

## SSL VPNs S ROUNDUP

**The current crop of appliances is mature, reliable, and packed with enough features to give IPSec VPNs a run for their money**

**T**RADITIONALLY, PROVIDING ROAD WARRIORS and business partners with access to back-end servers and resources has meant deploying an IPSec VPN. For site-to-site communication, IPSec remains the only game in town, but for client-to-enterprise links, it is falling out of favor precipitously. The administrative overhead associated with deploying IPSec client software has become overwhelming given the ever increasing number of clients to support. There is also the potential that IPSec tunneling will allow an untrusted device to punch a hole through the firewall — and directly into the heart of the network.

These kinds of basic problems with IPSec are why SSL VPNs are showing up on more and more IT radar screens. With an SSL VPN, there is no client software to install, let alone maintain. Not only does this cut down on IT labor, but it also means remote users aren't limited to specified locations. Public Internet kiosks, partner sites, a borrowed laptop — they all work.

More importantly, with an SSL VPN there is no open tunnel to the enterprise. SSL VPNs enforce security policies on each connection, allowing access only to specific resources based on user, location, and/or device. As with any good security control, everything is off-limits unless expressly allowed by the administrator.

**BY KEITH SCHULTZ | PHOTOGRAPHY BY MICHAEL BELK**

# The granularity of their access policies is where SSL VPN appliances really shine.

I explored the mechanics of SSL VPNs and explained how these appliances differ from their IPSec cousins in a similar roundup a year ago ([infoworld.com/2467](http://infoworld.com/2467)). This time around, I put six different SSL VPN appliances to the test to find out whether they've matured enough to replace enterprise-class IPSec deployments — and to determine which ones, if any, stand out from the rest.

## Packed With Features

The SSL VPN playing field gets more level with each product release cycle. Many of the appliances in this roundup are in their third generation and are technologically mature. The main features differentiating the products from one another are the way in which they implement security policies, how they handle remote end points, and how transparent the overall experience is to the end-user.

The granularity of their access poli-

cies is where SSL VPN appliances really shine. All the solutions reviewed here allow administrators to implement policies that change based not only on who is logging in but also on where they are logging in from.

In addition, every SSL appliance in this roundup supports some kind of end-point security software, although some do a better job than others. End-point software analyzes a client device, determines the level of confidence in its security, and applies access rights based on predefined “trust zones.” For instance, the software might determine that a user's laptop has anti-virus software and a personal firewall running on it, but because the laptop is attempting to connect via Wi-Fi from Starbucks, the appliance will only grant it proxied access, rather than full network access over an IPSec-style layer 3 tunnel. Currently no industrywide standard for end-point security control exists, but companies such as Cisco and Microsoft

are working to change that.

Beyond access controls, all the appliances reviewed offer additional security measures. All support “secure browsing” clients such as Sygate Secure Desktop. These clients create virtual sandboxes in which SSL sessions run. When a user closes the secure browser, its temporary files and session information go to a binary black hole. What's more, most SSL VPNs provide cache-cleaning software that covers users' tracks by removing temporary files, cookies, and other session information from the browser. These measures are very important for users connecting from publicly accessible PCs, but they aren't nearly as effective as using a secure browser because deleted files can often be recovered.

Other features that will interest some customers include VLAN support and clustering. VLANs allow for segregated traffic on the same physical network, a handy feature for service

Product	Overall Score
<b>AEP Networks Netilla Security Platform</b> AEP Networks <a href="http://netilla.com">netilla.com</a>	<b>8.0</b>
Security (35%)	9
Interoperability (25%)	7
Scalability (20%)	8
Setup (10%)	8
Value (10%)	7
<b>COST:</b> 100 users, \$34,300	
<b>BOTTOM LINE:</b> AEP has polished its NSP with this release, improving authentication support and adding end-point host checking via Sygate On-Demand. The NSP handles TCP-based thin-client applications in a unique way, using a method based on server proxy software from Tarantella. Although the NSP is a solid performer overall, its policy granularity could be improved.	
<b>Array Networks SPX3000</b> Array Networks <a href="http://arraynetworks.net">arraynetworks.net</a>	<b>8.5</b>
Security (35%)	9
Interoperability (25%)	8
Scalability (20%)	9
Setup (10%)	7
Value (10%)	8
<b>COST:</b> 100 users, \$25,000	
<b>BOTTOM LINE:</b> Array has added full layer 3 tunneling and Sygate-based end-point security checking with this release, making it competitive with other appliances. The SPX3000's Web proxy is the only one in the roundup to support complex content, including Flash. VLAN support is available, and the appliance itself can be partitioned into virtual sites. Its UI, however, is a little rough around the edges.	
<b>Aventail EX-1500</b> Aventail <a href="http://aventail.com">aventail.com</a>	<b>8.4</b>
Security (35%)	8
Interoperability (25%)	9
Scalability (20%)	8
Setup (10%)	9
Value (10%)	8
<b>COST:</b> 100 users, \$28,095	
<b>BOTTOM LINE:</b> The EX-1500 is a good all-around performer for secure remote access, but it only supports unidirectional TCP and UDP connections, rather than true IPSec-style layer 3 tunneling. On the plus side, its administration UI is easy to navigate and Aventail's end-point security management, when coupled with client software from WholeSecurity or Zone Labs, was the best of the bunch.	
<b>F5 Networks FirePass 4100</b> F5 Networks <a href="http://f5.com">f5.com</a>	<b>8.8</b>
Security (35%)	9
Interoperability (25%)	9
Scalability (20%)	9
Setup (10%)	7
Value (10%)	9
<b>COST:</b> 100 users, \$24,990	
<b>BOTTOM LINE:</b> The FirePass 4100 is one of the strongest platforms for Web, thin-client application, and layer 3 connectivity. It supports IPSec termination and includes a built-in browser-based remote desktop access application — features not normally found in an SSL VPN appliance. Unfortunately, F5 misses the mark with its homegrown end-point security software.	

# As opposed to other offerings, SPX3000 works not only with HTML, but also JavaScript, Cascading Style Sheets, cookies, and even Macromedia Flash.

providers or large enterprises. Clustering allows SSL VPN appliances to provide high availability through automatic fail-over and load balancing and can extend the number of concurrent users an appliance supports into the thousands. Given the relatively equal performance of the products in this roundup, it may be these and other niche features that ultimately tip the balance in favor of one particular product for any given customer.

## AEP Networks Netilla Security Platform

When last I visited the NSP (Netilla Security Platform), it was missing some core features necessary for an SSL VPN appliance ([infoworld.com/644](http://infoworld.com/644)). Since then, Netilla merged with AEP Systems to form AEP Networks and released Version 5 of its Netilla Dynatrust operating system. The new offering builds on the strengths of the previous release by adding previously

missing features such as LDAP support and end-point security checking.

As in its previous releases, the NSP uses “realms” to organize users, authentication schemes, and resource access policies into manageable groups and includes built-in support for Microsoft SMB (Server Message Block), Active Directory, SecurID, Kerberos, RADIUS, and local user authentication. The NSP also continues its tradition of using “authentication scopes” to pass user credentials to an application, enabling SSO (single sign-on). This method works but can lead to unnecessary administrative overhead when creating and managing links to Web resources.

As do all the appliances in this roundup, the NSP offers clients access to both Web-based and server-based applications. The NSP also offers layer 3 tunneling for direct IPsec-style network access, allowing TCP and UDP (User Datagram Protocol) traffic to pass through, and as do most appliances, it

supports full or split tunneling. Full tunneling means that all traffic, local and nonlocal, goes across the tunnel to the enterprise and is routed from there. Split tunneling routes enterprise traffic over the tunnel while other traffic — such as Internet traffic — goes out through the remote user’s default gateway. The method you choose will depend on the strictness of your security policies.

The NSP’s layer 3 tunnel is deployed as an ActiveX control, so layer 3 support is available only for Windows clients. This shortcoming is mitigated somewhat by the fact that the NSP handles thin-client access such as to terminal servers or “green-screen” legacy hosts in a way that’s different from that of any other appliance in this roundup. It uses Java client software and a proprietary protocol to connect the remote user to built-in proxy server software from Tarantella. The Tarantella server then makes the connection to the protected resource. This extra layer between client and server proxies all inbound traffic, regardless of its method of transport.

Also new to this release is support for Sygate’s On-Demand end-point policy enforcement software, which AEP Networks offers at additional cost. Client integrity scans can take place before and after authentication, and each realm can have its own specific host policy. The more advanced Sygate features are available only to clients on the Windows platform, but its cache-cleaning component will erase temporary files, cookies, and other session information for any Java-compatible browser.

When compared with those of other appliances, the NSP’s user interface is plain but easy to navigate. It still forces you to do some UI “link hopping” to create your realms, user authentication, and application definitions, but it could be worse. When I became comfortable with the UI’s organization, I had little trouble modifying or adding new applications and realms, although the NSP’s policy granularity is not as fine as that of some other products.

The NSP also has good internal logging and reporting capabilities, but it isn’t the best of the bunch in this regard.

**Juniper Networks  
NetScreen-SA 5000**  
Juniper Networks [juniper.net](http://juniper.net)

**EXCELLENT 8.9**

Security (35%)	9
Interoperability (25%)	9
Scalability (20%)	9
Setup (10%)	8
Value (10%)	9

**COST:** 100 users, \$33,995

**BOTTOM LINE:** There is nothing you can’t do with the NetScreen-SA 5000. It’s a beast of a box, providing exceptional capabilities with fine-grained control. All remote-access modes are available, and authentication services leave nothing to chance. It works with a wide range of third-party host checking software. The NetScreen-SA 5000’s weakest link may be the bewildering number of options its UI offers.

**Nokia Secure Access  
System 3.0**  
Nokia [nokia.com](http://nokia.com)

**GOOD 7.9**

Security (35%)	8
Interoperability (25%)	8
Scalability (20%)	8
Setup (10%)	7
Value (10%)	8

**COST:** 100 users, \$27,995

**BOTTOM LINE:** The NSAS will get you up and running quickly, but other areas of its UI could use some work. Although its Web-based access is top-notch, support for TCP/IP-based thin-client applications is clunky, and some admins may find scripting its end-point security software a chore. Lack of support for third-party end-point security software is a particular flaw; Nokia’s own just doesn’t measure up.

## How They Stack Up

The current crop of SSL VPN appliances is very feature-competitive, but the devil may be in the details when it comes to meeting your unique needs.

SSL VPN	End-point security			Hardware support			Modes of access			
	Vendors	Platforms	Scan before/after authentication	Max nodes in cluster	Network cards	FIPS 140-compliant	TCP application client	HTML handling	Full layer 3 tunnel	VLAN support
<b>AEP Networks Netilla Security Platform</b>	Sygate	Java, Windows	Both	Two	Two x 100Mbps	No	Java	Translates	Yes	No
<b>Array Networks SPX3000</b>	Sygate	Java, Windows	Before	32	Two x 1Gbps	No	ActiveX/Java	Rewrites	Yes	Yes
<b>Aventail Networks EX-1500</b>	WholeSecurity, Zone Labs	Java, Windows	Before	Two	Two x 1Gbps	No	ActiveX/Java/Win32	Translates	No	No
<b>F5 Networks FirePass 4100</b>	N/A	Windows	After	10	Four x 1Gbps	Yes	ActiveX/Java	Rewrites	Yes	Yes
<b>Juniper Networks NetScreen-SA 5000</b>	InfoExpress, McAfee, Sygate	Windows	Both	Eight	Two x 1Gbps	Yes	ActiveX/Java	Translates and rewrites	Yes	No
<b>Nokia Secure Access System 3.0</b>	N/A	Java, Windows	Before	Two	Four x 100Mbps	No	ActiveX	Translates	Yes	Yes

As do all the products in this roundup, the NSP supports both SNMP and Syslog logging. In addition, the NSP offers internally generated HTML graphs of basic system statistics.

Two-node clustering is part of the base NSP package, rounding out this solid offering. Clustering requires no additional hardware, although only a Hot-Stand-by configuration is supported.

### Array Networks SPX3000

When I first reviewed Array Networks' SSL VPN, I thought it needed to improve a bit to be a real player ([infoworld.com/674](http://infoworld.com/674)). In the past year, Array has enhanced its product through the inclusion of a layer 3 tunnel, site virtualization, and client-side host checking.

The SPX3000 provides all the modes of access that administrators have come to expect from an SSL VPN gateway. Policy enforcement is strong but not quite as granular as that found in the F5 FirePass 4100 or the Juniper NetScreen-SA 5000. As is the case with the other appliances in this roundup, Array's Web Resource Mapping service rewrites con-

tent as it passes through the appliance to obscure resource URLs. As opposed to the other offerings, however, the SPX3000 works not only with HTML but also JavaScript, Cascading Style Sheets, cookies, and even Macromedia Flash.

Array allows for easy access to file shares located on either Windows or NFS (Network File System) servers via its Web-based gateway. For client/server resources, the SPX3000 provides access in two ways. Application Manager is a Java applet that connects TCP-based applications to back-end services such as terminal servers. Windows Redirector, on the other hand, is a stand-alone application that is available only for Windows PCs running Internet Explorer but which allows for even greater control over access to specific resources.

New to this release is full, bidirectional layer 3 tunnel support. Administrators can define multiple tunnel definitions per virtual site, each with its own unique settings. For instance, one definition might include full tunneling, whereas another might specify split tunneling; and each can hand out IP addresses from a completely different DHCP pool.

Lack of cross-platform support is the price you pay for many of the more advanced features of SSL VPNs. Currently, the SPX3000's layer 3 tunnel is available only to clients running Windows, but Array says that Mac and Linux versions are in development.

Array's end-point security, including host checking and cache cleanup, is handled via Sygate On-Demand and Sygate Secure Desktop. Although the

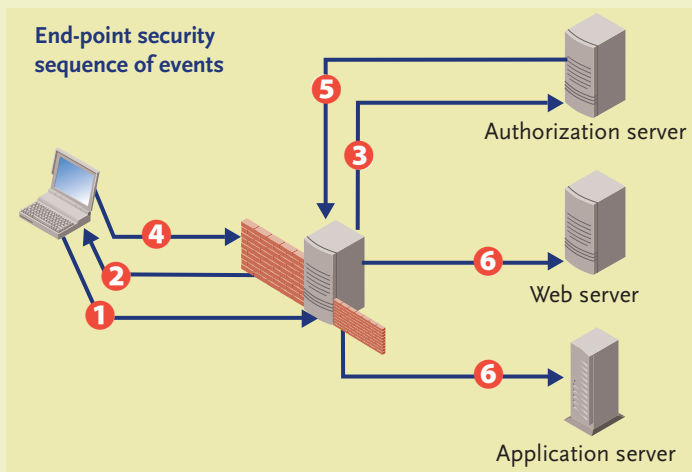


Array Networks SPX3000

## Locking Down the End Point

Whereas traditional mechanisms enforce security at the gateway, modern SSL VPN appliances extend control all the way to the remote desktop.

- 1 Remote PC connects to SSL VPN appliance
- 2 The appliance scans the remote PC before authorization is complete
- 3 SSL appliance forwards request to authorization server
- 4 Results of the remote PC scan are returned to the SSL appliance
- 5 If user is authenticated, the VPN appliance applies appropriate access policy based on the remote host configuration
- 6 If host check is OK and user authenticates, access is granted



end-point security component is tightly integrated in the SPX3000, it must be purchased separately. Host checking takes place only prior to authentication.

For large enterprises or service providers, the SPX3000 offers VLAN support, as well as "virtual sites." These allow admins to provision a single appliance into minisites, each with its own authentication and authorization settings. In addition, the appliance supports Active-Active and Active-Standby clustering configurations for as many as 32 nodes.

The administration UI of the SPX3000 isn't all that different from that of Array's previous releases. It's still a little bumpy, but it has improved. Similar items are grouped together to minimize UI fatigue, and each virtual site is self-contained. Delegated administration is well-supported; the appliance administrator assigns an individual user to administer a single virtual site, and only that virtual site. In all, I found that Array has successfully rounded out the SPX3000's feature set to make it competitive with any other appliance on the market.

### Aventail EX-1500

The EX-1500 is a good all-around performer for secure remote access. Aventail's Unified Policy engine makes life much easier for VPN administrators. Resources and users are tightly coupled, making policy definitions similar to a set of firewall rules. Instead of hopping all over the admin UI, everything is neatly nested together, and a handy Quick Start menu helps get you going. In fact, I was able to create a new access rule, complete with new resources and users, from a single screen — a small thing, perhaps, but one that busy IT managers will appreciate.

Each realm also includes access method and security zone definitions. Compatible authentication sources include LDAP, RADIUS, Active Directory, SecurID, and a local user database. Two-node clustering is available in an Active-Active configuration. Built-in load balancing and automatic fail-over require no additional hardware.

Endpoint Control 2.0, probably the best end-point security mechanism of any appliance reviewed here, has been added since I last reviewed Aventail's platform ([infoworld.com/2181](http://infoworld.com/2181)). When users connect to the appliance, Endpoint Control places them in specific

security "zones" based on their device profiles. A zone is a grouping that defines policy details such as whether to use a cache cleaner on the client's browser or to allow remote access (deny/allow all). This system makes it easy for administrators to create and maintain security policies that change as the user changes locations.

Endpoint Control relies on client-side software from WholeSecurity or Zone Labs to perform preauthentication host scans; either product must be purchased separately. Without these additions, Endpoint Control can still determine where a client is connecting from but cannot determine details about running processes and so on. For even more protection, the EX-1500 also works Aventail's cache cleaner and either Aventail Secure Desktop or Sygate On-Demand (also purchased separately).

The EX-1500 comes with excellent Web application support. It rewrites HTML on the fly and comes with some default Web application profiles to handle special applications such as Outlook Web Access — although none of the appliances in this roundup had trouble with either of the Test Center's Outlook Web Access 2000 and 2003 servers.

## For large enterprises or service providers, the SPX3000 offers VLAN support as well as “virtual sites”.

Thin-client support is Aventail OnDemand’s job. Not to be confused with Sygate On-Demand, Aventail OnDemand is a Java application that downloads on request to your browser and provides TCP application support.

Although good, Aventail’s logging features aren’t as comprehensive as those of the F5 FirePass 4100 or the Juniper NetScreen-SA 5000. The EX-1500 comes with support for Syslog, SNMP, and internal text logging but offers no built-in graphical reports.

One big drawback is that, as opposed to the other appliances reviewed here, the EX-1500 lacks any facility for true layer 3 tunneling. The included Aventail Connect utility almost makes up for this shortcoming, however. Aventail Connect is a Windows application installed on the remote PC that provides “network-level” access to backend resources. It is not a true layer 3 tunnel — remote users can ping in but not out — but it does provide full TCP and UDP inbound support. Aventail promises to deliver full bidirectional tunnel capabilities in a future release.

### F5 Networks FirePass 4100

Many features found in F5’s FirePass 1000 — which *InfoWorld* reviewed in October ([infoworld.com/2182](http://infoworld.com/2182)) — carry over to the FirePass 4100 but in an updated, more powerful way. The 4100 also includes some less common features among SSL VPNs, such as content filtering and anti-virus scanning, both of which are implemented using open source software. The FirePass can even terminate site-to-site IPSec tunnels, although it isn’t designed to handle client-to-site IPSec.

The FirePass offers the standard portal-based access for Web applications, application access via TCP-only AppTunnels, and a layer 3 connector

called Network Access. It also allows thin-client access to native host applications such as Citrix MetaFrame, Microsoft Terminal Services, X Windows, and “green-screen” legacy applications via special connector software. I tested the Terminal Services support against one of our Windows 2000 Servers and was surprised at how quick and smooth it was. The FirePass 4100’s layer 3 tunnel allows for both split and full tunneling and includes built-in VLAN support.

One notable feature of the FirePass 4100 is Desktop Access. Similar to the Beam application found in the enKoo-3000 ([infoworld.com/2468](http://infoworld.com/2468)), Desktop Access is remote access software for Windows that runs in a browser via a Java applet or an ActiveX control, either of which can be pushed to the remote client on demand.

The FirePass offers almost too many logging options. Every conceivable thing that can be logged, is, and support for SNMP and Syslog is included. Graphical reporting tools are also built in, making at-a-glance monitoring easy.

Authentication services in the FirePass 4100 include LDAP, RADIUS, Active Directory, Vasco DigiPass, basic HTTP authentication, client certificates, and local database. Each authentication scheme is assigned to a specific resource group. SSO for Windows resources is enabled by default and worked in every case I tested.

Clustering support is particularly strong in the FirePass 4100. Linking 10 nodes allows it to support as many as 10,000 concurrent users, and both Active-Active and Active-Standby clustering come standard.

The FirePass administrator UI suffers from a bit of “hyperlink overload,” but after spending some time hunting through the myriad options, I became

familiar with the layout, which proved fairly easy to navigate. There are also some nice features. For example, to avoid keystroke loggers on client PCs, F5 offers a graphical virtual keyboard for both user name and password.

The FirePass should be especially attractive to government users because F5 offers a version that complies with FIPS (Federal Information Processing Standard) 140, the U.S. National Institute of Standards and Technology specification that outlines security requirements for cryptographic modules. Most of the vendors represented here expect to have FIPS 140 compliance ready in 2005, but only F5 and Juniper offer compliant products today.

The one area where the FirePass could use some work is in end-point security management. Unlike other appliances, the FirePass relies on its own host checking software rather than partnering with a third party. Although F5’s offering does provide cache-cleaning options and a virtual desktop called Protected Workspace, it isn’t as powerful as the Sygate On-Demand engine. It will, however, check for running processes, Registry entries, OS and Internet Explorer service pack levels, and the presence of McAfee VirusScan. If a client fails any host check, its access falls back to a quarantine network. Unfortunately, the host check doesn’t take place until after the user has authenticated. F5 tells us that pre-authentication support is in development and is slated for the next software release.

### Juniper Networks NetScreen-SA 5000

*InfoWorld* reviewed the Neoteris Access Series SSL appliance in October 2003 ([infoworld.com/644](http://infoworld.com/644)). Now owned by Juniper, the heart of the old product

## Array has successfully rounded out the SPX3000's feature set to make it competitive with any other appliance on the market.

beats on in new and improved hardware and with a more mature security engine. The current software release, Version 4.2, still suffers from GUI fatigue and needs better organization, but overall, the product proved flexible and secure.

Remote users can authenticate against Active Directory, LDAP, RADIUS, Netegrity, digital certificates, or a local database, and each authentication realm can use multiple authentication servers. User roles map authenticated users into specific groups. These groups define what forms of remote access have been granted to a user, as well as any session-specific details such as inactivity time-out or session persistence. For example, an admin can create one role that includes Web access, Windows file shares, and Terminal Services and another that allows only Web access.

The NetScreen-SA 5000 provides all the standard remote-access methods, including Web, TCP-based, and layer 3. For Web applications, the granularity with which an administrator can define access policies is amazing, with settings to control all sorts of features, ranging from caching policies to HTML rewriting to compression. Despite all this perceived complexity, defining a Web policy turned out to be relatively simple. Web-based Windows, Unix file browsing, and Telnet support are also included.

TCP-based applications get routed through SAM (Security Access Manager), software that is available in Windows and Java versions. SAM can be configured to automatically launch based on a user's role.

Layer 3 tunneling is handled by Network Connect, Windows-only software that installs a virtual PPP adapter on a remote PC. Administrators can assign IP addresses to Network Connect

clients from a private DHCP pool. Full and split tunneling are available, as are custom DNS settings. Admins aren't given as fine-grained access controls on the tunnel as for other services, but what they get is definitely superior to what is available with IPsec. Juniper says Network Connect will be available for Mac OS X and Linux in the next major release.

The SA-500's end-point security mechanism, JEDI (Juniper Endpoint Defense Initiative), works with InfoExpress, McAfee, Sygate, and Zone Labs client software. The only downside is that JEDI works only on Windows.

At first glance, the administration UI looks awkward and confusing. Because of the sheer number of options and features available, GUI fatigue is inevitable. In practice, context-sensitive links quickly take you to related functions. Logging and reporting are first-rate, including real-time usage graphs.

Other than F5's FirePass 4100, the NetScreen-SA 5000 is the only appliance in our roundup that is available in a FIPS 140-compliant model. In addition, the NetScreen-SA 5000 handles high availability in an Active-Passive mode and can scale to eight nodes in a single cluster. VLAN support is not currently available, although Juniper says it is in development.

### Nokia Secure Access System 3.0

The NSAS (Nokia Secure Access System) provides everything you need for secure remote access without overwhelming you with its administration UI. It supports Web portal, file share, TCP application support, and layer 3 tunneling. Web application access is first rate and is very easy to define and maintain. A Web resource can be

added to the NSAS portal in a matter of a few clicks, which is not possible with some of the other appliances in this roundup.

Another difference is that the NSAS defines authentication schemes on a global scale and doesn't allow for multiple virtual sites, although the appliance does support multiple authentication schemes. Options include LDAP, Active Directory, NTLM (NT LAN Manager), RADIUS, PKI certificates, and use of local user databases. For high availability, NSAS can cluster two nodes with no additional hardware.

NSAS supports TCP-based applications through a Java helper program, but the overall UI needs a major face-lift. The user must query the portal to learn which local loopback address to connect to for each specific client program. All the other boxes we reviewed do a much better job hiding this process from the end-user.

Secure Connector, Nokia's IPsec replacement technology, is built into NSAS and supports full and split tunneling. Secure Connector allows admins to create a private IP address pool for remote users, as is possible with the Juniper NetScreen-SA 5000. NSAS uses firewall-style allow/deny rulesets to define access controls within the tunnel. Administrators can specify address ranges, ports, and protocols for access to specific resources and can even deny access to clients that don't meet anti-virus requirements. The Secure Connector client is available only for Windows PCs running Internet Explorer.

Secure Workspace is Nokia's virtual sandbox, and it, too, is available only to Windows and Internet Explorer users. As does Sygate's Secure Desktop, Secure Workspace deletes all temporary files, removes browsing history,

## What's missing is an industrywide standard that allows security policies to be enforced across multiple vendors and platforms.

and erases any session information. A floating toolbar allows you to switch between your local desktop and the secure desktop.

Nokia's Client Integrity Scan checks the remote PC to assess its status either before or after authentication. Administrators configure the scan using a custom scripting language. This has the benefit of allowing admins to build scripts specific to their needs, but it is likely to be time-consuming.

The administration UI in the NSAS is fairly easy to navigate. The amount of logging and monitoring information is almost overwhelming, as it is with the FirePass 4100, but the use of filters helps keep it manageable.

Unfortunately, the NSAS offers no support for third-party host checkers such as those offered by Sygate or WholeSecurity. Third-party support must be added to the NSAS to allow for easier integration into existing client security infrastructures and to provide

additional client-side management if it is to hold its own against the other appliances on the market.

### Ready to Switch?

To be fair, it doesn't make sense to tear out all your existing IPsec gear and immediately replace it with SSL. It does make sense, however, to start deploying SSL and migrating users to it. IPsec and SSL can coexist and complement each other, allowing for a gradual move from one platform to the other.

Even for an enterprise that has an extensive investment in IPsec, migration to SSL is justifiable. The support cost per client is so much greater with IPsec than with SSL that the labor cost savings will offset the expense of the new hardware. Long-term administration is also much easier to manage on an SSL VPN because everything is centrally located. Any policy updates or changes to client-side applets are automatically pushed

out on the next connect.

What's more, SSL VPNs simply offer better security than IPsec appliances do. All SSL VPN connections — even IPsec-style layer 3 connections — have access control policies associated with them. This allows administrators to grant access to specific resources, rather than opening up the entire network as you would with IPsec.

Each of the SSL VPN appliances reviewed here provides an admirable range of features that make them worthy competitors against any IPsec equivalent. After the smoke cleared and all the results had been tallied, the Juniper NetScreen-SA 5000 came out on top. Although not perfect, the NetScreen-SA 5000 passed every test thrown at it, and it never failed to meet challenges. Still, none of the competitors in this roundup is a bad choice. As this market continues to mature, you'll have more and more reasons to expect your next VPN to be an SSL one. ↻

