Microsoft

Security Watch

A QUARTERLY PUBLICATION

CONTENTS

ADVERTISER-SPONSORED CASE STUDIES

SECURITY WATCH FEBRUARY 2003

This special advertising section was produced by the *Windows & .NET Magazine* Custom Media Group in conjunction with Microsoft. This supplement appears as an insert in the February 2003 issue of *Windows & .NET Magazine*.

Defending Critical Servers from Today's Internet Attacks

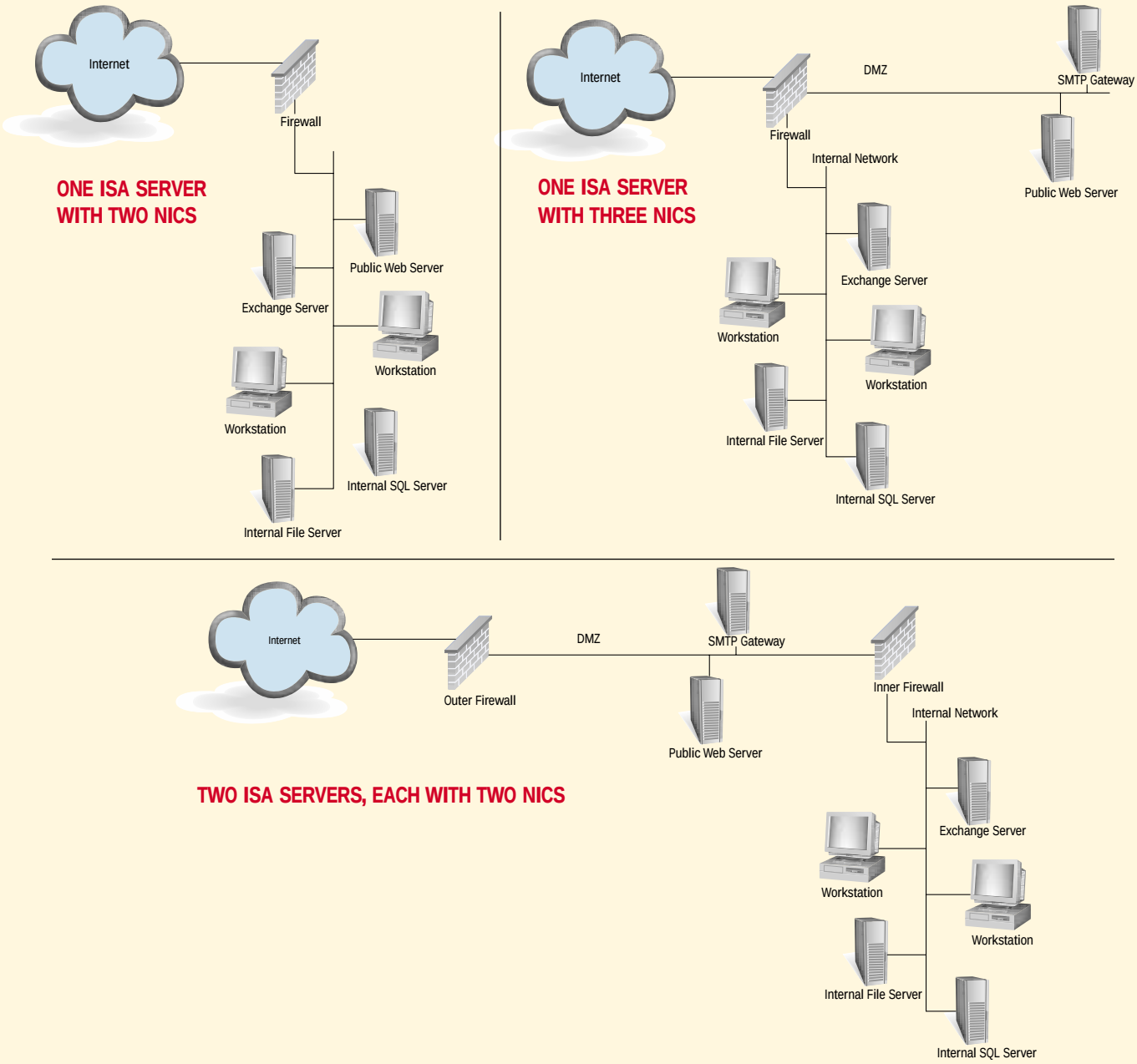
ISA Server Goes Beyond Traditional Firewall Filtering

Email servers, Web servers, and Web browsers serve as "point man" against attackers who, more and more often, target the application layer (layer 7 on the OSI model). The bane of organizations today is unwanted email such as bandwidth-gobbling spam and messages carrying hidden worms and viruses. But no business can survive without Internet email: telecommuters, traveling employees, and contractors need access to internal Exchange servers for email, collaboration, scheduling, and more. Providing that access, however, is complicated for administrators and users and fraught with security risks.

You can provide remote access to Exchange through a VPN, but such a solution complicates life for a user and presents greater risk because a VPN client is as connected to an internal network as if it was plugged in locally. Unless you implement further controls, what's to stop an attacker who compromises your VPN from going further? And while you don't mind a contractor or business partner accessing your Exchange or intranet Web server, do you want them to be able to access your financials or research and development? Providing remote access via Exchange Outlook Web Access (OWA) addresses part of the problem, but users must settle for limited functionality and adapt to a different interface. OWA also brings Internet Information Server (IIS) into the picture and the need to protect it as well. Adding a stateful inspection and packet filtering firewall (layer 4 on the OSI model) does little to protect an IIS server because today's attacks (e.g., Code Red, Nimda, Goner) target the application.

A traditional stateful inspection and packet filtering firewall sees that a packet is destined for a server on a given port and passes it on to the server in the internal network, yet today's attacks are *inside* the payload of these packets. As recently as a few years

FIGURE 1: Network Configurations Supported by ISA Server



ago, almost every packet traveling over port 80 was Web traffic. Today, port 80 traffic consists of Web browsing, OWA, XML Web Services and various instant messaging clients to name a few. Each of these http content types creates the potential for new types of exploits, buffer overflows, and other security holes. OWA content is secured by SSL. Traditional firewalls are unable to detect attacks with SSL traffic

LOOK TO ISA SERVER

Microsoft's firewall, Internet Security and Acceleration (ISA) Server 2000, provides classic packet filtering and stateful inspection — and is optimized for application-layer filtering, security that is vital for networks today. Its architecture is incredibly extensible, a feature that lets Microsoft and other vendors develop pluggable filters for specific applications. In addition, ISA internal network and makes the request on behalf of the client. Then the firewall receives the reply from the server and repackages the information into new packets sent to the client. This approach lets ISA Server be the middleman for all traffic, and ensures that no untrusted Internet user traffic is routed directly into the internal network.

ISA Server can also protect

You can download a six-month trial version of ISA Server from http://www.microsoft .com/isaserver

against application-layer attacks traveling inside content encrypted with SSL. ISA Server can inspect the SSL traffic, something most other firewalls cannot do. When a client sends an https (http with SSL) request to a Web server protected by ISA Server, the traffic stops at the ISA Server, where it is decrypted and inspected. After inspection, ISA Server sends valid requests to the internal Web server via http or https. After receiving a reply from the server, ISA Server forwards the reply to the client via the https connection.

ISA SERVER FUNCTIONALITY

ISA Server deals with the performance cost of application-layer filtering with reverse caching and scalability. ISA Server caches content frequently requested from your Web server and serves that content to the client directly from RAM, without bothering your Web server. You can scale up to a more powerful server or scale out with multiple, load-balanced ISA Servers. You can get further performance boosts with SSL acceleration hardware add-ons and content delivery add-ons from Microsoft partners (http://www .microsoft.com/isaserver /partners). You can download a six-month trial version of ISA Server from http://www.microsoft .com/isaserver.

ISA Server runs in one of three modes: cache, firewall, or integrated. Cache mode makes ISA Server only a caching server, with no firewall functionality enabled. You can cache popular Internet content for your users or you can use ISA Server's reverse caching capability to speed delivery of content from your Web site to other users. ISA Server cache arrays maintain speed and availability by sharing cached content with each other via ISA Server's Cache Array Routing Protocol. In firewall mode, ISA Server functions as a firewall with no caching turned on. In integrated mode, ISA Server functions both as a cache server and as a firewall. ISA Server also integrates directly into Active Directory (AD) so security policies can be created with existing AD users and groups.

ISA Server supports three network configurations (Figure 1). First, you can set up one ISA Server with two NICs connected to the Internet and an internal network. In this case, you don't have a separate DMZ network for servers accessible from the Internet. Second, you can install three NICs on your ISA server. The third NIC connects to your DMZ, called a three-homed DMZ. Third, you can install two ISA Servers, each with two NICs. The outer ISA Server connects to the Internet and the DMZ. The inner ISA Server connects to the DMZ and the internal network. This approach is called a back-to-back DMZ.

In ISA Server, you designate each NIC as internal or external by defining a local address table (LAT). The LAT includes all IP subnets on your internal network. Therefore, ISA Server classifies any NIC whose address falls within the LAT as internal; all other NICs are classified as external. ISA Server's application-level firewall features are available only for protecting internal computers. Therefore, the three-homed DMZ option provides only packet filtering and stateful inspection for your DMZ. Using either on ISA Server with two NICs or the back-to-back DMZ are the only options that give you a full ISA Server filtering capabilities for both the DMZ and the internal network.

FIGURE 2: Enabling Incoming SMTP and Default Authentication

FIGURE 3: SMTP Filter Properties, Attachments Tab

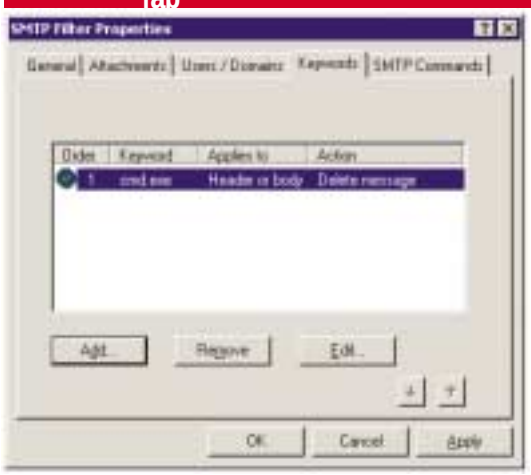
PROTECTING YOUR EXCHANGE SERVER

In addition to normal layer 4 protection, you can use ISA Server to protect Exchange Server in four different ways. First, you can use ISA Server's built-in SMTP filtering. Second, you can implement Exchange remote procedure call (RPC) filtering. Third, if you use OWA, you can use ISA Server's http filtering to protect the IIS server. Fourth, ISA Server includes a post office protocol (POP) filter that checks POP traffic for buffer overflow attempts. By implementing ISA Server's SMTP filtering between the Internet and your Exchange Server, you can erect a layer 7 perimeter defense that drops spam and malicious emails at the edge of your network. You can configure the SMTP filter to drop emails based on sender, domain name, and keywords and by extension, name, and size of attachments. To protect against attackers fooling around with the SMTP protocol for the purpose of exploiting buffer overflows, the SMTP filter enforces which SMTP commands are allowed and how long they are allowed. You can take further advantage of ISA Server's extensible architecture and plug-in third-party virus scanning add-ons such as Symantec's AntiVirus for ISA Server and Trend Micro's InterScan WebProtect. More information about these add-ons is available at http://www .microsoft.com isaserver/partners /contentsecurity.asp.

To configure settings for ISA Server to receive incoming SMTP emails, scan them, and then forward them to your Exchange Server, open ISA Management MMC and right click on Server Publishing Rules. "Select Secure Mail Server…" to start the Mail Server Security Wizard. Select default authentication for SMTP and make sure you also check content filtering (Figure 2). If you don't check that box, you won't activate the SMTP filter and you'll miss all its checks. Step through the rest of the wizard, which will ask you for the IP address of your internal SMTP server and the external address published on the Internet as the MX record for your DNS domain. This address must be one of the external addresses configured for your ISA server. The wizard creates the appropriate Server Publishing Rule and maps it to the SMTP filter.

Next, select the Application Filters folder under Extensions and double click on SMTP Filter. On the Attachments tab, you can delete, forward, or hold messages based on attachment name, file extension, or size (Figure 3). Holding or forwarding messages gives you a way to selectively allow the passage of messages to users who need an attachment that would ordinarily be blocked. Be aware that the SMTP filter doesn't look inside archive files such as zip files for inappropriate attachments. However, most Exchange and ISA Server AV plug-ins do provide this functionality. Consider the ISA Server SMTP filter as your first line of defense, to take broad strokes at filtering mail. Figure 4 shows the SMTP filter configured to reject messages that contain "cmd.exe" anywhere in the message. You can use keyword rules to catch messages that contain inappropriate or malicious words, but be careful.

FIGURE 4: SMTP Filter Properties, Keyword Tab



Raymond James and Associates Makes Aelita Part of Security Infrastructure

As a leader in financial services with a worldwide IT infrastructure, Raymond James (Financial Services) & Associates recognizes the value of IT audit data in monitoring security and improving operations. The challenge was in finding a single solution that could meet their data collection and analysis requirements with a zero footprint on remote servers. Scalability was also an issue as the company's IT infrastructure supports approximately 12,000 users across 2,200 locations.

"Our first requirement was to consolidate events across remote locations so we could more effectively respond to those events, whether they were security or systems related," said David Bryant, a senior information security engineer at Raymond James & Associates. "We wanted to accomplish this without installing anything on the remote servers so we didn't have to deal with load management and updates."

Bryant also wanted to integrate directory management with event management. "As a security person, I want to know about anything that changes in Active Directory. Having this information available through the same console as other security data helps ensure it gets analyzed and used."

After conducting a market search, Bryant found that "Aelita was the only company that had a solution that met all our requirements. In evaluating their technology, it was clear Aelita understood our needs from both a security and systems management perspective."

THE AELITA SOLUTION

Aelita's solution was integrated event log and directory analysis and reporting delivered through Aelita InTrust and Enterprise Directory Reporter.

InTrust is a robust and scalable enterprise event management, analysis and auditing system that collects, consolidates, analyzes and distributes security and operating data for use in security assessment, security auditing and troubleshooting. Enterprise Directory Reporter (EDR) offers a comprehensive directory reporting and security assessment solution for large-scale Windows NT/2000 networks, Active Directory, and Microsoft Exchange. The two products are integrated through a common reporting console that is used for consolidating and analyzing event log data and generating and distributing reports.

EVALUATING THE TECHNOLOGY

Before deploying Aelita's solution on the entire network, Bryant evaluated InTrust on 125 production servers for a period of nine months.

"The product was easy to set up and use and worked as advertised," said Bryant. "They had all the reports we needed and the user interface was intuitive enough that I didn't have to use the documentation to get started. We set it up one day and were viewing reports the next."

After a thorough evaluation in real-world conditions, Bryant extended the license for InTrust to 300 servers and added Enterprise Directory Reporter for directory management.

RESULTS

"The Aelita products are one of our main sources of security information and alerting," said Bryant. He receives a daily email from the system summarizing activity over the previous 24 hours. In addition, information for one of the company's divisions is extracted and used to create an HTML report that is automatically posted to the Web, where it is accessed and used by auditors.

> *"The Aelita products are one of our main sources of security information and alerting. They are an important part of our overall security infrastructure."*
>
> **David Bryant**
> *Senior Information Security Engineer*
> **Raymond James & Associates**

"We view the Aelita products as security tools first," Bryant said. "But the information being collected is also very useful outside of security. We plan on rolling out the Aelita Reporting Console to our operations and engineering group. Through the console they will be able to easily access Exchange statistics, server error logs, server crashes and the wealth of other data we are now able to consolidate, analyze and archive.

"Just having the system in place has made our network more secure as users are more conscious of their activities and our security policies because they know we are monitoring," Bryant concludes. "It gives us capabilities we didn't have and has become an important part of our overall security infrastructure."

SOLUTION

- InTrust™ (formerly EventAdmin)
  Consolidated Security Auditing and Monitoring for Windows-centric and Heterogeneous Networks
- Enterprise Directory Reporter™
  Security Auditing and Configuration for Windows NT/2000, Active Directory and Microsoft Exchange

AELITA SOFTWARE

800-263-0036 or
614-336-9223
sales@aelita.com
www.aelita.com

ælita™ SOFTWARE

FIGURE 5: Enabling Incoming Microsoft Exchange/Outlook

It's easy to drop legitimate emails with keyword rules. For instance, the rule in Figure 4 would drop not only malicious emails referencing the command prompt, but also legitimate emails that discuss the command prompt.

APPLYING ISA SERVER'S EXCHANGE RPC FILTER

Another important way you can protect access to Exchange is with ISA Server's Exchange RPC filter, which provides protection for Outlook to Exchange communication over untrusted networks — like the Internet — without a VPN. Normally, clients on the internal network communicate with Exchange via RPC and enjoy full functionality with Outlook. However, when the same user goes on the road he is often limited to OWA access or he must use a VPN to access the network and the Exchange server. This is because it's impossible to secure RPC traffic with a traditional layer 4 firewall. RPC uses the portmapper (TCP port 135) and various random high ports (TCP ports 1024 through 65535). Each RPC service has a different universally unique identifier (UUID). When an RPC service such as Exchange starts, it registers with Windows RPC portmapper. The portmapper assigns each RPC service a random high port and the service starts listening on that port. When a client such as Outlook needs to establish an RPC connection to a server such as Exchange, Outlook first connects to the portmapper and supplies the UUID of the RPC services it needs—in this case, those of Exchange. In this example, when an Outlook client connects via port 135 and supplies Exchange Server's UUID, the port mapper returns port 4000, 4001, and 4002. Next, the client reconnects over the newly learned port and starts communicating with the Exchange server. You can probably see why a layer 4 firewall would have trouble providing remote RPC access to Exchange but filter out other RPC traffic. You'd have to open 64513 ports out of a total of 65535!

However, with the RPC filter you can enable remote users to access the full functionality of Exchange via Outlook securely and transparently. ISA Server's RPC filter ensures that external clients make only valid Exchange remote procedure calls. The filter blocks other remote procedure calls such as domain controller related calls. The RPC filter dynamically opens ports on the ISA Server as "Outlook clients connect" and then forwards their remote procedure calls to the Exchange server. The RPC filter closes the ports as "Outlook clients disconnect." You can publish RPC access to your Exchange server and enable the Exchange logic in the RPC filter with the Mail Server Security Wizard introduced earlier. Simply check Incoming Microsoft Exchange/Outlook as shown in Figure 5. To encrypt RPC Internet traffic between your clients and the

FIGURE 6: Outlook 2002 Setting to Encrypt RPC Traffic

Exchange server, you'll need to configure your Outlook clients to encrypt connections to Exchange. The process for configuring this is different, depending on the Outlook client you use. Figure 6 shows the setting for Outlook 2002. ISA Server, with its new Feature Pack 1 add-on, allows an administrator to enforce the encryption of all Outlook-to-Exchange communication via the Exchange RPC filter. If an Outlook client tries to connect and isn't configured for RPC encryption, ISA Server will reject the connection. Because this is a client-level setting you could investigate using a group policy (Windows 2000 and Windows .NET Server 2003 domains) or system policy (Windows NT domains) to force all clients to use encryption.

You may find the following resources helpful when deploying this solution:

- Download new technical documentation and troubleshooting information for RPC, SMTP, POP, and IMAP Exchange Server publishing scenarios with ISA Server from http://www.microsoft.com/isaserver/featurepack1 (you can find the new content inside "docs.zip," available in the download section).

- Read "Configuring and Securing Microsoft Exchange 2000 Server and Clients with ISA Server," at http://www.microsoft.com/technet/prodtechnol/isa/deploy/isaexch.asp.

- Read "Deploying ISA Server" from the Microsoft Exchange 2000 Server Hosting Series, at http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/plan/ hostedexch/deploygd/aspd05xx.asp.

- Ensure that your clients can find your Exchange server via DNS, both while connected to your internal network and while on the Internet using the same DNS name used in Outlook's email account for the Exchange server by configuring a "split-brain" DNS environment. Details are at http://www.winnetmag.com/Articles/Index.cfm?ArticleID=21128&pg=2.

ISA Server Feature Pack 1 Delivers New Defenses for Exchange Server and IIS Installations

ISA Server Feature Pack 1 delivers enhanced security and ease of use beyond that of traditional firewalls for email server, Web server, and Exchange Outlook Web Access (OWA) deployments.

Providing external email complicates access and can compromise security. ISA Server Feature Pack 1 enhances email server security by improving the ability of ISA Server's SMTP filter to eliminate unwanted email messages. Feature Pack 1 also enhances the Exchange RPC filter, which provides protection for remote Outlook users accessing Exchange Server over untrusted networks without a VPN.

Hackers are bypassing traditional firewalls and more and more types of applications are using port 80. In response to this trend, URLScan for ISA Server offers protection from these types of Internet attacks to better secure Web and OWA servers. In addition, authentication is improved with support for RSA SecurID and basic authentication delegation to help restrict access to valid users.

Finally, many administrators find firewall configuration too complex. New wizards (including an OWA wizard), scenario walkthroughs, and technical documentation make configuration easier and answer the most commonly asked ISA Server questions.

Visit http://www.microsoft.com/isaserver/featurepack1 for more ISA Server Feature Pack 1 information or to download a copy.

PROTECTING IIS

Even if you publish your Exchange server to the Internet server via RPC, you still may need to maintain OWA access to Exchange. OWA is a powerful solution for traveling users who don't have a laptop or who can't reach your network via RPC or VPN (perhaps the company

business partner they are visiting has a very restrictive firewall for outgoing connections). In this scenario, protecting Exchange becomes a matter of protecting IIS because OWA runs on IIS.

ISA Server helps you protect IIS against Code Red and Nimda-style layer 7 attacks, because ISA Server inspects http and https at the application layer. To use ISA Server to protect Web servers (including OWA) on the internal network, you create a Web publishing rule that tells ISA Server to listen for http or https requests on its external interface, inspect them, and then send them to the destination server. To provide privacy for OWA traffic, you can configure your Web publishing rule to require SSL encryption between the external client and the ISA Server. SSL-protected Web sites require that the Web server present a certificate to the client proving that the Web server is authentic. You don't need to purchase a certificate for the internal network; you can deploy a Microsoft CA (it's free and included with Windows 2000). In this scenario, the Web server certificate resides on the ISA Server, not on the Web server. Once ISA Server receives an https request, it decrypts it, inspects it, and then resends the request to the internal Web server using http or https, depending on how you configure the Web publishing rule.

GOING BEYOND TRADITIONAL FIREWALLS

As you can see, ISA Server provides protection that a traditional firewall can't. With a traditional layer 4 firewall, SSL connections tunnel straight through the firewall to the Web server, possibly carrying layer 7 attacks including viruses and worms. At the ISA Server, you can implement strict controls on http and https content using URLScan for ISA Server, which is new in ISA Server Feature Pack 1. URLScan is an add-on filter for ISA Server that intercepts every request from the Internet that is destined for an internal Web server and scans each request for anything unusual. As the URLScan documentation notes, "Most attacks share a common characteristic — they involve the use of a request that's unusual in some way. For instance, the request might be extremely long, request an unusual action, be encoded using an alternate character set, or include character sequences that are rarely seen in legitimate requests."

ISA Server helps you protect IIS against Code Red and Nimda-style layer 7 attacks, because ISA Server inspects http and https at the application layer.

URLScan for ISA Server's task is to detect such anomalies in http and https requests. When URLScan detects something unusual, the tool prevents the request from being processed. Because of this approach, URLScan can help protect your server against future exploits that may follow known patterns — for example, in most buffer-overflow attacks, attackers form a URL that contains many nonfunctioning characters and some binary code that the computer executes. By rejecting unusually long requests and requests with high-bit characters (i.e., characters greater than 127), both of which are useful indicators of buffer-overflow attempts. URLScan prevents the buffer overflow from reaching the faulty region of IIS code. For further http and https protection, you can choose from ISA Server partner products such as Symantec's AntiVirus for ISA Server or intrusion detection plug-ins such as ISS's RealSecure for ISA Server.

Deep content inspection is a requirement for network security today. You can no longer trust ports and protocols to indicate user intent, which means the only way to know exactly what kind of traffic is traversing your firewall is to inspect it at the application layer. With a firewall such as ISA Server, you can help stop application-level attacks before they enter the internal network. The recent release of ISA Server Feature Pack 1 brings with it further enhancements for protecting Exchange, OWA, and IIS servers (see "ISA Server Feature Pack 1 Delivers New Defenses for Exchange Server and IIS Installations"). In addition to providing deep, layer 7 inspection out of the box, ISA Server boasts a wide array of partner plug-ins that let you add more best-of-breed enhancements where you need them. ◆

Sentian Keeps Central Power Systems' Employees Running Smoothly on the Internet

Central Power Systems, a privately held company, distributes air-cooled gasoline engines and parts for outdoor power equipment through a network of 4,000 registered service dealers in Ohio, Michigan, Indiana, West Virginia, Kentucky, Florida, and the Bahamas.

Employee access to the Internet can pose expensive productivity and liability issues for any company. A survey by Vault.com found that employers are incurring serious productivity hits from unmanaged Internet access: a whopping 25 percent of employees admitted to spending one hour or more per day surfing websites not related to work, and 22 percent said they spent 30 minutes to an hour a day. Workers can also expose their companies to legal liabilities, for example by viewing pornographic or racist Web sites, which can lead to costly lawsuits.

> *"I'd give Sentian a 10 out of 10, and I've already recommended it to others,"*
>
> **Ryan McAlister**
> *IT Manager*
> **Central Power Systems**

Central Power Systems' (CPS) management team brought these concerns to IT Manager Ryan McAlister. CPS wanted to ensure that company policies for appropriate Internet use would be enforced, and looked to McAlister to select a technology solution that would assist in that effort.

THE SOLUTION

After researching several options for enterprise-level protection, McAlister turned to N2H2. The quality of N2H2's filtering database-which had recently been rated number 1 in a major independent comparison of the leading filtering products impressed McAlister so much that he downloaded a copy of N2H2's Sentian for the Microsoft Internet Security and Acceleration (ISA) Server 2000.

Sentian's smooth design and powerful features reinforced McAlister's initial impressions. "Sentian was an easy integration with ISA. It was also really easy to use, and very manageable," said McAlister. "With Sentian I can easily set up groups with different levels of Internet access and generate custom reports."

> *"Sentian was an easy integration with ISA. It was also really easy to use, and very manageable. With Sentian I can easily set up groups with different levels of Internet access and generate custom reports."*
>
> **Ryan McAlister**
> *IT Manager*
> **Central Power Systems**

Central Power Systems has found Sentian does its job of keeping employees away from inappropriate sites in the workplace. "Users avoid visiting because they know they are being filtered; it is an effective reinforcer of company policy," said McAlister. An industry-best filtering database, a smooth integration with Microsoft ISA, flexible and easy-to-read reporting, and powerful management features through a simple interface all made Sentian a natural choice for Central Power Systems. "I'd give Sentian a 10 out of 10, and I've already recommended it to others," said McAlister.

N2H2

877-336-2999
www.n2h2.com

N2H2™
INTERNET CONTENT FILTERING

Windows Platform Secures Olympics Sites, Ensuring Revenues, Attracting Customers

MSNBC, a joint venture of NBC and Microsoft, produces MSNBC-TV, a 24-hour cable news network, and MSNBC.com, a comprehensive multimedia news and information service on the World Wide Web. MSNBC.com serves an average of 25 to 30 million page views to 4 to 5 million users daily, handling up to 35,000 simultaneous users. MSNBC.com has been rated the number one general news site by Media Metrix.

Time was short when the Salt Lake Organizing Committee — responsible for producing the 2002 Winter Olympic Games — met with MSNBC.com officials to discuss MSNBC.com's hosting of the two official Web sites for the games. It was June 2001, and there were just seven months until the Olympic torch would be lit and the site would have to go live. Key among the challenges facing MSNBC.com — which had to produce sites scalable and reliable enough to handle hundreds of millions of page views — was the challenge of security.

Previous Olympics sites, which had been hosted on UNIX and IBM platforms, had been attacked, and most had been brought down at some point. Despite the short timeline, MSNBC.com would have to devise a security plan equal to the extraordinary challenge posed by hack attacks, denial of service attacks, virus attacks, and others. A significant security breach could allow a hacker to crash the sites, costing tens of millions of dollars in lost advertising revenue and inflicting long-lasting harm to MSNBC.com's reputation and revenues.

To complicate matters, MSNBC.com's existing security environment consisted of a series of ad hoc third-party programs — including virus protection, intrusion detection, and a proxy/firewall client — that were not integrated with one another or with the operating system. That made it impossible to get the security components to work together or for the administrators to gain a comprehensive view of MSNBC.com's security situation.

Especially for Web sites with the unmatched visibility of Olympics.com and NBCOlympics.com, those gaps would be unacceptable.

"With the Olympics, we would be a bigger target for hackers than we'd ever been before," says Michael Corrigan, Director of Technology for MSNBC.com. "So, we needed the most comprehensive security environment we'd ever had — and we had to assemble it on an incredibly tight timeline and budget."

THE SOLUTION

To meet its various goals for a highly effective security environment that would be relatively quick and easy to deploy and maintain, MSNBC.com chose an implementation (Figure 1) based on the Microsoft Windows platform, including the Microsoft Windows 2000 Server family with the Active Directory service and Internet Information Services (IIS) 5.0, Group Policies, Microsoft Windows XP Professional with the Internet Connection Firewall (ICF) enabled on the desktop and Microsoft Internet Security and Acceleration (ISA) Server 2000 at the network edge. The solution also included Internet Security System (ISS) Black Ice on the Internet-facing desktops, Cisco routers on the Web farm and Cisco firewalls between the MSNBC.com sites and NBC's cable and television networks.

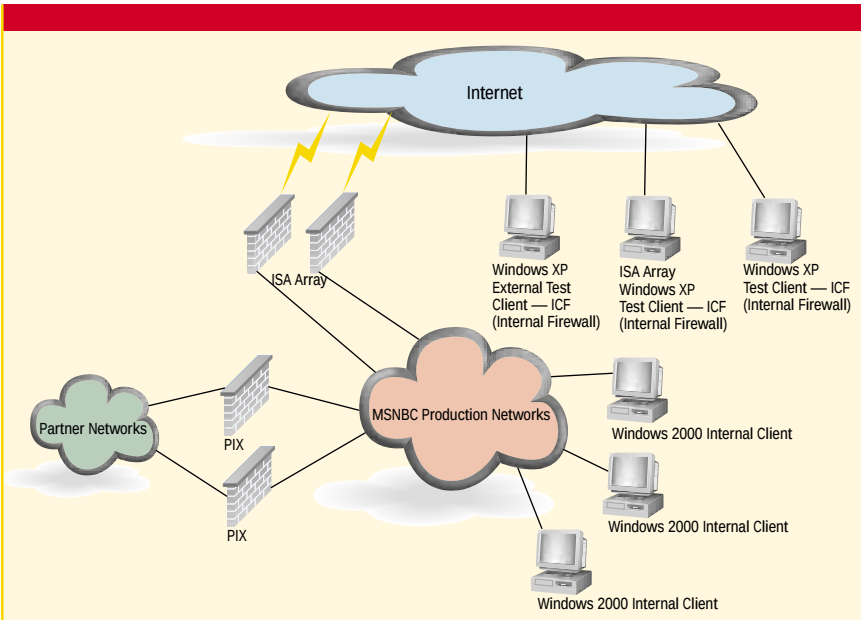


Figure 1 - The MSNBC.com solution

> *"We wanted to make it as hard as possible for attackers to hack us by placing a number of layers of security in their path."*
>
> **Dick Cullom**
> *Operations/Security Manager*

MSNBC.com knew that the Internet media industry would be watching closely to see how well the Microsoft technology held up to the high demands of the Olympics. MSNBC.com had Microsoft-certified technicians ensure that security concepts were implemented. In addition, it brought in outside consultants from Foundstone to check the security. The consultants confirmed that the systems were configured for maximum security and helped to put in place practices to help address inevitable future attacks.

"We wanted to make it as hard as possible for attackers to hack us by placing a number of layers of security in their path, knowing that no single layer would stop all the threats," says Dick Cullom, Operations/Security manager. "The Windows platform gave us a range of features, integrated into the operating system or associated with it, to facilitate the products' working well together."

Windows 2000 Server with Active Directory for "the Biggest Bang for the Buck"

A key layer in MSNBC.com's approach was upgrading all production servers to the Windows 2000 Server family (including Windows 2000 Advanced Server or Windows 2000 Datacenter Server, where appropriate) with Active Directory. That enabled MSNBC.com to employ Group Policies defining who could access the systems and under what conditions. For example, user-based Group Policies enforced the use of screen savers with passwords and complex (strong) passwords on both the server and the desktop.

"Group Policies made it easy to lock down security by automatically enforcing those policies on anyone logging on to our domain," says Corrigan. "We could ensure that no one could change content on the site other than our authorized editors. We migrated to Active Directory shortly before the Olympics, and this gave us the biggest bang for our buck. We had no problems at all with our Active Directory implementation, and it enabled us to standardize policies across the division, which we couldn't have done otherwise. What was an automated process would have been a full-time job for us in the past."

The Web servers also were divided into two data centers to increase bandwidth and provide redundant hosting. Hardware load-balancing was installed in part to offer security against denial-of-service attacks — which try to overwhelm servers by generating heavy traffic — and to allow other servers to compensate if a server went down. As additional measures to keep the sites active, MSNBC.com also set up redundant Web site, application, and database servers powered by Microsoft SQL Server 2000 and IIS 5.0, the Web server built into Windows 2000 Server.

ISA Server, Windows XP ICF Provide Complete Firewall Protection — and More

For production servers directly facing the Internet, MSNBC.com's firewall of choice was ISA Server. Corrigan says it was more flexible and better suited than were alternatives, because it included Web proxy, caching, and easy reporting functions, as well as enabled the use of Active Directory-based user accounts and Group Policies to control access through the firewall.

Because Active Directory enabled MSNBC to deploy a single configuration to all ISA Server computers in the installation using ISA Server enterprise policy, it was very difficult for Corrigan's team to make a configuration error. They could be confident that they had consistent security in all of their remote locations. The integrated event alerts feature in ISA Server was "a big plus" for detecting attacks, according to Corrigan, because the team always kept completely up-to-date on the status of servers in Redmond, Washington; Secaucus and Fort Lee, New Jersey; Salt Lake City, Utah; Washington, D.C.; London; and elsewhere. To meet NBC's corporate requirements, Cisco firewalls were used in the private links between NBC and MSNBC.com, providing yet another layer in the multi-faceted approach to security.

Servers weren't the only machines that MSNBC.com had connecting directly to the Internet. At least a dozen desktop PCs provided crucial monitoring capabilities that could not be implemented through the server firewall. Those machines were rebuilt to run Windows XP Professional with ICF — its built-in firewall — enabled and ISS Black Ice added for intrusion detection.

"Microsoft's putting firewall software into the operating system in Windows XP was another great move in helping to make computing more secure for the end user and easier for the administrator," says Corrigan. "In addition to making us more secure, the Windows XP Internet Connection Firewall gave us a single, consistent way to put security into effect on all of these machines. It was very simple and completely effective in blocking hacks."

Security Roll-up Package Facilitates Up-to-Date Implementation

MSNBC.com also implemented the security roll-up package that Microsoft released during the period leading up to the Olympics.

"The security roll-up package was the single best thing added to the mix of the secure platform," says Corrigan. "It made it easy to manage what would otherwise have been the time-consuming task of rebooting each machine multiple times, for each security upgrade. We trusted that Microsoft had tested the roll-up package and that it would work properly on our servers — and it did."

THE BENEFITS

Flawless Security Keep the Olympics Sites Up and Running

MSNBC.com sites running Microsoft technologies successfully repelled every attempted attack without any disruption of service. The largest single denial-of-service attack consisted of more than 200,000 automated requests coming during a peak usage period measuring 780,000 connections. In all, the sites endured eight attacks over the 17 days of the Olympics, including denial-of-service attacks, voting application attacks, e-mail viruses and syn attacks, while maintaining an Internet availability of 99.8 percent.

Cost-Effective Technologies Lower Cost-to-Manage While Speeding Time-to-Market

MSNBC.com not only met its goal of delivering service uninterrupted by security breaches, but also met the tight seven-month schedule and reduced the cost-to-manage.

"My biggest concern going into the Olympics was that we had too much to do and not enough time in which to do it, and that last-minute changes would snowball into real problems," says Corrigan. "But with the way the components of the Microsoft platform products automated so much of the setup and monitoring and worked so well together, we really had time to breathe-and to put additional security measures in place that we might have glossed over if we'd had to rush at the last minute."

For example, Corrigan notes that without the roll-up security updates, the time spent on coordinating multiple updates on nearly 100 internal servers and more than 60 Web servers would have made securing the environment "an almost impossible task." He also points to two help-desk people stationed at the Olympics to resolve on-site issues; those staffers wouldn't have been available if they had been required to service more labor-intensive technology in the back office. In all, Corrigan estimates that the Microsoft environment enabled MSNBC.com to save or redeploy about $125,000 in labor for the three months leading up to and culminating in the Olympics.

> *"In addition to making us more secure, the Windows XP Internet Connection Firewall gave us a single, consistent way to put security into effect on all of these machines."*
>
> **Michael Corrigan**
> *Director of Technology*
> **MSNBC.com**

MSNBC.com's "Secure Reputation" Boosts Revenues, Attracts Customers

"Far more important than the TCO savings was maintaining our reputation," says Corrigan. "If the sites had gone down or otherwise been corrupted, it would have been a debacle for us. Between emergency efforts to correct the problem and the lost revenues from advertisers, a security breach could easily have cost tens of millions of dollars. Thanks to the Microsoft platform, we avoided those costs and now we stand to generate significant new business because of our ability to run the Olympics sites securely."

Beyond avoiding the loss of millions of dollars, MSNBC.com stands to make millions of dollars from new, high-end customers that noticed the success of the Olympics sites and have invited the company to submit proposals for similar efforts. ◆

Windows Offers a Wide Range of VPN Options

Before Shopping for VPN Products, Be Aware of What You Can Get For Free

By Randy Franklin Smith

The term Virtual Private Network (VPN) applies to a complex array of technologies and business-need scenarios. Security, interoperability, ease of use, and administration are major considerations when selecting and deploying VPN technology. But before shopping for VPN products, you should be familiar with what you can get for free. The Windows platform offers a wide selection of VPN options that come either free with each Windows OS or that you can download from Microsoft's Web site (Figure 1 lists components that provide VPN capabilities for the Windows family).

Although the best things in life might be free, it's also nice when they integrate and slip into place smoothly with the rest of your Windows environment. This article will examine Windows VPN technology as it relates to the tangle of protocols available (PPTP, L2TP/IPSec, IPSec tunnel), the different Windows OSs (95, 98, ME, NT, Windows 2000, Windows XP, Windows .NET Server 2003), VPN business scenarios (remote access, site-to-site, extranet), authentication, VPN server security, and interoperability with non-Microsoft VPN products. I will examine each type of VPN, discuss what you can and can't do with Microsoft products, and share some secrets along the way. Unless I state otherwise, when I refer to a VPN server I mean a Windows 2000 (Win2K) or Windows .Net Server 2003 (Win.Net) computer with RRAS loaded and connected to the Internet with no firewall in between (although ISA Server and RRAS can coexist peacefully on the same computer). If you deploy your RRAS VPN server behind a firewall, the only VPN protocol that can be routed through the firewall is PPTP.

VPN BUSINESS SCENARIOS

When you consider technology solutions, you should always start with the business requirement you're trying to fulfill; so I'll start by discussing the three major VPN business scenarios. Although you might be familiar with these scenarios, you should note the technical issues I raise. These issues greatly affect your options and can create challenges when you implement a particular solution.

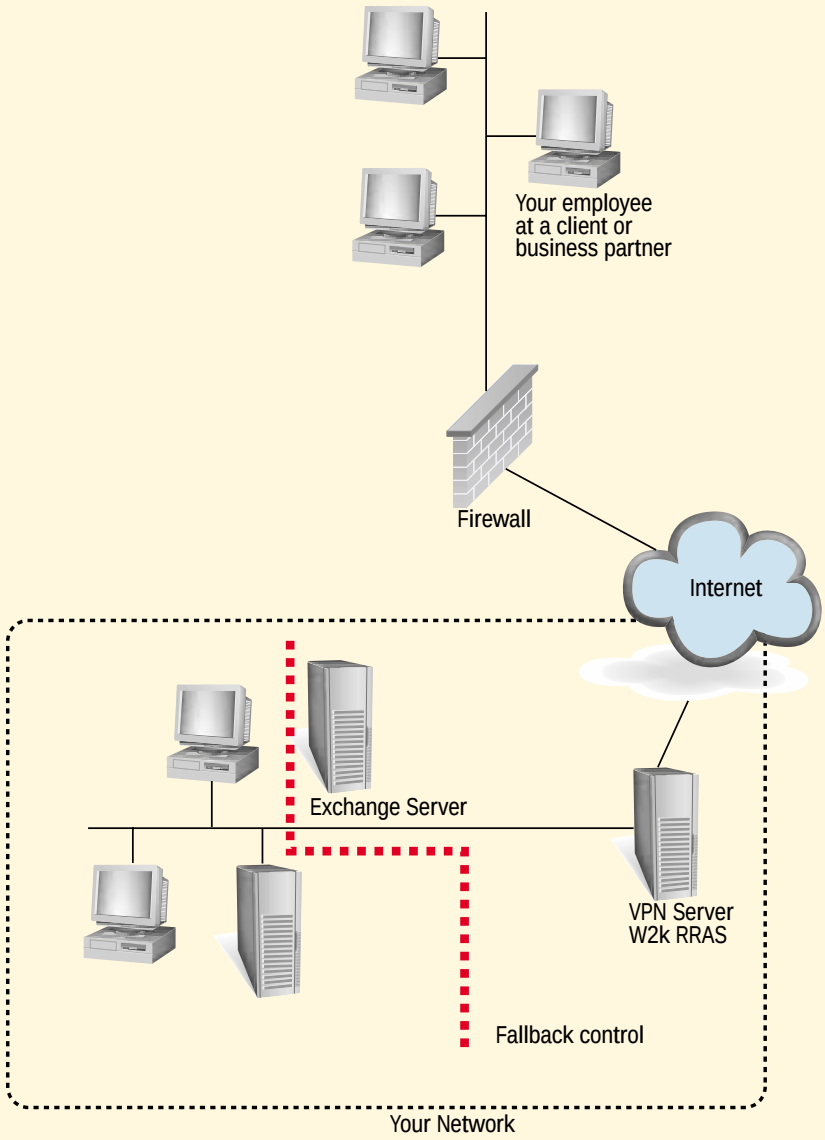
Remote Access VPN

First, most businesses need to provide remote access to employees on the road or working remotely (e.g., from a home office or remote consultants or other type of business partner). For remote access, you should consider technology on the client workstation, parties in the middle between the client and your VPN server, your VPN server, and your relationship with the remote user. The remote user might be an employee or a less trusted individual (e.g., a consultant or business partner). Usually, the client workstation will be running a Windows OS, but it might be a Macintosh or Unix workstation. Pre-Win2k OSs and non-Microsoft workstations impose a few limitations on the

FIGURE 1: Windows VPN Components

VPN server OS	NT, W2k, .NET
VPN client OS	W98, WME, NT, W2k, XP
VPN client to allow down-level client OSs to use L2TP/IPSEC	Microsoft L2TP/IPSec VPN Client
VPN server component	RRAS
RADIUS component	IAS
User account store	NT domain SAM, Active Directory
Automatic deployment of certificates for IPSEC related VPNS	Certificate Services, Active Directory, Group Policy

FIGURE 2: Remote Access from a Client



type of VPN protocols and authentication you can use. As you'll see shortly, for pre-Win2K OSs you can eliminate some of these limitations with a new download available from Microsoft.

Next, consider the parties between your remote user and your network. A user on the road might dial in to a local ISP POP and then use a VPN to access your network, he might use a Wayport connection at his hotel, or he might use some other fast access provider. Usually, neither of these scenarios affects your options, because mainstream ISPs seldom block any of the protocols at your disposal. But what if your remote user is an employee visiting one of your company's clients or suppliers and he wants to plug into their network, use a VPN through their firewall and across the Internet, and then access your network (Figure 2). You might run into a problem, depending on how strictly that company's firewall limits outgoing connections. (If you encounter this problem, you might check into http-tunnel solutions like the ones at www.http-tunnel.com, which let you tunnel out of a network to the Internet through http tcp port 80 and then establish your VPN through that http tunnel.)

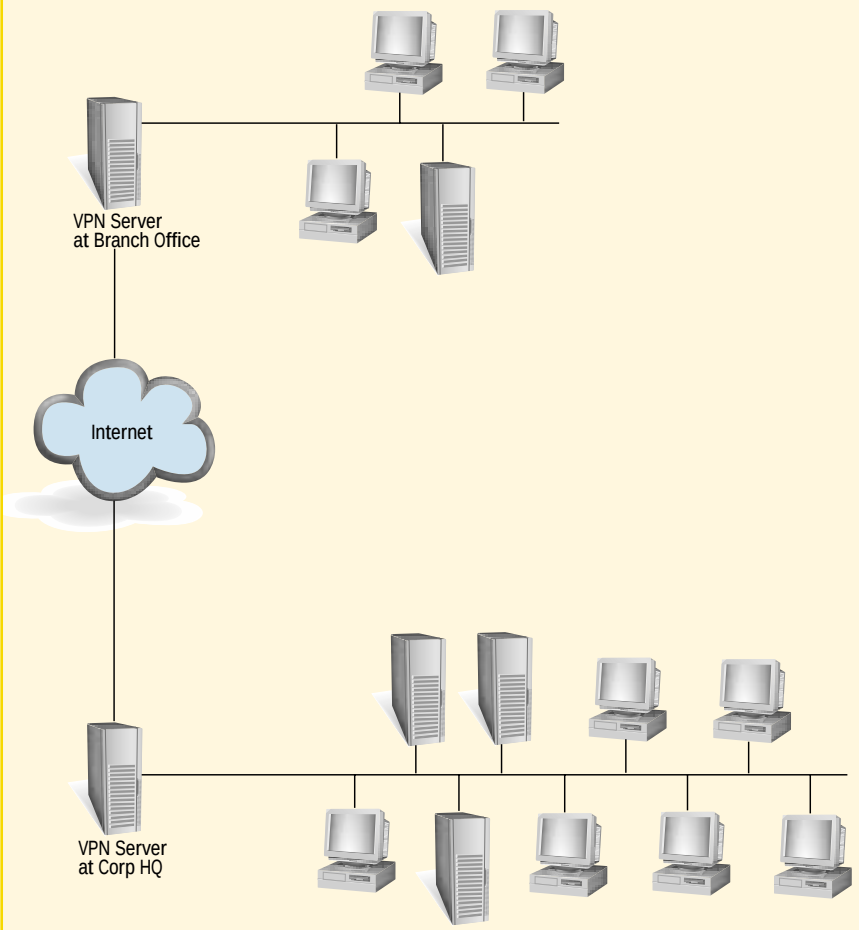
The same problem can arise with non-employees (e.g., a consultant whose workstation is behind another organization's firewall). Additionally, because this type of remote user is typically less trusted than an employee, you need to think about how much access he should be allowed once he successfully uses a VPN to access your network For example, if he's an Oracle consultant, should he be allowed to send packets to other computers on your network? A similar issue arises for all remote users, including trusted employees who dial in to your network. Depending on the protocol in use and the Windows OS installed on the client and VPN server, you might base authentication on traditional passwords, user certificates, tokens, or biometrics. If you use traditional password-based authentication, the possibility exists that Joe who just accessed your network via a VPN is actually an attacker who guessed Joe's password. To limit the risk of compromised remote user accounts, some companies limit remote employee access to the network via a VPN only to servers commonly needed by remote employees (e.g., Exchange servers and file servers) but prevent packets originating from the VPN reaching other areas of the network. That way you protect the greater portion of your network from attackers who gain entry via remote access. Of course, if an attacker

succeeds in compromising a server that you allow remote users to access, he might be able to stage further attacks from the server into otherwise inaccessible areas of your network — but that requires him to penetrate yet another layer of your defense-in-depth.

I use the term "fallback controls" to describe the idea of limiting remote user access to specific areas of your intranet. You can implement fallback controls in a variety of ways: on the VPN server, on routers, or on workstations and servers throughout the domain by using IP Security Policy filters deployed via Group Policy. The easiest and most flexible way is to create the fallback on your VPN server by using a remote access policy (RAP). With RAPs, you can perform IP packet filters based on the remote user and his group memberships. Router and IP Security Policy fallbacks are much less granular because the criteria for determining a prohibited packet is solely whether it's source address is part of the VPN client address range. If you have different types of users coming in through the same VPN server, you can't impose different rules for each user with fallbacks defined at the Router or with IP Security Policies. You can implement user- and group-specific fallback controls on a VPN server by creating a local or domain group named something like Oracle Consultants and adding the appropriate user accounts. Then, using the Routing and Remote Access MMC, you can add a remote access policy, link it to the Oracle Consultants group, and add an IP filter to the policy that limits traffic from the remote client to packets destination addressed to your Oracle server.

How to create such an RAP is explained in greater detail in the help text for Routing and Remote Access under "Apply packet filters for business partner extranet." You can define RAPs only on Win2K and Win.NET servers running RRAS. If your VPN server is running Windows NT, you'll need to use router or IP Security Policy fallbacks. Remember that remote access VPN clients need an IP address valid on the internal network. If you use either of these two fallbacks, make sure that your VPN server doles out IP addresses to remote clients from a reserved range of addresses, instead of leasing from a DHCP server. If remote clients use addresses within a range outside your DHCP address pools, you can identify and block those packets from reaching sensitive or unnecessary areas of your internal network (intranet). One other consideration with remote access VPNs is the security of the client computer. An insecure client computer can expose your entire internal network to attack. VPN clients may not have intrusion detection or virus scanning installed, or the OS or AV may not be current with security patches and signatures. These holes may allow attackers on the Internet who compromise the client to then invade your network through the VPN tunnel. These problems might occur on poorly maintained company computers, but many telecom-

FIGURE 3: Example Site-to-Site VPN



muters use a VPN to access networks from their personally owned computers, which are even less likely to be secure. New features in Win.NET's VPN functionality address these risks (see the sidebar, "Looking to the Future").

Site-to-Site VPN

Site-to-site VPNs (Figure 3) connect the internal networks of two or more sites within the same organization to one Wide Area Network using VPN links over the Internet instead of expensive dedicated lines. Usually, site-to-site VPNs are easier to deploy than extranet VPNs. With site-to-site VPNs, all you need is a Win2K server at each site connected to the site's local network and to the Internet. This scenario doesn't involve user authentication, but it does require VPN server-to-VPN server authentication. When establishing the VPN connection, one of the VPN servers assumes the role of client and initiates a connection with the other VPN server. After establishing the VPN connection, users on either site can connect to servers at the other site as though they were on the same LAN. How do the VPN servers know each other is authentic and not an impostor? Depending on the protocol and Windows OS installed on the VPN servers, you can base site-to-site VPN authentication on passwords associated with user accounts created for each server, on pre-shared secret keys defined in each server's registry, or on machine certificates issued by a certificate authority (CA).

Extranet VPN

Extranet VPNs let you connect your organization's network to one or more business partners' networks to facilitate extended supply chain needs or B2B-related traffic (Figure 4). This scenario is similar to site-to-site VPNs, but with a few important differences. First, the trust level is different. Although you might expect a branch office to have fully routed packet access to your headquarter's internal LAN, you shouldn't let computers in your business partner's network send packets anywhere on your network. Usually, business partners need access to only a small number of servers on your network and they should be limited to those computers by using a fallback control as discussed earlier in this article. The reason for limiting partner access within your network goes far beyond the fact that you trust business partners less than your employees. What if, due to lax security practices by your business partner, a destructive worm or DOS succeeds in spreading

Looking to the Future

With Windows .NET Server 2003 (Win.NET) VPN servers you'll be able to support L2TP/IPSec VPNs that cross NAT boundaries. This capability will let you migrate away from PPTP for your employees that must use a VPN from within another organization to access your network. Win.NET will expose more configurable IPSec parameters than ever, letting you interoperate with more IPSec implementations from other companies. Win.NET includes VPN wizards to simplify the setup of remote access, site-to-site, and extranet VPNs. And an especially exciting new feature is Win.NET's quarantine technology, which will help you address the risks involved with insecure client VPN computers.

Quarantine technology can prevent VPN clients from connecting unless an approved and up-to-date virus scanner is installed and the client itself is up-to-date and patched. You also get options for protecting against split-tunneling risks where a remote user browses the Internet and accesses your internal network at the same time. Win.NET implements quarantine technology on the client through the Connection Manager Administration Kit (CMAK). CMAK lets you compile an executable that you then distribute to VPN clients. The CMAK executable installs the appropriate VPN client software and configures the VPN connection, which greatly simplifies VPN client setup for administrators and users alike. More importantly, CMAK installs an engine that runs scripts executed on the client computer at crucial moments during the VPN connection process. These scripts implement the security checks described above. At the time of writing no support is available for deploying CMAK executables through software installation policies "in group" policy. However, you can still distribute the CMAK executable through tools like SMS.

NetIQ's AppManager Keeps e-government Managed and Secure

British Prime Minister Tony Blair has a goal: Achieve 100 percent electronic delivery of public sector services within the next four years.

The hub for these services is the government's recently launched Gateway web site, a flagship project setting a standard for e-government in Europe. Through its premier partnership status with Microsoft, NetIQ's applications management and security products are ensuring that Gateway achieves optimum availability, performance and recoverability.

ESTABLISHING E-GOVERNMENT

As the registration point for UK citizens who want to sign up for e-government services, Gateway provides the necessary routing and connecting services to all government departments and complements their individual web sites. The site also furnishes the security and authentication measures needed to enable the various parts of government to conduct secure transactions with citizens.

Initially, three government departments began offering online services through Gateway: the Inland Revenue, Customs and Excise and the Ministry for Agriculture, Fisheries and Foods. The first online services included the self-assessment of tax and the ability to file tax returns electronically.

FACING THE PROJECT CHALLENGES

Microsoft Consulting Services was entrusted with providing the software and managing the rollout of the applications, while Cable & Wireless was selected to host Gateway from its center in Swindon. The contract presented major challenges for Microsoft. The three government departments all used different technologies and had outsourced their management to different service providers. Each department also wanted to offer a unique e-service. Moreover, Microsoft was given a target of servicing 100 transactions per second from the start.

Clearly, systems management was a major issue. Government officials felt that any online representation of its services should be seen as seamless and operating smoothly at all times. Gateway had to be available 24x7 and protected by the best of security systems. Public confidence in the system's availability, reliability, performance and security was key.

An additional security worry was that the government's web sites are a natural target for hackers. With the need to interact with the likes of Customs & Excise online, deploying Public Key Infrastructure (PKI) level security to protect citizens' personal data was essential.

DELIVERING THE MANAGEMENT EXPERTISE

The need for state-of-the-art application management and security systems to deliver the high levels of performance and protection demanded by the Cabinet Office was clear. Done manually, the task would take a team of about 40 engineers. So, automated solutions were the answer. At this point, Microsoft engaged the help of its strategic partner in systems management, NetIQ.

"Only NetIQ's products could meet the demanding systems management requirements of the Gateway project."

Mark Jacklin
Microsoft Systems Management Consultant

After close collaboration with Microsoft on how to meet the tight 15-week deadline to create comprehensive end-to-end systems management architecture for Gateway, NetIQ deployed its AppManager Suite (AppManager) along with its Security Manager product. With its Active Threat Management solution, Security Manager combines the power of host-based intrusion detection with vulnerability assessment. Security Manager was chosen as an all-embracing, one-stop solution in a centralized console, rather than security products from various suppliers.

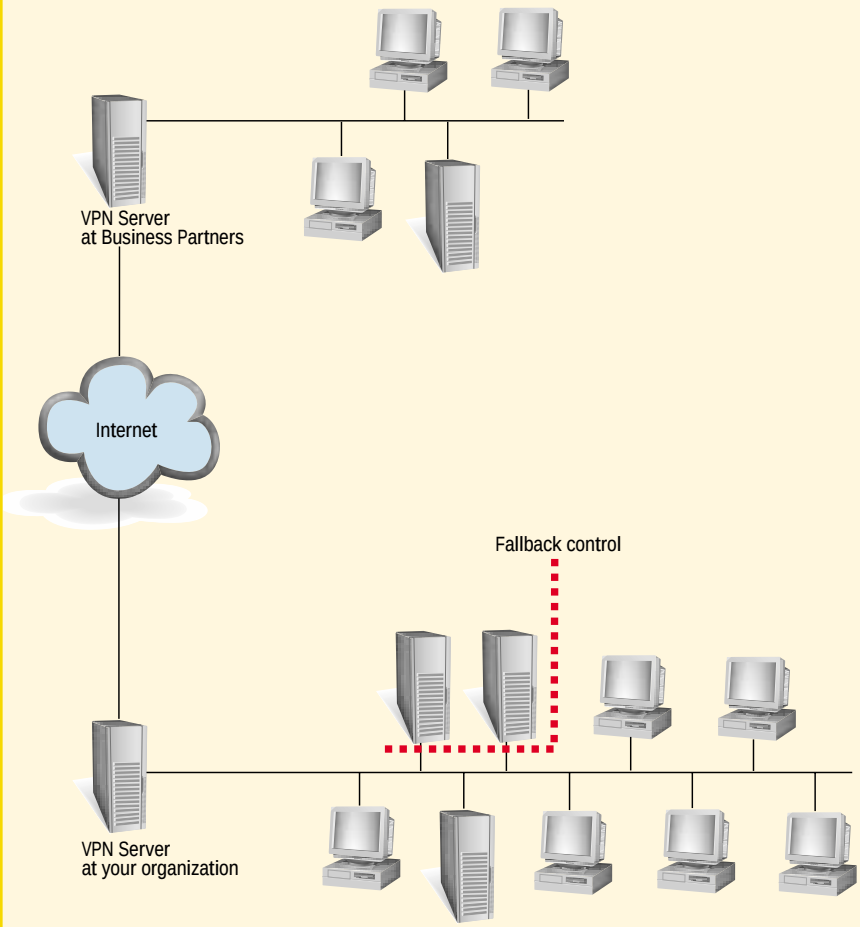
Mark Jacklin, Microsoft's systems management consultant on the project, said, "We were very pleased with the implementation of the NetIQ products. They were out of the box and monitoring the network very quickly, leaving us to complete the rest of the project's architecture with confidence. Only NetIQ's products could meet the demanding systems management requirements of the Gateway project, and so far they've done us proud."

Nearly six months after going live, AppManager and Security Manager continue to police approximately 60 servers hosting Gateway, which attracts hundreds of thousands of visitors every month. The systems do the mundane monitoring and troubleshooting, solving problems quickly, and proactively alerting the handful of IT staff on call to more serious issues as they brew.

NetIQ CORPORATION
713-548-1700 or 888-323-6768
info@netiq.com
www.netiq.com

through your business partner's network? Fallback controls will greatly slow or even prevent the malware from jumping over the VPN into your network. In fact, malware is also an issue in site-to-site VPNs because sites within the same organization often have different security standards and practices. Another important difference between site-to-site VPNs and extranet VPNs concerns interoperability. Most likely, your business partner uses a different VPN solution. Will it integrate with your Windows VPN server? Interoperability concerns may limit which protocols and authentication you can use and can often involve more troubleshooting than site-to-site VPNs.

FIGURE 4: Example Extranet VPN



VPN PROTOCOLS

Now let's look at each VPN protocol, discuss how it relates to authentication options, different Windows OSs, and interoperability. Each of the above scenarios supports one or more VPN protocols comprising PPTP, L2TP/IPSec, and IPSec tunnel. While the protocol and encryption algorithms supported by each protocol receive much attention, the choice of protocol is far less relevant to securing a VPN than the type of authentication you use. After all, the possibility of an attacker compromising a user name and password because someone stole or guessed a password, or an administrator failed to secure user accounts with strong password and lockout policies or failed to implement sound account management controls is more likely than an attacker using great technical skill to break the VPN protocol or its encryption. IPSec and L2TP are strong industry-standard protocols, but they support several different authentication options that differ greatly in level of risk. Even PPTP, having been bandaged to address vulnerabilities discovered by CounterPane Systems in 1998, is far from trivial to break and sufficient for typical corporate VPN requirements, as long as you implement strong passwords. The VPN protocol you use is far more important to the type of authentication you need, the Windows OSs you must support, and your interoperability requirements.

PPTP Protocal

PPTP, Microsoft's first VPN protocol, is supported by all versions of Windows, starting with Windows 95 (Win95). If you use PPTP with any NT or Win95 systems, make sure NT is current with Service Pack 4 or beyond and make sure you've loaded the lastest version of Dial Up Networking (version 1.3) on your Win95 systems. However, PPTP in Win95 supports only password-based authentication. An attacker can gain entry to your PPTP VPN from any computer on the Internet, if he comes up with the right user name and password. A much better way is to use the PPTP technology in Windows 2000, which includes support for EAP. By using EAP, you can get rid of passwords and replace them with smartcards, certificates, and even biometrics devices for your VPN authentication needs. These

FIGURE 5: VPN Clients

Client	Capabilities
W2k, XP	PPTP, L2TP/IPSec with EAS, IPSec tunnel
NT, W9x	PPTP L2TP/IPSec including EAP support (after loading new VPN client)
Mac OS X 10.2 Jaguar	PPTP
Linux	PPTP clients available. http://pptpclient.sourceforge.net/

new technologies are much harder to fake or steal than just a username and password. If your clients will sometimes be using a VPN to access your network from behind another company's firewall, that firewall must allow outgoing connections to PPTP. PPTP uses TCP port 1723 for the control channel and IP Protocol ID 47 for the data channel. The same issue applies in the unlikely case that your VPN server is behind your firewall.

L2TP/IPSec Protocol

For security, L2TP/IPSec is a great step forward from PPTP. L2TP, derived from PPTP and Cisco's Layer 2 Forwarding (L2F) tunneling protocol, provides the same advantages of PPTP in that it can carry multiple protocols and traverse firewalls that perform network address translation (NAT). Like PPTP, L2TP employs user authentication and would be exposed to some of the same man-in-the-middle attacks as PPTP. That's where the IPSec side of L2TP/IPSec comes in. Before making an L2TP connection, Windows (and other supporting OSs) initiates an IPSec connection. As explained in more detail below, IPSec performs computer-level authentication and then integrity checks each packet received and encrypts each packet sent. Thus, IPSec provides mutual machine-to-machine authentication, prevents man-in-the middle attacks, and provides encryption for the tunnel. IPSec also gives your L2TP/IPSec VPN much stronger encryption than PPTP; not so much in terms of encryption algorithm and key length, which is configurable, but more in terms of encryption implementation such as session key negotiation and lifetime. A strong encryption algorithm is part of the equation, but also important is how the two computers securely exchange the keys they will use. And you don't want to use a key too long or encrypt too much data because both situations improve the odds that someone will break your key. Both L2TP/IPSec and IPSec tunnel address these issues much better than PPTP.

After setting up the IPSec connection, Windows sets up the L2TP connection through the already established IPSec connection. User-level authentication occurs at the L2TP level. IPSec provides further protection by defeating dictionary attacks against the password used for the user authentication within L2TP. The encrypted tunnel is already set up by IPSec before user authentication takes place. Therefore, an attacker would have to break the IPSec encryption before tackling the password. L2TP also makes it possible to carry other traffic through your VPN tunnel (e.g., IPX traffic, which is important because, by itself, IPSec can carry only IP packets). If you could dissect an L2TP/IPSec packet, the outermost packet would be an IP packet with protocol 51 (IPSec ESP mode). Inside that packet, you'd find packet headers relating to L2TP. And inside those headers you'd find the actual packet sent by some application on the workstation.

Together L2TP/IPSec gives you both user-level and computer-level authentication. You can base the computer authentication on certificates or on a pre-shared key. Using L2TP/IPSec with pre-shared key machine authentication means an attacker would need to steal not only your user name and password, but also the pre-shared key stored on the user's workstation. Better yet, using certificates, the attacker would need to steal or gain physical access to the user's computer or succeed in obtaining a machine certificate from your CA under false pretenses, in addition to getting the user name and password. By default, Win2K and above support L2TP/IPSec, but you can download the Microsoft L2TP/IPSec VPN Client (http://www.microsoft com /windows2000/server/evaluation /news/bulletins/l2tpclient.asp) and install it on NT or W98-ME clients and get the same advantages. A Microsoft contact told me that although the new VPN client isn't officially supported on

Win95, people have used it successfully. Check out the "Administrator's Guide to Microsoft L2TP/IPSec VPN Client" at http://www.microsoft.com/windows2000/docs/VPNClient_AdminGuide.doc for good technical information about the new client. If your clients will sometimes be using a VPN to access your network from behind another company's firewall, you might run into problems with L2TP/IPSec.

If the firewall doesn't perform NAT, which is very unlikely, and if it is configured to let IPSec ESP packets (IP protocol 51) through then you might be successful. The problem is that IPSec doesn't support NAT traversal because portions of the packet, which is changed as it passes through a Network Address Translator, are also part of the information integrity checked by IPSec. When IPSec receives the NATed packet it balks. The IETF is working to enhance IPSec to handle NAT. Windows L2TP/IPSec clients use the draft (http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-reqts-02.txt) of this new IETF standard and can cross NAT boundaries right now. However, Win2K RRAS doesn't support NATed L2TP/IPSec at the VPN server end. Therefore, if the firewall in the situation above does perform NAT, your L2TP/IPSec VPN won't work until you upgrade your VPN server to Win.NET 2003, which is due out this spring.

IPSec Tunnel Protocol

The other VPN protocol, IPSec tunnel, has more limited application and it is the lightest weight in terms of performance. Whereas PPTP and L2TP/IPSec support remote access as well as site-to-site and extranet VPNs, IPSec tunnel supports only site-to-site and extranet VPNs because the IPSec protocol doesn't address remote access issues such as user authentication or the need to assign the remote workstation an IP address valid to the internal LAN. Also, IPSec tunnel doesn't support non-IP protocols such as IPX or multicast IP traffic. You have three options in IPSec for machine-to-machine encryption. As with L2TP/IPSec, you can choose between pre-shared key and certificates or, if both computers are part of the same Active Directory (AD) forest, you can use Kerberos, which requires no maintenance of credentials. Both computers authenticate using Kerberos tickets granted by the domain controller and based on their respective computer accounts in AD. Kerberos-based IPSec tunnels are difficult, if not impossible, to set up because both computers must be able to reach a DC before setting up the VPN. One other caveat with IPSec tunnels: you can build

FIGURE 6: VPN Protocols

Protocol	Capabilities					
	Authentication		Vulnerable to man-in-middle attacks or dictionary attacks?	Client OS	VPN Server OS	Can cross NAT?
	User	Machine				
PPTP	Yes	No	Yes	All Windows clients w95+ (Enhanced Dial Up Networking client and/or new VPN client may need to be installed on pre-w2k systems	NT W2k, .NET	Yes
L2TP/IPSec	Yes	Yes	No	Pre-W2k with new vpn client W2k XP	W2k, .NET	Yes (Windows clients only — no support from Wlndows VPN servers until .NET)
IPSec Tunnel	No	Yes	No	W2k XP	W2k, .NET	No

authenticated header (AH) tunnels or encapsulated security payload (ESP) tunnels. AH mode IPSec tunnels provide machine-level encryption and integrity, but no encryption.

As you can see, L2TP/IPSec offers the best of both PPTP and IPSec. L2TP provides user authentication and can route multiple protocols and multicast traffic by encapsulating the original packet inside an L2TP header before passing it on to IPSec. L2TP/IPSec enjoys good support among other vendors and is available on all Windows OSs thanks to the new VPN client. Thus, the big consideration when deciding between PPTP and L2TP for remote access is L2TP's requirement to install a certificate or pre-shared key on each client computer. This requirement is much safer, but also requires more work during implementation and maintenance. If your L2TP/IPSec clients are members of your domain, you can deploy certificates to them automatically via group policy. You'll need to set up an Enterprise CA and create a request for an IPSec certificate. You'll need to ensure that client computers are initially connected to the internal network so that they access group policy and install the VPN certificate before going on the road and trying to authenticate to your VPN server.

If you want smart card-, token-, or biometric-based authentication for your remote access VPN, Extensible Authentication Protocol (EAP) comes to the rescue. EAP is a framework authentication protocol that lets you plug in one or more types of user authentication, including tokens and biometrics. Win2K and later clients support EAP automatically. You must install the new VPN client to get EAP support on down-level clients. On your VPN server, you need Win2K or later and both RRAS and IAS installed. With L2TP/IPSec and EAP, you could set up a VPN that requires a machine certificate, a user certificate smart card, fingerprint scan, and PIN before allowing entry. Welcome to the CIA!

If your VPN must interoperate with other products, the solution might lie in any one of the three VPN protocols. PPTP enjoys wide support among VPN/Firewalls and non-Microsoft clients. But given PPTP's password authentication, you might think about IPSec tunnel because many products also support that protocol. But support for IPSec tunnel doesn't necessarily mean compatibility with another IPSec tunnel-compliant product. The reason is that IPSec is a framework protocol that doesn't mandate authentication, key exchange, or encryption specifics. Although some of these ambiguities will be addressed by the IETF's XAUTH initiative, currently each vendor tends to implement IPSec differently. IPSec tunnel is difficult to set up and troubleshoot because of the quantity of options that must be correctly configured on both systems. Thankfully, the latest versions of big-name VPN/Firewalls, such as Cisco, Nortel, and Checkpoint, now support L2TP/IPSec.

As you can see, you get considerable VPN functionality from the Windows family and I must concede that Microsoft is standing up to its commitment to security through the Strategic Technology Protection Program (STPP). Microsoft's release of a new VPN client lets you stay with a back-level Windows client without sacrificing VPN security. Before STPP, Microsoft always pointed to its newest OS if you wanted the best security. The nice thing about Windows VPN, besides being free, is integration with all other Windows components. You can automatically distribute certificates to your client workstations using group policy. Certificate Services automatically approves certificate requests from member computers by virtue of how domain computers are already authenticated to the domain via Kerberos. You don't need to create additional accounts for users because RRAS integrates with AD, and by using RAPs you can control VPN access through AD groups. More good security stuff is on the way with Win.NET's VPN-related enhancements and ISA Server's new feature pack. For a summary of VPN clients and protocols and their capabilities, see Figures 5 and 6, respectively. ◆

Randy Franklin Smith is a contributing editor for *Windows & .NET Magazine* and the primary instructor and course developer for MIS Training Institute's Windows NT/2000 security program. His firm, Monterey Technology Group, provides security consulting.

Microsoft ISA Server Partners

8E6 TEchnoLOGIES
Orange, CA
888-786-7999, or 714-282-6111
www.8e6technologies.com/isaserver

ACP
Birmingham, AL
www.acp-inc.com/isaserver

Aelita Software
Powell, OH
800-263-0036, or 614-336-9223 ext. 1
www.aelita.com/isaserver

AEP
Boston, MA
800-383-7716, or 617-443-4444
www.aep.ie/isaserver

Akonix
San Deigo, CA
619-814-2300
www.akonix.com/isaserver

Aspelle
Boston, MA
617-273-8114
www.aspelle.com/isaserver

Authenex
Oakland, CA
510-568-6070
www.authenex.com/isaserver

Burst Technology
Bonita Springs, FL
800-709-2551, or 239-495-5900
www.burstek.com/isaserver

Castify Networks
Alexandria, VA
703 370-5359
www.castify.net/isaserver

Chutney Technologies
Atlanta, GA
866-248-8639, or 404-442-9911
www.chutneytech.com/ISAserver/

CornerPost Software
Duffield, VA
276-431-7200
www.cornerpostsw.com/isaserver

F5 Networks
Seattle, WA
888-882-4447, or 206-272-5555
www.f5.com/isaserver

Finjan Software
Los Gatos, CA
888-346-5268, or 408-354-8975
www.finjan.com/isaserver

GFI Software
Cary, NC
888-243-4329, or 919-388-3373
www.gfi.com/isaserver

Hewlett-Packard
Atlanta, GA
800-752-0900
www.hp.com/isaserver

Infolibria
Waltham, MA
781-392-2200
www.infolibria.com/isaserver

Intellitactics
Bethesda, MD
888-495-4355, or 519-743-0144
www.intellitactics.com/isaserver

Internet Security Systems
Atlanta, GA
888-901-7477
www.iss.net/isaserver

N2H2
Seattle, WA
800-971-2622, or 206-336-1501
www.n2h2.com/isaserver

nCipher
Woburn, MA
800-624-7437, or 781-994-4000
www.ncipher.com/isaserver

NetIQ
San Jose, CA
888-323-6768, or 408-856-3000
www.netiq.com/isaserver

Nexus Technology
United Kingdom
isaserver@webconsent.net
www.webconsent.net/isaserver

PatchLink Corporation
Scottsdale, AZ
480-970-1025
www.patchlink.com/isaserver

Radware
Mahwah, NJ
888-234-5763, or 201-512-9771
www.radware.com/ISAServer

Rainfinity
San Jose, CA
877-724-6333
www.rainfinity.com/isaserver

RSA Security
Bedford, MA
877-772-4900
781-515-5000
www.rsasecurity.com/isaserver

Sane Solutions
North Kingstown, RI
800-407-3570, or 401-295-4809
www.sane.com/isaserver

Secure Computing Corporation
San Jose, CA
800-692-5625, or 408-979-6100
www.securecomputing.com/isaserver

Stonesoft
Atlanta, GA
770-668-1125
www.stonesoft.com/isaserver

SurfControl
Scotts Valley, CA
800-368-3366, or 831-431-1400
www.surfcontrol.com/isaserver

Tealeaf Technology
San Francisco, CA
415-495-8000
www.tealeaf.com/isaserver

Symantec
Cupertino, CA
408-517-8000
www.symantec.com/isaserver

Trend Micro
Cupertino, CA
800-228-5651, or 408- 257-1500
www.antivirus.com/isaserver

Venation
United Kingdom
+44 (0) 1473 707170
sales@venation.com
www.venation.com/isaserver

Wavecrest Computing
Melbourne, FL
321-953-5351
sales@wavecrest.net
www.wavecrest.net/isaserver

Websense
San Diego, CA
800-723-1166, or 858-320-8000
www.websense.com/isaserver

WebSpy
Kirkland, WA
425-828-4400
sales@webspy.com
www.webspy.com/isaserver

Aspelle Deploys ISA Server 2000 to Deliver Secure Access Technology

An investment bank was spending hundreds of millions of dollars on IT annually, with up to 40 percent on infrastructure alone. In addition, thousands was being spent on desktop support per user per year. The variety of locations, users, resources, and technologies employed yielded increasingly exponential complexity.

The bank's IT department was tasked with solving the operating problems resulting from this widely distributed user and resource base. Existing costs, and their future projections, were simply unacceptable. IT needed to find a way to centrally manage and optimize all of the resources used enterprise-wide. In addition, they needed to find a single, secure, reliable mechanism by which to centrally manage and deliver all of these resources to all of the bank's employees in its locations worldwide.

Tightly integrating proven security standards and Microsoft technologies such as ISA Server, the bank developed the Aspelle solution. So commercially viable was this offering that in 2001 the bank spun-out Aspelle, now an entirely separate independent software company.

THE SOLUTION

Aspelle Everywhere, built specifically for Windows 2000 and based on .NET, is able to deliver secure, client-less access to all corporate applications, regardless of a resource's underlying technology or the physical location of the user. Requiring only a Web browser and an Internet connection, the *Aspelle Everywhere* software platform securely enables access to a full range of applications and data including Intranet, Unix, Windows and legacy systems. *Aspelle Everywhere* offers a wide range of benefits to companies, including increased user productivity, improved response time to customer needs, and an overall reduction in technology-related overhead costs.

Drawing on many of ISA Server's security features, *Aspelle Everywhere* is an innovative solution for enterprises that not only want a secure, flexible and reliable alternative to traditional internal and external remote access technologies, but need to avoid many of the limitations and expenses of migrating existing applications to the Web. With this powerful combination of technology, *Aspelle Everywhere* enables users to safely retrieve resources that they are uniquely authenticated and authorized to access.

In implementations of *Aspelle Everywhere*, ISA Server resides in a company's DMZ (demilitarized zone). Here, *Aspelle Everywhere* provides authentication management through an ISA Server Web Filter and uses ISA Server's Web publishing functionality to securely deliver internal resources outside of the enterprise's infrastructure.

WORKING WITH ISA SERVER

Aspelle Everywhere extends ISA Server's authentication capabilities by adding support for SecurID, X.509, and SSL-encrypted username and password authentication. To ISA Server's firewall functionality, *Aspelle Everywhere* adds the ability to tunnel non-HTTP based TCP protocols via a SSL SOCKS client interface, delivering secure access to legacy TCP protocols via SOCKS and SSL.

To ISA Server's reverse Web proxy functionality, *Aspelle Everywhere* adds the ability to control access to specific resources (URLs) for individual users based on their own authorization and authentication rules stored in the Active Directory under the initiative's schema. *Aspelle Everywhere* checks that the user is authorized to view each URL they attempt to access.

Aspelle realizes that a business's competitive advantage depends upon its employees' ability to access their corporate applications quickly and cost-effectively, without compromising security, flexibility, or ease-of-use. "Undoubtedly, security, cost and complexity are three fundamental issues companies face when trying to expand the scope of access to their corporate information. By combining ISA Server's powerful authentication, authorization and resource delivery abilities with *Aspelle Everywhere's* non-invasive, software-based architecture, we have alleviated these barriers. Businesses can now conveniently and confidently provide users the access they need to succeed," notes Mark Turner, CEO of Aspelle.

> *"Businesses can now conveniently and confidently provide users the access they need to succeed."*
>
> **Mark Turner**
> *CEO,* **Aspelle**

ASPELLE

617-273-8114
www.aspelle.com/info

SurfControl Helps National Cooperative Bank Alleviate Concerns About Internet Access

As the Internet became a valuable tool needed by all employees of National Cooperative Bank (NCB), a financial services company based in Washington, D.C., the company raised questions about the risks of having access at every desktop. Starting in 2001, SurfControl helped NCB alleviate those concerns with easily customizable filters that help manage email and Web access.

"I know we're not spending administrative time chasing down problems and putting out fires. I feel a lot better from the standpoint that I have a solution locked down and that I don't have to worry as much."

Russell Schofield
Managing Director of Information Technology
National Cooperative Bank

In today's fast-paced financial services market, NCB has grown into the nation's leading financier of cooperative endeavors — from schools to independent grocers to housing groups. This cooperatively owned bank was created by Congressional charter in 1978, when it lent $10 million to natural food cooperatives and a handful of New York City housing co-ops in its first year of operation. NCB was privatized in 1981. These days, NCB has more than $1 billion in assets, features a broad array of financial products and services, and serves 1,841 customers.

THE CHALLENGE

NCB's employees surfed the Web freely, gathering information about clients, loans, and the financial services industry. Executives became concerned about other issues brought on by universal Internet access. A potential computer virus could cost the company money and resources. There was also the potential liability to the company if employees were to call up material on the Internet that might offend co-workers.

Employee email addresses were listed on NCB's original Web site, www.ncb.com. But employees started complaining to Russell Schofield, NCB's managing director of Information Technology, that they were getting a dozen or more unsolicited commercial emails per day.

THE SOLUTION

After evaluating the company's needs and objectives, NCB turned to SurfControl for a total filtering solution, which includes SurfControl Web and E-mail filtering products. In 2001, NCB installed SurfControl Web Filter for Microsoft ISA, a tool for managing corporate Internet access. NCB officials could tailor the tool to their Internet usage policies. To protect the company from liability, they wanted to block employees from accessing adult sites, hate sites, or sites that promote illegal activities such as online gambling. At the same time, they didn't want to block employees from visiting a health care Web site simply because it may have contained a non-sexual reference to the word "breast."

Other concerns for NCB information systems managers included the potential misuse of company bandwidth and the possibility that a computer virus could wreak havoc on the company's LAN. SurfControl let NCB set up specific user groups that prevented the majority of employees from downloading large files, such as MP3 files and digital movies, and prevented them from running .exe files that might contain viruses or other malicious code.

To address a growing concern over unsolicited email being sent to employees, NCB installed SurfControl's E-mail Filter, including the Anti-Spam Agent. Anti-Spam Agent lets network managers delay, isolate, or delete emails such as jokes, chain letters and get-rich quick schemes, in addition to graphical files such as GIFs and JPEGs that might contain offensive material.

THE RESULTS

Since installation of SurfControl E-mail Filter, NCB has had no computer virus and the total volume of email messages has been cut by 15 percent. Employees have stopped complaining about nuisance email and the company is confident it has the bandwidth to weather the next wave of Internet applications. Valuable corporate information that sits on computer hard drives is protected from viruses — and productivity is up.

"I know we're not spending administrative time chasing down problems and putting out fires," Schofield said. "I feel a lot better from the standpoint that I have a solution locked down and that I don't have to worry as much."

SurfControl
831- 431-1400
info@surfcontrol.com
www.surfcontrol.com

SurfControl®
The World's #1 Web & E-mail Filtering Company