

Configureer de ASA for MGCP Mail Server access in DMZ, binnen en buiten netwerken

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Mail Server in het DMZ-netwerk](#)

[Netwerkdigram](#)

[ASA-configuratie](#)

[ESMTP-TLS-configuratie](#)

[Mail Server in het binnennetwerk](#)

[Netwerkdigram](#)

[ASA-configuratie](#)

[Mail Server in het buitennetwerk](#)

[Netwerkdigram](#)

[ASA-configuratie](#)

[Verifiëren](#)

[Mail Server in het DMZ-netwerk](#)

[TCP-ping](#)

[verbinding](#)

[Vastlegging](#)

[NAT-vertalingen \(Xlaat\)](#)

[Mail Server in het binnennetwerk](#)

[TCP-ping](#)

[verbinding](#)

[Vastlegging](#)

[NAT-vertalingen \(Xlaat\)](#)

[Mail Server in het buitennetwerk](#)

[TCP-ping](#)

[verbinding](#)

[Vastlegging](#)

[NAT-vertalingen \(Xlaat\)](#)

[Problemen oplossen](#)

[Mail Server in het DMZ-netwerk](#)

[Packet-Tracer](#)

[Packet Capture](#)

[Mail Server in het binnennetwerk](#)

[Packet-Tracer](#)

[Mail Server in het buitennetwerk](#)

[Packet-Tracer](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een Cisco adaptieve security applicatie (ASA) kunt configureren voor toegang tot een Simple Mail Transfer Protocol (SMTP) server die zich bevindt in de gedemilitariseerde Zone (DMZ), het binnennetwerk of het externe netwerk.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA die softwareversie 9.1 of hoger uitvoert
- Cisco 2800C Series router met Cisco IOS-softwareversie 15.1(4)M6

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Configureren

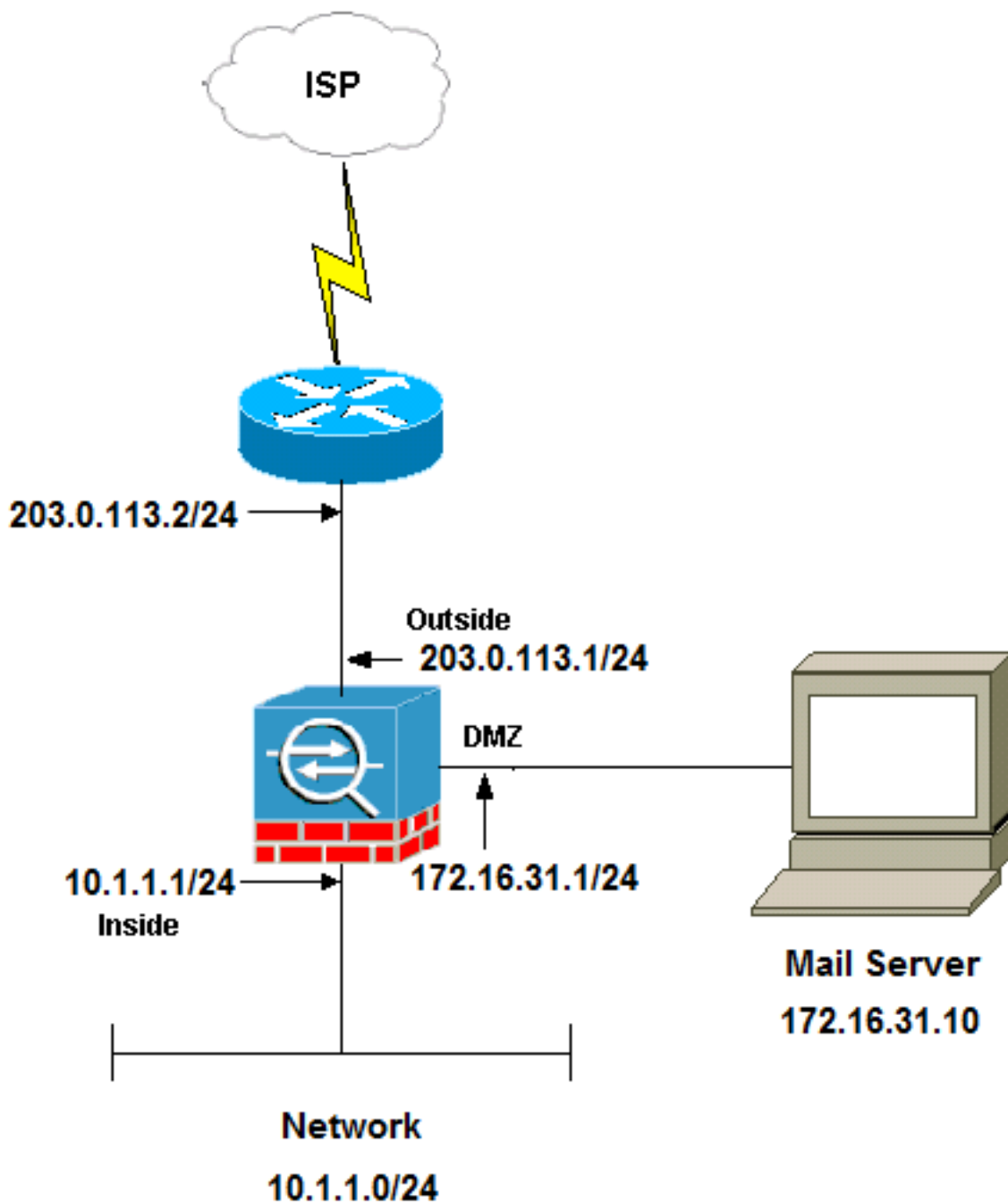
In deze sectie wordt beschreven hoe u de ASA moet configureren om de mailserver in het DMZ-netwerk, het binnennetwerk of het externe netwerk te bereiken.

Opmerking: Gebruik het [Opdrachtuppgereedschap](#) (alleen [geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Mail Server in het DMZ-netwerk

Netwerkdigram

De configuratie die in dit gedeelte wordt beschreven, gebruikt deze netwerkinstelling:



Opmerking: De IP-adresseringsschema's die in dit document worden gebruikt, zijn niet wettelijk routinematig op het internet. Ze zijn [RFC 1918](#) adressen die in een labomgeving gebruikt zijn.

De netwerkinstelling die in dit voorbeeld wordt gebruikt heeft de ASA met een binnennetwerk op **10.1.1.0/24** en een extern netwerk op **203.0.113.0/24**. De mailserver met IP adres **172.16.31.10**

bevindt zich in het DMZ-netwerk. U moet de netwerkadresomzetting (NAT) configureren om de mailserver toegankelijk te maken via het interne netwerk.

Om de externe gebruikers toegang te geven tot de mailserver, moet u een statische NAT en een toegangslijst configureren, in dit voorbeeld is `buitenkant_int`, zodat de externe gebruikers toegang kunnen krijgen tot de mailserver en de toegangslijst aan de externe interface kunnen binden.

ASA-configuratie

Dit is de ASA-configuratie voor dit voorbeeld:

```
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-configuratie

Als u TLS-encryptie (Transport Layer Security) voor e-mailcommunicatie gebruikt, dan laat de uitgebreide Simple Mail Transfer Protocol (ESMTP) - inspectiemogelijkheid (standaard ingeschakeld) in de ASA de pakketten vallen. Schakel de ESMTP-inspectiemogelijkheid uit zoals in het volgende voorbeeld, om de e-mails met TLS ingeschakeld te kunnen uitschakelen.

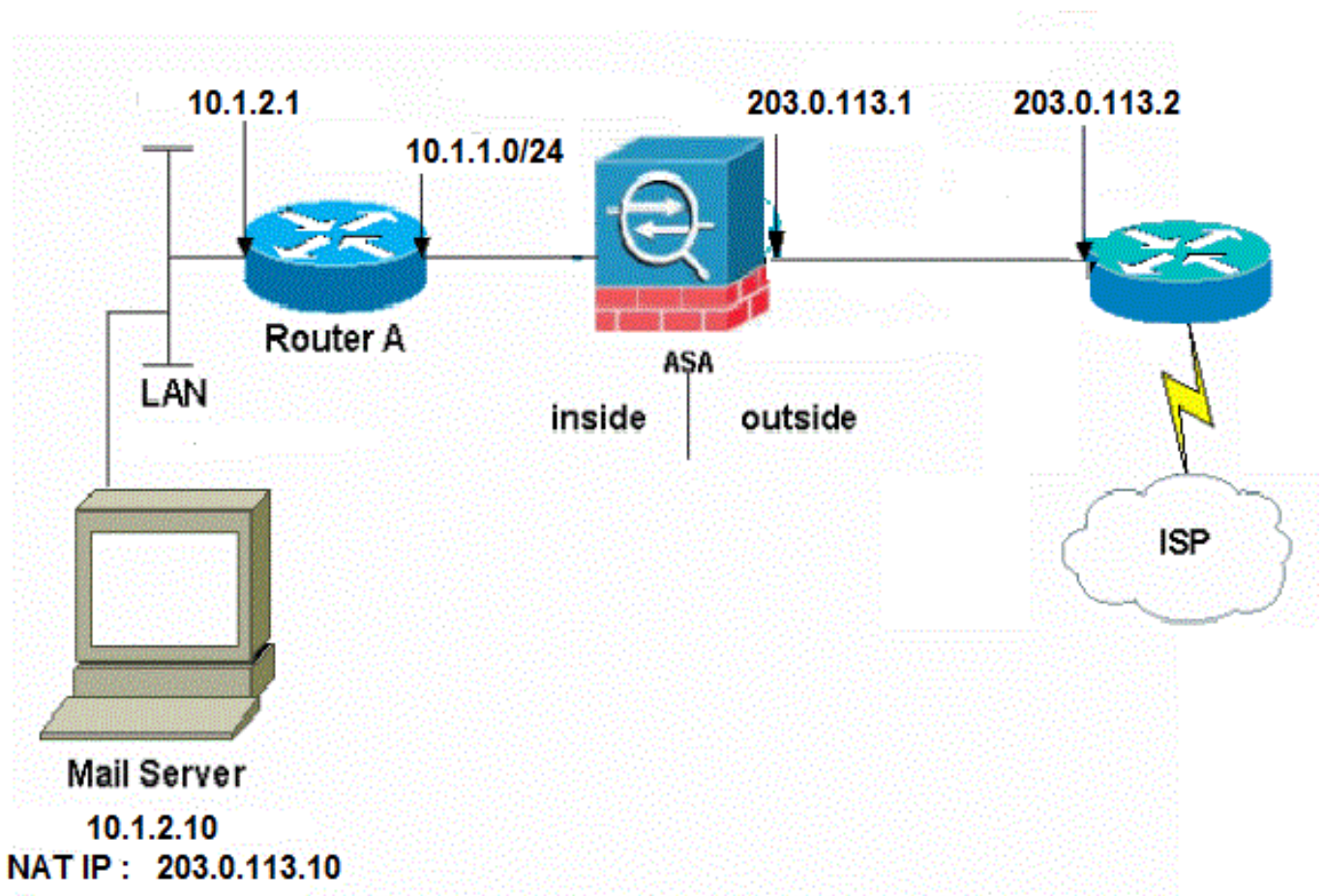
Opmerking: Raadpleeg Cisco bug-ID [CSCtn08326](#) (alleen [geregistreerde](#) klanten) voor meer informatie.

```
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
```

Mail Server in het binnennetwerk

Netwerkdigram

De configuratie die in dit gedeelte wordt beschreven, gebruikt deze netwerkinstelling:



De netwerkinstelling die in dit voorbeeld wordt gebruikt heeft de ASA met een binnennetwerk op 10.1.1.0/24 en een extern netwerk op 203.0.113.0/24. De mailserver met het IP adres 10.1.2.10 bevindt zich in het binnennetwerk.

ASA-configuratie

Dit is de ASA-configuratie voor dit voorbeeld:

```
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.

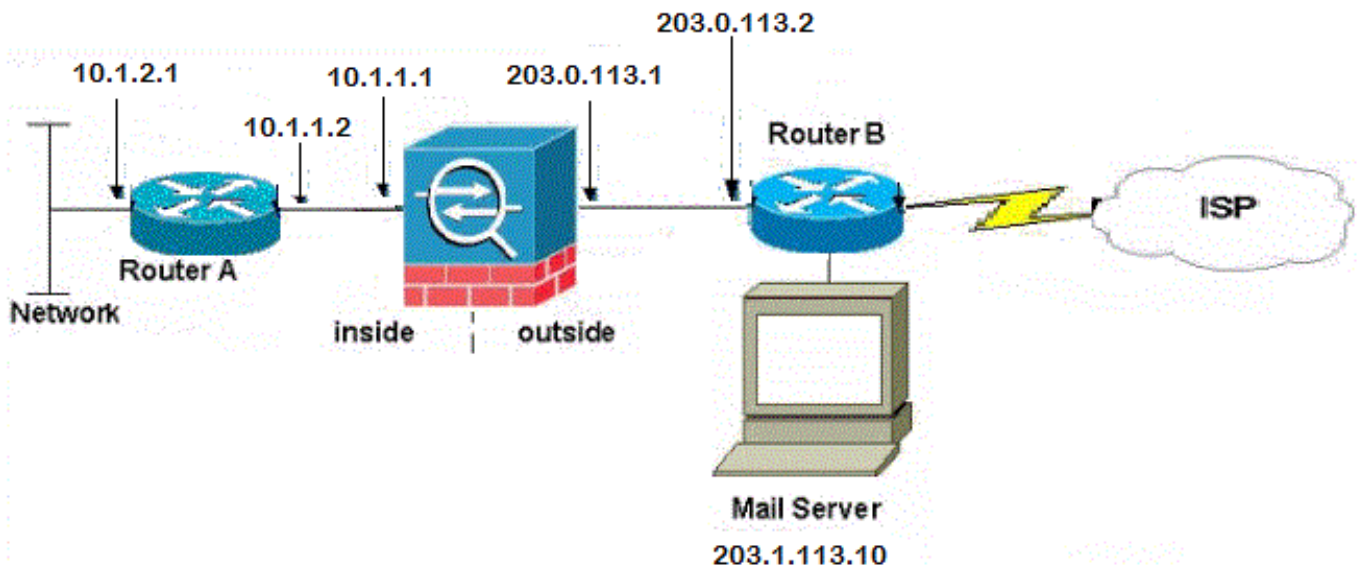
route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

```

Mail Server in het buitennetwerk

Netwerkdigram

De configuratie die in dit gedeelte wordt beschreven, gebruikt deze netwerkinstelling:



ASA-configuratie

Dit is de ASA-configuratie voor dit voorbeeld:

```

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

```

Verifiëren

Gebruik de informatie in deze sectie om te controleren of uw configuratie correct werkt.

Mail Server in het DMZ-netwerk

TCP-ping

TCP ping test een verbinding over TCP (de standaard is Internet Control Message Protocol (ICMP)). Een TCP pingen stuurt SYN-pakketten en denkt dat het ping succesvol is als het doelapparaat een SYN-ACK-pakket verstuurt. U kunt maximaal twee gelijktijdige TCP-pings tegelijkertijd uitvoeren.

Hierna volgt een voorbeeld:

```

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
```

verbinding

ASA is een stateful Firewall. Verkeersverkeer van de mailserver is toegestaan door de firewall omdat het overeenkomt met een verbinding in de firewallverbindingstabel. Het verkeer dat overeenkomt met een huidige verbinding wordt door de firewall toegestaan zonder te worden geblokkeerd door een toegangscontrolelijst (ACL).

In het volgende voorbeeld, vestigt de client op de externe interface een verbinding met de 203.0.113.10 host van de DMZ-interface. Deze verbinding wordt gemaakt met het TCP protocol en is twee seconden leeg geweest. De verbindingsvlaggen geven de huidige stand van deze verbinding aan:

```
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
```

Vastlegging

De ASA Firewall genereert systemen tijdens normaal gebruik. De systemen variëren in breedtegraad op basis van de houtkapconfiguratie. Deze output toont twee syslogs die op niveau zes (het *informatieniveau*) en niveau zeven (het *debugging level*) verschijnen:

```
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)
```

Het tweede syslog in dit voorbeeld geeft aan dat de Firewall een verbinding in zijn verbindingstabel voor dit specifieke verkeer tussen de client en server heeft gebouwd. Als de Firewall was geconfigureerd om deze verbindingsooging te blokkeren, of als een andere factor de creatie van deze verbinding remde (beperkte middelen of een mogelijke verkeerde configuratie), dan genereerde de Firewall geen logbestand dat aangeeft dat de verbinding was gebouwd. In plaats daarvan zou het een reden loggen om de connectie te ontkennen of een indicatie zijn van de factor die de verbinding remde om gecreëerd te worden.

Als ACL aan de buitenkant bijvoorbeeld niet is ingesteld om 172.16.31.10 toe te staan op poort 25, dan zou u dit logbestand zien wanneer het verkeer wordt ontkend:

```
%ASA-4-106100: toegang-lijst buitenkant_int ontkende tcp buiten bereik/203.0.113.2(3756) ->
```

dmz/172.16.31.10(25) hit-cnt 5 300-seconden interval

Dit zou voorkomen wanneer ACL zoals hier wordt getoond ontbreekt of verkeerd wordt ingesteld:

```
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-vertalingen (Xlaet)

Om te bevestigen dat de vertalingen worden gemaakt, kunt u de Xlate (vertaling) tabel bekijken. De opdracht **toont uitloop**, wanneer gecombineerd met het lokale sleutelwoord en het interne IP adres van de gastheer, toont alle ingangen die in de vertaallijst voor die gastheer aanwezig zijn. De volgende uitvoer toont aan dat er een vertaling is die op dit moment voor deze host tussen de DMZ en de buiteninterfaces is gebouwd. Het IP-adres van de DMZ-server wordt vertaald naar het 203.0.113.10-adres per de vorige configuratie. De vlaggen die zijn vermeld (s in dit voorbeeld) geven aan dat de vertaling *statisch* is.

```
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
```

Mail Server in het binnennetwerk

TCP-ping

Hier is een voorbeeld van TCP-ping-uitvoer:

```
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
```

verbinding

Hier is een voorbeeld van verbindingcontrole:

```
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
```

Vastlegging

Hier is een voorbeeld:

```
%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-vertalingen (Xlaat)

Hier zijn een paar voorbeelden die **details tonen** en uitgangen **tonen** van **xlate** commando's:

```
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
```

Mail Server in het buitennetwerk

TCP-ping

Hier is een voorbeeld van TCP-ping-uitvoer:

```
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
```

verbinding

Hier is een voorbeeld van verbindingsscontrole:

```
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
```

Vastlegging

Hier is een voorbeeld:

```
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-vertalingen (Xlaar)

Hier is een voorbeeld van het tonen van uitgever beveluitvoer:

```
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
```

Problemen oplossen

ASA biedt meerdere tools om connectiviteit op te lossen. Als de kwestie blijft voortbestaan nadat u de configuratie hebt geverifieerd en de uitgangen hebt gecontroleerd die in de vorige sectie

worden beschreven, kunnen deze gereedschappen en technieken u helpen de oorzaak van uw aansluitingsmislukking te bepalen.

Mail Server in het DMZ-netwerk

Packet-Tracer

De functionaliteit van de pakkettracer op de ASA staat u toe om een *gesimuleerd* pakket te specificeren en alle verschillende stappen, controles, en functies te bekijken die de Firewall doorvoert wanneer het verkeer verwerkt. Met dit gereedschap is het handig om een voorbeeld van verkeer te identificeren dat volgens u toegestaan *moet* worden om door de firewall te laten lopen, en die vijf-tupple te gebruiken om het verkeer te simuleren. In het volgende voorbeeld wordt de pakkettracer gebruikt om een verbindingspoging te simuleren die aan deze criteria voldoet:

- Het gesimuleerde pakje komt aan de **buitenkant**.
- Het protocol dat wordt gebruikt is **TCP**.
- Het gesimuleerde IP-adres van de client is **203.0.113.2**.
- De cliënt verstuurt verkeer dat afkomstig is van poort **1234**.
- Het verkeer is bestemd voor een server op IP-adres **203.0.113.10**.
- Het verkeer is bestemd voor haven **25**.

Hier is een voorbeeld van pakkettracer uitvoer:

```
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
```

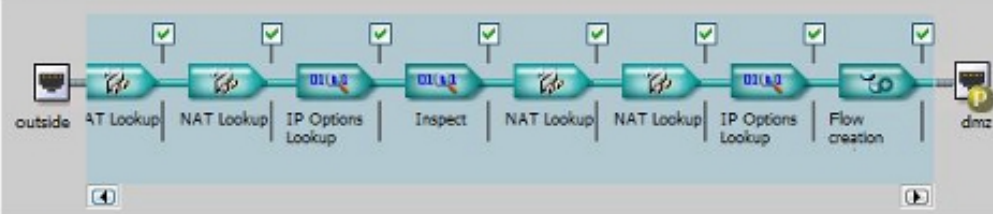
Hier is een voorbeeld in Cisco Adaptieve Security Devices Manager (ASDM):

Select the packet type and supply the packet parameters. Click Start to trace the packet.

Interface: Packet Type TCP UDP ICMP IP

Source: Destination:
 Source Port: Destination Port:

Show animation



Phase

UN-NAT

Type - UN-NAT Subtype - static Action - ALLOW [Show rule in NAT Rules table.](#)

Config

```
nat (dmz,outside) source static obj-172.16.31.10 obj-203.0.113.10
```

Info

```
NAT divert to egress interface dmz
Untranslate 203.0.113.10/25 to 172.16.31.10/25
```

ACCESS-LIST
 NAT
 NAT
 IP-OPTIONS
 INSPECT

Merk op dat de *DMZ*-interface in de vorige outputs niet wordt genoemd. Dit is een pakkettracer ontwerp. Het gereedschap vertelt je hoe de Firewall dat type verbindingsooging verwerkt, dat ook bevat hoe het hem zou leiden en uit welke interface.

Tip: Raadpleeg voor aanvullende informatie over de optie pakkettracer de optie [Tracing Packets met Packet Tracer](#) van de *Cisco ASA 5500 Series Configuration Guide met behulp van de CLI, 8.4 en 8.6*.

Packet Capture

De ASA Firewall kan verkeer vangen dat zijn interfaces binnenkomt of verlaat. Deze opnamefunctionaliteit is zeer nuttig omdat het definitief kan bewijzen of het verkeer aankomt of van een Firewall vertrekt. Het volgende voorbeeld toont de configuratie van twee Captures die respectievelijk **capd** en **capout** op de DMZ en de externe interfaces worden genoemd. De opnameopdrachten gebruiken een overeenkomend trefwoord, zodat u specifiek kunt zijn over het verkeer dat u wilt opnemen.

Voor de **opname die** in dit voorbeeld voorkomt, is aangegeven dat u het verkeer wilt koppelen dat gezien wordt op de DMZ interface (stress of stress) die TCP host 172.16.31.10/host 203.0.113.2 aanpast. Met andere woorden, u wilt elk TCP-verkeer opnemen dat verzonden wordt van host 172.16.31.10 naar host 203.0.113.2 of omgekeerd. Het gebruik van het overeenkomende sleutelwoord staat de Firewall toe om dat verkeer bidirectioneel te vangen. De opnameopdracht

die voor de externe interface is gedefinieerd, verwijst niet naar het IP-adres van de interne mailserver omdat de firewall een NAT op dat IP-adres van de mailserver voert. Als resultaat hiervan kunt u niet overeenkomen met dat IP-adres van de server. In plaats daarvan gebruikt het volgende voorbeeld het woord **elk** om aan te geven dat alle mogelijke IP adressen die voorwaarde zouden aanpassen.

Nadat u de Captures configureren dient u vervolgens te proberen opnieuw een verbinding op te zetten en vervolgens de opgenomen beelden te bekijken met de opdracht **SHOC_name>**. In dit voorbeeld, kunt u zien dat de buitengastheer met de postserver kon verbinden, zoals duidelijk door de TCP drierichtingshanddruk die in de Captures wordt gezien:

```
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
```

Mail Server in het binnennetwerk

Packet-Tracer

Hier is een voorbeeld van pakkettracer uitvoer:

```
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
```

Mail Server in het buitennetwerk

Packet-Tracer

Hier is een voorbeeld van pakkettracer uitvoer:

```
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
```

Gerelateerde informatie

- [Cisco ASA Series NextGeneration Systems](#)
- [ASA Packet Capture met CLI en ASDM Configuratievoorbeeld](#)
- [Cisco ASA Series CLI-configuratiegids, 9.0 - Netwerkoject met configuratie](#)

- [Technische ondersteuning en documentatie - Cisco-systemen](#)