPP *VPN command from the character-based interface except that you can view the trace while a connection is active.
- “View the VPN server job logs” on page 47
  Follow these instructions to view the job logs for the VPN Key Manager and the VPN Connection Manager.
- “Stop a VPN connection” on page 47
  Complete this task to stop active connections.
- “View the attributes of Security Associations (SA)” on page 47
  Complete this task to display the attributes of the Security Associations (SAs) that are associated with an enabled connection.
- “Delete VPN configuration objects” on page 47
  Before you delete a VPN configuration object from the VPN policy database, make sure you understand how it affects other VPN connections and connection groups.

Set default attributes for your connections

The default security values seed various fields when you initially create new VPN objects.

To set default security values for your VPN connections, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—>Network —>IP Policies**.
2. Right-click **Virtual Private Networking** and select **Defaults**.

3. Click **Help** if you have questions about how complete a page or any of its fields.
4. Click **OK** after you have completed each of the property sheets.

Reset connections in error state

To refresh a connection that is in the error state, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the connection you want to reset and select **Reset**. This resets the connection to the idle state. To reset multiple connections that are in the error state, select each connection you want to reset, right-click and select **Reset**.

View error information

To view information about connections in error, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the connection in error that you want to view and select **Error Information**.

View the attributes of active connections

To view the current attributes of an active or on-demand connection, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the active or on-demand connection that you want to view and select **Properties.**
4. Go to the **Current Attributes** page to view the attributes of the connection.

You can also view the attributes of all connections from the iSeries Navigator window. By default, the only attributes that display are Status, Description, and Connection Type. You can change what data displays by following these steps:

1. In iSeries Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. From the **Objects** menu, select **Columns**. This opens a dialog box which allows you to select which attributes you want to display in the iSeries Navigator window.

Be aware that when you change the columns to view, the changes are not specific to a particular user or PC, but rather, are system-wide.

Use the VPN server trace

To view the VPN server trace, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Virtual Private Networking**, select **Diagnostic Tools**, and then **Server Trace**.

To specify what type of trace you want the VPN Key Manager and the VPN Connection Manager to generate, follow these steps:

1. From the **Virtual Private Networking Trace** window, click

(Options).

2. On the **Connection Manager** page, specify what type of trace you want the Connection Manager server to run.
3. On the **Key Manager page**, specify what type of trace you want the Key Manager server to run.
4. Click **Help** if you have questions about how complete a page or any of its fields.
5. Click **OK** to save your changes.
6. Click

(Start) to start the trace. Click

(Refresh) periodically to view the latest trace information.

View the VPN server job logs

To view the current job logs of either the VPN Key Manager or the VPN Connection Manager, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies.**
2. Right-click **Virtual Private Networking** and select **Diagnostic Tools** and then select whichever server job log you want to view.

View the attributes of Security Associations (SA)

To view the attributes of the security associations (SAs) that are associated with an enabled connection. To do so, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the appropriate active connection and select **Security Associations.**The resulting window allows you to view the properties of each of the SAs associated with a specific connection.

Stop a VPN connection

To stop an active or on-demand connection, follow these steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the connection you want to stop and select **Stop**. To stop multiple connections, select each connection you want to stop, right-click and select **Stop**.

Delete VPN configuration objects

If you are certain you need to delete a VPN connection from the VPN policy database, perform the following steps:

1. In iSeries(TM) Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections**
2. Click **All Connections** to display a list of connections in the right pane.
3. Right-click the connection you want to delete and select **Delete**.

Troubleshoot VPN

VPN is a complex and rapidly changing technology that requires at least a basic knowledge of standard IPSec technologies. You must also be familiar with IP packet rules because VPN requires several filter rules in order to work properly. Because of this complexity, you may, from time to time, experience trouble with your VPN connections. Troubleshooting your VPN is not always an easy task. You must understand your system and your network environments, as well as the components you use to manage them. The following topics provide you with hints on how to troubleshoot the various problems you may encounter while using VPN:

- "Get started with troubleshooting VPN"
  Go here to begin finding and correcting your VPN connection problems.
- "Common VPN configuration errors and how to fix them" on page 49
  This topic identifies the most common user errors and provides possible resolutions.
- "Troubleshoot VPN with the QIPFILTER journal" on page 55
  This topic provides information about your VPN filter rules.
- "Troubleshoot VPN with the QVPN journal" on page 57
  This topic provides information about IP traffic and connections.
- "Troubleshoot VPN with the VPN job logs" on page 59
  This topic describes the various job logs that VPN uses.
- "Troubleshoot VPN with the OS/400 communications trace" on page 65
  This topic describes how to trace data on a communication line.

Get started with troubleshooting VPN

There are several ways to begin analyzing VPN problems:

1. Always make sure that you have applied the latest Program Temporary Fixes (PTFs).
2. Ensure that you meet the minimum "VPN setup requirements" on page 32.
3. Review any error messages that are found in the "View error information" on page 46 window or in the "Troubleshoot VPN with the VPN job logs" on page 59 for both the local and the remote systems. In fact, when you are troubleshooting VPN connection problems it is often necessary to look at both ends of the connection. Further, you need to take into account that there are four addresses you must check: The local and remote connection endpoints, which are the addresses where IPSec is applied to the IP packets, and the local and remote data endpoints, which are the source and destination addresses of the IP packets.
4. If the error messages you find do not provide enough information to solve the problem, check the "Troubleshoot VPN with the QIPFILTER journal" on page 55 journal.
5. The "Troubleshoot VPN with the OS/400 communications trace" on page 65 on the iSeries(TM) offers you a another place to find general information about whether the local system receives or sends connection requests.
6. The Trace TCP Application (TRCTCPAPP) command provides yet another way to isolate problems. Typically, IBM(R) Service uses TRCTCPAPP to obtain trace output in order to analyze connection problems.

Other things to check

If an error occurs after you set up a connection, and you are not sure where in the network the error occurred, try reducing the complexity of your environment. For example, instead of investigating all parts of a VPN connection at one time, start with the IP connection itself. The following list gives you some basic guidelines on how to start VPN problem analysis, from the simplest IP connection to the more complex VPN connection:

1. Start with an IP configuration between the local and remote host. Remove any IP filters on the interface that both the local and remote system use for communicating. Can you PING from the local to the remote host?

Note: Remember to prompt on the PING command; enter the remote system address and use PF10 for additional parameters, then enter the local IP address. This is particularly important when you have multiple physical or logical interfaces. It ensures that the right addresses are placed in the PING packets.

If you answer **yes**, then proceed to step 2. If you answer **no**, then check your IP configuration, interface status, and routing entries. If the configuration is correct, use a communication trace to check, for example, that a PING request leaves the system. If you send a PING request but you receive no response, the problem is most likely the network or remote system.

Note: There may be intermediate routers or firewall that do IP packet filtering and may be filtering the PING packets. PING is typically based on the ICMP protocol. If the PING is successful, you know you have connectivity. If the PING is unsuccessful, you only know the PING failed. You may want to try other IP protocols between the two systems, such as Telnet or FTP to verify connectivity.

2. Check the filter rules for VPN and ensure that they are activated. Does filtering start successfully? If you answer **yes**, then proceed to step 3. If you answer **no**, then check for error messages in the Packet Rules window in iSeries Navigator. Ensure that the filter rules do not specify Network Address Translation (NAT) for any VPN traffic.
3. "Start a VPN connection" on page 45. Does the connection start successfully? If you answer **yes**, then proceed to step 4. If you answer **no**, then check the QTOVMAN job log, the QTOKVPNIKE job logs for errors.
   When you use VPN, your Internet Service Provider (ISP) and every security gateway in your network must support the Authentication Header (AH) and Encapsulated Security Payload (ESP) protocols. Whether you choose to use AH or ESP depends on the proposals you define for your VPN connection.
4. Are you able to activate a user session over the VPN connection? If you answer **yes**, then the VPN connection works as required. If you answer **no**, then check the packet rules and the VPN dynamic-key groups and connections for filter definitions that do not allow the user traffic you want.

Common VPN configuration errors and how to fix them

This section describes of some of the more common problems that occur with VPN, and links you to tips on how to resolve them.

Note: When you configure VPN, you are actually creating several different configuration objects, each of which VPN requires to enable a connection. In terms of the VPN GUI, these objects are: The IP Security Policies and the Secure Connections. So, when this information refers to an object, it is referring to one or more of these parts of the VPN.

Common error messages you may encounter

Message	Symptom
"VPN error message: TCP5B28" on page 50	When you attempt to activate filter rules on an interface, you get this message: TCP5B28 CONNECTION_DEFINITION order violation
"VPN error message: Item not found" on page 51	When you right-click a VPN object and select either **Properties** or **Delete**, you get a message that says, **Item not found**.
"VPN error message: PARAMETER PINBUF IS NOT VALID" on page 51	When you attempt to start a connection, you get a message that says, **PARAMETER PINBUF IS NOT VALID...**

"VPN error message: Item not found, Remote key server..." on page 52	When you select **Properties** for a dynamic-key connection, you get an error that says that the server cannot find the remote key server you specified.
"VPN error message: Unable to update the object" on page 52	When you select **OK** on the property sheet for a dynamic-key group or manual connection, you get a message that tells you the system cannot update the object.
"VPN error message: Unable to encrypt key..." on page 53	You get a message that says that the system cannot encrypt your keys because the QRETSVRSEC value must be set to 1.
"VPN error message: CPF9821" on page 53	When you try to expand or open the IP Policies container in iSeries(TM) Navigator, the CPF9821- Not authorized to program QTFRPRS in QSYS library message appears.

Other problems you may run into

Error	Symptom
"VPN error: All keys are blank" on page 53	When you view the properties of a manual connection, all preshared keys and the algorithm keys for the connection are blank.
"VPN error: Sign-on for a different system appears when using Packet Rules" on page 54	The first time you use the Packet Rules interface in iSeries Navigator, a sign-on display appears for a system other than the current one.
"VPN error: Blank connection status in iSeries Navigator window" on page 54	A connection has no value in the **Status** column in the iSeries Navigator window.
"VPN error: Connection has enabled status after you stop it" on page 54	After you stop a connection, the iSeries Navigator window indicates that the connection is still enabled.
"VPN error: 3DES not a choice for encryption" on page 54	When you are working with an IKE policy transform, data policy transform, or a manual connection, the 3DES encryption algorithm is not a choice.
"VPN error: Unexpected columns display in the iSeries Navigator window" on page 54	You set up the columns you want to display in the iSeries Navigator window for your VPN connections; then, when you look at it later, different columns display.
"VPN error: Active filter rules fail to deactivate" on page 54	When you try to deactivate the current set of filter rules, the message, `The active rules failed to be deactivated` appears in the results window.
"VPN error: The key connection group for a connection changes" on page 55	When you create a dynamic-key connection, you specify a dynamic-key group and an identifier for the remote key server. Later, when you view the properties of the related connection object, the General page of the property sheet displays the same remote key server identifier, but a different dynamic-key group.

VPN error message: TCP5B28

Symptom:

When you attempt to activate filter rules on a specific interface, you receive this error message:

```
TCP5B28: CONNECTION_DEFINITION order violation
```

Possible resolution:
The filter rules you were attempting to activate contained connection definitions that were ordered differently than in a previously activated set of rules. The easiest way to resolve this error is to activate the rules file on **all interfaces** instead of on a specific interface.

VPN error message: Item not found

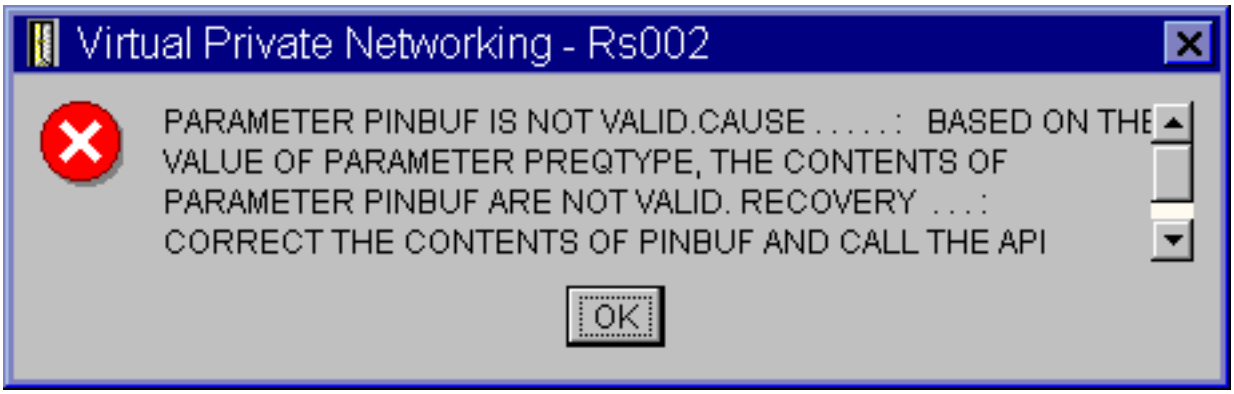
Symptom:
When you right-click an object in the Virtual Private Networking window and either select **Properties** or **Delete**, the following message appears:

Possible resolution:

- You may have deleted the object or renamed it, and have not refreshed the window yet. Consequently, the object still appears in the Virtual Private Networking window. To verify that this is the case, from the **View** menu, select **Refresh**. If the object still appears in the Virtual Private Networking window, continue to the next item in this list.
- When you configured the properties for the object, a communication error may have occurred between the VPN server and your iSeries(TM). Many of the objects that appear in the Virtual Private Networking window relate to more than one object in the VPN policy database. This means that communication errors may cause some of the objects in the database to continue to be related to an object in the VPN. Whenever you create or update an object, an error will occur when the loss of synchronization actually happens. The only way to fix the problem is to select **OK** on the error window. This launches the property sheet for the object in error. Only the name field on the property sheet has a value in it. Everything else is blank (or contains default values). Enter the correct attributes of the object, and select **OK** to save your changes.
- A similar error occurs when you try to delete the object. To fix this problem, complete the blank property sheet that opens when you click **OK** on the error message. This updates any links to the VPN policy database that were lost. You can now delete the object.

VPN error message: PARAMETER PINBUF IS NOT VALID

Symptom:
When you attempt to start a connection, a message similar to the following appears:



Possible resolution:
This happens when your system is set to use certain locales to which lowercase letters do not map correctly. To fix this error, either make sure that all objects use only uppercase letters, or change the locale of the system.

VPN error message: Item not found, Remote key server...

Symptom:
When you select **Properties** for a dynamic-key connection, a message like the following appears:

Possible resolution:
This happens when you create a connection with a particular remote key server identifier, and then the remote key server is removed from its dynamic-key group. To fix this error, click **OK** on the error message. This opens the property sheet for the dynamic-key connection that is in error. From here, you can either add the remote key server back into the dynamic-key group, or select another remote key server identifier. Click **OK** on the property sheet to save your changes.

VPN error message: Unable to update the object

Symptom:
When you select **OK** on the property sheet for a dynamic-key group or manual connection, the following message appears:

Possible resolution:
This error happens when an active connection is using the object you are trying to change. You cannot make changes to an object within an active connection. To make changes to an object, identify the appropriate active connection and then, right-click it and select **Stop** from the resulting context menu.

VPN error message: Unable to encrypt key...

Symptom:
The following error message appears:

Possible resolution:
QRETSVRSEC is a system value that indicates whether your system can store encrypted keys on it. If this value is set to 0, then preshared keys and the keys for the algorithms in a manual connection cannot be stored in the VPN policy database. To fix this problem, use a 5250 emulation session to your system. Type `wrksysval` at the command line and press **Enter**. Look for QRETSVRSEC in the list and type 2 (change) next to it. On the next panel, type 1 and press **Enter**.

VPN error message: CPF9821

Symptom:
When you try to expand the IP Policies container in iSeries(TM) Navigator, the `CPF9821- Not authorized to program QTFRPRS in QSYS library` message appears.

Possible resolution:
You may not have the required authority to retrieve the current status of Packet Rules or the VPN connection manager. Ensure that you have *IOSYSCFG authority to get access to the Packet Rules functions in iSeries Navigator.

VPN error: All keys are blank

Symptom:
All preshared keys and the algorithm keys for manual connections are blank.

Possible resolution:
This happens whenever the system value QRETSVRSEC is set back to 0. Setting this system value to 0

erases all of the keys in the VPN policy database. To fix this problem, you must set the system value to 1 and then reenter all of the keys. Refer to “VPN error message: Unable to encrypt key...” on page 53 for more information about how to do this.

VPN error: Sign-on for a different system appears when using Packet Rules

Symptom:
The first time you use Packet Rules, a sign-on display appears for a system other than the current one.

Possible resolution:
Packet Rules uses unicode to store the packet security rules in the integrated file system. The additional sign-on allows iSeries(TM) Access to obtain the appropriate conversion table for unicode. This will only occur once.

VPN error: Blank connection status in iSeries Navigator window

Symptom:
A connection has no value in the **Status** column in the iSeries(TM) Navigator window.

Possible resolution:
The blank status value indicates that the connection is in the middle of starting. That is, it is not running yet, but it has not had an error yet either. When you refresh the window, the connection will either display a status of `Error`, `Enabled`, `On-demand`, or `Idle`.

VPN error: Connection has enabled status after you stop it

Symptom:
After you stop a connection, the iSeries(TM) Navigator window indicates that the connection is still enabled.

Possible resolution:
This typically happens because you have not refreshed the iSeries Navigator window yet. As such, the window contains outdated information. To fix this, from the **View** menu, select **Refresh** .

VPN error: 3DES not a choice for encryption

Symptom:
When working with an IKE policy transform, data policy transform, or a manual connection, the 3DES encryption algorithm is not a choice.

Possible resolution:
Most likely, you only have the Cryptographic Access Provider AC2 (5722-AC2) product installed on your system, and not Cryptographic Access Provider AC3 (5722-AC3). AC2 only allows for the Data Encryption Standard (DES) encryption algorithm due to restrictions on key lengths.

VPN error: Unexpected columns display in the iSeries Navigator window

Symptom:
You set up the columns you want to display in the iSeries Navigator window for your VPN connections; then, when you look at it later, different columns display.

Possible resolution:
When you change the columns to view, the changes are not specific to a particular user or PC, but rather, are system-wide. So, when someone else changes the columns in the window, the changes affect everyone viewing connections on that system.

VPN error: Active filter rules fail to deactivate

Symptom:
When you try to deactivate the current set of filter rules, the message, `The active rules failed to be deactivated` appears in the results window.

Possible resolution:
Typically, this error message means that there is at least one active VPN connection. You must stop each of the connections that have a status of `enabled`. To do this, right-click each of the active connections and select **Stop**. You can now deactivate the filter rules.

VPN error: The key connection group for a connection changes

Symptom:
When you create a dynamic-key connection, you specify a dynamic-key group and an identifier for the remote key server. Later, when you select **Properties** on the related connection object, the **General** page of the property sheet displays the same remote key server identifier, but a different dynamic-key group.

Possible resolution:
The identifier is the only information stored in the VPN policy database that refers to the remote key server of the dynamic-key connection . When VPN looks up a policy for a remote key server, it looks for the first dynamic-key group that has that remote key server identifier in it. So, when you view the properties for one these connections, it uses the same dynamic-key group that VPN found. If you do not want to associate the dynamic-key group with that remote key server, you can do one of the following:

1. Remove the remote key server from the dynamic-key group.
2. Expand **By Groups** in the left pane of the VPN interface, and select and drag the dynamic-key group you want to the top of the table in the right pane. This ensures that VPN checks this dynamic-key group first for the remote key server.

Troubleshoot VPN with the QIPFILTER journal

The QIPFILTER journal is located in the QUSRSYS library and contains information about filter rule sets, as well as information about whether an IP datagram was permitted or denied. Logging is performed based on the journaling option you specify in your filter rules.

How to enable the IP Packet Filter journal
Use the Packet Rules editor in iSeries(TM) Navigator to activate the QIPFILTER journal. You must enable the logging function for each individual filter rule. There is no function that allows logging for all IP datagrams going into or out of the system.

Note: To enable the QIPFILTER journal, your filters must be deactivated.

The following steps describe how to enable journaling for a particular filter rule:

1. In iSeries Navigator, expand your server **—> Network—> IP Policies**.
2. Right-click **Packet Rules** and select **Configuration**. This displays the Packet Rules interface.
3. Open an existing filter rule file.
4. Double-click the filter rule you want to journal.
5. On the **General** page, select **FULL** in the **Journaling** field as in the dialog box shown above. This enables logging for this particular filter rule.
6. Click **OK**.
7. Save and activate the changed filter rule file.

If an IP datagram matches the definitions of the filter rule, an entry is made in the QIPFILTER journal.

How to use the QIPFILTER journal
OS/400(R) automatically creates the journal the first time you activate IP packet filtering. To view the entry-specific details in the journal, you can display the journal entries on the screen or you can use an output file.

By copying the journal entries to the output file, you can easily view the entries using query utilities such as Query/400 or SQL. You can also write your own HLL programs to process the entries in the output files.

The following is an example of the Display Journal (DSPJRN) command:

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Use the following steps to copy the QIPFILTER journal entries to the output file:

1. Create a copy of the system-supplied output file QSYS/QATOFIPF into a user library by using the Create Duplicate Object (CRTDUPOBJ) command. The following is an example of the CRTDUPOBJ command:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
       NEWOBJ(myfile)
   ```

2. Use the Display Journal (DSPJRN) command to copy the entries from the QUSRSYS/QIPFILTER journal to the output file you created in the previous step.

If you copy the DSPJRN into an output file that does not exist, the system creates a file for you, but this file does not contain the correct field descriptions.

Note: The QIPFILTER journal only contains permit or deny entries for filter rules where the journaling option is set to FULL. For example, if you set up only PERMIT filter rules, IP datagrams that are not explicitly permitted are denied. For those denied datagrams, no entry is added to the journal. For problem analysis you might add a filter rule that explicitly denies all other traffic and performs FULL journaling. Then, you will get DENY entries in the journal for all IP datagrams that are denied. Due to performance reasons, it is not recommended that you enable journaling for all filter rules. Once your filter sets are tested, reduce the journaling to a useful subset of entries.

See “QIPFILTER journal fields” for a table that describes the QIPFILTER output file.

QIPFILTER journal fields

The following table describes the fields in the QIPFILTER output file:

Field Name	Field Length	Numeric	Description	Comments
TFENTL	5	Y	Length of entry	
TFSEQN	10	Y	Sequence number	
TFCODE	1	N	Journal code	Always M
TFENTT	2	N	Entry type	Always TF
TFTIME	26	N	SAA timestamp	
TFJOB	10	N	Job name	
TFUSER	10	N	User profile	
TFNBR	6	Y	Job number	
TFPGM	10	N	Program name	
TFRES1	51	N	Reserved	
TFUSPF	10	N	User	
TFSYMN	8	N	System name	
TFRES2	20	N	Reserved	
TFRESA	50	N	Reserved	
TFLINE	10	N	Line description	*ALL if TFREVT is U* , Blank if TFREVT is L*, Line name if TFREVT is L

Field Name	Field Length	Numeric	Description	Comments
TFREVT	2	N	Rule event	L* or L when rules are loaded. U* when rules are unloaded, A when filter action
TFPDIR	1	N	IP Packet direction	O is outbound, I is inbound
TFRNUM	5	N	Rule number	Applies to the rule number in the active rules file
TFACT	6	N	Filter action taken	PERMIT, DENY, or IPSEC
TFPROT	4	N	Transport protocol	1 is ICMP 6 is TCP 17 is UDP 50 is ESP 51 is AH
TFSRCA	15	N	Source IP address	
TFSRCP	5	N	Source port	Garbage if TFPROT= 1 (ICMP)
TFDSTA	15	N	Destination IP address	
TFDSTP	5	N	Destination port	Garbage if TFPROT= 1 (ICMP)
TFTEXT	76	N	Additional text	Contains description if TFREVT= L* or U*

Troubleshoot VPN with the QVPN journal

VPN uses a separate journal to log information about the IP traffic and connections called the QVPN journal. The QVPN is stored in the QUSRSYS library. The journal code is M and the journal type is TS. You will rarely use journal entries on a daily basis. Instead, you might find them useful for troubleshooting and verifying that your system, keys, and connections are functioning in the manner that you specified. For example, journal entries help you understand what happens to your data packets. They also keep you informed of your current VPN status.

How to enable the VPN journal

Use the virtual private networking interface in iSeries(TM) Navigator to activate the VPN journal. There is no function that allows logging for all VPN connections. Therefore, you must enable the logging function for each individual dynamic-key group or manual connection.

The following steps describe how to enable the journal function for a particular dynamic-key group or manual connection:

1. In iSeries Navigator, expand your server **—> Network—> IP Policies—> Virtual Private Networking—> Secure Connections.**
2. For dyanamic-key groups, expand **By Group** and then right-click the dynamic key group for which you want to enable journaling and select **Properties.**
3. For manual connections, expand **All Connections** and then right-click the manual connection for which you want to enable journaling.
4. On the **General** page, select the level of journaling you require. You have the choice between four options. These are:

None
No journaling occurs for this connection group.
All
Journaling occurs for all connection activities, such as starting or stopping a connection, or key refreshes, as well as IP traffic information.
Connection Activity
Journaling occurs for such connection activity as starting or stopping a connection.
IP traffic
Journaling occurs for all of the VPN traffic that is associated with this connection. A log entry is made every time a filter rule is invoked. The system records IP traffic information in the journal QIPFILTER, which is located in the QUSRSYS library.

5. Click **OK**.
6. Start the connection to activate journaling.

Note: Before you can stop journaling, make sure that the connection is inactive. To change the journaling status of a connection group, make sure that no active connections are associated with that particular group.

How to use the VPN journal
To view the entry-specific details in the VPN journal, you can display the entries on the screen or you can use the output file.

By copying the journal entries to the output file, you can easily view the entries by using query utilities such as Query/400 or SQL. You can also write your own HLL programs to process the entries in the output files. The following is an example of the Display Journal (DSPJRN) command:

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Use the following steps to copy the VPN journal entries to the output file:

1. Create a copy of the system-supplied output file QSYS/QATOVSOF into a user library. You can do this by using the Create Duplicate Object (CRTDUPOBJ) command. The following is an example of the CRTDUPOBJ command:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. Use the Display Journal (DSPJRN) command to copy the entries from the QUSRSYS/QVPN journal to the output file created in the previous step. If you attempt to copy the DSPJRN into an output file that does not exist, the system creates a file for you, but this file does not contain the correct field descriptions.

See “QVPN journal fields” for a table that describes the fields in the QVPN output file.

QVPN journal fields

The following table describes the fields in the QVPN output file:

Field Name	Field Length	Numeric	Description	Comments
TSENTL	5	Y	Length of entry	
TSSEQN	10	Y	Sequence number	
TSCODE	1	N	Journal code	Always M
TSENTT	2	N	Entry type	Always TS
TSTIME	26	N	SAA entry timestamp	
TSJOB	10	N	Name of job	
TSUSER	10	N	User of job	

Field Name	Field Length	Numeric	Description	Comments
TSNBR	6	Y	Number of job	
TSPGM	10	N	Name of program	
TSRES1	51	N	Not used	
TSUSPF	10	N	User profile name	
TSSYNM	8	N	System name	
TSRES2	20	N	Not used	
TSRESA	50	N	Not used	
TSESDL	4	Y	Length of specific data	
TSCMPN	10	N	VPN component	
TSCONM	40	N	Connection name	
TSCOTY	10	N	Connection type	
TSCOS	10	N	Connection state	
TSCOSD	8	N	Start date	
TSCOST	6	N	Start time	
TSCOED	8	N	End date	
TSCOET	6	N	End time	
TSTRPR	10	N	Transport protocol	
TSLCAD	43	N	Local client address	
TSLCPR	11	N	Local ports	
TSRCAD	43	N	Remote client address	
TSCPR	11	N	Remote ports	
TSLEP	43	N	Local endpoint	
TSREP	43	N	Remote endpoint	
TSCORF	6	N	Times refreshed	
TSRFDA	8	N	Date of next refresh	
TSRFTI	6	N	Time of next refresh	
TSRFLS	8	N	Refresh life-size	
TSSAPH	1	N	SA Phase	
TSAUTH	10	N	Authentication type	
TSENCR	10	N	Encryption type	
TSDHGR	2	N	Diffie-Hellman group	
TSERRC	8	N	Error code	

Troubleshoot VPN with the VPN job logs

When you encounter problems with your VPN connections, it is always advisable to analyze the job logs. In fact, there are several job logs that contain error messages and other information related to a VPN environment.

It is important that you analyze job logs on both sides of the connection if both sides are iSeries(TM) servers. When a dynamic connection fails to start, it is helpful if you understand what is happening on the remote system.

The VPN jobs, QTOVMAN and QTOKVPNIKE, run in the subsystem QSYSWRK. You can “View the VPN server job logs” on page 47 from OS/400(R) iSeries Navigator.

This section introduces the most important jobs for a VPN environment. The following list shows the job names with a brief explanation of what the job is used for:

QTCPIP
This job is the base job that starts all the TCP/IP interfaces. If you have fundamental problems with TCP/IP in general, analyze the QTCPIP job log.

QTOKVPNIKE
The QTOKVPNIKE job is the VPN key manager job. The VPN key manager listens to UDP port 500 to perform the Internet Key Exchange (IKE) protocol processing.

QTOVMAN
This job is the connection manager for VPN connections. The related job log contains “Common VPN Connection Manager error messages” for every connection attempt that fails.

QTPPANSxxx
This job is used for PPP dial-up connections. It answers to connection attempts where *ANS is defined in a PPP profile.

QTPPPCTL
This is a PPP job for dial-out connections.

QTPPPL2TP
This is the Layer Two Tunneling Protocol (L2TP) manager job. If you have problems setting up an L2TP tunnel, look for messages in this job log.

Common VPN Connection Manager error messages

This section describes of some of the more common VPN Connection Manager error messages you may encounter.

In general, the VPN Connection Manager logs two messages in the QTOVMAN job log when an error occurs with a VPN connection. The first message provides details regarding the error. You can view information about these errors in iSeries(TM) Navigator by right-clicking the connection in error and selecting **Error Information**.

The second message describes the action you were attempting to perform on the connection when the error occurred. For example, starting or stopping it. Messages TCP8601, TCP8602, and TCP860A, described below, are typical examples of these second messages.

VPN Connection Manager error messages

Message	Cause	Recovery
TCP8601 Could not start VPN connection [*connection name*]	Could not start this VPN connection due to one of these reason codes: *0* - A previous message in the job log with the same VPN connection name has more detailed information. *1* - VPN policy configuration. *2* - Communications network failure. *3* - VPN Key Manager failed to negotiate a new security association. *4* - The remote endpoint for this connection is not configured properly. *5* - VPN Key Manager failed to respond to VPN Connection Manager. *6* - IP Security Component VPN connection load failure. *7* - PPP Component failure.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Correct the errors and try the request again. 3. Use iSeries Navigator to "View the attributes of active connections" on page 46. Connections that could not start will be in error state.
TCP8602 Error occurred stopping VPN connection [*connection name*]	The specified VPN connection was requested to be stopped, however, it did not stop or stopped in error due to Reason Code: *0* - A previous message in the job log with the same VPN connection name has more detailed information. *1* - The VPN connection does not exist. *2* - Internal communications failure with VPN Key Manager. *3* - Internal communications failure with IPSec component. *4* - Communication failure with VPN connection remote endpoint.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Correct the errors and try the request again. 3. Use iSeries Navigator to "View the attributes of active connections" on page 46. Connections that could not start will be in error state.
TCP8604 Start of VPN connection [*connection name*] failed	A start of this VPN connection failed due to one of these reason codes: *1* - Could not translate the remote host ame to an IP address. *2* - Could not translate the local host name to an IP address. *3* - VPN policy filter rule associated with this VPN connection is not loaded. *4* - A user-specified key value is not valid for its associated algorithm. *5* - The initiation value for the VP connection does not allow the specified action. *6* - A system role for the VPN connection is inconsistent with information from the connection group. *7* - Reserved. *8* - Data endpoints (local and remote addresses and services) of this VPN connection are inonsistent with information from the connection group. *9* - Identifier type not valid.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Correct the errors and try the request again. 3. Use iSeries Navigator to check or correct the VPN policy configuration. Ensure that the dynamic-key group associated with this connection has acceptable values configured.

Message	Cause	Recovery
TCP8605 VPN Connection Manager could not communicate with VPN Key Manager	The VPN Connection Manager requires the services of the VPN Key Manager to establish security associations for dynamic VPN connections. The VPN Connection Manager could not communicate with the VPN Key Manager.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Verify the *LOOPBACK interface is active by using the NETSTAT OPTION(*IFC) command. 3. End the VPN server by using the ENDTCPSVR SERVER(*VPN) command. Then restart the VPN server by using the STRTCPSRV SERVER(*VPN) command. **Note:** This causes all curent VPN connections to end.
TCP8606 The VPN Key Manager could not establish the requested security association for connection, [*connection name*]	The VPN Key Manager could not establish the requested security association due to one of these reason codes: *24* - VPN Key Manager key connection authentication failed. *8300* - Failure occurred during VPN Key Manager key connection negotiations. *8306* - No local preshared key found. *8307* - No remote IKE phase 1 policy found. *8308* - No remote preshared key found. *8327* - VPN Key Manager key connection negotiations timed out. *8400* - Failure occurred during VPN Key Manager VPN connection negotiations. *8407* - No remote IKE phase 2 policy found. *8408* - VPN Key Manager VPN connection negotiations timed out. *8500 or 8509* - VPN Key Manager network error has occurred.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Correct the errors and try the request again. 3. Use iSeries Navigator to check or correct the VPN policy configuration. Ensure that the dynamic-key group associated with this connection has acceptable values configured.
TCP8608 VPN connection, [*connection name*], could not obtain a NAT address	This dynamic-key group or data connection specified that network address translation (NAT) be done on one or more addresses, and that failed due to one of these likely reason codes: *1* - Address to apply NAT to is not a single IP address. *2* - All available addresses have been used.	1. Check the "View the VPN server job logs" on page 47 for additional messages. 2. Correct the errors and try the request again. 3. Use iSeries Navigator to check or correct the VPN policy. Ensure that the dynamic-key group associated with this connection has acceptable values for addresses configured.

Message	Cause	Recovery
TCP8620 Local connection endpoint not available	Could not enable this VPN connections because the local connection endpoint was not available.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Make sure the local connection endpoint is defined and started by using the NETSTAT OPTION(*IFC) command. 3. Correct any errors and try the request again.
TCP8621 Local data endpoint to available	Could not enable this VPN connection because the local data endpoint was not available.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Make sure the local connection endpoint is defined and started by using the NETSTAT OPTION(*IFC) command. 3. Correct any errors and try the request again.
TCP8622 Transport encapsulation not permitted with a gateway	Could not enable this VPN connection because the negotiated policy specified transport encapsulation mode and this connection is defined as a security gateway.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to change the VPN policy associated with this VPN connection. 3. Correct any errors and try the request again.
TCP8623 VPN connection overlaps with an existing one	Could not enable this VPN connection because an existing VPN connection is already enabled. This connection has a local data endpoint of, [*local data endpoint value*] and a remote data endpoint of, [*remote data endpoint value*].	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to view all enabled connections that have local data endpoints and remote data endpoints overlapping the connection. Change the policy of the existing connection if both connections are required. 3. Correct any errors and try the request again.

Message	Cause	Recovery
TCP8624 VPN connection not within scope of associated policy filter rule	Could not enable this VPN connection because the data endpoints are not within the defined policy filter rule.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to display the data endpoint restrictions for this connection or dynamic-key group. If **Subset of policy filter** or **Customize to match policy filter** is selected, then check the data endpoints of the connection. These must fit within the active filter rule that has an IPSEC action and a VPN connection name associated with this connection. Change the existing connection's policy or the filter rule to enable this connection. 3. Correct any errors and try the request again.
TCP8625 VPN connection failed an ESP algorithm check	Could not enable this VPN connection because the secret key associated with the connection was insufficient.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to display the policy associated with this connection and enter a different secret key. 3. Correct any errors and try the request again.
TCP8626 VPN connection endpoint is not the same as the data endpoint	Could not enable this VPN connection because the policy specifies that it is a host, and the VPN connection endpoint is not the same as the data endpoint.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to display the data endpoint restrictions for this connection or dynamic-key group. If **Subset of policy filter** or **Customize to match policy filter** is selected, then check the data endpoints of the connection. These must fit within the active filter rule that has an IPSEC action and a VPN connection name associated with this connection. Change the existing connection's policy or the filter rule to enable this connection. 3. Correct any errors and try the request again.

Message	Cause	Recovery
TCP8628 Policy filter rule not loaded	The policy filter rule for this connection is not active.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to display the active policy filters. Check the policy filter rule for this connection. 3. Correct any errors and try the request again.
TCP8629 IP packet dropped for VPN connection	This VPN connection has VPN NAT configured and the required set of NAT addresses has exceeded the available NAT addresses.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Use iSeries Navigator to increase the number of NAT addresses assigned for this VPN connection. 3. Correct any errors and try the request again.
TCP862A PPP connection failed to start	This VPN connection was associated with a PPP profile. When it was started, an attempt was made to start the PPP profile, but a failure occurred.	1. Check the "View the VPN server job logs" on page 47 for additional messages pertaining to this connection. 2. Check the joblog associated with the PPP connection. 3. Correct any errors and try the request again.

Troubleshoot VPN with the OS/400 communications trace

iSeries(TM) OS/400(R) provides the capability to trace data on a communications line, such as a local area network (LAN) or wide area network (WAN) interface. The average user may not understand the entire contents of the trace data. However, you can use the trace entries to determine whether a data exchange between the local and the remote systems took place.

Starting the communications trace

Use the Start Communications Trace (STRCMNTRC) command to start the communications trace on your system. The following is an example of the STRCMNTRC command:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('VPN Problems')
```

The command parameters are explained in the following list:

CFGOBJ (Configuration object)
The name of the configuration object to trace. The object is either a line description, a network interface description, or a network server description.

CFGTYPE(Configuration type)
Whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is being traced.

MAXSTG (Buffer size)
The buffer size for the trace. The default value is set to 128 KB. The range goes from 128 KB to 64 MB. The actual maximum system-wide buffer size is defined within the System Service Tools (SST).

Therefore, you may receive an error message when using a larger buffer size on the STRCMNTRC command than defined in the SST. Keep in mind that the sum of buffer sizes specified on all started communications traces must not exceed the maximum buffer size defined in the SST.

DTADIR (Data direction)
The direction of data traffic to be traced. The direction can be outbound traffic only (*SND), inbound traffic only (*RCV), or both directions (*BOTH).

TRCFULL (Trace full)
What occurs when the trace buffer is full. This parameter has two possible values. The default value is *WRAP, which means, when the trace buffer is full, the trace wraps to the beginning. The oldest trace records are written over by new ones as they are collected.

The second value *STOPTRC let the trace stop when the trace buffer, specified in the MAXSTG parameter is full of trace records. As general rule, always define the buffer size to be large enough to store all the trace records. If the trace wraps, you may lose important trace information. If you experience a highly intermittent problem, define the trace buffer to be large enough that a wrap of the buffer will not discard any important information.

USRDTA (Number of user bytes to trace)
Defines the number of data to be traced in the user data part of the data frames. By default only the first 100 bytes of user data are captured for LAN interfaces. For all other interfaces, all user data is captured. Make sure you specify *MAX if you suspect problems in the user data of a frame.

TEXT (Trace description)
Provides a meaningful description of the trace.

Stopping the communications trace
If you do not otherwise specify, the trace typically stops as soon as the condition for which you are tracing occurs. Use the End Communications Trace (ENDCMNTRC) command to stop the trace. The following command is an example of the ENDCMNTRC command:

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

The command has two parameters:

CFGOBJ (Configuration object)
The name of the configuration object for which the trace is running. The object is either a line description, a network interface description, or a network server description.

CFGTYPE (Configuration type)
Whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is being traced.

Printing the trace data
After you stop the communications trace, you need to print the trace data. Use the Print Communications Trace (PRTCMNTRC) command to perform this task. Since all line traffic is captured during the trace period, you have multiple filter options for output generation. Try to keep the spooled file as small as possible. This makes the analysis faster and more efficient. In the case of a VPN problem, filter on IP traffic only and, if possible, on a specific IP address. You also have the option of filtering on a specific IP port number. The following is an example of the PRTCMNTRC command:

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)
    SLTPORT(500) FMTBCD(*NO)
```

In this example, the trace is formatted for IP traffic and contains only data for the IP address, where the source or destination address is 10.50.21.1 and the source or destination IP port number is 500.

Only the most important command parameters for analyzing VPN problems, are explained below:

CFGOBJ (Configuration object)
The name of the configuration object for which the trace is running. The object is either a line description, a network interface description, or a network server description.

CFGTYPE (Configuration type)
Whether a line (*LIN), a network interface (*NWI), or a network server (*NWS) is being traced.

FMTTCP (Format TCP/IP data)
Whether to format the trace for TCP/IP and UDP/IP data. Specify *YES to format the trace for IP data.

TCPIPADR (Format TCP/IP data by address)
This parameter consists of two elements. If you specify IP addresses on both elements, only IP traffic between those addresses will print.

SLTPORT (IP port number)
The IP port number to filter.

FMTBCD (Format broadcast data)
Whether all broadcast frames are printed. Yes is the default. If you do not want; for example, Address Resolution Protocol (ARP) requests, specify *NO; otherwise you may be overwhelmed with broadcast messages.

Related information for VPN

For more VPN configuration scenarios and descriptions, see these other sources of information:

- **OS/400(R) V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries(TM) Server with Windows(R) 2000 VPN Clients, REDP0153**

  This IBM Redpaper provides a step-by-step process for configuring the VPN tunnel using V5R1 VPN and the Windows 2000 integrated L2TP and IPSec support.
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  This redbook explores VPN concepts and describes its implementation using IP security (IPSec) and Layer 2 Tunneling Protocol (L2TP) on OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  This redbook explores all the integrated security features available on the OS/400 system such as IP filters, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, auditing, and logging. It describes their use through practical examples.
- **Virtual Private Networking: Securing Connections**

  This Web page highlights latebreaking VPN news, lists the latest PTFs, and links to other sites of interest.
- **Other security related manuals and redbooks**
  Go here for a list of security related information available online.

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 want 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)

.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance, and WordPro are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

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

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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