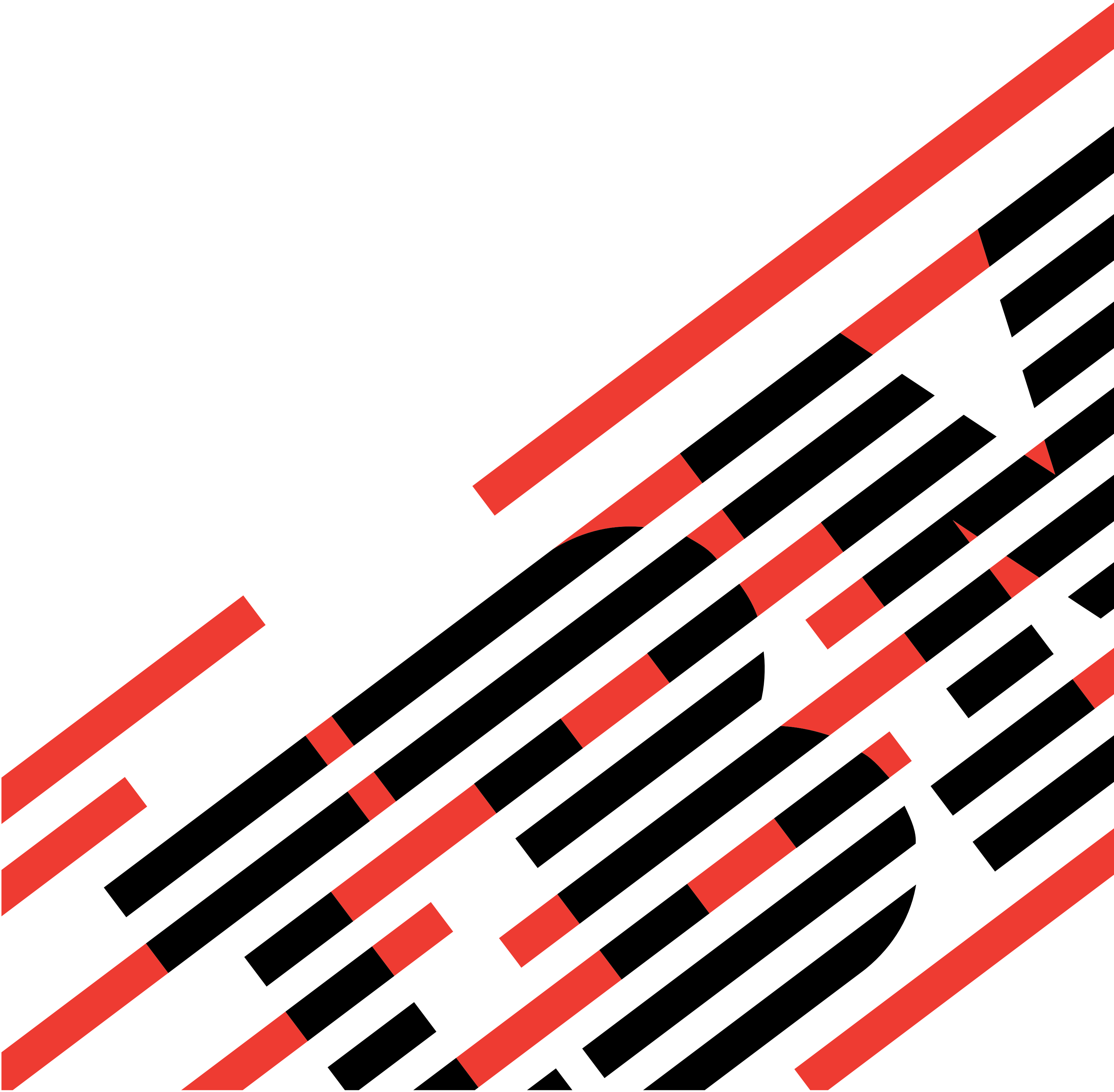
iSeries

IBM SecureWay: iSeries 400 and the Internet



iSeries

IBM SecureWay: iSeries 400 and the Internet

Contents

Part 1. IBM SecureWay: iSeries® and the Internet 1

Chapter 1. What's new for V5R1 3

Chapter 2. Print this topic 5

Chapter 3. iSeries 400 and Internet security 7

Chapter 4. Planning Internet security . . 9
The layered defense approach to security 10
Security policy and objectives 12
Scenario: JKL Toy Company e-business plans . . . 14

Chapter 5. Security levels for basic Internet readiness 17

Chapter 6. Network security options . . 19
Firewalls 20
iSeries Packet rules 22
Choosing iSeries network security options 23

Chapter 7. Application security options 25
Web serving security 25
Java Internet security 26
E-mail security 29
FTP security 30

Chapter 8. Transmission security options 33
Using digital certificates for SSL 34
SSL for secure Telnet access 35
SSL for secure Client Access Express 36
Virtual Private Networks (VPN) for secure private communications 36

Chapter 9. Internet security terminology 39

Part 1. IBM SecureWay: iSeries® and the Internet

Accessing the Internet from your LAN is a major step in the evolution of your network that will require you to reassess your security requirements. Fortunately, your iSeries 400 has integrated software solutions and security architecture to let you build a strong defense against potential Internet security pitfalls and intruders. Properly using these iSeries security offerings ensures that your customers, employees, and business partners can obtain the information they need to do business with you in a secure environment.

You can use the information that you find here to educate yourself about well-known security threats and how these risks relate to your Internet and e-business goals. Also, you will learn how to assess the risks versus the benefits of using the various security options that iSeries provides for dealing with these risks. And finally, you can determine how you can use this information to develop a network security plan that fits your business needs. you can ensure that your security policy

To learn more about Internet security risks and iSeries security solutions that you can use to protect your systems and resources, review this information:

- **What's new for V5R1**
  Use this information to learn about changes and additions to iSeries Internet security offerings for V5R1.
- **Print this topic**
  Use this information to access and print an Adobe Acrobat version of this topic.
- **iSeries and Internet security**
  Use this information to gain a general understanding of the strengths of iSeries security for e-business and the iSeries security offerings available to you.
- **Planning Internet security**
  Use this information to learn about how to create a security policy that covers your Internet and e-business security needs
- **iSeries system security levels for basic Internet readiness**
  Use this information to learn what system security you should have in place before you connect to the Internet.
- **Network security options**
  Use this information to learn about the network level security measures that you should consider using to protect your internal resources.
- **Application security options**
  Use this information to learn about common Internet security risks for a number of popular Internet applications and services and measures that you can take to manage these risks .
- **Transmission security options**
  Use this information to learn about the security measures that you can implement to protect your data as it flows across an untrusted network, such as the Internet. Learn more about security measures for using the Secure Sockets Layer (SSL), Client Access Express, and Virtual Private Network (VPN) connections.
- **iSeries Internet security options**
  Use this concise discussion on iSeries security options to help you choose the offerings to protect your systems and resources based on your Internet usage and e-business plans.

Note: If you are unfamiliar with security and Internet-related terms, you can review common security terminology as you work through this material.

Chapter 1. What’s new for V5R1

For V5R1, there are a number of improvements and additions to security offerings for your iSeries 400. The following list describes some of the more important functional security enhancements:

- **Digital Certificate Manager (DCM) enhancements**
  You can now use DCM to create and manage certificates that you can use to digitally sign objects to ensure their integrity and provide proof of origination for objects. You can also create and manage the corresponding signature verification certificates that you or others can use to authenticate the signature on a signed object to ensure that the data in the object is unchanged to verify proof of the object’s origination. You can also use DCM, or the appropriate APIs to sign an object and verify the signature on a object.
- **Digitally Signed Operating System**
  Starting with V5R1, OS/400 and IBM LPPs will be digitally signed by IBM. Users can verify that programs from IBM have not been altered since they were signed by IBM. Digital signature verification can be performed at restore time or by running the CHKOBJITG command. APIs are also available to allow customers and business partners to digitally sign and verify their applications.
- **New user profile password rules (QPWDLVL 2 and 3)**
  The user profile password length has been increased to allow from 1 to 128 characters. Passwords are case sensitive and, allow embedded blanks; for example ″This is my New Password.″ Trailing blanks are removed and a password cannot be all blanks.
- **User profile password enhancements**
  You can use the new system value QPWDLVL to set one of 4 options to control the password level of the system:
  - PWDLVL 0 — This setting allows passwords with a 10 byte length, and allows Netserver passwords to be retained. This is the default setting.
  - PWDLVL 1 — This setting allows passwords with a 10 byte length and eliminates Netserver passwords.
  - PWDLVL 2 — This setting allows passwords with a 128 character length, and retains passwords that conform to both the old and to the new password formats.
  - PWDLVL 3 — This setting allows passwords with a 128 character length, and removes old password formats.
- **IBM 4758–023 PCI Cryptographic Coprocessor support for more secure key storage**
  If your system has a IBM 4758–023 PCI Cryptographic Coprocessor installed, you can use it to store your digital certificate keys more securely. When you use DCM to create or renew certificates, you can choose to store the key directly in the coprocessor or to use the coprocessor master key to encrypt the private key and store it in a special keystore file. Also, when you use the coprocessor for key storage, you can improve Secure Sockets Layer (SSL) performance for your SSL-enabled applications. Because the coprocessor handles the task of decrypting the private key to present for the SSL handshake. You can also perform load balancing of SSL handshake processing across multiple 4758 cards.
- **Virtual private networking (VPN) certificate support**
  Prior to V5R1, the VPN Internet Key Exchange (IKE) servers could authenticate each other only through the use of a pre-shared key. Using a pre-shared key is less secure because you must communicate this key manually to the

administrator of the other endpoint for your VPN. Consequently, there is a possibility that the key could be exposed to others during the process of communicating the key. In V5R1 you can avoid this risk by using digital certificates to authenticate the endpoints instead of using a pre-shared key. You can use Digital Certificate Manager (DCM) to manage the certificates that your IKE server uses for establishing a dynamic VPN connection.

- **Secure Sockets Layer (SSL)-enabled application improvements**
  There are a number of SSL enhancements for V5R1. You can now configure your iSeries File Transfer Protocol (FTP) server to use SSL for secure communications sessions. You can also configure the FTP server to use digital certificates for client authentication. Additionally, OS/400 provides support for the 128-bit AES cipher in V5R1. AES is a new, faster, encryption algorithm that replaces the DES algorithm.
- **Simple Mail Transfer Protocol (SMTP) enhancements**
  SMTP now provides blacklist support based on Subject, Sender, and IP address.
- **Internet Setup Wizard**
  The popular Internet setup wizard available last release as a downloadable file is now available directly within Operations Navigator. You can use this wizard to configure an Internet connection for your iSeries system and secure it with automatically generated filter rules.
- **Program creation data retention enhancements**
  Programs that are created for V5R1 or later iSeries systems contain information that allows the program to be re-created at restore time, if necessary. The information needed to re-create the program remains with the program even when the observability of the program is removed. If a program validation error is determined to exist at the time the program is restored, the program will be re-created in order to correct the program validation error. The action of re-creating the program at restore time is not new to V5R1 iSeries. In previous releases, any program validation error that was encountered at restore time resulted in the program being re-created if possible (if observability existed in the program being restored). The difference with V5R1 iSeries or later programs is that the information needed to re-create the program remains, even when observability was removed from the program. Thus, any V5R1 or later program for which a validation failure is detected is re-created during restore and the alteration that caused the validation failure is removed.

Chapter 2. 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 the Adobe home page.

To view or download the PDF version, select IBM SecureWay: iSeries and the Internet (416 KB or 60 pages).

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**.

Chapter 3. iSeries 400 and Internet security

As an iSeries 400 owner exploring options for connecting your systems to the Internet, one of the first questions you will usually ask is, ″How do I begin to use the Internet for business purposes?″ The second question is, ″What should I know about security and the Internet?″ The focus of this material is to help you to answer this second question.

The answer to the question, ″What should I know about security and the Internet?″, is that it depends on how you want to use the Internet. Security issues related to the Internet are significant. Which issues you need to address are based on how you plan to use the Internet. Your first venture into the Internet might be to provide your internal network users with access to the web and Internet e-mail. You may also want the ability to transfer sensitive information from one site to another. Eventually, you may plan to use the Internet for e-commerce or to create an extranet between your company and your business partners and suppliers.

Before you get involved with the Internet, you should think through what you want to do and how you want to do it. Making decisions about both Internet usage and Internet security can be complex. You may find it helpful to review the page, Scenario: JKL Toy Company e-business plans, as you develop your own Internet usage plan. (Note: If you are unfamiliar with security and Internet-related terms, you can review common security terminology as you work through this material.)

Once you understand how you want to use the Internet for e-business, as well as the security issues and the available security tools, functions, and offerings, you can develop a security policy and objectives. A number of factors will affect the choices that you make in developing your security policy. When you extend your organization onto the Internet, your security policy is the critical cornerstone for ensuring that your systems and resources are secure.

iSeries 400 system security characteristics

In addition to a number of specific security offerings for protecting your system on the Internet, iSeries 400 has very strong system security characteristics, such as the following:

- Integrated security which is extremely difficult to circumvent compared to add-on security software packages offered on other systems.
- Object-based architecture which makes it technically difficult to create and spread a virus. On an iSeries, a file cannot pretend to be a program, nor can a program change another program. iSeries integrity features require you to use system-provided interfaces to access objects. You cannot access an object directly by its address in the system. You cannot take an offset and turn it into, or ″manufacture,″ a pointer. Pointer manipulation is a popular technique for hackers on other system architectures.
- Flexibility which lets you set up your system security to meet your specific requirements. You can use the Technical Studio Security Advisor, to help you determine which security recommendations fit your security needs.

iSeries advanced security offerings

iSeries also offers several specific security offerings that you can use to enhance your system security when you connect to the Internet. Depending on how you use the Internet, you may want to take advantage of one or more of these offerings:

- Virtual Private Networks (VPNs) are an extension of an enterprise's private intranet across a public network, such as the Internet. You can use a VPN to create a secure private connection, essentially by creating a private ″tunnel″ over a public network. VPN is an integrated feature of OS/400 available from the Operations Navigator interface.
- Packet rules is an integrated feature of OS/400 available from the Operations Navigator interface. This feature allows you to configure IP packet filter and network address translation (NAT) rules to control the flow of TCP/IP traffic into and out of your iSeries system.
- Secure Sockets Layer (SSL) application communications security allows you to configure applications to use SSL to establish secure connections between server applications and their clients. SSL was originally developed for secure web browser and server applications, but other applications can be enabled to use it. Many iSeries server applications are now enabled for SSL, including the IBM HTTP Server for iSeries, Client Access Express, File Transfer Protocol (FTP), Telnet, and many others.

Once you understand how you want to use the Internet, as well as the security issues and the available security tools, functions, and offerings, you are ready to develop a security policy and objectives. A number of factors will affect the choices that you make in developing your security policy. When you extend your organization onto the Internet, a security policy provides a critical cornerstone for making your system secure.

Note: To find more detailed information on how to begin using the Internet for business purposes, review these online Information Center topics and IBM redbooks:

- *Connecting to the Internet*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929).

Chapter 4. Planning Internet security

As you develop your Internet usage plans, you must carefully plan for your Internet security needs. You must gather detailed information about your Internet usage plans and document your internal network configuration. Based on the results of gathering this information, you can accurately evaluate your security needs.

For instance, you should document and describe such things as the following:
- Your current network configuration.
- DNS and e-mail server configuration information.
- Your connection to your Internet Service Provider (ISP).
- What services you want to use from the Internet.
- What services you want to provide to Internet users.

Documenting this type of information helps you determine where your security exposures are and what security measures you need to use to minimize these exposures.

For example, you decide that you want to allow your internal users to use Telnet to connect to hosts at a special research location. Your internal users need this service to help them develop new products for your company. However, you have some concerns about confidential data flowing unprotected across the Internet. If competitors capture and exploit this data, your company could face a financial risk. Having identified your usage needs (Telnet) and the associated risks (exposure of confidential information), you can determine what additional security measures you should implement to ensure data confidentiality for this usage (Secure Sockets Layer (SSL) enablement).

As you develop your Internet usage and security plans, you may find it helpful to review these topics:
- **The layered defense approach to security** provides information about the issues involved in creating a comprehensive security plan.
- **Security policy and objectives** provides information to help you better understand the issues involved in creating a comprehensive security plan.
- **Scenario: JKL Toy Company e-business plans** provides a practical model of a typical company Internet usage and security plans that you can use as you create your own.

Although, the product has been discontinued, you may still find it helpful to adapt and use the IBM Firewall for AS/400 planning worksheets to document your plans. These worksheets can help you gather important, detailed information about your Internet usage plans and internal network configuration, as well as help you evaluate your security needs. You can access these worksheets from the Firewall: Getting started topic in the V4R5 iSeries Information Center. Whether you decide to use a firewall product or not, you need to gather much of the same data for planning your Internet security strategy.

The layered defense approach to security

Your **security policy** defines what you want to protect and what you expect of your system users. It provides a basis for security planning when you design new applications or expand your current network. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords.

Note: You need to create and enact a security policy for your organization that minimizes the risks to your internal network. The inherent security features of iSeries 400, when properly configured, provide you with the ability to minimize many risks. When you connect your iSeries system to the Internet, however, you need to provide additional security measures to ensure the safety of your internal network.

Many risks are associated with using Internet access to conduct business activities. Whenever you create a security policy, you must balance providing services against controlling access to functions and data. With networking computers, security is more difficult because the communication channel itself is open to attack.

Some Internet services are more vulnerable to certain types of attacks than others. Therefore, it is critical that you understand the risks that are imposed by each service you intend to use or provide. In addition, understanding possible security risks helps you to determine a clear set of security objectives.

The Internet is home to a variety of individuals who a pose threat to the security of Internet communications. The following list describes some of the typical security risks you may encounter:

- **Passive attacks**: In a passive attack, the perpetrator simply monitors your network traffic to try to learn secrets. Such attacks can be either network-based (tracing the communications link) or system-based (replacing a system component with a Trojan horse program that captures data insidiously). Passive attacks are the most difficult to detect. Therefore, you should assume that someone is eavesdropping on everything you send across the Internet.
- **Active attacks:** In an active attack, the perpetrator is trying to break through your defenses and get into your network systems. There are several types of active attacks:
  - In **system access attempts**, the attacker attempts to exploit security loopholes to gain access and control over a client or server system.
  - In **spoofing** attacks, the attacker attempts to break through your defenses by masquerading as a trusted system, or a user persuades you to send secret information to him.
  - In **denial of service attacks**, an attacker tries to interfere with or shut down your operations by redirecting traffic or bombarding your system with junk.
  - In **cryptographic attacks**, an attacker will attempt to guess, or steal your passwords, or will use specialized tools to try to decrypt encrypted data.

Multiple layers of defense

Because potential Internet security risks can occur at a variety of levels, you need to set up security measures that provide multiple layers of defense against these risks. In general, when you connect to the Internet, you should not wonder **if** you will experience intrusion attempts or denial of service attacks. Instead, you should assume that you **will** experience a security problem. Consequently, your best defense is a thoughtful, proactive offense. Using a layered approach when you plan your Internet security strategy ensures that an attacker who penetrates one layer of defense will be stopped by a subsequent layer.

Your security strategy should cover measures that provide protection across the following layers of the traditional network computing model. Generally, you should plan your security from the most basic (system level security) through the most complex (transaction level security).

System level security
Your system security measures represent your last line of defense against an Internet-based security problem. Consequently, your first step in a total Internet security strategy must be to properly configure iSeries basic system security settings .

Network level security
Network security measures control access to your iSeries and other network systems. When you connect your network to the Internet, you should ensure that you have adequate network level security measures in place to protect your internal network resources from unauthorized access and intrusion. A firewall is the most common means for providing network security. Your Internet Service Provider (ISP) can and should provide an important element in your network security plan. Your network security scheme should outline what security measures your ISP will provide, such as filtering rules for the ISP router connection and public Domain Name Service (DNS) precautions.

Application level security
Application level security measures control how users can interact with specific applications. In general, you should configure security settings for each application that you use. However, you should take special care to set up security for those applications and services that you will be using from or providing to the Internet. These applications and services are vulnerable to misuse by unauthorized users looking for a way to gain access to your network systems. The security measures that you decide to use need to cover both server-side and client-side security exposures.

Transmission level security
Transmission level security measures protect data communications within and across networks. When you communicate across an untrusted network like the Internet, you cannot control how your traffic flows from source to destination. Your traffic and the data it carries flows through a number of different servers that you cannot control. Unless you set up security measures, such as configuring your applications to use the Secure Sockets Layer (SSL), your routed data is available for anyone to view and use. Transmission level security measures protect your data as it flows between the other security level boundaries.

When developing your overall Internet security policy, you should develop a security strategy for each layer individually. Additionally, you should describe how each set of strategies will interact with the others to provide a comprehensive security safety net for your business.

Security policy and objectives

Your security policy

Each Internet service that you use or provide poses risks to your iSeries system and the network to which it is connected. A security policy is a set of rules that apply to activities for the computer and communications resources that belong to an organization. These rules cover areas such as physical security, personnel security, administrative security, and network security.

Your **security policy** defines what you want to protect and what you expect of your system users. It provides a basis for security planning when you design new applications or expand your current network. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords. Your security policy should also describe how you will monitor the effectiveness of your security measures. Such monitoring helps you to determine whether someone may be attempting to circumvent your safeguards.

To develop your security policy, you must clearly define your security objectives. Once you create a security policy, you must take steps to put into effect the rules it contains. These steps include training employees and adding necessary software and hardware to enforce the rules. Also, when you make changes in your computing environment, you should update your security policy. This is to ensure that you address any new risks that your changes impose. You can find an example of a security policy for the JKL Toy Company in the iSeries Information Center in the ″Basic system security and planning″ topic.

Your security objectives

When you create and carry out a security policy, you must have clear objectives. Security objectives fall into one or more of these categories:

Resource protection

Your resource protection scheme ensures that only authorized users can access objects on the system. The ability to secure all types of system resources is an iSeries strength. You should carefully define the different categories of users that can access your system. Also, you should define what access authorization you want to give these groups of users as part of creating your security policy.

Authentication

The assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system. Traditionally, systems have used passwords and user names for authentication; digital certificates can provide a more secure method of authentication while offering other security benefits as well. When you link your system to a public network like the Internet, user authentication takes on new dimensions. An important difference between the Internet and your intranet is your ability to trust the identity of a user who signs on. Consequently, you should consider seriously the idea of using stronger authentication methods than traditional user name and password logon procedures provide. Authenticated users may have different types of permissions based on their authorization levels.

Authorization
The assurance that the person or computer at the other end of the session has permission to carry out the request. Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Usually, authorization is performed in context of authentication.

Integrity
The assurance that arriving information is the same as what was sent out. Understanding integrity requires you to understand the concepts of data integrity and system integrity.

- **Data integrity**: Data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data that is stored within your network, you may need additional security to ensure data integrity when data enters your system from untrusted sources. When data that enters your system comes from a public network, you may need security methods so that you can do the following:
  - Protect the data from being “sniffed” and interpreted, usually by encrypting it.
  - Ensure that the transmission has not been altered (data integrity).
  - Prove that the transmission occurred (non-repudiation). In the future, you might need the electronic equivalent of registered or certified mail.
- **System integrity**: Your system provides consistent, expected results with expected performance. For the iSeries, system integrity is the most commonly overlooked component of security because it is a fundamental part of iSeries architecture. iSeries architecture, for example, makes it extremely difficult for a mischief-maker to imitate or change an operating system program when you use security level 40 or 50.

Non-repudiation
Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to ″sign″ transactions, messages, and documents supports non-repudiation. Both the sender and the receiver agree that the exchange took place. The digital signature on the data provides the necessary proof.

Confidentiality
The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and the Secure Socket Layer (SSL) helps ensure confidentiality when transmitting data across untrusted networks. Your security policy should address how you will provide confidentiality for information within your network as well as when information leaves your network.

Auditing security activities
Monitoring security-relevant events to provide a log of both

successful and unsuccessful (denied) access. Successful access records tell you who is doing what on your systems. Unsuccessful (denied) access records tell you either that someone is attempting to break your security or that someone is having difficulty accessing your system.

Understanding your security objectives helps you create a security policy that covers all your networking and Internet security needs. You may find it helpful to review the JKL Toy Company e-business scenario as you define your objectives and create your security policy. The scenario company's Internet usage and security plan is representative of many real world implementations.

Scenario: JKL Toy Company e-business plans

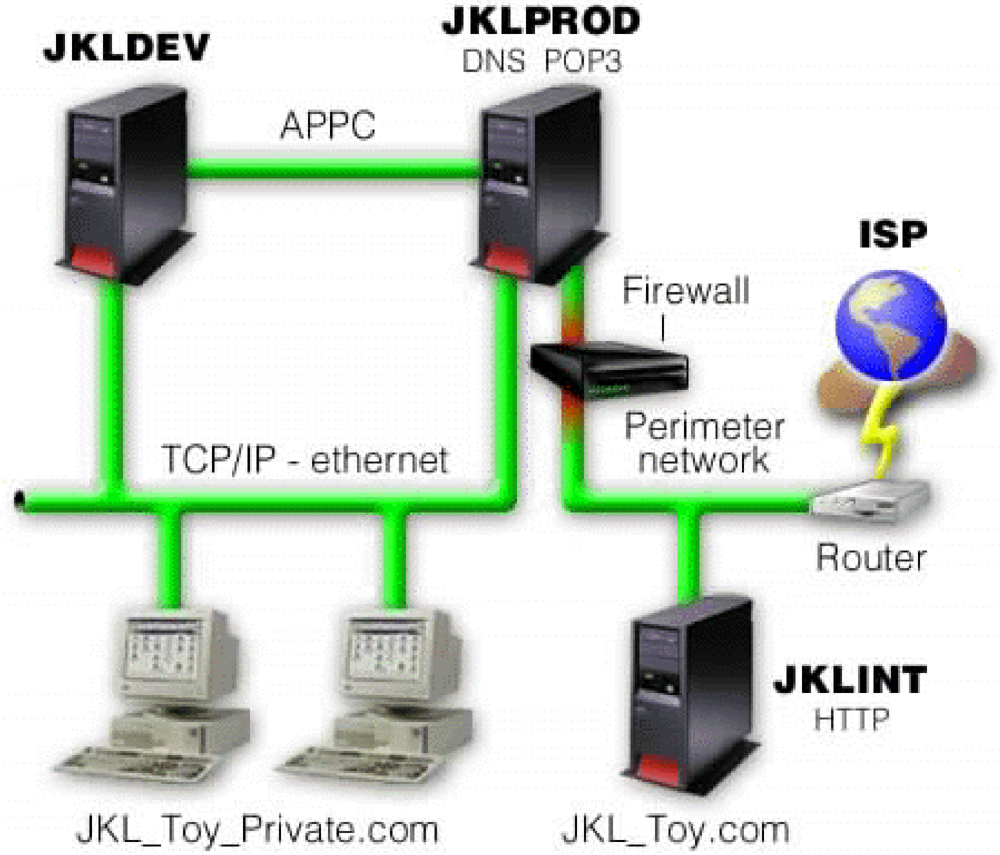
This scenario describes a typical business, the JKL Toy Company which has decided to expand its business objectives by using the Internet. Although the company is fictitious, their plans for using the Internet for e-business and their resulting security needs are representative of many real world company situations.

The JKL Toy Company is a small, but rapidly growing, manufacturer of toys, from jump ropes to kites to cuddly stuffed leopards. The company president is enthusiastic about the growth of the business and about how its new iSeries system can ease the burdens of that growth. Sharon Jones, the accounting manager, is responsible for iSeries system administration and system security.

The JKL Toy Company has been successfully using its security policy for its internal applications for over a year. The company now has plans to set up an intranet to more efficiently share internal information. The company also has plans to begin using the Internet to further its business goals. Included in these goals are plans for creating a corporate Internet marketing presence, including an online catalog. They also want to use the Internet to transmit sensitive information from remote sites to the corporate office. Additionally, the company wants to allow employees in the design laboratory to have Internet access for research and development purposes. Eventually, the company wants to allow customers to use their web site for direct online purchasing. Sharon is developing a report about the specific potential security risks for these activities and what security measures the company should use to minimize these risks. Sharon will be responsible for updating the company security policy and putting into practice the security measures that the company decides to use.

The goals of this increased Internet presence are as follows
- Promote general corporate image and presence as part of an overall marketing campaign.
- Provide an online product catalog for customers and sales staff.
- Improve customer service.
- Provide employee e-mail and World Wide Web access.

After ensuring that their iSeries systems have strong basic system security, JKL Toy company has decided to purchase and use a firewall product to provide network level protection. The firewall will shield their internal network from many potential Internet-related risks. Below is an illustration of the company Internet/network configuration.



As shown in the diagram, JKL Toy company has two primary iSeries systems. They use one system for development (JKLDEV) and one for production (JKLPROD) applications. Both of these systems handle mission-critical data and applications. Consequently, they are not comfortable running their Internet applications on these systems. Instead, they have chosen to add a new iSeries system (JKLINT) to run these applications.

The company has placed the new system on a perimeter network and is using a firewall between it and the main internal network of the company to ensure better separation between their network and the Internet. This separation decreases the Internet risks to which their internal systems are vulnerable. By designating the new iSeries as an Internet server only, the company also decreases the complexity of managing their network security.

The company will not run any mission-critical applications on the new iSeries system at this time. During this stage of their e-business plans the new system will provide a static public web site only. However, the company wants to implement security measures to protect the system and the public web site it runs to prevent service interruptions and other possible attacks. Consequently, the company will protect the system with packet filtering rules and network address translation (NAT) rules, as well as strong basic security measures.

As the company develops more advanced public applications (such as an e-commerce web site or extranet access) they will implement more advanced security measures.

Chapter 5. Security levels for basic Internet readiness

Your system security measures represent your last line of defense against an Internet-based security problem. Consequently, your first step in a total Internet security strategy must be to properly configure OS/400 basic security settings. You should do the following to ensure that your system security meets the minimum requirements:

- Set the security level (QSECURITY system value) to 50. Security level 50 provides the highest level of integrity protection, which is strongly recommended for protecting your system in high risk environments such as the Internet.

  Note: If you have a highly transaction oriented or an application that makes extensive use of the Integrated File System , operating at security level 50 may cause your system or the application to experience a performance degradation.

  For more detailed information about each iSeries security level, see Tips and Tools for Securing your iSeries.

  Note: If you are currently running at a security level lower than 50, you may need to update either your operating procedures or your applications. You should review information in the book, iSeries Security Reference , before changing to a higher security level.
- Set your security-relevant system values to be at least as restrictive as the recommended settings. You can use the Operations Navigation Security Wizard or the Technical Studio Security Advisor to compare your settings to the recommended settings.
- Ensure that no user profiles, including IBM-supplied user profiles, have default passwords. Use the Analyze Default Passwords (ANZDFTPWD) command to check whether you have default passwords.
- Use object authority to protect your important system resources. Take a restrictive approach on your system. That is, by default restrict everyone (PUBLIC *EXCLUDE) from system resources such as libraries and directories. Allow only a few users to access these restricted resources. Restricting access through menus is not sufficient in an Internet environment.
- You **must** set up object authority on your system. You can find more information about working with object authority in the iSeries Navigator chapter of Tips and Tools for Securing your iSeries .

To help you configure these minimum system security requirements, you can use either the **Security Advisor** (available from the Technical Studio Web site) or the **Security Wizard** (available from the iSeries Navigator interface). The Technical Studio Security Advisor provides you with a set of security recommendations based on your answers to a series of questions. You can then use these recommendations to configure the system security settings that you need. The Security Wizard also provides recommendations based on your answers to a series of questions. Unlike the Security Advisor, you can have the wizard use the recommendations to configure your system security settings for you.

The inherent security features of the iSeries, when properly configured and managed, provide you with the ability to minimize many risks. When you connect your iSeries to the Internet, however, you will need to provide additional security measures to ensure the safety of your internal network. After you ensure that your iSeries has good general system security in place, you are ready to configure additional security measures as part of your comprehensive security plan for Internet usage.

Chapter 6. Network security options

When connecting to an untrusted network, your security policy must describe a comprehensive security scheme, including the security measures that you will implement at the network level. Installing a firewall is one of the best means of deploying a comprehensive set of network security measures.

Also, your Internet Service Provider (ISP) can and should provide an important element in your network security plan. Your network security scheme should outline what security measures your Internet Service Provider (ISP) will provide, such as filtering rules for the ISP router connection and public Domain Name Service (DNS) precautions.

Although a firewall certainly represents one of your main lines of defense in your total security plan, it should not be your **only** line of defense. Because potential Internet security risks can occur at a variety of levels, you need to set up security measures that provide multiple layers of defense against these risks.

While a firewall provides a tremendous amount of protection from certain kinds of attack, a firewall is only part of your total security solution. For instance, a firewall cannot necessarily protect data that you send over the Internet through applications such as SMTP mail, FTP, and TELNET. Unless you choose to encrypt this data, anyone on the Internet can access it as it travels to its destination.

You should strongly consider using a firewall product as your main line of defense whenever you connect your iSeries system or your internal network to the Internet. Although you can no longer purchase the IBM Firewall for AS/400 product and support for the product is no longer available, there are a number of other products that you can use.

You can learn more about transitioning from an existing IBM Firewall for AS/400 to other products or to iSeries native network security features by reading All You Need to Know When Migrating from IBM Firewall for AS/400 (SG24-6152).

Because commercial firewall products provide a full range of network security technologies, the JKL Toy Company has chosen to use one in their e-business security scenario to protect their network. However, their firewall does not provide any protection for their new iSeries Internet server. Consequently, they have chosen to implement the iSeries Packet rules feature to create filter and NAT rules to control traffic for the Internet server.

About iSeries Packet rules

Packet filter rules let you protect your computer systems by rejecting or accepting IP packets according to criteria that you define. NAT rules allow you to hide your internal system information from external users by substituting one IP address for another, public IP address. Although IP packet filter and NAT rules are core network security technologies, they do not provide the same level of security that a fully functional firewall product does. You should carefully analyze your security needs and objectives when deciding between a complete firewall product and the iSeries packet rules feature.

Review the topic Choosing iSeries network security options to help you decide which approach is right for your security needs.

Firewalls

A firewall is a blockade between a secure internal network and an untrusted network such as the Internet. Most companies use a firewall to connect an internal network safely to the Internet, although you can use a firewall to secure one internal network from another also.

A firewall provides a controlled single point of contact (called a chokepoint) between your secure internal network and the untrusted network. The firewall:

- Lets users in your internal network use authorized resources that are located on the outside network.
- Prevents unauthorized users on the outside network from using resources on your internal network.

When you use a firewall as your gateway to the Internet (or other network), you reduce the risk to your internal network considerably. Using a firewall also makes administering network security easier because firewall functions carry out many of your security policy directives.

How a firewall works

To understand how a firewall works, imagine that your network is a building to which you want to control access. Your building has a lobby as the only entry point. In this lobby, you have receptionists to welcome visitors, security guards to watch visitors, video cameras to record visitor actions, and badge readers to authenticate visitors who enter the building.

These measures may work well to control access to your building. But, if an unauthorized person succeeds in entering your building, you have no way to protect the building against this intruder’s actions. If you monitor the intruder’s movements, however, you have a chance to detect any suspicious activity from the intruder.

Firewall components

A firewall is a collection of hardware and software that, when used together, prevent unauthorized access to a portion of a network. A firewall consists of the following components:

- Hardware. Firewall hardware usually consists of a separate computer or device dedicated to running the firewall software functions.
- Software. Firewall software provides a variety of applications. In terms of network security, a firewall provides these security controls through a variety of technologies:
  – Internet Protocol (IP) packet filtering
  – Network address translation (NAT) services
  – SOCKS server
  – Proxy servers for a variety of services such as HTTP, Telnet, FTP, and so forth
  – Mail relay services
  – Split Domain name services (DNS)
  – Logging
  – Real-time monitoring

Note: Some firewalls provide virtual private networking (VPN) services so that you can set up encrypted sessions between your firewall and other compatible firewalls.

Using firewall technologies

You can use the firewall proxy servers, SOCKS server, or NAT rules to provide internal users with safe access to services on the Internet. The proxy and SOCKS servers break TCP/IP connections at the firewall to hide internal network information from the untrusted network. The servers also provide additional logging capabilities.

You can use NAT to provide Internet users with easy access to a public server behind the firewall. The firewall still protects your network because NAT hides your internal IP addresses.

A firewall also can protect internal information by providing a DNS server for use by the firewall. In effect, you have two DNS servers: one that you use for data about the internal network, and one on the firewall for data about external networks and the firewall itself. This allows you to control outside access to information about your internal systems

When you define your firewall strategy, you may think it is sufficient to prohibit everything that presents a risk for the organization and allow everything else. However, because computer criminals constantly create new attack methods, you must anticipate ways to prevent these attacks. As in the example of the building, you also need to monitor for signs that, somehow, someone has breached your defenses. Generally, it is much more damaging and costly to recover from a break-in than to prevent one.

In the case of a firewall, your best strategy is to permit only those applications that you have tested and have confidence in. If you follow this strategy, you must exhaustively define the list of services you must run on your firewall. You can characterize each service by the direction of the connection (from inside to outside, or outside to inside). You should also list users who you will authorize to use each service and the machines that can issue a connection for it.

What a firewall can do to protect your network

You install a firewall between your network and your connection point to the Internet (or other untrusted network). The firewall then allows you to limit the points of entry into your network. A firewall provides a single point of contact (called a chokepoint) between your network and the Internet (see the figure below). Because you have a single point of contact, you have more control over which traffic to allow into and out of your network.

A firewall appears as a single address to the public. The firewall provides access to the untrusted network through proxy or SOCKS servers or network address translation (NAT) while hiding your internal network addresses. Consequently, the firewall maintains the privacy of your internal network. Keeping information about your network private is one way in which the firewall makes an impersonation attack (spoofing) less likely.

A firewall allows you to control traffic into and out of your network to minimize the risk of attack to your network. A firewall securely filters all traffic that enters your network so that only specific types of traffic for specific destinations can enter. This minimizes the risk that someone could use TELNET or file transfer protocol (FTP) to gain access to your internal systems.

What a firewall cannot do to protect your network

While a firewall provides a tremendous amount of protection from certain kinds of attack, a firewall is only part of your total security solution. For instance, a firewall cannot necessarily protect data that you send over the Internet through applications such as SMTP mail, FTP, and TELNET. Unless you choose to encrypt this data, anyone on the Internet can access it as it travels to its destination.

iSeries Packet rules

iSeries 400 Packet rules is an integrated feature of OS/400 available from the Operations Navigator interface. The packet rules feature allows you to configure two core network security technologies to control the flow of TCP/IP traffic to protect your iSeries system:

- Network address translation (NAT)
- IP packet filtering

Because NAT and IP filtering are integrated parts of your OS/400, they provide an economical way for you to secure your system. In some cases, these security technologies may provide everything you need without any additional purchases. These technologies, however, do not create a true, functional firewall. You can use IP packet security alone, or in conjunction with a firewall, depending on your security needs and objectives.

Note: You should not attempt to take advantage of the cost savings if you are planning to secure an iSeries production system. For situations such as this, the security of your system should take precedence over cost. To ensure that you provide maximum protection for your production system, you should consider using a firewall.

What are NAT and IP packet filtering and how do they work together?

Network address translation (NAT) changes the source or the destination IP addresses of packets that flow through the system. NAT provides a more transparent alternative to the proxy and SOCKS servers of a firewall. NAT can also simplify network configuration by enabling networks with incompatible addressing structures to connect to each other. Consequently, you can use NAT rules so that an iSeries system can function as a gateway between two networks which have conflicting or incompatible addressing schemes. You can also use NAT to hide the real IP addresses of one network by dynamically substituting one or more addresses for the real ones. Because IP packet filtering and NAT complement each other, you will often use them together to enhance network security.

Using NAT can also make it easier to operate a public web server behind a firewall. Public IP addresses for the web server translate to private internal IP addresses. This reduces the number of registered IP addresses that are required and minimizes impacts to the existing network. It also provides a mechanism for internal users to access the Internet while hiding the private internal IP addresses.

IP packet filtering provides the ability to selectively block or protect IP traffic based on information in the packet headers. You can use the Internet Setup Wizard in Operations Navigator to quickly and easily configure basic filtering rules to block unwanted network traffic.

You can use IP packet filtering to do the following:

- Create a set of filter rules to specify which IP packets to permit into your network and which to deny access into your network. When you create filter rules, you apply them to a physical interface (for example, a Token ring or Ethernet line). You can apply the rules to multiple physical interfaces, or you can apply different rules to each interface.
- Create rules to either permit or deny specific packets that are based on the following header information:
  - Destination IP address
  - Source IP address Protocol (for example, TCP, UDP, and so forth)
  - Destination port (for example, it is port 80 for HTTP)
  - Source port
  - IP datagram direction (inbound or outbound)
  - Forwarded or Local
- Prevent undesirable or unnecessary traffic from reaching applications on the system. Also, you can prevent traffic from forwarding to other systems. This includes low-level ICMP packets (for example, PING packets) for which no specific application server is required.
- Specify whether a filter rule creates a log entry with information about packets that matches the rule in a system journal. Once the information writes to a system journal, you cannot change the log entry. Consequently, the log is an ideal tool for auditing network activity.

Choosing iSeries network security options

Network security solutions that guard against unauthorized access generally rely on firewall technologies to provide the protection. To protect your iSeries 400 system, you can choose to use a full-capability firewall product or you can choose to put into effect specific network security technologies as part of the OS/400 TCP/IP implementation. This implementation consists of the Packet rules feature (which includes IP filtering and NAT) and HTTP for iSeries proxy server feature.

Choosing to use either the Packet rules feature or a firewall depends on your network environment, access requirements, and security needs. You should **strongly** consider using a firewall product as your main line of defense whenever you connect your iSeries system, or your internal network, to the Internet or other untrusted network.

A firewall is preferable in this case because a firewall typically is a dedicated hardware and software device with a limited number of interfaces for external access. When you use the OS/400 TCP/IP technologies for Internet access protection you are using a general purpose computing platform with a myriad number of interfaces and applications open to external access.

The difference is important for a number of reasons. For example, a dedicated firewall product does not provide any other functions or applications beyond those that comprise the firewall itself. Consequently, if an attacker successfully circumvents the firewall and gains access to the it, the attacker can not do much. Whereas, if an attacker circumvents the TCP/IP security functions on your iSeries, the attacker potentially could have access to a variety of useful applications, services, and data. The attacker can then use these to wreck havoc on the system itself or to gain access to other systems in your internal network.

So, is it ever acceptable to use the iSeries TCP/IP security features? As with all the security choices that you make, you must base your decision on the cost versus benefit trade-offs that you are willing to make. You must analyze your business goals and decide what risks you are willing to accept versus the cost of how you provide security to minimize these risks. The following table provides information about when it is appropriate to use TCP/IP security features versus a fully functional firewall device. You can use this table to determine whether you should use a firewall, TCP/IP security features, or a combination of both to provide your network and system protection.

Security technology	Best use of OS/400 TCP/IP technology	Best use of a fully functional firewall
IP packet filtering	• To provide **additional** protection for a single iSeries system, such as an public web server or an intranet system with sensitive data. • To protect a subnetwork of a corporate **intranet** when the iSeries system is acting as a gateway (casual router) to the rest of the network. • To control communication with a somewhat trusted partner over a **private network** or extranet where the iSeries system is acting as a gateway.	• To protect an entire corporate network from the **Internet** or other untrusted network to which your network is connected. • To protect a large subnetwork with heavy traffic from the remainder of a corporate network.
Network Address Translation (NAT)	• To enable the connection of two **private networks** with incompatible addressing structures. • To hide addresses in a subnetwork from a less trusted network.	• To hide addresses of clients accessing the **Internet** or other untrusted network. To use as an alternative to Proxy and SOCKS servers. • To make services of a system in a private network available to clients on the **Internet**.
Proxy server	• To proxy at **remote locations** in a corporate network when a central firewall provides access to the Internet.	• To proxy an entire corporate network when accessing the **Internet**.

To learn more about how to use the OS/400 TCP/IP security features, see these resources:

- Packet rules (filtering and NAT).
- HTTP Server Documentation Center.
- AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Chapter 7. Application security options

Application level security measures control how users can interact with specific applications. In general, you should configure security settings for each application that you use. However, you should take special care to set up security for those applications and services that you will be using from, or providing to, the Internet. These applications and services are vulnerable to misuse by unauthorized users looking for a way to gain access to your network systems. The security measures that you use need to cover both server-side and client-side security exposures.

While it is important to secure each application that you use, the security measures play a small part in your overall security policy implementation. The security measures that you put into place

To learn more about what you should do to secure several common Internet applications, review these pages:
- "Web serving security"
- "Java Internet security" on page 26
- "E-mail security" on page 29
- "FTP security" on page 30

Web serving security

When you provide access for visitors to your web site, you do not want to expose your viewers to information about how the site is set up and the coding that is used to generate the page. You want their visit to your page to be easy, fast, and seamless, with all the work being done behind the scenes. As an administrator, you want to ensure that your security practices do not negatively affect your Web site. When using your iSeries 400 as a web server, consider these points:

- The server administrator must define directives for the server before a client can interact with the HTTP server. There are two methods for creating security checks: general server directives and server protection directives. Any request to the web server must satisfy any and all restrictions that these directives provide before the server honors the request.
- You can create and edit these directives by using the server admin web pages for server configuration. Server directives allow you to control the overall behavior of the web server. Server protection directives allow you to specify and control the security models the server uses for specific URLs that the web server handles.
- You can use map or pass directives and the server admin web pages to configure the server.
  - Use map or pass directives to mask the file names on your iSeries web server. More specifically there are PASS server directives and MAP server directives that control the directories from which the web server serves URLs. You can also find an EXEC server directive that controls the libraries in which CGI-BIN programs reside.

    You define protection directives for each server URL. Not all URLs require a protection directive. But, if you want to control how a URL resource is accessed or by whom, then a protection directive for that URL is required.
  - Also, you can use the server Admin web pages to configure the server rather than using WRKHTTPCFG (Work with HTTP Configuration command) and typing the directives. Working with protection directives through the

command line interface can be very complicated. Therefore, it is recommended that you use the Admin web pages to ensure that you set up your directives correctly.

HTTP provides you with the capability to display data, but not alter data in a database file. However, there are some applications you will write that will need to update a database file. To do this, you can use CGI-BIN programs. For instance, you may want to create forms that, once users complete them, update an iSeries database. As security administrator, you should monitor the authorizations of that user profile and the functions that the CGI programs perform. Also, be sure to evaluate what sensitive objects might have inappropriate public authority.

Note: Common Gateway Interface (CGI) is an industry standard for the exchange of information between a web server and computer programs that are external to it. The programs can be written in any programming language that is supported on the operating system where the web server is running.

In addition to using CGI programs in your web pages, you may want to use Java. You should understand Java security before you add Java to your web pages.

The HTTP server provides an access log that you can use to monitor both accesses and attempted accesses through the server.

The proxy server receives HTTP requests from web browsers and resends them to web servers. Web servers that receive these requests are only aware of the proxy server IP address. They cannot determine the names or addresses of the PCs that originated the requests. The proxy server can handle URL requests for HTTP, File Transfer Protocol (FTP), Gopher, and WAIS.

You can also use the HTTP proxy support of the IBM HTTP Server for iSeries to consolidate web access. The proxy server can also log all URL requests that are for tracking purposes. You can then review the logs to monitor use and misuse of network resources.

You can find more information on this subject in the book *Tips and Tools for Securing Your iSeries.*

Java Internet security

Java programming is becoming increasingly widespread in today's computing environments. For example, you might be using the IBM Toolbox for Java or the IBM Development Kit for Java on your system to develop new applications. Consequently, you must prepare to deal with the security issues that are associated with Java. Although a firewall is a good defense against most general Internet security risks, it does not provide protection for many risks that using Java presents. Your security policy should include details for protecting your system against three areas of concern for Java: applications, applets, and servlets. Also, you should understand how Java and resource security interact in terms of authentication and authorization for Java programs.

Java applications

As a language, Java has some characteristics that protect Java programmers from unintentional errors that can cause integrity problems. (Other languages that are commonly used for PC applications, such as C or C++ do not protect the programmers from unintentional errors as strongly as Java does.) For example, Java uses strong typing which protects the programmer from using objects in unintended ways. Java does not allow pointer manipulation, which protects the programmer from accidentally going outside the memory boundaries of the program. From an application development perspective, you can view Java as you do other high-level languages. You should apply the same security rules for application design that you apply with other languages on your iSeries 400.

Java applets

Java applets are small Java programs that you can include in your HTML pages. Because applets run on the client, what they do is a concern to the client. However, a Java applet has the potential to access your iSeries 400. (An ODBC program or an advanced program-to-program communications (APPC) program that operates on a PC in your network can also access your iSeries.) In general, Java applets can establish a session only with the server from which the applet originated. Therefore, a Java applet can access your iSeries from a connected PC only when the applet came from your iSeries (such as from your web server).

An applet can attempt to connect to any TCP/IP port on a server. It does not have to talk to a software server that is written in Java. But, for servers that are written with the IBM Toolbox for Java, the applet must provide a user ID and password when it establishes connections back to the server. In this material, the servers described are all iSeries servers. (A server written in Java does not have to use the IBM Toolbox for Java). Typically, the IBM Toolbox for Java class prompts the user for a user ID and password for the first connection.

The applet can perform functions on the iSeries system only if the user profile has authorization to those functions. Therefore, a good resource security scheme is essential when you begin to use Java applets to provide new application function. When the system processes the requests from applets, it does not use the limited capability value in the profile of the user.

The applet viewer allows you to test an applet on the server system; however, it is not subject to browser security restrictions. Therefore, you should use the applet viewer to test your own applets only, never to run applets from outside sources. Java applets often write to the PC drive of the user, which may allow the applet the opportunity to perform a destructive action. However, you can use a digital certificate to sign a Java applet to establish its authenticity. The signed applet can write to the PC's local drives, even though the default setting for the browser prevents it. The signed applet can also write to mapped drives on your iSeries because they appear to the PC to be local drives.

Note: The behavior described above is generally true for Netscape Navigator and MS Internet Explorer. What actually happens depends on how you configure and manage the browsers that you use.

For Java applets that originate from your iSeries, you might need to use signed applets. However, you should instruct your users in general not to accept signed applets from unknown sources.

Beginning with V4R4, you can use the IBM Toolbox for Java to set up a Secure Sockets Layer (SSL) environment . You can also use the IBM Developer Toolkit for

Java to make a Java application secure with SSL. Using SSL with your Java applications ensures encryption of the data, including the user IDs and passwords that pass between the client and server. You can use Digital Certificate Manager to configure registered Java programs to use SSL.

Java servlets

Servlets are server-side components that are written in Java, which dynamically extend the functionality of a web server without changing web server code. The IBM WebSphere Application Server that ships with IBM HTTP Server for iSeries provides support for using servlets on iSeries systems.

You must use resource security on servlet objects that the server uses. However, applying resource security to a servlet does not sufficiently secure it. Once a web server loads a servlet, resource security does not prevent others from running it too. Consequently, you should use resource security in addition to using HTTP Server security controls and directives. For example, do not allow servlets to run under the profile of the web server only. In addition, you should control who can run the servlet (mask keywords in the protection directive) through the use of HTTP server groups and access control lists (ACL). Also, you should use the security features provided by your servlet development tools, such as those found in the WebSphere Application Server for iSeries.

Review these resources to learn more about general security measures for Java:
- IBM Developer Kit for Java Java Security.
- IBM Toolbox for Java security classes.
- Tips and Tools for Securing Your iSeries .

Java authentication and authorization to resources

IBM Toolbox for Java contains security classes to provide verification of the identity of the user and optionally assign that identity to the operating system thread for an application or servlet that is running on an iSeries system. Subsequent checks for resource security occur under the assigned identity. For more detailed information about these security classes, see IBM Toolbox for Java Authentication Services.

The IBM Developer Kit for Java provides support for the Java Authentication and Authorization Service (JAAS), which is a standard extension to the Java 2 Software Development Kit (J2SDK), Standard Edition. Currently, J2SDK provides access controls that are based on where the code originated and who signed the code (code source-based access controls). To learn more about using the J2SDK, see Java Authentication and Authorization Service.

Securing your Java applications with SSL

You can use Secure Sockets Layer (SSL) to secure communications for iSeries applications that you develop with IBM Developer Kit for Java. Client applications that use IBM Toolbox for Java can also take advantage of SSL. The process for enabling SSL for your own Java applications is somewhat different than enabling it for the other applications.

For more information about Secure Sockets Layer administration for Java applications, see these Information Center topics:
- IBM Toolbox for Java Secure Sockets Layer (SSL) environment .

- IBM Developer Toolkit for Java to make a Java application secure with SSL.

E-mail security

Using e-mail across the Internet or other untrusted network imposes security risks against which using a firewall may not protect. You must understand these risks to ensure that your security policy describes how you will minimize these risks.

E-mail is like other forms of communication. It is very important to use discretion before sending any confidential information through e-mail. Because your e-mail travels through many servers before you receive it, it is possible for someone to intercept and read your e-mail. Consequently, you may want to use security measures to protect the confidentiality of your e-mail.

Common e-mail security risks

These are some risks associated with using e-mail:

- **Flooding** (a type of denial of service attack) occurs when a system becomes overloaded with multiple e-mail messages. It is relatively easy for an attacker to create a simply program that sends millions of e-mail messages (including empty messages) to a single e-mail server to attempt to flood the server. Without proper security, the target server can experience a denial of server because the server's storage disk fills with useless messages. Or, the server stops responding because all server resources become involved in processing the mail from the attack.
- **Spamming** (junk e-mail) is another type of attack common to e-mail. With increasing numbers of businesses providing e-commerce over the Internet, we have seen an explosion of unwanted or unrequested for business related e-mail. This is the junk mail, that is being sent to a wide distribution list of e-mail users, filling the e-mail box of each user.
- **Confidentiality** is a risk associated with sending e-mail to another person through the Internet. This e-mail passes through many servers before it reaches your intended recipient. If you have not encrypted your message, a hacker can pick up and read your mail at any point along the delivery route.

E-mail security options

To guard against flooding and spamming risks, you must configure your e-mail server appropriately. Most server applications provide methods for dealing with these types of attacks. Also, you can work with your Internet Service Provider (ISP) to ensure that the ISP provides some additional protection from these attacks.

What additional security measures you need depend on the level of confidentiality that you need, as well as what security features your e-mail applications provide. For example, is keeping the contents of the e-mail message confidential sufficient? Or do you want to keep all information associated with the e-mail, such as the originating and target IP addresses, confidential?

Some applications have integrated security features that may provide the protection you need. Lotus Notes Domino™, for instance, provides several integrated security features including encryption capability for an entire document or for individual fields in a document.

In order to encrypt mail, Lotus Notes Domino creates a unique public and private key for each user. You use your private key to encrypt the message so that the message is readable to only those users that have your public key. You must send your public key to the intended receivers of your note so that they can use it to decipher your encrypted note. If someone sends you encrypted mail, Lotus Notes Domino uses the public key of the sender to decipher the note for you.

You can find information about using these Notes encryption features in the online help files for the program.

For more detailed information about security for Domino™ on the iSeries, see these references:

- Lotus Domino reference library.
- Lotus Notes user assistance web site.
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed (SG24-5341).
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990).

When you want to provide more confidentiality for e-mail or other information that flows between branch offices, remote clients, or business partners, you have a couple options.

If your e-mail server application supports it, you can use Secure Sockets Layer (SSL) to create a secure communications session between the server and e-mail clients. SSL also provides support for optional client-side authentication, when the client application is written to use it. Because the entire session is encrypted, SSL also ensures data integrity while the data is in transit.

Another option available to you is to configure a Virtual private network (VPN) connection. As of V4R4, you can use your iSeries to configure various VPN connections, including between remote clients and your iSeries system. When you use a VPN all traffic that flows between the communicating endpoints is encrypted, ensuring both data confidentiality and data integrity.

FTP security

FTP (File Transfer Protocol) provides the capability of transferring files between a client (a user on another system) and your server. You can also use the remote command capability to submit commands to the server. Consequently, FTP is very useful for working with remote systems, or to move files between systems. However, the use of FTP across the Internet, or other untrusted networks, exposes you to certain security risks. You must understand these risks to ensure that your security policy describes how you will minimize these risks.

- Your object authority scheme might not provide enough protection when you allow FTP on your system.

  For example, the public authority for your objects may be *USE, but today you are preventing most users from accessing those objects by using ″menu security″. (Menu security prevents users from doing anything that is not one of their menu options.) Since FTP users are not restricted to menus, they can read all objects on your system.Here are some options for controlling this security risk:
  - Put into effect full iSeries object security on the system (in other words, change the system’s security model from ″menu security″ to ″object security.″ This is your best, most secure option.
  - Write exit programs for FTP to restrict access to files which may be transferred through FTP. These exit programs should provide security that is

at least the equivalent as the security that the menu program provide. Many customers would probably want to make the FTP access controls even more restrictive. This option only covers FTP, not other interfaces such as ODBC, DDM, or DRDA.

Note: *USE authority to a file allows the user to download the file.
*CHANGE authority to a file allows the user to upload the file.

- A hacker can mount a ″denial of service″ attack with your FTP server to disable user profiles on the system. This is done by repeatedly attempting to log on with an incorrect password for a user profile until the user profile is disabled. This type of attack disables the profile if it reaches the maximum sign on count of three.

  What you can do to avoid this risk involves analyzing the trade-offs that you are willing to make to increase security to minimize the attack versus providing users with ease of access. The FTP server normally enforces the QMAXSIGN system value to prevent a hacker from having unlimited attempts to guess a password and therefore mount password attacks. Here are some options that you should consider using:
  – Use an FTP server logon exit program to reject logon requests by any system user profiles and those user profiles that you designate not be allowed FTP access. (When using such an exit program, logon attempts rejected by the server logon exit point for the user profiles that you block do **not** get counted against the profile's QMAXSIGN count.)
  – Use an FTP server logon exit program to limit the client machines from which a given user profile is allowed to access the FTP server. For example, if a person from Accounting is allowed FTP access, only allow that user profile FTP server access from computers which have IP addresses in the Accounting department.
  – Use an FTP server logon exit program to log the user name and IP address of all FTP logon attempts. Review these logs regularly, and whenever a profile is disabled by maximum password attempts, use the IP address information to identify the perpetrator and take appropriate measures.

Additionally, you can use FTP server exit points to provide an anonymous FTP function for guest users. Setting up a secure, anonymous FTP server requires exit programs for both the FTP server logon **and** FTP server request validation exit points.

Beginning in V5R1, you can use the Secure Sockets Layer (SSL) to provide secure communications sessions for your FTP server. Using SSL ensures that all FTP transmissions are encrypted to maintain confidentiality for all data that passes between the FTP server and the client, including user names and passwords. The FTP server supports the use of digital certificates for client authentication also.

To learn more about using FTP, its risks, and the security measures available to you, review these resources:

- Implementing FTP security .
- Anonymous FTP.
- Securing FTP.
- Tips and Tools for Securing your iSeries .

Chapter 8. Transmission security options

Remember that the JKL Toy company scenario has two primary iSeries 400 systems. They use one for development and the other for production applications. Both of these systems handle mission-critical data and applications. Consequently, they chose to add a new iSeries system on a perimeter network to handle their intranet and Internet applications.

Establishing a perimeter network ensures that they have some physical separation between their internal network and the Internet. This separation decreases the Internet risks to which their internal systems are vulnerable. By designating the new iSeries 400 as an Internet server only, the company also decreases the complexity of managing their network security.

Because of the pervasive need for security in an Internet environment, IBM is continually developing security offerings to ensure a secure networking environment for conducting e-business on the Internet. In an Internet environment you must ensure that you provide both system specific and application specific security. However, moving confidential information through a company intranet or across an Internet connection further increases the need to implement stronger security solutions. To combat these risks you should implement security measures that protect the transmission of data while it travels over the Internet.

You can minimize the risks associated with moving information across untrusted systems with two specific transmission level security offerings for iSeries: Secure Sockets Layer (SSL) secure communications and Virtual Private Networking (VPN) connections.

Securing applications with SSL

The Secure Sockets Layer (SSL) protocol is a de facto industry standard for securing communication between clients and servers. SSL was originally developed for web browser applications, but an increasing number of other applications are now able to use SSL. For iSeries, these include:
- IBM HTTP Server for iSeries (original and powered by Apache)
- FTP server
- Telnet server
- Distributed relational database architecture (DRDA) and distributed data management
- (DDM) server
- Management Central
- Directory Services Server (LDAP)
- Client Access Express applications, including Operations Navigator, and applications that are written to the Client Access Express set of application programming interfaces (APIs)
- Programs developed with Developer Kit for Java and client applications that use IBM Toolkit for Java
- Programs developed with Secure Sockets Layer (SSL) Application Programmable Interfaces (APIs) which can be used to enable SSL on applications. See the Secure Sockets Layer APIs for more information about how to write programs that use SSL.

Several of these applications also support the use of digital certificates for client authentication. SSL relies on digital certificates to authenticate the communication parties and to create a secure connection.

iSeries Virtual Private Networking (VPN)

You can use your iSeries system VPN connections to establish a secure communications channel between two endpoints. Like an SSL connection, the data that travels between the endpoints can be encrypted, thereby providing both data confidentiality and data integrity. VPN connections, however, allow you to limit the traffic flow to the endpoints that you specify and to restrict the type of traffic that can use the connection. Therefore, VPN connections provide some network level security by helping you to protect your network resources from unauthorized access.

Which method should you use?

Both of these security methods address the need for secure authentication, data confidentiality and data integrity. Which of these methods you should use depends on several factors. Factors to consider are who you are communicating with, what applications you use to communicate with them, how secure you need the communication to be, and what trade-offs in cost and performance you are willing to make to secure this communication.

Also, if you want to use a specific application with SSL, that application must be set up to use SSL. Although many applications cannot take advantage of SSL yet, many others, like Telnet and Client Access Express, have added SSL capability. VPNs on the other hand, allow you to protect all IP traffic that flows between specific connection endpoints.

For example, you may use HTTP over SSL currently to allow a business partner to communicate with a Web server on your internal network. If the Web server is the only secure application that you need between you and your business partner, then you may not want to switch to a VPN connection. However, if you want to expand your communications, you may want to use a VPN connection instead. Also, you may have a situation in which you need to protect traffic in a portion of your network, but you do not want to individually configure each client and server to use SSL. You could create a gateway-to-gateway VPN connection for that portion of the network. This would secure the traffic, but the connection is transparent to individual servers and clients on either side of the connection.

Using digital certificates for SSL

Digital certificates provide the foundation for using the Secure Sockets Layer (SSL) for secure communications and as a stronger means of authentication. iSeries 400 provides you with the ability to easily create and manage digital certificates for your systems and users with Digital Certificate Manager (DCM), an integrated feature of OS/400.

Additionally, you can configure some applications, such as the IBM HTTP Server for iSeries, to use digital certificates for a stronger method of client authentication instead of user name and passwords.

What is a digital certificate?

A digital certificate is a digital credential that validates the identity of the certificate owner, much as a passport does. A trusted third party, called a **Certificate authority (CA),** issues digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential.

Each CA has a policy to determine what identifying information the CA requires in order to issue a certificate. Some Internet CAs may require very little information, such as only requiring a distinguished name. This is the name of the person or server to whom a CA issues a digital certificate address and a digital e-mail address. A private key and a public key are generated for each certificate. The certificate contains the public key, while the browser or a secure file stores the private key. The owner of a certificate can use these keys to ″sign″ and encrypt data, such as messages and documents, sent between users and servers. Such digital signatures ensure the reliability of an item's origin and protects the integrity of the item.

Although many applications cannot take advantage of SSL yet, many others, like Telnet and Client Access Express, have added SSL capability. To learn how you can use SSL with iSeries applications, see **Securing applications with SSL** in the iSeries Information Center:

SSL for secure Telnet access

As of V4R4, you can use configure your Telnet server to use the Secure Sockets Layer (SSL) tosecure Telnet communications sessions. To configure your Telnet server to use SSL, you must use Digital Certificate Manager (DCM) to configure the certificate for the Telnet server to use. By default the Telnet server handles both secure and non-secure connections. However, you can configure Telnet so that it allows only secure Telnet sessions. Additionally, you can configure the Telnet server to use digital certificates for stronger client authentication.

When you choose to use SSL with Telnet, you gain some strong security benefits. For Telnet, besides server authentication, the data is encrypted prior to any Telnet protocol data flows. Once the SSL session is established, all Telnet protocols including user ID and password exchange, are encrypted.

The most important factor to consider when using the Telnet server is the sensitivity of the information that you use in a client session. If the information is sensitive or private, then you may find it beneficial to set up your iSeries Telnet server using SSL. When you configure a digital certificate for the Telnet application, the Telnet server is able to operate with both SSL and non-SSL clients. If your security policy requires that you always encrypt your Telnet sessions, you can disable all non-SSL Telnet sessions. When there is no need for you to use the SSL Telnet server, you can turn off the SSL port. You can disable the ports using the ADDTCPPORT command. Once you have turned off the port, the server provides non-SSL Telnet for the clients, and the SSL Telnet sessions are disabled.

To learn more about Telnet and about security tips for Telnet with and without SSL, see these resources:

- The Telnet Information Center topic provides the information that you need to use Telnet on your iSeries.
- Securing Telnet provides information on using SSL and Telnet together to secure Telnet communications sessions.
- Tips and Tools for Securing Your iSeries provides detailed information on Telnet security in the TCP/IP section.

SSL for secure Client Access Express

As of V4R4, you can use configure your Client Access Express servers to use the Secure Sockets Layer (SSL) to secure Client Access Express communications sessions. For example, as JKL Toy company has grown, they have added a number of regional traveling sales agents to their staff. These sales agents need to access information from iSeries production system in their home office about the status of toy availability and of manufacturing dates. Because this data is sensitive, JKL Toy has chosen to allow their sales agents to access the information through secure Client Access Express only.

Using SSL ensures that all traffic for the Client Access Express sessions are encrypted. This keeps data from being read while it is in transit between the local and remote hosts.

For more information about using Client Access Express with SSL, see these resources:

- Secure Sockets Layer Administration
- Securing Client Access Express and Operations Navigator
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

Virtual Private Networks (VPN) for secure private communications

With the rise in the use of virtual private networks (VPN) and the security they provide, JKL Toy company is exploring options to transmit data over the Internet. They have recently acquired another small toy manufacturing company that they intend to operate as a subsidiary of themselves. JKL will need to pass information between the two companies. Both companies use iSeries systems and using a VPN connection can provide the security that they need to communicate between the two networks. Creating a VPN is more cost-effective than using traditional leased lines.

Using VPN connections you can control and secure connections with branch offices, mobile employees, suppliers, business partners, and others.

These are some of the users who could benefit from using VPNs for connectivity:

- Remote and mobile users.
- Home office to the branch office or other off-site locations.
- Business-to-business communications.

Security risks occur if you do not limit user access to sensitive systems. Without limiting who can access a system, you may increase the chances that company information is not kept confidential. You need a plan that will allow only those who need to share information on a system to access that system. A VPN allows you to control network traffic while providing important security features such as authentication and data privacy. Creating multiple VPN connections allows you to control who can access which systems for each connection. For example, Accounting and Human Resources may link through their own VPN.

When you the allow users to connect to system over the Internet, you may be sending sensitive corporate data across public networks, which can expose this data to attack. One option for protecting transmitted data is to use encryption and authentication methods for ensuring privacy and security from outsiders. VPN connections provide a solution for a specific security need: securing communications between systems. VPN connections provide protection for data that flows between the two endpoints of the connection. Additionally, you can use Packet rules security to define what IP packets are allowed across the VPN.

You can use VPN to create secure connections to protect traffic that flows between controlled and trusted endpoints. However, you still must be wary about how much access you provide to your VPN partners. A VPN connection can encrypt data while it travels over public networks. But, depending on how you configure it, a VPN connection may not encrypt data as it flows across the internal networks that communicate through the connection. Consequently, you should carefully plan how to set up each VPN connection. Ensure that you give your VPN partner access to only those hosts or resources on your internal network that you want them to access.

For instance, you may have a vendor that needs to obtain information about what parts you have in stock. You have this information in a database that you use to update web pages on your intranet. You would like to allow this vendor to access these pages directly through a VPN connection. But you do not want the vendor to be able to access other system resources, such as the database itself. Fortunately, you can configure your VPN connection such that traffic between both endpoints is restricted to port 80. Port 80 is the default port that HTTP traffic uses. Consequently, your vendor can send and receive HTTP requests and responses over the connection only.

Because you can restrict the type of traffic that flows across the VPN connection, the connection provides a measure of network level security. However, VPN does not work in the same manner that a firewall does to regulate traffic into and out of your system. Also, a VPN connection is not the only means available to secure communications between your iSeries and other systems. Depending on your security needs, you may find that using SSL is a better fit.

Whether a VPN connection provides the security that you need depends on what you want to protect. Also, it depends on the trade-offs that you are willing to make to provide that security. As with any decision that you make about security, you should consider how a VPN connection supports your security policy.

Chapter 9. Internet security terminology

To establish a basis for discussing Internet security, start by defining some Internet terms. If you are already Internet-literate, you may want to skip this section.

Authentication

Authentication is verification that a remote client or server is actually who they claim to be. Authenticating ensures that you trust the remote peer to which you are connecting.

Cracker

A hacker with malicious intent.

Cryptography

The science of keeping data secure. Cryptography allows you to store information or to communicate with other parties while preventing non-involved parties from understanding the stored information or understanding the communication. Encryption transforms understandable text into an unintelligible piece of data (ciphertext). Decrypting restores the understandable text from the unintelligible data. Both processes involve a mathematical formula or algorithm and a secret sequence of data (the key).

There are two types of cryptography:

- In shared/secret key **(symmetric)** cryptography, one key is a shared secret between two communicating parties. Encryption and decryption both use the same key.
- In public key **(asymmetric)** cryptography, encryption, and decryption each use different keys. A party has two keys: A public key and a private key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. A message that is encrypted with someone's public key can be decrypted only with the associated private key. Alternately, a server or user can use a private key to ″sign″ a document and use a public key to decrypt a digital signature. This verifies the document's source.

Digital certificate

A digital certificate is a digital document that validates the identity of the certificate's owner, much as a passport does. A trusted party, called a Certificate Authority (CA) issues digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. You can use them for the following:

- Identification - who is the user
- Authentication - ensuring that the user is who he says that he is
- Integrity - determining whether the contents of a document have been altered by verifying the sender's digital ″signature″.
- Non-repudiation - guaranteeing that a user cannot claim to not have performed some action. For example, the user cannot dispute that he authorized an electronic purchase with a credit card.

Digital signature

A digital signature on an electronic document is equivalent to a personal signature on a written document. A digital signature provides proof of the document's origin. The certificate owner ″signs″ a document by using the private key that is associated with the certificate. The recipient of the document uses the corresponding public key to decrypt the signature, which verifies the sender as the source.

Digital certificate manager (DCM)
Digital Certificate Manager allows OS/400 to be a local Certificate Authority (CA). You can use DCM to create digital certificates for use by servers or users. You can import digital certificates that other CAs issue. You can also associate a digital certificate with an OS/400 user profile. You also use DCM to configure applications to use Secure Sockets Layer (SSL) for secure communications.

Distinguished name
A distinguished name is the name of the person or server to whom a Certificate Authority (CA) issues a digital certificate. The certificate provides this name to indicate certificate ownership. Depending on the policy of the CA that issues a certificate, the distinguished name can include other authorization information.

Domain name server (DNS)
An Internet host that converts Internet names to IP addresses, often by interacting with other DNS servers on the Internet. For example, many DNS servers might recognize

```
vnet.ibm.com
```

But perhaps only a few know the complete IP address for:

```
system1.vnet.ibm.com
```

When you attach to the Internet, your Internet client uses a domain name server to determine the IP address for the host system with which you wish to communicate.

Encryption
Encryption transforms data into a form that is unreadable by anyone who does not have the correct decrypting method. Unauthorized parties can still intercept the information. However, without the correct decrypting method, the information is incomprehensible.

Extranet
A private business network of several cooperating organizations located outside the corporate firewall. An extranet service uses the existing Internet infrastructure, including standard servers, e-mail clients, and Web browsers. This makes an extranet more economical than the creation and maintenance of a proprietary network. It enables trading partners, suppliers, and customers with common interests to use the extended Internet to form both tight business relations and a strong communication bond.

Firewall
A logical barrier between your internal network and an external network, such as the Internet. A firewall consists of one or more hardware and software systems. It controls the access and flow of information between secure or trusted systems and unsecure or untrusted systems.

Hacker
Any unauthorized person who tries to break into your system.

Hypertext Links
A way of presenting information online with connections—(called hypertext links) between one piece of information (called a hypertext node) and another.

Hypertext markup language (HTML)

The language that is used to define hypertext documents. Use HTML to indicate how your document should look (such as highlighting and type style) and how it should be linked to other documents or objects.

Hypertext transport protocol (HTTP)

The standard method for accessing hypertext documents.

Internet

The worldwide “″network of networks”″ that are connected to each other. And a suite of cooperating applications that allow computers connected to this ″network of networks″ to communicate with each other. The Internet provides browsable information, file transfer, remote logon, electronic mail, news, and other services. The Internet is often called “the Net”.

Internet client

A program (or user) that uses the Internet to make requests of and to receive results from an Internet server program. Different client programs are available to request different types of Internet services. A Web browser is one type of client program. File transfer protocol (FTP) is another.

Internet host

A computer that is connected to the Internet or an intranet. An Internet host might run more than one Internet server program. For example, the Internet host might run an FTP server to respond to requests from FTP client applications. The same host might run an HTTP server to respond to requests from clients using Web browsers. Server programs typically run in the background (in batch) on the host system.

Internet key exchange (IKE)

The IKE protocol, when used with IPSec, supports the automatic negotiation of security associations, as well as the automatic generation and refresh of cryptographic keys. Generally, IKE is used as part of virtual private networking.

Internet name

An alias for an IP address. An IP address is in long numeric form and is difficult to remember, such as 10.5.100.75. You can assign this IP address to an Internet name, such as

```
system1.vnet.ibm.com
```

An Internet name is also called a fully qualified domain name. When you see an advertisement that says, “Visit our home page”, the ″home page address″, includes the Internet name, not the IP address, because the Internet name is easier to remember.

A fully qualified domain name has several parts. For example,

```
system1.vnet.ibm.com
```

has the following parts:

`com`: All commercial networks. This part of the domain name is assigned by the *Internet* authority (an external organization). Different characters are assigned for different kinds of networks (such as `com` for commercial and `edu` for educational institutions).

`ibm`: The identifier for the organization. This part of the domain name is also assigned by the Internet authority, and it is unique. Only one organization in the world can have the identifier `ibm.com`

`vnet`: A grouping of systems within
`ibm.com`

This identifier is assigned internally. The administrator of `ibm.com` can create one or more groupings.

`system1`:
The name of an Internet host within the `vnet.ibm.com` group.

Internet server
A program (or set of programs) that accepts requests from corresponding client programs over the Internet and responds to those clients over the Internet. You can think of an Internet server as a site that an Internet client can access or visit. Different server programs support different services, such as the following:

- Browsing (a "home page" and links to other documents and objects).
- File transfer. The client can request, for example, to transfer files from the server to the client. The files might be software updates, product listings, or documents.
- Electronic commerce, such as the ability to request information or order products.

Internet service provider (ISP)
An organization that provides your connection to the Internet in much the same way that your local telephone company provides your connection to worldwide telephone networks.

Intranet
An organization's internal network that uses Internet tools, such as a Web browser or FTP.

IP address
An Internet Protocol (IP) address is the way that you are known on a TCP/IP network (the Internet is a very large TCP/IP network). An Internet server usually has an assigned unique IP address. An Internet client might use a temporary but unique IP address that is allocated by the ISP.

IP datagram
A unit of information that is sent across a TCP/IP network. An IP datagram (also called a packet) contains both data and header information, such as the IP addresses of the origin and of the destination.

IP filters
IP filtering provides the basic protection mechanism for the firewall. It allows you to determine what traffic passes across it based on IP session details. This protects the secure network from outsiders who use unsophisticated techniques (such as scanning for secure servers) or even the most sophisticated techniques (such as IP address spoofing). You should think of the filtering feature as the base on which the other tools are constructed. It provides the infrastructure in which they operate and denies access to all but the most determined cracker.

IPSec A set of protocols to support secure exchange of packets at the IP layer. IPSec is a set of standards that iSeries and many other systems use to carry out VPNs.

IP spoofing
An attempt to access your system by pretending to be a system (IP

address) that you normally trust. The would-be intruder sets up a system with an IP address that you trust. Router manufacturers have worked to build protections into their systems to detect and reject attempts to spoof.

Network address translation (NAT)
Provides a more transparent alternative to the proxy and SOCKS servers. It also simplifies network configuration by enabling networks with incompatible addressing structures to be connected. NAT provides two major functions. It can protect a public Web server that you want to operate from within your internal network. NAT provides this protection by allowing you to hide your server's ″true″ address behind an address that you make available to the public. And it provides a mechanism for internal users to access the Internet while hiding the private internal IP addresses. NAT provides protection when you allow internal users to access Internet services because you can hide their private addresses.

Non-repudiation
Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to ″sign″ transactions, messages, and documents supports non-repudiation.

Packet A datagram that includes information about the line protocol, such as Ethernet token-ring, or frame-relay.

Proxy Proxy server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and servers on the untrusted network. The proxy server breaks the TCP/IP connection to hide your internal network information (such as internal IP addresses). Hosts outside your network perceive the proxy server as the source of the communication.

Public key infrastructure (PKI)
A system of digital certificates, CA and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Secure Sockets Layer (SSL)
Created by Netscape, the SSL is the de facto industry standard for session encryption between clients and servers. SSL uses symmetric key encryption to encrypt the session between a server and client (user). The client and server negotiate this session key during an exchange of digital certificates. A different key is created for each client and server SSL session. Consequently, even if unauthorized users intercept and decrypt a session key (which is unlikely), they cannot use it to eavesdrop on current, future, or past SSL sessions.

Sniffing
The practice of monitoring or eavesdropping on electronic transmissions. Information that is sent across the Internet might pass through many routers before it reaches its destination. Router manufacturers, ISPs, and operating system developers have worked very hard to ensure that sniffing cannot occur on the Internet backbone. Incidents of successful sniffing are becoming increasingly rare. Most occur on private LANs that are connected to the Internet, rather than on the Internet backbone itself. However, you need to be aware of the possibility of sniffing because most TCP/IP transmissions are not encrypted.

SOCKS

SOCKS is a client/server architecture that transports TCP/IP traffic through a secure gateway. A SOCKS server performs many of the same services that a proxy server does.

Spoofing

The attackers masquerade as a trusted system to try to persuade you to send secret information to them.

TCP/IP

The primary communications protocol that is used on the Internet. TCP/IP stands for Transmission Control Protocol/Internet Protocol. You might also use TCP/IP on your internal network.

Trojan horse

A Trojan horse is a computer program that appears to perform a useful and innocent function. However, it contains hidden functions that use approved authorizations assigned to the user when they start the program. For example, it may copy your internal authorization information from your computer and send it back to the originator of the Trojan horse.

Virtual private network (VPN)

An extension of an enterprise's private intranet. You can use it across a public network such as the Internet, creating a secure private connection, essentially through a private ″tunnel″. VPNs securely convey information across the Internet connecting other users to your system. These include:

- Remote users
- Branch offices
- Business partners and suppliers

Web browser

The HTTP client application. A Web browser interprets HTML to display hypertext documents for the user. The user can access a hyperlinked object by clicking on (selecting) an area of the current document. That area is often called a **hot spot**. Internet Connection Web Explorer, and Netscape Navigator are examples of Web browsers.

World Wide Web (WWW)

A mesh of interconnected servers and clients that use the same standard format for creating documents (HTML) and accessing documents (HTTP). The mesh of links, both from server to server and from document to document, is metaphorically called **the Web**.

Printed in U.S.A.