



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 permitted without express written permission.

GIAC GSNA Certification
Auditing Networks, Perimeters, and Systems
GSNA Practical Assignment
Version 3.1
Option 1
Auditing the Fortigate-100 Firewall Appliance
Rama Chandran
Date: 15th, July 2004

© SANS Institute 2004. Author retains full rights.

Table of Contents

Auditing the Fortigate-100 Firewall Appliance	3
Abstract	3
Part 1: Research in Audit, Measurement practice, and control systems.....	4
Business Control Objectives	4
Detailed control objectives	5
Audit Scope.....	6
Purpose:.....	6
Role of Fortigate-100.....	6
Controls provided by Fortigate-100.....	6
Administering the Fortigate-100.....	7
Risks Analysis.....	8
Table 1: Key Business Processes that rely on the availability of the Fortigate-100.....	9
Table 2: Key Systems and Applications that rely on the integrity of the Fortigate-100	9
Risk Ratings	9
Table 3: Loss Impact Valuation Table.....	10
Table 4: The Integrity, Confidentiality and Availability requirements	11
Identified Risks to the Systems and Business Processes	11
Table 5: Identified Risks.....	16
Table 6: List of Controls.....	17
The Current State of Practice.....	18
Test Plan:	19
Part 2: Audit Checklist.....	20
Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings.....	40
3.1.0 Access and Configuration /Change Management.....	42
3.2.0 Port Filtering	58
3.3.0 Address Filtering.....	68
3.5.0 AV / File Blocking Protection	78
Part 4: Audit Report and Risk Assessment	81
Executive Report.....	81
Objectives	81
Scope and methodology.....	81
Discussion of Audit results	81
Current Status:	81
Table 7: Current status - Risks.....	82
Current Findings and Recommendation	82
Identified Vulnerabilities - Summary	82
Identified Vulnerabilities - Details.....	83
Additional Recommendations.....	87
References.....	88

Auditing the Fortigate-100 Firewall Appliance

Abstract

Today, instant sharing of information is possible between people and organizations using publicly connected global network. Corporations need to protect their information assets against malicious attacks that attempt to compromise their business infrastructure and comply with laws and regulations to demonstrate 'due diligence' to their stake holders and customers. Hacker attacks, worms and viruses can be remotely deployed against an organization to cripple their daily activities resulting in financial losses. Compromised internal systems can flood malicious data internally affecting productivity and corrupting the integrity of the company's information.

Technology can provide defenses to mitigate such attacks and a choice of multifarious protection is available at various cost levels. While the right technology choices are important to any business, this is especially true for Small and Medium Businesses. These companies typically operate closer to the bottom line, and must be careful to keep the cost of acquiring and managing technology as low as possible. Further, in the SMB world, where productivity is so closely linked to profits, technology must be reliable. The best way to lower total cost of ownership and heighten productivity is to buy reliable products and technologies, that work well on their own or together right from the beginning.

Lack of manpower renders small networks vulnerable to security problems. Besides administering the network, protecting the network against viruses and worms, applying latest security patches to systems adds to the work load of the network administrators. Recovering compromised systems and loading security software and patches to each machine consumes time and money.

To alleviate this and to mitigate various forms of network attacks, many vendors are providing integrated all-in-one Network Appliances to secure the internal Network. These are being deployed at many Small and Medium businesses. This audit examines one such appliance and investigates how they fit into a company's business objectives of protecting their information system that is connected to the public network.

Part 1: Research in Audit, Measurement practice, and control systems

Rama Marketing Inc. stocks and sells copper fittings for plumbing, for the building and industrial markets. They sell Commercial Industrial Division (CID) products which primarily consist of pressure rated metal valves made of bronze, iron, carbon and stainless steel, as well as ABS fittings, plumbing & heating valves and other sundry items such as frost free wall hydrants. Rama Marketing Inc. stocks and sells the entire ABC[®] product line. ABC[®] metal valves serve a wide variety of commercial, industrial and fire protection markets.

The company has a Local Area Network consisting of windows 2000 Domain controller, a windows 2000 Citrix server and 25 desktop and 60 thin clients. The company connects to the internet through a border router, firewall model Fortigate-100 from Fortinet Inc (<http://www.fortinet.com>).

The domain controller hosts their ERP program and is accessed through the CITRIX Application server. The CITRIX Server hosts all Microsoft Office productivity programs which are customized and accessed by Citrix ICA clients.

The company also runs an EDI application that connects to remote sites for B2B applications. The EDI application is available only on a specific single computer, the access to which is logically controlled. Only selected users are authorized to use the application. The company uses internet communication primarily for:

- E-mail
- Web Browsing: specific vendor sites for prices, catalogues, checking on the inventories etc.
- EDI
- Payroll transmission
- Electronic banking
- Remote branch/user connectivity.

Rama Inc. is also planning to deploy Internet critical applications in the near future

Business Control Objectives

IT Governance Institute has developed Control Objectives for Information and related Technology (COBIT[®]) QuickStart[®] framework, which provides a selection from their complete COBIT[®] framework as a baseline for small and medium enterprises. COBIT[®] helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. COBIT Quickstart[®] can be used as a baseline and a set of 'smart things to do' for many small and medium and other enterprises. It can also be a starting point for enterprises for their move towards an appropriate level of control and governance of IT (Ref Cobit Quickstart[®] Executive Summary).

(For more information <http://www.isaca.org/cobit>)

Rama Inc has adopted the following control objectives from COBIT® (Ref: COBIT® Control Objectives 3rd edition manual)

Domain: Delivery and Support

Process: DS5 – Ensure System Security

High level objective:

Control over the IT process of Ensuring System Security with the business goal of safeguarding information against unauthorized use, disclosure or modification, damage or loss is enabled by logical access controls which ensures access to systems, data and programs is restricted to authorized users and takes into consideration:

- confidentiality and privacy requirements
- authorization, authentication and access control
- user identification and authorization profiles
- need-to-have and need-to-know
- cryptographic key management
- incident handling, reporting and follow-up
- **virus prevention and detection**
- **firewalls**
- centralized security administration
- user training
- **tools for monitoring compliance, intrusion testing and reporting**

While all of the above are equally important, this audit is concerned only with

- Virus prevention, detection and reporting
- Firewalls
- Intrusion detection, prevention and reporting

Detailed control objectives:

There are 21 detailed control objectives that support the above High-Level Control objective. This audit is based on the two following detailed control objectives for the Domain DS5 - Delivery and Support (Ref: COBIT® Control Objectives 3rd edition) for Rama Inc.

DS5.20: Firewall Architecture and Connection with Public Networks

Control Objective: If connection to the internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

DS 5.19: Malicious software Prevention, Detection and correction

Control Objective: Regarding malicious software, such as computer viruses and Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

(Ref: COBIT® Control Objectives 3rd edition manual)

Audit Scope

I have chosen to audit the Fortigate-100 as it is the company's border router and Firewall. This appliance is expected to deliver the above two business control process objectives as a technical control for Rama Inc. This audit examines in detail how and how effectively, Fortigate-100 meets the above objectives.

Purpose:

1. Determine the threats and vulnerabilities related to the Fortigate-100 and their impact on business. (See: Risk Analysis)
2. Determine intended controls
 - a. First, I will determine if this appliance has the necessary required controls to protect against denial of service attacks, unauthorized access to internal resources and provide secure flow of information in both directions. This will be accomplished by researching the product specifications and the manufacturer's brochures. (See following : Controls provided by Fortigate-100)
3. Provide a checklist for testing

After determination of the intended controls,

 - a. I will create a Test Plan
 - b. Using the Test Plan, I will construct a test procedure through checklists for testing some of the chosen controls of this appliance. (See Part 2: Audit Check List).
4. Perform the test
 - a. I will use the checklist to test if the intended controls are in fact present and functioning accordingly and record the findings (See Part 3: Audit of Fortigate-100 – Testing, evidence and findings).

Role of Fortigate-100

The Fortigate-100 functions as the Border Router, Firewall, Antivirus Filter, Intrusion Detection and prevention. Located at the edge of the company's internal network, it is the company's only Gateway to the internet.

Controls provided by Fortigate-100

Taken from Fortigate Series 50/100 Brochure:

"FortiGate™ Antivirus Firewalls are dedicated, hardware-based units that deliver complete, real-time network protection services at the network edge. Underlying FortiOS™ operating system is ICSA-certified for Antivirus, Firewall, IPSec VPN, and

Intrusion Detection. The FortiGate-100 includes a DMZ port, traffic shaping, and increased throughput. The FortiGate-50 and FortiGate-100 are kept up to date automatically by Fortinet's FortiProtect Network, which provides continuous updates that ensure protection against the latest viruses, worms, Trojans, intrusions and other threats. (Ref: <http://www.fortinet.com>)

1. **Firewall (ICSA Certified)** - Industry standard stateful inspection firewall.
2. **Intrusion Detection (ICSA Certified)** - Customizable database of over 1300 attack signatures.
3. **Intrusion Prevention** - Active prevention of over 30 intrusions and attacks, including DoS and DDoS attacks, based on user-configurable thresholds.
4. **Network-based Antivirus (ICSA Certified)** - Detects and eliminates viruses and worms in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP) and Web (HTTP) and FTP traffic — without degrading Web performance.

Note: VPN and Web Content Filtering controls and not included in this audit.

Administering the Fortigate-100

FG-100 can be configured / administered either via a Web interface or a Command Line interface. In certain functions they complement each other and this audit uses both of them wherever it is effective and applicable.

The Fortigate web-based manager Setup Wizard guides one through the initial configuration steps. It can be used to configure the administrator password, the interface addresses, and the default gateway address.

Requirements for the web interface:

- An ethernet connection between the FortiGate-100 and management computer.
- Internet Explorer version 4.0 or higher on the management computer.

Command Line Interface (CLI)

The CLI is a full-featured management tool. It is used to configure the administrator password, the interface addresses, and the default gateway address and to configure advanced settings (Ref: Fortigate-100 Documentation CD-ROM).

Requirements for using CLI:

- A serial connection between the FortiGate-100 and management computer.
- A terminal emulation application (HyperTerminal for Windows) on the management computer.

Risks Analysis

Based on the business control objectives referred earlier under 'Detailed Control Objectives' (COBIT® ref: DS 5:19 and DS: 5.20). Rama Inc. analyzed the risks to their information system and the overall impact to their business. The company adopted Facilitated Risk Analysis Process (FRAP).

The risks and vulnerabilities to the Fortigate-100 Firewall / Router appliance was analyzed by a team of individuals that included business managers, who are familiar with business information needs, and technical staff who have a detailed understanding of potential system vulnerabilities and related controls. The team consists of:

- System User
- Company Business manager / Controller
- Network administrator
- HR manager

(Ref: The Information Security Risk Analysis by Thomas R. Peltier ISBN:0849308801)

During the session, the key business processes that depended on the availability of the Fortigate-100, the systems and applications that depended on the integrity of the Fortigate-100 were analyzed and listed (Tables 1 & 2). Using a Loss Impact Table (Table 3) the team proceeded to determine the Integrity, Confidentiality and Availability of the Fortigate-100 (Table 4) based on an established downtime (outage period). The identified risks to the system and business processes are presented in the 'Risk Statement Forms' (Ref: **Microsoft Solutions for security – Windows 200 Server Security Solutions; Chapter 3 – Page 58 'Risk Statement Form'**).

This risk analysis validates the significant importance of the Fortigate-100, as a technical control, in supporting the company's business objectives and its processes. The team's conclusions on the risks, their priority, and the required controls are documented in Tables 5 and 6. In Table 6 the checklist items are mapped to the controls, which in turn are mapped to the control objectives in an order of priority.

Table 1: Key Business Processes that rely on the availability of the Fortigate-100

Business Process 1	Internet (Access to Vendor , Supplier Inventory and Prices)
Business Process 1	Payroll
Business Process 2	Human Resource System
Business Process 3	Electronic Banking
Business Process 4	Electronic Data Interchange (Purchase orders, Invoices)
Business Process 5	E-mail and documents
Business Process 6	Customer support, inventory, order booking, shipping and delivery
Business Process 7	Accounting

Ref: The Information Security Risk Analysis by Thomas R. Peltier ISBN:0849308801

Table 2: Key Systems and Applications that rely on the integrity of the Fortigate-100

Systems (Servers)	Windows Domain Controller, Citrix Server
Application 1	Customer Orders, Inventory , Price Lists (ERP)
Application 2	Microsoft Office
Application 3	Payroll and Accounting
Application 4	Human Resources Program
Application 5	E-mail and document exchange

(Ref: The Information Security Risk Analysis by Thomas R. Peltier ISBN:0849308801)

Risk Ratings

The following guidelines (Ref: Microsoft Solutions for Security (Patterns and Practices) Windows 2000 server Security Solutions – Chapter 3: Understanding the Security Risk Management Discipline) were used to determine the risk exposure.

Probability Rating

Probability range	Probability value used for calculations	Natural language expression	Numeric score
1% through 33%	17%	Low	1
34% through 67%	50%	Medium	2
68% through 99%	84%	High	3

Impact Rating

Impact Factor: High = 3, Medium = 2, Low = 1

Risk Exposure = Impact x Probability

Probability impact	Low = 1	Medium = 2	High = 3
High = 3	3	6	9
Medium = 2	2	4	6
Low = 1	1	2	3

Low exposure = 1 or 2 Medium exposure = 3 or 4 High exposure = 6 or 9

Table 3: Loss Impact Valuation Table

Impact Value	Time Sensitivity	Intangible Loss (Dollar Loss Difficult to Estimate)		Tangible Loss
	Longest Tolerable Outage Period During Peak	Customer Satisfaction (Dissatisfied Customers)	Embarrassment (<i>Comes to Attention of</i>)	Financial
L	24 hours or less	0 – 10K	Few if anyone	Less than \$50K
M	25–72 hours	10,001– 15K	Company organization	\$50,001–\$300K
H	73 hours–5 days	15,001 and higher	Company Organization, Vendors	\$300,001 and above

Table 4: The Integrity, Confidentiality and Availability requirements

#	Key Business Processes or Business Functions Supported by Fortigate-100	Integrity (Impact Value)	Confidentiality (Impact Value)	Availability (Impact Value)
1	Internet (Access to Vendor, Supplier Inventory and Prices)	M	M	M
2	ERP System	H	H	H
2	Payroll	H	H	M
3	Human Resources	H	H	M
4	Electronic Banking	H	H	H
5	Electronic Data Interchange	H	H	H
6	E-mail, Documents	H	H	M

Identified Risks to the Systems and Business Processes

The identified risks are presented below in the form of risk statements (Ref: **Microsoft Solutions for security – Windows 200 Server Security Solutions; Chapter 3 – Page 58 ‘Risk Statement Form’**). Part 2: Audit Check List provides Risk of Non Compliance for each item. The risk items shown below are not in their order of priority.

© SANS Institute 2011

Risk Severity	High	Probability	H	Impact	H	Risk Item	1
Risk Condition	Unknown and dangerous services pass through the firewall freely. Important for Border Routers and as a Result...						
Risk Consequence	An intruder may set up a backdoor and by pass the Firewall Security. A hacker can traverse the entire company network and can damage one or several computers and data they contain. They can also leave programs that will help them connect remotely and record user accounts, password etc, which can be exploited. Employee's private and company's data are at high risk.						
Countermeasure	Firewall Policy, Port Filtering. Enable Intrusion Detection and Prevention.						
References	SANS GSNA Courseware – Auditing the perimeter. JANET-CERT: Services that router should block. http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 3.2 Protecting the network with the Router).						

Risk Severity	High	Probability	H	Impact	H	Risk Item	2
Risk Condition	Login by hostile agents or unauthorized users and as a Result...						
Risk Consequence	An intruder may set up an account and modify Firewall settings remotely, or modify the firewall administrator's account and deny their access to the firewall.						
Countermeasure	Access Configuration and Change Management						
References	Guidelines on Firewalls and Firewall Policy (NIST Publication 800-41) - Chapter 5.0 Firewall Administration						

Risk Severity	High	Probability	H	Impact	H	Risk Item	3
Risk Condition	Session hijacking						
and as a Result...							
Risk Consequence	Exposure of sensitive information to unauthorized listeners. Session hijacking can be used to obtain logon information that can be used to gain access to a system or confidential information.						
Countermeasure	Access Configuration and Change Management, Session encryption and stateful inspection at the firewall. Logs.						
References	Microsoft security guidance kit – Threats and countermeasures.						

Risk Severity	High	Probability	H	Impact	H	Risk Item	4
Risk Condition	IP Spoofing						
and as a Result...							
Risk Consequence	An intruder can change the source address of an IP packet to hide his / her true identity and send a malicious code or start a denial of service attack. The spoofed address may be external or from the trusted internal network.						
Countermeasure	Implement Access Control, RFC 2827 Filtering. Enable Intrusion Detection and Prevention.						
References	Microsoft Security Guidance Kit : Perimeter Firewall Design						

Risk Severity	High	Probability	H	Impact	H	Risk Item	5
Risk Condition	Flooding attacks or DDOS attacks using ICMP						
and as a Result...							
Risk Consequence	An intruder can gather internal network information using ICMP Protocol to perform denial of service attacks. ICMP can also be used for exploiting systems and as a covert channel for attacker's communications.						
Countermeasures	Disallow traceroute, ping, or any other ICMP messages. Enable Intrusion Detection and Prevention.						
References	http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html ; http://www.sans.org/rr/papers/60/477.pdf ; http://techrepublic.com.com/5102-6264-5087087.html						

Risk Severity	High	Probability	H	Impact	H	Risk Item	6
Risk Condition	Denial of service attacks						
and as a Result...							
Risk Consequence	The network resources are consumed disrupting and denying services to the legitimate users. This may result in loss of revenue and loss in productivity.						
Countermeasures	Firewall Policy, Use of firewall Filters, Intrusion Detection and Prevention, Patching and updating of software Firewall Logs.						
References	http://www.cert.org/tech_tips/denial_of_service.html ; http://www.cert.org/archive/pdf/DoS_trends.pdf ; Microsoft Security Guidance Kit:- Threats and Countermeasures						

Risk Severity	High	Probability	H	Impact	H	Risk Item	7
Risk Condition	Misconfigured router						
and as a Result...							
Risk Consequence	May result in unauthorized access or modification of organization's information resources. Denial-of-service attacks that target and use misconfigured network routing equipment pose an "imminent and real threat" to Internet security, according to a recent report by Carnegie Mellon University's federally funded CERT Coordination Center.						
Countermeasure	Regular Firewall Audit, Change Control						
References	http://www.computerworld.com/networkingtopics/networking/story/0,10801,65366,00.html						

Risk Severity	High	Probability	H	Impact	H	Risk Item	8
Risk Condition	Exposure to Viruses, Trojans etc.						
and as a Result...							
Risk Consequence	Critical data loss or system availability. An intruder may set up a backdoor and by pass the Firewall Security. A hacker can traverse the entire company network and can damage one or several computers and data they contain. They can also leave programs that will help them connect remotely, and record user accounts, password etc, which can exploited. Employee's private and company's data at high risk. Increased cost of recovery. 'An explosion in virus attacks affected two-thirds of companies in the past year, leading to significant dents in productivity.'*						
Countermeasure	AV Program, Acceptable use policy (Security Policies).						
References	* Pricewaterhousecoopers (PwC) puts cost of virus attacks at \$1tr http://software.silicon.com/security/0,39024655,11027559,00.htm						

© SANS Institute 2004, Author retained

Table 5: Identified Risks

#	Vulnerability / Exposure	Risk	Assets Impacted	Type	Risk Exposure	Controls
1	Default Firewall settings. Misconfigured Firewalls Unauthorized Router Access.	<ul style="list-style-type: none"> • Unknown and dangerous services pass through freely. • May be serving as unwitting participants in Denial of Service. • Login by hostile agents or unauthorized users, inability to attribute accountability. • Exposure of sensitive information to unauthorized listeners, session hijacking. • Address-spoofed DDoS traffic exiting the network, forwarding bad traffic to peers. • Flooding attacks or DDoS attacks using ICMP. • Malicious third parties may gain access to critical applications or sensitive data. • Denial of service where remote users may not be able to gain access to data. • Misconfigured router, which may result in unauthorized access or modification of organization's information resources. 	<ul style="list-style-type: none"> • Servers • Personnel Data • Customer Orders • Inventory • Pricelists • Documents • E-mail • Productivity • EDI 	INT CON AVA	3x3=9 HIGH	1,2,3,4
2	Malware, Spyware, Viruses and Trojans.	<ul style="list-style-type: none"> • Increased cost of recovery (correcting information and reestablishing services). • Loss of information (critical data, proprietary information, contracts). • Loss of trade secrets. • Increased cost of retrospectively securing the system. 		INT CON AVA	3x3=9 HIGH	5

Risk = Actual Risk **Type** = Integrity, Confidentiality, Availability **Control** = Controls identified to help mitigate the risk
 REFERENCE: Information Security Risk Analysis by Thomas R. Peltier.

Table 6: List of Controls

Control Objective	Controls	Checklist Item #	Control Description
<p>If connection to the internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.</p>	<p>1. Access and Configuration / change Management</p>		
	<ul style="list-style-type: none"> • Security Policies • FW Access Control • FW Configuration • FW RULEBASE Order 	<p>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12</p>	<p>Preventive</p>
	<p>2. Port Filtering</p>		
	<ul style="list-style-type: none"> • Permit only Required Protocols and Services • Reject Risky Protocols and services 	<p>13, 14, 15,16,17, 18, 19,20</p>	<p>Preventive</p>
	<p>3. Address Filtering</p>		
	<ul style="list-style-type: none"> • Reject all Traffic from the Internal Networks that bear a source IP address which does not belong to the internal network • Reject all Traffic from external networks that bears a source address belonging to the internal network • Reject all Traffic with a source or destination address belonging to any reserved, unroutable, or illegal address range. 	<p>21, 22, 23, 24, 25</p>	<p>Preventive: Defeating Denial of Service Attacks. IP Source Address Spoofing. SYN Flooding and IP Spoofing Attacks, Smurf IP Denial-of-Service Attacks.</p>
	<p>4. Intrusion Detection and prevention</p>		<p>Detective and Corrective</p>
	<ul style="list-style-type: none"> • Intrusion Detection • Intrusion Prevention • Audit and Logging 	<p>26, 27, 28, 29, 30, 31</p>	
<p>Regarding malicious software, such as computer viruses and Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.</p>	<p>5. Anti Virus Protection</p>		<p>Preventive and corrective</p>
	<ul style="list-style-type: none"> • Acceptable use policy • File Blocking 	<p>32, 33, 34, 35,</p>	

Reference: COBIT QuickStart, COBIT, CISA Review Manual 2003, Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1

The Current State of Practice

Control Objectives:

Information technology is no longer a self contained department. It involves users, managers and technologists and is pervasive throughout an organization and supports the organizations' business goals. Therefore, a framework is needed to ensure that computer-based technologies are applied in a cost-effective secure and appropriate manner.

COBIT[®] *Framework*, developed and promoted by the IT Governance Institute is a control model that focuses on the process rather than functions or applications. This allows self-assessment in order to make choices for control implementations and improvements over IT. COBIT[®] is the result of agreed upon standards by experts in the field of Information Technology and provides a good tool for IT governance. In summary: 'COBIT[®] helps organizations to adopt practices for planning and organizing, acquiring and implementing, delivering and monitoring IT and related technologies to ensure that they support the organizations' business objectives. It provides a basic understanding for every organization on the status of their IT systems and helps them to decide the required security and controls. The organizations can map their progress through establishing and monitoring key performance indicators and critical success factors. COBIT Quickstart[®] provides a selection from the complete COBIT framework and can be used as a baseline for many small and medium organizations. It is useful for auditors, IT managers, and implementers for light and easy-to-use approach to get started' (Ref: COBIT[®] Framework – 3rd edition). More detailed information can be obtained from <http://www.isaca.org/cobit>.

As we have done in this audit, an organization can pick and choose the control objectives that closely relate to their business objectives and gradually grow into other Control Domains of COBIT[®]. This facilitates an organization to baseline their IT governance and later on 'Benchmark' with their peer organizations.

Perimeter Security:

Security threats are growing in frequency and complexity and their ability to spread in a matter of minutes has also increased to cause severe damages. With the increased use of networks and the Internet in daily business computing, the risk of unauthorized users attempting to gain access to business critical resources is rising.

Perimeter security is an important component of a defense-in-depth strategy that includes security measures at multiple points within the organization. Identifying the features necessary in a perimeter firewall is an important step and I have gained most valuable information from Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 and Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations. These two resources were consulted in detail during this audit. In addition to some of the checklist items, the checklist format was modeled after the Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations. I tailored this audit based on the above, the GSNA Course book, Information found on SANS Portal, Microsoft Security Guidance Kit and other referred

material in the checklist, to develop a reproducible testing plan relevant to the specific Fortigate-100 Firewall / Router.

Risk Analysis:

There is a plethora of information available on risk assessment methodologies. The Information Security Risk Analysis by Thomas R. Peltier, provides guidance to perform the necessary risk evaluation and a workbook for understanding risk analysis to safeguard information assets within organizations. Another Source of information that I used is 'The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE[®]) developed at the Software Engineering Institute (SEISM) of the Carnegie Mellon University. The OCTAVE[®] self assessment approach for evaluating risks is driven by operational risk and security practices of the organization being assessed. The process based risk assessment methodology is described in a10 Volume guide and provides all the necessary worksheets. OCTAVE[®]-S is a variation of the OCTAVE[®] and is tailored to meet the specific needs of small organizations. Ref: OCTAVE[®]-S – Operationally Critical Threat, Asset, and Vulnerability Evaluation, Version 0.9: <http://www.cert.org/octave> Additional source of information on Risks is from Microsoft Corporation's Microsoft Solutions Guide for Securing Microsoft Windows 2000 Server (Ref: <http://support.microsoft.com/default.aspx?scid=kb;en-us:829031>). Chapter 3 'Security Risk Management Discipline' of this guide discusses in detail the approaches one could take in identifying, classifying and risk mitigating plans. It provides Risk Statement forms for analysis and prioritizing risks.

Often times, the risk assessment process and the methodology seem simple in theory based on a 'common sense' approach. But in real life situations, they can be challenging. Using the above referred guides, I was successful in developing questionnaires to identify the critical assets, the Process or Business Functions that depended on them, correlate risks to the assets and the controls that are required to mitigate the impacts. To assist non technical personnel on the impact, I have provided additional information (Risk of Non Compliance) on each checklist item, hopefully in simpler terms.

Test Plan:

1. Test firewall configuration for secure administration and Rulebase (See: Part 2:Audit Checklist - Section 2.1.0)
2. Test firewall configuration for allowed "outside-in' and "inside-out' services (See: Part 2:Audit Checklist - Section 2.2.0)
3. Test ingress and egress Address Access Control (See: Part 2:Audit Checklist - Section 2.3.0)
4. Test IDS for detection / prevention and Alert (See: Part 2:Audit Checklist - Section 2.4.0)

5. Test AV controls settings and File blocking protection (See: Part 2:Audit Checklist - Section 2.5.0)

(Ref: GSNA Courseware Section 7.2 – Auditing the Perimeter)

Part 2: Audit Checklist

Although there are verbal and general understanding of what services are required and the safe usage of computing systems in general, Rama Inc. do not have specific written security policies of any kind. Because of this, the firewall was audited against standards and best practices referred in the reference section of each item.

2.1.0 Access and Configuration /Change Management

N/A	Pass	Fail	#	Check List Item	RISK	
			1	a) Only FW administrator and other authorized personnel will be granted access to the FW for administration. b) Firewall should be administered from a trusted host.	H	
Risk of Non Compliance		Unauthorized user access and unsecured hosts leave the firewall susceptible for intruders to modify the firewall rules, corrupt its integrity and deny its availability to legitimate users.				
Procedure		Connect to internal interface of the firewall using SSH Client Putty. At the Command Line Interface (CLI) Login as Administrator and execute the following commands : a) Fortigate-100 # get system admin. Note the results b) Fortigate-100 # get config. Note the results.				
Verify		The results will show the admin users name and the specific trusted ip address from which they can connect to the FW and their read/write permissions.				
Conclusion						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.4 Router Accounts) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 3.3 – Managing the Router and 4.1.5. – Logins, Privileges, Passwords and Accounts). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			2	<i>The administrator and other authorized users account password will be encrypted and should be at least 6 characters long.</i>	H	
Risk of Non Compliance		Clear text passwords give easy access (password cracking) for intruders to misconfigure the firewall				
Procedure		At the CLI Login as Administrator and execute the following command: a) Fortigate-100 # get config. Note the results. b) Create a new user with a password less than 6 characters. A Warning should appear.				
Verify		The password is encrypted. For Passwords less than 6 characters a warning appears.				
Conclusion						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Security Operations (Section 3.5.5 Router Passwords). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.5. – Logins, Privileges, Passwords and Accounts). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			3	<i>The time out period for unattended console is set for no longer than 15 minutes. Activating this timeout period provides additional security</i>	H	
Risk of Non Compliance		Abuse from casual or malicious use through the open session (for longer timeout periods) by unauthorized users, if they get physical access to the session.				
Procedure		At the Command Line Interface (CLI) Login as Administrator and execute the following command: a) Fortigate-100 # get system option b) Login and wait for the expiration timeout period. The system must force you to re login				
Verify		The values for ‘Admin timeout’ is 15 minutes.				
Conclusion						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.4 Router Accounts). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK
			4	<i>The FW administrator will ensure modems will not be used for remote administration</i>	H
Risk of Non Compliance		War-dialing. Enables a backdoor for malicious purposes.			
Procedure		Check if an auxiliary console for Modem connection is available, if available check if it is disabled.			
Verify		Physically.			
Conclusion					
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.6 – Out-of-band Management) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.6 Remote Access) Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php			
Subjective		Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK
			5	<i>The FW administrator will disable FW interfaces that are not in use</i>	H
Risk of Non Compliance		Scanning and spoofing attacks, unauthorized access attempts to the firewall through un-trusted network. If successful, enables a backdoor for the intruder to the firewall and to the internal network.			
Procedure		At the CLI Execute the following command: Fortigate-100 # get system interface			
Verify		The lists of interfaces that are up are shown. Ensure that the DMZ interface is disabled.			
Conclusion					
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.6 – Out-of-band Management) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version1.1. Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php			
Subjective		Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK		
			6	<i>Ensure that only ports on the internal interface will be used for administrative access to the FW and they are restricted to SSH or SSL encryptions.</i>	H		
Risk of Non Compliance		Man-in-the-middle attack, Session hijacking.					
Procedure		At the CLI Execute the following command: a) Fortigate-100 # get system interface. Note the results. b) Try login to the external interface through web interface or using putty.					
Verify		Check if the line “access:” reads ‘ssh, https’ only for the internal interface. You should not be able to login to the external interface of the firewall.					
Conclusion							
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.7 – In-band Router Management) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 5.3 – Using SSH for Remote Administration security). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective			Objective	X	Evidence		Findings

N/A	Pass	Fail	#	Check List Item	RISK		
			7	<i>The FW administrator will ensure all administrative access and modification to the FW configuration are logged.</i>	H		
Risk of Non Compliance		Undetected firewall access violations and configuration changes to the firewall settings.					
Procedure		Log in as admin using the web interface: https://192.168.22.1 a) Select Log&Report>Log setting>Config Policy. b) Select HA activity event and select ok. Deselect HA activity event and select ok.					
Verify		a) Verify that under Log & Report > Log Setting > config Policy > Event log: ‘admin login/logout event’ and ‘when configuration has changed’ are selected. b) Check the logs to verify the log policy changes are recorded.					
Conclusion							
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.7 – In-band Router Management). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1) (Section 3.3.3 Logging and 4.5.2 – Configuring Logging and Time Services). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective			Objective	X	Evidence		Findings

N/A	Pass	Fail	#	Check List Item	RISK			
			8	<i>The current and previous router configuration are backed up and saved in a secure location.</i>	MH			
Risk of Non Compliance		Unauthorized configuration changes and corruption of the stored files. No backup protection affects Real-time Recovery Objective (RT0).						
Procedure		a) Ask admin to show the back up configuration file location. b) Create a new back up and store it in the same directory (for next item 9)						
Verify		Check the creation dates of the configuration back up files. They must be different. Check if the files are stored in a secure system.						
Conclusion								
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.3 –Logistics for Configuration Loading and Maintenance). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 3.3.2 Updating the Router and 4.1.8 – Logistics for configuration Loading and Maintenance). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
			9	<i>On the system where the configuration files are stored, the local operating system's security mechanisms will be used for restricting access to the files</i>	MH			
Risk of Non Compliance		Unauthorized configuration changes and corruption of the stored files. No backup protection affects Real-time Recovery Objective (RT0).						
Procedure		Ask admin to show the location of the backup configuration files. Compare the security permissions of the old and newly backed up configuration files (previous item 8).						
Verify		Check if the folder is located in a NTFS formatted volume. Check the security properties of the folder. Verify that only the administrator (S) of the firewall has full permission to the folder.						
Conclusion								
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.3 –Logistics for Configuration Loading and Maintenance). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.8 – Logistics for configuration Loading and Maintenance) Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK	
			10	<i>Ensure that the latest patches and updates are applied to the firewall components. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.</i>	H	
Risk of Non Compliance		Exploitation of known vulnerabilities.				
Procedure		a) Use web interface and login as the administrator. Note the Firmware, Anti Virus and attack definition Versions. b) Ask the Administrator to login at the Fortinet support site and show the latest versions of these items. c) Check Automatic update function if they are enabled.				
Verify		Compare the version numbers. The versions in Fortigate-100 must be the latest.				
Conclusion						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations. Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.5.5 Performing Cisco Software Updates). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK
			11	<i>Review the ruleset EXT > INT to ensure that they follow the order as follows:</i> <ul style="list-style-type: none"> • <i>firewall Lockdown</i> • <i>anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)</i> • <i>Deny unwanted inbound services</i> • <i>User permit rules (allow CITRIX ICA and HTTPS)</i> • <i>Noise drops (e.g. discard multicasts, OSPF and HSRP chatter)</i> • <i>Deny and Alert (alert systems administrator about traffic that is suspicious)</i> • <i>Deny and log (log remaining traffic for analysis)</i> <i>Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.</i>	H
Risk of Non Compliance		Misconfiguration. Ineffective rulesets.			
Procedure		Login as admin using the web interface. a) Select Firewall>Addresses>External - Note the results b) Select Firewall > Policy > 'EXT>INT' – Note the results			
Verify		Check the Rule order, as above. Make sure that logging is enabled for all the denied rules.			
Conclusion					

Reference	Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php Building Your Firewall Rulebase by Lance Spitzner http://www.spitzner.net/rules.html						
Subjective		Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK		
			12	<p><i>Review the ruleset INT > EXT to ensure that they follow the order as follows:</i></p> <ul style="list-style-type: none"> <i>allow ipsec tunnel</i> <i>anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)</i> <i>blocked unwanted outbound services</i> <i>User permit rules (e.g. allow HTTP to public web server)</i> <i>Deny and log (log remaining traffic for analysis)</i> <p><i>Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.</i></p>	H		
Risk of Non Compliance		Misconfiguration. Ineffective rulesets.					
Procedure		Login as admin using the web interface. Select Firewall>Addresses>Internal - Note the results Select Firewall > Policy > 'INT>EXT' – Note the results					
Verify		Check the Rule order, as above. Make sure that logging is enabled for all the denied rules.					
Conclusion							
Reference		Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php Building Your Firewall Rulebase by Lance Spitzner http://www.spitzner.net/rules.html					
Subjective		Objective	X	Evidence		Findings	

© SANS Institute

2.2.0 Port Filtering

N/A	Pass	Fail	#	Check List Item	RISK																																																		
			13	Reject the following non-required, risky protocols and services in either direction.	H																																																		
				<table border="1"> <thead> <tr> <th>Port (Transport)</th> <th>Service</th> </tr> </thead> <tbody> <tr><td>1 (TCP & UDP)</td><td>tcpmux</td></tr> <tr><td>7 (TCP & UDP)</td><td>echo</td></tr> <tr><td>9 (TCP & UDP)</td><td>discard</td></tr> <tr><td>11 (TCP)</td><td>systat</td></tr> <tr><td>13 (TCP & UDP)</td><td>daytime</td></tr> <tr><td>15 (TCP)</td><td>netstat</td></tr> <tr><td>19 (TCP & UDP)</td><td>chargen</td></tr> <tr><td>67 (UDP)</td><td>bootp</td></tr> <tr><td>69 (UDP)</td><td>tftp</td></tr> <tr><td>135 (TCP & UDP)</td><td>loc-srv</td></tr> <tr><td>137 (TCP & UDP)</td><td>netbios-ns</td></tr> <tr><td>138 (TCP & UDP)</td><td>netbios-dgm</td></tr> <tr><td>139 (TCP & UDP)</td><td>netbios-ssn</td></tr> <tr><td>177 (UDP)</td><td>xdmcp</td></tr> <tr><td>445 (TCP)</td><td>netbios (ds)</td></tr> <tr><td>512 (TCP)</td><td>rexec</td></tr> <tr><td>515 (TCP)</td><td>lpr</td></tr> <tr><td>517 (UDP)</td><td>talk</td></tr> <tr><td>518 (UDP)</td><td>ntalk</td></tr> <tr><td>540 (TCP)</td><td>uucp</td></tr> <tr><td>1900, 5000 (TCP & UDP)</td><td>Microsoft UPnP SSDP</td></tr> <tr><td>12345 (TCP)</td><td>NetBus</td></tr> <tr><td>12346 (TCP)</td><td>NetBus</td></tr> <tr><td>31337 (TCP & UDP)</td><td>Back Orifice</td></tr> </tbody> </table>	Port (Transport)	Service	1 (TCP & UDP)	tcpmux	7 (TCP & UDP)	echo	9 (TCP & UDP)	discard	11 (TCP)	systat	13 (TCP & UDP)	daytime	15 (TCP)	netstat	19 (TCP & UDP)	chargen	67 (UDP)	bootp	69 (UDP)	tftp	135 (TCP & UDP)	loc-srv	137 (TCP & UDP)	netbios-ns	138 (TCP & UDP)	netbios-dgm	139 (TCP & UDP)	netbios-ssn	177 (UDP)	xdmcp	445 (TCP)	netbios (ds)	512 (TCP)	rexec	515 (TCP)	lpr	517 (UDP)	talk	518 (UDP)	ntalk	540 (TCP)	uucp	1900, 5000 (TCP & UDP)	Microsoft UPnP SSDP	12345 (TCP)	NetBus	12346 (TCP)	NetBus	31337 (TCP & UDP)	Back Orifice	
Port (Transport)	Service																																																						
1 (TCP & UDP)	tcpmux																																																						
7 (TCP & UDP)	echo																																																						
9 (TCP & UDP)	discard																																																						
11 (TCP)	systat																																																						
13 (TCP & UDP)	daytime																																																						
15 (TCP)	netstat																																																						
19 (TCP & UDP)	chargen																																																						
67 (UDP)	bootp																																																						
69 (UDP)	tftp																																																						
135 (TCP & UDP)	loc-srv																																																						
137 (TCP & UDP)	netbios-ns																																																						
138 (TCP & UDP)	netbios-dgm																																																						
139 (TCP & UDP)	netbios-ssn																																																						
177 (UDP)	xdmcp																																																						
445 (TCP)	netbios (ds)																																																						
512 (TCP)	rexec																																																						
515 (TCP)	lpr																																																						
517 (UDP)	talk																																																						
518 (UDP)	ntalk																																																						
540 (TCP)	uucp																																																						
1900, 5000 (TCP & UDP)	Microsoft UPnP SSDP																																																						
12345 (TCP)	NetBus																																																						
12346 (TCP)	NetBus																																																						
31337 (TCP & UDP)	Back Orifice																																																						
Risk of Non Compliance	These ports can be used for denial of service and or sending malicious codes																																																						
Procedure	Login as admin to the web interface. Select Firewall > Service > Custom The custom services are additional ports/services that are not in the predefined list. A group Disallowed_ services contains all the ports that are unnecessary and denied entry to the network. Check that this group of services are denied and logging enabled both at the EXT>INT and INT > EXT Policies.																																																						
Verify	Verify that the list reflect the ports mentioned in this checklist.																																																						
Conclusion																																																							

Reference	Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 3.2 Protecting the network with the Router). JANET-CERT: Services that router should block. http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective		Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK
			14	<i>Permit only required inbound Protocols and Services</i>	H
Risk of Non Compliance	Intruders may exploit unknown and not required services.				
Procedure	Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29 Use following commands inbound from the internet for TCP and UDP Ports: <ul style="list-style-type: none"> • Nmap -n -P0 -sT -p 1-65535 -oN inbound-syn-scan.txt xxx.xxx.xxx.x27 • Nmap -n -P0 -sU -p 1-65535 -oN inbound-udp-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w inboundtcp-scan.cap host 192.168.22.1 tcpdump -nn -vvv -w inboundudp-scan.cap host 192.168.22.1				
Verify	Should only detect ports 443/tcp and 1494/tcp. Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion					
Reference	SANS – GSNA Courseware. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3 Functional Tests). SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective		Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			15	<i>Permit only required inbound Protocols and Services (Fin Scan)</i>	H	
Risk of Non Compliance		Intruders may exploit unknown and not required services. Helps to determine open and closed ports.				
Procedure		Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29 with FIN packets to see if they are handled differently. Use following commands. <ul style="list-style-type: none"> Nmap -n -P0 -sF -p 1-65535 -oN inbound-fin-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: <ul style="list-style-type: none"> tcpdump -nn -vvv -w inbound-fin-scan.cap host 192.168.22.1 				
Verify		Should not detect any open ports. Verify the logged data for the scanning activity Check tcpdump for records of the port scan traffic.				
Conclusion						
Reference		SANS – GSNA Courseware. SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			16	<i>Permit only required inbound Protocols and Services (ACK Scans).</i>	H	
Risk of Non Compliance		Intruders may exploit unknown and not required services. Helps to determine ports that allow established connections.				
Procedure		Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29 with ACK packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sA -p 1-65535 -oN inbound-ack-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: <ul style="list-style-type: none"> tcpdump -nn -vvv -w inbound-ACK-scan.cap host 192.168.22.1 				
Verify		Should not detect any open ports. Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion						
Reference		SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			17	<i>Permit only required Outbound Protocols and Services.</i>	H	
Risk of Non Compliance		Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks.				
Procedure		Perform Port scanning of the internal Interface IP from PC FreeBSD 192.168.22.210. Use following commands: <ul style="list-style-type: none"> • Nmap -n -P0 -sT --p 1-65535 -oN outbound-syn-scan.txt 192.168.22.1 • Nmap -n -P0 -sU --p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1 Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: <ul style="list-style-type: none"> • tcpdump -nn -vvv -w servicesouttcp-scan.cap host xxx.xxx.xxx.x27 (for TCP) • tcpdump -nn -vvv -w servicesoutudp-scan.cap host xxx.xxx.xxx.x27 (for UDP) 				
Verify		Should only detect ports 22/tcp and 443/tcp. Verify the logged data of the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion						
Reference		SANS – GSNA Courseware – Auditing the Perimeter. SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK
			18	<i>Permit only required Outbound Protocols and Services (FIN Scan Test).</i>	H
Risk of Non Compliance		Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks			
Procedure		Perform Port scanning of the internal Interface IP from PC FreeBSD 192.168.22.210 with FIN packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> • Nmap -n -P0 -sF --p 1-65535 -oN outbound-fin-scan.txt 192.168.22.1 Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: <ul style="list-style-type: none"> • tcpdump -nn -vvv -w outbound-fin-scan. cap host xxx.xxx.xxx.x27 			
Verify		Should not detect any open ports. Verify the logged data of the scanning activity. Check tcpdump for records of the port scan traffic.			
Conclusion					
Reference		SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504			

Subjective		Objective	X	Evidence		Findings	
------------	--	-----------	---	----------	--	----------	--

N/A	Pass	Fail	#	Check List Item	RISK		
			19	<i>Permit only required Outbound Protocols and Services (ACK Scan test).</i>	H		
Risk of Non Compliance	Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks						
Procedure	Perform Port scanning of the internal Interface IP from PC FBSD 192.168.22.210 with ACK packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sA -p 1-65535 -oN outbound-ack-scan.txt 192.168.22.1 (ACK Scan to look for open ports) Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w outbound-ack-scan. cap host xxx.xxx.xxx.x27						
Verify	Should not detect any open ports. Verify the logged data if the scanning activity is detected. Check tcpdump for records of the port scan traffic.						
Conclusion							
Reference	SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504						
Subjective		Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK		
			20	<i>Reject Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Log Event.</i>	M		
Risk of Non Compliance	Intruders may gather information for Denial of Service attacks.						
Procedure	Verify that ICMP protocol 8, 11, and 3 are blocked at the external interface. Login as admin to the web interface. Select Firewall > Policy > 'EXT>INT'. Check if this specific service is included in the disallowed_services group or by itself appears in the ruleset and set to deny access.						
Verify	Check predefined Service ICMP_Any is in the disallowed services list.						
Conclusion							
Reference	Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.2.2 - Exploit Protection) SANS – GSNA Courseware Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective	X	Objective	X	Evidence		Findings	

2.3.0 Address Filtering

N/A	Pass	Fail	#	Check List Item	RISK			
			21	<i>Reject all Traffic from the External Networks that bear following source IP address:</i> <i>0.0.0.0/8 Historical broadcast</i> <i>10.0.0.0/8 RFC 1918 private network</i> <i>169.254.0.0/16 Link local networks</i> <i>172.16.0.0/12 RFC 1918 private network</i> <i>192.168.0.0/16 RFC 1918 private network</i> <i>224.0.0.0/4 Class D multicast</i> <i>240.0.0.0/5 Class E reserved</i> <i>248.0.0.0/5 Unallocated</i> <i>255.255.255.255/32 Broadcast</i>	H			
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.						
Procedure		Login to Firewall as admin using the web interface. Select> firewall>Policy>'EXT>INT'						
Verify		Verify that the above addresses are included in the policy and set to deny access and logging is enabled.						
Conclusion								
Reference		MSDN – Chapter 15 – Securing your Network - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp SANS – GSNA Courseware. Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
			22	<i>Reject all Traffic from the Internal Networks that bear a source IP address which does not belong to the internal network (outbound)</i>	H			
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.						
Procedure		Check the firewall Int to Ext ruleset for the specific policy. From internal PC FBSD 192.168.22.210 execute command as below: a) hping -S xxx.xxx.xxx.x43 -a 192.168.0.20 -p 21 b) hping -S xxx.xxx.xxx.x43 -a 192.168.20.20 -p 21						
Verify		The addressees 192.168.22.0 /8 only should be allowed outbound access. Other 192.168.XXX.XXX should be denied access (policyid 21).						
Conclusion								
Reference		Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
			23	<i>Reject outbound traffic from a system using a source address that falls within the address ranges :10.0.0.0 /8, 172.16.0.0 /16, 165.255.0.0 /16</i>	H			
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.						
Procedure		Check the Firewall INT>EXT ruleset for the specific policy. From internal PC FBSD 192.168.22.210 execute command as below: hping -S 10.10.20.20 -a 172.16.20.20 -p ++21 hping -S xxx.xxx.xxx.x43 -a 10.10.20.20 hping -S xxx.xxx.xxx.x43-a 169.254.20.20						
Verify		Verify the above addresses are denied access. Verify the logs for the record of the denied activities.						
Conclusion								
Reference		Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
			24	<i>Reject inbound traffic from a system using a source address that falls within the address ranges : 10.0.0.0 /8, 172.16.0.0 /16, 165.255.0.0 /16</i>	H			
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.						
Procedure		Check the Firewall EXT>INT ruleset for the specific policy. From external PC FSAUDIT xxx.xxx.xxx.x29 execute command as below: a) hping -S xxx.xxx.xxx.x27 -a 10.10.21.21 -p 80 b) hping -S xxx.xxx.xxx.x27 -a 172.168.20.20 -p 23						
Verify		Verify the above addresses are denied access. Verify the logs for the record of the denied activities.						
Conclusion								
Reference		Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
			25	<i>Reject Outbound traffic containing broadcast addresses and Log event</i>	H			
Risk of Non Compliance		Unwitting participant in Denial of Service Attacks.						
Procedure		Check the Firewall INT>EXT ruleset for the specific policy. From internal PC FBSD 192.168.22.210 execute command as below: nmap -sS -O -P0 -e dc0 -S 255.255.255.255 192.168.22.1						
Verify		Check firewall logs to see if the broadcasts are recorded and dropped.						
Conclusion								
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.2.2 – Exploits Protection) Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

Intrusion Detection and prevention:

Some reasons for adding IDS to you firewall are:

- Double-checks misconfigured firewalls.
- Catches attacks that firewalls legitimate allow through (such as attacks against web servers).
- Catches attempts that fail.
- Catches insider hacking.

(Ref: Technical Incursion Countermeasures: FAQ – Network Intrusion Detection Systems
<http://www.ticm.com/kb/faq/idsfaq.html>)

Overview:

The Fortigate-100 has a real-time Network Intrusion Detection System (NIDS). The NIDS consists of three modules designed to detect, prevent and respond to attacks. The detection module detects a wide variety of suspicious network traffic and network-based attacks. The NIDS detects and prevents the following types of attacks:

- Denial of service attacks
- Reconnaissance
- Exploits
- NIDS evasion

For the purpose of this paper the checklist is designed to verify the configuration of IDS and ID prevention and perform a ip spoofing test to verify the preventive function of the IDS. The, IDS detection module consists of individual attack signatures contained in a group. For example:

Denial of Service attack signature group consists of:

ID	Rule Name	Revision
917505	Jolt attack	10
101580802	Land attack	10
286130179	Teardrop attack	10
286130180	UDP echo+chargen bomb	10
917509	IGMP dos attack	10
917510	IGMP dos attack	10
101580808	NAPTHA	10
101580815	Winnuke attack	10
917520	Cisco IPv4 SWIPE	10
917521	Cisco IPv4 Mobility	10
917522	Cisco IPv4 Sun ND	10
917523	Cisco IPv4 PIM	10

(Ref: Fortinet - Fortigate- NIDS Guide)

2.4.0 Intrusion Detection and Prevention

N/A	Pass	Fail	#	Check List Item	RISK	
			26	Interfaces both internal and external must be monitored for network-based attacks.	H	
Risk of Non Compliance		<ul style="list-style-type: none"> Inability to detect misconfigured firewalls. Inability to detect attacks that firewalls legitimately allow through (such as attacks against web servers). Inability to detect insider hacking. 				
Procedure		Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids detection interfaces				
Verify		Both the internal and external is set to ON. Verify the DMZ interface is set to OFF.				
Conclusion						
Reference		Fortinet – Fortigate NIDS Guide. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 5.5 CISCO IOS Intrusion Detection). Technical Incursion Countermeasures: FAQ – Network Intrusion Detection Systems http://www.ticm.com/kb/faq/idsfaq.html				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			27	Checksum verification must be turned ON. This feature tests files passing through the Fortigate-100 to make sure that they have not been changed in transit.	H	
Risk of Non Compliance		Inability to detect malicious changes in data during transit.				
Procedure		Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids detection checksum				
Verify		Verify the Conclusions: it must be IP: ON, TCP: ON, UDP: ON and ICMP:ON				
Conclusion						
Reference		Fortinet – Fortigate NIDS Guide.				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			28	All attack detection Signatures must be enabled. The NIDS detection module uses over 1000 signatures arranged into groups. By default all groups are enabled.	H	
Risk of Non Compliance		Inability to match and detect patterns of security violations of most common network attacks.				
Procedure		Open the web interface: https://192.168.22.1 . Login as admin. Go to NIDS > Detection > Signature List				
Verify		All signatures must be enabled.				
Conclusion						
Reference		Fortinet – Fortigate NIDS Guide. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 5.5 CISCO IOS Intrusion Detection).				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			29	NIDS attack prevention must be enabled. This module is disabled by default!	MH	
Risk of Non Compliance		Inability to prevent the damage either by dropping the packets or by blocking network access.				
Procedure		Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids prevention status.				
Verify		Verify IDP is enabled.				
Conclusion						
Reference		Fortinet – Fortigate NIDS Guide.				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			30	All attack prevention signatures must be enabled.	H	
Risk of Non Compliance		Inability to prevent the damage either by dropping the packets or by blocking network access.				
Procedure		Open the web interface: https://192.168.22.1 . Login as admin. Go to NIDS > Prevention				
Verify		‘Enable prevention’ is checked. Verify that all individual prevention signature groups are enabled.				
Conclusion						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 – DISA Field Security Operations. Fortinet – Fortigate NIDS Guide.				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK			
			31	Test ID Prevention is functioning.	H			
Risk of Non Compliance		Undetected internal or external attacks resulting in Denial of Service and or damage to systems and data.						
Procedure		From the internal Test PC FSBD 192.168.22.210 execute the following command hping -S 192.168.22.1 -a 255.255.255.255						
Verify		Check the IDS prevention detects and prevents and logs the attack.						
Conclusion								
Reference		Fortinet – Fortigate NIDS Guide.						
Subjective			Objective	X	Evidence		Findings	

2.5.0 AV / File Blocking Protection

In Fortigate-100 Antivirus protection is enabled in firewall policies. When it is enabled a content profile is selected that controls how the antivirus protection behaves. Content profiles control the type of traffic protected (HTTP, FTP, IMAP, POP3, SMTP), the type of antivirus protection (scan, block, quarantine) and the treatment of fragmented e-mail and oversized files or email. Note: Quarantine feature not available in Fortigate-100 series.

N/A	Pass	Fail	#	Check List Item	RISK			
			32	Content filtering must be enabled in the firewall policy.	MH			
Risk of Non Compliance		Malicious codes and viruses infecting internal network. Some may create backdoor connections for intruders.						
Procedure		Login to the web interface. Select Firewall>Policy>'INT>EXT'> Open (Edit) Policyid 2.						
Verify		Antivirus and Web filter must be enabled and the 'Strict' content profile must be in use.						
Conclusion								
Reference		Fortinet – Content Protection Guide						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK	
			33	Verify contents of 'Strict Content profile'. This controls how the antivirus protection behaves.	H	
Risk of Non Compliance		Downloading of infected files or programs containing malicious codes or viruses.				
Procedure		Login as admin at the web Interface. Select firewall> Content Profile>Strict.				
Verify		All options must be selected for protection, except 'pass fragmented e-mails'.				
Conclusion						
Reference		Fortinet – Content Protection Guide				
Subjective			Objective	X	Evidence	Findings

N/A	Pass	Fail	#	Check List Item	RISK	
			34	File blocking must be enabled to remove all files that pose a potential threat and to provide the best protection from active computer virus attacks.	H	
Risk of Non Compliance		Downloading of files or programs containing malicious codes or viruses.				
Procedure		Login to the web interface as admin. Select: Antivirus>File Block.				
Verify		Only files with .doc, .ppt, .xl extensions must be unblocked for HTTP, FTP, IMAP, POP3, SMTP protocols. All other file extensions must be blocked for all protocols.				
Conclusion						
Reference		Fortinet – Content Protection Guide				
Subjective			Objective	X	Evidence	Findings

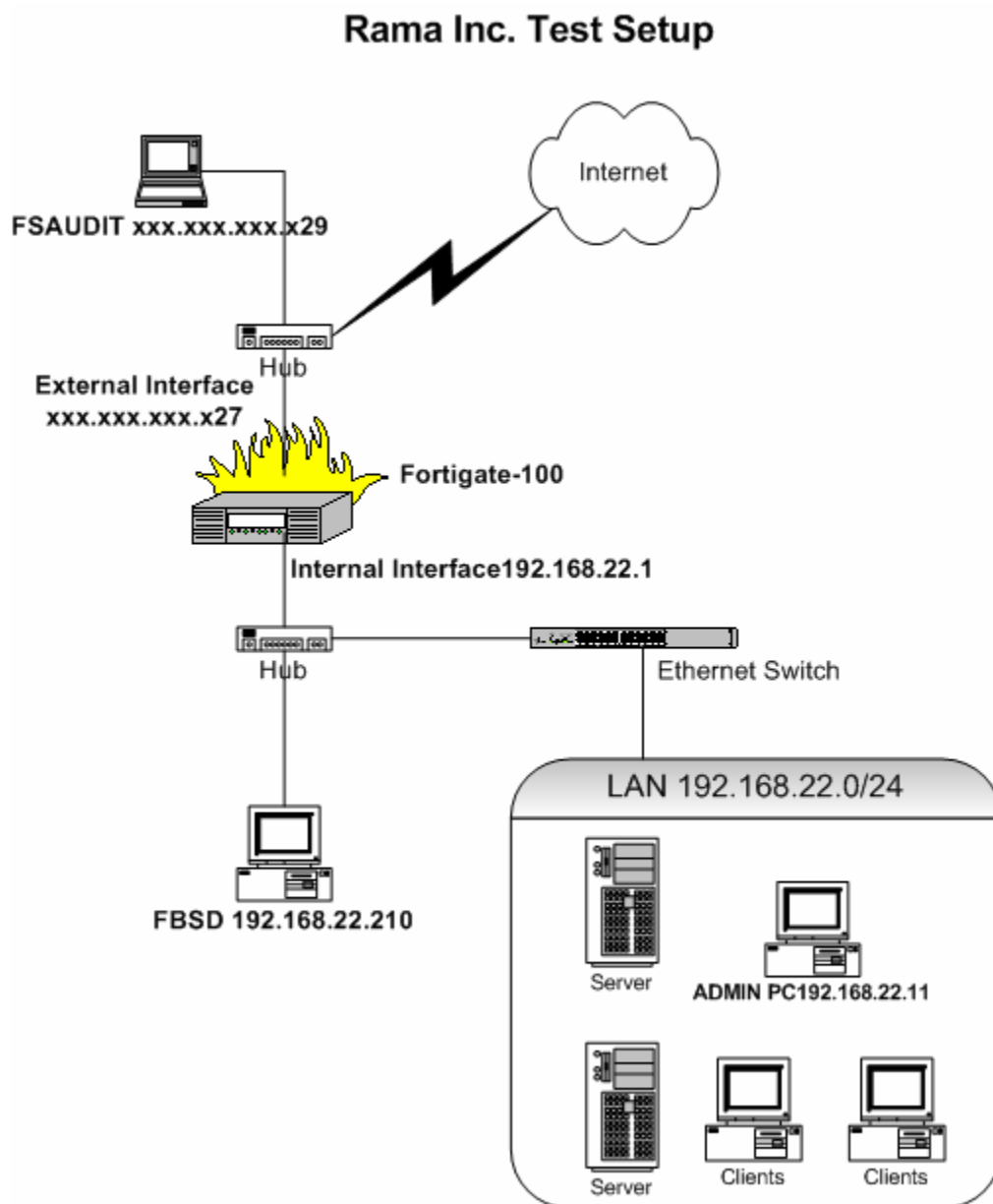
N/A	Pass	Fail	#	Check List Item	RISK	
			35	Test File blocking functionality.	H	
Risk of Non Compliance		Downloading of files or programs containing malicious codes or viruses.				
Procedure		From any internal PC browse to http://www.winzip.com and attempt to download a trial version of winzip.exe				
Verify		The down load must be blocked with a security alert message.				
Conclusion						
Reference		Fortinet – Content Protection Guide				
Subjective			Objective	X	Evidence	Findings

Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings

Firewall Internal Interface Address: 192.168.22.1/24

Firewall External Address: xxx.xxx.xxx.x27

Other Internet address used for testing: xxx.xxx.xxx.x43



Tools Used:

PC with FREEBSD Operating System (Ref:<http://www.freebsd.org/>) for Testing: INT > EXT (FBSD: 192.168.22.210)

PC with Redhat Linux Operating System (Ref:<http://fedora.redhat.com/>) for Testing: EXT > INT (Customer Provided Internet Address FSAUDIT: xxx.xxx.xxx.x29)

PC with Windows 2000 Professional for Firewall Administration and data collection (IP Address 192.168.22.11)

Software tools:

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. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL. (Ref: <http://www.insecure.org/nmap/>)

NmapNT: nmapNT V. 2.53 SP1 by ryan@eEye.com eEye Digital Security. nmapNT is a windows port of the most popular network scanning tool to date, nmap. Nmap, which to date only ran under Unix, has a superior ability to map out and scan remote networks. Now this same power can be taken advantage of from NT platforms (Ref:<http://www.eeye.com/html/resources/downloads/other/index.html>). NmapNT is based on nmap by fyodor@insecure.org (<http://www.insecure.org/nmap/>).

Hping: hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. (Ref: <http://www.hping.org/>)

Ethereal: Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. It has all of the standard [features](#) you would expect in a protocol analyzer, and several features not seen in any other product. Its open source [license](#) allows talented [experts](#) in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows. (Ref: <http://www.ethereal.com/>)

Tcpdump: It allows capturing, troubleshooting and analyzing network packets. More information can be obtained from <http://www.tcpdump.org/>

Putty: PuTTY is a free SSH, Telnet and Rlogin client for 32-bit Windows systems. SSH, Telnet and Rlogin are three ways of doing the same thing: logging in to a multi-user computer from another computer, over a network. It is written and maintained primarily by [Simon Tatham](#). Ref: <http://putty.bhni.net/>

Kiwi Syslog Daemon: Kiwi Syslog Daemon is a freeware Syslog Daemon for Windows. It receives, filters, logs, displays and forwards Syslog messages and SNMP traps from

hosts such as routers, switches, Unix hosts and any other syslog enabled device (Ref: <http://www.kiwisyslog.com/>)

Instructions:

Perform all testing and verifications as per procedure in each of the items in the checklist. Connect to the internal interface ip 192.168.22.1 of the firewall using secure shell program “putty” for Command Line Interface. Web interface must only be used with SSL: <https://192.168.22.1>. Use Command Line Interface (CLI) or Web Interface wherever applicable.

The Proof / Evidence of the tests are shown below each checklist item.

The Findings are noted in ‘Conclusion’.

3.1.0 Access and Configuration /Change Management

N/A	Pass	Fail	#	Check List Item	RISK			
	1.a X	1.b X	1	a) Only FW administrator and other authorized personnel will be granted access to the FW for administration. b) Firewall should be administered from a trusted host.	H			
Risk of Non Compliance		Unauthorized user access and unsecured hosts leave the firewall susceptible for intruders to modify the firewall rules, corrupt its integrity and deny its availability to legitimate users.						
Procedure:		Connect to internal interface of the firewall using SSH Client Putty. At the Command Line Interface (CLI) Login as Administrator and execute the following commands : a) Fortigate-100 # get system admin. Note the results b) Fortigate-100 # get config. Note the results.						
Verify		The results will show the admin users name and the specific trusted ip address from which they can connect to the FW and their read/write permissions.						
Conclusion		Although the results are for test 1.a is incompliance, it is recommended that an additional, separate, user with read write permissions is created for administering the Firewall. See Part 4: Identified Vulnerabilities – Details. Test 1.b Failed. It is presently set to be administered from any internal PC!						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.4 Router Accounts) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 3.3 –Managing the Router and 4.1.5. – Logins, Privileges, Passwords and Accounts) Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence	X	Findings	X

```

192.168.22.1 - PuTTY
login as: admin
admin@192.168.22.1's password:
Type ? for a list of commands.

Fortigate-100 # get system admin
name      ip          netmask    read per   write per
admin     0.0.0.0     0.0.0.0    allowed    allowed

Fortigate-100 # █

```

```

Fortigate-100 # get config
set system opmode nat
set system tcp_option enable
set system admin username admin password 'Enc $1$$p.kEiPgWlfYBnGpjR8&Si.' trusth
ost 0.0.0.0 0.0.0.0

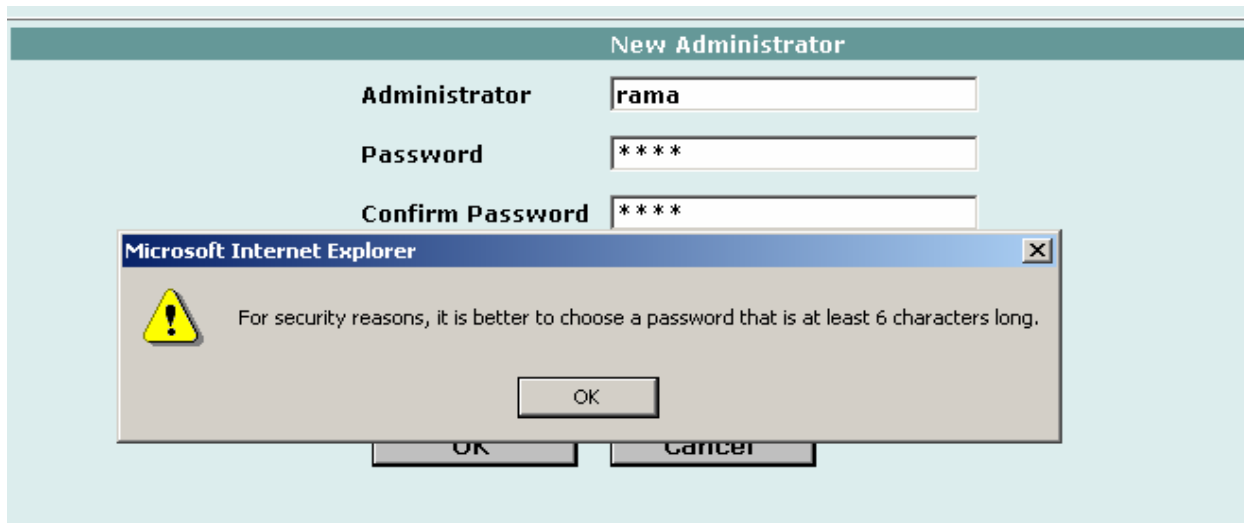
```

N/A	Pass	Fail	#	Check List Item	RISK		
	X		2	<i>The administrator and other authorized users account password will be encrypted and should be at least 6 characters long.</i>	H		
Risk of Non Compliance	Clear text passwords give easy access (password cracking) for intruders to misconfigure the firewall.						
Procedure	At the CLI Login as Administrator and execute the following command: a) Fortigate-100 # get config. Note the results. b) Create a new user with a password less than 6 characters. A Warning should appear.						
Verify	The password is encrypted. For Passwords less than 6 characters a warning appears.						
Conclusion	Password is encrypted and the warning appears						
Reference	Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Security Operations (Section 3.5.5 Router Passwords). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.5. – Logins, Privileges, Passwords and Accounts). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective		Objective	X	Evidence	X	Findings	X

```

Fortigate-100 # get config
set system opmode nat
set system tcp_option enable
set system admin username admin password 'Enc $1$$p.kEiPgWlfYBnGpjR8&Si.' trusth
ost 0.0.0.0 0.0.0.0

```



N/A	Pass	Fail	#	Check List Item	RISK		
	X		3	<i>The time out period for unattended console is set for no longer than 15 minutes. Activating this timeout period provides additional security</i>	H		
Risk of Non Compliance		Abuse from casual or malicious use through the open session (for longer timeout periods) by unauthorized users, if they get physical access to the session.					
Procedure		At the Command Line Interface (CLI) Login as Administrator and execute the following command: a) Fortigate-100 # get system option. Note the results. b) Login and wait for the expiration timeout period. The system must force you to re login					
Verify		The values for 'Admin timeout' is 15 minutes.					
Conclusion		The admin time out is in compliance and the timeout period is effective.					
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.4 Router Accounts). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective		Objective	X	Evidence	X	Findings	X

```

Fortigate-100 # get system option
Admin timeout: 15 minutes
Auth timeout: 15 minutes
interval: 5 seconds
fail_time: 5 times
Language: english
GUI refresh interval: 30 seconds
Configuration update:
    FortiManager      : 0.0.0.0
    SNMP community    :
    update on boot    : no
radius port: 1812

Fortigate-100 #

```

N/A	Pass	Fail	#	Check List Item	RISK			
	X		4	The FW administrator will ensure modems will not be used for remote administration	H			
Risk of Non Compliance		War-dialing. Enables a backdoor for malicious purposes.						
Procedure		Check if an auxiliary console for Modem Connection is available, if available check if it is disabled						
Verify		Physically.						
Conclusion		No Modem Connection Available for Fortigate-100 series.						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.6 – Out-of-band Management). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.6 Remote Access) Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence		Findings	

N/A	Pass	Fail	#	Check List Item	RISK			
		X	5	The FW administrator will disable FW interfaces that are not in use	H			
Risk of Non Compliance		Scanning and spoofing attacks, unauthorized access attempts to the firewall through un-trusted network. If successful, enables a backdoor for the intruder to the firewall and to the internal network.						
Procedure		At the CLI Execute the following command: Fortigate-100 # get system interface						
Verify		The lists of interfaces that are up are shown. Ensure that the DMZ interface is disabled.						
Conclusion		The DMZ Interface is not Disabled. It is Administratively up and running						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.6 – Out-of-band Management). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence	X	Findings	X

```
Fortigate-100 # get system interface
Interface internal
  primary IP address:192.168.22.1 255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0 0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FC
  (NIC mac address): (00:09:0f:02:00:fc)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping,https,ssh
  second access:
  Status:administrative UP      RUNNING
Interface external
  primary IP address:      255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0 0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FD
  (NIC mac address): (00:09:0f:02:00:fd)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping
  second access:
  Status:administrative UP      RUNNING
Interface dmz
  primary IP address:10.10.10.1 255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0 0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FE
  (NIC mac address): (00:09:0f:02:00:fe)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping,https
  second access:
  Status:administrative UP      RUNNING
```

N/A	Pass	Fail	#	Check List Item	RISK			
		X	6	<i>Ensure that only ports on the internal interface will be used for administrative access to the FW and they are restricted to SSH or SSL encryptions.</i>	H			
Risk of Non Compliance		Man-in-the-middle attack, Session hijacking.						
Procedure		At the CLI Execute the following command: a) Fortigate-100 # get system interface. Note the results. b) Try login to the external interface through web interface or using putty.						
Verify		Check if the line “access:” reads ‘ssh, https’ only for the internal interface. You should not be able to login to the external interface of the firewall.						
Conclusion		Although the tests results were positive. The DMZ is also set to be connected for connection through HTTPS!						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.7 – In-band Router Management) Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 5.3 – Using SSH for Remote Administration security). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence	X	Findings	X

© SANS Institute 2004, Author


```
Fortigate-100 # get system interface
Interface internal
  primary IP address:192.168.22.1 255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0    0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FC
  (NIC mac address): (00:09:0f:02:00:fc)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping,https,ssh
  second access:
  Status:administrative UP          RUNNING
Interface external
  primary IP address:                255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0    0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FD
  (NIC mac address): (00:09:0f:02:00:fd)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping
  second access:
  Status:administrative UP          RUNNING
Interface dmz
  primary IP address:10.10.10.1 255.255.255.0
  Detect Serv:      disable
  secondary IP address:0.0.0.0    0.0.0.0
  Detect Serv:      disable
  mac address: 00:09:0F:02:00:FE
  (NIC mac address): (00:09:0f:02:00:fe)
  mtu: OFF 1500bytes
  speed: auto
  zone:
  Log to this: enable
  access: ping,https
  second access:
  Status:administrative UP          RUNNING
```

N/A	Pass	Fail	#	Check List Item	RISK		
	X		7	The FW administrator will ensure all administrative access and modification to the FW configuration are logged.	H		
Risk of Non Compliance	Undetected firewall access violations and configuration changes to the firewall settings.						
Procedure	Log in as admin using the web interface: https://192.168.22.1 a) Select Log&Report>Log setting>Config Policy. b) Select HA activity event and select ok. Deselect HA activity event and select ok.						
Verify	a) Verify that under Log & Report > Log Setting > config Policy > Event log: 'admin login/logout event' and 'when configuration has changed' are selected. b) Check the logs to verify the log policy changes are recorded.						
Conclusion	In Compliance						
Reference	Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.5.7 – In-band Router Management Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1) (Section 3.3.3 Logging and 4.5.2 – Configuring Logging and Time Services). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective		Objective	X	Evidence	X	Findings	X

Log Setting Traffic Filter

Log to Remote Host
 IP: Port:
 Level: **Config Policy**
 CSV format: Enable

Log in WebTrends Enhanced Log Format
 IP:
 Level: **Config Policy**

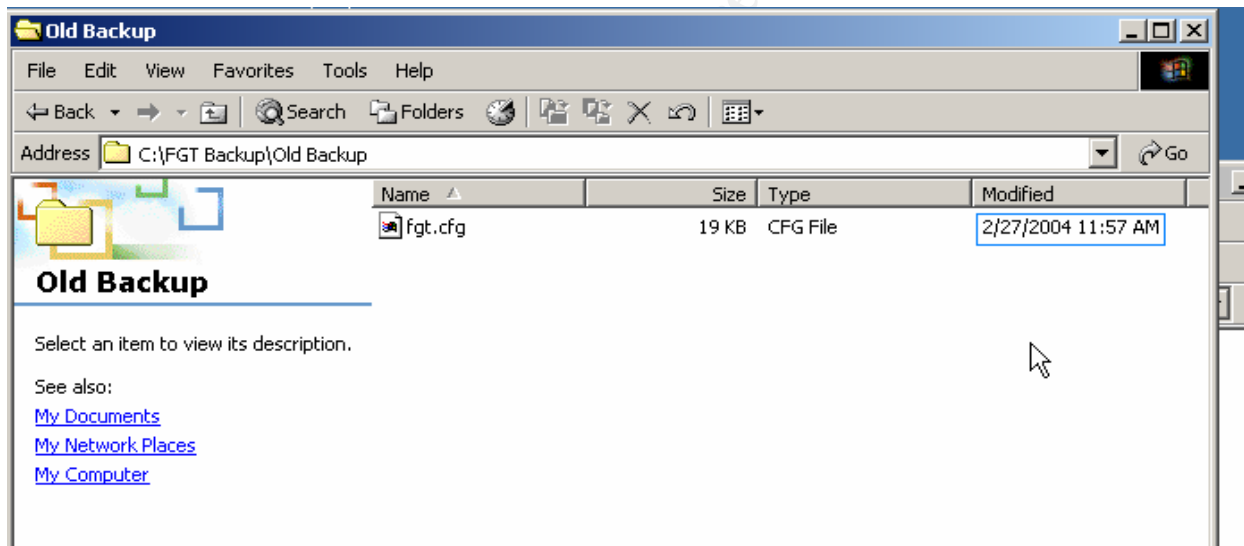
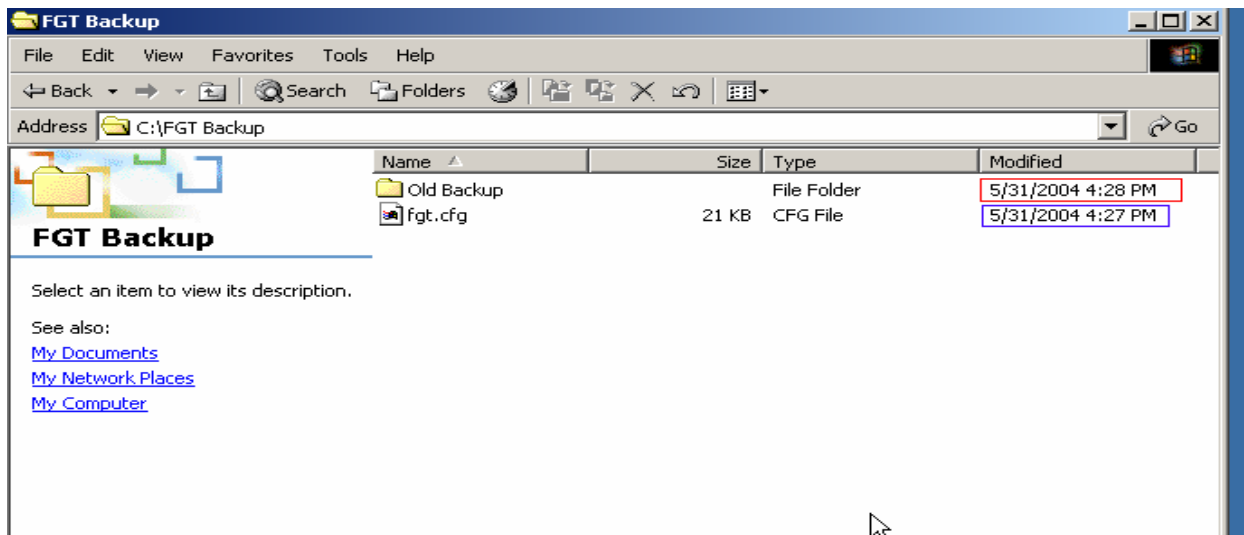
Log to Memory (all except traffic log)
 Level: **Config Policy**



```

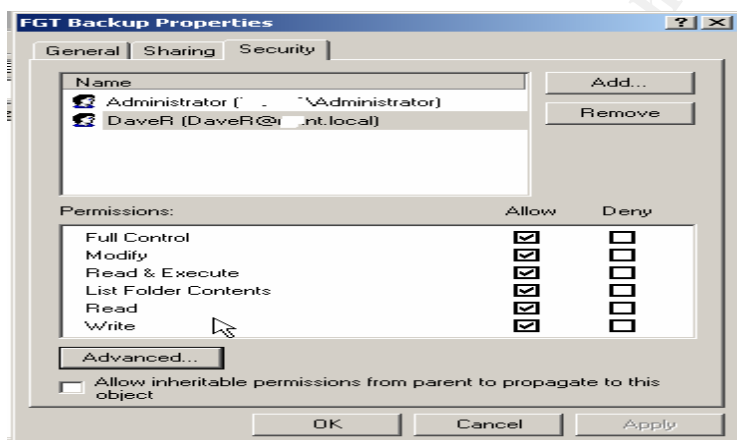
192.168.22.11"
Local7.INFO:192.168.22.1: date=2004-06-03 time=08:36:22 device_id=#GT1002801021129 log_id=0100090112 (type=event)
      subtype=config pri=information user=admin ui=GUI(192.168.22.1) module=log submodule=logsetting msg="Log
      Policy has been modified by user admin via GUI(192.168.22.11)"
  
```

N/A	Pass	Fail	#	Check List Item	RISK
	X		8	<i>The current and previous router configuration are backed up and saved in a secure location.</i>	MH
Risk of Non Compliance	Unauthorized configuration changes and corruption of the stored files. No backup protection affects Real-time Recovery Objective (RTO).				
Procedure	a) Ask admin to show the back up configuration file location. b) Create a new back up and store it in the same directory (for next item 9).				
Verify	Check the creation dates of the configuration back up files. They must be different. Check if the files are stored in a secure system.				
Conclusion	In compliance. The files are stored in a PC with Windows 2000 Professional Operating System, with admin access only. Note: The administrator consolidated the backup on the same date 5/31/2004. The old back up and the new backup are of different dates and the permissions set are identical.				
Reference	Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.3 –Logistics for Configuration Loading and Maintenance). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 3.3.2 Updating the Router and 4.1.8 – Logistics for configuration Loading and Maintenance). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective		Objective	X	Evidence	X Findings X



© SANS

N/A	Pass	Fail	#	Check List Item	RISK		
	X		9	<i>On the system where the configuration files are stored, the local operating system's security mechanisms will be used for restricting access to the files</i>	MH		
Risk of Non Compliance		Unauthorized configuration changes and corruption of the stored files. No backup protection affects Real-time Recovery Objective (RTO).					
Procedure		Ask admin to show the location of the backup configuration files. Compare the security permissions of the old and newly backed up configuration files (previous item 8).					
Verify		Check if the folder is located in a NTFS formatted volume. Check the security properties of the folder. Verify that only the administrator (S) of the firewall has full permission to the folder.					
Conclusion		The files are stored in a PC with Windows 2000 Professional Operating System, with admin access only					
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.3 –Logistics for Configuration Loading and Maintenance). Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.8 – Logistics for configuration Loading and Maintenance). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective		Objective	X	Evidence	X	Findings	X



N/A	Pass	Fail	#	Check List Item	RISK			
		X	10	Ensure that the latest patches and updates are applied to the firewall components. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.	H			
Risk of Non Compliance		Exploitation of known vulnerabilities.						
Procedure		a) Use web interface and login as the administrator. Note the Firmware, Anti Virus and attack definition Versions. b) Ask the Administrator to login at the Fortinet support site and show the latest versions of these items. c) Check Automatic update function if they are enabled.						
Verify		Compare the version numbers. The versions in Fortigate-100 must be the latest.						
Conclusion		Not in compliance. The firmware version is older (build212) version Build 251. Attack signatures and AV definitions are not the latest. Automatic update is not enabled. Manual update is in effect.						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations. Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.5.5 Performing Cisco Software Updates). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence	X	Findings	X

Host Name: Fortigate-100
Firmware Version: Fortigate-100 2.50,build212,040225
Antivirus Definitions Version: 4.126(09/03/2003 18:03)
Attack Definitions Version: 2.68(10/02/2003 15:14)
Serial Number: FGT1002801021129
Up Time: 1 (days) 15 (hours) 56 (minutes)
System Settings: [Backup](#) [Restore](#) [Restore Factory Defaults](#)
Operation Mode: [Change to Transparent Mode](#)
System: [Restart](#) [Shutdown](#)

Address: ftp://support.fortinet.com/v2.50/MR8/

Name	Size	Type	Modified
FGT_100-v250-build251-FORTINET.out	6.25 MB	OUT File	4/26/2004 9:34 AM
FGT_1K-v250-build251-FORTINET.out	6.36 MB	OUT File	4/26/2004 9:34 AM
FGT_200-v250-build251-FORTINET.out	6.32 MB	OUT File	4/26/2004 9:34 AM
FGT_3000-v250-build251-FORTINET.out	6.38 MB	OUT File	4/26/2004 9:34 AM

- View Products
- Add Registration
- Add/Renew Contract Number
- Download Virus/Attack Update
- Firmware Images

Download Virus/Attack Updates

Version: v2.50 | **v2.36** | v2.30

Product Model	Virus Definition	Attack Definition
FGT-100	OS2.5.0_4.348	2.50_2.109

N/A	Pass	Fail	#	Check List Item	RISK			
	X		11	<p><i>Review the ruleset EXT > INT to ensure that they follow the order as follows:</i></p> <ul style="list-style-type: none"> • <i>firewall Lockdown</i> • <i>anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)</i> • <i>Deny unwanted inbound services</i> • <i>User permit rules (allow CITRIX ICA and HTTPS)</i> • <i>Noise drops (e.g. discard multicasts, OSPF and HSRP chatter)</i> • <i>Deny and Alert (alert systems administrator about traffic that is suspicious)</i> • <i>Deny and log (log remaining traffic for analysis)</i> <p><i>Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.</i></p>	H			
Risk of Non Compliance		Misconfiguration. Ineffective rulesets.						
Procedure		Login as admin using the web interface. a) Select Firewall>Addresses>External - Note the results b) Select Firewall > Policy > 'EXT>INT' – Note the results						
Verify		Check the Rule order, as above. Make sure that logging is enabled for all the denied rules.						
Conclusion		The result gives the list of external addresses configured. The result gives the order of the firewall EXT>INT Policy. The firewall rule is in compliance and logging is enabled for all the denied rules.						
Reference		Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php Building Your Firewall Rulebase by Lance Spitzner http://www.spitzner.net/rules.html						
Subjective			Objective	X	Evidence	X	Findings	X

FORTINET

- System
- Firewall
 - Policy
 - Address
 - Service
 - Schedule
 - Virtual IP
 - IP Pool
 - IP/Mac Binding
 - Content Profile
- User
- VPN
- NIDS

Internal External DMZ Group

Name	IP/Netmask	Interface	Modify
External_All	0.0.0.0/0.0.0.0	external	
172_16	172.16.0.0/255.240.0.0	external	
10_0	10.0.0.0/255.0.0.0	external	
169_254	169.254.0.0/255.255.0.0	external	
224_0	224.0.0.0/255.0.0.0	external	
192_168_22_0	192.168.22.0/255.255.255.0	external	
EXT_BCAST	255.255.255.255/255.255.255.255	external	
Historical_Broadca	0.0.0.0/255.0.0.0	external	
CLASS_E	240.0.0.0/248.0.0.0	external	
Unallocated	248.0.0.0/248.0.0.0	external	

New

FORTINET

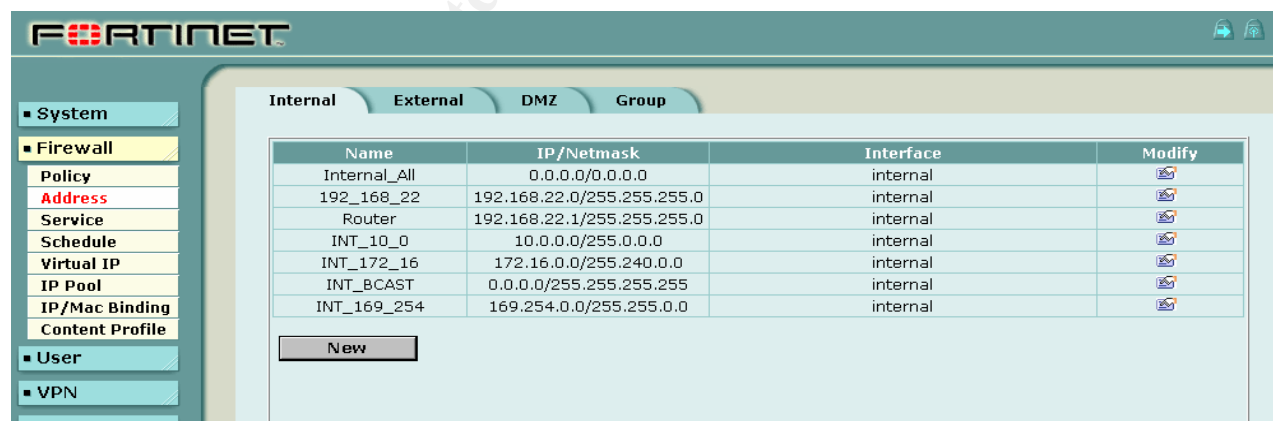
- System
- Firewall
 - Policy
 - Address
 - Service
 - Schedule
 - Virtual IP
 - IP Pool
 - IP/Mac Binding
 - Content Profile
- User
- VPN
- NIDS
- Anti-Virus
- Web Filter
- Email Filter
- Log&Report

Int->Ext Int->DMZ DMZ->Int DMZ->Ext Ext->Int Ext->DMZ

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	14	External_All	Router	Always	ANY	DENY	<input checked="" type="checkbox"/>	
2	20	EXT_BCAST	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
3	25	Historical_Broadca	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
4	26	CLASS_E	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
5	27	Unallocated	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
6	5	192_168_22_0	192_168_22	Always	ANY	DENY	<input checked="" type="checkbox"/>	
7	6	172_16	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
8	7	10_0	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
9	8	169_254	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
10	15	External_All	Internal_All	Always	Disallowed_service	DENY	<input checked="" type="checkbox"/>	
11	10	External_All	Internal_All	Always	6000_6063	DENY	<input checked="" type="checkbox"/>	
12	3	External_All	CITRIX_NFUSE	Always	CITRIX_ICA	ACCEPT	<input checked="" type="checkbox"/>	
13	4	External_All	http_server	Always	HTTPS	ACCEPT	<input checked="" type="checkbox"/>	
14	11	224_0	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
15	12	External_All	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	

New

N/A	Pass	Fail	#	Check List Item	RISK		
	X		12	<p>Review the ruleset INT > EXT to ensure that they follow the order as follows:</p> <ul style="list-style-type: none"> • allow ipsec tunnel • anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) • blocked unwanted outbound services • User permit rules (e.g. allow HTTP to public web server) • Deny and log (log remaining traffic for analysis) <p>Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.</p>	H		
Risk of Non Compliance		Misconfiguration. Ineffective rulesets.					
Procedure		Login as admin using the web interface. a) Select Firewall<Addresses>Internal - Note the results b) Select Firewall > Policy > 'INT>EXT' – Note the results					
Verify		Check the Rule order, as above. Make sure that logging is enabled for all the denied rules.					
Conclusion		<p>The result gives the list of internal addresses configured. The result gives the order of the firewall INT>EXT Policy. The order is in compliance and logging is enabled for denied accesses.</p>					
Reference		Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php Building Your Firewall Rulebase by Lance Spitzner http://www.spitzner.net/rules.html					
Subjective		Objective	X	Evidence	X	Findings	X



FORTINET

Int->Ext Int->DMZ DMZ->Int DMZ->Ext Ext->Int Ext->DMZ

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	1	192_168_22	External_All	Always	ANY	ENCRYPT	<input checked="" type="checkbox"/>	
2	19	INT_BCAST	External_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
3	13	Internal_All	External_All	Always	PROXY	DENY	<input checked="" type="checkbox"/>	
4	17	INT_172_16	External_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
5	24	INT_169_254	External_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
6	23	INT_10_0	External_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
7	2	192_168_22	External_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
8	21	Internal_All	External_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	

New

© SANS Institute 2004, Author retains full rights.

3.2.0 Port Filtering

N/A	Pass	Fail	#	Check List Item	RISK																																																																											
			13	<i>Reject the following non-required, risky protocols and services in either direction.</i>																																																																												
		X		<table border="1"> <thead> <tr> <th>Port (Transport)</th> <th>Service</th> <th>RISK</th> </tr> </thead> <tbody> <tr> <td>1 (TCP & UDP)</td> <td>tcpmux</td> <td></td> </tr> <tr> <td>7 (TCP & UDP)</td> <td>echo</td> <td></td> </tr> <tr> <td>9 (TCP & UDP)</td> <td>discard</td> <td></td> </tr> <tr> <td>11 (TCP)</td> <td>systat</td> <td></td> </tr> <tr> <td>13 (TCP & UDP)</td> <td>daytime</td> <td></td> </tr> <tr> <td>15 (TCP)</td> <td>netstat</td> <td></td> </tr> <tr> <td>19 (TCP & UDP)</td> <td>chargen</td> <td></td> </tr> <tr> <td>67 (UDP)</td> <td>bootp</td> <td></td> </tr> <tr> <td>69 (UDP)</td> <td>tftp</td> <td></td> </tr> <tr> <td>135 (TCP & UDP)</td> <td>loc-srv</td> <td></td> </tr> <tr> <td>137 (TCP & UDP)</td> <td>netbios-ns</td> <td>H</td> </tr> <tr> <td>138 (TCP & UDP)</td> <td>netbios-dgm</td> <td></td> </tr> <tr> <td>139 (TCP & UDP)</td> <td>netbios-ssn</td> <td></td> </tr> <tr> <td>177 (UDP)</td> <td>xdmcp</td> <td></td> </tr> <tr> <td>445 (TCP)</td> <td>netbios (ds)</td> <td></td> </tr> <tr> <td>512 (TCP)</td> <td>rexec</td> <td></td> </tr> <tr> <td>515 (TCP)</td> <td>lpr</td> <td></td> </tr> <tr> <td>517 (UDP)</td> <td>talk</td> <td></td> </tr> <tr> <td>518 (UDP)</td> <td>ntalk</td> <td></td> </tr> <tr> <td>540 (TCP)</td> <td>uucp</td> <td></td> </tr> <tr> <td>1900, 5000 (TCP & UDP)</td> <td>Microsoft UPnP SSDP</td> <td></td> </tr> <tr> <td>12345 (TCP)</td> <td>NetBus</td> <td></td> </tr> <tr> <td>12346 (TCP)</td> <td>NetBus</td> <td></td> </tr> <tr> <td>31337 (TCP & UDP)</td> <td>Back Orifice</td> <td></td> </tr> </tbody> </table>	Port (Transport)	Service	RISK	1 (TCP & UDP)	tcpmux		7 (TCP & UDP)	echo		9 (TCP & UDP)	discard		11 (TCP)	systat		13 (TCP & UDP)	daytime		15 (TCP)	netstat		19 (TCP & UDP)	chargen		67 (UDP)	bootp		69 (UDP)	tftp		135 (TCP & UDP)	loc-srv		137 (TCP & UDP)	netbios-ns	H	138 (TCP & UDP)	netbios-dgm		139 (TCP & UDP)	netbios-ssn		177 (UDP)	xdmcp		445 (TCP)	netbios (ds)		512 (TCP)	rexec		515 (TCP)	lpr		517 (UDP)	talk		518 (UDP)	ntalk		540 (TCP)	uucp		1900, 5000 (TCP & UDP)	Microsoft UPnP SSDP		12345 (TCP)	NetBus		12346 (TCP)	NetBus		31337 (TCP & UDP)	Back Orifice		
Port (Transport)	Service		RISK																																																																													
1 (TCP & UDP)	tcpmux																																																																															
7 (TCP & UDP)	echo																																																																															
9 (TCP & UDP)	discard																																																																															
11 (TCP)	systat																																																																															
13 (TCP & UDP)	daytime																																																																															
15 (TCP)	netstat																																																																															
19 (TCP & UDP)	chargen																																																																															
67 (UDP)	bootp																																																																															
69 (UDP)	tftp																																																																															
135 (TCP & UDP)	loc-srv																																																																															
137 (TCP & UDP)	netbios-ns		H																																																																													
138 (TCP & UDP)	netbios-dgm																																																																															
139 (TCP & UDP)	netbios-ssn																																																																															
177 (UDP)	xdmcp																																																																															
445 (TCP)	netbios (ds)																																																																															
512 (TCP)	rexec																																																																															
515 (TCP)	lpr																																																																															
517 (UDP)	talk																																																																															
518 (UDP)	ntalk																																																																															
540 (TCP)	uucp																																																																															
1900, 5000 (TCP & UDP)	Microsoft UPnP SSDP																																																																															
12345 (TCP)	NetBus																																																																															
12346 (TCP)	NetBus																																																																															
31337 (TCP & UDP)	Back Orifice																																																																															
Risk of Non Compliance	These Ports can be used for Denial of Service and or sending malicious codes.																																																																															
Procedure	Login as admin to the web interface. Select Firewall > Service > Custom The custom services are additional ports/services that are not in the predefined list. A group Disallowed_ services contains all the ports that are unnecessary and denied entry to the network. Check that this group of services are denied and logging enabled both at the EXT>INT and INT > EXT Policies.																																																																															
Verify	Verify that the list reflect the ports mentioned in this checklist.																																																																															
Conclusion	The list is in compliance for EXT>INT. The FW is a stateful inspection. No specific services are blocked outbound. Found a custom service defined as proxy not included in the denied outbound list.																																																																															

Reference	Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 3.2 Protecting the network with the Router).						
	JANET-CERT: Services that router should block. http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html						
	Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective		Objective	X	Evidence	X	Findings	X

The screenshot shows the Fortinet configuration interface for Firewall services. The 'Predefined' tab is selected. A table lists various services with their details and modify options.

Service Name	Detail	Modify
CITRIX_ICA	tcp/1-65535=>1494	
6000_6063	tcp/1-65535=>6000-6063	
PROXY	tcp/1-65535=>8000-8088	
445	tcp/1-65535=>445 udp/1-65535=>445	
Small_Services	tcp/1-65535=>1-19 udp/1-65535=>1-19	
Bootp	udp/1-65535=>67	
NETBIOS_135_139	tcp/1-65535=>135,1-65535=>137,1-65535=>138,1-65535=>139 udp/1-65535=>135,1-65535=>137,1-65535=>138,1-65535=>139	
MS_UPnP_SSDP	tcp/1-65535=>1900,1-65535=>5000 udp/1-65535=>1900,1-65535=>5000	
Netbus_BO	tcp/1-65535=>12345-12346,1-65535=>31337 udp/1-65535=>31337	

The screenshot shows the Fortinet configuration interface for Firewall groups. The 'Predefined' tab is selected. A table lists various groups with their members and modify options.

Group Name	Members	Modify
Disallowed_service	DHCP-Relay,DNS,FINGER,FTP,GOPHER,H323,SYSLOG,TALK,TELNET,445, TFTP,RIP,SNMP,Small_Services,NETBIOS_135_139,MS_UPnP_SSDP,Netbus_BO	

Below the table is a 'New' button.

© SANS Institute

FORTINET

Int->Ext Int->DMZ DMZ->Int DMZ->Ext Ext->Int Ext->DMZ

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	14	External_All	Router	Always	ANY	DENY	<input checked="" type="checkbox"/>	
2	20	EXT_BCAST	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
3	25	Historical_Broadca	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
4	26	CLASS_E	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
5	27	Unallocated	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
6	5	192_168_22_0	192_168_22	Always	ANY	DENY	<input checked="" type="checkbox"/>	
7	6	172_16	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
8	7	10_0	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
9	8	169_254	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
10	15	External_All	Internal_All	Always	Disallowed_service	DENY	<input checked="" type="checkbox"/>	
11	10	External_All	Internal_All	Always	6000_6063	DENY	<input checked="" type="checkbox"/>	
12	3	External_All	CITRIX_NFUSE	Always	CITRIX_ICA	ACCEPT	<input checked="" type="checkbox"/>	
13	4	External_All	http_server	Always	HTTPS	ACCEPT	<input checked="" type="checkbox"/>	
14	11	224_0	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	
15	12	External_All	Internal_All	Always	ANY	DENY	<input checked="" type="checkbox"/>	

New

© SANS Institute 2004, Author

N/A	Pass	Fail	#	Check List Item	RISK			
	X		14	Permit only required inbound Protocols and Services	H			
Risk of Non Compliance		Intruders may exploit unknown and not required services.						
Procedure		Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29. Use following commands inbound from the internet for TCP and UDP Ports: <ul style="list-style-type: none"> • Nmap -n -P0 -sT -p 1-65535 -oN inbound-syn-scan.txt xxx.xxx.xxx.x27 • Nmap -n -P0 -sU -p 1-65535 -oN inbound-udp-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w inboundtcp-scan.cap host 192.168.22.1 tcpdump -nn -vvv -w inboundudp-scan.cap host 192.168.22.1						
Verify		Should only detect ports 443/tcp and 1494/tcp. Verify the logged data for the scanning activity Check tcpdump for records of the port scan traffic.						
Conclusion		In compliance. Tcpcap did not register any traffic originating from scanning host. The scanning activity was detected.						
Reference		SANS – GSNA Courseware. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3 Functional Tests). SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504						
Subjective			Objective	X	Evidence	X	Findings	X

```
# nmap 3.50 scan initiated Fri Jul 9 07:12:10 2004 as: nmap -n -P0 -sT -p 1-65535 -oN
inbound-syn-scan.txt xxx.xxx.xxx.x27 [Interesting ports on xxx.xxx.xxx.x27:(The 65533 ports scanned
but not shown below are in state: filtered)]
PORT      STATE SERVICE
443/tcp   open  https
1494/tcp  open  citrix-ica
# Nmap run completed at Fri Jul 9 19:44:40 2004 -- 1 IP address (1 host up) scanned in 45150.948
seconds
```

```
# nmap 3.50 scan initiated Mon Jul 12 09:35:46 2004 as: nmap -n -P0 -sU -p 1-65535 -oN
inbound-udp-scan.txt xxx.xxx.xxx.x27
All 65535 scanned ports on xxx.xxx.xxx.x27 are: filtered
# Nmap run completed at Tue Jul 13 07:29:07 2004 -- 1 IP address (1 host up) scanned in 78801.685
seconds
```

date=2004-07-09,time=07:16:14,device_id=FGT1002801021129,log_id=0401110252,type=ids,subtype=prevention,pri=alert,attack_id=100663398,,src=xxx.xxx.xxx.x29,dst=xxx.xxx.xxx.x27,src_port=1140,dst_port=13028,interface=external,status=dropped,proto=6,service=13028/tcp,msg="TCP port scan [Reference: http://www.fortinet.com/ids/ID100663398]"

date=2004-07-09,time=07:18:02,device_id=FGT1002801021129,log_id=0401110252,type=ids,subtype=prevention,pri=alert,attack_id=100663398,,src=xxx.xxx.xxx.x29,dst=xxx.xxx.xxx.x27,src_port=1685,dst_port=30971,interface=external,status=dropped,proto=6,service=30971/tcp,msg="TCP port scan [Reference: http://www.fortinet.com/ids/ID100663398]"

N/A	Pass	Fail	#	Check List Item	RISK			
	X		15	Permit only required inbound Protocols and Services (Fin Scan).	H			
Risk of Non Compliance		Intruders may exploit unknown and not required services. Helps to determine open and closed ports.						
Procedure		Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29 with FIN packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sF -p 1-65535 -oN inbound-fin-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w inbound-fin-scan. cap host 192.168.22.1 						
Verify		Should not detect any open ports. Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.						
Conclusion		No ports detected. Scanning activity logged. No activity in tcpdump records.						
Reference		SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504						
Subjective		Objective		X	Evidence	X	Findings	X

```
# nmap 3.50 scan initiated wed Jul 14 11:48:17 2004 as: nmap -n -P0 -sF -p 1-65535 -oN
inbound-fin-scan.txt xxx.xxx.xxx.x27
All 65535 scanned ports on xxx.xxx.xxx.x27 are: filtered
# Nmap run completed at Thu Jul 15 09:42:05 2004 -- 1 IP address (1 host up) scanned in 78828.459
seconds
```

```
2004-07-14 11:58:33 Local7.Alert 192.168.22.1 date=2004-07-14,time=11:53:29,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=7274504,,src=xxx.xxx.xxx.x29,dst=xxx.xxx.xxx.x27,src_port=58736,dst_port=36463,status=detected,proto=6,service=36463/tcp,msg="tcpreassemble: STEALTH ACTIVITY (FIN scan)[Reference: http://www.fortinet.com/ids/ID7274504]"
```

```
2004-07-15 08:20:59 Local7.Alert 192.168.22.1 date=2004-07-15,time=08:15:46,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=7274504,,src=xxx.xxx.xxx.x29,dst=xxx.xxx.xxx.x27,src_port=58737,dst_port=39481,status=detected,proto=6,service=39481/tcp,msg="tcpreassemble: STEALTH ACTIVITY (FIN scan)[Reference: http://www.fortinet.com/ids/ID7274504]"
```

N/A	Pass	Fail	#	Check List Item	RISK
	X		16	Permit only required inbound Protocols and Services (ACK Scans).	H
Risk of Non Compliance	Intruders may exploit unknown and not required services. Helps to determine ports that allow established connections.				
Procedure	Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29 with ACK packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sA -p 1-65535 -oN inbound-ack-scan.txt xxx.xxx.xxx.x27 Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: <pre>tcpdump -nn -vvv -w inbound-ack-scan.cap host 192.168.22.1</pre>				
Verify	Should not detect any open ports Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion	No ports detected. Scanning activity logged. No activity in tcpdump records.				
Reference	SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective		Objective	X	Evidence	X Findings X

```
# nmap 3.50 scan initiated Tue Jul 13 12:20:56 2004 as: nmap -n -P0 -sA -p 1-65535 -oN inbound-ack-scan.txt xxx.xxx.xxx.x27 000
All 65535 scanned ports on xxx.xxx.xxx.x27 are: filtered00
# Nmap run completed at wed Jul 14 02:58:04 2004 -- 1 IP address (1 host up) scanned in 52628.584 seconds0
```


date=2004-07-

13,time=17:57:02,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=101449738,,src=xxx.xxx.xxx.x29,dst=xxx.xxx.xxx.x27,src_port=38115,dst_port=20432,status=detected,proto=6,service=20432/tcp,msg="ddos: shaft client to handler[Reference: http://www.fortinet.com/ids/ID101449738]"

2004-07-14 12:05:22 Local7.Alert 192.168.22.1 date=2004-07-

14,time=12:00:18,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=6553601,,interface=external,status=detected,msg="portscan: xxx.xxx.xxx.x29 is port-scanning to port 42463 on external (STEALTH)"

N/A	Pass	Fail	#	Check List Item	RISK
	X		17	Permit only required Outbound Protocols and Services.	H
Risk of Non Compliance	Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks				
Procedure	Perform Port scanning of the internal Interface IP from PC FBSD 192.168.22.210. Use following commands: <ul style="list-style-type: none"> • Nmap -n -P0 -sT -p 1-65535 -oN outbound-syn-scan.txt 192.168.22.1 • Nmap -n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1* (nmapnt -n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1)* • Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w servicesouttcp-scan.cap host xxx.xxx.xxx.x27 (for TCP) tcpdump -nn -vvv -w servicesoutudp-scan.cap host xxx.xxx.xxx.x.27 (for UDP) 				
Verify	Should only detect ports 22/tcp and 443/tcp Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion	Only port 22/tcp and 443/tcp were detected. Scanning activity logged. No activity in tcpdump records.				
Reference	SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective		Objective	X	Evidence	X Findings X

```
# nmap 3.50 scan initiated Thu Jul 8 10:29:27 2004 as: nmap -n -P0 -sT -p 1-65535 -oN
outbound-syn-scan.txt 192.168.22.1 0Interesting ports on 192.168.22.1:(The 65533 ports scanned but not shown
below are in state: filtered)000
PORT      STATE SERVICE000
22/tcp    open  ssh0
443/tcp   open  https0
# Nmap run completed at Thu Jul 8 18:48:44 2004 -- 1 IP address (1 host up) scanned in 29957.303 seconds0
```

```
# Nmap (v. nmap) scan initiated 2.53 as: nmapnt -n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt
192.168.22.1
All 65535 scanned ports on (192.168.22.1) are: filtered
# Nmap run completed at Tue Jul 13 07:30:13 2004 -- 1 IP address (1 host up) scanned in 78823 seconds
```

*Note: Due to hardware failure of PC that is running Free BSD (FSBD) we configured an available Windows 200 Professional PC with the same computer name and IP address to perform the above UDP test using NmapNT. This change applies to checklist items 17, 18 and 19 only.

```
date=2004-07-
08,time=10:37:58,device_id=FGT1002801021129,log_id=0401110252,type=ids,subtype=preven
tion,pri=alert,attack_id=100663398,,src=192.168.22.210,dst=192.168.22.1,src_port=4610,dst_po
rt=33337,interface=internal,status=dropped,proto=6,service=33337/tcp,msg="TCP port scan
[Reference: http://www.fortinet.com/ids/ID100663398]"
```

```
date=2004-07-
08,time=10:39:37,device_id=FGT1002801021129,log_id=0401110252,type=ids,subtype=preven
tion,pri=alert,attack_id=100663398,,src=192.168.22.210,dst=192.168.22.1,src_port=1104,dst_po
rt=58891,interface=internal,status=dropped,proto=6,service=58891/tcp,msg="TCP port scan
[Reference: http://www.fortinet.com/ids/ID100663398]"
```

N/A	Pass	Fail	#	Check List Item	RISK
	X		18	<i>Permit only required Outbound Protocols and Services (FIN Scan test).</i>	H
Risk of Non Compliance	Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks				
Procedure	Perform Port scanning of the internal Interface IP from PC FBSD 192.168.22.210 with FIN packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sF -p 1-65535 -oN outbound-fin-scan.txt 192.168.22.1* (nmapnt -n -P0 -sF -p 1-65535 -oN outbound-fin-scan.txt 192.168.22.1)* Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: tcpdump -nn -vvv -w outbound-fin-scan. cap host xxx.xxx.xxx.x27 				
Verify	Should not detect any open ports: Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion	No ports detected. Scanning activity logged. No activity in tcpdump records.				
Reference	SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective		Objective	X	Evidence	X Findings X

*Note: Due to hardware failure of PC that is running Free BSD (FSBD) we configured an available Windows 200 Professional PC with the same computer name and IP address to perform this test using NmapNT. This change applies to checklist items 17, 18 and 19 only.

```
# Nmap (v. nmap) scan initiated 2.53 as: nmapnt -n -P0 -sF -p 1-65535 -oN outbound-fin-scan.txt
192.168.22.1
All 65535 scanned ports on (192.168.22.1) are: filtered
# Nmap run completed at Sat Jul 10 06:23:42 2004 -- 1 IP address (1 host up) scanned in 79005 seconds
```

```
date=2004-07-
09,time=21:37:42,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detecti
on,pri=alert,attack_id=7274504,,src=192.168.22.210,dst=192.168.22.1,src_port=47068,dst_port
=40525,status=detected,proto=6,service=40525/tcp,msg="tcpreasembly: STEALTH
ACTIVITY (FIN scan)[Reference: http://www.fortinet.com/ids/ID7274504]"
```

```
date=2004-07-
09,time=21:37:48,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detecti
on,pri=alert,attack_id=7274504,,src=192.168.22.210,dst=192.168.22.1,src_port=47067,dst_port
=40535,status=detected,proto=6,service=40535/tcp,msg="tcpreasembly: STEALTH
ACTIVITY (FIN scan)[Reference: http://www.fortinet.com/ids/ID7274504]"
```

N/A	Pass	Fail	#	Check List Item	RISK
	X		19	<i>Permit only required Outbound Protocols and Services (ACK Scan test).</i>	H
Risk of Non Compliance	Malicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting participant in DDos attacks				
Procedure	Perform Port scanning of the internal Interface IP from PC FBSD 192.168.22.210 with ACK packets to see if they are handled differently. Use following commands: <ul style="list-style-type: none"> Nmap -n -P0 -sA -p 1-65535 -oN outbound-ack-scan.txt 192.168.22.1* (nmapnt -n -P0 -sA -p 1-65535 -oN outbound-ack-scan.txt 192.168.22.1)* Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: <pre>tcpdump -nn -vvv -w outbound-ack-scan. cap host xxx.xxx.xxx.x27</pre>				
Verify	Should not detect any open ports Verify the logged data for the scanning activity. Check tcpdump for records of the port scan traffic.				
Conclusion	No ports detected. Scanning activity logged. No activity in tcpdump records.				
Reference	SANS – GSNA Courseware SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton. Tuesday, March 16, 2004, 1:00pm EST (1800 UTC) http://www.sans.org/webcasts/show.php?webcastid=90504				
Subjective		Objective	X	Evidence	X Findings X

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -n -P0 -sA -p 1-65535 -oN outbound-ack-scan.txt 192.168.22.1
All 65535 scanned ports on (192.168.22.1) are: filtered
# Nmap run completed at Tue Jul 13 18:02:44 2004 -- 1 IP address (1 host up) scanned in 20571 seconds
```

*Note: Due to hardware failure of PC that is running Free BSD (FSBD), we configured an available Windows 200 Professional PC with the same computer name and IP address to perform this test using NmapNT. This change applies to checklist items 17, 18 and 19 only.

date=2004-07-

```
13,time=13:10:42,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=102367244,,src=192.168.22.210,dst=192.168.22.1,src_port=52105,dst_port=6496,status=detected,proto=6,service=6496/tcp,msg="scan: nmap TCP[Reference: http://www.fortinet.com/ids/ID102367244]"
```

date=2004-07-

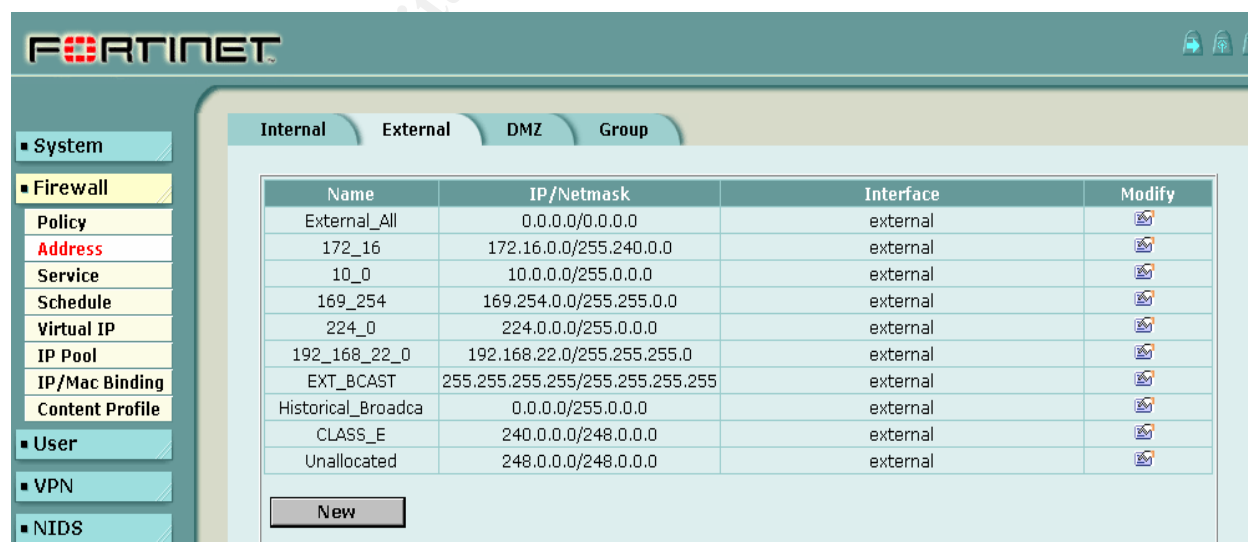
```
13,time=13:10:48,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=102367244,,src=192.168.22.210,dst=192.168.22.1,src_port=52105,dst_port=16381,status=detected,proto=6,service=16381/tcp,msg="scan: nmap TCP[Reference: http://www.fortinet.com/ids/ID102367244]"
```

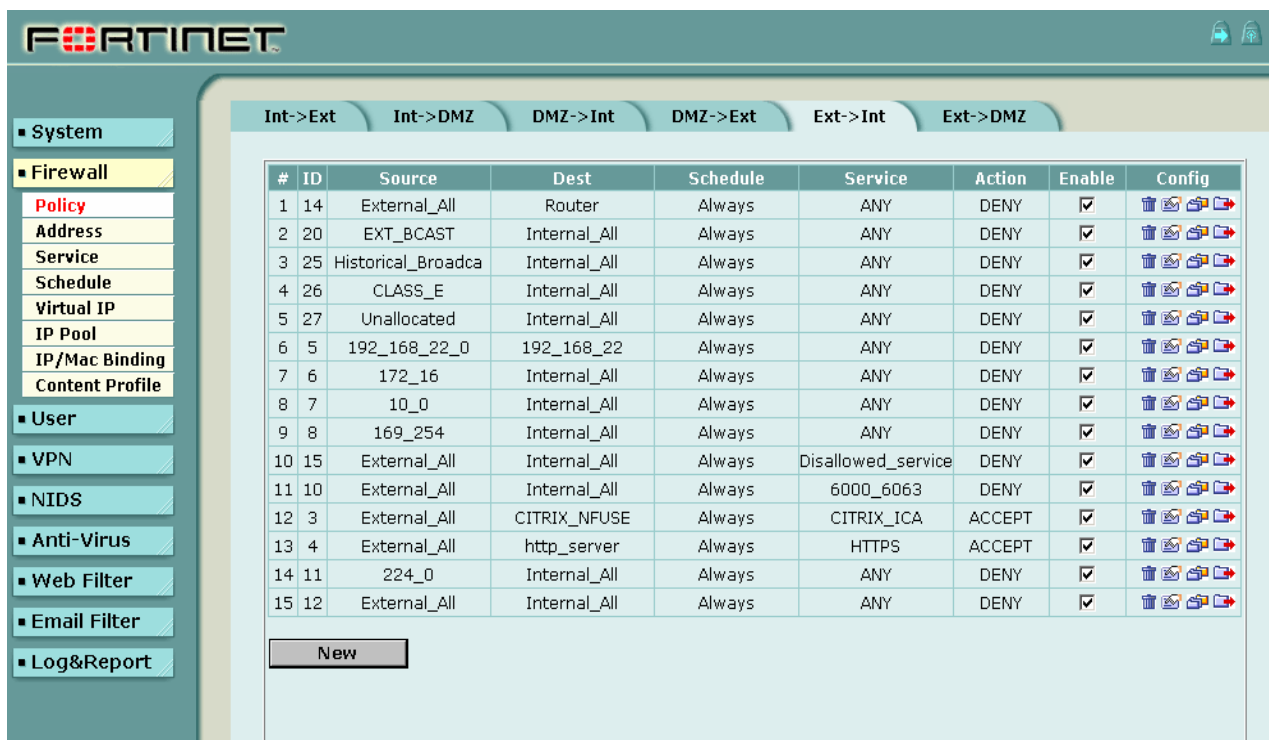
N/A	Pass	Fail	#	Check List Item	RISK			
		X	20	<i>Reject Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Log Event.</i>	M			
Risk of Non Compliance		Intruders may gather network information for Denial of Service attacks.						
Procedure		Verify that ICMP protocol 8, 11, and 3 are blocked at the external interface. Login as admin to the web interface. Select Firewall > Policy > 'EXT>INT'. Check if this specific service is included in the disallowed_services group or by itself appears in the ruleset and set to deny access.						
Verify		Check predefined Service ICMP_Any is in the disallowed services list.						
Conclusion		Not in Compliance. Either way. The predefined Service ICMP_Any is not in the disallowed services list.						
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.2.2 - Exploit Protection) SANS – GSNA Courseware Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective			Objective	X	Evidence	X	Findings	X

```
date=2004-06-02,time=14:35:23,device_id=FGT1002801021129,log_id=0400000000,type=ids,subtype=detection,pri=alert,attack_id=17956867,,src=192.168.22.11,dst=192.168.22.200,icmp_id=0x0200,icmp_type=0x08,icmp_code=0x00,status=detected,proto=1,service=icmp,msg="icmp: PING NMAP[Reference: http://www.fortinet.com/ids/ID17956867]"
```

3.3.0 Address Filtering

N/A	Pass	Fail	#	Check List Item	RISK		
	X		21	<i>Reject all Traffic from the External Networks that bear following source IP address:</i> <i>0.0.0.0/8 Historical broadcast</i> <i>10.0.0.0/8 RFC 1918 private network</i> <i>169.254.0.0/16 Link local networks</i> <i>172.16.0.0/12 RFC 1918 private network</i> <i>192.168.0.0/16 RFC 1918 private network</i> <i>224.0.0.0/4 Class D multicast</i> <i>240.0.0.0/5 Class E reserved</i> <i>248.0.0.0/5 Unallocated</i> <i>255.255.255.255/32 Broadcast</i>	H		
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.					
Procedure		Login to Firewall as admin using the web interface. Select> firewall>Policy>'EXT>INT'					
Verify		Verify that the above addresses are included in the policy and set to deny access and logging enabled.					
Conclusion		The address are included in the policy and set denied. Logging is enabled for all denied rules.					
Reference		MSDN – Chapter 15 – Securing your Network - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp SANS – GSNA Courseware. Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective		Objective	X	Evidence	X	Findings	X





N/A	Pass	Fail	#	Check List Item	RISK
	X		22	Reject all Traffic from the Internal Networks that bear a source IP address which does not belong to the internal network (outbound)	H
Risk of Non Compliance	IP Spoofing to start denial of service attempts or send malicious codes.				
Procedure	Check the firewall Int to Ext ruleset for the specific policy. From internal PC FBSD 192.168.22.210 execute command as below: a) hping -S xxx.xxx.xxx.x43 -a 192.168.0.20 -p 21 b) hping -S xxx.xxx.xxx.x43 -a 192.168.20.20 -p 21				
Verify	The addressees 192.168.22.0 /8 only should be allowed outbound access (Policyid 2) Other 192.168.XXX.XXX should be denied access (policyid 21)				
Conclusion	In compliance				
Reference	Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php				
Subjective		Objective	X	Evidence	X Findings X

date=2004-06-02,time=15:36:20,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=106657,duration=10,policyid=2,proto=6,service=80/tcp,status=accept,src=192.168.22.21,srcname=192.168.22.21,dst=xxx.xxx.xxx.x74,dstname=xxx.xxx.xxx.x74,src_int=internal,dst_int=external,sent=977,rcvd=5953,sent_pkt=8,rcvd_pkt=7,src_port=2796,dst_port=80,vpn=n/a,tran_ip=xxx.xxx.xxx.x27,tran_port=40975,

date=2004-06-02,time=14:55:07,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=103322,duration=10,policyid=2,proto=6,service=110/tcp,status=accept,src=192.168.22.220,srcname=192.168.22.220,dst=xxx.xxx.xxx.x97,dstname=xxx.xxx.xxx.x97,src_int=internal,dst_int=external,sent=595,rcvd=742,sent_pkt=10,rcvd_pkt=12,src_port=2668,dst_port=110,vpn=n/a,tran_ip=xxx.xxx.xxx.x27,tran_port=38776,

date=2004-06-02,time=15:26:00,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=105906,duration=0,policyid=21,proto=6,service=21/tcp,status=deny,src=192.168.0.20,srcname=192.168.0.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2013,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,

date=2004-06-02,time=15:26:01,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=105907,duration=0,policyid=21,proto=6,service=21/tcp,status=deny,src=192.168.0.20,srcname=192.168.0.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2014,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,

date=2004-06-02,time=15:36:07,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=106654,duration=0,policyid=21,proto=6,service=21/tcp,status=deny,src=192.168.20.20,srcname=192.168.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=1861,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,

date=2004-06-02,time=15:36:08,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=106655,duration=0,policyid=21,proto=6,service=21/tcp,status=deny,src=192.168.20.20,srcname=192.168.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=1862,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port=0

© SANS

N/A	Pass	Fail	#	Check List Item	RISK			
	X		23	Reject outbound traffic from a system using a source address that falls within the address ranges :10.0.0.0 /8 & 172.16.0.0 /16(RFC1918), 165.255.0.0 /16 (Link Local networks)	H			
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.						
Procedure		Check the Firewall INT>EXT ruleset for the specific policy. From internal PC FBSD 192.168.22.210 execute command as below: a) hping -S 10.10.20.20 -a 172.16.20.20 -p ++21 b) hping -S xxx.xxx.xxx.x43 -a 10.10.20.20 c) Hping -S xxx.xxx.xxx.x43 -a 169.254.20.20						
Verify		Verify the above addresses are denied access. Verify the logs for the record of the denied activities.						
Conclusion		In compliance						
Reference		Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php						
Subjective		Objective		X	Evidence	X	Findings	X

```
date=2004-06-02,time=14:23:23,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=100732,duration=0,policyid=17,proto=6,service=21/tcp,status=deny,src=172.16.20.20,srcname=172.16.20.20,dst=10.10.20.20,dstname=10.10.20.20,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2919,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,
```

```
date=2004-06-02,time=14:23:24,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=100734,duration=0,policyid=17,proto=6,service=22/tcp,status=deny,src=172.16.20.20,srcname=172.16.20.20,dst=10.10.20.20,dstname=10.10.20.20,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2920,dst_port=22,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,
```

```
date=2004-06-02,time=14:23:25,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=100735,duration=0,policyid=17,proto=6,service=23/tcp,status=deny,src=172.16.20.20,srcname=172.16.20.20,dst=10.10.20.20,dstname=10.10.20.20,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2921,dst_port=23,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,
```

```
date=2004-06-02,time=16:43:27,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=109641,duration=0,policyid=23,proto=6,service=0/tcp,status=deny,src=10.10.20.20,srcname=10.10.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=1754,dst_port=0,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,
```

```
date=2004-06-02,time=16:43:28,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=109642,duration=0,policyid=23,proto=6,service=0/tcp,status=deny,src=10.10.20.20,srcname=10.10.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=1755,dst_port=0,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,
```


date=2004-06-02,time=15:23:22,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=105625,duration=0,policyid=24,proto=6,service=21/tcp,status=deny,src=169.254.20.20,srcname=169.254.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2505,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port

date=2004-06-02,time=15:23:22,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=105628,duration=0,policyid=24,proto=6,service=21/tcp,status=deny,src=169.254.20.20,srcname=169.254.20.20,dst=xxx.xxx.xxx.x43,dstname=xxx.xxx.xxx.x43,src_int=internal,dst_int=external,sent=0,rcvd=0,src_port=2506,dst_port=21,vpn=n/a,tran_ip=0.0.0.0,tran_port

N/A	Pass	Fail	#	Check List Item	RISK
	X		24	Reject inbound traffic from a system using a source address that falls within the address ranges : 10.0.0.0 /8, 172.16.0.0 /16, 165.255.0.0 /16 (RFC 1918)	H
Risk of Non Compliance		IP Spoofing to start denial of service attempts or send malicious codes.			
Procedure		Check the Firewall EXT>INT ruleset for the specific policy. From external PC FSAUDIT xxx.xxx.xxx.x29 execute command as below: a) hping -S xxx.xxx.xxx.x27 -a 10.10.21.21 -p 80 b) hping -S xxx.xxx.xxx.x27 -a 172.168.20.20 -p 23			
Verify		Verify the above addresses are denied access. Verify the logs for the record of the denied activities			
Conclusion		In compliance			
Reference		Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php			
Subjective		Objective	X	Evidence	X Findings X

date=2004-06-01,time=09:46:53,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=28808,duration=40,policyid=0,proto=6,service=80/tcp,status=deny,src=172.16.20.20,srcname=172.16.20.20,dst=xxx.xxx.xxx.x27,dstname=xxx.xxx.xxx.x27,src_int=n/a,dst_int=external,sent=0,rcvd=0,src_port=62894,dst_port=80,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,

2004-06-01 09:45:21 Local7.Notice 192.168.22.1 date=2004-06-01,time=09:46:54,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=28839,duration=40,policyid=0,proto=6,service=80/tcp,status=deny,src=172.16.20.20,srcname=172.16.20.20,dst=xx.xxx.xxx.x27,dstname=xxx.xxx.xxx.x27,src_int=n/a,dst_int=external,sent=0,rcvd=0,src_port=62895,dst_port=80,vpn=n/a,tran_ip=0.0.0.0,tran_port=0,

N/A	Pass	Fail	#	Check List Item	RISK		
	X		25	Reject Outbound traffic containing broadcast addresses and Log event	H		
Risk of Non Compliance		Unwitting participant in Denial of Service Attacks.					
Procedure		Check the Firewall INT>EXT ruleset for the specific policy. From internal PC FBSD192.168.22.210 execute command as below: nmap -sS -O -P0 -e dc0 -S 255.255.255.255 192.168.22.1					
Verify		Check firewall logs to see if the broadcasts are recorded and dropped					
Conclusion		In Compliance					
Reference		Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.2.2 – Exploits Protection) Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php					
Subjective		Objective	X	Evidence	X	Findings	X

date=2004-06-03,time=14:39:06,device_id=FGT1002801021129,log_id=0401000002,type=ids,subtype=prevention,pri=alert,attack_id=109,src=255.255.255.255,dst=192.168.22.1,src_port=47765,dst_port=635,interface=internal,status=dropped,proto=6,service=635/tcp,msg="IP spoofing [Reference: http://www.fortinet.com/ids/ID109]"

date=2004-06-03,time=14:43:40,device_id=FGT1002801021129,log_id=0401000002,type=ids,subtype=prevention,pri=alert,attack_id=109,src=255.255.255.255,dst=192.168.22.1,src_port=2294,dst_port=21,interface=internal,status=dropped,proto=6,service=ftp,msg="IP spoofing [Reference: http://www.fortinet.com/ids/ID109]"

3.4.0 Intrusion Detection and prevention

N/A	Pass	Fail	#	Check List Item	RISK		
	X		26	Interfaces both internal and external must be monitored for network-based attacks	H		
Risk of Non Compliance		<ul style="list-style-type: none"> Inability to detect misconfigured firewalls. Inability to detect attacks that firewalls legitimately allow through (such as attacks against web servers). Inability to detect insider hacking. 					
Procedure		Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids detection interfaces					
Verify		Both the internal and external is set to ON. Verify the DMZ interface is set to OFF					
Conclusion		In compliance					
Reference		Fortinet – Fortigate NIDS Guide. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 5.5 CISCO IOS Intrusion Detection). Technical Incursion Countermeasures: FAQ – Network Intrusion Detection Systems http://www.ticm.com/kb/faq/idsfaq.html					
Subjective		Objective	X	Evidence	X	Findings	X

```

192.168.22.1 - PuTTY
login as: admin
admin@192.168.22.1's password:
Type ? for a list of commands.

Fortigate-100 # get nids detection interfaces
^
|
Unknown command.

Fortigate-100 # get nids detection interface
internal: On
external: On
dmz: Off

Fortigate-100 # █

```

N/A	Pass	Fail	#	Check List Item	RISK
	X		27	Checksum verification must be turned ON. This feature tests files passing through the Fortigate-100 to make sure that they have not been changed in transit.	H
Risk of Non Compliance	Inability to detect malicious changes in data during transit.				
Procedure	Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids detection checksum				
Verify	Verify the Conclusions: it must be IP: ON, TCP: ON, UDP: ON and ICMP:ON				
Conclusion	In compliance				
Reference	Fortinet – Fortigate NIDS Guide.				
Subjective		Objective	X	Evidence	X
				Findings	X

```

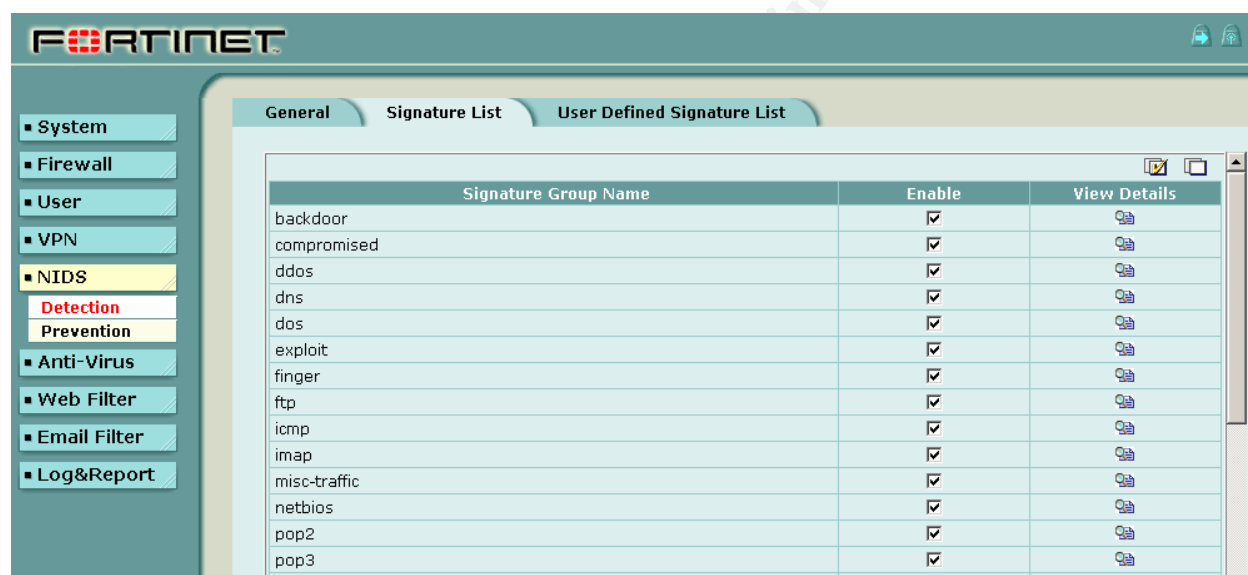
192.168.22.1 - PuTTY
login as: admin
admin@192.168.22.1's password:
Type ? for a list of commands.

Fortigate-100 # get nids detection checksum
IP: On
TCP: On
UDP: On
ICMP: On

Fortigate-100 # █

```

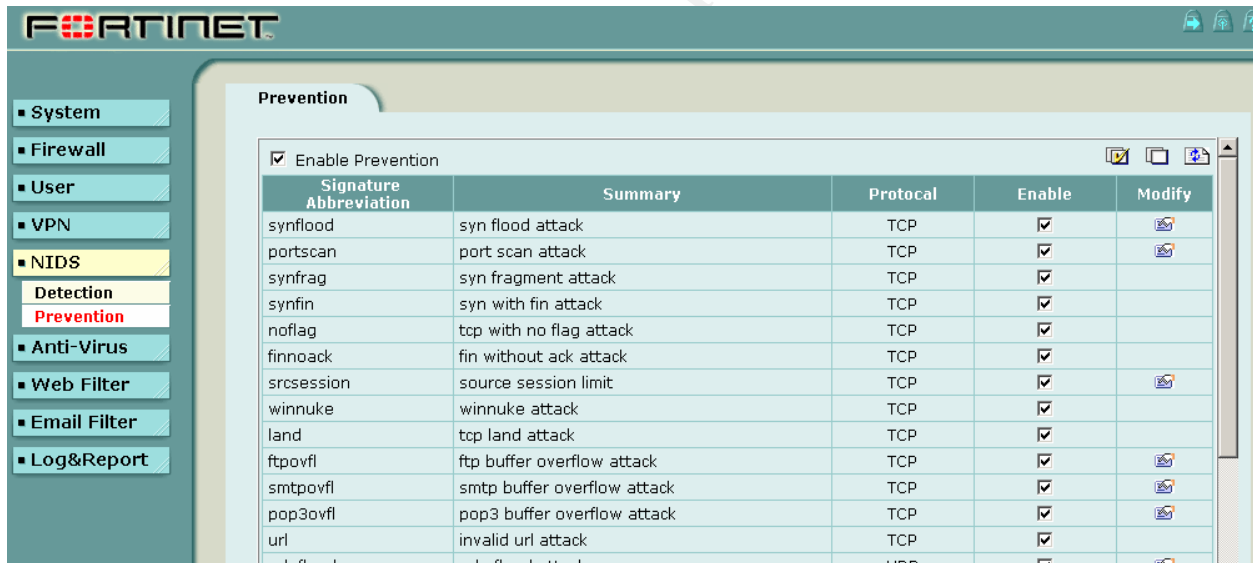
N/A	Pass	Fail	#	Check List Item	RISK
	X		28	All attack detection Signatures must be enabled. The NIDS detection module uses over 1000 signatures arranged into groups. By default all groups are enabled.	
Risk of Non Compliance		Inability to match and detect patterns of security violations of most common network attacks.			
Procedure		Open the web interface: https://192.168.22.1 . Login as admin. Go to NIDS > Detection > Signature List			
Verify		All signatures must be enabled			
Conclusion		In compliance. Only a partial list is shown below.			
Reference		Fortinet – Fortigate NIDS Guide. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 1.1 (Section 5.5 CISCO IOS Intrusion Detection).			
Subjective		Objective	X	Evidence	X
				Findings	X



N/A	Pass	Fail	#	Check List Item	RISK
	X		29	NIDS attack prevention must be enabled. This module is disabled by default!	MH
Risk of Non Compliance		Inability to prevent the damage either by dropping the packets or by blocking network access.			
Procedure		Login to the firewall internal interface 192.168.22.1 using “putty”. In the CLI dialogue execute the following commands: Fortigate-100 # get nids prevention status			
Verify		Verify IDP is enabled.			
Conclusion		In compliance.			
Reference		Fortinet – Fortigate NIDS Guide.			
Subjective		Objective	X	Evidence	X
				Findings	X

```
Fortigate-100 # get nids prevention status
IDP: enabled
Fortigate-100 #
```

N/A	Pass	Fail	#	Check List Item	RISK
	X		30	All attack prevention signatures must be enabled.	
Risk of Non Compliance		Inability to prevent the damage either by dropping the packets or by blocking network access.			
Procedure		Open the web interface: https://192.168.22.1 . Login as admin. Go to NIDS > Prevention			
Verify		'Enable prevention' is checked. Verify that all individual prevention signature groups are enabled.			
Conclusion		In Compliance. Only a partial list is shown below.			
Reference		Fortinet – Fortigate NIDS Guide.			
Subjective			Objective	X	Evidence
				X	Findings
					X



N/A	Pass	Fail	#	Check List Item	RISK			
	X		31	Test ID Prevention is functioning.	MH			
Risk of Non Compliance		Undetected internal or external attacks resulting Denial of Service and or damage to systems and data.						
Procedure		From the internal Test PC FSBD 192.168.22.210 execute the following command hping -S 192.168.22.1 -a 255.255.255.255						
Verify		Check the IDS prevention detects and prevents and logs the attack.						
Conclusion		In compliance. IP Spoofing was detected from internal network (IP 192.168.30.63/24) not belonging to the company's subnet. Requires further investigation. See Part 4: Identified Vulnerabilities.- Finding: - IP Spoofing see Part4: Identified Vulnerabilities – Summary .						
Reference		Fortinet – Fortigate NIDS Guide.						
Subjective			Objective	X	Evidence	X	Findings	X

This is Real Data

2004-06-02 08:40:34 log_id=0401000002 type=ids subtype=prevention pri=alert attack_id=109 src=192.168.30.63 dst=255.255.255.255 src_port=68 dst_port=67 interface=internal status=dropped proto=17 service=67/udp msg="IP spoofing [Reference: <http://www.fortinet.com/ids/ID109>]"

2004-06-02 08:33:02 log_id=0401000002 type=ids subtype=prevention pri=alert attack_id=109 src=192.168.30.63 dst=255.255.255.255 src_port=68 dst_port=67 interface=internal status=dropped proto=17 service=67/udp msg="IP spoofing [Reference: <http://www.fortinet.com/ids/ID109>]"

This is Test Data

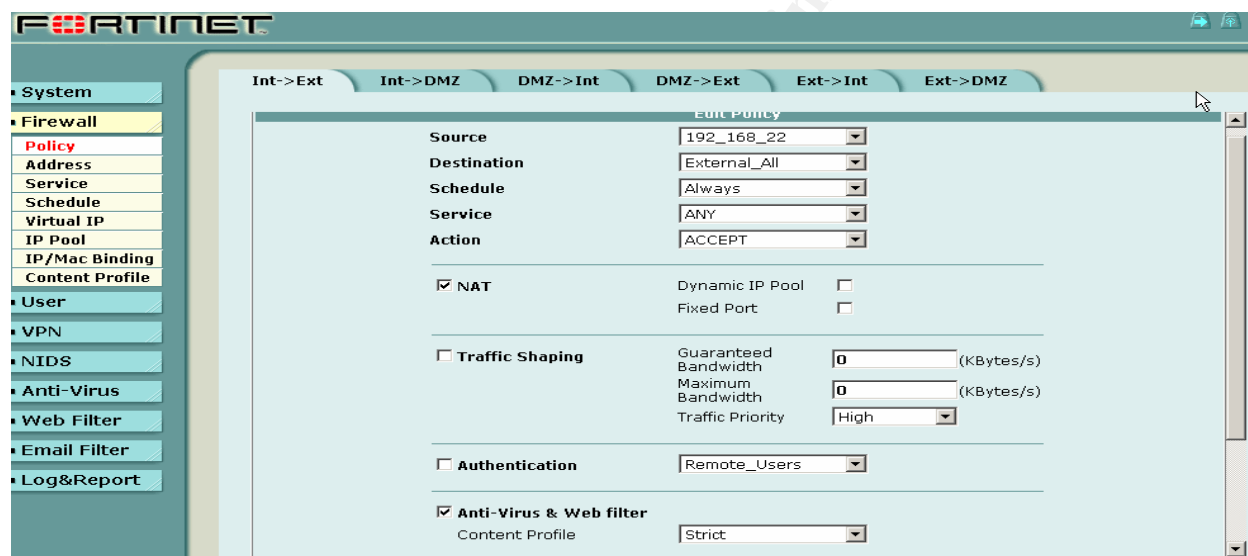
date=2004-06-03,time=14:24:16,device_id=FGT1002801021129,log_id=0401000002,type=ids,subtype=prevention,pri=alert,attack_id=109,,src=255.255.255.255,dst=192.168.22.1,src_port=61932,dst_port=27004,interface=internal,status=dropped,proto=6,service=27004/tcp,msg="IP spoofing [Reference: <http://www.fortinet.com/ids/ID109>]"

date=2004-06-03,time=14:25:16,device_id=FGT1002801021129,log_id=0401000002,type=ids,subtype=prevention,pri=alert,attack_id=109,,src=255.255.255.255,dst=192.168.22.1,src_port=61932,dst_port=647,interface=internal,status=dropped,proto=6,service=647/tcp,msg="IP spoofing [Reference: <http://www.fortinet.com/ids/ID109>]"

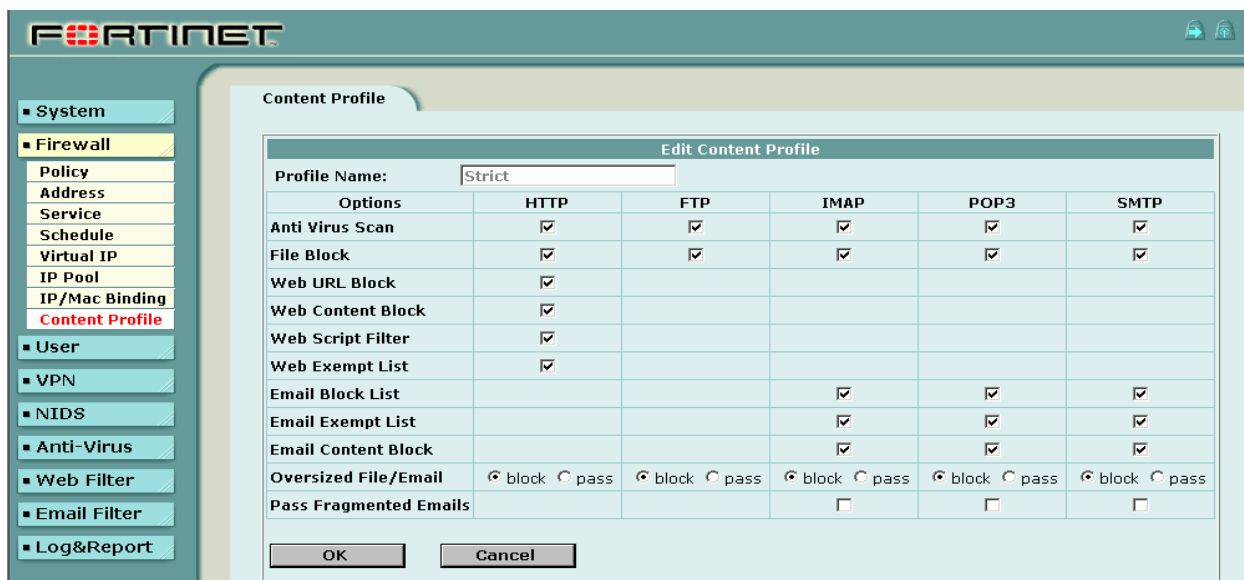
© SANS

3.5.0 AV / File Blocking Protection

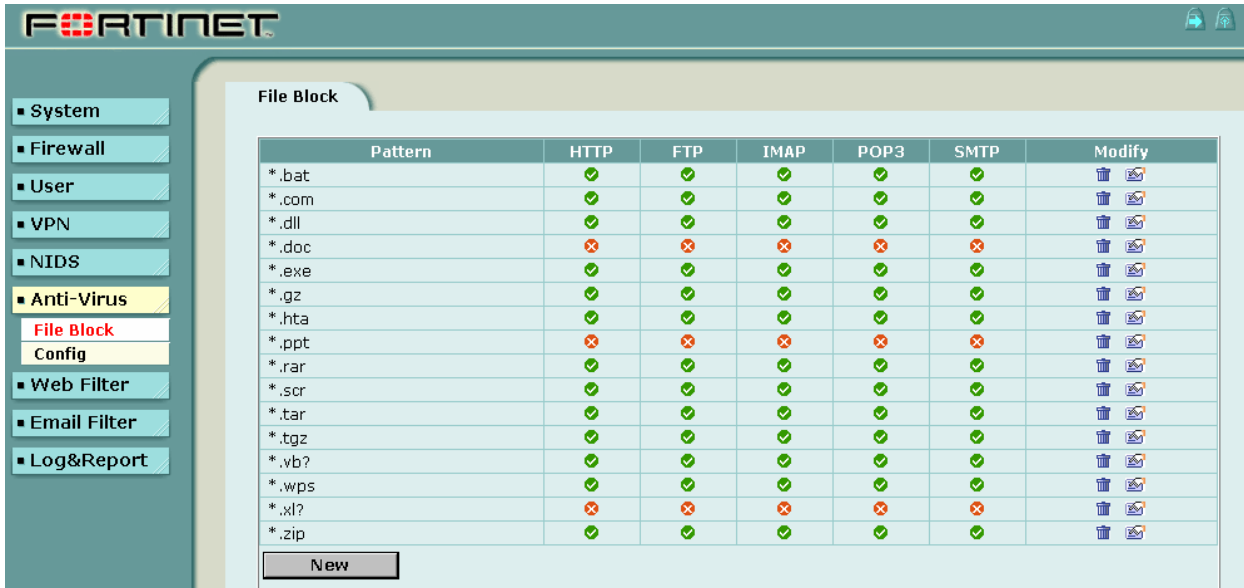
N/A	Pass	Fail	#	Check List Item	RISK
	X		32	Content filtering must be enabled in the firewall policy.	H
Risk of Non Compliance	Malicious codes and viruses infecting internal network. Some may create backdoor connections for intruders.				
Procedure	Login to the web interface. Select Firewall>Policy>'INT.EXT'> Open (Edit) Policyid 2.				
Verify	Antivirus and Web filter must be enabled and the 'Strict' content profile must be in use.				
Conclusion	In compliance				
Reference	Fortinet – Content Protection Guide				
Subjective		Objective	X	Evidence	X
				Findings	X



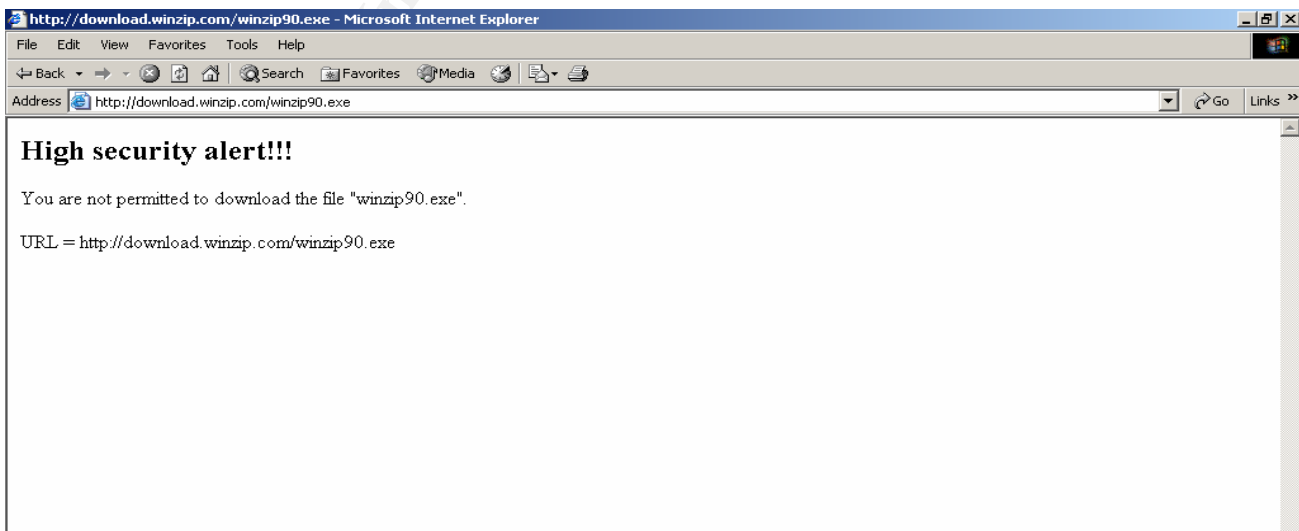
N/A	Pass	Fail	#	Check List Item	RISK
	X		33	Verify contents of 'Strict Content profile'. This controls how the antivirus protection behaves.	H
Risk of Non Compliance	Downloading of infected files or programs containing malicious codes or viruses.				
Procedure	Login as admin at the web Interface. Select firewall> Content Profile>Strict.				
Verify	All options must be selected for protection, except 'pass fragmented e-mails'.				
Conclusion	In Compliance				
Reference	Fortinet – Content Protection Guide				
Subjective		Objective	X	Evidence	X
				Findings	X



N/A	Pass	Fail	#	Check List Item	RISK
	X		34	File blocking must be enabled to remove all files that pose a potential threat and to provide the best protection from active computer virus attacks.	H
Risk of Non Compliance		Downloading of infected files or programs containing malicious codes or viruses.			
Procedure		Login to the web interface as admin. Select: Antivirus>File Block.			
Verify		Only files with .doc, .ppt, .xl extensions must be unblocked for HTTP, FTP, IMAP, POP3, SMTP protocols. All other file extensions must be blocked for all protocols.			
Conclusion		In compliance.			
Reference		Fortinet – Content Protection Guide			
Subjective			Objective	X	Evidence
				X	Findings
					X



N/A	Pass	Fail	#	Check List Item	RISK
	X		35	Test File blocking functionality.	H
Risk of Non Compliance	Downloading of files or programs containing malicious codes or viruses.				
Procedure	From any internal PC browse to http://www.winzip.com and attempt to download a trail version of winzip.exe				
Verify	The down load must be blocked with a security alert message.				
Conclusion	In compliance. The log has also recorded zip files that were blocked with the destination information.				
Reference	Fortinet – Content Protection Guide				
Subjective		Objective	X	Evidence	X
				Findings	X



Part 4: Audit Report and Risk Assessment

Executive Report

This is the audit report on Rama Inc.'s Firewall security. The company's computer networks are used to transmit critical administrative and financial data such as payroll, purchase orders and invoices, payments, e-mail and other information exchange over the internet. As the company plans to extend its Internet use to more critical applications, there are more opportunities for cyber intrusions, viruses and frequent denial of service attempts to the company's information system. This has created greater awareness for more enhanced Internet Security at Rama Inc.

Objectives

The objectives of the audit were to determine whether: (1) adequate controls are established to prevent, detect, and respond to unwanted Internet access to the company networks against denial of services and any unauthorized access to the internal resources. (2) Ensure working controls exist to protect information systems and technology from computer viruses. Controls should incorporate virus protection, detection, occurrence response and reporting.

Scope and methodology

We used COBIT as a reference tool to define the control objectives and Facilitated Risk Analysis Process to assess the risks and vulnerabilities to the company's networks through the firewall. We interviewed key officials and used non commercial software scanning tools to assess vulnerabilities and test firewall rules. We scanned the Firewall to identify installed network services. This audit was limited to the company's firewall model Fortigate -100, its configuration and its performance as a firewall, intrusion detection and Antivirus content protection control. This audit did not include security assessment of the company's internal network. The audit was conducted in accordance with best practices prescribed by SANS Institute and National Institute for Standards and Technologies, and other standards and guidelines as referenced through out this report.

Discussion of Audit results

The audit results confirm that the Fortigate-100 Firewall is performing its function as a technical control and meet the company's objectives. The controls are in place and are working as a defensive mechanism to thwart denial of service attacks, unauthorized access and protect the company's contents against antivirus and other intrusions. The details of the evidence and findings are listed in the previous section; Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings

There are a few vulnerabilities, anomalies and observations that require attention and are listed under Current Findings and Recommendations. Additional list of list of recommendations can be found at the end of this section.

Current Status:

The initial risks that were identified (Ref: Table 5) as at level HIGH, are mitigated to a level LOW. This is because of the intended controls (Ref: Table 6) are in place and are effective. The resultant risks are exemplified in Table 7 below:

Table 7: Current status - Risks

#	Vulnerability / Exposure	Risk	Risk Factor
1	Default Firewall Settings Misconfigured Firewalls Unauthorized Router Access	<ul style="list-style-type: none"> • Unknown and dangerous services pass through freely. • May be serving as unwitting participants in Denial of Service • Login by hostile agents or unauthorized users, inability to attribute accountability • Exposure of sensitive information to unauthorized listeners, session hijacking. • Address-spoofed DDoS traffic exiting your network, forwarding bad traffic to peers • Flooding attacks or DDoS attacks using ICMP. • Malicious third parties may gain access to critical applications or sensitive data • Denial of service where remote users may not be able to gain access to data • Misconfigured router, which may result in unauthorized access or modification of organization's information resources 	LOW
2	Malware, Spyware, Viruses and Trojans	<ul style="list-style-type: none"> • Increased cost of recovery (correcting information and reestablishing services) • Loss of information (critical data, proprietary information, contracts) • Loss of trade secrets • Increased cost of retrospectively securing the system 	LOW

Current Findings and Recommendation

Identified Vulnerabilities - Summary

- a) Lack of Policies.
- b) Firewall administration is not restricted to a specific trusted pc.
- c) Unused Firewall interface DMZ is not disabled.
- d) Firewall is missing the latest patches and updates.
- e) Risky services and protocols are not restricted in the outbound policy.
- f) ICMP Protocol is not set for rejection in the inbound policy

Finding: IP Spoofing:

During test of Checklist item 31 IP Spoofing attempts were detected by the Fortigate-100 IDS /prevention module. The spoofed address 192.168.30.63 does not belong to the company's internal network.

Root Cause: On investigations it was detected that an Internal PC in the accounting department had a pc with 2 two Network Interface Cards, one of which was connected to a network

192.168.30.0/24 belonging to adjacent neighboring firm XUZ Inc.! Further investigations revealed that it was a forgotten connection once used for sharing some resources! This backdoor connection is potentially dangerous and by passes the firewall! The administrator was instructed to remove the second network interface and remove the network connection on the wall.

A company security policy / Change Control and regular review of the log would have revealed this much earlier.

Identified Vulnerabilities - Details

Vulnerability	1	Checklist Item #	-	Risk (Not Implementing)	Low – Medium
Lack of Policies: Security Policy, Acceptable Use Policy.					
Description	Security policies define the procedures, guidelines and practices for configuring and managing security in an organization. Through committed enforcement of these policies, organizations can demonstrate due diligence to their stake holders and customers and reduce the risks to the organization's information assets.				
Threat	Lack of base line and no accountability.				
Audit Finding	-				
Recommendation	Security policies, standards and procedures provide information security a structure. Vulnerability assessments and risk analysis prepare the grounds for the choice of policies needed by the organization. Simple policies that meet the needs of the organization can be created. Guidance is available on the internet, SANS and other security resources				
Cost	NIL				
References	Importance of Corporate Policy: http://securityresponse.symantec.com/avcenter/security/Content/security_articles/corp.security.policy.html				
Compensating Controls	-				

Vulnerability	2	Checklist Item #	1.a	Risk (Not Implementing)	High
<p>Only FW administrator and other authorized personnel will be granted access to the FW for administration.</p> <p>Note: Although the results are for test 1.a is in compliance, it is recommended that an additional, separate, user with read write permissions is created for administering the Firewall.</p>					
Description	*In addition to how administrators access the router, there may be a need to have more than one level of administrator, or more than one administrative role.				
Threat	Dependence on only one administrator affects Real-time Recovery objectives.				
Audit Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist item 1				
Recommendation	*Define clearly the capabilities of each level or role in the router security policy. For example, one role might be 'network manager', and the administrators authorized to assume that role may be able to view and modify the configuration settings and interface parameters. Another role might be 'operators', administrators authorized to assume that role might be authorized only to clear connections and counters. In general, it is best to keep the number of fully privileged administrators to a minimum.				
*References	Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1 (Section 4.1.5. – Logins, Privileges, Passwords and Accounts)				
Cost	NIL				
Compensating Controls	Separation of duties.				

Vulnerability	3	Checklist Item #	1.b	Risk (Not Implementing)	High
FW Administration allowed only from specific trusted host.					
Description	Ensure that the computer allows administration from only an authenticated host.				
Threat	Unauthorized users may compromise the firewall through unsecured computers, using the idle or unused portion or id portion of the admin time out period (when left unguarded). Attempts to compromise include password cracking tools.				
Audit Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist item 1				
Recommendation	Allowing administration of the firewall from any connected computer is a security risk. The knowledge of the username and Password to connect to the computer from any internal PC can be obtained either through social engineering or using password cracking tools. Restricting the FW administration from a restricted PC adds additional layer to the defense-in-depth.				
Cost	NIL				
Compensating Controls	STRONG, Complex Passwords				

Vulnerability	4	Checklist Item #	5	Risk (Not Implementing)	Low- Medium
<i>The FW administrator will disable FW interfaces that are not in use.</i>					
Description	The DMZ Interface is unused and should be disabled.				
Threat	Hacking attempts, Firewall configuration changes				
Audit Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist Item 5				
Recommendation	An unused interface is not monitored or controlled, and it is probably not updated. This might expose your system to unknown attacks on those interfaces.				
Cost	- NIL-				
Compensating Controls	Regular systematic reviewing of log data.				

Vulnerability	5	Checklist Item #	10	Risk (Not Implementing)	Medium
<i>Ensure that the latest patches and updates are applied to the firewall components. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.</i>					
Description	Exploiting known software vulnerabilities is a primary means of gaining privileged access to a system or implementing a denial of service attack.				
Threat	Unauthorized Firewall configurations changes, new virus and worm attacks and exploitation of the known vulnerability				
Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist item 10				
Recommendation	Patch management is an important part of good security management practice. Company's should establish change control and patch management and monitor versions changes and hotfixes to the firewall and other operating systems. Subscription to manufacturer's notification services on this issue will be of great assistance.				
*References	Patches and Updates: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp				
Cost	NIL				
Compensating Controls	LOGS. Frequent review of logs				

Vulnerability	6	Checklist Item #	13	Risk (Not Implementing)	Medium
<i>Reject the following non-required, risky protocols and services in either direction.</i>					
Description	Checklist item 13 includes a list of known risky protocols and services that should be rejected either way. The firewall is configured to reject the listed services only inbound. The firewall is stateful inspection type and rejects the risky protocols when connections were attempted to these ports. However malicious programs, on compromised computers of the internal network may allow dangerous connections.				
Threat	Internal rogue applications connecting to these external ports creating backdoor.				
Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist 13				
Recommendation	Define a policy on required external services for internal users. Explicitly deny connection to un necessary external services including outbound proxy service connections and log events.				
Cost	- NIL-				
Compensating Controls	Logs. Frequent review of Logs for intrusions and Statetables. Regular auditing and scanning of internal network for unnecessary protocols and services. Security policies.				

Vulnerability	7	Checklist Item #	20	Risk (Not Implementing)	Low
<i>Reject Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Log Event.</i>					
Description	*ICMP is a stateless protocol that sits on top of IP and allows host availability information to be verified from one host to another.				
Threat	Network enumeration. <i>ICMP can be used to map the networks behind certain types of firewalls.</i> Intruders may gather network information for Denial of Service Attacks				
Finding	Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist item 22				
Recommendation	*Blocking ICMP traffic at the outer perimeter router protects you from attacks such as cascading ping floods. Other ICMP vulnerabilities exist that justify blocking this protocol. While ICMP can be used for troubleshooting, it can also be used for network discovery and mapping. Therefore, control the use of ICMP. If you must enable it, use it in echo-reply mode only.				
*Reference	Screen ICMP Traffic from the internal Network: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp				
Cost	-NIL-				
Compensating Controls	LOGS. Frequent review of intrusions, notices.				

Additional Recommendations

In this digital world of information exchange, a company's vital information can be stolen without being lost! Establishing an information security framework will minimize such risks and provide additional confidence in the company's information to the staff, clients, vendors and shareholders. This audit is just the beginning towards fulfillment of a secure information infrastructure. The company can further consolidate their Information Systems Security through an audit of their internal network for vulnerabilities and establishing key performance indicators by recording and measuring the increased /decreased incidents.

A good source to start with is the 'Security Self-Assessment Guide' a NIST special Publication 800-26. The document guides through five levels of effectiveness with checklists for each area of: Management Control, Operational Control and Technical Control. Additional recommendation includes:

- Frequent review of firewall policies and ports for unused rules.
- Conduct regular audits and Review Logs regularly
- Check periodically for information at the vendor site for helpful information on new virus attacks and the ID defenses (ports to be blocked etc).
- User awareness training will help reduce security related incidents.
- Risk analysis revealed the importance of the availability of the Fortigate-100. It is recommended that the company should make a backup system available for emergencies, to minimize downtime.

References

- SANS – GSNA Courseware.
- SANS Institute – Webcast – Auditing a Network Perimeter by Chris Brenton -Tuesday, March 16, 2004, 1:00pm EST (1800 UTC)
<http://www.sans.org/webcasts/show.php?webcastid=90504>
- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing – RFC 2267
- Requirements for IP Version 4 Routers – RFC 1812
- Consensus Roadmap for Defeating Distributed Denial of Service Attacks - SANS
- Router security – Approaches you can take today by Neal Ziring, NSA
- Guidelines on Firewalls and Firewall Policy-NIST Publication 800-41
- Network Infrastructure Security Checklist – Version 4, Release 2.2 – DISA Field Security Operations.
- Firewall Checklist by Naidu, K.
<http://www.sans.org/score/firewallchecklist.php>
- Building Your Firewall Rulebase by Lance Spitzner
<http://www.spitzner.net/rules.html>
- Improving Security on CISCO Routers – CISCO Document ID 13608.
- Integrated Security: Defending against Evolving Threats with Self-Defending Networks – CISCO White Paper.
- Help Defeat Denial of Service Attacks: Step-by-Step - SANS
Revision: 1.4 - Date: 2000/03/23 16:05:35 GMT
- CERT[®] Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
- CERT[®] Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks
- CERT[®] Coordination Center-Denial of Service Attacks
- Information Security Risk Analysis by Thomas R. Peltier.
ISBN:0849308801 Auerbach Publications
- Router Security Configuration Guide (SNAC) – NSA Revision 27, 2002, Version 1.1
- Microsoft Solutions Guide for Windows 200 Server
(<http://support.microsoft.com/default.aspx?scid=kb;en-us;829031>)
- Microsoft Security Guidance Kit
- Microsoft Patterns and Practices: Improving Web Application Security: Threats and Countermeasures -
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp>
- Services that router should block. http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html
- Technical Incursion Countermeasures: FAQ – Network Intrusion Detection Systems (<http://www.ticm.com/kb/faq/idsfaq.html>)
- CISA Review Manual 2003.

- COBIT QuickStart, COBIT – <http://www.isaca.org/cobit>
- OCTAVE[®]-S – Operationally Critical Threat, Asset, and Vulnerability Evaluation, Version 0.9: <http://www.cert.org/octave>
- Security Self-Assessment Guide - NIST special Publication 800-26.
- NIST Computer Security Resource Center web site at the URL: <http://csrc.nist.gov>
- Fortinet / Fortgate - Command Line Interface Reference Guide
- Fortinet / Fortigate – 100 NIDS Guide
- Fortinet / Fortigate – 100 Content Protection Guide
- Computerworld
(<http://www.computerworld.com/networkingtopics/networking/story/0,10801,65366,00.html>)
- Search Engines <http://www.google.com>

© SANS Institute 2004, Author retains full rights.