ASA: Netwerkverkeer vanuit de ASA naar het AIP SSM-configuratievoorbeeld verzenden

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het verzenden van netwerkverkeer dat door de Cisco ASA 5500 Series adaptieve security applicatie (ASA) doorgaat naar de IPS-module (Advanced Inspection and Prevention Security Services Module). Configuratievoorbeelden worden geleverd met de opdrachtregel-interface (CLI).

Raadpleeg ASA: Verzend het netwerkverkeer van de ASA naar het CSC-SSM Configuratievoorbeeld om netwerkverkeer van de Cisco ASA 5500 Series adaptieve security applicatie (ASA) naar de Content Security and Control Services Module (CSC-SSM) te verzenden.

Raadpleeg Virtual Sensors aan een Security Context (alleen AIP SSM) voor meer informatie over het verzenden van netwerkverkeer dat door de Cisco ASA 5500 Series adaptieve security applicatie (ASA) in meerdere contentmodus komt voor de geavanceerde inspectie en preventie security servicesmodule (AIP-SSM) (IPS).

Opmerking: Netwerkverkeer dat door de ASA heen gaat, omvat interne gebruikers die toegang

hebben tot het internet of internetgebruikers die toegang hebben tot door ASA beschermde bronnen in een gedemilitariseerde zone (DMZ) of binnen een netwerk. Netwerkverkeer dat naar en van de ASA wordt verzonden wordt niet naar de IPS-module verzonden voor inspectie. Een voorbeeld van verkeer dat niet naar de IPS module wordt verzonden omvat het pingen (ICMP) van de ASA interfaces of het Telnetting aan de ASA.

Opmerking: Het modulaire beleidskader dat door de ASA wordt gebruikt om verkeer voor inspectie te classificeren, ondersteunt IPv6 niet. Dus als u het IPv6-verkeer via ASA naar het AIP SSM stuurt, wordt dit niet ondersteund.

Opmerking: Raadpleeg voor meer informatie over de initiële configuratie van AIP-SSM de initiële configuratie van de AIP-SSM-sensor.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat het publiek een basisbegrip heeft van de manier waarop u Cisco ASA-software versie 8.x en IPS-softwareversie 6.x kunt configureren.

- De noodzakelijke configuratiecomponenten voor ASA 8.x omvatten interfaces, toegangslijsten, netwerkadresomzetting (NAT) en routing.
- De noodzakelijke configuratiecomponenten voor AIP-SSM (IPS software 6.x) omvatten netwerkinstelling, toegestane hosts, interfaceconconfiguratie, definities van handtekeningen en regels voor gebeurtenis.

Gebruikte componenten

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

- ASA 5510 met softwareversie 8.0.2
- AIP-SSM-10 met IPS-softwareversie 6.1.2

Opmerking: Dit configuratievoorbeeld is compatibel met Cisco ASA 5500 Series Firewall met OS 7.x en hoger en de AIP-SSM module met IPS 5.x en hoger.

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

Configureren

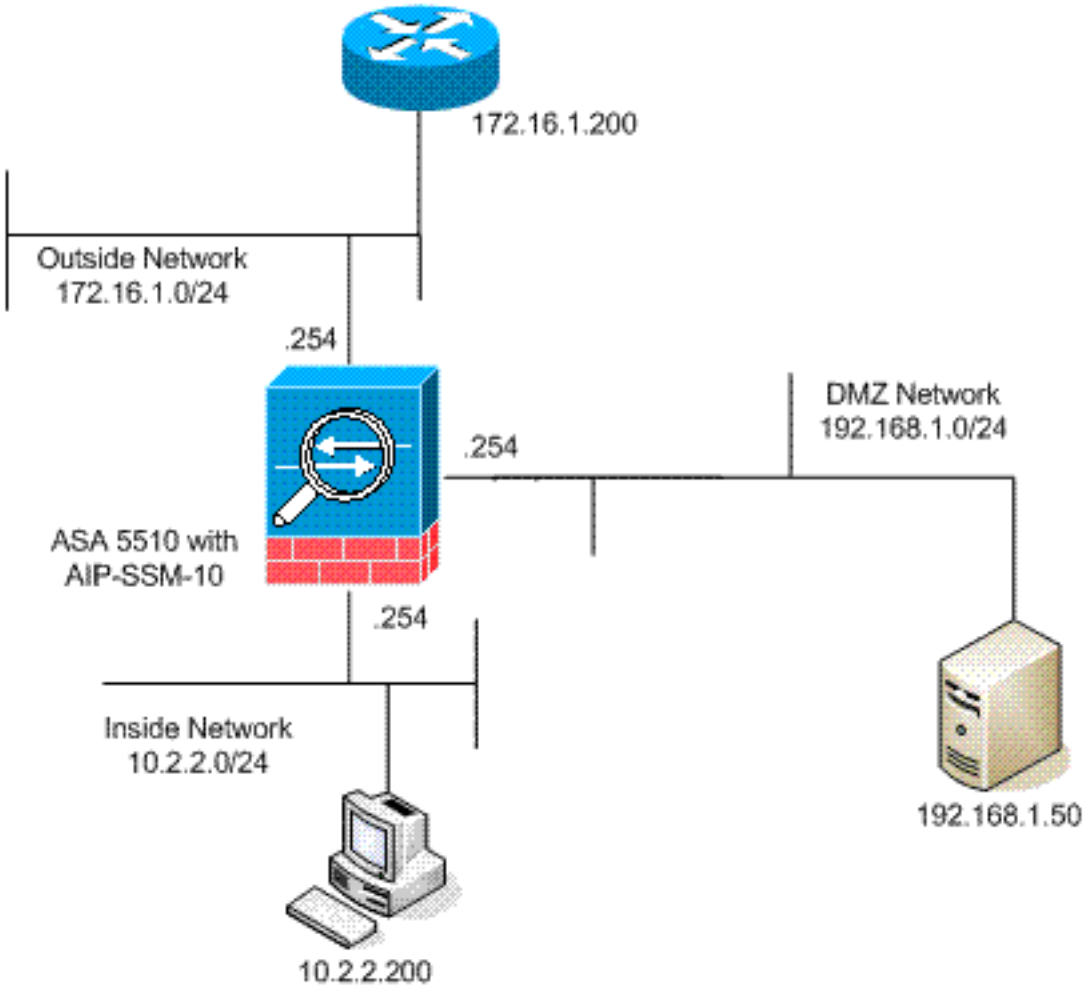
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Initiële configuratie

Dit document gebruikt deze configuraties. Zowel de ASA als AIP-SSM beginnen met een standaardconfiguratie maar hebben specifieke wijzigingen aangebracht voor testdoeleinden. De toevoegingen worden opgemerkt in de configuratie.

- ASA 5510
- AIP-SSM (IPS)

ASA 5510
ciscoasa#**show running-config** : Saved

```
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
!--- IP addressing is added to the default
configuration. interface Ethernet0/0 nameif outside
security-level 0 ip address 172.16.1.254 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 10.2.2.254 255.255.255.0 ! interface
Ethernet0/2 nameif dmz security-level 50 ip address
192.168.1.254 255.255.255.0 ! interface Management0/0
nameif management security-level 0 ip address
172.22.1.160 255.255.255.0 management-only ! passwd
9jNfZuG3TC5tCVH0 encrypted ftp mode passive !--- Access
lists are added in order to allow test !--- traffic
(ICMP and Telnet). access-list acl_outside_in extended
permit icmp any host 172.16.1.50 access-list
acl_inside_in extended permit ip 10.2.2.0 255.255.255.0
any access-list acl_dmz_in extended permit icmp
192.168.1.0 255.255.255.0 any pager lines 24 !---
Logging is enabled. logging enable logging buffered
debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500
mtu management 1500 asdm image disk0:/asdm-613.bin no
asdm history enable arp timeout 14400 !--- Translation
rules are added. global (outside) 1 172.16.1.100 global
(dmz) 1 192.168.1.100 nat (inside) 1 10.2.2.0
255.255.255.0 static (dmz,outside) 172.16.1.50
192.168.1.50 netmask 255.255.255.255 static (inside,dmz)
10.2.2.200 10.2.2.200 netmask 255.255.255.255 !---
Access lists are applied to the interfaces. access-group
acl_outside_in in interface outside access-group
acl_inside_in in interface inside access-group
acl_dmz_in in interface dmz 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 http
server enable http 0.0.0.0 0.0.0.0 dmz 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 !---
Out-of-the-box default configuration includes !---
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 !--- Out-of-the-box default
configuration includes !--- the service-policy
global_policy applied globally. prompt hostname context
. : end
```

AIP SSM (IPS)

```
AIP-SSM#show configuration
! ------------------------------
```

```
! Version 6.1(2)
! Current configuration last modified Mon Mar 23
21:46:47 2009
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
!--- The variables are defined. variables DMZ address
192.168.1.0-192.168.1.255 variables IN address 10.2.2.0-
10.2.2.255 exit ! ------------------------------ service
host network-settings !--- The management IP address is
set. host-ip 172.22.1.169/24,172.22.1.1 host-name AIP-
SSM telnet-option disabled access-list x.x.0.0/16 !---
The access list IP address is removed from the
configuration !--- because the specific IP address is
not relevant to this document. exit time-zone-settings
offset -360 standard-time-zone-name GMT-06:00 exit
summertime-option recurring offset 60 summertime-zone-
name UTC start-summertime month april week-of-month
first day-of-week sunday time-of-day 02:00:00 exit end-
summertime month october week-of-month last day-of-week
sunday time-of-day 02:00:00 exit exit exit ! -----------
------------------- service logger exit ! --------------
---------------- service network-access exit ! ---------
--------------------- service notification exit ! ------
------------------------ service signature-definition
sig0 !--- The signature is modified from the default
setting for testing purposes. signatures 2000 0 alert-
severity high engine atomic-ip event-action produce-
alert|produce-verbose-alert exit alert-frequency
summary-mode fire-all summary-key AxBx exit exit status
enabled true exit exit !--- The signature is modified
from the default setting for testing purposes.
signatures 2004 0 alert-severity high engine atomic-ip
event-action produce-alert|produce-verbose-alert exit
alert-frequency summary-mode fire-all summary-key AxBx
exit exit status enabled true exit exit !--- The custom
signature is added for testing purposes. signatures
60000 0 alert-severity high sig-fidelity-rating 75 sig-
description sig-name Telnet Command Authorization
Failure sig-string-info Command authorization failed
sig-comment signature triggers string command
authorization failed exit engine atomic-ip specify-l4-
protocol yes l4-protocol tcp no tcp-flags no tcp-mask
exit specify-payload-inspection yes regex-string Command
authorization failed exit exit exit exit exit ! --------
---------------------- service ssh-known-hosts exit ! --
---------------------------- service trusted-
certificates exit ! ------------------------------
service web-server enable-tls true exit AIP-SSM#
```

Opmerking: Als u geen toegang hebt tot de AIP-SSM-module met https, dan dient u deze stappen te voltooien:

- Configureer een IP-adres voor het beheer van de module. En u kunt de `lijst van de netwerktoegang` configureren, waarin u de IPs/IP-netwerken specificeert die zijn toegestaan om verbinding te maken met de IP-beheersoftware.
- Zorg dat u de externe Ethernet-interface van de AIP-module hebt aangesloten. De toegang tot de AIP-module is alleen mogelijk via deze interface.

Raadpleeg AIP-SSM initialiseren voor meer informatie.

Controleer al het verkeer met AIP-SSM in de inline of veelbelovende modus

De netwerkbeheerders en de bedrijfsleiding geven vaak aan dat alles moet worden gecontroleerd. Deze configuratie voldoet aan de eis om alles te controleren. Naast het toezicht op alles moeten er twee beslissingen worden genomen over de interactie tussen de ASA en AIP-SSM.

- Is de AIP-SSM-module actief of wordt ingezet in veelbelovende of inline modus?Promiscuous Mode betekent dat een kopie van de gegevens naar het AIP-SSM wordt verzonden terwijl de ASA de oorspronkelijke gegevens naar de bestemming stuurt. Het AIP-SSM in de veelbelovende modus kan worden beschouwd als een inbraakdetectiesysteem (IDS). In deze modus kan het trigger-pakket (het pakket dat het alarm veroorzaakt) nog steeds de bestemming bereiken. Shunning kan plaatshebben en extra pakketten van het bereiken van de bestemming tegenhouden, maar het slagpakket wordt niet gestopt.Inline modus betekent dat de ASA de gegevens voor inspectie naar het AIP-SSM stuurt. Als de gegevens AIP-SSM-inspectie doorgeven, keren de gegevens terug naar de ASA om verder te worden verwerkt en naar de bestemming te worden verzonden. Het AIP-SSM in inline modus kan worden beschouwd als een inbraakpreventiesysteem (IPS). In tegenstelling tot veelbelovende cuous Mode (IPS) kan de inline mode (IPS) feitelijk verhinderen dat het trigger-pakje op de bestemming terechtkomt.
- Als de ASA niet met AIP-SSM kan communiceren, hoe moet de ASA dan omgaan met geïnspecteerd verkeer? Voorbeelden van gevallen waarin de ASA niet met AIP-SSM kan communiceren zijn AIP-SSM-herladingen of als de module niet werkt en vervanging nodig heeft. In dit geval kan de ASA faalopen of faalgesloten worden.Als de unit niet-open is, kan de ASA door blijven gaan naar geïnspecteerd verkeer naar de eindbestemming indien het AIP-SSM niet kan worden bereikt.Gevallen van te inspecteren blokken wanneer de ASA niet met de AIP-SSM kan communiceren.**Opmerking:** Het te inspecteren verkeer wordt gedefinieerd met behulp van een toegangslijst. In deze voorbeelduitvoer, staat de toegang-lijst al IP verkeer van om het even welke bron tot om het even welke bestemming toe. Om die reden kan te inspecteren verkeer alles zijn dat door de ASA loopt.

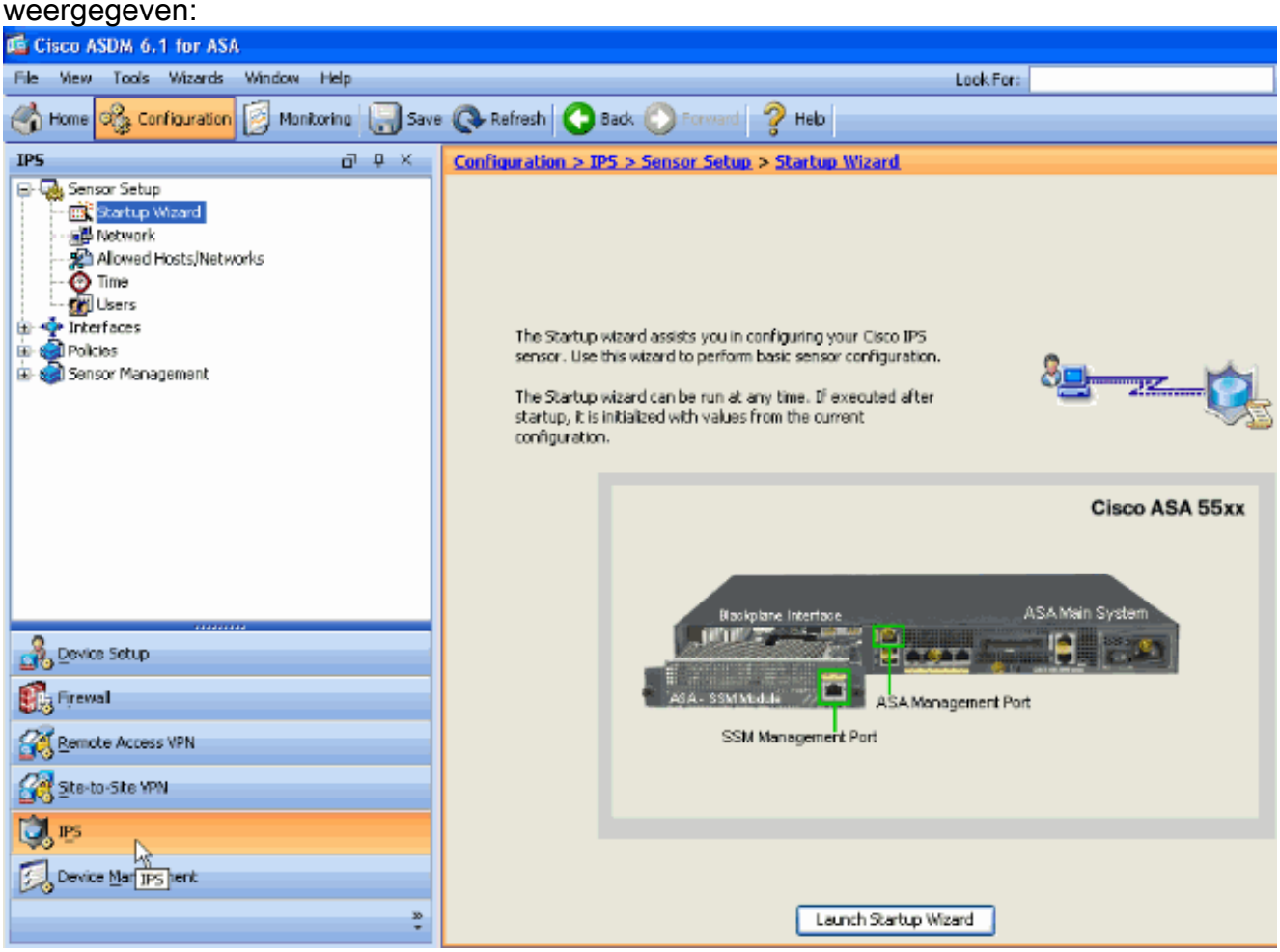
```
ciscoasa(config)#access-list traffic_for_ips permit ip any any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
!--- The match any command can be used in place of !--- the match access-list [access-list name]
command. !--- In this example, access-list traffic_for_ips permits !--- all traffic. The match
any command also !--- permits all traffic. You can use either configuration. !--- When you
define an access-list, it can ease troubleshooting.

ciscoasa(config)#policy-map global_policy
!--- Note that policy-map global_policy is a part of the !--- default configuration. In
addition, policy-map global_policy !--- is applied globally with the service-policy command.

ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
```

```
!--- Two decisions need to be made. !--- First, does the AIP-SSM function !--- in inline or
promiscuous mode? !--- Second, does the ASA fail-open or fail-closed? ciscoasa(config-pmap-
c)#ips promiscous fail-open
!--- If AIP-SSM is in promiscous mode, issue !--- the no ips promiscous fail-open command !---
in order to negate the command and then use !--- the ips inline fail-open command.
```

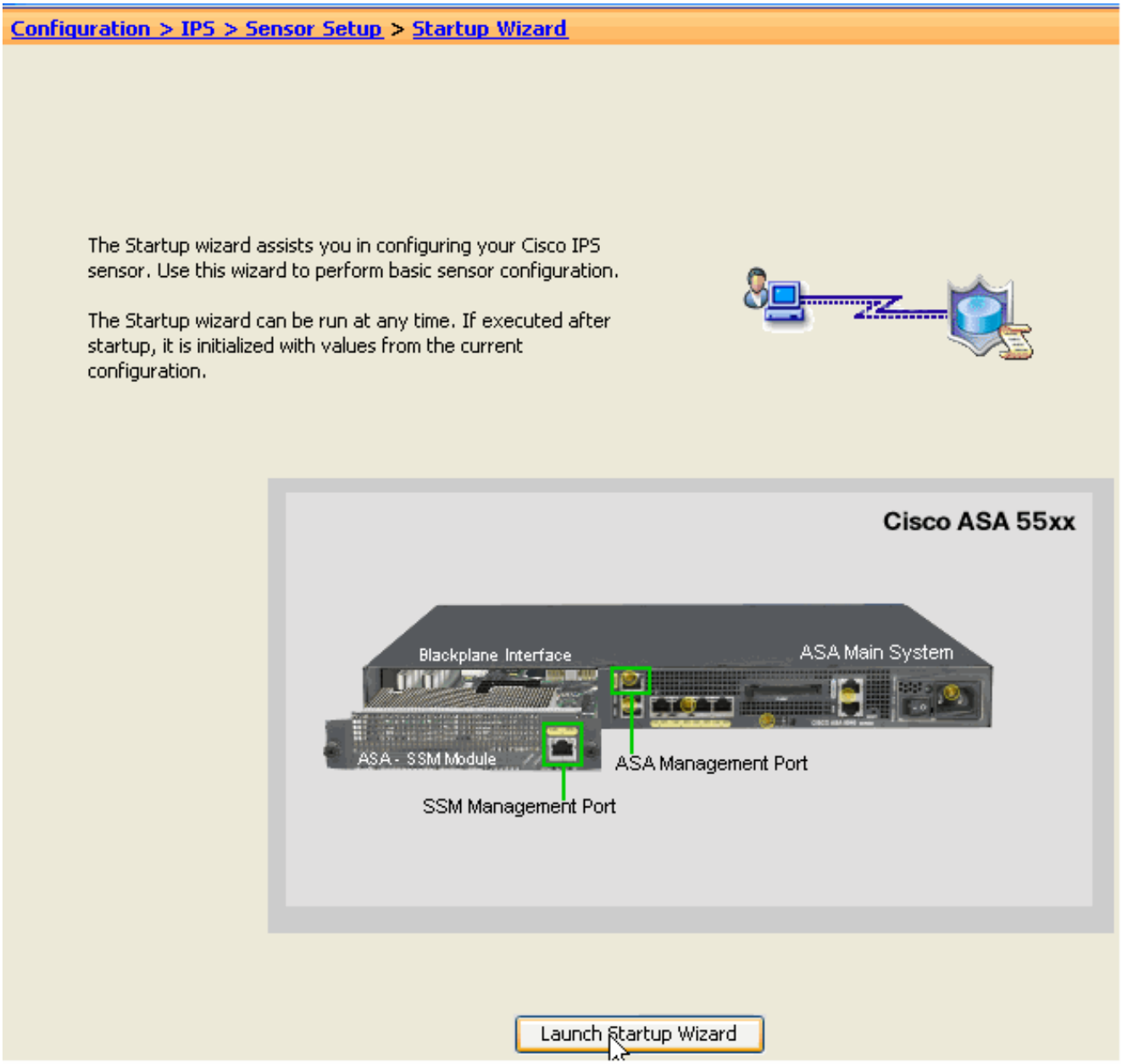
Controleer al verkeer met AIP-SSM door ASDM te gebruiken

Voltooi deze stappen om al het verkeer met AIP-SSM dat ASDM gebruikt te inspecteren:

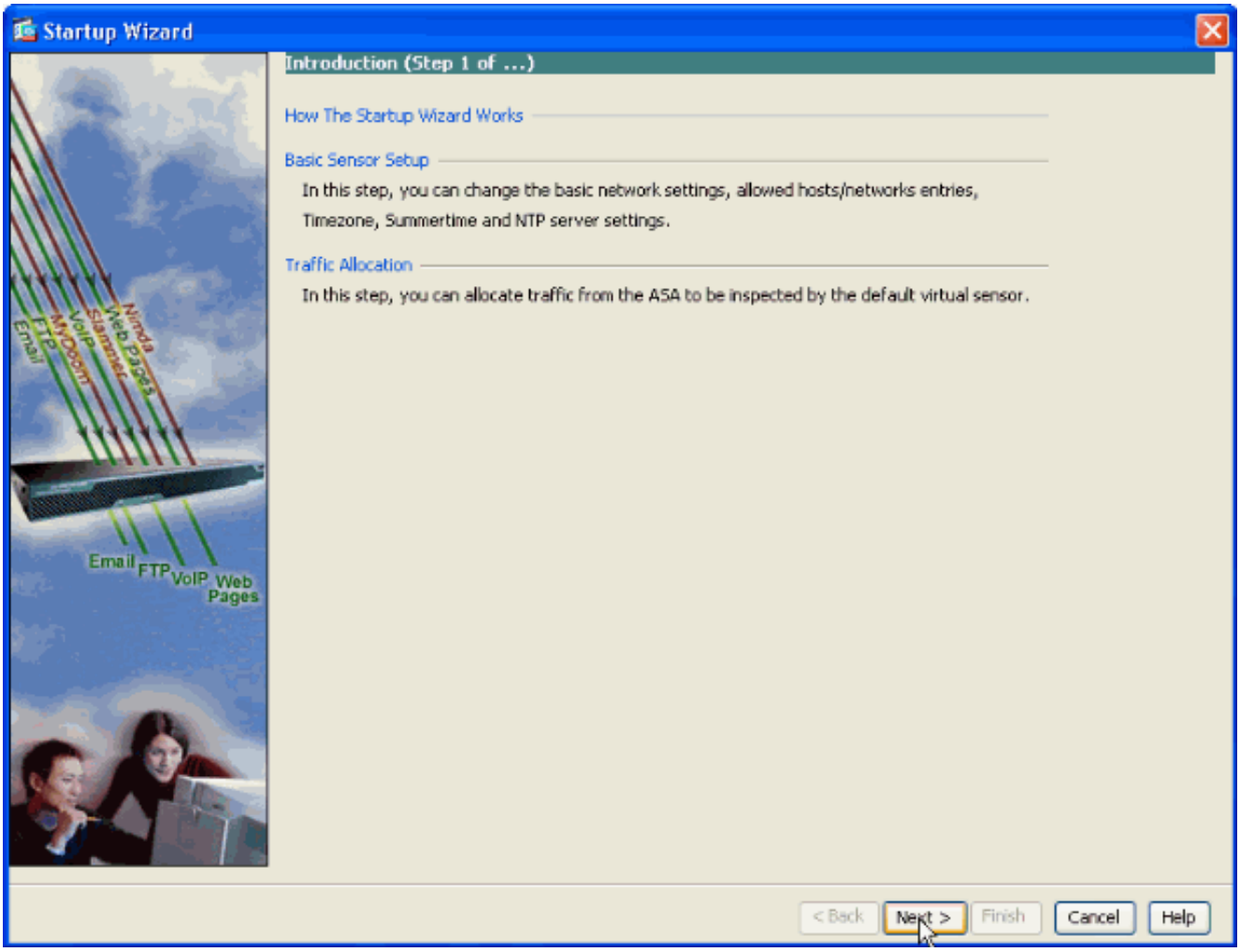
1. Kies **Configuratie > IPS > Sensor Setup > Opstartwizard** in ASDM startpagina om de configuratie te starten, zoals wordt weergegeven:



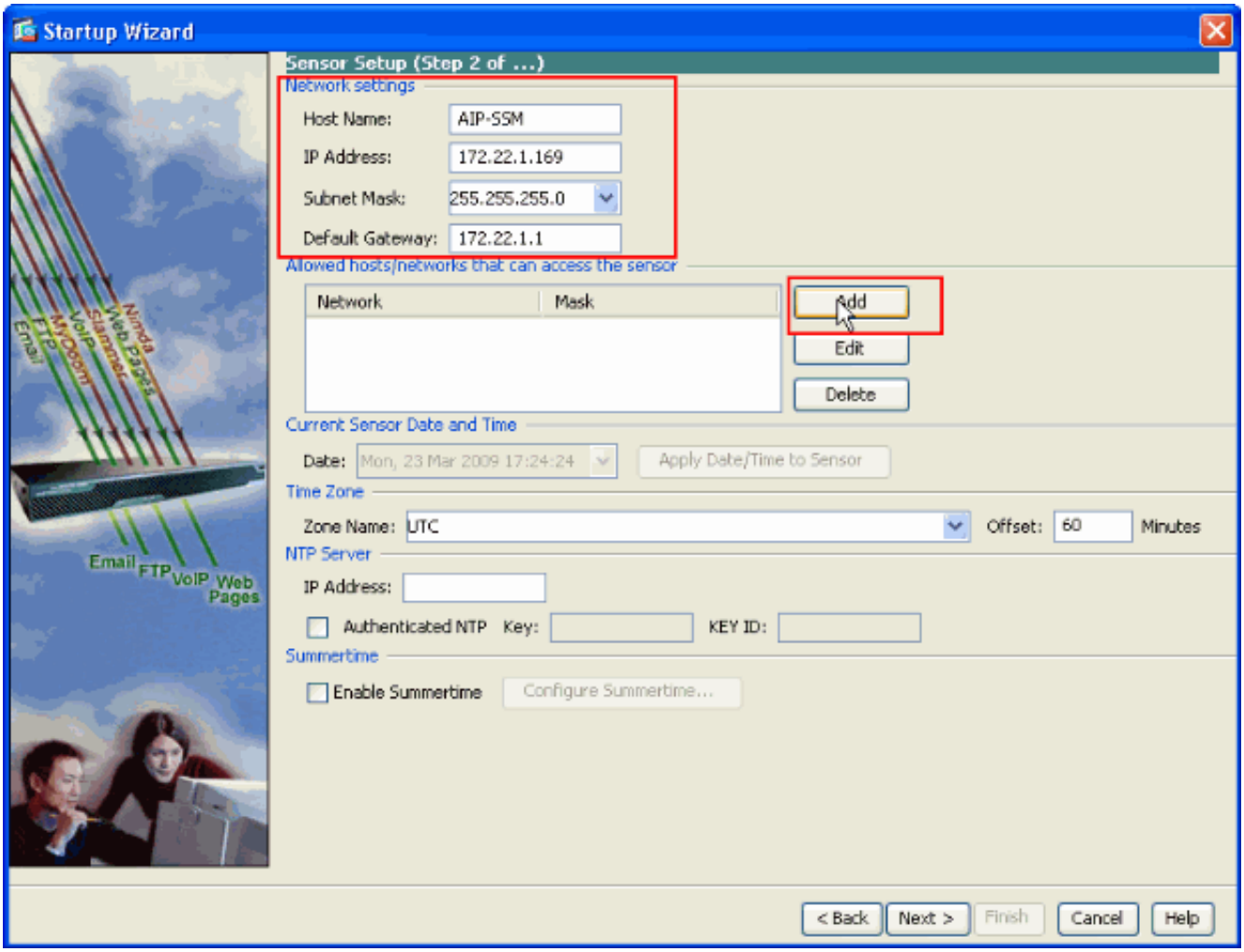
2. Klik op **Opstartwizard starten**.



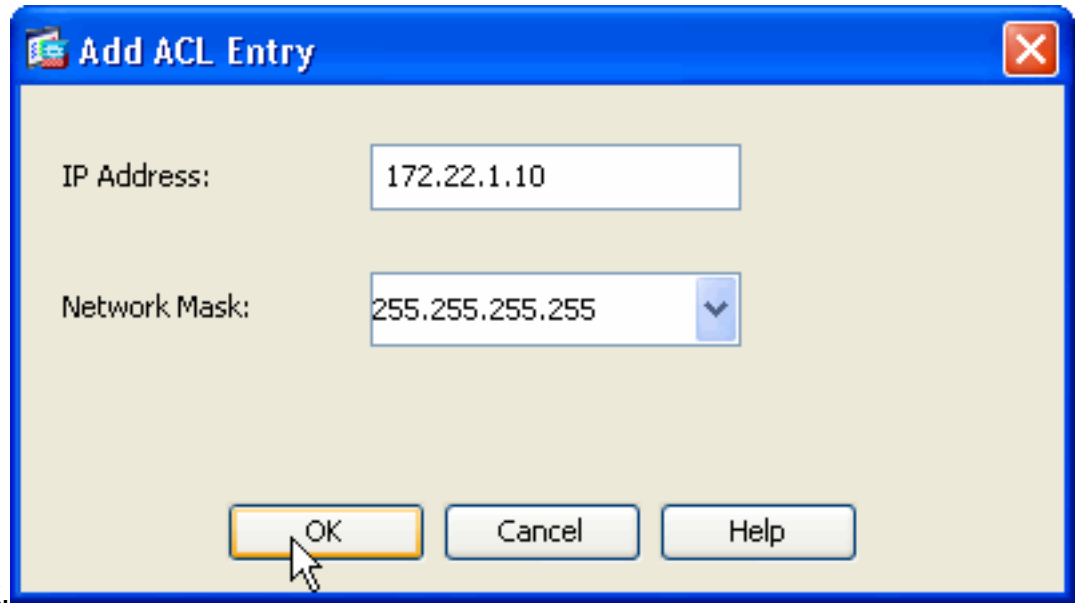
3. Klik op **Volgende** in het nieuwe venster dat verschijnt nadat u de opstartwizard hebt gestart.



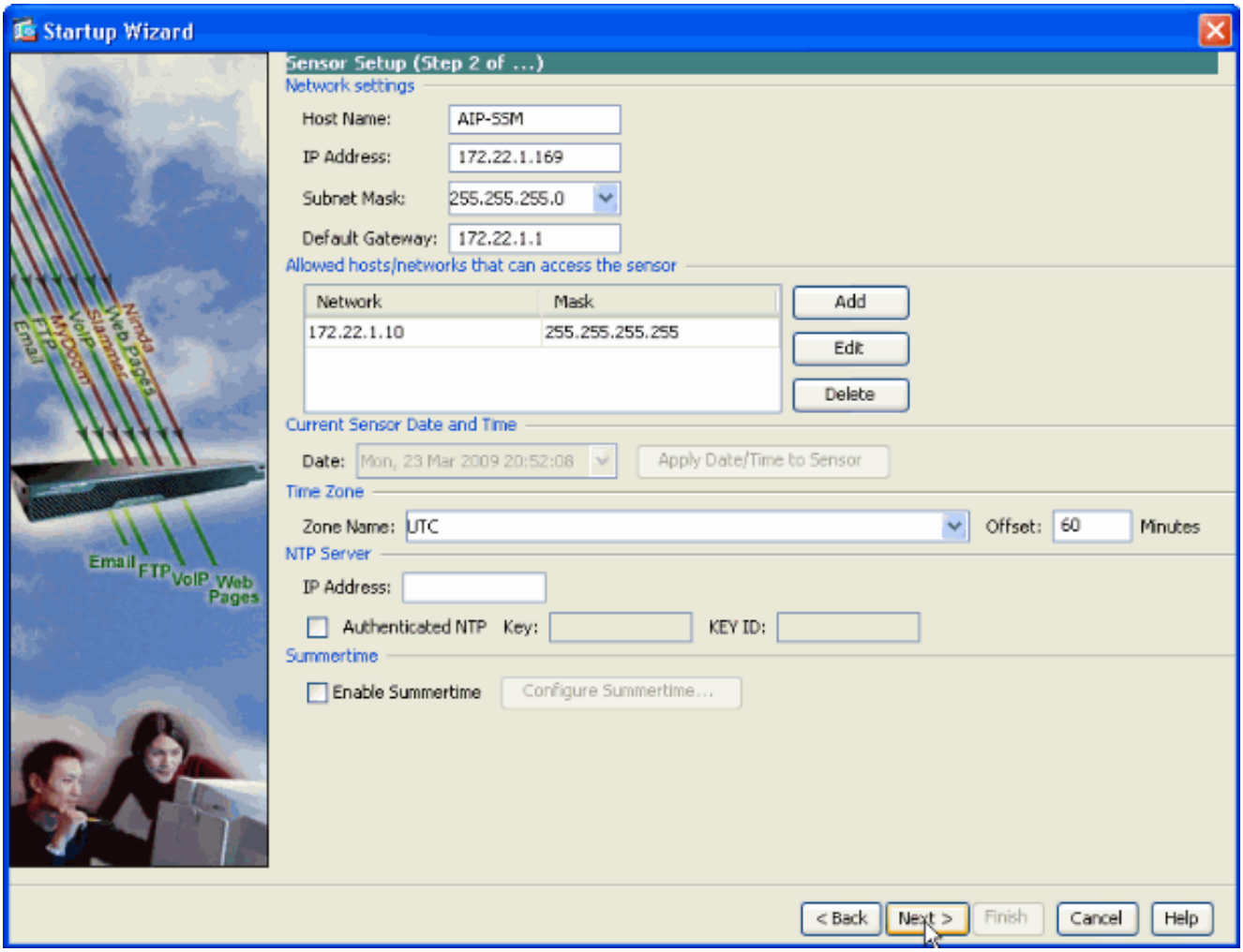
4. Typ in het nieuwe venster de naam van de host, het IP-adres, het subnetmasker en het standaardadres van de gateway voor de AIP-SSM-module in de respectievelijke ruimte die in het gedeelte Netwerkinstellingen is voorzien. Klik vervolgens op **Add** om de toegangslijsten toe te voegen om al verkeer met AIP-SSM toe te staan.



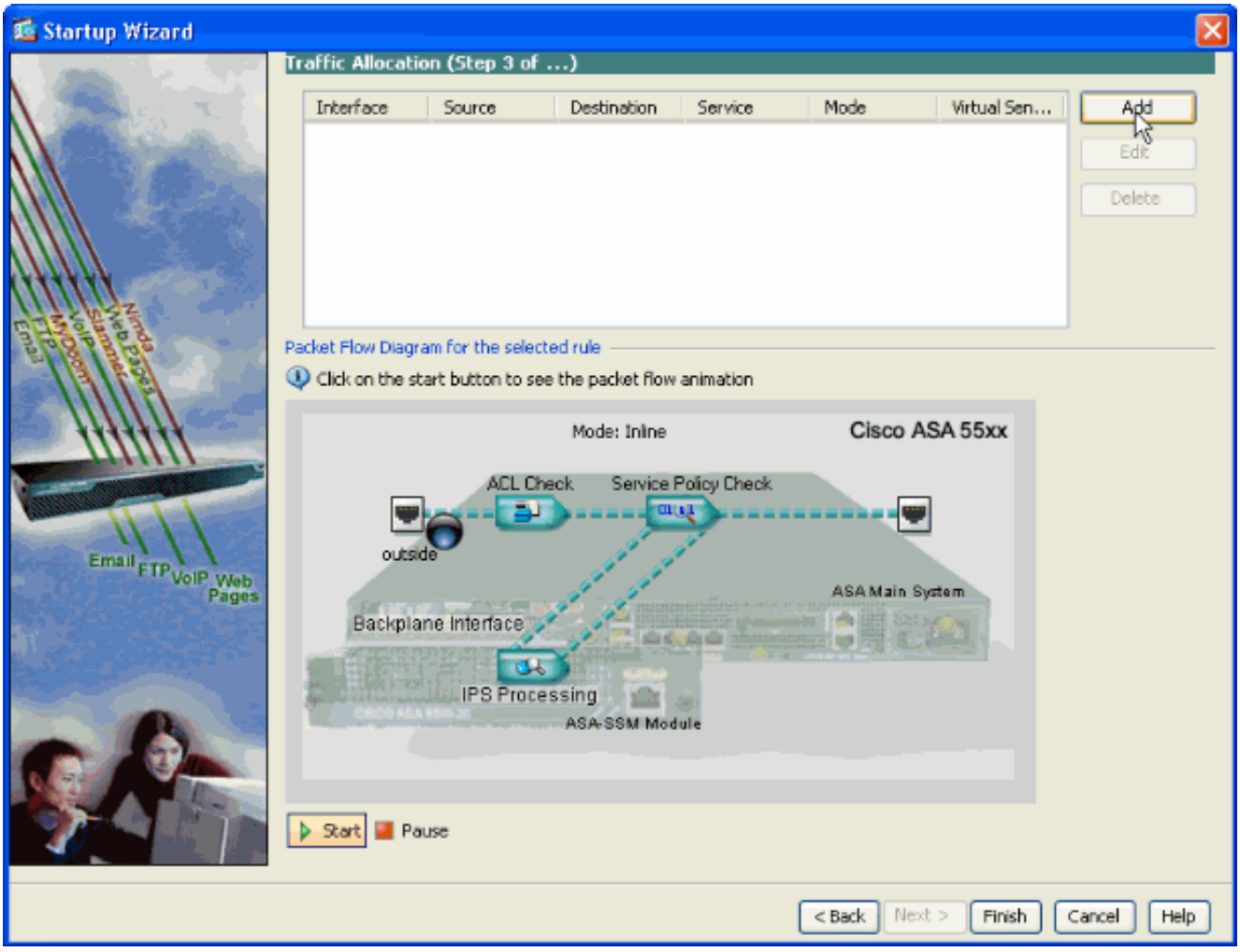
5. In het venster Toegang tot **ACL toevoegen** typt u het **IP-adres** en de informatie over **netwerkmasker** van de hosts/netwerken die toegang tot de sensor moeten hebben. Klik op OK.**Opmerking:** Het IP-adres van de host/het netwerk moet behoren tot het adresbereik van het beheernetwerk.



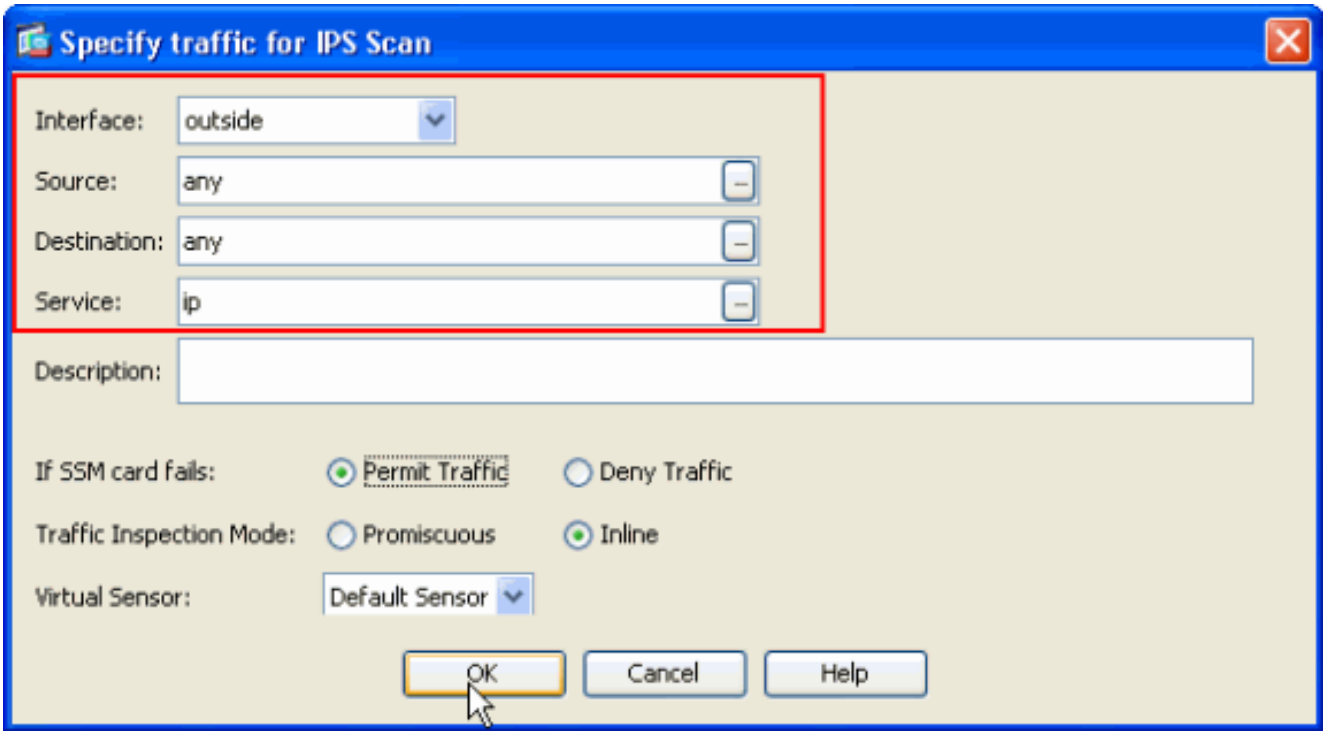
6. Klik op **Volgende** nadat u de details in de opgegeven ruimtes hebt opgegeven.



7. Klik op **Add** om de details van de verkeerstoewijzing te configureren.

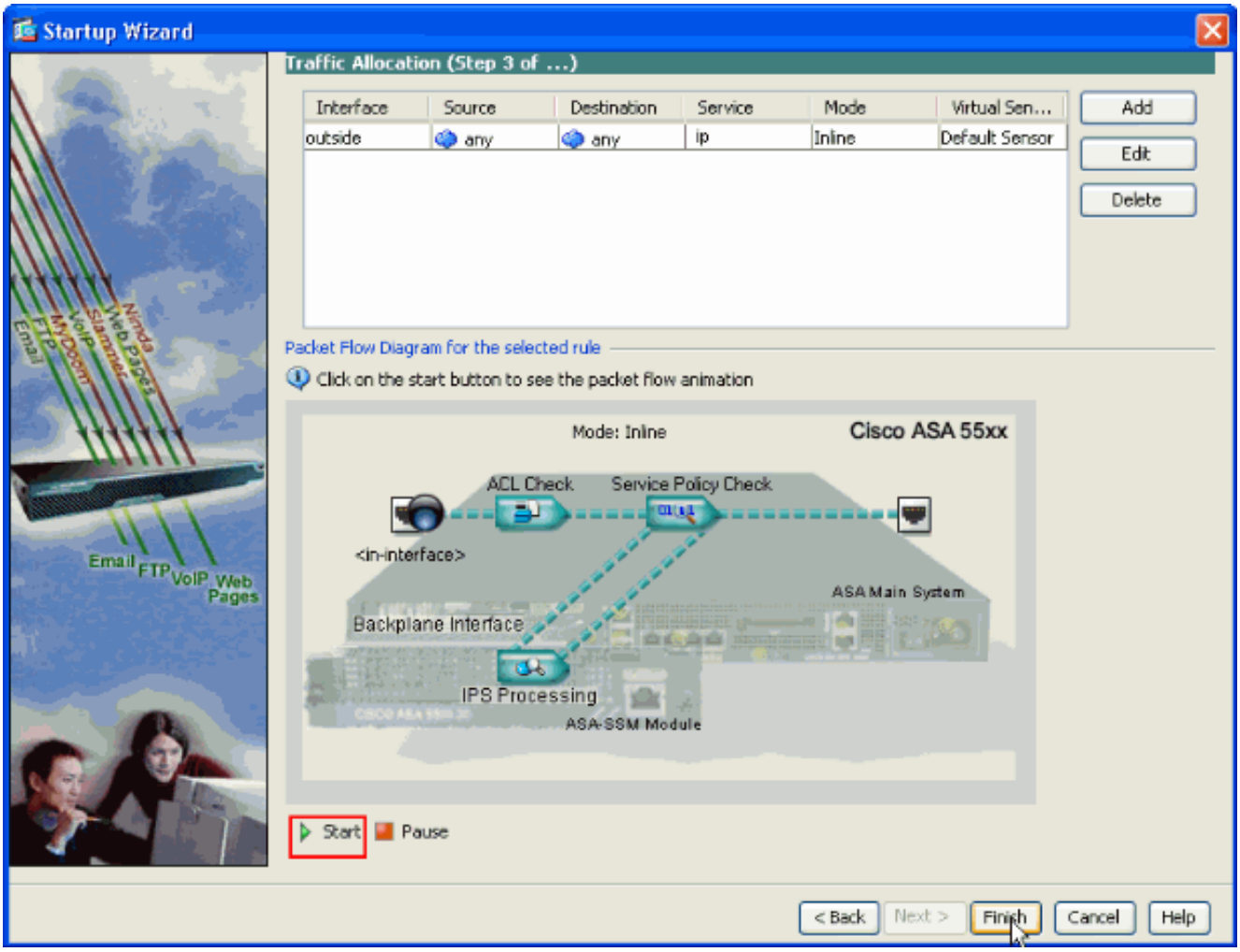


8. Geef de bron en het doelnetwerkadres op en ook het type service dat hier bijvoorbeeld IP wordt gebruikt. In dit voorbeeld wordt **elke** toepassing gebruikt voor bron en bestemming terwijl u al het verkeer met AIP-SSM inspecteert. Klik vervolgens op **OK**.



9. De ingestelde regels voor verkeerstoewijzing worden in dit venster weergegeven en u kunt zoveel regels toevoegen als nodig is als u dezelfde procedure hebt voltooid als wordt uitgelegd in stappen 7 en 8. Klik vervolgens op **Voltooien** en dit voltooit de ASDM

Configuration-procedure.**N.B.:** U kunt de pakketdoorvoeranimatie bekijken als u op **Start** klikt.



Controleer specifiek verkeer met AIP-SSM

Als de netwerkbeheerder de AIP-SSM monitor als een subset van al verkeer wil hebben, heeft de ASA twee onafhankelijke variabelen die kunnen worden aangepast. Eerst kan de toegangslijst worden geschreven om het benodigde verkeer op te nemen of uit te sluiten. Naast de wijziging van toegangslijsten kan een **dienstenbeleid** worden toegepast op een interface of mondiaal om het door het AIP-SSM geïnspecteerde verkeer te wijzigen.

Met verwijzing naar het netwerkdiagram in dit document wil de netwerkbeheerder het AIP-SSM om *al* het verkeer tussen het externe netwerk en DMZ-netwerk te controleren.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip any 192.168.1.0 255.255.255.0
ciscoasa(config)#access-list traffic_for_ips deny ip 192.168.1.0 255.255.255.0 10.2.2.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 192.168.1.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface dmz
```

```
!--- The access-list denies traffic from the inside network to the DMZ network !--- and traffic
to the inside network from the DMZ network. !--- In addition, the service-policy command is
applied to the DMZ interface.
```

Vervolgens wil de netwerkbeheerder AIP-SSM het verkeer dat van het binnennetwerk naar het externe netwerk *is* gestart, bewaken. Binnennetwerk naar DMZ wordt niet bewaakt.

Opmerking: Deze specifieke sectie vereist een middelmatig begrip van status, TCP, UDP, ICMP, verbinding en connectioneloze communicatie.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 10.2.2.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface inside
```

De toegangslijst ontkent verkeer dat op het binnennetwerk wordt geïnitieerd dat voor het netwerk DMZ bestemd is. De tweede toegangslijst lijnvergunningen of stuurt verkeer dat op het binnennetwerk wordt geïnitieerd voor het buitennetwerk naar AIP-SSM. Op dit moment speelt de status van de ASA in. Bijvoorbeeld, initieert een interne gebruiker een TCP verbinding (Telnet) aan een apparaat op het buitennetwerk (router). De gebruiker sluit zich aan op de router en logt in. De gebruiker geeft dan een routeropdracht uit die niet is geautoriseerd. De router reageert met `gefaalde` toestemming. Het gegevenspakket dat de `Opdrachtautorisatie` bevat `mislukte` string heeft een bron van de externe router en een bestemming van de interne gebruiker. De bron (buiten) en de bestemming (binnen) komen niet overeen met de toegangslijsten die eerder in dit document zijn gedefinieerd. ASA houdt stateful connecties bij, daarom wordt het gegevenspakket dat terugkeert (buiten naar binnen) naar AIP-SSM verzonden voor inspectie. Aangepaste handtekening 60000 0, dat op het AIP-SSM-alarm is ingesteld.

Opmerking: de standaardinstelling is dat de ASA de status niet behoudt voor ICMP-verkeer. In de vorige voorbeeldconfiguratie, de interne gebruiker pings (verzoek van de echo van ICMP) de externe router. De router reageert met een echo-antwoord van ICMP. AIP-SSM inspecteert het echo-verzoekpakket maar niet het echo-antwoordpakket. Als de ICMP-inspectie op de ASA is ingeschakeld, worden zowel het echo-verzoek als de echo-antwoordpakketten gecontroleerd door AIP-SSM.

sluiten specifiek netwerkverkeer uit van AIP-SSM-scannen

Het gegeven algemene voorbeeld geeft een visie op het vrijstellen van specifiek verkeer dat gescand moet worden door AIP-SSM. Om dit te kunnen uitvoeren, moet u een toegangslijst maken die de verkeersstroom bevat die van AIP-SSM-scannen moet worden uitgesloten. In dit voorbeeld is IPS de naam van de access-list die de verkeersstroom definieert die door AIP-SSM gescand wordt. Verkeer tussen <bron> en <bestemming> wordt niet gescand. al het andere verkeer wordt geïnspecteerd .

```
access-list IPS deny IP <source> <destination>
access-list IPS permit ip any any
```

```
!
class-map my_ips_class
  match access-list IPS
!
!
policy-map my-ids-policy
  class my-ips-class
   ips inline fail-open
```

Verifiëren

Controleer dat alarmgebeurtenissen worden geregistreerd in het AIP-SSM.

Log in op het AIP-SSM met de Administrator-gebruikersaccount. De opdracht **Show events alert** genereert deze uitvoer.

Opmerking: de uitvoer varieert op basis van signatuur, het type verkeer dat naar AIP-SSM wordt verzonden en de netwerkbelasting.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

```
show events alert

evIdsAlert: eventId=1156198930427770356 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 22:52:57 2006/08/24 17:52:57 UTC
  signature: description=Telnet Command Authorization Failure id=60000 version=custom
    subsigId: 0
    sigDetails: Command authorization failed
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 172.16.1.200
      port: 23
    target:
      addr: locality=IN 10.2.2.200
      port: 33189
  riskRatingValue: 75
  interface: ge0_1
  protocol: tcp


evIdsAlert: eventId=1156205750427770078 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC
  signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
```

```
      addr: locality=OUT 172.16.1.200
    target:
      addr: locality=DMZ 192.168.1.50
  triggerPacket:
000000  00 16 C7 9F 74 8C 00 15  2B 95 F9 5E 08 00 45 00  ....t...+..^..E.
000010  00 3C 2A 57 00 00 FF 01  21 B7 AC 10 01 C8 C0 A8  .<*W....!.......
000020  01 32 08 00 F5 DA 11 24  00 00 00 01 02 03 04 05  .2.....$........
000030  06 07 08 09 0A 0B 0C 0D  0E 0F 10 11 12 13 14 15  ................
000040  16 17 18 19 1A 1B 1C 1D  1E 1F                    ..........
  riskRatingValue: 100
  interface: ge0_1
  protocol: icmp


evIdsAlert: eventId=1156205750427770079 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC
  signature: description=ICMP Echo Reply id=2000 version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=DMZ 192.168.1.50
    target:
      addr: locality=OUT 172.16.1.200
  triggerPacket:
000000  00 16 C7 9F 74 8E 00 03  E3 02 6A 21 08 00 45 00  ....t.....j!..E.
000010  00 3C 2A 57 00 00 FF 01  36 4F AC 10 01 32 AC 10  .<*W....6O...2..
000020  01 C8 00 00 FD DA 11 24  00 00 00 01 02 03 04 05  .......$........
000030  06 07 08 09 0A 0B 0C 0D  0E 0F 10 11 12 13 14 15  ................
000040  16 17 18 19 1A 1B 1C 1D  1E 1F                    ..........
  riskRatingValue: 100
  interface: ge0_1
  protocol: icmp
```

In de steekproefformaties worden verschillende IPS-handtekeningen aangepast om op testverkeer te alarmeren. Handtekening 2000 en 2004 worden gewijzigd. Aangepaste handtekening 60000 wordt toegevoegd. In een labomgeving of een netwerk waar weinig gegevens door de ASA passeren, kan het nodig zijn om handtekeningen aan te passen om gebeurtenissen te veroorzaken. Als de ASA en AIP-SSM worden ingezet in een omgeving die een grote hoeveelheid verkeer doorgeeft, zullen de standaardinstellingen voor de handtekening waarschijnlijk een gebeurtenis genereren.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

Geef deze **show** opdrachten van de ASA uit.

- **toon module**—geeft informatie over het SSM op de ASA evenals systeeminformatie weer.
  `ciscoasa#show module`

```
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5510 Adaptive Security Appliance         ASA5510            JMX0935K040
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         JAB09440271

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 0012.d948.e912 to 0012.d948.e916  1.0          1.0(10)0     8.0(2)
  1 0013.c480.cc18 to 0013.c480.cc18  1.0          1.0(10)0     6.1(2)E3

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               6.1(2)E3

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
!--- Each of the areas highlighted indicate that !--- the ASA recognizes the AIP-SSM and the
AIP-SSM status is up.
```

- **show run**

```
ciscoasa#show run
!--- Output is suppressed. access-list traffic_for_ips extended permit ip any any ... class-
map ips_class_map match access-list traffic_for_ips ... policy-map global_policy ... class
ips_class_map ips inline fail-open ... service-policy global_policy global !--- Each of
these lines are needed !--- in order to send data to the AIP-SSM.
```

- **Toon toegang-lijst**-Toont de tellers voor een toegang-lijst.

```
ciscoasa#show access-list traffic_for_ips
access-list traffic_for_ips; 1 elements
access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286
!--- Confirms the access-list displays a hit count greater than zero.
```

Voordat u AIP-SSM installeert en gebruikt, gaat het netwerkverkeer door de ASA zoals verwacht? Als niet, kan het noodzakelijk zijn om het netwerk en de regels van het ASA toegangsbeleid problemen op te lossen.

Problemen met failover

- Als u twee ASA's in een failover-configuratie hebt en elk een AIP-SSM heeft, **moet** u de configuratie van de AIP-SSM's handmatig reproduceren. Alleen de configuratie van de ASA wordt gerepliceerd door het overnamemechanisme. AIP-SSM is niet in de failover opgenomen. Raadpleeg PIX/ASA 7.x Active/Standby-failover Configuration Voorbeeld voor meer informatie over failover-problemen.
- AIP-SSM neemt niet deel aan stateful failover als stateful failover is ingesteld op het ASA failover-paar.

Foutberichten

De IPS Module (AIP-SSM) produceert foutmeldingen zoals getoond en niet afgevinkt.

```
07Aug2007 18:59:50.468 0.757 interface[367] Cid/W errWarning Inline
data bypass has started.

  07Aug2007 18:59:59.619 9.151 mainApp[418] cplane/E Error during socket
read

  07Aug2007 19:03:13.219 193.600 nac[373] Cid/W errWarning New host ip
```

```
[192.168.101.76]

  07Aug2007 19:06:13.979 180.760 sensorApp[417] Cid/W errWarning
unspecifiedWarning:There are no interfaces assigned to any virtual
sensors. This can result in some packets not being monitored.

  07Aug2007 19:08:42.713 148.734 mainApp[394] cplane/E Error - accept()
call returned -1

  07Aug2007 19:08:42.740 0.027 interface[367] Cid/W errWarning Inline
data bypass has started.
```

De oorzaak van deze foutmelding is dat de IPS virtuele sensor niet is toegewezen aan de backplane interface van de ASA. De ASA is op de juiste manier ingesteld om verkeer naar de SSM-module te sturen, maar u moet de virtuele sensor toewijzen aan de backplane interface die de ASA maakt, zodat het SSM het verkeer kan scannen.

```
errorMessage: IpLogProcessor::addIpLog: Ran out of file descriptors  name=errWarn

errorMessage: IpLog 1701858066 terminated early due to lack of file handles.
name=ErrLimitExceeded
```

Deze berichten duiden erop dat IP-LOGGING is ingeschakeld, waardoor op hun beurt alle systeembronnen zijn opgepot. Cisco raadt aan IP LOGGING uit te schakelen omdat deze alleen mag worden gebruikt voor problemen/onderzoeksdoeleinden.

Opmerking: De `errWarning Inline data bypass is begonnen` met een foutmelding omdat de sensor de analysemachine tijdelijk opnieuw start na de signatuur-update, wat een noodzakelijk onderdeel is van het signatuur-update.

Ondersteuning van SLOG

Het AIP-SSM ondersteunt syslog niet als alarmformaat.

De standaardmethode om alarminformatie van AIP-SSM te ontvangen is door Security Devices Exchange (SDEE). Een andere optie is om individuele handtekeningen te configureren om een SNMP-val te genereren als een actie die moet worden ondernomen wanneer ze geactiveerd worden.

AIP-SSM-herstart

De AIP-SSM-module reageert niet goed.

Als de AIP-SSM-module niet correct reageert, start u de AIP-SSM-module opnieuw op zonder de ASA-module opnieuw op te starten. Gebruik de opdracht herladen **van module 1** om de AIP-SSM-module opnieuw op te starten en ASA niet opnieuw op te starten.

Waarschuwingen voor AIP-SSM

Kan AIP-SSM e-mailberichten naar gebruikers sturen?

Nee, het wordt niet ondersteund.

Gerelateerde informatie

- Cisco Security Appliance Opdracht Ref, versie 7.2
- Cisco Security applicatie System Log Messaging, versie 7.2
- Opdrachtreferentie voor Cisco-inbraakpreventiesysteem 5.1
- Technische ondersteuning en documentatie – Cisco Systems