ASA ：从 ASA 向 AIP SSM 发送网络流量的配置示例

目录

简介

本文档提供了一个有关如何将经由 Cisco ASA 5500 系列自适应安全设备 (ASA) 的网络数据流发送到高级检查和防御安全服务模块 (AIP-SSM) (IPS) 的配置示例。配置示例与命令行界面 (CLI) 一起提供。

请参阅 ASA：从 ASA 向 CSC-SSM 发送网络数据流配置示例，以便将网络数据流从 Cisco ASA 5500 系列自适应安全设备 (ASA) 发送到内容安全和控制安全服务模块 (CSC-SSM)。

参考分配虚拟传感器到安全上下文(仅AIP SSM)关于如何发送穿过Cisco ASA 5500系列可适应安全工具的网络流量的更多信息(ASA)在多个上下文模式到先进的检查和预防安全服务模块(AIP-SSM) (IPS)模块。

注意： 经由 ASA 的网络数据流包括访问 Internet 的内部用户或访问此类资源的 Internet 用户：隔离区 (DMZ) 或内部网络中由 ASA 保护的资源。不会将发送到 ASA 中或从 ASA 中发送的网络数据流发送到 IPS 模块中进行检查。不发送到 IPS 模块中的数据流包括用于 ping (ICMP) ASA 接口或使用 Telnet 访问 ASA 的数据流。

注意： ASA 用来对数据流进行分类以便实施检查的模块化策略框架不支持 IPv6。因此，如果您通过 ASA 将 IPv6 数据流转移至 AIP SSM，则不受支持。

注意： 关于AIP-SSM的更多信息初始配置，参考AIP-SSM传感器的初始配置。

先决条件

要求

本文档假定读者对如何配置 Cisco ASA 软件版本 8.x 和 IPS 软件版本 6.x 有基本的了解。

- ASA 8.x 的必要配置组件包括接口、访问列表、网络地址转换 (NAT) 和路由。
- AIP-SSM（IPS 软件 6.x）的必要配置组件包括网络设置、允许的主机、接口配置、签名定义和事件操作规则。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 8.0.2 的 ASA 5510
- IPS 软件版本为 6.1.2 的 AIP-SSM-10

注意： 此配置示例适用于 OS 7.x 及更高版本的任何 Cisco ASA 5500 系列防火墙和 IPS 5.x 及更高版本的 AIP-SSM 模块。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

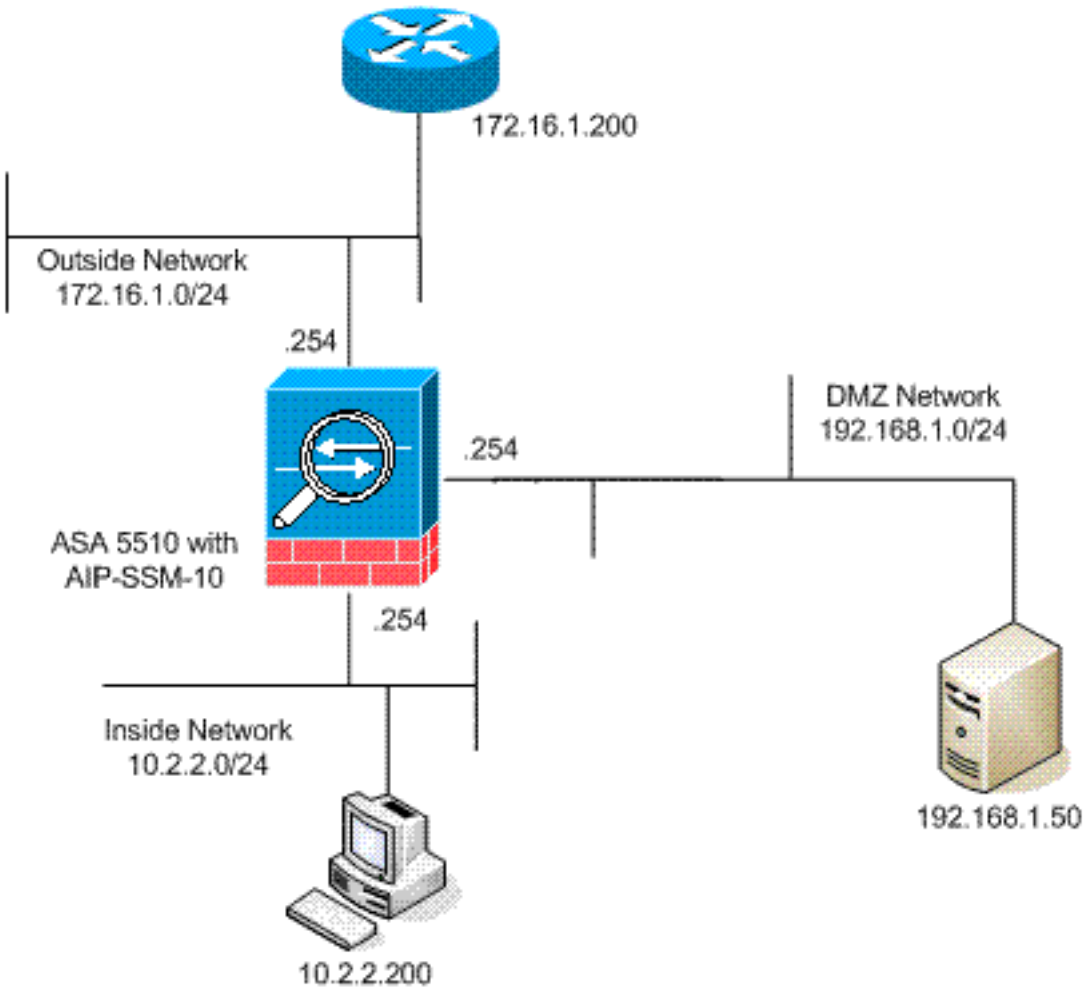
本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

网络图

本文档使用以下网络设置：



初始配置

本文档使用以下配置。ASA 和 AIP-SSM 最初均采用默认配置，但是针对测试目的对这些配置进行了特定更改。新增内容在配置中进行了标注。

- 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#
```

注意： 如果您用 https 无法访问 AIP-SSM 模块，请完成以下步骤：

- 为该模块配置管理 IP 地址。您可以配置 network access list，在其中指定允许连接到管理 IP 的 IP/IP 网络。
- 确保您已连接 AIP 模块的外部以太网接口。对 AIP 模块的管理访问只能通过此接口来实现。

有关详细信息，请参阅初始化 AIP-SSM 。

检查所有流量同线型的AIP-SSM或混杂模式

网络管理员和公司高级管理人员经常要求所有数据流都需要监控。此配置符合对所有数据流都进行监控的要求。除监控所有数据流之外，有关 ASA 和 AIP-SSM 交互的方式，需要做出以下两个决定。

- AIP-SSM 模块是以混合模式还是以内联模式运行或部署？混合模式表示，在 ASA 将原始数据转发到目标的同时，会将数据的副本发送到 AIP-SSM。可将混合模式的 AIP-SSM 视为入侵检测系统 (IDS)。在此模式下，触发数据包（引起警报的数据包）仍然能到达目的地。可能会发生避开情形，并因此阻止其他数据包到达目的地，不过不会使触发数据包停止。内联模式表示 ASA 将数据转发到 AIP-SSM 以便进行检查。如果数据通过 AIP-SSM 检查，则数据会返回到 ASA，以便对数据继续进行处理并发送到目的地。可将内联模式的 AIP-SSM 视为入侵防御系统 (IPS)。与混合模式不同的是，内联模式 (IPS) 实际上能够阻止触发数据包到达目的地。
- 在 ASA 无法与 AIP-SSM 通信的情况下，ASA 应如何处理待检查的数据流？ASA 无法与 AIP-SSM 通信的情形包括 AIP-SSM 重新加载，或者模块发生故障且需要替换。在这种情况下，ASA 可能会发生“故障后开放”(fail-open) 或“故障后关闭”(fail-closed) 情形。如果无法到达 AIP-SSM，则故障后开放会允许 ASA 继续将待检查的数据流传递至最终目的地。当 ASA 无法与 AIP-SSM 通信时，故障后关闭会阻止待检查的数据流。**注意：** 待检查的数据流使用访问列表进行定义。在此示例输出中，访问列表允许从任何源到任何目的地的所有 IP 数据流。因此，待检查的数据流可以是经由 ASA 的任何数据流。

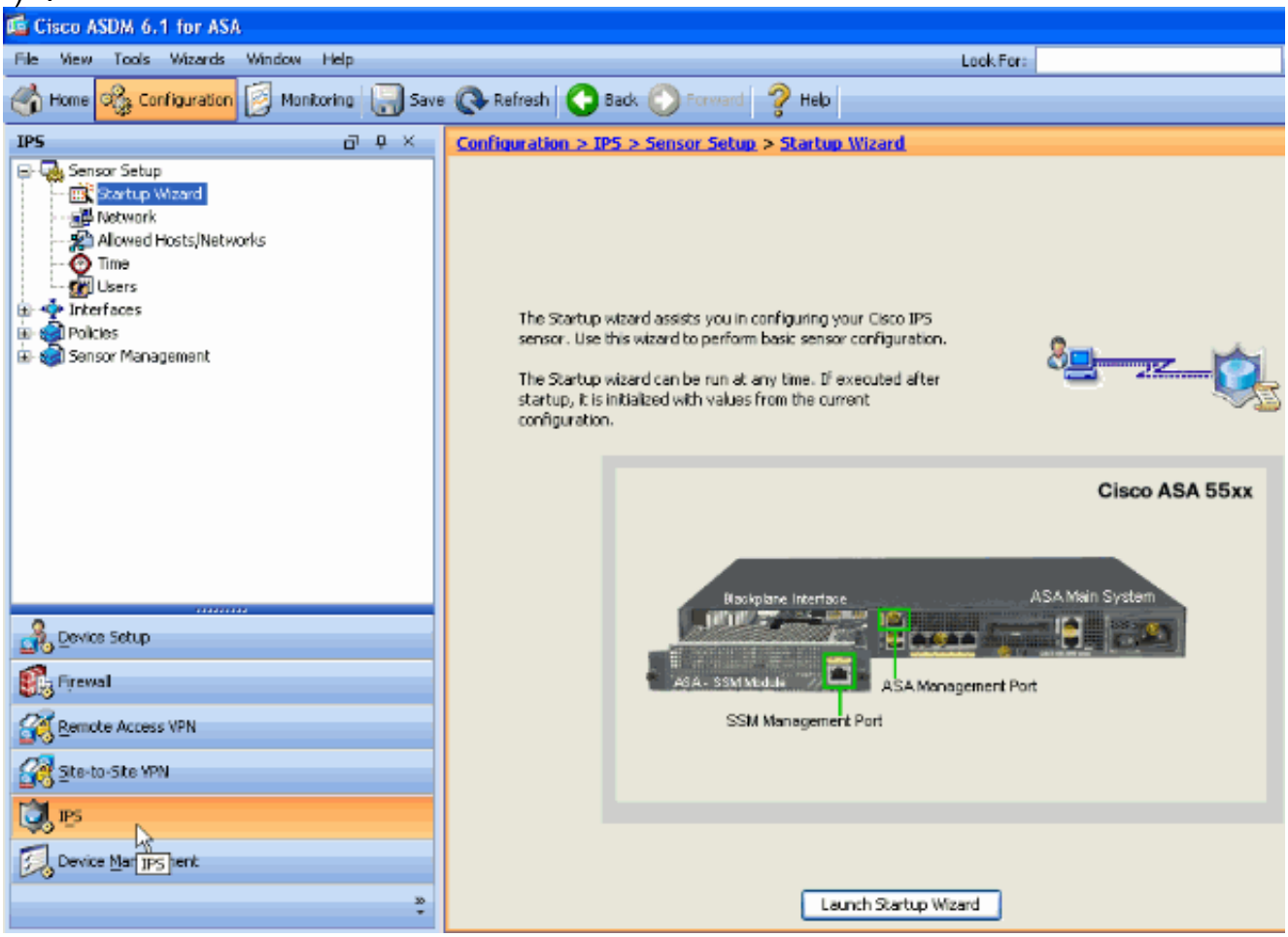
```
ciscoasa(config)#access-list traffic_for_ips permit ip any any ciscoasa(config)#class-map
```

```
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.
```

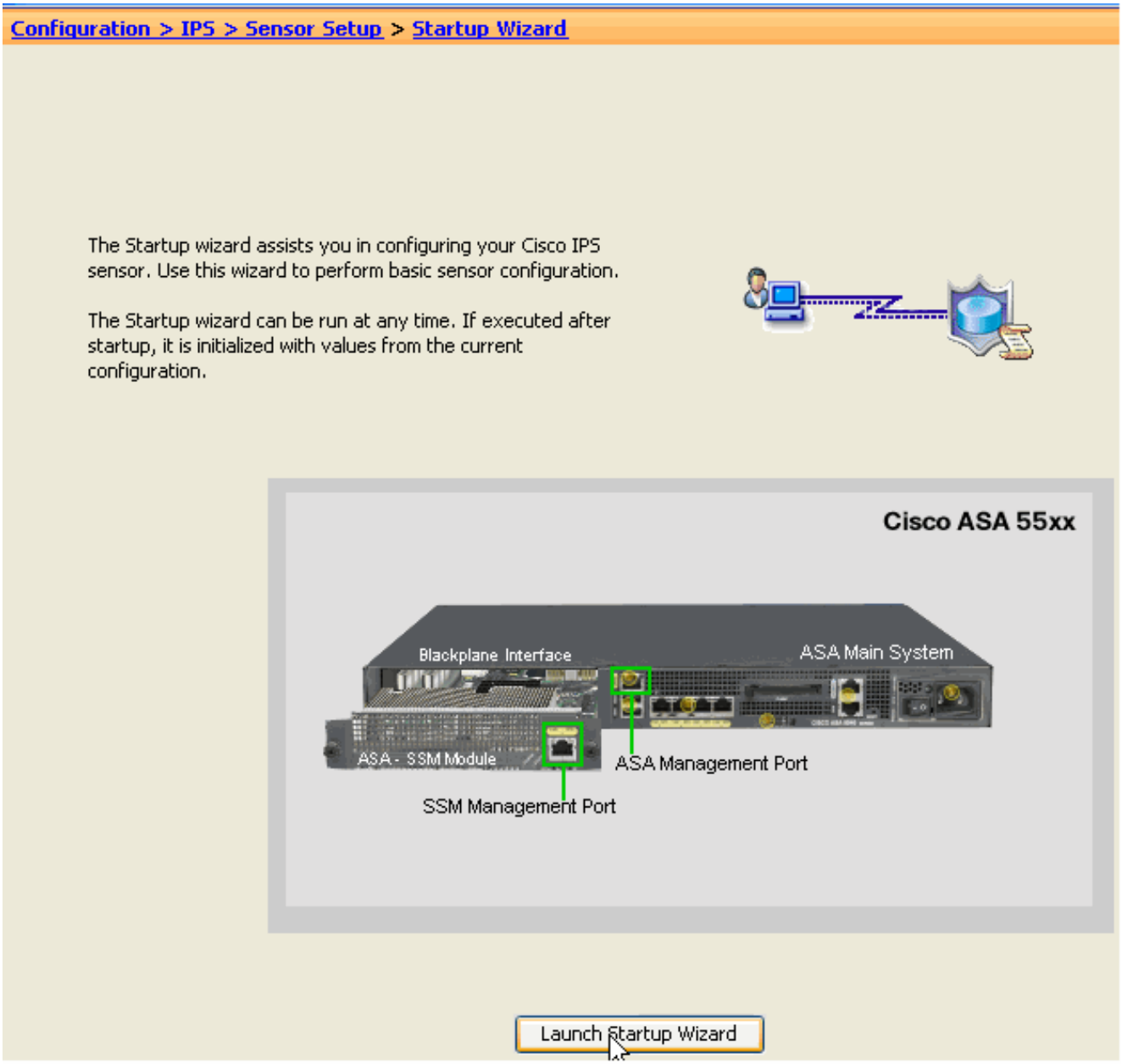
通过使用 ASDM 的 AIP-SSM 检查所有数据流

完成以下这些步骤可通过使用 ASDM 的 AIP-SSM 检查所有数据流：

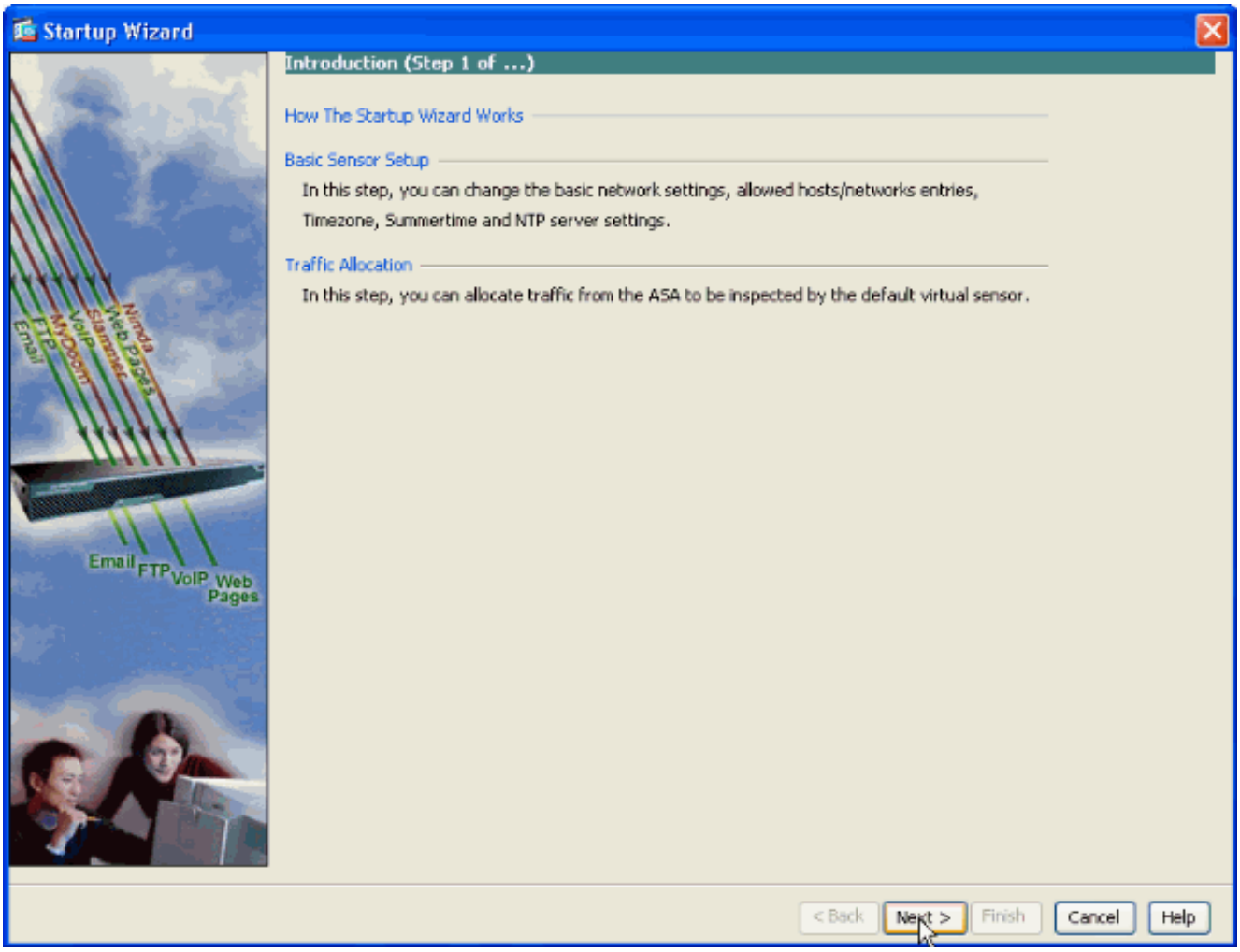
1. 在 ASDM 主页上依次选择 **Configuration > IPS > Sensor Setup > Startup Wizard** 以启动配置（如下所示）：



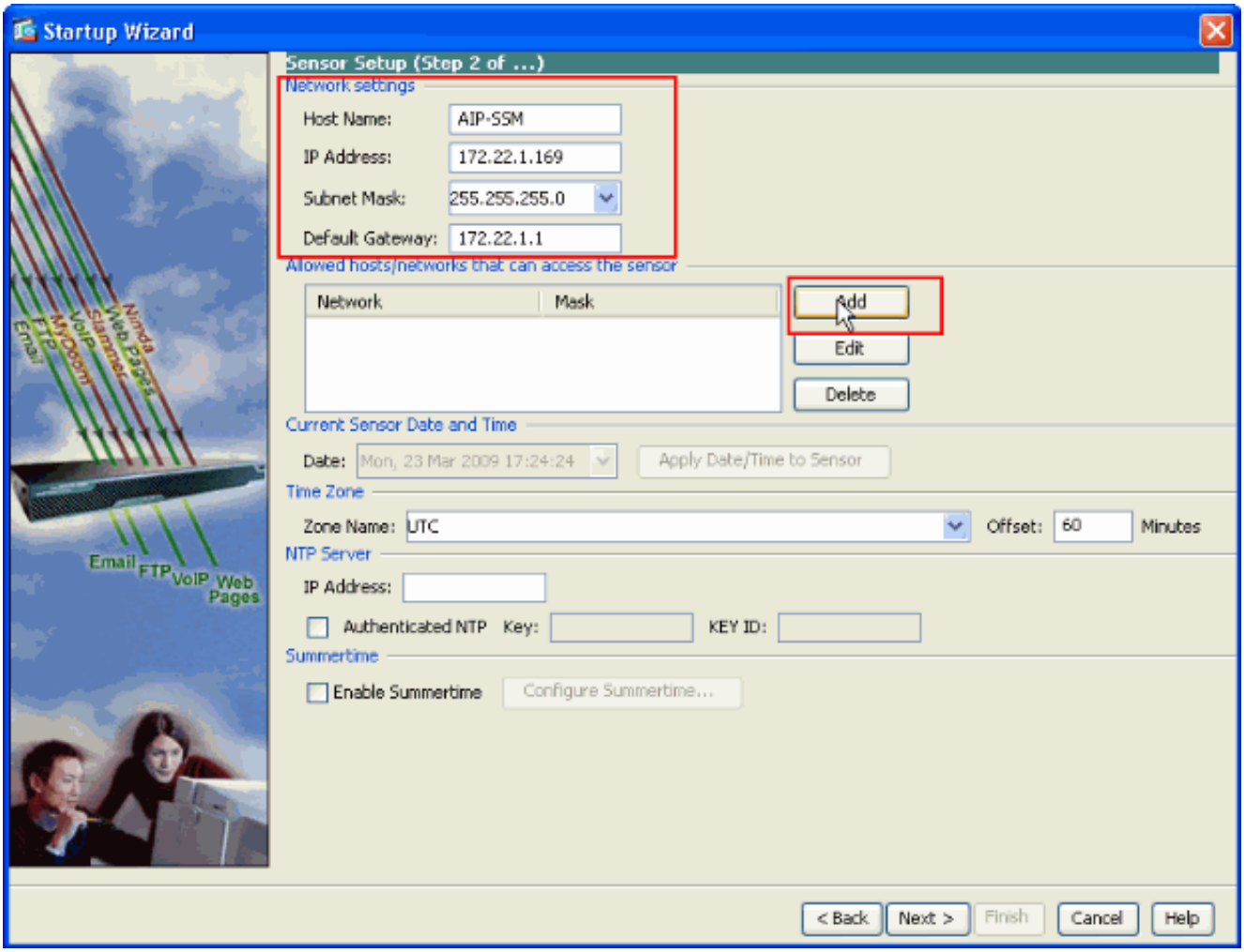
2. 单击 **Launch Startup Wizard**。



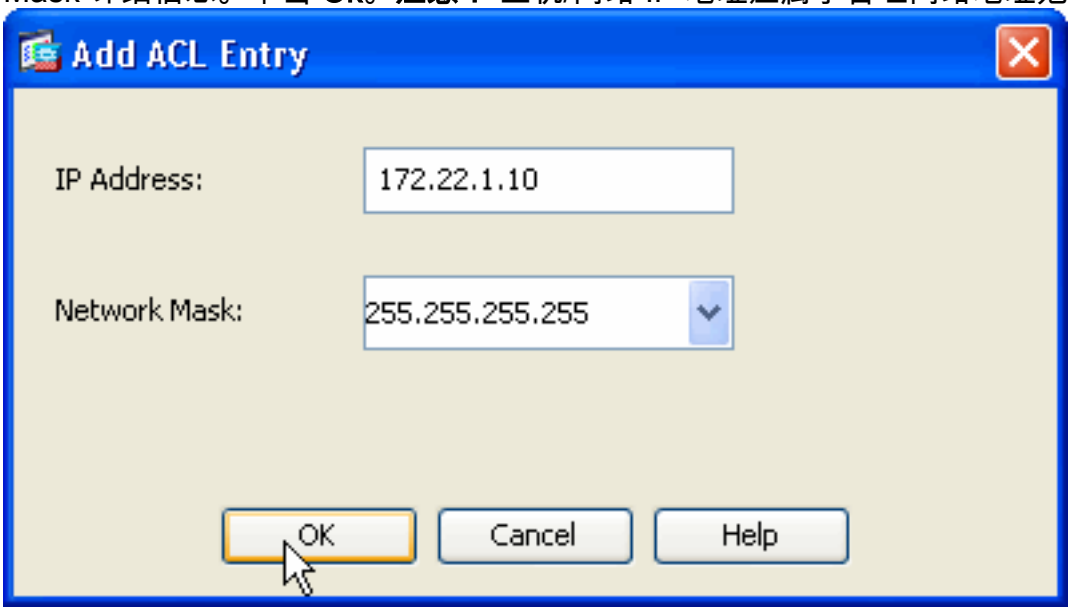
3. 在您将启动向导予以启动后所出现的新窗口中单击 **Next**。



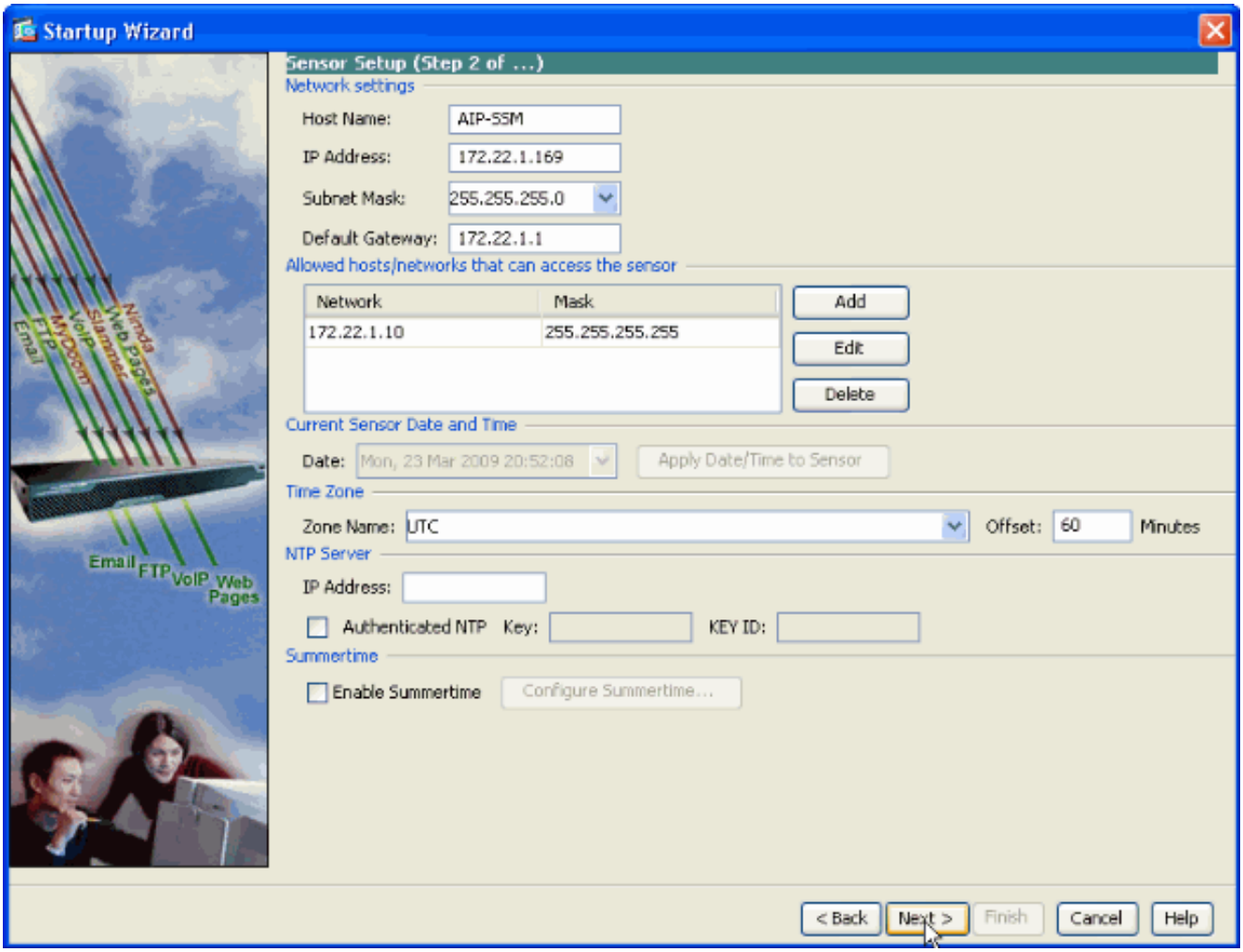
4. 在该新窗口中，在 Network settings 部分下所提供的相应空白处，提供 AIP-SSM 模块的 Host Name、IP Address、Subnet Mask 和 Default Gateway 地址。然后单击 **Add**，以便添加访问列表来允许经由 AIP-SSM 的所有数据流。



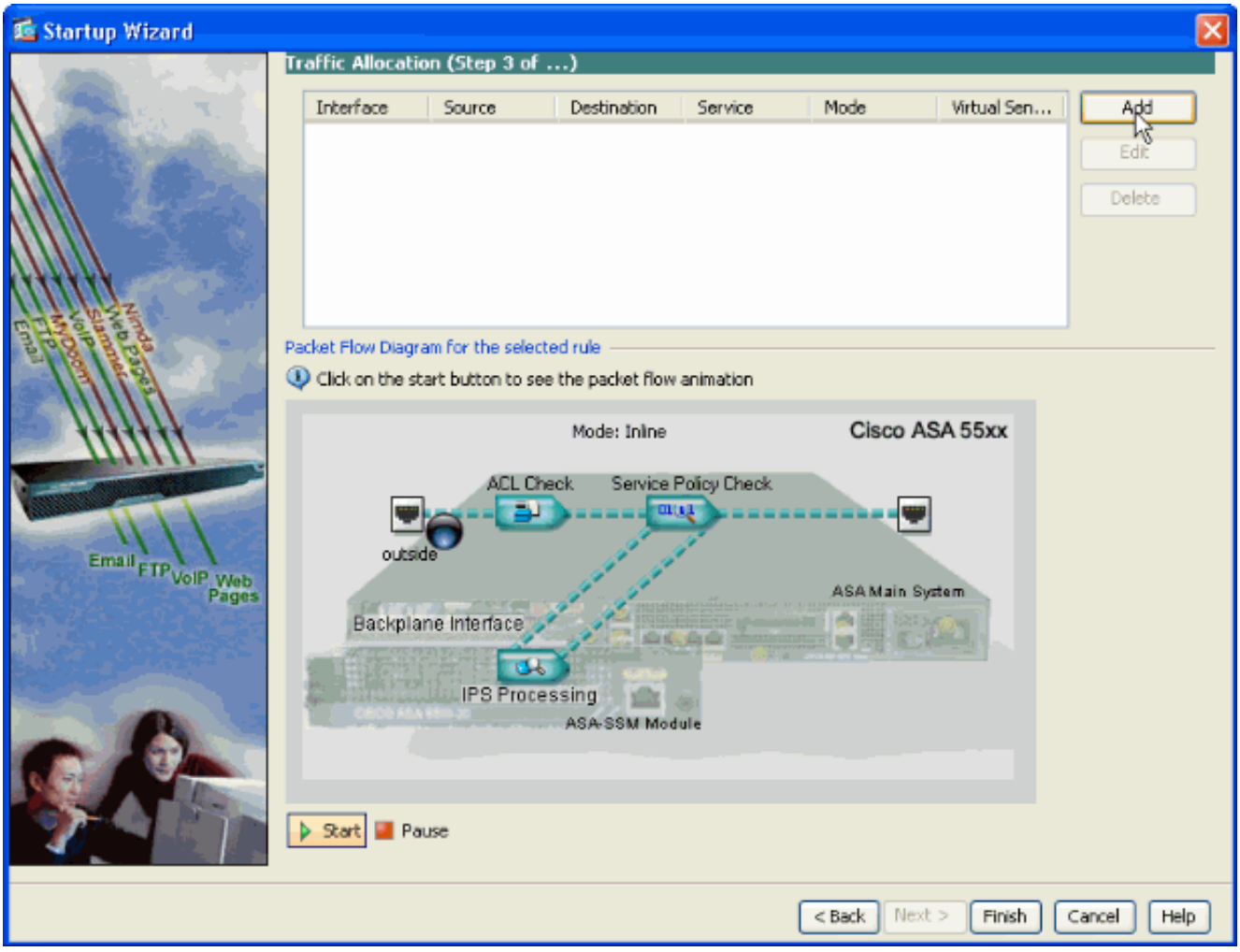
5. 在 **Add ACL Entry** 窗口中，提供允许其访问传感器的主机/网络的 IP Address 和 Network Mask 详细信息。单击 **Ok**。**注意：** 主机/网络 IP 地址应属于管理网络地址范围。



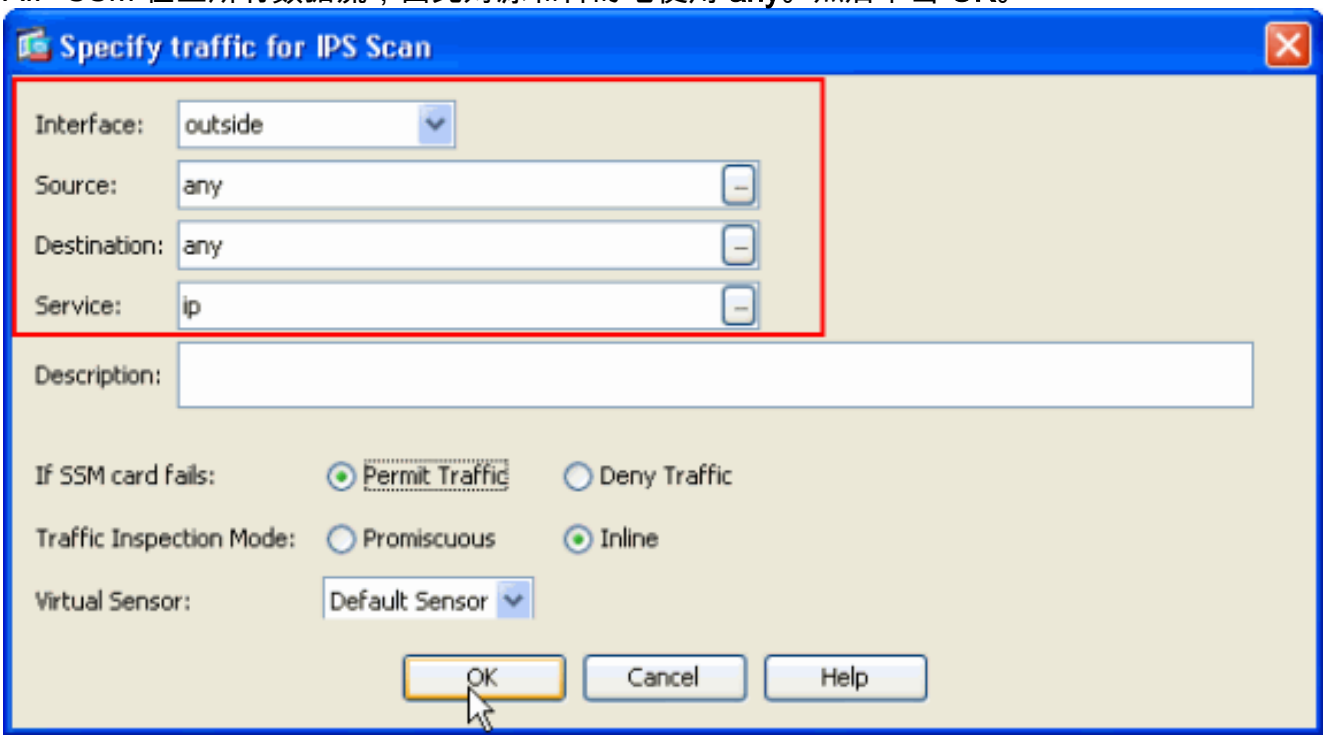
6. 在所提供的相应空白处提供详细信息之后，请单击 **Next**。



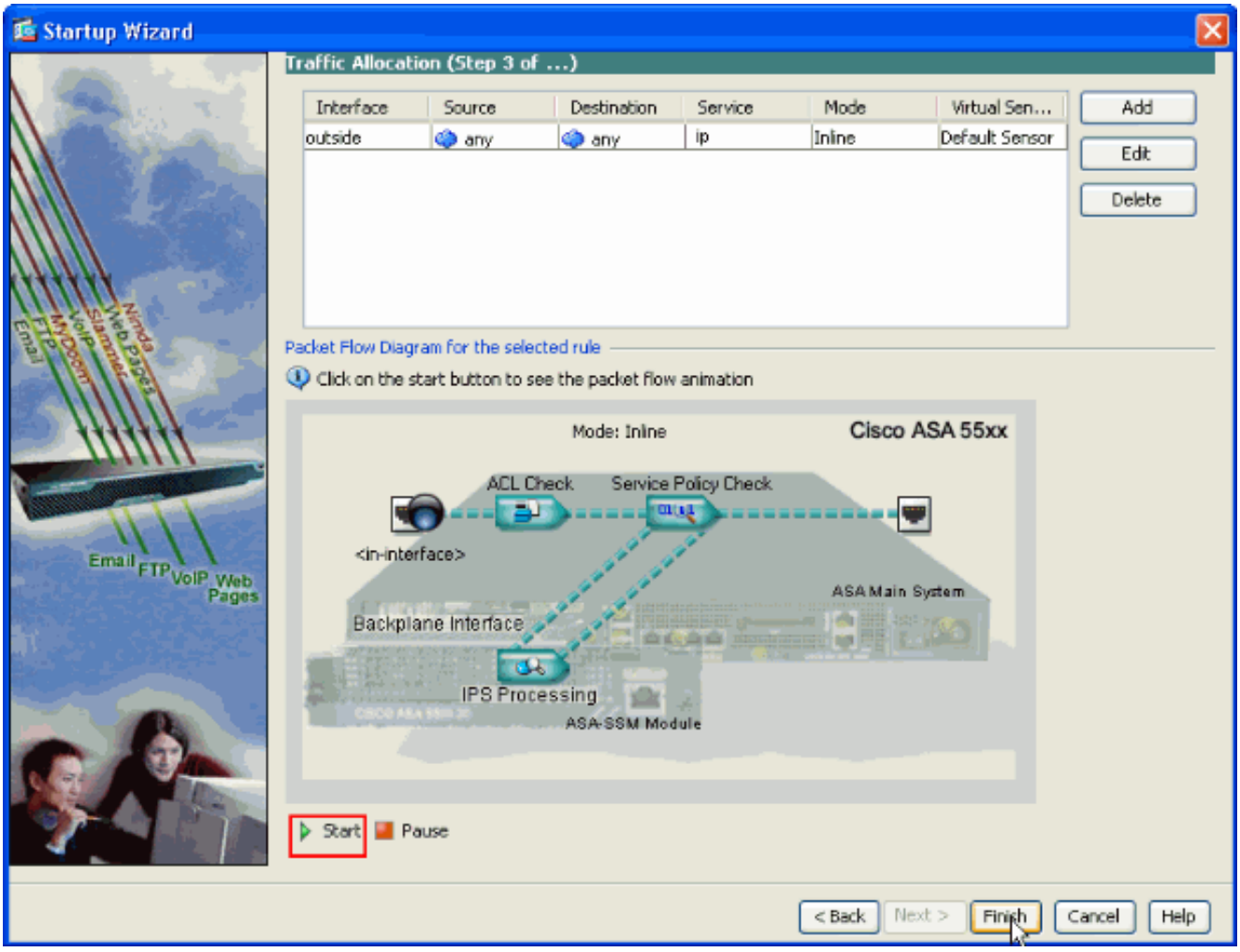
7. 单击 Add 以配置数据流分配详细信息。



8. 提供源和目的地网络地址，以及服务类型（如此处所用为 IP）。在本示例中，由于要使用 AIP-SSM 检查所有数据流，因此对源和目的地使用 **any**。然后单击 **OK**。



9. 所配置的 Traffic Allocation 规则会显示在此窗口中，您可以视需要重复执行第 7 步和第 8 步中所说明的过程，以此添加多个规则。然后单击 **Finish**，这样将完成 ASDM 配置过程。**注意**：如果单击 **Start**，便可以查看数据包流动画。



使用 AIP-SSM 检查特定数据流

如果网络管理员希望将 AIP-SSM 监控程序用作所有数据流的子集，则 ASA 有两个独立变量可以修改。首先，可以编写访问列表，以包含或排除必要的数据流。除对访问列表进行修改之外，还可将 **service-policy** 应用到接口或予以全局性应用，以便更改由 AIP-SSM 检查的数据流。

对于本文档中的网络图，网络管理员希望 AIP-SSM 检查外部网络和 DMZ 网络之间的*所有*数据流。

```
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.
```

其次，网络管理员希望 AIP-SSM 监控从内部网络*发起*、目的地为外部网络的数据流。不会监控从内部网络到 DMZ 网络的数据流。

注意： 此特定部分要求读者对状态、TCP、UDP、ICMP、连接和无连接通信拥有中等程度的了解。

```
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**

访问列表会拒绝从内部网络发起、目的地为 DMZ 网络的数据流。第二个访问列表行允许自内部网络发起、目的地为外部网络的数据流或将其发送到 AIP-SSM。此时，ASA 的状态开始发挥作用。例如，一个内部用户发起了目的为外部网络上某台设备（路由器）的 TCP 连接 (Telnet)。该用户成功连接到相应路由器并登录。然后，该用户发出一个未经授权的路由器命令。路由器以 Command authorizaton failed 做出响应。在 Command authorization failed 字符串所在的数据包中，包含外部路由器的源和内部用户的目的地。源（外部）和目的地（内部）与本文档中先前定义的访问列表不匹配。ASA 会跟踪有状态连接，因此，会将返回（从外部到内部）的数据包发送到 AIP-SSM 以供检查。在 AIP-SSM 上配置的自定义签名 60000 0 发出警报。

注意： 默认情况下，ASA 不会保留 ICMP 数据流的状态。在先前的配置示例中，内部用户会 ping（ICMP 回应请求）外部路由器。路由器以 ICMP 回声应答做出响应。AIP-SSM 检查回应请求数据包，但是不会检查回声应答数据包。如果在 ASA 上启用了 ICMP 检查，则 AIP-SSM 会既检查回应请求数据包也检查回声应答数据包。

从AIP-SSM扫描排除特定网络流量

给的概括的示例在豁免提供一张视图AIP-SSM将扫描的特定的流量。为了执行此，您需要创建包含通信流将从扫描在拒绝语句的AIP-SSM被排除的access-list。在本例中， IPS是定义了AIP-SSM将扫描的通信流的名称access-list。<source>和<destination>之间的流量从扫描被排除;其他流量被检查。

```
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
```

验证

验证警报事件是否已记录在 AIP-SSM 中。

使用管理员用户帐户登录 AIP-SSM。**show events alert** 命令生成以下命令输出。

注意： 输出因签名设置、发送至 AIP-SSM 的数据流类型和网络负载的不同而异。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

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

在此配置示例中，对几个 IPS 签名进行了调整以对测试数据流发出警报。修改了签名 2000 和 2004。添加了自定义签名 60000。在实验室环境或很少有数据经由 ASA 的网络中，可能必须修改签名才能触发事件。如果将 ASA 和 AIP-SSM 部署在传递大量数据流的环境中，则默认签名设置可能会生成事件。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

从 ASA 发出这些 **show** 命令。

- **show module** - 显示关于 ASA 上的 SSM 的信息以及系统信息。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** - 显示访问列表的计数器。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.*

在您安装并使用 AIP-SSM 之前，网络数据流是否能依预期经由 ASA？如果不能，则必须对网络和 ASA 访问策略规则进行故障排除。

与故障切换相关的问题

- 如果在一个故障切换配置中有两个 ASA，且每个 ASA 都有一个 AIP-SSM，则**必须**手动复制 AIP-SSM 的配置。故障切换机制只复制 ASA 的配置。故障切换不包括 AIP-SSM。有关故障切

换问题的详细信息，请参阅 PIX/ASA 7.x 活动/备用故障切换配置示例。
- 如果在 ASA 故障切换对上配置了有状态故障切换，则 AIP-SSM 不会参与有状态故障切换。

错误消息

IPS 模块 (AIP-SSM) 会产生所示的错误消息而不会激发事件。

```
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.
```

产生此错误消息的原因是，未将 IPS 虚拟传感器分配到 ASA 的背板接口。ASA 已针对将数据流发送到 SSM 模块的目的进行了正确设置，但是您需要将虚拟传感器分配到 ASA 创建的背板接口，这样 SSM 才能扫描数据流。

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

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

这些消息表明 IP LOGGING 已启用，而这样会占用全部系统资源。Cisco 建议禁用 IP LOGGING，因为只应将其用于故障排除/调查目的。

注意： errWarning Inline data bypass has started 错误消息为预期行为，因为传感器会在签名更新之后立即重新启动分析引擎，这是签名更新过程中的一个必要部分。

Syslog 支持

AIP-SSM 不支持将 syslog 用作一种警报形式。

接收来自 AIP-SSM 的警报信息的默认方法是通过安全设备事件交换 (SDEE)。您也可以配置单个签名以便生成 SNMP 陷阱，后者用作在触发签名时所需采取的操作。

AIP-SSM 重新启动

AIP-SSM 模块未正确响应。

如果 AIP-SSM 模块未正确响应，则请重新启动 AIP-SSM 模块，无需重新启动 ASA。使用 hw-module module 1 reload 命令可重新启动 AIP-SSM 模块而不重新启动 ASA。

AIP-SSM 电子邮件警报

AIP-SSM 是否能将电子邮件警报发送给用户？

不能，目前不支持。

相关信息

- Cisco 安全设备命令参考 7.2 版
- Cisco 安全设备系统日志消息 7.2 版
- Cisco 入侵防御系统 5.1 的命令参考
- 技术支持和文档 - Cisco Systems