# GIAC
## CERTIFICATIONS

# Global Information Assurance Certification Paper

## Copyright SANS Institute
## Author Retains Full Rights

# Auditing the NetScreen Secure Access

# SA-3000 Series SSL VPN Appliance

## (Formerly Neoteris IVE 3020)

**Alexander B. Stamatiou, CISSP**

**SANS GSNA**

**Practical Assignment Version 3.0**

**March 2004**

## Table of Contents

## Disclaimer

The following document contains information that is based on an actual SA-3000 that is currently in production at my current place of employment. Considering that this information is extremely confidential, all IP addresses, hostnames, and references made to the company have been altered or removed for their protection. Actual text and all screen shots used within this document have also been altered to protect the company.

## 1. Assignment 1 – Research in Audit, Measurement Practice, and Control

### 1.1 Introduction

Acme Corporation has tasked me to conduct an audit of their SSL VPN infrastructure, which primarily consists of one hardware component. The component is known as the NetScreen Secure Access SA-3000 series SSL VPN appliance, formerly known as the Neoteris Instant Virtual Extranet 3020. Acme Corporation would like to know if the SA-3000 operates as securely as the vendor claims. To fulfil this requirement, I've decided to test two scopes:

1. Secure connectivity between a PC connected to the Internet and the SA-3000 which is located at the customer's site. To conduct this test, I will use the primary application that Acme employees connect to; OWA (Outlook Web Access).

2. The second objective of this security audit is to ensure that the NetScreen SSL VPN appliance itself is in fact a secure device.

Throughout this audit, we will assume that all other components that are part of the SSL VPN formation are secured and without compromise. This would include: the PC connected to the Internet, the firewall that constitutes a DMZ to which the SA-3000 resides, and the OWA server itself.

### 1.2 Description of the system being audited

The NetScreen Secure Access SA-3000 is a hardened network appliance that provides security by intermediating data stream requests that flow between requesting clients and internal resources, enforcing the use of encryption for all supported TCP sessions. It achieves this by using the following dependencies:

1. A stripped-down pre-hardened version of the Linux operating system kernel.

2. SSL (Secure Sockets Layer) protocol, originally developed by Netscape to transmit information over the Internet in an encrypted state.

3. A pre-hardened version of Apache web server with OpenSSL + Mod_SSL components.

The SA-3000 is technically designed to be used as an edge device facing the Internet directly, to allow for remote access to internal resources using a standard web browser from any location. The device has two Ethernet interfaces; an external and an internal. If being used as an edge device, both interfaces are required. If placed on a public DMZ protected by a screen router or firewall, then only one interface is to be used.

Users authenticate to the SA-3000 using a "userid" and "password." This in turn is either validated by the SA-3000's local user database or internal network authentication servers. Once a session has been established, the SA-3000 provides secure access to a multitude of internal resources such as; web-mail, web-applications, network file sharing services, and native MAPI (Messaging Application Programming Interface).

The SA-3000 operates on the basis of a term knows as "clientless VPN." The technology is called "clientless" because it does not require the installation of additional software components (such as IPSEC) on the client PC to enable a secure session. It is a "transparent" solution that does not require additional network configuration changes on the client PC, other than what is needed for basic Internet connectivity. In this case, any standard web browser that supports SSL is the only requirement needed to connect. The browser will actually use HTTPS (HyperText Transport Protocol – Secure) which is basically HTTP over SSL/TLS.

In order to establish a secure connection utilizing SSL, an exchange of encryption keys is required on behalf of the client and the SA-3000. This is accomplished by use of the RSA key-exchange algorithm and either RC4 ciphers for 128-bit connections or Triple DES ciphers for 168-bit connections. The SA-3000 also supports 40-bit and 56-bit connections. However, since the US government repealed its ban on 128-bit encryption in 1997, this audit will primarily focus on connections that are 128-bit or greater. The supported SSL versions are; 2.0, 3.0, and TLS (Transport Layer Security), all options are configurable administrative options.

User authentication is achieved by either of the following options; SA-3000 internal database, Radius, LDAP/LDAPS, Windows Active Directory, Netegrity SiteMinder, or RSA ACE Server.

## Acme Corporation SA-3000 Configuration:

In the case of Acme Corporation, the SA-3000 resides on a DMZ protected by a Checkpoint firewall. Only one Ethernet interface on the SA-3000 is active, since it is not being used as an edge device. The firewall is configured to redirect all incoming HTTP (tcp/port 80) and HTTPS (tcp/port 443) connections destined for *<extranet.acme.com>* to the SA-3000. The registered DNS name *<extranet.acme.com>* resolves to a publicly assigned IP address. All incoming web-mail requests are redirected to the Checkpoint firewall (via proxy ARP), which in turn uses NAT (Network Address Translation) to hide the real (private) IP address of the SA-3000. Authentication is off-loaded to internal Radius servers; both a primary and a secondary for redundancy. The SA-3000 is configured to only accept SSL/TLS version 3 connections, and it forces the client browser to use Triple DES 168-bit encryption. The only application that is currently accessible via the SA-3000 is a Microsoft OWA server for web-mail services. The OWA server also resides on the DMZ; it is securely hardened and only accepts connections from the SA-3000. In turn, the Checkpoint firewall rules, will only allow the OWA server to connect to the Microsoft Exchange servers on the internal LAN. The only access that the SA-3000 has to the internal LAN, are the Radius servers for user authentication.

4

**Network Diagram:**



Acme Corporation — 10/27/03

Prepared by: Alexander Stamatiou

Acme Data Center
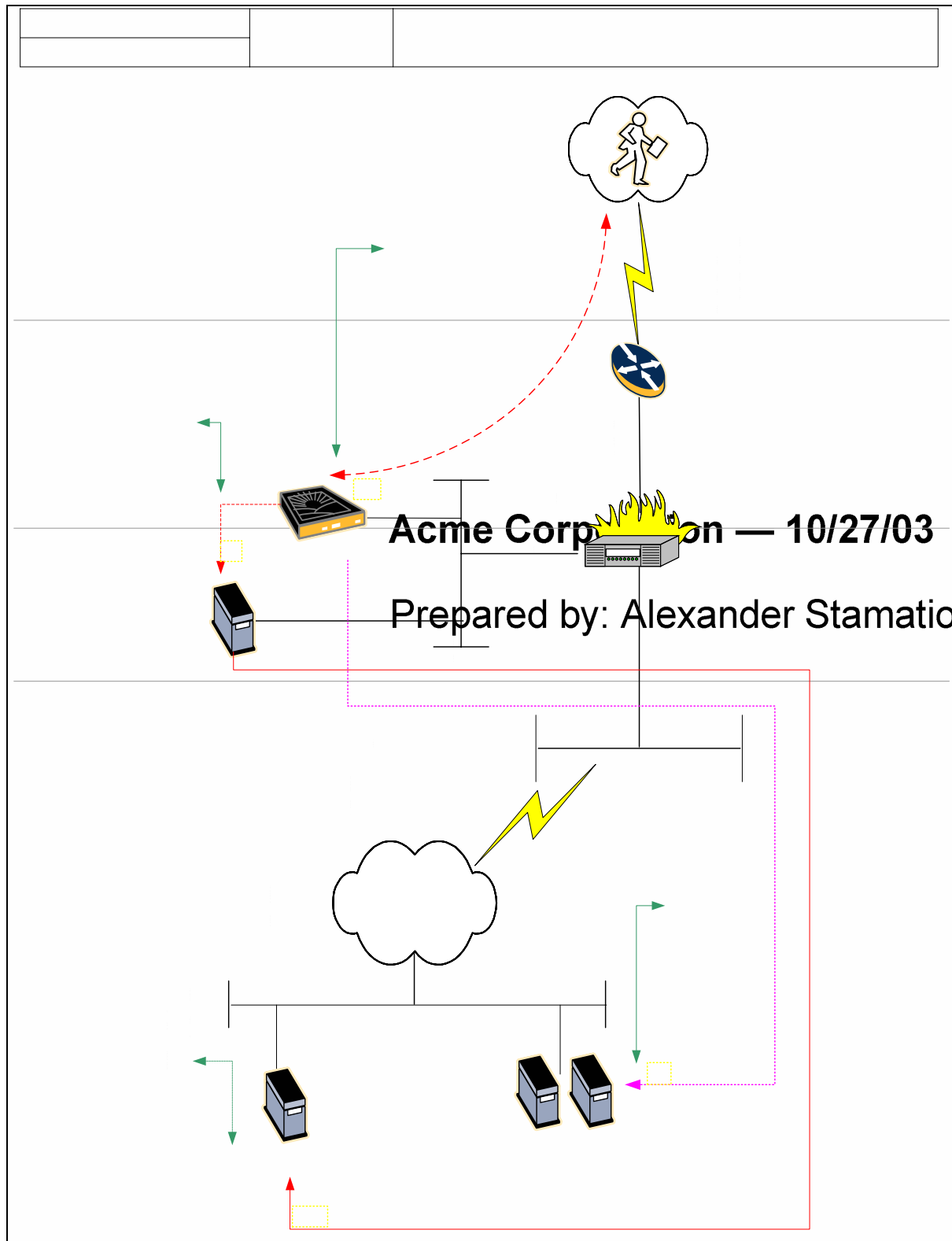
| SA-3000 General Settings | Details |
|---|---|
| System Software Package version | 3.3.1-S1 Release (build 5651) |
| SA-3000 Name | SA_3000 |
| Hostname | extranet.acme.com |
| Internal Interface | 100Mbs / Full Duplex / Auto Negotiation |
| Internal Interface IP | 10.5.1.2 |
| External Interface | Disabled |
| Static Route | 0.0.0.0 >> 10.5.1.1 |
| Web proxy | Disabled |
| DNS | 172.16.2.1 & 172.16.2.2 |
| Authentication Servers | Radius @ 172.16.3.1 & 172.16.3.2 Port 1645 |
| Public IP extranet.acme.com | 500.50.10.5 |
| Allowed SSL version | SSL v3 |
| Allowed Encryption Strength | Accept Only 168-bit |
| Page Caching | Off |
| Time Since Last Reboot | 20 Days, 15 Hours, 24 Minutes, 30 Seconds |
| Logging Disk | 10% Full |
| Maximum Concurrent Users Allowed | 100 |
| Sign-in password length | Minimum 6 characters |
| Basic Authentication Intermediation | Set to HIGH |
| Cache Control | No-Store |
| NTP Enabled | Yes |
| Sign-On Options | All accounts on enabled authentication servers |
| Administrator ID | Admin – Enabled on local |
| Idle Timeout | 10 minutes |
| Max Session Length | 30 minutes |
| Enable Roaming Session | Disabled |

## 1.3    Risk to the system being audited

The purpose of evaluating any significant risk to the SA-3000 is to ensure that any and all potentials are properly addressed throughout the audit process. Using best practices and a well developed audit plan, any & all discovered risks are easier to analyze and provide the appropriate measures to counteract the threats. To determine the risks associated with the SA-3000, I took the following specifics into consideration:

1. The risk itself.
2. The consequences if an unauthorized user decided to use the risk in a malicious way.
3. The probability that the risk could happen.
4. The severity level if it were to happen and the outcome.

The tables below describe some of the potential security risks that the SA-3000 may be subjected to:

| Risk #1 | A hacker gains root access to the SA-3000 system via command-line. |
|---|---|
| **Consequences** | With root access the hacker has the keys to the kingdom, and the ability to change anything on the SA-3000 to his advantage. The SA-3000 uses a Linux kernel, thus any & all files or scripts can be manipulated for malicious activities. |
| **Probability** | <u>Low Risk.</u> The SA-3000 is a hardened OS and it's completely stripped of all & any commands, giving anyone the inability to execute a root shell. |
| **Severity Level** | High Level. The system would be completely compromised. |

| Risk #2 | An unauthorized user gains access to the SA-3000 web-administration console from anywhere on the Internet. |
|---|---|
| **Consequences** | With administrative access to the web-admin console, an unauthorized user has the ability to change any and all configuration settings that apply to the operation of the SA-3000. This includes adding access to any supported resource on the LAN if the firewall has an open policy for the SA-3000 to "any." |
| **Probability** | <u>Medium Risk</u>. If the administrator fails to properly configure the following: does not make use of TCP Wrappers or blocked subnets, fails to change the "admin" username to something unique, utilize a cryptic password of long length, fails to create separate access rules on the firewall, and disable session roaming. |
| **Severity Level** | High Level. The system and the network would be completely compromised. |

| Risk #3 | Persistent cookies are allowed via the SA-3000 configuration settings. |
|---|---|
| **Consequences** | With cookie persistence enabled, it is possible that "login" session states are stored on the connecting client machine. |
| **Probability** | <u>Low Risk</u>. By default the SA-3000 has cookie persistence disabled for all connections. NetScreen also warns the administrator NOT to use cookie persistence unless it is absolutely necessary, making note that security can be compromised. |
| **Severity Level** | Medium Level. A hacker can use this information as an attempt to elevate his privileges, bypass authentication, or reveal specific details about the session ID. |

7

| Risk #4 | Using SSLv2, instead of v3. |
|---|---|
| **Consequences** | SSLv2 has well-known buffer-overflow exploits, which could allow a hacker to execute arbitrary code on the SA-3000. |
| **Probability** | High Risk. By default, the SA-3000 is configured to accept connections from both SSLv2 & v3 supported browsers. All browsers have been supporting SSLv3 for the better part of 2 years. |
| **Severity Level** | Medium Level. Using the exploits associated with SSLv2, a hacker could bypass some of the key features of the SA-3000's security control mechanisms. |


| Risk #5 | Intent to maliciously POWER DOWN the system. |
|---|---|
| **Consequences** | Authorized Acme users will not have the ability to access OWA web-mail services as a result. This could be considered a denial-of-service for the corporation, and would disrupt the ability for sales employees to access mail from anywhere. |
| **Probability** | Low Risk. Every MIS employee at Acme Corporation is required to use an access card to enter the data-center. Someone would need to loose their card, or an intruder would have to try to enter via an unlocked door. The data-center is monitored via CCTV and security guards. |
| **Severity Level** | High Level. When there's a will, there's a way. Intruders could enter undetected and maliciously power down the system without any indication. |


| Risk #6 | Radius Authentication not available. |
|---|---|
| **Consequences** | Acme users would not be able to authenticate to the SA-3000, thus unable to gain access to OWA. |
| **Probability** | Low Risk. The SA-3000 is configured to make use of a primary and secondary Radius server in the event that one fails. The network itself is fully redundant, thus a lack of connectivity is highly unlikely. |
| **Severity Level** | High Level. Without the ability to use Radius for authentication, access to the SA-3000 is not feasible. |


| Risk #7 | Open ports on the SA-3000. |
|---|---|
| **Consequences** | Such a vulnerability would give the hacker the ability to use a multitude of exploits to compromise the SA-3000 |
| **Probability** | Low Risk. The SA-3000 listens only on port 443, and does not have any other TCP ports active by design and function. |
| **Severity Level** | Medium Level. Depending on the open ports, a hacker could compromise the device using ports other than 443. |

| Risk #8 | Gaining unauthorized access to the SA-3000 console port. |
|---|---|
| **Consequences** | An intruder or hacker will have the ability to compromise the device severely. From the console, the following could be executed: change configuration settings, change the admin username and password, disable TCP wrappers, reboot the system, or rollback to a previous version. |
| **Probability** | <u>Low Risk.</u> The intruder or hacker would need to bypass all effective physical security controls. The Acme data-center makes use of CCTV and security guard protection, aside from requiring an access card to enter. |
| **Severity Level** | High Level. The intruder or hacker could render the SA-3000 useless, or reconfigure to their advantage. |

| Risk #9 | "dsCacheCleaner.exe" unable to install on the client machine properly. |
|---|---|
| **Consequences** | The ActiveX control will not be able to delete cacheable content from the client browser and all locally dependant directories. Thus, any files & content downloaded via the SA-3000 will remain on the client PC indefinitely. |
| **Probability** | <u>High Risk:</u> The "dsCacheCleaner.exe" will only install with local admin or power user privileges. In most cases, Acme's users do not have these rights. Hence, the cached content is most likely to stay on the local machine. |
| **Severity Level** | High Level. If shared systems are used to view attached files via OWA, those files will remain on that system as cacheable items. Anyone could potentially view this information. |

## 1.4     Current State of Practice

The task of researching the Internet and various other resources, as a means to find secure configurations and or auditing methods for the NetScreen Secure Access SA-3000 SSL-VPN appliance proved to be very challenging. I was actually very surprised that I couldn't find "best practice" methods or audit checklists that specifically focus on the SA-3000. My best tool up to now has been my personal experiences with the device and dealing with NetScreen technical support engineers. Most of the technical information that is specific to these SSL-VPN appliances can only be found via the vendors support knowledge-base or FAQ database. Although the technical manual provides decent information on how to use the various options via the web interface, it doesn't give the reader a good understanding of the various configuration parameters. Even technical newsgroups are limited with information, and I was shocked by this. It's usually easy to find answers to questions via technical newsgroups, but not in the case of the SA-3000.

On a good note, I managed to find good audit reports that tested the security effectiveness of the SA-3000 when it was known as the Neoteris IVE. These reports were written and provided by the following companies:

1. TruSecure – Statement of Opinion Regarding the Instant Virtual Extranet, Version 3.1 June 11th 2003.

   - The report focuses on the Neoteris IVE, and it basically validates the vendor's claims of a good security posture.

2. Cryptography Research Inc. – Neoteris System Evaluation, June 16th 2002.

   - This report describes the findings of an extremely detailed security audit preformed on the Neoteris IVE by CRI. It contains a wealth of information regarding; the state of the OS used, how the device primarily functions, what could be potential security issues, and what requires improvement.

   - Using this report as a reference, I was able to validate my claims that the OS is completely stripped of commands, making it almost impossible to gain root access to the system.

3. Dan Farmer – Review of the Neoteris Instant Virtual Extranet (IVE), January 2002.

   - The famous Dan Farmer has done a great job describing his audit findings when he tested the Neoteris IVE.  After physically tearing the box open and manipulating the OS, he was able to determine that SA-3000 uses a RedHat Linux Kernel, which is stripped and hardened.

   - The real importance of the Dan Farmer audit is in reference to the Apache Web daemon. Farmer explains that the SA-3000 is highly dependant upon Apache, and the security posture of the SA-3000 is predicated upon the stability and security of the web daemon.

4. METAGROUP – Delta 2327, Application Security Gateways Part 1 & 2 by David Thompson, July 3rd 2003.

- The primary focus of this report was to give the reader an understanding of ASG (Application Secure Gateways) and how they are best implemented in an environment. This report does not primarily focus on the SA-3000 or Neoteris IVE, but it does give good insight regarding the current state of this technology and the various issues/concerns.

- For one, this report verifies my claim that the SA-3000 or any other SSL VPN appliance should not be used as an edge device; rather they should be complimented with a good SPI firewall.

**Other references that were used:**

- US-CERT: SSLv2 Vulnerabilities: http://www.kb.cert.org/vuls/id/102795

- Linux Journal: Assessing the security of web applications: This URL provides a wealth of information in regards to best practices for implementing "cookie" security. >> http://www.linuxjournal.com/article.php?sid=3855

- The SSL Alternative by Mike Fratto, November 13<sup>th</sup> 2003 >> http://www.networkcomputing.com/showitem.jhtml?docid=1423f3

- US-CERT: OpenSSL Exploits: http://www.kb.cert.org/vuls/id/380864

- NetScreen SA Customer Support Site: http://support.neoteris.com In order to access this site, you must have a support contract with NetScreen. Located on this site are: support knowledge-base, FAQ database, and all the vendor specific manuals for their products.

## 2.0   Assignment 2 – Create an Audit Checklist

The properly assess the NetScreen SA-3000; the following audit checklists where created to test the identified risks mentioned in section 1.0 of this document. Each particular item listed in the checklist will contain the following information:

- Checklist Item Number = to be used for cross-referencing.
- Item Title = short and brief description of the item.
- Reference = all associated research material used for this item.
- Risk = identifies the risk and any potential consequences.
- Testing Procedure = description of the process using tools and/or commands.
- Compliance Criteria = is the system compliant?
- Objective or Subjective Test?

## 2.1   NetScreen audit checklist

| Audit Item 1 | Control Objective | Verify that command-line sessions with the SA-3000 as an attempt to gain access to the device cannot be initiated. |
|---|---|---|
| Reference | 1. Dan Farmer's Neoteris IVE security audit; page 4, second to last paragraph. http://www.ipm.com/fileadmin/PDF/Neoteris/Farmer_Security_report.pdf <br> 2. Cryptography Research Inc, page 15, paragraph 3.5.2 <br> 3. Personal experience and knowledge. ||
| Risk | If command sessions are allowed by the SA-3000, there's a possibility that a hacker could take "root" control of the system and compromise not only the device, but potentially the network itself and all associated resources behind it. ||
| Testing | Try using any of the following commands: <u>Telnet</u>, <u>SSH</u>, or any <u>Unix Shell</u> from either a command prompt or by using a GUI. Open a command prompt and type the following: **C:\telnet <ip address or hostname> or use any SSH client and attempt to connect to the device's public & private IP.** ||
| Compliance | Response upon attempting to connect should be **"could not open connection to the host, connection failed."** ||
| Objective/Subjective | Objective ||

| Audit Item 2 | Control Objective | Verify that only specified IP's can access the SA-3000 via the web-admin console. |
|---|---|---|
| Reference | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Personal experience and knowledge. ||
| Risk | If the administrator does not identify & configure the use of specific private IP's to ONLY have access to the web-admin console, any unauthorized user will have the ability to attempt a logon. ||
| Testing | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Administrators." Select the tab named "Authentication" and then "Address Restrictions." ||

| Compliance | Either option; "Administrators can sign in from any IP address" or "Administrators can only sign in from the following IP's" should be selected. Specified IP's would be specified with option 2 selected. |
|---|---|
| Objective/Subjective | Objective |

| Audit Item 3 | Control Objective | Verify that all sessions are encrypted from the client browser to the OWA server via the Internet by means of the SA-3000. |
|---|---|---|
| Reference | 1. Ethereal Packet Sniffing, by Angela D. Orebaugh – Syngress Publishers.<br>2. Personal experience and knowledge. | |
| Risk | Unencrypted information between the client browser and the OWA is susceptible to prying eyes on the Internet. Anyone can use a sniffing tool to capture the clear-text information and use it to their advantage. This would be a violation to Acme's external security policy. | |
| Testing | Use Ethereal or any sniffing capable utility to capture packets between the client browser and the OWA server to insure that all information is in fact encrypted. Install Ethereal on your client machine and configure it capture via promiscuous interface, enable "capture" and filter by "IP" to view the results. | |
| Compliance | If encrypted, the results via Ethereal should display all packets are in fact using SSLv3 & HTTPS; for all 3-way TCP handshakes included. | |
| Objective/Subjective | Objective | |

| Audit Item 4 | Control Objective | Verify that all authentication attempts & user session requests are being logged by the SA-3000. |
|---|---|---|
| Reference | 1. NetScreen SA-3000 Administration Manual available only on the customer website.<br>2. Personal experience and knowledge. | |
| Risk | 1. If authentication requests are not being logged, there is no conceivable way to know who's attempting to login to the SA-3000, and verify who does & doesn't have authorized privileges.<br>2. If user session requests are not being logged, there is no way to track the user's activity, or have an audit trail of which resources are being accessed. | |
| Testing | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "General Settings" and then "Log." Set your logs to the highest number being 5000 and select "update." Review the logs and look for good and then any erroneous entries. | |
| Compliance | 1. Failed authentication attempts to the Radius Server will read "authentication failure" or "user not defined on the authentication server."<br>2. Accepted authentication attempts to the Radius Server will read "authentication successful for user XYZ."<br>3. Able to track the allowed user's activity and follow an audit trail to the retrospective resources. | |
| Objective/Subjective | Objective | |

| Audit Item 5 | Control Objective | Verify that only ports 80 & 443 are listening via the SA-3000. |
|---|---|---|
| Reference | 1. Cryptography Research Inc, page 8, paragraph 3.1. <br> 2. Verifying which ports are listening – RedHat Security Guide Ch. 5 Server Security http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-ports.html | |
| Risk | Any other TCP ports that are unnecessarily open and listening on the SA-3000 are a potential security weakness, giving a hacker more opportunities to run specific attacks against non-required services. | |
| Testing | Use "Nmap" to scan both the public & private IP to determine what TCP services the device itself and/or the firewall is allowing to and from the SA-3000. | |
| Compliance | Results of an Nmap scan should display that only TCP ports 443 (SSL) and 80 (HTTP) are listening on the SA-3000 and being passed by the protecting firewall. | |
| Objective/Subjective | Objective | |

| Audit Item 6 | Control Objective | Verify that the SA-3000 only accepts the SSLv3 protocol. |
|---|---|---|
| Reference | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Personal experience and knowledge. <br> 3. CERT - http://www.kb.cert.org/vuls/id/102795 | |
| Risk | According to CERT advisories, anything other that SSLv3 is considered a security risk. There are certain exploits within the SSLv2 protocol that would allow a hacker to run arbitrary code on the targeted machine. | |
| Testing | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "General Settings" and then "Security." Check to see if SSLv3 has been selected. | |
| Compliance | On the SA-3000 web-admin console, the following should be displayed and selected "Accept Only SSL V3 & TLS (maximize security)." | |
| Objective/Subjective | Objective | |

| Audit Item 7 | Control Objective | Verify that the SA-3000 encrypts using Triple DES 168-bit ciphers. |
|---|---|---|
| Reference | Personal experience and knowledge. | |
| Risk | In the case of Acme Corporation's security policy, they only allow the use of 3DES 168-bit ciphers for all HTTPS connections to and from the OWA server via the SA-3000. Anything else is considered a violation of the corporate security policy. | |
| Testing | Using Internet Explorer as an example: Type in the URL https://extranet.acme.com and select "yes" to accept the SSL certificate. To check the established SSL browser security, from within IE go to "File, Properties" and check the security ciphers used under the section named "Connections." | |
| Compliance | Within "File, Properties" and under the section "Connections" the ciphers listed should state "Triple DES with 168-bit encryption (HIGH)." | |
| Objective/Subjective | Objective | |

| Audit Item 8 | Control Objective | Verify that the SA-3000 is using a trusted CA certificate. |
|---|---|---|
| **Reference** | 1. Cryptography Research Inc, page 4, paragraph 2.2. <br> 2. BlackHat Top Ten Web Attacks, http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf <br> 3. Personal experience and knowledge. | |
| **Risk** | If not used, there is a possibility that a hacker could initiate a server impersonation attack. | |
| **Testing** | Using Internet Explorer type in the following URL https://extranet.acme.com and wait for a "security alert" dialog box to appear. Check to see which of the three alerts has been validated or not. | |
| **Compliance** | If an SSL cert from a Trusted CA is installed and being used by the SA-3000, an alert would not be displayed by the client browser. | |
| **Objective/Subjective** | Objective | |

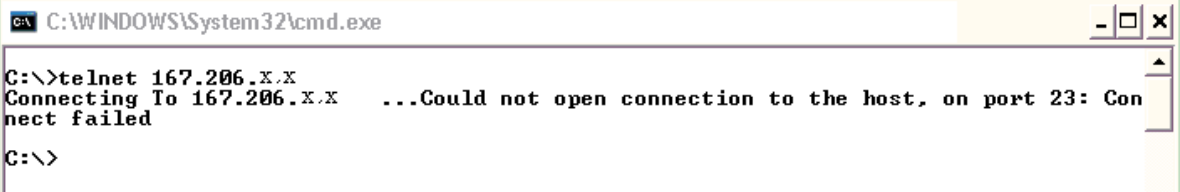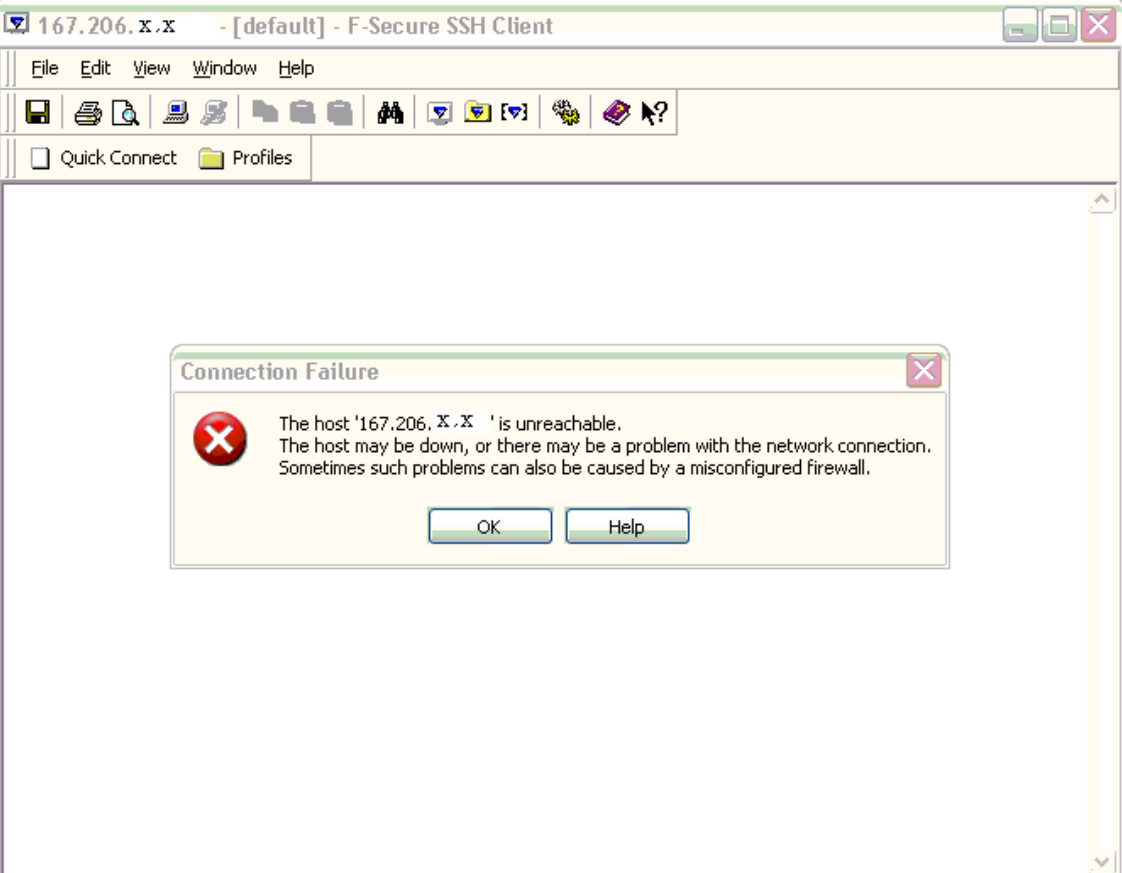| Audit Item 9 | Control Objective | Verify that the SA-3000 is not using persistent cookies for all client browsers that access OWA. |
|---|---|---|
| **Reference** | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Personal experience and knowledge. <br> 3. Linux Journal: http://www.linuxjournal.com/article.php?sid=3855 | |
| **Risk** | Information regarding the connected session to the SA-3000 is stored in either persistent or non-persistent cookies. In the case of persistence, that cookie is stored on the local hard-drive of a PC. That persistent cookie has a certain life, based on a time-stamp. However, until it's deleted, it contains user information that could be used by a hacker to gain additional insight that would increase the security risk level. | |
| **Testing** | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Groups" and then "named Group." Select "web" and check the item called "Enable Persistent Session Cookie." | |
| **Compliance** | By default, the setting for Persistent Cookies on the SA-3000 should not be enabled. It should read "Use user's setting (disabled)." | |
| **Objective/Subjective** | Objective | |

| Audit Item 10 | Control Objective | Verify that all cached browser information is deleted from the client upon logging off the SA-3000. |
|---|---|---|
| **Reference** | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Secrets of Computer Espionage, Tactics and Countermeasures, by Joel McNamara – Chapter 5, page 111, Gathering Evidence, browser cached information. <br> 3. Personal experience and knowledge. | |
| **Risk** | Any and all cached information left behind by the browser on a PC (especially a shared system, or kiosk) gives any non-Acme employee the ability to take a sneak peak at confidential information. | |

| Testing | 1. Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Groups" and then "named Group." Click on the tab "General" and then "Web." Scroll down to the section called "Enable Cache Cleaner." |
|---|---|
| | 2. On the client IE browser, "Tools, Internet Options, Temporary Internet Files, Settings, View Files and View Objects. |
| | 3. On the Windows system, "c:\Program Files\Neoteris." |
| Compliance | 1. The Windows file path < C:\Documents and Settings\atg007\Local Settings\Temporary Internet Files> should not leave any trace files when the user logs-out from the SA-3000. |
| | 2. The Windows file path < C:\WINDOWS\Downloaded Program Files> should contain a file called "NeoterisSetupControl." |
| | 3. The Windows file path <c:\Program Files\Neoteris> should contain a file called "dsCacheCleaner." |
| Objective/Subjective | Objective |

| Audit Item 11 | Control Objective | Verify that hostname encoding is turned-on to protect the OWA server name. |
|---|---|---|
| Reference | 1. NetScreen SA-3000 Administration Manual available only on the customer website. | |
| | 2. Personal experience and knowledge. | |
| | 3. RFC 1738 - http://www.faqs.org/rfcs/rfc1738.html | |
| Risk | Exposing the hostname in the URL path provides more than enough information about internal server names. This information should be kept private at all times. | |
| Testing | 1. Authenticate to the SA-3000, your automatically redirected to the OWA server. Check the URL path in the status bar within your browser. | |
| | 2. Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Groups" and then "named Group." Click on the tab "General" and then "Web." Check the option called "Enable Encoded Hostname." | |
| Compliance | 1. The URL path displayed by a standard browser should use encoding to mask the real server name. | |
| | 2. The option "Enable Encoded Hostname" should be set to "enabled." | |
| Objective/Subjective | Objective | |

| Audit Item 12 | Control Objective | Verify that Radius is configured to authenticate users to the SA-3000. |
|---|---|---|
| Reference | 1. NetScreen SA-3000 Administration Manual available only on the customer website. | |
| | 2. Personal experience and knowledge. | |
| Risk | Access to OWA will fail, thus remote users will not have the ability to check mail. | |
| Testing | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Authentication Servers" and check the <enabled or disabled status>. Then click on the assigned server name that represents the Radius instance and check the configuration parameters. Check the "group-authentication" parameters for an assigned "group" matched to the authentication instance. | |

| Compliance | The SA-3000 web-admin console should display the appropriate configuration settings for the Radius primary & secondary servers. Should include the following information: <u>IP addresses</u>, <u>port 1645</u>, <u>Radius shared-secret</u>, <u>Group Matching</u>, and server is <u>&lt;enabled&gt;</u>. |
|---|---|
| **Objective/Subjective** | Objective |

| **Audit Item 13** | **Control Objective**  Verify that the "web-admin" console is in fact using HTTPS. |
|---|---|
| **Reference** | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Personal experience and knowledge. |
| **Risk** | If the web-admin console was not using HTTPS to encrypt the information in transit, the configuration information could be potentially intercepted. |
| **Testing** | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 <br><br> To check the established SSL browser security, from within IE go to "File, Properties" and check "connections" & "address URL." |
| **Compliance** | The information should read: <br> 1. Connections = SSL <br> 2. Address URL = https in the beginning of the URL path. |
| **Objective/Subjective** | Objective |

| **Audit Item 14** | **Control Objective**  Verify that password protection for the SA-3000 console is enabled. |
|---|---|
| **Reference** | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. Personal experience and knowledge. |
| **Risk** | If the console is not password protected, and unauthorized person who has physical access to the SA-3000 could compromise certain functions of the device and render it useless. |
| **Testing** | Using a terminal emulator, open a 9600 baud connection from a remote PC or device that can make use of a serial connector cable. Once the session has been initiated, click on any key to start the console. |
| **Compliance** | The system should automatically prompt you for a admin username and password. |
| **Objective/Subjective** | Objective |

| **Audit Item 15** | **Control Objective**  Verify that the SA-3000 has the latest OS build level and all associated security patches per vendor recommendations. |
|---|---|
| **Reference** | 1. NetScreen SA-3000 Administration Manual available only on the customer website. <br> 2. NetScreen customer support site, security update information centre. <br> 3. Personal experience and knowledge. |
| **Risk** | Since the time of it's inception to the tech market space, the SA-3000 has had some exploits based on the fact that it runs Apache, OpenSSL, and relies on a Linux kernel. To keep the device within good operational security practices, not using the current security patch revisions could leave the SA-3000 exposed to these vulnerabilities. |

| | |
|---|---|
| **Testing** | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 |
| | 1. The opening page "System Settings," "General Settings." "System Software Package Version." |
| | 2. NetScreen customer support site, posts all the latest security patches for all its customers. |
| **Compliance** | The latest security build for the SA-3000 should read <3.3.1-S1 Release (Build 5651)> |
| **Objective/Subjective** | Objective |
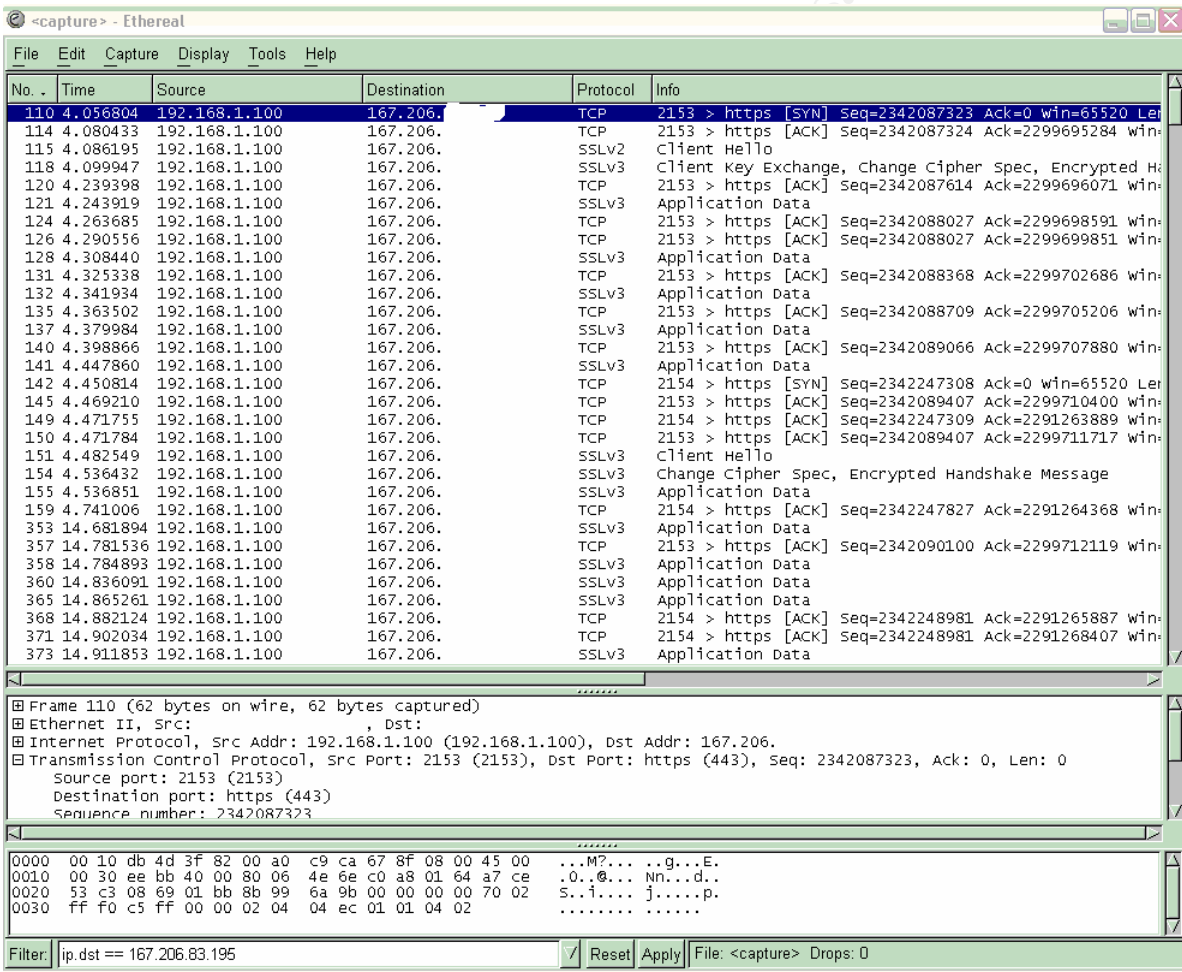
## 3.    Assignment 3 – Conduct the Audit

The following section will expand upon ten (10) of the most critical audit checks and will include the results and findings of each tested risk.
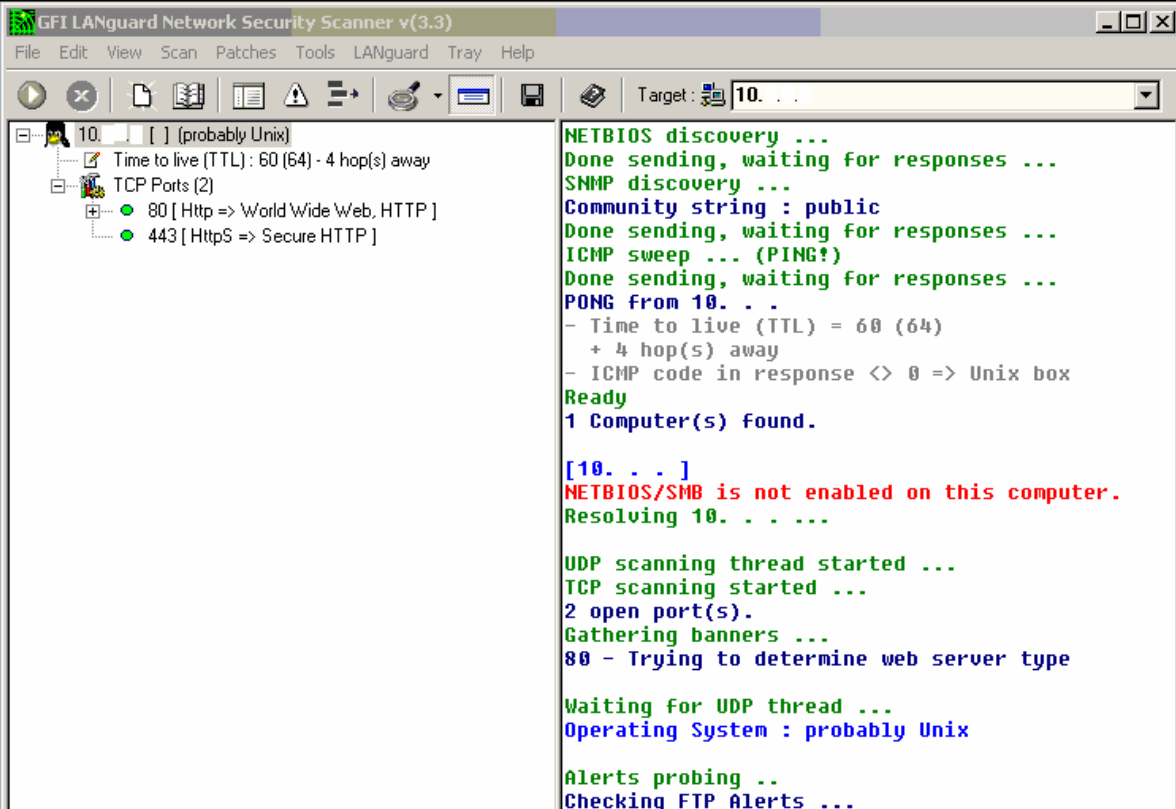
### 3.1    Actual Audit of NetScreen Secure Access SA-3000

| Audit Item 1 | Objective | Verify that command-line sessions with the SA-3000 as an attempt to gain access to the device cannot be initiated. | PASS |
|---|---|---|---|
| Test | | Used the following: <u>Telnet</u> and <u>SSH</u> to the SA-3000's internal & external IP address. <br><br> **1.  Telnet from a Windows XP Command Line:** <br><br>  <br><br> **2.  SSH to the SA-3000 using F-Secure SSH client:** <br><br>  | |

| Audit Item 2 | Objective | Verify that only specified IP's can access the SA-3000 via the web-admin console. | PASS |
|---|---|---|---|
| **Test** | | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 | |
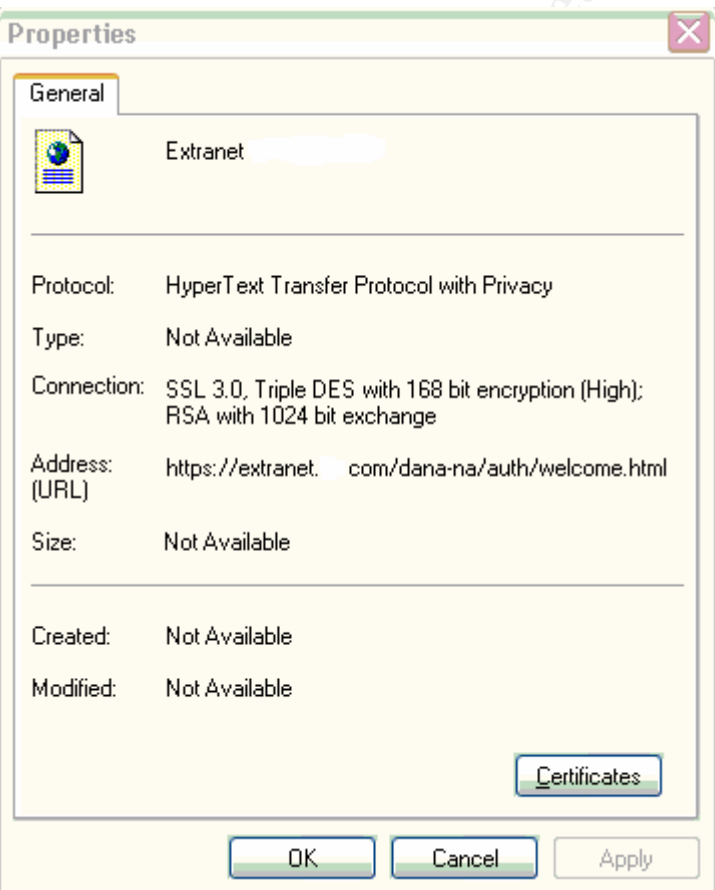
Login in and click on the tab named "Administrators." Select the tab named "Authentication" and then "Address Restrictions."

1. **SA-3000 Web-Admin Console Settings:**

## Administrators

Members   Session   Authentication

Authentication Server | Address Restrictions

○ Administrators can sign in from any IP address

● Administrators can only sign in from the following IP addresses:

| IP Address | Netmask | |
|---|---|---|
| 192.168.1.103 | 255.255.255.255 | Add |

2. **Testing Access From a Non-Listed IP address:**

Logins are not permitted from this IP address.

Username: [          ]

Password: [          ]

Unauthorized access to this system, illegal use of this system or use of this system in violation of company policy are strictly prohibited. Sign in to begin your secure session.

[ Sign In ]

Note: This is the
**Administrator Sign-In Page**.

If you don't want to sign in as an Administrator, return to the standard Sign-In Page.
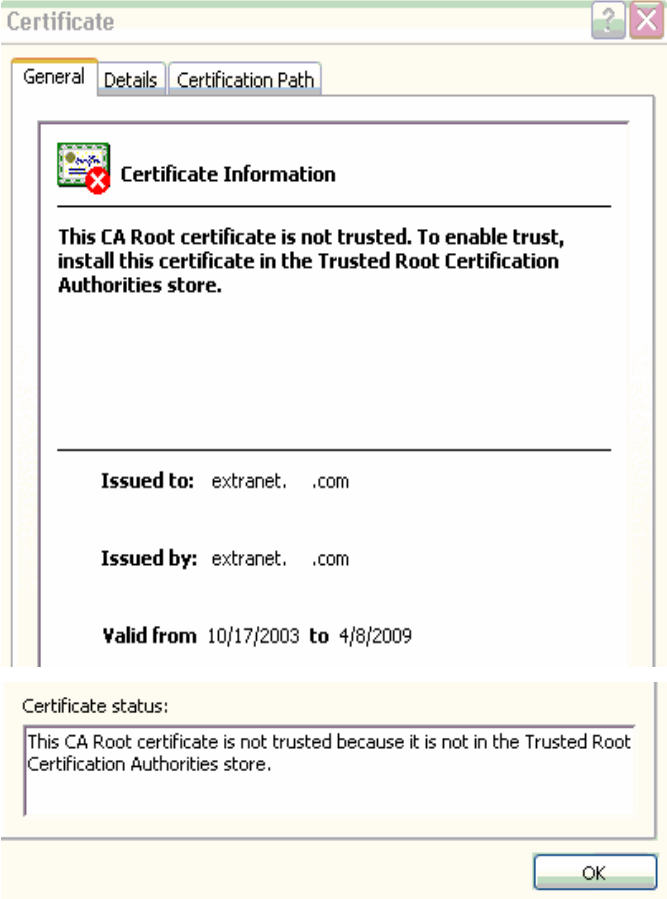
| Audit Item 3 | Objective | Verify that all sessions are encrypted from the client browser to the OWA server via the Internet by means of the SA-3000. | PASS |
| --- | --- | --- | --- |
| **Test** | Using Ethereal I was able to capture packets between the client browser and communication to the OWA server, to insure that all information is in fact encrypted. The capture is filtered by "IP" to view required the results.<br><br>**Ethereal Capture between an Internet client and the SA-3000:** | | |

```
<capture> - Ethereal
File  Edit  Capture  Display  Tools  Help

No. .  Time        Source          Destination   Protocol  Info
110  4.056804  192.168.1.100   167.206.        TCP     2153 > https [SYN] Seq=2342087323 Ack=0 win=65520 Len
114  4.080433  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342087324 Ack=2299695284 win=
115  4.086195  192.168.1.100   167.206.        SSLv2   Client Hello
118  4.099947  192.168.1.100   167.206.        SSLv3   Client Key Exchange, Change Cipher Spec, Encrypted Ha
120  4.239398  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342087614 Ack=2299696071 win=
121  4.243919  192.168.1.100   167.206.        SSLv3   Application Data
124  4.263685  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342088027 Ack=2299698591 win=
126  4.290556  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342088027 Ack=2299699851 win=
128  4.308440  192.168.1.100   167.206.        SSLv3   Application Data
131  4.325338  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342088368 Ack=2299702686 win=
132  4.341934  192.168.1.100   167.206.        SSLv3   Application Data
135  4.363502  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342088709 Ack=2299705206 win=
137  4.379984  192.168.1.100   167.206.        SSLv3   Application Data
140  4.398866  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342089066 Ack=2299707880 win=
141  4.447860  192.168.1.100   167.206.        SSLv3   Application Data
142  4.450814  192.168.1.100   167.206.        TCP     2154 > https [SYN] Seq=2342247308 Ack=0 win=65520 Len
145  4.469210  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342089407 Ack=2299710400 win=
149  4.471755  192.168.1.100   167.206.        TCP     2154 > https [ACK] Seq=2342247309 Ack=2291263889 win=
150  4.471784  192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342089407 Ack=2299711717 win=
151  4.482549  192.168.1.100   167.206.        SSLv3   Client Hello
154  4.536432  192.168.1.100   167.206.        SSLv3   Change Cipher Spec, Encrypted Handshake Message
155  4.536851  192.168.1.100   167.206.        SSLv3   Application Data
159  4.741006  192.168.1.100   167.206.        TCP     2154 > https [ACK] Seq=2342247827 Ack=2291264368 win=
353  14.681894 192.168.1.100   167.206.        SSLv3   Application Data
357  14.781536 192.168.1.100   167.206.        TCP     2153 > https [ACK] Seq=2342090100 Ack=2299712119 win=
358  14.784893 192.168.1.100   167.206.        SSLv3   Application Data
360  14.836091 192.168.1.100   167.206.        SSLv3   Application Data
365  14.865261 192.168.1.100   167.206.        SSLv3   Application Data
368  14.882124 192.168.1.100   167.206.        TCP     2154 > https [ACK] Seq=2342248981 Ack=2291265887 win=
371  14.902034 192.168.1.100   167.206.        TCP     2154 > https [ACK] Seq=2342248981 Ack=2291268407 win=
373  14.911853 192.168.1.100   167.206.        SSLv3   Application Data

⊞ Frame 110 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src:              , Dst:
⊞ Internet Protocol, Src Addr: 192.168.1.100 (192.168.1.100), Dst Addr: 167.206.
⊟ Transmission Control Protocol, Src Port: 2153 (2153), Dst Port: https (443), Seq: 2342087323, Ack: 0, Len: 0
     Source port: 2153 (2153)
     Destination port: https (443)
     Sequence number: 2342087323

0000  00 10 db 4d 3f 82 00 a0  c9 ca 67 8f 08 00 45 00   ...M?... ..g...E.
0010  00 30 ee bb 40 00 80 06  4e 6e c0 a8 01 64 a7 ce   .0..@... Nn...d..
0020  53 c3 08 69 01 bb 8b 99  6a 9b 00 00 00 00 70 02   S..i.... j.....p.
0030  ff f0 c5 ff 00 00 02 04  04 ec 01 01 04 02         ........ ......

Filter: ip.dst == 167.206.83.195          Reset  Apply  File: <capture> Drops: 0
```

| Audit Item 4 | Objective | Verify that all authentication attempts & user session requests are being logged by the SA-3000. | PASS |
|---|---|---|---|
| Test | | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "General Settings" and then "Log." | |

**Radius Authentication logged:**

```
(i) 2004/03/15 23:03:30 -        (     ) - Login succeeded for user          (24.189,        ).
(i) 2004/03/15 23:03:30 - System -          / from IP 24.189,        authenticated successfully using Radius authentication.
(i) 2004/03/15 23:03:30 - System - Get fixed IVE group for user          using authentication server
```

**User Sessions logged:**

```
(i) 2004/03/15 23:03:43 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/Navbar/inbox.gif HTTP/1.1
(i) 2004/03/15 23:03:43 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/inbox/main_fr.asp?view=1&store=0&obj=&acs= HTTP/1.1
(i) 2004/03/15 23:03:43 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/Navbar/nbInbox.asp HTTP/1.1
(i) 2004/03/15 23:03:42 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/root.asp HTTP/1.1
(i) 2004/03/15 23:03:41 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/LogonFrm.asp?isnewwindow=0&mailbox=alexander.stamatiou H
(i) 2004/03/15 23:03:34 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/images/right_top2.jpg HTTP/1.1
(i) 2004/03/15 23:03:34 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/images/go_button.gif HTTP/1.1
(i) 2004/03/15 23:03:34 -          - WebRequest ok : Host: seal.verisign.com, Request: GET /flash/seal_130x88.swf?fp=WEBMAIL.     .COM HTTP/1.1
(i) 2004/03/15 23:03:33 -          - WebRequest ok : Host: seal.verisign.com, Request: GET /getseal?host_name=webmail.    .com&size=L&use_flash=YES&use_transpa
(i) 2004/03/15 23:03:33 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/images/logofrx.jpg HTTP/1.1
(i) 2004/03/15 23:03:32 -          - WebRequest ok : Host: webmail.frx.com, Request: GET /exchange/logon.asp HTTP/1.1
(i) 2004/03/15 23:03:32 -          - WebRequest ok : Host: email.frx.com, Request: GET / HTTP/1.1
```

| Audit Item 5 | Objective | Verify that only ports 80 & 443 are listening via the SA-3000. | PASS |
|---|---|---|---|

| Test | Used "Nmap" and "GFI-LAN Guard" security scanners to sweep both the public & private IP of the SA-3000 to determine what TCP services the device itself and/or the firewall is allowing to and from. |
|---|---|

**Scan for open ports to verify for all TCP listeners, making sure only 80 and 443 exist:**

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (10. . . ):
(The 1584 ports scanned but not shown below are in state: filtered)
Port        State       Service
25/tcp      closed      smtp
80/tcp      open        http
443/tcp     open        https
465/tcp     closed      smtps
993/tcp     closed      imaps
995/tcp     closed      pop3s
6000/tcp    closed      X11
6001/tcp    closed      X11:1
6002/tcp    closed      X11:2
6003/tcp    closed      X11:3
```

```
6004/tcp    closed      X11:4
6005/tcp    closed      X11:5
6006/tcp    closed      X11:6
6007/tcp    closed      X11:7
6008/tcp    closed      X11:8
6009/tcp    closed      X11:9
6050/tcp    closed      arcserve
No exact OS matches for host (If you know what OS is ru
nning on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=3/16%Time=4056913E%O=80%C=25)
TSeq(Class=RI%gcd=1%SI=3E4CC5%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=3E471C%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=3E4610%IPID=Z%TS=100HZ)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
```

GFI LANguard Network Security Scanner v(3.3)

File   Edit   View   Scan   Patches   Tools   LANguard   Tray   Help

Target : 10. . .

```
10. . . [ ] (probably Unix)
    Time to live (TTL) : 60 (64) - 4 hop(s) away
    TCP Ports (2)
        80 [ Http => World Wide Web, HTTP ]
        443 [ HttpS => Secure HTTP ]
```

```
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 10. . .
- Time to live (TTL) = 60 (64)
  + 4 hop(s) away
- ICMP code in response <> 0 => Unix box
Ready
1 Computer(s) found.

[10. . . ]
NETBIOS/SMB is not enabled on this computer.
Resolving 10. . . ...

UDP scanning thread started ...
TCP scanning started ...
2 open port(s).
Gathering banners ...
80 - Trying to determine web server type

Waiting for UDP thread ...
Operating System : probably Unix

Alerts probing ..
Checking FTP Alerts ...
```

| Audit Item 6 | Objective | Verify that the SA-3000 only accepts the SSLv3 protocol. | PASS |
|---|---|---|---|
| **Test** | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "General Settings" and then "Security." Check to see if SSLv3 has been selected. <br><br> **SSLv3 Selected as only protocol allowed:** <br><br>  <br><br> **SSLv3 verified via client connection with a supports connections for both SSLv2 & 3:** <br><br>  | | |

| Audit Item 8 | Objective | Verify that the SA-3000 is using a trusted CA certificate. | FAIL |
|---|---|---|---|
| **Test** | | Using Internet Explorer type in the following URL https://extranet.acme.com and wait for a "security alert" dialog box to appear. Check to see which of the three alerts has been validated or not.<br><br>**Validate that a CA cert is being issued by the SA-3000:**<br><br> | |

| | |
|---|---|
| **Test 8**<br>**(Continued)** | **<u>Validate that a CA cert is configured on the SA-3000:</u>**<br><br>**Certificates**<br><br>Server Certificate   Applet Certificates<br><br>This certificate is used to secure network traffic to and from the IVE.<br><br>**Current Server Certificate**<br><br>**Server Certificate Details**<br>Issued To: extranet.   .com<br>Issued By: Self Signed<br>Valid:      Oct 17 19:14:53 2003 GMT to Apr 8 19:14:53 2009 GMT<br><br>Import / Renew ...<br><br>**Pending Certificate Signing Request**<br><br>**None**<br><br>New CSR... |

| Audit Item 10 | Objective | Verify that all cached browser information is deleted from the client upon logging off the SA-3000. | FAIL |
|---|---|---|---|
| **Test** | 1. Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 Login in and click on the tab named "Groups" and then "named Group." Click on the tab "General" and then "Web." Scroll down to the section called "Enable Cache Cleaner." **Cache Cleaner Configuration on SA-3000 (disabled):**  2. On the client IE browser, "Tools, Internet Options, Temporary Internet Files, Settings, View Files and View Objects. **Cached Files in IE Temp Directory (cached file exists after logoff).**  | | |

**IE Objects (NeoterisSetupControl does not exist – cache control not present):**

Address  C:\WINDOWS\Downloaded Program Files

Program File ▲

**Folder Tasks**

Share this folder

**Other Places**

WINDOWS
My Documents
Shared Documents
My Network Places

{00000075-9980-0010-8000-00AA0...
{2EC77245-C97C-4F5E-80D1-9B280...
{41F17733-B041-4099-A042-B518B...
Cult3D ActiveX Player
Office Update Installation Engine
QuickTime Object
Shockwave Flash Object
Update Class

**Test 10**
**(Continued)**
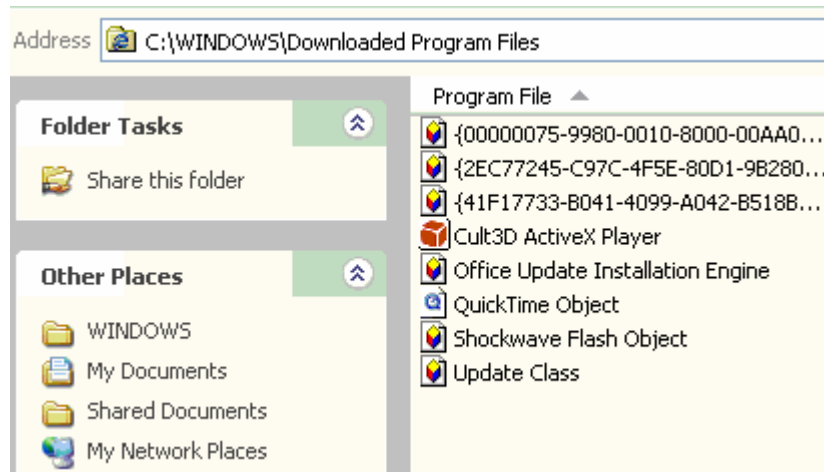
3.  On the Windows system, "c:\Program Files\Neoteris."

**Neoteris <dsCacheCleaner.exe> not present – cache removal utility not installed:**

C:\Program Files

× Name ▲

Program Files
  Acoustica MP3 To Wave Converter PLU
  Adobe
  ahead
  AirScanner Mobile Antivirus
  Alcohol Soft
  AmbiCom
  aod
  Applian
  AvantGo Connect
  AWOPR
  Cirond

Microsoft Plus!
Microsoft Visual Studio
MobiPocket.com
Movie Maker
MoviesMotion
Mp3 File Editor
Ms.Pacman
MSN
MSN Gaming Zone
NeoTracePro
NetMeeting
OfficeUpdate

| Audit Item 14 | Objective | Verify that password protection for the SA-3000 console is enabled. | PASS |
|---|---|---|---|
| **Testing** | | Using a terminal emulator, I opened a 9600 baud connection from a remote PC. <br><br> **SA-3000 Console (protected):** <br><br> Welcome to the Neoteris Serial Console! <br><br> Please input an administrator username and password. <br> Admin username: <br><br> **Toggle Console Password Control On/Off:** <br><br>  <br><br> Current version: 3.3.1-S1 Release (build 5651) <br> Rollback version: 3.3.1 Release (build 5147) <br><br> Please choose from among the following options: <br>   1. View/set network settings (IP, netmask, gateway, link speed, DNS, WINS) <br>   2. Create admin username and password <br>   3. Unblock IP address restrictions for administrators <br>   4. Remove SSL client-side authentication for administrators <br>   5. Display log <br>   6. Ping to a server <br>   7. Trace route to a server <br>   8. Remove all static routes <br>   9. Reboot IVE <br>  10. toggle password protection for the console (On) <br> Choice: | |

| Audit Item 15 | Objective | Verify that the SA-3000 has the latest OS build level and all associated security patches per vendor recommendations. | PASS |
|---|---|---|---|
| **Test** | Open the SA-3000 web-admin console by typing the private IP address of the device in any standard web browser: URL = https://10.5.1.2 <br><br> 1. Web-Admin initial page "System Settings," "General Settings." "System Software Package Version." <br><br> **Latest Software Build (up-to-date with vendor's recommendation:** <br><br>  | | |

### 3.2    Residual Risk?

As SANS clearly states, "residual risk = exposure – controls." Knowing this, it is safe to say that the exposure of the SA-3000 is on the most part pretty low. As for controls, there are a few additions that should have been enforced, as to increase the overall security posture evenmore. In the everyday world of information security, there will always be risks. It's important for Acme Corporation to determine what level of risk they are willing to assign the SA-3000? Meaning, if the device is compromised – what level of risk is deemed acceptable to the corporation. The best way to do that, is to base the "risk" level on the particular business system that the SA-3000 secures & supports. Also, should the SA-3000 be compromised, what other systems are potentially vulnerable. These are all important factors that need to taken into consideration in hopes of calculating an acceptable risk factor.

As for the SA-3000, its current configuration and deployement boasts a better than average level of exposure. However, the controls could be much better. During the actual audit, the SA-3000 failed against two crucial checks. If these controls were to be implemented, the overall security posture for the SA-3000 would increase dramatically. Thus, with the "controls" in the positive and the "exposure" being low – we can manage to reduce the risk. To accomplish this task, all that would be required is man-hours.

### 3.3    Is the System Auditable?

On the most part, the SA-3000 was actually quite fun to audit and not a very difficult task. Since the SA-3000 is an appliance, most of the core functionality of the operating system has been stripped to only include what it needs. Taking this into consideration, it was easier to develop a good checklist to test the core mechanics that most hackers would look to find inherent weaknesses. The trick is to concentrate on the way the product works. Thus, as a security auditor it was more challenging because I was required to base the foundation of my audit on practical experience. The other challenge of this audit was to develop a good set of "controls." Since all Application Security Gateways are relatively new to the market space, it's quite hard to find any developed audit checklists already in existence. As a result, I had to start from scratch and come up with my own methodologies for the NetScreen SA-3000.

## 4.    Assignment 4 – Audit Report

### 4.1    Executive summary

On the most part, I found the NetScreen SA-3000 to be a very secure product. It seems to better secure the OWA infrastructure than having just a standalone system on a public DMZ. Even if the OWA server was to have an SSL certificate installed, it still wouldn't provide the same level of security as the SA-3000. The basic principles of using "true application awareness" and "proxy" capabilities; better enhances the security posture of hosting a web-mail system on the Internet.

On the most part, the SA-3000 does exactly what the vendor claims. It secures all the connections using standard SSL protocols, does not require configuration changes on the client, and it effectively logs everything that passes through it. The logging capabilities are quite impressive, giving Acme Corporation the advantage of monitoring every authenticated request and all user session activity. In the long run, the logs capabilities are a very effective tool against any violations to the security policy.

The only real issues that I had with the SA-3000, is its lack of ability to control caching functions on the client. For the sake of protecting intellectual property, I would like to have seen a little more flexibility with cache-controls. The Cache-Cleaner function that NetScreen offers has limitations; based on what rights a user has on a desktop. With that, it is sometimes impossible to make it work. Thus, a shared computer can contain cached information once a user was to logoff of the SA-3000. That would especially apply to kiosks.

### 4.2    Audit findings/Risk/Recommendations/Costs/Compensating controls

Upon completion of the audit, the SA-3000 passed all security checks with the exception of two. Of the two that it missed; one can be easily fixed and the other is yet an issue that the vendor is well aware of. Here are the highlights of this audit, based on my findings:

- The SSL cert is a self-signed certificate that is automatically generated during the initial install of the SA-3000. From a security standpoint, it is fine to keep it this way. However, using a trusted certificate from a CA improves upon security. By using a trusted CA cert, you will reduce your risk as a result of impersonation attacks not being possible.

- The Cache-Cleaner option called "dsCacheCleaner.exe" only works when a user has "admin" or "power-user" rights on the client machine. Upon establishing a session with the SA-3000, an ActiveX control is temporarily installed on the client machine. This ActiveX control is state-aware and keeps track of all cached information that is placed within temporary directories. Once the user logs off, the dsCacheCleaner will remove all the cached information. It's hard to make a recommendation for this issue, as the vendor is aware that this only works with required privileges.

- Access to the web-admin is secure and extremely easy to operate. However, the web-admin console is accessible from anywhere. That means that it is

imperative to configure TCP wrappers and specify which IP addresses are allowed and not allowed. As a recommendation, the vendor should add more features to this option and allow for 2-factor authentication as a means to better secure the process.

- The addition of policies would make sense as well. This way it is possible to create different roles to the management interface, making harder to gain access to all controls.

- Authentication for administrative control is limited to a "local" database. Recommendation is that the password is changed frequently.

- Some of default features and settings should all be set to the highest security settings upon initial configuration.

- Open policies for access to resources should be "closed" and not "open."

- Firewall configurations should only allow "specific" access controls to resources. The vendor suggests an "any – any" rule from the SA-3000 to anything internally. I would not recommend this, its more secure to define specific rules on the firewall.

## 5 References

1. <u>TruSecure</u> – Statement of Opinion Regarding the Instant Virtual Extranet, Version 3.1 June 11th 2003.

2. <u>Cryptography Research Inc</u>. – Neoteris System Evaluation, June 16th 2002.

3. <u>Dan Farmer</u> – Review of the Neoteris Instant Virtual Extranet (IVE), January 2002.

4. <u>METAGROUP</u> – Delta 2327, Application Security Gateways Part 1 & 2 by David Thompson, July 3rd 2003.

5. US-CERT: SSLv2 Vulnerabilities: http://www.kb.cert.org/vuls/id/102795

6. Linux Journal: Assessing the security of web applications: This URL provides a wealth of information in regards to best practices for implementing "cookie" security. >> http://www.linuxjournal.com/article.php?sid=3855

7. The SSL Alternative by Mike Fratto, November 13th 2003 >> http://www.networkcomputing.com/showitem.jhtml?docid=1423f3

8. US-CERT: OpenSSL Exploits: http://www.kb.cert.org/vuls/id/380864

9. NetScreen SA Customer Support Site: http://support.neoteris.com In order to access this site, you must have a support contract with NetScreen. Located on this site are: support knowledge-base, FAQ database, and all the vendor specific manuals for their products.

10. RFC 1738 - http://www.faqs.org/rfcs/rfc1738.html

11. Secrets of Computer Espionage, Tactics and Countermeasures, by Joel McNamara – Chapter 5, page 111, Gathering Evidence, browser cached information.

12. Verifying which ports are listening – RedHat Security Guide Ch. 5 Server Security http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-ports.html

13. CERT - http://www.kb.cert.org/vuls/id/102795

14. BlackHat Top Ten Web Attacks, http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-shah.pdf