ASA 8.4(x) sluit een enkel intern netwerk aan op het voorbeeld van internetconfiguratie

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) kunt instellen met versie 8.4(1) voor gebruik op één intern netwerk.

Raadpleeg PIX/ASA: Een enkel intern netwerk aansluiten op het Internet Configuration Voorbeeld voor dezelfde configuratie op de ASA met versies 8.2 en eerder.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de ASA met versie 8.4(1).

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

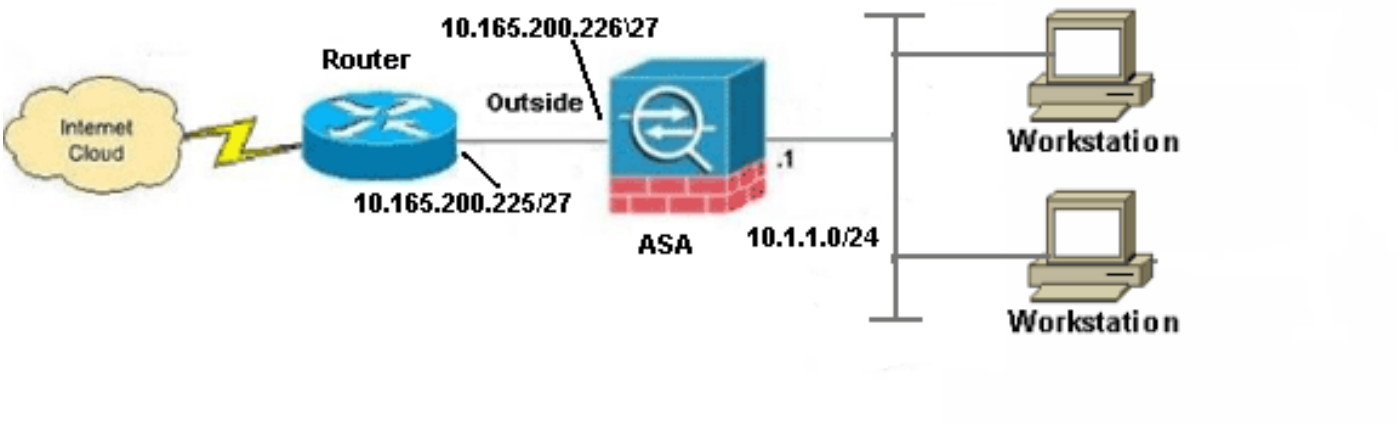
Configureren

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

> Opmerking: Om extra informatie over de opdrachten in dit document te vinden, gebruikt u het Opdrachtupgereedschap (alleen geregistreerde klanten).

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



> 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 gebruikt zijn.

ASA 8.4 configuratie

Dit document gebruikt deze configuraties:

- Routerconfiguratie
- ASA 8.4 en hoger-configuratie

Routerconfiguratie

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

ASA 8.4 en hoger-configuratie

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
timeout xlate 3:00:00
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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
```

```
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
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
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

> Opmerking: Raadpleeg voor meer informatie over de configuratie van Network Address Translation (NAT) en Port Address Translation (PAT) op ASA versie 8.4 de informatie over NAT.
>
> Raadpleeg voor meer informatie over de configuratie van toegangslijsten in ASA versie 8.4 de informatie over toegangslijsten.

Verifiëren

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 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
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 zonder geblokkeerd te worden door een interface-ACL.

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 | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

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 **op '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** heeft gebouwd in de verbindingstabel 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-vertalingen (Xlaat)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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 uitroltabel (vertaling) 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 binnen ontvangen IP en de haven worden vertaald naar het 10.165.200.226 adres per onze configuratie. De vlaggen of i geven aan dat de vertaling **dynamisch** is en een **portmap**. Klik hier

voor meer informatie over de verschillende NAT-configuraties: Informatie over NAT.

Problemen 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 10.1.1.154 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 doorvoert wanneer het verkeer verwerkt. Met dit gereedschap is het handig om een voorbeeld van verkeer te identificeren waarvan u vindt dat het toegestaan *moet* zijn om door de firewall te stappen en dat 5-pple te gebruiken 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 **10.1.1.154**.
- 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 Tracing pakketten met Packet Tracer worden gevonden.

Opnemen

```
ASA# capture capin interface inside match tcp host 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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** gaf u aan dat u verkeer op de binnenkant interface (**toegang of spanning) wilt koppelen dat TCP host 10.1.1.154 host 198.51.100.100** aansluit. Met andere woorden, u wilt elk TCP-verkeer opnemen dat van **host 10.1** wordt verzonden 1.1.154 voor **gastheer 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 opnieuw proberen een verbinding op te zetten, 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.

Gerelateerde informatie

- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems