ASA: Exemplo de Configuração para Envio de Tráfego de Rede do ASA para o AIP-SSM

Índice

Introdução

Este documento fornece uma configuração de exemplo de como enviar tráfego de rede que passa pelo Cisco ASA 5500 Series Adaptive Security Appliance (ASA) até o módulo Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS). Exemplos de configuração com a Command Line Interface (CLI) são fornecidos.

Refira o ASA: Exemplo de Configuração para Envio de Tráfego de Rede do ASA para o CSC-SSM para enviar tráfego do Cisco ASA 5500 Series Adaptive Security Appliance (ASA) para o Content Security and Control Security Services Module (CSC-SSM).

Refira a atribuição de sensores virtuais a um contexto de segurança (AIP SS somente) para obter mais informações sobre de como enviar o tráfego de rede que passa através da ferramenta de segurança adaptável do 5500 Series de Cisco ASA (ASA) no modo de contexto múltiplo ao módulo de Serviços de segurança avançado da inspeção e da prevenção (AIP-SSM) (IPS) módulo.

Nota: O tráfego de rede que atravessa o ASA inclui os usuários internos que alcançam o Internet ou os usuários do Internet que alcançam os recursos protegidos pelo ASA em uma zona desmilitarizada (DMZ) ou na rede interna. O tráfego de rede enviado a e do ASA não é enviado ao módulo ips para a inspeção. Um exemplo do tráfego não enviado ao módulo ips inclui sibilar (ICMP) as relações ou Telnetting ASA ao ASA.

Nota: A estrutura de política modular usada pelo ASA a fim classificar o tráfego para a inspeção não apoia o IPv6. Assim, não é possível desviar o tráfego IPv6 para o AIP SSM pelo ASA.

Nota: Para obter mais informações sobre da configuração inicial de AIP-SSM, refira a configuração inicial do sensor AIP-SSM.

Pré-requisitos

Requisitos

Este documento supõe que a audiência tem uma compreensão básica de como configurar a versão de software 8.x de Cisco ASA e a versão de software 6.x IPS.

- Os componentes da configuração necessária para ASA 8.x incluem relações, listas de acesso, Network Address Translation (NAT), e roteamento.
- Os componentes da configuração necessária para AIP-SSM (software 6.x IPS) incluem a instalação de rede, permitida anfitriões, configuração da interface, definições da assinatura, e regras da ação do evento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5510 com versão de software 8.0.2
- AIP-SSM-10 com versão de software 6.1.2 IPS

Nota: Este exemplo de configuração é compatível com todo o Firewall do 5500 Series de Cisco ASA com OS 7.x e mais tarde e o módulo AIP-SSM com IPS 5.x e mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

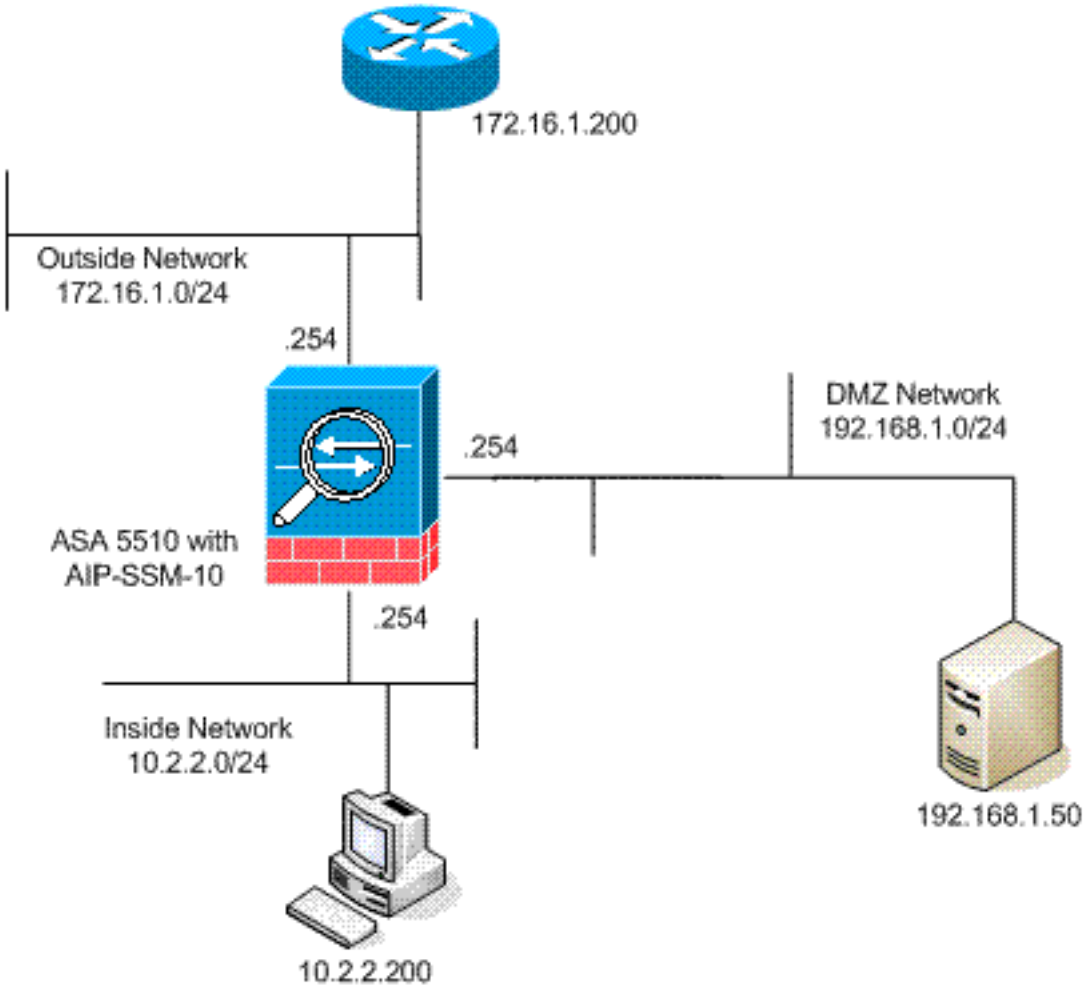
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações inicial

Este documento utiliza estas configurações. O começo ASA e AIP-SSM com uma configuração padrão mas tem as mudanças específicas feitas para propósitos testando. As adições são notadas na configuração.

- 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 SS (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 você é acesso incapaz o módulo AIP-SSM com https, termine então estas etapas:

- Configurar um endereço IP de gerenciamento para o módulo. E você pode configurar a `lista de acesso de rede`, em que você especifica as redes IPs/IP que são permitidas conectar ao IP de gerenciamento.
- Certifique-se de que você conectou a interface Ethernet externo do módulo de AIP. O acesso de gerenciamento ao módulo de AIP é possível através desta relação somente.

Refira a inicialização de AIP-SSM para mais informação.

Inspecione todo o tráfego com o AIP-SSM dentro inline ou modo misturado

Os administradores de rede e o gerenciamento sênior da empresa indicam frequentemente que tudo precisa de ser monitorado. Esta configuração cumpre a exigência monitorar tudo. Além do que a monitoração de tudo, duas decisões precisam de ser feitas sobre como o ASA e os AIP-SSM interagem.

- Reage o módulo AIP-SSM a funcionar ou ser distribuído do modo promíscuo ou inline?O modo misturado significa que uma cópia dos dados estiver enviada ao AIP-SSM quando o

ASA para a frente os dados originais sobre ao destino. O AIP-SSM no modo misturado pode ser considerado para ser um sistema de detecção de intrusões (IDS). Neste modo, o pacote do disparador (o pacote que causa o alarme) pode ainda alcançar o destino. Evitar pode ocorrer e parar pacotes adicionais de alcançar o destino, porém o pacote do disparador não é parado.O modo Inline significa que o ASA para a frente os dados ao AIP-SSM para a inspeção. Se os dados passam a inspeção AIP-SSM, os dados retornam ao ASA a fim continuar a ser processado e a enviaa ao destino. O AIP-SSM no modo inline pode ser considerado para ser um Intrusion Prevention System (IPS). Ao contrário do modo misturado, o modo inline (IPS) pode realmente parar o pacote do disparador de alcançar o destino.

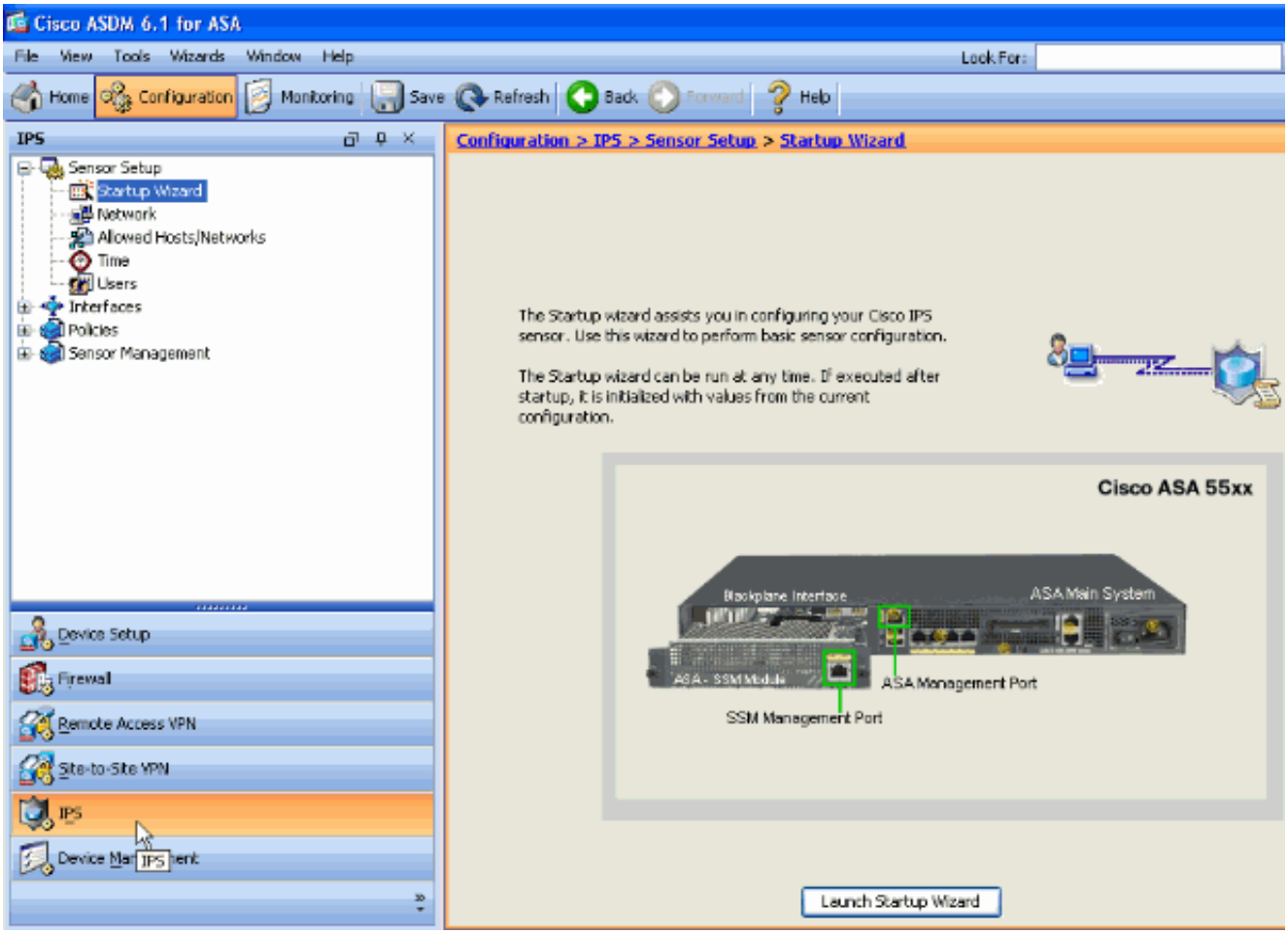
- Caso o ASA não puder se comunicar com o AIP-SSM, como deve o punho ASA à-estar-inspecionado traficar? Os exemplos dos exemplos quando o ASA não pode se comunicar com o AIP-SSM incluem reloads AIP-SSM ou se o módulo falha e precisa a substituição. Neste caso o ASA pode falha-aberto ou falha-fechado.Falha-aberto permite que o ASA continue a passar o tráfego à-estar-inspecionado ao destino final se o AIP-SSM não pode ser alcançado.os blocos Falha-fechados à-estar-inspecionaram o tráfego quando o ASA não pode se comunicar com o AIP-SSM.**Nota:** O tráfego à-estar-inspecionado é definido com o uso de uma lista de acesso. Nestas saídas de exemplo, a lista de acesso permite todo o tráfego IP de toda a fonte a qualquer destino. Consequentemente, o tráfego à-estar-inspecionado pode ser qualquer coisa que passa com o 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.
```

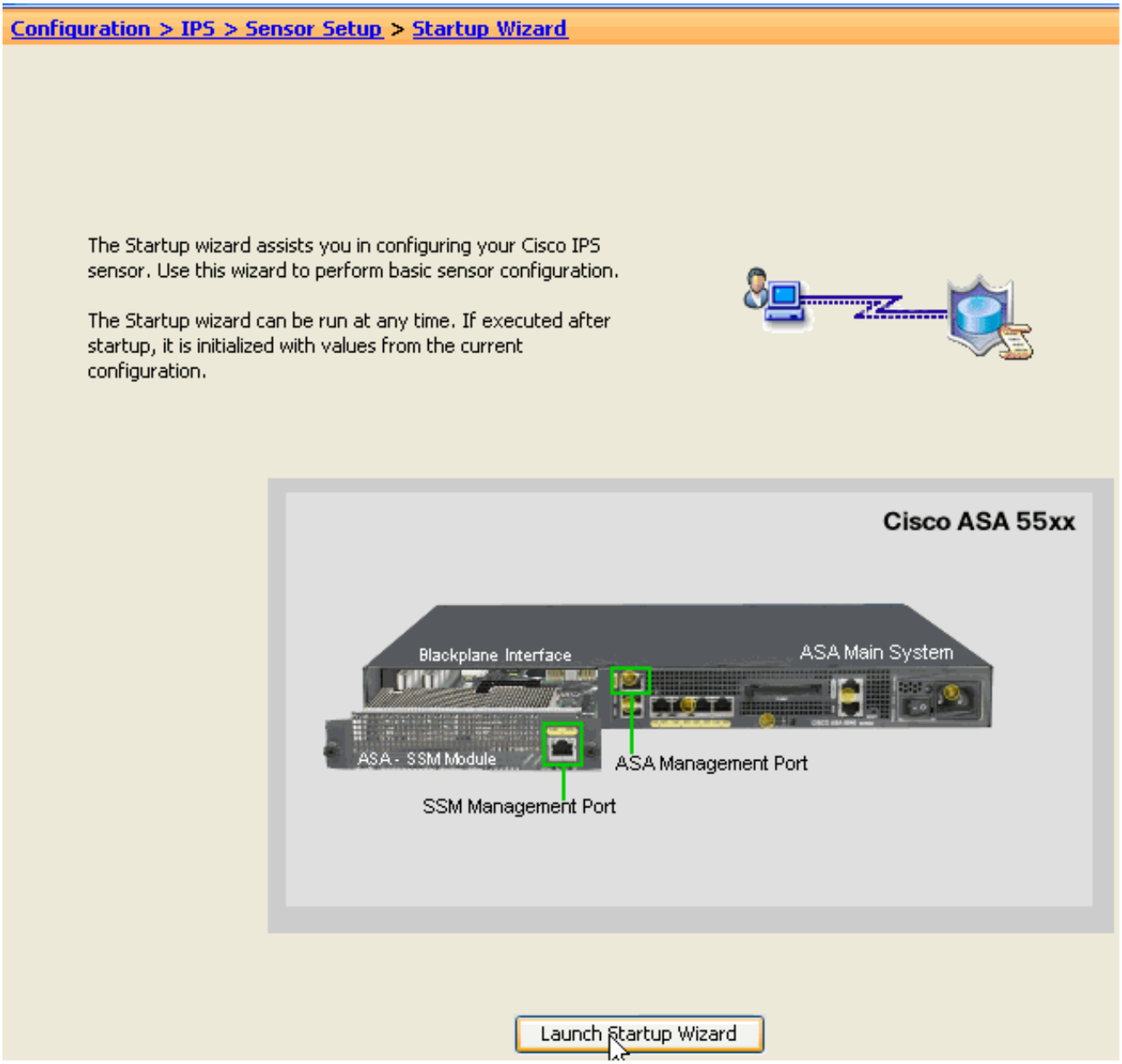
Inspecione todo o tráfego com o AIP-SSM usando o ASDM

Termine estas etapas a fim inspecionar todo o tráfego com AIP-SSM que usa o ASDM:.

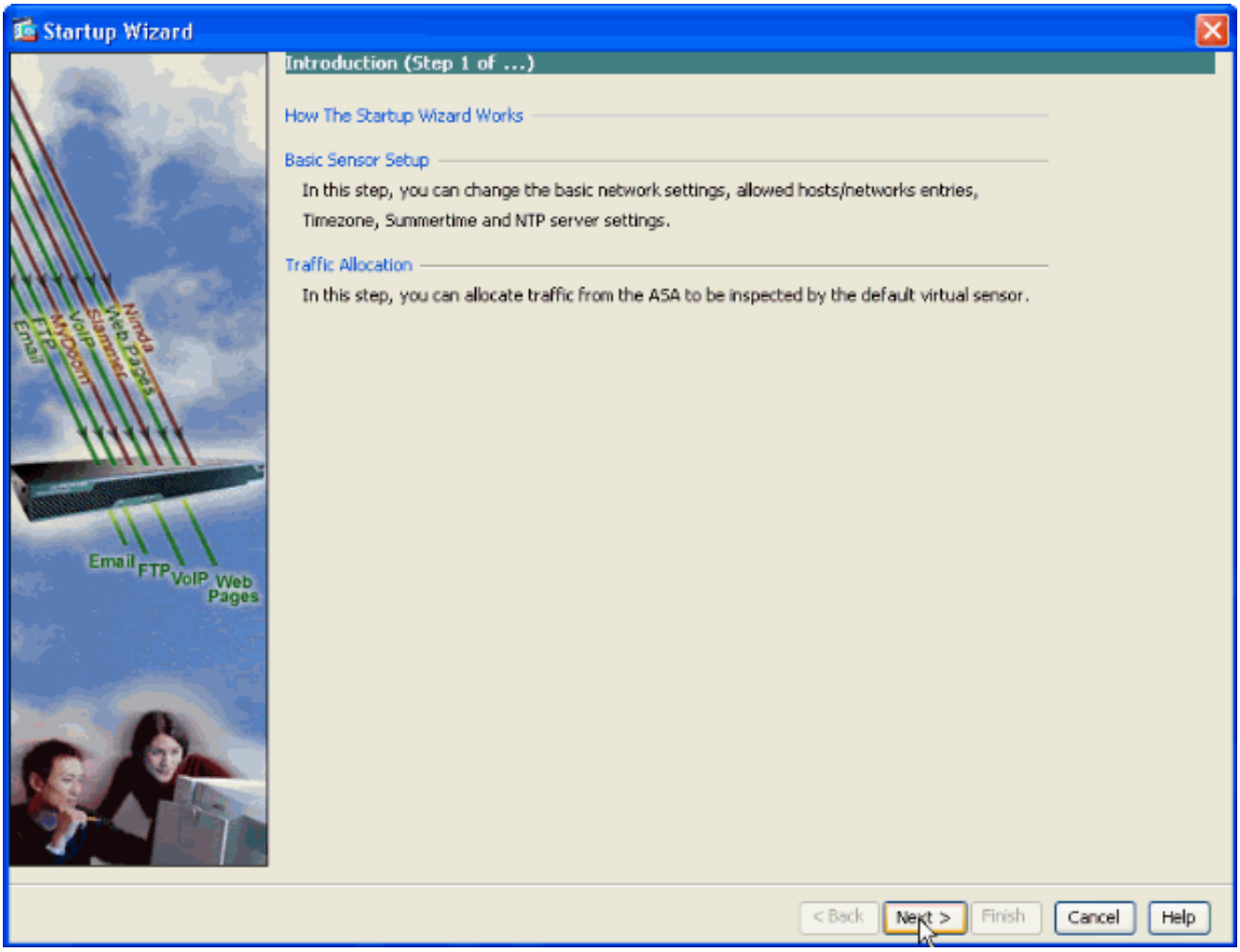
1. Escolha a **configuração > o IPS > o sensor Setup > assistente Startup no** Home Page ASDM para começar a configuração, como
   mostrado:



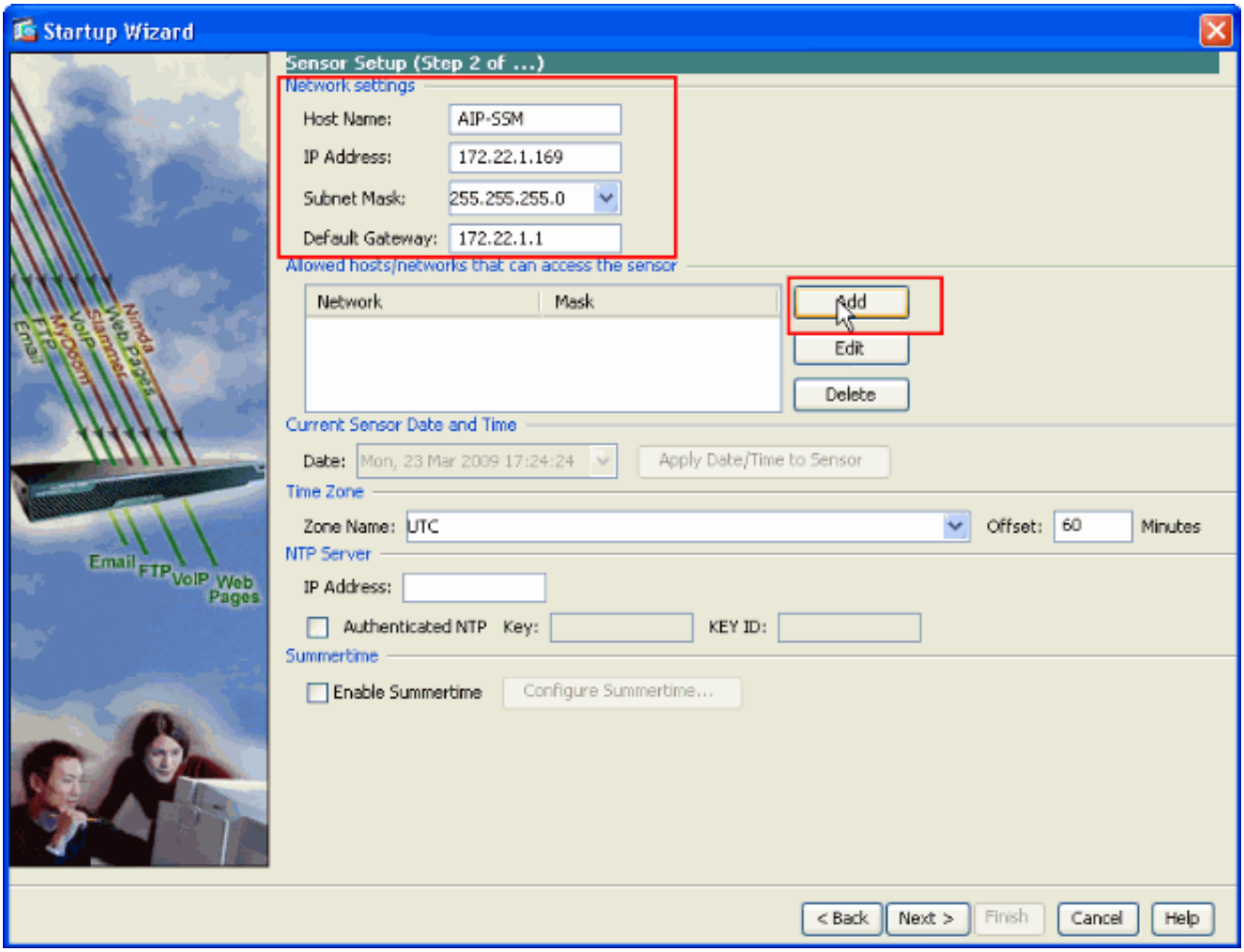
2. Clique o **assistente da partida do lançamento**.



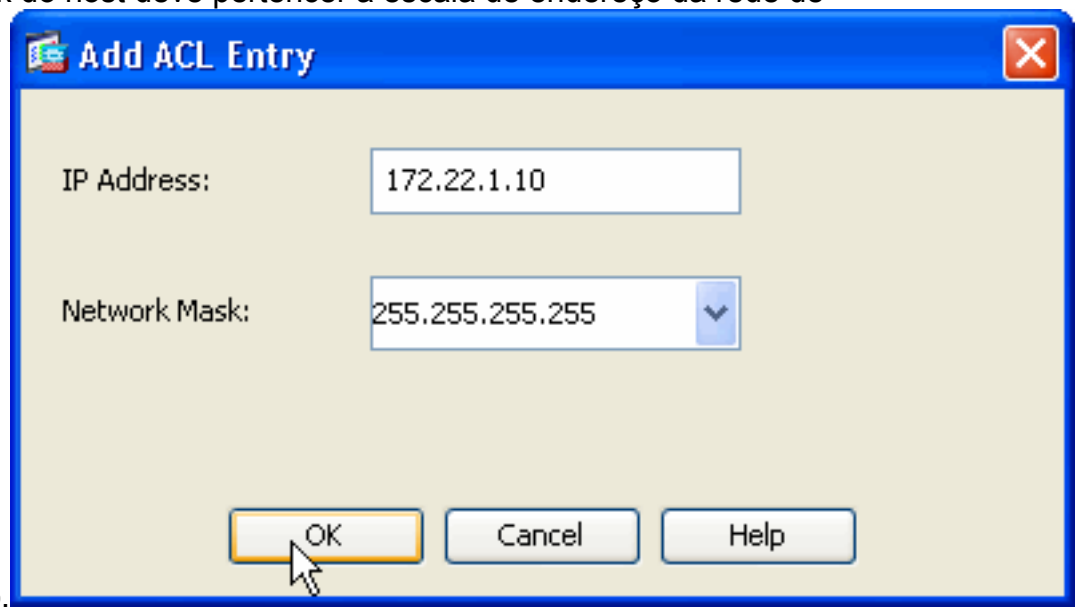
3. Clique **em seguida na** nova janela que vem acima depois que você lança o assistente startup.



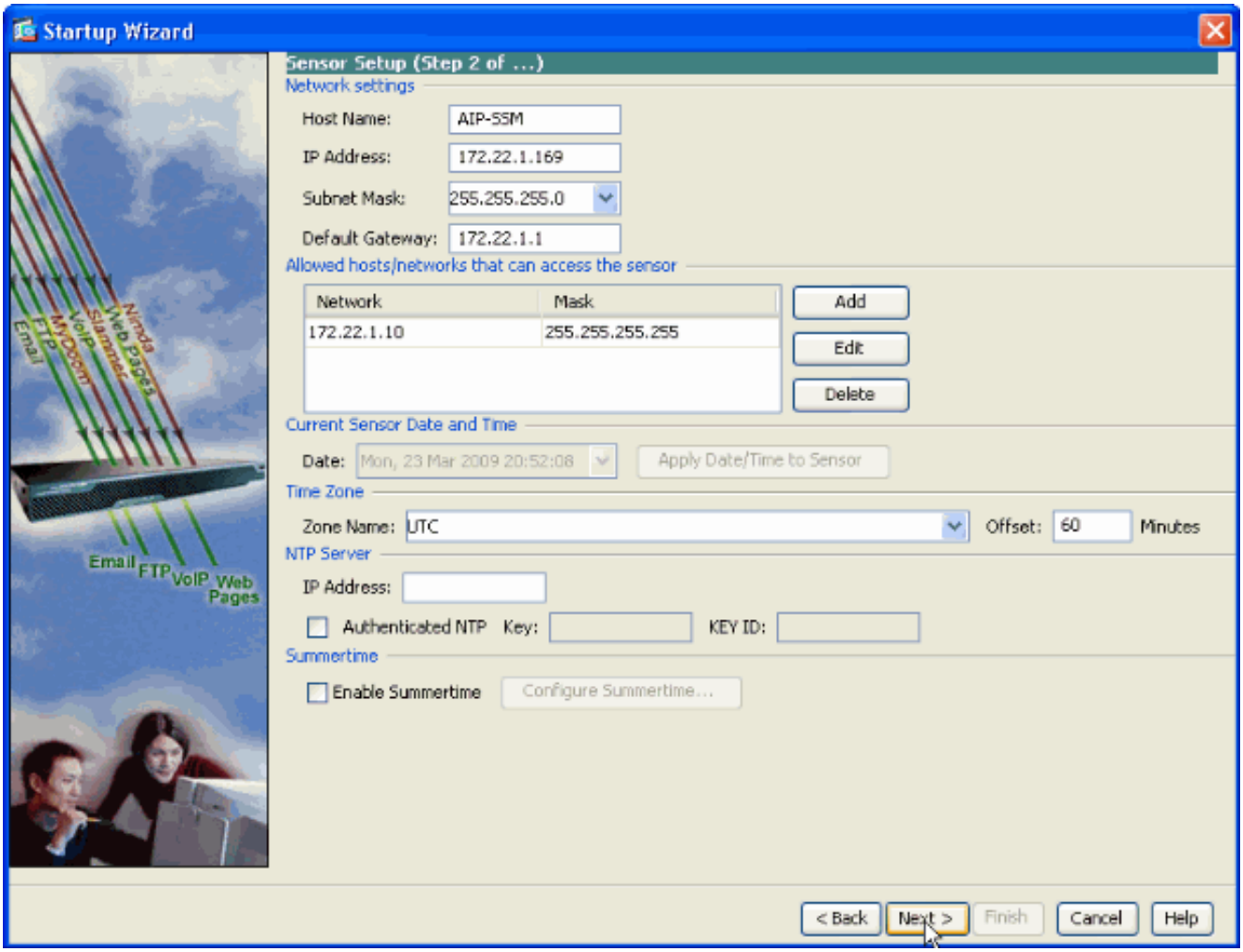
4. Na nova janela, forneça o nome de host, o endereço IP de Um ou Mais Servidores Cisco ICM NT, a máscara de sub-rede e o endereço de gateway padrão para o módulo AIP-SSM no espaço respectivo fornecido sob a seção das configurações de rede. Clique então **adicionam** a fim adicionar as listas de acesso para permitir todo o tráfego com AIP-SSM.



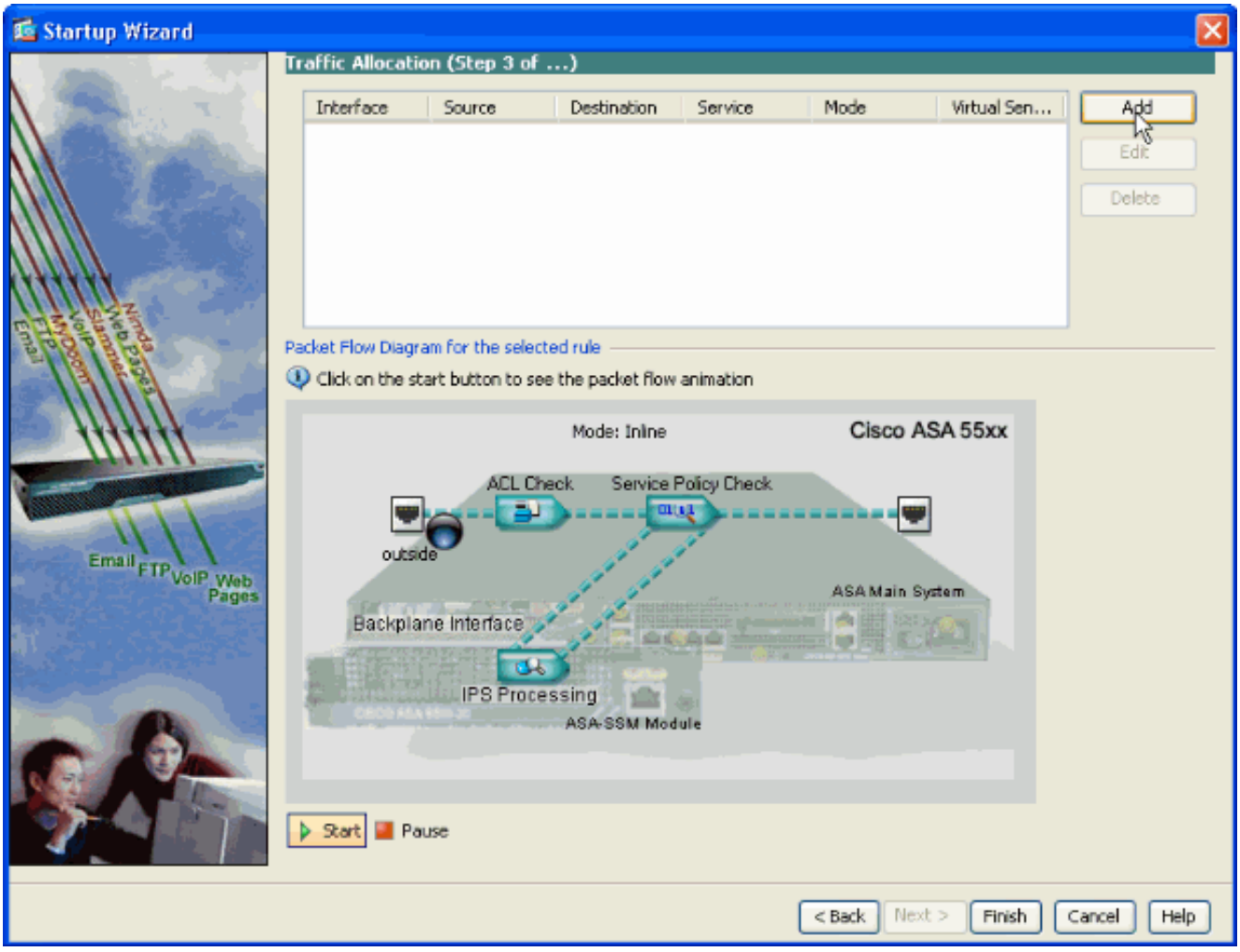
5. No indicador da **entrada ACL adicionar** forneça o **endereço IP de Um ou Mais Servidores Cisco ICM NT** e os detalhes da **máscara de rede dos** anfitriões/redes a ser reservados alcançar o sensor. Clique em **OK**.**Nota:** O endereço IP de Um ou Mais Servidores Cisco ICM NT do /Network do host deve pertencer à escala de endereço da rede de gerenciamento.



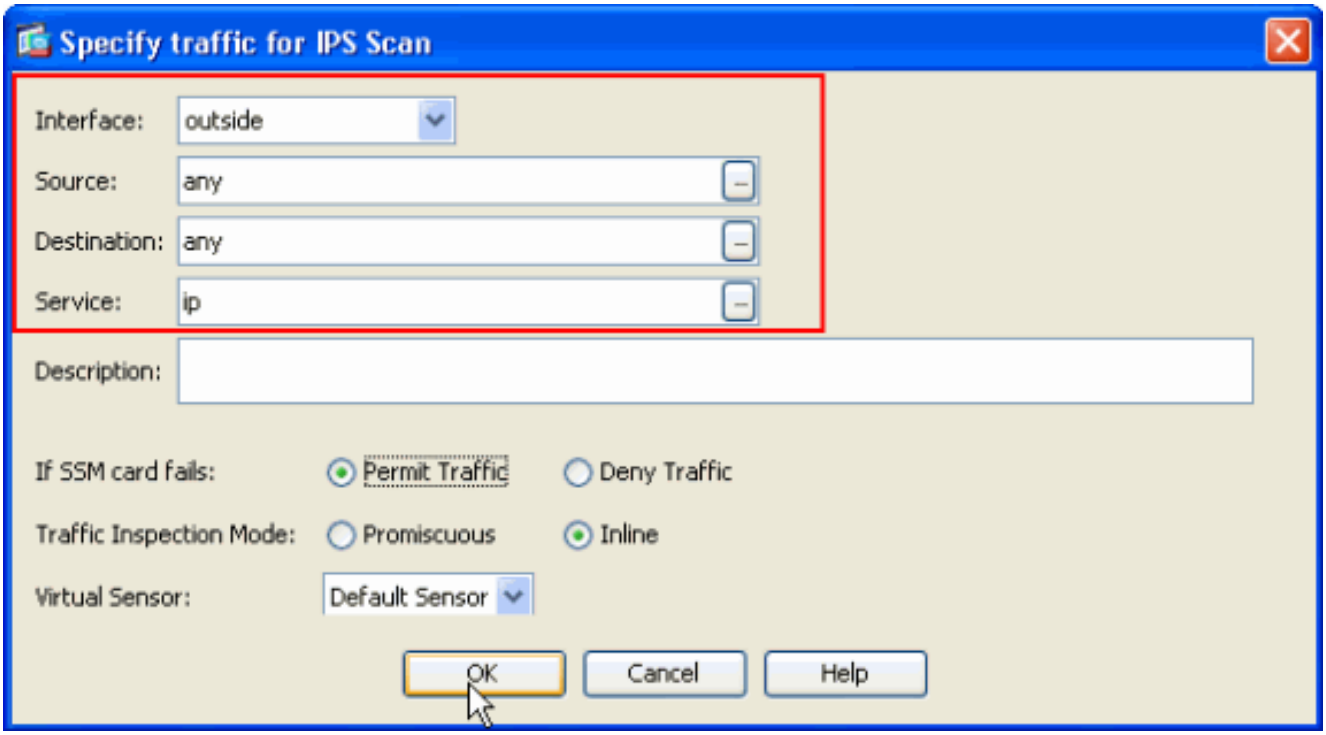
6. Clique **em seguida** depois que você fornece os detalhes nos espaços respectivos fornecidos.



7. O clique **adiciona** a fim configurar os detalhes da atribuição do tráfego.

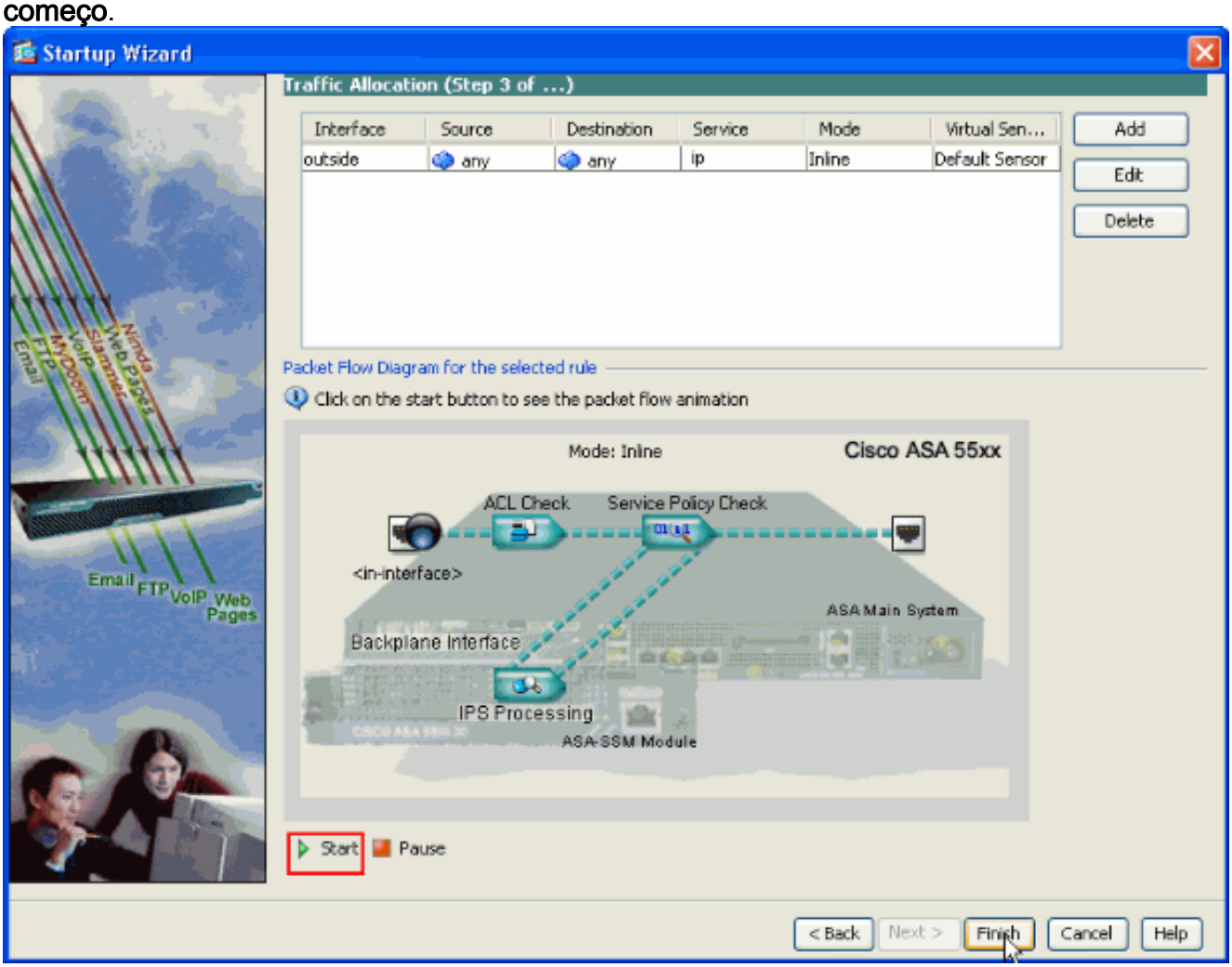


8. Forneça a fonte e o endereço de rede de destino e igualmente o tipo de serviço, por exemplo, IP são usados aqui. Neste exemplo, **algum** está usado para a fonte e o destino enquanto você inspeciona todo o tráfego com AIP-SSM. Em seguida, clique em "OK".



9. As regras configuradas da atribuição do tráfego são mostradas neste indicador e você pode adicionar tantas como regras como necessárias se você termina o mesmo procedimento como explicado em etapas 7 e 8. Clique então o **revestimento** e isto termina o procedimento

de configuração ASDM.**Nota:** Você pode ver a animação do fluxo de pacote de informação se você clica sobre o
começo.



Inspecione o tráfego específico com o AIP-SSM

Caso o administrador de rede quiser ter o monitor AIP-SSM como um subconjunto de todo o tráfego, o ASA tem duas variáveis independentes que podem ser alteradas. Primeiro, a lista de acesso pode ser preenchida para incluir ou excluir o tráfego necessário. Além da modificação de listas de acesso, uma opção **service-policy** pode ser aplicada a uma interface ou globalmente para alterar o tráfego inspecionado pelo AIP-SSM.

No que diz respeito ao diagrama de rede deste documento, o administrador de rede deseja que o AIP-SSM inspecione *todo* o tráfego entre a rede externa e a rede 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.
```

Em seguida, o administrador de rede deseja que o AIP-SSM monitore o tráfego *iniciado* pela rede interna para a rede externa. A rede interna à rede do DMZ não é monitorada.

Nota: Esta seção particular exige uma compreensão intermediária do statefulness, do TCP, do UDP, do ICMP, da conexão, e das comunicações sem conexão.

```
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
```

A lista de acesso nega o tráfego iniciado na rede interna destinada para a rede do DMZ. A segunda linha da lista de acesso permite ou envia o tráfego iniciado na rede interna destinada para a rede externa ao AIP-SSM. Neste momento o statefulness do ASA entra o jogo. Por exemplo, um usuário interno inicia uma conexão de TCP (telnet) a um dispositivo na rede externa (roteador). O usuário conecta com sucesso ao roteador e entra. O usuário emite então um comando router que não seja autorizado. O roteador responde com Command authorizaton failed. O pacote de dados que contém a string Command authorization failed tem como origem o roteador externo e o usuário interno como o destino. A fonte (fora) e o destino (para dentro) não combinam as listas de acesso definidas previamente neste documento. O ASA faz o acompanhamento das conexões stateful. Por isso, o pacote de dados que retorna (exterior para interior) é enviado para inspeção no AIP-SSM. A assinatura personalizada 60000 0, a qual foi configurada no AIP-SSM, aciona o alarme.

Nota: À revelia, o ASA não mantém o estado para o tráfego ICMP. Na configuração de exemplo precedente, o usuário interno sibila (requisição de eco ICMP) o roteador exterior. O roteador responde com resposta de eco ICMP. O AIP-SSM inspeciona o pacote de requisição de eco mas não o pacote de resposta de eco. Se a inspeção de ICMP é permitida no ASA, a requisição de eco e os pacotes de resposta de eco estão inspecionados pelo AIP-SSM.

Exclua o tráfego de rede específico da exploração AIP-SSM

O exemplo generalizado dado fornece uma vista em isentar o tráfego específico a ser feito a varredura por AIP-SSM. A fim executar isto, você precisa de criar uma lista de acesso que contenha o fluxo de tráfego que deve ser excluída da exploração AIP-SSM na instrução de negação. Neste exemplo, o IPS é o nome da lista de acesso que define o fluxo de tráfego a ser feito a varredura por AIP-SSM. O tráfego entre o **<source>** e o **<destination>** é excluído da exploração; todo tráfego restante é inspecionado.

```
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
```

Verificar

Verifique que os eventos alertas estão gravados no AIP-SSM.

Log no AIP-SSM com a conta de usuário do administrador. O comando **show events alert** gera esta saída.

Nota: A saída varia baseado em ajustes, em tipo de tráfego enviado ao AIP-SSM, e em carga de rede da assinatura.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

```
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
```

Nas configurações de amostra, diversas assinaturas IPS são ajustadas para alarmar-se no tráfego de teste. A assinatura 2000 e 2004 é alterada. A assinatura feita sob encomenda 60000 é adicionada. Em um ambiente de laboratório ou em uma rede em que poucos dados passam pelo ASA, talvez seja necessário modificar assinaturas para acionar eventos. Se o ASA e os AIP-SSM são distribuídos em um ambiente que passe uma grande quantidade de tráfego, os ajustes da assinatura do padrão são prováveis gerar um evento.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Emita estes **comandos show do** ASA.

- **módulo show** — Informação das mostras sobre o SS no ASA assim como na informação 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.`
- **lista de acesso da mostra** — Mostra os contadores para uma lista de acesso.`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 que você instale e use o AIP-SSM, o tráfego de rede passa com o ASA como esperado? Caso contrário, poderá ser necessário fazer o troubleshooting da rede e das regras das políticas de acesso ao ASA.

Problemas com Failover

- Se você tem dois ASA em uma configuração de failover e cada um tem um AIP-SSM, você **deve** manualmente replicate a configuração dos AIP-SS. Somente a configuração do ASA replicated pelo mecanismo do Failover. O AIP-SSM não é incluído no Failover. Refira PIX/ASA exemplo ativo/à espera 7.x da configuração de failover para obter mais informações sobre dos problemas do Failover.
- O AIP-SSM não participa na comutação classificada se a comutação classificada é configurada no par de failover ASA.

Mensagens de erro

O módulo IPS (AIP-SSM) produz mensagens de erro conforme mostrado, e não eventos de acionamento.

```
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.
```

A causa dessa mensagem de erro é que o sensor virtual do IPS não foi atribuído à interface traseira do ASA. O ASA está configurado da forma correta para enviar tráfego para o módulo SSM, mas você deve atribuir o sensor virtual à interface traseira criada pelo ASA para que o SSM possa examinar o tráfego.

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

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

`name=ErrLimitExceeded`
Essas mensagens são indicativas do IP LOGGING estar habilitado, o qual, por sua vez, se apropriou de todos os recursos do sistema. A Cisco recomenda desabilitar o IP LOGGING já que ele só deve ser usado para fins de troubleshooting/investigação.

Nota: `O desvio Inline errWarning dos dados começou o` Mensagem de Erro é comportamento esperado enquanto o sensor reinicia momentaneamente o motor da análise após a atualização de assinatura, que é uma necessária parte do processo da atualização de assinatura.

suporte de syslog

O AIP-SSM não apoia o Syslog como um formato alerta.

O método padrão para receber a informação alerta do AIP-SSM é com a troca do evento do dispositivo de segurança (SDEE). Uma outra opção é configurar assinaturas individuais a fim gerar uma armadilha de SNMP como uma ação para tomar quando são provocadas.

Repartição AIP-SSM

O módulo AIP-SSM não responde corretamente.

Se o módulo AIP-SSM não responde corretamente, a seguir recarregue o módulo AIP-SSM sem recarregar o ASA. Use o comando reload do módulo 1 do módulo HW a fim recarregar o módulo AIP-SSM e não recarregue o ASA.

Alerta do email AIP-SSM

Pode AIP-SSM enviar alertas do email aos usuários?

Não, não é apoiado.

Informações Relacionadas

- Referência de comandos do dispositivo do Cisco Security, versão 7.2
- Mensagens de Log de sistema do dispositivo do Cisco Security, versão 7.2
- Referência de comandos para o Sistema de prevenção de intrusões da Cisco 5.1
- Suporte Técnico e Documentação - Cisco Systems