Global Information Assurance Certification Paper

Auditing the Symantec Enterprise Firewall v7.0 for Windows NT: An Auditor's Perspective

GSNA Practical Assignment
Version 2.1, Option 1 (amended July 5, 2002)

Author: Tim Lewis
July 11, 2003

OVERVIEW

This paper documents an audit of Windows NT-based Symantec Enterprise Firewall (formerly Raptor Firewall) from an Auditor's perspective. The paper will document system description, risk assessment of the system, audit checklist development for the system, and a report on the results of an audit based on that checklist. As the Auditor, I have no prior knowledge of the company's policy or equipment. All information is collected from company personnel and documentation, personal experience, and public sources such as the Internet.

ASSIGNMENT 1 – RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL

SYSTEM DESCRIPTION

The subject of this audit is the Symantec Enterprise Firewall v7.0 for NT/2000. Those of you familiar with firewalls know that this firewall was originally known as the Raptor Firewall from Axent Corporation, who was acquired by Symantec. The Symantec Enterprise Firewall (hereafter referred to as "SEF") is an application level firewall, which is defined by Symantec as follows:

> In an application level firewall, a set of application-specific security proxies evaluates all attempts to pass data into or out of the protected network. The firewall receives an incoming connection, determines whether it is allowed, and creates a corresponding connection with the intended computer. It rewrites the source and destination information of the connection to keep information about your network secret. Therefore, for application level traffic, there are always two TCP or UDP connections, one between the firewall and the source, and another between the firewall and the destination.[1]

These features, as well as others, make the SEF a good solution for high security applications, which is why the Client selected it to protect its online analytics business serving more than twenty of their customers over the Internet. This business is one of the Client's primary sources of revenue, and as such, their customers' data which resides on the servers protected by the SEF is characterized as *classified-restricted*. This is the highest designation that can be assigned to information, as defined in the Client's Information Security Policies.

The SEF is running on an Intel-based Windows-NT Server, patched to Service Pack 6.0a. It is configured to connect to four networks: an outside network (which connects to the co-location facility's Internet mesh), a screened subnetwork, an internal production network, and an internal administrative network. The screened subnet contains a single physical Linux server virtualized into two separate servers, providing FTP and customer authentication services. The internal production network contains web switching logic and one large Unix server that serves the customer application instances. The internal administrative network contains Linux support servers as well as administrative access to the servers located in the internal production and screened subnetworks.

RISK OVERVIEW

The client uses a Sensitivity/Criticality system for classifying systems. To begin to identify and understand the risks associated with the use of the SEF, it is useful to classify the firewall with respect to Sensitivity and Criticality:

- Sensitivity: the sensitivity of the information the SEF protects, and;
- Criticality: the criticality of the SEF's continuing functionality to the organization's operations.

Sensitivity of Information

As was stated earlier in this paper, the SEF under audit protects the Client's customer data. These data are considered strategic to the Client's customer. Were these data to fall into the hands of a competitor, it could cause significant damage to the customer's present and future revenue streams. Therefore, the SEF is classified to be protecting information of the highest sensitivity level in the company, with the classification *Confidential-Registered*.

Criticality of Operation

Part of the reality of running an Internet business is the existence of Service Level Agreements. These agreements define, among other things, a promise to make the application available for a specific percentage of time. Some businesses, such as banks or stock exchanges, may promise their customers as much as 99.999% application availability, which equates to a little over 5 minutes of downtime per year. In our case, we promise the system will be available for customer use 99% of the time. This requirement results in a company criticality classification of *Essential*.

Given these classifications for the SEF, the Client's Information Security Policy requires that such a system pass through a formal accreditation process, whereby the administrator submits both a Security Plan and a Disaster Recovery Plan for approval by the Chief Security Officer prior to production deployment.

These plans are intended to identify and mitigate risks to information privacy, protection, and availability. What follows is an assessment of such risks.

RISK ASSESSMENT

For this assessment, the risks will first be classified into the following categories: Physical Security, Logical Security, and Management Controls.

1. Physical Security

Vulnerability:	Insufficient physical security controls
Threat:	High: Unauthorized local access to SEF management console could be acquired; Cables could be disconnected or damaged; Server could be powered off.
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Low: Facility is secured, cabinet is locked, screen saver is password-protected, and SEF management console uses strong passwords.

Vulnerability:	Insufficient environmental security controls
Threat:	High: Lack of power and cooling redundancy and/or automatic failover mechanisms could result in power and cooling interruptions; Lack of sufficient fire suppression systems could result in equipment destruction through fire or water damage.
Exposure:	High: Could result in loss of service.
Risk:	Low: Facility employs triple-redundant power and cooling systems, “dry-pipe” fire suppression systems, and VESDA (Very Early Smoke Detection Apparatus) smoke detection systems.

2. Logical Security

Vulnerability:	Insufficient remote access controls for server
Threat:	High: Unauthorized remote access to the firewall server could be obtained.
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Low: NT Server does not have remote access capabilities.

Vulnerability:	Insufficient Management Console access controls
Threat:	High: Unauthorized remote access to the firewall management console could be obtained.
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Low: Remote access must be specifically configured on the SEF, with only strong passwords allowed. Attack would require IP address and password. Legitimate remote access allowed over VPN only (no eavesdropping).

Vulnerability:	Insufficient admin training
Threat:	High: The SEF or server OS could be mis-configured, resulting in unauthorized access or insufficient protection.
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Medium: Though access to the SEF is highly restricted, it does not protect against lack of knowledge.

Vulnerability:	Errors in SEF code
Threat:	High: Unknown vulnerabilities in the SEF code could be exploited
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Medium: The SEF is well-known for its design and security, and the vendor is known for responsiveness to security issues.

3. Management Controls

Vulnerability:	Insufficient Disaster Recovery Policy
Threat:	Low: A disaster could visit the datacenter
Exposure:	High: Could result in loss of service.
Risk:	Low: Disasters sufficient to destroy the firewall are statistically rare, and are mitigated by physical and environmental security measures.

Vulnerability:	Insufficient Security Policy control
Threat:	High: If policy can be changed without review, policy may not match the SEF configuration, or may specify an insecure firewall configuration.
Exposure:	High: Could result in loss of service, or data.
Risk:	Medium: Access to the SEF management console is limited, administrators are trained, and changes are relatively rare.

Vulnerability:	Insufficient change controls
Threat:	High: Unauthorized changes could be made to the SEF or underlying OS.
Exposure:	High: Could result in loss of service, or compromise of customer information.
Risk:	Medium: Access controls limit who can make changes to the SEF, but insufficient change management controls could still allow for unauthorized changes.

CURRENT FIREWALL AUDIT PRACTICE

In researching the current state of practice for auditing the SEF, a search for material was conducted of five sources: the Internet, existing SANS practical assignments available at giac.org, SANS course materials, vendor documentation, and personal auditor experience.

INTERNET

The Google search engine was queried with combinations of the terms firewall, audit, best practices, checklists, assessment, Symantec Enterprise Firewall, etc. Though most of the searches yielded only general information on firewall auditing and generic audit checklists, some more specific information was uncovered. Following are descriptions of the most useful URLs found:

- **Canadian Handbook on Information Technology Security:**
  http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf

  This is a very good resource for those who want a good general overview IT security, including threat assessment, risk management, audit methods, and policy management.

- **ICSA Firewall Product Certification Criteria:**
  http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria_3.0a.shtml

  This document has good basic information on "what" to audit. This seems useful especially since the Symantec Enterprise Firewall is ICSA Labs certified.

- **"Auditing Firewalls: A practical Guide:**
  http://www.itsecurity.com/papers/p5.htm

  This document is an excellent overview of firewall auditing.

- **Lance Spitzner's firewall audit paper:**
  http://rootprompt.org/article.php3?article=323

  This paper shows up in many search query results, and is a good technical resource for generic firewall auditing.

- **ITSecurity.com Discussion on Change Control Procedures:**
  http://www.itsecurity.com/asktecs/jul1601.htm

  This paper is very useful in that it discusses the often-neglected are of Change Management for the firewall.

- **Treachery Unlimited – Audit Tools**
  http://www.treachery.net/tools/

  This is a comprehensive clearinghouse of Firewall Audit Tools.

- **UK Security Online – Vulnerability Auditing**
  http://www.uksecurityonline.com/services/vulnerabilityauditing.php

  This site contains some good descriptions and discussions about vulnerability assessment and auditing.

- **Mixter paper on Network Auditing**
  http://mixter.void.ru/auditing.html

  A very good and concise discussion on genera Network Auditing methods.

- **CESG Paper on Symantec Enterprise Firewall audit**
  http://www.cesg.gov.uk/site/iacs/itsec/media/sectarg/symantec7.pdf

  Surprisingly, an audit of this very firewall.

- **IT Auditing without Pain:**
  http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=430
- **Audits from Hell:**
  http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=177

  These two papers provided good real-world auditor experiences and advice.

PREVIOUS GIAC PRACTICALS
A search of the GIAC practicals archive at http://www.giac.org/GSNA.php revealed no specific information for the SEF. However, some contain useful general information that will be used to build an audit checklist.

SANS COURSE MATERIALS
Sections 7.1 (Auditing Principles and Concepts – David Hoelzler), 7.2 (Auditing the Perimeter – David Hoelzler), and 7.4 (Network Auditing Essentials -- John Green) from the SANS Track 7 “Auditing Networks, Perimeters, and Systems” courses provide useful information which may be useful in creating the audit checklist and performing the audit.

VENDOR DOCUMENTATION
Symantec Corporation’s documentation for the SEF does contain some useful configuration information that will be used in building the audit checklist.

ASSIGNMENT 2 – CREATE AN AUDIT CHECKLIST

Before documenting the checklist that will form the basis of the audit, I will first relate the security posture of the SEF as defined in its Security Plan. This posture is defined over four areas: Proxies, Rules Set, Remote Management Access, and VPN Access.

Proxies
As stated earlier, the SEF is an application level firewall; as such, it makes use of *Secure Proxies Services.* Each service is designed to listen for a specific type of connection[1]. One of these services, the G*eneric Service Parser*, is special in that it allows you to create services for protocols not handled by the supplied set of secure proxies[1].

The Secure Proxies description, and run status are:

Secure Proxy	Description	Status
FTPD	FTP Proxy	Enabled
GSPD	Generic Service Parser	Enabled
HTTPD	HTTP Proxy	Enabled
TELNETD	Telnet Proxy	Enabled
CIFSD	CIFS Proxy	Disabled
NBDGRAMD	NetBIOS Datagram Proxy	Disabled
DNSD	DNS Proxy	Enabled
NTPD	Network Time Protocol Proxy	Enabled
NNTPD	Network News Transfer Protocol Proxy	Disabled
SMTPD	Simple Mail Transfer Protocol Proxy	Enabled
PINGD	Ping Proxy	Enabled
RTSPD	Real Time Streaming Protocol Proxy	Disabled
SQLNETD	SQL Network Transfer Proxy	Disabled
H323D	Video Teleconferencing Proxy	Disabled

Rules Set
Earlier I described the various networks that the firewall interfaces to. Once again, they are:

- Outside Network
- Screened subnetwork
- Internal Production Network
- Internal Administrative Network

Traffic allowed between these networks is listed below:

Traffic path	Allowed traffic
Outside – Screened subnet, server 1	HTTP (80, 443), FTP, Ping, SSH
Outside – Screened subnet, server 2	FTP, Ping, SSH
Outside – Production Network	HTTP (port 80, 8080, 8082)
Production Network – Universe	NTP, Syslog
Screened Subnet – Universe	NTP, SMTP, Syslog
Administrative Network -- Universe	HTTP (80, 8088, 8443), NTP, SSH, SMTP, Syslog

Remote Management Console Access
Remote Firewall management access is highly restricted. This access is granted solely to Administrators in the IT organization of the company. Access control is governed by a two-factor authentication scheme requiring a valid IP address and a strong 10 character password, and all management console traffic, including the authentication phase, is passed through an encrypted tunnel. Further, management of the SEF is configured on the internal administrative network interface only, so remote management can be performed only through a private line between the data center and the corporate offices. When Administrators need to manage the SEF after hours, they must do so through the corporate office's SEF over a Triple-DES VPN connection. Finally, as was previously mentioned, there are no remote access capabilities configured for the NT Server itself.

VPN Access
The SEF is not configured for any VPN access.

AUDIT CHECKLIST

This checklist will be broken down into five categories: Policy and Documentation, Physical Security, Firewall Installation and Configuration, Remote Management Console access, and Firewall Rules Validation. The checklist format is derived in part on John Linehan's GSNA practical[2]. References are noted in each item.

Policy and Documentation

Test Number: PD1	Description: Firewall Security Plan Existence		
Reference: Linehan[2], Todd[3], personal experience			
Control objective: Verify Firewall Security Plan exists			
Risk: A firewall Security Plan is required for a firewall to be deployed. In its absence, the firewall configuration is left to Administrator interpretation.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify existence of plan	Plan Exists	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD2	Description: Firewall Security Plan Requirements Review		
Reference: Linehan[2], Todd[3], personal experience			
Control objective: Verify Firewall Plan defines requirements of firewall use.			
Risk: If the firewall Security Plan does not specify the rules of its use, it can be mis-configured and result in unauthorized access, loss of data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify plan defines firewall requirements	Plan defines restrictions on configuration and traffic in a clear manner.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD3	Description: Firewall Security Plan Comprehension		
Reference: Linehan[2], Todd[3], personal experience			
Control objective: Verify Firewall Security Plan is understood by Administrators			
Risk: A firewall Security Plan must be understood by those implementing the firewall, otherwise the Administrators will make their own decisions as to how to configure it.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify Administrators understand plan.	An interview with the Administrator(s) leaves the auditor with confidence that the Administrator understands the plan.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD4	Description: Change Management Policy Existence		
Reference: Linehan[2], ITSecurity AskTecs[4], personal experience			
Control objective: Verify presence of Change Management system as it pertains to the firewall.			
Risk: a lack of change control process for the firewall can result in undocumented changes. These changes are difficult to roll back in case of unexpected results, and can result in loss of data or confidence of customers.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify presence of Change Management Process, including policy and procedures.	Change Management Policy, procedures, and processes exist.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD5	Description: Change Management Policy Review		
Reference: Linehan[2], ITSecurity AskTecs[4], personal experience			
Control objective: Verify presence and effectiveness of Change Management system as it pertains to the firewall.			
Risk: An incomplete change management process could leave opportunities for unauthorized changes to firewall, resulting in loss of data or confidence of customers.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify the process defines: • who can request changes • in what forum the changes are considered • who can authorize them • change documentation requirements	A review of the documentation should reveal who can request changes; the change control review process, including required participants; who in the organization signs off the change; and a documented change plan, including a backout procedure, and a configuration backup procedure (backup procedure should create a configuration backup to a remote machine).	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD6	Description: Change Management Policy Comprehension		
Reference: Linehan[2], ITSecurity AskTecs[4], personal experience			
Control objective: Verify Change Management system is understood by Administrators.			
Risk: If Administrators do not understand the policy and process, they could make innocent but dangerous modifications to the firewall, which might result in destruction of the firewall, loss of configuration, Denial of Service, or unauthorized access.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify the Administrator(s) understand and follow the Change Management policy and procedures.	An interview with the Administrator(s) leaves the auditor confident that the policy and procedures are understood and followed.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD7	Description: SEF Installation Documentation Existence		
Reference: Linehan[2], Symantec Enterprise Firewall Install Guide v7.0 for Windows[5], personal experience			
Control objective: Ensure the documentation for installing the SEF exists.			
Risk: This documentation is critical if a disaster visits the firewall, requiring a complete re-install of the OS and SEF.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Locate Installation Manuals for SEF.	Administrator(s) should be able to locate current manuals for SEF installation. Manuals should be located near the SEF (at least in the same building).	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD8	Description: SEF Installation Documentation Comprehension		
Reference: Linehan[2], Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the documentation for installing the SEF is understood.			
Risk: Understanding how to re-install the firewall under pressure is critical for a rapid recovery of service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Interview Administrator(s) to verify Installation steps are understood by Administrator(s)	Administrator should demonstrate that the manual is clear and understood.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD9	Description: Disaster Recovery Plan Existence		
Reference: Linehan[2], personal experience			
Control objective: Verify presence of firewall Disaster Recovery Plan.			
Risk: A lack of a firewall Disaster Recovery Plan could result in a much longer recovery window, and result in extended loss of service to the application.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify presence of firewall Disaster Recovery Plan.	Plan exists	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD10	Description: Firewall Disaster Recovery Plan Review		
Reference: Linehan[2], personal experience			
Control objective: Verify completeness of Disaster Recovery Plan for firewall.			
Risk: An incomplete Disaster Recovery Plan could prolong recovery and result in extended loss of service in the event of a failure.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Review the firewall's Disaster Recovery Plan.	Verify the process defines: • how often the system is backed up • how the system is backed up. • how the system is recovered. • who can declare a firewall disaster • who is notified	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PD11	Description: Firewall Disaster Recovery Plan Comprehension		
Reference: Linehan[2], personal experience			
Control objective: Verify Disaster Recovery Plan is understood by Administrators.			
Risk: If Administrators do not understand this Plan, they could make mistakes during a crisis, resulting in lengthened recovery windows.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Interview the Administrator(s), learning what they know about the Disaster recovery Plan for the firewall.	Verify the Administrator(s) understand the Disaster Recovery Plan.	S	
Completed by:	Signature:	Date:	
Comments:			

Physical Security

Test Number: PS1	Description: Location of Firewall		
Reference: Linehan[2], personal experience			
Control objective: Verify firewall is installed in a secure environment			
Risk: If the firewall is in an insecure environment, it can be exposed to unauthorized change, physical damage, accidental Denial of Service, or loss of Environmental Support (Cooling, Power, etc.)			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Identify location of firewall	Firewall should be installed in a locked cabinet, or in a locked room.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PS2	Description: Firewall Access Control Policy		
Reference: Linehan[2], personal experience			
Control objective: Verify firewall access is limited to a defined set of personnel.			
Risk: If the firewall is in an insecure environment, it can be exposed to unauthorized change, physical damage, accidental Denial of Service, or loss of Environmental Support (Cooling, Power, etc.)			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Review access control policy.	An interview with personnel responsible for the physical security of the facility should discover: • A list of persons with authorized access to the firewall; • A list of persons who can modify the access control list; • Sufficient logging and monitoring mechanisms (log sheets, cameras, motion sensors) to verify who currently has (or has had) access to the firewall; • Access tokens such as "swipe' badges to control access to the room the firewall is in; • If firewall is in a locked cage, keys should be access controlled.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PS3	Description: Environmental Systems Validation		
Reference: Linehan[2], personal experience			
Control objective: Verify firewall is supported by sufficiently redundant environmental systems.			
Risk: If the firewall is in an insecure environment, it can be exposed to unauthorized change, physical damage, accidental Denial of Service, or loss of Environmental Support (Cooling, Power, etc.)			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Review Environmental Systems	An interview with data center personnel and a walkthrough of the facility should reveal: • Redundant power systems, including (at minimum) UPS and (preferably) backup power generation systems; • Sufficient Air Conditioning support the size of the room, and preferably redundant Air Conditioning systems. • Fire suppression systems, preferably an early smoke detection system.	S	
Completed by:	Signature:	Date:	
Comments:			

Test Number: PS4	Description: Physical Security Test		
Reference: Linehan[2], personal experience			
Control objective: Verify you cannot gain unauthorized access to the firewall.			
Risk: If the firewall is in an insecure environment, it can be exposed to unauthorized change, physical damage, accidental Denial of Service, or loss of Environmental Support (Cooling, Power, etc.)			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Attempt access to firewall location by attempting to open doors into the data center computing room.	Access should not be possible without explicit access being granted.	O	
Completed by:	Signature:	Date:	
Comments:			

Firewall Installation and Configuration

Test Number: FIC1	Description: NT Server Hardening – Service Pack Level		
Reference: Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the Server OS is at the proper Service Pack level.			
Risk: If the firewall is not properly hardened, the SEF could fail to protect the resources it is configured to protect, possibly resulting in unauthorized access or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Determine Service Pack level of the server.	Server should be patched to NT Service Pack 6a	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FIC2	Description: NT Server Hardening – Administrative Password setting		
Reference: Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the Server OS has a strong password set for the Administrator login, and that the screen saver is active and password-protected.			
Risk: If the firewall is not properly hardened, the SEF could fail to protect the resources it is configured to protect, possibly resulting in unauthorized access or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Check for password set for Administrative login to Server.	• Server Administrative login should not accept a zero-length password. • Password must be a minimum of 8-characters, mixed case and numbers.	O	
2. Test for a password prompt after interrupting the screen saver.	The screen saver should come on after 15 minutes of inactivity, and a password prompt should be displayed upon interrupting the screen saver.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FIC3	Description: NT Server Hardening – File System Verification		
Reference: Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the Firewall software is installed on an NTFS partition.			
Risk: If the firewall is not properly hardened, the SEF could fail to protect the resources it is configured to protect, possibly resulting in unauthorized access or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Determine Server's File System type by browsing the 'Drive Administrator' tool.	File System type should be NTFS	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FIC4	Description: NT Server Hardening – NIC Setup		
Reference: Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the Network Interface Cards (NICs) are properly configured for the firewall.			
Risk: If the firewall is not properly hardened, the SEF could fail to protect the resources it is configured to protect, possibly resulting in unauthorized access or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Identify the NIC configurations.	The NICs should be configured as follows: • Only TCP protocol configured. • Only static routes required for the firewall to locate hosts it is protecting should be configured. The Administrator should justify each route on the firewall server. • Only the external interface should have a default route assigned. • DNS address should be blank. • WINS address should be blank. • 'Enable DNS for WINS resolution' should be checked. • 'Enable LMHOSTS Lookup' should be unchecked.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FIC5	Description: Firewall Patch Management		
Reference: Symantec Enterprise Firewall Install Guide v7.0 for Windows[5]			
Control objective: Ensure the firewall is current with the latest patches from Symantec.			
Risk: If the firewall is not patched, it could be exposing a vulnerability that could be exploited, resulting in unauthorized access, Denial of Service, or data loss.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Identify current patch level of firewall.	The firewall has the most current patches installed.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FIC6	Description: Firewall Secure Proxy Status		
Reference: Security Plan			
Control objective: Ensure the firewall is only using the Secure Proxies allowed by the Security Plan for the firewall.			
Risk: If proxies are left enabled, they are a potential vulnerability that may be exploited, resulting in unauthorized access, Denial of Service, or data loss.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify that only necessary Proxies are enabled.	The following Secure Proxies should be enabled: • FTPD • GSPD • HTTPD • TELNETD • DNSD • NTPD • SMTPD • PINGD	O	
Completed by:	Signature:	Date:	
Comments:			

Remote Management Console Access

Test Number: RMC1	Description: Remote Management Console access		
Reference: Personal experience			
Control objective: To establish that the SEF is configured to grant remote management access only to authorized Administrators.			
Risk: Unauthorized access to the firewall remote management console could result in unauthorized changes or malicious alteration of the firewall, resulting in reduced security or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify the access control list for the Remote Management console on the firewall.	• Only Administrators' workstations should be configured to access the firewall Management console. • No wildcard IP addresses should be configured. • The password for each entry must be 10 characters minimum, mixed-case letters and numbers.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: RMC2	Description: Remote Management Console access		
Reference: Personal experience			
Control objective: To establish that the Remote Management Console client software is securely stored.			
Risk: Unauthorized access to this software would make an attempt to connect to the firewall possible.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify the client software for the Remote Management Console is secured in a locked cabinet or room.	The software should only be accessible by the Administrators and Security personnel.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: RMC3	Description: Remote Management Console access		
Reference: Personal experience			
Control objective: To establish that the firewall is configured to provide remote access via internal interfaces only.			
Risk: It is much more secure to keep the Remote Management capability off of the open Internet. By keeping Remote Management sessions over internal interfaces only, would-be attackers would have to break into the corporate office SEF before they could even attempt to gain a remote Management session on this SEF.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On a workstation with the Remote Management Console client installed, attempt to connect to the outside interface of the firewall.	Only internal interfaces can be configured for remote management access. The external interface must NEVER be configured for remote management access. Access should be denied.	O	
Completed by:	Signature:	Date:	
Comments:			

Firewall Rules Validation

Test Number: FV1	Description: Firewall Rule Validation (Outside Network to screened subnet server 1)		
Reference: Firewall Security Plan, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ftp (TCP 21) • http (TCP 80, 443 • ssh2 (TCP 22) • ping	O	
2. On the laptop: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against server1 from outside the firewall. On server1: Run tcpdump, configured to capture the traffic from the laptop IP address.	The tcpdump output should show traffic received from the laptop on: • TCP: 21, 22, 80, and 443.	O	
3. On the laptop: Ping server 1.	Verify a successful ping response.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FV2	Description: Firewall Rule Validation (Outside Network to screened subnet server 2)		
Reference: Firewall Security Plan, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ftp (TCP 21) • ssh2 (TCP 22) • ping	O	
2. On the laptop: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against server2 from outside the firewall. On server2: Run tcpdump, configured to capture the traffic from the laptop IP address.	The tcpdump output should show traffic received from the laptop on: • UDP: 20, 22.	O	
3. On the laptop: Ping server 2.	Verify a successful ping response.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FV3	Description: Firewall Rule Validation (Outside Network to Production Network)		
Reference: Firewall Security Plan, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • http (TCP 80, 8080, 8082)	O	
2. On the laptop: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against the outside interface of the firewall. On the firewall: Run tcpdump to listen on the internal Production interface, configured to capture the traffic incoming traffic.	The tcpdump output should show traffic received from the laptop on: • TCP: 80, 8080, 8082	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FV4	Description: Firewall Rule Validation (Production Network to Universe)		
Reference: Firewall Security Plan, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ntp (UDP 123) • syslog (UDP 514)	O	
2. On a Production Network host: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against a host on each of the other networks (Administrative, Screened subnet, Outside). On each host: Run tcpdump, configured to capture the traffic from the production host IP address.	The tcpdump output should show traffic received from the laptop on: • UDP: 123 and 514	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FV5	Description: Firewall Rule Validation (Screened subnet to Universe)		
Reference: Company security policy, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ntp (UDP 123) • syslog (UDP 514) • SMTP (TCP 25)	O	
2. On a Screened subnet host: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against a host on each of the other networks (Administrative, Production, Outside). On each host: Run tcpdump, configured to capture the traffic from the screened subnet host IP address.	The tcpdump output should show traffic received from the host on: • UDP 123 and 514 • TCP 25.	O	
Completed by:	Signature:	Date:	
Comments:			

Test Number: FV6	Description: Firewall Rule Validation (Administrative Network to Universe)		
Reference: Company security policy, Green[6]			
Control objective: To confirm that only traffic defined by the Firewall Security Plan is configured on the firewall.			
Risk: If traffic is allowed that is not defined by the Security Plan, vulnerabilities may be exposed to attack, resulting in loss of data, unauthorized access to data, or Denial of Service.			
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ntp (UDP 123) • syslog (UDP 514) • SMTP (TCP 25) • SSH (TCP 22)	O	
2. On an Administrative network host: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against a host on each of the other networks (Screened subnet, Production, Outside). On each host: Run tcpdump, configured to capture the traffic from the administrative host IP address.	The tcpdump output should show traffic received from the host on: • UDP: 123, 514 • TCP: 80, 8088, 8443, 25 and 22.	O	
Completed by:	Signature:	Date:	
Comments:			

ASSIGNMENT 3 – AUDIT EVIDENCE

Prior to writing this section, the Audit was conducted against the SEF. All commands run on computers were executed by an Administrator allocated for the audit.

From the complete audit checklist, the following audit checklist items are presented. Some are selected for the instructive value of demonstrating the audit step, others because they support audit findings pertinent to the Audit Report in Assignment 4.

Port Scanning Notes

The parts of the audit that test network traffic make use of two tools: **nmap** (http://www.insecure.org/nmap), a well known port scanning tool; and tcpdump (http://www.tcpdump.org), a well known packet capture and analysis tool. Further, as noted by Green[6], the only sure way to port scan through a Proxy firewall is to use nmap's '-sT' switch. This invokes the 'connect() scan' option, telling nmap to attempt a full TCP handshake with the target. In the absence of this option, the firewall will simply drop the nmap-generated packet. This method is used for all TCP scans.

SELECTED AUDIT ITEMS

Test Number: PD1	Description: Firewall Security Plan Existence		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify existence of SEF Security Plan	Plan Exists	O	Fail

Audit Item PD1.1: Firewall Security Policy Existence -- FAIL

When queried, only management knew the location of the Security Plan that defines the SEF's security. This is due the fact that the Information Security Policy is still in roll-out phase, and is not yet widely spread throughout the company. Administrators were not familiar with it.

Test Number: PD3	Description: Firewall Security Plan Comprehension		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify Administrators understand Firewall policy.	An interview with the Administrator(s) leaves the auditor with confidence that the Administrator understands the spirit of the Policy.	S	Fail

Audit Item PD3.1: Firewall Security Plan Comprehension -- FAIL
Since the Security Plan is rather new in the company, the Administrators understand the spirit of the Security Plan intuitively, but are not particularly aware of its contents. The Plan needs a more public rollout to be effective.

Test Number: PD4	Description: Change Management Policy Existence		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify presence of Change Management Process, including policy and procedures.	Change Management policy, procedures, and process exists.	O	Fail

Audit Item PD4.1: Change Management Policy Existence -- FAIL
The company currently has no formal Change Management Process or Policy. Rather, it used an informal system of notification, change documentation, and peer review. It would be beneficial to formalize this process, since the current one does not scale beyond more than a few people.

Test Number: PD7	Description: SEF Installation Documentation Existence		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Locate Installation Manuals for SEF.	Administrator(s) should be able to locate current manuals for SEF installation. Manuals should be located near the SEF (at least in the same building).	O	Fail

Audit Item PD7.1: SEF Installation Documentation Existence -- FAIL
Though the SEF documentation exists, it is in a building two miles away from the site where a recovery would take place. This documentation should be moved to the data center that houses the SEF.

Test Number: PD9	Description: Disaster Recovery Plan Existence		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify presence of firewall Disaster Recovery Plan.	Plan exists.	O	Fail

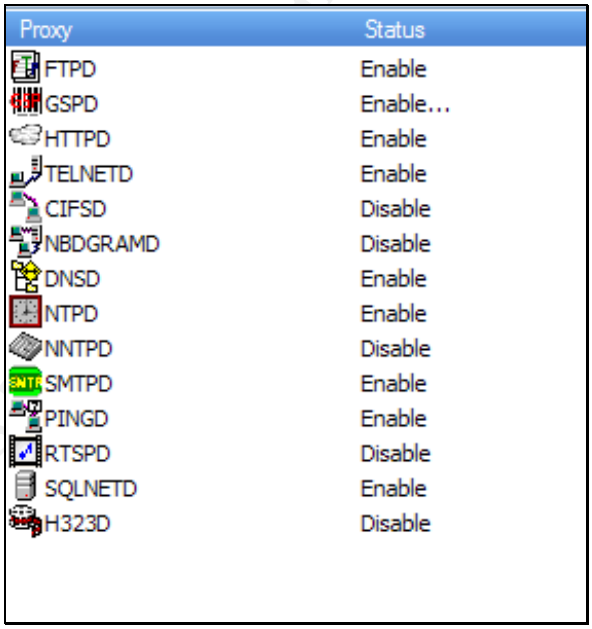
Audit Item PD9.1: Disaster Recovery Plan Existence -- FAIL
There is no Disaster Recovery Plan in existence for the firewall. It is recommended this be remedied, or at the very least, start a regiment of periodic backups of the firewall configuration.

Test Number: FIC5	Description: Firewall Patch Management		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Identify current patch level of firewall.	The firewall has the most current patches installed.	O	FAIL

Audit Item FIC5.1: Firewall Patch Management—FAIL
The firewall was found to be down rev. by one patch level, according to Symantec Technical Support. Further, there is no simple way to discover the current patch level of the firewall. The only current option offered is to compare file system time stamps.

Test Number: FIC6	Description: Firewall Secure Proxy Status		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify that only necessary Proxies are enabled.	The following Secure Proxies should be enabled: • FTPD • GSPD • HTTPD • TELNETD • DNSD • NTPD • SMTPD • PINGD	O	

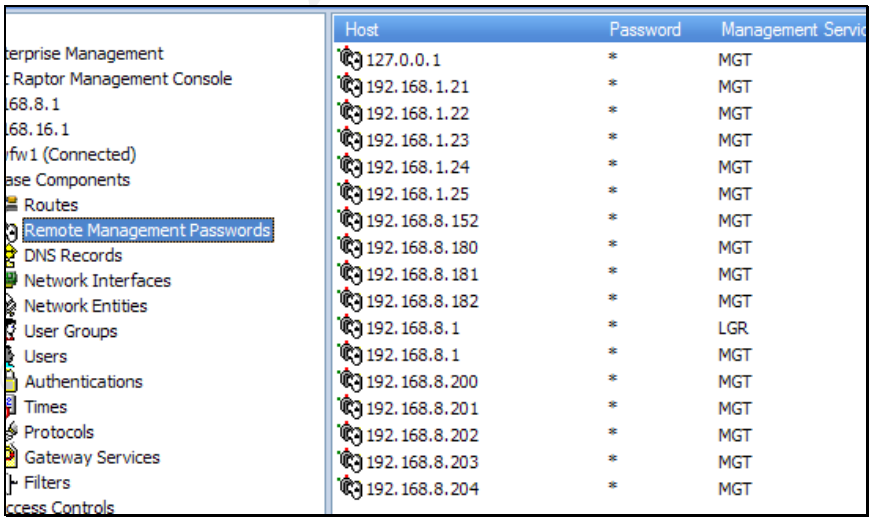
Audit Item FIC6.1: Firewall Secure Proxy Status -- FAIL
The firewall was configured such that certain unnecessary Secure Proxies were enabled:



The following Secure Proxies should be disabled until the business requires them: SQLNETD

Test Number: RMC1	Description: Remote Management Console access		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. Verify the access control list for the Remote Management console on the firewall.	• Only Administrators' workstations should be configured to access the firewall Management console. • No wildcard IP addresses should be configured. • The password for each entry must be 10 characters minimum, mixed-case letters and numbers.	O	Fail

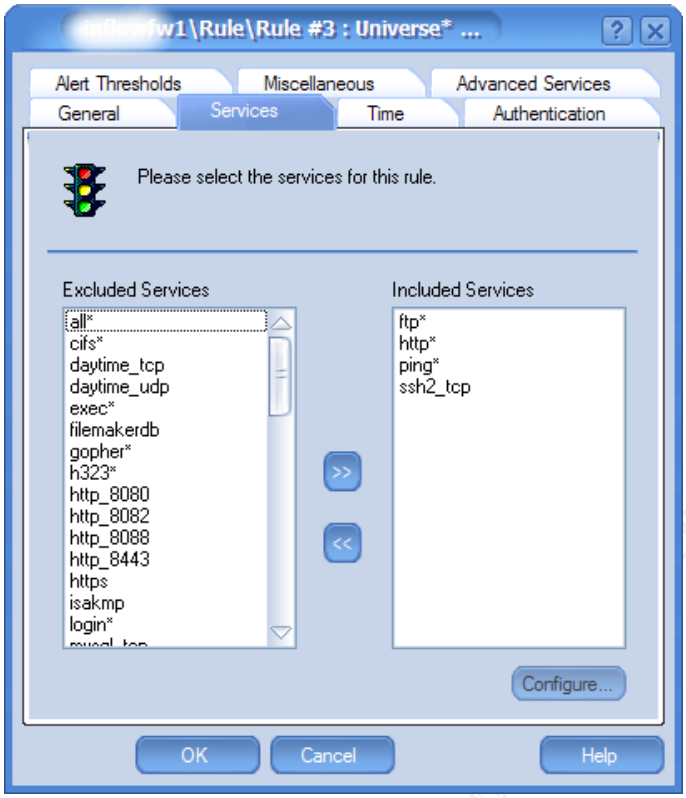
Audit Item RMC1.1: Remote Management Console access -- FAIL
Upon inspecting the firewall Remote Management Console configuration and interviewing the Administrator, it was determined that there were a number of old entries from previous Administrator workstations and home PCs:



It is advised to remove these 'orphaned' entries to reduce the possibility (albeit rare) of an exploit through these points of access.

Test Number: FV1	Description: Firewall Rule Validation (Outside Network to screened subnet server 1)		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ftp (TCP 21) • http (TCP 80, 443 • ssh2 (TCP 22) • ping	O	Pass
2. On the laptop: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against server1 from outside the firewall. On server1: Run tcpdump, configured to capture the traffic from the laptop IP address.	The tcpdump output should show traffic received from the laptop on: • TCP: 21, 22, 80, and 443.	O	Fail
3. On the laptop: Ping server 1.	Verify a successful ping response.	O	Pass

Audit Item FV1.1: Verify Rule Configuration - PASS
This audit step was performed by checking the rule configuration via the remote management console:



FV1.2: Port Scan Tests -- FAIL
As is noted in the checklist item FV1, the basic process employed to verify compliance are to place a system at the outside of the firewall (preferably plugged directly into the border switch), and configure it scan "Server 1" on the Screened subnet using **nmap**. "Server 1" will be listening for packets from the nmap host using tcpdump. The system is scanned for open TCP and UDP ports.

- TCP Scan: **`nmap -sT -P0 ww.xx.yy.zzz`**

```
[root@www root]# tcpdump -nn -t src host 68.7.xx.yyy
tcpdump: listening on eth0
68.7.xx.yyy.2894 > ww.xx.yy.zzz.22: S 2803849522:2803849522(0) win 8192 <mss 1460> (DF)
68.7.xx.yyy.2894 > ww.xx.yy.zzz.22: . ack 2025773791 win 8760 (DF)
68.7.xx.yyy.2894 > ww.xx.yy.zzz.22: . ack 2 win 8760 (DF)
68.7.xx.yyy.2894 > ww.xx.yy.zzz.22: . ack 33 win 64588 (DF)
```

- UDP Scan: **`nmap -sU -P0 ww.xx.yy.zzz`**

```
[root@www root]# tcpdump -nn -t src host 68.7.xx.yyy
tcpdump: listening on eth0
```

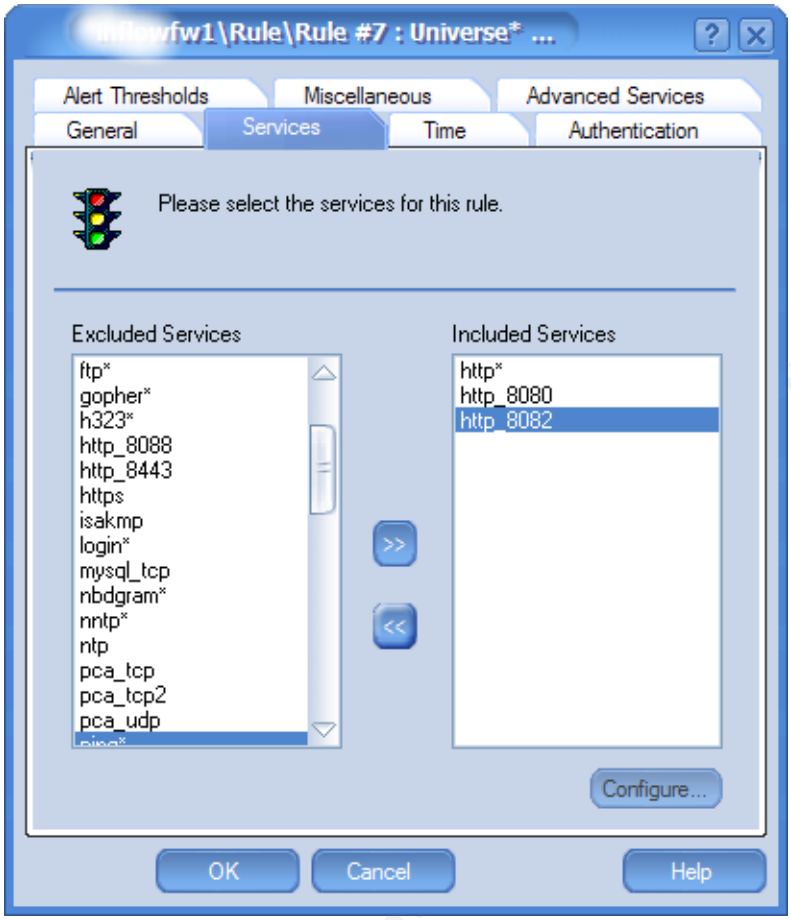
It was interesting to observe that the HTTP, HTTPS, and FTP nmap packets did not pass through the firewall to the host. A check with Symantec Technical Support revealed that this was in fact the case in their test lab as well. This appears to affect all Secure Proxy Services (except for the Generic Service Parser-based services, which pass through nmap traffic fine). Whether it is a bug or a 'feature' was not clarified at the time of this audit. Nevertheless, these protocols do pass through under normal circumstances (Customer FTP transactions, and HTTP browser queries work fine). So, the FAIL grade is procedural and illustrative only.

FV1.3: Ping Test -- PASS
This was tested with a using the 'ping' command from the host on the outside network.

```
C:\>ping ww.xx.yy.zzz

Pinging ww.xx.yy.zzz with 32 bytes of data:

Reply from ww.xx.yy.zzz: bytes=32 time=17ms TTL=118
Reply from ww.xx.yy.zzz: bytes=32 time=14ms TTL=118
Reply from ww.xx.yy.zzz: bytes=32 time=14ms TTL=118
Reply from ww.xx.yy.zzz: bytes=32 time=15ms TTL=118

Ping statistics for ww.xx.yy.zzz:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Test Number: FV3	Description: Firewall Rule Validation (Outside Network to Production Network)		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • http (TCP 80, 8080, 8082)	O	Pass
2. On the laptop: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against the outside interface of the firewall. On the firewall: Run tcpdump to listen on the internal Production interface, configured to capture the traffic from the laptop IP address.	The tcpdump output should show traffic received from the laptop on: • TCP: 80, 8080, 8082	O	Fail

Audit Step FV3.1: Verify Rule Configuration -- PASS
Again, this audit step was performed by checking the rule configuration via the remote management console:



FV3.2: Port Scan Tests -- FAIL
This scan was a little different based on how this network is used. In this case, HTTP traffic is directed to the outside address of the firewall, and is redirected to the load balancing device directly connected to the firewall, where it is dispatched to myriad servers sitting behind the device. Only HTTP traffic on the specific ports is configured for redirection. The same basic process port scanning process is employed here, except that tcpdump runs on the firewall, listening on the internal Production interface. So, I place a system at the outside of the firewall (again, preferably plugged directly into the border switch), and configure it to scan the outside interface of the firewall using **nmap**. The firewall will be listening for packets from the nmap host using tcpdump, configured to listen on the internal interface. The system is scanned for open TCP and UDP ports.

- TCP Scan: **`nmap -sT -P0 ww.xx.yy.zzz`** (outside address of the firewall)

```
[root@www root]# tcpdump -nn -t -i ww.xx.yy.zzy dst host 192.168.120.2
tcpdump: listening on eth0y.zzz.22: . ack 33 win 64588 (DF)
```

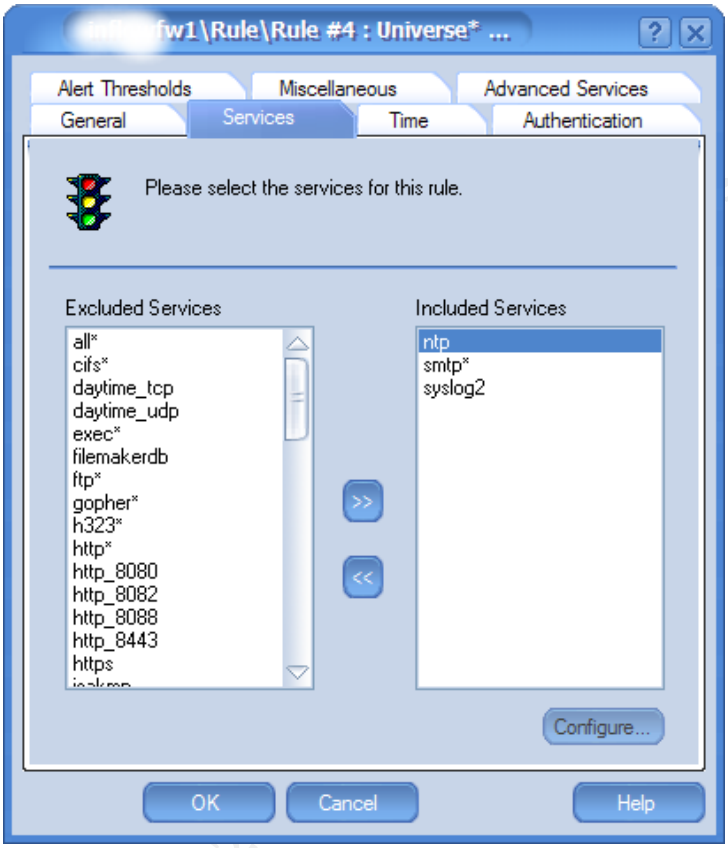
- UDP Scan: **`nmap -sU -P0 ww.xx.yy.zzz`** (outside address of the firewall)

```
[root@www root]# tcpdump -nn -t -i ww.xx.yy.zzy dst host 192.168.120.2
tcpdump: listening on eth0
```

We get the same affect as in FV1.2 owing to the Secure HTTP Proxy, so we see no nmap packets. It was verified that normal application traffic was passing through just fine: a failure to do so would mean loss of service for all customers, a condition I would know about in approx. 1.5 minutes. So, again a procedural FAIL only.

Test Number: FV5	Description: Firewall Rule Validation (Screened subnet to Universe)		
Test Procedure			
Test Steps	Compliance Criteria	O/S	Pass/Fail
1. On the remote management console, verify the allowed services for this rule.	The rule should show that the following services are enabled: • ntp (UDP 123) • syslog (UDP 514) • SMTP (TCP 25)	O	
2. On a Screened subnet host: Run NMAP in TCP connect() port scan mode (using the '-sT' switch) and in UDP port scan mode (using the '–sU' switch) against a host on each of the other networks (Administrative, Production, Outside). On each host: Run tcpdump, configured to capture the traffic from the laptop IP address.	The tcpdump output should show traffic received from the host on: • UDP 123 and 514 • TCP 25.	O	

Audit Item FV5.1: Verify Rule Configuration - PASS
This audit step was performed by checking the rule configuration via the remote management console:



FV5.2: Port Scan Tests -- PASS
As is noted in the checklist item FV5, testing this path involves configuring a system on the screened subnet to scan a host on the Administrative network using **nmap**. The Administrative host will be listening for packets from the nmap host using tcpdump. The system is scanned for open TCP and UDP ports.

- TCP Scan: **`nmap -sT -P0 192.168.16.30`**

```
[root@bu1 root]# tcpdump -t -nn src host 192.168.16.1
tcpdump: listening on eth0
192.168.16.1.14786 > 192.168.16.30.25: S 1144400155:1144400155(0) win 8192 <mss 1460>
(DF)
192.168.16.1.14786 > 192.168.16.30.25: S 3307921995:3307921995(0) win 8192 <mss 1460>
(DF)
192.168.16.1.14786 > 192.168.16.30.25: S 1890509573:1890509573(0) win 8192 <mss 1460>
(DF)
192.168.16.1.14786 > 192.168.16.30.25: S 1135163644:1135163644(0) win 8192 <mss 1460>
(DF)
```

- UDP Scan: **`nmap -sU -P0 192.168.16.30`**

```
[root@bu1 root]# tcpdump -t -nn src host ww.xx.yy.zz
tcpdump: listening on eth0
ww.xx.yy.zz.30872 > 192.168.16.30.514:  udp 0
ww.xx.yy.zz.30873 > 192.168.16.30.514:  udp 0
ww.xx.yy.zz.30874 > 192.168.16.30.123:  [len=0] v0 unspec strat 0 poll 0 prec 0
ww.xx.yy.zz.30875 > 192.168.16.30.123:  [len=0] v0 unspec strat 0 poll 0 prec 0
```

Two interesting things appeared from this test. First, port 25 came through, though it is over the Secure Proxy Service SMTPD. Symantec is aware of this and has not concluded testing as of this audit (you will recall the assertion that Secure Proxies do not pass nmap packets). Second, for the TCP Scan the listening host needed to listen for packets sourced from the Administrative Network's firewall interface, 192.168.16.1. The UDP scan did not require this, and was configured to listen for packets coming from the screened subnet host.

Residual Risk

The greatest risk revealed by this audit is the lack of a defined and documented Change Management Process, a lack of a well-publicized firewall Security plan, and a lack of a firewall Disaster Recovery Plan. Were these to exist, their presence would effectively eliminate nearly all of findings of this audit.

The lack of a well-publicized firewall Security Plan is not too concerning, as the Client only recently drafted their Information Security Policy, and is still in the roll-out phase.

The Disaster Recovery Plan document would be somewhat time-consuming to produce and validate. The lack of a Disaster Recovery Plan can be mitigated by putting in place a system of periodic backups of the firewall configuration. If periodic backups are not possible, then a backup could be mandated after each change.

The Change Management Process would require a bit more work to deploy. Draft documentation alone would require more than a person week (maybe two). Given the scarcity of resources for such a project, and the relatively low impact on security of the lack of such a process, it is not likely that this will get top priority. However, I vigorously recommend that it be addressed as soon as is humanly possible.

Beyond the Change Management, Security Plan, and Disaster Recovery Plan findings, no security flaws were uncovered in the firewall itself, and the remaining audit findings are relatively harmless. Most can be mediated by simply correcting the configurations, except for one: the lack of a patch management system within the product. Not being able to readily identify which patches are installed on the firewall is significant, as it makes it difficult to know at a glance if you are current. To mediate this, it is necessary to begin tracking the installed patches, and keep

up with the Symantec notices. Another form of mediation would be an Intrusion Detection System, or a Penetration Testing system that would regularly test the system for known vulnerabilities.

Auditability
For the most part, this firewall, based on the documented audit checklist, is auditable. Given this, areas of high subjectivity, such as 'comprehension' of policies and plans, requires a bit of skill on the part of the Auditor to verify. Nevertheless, it can be verified to a reasonable degree. Also, patch level verification is currently trickier than it should be, and password length for the remote management console entries can not be verified after they are created. Finally, the issues that arose surrounding how Secure Proxy Services (other than GSPD and SMTPD) treat nmap packets, made auditing these items difficult.

ASSIGNMENT 4 – AUDIT REPORT

Executive Summary
This audit was conducted on the Symantec Enterprise Firewall v7.0 for Windows. The firewall under audit was installed on a Windows NT Server, patched to Service Pack 6a. This firewall is used to protect the Client's Internet Analytics business.

The objective for this audit was to examine the process, policy and procedure directly relevant to the firewall operation and configuration, the physical environment the firewall is installed in, the access controls placed on the means of managing and configuring the firewall, and the ability for the firewall to protect the resources it was commissioned to protect. This objective was achieved.

The audit found that the firewall is a very good firewall, but it is poorly supported with the necessary policy and procedure to ensure proper configuration and best practice operation. Most notably absent are a Change Management Policy and Process, and a Disaster Recovery Plan for the firewall. It should be noted, that despite the absence of these items, the firewall has been remarkably well managed and implemented, as shown by the findings (and lack thereof) that follow.

Audit Findings

1. Security Plan for firewall is not well known outside of Management.

   Though the audit did verify the existence of the Security Plan for the firewall (**Audit Item PD1.1**), it was only through interviews with the IT Manager that it was located. Administrators were only 'anecdotally' aware of its existence

(**Audit Item PD3.1**). The IT Manager explained that the Information Security Policy for the Company had only recently been commissioned, and had not yet been rolled out.

The risk of Policy existing in this nebulous state is that the people who need to be implementing the policy---in this case, the Administrators--- are left no option but to configure the firewall to the best of their knowledge, with an unknown amount of business input into the process. This could result in the firewall being unintentionally configured in such a way that it exposes Customer data to unauthorized access, deletion, or loss of legitimate access.

2. No Change Management Policy or Process exists to support the firewall

   The audit revealed that there is no formal Change Management Policy or Process in place at the Company (**Audit Item PD4.1**). In its place are informal communications and change logs maintained between the Administrators.

   Some risks of not implementing a formal Change Management Policy and Process are:
   - Changes can be made that may not agree with business interests
   - Such changes are not subjected to critical technical review
   - Such changes are not guaranteed to have a backout plan in case of unexpected results.
   - Such changes are not guaranteed to be documented for audit trail purposes.

3. Firewall Installation documentation not located near firewall

   It was found during the audit (**Audit Item PD7.1**) that though the Installation Documentation for the firewall exists, it is located far away from the data center where the firewall is installed.

   In a disaster recovery event, where the firewall is completely destroyed, it is crucial that the Administrator responding to such a disaster is not burdened with locating documentation such as this. It is hard enough waking up at 3:30 a.m., trying to get your bearings while driving to a data center with one eye open; one should not be searching for the tools needed to perform the recovery. Not doing so will unnecessarily prolong the recovery process, and may incur ill will and lost confidence from customers who cannot access their data.

4. Disaster Recovery Plan for firewall does not exist

   Audit Item PD9.1 revealed that there is no Disaster Recovery Plan in existence. Not having one is a real threat for the Company's Internet business. Should the firewall be destroyed, it would take much longer to mobilize a recovery response in the absence of such a plan, and the recovery will be far from optimal. Not only would customers be upset at the prolonged outage, but the firewall configuration may be restored to a less-optimal security level, possibly exposing the customers' data.

5. The firewall lacks a graphical means of identifying its patch level

   Audit Item FIC5.1 revealed that this firewall lacks a simple way to identify which patches are installed on the firewall. It is very important that an Administrator is able to identify this critical piece of information. Without such a means, one could either re-install a patch that is already in place, wasting time, or assume a patch is installed that is not, exposing a vulnerability to the firewall that could lead to unauthorized access to customer data, data loss, or loss of access to such data.

6. Secure Proxies were not configured per the firewall Security Plan

   Audit Item FIC6.1 identified that the SQLNETD Secure Proxy was enabled, though it was identified as a disabled service in the Firewall Security Plan. An interview with an Administrator revealed that it had been turned on for a test, and was never disabled after the test.

   Again, a Change Management Process would have caught this. The relative risk of this to the system was low however, since the proxy was turned on, but no rules were configured to use it.

7. Unnecessary Remote Management Console entries were configured

   Audit Item RMC1.1 identified a number of entries in the firewall's remote management console that did not correspond to current Administrator workstation IP addresses. Upon interviewing an Administrator, the extra entries were identified as old IP addresses that had not been removed when workstations changed IP addresses or were re-deployed.

   The risk of this finding is relatively low, because remote access requires a valid IP, a valid password, and a machine configured to communicate over the company's private line to the data center. Hence, a remote management console session over the Internet requires a VPN connection through the

Company's corporate firewall. Remote management console access is not allowed directly through the external interface of this firewall.

8. Firewall Secure Proxies do not allow nmap-generated traffic to pass

   Audit Items FV1.2 and FV3.2 revealed that the Symantec Enterprise Firewall v7.0 has an unexpected behavior: The Secure Proxy Services (except for GSPD and SMTPD) do not pass nmap-generated traffic through the firewall. This was communicated to Symantec, and the behavior was reproduced in their Lab environment. This behavior does not affect normal traffic, such as customer FTP sessions, HTTP browser sessions, or SMTP mail sessions. There is currently no remedy for this behavior at the time of this audit.

   There is low risk resulting from this behavior, since all of the traffic that was suppressed was actually traffic the Client WANTS to pass through. The Administrators should stay on top of this issue, however, following the case opened with Symantec Technical Support.

Audit recommendations

1. **Remove old Remote Management Console entries and disable the SQLNETD proxy**

   These are low cost actions that could be implemented right away. However, this does not resolve the root cause problem, which is a lack of Change Management Policy and Process.

2. **Relocate Firewall Installation documentation to the data center, and take regular backups of the firewall configuration**

   These too are low cost actions that would yield simple yet significant benefits when the time comes to recover a failed firewall. Ideally, these would become part of a Disaster Recovery Plan for the firewall.

3. **Implement a Change Management system to control firewall changes**

   Lack of a change management system to control changes to the firewall is responsible for most of the audit findings. Implementing one is no small affair, though it need not be extremely costly. Since the company is small and has only three Administrators, the job of creating such a system, and selling it to the users of the system, is achievable in my opinion. It would probably take no more than a few weeks of a person's time to implement

it. The rewards would be far reaching though, so the decision to undertake such a project should be given serious consideration.

4. Write a Disaster Recovery Plan for the firewall

From my conversations with IT Management, the Disaster Recovery Plan was always meant to follow the creation of the Security Plan drafted for the firewall at the time of System Accreditation. If this is the case, it would be very beneficial to undertake this action. The cost of such an action would probably amount to few person-weeks of effort, and the Plan would not need to be overly extensive. It just needs to be effective.

The ability to react calmly in a disaster environment is predicated upon a plan the Administrators believe in, and have tested themselves. The confidence they would have in the presence of such planning would enable them to get to the business of rapid recovery, turning such events into an asset for the company by demonstrating to the Client's customers how quickly they are able to recover from such a disaster event.

5. Complete the rollout of the Information Security Policy company-wide

Taking this action would formally get the firewall Security Plan into the hands of the Administrators. Though completion of this roll-out may have significant costs associated with it, the benefits of completing it would be worthwhile. Should it be determined to be cost-prohibitive to accelerate the roll-out, it would be a good compromise to publish the Security Plan for the firewall alone.

References

[1] Symantec Corporation. "Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance – Reference Guide" 2001
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_ref.pdf

[2] Linehan, John. "Audit of Borderware 6.5 Firewall, an Auditor's Perspective" 2003
http://www.giac.org/practical/GSNA/John_Linehan_GSNA.pdf

[3] Todd, Bennett. Auditing Firewalls: A Practical Guide
http://www.itsecurity.com/papers/p5.htm

[4] Collaborative Work. ITSecurity.com "AskTecs" Clinic on Firewall Change Management, July 2003
http://www.itsecurity.com/asktecs/jul1601.htm

[5] Symantec Corp. "Symantec Enterprise Firewall and Symantec enterprise VPN Installation Guide for Windows" 2003
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_windows_install.pdf

[6] Green, John. "Network Auditing Essentials" from the SANS Track 7 "Auditing Networks, Perimeters, and Systems" 2003

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**