

Configuration

1 System: 192.168.3.11

Collection: **192.168.3.11 (2008-05-14 11:34:33)**

Generated: **Wednesday, May 14, 2008 11:34:49 AM**

For: **Test User test.user@email.com**

By: Ecora Auditor Professional 4.5 - Cisco Firewall Module 4.5.8118.18311

Using: Full Report (Configuration Report)

Description: The Configuration report provides detailed documentation of configuration settings for compliance audits, disaster recovery plans, security assessments, migration plans, troubleshooting, and preserving IT knowledge and decisions.

Full Report

Table of Contents

- 1 System Management 4**
 - 1.1 ASDM 4
 - 1.2 DNS 4
 - 1.3 Names 4
 - 1.4 Protocol Fixups 4
 - 1.5 Logging 4
 - 1.6 DHCP Server 5
 - 1.7 DHCP Relay Agent 5
 - 1.8 HTTP Server 5
 - 1.9 Telnet Server 5
 - 1.10 Secure Shell 6
 - 1.11 SNMP 6
 - 1.12 Failover 6
- 2 Interfaces 7**
 - 2.1 ethernet0 7
 - 2.2 ethernet1 7
 - 2.3 ethernet2 8
 - 2.4 ethernet3 8
 - 2.5 ethernet4 8
 - 2.6 ethernet5 9
- 3 Security Policy 9**

- 3.1 Class Maps 9
- 3.2 Inspect Policy Maps 9
- 3.3 Policy Maps 9
- 3.4 Access Lists 9
- 3.5 Conduits 10
- 3.6 Outbounds 10
- 3.7 Filter Rules 10
- 3.8 ICMP Rules 11
- 4 Intrusion Detection System 11**
- 5 Networks 11**
 - 5.1 NAT 11
 - 5.2 Static NAT 12
 - 5.3 Routes 12
- 6 AAA 12**
 - 6.1 AAA Servers 12
 - 6.2 Authentication 13
 - 6.3 Authorization 13
- 7 Virtual Private Network 13**
 - 7.1 General 13
 - 7.2 Internet Key Exchange 14
 - 7.3 IP Security 14
 - 7.4 Global settings for WebVPN 14
 - 7.5 Remote Access 15
- 8 Device Administration 15**
 - 8.1 Administration 15

Collected Not-Collected Legend

DEFAULT	The value presented in the report was not directly reported by the target, but implied by the current value or lack of a value for the attribute
UA	Unavailable attribute. The current configuration or version of target platform does not provide a value for this attribute. More detail in logs
FC	Collection of value failed
NS	Value not selected for collection

Organization Example Company

This report for **Example Company** has been prepared at the request of from the data set collected on **May-14-2008_11-34-33**.

This data set is composed of 1 firewall.

- 192.168.3.11

192.168.3.11

Hostname: **192.168.3.11**

The host name in the Cisco Firewall command-line prompt is **pixqa**.

IPSec domain name: **ecoraqa.com**

OS: **Cisco Secure PIX Firewall Version: 5.3(1)**

Platform Series: **PIX-515**

RAM: **64 MB RAM**

CPU: **CPU Pentium 200 MHz**

Flash: **i28F640J5 @ 0x300, 16MB**

BIOS flash: **AT29C257 @ 0xfffd8000, 32KB**

Serial number: **0x1cad5075**

Activation key: **0xf4e76075 0x46925d2c 0xe2ffe373 0x09c7b39b**

Uptime: **1 year 328 days**

Table 1. Licensed features

Feature	Value
Failover	Enabled
VPN-DES	Disabled
VPN-3DES	Disabled
Maximum Interfaces	6
Cut-through Proxy	Enabled
Guards	Enabled
Websense	Enabled
Throughput	Unlimited
ISAKMP peers	Unlimited

1 System Management

Cisco firewalls provide for the configuration of some basic system management features.

1.1 ASDM

ASDM history tracking: **disabled**

1.2 DNS

Retries: **DEFAULT: 2**

Timeout(sec): **DEFAULT: 2**

1.3 Names

Usage of the name commands is **allowed**.

aliases: ***NULL***

1.4 Protocol Fixups

Table 2. Protocol fixups

Protocol	Ports	Options
ftp	21	
http	80	
h323	1720	
rsh	514	
smtp	25	
sqlnet	1521	
sip	5060	

1.5 Logging

Logging is **started**.

Syslog facility: **20**

The size of the queue for storing syslog messages is **512**.

The failover standby unit **can't** send syslog messages.

Allow add a time stamp value on each message.

Disabled Messages: ***NULL***

Syslog messages are not sent to an internal buffer.

Syslog messages are not sent to the console.

Syslog messages are not sent by the email.

Permit new user sessions when a TCP-based syslog server is unavailable: **Disabled**

Syslog messages are not stored in the history table.

Syslog messages don't appear on telnet sessions to the Cisco Firewall console.

Syslog messages are not sent to the syslog servers.

syslogServers: ***NULL***

loggingLists: ***NULL***

Syslog messages are not sent to the ASDM log buffer.

1.6 DHCP Server

The DHCP server is **disabled**.

The length of the lease, in seconds, granted to DHCP client from the DHCP server: **DEFAULT: 3600**

1.7 DHCP Relay Agent

Timeout(sec): **60**

1.8 HTTP Server

HTTP server is **disabled**.

clients: ***NULL***

1.9 Telnet Server

Telnet session can be idle **5** minute(s) before being closed by Cisco Firewall.

Table 3. Permitted clients

Client	Interface
192.168.0.0/255.255.255.0	inside
host 192.168.3.11	inside
192.168.3.0/255.255.255.0	inside
192.168.8.0/255.255.255.0	inside

Client	Interface
192.168.28.0/255.255.255.0	inside
192.168.7.0/255.255.255.0	inside

1.10 Secure Shell

Secure Copy (SCP) on the security appliance **enabled**.

Session can be idle 5 minute(s) before being closed by Cisco Firewall.

Table 4. Permitted clients

Client	Interface
host 192.168.3.11	outside
192.168.3.0/255.255.255.0	outside
192.168.0.0/255.255.255.0	inside
host 192.168.3.11	inside
192.168.3.0/255.255.255.0	inside
192.168.28.0/255.255.255.0	inside
192.168.8.0/255.255.255.0	inside
192.168.7.0/255.255.255.0	inside

1.11 SNMP

Community key: **public**

Sending log messages as SNMP trap notifications is **disabled**.

1.12 Failover

Cisco Firewall failover feature is **disabled**.

Current Cisco Firewall is the **passive** unit.

Serial cable failover is used.

Table 5. Failover IP Addresses

Interface	IP Address
outside	0.0.0.0
inside	0.0.0.0
intf2	0.0.0.0
intf3	0.0.0.0

Interface	IP Address
intf4	0.0.0.0
intf5	0.0.0.0

macAddresses: ***NULL***

Stateful replication of HTTP sessions is **disallowed**.

Failover waits **15** second(s) before sending special failover 'hello' packets between the primary and standby units.

2 Interfaces

The section describes the interfaces configured on this firewall.

Permit communications between different interfaces that have the same security level: **disabled**

Permit communications in and out of the same interface: **disabled**

2.1 ethernet0

Interface is **enabled**.

Hardware Address: **0005.328f.ca14**

IRQ: **11**

Network interface speed: **100basetx**

MTU: **1500** bytes.

Interface name: **outside**

Security level: **security0**

IP Address: **10.10.10.5**. Netmask: **255.255.255.255**

2.2 ethernet1

Interface is **enabled**.

Hardware Address: **0005.328f.ca15**

IRQ: **10**

Network interface speed: **100basetx**

MTU: **1500** bytes.

Interface name: **inside**

Security level: **security100**

IP Address: **192.168.3.11**. Netmask: **255.255.255.0**

2.3 ethernet2

Interface is **disabled**.
Hardware Address: **00e0.b601.ef4d**
IRQ: **9**
Network interface speed: **100basetx**
MTU: **1500** bytes.
Interface name: **intf2**
Security level: **security10**
IP Address: **127.0.0.1**. Netmask: **255.255.255.255**

2.4 ethernet3

Interface is **disabled**.
Hardware Address: **00e0.b601.ef4c**
IRQ: **9**
Network interface speed: **100basetx**
MTU: **1500** bytes.
Interface name: **intf3**
Security level: **security15**
IP Address: **127.0.0.1**. Netmask: **255.255.255.255**

2.5 ethernet4

Interface is **disabled**.
Hardware Address: **00e0.b601.ef4b**
IRQ: **9**
Network interface speed: **100basetx**
MTU: **1500** bytes.
Interface name: **intf4**
Security level: **security20**
IP Address: **127.0.0.1**. Netmask: **255.255.255.255**

2.6 ethernet5

Interface is **disabled**.

Hardware Address: **00e0.b601.ef4a**

IRQ: **9**

Network interface speed: **100basetx**

MTU: **1500** bytes.

Interface name: **intf5**

Security level: **security25**

IP Address: **127.0.0.1**. Netmask: **255.255.255.255**

3 Security Policy

The section describes security policies applied on this firewall.

3.1 Class Maps

classMaps: ***NULL***

3.2 Inspect Policy Maps

inspectPolicyMaps: ***NULL***

3.3 Policy Maps

policyMaps: ***NULL***

3.4 Access Lists

The Access Control Lists configured are:

1. **101**
Rules
 - Action: **permit** Protocol: **ip**
Source: **192.168.3.0/255.255.255.0**

Destination: **192.168.168.0/255.255.255.0**
2. **102**
Rules

- Action: **permit** Protocol: **ip**
 Source: **192.168.3.0/255.255.255.0**
 Destination: **192.168.168.0/255.255.255.0**

3.5 Conduits

rules: ***NULL***

3.6 Outbounds

outbounds: ***NULL***

3.7 Filter Rules

axFilters: ***NULL***

javaFilters: ***NULL***

ftpFilters: ***NULL***

httpsFilters: ***NULL***

URL rules:

- Port: **http**
 Local address: **any**
 Foreign address: **any**
 When the server is unavailable, **disallow** outbound connections without filtering.

3.7.1 Filter Servers

Cache entries based on the URL **destination** address.

Table 6. Filter servers

Interface	Vendor	IP-Address	Port	Timeout	Protocol	Pro to Ver sion	TC P Co nn ecti ons Lim it
inside	*NULL*	192.168.0.10		5	TCP	1	

3.8 ICMP Rules

Table 7. ICMP Rules

Action	Message Type	Source	Interface
permit	echo	any	outside
permit	echo	any	inside
permit	DEFAULT: ALL	192.168.0.0/255.255.255.0	inside
permit	DEFAULT: ALL	192.168.3.0/255.255.255.0	inside

4 Intrusion Detection System

Disabled Signatures: ***NULL***

The default actions to be taken for **attack** signatures:

- alarm

The default actions to be taken for **informational** signatures:

- alarm

policies: ***NULL***

Flood guard is **disabled**.

5 Networks

The section describes network address translation and routing configuration.

5.1 NAT

NAT Groups:

- 0
 - NAT Entries:
 - **Policy NAT. ACL: 102**
 - Interface: **inside**
 - TCP ISN randomization protection is **enabled**.
 - Maximum number of simultaneous connections: **unlimited**
 - Maximum number of embryonic connections per host: **unlimited**
- globalAddresses: ***NULL***

5.2 Static NAT

entries: ***NULL***

5.3 Routes

Table 8. Routes

Interface	IP Address	Gateway	Metric, hops
outside	default route	10.10.10.1	1
inside	192.168.0.0/255.255.255.0	192.168.3.7	1
inside	192.168.7.0/255.255.255.0	192.168.3.7	1
inside	192.168.8.0/255.255.255.0	192.168.3.7	1
inside	192.168.28.0/255.255.255.0	192.168.3.7	1

6 AAA

The section describes accounting, authentication and authorization configured on this firewall.

6.1 AAA Servers

Radius accounting port: **DEFAULT: 1645**

Radius authentication port: **DEFAULT: 1646**

AAA server groups:

1. RADIUS. Authentication Protocol: **radius**
servers: ***NULL***
2. TACACS. Authentication Protocol: **tacacs+**
Servers:
 - o IP Address: **192.168.0.10**. Interface: **inside**
The timeout interval for the request: **5**
3. TACACS+. Authentication Protocol: **tacacs+**
servers: ***NULL***

6.2 Authentication

Table 9. Rules

Type	Service	Interface	Local	Foreign	Server Group Tag
Include	http	outside	any	any	TACACS

matches: ***NULL***

consoles: ***NULL***

Table 10. Authentication Prompts

Type	Prompt
prompt	"Hello Pix User"

6.3 Authorization

User authorization services are **disabled**.

7 Virtual Private Network

The section describes virtual private network configured on this firewall.

7.1 General

7.1.1 Client Update

The section describes client-update options.

7.1.2 Tunnel Group

The section describes tunnel groups configured on this firewall. ***NULL***

7.1.3 Group Policy

The section describes group policies configured on this firewall. ***NULL***

7.2 Internet Key Exchange

7.2.1 Internet Security Association Key Management Protocol

ISAKMP negotiation is **disabled**.

NAT traversal is **off**.

The ISAKMP identity: **hostname**

7.2.2 ISAKMP Policies

policies: ***NULL***

7.3 IP Security

7.3.1 Transform Sets

sets: ***NULL***

7.3.2 Crypto Maps

maps: ***NULL***

7.3.3 Dynamic Crypto Maps

maps: ***NULL***

7.4 Global settings for WebVPN

SVC files download: **disabled**

Display of the tunnel-group list on the WebVPN Login page: **disabled**

Default group policy: **DfltGrpPolicy**

7.5 Remote Access

7.5.1 Local IP Pools

Table 11. Local IP pools

Name	IP Address Range	Netmask
vpnpool1	192.168.168.1-192.168.168.254	

7.5.2 VPN Client

groups: ***NULL***

7.5.3 Easy VPN Remote

Easy VPN Remote connection is **disabled**.

Easy VPN management is through **clear network traffic**. ***NULL***

Mode: **network extension**

7.5.4 VP Dial-up Networking

VPDN is enabled on **outside** interface.

Table 12. Local Users

Username	Password	Stored Local
joeb	joeb	No

groups: ***NULL***

8 Device Administration

8.1 Administration

8.1.1 User Accounts

The section describes users in security appliance database configured on this firewall. ***NULL***

8.1.2 NTP

The section describes NTP server configured on this firewall.

8.1.3 SMTP

The section describes SMTP servers configured on this firewall.