



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

## Interested in learning more?

Check out the list of upcoming events offering  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gsna>

# **An Administrator's Report on Auditing a LEAF (Linux Embedded Appliance Firewall) System**

**SANS GSNA**  
**Practical Assignment Version 2.1**  
**Option 1, From an Administrator's Perspective**

Prepared by Brian Credeur  
September 20, 2002

# Table of Contents

<b><u>ASSIGNMENT 1 – RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL</u></b>	<b><u>1</u></b>
OVERVIEW	1
SYSTEM TO BE AUDITED	1
NETWORK DIAGRAM	1
FIREWALL SYSTEM CONFIGURATION	2
RISK	3
CURRENT STATE OF PRACTICE	5
<b><u>ASSIGNMENT 2 – CREATE AN AUDIT CHECKLIST</u></b>	<b><u>6</u></b>
OVERVIEW	6
NETWORK SECURITY POLICY	6
SYSTEM CHECKLIST	7
FIREWALL RULESET CHECKLIST	12
<b><u>ASSIGNMENT 3 – AUDIT EVIDENCE</u></b>	<b><u>16</u></b>
CONDUCT THE AUDIT	16
FIREWALL SECURITY POLICY	16
SYSTEM CHECKLIST	17
FIREWALL RULESET CHECKLIST	22
MEASURE RESIDUAL RISK	30
IS THE SYSTEM AUDITABLE?	30
<b><u>ASSIGNMENT 4 – RISK ASSESSMENT</u></b>	<b><u>31</u></b>
OVERVIEW	31
SUMMARY	31
AUDIT RESULTS	31
BACKGROUND/RISK	32
FAILED TEST	32
AREAS FOR IMPROVEMENT	32
SYSTEM CHANGES AND FURTHER TESTING	32
IMPROVEMENTS TO ELEMENTS TESTED BY RC7 AND RC11	32
SYSTEM JUSTIFICATION	37
FAILED TEST SC10	37
<b><u>REFERENCES</u></b>	<b><u>37</u></b>

# **An Administrator's Report on Auditing a LEAF (Linux Embedded Appliance Firewall) System**

## **Assignment 1 – Research in Audit, Measurement Practice, and Control**

### **Overview**

Our company, BDC Enterprises, is a small organization with less than 25 employees. We are connected to the Internet through an always-on, Asymmetrical Digital Subscriber Line (ADSL) service. Our Internet Service Provider has allocated a small block of eight (8) publicly routable IP addresses. Of those eight IP addresses, one is used for subnet identification, one is used for subnet broadcast, and one is used for the default gateway at the ISP. This leaves five (5) addresses that we may use to setup as servers or other publicly accessible computer systems.

We have a firewall that controls access to three distinct networks, the Outside Network (Public Internet), our Screened Network (DMZ), and our Local Network (or Internal Corporate Network). There are network services such as web and email that we make available to the public Internet as well as our local computer systems. What follows in this document are a detail of the audit definition, preparation, and execution and a risk analysis of the findings from the audit.

### **System to be Audited**

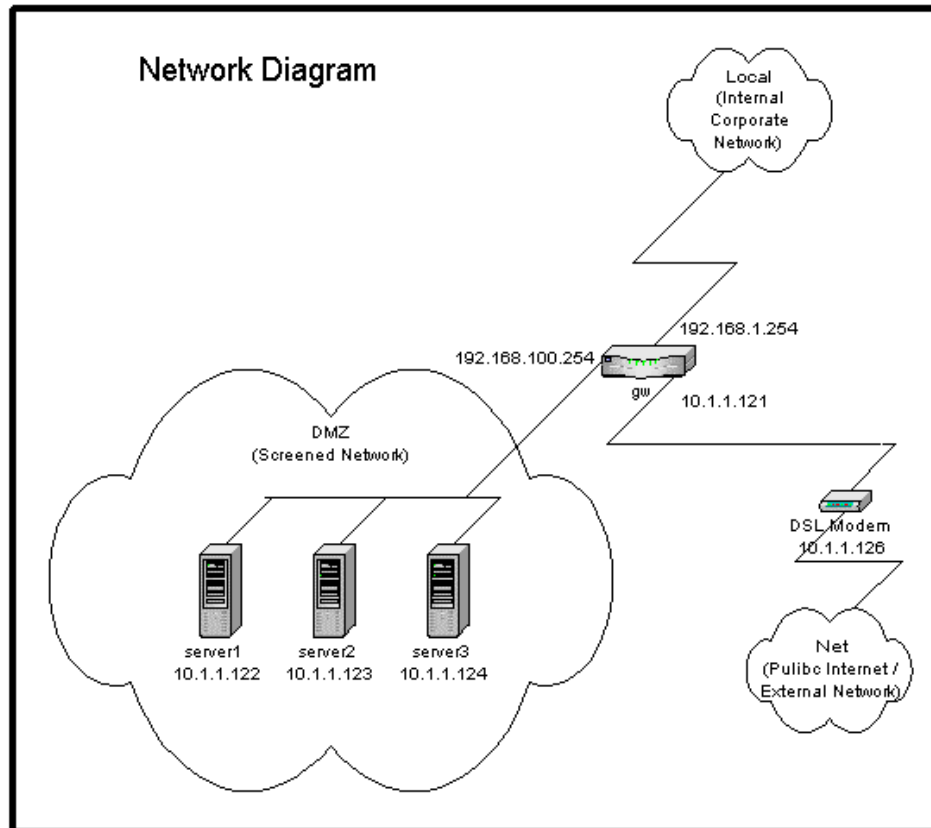
The computer system, 'gw', serves as an Internet gateway and firewall. A fundamental mechanism in the security of our company network, the firewall controls access between three distinct networks. Those networks are defined as:

Net	Public Internet or Outside Network
Local	Internal Corporate Network or Inside Network
DMZ	Screened Network or DMZ

This firewall is a production system, designed to implement our Security Policy, as it pertains to network connectivity and system accessibility.

### **Network Diagram**

The following diagram illustrates the logical network placement of the firewall, 'gw', and the different networks that it interconnects.



Please note that the IP addresses in the 10.1.1.0 network represent the real, public IP addresses. I have changed them to 10.1.1.0 addresses for security purposes in this paper.

## Firewall System Configuration

### Hardware Components of 'gw':

<b>CPU</b>	Intel Pentium, 133MHz
<b>RAM</b>	64MB EDO
<b>Video Card</b>	4MB VLB video card
<b>Network Card #1</b>	10/100 Ethernet
<b>Network Card #2</b>	10/100 Ethernet
<b>Network Card #3</b>	10/100 Ethernet
<b>Floppy Disk Drive</b>	3.5-in. 1.44MB Drive
<b>Hard Disk Drive</b>	NONE

### Software Components of 'gw':

<b>Operating System</b>	LEAF (Linux Embedded Application Firewall) Bering 1.0-rc3 distribution Linux 2.4.18 kernel
<b>Firewall Package</b>	Shorewall 1.3.7
<b>Additional Package</b>	Weblet: Small, read-only web server to view system info
<b>Additional Package</b>	Cmu-snmp: SNMP agent

The LEAF Bering distribution is the product of an open-source project which can be browsed at <http://leaf.sourceforge.net/>. The LEAF distributions are based upon technologies developed under the Linux Router Project (LRP). According to the LRP website, LRP is a "networking-centric micro-

distribution of Linux”<sup>1</sup>. More information on LRP may be found there well as the LEAF website. By leveraging the networking capabilities of the Linux kernel, including the routing, firewalling, and traffic shaping features and producing a very small, distribution footprint, secure systems can be created based upon this technology.

The Shoreline Firewall, commonly called “Shorewall”, is based upon iptables. Iptables is a kernel-level firewall subsystem that is used to implement stateless and stateful packet filtering. The Shorewall package contains a rule-generation engine, control scripts, and multiple configuration files. When the Shorewall is started, the configuration files are read and used by the rule-generation engine to establish packet filtering iptables rules, additional network interface configurations, traffic shaping rules, and more. For more information on the Shoreline Firewall, you may visit their homepage at <http://www.shorewall.net/>.

LEAF settings and configurations are performed from a text-based menu system. Additional LEAF packages that are installed, such as the Shorewall are seamlessly plugged into the menu system.

The implementation of LEAF on ‘gw’ boots and loads the complete operating system, applications, and configurations into a RAM disk (a storage area created by allocating a section of system memory and mounting it in the same way a hard disk would be used) from a single floppy diskette. As the LEAF system boots, the Linux kernel is loaded and the RAM disk is created. Then, specified packages are expanded into the RAM disk and activated via initialization scripts. The Shorewall components and configuration are contained in a single package stored on this same diskette, as are the weblet and cmu-snmp packages.

The floppy diskette is the only form of persistent storage for this system. This is a nice security feature as the floppy can be write-protected and the only way to disable the write-protection is to physically move the switch on the diskette. Therefore, when modifications need to be saved, the write-protection can be disabled on the floppy, changes may be written, and the floppy switched back to write-protected mode. In this fashion, system or configuration modifications can be kept persistent while a remote attacker can only modify the volatile data on the RAM disk. A reset of the system will cause it to reboot to the state that was last saved to the floppy diskette.

## **Risk**

The firewall is used to separate the Public network from the local, untrusted DMZ network from the trusted local, trusted corporate network. The firewall controls traffic between these distinct networks and logs using a configuration and ruleset with the intention of implementing the corporate Network Security Policy. Failure of the firewall either through mis-configuration or lack of capability to implement the Network Security Policy, or shortcomings in the policy, itself, represent identifiable risks to BDC Enterprises.

The following tables categorize and enumerate the risks associated with weaknesses in the firewall implementation. Including both technical and business concerns.

### **Risks to Firewall System**

<b>Category</b>	<b>Risk</b>	<b>Likelihood</b>	<b>Severity</b>	<b>Consequences</b>
Denial of Service	Network gateway unable to communicate with Internet	Medium	High	Customer web sites will not be accessible Internal users and DMZ hosts will not be able to access Internet Corporate E-mail loss or delays
System Compromise	Attacker is able to gain shell access on the firewall and/or execute arbitrary code	Low	High	Exposes internal and DMZ networks to Internet

<sup>1</sup> “Linux Router Project” URL <http://www.linuxrouter.org/>, September 2, 2001.

				Network and host information on firewall may be used for further attacks
Mis-configuration	Unintentional oversight in firewall configuration or rule set	Low-Medium	Medium-High	May expose internal and/or DMZ networks to Internet Network and host information on firewall may be viewable from Internet Firewall and/or system logs may be lost

### Risks to DMZ Systems

Category	Risk	Likelihood	Severity	Consequences
Denial of Service	One or more public servers are unable to communicate with Internet and/or local networks	Medium	Medium-High	Customer web sites will not be accessible Internal users and DMZ hosts will not be able to access Internet Corporate E-mail loss or delays
System Compromise	Attacker is able to gain access and/or control on one or more public servers and/or execute arbitrary code	Medium	Medium-High	Exposes system information to attacker Network and host information on server may be used for further attacks System may be used as point-of-attack for other systems on our network or others'
Information Compromise	Attacker is able access data that should be otherwise restricted	Medium	Medium-High	Public and/or sensitive information may be lost, leaked, or corrupted

### Risks to Internal Systems

Category	Risk	Likelihood	Severity	Consequences
Denial of Service	One or more internal systems are unable to communicate with Internet and/or local networks	Low-Medium	Medium	Users' productivity may be adversely affected.
System Compromise	Attacker is able to gain access and/or control on one or more internal systems and/or execute arbitrary code	Low-Medium	High	Exposes system information to attacker Network and host information on server may be used for further attacks System may be used as point-of-attack for other systems on our network or others'
Information Compromise	Attacker is able access data that should be otherwise restricted	Low-Medium	High	Public, sensitive, and/or confidential information

---

may be lost, leaked, or corrupted

---

### General Business Risks

Category	Risk	Likelihood	Severity	Consequences
External Threats	Attacks on the Company Network by people outside of the network	Medium-High	Medium-High	Negatively affect productivity, service offerings, etc. Defacement of website or adverse effect on company reputation Leakage, corruption, or loss of company assets Loss of client confidence or business
Internal Threats	Attempts by internal users to circumvent the firewall Internal users may seek to gain access to resources denied them by the firewall (which reflects the Network Security Policy, Acceptable Usage Policy, etc.)	Medium	Medium-High	Damage may range from decreased individual productivity to the channeling of critical company information to the outside

### Current State of Practice

A large number of resources exist in the area of auditing firewalls, in general, though there is no material on auditing a LEAF system, specifically. I took aspects from various sources to compile the checklist and audit procedures that are detailed in Assignment 2 and Assignment 3.

The System and Ruleset Checks detailed in Assignment 2 are comprised of control objectives that would be applicable to any type of firewall system. The control objectives for these checks were derived from research in auditing firewalls, in general. To more accurately test specific platform that is the LEAF system, it was necessary to tailor some of the actual test steps to that platform. Also, as LEAF is a based upon the Linux kernel, consideration was also given to the generalized category of a Linux-based firewall.

Resources for the more general firewall auditing techniques and procedures were:

- SANS Institute Course Material
- SANS Institute Forums and Reading Room
- ICSA Labs Firewall Community
- CERT
- CERIAS

Resources for the more LEAF- or Linux- specific auditing techniques and procedures were:

- The LEAF Project
- The Linux Router Project
- The Shoreline Firewall
- "The Linux System Administrator's Guide"
- "Linux Administrator's Security Guide"

References for these resources are found in the References section at the end of this document.

Tools used in conducting the tests in Assignment 3 were:

- Nessus <http://www.nessus.org/>
- Nmap <http://www.nmap.org/>

Hping2	<a href="http://www.hping.org/">http://www.hping.org/</a>
Snort IDS	<a href="http://www.snort.org/">http://www.snort.org/</a>
Tcpdump	<a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a>

## Assignment 2 – Create an Audit Checklist

### Overview

A checklist has been created to audit the LEAF system, 'gw'. As an administrator of the system, I had access to Network Security Policy and had intimate knowledge of the system and its configuration. The checklist that follows is divided into two areas of testing. The System Check (SC) items validate the firewall system by auditing the capabilities, configuration, operation, and maintenance of the system. The Ruleset Check (RC) items validate firewall system by auditing the functionality of the firewall ruleset, as implemented, with active network probes and referencing those with the Network Security Policy.

The scope of the audit is tightly focused on the security of firewall system, itself, and the ruleset that it implements with respect to the Network Security Policy. Though there are many more aspects to a full network security audit and though that is in-turn only a sub-set of an overall information system or company security audit, the scope of this audit does not include those areas. By focusing on the firewall system, the configuration and maintenance of the system, and the ability of the system to accurately implement the relevant areas of the Network Security Policy through a ruleset, the scope such that understanding of the subject and auditing process may be demonstrated.

### Network Security Policy

Security controls must be implemented to allow all inter-communication between the Internet and company networks (Internal Corporate Network as well as any Screened Networks that are within direct control of the company), but must prevent unauthorized access to network resources. The following sections detail what access to network resources is to be allowed.

#### Internet Access

Internal systems may access the Internet only through an approved Internet gateway. An approved Internet gateway may technically consist of more than one system for the sake of load-balancing, redundancy, or high-availability. All Internet gateways must have access controls compliant with this Network Security Policy. The Chief Information Security Officer must approve an Internet gateway prior to its being put into production.

#### Screened Network (DMZ)

In order to provide public network services, a set of systems will necessarily be designated for public accessibility. All publicly accessible servers must be placed in a screened network. A screened network must be segmented from the internal, corporate network and access controls must be implemented to restrict access to internal, corporate network resources from systems in this screened network.

All systems in a screened network must have network access controls to prevent unauthorized access from other systems in the same network.

#### Internal Network (Corporate Network)

Workstations, print servers, development computers, and other systems used for corporate business may be connected to the Internal Network. Systems connected to the internal network must not be simultaneously connected to any other network.

Virus-scanning software with current detection methods must be installed and active on all systems in the internal network for which such software is available. The Chief Information Security Office must approve any exceptions before a system can be connected to this network.

## Access to Network Resources

A detailed list of which network resources are accessible from which networks or systems must be kept current. This detailed list will be contained in a document titled "Accessible Network Resources". The Chief Information Security Office must approve any changes to this document. Any systems found in violation of this list must be immediately disconnected from any network.

## Access-Control System Requirements

Firewalls and other access control systems must be kept current with information security industry standards. Access control systems on general-purpose systems must log suspect or erroneous activity to disk. Access control systems on dedicated systems, such as a firewall or intrusion detection system must log to or send reports to another system within the internal network.

## Network and Console Logins

All systems connected to a local network (Internal or Screened), are required to request user authentication in order to login to the system. Screensavers or similar mechanisms to lock the desktop and request user authentication must be configured to active within 15 minutes of console idleness. It is suggested that users logoff or manually lock the desktop when leaving the work area.

## System Checklist

Identifiers are used to uniquely label each test. There the tests have been divided into two distinct categories, System Checks (SC) and Firewall Ruleset Checks (RC). The details of the tests in these categories follow.

<b>Identifier</b>	<b>SC1</b>
<b>Control Objective</b>	Test for unnecessary processes running on the firewall.
<b>Reference</b>	"Linux Administrator's Security Guide" and personal experience
<b>Risk</b>	Description: Unnecessary processes may consume system resources and, thus, adversely affect the performance of the firewall. Additionally, unnecessary processes may be services that open the firewall to local and/or remote exploits. Importance: medium-high Likelihood: low-medium
<b>Compliance</b>	Review the process table output for user processes that are superfluous to the operation and usage of the firewall
<b>Testing</b>	ps auxww > /tmp/test_sc1.txt
<b>Objective/Subjective</b>	This is somewhat subjective. It takes a high-level of knowledge of the services and applications that are needed for the operation and usage of the firewall as well as a critical perspective of what processes are deemed "necessary". It is recommended that experienced personnel agree upon what the "necessary" processes are and that a baseline document is created. A document such as this would then make the test objective.

<b>Identifier</b>	<b>SC2</b>
<b>Control Objective</b>	Test for unnecessary sockets listening on the firewall.
<b>Reference</b>	"Linux Administrator's Security Guide" and personal experience
<b>Risk</b>	Description: Unnecessary listeners represent services that may open the firewall to local and/or remote exploits. Importance: medium-high Likelihood: low-medium
<b>Compliance</b>	Review the network socket output for listeners that are superfluous to the operation and usage of the firewall
<b>Testing</b>	cd /proc/net cat tcp > /tmp/test_sc2a.txt

	cat udp > /tmp/test_sc2b.txt cat raw > /tmp/test_sc2c.txt
<b>Objective/Subjective</b>	This is somewhat subjective. It takes a high-level of knowledge of the services that are needed for the operation and usage of the firewall as well as a critical perspective of what services are deemed “necessary”. It is recommended that experienced personnel agree upon what the “necessary” services are and that a baseline document is created. A document such as this would then make the test objective.

<b>Identifier</b>	<b>SC3</b>
<b>Control Objective</b>	Test for system and firewall local logging.
<b>Reference</b>	“Linux Administrator’s Security Guide” and personal experience
<b>Risk</b>	Description: System- and firewall- related events should be logged to a local filesystem to provide important information to administrators. Without live system and firewall information, the ability to detect attacks and troubleshoot issues becomes very difficult. Local logging is desirable in case there is an issue with logging to a remote system (i.e., network outage, remote system is down, ...). Importance: high Likelihood: low-medium
<b>Compliance</b>	Review the output to verify that messages are being logged to a local filesystem in real-time.
<b>Testing</b>	cat /etc/syslog.conf > /tmp/test_sc3a.txt logger -t TESTMSG “Testing local system logging” grep ‘<firewall> kernel:’ /var/log/messages > \ /tmp/test_sc3b.txt grep ‘<firewall>.<domainname> TESTMSG:’ /var/log/messages > \ /tmp/test_sc3c.txt
<b>Objective/Subjective</b>	This is objective. Either the logfile is configured to be used and it contains the logging information, or not.

<b>Identifier</b>	<b>SC4</b>
<b>Control Objective</b>	Test for system and firewall remote logging.
<b>Reference</b>	“Linux Administrator’s Security Guide” and personal experience
<b>Risk</b>	Description: System- and firewall- related events should be logged to a remote loghost to provide important information to administrators. Without live system and firewall information, the ability to detect attacks and troubleshoot issues becomes very difficult. Remote logging is desirable in case such as when the local filesystem is full or the system has been compromised and local files may be modified. Importance: high Likelihood: low-medium
<b>Compliance</b>	Review the output to verify that messages are being logged to a remote loghost in real-time.
<b>Testing</b>	cat /etc/syslog.conf > /tmp/test_sc4a.txt logger -t TESTMSG “Testing remote system logging” On remote system: grep ‘<firewall> kernel:’ /var/log/messages > \ /tmp/test_sc4b.txt grep ‘<firewall>.<domainname> TESTMSG:’ /var/log/messages > \ /tmp/test_sc4c.txt
<b>Objective/Subjective</b>	This is objective. Either the logfile is configured to be used and it contains the logging information, or not. NOTE: There may be a configuration issue on the remote loghost preventing the log messages from being display. If the firewall is properly configured, but the remote

	loghost is not, then the test is still failed.
--	--

<b>Identifier</b>	<b>SC5</b>
<b>Control Objective</b>	Test that user authentication is required for console login.
<b>Reference</b>	ISCA Labs Firewall Certification Criteria 4.0, Baseline Module, Administration, AD3
<b>Risk</b>	Description: Uncontrolled access to the firewall configuration could result in accidental or intentional tampering or an information compromise. An attacker could change the network settings or rulesets on the firewall, rendering the firewall ineffective. Also, sensitive information about networks, hosts, services, etc. that are contained within the firewalls settings and rulesets may be gathered. Importance: high Likelihood: low-medium
<b>Compliance</b>	Visual inspection of the system console.
<b>Testing</b>	Verify that a terminal session requires a user to authenticate before being able to access system information or being able to configure the system.
<b>Objective/Subjective</b>	This is objective. Either the firewall system console requires a user to login or not.

<b>Identifier</b>	<b>SC6</b>
<b>Control Objective</b>	Test that user authentication is non-trivial.
<b>Reference</b>	"Linux Administrator's Security Guide" and personal experience
<b>Risk</b>	Description: Weak authentication can allow easy access to the firewall configuration and could result in tampering or an information compromise. An attacker could change the network settings or rulesets on the firewall, rendering the firewall ineffective. Also, sensitive information about networks, hosts, services, etc. that are contained within the firewalls settings and rulesets may be gathered. Importance: high Likelihood: low-medium
<b>Compliance</b>	This test is failed if any of these trivial attempts yield a successful login.
<b>Testing</b>	Attempt to login with blank login and password Attempt to login as 'root' with blank password Attempt to login as 'root' with other trivial passwords ('root', 'gw', 'password', 'secret', ...)
<b>Objective/Subjective</b>	This is objective. Either the firewall system console requires a user to login or not.

<b>Identifier</b>	<b>SC7</b>
<b>Control Objective</b>	Test that failed logins are logged.
<b>Reference</b>	ISCA Labs Firewall Certification Criteria 4.0, Baseline Module, Logging, LO2 and personal experience
<b>Risk</b>	Description: Administrators need to be able to know if someone has attempted to login to the system. Failed logins could indicate an attack to gain access to the system. Importance: high Likelihood: low-medium
<b>Compliance</b>	Review output to verify that the failed login attempts are shown.
<b>Testing</b>	cat /etc/syslog.conf > /tmp/test_sc7a.txt On the firewall: grep '<firewall> login' /var/log/auth.log > \ /tmp/test_sc7b.txt On the remote loghost: grep '<firewall>.<domainname> login' /var/log/messages > \

	/tmp/test_sc7c.txt NOTES: <ul style="list-style-type: none"> <li>- The failed login attempts from SC6 should be shown, here.</li> <li>- The logfile may be different (for example, /var/log/auth.log or /var/log/messages), depending on the syslog configuration.</li> <li>- The local and remote logs should both contain the messages</li> </ul>
<b>Objective/Subjective</b>	This is objective. Either the messages are logged or they are not.

<b>Identifier</b>	<b>SC8</b>
<b>Control Objective</b>	Test that successful logins are logged.
<b>Reference</b>	ISCA Labs Firewall Certification Criteria 4.0, Baseline Module, Logging, LO2 and personal experience
<b>Risk</b>	Description: Administrators need to be able to know if/when someone has successfully logged-in to the systems. The ability to track user activity helps identify changes that may not be logged in the change log and to provide an audit trail for suspicious activity. Importance: high Likelihood: low-medium
<b>Compliance</b>	Review output to verify that the successful logins are shown.
<b>Testing</b>	Login (or have an administrator login) to the system cat /etc/syslog.conf > /tmp/test_sc8a.txt On the firewall: grep '<firewall> login' /var/log/auth.log > \ /tmp/test_sc8b.txt On the remote loghost: grep '<firewall>.<domainname> login:' /var/log/messages > \ /tmp/test_sc8c.txt NOTES: <ul style="list-style-type: none"> <li>- The logfile may be different (for example, /var/log/auth.log or /var/log/messages), depending on the syslog configuration.</li> <li>- The local and remote logs should both contain the messages.</li> </ul>
<b>Objective/Subjective</b>	This is objective. Either the messages are logged or they are not.

<b>Identifier</b>	<b>SC9</b>
<b>Control Objective</b>	Test that when the system boots it maintains either a closed or active firewall configuration throughout.
<b>Reference</b>	ISCA Labs Firewall Certification Criteria 4.0, Baseline Module, Persistence, PE1.
<b>Risk</b>	Description: It would pose a security risk if the firewall were to be ineffective, even for a short period of time, at preventing unauthorized access to network resources. If the firewall exposes resources by allowing unauthorized access to network resources, those exposed resources may be attacked. Importance: high Likelihood: medium
<b>Compliance</b>	At no time during a system reset of the firewall should any hosts be able to access restricted network resources.
<b>Testing</b>	Power the firewall off Power the firewall back on Attempt to access resources that should not be accessible while the system is coming up. Example 1: Ping a host in the Screened Network that is running but that should not be accessible from a (Unix) host in the Outside Network:

	<pre>script /tmp/test_sc9a.txt ping &lt;screened_network_host&gt; when the firewall boot sequence is complete: CTRL-C exit</pre> <p>This test is failed if any of the pings are successful. Note the time and duration of the breach in relation to the boot processes of the firewall.</p> <p>Example 2:</p> <p>Attempt to connect to telnet to a host in the Internal Network from a host in the Screened Network that is running but that should not be accessible.</p> <pre>script /tmp/test_sc9b.txt telnet &lt;internal_network_host&gt; repeat the above command until the firewall boot sequence is complete exit</pre> <p>This test is failed if any of the connection attempts are successful. Note the time and duration of the breach in relation to the boot processes of the firewall.</p>
<b>Objective/Subjective</b>	This is objective. Either the protected systems and/or services are accessible or they are not.

<b>Identifier</b>	<b>SC10</b>
<b>Control Objective</b>	Test that idle console sessions are automatically closed.
<b>Reference</b>	ICSA Labs and SANS Reading Room
<b>Risk</b>	<p>Description: In the event that an administrator fails to manually close a system login when not working on the system, someone else would be able to walk-up and reconfigure or gain privileged information from the system.</p> <p>Importance: medium</p> <p>Likelihood: medium-low</p>
<b>Compliance</b>	Verify that the firewall is able to automatically close idle logins.
<b>Testing</b>	<p>Verify that the system has a mechanism to accomplish this. It may be a built-in default or one that is configurable. Either way the system documentation or the settings should state the idleness duration.</p> <p>Have an administrator login to the system and leave a session idle for a duration of time that would exceed the threshold and cause the automatic closure of the session.</p>
<b>Objective/Subjective</b>	This is objective. The system default or configurable setting that controls the time a system will wait before closing an idle session should be easily identified. Likewise, the duration test should prove whether the system closes the session or not.

<b>Identifier</b>	<b>SC11</b>
<b>Control Objective</b>	Test that firewall system backups are being maintained.
<b>Reference</b>	"The Linux System Administrator's Guide", The LEAF web site, SANS Reading Room, and personal experience
<b>Risk</b>	<p>Description: In the event that the boot media becomes damaged or the system hardware becomes unusable, having a backup of the system and/or its configuration can greatly simplify, speed-up, minimize errors in the process of rebuilding the firewall system. Also, regular backups can build a configuration history and can help in reverting to a previous configuration.</p> <p>Importance: medium-high</p>

	Likelihood: medium
<b>Compliance</b>	Verify that the firewall can be backed up and that the administrators maintain a backup routine.
<b>Testing</b>	Interview the administrators to determine if backups are being made and if they are adequately maintained.
<b>Objective/Subjective</b>	This is mostly objective. The ability to backup the system and the existence of backups is objective, however, whether those backups procedures are determined to be adequate or not may be a decision based upon the auditor's experience.

<b>Identifier</b>	<b>SC12</b>
<b>Control Objective</b>	Test that changes to the firewall hardware, software, configuration, and ruleset are being tracked and controlled.
<b>Reference</b>	SANS Reading Room Articles
<b>Risk</b>	Description: New features and security and security updates are released over time. If there are no procedures used to manage system or ruleset changes, then it becomes much more difficult for administrators to maintain awareness of what they are running and what may need to be updated. Additionally, for systems with multiple administrators, a configuration history or log becomes very useful in documenting changes that are made. Importance: medium-high Likelihood: medium
<b>Compliance</b>	Determine whether the change control procedures are being followed.
<b>Testing</b>	Interview the administrators to determine what change control procedures are being followed.
<b>Objective/Subjective</b>	This is mostly objective. The existence of a change history or log is objective, however, whether those configuration management procedures are determined to be adequate for a "controlled" system or not may be a decision based upon the auditor's experience.

### **Firewall Ruleset Checklist**

<b>Identifier</b>	<b>RC1</b>
<b>Control Objective</b>	Test for unapproved access to services on the firewall from the Outside Network.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan the firewall from the Outside Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC2</b>
<b>Control Objective</b>	Test for unapproved access to services in the Screened Network from the Outside Network.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of

	service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan hosts in the Screened Network from the Outside Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC3</b>
<b>Control Objective</b>	Test for unapproved access to services in the Internal Network from the Outside Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan hosts in the Internal Network from the Outside Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC4</b>
<b>Control Objective</b>	Test for ability to circumvent firewall from the Outside Network by spoofing IP source addresses.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: If the firewall can be circumvented in this fashion, then attackers may be able to gain network reconnaissance, generate a denial of service, exploit, or compromise local systems and services. Importance: medium Likelihood: low-medium
<b>Compliance</b>	All packets with spoofed IP source addresses should be prevented from traversing the firewall.
<b>Testing</b>	Setup a packet capturing system to collect packets for a target system in the Screened Network and for a target system in the Internal Network Issue packets from a host on the outside to each of the target systems, using a spoofed source IP address Save the packet captures into test_rc10_dmz.log and test_rc10_int.log, respectively.
<b>Objective/Subjective</b>	This is objective. Either the packets were able to traverse the firewall and were logged by the packet capturing systems or they were not.

<b>Identifier</b>	<b>RC5</b>
<b>Control Objective</b>	Test for unapproved access to services on the firewall from the Screened Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high

	Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan the firewall from the Screened Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC6</b>
<b>Control Objective</b>	Test for unapproved access to services in the Internal Network from the Screened Network.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan hosts in the Internal Network from the Screened Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC7</b>
<b>Control Objective</b>	Test for unapproved access to services in the Outside Network from the Screened Network.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to Internet systems from local systems may help enable a system to be used for unauthorized purposes or may allow a compromised system to be used for other attacks or a conduit for information leakage. A user logging on to a DMZ host to access an Internet host that is restricted to Corporate hosts. Importance: medium Likelihood: low-medium
<b>Compliance</b>	The accessibility to Internet services must be in compliance with the Network Security Policy
<b>Testing</b>	Review firewall rulesets to determine what systems and services on the Internet hosts from this network are able to access.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC8</b>
<b>Control Objective</b>	Test for ability to circumvent firewall from the Screened Network by spoofing IP source addresses.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: If the firewall can be circumvented in this fashion, then attackers may be able to gain network reconnaissance, generate a denial of service, exploit, or compromise local systems and services. Importance: medium Likelihood: low-medium
<b>Compliance</b>	All packets with spoofed IP source addresses should be prevented from traversing the firewall.

<b>Testing</b>	Setup a packet capturing system to collect packets for a target system in the Internal Network Issue packets from a host in the Screened Network to the target system, using a spoofed source IP address Save the packet captures into test_rc8.log.
<b>Objective/Subjective</b>	This is objective. Either the packets were able to traverse the firewall and were logged by the packet capturing systems or they were not.

<b>Identifier</b>	<b>RC9</b>
<b>Control Objective</b>	Test for unapproved access to services on the firewall from the Internal Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan the firewall from the Internal Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC10</b>
<b>Control Objective</b>	Test for unapproved access to services in the Screened Network from the Internal Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Testing</b>	Portscan hosts in the Screened Network from the Internal Network, using a network IDS, packet capture system, and/or the firewall logs to correlate the scan results.
<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.

<b>Identifier</b>	<b>RC11</b>
<b>Control Objective</b>	Test for unapproved access to services in the Outside Network from the Internal Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to Internet systems from local systems may help enable a system to be used for unauthorized purposes or may allow a compromised system to be used for other attacks or a conduit for information leakage. Importance: medium Likelihood: low-medium
<b>Compliance</b>	The accessibility to Internet services must be in compliance with the Network Security Policy
<b>Testing</b>	Review firewall rulesets to determine what systems and services on the Internet hosts from this network are able to access.

<b>Objective/Subjective</b>	This is objective. Either the accessible network resources are in compliance with the Network Security Policy or they are not.
<b>Identifier</b>	<b>RC12</b>
<b>Control Objective</b>	Test for ability to circumvent firewall from the Internal Network by spoofing IP source addresses.
<b>Reference</b>	Articles from the SANS Reading Room and personal experience
<b>Risk</b>	Description: If the firewall can be circumvented in this fashion, then attackers may be able to gain network reconnaissance, generate a denial of service, exploit, or compromise local systems and services. Importance: medium Likelihood: low-medium
<b>Compliance</b>	All packets with spoofed IP source addresses should be prevented from traversing the firewall.
<b>Testing</b>	Setup a packet capturing system to collect packets for a target system in the Screened Network Issue packets from a host in the Internal Network to the target system, using a spoofed source IP address Save the packet captures into test_rc12.log.
<b>Objective/Subjective</b>	This is objective. Either the packets were able to traverse the firewall and were logged by the packet capturing systems or they were not.

## Assignment 3 – Audit Evidence

### Conduct the Audit

The checklist from Assignment 2 has been followed and each of the 24 tests has been executed. The following sections outline the firewall security policy—as it is an implementation of the relevant area of the Network Security Policy—and examples showing how 10 of these 24 tests were performed and how the results were interpreted as per the checklist.

### Firewall Security Policy

It is the intention of the firewall system and its security policy is to be a tool for implementing the relevant areas of the Network Security Policy as the “Accessible Network Resources” document. A summary of the firewall security policy follows:

#### Default Policies

Internal hosts may reach any resource in the Outside.

Internal hosts may reach any resource in the DMZ.

DMZ hosts may reach any resource in the Outside.

All resources are denied to the Outside.

All resources are denied to all hosts.

#### Firewall Network Resources

The following services may be reached on the Firewall from the Inside:

From the Inside:	TCP	80
	UDP	161

#### DMZ Network Resources

The following DMZ resources may be reached from the Outside:

Server1 (10.1.1.122):	TCP	21, 22, 25, 80, 81, 554, 3782, 7070, 8080, 18009
	UDP	53, 3783
Server2 (10.1.1.123):	TCP	22, 25, 80
	UDP	53

Server3 (10.1.1.124):      TCP    21, 22, 6767, 8453  
                                 UDP    15121, 15122, 15123

All DMZ resources may be reached from the Inside.

### Internal Network Resources

The following Internal resources may be reached from the DMZ:

Server0 (192.168.1.1):    TCP    25  
                                 UDP    53

The following Internal resources may be reached from the Firewall:

Server0 (192.168.1.1):    TCP    37  
                                 UDP    53, 514

### Internet Access from DMZ Network

The DMZ hosts may reach any Outside resources.

### Internet Access from Internal Network

The Internal hosts may reach any Outside resources.

### Special Cases

ICMP type 8 (used by ping) is allowed as follows:

Firewall -> DMZ  
DMZ -> Firewall  
Local -> DMZ

In all other scenarios, ICMP type 8 is dropped.

### Shorewall Defaults

Shorewall has the following default actions:

Drop the following ports  
                                 UDP    1900  
Reject (instead of drop) the following ports  
                                 TCP    113, 113  
                                 UDP    137, 138, 139, 445

### System Checklist

The firewall has no services running that allow remote shells (such as a telnet or secure shell demon), therefore, to get screen captures from the firewall the output of commands were all redirected to text files. These files were then copied to a floppy diskette and moved over to the system that the firewall remotely logs to. Some of the screenshots are taken of the printing of the files to the terminal window on this remote loghost.

### Test Example #1 - SC1

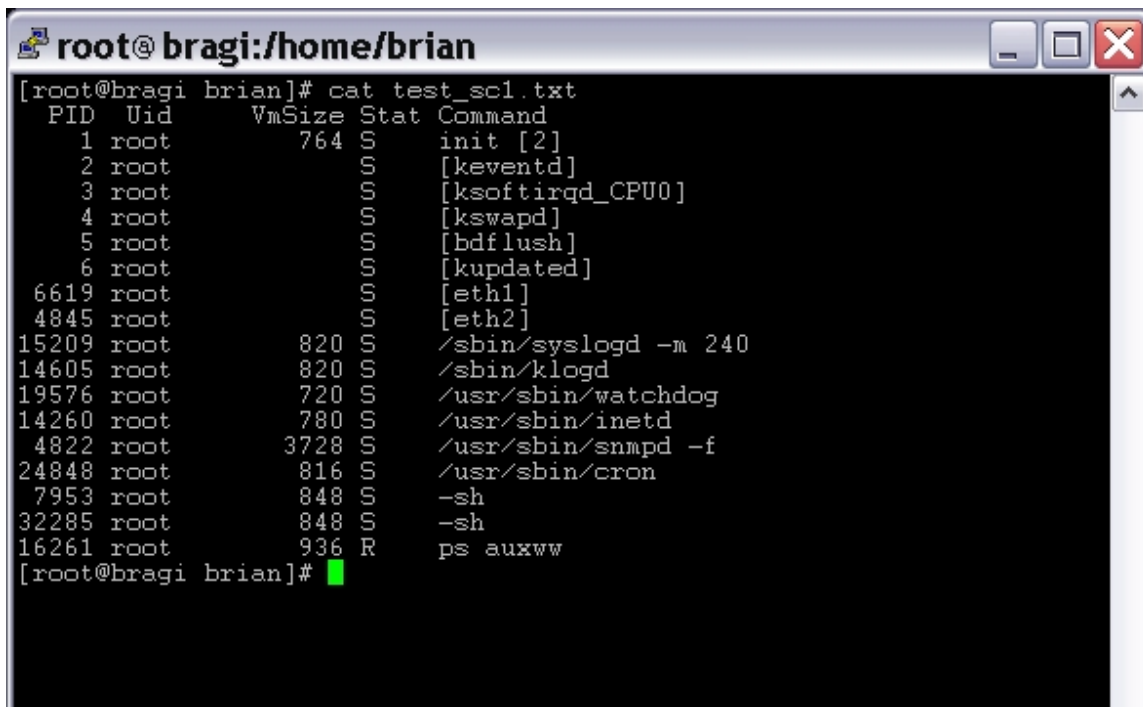
The firewall system passed this test.

All of the sockets that are listening on the firewall are approved.

The only processes that are not on the "necessary" process list for this system are the last three:

```
7953 root      848 S      -sh
32285 root     848 S      -sh
16261 root     936 R      ps auxww
```

These three processes, are incidental and are not of concern. At the time the audit was taking place, there were two concurrent logins to this system. One is the shell process that this test was run from and the other is for another console shell that the administrator was using at this time. The last process listed is the actual command that was run to capture the process table.



```
root@bragi:/home/brian
[root@bragi brian]# cat test_sc1.txt
  PID  Uid    VmSize Stat  Command
    1  root      764   S    init [2]
    2  root         S    [keventd]
    3  root         S    [ksoftirqd_CPU0]
    4  root         S    [kswapd]
    5  root         S    [bdflood]
    6  root         S    [kupdated]
 6619  root         S    [eth1]
4845   root         S    [eth2]
15209  root      820   S    /sbin/syslogd -m 240
14605  root      820   S    /sbin/klogd
19576  root      720   S    /usr/sbin/watchdog
14260  root      780   S    /usr/sbin/inetd
 4822  root     3728   S    /usr/sbin/snmpd -f
24848  root      816   S    /usr/sbin/cron
 7953  root      848   S    -sh
32285  root      848   S    -sh
16261  root      936   R    ps auxww
[root@bragi brian]#
```

## Test Example #2 - SC2

The firewall system passed this test.

All of the sockets that are listening on the firewall are approved.

There are two TCP sockets that are shown to be listening:

- 80 (0x50 in hex) is used by the HTTP service the weblet package provides.
- 1023 (0x3FF in hex) is used to display basic network interface statistics.

There are two UDP sockets that are shown to be listening:

- 161 (0xA1 in hex) is used by the SNMP services the cmu-snmp package provides.
- 514 (0x202 in hex) is the port used for logging system messages.

An empty table for the RAW sockets shows that there are no other protocols besides TCP and UDP that might have sockets listening on this system. NOTE: Other systems with the Linux 2.4 kernel may show IP protocols 0x1 (ICMP) or 0x6 (UDP), as well.

```
root@bragi:/home/brian
[root@bragi brian]# cat test_sc2a.txt
sl local_address rem_address st tx_queue rx_queue tr tm->when ret
rnsmt uid timeout inode
0: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 000
00000 0 0 3910 1 c3f94050 300 0 0 2 -1
1: 00000000:03FF 00000000:0000 0A 00000000:00000000 00:00000000 000
00000 0 0 3911 1 c3f943e0 300 0 0 2 -1
[root@bragi brian]# cat test_sc2b.txt
sl local_address rem_address st tx_queue rx_queue tr tm->when ret
rnsmt uid timeout inode
2: 00000000:0202 00000000:0000 07 00000000:00000000 00:00000000 000
00000 0 0 3850 2 c3cfe3d0
33: 00000000:00A1 00000000:0000 07 00000000:00000000 00:00000000 000
00000 0 0 3944 2 c3f94770
[root@bragi brian]# cat test_sc2c.txt
sl local_address rem_address st tx_queue rx_queue tr tm->when ret
rnsmt uid timeout inode
[root@bragi brian]#
```

### Test Example #3 - SC4

The firewall system passed this test.

The system is logging messages to a remote loghost.

An excerpt from the file 'test\_sc4a.txt', which is a copy of the file 'syslog.conf', shows that the firewall is configured to log to a remote host, 192.168.1.1.

```
*.* @192.168.1.1
```

The screenshot shows that the messages from both the SC3 and SC4 tests were captured in the logfiles on the remote loghost, 192.168.1.1.

```
root@bragi:/home/brian
[root@bragi brian]# grep 'gw.my.domain kernel:' /var/log/messages > /t
mp/test_sc4b.txt
[root@bragi brian]# grep 'gw.my.domain TESTMSG:' /var/log/messages > /
tmp/test_sc4c.txt
[root@bragi brian]# more /tmp/test_sc4c.txt
Sep 15 16:50:08 gw.my.domain TESTMSG: Testing local system logging
Sep 15 16:53:52 gw.my.domain TESTMSG: Testing remote system logging
[root@bragi brian]#
```

### Test Example #4 – SC8

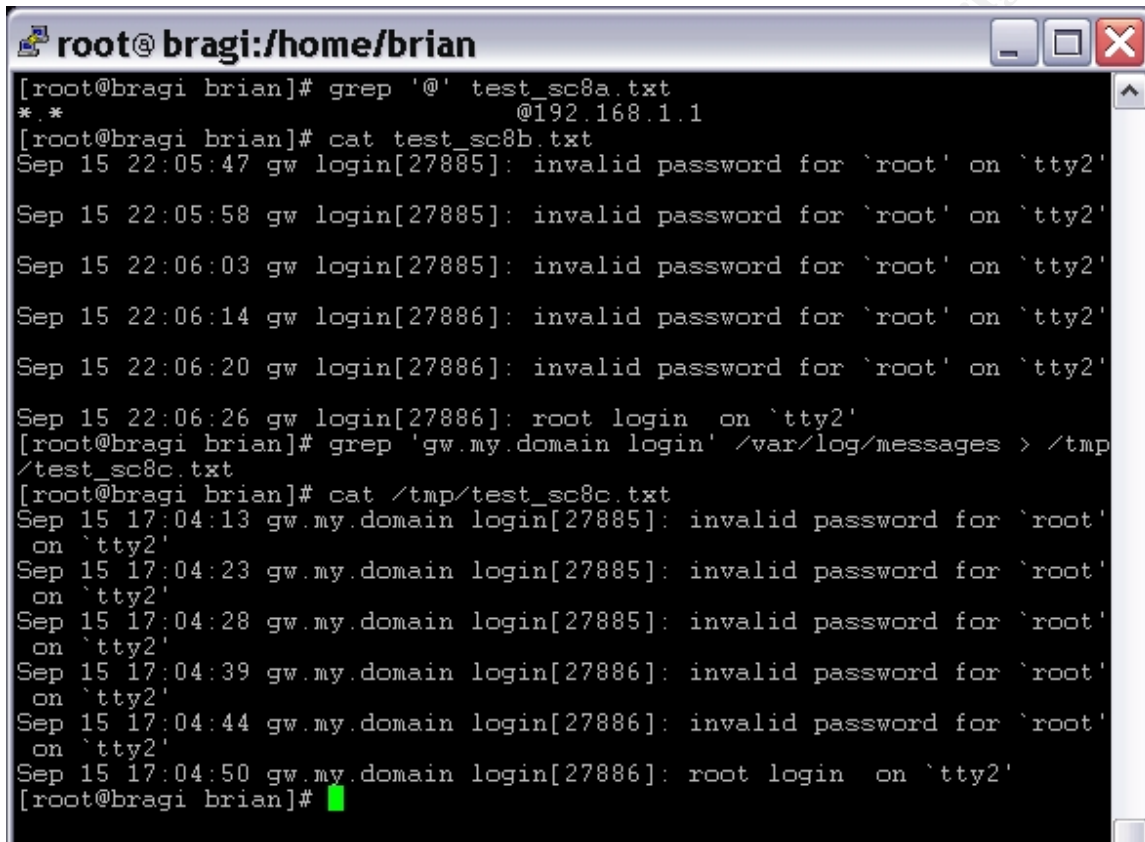
The firewall system passed this test.

The system logged successful logins to the local files and to the remote loghost.

The line extracted from 'test\_sc8a.txt' shows that the file 'syslog.conf' on 'gw' is configured to log messages to the remote loghost 192.168.1.1.

The printing of the file 'test\_sc8a.txt' shows that successful login attempts (and unsuccessful login attempts from SC6) are written to a local logfile.

The printing from the file 'test\_sc8c.txt' shows that these messages are also logged to the remote loghost.

A terminal window titled 'root@bragi:/home/brian' with standard window controls. The terminal shows the following commands and output:

```
[root@bragi brian]# grep '@' test_sc8a.txt
*.* @192.168.1.1
[root@bragi brian]# cat test_sc8b.txt
Sep 15 22:05:47 gw login[27885]: invalid password for `root' on `tty2'
Sep 15 22:05:58 gw login[27885]: invalid password for `root' on `tty2'
Sep 15 22:06:03 gw login[27885]: invalid password for `root' on `tty2'
Sep 15 22:06:14 gw login[27886]: invalid password for `root' on `tty2'
Sep 15 22:06:20 gw login[27886]: invalid password for `root' on `tty2'
Sep 15 22:06:26 gw login[27886]: root login on `tty2'
[root@bragi brian]# grep 'gw.my.domain login' /var/log/messages > /tmp/test_sc8c.txt
[root@bragi brian]# cat /tmp/test_sc8c.txt
Sep 15 17:04:13 gw.my.domain login[27885]: invalid password for `root' on `tty2'
Sep 15 17:04:23 gw.my.domain login[27885]: invalid password for `root' on `tty2'
Sep 15 17:04:28 gw.my.domain login[27885]: invalid password for `root' on `tty2'
Sep 15 17:04:39 gw.my.domain login[27886]: invalid password for `root' on `tty2'
Sep 15 17:04:44 gw.my.domain login[27886]: invalid password for `root' on `tty2'
Sep 15 17:04:50 gw.my.domain login[27886]: root login on `tty2'
[root@bragi brian]#
```

### Test Example #5 – SC9

The firewall system passed this test.

At no time during a system reset was the Outside host or the DMZ host able to access restricted network resources.

The drawing from “Test Example #6” shows how the scanner system was connected to the existing network.

A continuous ping was started on an Outside host to a DMZ host address and the output was stored in the file 'test\_sc9a.txt'. Another continuous ping was started on the Outside host to an Internal host address and the output was store in the file 'test\_sc9a2.txt'. Then a series of telnet attempts were made from a DMZ host to an Internal host. While all of this was going on, the firewall was reset.

The output from 'test\_sc9a.txt' is summarized here:

```
[root@hermes-rh72 brian]# ping 10.1.1.122
PING 10.1.1.122 (10.1.1.122) from 10.1.1.125 : 56(84) bytes of data.
```

```

From 10.1.1.125: Destination Host Unreachable
. . . <75 more of these messages> . . .
From 10.1.1.125: Destination Host Unreachable
From 10.1.1.125: Destination Host Unreachable

--- 10.1.1.122 ping statistics ---
166 packets transmitted, 0 packets received, +78 errors, 100%
packet loss

```

The output from 'test\_sc9a2.txt' is summarized here:

```

[root@hermes-rh72 brian]# route add -net 192.168.1.0 netmask
255.255.255.0 gw 10.1.1.121
[root@hermes-rh72 brian]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) from 10.1.1.125 : 56(84) bytes of
data.
From 10.1.1.125: Destination Host Unreachable
. . . <60 more of these messages> . . .
From 10.1.1.125: Destination Host Unreachable
From 10.1.1.125: Destination Host Unreachable

--- 192.168.1.1 ping statistics ---
150 packets transmitted, 0 packets received, +63 errors, 100%
packet loss

```

The above ping tests show that at no time was the Outside host able to communicate with the DMZ or Internal hosts.

NOTE: When the firewall was up, there were no responses to the stimuli at all, hence the higher number of packets transmitted than errors. While the firewall was down, the "Destination Host Unreachable" messages were reported as a result of the scanner being on the same segment as the outside interface of the firewall. The operating system on the scanner was able to detect that the network interface was down because it issued 'who has' ARP requests and did not get a response. This is simply a by-product of the two systems being physically connection to the same Ethernet hub.

The following is a script capture is an excerpt from the file 'test\_sc9b.txt'. It shows the attempts to made from a DMZ host to connect to the telnet service on an Internal host (something that is not allowed by the Network Security Policy). It shows that at no time was the DMZ host able to connect to the Internal host. The text in the angle-braces (<,>) are edits to show the timeline for the testing process.

```

<FIREWALL IS ACTIVE>
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: Connection refused
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: Connection refused

<FIREWALL IS RESET>
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: No route to host
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: No route to host

```

```

. . .
<FIREWALL CONTINUES TO BOOT>
. . .
<FIREWALL IS ACTIVE, AGAIN>
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: Connection refused
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: Connection refused
[brian@10.1.1.122 brian]$ telnet 192.168.1.1
Trying 192.168.1.1...

telnet: connect to address 192.168.1.1: Connection refused

```

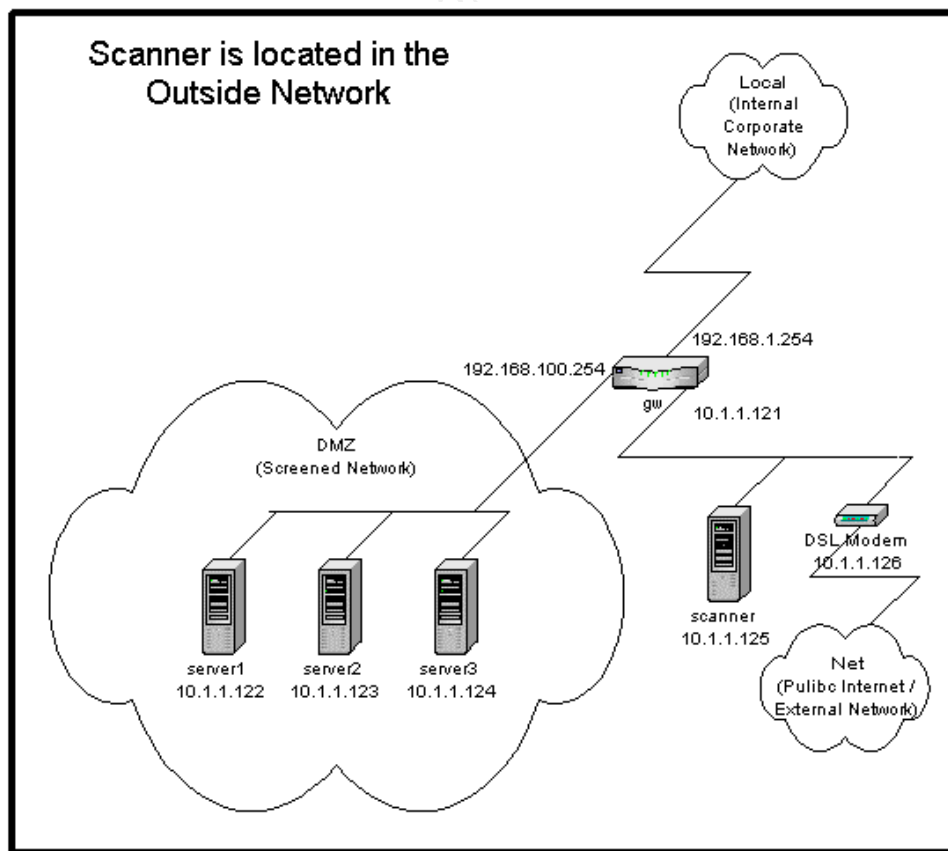
## Firewall Ruleset Checklist

### Test Example #6 – RC1

The firewall system passed this test.

The Outside host was unable to communicate with any network services on the firewall.

A portscan was performed, using nmap. Nmap will report TCP and UDP ports as being in one of three states, open, closed, or filtered. For more information on nmap, please refer to the Resources section. The following drawing shows how the scanner system was connected to the existing network.



The commands used to execute the test were:

```
[root@hermes-rh72 brian]# script test_rc1.txt
[root@hermes-rh72 brian]# nmap -sT -sU -P0 -p 1-65535 10.1.1.121
[root@hermes-rh72 brian]# exit
```

The following is a summary of the TCP output from that portscan.

```
# grep -v udp test_rc1.txt | grep -v '^$'
```

```
. . .
Port      State      Service
113/tcp    closed     auth
135/tcp    closed     loc-srv
```

This summary shows all TCP ports that were identified as not being filtered<sup>2</sup>, thus, all that is displayed here should be ports that are either closed or open. There are no TCP ports found to be open, so the firewall is not allowing access to any of its services.

The two TCP ports (113 and 135) shown here as closed are not accessible, however, the scanner did receive a response that the port could not be reached, as compared to filtered ports. There are reasons why this might be desirable for these ports<sup>3</sup>.

The following is a summary of the UDP output from that portscan.

```
# grep -v open test_rc1.txt | grep -v tcp | grep -v '^$'
```

```
. . .
Port      State      Service
137/udp    closed     netbios-ns
138/udp    closed     netbios-dgm
139/udp    closed     netbios-ssn
445/udp    closed     microsoft-ds
```

This summary shows all UDP ports that were not identified as being either filtered or open. The UDP ports (137-139, and 445) shown here as closed are not accessible by the scanner. There are reasons why this might be desirable for these ports<sup>4</sup>.

The following entries were logged, illustrating that the firewall was actively dropping some of these packets.

```
. . .
Sep 15 18:25:50 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=10.1.1.125
DST=10.1.1.121 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=52906 DF
PROTO=TCP SPT=43518 DPT=18294 WINDOW=5840 RES=0x00 SYN URGP=0
Sep 15 18:25:50 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=
```

---

<sup>2</sup> Filtered ports are that for which nmap received no response to its stimulus. The firewall is preventing the TCP packets from reaching the target host. If the firewall were not preventing this, it is expected that the scanner would receive a TCP RESET packet to indicate that there is no service listening on that port. Since the expected response is not received, the scanner calls these ports 'filtered'.

<sup>3</sup> Port 113 is the well-known port number for the TCP service ident or auth. This service is used as a method to further identify the originator of a remote connection to the local system. This protocol is particularly used by email transportation (SMTP) and file transfer (FTP) protocols. In this case, the request is rejected instead of being dropped. The result is still that the remote system was not allowed to connect to the server, however, the reject is considered to more "polite" as the remote host is able to close its connection immediately and move on, instead of waiting and eventually timing-out its request. The same notion is applied to the requests for connection to TCP port 135.

<sup>4</sup> The same notion as for TCP 113 and 135 is applied to UDP ports 137, 138, 139, and 445. These services are used by Microsoft systems for file and other information-sharing connections.

```

MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=10.1.1.125
DST=10.1.1.121 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=20038 DF
PROTO=TCP SPT=43519 DPT=32063 WINDOW=5840 RES=0x00 SYN URGP=0
Sep 15 18:25:50 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=10.1.1.125
DST=10.1.1.121 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=54981 DF
PROTO=TCP SPT=43520 DPT=10492 WINDOW=5840 RES=0x00 SYN URGP=0
Sep 15 18:25:50 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=10.1.1.125
DST=10.1.1.121 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=533 DF
PROTO=TCP SPT=43521 DPT=206 WINDOW=5840 RES=0x00 SYN URGP=0
Sep 15 18:25:50 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=10.1.1.125
DST=10.1.1.121 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=34929 DF
PROTO=TCP SPT=43522 DPT=1502 WINDOW=5840 RES=0x00 SYN URGP=0
. . .

```

### Test Example #7 – RC2

The firewall system passed this test.

The Outside host was unable to communicate with any unapproved network services on the DMZ hosts.

A portscan was performed, using nmap. The drawing from “Test Example #6” shows how the scanner system was connected to the existing network.

The commands used to execute the test were:

```

[root@hermes-rh72 brian]# script test_rc2.txt
[root@hermes-rh72 brian]# nmap -sT -sU -P0 -p 1-65535 10.1.1.122
10.1.1.123 10.1.1.124
[root@hermes-rh72 brian]# exit

```

The following is a summary of the TCP output from that portscan.

```

# grep -v udp test_rc2.txt | grep -v '^$'
Interesting ports on (10.1.1.122):

```

```

. . .
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
81/tcp    open       hosts2-ns
113/tcp   closed     auth
135/tcp   closed     loc-srv
554/tcp   open       rtsp
3782/tcp  closed     unknown
7070/tcp  open       unknown
8080/tcp  open       http-proxy
18009/tcp closed     unknown

```

```

Interesting ports on (10.1.1.123):

```

```

. . .
Port      State      Service

```

22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
113/tcp	closed	auth
135/tcp	closed	loc-srv

Interesting ports on (10.1.1.124):

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
113/tcp	closed	auth
135/tcp	closed	loc-srv
6767/tcp	closed	unknown
8453/tcp	closed	unknown

The items of interest are the open TCP ports:

10.1.1.122:	21, 22, 25, 80, 81, 554, 3782, 7070, 8080, 18009
10.1.1.123:	22, 25, 80
10.1.1.124:	21, 22, 6767, 8453

After reviewing the "Accessible Network Resources" document, these services were found to be authorized.

The following is a summary of the UDP output from that portscan.

```
# grep -v open test_rc2.txt | grep -v tcp | grep -v '^$'
```

Interesting ports on (10.1.1.122):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds
3783/udp	closed	unknown

Interesting ports on (10.1.1.123):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds

Interesting ports on (10.1.1.124):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds
15121/udp	closed	unknown
15122/udp	closed	unknown
15123/udp	closed	unknown

The items of interest are the open UDP ports:

10.1.1.122:	3783
10.1.1.123:	none
10.1.1.124:	15121, 15122, 15123

After reviewing the “Accessible Network Resources” document, these services were found to be authorized.

The following entries were logged, illustrating that the firewall was actively dropping some of these packets.

```
. . .
Sep 15 21:20:51 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=eth2 SRC=10.1.1.125
DST=10.1.1.122 LEN=60 TOS=0x00 PREC=0x
00 TTL=63 ID=15907 DF PROTO=TCP SPT=60103 DPT=9702 WINDOW=5840
RES=0x00 SYN URG=0
Sep 15 21:20:51 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=eth2 SRC=10.1.1.125
DST=10.1.1.122 LEN=60 TOS=0x00 PREC=0x
00 TTL=63 ID=45270 DF PROTO=TCP SPT=60104 DPT=35032 WINDOW=5840
RES=0x00 SYN URG=0
Sep 15 21:20:51 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=eth2 SRC=10.1.1.125
DST=10.1.1.122 LEN=60 TOS=0x00 PREC=0x
00 TTL=63 ID=6652 DF PROTO=TCP SPT=60105 DPT=56760 WINDOW=5840
RES=0x00 SYN URG=0
Sep 15 21:20:51 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=eth2 SRC=10.1.1.125
DST=10.1.1.122 LEN=60 TOS=0x00 PREC=0x
00 TTL=63 ID=16848 DF PROTO=TCP SPT=60106 DPT=6633 WINDOW=5840
RES=0x00 SYN URG=0
Sep 15 21:20:51 gw.my.domain kernel:
Shorewall:net2all:DROP:IN=eth0 OUT=eth2 SRC=10.1.1.125
DST=10.1.1.122 LEN=60 TOS=0x00 PREC=0x
00 TTL=63 ID=32576 DF PROTO=TCP SPT=60135 DPT=32052 WINDOW=5840
RES=0x00 SYN URG=0
. . .
```

### Test Example #8– RC4

The firewall system passed this test.

The scanner system received no successful responses to its spoofed stimulus and neither of the target hosts received a packet from the spoofed system. This demonstrates that the spoofed packets were not able to traverse the firewall.

Packets were crafted with spoofed source IP addresses, using hping2. Hping2 is a packet-generation tool that will allow one to create custom TCP, UDP, or ICMP packets. For more information on hping2, please refer to the Resources section. The drawing from “Test Example #6” shows how the scanner system was connected to the existing network.

The network stimulus was generated from the scanner system as follows:

```
[root@hermes-rh72 root]# hping2 -1 -a 192.168.1.3 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers +
0 data bytes

--- 192.168.1.1 hping statistic ---
6 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@hermes-rh72 root]# hping2 -1 -a 10.1.1.122 10.1.1.123
```

```
HPING 10.1.1.123 (eth0 10.1.1.123): icmp mode set, 28 headers + 0
data bytes
```

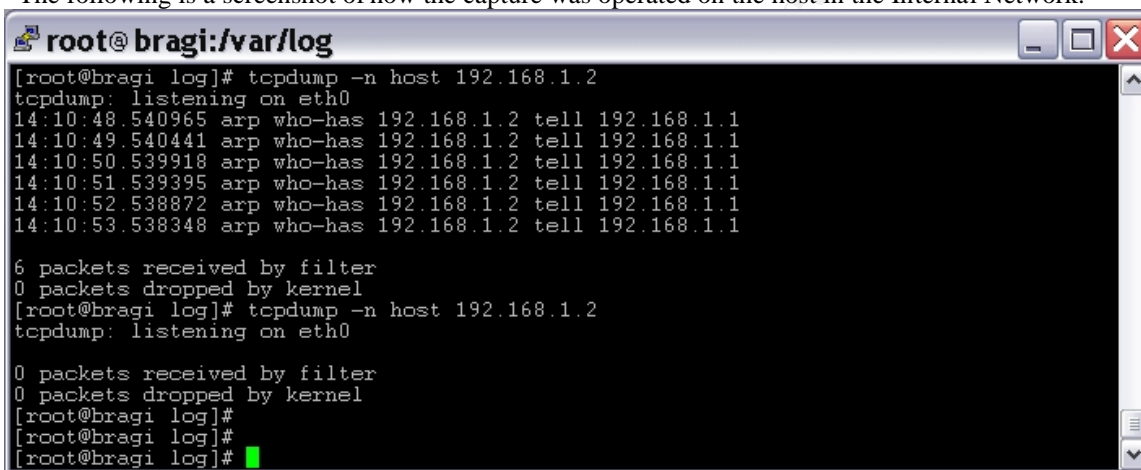
```
--- 10.1.1.123 hping statistic ---
6 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Packet captures were started on the target systems 10.1.1.123 and 192.168.1.1. The packet capture on the DMZ host was initiated with the following command:

```
[root@10.1.1.123 tmp]# tcpdump -n icmp
tcpdump: listening on eth0
```

```
0 packets received by filter
0 packets dropped by kernel
[root@10.1.1.123 tmp]#
```

The following is a screenshot of how the capture was operated on the host in the Internal Network.



```
root@bragi:/var/log
[root@bragi log]# tcpdump -n host 192.168.1.2
tcpdump: listening on eth0
14:10:48.540965 arp who-has 192.168.1.2 tell 192.168.1.1
14:10:49.540441 arp who-has 192.168.1.2 tell 192.168.1.1
14:10:50.539918 arp who-has 192.168.1.2 tell 192.168.1.1
14:10:51.539395 arp who-has 192.168.1.2 tell 192.168.1.1
14:10:52.538872 arp who-has 192.168.1.2 tell 192.168.1.1
14:10:53.538348 arp who-has 192.168.1.2 tell 192.168.1.1

6 packets received by filter
0 packets dropped by kernel
[root@bragi log]# tcpdump -n host 192.168.1.2
tcpdump: listening on eth0

0 packets received by filter
0 packets dropped by kernel
[root@bragi log]#
[root@bragi log]#
[root@bragi log]#
```

None of the spoofed packets from the tests shown in test\_rc4a.txt were successful. The following log entries show that the firewall logged the failed Internal-Internal spoof attempt:

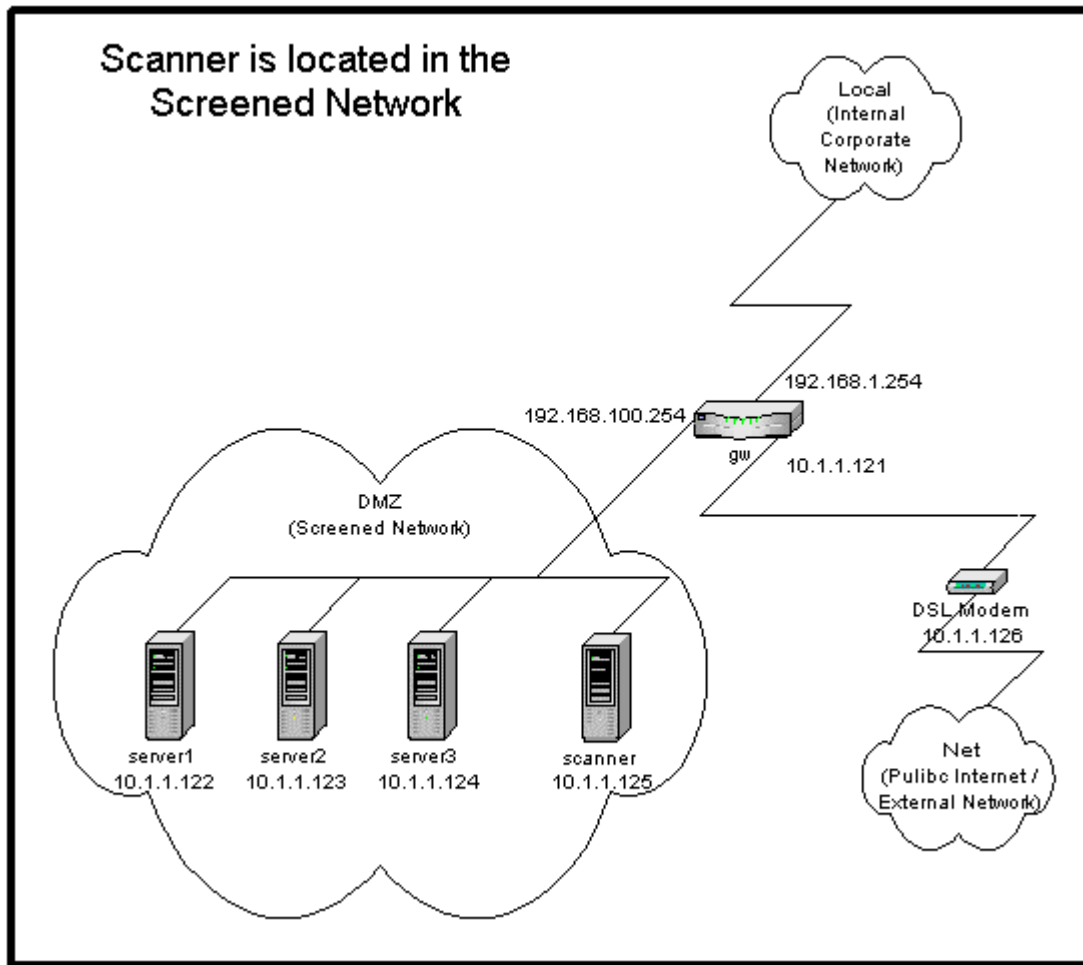
```
[root@bragi log]# grep '192.168.1.3' messages
Sep 16 14:48:14 gw.my.domain kernel:
Shorewall:man1918:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=192.168.1.3
DST=192.168.1.1 LEN=28 TOS=0x00 PREC=0x00 TTL=64 ID=35722
PROTO=ICMP TYPE=8 CODE=0 ID=33108 SEQ=0
Sep 16 14:48:15 gw.my.domain kernel:
Shorewall:man1918:DROP:IN=eth0 OUT=
MAC=00:20:af:06:97:25:00:50:56:78:8e:e0:08:00 SRC=192.168.1.3
DST=192.168.1.1 LEN=28 TOS=0x00 PREC=0x00 TTL=64 ID=4700
PROTO=ICMP TYPE=8 CODE=0 ID=33108 SEQ=256
. . .
```

### Test Example #9– RC5

The firewall system passed this test.

The Screened Network host was unable to communicate with any network services on any of the firewall interfaces.

A portscan was performed, using nmap. The following drawing shows how the scanner system was connected to the existing network.



The commands used to generate and the output resulting from the portscans were recorded in the script file 'test\_rc5a.txt'. The following is an excerpt from that file:

```
[root@hermes-rh72 root]# nmap -sT -sU -P0 -p 1-1023 10.1.1.121  
192.168.100.254 192.168.1.254
```

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )  
All 2046 scanned ports on gw-out.my.domain (10.1.1.121) are:  
closed  
All 2046 scanned ports on gw-dmz.my.domain (192.168.100.254) are:  
closed  
All 2046 scanned ports on gw.my.domain (192.168.1.254) are:  
closed
```

```
Nmap run completed -- 3 IP addresses (3 hosts up) scanned in 3074  
seconds
```

The results show that there were no ports on the firewall that were open to the host in the Screened Network.

## Test Example #10– RC6

The firewall system passed this test.

The Screened Network host was unable to communicate with any unapproved network services on the Internal hosts.

A portscan was performed, using nmap. The drawing from “Test Example #9” shows how the scanner system was connected to the existing network.

The commands used to generate and the output resulting from the portscans were recorded in the script file ‘test\_rc6a.txt’. The following is an excerpt from that file:

```
[root@hermes-rh72 root]# nmap -sT -sU -P0 -p 1-1023 192.168.1.1
192.168.1.3

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on server0.my.domain (192.168.1.1):
(The 2044 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp
53/udp    open       domain

All 2046 scanned ports on server00.my.domain (192.168.1.3) are:
closed

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 2074
seconds
[root@hermes-rh72 root]# nmap -sT -sU -P0 -p 1-100 192.168.1.2

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
All 200 scanned ports on (192.168.1.2) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 95
seconds
```

The items of interest are the open ports:

```
192.168.1.1:  TCP 25
              UDP 53
```

After reviewing the “Accessible Network Resources” document, these services were found to be authorized.

For the duration that the portscan was under way, one of the target hosts ran a packet capture with the tcpdump utility and that capture data was written to the file ‘test\_rc6b.dump’:

```
[root@bragi brian]# tcpdump -n -w test_rc6b.dump host 10.1.1.125
tcpdump: listening on eth0

14 packets received by filter
0 packets dropped by kernel
[root@bragi brian]# tcpdump -n -r test_rc6b.dump
21:47:57.239970 10.1.1.125.32769 > 192.168.1.1.domain: . . .
21:47:57.239970 192.168.1.1.domain > 10.1.1.125.32769: . . .
21:47:57.559804 10.1.1.125.38335 > 192.168.1.1.smtp: S
1419251894:1419251894(0) win 5840 <mss 1460,sackOK,timestamp
9010481 0,nop,wscale 0> (DF)
21:47:57.559804 192.168.1.1.smtp > 10.1.1.125.38335: S
3130844798:3130844798(0) ack 1419251895 win 5792 <mss
1460,sackOK,timestamp 44167971 9010481,nop,wscale 0> (DF)
```

```

21:47:57.569798 10.1.1.125.38335 > 192.168.1.1.smtp: . ack 1 win
5840 <nop,nop,timestamp 9010481 44167971> (DF)
21:47:57.579793 10.1.1.125.38335 > 192.168.1.1.smtp: R 1:1(0) ack
1 win 5840 <nop,nop,timestamp 9010482 44167971> (DF)
21:50:49.580513 10.1.1.125.60382 > 192.168.1.1.domain: . . .
21:50:50.550011 10.1.1.125.60383 > 192.168.1.1.domain: . . .
21:59:05.751268 10.1.1.125.60382 > 192.168.1.1.domain: . . .
21:59:13.446614 10.1.1.125.60383 > 192.168.1.1.domain: . . .
22:05:04.820519 10.1.1.125.60382 > 192.168.1.1.domain: . . .
22:05:08.427810 10.1.1.125.60383 > 192.168.1.1.domain: . . .
22:05:12.105060 10.1.1.125.32769 > 192.168.1.1.domain: . . .
22:05:12.105060 192.168.1.1.domain > 10.1.1.125.32769: . . .

```

A snort IDS system in the DMZ detected this portscan. The IDS, showed that a “noisy” scan was issued from the scanner system at IP address 10.1.1.125 by reporting the following portscan information.

```

. . .
Sep 16 22:24:54 10.1.1.125:50604 -> 192.168.1.1:175 UDP
Sep 16 22:24:55 10.1.1.125:50604 -> 192.168.1.1:589 UDP
Sep 16 22:24:56 10.1.1.125:50604 -> 192.168.1.1:409 UDP
Sep 16 22:25:00 10.1.1.125:50605 -> 192.168.1.1:641 UDP
Sep 16 22:25:01 10.1.1.125:50604 -> 192.168.1.1:682 UDP
Sep 16 22:25:06 10.1.1.125:50605 -> 192.168.1.1:53 UDP
. . .

```

The fact that the IDS detected that the packets were sent to all ports in the range specified by the nmap command, in consideration with the list of ports that the target hosts’ packet capture reported, is consistent with the results from nmap. The end result is that the scanner was able to reach only ports on the approved services list, smtp port (TCP/25) and the domain port (UDP/53), on the target host 192.168.1.1.

### ***Measure Residual Risk***

The firewall system passed all of the items on the audit checklist, and as a result this is very little residual risk associated with the firewall, itself, and the ruleset that it implements. There were a few enhancements that were recommended as a result of the findings from the checklist tests that were conducted. These are all minor enhancements and are in excess of the level of security that the Network Security Policy and the “Accessible Network Resources” document; however, the implementation of these recommendations would further the scope of protection that the firewall can provide. Additionally, there was one network service on the firewall that was on the approved services list, which has been removed from that list. The recommendations and decided changes are addressed in the Risk Assessment in Assignment 4.

In the bigger picture of network or information security—of which the firewall system and its ruleset are but a subset—there are many other areas that are outside the scope of this audit. While the firewall passed the audit, the security of the network as a whole comes into question. These include but are not limited to items such as the services running on the DMZ and Internal Network Hosts, virus-scanning, administrator and user practices and procedures, and the need for a network intrusion detection system. These items are certainly not with the scope of this audit, but management should consider their value with respect to the big picture.

### ***Is the System Auditable?***

Based upon the audit research and the personal experience of the auditor, it is believed that the checklist, testing methodology, and the risks that were addressed were valid. The test steps taken to audit the firewall system and the ruleset, were beyond the inspection of a written security policy.

The objective tests that were performed yielded evidence that the firewall successfully performs its functions under the scrutiny of various forms of external stimulus. By logging successful and failed logins

and rejected or dropped packets the firewall configuration showed an active response to the probes and spoofing attempts. Furthermore, the packet captures that were run on target systems in some of the checklist tests showed that the criteria for compliance were observed from other systems besides the firewall, itself.

The subjective tests are more nebulous, but are also valid tests. Especially, if the auditor shares relevant understanding of the test criteria and their findings with the people responsible for the firewall. This sharing of information can be beneficial to the auditor as well as the administrators and helps build a more aware community.

## Assignment 4 – Risk Assessment

### Overview

The checklist from Assignment 2 has been followed and the results of several of the tests have been detailed in Assignment 3. What follows in this section is an assessment of the risks to the system, based upon the findings from the completion of the checklist tests.

The scope of the audit was tightly focused on the security of firewall system, the ruleset that it implements, and the management of the firewall systems with respect to the Network Security Policy.

### Summary

An audit of the firewall system, 'gw', has been conducted and the capabilities, configuration, operation, and maintenance of the system have been evaluated as per the scope of the audit. The tests of the system demonstrate that the LEAF system, 'gw', was capable and effectively configured to satisfy the requirements for implementing the relevant areas of the Network Security Policy.

The checklist tests were performed to evaluate the security of the firewall system, as a whole, and the administration processes associated with that system. The items on this checklist were divided into two areas of testing:

- System Check (SC) items to validate the firewall system by auditing its capabilities, configuration, operation, and maintenance
- Ruleset Check (RC) items to validate the firewall system by auditing the functionality of the firewall ruleset, as implemented with respect to the Network Security Policy

### Audit Results

The firewall system was found to have successfully passed 11 of the 12 System Checks. All of the tested capabilities, mechanisms, and behaviors of the firewall system were in compliance with the control objectives with the exception of one test, SC10. The operation and maintenance of the firewall system was also found to pass all of the checks.

The firewall system was found to have successfully passed all 12 of the Ruleset Checks. None of the test packets able to access or traverse that firewall system which were not explicitly allowed by Network Security Policy.

The firewall system has been demonstrated to a capable system that is found to be well configured and adequately maintained. One System Check was failed and there are some recommendations, however, that can be made with the intention of improving the overall security of the network and the maintainability of the firewall system.

## Background/Risk

### Failed Test

The system was found to have failed the following checklist item.

Checklist Item	Risk / Area for Improvement	Impact
SC10	Internal Threats	Unauthorized personnel may have physical access to the firewall. If the firewall is unattended, but has an active login the person may be able to subvert the firewall or collect restricted information.

### Areas for Improvement

The following checklist items, though found to be compliant with the audit criteria, have been identified as areas that can be improved to improve the overall information security of the company:

Checklist Item	Risk / Area for Improvement	Impact
RC7	External Threats	Systems with services that are exposed to direct connections from outside systems are at a high risk of being attacked and possibly exploited. If those systems are compromised that there are no restrictions on their outbound connectivity they may be used as points-of-attack to other systems (the company's or others) or for channeling critical information to the outside.
RC10 and RC11	Internal Threats	Damage may range from decreased individual productivity to the channeling of critical company information to the outside. Additionally, the possibility that company systems may be used for points-of-attack to other systems (the company's or others), adversely affecting the company's reputation.

## System Changes and Further Testing

There are steps that may be taken to address the risks identified in the current state of the firewall system and its administration. The following tables detail the steps associated with each of the risks mentioned above.

### Improvements to Elements Tested by RC7 and RC11

Identifier	RC7
Control Objective	Test for unapproved access to services in the Outside Network from the Screened Network.
Reference	Articles from the SANS Reading Room and personal experience
Risk	Description: Unapproved access to Internet systems from local systems may help enable a system to be used for unauthorized purposes or may allow a compromised system to be used for other attacks or a conduit for information leakage. A user logging on to a DMZ host to access an Internet host that is restricted to Corporate hosts. Importance: medium Likelihood: low-medium
Compliance	The accessibility to Internet services must be in compliance with the Network Security Policy
Recommended	Create and implement a formal Change Control Procedure.

<b>Improvements</b>	
<b>Tasks</b>	Update “Accessible Network Resources” document and get it approved by the necessary company authorities. Re-configure the firewall ruleset and re-test for compliance.
<b>Costs</b>	2-4 hours to update and deploy new document. 2-4 hours to implement and new firewall ruleset and re-test.

<b>Identifier</b>	<b>RC10</b>
<b>Control Objective</b>	Test for unapproved access to services in the Screened Network from the Internal Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to services may result in a denial of service attack or the system being compromised. Importance: high Likelihood: low-medium
<b>Compliance</b>	The accessible services must be in compliance with the Network Security Policy
<b>Recommended Improvements</b>	Create and implement a formal Change Control Procedure.
<b>Tasks</b>	Update “Accessible Network Resources” document and get it approved by the necessary company authorities. Re-configure the firewall ruleset and re-test for compliance.
<b>Costs</b>	2-4 hours to update and deploy new document. 2-4 hours to implement and new firewall ruleset and re-test.

<b>Identifier</b>	<b>RC11</b>
<b>Control Objective</b>	Test for unapproved access to services in the Outside Network from the Internal Network.
<b>Reference</b>	Articles form the SANS Reading Room and personal experience
<b>Risk</b>	Description: Unapproved access to Internet systems from local systems may help enable a system to be used for unauthorized purposes or may allow a compromised system to be used for other attacks or a conduit for information leakage. Importance: medium Likelihood: low-medium
<b>Compliance</b>	The accessibility to Internet services must be in compliance with the Network Security Policy
<b>Recommended Improvements</b>	Create and implement a formal Change Control Procedure.
<b>Tasks</b>	Update “Accessible Network Resources” document and get it approved by the necessary company authorities. Re-configure the firewall ruleset and re-test for compliance.
<b>Costs</b>	2-4 hours to update and deploy new document. 2-4 hours to implement and new firewall ruleset and re-test.

Given the overlap between the tasks to improve the security of the items tested by RC7, RC10, and RC11, these concerns were addressed at the same time.

### **Update Documentation**

The “Accessible Network Resources” document was modified. The following is the re-working of the relevant areas of that document.

### **DMZ Network Resources**

The following DMZ resources may be reached from the Inside:

Server1 (10.1.1.122):	TCP	21, 22, 25, 80, 81, 554, 3782, 7070, 8080, 18009
	UDP	53, 3783
Server2 (10.1.1.123):	TCP	22, 25, 80
	UDP	53
Server3 (10.1.1.124):	TCP	21, 22, 6767, 8453
	UDP	15121, 15122, 15123

Select administration nodes will be able to access the following additional resources on each of the DMZ servers:

UDP 161

#### **Internet Access from DMZ Network**

The DMZ hosts may reach only the following Outside resources:

TCP 21, 80, 113, 443  
UDP 53

The email relay in the DMZ will also be able to reach the following outside resources:

TCP 25, 110

#### **Internet Access from Internal Network**

The Internal hosts may reach only the following Outside resources.

TCP 21, 22, 23, 80, 113, 443, 554

Select infrastructure servers will be able to reach the following additional outside resources:

UDP 53

#### **Re-Run Test RC7**

The firewall system passed this test.

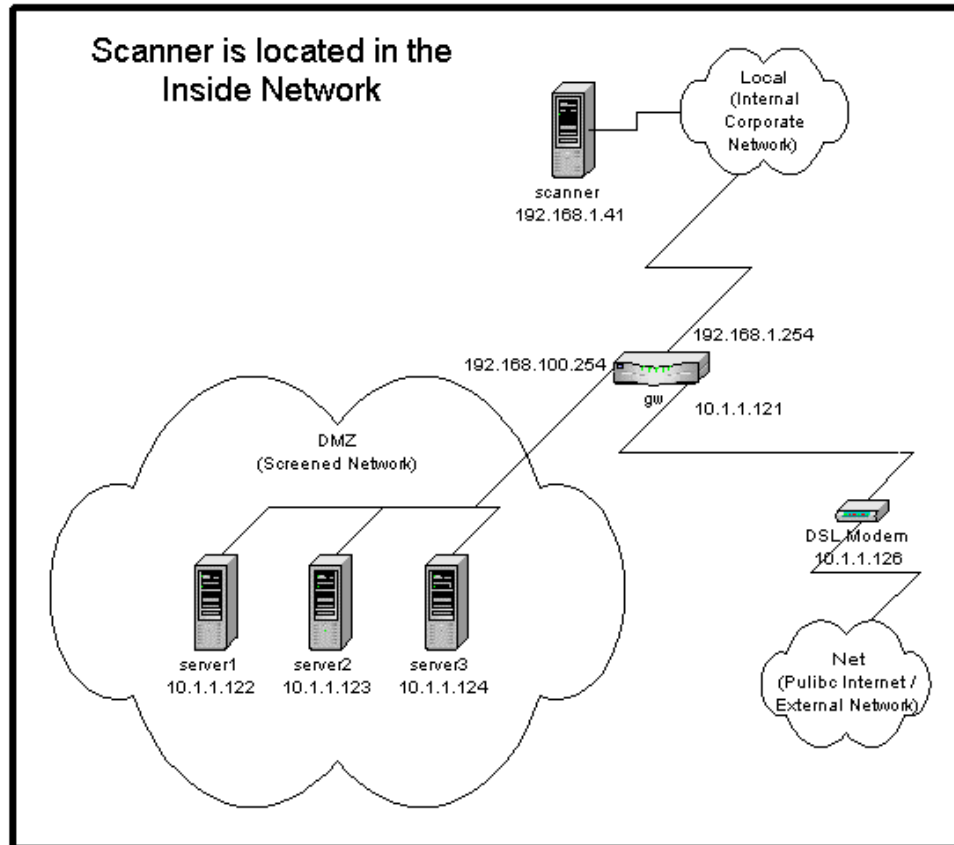
After the new firewall ruleset was implemented, the firewall rules were inspected for consistency with the updated Network Security Policy and found to be in compliance.

#### **Re-Run Test RC10**

The firewall system passed this test.

The Inside host was unable to communicate with any unapproved network services on the DMZ hosts.

A portscan was performed, using nmap. The following drawing shows how the scanner system was connected to the existing network.



The commands used to execute the test were:

```
[root@hermes-rh72 brian]# script retest_rc10.txt
[root@hermes-rh72 brian]# nmap -sT -sU -P0 -p 1-19000 10.1.1.122
10.1.1.123 10.1.1.124
[root@hermes-rh72 brian]# exit
```

The following is a summary of the TCP output from that portscan.

```
# grep -v udp retest_rc10.txt | grep -v '^$'
Interesting ports on (10.1.1.122):
...
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
81/tcp    open       hosts2-ns
113/tcp   closed     auth
135/tcp   closed     loc-srv
554/tcp   open       rtsp
3782/tcp  closed     unknown
7070/tcp  open       unknown
8080/tcp  open       http-proxy
18009/tcp closed     unknown

Interesting ports on (10.1.1.123):
...
Port      State      Service
```

22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
113/tcp	closed	auth
135/tcp	closed	loc-srv

Interesting ports on (10.1.1.124):

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
113/tcp	closed	auth
135/tcp	closed	loc-srv
6767/tcp	closed	unknown
8453/tcp	closed	unknown

The items of interest are the open TCP ports:

10.1.1.122:	21, 22, 25, 80, 81, 554, 3782, 7070, 8080, 18009
10.1.1.123:	22, 25, 80
10.1.1.124:	21, 22, 6767, 8453

After reviewing the newly revised "Accessible Network Resources" document, these services were found to be authorized.

The following is a summary of the UDP output from that portscan.

```
# grep -v open test_rc10.txt | grep -v tcp | grep -v '^$'
```

Interesting ports on (10.1.1.122):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds
3783/udp	closed	unknown

Interesting ports on (10.1.1.123):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds

Interesting ports on (10.1.1.124):

Port	State	Service
137/udp	closed	netbios-ns
138/udp	closed	netbios-dgm
139/udp	closed	netbios-ssn
445/udp	closed	microsoft-ds
15121/udp	closed	unknown
15122/udp	closed	unknown
15123/udp	closed	unknown

The items of interest are the open UDP ports:

10.1.1.122:	3783
10.1.1.123:	none
10.1.1.124:	15121, 15122, 15123

After reviewing the newly revised “Accessible Network Resources” document, these services were found to be authorized.

### Re-Run Test RC11

The firewall system passed this test.

After the new firewall ruleset was implemented, the firewall rules were inspected for consistency with the updated Network Security Policy and found to be in compliance. The security of the DMZ network has been improved by better protecting the servers from internal attacks, as has the

## System Justification

### Failed Test SC10

Though this test was failed and no reasonable solution has been found there are a simple administrative practice that can greatly reduce the risk of not having idle logins automatically closed.

<b>Identifier</b>	<b>SC10</b>
<b>Control Objective</b>	Test that idle console sessions are automatically closed.
<b>Reference</b>	ICSA Labs and SANS Reading Room
<b>Risk</b>	Description: In the event that an administrator fails to manually close a system login when not working on the system, someone else would be able to walk-up and reconfigure or gain privileged information from the system. Importance: medium Likelihood: medium-low
<b>Mitigation / Compensating Control</b>	There is no simple way to implement this functionality, however the simple administrative practice of being sure to logout whenever you one leaves the console unattended will go a very long way in mitigating the risk.

## References

“LEAF – Linux Embedded Appliance Firewall”, URL <http://leaf.sourceforge.net/> (September 16, 2002).

“Linux Router Project”, URL <http://www.linuxrouter.org/> (September 2, 2001).

“Shoreline Firewall”, URL <http://www.shorewall.net/>, Copyright © 2001,2002 Thomas M. Eastep (September 16, 2002).

Seifried, Kurt. “Linux Administrator’s Security Guide”, URL <http://www.seifried.org/lasg/>, Copyright Kurt Seifried 2001 (September 16, 2002).

“ICSA Labs' Firewall Community”, URL <http://www.icsalabs.com/html/communities/firewalls/index.shtml>, November 3, 2000.

“The SANS Institute ~ SysAdmin, Audit, Network, Security - Computer Security Education and Information Security Training”, URL <http://www.sans.org/>, Copyright © 2002 The SANS Institute (September 16, 2002).

“SANS Institute: Information Security Reading Room”, URL <http://rr.sans.org/index.php> (September 16, 2002).

Sutherland, John. “4th Generation of Linux Based Firewalls”, URL [http://rr.sans.org/firewall/4th\\_gen.php](http://rr.sans.org/firewall/4th_gen.php), April 11, 2001.

Mitchell, Jason. "Proactive Vulnerability Assessments with Nessus", URL <http://rr.sans.org/audit/proactive.php>, April 26, 2002.

Konigsberg, Bob. "Auditing Inside the Enterprise via Port Scanning & Related Tools", URL <http://rr.sans.org/audit/inside.php>, January 18, 2002.

Kamerling, Erik J. "The Hping2 Idle Host Scan", URL <http://rr.sans.org/audit/hping2.php>, February 26, 2001.

"CERT Coordination Center", URL <http://www.cert.org/>, Copyright 1997, 2002 Carnegie Mellon University, September 16, 2002 15:56:49 EDT.

"CERIAS – CERIAS / Purdue University", URL <http://www.cerias.purdue.edu/> (September 16, 2002).

"The Linux System Administrator's Guide", version 0.7, URL <http://www.tldp.org/LDP/sag/index.html>, Copyright 2001 Stephen Stafford (September 16, 2002).

© SANS Institute 2001 - 2002, Author retains full rights.