GIAC
CERTIFICATIONS

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

GIAC Practical

Fortigate-60 Firewall Security Audit: An Auditor's Perspective

GSNA Practical Assignment 3.1 (Amended February 24, 2004)
Option 1

Author: Brian Cook
Submitted December 1st, 2004

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract/ Summary 5

1 **Research in Audit, Measurement, and Control** 5

1.1 System Identification 6

1.2 Fortigate-60 Risk Evaluation 8

1.3 Current State of Practice 10

2 **Audit Checklist** 12

2.1 Administrative Practices 12

2.2 Firewall Operating System Security 17

2.3 Firewall Device Physical Security 19

2.4 Firewall Device Maintenance Controls 21

2.5 Transport Layer Security 29

2.6 Application Layer Security 30

2.7 Intrusion Detection/Prevention Administration 32

2.8 Anti Virus Gateway Administration 34

3 **Audit Example** 36

3.2.2 Firewall Operating System Security 43

3.2.3 Firewall Device Physical Security 48

3.2.4 Firewall Device Maintenance Controls 50

3.2.5 Transport Layer Security 58

3.2.5 Transport Layer Security 61

3.2.7 Intrusion Detection/Prevention Administration 63

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

4 **Sample Audit Report** 67

4.1 Title Page 67

4.2 Table of Contents 68

4.3 Executive Summary 69

4.4 Key Findings and Recommendations 69

4.5 General Background 70

4.6 Detailed Findings and Recommendations 71

4.7 Objectives, Scope & Procedures Performed 72

4.8 Summary of Procedures Performed 73

Table of Figures

Figure 1 – Network Diagram for CBMW Bank 7

Figure 2 – IT Risk Assessment Form 9

Figure 3.1 – External Nessus scan results in html format 45

Figure 3.2 – Screenshot of Nessus plug-in configuration 47

Figure 3.3 – Server Room Entrance 49

Figure 3.4 – Cabinet housing firewall 49

Figure 3.5 – Screen capture of remote host logging screen 51

Figure 3.6 – Screen capture of network interface settings 52

Figure 3.7 – Screen capture of remote administration users screen 54

Figure 3.8 – Screenshot of Nmap run in Terminal on Fedora Core2 60

Figure 3.9 – Script Filter configured to block Java Applet and Active X scripts 62

Figure 3.10 – NIDS detection interface setup screen. (Properly configured) 64

Figure 3.11 – Screenshot of NIDS Prevention (Properly configured) 67

© SANS Institute 2005 Author retains full rights.

Table of Exhibits

Exhibit Q – Firewall Audit Questionnaire 36

Exhibit I – Information Request Items 41

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Assignment 1 – Research in Audit, Measurement, and Control

Abstract

One of the biggest "cyber-myths" out there today is the belief that technology will protect us. Firewalls, VPNs, Intrusion Detection Systems, virus software etc. do not, by their presence alone, protect us from attacks and exploits of system vulnerabilities. While the technology is vital to securing the data, it is simply a tool. Just because I own a hammer and saw does not make me a carpenter. I have to know the purpose and capabilities of each tool and have the skill to use them properly.

While a poor carpenter's work is often easily identifiable, poor implementation of technology can be more difficult to recognize. An IT auditor's job is to use their knowledge and skills to examine an organization's use of technology and ensure that each tool is being used properly to build a secure IT infrastructure. Whereas a building inspector would use local building codes and blueprints to ensure a building is safe and built to specifications, an IT auditor must use industry best practice standards and the organization's policies to determine if the use of technology is achieving the desired goals of securing the data.

This paper focuses on one financial organization's first line of defense in securing the data, the perimeter firewall. In this instance, the device to be audited is the Fortinet Fortigate-60 firewall. Fortinet products are not as well known as comparable Cisco products, but most of the Fortinet models incorporate Antivirus and Intrusion Detection utilities in addition to the firewall capabilities. Having all three features in one device is more cost effective but also increases the scope and complexity of the audit. Each function of the device must be tested to ensure that each is performing in accordance with industry best practice and the organization's information security goals set out in its policies.

The goal of this paper is to provide an IT auditor with the methodologies and knowledge necessary to audit and secure the Fortigate-60 firewall device. The paper is divided into 4 sections as follows:

- *Section one explores the current state of practice for securing the perimeter, as well as an assessment of risks associated with the device being audited.*

- *Section two contains a comprehensive and detailed checklist, which describes acceptable settings and methodologies to achieve compliance. The checklist defines the objective, non-compliance risk, expected findings and the detailed testing methodology for each area in the program.*

- *Section three selects 10 items from the above checklist as an example of how the entire audit should be conducted in practice.*

© SANS Institute 2005 Author retains full rights.

- *Section four contains the end result of any audit, the audit report. The audit report contains an "Executive Summary" of the scope of the audit along with "Key Findings" and a recommendation summary. The audit report is one of the most important and difficult components of an audit as the auditor is communicating technical concepts and concerns to an often times non-technical audience. Failure to communicate findings in an understandable manner can lead to the audit findings going unaddressed and an organization continuing to operate in an unsecured fashion.*

1.1 System Identification

The organization contracting for this audit is CBMW, a community bank with limited in-house technical resources. While substantial business is conducted through the use of technology, those responsible for managing the technology are largely third party service providers. The bank has outsourced their perimeter defense to a nationally known perimeter defense company, Secure Networks.

The Executive Vice President (EVP) of the bank requested an audit of the bank's network after he attended an IT Security presentation at a recent conference. He was concerned that the bank had no independent verification that Secure Networks was providing them with proper security devices and methodologies. The Chief Information Officer (CIO) requested that the initial scope of the audit focus on the perimeter firewall device, which is one of two firewalls employed by the bank. The CIO felt that since the device serves as a firewall, virus gateway and intrusion detection/prevention system (three very important security functions) he needed assurance all three were properly configured and functioning according to internal policy and industry best practices.

The Fortigate-60 firewall is the perimeter firewall located at the periphery of the bank's internal network. The bank utilizes a full T1 for Internet access and third party vendor transaction services. Cisco routers and switches provide connectivity and a standalone Cisco intrusion detection device resides outside the Fortigate-60 firewall. The Cisco IDS is positioned at the perimeter and therefore configured to be the least sensitive of the three IDS devices on the network. The Fortigate IDS is configured to look at both incoming and outgoing traffic for anomalies. In addition, the bank's informational/marketing website runs on an Apache web server which resides in the DMZ provided by the Fortigate-60 firewall.

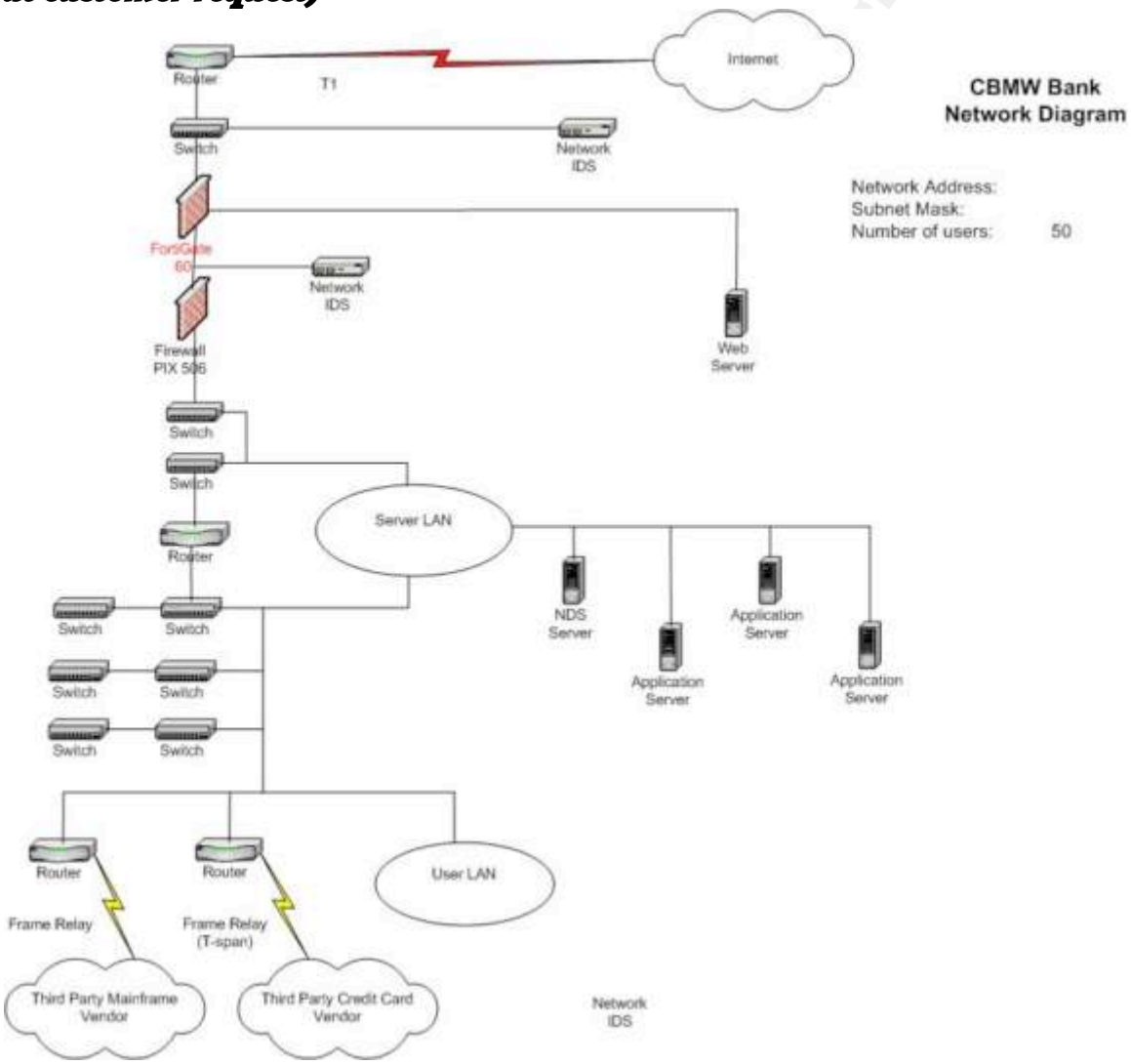
A second, non-redundant Pix 506 firewall for additional filtering and ingress/egress restrictions is attached to one internal port on the Fortigate-60. These devices protect three distinct LANs in the bank's network infrastructure. Each LAN is separate and unique in both architecture and purpose. The Server LAN houses the NDS server and three application servers. The User LAN facilitates the data connectivity for all internal users and contains the bank's Novell file server. The

© SANS Institute 2005 Author retains full rights.

*third LAN is an administration LAN that only select users with unique hardware configurations and network OS settings can access. (**See Figure 1**)*

E-mail is hosted by a third party vendor who utilizes F-Secure virus protection and content filtering before the mail contents reach the network users. Mail recipients use freely available third party e-mail software with additional filtering and junk mail control components.

Figure 1: Network Diagram for CBMW Bank (All IP addresses removed at customer request)



The bank relies on several third party vendors to conduct business and provide services. Internet access is vital for the bank to conduct their daily operational and customer service functions as set out below:

© SANS Institute 2005 Author retains full rights.

- *The bank relies on a VPN connection to their Internet Banking vendor for real time transactional services.*

- *Connection to real time credit card transactional data is vital for the Credit Card department to service customer accounts and handle customer service issues.*

- *Connection to the Federal Reserve is facilitated via secure token HTTPS sessions which is vital for wires and automated clearing house (ACH) activity.*

Bank staff must be able to quickly and securely access the Internet and also securely connect to several outside sites. Therefore the bank's firewall policies should describe the services and sites necessary for the bank's employees to operate. Likewise, the policy should also state which sites and services are not allowed. It is important that the policy explicitly state the firewall rules. Without these specific guidelines the bank increases the risk of the firewall restricting valid business functions or allowing unnecessary and possibly dangerous access to sites and services.

As mentioned earlier a third party perimeter defense company, Secure Networks (SN), manages the Fortigate-60 device. While all updates and changes to the device are strictly controlled by SN, a local bank administrator does have access to the HTTP administration interface for reporting and monitoring capabilities and in the event that SN cannot gain access remotely and emergency changes are necessary.

1.2 Fortigate-60 Risk Evaluation

Before conducting the audit a standard IT Risk Assessment form was used to evaluate the bank's overall IT Risk. While the overall risk assessment was valuable in allowing the CIO and Audit to gain a better understanding of the organization's risks as a whole, it also allowed us to assess the risks associated with the device being audited. Figure 2 on the next page is a screenshot of the section of the risk assessment dealing specifically with the Fortigate-60 device functions.

*This particular risk assessment deals specifically with **Inherent Risk**, or the risk of simply being in a business, in this case banking. **Residual Risk**, or the risk remaining after controls have been implemented will be evaluated during a later audit. Risk assessments assist management to identify the level of risk associated with each function and work to mitigate the risks identified. The end result of the risk assessment process is to identify areas where compensating controls can be implemented to lower the associated risk, as well as to monitor high risk areas where the risk remains high regardless of mitigating controls. Management should review those areas with high risk frequently to determine if new developments have emerged which could reduce the risk for the business function. The risk assessment*

© SANS Institute 2005 Author retains full rights.

performed ranked each of the functions, firewall, intrusion detection and anti-virus gateway on the low end of "Above Average Risk".

Figure 2: IT Risk Assessment Form

Significance Ranking - A measure of how important this item or area is to the bank. For example, an Information Security Policy may have increase in significance due to the privacy provisions of GLBA, combined with added emphasis on network and Internet security issues.

Risk Factor - A measure of how much related risk exists in your bank. For example, if your last regulatory examination contained exceptions related to the lack of an updated contingency plan then this area might carry a high risk factor. The fact that the plan is not up-to-date carries some risk, but the fact that is a repeat finding in your next examination, resulting in a poor rating could add to the risk.

IT RISK ASSESSMENT FORM

Orga: CBMW Bank
City, State

Information Technology Risk Assessment
Date 15-Aug-04

0.00 - 10.00	Low Risk
10.01 - 20.00	Below Average Risk
20.01 - 30.00	Average Risk
30.01 - 50.00	Above Average Risk
50.01 - 100.00	High Risk

Please enter a value in the applicable cells in Columns C and D.

Ref	Area	Significance Ranking .1 (Low) to 1.0 (High)	Risk Factor 0 (Low) to 100 (High)	Risk Rating	Risk Category
Firewall					
1	Lack of or poor policies	0.6	60	36.00	Above Average Risk
2	Lack of or poor change control	0.6	50	30.00	Average Risk
3	Unecessary services running	0.7	40	28.00	Average Risk
4	Firewall OS/Firmware not kept up to date	0.7	40	28.00	Average Risk
5	Firewall located in unsecured area	0.8	60	48.00	Above Average Risk
6	Lack of environmental controls for firewall	0.8	60	48.00	Above Average Risk
7	No system or event logging	0.8	70	56.00	High Risk
8	Unecessary administrative accounts on firewall	0.6	50	30.00	Average Risk
9	Poor encryption and security for remote admin.	0.7	50	35.00	Above Average Risk
10	Lack of or poor backup procedures	0.7	50	35.00	Above Average Risk
11	Lack of or poor testing of backups	0.6	50	30.00	Average Risk
12	Default user name and passwords not changed	0.5	50	25.00	Average Risk
13	Unecessary ports open on device	0.8	40	32.00	Above Average Risk
14	Lack of stateful inspection	0.8	50	40.00	Above Average Risk
15	Absence of "close on failure" feature	0.6	50	30.00	Average Risk
		Overall Firewall Risk		**35.79**	**Above Average Risk**
Intrusion Detection					
1	Lack of or poor policies	0.6	60	36.00	Above Average Risk
2	Lack of or poor change control	0.6	50	30.00	Average Risk
3	Lack of or poor event logging	0.8	60	48.00	Above Average Risk
4	Logs left unsecured	0.6	60	36.00	Above Average Risk
5	Lack or poor incident response	0.8	50	40.00	Above Average Risk
6	Lack of or poor reporting capabilities	0.5	40	20.00	Below Average Risk
7	IDS OS/Firmware not kept up to date	0.6	50	30.00	Average Risk
8	IDS located in unsecured area	0.8	60	48.00	Above Average Risk
9	Lack of environmental controls for IDS	0.8	60	48.00	Above Average Risk
10	Unecessary ports open on device	0.8	40	32.00	Above Average Risk
		Overall IDS Risk		**36.80**	**Above Average Risk**
Anti-Virus Gateway					
1	Lack of or poor policies	0.6	60	36.00	Above Average Risk
2	Failure to update virus definitions	0.8	60	48.00	Above Average Risk
3	Misconfigured virus gateway settings	0.6	50	30.00	Average Risk
4	Failure to detect new viruses	0.8	40	32.00	Above Average Risk
5	Lack of or poor gateway event monitoring	0.6	50	30.00	Average Risk
		Overall Anti-Virus Risk		**35.20**	**Above Average Risk**

specifically for the Fortinet line of products. Fortinet technical support is for

© SANS Institute 2005 Author retains full rights.

registered users only so beyond technical specifications there was not much useful information on their site. There were, however, several best practice resources for firewalls, intrusion detection systems and anti-virus gateways but nothing that addressed a device that included all three. It would be easy to assume that you could apply the best practices for each separate device type and build a suitable audit checklist. However, a "generic" audit program does not work for devices made by different vendors as the program would not address items specific to each device.

To gain more knowledge of the product itself, I contacted the local administrator and obtained the User Guide on CD-ROM. The CD-ROM contained indexed PDF documents making it simple to find and print the pertinent sections and begin to gain an understanding of the administration of the device, as well as the areas I needed to check to insure the device had been configured correctly. In addition, I was able to create an "Item Request List" which included step-by-step instructions for the local administrator to retrieve the information requested. This should help to avoid delays in the audit once we arrive on site.

In addition to device specific information I used the Internet to research industry standards to determine best practice for each of the three functions of the device. Several of these sites were found from reading the practicals of other SANS students in the "reading room" at http://www.sans.org/rr/. A few of the more informative sites found were:

S.C.O.R.E. http://www.sans.org/score/
Great resource for checklists, benchmarking tools, incident response forms and general security related FAQs. One great resource is the "Firewall Checklist" by Krishni Naidu.

Itsecurity.com http://www.itsecurity.com/
Contains some great whitepapers and best practice documentation for several security related areas.

Auditnet http://www.auditnet.org
Has an impressive amount of checklists and workprograms available for just about anything you can audit.

Knowledgeleader http://www.knowledgeleader.com
A membership resource with fees attached but they do give a free 30 day trial. Has some very professional resources for checklists, work programs and audit theory.

CERT http://www.cert.org
A good general information site with a really useful site index that lets you get right to the areas you are interested in.

© SANS Institute 2005 Author retains full rights.

There were also several good books that I was able to skim through and pull relevant information and useful items I included in the audit checklist. A full list of all resources used in developing the Fortinet-60 audit program can be found in the bibliography located at the end of this report.

© SANS Institute 2005, Author retains full rights.

Assignment 2 – Audit Checklist

2.1 Administrative Practices

© SANS Institute 2005 Author retains full rights.

Audit Step	2.1.1
Reference	"IT Auditing for Financial Institutions" Jimmy R. Sawyers Vol. 1
Control Objective	Establish if a General Security Policy that provides management and staff with guidance and direction for the organization's security goals exists.
Non Compliance Risk	Without clearly defined organizational security goals, security is left up to the individuals in the organization to define. These individual definitions may not be in line with the organization's overall security goals.
Compliance	A general Security Policy should exist
Testing	• From questionnaire determine if a General Security Policy exists. If so request a copy of the policy and review it to determine if the organization's security goals are clearly defined. • Interview the IT Manager and Systems Administrator to determine if they are aware of and familiar with the policy and it's goals. • Determine if employees are required to sign an acknowledgement that they have read and understand the policy.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.1.2

© SANS Institute 2005 Author retains full rights.

Reference	"IT Auditing for Financial Institutions" Jimmy R. Sawyers Vol. 1
Control Objective	Establish if a Firewall Policy that provides IT Management and staff with guidance and direction for the organization's security goals with regards to the Firewall exists.
Non Compliance Risk	Without clearly defined procedures for configuration, logging, change control, remote access, physical access, and patch management the organization risks having a Firewall in place that does not protect the organization in the manner that is required.
Compliance	A Firewall Policy outlining the manner in which the Firewall will be configured should exist.
Testing	• From questionnaire determine if a Firewall Policy exists. If so request a copy of the policy and review it to determine if it clearly defines the manner in which the Firewall will be configured. • Interview the IT Manager and Systems Administrator to determine if they are aware of and familiar with the policy and it's goals. • Obtain a copy of the Firewall configuration file to see if the configuration is in compliance with the Firewall Policy.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.1.3
Reference	"IT Auditing for Financial Institutions" Jimmy R. Sawyers Vol. 1

© SANS Institute 2005 Author retains full rights.

Control Objective	Establish if a Network Acceptable Use Policy that provides Management and staff with guidance and direction for the organization's security goals with regards to the network exists.
Non Compliance Risk	Without clearly defined policies for use of the network the organization cannot develop standardized policies regarding configuration of the firewall device in line with what is and is not acceptable use of the network.
Compliance	A Network Acceptable Use Policy outlining the manner in which the network should and should not be used exists.
Testing	• From questionnaire determine if a Network Acceptable Use Policy exists. If so request a copy of the policy and review it to determine if it clearly defines the manner in which the network should and should not be used. • Interview selected personnel to determine if they are aware of and familiar with the policy and it's goals. • Obtain a copy of the Firewall configuration file and compare it to the Network Acceptable Use Policy for compliance.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.1.4

© SANS Institute 2005 Author retains full rights.

Reference	"IT Auditing for Financial Institutions" Jimmy R. Sawyers Vol. 1
Control Objective	Establish if an Internet Usage Policy exists that provides management and staff with guidance and direction for the organization's security goals related to it's Internet connectivity.
Non Compliance Risk	Without clearly defined policies for use of the Internet, the organization cannot develop standardized policies regarding configuration of the firewall device in line with what is and is not acceptable use of the Internet.
Compliance	An Internet Usage Policy outlining the manner in which the network should and should not be used should exist.
Testing	• From questionnaire determine if an Internet Usage Policy exists. If so request a copy of the policy and review it to determine if it clearly defines what is and is not acceptable use of the Internet. • Interview selected personnel to determine if they are aware of and familiar with the policy and it's goals. • Obtain a copy of the Firewall configuration file. Visually inspect to see if the configuration is in compliance with the Internet Usage Policy.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.1.5

© SANS Institute 2005 Author retains full rights.

Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure the Firewall is covered by Change Control standards.
Non Compliance Risk	Changes to the Firewall that do not follow Change Control standards can result in security breaches and system failures due to mismanagement of rulesets and policies that can contradict each other and the overall goal of the Firewall device.
Compliance	Change Control standards exist.
Testing	• From questionnaire determine if Change Control standards exist. • Determine if the standards are documented. • If so request a copy of the standards and review them to determine if they clearly define the manner in which Change Control is managed.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	
Exceptions	

2.2 Firewall Operating System Security

© SANS Institute 2005 Author retains full rights.

Audit Step	2.2.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure only services required to meet business requirements are running on the system
Non Compliance Risk	Unnecessary services could allow intruders to gather information about the system or even facilitate an attack on the system.
Compliance	Only necessary services are running on the system.
Testing	• Obtain a copy of the Firewall Policy to determine what services should be enabled on the firewall. • Obtain a copy of the configuration file for the system to determine which services are enabled. Compare this to the allowed services stated in the Firewall Policy. • Using Nmap, and Nessus scan the system to determine which ports are listening and what services are running on those ports. If any ports or services other than those listed in the Firewall Policy and configuration file are running, then further attention should be given to whether the system is misconfigured or if in fact the system has been compromised.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	

© SANS Institute 2005 Author retains full rights.

Exceptions	

Audit Step	2.2.2
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure the OS is updated and patched to the latest stable version.
Non Compliance Risk	Failure to keep the OS updated and patched can leave the OS vulnerable to known security vulnerabilities. Out of date systems are open to attack and compromise of the internal network.
Compliance	The OS is updated to the most current stable version
Testing	• Have System Administrator log in to the web interface. Choose System > Status and choose the status tab. Note the firmware version . • Due to Fortinet's subscription support system the firmware version is not publicly available. Have the System Administrator log in to the Fortinet support site and provide a printout or screen capture of what the firmware version should be. • Compare the version numbers. If the system is not up to date determine through discussion with management and the System Administrator if there is a valid reason for the system not being updated.
Test Type	Objective/Subjective

© SANS Institute 2005 Author retains full rights.

Supporting Documentation	
Test Results	
Exceptions	

2.3 Firewall Device Physical Security

Audit Step	2.3.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Personal experience.
Control Objective	Firewall device physical location should be a secure area such as a combination or key card access data center or a locked server rack or cabinet.
Non Compliance Risk	Lack of adequate physical security for the firewall device could result in unauthorized changes to the configuration such as creation of back doors or intentional misconfiguration of features such as IDS or Anti-Virus.
Compliance	The firewall device resides in a restricted access data center or in a locked server rack or cabinet. Ideally both a restricted access data center and a locked server rack or cabinet would be utilized.
Testing	• Ask to be shown the device and note the location and security measures in place at the location. • If a secure location exists document the procedures for entry and exit from the location. • If server rack or cabinet is used note if a lock is present and in use.

© SANS Institute 2005 Author retains full rights.

	• If server rack or cabinet lock is used determine who has keys to locks.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.3.2
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com
Control Objective	Ensure the firewall is located in an area with environmental controls that promote reliable operation.
Non Compliance Risk	Lack of or improper environmental controls could contribute to the likelihood of failure of the device due to extremes in heat, moisture and airborne contaminants.
Compliance	The device is located in an area with proper environmental controls that protect it from extreme temperatures, humidity and airborne contaminants.
Testing	Examine the area where the device is located. • Are the air conditioning and humidity control systems for the area adequate to maintain temperatures within manufacturers' specifications? • Is the area kept free of dust, smoke, and other particulate matter, i.e., food? • Do fire and water detection devices that sound audible alarms protect the area?
Test Type	Objective/Subjective
Supporting Documentation	

© SANS Institute 2005 Author retains full rights.

Test Results	
Exceptions	

2.4 Firewall Device Maintenance Controls

Audit Step	2.4.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com "Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000. Fortigate-60 Documentation "Logging and Reporting"
Control Objective	Ensure system logging is enabled and the logs are stored in a secure fashion.
Non Compliance Risk	Not logging activities that pass through the firewall can result in the inability to detect intrusion attempts and can hinder or defeat forensic analysis of an intrusion event. Secure storage of logs prevents intruders from accessing and possibly altering the logs to hide evidence of their intrusion.
Compliance	Logging is enabled and the logs are stored in a secure fashion, preferably on a remote syslog server.
Testing	• Have System Administrator log in to the web interface. • Choose System>Network>Interface Select edit in the modify column beside the active interfaces (NIC) and ensure the "Log" setting is set to "Enable" for each. • Choose Log & Report > Log Setting.Verify that the "Log to

© SANS Institute 2005 Author retains full rights.

	Remote Host" box is checked and that a valid remote IP and Port number are entered.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.4.2
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Minimize the number of administrative accounts on the Firewall.
Non Compliance Risk	Lack of control of the number and type of administrative accounts on a firewall can lead to unmanageable change control and could result in confusion as to the level of security the Firewall affords and inconsistent rules for access.
Compliance	The number of administrative accounts is kept to a necessary minimum.
Testing	• From the Administration interface Go to System > Config and then click on the Admin tab. Capture a screenshot or printout of the settings. • Through interview with the local System Administrator establish the purpose of each account.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005 Author retains full rights.

Audit Step	2.4.3
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com
Control Objective	Remote administration conducted through appropriate vendor software, encryption and security methodology
Non Compliance Risk	The use of inappropriate software, encryption and security methodology (such as the use of Telnet, which broadcasts information "in the clear", lack of encryption for sessions and not logging sessions) for remote administration can allow intruders to obtain user names and passwords and other sensitive information that can grant them access to the firewall and system.
Compliance	Remote administration conducted through SSH or 128-bit Encrypted HTTPS and restricted by IP address
Testing	• From questionnaire determine if logical access to the firewall is restricted and if so how. • From questionnaire determine if remote administration is allowed. • From questionnaire determine what protocol is used for remote administration. • From questionnaire determine if there are written procedures and security guidelines in place. Obtain a copy of the procedures and guidelines and review.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005 Author retains full rights.

Audit Step	2.4.4
Reference	NIST "Guide to Firewall Selection and Policy Recommendations" John Wack, Ken Cutler, Jamie Pole
Control Objective	Determine if remote access sessions are logged.
Non Compliance Risk	Failure to log remote access sessions can result in undetected security breaches and poor change control.
Compliance	Remote access sessions are logged and the logs are stored securely
Testing	• From questionnaire determine if remote access sessions are logged. • Obtain a copy of the remote access log. Determine if the log notes: 1. Date and time of the remote session 2. User name 3. Source IP of the remote session
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.4.5
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com NIST "Guide to Firewall Selection and Policy Recommendations" John Wack, Ken Cutler, Jamie Pole Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure the Firewall has a documented backup procedure. Verify that backups and restoration procedures are tested

© SANS Institute 2005 Author retains full rights.

	and verified to insure they are viable
Non Compliance Risk	Failure to properly backup the firewall could result in the loss of configuration information as well as system and security log files. Failure to test backups can result in loss of configuration information, extended down time and risk of improper configuration when recovering from a device failure.
Compliance	Documented backup procedures exist and are followed. Backups are tested in a manner that ensures full system restoration can be completed in the event of device failure.
Testing	• From questionnaire determine if the Firewall is backed up and who is responsible for the backup procedures. • Request copies of the backup procedures. • Request backup testing procedures. • Request documentation of last backup test results.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Audit Step	2.4.6
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Personal experience. Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure default username and passwords have been changed
Non Compliance Risk	Failure to change default settings allows intruders easy access to devices and networks due to the easily attainable and widely known default user names and passwords for many popular devices.
Compliance	Default user name and password have been changed
Testing	▪ Obtain the default user name and password from the Firewall documentation. Observe local administrator attempt to gain access to the system via the web interface with this information.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.4.7
Reference	NIST "Guide to Firewall Selection and Policy Recommendations" John Wack, Ken Cutler, Jamie Pole Personal experience Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure that logical access is restricted to a designated local management workstation and that the workstation is physically secure
Non Compliance Risk	Unrestricted logical access could allow

© SANS Institute 2005 Author retains full rights.

	unauthorized remote access sessions from unsecured workstations. If the workstation is unsecured access could be gained by unauthorized personnel.
Compliance	Logical access should be restricted via IP address. The management workstation should be secured with password protection and not publicly accessible
Testing	• From questionnaire determine if logical access is restricted by IP address. • Have local administrator log in to the web administration interface Go to System > Config and then click on the Admin tab. Capture a screenshot or printout of the settings. • Note the location of the workstation the administrator logs into the web interface on. 1. Is the workstation in a publicly accessible area? 2. Is the workstation protected by a user name and password? 3. Does the workstation automatically log the user out after a specified period of inactivity?
Test Type	
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Audit Step	2.4.8
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure that the device is configured to stop all access if the device fails (close on failure)
Non Compliance Risk	If the device is not configured to stop traffic in the event of system or hardware failure there is the risk the device could stop working and go unnoticed. This would result in the organization going unprotected unknowingly.
Compliance	The device is configured to stop all traffic in the event of failure.
Testing	• From questionnaire determine if the device is capable of close on failure and if it is configured to do so. • Request documentation from the manufacturer or perimeter defense vendor.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

2.5 Transport Layer Security

© SANS Institute 2005 Author retains full rights.

Audit Step	2.5.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com "Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000.
Control Objective	Ensure only ports required to meet business requirements are open on the system
Non Compliance Risk	Unnecessary open ports could allow intruders to gather information about the system or even facilitate an attack on the system.
Compliance	Only necessary ports are open on the system.
Testing	• Obtain a copy of the Firewall Policy to determine what ports should be enabled on the firewall. • Obtain a copy of the configuration file for the system to determine which ports are enabled. Compare this to the allowed ports stated in the Firewall Policy. • Using Nmap, and Nessus scan the system to determine which ports are listening. If any ports other than those listed in the Firewall Policy and configuration file are running further attention should be given to whether the system is misconfigured or if in fact the system has been compromised.
Test Type	Objective/Subjective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

2.6 Application Layer Security

Audit Step	2.6.1
Reference	"Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000. Personal experience Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure that the firewall is using inbound filtering and only the application proxy services allowed by the firewall policy are running on the device.
Non Compliance Risk	If the firewall does not perform inbound filtering or allows unnecessary application proxy services, unnecessary or intentionally malformed packets may be introduced to the network.
Compliance	Inbound filtering is being used and only those application proxy services stated in the firewall policy are running on the device.
Testing	• Determine which application proxy services are allowed according to the firewall policy. • Compare the services allowed in the policy to the services that are allowed by inbound filtering on the firewall. Have the local administrator log on using the web interface. Go to Web Filter > Script Filter to determine what services are allowed.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005 Author retains full rights.

Audit Step	2.6.2
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com "Firewall Checklist" Krishni Naidu http://www.sans.org/score/firewallchecklist.php Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure that the device is using stateful inspection and closing ports to unsolicited traffic.
Non Compliance Risk	If the device is not using stateful inspection the device is not examining data at the application level and ports may be left open to unsolicited traffic.
Compliance	The device is using stateful inspection to track each connection traversing all interfaces of the firewall and makes sure they are valid.
Testing	• From questionnaire determine if the device is using stateful inspection. • Request documentation from the manufacturer or perimeter defense vendor verifying the device uses stateful inspection.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

2.7 Intrusion Detection/Prevention Administration

Audit Step	2.7.1
Reference	Personal experience Fortigate-60 Documentation "Network Intrusion Detection System (NIDS)"
Control Objective	Ensure that the intrusion detection feature is enabled and the proper interfaces are being monitored by the IDS.
Non Compliance Risk	From the Fortigate-60 user guide it was stated that the intrusion detection feature is on by default but can be disabled. It is important to verify that this feature is enabled and that the proper interfaces to the network are being monitored.
Compliance	The intrusion detection feature is enabled on the device.
Testing	• Have the local administrator log on to the web interface. Go to NIDS > Detection > General tab. Ensure that at least one interface is checked. If no interfaces are checked the IDS function is not enabled. • Through interview establish which interfaces should be enabled. Ensure that these interfaces are in fact checked and active in the NIDS > Detection > General tab.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Audit Step	2.7.2
Reference	Personal experience Fortigate-60 Documentation "Network Intrusion Detection System (NIDS)"
Control Objective	Ensure that the attack signatures feature is enabled on the IDS.
Non Compliance Risk	From the Fortigate-60 user guide it was stated that the NIDS attack signatures feature is on by default but can be disabled. It is important to verify that this feature is enabled.
Compliance	NIDS attack signatures are enabled.
Testing	• Have the local administrator log on to the web interface. Go to NIDS > Detection > Signature List tab. By default all signatures are checked and should be left so. If there are any signatures not checked establish if there are valid business reasons for them to be turned off.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

Audit Step	2.7.3
Reference	Personal experience Fortigate-60 Documentation "Network Intrusion Detection System (NIDS)"
Control Objective	Ensure that the NIDS attack prevention feature is enabled.
Non Compliance Risk	From the Fortigate-60 user guide it was stated that the NIDS attack prevention feature is disabled by default and that it is automatically disabled after a reboot or power loss. It is important to verify that this feature is enabled.

© SANS Institute 2005 Author retains full rights.

Compliance	The attack prevention feature is enabled.
Testing	• Have the local administrator log on to the web interface. Go to NIDS > Prevention. Ensure that the "Enable Prevention" in the upper left corner is checked.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

2.8 Anti-Virus Gateway Administration

Audit Step	2.8.1
Reference	Personal experience Fortigate-60 Documentation "Virus and attack definitions updates and registration"
Control Objective	Ensure that the antivirus and attack definitions are updated on a scheduled basis.
Non Compliance Risk	Out of date antivirus and attack definitions can expose the network to known viruses and attacks. Ensuring that a schedule is in place to automatically or manually update the definitions is vital to protecting the network from worms and viruses.
Compliance	The antivirus feature is configured to connect to the FortiResponse Distribution Network (FDN) and update the antivirus and attack definitions on a regularly scheduled basis
Testing	• Have the local administrator log on to the web interface. Got to System > Update. Review the

© SANS Institute 2005 Author retains full rights.

	settings to determine if, and how often, automatic definition updates are scheduled to occur. • Have the local administrator log on to the web interface. Go to System > Update. Review the Last Update Attempt and Last Update Status fields to determine when the definitions were last updated and if the update was successful.
Test Type	Objective
Supporting Documentation	
Test Results	
Exceptions	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Assignment 3 – Audit Example

Initial steps:

A brief pre-audit questionnaire was sent to the bank's CIO in order to gain a better understanding of the organization's policies, procedures, and knowledge regarding the Foritigate-60 firewall. The answers were discussed with the CIO and local administrator once audit arrived on site to ensure that the questions were understood and the answers were correct to the best of their knowledge. (**See Exhibit Q below**)

Exhibit Q: Firewall Audit Questionnaire

Please fill out a questionnaire for each firewall in place in the organization

Organization: CBMW Bank

Questionnaire completed by: CIO

Firewall type: Fortinet Fortigate-60

Internal designation: Fortigate 60

Question	***Response***
1) Does the organization maintain a general security policy? a) If yes, who is in charge of keeping the policy up to date? b) If yes, how often is the policy updated?	No, In process of creating with third party vendor
2) Does the organization maintain a firewall security policy? a) If yes, who is in charge of keeping the policy up to date? b) If yes, how often is the policy updated?	No.

© SANS Institute 2005 Author retains full rights.

3) Does an outside vendor manage or consult on configuration of the firewall? a) If yes, are there written agreements and procedures in place regarding the configuration of the firewall and its intended functions? b) If yes, are there written procedures in place for firewall configuration change management? c) If yes, how is the vendor notified of internal changes to network configuration or hardware changes that may affect the firewall's functions?	Yes Yes. Procedures and agreements but no procedures for configuration or intended functions. Yes. The Perimeter defense vendor has policies and procedures for testing and change management. Incident response form and e-mail change request forms.
4) Who is in charge of firewall log monitoring and management?	Perimeter Defense vendor Secure Networks (SN).
5) Are the firewall logs reviewed manually or is a diagnostic program used?	SN uses both methods to insure accuracy and minimal false positives.
6) Where are firewall logs stored?	SN stores logs on a remote server which is backed up daily. A local copy is also kept for redundancy.
7) How long are logs archived?	According to Service Level Agreements in Perpetuity
8) How is management notified of possible incidents with regards to the firewall?	Phone calls followed by e-mails.
9) Is the firewall configured with separate switches on each interface or are both interfaces on the same switch?	A secondary firewall is connected via twisted cable to the second interface.
10) Is the firewall configured to stop all	Yes per Fortinet and SN

© SANS Institute 2005 Author retains full rights.

access if the device fails (close on failure)?	
11) Is physical access to the firewall restricted and if so how?	Concentric locks on outer and inner doors and device resides in a locked cabinet.
12) Is logical access to the firewall restricted and if so how?	Restricted access via HTTPS and SSH further restricted by IP address.
13) Is remote access allowed to the firewall? a) If yes, what protocol is used? b) If yes, who is allowed remote access? c) If yes, are remote access sessions logged? d) If yes, are written procedures and security guidelines in place?	Yes. HTTPS, SSH Local admin and vendor restricted by IP address. Yes. (log requested and reviewed by Audit) Yes. SN has written procedures. (Requested and reviewed by Audit)
14) Does the firewall employ "Stateful" or "Static" filtering?	Both. Stateful through use of NAT and static through use of software.
15) Are all non-essential services disabled on the firewall?	Yes.
16) Does the device have an IDS function? a) If yes, who is in charge of monitoring the IDS function? b) If yes, how is management notified in the event of an IDS alert?	Yes. SN Phone call followed by e-mail
17) Are the firewall settings backed up in the event of device failure? a) If yes, how often? b) If yes, who is responsible for	Yes. After every change and every 30 days. SN

© SANS Institute 2005 Author retains full rights.

the backups? c) If yes, where are the backups stored?	 Same process as firewall logs above.
18) Does the organization have a DMZ? a) If yes, what devices reside in the DMZ? b) If yes, what types of traffic are allowed and how are restrictions managed?	Yes. Web server and two training PCs. Web – Port 80 and 443 (SSL) Internal – SSH, FTP **to** DMZ nothing allowed **from** DMZ.
19) Is a backup firewall in place? a) If yes, is the backup configured to be a failover device? b) If yes is it the same model as the primary device?	No. A secondary device is available but is not the same type and is not configured for failover or backup.
20) Does the firewall allow VPN connections? a) If yes, is a VPN utilized? b) If a VPN is utilized, are there security policies and procedures for VPN users to follow? c) If VPN is utilized, are VPN sessions logged?	Yes. No.
21) Does the firewall have anti-virus features? a) If yes, how are the virus definitions kept up to date? b) If yes, who is in charge of	Yes. Automatic update. SN

© SANS Institute 2005 Author retains full rights.

insuring the virus definitions are up to date?	
c) If yes, how often are the virus definition updated?	Weekly

After analyzing the answers to the questionnaire two initial areas of interest were found. Most notably no policies with regard to the firewall are exist. This will make several of the audit steps in our checklist more difficult as we are attempting to audit the device for compliance with the bank's policies. The other item to note is the use of a third party vendor for configuration and management of the device. The bank is relying on the vendor to certify the device is configured and functioning properly, however the vendor has no guidance from the bank as to how the device should be configured and what functions the device should be performing.

During the audit these questionnaire findings were discussed with the CIO. It appears that the CIO and local administrator are familiar with the perimeter defense vendor's practices and procedures and they have some degree of confidence in the vendor's expertise.

Scope Expansion:

While discussing the steps of the audit with the CIO it was decided that since an external scan of the device was already planned, the scope of the audit would be expanded to include response time of the vendor, Secure Networks, to an external "aggressive" scan against the bank's perimeter firewall. While incidence response procedures were in place with regards to what constituted an incident, who should be contacted and what methods of contact should be used, no real test of the monitoring service has been conducted.

Addendum to Information Request:

Due to the expanded scope of the audit the original Item Request List was modified to include requests for information from the perimeter defense vendor. Secure Networks (SN) after an external scan of the device *.

Exhibit I: Information Request Items

© SANS Institute 2005 Author retains full rights.

Pertaining to the Audit of the Fortinet Fortigate-60 Firewall

Required Before commencement of Audit

Any policies pertaining to security and firewall standards including Acceptable Use Policy.

Network Diagram (including all IDS and Firewall units and IP addresses)

Fortigate-60 Configuration in print and electronic format. (Analogous to the "Show Config" command on a Cisco Pix)

Fortigate-60 NIDS signature list (From web interface Go to NIDS>Detection>Signature List. Select View Details) in print and electronic format.

Fortigate-60 URL block list (From web interface Go to Web Filter>URL Block. Select Download URL Block List) in print and electronic format.

Fortigate-60 Script Filtering list if Script Filtering is enabled. (From web interface Go to Web Filter> Script Filter) in print and electronic format.

Fortigate-60 Exempt URL list if URL Exemption is enabled. (From web interface Go to Web Filter>Exempt URL) in print and electronic format.

Fortigate-60 Log Settings (From web interface Go to Log&Report>Log Setting) in print and electronic format.

Fortigate-60 NIDS Alert E-mail configuration (From web interface Go to Log&Report>Alert Mail> Configuration) in print and electronic format.

Fortigate-60 List of users and users with Admin rights.

Screen shot of Firewall Banner in print and electronic format.

Required after** Internal Scan **of Firewall

Fortigate-60 NIDS logs for one half hour before and after scan

Fortigate-60 Firewall logs for one half hour before and after scan

IDS logs from Locally managed Internal IDS system(s)

© SANS Institute 2005 Author retains full rights.

* Required after **External Scan** of Firewall:

Fortigate-60 NIDS logs from 24 hours prior to scan thru 12 hours after the scan.

Fortigate-60 Firewall logs from 24 hours prior to scan thru 12 hours after the scan.

Notation of time between commencement of scan and notification from Perimeter Defense Vendor.

Copy of incident report from Perimeter Defense Vendor.

Tools Used:

Hardware:

IBM R50 Laptop with Windows XP/Fedora Core2 dual boot

Software:

***Nessus* – From http://www.nessus.org**

Nessus is a full feature security scanner, which remotely audits an entire network or a single device and through use of Nessus Attack Scripting Language (NASL) runs multiple tests to detect both remote flaws as well as local flaws. Nessus incorporates the functionality of Nmap's TCP scanning techniques, along with NIDS evasion, URL encoding, SSL based services testing and Brute force logins for most available services. Nessus is a freely available open source utility that runs on Linux and Unix. A windows based client version is available but still relies on having a Linux or Unix installation running as the server for the client.

Nmap – From http://www.insecure.org/nmap/

"Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics."

Audit Step Examples:

© SANS Institute 2005 Author retains full rights.

Ten audit steps were taken from the checklist in section 2 to demonstrate how an actual audit of the Fortigate-60 device should be conducted.

For each audit step, results from the Testing section will be summarized in the Test Results section of the table. Below each audit step table, details of the procedures, tools used, screen captures and any photographic evidence found is displayed to help the reader understand what is necessary for the successful completion of each audit step.

3.2.2 *Firewall Operating System Security*

Audit Step	3.2.2.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure only services required to meet business requirements are running on the system
Non Compliance Risk	Unnecessary services could allow intruders to gather information about the system or even facilitate an attack on the system.
Compliance	Only necessary services are running on the system.
Testing	• Obtain a copy of the Firewall Policy to determine what services should be enabled on the firewall. • Obtain a copy of the configuration file for the system to determine which services are enabled. Compare this to the allowed services stated in the Firewall Policy. • Using Nessus, run an external scan on the device to determine which ports are listening and

© SANS Institute 2005 Author retains full rights.

	what services are running on those ports. If any services other than those listed in the Firewall Policy and configuration file are running further attention should be given to whether the system is misconfigured or if in fact the system has been compromised.
Test Type	Objective – Stimulus/Response
Supporting Documentation	Q2
Test Results	Through use of the questionnaire it was determined that a Firewall Policy does not exist. Since no Firewall Policy currently exists there is not an opportunity to assess whether the Firewall configuration is in compliance with the policy. Analysis of the firewall configuration showed that SSH, HTTPS, TCP and UDP were the only services that are configured to be running on the device. An external Nessus scan proved inconclusive due to the bank's use of NAT Overloading or Port Address Translation (PAT). (See **Figure 3.1**) An internal scan of the device confirmed that SSH v. 2.0 and HTTPS, TCP and UDP were the only services running on the system.
Exceptions	Exceptions noted: No firewall policy in place.

Figure 3.1 External Nessus scan results in html format.

© SANS Institute 2005 Author retains full rights.

An external “aggressive” Nessus scan was run after business hours. Due to the expanded scope of the audit this scan has two objectives:

- Confirm which services are running on the device.
- Test the response time and incident handling procedures of the perimeter defense vendor Secure Networks (SN).

External Nessus Scan Detail:

The html-formatted results of the external scan included over 40 pages of apparent open ports and running services. (See **Figure 3.1**) A second scan gave similar but slightly different results.

Further investigation and discussion with the local administrator led to the discovery that the bank utilizes NAT Overloading or Port Address Translation (PAT).

© SANS Institute 2005 Author retains full rights.

PAT allows an organization to use non-routable internal IP addresses that are then mapped to a range of unique routable IP addresses through an address translation table on a NAT enabled router. The router replaces the sending computer's non-routable IP address with the router's IP address. The router replaces the sending computer's source port with the port number that matches where the router saved the sending computer's information in the translation table. The table now contains a mapping of the computer's non-routable IP address and port number, matched to the router's IP address.

When the packet returns from the destination computer it is checked against the translation table to determine which computer on the internal network the packet belongs to. The router then changes the destination address and port to the one that was saved in the translation table and sends it to the appropriate internal computer. If no match is found the packet is dropped.

With this information in mind it was decided that an external scan of the device had to pass through the router and the information returned could not be relied on.

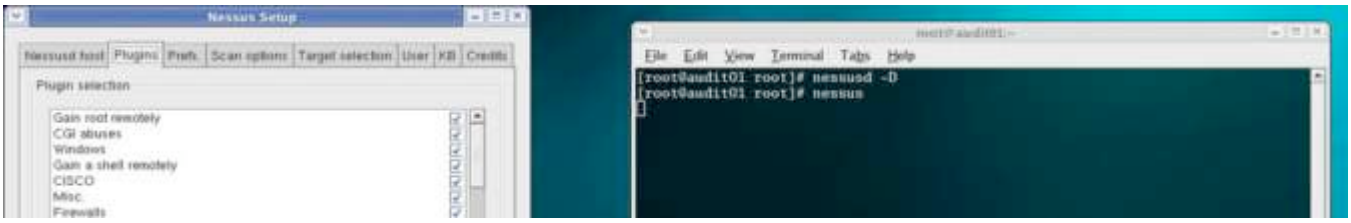
Scope Expansion Detail:

The secondary objective of the Nessus scan was to determine SN's response time to the aggressive scan of the Bank's perimeter. The audit laptop was booted into Fedora Core2 and a terminal window brought up. Nessus was activated using the following commands:

```
# nessusd -D        [This command activates the Nessus daemon]
# nessus            [This command activates the Nessus GUI]
```

Nessus is highly configurable with regards to how it scans a device or network. Using the plug-ins tab you can either configure each plug-in to run or not run, or choose either the "Enable all but dangerous plug-ins" or "Enable all" buttons (See **Figure 3.2**). For this scan, with the CIO's permission, audit enabled all of the available plug-ins.

Figure 3.2 Screenshot of Nessus plug-in configuration



© SANS Institute 2005 Author retains full rights.

SN was not notified of the scan for obvious reasons. The start time of the first scan was noted, as was the time of completion. The local administrator was the primary point of contact for any incident reporting. No notification from SN was received, even after a second scan was completed. SN was contacted the following day but had no record of any scans run against the device. The CIO will follow up with the vendor to determine if they are receiving the service they are contracting for from the perimeter defense vendor.

Addendum:

The following morning bank personnel were unable to access the Internet. After working with the Internet Service Provider and SN it was determined the bank's router was "frozen". The router was rebooted and Internet access was restored. Further tests by the local administrator and SN proved that the router was vulnerable to Denial of Service (DoS) attacks, which are part of the Nessus aggressive scan settings. This was due primarily to the bank's use of PAT, which utilizes a high amount of DRAM on the router. A patch for the vulnerability was requested from the router vendor however at the time of the audit no patch was available.

3.2.3 Firewall Device Physical Security

© SANS Institute 2005 Author retains full rights.

Audit Step	3.2.3.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Personal experience.
Control Objective	Firewall device physical location should be a secure area such as a combination or key card access data center or a locked server rack or cabinet.
Non Compliance Risk	Lack of adequate physical security for the firewall device could result in unauthorized changes to the configuration such as creation of back doors or intentional misconfiguration of features such as IDS or Anti-Virus.
Compliance	The firewall device resides in a restricted access data center or in a locked server rack or cabinet. Ideally both a restricted access data center and a locked server rack or cabinet would be utilized.
Testing	• Ask to be shown the device and note the location and security measures in place at the location. • If a secure location exists document the procedures for entry and exit from the location. • If server rack or cabinet is used note if a lock is present and in use. • If server rack or cabinet lock is used determine who has keys to locks.
Test Type	Objective/Subjective
Supporting Documentation	**Figure 3.2 – 3.3**
Test Results	The server room is protected by a steel

© SANS Institute 2005 Author retains full rights.

	door with a combination lock. (**see figure 3.3**) Only three people have the combination to the room with a backup copy of the combination in a sealed envelope in a fire safe with restricted access. Procedures for entry and exit from the room are informal due to the limited number of personnel with the combination. The Fortigate-60 device resides in a locked cabinet along with several other devices including switches and IDS devices. (**See figure 3.4**) The only personnel with keys to the cabinet are the CIO and local network administrator.
Exceptions	No exceptions noted.

Figure 3.3 Server Room Entrance

Figure 3.4 Cabinet housing firewall

3.2.4	Firewall Device Maintenance Controls

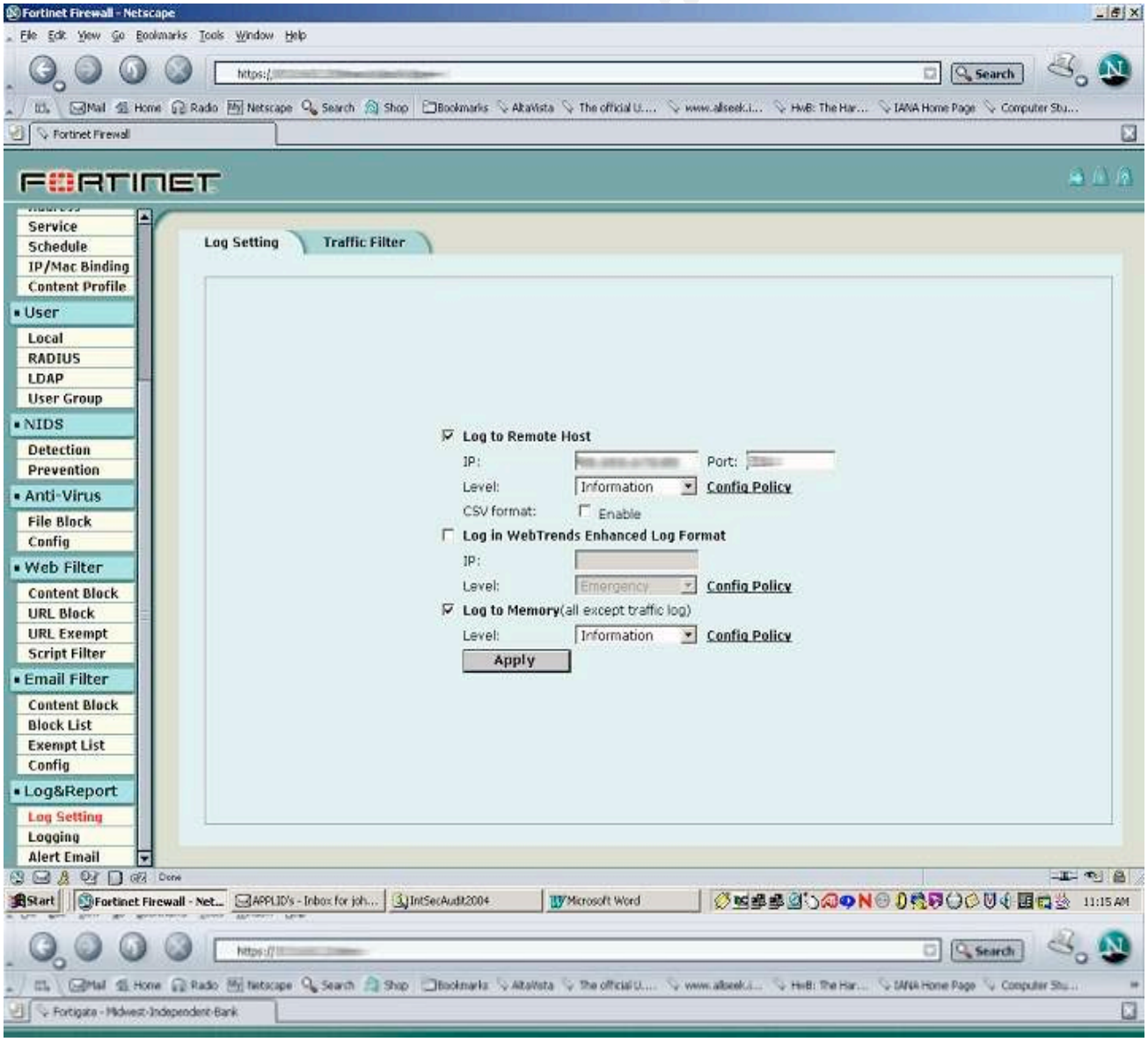
© SANS Institute 2005 Author retains full rights.

Audit Step	3.2.4.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com "Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000. Fortigate-60 Documentation "Logging and Reporting"
Control Objective	Ensure system logging is enabled and the logs are stored in a secure fashion.
Non Compliance Risk	Not logging activities that pass through the firewall can result in the inability to detect intrusion attempts and can hinder or defeat forensic analysis of an intrusion event. Secure storage of logs prevents intruders from accessing and possibly altering the logs to hide evidence of their intrusion.
Compliance	Logging is enabled and the logs are stored in a secure fashion, preferably on a remote syslog server.
Testing	• Have System Administrator log in to the web interface. • Choose Log & Report > Log Setting. Verify that the "Log to Remote Host" box is checked and that a valid remote IP and Port number are entered. • Choose System>Network>Interface Select edit in the modify column beside the active interfaces (NIC) and ensure the "Log" setting is set to "Enable" for each.
Test Type	Objective
Supporting Documentation	**Figure 3.5**
Test Results	The device is configured to log to a

© SANS Institute 2005 Author retains full rights.

	remote server at the Perimeter Defense Vendor's data center (See **Figure 3.5**). The logs are backed up each night. The log settings for the device are set to monitor the correct interfaces with appropriate access configured for each interface (See **Figure 3.6**).
Exceptions	No exceptions noted.

Figure 3.5 Screen capture of remote host logging screen



© SANS Institute 2005 Author retains full rights.

Screen shot obtained after firmware upgrade which changed graphics and layout of the web interface.

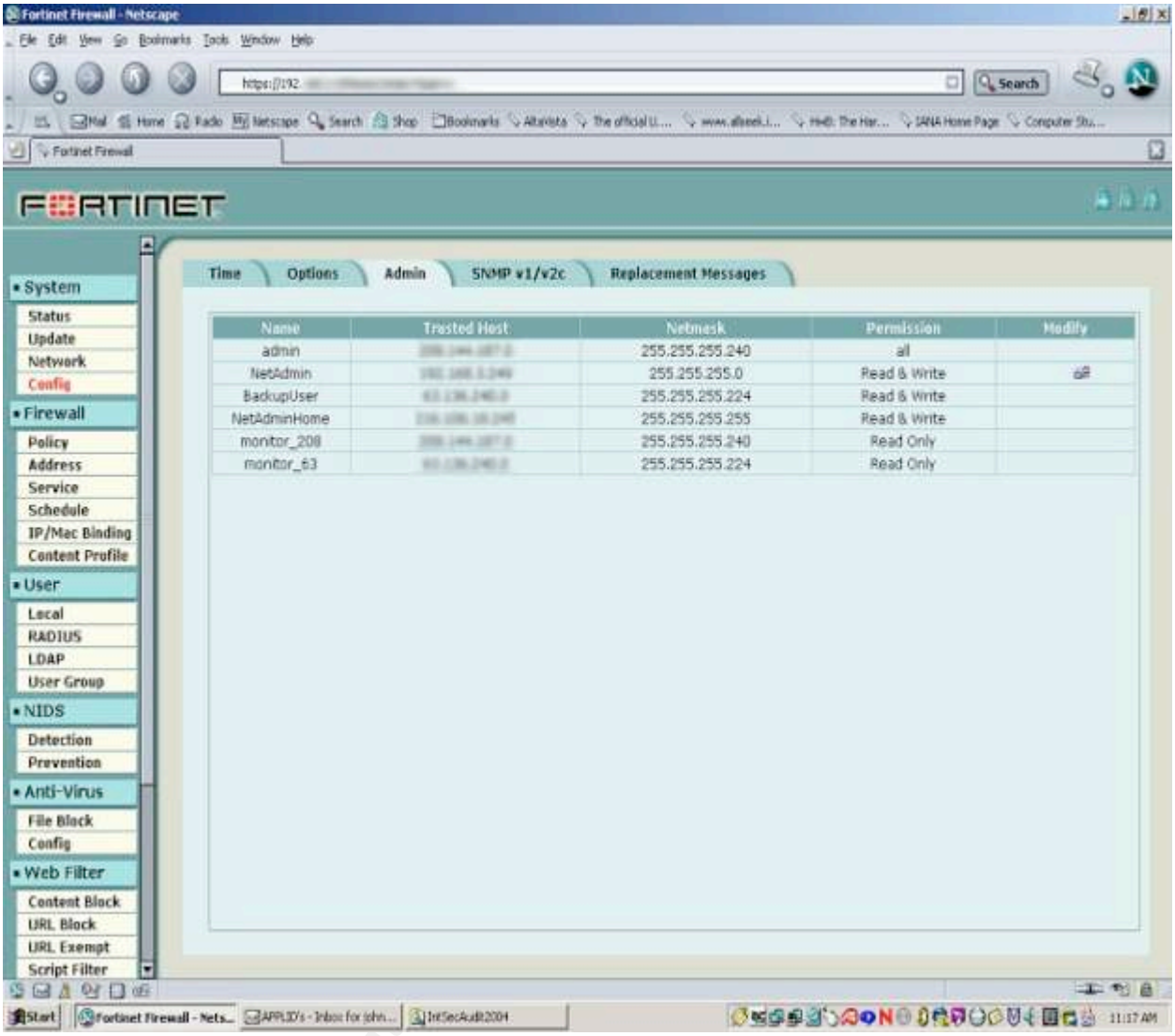
Audit Step	3.2.4.2
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Minimize the number of administrative accounts on the Firewall.
Non Compliance Risk	Lack of control of the number and type of administrative accounts on a firewall can lead to unmanageable change control and could result in confusion as to the level of security the Firewall affords and inconsistent rules for access.
Compliance	The number of administrative accounts

© SANS Institute 2005 Author retains full rights.

	is kept to a necessary minimum.
Testing	• From the Administration interface Go to System > Config and then click on the Admin tab. Capture a screenshot or printout of the settings. • Through interview with the local System Administrator establish the purpose of each account.
Test Type	Objective/Subjective
Supporting Documentation	**Figure 3.7**
Test Results	6 user accounts are configured. One is the general Admin account with the default password changed. The remaining are as follows: Netadmin – The local admin account used internally Backupuser – The remote admin account for the Perimeter Defense vendor's access. NetadminHome – The remote admin account for the local administrator to access the system from home. The remaining two accounts, monitor_208 and monitor_ 63, are monitor accounts to facilitate the perimeter defense vendor's automated reporting. (See **Figure 3.7**). In discussion with the System Administrator all accounts are deemed necessary by management.
Exceptions	No exceptions noted.

Figure 3.7 Screen capture of remote administration users screen.

© SANS Institute 2005 Author retains full rights.



Audit Step	3.2.4.3
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com
Control Objective	Remote administration conducted through appropriate vendor software, encryption and security methodology
Non Compliance Risk	The use of inappropriate software, encryption and security methodology (such as the use of Telnet, which broadcasts information "in the clear", lack of encryption for sessions and not logging sessions) for remote administration can allow intruders to

© SANS Institute 2005 Author retains full rights.

	obtain user names and passwords and other sensitive information that can grant them access to the firewall and system.
Compliance	Remote administration conducted through SSH or 128-bit Encrypted HTTPS and restricted by IP address
Testing	• From questionnaire determine if remote administration is allowed. • From questionnaire determine if logical access to the firewall is restricted and if so, how. • From questionnaire determine what protocol is used for remote administration. • From questionnaire determine if there are written procedures and security guidelines in place for remote administration. Obtain a copy of the procedures and guidelines and review.
Test Type	Objective
Supporting Documentation	Q12, Q13, Q13a, Q13d
Test Results	From the questionnaire and discussions with the local administrator it was determined that remote administration of the device is allowed. Logical access to the firewall is restricted via IP address or "Trusted Host". The only remote administration protocols used to access the device are SSH and HTTPS. From earlier scans SSH is version 2.0. Additionally all remote sessions are logged by the system. (See **Exhibit L**)

© SANS Institute 2005 Author retains full rights.

	Secure Networks provided a detailed guide that they give to each of their employees and to the local administrator of devices they manage. The document is thorough and concise in the procedures for accessing systems that SN manages.
Exceptions	No Exceptions noted.

Exhibit L: Sample from firewall log of remote administration session.

2004-07-13 09:42:59 log_id=0104000001 type=event subtype=admin pri=information user=monitor_208 ui=GUI(208.100.100.1) action=login status=success reason=none msg="User monitor_208 login successfully from GUI(208.100.100.1)"

SN also provided detailed change control procedures that must be followed before any change is made to the system via remote administration. While the procedures are proprietary and SN did not want them reproduced in whole, a summary of the key areas is presented below.

- Acceptable format for change requests
- Testing of device changes in lab setting
- Backup of existing configuration
- Testing of Backup
- Application of changes
- Change documentation including change request, lab work, backup test results

Audit Step	3.2.4.5
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com NIST "Guide to Firewall Selection and Policy Recommendations" John Wack, Ken Cutler, Jamie Pole Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure the Firewall has a documented backup procedure. Verify that backups and restoration procedures are tested

© SANS Institute 2005 Author retains full rights.

	and verified to insure they are viable
Non Compliance Risk	Failure to properly backup the firewall could result in the loss of configuration information as well as system and security log files. Failure to test backups can result in loss of configuration information, extended down time and risk of improper configuration when recovering from a device failure.
Compliance	Documented backup procedures exist and are followed. Backups are tested in a manner that ensures full system restoration can be completed in the event of device failure.
Testing	• From questionnaire determine if the Firewall is backed up and who is responsible for the backup procedures.. • Request backup testing procedures. • Request documentation of last backup test results.
Test Type	Objective
Supporting Documentation	Q17, Q17b
Test Results	SN is solely responsible for backing up the Fortinet-60 device configuration. Backup is initiated every 30 days and after every change. Backup procedures were reviewed and found to be detailed and thorough. The device configuration is backed up to the same server as the firewall logs. Additionally the backup is tested by restoring to a test device in SN's lab. A copy of the documentation for the last backup test was received and

© SANS Institute 2005 Author retains full rights.

	reviewed. All steps and procedures for restoring the backup configuration were followed and the test results reviewed and approved by SN management.
Exceptions	No Exceptions noted.

3.2.5 Transport Layer Security

Audit Step	3.2.5.1
Reference	"Firewall Security Best Practice Guidelines" http://www.knowledgeleader.com "Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000.
Control Objective	Ensure only ports required to meet business requirements are open on the system
Non Compliance Risk	Unnecessary open ports could allow intruders to gather information about the system or even facilitate an attack on the system.
Compliance	Only necessary ports are open on the system.
Testing	• Obtain a copy of the Firewall Policy to determine what ports should be enabled on the firewall. • Obtain a copy of the configuration file for the system to determine which ports are enabled. Compare this to the allowed ports stated in the Firewall Policy. • Using Nmap, scan the system to determine which ports are listening. If any ports other than those listed in the Firewall Policy and configuration

© SANS Institute 2005 Author retains full rights.

	file are running further attention should be given to whether the system is misconfigured or if in fact the system has been compromised.
Test Type	Objective-Stimulus/Response
Supporting Documentation	**Figure 3.8**
Test Results	Since no Firewall Policy is in place there is no way to audit the configuration against policy. Review of the configuration file showed that only ports 22 and 443 for SSH and HTTPS respectively, should be open on the firewall. An internal Nmap scan verified that only ports 22 and 443 are open and listening. All others are listed as "filtered".
Exceptions	Exception noted. No Firewall policy in place to compare configuration file.

Nmap Internal Scan Detail:

Nmap was used to scan for open ports on the Fortigate-60 device. The audit laptop was connected to the network, booted into Fedora Core2 and a terminal window brought up. The following command was entered at the command prompt:

`# nmap -sS -PT -PI -O -T 3 [Target IP]` (See **Figure 3.8**)

-sS tells Nmap to perform a TCP SYN scan, or "half open" scan. This command sends a SYN packet and then waits for a response. If a SYN/ACK is received it indicates a listening port. –sS is preferable to the normal TCP connect (-sT) because some firewalls and packet filters tend to drop probes without response.

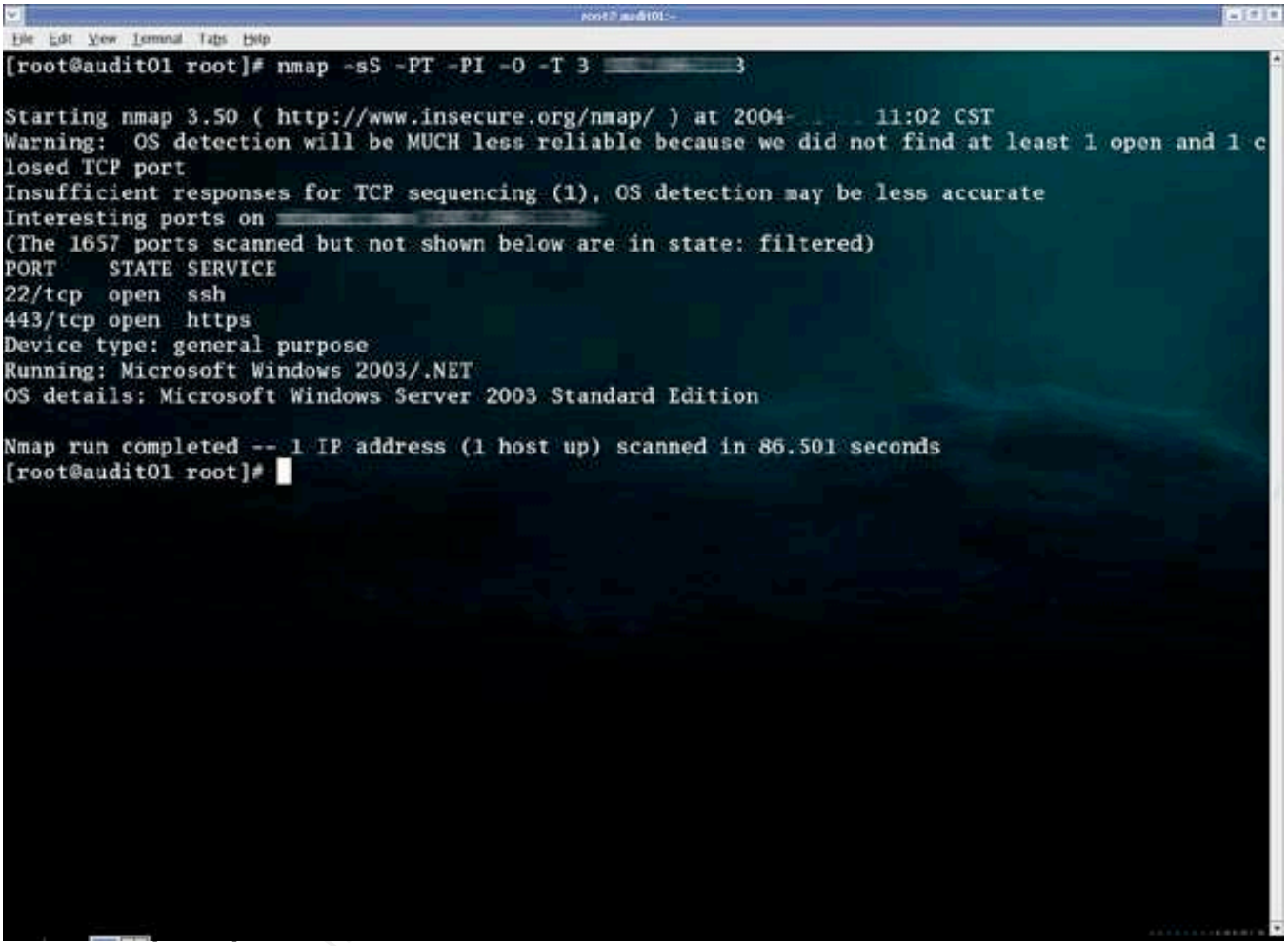
-PT and **–PI** tells Nmap to perform TCP and ICMP ping sweeps against the device. This is useful in bypassing firewall filters that look for either sweep type, but not both.

-O tells Nmap to activate remote host identification using TCP/IP fingerprinting. Many times Nmap can only give a best guess from the results of the TCP sequencing.

© SANS Institute 2005 Author retains full rights.

-T 3 tells Nmap to which timing policy to use for scanning. 3 is the setting for a Normal scan which scans more slowly, but eases the load on the network and reduces the possibility of crashing a machine or device.

Figure 3.8 Screenshot of Nmap run in Terminal on Fedora Core2



Nmap Output Detail:

```
[root@audit01 root]# nmap -sS -PT -PI -O -T 3 {Target IP
Address}

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at
2004  11:02 CST
Warning:  OS detection will be MUCH less reliable because
we did not find at least 1 open and 1 closed TCP port
```


© SANS Institute 2005 Author retains full rights.

```
Insufficient responses for TCP sequencing (1), OS detection
may be less accurate
```

-sS –PT –PI returns:

```
Interesting ports on {Target IP Address}
(The 1657 ports scanned but not shown below are in state:
filtered)
PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
```

-O returns:

```
Device type: general purpose
Running: Microsoft Windows 2003/.NET
OS details: Microsoft Windows Server 2003 Standard Edition
```

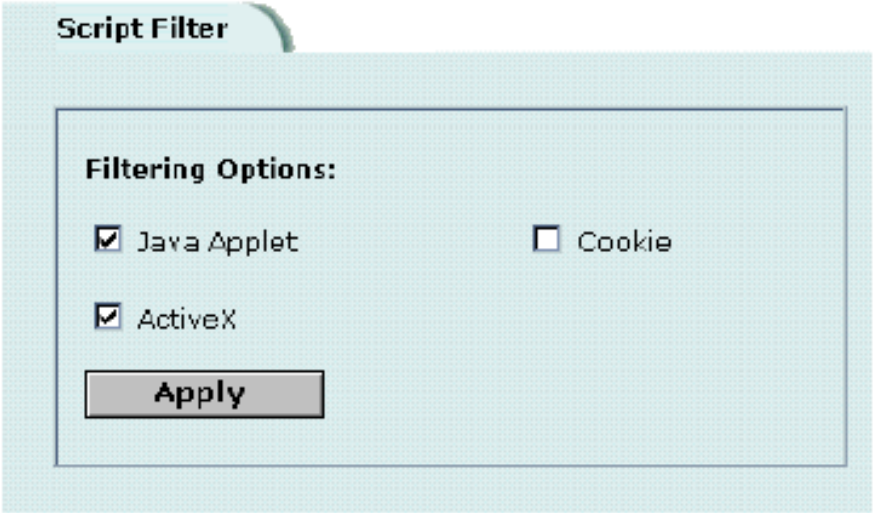
3.2.5 Transport Layer Security

Audit Step	3.2.6.1
Reference	"Building Internet Firewalls, 2d ed. Elizabeth D. Zwicky, Simone Cooper, and D. Brent Chapman 2000. Personal experience Fortigate-60 Documentation "Firewall Configuration"
Control Objective	Ensure that the firewall is using inbound filtering and only the application proxy services allowed by the firewall policy are running on the device.
Non Compliance Risk	If the firewall does not perform inbound filtering or allows unnecessary application proxy services, unnecessary or intentionally malformed packets may be introduced to the network.
Compliance	Inbound filtering is being used and only those application proxy services stated in the firewall policy are running on the device.
Testing	• Determine which application proxy services are allowed

© SANS Institute 2005 Author retains full rights.

	according to the firewall policy. • Compare the services allowed in the policy to the services that are allowed by inbound filtering on the firewall. Have the local administrator log on using the web interface. Go to Web Filter > Script Filter to determine what services are allowed.
Test Type	Objective
Supporting Documentation	**Figure 3.9**
Test Results	Since no Firewall Policy is in place there is no way to audit the configuration against policy. The script filtering capabilities of the Fortigate-60 device are limited to Java Applet, ActiveX and Cookie scripts.
Exceptions	Exceptions noted. No Firewall Policy in place.

Figure 3.9 Script Filter configured to block Java Applet and ActiveX scripts



3.2.7

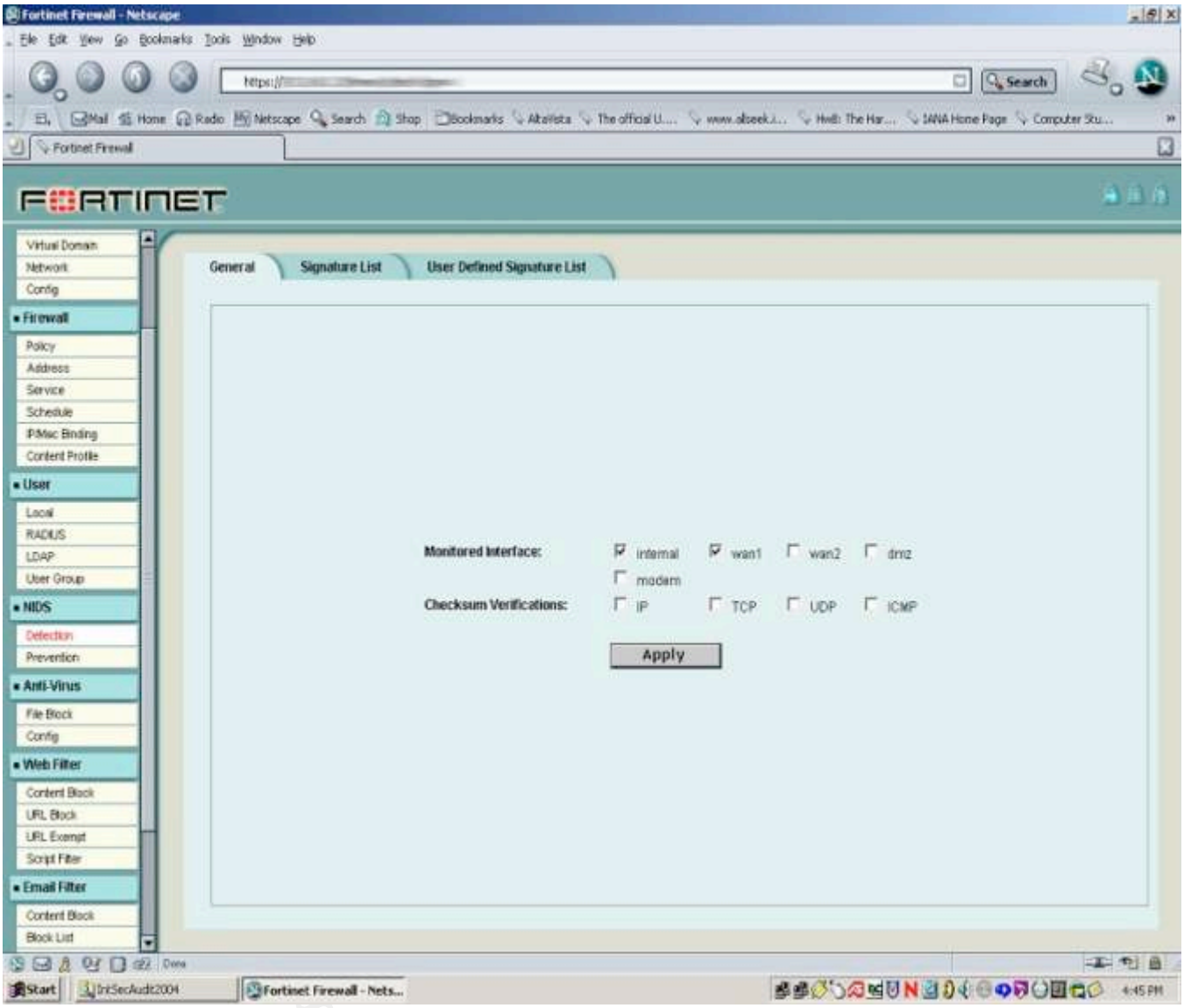
Audit Step	
Reference	Personal experience Fortigate-60 Documentation "Network Intrusion Detection System (NIDS)"
Control Objective	Ensure that the intrusion detection feature is enabled and the proper interfaces are being monitored by the

© SANS Institute 2005 Author retains full rights.

	IDS.
Non Compliance Risk	From the Fortigate-60 user guide it was stated that the intrusion detection feature is on by default but can be disabled. It is important to verify that this feature is enabled and that the proper interfaces to the network are being monitored.
Compliance	The intrusion detection feature is enabled on the device.
Testing	• Have the local administrator log on to the web interface. Go to NIDS > Detection > General tab. Ensure that at least one interface is checked. If no interfaces are checked the IDS function is not enabled. • Through interview establish which interfaces should be enabled. Ensure that these interfaces are in fact checked and active in the NIDS > Detection > General tab.
Test Type	Objective
Supporting Documentation	**Figure 3.10**
Test Results	The NIDS>Detection>General tab was accessed and it was discovered no interfaces were being monitored. After discussion with the CIO and SN a change request was submitted to SN and the "Internal" and "wan1" interfaces were checked. (See **Figure 3.10**) The CIO will investigate with SN why the lack of IDS activity (logging, incident reports, etc) went unnoticed and attempt to verify how long the device has been misconfigured.
Exceptions	Exception found. Issue resolved satisfactorily during course of audit. No exception noted.

© SANS Institute 2005 Author retains full rights.

Figure 3.10 NIDS detection interface setup screen. (Properly configured)



Audit Step	3.2.7.2
Reference	Personal experience Fortigate-60 Documentation "Network Intrusion Detection System (NIDS)"
Control Objective	Ensure that the attack signatures feature is enabled on the IDS.
Non Compliance Risk	From the Fortigate-60 user guide it was stated that the NIDS attack signatures feature is on by default but "After the

© SANS Institute 2005 Author retains full rights.

	Fortigate unit reboots, the NIDS attack prevention and synflood prevention are always disabled." It is important to ensure that the attack prevention and synflood prevention are enabled on the device.
Compliance	NIDS attack prevention and synflood prevention are enabled.
Testing	• Have the local administrator log on to the web interface. Go to NIDS > Prevention tab. Ensure the "Enable Prevention" check box in the upper left corner is checked. By default all signatures are checked and should be left so. If there are any signatures not checked establish if there are valid business reasons for them to be turned off.
Test Type	Objective
Supporting Documentation	**Figure 3.11**
Test Results	The local administrator logged into the web interface and the NIDS>Prevention section was accessed. It was discovered that the "Enable Prevention" check box was not checked. After discussion with the CIO and SN a change request was submitted to SN and the "Enable Prevention" check box was checked. SN was also apprised of the necessity to check this setting after any reboot of the system to ensure this feature is enabled.
Exceptions	Exception found. Issue resolved satisfactorily during course of audit. No exception noted.

© SANS Institute 2005 Author retains full rights.

Figure 3.11 Screenshot of NIDS Prevention (Properly configured)

Prevention

Enable Prevention

Signature Abbreviation	Summary	Protocol	Enable	Modify
synflood	syn flood attack	TCP	☑	
portscan	port scan attack	TCP	☑	
synfrag	syn fragment attack	TCP	☐	
synfin	syn with fin attack	TCP	☐	
noflag	tcp with no flag attack	TCP	☐	
finnoack	fin without ack attack	TCP	☑	
srcsession	source session limit	TCP	☐	
winnuke	winnuke attack	TCP	☐	
land	tcp land attack	TCP	☐	
ftpovfl	ftp buffer overflow attack	TCP	☐	
smtpovfl	smtp buffer overflow attack	TCP	☐	
pop3ovfl	pop3 buffer overflow attack	TCP	☑	
url	invalid url attack	TCP	☐	
udpflood	udp flood attack	UDP	☐	
udpland	udp land attack	UDP	☐	
udpsrcsession	udp source session limit	UDP	☐	
icmpflood	icmp flood attack	ICMP	☑	
icmpfrag	icmp fragment attack	ICMP	☑	
icmpdeath	ping of death attack	ICMP	☐	
icmplarge	large icmp packet attack	ICMP	☐	

Assignment 4 - Sample Audit Report

CBMW Bank Audit Report

© SANS Institute 2005 Author retains full rights.

Fortigate-60 Firewall Audit

Report Issued: August 25th, 2004

Audit Committee Distribution: **Audit and**
Report Completed by:

Brian Cook,
IT Auditor

Internal Distribution:
CIO
CEO
COO

© SANS Institute 2005, Author retains full rights.

Table of Contents

Executive Summary Pg 3

© SANS Institute 2005 Author retains full rights.

General Background Pg 4

Detailed Findings Pg 5

Objectives, Scope & Procedures Performed Pg 6

Testing Summary Pg 7-10

Appendices

Appendix A Pg 11

© SANS Institute 2005, Author retains full rights.

Executive Summary

External audit performed an audit on the bank's primary firewall between July 13th and July 22nd 2004. The objectives of this audit were to obtain an understanding of the key administrative and operational processes related to the device and to evaluate the adequacy and effectiveness of the device.

A secondary objective of the audit was to assess the perimeter defense vendor's responsiveness and reporting capabilities in the event of an intrusion attempt.

© SANS Institute 2005 Author retains full rights.

Key Findings and Recommendations

- Review of the bank's internal policies and procedures showed that no formal written policies and procedures related to firewall administration are in place. During the audit it was found that management has hired an outside consultant to develop an Information Security policy. External Audit **recommends** senior management ensure the policy is implemented by the end of 2004.

- While performing an external scan of the network Internal Audit was made aware of a vulnerability in the bank's router which causes the router to shut down resulting in loss of Internet and e-mail access as well as loss of connection with the Internet Banking vendor and the Federal Reserve. This vulnerability can be avoided by discontinuing the use of a specific network translation protocol (see detailed findings). External Audit **recommends** IT management determine if the benefits of using the network translation protocol outweigh the possibility of periodic Internet outages.

- During review of the firewall's Intrusion Detection feature it was discovered that several settings, necessary for the device to be fully functioning as an IDS, were disabled. This was discussed with the perimeter defense vendor and the necessary changes were made to the configuration to ensure that the IDS feature was fully functional. External audit has no further recommendations at this time.

- The perimeter defense vendor's responsiveness and reporting capabilities to management were not as expected. External Audit **recommends** that IT management work with the perimeter defense vendor to understand and clarify their monitoring and reporting capabilities and establish documented thresholds for incident reporting and notification.

General Background

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

CBMW's management recognizes the growing significance of, and reliance on, their IT infrastructure. The data transmitted over CBMW's network and stored on its servers is both vital and sensitive and every precaution must be taken to ensure the data's safety

© SANS Institute 2005 Author retains full rights.

and security. The consequences of a security breach of the organization's network is a serious matter. Loss of data, reputational damage, and financial loss are all very real possibilities. With CBMW, like most organizations, firewalls are the first major line of defense against outside intrusion.

As part of External audit's IT audit program an audit was conducted on the bank's primary firewall device, a Fortinet Fortigate-60 Antivirus firewall. This device is one of two firewalls present on the network. As part of an overall plan to increase both the defensive posture of CBMW's network and the ability to continually monitor the network IT management chose the Fortigate-60 for both its Antivirus capabilities and the built in Intrusion Detection System (IDS).

Configuration and administration of the Fortigate-60 firewall is primarily the responsibility of CBMW's perimeter defense vendor Secure Networks. While the local System Administrator can make changes if necessary, he does not have the testing and implementation resources available to the perimeter defense vendor. The vendor's change control procedures facilitate change requests, and include testing and implementation for each modification to the device.

This audit focused on three major functions of the device:

- Configuration and functionality of the Firewall feature.
- Configuration and functionality of the Intrusion Detection feature.
- Configuration and functionality of the Antivirus feature.

Industry best practices for each feature were researched and External Audit developed an audit program to conduct a comprehensive examination of the device to ensure it is configured and operating as intended and protecting the bank's network appropriately.

The bank's policies and procedures were reviewed as well as administrative practices for change management. Physical and logical access policies and procedures were also reviewed to ensure that local and remote access sessions are conducted using a secure methodology.

Detailed Findings and Recommendations

© SANS Institute 2005 Author retains full rights.

Policies

In reviewing the bank's internal policies and procedures it was noted that no formal written policies and procedures related to firewall administration are in place. During the audit it was found that management has hired an outside consultant to develop an Information Security policy. External Audit **recommends** senior management ensure this is a priority. Without clearly defined procedures for configuration, logging, change control, remote access, physical access, and patch management the organization risks having a firewall in place that does not protect the organization's network.

Router Vulnerability

While outside the scope of this audit, it should be mentioned that in the course of an external scan of the firewall an issue with the bank's router was discovered that makes the device vulnerable to Denial of Service attacks after a port scan of the router. In other words, by simply running a scan with freely available software, even without malicious intent, anyone can shut down the bank's Internet access.

This is due to the bank's use of Port Address Translation or PAT, which allows multiple computers to access the Internet using only one external IP address. This protocol puts an undue load on the router and causes it to shut down if it becomes overloaded. This stops all Internet and e-mail access as well as connectivity to external vendors. There is a possibility the device's manufacturer will provide a patch for this vulnerability at some point in the future but no specific commitment to do so has been expressed. External Audit **recommends** senior management determine if the benefits of utilizing PAT outweigh the probability of periodic Internet outages resulting from external scans of our system. This will be re-addressed in detail during a planned audit of the router device in question.

IDS Configuration

During review of the firewall's Intrusion Detection feature it was discovered that several settings, necessary for the device to be fully functioning as an IDS, were disabled. Specifically, the settings which tell the device which network to monitor, and attack prevention settings were disabled. This was discussed with the vendor and the necessary changes were made to the configuration to ensure that the IDS feature was fully functional. External audit has no further recommendations at this time.

IDS Vendor Response

Internal Audit performed an external, "aggressive" scan of the network from a remote location to assess the firewall's effectiveness and the perimeter defense vendor's

© SANS Institute 2005 Author retains full rights.

responsiveness and reporting capabilities. While the firewall was effective in blocking the scans intended actions, the perimeter defense vendor's responsiveness and reporting capabilities were not as expected. No notification was received of the incident and no record of the scan was found. External Audit **recommends** that IT management work with the perimeter defense vendor to understand and clarify their monitoring and reporting capabilities and establish documented thresholds for incident reporting and notification.

Objectives, Scope & Procedures Performed

Objectives:

- Ensure the device is configured and performing in compliance with the bank's policies and security goals.
- Verify the firewall configuration and functionality follow industry best practice guidelines.
- Verify the Antivirus configuration and functionality follow industry best practice guidelines.
- Verify the Intrusion Detection configuration and functionality follow industry best practice guidelines.

Scope:

The scope of this audit includes a review of the following areas:

- Policies and Administrative practices
- Physical and logical security of the device
- Configuration of firewall rule-sets
- Configuration of the Anti-virus feature
- Configuration of the IDS feature
- Enabled services running on the device
- Perimeter Defense vendor response

Summary of Procedures Performed:

- Interviewed IT management and appropriate staff to determine administrative practices and procedures.

© SANS Institute 2005 Author retains full rights.

- Interviewed Perimeter Defense vendor technical staff and management to determine administrative practices and procedures with regards to remote management and logical access.
- Reviewed existing policies and documentation of relevant procedures.
- Obtained an understanding of the device and its functions through research and requested items from IT.
- Physically inspected the device to determine level of physical security.
- Conducted both an external and an internal scan of device using Nessus scanning software and NMap software to test configuration settings and determine if unnecessary or unsecured services are running on the device.

© SANS Institute 2005, Author retains full rights.

Testing Summary of Fortigate-60 Firewall

The matrix below outlines testing performed and related results. Testing was conducted during the week of July 12th, 2004.

Testing Performed ***Observations***		
Policies and Administrative Practices		
1) Reviewed bank's policies and procedures for Network Security with regards to firewall administration and change control.		1) **Exception found**. No policies related to the

© SANS Institute 2005 Author retains full rights.

2) Reviewed Perimeter Defense vendor's policies and procedures for change control, remote access, backup and restoration procedures.		firewall are in place. IT management is in the process of developing and refining more comprehensive network policies with the help of Secure Networks and Superior Consulting. Senior management should ensure this is a priority. Without clearly defined procedures for configuration, logging, change control, remote access, physical access, and patch management the organization risks having a firewall in place that does not protect the organization. 2) No exceptions noted. Vendor policies and procedures are concise and cover all necessary areas.
Testing Performed Observations		
Physical and Logical Access to the device		
1) Inspected the physical security of the device.		1) No exceptions noted. The physical security of the device is

© SANS Institute 2005 Author retains full rights.

2) Reviewed the permissions and number of administration accounts to ensure they are kept to a minimum. 3) Reviewed remote access policies and procedures as well as the methods used for remote access to ensure proper procedures and methodology is used.		excellent with concentric layers of locks in place to protect access. 2) No exceptions noted. The administrator accounts include only accounts necessary for maintenance and monitoring of the device by Secure Networks and the local System Administrator. 3) No exceptions found. Guarded Network's remote access policies and procedures are comprehensive and well documented. The bank should develop procedures for *internal* logical access as well.
Testing Performed Observations		
Configuration of the Firewall Rulesets		

© SANS Institute 2005 Author retains full rights.

1) Visually reviewed printed version of Firewall configuration to ensure proper rule-sets are present and enabled. 2) Conducted external scan of device using Nessus scanning software to determine if any known vulnerabilities were present in the configuration.		1) No exceptions found. The Fortigate line of firewalls has what some would consider excessive rulesets (Best practice guidelines specify an average of 20 rulesets while the Fortigate has over 70) there may be some benefit to the extra layers of protection. 2) The results of the external scans were somewhat inconclusive due to the bank's use of PAT. However no known vulnerabilities were found. Due to the vulnerability of the router to Denial of Service attacks further scanning of the router was deemed too disruptive.

Testing Performed ***Observations***		
Configuration of Anti-Virus feature		
1) Visually reviewed printed version of Anti-virus configuration to ensure proper file patterns and services are present and enabled.		1) No exceptions found.

© SANS Institute 2005 Author retains full rights.

Testing Performed ***Observations***		
Configuration of IDS feature		
1) Visually reviewed printed version of IDS configuration to ensure proper file patterns and services are present and enabled 2) Requested IDS logs detailing external scan of device from Secure Networks.		1) **Exception found**. The configuration showed that most features for the IDS were disabled. Some confusion as to the designation of disabled vs. enabled was cleared up during conversations with Secure Networks. It was determined the IDS feature was not configured correctly and therefore was not logging network activity. The System Administrator worked with the vendor to enable the IDS feature during the course of the audit. No further recommendations necessary. 2) Secure Networks was unable to provide logs of the external scan due to misconfiguration of the IDS feature of the device.
Testing Performed ***Observations***		
Enabled Services running on the device		

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

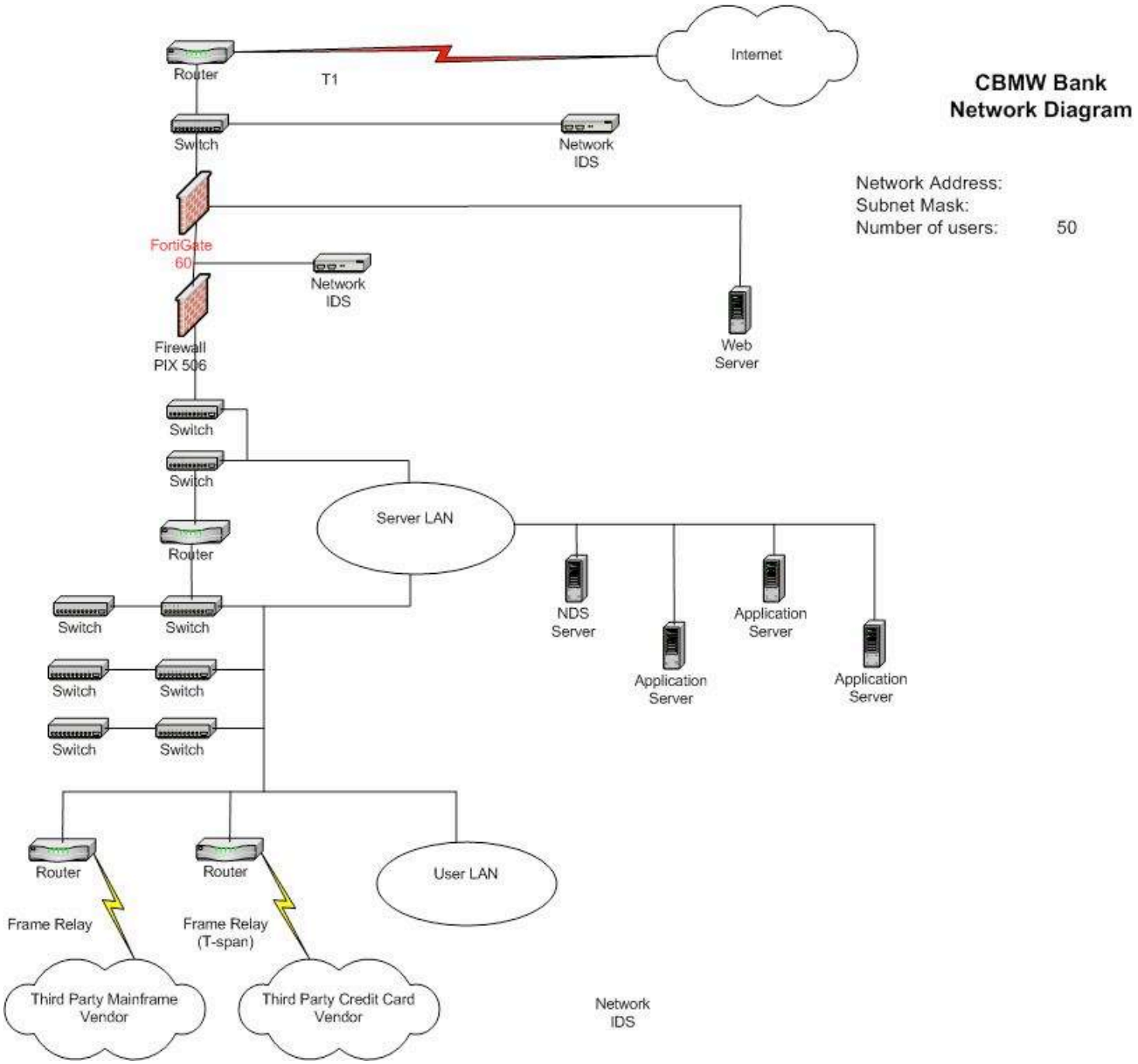
1) Conducted internal scan of the device using Nessus scanning software and a direct connection (via crossover cable plugged directly into hub connected to device) to determine if unnecessary or unsecured services such as FTP or Telnet were running.		1) No exceptions found. The scan of the device showed only HTTPS and SSH services were running, both being necessary for the device to function properly.

Audit Committee Chairman	**Date**
Audit Manager	**Date**
Senior Technology Officer	**Date**

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Appendix A



© SANS Institute 2005 Author retains full rights.

References

Fortigate-60 Installation and Configuration Guide Version 2.50 MR2

Zwicky, Elizabeth D, Simone Cooper and D Brent Chapman. Building Internet Firewalls, 2d ed. O'Reilly 2000.

Cheswick, Bill, Steve Bellovin and Avi Ruben. Practical Internet & Unix Security. O'Reilly 1996.

Sawyers, Jimmy R. IT Auditing for Financial Institutions 2 vols. Alex eSolutions 2004.

Wack, John, Ken Cutler and Jamie Pole
NIST "Guide to Firewall Selection and Policy Recommendations"
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

Krishni Naidu Firewall Checklist http://www.sans.org/score/firewallchecklist.php

Firewall Security Best Practice Guidelines http://www.knowledgeleader.com
(Fee based membership site with 30-day free trial with valid e-mail address)

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.