

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.

Security Audit of a Financial Institution's Site-to-Site VPN Tunnel Connection To a 3rd Party Internet Banking Vendor: An Auditor's Perspective

GSNA Practical Assignment Version 3.1, Option 1

Prepared by: Chris Kroll
July 26, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

As smaller financial institutions try to bridge the gap between their service offerings and those of their larger competitors, they often turn to third party vendors to aid them in this endeavor. Often times the successful delivery of these services require the transmission of sensitive financial institution data to an organization outside of their "domain". With the creation of new legislation such as the Gramm-Leach-Bliley Act which mandates that sensitive member information be protected at all cost, a financial institution can ill-afford to cut corners when addressing issues dealing with the transmission of member information.

This assessment will focus on one facet of a particular third party vendor's mode of data communications between a financial institution, in this case a credit union, and themselves. For this third party vendor, site-to-site tunneling achieved through the use of two Netscreen-5XP VPN appliances have been selected for secure member information transmission. Our assessment will focus exclusively on this communications link between these two organizations to determine whether or not the appropriate security controls are in place to ensure member data privacy as well as meet associated regulatory compliance and make recommendations where appropriate.

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Research in Audit, Measurement, Practice, and Control 4
1.1 Description of the Systems 4
1.2 Evaluation of Risk 7
1.3 Current State of Practice 10
2. Create An Audit Checklist 12
2.1 Audit Checklist 12
3. Conduct the Audit Testing, Evidence and Findings 27
4. Audit Report 45
4.1 Executive Summary 45
4.2 Audit Findings and Recommendations 45
5. References 49

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Research in Audit, Measurement, Practice, and Control

1.1 Description of the Systems

Overview

AB Systems, Inc. hosts and publishes several credit union internet banking websites. These websites allow credit union members to perform various queries and transactions, such as account balance and transfer of funds, on accounts they have with the credit unions. In order to provide real-time account information to the users of these internet banking sites, AB Systems needs to maintain secure, persistent connections to the credit unions' core banking systems (the servers that processes transactions and store account information). In an effort to provide a competitive price to the credit unions, AB Systems eliminates the need for a dedicated data communication circuit by making use of the existing internet connection already in place at the credit union's facility, in conjunction with site-to-site VPN (Virtual Private Networking) technology. This alternative provides a cost effective, secure, full-time connection between AB Systems' transaction server (the server that handles all transactional request from the website) and the credit union's core banking system over the internet.

Scope Of Audit

There are many applications and systems that are required to provide the end to end internet banking solution to AB Systems' credit union customers. However, the scope of this security audit will focus exclusively on the site-to-site VPN tunnel between AB Systems and the credit union. This will include the VPN appliances at both locations (AB Systems and the credit union), the operating system running on these appliances, and the controls in place to prevent unauthorized access to these appliances.

Doug R., Director of Operations at AB Systems, informed us that after testing several VPN appliances that support site-to-site tunneling, AB Systems decided on the Netsceen-5XP. The Netscreen-5XP is an entry level security appliance that provides firewall and VPN services for a broadband telecommuter and/or a branch office[1].

[1] NetScreen-5XP Users Guide p.V

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Figure 1.1: Netscreen 5XP

According to Doug , the decision to use the Netscreen-5XP was based primarily on its ability to restrict access over the VPN tunnel based on IP address, UDP/TCP port as well as which devices can initiate communications. To Doug, this level of granularity is important as it reduces the risk of compromise by rouge systems and/or employees from either organization.

As figure 1.2 shows, the Netscreen 5XPs are running the latest version of software, ScreenOS 5 (noted as Firmware Version). Additionally, AB Systems enabled the 256 bit AES (Advanced Encryption Standard) encryption that was included with ScreenOS 5[2].

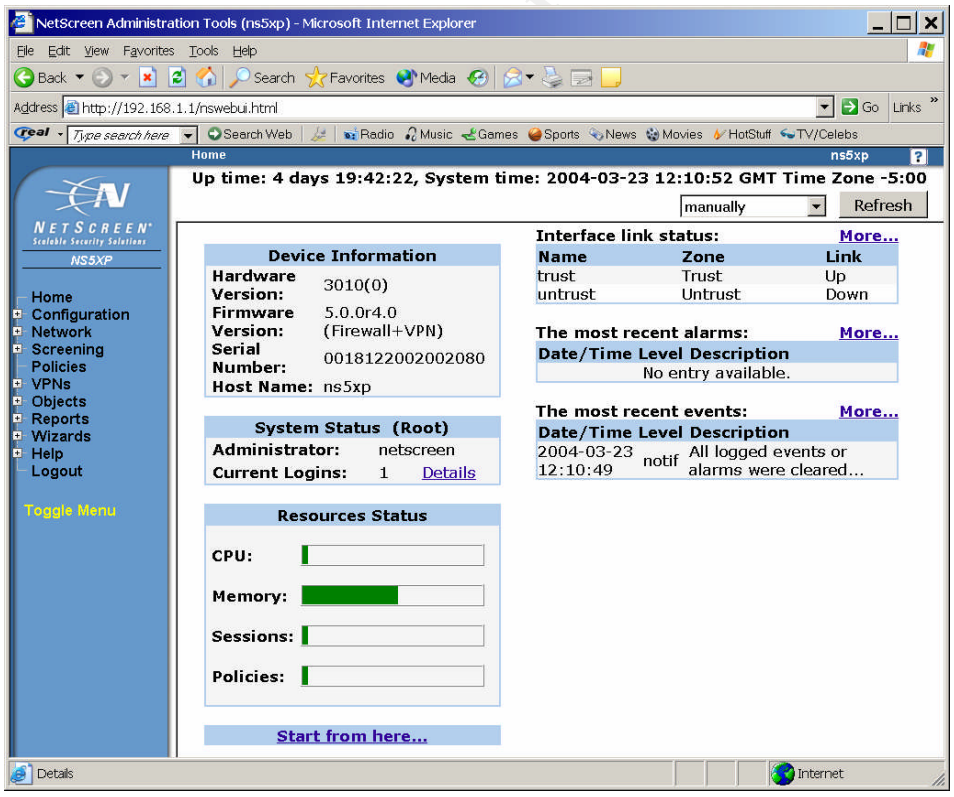


Figure 1.2: Netscreen-5XP Administrative Console

[2] NetScreen Concepts & Examples ScreenOS Reference Guide Volume5:VPNs p8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As previously mentioned, two systems use the site-to-site tunnel for communications. AB Systems' transaction server is a "home built" system running Windows 2000 Server and a custom application that performs transactions on the credit union's core banking system. The core banking system is an RS/6000 (model can vary depending on credit union size) running AIX. The credit union's data processing vendor maintains this system and restricts access from AB Systems' transaction server to TCP port 300. During this assessment, we will not be auditing either of these systems directly. However, we will test the ability of these systems to access other services/systems on the far-end network. Figure 1.2 provides an overview of the end to end connection.

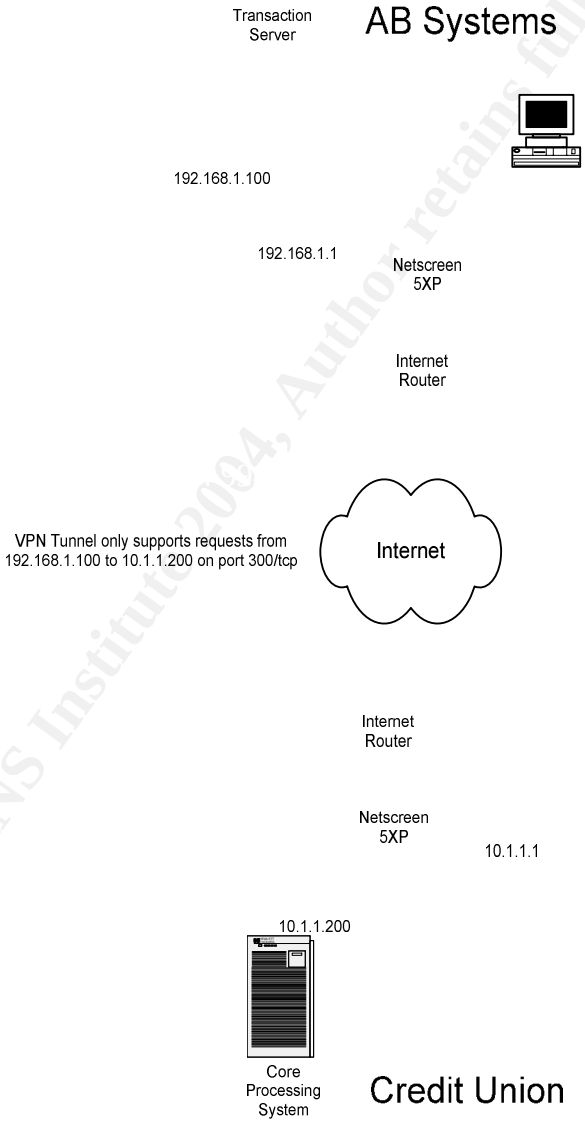


Figure 1.3: Site-to-Site VPN Overview

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In summary, our audit will report findings and make appropriate recommendations on the following items:

- Verify the effectiveness of the Netscreen-5XP configurations through the use of sophisticated scanning and sniffing software as they apply to the Threat Matrix (Table 1.1).
- Address any know vulnerabilities associated with the Netscreen-5XP OS 5.
- Review written security policies that apply to the Netscreen-5XPs and the Threat Matrix (Table 1.1)
- Review the physical access control to the Netscreen-5XPs.

1.2 Evaluation of Risk

AB Systems has taken on a huge responsibility by making sensitive member information available via the internet. With regulations and laws such as the Gramm-Leach-Bliley Act[3] and HIPPA[4] as well as hacking techniques becoming more sophisticated, it's a wonder that any business would want to take the risk of exposing an individual's personal information to the wrong person. To further complicate the matter, the site-to-site VPN tunnel that is maintained to all of AB Systems' credit union customers is essentially an extension of AB Systems' own network. However, to stay competitive in this market space and provide up to date information to the end users of this solution, certain risk need to be taken. This is why it is so important that AB Systems and the credit unions understand what these risk are and enforce strong information security practices. To be effective in this endeavor, the assets at risk, potential vulnerabilities to these assets, threats and potential damage that face these organizations need to be properly identified.

As stated previously, there are numerous systems involved in delivering the end-to-end home banking solution to the credit union customers . Below is a list of the most significant assets at risk within these organizations that fall within the scope of this audit:

Asset	Description
Netscreen-5XP VPN Appliances	These devices are the "gatekeepers" that protect AB Systems and the credit unions from each other as well as external threat sources. Compromise one of these and the potential for significant damage is almost guaranteed.

[3] http:// http://banking.senate.gov/conf/fintl5.pdf
[4] http://www.cms.hhs.gov/hipaa/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Credit Union Member information	This is the most significant asset that AB Systems is responsible for. In the financial industry, compromise of sensitive member information is a PR death sentence and could result in the closure of business for AB Systems and the credit union.

Table 1.1 Organizational Assets

To aid us in our endeavor to create an accurate threat matrix pursuant to our scope of work, we reviewed several resources. The National Institute of Standards and Technology (NIST) created a document titled *Risk Management Guide for Information Technology Systems*. This document provides a guideline to creating an effective risk management program through the use of proper threat identification and mitigation. We used the recommended nine step methodology[5] described within this document and our professional experience to create a threat matrix (Table 1.2) detailing the most significant threats facing AB Systems and the credit unions brought on by the site-to-site VPN Tunnel.

Threat ID	Threat	Potential Damage	Likelihood	Severity
1	Interception of VPN Traffic via "Sniffing" Techniques.	Compromise of sensitive member data.	Low	High
2	Denial of Service.	Downtime for Home Banking Website.	Medium	High
3	Unauthorized access to AB Systems' network by a credit union employee.	Compromise of sensitive member data from other organizations and other malicious activity.	Low	High
4	Unauthorized access to credit union network by an AB Systems employee.	Compromise of sensitive member data from and other malicious activity.	Low	High
5	Unauthorized access to credit union or AB Systems' network from the internet	Compromise of sensitive data from all associated organizations and other malicious activity	Low	High
6	Theft of VPN	Downtime for	Low	High

[5] Risk Management Guide for Information Technology Systems (NIST – SP 800-30) p8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Appliance.	Home Banking Website; Disclosure of configuration profile.		
7	Loss of event logs	Inability to perform forensics should a breach occur	Medium	High
8	Unauthorized access to VPN Appliance Configuration.	All of the above	Low	High
9	VPN Appliance OS Vulnerability Exposure.	All of the above	Medium	High

Table 1.2: Threat Matrix

With the threats described in table 1.2 and the help of NIST's *Risk Management Guide for Information Technology Systems* document, we are also able to create a list of the most significant vulnerabilities that we will need to address and the potential threats they pose.

Vulnerability	Threat
Unnecessary open TCP or UDP ports on the credit union's Netscreen-5XP to AB Systems' network.	- Unauthorized access to AB Systems' network by a credit union employee.
Unnecessary open TCP or UDP ports on the credit union's Netscreen-5XP to the internet.	- Unauthorized access to the internet network by a credit union employee.
Unnecessary open TCP or UDP ports on AB Systems' Netscreen-5XP to the credit union network.	- Unauthorized access to credit union network by an AB Systems employee.
Unnecessary open TCP or UDP ports on AB Systems' Netscreen-5XP to the internet.	- Unauthorized access to the internet network by an AB Systems employee.
Unnecessary open TCP or UDP ports on the Internet side of either Netscreen-5XP	- Unauthorized access to credit union or AB Systems' network from the internet - Unauthorized access to VPN Appliance Configuration.
Weak password settings and/or policies	- All of the above
Weak or non-existent encryption settings and/or policies	- Interception of VPN Traffic via "Sniffing" Techniques.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Weak physical access control policies	- Theft of Netscreeen-5XP VPN appliance
Weak event log settings and/or policies	-Loss of event logs
Weak or non-existent OS patch policies	-VPN Appliance OS Vulnerability Exposure.

Table 1.3 Vulnerability Matrix

1.3 Current State of Practice

VPN Technology has been around for quite a while. Because of this, there are many references publicly available that describe standards and implementations at every level. Although we could not find a specific "Best Practice" reference for AB Systems' particular implementation, we were able to draw from enough resources to piece together our own "Best Practice". These best practices are detailed in the compliance statements within each audit item.

To define a "Best Practice" for AB Systems' implementation we should first understand the history and variations of VPN Technology. The best reference we found for this information was the VPN Consortium[6]. The VPN Consortium (VPNC) is a large group of VPN Technology vendors (including Netscreen) who work together to achieve the following goals:

- Promote the products of its members to the press and to potential customers
- Increase interoperability between members by showing where the products interoperate
- Serve as the forum for the VPN manufacturers and service provider throughout the world
- Help the press and potential customers understand VPN technologies and standards
- Provide publicity and support for interoperability testing events

It should also be noted that the VPNC does not create standards; rather it supports and promotes current and developing standards set forth by The Internet Engineering Task Force (IETF)[7].

The VPNC states that there are three different types of VPNs; Trusted, Secure and Hybrid[8]. Trusted VPNs are described as one or more circuits leased from a communications provider where a single circuit acts like a single wire in the customer's network and that no one else will use that same circuit. The data is not encrypted and the customer places a high level of trust in the communications provider to maintain the integrity and privacy of those circuits.

[6] www.vpnc.org
[7] www.ietf.org
[8] http://www.vpnc.org/vpn-technologies.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

These types of VPNs were more prevalent when the Internet was still in it's infancy.

Secure VPNs are different from trusted VPNs in that they encrypt data before entering a communication provider's network (internet) and decrypt it after it leaves the provider's network. Encrypting the data before it enters the provider's network mitigates certain risk that may be present in the provider's network such a data sniffing. Even though the potential for data to be captured is still present, decrypting that data is a major task unto itself that some experts believe is nearly impossible, given a strong enough encryption algorithm[9].

Hybrid VPNs are a combination of both Trusted and Secure VPNs.

Based on the descriptions provided by the VPNC, we can determine that AB Systems' VPN implementation is that of a Secure VPN since AB Systems uses encryption and the internet (refer to figure 1.3). According to the VPNC, a Secure VPN should have the following three characteristics[10]:

- **All traffic on the secure VPN must be encrypted and authenticated.** This means that before any data can be exchanged, the two endpoints must first authenticate to one another. Once authenticated, only encrypted data can pass over the VPN.
- **The security properties of the VPN must be agreed to by all parties in the VPN.** Since both endpoints of our VPN are managed by AB Systems', this will not be an issue. However, the credit union should be educated as to the properties being used and why.
- **No one outside the VPN can effect the security properties of the VPN.** This addresses access control to the VPN appliances where an attacker could weaken the security properties that could ultimately result in downtime or a loss of sensitive data.

Although these characteristics are useful, they are too broad to direct us to specific options that should be configured on these Netscreen appliances. To further define our type of VPN and available configurable options, we referred back to Netscreen's *Concepts & Examples ScreenOS Reference Guide Volume5:VPNs.* This document is a key component for developing our audit checklist items that are specific to individual configuration options.

Some other considerations we need to take into account when building our "best practice" model are the details described in the Grahm-Leach-Bliley Act[11]. Although this document is not a guideline for configuring a VPN, it emphasizes the importance of maintaining the confidentiality of sensitive credit union member data. What we can infer from the information contained within this document is

[9] http://www.vpnc.org/vpn-technologies.html - 3. Usage scenarios for secure VPNs
[10] http://www.vpnc.org/vpn-technologies.html - 4.1 Secure VPN Requirements
[11] http://banking.senate.gov/conf/fintl5.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

that the credit union and/or credit union vendor should takes all necessary precautions available to them to ensure that sensitive member data is not compromised. For the purpose and scope of this audit, this means that AB Systems should configure the Netscreen appliance to only allow access over the VPN Tunnel to those devices and applications that require that level of access. Additionally, the VPN Tunnel should use the strongest authentication and encryption methods available on the Netscreen 25-XP.

I should also note that after many years of experience as an Information Security practitioner, personal experience plays a key component in creating the Audit Checklist.

2. Create An Audit Checklist

An audit checklist has been created to provide a blueprint to guide us through the audit process followed to assess the aforementioned risk noted in Section 1.2 of this document. Each checklist item will include the following information:

- Item Number – Used to identify the checklist item as well as cross referencing.
- Objective – States the objective/title of the checklist item.
- References – Source or sources used to aid in the creation of this checklist item.
- Vulnerability –The vulnerability being checked.
- Testing Procedure – Describes the tools and steps taken to perform this checklist item.
- Compliance Criteria – Describes the guidelines that the output of this test will be judged against.
- Objective / Subjective – Is the checklist item objective or subjective.
- Evidence – The output from the testing procedure.
- Findings – Describes the conclusion(s) derived from the information contained within the evidence.

2.1 Audit Checklist

Item 1	**Objective:** Ensure that data being transmitted between VPN devices cannot be viewed in clear text.
Reference	1. Personal Experience 2. *What is Encapsulating Security Payload (ESP)?* http://kbserver.netgear.com/kb_web_files/N101014.asp - an easy to understand definition. 3. *RFC 2406 - IP Encapsulating Security Payload (ESP)*

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	http://www.faqs.org/rfcs/rfc2406.html 4. *RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)* http://www.faqs.org/rfcs/rfc2408.html 5. Gramm-Leach Bliley Act – Title V http://banking.senate.gov/conf/fintl5.pdf
Vulnerability	Weak or non-existent encryption settings and/or policies
Procedure	1. Establish a network connection on the "Untrusted" side of either Netscreen VPN Appliance. To successfully capture packets, a "Dumb" Hub (no internal switch) will need to be placed in-between the Netscreen VPN Appliance and Internet router if one is not already present. 2. Launch Ethereal (V 0.10.11), click "Capture" on the tool bar then click "Start". This will bring up the Ethereal Capture Options window. 3. Ensure that the correct interface is selected (This is the first option). All other default options should correct. 4. Click the "O.K." button. This will bring up the Ethereal: Capture window. 5. Reboot one of the Netscreen VPN appliances. This will enable us to capture the initial hadshake between the two VPN appliances as well as the data transfer. 6. Have an AB Systems Employee Initiate a file transfer request on their transaction server. 7. Once the transfer is complete, click on the "Stop" button on Ethereal: Capture window. This will bring you back to Ethereal's main window with the captured data displayed.
Compliance	The captured data between the two Netscreen-5XP VPN appliances should only reveal three protocol types: ESP, ISAKMP and ARP. Any other protocol types discovered between these two devices would indicate that these devices are incorrectly configured.
Objective/ Subjective	Objective
Evidence	Refer to section 3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Findings	Refer to section 3

Item 2	**Objective:** Research any known vulnerabilities that apply to the Netscreen 5XP and ScreenOS 5
Reference	1. Personal experience 2. CERT Vulnerability Notes Database http://www.kb.cert.org/vuls 3. Security Focus bugtraq http://www.securityfocus.com/bid 4. Netscreen Security Notices http://www.juniper.net/support/security/alerts/
Vulnerability	Weak or non-existent OS patch policies
Procedure	1. Query the CERT Vulnerability Notes Database by connecting to *http://www.kb.cert.org/vuls* and using the keyword "Netscreen". Review all potential hits that reference the Netscreen 5XP or ScreenOS 5. 2. Query the Security Focus bugtraq site by connecting to http://www.securityfocus.com/bid. A. For Vendor, select Netscreen and click on the submit button. B. For Title, select ScreenOS and press submit. C. For Version, select 5 and press submit. 3. Connect to Juniper Network's Netscreen Security Notices by connecting http://www.juniper.net/support/security/alerts/. Review all potential hits that reference the Netscreen 5XP or ScreenOS 5.
Compliance	There should be no vulnerabilities discovered for the particular OS and configuration or a workaround should be implemented.
Objective/ Subjective	Objective
Evidence	Refer to section 3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Findings	Refer to section 3

Item 3	**Objective:** Check AB Systems Security Policy Manual for patch management policies.
Reference	1. Personal experience 2. *Windows Security Resource Kit*; Ben Smith and Brian Komar – Chapter 22 Patch Management
Vulnerability	Weak or non-existent OS patch policies
Procedure	1. Review AB Systems' Security Policy Manual for Policies, Standards and Procedures that address the following: A. Notification of available patches. B. How are patches obtained. C. Testing of new patches prior to deployment. D. What are the procedures for deployment 2. Interview System Administrator to discuss their level of awareness of these policies.
Compliance	At a minimum, the Security Policy should address how AB Systems keeps track of new patches (Notification) and the procedures for deploying them. Additionally, the System Administrator should be well educated on the policies without having to refer back to the written manual.
Objective/ Subjective	Objective – either the policies are there or they are not. Subjective – how in depth does AB Systems describe these policies and how well does the System Administrator know them.
Evidence	Refer to section 3
Findings	Refer to section 3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item 4	**Objective:** Scan for unnecessary open ports from the credit union's network towards AB Systems' network.
Reference	1. Personal experience 2. Insecure.org http://www.insecure.org/nmap/data/nmap_manpage.html 3. Foundstone.com http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm 4. Network Auditing Essentials Track 7 – Auditing Networks, Perimeters and Systems
Risk	Unnecessary open TCP or UDP ports on the credit union's Netscreen-5XP to AB Systems' network.
Procedure	1. Establish a network connection on the trusted side of the credit union's Netscreen VPN appliance with a valid IP address. 2. Launch NMAPWIN (v.1.3.1) and click on the "Discovery" tab. 3. Click the "Don't Ping" radial. 4. Click on the "Scan" tab then click on "Port Range" under "Scan Options". 5. Enter "1-65535" in the "Port Range" field. 6. In the "Hosts" field at the top of the screen, enter the target host's IP address then click on "Scan". 7. When scan is finished, the third box from the right on the bottom of the window will turn green. Remember to save this scan by copy and pasting the contents in the "Output" field. 8. Under "Mode", click on the "UDP" radial, then repeat steps 6 and 7. 9. Launch SuperScan (v.2.06). 10. Click on the "All ports from" radial and enter "1" in the left box and "65535" in the right. 11. Enter the target host's IP address in the "Start" and "Stop" Fields then click on the "Start" button. 12. When the scan is finished, the "Start" button will no longer be grayed out. Remember to save this scan by clicking the "Save" button.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compliance	Only TCP port 80 (Management) should be open on the Netscreen-5XP's "trusted" network connection. No other TCP or UDP ports should show open on the Netscreen-5XP's "trusted" network connection or AB Systems' network.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3

Item 5	**Objective**: Scan for unnecessary open ports from AB Systems' Network towards the credit union's network.
Reference	1. Personal experience 2. Insecure.org http://www.insecure.org/nmap/data/nmap_manpage.html 3. Foundstone.com http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm 4. Network Auditing Essentials Track 7 – Auditing Networks, Perimeters and Systems
Risk	Unnecessary open TCP or UDP ports on AB Systems' Netscreen-5XP to the credit union network.
Procedure	1. Establish a network connection on the trusted side of AB Systems' Netscreen VPN appliance with a valid IP address. 2. Launch NMAPWIN (v.1.3.1) and click on the "Discovery" tab. 3. Click the "Don't Ping" radial. 4. Click on the "Scan" tab then click on "Port Range" under "Scan Options". 5. Enter "1-65535" in the "Port Range" field. 6. In the "Hosts" field at the top of the screen, enter the target host's IP address then click on "Scan".

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	7. When scan is finished, the third box from the right on the bottom of the window will turn green. Remember to save this scan by copy and pasting the contents in the "Output" field. 8. Under "Mode", click on the "UDP" radial, then repeat steps 6 and 7. 9. Launch SuperScan (v.2.06). 10. Click on the "All ports from" radial and enter "1" in the left box and "65535" in the right. 11. Enter the target host's IP address in the "Start" and "Stop" Fields then click on the "Start" button. 12. When the scan is finished, the "Start" button will no longer be greyed out. Remember to save this scan by clicking the "Save" button.
Compliance	Only TCP port 80 (Management) should be open on the Netscreen-5XP's "trusted" network connection and TCP port 300 on the credit union's core banking system. No other TCP or UDP ports should show open on the Netscreen-5XP's "trusted" network connection or AB Systems' network.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3

Item 6	**Objective:** Scan for unnecessary open ports on the Netscreen VPN appliances from the internet.
Reference	1. Personal experience 2. Insecure.org http://www.insecure.org/nmap/data/nmap_manpage.html 3. Foundstone.com http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm 4. Network Auditing Essentials Track 7 – Auditing Networks,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Perimeters and Systems 5. Auditing the Perimeter Track 7 – Auditing Networks, Perimeters and Systems
Risk	Unnecessary open TCP or UDP ports on the Internet side of either Netscreen-5XP
Procedure	1. Establish a network connection to the internet. 2. Launch NMAPWIN (v.1.3.1) and click on the "Discovery" tab. 3. Click the "Don't Ping" radial. 4. Click on the "Scan" tab then click on "Port Range" under "Scan Options". 5. Enter "1-65535" in the "Port Range" field. 6. In the "Hosts" field at the top of the screen, enter the target host's IP address then click on "Scan". 7. When scan is finished, the third box from the right on the bottom of the window will turn green. Remember to save this scan by copy and pasting the contents in the "Output" field. 8. Under "Mode", click on the "UDP" radial, then repeat steps 6 and 7. 9. Launch SuperScan (v.2.06). 10. Click on the "All ports from" radial and enter "1" in the left box and "65535" in the right. 11. Enter the target host's IP address in the "Start" and "Stop" Fields then click on the "Start" button. 12. When the scan is finished, the "Start" button will no longer be grayed out. Remember to save this scan by clicking the "Save" button.
Compliance	No TCP or UDP ports should show open on either of the Netscreen-5XP's.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item 7	**Objective:** Check for internet access from the credit union's network via the Netscreen-5XP VPN appliance.
Reference	1. Personal experience 2. Insecure.org http://www.insecure.org/nmap/data/nmap_manpage.html 3. Foundstone.com http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm 4. Network Auditing Essentials Track 7 – Auditing Networks, Perimeters and Systems 5. Auditing the Perimeter Track 7 – Auditing Networks, Perimeters and Systems
Risk	Unnecessary open TCP or UDP ports on the credit union's Netscreen-5XP to the internet.
Procedure	1. Establish a network connection on the trusted side of the credit union's Netscreen VPN appliance with a valid IP address. 2. In your TCP/IP properties, enter the IP address of the Netscreen-5XP's trusted network connection as the default gateway. 3. Ensure that your browser settings are set NOT to use a proxy server. 4. Launch NMAPWIN (v.1.3.1) and click on the "Discovery" tab. 5. Click the "Don't Ping" radial. 6. Click on the "Scan" tab then click on "Port Range" under "Scan Options". 7. Enter "1-65535" in the "Port Range" field. 8. In the "Hosts" field at the top of the screen, *x.x.x.x* (our Honeypot) then click on "Scan". 9. When scan is finished, the third box from the right on the bottom of the window will turn green. Remember to save this scan by copy and pasting the contents in the "Output" field. 10. Under "Mode", click on the "UDP" radial, then repeat steps 6 and 7. 11. Launch SuperScan (v.2.06).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	12. Click on the “All ports from” radial and enter “1” in the left box and “65535” in the right. 13. Enter the Honeypot’s IP address in the “Start” and “Stop” Fields then click on the “Start” button. 14. When the scan is finished, the “Start” button will no longer be grayed out. Remember to save this scan by clicking the “Save” button.
Compliance	No TCP or UDP ports should show open.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3

Item 8	**Objective:** Check for internet access from AB Systems’ network via the Netscreen-5XP VPN appliance.
Reference	1. Personal experience 2. Insecure.org http://www.insecure.org/nmap/data/nmap_manpage.html 3. Foundstone.com http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm 4. Network Auditing Essentials Track 7 – Auditing Networks, Perimeters and Systems 5. Auditing the Perimeter Track 7 – Auditing Networks, Perimeters and Systems
Risk	Unnecessary open TCP or UDP ports on AB Systems’ Netscreen-5XP to the internet.
Procedure	1. Establish a network connection on the trusted side of AB Systems’ Netscreen VPN appliance with a valid IP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	address. 2. In your TCP/IP properties, enter the IP address of the Netscreen-5XP's trusted network connection as the default gateway. 3. Ensure that your browser settings are set NOT to use a proxy server. 4. Launch NMAPWIN (v.1.3.1) and click on the "Discovery" tab. 5. Click the "Don't Ping" radial. 6. Click on the "Scan" tab then click on "Port Range" under "Scan Options". 7. Enter "1-65535" in the "Port Range" field. 8. In the "Hosts" field at the top of the screen, *x.x.x.x* (our Honeypot) then click on "Scan". 9. When scan is finished, the third box from the right on the bottom of the window will turn green. Remember to save this scan by copy and pasting the contents in the "Output" field. 10. Under "Mode", click on the "UDP" radial, then repeat steps 6 and 7. 11. Launch SuperScan (v.2.06). 12. Click on the "All ports from" radial and enter "1" in the left box and "65535" in the right. 13. Enter the Honeypot's IP address in the "Start" and "Stop" Fields then click on the "Start" button. 14. When the scan is finished, the "Start" button will no longer be grayed out. Remember to save this scan by clicking the "Save" button.
Compliance	No TCP or UDP ports should show open.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3
Item 9	**Objective:** Assess the physical security controls that directly relate to the Netscreen VPN appliances.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Reference	1. Personal experience 2. *Let's Get Physical*; Mark Brunelli http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci968591,00.html 3. http://www.hidcorp.com/products/proximityproducts/entryprox.html 4. http://www.dir.state.tx.us/security/policies/physical_access_policy.doc 5. http://cis.tamu.edu/security/microsoft/PhysicalSecurity.ppt #5
Risk	Unauthorized access to AB Systems' network, Unauthorized access to the credit union's network and unauthorized access to the Netscreen VPN appliance's configuration. Theft of Netscreen VPN appliance.
Procedure	1. Review AB Systems' Security Policy Manual for Policies, Standards and Procedures that address the physical access control to the area where the Netscreen VPN appliances are kept. Areas that should be looked for, but not limited to: A. Key/Card issuance, management and privacy policies. B. How are visitors handled? Registration, Visitor Badge. C. Access revocation procedures due to termination of employment. D. Signage for restricted areas. 2. Physically inspect access controls. 3. Interview System Administrator to discuss their level of awareness of these policies
Compliance	At a minimum, AB Systems should have the policies that address items A, B, and C listed above. Additionally, the System Administrator should display a good understanding of these policies. The actual physical access controls should be consistent with the policies described in AB Systems Security Policy manual.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Objective/ Subjective	Objective – Either physical access policies exist or they do not. Subjective – The auditor must use their experience and references to judge whether or not AB Systems is compliant with this audit item.
Evidence	Refer to section 3
Findings	Refer to section 3

Item 10	**Objective:** Review event log settings and polices that apply to the Netscreen VPN appliance.
Reference	1. Personal experience 2. *NetScreen Concepts & Examples ScreenOS Reference Guide* Volume3:Administration 3. *The Importance of Logging and Traffic Monitoring for Information Security*, Seham Mohamed GadAllah 4. *Windows Security Resource Kit*; Ben Smith and Brian Komar – Chapter 12 Auditing Microsoft Windows Security Events
Risk	Weak event log settings and/or policies.
Procedure	1. Review AB Systems' Security Policy Manual for Policies, Standards and Procedures that address event log management. Areas that should be looked for, but not limited to: A. What events are to be logged? B. How long are logs retained? C. How often are logs reviewed and by whom? 2. Review actual log settings in use on the Netscreen VPN appliances(Note. This needs to be performed on both Netscreen VPN appliances). A. With an internet browser, connect to the administrative website of the Nescreen VPN appliance (http://x.x.x.x) and log in. B. On the left hand side of the screen, click on "configuration", "Report Settings" then "Log

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Settings". C. Record findings D. Click on "Syslog" and record settings. 3. Interview System Administrator to discuss their level of awareness of these policies
Compliance	At a minimum, logs should be retained for 30 days and reviewed weekly. AB Systems Security Policy manual should reflect this. Additionally, all security events should be logged. The Systems Administrator should display a thorough knowledge of these policies.
Objective/ Subjective	Objective – With regards to log policies Subjective – With regards to how well the System Administrator knows these policies.
Evidence	Refer to section 3
Findings	Refer to section 3

Item 11	**Objective:** Review password policies.
Reference	1. Personal experience 2. *Windows Security Resource Kit*; Ben Smith and Brian Komar – Chapter 3 Securing User Accounts and Passwords
Risk	Weak password settings and/or policies.
Procedure	1. Review AB Systems' Security Policy Manual for Policies, Standards and Procedures that address passwords. Areas that should be looked for, but not limited to: A. Password construction rules. B. Password rotation schedule. C. Password privacy.
Compliance	At a minimum, passwords should be seven characters, contain

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	one of each of the following: number, special character, upper and lowercase letters. Passwords should also not contain words, names, dates or easy to guess phrases.
Objective/ Subjective	Objective
Evidence	Refer to section 3
Findings	Refer to section 3

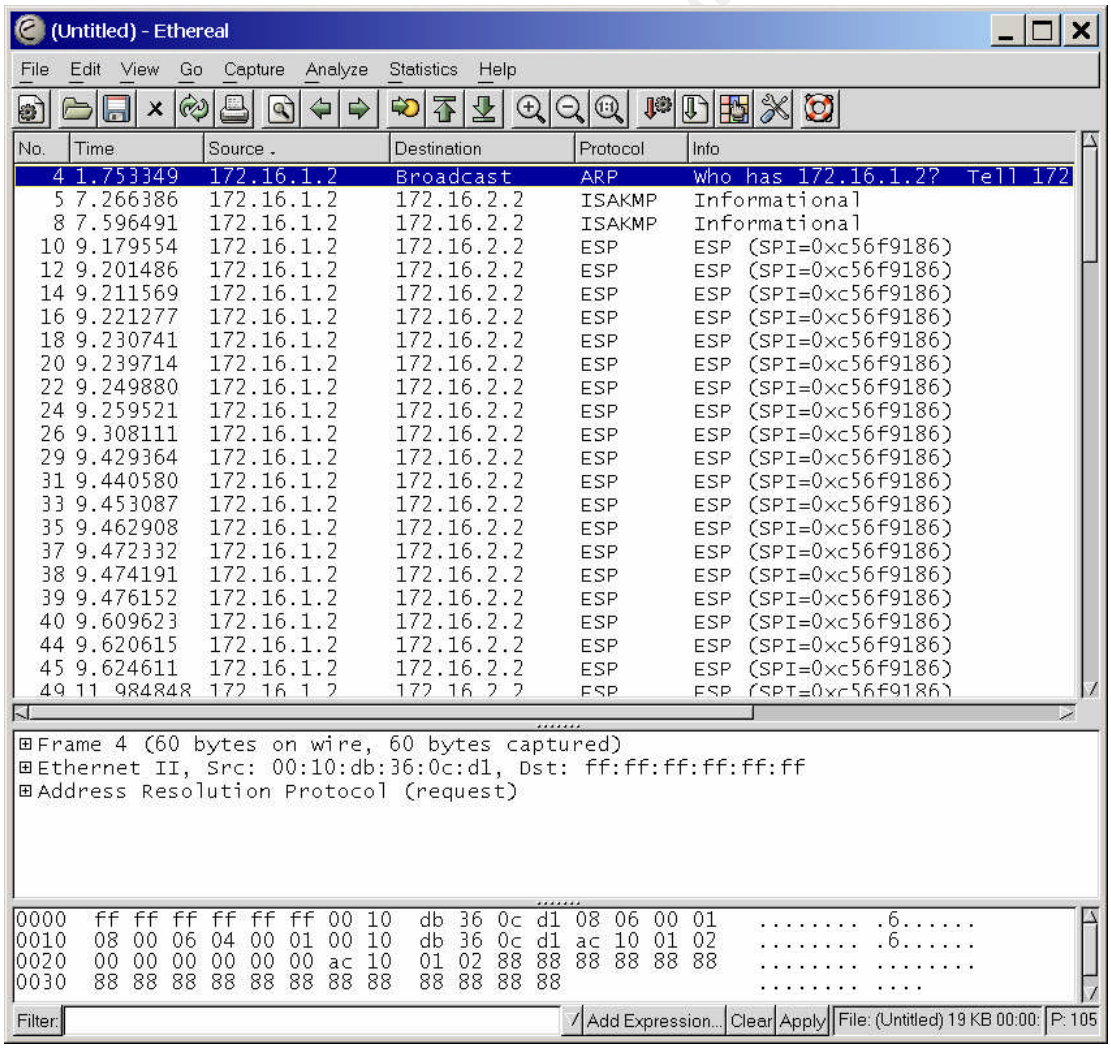
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

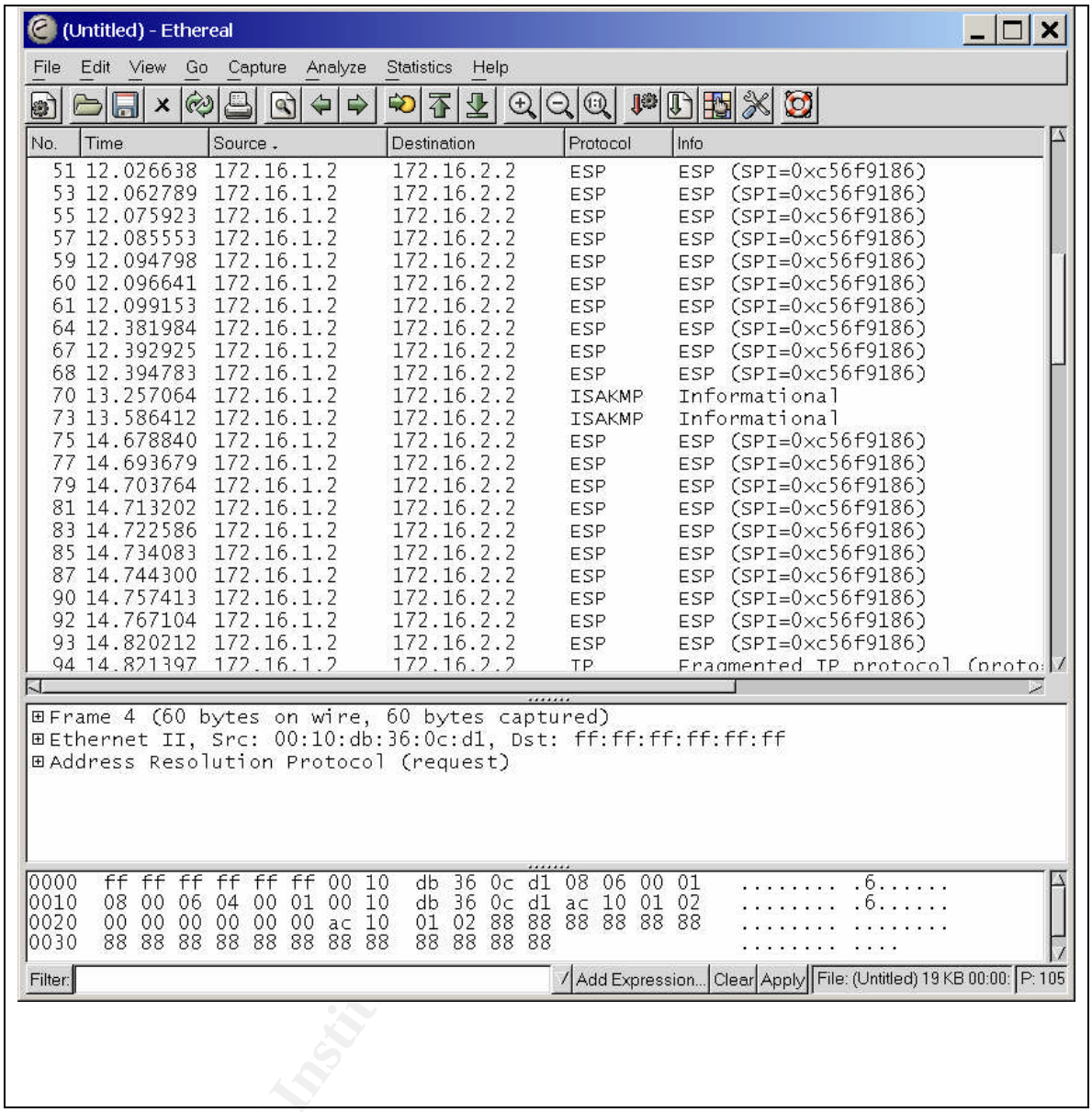
3. Conduct the Audit Testing, Evidence and Findings

Item 1	**Objective:** Ensure that data being transmitted between VPN devices cannot be viewed in clear text.

Audit:
Using Ethereal, we captured the data being transmitted between the two Netscreen-5XP VPN appliances. This packet capture included the initial handshake between these two devices (172.16.1.2 and 172.16.2.2) as well as a file transmission once the VPN tunnel was established. Below are screen shots of our results from this packet capture. Due to the number of frames involved, we were required to take several screen shots.

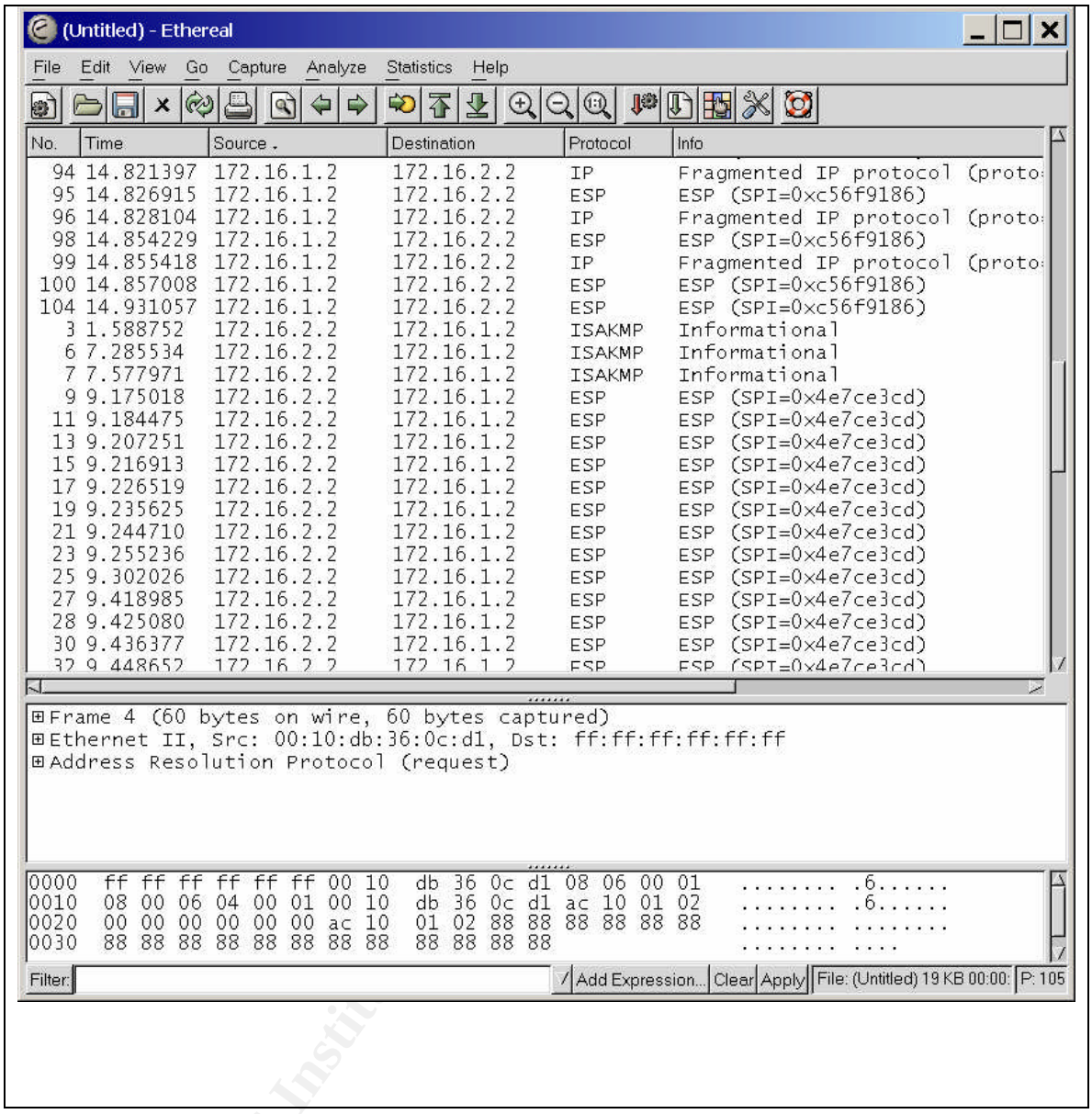


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



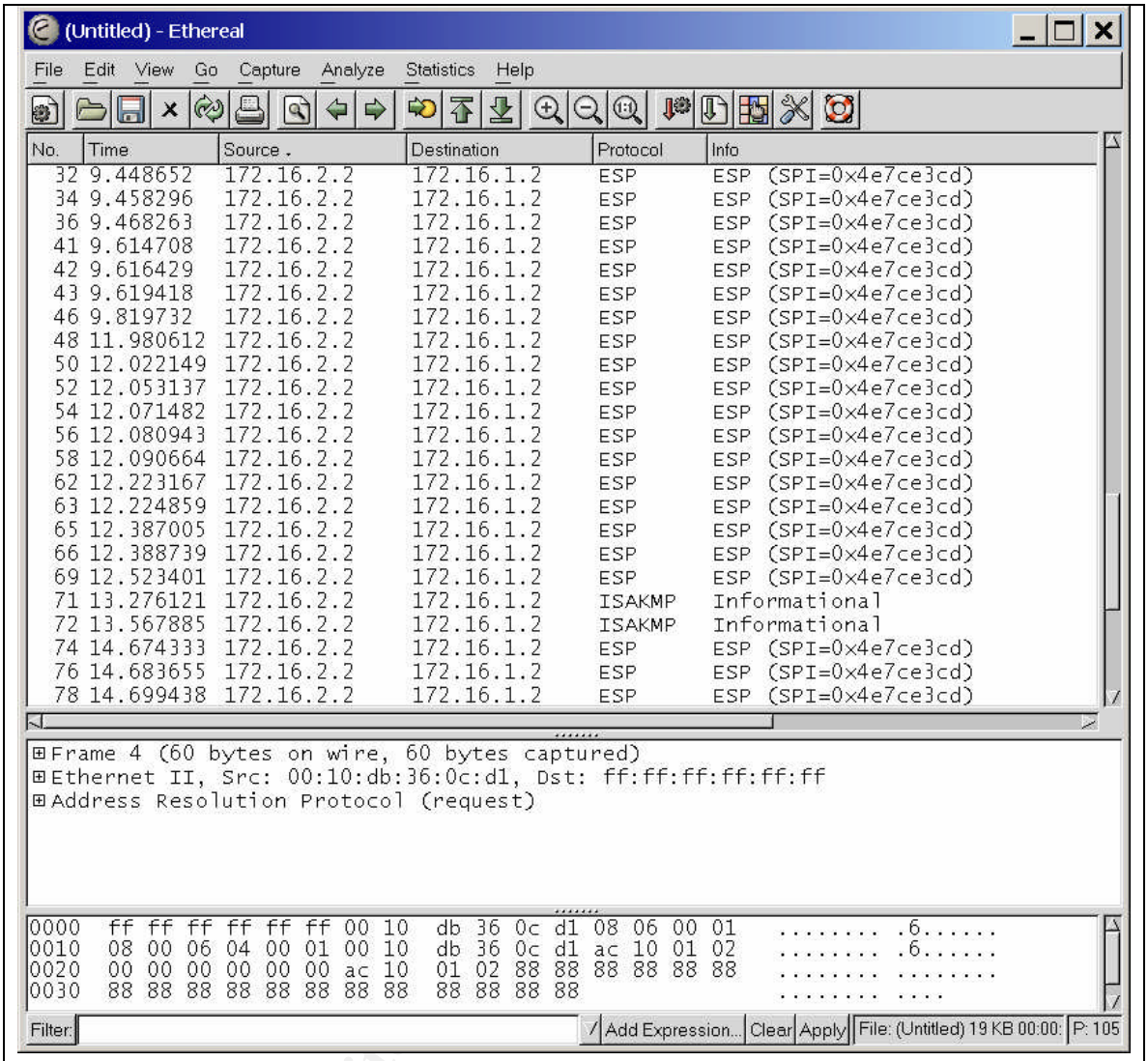
© SANS Institute

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



As stated in the Compliance section of this audit item, only ESP, ISAKMP and ARP protocols should be discovered by this packet capture. As the test results show, the results we expected and hoped to find were positive.

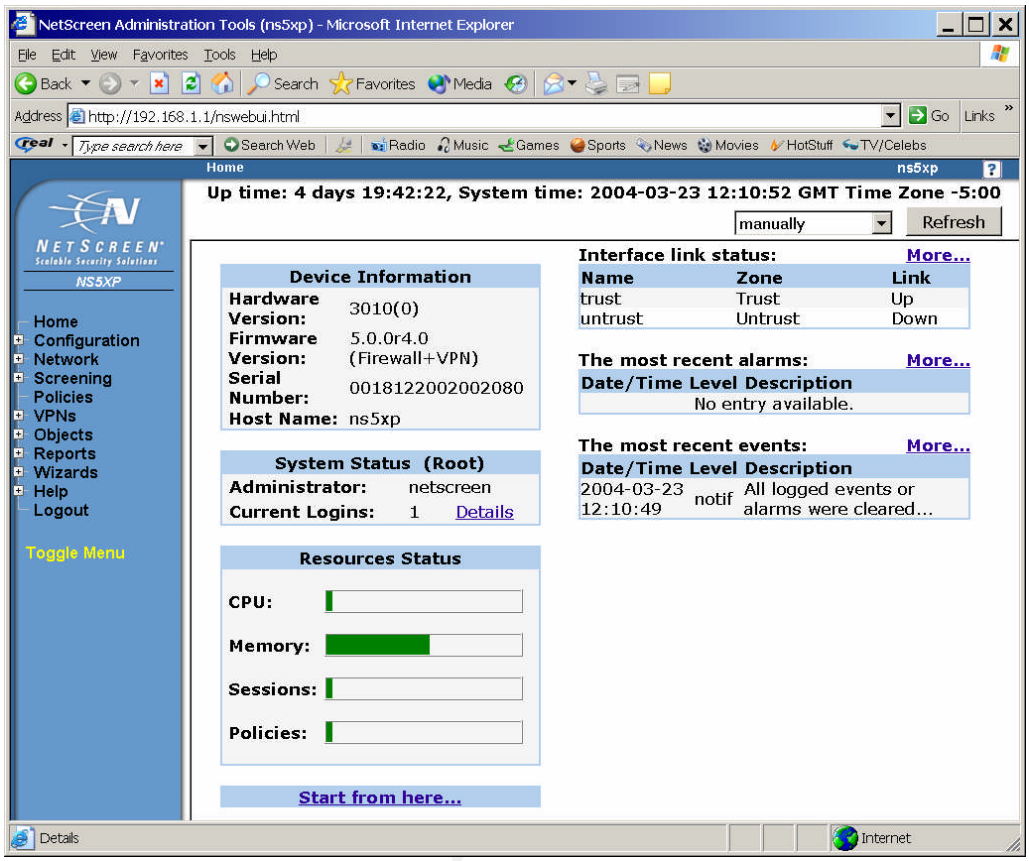
We should note that this test only validates the use of encryption and does not verify the level of encryption being used.

Compliance: The audit results fall within our compliance parameters

Item 2	**Objective:** Research any known vulnerabilities that apply to the Netscreen 5XP and ScreenOS 5

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Audit:
As stated earlier, the Netscreen-5XP VPN appliances are running ScreenOS5.

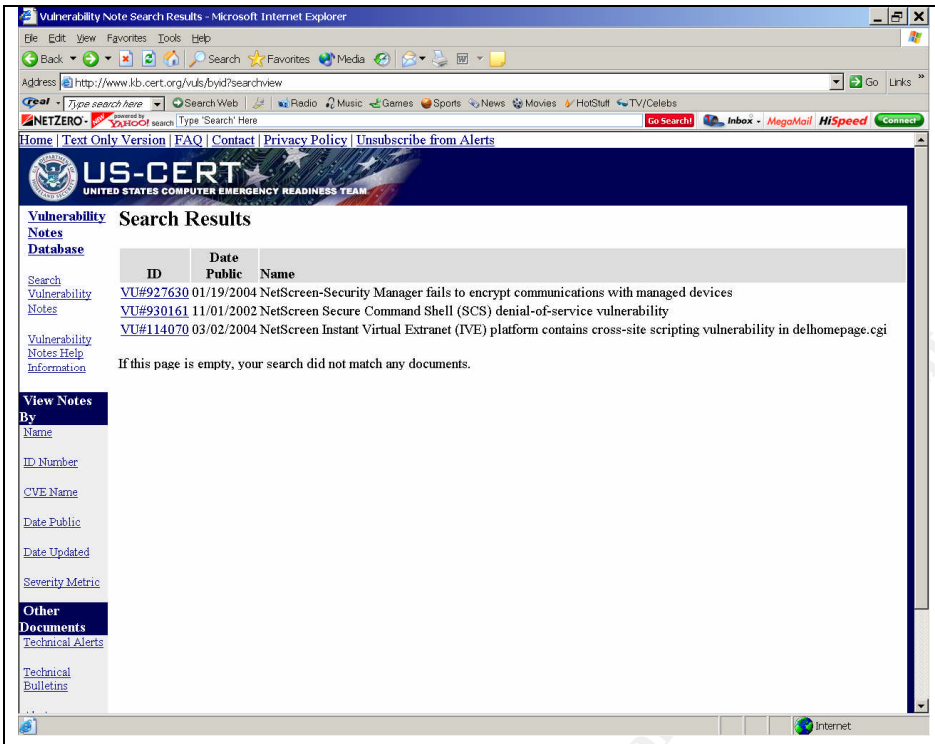


With this in mind, we researched several resources looking for known vulnerabilities that are applicable to this level of OS and configuration.

We first searched the CERT Vulnerability Notes Database http://www.kb.cert.org/vuls. A search on the word “Netscreen” returns the following:

© SANS Institute 2004,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

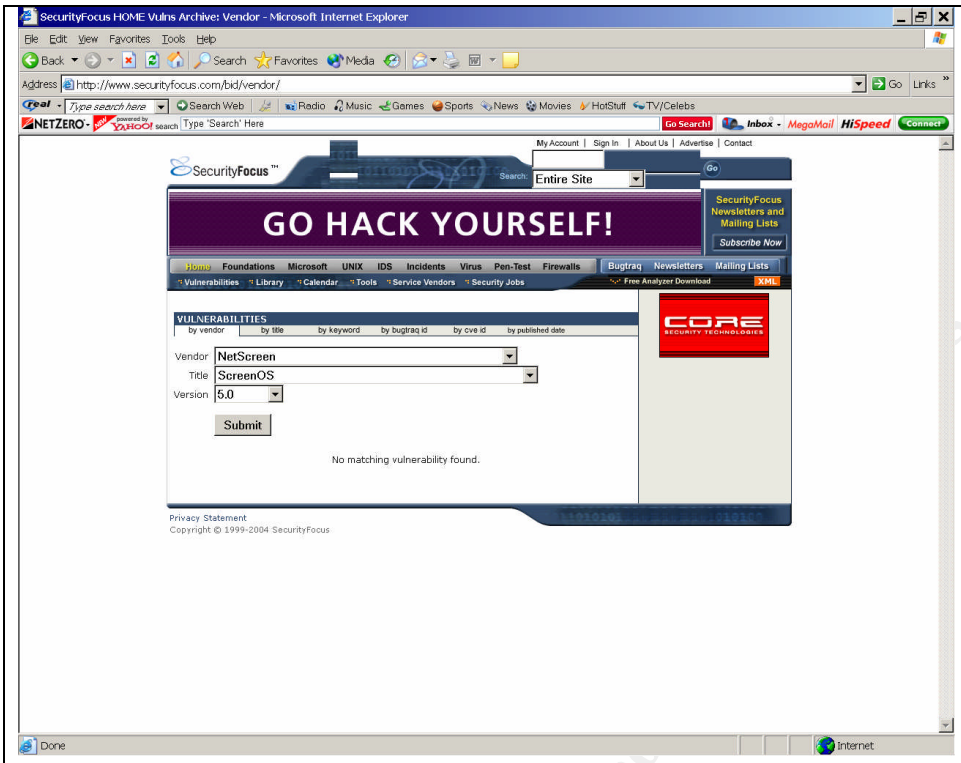


One of these posted vulnerabilities apply to Netscreen's OS5 (VU#927630). Of the remaining two, one predates OS5 and the other only applies to Netscreen's Instant Virtual Extranet product.

The one vulnerability applicable to OS5 does not apply to AB Systems' configuration. VU#927630 is only applicable if Netscreen Security Manager is used for centralized management. AB Systems has opted to manage their Netscreen appliances individually via the built-in web management console, thus making this vulnerability non-applicable.

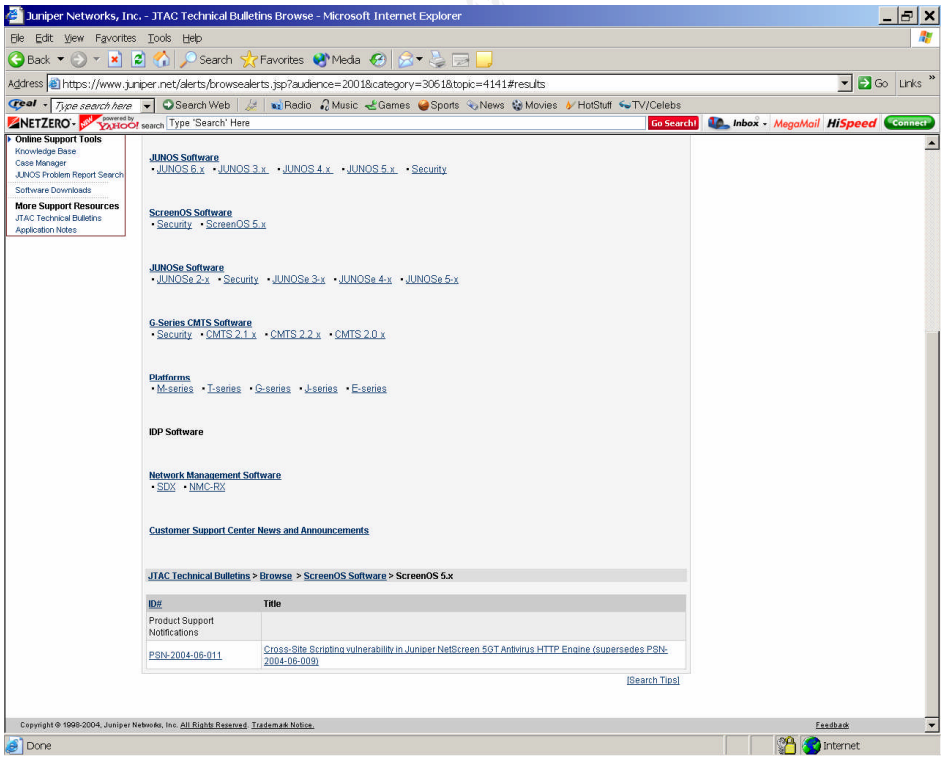
We also checked Security Focus http://www.securityfocus.com/bid for any potential vulnerabilities. Our query returned the following:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



As can be clearly seen, Security Focus has no listed vulnerabilities for OS5.

Finally, we checked the vendor's website. The results follow:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The only listed vulnerability related to OS5 running on a Netscreen-5GT and is not applicable to our installation. We should also note that this particular audit item is a prime reason why a security practitioner should not rely solely on one source for researching vulnerabilities as all three sources provided different results.
Compliance: The audit results fall within our compliance parameters as we found no applicable vulnerabilities.

Item 3	**Objective:** Check AB Systems Security Policy Manual for patch management policies.

Audit:

We searched AB Systems' Security Policy manual for topics that discuss the patch management process at AB Systems. The only reference of patch management we could find can be found on page 13 under the heading of *Prompt Implementation of Security Problem Fix Software, Scripts, Etc.* and state the following:

> "All security patching software, command scripts, and the like provided by operating system vendors, official computer emergency response teams (CERTs), and other trusted third parties will be promptly implemented subject to approval by Management. No software or patches will be loaded on production systems (Web Servers, SQL Servers, or other systems responsible for public productions) unless tested in a proxy environment first. Deviations to this rule may only be approved by management."

Although this statement mandates that patches be implemented immediately and that patches must be first tested in a proxy environment prior to implementation on production systems, it does leave out several areas we feel are critical to patch management policies. We feel that the following topics need to be addressed in the Security Policy manual:

A. Notification of available patches.
B. Procedures for deployment.

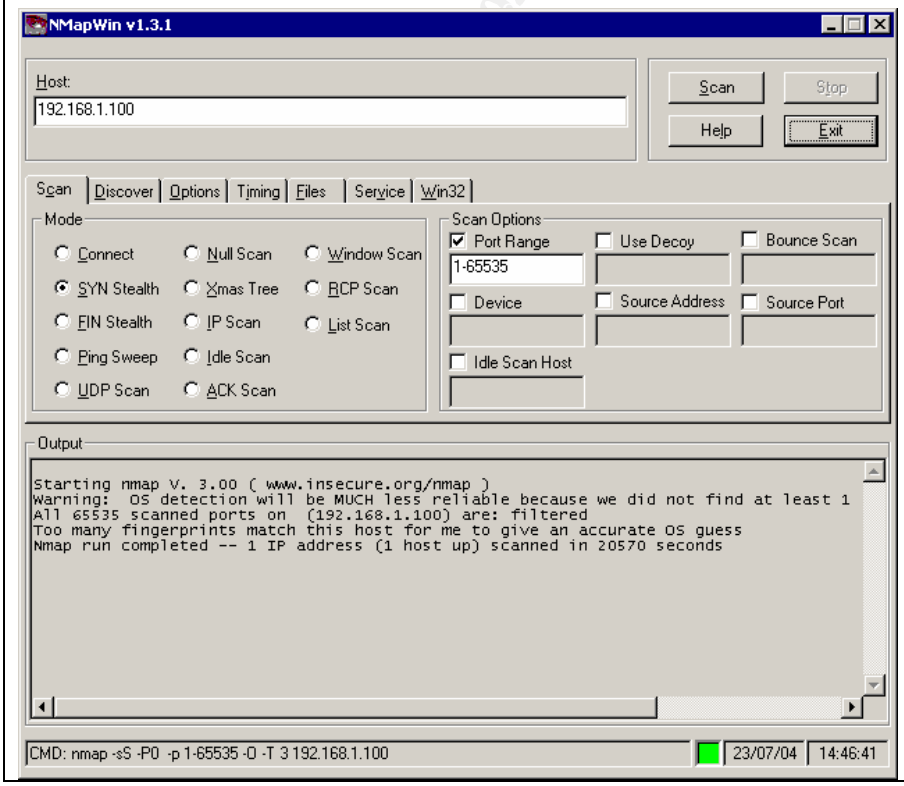
We also spoke with Doug R., Director of Operations and System Administrator at

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

AB Systems. With regards to notification of vulnerabilities and available patches, he told us that they rely primarily on email notifications from various sources such as Security Focus. He stated that AB Systems has a schedule of patching PCs and servers once a month but hardware devices such as the Netscreen-5XP are not included. He also relayed to us that nearly all the patches they implement are downloaded from vendor sites, implemented first in a lab environment, the deployed to production systems during non-peak hours.
Compliance: It is clear that Doug R. is educated on the proper patch management policies we look for in a successful patch management program. However, the written Security Policy could address these issues in greater detail.

Item 4	**Objective:** Scan for unnecessary open ports from the credit union's network towards AB Systems' network.

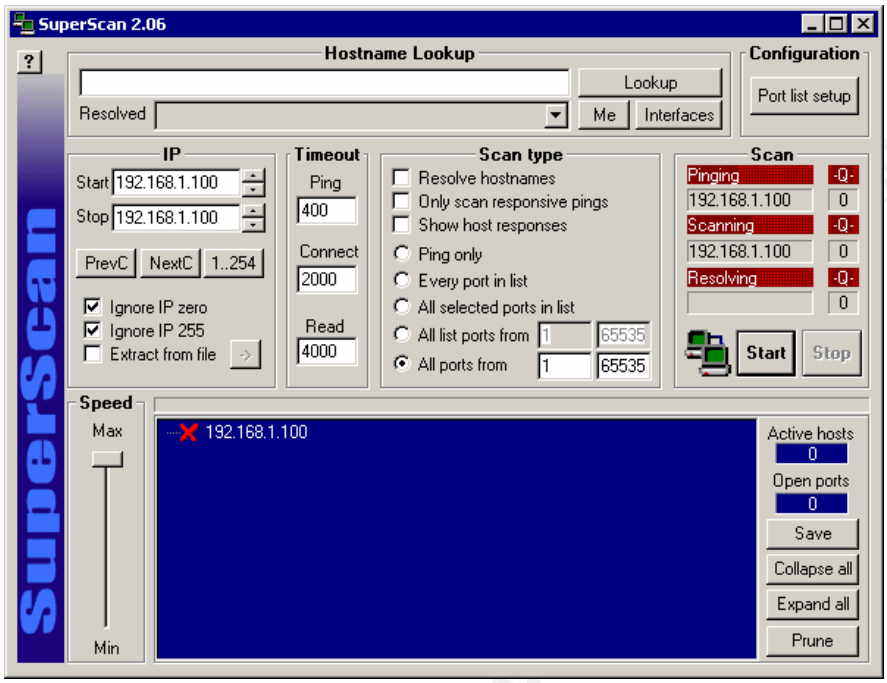
Audit:
The first tool we used for this audit was NMAPWin v1.3.0. We scanned the transaction server on AB Systems' network for open TCP ports and obtained the following results:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The results of this scan show that all TCP ports are filtered to this system.

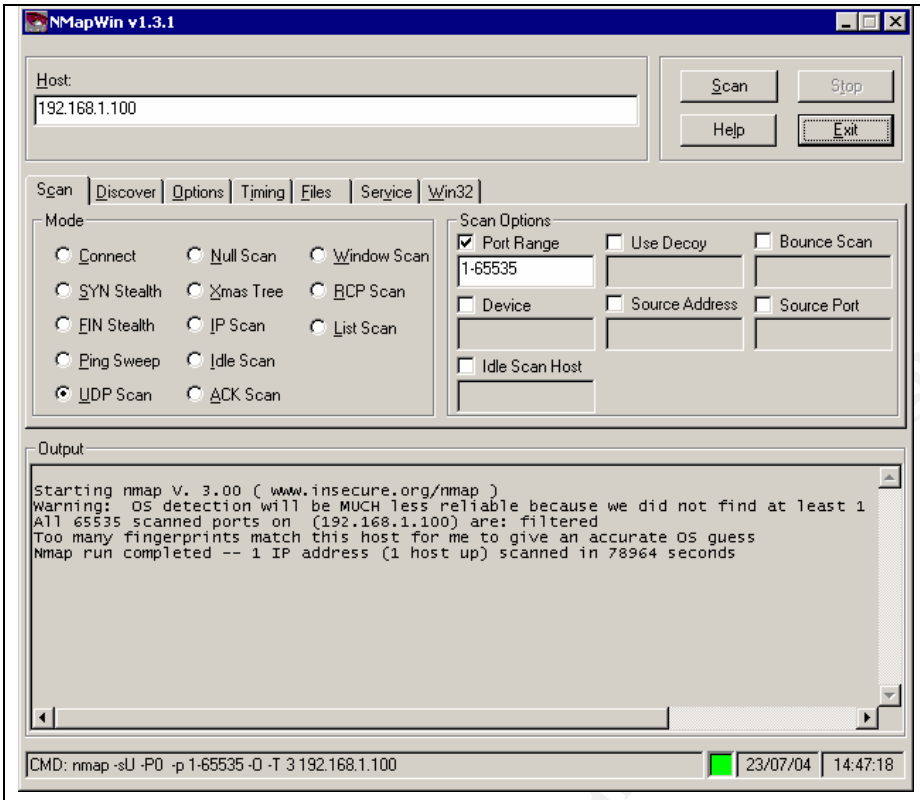
Even though NMAP is an effective tool, we also used SuperScan 2.06 to confirm our results from our NMAPWin TCP scan. This test returned the same results:



We used NMAPWin to scan AB Systems' network for open UDP ports and obtained the following results:

© SANS Institute 2004, All rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



We again find that all UDP ports are filtered as well.

We should note that SuperScan only supports TCP scanning.

Compliance: This audit item is within compliance parameters.

Item 5	**Objective**: Scan for unnecessary open ports from AB Systems' Network towards the credit union's network.

Audit:
Like item 4, we used the same sets of tools for this audit item; NMAPWin v1.3.0 and SuperScan 2.06 for TCP scanning and only NMAPWin v1.3.0 for UDP scanning. We should note that to keep the size of this audit file down, we elected not to insert screen shots into the remaining audits that used the same tools. Instead, we have cut and paste the command generated by NMAP and the associated output. The results follow:

NMAPWin TCP Scan:
CMD nmap –sS –p 1-65535 –O –T 3 10.1.1.200

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (10.1.1.200) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20720 seconds

The results of this scan show that all TCP ports are filtered to this system.

The SuperScan TCP Scan confirmed the NMAPWin Findings as all TCP ports are not listening.

NMAPWin UDP Scan:
CMD nmap –sU –p 1-65535 –O –T 3 10.1.1.200
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (10.1.1.200) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20520 seconds

The results of this scan show that all UDP ports are filtered to this system.

Compliance: This audit item is within compliance parameters.

Item 6	**Objective:** Scan for unnecessary open ports on the Netscreen VPN appliances from the internet.

Audit:
Using the same tools as before, we scanned both Netscreen-5XP's and obtained the following results:

NMAPWin TCP Scan:
CMD nmap –sS –p 1-65535 –O –T 3 172.16.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.1.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20615 seconds

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CMD nmap –sS –p 1-65535 –O –T 3 172.16.2.2
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.2.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20573 seconds

The results of these scans show that all TCP ports are filtered to both Netscreen VPN appliances.

Again, the SuperScan TCP Scan confirmed the NMAPWin Findings as all TCP ports are not listening.

NMAPWin UDP Scan:
CMD nmap –sU –p 1-65535 –O –T 3 172.16.1.2
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.1.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20529 seconds

CMD nmap –sU –p 1-65535 –O –T 3 172.16.2.2
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.2.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20566 seconds

The results of these scans show that all UDP ports are filtered to both Netscreen VPN appliances.

Compliance: This audit item is within compliance parameters.

Item 7	**Objective:** Check for internet access from the credit union's network via the Netscreen-5XP VPN appliance.
Audit:	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NMAPWin TCP Scan:
CMD nmap –sS –p 1-65535 –O –T 3 172.16.3.212
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.3.212) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20572 seconds

The results of this scan show that all TCP ports are filtered to the internet.

The SuperScan TCP Scan confirmed the NMAPWin Findings as all TCP ports are not listening.

NMAPWin UDP Scan:
CMD nmap –sU –p 1-65535 –O –T 3 172.16.3.212
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.3.212) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20565 seconds

The results of this scan show that all UDP ports are filtered to the internet.

Compliance: This audit item is within compliance parameters.

Item 8	**Objective:** Check for internet access from AB Systems' network via the Netscreen-5XP VPN appliance.

Audit:
NMAPWin TCP Scan:
CMD nmap –sS –p 1-65535 –O –T 3 172.16.3.212
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.3.212) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20568 seconds

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The results of this scan show that all TCP ports are filtered to the internet.

The SuperScan TCP Scan confirmed the NMAPWin Findings as all TCP ports are not listening.

NMAPWin UDP Scan:
CMD nmap –sU –p 1-65535 –O –T 3 172.16.3.212
Starting nmap V. 3.00 (www.insecure.org/nmap)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on (172.16.3.212) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 20569 seconds

The results of this scan show that all UDP ports are filtered to the internet.

Compliance: This audit item is within compliance parameters.

Item 9	**Objective:** Assess the physical security controls that directly relate to the Netscreen VPN appliances.

Audit:

We searched AB Systems' Security Policy manual for topics that discuss physical security in place at AB Systems. Starting on page 17 under the heading of *Physical Security*, AB Systems has written a comprehensive policy that addresses most of the topics we look for in a comprehensive physical security policy. However, we do feel that there is room for improvement. The following areas we feel need to be added or discussed in greater detail:

Handling Visitors – this topic is covered but should include statements that require visitors sign a guest register and are assigned a visitors badge.

Video Surveillance – this topic is covered but does not mention the retention times of surveillance tapes.

Signage – this topic needs to be added and include statements that require sings to be posted indicating that an area is off limits to unauthorized personnel.

Key/Card Privacy – this topic should be added and include statements that require employees to protect their Keys and access card and never lend them out.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

We also manually reviewed the physical controls in place at AB Systems. Since we were escorted by Doug R., the Systems Administrator, we also question him with regards to these policies in place.

There are three entrances that lead into AB Systems. Of these, only one is accessible by all employees. The other two are kept locked at all times and only three individuals have these keys; the two owners and the System Administrator.

The main entrance leads to another locked door that is only accessible with an electronic access card. This system, provided by HID Corporation, allows AB Systems to track who access the building and computer room at what time. The system also has the ability to restrict access via time but this function is not in use. Access through this entry point can be overridden with a four digit PIN but only by the same three individuals previously mentioned.

We should also note that cameras are placed throughout the building in strategic locations and tapes are kept for thirty days.

Visitors are required to sign a guest register and are provided a visitor badge. This badge is numbered and noted on the guest register. However, these badges are not dated so there is no expiration period.

Once inside, the computer room is the only restricted area in the building. The same HID system is used to protect this room and requires the use of a PIN to access. Only employees who need access to this room are provided PINs. This is where the NetScreen 5-XP on AB Systems' side resides.

We should also note that this item only pertains to the AB Systems side of the connection due to different configurations at various credit unions.

As stated earlier, we spoke with Doug R. during this review and found him to be quite knowledgeable of the policies in place with regards to physical security. He also stated that physical security is discussed with all credit unions as to what AB Systems has in place as well as what AB Systems expects from the credit union.

Compliance: AB Systems has installed a comprehensive physical security architecture that meets/exceeds our standards for this audit item. However, improvement could be made with regards to the written policies that address physical security making this audit item out of compliance.

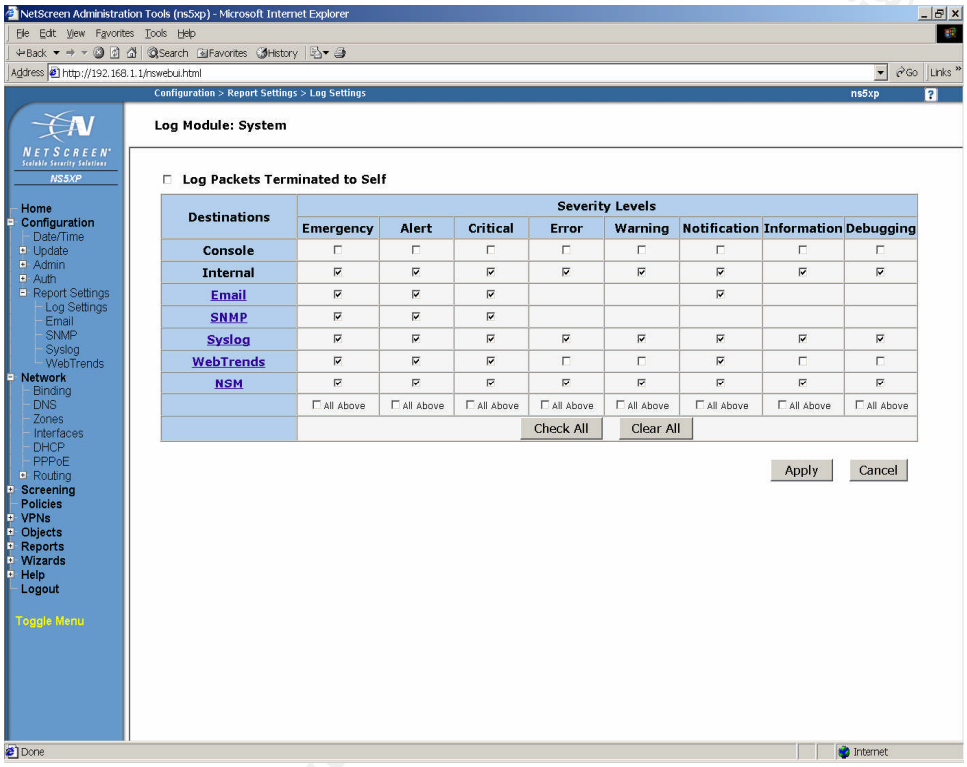
Item 10	**Objective:** Review event log settings and polices that apply to the Netscreen VPN appliance.

Audit:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

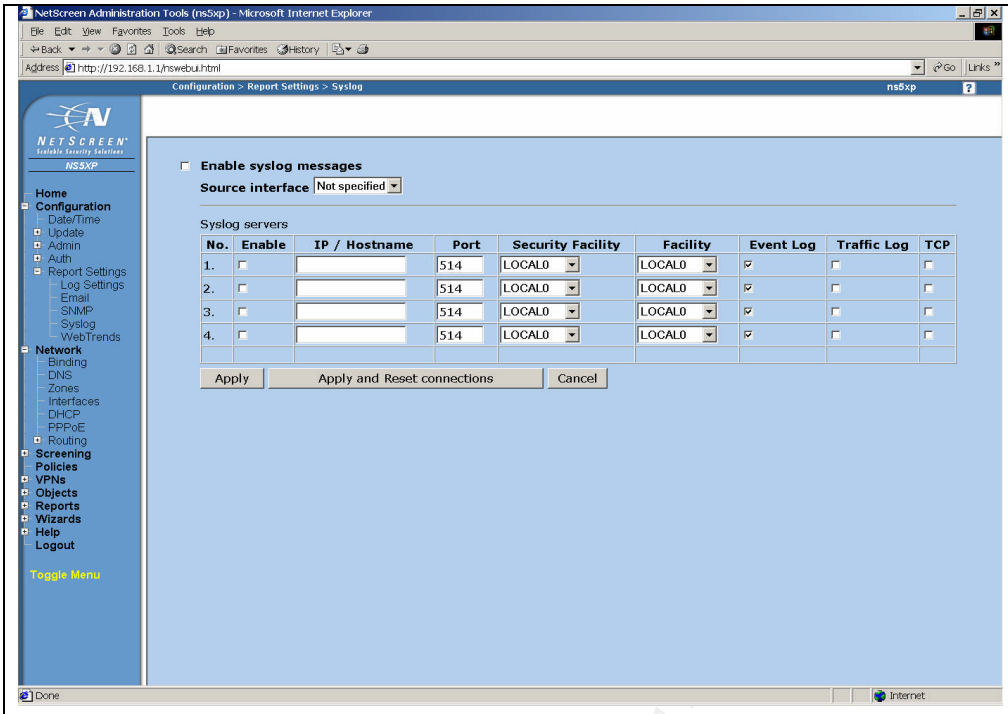
We searched AB Systems' Security Policy manual for topics that discuss the logging policies in place at AB Systems. Starting on page 11 under the heading of *Logging*, AB Systems has written a comprehensive policy that addresses all of the topics we look for in a comprehensive logging policy. The only exception to this is that throughout this section, only Servers are referenced instead of all critical systems. We feel that inclusion of all critical systems along with examples would be beneficial as it could prevent an oversight.

We also reviewed the log settings on the Netscreen-5XP's. Both were identical and were set to the default settings.



Fortunately, nearly all of the events are being logged, and the ones that aren't are not applicable (Webtrends and the console are not in use). However, the Netscreen 5-XP does not have the ability to store logs as it has no hard drive. Only logs from recent history can be viewed and if the system is rebooted, the few logs that had been stored are lost. This means that for AB Systems to retain these logs for a minimum of 30 days per the security policy, the Netscreen-5XP needs to make use of a Syslog server. Unfortunately, as the image below and Doug R. confirm, these logs are not being sent to a Syslog server for retention.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Additionally, Doug R. stated that the event logs for the Netscreen-5XPs are only reviewed when trouble shooting a problem.

Compliance: As the discussion above indicates, there is room for improvement for all aspects of this audit item making it non-compliant.

Item 11	**Objective:** Review password construction rules.

Audit:
We searched AB Systems' Security Policy manual for topics that discuss the password policies in place at AB Systems. Starting on page 6 under the heading of *User IDs and Passwords*, AB Systems has written a comprehensive policy that addresses all of the topics we look for in a comprehensive password policy such as strong password construction rules, prohibition of sharing passwords, safekeeping of passwords, and routine changing of passwords.

Unfortunately, the Netscreen-5XP cannot enforce password polices so it is up to the System Administrator to ensure that these rules are enforced. Currently, only Doug R. and one other technician know the passwords for the Netscreen-5XP's. These passwords are stored in a proprietary database (HanDbase Desktop 3.0) that is locally installed on each of their workstations. He informed us that

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

passwords used on the Netscreens conform to the following construction rules: 1. Passwords should be at least eight characters in length; 2. Passwords should be difficult to guess (i.e., should not be words in a dictionary, derivatives of the User's ID, or common character sequences); 3. Passwords should contain at least three of the following four types of characters: upper case letters, lower case letters, numerals, and non-alphanumeric "special" characters such as !@#$%^&*. He also informed us that these passwords are not rotated on a routine basis.
Compliance: Although AB Systems seems to have a well written and executed password policy, routine password rotation should be given consideration. However, given the size of this business and other security precautions in place, we feel that this one exception is not enough to make this audit item out of compliance.

4. Audit Report

4.1 Executive Summary

We were contracted by AB Systems to assess their security posture as it applies to the Netscreen-5XP VPN appliances and the site-to-site virtual private network they support. Some ancillary investigation into areas such as physical security and password polices were conducted and reported on, but only as they apply to the Netscreen-5XP VPN appliances.

As the findings below will show, AB Systems' implementation of site-to-site VPN's appears to be in a strong state of security with regards to unauthorized access to each organization's network, OS vulnerabilities and secure transmission of sensitive information. However, the findings will also show that that significant improvement can be made in the area of written security policies and log retention. Fortunately, these two areas are relatively inexpensive to correct and we feel confident that Doug R. and the rest of the staff at AB Systems are up to the task of implementing our recommendations.

4.2 Audit Findings and Recommendations

As stated earlier, the areas of improvement we found lie with written security polices and log retention. Below are our findings and recommendations for items that were out of compliance.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item 3 – Check AB Systems Security Policy Manual for patch management policies.

As was pointed out in this audit item, the only reference we could find regarding patch management was on page 13 under the heading of *Prompt Implementation of Security Problem Fix Software, Scripts, Etc.* and states the following:

> "All security patching software, command scripts, and the like provided by operating system vendors, official computer emergency response teams (CERTs), and other trusted third parties will be promptly implemented subject to approval by Management. No software or patches will be loaded on production systems (Web Servers, SQL Servers, or other systems responsible for public productions) unless tested in a proxy environment first. Deviations to this rule may only be approved by management."

Although this statement addresses some of the issues we look for in an effective patch management security policy, we feel this policy could use some additional information to make it more comprehensive. Topics that we would like to see included are as follows:

Notification: How is AB Systems notified and kept up to date of new security patches? We recommend using services such as CERT, the vendors of products in use and Security Focus.

Assessment: How does AB Systems keep track of systems and the software running on them to determine whether or not a system is an update candidate? With regards to the Netscreens, auditing tools are really not an option. However, creating a spreadsheet that tracks the installed OS', basic configurations, and dates for patch deployment would address this topic well.

Obtainment: What are the procedures for obtaining updates? Receiving hard copies of updates are the most secure way but very impractical when dealing with time-sensitive issues such as security patches. The best alternative is to download from the vendors website.

Testing: This policy is stated above with regards to proxy testing but should be broken out into its own topic.

Deployment: What time frame applies to when a patch is posted to when AB Systems deploys it? Bottom line here is to deploy a patch as soon as possible.

Having strong patch management policies will further reduce the potential for a system not being properly updated as well as place assigned responsibilities on individuals who participate in this practice. This in turn should heighten everyone's awareness who is involved thus ensuring these task are completed correctly and in a timely manner.

Item 9 – Assess the physical security controls that directly relate to the Netscreen VPN appliances.

During this portion of the audit, we found that AB Systems has taken strong steps limiting unauthorized access to not only the Netscreen-5XP VPN appliance but to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the entire facility as well. However, once again we find that even though the implementation is strong, the written policies could use improvement. As we stated in the audit item, these issues need to be added or expounded upon:

Handling Visitors – AB Systems touches on this topic but left out statements that require visitors sign a guest register and are assigned a visitors badge.

Video Surveillance – AB Systems states that anyone entering the premises is subject to video surveillance but does not mention the retention times of surveillance tapes.

Signage – This topic needs to be added and include statements that require sings to be posted indicating that an area is off limits to unauthorized personnel.

Key/Card Privacy – This topic should be added and include statements that require employees to protect their Keys and access cards and never lend them out.

Again, written policies place responsibilities on individuals with regards to what is expected of them. Should an individual fail to comply with a written policy, it gives management a foundation to stand on when levying punishment. This will in turn heighten the awareness of employees thus strengthening the overall security posture.

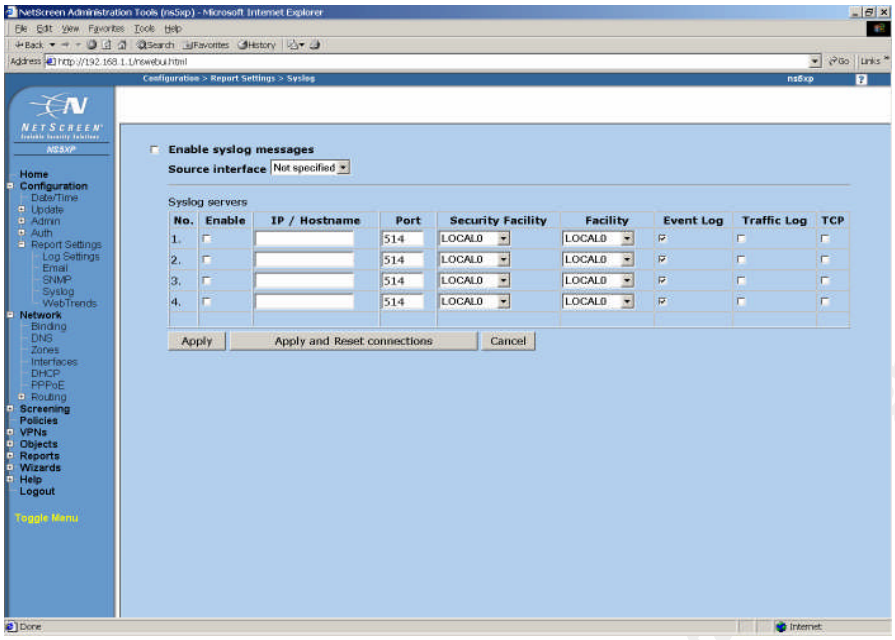
Item 10 – Review event log settings and policies that apply to the Netscreen VPN appliance.

This audit item showed a reversal of the last two items that were out of compliance. We found robust written policies in place regarding the logging of events only to find that some of these polices were not applied to the Netscreen VPN appliances.

As mentioned earlier, AB Systems security policy states that event logs are to be retained for a minimum of thirty days. Since the Netscreen VPN appliance does not support log retention of any length of time, and that event logs are lost every time the system is rebooted, a Syslog server is needed for event log retention. However, as is obvious from the screenshot below, the Netscreen VPN appliance is not configured to send logs to a Syslog server.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Since logs are not being stored and lost each time the Netscreen VPN appliance is rebooted, AB Systems has little to no way of reviewing logs after a short amount of time. Should a breach occur, these logs are critical to the forensic investigation.

We strongly suggest that AB Systems implement a Syslog server to retain logs for at least thirty days. In addition to the log retention benefits, a Syslog server can capture logs from multiple systems allowing AB Systems to consolidate logs and provide and easier method for review. We should also not that implementing a Syslog server can be relatively inexpensive as there are many shareware varieties available.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. References

1. Juniper Networks - NetScreen-5XP User's Guide Rev.A

2. Juniper Networks - NetScreen Concepts & Examples ScreenOS Reference Guide Volume5:VPNs Rev.E 2004

3. Juniper Networks - NetScreen Concepts & Examples ScreenOS Reference Guide Volume3:Administration 2004

4. US Senate Committee on Banking, Housing, and Urban Affairs - Gramm-Leach-Bliley Act – Title V, 1999 http://banking.senate.gov/conf/fintl5.pdf

5. Centers for Medicare and Medicaid Services – The Health Insurance Portability and Accountability Act, 1996 http://www.cms.hhs.gov/hipaa/

6. Gary Stonebumer, Alice Goguen, and Alexis Feringa - Risk Management Guide for Information Technology Systems, 2002 National Institute of Standards and Technology

7. Virtual Private Network Consortium - www.vpnc.org

8. The Internet Exchange Engineering Taskforce - www.ietf.org

9. Netgear - What is Encapsulating Security Payload (ESP)? http://kbserver.netgear.com/kb_web_files/N101014.asp

10. RFC 2406 - IP Encapsulating Security Payload (ESP) 1998 http://www.faqs.org/rfcs/rfc2406.html

11. RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) 1998 http://www.faqs.org/rfcs/rfc2408.html

12. CERT Vulnerability Notes Database http://www.kb.cert.org/vuls

13. Security Focus bugtraq http://www.securityfocus.com/bid

14. Netscreen Security Notices http://www.juniper.net/support/security/alerts/

15. Ben Smith and Brian Komar - Windows Security Resource Kit, 2003

16. Charlie Kaufman, Radia Perlman, and Mike Spciner – Network Security, Private Communications in a Public World, 1995

17. Insecure.org - http://www.insecure.org/nmap/data/nmap_manpage.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

18. Foundstone.com - http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm

19. SANS - Network Auditing Essentials Track 7 – Auditing Networks, Perimeters and Systems

20. SANS - Auditing the Perimeter Track 7 – Auditing Networks, Perimeters and Systems

21. Mark Brunelli - Let's Get Physical, 2003 http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci968591,00.html

22. HID Corporation http://www.hidcorp.com/products/proximityproducts/entryprox.html

23. State of Texas – Physical Security Policy Template http://www.dir.state.tx.us/security/policies/physical_access_policy.doc

24. Computing and Information Services - Physical Security, Power Point Presentation http://cis.tamu.edu/security/microsoft/PhysicalSecurity.ppt#5

25. Seham Mohamed GadAllah - The Importance of Logging and Traffic Monitoring for Information Security, 2003 GESC Practical Assignment

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.