Konfigurieren der ASA für den SMTP Mail Server-Zugriff in der DMZ, im Inside und im Außenbereich

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Cisco Adaptive Security Appliance (ASA) für den Zugriff auf einen SMTP-Server (Simple Mail Transfer Protocol) konfigurieren, der sich in der Demilitarized Zone (DMZ), im internen Netzwerk oder im externen Netzwerk befindet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA mit Softwareversion 9.1 oder höher
- Cisco Router der Serie 2800C mit Cisco IOS® Softwareversion 15.1(4)M6

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

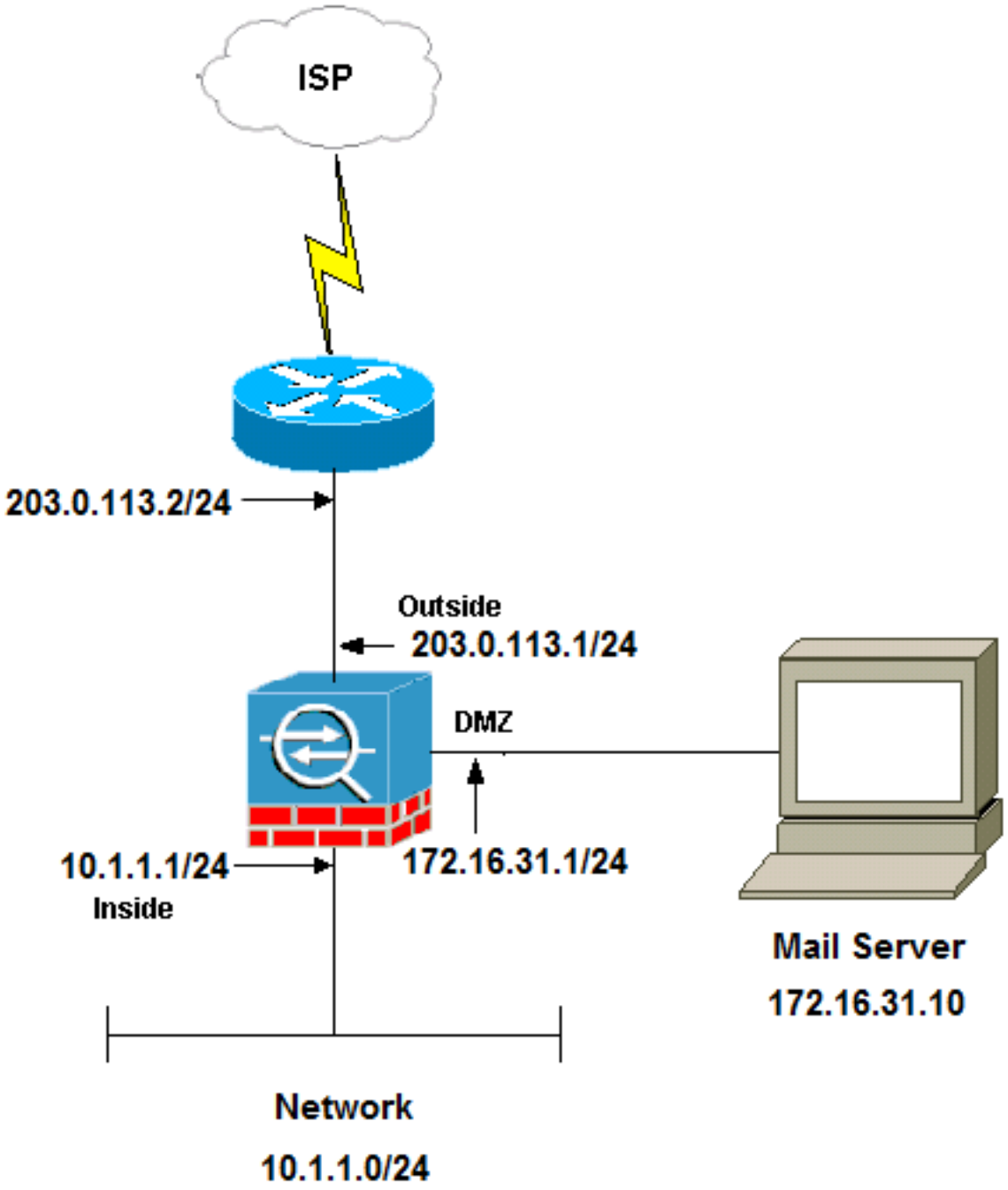
In diesem Abschnitt wird beschrieben, wie die ASA so konfiguriert wird, dass sie den Mailserver im DMZ-Netzwerk, im internen Netzwerk oder im externen Netzwerk erreicht.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen über die Befehle zu erhalten, die in diesem Abschnitt verwendet werden.

Mailserver im DMZ-Netzwerk

Netzwerkdiagramm

Die in diesem Abschnitt beschriebene Konfiguration verwendet die folgende Netzwerkeinrichtung:



Hinweis: Die in diesem Dokument verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet

wurden.

Die in diesem Beispiel verwendete Netzwerkeinrichtung hat die ASA mit einem internen Netzwerk unter **10.1.1.0/24** und einem externen Netzwerk unter **203.0.113.0/24**. Der Mailserver mit der IP-Adresse **172.16.31.10** befindet sich im DMZ-Netzwerk. Damit auf den Mail-Server im Netzwerk zugegriffen werden kann, müssen Sie die Identity Network Address Translation (NAT) konfigurieren.

Damit die externen Benutzer auf den Mailserver zugreifen können, müssen Sie eine statische NAT und eine Zugriffsliste konfigurieren, die in diesem Beispiel **außerhalb_int** ist, damit die externen Benutzer auf den Mailserver zugreifen und die Zugriffsliste an die externe Schnittstelle binden können.

ASA-Konfiguration

Dies ist die ASA-Konfiguration für dieses Beispiel:

```
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-Konfiguration

Wenn Sie die Transport Layer Security (TLS)-Verschlüsselung für die E-Mail-Kommunikation verwenden, werden die Pakete durch die ESMTP-Überprüfungsfunktion (standardmäßig aktiviert) in der ASA verworfen. Um E-Mails mit aktiviertem TLS zuzulassen, deaktivieren Sie die ESMTP-Überprüfungsfunktion, wie im nächsten Beispiel gezeigt.

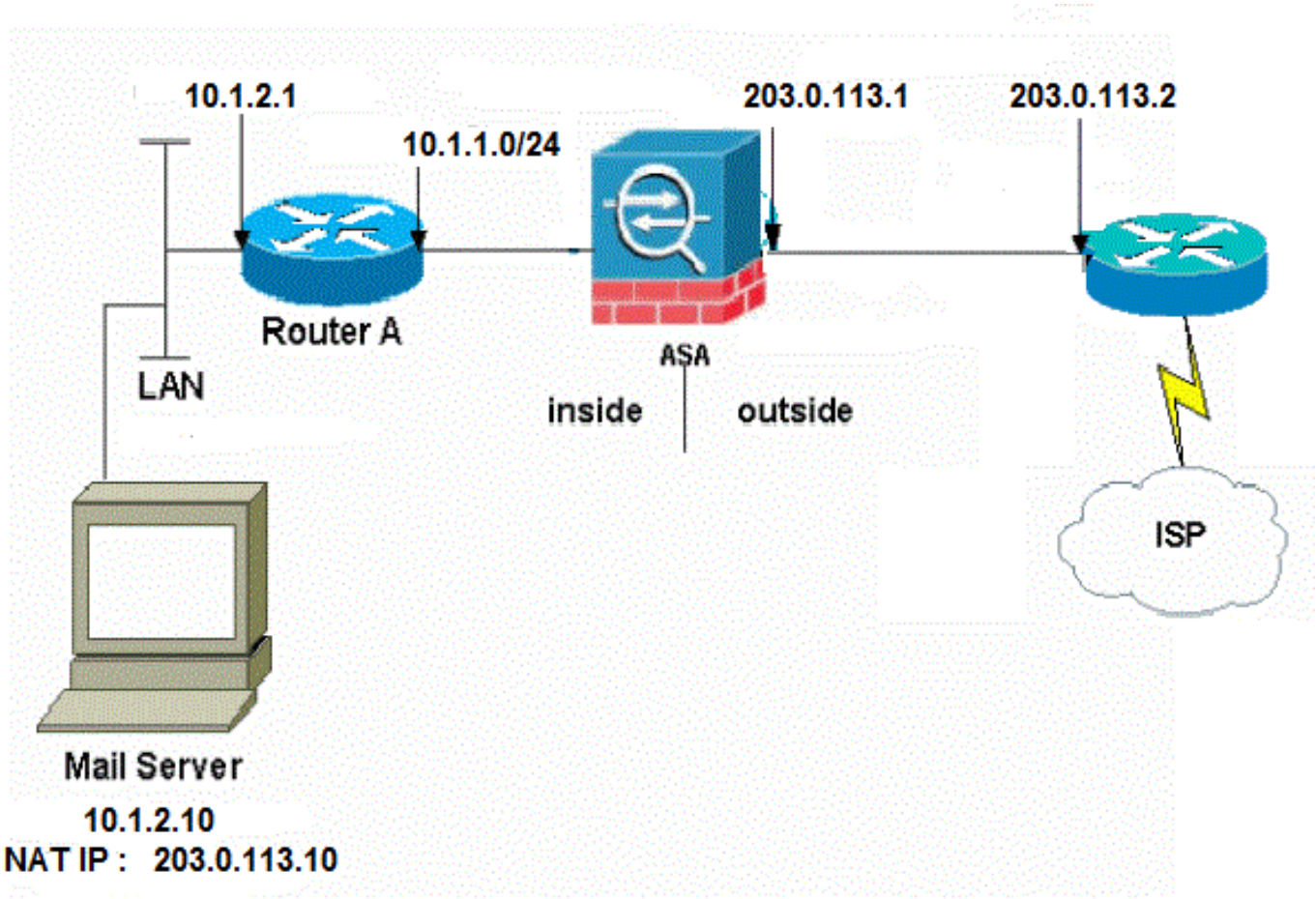
> **Hinweis**: Weitere Informationen finden Sie unter Cisco Bug ID CSCtn08326 (nur registrierte Kunden).

```
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
```

Mailserver im internen Netzwerk

Netzwerkdiagramm

Die in diesem Abschnitt beschriebene Konfiguration verwendet die folgende Netzwerkeinrichtung:



Die in diesem Beispiel verwendete Netzwerkeinrichtung hat die ASA mit einem internen Netzwerk unter **10.1.1.0/24** und einem externen Netzwerk unter **203.0.113.0/24**. Der Mailserver mit der IP-Adresse **10.1.2.10** befindet sich im internen Netzwerk.

ASA-Konfiguration

Dies ist die ASA-Konfiguration für dieses Beispiel:

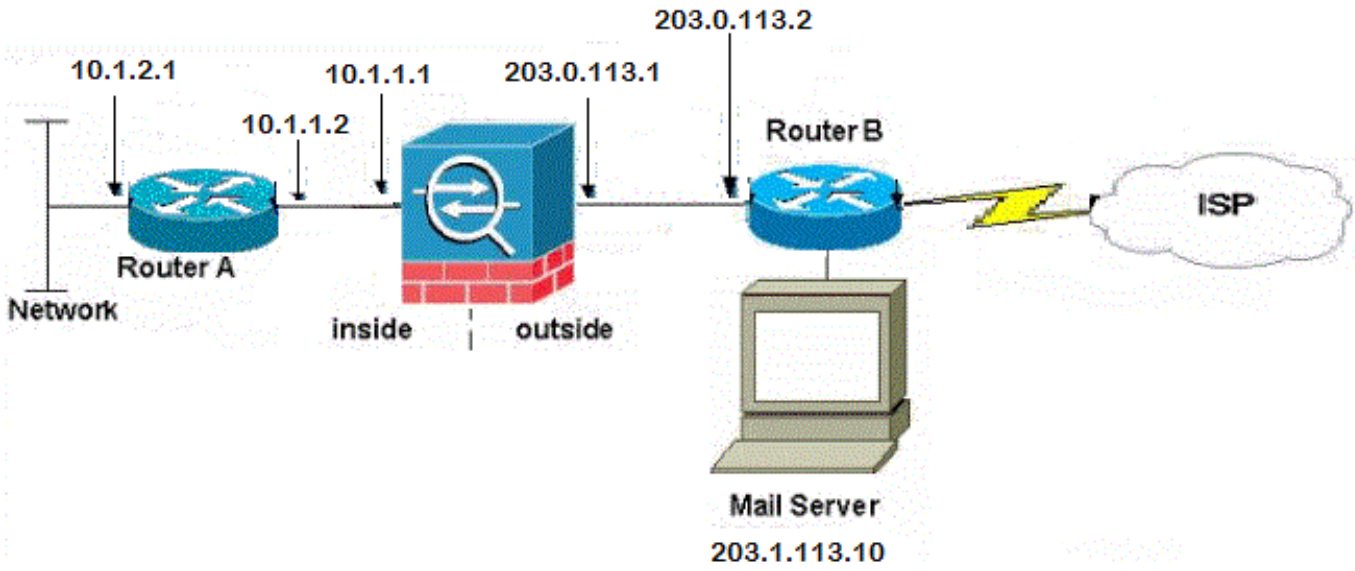
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- 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
```

Mailserver im externen Netzwerk

Netzwerkdiagramm

Die in diesem Abschnitt beschriebene Konfiguration verwendet die folgende Netzwerkeinrichtung:



ASA-Konfiguration

Dies ist die ASA-Konfiguration für dieses Beispiel:

```
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
```

Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Mailserver im DMZ-Netzwerk

TCP-Ping

Der TCP-Ping testet eine Verbindung über TCP (der Standardwert ist "Internet Control Message Protocol (ICMP)"). Ein TCP-Ping sendet SYN-Pakete und betrachtet den Ping als erfolgreich, wenn das Zielgerät ein SYN-ACK-Paket sendet. Sie können maximal zwei gleichzeitige TCP-Pings gleichzeitig ausführen.

Hier ein Beispiel:

```
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
```

Verbindung

Die ASA ist eine Stateful Firewall, und der Rückverkehr vom Mail-Server wird durch die Firewall zugelassen, da er mit einer Verbindung in der Firewall-Verbindungstabelle übereinstimmt. Der Datenverkehr, der mit einer aktuellen Verbindung übereinstimmt, wird über die Firewall zugelassen, ohne von einer Zugriffskontrollliste (ACL) für die Schnittstelle blockiert zu werden.

Im nächsten Beispiel stellt der Client an der externen Schnittstelle eine Verbindung zum 203.0.113.10-Host der DMZ-Schnittstelle her. Diese Verbindung wird mit dem TCP-Protokoll hergestellt und ist seit zwei Sekunden inaktiv. Die Verbindungsflags zeigen den aktuellen Status

dieser Verbindung an:

```
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
```

Protokollierung

Die ASA-Firewall erzeugt im Normalbetrieb Syslogs. Die Syslogs sind abhängig von der Protokollierungskonfiguration ausführlich dargestellt. Diese Ausgabe zeigt zwei Syslogs, die auf Ebene 6 (*Informationsstufe*) und auf Ebene 7 (*Debugging*-Ebene) angezeigt werden:

```
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)
```

Das zweite Syslog in diesem Beispiel zeigt an, dass die Firewall eine Verbindung in ihrer Verbindungstabelle für diesen spezifischen Datenverkehr zwischen Client und Server erstellt hat. Wenn die Firewall so konfiguriert wurde, dass dieser Verbindungsversuch blockiert wird, oder ein anderer Faktor die Herstellung dieser Verbindung behinderte (Ressourcenbeschränkungen oder eine mögliche Fehlkonfiguration), würde die Firewall kein Protokoll generieren, das angibt, dass die Verbindung hergestellt wurde. Stattdessen wird ein Grund für die Ablehnung der Verbindung oder ein Hinweis auf den Faktor protokolliert, der die Herstellung der Verbindung verhindert.

Wenn beispielsweise die externe Zugriffskontrollliste nicht so konfiguriert ist, dass sie **172.16.31.10** auf Port 25 zulässt, wird dieses Protokoll angezeigt, wenn der Datenverkehr abgelehnt wird:

%ASA-4-106100: access-list outside_int verweigerte tcp außerhalb/203.0.113.2(3756) -> dmz/172.16.31.10(25) Hit-Cnt-Intervall von 5 300 Sekunden

Dies tritt auf, wenn eine ACL fehlt oder falsch konfiguriert wurde, wie hier gezeigt:

```
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-Übersetzungen (Xlate)

Um zu bestätigen, dass die Übersetzungen erstellt wurden, können Sie die Tabelle Xlate (Übersetzung) überprüfen. Der Befehl **show xlate** zeigt in Kombination mit dem lokalen Schlüsselwort und der internen Host-IP-Adresse alle Einträge, die in der Übersetzungstabelle für diesen Host enthalten sind. Die nächste Ausgabe zeigt, dass für diesen Host derzeit eine Übersetzung zwischen der DMZ und den externen Schnittstellen erstellt wird. Die IP-Adresse des DMZ-Servers wird pro vorheriger Konfiguration in die Adresse 203.0.113.10 übersetzt. Die aufgelisteten Flags (**s** in diesem Beispiel) zeigen an, dass die Übersetzung *statisch* ist.

```
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
```

Mailserver im internen Netzwerk

TCP-Ping

Hier ein Beispiel für eine TCP-Ping-Ausgabe:

```
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
```

Verbindung

Hier ein Beispiel für die Verbindungsüberprüfung:

```
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
```

Protokollierung

Hier ein Beispiel für ein 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-Übersetzungen (Xlate)

Im Folgenden finden Sie einige Beispiele, **die detailgenaue Details anzeigen** und Befehlsausgaben **für Xlate** anzeigen:

```
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
```

Mailserver im externen Netzwerk

TCP-Ping

Hier ein Beispiel für eine TCP-Ping-Ausgabe:

```
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
```

Verbindung

Hier ein Beispiel für die Verbindungsüberprüfung:

```
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
```

Protokollierung

Hier ein Beispiel für ein Syslog:

```
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-Übersetzungen (Xlate)

Hier ein Beispiel für die Ausgabe des Befehls "show xlate":

```
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
```

Fehlerbehebung

Die ASA bietet mehrere Tools zur Behebung von Verbindungsproblemen. Wenn das Problem weiterhin besteht, nachdem Sie die Konfiguration überprüft und die im vorherigen Abschnitt beschriebenen Ausgaben überprüft haben, können Ihnen diese Tools und Techniken dabei helfen, die Ursache für den Verbindungsfehler zu ermitteln.

Mailserver im DMZ-Netzwerk

Packet Tracer

Die Packet Tracer-Funktion auf der ASA ermöglicht Ihnen, ein *simuliertes* Paket anzugeben und alle verschiedenen Schritte, Überprüfungen und Funktionen anzuzeigen, die die Firewall durchläuft, wenn sie Datenverkehr verarbeitet. Mit diesem Tool ist es hilfreich, ein Beispiel für Datenverkehr zu identifizieren, der Ihrer Meinung nach über die Firewall weitergeleitet werden *sollte*, und diesen 5-Tupel zu verwenden, um den Datenverkehr zu simulieren. Im nächsten Beispiel wird der Paket-Tracer verwendet, um einen Verbindungsversuch zu simulieren, der diese Kriterien erfüllt:

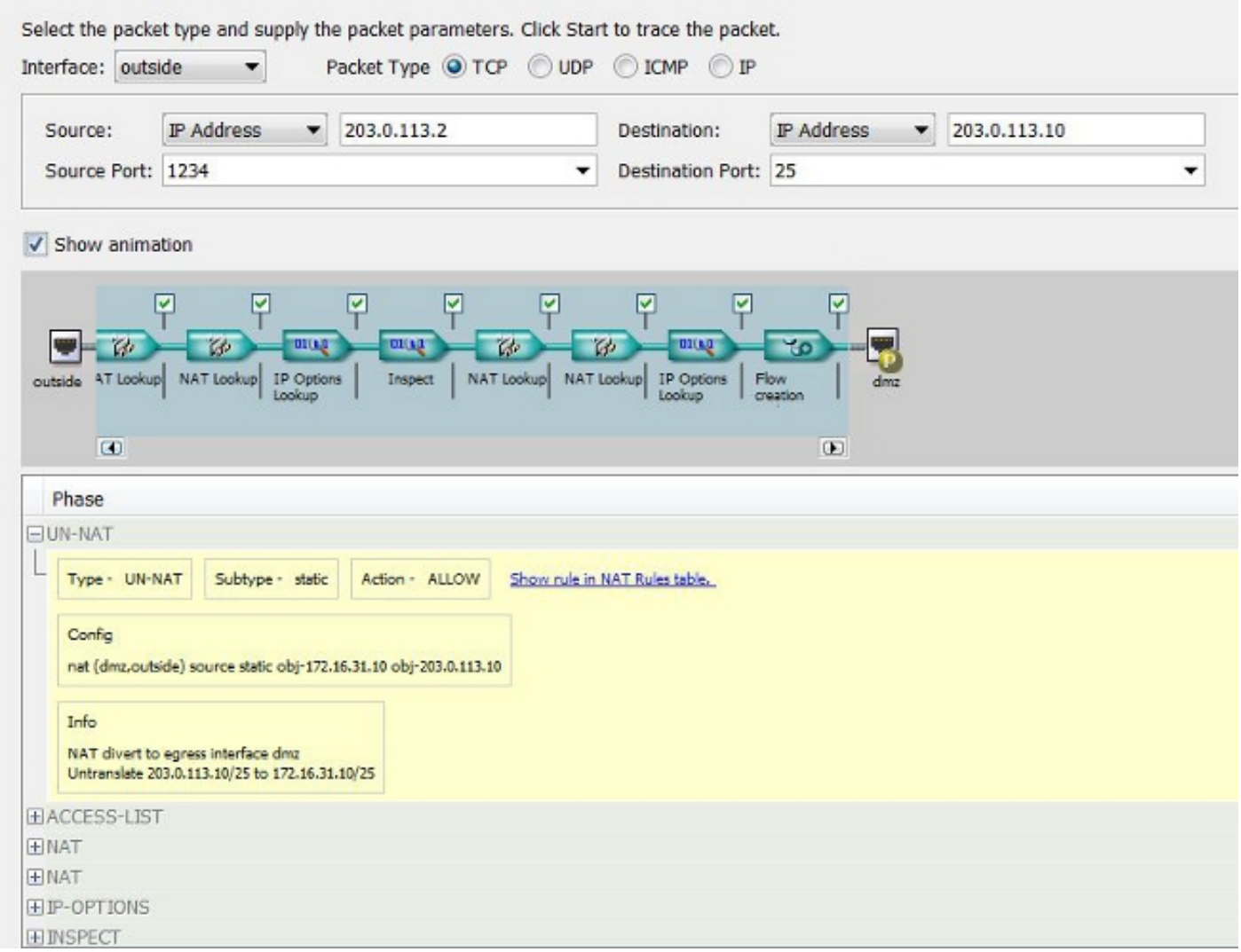
- Das simulierte Paket kommt an der Außenseite an.
- Das verwendete Protokoll ist TCP.

- Die simulierte Client-IP-Adresse lautet **203.0.113.2**.
- Der Client sendet Datenverkehr, der von Port **1234** stammt.
- Der Datenverkehr ist für einen Server mit der IP-Adresse **203.0.113.10** bestimmt.
- Der Datenverkehr ist für Port **25** bestimmt.

Im Folgenden finden Sie ein Beispiel für eine Pakettracer-Ausgabe:

```
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
```

Hier ein Beispiel für den Cisco Adaptive Security Device Manager (ASDM):



Beachten Sie, dass die *DMZ*-Schnittstelle in den vorherigen Ausgaben nicht erwähnt wird. Dies erfolgt über das Paket-Tracer-Design. Das Tool erklärt Ihnen, wie die Firewall diesen Verbindungsversuch verarbeitet. Dazu gehört auch, wie die Firewall diesen Verbindungsversuch weiterleitet und von welcher Schnittstelle sie entfernt wird.

> **Tipp**: Weitere Informationen über die Paketverfolgungsfunktion finden Sie im Abschnitt Tracing Packets with Packet Tracer (Ablaufverfolgungspakete mit Packet Tracer) im *Konfigurationshandbuch der Cisco Serie ASA 5500 unter Verwendung der CLI, 8.4 und 8.6*.

Paketerfassung

Die ASA Firewall kann Datenverkehr erfassen, der an den Schnittstellen eingeht oder diese verlässt. Diese Erfassungsfunktion ist sehr nützlich, da sie definitiv nachweisen kann, ob der Datenverkehr eine Firewall erreicht oder verlässt. Das nächste Beispiel zeigt die Konfiguration von zwei Captures mit dem Namen **capd** und **capout** auf der DMZ bzw. der externen Schnittstelle. Die Capture-Befehle verwenden ein Match-Schlüsselwort, mit dem Sie den Datenverkehr, den Sie erfassen möchten, genau bestimmen können.

Für den **Capture-Capd** in diesem Beispiel wird angegeben, dass Sie den auf der DMZ-Schnittstelle (ein- oder ausgehend) angezeigten Datenverkehr abgleichen möchten, der mit dem TCP-Host 172.16.31.10/host 203.0.113.2 übereinstimmt. Mit anderen Worten, Sie möchten jeden TCP-Datenverkehr erfassen, der von Host 172.16.31.10 an Host 203.0.113.2 gesendet wird, oder

umgekehrt. Durch die Verwendung des match-Schlüsselworts kann die Firewall diesen Datenverkehr bidirektional erfassen. Der für die externe Schnittstelle definierte Erfassungsbefehl verweist nicht auf die IP-Adresse des internen Mailservers, da die Firewall eine NAT für die IP-Adresse des Mailservers durchführt. Daher können Sie nicht mit dieser Server-IP-Adresse übereinstimmen. Stattdessen wird im nächsten Beispiel das Wort **any** verwendet, um anzugeben, dass alle möglichen IP-Adressen mit dieser Bedingung übereinstimmen.

Nachdem Sie die Captures konfiguriert haben, sollten Sie erneut versuchen, eine Verbindung herzustellen, und mit dem Befehl **show capture_name>** die Captures anzeigen. In diesem Beispiel sehen Sie, dass der externe Host eine Verbindung zum Mail-Server herstellen konnte. Dies wird durch den dreiseitigen TCP-Handshake deutlich, der in den Captures zu sehen ist:

```
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
```

Mailserver im internen Netzwerk

Packet Tracer

Im Folgenden finden Sie ein Beispiel für eine Pakettracer-Ausgabe:

```
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
```

Mailserver im externen Netzwerk

Packet Tracer

Im Folgenden finden Sie ein Beispiel für eine Pakettracer-Ausgabe:

```
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
```

Zugehörige Informationen

- Syslog-Meldungen der Cisco ASA-Serie
- ASA-Paketerfassung mit CLI- und ASDM-Konfigurationsbeispiel

- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie, 9.0 - Konfigurieren von Network Object NAT
- Technischer Support und Dokumentation - Cisco Systems