ASA 8.3: Establish and Troubleshoot Connectivity Through the Cisco Security Appliance

Contents

Introduction

When a Cisco Adaptive Security Appliance (ASA) is initially configured, it has a default security policy where everyone on the inside can get out, and nobody from the outside can get in. If your site requires a different security policy, you can allow outside users to connect to your web server through the ASA.

Once you establish basic connectivity through the Cisco ASA, you can make configuration changes to the firewall. Make sure any configuration changes you make to the ASA are in compliance with your site security policy.

Refer to PIX/ASA: Establish and Troubleshoot Connectivity through the Cisco Security Appliance for the identical configuration on Cisco ASA with versions 8.2 and earlier.

Prerequisites

Requirements

This document assumes that some basic configurations have already been completed on the Cisco ASA. Refer to these documents for examples of an initial ASA configuration:

- ASA 8.3(x): Connect a Single Internal Network to the Internet
- Configuring the PPPoE Client on a Cisco Adaptive Security Appliance (ASA)

Components Used

The information in this document is based on a Cisco Adaptive Security Appliance (ASA) that runs version 8.3 and later.

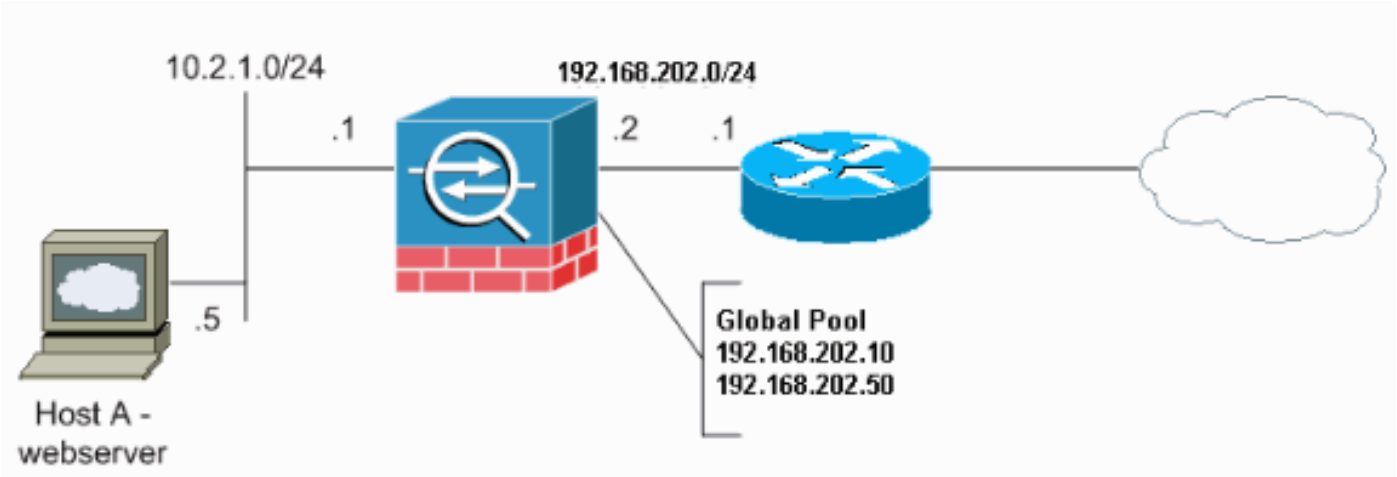
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

How Connectivity Through the ASA Works

In this network, Host A is the web server with an internal address of 10.2.1.5. The web server is assigned an external (translated) address of 192.168.202.5. Internet users must point to 192.168.202.5 in order to access the web server. The DNS entry for your web server needs to be that address. No other connections are allowed from the Internet.



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Configure Connectivity Through the Cisco ASA

Complete these steps in order to configure connectivity through the ASA:

1. Create a network object that defines the internal subnet and another network object for the IP pool range. Configure the NAT using these network objects:
   ```
   object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 192.168.202.10 192.168.202.50 nat (inside,outside) source dynamic inside-net outside-pat-pool
   ```
2. Assign a static translated address for the internal host to which Internet users have access.
   ```
   object network obj-10.2.1.5 host 10.2.1.5 nat (inside,outside) static 192.168.202.5
   ```

3. Use the **access-list** command to allow outside users through the Cisco ASA. Always use the translated address in the **access-list** command.
   ```
   access-list 101 permit tcp any host 192.168.202.5 eq www access-group 101 in interface outside
   ```

Allow ARP Broadcast Traffic

The security appliance connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall to an existing network. IP re-addressing is not necessary. IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. Address Resolution Protocols (ARPs) are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. For Layer 3 traffic that travels from a low to a high security interface, an extended access list is required.

Note: The transparent mode security appliance does not pass Cisco Discovery Protocol (CDP) packets or IPv6 packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for bridge protocol data units (BPDUs), which are supported.

Allowed MAC Addresses

These destination MAC addresses are allowed through the transparent firewall. MAC addresses not on this list are dropped:

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD
- Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

Traffic Not Allowed to Pass in Router Mode

In router mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).

For example, you can establish routing protocol adjacencies through a transparent firewall. You can allow Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol (BGP) traffic through based on an extended access list. Similarly, protocols such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) can pass through the security appliance.

Non-IP traffic (for example, AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType access list.

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended access list, you can allow Dynamic Host Configuration Protocol (DHCP) traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV.

Troubleshoot Connectivity Problems

If Internet users cannot access your website, complete these steps:

1. Make sure you have entered configuration addresses correctly:Valid external addressCorrect internal addressExternal DNS has translated address
2. Check the outside interface for errors.Cisco Security Appliance is preconfigured to auto-detect the speed and duplex settings on an interface. However, several situations exist that can cause the auto-negotiation process to fail. This results in either speed or duplex mismatches (and performance issues). For mission-critical network infrastructure, Cisco manually hardcodes the speed and duplex on each interface so there is no chance for error. These devices generally do not move around. Therefore, if you configure them properly, you should not need to change them.**Example:**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex full asa(config-if)#speed 100 asa(config-if)#exit` In some situations, hardcoding the speed and duplex settings leads to the generation of errors. Therefore, you need to configure the interface to the default setting of auto-detect mode as this example shows:**Example:**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex auto asa(config-if)#speed auto asa(config-if)#exit`
3. If the traffic does not send or receive through the interface of the ASA or the headend router, try to clear the ARP statistics.`asa#clear arp`
4. Use the **show run object** and **show run static** commands in order to make sure that static translation is enabled.**Example:**
   `object service www service tcp source eq www object network 192.168.202.2 host 192.168.202.2 object network 10.2.1.5 host 10.2.1.5 object service 1025 service tcp source eq 1025 nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www`In this scenario, the outside IP address is used as the mapped IP address for the web server.
   `nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www`
5. Check to see that the default route on the web server points to the inside interface of the ASA.
6. Check the translation table using the **show xlate** command in order to see if the translation was created.
7. Use the **logging buffered** command in order to check the log files to see if denies occur. (Look for the translated address and see if you see any denies.)
8. Use the **capture** command:
   `access-list webtraffic permit tcp any host 192.168.202.5 capture capture1 access-list webtraffic interface outside` **Note:** This command generates a significant amount of output. It can cause a router to hang or reload under heavy traffic loads.
9. If packets make it to the ASA, make sure your route to the web server from the ASA is correct. (Check the **route** commands in your ASA configuration.)
10. Check to see if proxy ARP is disabled. Issue the **show running-config sysopt** command in ASA 8.3.Here, proxy ARP is disabled by the **sysopt noproxyarp outside** command:`ciscoasa#show running-config sysopt no sysopt connection timewait sysopt connection tcpmss 1380 sysopt connection tcpmss minimum 0 no sysopt nodnsalias inbound no sysopt nodnsalias outbound no sysopt radius ignore-secret sysopt noproxyarp outside sysopt connection permit-vpn`In order to re-enable proxy ARP, enter this command in global configuration mode:`ciscoasa(config)#no sysopt noproxyarp outside` When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request and asks "Who is this IP address?". The device that

owns the IP address replies, "I own that IP address; here is my MAC address."Proxy ARP allows the security appliance to reply to an ARP request on behalf of hosts behind it. It does this by replying to ARP requests for the static mapped addresses of those hosts. The security appliance responds to the request with its own MAC address, then forwards the IP packets to the appropriate inside host.For example, in the diagram in this document, when an ARP request is made for the global IP address of the web server, 192.168.202.5, the security appliance responds with its own MAC address. If proxy ARP is not enabled in this situation, hosts on the outside network of the security appliance cannot reach the web server by issuing an ARP request for the address 192.168.202.5. Refer to the command reference for more information about the **sysopt** command.

11. If everything appears to be correct, and users still cannot access the web server, open a case with Cisco Technical Support.

Error Message - %ASA-4-407001:

A few hosts cannot connect to the Internet and the `Error Message - %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded` error message is received in the syslog. How is this error resolved?

This error message is received when the number of users exceeds the user limit of the license used. In order to resolve this error, upgrade the license to a higher number of users. This can be 50, 100, or unlimited user license as required.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Security Product Field Notices (including Cisco Adaptive Security Appliance (ASA))**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**