IP COMMUNICATIONS

Securing Cisco IP Telephony Networks

The real-world guide to securing Cisco-based IP telephony applications, devices, and networks

ciscopress.com

Akhil Behl, CCIE® No. 19564

Securing Cisco IP Telephony Networks

Akhil Behl

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

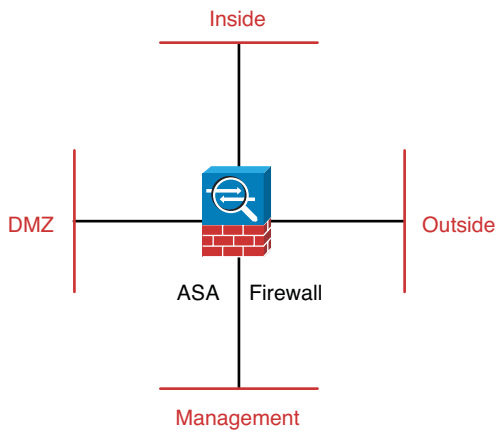

Figure 8-2 *Cisco ASA Physical/Logical Interfaces and Zones*

Although any interface can be configured as Inside, Outside, or DMZ, the usual practice is to configure the following:

- Interface 0 (Fast Ethernet or Gigabit) as outside
- Interface 1 (Fast Ethernet or Gigabit) as inside
- Any other (or consecutive) interface as DMZ

Note This assumes that your Cisco ASA model does not have any interfaces labeled as inside, outside, and so on. If so, it is best to configure the labeled interfaces as inside, outside, and so on, respectively.

This helps identify the interfaces physically on the appliance and to follow a logical sequence for interfaces.

Let's understand what each of these interfaces means to your IP Telephony network.

Inside Interface: Where the entities intended to be secured are placed; this interface is your friend. It helps protect the lifeline for your IP Telephony network, the call control servers, voice messaging servers, presence servers, transcoding, conferencing resources, and so on.

Outside Interface: Where all the crooks and rogue devices are supposed to be located. In other words, it is where your foes thrive, on the Internet and on the outside of your network domain. This interface is meant to liaise with the outside world, whether it is your ISP, a partner, or anyone on the Internet.

Demilitarized Zone (DMZ): Used to host servers that are required by users on the Internet. Because Internet servers are often the devices that hackers attack, even if they manage to compromise a host on the DMZ, they still must face the security appliance to get to the inside devices.

Management Interface: Provides an out-of-box management capability to the Cisco ASA administrator. Although a common practice by Cisco ASA administrators is to use the inside interface as the management interface, the management interface, however, is the recommended choice for managing the security appliance. The reason is that this interface does not route. This interface accepts traffic intended for only Cisco ASA and not the traffic destined for other networks.

Note This interface can support routing protocols so that it can be set as a peer with other routers in the network.

Cisco ASA Firewall: Security Levels

Each physical or logical interface must be assigned a security level that dictates the level of trust that an interface is embraced with. Security levels can be defined within a range of 0–100 with 0 being least secure and 100 being most secure, as depicted in Figure 8-3.

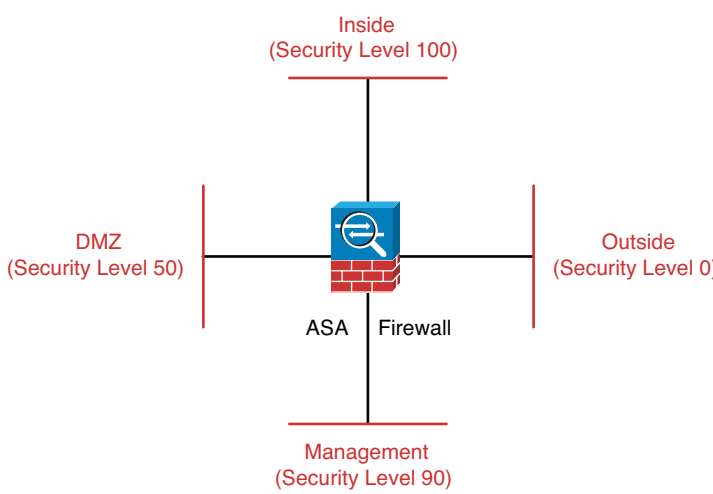

Figure 8-3 *Cisco ASA Physical/Logical Zones and Security Levels*

As you can observe, the inside interface is given a security level of 100 because this is the most secure interface where the core components of your IP Telephony network resides. On the other hand, the outside interface is assigned security level 0 because it faces the most untrusted network, the Internet, and the users of IP Telephony services

(where a potential attacker could be resident). DMZ is assigned level 50 because it is semi-trusted and lies between the bounds of the inside and outside. The management interface is assigned a security level of 90 because it is supposed to be a secure interface, assigned to management VLAN where only trusted machines can connect for managing Cisco ASA.

Example 8-1 explains how these interfaces can be configured (see Figure 8-3).

Example 8-1 *Cisco ASA Interface Configuration*

```
IPTASA(config)# interface fastethernet 0
IPTASA(config-if)# description Outside Interface for Internet
IPTASA(config-if)# nameif outside
IPTASA(config-if)# security-level 0
IPTASA(config-if)# ip address 1.1.1.1 255.255.255.0
IPTASA(config-if)# no shutdown
!
IPTASA(config-if)# interface fastethernet 1
IPTASA(config-if)# description Inside Interface for IP Telephony servers
IPTASA(config-if)# nameif inside
IPTASA(config-if)# security-level 100
IPTASA(config-if)# ip address 10.1.1.1 255.255.255.0
IPTASA(config-if)# no shutdown
!
IPTASA(config-if)# interface fastethernet 2
IPTASA(config-if)# description DMZ Interface for application servers
IPTASA(config-if)# nameif DMZ
IPTASA(config-if)# security-level 50
IPTASA(config-if)# ip address 172.16.1.1 255.255.255.0
IPTASA(config-if)# no shutdown
!
IPTASA(config-if)# interface management 0/0
IPTASA(config-if)# description Management Interface
IPTASA(config-if)# nameif management
IPTASA(config-if)# security-level 90
IPTASA(config-if)# ip address 192.168.1.1 255.255.255.0
IPTASA(config-if)# no shutdown
```

By default, interfaces on the same security level cannot communicate with each other since allowing communication between the same security interfaces would let traffic flow freely between all the same security interfaces without any access control (ACL). This, however, can be enabled by the **same-security-traffic permit inter-interface** command.

Cisco ASA: Firewall Modes

Cisco ASA can work in the following modes:

- Routed
- Transparent
- Multi context

In routed mode (Layer 3 firewall), Cisco ASA is considered to be a hop in the network. Routed mode supports many interfaces, and each interface should be on a different subnet. Cisco ASA, on the other hand, can also work in transparent mode. In this mode, it is a Layer 2 firewall that acts like a bump in the wire and is not seen as a hop to connected devices.

While depending on a network or an organization's requirement, Cisco ASA can be configured in transparent or routed mode; for an IP Telephony network to leverage Cisco ASA as an ALG Firewall, it should be configured in routed mode. As a transparent (mode) firewall, Cisco ASA has following limitations:

- When the firewall is set to transparent mode, you are limited to the use of two traffic forwarding interfaces.
- Sharing of contexts, when in multiple context mode, is not possible in transparent mode.
- A transparent firewall does not support QoS or Network Address Translation (NAT). Former is a pre-requisite for acceptable voice quality across network links.
- A transparent firewall does not offer multicast routing support.
- A transparent firewall supports site-to-site VPN configuration, however only for its own management traffic. This proves to be limiting factor for telecommuters or remote workers.

Note A transparent firewall can save you from changing your IP addressing scheme or readdressing the IP network, for example, for inside/outside subnets. For large enterprise networks, Cisco ASA as an internal firewall can be used in routed or transparent mode; however, at the perimeter, Cisco ASA is best used in routed mode for reasons mentioned earlier.

Cisco ASA supports firewall Multiple Context, also known as Firewall Multimode. Multiple Context mode can be viewed as having multiple separate virtual firewalls on the same physical hardware. Each context is its own security entity with its own security policy specifics and interfaces. Following firewall features are not supported in multiple context mode, such as

- VPN services (remote access or site-to-site VPN tunnels)
- Phone-Proxy

- Dynamic routing
- QoS
- Multicast routing
- Threat detection

For Cisco IP Telephony deployments, Cisco ASA should be configured in single (default) context, and multiple context mode should be avoided for the aforementioned reasons.

Cisco ASA: Network Address Translation

Cisco ASA can provide Network Address Translation (NAT) services, that is, it can change the IP address or port number or both for traffic going out of network (from a higher security interface to a lower security interface) and for traffic coming into your IP Telephony network (a lower security interface to a higher security interface). You can turn off NAT control, allowing packets to traverse Cisco ASA unaltered. This is particularly useful if you do not want to manipulate inside IPs to an outside address range (highly recommended for VoIP because RTP does not play well with NAT) or use RFC 1918 (private) addresses on internal servers, instead use the globally routable (public) network addresses on the IP Telephony and other servers (which is not a recommended practice). NAT control is disabled by default on Cisco ASA. Therefore, when you configure an out-of-the-box Cisco ASA, there's no NAT enabled on the security appliance.

Note For Cisco IP Telephony applications, servers, and network devices, use of RFC 1918 addresses is highly recommended and use of publicly routable addresses is discouraged.

Cisco ASA: UTM Appliance

As previously mentioned, Cisco ASA Firewall is a UTM bundle and can optionally provide IPS, content security, and VPN services. Some of these services (for example, IPS signatures and VPN) are indigenous to Cisco ASA, other services such as content security (antivirus engine, antispyware engine, proxy, and so on) are optional and can be enabled using an AIP-SSC module. Also, an AIP-SSM module gives Cisco ASA the capability for enhanced IPS functionality (hardware acceleration). These services are not essential for IP Telephony Security and are optional (depends on a network architecture and traffic analysis and filtering requirements). For details on Cisco ASA advance inspection features and intrusion prevention/detection for voice signaling and media traffic, see Appendix B, "Cisco IP Telephony: Firewalling and Intrusion Prevention."

Cisco ASA: IP Telephony Firewall

Cisco ASA provides comprehensive access control, threat protection, network policies, service protection, and voice/video confidentiality for real-time IP Telephony traffic.

Voice (and related) protocols supported by Cisco ASA are listed as following:

- SIP
- SCCP (Skinny)
- H.323 v1 - 4
- GTP (3G mobile wireless)
- MGCP
- TRP/RTCP/RTSP
- TAPI/JTAPI
- HTTP
- TFTP
- DNS
- TCP
- UDP
- LDAP

Cisco IP Telephony applications and third-party applications supported by Cisco ASA follow:

- Cisco Unified Communications Manager
- Cisco Unity/Unity Connection
- Cisco Unified Presence Server
- Cisco Unified IP Phones
- Cisco Unified Personal Communicator
- Cisco IP Communicator
- Cisco Unified Meeting Place
- Cisco Unified Contact Center Enterprise and Express
- Microsoft Windows Messenger, NetMeeting
- Real Player

Again, this is not an exhaustive list of applications supported by Cisco ASA. Figure 8-4 shows the various IP Telephony Security services that a Cisco ASA Firewall can deliver.