Cisco ASA Configuration Guidance

Abstract

The modern network perimeter is more complicated than ever. The number of applications, protocols, and attacks that a firewall is expected to support and protect against is growing every day. As firewalls increase in complexity, network administrators face a challenge of staying up-to-date on the technology to maintain, and configure, a secure perimeter.

This document provides security guidance for network administrator to assist in the initial out-of-the-box configuration of Cisco Adaptive Security Appliance (ASA) 5500 Next Generation Firewalls (software version 9.1). The guidance provided is based on a basic and simplistic security policy for common network architectures; however, the concepts discussed may be applied to complex policies and networks. It is the responsibility of an organization to develop a security policy that meets all of their specific needs. The topics covered are: secure management, interface configuration, auditing and logging, access control and hardening services provided by the Cisco ASA firewall.

Table of Contents

1. Introduction

1.1. About

Cisco offers a firewall solution to protect networks of all sizes with their ASA 5500 Series NG Firewall. The ASA is designed to stop attacks at the perimeter of a network and offers a rich feature set of capabilities to provide security against an array of network attacks.

While this guide is intended to help administrators harden the network appliance itself, as well as offers guidance on basic firewall services, the ASA has many other security features that are out of scope of this document. Those features are useful and should be deployed, given an operational requirement and the appropriate environment:

- Suite-B IPSec VPNs (Site to Site and Remote Access)
- Identity Based Firewall Security
- High Availability
- Web Security
- Protection from botnets
- Virtual Firewall
- Transparent (Layer 2) Firewall

1.2. Topology

The following diagram (Figure 1-1) depicts a common network topology protected by a firewall referred to as the three-pronged firewall and is referenced throughout this document. The topology includes three network segments that each are of a different level of trust: a demilitarized zone (DMZ), external/outside and internal/inside network. The external network is an untrusted, or less trusted, network (e.g. the Internet). The DMZ contains services that are accessible via the internal and external networks such as Email or Web Servers. Note that the DMZ may be omitted if there are no external facing services. Finally, the internal network is the most trusted which would be analogous to an agency/organization's network which all employees have access.

The three-pronged approach is the most common topology used today and is the recommended design when a DMZ is present. The management network, while not shown, should be an out-of-band network.

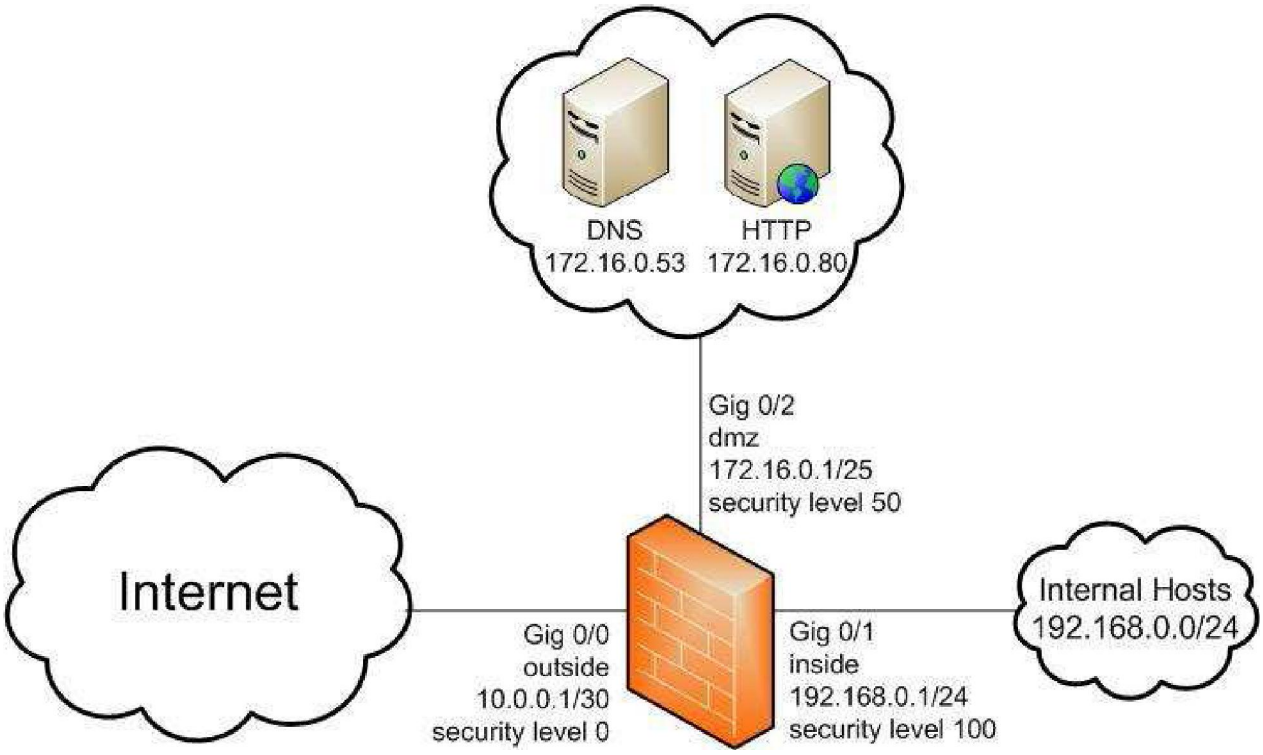

Figure 1-1: Three-Pronged Firewall Topology

2. Management

Properly securing management features/services of any network device is critical to securing not only the host, but also the network in its entirety. Management traffic should be kept out-of-band by configuring a separate management interface connected to the firewall. This interface should be connected to a stand-alone network and unable to route traffic through the firewall. The following sections outline the recommendations for a dedicated management interface as well as other available and important management features.

2.1. Dedicated Management Interface

In order to enforce the out-of-band management requirement, there should be a dedicated management interface that does not pass transit traffic. Cisco offers a management-only feature to enforce this and deny packets attempting to traverse the interface. The security-level should be set to 100 as a precaution to the management-only feature being disabled. Please refer to Section 3.2 for further explanation of security levels.

```
(config)# interface management 0/0
(config-if)# management-only
```

2.2. Passwords

For local user accounts, use the built-in password policy feature to enforce the organization's password policy. For guidance on password management please review National Institute of Standards and Technology (NIST) Special Publication 800-118 Guide to Enterprise Password Management. An example password policy would look something like:

- Users should change passwords every 90 days

```
(config)# password-policy lifetime 90
```

- Changed passwords should be at least 33% (4 out of 12 characters) different from the previous password

```
(config)# password-policy minimum-changes 4
```

- Passwords should be a minimum length of 12 characters

```
(config)# password-policy minimum-length 12
```

- Passwords should contain at least two characters lowercase, uppercase, numeric and special characters

```
(config)# password-policy minimum-lowercase 2
(config)# password-policy minimum-uppercase 2
(config)# password-policy minimum-numeric 2
(config)# password-policy minimum-special 2
```

2.3. Usernames

Individual accounts should be created for each administrator to allow for accountability and auditing. When using an Authentication, Authorized, and Accounting (AAA) server for authentication, a couple of accounts should be created locally on the ASA for administrators as a backup in case the AAA server fails. Also, appropriate privileges should be set on all accounts; an administrator with full access will have privilege level 15, whereas users that only need to view configurations may have privilege level 1. Locally stored VPN user accounts should not be authorized to run any command and should be give privilege level 0.

```
(config)# username JohnDoeAdmin password password123#! privilege 15
(config)# username JaneSmithViewer password p@$sWoRd456 privilege 1
(config)# username JohnDoeVPNUser password paS$789!worD privilege 0
```

2.4. Console

The console port is used for a serial connection to the firewall and is the preferred method for managing the ASA. This typically provides an out-of-band method of management that requires physical proximity to the firewall (unless there is a remote console switch/server). By default there is no authentication required for console access and no time out for idled sessions. Use authentication for console access whether it is the local user database, Remote Service Access Dial in User Server (RADIUS) or Terminal Access Controller Access-Control System (TACACS).

```
(config)# aaa authentication serial console local
```

2.5. Privileged Exec Mode

Privilege exec mode is used to make nearly all of the configuration changes to the firewall and it is recommended to limit access to this mode to administrators only. When a user first logs into the firewall they are placed into user exec mode which has limited privileges; however, by default there is no password required to enter privileged exec mode from user exec mode. A password should be set to prevent unauthorized users from altering the running configuration in privilege exec mode.

```
(config)# aaa authentication enable console local
```

2.6. Secure Shell (SSH)

SSH should be used for secure remote management as an alternative to the insecure telnet protocol. SSH uses RSA keys as part of the key exchange process, which by default are 1024 bits in length. Make sure to generate the largest RSA key possible (2048 bits as of 9.1). Also, set the firewall to accept only SSH version 2 and the Diffie Hellman key-exchange group to group 14.

```
(config)# crypto key generate rsa modulus 2048
(config)# ssh version 2
(config)# ssh key-exchange group dh-group14-sha1
(config)# aaa authentication ssh console LOCAL
```

Hosts that require access to the SSH service should be limited to specific hosts and/or networks. It is recommended to allow host access on a per IP address basis; however, if there are many hosts in a subnet that require SSH access, a network may be used with a limited sized subnet.

```
(config)# ssh 192.168.255.10 255.255.255.255 management
```

2.7. Adaptive Security Device Manager (ASDM)

ASDM is the graphical management application which uses SSL to provide a secure management connection to the ASA. RSA keys should be properly setup prior to enabling the http server on the ASA (See Secure Shell section 2.6 for commands and guidance for generating the proper keys). Hosts and/or networks allowed to access the ASA using ASDM should be limited to a refined set of hosts and/or subnets. ASDM management also has a unique feature to prevent long lived management sessions. It is recommended to set the session timeout to an hour or less.

```
(config)# http server enable
(config)# http 192.168.255.0 255.255.255.0 management
```

ASDM management also has a unique feature to prevent long lived management sessions. It is recommended to set the session timeout to an hour or less.

```
(config)# http server session-timeout 60
```

2.8. Management Session Timeouts

Idle management sessions of any kind should be automatically timed out after a short period of time. This limits the possibility of unauthorized access due to an Administrator forgetting to close a session. This should apply to all management services:

```
(config)# console timeout 9
(config)# ssh timeout 9
(config)# http server idle-timeout 9
```

2.9. System / ASDM Images

When booting, the ASA selects the first system image available in flash memory to load. Similarly, the ASA will hand out the first ASDM image available when requested by an administrator. It is recommended to explicitly define the images that the ASA should use when booting and for ASDM management. Doing so provides clarity in the configuration and prevents confusion during upgrades.

```
(config)# boot system flash:/asa911-4-k8.bin
(config)# asdm image flash:/asdm-712-102.bin
```

2.10. Banners

Login banners should be used on all networking devices as they offer multiple benefits. They are useful for informing possible intruders that access to the device is potentially illegal, and at the same time advises authorized users of their obligations regarding acceptable use of network devices. Use banners for all methods of managing the ASA. If using ASDM as a form of management it should be noted that a second, separate, banner command is required:

```
(config)# banner login You are accessing a U.S. Government (USG) ...
(config)# banner asdm You are accessing a U.S. Government (USG) ...
```

2.11. Simple Network Management Protocol (SNMP)

When using SNMP for management, auditing or logging, SNMP version three should be used with privacy and authentication. SHA should be used as the digest function for authentication, as well as AES 256 encryption should be used for privacy. Specific hosts should be identified in the configuration to allow for polling and/or traps (methods used by SNMP to gather and send information to hosts and servers).

```
(config)# snmp-server group MySNMPServerGroup v3 priv
(config)# snmp-server user JohnDoe MySNMPServerGroup v3 auth SHA
          p@$$W0rD1 priv AES 256 p@$$W0rD2
(config)# snmp-server host management 192.168.255.99 version 3
          JohnDoe
```

2.12. Updates

Keeping your Cisco ASA updated with the latest patches is one of the more important/beneficial security steps an administrator can perform. Determining release and hardware compatibility may be found at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html; Latest release

information can be found at http://www.cisco.com and navigating through the support page, security category and finally to Adaptive Security Appliance (ASA) Software. (Actual download requires a Cisco Connection Online (CCO) account).

Once the latest ASA image has been downloaded, it should be transferred to the firewall in a secure manner. There are several ways to securely copy files to the ASA, all of which require an IP address on an interface and should be transferred via the management interface.

```
(config)# ssh scopy enable
```

Then, from a Secure Copy (SCP) client copy the image to the ASA, e.g.

```
scp asa911-4-k8.bin JohnDoe@192.168.255.1:asa911-4-k8.bin
```

Or, if you have CiscoWorks Auto Update Server (AUS) you can setup automatic updates securely on the ASA.

```
(config)# auto-update server
          https://username:password@192.168.255.103/updates source
          management
```

2.13. Authentication

Accounts may be stored locally or on a remote AAA server, which are an excellent resource for managing many user accounts. If a remote AAA server is used, the local user database should be used as a backup method for authenticating users in the event that the AAA server becomes unreachable. The AAA server should reside in the management out-of-band network and the AAA server defined on the ASA should specify the interface where the designated AAA server is to be accessed.

```
(config)# aaa-server ManagementRadius protocol radius
(config)# aaa-server ManagementRadius (management) host
192.168.255.77
(config-aaa-server-host)# key R3@11yL0nGS3cuR3Key
(config)# aaa authentication ssh console ManagementRadius LOCAL
```

3. Interface Configuration

When setting up an interface you must set the name, security level, and IP address, as well as enable the interface. Provided below are individual recommendations for each of those steps.

3.1. Naming

Cisco requires that you assign a unique name to each interface which is referenced throughout the rest of the configuration. The names should represent the level of trust of the connected network. For example, the outside interface represents untrusted hosts (often the Internet) and could be labeled “outside”, “external” or “untrust”. The inside interface contains the most trusted hosts and is usually named “inside”, “internal” or “trust”. The DMZ should contain servers that may be accessed via the untrusted and/or trusted networks, with a name of “DMZ”, “Servers”, etc.

```
(config)# interface GigabitEthernet 0/0
(config-if)# nameif outside

(config)# interface GigabitEthernet 0/1
(config-if)# nameif inside

(config)# interface GigabitEthernet 0/2
(config-if)# nameif dmz

(config)# interface Management 0/0
(config-if)# nameif management
```

3.2. Security Levels

Each interface will have a security level from 0 (least trusted) to 100 (most trusted) associated with it. Note, Cisco has built in names that automatically set default security level values. Interfaces name “outside” or “inside” will have a security level of 0 or 100 respectively.

The purpose of the security levels is to enforce a standard default policy between interfaces without any extra configuration required from an administrator. Interfaces with a lower security level may not access host behind an interface with a greater than, or equal to, security level. E.g. Hosts from an interface with a security level 100 may send any traffic to any hosts on an interface with a security level of 0 to 99. Similarly, hosts on an interface with the security level 50 may send traffic to hosts on an interface with a security level of 0 to 49.

The security levels are required for the ASA to function and we recommend setting them appropriately. However, we also recommend applying Access Control Lists (ACLs) to all interfaces to override the default security level behavior of the ASA.

```
(config)# interface GigabitEthernet 0/0
(config-if)# security-level 0

(config)# interface GigabitEthernet 0/1
(config-if)# security-level 100

(config)# interface GigabitEthernet 0/2
(config-if)# security-level 50

(config)# interface Management 0/0
(config-if)# security-level 100
```

3.3. IP Addresses

IP Address subnet masks for each interface should be set to an appropriate size, e.g. often firewalls are placed between routers and really only require a /30 subnet.

```
(config)# interface GigabitEthernet 0/0
(config-if)# ip address 10.0.0.1 255.255.255.252

(config)# interface GigabitEthernet 0/1
(config-if)# ip address 192.168.0.1 255.255.255.0

(config)# interface GigabitEthernet 0/2
(config-if)# ip address 172.16.0.1 255.255.255.128

(config)# interface Management 0/0
(config-if)# ip address 192.168.255.1 255.255.255.0
```

3.4. Enabling

By default, all interfaces are administratively shutdown and you must enable each interface. It is recommended to only enable interfaces that are being used.

```
(config)# interface GigabitEthernet 0/0
(config-if)# no shutdown

(config)# interface GigabitEthernet 0/1
(config-if)# no shutdown

(config)# interface GigabitEthernet 0/2
(config-if)# no shutdown

(config)# interface Management 0/0
(config-if)# no shutdown
```

4. Auditing / Logging

Logging and auditing the logs are an integral part of maintaining a secure network. Data should be written both locally and to a central log server for analysis of attacks, network misuse and troubleshooting network issues. To turn on logging:

```
(config)# logging enable
```

4.1. Severity Levels

There are eight logging severity levels ranging from most to least severe: emergency, alert, critical, error, warning, notifications, informational and debugging. Recommended practice is to use at minimum the notification level, and even possibly the information level depending on the amount of messages generated from traffic on the network.

```
(config)# logging console debugging
(config)# logging asdm notifications
```

4.2. Buffer

Logging should be saved to a local buffer on the ASA using an appropriate amount of memory. When the buffer fills up, unsaved messages should be written to flash (space permitting). The example configuration writes the buffered messages to flash when the buffer fills up with 524,288 bytes of unsaved messages, using up to 64 MB in flash and only if there is 8 MB free disk space.

```
(config)# logging buffered notifications
(config)# logging buffer-size 524288
(config)# logging flash-bufferwrap
(config)# logging flash-maximum-allocation 65536
(config)# logging flash-minimum-free 8192
```

4.3. Syslog

Messages should also be sent to a remote device that is centralized, properly secured and preferably on an out-of-band management network. Syslog is a popular and acceptable way to offload logs to a centralized server:

```
(config)# logging host management 192.168.255.100
(config)# logging trap informational
```

4.4. Timestamps

Messages should contain a timestamp allowing an auditor to compare log messages and correlate network events across different hosts and\or log servers.

```
(config)# logging timestamp
```

4.5. Device ID

All messages should contain a unique identifier to easily be distinguished when auditing the central log server.

```
(config)# logging device-id ipaddress management
```

4.6. Local Time

Part of secure logging is keeping accurate time on all hosts. The clock should be set appropriately including using the correct timezone.

```
# clock set 12:00:00 10 May 2013
(config)# configure terminal
(config)# clock timezone EST -5
```

4.7. Network Time Protocol (NTP)

If possible, take advantage of NTP to keep accurate network time across all hosts in the network. NTP should be set to use authentication, via pre-shared keys, allowing all network devices to securely synchronize their time. Make sure to include the NTP server's IP address to the interface where the NTP server resides.

```
(config)# ntp authenticate
(config)# ntp authentication-key 1 md5 someNTPkey
(config)# ntp trusted-key 1
(config)# ntp server 192.168.7.10 key 1 source management
```

5. Service Hardening

5.1. Proxy Address Resolution Protocol (ARP)

Proxy ARP allows the firewall to respond to ARP requests when the interface address space is shared with Network/Port Address Translations (NAT/PAT). If NAT/PAT is not used or NAT/PAT is solely to the firewall's interface addresses, then the service should be disabled. Note, in this example PAT will be used on the outside interface and should be enabled (See Section 5.3).

```
(config)# sysopt noproxyarp management
(config)# sysopt noproxyarp inside
(config)# sysopt noproxyarp dmz

(config)# no sysopt noproxyarp outside
```

5.2. Internet Control Message Protocol (ICMP)

ICMP is used to relay error, control, and informational messages on an IP network. Additionally, ICMP can be used to gather information about a network device. ICMP should be disabled on all interfaces and limited to only administrative hosts that have an operational need on a case by case basis.

```
(config)# icmp deny any dmz
(config)# icmp deny any inside
(config)# icmp deny any outside

(config)# icmp permit host 192.168.255.5 management
(config)# icmp deny any management
```

5.3. Master Passphrase

Encrypts passwords stored in the ASA configuration that are stored in plaintext (e.g. AAA Servers, Logging, Failover, VPN Load Balancing, etc.).

```
(config)# key configs-key password-encryption
(config)# password encryption aes
```

5.4. Secure Socket Layer (SSL) Settings

The default SSL settings are configured to allow weak encryption methods along with older versions of SSL. It is recommended to set the allowed SSL encrypted protocols to AES 128 or AES 256 bit with SHA1 and ideally using Diffie Hellman (Some applications may not support DH and therefore non DH options should be chosen). Also, force the ASA as a client and server to only accept Transport Layer Security (TLS) version 1.

```
(config)# ssl encryption dhe-aes256-sha1 dhe-aes128-sha1
(config)# ssl server-version tlsv1-only
(config)# ssl client-version tlsv1-only
```

For the non DH option:

```
(config)# ssl encryption aes256-sha1 aes128-sha1
```

5.5. Anti Spoofing

Malicious users can spoof network addresses to potentially bypass ACLs on the firewall. To prevent this, use the anti spoofing feature of the ASA which performs a check on the source network address against the route table. Note that this feature requires all networks traversing the firewall have a valid route configured in the route table.

```
(config)# ip verify reverse-path interface dmz
(config)# ip verify reverse-path interface inside
(config)# ip verify reverse-path interface management
```

5.6. IP Fragments

IP fragmentation is a technique used to break up large datagrams into smaller datagrams to pass through a network. Attackers can leverage this to bypass firewall access lists and/or firewall inspection. It is recommended to disable IP fragmentation on all interfaces unless a specific operational need exists in the organization. The following commands prevent packets from being reassembled:

```
(config)# fragment chain 1 outside
(config)# fragment chain 1 inside
(config)# fragment chain 1 dmz
(config)# fragment chain 1 management
```

6. Firewall Protection

6.1. Access Control Lists (ACL)

As described in the interface configuration section, the ASA has a default behavior to permit traffic from hosts deemed at a higher security level to hosts of a lower security level. The exception to this rule is when an ACL is applied to an interface causing all initial transit traffic, for that particular interface, to be checked against the ACL. All interfaces should be configured with both IPv4 and IPv6.

In the example topology IPv6 is not operational and should not be seen by the firewall. The following access lists reflect that policy:

```
(config)# ipv6 access-list OUTSIDE_ACL deny ip any any log
          notifications
(config)# access-group OUTSIDE_ACL in interface outside

(config)# ipv6 access-list DMZ_ACL deny ip any any log alerts
(config)# access-group DMZ_ACL in interface dmz

(config)# ipv6 access-list INSIDE_ACL deny ip any any log warning
(config)# access-group INSIDE_ACL in interface inside
```

It is important to keep access lists as small and simple while maintaining the organization's security policy requirements. Large access lists are difficult to maintain, and to understand, especially for a firewall administrator that did not create the ACL. To help reduce complexity, and add readability to the ACL, use objects with meaningful names to define networks, hosts, services, etc.

```
(config)# object network WEB_SERVER
(configs-network-object)# host 172.16.0.80

(config)# object network DNS_SERVER
(configs-network-object)# host 172.16.0.53

(config)# object network INTERNAL_HOSTS
(configs-network-object)# subnet 192.168.0.0 255.255.255.0
```

Only allow traffic that is required for operational tasks; all other traffic should be denied by inserting the explicit *deny all* keywords. Use the *any* keyword as sparingly as possible (e.g. when referencing all hosts on the Internet). The following ACLs match a simple security policy of:

1. Internet users should be able to access the web server via http

```
(config)# access-list OUTSIDE_ACL extended permit tcp any object
          WEB_SERVER eq http
```

2. Internet users should be able to access the DNS server via DNS requests

```
(config)# access-list OUTSIDE_ACL extended permit tcp any object
          DNS_SERVER eq domain
```

3. Internet users should not have access to any other resources

```
(config)# access-list OUTSIDE_ACL extended deny ip any any log
          notifications

(config)# access-group OUTSIDE_ACL in interface outside
```

The DMZ policy is a much more restrictive policy:

1. DMZ Servers should never be able to initiate connections to internal hosts.

```
(config)# access-list DMZ_ACL extended deny ip any object
          INTERNAL_HOSTS log emergencies
```

2. The DNS Server should be able to perform DNS lookups to other DNS servers on the Internet.

```
(config)# access-list DMZ_ACL extended permit udp object DNS_SERVER
          any eq domain
```

3. DMZ Servers should not be able to communicate with hosts any hosts on the internet (excluding hosts defined in this security policy).

```
(config)# access-list DMZ_ACL extended deny ip any any log error

(config)# access-group DMZ_ACL in interface dmz
```

Internal hosts will typically have the most access to internal and external resources:

1. Internal hosts should have access to both internal and external Web Servers

```
(config)# access-list INSIDE_ACL extended permit tcp object
          INTERNAL_HOSTS any eq http
```

2. Internal hosts should use the organization's DNS server as their primary DNS and never an external DNS Server.

```
(config)# access-list INSIDE_ACL extended permit tcp object
          INTERNAL_HOSTS object DNS_SERVER eq domain
```

3. Internal hosts should not be allowed to pass any other protocols through the firewall.

```
(config)# access-list INSIDE_ACL extended deny ip any any log alert

(config)# access-group INSIDE_ACL in interface inside
```

6.2. IP Audit Policy

Intrusion Prevention Systems (IPS) are used in networks to audit malicious network activity and prevent known, and in some cases unknown, attacks. The IP Audit Policy

feature is a very basic IPS that inspects traffic containing a limited set of signatures that can alert an administrator via an alarm and/or drop packets. This feature is recommended in environments that have no other IPS devices.

```
(config)# ip audit info action alarm drop
(config)# ip audit attack action alarm drop
```

In the event that a particular IP option feature needs to be allowed through the firewall, an exception can be made to the configuration:

```
(config)# ip audit signature 2002 disable
```

6.3. NAT/PAT

The main use of NAT/PAT is to multiplex IP addresses (e.g. one or more public address to many private addresses), helping preserve the IPv4 address space. A side effect of NAT/PAT is confidentiality of an organization's internal network and is recommended for this reason:

```
(config)# network object MyDynamicPATObject
(config-network-object)# subnet 192.168.0.0 255.255.255.0
(config-network-object)# nat(inside,outside) dynamic 10.0.0.1
```

(Note: Instead of providing an IP address, you may specify to use the interface or a range of IP addresses via a network object.)

Static PAT should be used for services that are hosted inside your DMZ and only forwarding the necessary ports to each server.

```
(config)# network object MyStaticPATObject
(config-network-object)# host 172.16.0.80
(config-network-object)# nat(inside,outside) static 10.0.0.80 service
                         tcp 80 80
(config)# access-list OUTSIDE_ACL extended permit tcp any host
          10.0.0.80 eq 80
(config)# access-group OUTSIDE_ACL in interface outside
```

7. Bibliography

(U) Internet Site, "Cisco ASA Series Command Reference," cisco.com, Cisco Systems, Inc., 18 March 2013, http://www.cisco.com/en/US/docs/security/asa/command-reference/cmdref.html, viewed 12 May 2013,

(U) Internet Site, "Release Notes for the Cisco ASA Series, 9.1(x)," cisco.com, Cisco Systems, Inc., 14 March 2013, http://www.cisco.com/en/US/docs/security/asa/asa91/release/notes/asarn91.html, viewed 16 May 2013.

(U) Internet Site, “Guide to Enterprise Password Management (Draft),” Karen Scarfon and Murugiah Souppaya, National Institute of Standards and Technology, April 2009, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf, viewed 17 September 2013.

(U) Internet Site, "Cisco ASA Compatibility," cisco.com, Cisco Systems, Inc., 18 September 2013, http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html, viewed 18 September 2013.

8. Appendices

8.1. APPENDIX A - ACRONYMNS

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
AUS	Auto Update Server
CCO	Cisco Connection Online
DMZ	Demilitarized Zone
DH	Diffie-Hellman
EST	Eastern Standard Time
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
MB	Megabyte
NAT	Network Address Translation
NTP	Network Time Protocol
PAT	Port Address Translation
RSA	Rivest, Shamir and Adelman
SHA	Secure Hashing Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network