DMZ、内部ネットワーク、外部ネットワークでの SMTP メール サーバ アクセス用の ASA を設定する

内容

概要

このドキュメントでは、緩衝地帯（DMZ）、内部ネットワーク、または外部ネットワークに配置された Simple Mail Transfer Protocol（SMTP）サーバへのアクセスを Cisco 適応型セキュリティアプライアンス（ASA）で設定する方法を説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 9.1 以降を実行する Cisco ASA
- Cisco IOS®ソフトウェアリリース15.1(4)M6が稼働するCisco 2800Cシリーズルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

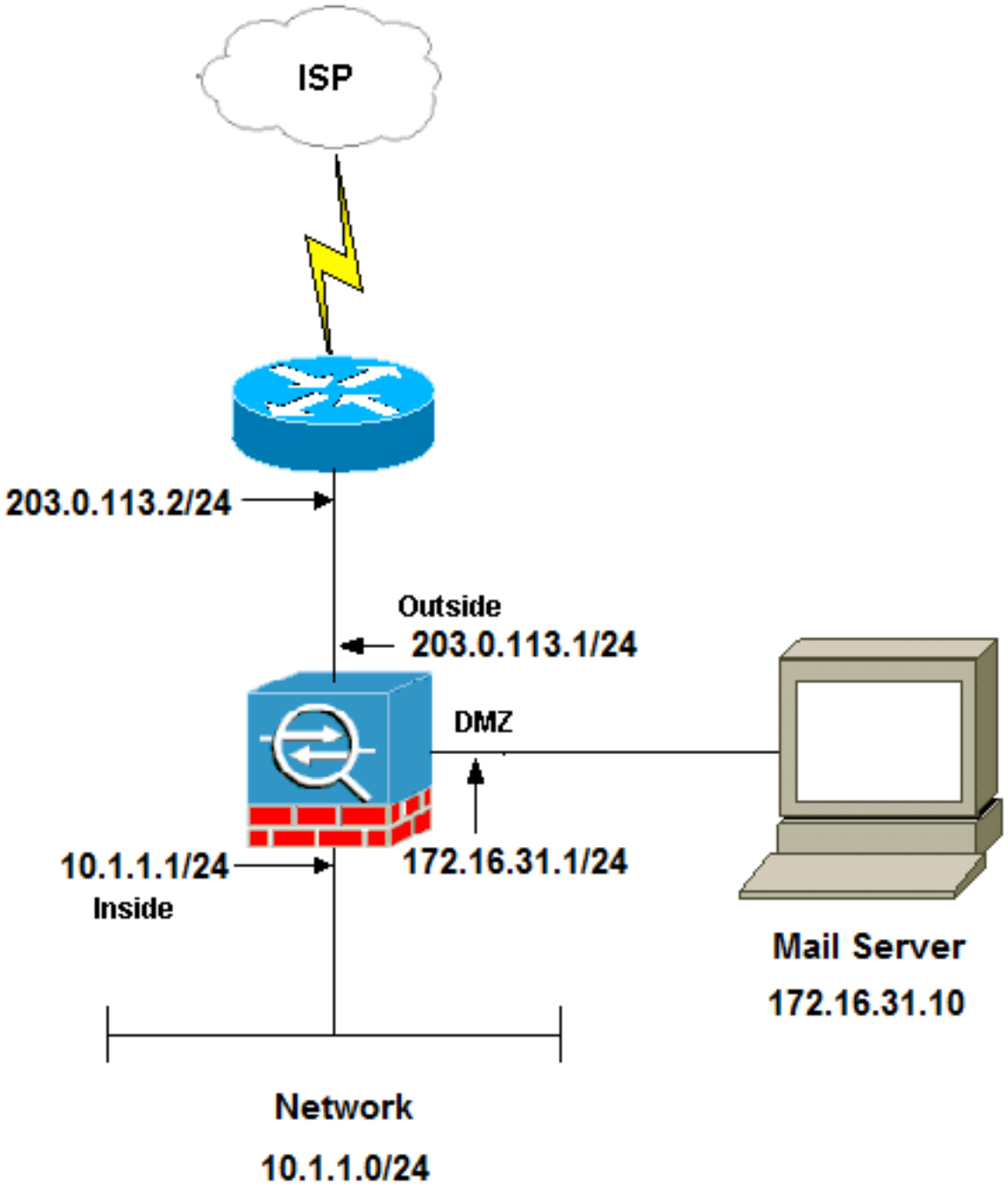
このセクションでは、DMZネットワーク、内部ネットワーク、または外部ネットワークのメールサーバに到達するようにASAを設定する方法について説明します。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

DMZネットワークのメールサーバ

ネットワーク図

このセクションで説明する設定では、次のネットワーク設定を使用します。



注：このドキュメントで使用されているIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 で使用されているアドレ

スであり、ラボ環境で使用されたものです。

この例で使用するネットワーク設定は、内部ネットワークが10.1.1.0/24で、外部ネットワークが203.0.113.0/24であるASAです。IPアドレスが172.16.31.10であるメールサーバはDMZネットワークにあります。内部ネットワークからメールサーバにアクセスするには、IDネットワークアドレス変換(NAT)を設定する必要があります。

外部ユーザがメールサーバにアクセスするには、スタティックNATとアクセスリスト(この例ではoutside_int)を設定して、外部ユーザがメールサーバにアクセスし、アクセスリストを外部インターフェイスにバインドできるようにする必要があります。

ASA の設定

次に、この例のASA設定を示します。

```
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 の設定

Eメール通信にTransport Layer Security(TLS)暗号化を使用する場合、ASAのExtended Simple Mail Transfer Protocol(ESMTP)インスペクション機能（デフォルトで有効）によってパケットがドロップされます。TLSが有効な電子メールを許可するには、次の例に示すようにESMTPインスペクション機能を無効にします。

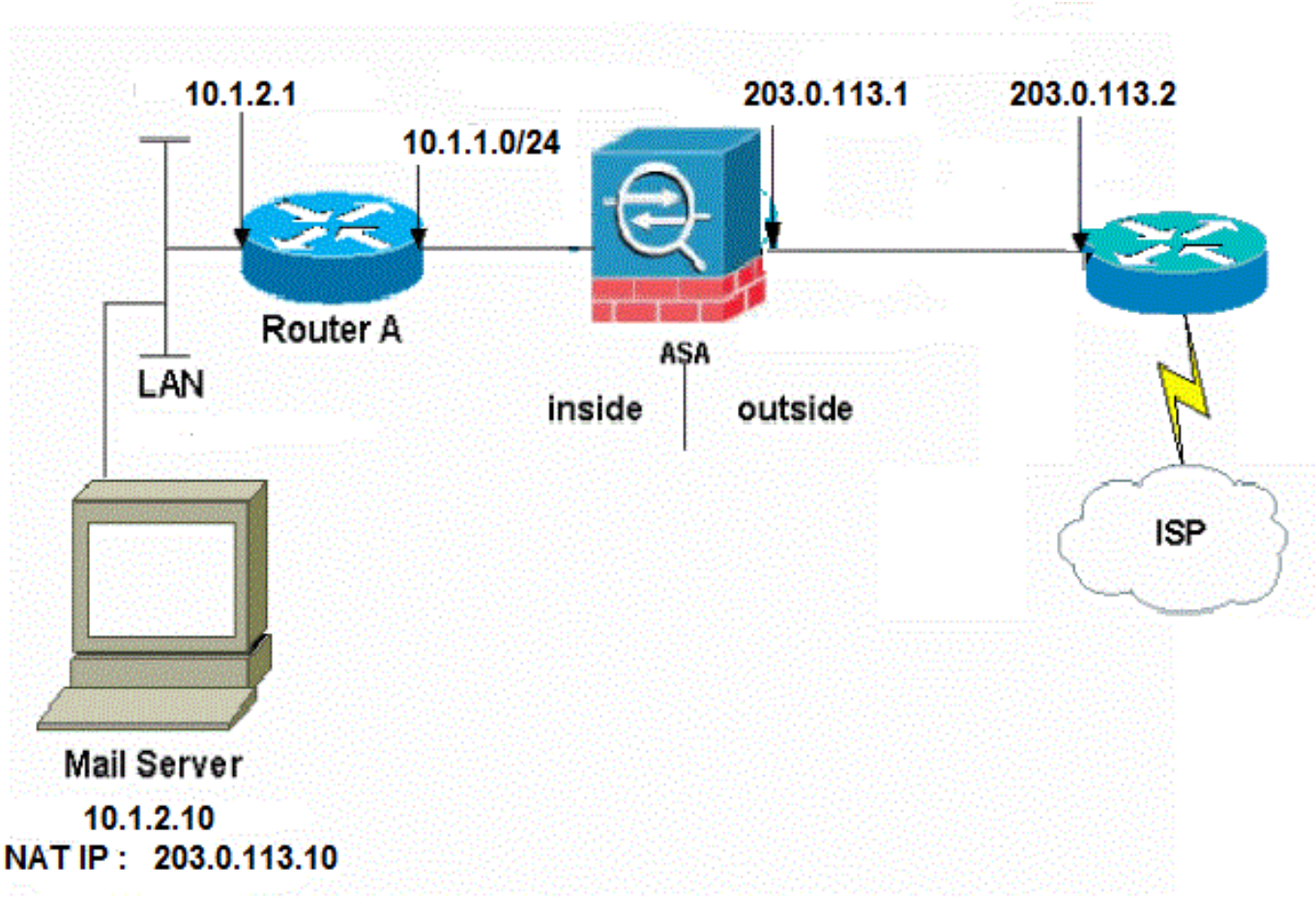
> **注**：詳細については、Cisco Bug ID CSCtn08326（登録ユーザ専用）を参照してください。

```
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
```

内部ネットワークのメールサーバ

ネットワーク図

このセクションで説明する設定では、次のネットワーク設定を使用します。



この例で使用するネットワーク設定は、内部ネットワークが10.1.1.0/24でし、外部ネットワークが203.0.113.0/24であるASAです。IPアドレスが10.1.2.10であるメールサーバは内部ネットワークにあります。

ASA の設定

次に、この例のASA設定を示します。

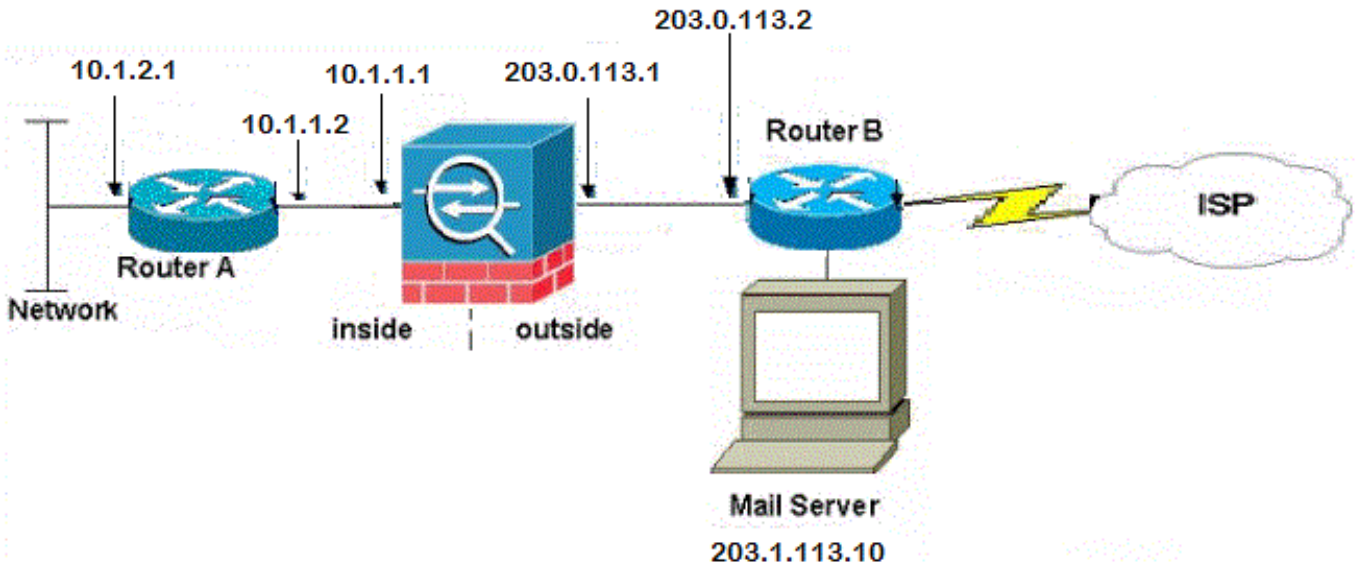
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- 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
```

外部ネットワークのメールサーバ

ネットワーク図

このセクションで説明する設定では、次のネットワーク設定を使用します。



ASA の設定

次に、この例のASA設定を示します。

```
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
```

確認

このセクションに記載されている情報を使用して、設定が適切に機能するか確認します。

DMZネットワークのメールサーバ

TCP ping

TCP pingは、TCP経由の接続をテストします(デフォルトはインターネット制御メッセージプロトコル(ICMP))。TCP pingはSYNパケットを送信し、宛先デバイスがSYN-ACKパケットを送信する場合は、pingが成功したと見なされます。同時に実行できるTCP pingは最大2つです。

以下が一例です。

```
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

ASAはステートフルファイアウォールであり、メールサーバからのリターントラフィックは、ファイアウォール接続テーブルの接続と一致するため、ファイアウォールを経由して戻されます。現在の接続に一致するトラフィックは、インターフェイスのアクセスコントロールリスト(ACL)によってブロックされることなく、ファイアウォールを通過できます。

次の例では、外部インターフェイスのクライアントがDMZインターフェイスの203.0.113.10ホストへの接続を確立します。この接続はTCPプロトコルで行われ、2秒間アイドル状態になっています。接続フラグは、この接続の現在の状態を示します。

```
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

ASA ファイアウォールは正常動作中に syslog を生成します。Syslog の詳細レベルはログ設定に基づきます。次の出力は、レベル6（情報レベル）とレベル7(デバッグレベル)の2つのsyslogを示しています。

```
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)
```

この例の2番目のsyslogは、クライアントとサーバ間のこの特定のトラフィックに対して、ファイアウォールが接続テーブルに接続を構築したことを示しています。この接続試行をブロックするようにファイアウォールが設定された場合や、その他の要因（リソース制約または設定ミスの可能性）によってこの接続の作成が妨げられる場合は、ファイアウォールは接続が確立されたことを示すログを生成しません。その代わりに、接続が拒否される理由、または接続の作成を妨げた要因を示す情報が記録されます。

たとえば、外部のACLがポート25で**172.16.31.10を許可するように設定されていない場合**は、トラフィックが拒否されると次のログが表示されます。

**%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**

これは、次に示すようにACLが見つからないか、誤って設定されている場合に発生します。

```
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 変換（Xlate）

変換が作成されたことを確認するには、Xlate（変換）テーブルを確認します。コマンド**show xlate**は、localキーワードおよび内部ホストのIPアドレスと組み合わせると、そのホストの変換テーブルに存在するすべてのエントリを表示します。次の出力は、DMZと外部インターフェイスの間にこのホスト用に現在作成されている変換があることを示しています。DMZサーバのIPアドレスは、前の設定で203.0.113.10アドレスに変換されます。リストされているフラグ(この**例では**)は、変換がスタティックであることを*示します*。

```
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
```

内部ネットワークのメールサーバ

TCP ping

TCP pingの出力例を次に示します。

```
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

次に接続確認例を示します。

```
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

syslogの例を次に示します。

```
%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 変換 (Xlate)

show nat detailコマンドとshow xlateコマンドの出力例を次に示します。

```
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
```

外部ネットワークのメールサーバ

TCP ping

TCP pingの出力例を次に示します。

```
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

次に接続確認例を示します。

```
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

syslogの例を次に示します。

```
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 変換（Xlate）

show xlateコマンドの出力例を次に示します。

```
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
```

トラブルシュート

ASA は接続をトラブルシュートするための複数のツールを提供しています。設定を確認し、前のセクションで説明した出力を確認しても問題が解決しない場合は、これらのツールとテクニックを使用して接続障害の原因を特定できます。

DMZネットワークのメールサーバ

パケット トレーサ

ASAのパケットトレーサー機能を使用すると、シミュレートされたパケットを指定して、ファイアウォールがトラフィックを処理するときに通過するさまざまな手順、チェック、および機能をすべて表示できます。このツールを使用すると、ファイアウォールの通過を許可する必要があると思われるトラフィックの例を特定し、*その5タプルを使用してトラフィックをシミュレートできます*。次の例では、パケットトレーサを使用して、次の基準を満たす接続試行をシミュレートします。

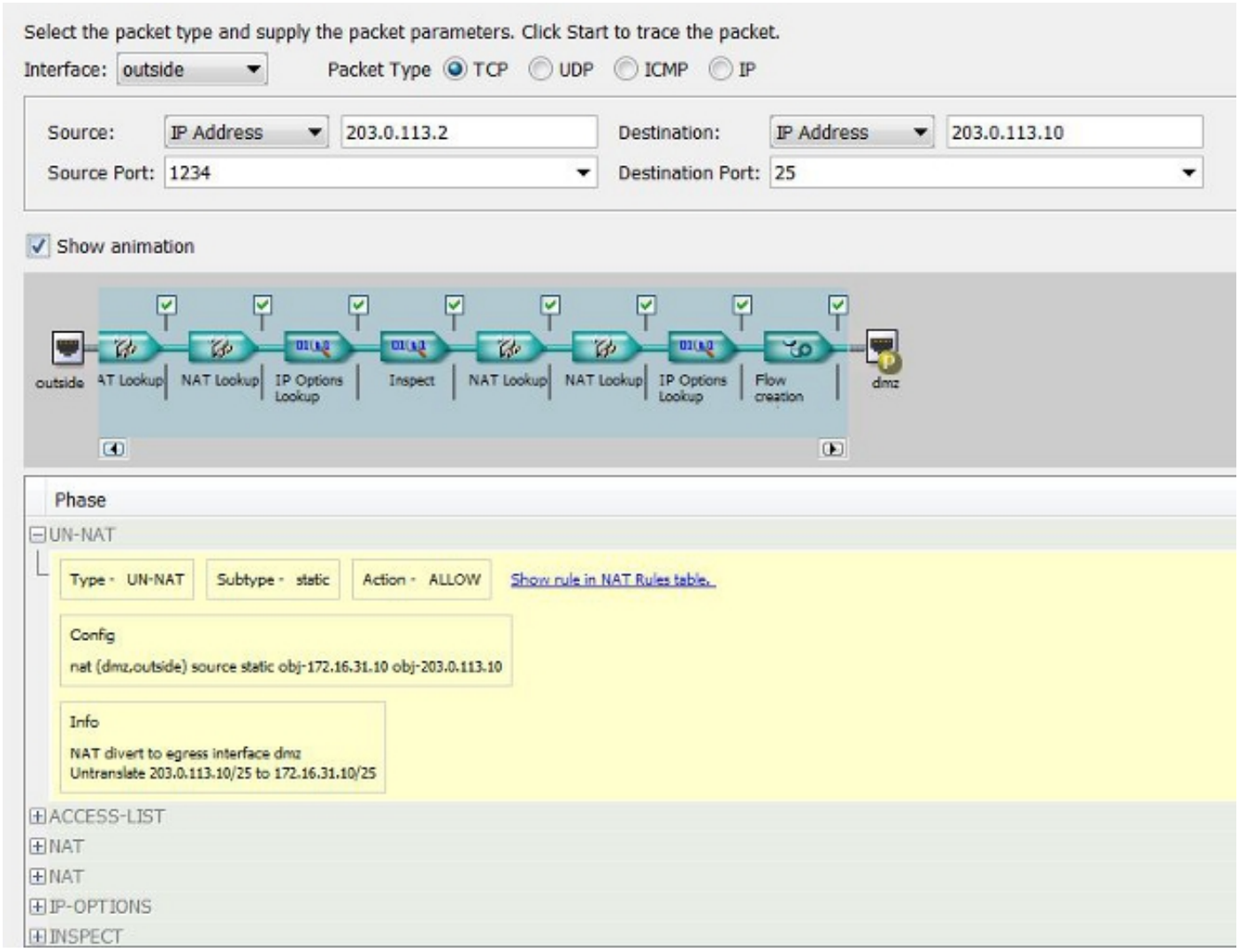
- シミュレートされたパケットが外部に**到着します**。
- 使用されるプロトコルは TCP です。
- シミュレートされたクライアントの IP アドレスが 203.0.113.2 である。
- クライアントは送信元がポート 1234 であるトラフィックを送信します。
- トラフィックは、IP アドレス **203.0.113.10** のサーバ宛てに送信されます。
- トラフィックはポート 25 宛てです。

パケットトレーサの出力例を次に示します。

```
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
```

Cisco Adaptive Security Device Manager(ASDM)の例を次に示します。



上記の出力には、DMZインターフェイスに関する*記述*がないことに注意してください。これはパケット トレーサの設計による動作です。このツールは、ファイアウォールがそのタイプの接続試行をどのように処理するかを示します。これには、ルーティング方法とどのインターフェイスからの接続試行を含まれます。

ヒント：パケットトレーサ機能の詳細については、CLI、8.4および8.6を使用した『*Cisco ASA 5500シリーズ設定ガイド*』の「*パケットトレーサを使用したパケットのトレース*」セクションを参照してください。

パケット キャプチャ

ASA ファイアウォールでは、インターフェイスに着信または発信するトラフィックをキャプチャできます。このキャプチャ機能は、トラフィックがファイアウォールに到達したか、ファイアウォールから送出されたかを確実に証明できるため、非常に便利です。次の例は、DMZおよび外部インターフェイス上の**capd**と**capout**という2つのキャプチャの設定を示しています。captureコマンドでは、matchキーワードを使用して、キャプチャするトラフィックを特定できます。

この例の**capture capd**では、TCPホスト172.16.31.10/host 203.0.113.2に一致するDMZインターフェイス（入力または出力）で表示されるトラフィックを照合することが示されています。つまり、ホスト172.16.31.10からホスト203.0.113.2（またはその逆）に送信されるTCPトラフィックをキャプチャします。match キーワードを使用することで、ファイアウォールでトラフィックを双方向でキャプチャできます。外部インターフェイスに定義されているcaptureコマンドは、ファイアウォールがそのメールサーバのIPアドレスにNATを実行するため、内部メールサーバのIPアドレスを参照しません。その結果、サーバのIPアドレスと一致できません。代わりに、次の例では、すべての可能なIPアドレスがその条件に一致することを示すために**any**という単語を使用しています。

キャプチャを設定した後、接続を再度確立し、**show capture <capture_name>コマンドでキャプチャの表示に進みます**。この例では、キャプチャに示されているTCP 3ウェイハンドシェイクによって明らかなように、外部ホストがメールサーバに接続できることがわかります。

```
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
```

内部ネットワークのメールサーバ

パケット トレーサ

パケットトレーサの出力例を次に示します。

```
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
```

外部ネットワークのメールサーバ

パケット トレーサ

パケットトレーサの出力例を次に示します。

```
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
```

関連情報

- Cisco ASA シリーズ Syslog メッセージ
- CLI および ASDM を使用した ASA パケット キャプチャの設定例
- Cisco ASAシリーズCLIコンフィギュレーションガイド9.0：ネットワークオブジェクトNATの設定
- テクニカルサポートとドキュメント - Cisco Systems