ASA 8.3 and Later: Mail (SMTP) Server Access on Outside Network Configuration Example

Contents

Introduction

This sample configuration provides information on how to set up the Adaptive Security Appliance (ASA) for access to a mail server located on the outside network.

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

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

Refer to PIX/ASA 7.x and later : Mail (SMTP) Server Access on Outside Network Configuration Example for the 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 Cisco CLI Analyzer 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 (192.168.1.0/30) and the outside network (209.64.3.0/30). The mail server with IP address 209.64.3.6 is located in the outside network. Configure NAT statement so that any traffic from the 192.168.2.x network that passes from the inside interface (Ethernet0) to the outside interface (Ethernet 1) translates to an address in the range of 209.64.3.129 through 209.64.3.253. The last available address (209.64.3.254) is reserved for Port Address Translation (PAT) .

Configurations

This document uses these configurations:

- ASA
- Router A
- Router B

ASA

```
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
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!

!--- Configure the inside interface. ? interface
Ethernet3 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!

!--- Configure the outside interface. interface
Ethernet4 nameif outside
 security-level 0
 ip address 209.64.3.1 255.255.255.252
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa831-k8.bin
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- This command states that any traffic !--- from the
192.168.2.x network that passes from the inside
interface (Ethernet0) !--- to the outside interface
(Ethernet 1) translates into an address !--- in the
range of 209.64.3.129 through 209.64.3.253 and contains
a subnet !--- mask of 255.255.255.128.   object network
obj-209.64.3.129_209.64.3.253
   range 209.64.3.129-209.64.3.253


!--- This command reserves the last available address
(209.64.3.254) for !--- for Port Address Translation
(PAT). In the previous statement, !--- each address
inside that requests a connection uses one !--- of the
```

```
addresses specified. If all of these addresses are in
use, !--- this statement provides a failsafe to allow
additional inside stations !--- to establish
connections. object network obj-209.64.3.254
   host 209.64.3.254

!--- This command indicates that all addresses in the
192.168.2.x range !--- that pass from the inside
(Ethernet0) to a corresponding global !--- designation
are done with NAT. !--- As outbound traffic is permitted
by default on the ASA, no !--- static commands are
needed. object-group network nat-pat-group
   network-object object obj-209.64.3.129_209.64.3.253
   network-object object obj-209.64.3.254

 object network obj-192.168.2.0
   subnet 192.168.2.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- Creates a static route for the 192.168.2.x network
with 192.168.1.2. !--- The ASA forwards packets with
these addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1

!--- Sets the default route for the ASA Firewall at
209.64.3.2. route outside 0.0.0.0 0.0.0.0 209.64.3.2 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
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!

!--- SMTP/ESMTP is inspected since "inspect esmtp" is
included in the map. policy-map global_policy class
inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:8a63de5ae2643c541a397c2de7901041
: end
```

Router A

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1
  !
  !
  line con 0
   transport input none
   line aux 0
   autoselect during-login
   line vty 0 4
   exec-timeout 5 0
   password ww
   login
  !
  end
```

Router B

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  interface Ethernet0
```

```
!--- Assigns an IP address to the ASA-facing Ethernet
interface. ip address 209.64.3.2 255.255.255.252 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the server-facing Ethernet interface. ip
address 209.64.3.5 255.255.255.252 no ip directed-
broadcast ! interface Serial0 !--- Assigns an IP address
to the Internet-facing interface. ip address 209.64.3.9
255.255.255.252 no ip directed-broadcast no ip mroute-
cache ! interface Serial1 no ip address no ip directed-
broadcast ! ip classless !--- All non-local packets are
to be sent out serial 0. In this case, !--- the IP
address on the other end of the serial interface is not
known, !--- or you can specify it here. ip route 0.0.0.0
0.0.0.0 serial 0
  !

!--- This statement is required to direct traffic
destined to the !--- 209.64.3.128 network (the ASA
global pool) to the ASA to be translated !--- back to
the inside addresses. ip route 209.64.3.128
255.255.255.128 209.64.3.1
  !
  !
  line con 0
   transport input none
  line aux 0
   autoselect during-login
  line vty 0 4
   exec-timeout 5 0
   password ww
   login
  !
  end
```

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 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

The Cisco CLI Analyzer supports certain **show** commands. Use the CLI Analyzer to view an analysis of **show** command output.

The **logging buffered 7** command directs messages to the ASA console. If connectivity to the mail server is a problem, examine the console debug messages to locate the IP addresses of the sending and receiving stations in order to determine the problem.

Related Information

- **Cisco ASA 5500-X Series Firewalls**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**