IBM® SecureWay® FirstSecure

Planning and Integration

Version 2

SCT7-EHNA-00

IBM® SecureWay® FirstSecure

Planning and Integration

Version 2

SCT7-EHNA-00

Note

Before using this information and the product it supports, read the general information under “Appendix. Notices” on page 99.

First Edition (October 1999)

This edition applies to IBM SecureWay FirstSecure Version 2 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this book

IBM® SecureWay® FirstSecure, also known as FirstSecure, is a comprehensive framework that helps your company:

- Secure all aspects of networking through the Web and other networks.
- Build on your current e-business investments. Modular offerings let you add security in a planned deployment.
- Reduce the total cost of ownership for conducting secure e-business.

This book describes FirstSecure, the products that make up FirstSecure, and gets you started planning to use the products.

The products described in this book are part of a staged release. Not all products might be available at the same time or in all countries. Consult your IBM marketing representative about the availability of any of these products.

Figures in this book

The figures in this book are for planning purposes only. Each figure illustrates only one of the countless arrangements of servers, clients, and applications that might be appropriate for your organization.

The format of the figures you see depends on the delivery mechanism of the book:

- Most figures in the Portable Document Format (PDF) version of the book are simpler to save disk space and to print faster.
- Figures in the printed version are more complex and take more storage space and longer printing time.

The figures in both versions are functionally equivalent and have identical captions and alternative text.

Who should read this book

This book is for system administrators who want to plan and integrate security for Web-based systems. You should already understand your network and your e-business applications.

How this book is organized

This book contains the following parts:

- "Part 1. FirstSecure overview" on page 1 gives an overview of FirstSecure, its component products, and the offerings that are available.
- "Part 2. Planning a secure e-business network" on page 15 describes planning for a secure e-business network.
- "Part 3. Installation and integration considerations" on page 53 describes the installation requirements and integration details of the FirstSecure products.
- "Chapter 16. Documentation provided with FirstSecure" on page 87 describes all the documentation available with FirstSecure.
- "Glossary" on page 103 defines security-related terms used in this book.

The book also includes a bibliography describing each product's documentation.

Year 2000

IBM SecureWay FirstSecure readiness is described below..

IBM products in IBM SecureWay FirstSecure

These products are Year 2000 ready. When used in accordance with their associated documentation, they are capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided that all products (for example, hardware, software, and firmware) used with the products properly exchange accurate date data with them.

Other vendor products

Other products have represented to IBM that the products are Year 2000 ready. However, IBM does not itself make any representations nor give any warranty as to the Year 2000 readiness of these products. Contact the manufacturer with any questions regarding the Year 2000 readiness of these products. Information regarding non-IBM products and services are ″Republications″ under the Information and Readiness Disclosure Act based on information supplied by other companies about the products and services they offer. They have represented to IBM that the products are Year 2000 ready. However, IBM does not itself make any representations nor give any warranty as to the Year 2000 readiness of these products. Contact the manufacturers with any questions regarding the Year 2000 readiness of this product. IBM has not

independently verified the contents of these Republications and takes no responsibility for the accuracy of completeness of information contained in such Republications.

Service and support

Contact IBM for service and support for all the products included in the SecureWay FirstSecure offering. Some of these products refer to non-IBM support. If you obtain these products as part of the SecureWay FirstSecure offering, contact IBM for service and support.

Conventions

This book uses the following typographical conventions:

- **Boldface type** indicates the name of an item you select, the name of a command, text a user types, or an example in running text.
- `Monospace type` indicates an example (such as a fictitious path or file name) or text that is displayed on the screen.

Web information

Information about last-minute updates to FirstSecure is available at www.ibm.com/software/security on the Internet at the following locations:

IBM SecureWay FirstSecure
www.ibm.com/software/security/firstsecure

Documentation is available at
www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director
www.ibm.com/software/security/policy

Documentation is available at
www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server
www.ibm.com/software/boundary

Documentation is available at
www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority
www.ibm.com/software/security/trust

Documentation is available at
www.ibm.com/software/securitytrust/library

An ITSO Redbook, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00 is available at www.ibm.com/redbooks on the Internet.

Part 1. FirstSecure overview

This part is an overview of FirstSecure and its component products. It contains a brief description of each product.

This part also describes the IBM Implementation Services.

Chapter 1. What is FirstSecure?

IBM SecureWay FirstSecure is part of the IBM integrated security solutions. FirstSecure is a comprehensive set of building blocks that help your company:

- Establish a secure e-business environment.
- Reduce the total cost of security ownership by simplifying security planning.
- Implement security policy more easily.
- Create a more effective e-business environment.

The FirstSecure components include virus protection, intrusion detection, access control, traffic content control, encryption, digital certificates, firewall technology, and application development toolkits. These functions are delivered by the IBM SecureWay family of security products as well as through offerings from other vendors, combining the best components of several security vendors. Additionally, Implementation Services are available for selected FirstSecure components. The FirstSecure building blocks are:

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure, provided through IBM SecureWay Trust Authority
- IBM SecureWay Toolbox

Because FirstSecure is a collection of products that can be installed independently, you can launch a planned move toward a secure environment. You can start in one area, test your improvements, and then continue to move toward more security. This reduces complexity and costs, and speeds deployment of Web applications and resources.

Why do you need FirstSecure ?

Your data and resources are vital to your e-business. Together, the products in FirstSecure provide:

Authorization
: Everybody has to follow the rules. Authorization admits only approved user access to your systems, data, applications, and networks.

Accountability
You can tell who did what when. Accountability lets you determine who did an action and which actions occurred during a specified time interval.

Assurance
You can be assured the system keeps its security promises. This protection lets you demonstrate and validate that the claimed level of security protection is enforced.

Availability
The system is there when you need it. This protection helps you keep your systems, data, networks, and applications usable by your employees, suppliers, partners, and customers.

Administration
You can define the rules. This protection lets you define, maintain, monitor, and modify policy information.

You can implement these protections based on corporate-wide policies to provide a protective mesh across the entire set of networks, systems, and applications in your enterprise. The presence of one vulnerable link between products in that mesh could render the remaining infrastructure useless.

This book ties each of the SecureWay building block products into the list of protections provided.

What are the FirstSecure building blocks?

FirstSecure contains component products that you can obtain as one group of all products or as separate, related products. These products, in turn, may have one or more component products. You can start with any product and build to a complete security solution.

Policy Director

Policy Director is the central focus of your security planning. Policy Director provides authorization and management for end-to-end security of Web resources over geographically dispersed intranets and extranets. Policy Director provides authentication, authorization, data security, and resource management. Use Policy Director along with standard Internet-based applications to build secure and well-managed intranets. Policy Director includes:

- Security Services
- Management Console
- Management server

- Security Manager (NetSEAL and WebSEAL)
- NetSEAT client
- Directory Services Broker
- Authorization server (third party application support)

Policy Director runs on Windows NT, AIX, and Solaris.

See "Chapter 5. Planning for Policy Director in your network" on page 31 for a more complete description of Policy Director.

SecureWay Boundary Server

The SecureWay Boundary Server products provide assurance, administration, and accountability for Web-based e-business applications. Secure boundaries are needed everywhere—between departments such as engineering and human resources, between headquarters networks and remote offices, between your company's network and the Internet, between your company's Web applications and customers, and between your company's network and business partners. Proper boundary security requires controlling both who can access your network and what information is entering and leaving your network.

This section describes the building blocks of the SecureWay Boundary Server. See "Chapter 12. SecureWay Boundary Server requirements and installation considerations" on page 59 for planning and integration considerations.

IBM SecureWay Firewall

The IBM SecureWay Firewall, also called IBM Firewall, enables safe, secure e-business by controlling all communications to and from the Internet. IBM Firewall provides the three critical firewall functions—filtering, proxy, and circuit level gateway—to give you a high level of both security and flexibility.

ACE/Server

The ACE/Server, from Security Dynamic, includes SecurID tokens (2 user licenses and 2 tokens). The ACE/Server adds an administrator logon and a *virtual private network* (VPN) connection to the IBM SecureWay Firewall.

MIMEsweeper for IBM SecureWay Release 2

MIMEsweeper, from Content Technology, includes components for Internet security. MAILsweeper checks e-mail to assure that no confidential information leaves your e-business, and that no unpermitted e-mail comes in.

WEBsweeper keeps unwanted Web material from entering your business. It scans for and accepts data only from permitted Java applets, executable code, or Web sites.

SurfinGate

SurfinGate, from Finjan Software Ltd., is a mobile code security solution for e-business. Because mobile code is now often pushed automatically and routinely into your e-business network from outside your intranet, you need more protection than firewalls. SurfinGate protects your network from attacks from Java, ActiveX, and JavaScript code. It identifies potential hostile attacks, away from critical resources, before they enter your network. It quarantines suspicious data for you to inspect before accepting it.

Intrusion Immunity

Intrusion Immunity provides Assurance in the form of enterprise detection and protection products. See “Chapter 13. Intrusion Immunity requirements and installation considerations” on page 67 for a Intrusion Immunity requirements. Intrusion Immunity includes Tivoli Cross-Site for Security and Norton AntiVirus.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security provides intrusion detection for systems that might be vulnerable to attack. With Tivoli Cross-Site for Security you can:

- Install Cross-Site for Security agents in your network to report suspicious incidents to the Cross-Site for Security management server.
- View intrusion data in pre-defined and custom reports.
- Detect and log unauthorized or suspicious activities in real time.
- Tune the security agents to reduce the number of false alarms.

Norton AntiVirus

Norton AntiVirus, a product of the Symantec Corporation, is one of the world’s leading antivirus software products. Norton AntiVirus can run constantly in the background to help keep your computers safe from viruses that might come in e-mail attachments, ActiveX controls, Java applets, Internet downloads, diskettes, software CDs, or files sent through a network. With Norton AntiVirus you can quarantine infected files. You can configure Norton AntiVirus to automatically inform you of updates and of newly discovered viruses.

Public Key Infrastructure

IBM FirstSecure supports Public Key Infrastructure (PKI) standards for cryptography and interoperability by providing IBM SecureWay Trust Authority.

SecureWay Trust Authority is a security solution supporting the issuance, renewal, and revocation of digital certificates. These certificates can be used in a wide range of Internet applications, providing a means to authenticate users and to ensure trusted communications. Trust Authority is based on the *Internet Engineering Task Force's* (IETF) *Public Key Infrastructure* (PKI) Working Group specifications. It includes:

- Support for IBM AIX and Microsoft Windows NT servers
- A registration authority (RA)
- A certificate authority (CA)
- User interfaces for requesting certificates and administering issued certificates
- An integrated *IBM SecureWay Directory*
- An *audit* subsystem
- Support for the SecureWay 4758 cryptographic coprocessor
- Support for *Smart Cards*

This infrastructure supports the complete certificate life-cycle, including enrollment and initial certification, key-pair update, certificate renewal, certificate and certificate revocation list publication, and certificate revocation. See "Chapter 14. Public Key Infrastructure requirements and installation considerations" on page 75 for more information.

Toolbox

The FirstSecure Toolbox is a set of security and security-related toolkits that are either part of or interoperable with the major components of FirstSecure. The toolkits help you:

- Integrate your applications with FirstSecure.
- Customize solutions and applications using FirstSecure.
- Create ISV and OEM applications that exploit FirstSecure.

The FirstSecure Toolbox toolkits APIs support the following security functions:

- Authorization services
- Certificate and management services
- Directory services
- Secure Sockets Layer protocol services

- KeyWorks cryptographic and trust management services
  - IBM Key Recovery Service Provider 1.1.3.0 APIs. The IBM Key Recovery Service Provider enables the recovery of encrypted information.
  - IBM Key Recovery Server 1.1.3.0. The IBM Key Recovery Server 1.1.3.0 is an application that, upon authorized request, can recover encrypted information when keys are unavailable, lost, or damaged.

    These two toolkits provide standard interfaces that applications can use to invoke critical security services as well as standard interfaces that security providers can use to plug into the toolkit. The standard interfaces are based on the Common Data Security Architecture (CDSA). These toolkits are available on Windows NT, Solaris, and AIX.

Implementation Services

FirstSecure Implementation Services can help your e-business get FirstSecure up and running quickly and efficiently. These separately billable services are provided by IBM and are performed by an experienced team of consultants. The FirstSecure Implementation Services include a FirstSecure Implementation Workshop and product level QuickStart installation services. IBM can also provide FirstSecure system integration services that are customized to your individual environment.

Contact your IBM representative for information and pricing options.

Chapter 2. What's new in Release 2

Release 2 simplifies the planning and installation of the IBM SecureWay FirstSecure products. The individual products are more integrated, products have been added, and management and control are more centralized.

Policy Director

The Policy Director has the following enhancements:

- Support for the IBM SecureWay Directory for the storage of user and group credential information.
- The latest updates to the Authorization API specification from the Open Group.
- Ability to define and edit IBM Firewall proxy user credentials using the Policy Director Management Console.
- A Policy Director Credentials Acquisition Service (CAS) that provides support for the use of external authentication services.
- Support for client-side certificate-based authentication using the new Policy Director Credentials Acquisition Service.
- The ability to write your own customized credentials acquisition service using the Interface Definition Language (IDL) interface between WebSEAL and the Policy Director CAS. Policy Director also provides the general server framework that handles Policy Director CAS server functions, such as startup, server registration, and signal handling.
- The choice of using a secure sockets layer (SSL) tunneling mechanism in addition to generic security services (GSS) tunneling.
- Use of the Policy Director Management console, or command line interface, to manage login and password policies.
- Use of the Policy Director Management Console, or command line interface, to manage single sign-on users, groups, and resources (targets).
- A Web-based single sign-on target password management tool.
- An integrated installation process.

SecureWay Boundary Server

The SecureWay Boundary Server has the following enhancements:

- A configuration GUI tying together some functions of SecureWay Boundary Server and Policy Director.

- A new configuration TaskGuide tying together some functions of SecureWay Boundary Server and Policy Director.

What's new in IBM SecureWay Firewall for AIX and NT

The IBM SecureWay Firewall, also called the IBM Firewall, has the following enhancements:

Secure mail proxy enhancements

The IBM Firewall Secure Mail Proxy has been enhanced to include the following new functions:

- Anti-SPAM algorithms including message blocking from known SPAMers (an exclusion list), verification checks on the validity and replyability of messages (known ways of blocking undesirable messages), configurable limits on the number of recipients per mail messages, configurable limits on the maximum size of a message
- Anti-spoofing support including integration with strong authentication mechanisms
- SNMP trap support and support for the MADMAN MIB
- Message tracking including the ability to seamlessly track messages between the firewall and Domino

Socks protocol version 5 enhancements

Socks protocol version 5 has been upgraded to include username-password authentication (UNPW), challenge/response authentication (CRAM), and authentication plug-ins.

Logging has been enhanced to give the user more control in classifying log messages and in specifying logging levels.

HTTP Proxy

The IBM SecureWay Firewall provides a full-featured HTTP proxy implementation based upon the IBM Web Traffic Express (WTE) product. The HTTP proxy efficiently handles browser requests through the IBM Firewall, eliminating the need for a socks server for Web browsing. Users can access useful information on the Internet, without compromising the security of their internal networks and without altering their client environment to implement HTTP proxy.

Remote Access Service

Windows NT Remote Access Service (RAS) provides network connections over dial-up, ISDN, or X.25 media using Point-to-Point Protocol (PPP). NDISWAN is a networking driver which is provided as part of RAS and converts the underlying PPP data to resemble Ethernet LAN data.

IBM SecureWay Firewall Enhancements for AIX

The IBM SecureWay Firewall for AIX offers numerous extensions:

Enhanced IPSec Support

Enhanced IPSec support including support for new headers. It also supports interoperability with several IBM servers and routers as well as many non-IBM VPN products that support the new headers.

Multi-Processor (MP) Support

Firewall users can exploit the multi-processor features of the RS/6000 for scaling and performance improvements.

Filters Enhancements

Better performance and more flexibility with configuration. You can tune the performance of your IBM SecureWay Firewall by choosing where to locate different types of filter rules.A frequency indicator provides the number of times a connection is used.

Network Address Translation

Support for many-to-one address mappings. These mappings are from multiple internal unregistered or private addresses to a registered legal address using port numbers to create the unique mappings.

Setup wizard

A wizard helps with the initial configuration of the IBM Firewall. This setup wizard enables a user, who does not have extensive knowledge of the IBM Firewall, to have a basic configuration up and running quickly after installation.

Network Security Auditor

The Network Security Auditor (NSA) checks your network servers and the IBM Firewall for security holes or configuration errors. It is faster and more robust.

What's new in MIMEsweeper for IBM SecureWay Release 2

MAILsweeper enhancements include:

- Scanning for key words to block harassing or libelous mail and to protect valuable data from leaving your company
- Blocking incoming junk e-mail
- Blocking individuals or groups from sending or receiving specified types of files
- Blocking or delaying files by size to avoid network contention

WEBsweeper enhancements include:

- Blocking employees from specified sites likely to be non work-related
- Helping prevent attacks to extract documents through HTML or e-mail address and site information through cookies

What's new in SurfinGate

SurfinGate has the following enhancements:

- JavaScript content inspection
- Mission-critical performance monitoring
- Increased policy management
- Support for File Transfer Protocol (FTP) and HTTPS protocols
- Plug-in integration with firewall HTTP proxy
- The ability to block or specific executable files from being downloaded into a user's computer

Intrusion Immunity

The Intrusion Immunity products now include Tivoli Cross-Site for Security.

What's new in Tivoli Cross-Site for Security

The Tivoli Cross-Site for Security provides intrusion detection. It lets you monitor network attacks on the integrity of your e-business.

What's new in Norton AntiVirus Solution Suite

The Norton AntiVirus Solution Suite, Release 3.0.4, includes the following updated versions:

- Norton AntiVirus 5.02 for Windows 95/98 and Windows NT Workstation
- Norton AntiVirus 5.02 for Windows NT Server
- Norton AntiVirus for IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 for Lotus Notes 2.0
- Norton AntiVirus for Lotus Notes 2.0
- Norton AntiVirus for Microsoft Exchange 1.5.2

Public Key Infrastructure

The Public Key Infrastructure component now includes Trust Authority.Trust Authority includes:

- An installation wizard to guide you through a simple installation on Windows NT.

- A pre-set configuration for the 4758 cryptographic card. You can change this information.
- A configuration wizard that checks validity of data before the background configuration programs begin.
- Error messages and reporting.
- Online documentation, including context-sensitive help for the Setup Wizards, Registration Authority Desktop, and an end-entity client application.

IBM SecureWay Toolbox

The Toolbox has the following enhancements:

- Policy Director APIs and documentation.
- Directory service APIs.
- Public Key Infrastructure (PKIX) APIs and documentation.
- The IBM Key Recovery Server 1.1.3.0 is now included in the Toolbox. It is available only in English.

Part 2. Planning a secure e-business network

Part 2 discusses planning for a secure e-business network.

The following chapters describe typical Internet traffic and security concerns and then they tell how the FirstSecure products work in your e-business network.

This section contains the following chapters:

- "Chapter 3. An e-business network overview" on page 17 describes a typical e-business network and the kinds of users, resources, and interactions that exist in a network. Your network may have more or fewer features, but you have the same security concerns and need the same security protection.
- "Chapter 4. Planning for FirstSecure in your e-business network" on page 29 ties the FirstSecure products into the network.
- "Chapter 5. Planning for Policy Director in your network" on page 31
- "Chapter 6. Planning for SecureWay Boundary Server in your network" on page 35
- "Chapter 7. Planning for Intrusion Immunity in your network" on page 41
- "Chapter 8. Planning for Public Key Infrastructure in your network" on page 47

Chapter 3. An e-business network overview

Your e-business network is made up of resources: data and data bases, users, customers, suppliers, programmers, hardware, company information, and so on. Let's look at some of these areas and see where you need security.

The Internet is a complex creation. Data travels through it from server to server and from user to user, in undefined paths that change from transmission to transmission.

Your business data transmissions across the Internet are mixed in with all the other Internet traffic. Along the way, data vital to your business might have passed through any server anywhere. And any Internet user may have tried to access your resources, your employees, and your data. Unfortunately, in addition to legitimate traffic for education, business, and pleasure, the Internet also carries malicious traffic, both innocent and deliberate. Figure 1 on page 18 is an overview of the Internet with your traffic passing through the Internet filled with everyone else's traffic.

FirstSecure helps you separate and secure your transmissions from all other traffic.

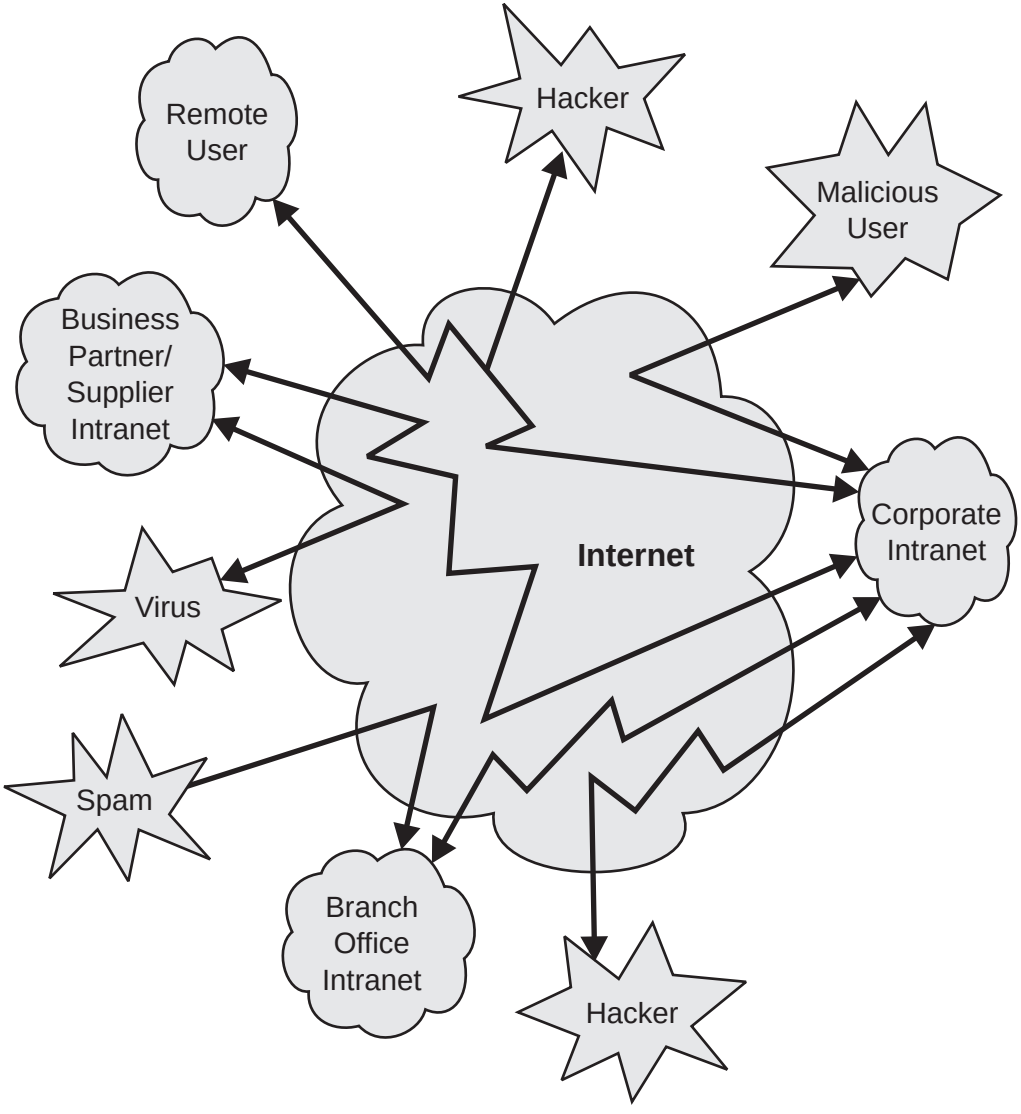


Figure 1. Overview of busy Internet with unrelated activity

You do not want to operate in this view of the Internet. You want the view in Figure 2 on page 19, an Internet made secure by FirstSecure.

The ideal Internet protected by FirstSecure

Much of your e-business traffic goes through the Internet. But, you do not want the typical view of the Internet as a vast collection of random data visible to almost anyone with a home computer. Figure 2 shows the Internet you want.

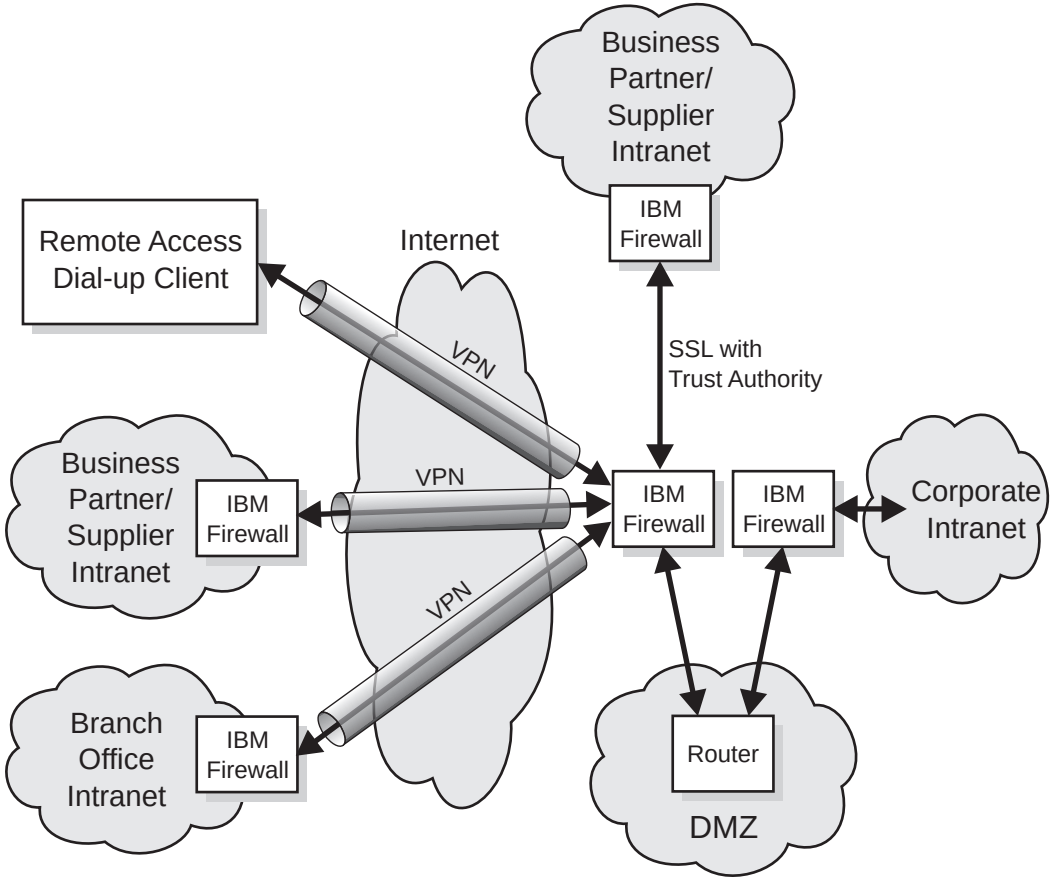


Figure 2. The Internet you want

While there is much good information available through the Internet, there are applications, data, and accesses you want to shield your business from. You want to make sure

- Your employees are not distracted from their assigned tasks.
- Your employees are protected from inappropriate e-mail.
- Your sensitive business information stays within your business.

The Virtual Private Network

A virtual private network (VPN) is the concept of a private connection, inaccessible to others, through the Internet. Figure 3 shows a typical VPN. The connection is, to the users at each end, secure from intrusion by unwanted users or applications. FirstSecure products, such as IBM SecureWay Firewall help you set up and support VPNs.

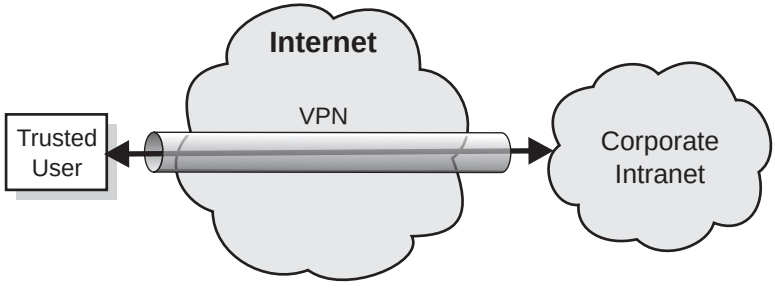


Figure 3. A typical virtual private network.

The demilitarized zone

The *demilitarized zone* (DMZ) is the body of resources that you allow outside users to access. You use IBM Firewall, MIMEsweeper, and other FirstSecure products to make sure that only users you want can access the DMZ, and that they can access only specified resources. Traffic into and out of the DMZ should be monitored for appropriateness.

Your company's catalog might be in the DMZ for any potential customer to browse through. Or, you might have informational brochures describing your company. Your FirstSecure components let only your trusted users access information beyond your DMZ.

Figure 4 on page 21 shows a typical DMZ.

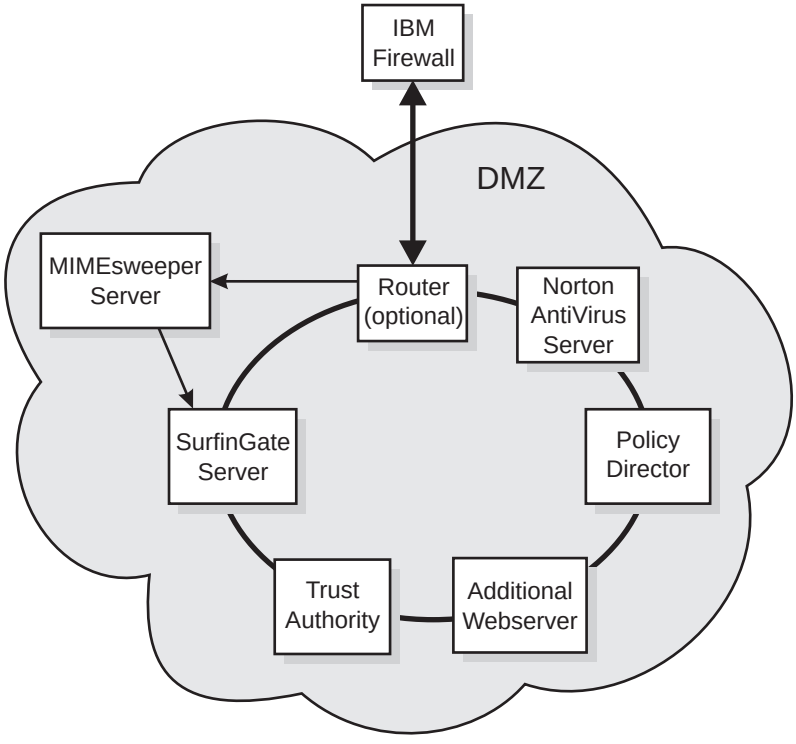


Figure 4. Typical DMZ with system resources

As you develop your secure applications, you can use the DMZ as an intranet test bed before you grant public access to those applications.

Now let's look at the kinds of information you use the Internet and your intranet for.

A typical corporate intranet

Your corporate intranet is where your company communicates within itself. It contains information and resources you do not share with the Internet. Your employees share data, send e-mail to each other, access corporate resources such as databases, printers, and scanners. Figure 5 on page 22 shows a typical corporate intranet.

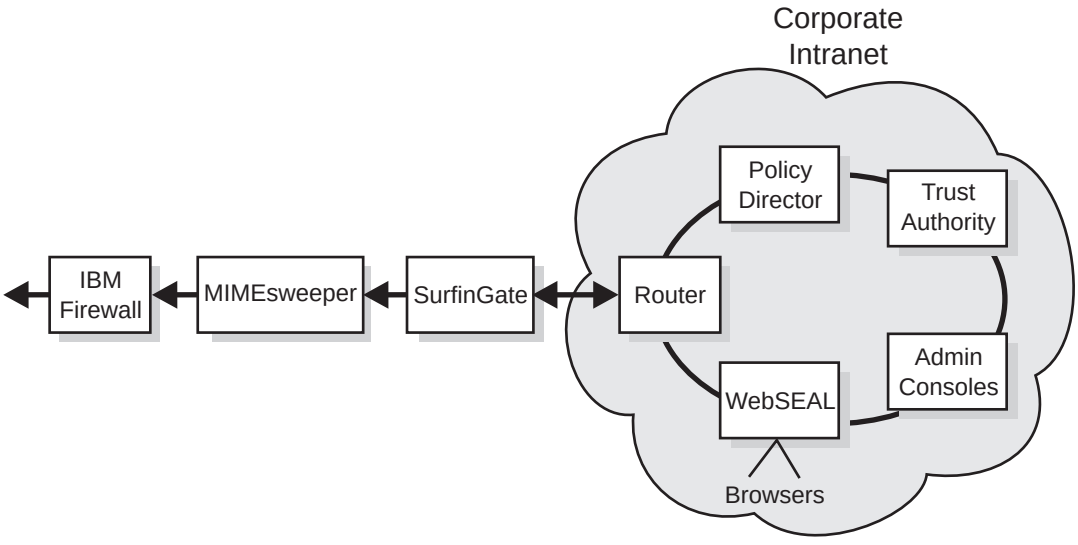


Figure 5. Overview of typical corporate intranet

You must make sure that your company confidential information stays within your company and that only the people allowed to do so can access that data. However, you have some data that you do want customers to use and access. For example, you want a depositor in your bank to be able to check an account balance, but you do not want that depositor to access employment records. Your IBM Firewall keeps your private information private.

IBM FirstSecure products help you keep your intranet secure. The Policy Director lets you set the access rules. IBM SecureWay Trust Authority makes sure users are who they claim to be. The Tivoli Cross-Site for Security lets you know if there are unauthorized attempts to access your intranet resources.

A typical corporate branch office intranet

Eemote employees here in your branch offices need access to the same data and other resources as your in-house employees. But, telephone connections for sending and receiving information are slow and unprotected from malicious interference. You want to use the Internet as a cost-saving measure and as a means of adding protection to your transactions. Figure 6 on page 23 shows a typical branch office communicating through the Internet to a central office.

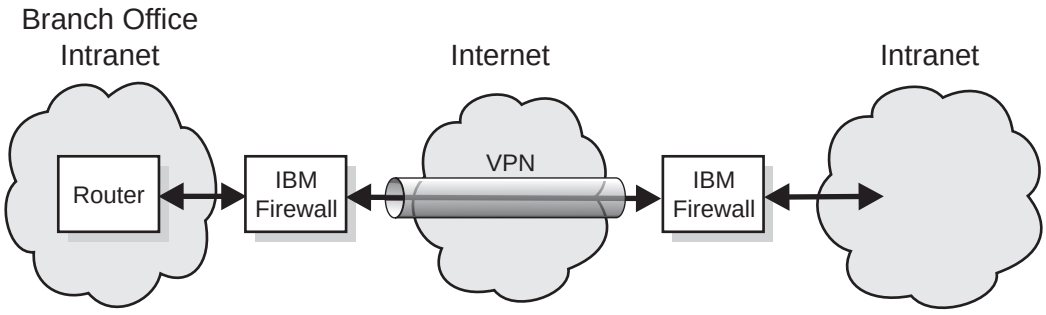


Figure 6. Branch office connected to a main office through a virtual private network

You want your transmissions and data to be as secure as if they were in one place within your enterprise. The *virtual private network* (VPN) is your tunnel through the Internet. You use the Internet as if it were your private intranet network.

A typical remote-access employee

Some of your employees may, at times or permanently, work remotely from your main office. An employee may access your network through the Internet with a dial-up or leased connection.

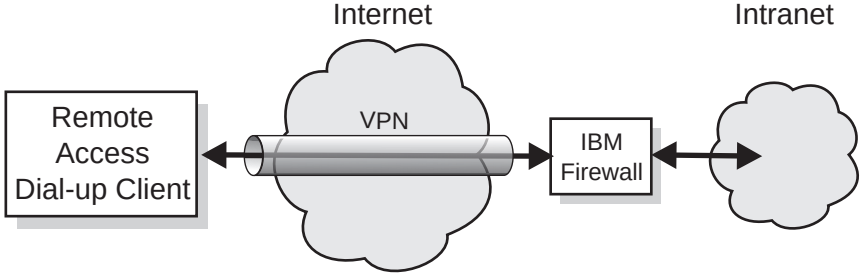


Figure 7. Remote access dial-up client connected to a main office through a virtual private network

The IBM Firewall protects this employee's transmissions.

A typical business partner or supplier intranet

Your business is more efficient when your business partners and suppliers can access some of your data directly. One supplier may be authorized to check inventory levels and to send new stock at specified levels. Another business partner may have access to selected records. An accounting firm might need access to other tax records but not to the business partner's records. Figure 8 on page 24

on page 24 and Figure 9 show a typical supplier or business partner. You want the business transactions to traverse the Internet as if traveling through a private connection.

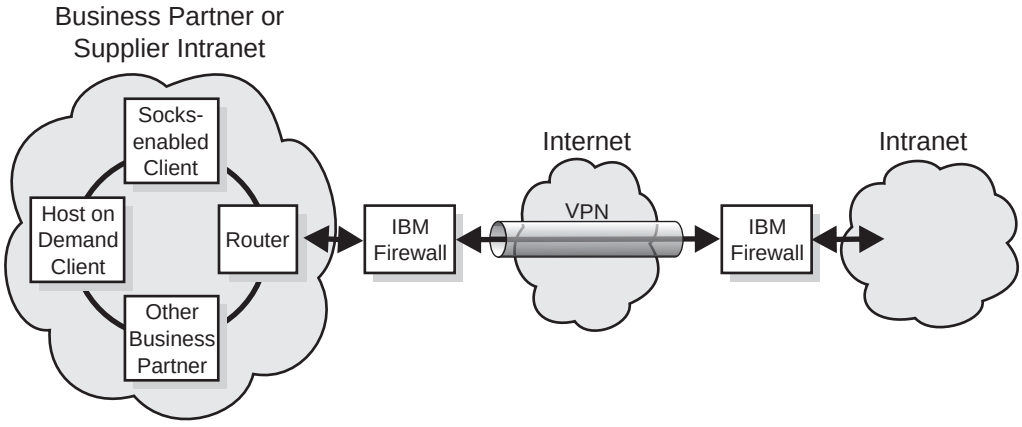


Figure 8. Typical business partner or supplier intranet using a virtual private network (VPN)

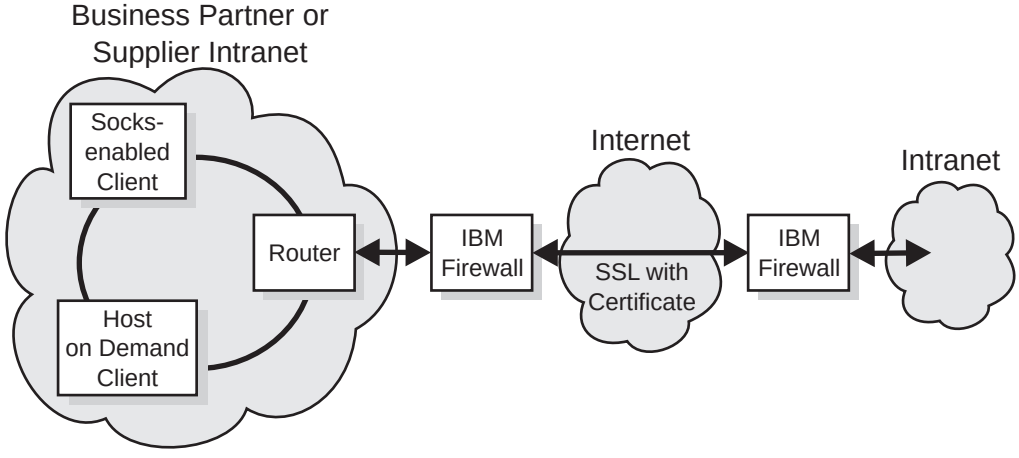


Figure 9. Typical business partner or supplier intranet using a Secure Sockets Layer (SSL) transmission protocol

This business partner is using Secure Sockets Layer (SSL) instead of using a VPN because the transmissions are encrypted from end to end. (The user could also use a VPN for an additional layer of security.)

You need to protect these users from each other, malicious interference, and from intruders. You need to protect their data transmissions from unauthorized listeners and from unauthorized senders. You also need to

ensure that these users access only the data you want to be accessible. And you want to make sure each of these users is the user that you expect.

Data and data bases

Data is one of the most valuable resources any business has. Some e-business data is designed to be available to all Internet users. For example, a hardware distributor might have his inventory and pricing list available for online shopping. A clothes retailer could have an illustrated online catalog of styles, colors and sizes for online shopping.

Before you grant access to data, you need to know who the requester is, and why the data is wanted. Use the Trust Authority to issue certificates to trusted users.

Other areas to protect

This book does not cover countermeasures for other areas of security. You also have to plan for:

- Site security, access and egress, and compartmentalization
- Physical security of laptop computers, personal computers and workstations, and other containers
- Personal security background checks
- Legal disclaimers of liability, contracts, and such
- Operational practices such as key management, information control, and security awareness and training

The operating system

Most operating systems are configured for high availability and for a rich set of functions. An effective secure approach would be to have only the minimum function necessary to do a given task. You should consider uninstalling or disabling all operating system features that you would not want an intruder to access.

Typical users

The Internet has many different kinds of users, some desirable, some not. An e-business wants users who are customers making online searches and purchases. And e-business also wants business partners to be able to access specific data to check inventory, make manufacturing decisions, or to comment on plans and activities within the business. The e-business also wants employees to be able to access the data they need to do their assigned tasks.

The Internet also has users that an e-business does not want: the hackers and spammers, the spreaders of viruses, the users who want access to your sensitive data. These users might even be within your e-business.

Before you grant access to any resource, you need to know who the requesting user is, what access that user should have to data and applications, and what records of user access should be kept.

Applications and application creation

Applications can be designed to include security. You can take advantage of encryption of data to be transmitted, certification of users asking for access, audit logs of users and transactions.

The Toolbox APIs let you add security to your applications.

Hardware security

Servers and data banks are part of a secure system. Although this book does not cover hardware, you need to plan for the physical security of servers and of workstations used for managing security.

Trust Authority hardware security

Although this section specifically covers the Trust Authority component, the considerations are applicable to all the FirstSecure components.

Isolate the area

Set up the server in an isolated room dedicated to CA activity. If possible, the room should have reinforced walls, a single solid-core wood or steel door, and a solidly constructed ceiling with no drop panels. The room should also have a raised floor to protect against discharges in the event of a fire.

Maintain the area

The room should provide an uninterruptible power supply for the computers, light fixtures, motion detectors, and heating and cooling systems. You should also audit the room's ventilation to ensure that the temperature is sufficient to combat the heat that is generated by the equipment.

Control access to the area

You can provide access to the physical area in a number of ways, for example, by using badges, or keypad-controlled door locks. To prevent malicious tampering by a single individual, you should install controls that require the presentation of proper credentials by at least two trusted individuals.

You should also monitor the room to track each time the secure area is accessed and by whom. For maximum security, install motion detectors both inside and outside the door.

Control communications

There should be no spare open ports on the Trust Authority server. You should configure the system so that it listens for requests only on those ports that are explicitly assigned to active Trust Authority applications.

Follow your own business's procedures and requirements for securing the hardware used in your e-business.

Chapter 4. Planning for FirstSecure in your e-business network

The following chapters in this part tie the products included in FirstSecure to your e-business. The chapters build on the illustrations in “Chapter 3. An e-business network overview” on page 17. Each product is described in some detail. For complete information about a product, refer to the documentation accompanying the product. The deployment scenarios are only suggestions.

In each deployment scenario, you follow the same basic steps:

1. Have all parts of your network use a common time reference to make auditing logs simpler and more accurate.
2. Start within your intranet to install and test components.
3. Once you are comfortable within your intranet, start building applications within your secure demilitarized zone (DMZ).
4. Traffic between your intranet and the demilitarized zone should pass through a firewall.
5. Build your external Internet applications and test them with test data.
6. Install a firewall to protect traffic between the Internet and your DMZ.
7. Let users access your network.

Planning a complete FirstSecure system

Here is a suggested order for deploying the FirstSecure products in your network. It is greatly simplified. See “Part 3. Installation and integration considerations” on page 53 for the detailed hardware and software requirements for each product and for integration considerations. Also, read the installation requirements and instructions that accompany each product. Many products also have up-to-date information available on the Internet. “Web information” on page xi lists the Web sites with FirstSecure information. The Redbook, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498 contains several more detailed scenarios.

1. Plan the security requirements you will need.
2. Install the Policy Director to meet those requirements.
3. Create and test your customer server application. Keep it within your corporate intranet for now, do not make it available on the Internet yet.
4. Install the IBM Firewall that protects the customer server application.
5. Add SurfinGate to the DMZ.

6. In your demilitarized zone (DMZ), add MIMEsweeper and Norton AntiVirus to protect your applications when you make them available on the Internet. When you make them available for external traffic, configure them to point to your servers.
7. Install the Tivoli Cross-Site for Security product for intrusion immunity and detection.
8. Within your DMZ add:
   - Web servers
   - Web catalog server
   - Web inventory server
   - Customer client applications
   - Secure customer client applications
   - One or more Cross-Site for Security agents

   Test all your applications within the firewall before opening them to traffic. Use the SecureWay Boundary Server's Network Security Auditor tool to test the rules you have set.
9. Install an instance of the IBM SecureWay Firewall to protect the software within your DMZ. Your default configuration should be "No traffic" so that you can test the installation before opening it to the public.
10. Install Trust Authority and issue certificates to trusted users.
11. Open your application to the Internet after all testing is completed.
12. Run the Network Security Auditor from outside your system to test the rules before announcing access to the public.
13. Check the audit logs created by the FirstSecure component programs to make sure there have been no untoward incidents.
14. Continue to check audit logs and add Cross-Site for Security agents as you add applications to your network.

Chapter 5. Planning for Policy Director in your network

FirstSecure gives you a consolidated, policy-driven point of control for heterogeneous Web environments. In environments where users access multiple back-end Web servers through browsers, the Policy Director provides

- A single sign-on for each Web user
- Identification verification
- Authorization checking of users requesting access to protected Web pages

With this support, you can authorize and secure:

- TCP/IP exchanges, such as HTML, Telnet, and POP3
- Third-party applications such as database systems
- Network management tools
- Applications developed in-house

With FirstSecure, users can authenticate to the Policy Director using the following mechanisms:

- Basic authentication over Secure Sockets Layer (SSL)
- Forms-based login over SSL
- SSL using client certificates
- Kerberos login

FirstSecure then controls the access of authenticated users to individual Web objects and network services and can limit unauthorized users to a subset of these resources.

Policy Director deployment

Policy Director manages the mapping between users and groups and resources. You use the Policy Director management console to:

- Define the users and groups who will use your resources.
- Define the objects needing protection. Objects might be the Web, TCP ports, methods, and interfaces.
- Define how users will access the resources and what the rules protecting the resources will be, such as read, modify, administer, run, or delete.

The following table describes the common Policy Director component configurations. Determine the appropriate configuration for your network. Then select those components during installation.

Refer to *IBM SecureWay Policy Director Up and Running* for more detail.

Configuration Example	Installed Components
A server running the single instance of the Management server for the secure domain. In this scenario, the Management server resides by itself on its own system. The Management server maintains the master authorization database for the secure domain, replicates this database throughout the secure domain, and maintains location information about other Policy Director server machines in the secure domain.	Management server only
A WebSEAL server. This scenario represents the solution for protecting a Web space. WebSEAL supports back-end servers, for high availability and fault tolerance.	Security Manager with WebSEAL
A NetSEAL server. This scenario represents the solution for securing a Virtual Private Network (VPN) and provides access control for legacy and third-party network services.	Security Manager with NetSEAL
A combination WebSEAL and NetSEAL server.	Security Manager with WebSEAL and NetSEAL
A server that provides access to the Policy Director Authorization Service for third-party applications.	Authorization server
A server that provides a development environment for developers who want to build third-party applications that use the authorization API.	Authorization server and ADK
A server providing the combined services of all the above configurations.	All components

Policy Director is a highly-distributed security system that can deploy its components in a variety of configurations on one or more machines. The following is an overview of deploying Policy Director in your network. Complete installation instructions are in *IBM SecureWay Policy Director Up and Running*.

1. Install the Policy Director security server.

   At least one computer in the secure domain must contain the Policy Director security server to set up a Policy Director secure domain. Refer to the installation and administration manuals and technical support resources for your required platforms.

Remaining servers can function with only DCE client installations (or NetSEAT on Windows NT systems).

2. Install the SecureWay Directory (LDAP) server.
3. Install Policy Director.
   - The Policy Director security server must be deployed first (see step 1 on page 32).
   - All Policy Director server installations require Policy Director Base.
   - If this is the *first* or *only* machine in the secure domain, you must install the Management server.

     If this is an *additional* machine in an existing secure domain with an existing Management server, do not install another Management server. There must be only one instance of the Management server in any given secure domain.
   - WebSEAL, NetSEAL, and third-party authorization server components are optional.
   - The Security Manager combines with WebSEAL to provide the WebSEAL HTTP server component and fine-grained HTTP access control, and with NetSEAL to provide the NetSEAL coarse-grained TCP/IP access control component.
4. Install the Management Console.

   The Management Console requires that you install either a DCE client (or NetSEAT for Windows NT) on the operating system (see step 1 on page 32).
5. The following dependencies apply to applications that are developed with the Authorization ADK:
   - You require the Policy Director package.
   - Install IVAuthADK on the application machine.
   - The operating system on which the application runs must have either a DCE client or NetSEAT for Windows NT systems.
   - The secure domain running an application must have an Authorization server installed on at least one computer in the secure domain. A typical development environment includes the Authorization server on the same operating system as the Authorization ADK.

Chapter 6. Planning for SecureWay Boundary Server in your network

FirstSecure provides security for Web-based applications that take advantage of existing security standards such as Secure Sockets Layer (SSL), SOCKS, and IPSec.

If your operating environment includes connections between two parts of the network with different trust characteristics, the SecureWay Boundary Server component of FirstSecure can help you address the following requirements:

- Safe connections to the Internet, minimizing the possibility of unauthorized access to your private network
- Large-scale extranet infrastructures for selectively sharing data with business partners and vendors
- Use of the Internet or other relatively untrusted network segments as a virtual private network (VPN), with messages kept confidential as they pass through the untrusted network's infrastructure

FirstSecure's SecureWay Boundary Server uses network address filtering, content filtering, proxy, and circuit-level gateway technologies. Through the combination of these technologies, SecureWay Boundary Server enables policy-driven, safe, secure e-business operations by controlling communications between networks with different trust characteristics.

SecureWay Boundary Server includes:

- IBM SecureWay Firewall, including ACE/Server
- MIMEsweeper for IBM SecureWay Release 2
- SurfinGate 4.05 for Windows NT
- Enhancements for policy management

See Figure 10 on page 36 for an overview of data flow in a complete SecureWay Boundary Server installation.

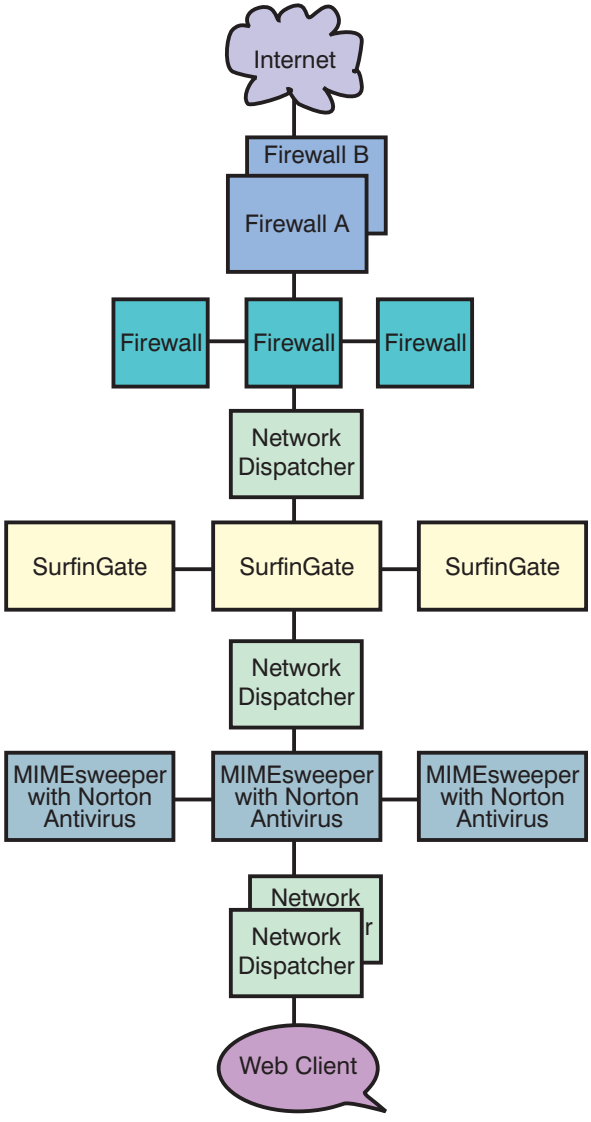


Figure 10. Overview of a data flow in SecureWay Boundary Server products

IBM SecureWay Firewall deployment

IBM SecureWay Firewall, also known as IBM Firewall, controls communications to and from the Internet. This firewall technology protects IBM's own assets.

See "SecureWay Boundary Server component considerations" on page 61 for installation considerations.

Among your networking concerns are:

- The need to connect to the Internet but prevent unauthorized access to your network, applications, and data
- Abuse of your networking assets by internal users
- Ways to plan a large-scale extranet infrastructure for business partners and vendors despite the high cost of configuration management
- The high cost of leased lines connecting branch offices
- Poor business productivity caused by ineffective, late, or misunderstood communications with partners and vendors
- The high administrative cost of managing software in non-native languages

IBM Firewall addresses these concerns. By allowing only explicitly permitted traffic through the firewall, IBM Firewall protects your network from outsiders. For further protection, vulnerability checking software included with IBM Firewall can *harden* the server on which IBM Firewall is running to ensure that hackers cannot get into or through the firewall. The IP addresses and configuration of the internal network are hidden from the untrusted network. All traffic through the firewall is logged and can be used to generate user activity reports.

IBM Firewall and its VPN configuration application allow you to deploy and inexpensively manage large-scale VPN infrastructures. Network studies have shown that customers can use VPNs to realize large savings over the cost of leased line solutions.

With IBM Firewall, you can connect your branch offices together using the Internet by deploying firewalls at each branch and using an IPSec-based tunnel.

IBM Firewall comes with the ACE/Server, a product of Security Dynamics Technologies, Inc. ACE/Server provides strong, centralized authentication services for enterprise networks so that only authorized users can gain access to network files, applications, and communications. Along with Security Dynamics Technologies, Inc.'s patented SecurID token technology, ACE/Server creates a barrier against unauthorized access. The authentication relies on two factors: users are required to both *have* something (a SecurID token card) and *know* something (a PIN) to be authenticated.

MIMEsweeper deployment

MIMEsweeper, a product of Content Technologies Ltd., performs content-based analysis of Internet and intranet data to identify any hidden threats and protect your network users from those threats.

See “SecureWay Boundary Server component considerations” on page 61 for installation considerations.

MIMEsweeper contains two basic modules, MAILsweeper and WEBsweeper, that protect your users in different ways. As mail and other Web data enter MIMEsweeper, MIMEsweeper verifies the addresses of the sender and receiver and then recursively disassembles the files into their component parts. MAILsweeper and WEBsweeper then analyze these parts to minimize the risk that threats can enter your private network.

FirstSecure includes both MAILsweeper 4.0 and WEBsweeper 3.2_5. Each is separately installable, configurable, and usable.

MAILsweeper can:

- Work with virus scanners that you choose to verify that the disassembled files are virus-free
- Detect and block macro bombs
- Scan for keywords to:
  - Help guard against harassment or offensive language in e-mail
  - Help protect valuable data from leaving the company
- Block incoming e-mail spam, leaving the network less congested and minimizing employee productivity loss
- Block individuals or groups from sending or receiving certain types of files, such as AVIs or MPEGs
- Block or delay files on the basis of size until the network can better accommodate the traffic

WEBsweeper can:

- Block employees from certain sites that are not likely to be work-related
- Help guard against inadvertent loss of confidential or sensitive documents

In addition, MIMEsweeper contains an application programming interface (API) you can use to integrate third-party URL blockers.

MIMEsweeper can be a major asset in protecting your company and your users from security threats from the Internet.

Note: Although the MIMEsweeper documentation may provide a Content Technologies contact for service and support, when you obtain MIMEsweeper for IBM SecureWay Release 2 as part of the SecureWay FirstSecure offering or the SecureWay Boundary Server offering, you should contact IBM for service and support.

SurfinGate deployment

SurfinGate, a product of Finjan Software Ltd., inspects mobile code such as JavaScript code, Java applets, and ActiveX controls to protect your network from damage such as data modification, information deletion, and illicit data gathering. SurfinGate inspects mobile code at the gateway level and identifies threatening code before it can enter your network. Mobile code can be selectively blocked or allowed on a per-user or per-department basis, and the code can be allowed or denied access to your company's network based on its intended function. With SurfinGate, administrators can enable mobile code and manage, control, and enforce company-wide security policy for ActiveX, Java, JavaScript, Visual Basic Script, plug-ins, and cookies.

SurfinGate includes the following components:
- SurfinGate Server
- SurfinConsole
- SurfinGate database
- Plugin for WTE integration

The SurfinGate Server acts as an HTTP proxy server or as a service to the firewall or proxy. The SurfinGate Server can be positioned after the corporate firewall and any other existing proxies, and also acts as an HTTP server. This architecture allows mobile code traffic to be stopped and inspected before attacks happen.

A network administrator uses the SurfinConsole to manage and set a central corporate security policy for mobile code. The SurfinConsole can control multiple SurfinGate Servers on the network and can enforce mobile code rules throughout the company by user or group, or through custom lists of unacceptable and acceptable code.

The SurfinGate database stores details of Applet Security Profiles (ASPs), including information about users and groups and their corresponding security policies. Because SurfinGate inspects the content of all mobile code dynamically, the database is not required for security, but it does help improve performance in large-scale operations.

Note: Although the SurfinGate documentation may provide a Finjan contact for service and support, when you obtain SurfinGate for Windows NT as part of the SecureWay FirstSecure offering or the SecureWay Boundary Server offering, you should contact IBM for service and support.

Chapter 7. Planning for Intrusion Immunity in your network

The security technologies described so far emphasize protection from security threats. An equally important aspect of security is detection of threats. The intrusion immunity products in FirstSecure provide intrusion detection and antivirus capabilities that allow your company to detect security threats.

Antivirus software provides protection from malicious code, including Trojan horses, worms, macro viruses, rogue ActiveX controls, and rogue Java applets. Virus protection is an essential part of any security solution. FirstSecure's antivirus products address these key antivirus requirements:

- Coverage of a broad set of clients for a comprehensive and consistent approach to the antivirus needs of both stationary and mobile clients.
- Subscription service for virus signatures. Updating virus signatures on a regular basis is crucial for maintaining effective protection against the latest forms of malicious code.
- Policy-driven distribution of antivirus updates from servers to clients to assure that your antivirus policies are put into effect.

Tivoli Cross-Site for Security deployment

Tivoli Cross-Site for Security provides network-based intrusion detection for systems that might be vulnerable to attack. You can deploy Tivoli Cross-Site for Security agents wherever your administrative domain connects to the Internet. Tivoli Cross-Site for Security monitors networks to detect internal and external attacks. It brings you the following benefits:

- Real-time intrusion detection that alerts the Cross-Site for Security administrator of potential attacks
- Configurable policy that lets you set different policy for agents in your DMZ and agents on your intranet
- Online modification of Security agent policy that lets you respond to changing environments quickly
- Integration with Tivoli's Enterprise applications so that you can augment your Tivoli enterprise management system

The Tivoli Cross-Site for Security can:

- Detect scans and floods
- Monitor IP traffic
- Monitor port services
- Detect DNS, mount service, and network file system requests and replies

- Detect portmapper service requests and reply dumps
- Detect RStatd calls
- Detect requests for specific map names and file names
- Detect SMB-based attacks on PC file servers
- Detect Internet control message protocol

Cross-Site for Security lets you monitor network traffic and detect attacks and intrusion attempts. It monitors traffic in both your DMZ that insulates your intranet from the Internet and on your internal network.

The types of intrusions that Cross-Site for Security can detect include:

- Signature, or pattern, detection
- Flood detection
- Network-based attacks
- Windows network attacks
- Remote procedure attacks
- Service exploitations
- Unauthorized network traffic
- Suspicious activity

Cross-Site for Security guards your network by using the Cross-Site for Security agent and the Cross-Site for Security management server. When an agent detects a critical attack, it sends an encrypted event to the Cross-Site for Security management server which immediately logs the information and responds. You can configure the Cross-Site for Security management server to send an alert to the console, post an e-mail to an administrator, or page an on-call administrator.

Obtaining a Tivoli Cross-Site for Security license key

To enable your Tivoli Cross-Site for Security product, you need a customized license key.

You can receive the license key by going to the Tivoli Cross-Site web site and completing the following steps:

1. Find the Passport Advantage Proof of Entitlement document that came with your FirstSecure products, including the Tivoli Cross-Site for Security CD-ROM, and also the *Tivoli Cross-Site for Security Installation*.
2. Locate the order number, an eight-digit number beginning with a 5, and your customer (site) number, a seven digit number beginning with a 7, on your Passport Advantage Proof of Entitlement. You use these numbers to access the Tivoli Cross-Site web site for the first time.

3. Log in to the Tivoli Cross-Site Web site using a web browser on a computer with Internet access. The URL for the web site is `www.cross-site.com/support/licensing/`.
4. Enter your order number, your customer number, and contact information. You must also supply the domain name of the server on which you plan to install Tivoli Cross-Site for Security.
5. Follow the additional instructions on the web.
6. If you have trouble accessing the Tivoli Cross-Site license key web site, contact Tivoli Cross-Site support at 1–800–2–TIVOLI, extension 9396 or by e-mail at licensing@cross-site.com.

Related Tivoli Cross-Site products

The Tivoli Cross-Site product family includes other components that are not part of the FirstSecure family:

- Tivoli Cross-Site for Availability monitors and reports how successfully end users are able to access your Web site.
- Tivoli Cross-Site for Deployment extends the reach of your enterprise, allowing you to distribute and manage critical applications and information over the Internet.

Although these products might be mentioned in the Tivoli Cross-Site for Security documentation, they must be purchased separately.

Monitoring traffic with Tivoli Cross-Site for Security

The Cross-Site for Security agent is an intelligent network sniffer. It continually monitors the packets on the network. The Cross-Site for Security agent filters these packets looking for various signatures that represent suspicious activity. These signatures can indicate attacks on the network.

The Cross-Site for Security agent runs as a *daemon* on UNIX, and as an NT service on Windows NT. Cross-Site for Security is configured to start automatically when the system boots up. It remains resident and runs in the background on the system whether or not a user is logged in.

When a potential attack is detected, the agent determines the severity and determines whether to notify the management server immediately or log the alert to a local file. Logs are periodically uploaded to the management server.

The agent also regularly contacts the Cross-Site for Security management server to let it know the agent is alive and running. This type of communication is called a *heartbeat*. You can configure the heartbeat intervals.

When the management server receives a heartbeat from the agent, the management server notifies the agent of any updated configuration information, new signatures, and upload schedules. The agent automatically downloads and installs these updates.

Tivoli Cross-Site for Security in your network

You can configure Cross-Site for Security to fit your business requirements. The main decisions are:

- Where to install the Cross-Site for Security management server?
- How many Cross-Site for Security agents do you need?
- Where to install the Cross-Site for Security agents?

These considerations, in addition to size, topology, and network bandwidth and traffic, are critical in determining the number of management servers and agents. See “Intrusion Immunity hardware and software requirements” on page 67 for installation considerations for Tivoli Cross-Site for Security.

Note: Although the Tivoli Cross-Site for Security documentation might describe service and support, when you obtain Tivoli Cross-Site for Security as part of the SecureWay FirstSecure offering, you should contact IBM for service and support.

Norton AntiVirus deployment

Norton AntiVirus, from Symantec Corporation, is one of the world’s leading antivirus software products. Norton AntiVirus can:

- Quarantine infected files
- Protect against viruses and malicious ActiveX controls and Java applets
- Protect against viruses that might come in from e-mail attachments, Internet downloads, floppy diskettes, software CDs, or a network

You can schedule Norton AntiVirus to run constantly in the background to help keep your computer safe. The Symantec researchers keep adding to the viruses Norton AntiVirus can detect. You can use the LiveUpdate feature to automatically retrieve new antivirus definitions from Symantec as often as once a week.

The quarantine feature of Norton AntiVirus isolates infected or suspicious files in a safe location on your computer, separated from other files to prevent the spread of the virus while you fix the file.

The Scan and Deliver wizard lets you send suspicious files to Symantec for evaluation. The Symantec AntiVirus Research Center (SARC) responds to help you fix the problem.

The Norton AntiVirus scanner, *Bloodhound*, runs in the background to watch and categorize the behavior of applications that are potentially infected with new viruses. If an application behaves like a virus and attempts to infect other programs, Bloodhound can stop the program, preventing infection of other files until you receive new virus updates.

Norton AntiVirus Solution Release 3.04 products provided in FirstSecure are:

- Desktop Solutions:
  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.02 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.02 for OS/2
- Server Solutions:
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 2.0 for Lotus Notes™ and OS/2
  - Norton AntiVirus 1.52 for Microsoft Exchange
- Gateway Solutions:
  - Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
  - Norton AntiVirus 1.04 for Firewalls
- Administration:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 for Tivoli IT Director
  - Other Administration Tools, including Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

More information about Norton AntiVirus is in contents.txt file in the root directory of the Norton AntiVirus CD.

Note: Although the Norton AntiVirus documentation may provide a Symantec contact for service and support, when you obtain Norton AntiVirus Solution Release 3.04 as part of the SecureWay FirstSecure offering, you should contact IBM for service and support.

For detailed installation steps, see the documentation that accompanies the specific products and the hardware and software requirements in “Chapter 13. Intrusion Immunity requirements and installation considerations” on page 67.

Chapter 8. Planning for Public Key Infrastructure in your network

The Trust Authority component of Public Key Infrastructure provides Internet applications with the means to authenticate users and ensure trusted communications. Built on public key infrastructure (PKI) standards for cryptography and interoperability, a Trust Authority system provides the infrastructure needed to issue, publish, and administer digital certificates. It includes:

- Support for IBM AIX and Microsoft Windows NT server platforms.
- A Registration Authority (RA) that handles the administrative tasks behind user registration. This administration, which can be implemented through automated processes or human decision-making, includes the following types of tasks:
  - Confirming a user's identity
  - Approving or rejecting requests to obtain, renew, or revoke certificates
  - Validating that the user has possession of the private key associated with the public key in a certificate
  - Following the rules in a given business process or certificate profile to issue particular types of certificates to particular types of users

  The RA also publishes information about certificates in an integrated public key Directory, the IBM SecureWay LDAP Directory.
- A trusted Certificate Authority (CA). The CA:
  - Issues digital certificates and generates digital key pairs that allow the certificates to be authenticated
  - Supports the complete certificate life cycle, from initial enrollment through certificate renewal and revocation
  - The RA updates the Directory immediately when a certificate is revoked
  - Can use cryptographic hardware, such as the IBM SecureWay 4758 PCI Cryptographic Coprocessor and Smart Cards, to extend its ability to protect keys
- Credential Central, a Web-based enrollment interface that makes it easy to obtain browser certificates, server certificates, and certificates for certain devices, such as Smart Cards. Administrators can also use these enrollment forms to preregister endusers for a PKIX certificate.
- The Trust Authority Client, a stand-alone Windows interface that allows users to obtain, renew, and revoke PKIX certificates without using a Web browser.

- The RA Desktop, a Web-based administrative interface that enables a human administrator to approve or reject requests to obtain, renew, or revoke certificates.
- An Audit subsystem that uses message authentication codes (MACs) to ensure that events it receives from the Trust Authority RA and CA can be authenticated. A configurable option allows audit records to also be integrity-protected when they are logged.
- Several administrative interfaces for configuring the system, changing secure passwords, cross-certifying CAs, integrity checking audit logs, and securely starting and stopping the system components.
- An application programming interface (API) that enables application developers to write custom PKI applications.
- Integrated run-time support for the IBM DB2 Universal Database. Separate databases exist for the IBM SecureWay Directory and the RA, CA, and Audit components.

Trust Authority deployment

See *IBM SecureWay Trust Authority Up and Running* for detailed planning and installation information. This book contains scenarios and steps for installation on Windows NT servers and on AIX.

Chapter 9. Planning for the SecureWay Toolbox in your enterprise

Plan to install the FirstSecure Toolbox in a development environment, not in your network. Test your applications within your development environment before making them available to outside users.

Authorization services

Authorization services let you monitor who is authorized to access your Web site. Authentication is based on passwords or public keys. These measures protect the integrity and confidentiality of the data on your site. Authorization services create access control lists (ACLs) that define who can access objects on your site and how they can access those objects. Authorization services also enable you to define protected objects and to create passwords for single sign-on. All of these security tools are centralized to make security policies easy to manage. Authorization services are supported by IBM SecureWay Policy Director authorization APIs.

Certificate authority services

Certificate authority services are supported by X.509 Public Key Infrastructure for Multiplatforms and the IBM KeyWorks Toolkit.

Certificate authority services allow you to ensure security through management of digital certificates. These services include APIs for the complete life cycle of these certificates: issuance, renewal, and revocation. They also publish certificate revocation lists. The APIs make use of public key cryptography and smart card technology as a means of authenticating the certificate users.

X.509 Public Key Infrastructure for Multiplatforms, also referred to as PKIX, is supplied through PKIX APIs. These APIs allow the creation, management, storage, distribution, and revocation of certificates through the end entity (EE), certificate authority (CA), and registration authority (RA) components. The APIs are enabled to interface with IBM SecureWay Trust Authority, and they are based on IBMKeyWorks.

For information about the PKIX APIs, refer to *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*. For more

information about IBM KeyWorks, refer to “Chapter 16. Documentation provided with FirstSecure” on page 87 for a list of documentation provided with the Toolbox.

Directory services

Directory services are supported by the IBM SecureWay Directory Client.

Directory services use Lightweight Directory Access Protocol (LDAP) to organize, control, and access directories. These services are based on a client/server model that provides client access to an LDAP server. Directory services provide a means of maintaining directory information in a central location for storage, updates, retrieval, and exchange. Directory Services use Secure Sockets Layer (SSL) to encrypt information.

For more information about directory services, refer to “Chapter 16. Documentation provided with FirstSecure” on page 87 for a complete list of IBM SecureWay Directory Client documentation provided with the Toolbox.

KeyWorks cryptographic and trust management services

Cryptographic and trust management services are supported by IBM KeyWorks Toolkit, which is also referred to as KeyWorks.

KeyWorks cryptographic and trust management services encrypt and decrypt information to control who has access to the information. These services create and verify digital signatures to authenticate the identities of individuals and computers on networks. A key recovery system that enables the recovery of encrypted information, without distributing the key, is incorporated in the IBM Key Recovery Service Provider.

KeyWorks is a cryptographic and trust services toolkit. It consists of a set of layered security services and associated programming interfaces that furnish an integrated set of information and communication security capabilities. Each layer builds on the more fundamental services of the layer directly below it. These layers start with fundamental components such as cryptographic algorithms, random numbers, and unique identification information in the lower layers, and build up to digital certificates, key management and recovery mechanisms, and secure transaction protocols in higher layers.

KeyWorks is enabled for National Language Support (NLS), which means that the product is not dependent on any language, script, culture, and coded character set.

For more information about the KeyWorksC APIs, refer to “Chapter 16. Documentation provided with FirstSecure” on page 87 for a list of KeyWorks documentation provided with the Toolbox.

Secure Sockets Layer protocol services

Secure Sockets Layer protocol services are supported by the IBMSecure Sockets Layer (SSL) Toolkit.

SSL protocol services let you decide who has access to your data. These services encrypt data using public and private keys for several purposes, including user authentication, prevention of access by unauthorized clients, and prevention of data tampering. You have control over who you issue certificates to, so you can control who trust with access to your data. SSL technology is incorporated in several other APIs for encrypting data and creating passwords.

Part 3. Installation and integration considerations

This section describes how the components fit together. It lists the hardware and software requirements for each product and any required applications or database products.

Chapter 10. Planning to install FirstSecure

Before you install the FirstSecure component products, read the following sections to make sure that you have the necessary hardware and software. Information about last-minute updates to FirstSecure is at www.ibm.com/software/security/firstsecure. Check the Web site for late updates before you start installing the products..

Detailed step-by-step instructions for installing and configuring the component products of FirstSecure are provided in the product literature for each of the component products.

General system requirements

This section describes the overall system requirements for FirstSecure products. For specific hardware and software requirements for each of the component products, see the specific component product.

To install the FirstSecure components, you need hardware that can run one of the following Server operating systems:

- Microsoft Windows NT Version 4 with service pack 5.
- AIX Version 4.3.1 or higher.
- Sun Solaris Version 2.6 or higher.

Note: On Solaris, The Toolbox requires Sun Solaris Version 2.6 with the May, 1999 Fix Pack.

Each of the FirstSecure component products runs on at least one of the operating systems listed above. Each component product section shows the supported operating system platforms and other prerequisite software for each component product. Within those operating systems you'll need servers, management consoles, and client systems. The following sections give an overview of those requirements.

Operating system requirements for servers and clients

See Table 1 for the operating system requirements for SecureWay products.

Table 1. Operating system requirements for servers and clients

Operating System	Minimum Server Level	Minimum Client Level
Windows NT	Version 4.0, Service Pack 5	Version 4.0, Service Pack 5
IBM AIX	Version 4.3.1	Version 4.3.1

Table 1. Operating system requirements for servers and clients (continued)

Operating System	Minimum Server Level	Minimum Client Level
Sun Solaris	Version 2.6	Version 2.6
Windows 95	N/A	All versions supported
Windows 98	N/A	All versions supported
Windows 3.1 (Norton AntiVirus only)	N/A	All versions supported
IBM OS/2 (Norton AntiVirus only)	N/A	Version 4.0, FixPak 6 or higher

Component product details and requirements

The sections that follow show the hardware and software requirements for the FirstSecure component products. The following chapters describe the building blocks in detail and give hardware and software requirements for each. The chapters also give an installation and configuration overview of each product, including a discussion of integrating with other components.

- "Chapter 11. Policy Director requirements and installation considerations" on page 57
- "Chapter 12. SecureWay Boundary Server requirements and installation considerations" on page 59
- "Chapter 13. Intrusion Immunity requirements and installation considerations" on page 67
- "Chapter 14. Public Key Infrastructure requirements and installation considerations" on page 75
- "Chapter 15. Toolbox installation requirements and considerations" on page 81

Chapter 11. Policy Director requirements and installation considerations

This chapter lists the hardware and software requirements for Policy Director. It also gives any installation considerations about integration with other FirstSecure products.

Policy Director hardware and software requirements

Table 2 lists the Policy Director hardware requirements.

Table 2. Hardware requirements for Policy Director

Platform	Minimum Disk Space	Minimum Memory
Windows NT server: Intel or Intel-compatible 80486 133 MHZ or higher	16 MB	64 MB
AIX server: hardware that runs AIX 4.3.1	16 MB	64 MB
Solaris server: hardware that runs Solaris 2.6	16 MB	64 MB

Software requirements for the Policy Director components are:

Policy Director servers

- Windows NT Server Version 4.0, Service Pack 5
- AIX Version 4.3.1
- Sun Solaris, Version 2.6

NetSEAT clients

- Windows NT Server Version 4.0, Service Pack 5
- Windows 95
- Windows 98

Management console

- Windows NT Workstation
- Windows NT Server Client
- AIX Version 4.3.1 Client
- Sun Solaris, Version 2.6 Client

Policy Director requires other software which is included in the package. Follow the directions in *IBM SecureWay Policy Director Up and Running* to install the software required for your Policy Director deployment.

Policy Director installation considerations

www.ibm.com/software/security/policy lists any updates to the current software prerequisites for Policy Director.

Integrating Policy Director and Trust Authority

The IBM SecureWay Trust Authority provides authentication by making sure each user is who that user claims to be. Trust Authority issues certificates to users based on information in the IBM SecureWay Directory, sometimes called Lightweight Directory Access Protocol or LDAP.

Policy Director, in turn, uses those certificates and provides authorization by making sure that each user has access only to allowed resources. Policy Director stores its information in that same IBM SecureWay Directory.

Your e-business can have a single user definition with all the Policy Director permissions, and all the Trust Authority information. If you also store SecureWay Boundary Server information in the IBM SecureWay Directory, the Policy Director can manage that for you, also.

Chapter 12. SecureWay Boundary Server requirements and installation considerations

This chapter lists the hardware and software requirements for SecureWay Boundary Server. It also gives any installation considerations about integration with other SecureWay Boundary Server products.

SecureWay Boundary Server hardware and software requirements

Hardware requirements for the SecureWay Boundary Server component products are in Table 3 and Table 4 on page 60.

Table 3. Hardware requirements for SecureWay Boundary Server component products

SecureWay Boundary Server Component	Machine Type	Disk Space	Memory	Other
IBM SecureWay Firewall[1]	NT: Pentium® 133 MHz or higher AIX: RS/6000 machine that supports AIX 4.3.2	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	2 network interface cards
ACE/Server	NT: Pentium 166 MHz or higher (single processors only) AIX: Machine that supports AIX 4.2	Primary server software: 50 MB Backup server: 22 MB Initial user database: 4 MB Installation: 240 MB	Minimum: 32 MB	Actual storage requirements are based on user population
SurfinGate				
Server	Pentium 233 MHz or higher	20 MB	Minimum: 128 MB Recommended: 256 MB	

Table 3. Hardware requirements for SecureWay Boundary Server component products (continued)

SecureWay Boundary Server Component	Machine Type	Disk Space	Memory	Other
Console	Pentium 233 MHz or higher	15 MB	Minimum: 32 MB Recommended: 64 MB	
MIMEsweeper for IBM SecureWay Release 2				
MAILsweeper	Pentium 200 MHz or higher	1 GB	64 MB	1 network interface card
WEBsweeper	Pentium 400 MHz or higher	1 GB	128 MB + 1 MB for each concurrent Web connection	1 network interface card

Notes:

1. See the documentation included with IBM Firewall for more detailed information.
2. 13 MB of disk space is also required for the Netscape browser.

Table 4. Software requirements for SecureWay Boundary Server component products

SecureWay Boundary Server Component	Microsoft Windows platforms		AIX	Solaris
	Client	Server	Server	Server
IBM SecureWay Firewall	Windows 95, IPSec client	Windows NT Server Version 4.0, Service Pack 5[1]	AIX 4.3.2	Not Available
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 or higher	Windows NT Server Version 4.0, Service Pack 5 or higher	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
Server	Not Available	Windows NT 4.0[2]	Not Available	Not Available
Console	Windows NT 4.0 or higher[2] Windows 95, Windows 98	Not Available	Not Available	Not Available
MIMEsweeper for IBM SecureWay Release 2				

Table 4. Software requirements for SecureWay Boundary Server component products (continued)

SecureWay Boundary Server Component	Microsoft Windows platforms		AIX	Solaris
	Client	**Server**	**Server**	**Server**
MAILsweeper	Not Available	Windows NT 4.0[3]	Not Available	Not Available
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 or higher	Windows NT 4.0[4]	Not Available	Not Available

Notes:

1. Check the documentation provided with IBM Firewall for Windows NT for any required fixes.
2. In addition:
   - Windows network client for Microsoft Windows is required.
   - Windows NT Workstation is not supported.
3. In addition:
   - NT 3.5.1 and Windows NT Workstation are not supported.
   - One of the following environments is required:
     - Microsoft Exchange
     - SMTP
     - cc:Mail™
     - Groupwise
     - Lotus Notes
4. See "MIMEsweeper considerations" on page 64 for MIMEsweeper recommendations.

SecureWay Boundary Server component considerations

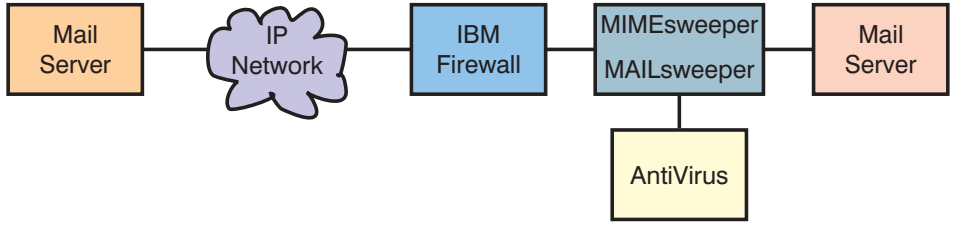
The following sections describe the installation and configuration considerations for the SecureWay Boundary Server component products.

IBM Firewall considerations

Considerations for IBM Firewall mainly involve where in the traffic stream you install it in relation to the other SecureWay Boundary Server products.

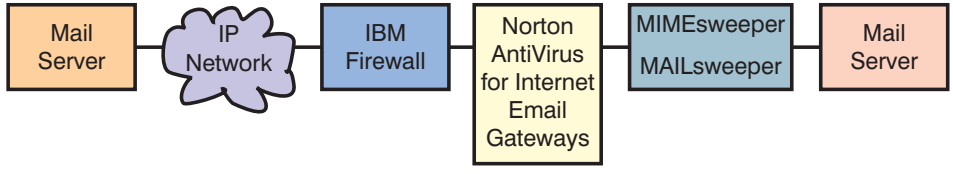
Sample configurations

IBM Firewall and MAILsweeper sample configuration: When you are installing both IBM Firewall and MIMEsweeper, you can use the configuration described in this section.



- MAILsweeper is the part of MIMEsweeper that checks the content of mail messages. MAILsweeper has a function to enable antivirus checks.
- MAILsweeper sits between IBM Firewall and the secure SMTP servers.
- IBM Firewall points to MAILsweeper as the mail host to forward mail.
  - IBM Firewall requires that the predefined mail rules be set up to allow mail traffic to flow.
- The SMTP servers must also point to MAILsweeper as the mail host to forward mail.
- MAILsweeper checks the content of forwarded mail messages that flow in both directions.

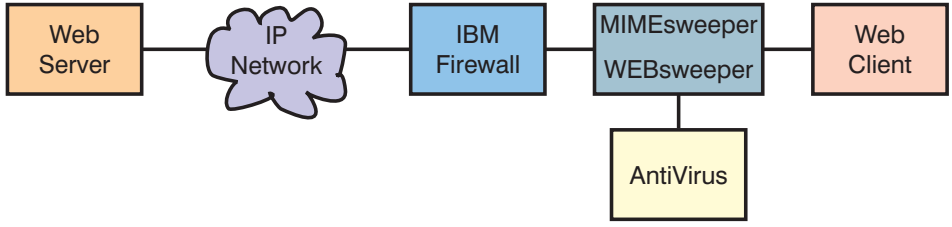
IBM Firewall, Norton AntiVirus for Internet Email Gateways, and MIMEsweeper sample configuration: If you are installing IBM Firewall, Norton AntiVirus for Internet Email Gateways, and MIMEsweeper, you can use the configuration described in this section. This scenario combines IBM Firewall, Norton AntiVirus for Internet Email Gateways, and MAILsweeper in a chain to check mail for viruses and content, as illustrated in the following diagram.



- The firewall points to Norton AntiVirus for Internet Email Gateways as its secure mail server. The correct firewall rules must be set to allow this specific traffic.
- Norton AntiVirus for Internet Email Gateways points to MAILsweeper as its mail forwarder for secure mail and to the firewall for mail destined outbound.
- MAILsweeper receives and checks mail forwarded to it. It then forwards the mail to the correct server depending on its routing tables or MX record lookups. If MAILsweeper and Norton AntiVirus for Internet Email

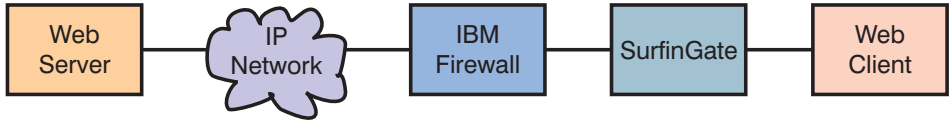
Gateways are on the same machine, you must change the receiving port for MAILsweeper to avoid conflict with Norton AntiVirus for Internet Email Gateways.

IBM Firewall and WEBsweeper sample configuration: If you are installing both IBM Firewall and MIMEsweeper, you can use the configuration described in this section.



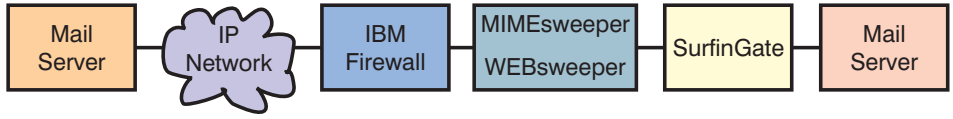
- WEBsweeper is the part of MIMEsweeper that checks Web traffic. WEBsweeper has a function to enable antivirus checks.
- WEBsweeper works as an intermediate proxy. Clients point to WEBsweeper as their proxy. WEBsweeper is then set to forward traffic to the firewall proxy.
- Rules must be set up on the firewall to allow proxy traffic.
- Proxy requests can come only from the secure network behind the firewall.
- WEBsweeper does not handle HTTPS. To use HTTPS, you must bypass WEBsweeper to avoid problems with the firewall and with ensuring that all Web traffic is checked. You must point directly to the firewall proxy. The Web traffic is still secure, but it is not checked by WEBsweeper.

IBM Firewall and SurfinGate sample configuration: If you are installing IBM Firewall and SurfinGate, you can use the configuration described in this section.



- SurfinGate checks Web traffic for ActiveX controls and other items.
- SurfinGate acts as an intermediate Web proxy. Clients point to SurfinGate as their proxy for HTTP, FTP, and HTTPS. SurfinGate then forwards the request to the IBM Firewall proxy.
- Rules must be set up on the firewall to allow proxy traffic.
- Proxy requests can come only from the secure network behind the firewall.

IBM Firewall, MIMEsweeper, and SurfinGate sample configuration: If you are installing IBM Firewall, MIMEsweeper, and SurfinGate, you can use the configuration described in this section.



- SurfinGate checks Web traffic for ActiveX controls and other items. It uses different checks than the WEBsweeper component of MIMEsweeper.
- SurfinGate and WEBsweeper act as intermediate Web proxies. Clients point to SurfinGate as their proxy for HTTP and FTP. SurfinGate then forwards the request to WEBsweeper. WEBsweeper then forwards the request to the IBM Firewall proxy.
- Rules must be set up on the firewall to allow proxy traffic. These rules are defined in the *IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide*.
- Proxy requests can come only from the secure network behind the firewall.
- WEBsweeper does not handle HTTPS. When using HTTPS, to avoid problems with the firewall and to ensure that all Web traffic is checked, you must bypass WEBsweeper. You must point directly to the firewall proxy. The Web traffic is still secure, but it is not checked by WEBsweeper.

MIMEsweeper considerations

The following is a typical WEBsweeper system:

- An Intel Pentium 400 MHz or higher
- 1GB disk space and 128 MB RAM
- Windows NT Server or Workstation Version 4.0 Server Service Pack 3 or higher
- TCP/IP protocol, including a host and domain name
- Antivirus tools

The following is a typical high volume WEBsweeper environment of up to 500 concurrent users:

- A dual Intel Pentium II, 450 MHz or higher
- 3GB disk space and 256 MB RAM
- Windows NT Server or Workstation Version 4.0 Server Service Pack 3 or higher
- TCP/IP protocol, including a host and domain name
- Antivirus tools

If your environment supports more than 500 concurrent users, then using multiple WEBsweeper servers is recommended.

Chapter 13. Intrusion Immunity requirements and installation considerations

This chapter lists the hardware and software requirements for the Intrusion Immunity components, Tivoli Cross-Site for Security and Norton AntiVirus.

Intrusion Immunity hardware and software requirements

The following section describes the installation and configuration documentation for the Intrusion Immunity component products.

Hardware and software requirements for Tivoli Cross-Site for Security are shown in Table 5, Table 6 on page 68, and Table 7 on page 68. Hardware and software requirements for the Norton AntiVirus component products are shown in Table 8 on page 69 and Table 9 on page 69.

Table 5. Hardware and software requirements for Tivoli Cross-Site for Security servers

Server requirements	
Operating System	• AIX 4.3.2 • Windows NT Version 4.0, Service Pack 5 • Solaris 2.5.1 or 2.6
Java	JDK 1.1.6 revision 04 or higher
Web server	Netscape Enterprise Server 3.51
Database	• IBM DB2 Release 5.2 • Oracle 7.3.4 (or 8.0.4 recommended) • Microsoft SQL Server
Disk space	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
Memory	256 MB
Swap space	300 MB (400 MB recommended)
Notes: 1. Netscape Enterprise Server 3.51 and 3.6 are not supported. 2. See the Patch requirements for Solaris in the installation documentation for the Tivoli Cross-Site for Security.	

Table 6. Hardware and software requirements for Tivoli Cross-Site for Security management console

Management console requirements	
Operating systems	• Windows 95 • Windows 98 • Windows NT Version 4.0, Service Pack 5 (166 MHz or higher machine recommended) • Solaris 2.5.1 or 2.6 running on Sun SPARC
Disk space	25 MB for all platforms
Memory	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

Table 7. Hardware and software requirements for Tivoli Cross-Site for Security agents

Agent requirements	
Operating systems	• Windows NT Version 4.0, Service Pack 5 or higher • AIX 4.3.2 • Solaris 2.5.1 or 2.6 running on Sun SPARC
Java	JDK 1.1.6 revision 04 or higher on Solaris (required for UNIX only)
Disk space	• 15 MB on Windows NT • 10 MB on AIX • 10 MB on Solaris
Memory	• 32 MB on Windows NT • 32 MB on AIX • 20 MB on Solaris
Notes: 1. Netscape Enterprise Server 3.51 and 3.6 are not supported. 2. See the Patch requirements for Solaris in the installation documentation for the Tivoli Cross-Site for Security .	

Table 8 on page 69 lists the hardware requirements for Norton AntiVirus.

Table 8. Hardware requirements for Norton AntiVirus.

Intrusion Immunity Component	Machine Type	Disk Space	Memory	Other
Norton AntiVirus	Intel CPU	24 MB	Minimum: 16 MB Recommended: 32 MB	CD-ROM drive
Norton AntiVirus for Internet E-mail Gateways	Pentium 133 or higher	6 MB	32 MB	CD-ROM drive 500 MB - 5 GB for efficient mail operation

Table 9. Software requirements for Norton AntiVirus

Intrusion Immunity Component	Microsoft Windows platforms		OS/2
	Client	Server	Client
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 or higher
Notes: 1. In addition, a TCP/IP Internet connection is required for Norton AntiVirus for Internet Email Gateways.			

Norton AntiVirus is not available on AIX and Solaris.

Tivoli Cross-Site for Security installation considerations

The following illustrations show typical placements of Cross-Site for Security agents and Cross-Site for Security management server in an e-business network.

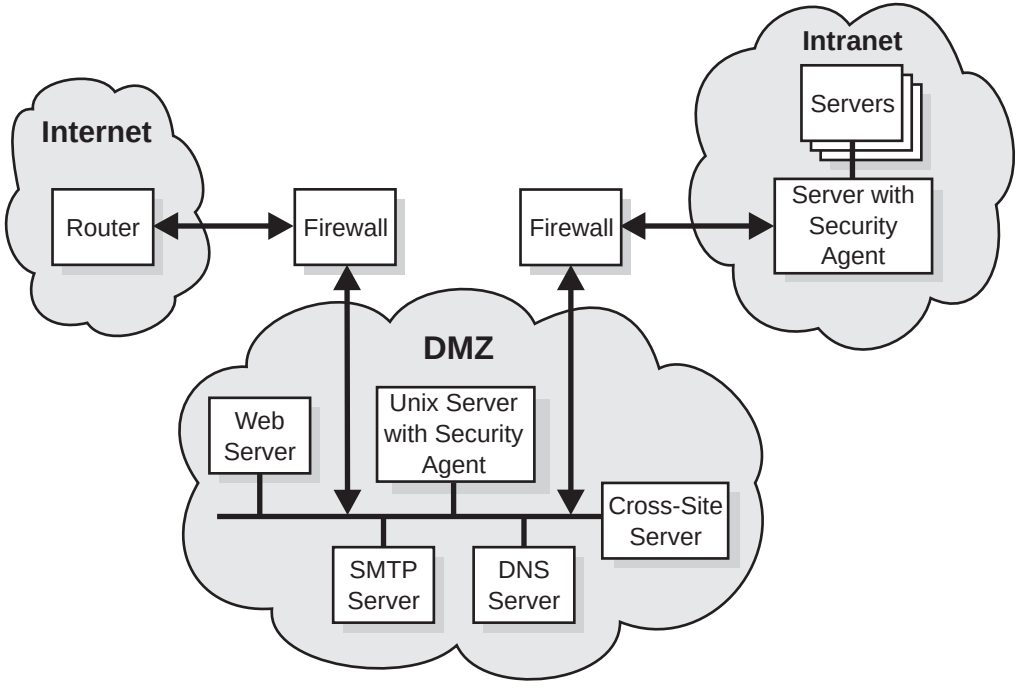


Figure 11. Installing the Cross-Site for Security management server in the DMZ

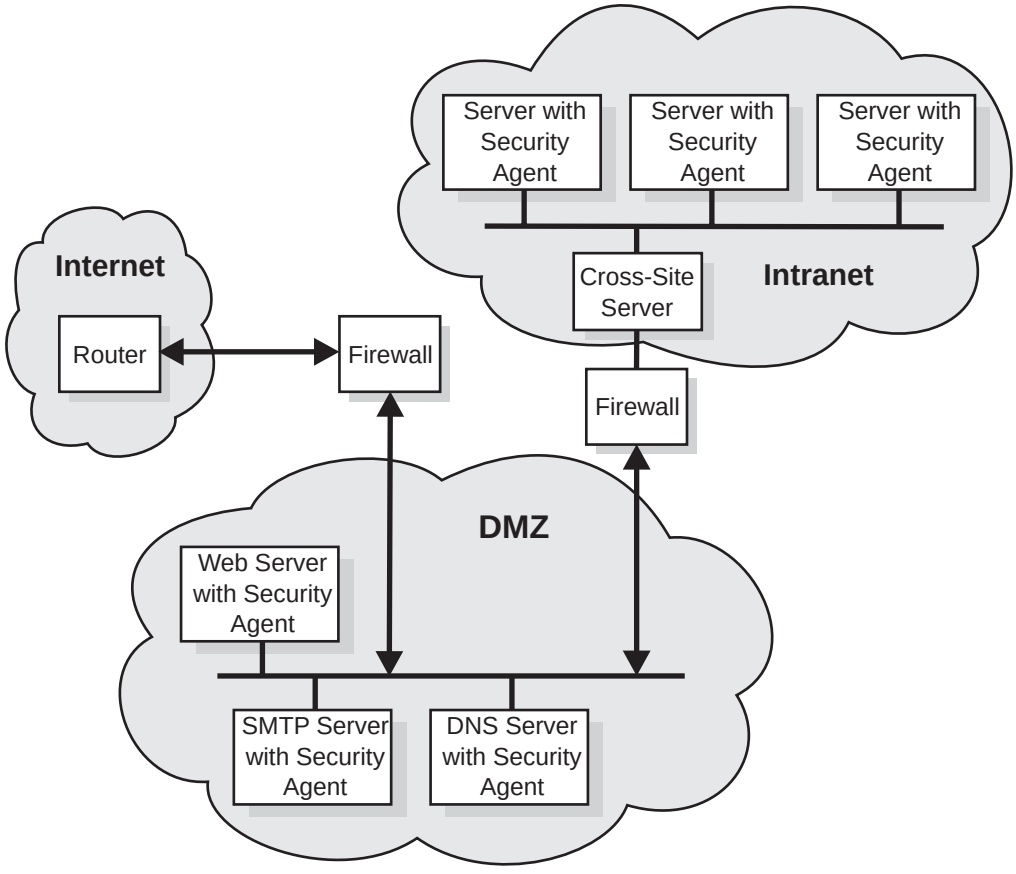


Figure 12. Installing the Cross-Site for Security management server in your intranet

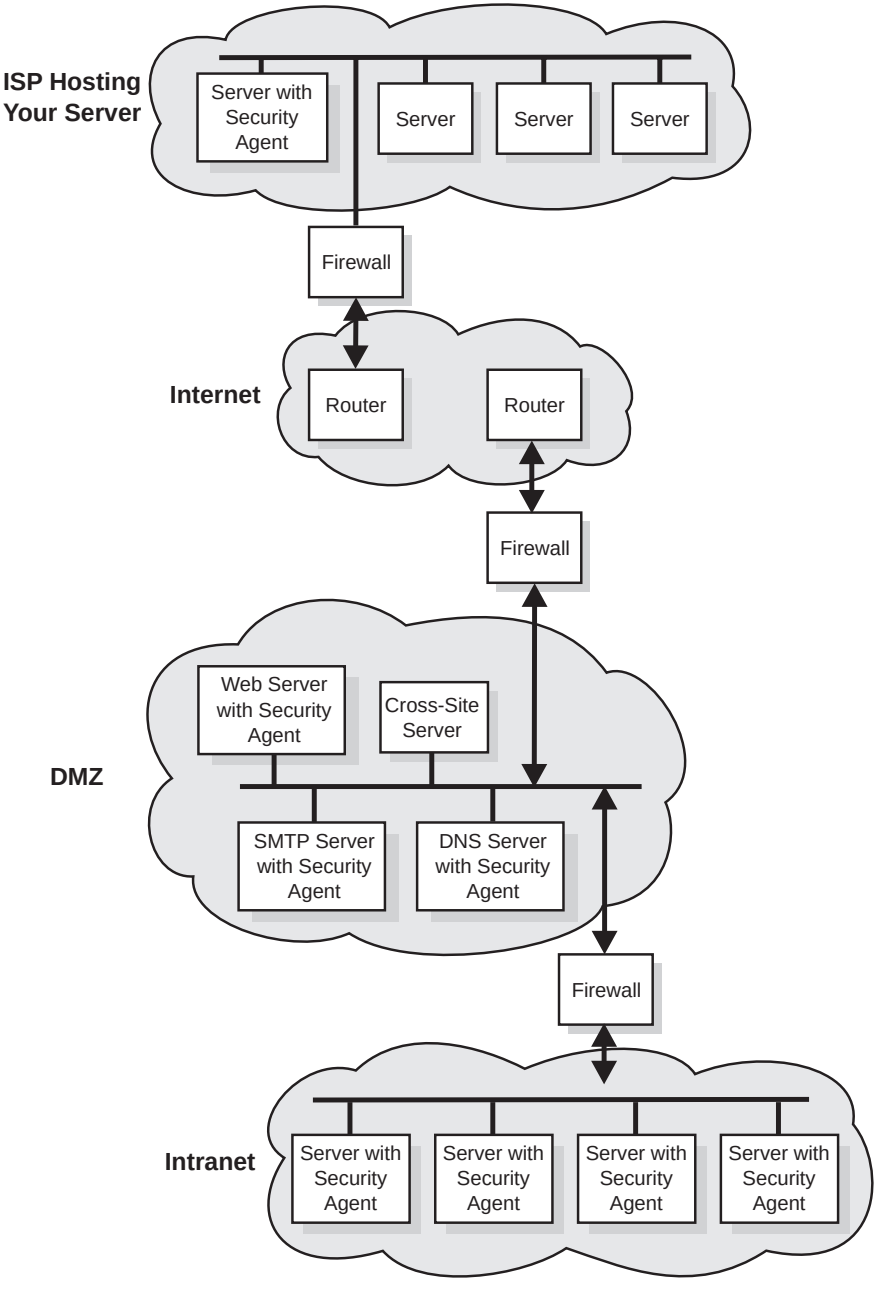


Figure 13. Installing the Cross-Site for Security management server in the DMZ supporting an Internet-connected server

Norton AntiVirus installation considerations

Information about installing Norton AntiVirus is in the file named contents.txt, which is in the root directory of the product CD.

Chapter 14. Public Key Infrastructure requirements and installation considerations

Companies today need a public-key infrastructure to secure e-business applications, and FirstSecure Trust Authority provides two levels of functions that implement a public-key infrastructure:

- Complete life cycle management of digital certificates providing:
  - The capability to request, renew, and revoke certificates
  - A registration authority to approve certificate requests
  - A certificate authority to create digital certificates and revocation lists
- Enhanced registration capabilities for enabling businesses to register their trusted e-business entities online. The registration application is built on the following principles:
  - The certificates being issued and managed must be worthy of the trust required by sensitive e-business applications, and the registration authority must be built to meet the same high trust and security requirements.
  - The application must provide the flexibility to support a variety of registration policies including manual or automated approvals, flexible on-site or off-site authentication, and the option to isolate registration policies into separate trusted domains.

The trust model helps to guarantee the accessibility, confidentiality, integrity, and authorship of your electronic transactions. Through digital encryption, certification, and signing, Trust Authority enables you to conduct secure e-business over the Internet, an intranet, or a virtual private network. For extended security of its signing key, the certificate authority is designed to work with cryptographic hardware.

Trust Authority server hardware and software requirements

Server software requirements for the Trust Authority component are listed in Table 10 on page 76.

Table 10. Server software and optional hardware requirements for Public Key Infrastructure Trust Authority component

Product	Notes
One of the following operating systems: • IBM AIX/6000 (AIX), version 4.3.2 • Microsoft Windows NT, version 4.0 with Service Pack 5	• Required. • You must install all Trust Authority server programs on the same platform. You cannot mix AIX and Windows NT machines in the same system configuration.
IBM SecureWay Directory Version 3.1.1	• Required; integrated with the Trust Authority code. • While installing Trust Authority, you can install the Directory software on the same machine where you install Trust Authority, or you can install it on a remote machine.
IBM WebSphere Application Server Version 2.02, Standard Edition. Includes IBM HTTP Server Version 1.3.3 and the Sun Java Development Kit (JDK) 1.1.7.	• Required; provided in the Trust Authority media package. • Before installing Trust Authority, you must install the Web server software on the same machine where you plan to install the Trust Authority and Trust Authority server software.
IBM DB2 Universal Database Enterprise Edition Version 5.2 with maintenance patch 9.	• Required; provided in the Trust Authority media package. • A unique database instance exists for each server component. Before installing Trust Authority, you must install DB2 on each machine that you plan to use as a Trust Authority server.
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, Model 001 • IBM SecureWay 4758 CCA Support Program, version 1.3.0.0 with maintenance patch 1.3.0.1	• *Optional*, and available only for AIX systems; you must order this product through normal IBM ordering channels. • Before installing Trust Authority, you must install the 4758 hardware and support program on the server where you plan to install the Trust Authority CA. • The 4758 cryptographic card requires a PCI bus on the RS/6000.

Table 11 on page 77 and Table 12 on page 78 list the server hardware requirements for the Trust Authority.

In Table 11 on page 77 and Table 12 on page 78:

- A small production environment issues hundreds of certificates each day.
- A medium production environment issues thousands of certificates each day.

- A large production environment issues many thousands of certificates each day. It may also be a system that provides third-party CA services to other organizations.

If you plan to run Trust Authority under Windows NT, IBM recommends that you install it on an IBM Netfinity® Server. The following table provides system sizing recommendations that are based on the number of certificates you expect to issue through a Trust Authority Certificate Authority.

Table 11. Sample Windows NT machine configuration

Machine Type	Processors	Disk Space	Memory
Small Production Environment			
Netfinity 3000	1 (450 MHz, Pentium II)	2 drives (9.1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 drives (9.1 GB)	512 MB
Medium Production Environment			
Netfinity 3000	1 (500 MHz, Pentium III)	4 drives (18.2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 drives (9.1 GB)	1 GB
Large Production Environment			
Netfinity 5500	2 (450 MHz, Pentium III)	4 drives (9.1 GB high speed)	1 GB
Netfinity 5500	4 (500 MHz, Pentium III Xeon with 1024K L2 Cache)	4 drives (9.1 GB high speed)	1 GB
Netfinity 7000	2 (500 MHz, Pentium III with 512K L2 Cache)	4 drives (9.1 GB high speed)	1 GB
Netfinity 7000	4 (500 MHz, Pentium III Xeon with 1024K L2 Cache)	4 drives (18.2 GB)	2 GB

If you plan to run Trust Authority under AIX, you must install it on an IBM RISC System/6000® machine. The following table provides system sizing recommendations that are based on the number of certificates you expect to issue through a Trust Authority Certificate Authority.

Table 12. Sample AIX machine hardware configuration

Machine Type	Processors	Disk Space	Memory
Small Production Environment			
F40	2 (233 MHz)	2 drives (9.1 GB, Ultra 2 Fast Wide)	512 MB
Medium Production Environment			
F40	2 (233 MHz)	3 drives (9.1 GB, Ultra 2 Fast Wide)	1 GB
Large Production Environment			
F50	4 (332 MHz)	5 drives (one 9.1 GB Ultra 2 Fast Wide plus four 9.1 GB SSA)	2 GB
H50	4 (332 MHz)	5 drives (one 9.1 GB Ultra 2 Fast Wide plus four 9.1 GB SSA)	2 GB
R50	6 (200 MHz)	2 drives (9.1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 drives (one 9.1 GB Ultra 2 Fast Wide plus a 7133 SSA Rack with four 9.1 GB SSA)	2 GB

Trust Authority client hardware and software requirements

IBM recommends the following workstation configuration for using the browser enrollment forms and for running the Trust Authority Client application.

- The following physical machine setup:
  - 166 MHz Intel 486 processor with 32 MB memory, at a minimum (200 MHz Intel Pentium processor with at least 64 MB of memory is preferred)
  - Graphics card
  - VGA video display, or better
  - Mouse or mouse-compatible pointing device
- One of the following operating systems:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT, version 4.0
- One of the following Web browsers:
  - Netscape Navigator or Netscape Communicator, version 3.0 or later
  - Microsoft Internet Explorer, version 4.0 or later, with Java enabled.

IBM KeyWorks Toolkit and IBM SecureWay Trust Authority interaction

Do not install IBM KeyWorks Toolkit on the same server as IBM SecureWay Trust Authority.

Chapter 15. Toolbox installation requirements and considerations

The FirstSecure Toolbox is a set of APIs to help your e-business develop secure applications.

- Authorization services
- Certificate and management services
- Directory services
- Secure Sockets Layer protocol services
- KeyWorks cryptographic and trust management services
  - IBM Key Recovery Service Provider 1.1.3.0 APIs. The IBM Key Recovery Service Provider enables the recovery of encrypted information.
  - IBM Key Recovery Server 1.1.3.0. The IBM Key Recovery Server 1.1.3.0 is an application that, upon authorized request, can recover encrypted information when keys are unavailable, lost, or damaged.

    These two toolkits provide standard interfaces that applications can use to invoke critical security services as well as standard interfaces that security providers can use to plug into the toolkit. The standard interfaces are based on the Common Data Security Architecture (CDSA). These toolkits are available on Windows NT, Solaris, and AIX.

Toolbox hardware and software requirements

Hardware requirements for the Toolbox are shown in Table 13.

Table 13. Hardware requirements for the Toolbox

Platform	Disk space	Memory
Version 4.0, Service Pack 5	2 - 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
Sun Solaris, Version 2.6 with May 1999 Fix Pak	4.2 GB	128 MB

Table 14. Hardware requirements for Toolbox component products

Toolkit	Machine Type	Disk Space	Memory
IBM KeyWorks Toolkit	Hardware that supports products running under: Windows NT Version 4.0, Service Pack 5 or higher Windows 95 AIX 4.2 or higher Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	Hardware that supports products running under: Windows NT Version 4.0, Service Pack 5 or higher Windows 95 AIX 4.2 or higher Sun Solaris	50 MB	32 MB

Software requirements for the Toolbox component products are shown in the following table.

Table 15. Software requirements for Toolbox component products

Toolbox Component	Microsoft Windows platforms		AIX	Solaris
	Client	**Server**	**Server**	**Server**
IBM KeyWorks Toolkit	Windows NT Version 4.0, Service Pack 5 or higher Windows 95	Windows NT Version 4.0, Service Pack 5 or higher Windows 95	AIX 4.2 or higher[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Version 4.0, Service Pack 5 or higher[2] Windows 95	Windows NT Version 4.0, Service Pack 5 or higher	AIX 4.2 or higher	Sun Solaris

Notes:

1. AIX client is also supported.
2. In addition, IBM KeyWorks Toolkit is required.

IBM KeyWorks Toolkit 1.1

The IBM KeyWorks Toolkit 1.1 provides application developers with an open, extendable, and standard means of accessing cryptographic and other security functions across different operating environments.

IBM KeyWorks Toolkit provides standard interfaces (APIs) that applications can use to invoke critical cryptographic, trust, and security services, as well as standard interfaces that Service Provider add-in modules can use to interface with the toolkit. These standard interfaces are based on Common Data Security Architecture (CDSA), a standard from The Open Group that was initially developed by Intel™ Corporation and extended by IBM into the KeyWorks Toolkit. When you use standard interfaces:

- Your company can choose the cryptographic and trust implementation that best suits its needs without making changes to applications that use the security services.
- The productivity of your application and middleware programmers is improved.

IBM KeyWorks Toolkit provides an insulating layer between applications and middleware as a class and the cryptographic functions and Service Providers. The toolkit contains a framework and Service Provider plug-in modules.

For applications, the framework provides the functionally rich Common Security Services Manager (CSSM) API from Intel Corporation's CDSA. IBM

has extended the CSSM API by adding key recovery functions. When you use IBM KeyWorks Toolkit, your application can:

- Encrypt and decrypt information
- Verify digital signatures for various purposes
- Retrieve certificates and certificate revocation lists from directories
- Create key recovery fields for key recovery and cryptographic backup
- Decide whether a certificate can be trusted, based on criteria established by systems designers and programmers at the instruction of users

Typically, an enterprise or OEM integrates IBM KeyWorks Toolkit and IBM Key Recovery Service Provider Toolkit with applications and middleware in a manner that allows the use of the CSSM APIs on the CSSM Framework. The product of this integration is a set of runtime applications and middleware for servers and clients that are distributed within the operating environment or environments. The other elements of FirstSecure will, over time, depend on IBM KeyWorks Toolkit for all cryptographic services and trust policy operations.

Integrators using IBM KeyWorks Toolkit should have systems engineers and programmers on staff with reasonably extensive experience with cryptographic design and programming as well as middleware and frameworks, or have access to contract integrators or OEMs with such experience.

For service providers, the framework provides the standard Service Provider Interface (SPI), the Open Group's CDSA. IBM has enhanced the SPI with the addition of key recovery functions.

IBM KeyWorks Toolkit (SDK) includes plug-in service provider modules that support open standards and proprietary public key certificates. These modules include PKCS#11, RSA Data Security's BSAFE cryptographic functions, X.509V3 certificates, the trust policies of Entrust and Verisign, and the Lightweight Directory Access Protocol (LDAP). The framework provides seamless integration of the cryptographic, trust, and security functions provided by the independent service provider modules.

IBM KeyWorks Toolkit can provide critical administrative functions, including:

- Protection against bypassing vital steps in a KeyWorks-supported process
- Verification that the Service Provider plug-in modules have not been altered prior to use
- Use of the Service Provider plug-in modules only through the framework
- Support for country-specific and enterprise-specific cryptography and trust policy usage

IBM KeyWorks Toolkit offers your company the following benefits:

- Allows you to change or substitute Service Provider modules without rewriting your applications and middleware
- Provides seamless support for hardware encryption and digital signature
- Supports LDAP directories and the DSA signature standard
- Does not require use of any particular Certificate Authority

More information about IBM KeyWorks Toolkit can be found in the *IBM KeyWorks Toolkit Developer's Guide*.

IBM KeyWorks Toolkit and IBM SecureWay Trust Authority interaction

Do not install IBM KeyWorks Toolkit on the same server as IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

The IBM Key Recovery Service Provider 1.1.3.0 , provided in toolkit format, is a Service Provider module that uses the standard functions provided by the IBM KeyWorks Toolkit. The IBM Key Recovery Service Provider enables the recovery of stored and transmitted encrypted information without collecting and escrowing private keys and creating single points of cryptographic vulnerability.

Because IBM Key Recovery Service Provider uses the standard functions provided by IBM KeyWorks Toolkit, the key recovery function can be used with different cryptographic suppliers, standard certificates from various Certificate Authorities, trust policies from Verisign and Entrust, and any directory that can be accessed by LDAP. The IBM Key Recovery Service Provider creates key recovery information based on the session key associated with the communication between correspondents.

More information about IBM Key Recovery Service Provider is in the *Key Recovery Server Installation and Usage Guide*, which is provided in the FirstSecure Documentation Pack.

Chapter 16. Documentation provided with FirstSecure

Each component product included in FirstSecure provides its own documentation. This chapter gives information about the documentation included with each of the FirstSecure component products.

A media pack and a documentation pack are available for SecureWay FirstSecure, SecureWay Policy Director, and SecureWay Boundary Server. Media packs contain product CDs that you use to install the component products in the offering, and some of these CDs contain online documentation. Documentation packs contain hardcopy books for those component products that provide them. “FirstSecure documentation pack” on page 95 lists the contents of the documentation packs.

Policy Director

The following documentation is provided with the Policy Director component products.

IBM SecureWay Policy Director Up and Running
: Tells how to install and configure the IBM SecureWay Policy Director.

IBM SecureWay Policy Director Administration Guide
: Tells how to administer the IBM SecureWay Policy Director. This book is provided in PDF format.

IBM SecureWay Policy Director Programming Guide and Reference
: Tells how to write programs for the IBM SecureWay Policy Director. This book is provided in PDF format.

Product readme
: This information is available on the Web at www.ibm.com/software/security/policy

SecureWay Boundary Server

The following book describes the SecureWay Boundary Server component products, their requirements and their interactions.

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running
: A hardcopy book that describes the SecureWay Boundary Server component products.

The following sections describe the documentation provided with the SecureWay Boundary Server component products.

IBM SecureWay Firewall

All IBM Firewall documentation is provided softcopy. IBM Firewall provides the following documentation:

IBM SecureWay Firewall for AIX Setup and Installation
: Instructions for installing and setting up the IBM SecureWay Firewall for AIX.

IBM SecureWay Firewall for Windows NT Setup and Installation
: Instructions for installing and setting up the IBM SecureWay Firewall for Windows NT.

IBM SecureWay Firewall for AIX User's Guide
: Instructions for installing and setting up the IBM SecureWay Firewall for Windows NT.

IBM SecureWay Firewall for Windows NT User's Guide
: Information about using IBM Firewall for Windows NT.

IBM SecureWay Firewall for Windows NT Reference
: Contains reference material for using IBM Firewall for Windows NT.

IBM SecureWay Firewall for AIX Reference
: Contains reference material for using IBM Firewall for AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
: Contains instructions for problem determination.

IBM SecureWay Firewall VPN Client User's Guide
: Tells how to set up and use a virtual private network.

MIMEsweeper

MIMEsweeper includes the following documentation:

MIMEsweeper Administrator's Guide
: Contains a Release Notes section, followed by information for the administrator, including planning and installation information.

  This book is provided in HTML format on the product CD. You can view it online by viewing the file named \DOC\MANUAL.HTM with a Web browser.

MIMEsweeper Release Notes
: Contains updated documentation, including installation information and instructions for viewing the documentation online.

This book is provided in HTML format on the product CD. You can view it online by viewing the file named \DOC\RELNOTES.HTM with a Web browser.

MIMEsweeper Configuration Editor Help
Contains information about editing MIMEsweeper configuration files.

This document is provided in HTML format on the product CD.

SurfinGate

SurfinGate includes the following softcopy documentation:

SurfinGate Installation Guide
Information about installing and configuring the SurfinGate 4.05 components on Windows NT. A PDF version of the *SurfinGate Installation Guide* is on the product CD in the following file: \docs\install.pdf.

SurfinGate User Guide
Information about planning for and using SurfinGate. A PDF version of the *SurfinGate User Guide* is provided on the product CD in the following file: \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
Information about SurfinGate 4.05, including system requirements and product limitations. A PDF version of the *SurfinGate 4.05 for Windows NT Release Notes* is provided on the product CD in the following file: \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
Online document that discusses changes to SurfinGate. This document is on the product CD in the following file: \docs\rnappen.pdf.

Intrusion Immunity

The following sections describe the documentation provided with the Intrusion Immunity component product.

Tivoli Cross-Site for Security

The Tivoli Cross-Site for Security, Version 1.1 includes the following documentation in .pdf format:

Tivoli Cross-Site for Security Installation
This document gives detailed requirements for installation and takes you through the installation steps.

Tivoli Cross-Site for Security User's Guide
This document gives an overview of the product, instructions for

using the console and performing tasks, reference information such as command line interfaces, the configuration files, and a glossary. You can access this document on the product CD-ROM.

Norton AntiVirus

Norton AntiVirus includes the following documentation for components supported in FirstSecure. All the documents except the contents.txt file are delivered in PDF format on the Norton AntiVirus CD. The contents.txt file is an ASCII file on the product CD.

Documentation contents of the Norton AntiVirus Solution Release 3.04 CD

The Norton AntiVirus Solution Release 3.04 CD file called \contents.txt lists all the documentation included on the CD.

Administration solutions:

Norton AntiVirus Solution Implementation Guide
See \docs\admin\navimp.pdf on the product CD.

Norton AntiVirus Command-Line Scanner
See \docs\navc\navcugd.pdf on the product CD.

Emergency Rescue Disk creation
See \navc\readme.txt on the product CD.

Server solutions:

Norton AntiVirus for Windows NT Server Administrator's Guide
See \docs\admin\navnts50.pdf on the product CD.

Norton AntiVirus for NetWare User's Guide
See \docs\NAVNLM\NVN4.pdf on the product CD.

Norton AntiVirus for Lotus Notes Installation Guide
See \docs\NAVNOTES\NAVNOTES.pdf on the product CD.

Norton AntiVirus for Lotus Notes Installation Guide
See \docs\NAVNOTES\NAVNOTES.pdf on the product CD.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
See \docs\NOTESOS2\NOTESOS2.pdf on the product CD.

Norton AntiVirus for Microsoft Exchange Installation Guide
See \docs\NAVXCHNG\NAVXCHNG.pdf on the product CD.

Gateway solutions:

Norton AntiVirus for Internet Email Gateway User's Guide
See \docs\navieg\navieg.pdf on the product CD.

Norton AntiVirus for Firewalls Administrator's Guide
See \docs\navfw\navfw.pdf on the product CD.

Desktop solutions:

Norton AntiVirus User's Guide for Windows 3.1/DOS
See \docs\navwks\nav4dusr.pdf on the product CD.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
See \docs\navwks\nav4dref.pdf on the product CD.

Norton AntiVirus for Windows 95/98 User's Guide
See \docs\navwks\nav98usr.pdf on the product CD.

Norton AntiVirus for Windows 95/98 Reference Guide
See \docs\navwks\nav98ref.pdf on the product CD.

Norton AntiVirus for Windows NT User's Guide
See \docs\navwks\nav5nusr.pdf on the product CD.

Norton AntiVirus for Windows NT Reference Guide
See \docs\navwks\nav5nref.pdf on the product CD.

Norton AntiVirus v4.0 User's Guide for Windows NT
See \docs\351\navntugd.pdf on the product CD.

Norton AntiVirus v4.0 Reference Guide for Windows NT
See \docs\351\navntref.pdf on the product CD.

Norton AntiVirus User's Guide for OS/2
See \docs\navos2\navos2ug.pdf on the product CD.

Norton AntiVirus Distribution Guide for OS/2
See \docs\navos2\navos2dg.pdf on the product CD.

Norton AntiVirus for Macintosh User's Guide
See \docs\navmac\navmac.pdf on the product CD.

White papers on the Norton AntiVirus Solution Release 3.04 CD: The CD also contains white papers in the directory \sarc. Each white paper is in .pdf format.

Videos on the Norton AntiVirus Solution Release 3.04 CD: The CD also contains videos. To view a video, you must have Media Player or another program capable of playing .AVI files. The videos are in the following files:

SARC \sarc\sarc.avi

About Viruses
\sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour
\navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You
\navtour\alert\demo32.exe

A Tour of Norton System Center
\nsctour\setup.exe

or, to run the tour directly from the CD,

\nsctour\demo32.exe

More information about the tour is in the file \ncstour\readme.txt

Trust Authority

The IBM SecureWay Trust Authority product documentation is available in Portable Document Format (PDF) and HTML format on the *Trust Authority Documentation* CD-ROM. Much of the information has been translated into the languages Trust Authority supports. For instructions on how to access a publication in the language of your choice, see the product *Readme* file. The latest version of the *Readme* file is always available on the Library page of the IBM SecureWay Trust Authority web site at
http://www.ibm.com/software/security/trust/library

The Trust Authority library includes the following documentation:

IBM SecureWay Trust Authority Up and Running
This book is an overview of the product. It lists the product requirements, includes installation procedures, and provides information about how to access the online help available for each product component. In addition to being available on the *Documentation* CD-ROM, this book is printed and distributed with the product.

IBM SecureWay Trust Authority System Administration Guide
This book contains general information about administering the Trust Authority system. It includes procedures for starting and stopping the servers, changing passwords, administering the certificate authority, performing audits, and running data integrity checks.

IBM SecureWay Trust Authority Configuration Guide
This book contains information about how to use the Setup Wizard to configure a Trust Authority system. You can access the HTML version of this guide while viewing online help for the Wizard.

IBM SecureWay Trust Authority Registration Authority Desktop Guide
This book contains information about how to use the RA Desktop to administer certificates throughout the certificate life cycle. You can access the HTML version of this guide while viewing online help for the Desktop.

IBM SecureWay Trust Authority User's Guide
This book contains information about how to obtain certificates. It provides procedures for using the Trust Authority enrollment forms to request certificates for browsers, servers, and devices. It also shows users how to preregister for a PKIX certificate, and how to use the Trust Authority Client to store and administer PKIX certificates. You can access the HTML version of this guide while viewing online help for the Client.

Toolbox

The following sections describe the documentation provided with the Toolbox component products.

The Toolbox APIs

All Toolbox documentation is available at the following web site:`www.ibm.com/software/security/firstsecure/library`. The following documentation is included:

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
Provides an overview of the APIs and iKeyman. Defines each API, its syntax, and its usage.

IBM SecureWay Directory Client SDK Programming Reference
Includes various LDAP sample client programs and an LDAP client library that provides application access to the LDAP servers. Support is provided for C and for Java.

IBM SecureWay Policy Director Programming Guide and Reference
Defines each API, its syntax, and its usage.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide Gives installation instructions and requirements.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
Provides information for programmers developing applications using the IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms, also known as PKIX. Includes an overview of the product, instructions for writing programs for the separate PKIX components, and descriptions of the PKIX APIs.

IBM KeyWorks Toolkit

All documentation provided with IBM KeyWorks Toolkit is online, in PDF format on the product CD. The documentation is as follows:

IBM KeyWorks Toolkit Developer's Guide
Presents an overview of the toolkit. Also explains how to integrate the toolkit into applications and contains a sample application.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Defines the interface that application developers use to access security services provided by the framework and service provider modules.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
Describes the features common to all the toolkit service provider modules. This document should be used in conjunction with the individual Service Provider Interface Specifications in order to build a service provider module.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Defines the interface to which cryptography service provider modules must conform in order to be accessible through the toolkit.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Defines the interface to which key recovery service provider modules must conform in order to be accessible through the toolkit.

IBM KeyWorks Toolkit Trust Policy Interface Specification
Defines the interface to which policy makers, such as Certificate Authorities, Certificate Issuers, and policy-making application developers, must conform in order to extend the toolkit with model or application-specific policies.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
Defines the interface to which certificate library developers must conform to provide format-specific certificate manipulation services to numerous toolkit applications and trust policy modules.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
Defines the interface to which library developers must conform to provide format-specific or format-independent persistent storage of certificates.

IBM Key Recovery Service Provider

The following documentation is provided with IBM Key Recovery Service Provider in PDF format on the product CD:

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide Provides an understanding of key recovery concepts, guidance in setting up a key recovery solution for an organization, and procedures for installing, configuring, and operating the IBM Key Recovery Server.

Redbooks about security

The following redbooks, produced by the IBM International Technical Support Organization (ITSO) cover security-related products and processes. They are available at www.us.ibm.com/redbooks.

- *Understanding the IBM SecureWay FirstSecure Framework*
- *High Availability IBM eNetwork Firewall*

Documentation packs

The following documentation packs are available for IBM SecureWay FirstSecure.

FirstSecure documentation pack

The FirstSecure documentation pack contains the following books:

- FirstSecure License Information
- *IBM SecureWay FirstSecure Planning and Integration*
- *IBM SecureWay Policy Director Up and Running*
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*
- *IBM SecureWay Trust Authority Up and Running*
- *Tivoli Cross-Site for Security Installation*

Policy Director documentation pack

The Policy Director documentation pack contains the following books:

- Policy Director License Information
- *IBM SecureWay Policy Director Up and Running*

SecureWay Boundary Server documentation pack

The SecureWay Boundary Server documentation pack contains the following books:

- SecureWay Boundary Server License Information
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

Part 4. Appendixes

Appendix. Notices

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

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

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

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make

improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

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

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

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

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

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

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

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

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

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

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

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

Trademarks

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

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Lotus, Lotus Notes, Domino, and cc:Mail are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

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

Tivoli is a trademark of Tivoli Systems Inc. in the United States, or other countries, or both.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

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

Glossary

This glossary defines terms and abbreviations, used in this book, that may be new or unfamiliar and terms that may be of interest. It includes terms and definitions from:

- The IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- The American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

.

A

Access control. In computer security, the process of ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.

access control list. A mechanism for limiting use of a specific resource to authorized users.

ACL. Access Control List.

ActiveX. In Microsoft programming, a set of object-oriented technologies and terms.

agent. In Tivoli Cross-Site for Security, a smart IP packet monitor that catches packets, checks them for abnormalities on different network layers, and keeps track of the status of established connections and statistics.

Apache server. A set of freely available web server software.

API. Application programming interface.

Applet. A computer program written in Java that runs inside a Java-compatible browser such as Netscape Navigator. Also known as a Java applet.

application program interface. A functional interface that allows an application program written in a high-level language to use specific functions.

audit trail. Data, in the form of a logical path, that links a sequence of events. An audit trail can be used to trace transactions or the history of a given activity. For example, it may track activity in a customer account.

authentication. The process of reliably determining the identity of a communicating party.

Authorization. The process of determining what types of activities a user is permitted to perform. Typically authorization occurs after authentication.

B

Bloodhound. In Norton AntiVirus, the component that tracks down a virus.

C

cell. In DCE, a group of users, systems, and resources that are typically centered around a common purpose and that share security, administrative, and naming boundaries. A cell usually consists of users, machines, and resources that share a common purpose and a greater level of trust with each other than with users, machines, and resources outside the cell.

Cell directory service. A component of a Distributed Computing Environment (DCE) that manages a database of information about resources within a DCE cell.

certificate authority. The entity, software application, or persons responsible for following an organizations's security policies and assigning secure electronic identities in the form of certificates. The certificate authority processes requests to issue, renew, and revoke certificates.

Channel. A path along which signals can be sent.

Circuit-level gateway. In a firewall, a proxy server that redirects a client's request through the firewall to the intended server.

Client. (1) A functional unit that receives shared services from a server. (2) A computer or program that requests a service of another computer or program.

Content filtering. Dissembling a transmission to read the contents in order to determine whether the transmission meets specific content standards.

D

daemon. In AIX, a program that remains resident waiting to service a request.

DCE. Distributed Computing Environment.

Digital certificate. An electronic credential issued by a trusted third party to a person or entity. A certificate contains information about the entity it certifies.

Distributed Computing Environment. Services and tools that support the creation, use, and maintenance of distributed applications in a heterogeneous computing environment.

E

e-business. The conducting of business transactions over networks and through computers. It includes buying and selling goods and services. It also includes transferring funds through digital communications.

e-commerce. Conducting business-to-business transactions. It includes buying and selling goods and services (with customers, suppliers, vendors, and others) on the Internet. It is a primary element of e-business.

encrypt. To scramble information so that only someone knowing the appropriate decryption code can obtain the original information through decryption.

extranet. A derivative of the Internet that uses similar technology. Companies are beginning to apply Web publishing, electronic commerce, messaging, and groupware to multiple communities of customers, partners, and internal staff.

F

File Transfer Protocol (FTP). An Internet client/server protocol that can be used to transfer files between computers.

firewall. A system or combination of systems that enforces a boundary between two or more networks.

G

gateway. A system that allows incompatible networks or applications to communicate with each other.

H

hacker. A person who attempts access to a machine or system without proper authorization. Hackers typically tend to use resources without permission.

heartbeat. A communication from a program to a management program to confirm activity; the program tells the management program that it is still active, doing its tasks.

I

IDE. Integrated development environment.

Implementation Services. The on-site installation support provided by IBM

incident. In Tivoli Cross-Site for Security, a suspicious activity that might be an attack on the system.

integrated development environment. A program for application development that lets you code the application, run it with breakpoints, and receive diagnostic help for program errors.

Internet. A world-wide collection of networks that provide electronic communication between computers. It enables them to communicate with each other through software devices such as electronic mail or Web browsers. For example, some universities are on a network that, in turn, links with other similar networks to form the Internet.

intranet. A network within an enterprise that usually resides behind firewalls. It is a derivative of the Internet that uses similar technology. Technically, intranet is a mere extension of the Internet. HTML (a language used for graphical representation of information) and HTTP (a protocol that moves hypertext files across the Internet) are some of the commonalities.

IntraVerse server. In IntraVerse, a system on the network that contains the IntraVerse server software and that can communicate with all the host systems that are running on the NetSEAT client software. The IntraVerse server refers to a system or combination of systems that run the product's related programs.

IPSec. An Internet Protocol Security standard developed by the IETF. IPSec is a network layer protocol designed to provide cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality. Because of its strong authentication features, it has been adopted by many VPN product vendors as the protocol for establishing secure point-to-point connections through the Internet.

ISV. Independent Software Vendor.

J

Java. A set of network-aware, non-platform-specific computer technologies developed by Sun Microsystems, Incorporated. The Java environment consists of the Java OS, the virtual machines for various platforms, the object-oriented Java programming language, and several class libraries.

JavaScript. A scripting language that resembles Java and was developed by Netscape for use with the Netscape browser.

K

Kerberos. A secure method for authenticating a service requesting a computer. Kerberos was developed in the Athena Project at the Massachusetts Institute of Technology (MIT). In Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades. Kerberos lets a user request an encrypted ticket from an authentication process that can then be used to request a specific service from a server. The user's password need not pass through the network.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol. In IBM SecureWay Directory, LDAP provides a way to maintain directory information in a central location for storage, updating, retrieval, and exchange.

M

macro bomb. A saved sequence of commands sent to another user to cause unwanted results.

MPEG. The standard under development by the Moving Pictures Experts Group for compressing and storing motion video and animation in digital form.

mobile code. Pertaining to computing that is performed on a portable computer by a user

who is frequently moving among various locations and using different types of network connections (for example, dial-up, LAN, or wireless).

N

namespace. As relates to the Directory, the external structure of names that is accessible to users.

network address filtering. The process of checking the address of incoming or outgoing e-mail to verify the acceptability of the recipient or sender.

non-repudiation. The use of a digital private key to prevent the signer of a document from falsely denying having signed it.

O

object request broker. In object-oriented programming, software that serves as an intermediary by transparently enabling objects to exchange requests and responses.

OEM. Original equipment manufacturer.

P

plug-in. A program that you can use as part of your Web browser.

principal. In DCE, an entity that can communicate securely with another entity through DCE security. Principles can be users, servers, or computers.

proxy server. An intermediary between the computer requesting access (A) and the computer being accessed (B). Thus, if an end user makes a request for a resource from computer A, this request is directed to a proxy server. The proxy server makes the request, gets the response from computer B, and then forwards the response to the end user. Proxy servers are useful for accessing World Wide Web resources from inside a firewall.

public key. The key in a public/private key pair that is made available to others. It enables them to direct a transaction to the owner of the key or to verify a digital signature. Data encrypted with a public key can be decrypted only with the corresponding private key. *See also* public/private key pair.

public/private key pair. A public/private key pair is part of the concept of key pair cryptography (introduced in 1976 by Diffie and Hellman to solve the key management problem). In their concept, each person obtains a pair of keys, one called the public key and the other called the private key. Each person's public key is made public while the private key is kept secret. The sender and receiver do not need to share secret information: all communications involve only public keys, and no private key is ever transmitted or shared. It is no longer necessary to trust some communications channel to be secure against eavesdropping or betrayal. The only requirement is that public keys are associated with their users in a trusted (authenticated) manner, for instance in a trusted directory. Anyone can send a confidential message by using public information. However, the message can be decrypted only with a private key, which is in the possession of the intended recipient. Furthermore, key pair cryptography can be used not only for privacy (encryption), but also for authentication (digital signatures).

R

remote procedure call. (1) A facility that a client uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation. (2) A client request to a service provider located in another node.

RPC. In DCE, a remote procedure call

S

Secure Sockets Layer (SSL). (1) An IETF standard communications protocol with built-in security services that are as transparent as

possible to the end user. It provides a digitally secure communications channel. (2) An SSL-capable server usually accepts SSL connection requests on a different port than the standard HTTP requests. SSL creates a session during which the handshake needs to happen only once. After the handshake is finished, communication is encrypted. Message integrity checks are performed until the SSL session expires.

SecurID token. The ACE/Server authentication method from Security Dynamics includes a user ID and a SecurID token. When you log in remotely, you get your password from the SecurID token. The password changes every 60 seconds and is good for one-time use only. Even if someone does intercept your password over the open network, the password is not valid for additional use.

server. (1) In a network, a data station that provides facilities to other stations; for example, a file server. (2) In TCP/IP, a system in a network that handles the requests of a system at another site, called a client/server.

SOCKS protocol. A protocol that enables an application in a secure network to communicate through a firewall through a socks server.

socks server. A circuit-level gateway that provides a secure one-way connection through a firewall to server applications in a nonsecure network.

spam. unsolicited e-mail, often sent to a multitude of recipients.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

Transmission Control Protocol/Internet Protocol. A set of communication protocols that support peer-to-peer connectivity functions for local and wide area networks.

U

Universal Resource Locator. The naming convention used for World Wide Web communication where the path of a Web object begins with the service name, the organization name, the path, and the filename, for example, http://www.ibm.com/software/security/firstsecure.

URL. Universal Resource Locator.

V

vault. A vault uses encryption to protect information against disclosure to unauthorized persons such as system administrators and owners of other vaults. It also uses digital signing to protect against tampering, and digital certification to protect against communication with unknown parties. It also uses encryption, signing, and certification to transmit information securely to other vaults.

virtual private network. A private data network that uses the Internet rather than phone lines to establish remote connections. Because users access corporate network resources through an Internet Service Provider (ISP) rather than a telephone company, organizations can significantly reduce remote access costs. A VPN also enhances the security of data exchanges. In traditional firewall technology, message content can be encrypted, but the source and destination addresses are not. In VPN technology, users can establish a tunnel connection in which the entire information packet (content and header) is encrypted and encapsulated.

VPN. Virtual Private Network.

W

Web application. An application designed for access through the World Wide Web.

Web browser. Client software that runs on your desktop PC and enables you to browse the World Wide Web or local pages. It is a retrieval tool that provides universal access to the large collection of hypermedia material available in the Web and Internet. Examples are Netscape Navigator and Microsoft Internet Explorer. *See also* server.

Web object. Data that is made available through a Web browser. A Web object can be a Web page, a part of a Web page, a file, an image, a directory, a CGI program, or a Java applet.

Web server. A server program that responds to requests for information resources from browser programs.

wizard. A dialog within an application that uses step-by-step instructions to guide a user through a specific task.

worm. A computer virus that can do harm.

X

X.509. A widely-accepted certificate standard designed to support secure management and distribution of digitally signed PKI certificates across secure Internet networks. The X.509 certificate defines data structures that accommodate procedures related to distribution of public keys digitally signed by trusted third parties.

Index

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Part Number: CT7EHNA

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

CT7EHNA

SCT7-EHNA-00