

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Interested in learning more?

Check out the list of upcoming events offering "Auditing Systems, Applications, and the Cloud (Audit 507)" at http://www.giac.org/registration/gsna

# Audit of an SSL VPN; Secure remote email solution for a financial institution

# **GSNA Practical V3.1 Option 1**

Kimberly M. Novobilsky April 13, 2004

As part of GIAC practical repository.

#### Abstract

The purpose of this paper is to perform an audit of the Neoteris Instant Virtual Extranet (IVE) 5000, Version 4.0 Build 5531, an SSL VPN appliance, which is currently undergoing a Proof of Concept (POC) for secure remote access to corporate email at a large financial institution. The results of this audit will aid in the determination to implement this solution. In order to implement this product as a secure remote access solution for corporate email, a through audit and risk assessment will be performed to ensure compliance with corporate policy as well as applicable regulations and laws, i.e. Gramm-Leach Bliley Act, Sarbanes-Oxley, etc. This audit will also determine if the following threats have been appropriately mitigated or reduced; corporate data residing on non-corporate assets, unauthorized access, virus, worms, Trojans, and other malware being introduced to the corporate network, non-compliance with applicable laws and regulations. An audit checklist was created to provide a means for performing this audit. Items included in the checklist are as follows; port scan, Secure Application Management, Cache cleaner, warning banner, removal of cookies, authentication - administrator password policy, re-authentication required after timeout, two-factor authentication, access controls, audit trail for all transactions, segregation of duties, Encryption -SSL, valid SSL certificate, control of corporate data – Host Checker, and Protection against viruses, worms, Trojans, etc. After careful analysis of the data obtained through the performance of the audit the following recommendation was made. Recommendation: The IVE SSL VPN should be implemented as the corporation's solution for secure remote access to email. This solution provides additional functionalities, which will increase the Return On Investment (ROI), by reducing the utilization of more costly remote access solutions. A through risk assessment of these functionalities must be completed before they are implemented.

# **Table of Contents**

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 3 of 60

ITEM NUMBER 13: VALID SSL CERTIFICATE	39
ITEM NUMBER 14: CONTROL OF CORPORATE DATA – HOST CHECKER	41
ITEM NUMBER 15: PROTECTION AGAINST VIRUSES, WORMS, TROJANS	
ETC.	
RISK ASSESSMENT	
EXECUTIVE SUMMARY	45
AUDIT FINDINGS	
Threat One: Corporate Data residing on non-corporate assets	
Threat Two: Unauthorized access	49
Threat Three: Virus, worms, Trojans, and other malware being introduce	
the corporate network	
Threat Four: Non-compliance with corporate policy applicable laws and regulations	
AUDIT RECOMMENDATIONS	
COST	
COMPENSATING CONTROLS	
Policy	58
User Documentation	58
Hardware and Software	
	58
WORKS CONSULTED	59

Author retains full rights.

# Introduction

The purpose of this paper is to perform an audit of the Neoteris Instant Virtual Extranet (IVE) 5000, Version 4.0 Build 5531, an SSL VPN appliance, which is currently undergoing a Proof of Concept (POC) for secure remote access to corporate email at a large financial institution. The results of this audit will aid in the determination to implement this solution. In order to implement this product as a secure remote access solution for corporate email, a through audit and risk assessment will be performed to ensure compliance with corporate policy as well as applicable regulations and laws, i.e. Gramm-Leach Bliley Act, Sarbanes-Oxley, etc. The solution must meet the following criteria:

- Secure remote access to corporate email
- Simple user interface (web browser)
- Two-factor strong authentication
- Logging of all activity
- Appropriate level of control regarding corporate information and data
- Accessible from any computer with Internet access
- Zero Footprints left on computer utilized for access

This audit will determine if the solution meets the above criteria, if gaps exist and their associated risk, if additional controls can be implemented to eliminate the gaps, as well as a recommendation regarding implementation.

# Significant Risks

# **Threat Impact Analysis**

A threat is defined as an event/s that impact the operation of the asset, or the value of the asset and/or products produced by the asset (Nichols). Threats may prevent, alter the operation, or corrupt the operation of the asset (Nichols). A threat has the capacity to inflict damage, when this occurs it creates an impact on the corporation. The impact can be felt in many ways, disruptions in business, loss of productivity, violation of regulations and laws, privacy violations, criminal activity and fraud, loss or alteration of data, reputational consequences, decline of stock value, as well as others. The impact can manifest itself in one or multiple ways immediately or over time.

Threat	Impact
Corporate data residing on non-corporate assets	Improper disclosure of corporate information. Cyber-crime and terrorism is becoming a growing concern for financial institutions due to the volume of financial transactions that are occurring over electronic networks, both public and dedicated networks.
Unauthorized Access	Improper access to corporate systems In a report released March 5, 2003, "Efforts of the Financial Services Sector to Assess Cyber Threats," the U.S. General Accounting Office concluded that entities handling monetary transactions face a particularly high risk of attack by criminals or terrorist organizations (Glasner). The attractiveness for criminals and terrorist to attack financial institutions is for financial gain and/or disruption to the U.S. economy.
Virus, worms, Trojans, and other malware being introduced to the corporate network	<ul> <li>Data loss or alteration</li> <li>Improper disclosure of corporate information including privacy data</li> <li>Denial of Service attack</li> <li>Loss of productivity</li> <li>The following statistics illustrate the number of incidents reported in 2003 and the estimated business impact (RSA Conference 2004).</li> <li>The number of incidents reported to the CERT coordination center increased 40 percent in 2003.</li> <li>In August 2003, enterprises saw a rapid fire of virus attacks – "Blaster" and "So Big" viruses came with a \$3.5 billion price tag, and are estimated to be responsible for more than 2 million infections</li> </ul>
Non-compliance with applicable regulations and laws • Sarbanes-Oxley • GLBA • California SB 1386 • HIPPA	<ul> <li>Corporation may be subjected to</li> <li>Violations sited by OCC and other regulatory bodies</li> <li>Fines</li> <li>Imprisonment of corporate officers</li> <li>Decline in reputation – customers lose faith in corporation</li> <li>Decline of Stock Value</li> </ul>

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 6 of 60

	Due to the demise of several large corporations over the last few years (i.e. Enron, Anderson). The Federal government has imposed stricter regulations and laws, regarding financial reporting and privacy. At the heart of financial reporting are Information Technology systems that maintain and process the financial data. Information Security provides the controls or the fortress around the systems in order to maintain the credibility of the organizations financial data and processing.
--	--

# **Role of Instant Virtual Extranet 5000**

Technology is a means to an end; corporations will only incur the cost of a technology if it is something that is beneficial to the business. During this proof of concept a business case as well as cost/benefit analysis is being conducted to ensure the solution will be adequately used if implemented.

Role of IVE 5000	Information Asset Affected
Secure remote access to corporate email	Corporate email system and data contained within

# Vulnerability Analysis

Vulnerability is defined as a weakness or deficiency in controls. Exposure factor is a measure of the magnitude of loss or impact on the value of an asset (CISSP Open Study Guide). Exposure factor is expressed as a percent, ranging from 0% to 100%, of asset value loss arising from a threat event (CISSP Open Study Guide). The potential impact to the corporation is then evaluated based on what the impact would be if the vulnerability were exploited. The following table does not take into consideration controls that are implemented to mitigate the vulnerability or decrease the exposure factor. For example a backup/recovery system could reduce the impact that a virus has on the corporation by providing an alternative system that could be inserted in place of the infected system, while it is under going restoration.

Vulnerability	Degree of Exposure	Potential Impact on Corporation
System vulnerable to introduction of a virus, worm, Trojan or other malware into the corporate network	20%	<ul> <li>Data loss or alteration</li> <li>Improper disclosure of corporate information including privacy data</li> </ul>

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 7 of 60

	1	
		Denial of Service attack
		<ul> <li>Loss of productivity</li> </ul>
Denial of Service	100%	<ul> <li>Loss of productivity</li> </ul>
		<ul> <li>Inability to utilize system</li> </ul>
Inappropriate session	20%	Data not encrypted in transport
management (SSL)		resulting in improper disclosure
Inappropriate use of	30%	Data not encrypted in transport
encryption		resulting in improper disclosure
Inappropriate access	40%	<ul> <li>Non-authorized persons</li> </ul>
controls		gaining access or
		privileged access to the
		system
		<ul> <li>Non-employees gaining</li> </ul>
		access to the system
Inappropriate	40%	<ul> <li>Non-authorized persons</li> </ul>
authentication controls		gaining access or
		privileged access to the
		system
	O'	<ul> <li>Non-employees gaining</li> </ul>
		access to the system
Inappropriate level of	35%	<ul> <li>Failure to detect</li> </ul>
logging and monitoring		inappropriate activity or
		breach
		<ul> <li>Lack of forensic evidence</li> </ul>
	050/	
Insecure administration	35%	Unauthorized person gaining
		access or privilege access to
S. S.		system.
Insecure remote	30%	Unauthorized person gaining
administration	5070	access or privilege access to
		system.
Idle session (timeout)	50%	Unauthorized person could
		gain access if user session
$\sim$		becomes idle and does not
		automatically timeout
Corporate data residing	10%	Unauthorized disclosure of
on non-corporate asset		corporate data
Cookies persisting on	10%	Cookies could identify users of
system after log out		system and customizations
	1 · · · · · · · · · · · · · · · · · · ·	

# Technical Vulnerability Assessment Based on OSI Model

The following analysis of vulnerabilities was based on the OSI model. This approach was used to provide a glimpse of the vulnerabilities that can occur at each layer without going into detail and naming each and every vulnerability that exists. Through an understanding of the OSI model and the vulnerabilities associated with each layer, controls can be implemented to reduce the risk at each layer. This approach was used since the purpose of this audit/assessment is to analyze and evaluate the risk of the system.

Technical Vulnerability Assessment Based on OSI Model	Degree of Exposure Reduced by Mitigating Control	Potential Impact on Corporation
1. Physical	5% - System located in building with limited key card access and in server room which has restricted limited key card access	<ul> <li>Unauthorized access to system</li> <li>Denial of Service</li> </ul>
2. Data Link	5% - Two network interface cards (NIC), installed, therefore 2 MAC addresses have been configured - one for user access and one for administrative access	<ul> <li>User interface denial of service – The impact has been reduced due to the implementation of controls. If this occurs the administrative interface can be used to access the system.</li> </ul>
3. Network	N/A	The network and routers that provide access to this system are beyond the scope of this audit/assessment
4. Transport	10% - Server located in DMZ behind a firewall	Denial of Service attack from port scanning. Exploitation of vulnerabilities related to unused open ports, which could result in unauthorized access.
5. Session	5% - SSL (Secure Sockets Layer)	Inappropriate access to system via session hijacking

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 9 of 60

6. Presentation	10% - Coding is in HTML over HTTPS	Acceptance of inappropriate format of data could lead to unauthorized access to restricted directories
7. Application	50% - Anti-virus programs installed on corporate assets	Introduction of a virus, worm, Trojan or other malware into the corporate network

# **Current State of Practice**

Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003. URL:

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=1520 1419&classroom= (January 2004).

Secure Sockets Layer (SSL) for remote access is based on a simple concept: use the encryption and authentication capabilities built into every Web browser to provide secure remote access to corporate applications (Conry-Murray). The greatest asset of a SSL VPN is also its greatest weakness, remote access from any location including home machines, libraries, airport kiosks, Internet cafes, or any other computer with access to the Internet. While the freedom may boost productivity, it also exposes your network to an unlimited number of computers whose security state is unknown (and in some cases unknowable) (Conry-Murray). The unknown security state of computers connecting to your network puts it at risk for infection by virus, worms, Trojans as well as other malware. The SSL VPN System may increase productivity but it also decreases the control over corporate information. An audit/assessment of a SSL VPN System must address these as well as other concerns and determine if the appropriate mitigations are in place or if recommendations can be implemented to decrease the risk.

An audit of a SSL VPN System should address at a minimum the following four concerns (Conry-Murray).

- 1. Users will access corporate resources from untrusted (and untrustworthy) computers
- 2. Strong user authentication requires add-ons
- 3. Remote machines may block applets required for sophisticated SSL remote access
- 4. Sensitive information may remain on the remote machine

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." URL:

http://216.239.51.104/search?q=cache:bmMUT7AhU64J:www.rainbow.com/Libra ry/8/Compliance%2520with%2520an%2520SSL%2520VPN.pdf+rainbow.com+c ompliance+SSL+VPN+Cynthia&hl=en&ie=UTF-8 (April 2004)

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 10 of 60 Provides an audit checklist for a SSL VPN that is derived from the COBIT audit guidelines. The focus of this audit checklist is corporate compliance in regards to the following three objectives.

- 1. Providing a central policy manager for all users employees or outside groups
- 2. Ensuring a high degree of data integrity because of the ability to limit application access and audit data

3. Reducing risk management by limiting the ability to access data Items 1 thru 3. (Kawamura).

Cryptography Research, Inc. "Neoteris System Evaluation." 16 January 2002. Confidential copies can be obtained by contacting Neoteris.

Provides a review of the Neoteris Server focusing on the architecture, security features, and suggestions for deployment

Farmer, Dan. "Review of the Neoteris Instant Virtual Extranet (IVE) Appliance." January 2002. URL:

http://216.239.51.104/search?q=cache:cSchiDsBUHIJ:www.ipm.com/fileadmin/P DF/Neoteris/Farmer\_Security\_report.pdf+Dan+Farmer+January+2002+review+n eoteris&hl=en&ie=UTF-8 (March 2004).

Examination of a IVE appliance focusing on the following topics; security, VPNs, Problems with VPNs, Trust, Complexity and Cryptography, Auditing, Education, IVE – Redux, and Potential Problems.

Neoteris. "Securing Remote Access, whitepaper." November 2002. Confidential copies can be obtained by contacting Neoteris.

The paper describes how the IVE can increase security, the current security landscape, security principles related to remote access, points of attack that can be made more vulnerable by remote access solutions, and how deploying the IVE can reduce the risk of a remote access solution and increase overall security

# Audit Checklist

# Item Number 1: Port Scan – checking for open ports

Reference:

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

**Risk:** Exploitation of vulnerabilities related to unused open ports, which could result in unauthorized access.

#### **Testing Procedure:**

Perform the following nmap scan Nmap –sS -O -v –p 1-65535 xxx.xxx.xxx.xxx

sS – TCP Syn scan – half open scanning

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 11 of 60 O – remote host identification via TCP/IP fingerprinting

v - verbose

p – scan port range 1-65535

xxx.xxx.xxx.xxx – IP address of SSL VPN System

**Compliance Criteria:** Port 443 is the only port open on the system.

Test Nature: Objective

The purpose of this audit item is to ensure that only ports necessary for proper operation of the system remain open. All other ports are to be closed, ensuring that the ports are appropriately locked down.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

#### **Item Number 2: Secure Application Management**

#### **Reference:**

Warden, Waheed. "An Intro to SSL VPN." 1 December 2003, URL: http://www.webpronews.com/it/networksystems/wpn-21-

20031201AnIntrotoSSLVPN.html (March 2004).

**Risk:** Disclosure of corporate data due to downloading or viewing on noncorporate asset. Unauthorized access to system and/or applications

#### **Testing Procedure**

Test A: Secure Application Manager Functioning Properly

- 1. Login to IVE system utilizing username and SecurID passcode
- 2. System will prompt you to view the Certificate. Accept the certificate for this audit item; another audit item will address the integrity of the certificate.
- 3. Verify Secure Application Manager is launched



- 4. Accept Install of Secure Application Manager when prompted
- 5. Verify that a small window appears stating that the Secure Application Manager – Session Manager is started and status is OK – along with a reminder to not close this window
- 6. Access corporate email system you will have to login with your username and password for your email account
- 7. Logout of the system

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 12 of 60

- 8. Screen stating Cache Cleaner will begin
- 9. Upon completion of cache cleaner the system will state that your session has ended and provide a link to login again if you desire.
- 10. Type in a new URL in the address field for example www.yahoo.com
- 11. Click on the back button
- 12. Verify that the pages associated with the IVE system were not visible or accessible, ensuring that the pages have not been locally cached allowing an unauthorized user to obtain access once an authorized user logs out and walks away from the system.

Test B: Secure Application Manager Configuration

- 1. Login to the IVE system as administrator
- 2. From the Central Manager > System > Configuration
- 3. Click on the Security Tab
- 4. Scroll down to the Basic Authentication Intermediation option
- 5. Verify that the Basic Authentication Intermediation has been set to "Enable Intermediation" (maximize security)

🚰 Central Manager - Se	ecurity Options - Microsoft Internet Explorer	<u>_                                    </u>
<u>File E</u> dit <u>V</u> iew F <u>a</u> vo	orites Iools Help	
🗢 Back 🔹 🔿 👻 🙆	계 🕅 @ Search 📷 Favorites 🝏 🛃 - 🎒 🗹 - 🗐	
Address 🕘 https:/	curity/security.cgi 💌 🖉 Go	Links »
Google -	🔄 👽 🖛 arch Web 🔹 🦛 🤲 😻 🛛 📳 AutoFill 🔼 🛛 🛃 Options 💼 👻 🥒	
▷ Troubleshooting	Basic authentication intermediation Browsers cache basic authentication credentials, possibly allowing users to access resources through a shared browser using another user's credentials. The IVE can intermediate basic authentication to prevent this.	
	Enable intermediation (maximize security)	
	m igcap Enable intermediation AND single sign-in for intranet sites (security and convenience)	
	$\Bbbacklinetic {f C}$ Disable intermediation (standard browser behavior, not recommended)	
E	A linernet	

**Compliance Criteria:** Secure application manager has been implemented and functioning properly.

Test Nature: Objective

The purpose of this audit item is to ensure that information does not remain on the system being used to access the SSL VPN and ensure that an unauthorized user cannot gain access to the system. Upon an authorized user logging out of the system an unauthorized user cannot gain access to the IVE by clicking on the back button on the browser. As stated in the IVE System Help file, the secure application manager provides secure application level-remote access to enterprise servers from client applications. The IVE System Help file also stated that enabling intermediate basic authentication would prevent an unauthorized user from accessing resources through a shared browser using another user's credentials. This is a risk due to the fact that browsers often cache basic authentication credentials.

**Evidence:** Placeholder to be completed during audit testing **Findings:** Placeholder to be completed after audit testing

# Item Number 3: Cache Cleaner Reference:

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 13 of 60 Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003. URL:

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=152 01419&classroom= (January 2004).

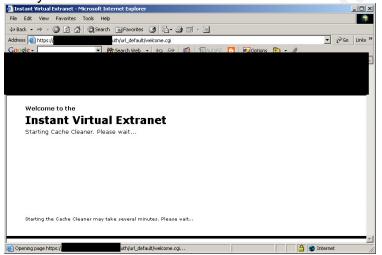
Warden, Waheed. "An Intro to SSL VPN." 1 December 2003, URL: <u>http://www.webpronews.com/it/networksystems/wpn-21-</u>20031201AnIntrotoSSLVPN.html (March 2004).

**Risk:** Disclosure of corporate data due to downloading or viewing on non-corporate asset.

#### Testing Procedure

Test A: Cache Cleaner Functioning Properly

1. Verify that cache cleaner is started



- 2. Login to IVE system utilizing username and SecurID passcode
- System will prompt you to view the Certificate. Accept the certificate for this audit item; another audit item will address the integrity of the certificate.
- 4. Secure Application Manager is launched
- 5. Accept Install of Secure Application Manager when prompted
- Small window will appear stating that the Secure Application Manager Session Manager is started and status is OK – along with a reminder to not close this window
- 7. Access corporate email system you will have to login with your username and password for your email account
- 8. Logout of the system
- 9. Verify that the Cache Cleaner is executed
- 10. Verify that upon completion of cache cleaner the system states that your session has ended and provide a link to login again if you desire.
- 11. Verify that any files viewed during the IVE session have been removed from c:\temp
- 12. Verify that any files viewed during the IVE session do not appear in the

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 14 of 60 list of recent documents. To do this - Click on Start button, Click on documents and view the pop-up list of documents.

Test B: Cache Cleaner Configuration

- 1. Login to the IVE system as administrator
- 2. Under Central Manager > System > Configuration
- 3. Click the Security Tab > Cache Cleaner
- 4. Verify that the cache cleaner is operating and the cleaner frequency and status update frequency have been set according to corporate policy.

**Compliance Criteria:** Automatic removal of all temporary files from system upon logout. Cache cleaner implemented and functioning appropriately.

Test Nature: Objective

The purpose of this audit item is to ensure that corporate data viewed through the SSL VPN does not remain on the machine after the user logs off the system. If the cache is not cleared remnants or whole documents, which may include corporate data, may remain on the system and be viewed by the next person that utilizes the machine.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 4: Warning Banner

#### Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN."

**Risk:** If a warning banner is not present during logon and a criminal or other unauthorized person gains access to the system the prosecution of that crime may not be held up in court.

#### Testing Procedure

- 1. Login to IVE utilizing username and SecurID passcode
- 2. Determine if a warning banner is presented before access is provided to the system.

# Compliance Criteria: Standard corporate warning banner is presented.

Test Nature: Objective

The purpose of this audit item is to ensure that a person accessing the system realizes that the system that they are accessing is a corporate system and unauthorized access to the system is not permitted. Also that upon accessing the system the user is subject to all forms of monitoring, including keystroke monitoring.

**Evidence:** Placeholder to be completed during audit testing **Findings:** Placeholder to be completed after audit testing

# Item Number 5: Removal of Cookies Reference:

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 15 of 60 Cryptography Research, Inc. "Neoteris System Evaluation." 16 January 2002. Confidential copies can be obtained by contacting Neoteris.

Neoteris. "Securing Remote Access, white paper." November 2002. Confidential copies can be obtained by contacting Neoteris.

**Risk:** Cookies could identify systems, applications, users of system and customizations.

#### **Testing Procedure**

Test A: Cookie removal through IVE system

- 1. Login to IVE utilizing username and SecurID passcode
- 2. Click on "Advanced Preferences"
- 3. Verify the number of cookies currently being stored

Instant Virtual I	Extranet - Microsoft Internet Explorer
<u>E</u> lle <u>E</u> dit ⊻iew	Favorites Iools Help
😓 Back 👻 =	arch 🔝 Favorites 🧭 🖏 🖬 🖉 - 🖻
Address 餐 h	(pref/advpref.cgi 🔽 🔗 Go Lini
Coogle -	🔄 📸 Search Web 👻 🦡 🦇 🎁 AutoFill 🤷 🚾 Options 💼 👻 🥒
	Help   Sian Qu
	Advanced Preferences
Browsing	Advanced Freierences
D Bookmarks	The following are advanced options that allow you to manage various information and settings cached on
Applications	the server.
D Client Applications	Cookies
D Terminal Sessions	The server is maintaining 9 cookies from various Web sites. Cookies are small files used by some Web sites to save your preferences and settings. You can remove them if you prefer to do so, but note that doing so may cause some
Meeting	Web sites to reset your preferences and settings.
System	
D Preferences	Delete Cookies
Advanced Preferences	Java Secure Application Manager
	To support client applications, the Secure Application Manager makes changes to your system. In most cases, your system is restored when the Secure Application Manager exits. Click the Restore System Settings button to undo these changes to your system.
	Restore System Settings
	- Xari
Licensed to NetScr	een Evaluation 4.0 A3050 4 Week Ext.

- 4. Click on "Delete Cookies"
- 5. Verify that the current number of cookies now being stored is 0 (zero) and "Cookies have been deleted" appears on screen.

Test B: Cookie removed from browser Netscape Browser

- 1. Select "Edit"
- 2. Select "Preferences"
- 3. Select "Privacy and Security" expand menu
- 4. Select "Cookies" in expanded menu
- 5. Select "Manage Stored Cookies" Radio button
- 6. Select "Stored Cookies" Tab
- 7. Verify that the "Site list" and "Cookie Name" associated with the IVE and corporation have been removed.

**Compliance Criteria:** All cookies associated with the IVE system have been removed.

**Test Nature:** Objective The purpose of this audit item is to ensure that cookies are removed from the

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 16 of 60 system that is being utilized for access. Cookies often contain information such as user ids, passwords, preferences, configurations, etc. By viewing and obtaining the cookie an unauthorized person may be able to gain knowledge of the system and how it works.

Evidence: Placeholder to be completed during audit testing

**Findings:** Placeholder to be completed after audit testing

#### Item Number 6: Authentication-Administrator Password Policy Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." **Risk:** Weak passwords can be easily guessed/compromised allowing unauthorized access to the system.

#### **Testing Procedure**

- 1. Login into the IVE system as administrator
- 2. From the Central Management Page > Administrators > Authentication
- 3. Click on the Authentication Policy Tab then the Password Option

🕗 Central Manager - Au	thentication - Restrictions - Microsoft Internet Explorer
File Edit View Favor	nites Iools Help
🗢 Back 🔹 🔿 👻 🔯	Al @Search GilFavorites 🚳 🔂 - 🎒 🗹 - 🗐
Address 🕘 https:/	rtificate=0&PolicyRealm=1&isAnonymous=0&realmType=admin 💌 🔗 🐻 Links
Google -	💌 💏 Search Web 🔹 😽 🕬 🤯 📲 AutoFili 🧕 🛃 Options 💼 🔹 🥒
Central Manage	Help   Sign Out
System	Administrator Authentication Realms > Admin Users
D Status	Admini Osers
D Configuration D Network	General Authentication Policy Role Mapping
D Clustering	Source IP   Browser   Certificate   Password   Host Checker   Limits
D Log/Monitoring	Source IP   Drowser   Certificate   Password   Host Checker   Limits
D Signing In	Options
Administrators	Options
Authentication	Allow all users (passwords of any length)
D Delegation	Only allow users that have passwords of a minimum length:
Users	
D Authentication	Minimum Length: 4 characters
D Roles D New User	Note: Local user and administrator passwords must always be at least 6 characters, regardless of the value entered for the minimum length.
Resource Policies	Password Management
	rasshord management
D Web D Files	🗹 Enable Password Management
D SAM	
D Teinet/SSH	
D Network Connect	Save Changes ?
D Meetings D Email Client	Save Changes
Maintenance	
D System	
D Import/Export	
D Push Config	
 ല്	🔒 🧧 Internet

- Verify the password length complies with the corporate password policy. Please be advised of the Note listed beneath minimum length. Note: Local user and administrator passwords must always be at least 6 characters, regardless of the value entered for the minimum length.
- 5. A manual audit will need to be performed to verify the remainder of the compliance items listed in the password policy.

**Compliance Criteria:** Back-up administrator passwords are in compliance with the corporate password policy.

#### Test Nature: Objective

Although two-factor authentication is being utilized for user access, a few static passwords exist for administrative access. These static passwords exist as a

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 17 of 60 back-up in case the two-factor authentication system is unavailable and administration of the IVE is necessary. Therefore this audit item will only be verifying that the static administrator passwords comply with the corporate password policy.

The purpose of this audit item is to ensure that the corporate password policy is being appropriately implemented. A copy of the corporate password policy will need to be obtained to complete this item; the corporate password policy is not included in this report due to corporate security and confidentiality concerns. A high-level list of password concerns is listed below:

-Initial logon identifying mandatory password change

-Appropriate password length

-Enforced frequency of password changes

-Password dictionary checking for not allowed passwords

-Password meets complexity requirements

-Protection of emergency passwords

Some of the items in the above list were obtained from the following reference Balancing Security and Compliance with an SSL VPN (Kawamura).

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

#### Item Number 7: Re-authentication required after timeout Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN."

**Risk:** Unauthorized access to the system via a session initiated by a valid user.

# Testing Procedure

- 1. Login to the IVE system
- 2. Walk away leaving the system idle for 15 minutes (According to corporate policy, 15 minutes is the designated timeout for this classification of system)
- 3. Verify that upon returning after 17 minutes that access could not be gained without logging in again, supplying username and password.

**Compliance Criteria:** Session times out after 15 minutes of inactivity.

Test Nature: Objective

The purpose of this audit item is to aid in ensuring that unauthorized access does not occur, as a result of a user failing to log out. For example, a user may walk away from the system being used for access without logging out of the system. If this occurs an unauthorized user could gain access to the system via a session already initiated by a valid user.

**Evidence:** Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 8: Two-factor authentication

#### **Reference:**

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." **Risk:** Risk of unauthorized access to the system increases if a weak authentication mechanism is used.

#### Testing Procedure

Test A: Attempt to login to the IVE system with username and password WARNING: Obtain proper permission and authorization before conducting this type of test. Also ensure that this effort has been coordinated with the system administrator.

- 1. Utilizing Brutus Authentication Engine Test Version 2 to attempt to login to the IVE system with a username and password with the following settings:
- 2. Target IVE System IP address
- 3. Type HTTP (Basic Authentication)
- 4. Port 443
- 5. HTTP try each of the following HEAD, GET, PUT
- 6. UserID Utilize one setup for this testing effort
- 7. Pass Mode Brute Force
- 8. Variations to these settings may be utilized in order to develop a level of comfort that the amount of testing is adequate to

Test B: Verify two-factor authentication configuration settings

- 1. Login to the IVE system as administrator
- 2. Under Central Manager select Users > Authentication
- 3. Verify each of the user Authentication Realms to ensure that users are authenticating to the appropriate server, which is a two-factor authentication solution utilized by the corporation.

**Compliance Criteria:** Authentication to the IVE system is utilizing the corporate standard two-factor authentication system. Users are only able to login in by authenticating with two-factors.

# Test Nature: Objective

The purpose of this audit item is to determine if two-factor authentication is being utilized and ensure that it is implemented appropriately. This will reduce the risk of unauthorized access by requiring two factors for authentication. Twofactor authentication requires something a user knows and something a user possess.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 9: Access Controls

#### Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." **Risk:** Unauthorized users able to access system.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 19 of 60

#### Testing Procedure

- 1. Obtain a username and SecurID token that does not have access to the IVE SSL VPN System.
- 2. Utilizing these credentials attempt to login to the IVE SSL VPN system

**Compliance Criteria:** A user that has not been granted permission to utilize the IVE SSL VPN System is not able to access the IVE SSL VPN System.

Test Nature: Objective

The purpose of this audit item is to ensure that authorization to utilize the SSL VPN is granted via an employee's manager through the provisioning system. Although an employee possess a SecurID token they do not automatically have access to the SSL VPN.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 10: Audit Trail for all transactions

#### **Reference:**

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." **Risk:** Failure to log all transactions can result in a loss of forensic data should a breach or other inappropriate activity occur.

#### **Testing Procedure**

- Test A: Verification of logs
  - 1. Login to the IVE System as administrator
  - 2. Under Central Manager > System > Log Monitoring
  - 3. The following Tabs exist Events, User Access, Admin Access, SNMP, and Statistics. The logging that the corporation is concerned with is Events, User Access, and Admin Access.
  - 4. Go to the Admin Access Tab
  - 5. Verify that upon access the system to perform this audit check, that the admin access was logged.
  - 6. Open another browser
  - 7. Login to the IVE System as a user
  - 8. Go back to the first browser (admin login) and select the User Access Tab
  - 9. Verify that upon logging in as a user that the user access was logged.

#### Test B: Log Setting Verification

- 1. Login to the IVE System as administrator
- 2. Under Central Manager > System > Log Monitoring
- 3. The following Tabs exist Events, User Access, Admin Access, SNMP, and Statistics. The logging that the corporation is concerned with is Events, User Access, and Admin Access.
- 4. Go to the Admin Access Tab > Settings
- 5. Verify that the appropriate administrator access activities being logged are in compliance with corporate logging requirements

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 20 of 60

- 6. Go to the User Access Tab > Settings
- 7. Verify that the appropriate user access activities being logged are in compliance with corporate logging requirements
- 8. Go to the Events Tab > Settings
- 9. Verify that the appropriate event activities being logged are in compliance with corporate logging requirements.

**Compliance Criteria:** All system accesses are logged. Events are logged according to corporate policy.

Test Nature: Objective

The purpose of this audit item is to ensure that required transactions are logged/monitored. This will also help to ensure that the corporation is in compliance with applicable laws and regulations by ensuring a full audit trail exists and documents the controls structure that is in place for handling corporate data.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 11: Segregation of Duties

#### Reference:

Personal experience as well as conversations with auditors regarding applicable regulations and laws pertaining to the financial services industry.

Risk: Failure to detect malicious or inappropriate activity

#### **Testing Procedure**

- 1. Login to the IVE System as administrator
- 2. Under Central Manager > Administration > Delegation
- 3. Select an admin role
- 4. Select the System Tab
- 5. Verify the access rights that the administrator has to each aspect of the system ensuring that proper segregation of duties is present for the administrators.

	-	n - Microsoft Internet Explorer		
	ites <u>T</u> ools <u>H</u> elp			-
⇐ Back    ⇒    🙆 🔮		es 🎯 🖏 🗃 🖬 🖌 🗒		1
Address i http:		adminRoleSystem.cgi?role=0000000001.000003.0		Links »
Google -	💌 💏 Search Wel	b 🔹 🚧 🚧 🎼 AutoFill 🕒 🛃 Options 🛅 🔹 🥒		
D Configuration				-
D Network	General System U	ser Role Admin		
<ul> <li>Clustering</li> <li>Log/Monitoring</li> <li>Signing In</li> </ul>	Specify allowed system	n and policy functions for this administrator role.		
Administrators	System tasks	Write All		
<ul> <li>Delegation</li> </ul>	Status*:	Write Clustering: Write		
Users	Configuration:	Write Log/Monitoring Write		
D Authentication	Network:	Write		
D Roles D New User		,		
Resource Policies	Maintenance tasks	Write All		
D Web	System:	Write Archiving: Write		
D Files D SAM	Troubleshooting:	Write		
D Telnet/SSH	in outside in the string.			
<ul> <li>Network Connect</li> <li>Meetings</li> </ul>	Resource policies	Write All		
D Email Client	Web:	Write Files: Write		
Maintenance	SAM:	Write Telnet/SSH: Write		
D System	Network Connect:			
<ul> <li>Import/Export</li> <li>Push Config</li> </ul>	Email Client:	Write		
D Archiving	Linai Client.	VVILC		
D Troubleshooting	Users			
	Authentication:	Write 💌		
Done			🔒 🥥 Internet	

**Compliance Criteria:** Proper segregation of duties exists so that malicious or inappropriate activity can be detected.

Test Nature: Objective

The purpose of this audit item is to determine is appropriate segregation of duties exists. Lack of segregation of duties can result in an administrator having access to the data on the system, access controls, provisioning of users, log files, security controls, etc. This provides the administrator the ability to perform malicious or inappropriate activity and then cover their tracks, removing all traces of the malicious or inappropriate activity.

Evidence: Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 12: Encryption – Secure Sockets Layer (SSL)

Reference:

Larsen, Rich. "An Overview of the SSL Protocol and Application to Virtual Private Networks", 29 September 2003, URL:

http://www.giac.org/practical/GSEC/Rich\_Larsen\_GSEC.pdf (March 2004).

**Risk:** If session is not encrypted a man in the middle could capture and read the data being accessed. Weak encryption algorithms and their implementation could lead to compromise, loss, or alteration of data.

#### **Testing Procedure**

- 1. Login to IVE SSL VPN System as administrator
- 2. Under Central Manager > System > Configuration
- 3. Select the Security Tab > Security Options
- 4. Verify that only SSL V3 and TLS are permitted
- 5. Verify that encryption strength must be 128-bit or greater

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 22 of 60 **Compliance Criteria:** Encryption Strength is 128-bit or stronger, complying with corporate policy. Browser accessing IVE SSL VPN System must utilize SSL V3.

#### Test Nature: Objective

The purpose of this audit item is to ensure that not only is the session encrypted preventing unauthorized access to the data while in transport but the encryption strength is in compliance with the corporate policy of 128-bit or greater.

**Evidence:** Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Item Number 13: Valid SSL certificate

#### **Reference:**

Larsen, Rich. "An Overview of the SSL Protocol and Application to Virtual Private Networks", 29 September 2003, URL:

http://www.giac.org/practical/GSEC/Rich\_Larsen\_GSEC.pdf (March 2004).

#### **Risk:** Unauthorized access to the system.

#### **Testing Procedure**

- 1. Type in URL of IVE SSL VPN System into the browser address bar
- 2. A Security Alert will be displayed
- 3. Verify that the information presented in the Security Alert is appropriate
- 4. Click on Examine Certificate
- 5. Verify the certificate general information and details.

**Compliance Criteria:** The certificate is a valid certificate from a trusted CA (Certificate Authority) and utilizes corporate approved encryption.

Test Nature: Objective

The purpose of this audit item is to ensure that a user is accessing the appropriate system. The SSL certificate verifies that the system that is being accessed is owned/operated by the party that user believes it to be. For example a man in the middle type of attack could occur when a user attempts to access the system but instead accesses a malicious system, via a redirect from the malicious system. This malicious system could then capture the logon credentials and use them to perform a valid logon to the system, resulting in an unauthorized person access the system via a valid logon.

**Evidence:** Placeholder to be completed during audit testing **Findings:** Placeholder to be completed after audit testing

# Item Number 14: Control of corporate data – Host Checker Reference:

Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003.

**Risk:** Inappropriate disclosure or unauthorized access to corporate data

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 23 of 60

#### **Testing Procedure**

Test A: Host Checker Implementation and Configuration

- 1. Login to IVE system as administrator
- 2. Under Central Manager > System > Configuration > Security
- 3. Select the Host Checker Tab
- 4. View the Host Checker Policies
- 5. Verify that a Host Checker Policy exists that will determine if the asset is a corporate asset, this can occur through verification of one or more of the following: a custom DDL, a specific file, a certain process, or a registry setting.
- 6. Upon obtaining the Host Checker Policy Verification items examine a corporate asset to determine if these items exist.
- 7. Then examine a non-corporate asset to determine if these items exist.

Test B: Verification of privileges when accessing IVE System through Corporate asset

- 1. Login to IVE System from a Corporate Asset
- 2. Access the email system
- 3. Open an email message containing an attachment
- 4. Open the attachment
- 5. Attempt to download the attachment to the local machine.
- 6. Verify that the attachment could be downloaded.

Test C: Verification of Privileges when accessing IVE System through a non-Corporate asset.

- 1. Login to IVE System from a non-Corporate Asset
- 1. Access the email system
- 2. Open an email message containing an attachment
- 3. Open the attachment
- 4. Attempt to download the attachment to the local machine.
- 5. Verify that the attachment could NOT be downloaded.

**Compliance Criteria:** A unique identifier will exist on a Corporate owned asset that can be verified by the Host Checker before allowing a user certain privileges on the system, such as downloading attachments. Users are not able to download attachments to non-Corporate assets.

#### Test Nature: Objective

The purpose of this audit item is to ensure that adequate controls are in place to prevent inappropriate disclosure of corporate data. If a user is able to download email attachments then corporate data may end up on non-corporate assets, resulting in inappropriate disclosure and unauthorized access to corporate data. If a user is accessing the IVE SSL VPN System on a Corporate owned asset the user will have the ability to download attachments to that asset. However if the user is access the IVE SSL VPN System on a public or shared asset, non-corporate then they will not be able to download attachments. **Evidence:** Placeholder to be completed during audit testing

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 24 of 60 **Findings:** Placeholder to be completed after audit testing

# Item Number 15: Protection against viruses, worms, Trojans, etc.

#### **Reference:**

Henderickson, Dana. "Are SSL VPNs Secure and Flexible Enough?." March 2003. URL: <u>http://www.breakawaymg.com/readingroom/bmg\_sslvpn1.pdf</u> (March 2004).

**Risk:** Point of entry into the corporate network for viruses, worms, Trojans, etc, which may result in data loss or alteration, improper disclosure of corporate information including privacy data, denial of Service attack, loss of productivity as well as other damage.

#### Testing Procedure

- 1. Login to IVE system as administrator
- 2. Select Users > Authentication
- 3. Click on the Authentication Policy Tab
- 4. Click on Host Checker
- 5. Verify that Host Checker is required for all users.

**Compliance Criteria:** Host Checker is implemented and functioning properly. Policies exist to only allow hosts that have the required anti-virus program and/or firewall.

Test Nature: Objective

The purpose of this audit item is to ensure that adequate controls are in place to prevent viruses, worms, Trojans, and other malicious programs from being introduced to the corporate network.

**Evidence:** Placeholder to be completed during audit testing

Findings: Placeholder to be completed after audit testing

# Audit Testing – Evidence and Findings

# Item Number 2: Secure Application Management

#### Reference:

Warden, Waheed. "An Intro to SSL VPN." 1 December 2003, URL: <u>http://www.webpronews.com/it/networksystems/wpn-21-</u>

20031201AnIntrotoSSLVPN.html (March 2004).

**Risk:** Disclosure of corporate data due to downloading or viewing on noncorporate asset. Unauthorized access to system and/or applications

#### **Testing Procedure**

Test A: Secure Application Manager Functioning Properly

- 1. Login to IVE system utilizing username and SecurID passcode
- 2. System will prompt you to view the Certificate. Accept the certificate for this audit item; another audit item will address the integrity of the

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 25 of 60 certificate.

- 3. Verify Secure Application Manager is launched
- 4. Accept Install of Secure Application Manager when prompted
- Verify that a small window appears stating that the Secure Application Manager – Session Manager is started and status is OK – along with a reminder to not close this window
- 6. Access corporate email system you will have to login with your username and password for your email account
- 7. Logout of the system
- 8. Screen stating Cache Cleaner will begin
- 9. Upon completion of cache cleaner the system will state that your session has ended and provide a link to login again if you desire.
- 10. Type in a new URL in the address field for example www.yahoo.com
- 11. Click on the back button
- 12. Verify that the pages associated with the IVE system were not visible or accessible, ensuring that the pages have not been locally cached allowing an unauthorized user to obtain access once an authorized user logs out and walks away from the system.

Test B: Secure Application Manager Configuration

- 1. Login to the IVE system as administrator
- 2. From the Central Manager > System > Configuration
- 3. Click on the Security Tab
- 4. Scroll down to the Basic Authentication Intermediation option
- 5. Verify that the Basic Authentication Intermediation has been set to "Enable Intermediation" (maximize security)

**Compliance Criteria:** Secure application manager has been implemented and functioning properly.

# Test Nature: Objective

The purpose of this audit item is to ensure that information does not remain on the system being used to access the SSL VPN and ensure that an unauthorized user cannot gain access to the system. Upon an authorized user logging out of the system an unauthorized user cannot gain access to the IVE by clicking on the back button on the browser. As stated in the IVE System Help file, the secure application manager provides secure application level-remote access to enterprise servers from client applications. The IVE System Help file also stated that enabling intermediate basic authentication will prevent an unauthorized user from accessing resources through a shared browser using another user's credentials. This is a risk due to the fact that browsers often cache basic authentication credentials.

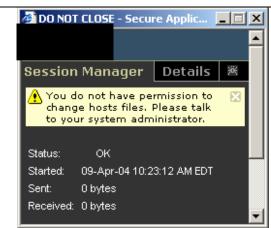
#### Evidence:

Test A: Secure Application Manager Functioning Properly 3) Verify Secure Application Manager is launched

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 26 of 60

DO NOT CLOSE - Secu LoadingPlease Please wait for the se to load before launchi applications.	Wait ssion manager
4) Accept Install of Se	ecure Application Manager when prompted
Security Warning	Do you want to install and run "C:\DOCU         \LDCALS*T\Temp\UVM9.tmp" signed on 27772004 2:08         AM and distributed by:         NetScreen Technologies, Inc.         Publisher authenticity verified by VeriSign Class 3 Code         Signing 2001 CA         Caution: NetScreen Technologies, Inc. asserts that this content is safe. You should only install/view this content if you trust NetScreen Technologies, Inc. to make that assertion.         SIGNED WITH PERMISSIONS Full Permissions <ul> <li>Always trust content from NetScreen Technologies, Inc.</li> </ul>
	Yes More Info
, .	window appears stating that the Secure Application lanager is started and status is OK – along with a reminder

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 27 of 60

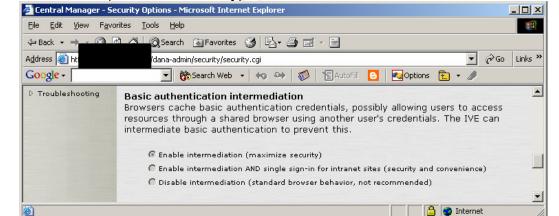


12) Verify that the pages associated with the IVE system were not visible or accessible, ensuring that the pages have not been locally cached allowing an unauthorized user to obtain access once an authorized user logs out and walks away from the system.

Clicking the Back button did not give access to the system. The login page was presented requiring the user to re-authenticate to obtain access to the system

Test B: Secure Application Manager Configuration

5) Verify that the Basic Authentication Intermediation has been set to "Enable Intermediation" (maximize security)



#### Findings:

- Upon logging into the IVE SSL VPN System the Secure Application Manager successfully launches
- A small temporary file is installed on the sytem being utilized to access the IVE SSL VPN System, which is removed upon logging out.
- The Session Manager window must remain open and active while a user is logged into the IVE SSL VPN System.
- Upon logging off the IVE SSL VPN System, access cannot be gained by clicking the Back button on the browser. When this occurs the user is presented with the log in page which requires the user to re-authenticate.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 28 of 60

# Item Number 3: Cache Cleaner

#### **Reference:**

Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003. URL:

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=152 01419&classroom= (January 2004).

Warden, Waheed. "An Intro to SSL VPN." 1 December 2003, URL: <u>http://www.webpronews.com/it/networksystems/wpn-21-</u>20031201AnIntrotoSSLVPN.html (March 2004).

**Risk:** Disclosure of corporate data due to downloading or viewing on non-corporate asset.

#### **Testing Procedure**

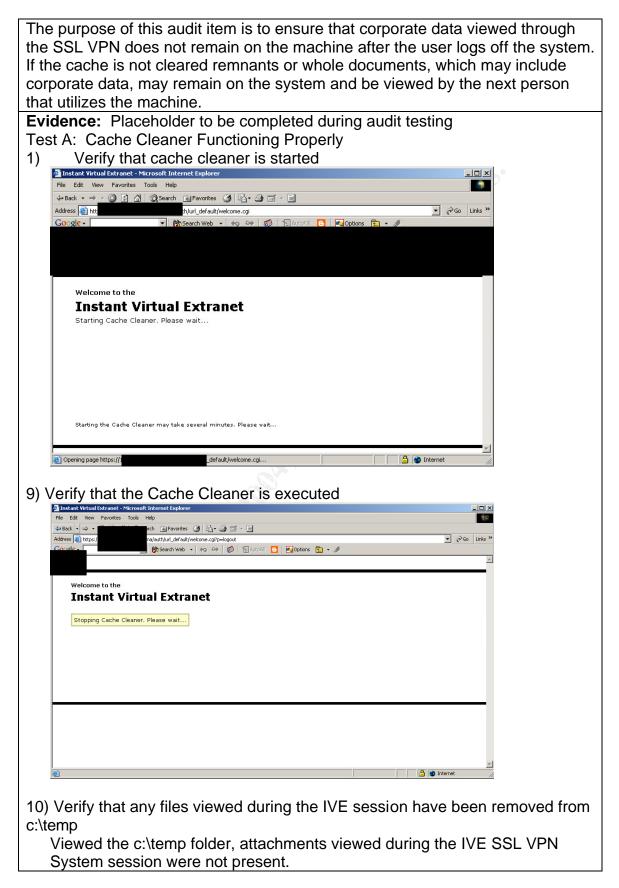
Test A: Cache Cleaner Functioning Properly

- 1. Verify that cache cleaner is started
- 2. Login to IVE system utilizing username and SecurID passcode
- 3. System will prompt you to view the Certificate. Accept the certificate for this audit item; another audit item will address the integrity of the certificate.
- 4. Secure Application Manager is launched
- 5. Accept Install of Secure Application Manager when prompted
- Small window will appear stating that the Secure Application Manager Session Manager is started and status is OK – along with a reminder to not close this window
- 7. Access corporate email system you will have to login with your username and password for your email account
- 8. Logout of the system
- 9. Verify that the Cache Cleaner is executed
- 10. Verify that any files viewed during the IVE session have been removed from c:\temp
- 11. Verify that any files viewed during the IVE session do not appear in the list of recent documents. To do this Click on Start button, Click on documents and view the pop-up list of documents.

# Test B: Cache Cleaner Configuration

- 1. Login to the IVE system as administrator
- 2. Under Central Manager > System > Configuration
- 3. Click the Security Tab > Cache Cleaner
- 4. Verify that the cache cleaner is operating and the cleaner frequency and status update frequency have been set according to corporate policy.

**Compliance Criteria:** Automatic removal of all temporary files from system upon logout. Cache cleaner implemented and functioning appropriately. **Test Nature:** Objective



----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 30 of 60 11) Verify that any files viewed during the IVE session do not appear in the list of recent documents. To do this - Click on Start button, Click on documents and view the pop-up list of documents.

Viewed the list of recent documents, attachments viewed during the IVE SSL VPN System session were not present.

Test B: Cache Cleaner Configuration

4) Verify that the cache cleaner is operating and the cleaner frequency and status update frequency have been set according to corporate policy.

Concile Concile Contral Manager  System Configuration Conf	🎒 Central Manager - Ca	ache Cleaner Settings - Microsoft Internet Explorer	
Address is https:// Google	Ele Edit View Favo	vites Iools Help	19 (B)
Coorder <ul> <li>Status</li> <li>Status</li> <li>Configuration</li> <li>Status</li> <li>Configuration</li> <li>Status</li> <li>Status<td>🗢 Back 🔹 🔿 👻 🧰</td><td>Search 📾 Favorites 🧭 🛃 - 🎒 🗹 - 🗐</td><td></td></li></ul>	🗢 Back 🔹 🔿 👻 🧰	Search 📾 Favorites 🧭 🛃 - 🎒 🗹 - 🗐	
Concile Contral Manager  Configuration  System Configuration Status Configuration Status Configuration Configuration Configuration Status Configuration Conf	Address 🙆 https://	ana-admin/auth/ccsettings.cgi	▼ 🖓 Go Links ×
Central Manager       Web   Sign dot _         System       Configuration         Status       Configuration         Status       Configuration         Network       Certificates         Network       Security Options         Status       Security Options         Clearer       Certificates         Security Options       Host Checker         Security Options       Host Checker         Administrators       Clearer Frequency :         Delegation       Status Update Frequency :         Seres       Save Dices         Net User       Save Changes         System       Save Changes         Status Update Frequency :       Save Changes         Status Update Frequency :       Save Changes         Net User Officer       Save Changes         Status Update Frequency :       Save Changes         Status       Save Changes	Google -	🔻 🎆 Search Web 👻 🦡 🦇 🧊 🔚 Autoriti 🧕 🔽 Options 🛐 🕶 🥒	
System       Configuration         I status       Configuration         Network       Security Options   Host Checker   Cache Cleaner         I consider in the Cleaner       Security Options   Host Checker   Cache Cleaner         Administrators       Cleaner Frequency :			Help   Sign Out 🗖
Status       Configuration         Configuration       Cicensing       Security       Certificates         Network       Security Options   Host Chacker   Cache Cleaner       Security Options   Host Chacker   Cache Cleaner         Administrators       Cleaner Frequency :			
Conserved Conse	System	Configuration	
Classifier       Security Options       Host Checker       Cashe Cleaner         D Log/Monitoring       D Log/Monitoring       D Log/Monitoring       D Log/Monitoring         D Log/Monitoring       Cleaner Frequency:       20 minutes min=1, max=60         D Authonication       Status Update Frequency:       5 minutes min=1, max=60         D Authonication       Status Update Frequency:       5 minutes min=1, max=60         D Authonication       Save Changes       Save Changes         D Net User       Save Changes       Save Changes         D Wab       Files       Save Changes         D Network Conect       Save Changes       Save Changes         D Network Conect       Entail Cleanet       Save Changes         D System       D Import/Sport       Save Changes         D Status Conect       Save Changes       Save Changes         D System       Save Changes       Save Changes         D System       Save Changes       Save Changes         D Status Conect       Save Changes       Save Changes         D System       Save Changes       Save Changes         D Save Changes       Save Changes       Save Changes         D Save Changes       Save Changes       Save Changes		Licensing Security Certificates	
<ul> <li>Log/Monitoring</li> <li>Signing In</li> <li>Administrators</li> <li>Administrators</li> <li>Authentication</li> <li>Status Update Frequency: 20 minutes min=1, max=60</li> <li>Status Update Frequency: 3 minutes min=1, max=60</li> <li>Authentication</li> <li>Authentication</li> <li>Rela</li> <li>New User</li> </ul> Resource Policies           Status Update Frequency: New User           P Authentication           Status Update Frequency:           Some Changes             New User             New User             Status Update Frequency:             Some Changes             New User             Status Update Frequency:             Some Changes             New User             Some Changes             Status Update Frequency:             Some Changes             Status Update Frequency:             Status Update Frequency:             Some Changes             Status Update Frequency:             Some Changes             Status Update Frequency:             Status Updat		Security Options   Host Checker   Cache Cleaner	
Administrators       Cleaner Frequency : 20 minutes min=1, max=60         > Autentication       Status Update Frequency: 5 minutes min=1, max=60         Users       Autentication         > Autentication       Save Changes         > Autentication       Save Changes         > Nav User       Save Changes         > Nav User       Save Changes         > Wab       Save Changes         > False       Save Changes         > Save Distance       Save Distance         > Save Distance       Save Distance         > Save Distance       Save Distance	D Log/Monitoring		
Cleaner Frequency:     20     minutes min=1, max=60       Valuentication     Status Update Frequency:     iminutes min=1, max=60       Valuentication     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes       Nave User     Serve Changes       Status Update Frequency:     Serve Changes <td>D Signing In</td> <td></td> <td></td>	D Signing In		
<ul> <li>Authentication</li> <li>Authentication</li> <li>Status Update Frequency: s minutes min=1, max=60</li> <li>Users</li> <li>Authonication</li> <li>Barler</li> <li>Status Changes</li> <li>New User</li> <li>New User</li> <li>New User</li> <li>Rescurre Policies</li> <li>Wab</li> <li>Files</li> <li>SaM</li> <li>SaM</li> <li>Status Changes</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Insert/StH</li> <li>Strain Changes</li> </ul>	Administrators		
Users   Authoritication  Resource Policies  Save Changes  New User  Resource Policies  Save Changes  New Use  Resource Policies  Save Changes  New Use  Resource Policies  Save Changes  New Use  Resource Policies  Save Changes  Save Changes Save Changes  Save Changes  Save Changes  Save Changes  Save Changes  Save Changes  Save Changes Save Changes  Save Changes Sa	D Authentication	Cleaner Frequency : [20 minutes min=1, max=60	
Authentication     Bone Changes       New User     Resource Policies       Sease     Policies       Web     Policies       SAM     Policies       SAM     Policies       Same     Policies       Same     Policies       Same     Policies       Same     Policies       Mattering     Policies       Mattering     Policies       Same     Policies       Disport/Sport     Policies       Policies     Policies	Delegation	Status Update Frequency: 5 minutes min=1, max=60	
Bear     Save Changes       New User     Resource Policies       Web     Image: Same Same Same Same Same Same Same Same	Users		
New Usar       P New Usar	D Authentication		
Resource Policies		Save Changes	
Wab       D Files       D SaM       D TalneyS9H       D Network Connet       D Methods	D New User		
Files       > SAM       > Telney\$SH       > Netwick Connect       > Meetings       > Email Client       Maintenance       > System       > Import[sport]       > Pachonip       > Achume	<b>Resource Policies</b>		
D SAM D Talnet/SM D Talnet/SM D Talnet/SM D Metring D Metring D Final Clent Maintenance D System D System D Import/sport D Import/sport D Auchimage D	▷ Web		
Image: SSH         D Network Connect         D Meetings         D Email Client         Maintenance         D System         D System         D Import/Sport         D Amongo         Adultion         Adultion			
D Nativark Connect D Materians D Final Clent Maintenance D System D Import/sport D Import/sport D Puth Config D Adultion T T T T T T T T T T T T T T T T T T T			
D Meetings D Final Clent Mainteance S system D Import/Export D Public Config D Addulare Addu			
Maintenance	D Meetings		
> System           > Import/Export           > Push Config           > Andreine	D Email Client		
D Import/Export           D Push Config           D Addulation	Maintenance		
D Push Config	D System		
N Aveluina	D Import/Export		
	e Archiving		🔒 🙍 Internet

#### Findings:

- Upon accessing the IVE SSL VPN System, even before the login screen is presented to the user the cache cleaner is started.
- Upon logging out or session timeout the cache cleaner is executed again and then stopped.
- Files viewed during the session do not appear in the c:\temp folder.
- Files viewed during the session do not appear in the list of recent documents.
- Cache Cleaner is implemented and configured to perform a status update every 5 minutes and perform the cache cleaner function every 20 minutes. This is in compliance with corporate policy.

# Item Number 4: Warning Banner

# Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN."

**Risk:** If a warning banner is not present during logon and a criminal or other unauthorized person gains access to the system the prosecution of that crime may not be held up in court.

# **Testing Procedure**

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 31 of 60

- 1. Login to IVE utilizing username and SecurID passcode
- 2. Determine if a warning banner is presented before access is provided to the system.

Compliance Criteria: Standard corporate warning banner is presented.

# Test Nature: Objective

The purpose of this audit item is to ensure that a person accessing the system realizes that the system that they are accessing is a corporate system and unauthorized access to the system is not permitted. Also that upon accessing the system the user is subject to all forms of monitoring, including keystroke monitoring.

# Evidence:

Upon logging onto system a warning banner was not presented.

# Findings:

Upon logging into the IVE SSL VPN System a warning banner was not presented.

# Item Number 5: Removal of Cookies

# **Reference:**

Cryptography Research, Inc. "Neoteris System Evaluation." 16 January 2002. Confidential copies can be obtained by contacting Neoteris.

Neoteris. "Securing Remote Access, whitepaper." November 2002. Confidential copies can be obtained by contacting Neoteris.

**Risk:** Cookies could identify systems, applications, users of system and customizations.

# **Testing Procedure**

Test A: Cookie removal through IVE system

- 1. Login to IVE utilizing username and SecurID passcode
- 2. Click on System > Advanced Preferences > Cookies
- 3. Verify the number of cookies currently being stored

	tranet - Microsoft Internet Explorer	
	gontos jour jour 2 2 2 QSearch BaFavorites (3 Es+ 2 2 2 - 5	
	vpref.cgi 💌 🖉 🍘	inks »
	earch Web 👻 🏟 🐼 🔀 AutoFil 🖸 🔩 Options 💼 👻 🥒	
	Advanced Preferences	ut .
Browsing		
D Bookmarks Applications	The following are advanced options that allow you to manage various information and settings cached or the server.	
D Client	Cookies	
Applications D Terminal	The server is maintaining 9 cookies from various Web sites. Cookies are small files used by some Web sites to save	
Sessions D Meeting	your preferences and settings. You can remove them if you prefer to do so, but note that doing so may cause some Web sites to reset your preferences and settings.	
System	Delete Cookies	
Preferences     Advanced		
Preferences	Java Secure Application Manager	
	To support client applications, the Secure Application Manager makes changes to your system. In most cases, your system is restored when the Secure Application Manager exits. Click the Restore System Settings button to undo these changes to your system.	
	changes to your system.	
	Restore System Settings	
Licensed to NetScre	en Evaluation 4.0 A3050 4 Week Ext.	_
🖉 Done	🔒 💓 Internet	11.
4. Click	c on "Delete Cookies"	
5. Verit	y that the current number of cookies now being	stored is 0 (zero)
	"Cookies have been deleted" appears on scree	· · · · ·
anu	Cookies have been deleted appears on scree	
-		
est B: Co	okie removed from browser	
etscape E	Browser	
	ct "Edit"	
	ct "Preferences"	
3. Sele	ct "Privacy and Security" expand menu	
4. Sele	ct "Cookies" in expanded menu	
	ct "Manage Stored Cookies" Radio button	
	ct "Stored Cookies" Tab	
7. Veri	y that the "Site list" and "Cookie Name" associa	ated with the IVE and
corp	oration have been removed.	
00.15		
•	e Criteria: All cookies associated with the IVE	system have been
moved.		
est Natur	e: Objective	
	e of this audit item is to ensure that cookies are	removed from the
ystem tha	t is being utilized for access. Cookies often cor	itain information such

system that is being utilized for access. Cookies often contain information such as user ids, passwords, preferences, configurations, etc. By viewing and obtaining the cookie an unauthorized person may be able to gain knowledge of the system and how it works.

#### Evidence:

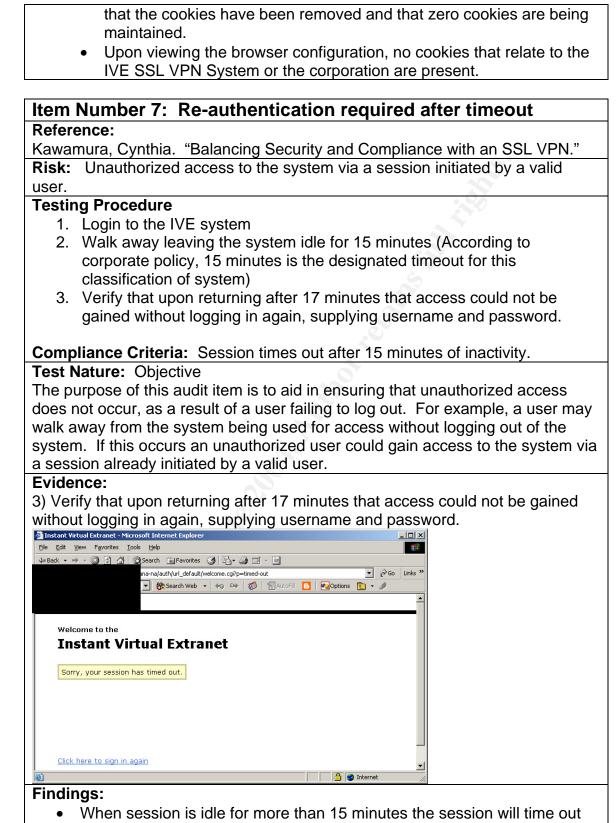
Test A: Cookie removal through IVE system

3) Verify the number of cookies currently being stored

	net - Microsoft Internet Explorer	×
Eile Edit View Favo ⇔ Back → → ~ (2)	nites Iools Help 2) 값 @Q.Search @JFavorites ④ 문과 ④ 37 / 글	
	earch Web 🔻 🔦 🌳 🤯 🔚 AutoFili 🕒 🛃 Options 💼 👻 🥒	
		lp   Sign Out
Browsing	dvanced Preferences	
D Bookmarks T	he following are advanced options that allow you to manage various information and settings c	ached on
Applications	ne server.	
D Client Applications	sookies	
Sessions D Meeting	The server is maintaining 9 cookies from various Web sites. Cookies are small files used by some Web site your preferences and settings. You can remove them if you prefer to do so, but note that doing so may cau Web sites to reset your preferences and settings.	se some
System	Delete Cookies	
Preferences     Advanced     Preferences		
Prenerences	ava Secure Application Manager To support client applications, the Secure Application Manager makes changes to your system. In most case	
	system is restored when the Secure Application Manager exits. Click the Restore System Settings button to changes to your system.	indo these
	Restore System Settings	
Licensed to NetScreen I	ivaluation 4.0 A3050 4 Week Ext.	₹N .
Done		
JUNIES HAV	ve been deleted" appears on screen.	
	kie removal through browser settings	
•	the "Site list" and "Cookie Name" associa	ted with the IVE and
rporation h	nave been removed.	
Cookie Manager		
Stored Cookies Co	okie Sites	
Sites that can and	cannot store cookies on your computer.	
Site	Status	
Remove Site	Remove All Sites	
	Close Help	
ndings:		
• Co	ookies can be removed from the machine I	being utilized to access
the	e IVE SSL VPN System, through System>	Advanced Preferences
	ookies.	
		stom is listed along with
	e number of cookies maintained by the sy	SIGHT IS HOLEY AIVING WILL
the	e option to delete the cookies.	

• Upon Clicking "Delete Cookies" the screen will refresh now stating

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 34 of 60



and the user is required to re-authenticate

## Item Number 10: Audit Trail for all transactions

## Reference:

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." **Risk:** Failure to log all transactions can result in a loss of forensic data should a breach or other inappropriate activity occur.

## Testing Procedure

Test A: Verification of logs

- 1. Login to the IVE System as administrator
- 2. Under Central Manager > System > Log Monitoring
- 3. The following Tabs exist Events, User Access, Admin Access, SNMP, and Statistics. The logging that the corporation is concerned with is Events, User Access, and Admin Access.
- 4. Go to the Admin Access Tab
- 5. Verify that upon access the system to perform this audit check, that the admin access was logged.
- 6. Open another browser
- 7. Login to the IVE System as a user
- 8. Go back to the first browser (admin login) and select the User Access Tab
- 9. Verify that upon logging in as a user that the user access was logged.

## Test B: Log Setting Verification

- 1. Login to the IVE System as administrator
- 2. Under Central Manager > System > Log Monitoring
- 3. The following Tabs exist Events, User Access, Admin Access, SNMP, and Statistics. The logging that the corporation is concerned with is Events, User Access, and Admin Access.
- 4. Go to the Admin Access Tab > Settings
- 5. Verify that the appropriate administrator access activities being logged are in compliance with corporate logging requirements
- 6. Go to the User Access Tab > Settings
- 7. Verify that the appropriate user access activities being logged are in compliance with corporate logging requirements
- 8. Go to the Events Tab > Settings
- 9. Verify that the appropriate event activities being logged are in compliance with corporate logging requirements.

**Compliance Criteria:** All system accesses are logged. Events are logged according to corporate policy.

## Test Nature: Objective

The purpose of this audit item is to ensure that required transactions are logged/monitored. This will also help to ensure that the corporation is in compliance with applicable laws and regulations by ensuring a full audit trail exists and documents the controls structure that is in place for handling corporate data.

#### **Evidence:**

Test A: Verification of logs

5) Verify that upon access the system to perform this audit check, that the admin access was logged.

Logs were reviewed and did contain the following information regarding administrator access; time and date of access, IP of system utilized for access, Administrator ID, Administrator Realm, Authentication server.

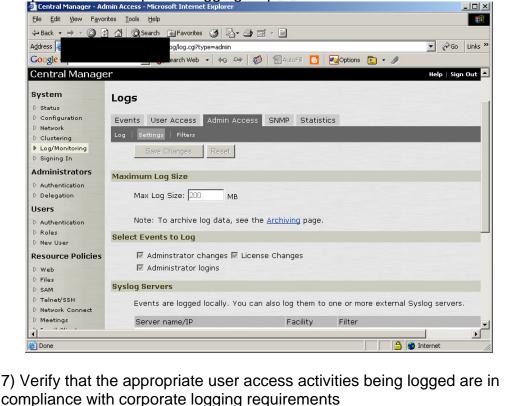
Note: Logs not included in this report due to the amount of scrubbing that would be necessary to prevent disclosure of corporate data.

9) Verify that upon logging in as a user that the user access was logged. Logs were reviewed and did contain the following information regarding user access; time and date of access, IP of system utilized for access, User ID, Authentication server.

Note: Logs not included in this report due to the amount of scrubbing that would be necessary to prevent disclosure of corporate data

Test B: Log Setting Verification

5) Verify that the appropriate administrator access activities being logged are in compliance with corporate logging requirements



	er Access - Microsoft Internet E	xplorer				_ <b>_ _ _</b>
<u>ile E</u> dit <u>V</u> iew F <u>a</u> vo						
⊨ Back 🔹 🔿 👻 [	🖞 🚮 📿 Search 📓 Favorites	3 B - 2 - 3				
d	min/log/log.cgi?ty	pe=access				▼ 🖉 Go Links »
G <mark>oogle -</mark>	🗾 😚 Search Web	•   🐽 👄   😻   📳 Auto	ifil 🕒 🛛	🔽 Options   💼 🔹 🥖		
Central Manag	er					Help   Sign Out 📥
System	Logs					
D Status						
D Configuration	Events User Access	Admin Access SNMP	Statistic	s		
D Network D Clustering	Log   Settings   Filters					
Log/Monitoring	Save Changes	Reset				
D Signing In	Dave Changes	IVEDEL				
Administrators	Maximum Log Size					
D Authentication						
Delegation	Max Log Size: 200	MB				
Jsers						
D Authentication	Note: To archive lo	ig data, see the <u>Archivir</u>	ig page.			
D Roles	Select Events to Log					
D New User	_	-				
lesource Policies	🔽 Login/logout	Web Requests				
D Web	🔽 Java Proxy					
D Files D SAM	Vser Settings	Meeting				
D Telnet/SSH		I 🕅 Email Requests				
D Network Connect	Metwork Conne	ot				
D Meetings D Email Client	Syslog Servers					
Maintenance	Events are logged	locally. You can also log	them to c	ne or more extern	al Syslog servers.	
D System	Server name/IP	Fa	cility	Filter		
· · · · · · · · · · · · · · · · · · ·						
<u>b</u>					🔒 🥥 Ia	nternet

9) Verify that the appropriate event activities being logged are in compliance with corporate logging requirements.

#### Findings:

- The following Administrator Access to the IVE SSL VPN System is logged; Administrator Changes, License Changes, and Administrator Logins.
- The following User Access to the IVE SSL VPN System is logged; Login/Logout, Java Proxy, User Settings, Secure Terminal, Network Connect, Web Requests, File Requests, Meeting, Email Requests
- The following Events on the IVE SSL VPN System are logged; Connection Requests, System Status, Rewrite, System Errors, Email Proxy Events, Statistics, Reverse Proxy, Meeting Events. The following option is available but not currently included in the IVE SSL VPN System logging – Performance
- Logs files are rotated and overwritten upon reaching designated maximum log size. However before being overwritten they are moved to a central log repository for long-term retention and back up.

## Item Number 12: Encryption – Secure Sockets Layer (SSL) Reference:

Larsen, Rich. "An Overview of the SSL Protocol and Application to Virtual Private Networks", 29 September 2003, URL: http://www.giac.org/practical/GSEC/Rich Larsen GSEC.pdf (March 2004).

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 38 of 60

**Risk:** If session is not encrypted a man in the middle could capture and read the data being accessed. Weak encryption algorithms and their implementation could lead to compromise, loss, or alteration of data. **Testing Procedure** 1. Login to IVE SSL VPN System as administrator 2. Under Central Manager > System > Configuration 3. Select the Security Tab > Security Options 4. Verify that only SSL V3 and TLS are permitted 5. Verify that encryption strength must be 128-bit or greater Compliance Criteria: Encryption Strength is 128-bit or stronger, complying with corporate policy. Browser accessing IVE SSL VPN System must utilize SSL V3. Test Nature: Objective The purpose of this audit item is to ensure that not only is the session encrypted preventing unauthorized access to the data while in transport but the encryption strength is in compliance with the corporate policy of 128-bit or greater. Evidence: Verify that only SSL V3 and TLS are permitted 5) Verify that encryption strength must be 128-bit or greater File Edit View Favorites Tools Held 🕁 Back 🔹 🔿 🗸 🙆 🖓 🖓 Search 📾 Favorites 🍏 🖏 🚽 🎒 🖉 🗸 🗐 a-admin/secunity/secunity.cgi Kassearch Web + 40 AP 🔂 TakutoFill 🕒 Republic 🛐 + 🌶 ▼ 🖓 Go Links <sup>20</sup> Central Manager Help | Sign Out 📥 System Configuration D Status D Configuration Licensing Security Certificates Network Clustering Log/Monitoring Signing In Administrators Allowed SSL and TLS Version The older SSL V2 protocol has V2. The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. Older browsers may only support SSL Delegation Accept only SSL V3 and TLS (maximize security) Users C Accept SSL V2 and V3 and TLS (maximize browser compatibility) Authentication Roles Allowed Encryption Strength Stronger ciphers improve the security of SSL encryption. Some browsers may only support 40-bit ciphers. New User **Resource Policies** C Accept only 168-bit and greater (maximize security) D Web D Files @ Accept only 128-bit and greater (security and browser compatibility) C Accept 40-bit and greater (maximize browser compatibility) D SAM SAM
 Teinet/SSH
 Network Connect
 Browsing to SSL Sites
 Neetings
 This appliance supports browsing to SSL protected Web sites, but the site certificate will not be validated. If you have concerns about the validity of the site certificate, disable this capability. Maintenance C Disable browsing to SSL sites (maximize security) Import/Export 📄 🔒 🌍 Internet Findings: Encryption Strength is set to 128-bits or greater.

Only Browsers utilizing SSL V3 and TLS are permitted to access the system.

## Item Number 13: Valid SSL certificate

#### **Reference:**

Larsen, Rich. "An Overview of the SSL Protocol and Application to Virtual

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 39 of 60 Private Networks", 29 September 2003, URL: http://www.giac.org/practical/GSEC/Rich\_Larsen\_GSEC.pdf (March 2004).

Risk: Unauthorized access to the system.

#### **Testing Procedure**

- 1. Type in URL of IVE SSL VPN System into the browser address bar
- 2. A Security Alert will be displayed
- 3. Verify that the information presented in the Security Alert is appropriate
- 4. Click on Examine Certificate
- 5. Verify the certificate general information and details.

**Compliance Criteria:** The certificate is a valid certificate from a trusted CA (Certificate Authority) and utilizes corporate approved encryption.

#### Test Nature: Objective

The purpose of this audit item is to ensure that a user is accessing the appropriate system. The SSL certificate verifies that the system that is being accessed is owned/operated by the party that user believes it to be. For example a man in the middle type of attack could occur when a user attempts to access the system but instead accesses a malicious system, via a redirect from the malicious system. This malicious system could then capture the logon credentials and use them to perform a valid logon to the system, resulting in an unauthorized person access the system via a valid logon.

#### Evidence:

3) Verify that the information presented in the Security Alert is appropriate

	Unable to verify the identity of us a trusted site.
$+ \lambda$	Possible reasons for this error:
	- Your browser does not recognize the Certificate Authority that issued the site's certificate.
	- The site's certificate is incomplete due to a server misconfiguration.
	<ul> <li>You are connected to a site pretending to be considered to be possibly to obtain your confidential information.</li> </ul>
	Please notify the site's webmaster about this problem.
	Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site
	O Accept this certificate permanently
	<ul> <li>Accept this certificate temporarily for this session</li> </ul>
	igodot Do not accept this certificate and do not connect to this Web site
	OK Cancel <u>H</u> elp

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 40 of 60

Issued To Common Name (CN) Organization (O) Organizational Unit (OI Serial Number Issued By Common Name (CN) Organization (O) Organizational Unit (OI	2A:B4:1D	i antes
Validity Issued On Expires On	10/15/2003 4/6/2009	
Fingerprints SHA1 Fingerprint MD5 Fingerprint	D9:EF:31 2E:51:29	

- The certificate date is valid.
- An appropriate encryption algorithm is being utilized SHA1

## Item Number 14: Control of corporate data – Host Checker

#### **Reference:**

Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003.

#### **Risk:** Inappropriate disclosure or unauthorized access to corporate data

## **Testing Procedure**

Test A: Host Checker Implementation and Configuration

- 1. Login to IVE system as administrator
- 2. Under Central Manager > System > Configuration > Security
- 3. Select the Host Checker Tab
- 4. View the Host Checker Policies

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 41 of 60

	ost Checker Policy - Microsoft Internet Explorer	<u> </u>
<u>File E</u> dit <u>V</u> iew F <u>a</u> vi		
⇔ Back ▼ ⇒ ▼ (⊠)	👌 🐴 🧑 Search 📷 Favorites 🥳 🗟 🕶 🎒 🗹 🖉	
Address 🕘 https	ana-admin/auth/hcpolicy.cgi?action=list	▼ 🖉 Go Links ≫
Google -	🔽 👸 Search Web 👻 🦛 🤐 🧊 🗄 AutoFil 🧕 🔩 Options 💼	) • <i>D</i>
centranmanay		
System	Configuration	
D Status	Configuration	
Configuration	Licensing Security Certificates	
D Network		
D Clustering	Security Options   Host Checker   Cache Cleaner	
<ul> <li>Log/Monitoring</li> <li>Signing In</li> </ul>		
Administrators	Perform check every: 1 minutes Save Changes	
	Perform check every: 1 minutes Save Changes	
<ul> <li>Authentication</li> <li>Delegation</li> </ul>		
Users	New Delete	
D Authentication	D Hast Charles Deliau	
D Roles	Host Checker Policy	
ē)		🔒 🎯 Internet 🅢
the fo regis 6. Upor corpo 7. Then Test B: Ver Corporate a 1. Logir 2. Acce 3. Oper 4. Oper 5. Atter	porate asset, this can occur through verific ollowing: a custom DDL, a specific file, a c try setting. In obtaining the Host Checker Policy Verific orate asset to determine if these items exist a examine a non-corporate asset to determ rification of privileges when accessing IVE asset in to IVE System from a Corporate Asset ass the email system in an email message containing an attachm in the attachment in the attachment to the local y that the attachment was able to be dowr	certain process, or a cation items examine a st. nine if these items exist. System through nent al machine.
Corporate a 1. Logir 2. Acce 3. Oper 4. Oper 5. Atter	rification of Privileges when accessing IVE asset. In to IVE System from a non-Corporate Ass ass the email system In an email message containing an attachn in the attachment npt to download the attachment to the loca y that the attachment was NOT able to be	set nent al machine.
hat can be privileges o o download <b>Test Nature</b>	e Criteria: A unique identifier will exist or verified by the Host Checker before allow n the system, such as downloading attach d attachments to non-Corporate assets. e: Objective	ing a user certain ments. Users are not abl
he purpos	e of this audit item is to ensure that adequ	ate controls are in place.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 42 of 60 prevent inappropriate disclosure of corporate data. If a user is able to download email attachments then corporate data may end up on non-corporate assets, resulting in inappropriate disclosure and unauthorized access to corporate data. If a user is accessing the IVE SSL VPN System on a Corporate owned asset the user will have the ability to download attachments to that asset. However if the user is access the IVE SSL VPN System on a public or shared asset, noncorporate then they will not be able to download attachments.

#### Evidence:

Test A: Host Checker Implementation and Configuration 4) View the Host Checker Policies

🏄 Central Manager - H	lost Checker Policy - Microsoft Internet Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	rorites Iools Help
🕁 Back 🔹 🤿 👻 🙆	🕅 🔏 🔯 Search 📷 Favorites 🧭 🖏 - 🎒 🗹 - 🗐
Address 🎒 https:	/dana-admin/auth/hcpolicy.cgi?action=list 🗹 🖉 Go Lini
Google -	💌 💏 Search Web 👻 🦡 🥪 🤯 🔚 AutoFill 🕒 🛃 Options 🛅 🔹 🥒
Certir ar Manay	CI Help   sign Out
System	Configuration
D Status	
Configuration	Licensing Security Certificates
D Network	Security Options Host Checker Cache Cleaner
D Clustering	Security Options Host Checker Caule Cleaner
D Log/Monitoring	
D Signing In	
Administrators	Perform check every: 1 minutes Save Changes
D Authentication	
D Delegation	New Delete
Users	
D Authentication	🖾 Host Checker Policy
D Roles	
<u>ē</u>	🕒 🙆 🔮 Internet

5) Verify that a Host Checker Policy exists that will determine if the asset is a corporate asset, this can occur through verification of one or more of the following: a custom DDL, a specific file, a certain process, or a registry setting.

A Host Checker Policy Exists that will check for a specific registry setting, that exists on Corporate assets.

Test B: Verification of privileges when accessing IVE System through Corporate asset

6) Verify that the attachment could be downloaded.

IVE SSL VPN System was accessed from a corporate asset on a public network; an email attachment was successfully downloaded to the corporate asset.

Test C: Verification of Privileges when accessing IVE System through a non-Corporate asset.

6) Verify that the attachment could NOT be downloaded.

Access to the IVE SSL VPN System was attempted from a non-corporate asset on a public network. Access to the IVE SSL VPN System was denied; web page appeared stating, "You do not have permission to authenticate to the system. Please contract your administrator for more information."

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 43 of 60



- Host Checker Policy exists to determine if a system is a corporate asset.
- Host Checker is configured to permit a user to download attachments, when accessing the IVE SSL VPN from a corporate asset.
- Unable to access IVE SSL VPN from a non-corporate asset.

# Item Number 15: Protection against viruses, worms, Trojans, etc.

#### **Reference:**

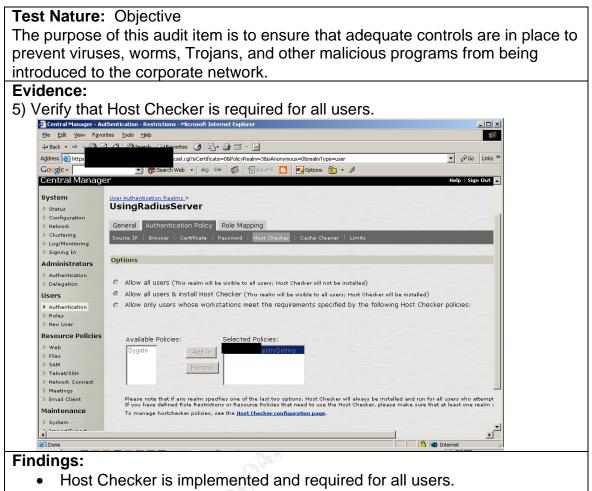
Henderickson, Dana. "Are SSL VPNs Secure and Flexible Enough?." March 2003. URL: <u>http://www.breakawaymg.com/readingroom/bmg\_sslvpn1.pdf</u> (March 2004).

**Risk:** Point of entry into the corporate network for viruses, worms, Trojans, etc, which may result in data loss or alteration, improper disclosure of corporate information including privacy data, denial of Service attack, loss of productivity as well as other damage.

#### **Testing Procedure**

- 1. Login to IVE system as administrator
- 2. Select Users > Authentication
- 3. Click on the Authentication Policy Tab
- 4. Click on Host Checker
- 5. Verify that Host Checker is required for all users.

**Compliance Criteria:** Host Checker is implemented and functioning properly. Policies exist to only allow hosts that have the required anti-virus program and/or firewall.



Host Checker is configured to determine if the system being utilized for access has a specific anti-virus program and a host-based firewall active and up to date.

## **Risk Assessment**

## **Executive Summary**

The IVE SSL VPN System succeeds in providing the corporation with secure remote access to email. The IVE SSL VPN System is a "zero footprint" solution; zero remnants remain on the system being utilized for access. It can be accessed from any computer with Internet access via a web browser. Strong two-factor authentication as well as logging of all activity enables the corporation to be in compliance with applicable laws and regulations for this solution.

The audit/ risk assessment of this system has identified the following areas of compliance with corporate policy, as well as applicable laws and regulations:

Zero Footprints

- Secure Application Manger is implemented and functioning properly
- Cache Cleaner is implemented and functioning properly
- Cookies are removed from the system

Access Controls

- Re-authentication required after timeout
- Warning banner

Logging

 Admin access, user access, and many events logged providing for a full audit trail

Data secure during transport

• 128-bit SSL Encryption

Control of Corporate Data

Host Checker Implemented

Protection against virus, worms, Trojans, and other malware

• Host Checker Implemented, restricting access to machines with up to date anti-virus and host-based firewall

Enhancements to the system should be made before the system is moved to production in the following areas to ensure compliance with applicable laws and regulations.

Data secure during transport

 SSL Certificate is issued by corporation not widely trusted Certificate Authority. This may lead to some confusion and hesitation from users since they will be presented with a security alert when accessing the system asking them if they want to proceed.

Control of Corporate Data

 Host Checker Implemented however it is not functioning properly. Users obtaining access to the IVE SSL VPN system from a corporate asset should be allowed to view and download attachments. Users obtaining access to the IVE SSL VPN system from a public machine or noncorporate asset should only be permitted to view attachments, downloading is not permitted.

The cost of these enhancements is minimal. Configuration changes and user education can accomplish both of these enhancements. No additional systems are required for these enhancements.

Recommendation: The IVE SSL VPN should be implemented as the corporation's solution for secure remote access to email. This solution provides additional functionalities, which will increase the Return On Investment (ROI), by reducing the utilization of more costly remote access solutions. A through risk assessment of these functionalities must be completed before they are implemented.

## Audit Findings

The following threats have the potential to impact the IVE SSL VPN System. The audit items listed below were performed to determine if the risk has been appropriately mitigated or reduced for each threat.

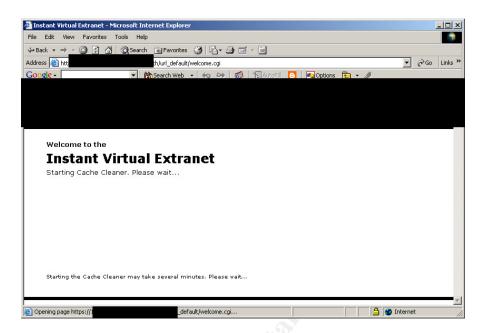
#### Threat One: Corporate Data residing on non-corporate assets

Zero Footprints are to be left on the system being utilized for access; no remnants of the data viewed, applications accessed, or systems accessed are to remain on the system.

- Secure Application Manger is implemented and functioning properly
  - Audit Item Number 2: Secure Application Manager
     Test A: Secure Application Manager Functioning Properly
     Secure Application Manager is launched upon logging in to the system;
     a temporary file is then installed on the machine being used for access,
     which is removed upon logging out. The Secure Application Session
     Manager small window must remain open and active during the
     session; warning exists notifying the user to "DO NOT CLOSE".



- Cache Cleaner is implemented and functioning properly
  - Audit Item Number 3: Cache Cleaner
    - Test A: Cache Cleaner Functioning Properly Upon accessing the system, even before a user logs in the cache cleaner is started. Upon logging out of the system the cache cleaner is executed and then stopped.



The c:\temp folders as well as the list of recent documents were examined to reveal that no documents viewed during the IVE SSL VPN session remained on the system after a user logged out.

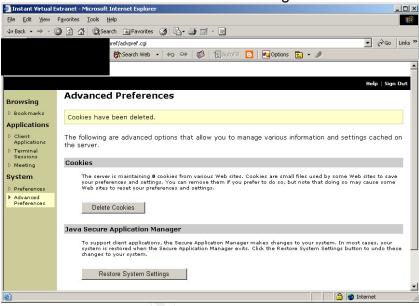
Test B: The Cache Cleaner is implemented and configured to perform a status update every 5 minutes and perform the cache cleaner function every 20 minutes. This is in compliance with the corporate information security policy related to temporary retention of data.

he Cleaner Settings - Microsoft Internet Explorer	
tes Iools Help	1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -
Search 🗑 Favorites 🧭 🛃 - 🍠 🗹 - 🗐	
ana-admin/auth/ccsettings.cgi	▼ 🖓 Go Links ×
👻 🎊 Search Web 👻 🏟 🕬 🤯 🔚 AutoFill 🕒 🔽 Options 🛐 👻 🥒	
	Help   Sign Out 🔺
Configuration	
Licensing Security Certificates	
Security Options   Host Checker   Cache Cleaner	
Cleaner Frequency : 20 minutes min=1, max=60	
Status Undate Frequency: 5 minutes minutes	
Status opdate rrequercy, p	
Curr Observer	
Dave Changes	
	·
	ana-admin(auth(costings.cgi ) (b)Search Web + 49 (b) (c)AutoFil (c) (c)Options (c) + // (c)Onfiguration Licensing Security Certificates Security Options   Host Checker   Cache Cleaner

- Cookies are removed from the system
  - Audit Item Number 5: Removal of Cookies

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 48 of 60 Test A: Removal of Cookies through IVE System

The number of cookies that are being stored on the system can be obtained by accessing System> Advanced Preferences > Cookies. An option also exists on this page to remove stored cookies; a user can do this by clicking on the "delete cookies" button. Upon executing "delete cookies" the system will state that cookies have been deleted and zero cookies are being maintained.



Test B: Cookies removed from browser settings

A review of the browser settings/configuration was performed to ensure that all cookies were removed that relate to the IVE SSL VPN System or the corporation. The review determined that all cookies had been removed upon user log out.

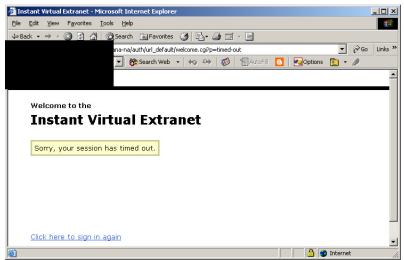
The threat of corporate data residing on corporate assets has been mitigated by the controls implemented above. These controls work together to ensure that zero footprints remain on the system being utilized to access the IVE SSL VPN System.

#### Threat Two: Unauthorized access

Access Controls are deployed to prevent unauthorized access to the system while allowing authorized access to the system.

- Re-authentication required after timeout
  - Audit Item Number 7: Re-authentication required after timeout Session time is set to 15 minutes. If a user session is idle for more than 15 minutes the user is informed that their session has timed out and that they can log in again if they choose. Logging in again requires the user to supply their credentials and to re-authenticate to the IVE SSL VPN System.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 49 of 60



- · Prevention of unauthorized access via a shared browser
  - Audit Item Number 2: Secure Application Manager
     Test B: Secure Application Manager Configuration
     Secure Application Manager has been configured to enable Basic
     Authentication Intermediation maximizing security for this feature. This
     prevents an unauthorized user from clicking the Back button on the
     browser and accessing the authorized user's session.

🏄 Central Manager - Se	ecurity Options - Microsoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vo	orites <u>T</u> ools <u>H</u> elp	-
🗢 Back 🔹 🤿 🖉 [	한 🚰 😡 Search 📷 Favorites 🧭 🖏 - 🎒 🗹 - 🗐	
Address 🙆 https:	ia-admin/security/security.cgi 🔽 🔗 Go	Links »
Google -	🔄 💏 Search Web 🔹 🏟 🍛 🚿 📲 AutoFill 🕒 🚾 Options 💼 🔹 🥒	
▷ Troubleshooting	Basic authentication intermediation Browsers cache basic authentication credentials, possibly allowing users to access resources through a shared browser using another user's credentials. The IVE can intermediate basic authentication to prevent this.	
	Enable intermediation (maximize security) Enable intermediation AND single sign-in for intranet sites (security and convenience)	
	C Disable intermediation (standard browser behavior, not recommended)	Ŧ
ê	🕒 🍙 🔮 Internet	
Con 1		

- Warning Banner
  - Audit Item Number 4: Warning Banner
  - Upon logging into the system, before or after a user enters their credentials a warning banner is not presented informing the user that they are accessing a corporate system.

In order to mitigate the threat of unauthorized access to the system security controls must be implemented. The above controls prevent an unauthorized user from being able to access the system through the use of an authorized user's session. A User's session will automatically timeout, if a user neglects to logout when they are finished. In order to provide legal ramifications of unauthorized access a warning banner must be presented.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 50 of 60

## Threat Three: Virus, worms, Trojans, and other malware being introduced to the corporate network

Protection against virus, worms, Trojans, and other malware is necessary in this world of interconnected systems. Virus, worm, Trojans and other malware have wreaked havoc when introduced to a corporate network.

- Host Checker Implemented, restricting access to machines with up to date anti-virus and host-based firewall
  - Audit Item Number 15: Protection against viruses, worms, Trojans, etc.

Host Checker is implemented and required for all users. The host checker is configured to determine if the system being utilized for access has an anti-virus program and a host-based firewall active and up to date.

🚈 Central Manager - Aut	hentication - Restrictions - Microsoft Internet Explorer
<u>Eile E</u> dit ⊻iew F <u>a</u> vori	tes Iools Help
(= Back	Al A Search CitEsyorites 🎯 🖏 - 🌆 🗹 - 🗐
Address 🕘 https	csel.cgi7isCertificate=0&PolicyRealm=3&isAnonymous=0&realmType=user 🔍 🗸 🔗 Go Links »
Google -	▼ 🐻 Search Web - +9 ↔ 🚳 📲 AutoFil 🕒 💀 Options 💼 - 🥢
Central Manage	
System	User Authentication Realms >
D Status	UsingRadiusServer
D Configuration	
D Network	General Authentication Policy Role Mapping
D Clustering	Source IP   Browser   Certificate   Password   Host Checker   Cache Cleaner   Limits
D Log/Monitoring	
D Signing In	Options
Administrators	options
D Authentication	
D Delegation	Allow all USERS (This realm will be visible to all users; Host Checker will not be installed)
Users	Illow all users & install Host Checker (This realm will be visible to all users; Host Checker will be installed)
Authentication	Allow only users whose workstations meet the requirements specified by the following Host Checker policies:
D Roles	
D New User	
<b>Resource Policies</b>	Available Policies: Selected Policies:
D Web	
D Files	Sygate Add -> gistrySetting
D SAM	Remove
D Telnet/SSH	IXEIIIUVE
D Network Connect	
D Meetings	
D Email Client	Please note that if any realm specifies one of the last two options, Host Checker will always be installed and run for all users who attempt If you have defined Role Restrictions or Resource Policies that need to use the Host Checker, please make sure that at least one realm :
Maintenance	To manage hostchecker policies, see the <u>Host Checker configuration page</u> .
D System	
· · · · · · · · · · · · · · · · · · ·	
<li>Done</li>	A w Internet

In order to mitigate the threat of virus, worms, Trojans, and other malware being introduced to the corporate network, host checker must be appropriately configured and implemented. Host Checker is currently implemented; to determine if a specific active, up to date anti-virus and host based firewall exists.

# Threat Four: Non-compliance with corporate policy applicable laws and regulations

Logging of activity is necessary to demonstrate that adequate controls structures are in place regarding the access of data.

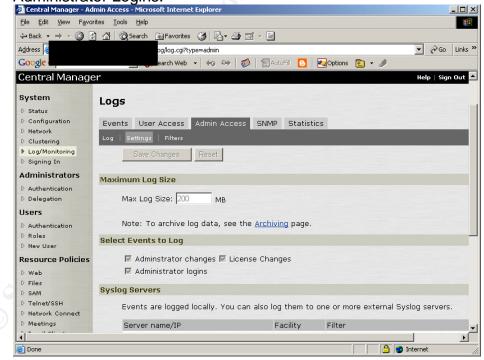
- Admin access, user access, and many events logged providing for a full audit trail
  - Audit Item Number 10: Audit Trail for all transactions Test A: A review of the administrator logs were performed to ensure that when an administrator logs in that this activity is recorded. Administrator access logs contained the following

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 51 of 60 details; time and date of access, IP of system utilized for access, Administrator ID, Administrator Realm, Authentication server. A review of the user logs were also performed to ensure that when a user logs in that this activity is recorded. User access logs contained the following details; time and date of access, IP of system utilized for access, User ID, Authentication server. Note: Logs were not included in this report due to the amount of data that would need to be removed to prevent disclosure of corporate information.

Test B: Log Setting Verification

The log settings were also reviewed to ensure that the items selected to be logged are in compliance with corporate policy as well applicable laws and regulations.

The following Administrator Access to the IVE SSL VPN System is logged; Administrator Changes, License Changes, and Administrator Logins.



The following User Access to the IVE SSL VPN System is logged; Login/Logout, Java Proxy, User Settings, Secure Terminal, Network Connect, Web Requests, File Requests, Meeting, Email Requests

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 52 of 60

🚰 Central Manager - Us	ser Access - Microsoft Internet Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vor	vrites Tools Help
🗢 Back 🔹 🔿 🖌 🙆 🧕	2 🚮 🔞 Search 🗃 Favorites 🧭 🛃 - 🎒 🗹 - 🗐
Ad	min/log/log.cgi?type=access
Google -	🔽 💏 Search Web 👻 🦡 🧀 🐔 🔀 Autorial 🕒 🛃 Options 🔂 🗸 🥒
Central Manage	Cr Help   Sign Out 📥
System	
D Status	Logs
D Configuration	Events User Access Admin Access SNMP Statistics
D Network	
D Clustering	Log Settings Filters
Log/Monitoring D Signing In	Save Changes Reset
Administrators	
	Maximum Log Size
<ul> <li>Authentication</li> <li>Delegation</li> </ul>	Max Log Size: 200 MB
Users	Man Log oldor (Loo
D Authentication	Note: To archive log data, see the <u>Archiving</u> page.
D Roles	Select Events to Log
D New User	Select Events to Log
<b>Resource Policies</b>	🔽 Login/logout 🛛 🔽 Web Requests
D Web	🔽 Java Proxy 🕅 File Requests
D Files	🔽 User Settings 🛛 Meeting
D SAM D Telnet/SSH	🔽 Secure Terminal 🔽 Email Requests
D Network Connect	Vetwork Connect
D Meetings	Syslog Servers
D Email Client	
Maintenance	Events are logged locally. You can also log them to one or more external Syslog servers.
D System	Server name/IP Facility Filter
1	
e	📃 🔂 😰 Internet

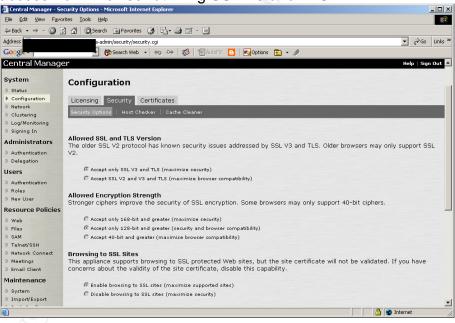
The following Events on the IVE SSL VPN System are logged; Connection Requests, System Status, Rewrite, System Errors, Email Proxy Events, Statistics, Reverse Proxy, Meeting Events. The following option is available but not currently included in the IVE SSL VPN System logging – Performance

<u>File Edit View Favori</u>	ites Tools Help
😓 Back 🔹 🔿 👻 🔯	) 🔏 🔞 Search 📾 Favorites 👹 🔩 - 🎿 🗹 - 🗎
Addres:	bg/log.cgi?type=events ▼ ∂Go
Google -	▼ 🍪 Search Web ▼ 🐗 🌳 🚳 📳 AutoFill 🕒 🛃 Options 💼 ▼ 🥖
Central Manage	}* Help   Sign
System	Logs
D Configuration	Events User Access Admin Access SNMP Statistics
D Network	
D Clustering	Log Settings Filters
Log/Monitoring	Save Changes Reset
D Signing In	
Administrators	Maximum Log Size
D Authentication	
D Delegation	Max Log Size: 200 MB
Users	
D Authentication	Note: To archive log data, see the <u>Archiving</u> page.
D Roles	Select Events to Log
D New User	allect Events to Log
<b>Resource Policies</b>	🔽 Connection Requests 🖾 Statistics
D Web	🔽 System Status 🔲 Performance
D Files	Reverse Proxy
D SAM	🔽 System Errors 🛛 🔽 Meeting Events
D Telnet/SSH	F Email Proxy Events
D Network Connect	Ender Hoxy Evenes
<ul> <li>D Meetings</li> <li>D Email Client</li> </ul>	Syslog Servers
Maintenance	Events are logged locally. You can also log them to one or more external Syslog servers.
D System	Server name/IP Facility Filter
D. Import/Export	

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 53 of 60 Logs files are rotated and overwritten upon reaching designated maximum log size. However before being overwritten they are moved to a central log repository for long-term retention and back up.

Data security during transport is essential for control of corporate information and financial data regarding compliance with applicable laws and regulations.

- 128-bit SSL Encryption is required by corporate policy.
  - Audit Item Number 12: Encryption Secure Sockets Layer (SSL) Corporate policy requires that a minimum of 128-bit encryption be utilized when data is being transported outside the corporation. The IVE SSL VPN System is configured to only accept 128-bit or higher encryption strength. It is also configured to only accept access from Browser utilizing SSL V3 and TLS.



- Valid SSL Certificate
  - Audit Item Number 13: Valid SSL Certificate
    - The corporation has issued the SSL certificate presented to the users upon accessing the IVE SSLVPN. This causes a security alert to be presented to the user stating that the certificate authority is not a trusted source, or there is a server misconfiguration, or that the user is connecting to a site that is pretending to be the IVE SSL VPN System. The certificate does have a valid date and utilizes the SHA1 encryption algorithm, which is on the list of approved algorithms dictated by the information security department.

		· · · · · · · · · · · · · · · · · · ·
Issued To Common Name (CN) Organization (O) Organizational Unit (C Serial Number	U) 2A;B4:1D	
<b>Issued By</b> Common Name (CN) Organization (O) Organizational Unit (C	U)	
Validity		
Issued On Expires On	10/15/2003 4/6/2009	
Fingerprints		
SHA1 Fingerprint MD5 Fingerprint	D9:EF:31 2E:51:29	

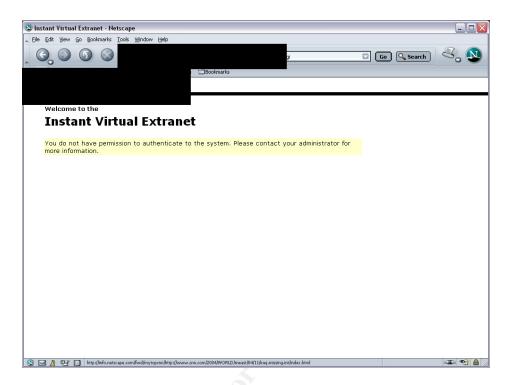
#### Control of Corporate Data

- Host Checker Implemented
  - Audit Item Number 14: Control of Corporate Data Host Checker Test A: Host Checker Implementation and Configuration Host Checker policies exist that will determine if the machine being utilized for access is a corporate asset. This determination is currently being made by the existence of a specific registry setting. Test B: Verification of privileges when accessing the IVE SSL VPN System through a corporate asset.

The IVE SSL VPN System was accessed from a corporate asset on a public network; an email attachment was successfully downloaded to the corporate asset.

Test C: Verification of privileges when accessing the IVE SSL VPN System through a non-corporate asset

Access to the IVE SSL VPN System was attempted from a noncorporate asset on a public network. Access to the IVE SSL VPN System was denied, so this test could not be completed.



In order for a corporation to be in compliance with its own corporate policy as well as applicable laws and regulations they must have appropriate controls in place to ensure the confidentiality, integrity, and security of financial data, financial reports, customer information, employee information, as well as other types of data. Logging of all transactions provides a full audit trail of access to the corporation's data. This audit trail can be utilized for forensic investigations as well as be monitored for on-going compliance of the system. Corporate data must also be secured during transport preventing unauthorized persons from being able to obtain the corporation's data. The use of 128-bit encryption provides this capability. The SSL Certificate provides the user with the assurance that the system that they are accessing is really the system that they want to access. The host checker upon proper configuration will provide for the control of the location of corporate data. The audits of the above controls, which are implemented, provide the corporation with the appropriate controls necessary to be in compliance with corporate policy and applicable laws and regulations.

## **Audit Recommendations**

 SSL Certificate is issued by corporation not a widely trusted Certificate Authority that is on most browser's approved lists. This may lead to some confusion and hesitation from users since they will be presented with a security alert when accessing the system asking them if they want to proceed. Before this system moves to production this confusion should be eliminated. A few possible ways to eliminate this confusion is to purchase a SSL Certificate form a widely trusted Certificate Authority, user education and associated documentation.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 56 of 60

- 2. Host Checker Implemented however it is not functioning properly. Users obtaining access to the IVE SSL VPN system from a corporate asset should be allowed to view and download attachments. Users obtaining access to the IVE SSL VPN system from a public machine or noncorporate asset should only be permitted to view attachments, downloading of attachments is not permitted.
- 3. In order to mitigate the threat of virus, worms, Trojans, and other malware being introduced to the corporate network, host checker must be appropriately configured and implemented. Host Checker is currently implemented; to determine if a specific active, up to date anti-virus and host based firewall exists. However a user accessing the system may be utilizing a machine with a different brand of anti-virus or host-based firewall. The host checker policies will need to be expanded to include other popular anti-virus and host-based firewall programs in order to provide users with access to the IVE SSL VPN System from public or noncorporate assets.
- 4. A warning banner should be presented upon logging into the system, stating that the user is accessing a corporate asset. Currently upon loggin into the system a banner is not presented. The banner will aid the corporation when pursuing legal action for unauthorized access to the system.

The POC (Proof of Concept) has been successful in demonstrating that the IVE SSL VPN System can be implemented as a corporate solution for secure remote access to corporate email. However before moving forward and installing this system in production further configuration changes and their associated testing will need to occur. This system also offers additional functionalities, which should undergo the proper assessment and testing before implementing these functionalities. Once the system is put into production it should be added to risk management's list of systems that require regular reviews, to ensure that the security of the system is maintained.

## Cost

A SSL Certificate from a trusted and well-known Certificate Authority may be purchased. This will prevent confusion for the users who receive security alerts when attempting to access the IVE SSL VPN System.

Implementation of the remainder of the audit recommendations only requires configuration changes and the associated testing, man-hours to perform the tasks. User documentation and education will also need to be completed, resulting in additional man-hours. No additional hardware, software, or systems will need to be purchased.

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 57 of 60 © SANS Institute 2004.

## **Compensating Controls**

## Policy

The corporate remote access policy must be reviewed in order to ensure that issues created by the use of the IVE SSL VPN System have been properly addressed.

#### User Documentation

The following documentation should be developed and distributed to the user community upon deployment of this system.

- Instructions how to use the system including functionalities and features
- Guidelines for when to use this system
- FAQ Frequently Asked Questions
- User Accountability Statement user understands and acknowledges the granting of privileges to utilize this system

The purpose of this documentation is to define appropriate use, increase ease of use, and increase acceptance of this solution.

#### Hardware and Software

Additional add-ons, compensating controls, or systems are not recommended at this time for secure remote access to corporate email. If additional functionalities are implemented an audit/risk assessment will be performed in order to determine if additional compensating controls are necessary.

## Conclusion

The IVE SSL VPN should be implemented as the corporation's solution for secure remote access to email. The above audit recommendations should be considered when implementing the system. This solution provides additional functionalities, which will increase the Return On Investment (ROI), by reducing the utilization of more costly remote access solutions. A through risk assessment of these functionalities must be completed before they are implemented.

## **Works Consulted**

Carlsson, Marcel M. B. "Technical security audit of a customer support web application portal: the independent auditor perspective", 24 November 2003 URL: <u>http://www.giac.org/practical/GSNA/Marcel\_Carlsson\_GSNA.pdf</u> (February 2004).

"The CISSP Open Study Guide Web Site, Terms and Definitions." URL: <u>http://www.cccure.org/Documents/HISM/229-230.html</u> (March 2004).

Conry-Murray, Andrew. "SSL VPNs: Remote Access for the Masses", Network Magazine. October 2003. URL:

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=1520 1419&classroom= (January 2004).

Cryptography Research, Inc. "Neoteris System Evaluation." 16 January 2002. Confidential copies can be obtained by contacting Neoteris.

Farmer, Dan. "Review of the Neoteris Instant Virtual Extranet (IVE) Appliance." January 2002. URL:

http://216.239.51.104/search?q=cache:cSchiDsBUHIJ:www.ipm.com/fileadmin/P DF/Neoteris/Farmer\_Security\_report.pdf+Dan+Farmer+January+2002+review+n eoteris&hl=en&ie=UTF-8 (March 2004).

Ferrigni, Steven. "SSL Remote Access VPNs Is this the end of IPSEC?", 22 October 2003, URL:

http://www.giac.org/practical/GSEC/Steven\_Ferrigni\_GSEC.pdf (February 2004).

Glasner, Joanna. "Cybercrime Follow Money Trail" <u>Wired News</u>. 5 March 2003. URL: <u>http://www.wired.com/news/business/0,1367,57911,00.html (March 2004)</u>.

Henderickson, Dana. "Are SSL VPNs Secure and Flexible Enough?." March 2003. URL: <u>http://www.breakawaymg.com/readingroom/bmg\_sslvpn1.pdf</u> (March 2004).

Kawamura, Cynthia. "Balancing Security and Compliance with an SSL VPN." URL:

http://216.239.51.104/search?q=cache:bmMUT7AhU64J:www.rainbow.com/Libra ry/8/Compliance%2520with%2520an%2520SSL%2520VPN.pdf+rainbow.com+c ompliance+SSL+VPN+Cynthia&hl=en&ie=UTF-8 (April 2004)

Larsen, Rich. "An Overview of the SSL Protocol and Application to Virtual Private Networks", 29 September 2003, URL: <u>http://www.giac.org/practical/GSEC/Rich\_Larsen\_GSEC.pdf</u> (March 2004).

Neoteris "Instant Virtual Extranet Design Guide." (April 2004).

----Audit of SSL VPN; Secure remote email solution for a financial institution-----Author retains all rights Page 59 of 60 Neoteris "IVE 5000 Help file." (April 2004).

Neoteris. "Securing Remote Access, whitepaper." November 2002. Confidential copies can be obtained by contacting Neoteris.

Nichols, Arthur. "A Perspective on Threats in the Risk Analysis Process." URL: http://www.sans.org/rr/papers/index.php?id=63 (March 2004).

"RSA Conference 2004 Announces Results of the 2<sup>nd</sup> Annual Internet Insecurity Index." February 2004, URL:

http://www.rsasecurity.com/company/news/releases/pr.asp?doc\_id=3389 (March 2004)

"The 7 Layers of the OSI Model" URL: http://webopedia.internet.com/quick\_ref/OSI\_Layers.asp (March 2004).

Surman, Glenn. "Understanding security using the OSI model." 20 March 2002. URL: http://www.sans.org/rr/papers/index.php?id=377 (March 2004).

Warden, Waheed. "An Intro to SSL VPN." 1 December 2003, URL: http://www.webpronews.com/it/networksystems/wpn-21-20031201AnIntrotoSSLVPN.html (March 2004).

Williams, Phil, Casey Dunlevy, and Tim Shimeall. "Intelligence Analysis for Internet Security." Cert Coordination Center, URL: http://www.cert.org/archive/html/Analysis10a.html (March 2004).

As part of GIAC practical repository.