# ASA release 9.1(x) Connection van drie interne netwerken met voorbeeld voor internetconfiguratie

## Inhoud



## Inleiding

Dit document bevat informatie over het instellen van de Cisco adaptieve security applicatie (ASA) versie 9.1(5) voor gebruik met drie interne netwerken. Statische routes worden gebruikt op de routers voor eenvoud.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco adaptieve security applicatie (ASA) versie 9.1(5).

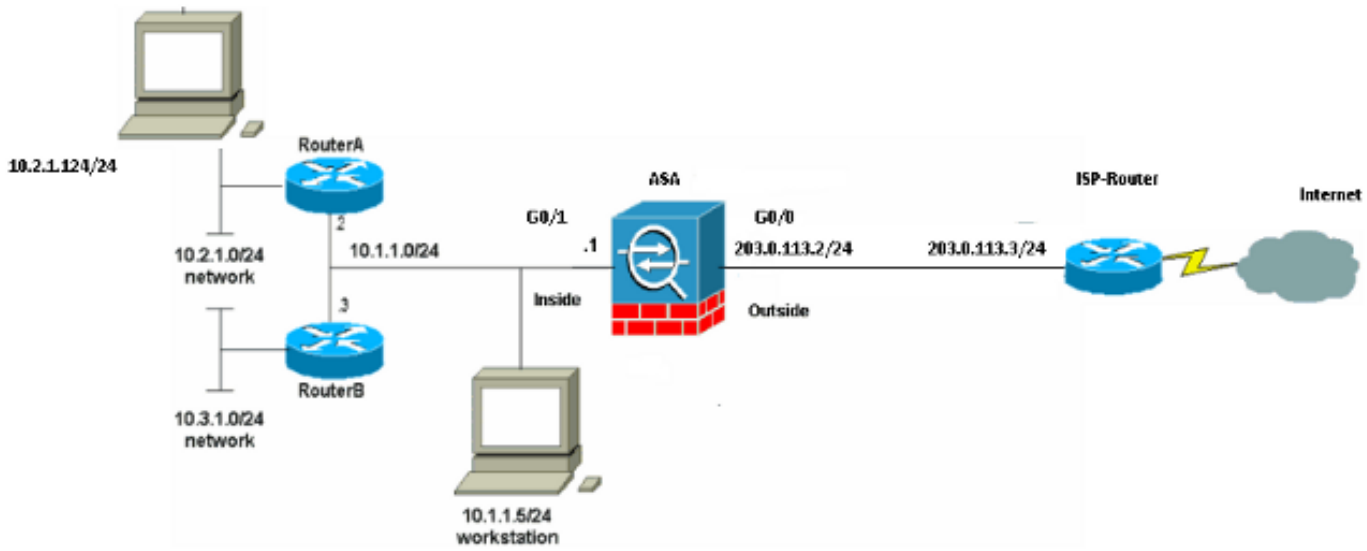
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

## Netwerkdiagram




> Opmerking: De IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918-adressen die in een labomgeving zijn gebruikt.

## ASA 9.1 configuratie

Dit document gebruikt deze configuraties. Als u de output van een opdracht **schrijfterminal** van uw Cisco-apparaat hebt, kunt u uitgangsinterfaces gebruiken (alleen geregistreerde klanten) om potentiële problemen en oplossingen weer te geven.

### Configuraties

- Configuratie router A
- Configuratie van router B
- ASA versie 9.1 en later-configuratie

#### Configuratie router A

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
```

```
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
```

```
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

### Configuratie van router B

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
```

```
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

### ASA versie 9.1 en later-configuratie

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
```

```
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

# Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Probeer een website via HTTP te benaderen met een webbrowser. Dit voorbeeld gebruikt een site die wordt gehost op 198.51.100.100. Als de verbinding succesvol is, kan deze output worden gezien op de ASA CLI.

### verbinding

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
flags UIO
```

ASA is een stateful firewall en het retourverkeer van de webserver is toegestaan door de firewall omdat het overeenkomt met een ***verbinding*** in de verbindingstabel van de firewall. Het verkeer dat overeenkomt met een verbinding die al bestaat, is toegestaan door de firewall en is niet geblokkeerd door een ACL-interface.

In de vorige output heeft de client op de interne interface een verbinding met de host van de externe interface gecreëerd. Deze verbinding wordt gemaakt met het TCP protocol en is gedurende zes seconden leeg geweest. De verbindingsvlaggen geven de huidige status van deze verbinding aan. Meer informatie over verbindingsvlaggen kan in ASA TCP verbindingsvlaggen worden gevonden.

## Syslog

```
ASA(config)# show log | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

De ASA Firewall genereert systemen tijdens normaal gebruik. De systemen variëren in breedtegraad op basis van de houtkapconfiguratie. De output laat twee syslogs zien die op niveau zes worden gezien, of ‘informatieniveau'.

In dit voorbeeld worden twee syslogs gegenereerd. Het eerste is een logbericht dat aangeeft dat de firewall een vertaling heeft gemaakt, in het bijzonder een dynamische TCP-vertaling (PAT). Het geeft het bron-IP-adres en de poort en het vertaalde IP-adres en -poort aan als de verkeersverplaatsingen van de binnenkant naar de externe interfaces.

Het tweede signaal geeft aan dat de firewall een verbinding in zijn verbindingstabel heeft gebouwd voor dit specifieke verkeer tussen de client en de server. Als de firewall was geconfigureerd om deze verbindingspoging te blokkeren, of als een andere factor de creatie van deze verbinding remde (middelbeperkingen of een mogelijke fouconfiguratie), zou de firewall geen logbestand genereren 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 welke factor de connectie remde.

## NAT-omzetting

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

Als deel van deze configuratie wordt PAT geconfigureerd om de interne IP-adressen van de host te vertalen naar adressen die op het internet routeerbaar zijn. Om te bevestigen dat deze vertalingen worden gemaakt, kunt u de NAT-vertaaltabel (xlate) bekijken. De opdracht **toont uitloop,** wanneer gecombineerd met het **lokale** sleutelwoord en het IP adres van de interne

gastheer, alle ingangen in de vertaaltabel voor die gastheer tonen. De vorige output toont dat er een vertaling is die momenteel voor deze gastheer tussen de binnen en buiten interfaces wordt gebouwd. De binnenhost IP en de poort worden vertaald naar het 203.0.113.2-adres per onze configuratie. De vlaggen of i geven aan dat de vertaling **dynamisch** is en een **portmap**. Meer informatie over de verschillende NAT-configuraties is te vinden in Informatie over NAT.

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

ASA biedt meerdere tools om connectiviteit op te lossen. Als het probleem blijft bestaan nadat u de configuratie hebt geverifieerd en de eerder genoemde uitvoer hebt gecontroleerd, kunnen deze gereedschappen en technieken de oorzaak van uw aansluitingsfalen helpen bepalen.

## Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

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 zien die de firewall 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 door te gaan en gebruik dat 5-paars om verkeer te simuleren. In het vorige voorbeeld wordt de pakkettracer gebruikt om een verbindingspoging te simuleren die aan deze criteria voldoet:

- Het gesimuleerde pakje komt **binnenin** aan.
- Het gebruikte protocol is **TCP**.
- Het gesimuleerde IP-adres van de client is **10.2.1.124**.
- De cliënt verstuurt verkeer vanuit haven **1234**.
- Het verkeer is bestemd voor een server op IP-adres **198.51.100.100**.
- Het verkeer is bestemd voor haven **80**.

Merk op dat er geen melding was van de interface **buiten** de opdracht. Dit is een pakkettracer ontwerp. Het gereedschap vertelt u hoe de firewall dat type van verbindingspoging verwerkt, dat omvat hoe het het zou leiden, en uit welke interface. Meer informatie over pakkettracer kan in het Traceren van pakketten met Packet Tracer worden gevonden.

## Opnemen

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
```

```
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured

  1: 11:31:23.432655       10.2.1.124.18711 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

De ASA firewall kan verkeer vangen dat zijn interfaces in of verlaat. Deze opnamefunctionaliteit is fantastisch omdat het definitief kan bewijzen of het verkeer aankomt of van een firewall vertrekt. Het vorige voorbeeld toonde de configuratie van twee Captures genaamd **capin** en **capout** op de binnen- en buitenkant interfaces respectievelijk. De opnameopdrachten hebben het trefwoord gebruikt, waardoor je specifiek kunt zijn over het verkeer dat je wilt opnemen.

Voor de opname **capin** werd aangegeven dat je verkeer op de binnenkant interface (**stress of spanning) wilt koppelen dat TCP host 10.2.1.124 host 198.51.100.100** aansluit. Met andere woorden, je wilt elk TCP-verkeer opnemen dat van **host 10.0** wordt **verzonden 2.1.124 gastland 198.51.100.100** of **omgekeerd.** Het gebruik van het **overeenkomende** sleutelwoord staat de firewall toe om dat verkeer bidirectioneel te vangen. Het opnameopdracht die voor de externe interface is gedefinieerd, verwijst niet naar het interne client-IP-adres omdat de firewall PAT op dat client-IP-adres uitvoert. Als resultaat hiervan kunt u niet met dat client-IP-adres **overeenkomen**. In plaats daarvan gebruikt dit voorbeeld **om** aan te geven dat alle mogelijke IP-adressen met deze voorwaarde overeenkomen.

Nadat u de Captures configureren zou u vervolgens proberen om opnieuw een verbinding tot stand te brengen, en vervolgens de opgenomen beelden met de opdracht **Show*<shot_name>*** te bekijken. In dit voorbeeld, kunt u zien dat de client in staat was om verbinding te maken met de server zoals duidelijk door de TCP 3-manier handdruk die in de Captures wordt gezien.