THE TOLLY GROUP

No. 204133 June 2004

Aventail Corp.

Aventail® EX-1500™

Competitive SSL VPN Feature Analysis versus F5 Networks FirePass 1000 and Juniper Networks NetScreen-SA EA150

1989 - 2004 15 Years TOLLY

Test Summary

Premise: *SSL VPNs are rapidly taking the place of traditional IPSec VPNs for remote access and extranet use. Secure Sockets Layer (SSL) VPNs offer greater scalability and flexibility with proven security. SSL VPN vendors combine SSL encryption and proxy technology to increase user productivity by providing authorized users with access to corporate applications and data from any Internet browser, while reducing administration through centralized management of access policy. Yet all SSL VPN products are not alike. Users need to understand the depth of feature/function support and how it impacts the benefits they expect from their SSL VPN solution: breadth and ease of end-user access and productivity; ease of administration to manage access control policy; and security.*

Aventail Corp. commissioned The Tolly Group to evaluate its Aventail® EX-1500™, an SSL VPN appliance that provides users with clientless[1] access from any PC with Internet access to the network applications and resources they need to be productive. The Tolly Group examined the feature/functionality of the EX-1500 versus F5 Networks FirePass 1000 and

[1] "Clientless" means that no software beyond a standard browser and, for client-server applications, a Java Run-time Environment, needs to be pre-installed on the client. All needed "intelligence" is downloaded at session initiation.

Test Highlights

- Delivers a broader feature set, with richer capabilities, than either of the other SSL VPN appliances tested
- Offers the most complete directory integration of the appliances tested, dynamically controlling access based on all of a user's current group memberships
- Serves up the most secure SSL VPN solution when compared with either of the other SSL VPN appliances

Access Control Policy Feature Validation

TV Certification Number	Feature[1]	Aventail EX-1500	Juniper Networks NetScreen-SA EA150	F5 Networks FirePass 1000
10760	Dynamic Group Mapping – Active Directory	P	P	P
10761	Multiple Group Membership – Active Directory	P	P	F
10762	Access Management at Windows Domain Level	P	F	F
10763	Access Management at Windows Share Level	P	P	P
10764	Access Management at Full Path Level	P	F	F
10765	Resource Request Auto-translate – Fully Qualifed Domain Name	P	P	P
10766	Resource Request Auto-translate – Short Host Name	P	P	P
10768	Resource Request Auto-translate – Alternate DNS Name	P	P	P
10769	Policy Management via Global Alias	P	F	F

[1] A failing grade indicates that a product either did not support the feature or the product did not meet the requirements for feature validation.

Source: The Tolly Group, June 2004 *Figure 1*

Juniper Networks NetScreen-SA EA150, both SSL VPN appliances. The NetScreen-SA EA150 uses the same software distribution (Ver. 4.0 Patch 1 Build 5871) – available on Juniper's Web site, as the NetScreen-SA1000, which is the currently available model.

Tolly Group engineers compared the feature/functionality of the three SSL VPN products in three categories: Access control policy, end-point security and system security. All three products were subjected to a battery of feature validation tests as defined under The Tolly Group's Tolly Verified certification program. Engineers examined the products during May and June 2004.

Overall, Tolly Group engineers found that the Aventail EX-1500 offers the most robust set of features/functions of the three products. On the access control side, the EX-1500 supported all nine of the features engineers examined, and even when other vendors matched the feature availability, the EX-1500 offered more robust functionality that makes management simpler. On the end-point security side, again the EX-1500 offered every feature examined, while the other products failed 20% or more of the tests. And in the system security validation, the EX-1500 again offered support for all three features, while rival products only offered a subset.

End-point Security Feature Validation

TV Certification Number	Feature[1]	Aventail EX-1500	Juniper Networks NetScreen-SA EA150	F5 Networks FirePass 1000
10751	Client Session Cleanup – Browser History	P	F	P
10752	Client Session Cleanup – Browser Cookies	P	P	P
10753	Client Session Cleanup – Temporary Files	P	P	P
10770	Client Session Cleanup – Email Attachments	P	F	P
10771	Client Session Cleanup – Downloaded Files	P	F	F
10772	Client Session Cleanup – Autocomplete Passwords	P	F	P
10773	Client Session Cleanup – Complete Removal Irrespective of Session Termination Cause	P	F	P
10774	Trigger for Client Cleanup – Explicit Logoff	P	P	P
10775	Trigger for Client Cleanup – Timeout	P	P	P
10776	Trigger for Client Cleanup – Browser Close	P	F	P
10777	Local Data Encryption	P	F	F
10778	Prevention of Local File Save or Copy	P	F	F
10779	Data Protection in the Event of System Failure	P	F	P
10780	Non-recoverable Deletion of Session Data	P	F	P

[1] A failing grade indicates that a product either did not support the feature or the product did not meet the requirements for feature validation.

Source: The Tolly Group, June 2004 *Figure 2*

Results

Access control policy validation

The Tolly Group verified the feature availability/functionality of nine access control options. The Aventail EX-1500 was the only product that offered support for all nine features examined by engineers. (See Figure 1.)

Moreover, even though the two competitive products examined matched the Aventail EX-1500 in some feature areas, engineers found a sizable difference in the way the features were implemented and the corresponding functionality they deliver. Engineers also found the Aventail EX-1500 management interface easier to understand and to configure than the other two appliances tested.

One case in point was with the Dynamic Group Mapping – Active Directory feature as defined by Tolly Verified (http://www.tolly.com/TV/ProgDetail.aspx?ProgramID=10760). Here engineers established that the SSL VPN appliance dynami-

cally queries Microsoft Active Directory to determine group membership of system users. With Aventail's EX-1500, user and group changes to the directory are automatically recognized. On another front, the Aventail EX-1500 supports Multiple Group Memberships for Active Directory. That means a user may be in more than one group, each with varying privileges, and the EX-1500 uses both group memberships concurrently. By contrast, the FirePass 1000 supports only a single group membership at any given time, making it harder for the administrator to use an existing directory or requiring the user to log on with different credentials to get access to different resources.

There were several features that the Aventail EX-1500 offered that rival products did not. For instance, the EX-1500 supports Access Management at Windows Domain Level. A system that provides this level of management allows an administrator to simply control access for an entire Windows Domain within a large corporate environment, without having to list each server. This improves the ease and scalability of security management.

Also, the EX-1500 offers Access Management at Full Path Level. A system that provides this level of management allows an administrator to control access at a very granular level, even to a directory or file, which strengthens security policy.

The EX-1500 delivers Policy Management via an object-based policy model. This makes security management significantly more efficient by allowing system managers to avoid having to find and manually update all occurrences of a resource when making a change.

Aventail Corp.

Aventail EX-1500

Tolly Verified Feature/Functionality Evaluation

End-point Security

Engineers tested 14 end-point security features that implement security at the user level. With SSL VPNs, users have the freedom to access corporate resources from a variety of untrusted systems, including home PCs, public kiosks at airports and trade shows, courtesy PCs in libraries and hotels, as well as PDAs and corporate laptops.

The SSL VPN products evaluated implement a level of security to

Aventail Corp.
Aventail EX-1500
Product Specifications*

Clientless anywhere access

- Broadest device and platform support
- Broadest range of access options
- Secure access to enterprise applications
  - Web applications
  - Client-server applications
  - Windows file shares
- Single sign-on adapters

End-point control

- Aventail Cache Control (data protection)
- Aventail Secure Desktop (advanced session protection)
- Application detection
- Source IP and digital certificate
- Integration with personal firewall, host integrity, and anti-virus products

Policy and security

- SSL encryption
- Network and device protection
- No direct connections to the network
- Authorization by user, group, realm, source, destination, time
- Object-based policy model

Manageability, reliability, and scalability

- Web-based management console
- Support for all popular directories and authentication methods
- High availability cluster with built-in load balancing and stateful failover
- Monitoring, logging, auditing, and reporting

For more information contact:
Aventail Corp.
808 Howell St.
Seattle, WA 98101
Phone: (206) 215-1111 or
1 (877) AVENTAIL (U.S.)
E-mail: info@aventail.com
URL: http://www.aventail.com

**Vendor-supplied information not verified by The Tolly Group*

System Security Feature Validation

TV Certification Number	Feature [1]	Aventail EX-1500	Juniper Networks NetScreen-SA EA150	F5 Networks FirePass 1000
10781	Default Access - Secure	P	P	P
10783	Secure Session Cookies	P	F	P
10784	Dynamic Validation of Certificates	P	F	F

[1] A failing grade indicates that a product either did not support the feature or the product did not meet the requirements for feature validation.

Source: The Tolly Group, June 2004

Figure 3

deal with those untrusted access devices to mitigate the risks of sensitive corporate information being stored locally to cache, saved to a hard drive, or left open for unauthorized users to view.

SSL VPN security products tested offer varying degrees of features to cleanse caches, sweep for stored Web cookies or files, and guard against corporate resources being exposed.

First, engineers examined a number of features that focus on cleanup of client sessions and the residual files, cookies, passwords, browser history and other items the SSL VPN session may leave behind. Tests show that Aventail® Cache Control™ removed the session data completely upon termination of the session irrespective of how the termination occurred.

Aventail Secure Desktop provides additional data protection. Any files viewed or downloaded on a PC client are written to an encrypted data store, which is completely erased at the end of the session. Unlike products that only delete the browser cache, this capability provides comprehensive real-time protection for SSL VPN sessions.

Even though all three products offered a specific cache-cleaning feature, the usefulness of the feature varied considerably from product to product. Case in point: The Tolly Group's examination of the feature, Trigger for Client Cleanup – Explicit Logoff. Engineers used this test to confirm that a specified event will trigger the client security cleanup process to run. While all three products supported the feature, only the Aventail EX-1500 and its Cache Control delivered a full client cleanup, whereas the Juniper/NetScreen-SA EA150 left behind the cookies and temporary files.

There were a number of end-point security tests that the Aventail EX-1500 passed but the two rival products failed. (See Figure 2.) For instance, in the Local Data Encryption test, engineers found that, while a protected SSL VPN session is in progress, working data (e.g., an MS Word file being viewed by the user) cannot be accessed by another person having simultaneous access to the client PC hard drive. This capability provides for use of the SSL VPN solution in a non-secure, "public" environment like a kiosk, hotel or library-based PC. Both the Juniper and the F5 Networks products failed this test.

Both the Juniper/NetScreen and the F5 Networks products also failed a Tolly Verified test for Prevention of Local File Save or Copy. This test confirms that the tested appliance can prevent the client PC user from accidentally or intentionally saving a file locally to fixed or removable media. The Aventail EX-1500 passed this test.

In a test for Non-recoverable Deletion of Session Data, engineers sought to confirm that data deleted during the session cannot be recovered via "Undelete" utility programs. Engineers used a

free software tool named "Final Recovery" version 1.3 to trace the deleted files. The Aventail EX-1500 passed this Tolly Verified test, as engineers were not able to trace any of the downloaded files after the Cache Control ran. The FirePass 1000 also passed the test. This capability prevents corporate data from being recovered from SSL-VPN sessions. Test results also show that the Juniper/ NetScreen-SA EA150 is less secure than the Aventail EX-1500. The Juniper/ NetScreen product, for instance, left deleted files in the Windows "recycle bin." The FirePass 1000 also did this by default, requiring the administrator to configure a more secure behavior.

System Security

In the system security tests, the Aventail EX-1500 was the only product tested to pass all three tests.

All of the products tested passed the basic Default Access – Secure test that confirms that the default policy mode for clients accessing the tested appliance is to deny access unless explicitly permitted.

Only the Aventail EX-1500 passed the Tolly Verfied test for Server Certificate Validation, which is designed to confirm that the tested appliance can dynamically verify the validity of certificates associated with resources and deny connectivity when an invalid certificate is encountered. (See Figure 3.) This test has implications for corporate users since passing the test assures buyers that the product can detect a "man in the middle" attack inside the enterprise network, preventing theft of passwords or sensitive data.

Saving session cookies to the client may provide an attacker who has access to the system with the information needed to hijack a user's session in progress. Tolly Engineers verified that that the Juniper/NetScreen product did write session cookies to the client hard disk.

Analysis

All of the products in this feature comparison offer basic SSL VPN capabilities. But enterprise network decision makers often require more than just basic services; they need a cohesive set of access control and security functions that provides a high level of SSL VPN security and meshes with enterprise security needs and policies.

Of the three products examined, the Aventail EX-1500 delivered the combination of SSL VPN services most likely to be needed by enterprise users. The Aventail EX-1500 offered the broadest set of features/ functions tested. Perhaps more importantly, even though the F5 Networks and Juniper Networks products may have matched the Aventail EX-1500 on a feature-by-feature basis in some cases, tests show that the Aventail product often has a more powerful and secure implementation of the feature that provides greater functionality for users and mitigates risk for IT managers.

Finally, while The Tolly Group tested the Aventail EX-1500 with ASAP Platform 7.1-beta software, the company has since shipped version 7.1.

Test Configuration and Methodology

The Tolly Group tested an Aventail EX-1500, Version 7.1.0-24. Tests also focused on a Juniper Networks NetScreen-SA EA150, System software version 4.0 Patch 1 (Build 5871) and an F5 Networks FirePass 1000 Version 4.0.2, FirePass Build URM-4.0-20031213. (The F5 networks retest was done with FirePass Version 4.1.1, FirePass Build URM-4.1-20040224.)

For the test bed (See Figure 4), each SSL VPN appliance was configured with two interfaces – one to the external network to provide access for a remote user, and another to the internal network to provide access to resources.

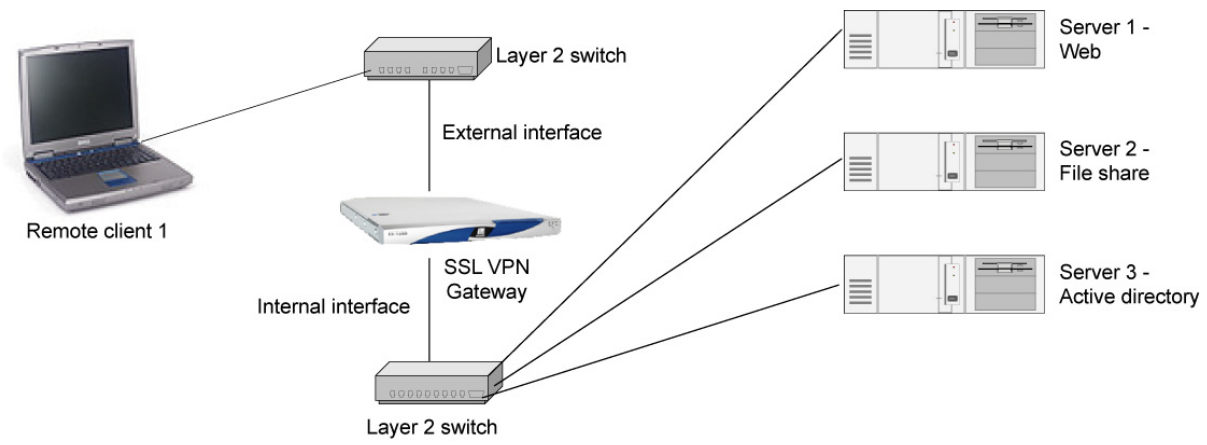
All test methodologies for Tolly Verified tests are available on the Tolly Group Web site at: http://www.tolly.com/TV/TV_home.aspx. Testing for the end-point security section was conducted using a Microsoft Windows Professional XP SP1 client running Microsoft Internet Explorer V6.0.

Equipment Acquisition and Support

Both the F5 Networks FirePass 1000 and the Juniper Networks NetScreen-SA EA150 products were acquired through normal product distribution channels. The Tolly Group contacted executives at the vendor companies and invited them to review and to comment on the Tolly Verified test results.

Officials from F5 Networks disputed some test results, noting that a more current software version than used in testing is available with some of the features/functions tested. F5 Networks worked diligently with The Tolly Group to retest with that updated software and demonstrated

Test Bed



Source: The Tolly Group, June 2004

Figure 4

that some functions that initially failed do indeed work with the software update. F5's test data in this report represents the retested results.

Officials from Juniper/NetScreen engaged in a dialog with The Tolly Group for two calendar weeks to resolve testing issues.

Juniper/NetScreen elected not to provide an official response concerning its product performance.

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Finisar Corp.	Surveyor ver 5.0	http://www.finisar.com

Tolly Group Services

With more than 15 years of testing experience of leading-edge network technologies, The Tolly Group employs time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy. Plus, unlike narrowly focused testing shops, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure. The company offers an unparalleled array of reports and services including: Test Summaries, Tolly Verifieds, performance certification programs, educational Webcasts, white paper production, proof-of-concept testing, network planning, industry studies, end-user services, strategic consulting and integrated marketing services. Learn more about The Tolly Group services by calling (561) 391-5610, or send E-mail to sales@tolly.com.

For info on the Fair Testing Charter, visit: http://www.tolly.com/Corporate/FTC.aspx

Project Profile

Sponsor: Aventail Corp.
Document number: 204133
Product class: SSL VPN appliance
Products under test:

- Aventail EX-1500 with ASAP Platform 7.1-beta
- Juniper Networks NetScreen-SA-150, System software version 4.0Patch 1 (Build 5871)
- F5 Networks FirePass 1000 Version 4.1.1, FirePass Build URM-4.1-20040224

Testing window: May 2004 to June 2004
Software status:

- Aventail EX-1500: Beta version tested; ASAP 7.1 is generally available
- Juniper/NetScreen-SA EA150: Generally available
- FirePass 1000: Generally available

For more information on this document, or other services offered by The Tolly Group, visit our World Wide Web site at http://www.tolly.com, send E-mail to sales@tolly.com, call (561) 391-5610.

The Tolly Group doc. 204133 rev. clk 28 June 04