Configure the ASA for SMTP Mail Server Access in DMZ, Inside, and Outside Networks

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Mail Server in the DMZ Network
  - Network Diagram
  - ASA Configuration
  - ESMTP TLS Configuration
- Mail Server in the InsideNetwork
  - Network Diagram
  - ASA Configuration
- Mail Server in the Outside Network
  - Network Diagram
  - ASA Configuration

Verify

- Mail Server in the DMZ Network
  - TCP Ping
  - Connection
  - Logging
  - NAT Translations (Xlate)
- Mail Server in the InsideNetwork
  - TCP Ping
  - Connection
  - Logging
  - NAT Translations (Xlate)
- Mail Server in the Outside Network
  - TCP Ping
  - Connection
  - Logging
  - NAT Translations (Xlate)

Troubleshoot

- Mail Server in the DMZ Network
  - Packet-Tracer
  - Packet Capture
- Mail Server in the InsideNetwork
  - Packet-Tracer
- Mail Server in the Outside Network
  - Packet-Tracer

Related Information

Introduction

This document describes how to configure a Cisco Adaptive Security Appliance (ASA) for access to a Simple Mail Transfer Protocol (SMTP) server that is located in the Demilitarized Zone (DMZ), the inside network, or the outside network.

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 ASA that runs software Version 9.1 or later
- Cisco 2800C Series Router with Cisco IOS® Software Release 15.1(4)M6

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, ensure that you understand the potential impact of any command.

Conventions

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

Configure

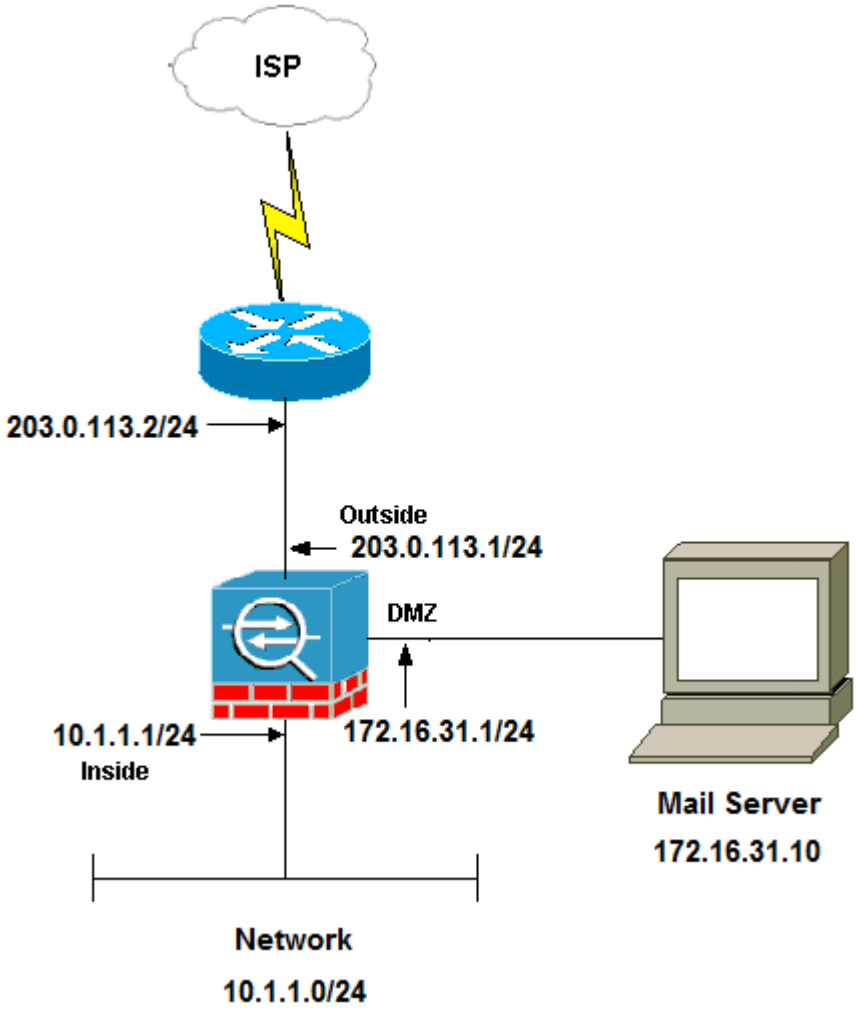
This section describes how to configure the ASA in order to reach the mail server in the DMZ network, the inside network, or the outside network.

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

Mail Server in the DMZ Network

Network Diagram

The configuration that is described in this section uses this network setup:



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

The network setup that is used in this example has the ASA with an inside network at **10.1.1.0/24** and an outside network at **203.0.113.0/24**. The mail server with IP address **172.16.31.10** is located in the DMZ network. In order for the mail server to be accessed by the inside network, you must configure the identity Network Address Translation (NAT).

In order for the outside users to access the mail server, you must configure a static NAT and an access list, which is **outside_int** in this example, in order to permit the outside users to access the mail server and bind the access list to the outside interface.

ASA Configuration

This is the ASA configuration for this example:

```
<#root>

show run


: Saved
:
```

```
ASA Version 9.1(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names


!--- Configure the dmz interface.


interface GigabitEthernet0/0
 nameif dmz
 security-level 50
 ip address 172.16.31.1 255.255.255.0
!

!--- Configure the outside interface.




interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0


!--- Configure inside interface.


interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa912-k8.bin
ftp mode passive


!--- This access list allows hosts to access
!--- IP address 172.16.31.10 for the SMTP port from outside.



access-list outside_int extended permit tcp any4 host 172.16.31.10 eq smtp
```

```
object network obj1-10.1.1.0
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic interface



!--- 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 Auto-NAT uses address translation.
!--- Hosts that access the mail server from the outside
!--- use the 203.0.113.10 address.




object network obj-172.16.31.10
   host 172.16.31.10
   nat (dmz,outside) static 203.0.113.10

access-group outside_int in interface outside







route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512



!--- 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
```

ESMTP TLS Configuration

If you use Transport Layer Security (TLS) encryption for email communication, then the Extended Simple Mail Transfer Protocol (ESMTP) inspection feature (enabled by default) in the ASA drops the packets. In order to allow the emails with TLS enabled, disable the ESMTP inspection feature as shown in the next example.

Note: Refer to Cisco bug ID CSCtn08326 (registered customers only) for more information.

```
<#root>

ciscoasa(config)#

policy-map global_policy

ciscoasa(config-pmap)#

class inspection_default

ciscoasa(config-pmap-c)#

no inspect esmtp

ciscoasa(config-pmap-c)#

exit

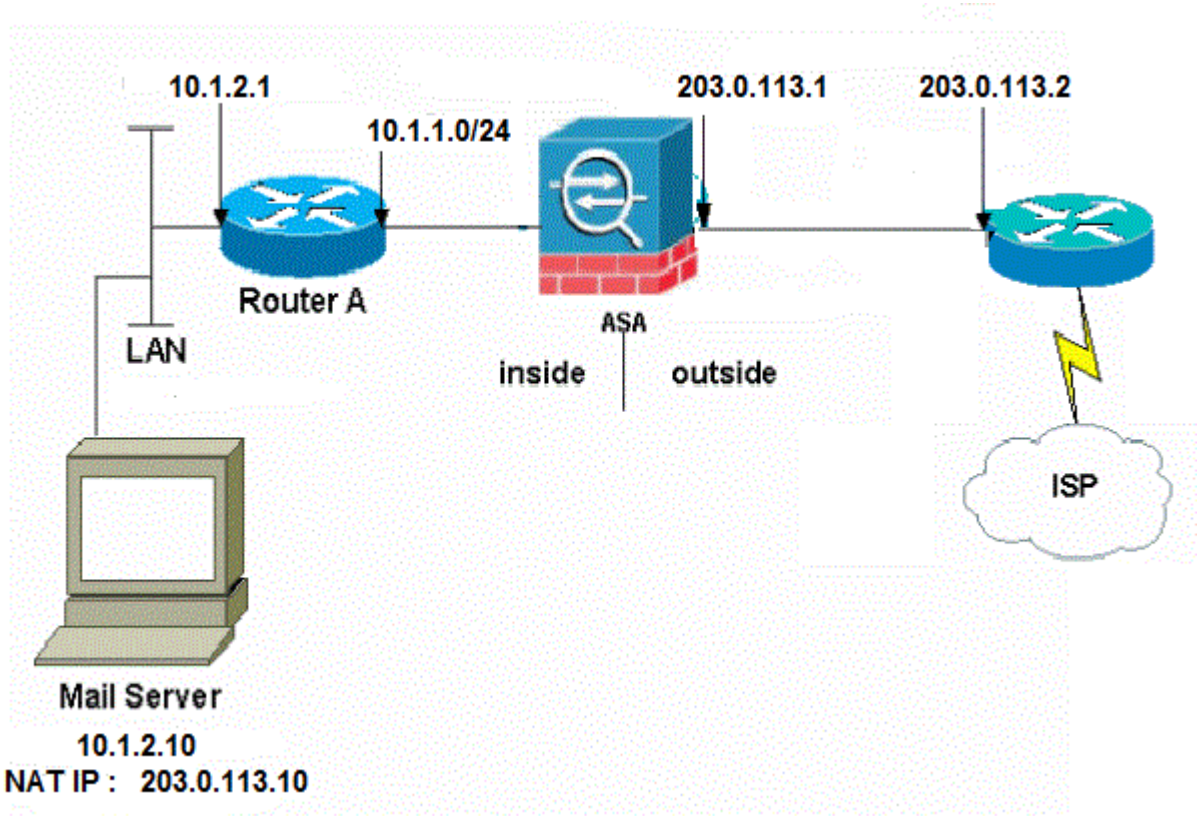
ciscoasa(config-pmap)#

exit
```

Mail Server in the Inside Network

Network Diagram

The configuration that is described in this section uses this network setup:



The network setup that is used in this example has the ASA with an inside network at **10.1.1.0/24** and an outside network at **203.0.113.0/24**. The mail server with the IP address **10.1.2.10** is located in the inside network.

ASA Configuration

This is the ASA configuration for this example:

```
<#root>

ASA#

show run

: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- Define the IP address for the inside interface.



interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
```

!--- Define the IP address for the outside interface.

```
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--
```

!--- Create an access list that permits Simple
!--- Mail Transfer Protocol (SMTP) traffic from anywhere
!--- to the host at 203.0.113.10 (our server). The name of this list is
!--- smtp. Add additional lines to this access list as required.
!---

Note:

There is one and only one access list allowed per
!--- interface per direction, for example, inbound on the outside interface.
!--- Because of limitation, any additional lines that need placement in
!--- the access list need to be specified here. If the server
!--- in question is not SMTP, replace the occurrences of SMTP with
!--- www, DNS, POP3, or whatever else is required.

```
access-list smtp extended permit tcp any host 10.1.2.10 eq smtp

--Omitted--
```

!--- Specify that any traffic that originates inside from the
!--- 10.1.2.x network NATs (PAT) to 203.0.113.9 if
!--- such traffic passes through the outside interface.

```
object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic 203.0.113.9
```

!--- Define a static translation between 10.1.2.10 on the inside and
!--- 203.0.113.10 on the outside. These are the addresses to be used by
!--- the server located inside the ASA.

```
object network obj-10.1.2.10
host 10.1.2.10
nat (inside,outside) static 203.0.113.10


!--- Apply the access list named smtp inbound on the outside interface.



access-group smtp in interface outside


!--- Instruct the ASA to hand any traffic destined for 10.1.2.0
!--- to the router at 10.1.1.2.



route inside 10.1.2.0 255.255.255.0 10.1.1.2 1


!--- Set the default route to  203.0.113.2.
!--- The ASA assumes that this address is a router address.

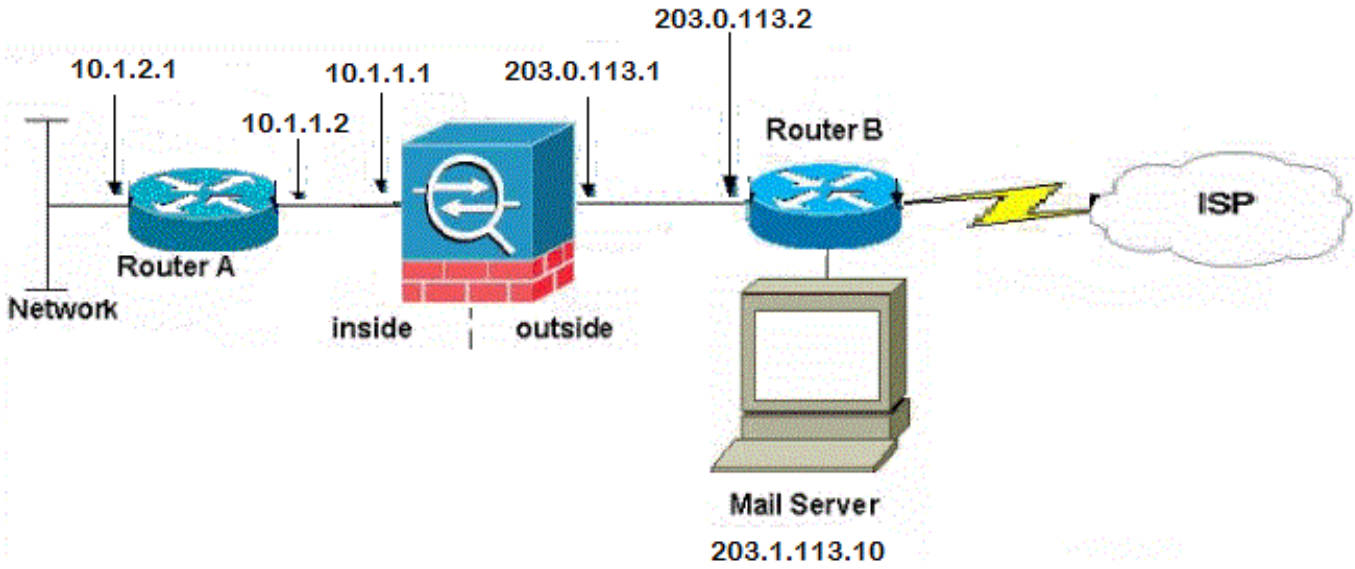


route outside 0.0.0.0 0.0.0.0 203.0.113.2 1
```

Mail Server in the Outside Network

Network Diagram

The configuration that is described in this section uses this network setup:



ASA Configuration

This is the ASA configuration for this example:

<#root>

ASA#

show run

```
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!--- Define the IP address for the inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
```

```
!--- Define the IP address for the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--



!--- This command indicates that all addresses in the 10.1.2.x range
!--- that pass from the inside (GigabitEthernet0/2) to a corresponding global
!--- destination are done with dynamic PAT.
!--- As outbound traffic is permitted by default on the ASA, no
!--- static commands are needed.




object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic interface


!--- Creates a static route for the 10.1.2.x network.
!--- The ASA forwards packets with these addresses to the router
!--- at 10.1.1.2




route inside 10.1.2.0 255.255.255.0 10.1.1.2 1


!--- Sets the default route for the ASA Firewall at 203.0.113.2



route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

--Omitted--

: end
```

Verify

Use the information that is provided in this section in order to verify that your configuration works properly.

Mail Server in the DMZ Network

TCP Ping

The TCP ping tests a connection over TCP (the default is Internet Control Message Protocol (ICMP)). A TCP ping sends SYN packets and considers the ping successful if the destination device sends a SYN-ACK packet. You can run at most two concurrent TCP pings at a time.

Here is an example:

<#root>

```
ciscoasa(config)#
```

ping tcp

```
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connection

The ASA is a stateful Firewall, and return traffic from the mail server is allowed back through the Firewall because it matches a connection in the Firewall connection table. The traffic that matches a current connection is allowed through the Firewall without being blocked by an interface Access Control List (ACL).

In the next example, the client on the outside interface establishes a connection to the 203.0.113.10 host of the DMZ interface. This connection is made with the TCP protocol and has been idle for two seconds. The connection flags indicate the current state of this connection:

```
<#root>

ciscoasa(config)#

show conn  address  172.16.31.10


1 in use, 2 most used
TCP outside  203.0.113.2:16678 dmz  172.16.31.10:25, idle 0:00:02, bytes 921, flags UIO
```

Logging

The ASA Firewall generates syslogs during normal operation. The syslogs range in verbosity based on the logging configuration. This output shows two syslogs that appear at level six (the *informational* level) and level seven (the *debugging* level):

```
<#root>

ciscoasa(config)#

show logging  | i 172.16.31.10


%ASA-7-609001: Built local-host dmz:172.16.31.10

%ASA-6-302013: Built inbound TCP connection 11 for outside:203.0.113.2/16678
 (203.0.113.2/16678) to dmz:172.16.31.10/25 (203.0.113.10/25)
```

The second syslog in this example indicates that the Firewall has built a connection in its connection table for this specific traffic between the client and server. If the Firewall was configured in order to block this connection attempt, or some other factor inhibited the creation of this connection (resource constraints or a

possible misconfiguration), the Firewall would not generate a log that indicates that the connection was built. Instead, it would log a reason for the connection to be denied or an indication about the factor that inhibited the connection from being created.

For instance, if the ACL on the outside is not configured to permit **172.16.31.10** on port 25, then you would see this log when the traffic is denied:

%ASA-4-106100: access-list outside_int denied tcp outside/203.0.113.2(3756) -> dmz/172.16.31.10(25) hit-cnt 5 300-second interval

This would occur when an ACL is missing or misconfigured as shown here:

```
access-list outside_int extended permit tcp any4 host 172.16.31.10 eq http

access-list outside_int extended deny ip any4 any4
```

NAT Translations (Xlate)

In order to confirm that the translations are created, you can check the Xlate (translation) table. The command **show xlate**, when combined with the local keyword and the internal host IP address, shows all of the entries that are present in the translation table for that host. The next output shows that there is a translation currently built for this host between the DMZ and the outside interfaces. The DMZ server IP address is translated to the 203.0.113.10 address per the previous configuration. The flags that are listed (**s** in this example) indicate that the translation is *static*.

```
<#root>

ciscoasa(config)#

show nat detail


Manual NAT Policies (Section 1)
1 (dmz) to (outside) source static obj-172.16.31.10 obj-203.0.113.10
    translate_hits = 7, untranslate_hits = 6
    Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32


Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static obj-172.16.31.10 203.0.113.10
    translate_hits = 1, untranslate_hits = 5
    Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24


ciscoasa(config)#

show xlate
```

```
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:172.16.31.10 to outside:203.0.113.10
    flags s idle 0:10:48 timeout 0:00:00
NAT from inside:10.1.1.0/24 to dmz:10.1.1.0/24
    flags sI idle 79:56:17 timeout 0:00:00
NAT from dmz:172.16.31.10 to outside:203.0.113.10
    flags sT idle 0:01:02 timeout 0:00:00
NAT from outside:0.0.0.0/0 to dmz:0.0.0.0/0
    flags sIT idle 0:01:02 timeout 0:00:00
```

Mail Server in the Inside Network

TCP Ping

Here is an example TCP ping output:

<#root>

```
ciscoasa(config)#
```

PING TCP

```
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
```

```
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connection

Here is an example connection verification:

<#root>

```
ciscoasa(config)#
```

```
show conn  address  10.1.2.10
```

```
1 in use, 2 most used
TCP outside  203.0.113.2:5672 inside  10.1.2.10:25, idle 0:00:05, bytes 871, flags UIO
```

Logging

Here is an example syslog:

```
%ASA-6-302013: Built inbound TCP connection 553 for outside:203.0.113.2/19198
 (203.0.113.2/19198) to inside:10.1.2.10/25 (203.0.113.10/25)
```

NAT Translations (Xlate)

Here are some example **show nat detail** and **show xlate** command outputs:

<#root>

```
ciscoasa(config)#
```

```
show nat detail
```

```
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-10.1.2.10 203.0.113.10
    translate_hits = 0, untranslate_hits = 15
    Source - Origin: 10.1.2.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24
```

```
ciscoasa(config)#
```

```
show xlate
```

```
NAT from inside:10.1.2.10 to outside:203.0.113.10
    flags s idle 0:00:03 timeout 0:00:00
```

Mail Server in the Outside Network

TCP Ping

Here is an example TCP ping output:

<#root>

```
ciscoasa#
```

```
PING TCP
```

```
Interface: inside
Target IP address: 203.1.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 10.1.2.10
Source port: [0] 1234
Repeat count: [5] 5
```

```
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.1.113.10 port 25
from 10.1.2.10 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connection

Here is an example connection verification:

<#root>

```
ciscoasa#
```

show conn address 203.1.113.10

```
1 in use, 2 most used
TCP inside 10.1.2.10:13539 outside 203.1.113.10:25, idle 0:00:02, bytes 898, flags UIO
```

Logging

Here is an example syslog:

<#root>

```
ciscoasa#
```

show logging | i 203.1.113.10

```
%ASA-6-302013: Built outbound TCP connection 590 for outside:203.1.113.10/25
 (203.1.113.10/25) to inside:10.1.2.10/1234 (203.0.113.1/1234)
```

NAT Translations (Xlate)

Here is an example **show xlate** command output:

```
<#root>

ciscoasa#

show xlate | i 10.1.2.10



TCP PAT from inside:10.1.2.10/1234 to outside:203.0.113.1/1234 flags ri idle
 0:00:04 timeout 0:00:30
```

Troubleshoot

The ASA provides multiple tools with which to troubleshoot connectivity. If the issue persists after you verify the configuration and check the outputs that are described in the previous section, these tools and techniques can help you determine the cause of your connectivity failure.

Mail Server in the DMZ Network

Packet-Tracer

The packet tracerfunctionality on the ASA allows you to specify a *simulated* packet and view all of the various steps, checks, and functions that the Firewall goes through when it processes traffic. With this tool, it is helpful to identify an example of traffic that you believe *must* be allowed to pass through the Firewall, and use that five-tupple in order to simulate the traffic. In the next example, the packet tracer is used in order to simulate a connection attempt that meets these criteria:

- The simulated packet arrives on the **outside**.
- The protocol that is used is **TCP**.
- The simulated client IP address is **203.0.113.2**.
- The client sends traffic that is sourced from port **1234**.
- The traffic is destined to a server at IP address **203.0.113.10**.
- The traffic is destined to port **25**.

Here is an example packet tracer output:

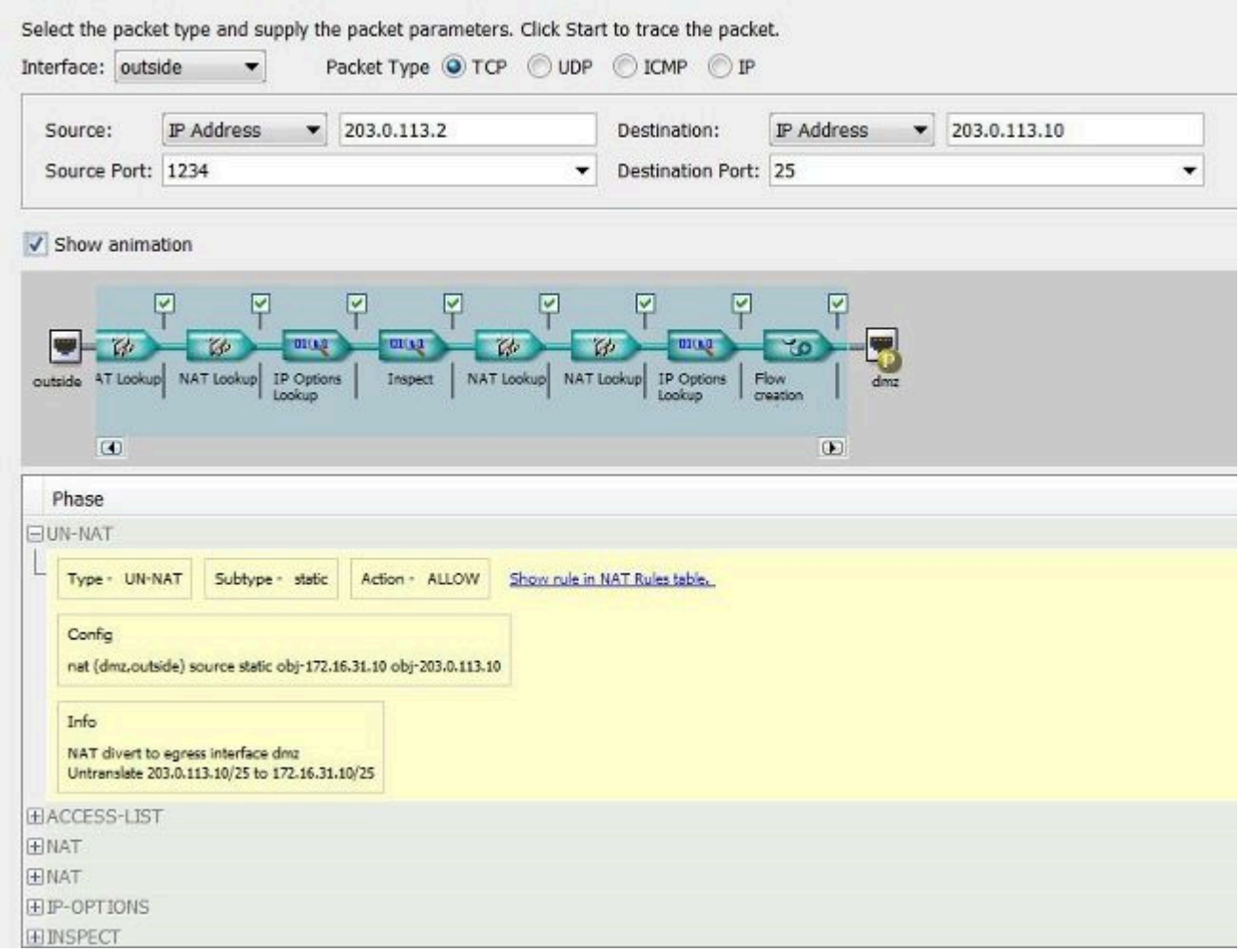
```
packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.31.10 obj-203.0.113.10
Additional Information:
NAT divert to egress interface dmz
Untranslate 203.0.113.10/25 to 172.16.31.10/25
```

```
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Here is an example on the Cisco Adaptive Security Device Manager (ASDM):



Notice that there is no mention of the *DMZ* interface in the previous outputs. This is by packet tracer design. The tool tells you how the Firewall processes that type of connection attempt, which includes how it would route it and out of which interface.

Tip: For additional information about the packet tracer feature, refer to the Tracing packets with Packet Tracer section of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6.*

Packet Capture

The ASA Firewall can capture traffic that enters or leaves its interfaces. This capture functionality is very useful because it can definitively prove whether traffic arrives at, or leaves from, a Firewall. The next example shows the configuration of two captures named **capd** and **capout** on the DMZ and outside interfaces, respectively. The capture commands use a match keyword, which allows you to be specific about the traffic that you want to capture.

For the **capture capd** in this example, it is indicated that you want to match the traffic seen on the DMZ interface (ingress or egress) that matches TCP host 172.16.31.10/host 203.0.113.2. In other words, you want to capture any TCP traffic that is sent from host 172.16.31.10 to host 203.0.113.2, or vice versa. The use of the match keyword allows the Firewall to capture that traffic bidirectionally. The capture command that is defined for the outside interface does not reference the internal mail server IP address because the Firewall conducts an NAT on that mail server IP address. As a result, you cannot match with that server IP address. Instead, the next example uses the word **any** in order to indicate that all possible IP addresses would match that condition.

After you configure the captures, you must then attempt to establish a connection again and proceed to view the captures with the **show capture <capture_name>** command. In this example, you can see that the outside host was able to connect to the mail server, as evident by the TCP three-way handshake that is seen in the captures:

<#root>

ASA#

capture capd interface dmz match tcp host 172.16.31.10 any

ASA#

capture capout interface outside match tcp any host 203.0.113.10

ASA#

show capture capd

3 packets captured

```
   1: 11:31:23.432655       203.0.113.2.65281 > 172.16.31.10.25: S 780523448:
   780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   2: 11:31:23.712518       172.16.31.10.25 > 203.0.113.2.65281: S 2123396067:
   2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
   3: 11:31:23.712884       203.0.113.2.65281 > 172.16.31.10.25. ack 2123396068
   win 32768
```

ASA#

show capture capout

3 packets captured

```
   1: 11:31:23.432869       203.0.113.2.65281 > 203.0.113.10.25: S 1633080465:
   1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
   2: 11:31:23.712472       203.0.113.10.25 > 203.0.113.2.65281: S 95714629:
   95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
   3: 11:31:23.712914        203.0.113.2.65281 > 203.0.113.10.25: . ack 95714630
   win 32768
```

Mail Server in the Inside Network

Packet-Tracer

Here is an example packet tracer output:

```
CLI : packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.1.2.10
 nat (inside,outside) static 203.0.113.10
Additional Information:
NAT divert to egress interface inside
Untranslate 203.0.113.10/25 to 10.1.2.10/25

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group smtp in interface outside
access-list smtp extended permit tcp any4 host 10.1.2.10 eq smtp
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x77dd2c50, priority=13, domain=permit, deny=false
        hits=1, user_data=0x735dc880, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
        dst ip/id=10.1.2.10, mask=255.255.255.255, port=25, tag=0, dscp=0x0
        input_ifc=outside, output_ifc=any
```

Mail Server in the Outside Network

Packet-Tracer

Here is an example packet tracer output:

```
CLI :  packet-tracer input inside tcp 10.1.2.10 1234 203.1.113.10 25 detailed

--Omitted--

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 203.1.113.0 255.255.255.0 outside

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.1.2.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.1.2.10/1234 to 203.0.113.1/1234
Forward Flow based lookup yields rule:
in id=0x778b14a8, priority=6, domain=nat, deny=false
hits=11, user_data=0x778b0f48, cs_id=0x0, flags=0x0, protocol=0
src ip/id=10.1.2.0, mask=255.255.255.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=inside, output_ifc=outside
```

Related Information

- **ASA Packet Captures with CLI and ASDM Configuration Example**
- **Cisco ASA Series CLI Configuration Guide – Configuring Network Object NAT**
- **Technical Support & Documentation - Cisco Systems**