Virtual private networking
Virtual private networking ........................................... 1
What’s new for V5R1 ............................................... 2
Print this topic ..................................................... 3
Migrating from a prior release ................................. 3
VPN scenarios .................................................... 4
  VPN scenario: Branch office connection ...................... 5
  VPN scenario: Business to business connection ............... 10
  VPN scenario: L2TP voluntary tunnel protected by VPN ....... 15
VPN protocols and concepts ..................................... 22
  IP Security (IPSec) protocols .................................. 22
  Internet Key Exchange protocol ............................. 25
  Layer 2 Tunnel Protocol (L2TP) ............................ 26
  Network address translation for VPN ......................... 27
  IP Compression (IPComp) ................................... 27
OS/400 VPN setup requirements ............................... 28
Planning for VPN ............................................... 28
  Determine what type of VPN to create ....................... 28
  Complete the VPN planning worksheets ...................... 29
Configuring VPN ............................................... 32
  Configuring connections with the VPN Connection wizard ... 34
  Configuring VPN security policies ......................... 34
  Configuring the VPN secure connection ..................... 35
  Configuring a manual connection ............................ 36
  Configuring VPN packet rules .............................. 37
Starting a VPN connection ..................................... 41
Managing OS/400 VPN with Operations Navigator ............. 42
  Setting default attributes for your connections .......... 42
  Resetting connections in error state ....................... 42
  Viewing error information ................................. 43
  Viewing the attributes of active connections ............... 43
  Using the VPN server trace ............................... 43
  Viewing the VPN server job logs ........................... 44
  Stopping a VPN connection ................................. 44
  Viewing the attributes of Security Associations (SA) ....... 44
Deleting VPN configuration objects .......................... 44
Troubleshooting OS/400 VPN ................................. 44
  Getting started with troubleshooting OS/400 VPN ......... 45
  Common OS/400 VPN configuration errors and how to fix them 46
  Troubleshooting OS/400 VPN with the QIPFILTER journal .... 52
  Troubleshooting OS/400 VPN with the QVPN journal ....... 55
  Troubleshooting OS/400 VPN the VPN job logs .................. 57
  Troubleshooting OS/400 VPN with the OS/400 Communications trace .... 63
Other VPN information ......................................... 65
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 VPN is an optionally-installable component of Operations 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.

OS/400 VPN runs on the network layer of the TCP/IP layered communications stack model. Specifically, OS/400 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.

OS/400 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 impact a VPN will have on your entire network. Proper planning and implementation are essential to your success. You should review these topics to ensure that you know how VPNs work and how you might use them:

What's new for V5R1?
This topic describes what information is new or significantly changed in this release.

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

Migrating from an earlier version of OS/400 VPN
If you have questions about migrating to OS/400 VPN from an earlier version, this topic highlights what you need to know to ensure a smooth upgrade.

VPN scenarios
Review these scenarios to become familiar with the basic VPN types and the steps involved in configuring them.

VPN protocols and concepts
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 OS/400 VPN uses in its implementation.

OS/400 VPN setup requirements
Before you begin, ensure that you meet the minimum requirements for creating a VPN.

Planning VPN
After you determine that you meet the minimum setup requirements, you can begin configuring your VPN. The first step is planning. You must determine what type of VPN best suits your specific business needs, and then use the VPN planning advisor to generate a planning worksheet that is customized to your specifications.
Configuring VPN
After planning for your VPN, you can begin configuring it. This topic provides you with an overview of what you can do with OS/400 VPN and how to do it.

Managing VPN
This topic describes various tasks you can perform to manage your active VPN connections, including how to make changes to, monitor, or delete them.

Troubleshooting OS/400 VPN
Refer to this topic when you experience problems with your VPN connections.

Other VPN information
Go here for links to other sources of VPN information and related topics.

What’s new for V5R1
Changes to the Version 5 Release 1 (V5R1) Virtual private networking topic include:

- Enhancements to the basic configuration scenarios from last release.
- Updates to the VPN planning advisor that helps you determine what type of VPN you should create to address your specific business needs. The advisor also suggests what steps you must take to configure the VPN.
- More troubleshooting information including a table that lists error messages, result codes, and recovery information.
- Information about migrating from a prior release of the operating system.

Enhancements to the V5R1 OS/400 VPN function include:

- The addition of digital signature support for Internet Key Exchange (IKE) phase 1 authentication (See [25]). In prior releases, OS/400 VPN only supported preshared keys as the authentication method it used for phase 1 negotiations.
- Support for on-demand connections. An on-demand connection starts only after IP datagrams that are destined for a specific VPN connection attempt to flow. In other words, the connection is only enabled when it is needed. On-demand connections require that the policy filter be loaded, the VPN server be running, and the appropriate interface be active on the system. After a period of inactivity on the connection, the VPN connection will become inactive while it waits for more IP datagrams to flow.
- A system-wide responder IKE policy that lists which algorithms your system will accept when it responds to an IKE request.
- Policy filter rules can be generated automatically by the VPN graphical user interface (GUI). However, if you created VPN connections in prior releases of the operating system (V4R4 or V4R5), and plan to configure new connections in V5R1, you should read this article: “Before you begin configuring VPN packet rules.” It describes some things you need to consider to ensure that all of your filter rules load correctly and work the way you intend.
- Additional network address translation for VPN (VPN NAT) support.
- Support for the IP Compression (IPComp) protocol. IPComp reduces the size of an IP datagram by compressing it to increase the communication performance between two VPN partners.
- VPN connections can now be applied to *OPC interfaces (OptiConnect).
Print this topic

You can view or download a PDF version of this document for viewing or printing. You must have Adobe Acrobat Reader installed to view PDF files. You can download a copy from


To view or download the PDF version, select Virtual private networking (VPN) (about 95 pages or 509 KB).

To save a PDF on your workstation for viewing or printing:
1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click File.
3. Click Save As...
4. Navigate to the directory in which you would like to save the PDF.
5. Click Save.

Migrating from a prior release

When you upgrade to V5R1 from either V4R4 or V4R5 of the operating system all of your existing configurations and VPN database objects, which are located in the QUSRYSYS library, will migrate automatically to the new version’s format. Be aware however, that the new format of the VPN policy database makes it impossible to restore an earlier version once you have installed V5R1.

The following table lists each of the VPN database objects by release. You need this information when you back up your VPN configurations. It is always a good idea to keep a current backup of your VPN Policy. In addition, you should always backup your VPN Policy prior to migrating.

Objects in bold denote those that have been replaced or added this release.

<table>
<thead>
<tr>
<th>V4R4 and V4R5 VPN database objects</th>
<th>V5R1 VPN database objects</th>
</tr>
</thead>
</table>

Virtual private networking 3
Related information

In V5R1, OS/400 VPN can create your VPN packet rules automatically. If you have policy filter rules (rules with an action type of IPSEC) that you created in V4R4 or V4R5, and you want to use those same rules in V5R1, but also plan to create new connections, there are several items you need to consider. Review this topic, "Before you begin configuring your VPN packet rules" for the details.

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: Branch office connection**
  In this scenario, your company wants to establish a VPN between the subnets of two remote departments through a pair of iSeries 400 computers acting as VPN gateways.

- **VPN scenario: Business to Business connection**
  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: L2TP voluntary tunnel protected by VPN**
  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.

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

- **Remote Access to AS/400 with Windows 2000 VPN clients, REDP0036**
  This redpaper describes how to implement secure connections for traveling employees and virtual office employees that need access to the corporate office. The remote users access the corporate office AS/400 system using a PC with Windows 2000. The connection is secured by a VPN (L2TP tunnel protected by IPSec).

- **AS/400 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 native network security features available on the AS/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.

- **Set Up a VPN (Virtual Private Network) to Securely Manage Your AS/400 Across the Internet**
  In this Technical Studio topic, you’ll set up a virtual private network (VPN) that uses IP Security (IPSec) protocol and Layer 2 Tunneling Protocol (L2TP) to protect and conceal sensitive information from hackers and thieves who prowl the Internet.

**VPN scenario: 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 could be the company's own private network or the public Internet.

**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. In fact, you should consider the security risks involved any time you connect to the Internet. Review this redbook, AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00, for a detailed description of various methods for reducing these risks.

**Scenario 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 Internet addresses to each client.

Scenario 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 400 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.

Scenario details

The following figure illustrates the network characteristics of MyCo.

Human Resources Department
• iSeries-A runs on OS/400 Version 5 Release 1 (V5R1) and acts as the Human Resources Department 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 1 (V5R1) and acts as the Finance Department 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.

Configure the connection

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, please refer to TCP/IP routing and workload balancing in the Information Center.
2. Complete the planning worksheets and checklists for both systems.
3. Configure (See 9) VPN on the Human Resources VPN gateway (iSeries-A).
4. Configure (See 9) VPN on the Finance VPN gateway (iSeries-C).
5. Activate (See 9) filter rules on both servers.
6. Start the connection from iSeries-A.
7. Test communications between the two remote subnets.

Branch office connection: 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 should 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.

<p>| Prerequisite checklist | Answers |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your OS/400 V5R1 (5722-SS1) or later?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is Cryptographic Access Provider (5722-AC2 or AC3) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is Client Access Express (5722-XE1) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is OS/400 Operations Navigator installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the Network subcomponent of Operations Navigator installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is TCP/IP configured on your iSeries 400 (including IP interfaces, routes, local host name, and local domain name)?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is normal TCP/IP communication established between the required endpoints?</td>
<td>Yes</td>
</tr>
<tr>
<td>Have you applied the latest program temporary fixes (PTFs)?</td>
<td>Yes</td>
</tr>
<tr>
<td>If the VPN tunnel traverses firewalls or routers that implement IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?</td>
<td>Yes</td>
</tr>
<tr>
<td>Are the firewalls configured to enable IP forwarding?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You need this information to configure the VPN

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

**Step 3: Configure VPN on iSeries-A**

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

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 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. Enter 204.146.18.227 in 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 appears, select No, packet rules will be activated at a later time and then click OK.

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, 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 Operations Navigator, expand **iSeries-A ->Network ->IP Policies**.
2. Right-click **Packet Rules** and select **Configuration**. This displays the Packet Rules interface.
3. From the **File** menu, select **New File**.
4. From the **File** menu, select **Activate**. A dialog opens that allows you to specify whether to activate the rules on a specific interface or on all interfaces. We recommend that you always activate your rules on all interfaces.
5. Click **OK** on the dialog to confirm that you want to verify and activate the rules on the interface or interfaces you specified. When the verification process completes, a message log displays at the bottom of the window. If the system was able to verify the rules as error free, the system activates them. If there are errors, you must resolve them before you attempt to reactivate the rules.
6. Repeat these steps to activate packet rules on iSeries-C.

**Step 6: Start connection**

Follow these steps to start the HRgw2FINgw connection from iSeries-A:

1. In Operations 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 **HRgw2FINgw** and select **Start**.
6. From the **View** menu, select **Refresh**. If the connection starts successfully, the status should 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 you have successfully started the connection, you should test the connectivity to ensure that the remote subnets can communicate with each other. To do this, follow these steps:

1. In Operations Navigator, expand **iSeries-A ->Network**.
2. Right-click **TCP/IP Configuration** and select **Utilities** and then select **Ping**.
3. From the **Ping from** dialog, 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: 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. OS/400 VPN offers an alternative for companies who desire 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.

**Scenario 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 should 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.

**Scenario details**

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

![Network diagram]

**MyCo Supply Network**
- iSeries-A runs on OS/400 Version 5 Release 1 (V5R1).
- 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 1 (V5R1).
• 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

Configure the connection

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 allows ensures that hosts on each subnet route properly to their respective gateway for access to the remote subnet. You should 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, please refer to TCP/IP routing and workload balancing in the Information Center.
2. Complete the planning worksheets and checklists for both systems.
3. Configure (See 13) VPN on iSeries-A in MyCo’s Supply network.
4. Configure (See 14) VPN on iSeries-C in TheirCo’s Manufacturing network.
5. Activate (See 14) filter rules on both servers.
6. Start the connection from iSeries-A.
7. Test communications between the two remote subnets.

Business to business connection: 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 should 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.

<table>
<thead>
<tr>
<th>Prerequisite checklist</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your OS/400 V5R1 (5722-SS1) or later?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is Cryptographic Access Provider (5722-AC2 or AC3) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is Client Access Express (5722-XE1) installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is OS/400 Operations Navigator installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the Network subcomponent of Operations Navigator installed?</td>
<td>Yes</td>
</tr>
<tr>
<td>Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1? Yes
Is TCP/IP configured on your iSeries 400 (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 implement 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

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of connection are you creating?</td>
<td>host-to-host</td>
</tr>
<tr>
<td>What will you name the dynamic-key group?</td>
<td>MyCo2TheirCo</td>
</tr>
<tr>
<td>What type of security and system performance do you require to protect your keys?</td>
<td>highest</td>
</tr>
<tr>
<td>Are you using certificates to authenticate the connection?</td>
<td>Yes</td>
</tr>
<tr>
<td>If no, what is the preshared key?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the local key server?</td>
<td>IP address: 10.6.1.1</td>
</tr>
<tr>
<td>What is the identifier of the local data endpoint?</td>
<td>IP address: 10.6.1.1</td>
</tr>
<tr>
<td>What is the identifier of the remote key server?</td>
<td>IP address: 10.196.8.6</td>
</tr>
<tr>
<td>What is the identifier of the remote data endpoint?</td>
<td>IP address: 10.196.8.6</td>
</tr>
<tr>
<td>What ports and protocols do you want to allow to flow through the connection?</td>
<td>Any</td>
</tr>
<tr>
<td>What type of security and system performance do you require to protect your data?</td>
<td>highest</td>
</tr>
<tr>
<td>To which interfaces does the connection apply?</td>
<td>TRLINE</td>
</tr>
</tbody>
</table>

Step 3: Configure VPN on iSeries-A

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

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 should 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 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:
2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface.
3. From the File menu, select New File.
4. From the File menu, select Activate. A dialog opens that allows you to specify whether to activate the rules on a specific interface or on all interfaces. We recommend that you always activate your filter rules on all interfaces.
5. Click OK on the dialog to confirm that you want to verify and activate the rules on the interface or interfaces you specified. When the verification process completes, a message log displays at the
bottom of the window. If the system was able to verify the rules as error free, the system activates them. If there are errors, you must resolve them before you attempt to reactivate the rules.

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:
2. If the VPN server is not started, right-click Virtual Private Networking and select Start. This starts the VPN server.
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 should 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, you should test the connectivity to ensure that the remote hosts can communicate with each other. To do this, follow these steps:
1. In Operations Navigator, expand iSeries-A —>Network.
2. Right-click TCP/IP Configuration and select Utilities and then select Ping.
3. From the Ping from dialog, 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: L2TP voluntary tunnel protected by VPN

Suppose your company has a small branch office in another state. Throughout any given workday the branch office may require access to confidential information on an iSeries 400 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 would like to read more about L2TP concepts, see Layer 2 Tunnel Protocol (L2TP).

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. In fact, you should consider the security risks involved any time you connect to the Internet. Review this redbook, AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00, for a detailed description of various methods for reducing these risks.
Scenario objectives

In this scenario, a branch office iSeries 400 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.

Scenario details

The following figure illustrates the network characteristics for this scenario:

![Network diagram](image)

**iSeries-A**
- Must have access to TCP/IP applications on all systems 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.

Configure the connection

Assuming that TCP/IP configuration already exists and works, you must complete the following tasks:
1. Configure VPN (See 17) on iSeries-A.
2. Configure a PPP (See 19) connection profile and virtual line for iSeries-A.
3. Apply the dynamic-key group to the PPP profile.
4. Configure VPN on iSeries-B.
5. Configure a PPP connection profile and virtual line for iSeries-B.
6. Activate packet rules on iSeries-A and iSeries-B.
7. Start the connection from iSeries-A.

L2TP voluntary tunnel protected by VPN: Configuration details
After you verify that TCP/IP is working properly and your iSeries servers can communicate, you are ready to begin configuring the VPN.

Step 1: Configure VPN on iSeries-A

Follow these steps to configure VPN on iSeries-A:

1. Configure the Internet Key Exchange policy
   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 preshared key to authenticate this policy.
   e. Enter the preshared key in the Key field. Treat your preshared key as you would 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)
   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 to 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.

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:

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 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.
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:

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 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.

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**

OS/400 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:

2. Right-click **Packet Rules** and select **Configuration**. This displays the Packet Rules interface.
3. From the **File** menu, select **New File**.
4. From the **File** menu, select **Activate**. A dialog opens that allows you to specify whether to activate the rules on a specific interface or on all interfaces. We recommend that you activate your rules on all interfaces.
5. Click **OK** on the dialog to confirm that you want to verify and activate the rules on the interface or interfaces you specified. When the verification process completes, a message log displays at the bottom of the window. If the system was able to verify the rules as error free, the system activates them. If there are errors, you must resolve them before you attempt to reactivate the rules.
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:

2. Click **Responder Connection Profiles** to display a list of responder profiles in the right-pane.
3. Right-click to branch 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:

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 protocols and concepts

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

- **IP Security (IPSec) protocols**
  IPSec provides a stable, long lasting base for providing network layer security.

- **Internet Key Exchange (IKE) protocol**
  A dynamic VPN provides additional security for your communications by using IKE. IKE allows the VPN servers on each end of the connection to negotiate new keys at specified intervals.

- **Layer 2 Tunneling Protocol (L2TP)**
  If you plan to use a VPN connection to secure communications between your network and remote clients, you should also be familiar with L2TP.

- **Network address translation for VPN (VPN NAT)**
  OS/400 VPN also supports network address translation (NAT). VPN NAT differs from traditional NAT in that it translates addresses before applying the IKE and IPSec protocols.

- **IP compression (IPComp)**
  IPComp reduces the size of IP datagrams by compressing the datagrams to increase the communication performance between two VPN partners.

**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 implemented throughout the extended network with little or no manual configuration.

OS/400 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 implementation 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 (AH) protocol**
- **Encapsulating Security Payload (ESP) protocol**
- **Combining AH and ESP protocols**
- **Internet Key Exchange (IKE) protocols**

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 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 en route 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 (ESP) 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, on the other hand, 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 implemented. 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, OS/400 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.


### 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 (AH) 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 could 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 VPN uses Data Encryption Standard (DES), triple-DES (3DES), RC5, and RC4 for encryption.

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.


**AH and ESP combined**
OS/400 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.

**Internet Key Exchange protocol**
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 OS/400 VPN key manager is IBM’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 OS/400 VPN key manager uses two distinct phases in its implementation. *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. OS/400 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 upon 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 phone or through registered mail, prior to IKE negotiations. You should treat your preshared key as you would 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 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*, on the other hand, 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 upon 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 OS/400 VPN, you must define an IKE policy to enable phase 1 negotiations and a data policy to govern phase 2 negotiations.

**Suggested reading**

If you want to read more about the Internet Key Exchange (IKE) protocol and key management, you should 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 OS/400 VPN. With a compulsory tunnel, the ISP must support L2TP.

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.

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.

**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 would 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, OS/400 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 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 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?

**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.

**OS/400 VPN setup requirements**

To function properly on iSeries 400 and with network clients, ensure your iSeries and client PC meet the following requirements:

**iSeries requirements**
- OS/400, Version 5 Release 1 (5722-SS1), or later
- Digital Certificate Manager (5722-SS1 Option 34)
- Cryptographic Access Provider (5722-AC2 or AC3)
- Client Access Express (5722-XE1) and OS/400 Operations Navigator
  - Network component of OS/400 Operations 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 32-bit operating system (Windows 95, 98, NT) 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 clients
- Client Access Express and OS/400 Operations 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

**Planning 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 any one of these resources to gather all the information that you need to ensure that your VPN is a success:

- **Determine what type of VPN to create**
  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.

- **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**
  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 implementing your VPN, you can begin configuring it.

**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, on the other hand, 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**
  Complete this worksheet before you configure a dynamic connection.

- **Planning worksheet for manual connections**
  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 do not have 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**.
You should answer each question before you proceed with your VPN setup.

### Prerequisite checklist

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your OS/400 V5R1 (5722-SS1) or later?</td>
<td></td>
</tr>
<tr>
<td>Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?</td>
<td></td>
</tr>
<tr>
<td>Is Cryptographic Access Provider (5722-AC2 or AC3) installed?</td>
<td></td>
</tr>
<tr>
<td>Is Client Access Express (5722-XE1) installed?</td>
<td></td>
</tr>
<tr>
<td>Is OS/400 Operations Navigator installed?</td>
<td></td>
</tr>
<tr>
<td>Is the Network subcomponent of Operations Navigator installed?</td>
<td></td>
</tr>
<tr>
<td>Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?</td>
<td></td>
</tr>
<tr>
<td>Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?</td>
<td></td>
</tr>
<tr>
<td>Is TCP/IP configured on your iSeries 400 (including IP interfaces, routes, local host name, and local domain name)?</td>
<td></td>
</tr>
<tr>
<td>Is normal TCP/IP communication established between the required endpoints?</td>
<td></td>
</tr>
<tr>
<td>Have you applied the latest program temporary fixes (PTFs)?</td>
<td></td>
</tr>
<tr>
<td>If the VPN tunnel traverses firewalls or routers that implement IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?</td>
<td></td>
</tr>
<tr>
<td>Are the firewalls or routers configured to permit IKE (UDP port 500), AH, and ESP protocols?</td>
<td></td>
</tr>
<tr>
<td>Are the firewalls configured to enable IP forwarding?</td>
<td></td>
</tr>
</tbody>
</table>

### You need this information to configure a dynamic VPN connection

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of connection are you creating?</td>
<td></td>
</tr>
<tr>
<td>• Gateway-to-gateway</td>
<td></td>
</tr>
<tr>
<td>• Host-to-gateway</td>
<td></td>
</tr>
<tr>
<td>• Gateway-to-host</td>
<td></td>
</tr>
<tr>
<td>• Host-to-host</td>
<td></td>
</tr>
<tr>
<td>What will you name the dynamic-key group?</td>
<td></td>
</tr>
<tr>
<td>What type of security and system performance do you require to protect your keys?</td>
<td></td>
</tr>
<tr>
<td>• Highest security, lowest performance</td>
<td></td>
</tr>
<tr>
<td>• Balance security and performance</td>
<td></td>
</tr>
<tr>
<td>• Lowest security and highest performance</td>
<td></td>
</tr>
<tr>
<td>Are you using certificates to authenticate the connection?</td>
<td></td>
</tr>
<tr>
<td>If no, what is the preshared key?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the local key server?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the local data endpoint?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the remote key server?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the remote data endpoint?</td>
<td></td>
</tr>
<tr>
<td>What type of security and system performance do you require to protect your data?</td>
<td></td>
</tr>
<tr>
<td>• Highest security, lowest performance</td>
<td></td>
</tr>
<tr>
<td>• Balance security and performance</td>
<td></td>
</tr>
<tr>
<td>• Lowest security and highest performance</td>
<td></td>
</tr>
</tbody>
</table>
Planning worksheet for manual connections

Complete this worksheet to assist you in creating your manual virtual private network (VPN) connection.

You should answer each of these questions before you proceed with your VPN setup:

<table>
<thead>
<tr>
<th>Prerequisite checklist</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is your OS/400 V5R1(5722-SS1) or later?</td>
<td></td>
</tr>
<tr>
<td>Is the Digital Certificate Manager option (5722-SS1 Option 34) installed?</td>
<td></td>
</tr>
<tr>
<td>Is Cryptographic Access Provider (5722-AC2 or AC3) installed?</td>
<td></td>
</tr>
<tr>
<td>Is Client Access Express (5722-XE1) installed?</td>
<td></td>
</tr>
<tr>
<td>Is OS/400 Operations Navigator installed?</td>
<td></td>
</tr>
<tr>
<td>Is the Network subcomponent of Operations Navigator installed?</td>
<td></td>
</tr>
<tr>
<td>Is TCP/IP Connectivity Utilities for OS/400 (5722-TC1) installed?</td>
<td></td>
</tr>
<tr>
<td>Did you set the retain server security data (QRETSVRSEC *SEC) system value to 1?</td>
<td></td>
</tr>
<tr>
<td>Is TCP/IP configured on your iSeries 400 (including IP interfaces, routes, local host name, and local domain name)?</td>
<td></td>
</tr>
<tr>
<td>Is normal TCP/IP communication established between the required endpoints?</td>
<td></td>
</tr>
<tr>
<td>Have you applied the latest program temporary fixes (PTFs)?</td>
<td></td>
</tr>
<tr>
<td>If the VPN tunnel traverses firewalls or routers that implement IP packet filtering, do the firewall or router filter rules support AH and ESP protocols?</td>
<td></td>
</tr>
<tr>
<td>Are the firewalls or routers configured to permit the AH and ESP protocols?</td>
<td></td>
</tr>
<tr>
<td>Are the firewalls configured to enable IP forwarding?</td>
<td></td>
</tr>
</tbody>
</table>

You need this information to configure a manual VPN

<table>
<thead>
<tr>
<th>You need this information to configure a manual VPN</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of connection are you creating?</td>
<td></td>
</tr>
<tr>
<td>• Host-to-host</td>
<td></td>
</tr>
<tr>
<td>• Host-to-gateway</td>
<td></td>
</tr>
<tr>
<td>• Gateway-to-host</td>
<td></td>
</tr>
<tr>
<td>• Gateway-to-gateway</td>
<td></td>
</tr>
<tr>
<td>What will you name the connection?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the local connection endpoint?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the remote connection endpoint?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the local data endpoint?</td>
<td></td>
</tr>
<tr>
<td>What is the identifier of the remote data endpoint?</td>
<td></td>
</tr>
<tr>
<td>What type of traffic will you allow for this connection (local port, remote port, and protocol)?</td>
<td></td>
</tr>
<tr>
<td>Do you require address translation for this connection? See Network address translation for VPN for more information.</td>
<td></td>
</tr>
<tr>
<td>Will you use tunnel mode or transport mode?</td>
<td></td>
</tr>
<tr>
<td>Which IPSec protocol will the connection use (AH, ESP, or AH with ESP)? See IP Security (IPSec) for more information.</td>
<td></td>
</tr>
<tr>
<td>Which authentication algorithm will the connection use (HMAC-MD5 or HMAC-SHA)?</td>
<td></td>
</tr>
<tr>
<td>Which encryption algorithm will the connection use (DES-CBC or 3DES-CBC)?</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** You specify an encryption algorithm only if you selected ESP as your IPSec protocol.
### Configuring VPN

The OS/400 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 (See 33)** connection, on the other hand, is one where you must configure all of your VPN properties by hand. 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?**

A VPN is actually a group of configuration objects that define the characteristics of a connection. A dynamic VPN connection requires each of the following objects to work properly. Follow the links below for specific information on how to configure them:

<table>
<thead>
<tr>
<th>You need this information to configure a manual VPN</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
Configure connections with the Connection wizard

In general, you should use the Connection wizard to create all of your dynamic connections. The wizard automatically creates each of the configuration objects OS/400 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**
   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 secure connections**
   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 OS/400 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 packet rules**
   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** rule permits 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.

   In general, you will only need to configure packet rules for your VPN when you are migrating from a prior release and have packet rules that you wish to continue using. If this is the case, you should review the topic, Before you begin configuring VPN packet rules.

4. **Define an interface for the rules**
   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 packet rules**
   After you define an interface for your packet rules, you must activate them before you can start the connection.

6. **Start the connection**
   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 on how to configure a manual connection:

1. **Configure manual connections**
   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 OS/400 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 policy filter rule
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 rules
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 packet rules
After you define an interface for your packet rules, you must activate them before you can start the connection.

5. Start the connection
Complete this task to start connections that are initiated locally.

Configuring connections with the VPN Connection wizard

The VPN 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 OS/400 VPN requires to work properly, including the packet rules. However, if you need to add function to your VPN; for example, journaling or address translation, 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 important information that you will need to create your VPN.

To create a VPN with the Connection wizard, follow these steps:
2. Right-click Virtual Private Networking and select New Connection to start the Connection wizard.
3. Complete the wizard to create a basic VPN connection. Click Help if you need assistance.

Configuring 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 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 secure connections.

### Configuring an Internet Key Exchange (IKE) policy

An IKE policy defines what level of authentication or 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. OS/400 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:

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.

### Configuring 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.

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

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.

### Configuring 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 should 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:**

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:**

2. In the left-pane of the Operations 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 packet rules that the connection requires to work properly.

**Note:** In most cases, you should allow the OS/400 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 by hand and then activate them.

**Configuring 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:

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, you should allow the OS/400 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 by hand and then activate them.

Configuring VPN packet rules

If you are creating a connection for the first time, you should allow OS/400 VPN to automatically generate the VPN packet rules for you. You can do this by either using the Connection wizard or the OS/400 VPN properties pages to configure your connection.

If you decide to create your packet rules by hand, you should create any additional rules by hand as well. Conversely, if you have OS/400 VPN generate your policy filter rules, you should create all additional policy filter rules this way. Review, “Before you begin configuring VPN packet rules,” for more details.

Follow the links below to learn how to configure the VPN packet rules by hand:

Packet rules required for dynamic connections

- **Pre-IPSec rule**
  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 OS/400 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.

- **Policy filter rule**
  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 fail 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 the interface to which they apply, and then activate 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 400. This includes your connection to Operations Navigator, which you use to configure the filter rules.

If the filter rules do not permit Operations Navigator traffic, Operations Navigator cannot communicate with your iSeries 400. If you find yourself in this situation, you will have to log on to your iSeries using an interface that still has connectivity, such as the operations console. Use the RMVTCPTBL TBL(*ALL) command to remove all filters on this system. This command also ends the *VPN servers and then restarts them. Then, configure your filters and reactivates them.

Before you begin configuring VPN packet rules

In prior releases of the operating system, you had to configure the VPN packet rules, by hand, as a separate step. They were not generated automatically as part of your VPN configurations. In V5R1, OS/400 VPN can now create these packet rules automatically. However, 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 in V5R1. Or, perhaps OS/400 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 interface. Contrast this with the OPNAV rules file, which is the rules file that OS/400 VPN automatically generates as part of V5R1 VPN configurations.

- If you have VPN connections from either V4R4 or V4R5 and do not plan to configure other VPN connections in V5R1, you can activate your filter rules and start the connections, as usual.
- If OS/400 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 interface. If any of these non-VPN filter rules need to come before the OPNAV filters, then their set names must begin with PREIPSEC. For example, PREIPSEC_MYRULES. The set names of all other non-VPN rules should not have the PREIPSEC prefix. For example, MORERULES.
- Whenever possible, allow the VPN interface to create all of your policy filter rules. If your customer rules file is relatively simple, you should consider reconfiguring all of your pre-V5R1 policy filters by using the VPN interface. You can do this by removing the appropriate filter definitions from your customer rules file, and selecting the Generate the following policy filter for this group option on the Dynamic-Key Group - Connections page in the VPN interface. 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 OPNAV rules file, you will need to add PREIPSEC to the front of the set name. This ensures that your customer rules and the OPNAV work together as you intend.
- If you plan to use the policy filter rules you created by hand, create all subsequent policy filter rules by hand. Conversely, if you plan to allow the VPN interface to create the policy filter rules for you, all of your subsequent policy filter rules should be created this way.
- When you want to activate only the OPNAV rules, follow these steps:
  2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface.
  3. From the File menu, select New File.
  4. From the File menu, select Activate.
- When you want to activate both the customer rules file and the OPNAV rule file, follow these steps:
  2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface.
  3. Open the rules file that you want to activate.
  4. From the File menu select Activate.

This merges the customer rules files with OPNAV rule file in a specific order for each FILTER_INTERFACE statement. For a given interface the merging order is as follows:

1. Customer sets whose names begin with PREIPSEC
2. OPNAV sets whose name begins with PREIPSEC. In V5R1, PREIPSEC_PERMITALLLIKE is the only pre-IPSec set in the OPNAV rule.
3. OPNAV sets with ACTION=IPSEC (policy filters)
4. Customer sets with ACTION=IPSEC (policy filters)
5. Customer sets with anything else.
6. OPNAV sets with anything else. In V5R1, OPNAV_PERMIT_NONVPN is the only one of this type.

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.

- If you only want to activate your customer rules files, then you must make sure that no OPNAV filters exist. You can do this by selecting the The policy filter will be defined in Packet Rules option on the Dynamic-Key Group - Connections page for each dynamic-key group or the Manual Connection - Connection page for your manual connections.
• 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.

• You should always verify your filter rules before you attempt to activate them. If the verify runs without errors, you should then check EXPANDED.OUT to ensure the rules are ordered as you intend. After you complete this step, then you can activate the rules.

Configuring the pre-IPSec filter rule

Attention: You should only complete this task if you have specified that you do not want OS/400 VPN to generate your pre-IPSec IKE filters 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:

2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface, which allows you to create or edit filter and NAT rules for your iSeries 400.
3. From the File menu, select New File.
4. Right-click Filters and select New Filter.
5. On the General page, specify a set name for your VPN filter rules. We recommend 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. The set that contains your pre-IPSec filter rules must have 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.

Configuring a policy filter rule

Attention: You should only complete this task if you have specified that you do not want OS/400 VPN to generate your policy filter rule automatically.
The IPSEC policy filter rule 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 interface should still be open; go to step four.

2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface, which allows you to create or edit filter and NAT rules for your iSeries 400.
3. From the File menu, select New File.
4. Right-click Filters and select New Filter.
5. On the General page, specify a set name for your VPN filter rules. We recommend 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 the interface 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.

### Defining 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 an interface to which to apply them.

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 should still be open; go to step four.

2. Right-click Packet Rules and select Configuration. This displays the Packet Rules interface, which allows you to create or edit filter and NAT rules for your iSeries 400.
3. From the File menu, select New File.
4. Right-click **Filter Interfaces** and select **New 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/TCP/IP/RULEGEN`

   This directory is for system use only. If you ever need to use the `RMVTCPBL *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 them before you can start the VPN.

### Activating the VPN packet rules

You must activate the VPN packet rules before you can start your VPN connection. You cannot activate a rule set unless you have the rule file open. Further, you cannot activate (or deactivate) filter rules when VPN connections are running. So, before you activate your VPN filter rules, ensure that there are no active connections associated with them. How you created the packet rules determines how you activate them:

**Activate packet rules generated by OS/400 VPN**

1. In Operations Navigator, expand your server —> **Network** —> **IP Policies**.
2. Right-click **Packet Rules** and select **Configuration**. This displays the Packet Rules interface.
3. From the **File** menu, select **New File**.
4. From the **File** menu, select **Activate**. A dialog opens that allows you to specify whether to activate the rules on a specific interface or on all interfaces. It is recommended that you always activate your packet rules on all interfaces.
5. Click **OK** on the dialog to confirm that you want to verify and activate the rules on the interface or interfaces you specified. When the verification process completes, a message log displays at the bottom of the window. If the system was able to verify the rules as error free, the system activates them. If there are errors, you must resolve them before you attempt to reactivate the rules.

**Activate packet rules configured by hand**

1. In Operations Navigator, expand your server —> **Network** —> **IP Policies**.
2. Right-click **Packet Rules** and select **Configuration**. This displays the Packet Rules interface.
3. Open the rules file that you want to activate.
4. From the **File** menu select **Activate**. A dialog opens that allows you to specify whether to activate the rules on a specific interface or on all interfaces. It is recommended that you always activate your packet rules on all interfaces.
5. Click **OK** on the dialog to confirm that you want to verify and activate the rules on the interface or interfaces you specified. When the verification process completes, a message log displays at the bottom of the window. If the system was able to verify the rules as error free, the system activates them. If there are errors, you must resolve them before you attempt to reactivate the rules.

After you activate your filter rules, you can start your VPN connection.

### Starting a VPN connection

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

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 activated.


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.

Managing OS/400 VPN with Operations Navigator

Use the OS/400 VPN interface to handle all of your management tasks, including:

• Starting a VPN connection
  Complete this task to start connections you will initiate locally.

• Setting 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.

• Resetting connections in error state
  Resetting connections in error returns them to the idle state.

• Viewing error information
  Complete this task to help you determine why your connection is in error.

• Viewing the attributes of active connections
  Complete this task to check the status and other attributes of your active connections.

• Using the VPN server trace
  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 green screen except that you can view the trace while a connection is active.

• Viewing the VPN server job logs
  Follow these instructions to view the job logs for the VPN Key Manager and the VPN Connection Manager.

• Stopping connections
  Complete this task to stop active connections.

• Viewing the attributes of Security Associations (SA)
  Complete this task to display the attributes of the Security Associations (SAs) that are associated with an enabled connection.

• Deleting VPN configuration objects
  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.

Setting 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:


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.

Resetting connections in error state

To refresh a connection that is in the error state, follow these steps:
1. In Operations 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**.

**Viewing error information**
To view information about connections in error, follow these steps:
1. In Operations 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**.

**Viewing the attributes of active connections**
To view the current attributes of an active or on-demand connection, follow these steps:
1. In Operations 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 Operations 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 Operations 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 which allows you to select which attributes you want to display in the Operations 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.

**Using the VPN server trace**
To view the VPN server trace, follow these steps:
1. In Operations 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.

**Viewing 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 Operations 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.

**Stopping a VPN connection**

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

1. In Operations 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**.

**Viewing 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 Operations 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.

**Deleting 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 Operations 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**.

**Troubleshooting OS/400 VPN**

VPN is a complex and rapidly changing technology that requires at least a basic knowledge of standard IPSec technologies. You should also be familiar with IP packet rules because OS/400 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 OS/400 VPN:

- **Getting started with OS/400 VPN troubleshooting**
  Go here to begin finding and correcting your VPN connection problems.

- **Common OS/400 VPN configuration errors and how to fix them**
  This topic identifies the most common user errors and provides possible resolutions.
Getting started with troubleshooting OS/400 VPN

There are several ways to begin analyzing OS/400 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.
3. Review any error messages that are found in the Error Information window or in the VPN server job logs 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 IP filter journal.
5. The communication trace on the iSeries 400 offers you 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 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 Internet 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 Operations Navigator. Ensure that the filter rules do not specify Network Address Translation (NAT) for any VPN traffic.

3. Start your VPN connection. 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 desired. 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 desired user traffic.

Common OS/400 VPN configuration errors and how to fix them

This section describes some of the more common problems that occur with OS/400 VPN, and links you to tips on how to resolve them.

Note: When you configure OS/400 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

<table>
<thead>
<tr>
<th>Message</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP5B28</td>
<td>When you attempt to activate filter rules on an interface, you get this message: TCP5B28 CONNECTION_DEFINITION order violation</td>
</tr>
<tr>
<td>Item not found</td>
<td>When you right-click a VPN object and select either Properties or Delete, you get a message that says, Item not found.</td>
</tr>
<tr>
<td>PARAMETER PINBUF IS NOT VALID</td>
<td>When you attempt to start a connection, you get a message that says, PARAMETER PINBUF IS NOT VALID...</td>
</tr>
<tr>
<td>Item not found, Remote key server...</td>
<td>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.</td>
</tr>
<tr>
<td>Unable to update the object</td>
<td>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.</td>
</tr>
<tr>
<td>Unable to encrypt key...</td>
<td>You get a message that says that the system cannot encrypt your keys because the QRETSVRSEC value must be set to 1.</td>
</tr>
<tr>
<td>CPF9821</td>
<td>When you try to expand or open the IP Policies container in Operations Navigator, the CPF9821- Not authorized to program QTFRPRS in QSYS library message appears.</td>
</tr>
</tbody>
</table>

Other problems you may run into
<table>
<thead>
<tr>
<th>Error</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>All keys are blank</td>
<td>When you view the properties of a manual connection, all preshared keys and the algorithm keys for the connection are blank.</td>
</tr>
<tr>
<td>Sign-on for a different system appears</td>
<td>The first time you use the Packet Rules interface in Operations Navigator, a sign-on display appears for a system other than the current one.</td>
</tr>
<tr>
<td>No connection status</td>
<td>A connection has no value in the <strong>Status</strong> column in the Operations Navigator window.</td>
</tr>
<tr>
<td>Stopped connections still enabled</td>
<td>After you stop a connection, the Operations Navigator window indicates that the connection is still enabled.</td>
</tr>
<tr>
<td>3DES not a choice for encryption</td>
<td>When you are working with an IKE policy transform, data policy transform, or a manual connection, the 3DES encryption algorithm is not a choice.</td>
</tr>
<tr>
<td>Unexpected columns display</td>
<td>You set up the columns you want to display in the Operations Navigator window for your VPN connections; then, when you look at it later, different columns display.</td>
</tr>
<tr>
<td>Active filter rules fail to deactivate</td>
<td>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.</td>
</tr>
<tr>
<td>The dynamic-key group for a connection changes</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 400. 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 should 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 Operations 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. You should now have access to the Packet Rules functions in Operations 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 Error message: Unable to encrypt keys 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 Client Access Express to obtain the appropriate conversion table for unicode. This should only occur once.

VPN error: Blank connection status in Operations Navigator window
Symptom:
A connection has no value in the Status column in the Operations 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 should 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 Operations Navigator window indicates that the connection is still enabled.

Possible resolution:
This typically happens because you have not refreshed the Operations 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 Operations Navigator window
Symptom:
You set up the columns you want to display in the Operations 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 should now be able to 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 OS/400 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 OS/400 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 desired dynamic-key group to the top of the table in the right pane. This ensures that OS/400 VPN checks this dynamic-key group first for the remote key server.
Troubleshooting OS/400 VPN with the QIPFILTER journal

The QIPFILTER journal is located in the QUSR SY S 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 interface in Operations Navigator to activate the QIPFILTER journal. You have to 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:

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 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 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) JRNCD(M) ENTTYP((TF)) OUTPUT(*OUTFILE)
OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTTLEN(*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 QUSR SYS/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 proper 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 setup 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:

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

54 iSeries: Virtual private networking
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFREVT</td>
<td>2</td>
<td>N</td>
<td>Rule event</td>
</tr>
<tr>
<td>TFPDIR</td>
<td>1</td>
<td>N</td>
<td>IP Packet direction</td>
</tr>
<tr>
<td>TFRNUM</td>
<td>5</td>
<td>N</td>
<td>Rule number</td>
</tr>
<tr>
<td>TFACT</td>
<td>6</td>
<td>N</td>
<td>Filter action taken</td>
</tr>
<tr>
<td>TFPROT</td>
<td>4</td>
<td>N</td>
<td>Transport protocol</td>
</tr>
<tr>
<td>TFSRCA</td>
<td>15</td>
<td>N</td>
<td>Source IP address</td>
</tr>
<tr>
<td>TFSRCP</td>
<td>5</td>
<td>N</td>
<td>Source port</td>
</tr>
<tr>
<td>TFDSTA</td>
<td>15</td>
<td>N</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>TFDSTP</td>
<td>5</td>
<td>N</td>
<td>Destination port</td>
</tr>
<tr>
<td>TTEXT</td>
<td>76</td>
<td>N</td>
<td>Additional text</td>
</tr>
</tbody>
</table>

**Troubleshooting OS/400 VPN with the QVPN journal**

OS/400 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 option of OS/400 Operations Navigator to activate the VPN journal. There is no function that allows logging for all VPN connections. Therefore, you have to 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:

2. For dynamic-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) OUTFILM1(*TYPE4)
   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 proper 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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Length</th>
<th>Numeric</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSENL</td>
<td>5</td>
<td>Y</td>
<td>Length of entry</td>
<td></td>
</tr>
<tr>
<td>TSSEQN</td>
<td>10</td>
<td>Y</td>
<td>Sequence number</td>
<td></td>
</tr>
<tr>
<td>TSCODE</td>
<td>1</td>
<td>N</td>
<td>Journal code</td>
<td>Always M</td>
</tr>
<tr>
<td>TSENTT</td>
<td>2</td>
<td>N</td>
<td>Entry type</td>
<td>Always TS</td>
</tr>
<tr>
<td>TSTIME</td>
<td>26</td>
<td>N</td>
<td>SAA entry timestamp</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting OS/400 VPN 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 400 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 QTOKVPNIE, run in the subsystem QSYSWRK. You can view their respective job logs from OS/400 Operations 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.

**QTOKVPNIE**
The QTOKVPNIE 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 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 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 Operations 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

<table>
<thead>
<tr>
<th>Message</th>
<th>Cause</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 job logs for additional messages.
2. Correct the errors and try the request again.
3. Use Operations Navigator to view the connection status. 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 job logs for additional messages.
2. Correct the errors and try the request again.
3. Use Operations Navigator to view the connection status. 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 name 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 VPN 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 inconsistent with information from the connection group.
9 - Identifier type not valid.

1. Check the job logs for additional messages.
2. Correct the errors and try the request again.
3. Use Operations Navigator to check or correct the VPN policy configuration. Ensure that the dynamic-key group associated with this connection has acceptable values configured.
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 job logs 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 STRTCPSSRV SERVER(*VPN) command.
   **Note:** This causes all current 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 job logs for additional messages.
2. Correct the errors and try the request again.
3. Use Operations 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 job logs for additional messages.
2. Correct the errors and try the request again.
3. Use Operations Navigator to check or correct the VPN policy. Ensure that the dynamic-key group associated with this connection has acceptable values for addresses configured.

TCP8620
Local connection endpoint not available

Could not enable this VPN connections because the local connection endpoint was not available.

1. Check the job logs 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 job logs 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 job logs for additional messages pertaining to this connection.
2. Use Operations 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 job logs for additional messages pertaining to this connection.
2. Use Operations 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.

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 job logs for additional messages pertaining to this connection.
2. Use Operations 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 job logs for additional messages pertaining to this connection.
2. Use Operations 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 job logs for additional messages pertaining to this connection.
2. Use Operations 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.

TCP8628
Policy filter rule not loaded

The policy filter rule for this connection is not active.

1. Check the job logs for additional messages pertaining to this connection.
2. Use Operations 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 job logs for additional messages pertaining to this connection.
2. Use Operations 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 job logs 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.
Troubleshooting OS/400 VPN with the OS/400 Communications trace

iSeries 400 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 usually 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, you should 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) TCPIPADDR('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.

- **TCPIPADDR** (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.
Other VPN information

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

- **Remote Access to AS/400 with Windows 2000 VPN clients, REDP0036**
  This redpaper describes how to implement secure connections for traveling employees and virtual office employees that need access to the corporate office. The remote users access the corporate office AS/400 system using a PC with Windows 2000. The connection is secured by a VPN (L2TP tunnel protected by IPSec).

- **AS/400 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 native network security features available on the AS/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.

- **Set Up a VPN (Virtual Private Network) to Securely Manage Your AS/400 Across the Internet**
  In this Technical Studio topic, you'll set up a virtual private network (VPN) that uses IP Security (IPSec) protocol and Layer 2 Tunneling Protocol (L2TP) to protect and conceal sensitive information from hackers and thieves who prowl the Internet.

- **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.