ASA: Envíe el tráfico de la red del ASA al ejemplo de la configuración SSM AIP

Contenido

Introducción

Este documento proporciona una configuración de ejemplo que explica cómo enviar el tráfico de red que pasa a través de Cisco ASA 5500 Series Adaptive Security Appliance (ASA) al módulo (IPS) de Advanced Inspection and Prevention Security Services Module (AIP-SSM). Los ejemplos de la configuración se proporcionan el comando line interface(cli).

Refiera al ASA: Envíe el tráfico de la red del ASA al ejemplo de la configuración CSC-SSM para enviar el tráfico de la red del dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA) al módulo de Servicios de seguridad contento de la Seguridad y del control (CSC-SSM).

Refiera a asignar los sensores virtuales a un contexto de seguridad (SSM AIP solamente) para más información sobre cómo enviar el tráfico de la red que pasa a través del dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA) en el modo múltiple del contexto al módulo de Servicios de seguridad avanzado del examen y de la prevención (AIP-SSM) (IPS) módulo.

Nota: El tráfico de la red que atraviesa el ASA incluye a los usuarios internos que tienen acceso a Internet o a los usuarios de Internet que tienen acceso a los recursos protegidos por el ASA en una zona desmilitarizada (DMZ) o la red interna. El tráfico de la red enviado a y desde el ASA no se envía al módulo ips para el examen. Un ejemplo del tráfico no enviado al módulo ips incluye hacer ping (ICMP) los interfaces o Telnetting ASA al ASA.

Nota: El Marco de políticas modular usado por el ASA para clasificar el tráfico para el examen no utiliza el IPv6. Tan si usted desvía el tráfico del IPv6 a los SSM AIP a través del ASA, no se utiliza.

Nota: Para más información sobre la configuración inicial de AIP-SSM, refiera a la configuración inicial del sensor AIP-SSM.

prerrequisitos

Requisitos

Este documento asume que la audiencia tiene una comprensión básica de cómo configurar la versión de software 8.x de Cisco ASA y la versión de software 6.x IPS.

- Los componentes de la configuración necesaria para ASA 8.x incluyen los interfaces, las Listas de acceso, el Network Address Translation (NAT), y la encaminamiento.
- Los componentes de la configuración necesaria para AIP-SSM (software 6.x IPS) incluyen la configuración de la red, no prohibida los host, la configuración de la interfaz, las definiciones de la firma, y las reglas de la acción del evento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5510 con la versión de software 8.0.2
- AIP-SSM-10 con la versión de software 6.1.2 IPS

Nota: Este ejemplo de la configuración es compatible con cualquier Firewall de las 5500 Series de Cisco ASA con OS 7.x y más adelante y el módulo AIP-SSM con IPS 5.x y más adelante.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este

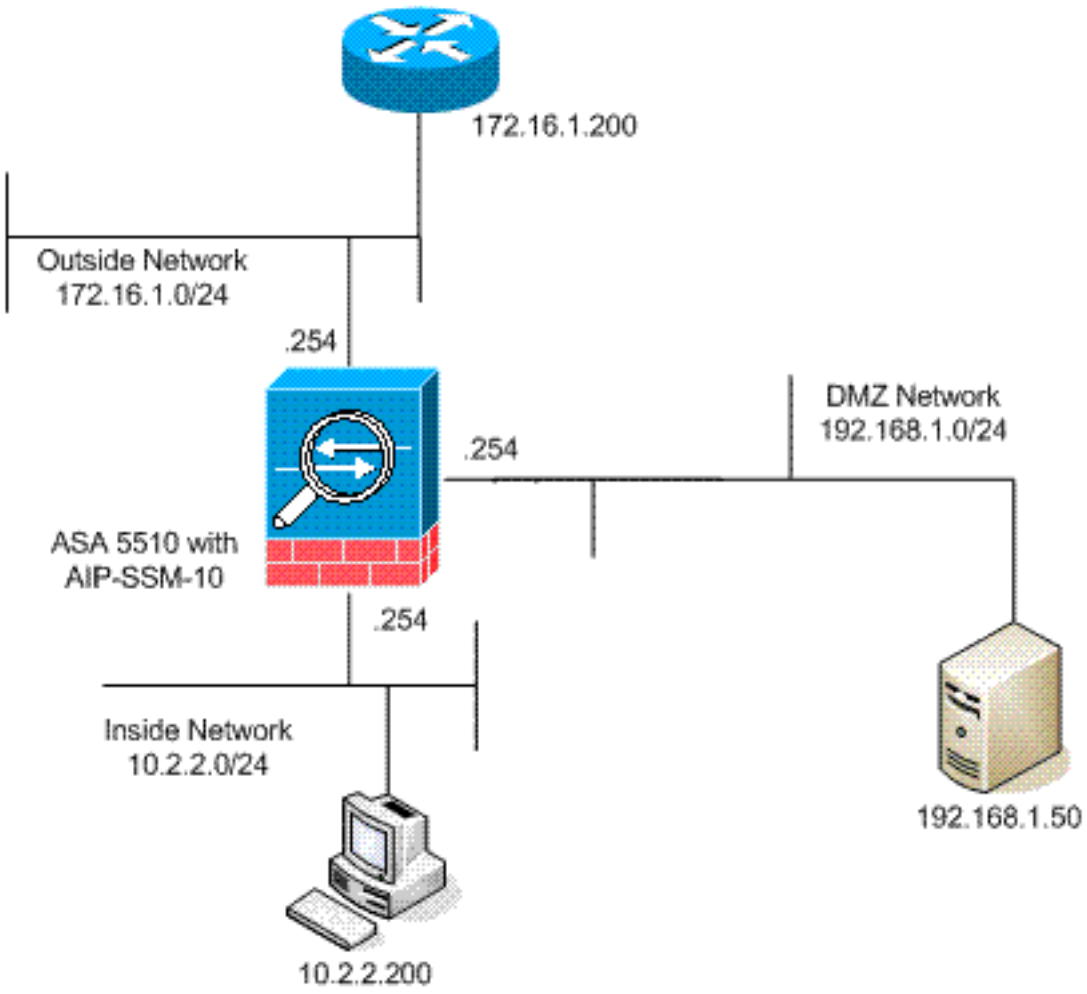
documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918 que se han utilizado en un entorno del laboratorio.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones iniciales

Este documento utiliza estas configuraciones. El comienzo ASA y AIP-SSM con una configuración de valor por defecto pero tiene cambios específicos realizados para comprobar. Las adiciones se observan en la configuración.

- 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
```

SSM AIP (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: Si usted es acceso incapaz el módulo AIP-SSM con los https, después complete estos pasos:

- Configure una dirección IP de la Administración para el módulo. Y usted puede configurar la `lista de acceso a la red`, en la cual usted especifica las redes IPs/IP que se permiten conectar con el IP de administración.
- Asegúrese de que usted haya conectado el interfaz externo de los Ethernetes del módulo AIP. El Acceso de administración al módulo AIP es posible a través de este interfaz solamente.

Refiera a AIP-SSM de incialización para más información.

Examine todo el tráfico con el AIP-SSM adentro en línea o el modo promiscuo

Los administradores de la red y la gerencia general de la compañía indican a menudo que todo necesita ser vigilado. Esta configuración cumple el requisito de vigilar todo. Además de vigilar todo, dos decisiones necesitan ser tomadas sobre cómo obran recíprocamente el ASA y los AIP-SSM.

- ¿Está el módulo AIP-SSM a funcionar o que se desplegará en el modo promiscuo o en línea?El modo promiscuo significa que una copia de los datos está enviada al AIP-SSM mientras que el ASA adelante las informaciones originales encendido al destino. El AIP-SSM en el modo promiscuo se puede considerar para ser un sistema de la detección de intrusos (identificación). En este modo, el paquete del activador (el paquete que causa la alarma) puede todavía alcanzar el destino. El evitar puede ocurrir y parar los paquetes adicionales de alcanzar el destino, no obstante el paquete del activador no se para.El modo en línea significa que el ASA adelante los datos al AIP-SSM para el examen. Si los datos pasan el examen AIP-SSM, los datos vuelven al ASA para continuar siendo procesado y siendo enviado al destino. El AIP-SSM en el modo en línea se puede considerar para ser un Sistema de prevención de intrusiones (IPS). A diferencia del modo promiscuo, el modo en línea (IPS) puede parar realmente el paquete del activador de alcanzar el destino.
- ¿En caso que el ASA no pueda comunicar con el AIP-SSM, cómo debe la manija ASA a-ser-examinada traficar? Los ejemplos de los casos cuando el ASA no puede comunicar con AIP-SSM incluyen las recargas AIP-SSM o si el módulo falla y necesita el reemplazo. En este caso el ASA puede fracaso-abierto o fracaso-cerrado.Fracaso-abierto permite que el ASA continúe pasando el tráfico a-ser-examinado al destino final si el AIP-SSM no puede ser alcanzado.los bloques Fracaso-cerrados a-ser-examinaron el tráfico cuando el ASA no puede comunicar con el AIP-SSM.**Nota:** El tráfico a-ser-examinado se define con el uso de una acceso-lista. En esta salida de ejemplo, la acceso-lista permite todo el tráfico IP de cualquier fuente a cualquier destino. Por lo tanto, el tráfico a-ser-examinado puede ser cualquier cosa que pasa a través del 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
```

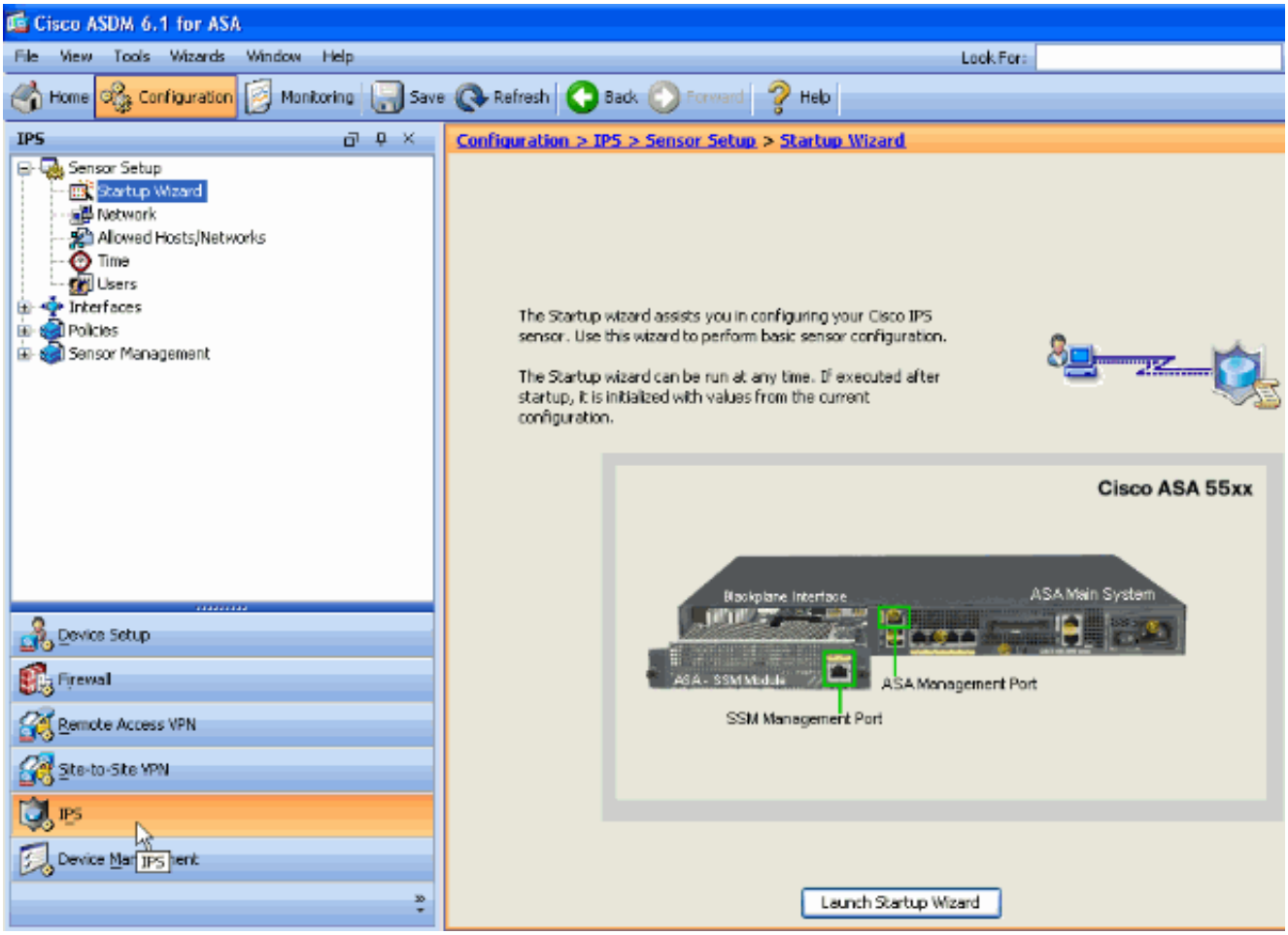
```
!--- Note that policy-map global_policy is a part of the !--- default configuration. In
addition, policy-map global_policy !--- is applied globally with the service-policy command.

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.
```

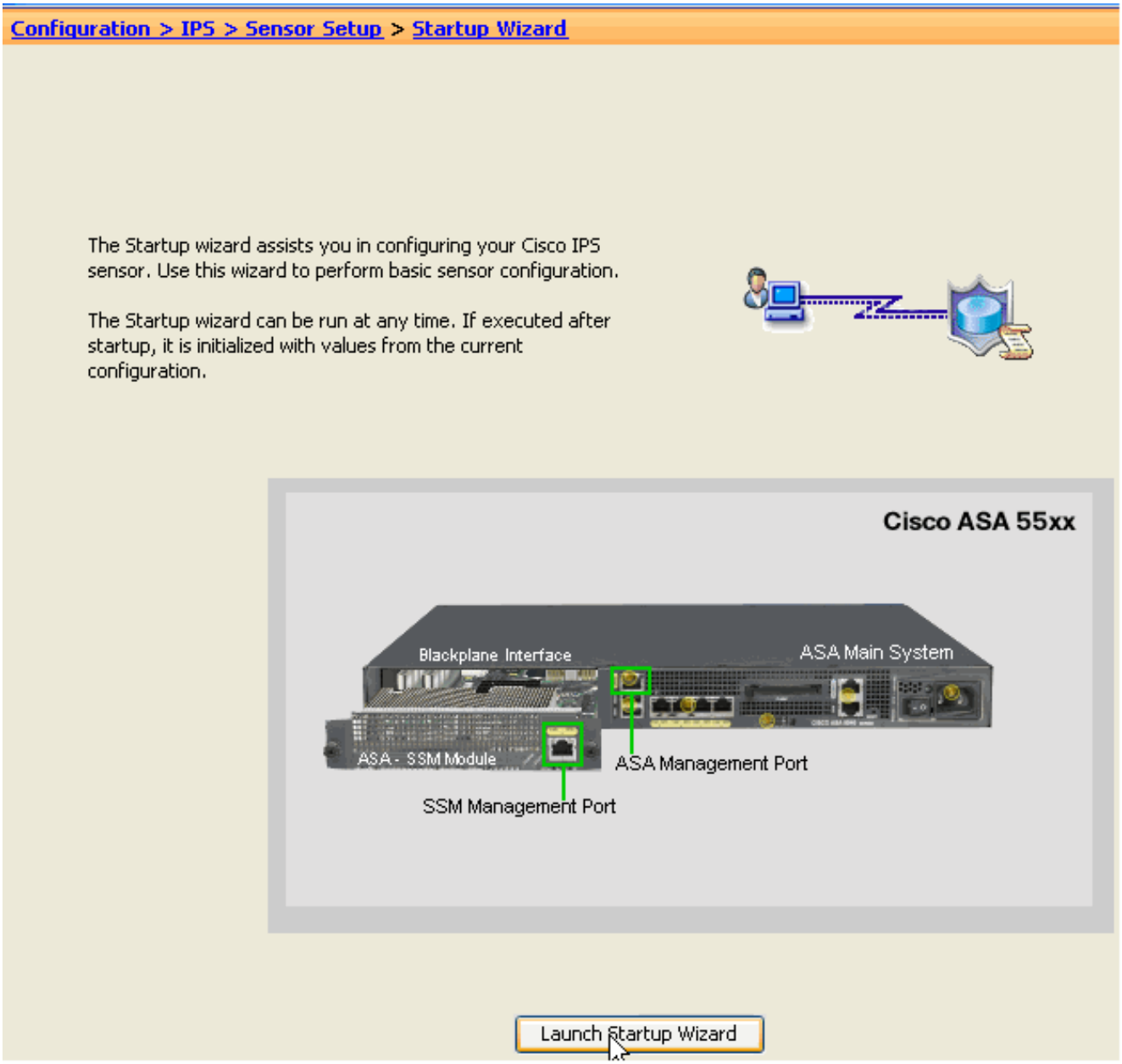
Examine todo el tráfico con el AIP-SSM usando ASDM

Complete estos pasos para examinar todo el tráfico con AIP-SSM que utilice ASDM:.

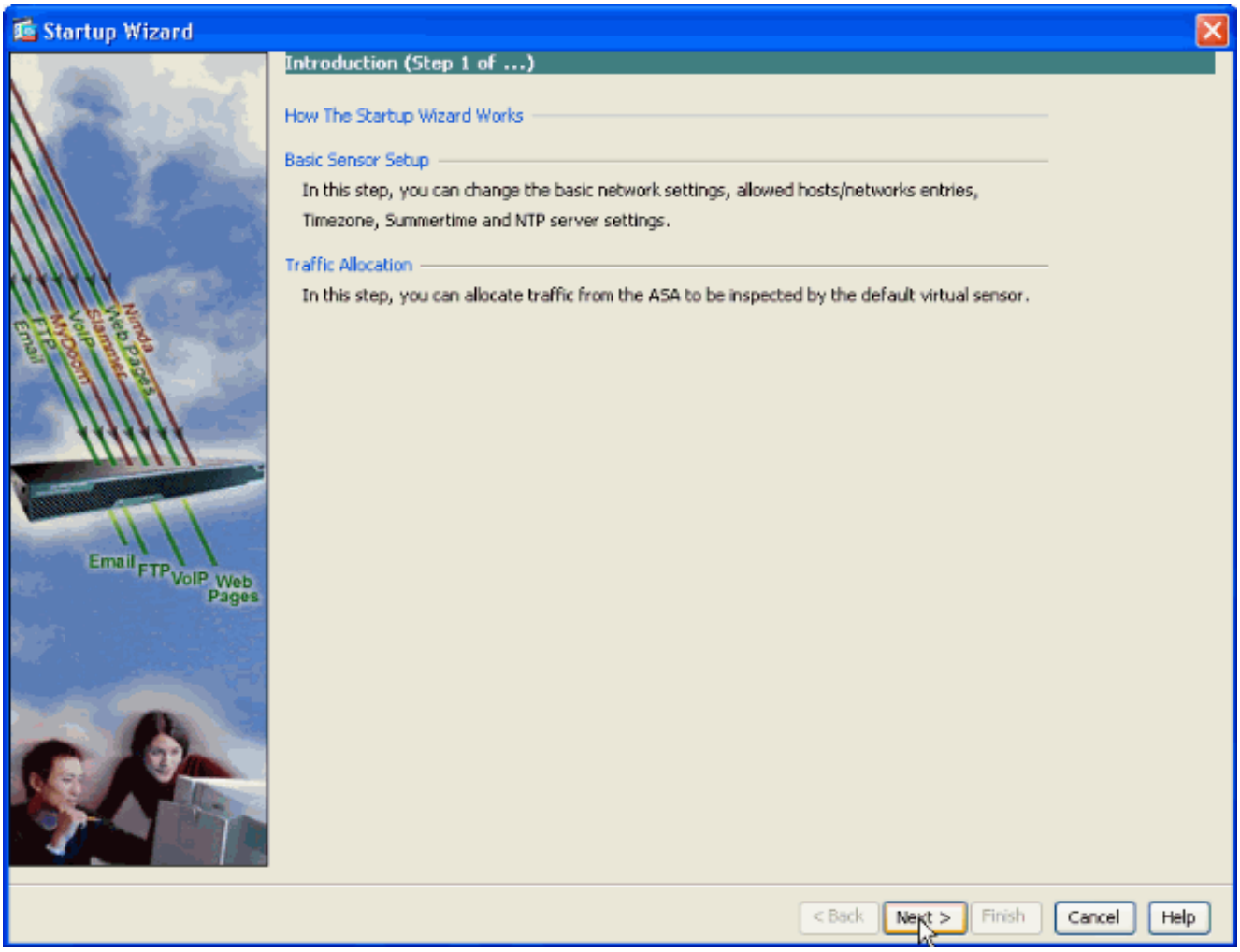
1. Elija la **configuración > el IPS > el sensor puesto > Asisitente de lanzamiento** en el Home Page ASDM para comenzar la configuración, como se muestra:



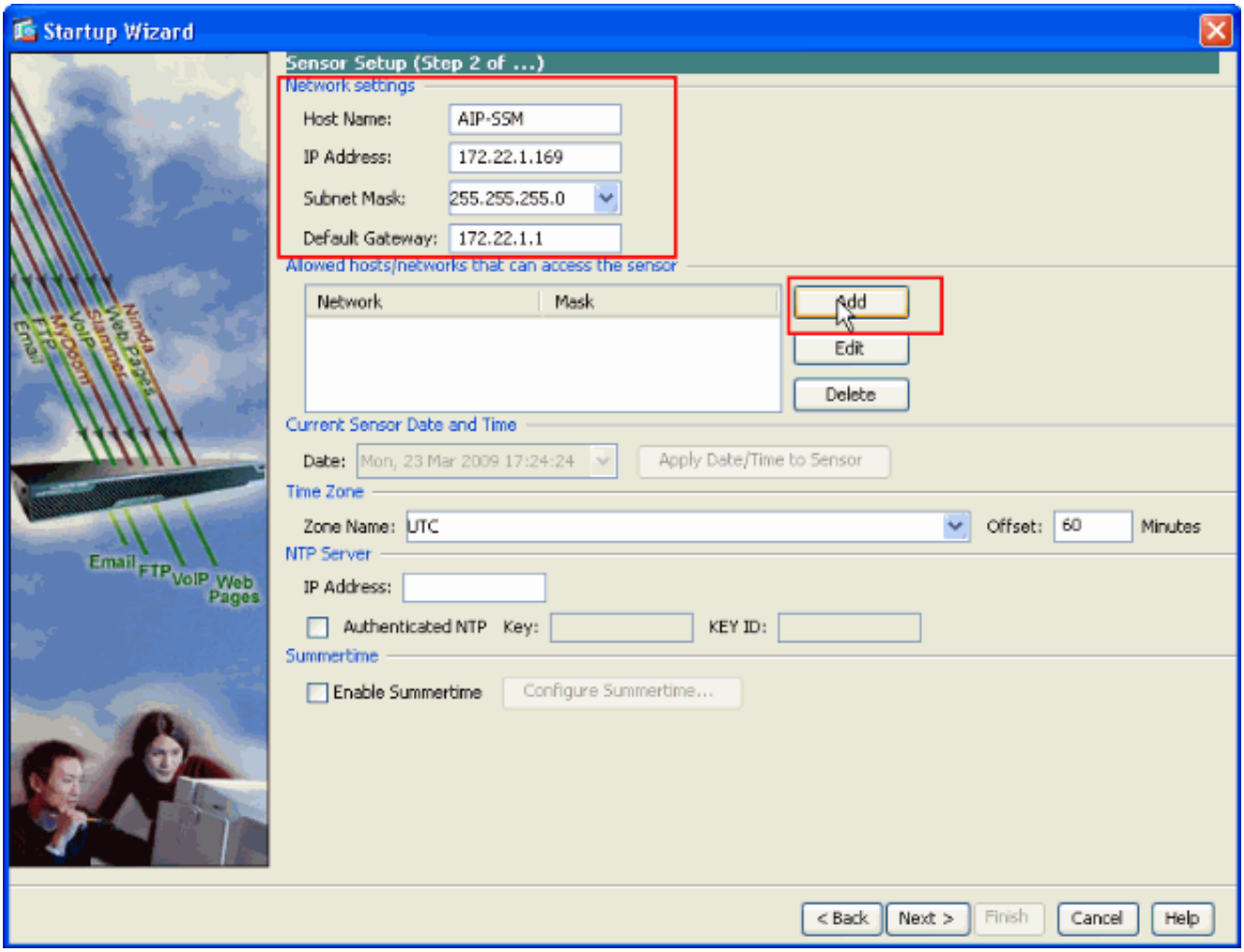
2. Haga clic al **Asisitente del lanzamiento del lanzamiento**.



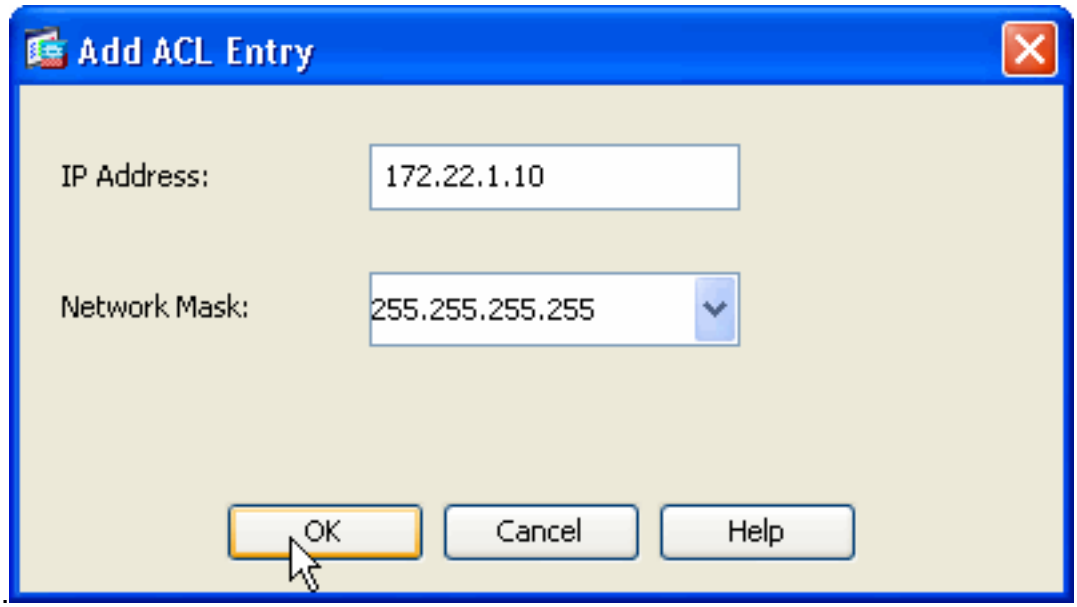
3. Haga clic **después** en la nueva ventana que sube después de que usted lance al Asisitente de
lanzamiento.



4. En la nueva ventana, proporcione al nombre de host, a la dirección IP, a la máscara de subred y a la dirección del gateway del valor por defecto para el módulo AIP-SSM en el espacio respectivo proporcionado bajo sección de las configuraciones de red. Entonces haga clic **agregan** para agregar las Listas de acceso para permitir todo el tráfico con AIP-SSM.

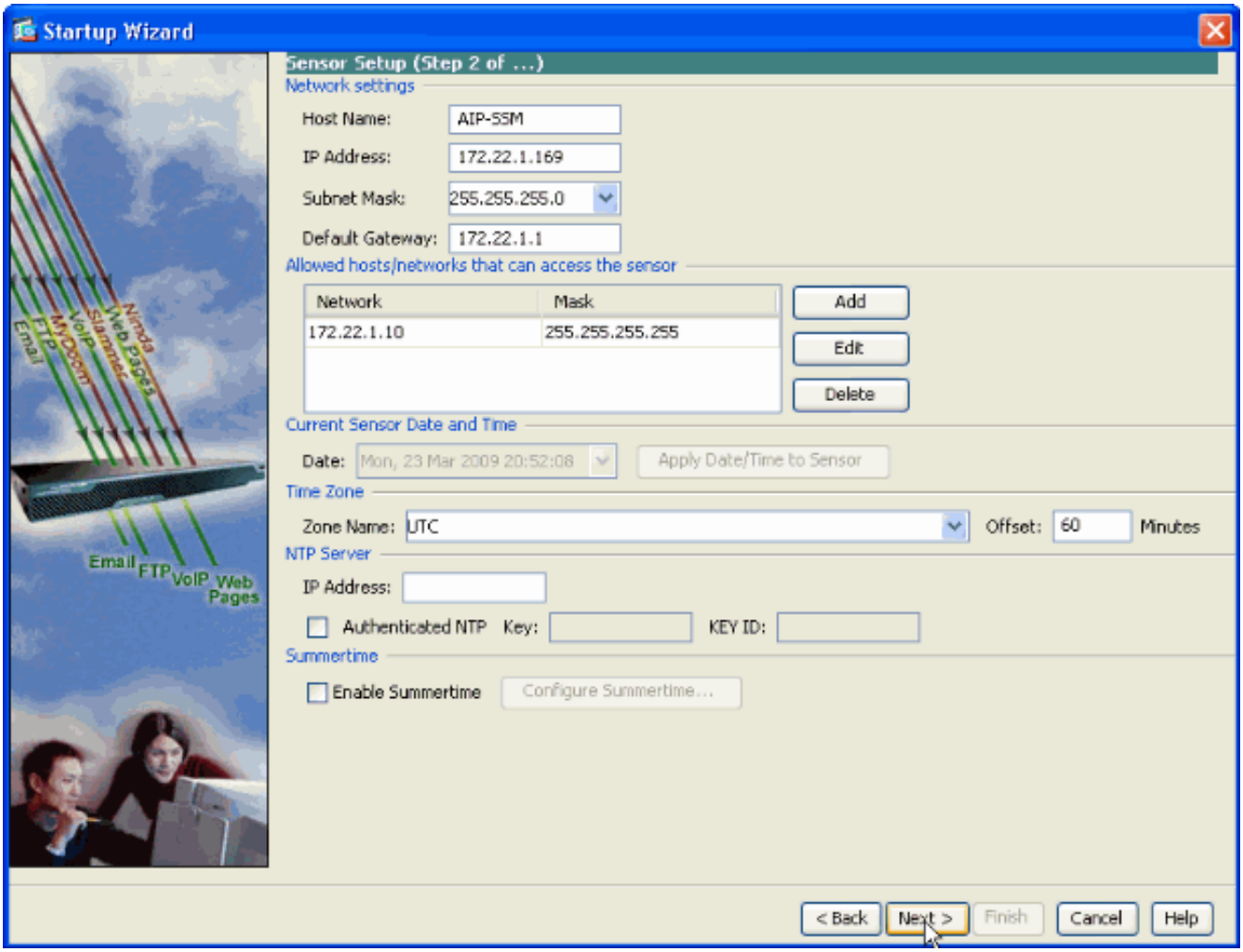


5. En la ventana de la **entrada ACL del agregar** proporcione a la **dirección IP** y a los detalles de la **máscara de la red de los** host/de las redes que se permitirán tener acceso al sensor. Click OK.**Nota:** La dirección IP del host/de la red debe pertenecer al rango de direccionamiento de red de

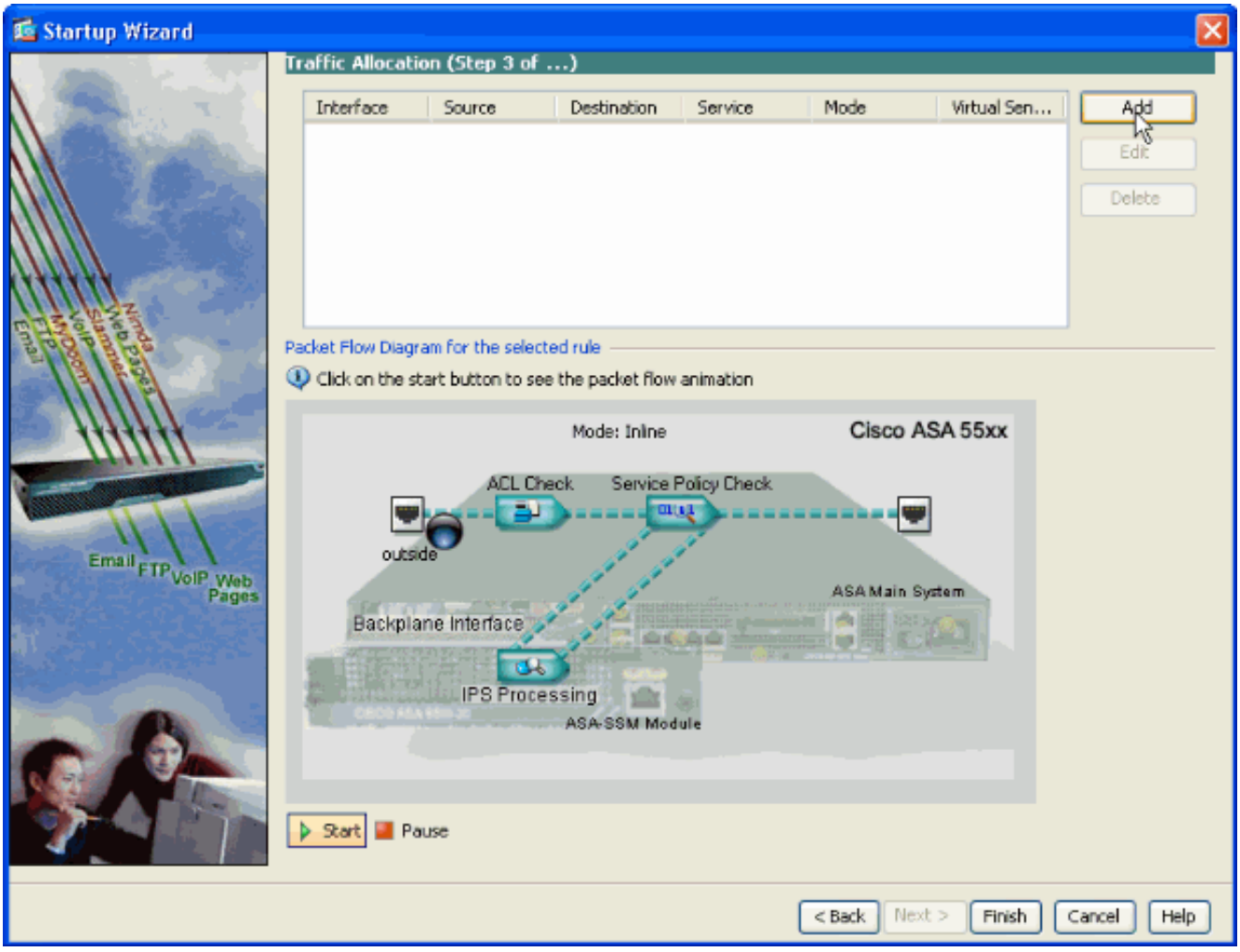


administración.

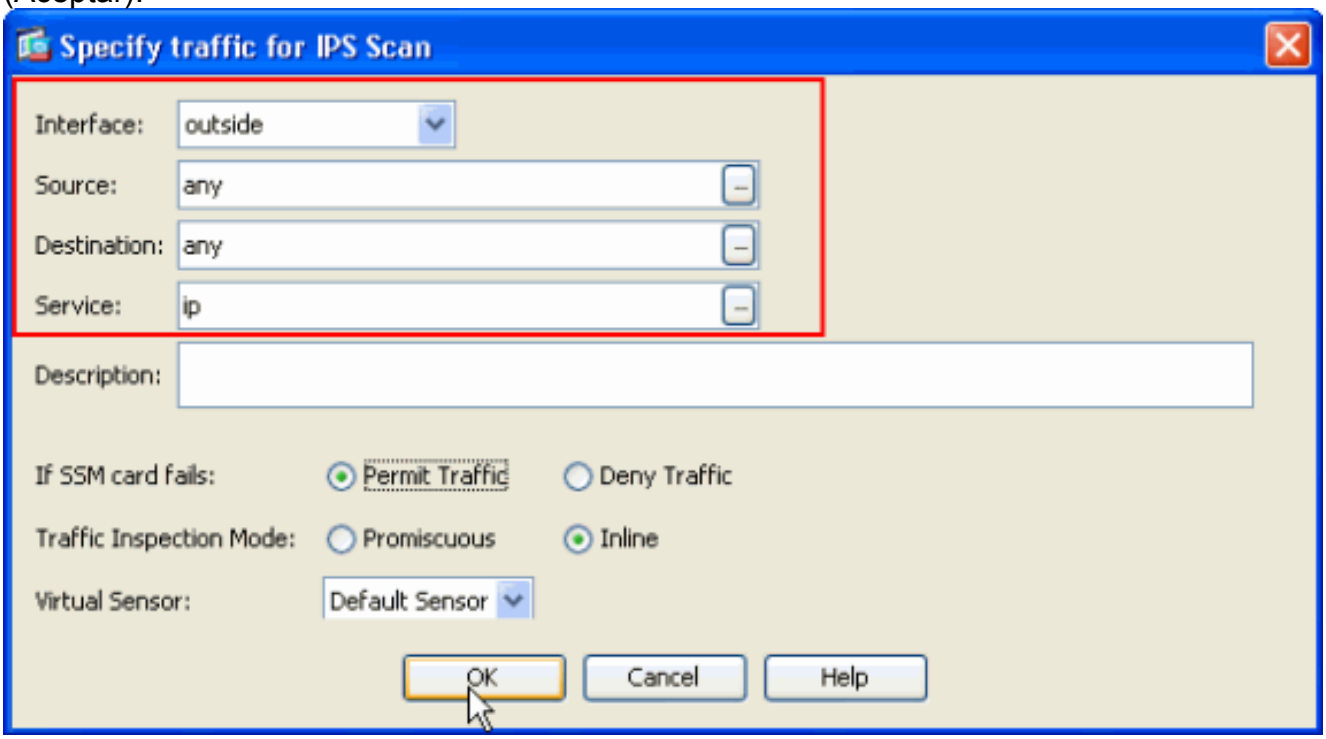
6. Tecleo **después** después de que usted proporcione a los detalles en los espacios respectivos proporcionados.



7. El tecleo **agrega** para configurar los detalles de la asignación del tráfico.

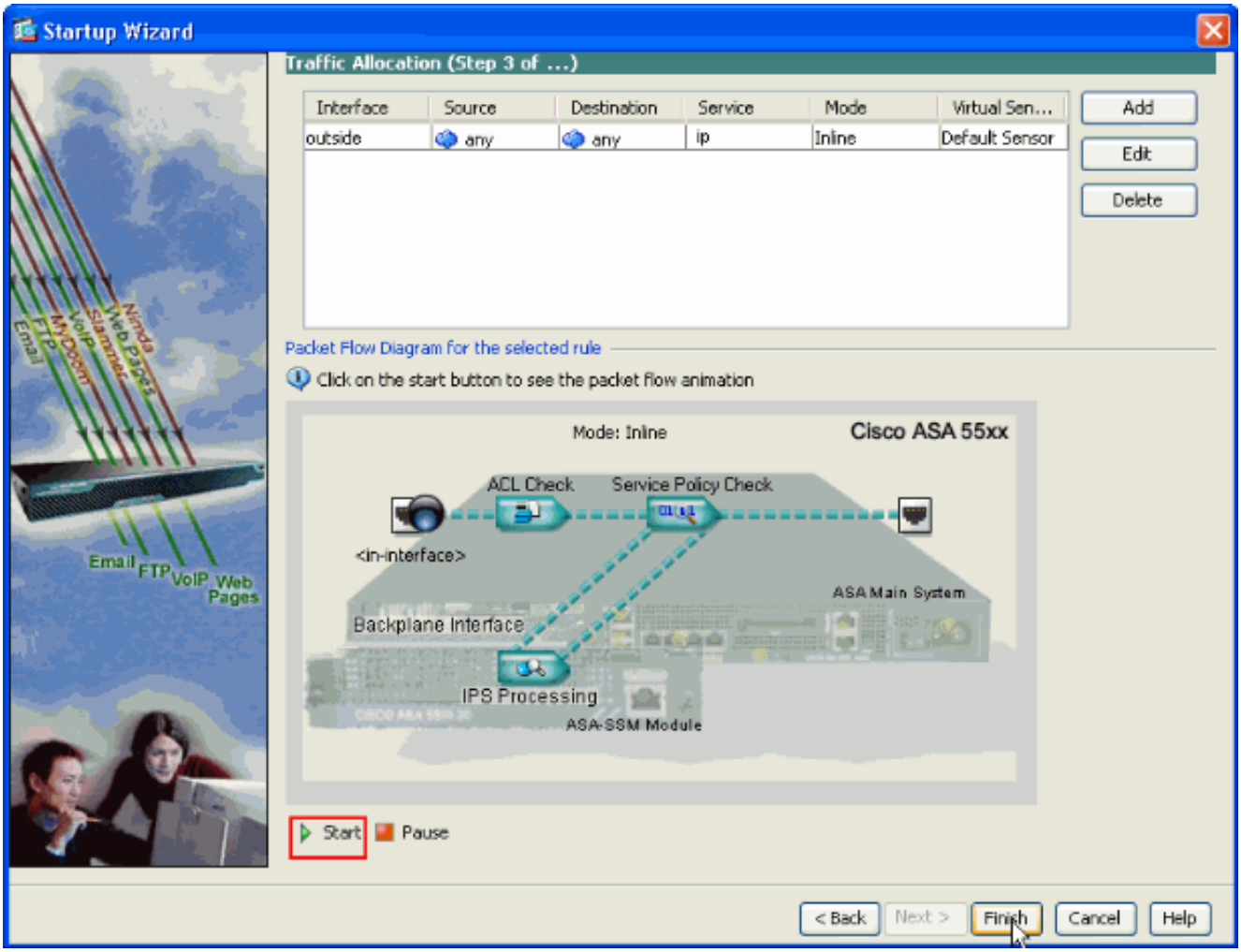


8. Proporcione a la fuente y utilizan el direccionamiento de red de destino y también al tipo de servicio, por ejemplo, IP aquí. En este ejemplo, **ninguno** se utiliza para la fuente y el destino mientras que usted examina todo el tráfico con AIP-SSM. Luego haga clic en OK (Aceptar).



9. Las reglas configuradas de la asignación del tráfico se muestran en esta ventana y usted puede agregar tantas reglas según las necesidades si usted completa el mismo procedimiento como se explica en los pasos 7 y 8. Entonces el clic en Finalizar y éste

completa el Procedimiento de configuración ASDM.**Nota:** Usted puede ver la animación del flujo de paquetes si usted hace clic en el **comienzo**.



Examine el tráfico específico con el AIP-SSM

En caso que el administrador de la red quiera tener el monitor AIP-SSM como subconjunto de todo el tráfico, el ASA tiene dos variables independientes que puedan ser modificadas. Primero, la acceso-lista se puede escribir para incluir o para excluir el tráfico necesario. Además de la modificación de las Listas de acceso, una servicio-**directiva** puede ser aplicada a un interfaz o global para cambiar el tráfico examinadas por el AIP-SSM.

Referente al diagrama de la red en este documento, el administrador de la red quisiera que el AIP-SSM examinara *todo el* tráfico entre la red externa y la red 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.
```

Después, el administrador de la red quisiera que el AIP-SSM vigilara el tráfico *iniciado de la* red interna a la red externa. La red interna a la red DMZ no se vigila.

Nota: Esta sección determinada requiere una comprensión intermedia del statefulness, del TCP, del UDP, del ICMP, de la conexión, y de las comunicaciones sin conexión.

```
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
```

La acceso-lista niega el tráfico iniciado en la red interna destinada para la red DMZ. La segunda línea de la acceso-lista permite o envía el tráfico iniciado en la red interna destinada para la red externa al AIP-SSM. A este punto el statefulness del ASA entra en el juego. Por ejemplo, un usuario interno inicia una conexión TCP (Telnet) a un dispositivo en la red externa (router). El usuario conecta con éxito con el router y abre una sesión. El usuario entonces publica un comando router que no se autorice. El router responde con el `authorizaton del comando fallado`. El paquete de datos que contiene la cadena `fallada comando authorization` tiene una fuente del router externo y de un destino del usuario interior. La fuente (afuera) y el destino (dentro) no hacen juego las Listas de acceso definidas previamente en este documento. El ASA no pierde de vista las conexiones stateful, debido a esto, el paquete de datos que las devoluciones (afuera ante el interior) están enviadas al AIP-SSM para el examen. La firma de encargo 60000 0, que se configura en el AIP-SSM, alarma.

Nota: Por abandono, el ASA no guarda el estado para el tráfico ICMP. En la configuración de muestra anterior, el usuario interno hace ping (petición de la generación de eco ICMP) al router externo. El router responde con la Respuesta de eco ICMP. El AIP-SSM examina el paquete de pedidos de la generación de eco pero no el paquete de la Respuesta de eco. Si el examen ICMP se activa en el ASA, ambos los paquetes de la petición y de la Respuesta de eco de la generación de eco son examinados por el AIP-SSM.

Excluya el tráfico de la red específico de la exploración AIP-SSM

El ejemplo generalizado dado proporciona a una visión en la exención del tráfico específico que se analizará por AIP-SSM. Para realizar esto, usted necesita crear una acceso-lista que contenga el flujo de tráfico que debe ser excluido de la exploración AIP-SSM en el enunciado de negación. En este ejemplo, el IPS es el nombre de la acceso-lista que define el flujo de tráfico que se analizará por AIP-SSM. Trafique entre el <source> y <destination> se excluyen de la exploración; se examina el resto del tráfico.

```
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
```

Verificación

Verifique que los eventos alertas estén registrados en el AIP-SSM.

Registro en el AIP-SSM con la cuenta de usuario del administrador. El comando **alerta de los eventos de la demostración** genera esta salida.

Nota: La salida varía basado en las configuraciones, el tipo de tráfico enviado al AIP-SSM, y la carga de la red de la firma.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida 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
```

En las configuraciones de muestra, varias firmas IPS se adaptan para alarmar en el tráfico de prueba. Se modifica la firma 2000 y 2004. Se agrega la firma de encargo 60000. En un entorno del laboratorio o una red adonde pocos datos pasan a través del ASA, puede ser necesario modificar las firmas para accionar los eventos. Si el ASA y los AIP-SSM se despliegan en un entorno que pase una gran cantidad de tráfico, las configuraciones de la firma del valor por defecto son probables generar un evento.

Troubleshooting

Esta sección brinda información que puede utilizar para la solución de problemas en su configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Publique estos **comandos show del** ASA.

- **módulo de la demostración** — Información de las demostraciones sobre los SSM en la información ASA así como de 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.
```

- **acceso-lista de la demostración** — Muestra los contadores para una acceso-lista.

```
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.
```

¿Antes de que usted instale y utilice el AIP-SSM, el tráfico de la red pasa a través del ASA como se esperaba? Si no, puede ser necesario resolver problemas las reglas de la red y de la política de acceso ASA.

Problemas con la Conmutación por falla

- Si usted tiene dos ASA en una configuración de failover y cada uno tiene un AIP-SSM, usted debe replicar manualmente la configuración del AIP-SS. Solamente la configuración del ASA es replegada por el mecanismo de failover. El AIP-SSM no se incluye en el failover. Refiera al PIX/ASA ejemplo activo/espera 7.x de la Conmutación por falla de la configuración para más información sobre los problemas de la Conmutación por falla.
- El AIP-SSM no participa en la falla de estado si configuran a la falla de estado en el par de fallas ASA.

Mensajes de error

El módulo ips (AIP-SSM) produce los mensajes de error los eventos como se muestra y que no encienden.

```
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 para este mensaje de error es que el sensor virtual IPS no fue asignado a la interfaz de backplane del ASA. El ASA se pone de la manera correcta para enviar el tráfico al módulo SSM, pero usted necesita asignar el sensor virtual a la interfaz de backplane que el ASA crea para que los SSM analicen el tráfico.

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

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

Estos mensajes son indicativos del REGISTRO IP que es activado, que a su vez hogged encima de todos los recursos del sistema. Cisco recomienda inhabilitar el REGISTRO IP mientras que debe ser utilizado solamente para resolver problemas/los propósitos investigadores solamente.

Nota: `Puente en línea errWarning de los datos ha comenzado el` mensaje de error es conducta esperada mientras que el sensor recomienza momentáneamente el motor del análisis después de la actualización de firma, que es una parte de necesaria el proceso de la actualización de firma.

Soporte de Syslog

El AIP-SSM no utiliza el Syslog pues un formato alerta.

El método predeterminado para recibir la información alerta del AIP-SSM está con el intercambio del evento del dispositivo de seguridad (SDEE). Otra opción es configurar las firmas individuales para generar un SNMP trap como acción para tomar cuando se accionan.

Reinicialización AIP-SSM

El módulo AIP-SSM no responde correctamente.

Si no responde el módulo AIP-SSM correctamente, después reinicie el módulo AIP-SSM sin reiniciar el ASA. Utilice el comando reload del módulo 1 del hw-módulo para reiniciar el módulo AIP-SSM y no reinicie el ASA.

Alerta del correo electrónico AIP-SSM

¿Puede AIP-SSM enviar las alertas del correo electrónico a los usuarios?

No, no se utiliza.

Información Relacionada

- Referencia del comando del dispositivo del Cisco Security, versión 7.2
- Mensajes del registro del sistema del dispositivo del Cisco Security, versión 7.2
- Referencia del comando para el Cisco Intrusion Prevention System 5.1
- Soporte Técnico y Documentación - Cisco Systems