

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

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

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

Table of Contents

| Auditing the Fortigate-100 Firewall Appliance | |
|---|-----|
| Abstract | |
| Part 1: Research in Audit, Measurement practice, and control systems | . 4 |
| Business Control Objectives | |
| Detailed control objectives | . 5 |
| Audit Scope | |
| Purpose: | . 6 |
| Role of Fortigate-100 | . 6 |
| Controls provided by Fortigate-100 | . 6 |
| Administering the Fortigate-100 | . 7 |
| Risks Analysis | |
| 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 | |
| Table 3: Loss Impact Valuation Table | 10 |
| Table 4: The Integrity, Confidentiality and Availability requirements | 11 |
| Identified Risks to the Systems and Business Processes | |
| Table 5: Identified Risks | |
| Table 6: List of Controls | 17 |
| The Current State of Practice | 18 |
| Test Plan: | |
| Part 2: Audit Checklist | 20 |
| Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings | 40 |
| 3.1.0 Access and Configuration /Change Management | |
| 3.2.0 Port Filtering | |
| 3.3.0 Address Filtering | 68 |
| 3.5.0 AV / File Blocking Protection | |
| Part 4: Audit Report and Risk Assessment | |
| Executive Report. | |
| Objectives | 81 |
| Scope and methodology | 81 |
| Discussion of Audit results | 81 |
| Current Status: | 81 |
| Table 7: Current status - Risks | 82 |
| Current Findings and Recommendation | |
| Identified Vulnerabilities - Summary | |
| Identified Vulnerabilities - Details. | |
| Additional Recommendations | |
| 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. Theses 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: <u>http://www.fortinet.com</u>)

- 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.
- 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: Fortgate-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 Fortogate-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.

| 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 |

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

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 |

Risk Exposure = Impact x Probability

| 0470 | Ingn | 0 | | | | | |
|---|---|---|--|--|--|--|--|
| | | | | | | | |
| Impact Factor: High = 3, Medium = 2, Low = 1 | | | | | | | |
| | | | | | | | |
| Risk Exposure = Impact x Probability | | | | | | | |
| Low = 1 | Medium = 2 | High = 3 | | | | | |
| 3 | 6 | 9 | | | | | |
| 2 | 4 | 6 | | | | | |
| 1 | 2 | 3 | | | | | |
| Low exposure = 1 or 2 Medium exposure = 3 or 4 High exposure = 6 or 9 | | | | | | | |
| | = 3, Medium = 2, Low pact x Probability Low = 1 3 2 1 | = 3, Medium = 2, Low = 1 pact x Probability Low = 1 Medium = 2 3 6 2 4 1 2 | | | | | |

Table 3: Loss Impact Valuation Table

| | Time Sensitivity | Intangible Loss (De | Tangible Loss | |
|-----------------|---|---|--|-----------------|
| Impact Value | Longest Tolerable Outage Period During Peak | Customer Satisfaction (Dissatisfied Customers) | Embarrassment (Comes to Attention of) | Financial |
| L | 24 hours or less | 0 – 10K | Few if anyone | Less than \$50K |
| М | 25–72 hours | 10,001– 15K | Company organization | \$50,001-\$300K |
| Н | 73 hours–5 days | 15,001 and higher | | \$300,001and |
| | | Č V | Vendors | 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) | М | М | М |
| 2 | ERP System | Н | Н | Н |
| 2 | Payroll | Н | H | М |
| 3 | Human Resources | Н | Н | М |
| 4 | Electronic Banking | Н | К | Н |
| 5 | Electronic Data Interchange | Н | Н | Н |
| 6 | E-mail, Documents | Н | Н | М |

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.

| Risk Severity | High | Probability | H | Impact H | Risk Item 1 | | | | | | | | |
|----------------|---|--|-------------------|-------------------------|-------------------------------|--|--|--|--|--|--|--|--|
| Risk Condition | Unknown and dar | known and dangerous services pass through the firewall freely. Important for Border Routers | | | | | | | | | | | |
| | and as a Result | | | | | | | | | | | | |
| Risk | Risk An intruder may set up a backdoor and by pass the Firewall Security. A hacker can traverse the entire | | | | | | | | | | | | |
| Consequence | company network | pany network and can damage one or several computers and data they contain. They can also | | | | | | | | | | | |
| | leave programs the | ve programs that will help them connect remotely and record user accounts, password etc, which can | | | | | | | | | | | |
| | exploited. Employ | ee's private and comp | pany's data are a | at high risk. | | | | | | | | | |
| Countermeasure | Firewall Policy, P | ort Filtering. Enable In | trusion Detection | n and Prevention. | | | | | | | | | |
| References | | seware – Auditing the pe | | | | | | | | | | | |
| | | vices that router should | | ja.net/CERT/JANET- | | | | | | | | | |
| | | <u>isco/local_services.html</u> | | | | | | | | | | | |
| | Router Security Co | nfiguration Guide (SNA | C) – NSA Revisio | n Sep, 27, 2002, Versio | n 1.1 (Section 3.2 Protecting | | | | | | | | |
| | the network with th | e Router). | 2 | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

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

| Risk Severity | High |] [| Probability | Н | | Impact | Н | | Risk Item | 3 |
|--|--|--|-------------|---|---|--------|---|--|------------------|---|
| Risk Condition | Session | hijacking | | | | , c | | | | |
| and as a Result | | | | | | | | | | |
| Risk Exposure of sensitive information to unauthorized listeners. Session hijacking can be used to obtain | | | | | | | | | | |
| Consequence | logon inf | logon information that can be used to gain access to a system or confidential information. | | | | | | | | |
| Countermeasure | | | | | | | | | | |
| References | Microsoft security guidance kit – Threats and countermeasures. | | | | | | | | | |
| | | | | | S | | | | | |

| Risk Severity | High | Probability | Н | Impact H | Risk Item 4 | | | | | |
|-----------------------|----------------|--|------------------|----------|-------------|--|--|--|--|--|
| Risk Condition | IP Spoofing | | | | | | | | | |
| and as a Result | | | | | | | | | | |
| | malicious code | 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 Acc | Implement Access Control, RFC 2827 Filtering. Enable Intrusion Detection and Prevention. | | | | | | | | |
| References | Microsoft Secu | urity Guidance Kit : Peri | meter Firewall D | esign | | | | | | |

| | | | | no no | | | | | | | |
|---------------------|-----------------|---|-----------|-----------|--------|----------------------------------|------------|----------|----------------------------|---------------|-----|
| Risk Severity | | | | obability | | | Impact | : H | | Risk Item | 5 |
| Risk Condition | Flooding | g attacks | or DDOS | S attacks | using | ICMP | | | | | |
| | and as a Result | | | | | | | | | | |
| Risk Consequence | attacks. | 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 | v tracerou | te, ping, | or any ot | her IC | MP messag | es. Enable | e Intrus | sion Detection | and Preventio | on. |
| References | | | | | | vention/cisco, tp://techreput | | | <u>l;</u> 6264-5087087. | <u>html</u> | |

| Risk Severity | High | | Probabi | l ity H | 7 | Impact | Н | | Risk Item | 6 | |
|--|-----------|--|---------|----------------|-----------|--------|---|--|-----------|---|--|
| Risk Condition | Denial of | of service | attacks | | | | | | | | |
| | | | ä | and as a | a Result… | | | | | | |
| Risk The network resources are consumed disrupting and denying services to the legitimate users. This | | | | | | | | | | | |
| Consequence | may res | ay 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 | ſ | Probability | H | | Impact H |] | Risk Item | 7 | | |
|-----------------------|------------|---|---------------------|-----------|--------------------|-----------------------|-----------------|--------------------|---|--|--|
| Risk Condition | Misconfig | jured rout | er | | | | | | | | |
| | | | and | as a Res | sult | | | | | | |
| Risk | May resu | lt in unau | thorized access or | modifica | ation of org | anization's inf | ormation resou | rces. Denial-of- | | | |
| Consequence | | rvice attacks that target and use misconfigured network routing equipment pose an "imminent and | | | | | | | | | |
| | real threa | it" to Inter | net security, accor | ding to a | i recent rep | ort by Carneg | jie Mellon Univ | ersity's federally | | | |
| | funded C | ERT Coo | rdination Center. | | | | | | | | |
| Countermeasure | Regular F | Firewall A | udit, Change Conti | rol | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| References | http://ww | w.compu | terworld.com/netwo | orkingtor | <u>pics/networ</u> | <u>king/story/0,1</u> | 0801,65366,00 | <u>).html</u> | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

| Risk Severity | High | | Prol | bability | Н |] | Impact | Н | | Risk Item | 8 | |
|------------------|-------------------------------------|---|--|--|--------------------------------|--|--|-----------------------------------|--|--|---|--|
| Risk Condition | Expos | ure to Vir | uses, Troja | ans etc. | | | | | | | | |
| | | | | and | as a | Result | | | | | | |
| Risk Consequence | Securi compu and re data a | ity. A hack uters and e cord user t high risk | er can trav data they c accounts, . Increased | verse the contain. passwo d cost of | e ent They rd et recc | ire company ne can also leave c, which can e | etwork and program xploited. E osion in v | d car s tha Emplo irus a | n damage one it will help then byee's private attacks affecte | pass the Firewa or several n connect remot and company's d two-thirds of | | |
| Countermeasure | AV Pr | Program, Acceptable use policy (Security Policies). | | | | | | | | | | |
| References | | Pricewaterhousecoopers (PwC) puts cost of virus attacks at \$1tr tp://software.silicon.com/security/0,39024655,11027559,00.htm | | | | | | | | | | |

JICY (Sec .C) puts cost of virus at ry/0.39024655,11027559,00.ht.

Table 5: Identified Risks

| # | Vulnerability / Exposure | Risk | Assets Impacted | Туре | Risk Exposure | Controls |
|---|--|--|---|-------------------|------------------|----------|
| 1 | Default Firewall settings. Misconfigured Firewalls Unauthorized Router Access. | 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. | 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. | 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 |
|---|--|--|---|
| | 1. Access and Configuration / change Management | | |
| | Security Policies FW Access Control FW Configuration FW RULEBASE Order | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 | Preventive |
| | 2. Port Filtering | | |
| If connection to the internet or other public networks exists, adequate firewalls should be operative to protect | Permit only Required Protocols and Services Reject Risky Protocols and services | 13, 14, 15,16,17, 18, 19,20 | Preventive |
| against denial of services and any | 3. Address Filtering | | |
| 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. | 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. | 21, 22, 23, 24, 25 | Preventive: Defeating Denial of Service Attacks. IP Source Address Spoofing. SYN Flooding and IP Spoofing Attacks, Smurf IP Denial-of- Service Attacks. |
| | 4. Intrusion Detection and prevention | | Detective and Corrective |
| | Intrusion Detection Intrusion Prevention Audit and Logging | 26, 27, 28, 29, 30, 31 | |
| Regarding malicious software, such | 5. Anti Virus Protection | | Preventive and corrective |
| 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 | Acceptable use policy File Blocking | 32, 33, 34, 35, | |
| incorporate virus protection, detection, occurrence response and reporting. | A Review Menuel 2002, Review Security Configuration Cuide (| | on 27, 2002, Vorsion 1,1 |

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)
- 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 | | | trator and other aut | | | |
| | | | 1 | Ū. | | ess to the FW for ad administered from a | | Н | |
| Risk of Compl | | | to m | user access and un odify the firewall r | secur | ed hosts leave the fin corrupt its integrity | rewall susceptible for | | |
| Proced | lure | 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 | | | | | | name and the specif I their read/write per | • | from | |
| Conclu | usion | | | Sec. 1 | | | | | |
| ReferenceNetwork 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 | | | | | | | ion 1.1 s and | | |
| | Subjective Objective X Evidence Findings | | | | | | | | |

| N/A | Pass | Fail | # | Check List Item | RISK | | | | | |
|-------|---|---|--|---|------|--|--|--|--|--|
| | | | 2 | The administrator and other authorized users account password will be encrypted and should be at least 6 characters long. | Н | | | | | |
| | of Non pliance | | | passwords give easy access (password cracking) for intruders to re the firewall | | | | | | |
| Proc | 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. | | | | | | | | | |
| Verif | fy | The pa | The password is encrypted. For Passwords less than 6 characters a warning appears. | | | | | | | |
| Cone | clusion | | | 20 | | | | | | |
| Refe | rence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | | |
| | SubjectiveObjectiveXEvidenc eFindings | | | | | | | | | |
| | | | | | | | | | | |

| N/A | Pass | Fail | # | Chec | k List Item | | RISK |
|---|---|------|-------|--|-------------|-----|------|
| | | | 3 | The time out period for unatt than 15 minutes. Activating th additional security | | 0 0 | Н |
| Risk of Compl | | | | casual or malicious use throu unauthorized users, if they ge | • | | out |
| Proced | 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 | 7 | The | value | s for 'Admin timeout' is 1 | 15 minutes. | | |
| Concl | usion | | | | | | |
| 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 | The FW administra remote administrat | | vill ensure modems will | l not be used for | Н | | |
| Risk o Comp | | War-di | 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. | | | | | | | | check if | | |
| Verify | 7 | Physic | Physically. | | | | | | | |
| Concl | lusion | | | | | | N. | | | |
| Refere | ence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | | |
| | Subjective Objective X Evidence Finding | | | | | | ings | | | |
| | A CONTRACT OF A | | | | | | | | | |

| N/A | Pass | Fail | # | | Check | List Item | | RISK | |
|-------------------|---|--|---|--|--------------|------------------|-------------------|------------|--|
| | | | 5 | The FW administra in use | ator will di | sable FW interfo | aces that are not | Н | |
| Risk of Compli | | un-tru | sted r | nd spoofing attacks, network. If successf nternal network. | | | 1 | 0 | |
| Procedu | ure | 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. | | | | | | |
| Conclu | ision | | | | | | | | |
| Referer | ReferenceNetwork 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. Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php | | | | | | | ersion1.1. | |
| | Subjec | tive | | Objective X Evidence Findings | | | | | |
| | | | | | | | | | |

| N/A | Pass | Fail | # | | (| Check List Item | | | RISK |
|--|--|--|--|--|-------|---|-----|----------------|-----------|
| | | | 6 | 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. | | | | | |
| Risk o Comp | | Man-i | n-the- | middle attack, Sess | ion h | ijacking. | | | |
| | | At the | At the CLI Execute the following command: | | | | | | |
| Proce | dure | a) | a) Fortigate-100 # get system interface. Note the results. | | | | | | |
| b) Try login to the external interface through web interface or using putty. | | | | | | | ty. | | |
| Verify | 7 | | | | | n, https' only for the terface of the firewa | | l interface. Y | ou should |
| Concl | usion | | | | | | | | |
| Refere | ence | 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 | | | | | | | rsion 1.1 |
| | Subjective Objective X Evidence Findings | | | | | | | | |

| N/A | Pass | Fail | # | | | Check List Item | | | RISK | | | |
|--|--|---|---|---------------------|--|---|--------|----------------|------|--|--|--|
| | | | 7 | | e FW administrator will ensure all administrative access I modification to the FW configuration are logged. | | | | | | | |
| Risk o Comp | | | Undetected firewall access violations and configuration changes to the firewall settings. | | | | | | | | | |
| Procee | dure | Log in as admin using the web interface: <u>https://192.168.22.1</u> 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 | admin | login/logout event' | and | t > Log Setting > con 'when configuration policy changes are re | has ch | anged' are sel | • | | | |
| Concl | usion | | 22 | | | | | | | | | |
| Refere | 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 | # | | Cł | neck List Item | | RISK | |
|---|--------|-------------------------------------|---|--|---------------------------|--|--|-----------------------------------|--|
| | | | 8 | The current and pre and saved in a secu | | s router configuration cation. | are backed up | MH | |
| Risk of Non ComplianceUnauthorized configuration changes and corruption of the stored files. protection affects Real-time Recovery Objective (RT0). | | | | | | | | backup | |
| Procee | dure | | | | - | onfiguration file loca | |) | |
| Verify | | | heck the creation dates of the configuration back up files. They must be different. heck if the files are stored in a secure system. | | | | | | |
| Concl | usion | | | | | | | | |
| Refere | ence | Opera Route (Section and M | tions r Secu on 3.3 lainter | (Section 3.6.3 –Logi urity Configuration (3.2 Updating the Rou nance). | stics Guide Iter ai | cklist – Version 4, Re for Configuration Los (SNAC) – NSA Rev nd 4.1.8 – Logistics fo //www.sans.org/score | ading and Mainte sion 27, 2002, V or configuration I | enance). ersion 1.1 Loading | |
| | Subjec | ctive | ve Objective X Evidence Findings | | | | | | |
| | | | | • | | 6 | • | | |

| N/A | Pass | Fail | # | | Check List Item | | RISK | | |
|--|--------------------------------------|---|---|--|---|---|------|--|--|
| | | | On the system where the configuration files are stored, the local9operating system's security mechanisms will be used forMHrestricting access to the files | | | | | | |
| Risk of Non Unauthorized configuration changes and corruption of the stored files. No backup Compliance protection affects Real-time Recovery Objective (RT0). | | | | | | | cup | | |
| Proce | edure | Compa (previo | 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). | | | | | | |
| Verif | ÿ | | folder | | a NTFS formatted volume a administrator (S) of the | • | | | |
| Conc | clusion | | 2 | | | | | | |
| Refer | rence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | |
| | SubjectiveObjectiveXEvidenceFindings | | | | | | ings | | |

| N/A | Pass | Fail | # | | | Check List Item | | | F | RISK |
|--------------------------------------|-------------------|------------------|--|---|------|--|-------|------------------|---|------|
| | | | 10Ensure 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 | | | | | | | |
| | of Non pliance | Explo | xploitation of known vulnerabilities. | | | | | | | |
| Proce | edure | at b) A of | tack d sk the f these | efinition Versions. Administrator to log items. | gin | the administrator. Note at the Fortinet support s | | | | |
| | | c) C | heck A | Automatic update fui | ncti | on if they are enabled. | | | | |
| Verif | y | Comp | are th | e version numbers. 7 | The | versions in Fortigate-10 | 00 mu | st be the latest | • | |
| Conc | lusion | | | | | S. | | | | |
| Refer | ence | Route (Secti | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | |
| SubjectiveObjectiveXEvidenceFindings | | | | | | | | | | |

| | - | | N' | - |
|---------------------------|-------|---------|--|---------------|
| N/A Pass | Fail | # | Check List Item | RISK |
| | | 11 | Review the ruleset EXT > INT to ensure that they follow the order as follows: firewall Lockdown anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) Deny unwanted inbound services User permit rules (allow CITRIX ICA and HTTPS) Noise drops (e.g. discard multicasts, OSPF and HSRP chatter) Deny and Alert (alert systems administrator about traffic that is suspicious) Deny and log (log remaining traffic for analysis) 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. | Н |
| Risk of Non Compliance | Misco | onfigu | uration. Ineffective rulesets. | |
| Procedure | a) S | elect | lmin using the web interface. Firewall>Addresses>External - Note the results Firewall > Policy > 'EXT>INT' – Note the results | |
| Verify | Check | k the l | Rule order, as above. Make sure that logging is enabled for all the | denied rules. |
| Conclusion | | | | |

| Reference | | hecklist by Naidu, K our Firewall Ruleba | _ | | | |
|-----------|--------|---|---|----------|----------|--|
| Subj | ective | Objective | X | Evidence | Findings | |

| N/A | Pass | Fail | # | | C | neck List Item | | RISK |
|------------------|-------|---------|---------|---|---|---|--|--------------|
| | | | 12 | as follows: allow ipsec tunnel anti-spoofing filter addresses appeari blocked unwanted User permit rules Deny and log (log Firewalls operate on a is important to ensure | rs (bl ing fr outb (e.g. rema a firs that | | s, internal veb server) is) vbove structure t out instead of | Н |
| Risk of Compl | | Misco | onfigur | ation. Ineffective rules | ets. | 10 | | |
| | | - | | nin using the web inter | | 0 | | |
| Proced | lure | | | all>Addresses>Interna | | | | |
| | | | | all > Policy > 'INT>E | | | | |
| Verify | | Check | the R | ule order, as above. Ma | ake si | are that logging is enabl | ed for all the deni | ed rules. |
| Conclu | usion | | | | | | | |
| Refere | nce | | | | | ww.sans.org/score/firev nce Spitzner <u>http://www</u> | | <u>.html</u> |
| | Sub | jective | | Objective | Х | Evidence | Findi | ngs |
| | | | | | | | | |

2.2.0 Port Filtering

| N/A | 0 Port Fi Pass | Fail | # | Chec | k List Item | RISK | | | |
|------------------|-------------------|--------------------------------|------------------------------|--|--|------|--|--|--|
| 1 1/11 | 1 400 | 1 411 | | | wired, risky protocols and services | | | | |
| | | | 13 | in either direction. | | Н | | | |
| | | | | 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 | | | | |
| | | | 13 | 5 (TCP & UDP) | loc-srv | | | | |
| | | | 13 | 7 (TCP & UDP) | netbios-ns | | | | |
| | | | 13 | 8 (TCP & UDP) | netbios-dgm | | | | |
| | | | 13 | 9 (TCP & UDP) | netbios-ssn | | | | |
| | | | 17 | 7 (UDP) | xdmcp | | | | |
| | | | 44 | 5 (TCP) | netbios (ds) | | | | |
| | | | 51 | 2 (TCP) | rexec | | | | |
| | | | 51 | 5 (TCP) | lpr | | | | |
| | | | 51 | 7 (UDP) | talk | | | | |
| | | | 51 | 8 (UDP) | ntalk | | | | |
| | | | 54 | 0 (TCP) | uucp | | | | |
| | | | 19 | 00, 5000 (TCP & UDP) | Microsoft UPnP SSDP | | | | |
| | | | 12 | 345 (TCP) | NetBus | | | | |
| | | | 12 | 346 (TCP) | NetBus | | | | |
| | | | 31 | 337 (TCP & UDP) | Back Orifice | | | | |
| Risk of Compl | | These p | oorts c | an be used for denial of service | e and or sending malicious codes | | | | |
| Proced | lure | The cus group I the netv | stom s Disallo work. (| ervices are additional ports/ser wed_ services contains all the | n to the web interface. Select Firewall > Service > Custom rvices are additional ports/services that are not in the predefined list ved_ services contains all the ports that are unnecessary and denied heck that this group of services are denied and logging enabled bot INT > EXT Policies. | | | | |
| Verify | | Verify | that th | e list reflect the ports mentione | ed in this checklist. | | | | |
| Concl | | | | * | | | | | |
| Conci | usivii | ļ | | | | | | | |

| Reference | (Section 3.2 F JANET-CER' <u>CERT/preven</u> | Protecting the netw Γ: Services that ro tion/cisco/local_se | ork v uter s ervice | hould block. http://ww | ww.ja.r | net/CERT/JANET- | n 1.1 | |
|-----------|--|---|---------------------------|------------------------|---------|-----------------|-------|--|
| Sub | ojective | tive Objective X Evidence Findings | | | | | | |

| N/A | Pass | Fail | # | | Check L | ist Item | | RISK | |
|------------------|--|------------------------------------|---|-------------------------------------|-----------------|--------------------|----------------|--------|--|
| | | | 14 | Permit only requir | ed inbound Pr | otocols and Servi | ces | Н | |
| Risk of Compl | | Intrud | ers ma | y exploit unknown a | and not require | d services. | 0 | | |
| | Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.x29 following commands inbound from the internet for TCP and UDP Ports: | | | | | | | | |
| | | • N | map - | n –P0 -sT –p 1-6553 | 35–oN inbour | nd-syn-scan.txt xx | x.xxx.xxx.x27 | | |
| | | • N: | map – | n –P0 –sU –p 1-6553 | 35 –oN inboun | d-udp-scan.txt xx | x.xxx.xxx.x27 | | |
| Proced | lure | | | mp Packet capture o und packets: | n the internal | network side. Use | following comm | and to | |
| | | tcpdu | np -nr | -vvv –w inboundtc | p-scan.cap hos | st 192.168.22.1 | | | |
| | | tcpdui | np -nr | -vvv –w inboundud | dp-scan.cap ho | st 192.168.22.1 | | | |
| | | | | | | | | | |
| | | Shoul | d only | detect ports 443/tcp | and 1494/tcp. | | | | |
| Verify | | Verify | the lo | gged data for the sca | anning activity | • | | | |
| | | Check | tcpdu | mp for records of the | e port scan tra | fic. | | | |
| Conclu | ision | | | 0 | | | | | |
| Refere | nce | Route (Section SANS Tuesd | 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 | | | | | | |
| | Sub | jective | <u></u> | Objective | X | Evidence | Find | ings | |
| | | 0 | | | | | | - | |

| N/A | Pass | Fail | # | | | Check List Item | | RISK | | |
|----------------|-------|--|--|---|-------|--|--------------------|----------|--|--|
| | | | 15Permit only required inbound Protocols and Services (Fin Scan)H | | | | | | | |
| Risk o Comp | | Intrud closed | | • • | and | not required services. H | Helps to determine | open and | | |
| | | with H | FIN pa | ckets to see if they a | are h | I Interface IP from PC andled differently. Use oN inbound-fin-scan.t | following comman | nds. | | |
| Proced | lure | Set up | o tepdi | * | | e internal network side | | | | |
| | | • tc | pdum | p -nn -vvv –w inbo | und-f | in-scan.cap host 192.1 | 68.22.1 | | | |
| T 7 10 | | | | detect any open port | | | S | | | |
| Verify | | | | ogged data for the so ump for records of the solution of the s | | | | | | |
| Concl | usion | | | | | | | | | |
| Refere | ence | 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 | | | | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Find | ings | | |
| | | | | | 1 | | | | | |

| N/A | Pass | Fail | # | | | Check List Item | | | RISK |
|------------------|--|---|---|--------------------------------------|-------|------------------------|--------|--------------|------------|
| | | | 16 | Permit only requir Scans). | ed in | bound Protocols and | Servic | es (ACK | Н |
| Risk of Compl | | | | y exploit unknown ished connections. | and 1 | not required services. | Helps | to determine | ports that |
| | | Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.x29 with ACK packets to see if they are handled differently. Use following commands: | | | | | | | |
| Proced | | • N | Nmap –n –P0 -sA –p 1-65535 –oN inbound-ack-scan.txt xxx.xxx.xx27 | | | | | | |
| rroceu | lure | | Set up tcpdump Packet capture on the internal network side. Use following command to capture inbound packets: | | | | | | |
| | | • to | pdump | o -nn -vvv -w inbou | nd-A | CK-scan.cap host 19 | 2.168. | 22.1 | |
| | | Shoul | d not c | letect any open port | s. | | | | |
| Verify | | Verify | y the lo | ogged data for the so | anni | ng activity. | | | |
| | | Checl | c tepdu | mp for records of th | ne po | rt scan traffic. | | | |
| Concl | usion | | | | | | | | |
| Refere | ference 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 | Х | Evidence | | Find | ings |

| N/A | Pass | Fail | # | Check List Item RISK | | | | | | |
|----------------|---|--------|--|---|--|--|--|--|--|--|
| | | | 17Permit only required Outbound Protocols and Services.H | | | | | | | |
| Risk o Comp | | intruc | ler aff | programs, proxy connections may provide back door connections to an fecting confidentiality and integrity of data. Become an unwitting in DDos attacks. | | | | | | |
| | | Use f | ollow | ort scanning of the internal Interface IP from PC FBSD 192.168.22.210. ing commands: | | | | | | |
| Procee | lure | • N | Imap | -n -P0 -sTp 1-65535 -oN outbound-syn-scan.txt 192.168.22.1 -n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1 lump Packet capture on the external network side. Use following command | | | | | | |
| | | to cap | oture i | inbound packets: p -nn -vvv -w servicesouttcp-scan.cap host xxx.xxx.xx27 (for TCP) | | | | | | |
| | | | - | np -nn -vvv -w servicesoutudp-scan.cap host xxx.xxx.xx27 (for UDP) | | | | | | |
| Verify | | | | y detect ports 22/tcp and 443/tcp. logged data of the scanning activity. | | | | | | |
| | | Chec | k tepd | lump for records of the port scan traffic. | | | | | | |
| Concl | usion | | | | | | | | | |
| Refere | ReferenceSANS – 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 | | | | | | | | | |
| | Subj | ective | | Objective X Evidence Findings | | | | | | |

| N/A | Pass | Fail | # | Check List Item | RISK | | | | | |
|--|----------|---|---|---|-----------|--|--|--|--|--|
| | | | 18 | Permit only required Outbound Protocols and Services (FIN Scan Test). | Н | | | | | |
| Risk of Non ComplianceMalicious programs, proxy connections may provide back door connections intruder affecting confidentiality and integrity of data. Become an unwitting in DDos attacks | | | | | | | | | | |
| | | | | t scanning of the internal Interface IP from PC FBSD 192.168.22 to see if they are handled differently. Use following commands: | .210 with | | | | | |
| Procee | duna | • N1 | • Nmap –n –P0 -sF –p 1-65535 –oN outbound-fin-scan.txt 192.168.22.1 | | | | | | | |
| rioced | uure | Set up tcpdump Packet capture on the external network side. Use following command to capture inbound packets: | | | | | | | | |
| | | • tcj | odump | -nn -vvv -w outbound-fin-scan. cap host xxx.xxx.xx27 | | | | | | |
| | | Should | l not d | etect any open ports. | | | | | | |
| Verify | , | Verify the logged data of the scanning activity. | | | | | | | | |
| | | Check | tcpdu | mp for records of the port scan traffic. | | | | | | |
| Concl | lusion | | | | | | | | | |
| Refere | ence | SANS Tuesda | Instite ay, Ma | NA Courseware ute – Webcast – Auditing a Network Perimeter by Chris Brenton. arch 16, 2004, 1:00pm EST (1800 UTC) w.sans.org/webcasts/show.php?webcastid=90504 | | | | | | |

| | Sub | ojective | | Objective | Х | Evidence | | Findir | ngs |
|---|-------|---|---------|---|------|------------------------|---------|--------------|------|
| N/A | Pass | Fail | # | | C | heck List Item | | | RISK |
| | | | 19 | Permit only required Scan test). | d Ou | tbound Protocols ar | nd Serv | vices (ACK | Н |
| Risk o Compl | | 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 | | | | | | | |
| | | ACK | packe | t scanning of the intensity to see if they are has $p = \frac{1}{2} \frac{6553}{2}$ | ndle | d differently. Use for | ollowir | ng commands: | |
| Procee | lure | 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.x27 | | | | | | | |
| | | Should not detect any open ports. | | | | | | | |
| Verify | | Verify the logged data if the scanning activity is detected. | | | | | | | |
| | | Check | c tepdi | imp for records of the | por | t scan traffic. | | | |
| Concl | usion | | | | | | | | |
| ReferenceSANS – 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 | | | | | | | | | |
| | Subj | ective | | Objective | X | Evidence | | Findi | ngs |

| N/A | Pass | Fail | # | | (| Check List Item | | RISK |
|--------|--|--|--------|--|-----|--|--------------------|------|
| | | | 20 | Reject Inbound tra Message Protocol | | ontaining ICMP (Int fic. Log Event. | ternet Control | М |
| | Risk of Non ComplianceIntruders may gather information for Denial of Service attacks. | | | | | | | |
| Procee | dure | e 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 | k pred | efined Service IC | MP_ | Any is in the disall | owed services list | |
| Concl | usion | | | | | | | |
| Refere | ence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | |
| | Subjective | | | Objective | Χ | Evidence | Find | |

2.3.0 Address Filtering

| N/A | Pass | Fail | # | | C | heck List Item | | RISK | | | |
|----------------|--|------------------|-------|---|----------|----------------------|---------------------|----------|--|--|--|
| | | | 21 | Reject all Traffic following source 0.0.0.0/8 Historic 10.0.0.0/8 RFC 1 169.254.0.0/16 L 172.16.0.0/12 RF 192.168.0.0/16 R 224.0.0.0/4 Class 240.0.0.0/5 Class 248.0.0.0/5 Unall 255.255.255.255/ | Н | | | | | | |
| Risk o Comp | | IP Spo | ofing | to start denial of se | ervice a | attempts or send mal | licious codes. | | | | |
| | | | | Login to Firewall as admin using the web interface. Select> irewall>Policy>'EXT>INT' | | | | | | | |
| Verify | 7 | Verify loggin | | | are in | cluded in the policy | and set to deny acc | cess and | | | |
| Conc | lusion | | | | | | | | | | |
| Refere | 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 | | | | | | | .php | | | |
| | Subj | ective | | Objective | X | Evidence | | lings | | | |
| | | | | | | | | | | | |

| N/A | Pass | Fail | # | | C | heck List Item | | RISK | |
|----------------|--|--------|--------|-----------------------|--|--|----------------|------|--|
| | | | 22 | source IP addres. | Reject all Traffic from the Internal Networks that bear a source IP address which does not belong to the internal network (outbound) | | | | |
| Risk o Comp | | IP Spo | oofing | to start denial of se | ervice a | ttempts or send ma | licious codes. | | |
| Procee | ProcedureCheck 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.x43 -a 192.168.0.20 -p 21 b) hping -S xxx.xxx.x43 -a 192.168.20.20 -p 21 | | | | | | FBSD | | |
| Verify | | | | | • | hould be allowed o lenied access (polic | | | |
| Concl | usion | | | | | | | | |
| Refere | Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2Implementing Firewall Ruleset).Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version1.1 (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 | | ffic from a system using address ranges :10.0.0. 5 | | Н | | |
| Risk of Non ComplianceIP Spoofing to start denial of service attempts or send malicious codes. | | | | | | | | | |
| | | | | ewall INT>EXT rul | eset for the specific poli d as below: | cy. From internal Po | C FBSD | | |
| Procee | dure | hping -S 10.10.20.20 -a 172.16.20.20 -p ++21 | | | | | | | |
| | | hping -S xxx.xxx.x43 -a 10.10.20.20 | | | | | | | |
| | | hping –S xxx.xxx.x43–a 169.254.20.20 | | | | | | | |
| Vonifu | 7 | Verify the above addresses are denied access. | | | | | | | |
| Verify | | Verify the logs for the record of the denied activities. | | | | | | | |
| Concl | lusion | | | | | | | | |
| Refere | ence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | |
| | Subjective | | | Objective | X Evidence | Find | ings | | |

| N/A | Pass | Fail | # | | С | heck 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> | | | | | |
| Risk of Non Compliance IP Spoofing to start denial of service attempts or send malicious codes. | | | | | | | | | |
| Procee | ProcedureCheck the Firewall EXT>INT ruleset for the specific policy. From external PC FSAUDIT xxx.xxx.xx29 execute command as below: a) hping -S xxx.xxx.x27 -a 10.10.21.21 -p 80 b) hping -S xxx.xxx.x27 -a 172.168.20.20 -p 23 | | | | | | ΡC | | |
| Verify | 7 | • | | bove addresses are ogs for the record o | | | | | |
| Concl | lusion | | | | | | | | |
| Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2Implementing Firewall Ruleset).Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version1.1 (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 | # | | Che | ck List Item | | RISK | | |
|---|--------|---|--|------------------------------|------------|--------------------|-------------------|------|--|--|
| | | | 25 | Reject Outbound Log event | traffic co | ntaining broadce | ast addresses and | Н | | |
| Risk o Comp | | Unwitting participant in Denial of Service Attacks. | | | | | | | | |
| ProcedureCheck the Firewall INT>EXT ruleset for the specific policy. From internal PC FBS192.168.22.210 execute command as below: | | | | | | C FBSD | | | | |
| | | nmap | nmap –sS –O -PO -e dcO -S 255.255.255.192.168.22.1 | | | | | | | |
| Verify | , | Check | firewa | all logs to see if the | broadcas | sts are recorded a | and dropped. | | | |
| Concl | lusion | ċ | | | | | | | | |
| Refere | ence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | | |
| 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:

| | nee allact eighalane greap benelete en | | | | | | |
|---|--|----------|--|--|--|--|--|
| 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 | # | | Cl | neck List Item | | RISK | | |
|----------------|--------|----------------------------|----------------------------------|--|---|----------------------|----------------------|---------|--|--|
| | | | 26 | Interfaces both internetwork-based atta | | nd external must b | e monitored for | Н | | |
| | | • | Inabi | lity to detect misco | nfigur | ed firewalls. | | | | |
| Risk o Comp | | • | | lity to detect attack ks against web serv | | firewalls legitimate | ely allow through (s | such as | | |
| | | • | Inabi | lity to detect inside | . | | | | | |
| Procee | dure | • | | | ewall internal interface 192.168.22.1 using "putty". In the CLI dialogue owing commands: Fortigate-100 # get nids detection interfaces | | | | | |
| Verify | 7 | Both t | he inter | rnal and external is | set to | ON. | | | | |
| verny | | Verify | the DN | MZ interface is set t | wing commands: Fortigate-100 # get nids detection interfaces and external is set to ON. interface is set to OFF. | | | | | |
| Concl | lusion | | | | | | | | | |
| Refere | ence | Router 1.1 (So Techn | r Securi ection 5 ical Inc | ortigate NIDS Guide. rity Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version 5.5 CISCO IOS Intrusion Detection). cursion Countermeasures: FAQ – Network Intrusion Detection Systems icm.com/kb/faq/idsfaq.html | | | | | | |
| | Subj | ective | | Objective | X | Evidence | Find | lings | | |

| N/A | Pass | Fail | # | | Cł | eck List Item | | RISK | | | |
|---|------------|--------|--|----------------------|--|-----------------|------------------|------|--|--|--|
| | | | 27 | files passing throug | ecksum verification must be turned ON. This feature tests as passing through the Fortigate-100 to make sure that they are not been changed in transit. | | | | | | |
| Risk of Non Compliance Inability to detect malicious changes in data during transit. | | | | | | | | | | | |
| Procee | lure | • | 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 C | onclusions: it must | be IP: | ON, TCP: ON, UD | P: ON and ICMP:C | N | | | |
| Concl | usion | | Ś | Ÿ | | | | | | | |
| Refere | ence | Fortin | Fortinet – Fortigate NIDS Guide. | | | | | | | | |
| | Subjective | | 7 | Objective | Х | Evidence | Find | ings | | | |

| N/A | Pass | Fail | # | | Cł | neck List Item | | | RISK | |
|----------------|--|-------------------|--|--|---------|----------------------|---------|--------------|---------|--|
| | | | 28 | All attack detection detection module u groups. By default | ises ov | er 1000 signatures | | | Н | |
| Risk o Comp | | Inabil: attack | - | atch and detect pat | terns o | f security violation | s of mo | ost common i | network | |
| Proce | dure | - | Depen the web interface: <u>https://192.168.22.1</u> . Login as admin. Go to NIDS > Detection > Signature List | | | | | | | |
| Verify | 7 | All sig | gnatures | ires must be enabled. | | | | | | |
| Conc | lusion | | | | | | 2 | | | |
| Refere | ence | Route | 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 Findin | | | | | | ngs | | | |
| | | | | | | | · | | | |

| N/A | Pass | Fail | # | | Cł | neck List Item | | RISK | | |
|---|------------|--|----------------------------------|--|----|----------------|-----------|-------|--|--|
| | | | 29 | NIDS attack preve disabled by default | 2 | | | | | |
| Risk of Non Compliance Inability to prevent the damage either by dropping the packets or by blocking network access. Image: A state of the state o | | | | | | | g network | | | |
| Proce | dure | 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 | 7 | Verify | IDP i | s enabled. |) | | | | | |
| Concl | lusion | | | 0 | | | | | | |
| Refere | ence | Fortin | Fortinet – Fortigate NIDS Guide. | | | | | | | |
| | Subjective | | | Objective X Evidence Find | | | | lings | | |
| | | | | | | | | | | |

| N/A | Pass | Fail | # | | С | heck List Item | | RISK | | |
|----------------|-------|-------------------|---|---|--|---------------------|---------------------|-----------|--|--|
| | | | 30 | All attack preven | tion si | gnatures must be er | nabled. | Н | | |
| Risk o Comp | | Inabili access | | prevent the damage | either | by dropping the pa | ckets or by blockin | g network | | |
| Procee | dure | . | n the web interface: <u>https://192.168.22.1</u> . Login as admin. Go to NIDS > vention | | | | | | | |
| Verify | | 'Enabl | | ention' is checked | ention' is checked. Verify that all individual prevention signature groups | | | | | |
| Concl | usion | | | | | | | | | |
| Refere | ence | Securi | ty Ope | nfrastructure Security Checklist – Version 4, Release 2.2 – DISA Field perations. Fortigate NIDS Guide. | | | | | | |
| | | | | Find | ings | | | | | |

| Risk of Non Compliance 31 Test ID Prevention is functioning. Procedure Undetected internal or external attacks resulting in Denial of Service and or 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 | H amage to | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| Compliance systems and data. Procedure From the internal Test PC FSBD 192.168.22.210 execute the following command | amage to | | | | | | | |
| 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. | Fortinet – Fortigate NIDS Guide. | | | | | | | |
| Subjective Objective X Evidence Finding | | | | | | | | |

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 | # | | Ch | eck List Item | | RIS | K | |
|--------|------------|---|-------------------------------------|----------------------|---------|---------------------|----------------------|---------|---|--|
| | | | 32 | Content filtering m | nust be | enabled in the fire | wall policy. | Mł | Η | |
| | | | | | | | | | | |
| Proce | dure | Login to the web interface. Select Firewall>Policy>'INT>EXT'> Open (Edit) Policyid 2. | | | | | | | | |
| Verify | 7 | Antivi use. | rus an | d Web filter must be | e enabl | ed and the 'Strict' | content profile must | t be in | | |
| Concl | lusion | | .C | | | | | | | |
| Refere | ence | Fortin | Fortinet – Content Protection Guide | | | | | | | |
| | Subjective | | | Objective | Х | Evidence | Findi | ings | | |

| N/A | Pass | Fail | # | | Ch | eck List Item | | | RISK | |
|----------------|------------|---|--|----------------------|---|----------------------|-------|----------------|------|--|
| | | | 33 | | Verify contents of 'Strict Content profile'. This controls how he antivirus protection behaves. | | | | | |
| Risk o Comp | | Down | Downloading of infected files or programs containing malicious codes or viruses. | | | | | | | |
| Proce | dure | Login as admin at the web Interface. Select firewall> Content Profile>Strict. | | | | | | | | |
| Verify | 7 | All op | tions n | nust be selected for | protec | tion, except 'pass f | ragme | nted e-mails'. | | |
| Concl | lusion | | | | | | | | | |
| Refere | ence | Fortin | Fortinet – Content Protection Guide | | | | | | | |
| | Subjective | | | Objective | Х | Evidence | | Findi | ngs | |

| N/A | Pass | Fail | # | | Cł | eck List Item | | RISK | | | |
|----------------|------------------|---|--|---|----------|---------------|--|-------|--|--|--|
| | | | 34 | File blocking must potential threat and computer virus atta | l to pro | | | Н | | | |
| Risk o Comp | of Non liance | Non ance Downloading of files or programs containing malicious codes or viruses. | | | | | | | | | |
| Proce | dure | Login | | | | | | | | | |
| Verify | 7 | - | 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. | | | | | | | | |
| Conc | lusion | | | | | | | | | | |
| Refere | ence | Forti | net – C | ontent Protection G | uide | | | | | | |
| | Subje | ctive Objective X Evidence Findings | | | | | | | | | |
| | | | | dife dife | | | | | | | |
| NT/A | D | TT - 21 | ш | | | l- T - 4 T4 | | DICIZ | | | |

| N/A | Pass | Fail | # | | Cł | eck List Item | | RISK | | |
|---|--|--------|-------------------------------------|--------------------|----------|--------------------|-------|------|--|--|
| | | | 35 | Test File blocking | function | onality. | | Н | | |
| Risk of Non Compliance Downloading of files or programs containing malicious codes or viruses. | | | | | | | | | | |
| Procee | Here From any internal PC browse to <u>http://www.winzip.com</u> and attempt to download a trial version of winzip.exe | | | | | | | | | |
| Verify | , | The de | own lo | ad must be blocked | with a | security alert mes | sage. | | | |
| Concl | usion |) | | | | | | | | |
| Refere | ence | Fortin | Fortinet – Content Protection Guide | | | | | | | |
| | Subjective | | | Objective | Х | Evidence | Find | ings | | |

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

Firewall Internal Interface Address: 192.168.22.1/24 Firewall External Address: xxx.xxx.xx27 Other Internet address used for testing: xxx.xxx.x43



Rama Inc. Test Setup

Tools Used:

PC with FREEBSD Operating System (Ref:<u>http://www.freebsd.org/</u>) for Testing: INT > EXT (FBSD: 192.168.22.210) PC with Redhat Linux Operating System (Ref:<u>http://fedora.redhat.com/</u>) for Testing: EXT > INT (Customer Provided Internet Address FSAUDIT: xxx.xxx.xx29 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 <u>ryan@eEye.com</u> 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:<u>http://www.eeye.com/html/resources/downloads/other/index.html</u>). NmapNT is based on nmap by fyodor@insecure.org (<u>http://www.insecure.org/nmap/</u>).

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 <u>features</u> you would expect in a protocol analyzer, and several features not seen in any other product. Its open source <u>license</u> allows talented <u>experts</u> in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows. (Ref: <u>http://www.ethereal.com/</u>)

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

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 <u>Simon Tatham</u>. Ref: <u>http://putty.bhni.net/</u>

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: <u>http://www.kiwisyslog.com/</u>)

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: <u>https://192.168.22.1</u>. 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'.

| N/A | Pass | Fail | # | | | Check List Item | | | RI | SK |
|----------------|----------|---|--|--|---------------|--|---------|----------------|-----|----|
| | 1.a X | 1.b X | 1 | be granted acce | ess to | ator and other author the FW for adminis administered from a t | tration | | H | Η |
| Risk o Comp | | | ers to | modify the firewall | | ured hosts leave the f s, corrupt its integrity | | - | | .0 |
| Procee | lure: | Line I a) Fo | | | | | | | | |
| Verify | | | | Its will show the admin users name and the specific trusted ip address from ney can connect to the FW and their read/write permissions. | | | | | | |
| Concl | usion | additio Firewa | onal, all. S | separate, user with r ee Part 4: Identified | ead v Vuln | is incompliance, it is write permissions is c erabilities – Details. be administered from | created | for administer | | ie |
| Refere | ence | Netwo Opera Router (Section Accou | Test 1.b Failed. It is presently set to be administered from any internal PC! 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Х | Findi | ngs | Х |

3.1.0 Access and Configuration /Change Management

| 🔮 192.168.22.1 | - PuTTY | | | | 미의 |
|----------------|---------------------|---------|----------|-----------|----------|
| login as: ac | lmin | | | | _ |
| admin0192.16 | 58.22.1's password: | : | | | |
| Type ? for a | a list of commands. | | | | |
| | | | | | |
| | | | | | |
| Fortigate-10 |)0 # get system adr | nin | | | |
| name | ip | netmask | read per | write per | |
| admin | 0.0.0 | 0.0.0.0 | allowed | allowed | |
| | - " □ | | | | |
| Fortigate-10 | JO # [] | | | | |
| | | | | | |

Fortigate-100 # get config set system opmode nat set system tcp_option enable set system admin username admin password 'Enc \$1\$\$p.kEiPgwLfYBnGpjR8ASi.' trusth ost 0.0.0.0 0.0.0.0

| N/A | Pass | Fail | # | | Chec | k List Item | 1 | | RISK | | |
|---|-------------------|--|--|----------------------------|-------|--------------|---------|---------------------|-------|--|--|
| | X | | 2The administrator and other authorized users account password will be encrypted and should be at least 6 characters long.H | | | | | | | | |
| | of Non pliance | Clear text passwords give easy access (password cracking) for intruders to misconfigure the firewall. | | | | | | | | | |
| ProcedureAt 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. | | | | | | | | ing | | | |
| Verif | Ŷ | The p | assv | ord is encrypted. For Pass | sword | ls less than | 6 chara | cters a warning app | ears. | | |
| Conc | clusion | Pass | wor | d is encrypted and the | warr | ning appea | ırs | | | | |
| Refer | rence | 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 | Evidenc e | Х | Findi | | | |

| For | 'ortigate-100 | |
|-----|---|-----------------|
| set | et system opmode nat | |
| set | et system tcp_option enable | |
| set | et system admin username admin password 'Enc \$1\$\$p.kEiPgwLfYBnGp | jR8ASi.' trusth |
| ost | st 0.0.0.0 0.0.0.0 | |

| | New Administrator | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|
| Administrator | rama | | | | | | | | |
| Password | * * * * | | | | | | | | |
| Confirm Password | *** | | | | | | | | |
| Microsoft Internet Explorer | × | | | | | | | | |
| For security reasons, it is better to choo | ose a password that is at least 6 characters long. | | | | | | | | |
| OK | ОК | | | | | | | | |
| UK | Cancer | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| N/A | Pass | Fail | # | | Ch | eck List Item | | | RISK |
|---|---|--------|-------------------------|---|---|------------------|----------|--------------|------|
| | X | | 3 | - | d for unattended console is set for no longer ctivating this timeout period provides H | | | | |
| | Risk of NonAbuse from casual or malicious use through the open session (for longer timeout periods) by unauthorized users, if they get physical access to the session. | | | | | | | out | |
| Proced | lure | | ing co Forti Logi | nand Line Interface mmand: igate-100 # get syst in and wait for the e login | em opt | ion. Note the re | esults. | | |
| Verify | 7 | The v | alues | for 'Admin time | out' i | s 15 minutes. | | | |
| Conclu | ision | The ad | lmin ti | me out is in compl | ance a | nd the timeout | period | s effective. | |
| ReferenceNetwork 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 Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php | | | | | | | sion 1.1 | | |
| | Subjective | | | Objective | Х | Evidence | Х | Findings | Х |

```
Fortigate-100 # <u>get system</u> 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 | | | RI | SK |
|---|---------|------|---|------------------|------|---------------------|--------|-------|-----|----|
| | Х | | 4 <i>The FW administrator will ensure modems will not be used for remote administration</i> | | | | | | I | Η |
| Risk of Non ComplianceWar-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 | | | | | | | k if | | | |
| Verify Physically. | | | | | | | | | | |
| Concl | lusion | No M | ode | em Connection Av | aila | ble for Fortigate-1 | 00 ser | ies. | | |
| ReferenceNetwork 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 (Section 4.1.6 Remote Access) Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php | | | | | | | 1.1 | | | |
| | Subject | ive | | Objective | Х | Evidence | | Findi | ngs | |
| | | | | | | | | | | |

| N/A | Pass | Fail | # | Check List Item | RISK | | | | |
|--|-------|---|--------|---|-------------|--|--|--|--|
| | | Х | 5 | The FW administrator will disable FW interfaces that are not in use | Н | | | | |
| Risk of Non ComplianceScanning 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. | | | | | | | | | |
| Procee | lure | At the CLI Execute the following command: Fortigate-100 # get system interface | | | | | | | |
| Verify | | The list | sts of | interfaces that are up are shown. Ensure that the DMZ interface i | s disabled. | | | | |
| Concl | usion | The I | OMZ | Interface is not Disabled. It is Administratively up and | running | | | | |
| Refere | ence | 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 | | | | | | | |
| | | | | Objective X Evidence X Find | ings X | | | | |

| Fortigate_100 ff get evetom interfege | |
|--|-----------------|
| 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 |
| Detect Serv: disable | |
| mac address: 00:09:0F:02:00:FC | |
| (NIC mac address): (00:09:0f:0) | 2:00: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:0) | |
| 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:0) | |
| 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 | | | | | | | SK | | | |
|--|-------|-----------------------------------|--|--|--|----------|------------------|--------|------|--|--|--|
| | | | | - 1 | orts on the internal interfo | | | | | | | |
| | | Х | 6 | | access to the FW and they | , are re | stricted to |] | Η | | | |
| | | | | SSH or SSL encryp | otions. | | | | | | | |
| Risk of Compl | | Man-ii | n-the | -middle attack, Sess | ion hijacking. | | | | | | | |
| | | At the | At the CLI Execute the following command: | | | | | | | | | |
| Proced | lure | a) | a) Fortigate-100 # get system interface. Note the results. | | | | | | | | | |
| | | b) | - | | al interface through web in | | _ = = | | | | | |
| Verify | | | | | ls 'ssh, https' only for the nal interface of the firewa | | l interface. Y | You sh | ould | | | |
| Concl | usion | | | the tests results v l for connection t | vere positive. The DM hrough HTTPS! | Z is al | so set to be | 9 | | | | |
| | | | | | y Checklist – Version 4, R | Release | 2.2 DISA Fi | ield | | | | |
| | | Operat | tions | (Section 3.5.7 – In- | band Router Management | t) | | | | | | |
| Refere | nce | | | | Guide (SNAC) – NSA Re | | 27, 2002, Ve | ersion | 1.1 | | | |
| | | | | | Remote Administration sec | | vallabooklist | + nhn | | | | |
| Firewall Checklist by Naidu, K. <u>http://www.sans.org/score/firewallchecklist</u> | | | | | | | | | | | | |
| | Subi | ective | | Objective | X Evidence | X | Find | lings | X | | | |
| | Subj | ective | | Objective | X Evidence | X | Find | lings | X | | | |
| | | | | situte age | X Evidence | X | Find | lings | X | | | |
| | | ective | | situte age | X Evidence | X | Finc | dings | X | | | |

```
Fortigate-100 # get system interface
Interface
       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 1500bvtes
       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 | # | | С | heck List Item | | | RISK | | |
|--------|---|---|--------|---|---|----------------------|---------|---------------|-----------|--|--|
| | Х | | 7 | | The FW administrator will ensure all administrative access and modification to the FW configuration are logged.H | | | | | | |
| | Risk of NonUndetected firewall access violations and configuration changes to the firewall settings. | | | | | | | all | | | |
| Procee | ProcedureLog 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. | | | | | | | | elect ok. | | |
| Verify | , | lo | gin/lo | that under Log & Ro ogout event' and 'wh the logs to verify the | nen co | onfiguration has cha | nged' a | are selected. | g: 'admin | | |
| Concl | usion | In Co | mplia | nce | | | | Y | | | |
| Refere | ence | 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 | Х | Evidence | Х | Findi | | | |



| Log Setting Traffic Filter |
|--------------------------------|
| Remote I |
| 🔽 Traffic Log |
| 🔽 Event Log |
| When configuration has changed |
| IPSec negotiation event |
| DHCP service event |
| L2TP/PPTP/PPPoE service event |
| 🗹 Admin login/logout event |
| IP/MAC binding event |
| System activity event |
| 🗖 HA activity event |
| Firewall authentication event |
| 🗖 Route gateway event |
| 🔽 Failed update |
| Successful update |
| FDN error |
| OK Cancel |

(4)2.168.22.11)"

| <u>\.</u> | | | |
|--------------------------|-----------------|---------------|--|
| Local7.Info 192.168.22,1 | date=2004-D6-03 | time=08:36(22 | device_id=ffGT1002801021129 |
| subtype=config | pri=information | user=admin | ui=GUI(192.168.22.11) module=log submodule=logsetting msg="Log |
| Policy has | been modified | by user | admin via GUI(192.168.22.11)" |

| N/A | Pass | Fail | # | | Cł | neck List Item | | | RI | SK |
|--------|---|---|-----------------|--|---------------|--------------------|---------|---------------|--------|------|
| | Х | | 8 | The current and pre and saved in a secu | | | tion ar | e backed up | Ν | ſH |
| | | | | orized configuration on affects Real-time | | • | | stored files. | No bao | ckup |
| Procee | Procedurea)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. | | | | | | | | .t. |
| Concl | usion | System the same | n, wit ne da | tee. The files are stor the admin access only the 5/31/2004. The of nissions set are iden | . No d bac | te: The administra | tor con | solidated the | backuj | p on |
| Refere | and the permissions set are identical.Network Infrastructure Security Checklist – Version 4, Release 2.2 DISA Field Operations (Section 3.6.3 –Logistics for Configuration Loading and Maintenance).ReferenceRouter 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 | | | | | | | | 1.1 | |
| | Subjective | | | Objective | Х | Evidence | Х | Find | ings | Х |

| 🔁 FGT Backup | | | | |
|---|---------------------|-------|---------------------------------|--|
| File Edit View Favorites Tools | Help | | | 10 A |
| 🗢 Back 🔹 🔿 👻 🔂 🔞 Search | 🔁 Folders 🛛 🕥 🛛 🖓 🛛 | ł×∽ ≡ | - | |
| Address 🔄 C:\FGT Backup | | | | ▼ 🖗 😡 |
| FGT Backup | Name A | | Type File Folder CFG File | Modified 5/31/2004 4:28 PM 5/31/2004 4:27 PM |
| Select an item to view its description. See also: <u>My Documents</u> <u>My Network Places</u> <u>My Computer</u> | - | | | |

| | | | 1 | | |
|---|-------------------|---------|----------|---------------------------------------|------------|
| 🔁 Old Backup | | | | | |
| File Edit View Favorites Tools | Help | | | | 11 |
| 🗢 Back 🔹 🔿 👻 🖹 🥘 Search | 🔁 Folders 🛛 🎯 🛛 🚰 | n X 🛛 🖩 | - | | |
| Address 🗀 C:\FGT Backup\Old Backup | | | | | <i>∂</i> ⊙ |
| | Name 🛆 | Size | Туре | Modified | |
| | 🔊 fgt.cfg | 19 KB | CFG File | 2/27/2004 11:57 | 7 AM |
| Old Backup | | | | | |
| | - | | | | |
| Select an item to view its description. | | | | \searrow | |
| See also: | | | | , , , , , , , , , , , , , , , , , , , | |
| My Documents My Network Places | | | | | |
| My Computer | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| N/A | Pass | Fail | # | Check List Item | RI | SK | | | |
|--|--|---|--|-----------------------------|----|----|--|--|--|
| | Х | | On the system where the configuration files are stored, the9local operating system's security mechanisms will be used for restricting access to the files | | | | | | |
| | Risk of NonUnauthorized configuration changes and corruption of the stored files. No backupComplianceprotection 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 pf the folder. Verify that only the administrator (S) of the firewall has full permission to the folder. | | | | | | | |
| Concl | Conclusion The files are stored in a PC with Windows 2000 Professional Operating System, with admin access only | | | | | | | | |
| Refere | ReferenceNetwork 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 | | | | | | | | |
| | Subj | ective | | Objective X Evidence X Find | | Х | | | |
| | | | | | | | | | |

| FGT Backu | up Properties | <u>?</u> × |
|---|--|----------------|
| General | Sharing Security | |
| Name | | Add 1 |
| | ; dministrator (° , °\Administrator) | Add |
| | aveR (DaveR@i _nt.local) | Remove |
| | | 15 |
| | | |
| | | |
| Permissi | sions: All | w Denv |
| Eull | Control | |
| Modil | ify | |
| Read | d & Execute | |
| | Folder Contents | |
| Read | – | |
| | | |
| Adva | anced | |
| | w inheritable permissions from parent to pro | pagate to this |
| obje | ect | |
| | OK Cancel | Apply |
| <u>, </u> | A. | |
| | | |
| | | |

| N/A | Pass | Fail | # | Check L | list Item | | RISK | | |
|--|--|---|---|---------------------------------|------------------|-----------------------|------|--|--|
| | | Х | X10Ensure 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. | | | | | | | | |
| a) Use web interface and login as the administrator. Note the Firmware, Anti Virus and attack definition Versions. | | | | | | | | | |
| Procee | Procedureb) Ask the Administrator to login at the Fortinet support site and show the latest versions of these items. | | | | | | | | |
| | | c) Ch | neck A | tomatic update function if they | are enabled. | | | | |
| Verify | , | Comp | are the | version numbers. The versions | in Fortigate-100 |) must be the latest. | | | |
| Concl | usion | Not in compliance. The firmware version is older (build212) version Buildusion251. Attack signatures and AV definitions are not the latest.Automatic update is not enabled. Manual update is in effect. | | | | | | | |
| Refere | 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 | | | | | | | | |
| | Sub | jective | | Objective X | Evidence 2 | X Finding | gs 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: | <u>Change to Transparent Mode</u> |
| System: | Restart Shutdown |

| Address in the Address Address Address Address Address | /v2.50/MR8/ | | 🖌 🄁 Co | Links » 📆 🔹 |
|--|-------------------------------------|---------------|--------------|--------------|
| Google - | 🔹 👸 Search Web 🔹 🚿 🗗 61 blocked | '뒽 AutoFill 🔒 | 🔩 Options 🥒 | |
| | Name 🔺 | Size Typ | De Modif | fied |
| Folder Tasks 🔹 🔕 | FGT 100-v250-build251-FORTINET.out | 6.25 MB OUT | r File 4/26/ | 2004 9:34 AM |
| Rename this item | FGT 1K-v250-build251-FORTINET.out | 6.36 MB OUT | r File 4/26/ | 2004 9:34 AM |
| 6 <u>6</u> | FGT 200-v250-build251-FORTINET.out | 6.32 MB OUT | r File 4/26/ | 2004 9:34 AM |
| Move this item | FGT 3000-v250-build251-FORTINET.out | 6.38 MB OUT | r File 4/26/ | 2004 9:34 AM |

| | | | Support |
|--|----------------|------------------|--------------------------------|
| View Products Add Registration Add/Renew | Download Virus | /Attack Updates | Version: v2.50 v2.36 v2.30 |
| Contract Number | Product Model | Virus Definition | Attack Definition |
| Download Virus/Attack Update | FGT-100 | OS2.5.0_4.348 | 2.50_2.109 |
| | | | |

| N/A | Pass | Fail | # | Check List Item | RISK |
|----------------|------------------|-----------------------|--------------------|---|-----------|
| 1.1/2 | X | ran | 11 | Review the ruleset EXT > INT to ensure that they follow the order as follows: firewall Lockdown anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) Deny unwanted inbound services User permit rules (allow CITRIX ICA and HTTPS) Noise drops (e.g. discard multicasts, OSPF and HSRP chatter) Deny and Alert (alert systems administrator about traffic that is suspicious) Deny and log (log remaining traffic for analysis) 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. | H |
| Risk o Comp | of Non liance | Misco | onfigu | ration. Ineffective rulesets. | |
| Proce | | a) S b) S Checl | elect F elect F | min using the web interface. Firewall>Addresses>External - Note the results Firewall > Policy > 'EXT>INT' – Note the results Rule order, as above. Make sure that logging is enabled for all the | e denied |
| | lusion | The | result firew | t gives the list of external addresses configured. t gives the order of the firewall EXT>INT Policy. vall rule is in compliance and logging is enabled for all th | he denied |
| Refere | ence | Firew | all Ch | ecklist by Naidu, K. <u>http://www.sans.org/score/firewallchecklist</u> our Firewall Rulebase by Lance Spitzner <u>http://www.spitzner.net</u> | |
| | Subj | ective | | ObjectiveXEvidenceXFindi | ings X |

| FCRTINE | ΞT | | | A 🗟 🖉 |
|------------------------------|--------------------|---------------------------------|-----------|----------|
| • System | Internal Extern | al DMZ Group | | |
| Firewall | Name | IP/Netmask | Interface | Modify |
| Policy | External_All | 0.0.0/0.0.0.0 | external | S |
| Address | 172_16 | 172.16.0.0/255.240.0.0 | external | ≦ |
| Service | 10_0 | 10.0.0/255.0.0.0 | external | S |
| Schedule | 169_254 | 169.254.0.0/255.255.0.0 | external | S |
| Virtual IP | 224_0 | 224.0.0.0/255.0.0.0 | external | 1 |
| IP Pool | 192_168_22_0 | 192.168.22.0/255.255.255.0 | external | 1 |
| IP/Mac Binding | EXT_BCAST | 255.255.255.255/255.255.255.255 | external | 2 |
| Content Profile | Historical_Broadca | 0.0.0/255.0.0.0 | external | S |
| • User | CLASS_E | 240.0.0.0/248.0.0.0 | external | 1 |
| - 0301 | Unallocated | 248.0.0.0/248.0.0.0 | external | 2 |
| • VPN | New | | | |
| • NIDS | New | | | |
| | | | | |

| -irewall | | # ID | Source | Dest | Schedule | Service | Action | Enable | Config |
|----------------------------------|---|------|--------------------|--------------|----------|--------------------|--------|--------|--------|
| olicy | : | 1 14 | External_All | Router | Always | ANY | DENY | • | 1 🔊 🖆 |
| ddress | 2 | 2 20 | EXT_BCAST | Internal_All | Always | ANY | DENY | • | 1 🔊 🖆 |
| ervice | 3 | 3 25 | Historical_Broadca | Internal_All | Always | ANY | DENY | ~ | 1 🔊 🖆 |
| chedule | 4 | 4 26 | CLASS_E | Internal_All | Always | ANY | DENY | ~ | 1 🐼 🖆 |
| rtual IP | Ę | 5 27 | Unallocated | Internal_All | Always | ANY | DENY | | 1 🖸 🖆 |
| Pool | ť | 5 5 | 192_168_22_0 | 192_168_22 | Always | ANY | DENY | • | 1 🗟 🖆 |
| P/Mac Binding Intent Profile | ; | 76 | 172_16 | Internal_All | Always | ANY | DENY | • | 1 🖸 🖆 |
| | 8 | 3 7 | 10_0 | Internal_All | Always | ANY | DENY | • | 1 🗟 🖆 |
| ser / | 9 | 9 8 | 169_254 | Internal_All | Always | ANY | DENY | ~ | 1 🔊 🖆 |
| N / | 1 | 0 15 | External_All | Internal_All | Always | Disallowed_service | DENY | ~ | 1 🗟 |
| DS | 1 | 1 10 | External_All | Internal_All | Always | 6000_6063 | DENY | • | 1 🗟 🖆 |
| | 1 | 2 3 | External_All | CITRIX_NFUSE | Always | CITRIX_ICA | ACCEPT | | 1 🖸 🖆 |
| nti-Virus | 1 | 3 4 | External_All | http_server | Always | HTTPS | ACCEPT | | 1 🔊 🖆 |
| eb Filter | 1 | 4 11 | 224_0 | Internal_All | Always | ANY | DENY | • | 1 🔊 🖆 |
| | 1 | 5 12 | External_All | Internal_All | Always | ANY | DENY | • | 1 🖻 🖆 |
| mail Filte r og&Report | 5 | | lew | | | | | | |

| N/A | Pass | Fail | # | Check List Item | RISK | | |
|----------------|-------|---|---------|--|----------|--|--|
| | Х | | 12 | Review the ruleset INT > EXT to ensure that they follow the order as follows: 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) 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. | | | |
| Risk o Comp | | Misco | | tion. Ineffective rulesets. | | | |
| Procee | lure | a) Se | lect Fi | nin using the web interface. rewall <addresses>Internal - Note the results rewall > Policy > 'INT>EXT' – Note the results</addresses> | | | |
| Verify | | Check the Rule order, as above. Make sure that logging is enabled for all the denied rules. | | | | | |
| Concl | usion | 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. | | | | | |
| Refere | ence | Firewa | all Che | cklist by Naidu, K. <u>http://www.sans.org/score/firewallcheckl</u> Ir Firewall Rulebase by Lance Spitzner <u>http://www.spitzner.i</u> | ist.php | | |
| | Sub | jective | | | ndings X | | |
| | | | | 0. | | | |

| System | Internal Externa | I DMZ Group | | |
|--------------------------|------------------|----------------------------|-----------|----------|
| Firewall | Name | IP/Netmask | Interface | Modify |
| Policy | Internal_All | 0.0.0.0/0.0.0 | internal | S |
| Address | 192_168_22 | 192.168.22.0/255.255.255.0 | internal | <u></u> |
| Service | Router | 192.168.22.1/255.255.255.0 | internal | 2 |
| Schedule | INT_10_0 | 10.0.0/255.0.0.0 | internal | 2 |
| Virtual IP | INT_172_16 | 172.16.0.0/255.240.0.0 | internal | 2 |
| IP Pool | INT_BCAST | 0.0.0/255.255.255.255 | internal | 2 |
| IP/Mac Binding | INT_169_254 | 169.254.0.0/255.255.0.0 | internal | S |
| Content Profile User VPN | New | | | |

| Fürtin | IET | | | | | | | | A |
|-----------------------|-----|-------|--------------|--------------|----------|----------|----------|--------|---------|
| System | Int | ->Ext | Int->DMZ | DMZ->Int | DMZ->Ext | Ext->Int | Ext->DMZ | | |
| Status | # | ID | Source | Dest | Schedule | Service | Action | Enable | Config |
| Update Network | 1 | 1 | 192_168_22 | External_All | Always | ANY | ENCRYPT | V | 1 🗟 🗗 🕩 |
| RIP | 2 | 19 | INT_BCAST | External_All | Always | ANY | DENY | | 1 🖌 🖓 🕞 |
| Config | 3 | 13 | Internal_All | External_All | Always | PROXY | DENY | • | 1 🖌 🖓 🖿 |
| irewall | 4 | 17 | INT_172_16 | External_All | Always | ANY | DENY | • | 1 🖌 🖓 🖿 |
| | 5 | 24 | INT_169_254 | External_All | Always | ANY | DENY | | 1 🖉 🗇 🕒 |
| Policy Address | 6 | 23 | INT_10_0 | External_All | Always | ANY | DENY | • | 1 🖌 🖓 🖿 |
| Service | 7 | 2 | 192_168_22 | External_All | Always | ANY | ACCEPT | | 1 🖌 🗗 🖿 |
| Schedule | 8 | 21 | Internal_All | External_All | Always | ANY | DENY | | 1 🖌 🖓 🖿 |
| Virtual IP IP Pool | | N | ew | | | | R | | |
| ID /Mac Binding | | | | | | | Ŋ | | |

3.2.0 Port Filtering

| N/A | Pass | Fail | # | | Check I | List Item | RISK |
|-------------------|-------|-------|--------|-----------|--|-------------------------------------|------------|
| | | | 13 | | 0 0 1 | ed, risky protocols and services | |
| | | | | | r direction. | ~ . | |
| | | | | P | ort (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 | |
| | | Х | | 137 | (TCP & UDP) | netbios-ns | Н |
| | | | | 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, 50 | 000 (TCP & UDP) | Microsoft UPnP SSDP | |
| | | | | 12345 | (TCP) | NetBus | |
| | | | | 12346 | (TCP) | NetBus | |
| | | | | 31337 | (TCP & UDP) | Back Orifice | |
| Risk of Compli | | These | e Por | ts can be | used for Denial of Servio | ce and or sending malicious codes | |
| | | Logir | n as a | dmin to t | he web interface. Select | Firewall > Service > Custom | |
| | | | | | - | vices that are not in the predefine | |
| Proced | ure | | | | | ports that are unnecessary and der | |
| | | | | | ck that this group of serv NT > EXT Policies. | vices are denied and logging enabli | led both a |
| Vorte | | | | | | ad in this shashlist | |
| Verify | | | - | | eflect the ports mentione | | |
| a . | • | | | 1 | | The FW is a stateful inspection | |
| Conclu | ision | - | | | | Found a custom service defined | a as |
| | | prox | y not | included | d in the denied outbour | na 11st. | |

| Reference | 1.1 (Secti JANET-C <u>CERT/pre</u> | ecurity Configuration ion 3.2 Protecting the CERT: Services that ro evention/cisco/local_s Checklist by Naidu, K | netwo outer ervic | ork with the Router). should block. <u>http://v</u> es.html | <u>www.j</u> | a.net/CERT/JANET | |
|-----------|--|--|-------------------------|---|--------------|------------------|---|
| Subj | ective | Objective | Х | Evidence | Х | Findings | Х |

| | TET. | | A |
|--|------------------|--|----------|
| | | | |
| • System | Predefined Custo | m Group | |
| • Firewall | Protocol: All | List New | |
| Policy | Service Name | Detail | Modify |
| Address | CITRIX_ICA | tcp/1-65535=>1494 | |
| Service | 6000_6063 | tcp/1-65535=>6000-6063 | |
| Schedule | PROXY | tcp/1-65535=>8000-8088 | S |
| Virtual IP | 445 | tcp/1-65535=>445 udp/1-65535=>445 | ≥ |
| IP Pool | Small_Services | tcp/1-65535=>1-19 udp/1-65535=>1-19 | |
| IP/Mac Binding | Bootp | udp/1-65535=>67 | S |
| Content Profile | 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 | S |
| • VPN | MS_UPnP_SSDP | tcp/1-65535=>1900,1-65535=>5000 udp/1-65535=>1900,1- 65535=>5000 | S |
| | Netbus_BO | tcp/1-65535=>12345-12346,1-65535=>31337 udp/1-65535=>31337 | ≥ |
| • NIDS • Anti-Virus • Web Eilter | | | |

| Predefined Cu | stom Group | |
|--------------------|--|--------|
| | | |
| 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 | 5 |
| New | | |
| | | |

| | Int- | >Ext | t Int->DMZ | DMZ->Int | DMZ->Ext | Ext->Int E | xt->DMZ | | |
|-----------------|------|------|--------------------|--------------|----------|--------------------|---------|----------|---------|
| stem | | | | , | , | | | , | |
| ewall | # | ID | Source | Dest | Schedule | Service | Action | Enable | Config |
| licy | 1 | 14 | External_All | Router | Always | ANY | DENY | V | 1 🐼 🗇 🕻 |
| dress | 2 | 20 | EXT_BCAST | Internal_All | Always | ANY | DENY | | 1 🗟 🖓 🕻 |
| vice | 3 | 25 | Historical_Broadca | Internal_All | Always | ANY | DENY | | 1 🔊 🖓 🕻 |
| edule wal IP | 4 | 26 | CLASS_E | Internal_All | Always | ANY | DENY | | 1 🔊 🗇 🛙 |
| Pool | 5 | 27 | Unallocated | Internal_All | Always | ANY | DENY | | 1 🗟 🗗 🛙 |
| Mac Binding | 6 | 5 | 192_168_22_0 | 192_168_22 | Always | ANY | DENY | | 1 🖌 🖓 1 |
| tent Profile | 7 | 6 | 172_16 | Internal_All | Always | ANY | DENY | | 1 🖌 🖓 1 |
| | 8 | 7 | 10_0 | Internal_All | Always | ANY | DENY | | 1 🖌 🖓 1 |
| | 9 | 8 | 169_254 | Internal_All | Always | ANY | DENY | | 1 🗟 🖓 🕻 |
| | | 15 | External_All | Internal_All | | Disallowed_service | | | 1 🗟 🖓 🕻 |
| s | | 10 | External_All | Internal_All | Always | 6000_6063 | DENY | | 1 🗟 🖓 🕻 |
| -Virus | | 3 | External_All | CITRIX_NFUSE | Always | CITRIX_ICA | ACCEPT | | |
| virus | | 4 | External_All | http_server | Always | HTTPS | ACCEPT | | |
| Filter | | 11 | 224_0 | Internal_All | Always | ANY | DENY | | 1 5 5 C |
| Filter | 10 | 12 | External_All | Internal_All | Always | ANY | DENY | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | 5 | | | | | | | | |
| | | | | | | | | | |
| | S | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

| N/A | Pass | Fail | # | | Check | List Item | | | R | ISK |
|---|-------|--|---|---|---------------|-----------------|-----------|--------------|-------|-----|
| | Х | | 14 | Permit only requ | ired inbound | l Protocols an | d Serv | ices |] | Н |
| Risk o Comp | | Intruc | lers m | ay exploit unknow | n and not rea | quired services | s. | | | |
| Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.xxx.x29. Use following commands inbound from the internet for TCP UDP Ports:• Nmap -n -P0 -sT -p 1-65535 -oN inbound-syn-scan.txt xxx.xxx.x27• Nmap -n -P0 -sU -p 1-65535 -oN inbound-udp-scan.txt xxx.xxx.x27• Set up tcpdump Packet capture on the internal network side. Use following com to capture inbound packets: | | | | | | | x27 27 | | | |
| Verify | | Verif | y the l | v detect ports 443/to ogged data for the ump for records of | scanning act | ivity | | | | |
| Concl | usion | | | ance. Tcpdump o nost. The scannin | | | | riginating f | rom | |
| Refere | ence | SANS Route 1.1 (S SANS Tuesc | scanning host. The scanning activity was detected. 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 | | | | | | | |
| | Subj | ective | | Objective | X | Evidence | Х | Fine | dings | Х |

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 0Interesting ports on xxx.xxx.xx27:0(The 65533 ports scanned but not shown below are in state: filtered)000 PORT STATE SERVICE0000 443/tcp open https0 1494/tcp open citrix-ica00 # Nmap run completed at Fri Jul 9 19:44:40 2004 -- 1 IP address (1 host up) scanned in 45150.948 seconds0

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 000 All 65535 scanned ports on xxx.xxx.xx27 are: filtered00 # Nmap run completed at Tue Jul 13 07:29:07 2004 -- 1 IP address (1 host up) scanned in 78801.685 seconds0

date=2004-07-

09,time=07:16:14,device_id=FGT1002801021129,log_id=0401110252,type=ids,subtype=preven tion,pri=alert,attack_id=100663398,,src=xxx.xxx.x29,dst=xxx.xxx.x27,src_port=1140,d st_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=preven tion,pri=alert,attack_id=100663398,,src=xxx.xxx.x29,dst=xxx.xxx.x27,src_port=1685,d st_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 | | | RI | SK |
|----------------|--|--|--------|--|--------|---------------------|---------|------------|-----|------|
| | Х | | 15 | Permit only requi | red ir | nbound Protocols an | nd Serv | ices (Fin | I | Η |
| Risk o Comp | | | | | | | | | | and |
| Procee | dure | Perform Port scanning of the external Interface IP from PC FSAUDIT xxx.xxx.x29 with FIN packets to see if they are handled differently. Use following commands: Nmap -n -P0 -sF -p 1-65535 -oN inbound-fin-scan.txt 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 | | | | | | | | ving |
| Verify | 7 | Verify | the lo | etect any open ports gged data for the sc mp for records of th | annir | • • | | | | |
| Concl | lusion | _ | | etected. Scanning | acti | vity logged. No a | ctivity | in tcpdump | | |
| Refere | records. 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 | | | | | | | | | |
| | Sub | jective | | Objective | Х | Evidence | Х | Findi | ngs | Х |

nmap 3.50 scan initiated wed Jul 14 11:48:17 2004 as: nmap -n -PO -sF -p 1-65535 -oN inbound-fin-scan.txt xxx.xxx.xxx.x27 D

All 65535 scanned ports on xxx.xxx.xxx.x27 are: filtered00

Nmap run completed at Thu Jul 15 09:42:05 2004 -- 1 IP address (1 host up) scanned in 78828.459 secondsD

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.xx29,dst=xxx.xxx.x27,src_ port=58736,dst_port=36463,status=detected,proto=6,service=36463/tcp,msg="tcprease mbly: 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.xx29,dst=xxx.xxx.x27,src_ port=58737,dst_port=39481,status=detected,proto=6,service=39481/tcp,msg="tcprease mbly: STEALTH ACTIVITY (FIN scan)[Reference: http://www.fortinet.com/ids/ID7274504]"

| NT/A | Daga | Fail | Fail # Check List Item RISK | | | | | | | | |
|---------|--------|-------------------------------------|-----------------------------------|--------------------------------------|-------------|---------|------------|----------|-----|--|--|
| N/A | Pass | Fall | Ħ | | | | | KI | SK | | |
| | Х | | 16 | Permit only required inbound Pro | ptocols and | Servic | es (ACK | 1 | Н | | |
| | | | | Scans). | | | | | | | |
| Risk of | f Non | Intruc | lers m | y exploit unknown and not require | d services. | Helps | to determ | ine port | s | | |
| Comp | liance | that allow established connections. | | | | | | | | | |
| | | Perfo | rm Po | scanning of the external Interface | IP from P | C FSA | UDIT | | | | |
| | | xxx.x | XX.XXX | x29 with ACK packets to see if th | ey are hand | dled di | fferently. | Use | | | |
| | | follow | ving co | mmands: | - | | - | | | | |
| Procee | lure | • N | map - | n –P0 -sA –p 1-65535 –oN inbour | nd-ack-sca | n.txt x | xx.xxx.xx | x.x27 | | | |
| | | Set up | o tepdu | mp Packet capture on the internal | network sid | de. Use | following | g comma | and | | |
| | | to cap | oture in | bound packets: | | | | | | | |
| | | tcpdu | mp -ni | -vvv -w inbound-ack-scan.cap ho | ost 192.168 | .22.1 | | | | | |
| | | Shoul | d not | etect any open ports | | | | | | | |
| Verify | | Verif | y the l | gged data for the scanning activity | <i>.</i> | | | | | | |
| | | Checl | s tepdu | mp for records of the port scan trat | ffic. | | | | | | |
| Concl | usion | No p | orts d | etected. Scanning activity logg | ged. No ac | etivity | in tcpdu | mp | | | |
| Conci | usion | recor | rds. | | | | | | | | |
| | | SANS | S - GS | NA Courseware | | | | | | | |
| Refere | nco | SANS | 5 Instit | te – Webcast – Auditing a Networ | rk Perimete | er by C | hris Brent | on. | | | |
| Kelele | | Tuesc | lay, M | rch 16, 2004, 1:00pm EST (1800 | UTC) | | | | | | |
| | | http | ://ww | w.sans.org/webcasts/show.p | php?webca | astid | =90504 | | | | |
| | Subj | ective | | Objective X E | Evidence | Χ | Fii | ndings | Х | | |

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.xx27 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.xx29,dst=xxx.xxx.x27,sr c_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="portsca n: xxx.xxx.xx29 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 o Comp | | intruc | ler aff | programs, proxy connections may provide back door connections to an fecting confidentiality and integrity of data. Become an unwitting in DDos attacks | |
| | | Use f | ollow | ort scanning of the internal Interface IP from PC FBSD 192.168.22.210. ing commands: -n -P0 -sTp 1-65535 -oN outbound-syn-scan.txt 192.168.22.1 | |
| Procee | lure | | - | -n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1* n -P0 -sU -p 1-65535 -oN outbound-udp-scan.txt 192.168.22.1)* | |
| | | | | tcpdump Packet capture on the external network side. Use following and to capture inbound packets: | |
| | | _ | - | nn -vvv -w servicesouttcp-scan.cap host xxx.xxx.xx27 (for TCP) nn -vvv -w servicesoutudp-scan.cap host xxx.xxx.xxx.x27 (for UDP) | |
| Verify | | Verif | y the I | y detect ports 22/tcp and 443/tcp logged data for the scanning activity. lump for records of the port scan traffic. | |
| Concl | usion | • | - | t 22/tcp and 443/tcp were detected. Scanning activity logged. No a tcpdump records. | |
| Refere | ence | SANS Tuesc | S Insti lay, N | SNA Courseware itute – Webcast – Auditing a Network Perimeter by Chris Brenton. Iarch 16, 2004, 1:00pm EST (1800 UTC) ww.sans.org/webcasts/show.php?webcastid=90504 | |
| | Subj | ective | | Objective X Evidence X Findings X | ζ |

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 192.168.22.1:0(The 65533 ports scanned but not shown below are in state: filtered)000 PORT STATE SERVICE000 22/tcp open ssh0 443/tcp open https00 # 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 -PO -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]"

| | | 1 | | | | | | | | |
|---|-------|--|---------|-------------------------------------|--|----------|------------------|--------|--|--|
| N/A | Pass | Fail#Check List ItemRISK10Permit only required Outbound Protocols and Services (FINH | | | | | | | | |
| | Х | | 18 | Permit only required Scan test). | d Outbound Protocols | and Ser | vices (FIN | Н | | |
| Risk of Non ComplianceMalicious programs, proxy connections may provide back door connections to an intruder affecting confidentiality and integrity of data. Become an unwitting particip- in DDos attacks | | | | | | | | | | |
| | | FIN p | ackets | to see if they are har | ernal Interface IP from adled differently. Use 3 35 –oN outbound-fin-s | followir | ng commands: | 0 with | | |
| Procee | lure | | - | - | N outbound-fin-scan.t | | | | | |
| | | | - | cpdump Packet capture inbound | re on the external netw l packets: | ork sid | e. Use following | | | |
| | | tcpdu | mp -n | n -vvv -w outbound- | fin-scan. cap host xxx. | xxx.xxx | .x27 | | | |
| | | Shoul | d not | detect any open ports | : | | | | | |
| Verify | | Verif | y the l | ogged data for the sca | anning activity. | | | | | |
| | | Checl | c tepdi | ump for records of the | e port scan traffic. | | | | | |
| Concl | usion | No p recor | | letected. Scanning | activity logged. No | activity | y in tcpdump | | | |
| 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 | | | | | | | | | | |
| | Subj | ective | | | X Evidence | X | Finding | s 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]"

| RISK H | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|
| Н | | | | | | | | | | |
| 19Permit only required Outbound Protocols and Services (ACK Scan test).HMalicious programs, proxy connections may provide back door connections to an | | | | | | | | | | |
| o an | | | | | | | | | | |
| 210 with | | | | | | | | | | |
| : | | | | | | | | | | |
| (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: | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Verify the logged data for the scanning activity. | | | | | | | | | | |
| Check tcpdump for records of the port scan traffic. | | | | | | | | | | |
| No ports detected. Scanning activity logged. No activity in tcpdump records. | | | | | | | | | | |
| SANS – GSNA Courseware | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| ngs X | | | | | | | | | | |
| s ** p | | | | | | | | | | |

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=192.168.22.210dst=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_por t=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 | | | | | | | | | | | |
|----------------|-------|--|--|--------------------|-----|---------------------|-------|---------------|------|---|--|--|--|
| 11/11 | 1 455 | X | Reject Inbound traffic containing ICMP (Internet Control | | | | | | | | | | |
| Risk o Comp | | Intruders may gather network information for Denial of Service attacks. | | | | | | | | | | | |
| Procee | lure | 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 | | Chec | k prec | lefined Service IC | MP_ | Any is in the disal | lowed | services list | | | | | |
| Concl | usion | Not in Compliance. Either way. The predefined Service ICMP_Any is not in the disallowed services list. | | | | | | | | | | | |
| Refere | ence | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Х | Find | ings | Х | | | |

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=1b2.168.22.200,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 | # | | Cł | neck List Item | | | RI | SK | |
|--|--|---|----|--|----|----------------|---|-----------------|----|----|--|
| | х | | 21 | Reject all Traffic from the External Networks that bear following source IP address: 0.0.0.0/8 Historical broadcast 10.0.0.0/8 RFC 1918 private network 169.254.0.0/16 Link local networksH1172.16.0.0/12 RFC 1918 private network 192.168.0.0/16 RFC 1918 private network 224.0.0.0/4 Class D multicast 240.0.0.0/5 Class E reserved 248.0.0.0/5 Unallocated 255.255.255.255/32 BroadcastH | | | | | | | |
| | isk of Non ompliance 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. | | | | | | | | ıd | | |
| Concl | lusion | The address are included in the policy and set denied. Logging is enabled for all denied rules. | | | | | | | | ed | |
| 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/fir | | | | | | | | wallchecklist.p | hp | | |
| | Subj | ective | | Objective | X | Evidence | Х | Findir | - | Х | |
| | | | | | | | | | | | |

FERTINET

| System | | al DMZ Group | | |
|-----------------|--------------------|---------------------------------|-----------|----------|
| Firewall | Name | IP/Netmask | Interface | Modify |
| Policy | External_All | 0.0.0/0.0.0 | external | ≥ |
| Address | 172_16 | 172.16.0.0/255.240.0.0 | external | S |
| Service | 10_0 | 10.0.0/255.0.0.0 | external | S |
| Schedule | 169_254 | 169.254.0.0/255.255.0.0 | external | S |
| Virtual IP | 224_0 | 224.0.0.0/255.0.0.0 | external | S |
| IP Pool | 192_168_22_0 | 192.168.22.0/255.255.255.0 | external | ≤ |
| IP/Mac Binding | EXT_BCAST | 255.255.255.255/255.255.255.255 | external | S |
| Content Profile | Historical_Broadca | 0.0.0/255.0.0.0 | external | 1 |
| User | CLASS_E | 240.0.0.0/248.0.0.0 | external | S |
| | Unallocated | 248.0.0.0/248.0.0.0 | external | 2 |

| System | Int- | >Ex | t Int->DMZ | DMZ->Int | DMZ->Ext | Ext->Int E | xt->DMZ | | |
|-----------------|------|-----|--------------------|--------------|----------|--------------------|---------|----------|---------|
| , | | | | | | | | | |
| irewall | # | ID | Source | Dest | Schedule | Service | Action | Enable | Config |
| Policy | 1 | 14 | External_All | Router | Always | ANY | DENY | | 1 🔂 🗇 🕩 |
| ddress | 2 | 20 | EXT_BCAST | Internal_All | Always | ANY | DENY | V | 1 🖌 🖓 🖿 |
| ervice | 3 | 25 | Historical_Broadca | Internal_All | Always | ANY | DENY | | 1 🐨 🗇 🕩 |
| Schedule | 4 | 26 | CLASS_E | Internal_All | Always | ANY | DENY | | 1 🖌 🗇 🖿 |
| 'irtual IP | 5 | 27 | Unallocated | Internal All | Always | ANY | DENY | | 1 🐨 🗗 🕩 |
| P Pool | 6 | 5 | 192_168_22_0 | 192_168_22 | Always | ANY | DENY | V | 1 🗟 🗗 🕞 |
| P/Mac Binding | 7 | 6 | 172 16 | Internal All | Always | ANY | DENY | V | 1 🖌 🗇 🖿 |
| Content Profile | 8 | 7 | 10 0 | Internal All | Always | ANY | DENY | <u> </u> | 1 🖌 🖓 🕩 |
| ser | 9 | 8 | 169_254 | Internal_All | Always | ANY | DENY | | 1 🛛 🗇 🕩 |
| PN | 10 | 15 | External All | Internal All | Always | Disallowed service | DENY | <u> </u> | 1 🖌 🖓 🖿 |
| | | 10 | External_All | Internal All | Always | 6000 6063 | DENY | <u> </u> | 1 🖌 🖓 🕩 |
| IDS | | 3 | External All | CITRIX NEUSE | Always | CITRIX ICA | ACCEPT | - - | 1 🖌 🖓 🕩 |
| nti-Virus | 13 | | External All | http server | Always | HTTPS | ACCEPT | | 1 🖌 🖓 🕩 |
| tab Eilban | | 11 | 224_0 | Internal All | Always | ANY | DENY | | 100 |
| leb Filter | | 12 | External All | Internal_All | Always | ANY | DENY | N N | |
| mail Filter | 13 | 12 | External_All | Internal_All | Aiways | ANT | DENT | | |
| .og&Report | | N | lew | | | | | | |

| N/A | Pass | Fail | # | | С | heck List Item | | | RI | SK | | |
|---|---|--|---|--|--|-------------------|---------|---------------|-------|------|--|--|
| | Х | | 22 | source IP addres | Reject all Traffic from the Internal Networks that bear a source IP address which does not belong to the internal network (outbound) | | | | | | | |
| | of Non pliance IP Spoofing to start denial of service attempts or send malicious codes. | | | | | | | | | | | |
| Check the firewall Int to Ext ruleset for the specific policy. From internal PC FI 192.168.22.210 execute command as below: | | | | | | | | FBS | D | | | |
| Proce | dure | a) hping –S xxx.xxx.xx43 –a 192.168.0.20 –p 21 | | | | | | | | | | |
| | | | b) hping –S xxx.xxx.xx43 –a 192.168.20.20 –p 21 | | | | | | | | | |
| | | | | | | | | | | | | |
| Verify | 7 | The addressees 192.168.22.0 /8 only should be allowed outbound access (Policyid 2) | | | | | | | | | | |
| verny | / | Other 192.168.XXX.XXX should be denied access (policyid 21) | | | | | | | | | | |
| Concl | lusion | In co | In compliance | | | | | | | | | |
| | | Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 | | | | | | | | | | |
| D.C | | | Implementing Firewall Ruleset). Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, Version | | | | | | | | | |
| Refere | ence | | | • | | (SNAC) – NSA Re | evision | Sep, 27, 2002 | , Ver | sion | | |
| | | | | 6.3.2. – Attack Tes cklist by Naidu K | , | /www.sans.org/sco | re/fire | wallchecklist | ohn | | | |
| | Subi | ective | | Objective | . <u>пцр./</u> Х | Evidence | X | Findi | | X | | |
| | Bubj | cenve | | Objective | 11 | Lvidence | 11 | 1 mui | 1185 | 11 | | |

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<mark>,status=accept,src=192.168.22.21,</mark> srcname=192.168.22.21,dst=xxx.xxx.x74,dstname=xxx.xxx.x74,src_int=internal,dst_int=externa I,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.x97,dstname=xxx.xxx.x97,src_int=internal,dst_int=extern al,sent=595,rcvd=742,sent_pkt=10,rcvd_pkt=12,src_port=2668,dst_port=110,vpn=n/a,tran_ip=xxx.xxx.xx x.x27,tran_port=38776,

date=2004-06-

02,time=15:26:00,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,p ri=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.x43,dstname=xxx.xxx.x43,src_int=internal,dst_int=extern al,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;p ri=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;xx43;dstname=xxx;xxx;xx43;src_int=internal;dst_int=extern al;sent=0;rcvd=0;src_port=2014;dst_port=21;vpn=n/a;tran_ip=0.0.00;tran_port=0;

date=2004-06-

02,time=15:36:07,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pr i=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=extern al,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,pr i=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.xx43,dstname=xxx.xxx.xx43,src_int=internal,dst_int=extern al,sent=0,rcvd=0,src_port=1862,dst_port=21,vpn=n/a,tran_ip=0.0.00,tran_port=0]

| N/A | Pass | Fail | # | Check List Item | RISK | | | | | | |
|----------------|--|---|--|----------------------------|----------|--|--|--|--|--|--|
| | X | | Reject outbound traffic from a system using a source address23that falls within the address ranges :10.0.0.0/8 & 172.16.0.0/16(RFC1918), 165.255.0.0/16 (Link Local networks) | | | | | | | | |
| Risk o Comp | of Non oliance | IP Spooting to start denial of service attempts or send malicious codes | | | | | | | | | |
| Proce | ProcedureCheck the Firewall INT>EXT ruleset for the specific policy. From internal PC FBSI 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.x43 -a 10.10.20.20 c) Hping -S xxx.xxx.x43 -a 169.254.20.20 | | | | | | | | | | |
| Verify | ove addresses are denied access. gs for the record of the denied activities. | | | | | | | | | | |
| Conc | lusion | In compliance | | | | | | | | | |
| Refere | Reference Guidelines on Firewalls and Firewall Policy NIST Publication 900-41 (Section 4.2 Implementing Firewall Ruleset). Reference 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 | | | | | | | | | | |
| | Subj | ective | | Objective X Evidence X Fin | ndings 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,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, 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.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=0.0.00,tran_port=0,

log_id=0001000002,type=traffic,subtype=session,pri=notice,SN=109642,duration=0,policyid=23,p roto=6,service=0/tcp**[status=deny,src=10.10.20.20]**srcname=10.10.20.20,dst=xxx.xxx.x43,d stname=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=0.0.00,tran_port=0,
date=2004-06-

02,time=15:23:22,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pr i=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.x43,dstname=xxx.xxx.x43,src_int=internal,dst_int=extern al,sent=0,rcvd=0,src_port=2505,dst_port=21,vpn=n/a,tran_ip=0.0.00,tran_port

date=2004-06-

02,time=15:23:22,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pr i=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.x43,dstname=xxx.xxx.x43,src_int=internal,dst_int=extern al,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 | # | | Cl | neck List Item | | | RI | ISK | |
|--|-------------------|--------------------------|---|--|---------|--|---------|--------|-----|-----|--|
| | X | | 24 | | e addr | om a system using a ess ranges : 10.0.0. C 1918) | | | I | H | |
| | of Non oliance | IP Spo | oofing | to start denial of ser | rvice a | ttempts or send ma | licious | codes. | | | |
| ProcedureCheck the Firewall EXT>INT ruleset for the specific policy. From external PC FSAUDIT xxx.xxx.x29 execute command as below: a) hping -S xxx.xxx.x27 -a 10.10.21.21 -p 80 b) hping -S xxx.xxx.x27 -a 172.168.20.20 -p 23 | | | | | | | | | | | |
| Verify | ÿ | - | the al | bove addresses are of gs for the record of | lenied | access. | | | | | |
| Conc | lusion | In co | mplian | ce | | | | | | | |
| Refer | ence | Imple Route 1.1 (S | 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. <u>http://www.sans.org/score/firewallchecklist.php</u> | | | | | | | | |
| | Subject | ive | | Objective | Χ | Evidence | Х | Findiı | ngs | Х | |

date=2004-06-

01,time=09:46:53,device_id=FGT1002801021129,log_id=0001000002,type=traffic,subtype=session,pr i=notice,SN=28808,duration=40,policyid=0,proto=6,service=80/tcp**status=deny,src=172.16.20.20**,src name=172.16.20.20,dst=xxx.xxx.xxx.x27,dstname=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=0.0.00,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,srcn ame=172.16.20.20,dst=xx.xxx.xxx.x27,dstname=xxx.xxx.xxx.x27,src_int=n/a,dst_int=external,sent=0,rc vd=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 | | | |
|--|-------|--------|---------|---|------|--|--|--|
| | Х | | 25 | <i>Reject Outbound traffic containing broadcast addresses and Log event</i> | Н | | | |
| Risk o Comp | | Unwit | ting pa | articipant in Denial of Service Attacks. | | | | |
| ProcedureCheck 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 255.255.255 192.168.22.1 | | | | | | | | |
| Verify | 7 | Check | firewa | all logs to see if the broadcasts are recorded and dropped | | | | |
| Conc | usion | In Cor | mplian | ce | | | | |
| ReferenceNetwork 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, Vers 1.1 (Section 6.3.2. – Attack Tests). Firewall Checklist by Naidu, K. http://www.sans.org/score/firewallchecklist.php | | | | | | | | |
| | Subj | ective | | Objective X Evidence X Findi | | | | |

date=2004-06-03,time=14:39:06,device_id=FGT1002801021129,log_id=

0401000002,type=ids,subtype=prevention,pri=alert,attack_id=109,jsrc=255.255.255.255.255,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=255.255.255.255.255,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 | # | • | Cl | neck List Item | | | RI | ISK |
|--|----------|-------|---------------|--|--------------|----------------------|----------|---------------|-------|-----|
| | Х | | 26 | Interfaces both internetwork-based atta | | nd external must be | e moni | tored for |] | H |
| Risk o Comp | | • | Inab attac | ility to detect misco ility to detect attack ks against web serv ility to detect inside | s that ers). | firewalls legitimate | ely allo | w through (su | ch as | 5 |
| ProcedureLogin to the firewall internal interface 192.168.22.1 using "putty". In the CLI dialo execute the following commands: Fortigate-100 # get nids detection interfaces | | | | | | | ogue | | | |
| Verify | | | | rnal and external is MZ interface is set | | | | | | |
| Concl | usion | In co | mplia | nce | | | | | | |
| Reference Fortinet – Fortigate NIDS Guide. Reference 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 | | | | | | | | | | |
| | Subjecti | ive | | Objective | Х | Evidence | Х | Findi | ngs | Х |

| ₽ 192.168.22.1 - PuTTY | | : |
|--|---------------------|---|
| login as: admin admin0192.168.22.1's password: Type ? for a list of commands. | | |
| | interfaces ^ | |
| Unknown command. Fortigate-100 # get nids detection : internal: On external: On dmz: Off | interface | |
| Fortigate-100 # | | |

| N/A | Pass | Fail | # | | Cl | neck List Item | | | RI | SK |
|--|--|-------|-------|---|---------|---------------------|---------|-------------|----|------|
| | | | | Checksum verifica | tion m | ust be turned ON. | This fe | ature tests | | |
| | Х | | 27 | files passing throug | gh the | Fortigate-100 to ma | ake su | e that they | H | Н |
| | | | | have not been chan | iged in | transit. | | - | | |
| | Risk of Non ComplianceInability to detect malicious changes in data during transit. | | | | | | | | | |
| Proced | lure | - | | e firewall internal in following command | | | | - | | ogue |
| Verify | | Verif | y the | Conclusions: it must | be IP: | ON, TCP: ON, UI | OP: ON | and ICMP:ON | I | |
| Concl | usion | In co | mpli | ance | | | | | | |
| Reference Fortinet – Fortigate NIDS Guide. | | | | | | | | | | |
| | Subje | ctive | | Objective | Х | Evidence | Х | Finding | gs | Х |
| | | | | | | | | | | |



| N/A | Pass | Fail | # | | Cl | neck List Item | | F | RISK |
|--------|---|--------|--------|--|---------|---------------------|---------|-------------------|--------|
| | Х | | 28 | All attack detection detection module u groups. By default | ises ov | er 1000 signatures | | | |
| | Risk of Non ComplianceInability to match and detect patterns of security violations of most common attacks. | | | | | | | nost common netv | vork |
| Proce | dure | - | the we | eb interface: <u>https://</u> List | 192.16 | 8.22.1. Login as ad | dmin. (| Go to NIDS > Det | ection |
| Verify | 7 | All si | gnatur | es must be enabled | | | | \$ | |
| Conc | lusion | In co | omplia | ance. Only a parti | al list | is shown below. | | | |
| Refere | ReferenceFortinet – Fortigate NIDS Guide. Router Security Configuration Guide (SNAC) – NSA Revision Sep, 27, 2002, V 1.1 (Section 5.5 CISCO IOS Intrusion Detection). | | | | | | | Sep, 27, 2002, Vo | ersion |
| | Subje | ctive | | Objective | Х | Evidence | Х | Findings | X |
| | | | | | | | | | • |

| E RTIN | | | <u> </u> |
|----------------|---|----------|--------------|
| System | General Signature List User Defined Signature Lis | t | |
| Firewall | | | 1 |
| User | Signature Group Name | Enable | View Details |
| | backdoor | | Q2 |
| VPN | compromised | | Qa |
| NIDS | ddos | | Qà |
| Detection | dns | V | Qà |
| Prevention | dos | V | Qa |
| | exploit | V | Qa |
| Anti-Virus | finger | V | Qa |
| Web Filter | ftp | v | Qa |
| Email Filter | icmp | V | Qa |
| | imap | | Qa |
| Log&Report | misc-traffic | | Qa |
| | netbios | | Qa |
| | pop2 | | Qa |
| | pop3 | | Qa |
| | | - | ~ |

| N/A | Pass | Fail | # | | Cł | neck List Item | | | RI | SK |
|----------------|--|-------------------|--------|---|----------|---------------------|---------|---------------|-------|-----|
| | Х | | 29 | NIDS attack preve disabled by defaul | dule is | М | Η | | | |
| Risk o Comp | | Inabili access | • • | revent the damage of | either l | by dropping the pac | ckets o | r by blocking | netwo | ork |
| Procee | dure | | | firewall internal into ollowing command | | | | | dialo | gue |
| Verify | 7 | Verify | IDP is | s enabled. | | | | | | |
| Concl | lusion | In co | mplia | nce. | | | | | | |
| Refere | Reference Fortinet – Fortigate NIDS Guide. | | | | | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Х | Findi | ngs | Х |

<u>Fortigate-100 #</u> get nids prevention status IDP: enabled

Fortigate-100 #

| N/A | Pass | Fail | # | | C | heck List Item | | | RISK | |
|----------------|-------|---|---------|-----------------------|-----------|-----------------------|--------|------------------|--------|--|
| | Х | | 30 | All attack prevent | tion si | gnatures must be er | nabled | | | |
| Risk o Comp | | Inabili access | • • | prevent the damage | either | by dropping the pa | ckets | or by blocking n | etwork | |
| Procee | dure | Open the web interface: <u>https://192.168.22.1</u> . Login as admin. Go to NIDS > Prevention | | | | | | | | |
| Verify | | 'Enab are en | | ention' is checked. | Verif | y that all individual | preve | ntion signature | groups | |
| Concl | usion | In Cor | nplian | ce. Only a partial li | ist is sl | nown below. | | | | |
| Refere | ence | Fortin | et – Fo | ortigate NIDS Guid | e. | .9 | | | | |
| Subjective | | | | Objective | Х | Evidence | Х | Finding | gs X | |
| | | | | | | | | | | |

| ystem | Prevention | | | | |
|-----------------------|---------------------------|-----------------------------|----------|----------|----------|
| rewall | 🔽 Enable Preventior | 1 | | | 12 🗖 |
| lser | Signature Abbreviation | Summary | Protocal | Enable | Modify |
| PN | synflood | syn flood attack | TCP | V | S |
| IDS | portscan | port scan attack | TCP | | S |
| | synfrag | syn fragment attack | TCP | V | |
| etection revention | synfin | syn with fin attack | TCP | | |
| | noflag | top with no flag attack | TCP | | |
| nti-Virus | finnoack | fin without ack attack | TCP | | |
| eb Filter | srcsession | source session limit | TCP | 2 | 1 |
| | winnuke | winnuke attack | TCP | 2 | |
| nail Filter | land | top land attack | TCP | V | |
| g&Report | ftpovfl | ftp buffer overflow attack | TCP | V | S |
| | smtpovfl | smtp buffer overflow attack | TCP | V | S |
| | pop3ovfl | pop3 buffer overflow attack | TCP | V | S |
| | url | invalid url attack | TCP | V | |
| | udaflood | ude flood attack | LIDB | | 1207 |

| N/A | Pass | Fail | # | | C | heck List Item | | | RI | SK |
|--|-------|--|--------|---------------------|------------------------------------|----------------------|----------|----------------|-------|----|
| | Х | | 31 | Test ID Preventio | Test ID Prevention is functioning. | | | | | |
| Risk o Comp | | Undet system | | | attack | s resulting Denial o | of Serv | ice and or dam | age t | 0 |
| Procee | lure | From the internal Test PC FSBD 192.168.22.210 execute the following command hping -S 192.168.22.1 –a 255.2555.255 | | | | | | | | |
| Verify | | Check | the ID | OS prevention detec | cts and | prevents and logs | the atta | ack. | | |
| ConclusionIn compliance. IP Spoofing was detected from internal network (IP 19 not belonging to the company's subnet. Requires further investigation Identified Vulnerabilities Finding: - IP Spoofing see Part4: Identified - Summary. | | | | | | igation. See Pa | rt 4: | , | | |
| Reference Fortinet – Fortigate NIDS Guide. | | | | | | | | | | |
| | Subje | | | Objective | Х | Evidence | X | Findir | ngs | Х |

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=255.255.255.255.255, 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=255.255.255.255.255, 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]

| N/A | Pass | Fail | # | | Cl | neck List Item | | | RIS | SK |
|--------|-------------------|----------------|---|----------------------|---------|---------------------|--------|---------------|-------|-------------|
| | Х | | 32 | Content filtering m | ust be | enabled in the fire | wall p | olicy. | Н | [|
| | of Non oliance | | Malicious codes and viruses infecting internal network. Some may create backdoor connections for intruders. | | | | | | | |
| Proce | dure | Login 2. | to the | web interface. Selec | et Fire | wall>Policy>'INT. | EXT'> | > Open (Edit) | Polic | yid |
| Verify | 7 | Antivi use. | Antivirus and Web filter must be enabled and the 'Strict' content profile must be in use. | | | | | | | |
| Conc | lusion | In co | mplia | nce | | | 2 |) | | |
| Refere | ence | Fortin | et – Co | ontent Protection Gu | iide | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Х | Findi | ngs | Х |
| | | | | | | | | | | |
| | | | | | | | | | | - X - X - X |

3.5.0 AV / File Blocking Protection

| חפד | | | | |
|----------|-------------------------|-------------------------|-------|------------|
| Int->Ext | t Int->DMZ DMZ->Int | DMZ->Ext Ext | ->Int | Ext->DMZ |
| | | | | |
| | _ | Eult Pulicy | | |
| | Source | 192_168_22 | - | |
| | Destination | External_All | - | |
| | Schedule | Always | - | |
| | Service | ANY | - | |
| | | | | |
| | Action | ACCEPT | • | |
| | | | | |
| | ✓ NAT | Dynamic IP Pool | | |
| | | Fixed Port | | |
| | | | | |
| | 🗖 Traffic Shaping | Guaranteed Bandwidth | 0 | (KBytes/s) |
| | | Maximum | · | |
| | | Bandwidth | 0 | (KBytes/s) |
| | | Traffic Priority | High | ~ |
| | | | | |
| | Authentication | Remote Users | - | |
| | | , _ | | |
| | Anti-Virus & Web filter | | | |
| | | Chuist | | |
| | Content Profile | Strict | • | |

| N/A | Pass | Fail | # | Check List Item R | | | | | | |
|---------------------------------------|---|--------|---|---|--------|----------------------|-------|----------------|--|---|
| | Х | | 33 | Verify contents of 'Strict Content profile'. This controls how the antivirus protection behaves. | | | | | | - |
| | Risk of Non ComplianceDownloading of infected files or programs containing malicious codes or viruses. | | | | | | | | | |
| Proce | dure | Login | Login as admin at the web Interface. Select firewall> Content Profile>Strict. | | | | | | | |
| Verify | 7 | All op | tions n | nust be selected for | protec | tion, except 'pass f | ragme | nted e-mails'. | | |
| Conc | lusion | In Co | mplia | ince | | | | | | |
| Refere | ence | Fortin | Fortinet – Content Protection Guide | | | | | | | |
| SubjectiveObjectiveXEvidenceXFindings | | | | | | gs | Х | | | |

| System | Content Profile | | | | | |
|------------------------|------------------------|----------------|----------------|----------------|----------------|--------------|
| Firewall | | | Edit Content I | Profile | | |
| Policy | Profile Name: | trict | | | | |
| Address | Options | НТТР | FTP | IMAP | РОРЗ | SMTP |
| Service Schedule | Anti Virus Scan | V | v | V | v | v |
| Schedule Virtual IP | File Block | V | V | V | V | ~ |
| IP Pool | Web URL Block | | | | | |
| P/Mac Binding | Web Content Block | <u>।</u> | | | | |
| Content Profile | Web Script Filter | <u>।</u> | | | | |
| Jser | | | | | | |
| /PN | Web Exempt List | | | | | |
| ITDO | Email Block List | | | | | |
| JIDS | Email Exempt List | | | | V | V |
| nti-Virus | Email Content Block | | | V | V | V |
| Veb Filter | Oversized File/Email | • block O pass | I block O pass | ● block ○ pass | ● block ● pass | block O pas: |
| mail Filter | Pass Fragmented Emails | | | | | |

| N/A | Pass | Fail | # | | Ch | eck List Item | | | RI | SK |
|--------|--|--|---------|---|----------|---------------|---|--------|-----|----|
| | Х | | 34 | File blocking must potential threat and computer virus atta | l to pro | | | - | ł | ł |
| | of Non pliance Downloading of infected files or programs containing malicious codes or viruses. | | | | | | | | | |
| Proce | dure | Login to the web interface as admin. Select: Antivirus>File Block. | | | | | | | | |
| Verify | 7 | | | ith .doc, .ppt, .xl ext P protocols. All othe | | | | | | |
| Conc | lusion | In co | mplia | nce. | | | | | | |
| Refere | ence | Fortin | et – Co | ontent Protection Gu | iide | | | | | |
| | Subj | ective | | Objective | Х | Evidence | Х | Findir | ngs | Х |
| | Subjective X Evidence X Findings | | | | | | | | | |

| ystem | File Block | | | | | | |
|-------------|------------|----------|----------|----------|----------|----------|--------|
| irewall | Pattern | НТТР | FTP | IMAP | РОРЗ | SMTP | Modify |
| ser | *.bat | Ø | Ø | Ø | Ø | S | 💼 🔊 |
| sei | *.com | Ø | Ø | O | O | Ø | 💼 🔊 |
| PN | *.dll | O | Ø | O | Ø | O | 💼 🔊 |
| TRO | *.doc | 8 | 8 | 8 | 8 | 8 | 💼 🔊 |
| IDS | *.exe | Ø | 0 | O | 0 | O | 💼 🔊 |
| nti-Virus | *.gz | O | 0 | O | 0 | O | 💼 🔊 |
| ile Block | *.hta | Ø | Ø | O | O | O | 💼 🔊 |
| onfig | *.ppt | 8 | 8 | 8 | | 8 | 💼 🔊 |
| | *.rar | Ø | Ø | O | Ø | O | 💼 🔊 |
| /eb Filter | *.scr | Ø | Ø | O | O | O | 💼 🔊 |
| mail Filter | *.tar | Ø | Ø | O | O | O | 1 🔊 |
| | *.tgz | Ø | 0 | O | Ø | O | 1 🔊 |
| og&Report | *.vb? | Ø | Ø | O | Ø | O | 1 🔊 |
| | *.wps | Ø | Ø | O | Ø | O | 💼 🔊 |
| | *.xl? | 8 | 8 | 8 | | 8 | 💼 🔊 |
| | *.zip | Ø | O | O | O | O | 💼 🔊 |

| | | - | | | | | | | | |
|----------------|-------|--------|--|--------------------|----------------------------------|---------------------|-------|---|-------|----|
| | | | | | | | | | | |
| N/A | Pass | Fail | # | | Cl | neck List Item | | | RI | SK |
| | Х | | 35 | Test File blocking | est File blocking functionality. | | | | | Η |
| Risk o Comp | | Down | Downloading of files or programs containing malicious codes or viruses. | | | | | | | |
| Procee | dure | | From any internal PC browse to http://www.winzip.com and attempt to download a trail version of winzip.exe | | | | | | trail | |
| Verify | , | The do | own lo | ad must be blocked | with a | security alert mess | sage. | | | |
| Concl | usion | | In compliance. The log has also recorded zip files that were blocked with the destination information. | | | | | | | 1 |
| Refere | ence | Fortin | Fortinet – Content Protection Guide | | | | | | | |
| | Subj | ective | cctive Objective X Evidence X Findings X | | | | | Х | | |
| | | | | | | | | | | |

| 🚳 http://download.winzip.com/winzip90.exe - Microsoft Internet Explorer | |
|---|----------------|
| File Edit View Favorites Tools Help | |
| ↔ Back • → → ③ 😰 🏠 @ Search 📾 Favorites @ Media 🎯 🖏 • 🎒 | |
| Address 🕘 http://download.winzip.com/winzip90.exe | ▼ 🖓 Go Links ≫ |
| | <u> </u> |

High security alert!!!

You are not permitted to download the file "winzip90.exe".

 ${\rm URL} = {\rm http://download.winzip.com/winzip90.exe}$

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 | 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 | Increased cot 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 Po | licy, Acceptable U | se Polic | у. | \$0 | | | |
| Description | co co du | 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 | La | Lack of base line and no accountability. | | | | | | |
| Audit Finding | Finding - | | | | | | | |
| Recommendatio | a s gro po Gu | structure. Vulnerab bunds for the choic licies that meet the | ility ass e of pol needs | essments and risk | | | | |
| Cost | NI | | | | | | | |
| References | <u>htt</u> | Importance of Corporate Policy: <u>http://securityresponse.symantec.com/avcenter/security/Content/security</u> .articles/corp.security.policy.html | | | | | | |
| Compensating Controls | - | - 43 | | | | | | |

| Vulnerability | 2 | Checklist Item # | 1.a | Risk (Not Implementing) | High | | |
|-------------------------------|-------------------------------|--|--------|--|-------------------|--|--|
| Only FW admin administration. | istrator and | other authorized | person | nel will be granted acc | ess to the FW for | | |
| | | | | nce, it is recommended the recommended the recommended the recommendation of the | | | |
| Description | ne | | | ators access the router, level of administrator, or | 2 | | |
| Threat | | pendence on only jectives. | one ad | ministrator affects Real-t | ime Recovery | | |
| Audit Finding | | <u>rt 3: Audit of Fortiga</u> m 1 | 100 - | - Testing, Evidence and Fin | dings Checklist | | |
| Recommendatio | po ad mi mi it is | *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 | Ve | | | n Guide (SNAC) – NSA Logins, Privileges, Pass | | | |
| Cost | NI | | | | | | |
| Compensating Controls | Se | paration of duties. | | | | | |
| | | | | | | | |

| Vulnerability | 3 | Checklist Item # | 1.b | Risk (Not Implementing) | High | | |
|--|----------------------|---|------------------|-----------------------------|-------------------|--|--|
| FW Administration | on allowed o | only from specific tr | usted h | ost. | | | |
| Description | | Ensure that the computer allows administration from only an authenticated host. | | | | | |
| Threat Unauthorized users may compror computers, using the idle or unus time out period (when left unguard password cracking tools. | | | | unused portion or id por | tion of the admin | | |
| Audit Finding | | <u>rt 3: Audit of Fortiga</u> m 1 | <u>ate-100 –</u> | - Testing, Evidence and Fi | ndings_Checklist | | |
| Recommendatio | se to sc Re | 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 | N | L | | | | | |
| Compensating Controls STRONG, Complex Passwords | | | | | | | |

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

| Vulnerability | 5 | Checklist Item # | 10 | Risk (Not Implementing) | Medium | | | |
|--|--|---|----|-----------------------------|---------|--|--|--|
| 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. | | | | | | | | |
| 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 | nces Patches and Updates: http://msdn.microsoft.com/library/default.asp?url=/library/en- us/dnnetsec/html/thcmch15.asp | | | | ary/en- | | | |
| Cost | N | NIL | | | | | | |
| Compensating Controls | LC | LOGS. Frequent review of logs | | | | | | |

| Vulnerability | 6 | Checklist Item # | 13 | Risk (Not Implementing) | Medium | | |
|--|---|--|----|-----------------------------|----------------------|--|--|
| Reject the following non-required, risky protocols and services in either direction. | | | | | | | |
| 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 | Finding Part 3: Audit of Fortigate-100 – Testing, Evidence and Findings Checklist | | | | indings Checklist 13 | | |
| Recommendation | | Define a policy on required external services for internal users. Explicity 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 | | |
|---|--|---|----|-----------------------------|-----|--|--|
| Reject Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Log Event. | | | | | | | |
| 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: <u>http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp</u> | | | | rary/en- | | | |
| Cost | - | -NIL- | | | | | |
| Compensating Controls | ng 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) <u>http://www.sans.org/webcasts/show.php?webcastid=90504</u>
- 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. <u>http://www.sans.org/score/firewallchecklist.php</u>
- Building Your Firewall Rulebase by Lance Spitzner
 <u>http://www.spitzner.net/rules.html</u>
- 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 (<u>http://support.microsoft.com/default.aspx?scid=kb;en-us;829031</u>)
- Microsoft Security Guidance Kit
- Microsoft Patterns and Practices: Improving Web Application Security: Threats and Countermeasures -<u>http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/thcmch15.asp</u>
- Services that router should block.<u>http://www.ja.net/CERT/JANET-CERT/prevention/cisco/local_services.html</u>
- Technical Incursion Countermeasures: FAQ Network Intrusion Detection Systems <u>http://www.ticm.com/kb/faq/idsfaq.html</u>)
- CISA Review Manual 2003.

- COBIT QuickStart, COBIT http://www.isaca.org/cobit
- OCTAVE[®]-S Operationally Critical Threat, Asset, and Vulnerability Evaluation, Version 0.9: <u>http://www.cert.org/octave</u>
- Security Self-Assessment Guide NIST special Publication 800-26.
- NIST Computer Security Resource Center web site at the URL: <u>http://csrc.nist.gov</u>
- Fortinet / Fortgate Command Line Interface Reference Guide
- Fortinet / Fortigate 100 NIDS Guide
- Fortinet / Fortigate 100 Content Protection Guide
- Computerworld (<u>http://www.computerworld.com/networkingtopics/networking/story/0,1</u> 0801,65366,00.html)
- Search Engines <u>http://www.google.com</u>