



The authoritative, unbiased source for IT certification, research and testing



WHITE PAPER

September 2005

A white paper
commissioned by
Check Point
Software
Technologies

Document #205132

SSL VPN Gateways: Delivering Superior ROI With Integrated Security

*Check Point Proactively Guards
Against More Remote Access SSL VPN
Attacks in a Single Gateway for
Greater ROI than Cisco, F5 or Juniper*





Terms of Usage

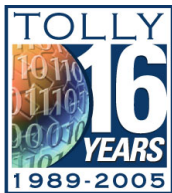
Entire contents © 2005 The Tolly Group, Inc. All rights reserved.

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, this document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information. When foreign translations exist, this English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

Tolly Group Vendor Services



With more than 16 years experience validating leading-edge Information Technology products and services; [The Tolly Group](http://www.tolly.com) has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.

The Tolly Group's flagship service is its Tolly Up-To-Spec testing brand. Users or vendors commission The Tolly Group to benchmark the performance characteristics, or assess the features and functions, of a single product, or a group of competitive products. Such independent product assessments provide users with an objective view of a product or group of products and validate vendor claims. See the Tolly Group's Web site at <http://www.tolly.com>.

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document was authored by:

Charles Bruno,
Executive Editor
The Tolly Group

Table of Contents

5	Robust and Intelligent Security
7	High-Level Findings
9	Total Cost of Ownership
12	Intelligent Approach to Security
14	Appendix A. Tunnel Attacks
14	Oversized PING Attack
14	Network Quota DoS Attack
15	FTP Bounce Attack
16	Server Message Block Attack
16	Domain Name Service UDP Enforcement Attack
18	Appendix B. Web Attack Tests
18	Buffer Overflow Attack Test
19	Command Invocation Vulnerability Test
19	Cross-Site Scripting
20	SQL Injection Attack
20	Command Injection Attack
21	Directory Traversal Vulnerability Test
22	HTTP Protocol Vulnerability Test
23	WebDAV Extension Attack
25	Appendix C. Devices Under Test
26	Appendix D. Test Tools Utilized
27	Appendix E. Competitive Vendor Interaction

List of Figures

- 7 Figure 1: Tunneling and Web Attack Results
- 10 Figure 2: Total Cost-of-Ownership Comparison of Comprehensive Remote Access Security Solution
- 14 Figure 3: Oversized PING Attack Test Results
- 15 Figure 5: FTP Bounce Attack
- 15 Figure 4: Network Quota DoS Attack
- 16 Figure 6: Server Message Block Attack
- 17 Figure 7: DNS UDP Enforcement Attack
- 18 Figure 8: Malicious Code Protector
- 19 Figure 9: General Worm Catcher
- 19 Figure 10: Cross-Site Scripting Attack
- 20 Figure 11: SQL Injection Attack
- 21 Figure 12: Command Injection Attack
- 22 Figure 13: Directory Traversal Attack
- 23 Figure 14: HTTP Compliance
- 24 Figure 15: WebDAV Extension Attack

SSL VPN Gateways: Delivering Superior ROI With Integrated Security

Robust and Intelligent Security

With the emergence of secure Web browsing via Secure Sockets Layer (SSL) coupled with virtual private networks (VPNs), vendors rushed to market to capture the mindshare and the market share of a business consumer base anxious to provide secure access via the Web to telecommuting users, business partners and suppliers.

As SSL VPN products hit the market, differences began to emerge. Some vendors believed that once clients were authenticated into the network they should have free reign. A smaller number of vendors believe that intentional or unintentional mischief can occur across the connection after authentication has taken place.

Consequently, a number of SSL VPN products on the market today focus their security on providing basic SSL VPN tunnel connectivity services and optional client endpoint security. These SSL VPN appliances assume that once the user is authenticated and granted access to the corporate backend, that there is little need for monitoring a VPN tunnel or a Web transport for threats.

The problem with this approach is that often internal applications are not security hardened as they were never intended to be exposed to the outside world. SSL VPN remote access is about making internal resources available outside the corporate walls, therefore the dynamics have changed wherein application, Web, and endpoint security have become important for the security-conscious enterprise.

SSL VPNs access the network level, not only Web applications, which is why network-level security becomes a concern beyond the Web for protocols such as FTP, DNS, MSFT file shares, etc. These are protocols that now are at the mercy of viruses, malicious code and spammers.

Hackers and spammers have changed tactics. Their focus now is not just on infecting the client, but using the network as a transport to carry infected Trojan programs and other malicious code to the applications and the servers that house them along with mission-critical data. SSL VPN gateways offer a line of protection much like firewalls, and if breached, the risk of damage to network, system and application resources is enormous. This is precisely why Check Point believes it is

imperative for any SSL VPN solution to deliver a broad breadth of security services – for the SSL VPN client, for the network transport and to protect those precious backend assets.

There are two basic modes of SSL VPN access – one being the "secure browser" Web application interface and the other being the pure "VPN" network transport-level (tunnel) access.

Inspection is an extremely important element for inclusion on any SSL VPN gateway, regardless of access type. In situations where there are perimeter firewalls required for deep inspection, the application inspection is rendered virtually useless due to the encrypted packets. In situations where there is an internal firewall, the decrypted packets coming from the SSL VPN gateway allow inspection, but any user context associated with the traffic is void as the firewall just sees that there is decrypted traffic coming from the SSL VPN gateway. This would make any forensics or logging useless for tracking a malicious user. Worse, if an internal application uses SSL then all traffic passed to the application completely bypasses perimeter inspection.

In essence, SSL VPN security for any size company requires robust and intelligent security.

Unlike vendors that focused their SSL VPN offerings on basic SSL VPN connectivity only, Check Point Software Technologies, Inc. took an approach with its Connectra SSL VPN gateway that held that all traffic should be inspected – from the endpoint all the way to backend servers and applications. Connectra is a complete Web security gateway that provides both SSL VPN remote access and integrated intrusion protection in a single, unified security solution. Unlike some SSL gateways, Check Point's Connectra contains IPS functionality which is updateable in real-time. So, in addition to the traditional Web and network functions of an SSL device, Connectra also detects and blocks attacks, offering real-time security capabilities for endpoints and for application security.

Check Point commissioned The Tolly Group to validate the security and functionality claims the company has made concerning the Connectra SSL/VPN appliance. In total, 13 tests were conducted in August 2005 at a Check Point lab in Tel Aviv, Israel, and validated on-site by Tolly Group personnel. These tests are representative of the types of activity SSL VPN gateways likely would encounter.

Engineers determined whether a given device would detect and stop particular, well-known attacks introduced over either the Web or network transport connection of the SSL VPN under test. Check Point's Connectra NGX was tested (on a pass/fail basis) against three other SSL VPN products: F5 Networks, Inc.'s FirePass 1000, Cisco Systems Inc.'s VPN Concentrator 3005 and Juniper Networks, Inc. NetScreen-SA 1000. (See Appendix C. Devices Under Test, page 25.)

The Tolly Group invited all three competitive equipment vendors to participate in the testing, and offered them the opportunity to review and comment on the test methodology and review and comment on the test results. Only Cisco requested a copy of the test methodology, but did not comment on it. Moreover, while The Tolly Group shared test results with all three vendors, only F5 Networks responded. (See Appendix E: Competitive Vendor Interaction, page 27.)

Tests were divided into two groups: Tunneling attacks and Web-borne attacks. The tunneling attacks simulated what would happen as remote users attempted to login and use backend corporate computing resources over an SSL VPN tunnel. The Web attacks represent possible threats corporations would encounter as users access corporate data via Web-based applications. In each case, the four SSL VPN products tested were evaluated on a pass/fail basis.

In addition to verifying gateway capabilities claims, The Tolly Group examined, at a high level, the return on investment of Connectra NGX versus the rival products tested.

High-Level Findings

Figure 1: Tunneling and Web Attack Results

Tunneling and Web Attack Test Results					
Test	Security advisory #	Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
Oversize PING attack	CA-1996-21				
Network quota Denial-of-Service attack	Multiple advisories				
FTP bounce attack	CA-1997-27				
Server Message Block (SMB) attack	CA-2003-08				
Domain Name Service (DNS) UDP Enforcement attack	Multiple advisories				
Malicious code protector	MS02-028				
General worm catcher	CA-2001-26				
Cross-site scripting attack	CAN-2005-2735				
SQL injection attack	CAN-2004-1519				
Command injection attack	CAN-2005-0239				
Directory traversal	CAN-2003-0676				
HTTP compliance	CAN-2004-2035				
WebDAV extension attack	CAN-2005-1274				

= Pass = Fail

Tests show that within the scope of attacks used for this round of testing, Check Point's Connectra NGX offers much greater depth of protection over SSL VPN links than any of the other three products.

In tunneling attack tests, Connectra NGX passed all five tests. That is, Connectra NGX was able to detect the attack and stop it, while the other products failed four out of the five tests, or in the case of the FirePass 1000, failed three of the five tests. (See Figure 1.) Complete details of the tunneling tests are available in Appendix A, page 14.

In the Web attack tests, Connectra NGX passed all eight tests. Both the F5 FirePass 1000 and the Juniper NetScreen-SA 1000 failed seven out of eight tests, and the Cisco VPN Concentrator failed all eight tests. Complete details of the Web attack tests are available in Appendix B, page 18.

Tests results underscore a basic philosophical difference in the architectures of the tested products. Check Point integrates endpoint security with extensive gateway-based security facilities that focus on protecting the network transport, guard against application attacks and protect backend Web servers and applications from network-borne threats.

F5, Cisco and Juniper, on the other hand, focus their products almost exclusively on delivering basic SSL connectivity and some endpoint security via third-party relationships. Once the user is authenticated, there is little these devices do to monitor the network connection, or protect servers and applications. Instead, these vendors often rely upon the introduction of a second device, married to the SSL VPN gateway, such as an IPS, to provide capabilities that Check Point integrates into a single device.

Naturally, this has enormous implications for cost of ownership, and for managing the integrated solution.

Total Cost of Ownership

The architectural differences between Check Point's Connectra NGX and the competitive devices tested paint a dramatic contrast with regards to the performance and security functionality users can deploy.

That contrast between the products comes sharply into focus as users examine the upfront and ongoing cost-of-ownership issues regarding Connectra NGX and the trio of rival devices tested.

The integration strategy embraced by Check Point with Connectra NGX pays off handsomely for users on several fronts:

- Upfront capital costs (for the gateway and management functions) is less with Connectra NGX
- Operational and maintenance costs are lower with Connectra NGX
- Security updates are less costly with Connectra NGX
- Endpoint security is less costly to deploy and manage

Purely from a hardware deployment cost perspective, Connectra NGX offers a compelling case since it offers a fully integrated package with SSL VPN connectivity, robust endpoint security and backend server and application security functions. Connectra also includes unified management across all Check Point solutions as well as real-time update services.

For each of the products tested, The Tolly Group examined the upfront hardware/software costs, plus annual maintenance/support costs for a 100-user configuration. In instances where products did not offer intrusion detection/prevention capabilities, The Tolly Group factored in the cost of an intrusion prevention system (IPS).

The cost of the Check Point Connectra 1000 solution, was \$24,725, which broke down to \$15,000 for the SSL VPN gateway, \$1,000 for the SmartDefense Advisory Service, \$5,500 for endpoint security software, and just over \$3,000 for a support contract.

Competitive solution costs ranged anywhere from 9% higher to almost three times the cost of the Check Point Connectra solution.

Cisco's tandem solution of a VPN Concentrator 3020 and a Cisco IDS 4215 cost \$26,943 - with \$8,000 of that price going to the intrusion detection functionality that already is bundled into the Connectra 1000. Moreover, Cisco's support cost is 22% higher than the Connectra 1000 support pricing.

The Juniper Networks NetScreen-SA 1020/Juniper IDP-50 tandem cost a whopping \$47,167, or more than 90% higher than the Connectra 1000 pack-

age. Here, the SSL VPN gateway costs about the same as the Connectra 1000, but users have to kick in another \$16,000 for an IPS and network/application extension option. And since Juniper doesn't offer its own endpoint software, users would pay over \$10,000 for third-party software.

Finally, the F5 Networks FirePass 1000, bundled with a TrafficShield 4100, would cost users just over \$70,000, or nearly three times the cost of the Check Point solution. Not only do users pay a premium for the SSL VPN gateway, but the \$39,995 cost of the TrafficShield firewall/IPS raises the F5 solution price considerably. Moreover, the \$7,205 cost for support is by far the highest of all support costs and more than double what Check Point charges.

Figure 2: Total Cost-of-Ownership Comparison of Comprehensive Remote Access Security Solution

Total Cost-of-Ownership Comparison of Comprehensive Remote Access Security Solution (List Prices for 100 Concurrent Users)				
Gateway	Check Point Connectra 1000	Juniper SA-1020 and Juniper IDP-50	F5 Firepass 1000 and TrafficShield 4100	Cisco 3020 Concentrator and Cisco IDS 4215
SSL VPN	\$15,000	\$14,995	\$19,990	\$14,995
IPS	Included	\$8,995	\$39,995	\$8,000
Network/ Application extension	Included	\$6,995	\$2,995	N/A
Subscription Services				
SSL VPN gateway	SmartDefense Service \$1,000	Not Available	Not Available	Not Available
IPS update services		Included	Not Available	Included
Endpoint Security				
Endpoint security	Integrated Integrity Clientless Security -- 100 concurrent users \$5,500	Third-party software -- List based on \$104 per user (100) \$10,400	Basic functionality included	Cisco Secure Desktop (included)
Support				
SSL VPN	\$3,225	\$5,782	\$7,205	\$3,948
IPS maintenance (Including software updates)				
Endpoint security				
Totals	\$24,725	\$47,167	\$70,185	\$26,943

Note: Prices were obtained from vendor sales lists; all prices are in U.S. dollars.

Tests show that the cost-of-ownership issues extend well beyond implementation pricing. The rival devices tested lack the depth of functionality offered by Connectra NGX. In fact, Cisco, Juniper and F5 need to sup-

plement their respective SSL VPN solutions with an IPS in order to secure the same amount of applications that Connectra NGX can with Check Point's Application Intelligence and Web Intelligence.

The total cost for the F5, Juniper and Cisco solutions increases when buyers add in the cost of a supplemental IPS in addition to an F5 FirePass, Juniper NetScreen-SA or Cisco VPN Concentrator. Both the Cisco IDS, the Juniper IDP, and the F5 Firepass with TrafficShield, require separate management and online update systems which further increase the total cost of their solutions.

Another cost advantage in favor of Check Point Connectra is that the company includes Web Intelligence in the gateway. Web Intelligence, with Malicious Code Protector, inspects Web content and embedded application code. Essentially, it is Web application firewall technology for Check Point products. Among other tasks, it guards against:

- SQL Injection
- Command Injection
- HTTP Format Sizes
- Allowed HTTP Methods
- HTTP Header Spoofing

By contrast, with F5's FirePass, users only have limited Web protection. Both Cisco and Juniper do not offer Web protections, although they both recently purchased the technology through acquisitions; it is still unclear when, how, or at what cost these acquisitions will be integrated into their SSL VPN solutions.

In addition to Web protection, Check Point incorporates integrated endpoint security in Connectra NGX. Cisco, Juniper and F5 offer some minimal endpoint security features such as host checking, cache cleaning, and enforced policy compliance, but they require the integration and purchase of separate third-party solutions at a much higher cost to have an equivalent level of endpoint security to Connectra.

One of the key cost-of-ownership points pertaining to Connectra NGX is that Check Point's integrated intrusion prevention allows for single-box protection with extensive protocol protection. The other SSL VPN solutions tested require two gateways – one for SSL VPN protection and one for IPS protection – and two management systems. Check Point's SMART management system can manage all Check Point gateways. Ultimately, this reduces the administrative overhead associated with managing two devices.

Finally, from a TCO perspective, Check Point's SmartDefense provides a single update service mechanism. Cisco does not offer an update service for its VPN concentrator, but does for its IPS offering; Juniper offers only one update service for its IPS service.

Intelligent Approach to Security

In today's rapidly changing security landscape, users need an enterprise-class security solution that delivers multiple services from a single platform. This helps curb costs dramatically and simplifies day-to-day management of the network, and helps make the network perimeter more responsive, and even proactive, against new attacks.

Testing validated by The Tolly Group shows that Check Point's Application Intelligence provides protection for a greater number of applications than F5, Cisco or Juniper offer in their SSL VPN gateways.

Test show that the Check Point Connectra NGX provides three levels of SSL VPN security compared to rivals unidimensional security approach:

- Network layer security for IP ICMP and TCP
- Application layer security for FTP, DNS protocols, Microsoft protocols and preemptive worm protection
- Stateful inspection

Of the competitive devices tested, F5's FirePass 1000 appears to offer limited Web protection and some network-level protection. Cisco's VPN Concentrator 3005 contains minimal application-level inspection methods. And Juniper Networks' NetScreen-SA 1000 ignores mission-critical applications.

By contrast, Connectra NGX provides a plethora of Web protection including:

- Buffer overflow
- Cross-site scripting preemptive protection
- SQL/LDAP/Shell injection preemptive protection
- Directory listing preemptive protection
- Header spoofing preemptive protection
- Directory traversal preemptive protection
- ASCII-only header encoding enforcement

Further, when buyers compare endpoint security offered by the tested gateways, they'll find that Connectra NGX utilizes Check Point Integrity Client Security (ICS). ICS delivers a range of endpoint security far richer than the other devices tested. Case in point: Check Point's integrated malware/spyware detection with remediation help for worms, Trojans, hacker tools, keystroke loggers, adware, browser plug-ins, dialers, third-party cookies, spyware, and heuristic and signature rules.

ICS also is integrated into Connectra and does not require the use of external servers, which is required by some vendors who license the technology.

ICS features an Integrity Secure Browser (ISB) that continuously encrypts local cache in case there is an abrupt session termination (ie. The computer is switched off in mid-session), the cache will be unavailable. (Note: The Tolly Group did not test endpoint security features for this report.)

ICS delivers flexible restrictions for policy enforcement levels and does not require a dedicated server for management.

Juniper, Cisco, and F5 all purport to offer some sort of minimal host checking, cache cleanup, and policy enforcement, but additional endpoint security depth requires the integration of third-party endpoint software solutions that have separate management servers and interfaces at a much higher cost, which increases TCO, deployment, and management complexity.

On another front, tests show Check Point's Connectra NGX offers better access control than the other products tested. Connectra NGX was the only product tested that does not use port forwarding for remote access to applications. Port forwarding can allow worms and unauthorized file share access.

Additionally, Check Point's Connectra NGX is compelling because SmartDefense updates are added to the gateway in real time, including protections for new protocols. The gateway does not require major OS/hardware upgrades to add support for new protocols.

Finally, Check Point offers a better value and more compelling cost-of-ownership story than the other gateways tested. Connectra NGX is an integrated platform, and does not require integration with a second IPS product to expand security coverage, unlike some of the other devices tested.

Moreover, the single integrated package means users deploy and manage a single device, which reduces administrative overhead and results in management cost savings.

Users looking for a multifunctional, reliable security gateway for SSL VPN connections will find Connectra NGX a capable device architected to support a broad range of security needs both on network endpoints, for the security of network transports and SSL tunnels, and for protection of backend servers and network applications. And that's not some marketing hype; it's evidence based on solid hands-on testing of all three products. It's just a fact.

Appendix A. Tunnel Attacks





Oversized PING Attack



Oversize PING is a large-sized ICMP "PING" request that can crash the target computer. It is caused by sending an excessively long ICMP echo request data payload. Engineers set up and configured each device under test (DUT) to block any suspicious attack. Engineers then checked the Web security logs to verify that each DUT blocked the attack. The PING payload was set to 65,354 bytes.

The testbed environment was designed to simulate the most common type of customer deployment — a client at an Internet kiosk accessing the SSL-VPN appliance which is located at the company's DMZ via the Internet. After successful authentication, the SSL-VPN appliance acts as a gateway to the internal company network, thus providing access to internal Web applications, mail and file servers.

All scenarios developed for this benchmark simulate an authenticated client who is granted access to the company's network. Each test described in this document refers to a possible attack that a user can issue remotely against the company's internal network in order to elevate his privileges, access unauthorized resources or disrupt network or application availability.

Figure 3: Oversized PING Attack Test Results

Oversized PING Attack Test Results			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

For this test, a PING was sent from a client to a target across the SSL VPN gateway, thus involving the SSL device's capabilities to stop it. For this test, gateways that successfully identified and stopped the PING from reaching the target successfully passed the test.





For the Oversized PING Attack test, all four tested devices passed.



Network Quota DoS Attack

Network-level Denial-of-Service (DoS) attacks are mostly based on sending the victim repetitive requests until the server is unable to serve other clients. In other words, an application that consumes an abundance of sessions may need a governor, of sorts, imposed so it doesn't choke the ability of other applications to establish sessions.

In this test, engineers logged into the Web-SSL portal and simultaneously sent multiple requests to a Web page from the protected server. Then, engineers ensured that the DoS attack had been detected and blocked by each DUT. (A proprietary Java script was used to generate up to 10,000 sessions.)

Figure 4: Network Quota DoS Attack

Network Quota DoS Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Engineers checked the security logs and the packet capture from a sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.

Only the Check Point Connectra NGX was able to detect and block the session-greedy application, while the F5, Cisco and Juniper products failed because they allowed all sessions to pass through the DUT.

FTP Bounce Attack

FTP bounce attack is an exploit of the FTP protocol whereby an attacker is able to use the PORT command to request indirect access to ports by using the victim machine as a middle man for the request. Engineers set up and configured each DUT to block any suspicious attack.





During the test, engineers connected to the FTP service running on the protected server with Windows 2000 Server and attempted to connect to another host by issuing a malicious PORT command.



The test was implemented by using "Netcat (ver. 0.7.1)" to connect to the protected server and issued the following commands:

```
USER anonymous
PASS x@x.com
PORT 10.0.0.5.0.80
LIST
QUIT
```

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.

Figure 5: FTP Bounce Attack

FTP Bounce Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Results show that both the Check Point Connectra NGX and the F5 Networks FirePass 1000 blocked the FTP Bounce PORT command, although the F5 device dropped the session without graceful termination and did not log the event. (Blocking the attack means the product "passed" the test, whereas products that allowed the attack through to the network resources "failed.") Both the Cisco VPN Concentrator 3005 and the Juniper NetScreen-SA 1000 failed the test.

Server Message Block Attack





Server Message Block (SMB) is the communications protocol used by Windows-based operating systems to support sharing of resources across a network. Today, worms spread via file shares often infect startup directories to assure that the infected host executes the worm after reboot. Engineers set up and configured each DUT to block any suspicious attack. The engineers then attempted to copy an executable file into the startup folder.



Engineers first attempted to access the shared startup folder of the protected server and copy an executable file to it. This attack is implemented by establishing a NetBIOS connection to a shared folder of the protected server, and requested to list the "startup" sub-directory.

Then, engineers implemented the attack by issuing the following commands on the client machine after authentication has been successful:

```
net use \\<server ip>\shared <pass>/user:administrator
dir \\<server ip>\shared\startup\
copy test.exe \\<server ip>\shared\startup
```

Figure 6: Server Message Block Attack

Server Message Block Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.





In the SMB Attack test, only the Check Point Connectra NGX passed. The Cisco VPN Concentrator 3005, F5 FirePass 1000 and Juniper NetScreen-SA 1000 all allowed engineers to copy an executable file into the target "startup" directory.



Domain Name Service UDP Enforcement Attack

Domain Name Service (DNS) is a commonly used network protocol by both clients and servers, which makes it both a preferred protocol for server compromise and a covert command-and-control channel of Trojan software. Engineers set up and configured each DUT to block suspicious attacks.

Engineers sent a malformed UDP DNS request to the protected server using the Netcat (ver. 0.7.1) tool.

Figure 7: DNS UDP Enforcement Attack

DNS UDP Enforcement Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.

Here, again, only the Check Point Connectra NGX passed the test. For each of the other three devices, the DUT did not block the attack and subsequently a malformed DNS packet was traced on the server side, indicating the attack had reached its target.

Appendix B. Web Attack Tests

Users' SSL VPN Web services might not be aware that they are running through SSL VPN gateways as, to them, all they see is the target Web application.

However, as part of the protection provided by an SSL VPN device, the device is typically terminating their Web session and proxying it to the target Web server. By taking the terminate-and-proxy approach, an SSL VPN device has the opportunity (at least) of inspecting any traffic it forwards. The level of inspection, though, varies dramatically across vendors.





These next sections examine the DUTs and their ability to respond to various Web-borne attacks.

Buffer Overflow Attack Test

At the heart of Connectra NGX is a Check Point Web Intelligence technology called Malicious Code Protector that inspects client requests for potential attacker payloads delivered by buffer overflows. A vulnerability in HTTP's 'chunked' transfer encoding, used in combination with the processing of HTR request sessions (related to Microsoft scripting) can be exploited to execute arbitrary code remotely on a vulnerable machine. By sending a carefully crafted HTTP request, an attacker can overwrite a section of the vulnerable machine's heap space. Data structures in the overwritten heap can be manipulated to move attacker-supplied data to attacker supplied memory addresses, thereby altering the flow of execution into an attacker supplied payload.



Engineers set up and configured each DUT to block suspicious attacks. Engineers then launched a publicly available exploit against the protected server which addresses the aforementioned vulnerability. The test was implemented by sending a malicious HTTP request which was crafted by the Metasploit framework to attack a Windows NT 4 machine. The payload of this request opened a listening socket on TCP port 4444 on the remote server and spawned a shell for anyone who connected to it.

Figure 8: Malicious Code Protector

Malicious Code Protector			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.

Only the Check Point Connectra NGX passed the test. For each of the other three devices, network traces showed that the malicious request was passed through by the gateway to the server.





 = Pass  = Fail

Command Invocation Vulnerability Test

Internet worms spread by a variety of methods, yet most of the recent worms invoke the command line interface to infect vulnerable hosts. This is often achieved by directory traversal techniques paired with the invocation of the 'cmd.exe' file. In this test scenario, engineers set up and configured each DUT to block any suspicious attack.

Engineers then tried to invoke 'cmd.exe' with a GET HTTP request. The test was implemented by sending a recorded request for: "/<server ip>/WebGoat/cmd.exe" using Internet Explorer from a Windows XP client machine.

Figure 9: General Worm Catcher

General Worm Catcher			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the suspicious attack.

Once again, only the Check Point Connectra NGX passed the test. Not only did Connectra NGX block the attack, but it messaged the user that the attack was blocked. For each of the other three devices, network traces showed that the malicious request was passed through by the gateway to the server.

Cross-Site Scripting

Cross-site scripting represents an attack based on causing the user's Web browser to execute a malicious script in the context of a trusted site.

Successful exploitation of this attack allows a malicious user to embed malicious code (in the form of Javascript or VBScript) in input fields which are inserted back to the server response. This allows an attacker to execute arbitrary code on an unsuspecting user with the trust level granted to the victim site.



Figure 10: Cross-Site Scripting Attack

Cross-Site Scripting Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

In this test scenario, engineers set up and configured each DUT to block suspicious attacks.

Engineers sent the string "" as a parameter value to the "reflected cross-site scripting (XSS)" page of WebGoat from a Windows XP machine using the Web browser (Internet Explorer).

Tests show that the Check point Connectra NGX and the F5 FirePass 1000 passed this test.

 = Pass  = Fail

While Connectra NGX detected and blocked the attack (and sent a message to the client), the FirePass 1000 simply detected "<" and stopped it as illegal.

Both the Cisco and the Juniper devices allowed the attack to pass through to the server.

SQL Injection Attack

Some applications do not validate user input and allow malicious users to issue commands directly to an application's database. This attack enables the attacker to change SQL values, concatenate SQL statements, add function calls and stored-procedures to a statement and more. Successful exploitation of this attack could result in unauthorized data access, record manipulation and general server compromise.





Engineers set up and configured each DUT to block suspicious attacks.



Engineers sent the string "101 or userid in (select userid from user_data)" as a SQL parameter value to the "SQL Injection" page of WebGoat from a Windows XP machine using the Internet Explorer Web browser.

Engineers checked the security logs and the packet capture from the sniffer tool to verify that the DUT detected and blocked the SQL injection attack.

Tests show that only the Check Point Connectra NGX successfully defended against the SQL injection attack. As with other successful detections, Connectra NGX messaged the client that the attack was blocked. By contrast, the F5 Networks, Cisco and Juniper products tested all passed the malicious request on to the server.

Figure 11: SQL Injection Attack

SQL Injection Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

In the case of the F5 FirePass 1000, the device allowed the SQL query to be injected into the input line. However, since F5 Networks claims that the FirePass 1000 does offer SQL injection protection, another test was done to illustrate that the vendor has SOME protection. The F5 FirePass 1000 successfully filtered an attempt to "escape" the SQL query string (') and concatenate an additional SQL query.

Command Injection Attack

Nearly every programming language allows the use of so-called "system-commands," and many applications make use of this type of functionality. System interfaces in programming and scripting languages pass input (commands) to the underlying operating system.

The operating system executes the given input and returns its output to the standard output along with various return codes to the application such as successful, unsuccessful, etc.

The specific command used was: "FORMAT T:" (an unknown drive on the server).





System commands can be a very convenient feature, which can be integrated with little effort into a Web-application. Common usage for these commands in Web applications are file handling (remove, copy), sending E-mail messages and calling operating system tools to modify the application's input and output in various ways (filters).



A malicious user can inject meta-characters, malicious commands, or command modifiers to vulnerable request parameters and the Web application will pass these blindly on to the operating system for execution.

In this test, engineers sent the string, "BasicAuthentication.help | FORMAT T:" as a parameter value to the "Command Injection" page of WebGoat from the Windows XP client machine.

Engineers then checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the command injection attack.

Figure 12: Command Injection Attack

Command Injection Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Tests show that only the Check Point Connectra NGX successfully defended against the command injection attack.

In every case, the competitive devices tested passed the command injection through to the Web server where it was processed and displayed a "dir" listing at the bottom of the returned HTML, in effect granting directory access to the intruder.

Directory Traversal Vulnerability Test

Many Web applications utilize the file system of the Web server in a presentation tier to temporarily and/or permanently save information. This may include page assets like image files, static HTML or applications like CGIs. The WWW-ROOT directory is typically the virtual root directory within a Web server which is accessible to an HTTP Client. Web applications may store data inside and/or outside WWW-ROOT in designated locations.

If the application does not properly check and handle meta-characters used to describe paths, for example "../" or its URL-encoded equivalent, it is possible that the application is vulnerable to a "Path

Traversal" attack. The attacker can construct a malicious request to return data from physical file locations such as '/etc/passwd'. This is often referred to as the "file disclosure" vulnerability.

Attackers may also use these properties to create specially crafted URLs. Path traversal attacks are typically used in conjunction with other attacks like direct OS commands or direct SQL injection.





Engineers set up and configured each DUT to block suspicious attacks.



Engineers then attempted to traverse beyond the application's Web root directory using the Windows XP client machine. This test was implemented by requesting the following URL or functional equivalent (the actual URL doesn't matter just the traversal component):

```
/Web/WebGoat/%2e%2e/%2e%2e/%2e%2e/X/WebGoat/attack
```

Note: %2e is the URL encoded version of a "dot" (.).

Figure 13: Directory Traversal Attack

Directory Traversal Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

 = Pass  = Fail

Engineers then checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the command injection attack.

Tests show that the CheckPoint Connectra NGX and the Juniper NetScreen-SA 1000 passed the Directory Traversal test. However, both the F5 Networks FirePass 1000 and the Cisco VPN Concentrator 3005 permitted the attacker to go past the Web root into other parts of the server.

HTTP Protocol Vulnerability Test

HTTP is the basic protocol used for Web browsing implemented between clients and servers, which makes it both a preferred protocol for server compromise, and a covert command and control channel of Trojan software.

In this test scenario, engineers set up and configured each DUT to enforce ASCII-only data in HTTP headers. Then, engineers checked to determine if malicious attempts to send HTTP requests with malformed headers to the Web server were detected and blocked by each DUT. The header had the arbitrary hex values of '07FE' inserted in the User Agent HTTP header field.

Engineers sent a corrupt HTTP request to the protected server. Corruption was achieved by adding an extra malformed header to the request:

```
GET
/Web/WebGoat/images/back2.GIF,CVPHost=192.168.35.245
HTTP/1.0

Accept: */*

Accept-Language: he

Connection: close

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1) ((HEX: '07FE' inserted into

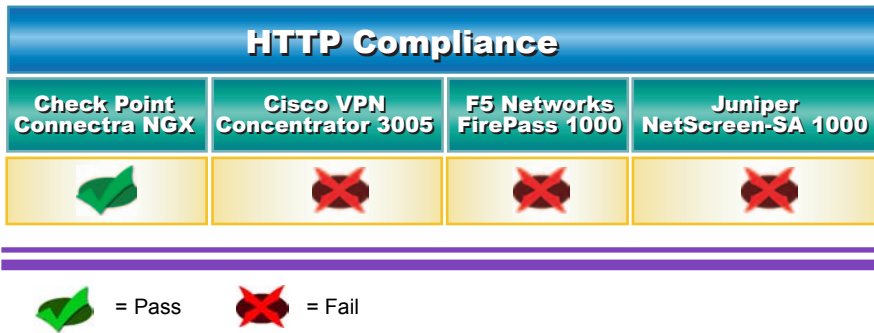
useragent via hex editor

Host: 192.168.35.44

Cookie: __fnbDropDownState=1;
SESSION_ID=7ce3ab64395a227297ba7b8613422e41
```

Engineers then checked the security logs and the packet capture from the sniffer tool to verify that the DUT effectively detected and blocked the command injection attack.

Figure 14: HTTP Compliance



Tests show that only the Check Point Connectra NGX successfully passed the HTTP compliance test.

Not only did the Connectra NGX detect and block the attack, but the device also messaged the client, specifying the invalid characters in the input message.

In the case of the rival products tested, each permitted an illegal binary field to pass to the server.





WebDAV Extension Attack

WebDAV is an extension of the HTTP protocol, designed to support authoring and versioning of files via HTTP. As this is a relatively new protocol, many implementations still contain flaws which allow an attacker to harm the server in various methods.

Engineers set up and configured each DUT to block any suspicious attacks.

Engineers then attempted to access a server file with the LOCK WebDAV HTTP method. The test was implemented by replacing the GET method of a GIF file request to LOCK and resending it to the Windows 2000 protected server.



Figure 15: WebDAV Extension Attack

WebDAV Extension Attack			
Check Point Connectra NGX	Cisco VPN Concentrator 3005	F5 Networks FirePass 1000	Juniper NetScreen-SA 1000
			

Engineers attempted to determine that malicious attempts to send HTTP requests to the Web server had been detected and blocked by each DUT.

Only Connectra NGX passed the WebDAV Extension Attack test.

The other three devices tested all passed the "LOCK" request on the Web server.

 = Pass  = Fail

Appendix C. Devices Under Test

Devices Under Test		
Company	Model Tested	Version
Check Point Software Technologies Ltd.	Connectra NGX	NGX (build 100) GA
F5 Networks, Inc.	FirePass 1000	OS 5.4.2
Cisco Systems, Inc.	Cisco VPN Concentrator 3005	OS 4.7.1
Juniper Networks, Inc.	Juniper NetScreen-SA 1000	ScreenOS 5.0R1 (build 8555)

Appendix D. Test Tools Utilized

Public Domain Test Tools Utilized		
Model Tested	Version	Details
Ethereal	0.10.12	http://www.ethereal.com/
MetaSploit Framework	2.4	http://www.metasploit.com/projects/Framework/
Netcat	0.7.1	http://netcat.sourceforge.net/
Paros Proxy	3.1.3	http://www.parosproxy.org
Webgoat	3.7	http://www.owasp.org/software/webgoat.html

Appendix E. Competitive Vendor Interaction

In accordance with The Tolly Group's Fair Testing Charter, Tolly Group personnel reached out to Cisco Systems, F5 Networks and Juniper Networks multiple times during the course of the project. The Tolly Group invited the vendors to comment on test methodology prior to testing, provide product support and comment on test results related to their product.

Only F5 Networks offered comment on the test results. The Tolly Group shared results of the F5 Networks FirePass 1000 with the company and asked it to comment on the device performance.

An F5 Networks' press relations spokesperson responded in an E-mail dated 06 Sept 2005, 8:08 p.m. A portion of her response follows:

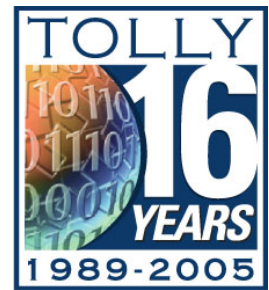
"Protecting against the types of Internet attacks that your tests cover is really the job of a proper application firewall, such as F5's Traffic Shield product. But, for a real-world test of application firewall security the tests being performed would be extremely inadequate..."

...Our concern is that by limiting the testing to just the 'hand picked' criteria may give a false sense of security to customers as they may be lead to believe they do not need a separate application firewall."

"Though our FirePass appliance does provide some limited application firewall features they are primarily designed to protect its Web management interface. These are not intended to replace full application firewalls such as F5's Traffic Shield product and no security-minded organization cognizant of security best practices would use it for that."

###

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.



The Tolly Group, Inc.
3701 FAU Blvd. Suite 100
Boca Raton, FL 33431
Phone: 561.391.5610
Fax: 561.391.5810
<http://www.tolly.com>
info@tolly.com

