IBM SecureWay® Boundary Server for Windows NT® and AIX

Up and Running

Version 2.0

SCT6-RZNA-00

IBM SecureWay® Boundary Server for Windows NT® and AIX

Up and Running

Version 2.0

SCT6-RZNA-00

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix B. Notices” on page 37.

This edition applies to Version 2, release 0, modification 0 of IBM SecureWay Boundary Server product (GC31-8733-00) and to all subsequent releases and modifications until otherwise indicated in new editions.

Second Edition (October 1999)

Contents

About this book

This book explains how to plan for, install, configure, use, and troubleshoot IBM SecureWay® Boundary Server for Windows NT® and AIX.

It is important that you have a sound knowledge of firewalls, virtual private networks, content security, and network administration before you install and configure the SecureWay Boundary Server. Because you will set up and configure a firewall that controls the access in and out of your network, you must first understand how the network operates. Especially, you need to understand the basics of IP addresses, fully qualified names, and subnet masks.

Who should read this book

This book is intended for network or system security administrators who install, administer, and use the IBM SecureWay Boundary Sever.

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 (for example, hardware, software, and firmware) used with the products properly exchange accurate date data with them.

Service and support

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

How this book is organized

This book contains the following chapters:

- “Chapter 1. Overview of SecureWay Boundary Server” on page 1 gives an overview of SecureWay Boundary Server and its components.
- “Chapter 2. Introducing IBM’s SecureWay Boundary Server” on page 5 provides information on why you need SecureWay Boundary Server.
- “Chapter 3. Before you install SecureWay Boundary Server” on page 11 provides information on how to plan for SecureWay Boundary Server.
- “Chapter 4. Requirements for IBM SecureWay Boundary Server (SBS)” on page 15 provides information for the minimum requirements for SecureWay Boundary Server.

- "Chapter 5. Installing and Configuring SecureWay Boundary Server" on page 17 describes installation and configuration of SecureWay Boundary Server on Windows NT and AIX operating systems
- "Chapter 6. Related Documentation" on page 31 tells you where to find other documentation for SecureWay Boundary Server and documentation for related products.

Conventions

This book uses the following conventions:

Convention	Meaning
bold	User interface elements such as check boxes, buttons, and commands
monospace	Syntax and directory defaults that are relvant to SecureWay Boundary Server
->	Shows a series of selections from a menu. For example: Select **File-> Run** means click **File**, and then click **Run**

Web information

Information about last-minute updates to SecureWay Boundary Server is available at the following Web address:

http://www.ibm.com/software/security/boundary/library

Information about updates to other IBM SecureWay FirstSecure products is available at the following Web address:

http://www.ibm.com/software/security/firstsecure/library

What is new?

Version 2.0 of SecureWay Boundary Server contains a number of new features. The most significant new features are listed here.

Integration with SecureWay Policy Director

The SecureWay Policy Director can manage Firewall Proxy users, if Firewall is SecureWay Boundary Server enabled. Firewall Proxy users are defined for the following Firewall services:

- Telnet
- FTP

- HTTP
- Socks

Users and their associated policies are stored in a Lightweight Directory Access Protocol (LDAP) database.

The SecureWay Directory provides LDAP to maintain directory information in a central location for storage, updates, retrieval, and exchange. SecureWay Policy Director manages the Firewall proxy users in the LDAP database.

Routing Efficiencies

Routing efficiencies use a Finjan SurfinGate plugin to short circuit network traffic for content filtering.

Intrusion Blocking

Command line programs to create dynamic DENY rules on the Firewall. Intrusion blocking can be integrated into an automated script.

IBM SecureWay Firewall 4.1

The IBM SecureWay Firewall for Windows NT offers:

Remote Access Service

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

IBM SecureWay Firewall Enhancements for AIX 4.1

The IBM SecureWay Firewall for AIX offers:

Enhanced IPSec Support

The IBM SecureWay Firewall 4.1 includes enhanced IPSec support including triple-DES encryption, support for new headers. It also supports interoperability with several IBM servers and routers as well as many non-IBM VPN products that support the new headers.

Symmetric Multi-Processor (SMP)

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

Filters Enhancements

Filters have been enhanced to provide better performance with configuration. You can tune the performance of your Firewall by choosing where to locate different types of filter rules. In addition, the number of times a connection is used is logged.

Setup Wizard

A wizard aids with the initial configuration of the IBM SecureWay Firewall. This setup wizard lets new users have a basic Firewall configuration up and running quickly after installation of the IBM Firewall.

Network Security Auditor

The Network Security Auditor (NSA) checks your network servers and the Firewall for security holes or configuration errors. It has been enhanced to be faster and more robust.

National Language Support for German

National language support for German is now offered in addition to Brazilian, Portuguese, English, French, Italian, Japanese, Korean, simplified Chinese, Spanish, and traditional Chinese.

Network Address Translation

Network address translation (NAT) has been enhanced to support many-to-one address mappings. These mappings are from multiple internal unregistered or private addresses to a registered legal address using port numbers to create the unique mappings.

Common functions supported by AIX and Windows NT

Security Dynamics ACE/Server

Security Dynamics ACE/Server provides two factors of authentication. This feature is enhanced and protects your network and data resources from potentially devastating accidental or malicious intrusion.

Secure Mail Proxy Enhancements

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

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

Socks Protocol Version 5 Enhancements

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

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

HTTP Proxy

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

MIMEsweeper 2.0 for SecureWay

MIMEsweeper has three major components: **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5**, and **WEBsweeper 1.0_2**. Some enhancements are:

MAILsweeper

MAILsweeper 4.1_2 for SMTP is a major upgrade to Content Technologies flagship MIMEsweeper product. It offers the following new features:

- An easy to use, hierarchical policy architecture provides the flexibility to apply policies at the appropriate organizational level-right down to the individual user
- An industry standard graphical user interface (GUI) simplifies software configuration, policy creation and administration
- A new Split Delivery feature is a function of the hierarchical policy implementation of version 4. For messages with multiple recipients, policies are applied to each recipient. Authorized recipients receive the message while unauthorized recipients are denied
- Multi-threaded message processing improves throughput and adds robustness by allowing message processing to continue, using remaining threads, if an error occurs on one or more threads
- In conjunction with other vendor's anti-virus products, MAILsweeper provides virus detection and cleaning of messages and attachments.
- Advanced text analysis using NEAR, AND, NOT, and OR expressions provide tremendous flexibility in creating comprehensive, effective scenarios based on message syntax or architecture
- Enhanced auditing tools that can send data to any ODBC-compliant database
- Support the Real-Time Black List (RBL) server which lists sites that are known to send out junk email. MAILsweeper can refuse to accept connections from any host in this list
- Content security is easier to manage through attractive reports/graphs/charts of email traffic
- Integration with LDAP directories

- Delivery Service Notification (DSN) now supports SNMP and NT Alerter

WEBsweeper

- Additional performance enhancements improve data processing speed.
- Works with Virus Scanners for HTTP and FTP traffic

WEBsweeper HTTPS

- WEBsweeper now provides full support for the web based e-commerce applications through a new HTTPS proxy solution

SurfinGate 4.05

SurfinGate enhancements include:

JavaScript Content Inspection

SurfinGate 4.05 looks for potentially problematic JavaScript operations and stops JavaScripts that conflict with corporate security policy. SurfinGate 4.05 allows administrators to centrally set and enforce a policy for JavaScript, Java, and ActiveX, with smart filtering for VisualBasic Script and cookies.

Mission Critical Performance Monitoring

SurfinGate 4.05 includes an automatic tool that detects abnormal behavior (such as runtime errors) and re-starts SurfinGate in case of failure. This is an essential security feature for mission critical areas.

Increased Policy Management

SurfinGate enters unresolved applet profiles into the database for automatic blocking. Administrators can edit the list of applets/controls.

Support for FTP and SSL Protocol

SurfinGate 4.05 monitors File Transfer Protocol (FTP) channels for mobile code, keeping watch on code that could otherwise sneak in unnoticed from the Internet. In addition to FTP, SurfinGate monitors HTTP traffic for mobile code and passes HTTPS traffic to additional devices.

Plugin integration with firewall HTTP proxy

SurfinGate will work as a proxy in a proxy chain or through a plugin in Web Traffic Express on the Firewall for Windows NT.

Chapter 1. Overview of SecureWay Boundary Server

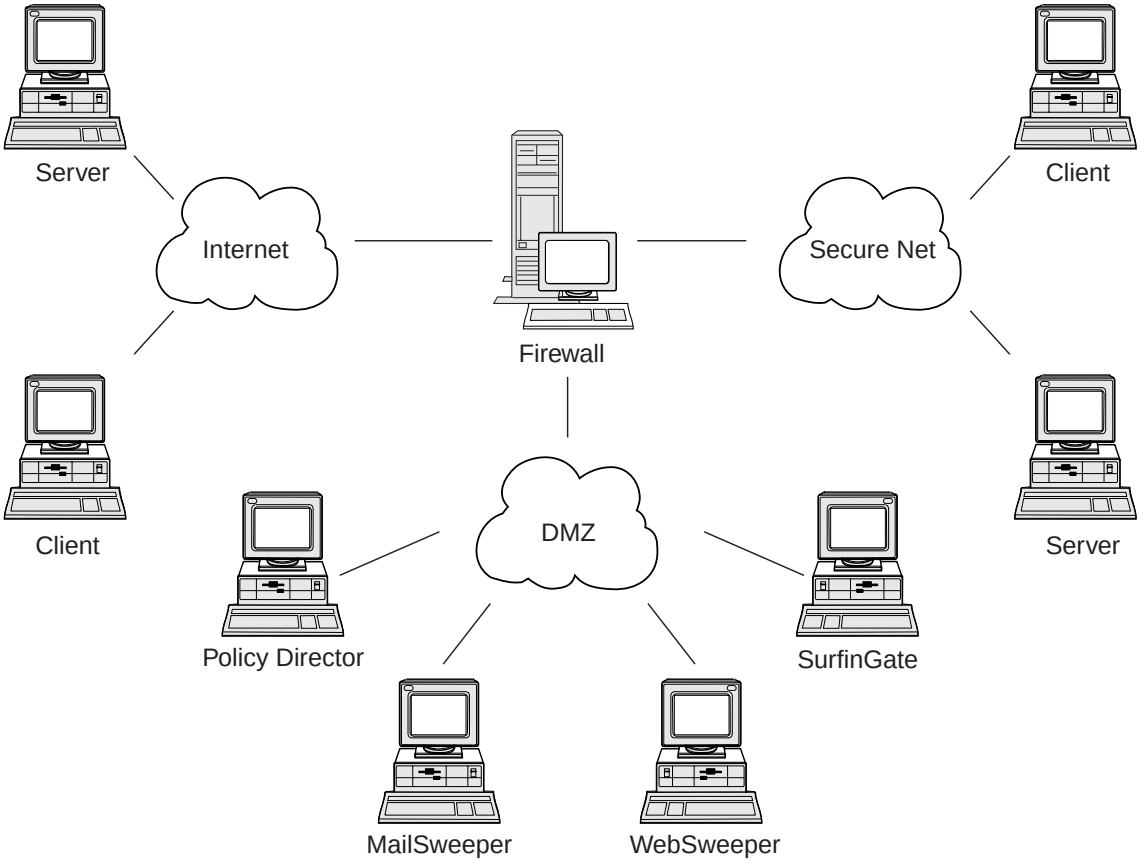


Figure 1. An example of an IBM SecureWay Boundary Server configuration

This example diagrams five workstations using MAILsweeper, WEBsweeper, Policy Director, and SurfinGate components to monitor and route web traffic and mail between clients and servers using a Firewall. For this example, we will use five physically separate workstations.

Typical SecureWay Boundary Server Examples

We recommend you use the following machines for a minimum setup:

Table 1. Hardware requirements for Boundary Server component products

Product	**Machine**
IBM Firewall	Windows NT or AIX

Table 1. Hardware requirements for Boundary Server component products (continued)

MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

If you want to take full advantage of SecureWay Boundary Server, SecureWay Policy Director must be in your network. This allows Firewall proxy users to be stored in SecureWay Directory (LDAP).

HTTP Example (Windows NT Firewall): In a typical scenario, an HTTP request for content on the Internet would originate at the client machine. The request would flow first to the to WEBsweeper. On the outbound path, the request would simply be proxied by WEBsweeper to the Firewall HTTP proxy.

At the Firewall HTTP proxy, the user would be authenticated. If this is the first request from the client browsing session, a User ID/Password challenge would be presented. The User ID would be used to look up the client's security policy in the LDAP database administered by the Policy Director. Depending on the HTTP authentication policy for the client, and the result of checking the password entered, the request may be denied, or permitted to proceed. The authentication operation may require further accesses to the LDAP database, or to the Security Dynamics ACE server. On subsequent requests from the same browsing session, the browser will provide the User ID/Password automatically. The client will not be challenged, but each request will still be authenticated through the same process as the first request.

If the authentication is successful, the request will be proxied to the requested server on the Internet.

When the content from the Internet server is received back at the Firewall HTTP proxy, it will be examined by the SurfinGate plugin. Group information for the user, obtained from the LDAP database, will be made available to the plugin to base policy decisions on. If the content contains nothing of interest to SurfinGate, it will pass quickly through the plugin, with minimal processing overhead. Content containing JavaScript will be filtered in the plugin. Content containing Java or ActiveX will be forwarded to the SurfinGate server for filtering, and the filtered content will be returned to the Firewall HTTP proxy. The content resulting from the processing of the SurfinGate plugin will be sent back to the WEBsweeper server.

When the content arrives back at the WEBsweeper server, it will be filtered according to WEBsweeper policies, then returned back to the client.

HTTP Example (AIX Firewall): On AIX the flow of traffic is essentially identical, except that there is no SurfinGate plugin available for the AIX Firewall. Therefore the SurfinGate server must be set up as a proxy in a proxy chain from the client to the Firewall. WEBsweeper should be set up to forward requests to the SurfinGate server rather than directly to the Firewall HTTP proxy. The SurfinGate server must then be configured to forward requests to the Firewall HTTP proxy. No group information will be available at the SurfinGate server, so policy decisions can be based only on IP address.

Mail Example: MAILsweeper is set up as a mail gateway. Mail that arrives at the MAILsweeper server has its content filtered before it is forwarded to the next mail server.

Each of your secure mail servers must be configured to forward client mail requests to the MAILsweeper server. The Firewall mail exchanger must be configured to forward incoming mail to the MAILsweeper server.

MAILsweeper must be configured to send the mail addressed to any external domains to the Firewall mail exchanger. MAILsweeper must be configured to send the mail addressed to internal domains to the correct secure mail server.

Chapter 2. Introducing IBM's SecureWay Boundary Server

This chapter gives an overview of SecureWay Boundary Server and includes the following sections:

What is SecureWay Boundary Server?

IBM SecureWay Boundary Server brings together, for the first time, a complete boundary security solution. SecureWay Boundary Server provides firewall protection, virtual private networking (VPN), and content security. SecureWay Boundary Server brings together technology from the security industry into an integrated solution with IBM support and services standing behind it. This solution includes:

- IBM SecureWay Firewall 4.1 (includes Security Dynamic ACE/Server)
- MIMEsweeper from Content Technologies
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS proxy 1.0_2
- SurfinGate 4.05 from Finjan
  - SurfinGate Server
  - SurfinConsole
  - SurfinGate database
  - SurfinGate Plugin for WTE integration for Windows NT 1.0

Why Do I Need SecureWay Boundary Server?

Secure boundaries are needed everywhere– between departments, such as engineering and human resources, headquarters network and remote offices, your company's network and the Internet, your company's Web applications and customers, your company's network or applications and business partners. Boundary security not only protects your network, applications and information, but also extends their reach. Proper boundary security requires controlling both who can access your network and what information is entering or leaving your network.

How Does SecureWay Boundary Server Fit Into FirstSecure?

IBM SecureWay FirstSecure is a package of integrated products. It provides a comprehensive framework to help you secure all aspects of networking over the Internet and other networks. It helps you to build on your current investments with modular, interoperable offerings and to minimize the total cost of ownership for doing secure e-business. It provides virus protection, access control, traffic content control, encryption, digital certificates, firewall, toolkits and implementation services.

Boundary Server is a package of products that fits within FirstSecure. It creates a boundary to the Internet that you can use to block potentially harmful viruses (using adjunct virus scanning products), JavaScript, Java applets, ActiveX controls, and even junk email (SPAM). With Boundary Server, you control exactly what you want to enter your network from the Internet. With SecureWay Policy Director, you manage Firewall proxy users and their authentication policies.

What Are the Components of SecureWay Boundary Server?

The three components of SecureWay Boundary Server consist of IBM Firewall, MIMEsweeper, and SurfinGate. SecureWay Boundary Server provides integration with IBM SecureWay Policy Director.

Overview of IBM SecureWay Boundary Server

IBM SecureWay Boundary Server provides large organizations the protection, access control, and content security needed to exploit e-business by safely opening their enterprise to customers, suppliers, and partners. The features include:

- Firewall protection for your network
- Virtual Private Networking (VPN) to extend your network's reach
- Content scanner for email and web traffic to protect your company's data, image, and liability and productivity

The SecureWay Boundary Server brings together the best-of-breed technology from the industry into an integrated solution with IBM support and services standing behind it. It is available for AIX and Windows NT operating systems.

Function of SecureWay Boundary Server

The SecureWay Boundary Server applies packet filtering, proxies, and Socks server technology and content security to hide and protect your network and systems. These technologies enable administrators to explicitly define what data is allowed to pass into and out of your network. This helps prevent ″denial of service attacks″ and hackers attempts to penetrate the network and limits legal liabilities. The SecureWay Boundary Server offers a VPN solution to enable you to replace remote servers and modem banks with an Internet based solution.

When deployed with the Policy Director, the SecureWay Boundary Server offers authentication of users using a central policy–based scheme. Anti–Virus software can be used with SecureWay Boundary Server to provide virus protection for your site.

Overview of IBM SecureWay Policy Director

Policy Director is a stand-alone authorization and security management solution that provides end-to-end security of resources over geographically dispersed intranets and extranets. An extranet is a virtual private network (VPN) that uses access control and security features to restrict the use of one or more Intranets attached to the Internet to selected subscribers. Policy Director provides authentication, authorization, data security, and resource management services. You use Policy Director in conjunction with standard Internet-based applications to build secure and well-managed intranets and extranets.

Function of IBM SecureWay Policy Director

When used with SecureWay Boundary Server, IBM SecureWay Policy Director provides storage of proxy user policies and authentication information.

Overview of IBM SecureWay Firewall

The IBM SecureWay Firewall is a network security program. A firewall is a blockade between one or more secure, internal private networks and other networks or the Internet. A firewall prevents unwanted or unauthorized communication into or out of the secure network.

Function of IBM SecureWay Firewall

The IBM SecureWay Firewall restricts access between a protected network, Internet, and other sets of networks. It also does the following:

- Restricts people to entering at a carefully controlled point
- Prevents attackers from getting close to other defenses
- Restricts people to leaving at a carefully controlled point
- Internal firewalls segregate sensitive internal information from unauthorized employees
- Restricts what traffic can go in and out of the network

Overview of MIMEsweeper

MIMEsweeper provides Content Security, by analyzing the data passing through the Firewall via electronic mail or the world wide web. Content Security allows organizations to effectively manage business issues related to the use of email and the world wide web. These issues can be divided into network integrity and business integrity.

Filtering for network integrity can:

- Identify and remove viruses in incoming and outgoing email

- Filter undesirable file types
- Manage oversize files
- Protect networks from congestion or loss of service from mail-bomb attacks

Filtering for business integrity can:

- Prevent confidentiality breaches and loss of trade secrets
- Limit exposure to legal liability
- Reduce loss from employee misuse of email and world wide web services
- Protect from loss of network service through misuse and hostile attacks

Threats to network integrity can corrupt or erase data, disrupt email flow and ruin system hardware, all of which can result in network downtime, lost productivity and high cleanup and recovery costs.

Threats to business integrity, however, can be far more destructive, resulting in enormous legal costs, lost intellectual property, and damaged corporate reputation and credibility. Business integrity issues can bring your commercial operations to a standstill.

MIMEsweeper is the industry leading product for protecting organizations from the network and business integrity issues posed by organizational usage of email and the Internet.

Function of MIMEsweeper

MIMEsweeper can:

- Add legal disclaimers to outbound mail
- Protect confidential documents and data
- Authorize and control email and web based users
- Quarantine or block offensive material
- Block junk email
- Scan attachments and downloads for appropriate content
- Stop viruses and malicious code
- Block inappropriate web pages and sites
- Report, log, and archive

Overview of SurfinGate

SurfinGate 4.05 is a mobile code security tool for any business using the Internet, extranet, or intranet for business transactions. Through content inspection of mobile code, including JavaScript, SurfinGate helps protect computer networks from hostile or unintentional damage including industrial espionage, data modification, and information deletion. SurfinGate's content inspection process inspects Java, JavaScript, and ActiveX mobile code content at the gateway level, away from critical resources, and

assigns an unique ID and applet security profile (ASP) to code, noting any possible security breaches. SurfinGate identifies potentially problematic code before it can enter the network.

SurfinGate 4.05 includes four components:

- SurfinGate Server
- SurfinConsole
- SurfinGate database
- SurfinGate Plugin for WTE integration for Windows NT

SurfinGate Server acts as an HTTP proxy server. SurfinGate can be positioned as part of a proxy chain along with the Firewall HTTP proxy and the WEBsweeper proxy. For Windows NT, it can alternatively be used as a plugin for the Firewall HTTP proxy. When used as a plugin, SurfinGate will get group information for the proxy user making the request. SurfinGate filtering policies can be based on this group information. This architecture allows mobile code traffic to be stopped and inspected before attacks happen. This component provides protection as per the corporate security policy.

SurfinConsole is a user-friendly interface for managing and setting 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 organization per user, per group, or through custom lists or unacceptable and acceptable code.

The SurfinGate database stores details of applet security profiles (ASP), including information regarding users and groups and their corresponding security policies. The database can use a built-in access database engine or an existing Oracle database. Because SurfinGate inspects content of all mobile code on the fly, the database is not required for security, but does help improve performance in large-scale operations.

Function of SurfinGate

SurfinGate provides:

- Gateway level content inspection server for Java applets, Active X controls, JavaScript
- Realtime monitoring, dynamic inspection
- Enforcement of security policy for web based mobile code
- Inspection of ″mobile code″ (for example, Java applets, ActiveX controls, JavaScript, Visual Basic scripts, plug-ins, cookies)

SurfinGate can work with a proxy in a proxy chain or through a WTE plugin on the Firewall for Windows NT.

Chapter 3. Before you install SecureWay Boundary Server

This chapter shows you how to get ready to install SecureWay Boundary Server using the wizard and includes the following sections:

How Do You Prepare?

This section will show you how to prepare the components for SecureWay Boundary Server.

Integration with SecureWay Policy Director

For a basic IBM SecureWay Policy Director setup on Windows NT or AIX , do the following:

1. Verify that your operating system is properly configured to support Policy Director.
2. Determine which server components best fit your deployment requirements and on which machines to install these components.
3. Install and configure a DCE infrastructure if one does not exist.
4. Install and configure the SecureWay Directory (LDAP).
5. Configure the Certificate Authorization Service (CAS) if you will be doing client certificate authentication.
6. Install the NetSEAT client.
7. Install the Policy Director server components.
8. Install the Management Console.

For more information on Policy Director, refer to *Policy Director Up and Running 3.0*.

SecureWay Firewall

For a basic IBM Firewall setup on Windows NT or AIX, do the following:

1. Ensure you have the prerequisites, listed in "Hardware Requirements for SecureWay Boundary Server" on page 15.
2. Plan for your IBM Firewall setup. Decide in advance which functions of the firewall you want to use and how you want to use them.
3. Tell the Firewall which of its interfaces are connected to secure networks. You must have a secure interface and a nonsecure interface for your firewall to work properly. From the configuration client navigation tree, open the System Administration folder and click **Interfaces** to see a list of the network interfaces on your firewall. To change the security status of an interface, select an interface and click **Change**.

Note: If you are going to connect to the Internet, contact your Internet Service Provider (ISP) to obtain a registered IP address for the Firewall nonsecure interface.

4. Set up your general security policy by accessing the **Security Policy** dialog in the System Administration folder. For typical Firewall configurations:
   - Permit DNS queries
   - Deny broadcast message to nonsecure interface
   - Deny Socks to nonsecure adapters
5. Set up your domain name service and mail service. Efficient communication will not take place if you do not provide DNS resolution. Access these functions from the System Administration folder on the configuration client navigation tree.
6. Define key elements of your network(s) to the firewall using the **Network Objects** function in the configuration client navigation tree. Network Objects control traffic through the Firewall. Define the following key elements as network objects:
   - Secure Interface of the Firewall
   - Nonsecure Interface of the Firewall
   - Secure Network
   - Each subnet on your secure network
   - A host network object for your Security Dynamics servers and your Windows NT domain servers, if appropriate
7. Enable services on the Firewall. These are the methods (such as socks or proxy) by which users in the secure network can access the nonsecure network. Which services get implemented depends on decisions you made at the planning stage. Implementing a service often requires setting up some connection configurations to allow certain types of traffic. For example, if you want to allow your secure users to surf the Web on the Internet by using HTTP Proxy, you not only need to configure the HTTP Proxy daemon on the Firewall, but you also need to set up connections to allow HTTP traffic. If you going to set up Policy Director, see the section “Integration with SecureWay Policy Director” on page 11.
8. **Windows NT only:** Because the hardening process disables NETBIOS, if you want to use Windows NT domain passwords for authentication, you must configure the Windows client code that implements the ability to search trusted Windows NT domains for authentication purposes. The trusted Windows NT servers must have TCP/IP host names and addresses and have TCP/IP connectivity between them and the Firewall. The firewall administrator needs to create connections between the Firewall and the trusted Windows NT servers in order to permit traffic to flow between the two.
9. If you will be using network address translation, first contact your ISP to obtain a registered Internet address for use with many-to-one address translation. This address is in addition to the address you requested in step 3 on page 11. Then, go to the *Add NAT Configuration* panel to add the registered Internet address in the *Many-to-One IP Address* field.

Following these steps should help you to get a basic firewall configuration up and running. The IBM Firewall provides other functions, such as system logs to help you ensure the security of your network.

If the Firewall shuts down either normally or abnormally, your configuration data is not affected because it is saved to the hard drive and is automatically reactivated upon rebooting. However, certain firewall log messages will occur indicating that some active connections were interrupted, for example, an active FTP session.

SecureWay Boundary Server

You can use the SecureWay Boundary Server wizard to setup up Firewall to use IBM SecureWay Policy Director for user administration to integrate with Policy Director. Optionally, this wizard configures the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin (Windows NT only).

The information that you will need to configure IBM SecureWay Boundary Server for Firewall is:

- The host name and domain of the IBM SecureWay Directory server that the Firewall will use.
- The number of the port on which the IBM SecureWay Directory server is listening. The default port is 389.
- The SecurityMaster password for the IBM SecureWay Directory server.
- The domain name to use to distinguish the proxy users for this Firewall. Any firewalls using this name will administer the same set of users. Normally you would use the fully qualified hostname of the Firewall machine.
- The Firewall administrator name used to access the proxy users stored in the SecureWay Directory. This name will be granted access to modify all proxy users created in SecureWay Policy Director. You should use the fully qualified host name of the Firewall machine.
- The Distinguished Name that the IBM SecureWay Directory uses as a root from which to start searching for Firewall users in the database. This should be the suffix you created in SecureWay Directory to store Policy Director users.
- A password for administrator ID of the Firewall to use when connecting to IBM SecureWay Directory server.

You will need to create a connection to allow traffic to flow between the Firewall and the SecureWay Directory server.

Ensure you have the prerequisites, listed in “Hardware Requirements for SecureWay Boundary Server” on page 15.

SurfinGate

To prepare to use SurfinGate, you must have Windows NT Service Pack 5 installed. Ensure you have the prerequisites, listed in “Hardware Requirements for SecureWay Boundary Server” on page 15.

Perform the following to prepare to use SurfinGate:

- If you are using Oracle database, it must be configured.

- If you are using Windows NT Firewall, you need to decide whether to use plugin or proxy mode.
- To enable SurfinGate plugin on WTE, install the SurfinGate plugin on the Firewall machine and run the SecureWay Boundary Server wizard.
- You need to create a connection to allow traffic to flow from the SurfinGate plugin to the SurfinGate server.
- If you are using the SurfinGate plugin, you need to create a connection on the Firewall to allow HTTP traffic to flow from the SurfinGate server directly to the Internet.

MIMEsweeper

To prepare to use MIMEsweeper, you need to understand how your network is going to work. Ensure you have the prerequisites, listed in "Hardware Requirements for SecureWay Boundary Server" on page 15.

MAILsweeper

If you configure MIMEsweeper, MAILsweeper and WEBsweeper need to be on separate machines.

Perform the following tasks before configuring MAILsweeper:

- Determine the mail domains that you use internally. MAILsweeper and the Firewall mail exchanger must be configured to accept mail for each of these mail domains.
- Determine which secure mail servers support each of your domains. MAILsweeper must be configured to forward mail addressed to any of your mail domains to the correct secure mail server.
- Determine the address of the MAILsweeper server. Each of your secure mail servers must be configured to forward the mail received from internal clients to the MAILsweeper server.
- Determine the address of the Firewall. MAILsweeper must be configured to forward mail addressed to external domains to the Firewall mail exchanger.

WEBsweeper

Perform the following tasks before configuring WEBsweeper:

- Determine the address of the WEBsweeper server. This will be needed by each of the client web browsers in your network. The browsers must be configured to use the WEBsweeper server as their proxies for HTTP, FTP and HTTPS.
- Determine the address of the secure interface of your Firewall. WEBsweeper must be configured to forward proxy requests to the HTTP proxy residing on the Firewall.
- If you do not want clients to be able to bypass web content filtering, you will need to set up a connection on the Firewall to limit proxy access to your WEBsweeper and/or SurfinGate servers.

Chapter 4. Requirements for IBM SecureWay Boundary Server (SBS)

This chapter gives you the minimum requirements for SecureWay Boundary Server.

Hardware Requirements for SecureWay 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
Policy Director	N/A	64 MB	16 MB	N/A
IBM Firewall	• Windows NT: 266 MHz or higher • AIX: RS/6000 machine that supports 4.3.2	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	2 network interface cards (NIC)
ACE/Server	• Windows NT: 166 MHz 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: 240 MB	Minimum: 32 MB	Actual storage requirements are based on user population
MAILsweeper	Windows NT: 400 MHz processor or higher	1 GB	128 MB	N/A
WEBsweeper	Windows NT: 450 MHz processor or higher	1 GB	128 MB	N/A
WEBsweeper system requirements for High Volume Environment	Windows NT: 450 MHz processor or higher	3 GB	512 MB	N/A
SurfinGate 4.05 Server	Windows NT: 233 MHz processor or higher	20 MB	256 MB	N/A
SurfinGate 4.05 Console	Windows NT: 233 MHz processor or higher	15 MB	64 MB	N/A

Note: See IBM SecureWay Firewall for AIX or Windows NT Version Setup and Installation for Multiple Languages for more details. 138 MB of Disk Space is also required for the Netscape Browser.

Software Requirements for SecureWay Boundary Server

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

Table 3. Minimum Software requirements for Boundary Server component products

Product	Windows	AIX	Other
Policy Director servers	Windows NT version 4.0 with Service Pack 5	4.3.1	N/A
IBM Firewall	Windows NT version 4.0 with Service Pack 5	4.3.2	N/A
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	N/A
MAILsweeper	Windows NT version 4.0 with Service Pack 5; Internet Explorer 4.01 or higher; Microsoft Management Console 1.1; NTFS drive; Windows Messaging	N/A	Anti-Virus tools that you wish to use
WEBsweeper	Windows NT version 4.0 with Service Pack 5	N/A	Anti-Virus tools that you wish to use
SurfinGate Server	Windows NT 4.0 version with Service Pack 5	N/A	N/A
SurfinGate 4.05 Console	Windows NT version 4.0 with Service Pack 5 or Windows 95	N/A	N/A

Chapter 5. Installing and Configuring SecureWay Boundary Server

This chapter tells you how to configure and install SecureWay Boundary Server on Windows NT and AIX.

Installing SecureWay Boundary Server components

This section helps you install IBM SecureWay Firewall, SurfinGate, and MIMEsweeper for Windows NT and AIX.

Installing SecureWay Firewall

For more information about a basic configuration for the IBM SecureWay Firewall for Windows NT and AIX, see "How Do You Prepare?" on page 11. It explains how to define a secure interface, how to determine your security policy, and how to define network objects. For more information on installing SecureWay Firewall, see *IBM SecureWay Firewall Installation Guide for AIX* and *IBM SecureWay Firewall Installation Guide for Windows NT*.

Installing SecureWay Directory

If you are using the LDAP feature of SecureWay Boundary Server, you must install SecureWay Directory, see *IBM SecureWay Policy Director Up and Running 3.0*.

The SecureWay Directory server must be located on the secure side of your Firewall, or within the Firewall secure Demilitarized Zone (DMZ).

Installing SecureWay Policy Director

If you are using the LDAP feature of SecureWay Boundary Server, you must install SecureWay Policy Director (see *IBM SecureWay Policy Director Up and Running 3.0*).

Installing SecureWay Boundary Server

To install SecureWay Boundary Server on Windows NT, do the following:

- Install SecureWay Firewall for Windows NT
- From SecureWay Boundary Server CD, run setup.exe
- Choose your language and click **OK**
- InstallShield will ask where you want to install SecureWay Boundary Server. The Windows NT default directory is C:\Program Files\IBM\SBS
- Reboot

To install SecureWay Boundary Server on AIX, do the following:

- Install SecureWay Firewall for AIX
- Put CD in and install using SMITTY
- Select Software Installation and Maintenance
- Select Install and Update Software
- Select Install and Update from Latest Available Software
- When asked for the INPUT device, list the selections and choose the CD-ROM Drive
- List the selections for SOFTWARE to install, and choose sbs.
- Press **Enter** to install the software
- Reboot

Installing SurfinGate

SurfinGate has two components: SurfinGate Server and SurfinGate Console. To install either component of SurfinGate, see the Installation guide located in `\docs\install.pdf` on the SurfinGate CD.

SurfinGate plugin

To install the SurfinGate plugin on the IBM SecureWay Firewall For Windows NT, see the Installation guide located in `\docs` directory on the SurfinGate CD.

Installing MIMEsweeper

MIMEsweeper has three components: MAILsweeper, WEBsweeper, and WEBsweeper HTTPS.

: MAILsweeper 4.1 is required to be installed on an NTFS partition.

Installing MAILsweeper

To install MAILsweeper, see the *Getting Started Guide* located in `\install\MSW4_0_2\docs\qsg.pdf` on the MIMEsweeper CD.

Do **NOT** install the MAILsweeper on the same machine as the WEBsweeper HTTP proxy.

Do **NOT** install the MAILsweeper on the same machine as the WEBsweeper HTTPS proxy.

If you install `MAPI32.dll` from the Windows NT CD and then install Microsoft Management Console 1.1 from the MIMEsweeper CD, the correct version of `MAPI32.dll` is overwritten with a back level version installed with Microsoft Management Console. After installing the Microsoft Management Console, make sure you install `MAPI32.dll`version 4.0 or later. The `dll` is normally found in the Windows Messaging component.

Installing WEBsweeper

To install WEBsweeper, see the *Administrator's Guide* located in `\install\WSW3_2_5\docs\manual.pdf` on the MIMEsweeper CD.

: Do **NOT** install the WEBsweeper on the same machine as MAILsweeper.

Installing WEBsweeper HTTPS

To install WEBsweeper HTTPS, see the *Readme* located in `\install\WSWHTTPS1_0_2\readme.txt` on the MIMEsweeper CD.

Do **NOT** install the WEBsweeper HTTPS proxy on the same machine as MAILsweeper.

Configuring the SecureWay Boundary Server Components

Configuring SecureWay Firewall

For a basic IBM Firewall setup:

1. Plan for your IBM Firewall setup. Decide in advance which functions of the Firewall you want to use and how you want to use them.
2. Tell the Firewall which of its interfaces are connected to secure networks. You must have a secure interface and a nonsecure interface for your firewall to work properly. From the configuration client navigation tree, open the System Administration folder and click **Interfaces** to see a list of the network interfaces on your firewall. To change the security status of an interface, select an interface and click **Change**.
3. Set up your general security policy by accessing the **Security Policy** dialog in the System Administration folder. For typical Firewall configurations:
   - Permit DNS queries
   - Deny broadcast message to nonsecure interface
   - Deny Socks to nonsecure adapters
4. Set up your domain name service and mail service. Efficient communication will not take place if you do not provide DNS resolution. Access these functions from the System Administration folder on the configuration client navigation tree.
5. Define key elements of your network to the Firewall using the **Network Objects** function in the configuration client navigation tree. Network Objects control traffic through the Firewall. Define the following key elements as network objects:
   - Secure Interface of the Firewall
   - Nonsecure Interface of the Firewall
   - Secure Network
   - Each subnet on your secure network
   - A host network object for your Security Dynamics servers and your Windows NT domain servers, if appropriate
6. Enable services on the Firewall. These are the methods by which users in the secure network can access the nonsecure network (such as socks or proxy). Which services get implemented depend on decisions you made at the planning stage.

Implementing a service often requires setting up some connection configurations to allow certain types of traffic. For example, if you want to allow your secure users to surf the web on the Internet by using HTTP Proxy, not only do you need to configure the HTTP Proxy daemon on the Firewall, but you also need to set up connections to allow HTTP traffic.

7. Set up Firewall users. If you require authentication for functions like outbound Web access or for Firewall administrators, you need to define these users to the Firewall. If you will using SecureWay Policy Director to store proxy users in LDAP, do not create proxy users at this time. Use the Policy Director console to create Firewall proxy users during Policy Director configuration.

These steps should help you to get a basic Firewall configuration up and running. The IBM Firewall provides other functions, such as system logs to help you ensure the security of your network.

If the Firewall shuts down either normally or abnormally, your configuration data is not be affected because it is saved to the hard drive and will automatically be reactivated upon rebooting. However, certain firewall log messages might occur indicating that some active connections were interrupted, for example, an active FTP session.

Configuring SecureWay Firewall for Policy Director Integration

The Firewall must be configured to use IBM SecureWay Policy Director with the SecureWay Boundary Server Wizard in order to take advantage of integration with Policy Director. If IBM SecureWay Policy Director is not used, proxy users are defined by the Firewall Graphical User Interface (GUI) only. Such users cannot be managed by the SecureWay Policy Director.

A connection will have to be created to allow the SecureWay Firewall to talk to the SecureWay Directory. The SecureWay Directory has to be on the secure side of the Firewall, either a secure DMZ or secure network.

For more information about how to setup connections, see the *IBM SecureWay Firewall User's Guide for Windows NT* and *IBM SecureWay Firewall User's Guide for AIX*. Information to setup the connection will follow.

For the request these are the items you will need to setup the outbound rule:

- The source will be the secure adapter address of the Firewall.
- The destination will be the SecureWay Directory address.
- The source port will be greater than 1023
- The destination port will be equal to 389.
- The interface will be secure.
- The routing will be local.
- The direction will be outbound.

For the reply these are the items you will need to setup the inbound rule:

- The source will be the SecureWay Directory address.

- The destination will be the secure adapter address of the Firewall.
- The source port will equal to 389
- The destination port will be greater than 1023
- The interface will be secure.
- The routing will be local.
- The direction will be inbound.

An example of the connection is shown below:

```
# Service : ldap
# Description :

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

Run the SecureWay Boundary Server setup wizard. Select option to enable firewall to work with Policy Director. For more information, see “Configuring SecureWay Boundary Server for Policy Director Integration” on page 23.

Configuring SecureWay Firewall to Use the SurfinGate Plugin (Windows NT only)

A connection will have to be created to allow the SecureWay Firewall to talk to the SurfinGate server. The SurfinGate server should be on the secure side of your Firewall.

For more information on how to setup connections, see the *IBM SecureWay Firewall User's Guide for Windows NT*. Information to setup the connection will follow.

For the request these are the items you will need to setup the outbound rule:

- The source will be the secure adapter address of the Firewall.
- The destination will be the address of the SurfinGate server.
- The source port will be greater than 1023.
- The destination port will be equal to 3141.
- The interface will be secure.
- The routing will be local.
- The direction will be outbound.

For the request these are the items you will need to setup the inbound rule:

- The source will be the address of the SurfinGate server.
- The destination will be the secure adapter address of the Firewall.
- The source port will be equal to 3141.

- The destination port will be greater than 1023.
- The interface will be secure.
- The routing will be local.
- The direction will be inbound.

An example of such a connection is shown below:

```
# Service : SurfinGate Plugin Communication
# Description:

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y

Note: The connections should be on the same line.
```

A connection will also have to be created to allow the SurfinGate server to access HTTP servers on the Internet. To set up the connection you will need the following information:

- The source will be the SurfinGate server
- The destination will be ″The World″
- The service will be the ″HTTP direct out″ predefined service

You will also need to configure the SurfinGate server to allow the data that will be scanned. In SurfinConsole, (the administration interface of SurfinGate) you need to check the **Plugin Mode** option under the General tab.

Configuring SecureWay Firewall to Use MAILsweeper

The Mail Exchanger defined in the SecureWay Firewall needs to point to the MAILsweeper machine instead of the actual secure mailserver. MAILsweeper itself will deliver mail to the secure mailservers.

Configuring SecureWay Policy Director

Ensure that SecureWay Directory has been installed. You must know the address of the machine where SecureWay Directory is installed, the port it is listening on, the administrator ID on the SecureWay Directory server, and the administrator password.

Install the SecureWay Directory LDAP client on the same machine as SecureWay Policy Director. (The client may already be installed, if you are using the same machine for your SecureWay Directory, and your SecureWay Policy Director.)

You must modify the LDAP schema of the SecureWay Directory to support Policy Director eProxyUsers. The schema additions are stored in two files provided by Policy Director. You will need the files `secschema.def` and `puschema.def` located in the `/schema` directory of the Policy Director CD.

To modify the LDAP schema on the SecureWay Directory server, run the following commands on the Policy Director machine:

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secscher

ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschema.
```

Where:

- <LDAPHOST> is the SecureWay Directory server name
- <LDAPPORT> is the port the server is listening on
- <LDAPADMINUSER> is the administrator id
- <LDAPADMINPWD> is the administrator password

Once you have modified the LDAP schema to support proxy users, you must enable proxy user manipulation for the Policy Director Console. To do this you must uncomment the Proxyusers TaskView line in the `console.properties` file located in `\Program Files\IBM\IVConsole` directory.

Configuring SecureWay Directory

You must define a suffix to the SecureWay Directory which will be used as the root where Policy Director users are stored. To add a suffix to LDAP, see the *IBM SecureWay Directory Administrator's Guide*. For example, a typical suffix might be:

```
o=yourcompany,c=yourcountry
```

Once you have added the suffix for storing Policy Director users, you must set its Access Control List (ACL) correctly. You must provide all access rights to the new suffix for the Policy Director security group. The Distinguished Name (DN) for the Policy Director security group is:

```
cn=securitygroup,secauthority=default
```

Configuring SecureWay Boundary Server for Policy Director Integration

You can configure the SecureWay Boundary server using the wizard. This wizard guides you through the steps required to set up Firewall to work with other products in Boundary Server and Policy Director. The panels that follow ask you questions about your LDAP server. When you have filled in all the necessary information, the wizard will set up Firewall to use the same LDAP database that Policy Director is using for user and group policy. This wizard can also configure or unconfigure the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin (Windows NT Firewall only).

To configure the IBM SecureWay Boundary Server, run the SecureWay Boundary Server wizard. On AIX run the command **sbswizard**, on Windows NT, select **Start->Programs->SecureWay Boundary Server**. This will bring up the SBS wizard.

1. Select the option to **Set up Firewall to share an LDAP database with Policy Director**".

2. Answer the questions presented using the information in “SecureWay Boundary Server” on page 13.

Configuring SecureWay Boundary Server to Enable the SurfinGate Plugin (Windows NT only)

Select **Start->Programs->SecureWay Boundary Server**. This will bring up the SBS wizard.

1. Select the option to **Configure the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin**.
2. Complete the dialog.

Configuring SurfinGate

On Windows NT, there are two ways to configure SurfinGate:

- As a chained proxy
- As a plugin for the Firewall HTTP proxy

On AIX, there is one way to configure SurfinGate:

- As a chained proxy

Configuring SurfinGate as a Chained Proxy

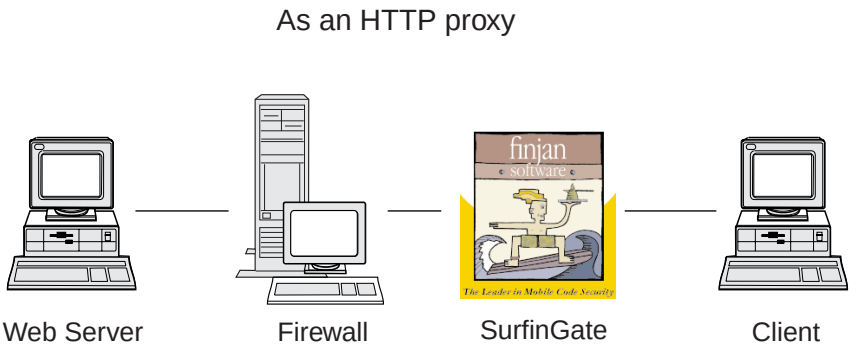


Figure 2. SurfinGate configurations

The client web browsers need to be configured to use SurfinGate as the proxy for HTTP, FTP and HTTPS. Be sure to specify the port number on which SurfinGate is listening (default is 8080).

In SurfinConsole (the administration interface of SurfinGate) you will need to check the **Proxy Mode** option under the General tab. You should also enter the address and port number of the Firewall’s HTTP proxy in the Next Proxy field of the Proxy tab. Alternatively, if you have additional proxies already defined, you may point to them as the next proxy.

Configuring SurfinGate as a Plugin for the Firewall HTTP Proxy

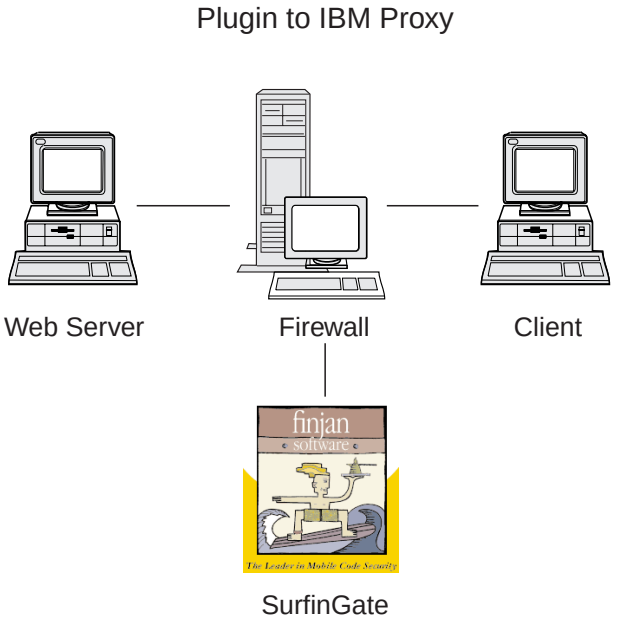


Figure 3. SurfinGate configurations

The client web browsers need to be configured to use the Firewall HTTP proxy as the proxy for HTTP, FTP and HTTPS. Specify the port number on which the Firewall HTTP proxy is listening (default is 8080).

In SurfinConsole (the administration interface of SurfinGate), you will need to check the **Plugin Mode** option under the General tab.

Note: This functionality is only available on the SecureWay Firewall for Windows NT.

Configuring MIMEsweeper

Configuring MAILsweeper

Figure 4. MAILsweeper configurations

If you have a simple environment, MAILsweeper should be configured by the questions asked during the install. To do additional configuration, do the following: **Start->Programs->MAILsweeper for SMTP->MAILsweeper for SMTP Console.** For more information, see the *MAILsweeper Getting Started Guide*.

Configuring WEBsweeper

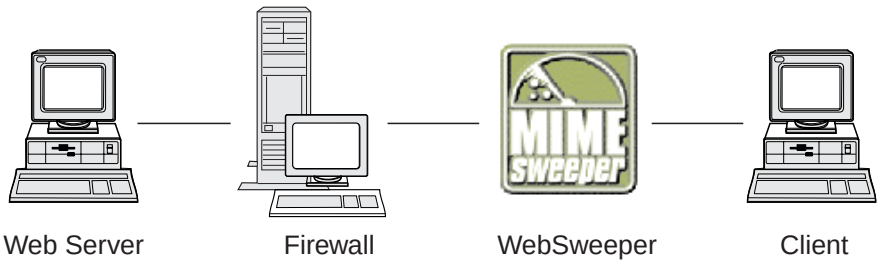


Figure 5. WEBsweeper configurations

To configure, go to the Control Panel and select WEBsweeper applet. For more information, see *WEBsweeper Administrator's Guide* located on the MIMEsweeper CD.

Configuring WEBsweeper HTTPS

To configure, go to the Control Panel and select WEBsweeper HTTPS applet. For more information, see *WEBsweeper Administrator's Guide*.

Intrusion Blocking

Use the command line utilities to create filters that can block specific IP addresses. The addresses to be blocked can be determined dynamically as a result of content inspection. The commands are:

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

If the program is invoked without any parameters it will display a prompt for the format of the parameters required.

The parameters are:

Filter ID

For Windows NT Firewall, the following applies: An ID may be assigned to filters in order to organize their maintenance. IDs are assigned in ascending order beginning with 1, and if the ID is supplied which is higher than the next available ID number, then the ID assigned will be the next available ID number, not the ID number supplied to the program. For instance if some rules exist with ID 1, and you try to create a set of filter rules with ID 3, instead ID 2 will be assigned. Multiple rules may be assigned the same ID number. When rules are deleted using the delete_dynamic program they are referenced by ID and therefore when creating rules by ID plan on having them deleted as a group if they share the same ID.

When the rule has been added the ID number used is displayed.

Filter ID

For AIX Firewall, the following applies: ID can be assigned by number. For example, if you say filter id is ID 12, then it will be assigned ID=12. There can not be filters assigned with the same ID number on AIX. Each filter will have its own unique ID.

Source IP address

The IP address to use for the source of the packets should be entered in dotted decimal notation, for instance 255.255.255.255.

Source IP Mask

This field is used in conjunction with the source IP address and is entered in dotted decimal notation. For instance if the source IP address entered is 10.5.8.0 and the source IP mask is 255.255.255.0, then all packets from 10.5.8.1 through 10.5.8.255 will be matched.

Destination IP address

The IP address to use for the destination of the packets should be entered in dotted decimal notation, for instance 255.255.255.255.

Destination IP Mask

This field is used in conjunction with the destination IP address and is entered in dotted decimal notation. For instance if the destination IP address entered is 10.5.8.0 and the destination IP mask is 255.255.255.0, then all packets from 10.5.8.1 through 10.5.8.255 will be matched.

Adapter

The adapter specification is:

S for adapters designated as secure

N for adapters designated as nonsecure

B for all adapters (both secure and nonsecure)

Packets that originate from the adapter(s) which meet the specified type will match the rule.

Scope The scope of packet traversal through the firewall is specified with this parameter, which can be one of the following values:

L for local packets

R for routed packets

B for both local and routed packets

Direction

Specifies traffic traveling inbound, outbound, or both ways.

I for inbound traffic

O for outbound traffic

B for both inbound and outbound traffic

Logging

Specify Y to turn logging on or N to turn logging off for the dynamic filter activity.

fwdelete_dynamic

If this program is invoked with no parameters, then all currently defined dynamic filters are listed.

```
>>>>  Dynamic Rule Id           =  1
 >>>>>>>>  Jump                 =  0
 >>>>>>>>  Filter Action        =  Deny
 >>>>>>>>  Source Address       =  9.192.8.7
 >>>>>>>>  Source Mask          =  255.255.255.0
 >>>>>>>>  Destination Address  =  9.192.240.1
 >>>>>>>>  Destination Mask     =  255.255.255.0
 >>>>>>>>  Protocol             =  Any
 >>>>>>>>  Source Port          =  Any 0
 >>>>>>>>  Destination Port     =  Any 0
 >>>>>>>>  Adapter              =  Both (Secure and NonSecure)
 >>>>>>>>  Scope                =  Both (Routed and Local)
 >>>>>>>>  Direction            =  Both (Inbound and Outbound)
 >>>>>>>>  Tunnel Id            =  0
 >>>>>>>>  Logging Enabled      =  Unavailable
 >>>>>>>>  Fragments Allowed    =  No
```

Note: The `fwdelete_dynamic` command should be used to first verify that the rules to be deleted have the ID expected.

When the program is invoked with a valid filter ID then the dynamic rule are deleted and the number of rules deleted is displayed in the form x Rules found with id: x.

WARNING: If you try to add a duplicate filter, it will tell you a filter already exists. If you try to add a filter without a Filter ID, you will receive a warning error.

: AIX intrusion blocking can be overridden if there are rules in the upper level rule set. If
: Intrusion blocking is used most rules need to be in the lower level rule set. Dynamic
: rules get added in the middle of these two sets of rules. If there is a rule in the upper
: level allowing traffic you can not turn off the traffic with the dynamic rules.

Testing Your Configuration

After you have done all the setup in the previous chapters, the setup needs to be tested. To test the configuration of SecureWay Boundary Server do the following:

1. Setup a Firewall Proxy user using the Policy Director. Set the user to use Firewall password for secure telnet and set the password for the user.
2. Run the SecureWay Boundary Server wizard to establish the link between the Firewall and the Directory (LDAP).
3. From a secure client start a proxy telnet session.
4. Enter the user setup on Policy Director.
5. You will be prompted for a password.
6. You are now authenticated.

Chapter 6. Related Documentation

You can use the documentation listed in this chapter to find more information about IBM SecureWay Boundary Server Version 2.0 and related products.

IBM SecureWay FirstSecure

The following book *IBM SecureWay FirstSecure Planning and Integration, Version 2.0* contains information about FirstSecure. This book describes FirstSecure and the products that make up FirstSecure and helps you start planning to use all the IBM SecureWay products.

IBM SecureWay Firewall

The following documents contain information about IBM SecureWay Firewall for Windows NT and are available in PDF and HTM format located in the `x:\books\en_US` directory on the IBM SecureWay Firewall CD:

- *IBM SecureWay Firewall for Windows NT Setup and Installation*
- *IBM SecureWay Firewall for Windows NT User's Guide*
- *IBM SecureWay Firewall for Windows NT Reference*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3* (a redbook)

The following documents contain information about IBM SecureWay Firewall for AIX and are available in PDF and HTM format located in the `books/en_US` directory on the IBM SecureWay Firewall CD:

- *IBM SecureWay Firewall for AIX Setup and Installation*
- *IBM SecureWay Firewall for AIX User's Guide*
- *IBM SecureWay Firewall for AIX Reference*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (a redbook)

MIMEsweeper

MAILsweeper

The following documents contain information about MAILsweeper and are available in PDF and HTM format under \install on the MIMEsweeper CD:

- *Getting Started Guide* is located in \install\MSW4_0_2\Doc\qsg.pdf
- Readme is located in \install\MSW4_0_2\README.htm

WEBsweeper

The following documents contain information about WEBsweeper and are available in PDF and HTM format under \install on the MIMEsweeper CD:

- *WEBsweeper Administrator's Guide* is located in \install\WSW3_2_5\Doc\manual.pdf
- Release Note is located in \install\WSW3_2_5\Doc\RELNOTES.htm

WEBsweeper HTTPS Proxy

The following document contains information about WEBsweeper HTTPS proxy and is available in TXT format under \install on the MIMEsweeper CD:

- Readme is located in \install\WSWHTTPS1_0_2\readme.txt

SurfinGate

The following documents contain information about SurfinGate and are available in PDF format under \docs on SurfinGate CD:

- (sgig403)- *SurfinGate Installation Guide*.
- (sgum403)-*SurfinGate User's Manual*.
- Release Note is located in \Docs\SFG 405 RelNotes.pdf
- Information about the SurfinGate plugin is located in the \docs directory.
- (sgumappen405)-*SurfinGate User's Manual Appendix*
- (sgrm405)-*SurfinGate Readme* file is available in text format.

Appendix A. Troubleshooting

This chapter helps you detect and resolve problems associated with SecureWay Boundary Server.

Solving Common Problems for the IBM SecureWay Firewall

Routing Problems

The IBM Firewall provides a feature on the **Security Policy** dialog box entitled *Test IP Routing*, which can be useful for debugging routing problems. Enable this checkbox, activate your Connection configuration, and enable Connection Rules Logging. Then examine your `firewall log` to view detailed information about all packets flowing through your firewall.

Perform these tests first using IP addresses, then using host names.

Cannot Ping Hosts From the Firewall

Problem Explanation
Your network interface is not configured properly.

Recommended Action
See your operating system documentation.

Problem Explanation
Your connection to the nonsecure network is not configured properly.

Recommended Action
Contact your Internet Service Provider for assistance.

Problem Explanation
If your secure network is isolated behind a router, your firewall must have a static route to that router. Use `netstat -rn` to verify static routing:

```
netstat -rn
```

The output should be as follows for Protocol Family 2:

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Figure 6. Sample output from netstat -rn.

nrr.nrr.nrr.nrr
represents your router to the internet and is the default route. The default route is a static route (Flag=UG).

nnn.nnn.nnn
represents your nonsecure domain. This is an interface route (Flag=U).

nnn.nnn.nnn.nnn
represents your nonsecure interface.

sss.sss.sss
represents your secure domain. This is an interface route (Flag=U).

sss.sss.sss.sss
represents your secure interface.

ss1.ss1.ss1
represents a subdomain on the secure side of your network and srr.srr.srr.srr represents the router to that subdomain. This is a static route (Flag=UG).

127.0.0.1
is the loopback or local host. This is an interface route (Flag=U).

You should have an interface route for each interface and your default route should point to the router on the nonsecure side of the firewall.

Recommended Action
Add a static route to your router. Contact your router administrator. Use the `route add` command.

Problem Explanation
The subnet mask on your secure interface or the host you are trying to contact may be incorrect.

Recommended Action
Use your client's configuration utilities to correct the mask settings.

Cannot Ping Nonsecure Hosts From Secure Hosts (Or Vice-versa)

Problem Explanation
Each router adjacent to the firewall must contain a static route specifying the firewall as the gateway for destination networks beyond the firewall.

Recommended Action
Contact the router's administrator.

Problem Explanation
If your secure network uses addresses that are not registered and routable on the nonsecure network, including private addresses as specified in RFC 1597, packets will not be routed back to the sender.

Recommended Action
For Windows NT only: Use a client with a registered address. The firewall's NAT feature may be used for TCP and UDP traffic, but NAT will not translate addresses in ICMP packets like ping.

Recommended Action
For AIX only: Use a client with a registered address.

DNS fails

Note: DNS is for Windows NT only.

Problem Explanation

You received DNS error messages because you configured Microsoft DNS Service with the Microsoft DNS Service Manager.

Recommended Action

Refer back to the Installation instructions and

1. Remove Microsoft DNS by deleting the entire directory: `\winnt\system32\DNS`
2. Reinstall Microsoft DNS
3. Reboot
4. Reinstall the DNS hotfix
5. Reboot

Solving Common Problems–MIMEsweeper

WEBsweeper and MAILsweeper Do Not Seem to Work on the Same Machine

Problem Explanation

Problems when trying to run MAILsweeper and WEBsweeper on the same machine.

Recommended Action

Install MAILsweeper on one machine and WEBsweeper on a separate machine.

Slow Performance of WEBsweeper

Problem Explanation

Unsatisfactory delays in downloading web content when using WEBsweeper.

Recommended Action

1. Disable logging using the WEBsweeper Control Panel applet.
2. Install WEBsweeper on the fastest hardware you can afford to use.

Problems with Licensing of WEBsweeper

Problem Explanation

When installing WEBsweeper 3.2_5 on a machine that has had a previous version of WEBsweeper installed there may be a license key conflict. When WEBsweeper is started, if an Internal Windows Error message: 2140 occurs, check the application log in event viewer. The message from WEBsweeper is: ″PAKMSG error: Username conflicts with previously defined license section.″

Recommended Action

Remove the old license key from the Windows registry. Load regedit and look under the path \\HKEY_LOCAL_MACHINE\SOFTWARE\Content

Technologies\MIMEsweeper\License. If there are more than one key found here, delete the one that is not labeled ″IBM MIMEsweeper System″. Reboot.

WEBsweeper has Problems Downloading Large Files

Problem Explanation

WEBsweeper may run out of virtual memory to store files while filtering.

Recommended Action

Increase amount of physically memory on WEBsweeper server.

Solving Common Problems—SurfinGate

SurfinConsole Stops Responding While Microsoft Internet Explorer is Open

Problem Explanation

The SurfinConsole application exhibits strange behavior or stops responding while Internet Explorer is open. These two applications have a conflict and can not be executed at the same time.

Recommended Action

Do not load Internet Explorer and SurfinConsole at the same time.

Slow Performance of SurfinGate Plugin

Problem Explanation

Mobile code downloads via the web are very slow using the SurfinGate Plugin.

Recommended Action

Be sure the Next Proxy field is set to the SecureWay Firewall HTTP proxy in the Proxy section of SurfinConsole.

Appendix B. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that IBM product, program or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504–1785, U.S.A.

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:

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

The program is NOT licensed under the terms of the IBM Customer Agreement (ICA). It is licensed under the terms of the ″IBM International Program License Agreement″ (IPLA).

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

This product includes computer software created and made available by CERN. This acknowledgement shall be mentioned in full in any product which includes the CERN computer software included herein or parts thereof.

Trademarks

The following terms are trademarks of IBM Corporation in the United States or other countries or both.

AIX

IBM

Microsoft and Windows NT are trademarks or registered trademarks of the Microsoft Corporation.

**SurfinGate is a trademark of Finjan Software, Ltd.

**MIMEsweeper, **MAILsweeper, and **WEBsweeper are trademarks of Content Technologies, Ltd.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Glossary

C

client. A computer system or process that requests a service of another computer system or process that is typically referred to as a server. Multiple clients may share access to a common server.

D

default. A value, attribute, or option that is assumed when none is explicitly specified.

DMZ. Demilitarized Zone. A device to prevent outsider users from getting direct access to a server that has company data.

F

Firewall. A functional unit that protects and controls the connection of one network to other networks. The firewall prevents unwanted or unauthorized communication traffic from entering the protected network and allows only selected communication traffic to leave the protected network.

FTP (File Transfer Protocol). An application protocol used for transferring files to and from network computers. FTP requires a user ID and sometimes a password to allow access to files on a remote host system.

G

gateway. A functional unit that interconnects two computer networks with different architectures.

I

Internet. The worldwide collection of interconnected networks that use the Internet suite of protocols and permit public access.

ICMP. Internet Control Message Protocol. The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source.

intranet. A secure, private network that integrates Internet standards and applications (such as Web browsers) with an organization's existing computer networking infrastructure.

IP. Internet Protocol. A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical layer.

IP address. Internet Protocol address. The unique 32–bit address that specifies the actual location of each device or workstation in a network. It is also known as an Internet address.

IPSEC. Internet Protocol Security. A developing standard for security at the network or packet processing layer of network communication.

L

loopback interface. An interface that bypasses unnecessary communications functions when the information is addressed to an entity within the same system.

N

NAT. Network Address Translation. In a firewall, the conversion of secure IP addresses to external registered addresses. This enables communication with external networks but masks the IP addresses that are used inside the firewall.

P

PICS. Platform for Internet Content Selection. PICS-enabled clients allow the users to determine which rating services they want to use and, for each rating service, which ratings are acceptable and which are unacceptable.

ping. A command that sends Internet Control Message Protocol (ICMP) echo-request packets to a host, gateway, or router with the expectation of receiving a reply.

port. A number that identifies an abstracted communication device. Web servers use port 80 by default.

protocol. The set of rules governing the operation of functional units of a communication system if communication is to take place. Protocols can determine low-level details of machine-to-machine interfaces, such as the order in which bits from a byte are sent; they can also determine high-level exchanges between application programs, such as file transfer.

S

server. A computer that provides shared services to other computers over a network; for example, a file server, a print server, or a mail server.

server address. The unique code assigned to each computer that provides shared services to other computers over a network; for example, a file server, a print server, or a mail server. A standard IP address is a 32-bit address field. The server address can be either the dotted decimal IP address or the host name.

service. A function provided by one or more nodes; for example, HTTP, FTP, Telnet.

shell. The software that accepts and processes command lines from a user's workstation. The Korn shell is one of several UNIX shells available.

SMTP. Simple Mail Transfer Protocol. In the Internet suite of protocols, an application protocol for transferring mail among users in the Internet environment. SMTP specifies the mail exchange sequences and message format. It assumes that the Transmission Control Protocol (TCP) is the underlying protocol.

T

TCP. Transmission Control Protocol. A communications protocol used on the Internet. TCP provides reliable host-to-host exchange of information. It uses IP as the underlying protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol. A suite of protocols designed to allow communication between networks regardless of the communication technologies used in each network.

Telnet. Terminal emulation protocol, a TCP/IP application protocol for remote connection service. Telnet allows a user at one site to gain access to a remote host as if the user's workstation were connected directly to that remote host.

timeout. The time interval allotted for an operation to occur.

U

UDP. User Datagram Protocol. In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

VPN. Virtual Private Network (VPN). A network comprised of one or more secure IP tunnels connecting two or more networks.

W

Web. The network of HTTP servers that contain programs and files, many of them hypertext documents that contain links to other documents on HTTP servers. Also World Wide Web.

WTE. Web Traffic Express (WTE). A caching proxy server that can help speed up end-user response time through highly-efficient caching schemes. Flexible PICS filtering helps network administrators control access to Web-based information at one central location.

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

Readers' Comments — We'd Like to Hear from You

IBM SecureWay® Boundary Server for Windows NT® and AIX
Up and Running
Version 2.0

Publication No. SCT6-RZNA-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

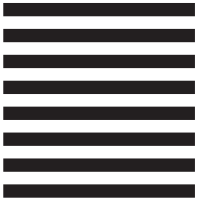
Phone No. _____

Readers' Comments — We'd Like to Hear from You
SCT6-RZNA-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SCT6-RZNA-00

Cut or Fold
Along Line

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

SCT6-RZNA-00

Spine information:

IBM SecureWay® Boundary Server for Windows NT® and AIX

Up and Running

Version 2.0