ASA 8.3 and Later: Mail (SMTP) Server Access on the DMZ Configuration Example

Contents

Introduction

This sample configuration demonstrates how to set up the ASA Security Appliance for access to a Simple Mail Transfer Protocol (SMTP) server located on the Demilitarized Zone (DMZ) network.

Refer to ASA 8.3 and Later: Mail (SMTP) Server Access on Inside Network Configuration Example for more information on how to set up the ASA Security Appliance for access to a mail/SMTP server located on the Inside network.

Refer to ASA 8.3 and Later: Mail (SMTP) Server Access on Outside Network Configuration Example for more information on how to set up the ASA Security Appliance for access to a mail/SMTP server located on the Outside network.

Refer to PIX/ASA 7.x and above: Mail (SMTP) Server Access on the DMZ Configuration Example for identical configuration on Cisco Adaptive Security Appliance (ASA) with versions 8.2 and earlier.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance (ASA) that runs version 8.3 and later.
- Cisco 1841 Router with Cisco IOS® Software Release 12.4(20)T

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.

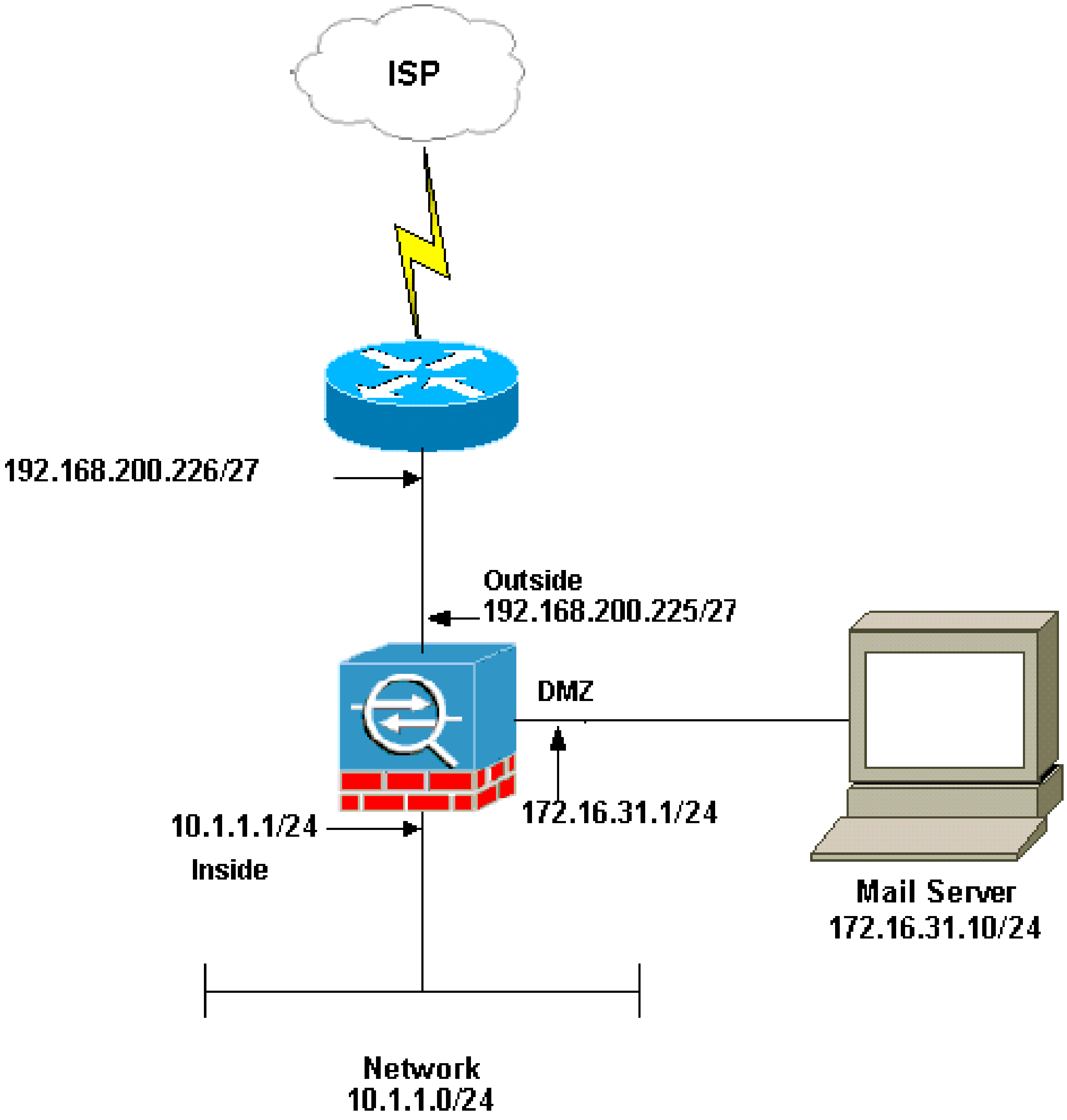
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



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

The network setup used in this example has the ASA with inside network (10.1.1.0/24) and the outside network (192.168.200.0/27). The mail server with IP address 172.16.31.10 is located in the Demilitarized Zone (DMZ) network. For the Mailserver to be accessed by the inside, users configure the identity NAT. Configure an access list, which is **dmz_int** in this example, in order to allow the outgoing SMTP connections from the Mailserver to the hosts in the inside network and bind it to the DMZ interface.

Similarly for the outside users to access the Mailserver configure a static NAT and also an access list, which is **outside_int** in this example, in order to permit outside users to access the Mailserver and bind this access list to the outside interface.

ASA Configuration

This document uses this configuration:

ASA Configuration

```
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0
shutdown no nameif security-level 0 no ip address !
interface Ethernet1 shutdown no nameif no security-level
no ip address ! interface Ethernet2 no nameif no
security-level no ip address ! !--- Configure the inside
interface. interface Ethernet3 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! !---
Configure the outside interface. interface Ethernet4
nameif outside security-level 0 ip address
192.168.200.225 255.255.255.224 ! !--- Configure dmz
interface. interface Ethernet5 nameif dmz security-level
10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host 192.168.200.227 eq smtp !--- Allows outgoing
SMTP connections. !--- This access list allows host IP
172.16.31.10 !--- sourcing the SMTP port to access any
host. access-list dmz_int extended permit tcp host
172.16.31.10 eq smtp any pager lines 24 mtu BB 1500 mtu
inside 1500 mtu outside 1500 mtu dmz 1500 no failover no
asdm history enable arp timeout 14400 object network
obj-192.168.200.228-192.168.200.253 range
192.168.200.228-192.168.200.253 object network obj-
192.168.200.254 host 192.168.200.254 object-group
network nat-pat-group network-object object obj-
192.168.200.228-192.168.200.253 network-object object
obj-192.168.200.254 object network obj-10.1.1.0 subnet
10.1.1.0 255.255.255.0 nat (inside,outside) dynamic nat-
pat-group !--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0 subnet
10.1.1.0 255.255.255.0 nat (inside,dmz) static obj-
10.1.1.0 !--- This network static uses address
translation. !--- Hosts that access the mail server from
the outside !--- use the 192.168.200.227 address. object
network obj-172.16.31.10 host 172.16.31.10 nat
(dmz,outside) static 192.168.200.227 access-group
outside_int in interface outside access-group dmz_int in
interface dmz route outside 0.0.0.0 0.0.0.0
192.168.200.226 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 timeout uauth 0:05:00 absolute no snmp-server
location no snmp-server contact telnet timeout 5 ssh
timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.
service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda : end
```

```
[OK]
```

ESMTP TLS Configuration

Note: If you use Transport Layer Security (TLS) encryption for e-mail communication then the ESMTP inspection feature (enabled by default) in the ASA drops the packets. In order to allow the e-mails with TLS enabled, disable the ESMTP inspection feature as this output shows. Refer to Cisco bug ID CSCtn08326 (registered customers only) for more information.

```
ciscoasa(config)#policy-map global_policy ciscoasa(config-pmap)#class
inspection_default ciscoasa(config-pmap-c)#no inspect esmtp ciscoasa(config-pmap-
c)#exit ciscoasa(config-pmap)#exit
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **debug icmp trace** —Shows whether Internet Control Message Protocol (ICMP) requests from the hosts reach the ASA. You need to add the **access-list** command in order to permit ICMP in your configuration in order to run this debug.**Note:** In order to use this debug, make sure you allow ICMP in the `access-list outside_int` as this output shows:
  ```
  access-list outside_int
  extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- **logging buffered 7** —Used in global configuration mode to enable the adaptive security appliance to send syslog messages to the log buffer. The contents of the ASA log buffer can be seen with the **show logging** command.

Refer to Configure Syslog using ASDM for more information on how to set up logging.

Related Information

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