DMZ, 내부 및 외부 네트워크에서 SMTP 메일 서버 액세스를 위한 ASA 구성

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
표기 규칙
구성
DMZ 네트워크의 메일 서버
네트워크 다이어그램
ASA 컨피그레이션
ESMTP TLS 컨피그레이션
내부 네트워크의 메일 서버
네트워크 다이어그램
ASA 컨피그레이션
외부 네트워크의 메일 서버
네트워크 다이어그램
ASA 컨피그레이션
다음을 확인합니다.
DMZ 네트워크의 메일 서버
TCP Ping
연결
로깅
NAT 변환(Xlate)
내부 네트워크의 메일 서버
TCP Ping
연결
로깅
NAT 변환(Xlate)
외부 네트워크의 메일 서버
TCP Ping
연결
로깅
NAT 변환(Xlate)
문제 해결
DMZ 네트워크의 메일 서버
패킷 추적기
패킷 캡처

내부 네트워크의 메일 서버
패킷 추적기
외부 네트워크의 메일 서버
패킷 추적기
관련 정보

소개

이 문서에서는 DMZ(Demilitarized Zone), 내부 네트워크 또는 외부 네트워크에 있는 SMTP(Simple Mail Transfer Protocol) 서버에 액세스하기 위해 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.1 이상을 실행하는 Cisco ASA
- Cisco 2800C Series Router with Cisco IOS® Software 릴리스 15.1(4)M6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

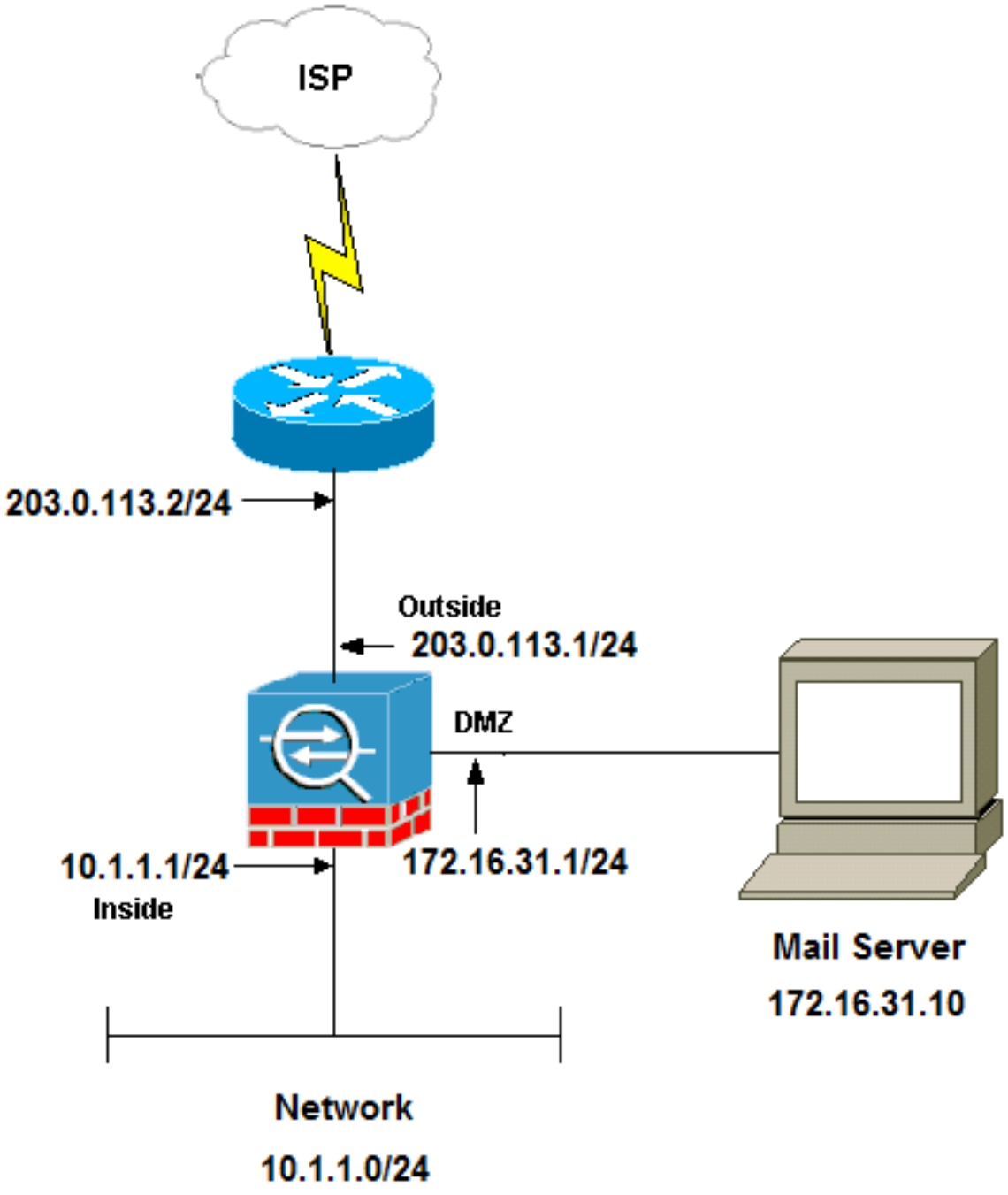
이 섹션에서는 DMZ 네트워크, 내부 네트워크 또는 외부 네트워크의 메일 서버에 연결하기 위해 ASA를 구성하는 방법에 대해 설명합니다.

> **참고:**Command Lookup Tool(등록된 고객만 해당)을 사용하여 이 섹션에서 사용되는 명령에 대한 자세한 정보를 얻을 수 있습니다.

DMZ 네트워크의 메일 서버

네트워크 다이어그램

이 섹션에서 설명하는 컨피그레이션에서는 다음 네트워크 설정을 사용합니다.



참고:이 문서에서 사용되는 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 사용되는 네트워크 설정에는 내부 네트워크가 **10.1.1.0/24**인 ASA와 **203.0.113.0/24**의 외부 네트워크가 있습니다. IP 주소가 **172.16.31.10인** 메일 서버는 DMZ 네트워크에 있습니다.내부 네트워크에서 메일 서버에 액세스하려면 ID NAT(Network Address Translation)를 구성해야 합니다.

외부 사용자가 메일 서버에 액세스하려면 외부 사용자가 메일 서버에 액세스하고 액세스 목록을 외부 인터페이스에 바인딩하도록 허용하려면 이 예에서 **outside_int**인 고정 NAT 및 액세스 목록을 구성해야 합니다.

ASA 컨피그레이션

다음은 이 예제의 ASA 컨피그레이션입니다.

```
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 컨피그레이션

이메일 통신에 TLS(Transport Layer Security) 암호화를 사용하는 경우 ASA에서 기본적으로 활성화된 ESMTP(Extended Simple Mail Transfer Protocol) 검사 기능이 패킷을 삭제합니다.TLS가 활성화된 이메일을 허용하려면 다음 예와 같이 ESMTP 검사 기능을 비활성화합니다.

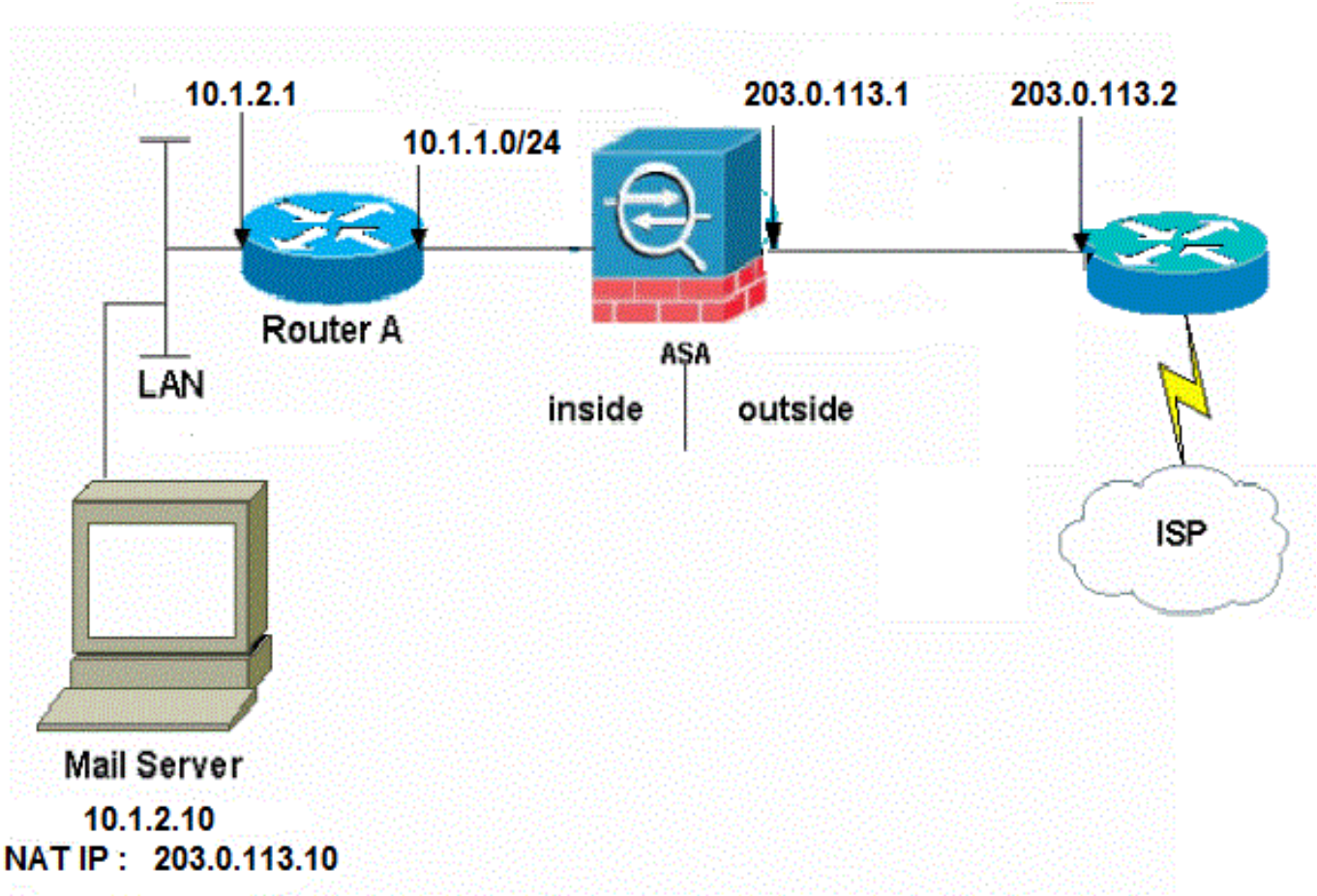
참고:자세한 내용은 Cisco 버그 ID CSCtn08326(등록된 고객만 해당)을 참조하십시오.

```
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
```

내부 네트워크의 메일 서버

네트워크 다이어그램

이 섹션에서 설명하는 컨피그레이션에서는 다음 네트워크 설정을 사용합니다.



이 예에서 사용되는 네트워크 설정에는 내부 네트워크가 **10.1.1.0/24**인 ASA와 **203.0.113.0/24**의 외부 네트워크가 있습니다. IP 주소가 **10.1.2.10인** 메일 서버는 내부 네트워크에 있습니다.

ASA 컨피그레이션

다음은 이 예제의 ASA 컨피그레이션입니다.

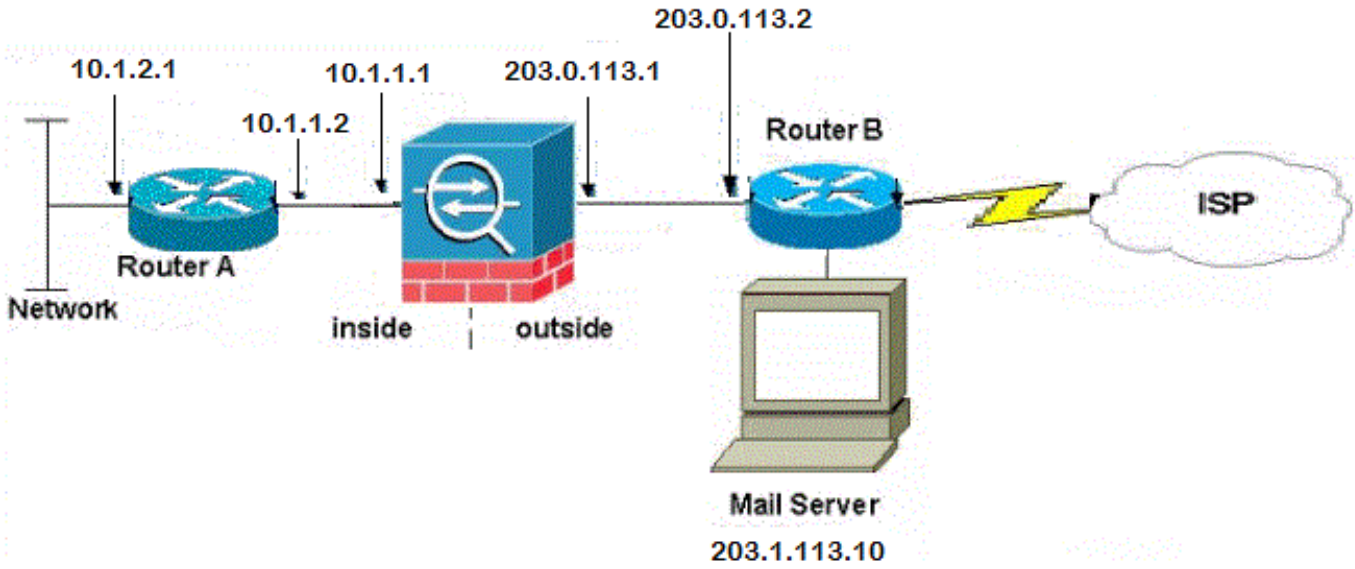
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- 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
```

외부 네트워크의 메일 서버

네트워크 다이어그램

이 섹션에서 설명하는 컨피그레이션에서는 다음 네트워크 설정을 사용합니다.



ASA 컨피그레이션

다음은 이 예제의 ASA 컨피그레이션입니다.

```
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
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 제공된 정보를 사용하십시오.

DMZ 네트워크의 메일 서버

TCP Ping

TCP ping은 TCP를 통한 연결을 테스트합니다(기본값은 ICMP(Internet Control Message Protocol)).TCP ping은 SYN 패킷을 전송하고 대상 디바이스가 SYN-ACK 패킷을 전송하는 경우 ping을 성공한 것으로 간주합니다.한 번에 최대 두 개의 동시 TCP ping을 실행할 수 있습니다.

예를 들면 다음과 같습니다.

```
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
```

연결

ASA는 스테이트풀 방화벽이며, 방화벽 연결 테이블의 연결과 일치하므로 메일 서버의 반환 트래픽이 방화벽을 통해 다시 허용됩니다.현재 연결과 일치하는 트래픽은 인터페이스 ACL(Access Control List)에 의해 차단되지 않고 방화벽을 통해 허용됩니다.

다음 예에서는 외부 인터페이스의 클라이언트가 DMZ 인터페이스의 203.0.113.10 호스트에 대한 연결을 설정합니다.이 연결은 TCP 프로토콜로 이루어지며 2초 동안 유휴 상태가 되었습니다.연결 플래그는 이 연결의 현재 상태를 나타냅니다.

```
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
```

로깅

ASA 방화벽은 정상 작동 중에 syslog를 생성합니다.syslogs는 로깅 컨피그레이션을 기반으로 자세한 범위를 제공합니다.이 출력은 레벨 6(*정보* 레벨) 및 레벨 7(*디버깅* 레벨)에 나타나는 두 개의 syslog를 보여줍니다.

```
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)
```

이 예에서 두 번째 syslog는 방화벽이 클라이언트와 서버 간의 이 특정 트래픽에 대한 연결 테이블에 연결을 구축했음을 나타냅니다.이 연결 시도를 차단하도록 방화벽이 구성되었거나 이 연결의 생성을 방해하는 다른 요인(리소스 제약 조건 또는 컨피그레이션 오류 가능성)이 있는 경우 방화벽은 연결이 구축되었음을 나타내는 로그를 생성하지 않습니다.대신 연결이 거부되는 이유 또는 연결을 만드는 것을 방해하는 요소에 대한 표시를 기록합니다.

예를 들어, 외부의 ACL이 포트 25에서 **172.16.31.10을 허용하도록** 구성되지 않은 경우 트래픽이 거부될 때 이 로그를 볼 수 있습니다.

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

이는 ACL이 누락되었거나 여기에 표시된 대로 잘못 구성된 경우에 발생합니다.

```
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 변환(Xlate)

번역이 생성되었는지 확인하기 위해 Xlate (translation) 테이블을 확인할 수 있습니다.명령 **show xlate**는 local 키워드 및 내부 호스트 IP 주소와 결합되면 해당 호스트의 변환 테이블에 있는 모든 항목을 표시합니다.다음 출력에서는 DMZ와 외부 인터페이스 간에 이 호스트에 대해 현재 구축된 변환이 있음을 보여줍니다.DMZ 서버 IP 주소는 이전 컨피그레이션에 따라 203.0.113.10 주소로 변환됩니다.나열된 플래그(이 예에서)는 변환이 *정적임을* 나타냅니다.

```
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
```

내부 네트워크의 메일 서버

TCP Ping

다음은 TCP ping 출력의 예입니다.

```
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
```

연결

연결 확인 예는 다음과 같습니다.

```
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
```

로깅

다음은 syslog의 예입니다.

```
%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 변환(Xlate)

다음은 show nat detail 및 show xlate 명령 출력의 몇 가지 예입니다.

```
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
```

외부 네트워크의 메일 서버

TCP Ping

다음은 TCP ping 출력의 예입니다.

```
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
```

연결

연결 확인 예는 다음과 같습니다.

```
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
```

로깅

다음은 syslog의 예입니다.

```
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 변환(Xlate)

다음은 show xlate 명령 출력**의** 예입니다.

```
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
```

문제 해결

ASA는 연결 문제를 해결할 수 있는 여러 툴을 제공합니다.컨피그레이션을 확인하고 이전 섹션에서 설명한 출력을 확인한 후에도 문제가 계속되면 이러한 툴 및 기술을 통해 연결 오류의 원인을 확인할 수 있습니다.

DMZ 네트워크의 메일 서버

패킷 추적기

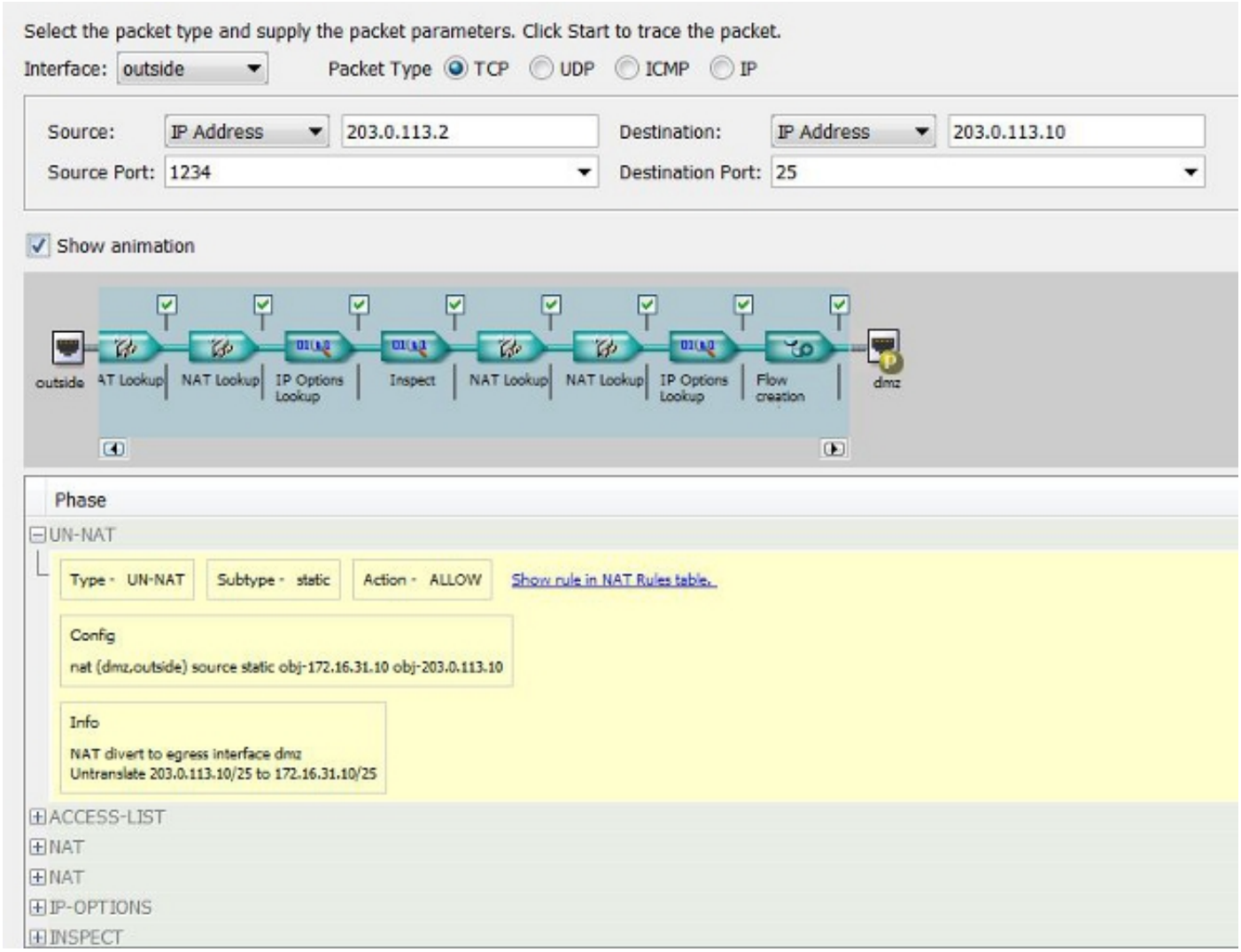
ASA의 패킷 추적기 **기능**을 사용하면 *시뮬레이션된* 패킷을 지정하고, 방화벽이 트래픽을 처리할 때 수행하는 다양한 단계, 검사 및 기능을 모두 볼 수 있습니다.이 툴을 사용하면 방화벽을 통과하도록 허용되어야 *한다고* 생각하는 트래픽의 예를 식별하고 트래픽을 시뮬레이션하기 위해 이 5튜플을 사용하는 것이 좋습니다.다음 예에서는 다음 조건을 충족하는 연결 시도를 시뮬레이션하기 위해 패킷 추적기를 사용합니다.

- 시뮬레이션된 패킷이 **외부**에 **도착합니다**.
- 사용되는 프로토콜은 **TCP**입니다.
- 시뮬레이션된 클라이언트 IP 주소는 **203.0.113.2입니다**.
- 클라이언트는 포트 **1234**에서 소싱된 트래픽을 **전송합니다**.
- 트래픽은 IP 주소 **203.0.113.10의** 서버로 **이동됩니다**.
- 트래픽은 포트 **25**로 이동됩니다.

다음은 패킷 추적기 출력의 예입니다.

```
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
```

다음은 Cisco ASDM(Adaptive Security Device Manager)의 예입니다.



이전 출력에 *DMZ* 인터페이스에 대한 언급이 없습니다.이는 패킷 추적기 설계에 의한 것입니다.이 툴은 방화벽이 어떤 인터페이스에서 어떤 인터페이스를 라우팅할지 포함하여 어떤 유형의 연결 시도를 처리하는지 알려줍니다.

> **팁:**패킷 추적기 기능에 대한 자세한 내용은 *CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드*의 Tracing Packets with Packet Tracer 섹션을 참조하십시오.

패킷 캡처

ASA 방화벽은 인터페이스를 드나드는 트래픽을 캡처할 수 있습니다.이 캡처 기능은 트래픽이 방화벽에 도달하는지 또는 방화벽에서 출발하는지 여부를 명확히 확인할 수 있으므로 매우 유용합니다.다음 예에서는 각각 DMZ 및 외부 인터페이스**에서 capd** 및 capout이라는 두 캡처의 컨피그레이션을 보여줍니다.capture 명령은 캡처할 트래픽에 대해 구체적으로 지정할 수 있는 match 키워드를 사용합니다.

이 예에서 **capture capd**의 경우 TCP 호스트 172.16.31.10/host 203.0.113.2과 일치하는 DMZ 인터페이스(인그레스 또는 이그레스)에 표시된 트래픽을 매칭할 것임을 나타냅니다. 즉, 호스트 172.16.31.10에서 호스트 203.0.113.2으로 또는 그 반대로 전송되는 모든 TCP 트래픽을 캡처할 수 있습니다.match 키워드를 사용하면 방화벽에서 해당 트래픽을 양방향으로 캡처할 수 있습니다.외부 인터페이스에 대해 정의된 capture 명령은 내부 메일 서버 IP 주소를 참조하지 않습니다. 방화벽이 해당 메일 서버 IP 주소에 대해 NAT를 수행하기 때문입니다.따라서 해당 서버 IP 주소와 일치시킬 수 없습니다.대신 다음 예에서는 **any**라는 단어를 사용하여 가능한 모든 IP 주소가 해당 조건과

일치함을 나타냅니다.

캡처를 구성한 후 다시 연결을 설정하고 show capture **<capture_name>** 명령을 사용하여 캡처를 **계속** 확인해야 합니다.이 예에서는 외부 호스트가 다음 캡처에서 볼 수 있는 TCP 3-way 핸드셰이크에 의해 분명하게 인식되어 메일 서버에 연결할 수 있음을 확인할 수 있습니다.

```
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
```

내부 네트워크의 메일 서버

패킷 추적기

다음은 패킷 추적기 출력의 예입니다.

```
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
```

외부 네트워크의 메일 서버

패킷 추적기

다음은 패킷 추적기 출력의 예입니다.

```
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
```

관련 정보

- Cisco ASA Series Syslog 메시지
- CLI 및 ASDM을 사용한 ASA 패킷 캡처 컨피그레이션 예
- Cisco ASA Series CLI 컨피그레이션 가이드, 9.0 - 네트워크 개체 NAT 구성
- 기술 지원 및 문서 - Cisco Systems