## Abstract

This paper explains to IT professionals how IBM SecureWay® Boundary Server provides perimeter security for safe and effective use of the Internet for e-business. SecureWay Boundary Server provides a trusted environment that protects your network by controlling who can enter or leave it and what they can access, and helps reduce the risk of potential legal liabilities. SecureWay Boundary Server can also be packaged with other FirstSecure components, such as IBM SecureWay Policy Director, to help reduce risk by reducing complexity through integrated, yet modular solutions, while lowering the total cost of secure computing.

## e-business—a new paradigm

The Internet is transforming and defining an entirely new way of doing business—e-business—a marketplace opportunity that allows businesses to attract new customers, transact business across the Internet and realize significant cost savings compared with traditional ways of doing business. e-business involves the transformation of internal business processes to secure integrated processes that allow normal business to be conducted with customers, employees and business partners across the Internet 24 hours a day, 7 days a week, 365 days a year.

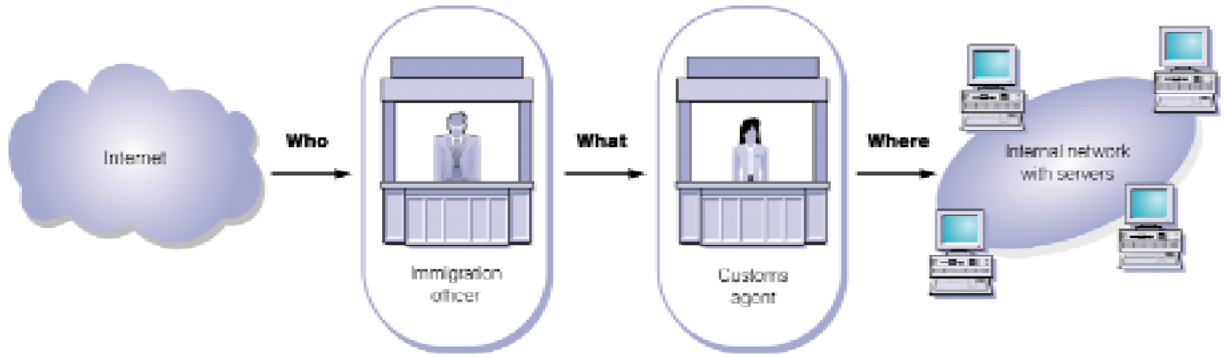
This new transformation has dramatically reshaped the way engagements are done by changing business goals, competitive advantages, targeted audiences, geographical range, and revenue potentials. For successful e-business, businesses must provide a secure, trusted environment. The cry for increased security and a trusted environment is being echoed by businesses, customers, employees, business partners and governments. Everyone must feel confident that his or her use of the Internet is private and data or applications are secure. But many customers worry whether e-business is a trusted environment where they can conduct business safely and without compromising security.

To address this, companies initially built very effective security perimeters (“walls”) around their businesses. But over the past several years they have also built an 8-lane highway overpass! This 8-lane highway overpass is their employees' e-mail and Web surfing. The volume of data flowing unchecked in and out of your network today is enormous. For example, today the Internet will deliver more mail than the United States Postal Service... and the volume continues to grow! The content of this data can present serious financial impacts to your company. The impacts can be to your employees' productivity from viruses, junk mail, the loss of critical business data (even your trade secrets), and even legal issues such as harassment or misrepresentation

Companies have relied on firewalls to provide security for their enterprise-because they let the “good guys” in and kept the “bad guys” out. Firewalls can be compared to immigration officers. If the passport is valid and the person is not on the “deny” list, then the person is allowed to enter the country. Immigration does not necessarily keep the impostors out or search what the person is carrying in or out of the country. Nor can a policy be enforced as to “what” the person can do and where the person may go. Additional levels of screening are needed to achieve and enforce a complete security policy. An individual who completes the immigration process must get through customs. A customs agent will screen for illegal or banned items that the individual may be carrying. This additional step helps police the “what” the individual is carrying and enforces country policy.

The two steps of screening by the immigration officer and the customs officer can be thought of as providing perimeter or boundary security. They prevent bad guys entering, and they screen what is being carried across the border or boundary.

The IBM Boundary Server provides very similar security for customer networks. It helps prevent the bad guys and impostors from entering your network and polices what the good guys can bring in with them, such as inappropriate material, viruses and other harmful code.



## First line of defense ... a must

As more and more individuals get access to the Internet, the need for an Internet usage policy and its enforcement becomes a must for businesses. SecureWay Boundary Server aids in the enforcement of an Internet usage policy by policing the “who” and the “what” that enters or leaves a business environment. The firewall component polices “who” enters and leaves, and the content security and mobile code security polices “what” gets in and out of a business. Doing e-business must contain both, not just who enters but what gets in and out.

What gets in and out of an environment is becoming more significant in the emerging Internet environment. Problems such as loss of data, inappropriate use of business resources, and legal liabilities are becoming very important to businesses. Michael R. Overly, in his book *e-policy*[1],

[1] Overly, Michael, *e-policy, How to Develop Compute, E-mail, and Internet Guidelines to Protect_Your Company and Its Assets* (New York: Amacom, 1999).

outlines a number of issues that corporations must face as e-business rolls out. These issues include, potential claims by employees, potential claims by third persons, and protecting corporate information and resources. E-mail is truly a saving grace in today's environment, but it carries a number of liabilities, as described by Overly. These liabilities include loss of information, reduced operational effectiveness, confidentiality breaches, exposure to legal liability, lost of productivity and damage to reputation through misuse of e-mail. All of these liabilities have a direct effect on e-business. A business must consider them all as it defines its Internet and intranet policy.

Overly defines six essentials for every good policy:

1. The computer belongs to the business
2. Expectations of privacy
3. Monitoring
4. Care in drafting e-mail
5. Avoiding inappropriate content
6. Employee sign-off

Once a policy is in place, a corporation must begin to enforce it, and that's where SecureWay Boundary Server comes in. SecureWay Boundary Server provides functions to help enforce a number of the above elements of a good policy, such as monitoring inappropriate use of the Internet, ensuring privacy of information during transit over the Internet, alerting employees of potential Internet policy violations, and screening e-mail content for data loss or inappropriate content that may lead to a legal liability or theft of corporate secrets.

Enforcing an Internet Usage Policy with SecureWay Boundary Server will help protect your company from:

- Computer viruses from the Internet
- Productivity impacts of junk e-mail
- Productivity loss from employees' inappropriate Web surfing (for example, sports, stock market)
- Harm to the company's reputation caused by receiving or sending inappropriate content, such as pornography
- Network bottlenecks caused by unsolicited e-mail, large attachments or data streaming applications
- Loss or theft of critical business data, such as patient records, customer lists, product strategies, and so on
- Legal liabilities from employee e-mail, such as sexual harassment or company misrepresentation

## IBM SecureWay Boundary Server—a complete perimeter security solution enabling safe and effective use of the Internet

The IBM SecureWay Boundary Server brings together a complete perimeter security solution that:

- Helps protect customer networks from hackers and intruders (bad guys)
- Guards against viruses and mobile code (what enters the enterprise)
- Helps provide a defense against loss of trade secrets or confidential data (what leaves the enterprise)
- May help lower the risks of potential of legal liabilities

SecureWay Boundary Server enables e-business by providing a trusted environment where customers, employees and business partners feel safe and can be assured that their use of e-business is protected.  It speeds the deployment of e-business applications and services by reducing the need to write specific security code in applications. It also delivers a comprehensive security solution in conjunction with other FirstSecure components.

The SecureWay Boundary Server offers an integrated set of products that bring together firewall security, content security, mobile code security and integration with the IBM SecureWay Policy Director for policy management.

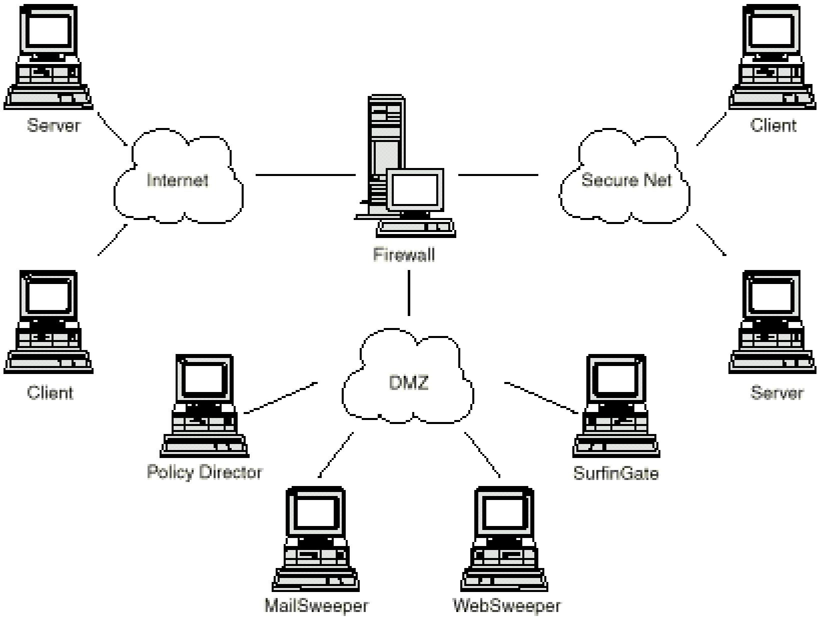


*Figure 1. An example of an IBM SecureWay Boundary Server configuration*

## Components of SecureWay Boundary Server

Firewall Security provides:

- Filtering (including dynamic), proxy (HTTP, mail, FTP and Telnet), and circuit-level gateway to provide customers with a high level of security and flexibility
- Network address translation (NAT) to hide critical resources and reduce the need for registered Internet addresses
- Virtual private network (VPN) support to provide privacy for secure remote connections, through encryption and authentication of traffic into and out of your network
- Two-way control of users, both inside and outside the enterprise
- Strong, two-factor authentication of administrators by incorporating RSA’s ACE/Server and two SecurID Tokens
- Enterprise Firewall Manager to enable multiple firewalls to be managed from a central point helping further reduce the cost and complexity of managing multiple firewalls
- Extensive logging and reporting to help you better manage and audit the perimeter environment

Content Security provides:

- The ability to reduce confidentiality breaches and loss of trade secrets
- The ability to reduce exposure to legal liability including scanning for inappropriate data and adding disclaimers to e-mail
- Reduced loss of productivity due to misuse of e-mail and Web services
- Protection from loss of network service through misuse and hostile attacks
- Filtering of inappropriate e-mail and Web content, including URL blocking
- Management of oversize files sent to and from the Internet
- Screening for viruses, quarantining them and removing the potential threat
- Protection of your enterprise from junk e-mail that may cause performance problems or loss of network resources
- Decomposition of all e-mail attachments and Web page content to prevent harmful or inappropriate material from entering your network

Mobile Code Security provides:

- Inspection of all mobile code entering the enterprise

- Detection of problematic JavaScript™ operations and blocking of JavaScripts that conflict with corporate security policy
- Screening of Java™ applets and ActiveX® controls for abnormal behavior such as runtime errors or malicious activity
- Monitoring File Transfer Protocol for mobile code, keeping watch on code that could otherwise sneak in unnoticed from the Internet
- Blocking known applets/controls from entering the enterprise, therefore avoiding security risks
- Policy management for JavaScript, Java, and ActiveX, with smart filtering for Visual Basic® Script and cookies

## Part of a total IBM integrated security solution

**The solution—enforcement of an Internet usage policy**
The SecureWay Boundary Server is a complete perimeter security solution, providing safe and effective use of the Internet. Boundary Server goes beyond a firewall by not only managing who accesses your network, but also what enters or leaves your network. Boundary Server enables you to define and enforce Internet usage policies that help protect your company from serious financial liabilities.

With SecureWay Boundary Server and FirstSecure, IBM is the only vendor to offer a complete perimeter security solution, combining best-of-breed firewall, content and mobile code security integrated into a security framework for e-business. It is offered at a very attractive price with IBM service and support standing behind it. Secureway Boundary Server can be deployed with the SecureWay Policy Director to provide policy management for your perimeter environment. SecureWay Policy Director provides a centralized point for defining, administering and enforcing security policy related to authentication and access control. FirstSecure, which includes SecureWay Policy Director, SecureWay Boundary Server, Intrusion immunity (intrusion detection and antivirus), Trust Authority (PKI support) and the SecureWay Toolbox (collection of software development security toolkits), is unmatched in providing policy-based security solutions for trusted e-business.

---