Everything You Need to Know About Network Security

AXENT Technologies, Inc.
2400 Research Blvd.
Rockville, Maryland 20850
1-888-44-AXENT
www.axent.com

Additional copies of this document or other AXENT publications may be ordered from your authorized distributor or directly from AXENT.

AXENT Technologies, Inc.
2400 Research Blvd. Suite 200
Rockville, MD 20850
1-888-44-AXENT
(301) 258-5043 (outside USA)
FAX: (301) 227-3745
Internet: www.axent.com

Table of Contents

Introduction

Every company has felt the benefits of networking: faster internal processes, streamlined communications, increased productivity for telecommuters and mobile users, and the tangible achievement of a global market. Once a company taps the power of Internet commerce, virtual office resources, and instantaneous remote office feedback, the demand for access increases. Key trends driving the astounding growth of the Internet as a business tool include:

Increasingly Mobile Workforce

Businesses are relying more and more on a mobile workforce to remain competitive. The sales force needs to be able to access corporate files on demand. Often, the successful sales person is the one who can turn around an RFP or process an order quickly, without waiting for the mail. Our global economy requires employees to be able to conduct business from anywhere on the road, anytime. Other employees, including telecommuters and contract workers, demand a flexible working environment, one in which they can perform their jobs from the convenience of a home office.

Development of Extranets

Businesses increasingly need to interact on-line with their suppliers and business partners. web-based technology, such as browsers and servers, is becoming a popular means of organizing and exchanging information. As industries consolidate and form alliances, extranets allow two companies to share information and collaborate on projects. By making use of the Internet and web-based technologies, businesses can offer services to authorized customers easily, quickly and without a significant investment.

Need for an Alternative to Leased Lines

Previously, companies wishing to establish a private network have had no choice but to use a dedicated line, typically leased from the phone

company. Recent research estimates that companies can save up to 70% over the cost of leased lines (Forrester Research). The following chart compares the advantages of VPN over this alternative:

Traditional Leased Line	Virtual Private Network
Monthly long-distance charges	Pay only for actual usage
Significant equipment investment – separate modem banks, terminal adapters, remote access servers, etc.	Reduced equipment investment – clients/server, tokens (optional)
Interface can be difficult to learn and use	Simplified, familiar user interface
Incompatible with customers, suppliers, trusted partner's systems	Instant compatibility

Security Risk Also Growing

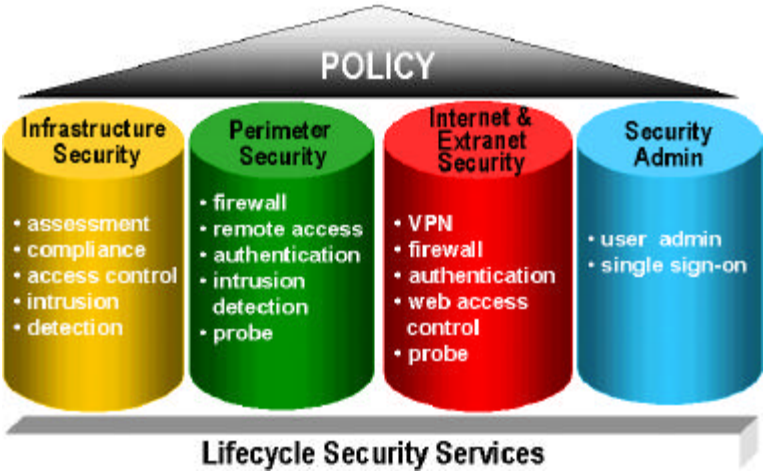
The more complex networking becomes, the greater the challenge becomes to keep them secure. As your Internet and mobile computing infrastructure continues to expand, the access points into corporate data from the Internet and dial-up phone lines multiply. Each access point represents a possible vulnerability that may be exploited to gain unauthorized entry into your network.

Threats from hackers have become legendary. The reality is even scarier – in a recent study by InternetWeek, 60% of respondents stated they have been penetrated over 30 times from the outside. And the risks are high: the lost productivity or wholesale loss of vital information resulting from these security breaches is estimated to cost businesses more than $5 billion annually.

Securing intellectual assets while allowing transparent access to authorized personnel becomes the dilemma of the CIO and the headache of the network administrator. How do you connect safely to the Internet? How do you protect your vital information resources from hackers, competitors, and electronic vandals? How can you safely connect to other organizations

or even other subnets? How can you ensure that only authorized individuals are accessing your information? Where do you begin?

The first step is to formulate a security policy, identifying key assets to secure, and which assets you want to extend to whom. This process will help you establish specific security goals and a plan to tackle them. While this guide will focus on perimeter and Internet security, outlining the key security issues all networked company must address for safe connection to the Internet, realize you need a well-rounded strategy that encompasses the four categories of information security: Infrastructure Security, Administration Security, Perimeter Security and Internet & Extranet Security.



Every enterprise – whether newly emerging or an established multinational – has security needs that extend beyond unauthorized access over the public network. While external threats from hackers are very real, attacks from disgruntled employees are actually much more common and typically more damaging. Developing a security framework means more than implementing a strong perimeter and Internet defense. It requires an approach that both protects vital resources, and supports business needs at all levels of the enterprise.

For more information on how to develop a security policy, please see our guide *Information Security Handbook for Enterprise Computing*

Perimeter Security

Think of your corporate network as your fortress. To secure it against invaders, you must first build an impenetrable wall around it. You lower and raise the drawbridge, allowing in only those people who have correctly identified themselves using the secret password. Every now and then, you circle the fortress to ensure there are no cracks or holes that may be used by marauders seeking to gain a foothold inside. And finally, you install a sentry atop the fortress to stand perpetual guard, ring the alarms when trouble approaches, and launch the flaming arrows to repel the wily intruders who dare to try and climb the fortress walls.

Step One: Secure the Perimeter with an "Airtight" Firewall

Your first line of defense within the enterprise is protecting access to and from the Internet. Without this protection, the door open to the Internet is also door open to the corporate network. A firewall effectively puts a barrier between your corporate network and the outside, securing the perimeter and repelling hackers. The firewall acts as a single point of entry where all traffic coming into the network can be audited, authorized and authenticated. Any suspicious activity – based on rules you establish -- sets off an alert.

How to Choose a Firewall

When evaluating any firewall, it is important to ask each of these questions:

- How are rules created?
- Does it hide network addresses?
- Does it support strong authentication?

- Is it multi-homed to protect web and mail servers on the network from attack?
- Does it filter Java and ActiveX?
- How does it harden the OS?
- Can it handle all your network traffic without sacrificing security?
- Does it provide logging and alerting?
- Is it easy to use?
- Does it support add-on reporting software?
- Does it provide content blocking?
- Is it scalable to accommodate future needs?
- Can remote site firewalls and mobile users be added easily?
- Is it interoperable with other products on the market?

Types of Firewalls

There are three basic types of firewalls on the market today, each offering varying degrees of security and flexibility: routers, stateful packet filtering systems, and application-level proxy firewalls. A simple router, while inexpensive, is unacceptable for the vast majority of business needs. Routers cannot protect against network level attacks such as IP spoofing, source routing, TCP SYN Flood, Ping of Death and other such attacks not related to authorization of connections. Routers also do not provide the level of flexibility and features of a full-security enterprise firewall, such as virtual private networking capability, logging, and authentication.

Stateful systems examine individual packets at or just before the network layer in the protocol stack. This speeds up rule- processing and prevents packets not associated with an already established connection from getting through. In contrast, application-level firewalls authorize connections and examine the data stream by forcing all network traffic to be handled by an intelligent application running on the firewall system specific to the service (FTP, HTTP, SMTP, etc.). Such proxying gives you control over application-level functions and protection against application-level attacks, an absolute priority for almost all organizations. While many stateful

systems include some limited proxy technology, most do not protect you against attacks embedded in the application stream, such as buffer overrun and illegal or unsafe application commands. Application-level firewalls, on the other hand, are designed to thwart the most sophisticated embedded attacks including those spanning multiple network packets.

Factors to Consider:

Network Interfaces

Most application proxy firewalls are multi-homed to create a physical separation of the protected and untrusted networks. Having at least three network interfaces is desirable for protecting public web and mail servers on this network against attack. Some firewalls can connect directly to the Internet via integrated ISDN or Frame Relay connections, eliminating the need for a separate external router. This “air-tight,” reliable security ensures unauthorized traffic cannot pass through the firewall.

Address Translation and/or Hiding

Your firewall should be able to translate source and/or destination IP addresses from their original to a different address. The translation is required for a couple reasons. The first is to hide all the internal addresses of a network. Hiding the addresses ensures that would-be attackers have little or no information about your inside systems that could be used to attack them. Secondly, translation helps to conserve address space. It is very difficult to get a full range of registered IPv4 addresses from the Internic. With address hiding/aggregation, it is possible to use only a few registered addresses to represent all the computer systems behind the firewall.

Because of the use of proxies, application-level firewalls automatically translate all internal addresses to a single outside or registered address. Packet filter firewalls need to be explicitly programmed to translate and/or hide addresses, a cumbersome and tedious task.

Creation of Access Rules

The firewall follows a set of rules that you configure according to your security policy. These rules authorize how to handle and the flow of traffic based on host and network addresses, and other parameters such as time and date range. Your firewall's security is very dependent on your ability to configure these rules properly. If you establish these rules incorrectly, you may inadvertently create a security hole.

Most firewalls use order-dependent, first-fit rules. These order-dependent systems are notoriously easy to misconfigure. If the administrator is not extremely careful when establishing the policy or later adding to it, an incorrect ordering of rules could lead to a serious security breach.

Some firewalls employ non-order-dependent, best-fit rules to greatly simplify policy creation and eliminate the risk of operator error. Best-fit access rules eliminate the chance of one rule superseding and nullifying the other and inadvertently creating a security hole. As your security needs evolve and become more complex, this type of firewall gives you the flexibility to add rules simply and without risk of misconfiguration. Overall, best-fit systems are more intuitive and easier to manage, leading to a more secure firewall system.

Operating System Hardening

At a bare minimum, your firewall should offer some form of operating system hardening at the time the firewall is installed. Ideally, this hardening should be completely automatic, and not require extensive manual configuration, which increases the risk of operator error. Some firewalls offer automatic OS hardening both at installation and during operation. These firewalls continuously monitor the operating system to ensure it is always operating correctly.

Speed/Performance

Your firewall acts as the gateway for all communications into and out of your corporate network, authenticating users, encrypting and decrypting messages, and routing these messages within your network. The firewall must tightly control security while handling traffic from hundreds of users without slowing down network traffic. Because packet filtering firewalls

do not handle each and every connection, they have historically provided somewhat faster performance. Some application proxy firewalls now provide features to greatly improve performance without sacrificing security.

Authentication

Your firewall should be able to authenticate users attempting connection to your network. This may be as simple as requiring a password. In some cases, authorizations based solely on the IP address is not possible (due to DHCP) or not secure enough (due to external IP addresses being easily spoofed). A firewall can provide authentication for services such as FTP, HTTP, and Telnet so that only specific users or groups of users are allowed access from one network to another.

Authentication tokens verify the identity and authorize access to network users according to your policy. These schemes generate a new password with each login to eliminate the threat of password replay attacks.

Logging

A record of each connection that attempted to connect to or through the firewall. This would include both successful and unsuccessful attempts. The logging gives an administrator a non-repudiable record of what has happened. It can also be used to track how a company is using the Internet. An adequate record would include items such as date/time, source and destination IP Addresses, usernames, service type (FTP, HTTP, etc.) and files or URLs transferred. Some firewalls offer the ability to disable logging. This is strongly discouraged since it would be impossible to reconstruct or trace attack activity when it occurs.

Alerting

Alerting is the mechanism to notify an administrator when the firewall needs attention. This is typically done via e-mail, pager, SNMP traps and/or changing the state of the firewall system by playing sound files or changing colors of the screen. Any firewall, at best, can only suspect when an attack is occurring (otherwise, if it knew when a break-in occurred, it

would have prevented the attack in the first place). Alerting is the means to let administrators know of suspicious or unusual activity.

Virtual Private Networking Capability

Virtual private networking capabilities allow distributed companies to extend the network beyond physical boundaries and provide secure communications to a mobile sales force or remote branch offices. Having VPN capabilities integrated with the firewall makes it easier to manage your security policy from one location and one user interface.

Adaptability

Look for a firewall that can adapt seamlessly to future requirements, whether you need to upgrade hardware, manage security at a remote site, add a mobile sales force, or interoperate with your business partners' systems. Non-proprietary systems using standard hardware systems and standard OSs are generally the best approach. This will allow the systems to be re-used when the firewall needs to be replaced. Look for interoperability features, crucial for integrating your firewall system into mixed environments. Adherence to industry standards ensures interoperability with your suppliers, customers, and strategic partners to whom you may wish to extend network access.

Content Blocking

While the Internet offers a lot of useful information, it also presents opportunities for misuse. Some firewalls offer integrated blocking mechanisms that allow you to restrict web or newsgroup browsing of non-productive or objectionable material. These filters allow you to give employees the Internet access they need, while enforcing corporate policies.

Step 2: Check Perimeter Security

Once the firewall is installed and configured, your next step is to test it out thoroughly to ensure you haven't left open or inadvertently created any compromising holes or weaknesses that could be exploited. Because networks are complex and constantly changing, such penetration tests should be performed on a routine basis.

You could hire an expensive "tiger team" to conduct a penetration test. While this may make sense on a one-time basis, it's hardly something you can afford every month. A more cost effective and efficient choice is a probe tool. Probe tools check for common ways to break in to networks and analyze the risk of each vulnerability they find. Some probe tools will automatically perform perimeter as well as internal network vulnerability checks, assessing risks and even providing expert advice concerning security problems they find. As a result, you can quickly pinpoint holes in the network and plug them, before data is stolen or damaged.

How to Choose a Probe Tool

Be sure the probe you choose checks for vulnerabilities not only from inside the firewall, but outside as well. This will provide a hacker's-eye view of your network vulnerability. Choose a scanner that employs multiple protocols – not just IP -- to detect vulnerable network resources, such as NetWare, which can be accessed in non-IP ways. Traditionally, these scanners have only been able to probe a single box at a time. Sophisticated scanners are now available to test multiple systems simultaneously, revealing how minor vulnerabilities can be exploited together, creating a major security risk.

Step 3: Install a Sentry

While a firewall will alert you of suspicious activity, it does nothing to stop it. Attempting to manually review log file is hopelessly time-consuming and a losing battle. Installing an automatic intrusion detector

gives you an extra measure of protection. An intrusion detector acts like a sentry to guard the perimeter and immediately detect and respond to attacks on the network. The main reason for intrusion detection is not to prevent intrusion, but to catch the intrusion and stop it before anything can happen. Some of the automated responses typically include notifying a security administrator; stopping the offending session, shutting the system down; turning off down Internet links; disabling users; or executing a predefined command procedure. Intrusion detectors provide round the clock protection, 24 hours a day, 7 days a week.

How to Choose an Intrusion Detection Solution

An effective method for real-time intrusion detection is to monitor security-related activity occurring on the various systems and devices that make up the network. While most activity monitors watch the operating system audit trails, more sophisticated tools also:

- Track audit trails from applications, databases, web servers, routers, firewalls, etc.
- Monitor critical files for Trojan horses, unauthorized changes, etc.
- Watch TCP and UDP port activity
- Accept SNMP traps and triggers

Real-time activity monitors can detect attacks such as attempts to access unauthorized files or to replace the log-in program with a new version. Unlike packet sniffers, they can detect when a user illegally obtains “root” or administrator access. When suspicious activity is detected, the real-time activity monitor can take immediate action before damage is done.

The advantage of real-time activity monitors is that they deploy close to the mission-critical data and applications. Monitoring for attacks from both inside and outside the network becomes much easier, since all of the devices are being watched. In addition, many application and operating system-level attacks are not discernable at the packet level and require system level monitoring to detect.

When choosing an intrusion detector, look for one that can be managed from a central console, while still monitoring activity through the entire

network. The detector should rely on the devices themselves first-level packet monitoring. Events that manage to slip through the device's capabilities to catch them are then evaluated by the intrusion detector. Suspicious activity from multiple locations in the network should be correlated as it occurs. For example, an intruder may use a hacker program to attempt to guess the root password on a hundred UNIX systems at the same time.

The software should be able to detect intrusions even if network connections are encrypted or if attackers use direct dial-up connections. The detector should log critical security activity on manager systems. This makes it difficult for hackers to cover their tracks, since activity is logged on another system in the network -–not just on a local audit trail. It also centralizes and facilitates audit trail management. And finally, because new attacks are being created everyday, the intrusion detector should be easily updated to handle new scenarios on a regular basis. The vendor should publish these scenarios on the web so you can download them and rapidly deploy them throughout the enterprise.

For more information, see our "*Guide to Intrusion Detection*"

Step 4: Prevent Unauthorized Access via Dial-Up

Preventing unauthorized access to your network is the final piece of perimeter security. Without authentication, a hacker can easily impersonate legitimate users to gain access to the corporate network.. How do you ensure remote users have access to the computer resources they need to do their job without sacrificing corporate network security? You determine the user is who he claims to be by requesting some form of authentication. There are two basic types of authentication schemes being used by today's operating systems, communication servers, and firewalls:

- Static (hard-coded) password
- Two-factor (strong) authentication

Traditional static IDs and passwords have been proven to be inadequate for uniquely authenticating users. Static passwords are too easily known by others, shared, guessed, and cracked. Forcing users to regularly change their passwords causes them to choose passwords that are easily known and compromised. Because today's users have so many passwords to remember they write them down and leave them in public view.

Passwords may also be compromised with hacker tools such as password sniffers, network sniffers, dictionary attacks, etc. Once passwords are stolen, legitimate users can be easily impersonated and access your files with ease.

Two-Factor Authentication

Two-factor authentication systems uniquely authenticate users without forcing them to remember another new password. Two-factor authentication is based on the proven principle of something unique that the user has -- a token -- and something unique that the user knows -- a PIN number to activate the token. This process creates a unique one-time password that cannot be guessed, shared, or cracked. For that reason, two-factor authentication is highly preferable to other less, secure schemes.

Software vs Hand-held Tokens

While software and hand-held tokens are equally secure, each has its distinct advantages. Software tokens are ideal for users who employ a single device to log-on to the network, whereas hand-held tokens are best utilized by users who frequently log-on from many different computing locations and platforms. Hand-held tokens are easily lost or stolen and are twice the cost of software tokens. On the other hand, because software tokens are transparent to the user, they are easier to use. Additionally, they eliminate the need for users to carry a separate hand-held token. The user's laptop computer or PC becomes a token when the software token is activated.

For more information on authentication, see our guide,

Security Briefcase Handbook

Internet & Extranet Security

While the affordability and availability of the Internet make it an attractive business tool, it is a public network that offers no security. Communicating over the internet is extremely risky without the right technology. E-mail, files and passwords are easily intercepted by a variety of "sniffers" and hacker tools. In fact, many hacker tools are commonly available on the Internet for free. How do you protect sensitive data from prying eyes as it travels through the Internet? While the Internet can be leveraged as a cost-efficient means to extend your corporate network virtually anywhere, how do you establish a secure, private network to your multiple sites, telecommuters, and road warriors distributed across the world? web-based browsers and servers give you the ability to centralize information and services -- how do you extend selective access to business partners, suppliers, and customers, without compromising security?

Step 1: Implement a Virtual Private Network

What is a Virtual Private Network?

A virtual private network combines authentication with data encryption and authorization to protect information en route over the public Internet. VPN technology:

1. Establishes a secure tunnel between the remote user and the corporate network

2. Encapsulates and encrypts data packets

3. Authenticates the user and authorizes user access of the corporate resources on the network.

Encryption

Before transmission, the data is encrypted and encapsulated to protect it from prying eyes. Information can not be viewed, modified or intercepted in a usable form from these encrypted packets. Additionally, the intercepted information does not provide any usable information about the protected hosts on the corporate network. It uses powerful, industry-standard encryption algorithms to ensure that data traveling over the Internet, WANs, customer's network or an Intranet cannot be intercepted. The product you select should support a strong encryption algorithm, "strong" being relative to the sensitivity of your data. Most vendors offer the option of a 40-bit encryption key. The 40-bit key length was chosen because the US Government allows the export of 40-bit encryption without any export control. 40-bit encryption will stop a casual cracker, but should not be considered strong.

Encryption using 56-bit Data Encryption Standard, or DES, algorithm are approximately 65,000 times stronger than 40-bit algorithms. Although there has been recent publicity about a successful, concerted Internet effort to crack a short DES message, for most purposes DES is considered to be very strong. For US and Canadian use, even stronger algorithms can be used. In general, these algorithms, such as Triple-DES, use longer key lengths to provide more protection.

Step 2: Identify Those Accessing Information

Virtual private networking products must provide a way of ensuring, or authenticating, the user's identity. Traditional authentication relies on passwords that are static or reusable. These are easily obtained by hackers and are often left lying around on Post-It notes or written down in a user's planner or wallet. Strong, or two-factor, authentication, provides the highest level of remote access security without burdening users with additional passwords or log-in procedures. Additionally it provides a highly reliable user-accountability mechanism. When prompted, a user enters his or her PIN to launch a transparent strong authentication dialog between the user and the network. The data exchanged during the one-time

challenge/response interaction is valid only once, and the user's PIN is never transmitted over the public network. Even if the exchange is intercepted by any number of hacking techniques, it is no longer valid for access.

Authentication is useless if your users are tempted to bypass it. The easier and simpler it is to use, the greater the chance it won't be circumvented, thus compromising security. The best authentication schemes consolidate the number of sign-on steps, enabling users to simply enter an ID and Password upon login onto the laptop or PC. The user's PIN is the only requirement necessary to activate secure remote access. Strong, two-factor authentication is performed transparently to the end user.

Authentication is not only used to verify the identity of an individual, but to determine what resources he may have access to. For example, your remote and mobile employees might be given access to the same amount of information your in-house employees may see: financial, competitive, and product information. Your business partners, on the other hand, may have access only to specific information related to a collaborative project, but need to block them from competitive or financial information. And you may grant your customers access to specific web-based services you offer exclusively, but not to the confidential details of your business. Each of these users require a different security strategy: remote, mobile and extranet.

Step 3: Remote Access Control

Remote users at multiple branch sites require the same security level as your corporate headquarters. That means fortifying their perimeter with a firewall, checking it routinely with a probe tool, and installing an intrusion detector for proactive response to intruders. Each firewall may then be linked via a virtual private network.

Look for a firewall that offers integrated VPN capability and support of multiple remote firewalls. Centralized management via the corporate firewall provides the maximum flexibility and security, and offers a cost savings as well. The remote firewalls provide essentially the same product functionality, minus the management interface.

Step 4: Mobile Access Control

Client VPN software runs on the user's laptop PC. The server may be a integrated into the firewall or reside on a gateway that is behind the firewall. There are advantages and disadvantages to both. Firewall-dependent software guarantees compatibility from firewall to VPN client. Multiple VPNs are managed from the one central firewall console. By contrast, firewall-independent VPN software provides an advantage to network managers with many types of incompatible firewalls, and because it is independent of the firewall, has no impact on its performance. Multiple VPNs are centrally managed via the VPN server interface.

Growing laptop theft is major concern. According to Safeware Insurance, a major computer insurer, more than 250,000 laptop computers were reported stolen in 1996, representing a 27% increase from 1995 and a loss of more than $800 million in hardware and software assets. Every business notebook contains proprietary data, ranging from customer contact information to financial information. How do you secure the information on your mobile users' laptops? VPN products feature local file encryption to ensure that data on the PC cannot be viewed by unauthorized users. Sensitive files are encrypted and decrypted. Many desktop data encryption solutions require end users to manually encrypt or decrypt data each time they access a particular file. Nearly all users, often in a hurry, do not remember to take this step—leaving data unprotected even though the software is on their laptop. Some products do this automatically, enabling busy end users to effortlessly protect data stored on laptops. Newly created files are automatically protected, no matter where the files are created and stored (locally, on file servers, floppy drives or even as they are transmitted across the network). Idle workstation protection guards unattended PCs that are left on or connected to a network by automatically displaying the Windows screen saver after a set period of time, requiring end users to log on again in order to gain access to the system.

For more information on secure mobile access, see our guide,

Security Briefcase Handbook

Step 5: Secure Remote Web Access

Companies are rapidly deploying web-based applications as a convenient way of publishing information and accessing corporate services making it available in one central location. Your web applications provide access to valuable company information and are visited frequently. Unfortunately, internal web servers are critical resources that make good targets for internal hackers. How can you extend that access to your customers, vendors and partners without compromising security? With such a diverse audience accessing web-based information, how can you control and manage who gets in and what they are allowed to access?

Providing secure, centralized access control to web-based information is particularly challenging given the limitations of today's web technology. While the combination of a web browser and a web server is a powerful communication vehicle, much of today's custom-developed web technology, such as cookies, are not designed for security and scalability. Multiple servers require individual authentication and administration, and multiple services maintain their own tracking facilities and must be managed separately. New web security technology is now available to provide web-based security administration out-of-the-box. Features to look for when evaluating web security technology include:

Scalability

The access control system you implement should be independent of the web application architecture and provide an easy-to-use centralized administration interface. This allows web developers to reuse the web applications to meet expanding requirements without re-engineering the access control system. It also eliminates the need to re-train site administrators.

Single sign-on for secure access control

For secure access control, a tool's architecture should include a centralized server to challenge users for credentials and verify them utilizing existing authentication methods or user directories. It should also provide a

mechanism to administer "tickets" to carry the User's authorization information and not require further authentication. The user should only be required to have a standard web browser—and, since the communications are occurring over the Internet, the security administrator must have the flexibility to encrypt all information exchanging during the authentication.

After the initial authentication and "ticketing," the user should be able to move within the web site and be able to access content allowed by the content administrator without needing additional authentication for that session. If "tickets" are to be used to store user access information on the web browser, however, the access control system must handle two security issues. First, it must prevent a hacker, who may have obtained a ticket from "sniffing" the wire, from modifying that ticket to gain access. Second, it must ensure that the administrator can specify a set time period for the ticket to be valid.

Security exposures from user name/password authentication can be avoided by using tools that require only a single sign-on for accessing web applications. This eliminates the risk of users storing multiple, hard-to-remember passwords in unsecured locations (e.g., on message pads next to their computer or in their planners) where they can be easily spotted and "stolen." Furthermore, using tools that require password validation only once—on the first request—reduces the risk of hackers "snooping" user names and passwords as they are transmitted across the network.

Centralized Security Management

Solutions that provide for centralized control capabilities can alleviate these frustrations for managers *and* end users. Security administrators need access control applications that provide a graphical user interface (GUI) to select authentication methods, set up and manage user access across one or more web servers. In addition, because most corporations also have separate webmasters and content administrators for each major web server, the access control application should not only provide a centralized security administration interface but also allow separate content administrators to apply the access protection specific directories and content that they manage. This is especially important given that the web content is normally extremely dynamic and the privileges assigned to the users are not static.

Interoperability

When selecting web access security tools, consideration should be given to those that offer multi-platform support. A tool should provide centralized access control for both NT and UNIX web-servers, thus protecting UNIX-based content with NT domain credentials. As your web site becomes even more successful, new services will be added and traffic will increase. You need a solution that will adapt to your growing needs. Traditional approaches fail in a cross-platform environment. They depend on web servers, secure sockets layer (SSL), encryption and application programming that often degrade web applications and usability and can open – rather than close – the door to unauthorized access. Choose a web security technology that installs and integrates seamlessly with existing platforms and security infrastructures by using standard security and web protocols to communicate between components.

Multiple Authentication System Support

Users should have the flexibility to require traditional reusable passwords for authentication or require strong token authentication before accessing web services.

AXENT Security Framework

Today's distributed computing environment places your organization's valuable information at risk. The AXENT Security Framework addresses key security issues to protect information and to enable secure communications. The components of the AXENT Framework match security solutions with your unique business needs and ensure that vital information is protected at all levels of the enterprise. Geared for business, AXENT's state-of-the-art solutions are integrated, easy to use and, of course, highly secure.

Information Security Policy

Information security begins with a sound security policy that balances the confidentiality and integrity of information against the cost of protecting that information and its level of availability. Without a written policy, your organization runs the risk of being misunderstood by its employees and makes it difficult to enforce disciplinary measures of a violation if established policies are not implemented.

Infrastructure Security

A solid organizational infrastructure is essential to protecting confidential information. With the advent of enterprise-wide computing it is important to have the ability to define, manage and enforce security policies across your entire networking environment. Security tools must be able to cross-heterogeneous environments to periodically review and automatically notify you of a policy violation by the system from one central workstation.

Enterprise Security Manager™

ESM is an enterprise-wide security management solution that defines, manages and enforces your information security policy. Enterprise Security Manager proactively checks the entire enterprise for security vulnerabilities, assesses security risks, and centrally controls security parameters on over 55 platforms.

Intruder Alert™

Intruder Alert monitors systems and networks in real-time to detect security breaches and suspicious activities and will respond automatically according to your established security policy. It works across your entire enterprise including LANs, WANs, intranets and the Internet.

PCShield™

PCShield is a complete policy-driven security system for PCs and notebooks that protects the confidentiality and integrity of valuable data, and controls access to critical system resources. PCShield's transparent integration with the Windows® 95, Windows® 98 and Windows NT® operating systems and its centralized administration facility make it easy for you to implement and manage.

Privilege Manager™ for UNIX®

Privilege Manager for UNIX is the first out-of-the-box solution to help you control access to root privileges. It allows delegation of UNIX root authority, so that you can implement reasonable security controls, without impacting the ability of users to perform their daily work.

NetRecon™

NetRecon is a third-generation enterprise-wide security probe that leverages UltraScan™ technology to execute multiple scans simultaneously to quickly find, analyze and report perimeter and internal security vulnerabilities.

Perimeter Security

Organizations must secure information against unwanted users and hackers, yet enable authorized users to connect to the network. Balancing these needs requires a solution set that protects the perimeter, checks and detects attacks to the perimeter and controls access to information.

Raptor Firewall

Raptor Firewall combines the highest level of perimeter security available with the performance, interoperability, scalability, and ease of use to meet your business goals. This award-winning firewall provides centralized, real-time enterprise security across the Internet, intranets, mobile computing and remote sites to give authorized users seamless, secure network access. The Raptor Firewall includes the first and only IPSec™ certified VPN server for Windows NT®.

Defender

Defender implements a two-factor authentication system to create one-time passwords that uniquely authenticates users and grants access over dial-up, ISDN, Internet, and on-LAN connections.

Intruder Alert

Intruder Alert detects and responds to security breaches and suspicious activities from the outside the perimeter, as well as from within. Intruder Alert monitors systems and networks in real-time to detect security breaches and suspicious activities and will respond automatically according to your established security policy. It works across your entire enterprise including LANs, WANs, intranets and the Internet.

NetRecon

NetRecon is a third-generation enterprise-wide security probe that leverages UltraScan™ technology to execute multiple scans simultaneously to quickly find, analyze and report perimeter and internal security vulnerabilities.

Internet & Extranet Security

The Internet is a valuable resource that enables organizations to communicate more efficiently, reduce telecommunication costs and provide more timely information. The challenge is to deliver Internet services without compromising the security of your organization's network.

Security Briefcase™

Security Briefcase includes everything you need for remote access security. Security Briefcase bundles a virtual private network, two-factor user authentication and PC/laptop transparent data encryption to securely and remotely access information via the Internet.

WebDefender™

WebDefender provides secure single sign-on access control across a company's growing number of web applications and web servers. WebDefender centralizes the management of end user authentication and authorization to lower the cost of deploying your Web applications.

Defender

Defender helps reduce the risk of unwanted intrusions across the Internet with its two-factor authentication system that creates one-time passwords that uniquely authenticate users and grants access over dial-up, ISDN, Internet, and on-LAN connections.

RaptorMobile™

RaptorMobile is a proven virtual private networking (VPN) client providing laptop/desktop PC to server encryption and authentication. RaptorMobile extends easy to use network security to laptop users and telecommuters while allowing seamless access anywhere in the world.

Raptor Firewall

Raptor Firewall not only guards the perimeter of an organization but also provides maximum security from unwanted Internet attacks. Raptor Firewall has the performance; interoperability, scalability, and ease of use you need to meet your business goals. This award-winning firewall provides centralized, real-time enterprise security across the Internet, intranets, mobile computing and remote sites to give authorized users seamless, secure network access. The Raptor Firewall includes the first and only IPSec™ certified VPN server for Windows NT®.

NetRecon

NetRecon reduces threats from the Internet with its third-generation enterprise-wide security probe that leverages UltraScan™ technology to execute multiple scans simultaneously to quickly find, analyze and report perimeter and internal security vulnerabilities.

Security Administration

Today's enterprise computing environments consist of multiple operating systems running applications from different vendors and accessed by multiple client platforms. Organizations need a cost effective secure solution to manage and administer users and the computing resources from one central location.

Enterprise Resource Manager™

Enterprise Resource Manager greatly simplifies administrative tasks for systems and security managers from one central repository. It provides enterprise-wide user and resource administration across distributed computing platforms, as well secure single sign-on to platforms and applications.

Resource Manager™ for UNIX®

Resource Manager for UNIX provides a graphical representation of system administration no matter what vendor's variation of UNIX you are using. As part of the comprehensive Enterprise Resource Manager family the Resource Manager for UNIX user interface provides full point-and-click use, drag and drop icons and on-line help. Managing UNIX system users across heterogeneous platforms has never been easier.

Lifecycle Security Services

AXENT is dedicated to making sure that you have the services required to help before, during and after a solution installation. AXENT's subsidiary Secure Network Consulting inc. (SNCi) offers a full range of lifecycle security support services including firewall installation, enterprise security management planning and diagnostic vulnerability assessment services. In addition SNCi customizes services and provides security policy and procedures development, corporate-wide education and training, configuration management, network security monitoring, security metrics, business continuity and a comprehensive risk management program. These services, coupled with extensive experience with leading-edge technologies, enable SNCi to facilitate the implementation and utilization of information security solutions.

For all your information security needs, just do what 40 of the Fortune 50 did. Call AXENT at 1 888 44 AXENT or visit us online at www.axent.com