ASA: Invio del traffico di rete dall'ASA all'esempio di configurazione di SSM AIP

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per inviare il traffico di rete che passa attraverso Cisco ASA serie 5500 Adaptive Security Appliance (ASA) al modulo AIP-SSM (Advanced Inspection and Prevention Security Services Module). Esempi di configurazione vengono forniti con l'interfaccia della riga di comando (CLI).

Per ulteriori informazioni, fare riferimento al documento ASA: Inviare il traffico di rete dall'appliance ASA all'esempio di configurazione CSC-SSM per inviare il traffico di rete da Cisco ASA serie 5500 Adaptive Security Appliance (ASA) al modulo CSC-SSM (Content Security and Control Security Services Module).

Per ulteriori informazioni su come inviare il traffico di rete che attraversa Cisco ASA 5500 Adaptive Security Appliance (ASA) in modalità contesto multiplo al modulo Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS), fare riferimento a Assegnazione di sensori virtuali a un contesto di sicurezza (solo AIP SSM).

Nota: il traffico di rete che attraversa l'appliance ASA include gli utenti interni che accedono a Internet o gli utenti Internet che accedono alle risorse protette dall'ASA in una zona demilitarizzata (DMZ) o all'interno della rete. Il traffico di rete inviato da e verso l'appliance ASA non viene inviato al modulo IPS per l'ispezione. Un esempio di traffico non inviato al modulo IPS è il ping (ICMP) tra le interfacce ASA o il collegamento in modalità Telnet all'appliance ASA.

Nota: la struttura di criteri modulare utilizzata dall'ASA per classificare il traffico per l'ispezione non supporta IPv6. Pertanto, se si devia il traffico IPv6 verso il server SSM AIP tramite ASA, il protocollo non è supportato.

Nota: per ulteriori informazioni sulla configurazione iniziale di AIP-SSM, consultare il documento sulla configurazione iniziale del sensore AIP-SSM.

Prerequisiti

Requisiti

in questo documento si presume che il pubblico abbia una conoscenza di base di come configurare il software Cisco ASA versione 8.x e il software IPS versione 6.x.

- I componenti di configurazione necessari per ASA 8.x includono interfacce, elenchi degli accessi, NAT (Network Address Translation) e routing.
- I componenti di configurazione necessari per AIP-SSM (software IPS 6.x) includono l'installazione della rete, gli host consentiti, la configurazione dell'interfaccia, le definizioni delle firme e le regole di azione degli eventi.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5510 con software versione 8.0.2
- AIP-SSM-10 con software IPS versione 6.1.2

Nota: questo esempio di configurazione è compatibile con qualsiasi firewall Cisco ASA serie 5500 con OS 7.x e versioni successive e con il modulo AIP-SM con IPS 5.x e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità

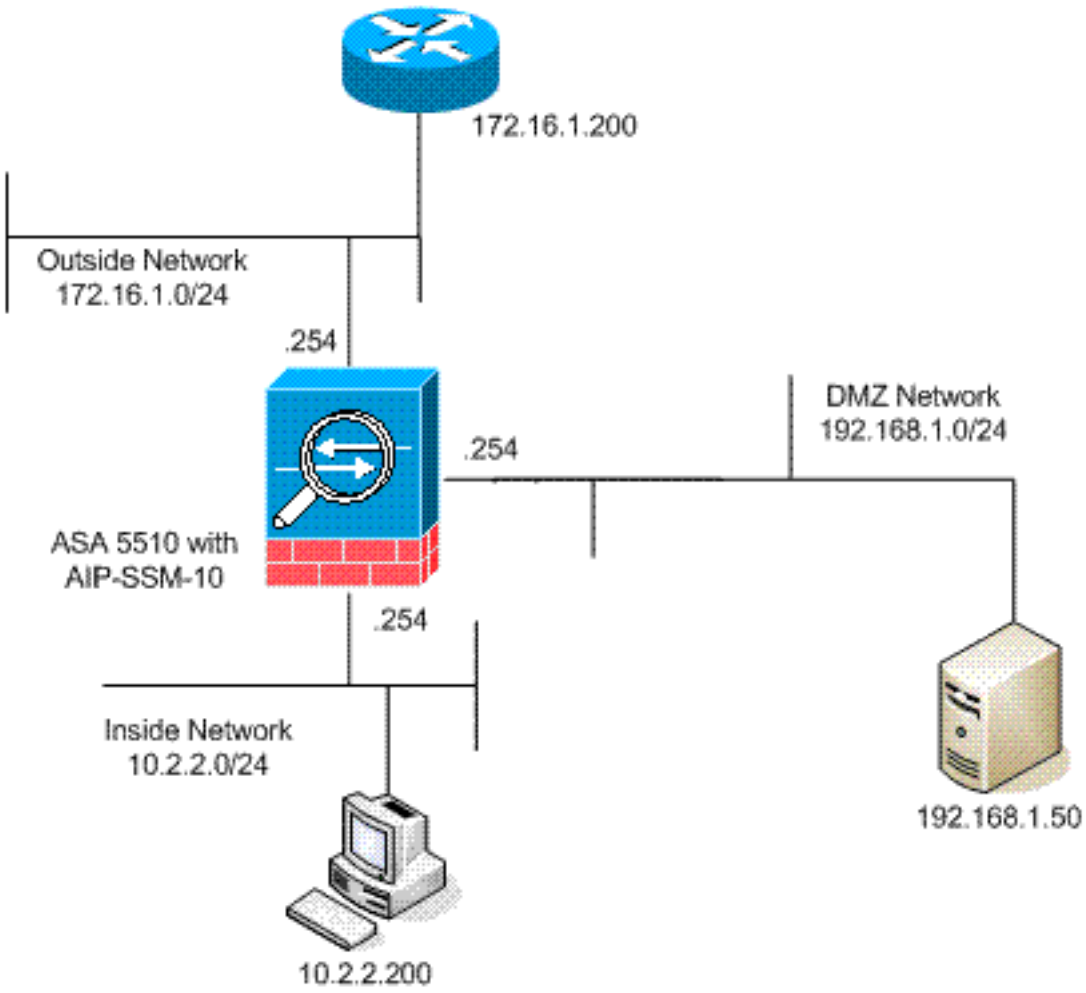
descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni iniziali

Nel documento vengono usate queste configurazioni. Sia l'ASA che l'AIP-SSM iniziano con una configurazione predefinita, ma hanno apportato modifiche specifiche a scopo di test. Le aggiunte vengono annotate nella configurazione.

- 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#
```

Nota: se non è possibile accedere al modulo AIP-SSM con https, attenersi alla seguente procedura:

- Configurare un indirizzo IP di gestione per il modulo. Inoltre, è possibile configurare l'`elenco degli accessi alla rete`, in cui è possibile specificare gli IP/le reti IP che possono connettersi all'IP di gestione.
- Accertarsi di aver collegato l'interfaccia Ethernet esterna del modulo AIP. L'accesso dei manager al modulo AIP è possibile solo tramite questa interfaccia.

Per ulteriori informazioni, fare riferimento a Inizializzazione di AIP-SSM.

Ispezionare tutto il traffico con AIP-SSM in modalità inline o promiscua

Gli amministratori di rete e i dirigenti aziendali indicano spesso che è necessario monitorare tutto. Questa configurazione soddisfa il requisito del monitoraggio completo. Oltre a monitorare tutto, devono essere prese due decisioni su come interagiscono l'ASA e l'AIP-SSM.

- Il modulo AIP-SSM deve funzionare o essere distribuito in modalità promiscua o inline?In modalità promiscua, una copia dei dati viene inviata all'AIP-SSM mentre l'ASA inoltra i dati originali alla destinazione. L'AIP-SSM in modalità promiscua può essere considerato un sistema di rilevamento intrusioni (IDS). In questa modalità, il pacchetto di innesco (il pacchetto che causa l'allarme) può ancora raggiungere la destinazione. Lo shun può avvenire e impedire ad altri pacchetti di raggiungere la destinazione, ma il pacchetto di attivazione non viene arrestato.In modalità inline, l'ASA inoltra i dati all'AIP-SSM per l'ispezione. Se i dati superano l'ispezione AIP-SSM, vengono restituiti all'appliance ASA in modo da poter continuare l'elaborazione e l'invio alla destinazione. L'AIP-SSM in modalità inline può essere considerato un sistema di prevenzione delle intrusioni (IPS). A differenza della modalità promiscua, la modalità inline (IPS) può effettivamente impedire al pacchetto di trigger di raggiungere la destinazione.
- Nel caso in cui l'ASA non sia in grado di comunicare con l'AIP-SSM, in che modo deve gestire il traffico da ispezionare? Esempi di istanze in cui l'ASA non è in grado di comunicare con AIP-SSM includono i ricaricamenti AIP-SSM o se il modulo non funziona e deve essere sostituito. In questo caso, l'appliance ASA può essere aperta o chiusa con errori.La funzione Fail-open permette all'ASA di continuare a trasmettere il traffico da ispezionare alla destinazione finale se non è possibile raggiungere l'AIP-SSM.Impossibile chiudere i blocchi per sottoporre il traffico a ispezione quando l'ASA non può comunicare con AIP-SSM.**Nota:** il traffico da ispezionare è definito usando un elenco degli accessi. Nell'output di questo esempio, l'elenco degli accessi consente tutto il traffico IP da qualsiasi origine a qualsiasi destinazione. Pertanto, il traffico da ispezionare può essere qualsiasi cosa che passi attraverso l'ASA.

```
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
```

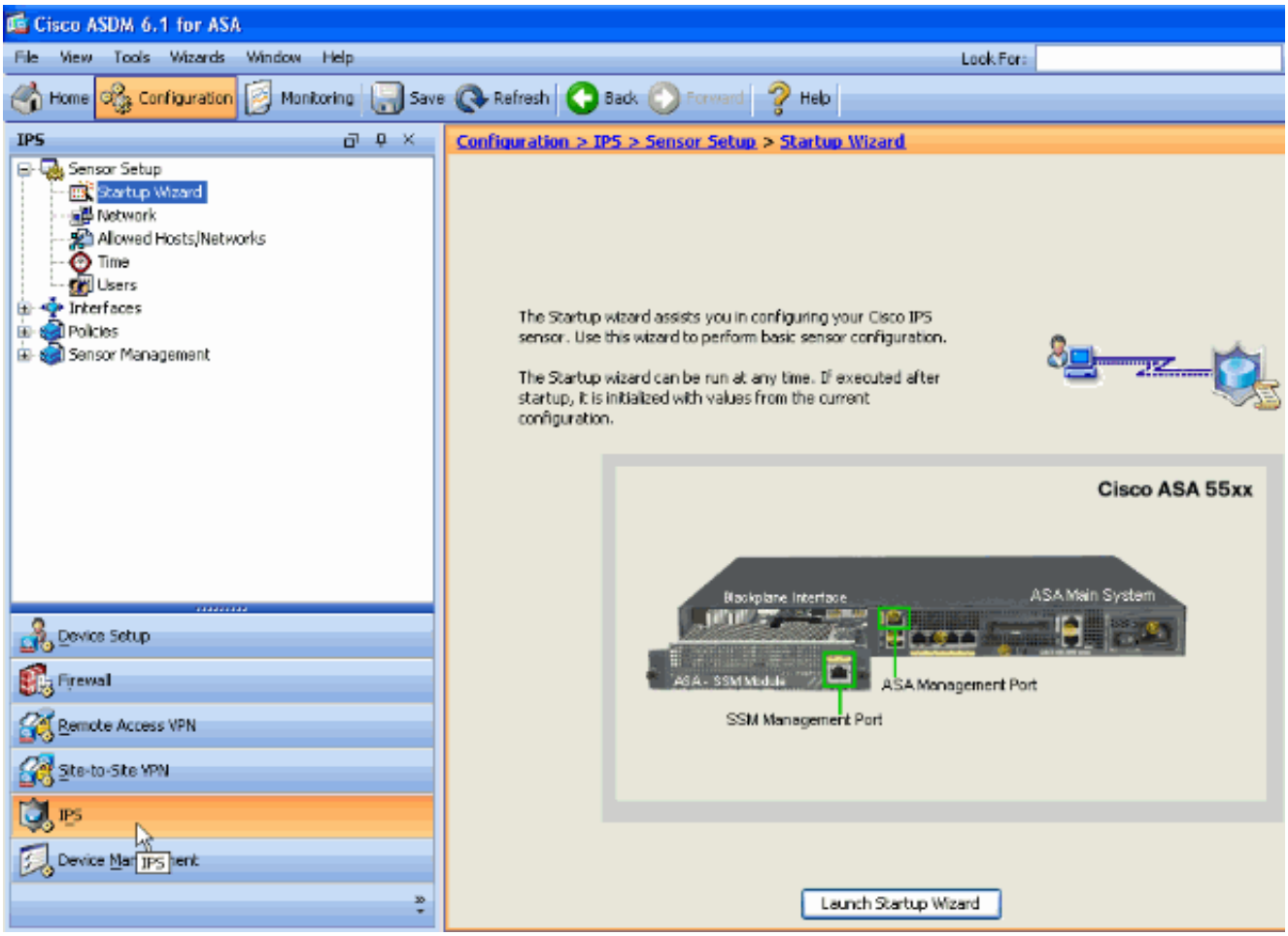
```
addition, policy-map global_policy !--- is applied globally with the service-policy command.

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.
```

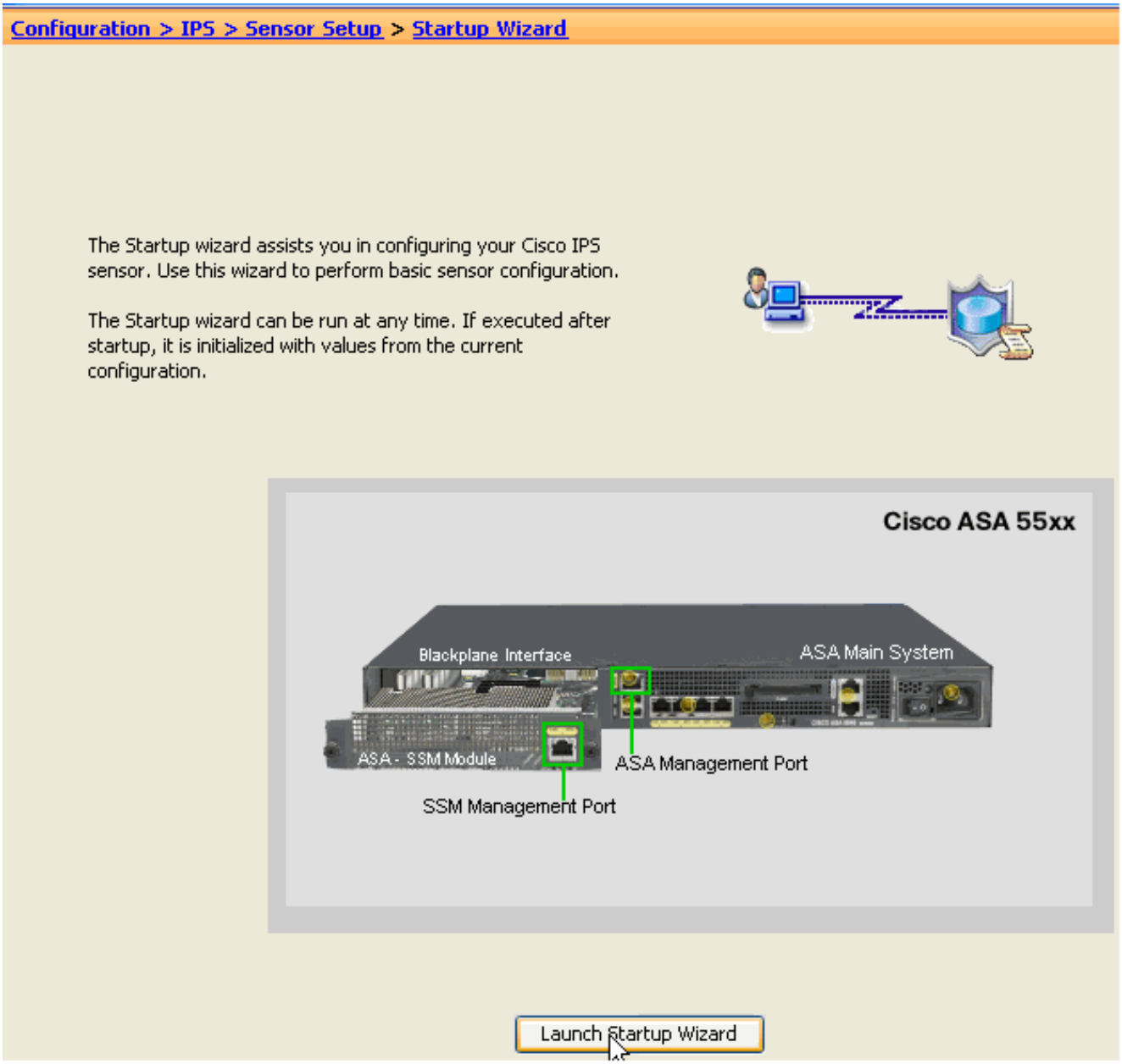
Ispezionare tutto il traffico con AIP-SSM utilizzando ASDM

Completare questa procedura per ispezionare tutto il traffico con AIP-SSM che usa ASDM:.

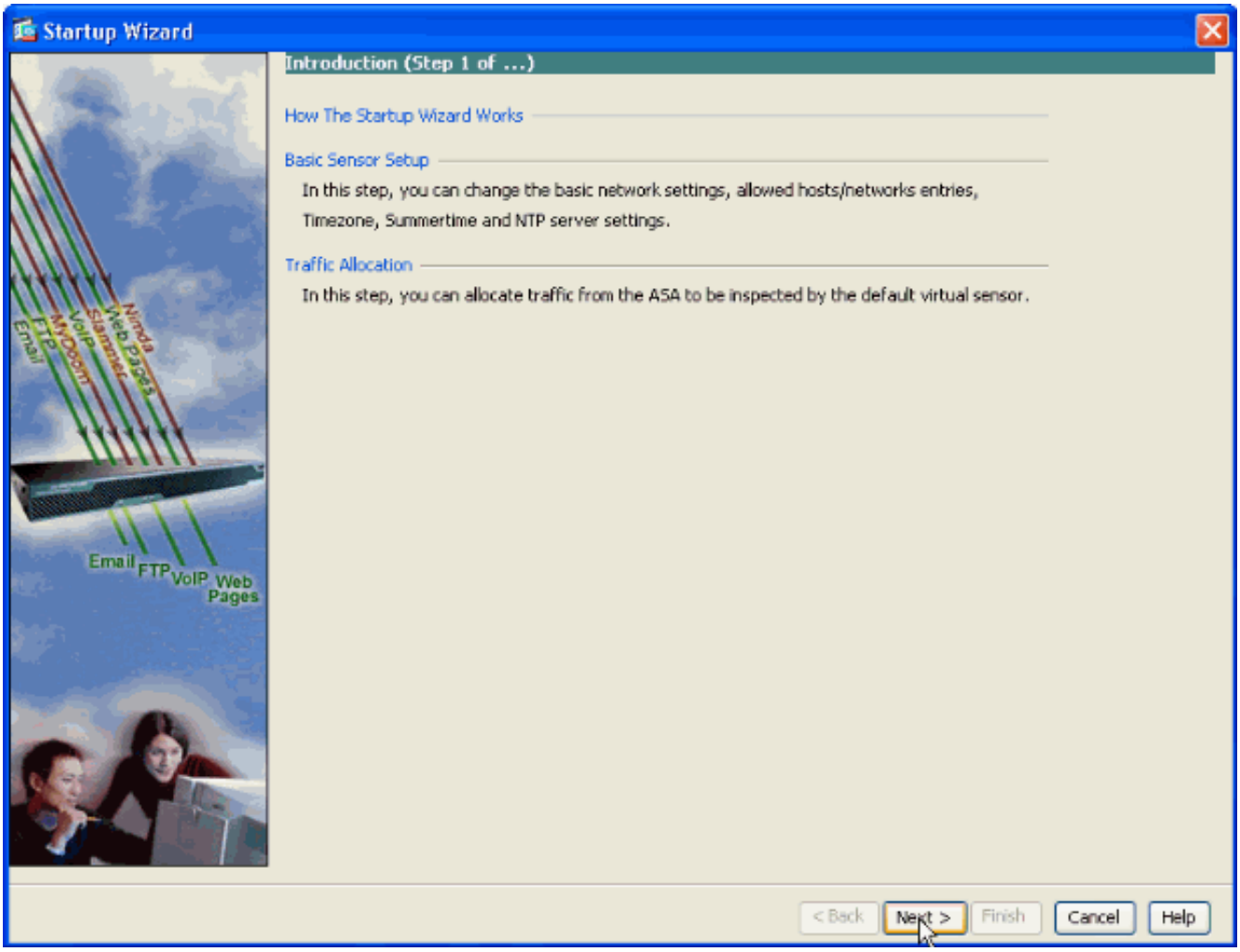
1. Scegliere **Configurazione > IPS > Impostazione sensore > Avvio guidato** nella home page di ASDM per avviare la configurazione, come mostrato:



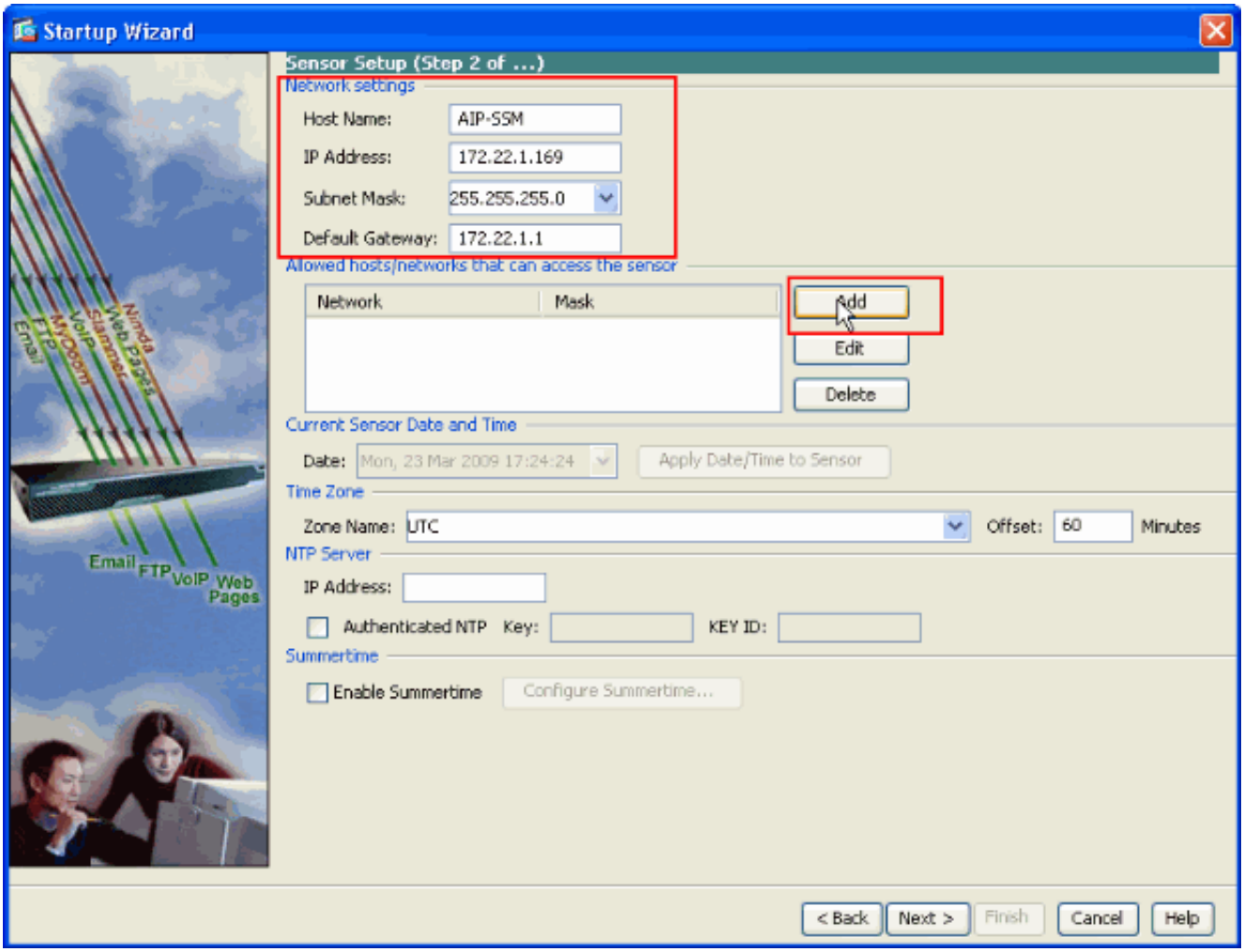
2. Fare clic su **Avvia Avvio guidato**.



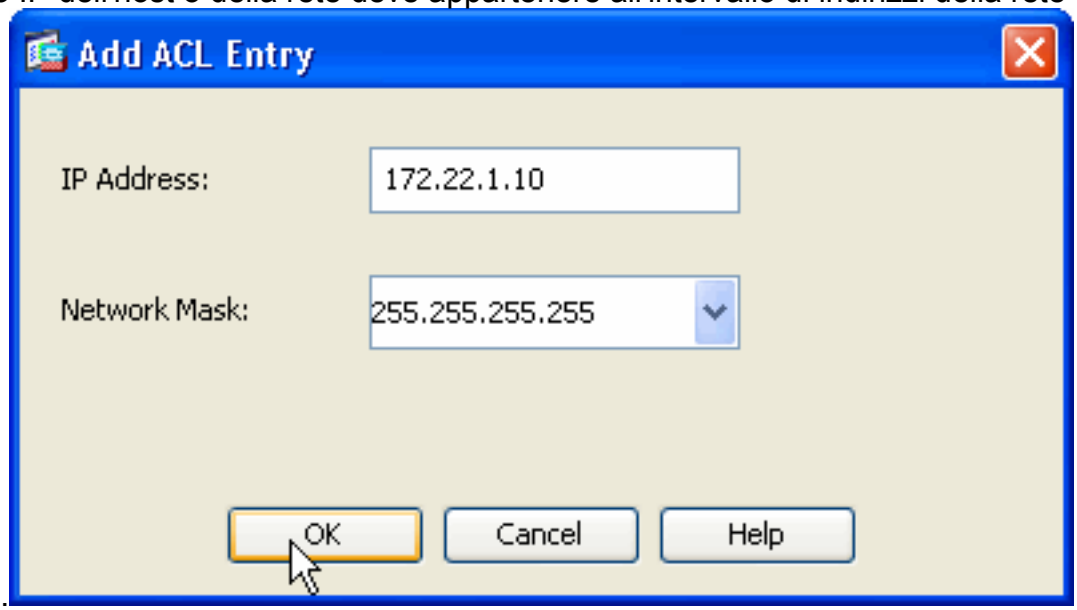
3. Fare clic su **Avanti** nella nuova finestra visualizzata dopo l'avvio della procedura guidata.



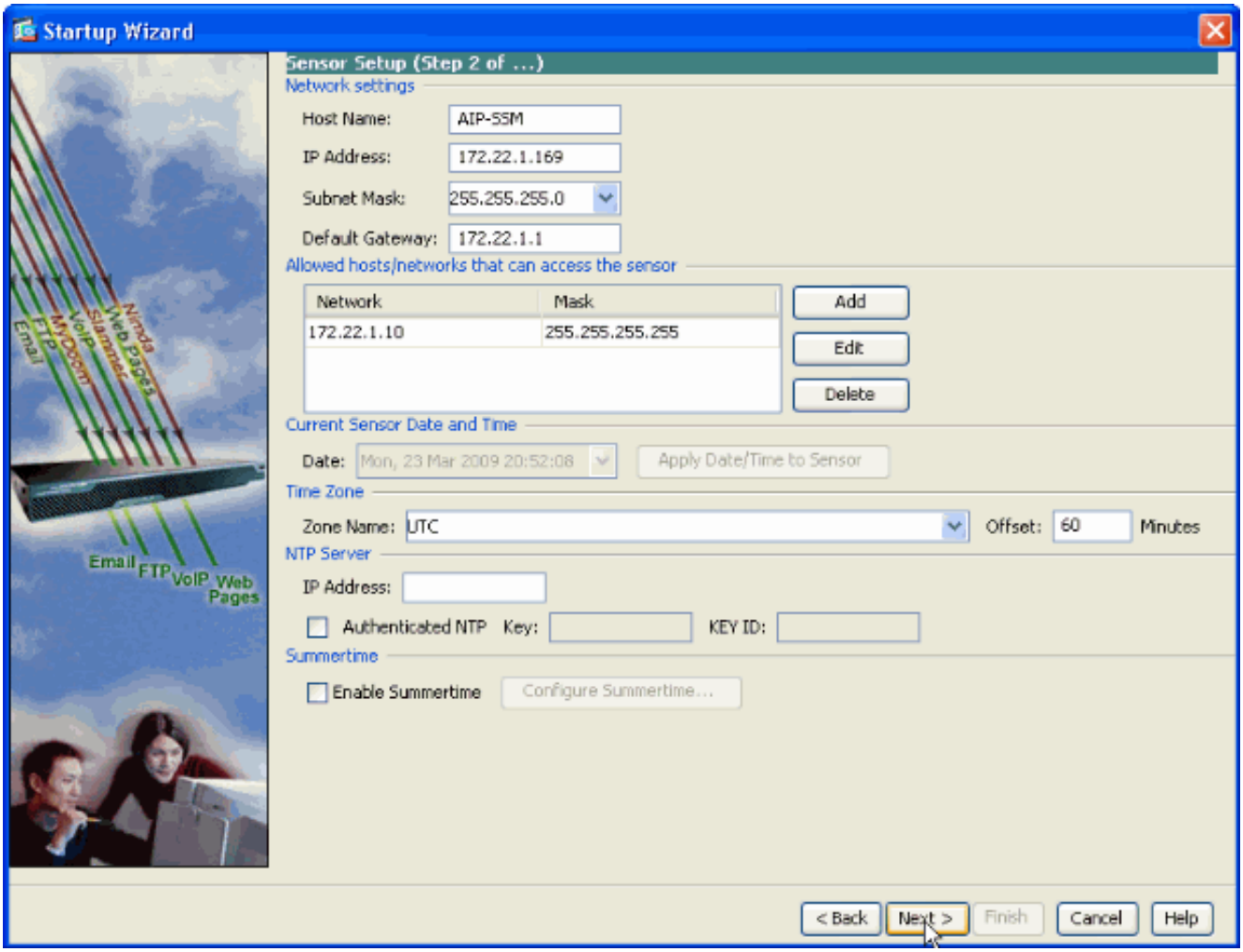
4. Nella nuova finestra, fornire il nome dell'host, l'indirizzo IP, la subnet mask e l'indirizzo del gateway predefinito per il modulo AIP-SSM nello spazio disponibile nella sezione Impostazioni di rete. Quindi, fare clic su **Add** (Aggiungi) per aggiungere gli elenchi degli accessi e consentire tutto il traffico con AIP-SSM.



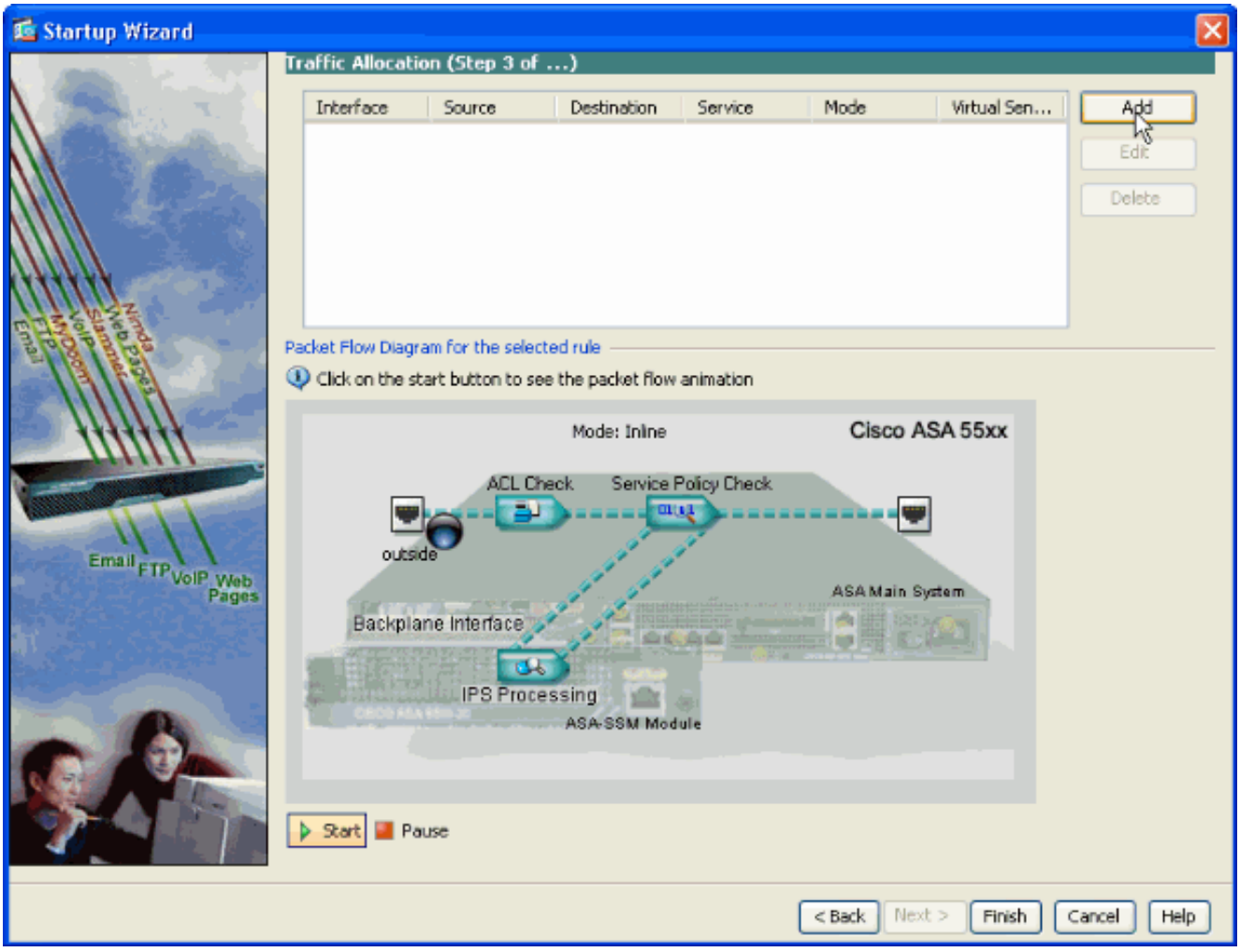
5. Nella finestra **Add ACL Entry** (Aggiungi voce ACL), fornire l'**indirizzo IP** e i dettagli **Network Mask** degli host/delle reti a cui è consentito accedere al sensore. Fare clic su OK.**Nota:** l'indirizzo IP dell'host o della rete deve appartenere all'intervallo di indirizzi della rete di gestione.



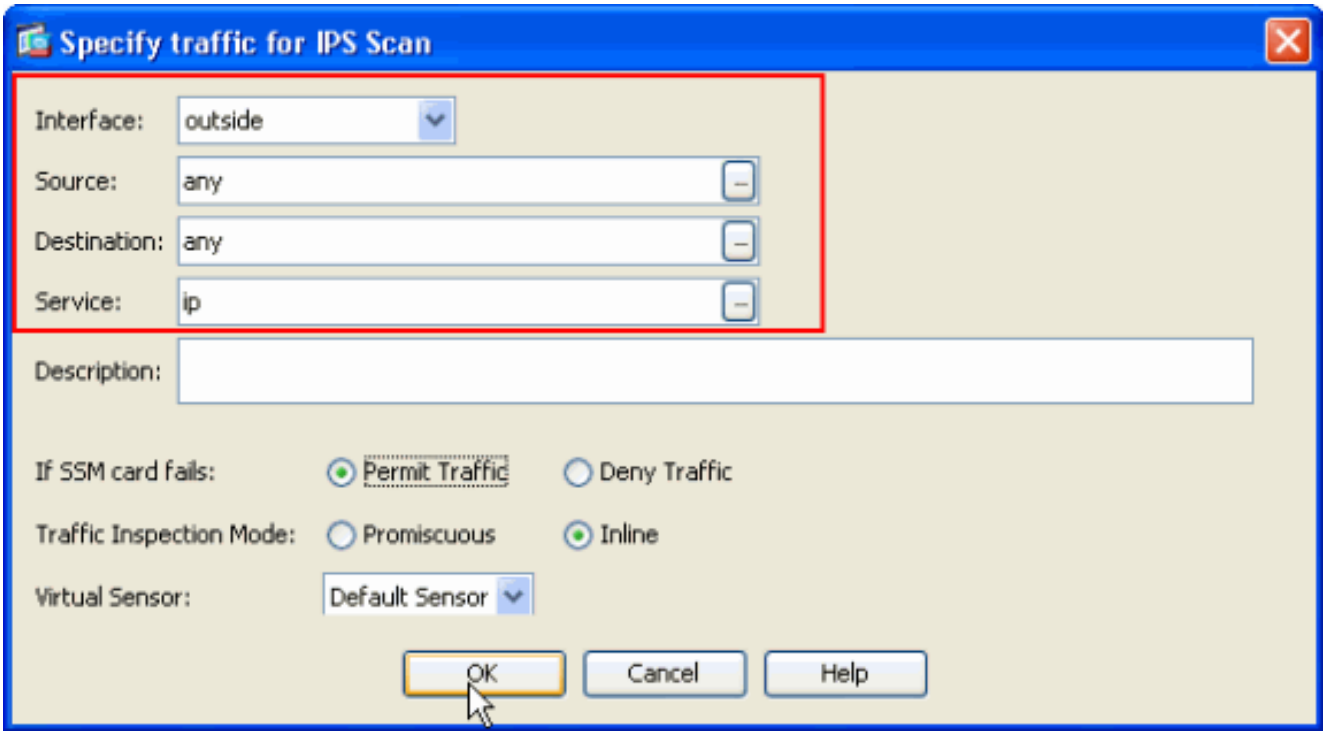
6. Fare clic su **Next** (Avanti) dopo aver fornito i dettagli negli spazi appositi.



7. Per configurare i dettagli di allocazione del traffico, fare clic su **Add** (Aggiungi).

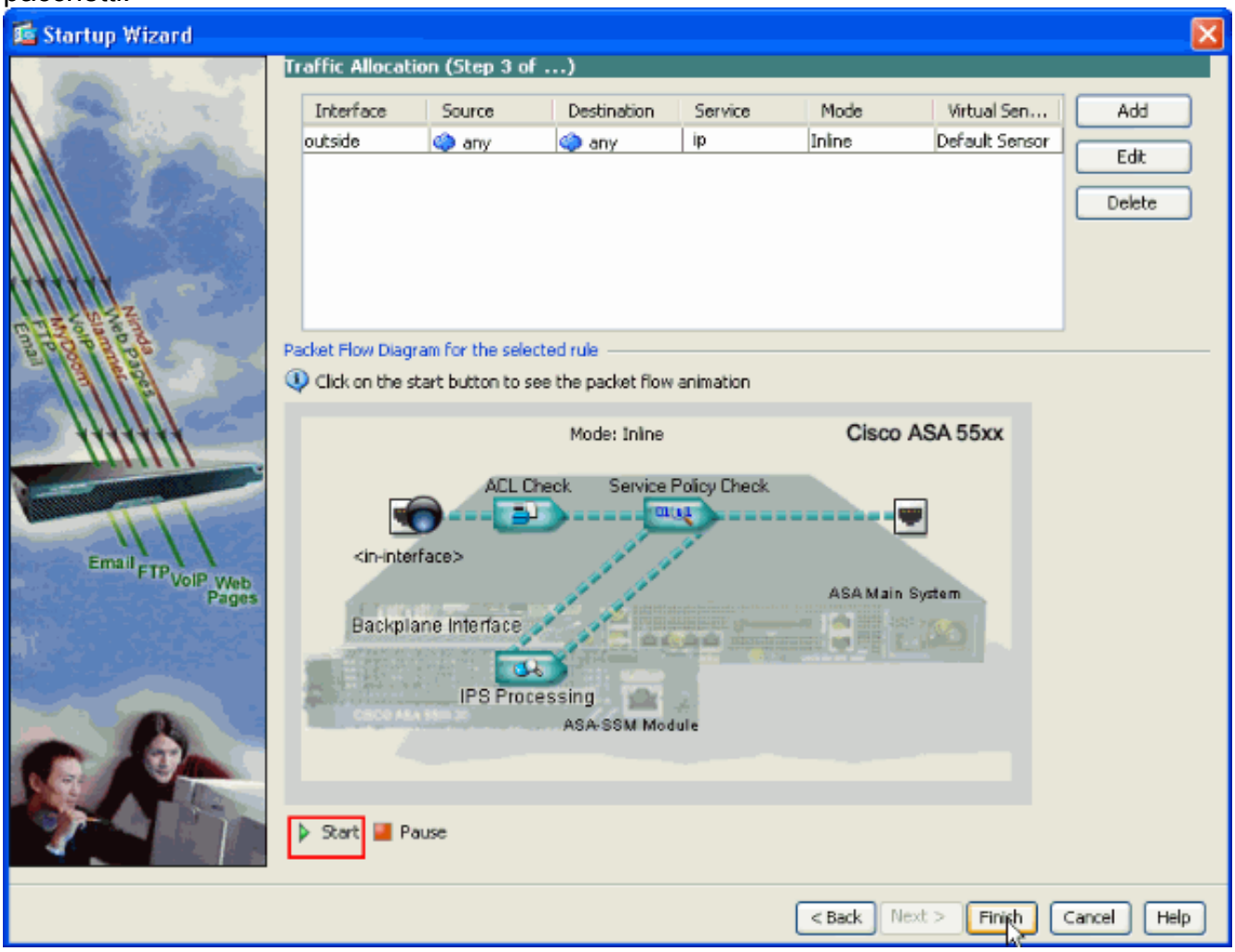


8. Specificare l'indirizzo di rete di origine e di destinazione, nonché il tipo di servizio, ad esempio IP. Nell'esempio, **any** viene usato per l'origine e la destinazione quando si ispeziona tutto il traffico con AIP-SSM. Quindi fare clic su **OK**.



9. In questa finestra vengono visualizzate le regole di allocazione del traffico configurate ed è possibile aggiungere tutte le regole necessarie se si completa la stessa procedura descritta nei passaggi 7 e 8. Quindi, fare clic su **Fine** per completare la procedura di configurazione

ASDM.**Nota:** se si fa clic su **Start**, è possibile visualizzare l'animazione del flusso dei pacchetti.



Ispezionare il traffico specifico con AIP-SSM

Se l'amministratore di rete desidera che il monitor AIP-SSM sia un sottoinsieme di tutto il traffico, l'ASA ha due variabili indipendenti che possono essere modificate. Innanzitutto, è possibile scrivere l'elenco degli accessi per includere o escludere il traffico necessario. Oltre a modificare gli elenchi degli accessi, è possibile applicare una **policy sui servizi** a un'interfaccia o a livello globale per modificare il traffico ispezionato dall'AIP-SSM.

In riferimento al diagramma di rete illustrato in questo documento, l'amministratore di rete desidera che l'AIP-SSM controlli *tutto* il traffico tra la rete esterna e la rete DMZ.

```
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.
```

Successivamente, l'amministratore di rete desidera che l'AIP-SSM monitori il traffico *avviato* dalla rete interna alla rete esterna. La connessione tra la rete interna e la rete DMZ non viene monitorata.

Nota: questa sezione richiede una comprensione intermedia di statefulness, TCP, UDP, ICMP, connessione e comunicazioni senza connessione.

```
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
```

L'elenco degli accessi impedisce al traffico iniziato sulla rete interna e destinato alla rete DMZ. La seconda linea dell'elenco degli accessi consente o invia il traffico iniziato sulla rete interna destinato alla rete esterna all'AIP-SSM. A questo punto entra in gioco la statualità dell'ASA. Ad esempio, un utente interno avvia una connessione TCP (Telnet) a un dispositivo sulla rete esterna (router). L'utente si connette al router e accede. L'utente quindi usa un comando del router non autorizzato. Il router risponde con l'`autorizzazione del comando non riuscita`. Il pacchetto di dati che contiene la stringa di `autorizzazione comando non riuscita` ha un'origine del router esterno e una destinazione dell'utente interno. L'origine (esterna) e la destinazione (interna) non corrispondono agli elenchi degli accessi definiti in precedenza nel presente documento. L'ASA tiene traccia delle connessioni con stato. Per questo motivo, il pacchetto dati che torna (dall'esterno all'interno) viene inviato all'AIP-SSM per l'ispezione. Avvisi della firma personalizzata 60000 0, configurata sull'AIP-SSM.

Nota: per impostazione predefinita, l'ASA non mantiene lo stato sul traffico ICMP. Nella configurazione di esempio precedente, l'utente interno esegue il ping (richiesta echo ICMP) sul router esterno. Il router risponde con una risposta echo ICMP. AIP-SSM controlla il pacchetto di richiesta echo ma non il pacchetto di risposta echo. Se l'ispezione ICMP è abilitata sull'appliance ASA, sia la richiesta echo che i pacchetti di risposta echo vengono ispezionati dall'ISP-SSM.

Escludi traffico di rete specifico dalla scansione AIP-SSM

Nell'esempio generalizzato fornito viene illustrata l'esenzione del traffico specifico che deve essere analizzato da AIP-SSM. Per eseguire questa operazione, è necessario creare un elenco degli accessi contenente il flusso di traffico da escludere dall'analisi AIP-SSM nell'istruzione Deny. Nell'esempio, IPS è il nome dell'elenco degli accessi che definisce il flusso del traffico da analizzare con AIP-SSM. Il traffico tra **<origine>** e **<destinazione>** viene escluso dalla scansione; tutto il resto del traffico viene ispezionato.

```
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
```

Verifica

Verificare che gli eventi di avviso siano registrati in AIP-SSM.

Accedere a AIP-SSM con l'account utente amministratore. Questo output viene generato dal comando **show events alert**.

Nota: l'output varia in base alle impostazioni della firma, al tipo di traffico inviato all'AIP-SSM e al carico di rete.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

```
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
```

Nelle configurazioni di esempio, diverse firme IPS vengono sintonizzate per generare un allarme sul traffico di prova. Le firme 2000 e 2004 sono state modificate. È stata aggiunta la firma personalizzata 60000. In un ambiente lab o in una rete in cui pochi dati passano attraverso l'ASA, può essere necessario modificare le firme per attivare gli eventi. Se l'ASA e l'SSM AIP vengono distribuiti in un ambiente che supera una grande quantità di traffico, è probabile che le impostazioni della firma predefinite generino un evento.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Usare questi comandi **show** dell'appliance ASA.

- **show module**: visualizza le informazioni sull'SSM sull'appliance ASA e le informazioni sul sistema.
  ```
  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.
```

- **show access-list**: visualizza i contatori per un elenco degli accessi.

```
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.
```

Prima di installare e utilizzare il modulo AIP-SSM, il traffico di rete attraversa l'appliance ASA come previsto? In caso contrario, potrebbe essere necessario risolvere i problemi relativi alle regole di accesso alla rete e all'appliance ASA.

Problemi di failover

- Se si hanno due appliance ASA in una configurazione di failover e ognuna ha un modulo AIP-SSM, è **necessario** replicare manualmente la configurazione dei moduli AIP-SSM. Solo la configurazione dell'ASA viene replicata dal meccanismo di failover. AIP-SSM non è incluso nel failover. Per ulteriori informazioni sui problemi di failover, consultare l'esempio di configurazione del failover attivo/standby di PIX/ASA 7.x.
- AIP-SSM non partecipa al failover con stato se il failover con stato è configurato sulla coppia di failover ASA.

Messaggi di errore

Il modulo IPS (AIP-SSM) genera messaggi di errore come mostrato e non eventi di attivazione.

```
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.
```

La causa di questo messaggio di errore è che il sensore virtuale IPS non è stato assegnato all'interfaccia del backplane dell'ASA. L'ASA è configurata correttamente per inviare il traffico al modulo SSM, ma è necessario assegnare il sensore virtuale all'interfaccia del backplane creata dall'ASA per consentire all'SSM di analizzare il traffico.

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

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

Questi messaggi sono indicativi dell'abilitazione della registrazione IP, che a sua volta ha connesso tutte le risorse del sistema. Cisco consiglia di disabilitare la registrazione IP in quanto deve essere utilizzata solo a scopo di risoluzione dei problemi/indagine.

Nota: il messaggio di errore `errWarning Inline Data Bypass has STARTED` è previsto in quanto il sensore riavvia momentaneamente il motore di analisi dopo l'aggiornamento della firma, che è una parte necessaria del processo di aggiornamento della firma.

Supporto Syslog

AIP-SSM non supporta syslog come formato di avviso.

Il metodo predefinito per ricevere le informazioni sugli avvisi da AIP-SSM è tramite Security Device Event Exchange (SDEE). In alternativa, è possibile configurare le singole firme in modo da generare una trap SNMP come azione da eseguire quando vengono attivate.

Riavvio AIP-SSM

Il modulo AIP-SSM non risponde correttamente.

Se il modulo AIP-SSM non risponde correttamente, riavviare il modulo AIP-SSM senza riavviare l'appliance ASA. Usare il comando **hw-module module 1 reload** per riavviare il modulo AIP-SSM e non riavviare l'appliance ASA.

Avviso e-mail AIP-SSM

AIP-SSM può inviare avvisi e-mail agli utenti?

No, non è supportato.

Informazioni correlate

- Guida di riferimento ai comandi di Cisco Security Appliance, versione 7.2
- Messaggi del registro di sistema di Cisco Security Appliance, versione 7.2
- Guida di riferimento ai comandi di Cisco Intrusion Prevention System 5.1
- Documentazione e supporto tecnico – Cisco Systems