



SSL VPNs

Aventail and F5 Extend Their Reach

Companies inject policy enforcement into already strong SSL VPNs

DURING THE PAST FEW YEARS, SSL VPNs have matured from devices offering very basic application support to enterprise-ready security jacks-of-all-trades, capable of handling thousands of users and a wide range of connectivity options. Security features are evolving, with extensive host checking taking place prior to user log-on and adaptive, dynamic security policies being applied accordingly.

SSL VPNs are continuing to win over new converts for several reasons: They don't need a "fat client" on a device to function; they require less administrative management; and they can reduce help-desk support calls dramatically. No longer relegated to designer solutions, SSL VPNs are more commonly being added to routers and core network concentrators through a software upgrade or licensing option. Additional refinement of existing features notwithstanding, more noticeable is the absence of any landmark changes to the overall technology in the past 12 months.

I recently looked at the latest



F5 FirePass 4100

releases from two of the SSL VPN market leaders. Both the Aventail EX-2500 and the F5 Networks FirePass 4100 continue to mature and provide excellent platforms from which to build a secure remote access solution. Each appliance comes with updated hardware for greater scalability, as well as software improvements that take existing capabilities to new heights.

Same Technology, New Uses

Few would have thought that SSL VPNs, as a secure remote access technology, would help provide a solution for internal network access control. Yet some companies are forcing their local network users to log in to the SSL appliance's Web portal before gaining access to corporate resources.

This serves a couple of purposes. First, it allows administrators to perform a preflight check on the client device before permitting access to the network. For example, both the Aventail and F5

boxes can perform end-point security audits to determine the level of trust to apply to the host and deny entry if it fails any test.

This type of policy enforcement intrudes on local policy platforms such as the ConSentry Secure LAN Controller and Elemental Compliance System, although the latter provides a much more granular and flexible system for classifying clients on the network. Aventail and F5 are heading in the right direction, but they have a ways to go to catch up to these two products.

Second, by having users log in to an SSL VPN portal, admins have additional control over the applications and resources those users will be accessing. It allows very granular access control rules to be deployed so that resources can only be accessed a specific way, reducing their exposure to unauthorized guests and al-

Both boxes can perform end-point security audits to determine the level of trust to apply to the host and deny entry if it fails any test.

lowing admins to perform resource control management from one UI, not many.

As an additional benefit, admins can encrypt all traffic to the resources using SSL for better internal security. With all the encrypted traffic flying around, however, network monitoring and management tools won't be capable of correctly identifying and classifying the data flows. Monitoring tools that peer into TCP traffic will be blinded by the SSL packets, and routers and switches will have trouble identifying traffic to apply QoS policy. Use encryption wisely; it may not be suitable for everything.

Aventail EX-2500

The folks at Aventail have been building a great SSL VPN appliance for quite some time (infoworld.com/2181), and the current software release — Aventail ST (Smart Tunneling) — is no exception. I recently tested the EX-2500 with the latest software and found the features to be good enhancements to an already solid solution.

The EX-2500 is a new hardware platform for Aventail. It features a 1U chassis and scales to as many as 2,000 concurrent users per box. One of the more significant improvements is its capability of providing secure remote access to a wide range of mobile devices such as smartphones and PDAs. Aventail Mobile detects the device type at log-on and formats the display to fit the connected device. The feature can place the device into specific policy zones for access control.

Mobile supports BlackBerry, Palm, Windows Mobile, DoCoMo, and Symbian systems.

Another new feature, Aventail's Native Access Modules, provides access to Microsoft Terminal Services and Citrix applications via the appliance without a "fat" client installed on the remote device. I really like this feature because it allowed me to consolidate various Terminal Server connections into one browser-based portal and provided access from within the browser. In fact, instead of being tied to Internet Explorer, as Microsoft's Web-based Terminal Server client is, I easily connected using Firefox.

End-point security also improved with the addition of tools for more flexible application verification. Admins can now create end-point checks based on MD5 checksums, wildcards, and relative dates, allowing for even greater verification of host systems. This increased level of host checking allows for in-depth inspection of a client device to make sure it conforms to the established security policy. Aventail's dynamic, adaptive security engine then places the device in the appropriate policy based on how it fared during the host check.

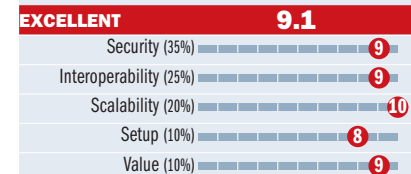
Through improved integration with Netegrity and RSA, Aventail ST also has better single sign-on support than in previous versions. Password management through the Web portal has also improved. In the past, if a user's password was going to expire, he or she would be notified at log-on but would have no means of

updating it. Now the password can be updated right through the portal, eliminating lock-out problems and help desk calls.

The EX-2500 with Aventail ST is a strong step forward in the ongoing evolution of the SSL VPN. It isn't missing any features and provides one of the best platforms for remote users, as well as exposed applications and resources. End-point control is good, and I like how it can fit into an overall internal security policy. Resource definition isn't as flexible as in the FirePass, but outside the most demanding situations, that should not be a problem. Look for its internal policy management to evolve into something that can give the big boys a run for their money.

F5 FirePass 4100

F5 Networks f5.com



COST: \$24,995, includes all services licensed for 100 concurrent users

PLATFORMS: OSes: Windows, Linux, and Mac, as well as BlackBerry, Palm, Windows Mobile, and various smartphones; browsers: Internet Explorer, Firefox, and minibrowsers

BOTTOM LINE: The FirePass 4100 is an excellent all-around SSL VPN appliance. It has all of the scalability an enterprise could want, and it supports a wide range of remote access options. Its end-point control Visual Policy Editor provides a flow-based view of creating log-on sequences that takes the guesswork out of the equation. Although there are some idiosyncrasies when creating Web application shortcuts, the overall functionality and customization more than make up for them.

F5 FirePass 4100

F5's FirePass is still one of the most complete SSL VPN solutions available. As does the EX-2500, FirePass provides a wide range of application and network support, including support for Unix and Windows file shares, X11 for Mac OS X, legacy "green screen" hosts, and various flavors of terminal services. FirePass also supports various browser types such as I-mode and WAP phones, as well as Pocket PC.

This release, Version 5.5, comes with enhanced and powerful end-point control that allows administrators to create various security policies based on the "who, what, and where" of the client. F5's end-point control provides the means for deftly handling host policy classification. FirePass works with nearly every anti-virus and personal firewall product on the market for maximum flexibility and security enforcement.

One of FirePass' brightest spots is the Visual Policy Editor. This tool graphically depicts each step of the log-on sequence and allows admins to craft end-point policy quickly. What I really liked about the policy editor is that I could not only create pre-log-on sequences but also post-log-on and remediation sequences. For example, if a host passed the initial verification steps and had a valid anti-virus program but its signatures were out of date, I could pass it to a page with information on updating its virus signatures instead of simply denying access.

For added scalability, a FirePass, or even a cluster of FirePasses, can offload SSL processing to an F5 Big-IP appliance. Moving this CPU-intensive processing to an appliance built for SSL tasks makes a lot of sense, and it allows the FirePass to serve a virtually unlimited number of users.

FirePass still isn't one of the easi-

est devices to set up and configure, but it does give ultimate control to administrators. Every aspect of the appliance, from SSL encryption strength to policy enforcement per access method, is exposed. And IPsec site-to-site tunneling is still available in the FirePass.

The FirePass is one of the best SSL VPN appliances available. It has exceptional access support and an excellent end-point control engine. SSL offload to the Big-IP appliance is a major plus, and the flexibility in the policy enforcement is first rate. Resource definition almost provides too many choices, and it could more fully support Linux and Mac users. But for the most part, there isn't any scenario that the FirePass can't handle.

SSL VPNs will continue to evolve and expand their roles in network security. Both Aventail and F5 are paving the way with tighter policy and host integration; look for the

SSL VPNs The F5 edges out the Aventail in its broader support for third-party security products and better scalability. The Aventail, however, boasts superior support for third-party security products.

	Supported end-point security platforms	Pre-/post-host-scan authentication	Supported third-party end-point security products	VLAN support	Maximum nodes per cluster (without external hardware)	Number of NICs	Supported connections for application tunneling	Web access rewrites vs. translates HTML	Full layer 3 tunnel	FIPS 140-2 compliance
Aventail EX-2500	Windows, Mac, and Linux; BlackBerry, Palm OS, Windows Mobile, DoCoMo, and Symbian portables	Pre	WholeSecurity, ZoneLabs	No	Two	Two 1Gbs	Java/ActiveX/Win32	Translates	Yes	Yes
F5 Firepass 4100	Windows; BlackBerry, Palm OS, Windows Mobile, and various smartphones; limited support for Mac and Linux	Pre	More than 100 products	Yes	10	Four 1Gbs	Java/ActiveX	Rewrites	Yes	Yes

shift to internal protection to continue. I really like the overall flexibility and functionality of the FirePass 4100. It provides exceptional scalability, and the Visual Policy Editor makes it easy to understand the pre-

and post-log-on process. Avenail's EX-2500 is easier than FirePass to deploy and now includes native Citrix and MS Terminal Server support. The EX-2500 is a very capable performer that just doesn't quite

scale like the 4100.

Will SSL VPNs take over internal network security? Only time will tell, as more security features are stuffed into these already-bursting devices.

— Keith Schultz

