IBM® SecureWay® FirstSecure

SCT7-VYNA-00

Up and Running

IBM® SecureWay® FirstSecure

SCT7-VYNA-00

Up and Running

Note

Before using this information and the product it supports, read the general information under Appendix A, “Notices” on page 53.

First Edition (March 1999)

This edition applies to version 1 of IBM SecureWay FirstSecure and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Welcome to IBM® SecureWay® FirstSecure

IBM SecureWay FirstSecure, also known as FirstSecure, provides a comprehensive framework to help your company secure all aspects of networking via the Web and other networks, while helping you build on your current investments with modular, interoperable offerings and reduce the total cost of ownership for conducting secure e-business.

This book describes FirstSecure and contains the following chapters:

- Chapter 1, “What is FirstSecure?” on page 1 gives an overview of FirstSecure, its component products, and the offerings that are available.
- Chapter 2, “Planning for FirstSecure” on page 25 provides information you need to plan your FirstSecure installation.
- Chapter 3, “Installation and Configuration” on page 35 tells you where to find installation information for the FirstSecure component products.
- Chapter 4, “Documentation provided with FirstSecure” on page 45 lists the documentation provided with the FirstSecure component products.

Who should read this book

This book, *Up and Running*, is intended for system administrators in companies that want to integrate security for Web-based systems with legacy-based systems for the first time.

Conventions

Knowing the conventions used in this book will help you use it more efficiently.

- **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.
- *Italics type* indicates new terms, book titles, or variable information that must be replaced by an actual value.
- `Monospace type` indicates an example (such as a fictitious path or file name) or text that is displayed on the screen.

Related information

Information about last-minute updates to FirstSecure is available on the Internet at Web address http://www.software.ibm.com/security/firstsecure/library.

A list of documentation that is included with FirstSecure's component products is given in Chapter 4, “Documentation provided with FirstSecure” on page 45.

Chapter 1. What is FirstSecure?

FirstSecure is part of the IBM Integrated Security Solutions. FirstSecure provides a comprehensive, modular framework to help your company establish a secure e-business environment. By simplifying security, FirstSecure helps reduce the total cost of security ownership, enables security policy to be implemented more easily, and increases the effectiveness of the secure e-business environment.

FirstSecure provides virus protection, access control, traffic content control, encryption, digital certificates, firewall technology, and toolkits. These functions are delivered by IBM's existing family of security products as well as through new offerings from other vendors, combining the best components of many security vendors. Additionally, Implementation Services are available for selected FirstSecure components.

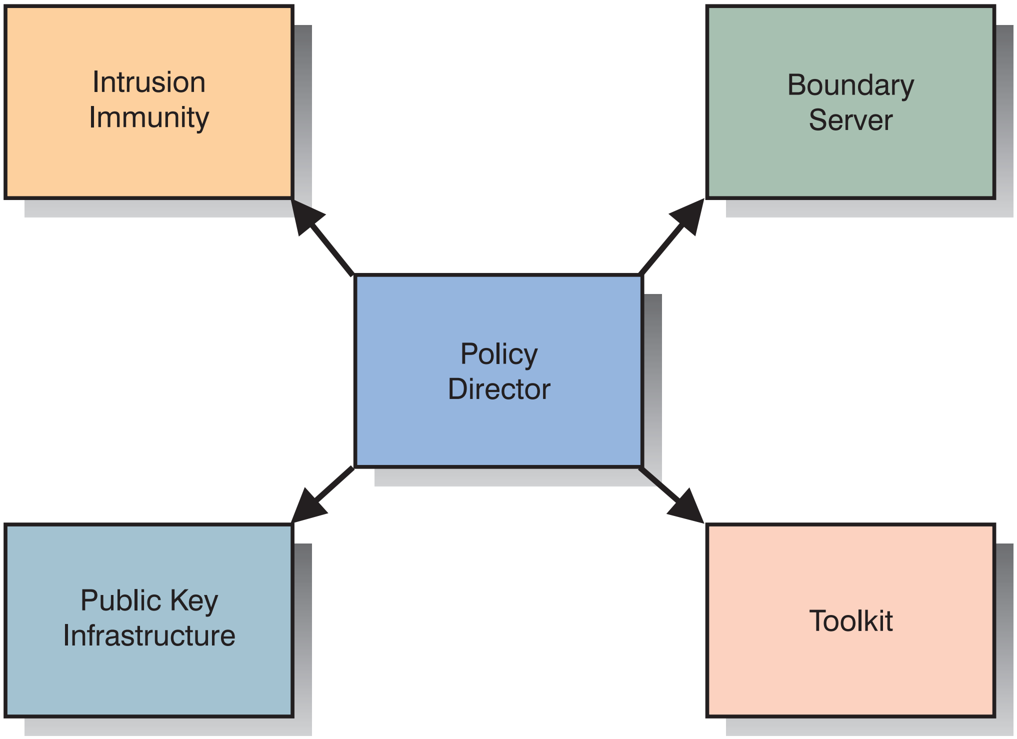
FirstSecure provides a basic foundation for security in your network environment. It enables you to begin to implement and enforce your security policies. This reduces complexity and costs, and allows deployment of Web applications and resources.

What's included in FirstSecure?

FirstSecure contains component products that provide the following types of security technologies:

- Policy Director for a consolidated, policy-driven point of control for heterogeneous Web environments
- Boundary Server, providing security for Web-based e-business applications
- Intrusion Immunity in the form of enterprise antivirus products
- Public Key Infrastructure
- Toolkits for application developers

FirstSecure Implementation Services are intended to get the FirstSecure framework up and operational quickly and efficiently. These services include a workshop, high-level implementation plan, and quickstart installation for selected components of FirstSecure.



To secure your e-business environment, the following offerings are available :

- SecureWay FirstSecure
- SecureWay Boundary Server
- SecureWay Policy Director

The SecureWay FirstSecure offering includes:

- Policy Director:
    - IntraVerse 2.1.2 from DASCOM, which includes the following components:
        - IntraVerse Security Manager, which contains:
            - WebSEAL with GSO™ support
            - NetSEAL
        - NetSEAT Client
        - Security Services
        - Management Console
        - Management Server
        - Directory Services Broker (DSB)
        - Authorization Server
    - IBM Global Sign-On™, Version 2.0.200 (GSO)
- Boundary Server:

  - IBM eNetwork™ Firewall version 3.3, including a two-user license to the Security Dynamics Technologies, Inc., ACE/Server
  - MIMEsweeper Version 3.2 from Content Technologies Ltd.
  - SurfinGate 4.03 for Windows® NT™ from Finjan Software Ltd.
- Intrusion Immunity:
  - Norton AntiVirus Solution Release 3.0.3 from Symantec Corporation
- Public Key Infrastructure:
  - IBM Vault Registry 2.2.2
- Toolkit:
  - IBM KeyWorks Toolkit 1.1
  - IBM Key Recovery Service Provider 1.1

The SecureWay Policy Director offering includes:

- IntraVerse 2.1.2 from DASCOM, which includes the following components:
  - IntraVerse Security Manager, which contains:
    - WebSEAL with GSO support
    - NetSEAL
  - NetSEAT Client
  - Security Services
  - Management Console
  - Management Server
  - Directory Services Broker (DSB)
  - Authorization Server
- IBM Global Sign-On, Version 2.0.200 (GSO)

The SecureWay Boundary Server offering includes:

- IBM eNetwork Firewall version 3.3, including a two-user license to the Security Dynamics Technologies, Inc., ACE/Server
- MIMEsweeper Version 3.2 from Content Technologies Ltd.
- SurfinGate 4.03 for Windows NT from Finjan Software Ltd.

For each offering, a Media Pack and a Documentation Pack are available. Media Packs contain product CDs that you use to install the component products in the offering. Documentation Packs contain hardcopy books for those products that provide them.

More about FirstSecure

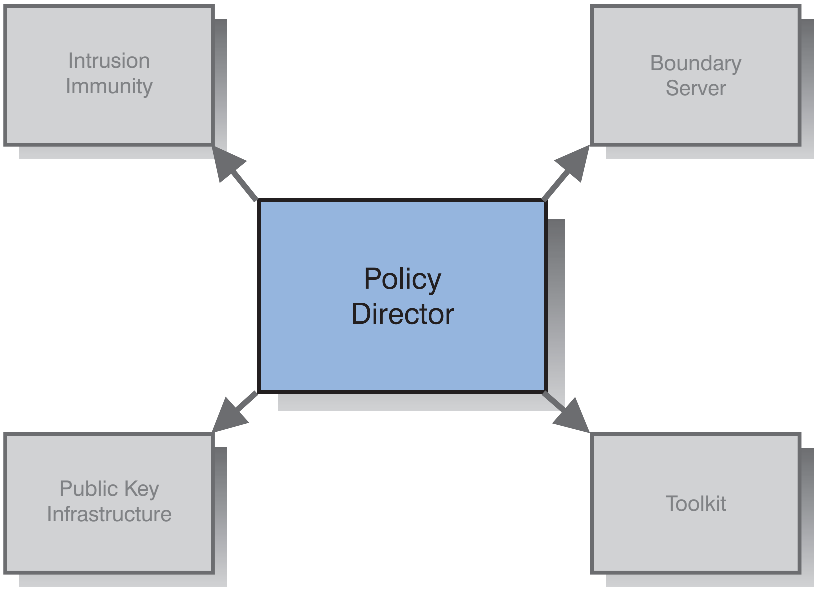
The description of the FirstSecure offering is grouped into the categories of security technologies that are provided:

- Policy Director
- Boundary Server
- Intrusion Immunity
- Public Key Infrastructure
- Toolkit

Policy Director

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, along with the ability to verify identities and perform a fine-grained authorization check of any user who requests access to a protected Web page. With this support, you can authorize and secure:

- HTML, Telnet, and FTP exchanges
- Third-party applications such as database systems
- Network management tools
- Object request brokers
- 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
- X.509 digital 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.

The Policy Director includes:

- IntraVerse 2.1.2, which includes the following components:
  - IntraVerse Security Manager, which contains:
    - WebSEAL with GSO support
    - NetSEAL
  - NetSEAT Client
  - Security Services
  - Management Console
  - Management Server
  - Directory Services Broker (DSB)
  - Authorization Server
- IBM Global Sign-On, Version 2.0.200

IntraVerse 2.1.2

IntraVerse 2.1.2 is a product of DASCOM. The components of IntraVerse 2.1.2 provide security for intranet-based resources and other network resources.

Security Manager: The Security Manager component includes WebSEAL with GSO support and NetSEAL.

WebSEAL with GSO support: WebSEAL helps you secure and manage your intranet-based resources. Access to these resources is available through both your Web-based intranet and the Internet. WebSEAL is a high-performance authorization engine for Web applications.

WebSEAL provides a consolidated point of control for heterogeneous Web environments, allowing you to control authorization of and manage your entire Web site, no matter how many different servers or different types of servers are involved.

WebSEAL extends fine-grained security to industry Web servers including IBM HTTP servers, Apache servers, and Netscape, Oracle, and Microsoft® Web servers. WebSEAL can be used as a smart and secure front end to your existing intranet implementation.

WebSEAL implements a highly scalable, highly available, multi-tiered model for the Web. The tiers are composed of clients, junction servers, and Web servers. As the authorization engine for the Web, WebSEAL allows fine-grained access control to all your Web objects, including HTML pages, graphics, Common Gateway Interface (CGI), Java™ applications, and database queries.

WebSEAL provides user level client/server security on a per-connection basis. WebSEAL is independent of network topology and location.

WebSEAL provides security through the following mechanisms:

Authentication User identities can be positively established through the use of login accounts and encrypted passwords that are managed by the Security Server.

Authorization After the user's identity is positively established, access to parts of your intranet are granted or denied based on the user's identity. Access controls can also be used to allow unauthenticated users (those who did not log in through the Security Server) access to selected sections of your intranet. Access controls are placed on the individual Web objects rather than on the network channel.

Data privacy and integrity
Encryption technology can be used to minimize the risk that your sensitive information could be intercepted or read by unauthorized users or suffer undetected corruption.

Auditing All attempts to access your intranet through WebSEAL can be audited and logged.

WebSEAL integrates with the single sign-on services provided by IBM Global Sign-On, Version 2.0.200. Integrated WebSEAL and GSO provide these benefits:

- Authorization products that can make use of GSO's comprehensive single sign-on and authentication mechanisms, increasing the flexibility and power of the native Web single sign-on solution.
- Back-end servers no longer need to use the same user names as IntraVerse. This makes it easier to integrate legacy systems, where non-Web access methods may already be deployed and it is not possible to integrate tightly with IntraVerse.

NetSEAL: NetSEAL enables your organization to authorize and secure all of your traditional Internet services, such as Telnet and FTP, as well as your 3rd-party applications such as database systems, network management tools, and object request brokers. NetSEAL even enables you to extend access to your in-house applications to users with proper authorization.

Managed access to your network resources is provided to users through both your company's intranet and through the Internet for your remote users without the need to change your existing applications on the client or the server.

NetSEAL separates the authorization policy and the application, providing a level of abstraction between physical and logical views of your security policy for network data.

NetSEAL provides user level client/server security on a per-connection basis. Unlike firewall products, NetSEAL is independent of network topology and location. NetSEAL can be centrally managed for the entire enterprise and can be configured to complement and extend your existing firewall product. When you use NetSEAL with your firewall, your access policy is determined by your business policy.

NetSEAL is a fully extensible authorization engine that allows end-to-end tunneling. This means that by using architecture-independent plug-ins, fine-grained authorization can be applied to new applications. NetSEAL allows integration with third-party authorization infrastructures and provides authorization for applications that include conferencing, database, EDI, and even CORBA ORBs.

NetSEAL provides security in the following ways:

Authentication User and server system identities can be positively established through the use of login accounts and encrypted passwords managed by the Security Server. NetSEAL provides mutual authentication for clients and servers.

Authorization After identity is positively established, access to network based applications is granted or denied based on the user's identity. Access controls can also be used to allow unauthenticated users (those who did not log in through the Security Server) access to selected sections of the network. Access controls are placed on the individual network objects rather than on the network channel. Authorization is available at the application level on both the client and the server.

Data privacy and integrity
Encryption technology can be employed to minimize the risk that your sensitive information could be intercepted or read by unauthorized users or suffer undetected corruption.

Auditing All attempts to access a resource secured by NetSEAL can be audited and logged.

NetSEAL provides a complete secure authorization and network management solution. It enables you to effectively manage your network environment and provide access to secured information to both internal and external users.

NetSEAT Client: NetSEAT is a small network services module that resides on a client machine. NetSEAT acts as a proxy for communication between the client application and one or more IntraVerse servers. The NetSEAT client provides full integration with the IntraVerse security mechanism.

NetSEAT also provides security, remote procedure call (RPC), and directory services for DCE applications on the machine. NetSEAT helps to reduce installation and configuration effort, making it easier to deploy applications based on DCE. NetSEAT supports multi-cell capabilities, allowing users to log in to several different secure domains simultaneously.

The NetSEAT Client intercepts all outgoing TCP/IP traffic and, when necessary, tunnels the traffic to the NetSEAL server on the destination machine. It also intercepts all outgoing HTTP requests and can forward the requests to the destination WebSEAL server. It transparently maps logical URLs to physical WebSEAL servers, allowing Web resources to be relocated or replicated without affecting the end-user.

Security Server: The Security Server contains all the underlying services responsible for ensuring a secure environment. The Security Server provides a centralized authentication service for all principals in the secure domain.

The Security Server maintains a centralized registry database that contains an account entry for all valid users who participate in the secure domain. This registry database can be replicated throughout the secure domain to prevent a single point of failure.

Management Console: The Management Console is a graphical application used to securely manage all IntraVerse components. From the Management Console, you manage the Security Server registry, the master authorization database, and all IntraVerse servers. The Management Console also allows you to add and delete users or groups and apply access controls (ACLs) to objects. It uses the NetSEAT Client to perform these management tasks through secure communication channels.

Management Server: The Management Server maintains the master authorization (ACL) database for the secure domain. The Management Server is responsible for updating all authorization database replicas throughout the secure domain. The Management Server also maintains location information about the other IntraVerse servers in the secure domain.

Directory Services Broker: To make the NetSEAT Client as lightweight as possible, the traditional Cell Directory Service has been moved off the client machine. Instead, the Directory Services Broker (DSB) is used by the NetSEAT client as a gateway to the directory service.

The DSB is installed on a server machine and is shared by many clients. Multiple DSBs can be installed in a cell to provide high availability and load balancing.

Authorization Server: The NetSEAL authorization service includes an application programming interface (API) that can be used from within any application to provide that application with sophisticated access control processing.

The Authorization Server allows these custom applications to use the IntraVerse Authorization Service to make fine-grained application level authorization decisions.

Several Authorization Servers can be installed in a secure domain to provide high availability and load balancing.

More information about IntraVerse 2.1.2 can be found in the *IntraVerse 2.1 for Windows NT Release Notes, Version 2.1.2*; the *IntraVerse 2.1 for AIX Release Notes, Version 2.1.2*; or the *IntraVerse 2.1 for Solaris Release Notes, Version 2.1.2*. All of these documents are included in the FirstSecure Documentation Pack and the Policy Director Documentation Pack.

Note: Although the IntraVerse documentation may provide a DASCOM contact for service and support, if you obtain IntraVerse 2.1.2 as part of the SecureWay FirstSecure offering or the SecureWay Policy Director offering, you should contact IBM for service and support.

IBM Global Sign-On

IBM Global Sign-On (GSO) is a product of the IBM Corporation. This version of GSO is intended for customers who want a coordinated login to Web-based resources in conjunction with the IntraVerse 2.1.2 product only. GSO provides enhanced support to the IntraVerse WebSEAL solution by allowing users to access Web resources using their existing identities even when these user names are not within the IntraVerse user namespace. For example, a user has different user IDs on different systems but only one user ID on IntraVerse. When using IntraVerse alone, only the IntraVerse user ID is used to access multiple Web resources. But when GSO is used in conjunction with IntraVerse, the appropriate user ID can be used to access each Web resource.

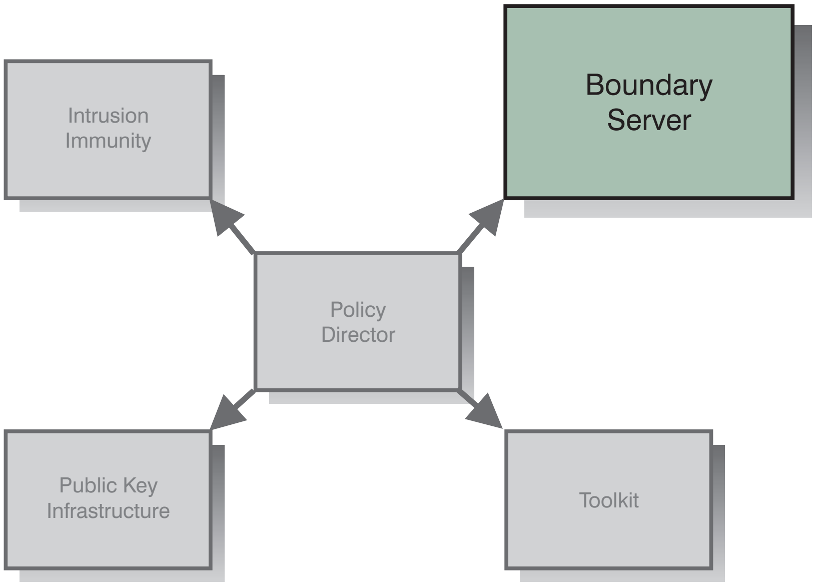
When you use both IntraVerse and GSO, IntraVerse's authorization products use GSO's single sign-on and authentication mechanisms, giving you an IntraVerse Web single sign-on solution that is more flexible and powerful than when you use IntraVerse alone.

Tivoli™ GSO is the recommended solution for customers who want an enterprise single sign-on solution for logging on to host-based resources, network operating systems, and databases.

More information about IBM Global Sign-On can be found in *IBM Global Sign-On, Version 2.0.200 Up and Running*, which is included in the FirstSecure Documentation Pack and the Policy Director Documentation Pack.

Boundary Server

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

Boundary Server includes:

- IBM eNetwork Firewall version 3.3, including ACE/Server
- MIMEsweeper version 3.2
- SurfinGate 4.03 for Windows NT

IBM eNetwork Firewall version 3.3

IBM eNetwork Firewall version 3.3, also known as IBM Firewall, enables safe, secure e-business by controlling all communications to and from the Internet. This firewall technology has been protecting IBM's assets and the assets of other global corporations for more than ten years. IBM Firewall contains all three critical firewall architectures – filtering, proxy, and circuit level gateway – to provide customers with a high level of both security and flexibility.

Companies have many concerns about networking. Among those concerns are:

- The need to connect to the Internet but prevent unauthorized access to the company's network, applications, and data
- Abuse of the company's networking assets by internal users
- Deployment of 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.

Vendors and business partners can be safely connected over the Internet, and their access to your network can be strongly controlled by establishing a VPN tunnel. This ensures that the partner has access to only the networks, servers, or applications you permit the partner to use.

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.

Provided with IBM Firewall is a two-user 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. For implementations that require it, this provides authentication that relies on two factors: users are required to both *have* something (a SecurID token card) and *know* something (a PIN) to be authenticated.

More information about IBM Firewall can be found in one of the following books, depending on your operating system:

- *IBM eNetwork Firewall for Windows NT Version 3.3 Setup and Installation for Multiple Languages*
- *IBM eNetwork Firewall for AIX Version 3.3 Setup and Installation for Multiple Languages*

These documents are included in the FirstSecure Documentation Pack and the Boundary Server Documentation Pack.

MIMEsweeper Version 3.2

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

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.

MAILsweeper can be used to:

- 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 be used to:

- Block employees from certain sites that are not likely to be work-related
- Detect and, if necessary, block dangerous Java applets and ActiveX controls before they enter the network
- 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.

More information about MIMEsweeper can be found in *MIMEsweeper Administrator's Guide Version 3.2* which is provided on the MIMEsweeper product CD.

Note: Although the MIMEsweeper documentation may provide a Content Technologies contact for service and support, if you obtain MIMEsweeper 3.2 as part of the SecureWay FirstSecure offering or the SecureWay Boundary Server offering, you should contact IBM for service and support.

SurfinGate 4.03 for Windows NT

SurfinGate 4.03 is a product of Finjan Software Ltd. SurfinGate 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 three components:

- SurfinGate Server
- SurfinConsole
- SurfinGate database

The SurfinGate Server acts as an HTTP proxy server or as a service to the firewall or proxy. 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.

SurfinConsole is the user-friendly interface that the network administrator can use to manage and set a central corporate security policy for mobile code. 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/acceptable code.

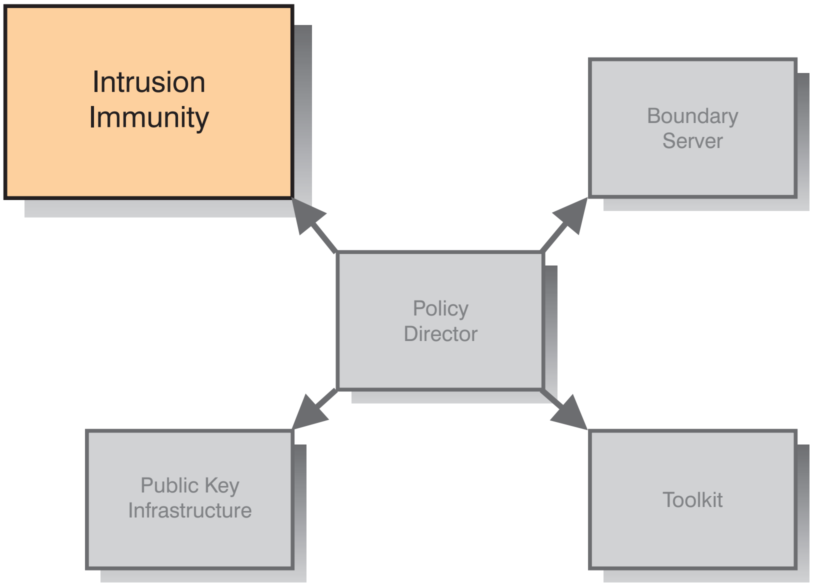
The SurfinGate database stores details of Applet Security Profiles (ASPs), including information about users and groups and their corresponding security policies. Because SurfinGate inspects the content of all mobile code dynamically, the database is not required for security, but it does help improve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

More information about SurfinGate can be found in *SurfinGate 4.03 for Windows NT Installation Guide*, which is included in the FirstSecure Documentation Pack and the Boundary Server Documentation Pack.

Note: Although the SurfinGate documentation may provide a Finjan contact for service and support, if you obtain SurfinGate 4.03 for Windows NT as part of the SecureWay FirstSecure offering or the SecureWay Boundary Server offering, you should contact IBM for service and support.

Intrusion Immunity

The security technologies described so far emphasize *protection* from security threats. An equally important aspect of security is *detection* of threats. Intrusion immunity products in FirstSecure provide state-of-the-art antivirus capabilities that allow your company to detect security threats.



Antivirus software provides protection from all kinds of 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. This ensures a comprehensive and consistent approach to addressing 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. This level of control assures that your antivirus policies are being put into effect.

Intrusion Immunity in FirstSecure is provided by Norton AntiVirus Solution Release 3.0.3.

Norton AntiVirus Solution Release 3.0.3

Norton AntiVirus Solution Release 3.0.3 is a product of Symantec Corporation. Norton AntiVirus is one of the world's leading antivirus software products. Features in this version let you quarantine infected files and easily get help from Symantec researchers, and this version of Norton AntiVirus automatically helps protect you against viruses as well as malicious ActiveX controls and Java applets. Norton AntiVirus can run constantly in the background to help keep your computer safe from viruses that might come in from e-mail attachments, Internet downloads, floppy diskettes, software CDs, or a network. Norton AntiVirus can be scheduled to automatically retrieve new antivirus definitions from Symantec as often as once a week.

The quarantine feature of Norton AntiVirus 5.0 isolates infected or suspicious files in a safe location on your computer, separated from other files. This helps prevent the spread of the virus while you fix the file.

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

The LiveUpdate feature of Norton AntiVirus lets you download only the new virus definitions you need from Symantec quickly and efficiently. You can receive fully tested virus definition updates weekly.

Norton AntiVirus provides protection against malicious code, thus helping you surf the Internet with greater safety. Besides detecting viruses, Norton AntiVirus can automatically block destructive ActiveX controls, Trojan horses, and Java applets from entering your computer. SARC's team of virus experts develops identification and detection for new computer viruses that appear, and these experts provide either a repair or a delete operation to protect you against the latest virus threats.

Norton AntiVirus can run constantly in the background to help keep your workstations, servers, and gateways safe. Its heuristics scanner, Bloodhound, watches and categorizes 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 3.0.3 products provided in FirstSecure are:

- Desktop Solutions:
  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.01 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 4.0
  - Norton AntiVirus 5.01 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.0 for OS/2
- Server Solutions:
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.01 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 1.02 for Lotus Notes™
  - Norton AntiVirus 1.5 for Microsoft Exchange
- Gateway Solutions:
  - Norton AntiVirus 1.02 for Internet Email Gateways for NT

  - Norton AntiVirus 1.01 for Firewalls

- Administration:

  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli IT Director
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise
  - Other Administration Tools, including Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

More information about Norton AntiVirus can be found in the file named contents.txt, which is in the root directory of the Norton AntiVirus CD.

Note: Although the Norton AntiVirus documentation may provide a Symantec contact for service and support, if you obtain Norton AntiVirus Solution Release 3.0.3 as part of the SecureWay FirstSecure offering, you should contact IBM for service and support.

Public Key Infrastructure

Companies today need a public-key infrastructure to secure e-business applications, and FirstSecure 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

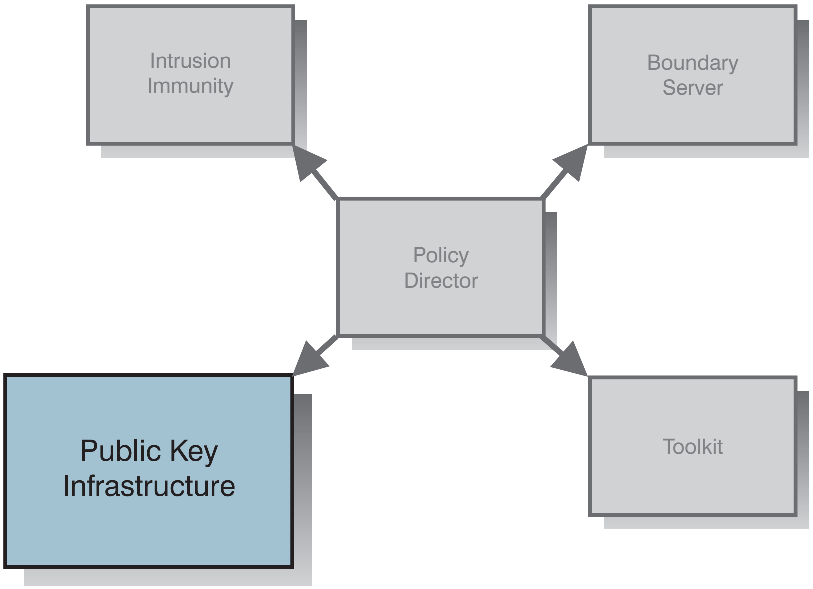
  - A registration authority to approve certificate requests

  - A certificate authority to create and publish 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 authorities into separate trusted domains.



The enhanced trust model helps ensure that the integrity, authenticity, and information privacy of your registration transactions are not compromised. Unauthorized third parties (including system administrators and system operators) are prevented from accessing sensitive registration data or invoking the registration applications. Data is protected in special areas of memory through the use of digital certificates and encryption for authentication, access control, and privacy. The certificate authority is designed to work with cryptographic hardware for extra security.

In FirstSecure, the Public Key Infrastructure is provided through IBM Vault Registry.

IBM Vault Registry 2.2.2

IBM Vault Registry 2.2.2 provides an integrated solution for registering and certifying users who must access, through the Web, sensitive documents, services, and e-business applications controlled by company policies. With IBM Vault Registry, your company can establish the level of trust you need to conduct e-business on the Internet with confidence and security.

Digital certificates are evolving as an accepted means for authentication and access control over untrusted networks, but the certificates are only as valuable as the degree of trust and security involved in registering and certifying the participants. IBM Vault Registry provides a robust, integrated, security-rich solution for managing the registration of and issuance of digital certificates to trusted entities.

IBM Vault Registry provides seamless integration of the components you need to run your own Certificate Authority (CA), reducing the cost and complexity of assembling such a system from multiple vendor offerings. It implements an enhanced trust model that reduces the risk of compromise to the integrity, authenticity, and information privacy of registration transactions. Registration data and the applications themselves are shielded from unauthorized users, whether external or internal. Using digital certificates for authentication and access control, data is protected in special areas of memory (*vaults*) against unauthorized access. The vault software can be compared to a safe deposit box at the bank that protects valuable assets even from bank employees.

IBM Vault Registry is scalable to meet the growing needs of your business, and it offers the flexibility of customization, which helps to protect your investment.

IBM Vault Registry provides you the security and robust operations capability you need to support your high-trust, multi-CA environment under consolidated systems management.

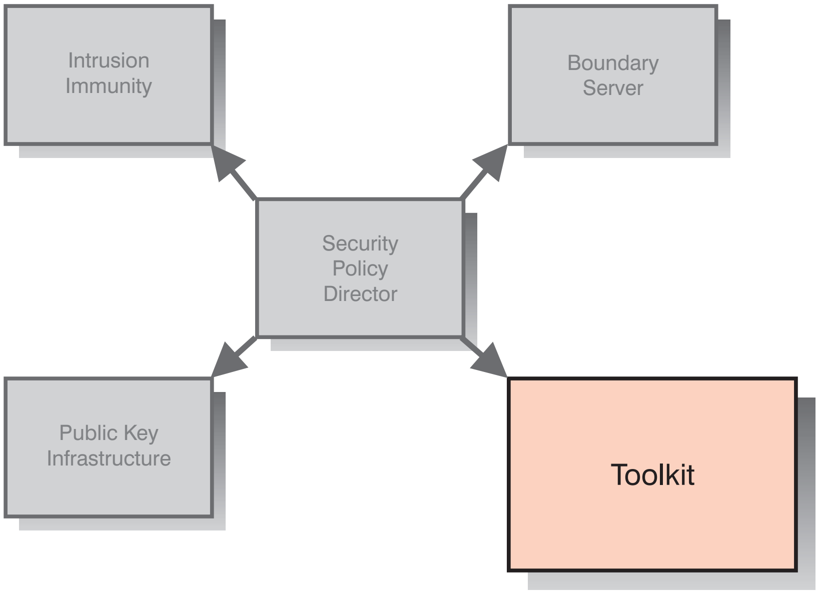
Included in IBM Vault Registry is the IBM Vault Controller component. IBM Vault Controller provides and manages execution environments for server programs that are running on behalf of users who identify themselves using public key credentials. Separate and persistently unique execution environments and resources are dedicated to each authorized individual. These environments and resources, known as vaults, are accessible from any SSL-enabled Web browser that contains the corresponding vault access certificates. Information stored in vaults is protected against disclosure to unauthorized persons by encryption (for example, system administrators and other vault owners), against tampering by digital signing, and against untrusted communications with unknown parties by using digital certificates. Information can also be transmitted to other vaults using encryption, signing, and certificates for security. All vaults managed by a single instance of the IBM Vault Controller use a single instance of a vault certificate management system, called the Vault CA. The Vault CA issues and manages the vaults' encryption, signing, and vault access (SSL) certificates.

Additionally, IBM Vault Registry requires you to install IBM DB2® Universal Database™ Enterprise Edition, Version 5.2, and IBM eNetwork LDAP Directory Server Version 2.1, which are included with IBM Vault Registry 2.2.2.

More information about IBM Vault Registry can be found in the *IBM Vault Registry Installation and Configuration Guide*, which is provided in the FirstSecure Documentation Pack.

Toolkit

The FirstSecure Security ToolBox is a set of tools, most of which use Public Key technology and certificates to provide cryptology and trust policies in support of FirstSecure.



The Security ToolBox products initially included in FirstSecure are:

- IBM KeyWorks Toolkit, a software development kit (SDK)
- IBM Key Recovery Service Provider Toolkit

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 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/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. It is strongly recommended that integrators using IBM KeyWorks Toolkit have on staff systems engineers and programmers 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 these 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*, which is provided in the FirstSecure Documentation Pack.

IBM Key Recovery Service Provider Toolkit 1.1

The IBM Key Recovery Service Provider 1.1, 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 can be found in the *Key Recovery Server Installation and Usage Guide*, which is provided in the FirstSecure Documentation Pack.

Implementation Services

The FirstSecure Implementation Services are intended to get the FirstSecure framework up and operational quickly and efficiently. These separately billable services are provided by IBM and are performed by an experienced team of consultants. The close ties of IBM's services organization to the product development organization enhances access to product expertise and increases the level of effective resolution of implementation issues.

The FirstSecure Implementation Services include a workshop, development of a high-level implementation plan, and quickstart installation.

Workshop The workshop covers design, architecture, and education for the SecureWay Policy Director, SecureWay Boundary Server, and IBM Vault Registry.

Implementation Plan A high-level implementation plan is developed using the information gathered during the workshop.

QuickStart Pilot Installation
Selected FirstSecure components are installed and tested in a non-production environment. Customers select which components, and how many, to install and test based on the number of registered users acquired.

There is a tier approach to the level of services that is provided by the FirstSecure offering. This tier approach is based on the number of registered users. Contact your IBM representative for information and pricing options.

Year 2000 Readiness

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

Service and Support

Contact IBM for service and support of **all the products** included in the SecureWay FirstSecure offering, the SecureWay Boundary Server offering, or the SecureWay Policy Director offering.

Chapter 2. Planning for FirstSecure

Before you install the FirstSecure component products, be sure to read the following sections to make sure that you have the necessary hardware and software. Information about last-minute updates to FirstSecure is available on the Internet at Web address http://www.software.ibm.com/security/firstsecure/library. Be sure to read the information before you start installing.

Instructions for installing and configuring the component products of FirstSecure are provided in the product literature for each of the component products. See Chapter 3, “Installation and Configuration” on page 35 for a list of the component products and information about locating the installation and configuration instructions for each product.

General system requirements

The general hardware and software requirements for FirstSecure are listed in this section. For specific hardware requirements for each of the component products, see “Hardware requirements” on page 26. For software requirements for the component products, see “Software requirements” on page 30.

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

- AIX Version 4.3.x or later
- Microsoft Windows NT Version 4
- Sun Solaris Version 4.3 or higher

Each of the FirstSecure component products runs on at least one of these operating systems. “Software requirements” on page 30 shows the supported operating system platforms and other prerequisite software for each component product.

Component product requirements

The sections that follow show the hardware and software requirements for the FirstSecure component products.

Hardware requirements

The tables in this section list hardware requirements for the FirstSecure component products. There is a table for each of the security technologies provided in FirstSecure.

Policy Director

Hardware requirements for the Policy Director component products are shown in the following table.

Table 1. Hardware requirements for Policy Director component products

Policy Director Component	Machine Type	Disk Space	Memory
IntraVerse, including: • NetSEAL • WebSEAL with GSO support	NT server: Intel or Intel-compatible 80486 33mHZ or higher AIX server: hardware that runs AIX 4.3.1 Solaris server: hardware that runs Solaris 2.5.1	All platforms: 16MB	All platforms: 64MB
NetSEAT	Intel or Intel-compatible 80486 33mHZ or higher	2MB	NT Client: 32MB Windows 95/98 Client: 16MB
IBM Global Sign-On[1]	Client or NT server: Intel or Intel-compatible 80486 33mHZ or higher AIX server: hardware that runs AIX 4.3.1 Solaris server: hardware that runs Solaris 2.5.1	NT server: 12MB NT or Windows 95/98 Client: 10MB AIX server: 2MB Solaris server: 6MB	NT server: 32MB NT Client: 24MB Windows 95/98 Client: 16MB AIX server: 64MB Solaris server: 64MB

Notes:

1. See *IBM Global Sign-On, Version 2.0.200 Up and Running* for more information.

Boundary Server

Hardware requirements for the Boundary Server component products are shown in the following table.

Table 2. Hardware requirements for Boundary Server component products

Boundary Server Component	Machine Type	Disk Space	Memory	Other
IBM Firewall[1]	NT: Pentium® 133 or higher AIX: RS/6000 machine that supports AIX 4.3.2	NT: 24MB[2] AIX: 307MB	NT: 64MB AIX: 64MB	2 network interface cards
ACE/Server	NT: Pentium 166 or higher (single processors only) AIX: Machine that supports AIX 4.2	Primary server software: 50 MB Backup server: 22MB Initial user database: 4MB Installation: 240MB	Minimum: 32MB	Actual storage requirements are based on user population
SurfinGate 4.03				
Server	Pentium 233 or higher	20MB	Minimum: 128MB Recommended: 256MB	
Console	Pentium 233 or higher	15MB	Minimum: 32MB Recommended: 64MB	
MIMEsweeper				
MAILsweeper	Pentium 200 or higher	1GB	64MB	1 network interface card
WEBsweeper	Pentium 266 or higher	1GB	64MB + 1MB for each concurrent Web connection	1 network interface card

Notes:

1. See *IBM eNetwork Firewall for AIX Version 3.3 Setup and Installation for Multiple Languages* or *IBM eNetwork Firewall for Windows NT Version 3.3 Setup and Installation for Multiple Languages* for more detailed information.
2. 13MB of Disk Space is also required for the Netscape Browser.

Intrusion Immunity

Hardware requirements for the Intrusion Immunity component products are shown in the following table.

Table 3. Hardware requirements for Intrusion Immunity component product

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

Public Key Infrastructure

Hardware requirements for the Public Key Infrastructure component products are shown in the following table.

Table 4. Hardware requirements for Public Key Infrastructure component product

Public Key Infrastructure Component	Machine Type	Disk Space	Memory
IBM Vault Registry	RS/6000® machine of type: 7017-S70, 4-, 8-, or 12-way SMP 7025-F50, 1- to 4-way deskside SMP 7026-H50, 1- to 4-way rack SMP	Dependent on installation type. See Table 5 on page 30 for details.	Dependent on installation type. See Table 5 on page 30 for details.

The recommended hardware configuration for IBM Vault Registry is dependent on your use of the product. The following table lists minimum hardware requirements for IBM Vault Registry for different type of installations.

Table 5. Minimum Hardware Requirements for IBM Vault Registry by installation type

Installation Type	Number of Processors	Disk Space	Memory
Proof of concept pilots	2	9GB	512MB
Small development environments	2	9GB	512MB
Small production environments	4	18GB	1GB
Large development environments	4	18GB	1GB
Large production environments	8	18GB	1GB

Toolkit

Hardware requirements for the Toolkit component products are shown in the following table.

Table 6. Hardware requirements for Toolkit component products

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

Software requirements

The tables in this section list software requirements for the FirstSecure component products. There is a table for each of the security technologies provided in FirstSecure.

Policy Director

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

Table 7. Software requirements for Policy Director component products

Policy Director Component	Microsoft Windows platforms		AIX	Solaris
	Client	Server	Server	Server
IntraVerse, including: • NetSEAL • WebSEAL with GSO support	Not Available	Windows NT Server 4.0, Service Pack 3	AIX 4.3 or higher	Sun Solaris 2.5.x
NetSEAT	Windows NT 4.0, Service Pack 3 Windows 95, Windows 98	Not Available	Not Available	Not Available
IBM Global Sign-On[1,2]	Windows NT 4.0, Service Pack 3 Windows 95, Windows 98	Windows NT 4.0, Service Pack 3	AIX 4.3	Sun Solaris 2.5.1

Notes:

1. Before configuring GSO, the DCE client must be installed. See *IBM Global Sign-On, Version 2.0.200 Up and Running* for information.
2. The OS/2® client is not supported.

Boundary Server

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

Table 8. Software requirements for Boundary Server component products

Boundary Server Component	Microsoft Windows platforms		AIX	Solaris
	Client	**Server**	**Server**	**Server**
IBM Firewall	Windows 95, IPSEC client	Windows NT Server 4.0, Service Pack 3[1]	AIX 4.3.2	Not Available
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 or higher	Windows NT Server 4.0, Service Pack 2 or higher	AIX 4.2	Solaris 2.5.1
SurfinGate 4.03				
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				
MAILsweeper	Not Available	Windows NT 4.0[3]	Not Available	Not Available
WEBsweeper	Not Available	Windows NT 4.0[4]	Not Available	Not Available

Notes:

1. IBM Firewall for NT also requires:
   - Post Service Pack 3 Hot Fixes, installed in the following order:
     a. ndis-fix
     b. dns-fix
     c. simptcp-fix (chargeni.exe)
     d. teardrop2-fix
   - Target drive and Windows NT drive must be formatted with NTFS
2. In addition:
   - Windows network client for Microsoft Windows is required.
   - NT Workstation is not supported.
3. In addition:
   - NT 3.5.1 and NT Workstation are not supported.
   - One of the following environments is required:
     – Microsoft Exchange
     – SMTP
     – cc:Mail™
     – Groupwise
     – Lotus Notes
4. NT Workstation is not supported.

Intrusion Immunity

Software requirements for the Intrusion Immunity component product are shown in the following table.

Table 9. Software requirements for Intrusion Immunity component product

Intrusion Immunity Component	**Microsoft Windows platforms**		**AIX**	**OS/2**
	Client	**Server**	**Server**	**Client**
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98 Windows 3.1 DOS 5.0	Windows NT 4.0	Not Available	OS/2 2.11 or higher

Notes:

1. In addition, a TCP/IP Internet connection is required for Norton AntiVirus for Internet Email Gateways.

Public Key Infrastructure

Software requirements for the Public Key Infrastructure component product are shown in the following table.

Table 10. Software requirements for Public Key Infrastructure component product

Public Key Infrastructure Component	Microsoft Windows platforms		AIX	Solaris
	Client	Server	Server	Server
IBM Vault Registry[1]	Vault Agent, Vault Certificate Validator: Windows NT 4.0	Vault Agent: Windows NT 4.0	Vault Registry: AIX/6000® Version 4.3.2	Not Available

Notes:

1. In addition:
   - For Vault Controller, the Web server product supplied with Vault Registry is required.
   - You must also install IBM DB2 Universal Database Enterprise Edition, Version 5.2 with FixPacks U459852 and U461709, and IBM eNetwork LDAP Directory Server Version 2.1, which are provided with IBM Vault Registry 2.2.2.
   - One of these Web browsers is required:
     - Netscape Navigator 4.0 or higher
     - Netscape Communicator 4.0 or higher
     - Microsoft Internet Explorer 4.0 or higher
   - AIX client is also supported.

Toolkit

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

Table 11. Software requirements for Toolkit component products

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

Notes:

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

Chapter 3. Installation and Configuration

Instructions for installing and configuring the FirstSecure component products are provided in the documentation for each of the products. The sections that follow tell you where you can find installation and configuration information for each component product. In addition, if there is helpful installation or configuration information that is not included in the documentation for a component product, it is described in the “Additional considerations” section for that product.

Policy Director

The following sections describe the installation and configuration documentation for the Policy Director component products.

See Web address http://www.software.ibm.com/security/firstsecure/library on the Internet for a list of the current software prerequisites for Policy Director.

IntraVerse 2.1.2

Information about planning for and installing IntraVerse 2.1.2 is provided in one of the following documents, depending on your operating system.

Windows NT	*IntraVerse 2.1 for Windows NT Release Notes, Version 2.1.2*
AIX	*IntraVerse 2.1 for AIX Release Notes, Version 2.1.2*
Solaris	*IntraVerse 2.1 for Solaris Release Notes, Version 2.1.2*

In addition, information about planning for and installing the NetSEAT Client is provided in the *IntraVerse NetSEAT Client Release Notes.* This PDF file can be accessed on the NetSEAT CD from the file \NetSEAT\Docs\index.html.

Before you begin to install, be sure to read “Additional considerations.”

Additional considerations

The following sections describe additional installation and configuration considerations for IntraVerse 2.1.2.

Installing both IntraVerse and IBM Global Sign-On: Be sure to read the following information if you plan to install both IntraVerse 2.1.2 and IBM Global Sign-On.

Installing the GSO client and the IntraVerse client: The recommended GSO administration console machine contains the following IntraVerse and GSO components:

- IntraVerse NetSEAT Client
- GSO administration console (GSO client)
- IntraVerse Management Console

To install and configure these components, use the following procedure:

1. Using the IntraVerse 2.1 Upgrade CD, install and configure:
   a. IntraVerse NetSEAT Client 2.1.2
   b. IntraVerse Management Console
2. Using the GSO CD, install and configure the GSO administration console

Note: Both the IntraVerse Management Console and the GSO administration console require and provide a version of IntraVerse NetSEAT. When installing these console products on the same machine, always install *only* the IntraVerse version of the NetSEAT Client. Therefore, do *not* install the NetSEAT client from the GSO CD, as documented in the *IBM Global Sign-On, Version 2.0.200 Up and Running* book. In addition, do *not* use the cfgclient command to configure the NetSEAT client.

Installing the GSO server and the IntraVerse servers: The recommended GSO server machine contains the following components:

- DCE
- GSO server
- IntraVerse NetSEAT Client (Windows NT only)
- IntraVerse servers (including IntraVerse WebSEAL and IntraVerse NetSEAL)

To install and configure these components, use the following procedure:

1. Using the GSO CD, install:
   a. DCE
   b. GSO server
2. Configure DCE
3. Using the IntraVerse 2.1 Upgrade CD, install the Directory Services Broker (DSB) supplied by IntraVerse as follows:
   a. On a Windows NT machine with NetSEAT 2.1.2 installed, install the enterprise deployment toolkit (EDT). The EDT contains various versions of the DSB. Refer to Section 6.1 of the *IntraVerse NetSEAT Client Administration Guide* for instructions.

b. Copy the correct DSB from the Windows NT machine to the IntraVerse server. For complete instructions, see the *IntraVerse NetSEAT Client Administration Guide*. However, do not install the DSB in the DCE directory on the server machine, as is documented in the *IntraVerse NetSEAT Client Administration Guide*. Instead, do the following:

   - Rename the existing DSB that was supplied with the GSO server.
   - Copy the DSB supplied with the IntraVerse server into the GSO directory that contains the renamed DSB.

   Note: Both the IntraVerse server and the GSO server require and provide a version of the IntraVerse DSB. When installing both the IntraVerse and the GSO servers on the same machine, install *only* the IntraVerse version of the DSB. Therefore, do *not* install the DSB from the GSO CD, as documented in the *IBM Global Sign-On, Version 2.0.200 Up and Running* book.

   If the GSO server has already been configured on the machine, the GSO-supplied DSB is configured and started. If this is the case, the DSB must be stopped before it can be replaced with the IntraVerse-supplied DSB.

4. Configure GSO.
5. Using the IntraVerse 2.1 Upgrade CD, install and configure:
   - NetSEAT 2.1.2 (Windows NT only)
   - The IntraVerse servers

IBM Global Sign-On, Version 2.0.200

Installation information for IBM Global Sign-On, Version 2.0.200 is provided in the hardcopy book *IBM Global Sign-On, Version 2.0.200 Up and Running*.

Before you begin to install, be sure to read “Additional considerations.”

Additional considerations

The following sections describe additional installation and configuration considerations for IntraVerse 2.1.2.

Installing both IBM Global Sign-On and IntraVerse: Be sure to read the following information if you plan to install both IntraVerse 2.1.2 and IBM Global Sign-On.

Installing the GSO client and the IntraVerse client: For information about installing both the GSO client and the IntraVerse client, see “Installing the GSO client and the IntraVerse client” on page 36.

Installing the GSO server and the IntraVerse servers: For information about installing both the GSO server and the IntraVerse servers, see "Installing the GSO server and the IntraVerse servers" on page 36.

Boundary Server

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

IBM eNetwork Firewall version 3.3

Information about installing IBM Firewall is provided in one of the following hardcopy books, depending on your operating system:

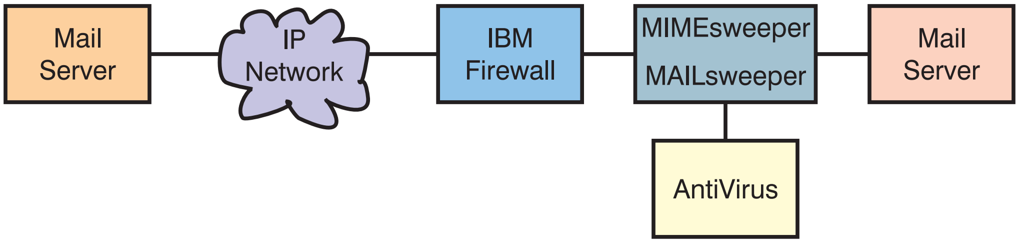
Windows NT	*IBM eNetwork Firewall for Windows NT Version 3.3 Setup and Installation for Multiple Languages*
AIX	*IBM eNetwork Firewall for AIX Version 3.3 Setup and Installation for Multiple Languages*

Information about installing ACE/Server is in the hardcopy booklet, *Quick Start Guides*. The booklet contains a section for installation and administration for each supported platform.

Additional considerations

The following information describes additional installation and configuration considerations, as well as sample configurations, for IBM Firewall.

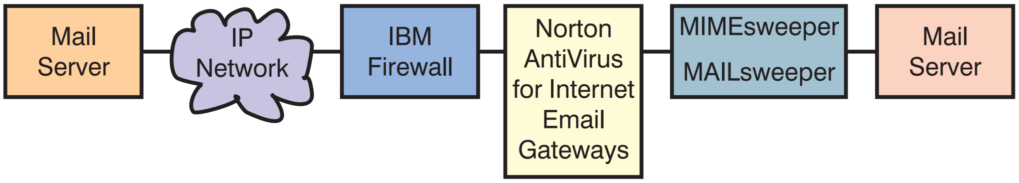
IBM Firewall and MAILsweeper sample configuration: When you are installing both IBM Firewall and MIMEsweeper, you can use the setup described in this section.



- MAILsweeper is the part of MIMEsweeper that checks the content of mail messages. MAILsweeper has a function to enable antivirus checks.

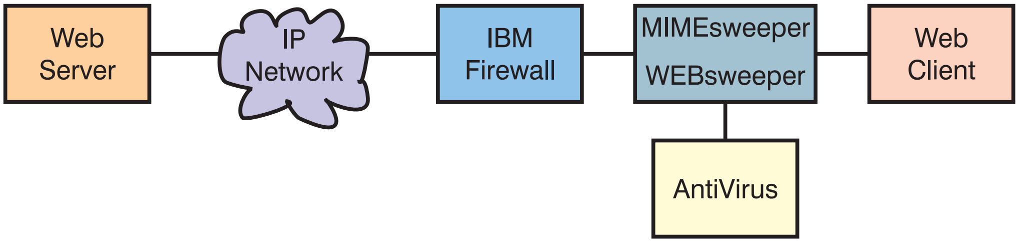
- MAILsweeper sits between IBM Firewall and the secure SMTP servers.
- IBM Firewall points to MAILsweeper as the mail host to forward mail.
  - IBM Firewall requires that the predefined mail rules be set up to allow mail traffic to flow. These rules are defined in the *IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide*.
- 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 setup 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.



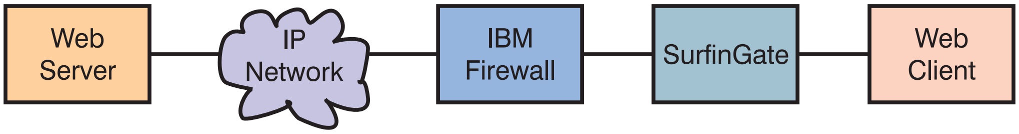
- The firewall points to Norton AntiVirus for Internet Email Gateways as its secure mail server. The correct firewall rules must be set to allow this specific traffic.
- Norton AntiVirus for Internet Email Gateways points to MAILsweeper as its mail forwarder for secure mail and to the firewall for mail destined outbound.
- MAILsweeper receives and checks mail forwarded to it. It then forwards it 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 setup described in this section.



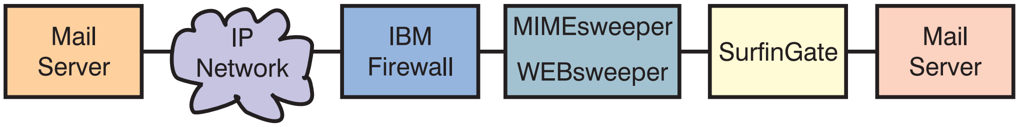
- WEBsweeper is the part of MIMEsweeper that checks Web traffic. WEBsweeper has a function to enable antivirus checks.
- WEBsweeper works as an intermediate proxy. Clients point to WEBsweeper as their proxy. WEBsweeper is then set to forward traffic to the firewall proxy.
- Rules must be set up on the firewall to allow proxy traffic. 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. 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 setup 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. 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.

IBM Firewall, MIMEsweeper, and SurfinGate sample configuration: If you are installing IBM Firewall, MIMEsweeper, and SurfinGate, you can use the setup 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

Information about installing MIMEsweeper is provided in the online document, *MIMEsweeper Administrator's Guide Version 3.2*. Chapter 2 contains information about MAILsweeper deployment and installation, while chapter 3 contains information about WEBsweeper deployment and installation.

Additional considerations

The following information describes additional installation and configuration considerations, as well as sample configurations, for MIMEsweeper.

MAILsweeper and IBM Firewall sample configuration: See “IBM Firewall and MAILsweeper sample configuration” on page 38 for information about installing both MAILsweeper and IBM Firewall.

MIMEsweeper, IBM Firewall, and Norton AntiVirus for Internet Email Gateways sample configuration: See “IBM Firewall, Norton AntiVirus for Internet Email Gateways, and MIMEsweeper sample configuration” on page 39 for information about installing MIMEsweeper, IBM Firewall, and Norton AntiVirus for Internet Email Gateways.

WEBsweeper and IBM Firewall sample configuration: See “IBM Firewall and WEBsweeper sample configuration” on page 39 for information about installing WEBsweeper and IBM Firewall.

MIMEsweeper, IBM Firewall, and SurfinGate sample configuration: See “IBM Firewall, MIMEsweeper, and SurfinGate sample configuration” on page 40 for information about installing MIMEsweeper, IBM Firewall, and SurfinGate.

SurfinGate

Instructions for installing SurfinGate are contained in the hardcopy book, *SurfinGate 4.03 for Windows NT Installation Guide*. Chapter 1 contains installation instructions.

Additional considerations

The following information describes additional installation and configuration considerations, as well as sample configurations, for SurfinGate.

SurfinGate, IBM Firewall, and MIMEsweeper sample configuration: See “IBM Firewall, MIMEsweeper, and SurfinGate sample configuration” on page 40 for information about installing SurfinGate, IBM Firewall, and MIMEsweeper.

IBM Firewall and SurfinGate sample configuration: See “IBM Firewall and SurfinGate sample configuration” on page 40 for information about installing SurfinGate and IBM Firewall.

Intrusion Immunity

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

Norton AntiVirus Solution Release 3.0.3

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

Additional considerations

The following information describes additional installation and configuration considerations, as well as a sample configuration, for Norton AntiVirus.

Norton AntiVirus for Internet Email Gateways, IBM Firewall, and MIMEsweeper sample configuration: See “IBM Firewall, Norton AntiVirus for Internet Email Gateways, and MIMEsweeper sample configuration” on page 39 for information about installing Norton AntiVirus for Internet Email Gateways, IBM Firewall, and MIMEsweeper.

Public Key Infrastructure

The following sections describe the installation and configuration documentation for the Public Key Infrastructure component product.

IBM Vault Registry

Information about installing and configuring IBM Vault Registry is provided in the hardcopy book, *IBM Vault Registry Installation and Configuration Guide*.

Toolkit

The following sections describe the installation and configuration documentation for the Toolkit component products.

IBM KeyWorks Toolkit

Information about integrating the IBM KeyWorks Toolkit into applications is contained in the online document, *IBM KeyWorks Toolkit Developer's Guide*.

IBM Key Recovery Service Provider

Installation information for IBM Key Recovery Service Provider is provided in the hardcopy document, *Key Recovery Server Installation and Usage Guide*.

Chapter 4. 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.

For each offering – SecureWay FirstSecure, SecureWay Policy Director, and SecureWay Boundary Server – a Media Pack and a Documentation Pack are available. 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.

Policy Director

The following sections describe the documentation provided with the Policy Director component products.

IntraVerse 2.1.2

IntraVerse 2.1.2 includes the following documentation, which may be hardcopy or online in HTML, PDF, or PostScript format:

IntraVerse 2.1 for Windows NT Release Notes, Version 2.1.2
Hardcopy document that contains planning and installation information.

IntraVerse 2.1 for AIX Release Notes, Version 2.1.2
Hardcopy document that contains planning and installation information.

IntraVerse 2.1 for Solaris Release Notes, Version 2.1.2
Hardcopy document that contains planning and installation information.

IntraVerse 2.1 Administration Guide
Hardcopy document. Also provided online in a subdirectory in the /Documents directory on the IntraVerse CD.

IntraVerse NetSEAT Client Release Notes
Online document. This file can be accessed on the NetSEAT CD from the file \NetSEAT\Docs\index.html.

IntraVerse NetSEAT Client Overview
Online document. This file can be accessed on the NetSEAT CD from the file \NetSEAT\Docs\index.html.

IntraVerse NetSEAT Client Administration Guide
Online document. This file can be accessed on the NetSEAT CD from the file \NetSEAT\Docs\index.html.

IntraVerse NetSEAT Application Development Kit Programmer's Guide
Online document. This file can be accessed on the NetSEAT CD from the file \NetSEAT\Docs\index.html.

IBM Global Sign-On, Version 2.0.200

IBM Global Sign-On includes the following documentation:

IBM Global Sign-On, Version 2.0.200 Up and Running
Provided as a hardcopy book.

Global Sign-On Administration Help
Online client help documentation that is provided as an online book. For instructions for accessing this documentation online, see *IBM Global Sign-On, Version 2.0.200 Up and Running*.

Boundary Server

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

IBM eNetwork Firewall version 3.3

IBM Firewall provides the following documentation:

IBM eNetwork Firewall for AIX Version 3.3 Setup and Installation for Multiple Languages
Hardcopy booklet that contains instructions for installing and setting up the IBM eNetwork Firewall for AIX.

IBM eNetwork Firewall for Windows NT Version 3.3 Setup and Installation for Multiple Languages
Hardcopy booklet that contains instructions for installing and setting up the IBM eNetwork Firewall for Windows NT.

IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide
Contains information about using IBM Firewall for Windows NT. Available in three formats:

- PDF on the CD
- HTML accessible through the IBM Firewall graphical user interface (GUI)
- Hardcopy, separately orderable using order number GC31–8658–02

IBM eNetwork Firewall Version 3.3 for Windows NT Reference
Contains reference material for using IBM Firewall for Windows NT. Available in three formats:

- PDF on the CD
- HTML accessible through the IBM Firewall graphical user interface (GUI)
- Hardcopy, separately orderable using order number SC31–8659–02

ACE/Server, a component of IBM Firewall, provides the following documentation:

Quick Start Guides
Hardcopy booklet that contains instructions for installing and administering ACE/Server on all supported platforms.

README Provided in hardcopy.

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 documentation:

SurfinGate Installation Guide
Hardcopy book that contains information about installing and configuring the SurfinGate 4.03 components on Windows NT.

In addition, a PDF version of the *SurfinGate Installation Guide* is provided on the product CD in the following file: \docs\install.pdf.

SurfinGate User Guide
Hardcopy book that contains 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 4.03 for Windows NT Release Notes
Hardcopy document that provides information about SurfinGate 4.03, including system requirements and product limitations.

A PDF version of the *SurfinGate 4.03 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 an upgrade to SurfinGate to improve the level of protection against a particular type of security threat. This document is provided 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.

Norton AntiVirus Solution Release 3.0.3

Norton AntiVirus Solution Release 3.0.3 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 Solution Release 3.0.3 CD. The contents.txt file is an ASCII file on the product CD.

Contents of the Norton AntiVirus Solution Release 3.0.3 CD
See \contents.txt on the product CD.

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

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

Norton System Center Administrator's Guide
See \docs\admin\nscoem.pdf on the product CD.

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

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

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

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

Norton AntiVirus for Windows 95/98 Reference Guide
See \docs\navwks\nav59ref.pdf on the product CD.

Norton AntiVirus for Windows 95/98 User's Guide
See \docs\navwks\nav59usr.pdf on the product CD.

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

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

Public Key Infrastructure

The following section describes the documentation provided with the Public Key Infrastructure component product.

IBM Vault Registry

IBM Vault Registry includes the following books. All language versions are delivered in PostScript, PDF, and HTML format on the IBM Vault Registry documentation CD. Instructions for accessing the online documents are provided in the product README file in the root directory of the product documentation CD. Additionally, hardcopy is provided for the first two books in the list.

IBM Vault Registry General Information Guide
Introduces the Vault Registry product, describes the system components, and includes scenarios that show how to use vault technology to implement

secure, trusted applications in your enterprise. This book is also provided in hardcopy.

IBM Vault Registry Installation and Configuration Guide
Provides procedures for installing and configuring Vault Registry server components: Vault Controller, Vault Certificate Management System, Vault Registration Application for AIX, and corequisite products. This book is also provided in hardcopy.

IBM Vault Registry System Operations Guide
Provides information about how to monitor and administer a Vault Registry system. Information is included about logging, reporting, and backup and recovery.

IBM Vault Registry Messages and Codes
Lists the messages produced by the Vault Registry product components. The message descriptions explain how to resolve the errors.

IBM Vault Controller for AIX Programming Reference
Provides application developers with a complete reference to the syntax of each Vault Controller application program interface (API) function.

IBM Vault Controller for AIX Programming Guide
Provides application developers with information about how to write vault-based applications by using the API functions documented in the *IBM Vault Controller for AIX Programming Reference*.

IBM Vault Agent User Guide and Reference
Provides procedures for installing, configuring, and developing applications for the Vault Agent client component. Included is a complete reference to the syntax of each API function provided for the Vault Agent.

IBM Vault Certificate Validator User Guide and Reference
Provides procedures for installing and developing applications for the Vault Certificate Validator client component. Included is a complete reference to the syntax of each API function provided for the Vault Certificate Validator.

IBM Vault Registration Application for AIX Customization Guide
Provides application developers with information about how to customize the Vault Registration Application according to the needs and preferences of your organization's e-business goals.

IBM Vault Registry Registration Authority User Guide
Provides registration authority (RA) and Master RA users with information about how to administer certificates and registration requests.

Toolkit

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

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 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 KeyWorks Toolkit Key Recovery Service Provider Interface 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 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 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:

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.

Appendix A. 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.

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
OS/2
RS/6000
SecureWay

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

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

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.

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

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

Index

Part Number: CT7VYNA

Printed in U.S.A.