



# 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>

***Auditing Networks, Perimeters, and Systems***  
***GSNA Practical Assignment***

Version 2.1 (amended July 5, 2002)

***Auditing a Cisco PIX firewall***  
***An auditor's perspective***

© SANS Institute 2003, Author retains full rights.

## ***Abstract***

A large scale software development for TLA Enterprises has been outsourced to a third party developer. The developer's use servers and workstations that are not compliant with TLA's Standard Operating Environment. TLA and the developers must maintain a high level of information and file sharing for the project to be a success. The third party developers are on site at TLA's premises in a shared office environment. If the developer's machines were connected to TLA's internal network they would raise the risk of vulnerabilities through many lines of attack.

TLA Enterprises decided to separate their internal networks from the development environment with a Cisco PIX 515E firewall. The firewall connects TLA's internal network to the development environments and permits connectivity to specific networks resources. The firewall installation and configuration is being audited against best practice.

Thirteen of the twenty control points passed the audit tests. A significant proportion of the non-conformances found in this audit come from minor configuration issues and a lack of understanding from the third party developers. The majority of non-conformance could be prevented if the firewall was installed and tested against an adequate standard and through additional training of the developers. The controls that are in place have been inadvertently circumvented by the developers and there is a continual high level risk of this reoccurring.

## Table of Contents

Assignment 1 .....	4
Audit scope .....	4
Risk evaluation .....	5
Current state of practice .....	9
Assignment 2 .....	10
Audit checklist .....	10
Assignment 3 .....	30
The audit .....	30
Residual Risk .....	59
Auditability of the system .....	62
Assignment 4 .....	63
Executive summary .....	63
Audit findings .....	63
Background and audit recommendations (with costs) .....	65
Additional recommendations and mitigations .....	67
Appendix A – Risk table methodology .....	69
Appendix B – Nessus scan results .....	71
Appendix C - References .....	90

## Assignment 1

### Audit scope

TLA Enterprises has engaged a third party development organisation to build an application on their behalf. The application will be developed on TLA's premises using the Developers workstation environment. For the Developers to perform their function, network connectivity is required between the groups, but TLA's network must maintain its security levels. A Cisco PIX 515 firewall was selected to provide the network connectivity, whilst enforcing network segregation. The firewall is the system being audited.

Cisco PIX is a stateful firewall, that is the firewall maintains a state table of all connections. The firewall filtering decisions are made on the static rules, plus any stateful responses for existing connections. This type of firewall is superior, and simpler to configure than a packet filtering firewall.

The specifications of the installed firewall are shown in the following table.

Item	Specification
Operating System	Cisco PIX Firewall Version 6.3(1)
PDM image	Cisco PIX Device Manager Version 3.0(1)
Model	PIX-515E
RAM	32 MB RAM
CPU	Pentium II 433 MHz
Flash	16MB
Ethernet interfaces	3*10/100Mb
License	Restricted
Encryption	DES only
Serial Number	80xxxxxx (0x3xxxxxx )

**Table 1 - Cisco PIX firewall specifications**

The purpose of this device is to separate three networks (Refer to Figure 1 - Network connectivity diagram) as described below.

1. The main network contains TLA's corporate network.
2. The second network is a DMZ which contains a number of development servers built by TLA
3. The third network is another DMZ which has a number of third party developers using their own equipment (Non TLA SOE) located on TLA's premises.

The network design is to protect TLA's network computers from the unknown development environment, and to provide a level of file sharing and network resources to allow the developers to perform their assignment.

Note: This document uses fictitious names, and IP addresses throughout.

## Risk evaluation

### Discussion

A typical relationship between a customer and developer is at separate premises and therefore separate networks. Due to the scale of the development, and necessity for constant dialogue between all parties it was decided to host the development at the TLA Enterprises premises. To ensure the development is unimpeded, the Developers require network services from TLA's private network. The Developers will not be using TLA's Standard Operating Environment (SOE) workstations. Any change or variation from the known state (TLA SOE workstation environment) increases the risk to TLA as there is a larger variety of systems, software, operating systems, and patch revisions on the network, therefore the decision to provide a segregated environment for the Developers.

TLA decided to separate the non SOE workstations from their private network to minimise the exposure to non standard environment. The risks that non standardised workstations can bring to a secured network include;

- vulnerabilities through un-patched software,
- vulnerabilities through different software,
- data corruption through different versions of software,
- virus or worm outbreak through non existent, or out of date anti-virus software,
- proprietary information leakage through the use of unauthorised software (such as packet sniffers and keystroke loggers).

These risks could result in the following outcomes;

- Financial loss resulting from fraudulent activity
- Loss of TLA's intellectual property
- Loss of business opportunity through disruption of service
- Unauthorized use of resources
- Loss of customer confidence or respect
- Costs resulting from uncertainties (lost time/opportunity cost).

For example, should the non SOE workstations be directly connected to the private network, the result to TLA Enterprises could be an outbreak of a denial of service worm (network bandwidth is consumed due to the worms talking to each other) such as the recent Slammer (AKA Sapphire, or Slapper) worm. The Slammer worm was reported to have cost businesses in the order of \$1 billion in its first five days<sup>1</sup>. For TLA, the impact could translate to slow or no connection to the business systems at the data centres, which would result in email not functioning, the customer service centres would be unable to function reliably and a multitude of other issues.

One design challenge concerns the "virtual segregation" of the workstations connecting to the TLA and Developer networks. While these two networks must be kept separate, the users concerned will be working side by side (physically co-located). The control to ensure compliance is a written requirement for all non SOE workstations (Developer) and servers to be connected via the firewall. This is enacted

by the labelling the desks SOE and non SOE. The non SOE workstations will function as if they are connected to a different network. As both parties ( TLA and the Developers ) require access to the development servers they have been placed in a DMZ between the Developers network and TLA's network.

A firewall is being used as a control to limit the exposure of the non SOE workstations to the TLA's network. This is the device that is being audited. The diagram below shows the network connectivity where the firewall is controlling access.

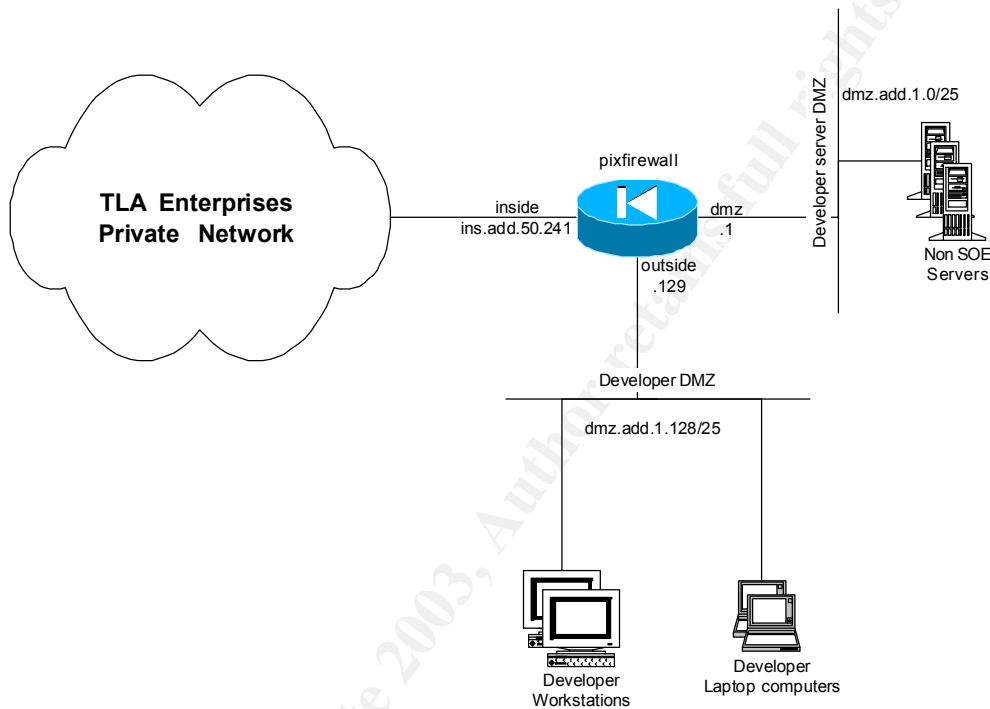


Figure 1 - Network connectivity diagram

A detailed explanation of the risk evaluation table methodology is detailed in Appendix A – Risk table methodology

Item	Threat	Likelihood (of exploit)	Consequence	Resultant risk
1. Misconfigured firewall ruleset	T1) More (or less) of the TLA's intellectual property will be accessed by the Developers	L1) Medium	C1) Serious	RR1) High
	T2) A computer virus outbreak can spread from the isolated network to TLA's production environment resulting in the loss of business opportunity	L2) High	C2) Damaging	RR2) High
	T3) TLA could suffer from unauthorised use of resources by a third party.	L3) High	C3) Minor	RR3) Medium
2. Vulnerability in firewall software	T4) The firewall could be compromised and the ruleset could be altered	L4) Low	C4) Damaging	RR4) Medium
3. Unnecessary firewall rules	T5) The larger the firewall ruleset the greater the probability of a configuration error in the future.	L5) High	C5) Serious	RR5) Critical
	T6) Unnecessary rules increase the maintenance overhead of managing the firewall and therefore decrease the resources to manage other security issues	L6) High	C6) Serious	RR6) Critical
	T7) Uncertainty about the need for a firewall rule could lead to further rules being added to other firewalls when using this firewall ruleset as an example	L7) Low	C7) Significant	RR7) Medium
4. Firewall ruleset experiences unauthorised modification	T8) Vulnerability in protocol used to administer firewall	L8) Low	C8) Damaging	RR8) Medium
5. Firewall is susceptible to DoS attack	T9) A DoS attack could render the firewall inoperable and unable to process legitimate traffic	L9) Very low	C9) Significant	RR9) Low
6. Unauthorised administrator access to firewall	T10) Configuration could be changed to permit more access to the TLA's network	L10) Low	C10) Damaging	RR10) Medium
	T11) Configuration could be damaged, rendering the firewall inoperable or compromised	L11) Low	C11) Significant	RR11) Medium
7. Inability to restore service due to hardware fail over or configuration corruption	T12) Configuration could be lost due to inadequate backup procedures	L12) Low	C12) Significant	RR12) Medium



8. Firewall may be negated due to lack of understanding of need for network segregation	T13) Unauthorised machines could connect to TLA's network without filtering being in place	L13) High	C13) Significant	RR13) High
---	--	-----------	------------------	------------

© SANS Institute 2003, Author retains full rights.

## Current state of practice

There are a number of firewall checklists available on the Internet. Most of these are based on the work of Lance Spitzner. Spitzner's works [Auditing your firewall setup](#), and [Building your firewall rulebase](#), in conjunction with Krishni Naidu's work, [Firewall checklist](#), form much of the basis of the work by Rick Yuen's [Auditing a Cisco PIX firewall: An Auditor Perspective](#).

These works, and other generic and vendor specific firewall documents listed below were reviewed and used as the basis for developing the checklist for the firewall. However these works are predominately concerned with auditing firewalls that are connected to the Internet. The environment in question does not have direct Internet connectivity, nor is it providing web services to the Internet at large.

The requirement in this instance is to provide business connectivity for a group of third party developers (internal network services - http proxy server, http email, and file sharing) whilst TLA Enterprises maintains their current level of network security. Other documents that were referenced to create the checklist were [Installation and Configuration for Common Criteria EAL4 Evaluated Cisco PIX Firewall Version 6.2\(2\) by Cisco Systems](#) and [Securing the Internal Network from the Internet Perimeter with a PIX Firewall: Another Layer of Protection](#) by Naeem Qasim. The Cisco document describes configuration practices to achieve EAL4 Common Criteria Certified Cisco Secure PIX Firewall, and is of limited use in this application. Naeem Qasim's work is a good introduction to configuring the PIX firewall, but of limited use in building the checklist.

A number of other documents were reviewed to obtain a broader understanding of the current state of practice. Specifically these documents were;

- [GIAC LevelTwo, Firewalls, Perimeter Protection, and VPNs, Practical Assignment for Capitol SANS, December 10 -15, 2000, Lenny Zeltser](#)
- [Firewall, VPN, IDS, and Router Tips #3: Cisco PIX Firewall Resources](#)
- [Cisco TAC, Field Notices, PIX 500 series firewalls](#)
- [Security and Electronic Security and Electronic Commerce](#), Ron Helsley, Jeff Reich
- [SecurityFocus Online Vulnerabilities](#)
- [CERT Security Improvement Modules](#)

Of note is the pending development by The Center for Internet Security of a "Benchmark and Scoring Tool" for the Cisco PIX Firewall. CIS have developed widely accepted benchmarks for Cisco routers, Windows and Unix. Many of these benchmark tools are freely available. Further details are available at <http://www.cisecurity.org/bench.html>. Another item of note is that Cisco does not have a checklist or best practice guide available for public consumption at this stage.

## Assignment 2

### Audit checklist

<b>Control point</b>	<b>1</b>
<b>Reference</b>	Original contribution , Northcutt <sup>1</sup>
<b>Control Objective</b>	Ensure only approved rules are configured on the firewall.
<b>Risk</b>	T1, T2, T3, T10, T11
<b>Compliance</b>	No difference between the active ruleset versus the approved ruleset
<b>Testing</b>	<p>Compare original firewall ruleset and approved changes (in TLA's Change Management system) against current ruleset .</p> <p>The firewall was configured and installed under approved Change x429 on 22/4/03. A further Change x503 was approved on 14/06/03 to make configuration modifications.</p> <p><b><u>On firewall</u></b> write memory write net ins.add.50.1:pixfirewall</p> <p><b><u>On *nix host</u></b> diff CRx429 pixfirewall</p> <p>Expected results</p> <ul style="list-style-type: none"> <li>• CRx503 – one line removed and one line included</li> <li>• Written by date changed</li> <li>• Cryptochecksum number changed</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>2</b>
<b>Reference</b>	Original contribution
<b>Control Objective</b>	Ensure all DMZ users (from third party developers) are aware of, and comply with policy of network separation
<b>Risk</b>	T13
<b>Compliance</b>	Survey results with developers of over 80% awareness
<b>Testing</b>	<p>Survey developers confirming;</p> <ol style="list-style-type: none"> <li>1) They are aware of the need for network separation</li> <li>2) Policy was communicated promptly</li> <li>3) Any inconveniences that tempt ignoring network separation</li> <li>4) Compliance with network separation policy</li> </ol> <hr/> <p><b><u>Survey</u></b> 1. Are you aware of the need and reasons for the networks to be separated?</p> <p>Yes No</p> <p>Reasons:</p> <ol style="list-style-type: none"> <li>1.</li> </ol>

	<p>2.</p> <p>3.</p> <p>2. Was this communicated to you in a timely manner when you started on site? Yes No</p> <p>3. Are there any circumstances in your time on site that have led to wishing to be directly connected to the corporate network?  Yes No</p> <p>4. Are you permitted to connect to YOUR corporate LAN or other networks whilst connected to the TLA's network  Yes No</p>
<b>Objective/ Subjective</b>	Subjective

<b>Control point</b>	<b>3</b>
<b>Reference</b>	Spitzner <sup>III</sup> , Northcutt <sup>IV</sup>
<b>Control Objective</b>	Ensure the size of the ruleset is manageable
<b>Risk</b>	T1, T2, T3, T5, T6, T7, T10, T11
<b>Compliance</b>	Number of rules should be no more than 30
<b>Testing</b>	<p>Count rules on copy of running configuration</p> <p><b><u>On a *nux host</u></b></p> <p># count the number of access -list lines in the firewall configuration file (pixfirewall)</p> <p>1) grep access-list pixfirewall   grep -v remark   wc -l</p> <p>2) Confirm via manual count</p>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>4</b>
<b>Reference</b>	Spitzner <sup>V</sup> , Naidu <sup>VI</sup> , Yuen <sup>VII</sup> , Original contribution
<b>Control Objective</b>	Ensure events are being logged on the syslog server correctly
<b>Risk</b>	T1, T2, T3
<b>Compliance</b>	<p>Generate unauthorized traffic destined for a higher security network on the outside and DMZ segments</p> <p>Verify dropped packets and system events log to syslog server on inside (secured) network</p>
<b>Testing</b>	<p><b><u>From Outside to DMZ</u></b></p> <p><b><u>On Outside host</u></b></p> <p>telnet ins.add.50.1</p>

	<p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <ul style="list-style-type: none"> <li>• Confirm packets denied</li> </ul> <p><b><u>Packet sniffer on inside host</u></b> tcpdump -nn src host dmz.add.1.140</p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• 0 packets received by filter</li> </ul> <hr/> <p><b><u>From DMZ to inside</u></b></p> <p><b><u>On DMZ host</u></b> telnet ins.add.50.1</p> <p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <ul style="list-style-type: none"> <li>• Confirm packets denied</li> </ul> <p><b><u>Packet sniffer on inside host</u></b> tcpdump -nn src host dmz.add.1.10</p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• 0 packets received by filter</li> </ul>
<b>Objective/ Subjective</b>	Objective
<b>Control point</b>	5
<b>Reference</b>	Naidu <sup>viii</sup>
<b>Control Objective</b>	Prevent leakage of TLA's network information
<b>Risk</b>	T1, T3
<b>Compliance</b>	Failed DNS zone transfers from the DMZ and outside networks Attempt logged by firewall
<b>Testing</b>	<p><b><u>From outside</u></b> <b><u>On outside host</u></b> dig @ins.add.50.1 mydomain.com AXFR</p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• connection time s out</li> <li>• no result is returned</li> </ul> <p><b><u>On syslog server</u></b> tail -f -n0 /var/log/messages   grep ins.add.50.241</p> <p>Confirm:</p>

	<ul style="list-style-type: none"> <li>packets destined for DNS server are denied</li> </ul> <hr/> <b><u>From DMZ</u></b> <b><u>On DMZ host</u></b> dig @ins.add.50.1 mydomain.com AXFR  Confirm: <ul style="list-style-type: none"> <li>connection times out</li> <li>no result is returned</li> </ul> <b><u>On syslog server</u></b> tail -f -n0 /var/log/messages   grep ins.add.50.241  Confirm: <ul style="list-style-type: none"> <li>packets destined for DNS server are denied</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>6</b>
<b>Reference</b>	Spitzner <sup>x</sup> Yuen <sup>x</sup>
<b>Control Objective</b>	Confirm correct firewall filtering operation and integrity of rulebase
<b>Risk</b>	T1, T2, T3, T4
<b>Compliance</b>	Fire wall drops and logs all packets not explicitly permitted by an approved firewall rule . Only permitted packets are received at the destination host.
<b>Testing</b>	nmap using TCP SYN and UDP across the firewall to hosts on higher security networks. The selected host(s) have firewall access-list rules permitting certain packets.  <b><u>From outside to DMZ</u></b> <b><u>Permitted ports</u></b> tcp/135 tcp/137 tcp/139 udp/138 udp/137  <b><u>On outside host</u></b> #stealth SYN scan open ports across the firewall nmap -v -sS -P0 -p1-65535 dmz.add.1.10  #scan UDP open ports across the firewall nmap -v -sU -P0 -p1-65535 dmz.add.1.10  Confirm: <ul style="list-style-type: none"> <li>nmap shows all scanned ports are filtered except permitted ports above</li> </ul> <b><u>On syslog server</u></b>

	<pre>tail -f -n0 /var/log/messages   grep ins.add.50.241</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• firewall drops all packets except permitted ports above</li> </ul> <p><b><u>On DMZ host</u></b>  <pre>tcpdump -nn src host dmz.add.1.140</pre></p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• destination host receives no packets except those to the permitted ports above</li> </ul> <hr/> <p><b><u>From DMZ to inside</u></b>  <b><u>Permitted ports</u></b>  <pre>tcp/137 tcp/139 udp/137 tcp/9100 udp/161</pre></p> <p><b><u>On DMZ host</u></b>  <pre>#stealth SYN scan open ports across the firewall nmap -v -sS -P0 -p1-65535 ins.add.50.1</pre></p> <p><pre>#scan UDP open ports across the firewall nmap -v -sU -P0 -p1-65535 ins.add.50.1</pre></p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• nmap shows all scanned ports are filtered except permitted ports above</li> </ul> <p><b><u>On syslog server</u></b>  <pre>tail -f -n0 /var/log/messages   grep ins.add.50.241</pre></p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• firewall drops all packets except permitted ports above</li> </ul> <p><b><u>On DMZ host</u></b>  <pre>tcpdump -nn src host dmz.add.1.10</pre></p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>• destination host receives no packets except those to the permitted ports above</li> </ul>
<b>Objective/ Subjective</b>	Objective
<b>Control point</b>	<b>7</b>

<b>Reference</b>	Naidu <sup>xi</sup>
<b>Control Objective</b>	Confirm latest operating system image to minimise the risk of known vulnerabilities
<b>Risk</b>	T4, T9
<b>Compliance</b>	Verify the software image version running on the firewall is the latest available from the manufacturer
<b>Testing</b>	<p>Record image version and compare with latest available from manufacturer's support website</p> <p><b><u>On firewall console</u></b></p> <p>show version   include Version</p> <p><b><u>On Cisco Software Centre</u></b>  <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/pix?sort=release%20ASC">http://www.cisco.com/cgi-bin/tablebuild.pl/pix?sort=release%20ASC</a></p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>latest version of Firewall software is running on the firewall</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	8
<b>Reference</b>	Naidu <sup>xii</sup> IANA <sup>xiii</sup>
<b>Control Objective</b>	Confirm only packets from appropriate source addresses can be sent through the firewall
<b>Risk</b>	T4, T10, T11
<b>Compliance</b>	Verify firewall drops spoofed, private (RFC 1918), and illegal address packets
<b>Testing</b>	<p>Use hping2 to spoof source addresses of packets on all attached networks</p> <p>Confirm packets did not reach their destination</p> <p>Confirm packets were dropped by the firewall and logged</p> <p><b><u>From outside host to DMZ</u></b></p> <p><b><u>On outside host</u></b></p> <p>#Standard unroutables  hping2 -a 255.255.255.255 -c 5 --icmp dmz.add.1.10  hping2 -a 127.0.0.1 -c 5 --icmp dmz.add.1.10</p> <p>#Private (RFC 1918) addresses  hping2 -a 10.0.0.10 -c 5 --icmp dmz.add.1.10  hping2 -a 172.16.0.10 -c 5 --icmp dmz.add.1.10  hping2 -a 192.168.0.10 -c 5 --icmp dmz.add.1.10</p> <p>#Multicast address  hping2 -a 224.0.0.7 -c 5 --icmp dmz.add.1.10</p> <p>#Reserved addresses</p>



	<pre>hping2 -a 240.0.0.0 -c 5 --icmp dmz.add.1.10</pre> <p>#Spoofed internal addresses</p> <pre>hping2 -a ins.add.50.10 -c 5 --icmp dmz.add.1.10</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>no responses received by hping2</li> </ul> <p><b><u>On DMZ host</u></b></p> <pre>[user@dmz tmp]# tcpdump -nn 'not port 22 and dst host dmz.add.1.10'</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>no packets received by tcpdump</li> </ul> <p><b><u>On syslog server</u></b></p> <pre>tail -f -n0 messages   grep ins.add.50.241</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>each “ICMP echo request” is denied by an “%PIX -1-106021: Deny icmp reverse path check”</li> </ul> <p><b><u>From DMZ host to inside</u></b></p> <p><b><u>On DMZ host</u></b></p> <pre>#Standard unroutables hping2 -a 255.255.255.255 -c 5 --icmp dmz.add.1.10 hping2 -a 127.0.0.1 -c 5 --icmp dmz.add.1.10</pre> <p>#Private (RFC 1918) addresses</p> <pre>hping2 -a 10.0.0.10 -c 5 --icmp dmz.add.1.10 hping2 -a 172.16.0.10 -c 5 --icmp dmz.add.1.10 hping2 -a 192.168.0.10 -c 5 --icmp dmz.add.1.10</pre> <p>#Multicast address</p> <pre>hping2 -a 224.0.0.7 -c 5 --icmp dmz.add.1.10</pre> <p>#Reserved addresses</p> <pre>hping2 -a 240.0.0.0 -c 5 --icmp dmz.add.1.10</pre> <p>#Spoofed internal addresses</p> <pre>hping2 -a ins.add.50.10 -c 5 --icmp dmz.add.1.10</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>no responses received by hping2</li> </ul> <p><b><u>On Inside host</u></b></p> <pre>[user@dmz tmp]# tcpdump -nn 'not port 22 and dst host ins.add.50.1'</pre>
--	---

	<p>Confirm:</p> <ul style="list-style-type: none"> <li>no packets received by tcpdump</li> </ul> <p><b><u>On syslog server</u></b>  tail -f -n0 messages   grep ins.add.50.241</p> <p>Confirm:</p> <ul style="list-style-type: none"> <li>each “ICMP echo request” is denied by an “%PIX -1-106021: Deny icmp reverse path check”</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>9</b>
<b>Reference</b>	Original contribution
<b>Control Objective</b>	Ensure Developers on the outside network are not subverting network separation controls by connecting to inside networks.
<b>Risk</b>	T1, T2, T3, T13
<b>Compliance</b>	<p>Developers machines are not recorded in the Web content filtering Software Workstation database on the internal networks</p> <ul style="list-style-type: none"> <li>ins.add.50.*</li> <li>ins.add.51.*</li> <li>ins.add.52.*</li> </ul>
<b>Testing</b>	<p>Copy web content filtering server usage database to local workstation from content filtering server.</p> <p>Filter out machines not connected to subnets at this site, and non SOE workstations, laptops and servers by running the following SQL statement in a query window using Microsoft Access.</p> <pre>SELECT Workstations.IP_Address, Workstations.Workstation_Name, Workstations.First_Access, Workstations.Last_Access FROM Workstations WHERE ( ((Workstations.IP_Address) Like " ins.add.50.*" Or (Workstations.IP_Address) Like " ins.add.51.*" Or (Workstations.IP_Address) Like " ins.add.52.*") AND ((Workstations.Workstation_Name) Not Like " DK#####" And (Workstations.Workstation_Name) Not Like "LP #####" And (Workstations.Workstation_Name) Not Like "?? -??-.*") );</pre> <p>Confirm:</p> <ul style="list-style-type: none"> <li>query returns no records</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>10</b>
----------------------	-----------

<b>Reference</b>	Yuen <sup>xiv</sup>
<b>Control Objective</b>	Ensure no significant firewall software bugs are in the running software image
<b>Risk</b>	T4
<b>Compliance</b>	No significant software bugs reported for PIX OS 6.3(1)
<b>Testing</b>	<p>Review Cisco bug tool ( <a href="http://www.cisco.com/cgi-bin/Support/Bugtool/bugnav2.pl?swver1=&amp;fset1=&amp;severity1=&amp;resultsperpage1=&amp;target1=&amp;train1=&amp;swver=6.3&amp;target=1&amp;train=&amp;mdf_label=Cisco+PIX+500+Series+Firewalls&amp;swver2=6.3&amp;target2=1&amp;keyw=&amp;operator=and&amp;resultsperpage=50&amp;severity=%3C%3D+3&amp;Submit=+++Next+++&amp;cc_product=PIX+Firewall">http://www.cisco.com/cgi-bin/Support/Bugtool/bugnav2.pl?swver1=&amp;fset1=&amp;severity1=&amp;resultsperpage1=&amp;target1=&amp;train1=&amp;swver=6.3&amp;target=1&amp;train=&amp;mdf_label=Cisco+PIX+500+Series+Firewalls&amp;swver2=6.3&amp;target2=1&amp;keyw=&amp;operator=and&amp;resultsperpage=50&amp;severity=%3C%3D+3&amp;Submit=+++Next+++&amp;cc_product=PIX+Firewall</a>)– (requires CCO login )</p> <p>Review Bugtraq (<a href="http://www.securityfocus.com/search?submit=yes&amp;category=23&amp;order=DESC&amp;query=pix">http://www.securityfocus.com/search?submit=yes&amp;category=23&amp;order=DESC&amp;query=pix</a> )</p> <p>Review CERT Vulnerabilities (<a href="http://www.kb.cert.org/vuls">http://www.kb.cert.org/vuls</a> )</p> <ul style="list-style-type: none"> <li>Keywords – Cisco firewall, PIX</li> </ul> <p>Review Cisco PIX Firewall Release Notes Version 6.3 – Open Caveats section</p> <p>(<a href="http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63notes/pixrn63.htm#32434">http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63notes/pixrn63.htm#32434</a> )</p>
<b>Objective/ Subjective</b>	Subjective (significance)

<b>Control point</b>	11
<b>Reference</b>	Own contribution, Cisco Systems <sup>xv</sup>
<b>Control Objective</b>	Ensure the firewall logs events at the correct time
<b>Risk</b>	T1, T2, T3
<b>Compliance</b>	<p>The firewall is synced to an accurate NTP server</p> <p>Ensure “logging timestamp” command in the configuration,</p> <p>Ensure events logged on the syslog server have the firewalls timestamp in each record</p> <p>Ensure “clock timezone zone nn” is set in PIX configuration</p>
<b>Testing</b>	<p><b><u>The firewall is synced to an accurate NTP server</u></b>  <b><u>On firewall</u></b>  show ntp status</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>Output states “Clock is synchronized” to ins.add.50.1</li> </ul> <p><b><u>“logging timestamp” command in the configuration</u></b>  <b><u>On firewall</u></b>  show running   include timestamp</p>

	<p>Ensure:</p> <ul style="list-style-type: none"> <li>Output includes “logging timestamp” statement</li> </ul> <p><b><u>Events logged on the syslog server have the firewalls timestamp in each record</u></b></p> <p><b><u>On syslog server</u></b> tail -n0 -f messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>Synchronised time appears twice per log entry</li> </ul> <p><b>“clock timezone zone nn” command is in firewall configuration</b></p> <p><b><u>On Firewall</u></b> <b>“clock timezone zone nn” command is in firewall configuration</b></p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>“clock timezone zone nn” statement is in the output.</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>12</b>
<b>Reference</b>	Naidu <sup>xvi</sup> , Yuen <sup>xvii</sup>
<b>Control Objective</b>	Ensure the firewall rules cannot be circumvented by flaws in the state table
<b>Risk</b>	T4
<b>Compliance</b>	Session state is appropriately maintained by firewall and does not permit sessions initiated with ACK packets
<b>Testing</b>	<p>Session state is appropriately maintained by firewall and does not permit sessions initiated with ACK packets</p> <p>Nmap with ACK packets from outside and DMZ segments to inside segment</p> <p>Confirm no packets received by target</p> <p>Confirm nmap reports all ports filtered</p> <p><b><u>On outside host</u></b> nmap -P0 -sA ins.add.50.1</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>nmap reports all ports are filtered</li> </ul> <p><b><u>On target host</u></b> tcpdump -nn 'src host dmz.add.1.140'</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>tcpdump reports 0 packets received by filter</li> </ul> <hr/> <p><b><u>On DMZ server</u></b> nmap -P0 -sA ins.add.50.1</p> <p>Ensure:</p>

	<ul style="list-style-type: none"> <li>nmap reports all ports are filtered</li> </ul> <p><b><u>On target host</u></b>  [user@inside log]# tcpdump -nn 'src host dmz.add.1.10'  Ensure:</p> <ul style="list-style-type: none"> <li>tcpdump reports 0 packets received by filter</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	13
<b>Reference</b>	
<b>Control Objective</b>	Ensure inbuilt IDS is functioning and logging
<b>Risk</b>	T2
<b>Compliance</b>	Syslog records attack and firewall drops packet (if appropriate)
<b>Testing</b>	<p><b><u>Land attack</u></b>  <b><u>Outside to DMZ</u></b>  <b><u>On outside host</u></b>  hping2 -a dmz.add.1.10 -S -c 2 dmz.add.1.10</p> <p><b><u>On target host</u></b>  tcpdump -nn net sub.net.0.0/8</p> <p><b><u>On syslog server</u></b>  tail -f /var/log/messages   grep ins.add.50.24 1</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>syslog reports LAND ATTACK</li> <li>syslog reports packets dropped</li> <li>hping2 reports 100% packet loss</li> <li>tcpdump reports no packets from source host</li> </ul> <p><b><u>DMZ to inside</u></b>  <b><u>On DMZ host</u></b>  hping2 -a ins.add.50.1 -S -c 2 ins.add.50.1</p> <p><b><u>On target host</u></b>  tcpdump -nn net sub.net.0.0/8</p> <p><b><u>On syslog server</u></b>  tail -f /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>syslog reports LAND ATTACK</li> <li>syslog reports packets dropped</li> <li>hping2 reports 100% packet loss</li> <li>tcpdump reports no packets from source host</li> </ul> <p><b><u>ICMP fragment attack</u></b>  <b><u>Outside to DMZ</u></b></p>

	<p><b><u>On outside host</u></b> hping2 --icmp -d 1024 -f -c 5 dmz.add.1.10</p> <p><b><u>On target host</u></b> tcpdump -nn net sub.net.0.0/8 and not port 22</p> <p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>• syslog reports ICMP fragment</li> <li>• hping2 reports 100% packet loss</li> <li>• tcpdump reports no packets from source host</li> </ul> <p><b><u>DMZ to inside</u></b> <b><u>On DMZ host</u></b> hping2 --icmp -d 1024 -f -c 5 ins.add.50.1</p> <p><b><u>On target host</u></b> tcpdump -nn net sub.net.0.0/8</p> <p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>• syslog reports ICMP fragment</li> <li>• hping2 reports 100% packet loss</li> <li>• tcpdump reports no packets from source host</li> </ul> <hr/> <p><b><u>ICMP large ping packet attack</u></b> <b><u>Outside to DMZ</u></b> <b><u>On outside host</u></b> hping2 --icmp -d 1024 -c 5 dmz.add.1.10</p> <p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>• syslog reports Large ICMP packet</li> </ul> <p><b><u>DMZ to inside</u></b> <b><u>On DMZ host</u></b> hping2 --icmp -d 1024 -c 5 ins.add.50.1</p> <p><b><u>On syslog server</u></b> tail -f /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>• syslog reports Large ICMP packet</li> </ul>
--	--

<b>Objective/ Subjective</b>	Objective
<b>Control point</b>	<b>14</b>
<b>Reference</b>	Naidu <sup>xviii</sup> , Own contribution, IANA <sup>xix</sup>
<b>Control Objective</b>	Minimise the leakage of TLA's data
<b>Risk</b>	T1, T3
<b>Compliance</b>	Ensure ICMP echo -request and ICMP reply are the only ICMP types that can originate from the outside and DMZ segments to more secure segments.
<b>Testing</b>	<p>From the outside and DMZ networks use hping2 with two other types of ICMP types to ping across the firewall.</p> <p>Confirm the packets are dropped and logged by the firewall</p> <p>Confirm the packets are not received at the destination host with tcpdump.</p> <p><b><u>From outside &amp; DMZ host</u></b>  #icmp timestamp request  hping2 --icmp-ts -c 2 ins.add.50.1  #icmp address-mask request  hping2 --icmp-addr -c 2 ins.add.50.1</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>• 100% packet loss</li> </ul> <p><b><u>On destination host</u></b>  #remove lots of noise as this is the syslog &amp; ntp server  tcpdump -nn src net.sub.net.0.0/8 and not port 22 and not arp and not udp port 123 and not udp port 138 and not udp port 514  Ensure:</p> <ul style="list-style-type: none"> <li>• no ping packets received on destination host</li> </ul> <p><b><u>On syslog server</u></b>  tail -f -n0 /var/log/messages   grep ins.add.50.241  Ensure:</p> <ul style="list-style-type: none"> <li>• icmp timestamp request logged and dropped by firewall</li> <li>• icmp mask request logged and dropped by firewall</li> </ul> <hr/> <p><b><u>From DMZ to inside</u></b>  <b><u>On DMZ host</u></b>  #icmp timestamp request  hping2 --icmp-ts -c 2 ins.add.50.1  #icmp address-mask request  hping2 --icmp-addr -c 2 ins.add.50.1  Ensure:</p> <ul style="list-style-type: none"> <li>• 100% packet loss</li> </ul> <p><b><u>On destination host (inside)</u></b></p>

	<pre>#remove the noise as this is the syslog and ntp server tcpdump -nn src net.sub.net.0.0/8 and not port 22 and not arp and not udp port 123 and not udp port 138 and not udp port 514 tcpdump: listening on eth0</pre> <p>Ensure:</p> <ul style="list-style-type: none"> <li>no ping packets received on destination host</li> </ul> <p><b><u>On syslog server</u></b>  tail -f -n0 /var/log/messages   grep ins.add.50.241</p> <p>Ensure:</p> <ul style="list-style-type: none"> <li>icmp timestamp request logged and dropped by firewall</li> <li>icmp mask request logged and dropped by firewall</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>15</b>
<b>Reference</b>	Yuen <sup>xx</sup> , Own contribution
<b>Control Objective</b>	Ensure firewall integrity through permitting encrypted administration protocols only
<b>Risk</b>	T8
<b>Compliance</b>	<p>Confirm http and telnet are disabled through configuration review and testing from all interfaces.</p> <p>Connect to firewall via secure protocols ssh and https</p> <p>TCP nmap of all firewall interfaces should only show ssh and https ports open on the inside interface</p>
<b>Testing</b>	<p><b><u>On firewall</u></b>  show http  Ensure:</p> <ul style="list-style-type: none"> <li>http server enabled</li> <li>http server access from inside interface only</li> <li>http server access from 24 bit subnet</li> </ul> <p>show telnet  Ensure:</p> <ul style="list-style-type: none"> <li>null response</li> </ul> <p>show ssh  Ensure:</p> <ul style="list-style-type: none"> <li>ssh access from inside interface</li> <li>ssh access from 24 bit subnet</li> </ul> <p><b><u>On inside host</u></b>  telnet ins.add.50.241  Ensure:</p> <ul style="list-style-type: none"> <li>connection is refused</li> </ul>



telnet ins.add.50.241 80

Ensure:

- connection is refused

nmap -sT -P0 -p1-65535 ins.add.50.241

Ensure:

- Port 22/tcp is open
- Port 443/tcp is open
- All other ports are closed

ssh -c des admin@ins.add.50.241

Ensure:

- Connection is established
- Encryption is DES or 3DES

### **On DMZ host**

telnet dmz.add.1.1

Ensure:

- connection is refused

telnet dmz.add.1.1 80

Ensure:

- connection is refused

ssh -c des admin@dmz.add.1.1

Ensure:

- connection is refused

nmap -sT -P0 -p1-65535 dmz.add.1.1

Ensure:

- All 65535 ports are closed

### **On outside host**

telnet dmz.add.1.129

Ensure:

- connection is refused

telnet dmz.add.1.129 80

Ensure:

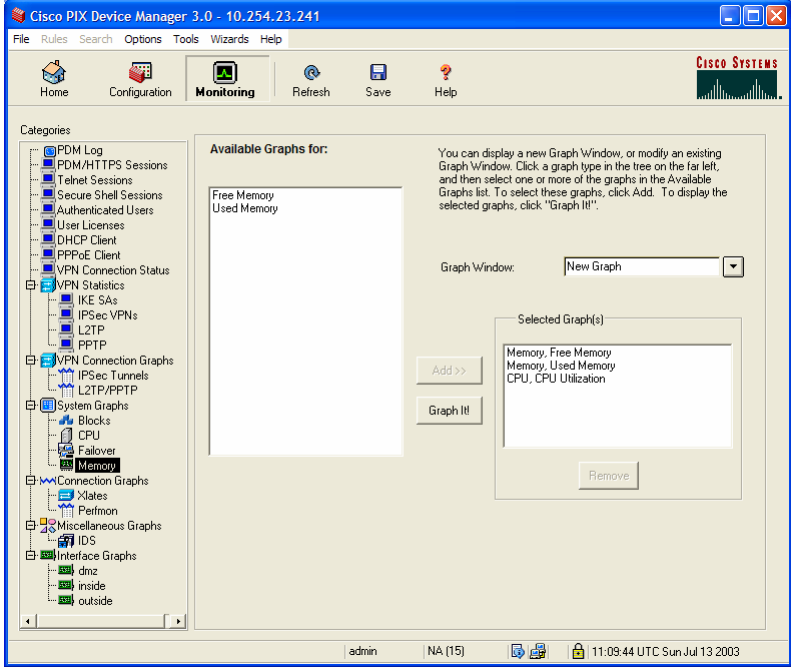
	<ul style="list-style-type: none"> <li>connection is refused</li> </ul> <pre>nmap -sT -P0 -p1-65535 dmz.add.1.129</pre> <p>Ensure:</p> <ul style="list-style-type: none"> <li>All 65535 ports are closed</li> </ul> <pre>ssh -c des admin@dmz.add.1.129</pre> <p>Ensure:</p> <ul style="list-style-type: none"> <li>Ssh connection is denied</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>16</b>
<b>Reference</b>	Own contribution
<b>Control Objective</b>	Ensure traceability of firewall logs. PIX will log using name instruction to the log file. (Name is the name command as known to the local PIX and subject to configuration change, and could clash with DNS entry causing confusion. Problem akin to using a hosts file)
<b>Risk</b>	T1, T7
<b>Compliance</b>	Confirm no name commands in firewall configuration and no names logged in log file
<b>Testing</b>	<p><b><u>On firewall</u></b></p> <pre>show run   grep ^name   exclude nameif</pre> <p>Ensure:</p> <ul style="list-style-type: none"> <li>null response</li> </ul> <p><b><u>On *nix host</u></b></p> <p>Copy syslog file to temporary directory</p> <p>Run following script in temporary directory</p> <p>Record number of words found</p> <hr/> <pre>#!/bin/sh #remove temp files rm messages.1 messages.2  #grep out interesting lines to temp file grep 'ins.add.50.241' messages   grep Deny   grep src   grep dst &gt; messages.1  #remove all uninteresting fields cut -d " " -f13,15 messages.1 &gt; messages.2  #remove all known words &amp; count words (names) remaining sed -e 's/outside://' -e 's/inside://' -e 's/dmz://' -e 's/[0-9]//g' -e 's/./g' -e 's/\\/g' -e 's/ //g' -e 's/n/' messages.2   wc -w</pre>

	Ensure: <ul style="list-style-type: none"> <li>result is 0</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>17</b>
<b>Reference</b>	Own contribution , Northcutt <sup>xxi</sup>
<b>Control Objective</b>	Rule base can be easily read by administrators therefore minimising the chance of misunderstanding the purpose of a rule
<b>Risk</b>	T6, T7
<b>Compliance</b>	Confirm each rule has valid description and change number
<b>Testing</b>	Have the system administrator show informative descriptions with Change Number in the rulebase for each rule . Ensure: <ul style="list-style-type: none"> <li>each rule has a preceding access -list &lt;acl-name&gt; remark line</li> </ul>
<b>Objective/ Subjective</b>	Objective

<b>Control point</b>	<b>18</b>
<b>Reference</b>	Lance Spitzner <sup>xxii</sup>
<b>Control Objective</b>	Ensure firewall operating stability
<b>Risk</b>	T2, T9
<b>Compliance</b>	Firewall stability is not compromised by a DOS attack
<b>Testing</b>	Record memory and CPU utilisation on firewall with Cisco PIX Device Manager (PDM). 1) <a href="https://ins.add.50.241">https://ins.add.50.241</a> (firewall inside interface) with Internet Explorer 2) Select the monitoring button 3) Select <ul style="list-style-type: none"> <li>a) System graph <ul style="list-style-type: none"> <li>i) CPU <ul style="list-style-type: none"> <li>(1) CPU Utilisation</li> <li>(2) Add</li> </ul> </li> <li>ii) Memory <ul style="list-style-type: none"> <li>(1) Free memory</li> <li>(2) Add</li> <li>(3) Used memory</li> <li>(4) Add</li> </ul> </li> </ul> </li> <li>b) Graph it</li> </ul>

	 <p>Launch Nessus DOS attacks from the outside and inside networks against the local firewall interface.</p> <p>Include the following plug-in families:</p> <ul style="list-style-type: none"> <li>• Cisco</li> <li>• DOS</li> <li>• Gain a shell remotely</li> <li>• Gain root remotely</li> <li>• General</li> </ul> <p>Deselect all port scanners</p> <p>Review log firewall files for critical errors and confirm firewall memory and utilisation not significantly degraded</p>
<b>Objective/ Subjective</b>	<p>Log file review – Objective</p> <p>Memory and utilisation – Subjective</p>

<b>Control point</b>	<b>19</b>
<b>Reference</b>	Own contribution, Cisco Systems <sup>xxiii</sup> , Northcutt <sup>xxiv</sup>
<b>Control Objective</b>	Ensure firewall configuration can be restored in the event of configuration corruption or hardware failure.
<b>Risk</b>	T8, T10, T11, T12
<b>Compliance</b>	Administrator can show method of saving configuration post change and compare saved configuration and running configuration.
<b>Testing</b>	Administrator demonstrates repeatable process for saving configuration and explains process for restoring configuration. Ensure:

	<ul style="list-style-type: none"> <li>Process is written and repeatable</li> </ul> <p><b><u>On Firewall</u></b> write net ins.add.50.1:pixfirewall</p> <p><b><u>On *nux host</u></b> Diff pixfirewall pixfirewall .stored.configuration Ensure:</p> <ul style="list-style-type: none"> <li>No configuration differences reported.</li> </ul>
<b>Objective/ Subjective</b>	Diff – Objective, Repeatable process – Subjective

<b>Control point</b>	<b>20</b>
<b>Reference</b>	Own contribution , Northcutt <sup>xxv</sup>
<b>Control Objective</b>	Ensure firewall rules are relevant to the current situation
<b>Risk</b>	T5, T6, T7
<b>Compliance</b>	Record access-list hit counts over consecutive weeks for at least three periods.
<b>Testing</b>	On firewall – show access-list   include hitcnt  Record in log file and compare with next weeks results
<b>Objective/ Subjective</b>	Objective

Table showing threats mitigated by control points

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13
Cp1	*	*	*							*	*		
Cp2													*
Cp3	*	*	*		*	*	*			*	*		
Cp4	*	*	*										
Cp5	*		*										
Cp6	*	*	*	*									
Cp7				*					*				
Cp8				*						*	*		
Cp9	*	*	*										*
Cp10				*									
Cp11	*	*	*										
Cp12				*									
Cp13		*											
Cp14	*		*										
Cp15								*					
Cp16	*						*						
Cp17						*	*						
Cp18		*							*				
Cp19								*		*	*	*	
Cp20					*	*	*						

\* denotes checkpoint address this threat

## Assignment 3

### The audit

#### Note:

- 1) To facilitate the audit and testing a machine in the DMZ network was replaced with a RedHat Linux 7.3 workstation. After the audit the original server was placed back in the DMZ network.
- 2) Written approval was given by the Information Security Manager of TLA Enterprises to conduct the audit, and to replace the workstation as outlined above.
- 3) Syntax used in audit test and findings
  - a. Failures are indicated by **yellow highlighting**
  - b. **Bold** indicates key points of success
  - c. **Bold and underline** is a heading

Control Point	2															
Control Objective	Ensure all DMZ users (from third party developers ) are aware of, and comply with policy of network separation.															
Test and findings	<p><b><u>Survey</u></b></p> <p>1. Are you aware of the need and reasons for the networks to be separated?</p> <p>Yes No</p> <p>Reasons:</p> <p>1.</p> <p>2.</p> <p>3.</p> <p>2. Was this communicated to you in a timely manner when you started on site?</p> <p>Yes No</p> <p>3. Are there any circu mstances in your time on site that have led to wishing to be directly connected to the corporate network?</p> <p>Yes No</p> <p>4. Are you permitted to connect to YOUR corporate LAN or other networks whilst connected to the TLA’s network</p> <p>Yes No</p> <table><tr><td><b>Question</b></td><td><b>1</b></td><td><b>2</b></td><td><b>3</b></td><td><b>4</b></td></tr><tr><td><b>Preferred answer</b></td><td><b>Yes</b></td><td><b>Yes</b></td><td><b>No</b></td><td><b>No</b></td></tr><tr><td>Respondent 1</td><td>No</td><td>Yes</td><td>Yes</td><td>Yes</td></tr></table>	<b>Question</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>Preferred answer</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>	<b>No</b>	Respondent 1	No	Yes	Yes	Yes
<b>Question</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>												
<b>Preferred answer</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>	<b>No</b>												
Respondent 1	No	Yes	Yes	Yes												

	<p>Respondent 2      Yes    Yes    Yes    No</p> <p>Respondent 3      Yes    Yes    No    No</p> <p>Respondent 4      Yes    Yes    No    No</p> <p>Respondent 5      Yes    No    Yes    No</p> <p>Respondent 6      No    No    No    Yes</p> <p>Respondent 7      Yes    Yes    No    No</p> <p>Respondent 8      Yes    Yes    No    No</p> <p>Respondent 9      Yes    Yes    Yes    No</p> <p>Respondent 10      Yes    Yes    No    Yes</p> <p>Respondent 11      No    No    No    No</p> <p>Respondent 12      Yes    Yes    Yes    Yes</p> <p>Respondent 13      Yes    No    Yes    No</p> <p>Respondent 14      Yes    Yes    Yes    No</p> <p>Respondent 15      No    No    No    No</p> <p>Respondent 16      Yes    Yes    No    No</p> <p>Respondent 17      Yes    Yes    No    Yes</p> <p>Respondent 18      Yes    Yes    No    Yes</p> <p>Respondent 19      Yes    Yes    No    Yes</p> <p>Respondent 20      Yes    Yes    No    Yes</p> <p>Respondent 21      Yes    Yes    No    No</p> <p>Respondent 22      Yes    No    Yes    No</p> <p>Respondent 23      No    Yes    Yes    No</p> <p>Respondent 24      No    Yes    Yes    No</p> <p>Respondent 25      Yes    No    Yes    No</p> <p>Respondent 26      Yes    No    No    No</p> <p><b>Responded with preferred answer</b>      <b>77%    69%    58%    69%</b></p>
Compliance	<p><b>1: Fail; 2: Fail; 3: Fail; 4: Fail</b></p> <ul style="list-style-type: none"> <li>All results &lt; 80% favourable</li> </ul>
Compliance	<b>Fail</b>

<b>Control Point</b>	<b>7</b>
Control Objective	Confirm latest software image to minimise the risk of known vulnerabilities
Test and findings	<p><u><b>On firewall console</b></u></p> <pre>pixfirewall# show version   include Version Cisco PIX Firewall Version 6.3(1) Cisco PIX Device Manager Version 3.0(1)</pre> <p><u><b>On Cisco Software Centre</b></u></p> <p><a href="http://www.cisco.com/cgi-bin/tablebuild.pl/pix?sort=release%20ASC">http://www.cisco.com/cgi-bin/tablebuild.pl/pix?sort=release%20ASC</a></p>



Select a File to Download

Sort by:

Filename	Release	Date	Size (Bytes)
<a href="#">pix631.bin</a> Binary REQUIRES 32 MB RAM AND 8MB FLASH	6.3.1.ED	25-MAR-2003	2045952
<a href="#">pix622.bin</a> Binary REQUIRES 32 MB RAM AND 8MB FLASH	6.2.2.ED	28-JUN-2002	1658880
<a href="#">pix614.bin</a> Binary REQUIRES 32 MB RAM AND 8MB FLASH	6.1.4.GD	15-JUL-2002	2598912
<a href="#">bh61.bin</a> Boot Helper Binary	6.1.1.ED	17-SEP-2001	221184

Compliance

**Pass**

Note running ED (Early Deployment) software. A more conservative option would be to run Version 6.1(4)GD (General Deployment) software, however 6.1(4) is almost one year old.

<b>Control Point</b>	<b>8</b>
<b>Control Objective</b>	Confirm only packets from appropriate source addresses can be sent through the firewall
<b>Test and findings</b>	<p>Verify only packets from appropriate source addresses can be sent through the firewall</p> <p>Use hping2 to spoof source addresses of packets on all attached networks</p> <p>Confirm packets did not reach their destination</p> <p>Confirm packets were dropped by the firewall and logged</p> <p><u><b>From outside host to DMZ</b></u></p> <p><u><b>On outside host</b></u></p> <pre>[user@outside tmp]# cat test8 #Standard unroutables hping2 -a 255.255.255.255 -c 5 --icmp dmz.add.1.10 hping2 -a 127.0.0.1 -c 5 --icmp dmz.add.1.10  #Private (RFC 1918) addresses hping2 -a 10.0.0.10 -c 5 --icmp dmz.add.1.10 hping2 -a 172.16.0.10 -c 5 --icmp dmz.add.1.10 hping2 -a 192.168.0.10 -c 5 --icmp dmz.add.1.10  #Multicast address hping2 -a 224.0.0.7 -c 5 --icmp dmz.add.1.10  #Reserved addresses hping2 -a 240.0.0.0 -c 5 --icmp dmz.add.1.10  #Spoofed internal addresses hping2 -a ins.add.50.10 -c 5 --icmp dmz.add.1.10 [user@outside tmp]# ./test8</pre>

	<pre> HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms HPING dmz.add.1.10 (eth0 dmz.add.1.10): icmp mode set, 28 headers + 0 data bytes  --- dmz.add.1.10 hping statistic --- 5 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms </pre> <p><b><u>On DMZ host</u></b></p>
--	--

	<pre>[user@dmz tmp]# tcpdump -nn 'not port 22 and dst host dmz.add.1.10'</pre> <p>tcpdump: listening on eth0</p> <p><b>0 packets received by filter</b>  <b>0 packets dropped by kernel</b></p> <pre>[user@dmz tmp]#</pre> <p><u>syslog server</u></p> <pre>tail -f -n0 messages   grep ins.add.50.241</pre> <pre>[user@inside log]# tail -f -n0 messages   grep ins.add.50.241</pre> <p>Jul 11 16:50:13 ins.add.50.241 Jul 11 2003 06:50:13: %PIX -4-400014:  IDS:2004 ICMP echo request from 255.255.255.255 to dmz.add.1.10 on  interface outside</p> <p>Jul 11 16:50:13 ins.add.50.241 Jul 11 2003 06:50:13: %PIX -2-106016: Deny IP  spooof from (255.255.255.255) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:14 ins.add.50.241 Jul 11 2003 06:50:14: %PIX -4-400014:  IDS:2004 ICMP echo request from 255.255.255.255 to dmz.add.1.10 on  interface outside</p> <p>Jul 11 16:50:14 ins.add.50.241 Jul 11 2003 06:50:14: %PIX -2-106016: Deny IP  spooof from (255.255.255.255) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:15 ins.add.50.241 Jul 11 2003 06:50:15: %PIX -4-400014:  IDS:2004 ICMP echo request from 255.255.255.255 to dmz.add.1.10 on  interface outside</p> <p>Jul 11 16:50:15 ins.add.50.241 Jul 11 2003 06:50:15: %PIX -2-106016: Deny IP  spooof from (255.255.255.255) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:16 ins.add.50.241 Jul 11 2003 06:50:16: %PIX -4-400014:  IDS:2004 ICMP echo request from 255.255.255.255 to dmz.add.1.10 on  interface outside</p> <p>Jul 11 16:50:16 ins.add.50.241 Jul 11 2003 06:50:16: %PIX -2-106016: Deny IP  spooof from (255.255.255.255) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:17 ins.add.50.241 Jul 11 2003 06:50:17: %PIX -4-400014:  IDS:2004 ICMP echo request from 255.255.255.255 to dmz.add.1.10 on  interface outside</p> <p>Jul 11 16:50:17 ins.add.50.241 Jul 11 2003 06:50:17: %PIX -2-106016: Deny IP  spooof from (255.255.255.255) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:27 ins.add.50.241 Jul 11 2003 06:50:27: %PIX -4-400014:  IDS:2004 ICMP echo request from 127.0.0.1 to dmz.add.1.10 on interface  outside</p> <p>Jul 11 16:50:27 ins.add.50.241 Jul 11 2003 06:50:27: %PIX -2-106016: Deny IP  spooof from (127.0.0.1) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:28 ins.add.50.241 Jul 11 2003 06:50:28: %PIX -4-400014:  IDS:2004 ICMP echo request from 127.0.0.1 to dmz.add.1.10 on interface  outside</p> <p>Jul 11 16:50:28 ins.add.50.241 Jul 11 2003 06:50:28: %PIX -2-106016: Deny IP  spooof from (127.0.0.1) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:29 ins.add.50.241 Jul 11 2003 06:50:29: %PIX -4-400014:  IDS:2004 ICMP echo request from 127.0.0.1 to dmz.add.1.10 on interface  outside</p> <p>Jul 11 16:50:29 ins.add.50.241 Jul 11 2003 06:50:29: %PIX -2-106016: Deny IP  spooof from (127.0.0.1) to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:50:30 ins.add.50.241 Jul 11 2003 06:50:30: %PIX -4-400014:</p>
--	---

	IDS:2004 ICMP echo request from 127.0.0.1 to dmz.add.1.10 on interface outside Jul 11 16:50:30 ins.add.50.241 Jul 11 2003 06:50:30: %PIX -2-106016: Deny IP spoof from (127.0.0.1) to dmz.add.1.10 on interface outside Jul 11 16:50:31 ins.add.50.241 Jul 11 2003 06:50:31: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to dmz.add.1.10 on interface outside Jul 11 16:50:31 ins.add.50.241 Jul 11 2003 06:50:31: %P IX-2-106016: Deny IP spoof from (127.0.0.1) to dmz.add.1.10 on interface outside Jul 11 16:50:41 ins.add.50.241 Jul 11 2003 06:50:41: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:41 ins.add.50.241 Jul 11 2003 06:50:41: %PIX -1-106021: Deny icmp reverse path check from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:42 ins.add.50.241 Jul 11 2003 06:50:42: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:42 ins.add.50.241 Jul 11 2003 06:50:42: %PIX -1-106021: Deny icmp reverse path check from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:43 ins.add.50.241 Jul 11 2003 06:50:43: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:43 ins.add.50.241 Jul 11 2003 06:50:43: %PIX -1-106021: Deny icmp reverse path check from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:44 ins.add.50.241 Jul 11 2003 06:50:44: %P IX-4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:44 ins.add.50.241 Jul 11 2003 06:50:44: %PIX -1-106021: Deny icmp reverse path check from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:45 ins.add.50.241 Jul 11 2003 06:50:45: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:45 ins.add.50.241 Jul 11 2003 06:50:45: %PIX -1-106021: Deny icmp reverse path check from 10.0.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:55 ins.add.50.241 Jul 11 2003 06:50:55: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:55 ins.add.50.241 Jul 11 2003 06:50:55: %PIX -1-106021: Deny icmp reverse path check from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:56 ins.add.50.241 Jul 11 2003 06:50:56: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:56 ins.add.50.241 Jul 11 2003 06:50:56: %PIX -1-106021: Deny icmp reverse path check from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:57 ins.add.50.241 Jul 11 2003 06:50:57: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:57 ins.add.50.241 Jul 11 2003 06:50:57: %PIX -1-106021: Deny icmp reverse path check from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:58 ins.add.50.241 Jul 11 2003 06:50:58: %PIX -4-400014:
--	---

	IDS:2004 ICMP echo request from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:58 ins.add.50.241 Jul 11 2003 06:50:58: %PIX -1-106021: Deny icmp reverse path check from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:59 ins.add.50.241 Jul 11 2003 06:50:59: %P IX-4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:50:59 ins.add.50.241 Jul 11 2003 06:50:59: %PIX -1-106021: Deny icmp reverse path check from 172.16.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:09 ins.add.50.241 Jul 11 2003 06:51:09: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:09 ins.add.50.241 Jul 11 2003 06:51:09: %PIX -1-106021: Deny icmp reverse path check from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:10 ins.add.50.241 Jul 11 2003 06:51:10: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:10 ins.add.50.241 Jul 11 2003 06:51:10: %PIX -1-106021: Deny icmp reverse path check from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:11 ins.add.50.241 Jul 11 2003 06:51:11: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:11 ins.add.50.241 Jul 11 2003 06:51:11: %PIX -1-106021: Deny icmp reverse path check from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:12 ins.add.50.241 Jul 11 2003 06:51:12: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:12 ins.add.50.241 Jul 11 2003 06:51:12: %PIX -1-106021: Deny icmp reverse path check from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:13 ins.add.50.241 Jul 11 2003 06:51:13: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:13 ins.add.50.241 Jul 11 2003 06:51:13: %PIX -1-106021: Deny icmp reverse path check from 192.168.0.10 to dmz.add.1.10 on interface outside Jul 11 16:51:23 ins.add.50.241 Jul 11 2003 06:51:23: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:23 ins.add.50.241 Jul 11 2003 06:51:23: %PIX -1-106021: Deny icmp reverse path check from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:24 ins.add.50.241 Jul 11 2003 06:51:24: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:24 ins.add.50.241 Jul 11 2003 06:51:24: %PIX -1-106021: Deny icmp reverse path check from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:25 ins.add.50.241 Jul 11 2003 06:51:25: %PIX -4-400014:
--	---

	IDS:2004 ICMP echo request from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:25 ins.add.50.241 Jul 11 2003 06:51:25: %PIX -1-106021: Deny icmp reverse path check from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:26 ins.add.50.241 Jul 11 2003 06:51:26: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:26 ins.add.50.241 Jul 11 2003 06:51:26: %PIX -1-106021: Deny icmp reverse path check from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:27 ins.add.50.241 Jul 11 2003 06:51:27: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:27 ins.add.50.241 Jul 11 2003 06:51:27: %PIX -1-106021: Deny icmp reverse path check from 224.0.0.7 to dmz.add.1.10 on interface outside Jul 11 16:51:37 ins.add.50.241 Jul 11 2003 06:51:37: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:37 ins.add.50.241 Jul 11 2003 06:51:37: %PIX -1-106021: Deny icmp reverse path check from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:38 ins.add.50.241 Jul 11 2003 06:51:38: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:38 ins.add.50.241 Jul 11 2003 06:51:38: %PIX -1-106021: Deny icmp reverse path check from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:39 ins.add.50.241 Jul 11 2003 06:51:39: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:39 ins.add.50.241 Jul 11 2003 06:51:39: %PIX -1-106021: Deny icmp reverse path check from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:40 ins.add.50.241 Jul 11 2003 06:51:40: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:40 ins.add.50.241 Jul 11 2003 06:51:40: %PIX -1-106021: Deny icmp reverse path check from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:41 ins.add.50.241 Jul 11 2003 06:51:41: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:41 ins.add.50.241 Jul 11 2003 06:51:41: %PIX -1-106021: Deny icmp reverse path check from 240.0.0.0 to dmz.add.1.10 on interface outside Jul 11 16:51:51 ins.add.50.241 Jul 11 2003 06:51:51: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to dmz.add.1.10 on interface outside Jul 11 16:51:51 ins.add.50.241 Jul 11 2003 06:51:51: %PIX -1-106021: Deny icmp reverse path check from ins.add.50.10 to dmz.add.1.10 on interface outside Jul 11 16:51:52 ins.add.50.241 Jul 11 2003 06:51:52: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to dmz.add.1.10 on interface outside Jul 11 16:51:52 ins.add.50.241 Jul 11 2003 06:51:52: %PIX -1-106021: Deny icmp reverse path check from ins.add.50.10 to dmz.add.1.10 on interface
--	---

	<p>outside</p> <p>Jul 11 16:51:53 ins.add.50.241 Jul 11 2003 06:51:53: %PIX-4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:51:53 ins.add.50.241 Jul 11 2003 06:51:53: %PIX -1-106021: Deny icmp reverse path check from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:51:54 ins.add.50.241 Jul 11 2003 06:51:54: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:51:54 ins.add.50.241 Jul 11 2003 06:51:54: %PIX -1-106021: Deny icmp reverse path check from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:51:55 ins.add.50.241 Jul 11 2003 06:51:55: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p>Jul 11 16:51:55 ins.add.50.241 Jul 11 2003 06:51:55: %PIX -1-106021: Deny icmp reverse path check from ins.add.50.10 to dmz.add.1.10 on interface outside</p> <p><b><u>From DMZ to inside</u></b></p> <p><b><u>On DMZ host</u></b></p> <p>[user@dmz tmp]# cat test8</p> <p>#Standard unroutables</p> <p>hping2 -a 255.255.255.255 -c 5 --icmp ins.add.50.1</p> <p>hping2 -a 127.0.0.1 -c 5 --icmp ins.add.50.1</p> <p>#Private (RFC 1918) addresses</p> <p>hping2 -a 10.0.0.10 -c 5 --icmp ins.add.50.1</p> <p>hping2 -a 172.16.0.10 -c 5 --icmp ins.add.50.1</p> <p>hping2 -a 192.168.0.10 -c 5 --icmp ins.add.50.1</p> <p>#Multicast address</p> <p>hping2 -a 224.0.0.7 -c 5 --icmp ins.add.50.1</p> <p>#Reserved addresses</p> <p>hping2 -a 240.0.0.0 -c 5 --icmp ins.add.50.1</p> <p>#Spoofed internal addresses</p> <p>hping2 -a ins.add.50.10 -c 5 --icmp ins.add.50.1</p> <p>[user@dmz tmp]# ./test8</p> <p>HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes</p> <p>---</p> <p>ins.add.50.1 hping statistic ---</p> <p>5 packets tramitted, 0 packets received, 100% packet loss</p> <p>round-trip min/avg/max = 0.0/0.0/0.0 ms</p> <p>HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes</p>
--	--

```
17:02:19.904715 10.0.0.10 > ins.add.50.1: icmp: echo request
17:02:20.886169 10.0.0.10 > ins.add.50.1: icmp: echo request
17:02:21.886504 10.0.0.10 > ins.add.50.1: icmp: echo request
17:02:22.886698 10.0.0.10 > ins.add.50.1: icmp: echo request
17:02:23.886997 10.0.0.10 > ins.add.50.1: icmp: echo request
17:02:33.900175 172.16.0.10 > ins.add.50.1: icmp: echo request
```



```

17:02:34.886894 172.16.0.10 > ins.add.50.1: icmp: echo request
17:02:35.886862 172.16.0.10 > ins.add.50.1: icmp: echo request
17:02:36.884901 172.16.0.10 > ins.add.50.1: icmp: echo request
17:02:37.885669 172.16.0.10 > ins.add.50.1: icmp: echo request
17:02:47.894028 192.168.0.10 > ins.add.50.1: icmp: echo request
17:02:48.885132 192.168.0.10 > ins.add.50.1: icmp: echo request
17:02:49.885736 192.168.0.10 > ins.add.50.1: icmp: echo request
17:02:50.884726 192.168.0.10 > ins.add.50.1: icmp: echo request
17:02:51.884860 192.168.0.10 > ins.add.50.1: icmp: echo request
17:03:01.890206 224.0.0.7 > ins.add.50.1: icmp: echo request
17:03:02.884650 224.0.0.7 > ins.add.50.1: icmp: echo request
17:03:03.884787 224.0.0.7 > ins.add.50.1: icmp: echo request
17:03:04.885103 224.0.0.7 > ins.add.50.1: icmp: echo request
17:03:06.179834 224.0.0.7 > ins.add.50.1: icmp: echo request
17:03:15.902840 240.0.0.0 > ins.add.50.1: icmp: echo request
17:03:16.884936 240.0.0.0 > ins.add.50.1: icmp: echo request
17:03:17.884883 240.0.0.0 > ins.add.50.1: icmp: echo request
17:03:18.884975 240.0.0.0 > ins.add.50.1: icmp: echo request
17:03:19.884784 240.0.0.0 > ins.add.50.1: icmp: echo request
17:03:29.898547 ins.add.50.10 > ins.add.50.1: icmp: echo request
17:03:30.884328 ins.add.50.10 > ins.add.50.1: icmp: echo request
17:03:31.884199 ins.add.50.10 > ins.add.50.1: icmp: echo request
17:03:32.884190 ins.add.50.10 > ins.add.50.1: icmp: echo request
17:03:33.884110 ins.add.50.10 > ins.add.50.1: icmp: echo request

```

30 packets received by filter

0 packets dropped by kernel

#### On syslog server

```
[user@inside log]# tail -f -n0 messages | grep ins.add.50.241
```

```
Jul 11 17:01:51 ins.add.50.241 Jul 11 2003 07:01:51: %PIX-4-400014:
```

```
IDS:2004 ICMP echo request from 255.255.255.255 to ins.add.50.1 on
interface dmz
```

```
Jul 11 17:01:51 ins.add.50.241 Jul 11 2003 07:01:51: %PIX-2-106016: Deny IP
spooof from (255.255.255.255) to ins.add.50.1 on interface dmz
```

```
Jul 11 17:01:52 ins.add.50.241 Jul 11 2003 07:01:52: %PIX-4-400014:
```

```
IDS:2004 ICMP echo request from 255.255.255.255 to ins.add.50.1 on
interface dmz
```

```
Jul 11 17:01:52 ins.add.50.241 Jul 11 2003 07:01:52: %PIX-2-106016: Deny IP
spooof from (255.255.255.255) to ins.add.50.1 on interface dmz
```

```
Jul 11 17:01:53 ins.add.50.241 Jul 11 2003 07:01:53: %PIX-4-400014:
```

```
IDS:2004 ICMP echo request from 255.255.255.255 to ins.add.50.1 on
interface dmz
```

```
Jul 11 17:01:53 ins.add.50.241 Jul 11 2003 07:01:53: %PIX-2-106016: Deny IP
spooof from (255.255.255.255) to ins.add.50.1 on interface dmz
```

```
Jul 11 17:01:54 ins.add.50.241 Jul 11 2003 07:01:54: %PIX-4-400014:
```

```
IDS:2004 ICMP echo request from 255.255.255.255 to ins.add.50.1 on
interface dmz
```

```
Jul 11 17:01:54 ins.add.50.241 Jul 11 2003 07:01:54: %PIX-2-106016: Deny IP
spooof from (255.255.255.255) to ins.add.50.1 on interface dmz
```

Jul 11 17:01:55 ins.add.50.241 Jul 11 2003 07:01:55: %PIX -4-400014: IDS:2004 ICMP echo request from 255.255.255.255 to ins.add.50.1 on interface dmz
Jul 11 17:01:55 ins.add.50.241 Jul 11 2003 07:01:55: %PIX -2-106016: Deny IP spooof from (255.255.255.255) to ins.add.50.1 on interface dmz
Jul 11 17:02:05 ins.add.50.241 Jul 11 2003 07:02:05: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to ins.add.50.1 on interface dmz
Jul 11 17:02:05 ins.add.50.241 Jul 11 2003 07:02:05: %PIX -2-106016: Deny IP spooof from (127.0.0.1) to ins.add.50.1 on interface dmz
Jul 11 17:02:06 ins.add.50.241 Jul 11 2003 07:02:06: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to ins.add.50.1 on interface dmz
Jul 11 17:02:06 ins.add.50.241 Jul 11 2003 07:02:06: %PIX -2-106016: Deny IP spooof from (127.0.0.1) to ins.add.50.1 on interface dmz
Jul 11 17:02:07 ins.add.50.241 Jul 11 2003 07:02:07: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to ins.add.50.1 on interface dmz
Jul 11 17:02:07 ins.add.50.241 Jul 11 2003 07:02:07: %PIX -2-106016: Deny IP spooof from (127.0.0.1) to ins.add.50.1 on interface dmz
Jul 11 17:02:08 ins.add.50.241 Jul 11 2003 07:02:08: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to ins.add.50.1 on interface dmz
Jul 11 17:02:08 ins.add.50.241 Jul 11 2003 07:02:08: %PIX -2-106016: Deny IP spooof from (127.0.0.1) to ins.add.50.1 on interface dmz
Jul 11 17:02:09 ins.add.50.241 Jul 11 2003 07:02:09: %PIX -4-400014: IDS:2004 ICMP echo request from 127.0.0.1 to ins.add.50.1 on interface dmz
Jul 11 17:02:09 ins.add.50.241 Jul 11 2003 07:02:09: %PIX -2-106016: Deny IP spooof from (127.0.0.1) to ins.add.50.1 on interface dmz
Jul 11 17:02:19 ins.add.50.241 Jul 11 2003 07:02:19: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:21 ins.add.50.241 Jul 11 2003 07:02:21: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:22 ins.add.50.241 Jul 11 2003 07:02:22: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:23 ins.add.50.241 Jul 11 2003 07:02:23: %PIX -4-400014: IDS:2004 ICMP echo request from 10.0.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:33 ins.add.50.241 Jul 11 2003 07:02:33: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:34 ins.add.50.241 Jul 11 2003 07:02:34: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:36 ins.add.50.241 Jul 11 2003 07:02:36: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:37 ins.add.50.241 Jul 11 2003 07:02:37: %PIX -4-400014: IDS:2004 ICMP echo request from 172.16.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:47 ins.add.50.241 Jul 11 2003 07:02:47: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to ins.add.50.1 on interface dmz
Jul 11 17:02:48 ins.add.50.241 Jul 11 2003 07:02:48: %PIX -4-400014:

	IDS:2004 ICMP echo request from 192.168.0.10 to ins.add.50.1 on interface dmz Jul 11 17:02:49 ins.add.50.241 Jul 11 2003 07:02:49: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to ins.add.50.1 on interface dmz Jul 11 17:02:51 ins.add.50.241 Jul 11 2003 07:02:51: %PIX -4-400014: IDS:2004 ICMP echo request from 192.168.0.10 to ins.add.50.1 on interface dmz Jul 11 17:03:01 ins.add.50.241 Jul 11 2003 07:03:01: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to ins.add.50.1 on interface dmz Jul 11 17:03:02 ins.add.50.241 Jul 11 2003 07:03:02: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to ins.add.50.1 on interface dmz Jul 11 17:03:03 ins.add.50.241 Jul 11 2003 07:03:03: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to ins.add.50.1 on interface dmz Jul 11 17:03:04 ins.add.50.241 Jul 11 2003 07:03:04: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to ins.add.50.1 on interface dmz Jul 11 17:03:06 ins.add.50.241 Jul 11 2003 07:03:06: %PIX -4-400014: IDS:2004 ICMP echo request from 224.0.0.7 to ins.add.50.1 on interface dmz Jul 11 17:03:15 ins.add.50.241 Jul 11 2003 07:03:15: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to ins.add.50.1 on interface dmz Jul 11 17:03:16 ins.add.50.241 Jul 11 2003 07:03:16: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to ins.add.50.1 on interface dmz Jul 11 17:03:17 ins.add.50.241 Jul 11 2003 07:03:17: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to ins.add.50.1 on interface dmz Jul 11 17:03:18 ins.add.50.241 Jul 11 2003 07:03:18: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to ins.add.50.1 on interface dmz Jul 11 17:03:19 ins.add.50.241 Jul 11 2003 07:03:19: %PIX -4-400014: IDS:2004 ICMP echo request from 240.0.0.0 to ins.add.50.1 on interface dmz Jul 11 17:03:29 ins.add.50.241 Jul 11 2003 07:03:29: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to ins.add.50.1 on interface dmz Jul 11 17:03:30 ins.add.50.241 Jul 11 2003 07:03:30: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to ins.add.50.1 on interface dmz Jul 11 17:03:31 ins.add.50.241 Jul 11 2003 07:03:31: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to ins.add.50.1 on interface dmz Jul 11 17:03:32 ins.add.50.241 Jul 11 2003 07:03:32: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to ins.add.50.1 on interface dmz Jul 11 17:03:33 ins.add.50.241 Jul 11 2003 07:03:33: %PIX -4-400014: IDS:2004 ICMP echo request from ins.add.50.10 to ins.add.50.1 on interface dmz
Compliance	<b>Outside to DMZ – Pass</b> <b>DMZ to Inside – Fail</b> <ul style="list-style-type: none"> <li>spoofed packets were successfully sent across the firewall</li> </ul>
Control Point	9
Control	Ensure Developers on the outside network are not subverting network

Objective	separation controls by connecting to inside networks.																												
Test and findings	<p>Note: Web content filtering software was selected as an audit tool as it is the only commonly used service that logs IP address and workstation name.</p> <p>Copy web content filtering server usage database to local workstation from content filtering server.</p> <p>Run the following SQL statement in a query window using Microsoft Access</p> <pre>SELECT Workstations.IP_Address, Workstations.Workstation_Name, Workstations.First_Access, Workstations.Last_Access FROM Workstations WHERE ( ((Workstations.IP_Address) Like " Ins.add.50.*" Or (Workstations.IP_Address) Like " Ins.add.51.*" Or (Workstations.IP_Address) Like " Ins.add.52.*") AND ((Workstations.Workstation_Name) Not Like "D0#####" And (Workstations.Workstation_Name) Not Like "L0#####" And (Workstations.Workstation_Name) Not Like "?? -???.*") );</pre> <p><b>Results</b></p> <table><tr><th colspan="4">Workstations subverting firewall</th></tr><tr><th>IP_Address</th><th>Workstation_Name</th><th>First_Access</th><th>Last_Access</th></tr><tr><td>Ins.add.51.114</td><td>WSIDD10A555 C8BA</td><td>9/07/2003 10:26:22 AM</td><td>10/07/2003 1:05:38 PM</td></tr><tr><td>Ins.add.51.199</td><td>WSIDD096555 04AE</td><td>9/07/2003 10:31:04 AM</td><td>10/07/2003 2:05:52 PM</td></tr><tr><td>Ins.add.51.110</td><td>WSIDD10A555 DE99</td><td>9/07/2003 10:33:12 AM</td><td>10/07/2003 4:09:12 PM</td></tr><tr><td>Ins.add.51.175</td><td>WSIDD02B30555 C7</td><td>9/07/2003 11:03:05 AM</td><td>10/07/2003 2:27:31 PM</td></tr><tr><td>Ins.add.52.202</td><td>Ins.add.52.202</td><td>9/07/2003 12:06:50 PM</td><td>9/07/2003 3:11:19 PM</td></tr></table>	Workstations subverting firewall				IP_Address	Workstation_Name	First_Access	Last_Access	Ins.add.51.114	WSIDD10A555 C8BA	9/07/2003 10:26:22 AM	10/07/2003 1:05:38 PM	Ins.add.51.199	WSIDD096555 04AE	9/07/2003 10:31:04 AM	10/07/2003 2:05:52 PM	Ins.add.51.110	WSIDD10A555 DE99	9/07/2003 10:33:12 AM	10/07/2003 4:09:12 PM	Ins.add.51.175	WSIDD02B30555 C7	9/07/2003 11:03:05 AM	10/07/2003 2:27:31 PM	Ins.add.52.202	Ins.add.52.202	9/07/2003 12:06:50 PM	9/07/2003 3:11:19 PM
Workstations subverting firewall																													
IP_Address	Workstation_Name	First_Access	Last_Access																										
Ins.add.51.114	WSIDD10A555 C8BA	9/07/2003 10:26:22 AM	10/07/2003 1:05:38 PM																										
Ins.add.51.199	WSIDD096555 04AE	9/07/2003 10:31:04 AM	10/07/2003 2:05:52 PM																										
Ins.add.51.110	WSIDD10A555 DE99	9/07/2003 10:33:12 AM	10/07/2003 4:09:12 PM																										
Ins.add.51.175	WSIDD02B30555 C7	9/07/2003 11:03:05 AM	10/07/2003 2:27:31 PM																										
Ins.add.52.202	Ins.add.52.202	9/07/2003 12:06:50 PM	9/07/2003 3:11:19 PM																										
Compliance	<b>Fail</b>																												

Control Point	11
Control Objective	Ensure the firewall logs events at the correct time
Test and findings	<p><b><u>The firewall is synced to an accurate NTP server</u></b>  pixfirewall# show ntp status</p> <p><b>Clock is synchronized</b>, stratum 4, reference is ins.add.50.1  nominal freq is 99.9984 Hz, actual freq is 99.9931 Hz, precision is 2**6  reference time is c2b91c1a.c42df508 (11:20:58.766 UTC Fri Jul 11 2003)  clock offset is 0.0218 msec, root delay is 18.94 msec  root dispersion is 44.53 msec, peer dispersion is 0.06 msec  pixfirewall#</p> <p><b><u>Ensure “logging timestamp” command in the configuration</u></b>  pixfirewall# show running   include timestamp  <b>logging timestamp</b>  pixfirewall#</p>

	<p><b><u>Ensure events logged on the syslog server have the firew alls timestamp in each record</u></b></p> <pre>[user@inside log]# tail -n0 -f messages   grep ins.add.50.241 Jul 11 21:30:11 ins.add.50.241 Jul 11 2003 11:30:11: %PIX-4-400010: IDS:2000 ICMP echo reply from dmz.add.1.10 to ins.add.50.1 on interface dmz Jul 11 21:30:12 ins.add.50.241 Jul 11 2003 11:30:12: %PIX-4-400010: IDS:2000 ICMP echo reply from dmz.add.1.10 to ins.add.50.1 on interface dmz</pre> <p><b><u>Ensure “clock timezone zone nn” is set in PIX configuration</u></b></p> <pre>pixfirewall#Show running   include timezone pixfirewall#</pre>
Compliance	<p><b>Fail</b></p> <ul style="list-style-type: none"> <li>• clock timezone zone nn not in configuration</li> <li>• Firewall event timestamp is 10 hours behind syslog timestamp</li> </ul>

<b>Control Point</b>	<b>14</b>
<b>Control Objective</b>	Minimise the leakage of TLA’s data
<b>Test and findings</b>	<p>Ensure ICMP echo -request and ICMP reply are the only I CMP types that can originate from the outside and DMZ segments to more secure segments.</p> <p>From the outside and DMZ networks use hping2 with at least two other types of ICMP types.</p> <p>Confirm the packets are dropped and logged by the firewall Confirm the packets are not received at the destination host with tcpdump.</p> <p><b><u>From outside &amp; DMZ host</u></b></p> <pre>#icmp timestamp request hping2 --icmp-ts -c 2 ins.add.50.1 #icmp address-mask request hping2 --icmp-addr -c 2 ins.add.50.1</pre> <p><b><u>On destination host</u></b></p> <pre>[user@inside tmp]# tcpdump -nn src net sub.net.0.0/8 and not port 22 and not arp and not udp port 123 and not udp port 138 and not udp port 514</pre> <p><b><u>On syslog server</u></b></p> <pre>[user@inside log]# tail -f -n0 /var/log/messages   grep ins.add.50.241</pre> <p><b><u>From outside to inside</u></b></p> <p><b><u>On outside host</u></b></p> <pre>[user@outside root]# #icmp timestamp request [user@outside root]# hping2 --icmp-ts -c 2 ins.add.50.1 HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes len=46 ip= ins.add.50.1 ttl=255 id=49322 icmp_seq=0 rtt=0.6 ms ICMP timestamp: Originat e=18592902 Receive=18592935 Transmit=18592935</pre>

	<pre> ICMP timestamp RTT tsrtt=1  len=46 ip= ins.add.50.1 ttl=255 id=49323 icmp_seq=1 rtt=0.4 ms ICMP timestamp: Originate=18593900 Receive=18593931 Transmit=18593931 ICMP timestamp RTT tsrtt=0  --- ins.add.50.1 hping statistic --- 2 packets tramitted, 2 packets received, 0% packet loss round-trip min/avg/max = 0.4/0.5/0.6 ms [user@outside root]# #icmp address -mask request [user@outside root]# hping2 --icmp-addr -c 2 ins.add.50.1 HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes  --- ins.add.50.1 hping statistic --- 2 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms  <b><u>On destination host (inside)</u></b> [user@inside tmp]# tcpdump -nn src net sub.net.0.0/8 and not port 22 and not arp and not udp port 123 and not udp port 138 and not udp port 514 tcpdump: listening on eth0 15:09:52.935028 dmz.add.1.140 &gt; ins.add.50.1: icmp: time stamp query id 8737 seq 0 15:09:52.935580 ins.add.50.1 &gt; dmz.add.1.140: icmp: time stamp reply id 8737 seq 0 : org 0x11bb486 recv 0x11bb4a7 xmit 0x11bb4a7 15:09:53.931111 dmz.add.1.140 &gt; ins.add.50.1: icmp: time stamp query id 8737 seq 256 15:09:53.931260 ins.add.50.1 &gt; dmz.add.1.140: icmp: time stamp reply id 8737 seq 256 : org 0x11bb86c recv 0x11bb88b xmit 0x11bb88b 15:09:53.937813 dmz.add.1.140 &gt; ins.add.50.1: icmp: address mask request 15:09:54.927068 dmz.add.1.140 &gt; ins.add.50.1: icmp: address mask request  6 packets received by filter 0 packets dropped by kernel  <b><u>On syslog server</u></b> [user@inside log]# tail -f -n0 /var/log/messages   grep ins.add.50.241 Jul 12 15:09:52 ins.add.50.241 Jul 12 2003 05:09:52: %PIX -4-400017: IDS:2007 ICMP time request from dmz.add.1.140 to ins.add.50.1 on interface outside Jul 12 15:09:53 ins.add.50.241 Jul 12 2003 05:09:53: %PIX -4-400017: IDS:2007 ICMP time request from dmz.add.1.140 to ins.add.50.1 on interface outside Jul 12 15:09:53 ins.add.50.241 Jul 12 2003 05:09:53: %PIX -4-400021: IDS:2011 ICMP address mask request from dmz.add.1.140 to ins.add.50.1 on interface outside Jul 12 15:09:54 ins.add.50.241 Jul 12 2003 05:09:54: %PIX -4-400021: IDS:2011 ICMP address mask request from dmz.add.1.140 to ins.add.50.1 on </pre>
--	--

	<pre> interface outside  <b><u>From DMZ to inside</u></b> <b><u>On DMZ host</u></b> [user@dmz root]# hping2 --icmp-ts -c 2 ins.add.50.1 HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes len=46 ip= ins.add.50.1 ttl=255 id=15389 icmp_seq=0 rtt=0.7 ms ICMP timestamp: Originate=19347691 Receive=19338475 Transmit=19338475 ICMP timestamp RTT tsrtt=1  len=46 ip= ins.add.50.1 ttl=255 id=15390 icmp_seq=1 rtt=0.4 ms ICMP timestamp: Originate=19348686 Receive=19339463 Transmit=19339463 ICMP timestamp RTT tsrtt=0  --- ins.add.50.1 hping statistic --- 2 packets tramitted, 2 packets received, 0% packet loss round-trip min/avg/max = 0.4/0.5/0.7 ms [user@dmz root]# #icmp address -mask request [user@dmz root]# hping2 --icmp-addr -c 2 ins.add.50.1 HPING ins.add.50.1 (eth0 ins.add.50.1): icmp mode set, 28 headers + 0 data bytes  --- ins.add.50.1 hping statistic --- 2 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms [user@dmz root]#  <b><u>On destination host</u></b> [user@inside tmp]# tcpdump -nn src net sub.net.0.0/8 and not port 22 and not arp and not udp port 123 and not udp port 138 a nd not udp port 514 tcpdump: listening on eth0 15:22:18.475573 dmz.add.1.10 &gt; ins.add.50.1: icmp: time stamp query id 27422 seq 0 15:22:18.476240 ins.add.50.1 &gt; dmz.add.1.10: icmp: time stamp reply id 27422 seq 0 : org 0x12738eb rec v 0x12714eb xmit 0x12714 eb 15:22:19.463881 dmz.add.1.10 &gt; ins.add.50.1: icmp: time stamp query id 27422 seq 256 15:22:19.464014 ins.add.50.1 &gt; dmz.add.1.10: icmp: time stamp reply id 27422 seq 256 : org 0x1273cce rec v 0x12718c7 xmit 0x12718c7 15:22:19.497873 dmz.add.1.10 &gt; ins.add.50.1: icmp: address mask request 15:22:20.463508 dmz.add.1.10 &gt; ins.add.50.1: icmp: address mask request  6 packets received by filter 0 packets dropped by kernel  <b><u>On syslog server</u></b> </pre>
--	---



	<pre>[user@inside log]# tail -f -n0 /var/log/messages   grep ins.add.50.241 Jul 12 15:22:18 ins.add.50.241 Jul 12 2003 05:22:18: %PIX -4-400017: IDS:2007 ICMP time request from dmz.add.1.10 to ins.add.50.1 on interface dmz Jul 12 15:22:19 ins.add.50.241 Jul 12 2003 05:22:19: %PIX -4-400017: IDS:2007 ICMP time request from dmz.add.1.10 to ins.add.50.1 on interface dmz Jul 12 15:22:19 ins.add.50.241 Jul 12 2003 05:22:19: %PIX -4-400021: IDS:2011 ICMP address mask request from dmz.add.1.10 to ins.add.50.1 on interface dmz Jul 12 15:22:20 ins.add.50.241 Jul 12 2003 05:22:20: %PIX -4-400021: IDS:2011 ICMP address mask request from dmz.add.1.10 to ins.add.50.1 on interface dmz</pre>
Compliance	<b>Fail</b> (same results for outside to inside & DMZ to inside) <ul style="list-style-type: none"> <li>• All packets received at destination host</li> <li>• ICMP timestamp responses received at source host</li> <li>• Packets not dropped by firewall</li> </ul>

<b>Control Point</b>	<b>15</b>
Control Objective	Ensure firewall integrity through permitting encrypted administration protocols only
Test and findings	<p>Confirm http and telnet are disabled through configuration review and testing from all interfaces.</p> <p>Connect to firewall console via ssh</p> <p>TCP nmap of all firewall interfaces should only show ssh port open on the inside interface</p> <p><b><u>On outside host</u></b>  telnet dmz.add.1.129  telnet dmz.add.1.129 80</p> <p>ssh -c des admin@dmz.add.1.129  nmap -sT -P0 dmz.add.1.129</p> <p><b><u>On DMZ host</u></b>  telnet dmz.add.1.1  telnet dmz.add.1.1 80</p> <p>ssh -c des admin@dmz.add.1.1  nmap -sT -P0 dmz.add.1.1</p> <p><b><u>On inside host</u></b>  [user@inside tmp]# telnet ins.add.50.241  Trying ins.add.50.241...  telnet: connect to address ins.add.50.241: <b>Connection refused</b>  [user@inside tmp]#</p>



	<pre> [user@inside tmp]# telnet ins.add.50.241 80 Trying ins.add.50.241... telnet: connect to address ins.add.50.241: <b>Connection refused</b> [user@inside tmp]# [user@inside tmp]# nmap -sT -P0 -p1-65535 ins.add.50.241  Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ ) Interesting ports on pixfirewall ( ins.add.50.241): (The 65533 ports scanned but not shown below are in state: closed) Port      State      Service 22/tcp    open      ssh 443/tcp   open      https  Nmap run completed -- 1 IP address (1 host up) scanned in 13 seconds [user@inside tmp]# [user@inside tmp]# ssh -c des admin@ins.add.50.241 Warning: use of <b>DES</b> is strongly discouraged due to cryptographic weaknesses admin@ins.add.50.241's password: Type help or '?' for a list of available commands. pixfirewall&gt; pixfirewall&gt; q  Logoff  Connection to ins.add.50.241 closed. [user@inside tmp]#  <b><u>On firewall</u></b> pixfirewall# show http <b>http server enabled</b> ins.add.50.0 255.255.255.0 inside pixfirewall# <b>show telnet</b> pixfirewall# pixfirewall# show ssh <b>ins.add.50.0 255.255.255.0 inside</b> pixfirewall#  <b><u>On DMZ host</u></b>  [user@dmz root]# telnet dmz.add.1.1 Trying dmz.add.1.1... telnet: connect to address dmz.add.1.1: <b>Connection refused</b> [user@dmz root]# telnet dmz.add.1.1 80 Trying dmz.add.1.1... telnet: connect to address dmz.add.1.1: <b>Connection refused</b> [user@dmz root]# [user@dmz root]# ssh -c des admin@dmz.add.1.1 ssh: connect to address dmz.add.1.1 port 22: <b>Connection refused</b> [user@dmz root]# nmap -sT -P0 -p1-65535 dmz.add.1.1 </pre>
--	---

	<p>Starting nmap V. 2.54BET A31 ( www.insecure.org/nmap/ )  <b>All 65535 scanned ports on ( dmz.add.1.1) are: closed</b></p> <p>Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds  [user@dmz root]#</p> <p><b><u>On outside host</u></b>  [root@sis-laptop1 root]# telnet dmz.add.1.129  Trying dmz.add.1.129...  telnet: connect to address dmz.add.1.129: <b>Connection timed out</b>  [root@sis-laptop1 root]# telnet dmz.add.1.129 80  Trying dmz.add.1.129...  telnet: connect to address dmz.add.1.129: <b>Connection timed out</b>  [root@sis-laptop1 root]#  [root@sis-laptop1 root]# nmap -sT -P0 -p1-65535 dmz.add.1.129</p> <p>Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )  <b>All 65535 scanned ports on ( dmz.add.1.129) are: filtered</b></p> <p>Nmap run completed -- 1 IP address (1 host up) scanned in 20704 seconds  You have new mail in /var/spool/mail /root  [root@sis-laptop1 root]#  [root@sis-laptop1 root]# ssh -c des admin@ dmz.add.1.129  ssh: connect to address dmz.add.1.129 port 22: <b>Connection timed out</b>  [root@sis-laptop1 root]#</p>
Compliance	<b>Pass</b>

<b>Control Point</b>	<b>16</b>
Control Objective	Ensure traceability of firewall logs. PIX will log using name instruction to the log file.
Test and findings	<p>Confirm no name commands in firewall configuration  <b><u>On firewall</u></b>  pixfirewall# show run   grep ^name   exclude nameif  <b>name dmz.add.1.10 ntx-fs1</b>  pixfirewall#</p> <p><b><u>On *nix host</u></b>  Copy syslog file to temporary directory  Run following script in temporary directory  Record number of words found</p> <p>[user@inside pixfirewall]# cat mess.sh  #!/bin/sh  #remove temp files  rm messages.1 messages.2</p>



### **Scan configuration and results**

Scan configuration was performed using the following plug-in families

- Cisco
- DOS
- Gain a shell remotely
- Gain root remotely
- General

Other configuration

- No port scan

Refer to Appendix B – Nessus scan results for full scan report

### **NESSUS SECURITY SCAN REPORT**

Created 13.07.2003                      Sorted by host names

Session Name : pix from outside  
Start Time : 13.07.2003 10:35:18  
Finish Time : 13.07.2003 11:01:48  
Elapsed Time : 0 day(s) 00:26:30

	<pre> --- cut ---  Total security holes found : 0     high severity : 0     low severity : 0     informational : 0  Scanned hosts:  Name                High Low  Info ----- dmz.add.1.129        0    0    0  <b>Firewall syslog</b> [user@inside root]# tail -f /var/log/messages   grep ins.add.50.241 Jul 13 01:32:34 ins.add.50.241 Jul 12 2003 15:32:34: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 01:40:44 ins.add.50.241 Jul 12 2003 15:40:44: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 01:40:47 ins.add.50.241 Jul 12 2003 15:40:47: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 01:40:50 ins.add.50.241 Jul 12 2003 15:40:50: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 01:40:53 ins.add.50.241 Jul 12 2003 15:40:53: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 01:40:53 ins.add.50.241 Jul 12 2003 15:40:53: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 03:01:58 ins.add.50.241 Jul 12 2003 17:01:58: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 03:02:01 ins.add.50.241 Jul 12 2003 17:02:01: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 03:02:04 ins.add.50.241 Jul 12 2003 17:02:04: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp Jul 13 03:02:07 ins.add.50.241 Jul 12 2003 17:02:07: %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp  [user@inside root]# tail -f -n0 /var/log/messages   grep ins.add.50.241 Jul 13 03:02:07 ins.add.50.241 Jul 12 2003 17:02:07: %PIX-4-402106: Rec'd </pre>
--	---

	<p>packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:34:29 ins.add.50.241 Jul 13 2003 00:34:29: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:34:32 ins.add.50.241 Jul 13 2003 00:34:32: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:34:45 ins.add.50.241 Jul 13 2003 00:34:45: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:34:48 ins.add.50.241 Jul 13 2003 00:34:48: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:35:05 ins.add.50.241 Jul 13 2003 00:35:05: %PIX -4-500004: Invalid transport field for protocol=6, from dmz.add.1.140/2285 to dmz.add.1.129/0</p> <p>Jul 13 10:35:08 ins.add.50.241 Jul 13 2003 00:35:08: %PIX -4-500004: Invalid transport field for protocol=6, from dmz.add.1.140/2285 to dmz.add.1.129/0</p> <p>Jul 13 10:35:15 ins.add.50.241 Jul 13 2003 00:35:15: %PIX -4-400010: IDS:2000 ICMP echo reply from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:16 ins.add.50.241 Jul 13 2003 00:35:16: %PIX -4-400010: IDS:2000 ICMP echo reply from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:25 ins.add.50.241 Jul 13 2003 00:35:25: %PIX -4-400026: IDS:3040 TCP NULL flags from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:30 ins.add.50.241 Jul 13 2003 00:35:30: %PIX -4-400026: IDS:3040 TCP NULL flags from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:35 ins.add.50.241 Jul 13 2003 00:35:35: %PIX -4-400026: IDS:3040 TCP NULL flags from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:40 ins.add.50.241 Jul 13 2003 00:35:40: %PIX -4-400026: IDS:3040 TCP NULL flags from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:35:45 ins.add.50.241 Jul 13 2003 00:35:45: %PIX -4-400026: IDS:3040 TCP NULL flags from dmz.add.1.140 to dmz.add.1.129 on interface outside</p> <p>Jul 13 10:36:11 ins.add.50.241 Jul 13 2003 00:36:11: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:36:14 ins.add.50.241 Jul 13 2003 00:36:14: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:36:21 ins.add.50.241 Jul 13 2003 00:36:21: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr= dmz.add.1.140, prot= tcp</p> <p>Jul 13 10:36:21 ins.add.50.241 Jul 13 2003 00:36:21: %PIX -4-402106: Rec'd packet not an IPSEC packet. (ip) dest_addr= dmz.add.1.129, src_addr=</p>
--	--

dmz.add.1.140, prot= tcp  
Jul 13 10:36:24 ins.add.50.241 Jul 13 2003 00:36:24: %PIX -4-402106: Rec'd  
packet not an IPSEC packet. (ip) dest\_addr= dmz.add.1.129, src\_addr=  
dmz.add.1.140, prot= tcp

Jul 13 10:36:24 ins.add.50.241 Jul 13 2003 00:36:24: %PIX -4-402106: Rec'd  
packet not an IPSEC packet. (ip) dest\_a ddr= dmz.add.1.129, src\_addr=  
dmz.add.1.140, prot= tcp

### Inside

### Firewall statistics before/during/after Nessus scan

### Scan configuration and results

Refer to Appendix B – Nessus scan results for full scan report

#### NESSUS SECURITY SCAN REPORT

Created 13.07.2003

Sorted by host names

Session Name : pix from inside

Start Time : 13.07.2003 11:25:28

Finish Time : 13.07.2003 11:32:23

Elapsed Time : 0 day(s) 00:06:54

--- cut ---

Total security holes found : 6  
    high severity : 0  
    low severity : 4  
    informational : 2

**Scanned hosts:**

Name	High	Low	Info
ins.add.50 .241	0	4	2

Host: ins.add.50 .241

Open ports:

ssh (22/tcp)  
general/tcp

Service: general/tcp  
Severity: Low

The remote host uses non -random IP IDs, that is, it is possible to predict the next value of the ip\_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch  
Risk factor : Low

Service: ssh (22/tcp)  
Severity: Low

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.5

Service: ssh (22/tcp)  
Severity: Low

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution :  
If you use OpenSSH, set the option 'Protocol' to '2'  
If you use SSH.com's set the option 'SshCompatibility' to 'no'



	<p>Risk factor : Low</p> <p>Service: ssh (22/tcp) Severity: Low</p> <p>Remote SSH version : SSH -1.5-Cisco-1.25</p> <p><b><u>Syslog of scan</u></b>  [user@inside root]# tail -f -n0 /var/log/messages   grep ins.add.50.241  Jul 13 11:24:42 ins.add.50.241 Jul 13 2003 01:24:42: %PIX -4-500004: Invalid transport field for protocol=6, from ins.add.50.2/1093 to ins.add.50.241/0  Jul 13 11:24:45 ins.add.50.241 Jul 13 2003 01:24:45: %PIX -4-500004: Invalid transport field for protocol=6, from ins.add.50.2/1093 to ins.add.50.241/0  Jul 13 11:24:46 ins.add.50.241 Jul 13 2003 01:24:46: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:47 ins.add.50.241 Jul 13 2003 01:24:47: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:48 ins.add.50.241 Jul 13 2003 01:24:48: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:49 ins.add.50.241 Jul 13 2003 01:24:49: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:50 ins.add.50.241 Jul 13 2003 01:24:50: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:51 ins.add.50.241 Jul 13 2003 01:24:51: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:52 ins.add.50.241 Jul 13 2003 01:24:52: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:53 ins.add.50.241 Jul 13 2003 01:24:53: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:54 ins.add.50.241 Jul 13 2003 01:24:54: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:55 ins.add.50.241 Jul 13 2003 01:24:55: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:56 ins.add.50.241 Jul 13 2003 01:24:56: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2  Jul 13 11:24:57 ins.add.50.241 Jul 13 2003 01:24:57: %PIX -3-610001: NTP daemon interface inside: Packet denied from ins.add.50.2</p>
Compliance	<p><b>Pass</b></p> <ul style="list-style-type: none"> <li>No significant or lasting effect was made to the CPU utilisation or memory usage on the firewall</li> <li>No errors were detected in the firewall syslog</li> </ul>

<b>Control Point</b>	<b>20</b>
Control Objective	Ensure firewall rules are relevant to the current situation
Test and findings	Record access-list hit counts over consecutive weeks for at least three periods. Record in a spreadsheet and compare with next weeks results

ACL	hitcnt 13-Jun	hitcnt 20-Jun	hitcnt 27-Jun	Packets/week Week 1	Packets/week Week 2	Total packet count (2 weeks)
inside1	18411	25425	34169	7,014	8,744	15,758
outside1	1	3	3	2	-	2
outside2	0	0	0	-	-	-
outside3	2736	3442	4268	706	826	1,532
outside4	0	0	0	-	-	-
outside5	151	218	305	67	87	154
outside6	55503	73019	104013	17,516	30,994	48,510
outside7	135588	181815	254556	46,227	72,741	118,968
outside8	86356	114095	147920	27,739	33,825	61,564
outside9	10294	13302	17727	3,008	4,425	7,433
dmz1	8529	11097	13856	2,568	2,759	5,327
dmz2	0	0	0	-	-	-
dmz3	3382	4638	5864	1,256	1,226	2,482
dmz4	3562	4729	5914	1,167	1,185	2,352
dmz5	2291	2682	3273	391	591	982
dmz6	8844	12113	16925	3,269	4,812	8,081
dmz7	1723	2220	3845	497	1,625	2,122
dmz8	69	90	110	21	20	41
dmz9	952	1091	1261	139	170	309
dmz10	3569	4890	6296	1,321	1,406	2,727
dmz11	5475	7331	9200	1,856	1,869	3,725

#### **Review of low hitcnt rules**

outside1, outside2, outside4, dmz2 show very low hit counts.

##### **access-list outside line 1**

permit tcp dmz.add.1.128 255.255.255.128 host ntx -fs1 eq 135

- Two packets in one week. Rule is not for a redundant service and is therefore unnecessary.

##### **access-list outside line 2**

permit tcp dmz.add.1.128 255.255.255.128 host ntx -fs1 eq 137

- No packets in two weeks. Rule is not for a redundant service and is therefore unnecessary.

##### **access-list outside line 4**

permit udp dmz.add.1.128 255.255.255.128 eq netbios -dgm host ntx -fs1 eq netbios -dgm

	<ul style="list-style-type: none"> <li>No packets in two weeks. Rule is not for a redundant service and is therefore unnecessary.</li> </ul> <p><b>access-list dmz line 2</b>  permit icmp any any</p> <ul style="list-style-type: none"> <li>No packets in two weeks. Rule is to permit connectivity testing from the DMZ to the inside network. Will be used for troubleshooting if necessary. Rule is required.</li> </ul>
Compliance	<p><b>Fail</b></p> <p>Three rules were found to not be used and having no purpose for redundant services (eg. Secondary DNS server) .</p>

## Residual Risk

Seven Control Points failed their audit tests. The residual risk (after recommended actions are applied) is shown in the following tables.

<b>Control Point 2</b>	<b>Ensure all DMZ users (from third party developers are aware of, and comply with policy of network separation)</b>
<b>Discussion</b>	This control point had four subjective tests, via a questionnaire, and failed on each test. Failure of this control point shows that the training and induction process for the developers has been unsuccessful, and they could innocently subvert the security controls that have been put in place. This would place increase the Information Security risks TLA Enterprises as some machines on the private network are uncontrolled.
<b>Risk mitigation</b>	The induction program should be reviewed and delivered to the developers once more. The success of the program should be measured by reissuing the questionnaire. Additionally a process should be written to ensure developers cannot commence on TLA Enterprises premises without having completed the induction program.
<b>Cost estimation</b>	Reviewing induction program and deliver training – 2 days \$3,000 @ \$1500/day Retrain developers (30 minute training session * 30 developers @ \$200/hour \$3,000 <b>Total <u>\$6,000</u></b>
<b>Residual risk</b>	<b>High</b> - Even with the training a malicious user could still subvert the security controls.

<b>Control Point 8</b>	<b>Confirm only packets from appropriate source addresses can be sent through the firewall</b>
<b>Discussion</b>	Packets with spoofed addresses were not able to be sent from the Outside to the DMZ network, but they were able to be sent from the DMZ network to the Inside network. The residual risk is minimised as there are only a few machines in the DMZ network and they do not have Developers logging on locally.  Should this risk remain unmitigated any host in the DMZ network can send packets from falsified source addresses and potentially create problems with inside (private) network hosts.
<b>Risk mitigation</b>	This risk can be readily mitigated by updating the firewall configuration to enable the “ip verify reverse -path interface <interface-name>” statement
<b>Cost estimation</b>	Reconfigure firewall with “ip verify reverse -path” statement \$400 and test – 2 hours @ \$200/hour <b>Total <u>\$ 400</u></b>
<b>Residual risk</b>	<b>Low</b> – the reconfiguration of the firewall can be completed quickly and can be completed without any interruption.

<b>Control Point 9</b>	<b>Ensure Developers on the outside network are not subverting network separation controls by connecting to inside networks.</b>
<b>Discussion</b>	This control failed as it was found that developers were directly connecting their machines to the inside network. Further investigation by TLA staff

	revealed desks were incorrectly labelled and other developers had not been inducted to the site. The risk increase is the same as per Control Point 2 above.								
<b>Risk mitigation</b>	<p>Control Point 2 above already recommends that the induction and training program be revisited and delivered. Further to this TLA Information Security should monitor the inside networks at this site for further activity. The method of using the Web content filtering software logs as a control point is not ideal as this necessitates a considerable amount of manual effort.</p> <p>The risk would be mitigated by implementing authentication at the network edge. Currently any host that connects via a network cable at TLA is automatically assigned an address from a DHCP (Dynamic Host Configuration Protocol) server. This grants them access to the network automatically. Authentication at the network edge would mean that a workstation would have to authenticate to a central authentication server before being assigned an IP address by the DHCP server. This would mean that non SOE workstations would not be able to connect to any network segment with 802.1x enabled.</p> <p>An initial review of the current network switching at TLA shows it supports 802.1x. A detailed review should be conducted and a recommendation should be put forward.</p>								
<b>Cost estimation</b>	<table> <tr> <td>Reviewing suitability for implementing network edge authentication – 1 days @ \$1500/day</td><td>\$1,500</td></tr> <tr> <td>Test implementation of network edge authentication – 2 days @ \$1,500/day</td><td>\$3,000</td></tr> <tr> <td>Implementation of network edge authentication – 5 days @ \$1,500/day</td><td>\$7,500</td></tr> <tr> <td><b>Total</b></td><td><b><u>\$12,000</u></b></td></tr> </table>	Reviewing suitability for implementing network edge authentication – 1 days @ \$1500/day	\$1,500	Test implementation of network edge authentication – 2 days @ \$1,500/day	\$3,000	Implementation of network edge authentication – 5 days @ \$1,500/day	\$7,500	<b>Total</b>	<b><u>\$12,000</u></b>
Reviewing suitability for implementing network edge authentication – 1 days @ \$1500/day	\$1,500								
Test implementation of network edge authentication – 2 days @ \$1,500/day	\$3,000								
Implementation of network edge authentication – 5 days @ \$1,500/day	\$7,500								
<b>Total</b>	<b><u>\$12,000</u></b>								
<b>Residual risk</b>	<p><b>Low</b> – implementation of network edge authentication would almost negate any chance of non SOE workstations connecting to the inside network.</p> <p>Until this risk can be mitigated it is recommended that the Web content filtering Software logs be reviewed on a daily basis.</p>								

<b>Control Point 11</b>	<b>Ensure the firewall logs events at the correct time</b>
<b>Discussion</b>	<p>The syslog server and the firewall are logging events with a constant discrepancy of 10 hours. This makes any event correlation with multiple devices more difficult and unreliable. Any prosecution that relied on forensics from the firewall logs would be compromised or at least closely scrutinised due to the time difference.</p> <p>From reviewing the firewall configuration the non-conformance appears to be due to the lack of the “clock timezone zone nn” statement. This should be tested and installed in the firewall configuration. Effects on Cisco PIX Device Manager should be tested as previous versions of PDM skewed monitoring statistics if the firewall was not set to the UTC timezone.</p>
<b>Risk</b>	The firewall should have the statement “clock timezone zone nn”

<b>mitigation</b>	implemented and tested .	
<b>Cost estimation</b>	Implement and test “clock timezone zone nn” statement and test – 2 hours @ \$200/hour	\$400
	<b>Total</b>	<b>\$ 400</b>
<b>Residual risk</b>	<b>Low</b> – it is expected that the implementation of the statement above with resolve this issue quickly and without impact on any system user.	

<b>Control Point 14</b>	<b>Minimise the leakage of TLA’s data</b>	
<b>Discussion</b>	<p>This control failed as there appear to be no controls on the type of ICMP packets that are permitted to be sent through the firewall. ICMP is typically used today to test connectivity from one point to another. Many networks block ICMP across a firewall, but with the semi-trusted relationship between TLA and the Developers ICMP has been allowed through the firewall.</p> <p>ICMP has many more features than the typical usage of “Echo” and “ Echo Reply”. Over twenty types of ICMP have been defined <sup>xxvi</sup>. Each ICMP type will transmit information such as “Address mask” and “Timestamp”. These requests have no function for the Developers and should be denied at the firewall.</p>	
<b>Risk mitigation</b>	The current ICMP permissions should be revoked and the “Echo” and “Echo Reply” ICMP types permitted.	
<b>Cost estimation</b>	Implement and test “ICMP Echo and Echo Reply” permissions – 2 hours @ \$200/hour	\$400
	<b>Total</b>	<b>\$ 400</b>
<b>Residual risk</b>	<b>Low</b> – it is expected that the implementation of the statement above with resolve this issue quickly and without impact on any system user.	

<b>Control Point 16</b>	<b>Ensure traceability of firewall logs. PIX will log using name instruction to the log file.</b>	
<b>Discussion</b>	If a name statement matches the IP address being logged, the Cisco PIX firewall logs the name and not the IP address. As the firewall configuration can be changed any traceability and forensics can be compromised. It is the auditor’s opinion that name statements make reading of any log files more difficult, especially over time.	
<b>Risk mitigation</b>	Remove all name statements from the firewall configuration and test.	
<b>Cost estimation</b>	Remove all name statements from the firewall configuration – 1 hour @ \$200/hour	\$200
	<b>Total</b>	<b>\$ 200</b>
<b>Residual risk</b>	<b>Low</b> – it is expected that the implementation of the statement above with resolve this issue quickly and without impact on any system user.	

<b>Control Point 20</b>	<b>Ensure firewall rules are relevant to the current situation</b>	
<b>Discussion</b>	Three firewall rules were found to have almost no traffic over a two week period. One rule had two packets in a week and the other two rules had no packets. These rules are not necessary to the continued function of the	

	firewall and should be removed to ensure minimal exposure
<b>Risk mitigation</b>	The three firewall rules should be removed from the configuration. If any problems arise they can be quickly reinstated as they are known.
<b>Cost estimation</b>	Remove all unnecessary rules and test functionality – 1 day \$1,500 @ \$1500/day <b>Total</b> <b><u>\$1,500</u></b>
<b>Residual risk</b>	<b>Low</b> – it is expected with the removal of these rules will resolve this issue quickly and without impact on any system user.

### Auditability of the system

The following audit objectives of ensuring were all met.

- Traceability;
- Prevention of leakage of TLA's intellectual property ;
- Security of firewall configuration ; and
- Compliance with network segregation policy.

There were no issues with any of the tests performed on the firewall, therefore the system is auditable. However the usage of web filtering software is not the ideal test for compliance with the network segregation policy. A central authentication host that records all logon activity should be installed. Authentication should be a prerequisite to gain access outside of the DMZ networks. Refer to “ Additional recommendations and mitigations ” for more details.

## Assignment 4

### Executive summary

The Cisco PIX firewall used by TLA Enterprises to segregate the third party developers from TLA's private network is functioning adequately. However, seven audit non-conformances were found during the audit. The majority of non-conformances can be addressed by minor configuration changes or additional training/induction for the third party Developers.

The objectives of the audit were achieved, but further work by TLA is necessary to ensure the firewall is maintained to best practice.

Note: The Cisco PIX firewall uses a different operating system to Cisco routers. A major vulnerability announcement was recently made by Cisco that does **not** relate to the firewall being audited.

### Audit findings

The non-conformances are prioritised according to severity and summarised in the following table. The test results for the control points can be found in Section "Assignment 3".

Control Point	Description	Residual Risk	Non-conformance(s)
2	Ensure all DMZ users (from third party developers) are aware of, and comply with policy of network separation	High	Significant proportions (> 20%) of the on-site Developers were generally unaware of the requirement and need for network separation.
8	Confirm only packets from appropriate source addresses can be sent through the firewall	Low	Spoofed packets can be sent from the DMZ network to other networks.
9	Ensure Developers on the outside network are not subverting network separation controls by connecting to inside networks.	Low	Developers were found to be directly connecting to TLA's inside network either through a lack of knowledge (refer CP2 above) or the desks were label led incorrectly.
11	Ensure the firewall logs events at the correct time	Low	The firewall logs to a syslog server on the inside (secure) network. The firewall



14	Minimise the leakage of TLA's data	Low	timestamps each log entry 10 hours prior to the time the syslog server timestamps the same log entry.
16	Ensure traceability of firewall logs. PIX will log using name instruction to the log file.	Low	All ICMP types are permitted to pass through the firewall. This can facilitate the leakage of corporate information to the Developer network. The name command in a Cisco PIX is specific to the current configuration and when this is logged to a syslog server it can only be read in conjunction with the configuration file. The current configuration was found to have name entries that were logging to the syslog server.
20	Ensure firewall rules are relevant to the current situation	Low	Three firewall rules were found to be superfluous to the current requirements as there were not used for two weeks or longer.

## Background and audit recommendations (with costs)

The following table summarises the background, audit recommendations, and the costs of mitigating that risk (to the level outline in the table above)

Control Point	Description	Background and audit recommendations	Estimated costs
2	Ensure all DMZ users (from third party developers) are aware of, and comply with policy of network separation	<p>If DMZ users (the Developers) connect to the inside network they increase the likelihood of financial loss through the loss of intellectual property, disruption in business (due to virus or worm outbreak, or malicious damage), the unauthorised use of resources or other possibilities.</p> <p>The recommendations are to re-evaluate the training and induction program given to the developers and retrain the developers.</p>	\$6,000
8	Confirm only packets from appropriate source addresses can be sent through the firewall	<p>The controls on the firewall do not prevent the hosts in the DMZ from sending packets from illegal or spoofed (faked) addresses. This could result in Denial of Service (DoS) attacks on TLA's private network, which would likely impact business continuity.</p> <p>Updating the configuration of the firewall will prevent this from happening in the future.</p>	\$400
9	Ensure Developers on the outside network are not subverting network separation controls by connecting to inside networks.	<p>If DMZ users (the Developers) connect to the inside network they increase the likelihood of financial loss through the loss of intellectual property, disruption in business (due to virus or worm outbreak, or malicious damage), the unauthorised use of resources or other possibilities.</p> <p>The current controls do not prevent malicious individuals from connecting to the private network. It is recommended to implement edge based authentication to prevent any non SOE machine from getting on the network at the development site.</p>	\$12,000
11	Ensure the firewall logs events at the correct time	<p>The firewall logs events to a remote (syslog) server to ensure logs can be kept for extended periods and cannot be tampered with should the firewall be compromised.</p>	\$400

		<p>The entries in the syslog file are timestamped by the syslog server, and also timestamped by the firewall. The times of these timestamps do not correspond.</p> <p>Updating the configuration of the firewall will prevent this from happening in the future.</p>	
14	Minimise the leakage of TLA's data	<p>The ICMP protocol (including ping) is typically used to test connectivity between two machines. There are numerous other uses of ICMP that respond with network and host information. This information could be gathered and used to launch a tailored attack on hosts holding TLA's intellectual property.</p> <p>It is recommended to block all ICMP other than those required for the standard ping command. Updating the configuration of the firewall will prevent this from happening in the future.</p>	\$400
16	Ensure traceability of firewall logs. PIX will log using name instruction to the log file.	<p>The Cisco PIX firewall uses a local table of names to resolve IP addresses rather than using DNS. This is done to protect the firewall from a corrupt DNS. However the firewall logs messages to the syslog server with the locally stored name instead of the IP address. This means anyone reading a firewall log must have a copy of the firewall configuration from the time when the log was written. This is not practical as the name entries in the firewall can be readily altered and not typically stored with the firewall configurations.</p> <p>It is recommended to remove all name entries from the firewall to ensure all entries are logged as IP addresses.</p>	\$200
20	Ensure firewall rules are relevant to the current situation	<p>Best practice in writing firewall a rulebase is to use the principle of least privilege. In other words "don't give any more access than is necessary". There are a number of rules in the current rulebase that were not used in a two week period. It is recommended that these rules be removed as they grant the developers greater access to TLA's network and intellectual property than is required.</p>	\$1,500
<b>Total</b>			<b>\$20,900</b>

## Additional recommendations and mitigations

Not specifically covered by the audit scope, but relate to the root cause(s) of the problems or pertinent observations by the auditor.

Control Point	Description	Additional recommendations/Mitigations	Estimated costs
2	Ensure all DMZ users (from third party developers) are aware of, and comply with policy of network separation	<p>This non-conformance would be mitigated by to implement edge based authentication as recommended in CP9 in the preceding table.</p> <p>An alternate approach would be to provide the developers with TLA Enterprises SOE workstations (30 workstations @ \$2,500/workstation)</p>	<p>As per CP9 in preceding table</p> <p>\$75,000</p>
8	Confirm only packets from appropriate source addresses can be sent through the firewall	The firewall has a very limited Intrusion Detection System (IDS) inbuilt. A fully functional Network IDS such as Snort (freeware) or Symantec's Norton, or Enterasys' Dragon would provide a greater level of Intrusion Detection through using a larger IDS signature base, and event correlation. This type of system could alert TLA's Information Security team of an attempted attack from the Developer networks.	\$10,000-\$100,000
9	Ensure Developers on the outside network are not subverting network separation controls by connecting to inside networks.	As per CP2 and CP8	
20	Ensure firewall rules are relevant to the current situation	Periodic monitoring of the relevance of the firewall rules (via hit counts) would ensure that rules without any further use were removed from the rulebase. This would ensure the relevance of the current rulebase and minimise the exposure of TLA business to the development environment.	

		A periodic review and report could be conducted for approximately 1 days work @ \$1,500/day	\$1,500
N/A	Level of encryption in terminal administration session	<p>The current firewall uses SSH Version 1 .5, which Cisco ships with the DES (or single DES) encryption. SSH Version 1 .5 is widely accepted as an insecure protocol as it is now trivial to crack the encryption and many flaws have been found. It is recommended that the SSH2 license be purchased and installed. Cisco ships this license as part of the 3-DES (triple DES) license kit.</p> <p>License: PIX-515-VPN-3DES= \$50  Installation and testing – 2 hours @ \$200/hour \$400</p>	\$450
N/A	Implementation against standards	<p>A significant proportion of the non -conformances found in this audit come from minor configuration issues. Many of these could be prevented if the firewall was installed and tested against an adequate standard.</p> <p>Firewall standard development – 5 days @ \$1,500/day</p>	\$7,500
N/A	Traceable logon process	<p>The current development environment does not require a centrally administered logon to gain access to TLA's corporate resources. Whilst access has been filtered, any abuse of these resources would be difficult to prove without a logon record th at identified an individual.</p> <p>Firewall changes – 2 days @ \$1,500/day</p>	\$3,000

## Appendix A – Risk table methodology

HANDBOOK 3, RISK MANAGEMENT, Version 1.0

The risk assessment table is based on the approach shown in Australian Communications- Electron Security Instruction 33 (ACSI 33) HANDBOOK 3, RISK MANAGEMENT, Version 1.0<sup>xxvii</sup>.

Probability	Frequency
Negligible	Unlikely to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

Table 2 – Threat Probability Rating

Consequence	Impact
Insignificant	Will have almost no impact if threat is realised.
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or departments. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair.
Serious	May cause extended system outage, and/or loss of connected customers or business confidence. May result in compromise of large amounts of information or services.
Grave	May cause system to be permanently closed, and/or be subsumed by another (secure) environment. May result in complete compromise of the Corporation

Table 3 - Consequence Estimation Rating

<b>Threat</b>	<b>Insignificant</b>	<b>Minor</b>	<b>Significant</b>	<b>Damaging</b>	<b>Serious</b>	<b>Grave</b>
<b>Negligible</b>	Nil	Nil	Nil	Nil	Nil	Nil
<b>Very Low</b>	Nil	Low	Low	Low	Medium	Medium
<b>Low</b>	Nil	Low	Medium	Medium	High	High
<b>Medium</b>	Nil	Low	Medium	High	High	Critical
<b>High</b>	Nil	Medium	High	High	Critical	Extreme
<b>Very High</b>	Nil	Medium	High	Critical	Extreme	Extreme
<b>Extreme</b>	Nil	Medium	High	Critical	Extreme	Extreme

**Table 4 - Resultant Risk**

<b>Residual Risk</b>	<b>Rating</b>
Nil	0
Low	1
Medium	2
High	3
Critical	4
Extreme	5

**Table 5 - Countermeasure Priority Rating**

© SANS Institute 2003, Author retains full rights

## Appendix B – Nessus scan results

### NESSUS SECURITY SCAN REPORT

Created 13.07.2003

Sorted by host names

Session Name : **pix from outside**  
Start Time : 13.07.2003 10:35:18  
Finish Time : 13.07.2003 11:01:48  
Elapsed Time : 0 day(s) 00:26:3 0

Plugins used in this scan:

Id	Name
10018	Knox Arkeia buffer overflow
10728	Determine if Bind 9 is running
10515	Too long authorization
11519	mod_jk chunked encoding DoS
11288	CSCdu15622
10717	SHOUTcast Server DoS detector vulnerability
10977	CSCds07326
11152	BIND vulnerable to cached RR overflow
10754	Cisco password not set
11320	The remote BIND has dynamic updates enabled
11169	SSH setsid() vulnerab ility
10028	Determine which version of BIND name daemon is running
10687	Too long POST command
11341	SSH1 SSH Daemon Logging Failure
11047	Jigsaw webserver MS/DOS device DoS
11198	BitKeeper remote command execution
10022	Axent Raptor's DoS
11312	DHCP server overflow / format string bug
10329	BIND iquery overflow
10012	Alibaba 2.0 buffer overflow
10107	HTTP Server type and version
11082	Boozt index.cgi overflow
11642	Helix RealServer Buffer Overrun
11389	rsync modules
10387	cisco http DoS
10984	CSCdu81936
10353	Interscan 3.32 SMTP Denial
11697	IRCXPro Default Admin password
10411	klogind overflow
11614	Novell FTP DoS
10983	CSCdu20643
11014	Cisco Aironet Telnet DoS
10102	HotSync Manager Denial of Service attack
10145	Microsoft's SQL TCP/IP denial of service
10423	qpopper euidl problem
11133	Generic format string
10136	MDaemon crash
10315	WINS UDP flood denial
11410	Notes detection
11422	Unconfigured web server
10175	Detect presence of PGPNet server and its version
10735	Generic flood
11512	Kerberos 5 issues



11495 tanned format string vulnerability  
10727 Buffer overflow in Solaris in.lpd  
10182 Livingston Portmaster crash  
11110 SMB null param count DoS  
11645 wsmpp3d command execution  
10159 News Server type and version  
11338 Lotus Domino Vulnerabilities  
10605 BIND vulnerable to overflows  
11403 iPlanet Application Server Buffer Overflow  
10517 pam\_smb / pam\_ntdom overflow  
10881 SSH protocol versions supported  
10269 SSH Overflow  
10254 SLMail denial of service  
10857 SNMP bad length field DoS  
11159 MS RPC Services null pointer reference DoS  
10048 Communigate Pro overflow  
11283 CSCdp58462  
11547 CSCea42030  
11544 MonkeyWeb POST with too much data  
10292 uw-imap buffer overflow  
10647 ntpd overflow  
10346 Mercur WebView WebClient  
11150 Tomcat servlet engine MD/DOS device names denial of service  
10782 Formmail Version Information Disclosure  
10271 stream.c  
11651 Batalla Naval Overflow  
11650 MAILsweeper PowerPoint DoS  
10184 Various pop3 overflows  
11036 SMTP antivirus scanner DoS  
11689 Cisco IDS Device Manager Detection  
11613 CP syslog overflow  
11311 shtml.exe overflow  
10062 Eicon Diehl LAN ISDN modem DoS  
11314 Buffer overflow in Microsoft Telnet  
10879 Shell Command Execution Vulnerability  
10488 FTP Serv -U 2.5e DoS  
11540 PPTP overflow  
10657 NT IIS 5.0 Malformed HTTP Printer Request Header Buffer  
Overflow Vulnerability  
10886 BIND vulnerable to DNS storm  
11291 CSCdv66718  
11335 mibiisa overflow  
11021 irix rpc.passwd overflow  
11632 CSCdx17916, CSCdx61997  
10786 Samba Remote Arbitrary File Creation  
10559 XMail APOP Overflow  
11075 dwhttpd format string  
10381 Piranha's RH6.2 default password  
11552 mod\_ntlm overflow / format string bug  
11175 Too long line  
10719 MySQL Server version  
10320 Too long URL  
10354 vqServer administrative port  
10130 ipop2d buffer overflow  
11619 Eserv Memory Leaks  
10497 Microsoft Frontpage DoS  
10635 Marconi ASX DoS  
10607 SSH1 CRC -32 compensation att ack  
10129 INN version check  
10123 Imail's imap buffer overflow  
11510 BIND 4.x resolver overflow

10744 VisualRoute Web Server Detection  
11380 CSCdz39284, CSCdz41124  
10134 Linux 2.1.89 - 2.2.3 : 0 length fragment bug  
11096 Avirt gateway insecure telnet proxy  
11560 WebServer 4D GET Buffer Overflow  
11199 Multiple vulnerabilities in CUPS  
11594 CSCdea77143, CSCdz15393, CSCdt84906  
10414 WinLogon.exe DoS  
10580 netscape imap buffer overflow after logon  
11295 CSCdx39981  
10496 Imail Host: overflow  
11655 D-Link router overflow  
11136 /bin/login overflow exploitation  
11296 CSCdx54675  
10745 WorldClient for MDaemon Server Detection  
11342 PKCS #1 Version 1.5 Session Key Retrieval  
11131 Sambar web server DOS  
10741 SiteScope Web Administration Server Detection  
10384 IRIX Objectserver  
10995 Sun JavaServer Default Admin Password  
10375 Ken! DoS  
10109 SCO i2odialogd buffer overrun  
10802 OpenSSH < 3.0.1  
10199 RealServer Ramgen crash (ramcrash)  
10737 Oracle Applications One -Hour Install Detect  
10139 MDaemon Worldclient crash  
10160 Nortel Contivity DoS  
11473 EMule DoS  
11494 l2tpd DoS  
10871 DB2 DOS  
10980 CSCdt62732  
11063 LabView web server DoS  
10263 SMTP Server type and version  
10884 NTP read variables  
11026 Access Point detection  
10684 yppasswdd overflow  
11077 HTTP Cookie overflow  
10558 Exchange Malformed MIME header  
10976 CSCds04747  
11002 DNS Server Detection  
10753 AOLserver Default Password  
10878 Sun Cobalt Adaptive Firewall Detection  
10030 Bonk  
11543 mod\_access\_referer 1.0.2 NULL pointer dereference  
11024 p-smash DoS (ICMP 9 flood)  
11062 BadBlue invalid GET DoS  
10374 uw-imap buffer overflow after logon  
11030 Apache chunked encoding  
10973 CSCdi34061  
10827 SysV /bin/login buffer overflow (telnet)  
11381 CSCdw33027  
10443 Predictable TCP sequence number  
10108 Hyperbomb  
11340 SSH Secure -RPC Weak Encrypted Authentication  
10042 Chameleon SMTPd overflow  
11435 ActiveSync packet overflow  
10116 IIS buffer overflow  
10421 Rockliffe's MailSite overflow  
10927 BlackIce DoS (ping flood)  
10935 IIS ASP ISAPI filter Overflow  
10169 OpenLink web config buffer overflow

11113 Samba Buffer Overflow  
10200 RealServer G2 buffer overrun  
11545 Xeneo Web Server 2.2.9.0 DoS  
11343 OpenSSH Client Unauthorized Remote Forwarding  
11056 CSCdy03429  
10923 Squid overflows  
11294 CSCdw50657  
11339 scp File Create/Overwrite  
10206 Rover pop3 overflow  
10255 SLMail:27 denial of service  
10438 Netwin's DMail ETRN overflow  
10699 IIS FrontPage DoS II  
10755 Microsoft Exchange Public Folders Information Leak  
10197 qpopper LIST buffer overflow  
11140 UDDI detection  
10978 CSCds66191  
11084 Infinite HTTP request  
10963 Compaq Web Based Management Agent Proxy Vulnerability  
10183 pnservr crash  
10162 Notes MTA denial  
11390 rsync array overflow  
11559 Network Chemistry Wireless Sensor Detection  
11299 MySQL double free()  
11289 CSCdu35577  
10171 Oracle Web Server denial of Service  
11004 WhatsUp Gold Default Admin Account  
10951 cachefs overflow  
10965 SSH 3 AllowedAuthentication  
11279 Webmin Session ID Spoofing  
10708 SSH 3.0.0  
10970 GSR ACL pub  
10118 IIS FTP server crash  
11141 Crash SMC AP  
10133 Land  
11376 qpopper Qvsnprintf buffer overflow  
10441 AFS client version  
10685 IIS ISAPI Overflow  
10125 Imap buffer overflow  
11061 HTTP version number overflow  
10313 WindowsNT PPTP flood denial  
10731 HealthD detection  
10690 GoodTech ftpd DoS  
10826 Unprotected Netware Management Portal  
10882 SSH protocol version 1 enabled  
11579 FTgate DoS  
10740 SiteScope Web Management Server Detect  
10439 OpenSSH < 2.1.1 UseLogin feature  
10392 rfparalyze  
11155 LiteServe URL Decoding DoS  
10310 Wingate denial of service  
10138 MDaemon Webconfig crash  
10202 remwatch  
10201 Relative IP Identification number change  
10196 qpopper buffer overflow  
11382 CSCdv85279, CSCdw59394  
10954 OpenSSH AFS/Kerberos ticket/token passing  
10929 FTP Windows 98 MS/DOS device names DOS  
10445 AnalogX denial of service by long CGI name  
10561 cisco 675 http DoS  
11174 HTTP negative Content-Length DoS  
10406 IIS Malformed Extension Data in URL

10366 AnalogX denial of service  
10344 Detect the presence of Napster  
11570 MDAemon DELE DoS  
11195 SSH Multiple Vulns  
10804 rwhois format string attack (2)  
11521 Abyss httpd crash  
11127 HTTP 1.0 header overflow  
10268 SSH Insertion Attack  
11192 multiple MySQL flaws  
10442 NAI PGP Cert Server DoS  
10705 SimpleServer remote execution  
10302 robot(s).txt exists on the Web Server  
11059 Trend Micro OfficeScan Denial of service  
11513 Solaris lpd remote command execution  
10663 DHCP server info gathering  
10659 snmpXdmid overflow  
11081 Oracle9iAS too long URL  
11484 apcupsd overflows  
11013 Cisco VoIP phones DoS  
11031 OpenSSH <= 3.3  
11277 clarkconnectd detection  
10326 Yahoo Messenger Denial of Service attack  
10636 Orange DoS  
10257 SmartServer pop3 overflow  
11028 IIS .HTR overflow  
10820 F5 Device Default Support Password  
11355 Buffer overflow in AIX lpd  
10450 Dragon FTP overflow  
10272 SunKill  
10119 NT IIS Malformed HTTP Request Header DoS Vulnerability  
10812 libgtop\_daemon format string  
10461 Check for RealServer DoS  
10700 Cisco IOS HTTP Configuration Arbitrary Administrative Access  
11278 Quicktime/Darwin Remote Admin Exploit  
11128 redhat Interchange  
11313 MCMS : Buffer overflow in Profile Service  
10019 Ascend Kill  
11456 PostgreSQL multiple flaws  
11130 BrowseGate HTTP headers overflows  
11517 Leafnode Resource Exhaustion  
11040 HTTP TRACE  
10092 FTP Server type and version  
10170 OShare  
10163 Novell Border Manager  
11202 Enhypdra Multiserver Default Password  
11156 IRC daemon identification  
10185 POP3 Server type and version detected  
11474 NetGear ProSafe VPN Login DoS  
10463 vpopmail input validation bug  
11285 CSCdy26428  
11108 Omron WorldView Wnn Overflow  
10718 DCShop exposes sensitive files  
10981 CSCdt65960  
11520 HP Instant TopTools DoS  
10322 Xitami Web Server buffer overflow  
10808 DoSable Oracle WebCache server  
10742 Amanda Index Server version  
11209 Apache < 2.0.44 DOS device name  
10941 IPSEC IKE check  
11167 Webserver4everyone too long URL  
11442 Samba TNG multiple flaws

11168 Samba Unicode Buffer Overflow  
10273 Detect SWAT server port  
11598 MailMax IMAP overflows  
11292 CSCdv88230, CSCdw22408  
11577 MDaemon IMAP CREATE overflow  
11069 HTTP User-Agent overflow  
10793 Cobalt Web Administration Server Detection  
10764 Shopping Cart Arbitrary Command Execution (Hassan)  
10154 Netscape Enterp rise 'Accept' buffer overflow  
10752 Apache Auth Module SQL Insertion Attack  
11603 MacOS X Directory Service DoS  
10791 Ultraseek Web Server Detect  
11523 Samba trans2open buffer overflow  
10759 Content-Location HTTP Header  
10732 IIS 5.0 WebDav Memory Leakage  
11406 Buffer overflow in BSD in.lpd  
10472 SSH Kerberos issue  
11068 iPlanet chunked encoding  
10425 NAI Management Agent overflow  
10987 CSCdw67458  
10361 SalesLogix Eviewer WebApp crash  
10312 WindowsNT DNS flood denial  
10600 ICECast Format String  
10204 rfpoison  
11475 3com RAS 1500 DoS  
10982 CSCdt93866  
11409 ePolicy orchestrator format string  
10654 Oracle Application Server Overflow  
11060 OpenSSL overflow (generic test)  
10388 Cassandra NNTP Server DoS  
11054 fakeidentd overflow  
10625 IMAP4rev1 buffer overflow after login  
10451 Dragon telnet overflow  
10557 WebShield  
10338 smad  
10179 pimp  
10709 TESO in.telnetd buffer overflow  
10538 iWS shtml overflow  
11402 iPlanet Application Server Detection  
10883 OpenSSH Channel Code Off by 1  
10590 SWAT allows user names to be obtained by brute force  
11297 CSCdy38035  
11184 vxworks ftpd buffer overflow Denial of Service  
11089 Webseal denial of service  
10595 DNS AXFR  
10325 Xtramail pop3 overflow  
11076 Oracle webcache admin interface  
11525 WWW fingerprinting  
10051 A CVS pserver is running  
11196 Cyrus IMAP pre-login buffer overrun  
11280 Usermin Session ID Spoofing  
10046 Cisco DoS  
10074 Firewall/1 UDP port 0 DoS  
11085 Personal Web Sharing overflow  
10137 MDaemon DoS  
10522 LPRng malformed input  
10762 RTSP Server type and version  
11511 Kerberos IV cryptographic weaknesses  
11483 apcnisd detection  
10377 RealServer denial of Service  
11637 MailMax IMAP overflows (2)

10972 Multiple SSH vulnerabilities  
10937 IIS FrontPage ISAPI Denial of Service  
10667 IIS 5.0 PROPFIND Vulnerability  
10436 INN version check (2)  
10966 IMAP4buffer overflow in the BODY command  
11268 OS fingerprint  
10267 SSH Server type and version  
10380 rsh on finger output  
11051 BIND9 DoS  
10950 rpc.walld format string  
10054 Delegate overflow  
10858 SNMP bad length field DoS (2)  
10026 BFTelnet DoS  
10135 LinuxConf grants network access  
11228 Unreal Engine flaws  
10746 Compaq WBEM Server Detection  
11235 Too long OPTIONS parameter  
10637 Sedum DoS  
11181 WebSphere Host header overflow  
11546 Xeneo web server %A DoS  
11388 l2tpd < 0.68 overflow  
11354 Buffer overflow in FreeBSD 2.x lpd  
10748 Mediahouse Statistics Web Server Detect  
10066 FakeBO buffer overflow  
11384 Public CVS pserver  
11337 mountd overflow  
10979 CSCdt46181  
11204 Apache Tomcat Default Accounts  
10682 CISCO view -source DoS  
11035 AnalogX SimpleServer:WWW DoS  
10790 rwhois format string attack  
10311 Wingate POP3 USER overflow  
11383 CSCdz60229, CSCdy87221, CSCdu75477  
10925 Oracle Jserv Executes outside of doc\_root  
10418 Standard & Poors detection  
10285 thttpd 2.04 buffer overflow  
11126 SOCKS4A hostname overflow  
10422 MDBMS overflow  
10168 Detect talkd server port and protocol version  
10545 Cisco Catalyst Web Execution  
10985 CSCdv48261  
10743 Tripwire for Webpages Detection  
10974 CSCdi36962  
10314 Winnuke  
10918 Apache -SSL overflow  
11424 WebDAV enabled  
11114 Canna Overflow  
11624 SHOUTcast Server logfiles XSS  
10967 Shambala web server DoS  
10124 Imail's imonitor buffer overflow  
10631 IIS propfind DoS  
10946 Gnutella server detection  
10474 GAMSsoft TelSrv 1.4/1.5 Overflow  
10266 UDP null size going to SNMP DoS  
10279 Teardrop  
11208 Netscape Enterprise Default Administrative Password  
10029 BIND vulnerable  
10707 McAfee myCIO detection  
11162 WebSphere Edge caching proxy denial of service  
10986 CSCdw19195  
10876 Delta UPS Daemon Detection

10585 IIS FrontPage DoS  
10975 CSCdp35794  
10096 rsh with null username  
11379 CSCdx92043  
10582 HTTP version spoken  
11012 ATA-186 password circumvention / recovery  
10768 DoSable squid proxy server  
11287 CSCdt56514  
10147 A Nessus Daemon is running  
11318 BIND 9 overflow  
10111 iParty  
10608 OpenSSH 2.3.1 authentication bypass vulnerability  
10633 Savant DoS  
10999 Linksys Router Default Password  
10410 ICEcap default password  
10161 rlogin -froot  
10560 SuSE's identd overflow  
11612 PXE server overflow  
11164 SOCKS4 username overflow  
10856 PHP-Nuke sql\_debug Information Disclosure  
10017 Annex DoS  
10689 Netscape Enterprise '../' buffer overflow  
10539 Useable remote name server  
11414 IMAP Banner  
10020 + + + ATH0 modem hangup  
10930 HTTP Windows 98 MS/DOS device names DOS  
10097 GroupWise buffer overflow  
10771 OpenSSH 2.5.x -> 2.9.x adv.option  
11078 HTTP header overflow  
10462 Amanda client version  
10347 ICQ Denial of Service attack  
11290 CSCdu82823  
10578 Oops buffer overflow  
11033 Misc information on News server  
10251 rpc.nisd overflow  
11099 Pi3Web Webserver v2.0 Buffer Overflow  
11600 NetCharts Server Default Password  
11563 Oracle LINK overflow  
11129 HTTP 1.1 header overflow  
10420 Gauntlet overflow  
10289 Microsoft Media Server 4.1 - DoS  
11023 lpd, dvips and remote command execution  
10738 Oracle Web Administration Server Detection  
11188 X Font Service Buffer Overflow  
10089 FTP ServU CWD overflow  
10596 Tinyproxy heap overflow  
11293 CSCdx07754, CSCdx24622, CSCdx24632  
10155 Netscape Enterprise Server DoS  
11398 Samba Fragment Reassembly Overflow  
10939 MSDTC denial of service by flooding with null bytes  
11412 IIS : WebDAV Overflow (MS03 -007)  
10828 SysV /bin/login buffer overflow (rlogin)  
10823 OpenSSH UseLogin Environment Variables  
10751 Kazaa / Morpheus Client Detection  
10148 Nestea  
10059 Domino HTTP Denial  
11090 AppSocket DoS  
10833 dtspcd overflow  
10971 GSR ICMP unreachable  
11385 CVS pserver double free() bug  
11556 CISCO Secure ACS Management Interface Login Overflow

```

11695 Pi3Web Webserver v2.0 Denial of Service
10540 NSM format strings vulnerability
10816 Webalizer Cross Site Scripting Vulnerability
10281 Detect Server type and version via Telnet
11065 HTTP method overflow
10117 IIS 'GET ../../'

```

Preferences settings for this scan:

```

max_hosts                = 16
max_checks               = 10
log_whole_attack         = yes
cgi_path                 = /cgi -bin
port_range               = 1 -1024
optimize_test            = yes
language                 = english
checks_read_timeout      = 5
non_simult_ports         = 139, 445
plugins_timeout          = 320
safe_checks              = yes
auto_enable_dependencies = no
use_mac_addr             = no
save_knowledge_base      = no
kb_restore               = no
only_test_hosts_whose_kb_we_dont_have = no
only_test_hosts_whose_kb_we_have     = no
kb_dont_replay_scanners  = no
kb_dont_replay_info_gathering = no
kb_dont_replay_attacks   = no
kb_dont_replay_denials   = no
kb_max_age               = 864000
plugin_upload            = no
plugin_upload_suffixes   = .nasl, .inc
ntp_save_sessions        = yes
ntp_detached_sessions    = yes
server_info_nessusd_version = 2.0.6
server_info_libnasl_version = 2.0.6
server_info_libnessus_version = 2.0.6
server_info_thread_manager = fork
server_info_os            = Linux
server_info_os_version    = 2.4.18 -3
reverse_lookup            = no
ntp_keep_communication_alive = yes
ntp_opt_show_end          = yes
save_session              = no
detached_scan             = no
continuous_scan           = no

```

```

Total security holes found : 0
    high severity : 0
    low severity : 0
    informational : 0

```

Scanned hosts:

Name	High	Low	Info
-----	-----	-----	-----
dmz.add.1.129	0	0	0



# NESSUS SECURITY SCAN REPORT

Created 13.07.2003

Sorted by host names

Session Name : **pix from inside**  
Start Time : 13.07.2003 11:25:28  
Finish Time : 13.07.2003 11:32:23  
Elapsed Time : 0 day(s) 00:06:54

## Plugins used in this scan:

Id	Name
-----	-----
10018	Knox Arkeia buffer overflow
10728	Determine if Bind 9 is running
10515	Too long authorization
11519	mod_jk chunked encoding DoS
11288	CSCdu15622
10717	SHOUTcast Server DoS detector vulnerability
10977	CSCds07326
11152	BIND vulnerable to cached RR overflow
10754	Cisco password not set
11320	The remote BIND has dynamic updates enabled
11169	SSH setsid() vulnerability
10028	Determine which version of BIND name daemon is running
10687	Too long POST command
11341	SSH1 SSH Daemon Logging Failure
11047	Jigsaw webserver MS/DOS device DoS
11198	BitKeeper remote command execution
10022	Axent Raptor's DoS
11312	DHCP server overflow / format string bug
10329	BIND query overflow
10012	Alibaba 2.0 buffer overflow
10107	HTTP Server type and version
11082	Boozt index.cgi overflow
11642	Helix RealServer Buffer Overrun
11389	rsync modules
10387	cisco http DoS
10984	CSCdu81936
10353	InterScan 3.32 SMTP Denial
11697	IRCXPro Default Admin password
10411	klogind overflow
11614	Novell FTP DoS
10983	CSCdu20643
11014	Cisco Aironet Telnet DoS
10102	HotSync Manager Denial of Service attack
10145	Microsoft's SQL TCP/IP denial of service
10423	qpopper euidl problem
11133	Generic format string
10136	MDaemon crash
10315	WINS UDP flood denial
11410	Notes detection
11422	Unconfigured web server
10175	Detect presence of PGPNet server and its version
10735	Generic flood
11512	Kerberos 5 issues
11495	tanned format string vulnerability
10727	Buffer overflow in Solaris in.lpd
10182	Livingston Portmaster crash

11110 SMB null param count DoS  
 11645 wsm3d command execution  
 10159 News Server type and version  
 11338 Lotus Domino Vulnerabilities  
 10605 BIND vulnerable to overflows  
 11403 iPlanet Application Server Buffer Overflow  
 10517 pam\_smb / pam\_ntdom overflow  
 10881 SSH protocol versions supported  
 10269 SSH Overflow  
 10254 SLMail denial of service  
 10857 SNMP bad length field DoS  
 11159 MS RPC Services null pointer reference DoS  
 10048 Communicate Pro overflow  
 11283 CSCdp58462  
 11547 CSCea42030  
 11544 MonkeyWeb POST with too much data  
 10292 uw-imap buffer overflow  
 10647 ntpd overflow  
 10346 Mercur WebView WebClient  
 11150 Tomcat servlet engine MD/DOS device names denial of service  
 10782 Formmail Version Information Disclosure  
 10271 stream.c  
 11651 Batalla Naval Overflow  
 11650 MAILsweeper PowerPoint DoS  
 10184 Various pop3 overflows  
 11036 SMTP antivirus scanner DoS  
 11689 Cisco IDS Device Manager Detection  
 11613 CP syslog overflow  
 11311 shtml.exe overflow  
 10062 Eicon Diehl LAN ISDN modem DoS  
 11314 Buffer overflow in Microsoft Telnet  
 10879 Shell Command Execution Vulnerability  
 10488 FTP Serv -U 2.5e DoS  
 11540 PPTP overflow  
 10657 NT IIS 5.0 Malformed HTTP Printer Request Header Buffer  
 Overflow Vulnerability  
 10886 BIND vulnerable to DNS storm  
 11291 CSCdv66718  
 11335 mibiisa overflow  
 11021 irix rpc.passwd overflow  
 11632 CSCdx17916, CSCdx61997  
 10786 Samba Remote Arbitrary File Creation  
 10559 XMail APOP Overflow  
 11075 dwhhttpd format string  
 10381 Piranha's RH6.2 default password  
 11552 mod\_ntlm overflow / format string bug  
 11175 Too long line  
 10719 MySQL Server version  
 10320 Too long URL  
 10354 vqServer administrative port  
 10130 ipop2d buffer overflow  
 11619 Eserv Memory Leaks  
 10497 Microsoft Frontpage DoS  
 10635 Marconi ASX DoS  
 10607 SSH1 CRC -32 compensation attack  
 10129 INN version check  
 10123 Imail's imap buffer overflow  
 11510 BIND 4.x resolver overflow  
 10744 VisualRoute Web Server Detection  
 11380 CSCdz39284, CSCdz41124  
 10134 Linux 2.1.89 - 2.2.3 : 0 length fragment bug

11096 Avirt gateway insecure telnet proxy  
11560 WebServer 4D GET Buffer Overflow  
11199 Multiple vulnerabilities in CUPS  
11594 CSCdea77143, CSCdz15393, CSCdt84906  
10414 WinLogon.exe DoS  
10580 netscape imap buffer overflow after login  
11295 CSCdx39981  
10496 Imail Host: overflow  
11655 D-Link router overflow  
11136 /bin/login overflow exploitation  
11296 CSCdx54675  
10745 WorldClient for MDaemon Server Detection  
11342 PKCS #1 Version 1.5 Session Key Retrieval  
11131 Sambar web server DOS  
10741 SiteScope Web Administration Server Detection  
10384 IRIX Objectserver  
10995 Sun JavaServer Default Admin Password  
10375 Ken! DoS  
10109 SCO i2odialogd buffer ov errun  
10802 OpenSSH < 3.0.1  
10199 RealServer Ramgen crash (ramcrash)  
10737 Oracle Applications One -Hour Install Detect  
10139 MDaemon Worldclient crash  
10160 Nortel Contivity DoS  
11473 EMule DoS  
11494 l2tpd DoS  
10871 DB2 DOS  
10980 CSCdt627 32  
11063 LabView web server DoS  
10263 SMTP Server type and version  
10884 NTP read variables  
11026 Access Point detection  
10684 yppasswdd overflow  
11077 HTTP Cookie overflow  
10558 Exchange Malformed MIME header  
10976 CSCds04747  
11002 DNS Server Detection  
10753 AOLserver Default Password  
10878 Sun Cobalt Adaptive Firewall Detection  
10030 Bonk  
11543 mod\_access\_referer 1.0.2 NULL pointer dereference  
11024 p-smash DoS (ICMP 9 flood)  
11062 BadBlue invalid GET DoS  
10374 uw-imap buffer overflow after login  
11030 Apache chunked encoding  
10973 CSCdi34061  
10827 SysV /bin/login buffer overflow (telnet)  
11381 CSCdw33027  
10443 Predictable TCP sequence number  
10108 Hyperbomb  
11340 SSH Secure -RPC Weak Encrypted Authentication  
10042 Chameleon SMTPd overflow  
11435 ActiveSync packet overflow  
10116 IIS buffer overflow  
10421 Rockliffe's MailSite overflow  
10927 BlackIce DoS (ping flood)  
10935 IIS ASP ISAPI filter Overflow  
10169 OpenLink web config buffer overflow  
11113 Samba Buffer Overflow  
10200 RealServer G2 buffer overrun  
11545 Xeneo Web Server 2.2.9.0 DoS

11343 OpenSSH Client Unauthorized Remote Forwarding  
11056 CSCdy03429  
10923 Squid overflows  
11294 CSCdw50657  
11339 scp File Create/Overwrite  
10206 Rover pop3 overflow  
10255 SLMail:27 denial of service  
10438 Netwin's DMail ETRN overflow  
10699 IIS FrontPage DoS II  
10755 Microsoft Exchange Public Folders Information Leak  
10197 qpopper LIST buffer overflow  
11140 UDDI detection  
10978 CSCds6619 1  
11084 Infinite HTTP request  
10963 Compaq Web Based Management Agent Proxy Vulnerability  
10183 pnserver crash  
10162 Notes MTA denial  
11390 rsync array overflow  
11559 Network Chemistry Wireless Sensor Detection  
11299 MySQL double free()  
11289 CSCdu35577  
10171 Oracle Web Server denial of Service  
11004 WhatsUp Gold Default Admin Account  
10951 cachefs overflow  
10965 SSH 3 AllowedAuthentication  
11279 Webmin Session ID Spoofing  
10708 SSH 3.0.0  
10970 GSR ACL pub  
10118 IIS FTP server crash  
11141 Crash SMC AP  
10133 Land  
11376 qpopper Qvsnprintf buffer overflow  
10441 AFS client version  
10685 IIS ISAPI Overflow  
10125 Imap buffer overflow  
11061 HTTP version number overflow  
10313 WindowsNT PPTP flood denial  
10731 Health D detection  
10690 GoodTech ftpd DoS  
10826 Unprotected Netware Management Portal  
10882 SSH protocol version 1 enabled  
11579 FTgate DoS  
10740 SiteScope Web Management Server Detect  
10439 OpenSSH < 2.1.1 UseLogin feature  
10392 rfparalyze  
11155 LiteServe URL Decoding DoS  
10310 Wingate denial of service  
10138 MDaemon Webconfig crash  
10202 remwatch  
10201 Relative IP Identification number change  
10196 qpopper buffer overflow  
11382 CSCdv85279, CSCdw59394  
10954 OpenSSH AFS/Kerberos ticket token passing  
10929 FTP Windows 98 MS/DOS device names DOS  
10445 AnalogX denial of service by long CGI name  
10561 cisco 675 http DoS  
11174 HTTP negative Content -Length DoS  
10406 IIS Malformed Extension Data in URL  
10366 AnalogX denial of service  
10344 Detect the presence of Napster  
11570 MDaemon DELETE DoS

11195 SSH Multiple Vulns  
10804 rwhois format string attack (2)  
11521 Abyss httpd crash  
11127 HTTP 1.0 header overflow  
10268 SSH Insertion Attack  
11192 multiple MySQL flaws  
10442 NAI PGP Cert Server DoS  
10705 SimpleServer remote execution  
10302 robot(s).txt exists on the Web Server  
11059 Trend Micro OfficeScan Denial of service  
11513 Solaris lpd remote command execution  
10663 DHCP server info gathering  
10659 snmpXdmid overflow  
11081 Oracle9iAS too long URL  
11484 apcupsd overflows  
11013 Cisco VoIP phones DoS  
11031 OpenSSH <= 3.3  
11277 clarkconnectd detection  
10326 Yahoo Messenger Denial of Service attack  
10636 Orange DoS  
10257 SmartServer pop3 overfl ow  
11028 IIS .HTR overflow  
10820 F5 Device Default Support Password  
11355 Buffer overflow in AIX lpd  
10450 Dragon FTP overflow  
10272 SunKill  
10119 NT IIS Malformed HTTP Request Header DoS Vulnerability  
10812 libgtop\_daemon format string  
10461 Check for RealServer DoS  
10700 Cisco IOS HTTP Configuration Arbitrary Administrative Access  
11278 Quicktime/Darwin Remote Admin Exploit  
11128 redhat Interchange  
11313 MCMS : Buffer overflow in Profile Service  
10019 Ascend Kill  
11456 Postgres QL multiple flaws  
11130 BrowseGate HTTP headers overflows  
11517 Leafnode Resource Exhaustion  
11040 HTTP TRACE  
10092 FTP Server type and version  
10170 OShare  
10163 Novell Border Manager  
11202 Enhadra Multiserver Default Password  
11156 IRC da emon identification  
10185 POP3 Server type and version detected  
11474 NetGear ProSafe VPN Login DoS  
10463 vpopmail input validation bug  
11285 CSCdy26428  
11108 Omron WorldView Wnn Overflow  
10718 DCShop exposes sensitive files  
10981 CSCdt65960  
11520 HP Instant TopTools DoS  
10322 Xitami Web Server buffer overflow  
10808 DoSable Oracle WebCache server  
10742 Amanda Index Server version  
11209 Apache < 2.0.44 DOS device name  
10941 IPSEC IKE check  
11167 Webserver4everyone too long URL  
11442 Samba TNG multiple flaws  
11168 Samba Unicode Buffer Overflow  
10273 Detect SWAT server port  
11598 MailMax IMAP overflows

11292 CSCdv88230, CSCdw22408  
11577 MDAemon IMAP CREATE overflow  
11069 HTTP User -Agent overflow  
10793 Cobalt Web Administration Server Detection  
10764 Shopping Cart Arbitrary Command Execution (Hassan)  
10154 Netscape Enterprise 'Accept' buffer overflow  
10752 Apache Auth Module SQL Insertion Attack  
11603 MacOS X Directory Service DoS  
10791 Ultraseek Web Server Detection  
11523 Samba trans2open buffer overflow  
10759 Content -Location HTTP Header  
10732 IIS 5.0 WebDav Memory Leakage  
11406 Buffer overflow in BSD in.lpd  
10472 SSH Kerberos issue  
11068 iPlanet chunked encoding  
10425 NAI Management Agent overflow  
10987 CSCdw67458  
10361 SalesLogix Eviewer WebApp crash  
10312 WindowsNT DNS flood denial  
10600 ICECast Format String  
10204 rfpoison  
11475 3com RAS 1500 DoS  
10982 CSCdt93866  
11409 ePolicy orchestrator format string  
10654 Oracle Application Server Overflow  
11060 OpenSSL overflow (generic test)  
10388 Cassandra NNTP Server DoS  
11054 fakeidentd overflow  
10625 IMAP4rev1 buffer overflow after login  
10451 Dragon telnet overflow  
10557 WebShield  
10338 smad  
10179 pimp  
10709 TESO in. telnetd buffer overflow  
10538 iWS shtml overflow  
11402 iPlanet Application Server Detection  
10883 OpenSSH Channel Code Off by 1  
10590 SWAT allows user names to be obtained by brute force  
11297 CSCdy38035  
11184 vxworks ftpd buffer overflow Denial of Service  
11089 Webseal denial of service  
10595 DNS AXFR  
10325 Xtramail pop3 overflow  
11076 Oracle webcache admin interface  
11525 WWW fingerprinting  
10051 A CVS pserver is running  
11196 Cyrus IMAP pre -login buffer overrun  
11280 Usermin Session ID Spoofing  
10046 Cisco DoS  
10074 Firewall/1 UDP port 0 DoS  
11085 Personal Web Sharing overflow  
10137 MDAemon DoS  
10522 LPRng malformed input  
10762 RTSP Server type and version  
11511 Kerberos IV cryptographic weaknesses  
11483 apcnisd detection  
10377 RealServer denial of Service  
11637 MailMax IMAP overflows (2)  
10972 Multiple SSH vulnerabilities  
10937 IIS FrontPage ISAPI Denial of Service  
10667 IIS 5.0 PROPFIND Vulnerability

10436 INN version check (2)  
10966 IMAP4buffer overflow in the BODY command  
11268 OS fingerprint  
10267 SSH Server type and version  
10380 rsh on finger output  
11051 BIND9 DoS  
10950 rpc.walld format string  
10054 Delegate overflow  
10858 SNMP bad length field DoS (2)  
10026 BFTelnet DoS  
10135 LinuxConf grants network access  
11228 Unreal Engine flaws  
10746 Compaq WBEM Server Detection  
11235 Too long OPTIONS parameter  
10637 Sedum DoS  
11181 WebSphere Host header overflow  
11546 Xeneo web server %A DoS  
11388 l2tpd < 0.68 overflow  
11354 Buffer overflow in FreeBSD 2.x lpd  
10748 Mediahouse Statistics Web Server Detect  
10066 FakeBO buffer overflow  
11384 Public CVS pserver  
11337 mountd overflow  
10979 CSCdt46181  
11204 Apache Tomcat Default Accounts  
10682 CISCO view -source DoS  
11035 AnalogX SimpleServer:WWW DoS  
10790 rwhois format string attack  
10311 Wingate POP3 USER overflow  
11383 CSCdz60229, CSCdy87221, CSCdu75477  
10925 Oracle Jserv Executes outside of doc\_root  
10418 Standard & Poors detection  
10285 thttpd 2.04 buffer overflow  
11126 SOCKS4A hostname overflow  
10422 MDBMS overflow  
10168 Detect talkd server port and protocol version  
10545 Cisco Catalyst Web Execution  
10985 CSCdv48261  
10743 Tripwire for Webpages Detection  
10974 CSCdi36962  
10314 Winnuke  
10918 Apache -SSL overflow  
11424 WebDAV enabled  
11114 Canna Overflow  
11624 SHOUTcast Server logfiles XSS  
10967 Shambala web server DoS  
10124 Imail's imonitor buffer overflow  
10631 IIS propfind DoS  
10946 Gnutella servent detection  
10474 GAMSoft TelSrv 1.4/1.5 Overflow  
10266 UDP null size going to SNMP DoS  
10279 Teardrop  
11208 Netscape Enterprise Default Administrative Password  
10029 BIND vulnerable  
10707 McAfee myCIO detection  
11162 WebSphere Edge caching proxy denial of service  
10986 CSCdw19195  
10876 Delta UPS Daemon Detection  
10585 IIS FrontPage DoS  
10975 CSCdp35794  
10096 rsh with null username

11379 CSCdx92043  
10582 HTTP version spoken  
11012 ATA-186 password circumvention / recovery  
10768 DoSable squid proxy server  
11287 CSCdt56514  
10147 A Nessus Daemon is running  
11318 BIND 9 overflow  
10111 iParty  
10608 OpenSSH 2.3.1 authentication bypass vulnerability  
10633 Savant DoS  
10999 Linksys Router Default Password  
10410 ICEcap default password  
10161 rlogin -froot  
10560 SuSE's identd overflow  
11612 PXE server overflow  
11164 SOCKS4 username overflow  
10856 PHP-Nuke sql\_debug Information Disclosure  
10017 Annex DoS  
10689 Netscape Enterprise '../' buffer overflow  
10539 Useable remote name server  
11414 IMAP Banner  
10020 + + + ATH0 modem hangup  
10930 HTTP Windows 98 MS/DOS device names DOS  
10097 GroupWise buffer overflow  
10771 OpenSSH 2.5.x -> 2.9.x adv.option  
11078 HTTP header overflow  
10462 Amanda client version  
10347 ICQ Denial of Service attack  
11290 CSCdu82823  
10578 Oops buffer overflow  
11033 Misc information on News server  
10251 rpc.nisd overflow  
11099 Pi3Web Webserver v2.0 Buffer Overflow  
11600 NetCharts Server Default Password  
11563 Oracle LINK overflow  
11129 HTTP 1.1 header overflow  
10420 Gauntlet overflow  
10289 Microsoft Media Server 4.1 - DoS  
11023 lpd, dvips and remote command execution  
10738 Oracle Web Administration Server Detection  
11188 X Font Service Buffer Overflow  
10089 FTP ServU CWD overflow  
10596 Tinyproxy heap overflow  
11293 CSCdx07754, CSCdx24622, CSCdx24632  
10155 Netscape Enterprise Server DoS  
11398 Samba Fragment Reassembly Overflow  
10939 MSDTC denial of service by flooding with nul bytes  
11412 IIS : WebDAV Overflow (MS03-007)  
10828 SysV /bin/login buffer overflow (rlogin)  
10823 OpenSSH UseLogin Environment Variables  
10751 Kazaa / Morpheus Client Detection  
10148 Nestea  
10059 Domino HTTP Denial  
11090 AppSocket DoS  
10833 dtspcd overflow  
10971 GSR ICMP unreachable  
11385 CVS pserver double free() bug  
11556 CISCO Secure ACS Management Interface Login Overflow  
11695 Pi3Web Webserver v2.0 Denial of Service  
10540 NSM format strings vulnerability  
10816 Webalizer Cross Site Scripting Vulnerability



```

10281 Detect Server type and version via Telnet
11065 HTTP method overflow
10117 IIS 'GET ../../'

```

Preferences settings for this scan:

```

max_hosts                = 16
max_checks               = 10
log_whole_attack         = yes
cgi_path                 = /cgi -bin
port_range               = 1 -1024
optimize_test            = yes
language                 = english
checks_read_timeout     = 5
non_simult_ports         = 139, 445
plugins_timeout          = 320
safe_checks              = yes
auto_enable_dependencies = no
use_mac_addr             = no
save_knowledge_base      = no
kb_restore               = no
only_test_hosts_whose_kb_we_dont_have = no
only_test_hosts_whose_kb_we_have     = no
kb_dont_replay_scanners = no
kb_dont_replay_info_gathering = no
kb_dont_replay_attacks  = no
kb_dont_replay_denials  = no
kb_max_age               = 864000
plugin_upload            = no
plugin_upload_suffixes  = .nasl, .inc
ntp_save_sessions        = yes
ntp_detached_sessions    = yes
server_info_nessusd_version = 2.0.6
server_info_libnasl_version = 2.0.6
server_info_libnessus_version = 2.0.6
server_info_thread_manager = fork
server_info_os            = Linux
server_info_os_version    = 2.4.18 -3
reverse_lookup            = no
ntp_keep_communication_alive = yes
ntp_opt_show_end         = yes
save_session             = no
detached_scan            = no
continuous_scan          = no

```

```

Total security holes found : 6
    high severity : 0
    low severity  : 4
    informational : 2

```

Scanned hosts:

Name	High	Low	Info
ins.add.50.241	0	4	2

Host: ins.add.50.241

Open ports:

ssh (22/tcp)  
general/tcp

Service: general/tcp  
Severity: Low

The remote host uses non -random IP IDs, that is, it is possible to predict the next value of the ip\_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch  
Risk factor : Low

Service: ssh (22/tcp )  
Severity: Low

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.5

Service: ssh (22/tcp)  
Severity: Low

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution :  
If you use OpenSSH, set the option 'Protocol' to '2'  
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

Risk factor : Low

Service: ssh (22/tcp)  
Severity: Low

Remote SSH version : SSH -1.5-Cisco-1.25

## Appendix C - References

- <sup>i</sup> Lemos, R., Counting the cost of Slammer, January 31, 2003, URL: <http://news.com.com/2100-1001-982955.html> (23/05/2003)
- <sup>ii</sup> Northcutt, S., Track 7.2, Auditing the Permitter, SANS Institute, 2003. pg. 3 -12
- <sup>iii</sup> Spitzner, L., Building your own firewall rulebase, January 26, 2000, URL: <http://www.spitzner.net/rules.html> (16/05/2003)
- <sup>iv</sup> Northcutt, S., Track 7.2, Auditing the Permitter, SANS Institute, 2003. pg. 4 -18
- <sup>v</sup> Spitzner, L., Building your own firewall rulebase, January 26, 2000, URL: <http://www.spitzner.net/rules.html> (16/05/2003)
- <sup>vi</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 4 (21/05/2003)
- <sup>vii</sup> Yuen, R. W., 2003, Auditing a Cisco PIX firewall: An Auditor Perspective, 2003, URL: [http://www.giac.org/practical/GSNA/Rick\\_Yuen\\_GSNA.pdf](http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf), Checklist item 14 (13/05/2003)
- <sup>viii</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 11 (21/05/2003)
- <sup>ix</sup> Spitzner, L., Building your own firewall rulebase, January 26, 2000, URL: <http://www.spitzner.net/rules.html> (16/05/2003)
- <sup>x</sup> Yuen, R. W., 2003, Auditing a Cisco PIX firewall: An Auditor Perspective, 2003, URL: [http://www.giac.org/practical/GSNA/Rick\\_Yuen\\_GSNA.pdf](http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf), Page 13 (13/05/2003)
- <sup>xi</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 5 (21/05/2003)
- <sup>xii</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 9 (21/05/2003)
- <sup>xiii</sup> Internet Assigned Numbers Authority, Internet Multicast Addresses, 09/07/2003, URL: <http://www.iana.org/assignments/multicast-addresses> (10/07/2003)
- <sup>xiv</sup> Yuen, R. W., 2003, Auditing a Cisco PIX firewall: An Auditor Perspective, 2003, URL: [http://www.giac.org/practical/GSNA/Rick\\_Yuen\\_GSNA.pdf](http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf), Checklist item 2 (13/05/2003)
- <sup>xv</sup> Cisco Systems, Installation and Configuration for the Cisco PIX Firewall – EAL4 Certification Version 5.2(3), 23/01/2001 URL: [http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v52/ea14v523.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ea14v523.htm) (28/06/03)
- <sup>xvi</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 23 (21/05/2003)
- <sup>xvii</sup> Yuen, R. W., 2003, Auditing a Cisco PIX firewall: An Auditor Perspective, 2003, URL: [http://www.giac.org/practical/GSNA/Rick\\_Yuen\\_GSNA.pdf](http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf), Checklist item 19 (13/05/2003)
- <sup>xviii</sup> Naidu, K., Firewall Checklist, URL: <http://www.sans.org/score/checklists/FirewallChecklist.doc>, Checklist item 15 (21/05/2003)
- <sup>xx</sup> Internet Assigned Numbers Authority, ICMP TYPE NUMBERS, 27/08/2001, URL: <http://www.iana.org/assignments/icmp-parameters> (10/07/2003)

---

<sup>xx</sup> Yuen, R. W., 2003, Auditing a Cisco PIX firewall: An Auditor Perspective, 2003,  
URL: [http://www.giac.org/practical/GSN\\_A/Rick\\_Yuen\\_GSNA.pdf](http://www.giac.org/practical/GSN_A/Rick_Yuen_GSNA.pdf), Risk 7 (13/05/2003)

<sup>xxi</sup> Northcutt, S., Track 7.2, Auditing the Perimeter, SANS Institute, 2003. page 3 -14

<sup>xxii</sup> Spitzner, L., Building your own firewall rulebase, January 26, 2000,  
URL: <http://www.spitzner.net/rules.html> (16/05/2003)

<sup>xxiii</sup> Cisco Systems, Installation and Configuration for the Cisco PIX Firewall – EAL4 Certification  
Version 5.2(3), 23/01/2001  
URL: [http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v52/ea14v523.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ea14v523.htm) (28/06/03)

<sup>xxiv</sup> Northcutt, S., Track 7.2, Auditing the Permitter, SANS Institute, 2003. page 4 -16

<sup>xxv</sup> Northcutt, S., Track 7.2, Auditing the Permitter, SANS Institute, 2003. page 4 -35

<sup>xxvi</sup> Internet Assigned Numbers Authority, Internet Multicast Addresses, 09/07/2003,  
URL: <http://www.iana.org/assignments/multicast-addresses> (05/07/2003)

<sup>xxvii</sup> Defence Signals Directorate, Australian Communications -Electronic Security Instruction 33 (ACSI  
33) HANDBOOK 3 RISK MANAGEMENT, Version 1.0  
URL: <http://www.dsd.gov.au/infosec/acs33/HB3.html> (14/05/2003)

© SANS Institute 2003, Author retains full rights.