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.

Preview from Notesale.co.uk
Page 2 of 22

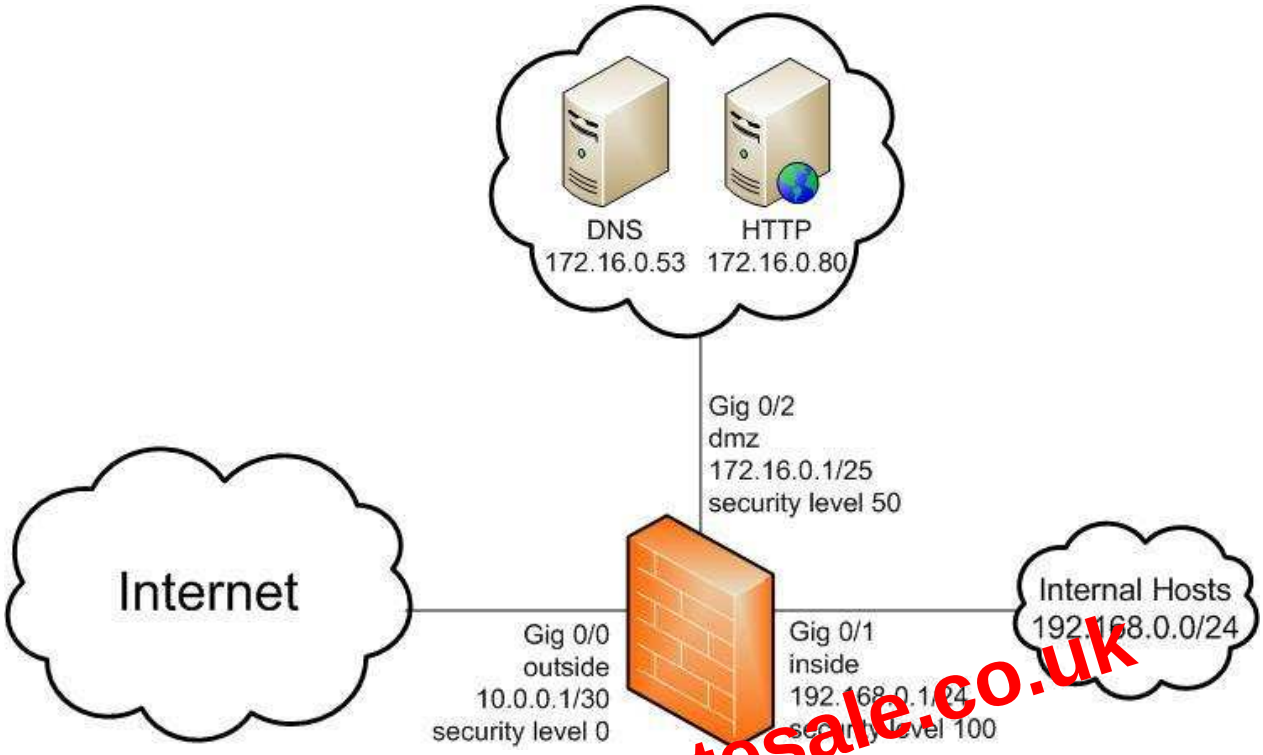

Figure 1.1: Three-Pronged Firewall Topology

Preview from Notesale.co.uk
Page 6 of 22

```
(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
```

Preview from Notesale.co.uk
Page 8 of 22

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
```