



Juniper Networks – NetScreen Secure Access (SSL VPN) February 2005

iSEC Partners, LLC is a digital security firm that specializes in application, network, host, and product security. iSEC's Independent Security Reports (iSRs) are used by security conscious companies to verify product attributes in terms of security best practices, standard security functionality, and product protection. iSEC's iSR process involves independent evaluation of a product or product feature. iSEC evaluates the security posture, tests security assertions, and produces an independent report. For more information about iSRs, please refer to www.isecpartners.com

Juniper Networks engaged Information Security Partners, LLC (iSEC) to develop a Security Assurance Program for the Instant Virtual Extranet (IVE) platform running on Secure Access (SSL VPN) appliances. The program is comprised of a series of security assessments where tests are conducted to determine what an unauthorized user might accomplish with the IVE platform on the SSL VPN appliance.

The iSEC assessment program involves assessments that model specific threat scenarios, identify vulnerabilities, and enumerate exploitation possibilities. While the testing methodology is flexible, each assessment includes the following processes:

- Documentation review
- Developer interviews
- Threat profiling
- Design review of new features and functions
- Active testing of mutually agreed upon features and functions
- Review of changes made to fix previously identified issues of concern
- Manual and automated penetration testing
- Code review (for validation, and discovery)
- Validation testing of "security assertions"

iSEC will issue an Independent Security Report (iSR) at the completion of each security assessment. The iSR will summarize the high-level security goals of the IVE platform assessment and validate specific security assertions made by Juniper Networks.

Security Assessment

Prior to completing this iSR, iSEC conducted twenty person (20) days of testing in November 2004. The testing was conducted on versions 4.1.1 and 4.2 of the IVE platform. The following aspects were the primary focus areas during iSEC's testing:

- Appliance (Device) Security
- Authentication, Authorization, and Auditing (AAA)

Throughout the testing period, technical staff at Juniper Networks worked closely with the iSEC security team, and iSEC can report that Juniper Networks is committed to ongoing security in the IVE platform on its SSL VPN appliances.

Assessment Security Assertions

This iSR has been developed to give Juniper Networks the opportunity to highlight security features within the IVE platform on its SSL VPN appliances and to show how these security features help Juniper achieve the following high-level security goals:

Appliance Security

1. The IVE platform protects local and cached credentials, passwords, cookies, certificates, and private keys from local attack on the SSL VPN appliance physical storage.
2. The appliance must use a hardened and minimized operating system and utilize strong run-time protections for attacks against network services.
3. The IVE platform's custom web server is not susceptible to standard attacks against IIS or Apache web services.

Authentication, Authorization, and Auditing

4. The IVE platform is able to protect against injection and pre-authentication attacks.
5. The IVE platform is able to protect against session stealing, which includes the following attacks: Cross-site Scripting, Cookie Guessing, and Input Validation.
6. The IVE platform's audit system cannot be avoided, overloaded, or spoofed.
7. The IVE platform's audit system tracks all system events, administrative changes, and user activity.
8. The IVE platform must not create security vulnerabilities when authenticating users against an external source such as Active Directory (Kerberos support) and NT Domains (NTLMv2).

Security Assertions Results

iSEC security testing contains five levels of measurement. The results for each test conducted by iSEC are categorized according to the following table.

Summary of Testing Results		
Measurement	Score	Explanation
Excellent	5	Significantly exceeding industry standards
Good	4	Exceeding industry standards
Satisfactory	3	Meeting industry standards
Poor	2	Below industry standards
Bad	1	Significantly below industry standards

The following table summarizes the results of iSEC's testing based on Juniper's security assertions.

Summary of Testing Results Juniper Networks IVE Platform	
Security Assertion	Results
Assertion 1: The appliance must protect local and cached credentials, passwords, cookies, certificates, and private keys from attack on its physical storage.	Good (4)
Assertion 2: The appliance must use a hardened and minimized operating system and utilize strong run-time protections for attacks against network services.	Good (4)
Assertion 3: The appliance's web server is not susceptible to standard attacks against IIS or Apache web services.	Excellent (5)
Assertion 4: The appliance must protect against injection and pre-authentication attacks.	Excellent (5)
Assertion 5: The appliance must protect against session stealing, which includes the following attacks: Cross-site Scripting, Session Hijacking, SQL Injection.	Good (4)
Assertion 6: The appliance's audit system cannot be avoided, overloaded, or spoofed.	Good (4)
Assertion 7: The appliance's audit system tracks all system events, administrative changes, and user activity.	Excellent (5)
Assertion 8: The appliance must not create security vulnerabilities when authenticating users against an external source such as Active Directory (Kerberos support) and NT Domains (NTLMv2).	Excellent (5)

Detailed Explanation of iSEC Testing:

The following section lists the each security assertion by Juniper, iSEC’s testing process, and the overall results.

Security Goal #1 Juniper has taken a “Defense in Depth” approach for the physical and digital security of its IVE-based appliances.	
Assertion 1: The appliance must protect local and cached credentials, passwords, cookies, certificates, and private keys from local attack on its physical storage.	
Testing Process: iSEC disassembled the SSL VPN appliance, which is based on x86 server hardware, and attempted to reverse engineer the software on the disk. Standard reverse engineering tools, such as hex editors, forensics software, disassemblers, virtual machine platforms, and hardware simulators were used to analyze and modify the IVE software platform.	The following techniques where used to analyze the SSL VPN appliance drive: <ul style="list-style-type: none">• The disk was examined block by block using standard disk forensic software.• The boot loader and kernel were disassembled and examined to analyze cryptographic protections and the boot order.• The boot loader and kernel where modified to attempt interactive access to the system.• The IVE platform was executed in an instrumented virtual machine and simulated hardware environments, to allow for run-time debugging and reverse-engineering.
Customer Impact: SSL VPN devices, by design, process and store sensitive information such as user credentials, access logs, and possibly confidential company information. Customers deploying such products must be aware of the possibility of information exposure if an attacker gains physical or logical access to the device. Likewise, security precautions taken to protect sensitive information should be part of the purchasing decision.	
Results: Good (4) The Juniper IVE platform encrypts the root and data partitions on the system hard drive. User credentials, passwords, cookies, certificates, and private keys are protected, using a strong, peer-reviewed cipher: AES-128. Juniper properly uses AES in a CBC mode, with cryptographically strong protections against modification of the root partition cipher text. The only plain-text partitions on the disk belong to the virtual memory swap space and the kernel, which is unencrypted to allow system bootstrapping.	

With enough time and resources, reverse engineering techniques such as disassembly, binary modification or instrumented simulations of the IVE kernel can be used to eventually gain access to the encrypted information. The techniques necessary to perform this attack are advanced and time consuming, and Juniper uses several levels of protection to increase the difficulty of reverse engineering. During our investigation, iSEC employed such techniques and confirmed that Juniper uses advanced protections against reverse engineering.

In iSEC's judgment, the Juniper SSL VPN appliance goes well beyond industry standards in protecting against attacks, including those conducted by advanced attackers who have physical control of the appliance. Without specialized tamper-resistant hardware, it is impossible to prevent a highly skilled attacker with an infinite amount of time and physical control of the appliance from gaining access to the information stored on the drive. In the case of many other network and server appliances, such attacks are trivial for a novice attacker.

Drive encryption has an added benefit beyond protecting secrets on stolen appliances; such encryption makes it very difficult for attackers to discover vulnerabilities through reverse engineering the operating system or service binaries.

Assertion 2: The appliance must use a hardened and minimized operating system and utilize strong run-time protections for attacks against network services.

Testing Process:

iSEC was provided with the 4.1.1 and 4.2 IVE platforms, as well as source code for the IVE kernel and important network services. The operating system's configuration files, access controls, running processes, and running kernel configuration were examined and compared against known best practices for minimized Linux systems.

iSEC examined the system in order to verify the following items:

- The IVE kernel is modified to provide executable space protections and address randomization.
- The IVE's base Linux operating system is minimized to contain only absolutely necessary binaries, services, and functionality.
- 3rd party network services, such as the SNMP daemon and DNS resolver are isolated to protect against potential exploit.
- The IVE uses secure firewall and packet routing configurations.

Customer Impact:

Customers using SSL VPN solutions that run on standard operating systems such as Linux or Windows should ensure that the SSL VPN gateway uses a hardened operating system. General purpose platforms that have not been hardened against OS exploits and attacks may be vulnerable to system compromise and downtime.

Results: Good (4)

iSEC examined the source code and build configuration of the IVE Linux kernel, as well as a running IVE kernel. Findings determined that strong execution protections are in place. Specifically, non-executable page protections and address space randomization are used to protect against the most common buffer overflow exploits. Recent research has shown that such protections can be circumvented by highly experienced shell-code writers; however, such exploits would have to be specifically targeted against the Juniper platform, and would most likely require access to a running appliance. Exploits for off-the-shelf Linux operating systems, would not be effective against a similar vulnerability if it also existed in the Juniper IVE platform.

The running IVE operating system is highly minimized and contains only the files and processes necessary for its role. Optional services are not started unless specifically configured in the administrative interface.

A chroot jail is utilized for most un-trusted services, and would effectively block an attacker from gaining full access to the appliance in case of a vulnerability in one of these programs. Proper file permissions are used to restrict sensitive information.

The IVE Platform uses kernel packet filtering to prevent inbound traffic on the un-trusted interface, except for ports 80 and 443, and DNS traffic. In addition to standard routing rules, the IVE kernel has been modified to prevent sensitive information from being sent out of the un-trusted interface.

Overall, the Juniper IVE platform is significantly more secure than most Linux-based network appliances and provides commendable protection against the possibility of future vulnerabilities in Juniper's platform, system services, or other software delivered on the appliance.

Security Goal #2

The Juniper IVE platform is not susceptible to traditional web server vulnerabilities and commercial automated scanners

Assertion 3: The appliance's web server is not susceptible to attacks against IIS or Apache web services.

Testing Process:

iSEC executed many IIS and Apache attacks in order to determine if common web server attack classes are successful in enumerating or compromising the IVE's web server.

Types of access operations attempted:

- Buffer overflows
- Directory traversal
- Denial of service
- DCOM
- Front Page Extensions
- Sample page codes
- Double decode
- Mod_cookie
- CGI
- Indexing exploits
- Unauthenticated URL access
- HTTP/S uploads

Customer Impact:

Customers using SSL VPN technology for business partner extranets and remote access deployments often deploy these gateways in the DMZ so services are accessible from the Internet. Any SSL VPN solution whose web server is based on Apache or IIS is likely to be vulnerable to some subset of these commonly used web server attacks and potentially leaves the DMZ and the internal resources and applications at a higher level of risk than is necessary for business applications

Results: Excellent (5)

iSEC was able to validate that the IVE platform is not vulnerable to attacks against common web servers such as IIS or Apache. Standard web server attacks conducted by iSEC using automated scanners or manual techniques were not successful. Automated scans did return some false positives, but each of these was researched and determined to a false positive that resulted from assumptions within the scanning tool or other limitations of the test utility. The immunity of the IVE web server to standard attacks can be attributed to the fact that Juniper has written their own minimized web server, which shares no code base with IIS, Apache, or any other commercial or open-source product.

Security Goal #3
The Juniper IVE platform employs strong protects against injection and pre-authentication attacks

Assertion 4: The appliance must protect against injection and pre-authentication attacks.

<p>Testing Process:</p> <p>iSEC configured a Juniper SSL VPN appliance using Radius, Windows 2003 Active Directory, and LDAP authentication servers. iSEC then attempted to attack the IVE user and administrator login pages, as well as the authentication servers, with standard attacks.</p> <p>Multiple encoding types, such as non-minimal UTF-8 and non-English code pages, were used on character injection attacks.</p>	<p>Types of attacks attempted:</p> <p>Against the Web Server:</p> <ul style="list-style-type: none"> • Form field overflow and format string attacks • Perl script injection attacks • HTTP Header overflow and format string attacks • Cross-site scripting attacks • Standard SSL vulnerabilities <p>Against the Authentication Servers:</p> <ul style="list-style-type: none"> • SQL Injection attacks (for SQL based LDAP servers) • Field overflow and format string attacks • LDAP dangerous character injection attacks • Brute force password guessing
---	--

Customer Impact:

Customers using SSL VPN technology for business partner extranets and remote access deployments often make the gateway devices available from the Internet to access the internal network. Any SSL VPN solution whose authentication process can be subverted or exploited would allow attackers to bypass all security filtering devices, such as firewalls, VPNs, and routers, allowing access to the internal network.

Results: Excellent (5)

iSEC was unable to crash or exploit the IVE web server or authentication application using any known attacks or targeted “fuzzing.” Fuzzing is an advanced technique for finding flaws in network communications protocols that involves the submission of random data and data types to an entity in order to solicit unexpected results that enable an attack.

Examination of network traces on the trusted network revealed that dangerous authentication information, such as overly long fields and LDAP escape characters, were not included in back-end communications to the authentication servers. This behavior of trimming anomalous

information from requests is an example of the excellent protections provided by the IVE Platform.

Assertion 5: The appliance must protect against session stealing, which includes the following attacks:

- Cross-site Scripting
- Session Hijacking
- SQL Injection

Testing Process:

iSEC attempted multiple Cross-site Scripting, Cookie Guessing, and input validation attacks in order to bypass filters for viewing and executing scripts between users.

iSEC attempt the following types of control and cross site scripting characters during the testing:

ASCII, and Unicode representations of:

- o “
- o >
- o <
- o ;
- o ‘
- o &

In addition to direct inclusion of these characters in objects, iSEC also tried to bypass output filtering with non-minimal UTF-8 encodings of the target characters, and use of alternate interfaces for input.

Types of access operations attempted:

List of views evaluated:

- Welcome (login)
- Status
- Configuration
- Network
- Clustering
- Log/Monitoring
- Singing-in
- Troubleshooting
- Windows Files
- Unix Files
- Secure Meeting

List of fields:

- Username
- Password
- NSlookup
- Traceroute
- ARP
- Secure Meeting Search Users

Customer Impact:

Customers using SSL VPN technology to access file servers, E-mail, and other internal network services rely on the strength of session token used by the SSL VPN gateway. The token identifies important session information and enables the user to engage in transaction with the SSL gateway and follow-on resources. Weak protections potentially allow unauthorized users to access the internal systems via a SSL VPN after successfully engaging in a cross-site scripting or URL injection attack by hijacking the user’s session.

Results: Good (4)

SQL injection attacks produce no successful attacks in the IVE platform, equating to strong separation between the access features and internal data storage on the SSL VPN appliance.

Session hijacking by guessing/predicting the session token was not possible due to the fact that the application is using strong and unpredictable session tokens for end-user and administrators. The session tokens have sufficient entropy to defend against session guessing attacks, and are not predictable to an attacker. Even if the attacker has access to the machine and can generate a set of sample session tokens before and after the target session tokens is generated, session hijacking attacks were unsuccessful. No duplicate session tokens were found to be generated by the system, and the system changed the user's session token whenever the user authenticated as a different user and after a periodic timeout of the user's session token.

Input filtering and output filtering are quite strong throughout most of the application, including protections against UTF-8 encoding of script tags and commands in most display fields. The IVE Platform's audit log provides a good example of input filtering.

During the security audit engagement, iSEC did identify a few instances of cross-site scripting vulnerabilities in a prior version of the IVE software. Fixes for these problems were validated in the production release IVE 4.2R1.

Security Goal #4

The Juniper IVE platform supports strong Auditing mechanisms

Assertion 6: The appliance audit system cannot be avoided, overloaded, or spoofed.

Testing Process:

iSEC executed several subversion, tampering, and overloading attacks against the IVE platform the integrity of the audit log.

Types of access operations attempted:

iSEC attempted the following attacks:

- iSEC attempted to create log entries with fake or incorrect data in order for the system to log incorrect username or dates/time entries.
- iSEC also attempted to avoid the audit system by authenticating without an audit trail or modifying settings as an authenticated user without an audit trail.
- iSEC attempted to overload the log files by creating a large amount of audit entries to override existing entries in the logs.

Customer Impact:

Customers using SSL VPN technology are allowing access to sensitive internal networks from host that are connected to and through connection that transit the un-trusted Internet. In order to provide evidence of non-repudiation and to conduct reliable forensic analysis, auditing systems for SSL VPN technology should be very detailed, specific, and should not be deleted, overwritten, or avoided in order to protect the integrity of that audit log.

Results: Good (4)

Attempts to avoid the audit system or create fake audit entries failed on numerous attempts when using multiple attack methods. Attempts to overload the audit system were only successful when the maximum log limit was reached (400MB on a default install and up to 500MB) and when no external log servers or archive systems were configured (e.g. syslog, scp, etc.). All other attempts to overload the audit system were unsuccessful.

Assertion 7: The appliance's audit system tracks all system events, administrative changes, and user activity.

Testing Process:

iSEC performed several actions before and after a successful login to the IVE platform in order to ensure that all actions, both significant and minor, are tracked, logged, and stored with adequate detail.

Types of access operations attempted:

iSEC attempted the following attacks:

- iSEC attempted unauthorized actions before authentication, such as login attempts, to ensure log entries are tracked on failed attempts or unauthenticated users.
- iSEC attempted several actions on each application on the IVE, such as web browsing (URL location logging), File Server access (file access, modify, delete logging), and meeting options (create or attending a meeting) to ensure that all end-user actions are logged, tracked, and stored in adequate detail.
- iSEC attempted administrator level actions, such as creating a new user, delete a user, granting or denying access rights to users, changing configuration options on each IVE application, to ensure that all administrator level actions are logged, tracked, and stored in adequate detail.

Customer Impact:

Customers that require auditing of all activity on the SSL VPN gateway should analyze how much information is actually recorded. HIPAA, OCC, SEC, and many other regulatory constraints often require user access to be logged and tracked thoroughly. An SSL VPN device without exhaustive logging can possibly allow users to access systems without any audit trail.

Results: Excellent (5)

Attempts to ensure the audit system logs, tracks, and stores authenticated end-user, unauthenticated user, and administrator activity was performed. All attempts to perform activity and avoiding being tracked by the SSL VPN failed, including several administrator level actions, such as adding or removing configuration settings, and end-user service actions, such as web URL access, file server access, and secure meeting activity.

Security Goal #5

The Juniper IVE platform supports strong Authentication mechanisms

Assertion 8: The appliance must not expose the deployment to security vulnerabilities in legacy protocols when authenticating users against an external source, such as Active Directory (Kerberos support) and NT Domains (NTLMv2).

Testing Process:

iSEC configured the SSL VPN appliance to use the “Kerberos or NTLMv2 Only” option and then attempted downgrade attacks in order to force the SSL VPN appliance to use weaker hashing algorithms such as NTLM or plain-text authentication.

Types of access operations attempted:

During the attack, iSEC sniffed all communication between the SSL VPN appliance and back end servers, such as an Active Directory server, in order to capture NTLM hashes, plain-text communication, or Kerberos session tickets. iSEC blocked port 88 on all Active Directory servers to force the machine to use NTLM or NTLMv2 during authentication. Additionally, iSEC used Windows 95/98 machines without Kerberos and attempted to authenticate to an Active Directory servers via the SSL VPN appliance.

Customer Impact:

Customers who use Windows Authentication (Active Directory) should require that the SSL VPN gateway support the Microsoft-endorsed secure protocol for authentication: Kerberos. Further, due to the numerous exploits and vulnerabilities associated with NTLMv1 and LM (LANMAN), the SSL VPN gateway must be able to prevent downgrade attacks that could compromise all user authentications in the presence of internal attacker. NTLMv1 and LM credentials can be “cracked” with several freely available hacking utilities, so it is important that your SSL VPN deployment supports Kerberos or at least NTLMv2.

Results: Excellent (5)

When in “Kerberos or NTLMv2 Only” mode, the SSL VPN appliance was able to prevent attackers to downgrade to weaker authentication methods that would expose end-user names and passwords. This functionality preserves the user-credential protections native in Windows 2000/2003. When attempting LM or NTLMv1 downgrade attacks, the IVE platform was able to deny access to the weaker authentication method and thus maintaining support of the Microsoft endorsed secure protocol for authentication (Kerberos) or NTLMv2.