

ENTERPRISES ARE BEING DRAWN TO SSL VPNs BY THE PROMISE of easier support for roaming users—there’s no need to install a thick client that is closely tied to a particular operating system and requires an IT department to touch each endpoint. With nothing more than a Web browser, users can securely connect to internal networks from just about any machine, anywhere.

But reality is quite different. In fact, many corporate IT departments that start down the SSL VPN path because of minimum client requirements discover that the requirements aren’t so minimal, especially to support a heterogeneous network. SSL products still require a great deal of administration, configuration and support, as was evident in *Information Security’s* extensive tests of five leading products.

We tested four hardware solutions—Aventail’s ST EX-2500, Gisco Systems’ ASA 5540, F5 Networks’ FirePass 4100 and Juniper Networks’ Secure Access (SA) 6000 SP—and one software product, Check Point Software Technologies’ Connectra NGX R61 (Check Point also sells its product as an appliance).

Not So Simple

Are you ready to rid your enterprise of a client-based VPN in favor of simple SSL? Tread carefully. We sort through five SSL VPNs, and uncover which best conquer the many challenges. BY DAVID STROM

About this review



Aventail's ST EX-2500



Check Point Software Technologies' Connectra NGX R61



Cisco Systems' ASA 5540



F5 Networks' FirePass 4100



Juniper Networks' SA 6000 SP

Information Security invited 17 SSL VPN vendors to apply for consideration for testing, and selected the five best responses based on a combination of pre-eminence in the security market and our judgment about features and the ability to support a large, complex network such as Stanford University's network. Nokia declined to apply without giving a reason, Symantec did not submit a product because it is focusing on the UTM market, and SonicWALL passed because of its SMB focus.

We set up a test lab on the Stanford campus, using the university's production network and tapping into resources on its enterprise backbone. Stanford has an older IPsec VPN configuration and was interested in an SSL VPN gateway.

All of the VPN gateways were placed on a separate server network, along with a Windows Server 2003, a Linux server, and an RSA SecurID ACE appliance that was used for two-

factor authentication with its key fobs. We also set up an Avocent DSR 1031 KVM switch that allowed us to control all of these servers via a Web browser, and was used to test the ability of each VPN to support complex Web applications.

All of these servers were placed behind a firewall that blocked all access, with the exception of a client coming from one of the VPNs. A separate network contained four client PCs running Windows XP with SP2, Windows 2000, Windows 98 SR2 and Mac OS X v10.4, each with the latest patches and updates applied.

Each Windows client ran both IE v6.0 and Firefox v1.5 browsers. The Mac ran IE v5.2, Firefox v1.5, and Safari v2.0.3. The test lab also connected to a production Microsoft Active Directory server that was also running RADIUS and LDAP services, and an Exchange 2003 server that was configured for IMAP, POP and Outlook Web Access. • —DAVID STROM

The products were tested in a purpose-built lab on the Stanford University campus in California (See "About This Review," above), with the help of the backbone networking group that runs the main university data center and operates the major network infrastructure on campus. We analyzed and graded their capabilities (See "Making the Grade," p. 44) for enterprise management and control, client support, applications support, and authentication and access control.

Enterprise Management and Control

Anyone who will deploy an SSL VPN will have to spend a lot of time getting accustomed to its administrative interface. The issue for these products is that because they touch a lot of different places in the network, you will have different people assigned to different roles in their administration. Juniper and F5 seemed to understand this situation the best.

These are complex products. There are so many knobs to turn, especially with so many admins doing the tuning, it's easy to make a serious mistake. In all cases, it was easy to check the wrong item on one particular screen and render a working system useless. For example, with a few misplaced mouse clicks we could easily destroy a lot of hard work

performed setting up the entire endpoint security subsystem, or ruin our authentication connections. (For example, when setting Juniper's configurations, you need to be careful to save your changes before you navigate to another menu—it doesn't save changes automatically.)

All the products except Cisco's use a Web server to set up and control configuration parameters; Cisco requires its ADSM client for this purpose, which seems outdated. We examined how multiple boxes can be administered, whether administrators can see who is logged in at any given moment and kill that particular user's session, and what auditing, reporting and debugging features were available.

Cisco's administrative tools were the worst, and F5's were the best.

The biggest differentiator among the five products was the ability for multiple users with different administrative roles to manage the box concurrently. This is critical in large-scale deployments, where multiple people will be adding users, changing access policies and setting up individual portal pages.

We especially liked the ability of F5 to specify the particular menu choices each admin can use. Its Administrative Realms page offers complete granularity when it comes to

Trying to connect

One of the most interesting results of our testing was the difficulty each vendor had in supporting the most basic VPN activity: the ability to mount a Windows file server and connect to one of its shared drives, and open and copy files to this network share. Only Juniper was able to complete this task in the time allotted, and even it had to struggle to figure out the problem.

That problem was Stanford's wide-open network—its servers are directly connected to the Internet, with no intervening firewalls. To protect themselves and these resources, Stanford's server support group has locked down its user authentication to use NTLM v2. This requires stronger authentication than the original version that supported the LAN Manager-style username and password combinations that are sent over the wire in the clear.

SSL gateways can't talk this protocol to the Windows file servers, so users must employ the network extension client to authenticate. When we tried to set up a share for the thin clients using each vendor's portal pages, the logins failed. Juniper has a setting that specifically turns on v2 authentication, while Aventail required a manual editing of its start.sh file to enable it. F5 and Cisco don't support this protocol. Check Point says the problem was longer passwords that didn't parse in its Samba client.

—DAVID STROM

assigning particular admin rights to different subsets of the overall functionality.

In contrast, Check Point allows only a single administrator to log in at any given moment. Cisco also lacks the ability to assign different roles to multiple administrators.

Aventail isn't much of an improvement; it comes with three administrative templates that offer some granularity to allow multiple people to manage its software.

Layouts of administrative menus are subjective, but we found ourselves coming back to Juniper's whenever we wanted to get something done quickly. They're set up very logically for VPN management and have clear-cut menus to control Linux, Mac and Windows clients, which we found easiest to work with. We were able to handle multiple administrators easily.

The various functions and menu layouts made F5's admin interface the best of the five. It is clean and well laid out. While some of the menu choices are a bit obscure, most are redisplayed in a manner that makes it easy to add policies and set up your applications.

Cisco's ADSM administrative interface is so miserably designed that it presented problems for its support engineers; often, they couldn't quickly locate the appropriate screen. ADSM has multiple hierarchies of menus within menus, making it easy to get lost several screens down.

Each of these products could do a better job with debu-

gging tools, especially when it comes to setting up authentication servers (discussed later). Nevertheless, we liked F5's feature that allows an admin to log in to the gateway as a user. If something isn't working, the admin can go directly into the configuration console to make changes without having to log in with a separate browser session. The other products were more cumbersome in switching between administrator and ordinary user.

Aventail has a nice initial installation routine that steps you through the process, but its administrative interface lacks the "breadcrumb" display to show the complete path you took through its sometimes convoluted menu trees, something we found useful among its competitors.

Client Support

The most important part of any SSL VPN is how it supports users of the product. We tested Firefox and Internet Explorer browsers (and Safari on the Mac) on a variety of operating systems, as well as each product's endpoint security checking and remediation routines.

Each SSL product supports Windows XP/2000 and recent versions of Internet Explorer to connect to their gateways, and

all except Aventail offered solid support for Firefox browsers.

All of the products have a network extension client for Windows and IE, but none of them have a network extension client that completely works with Windows 98 or completely supports the Mac OS. At the time of our tests in June, only Aventail had a Mac OS network extension client that worked on the newer Intel-based Macs. Aventail's Mac network extension client is a bit cumbersome in that users must authenticate twice—once in the browser, and then once in the client preferences.

Juniper had the best overall client support, including the best support for Windows 98, provided it was running the latest version of Internet Explorer, but not all applications worked completely, such as the Java-based SSH client.

All of the products required administrative access to the remote client machine for the initial install of their network extension client. This could be a problem for corporations that lock down their machines with restrictive logins and don't allow users to install their own software.

Speaking of locking down machines, endpoint security is an increasingly critical part of client support. But this area is still very much a work in progress. Some SSL VPNs—such as Check Point—offer endpoint security as an extra cost option, while others have partnered with a variety of suppliers to perform health assessments and remediation.

Support for antivirus products is the first, critical consideration. Both F5 and Juniper make use of the OPSWAT database of dozens of antivirus products. Cisco supports more than a dozen, while the others have more limited support.

The products offer varying degrees of control over what endpoint conditions they check for either prior to or just after login. Juniper and Check Point have the most granularity in terms of type of OS and conditions, such as whether particular antivirus, firewalls and other malware blockers are running. For example, Juniper's remediation measures include the ability to delete specific files or terminate particular processes, or to run custom scripts.

Network administrators who are comfortable creating firewall rule sets will find the process of crafting endpoint security policy very similar. We particularly liked F5's nifty visual policy editor, which works like a flowchart, and adds features such as the ability to check for particular IE versions and the presence of a Google Desktop indexing engine. However, testing and deploying the right series of policies is still somewhat cumbersome because of all the choices available.

Finally, all the vendors offer a desktop "sandbox" mode, in which a Windows user (no Mac or Linux support) can log in to a completely protected workspace that prevents users from saving files locally, and cleans up afterward, leaving behind no evidence of files or cookies. This is very useful in insecure environments, such as at an Internet café or other public computers.

Juniper has the most fine-grained control over what users can and can't do once they are inside this protected environment, such as permit access to printers, make changes to the Windows Control Panel, or allow particular IE browsers with particular encryption key strengths.

Applications Support

Corporate VPN administrators will need to carefully examine every application and test to make sure that it works for each client, and under both thin and network extension clients. This is where SSL VPNs are weakest: IPSec products can handle a wider range of applications without any configuration, since they own the entire protocol stack.

We tested a variety of simple and complex applications to see how well they would work on each product. We tried to connect to a Windows file share on the local LAN, to an FTP and SSH server, and view a variety of Web servers that were behind a firewall. We also tried to run Outlook Web Access and connect to a Java-based Avocent KVM over IP server.

With each application, we used a browser-based client to connect to a custom Web portal page linking to each application, and with the network extension client (if it was available for that particular platform).

Juniper had the widest support for applications, and has a nice way to debug URLs entered into its portal configuration screen.

Assembling "Team VPN"

We assembled a medium-sized team to gather all the expertise required to configure our five products. You should be prepared to assemble a similar team when testing and deploying your SSL gateway.

This is because the SSL gateway touches many different parts of your enterprise computing infrastructure. If you have segregated your support into desktop, server, network backbone, network applications and end user departments, as Stanford does, you will need representatives from each of these groups.

For example, while testing our products we needed one person to correctly specify the parameters for Stanford's LDAP and RADIUS servers; another to determine how to connect to its Windows file servers; a third person to configure desktops; a fourth for the firewalls, routers and switches; a fifth to set up our Linux server; and a sixth to answer specific security questions that no one else could answer, such as troubleshooting authentication issues and more complex Windows servers issues.

—DAVID STROM

Surprisingly, the biggest issue with our tests was connecting to a Windows file server shared drive. This is a relatively simple task, but it confounded all the products except Juniper and Aventail (See "Trying to Connect," p. 40).

Certain complex Web applications, such as the Avocent KVM over IP, gave us trouble as well. Aventail was the only product that could support the Avocent KVM session inside a browser, but it only worked with IE. The others required their network extension clients to enable viewing remote desktops over their VPN connections.

While Cisco wasn't alone in its failure to support Mac Intel clients, even its thin client couldn't browse Windows file shares on these Macs, which is a bug. Check Point and F5 also had some issues and couldn't support all the applications as well as Juniper did.

Authentication and Access Control

We tested the products with existing RADIUS and LDAP servers on the Stanford network, as well as a test RSA SecurID application to provide two-factor authentication.

All five products were able to use all three of these servers, although it took some doing to get everything working.

We also examined each product to see how granular their access levels could be—such as restricting users to

Key SSL VPN features

FEATURE	Aventail ST EX-2500	Check Point Connectra NGX R61	Cisco ASA 5540	F5 Fire Pass 4100	Juniper SA 6000 SP
Support for multiple admin realms	Fair	No	Poor	Good	Good
OPSWAT AV SDK support	Next release	No	No	Yes	Yes
Firefox support	Poor	Yes	Yes	Browser plugin	Yes
LDAP troubleshooting tools	Good	Poor	Fair	Fair	Good
Support for outside AAA servers	No ¹	Yes	Yes	Yes	No ¹
Access by time, source IP, etc.	Yes	No	Yes	Yes	Yes
Mac-Intel net extension client	Yes	Next release	Next release	Next release	Next release
# NICs per box ²	2	Varies ³	2	4	2
Active/Active HA cluster	Yes	Yes	Yes	No	No
Native RSA ACE server support	No	Yes	Yes	Yes	Yes

Notes:

¹ Must run single-homed to connect to any outside authorization/authentication servers

² Not including any interfaces for clustered connections

³ Software-only solution; can be installed on any reasonable server; available as appliance

only log in at a particular time of day, or with specific source IP addresses. All the products except Check Point can set access by time of day or by source IP address.

Check Point clearly lagged behind the others in terms of setup and features, and Cisco was superior in this category.

The most vexing part of our setup was in connecting each box to the Stanford LDAP server. This was a combination of our own mistakes in getting the various parameters right—such as entering the correct IP address of each server—and each product's poor debugging tools in telling us when we made mistakes.

Check Point had the worst set of debugging tools, while Aventail and Juniper had the best. Juniper provides syntax examples you can use to type in the correct strings, and Aventail has the dearest screens that prompt you for the required information.

Getting the RSA SecurID ACE server set up was simple for those vendors—all but Aventail—that explicitly support it. For Aventail, we had to connect to the ACE server via RADIUS protocols.

Cisco, Aventail and Juniper segregate their authentication realms for each user group on their Web-based login pages, making it easier to test whether each realm is working properly.

Each product comes with two network interfaces and can be run in what is called dual-homed configuration—one interface is connected to the public network, and one lives on a private network with access to protected resources.

However, we weren't able to connect Juniper and

Aventail's products in this fashion because of how both products work with external network resources—they assume that all authentication servers are attached on the internal network. In our situation, these RADIUS and LDAP servers were outside the protected network and operated on the general campus network.

Having dual NICs is a better security practice, because you physically separate your two networks. Having the AAA servers on the internal network is also a better security practice, but what's the point if you can't get there via the VPN?

So, we had to operate both of these products on a single interface, which may not be acceptable in certain corporate situations. A typical example is an organization that uses three layers of firewalls to separate its most important apps and critical servers from the outside. One plus for Cisco is that you can assign authentication servers on either its internal or external interfaces.

There's Work Ahead

The bottom line is that these are complex products with all sorts of fineries to their operations. They require a team of sharp folks from various areas of your IT infrastructure to deploy properly (see "Assembling Team VPN," p. 41). SSL VPNs are quirky, difficult to install and set up, and offer spotty support for users beyond the Windows 2000/XP and IE envelope. Certainly, if you have a very heterogeneous network, or a large group of custom-built corporate applications, you will have a long test and rollout ahead.

Making the grade

	Aventail ST EX-2500 www.aventail.com	Check Point Software Technologies Connectra NGX R61 www.checkpoint.com	Cisco Systems ASA 5540 www.cisco.com	F5 Networks FirePass 4100 www.f5.com	Juniper Networks SA 6000 SP www.juniper.com
Cost per 100 users	\$26,995*	\$15,000**	\$24,990	\$24,990	\$40,990***
Cost per 1,000 users	\$62,995*	\$60,000**	\$55,995	\$69,990	\$93,990***
Enterprise Management	B-	B-	D	A-	B+
Client support	B-	C+	C	B	B+
Apps support	B	B	B	B	A
AAA control	B	C+	B+	B	B
Verdict	B- Pros: Mac support; good LDAP setup/debug tools. Cons: Can't support external authentication servers outside the protected internal network; no Windows 98 support.	C+ Pros: Solid endpoint security tools. Cons: Miserable Mac client, poor debugging tools for AAA server setup; requires three IP addresses; poorly differentiated administration.	C+ Pros: Supports both IPSec and SSL gateways; flexible feature set for authentication servers. Cons: Poor administrative interface; limited administrative realms.	B Pros: Endpoint checking tools with nifty policy editor; instant configuration updates; multiple concurrent admins; Firefox network extension. Cons: Spotty Mac support; mediocre authentication debug tools.	B+ Pros: Non-Windows client support; solid administrative features; logical menu. Cons: Can't support external authentication servers outside internal network; high overall cost.

*Thin client terminal emulation costs \$4,995 for 100 users and \$19,990 for 1,000.

**Network access control requires Integrity, costing an additional \$5,500 and \$13,500 for 100 and 1,000 users, respectively.

***Juniper's SA 5000, which is comparable to the other appliances tested, with a top price of \$75,985.

Given that reality, there are clear differentiations that put some products ahead of the pack.

Juniper's SA 6000 SP was the clear winner in overall usability, features, and flexibility of operations. It took the least time to get set up and working, despite some complex menus and some oddly placed items.

The F5 FirePass was next, with sophisticated endpoint checking routines and a long list of supported antivirus programs. It has a visual policy editor that anyone who has done any flowcharting will glow onto.

Aventail's EX-2500 is an interesting study in contrasts. It has leading-edge functionality yet is missing basic key ingredients. It was the only product not to offer native RSA SecurID ACE support, yet it had some great debugging tools for setting up LDAP servers.

If there is a feature missing from the Cisco VPN gateway, we would be hard pressed to find it—and that, in a nutshell, is the problem. You can run both IPSec and SSL VPN clients from the same gateway, and set various user and group policies that are so extremely intricate that you dare not touch them once you have them working. The issue is that Cisco's administrative interface is complex and a bear to set up.

Check Point Connectra's biggest issue was the lack of differentiated, departmental-based administrative roles. It also has the weakest support for authentication servers and poorest overall client support. On the other hand, if you already have other Check Point products, such as firewalls and IPSees, you can manage all of this gear from a single console.

David Strom is a freelance writer, speaker and former editor-in-chief of Tom's Hardware and Network Computing magazines. Send your thoughts on this article to feedback@infosecuritymag.com.

Information Security thanks the Stanford University IT department for its help in creating such a rich test environment, and especially its director of networking systems, Mark Miyasaki. Specifically, we thank Paul Murray, Johan van Reijendam, Steve Tingley, Russell Scheil, Ross Wilper, Sean Riordan, Leroy Altman and Jason Craig for all their help with this project.

 Get expert SSL VPN help at www.searchsecurity.com/ismag