ASA: Netzwerkverkehr von der ASA an das AIP SSM-Konfigurationsbeispiel senden

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für das Senden von Netzwerkverkehr, der über die Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 an das Advanced Inspection and Prevention Security Services Module (AIP-SSM)-Modul (IPS) geleitet wird. Konfigurationsbeispiele werden über die Befehlszeilenschnittstelle (CLI) bereitgestellt.

Weitere Informationen finden Sie unter ASA: Senden Sie Netzwerkverkehr von der ASA an das CSC-SSM-Konfigurationsbeispiel, um Netzwerkverkehr von der Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 an das Content Security and Control Security Services Module (CSC-SSM) zu senden.

Unter Zuweisen virtueller Sensoren zu einem Sicherheitskontext (nur AIP SSM) finden Sie weitere Informationen zum Senden von Netzwerkverkehr, der über die Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 im Multiple-Context-Modus zum Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS)-Modul geleitet wird.

Hinweis: Netzwerkverkehr, der die ASA passiert, umfasst interne Benutzer, die auf das Internet zugreifen, oder Internetbenutzer, die auf durch ASA geschützte Ressourcen in einer demilitarisierten Zone (DMZ) oder im Netzwerk zugreifen. Netzwerkverkehr, der von und an die ASA gesendet wird, wird nicht zur Prüfung an das IPS-Modul gesendet. Ein Beispiel für Datenverkehr, der nicht an das IPS-Modul gesendet wird, ist Ping (ICMP) an den ASA-Schnittstellen oder Telnet an die ASA.

Hinweis: Das modulare Richtlinien-Framework, das von der ASA zur Klassifizierung des Datenverkehrs zur Überprüfung verwendet wird, unterstützt IPv6 nicht. Wenn Sie also den IPv6-Datenverkehr über ASA an das AIP SSM umleiten, wird er nicht unterstützt.

Hinweis: Weitere Informationen zur Erstkonfiguration von AIP-SSM finden Sie unter Erstkonfiguration des AIP-SSM-Sensors.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Zielgruppe grundlegende Kenntnisse über die Konfiguration der Cisco ASA Software Version 8.x und der IPS-Software Version 6.x hat.

- Die erforderlichen Konfigurationskomponenten für ASA 8.x umfassen Schnittstellen, Zugriffslisten, Network Address Translation (NAT) und Routing.
- Zu den erforderlichen Konfigurationskomponenten für die AIP-SSM (IPS Software 6.x) gehören die Netzwerkeinrichtung, zulässige Hosts, die Schnittstellenkonfiguration, Signaturdefinitionen und Ereignishandlungsregeln.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA 5510 mit Softwareversion 8.0.2
- AIP-SSM-10 mit IPS-Software, Version 6.1.2

Hinweis: Dieses Konfigurationsbeispiel ist mit jeder Firewall der Cisco Serie ASA 5500 ab OS 7.x und dem AIP-SSM-Modul ab IPS 5.x kompatibel.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

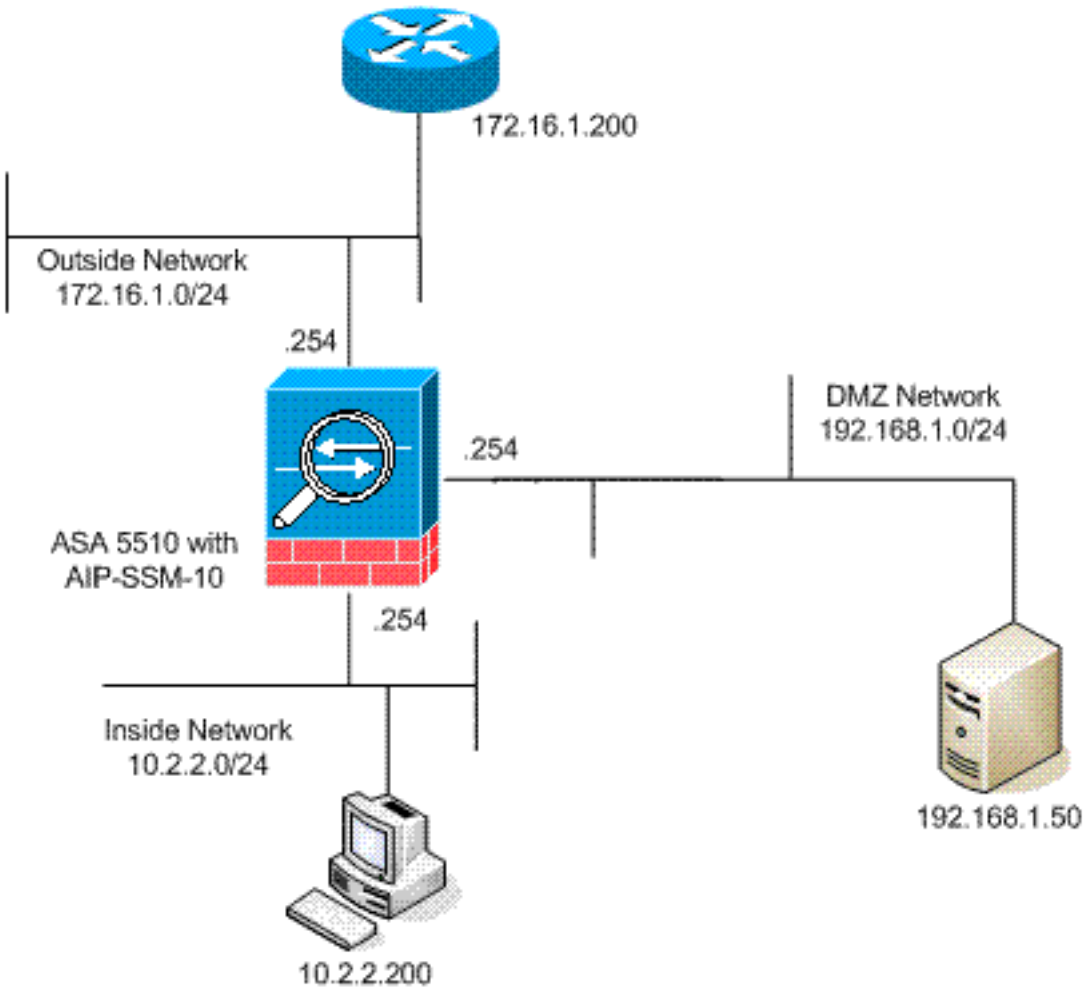
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Erstkonfiguration

In diesem Dokument werden diese Konfigurationen verwendet. Sowohl ASA als auch AIP-SSM beginnen mit einer Standardkonfiguration, haben jedoch spezifische Änderungen zu Testzwecken vorgenommen. Ergänzungen sind in der Konfiguration aufgeführt.

- 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#
```

Hinweis: Wenn Sie mit https nicht auf das AIP-SSM-Modul zugreifen können, gehen Sie wie folgt vor:

- Konfigurieren Sie eine Management-IP-Adresse für das Modul. Außerdem können Sie die `Netzwerkzugriffsliste` konfigurieren, in der Sie die IPs/IP-Netzwerke angeben, die mit der Management-IP verbunden werden dürfen.
- Stellen Sie sicher, dass Sie die externe Ethernet-Schnittstelle des AIP-Moduls angeschlossen haben. Managementzugriff auf das AIP-Modul ist nur über diese Schnittstelle möglich.

Weitere Informationen finden Sie unter Initialisieren von AIP-SSM.

AIP-SSM im Inline- oder Promiscous-Modus für die Überprüfung des gesamten Datenverkehrs

Netzwerkadministratoren und die Unternehmensleitung geben häufig an, dass alles überwacht werden muss. Diese Konfiguration erfüllt die Anforderung, alles zu überwachen. Neben der Überwachung müssen zwei Entscheidungen bezüglich der Interaktion zwischen ASA und AIP-SSM getroffen werden.

- Funktioniert das AIP-SSM-Modul oder wird es im Promiscuous- oder Inline-Modus bereitgestellt?Der Promiscuous-Modus bedeutet, dass eine Kopie der Daten an das AIP-SSM gesendet wird, während die ASA die ursprünglichen Daten an das Ziel weiterleitet. Das AIP-SSM im Promiscuous-Modus kann als Intrusion Detection System (IDS) angesehen werden. In diesem Modus kann das Triggerpaket (das Paket, das den Alarm auslöst) immer noch das Ziel erreichen. Das Shunking kann stattfinden und verhindern, dass zusätzliche Pakete das Ziel erreichen, aber das Trigger-Paket wird nicht gestoppt.Der Inline-Modus bedeutet, dass die ASA die Daten zur Prüfung an das AIP-SSM weiterleitet. Wenn die Daten die AIP-SSM-Prüfung bestehen, werden sie an die ASA zurückgegeben, um die Verarbeitung fortzusetzen und an das Ziel zu senden. Das AIP-SSM im Inline-Modus kann als Intrusion Prevention System (IPS) angesehen werden. Im Gegensatz zum Promiscuous-Modus kann der Inline-Modus (IPS) tatsächlich verhindern, dass das Triggerpaket das Ziel erreicht.
- Falls die ASA nicht mit dem AIP-SSM kommunizieren kann, wie sollte die ASA den zu inspizierenden Datenverkehr handhaben? Beispiele für Fälle, in denen die ASA nicht mit AIP-SSM kommunizieren kann, sind AIP-SSM-Neuladungen oder der Ausfall des Moduls und der Austausch des Moduls. In diesem Fall kann die ASA das Fail-Open- oder Fail-Close-Verfahren ausführen.Durch das Fail-Open kann die ASA weiterhin zu überprüfenden Datenverkehr an das endgültige Ziel weiterleiten, wenn das AIP-SSM nicht erreicht werden kann.Fail-Closed blockiert den zu inspizierenden Datenverkehr, wenn die ASA nicht mit dem AIP-SSM kommunizieren kann.**Hinweis:** Der zu inspizierende Datenverkehr wird mithilfe einer Zugriffsliste definiert. In dieser Beispielausgabe lässt die Zugriffsliste den gesamten IP-Datenverkehr von einer Quelle zu einem beliebigen Ziel zu. Daher kann der zu überprüfende Datenverkehr alles sein, was die ASA durchläuft.

```
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.
```

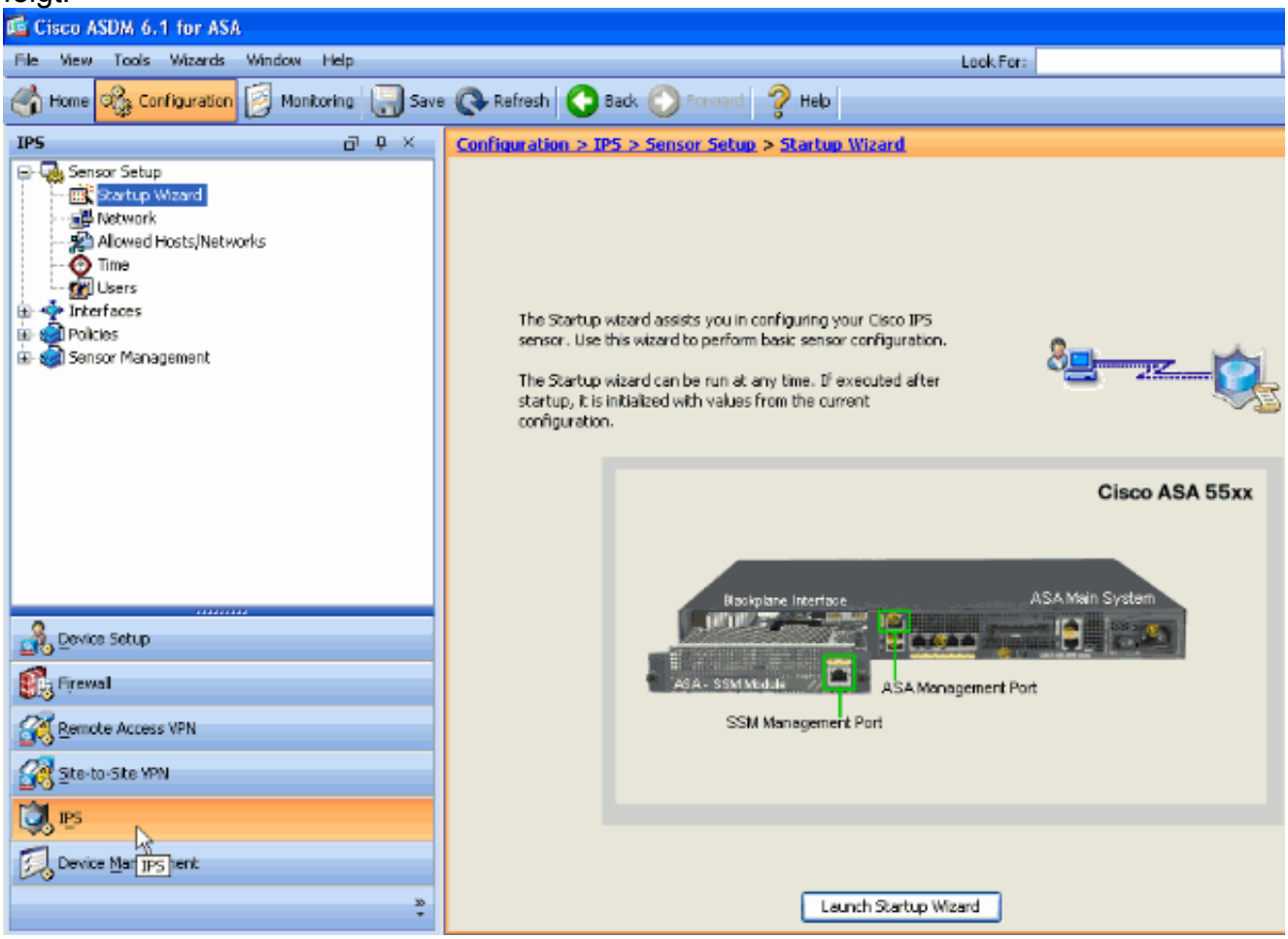
```
ciscoasa(config)#policy-map global_policy
!--- Note that policy-map global_policy is a part of the !--- default configuration. In
addition, policy-map global_policy !--- is applied globally with the service-policy command.

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.
```

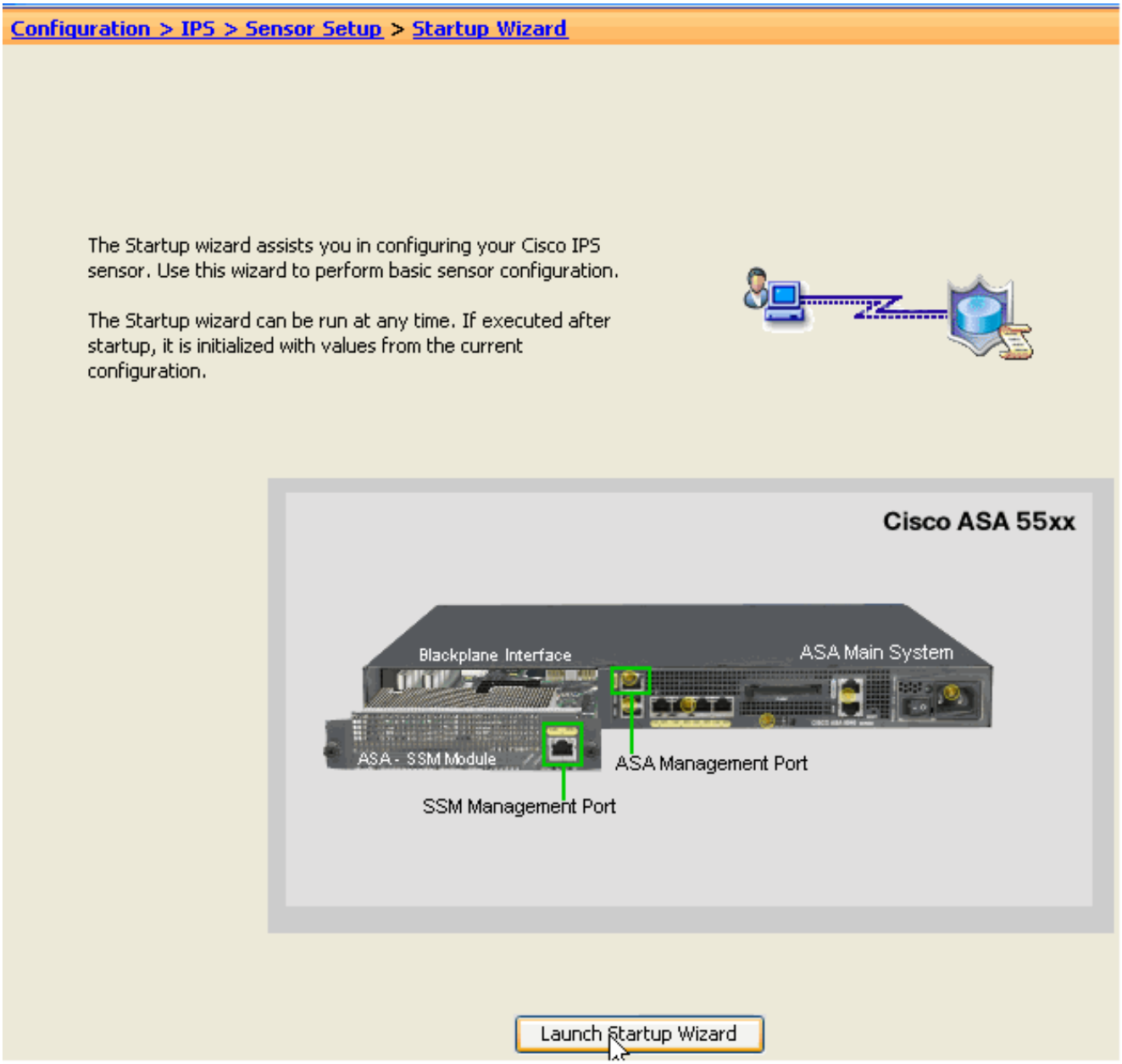
Überprüfen Sie den gesamten Datenverkehr mit dem AIP-SSM mithilfe von ASDM.

Gehen Sie wie folgt vor, um den gesamten Datenverkehr mit AIP-SSM zu überprüfen, das ASDM verwendet:.

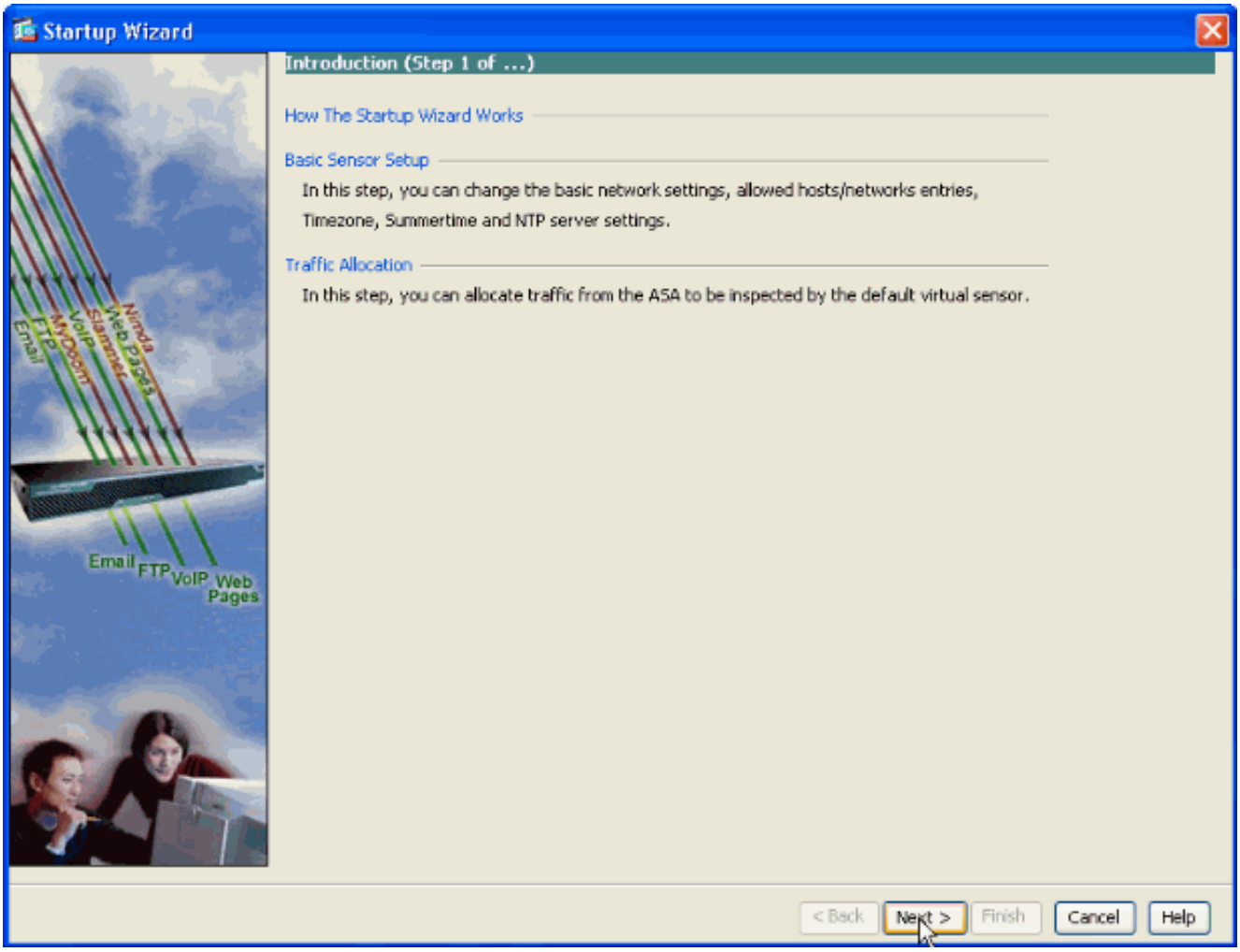
1. Wählen Sie **Configuration > IPS > Sensor Setup > Startup Wizard (Konfiguration > IPS > Sensor-Setup > Startup-Assistent)** auf der ASDM-Startseite, um die Konfiguration zu starten, wie folgt:



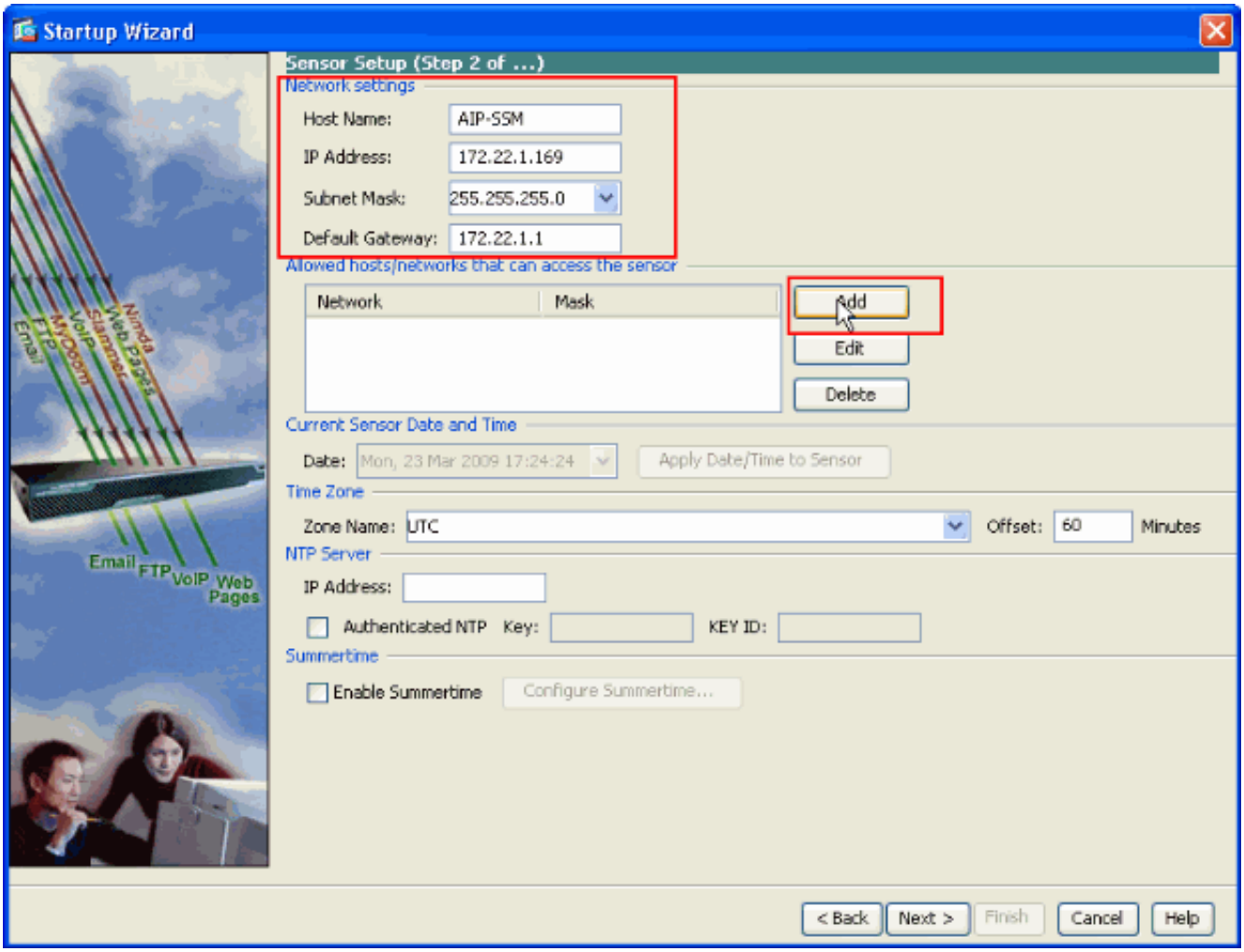
2. Klicken Sie auf **Start-Assistent starten**.



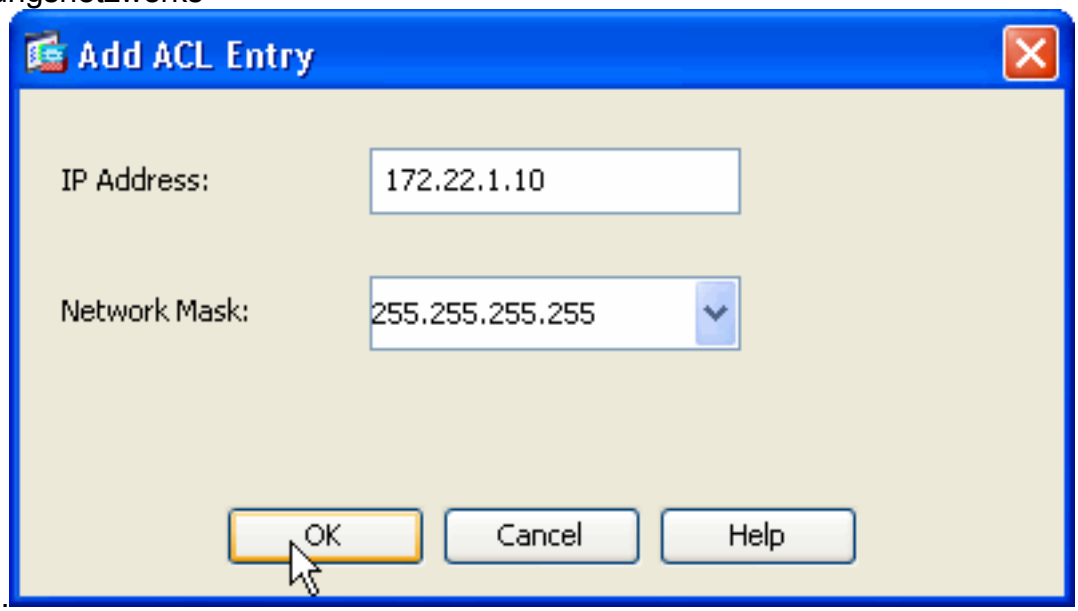
3. Klicken Sie im neuen Fenster, das nach dem Start des Assistenten angezeigt wird, auf **Weiter**.



4. Geben Sie im neuen Fenster den Hostnamen, die IP-Adresse, die Subnetzmaske und die Adresse des Standard-Gateways für das AIP-SSM-Modul im entsprechenden Feld im Abschnitt Netzwerkeinstellungen an. Klicken Sie dann auf **Hinzufügen**, um die Zugriffslisten hinzuzufügen, um den gesamten Datenverkehr mit AIP-SSM zuzulassen.

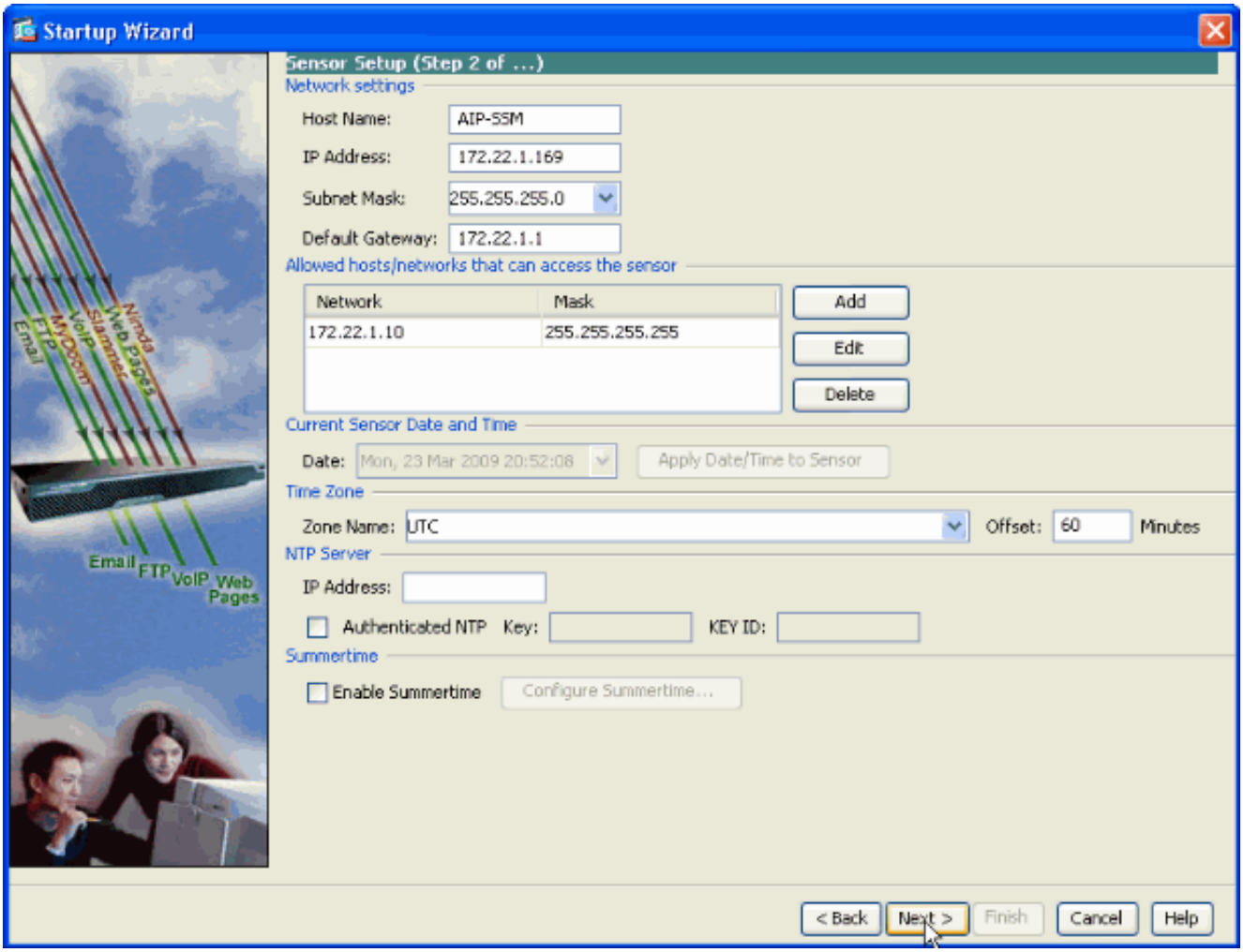


5. Geben Sie im Fenster **Add ACL Entry (ACL-Eintrag hinzufügen)** die **IP-Adresse** und die **Netzwerkmaske** an, welche Hosts/Netzwerke auf den Sensor zugreifen dürfen. Klicken Sie auf **OK**.**Hinweis:** Die Host-/Netzwerk-IP-Adresse muss zum Adressbereich des Verwaltungsnetzwerks

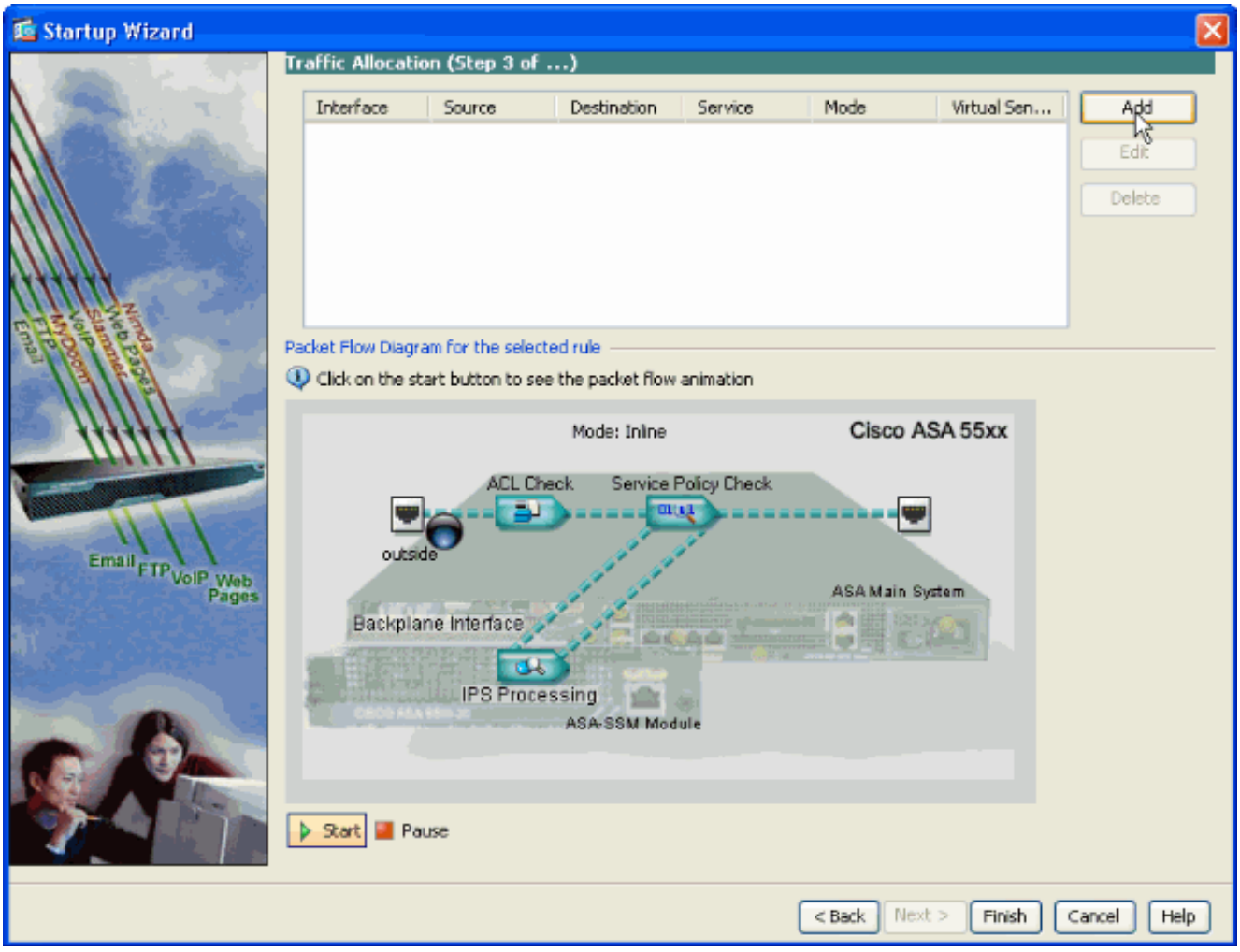


gehören.

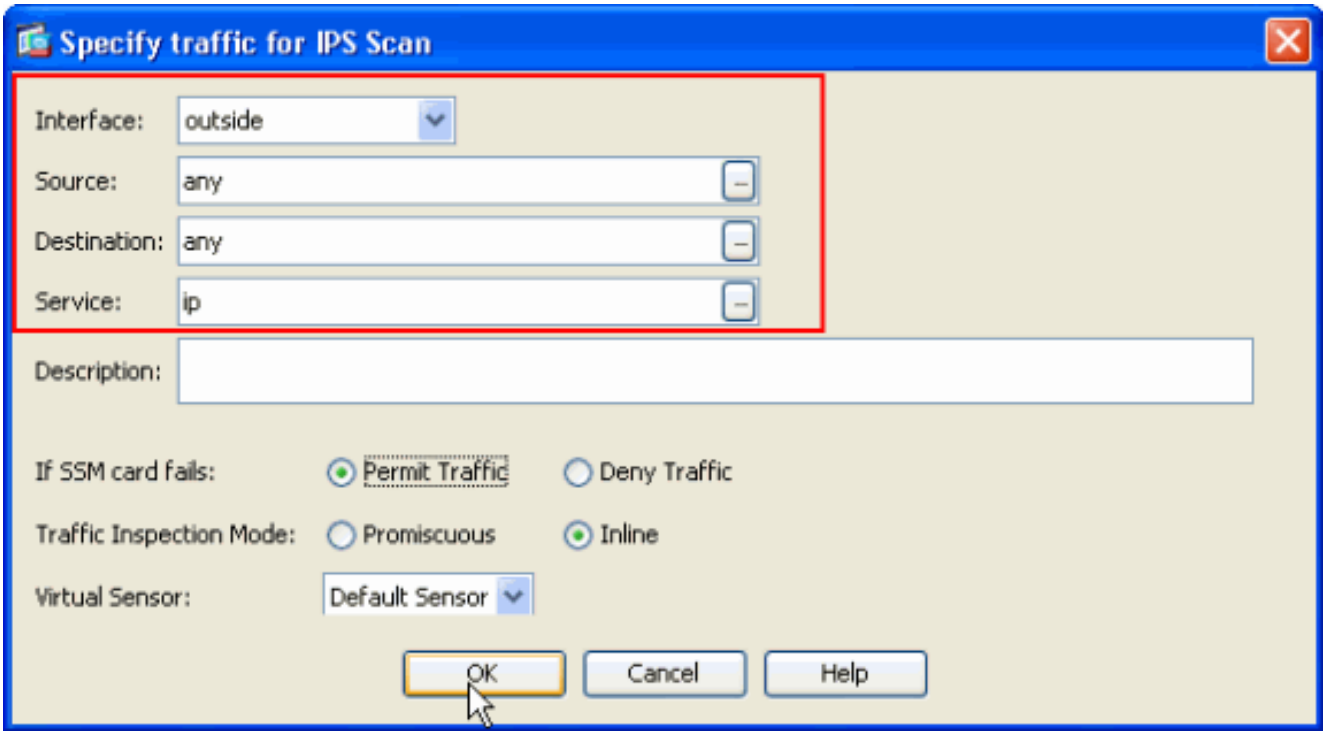
6. Klicken Sie auf **Weiter**, nachdem Sie die Details in den entsprechenden Bereichen angegeben
haben.



7. Klicken Sie auf **Hinzufügen**, um die Details zur Datenverkehrszuweisung zu konfigurieren.

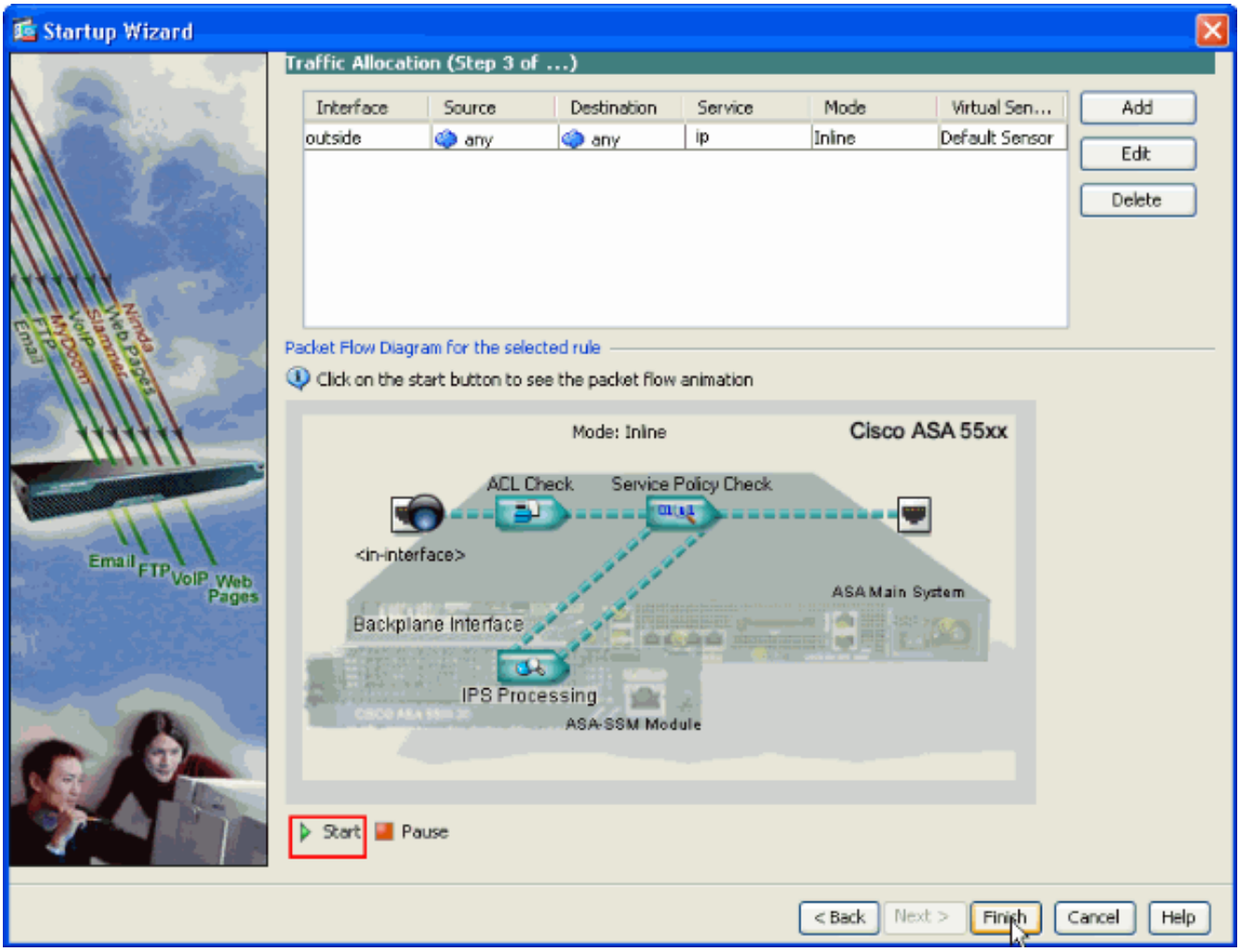


8. Geben Sie die Quell- und Zielnetzwerkadresse sowie den Servicetyp an, z. B. wird hier IP verwendet. In diesem Beispiel wird **jeder** für Quelle und Ziel verwendet, wenn Sie den gesamten Datenverkehr mit AIP-SSM überprüfen. Klicken Sie anschließend auf **OK**.



9. In diesem Fenster werden konfigurierte Regeln für die Datenverkehrszuweisung angezeigt. Sie können nach Bedarf beliebig viele Regeln hinzufügen, wenn Sie die in den Schritten 7 und 8 beschriebenen Schritte ausführen. Klicken Sie anschließend auf **Fertig stellen**, um das

ASDM-Konfigurationsverfahren abzuschließen.**Hinweis:** Sie können die Animation zum Paketfluss anzeigen, wenn Sie auf **Start** klicken.



Überprüfen Sie spezifischen Datenverkehr mit dem AIP-SSM.

Wenn der Netzwerkadministrator den AIP-SSM-Monitor als Teilmenge des gesamten Datenverkehrs verwenden möchte, verfügt die ASA über zwei unabhängige Variablen, die geändert werden können. Zunächst kann die Zugriffsliste so geschrieben werden, dass der erforderliche Datenverkehr ein- oder ausgeschlossen wird. Zusätzlich zur Änderung von Zugriffslisten kann eine **Dienstrichtlinie** auf eine Schnittstelle oder global angewendet werden, um den vom AIP-SSM inspizierten Datenverkehr zu ändern.

In Bezug auf das Netzwerkdiagramm in diesem Dokument möchte der Netzwerkadministrator, dass das AIP-SSM *den gesamten* Datenverkehr zwischen dem externen Netzwerk und dem DMZ-Netzwerk überprüft.

```
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.
```

Als Nächstes soll der Netzwerkadministrator mithilfe des AIP-SSM den *vom* internen Netzwerk zum externen Netzwerk *initiierten* Datenverkehr überwachen. Innerhalb des Netzwerks mit dem DMZ-Netzwerk wird keine Überwachung durchgeführt.

Hinweis: Dieser Abschnitt erfordert ein Zwischen-Verständnis von Status, TCP, UDP, ICMP, Verbindungs- und verbindungsloser Kommunikation.

```
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
```

Die Zugriffsliste verweigert den im internen Netzwerk initiierten Datenverkehr, der für das DMZ-Netzwerk bestimmt ist. Die zweite Zugriffslistenleitung erlaubt oder sendet Datenverkehr, der im internen Netzwerk für das externe Netzwerk initiiert wurde, an das AIP-SSM. An diesem Punkt kommt die Stateful-Funktion der ASA ins Spiel. Beispielsweise initiiert ein interner Benutzer eine TCP-Verbindung (Telnet) mit einem Gerät im externen Netzwerk (Router). Der Benutzer stellt erfolgreich eine Verbindung zum Router her und meldet sich an. Der Benutzer gibt dann einen Router-Befehl aus, der nicht autorisiert ist. Der Router reagiert mit `fehlgeschlagener Befehlsautorisierung`. Das Datenpaket, das die `Zeichenfolge Command Authorization failed` enthält, enthält eine Quelle des externen Routers und ein Ziel des internen Benutzers. Quelle (außen) und Ziel (innen) stimmen nicht mit den zuvor in diesem Dokument definierten Zugriffslisten überein. Die ASA überwacht die zustandsbehafteten Verbindungen. Aus diesem Grund wird das (von außen nach innen) zurückgegebene Datenpaket zur Überprüfung an das AIP-SSM gesendet. Benutzerdefinierte Signatur 60000 0, die auf dem AIP-SSM konfiguriert ist, Alarme.

Hinweis: Standardmäßig behält die ASA den Status für ICMP-Datenverkehr nicht bei. In der vorherigen Beispielkonfiguration pingen die internen Benutzer (ICMP-Echoanfrage) den externen Router. Der Router reagiert mit ICMP-Echo-Antwort. Das AIP-SSM überprüft das Echo-Anforderungspaket, jedoch nicht das Echo-Antwort-Paket. Wenn die ICMP-Prüfung auf der ASA aktiviert ist, werden sowohl die Echo-Anforderung als auch die Echo-Antwort-Pakete vom AIP-SSM überprüft.

Bestimmten Netzwerkverkehr von der AIP-SSM-Prüfung ausschließen

Das angegebene generalisierte Beispiel bietet eine Ansicht zum Ausnehmen des spezifischen Datenverkehrs, der von AIP-SSM gescannt werden soll. Dazu müssen Sie eine Zugriffsliste erstellen, die den Datenverkehrsfluss enthält, der vom AIP-SSM-Scannen in deny-Anweisung ausgeschlossen werden soll. In diesem Beispiel ist IPS der Name der Zugriffsliste, die den von AIP-SSM zu scannenden Datenverkehrsfluss definiert. Datenverkehr zwischen <source> und

<destination> wird vom Scannen ausgeschlossen. der restliche Datenverkehr überprüft wird.

```
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
```

Überprüfen

Überprüfen Sie, ob Warnungsereignisse im AIP-SSM aufgezeichnet werden.

Melden Sie sich mit dem Administratorkonto beim AIP-SSM an. Der Befehl **show events alert** generiert diese Ausgabe.

Hinweis: Die Ausgabe hängt von den Signatureinstellungen, der Art des an das AIP-SSM gesendeten Datenverkehrs und der Netzwerkauslastung ab.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

```
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 den Beispielkonfigurationen werden mehrere IPS-Signaturen für Warnmeldungen beim Testdatenverkehr konfiguriert. Signatur 2000 und 2004 werden geändert. Die benutzerdefinierte Signatur 60000 wird hinzugefügt. In einer Laborumgebung oder einem Netzwerk, in dem nur wenige Daten durch die ASA übertragen werden, kann es erforderlich sein, Signaturen zu ändern, um Ereignisse auszulösen. Wenn ASA und AIP-SSM in einer Umgebung bereitgestellt werden, die eine große Datenverkehrsmenge übergibt, werden die Standardsignatureinstellungen wahrscheinlich ein Ereignis generieren.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Stellen Sie diese **show**-Befehle von der ASA aus.

- **show module**: Zeigt Informationen über das SSM auf der ASA sowie Systeminformationen an.

```
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.
```

- **Schaulauf**

```
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.
```

- **show access-list** - Zeigt die Zähler für eine Zugriffsliste an.

```
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.
```

Lässt sich der Netzwerkverkehr wie erwartet über die ASA leiten, bevor Sie das AIP-SSM installieren und verwenden? Andernfalls kann es erforderlich sein, eine Fehlerbehebung für die Regeln der Netzwerk- und ASA-Zugriffsrichtlinien durchzuführen.

Probleme mit Failover

- Wenn sich zwei ASAs in einer Failover-Konfiguration befinden und beide über ein AIP-SSM verfügen, **müssen** Sie die Konfiguration der AIP-SSMs manuell replizieren. Nur die Konfiguration der ASA wird vom Failover-Mechanismus repliziert. Das AIP-SSM ist nicht im Failover enthalten. Weitere Informationen zu Failover-Problemen finden Sie im Konfigurationsbeispiel für PIX/ASA 7.x-Aktiv/Standby-Failover.
- Das AIP-SSM ist nicht an Stateful Failover beteiligt, wenn für das ASA-Failover-Paar Stateful Failover konfiguriert wurde.

Fehlermeldungen

Das IPS-Modul (AIP-SSM) erzeugt Fehlermeldungen wie dargestellt und keine Brennereignisse.

```
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.
```

Die Ursache für diese Fehlermeldung ist, dass der virtuelle IPS-Sensor nicht der Backplane-Schnittstelle der ASA zugewiesen wurde. Die ASA ist korrekt eingerichtet, um Datenverkehr an das SSM-Modul zu senden. Sie müssen den virtuellen Sensor jedoch der Backplane-Schnittstelle zuweisen, die die ASA erstellt, damit das SSM den Datenverkehr scannen kann.

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

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

Diese Meldungen zeigen an, dass IP LOGGING aktiviert wird, wodurch wiederum alle Systemressourcen gehostet werden. Cisco empfiehlt, IP-PROTOKOLLIERUNG zu deaktivieren, da diese nur zur Fehlerbehebung/zu Ermittlungszwecken verwendet werden sollte.

Hinweis: Die `Inline-Datenumgehung` der `Fehlermeldung hat begonnen`, es wird ein erwartetes Verhalten erwartet, da der Sensor die Analyse-Engine nach dem Signatur-Update, das ein notwendiger Teil des Signatur-Aktualisierungsvorgangs ist, vorübergehend neu startet.

Syslog-Unterstützung

Das AIP-SSM unterstützt Syslog nicht als Warnformat.

Die Standardmethode zum Empfang von Warnmeldungen vom AIP-SSM ist der Security Device Event Exchange (SDEE). Eine weitere Option besteht darin, einzelne Signaturen zu konfigurieren, um ein SNMP-Trap als Aktion zu generieren, die beim Auslösen der Signaturen ausgeführt wird.

AIP-SSM-Neustart

Das AIP-SSM-Modul reagiert nicht richtig.

Wenn das AIP-SSM-Modul nicht ordnungsgemäß reagiert, starten Sie das AIP-SSM-Modul neu, ohne die ASA neu zu starten. Verwenden Sie den Befehl **hw-module-Modul 1 reload** (Neustarten), um das AIP-SSM-Modul neu zu starten und ASA nicht neu zu starten.

AIP-SSM-E-Mail-Warnung

Kann AIP-SSM E-Mail-Benachrichtigungen an Benutzer senden?

Nein, es wird nicht unterstützt.

Zugehörige Informationen

- Cisco Security Appliance Command Reference, Version 7.2
- Systemprotokollmeldungen der Cisco Security Appliance, Version 7.2
- Befehlsreferenz für Cisco Intrusion Prevention System 5.1
- Technischer Support und Dokumentation - Cisco Systems