Probleemoplossing met verbindingen via PIX en ASA

Inhoud

Inleiding

Dit document bevat ideeën en suggesties voor het oplossen van problemen wanneer u Cisco ASA 5500 Series adaptieve security applicatie (ASA) en Cisco PIX 500 Series security applicatie gebruikt. Vaker wel dan niet, wanneer toepassingen of netwerkbronnen breken of niet beschikbaar zijn, hebben firewalls (PIX of ASA) de neiging een primair doel te zijn en de schuld te krijgen als oorzaak van stroomstoringen. Met wat testen op de ASA of PIX, kan een beheerder bepalen of de

ASA/PIX het probleem veroorzaakt.

Raadpleeg PIX/ASA: Connectiviteit met Cisco security applicatie realiseren en probleemoplossing door de Cisco security applicatie om meer te weten te komen over de interface-gerelateerde probleemoplossing op de Cisco security applicaties.

Opmerking: dit document is gericht op de ASA en PIX. Zodra de probleemoplossing op de ASA of PIX is voltooid, is het waarschijnlijk dat een extra probleemoplossing noodzakelijk is met andere apparaten (routers, switches, servers, enzovoort).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA 5510 met OS 7.2.1 en 8.3.

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.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

- ASA en PIX OS 7.0, 7.1, 8.3 en hoger
- Firewallservicesmodule (FWSM) 2.2, 2.3 en 3.1

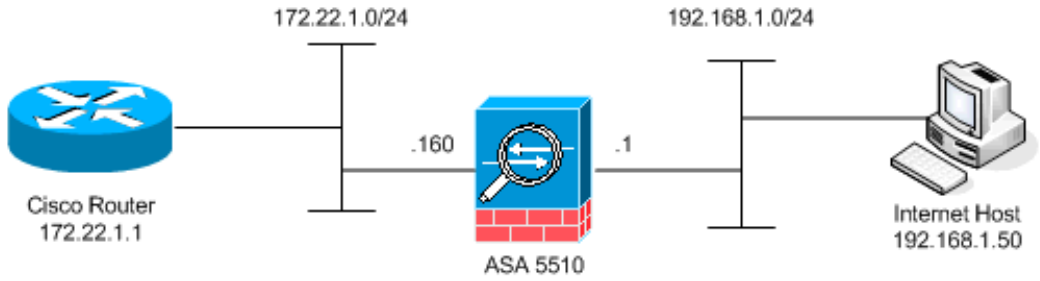
Opmerking: specifieke opdrachten en syntax kunnen tussen softwareversies verschillen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Het voorbeeld veronderstelt dat de ASA of PIX in productie is. De ASA/PIX-configuratie kan relatief simpel (slechts 50 lijnen van configuratie) of complex (honderden tot duizenden configuratielijnen) zijn. Gebruikers (klanten) of servers kunnen zich op een beveiligd netwerk (binnen) of op een onveilig netwerk (DMZ of daarbuiten) bevinden.



De ASA begint met deze configuratie. De configuratie is bedoeld om het lab een referentiepunt te geven.

ASA initiële configuratie

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
```

```
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


!--- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside 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 uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters 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 netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Probleem

Een gebruiker neemt contact op met de IT-afdeling en meldt dat toepassing X niet langer werkt. Het incident escaleert naar de ASA/PIX-beheerder. De beheerder heeft weinig kennis van deze specifieke toepassing. Met het gebruik van de ASA/PIX, ontdekt de beheerder welke havens en protocollen toepassing X gebruikt evenals wat de oorzaak van het probleem zou kunnen zijn.

Oplossing

De ASA/PIX-beheerder moet zoveel mogelijk informatie van de gebruiker verzamelen. Handige informatie omvat:

- IP-adres bron: dit is meestal het werkstation of de computer van de gebruiker.
- IP-adres bestemming—het IP-adres van de server dat de gebruiker of toepassing probeert aan te sluiten.
- poorten en protocollen die de toepassing gebruikt

Vaak heeft de beheerder geluk als hij een antwoord op een van deze vragen kan krijgen. De beheerder kan bijvoorbeeld geen informatie verzamelen. Een review van ASA/PIX syslig-berichten is ideaal maar het is moeilijk om het probleem te vinden als de beheerder niet weet wat te zoeken.

Stap 1 - Ontdek het IP-adres van de gebruiker

Er zijn veel manieren om het IP-adres van de gebruiker te ontdekken. Dit document gaat over de ASA en PIX, dus dit voorbeeld gebruikt de ASA en PIX om het IP adres te ontdekken.

De gebruiker probeert te communiceren met de ASA/PIX. Deze communicatie kan ICMP, telnet, SSH of HTTP zijn. Het gekozen protocol moet een beperkte activiteit op de ASA/PIX hebben. In dit specifieke voorbeeld, pingelt de gebruiker de binneninterface van de ASA.

De beheerder moet één of meer van deze opties instellen en dan de gebruiker de interne interface van de ASA hebben.

- **Syslog**Controleer of het loggen is ingeschakeld. Het logniveau moet worden ingesteld op **debug**. Vastlegging kan op verschillende locaties worden verzonden. Dit voorbeeld gebruikt de ASA logbuffer. Mogelijk hebt u een externe logserver nodig in productieomgevingen.
```
ciscoasa(config)#logging enable
ciscoasa(config)#logging buffered debugging
```

  De gebruiker stopt de interne interface van de ASA (ping 192.168.1.1). Deze uitvoer wordt weergegeven.
```
ciscoasa#show logging
!--- Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
%ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
!--- The user IP address is 192.168.1.50.
```
- **ASA Capture optie**De beheerder moet een toegangslijst maken die bepaalt wat het verkeer dat de ASA moet opnemen. Nadat de toegangslijst is gedefinieerd, neemt de opdracht Opnemen de toegangslijst op en past deze op een interface toe.
```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

  De gebruiker stopt de interne interface van de ASA (ping 192.168.1.1). Deze uitvoer wordt weergegeven.
```
ciscoasa#show capture inside_interface
   1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
 !--- The user IP address is 192.168.1.50.
```
  Opmerking: om het opnamebestand te kunnen downloaden naar een systeem als etherisch, kunt u dit doen zoals in deze uitvoer wordt weergegeven.
```
!--- Open an Internet Explorer and browse with this https link format: https://[
```

  Raadpleeg ASA/PIX: Packet Capturing met CLI en ASDM Configuration Voorbeeld om meer te weten te komen over Packet Capturing in ASA.
- **Debuggen**De opdracht **Icmp-**sporen **debug** wordt gebruikt om het ICMP-verkeer van de gebruiker op te nemen.
```
ciscoasa#debug icmp trace
```

  De gebruiker stopt de interne interface van de ASA (ping 192.168.1.1). Deze uitvoer wordt op de console weergegeven.
```
ciscoasa#
```

```
!--- Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

Om **debug icmp-**overtrekken uit te schakelen, gebruikt u een van deze opdrachten:**geen debug-icmpicmp-sporen terugvindenalles ontdooien**, **alles** ongedaan **maken** of **helemaal afluisteren**

Elk van deze drie opties helpt de beheerder om het bron IP-adres te bepalen. In dit voorbeeld is het IP-bronadres van de gebruiker 192.168.1.50. De beheerder is klaar om meer te weten te komen over toepassing X en de oorzaak van het probleem te bepalen.

Stap 2 - Zoek de oorzaak van het probleem

Met betrekking tot de informatie in het gedeelte Stap 1 van dit document opgesomd, weet de beheerder nu de bron van een toepassing X sessie. De beheerder is klaar om meer over toepassing X te weten te komen en om te beginnen te vinden waar de kwesties zouden kunnen zijn.

De ASA/PIX-beheerder moet de ASA voorbereiden op ten minste één van deze vermelde suggesties. Zodra de beheerder klaar is, start de gebruiker toepassing X en beperkt hij alle andere activiteit omdat extra gebruikersactiviteit verwarring kan veroorzaken of de ASA/PIX-beheerder kan misleiden.

- **Controleer de syslogberichten.**Zoeken naar het IP-bronadres van de gebruiker die u in Stap 1 hebt geplaatst. De gebruiker initieert toepassing X. De ASA-beheerder geeft de opdracht **voor** vastlegging weer en geeft de uitvoer weer.

  ```
  ciscoasa#show logging
  !--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-
  305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
  outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
  outside:172.22.1.1/80
  (172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
  ```

  De logboeken onthullen dat het bestemming IP adres 172.22.1.1 is, het protocol is TCP, de doelpoort is HTTP/80 en dat verkeer naar de externe interface wordt verzonden.
- **De opnamefilters wijzigen.**De **access-list binnenkant_test** opdracht werd eerder gebruikt en wordt hier gebruikt.

  ```
  ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
  !--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the
  ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
  !--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.
  ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
  ciscoasa(config)#clear capture inside_interface
  !--- Clears the previously logged data. !--- The no capture inside_interface removes/deletes
  the capture.
  ```

  De gebruiker initieert toepassing X. De ASA beheerder geeft dan de opdracht **opname in_interface uit** en bekijkt de uitvoer.

  ```
  ciscoasa(config)#show capture inside_interface
  1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
  S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
  2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
  S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
  3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
  S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
  ```

Het opgenomen verkeer geeft de beheerder verschillende waardevolle informatie:Doeladres: 172.22.1.1Poortnummer-80/http:Protocol—TCP (noteer de "S" of de systeemvlag)Bovendien weet de beheerder ook dat het gegevensverkeer voor toepassing X in de ASA aankomt.Als de output deze opdrachtoutput van **show** binnenkant_interface was geweest, dan werd het toepassingsverkeer of nooit de ASA bereikt of werd het opnamefilter niet ingesteld om het verkeer op te nemen:

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

In dit geval moet de beheerder overwegen de computer van de gebruiker en om het even welke router of andere netwerkapparaten in het pad tussen de gebruikerscomputer en de ASA te onderzoeken.**Opmerking:** Wanneer het verkeer op een interface aankomt, registreert de opdracht de gegevens voordat een ASA security beleid het verkeer analyseert. Een toegangslijst ontkent bijvoorbeeld al het inkomende verkeer op een interface. De opdracht **opnemen** registreert het verkeer nog. Het ASA-beveiligingsbeleid analyseert dan het verkeer.

- **Debuggen**De beheerder is niet bekend met toepassing X en weet derhalve niet welke van de debug-diensten het mogelijk maakt X-onderzoek toe te passen. Debug is op dit moment mogelijk niet de beste optie voor het oplossen van problemen.

Met de informatie die in Stap 2 wordt verzameld, krijgt de ASA-beheerder verschillende bits waardevolle informatie. De beheerder weet het verkeer aankomt op de binneninterface van de ASA, bron IP adres, bestemming IP adres en de de diensttoepassing X gebruikt (TCP/80). Vanuit de syslogs weet de beheerder ook dat de communicatie aanvankelijk was toegestaan.

Stap 3 - Toepassingsverkeer bevestigen en bewaken

De ASA beheerder wil bevestigen dat het X-verkeer van toepassing de ASA heeft verlaten zowel als elk retourverkeer van de X applicatie server controleert.

- **Controleer de syslogberichten.**Filter syslogberichten voor het bron IP adres (192.168.1.50) of het bestemming IP adres (172.22.1.1). Vanaf de opdrachtregel ziet het filteren van slogberichten er uit als **het registreren | 192.168.1.50 omvatten** of **show logging logging logging | bevat 172.22.1.1**. In dit voorbeeld wordt de opdracht **show logging logging logging logging logging logging** gebruikt zonder filters. De uitvoer wordt onderdrukt om het lezen gemakkelijk te maken.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

Het syslogbericht geeft de verbinding aan die gesloten is vanwege de SYN-onderbreking. Dit vertelt de beheerder dat er geen applicatie X serverreacties werden ontvangen door de ASA. De redenen om het bericht te blokkeren kunnen variëren.De SYN timeout wordt ingelogd vanwege een gedwongen connectie beëindiging na 30 seconden die plaatsvindt na de drierichtingshanddruk voltooiing. Dit probleem doet zich meestal voor als de server niet reageert op een verbindingsverzoek en in de meeste gevallen geen verband houdt met de configuratie op PIX/ASA.Raadpleeg deze controlelijst om dit probleem op te lossen:Zorg

ervoor dat het statische commando correct is ingevoerd en dat het geen overlap maakt met andere statische opdrachten, bijvoorbeeld,

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

Het statische NAT in ASA 8.3 en hoger kan worden geconfigureerd zoals hieronder wordt getoond:

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

Zorg ervoor dat er een toegangslijst bestaat om toegang van buitenaf tot het mondiale IP-adres mogelijk te maken en dat deze aan de interface is gebonden:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

Voor een succesvolle verbinding met de server moet de standaardgateway op de server naar de DMZ-interface van PIX/ASA wijzen.Raadpleeg ASA-systeemmeldingen voor meer informatie over de systeemmeldingen.

- **Maak een nieuw opnamefilter.**Van eerder opgenomen verkeer en syslog berichten weet de beheerder dat toepassing X de ASA door de externe interface moet verlaten.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
!--- When you leave the source as 'any', it allows !--- the administrator to monitor any
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
!--- When you reverse the source and destination information, !--- it allows return traffic
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
interface outside
```

De gebruiker moet een nieuwe sessie met toepassing X starten. Nadat de gebruiker een nieuwe toepassing X sessie is gestart, moet de ASA beheerder de **show opname externe_interface** opdracht geven op de ASA.

```
ciscoasa(config)#show capture outside_interface
3 packets captured
   1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
   2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
   3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

De opname toont verkeer dat de externe interface verlaat maar geeft geen antwoordverkeer weer vanaf de 172.2.1.1 server. Deze opname toont de gegevens zoals het ASA verlaat.

- **Gebruik de optie pakkettracer.**Bij vorige secties heeft de ASA-beheerder genoeg informatie geleerd om de **pakkettracer** optie in de ASA te gebruiken.**Opmerking:** de ASA ondersteunt de **pakkettracer** opdracht beginnend in versie 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any
number can be used. !--- More common source ports typically range !--- between 1025 and
65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC
Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule
Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW
Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type:
ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0
255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-
group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
```

```
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the
next host !--- that should receive the data packet. Result: input-interface: inside input-
status: up input-line-status: up output-interface: outside output-status: up output-line-
status: up Action: allow
```

De belangrijkste output van het **pakje-tracer** bevel is de laatste lijn, die `Actie` is: `Laat maar`.

De drie opties in Stap 3 tonen elke beheerder dat de ASA niet verantwoordelijk is voor de X-problemen van de toepassing. Het X-verkeer van de toepassing verlaat de ASA en de ASA ontvangt geen antwoord van de X-server van de toepassing.

Wat is de volgende?

Er zijn veel componenten waarmee toepassing X voor gebruikers correct kan werken. De componenten omvatten de computer van de gebruiker, de toepassing X client, routing, toegangsbeleid en de toepassing X server. In het vorige voorbeeld hebben we bewezen dat de ASA het X-verkeer van toepassing ontvangt en doorstuurt. De server en toepassing X beheerders moeten nu betrokken worden. Administrateurs moeten verifiëren dat de toepassingsservices worden uitgevoerd, alle logbestanden op de server bekijken en controleren of het gebruikersverkeer wordt ontvangen door de server en toepassing X.

Probleem: Laatste foutmelding van TCP-proxy

U ontvangt deze foutmelding:

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

Oplossing

Uitleg: Dit bericht toont wanneer de limiet van de herassemblagebuffer tijdens het assembleren van TCP segmenten wordt overschreden.

- *source_address/source_port* - Het bronIP-adres en de bronpoort van het pakket waarmee de verbinding wordt gestart.

- *dest_address/dest_port* - Het bestemming IP-adres en de doelpoort van het pakket dat de verbinding initieert.
- *interface_interne* - De naam van de interface waarop het pakje dat de verbinding heeft gestart wordt ontvangen.
- *interface_out* - De naam van de interface waarop het pakket dat de verbinding heeft gestart, wordt afgesloten.
- *limiet* - de geconfigureerde embryonale verbindingsgrens voor de verkeersklasse.

De resolutie voor dit probleem is om de RTSP-inspectie in het beveiligingsapparaat uit te schakelen zoals aangegeven.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

Raadpleeg Cisco bug-ID CSCsl15229 (alleen geregistreerde klanten) voor meer informatie.

Probleem: "%ASA-6-1003: Routing heeft geen volgende hop voor protocol vanuit een src-interface" foutmelding

ASA vermindert verkeer met de `fout:%ASA-6-1003: Routing heeft niet de volgende-hop voor protocol gevonden op basis van src-interface:src IP/src-poort naar testinterface:dest IP/dest poort` foutmelding.

Oplossing

Deze fout komt voor wanneer de ASA probeert om de volgende hop op een interface te vinden die tabel routeert. Meestal wordt dit bericht ontvangen wanneer ASA een vertaling (extensie) op één interface heeft gebouwd en een route op een andere interface wijst. Controleer op een foutieve configuratie van de NAT-verklaringen. De fout kan worden opgelost door een oplossing te vinden voor de verkeerde configuratie.

Probleem: Verbinding geblokkeerd door ASA met " %ASA-5-305013: Asymmetric NAT-regels voor voorwaartse en omgekeerde stromen" foutmelding

De verbinding wordt geblokkeerd door ASA, en deze foutmelding wordt ontvangen:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

Oplossing

Wanneer NAT wordt uitgevoerd, probeert ASA ook het pakket om te keren en controleert of dit elke vertaling raakt. Als de vertaalfunctie van een NAT of een andere NAT niet raakt, zit er een mismatch in. U ziet deze foutmelding het meest wanneer er verschillende NAT-regels zijn ingesteld voor uitgaande en inkomende verkeer met dezelfde bron en bestemming. Controleer de NAT-verklaring voor het betrokken verkeer.

Probleem: Ontvang een fout - %ASA-5-321001: Grenswaarde van 10000 voor het systeem

Oplossing

Deze fout betekent dat de verbindingen voor een server die over een ASA beschikt hun maximum hebben bereikt. Dit kan een indicatie zijn van een DoS-aanval op een server in uw netwerk. Gebruik MPF op de ASA en verlaag de limiet van de embryonale connecties. Schakel ook Dead Connection Detection (DCD) in. Raadpleeg het gedeelte Configuration:

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

Probleem: Ontvang fout %PIX-1-106021: Ontken TCP/UDP reverse path check van src_addr tot dest_addr op interface int_name

Oplossing

Dit logbericht wordt ontvangen wanneer de controle van het omgekeerde pad is ingeschakeld. Geef deze opdracht uit om het probleem op te lossen en blokkeer de controle van het omgekeerde pad:

```
no ip verify reverse-path interface
```

Probleem: Interruptie van internetconnectiviteit door detectie van bedreigingen

Deze foutmelding wordt ontvangen op de ASA:

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
```

```
per second, max configured rate is 5; Cumulative total count is 2526
```

Oplossing

Dit bericht wordt gegenereerd door detectie van bedreigingen vanwege de standaardconfiguratie wanneer een abnormaal verkeersgedrag wordt gedetecteerd. Het bericht richt zich op Miralix Licentie 3000, die een TCP/UDP-poort is. Zoek het apparaat dat poort 3000 gebruikt. Controleer de ASDM grafische statistieken voor bedreigingsdetectie en controleer de topaanvallen om te zien of het poort 3000 en het IP-adres van de bron weergeeft. Als het een legitiem apparaat is, kunt u het basisbedreigingsdetectiesnelheid op ASA verhogen om deze foutmelding op te lossen.

Gerelateerde informatie

- Cisco ASA-opdracht
- Cisco PIX-opdracht Referentie
- Cisco ASA fout- en systeemmeldingen
- Cisco PIX-fout- en systeemmeldingen
- Cisco ASA 5500 Series adaptieve security applicaties
- Cisco PIX 500 Series security applicaties
- Technische ondersteuning en documentatie – Cisco Systems