為DMZ、內部和外部網路中的SMTP郵件伺服器訪問配置ASA

目錄

簡介
必要條件
需求
採用元件
慣例
設定
DMZ網路中的郵件伺服器
網路圖表
ASA配置
ESMTP TLS配置
內部網路中的郵件伺服器
網路圖表
ASA配置
外部網路中的郵件伺服器
網路圖表
ASA配置
驗證
DMZ網路中的郵件伺服器
TCP Ping
連線
記錄
NAT轉譯(Xlate)
內部網路中的郵件伺服器
TCP Ping
連線
記錄
NAT轉譯(Xlate)
外部網路中的郵件伺服器
TCP Ping
連線
記錄
NAT轉譯(Xlate)
疑難排解
DMZ網路中的郵件伺服器
Packet Tracer
封包擷取

內部網路中的郵件伺服器
Packet Tracer
外部網路中的郵件伺服器
Packet Tracer
相關資訊

簡介

本文說明如何配置思科自適應安全裝置(ASA)，使其可以訪問位於非軍事區(DMZ)、內部網路或外部網路中的簡單郵件傳輸協定(SMTP)伺服器。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本9.1或更高版本的Cisco ASA
- 採用Cisco IOS®軟體版本15.^{1}(4)M6的Cisco 2800C系列路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

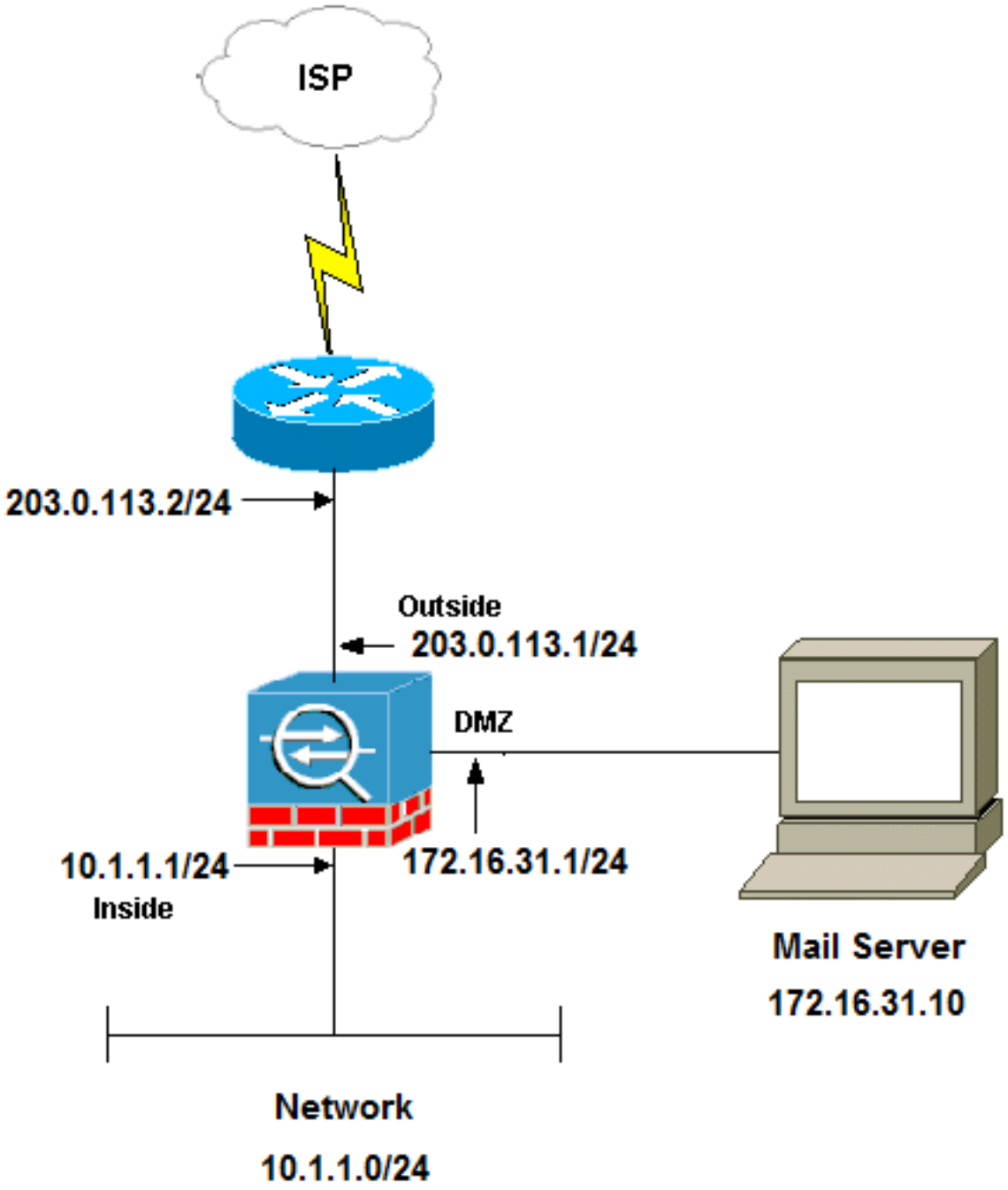
本節介紹如何配置ASA以訪問DMZ網路中的郵件伺服器、內部網路或外部網路。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

DMZ網路中的郵件伺服器

網路圖表

本節所述的設定使用以下網路設定：



附註：本文檔中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

本示例中使用的網路設定具有內部網路為**10.1.1.0/24**，外部網路為**203.0.113.0/24**的ASA。IP地址為**172.16.31.10**的郵件伺服器位於DMZ網路中。要使內部網路訪問郵件伺服器，您必須配置身份網路地址轉換(NAT)。

為了使外部使用者能夠訪問郵件伺服器，您必須配置靜態NAT和訪問清單(在本例中為**outside_int**)，以允許外部使用者訪問郵件伺服器並將訪問清單繫結到外部介面。

ASA配置

以下是此示例的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

如果您對電子郵件通訊使用傳輸層安全(TLS)加密，則ASA中的擴展簡單郵件傳輸協定(ESMTP)檢查功能（預設啟用）會丟棄資料包。為了允許啟用TLS的電子郵件，請禁用ESMTP檢查功能，如下例所示。

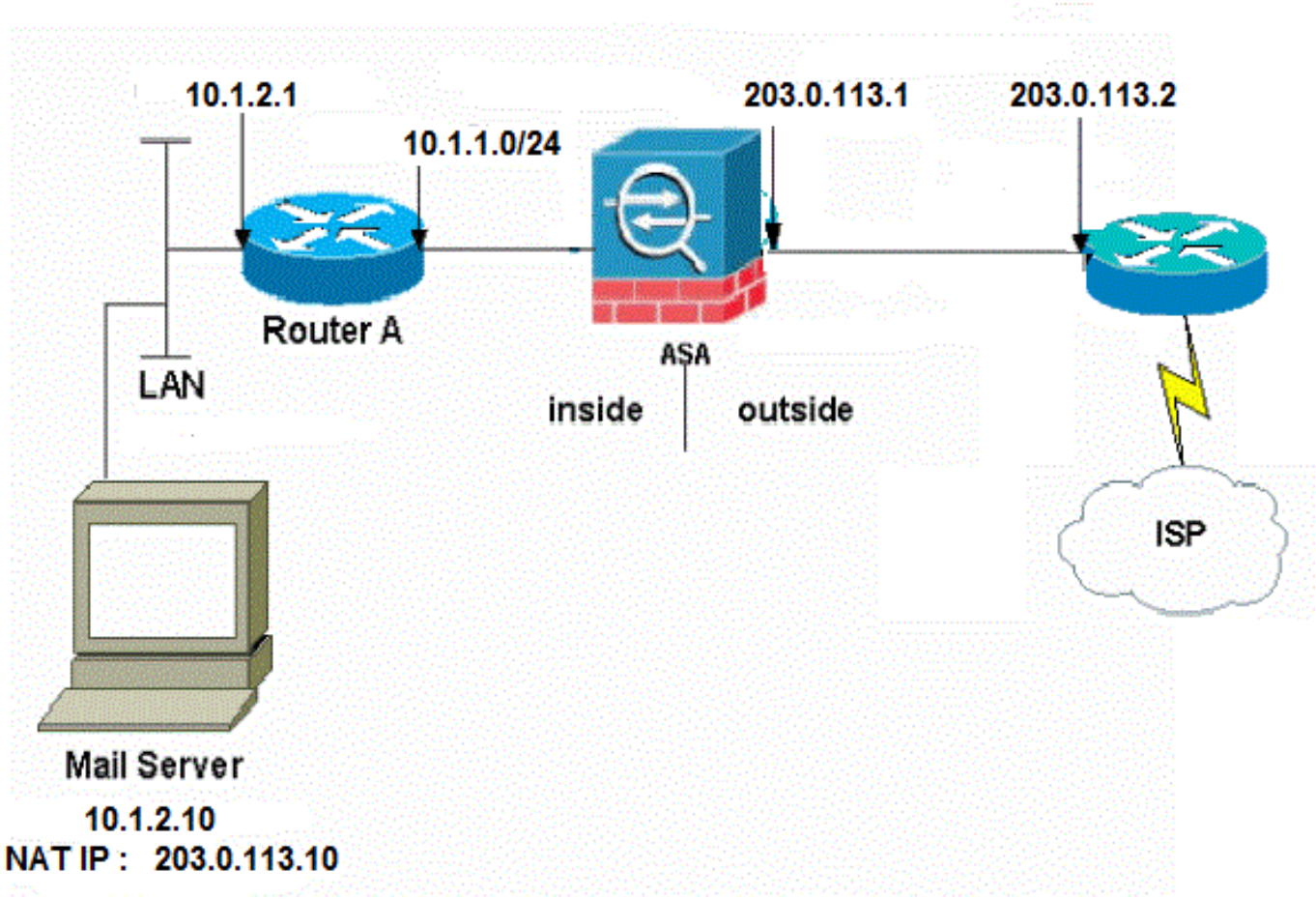
> **附註**：如需詳細資訊，請參閱Cisco錯誤ID CSCtn08326(僅限註冊客戶)。

```
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
```

內部網路中的郵件伺服器

網路圖表

本節所述的設定使用以下網路設定：



本示例中使用的網路設定具有內部網路為10.1.1.0/24，外部網路為203.0.113.0/24的ASA。IP地址為10.1.2.10的郵件伺服器位於內部網路中。

ASA配置

以下是此示例的ASA配置：

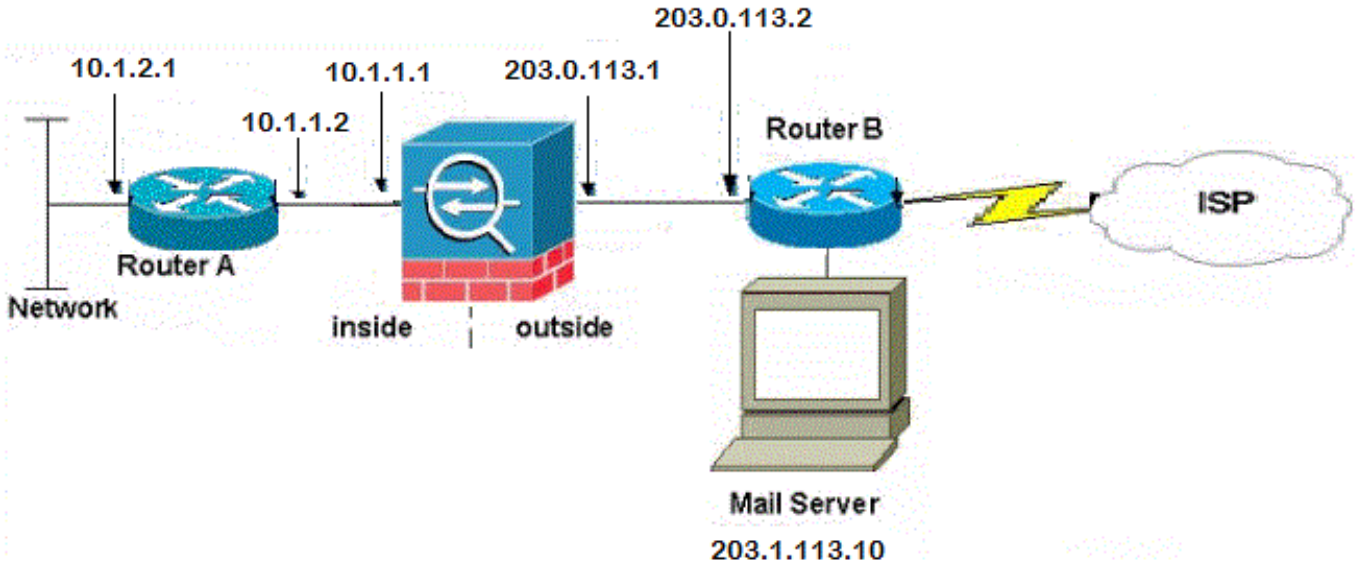
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
```

```
!
--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
```

外部網路中的郵件伺服器

網路圖表

本節所述的設定使用以下網路設定：



ASA配置

以下是此示例的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
```

驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

DMZ網路中的郵件伺服器

TCP Ping

TCP ping會測試透過TCP建立的連線(預設為網際網路控制訊息通訊協定(ICMP))。TCP ping會傳送SYN封包，如果目的地裝置傳送了SYN-ACK封包，便會認為ping成功。一次最多可以同時執行兩個TCP ping。

以下是範例：

```
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
```

連線

ASA是有狀態防火牆，並且允許來自郵件伺服器的返回流量通過防火牆，因為它與防火牆連線表中的連線相匹配。允許與當前連線匹配的流量通過防火牆，而無需被介面訪問控制清單(ACL)阻止。

在下一個示例中，外部介面上的客戶端與DMZ介面的203.0.113.10主機建立連線。此連線是使用TCP協定建立並且已空閒兩秒。連線標誌指示此連線的當前狀態：

```
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
```

記錄

ASA防火牆在正常運行期間生成系統日誌。系統日誌的範圍取決於日誌記錄配置。此輸出顯示在級別6（資訊級別）和級別7(調試級別)顯示的兩個*系統*日誌：

```
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)
```

此示例中的第二個系統日誌表示防火牆已在其連線表中為客戶端和伺服器之間的此特定流量建立了連線。如果防火牆配置為阻止此連線嘗試，或者某個其他因素阻止了此連線的建立（資源限制或可能的配置錯誤），則防火牆將不會生成指示已建立連線的日誌。相反，它將記錄拒絕連線的原因或禁止建立連線的因素的指示。

例如，如果外部的ACL未設定為允許連線埠25上的172.16.31.10，則流量遭到拒絕時會顯示以下日誌：

%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秒間隔

如果ACL丟失或配置錯誤（如下所示），就會發生這種情況：

```
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轉譯(Xlate)

為了確認已建立轉換，您可以檢查Xlate（轉換）表。show xlate命令與local關鍵字和內部主機IP地址組合使用時，會顯示該主機轉換表中存在的所有條目。下一個輸出顯示，當前已為此主機在DMZ和外部介面之間構建轉換。根據之前的配置，DMZ伺服器IP地址被轉換為203.0.113.10地址。列出的標誌(在本例中)表示轉換是靜態*的*。

```
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
```

內部網路中的郵件伺服器

TCP Ping

以下是TCP ping輸出的範例：

```
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
```

連線

以下是連線驗證範例：

```
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
```

記錄

以下是系統日誌示例：

```
%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轉譯(Xlate)

以下是一些**show nat detail**和**show xlate**命令輸出的範例：

```
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
```

外部網路中的郵件伺服器

TCP Ping

以下是TCP ping輸出的範例：

```
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
```

連線

以下是連線驗證範例：

```
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
```

記錄

以下是系統日誌示例：

```
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轉譯(Xlate)

以下是**show xlate命令**輸出範例：

```
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
```

疑難排解

ASA提供多種工具用於排除連線故障。如果在驗證配置並檢查前一節中介紹的輸出後，問題仍然存在，則這些工具和技術可幫助您確定連線失敗的原因。

DMZ網路中的郵件伺服器

Packet Tracer

ASA上的Packet Tracer功能允許您指定模擬的數*據*包，並檢視防火牆處理流量時執行的所有各種步驟、檢查和功能。使用此工具，識別您認為應該允許通過防火牆的流量示例，並使用該五元組來模擬流量*是很有幫助*的。在下一個示例中，使用Packet Tracer模擬符合以下條件的連線嘗試：

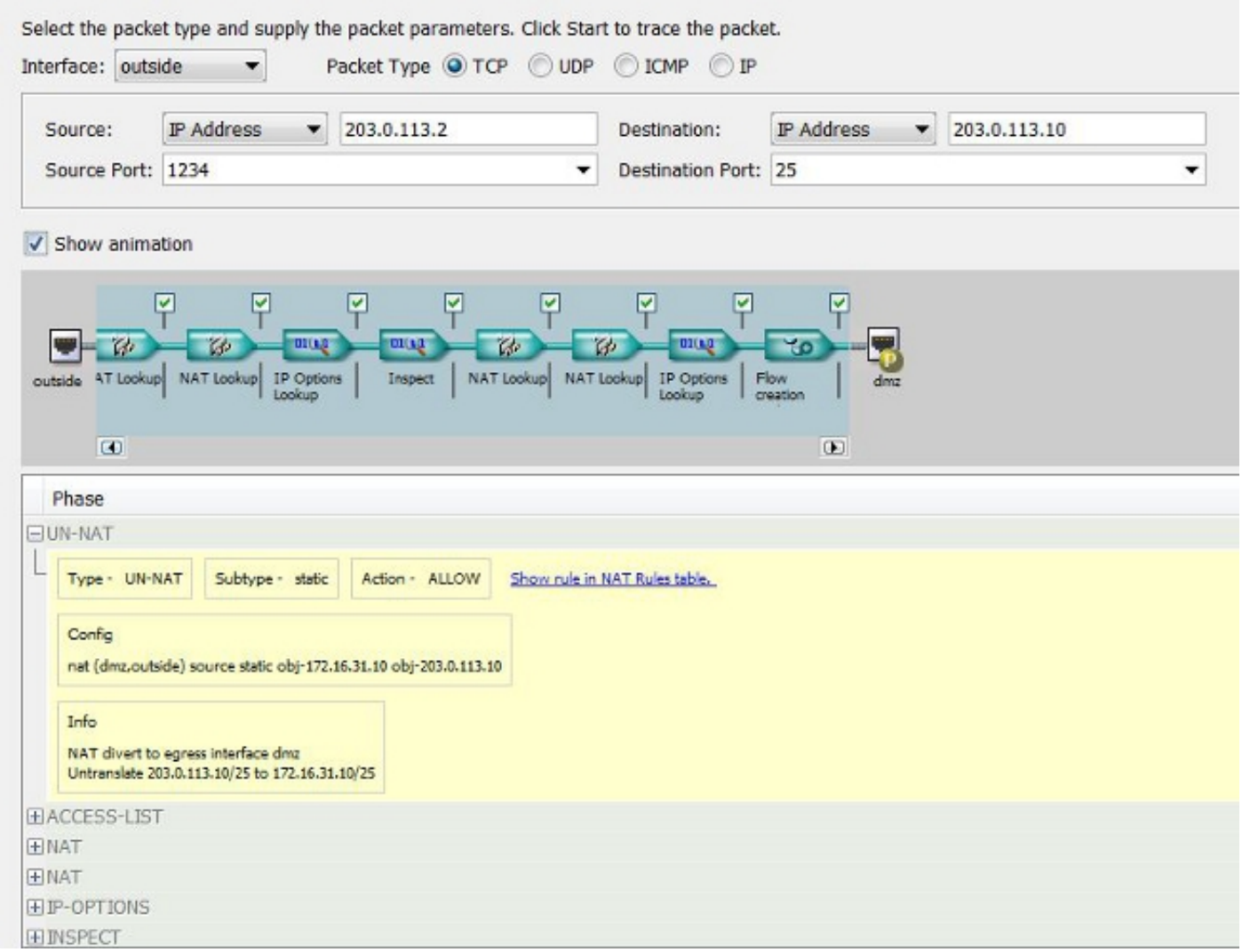
- 模擬資料包到達**外部**。
- 使用的協定是**TCP**。
- 模擬客戶端IP地址為**203.0.113.2**。
- 使用者端傳送源自連線埠1234的**流量**。
- 流量將發往IP地址為**203.0.113.10**的伺服器。
- 流量將傳至連線埠**25**。

以下是Packet Tracer輸出示例：

```
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
```

以下是思科調適型資安裝置管理員(ASDM)上的範例：



請注意，之前的輸出中並未提及*DMZ*介面。這是通過Packet Tracer設計的。該工具將告訴您防火牆如何處理此類連線嘗試，包括它將如何路由它以及從哪個介面發出。

> **提示：**有關Packet Tracer功能的其他資訊，請參閱*使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南*的使用Packet Tracer跟蹤資料包部分。

封包擷取

ASA防火牆可以捕獲進入或離開其介面的流量。此擷取功能非常有用，因為它可以確實證明流量是到達防火牆或從防火牆離開。下一個示例顯示了在DMZ和外部介面上分別配置兩個名為**capd**和**capout**的捕獲。capture命令使用match關鍵字，允許您具體說明要捕獲的流量。

在本範例中，擷取**capd**表示您要與在DMZ介面上看到的與TCP主機172.16.31.10/host 203.0.113.2相符的流量（輸入或輸出）相符。換句話說，您要擷取從主機172.16.31.10傳送到主機203.0.113.2的任何TCP流量，反之亦然。使用match關鍵字允許防火牆雙向捕獲該流量。為外部介面定義的capture命令未引用內部郵件伺服器IP地址，因為防火牆在該郵件伺服器IP地址上執行NAT。因此，您無法與該伺服器IP地址匹配。相反，下一個示例使用**any**一詞來表示所有可能的IP地址都將與該條件匹配。

配置捕獲後，您應嘗試再次建立連線，並繼續使用**show capture <capture_name>**命令檢視捕獲。在此範例中，您可以看到外部主機能夠連線到郵件伺服器，如擷取中所看到的TCP三次交握所示：

```
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
```

內部網路中的郵件伺服器

Packet Tracer

以下是Packet Tracer輸出示例：

```
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
```

外部網路中的郵件伺服器

Packet Tracer

以下是Packet Tracer輸出示例：

```
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
```

相關資訊

- [Cisco ASA系列系統日誌消息]

- 使用CLI和ASDM的ASA資料包捕獲配置示例
- Cisco ASA系列CLI配置指南9.0 — 配置網路對象NAT
- 技術支援與檔案 — Cisco Systems