在DMZ、Inside和Outside Networks中配置ASA以访问SMTP邮件服务器

目录

简介

本文档介绍如何配置思科自适应安全设备(ASA)以访问位于隔离区(DMZ)、内部网络或外部网络中的简单邮件传输协议(SMTP)服务器。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本9.1或更高版本的Cisco ASA
- 采用Cisco IOS®软件版本15.1(4)^{M6}的Cisco 2800C系列路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

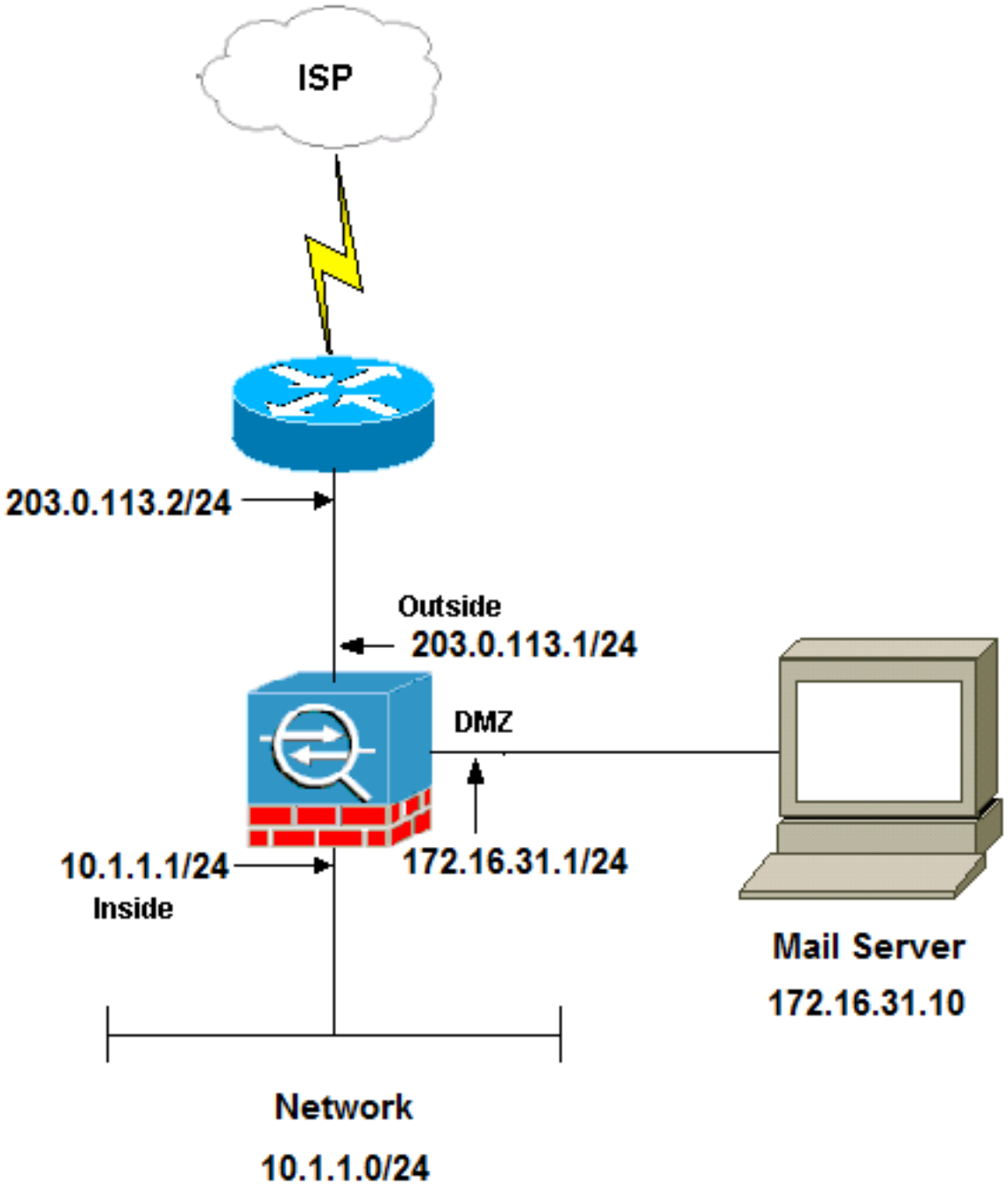
本节介绍如何配置ASA以访问DMZ网络、内部网络或外部网络中的邮件服务器。

> **注意**：使用命令查找工具(仅注册客户)可获取有关本节中使用的命令的详细信息。

DMZ网络中的邮件服务器

网络图

本节中介绍的配置使用以下网络设置：



注意：本文档中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

本示例中使用的网络设置的ASA内部网络为**10.1.1.0/24**，外部网络为**203.0.113.0/24**。IP地址为**172.16.31.10**的邮件服务器位于DMZ网络中。要使内部网络访问邮件服务器，必须配置身份网络地址转换(NAT)。

为了让外部用户访问邮件服务器，必须配置静态NAT和访问列表(在本例中为**outside_int**)，以便允许外部用户访问邮件服务器并将访问列表绑定到外部接口。

ASA 配置

以下是本示例的ASA配置：

```
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 配置

如果将传输层安全(TLS)加密用于电子邮件通信，则ASA中的扩展简单邮件传输协议(ESMTP)检测功能（默认启用）会丢弃数据包。要允许启用TLS的邮件，请禁用ESMTP检测功能，如下例所示。

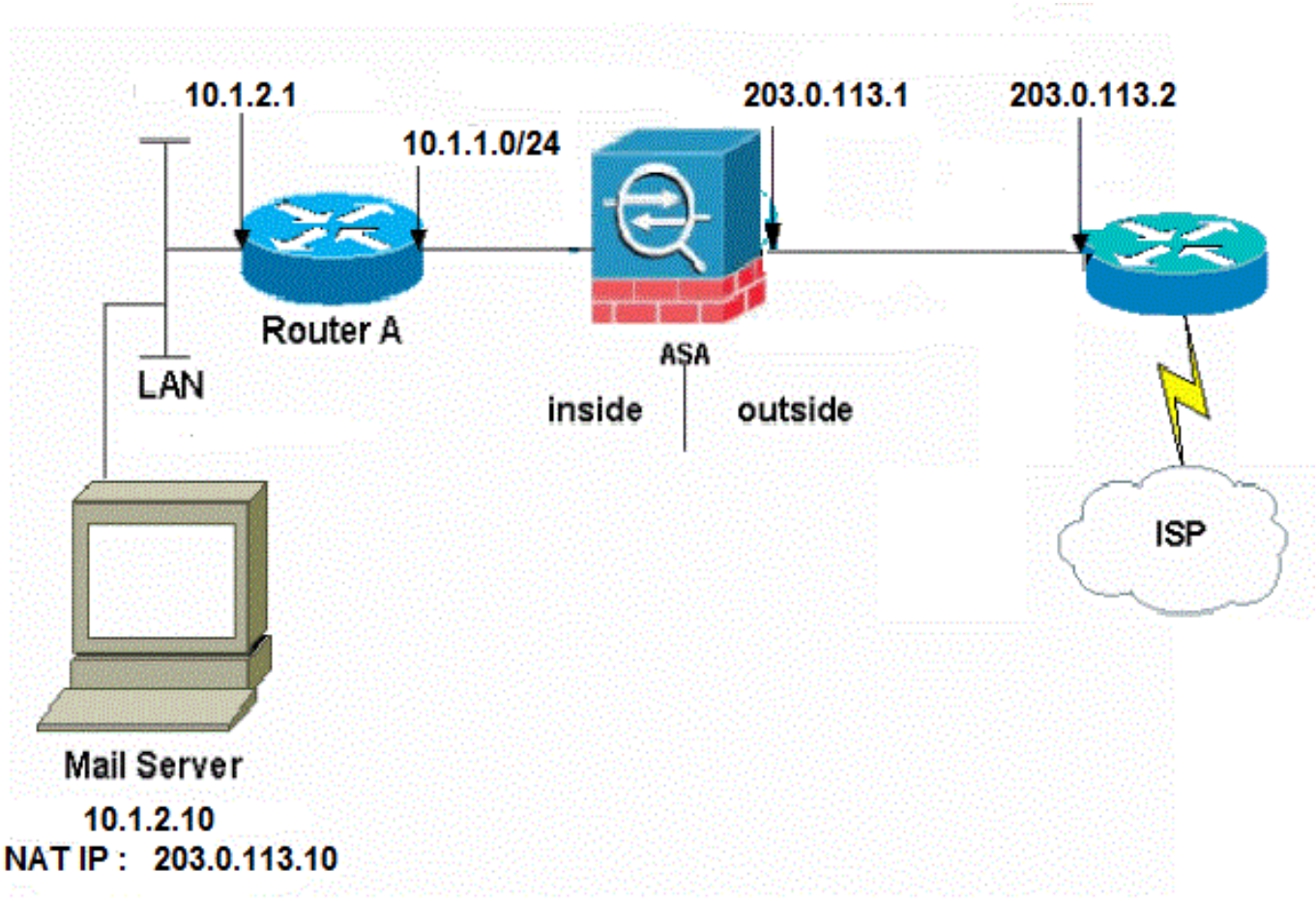
> **注意**：有关更多信息，请参阅思科漏洞 ID CSCtn08326（仅限注册用户）。

```
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
```

内部网络中的邮件服务器

网络图

本节中介绍的配置使用以下网络设置：



本示例中使用的网络设置的ASA内部网络为10.1.1.0/24，外部网络为203.0.113.0/24。IP地址为10.1.2.10的邮件服务器位于内部网络中。

ASA 配置

以下是本示例的ASA配置：

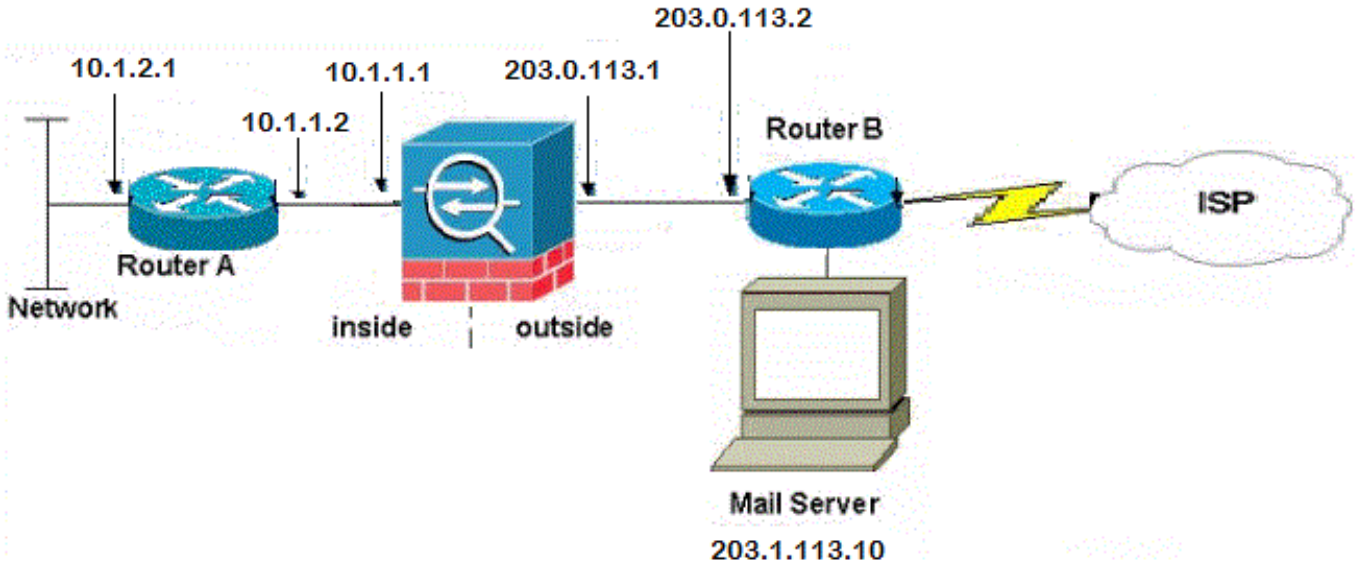
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
```

```
!
--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
```

外部网络中的邮件服务器

网络图

本节中介绍的配置使用以下网络设置：



ASA 配置

以下是本示例的ASA配置：

```
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
```

验证

使用本节中提供的信息验证配置是否正常工作。

DMZ网络中的邮件服务器

TCP Ping

TCP ping测试通过TCP的连接(默认为Internet控制消息协议(ICMP))。TCP ping发送SYN数据包，如果目的设备发送SYN-ACK数据包，则认为ping成功。您一次最多可以运行两次并发TCP ping。

示例如下：

```
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
```

连接

ASA是状态防火墙，来自邮件服务器的返回流量允许通过防火墙返回，因为它与防火墙连接表中的连接匹配。与当前连接匹配的流量可以通过防火墙，而不会被接口访问控制列表(ACL)阻止。

在下一个示例中，外部接口上的客户端与DMZ接口的203.0.113.10主机建立连接。此连接使用TCP协议建立，已空闲两秒。连接标志指示此连接的当前状态：

```
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
```

日志记录

在正常运行期间，ASA 防火墙会生成系统日志。根据日志记录配置，系统日志的内容十分丰富。此输出显示出两个系统日志，分别显示在第6级(*信息*级)和第7级(调试级):

```
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)
```

本示例中的第二个系统日志表示防火墙已在其连接表中为客户端和服务器之间的此特定流量建立连接。如果防火墙已配置为阻止此连接尝试，或者有其他因素禁止创建此连接（资源限制或配置错误），防火墙不会生成日志来表明建立了此连接。相反，它会记录连接被拒绝的原因或有关阻止创建连接的因素的指示。

例如，如果外部的ACL未配置为允许端口25上的**172.16.31.10**，则当流量被拒绝时，您将看到此日志：

%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秒间隔

如下所示，当ACL缺失或配置错误时，会发生这种情况：

```
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 转换 (Xlate)

要确认已创建转换，可以检查Xlate（转换）表。命令**show xlate**与local关键字和内部主机IP地址结合使用时，会显示该主机转换表中存在的所有条目。下一个输出显示当前为此主机在DMZ和外部接口之间构建的转换。DMZ服务器IP地址根据之前的配置转换为203.0.113.10地址。列出的标志(**本**例中的)表示转换是*静态*。

```
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
```

内部网络中的邮件服务器

TCP Ping

以下是TCP ping输出示例：

```
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
```

连接

以下是连接验证示例：

```
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
```

日志记录

以下是系统日志示例：

```
%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 转换 (Xlate)

以下是show nat detail和**show xlate命令输出的一些**示例：

```
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
```

外部网络中的邮件服务器

TCP Ping

以下是TCP ping输出示例：

```
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
```

连接

以下是连接验证示例：

```
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
```

日志记录

以下是系统日志示例：

```
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 转换 (Xlate)

以下是show xlate命令输出示例：

```
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
```

故障排除

ASA提供多种工具来排除连接故障。如果在您验证配置并检查上一节所述的输出后问题仍然存在，这些工具和技术可能有助于您确定连接故障的原因。

DMZ网络中的邮件服务器

Packet-Tracer

ASA上的Packet Tracer功能允许您指定模拟数据包，并查看防火墙在处理流量时执行的所有步骤、检查和功能。使用此工具，可以确定您认为应允许其通过防火墙的流量示例，并使用该五管来模拟流量，这非常有帮助。在下一个示例中，使用Packet Tracer来模拟符合以下条件的连接尝试：

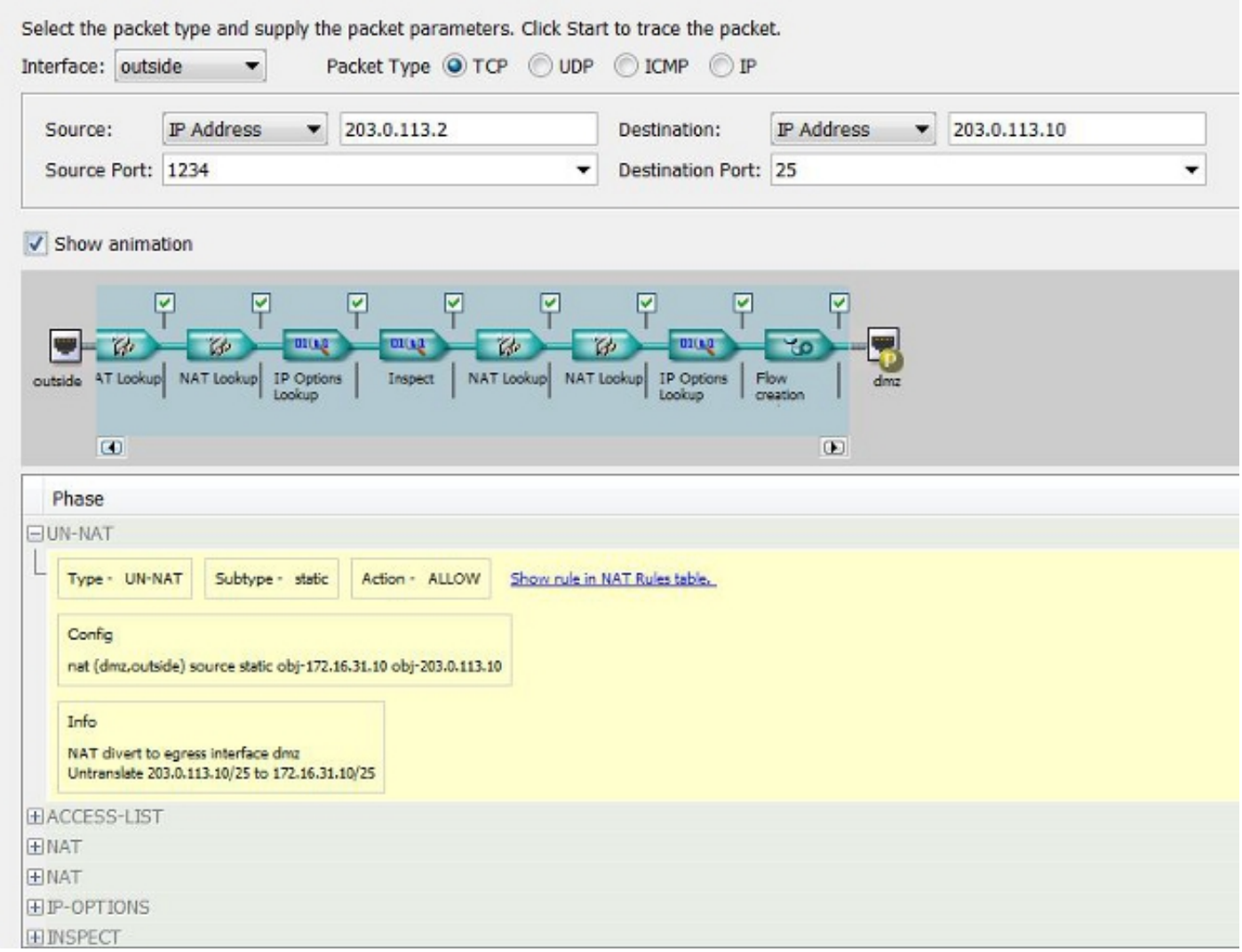
- 模拟数据包到达外部。
- 使用的协议是TCP。
- 模拟客户端 IP 地址为 203.0.113.2。
- 客户端发送来自端口1234的流量。
- 流量的目的位置是 IP 地址为 203.0.113.10 的服务器。
- 流量抵达于端口 25。

以下是Packet Tracer输出示例：

```
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
```

以下是思科自适应安全设备管理器(ASDM)的示例：



请注意，在前面的输出中*未提*及DMZ接口。这是由于 Packet Tracer 设计上的原因。该工具将告诉您防火墙如何处理该类型的连接尝试，包括如何将其路由以及从哪个接口发出。

> **提示：**有关Packet Tracer功能的其他信息，请参阅*Cisco ASA 5500系列配置指南（使用CLI、8.4和8.6）的*使用Packet Tracer跟踪数据包部分。

数据包捕获

ASA 防火墙可以捕获进入或离开接口的流量。此捕获功能非常有用，因为它可以明确证明流量是到达还是离开防火墙。下一个示例显示在DMZ和外部接口上分别配置两个名为**capd**和**capout**的捕获。capture命令使用match关键字，该关键字允许您特定于要捕获的流量。

对于本例中的**capture capd** ，表示要匹配在DMZ接口（入口或出口）上发现的与TCP主机172.16.31.10/host 203.0.113.2匹配的流量。换句话说，要捕获从主机172.16.31发送的任何TCP流量。10到主机203.0.113.2，反之亦然。使用 match 关键字可以使防火墙双向捕捉流量。为外部接口定义的capture命令不引用内部邮件服务器IP地址，因为防火墙对该邮件服务器IP地址执行NAT。因此，您无法与该服务器IP地址匹配。相反，下一个示例使用单词**any**来表示所有可能的IP地址都与该条件匹配。

配置捕获后，应再次尝试建立连接，然后使用show capture <capture_name>命**令继续查看捕**获。在本例中，您可以看到外部主机能够连接到邮件服务器，如捕获中看到的TCP三次握手所示：

```
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
```

内部网络中的邮件服务器

Packet-Tracer

以下是Packet Tracer输出示例：

```
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
```

外部网络中的邮件服务器

Packet-Tracer

以下是Packet Tracer输出示例：

```
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
```

相关信息

- [Cisco ASA系列系统日志消息]

- 通过 CLI 和 ASDM 配置实现 ASA 数据包捕获示例
- Cisco ASA系列CLI配置指南，9.0 — 配置网络对象NAT
- 技术支持和文档 — Cisco Systems