ASA： ASA から AIP SSM にネットワーク トラフィックを送信する設定例

目次

はじめに

このドキュメントでは、Cisco ASA 5500 シリーズ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）経由で Advanced Inspection and Prevention Security Services Module（AIP-SSM）（IPS）モジュールへネットワーク トラフィックを送信する方法の設定例について説明します。 設定例では、Command Line Interface（CLI; コマンドライン インターフェイス）を使用します。

「ASA： ASA から CSC-SSM 設定例へのネットワーク トラフィックの送信」を参照して、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）から Content Security and Control セキュリティ サービス モジュール（CSC-SSM）へネットワーク トラフィックを送信します。

マルチ コンテキスト モードの Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスから Advanced Inspection and Prevention セキュリティ サービス モジュール（AIP-SSM）（IPS）モジュールにパス スルーするネットワーク トラフィックを送信する方法の詳細については、「仮想センサーのセキュリティ コンテキスト（AIP SSM のみ）への割り当て」を参

照してください。

注: ASA を通過するネットワーク トラフィックには、緩衝地帯（DMZ）または内部ネットワークで、インターネットにアクセスする内部ユーザ、または、ASA によって保護されているリソースにアクセスするインターネット ユーザが含まれます。 ASA から送信される、もしくは ASA へ送信されるネットワーク トラフィックは、検査のために IPS モジュールには送信されません。 IPS モジュールに送信されないトラフィックの例としては、ASA インターフェイスへの PING の実行（ICMP）や ASA への Telnet の実行などが挙げられます。

注: 検査用にトラフィックを分類するために ASA で使用されるモジュラ ポリシー フレームワークは、IPv6 をサポートしていません。 そのため、ASA を経由して IPv6 トラフィックを AIP SSM へ転送する場合、IPv6 トラフィックはサポートされません。

注: AIP-SSM の初期設定の詳細については、「AIP-SSM センサーの初期設定」を参照してください。

前提条件

要件

このドキュメントは、Cisco ASA ソフトウェア バージョン 8.x および IPS ソフトウェア バージョン 6.x を設定する方法について基本的な知識がある対象者を想定しています。

- ASA 8.x に必要な設定コンポーネントには、インターフェイス、アクセス リスト、ネットワーク アドレス変換（NAT）、およびルーティングが含まれます。
- AIP SSM（IPS ソフトウェア 6.x）に必要な設定コンポーネントには、ネットワーク設定、許可されているホスト、インターフェイス設定、シグネチャ定義、およびイベント アクション ルールが含まれます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0.2 が稼働する ASA 5510
- IPS ソフトウェア バージョン 6.1.2 が稼働する AIP-SSM-10

注: この設定例は、OS 7.x 以降が稼働する Cisco ASA 5500 シリーズ ファイアウォールおよび IPS 5.x 以降が稼働する AIP-SSM モジュールと互換性があります。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

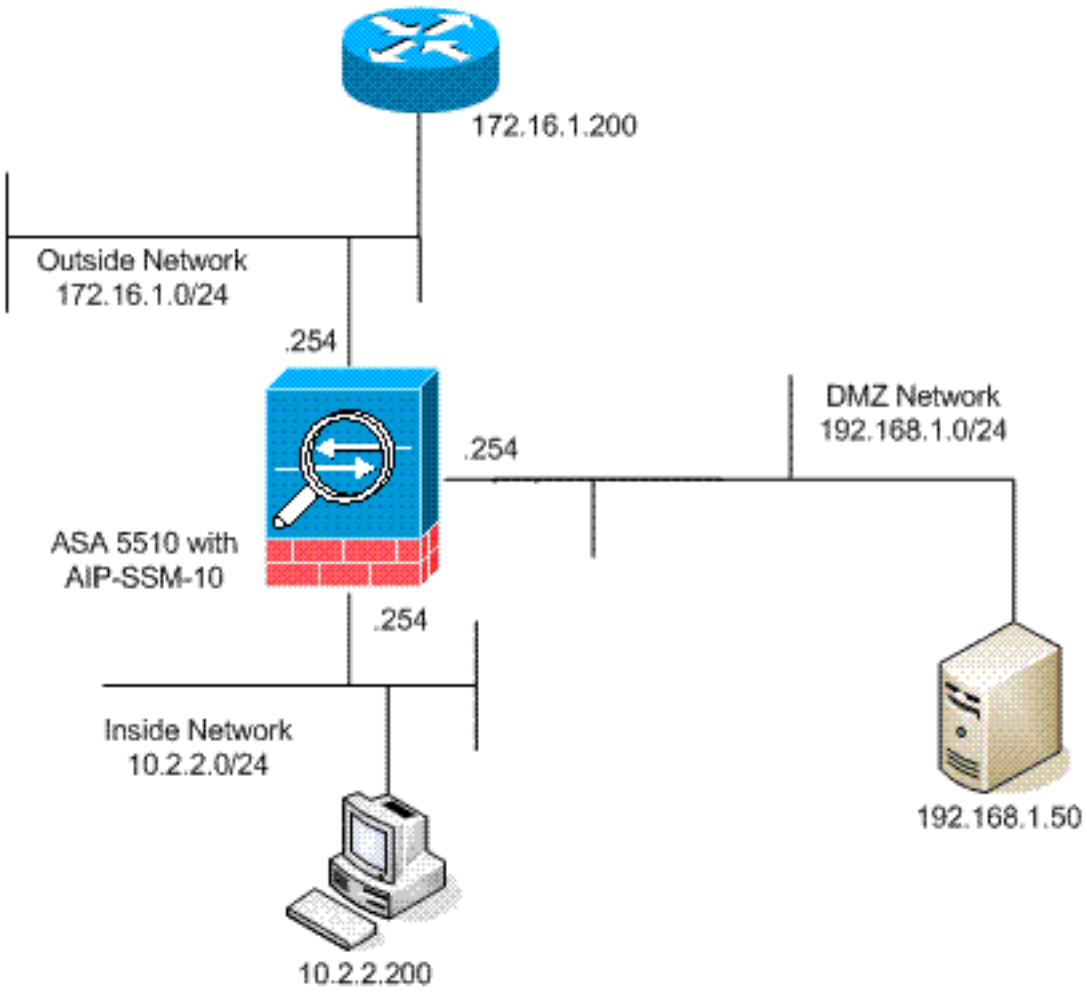
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは、ラボ環境で使用された RFC 1918 のアドレスです。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



初期設定

このドキュメントでは、次の設定を使用します。 ASA と AIP-SSM のどちらもデフォルト設定から開始されますが、テストを目的として特定の変更が行われています。 追加部分については設定内にその旨が注記されています。

- 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: https を使用して AIP-SSM モジュールにアクセスできない場合は、次のステップを実行します。

- モジュール用に管理 IP アドレスを設定します。 次に、IPs/IP ネットワークを指定するネットワーク アクセスリストを設定します。 IPs/IP ネットワークは、管理 IP への接続が許可されています。
- AIP モジュールの外部イーサネット インターフェイスに接続していることを確認します。 AIP モジュールへの管理アクセスは、このインターフェイスからのみ可能です。

詳細については、「AIP-SSM の初期化」を参照してください。

インライン モードまたは無差別モードでの AIP-SSM によるすべてのトラフィックの検査

多くの場合、ネットワーク管理者や企業の上級管理職は、すべてのイベントを監視できる必要があります。 この設定は、すべてのイベントを監視するための要件を満たしています。 すべてのイベントを監視することに加えて、ASA と AIP-SSM のインタラクションの方法について 2 つの判断が必要になります。

- AIP-SSM モジュールがプロミスキャス モードとインライン モードのどちらで配備されるのか。プロミスキャス モードでは、ASA が元のデータを宛先に転送する一方で、データのコピーが AIP-SSM に送信されます。 プロミスキャス モードの AIP-SSM は、Intrusion Detection System (IDS; 侵入検知システム) として認識される場合があります。 このモードでは、トリガー パケット (アラームの原因となるパケット) が宛先に到達することができます。 回避が発生し、追加パケットによる宛先への到達が中断される場合がありますが、トリガー パケットは中断されません。インライン モードでは、検査を目的として、ASA によって AIP-SSM にデータが転送されます。 AIP-SSM の検査に合格したデータは ASA に返され、処理が継続されて宛先に送信されます。 インライン モードの AIP-SSM は、Intrusion Prevention System (IPS; 侵入防御システム) として認識される場合があります。 プロミスキャス モードとは異なり、インライン モード (IPS) では実際にトリガー パケットによる宛先への到達が中断されます。
- ASA が AIP-SSM と通信できない場合、ASA は検査対象のトラフィックをどのように処理する必要があるのか。 ASA が AIP-SSM と通信できない場合の例には、AIP-SSM がリロードする場合やモジュールに障害が発生して交換が必要な場合などがあります。 この場合、ASA がフェール オープンまたはフェール クローズとなる可能性があります。フェール オープンを使用すると、AIP-SSM に到達不可能な場合に、ASA が検査対象のトラフィックを最終宛先へ受け渡すことが可能になります。フェール クローズでは、ASA が AIP-SSM と通信できない場合に検査対象のトラフィックをブロックします。**注:** 検査対象のトラフィックは、アクセス リストを使用して定義されます。 この出力例では、アクセス リストによって任意の発信元から任意の宛先へのすべての IP トラフィックが許可されます。 したがって、検査対象のトラフィックは ASA を通過するすべてのトラフィックである可能性があります。

```
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
```

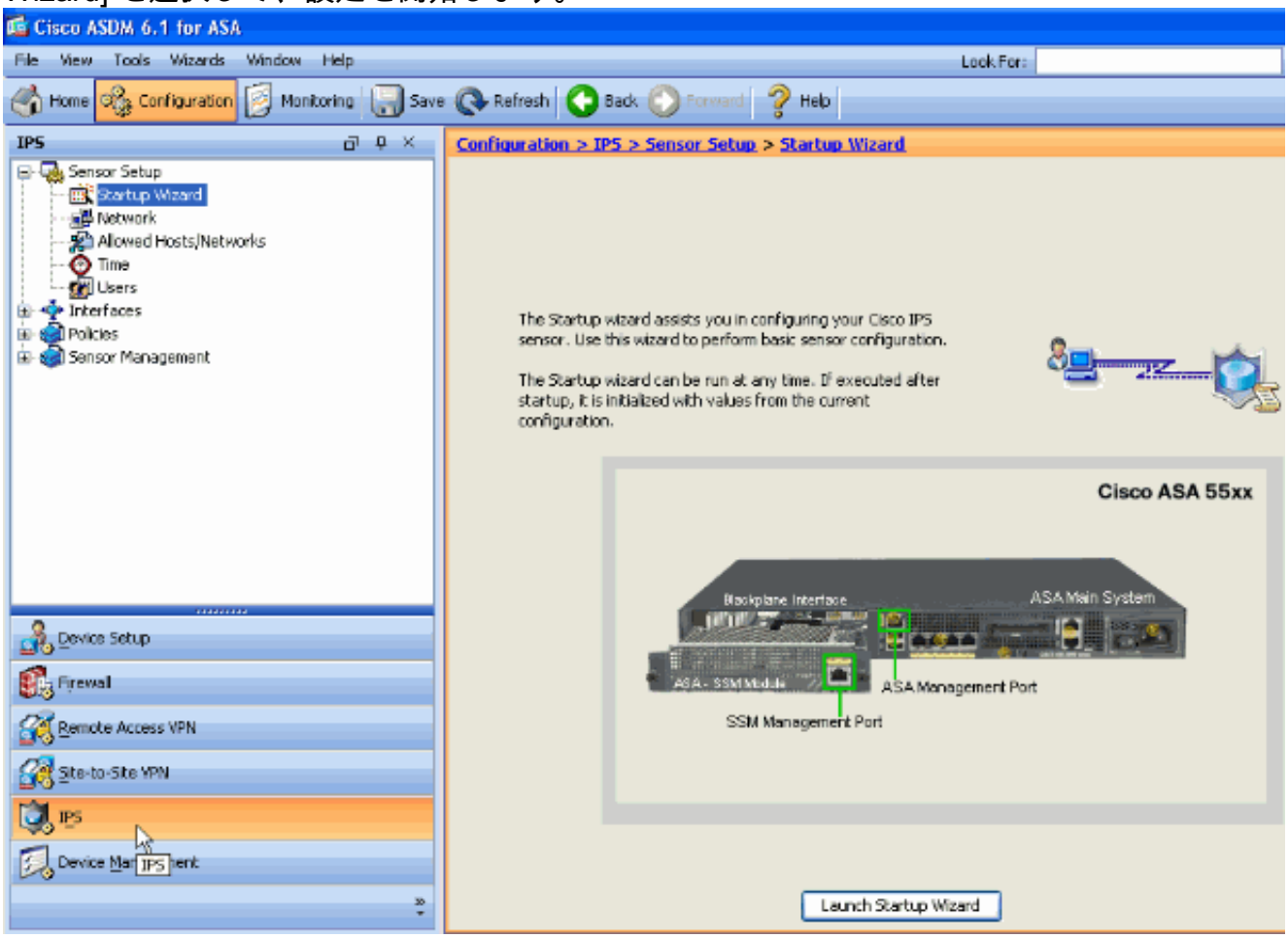
```
!--- Note that policy-map global_policy is a part of the !--- default configuration. In
addition, policy-map global_policy !--- is applied globally with the service-policy command.

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.
```

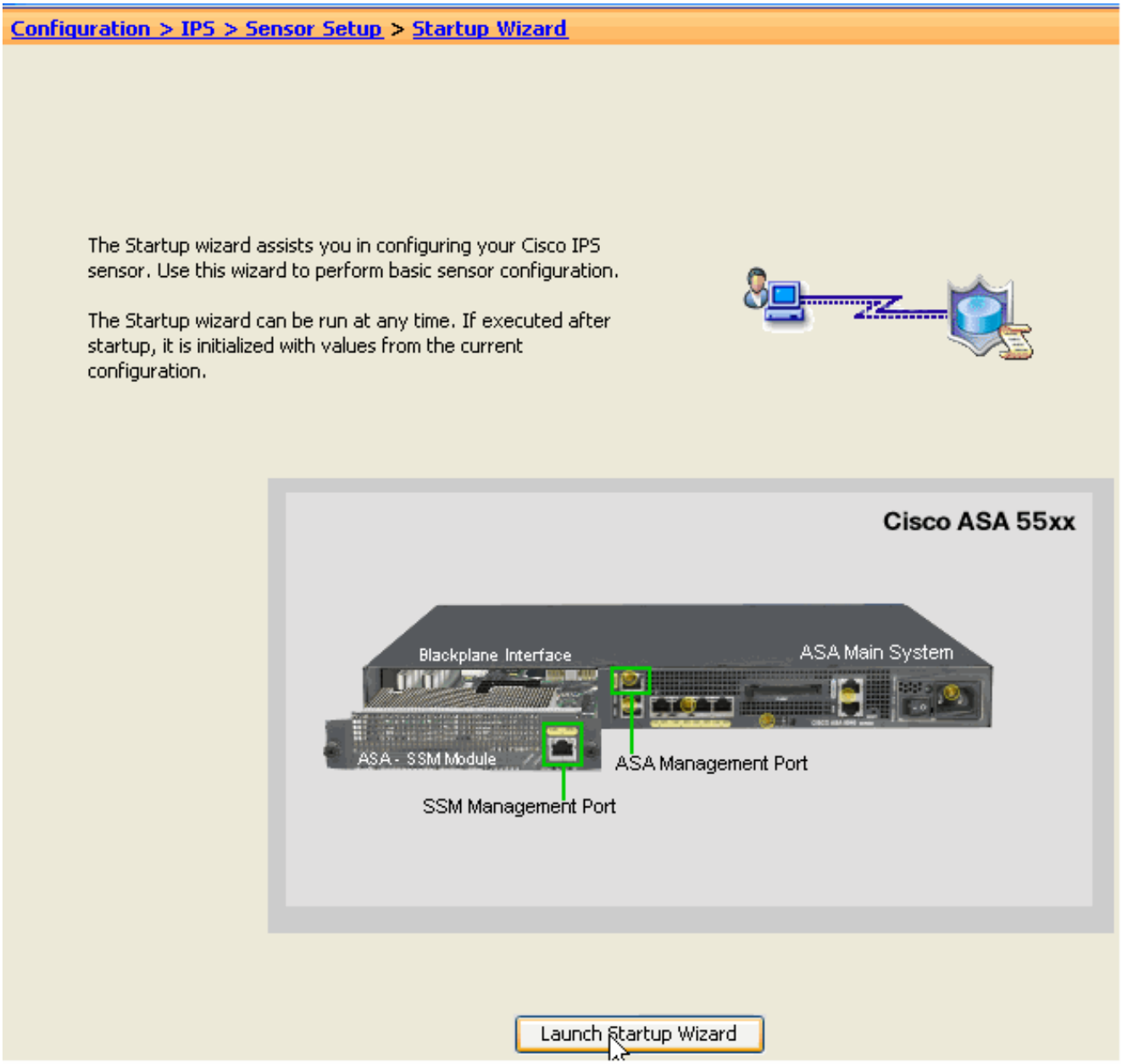
ASDM を使用した AIP-SSM によるすべてのトラフィックの検査

次のステップを実行して、ASDM を使用して AIP-SSM ですべてのトラフィックを検査します。

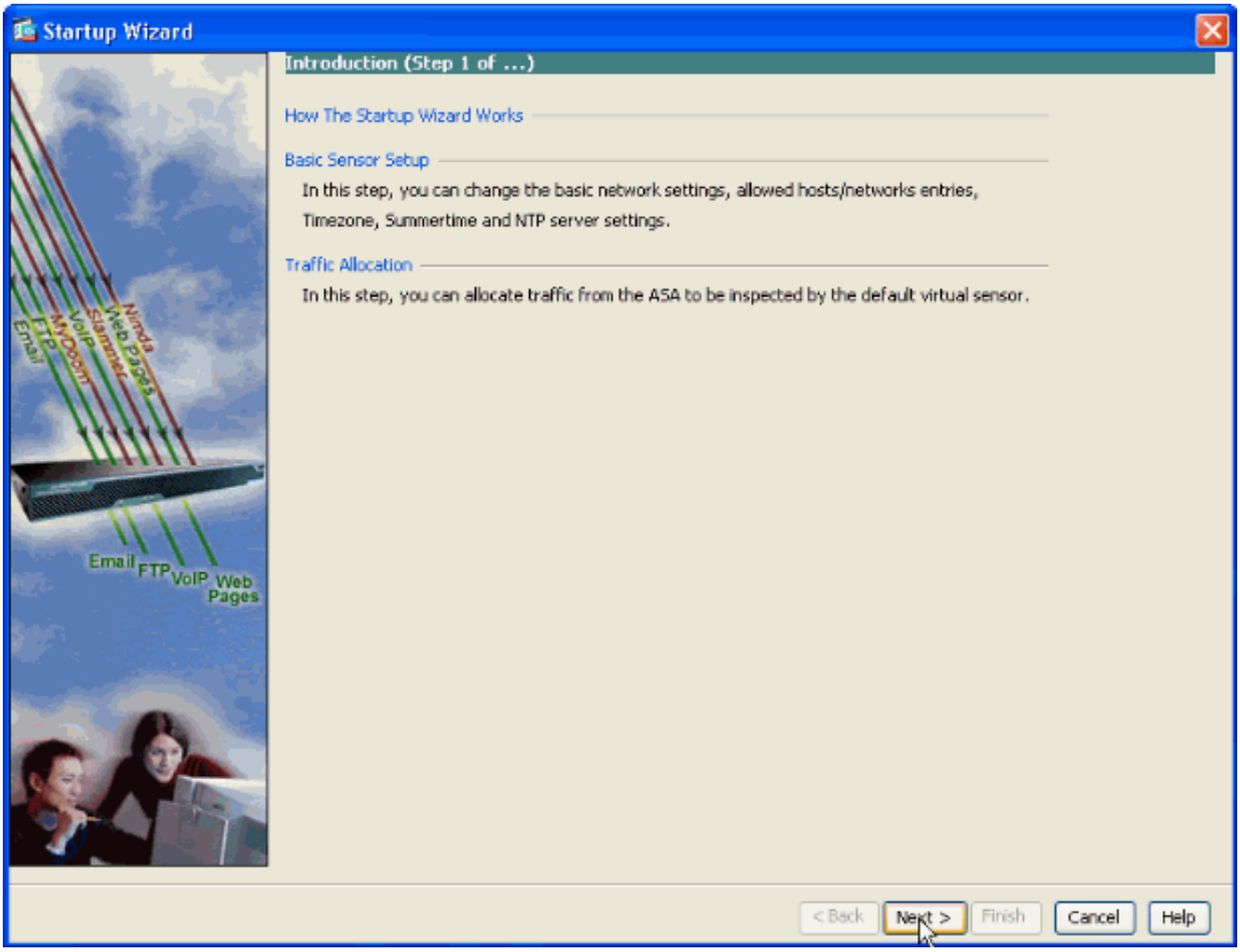
1. 次に示すように、[ASDM] ホームページで [Configuration] > [IPS] > [Sensor Setup] > [Startup Wizard] を選択して、設定を開始します。



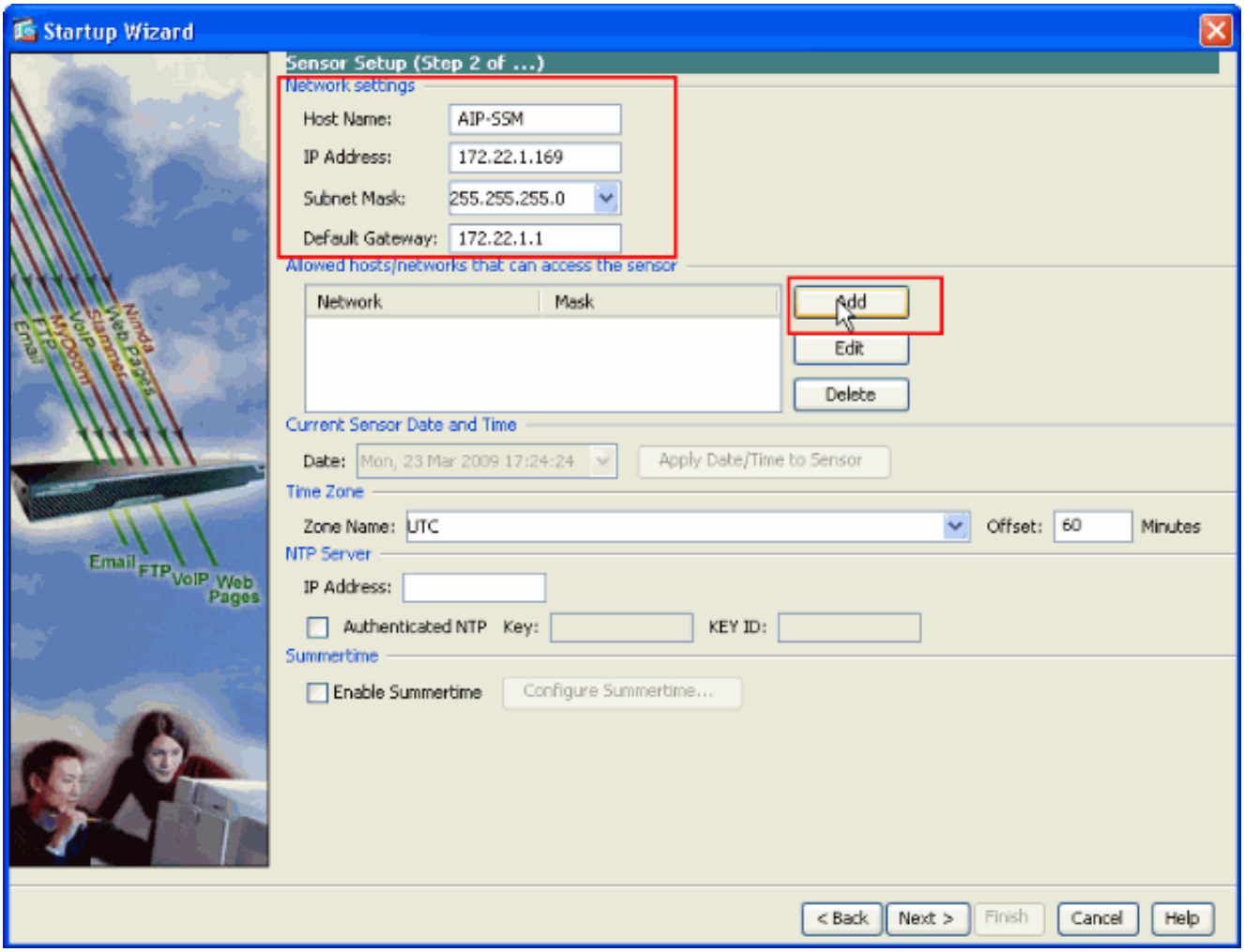
2. [Launch Startup Wizard]をクリックします。



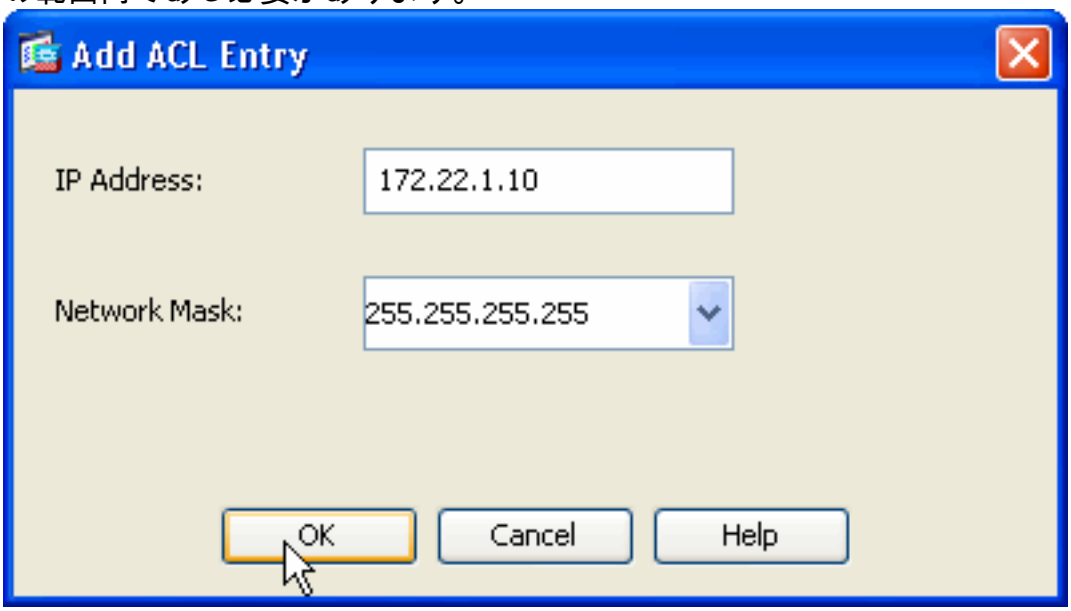
3. スタートアップ ウィザードを起動後に表示される新しいウィンドウで、[Next] をクリックします。



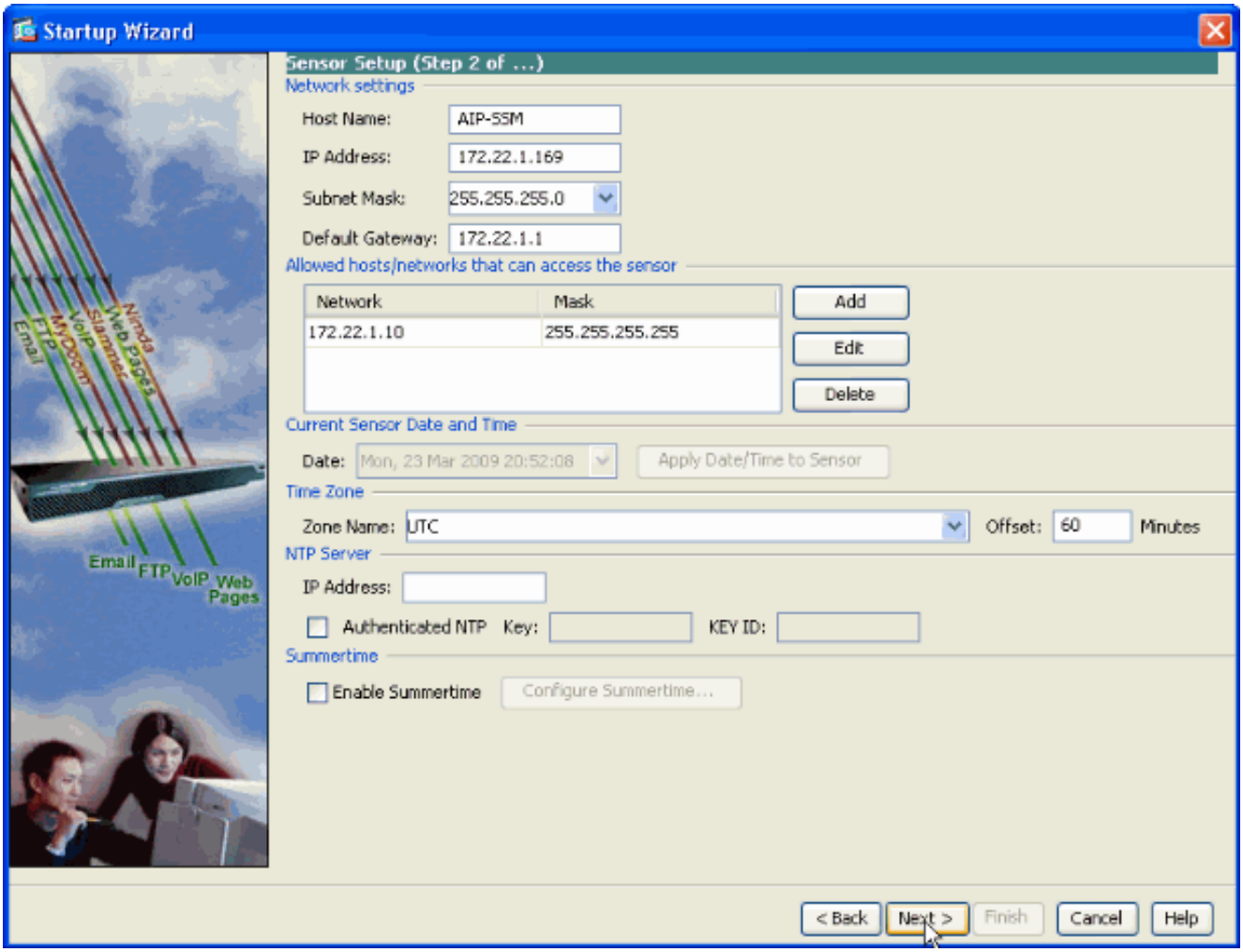
4. 新しいウィンドウでは、[Network Settings] セクションに表示される各領域で、AIP-SSM モジュールの [Host Name]、[IP Address]、[Subnet Mask]、および [Default Gateway address] を入力します。 AIP-SSM を使用してすべてのトラフィックを許可するようにアクセスリストを追加するには、[Add] をクリックします。



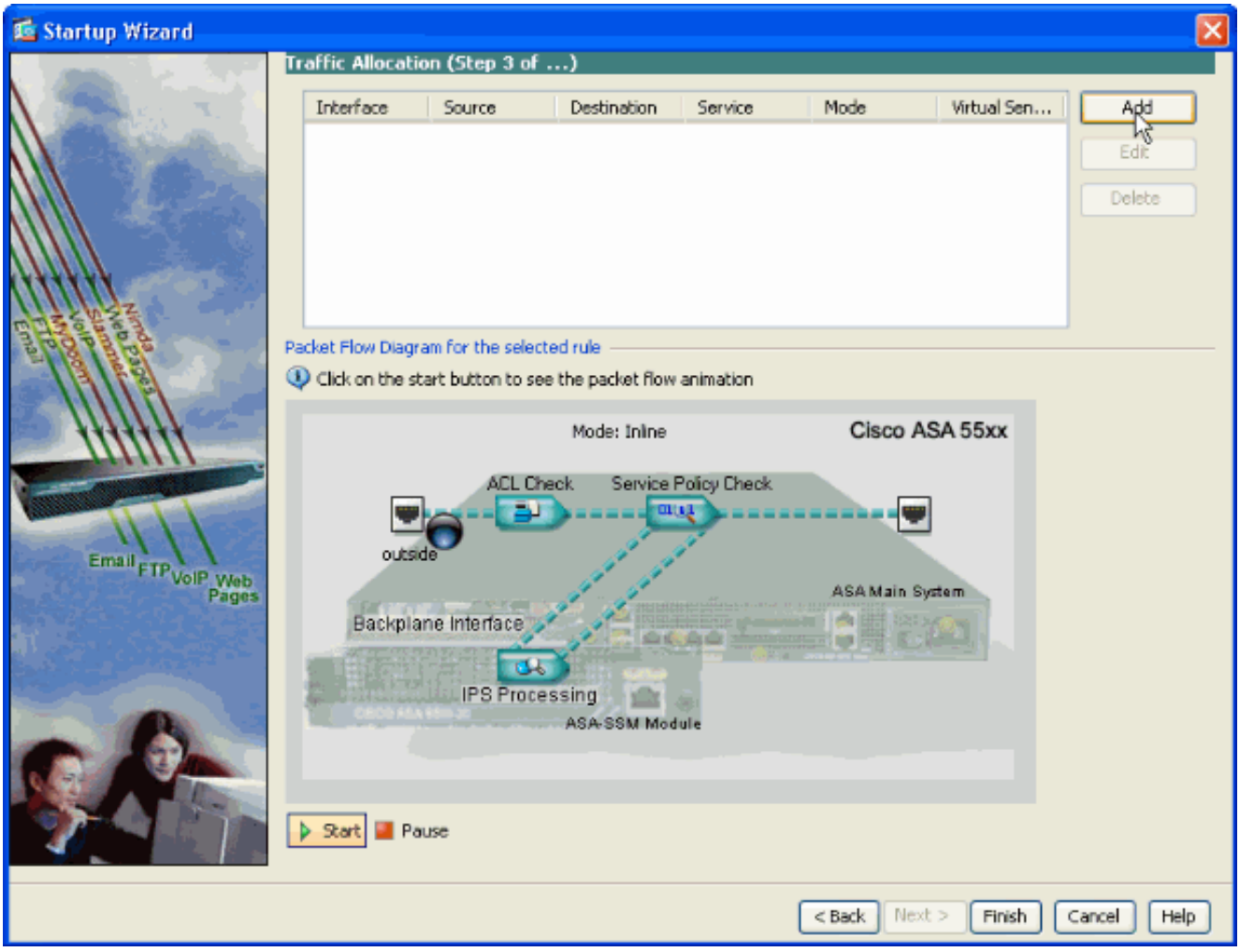
5. [Add ACL Entry] ウィンドウでは、ホストおよびネットワークの [IP Address] および [Network Mask] の詳細を入力して、センサーにアクセスできるようにします。 [OK] をクリックします。**注:** ホストおよびネットワークの IP アドレスは、管理ネットワークのアドレスの範囲内である必要があります。



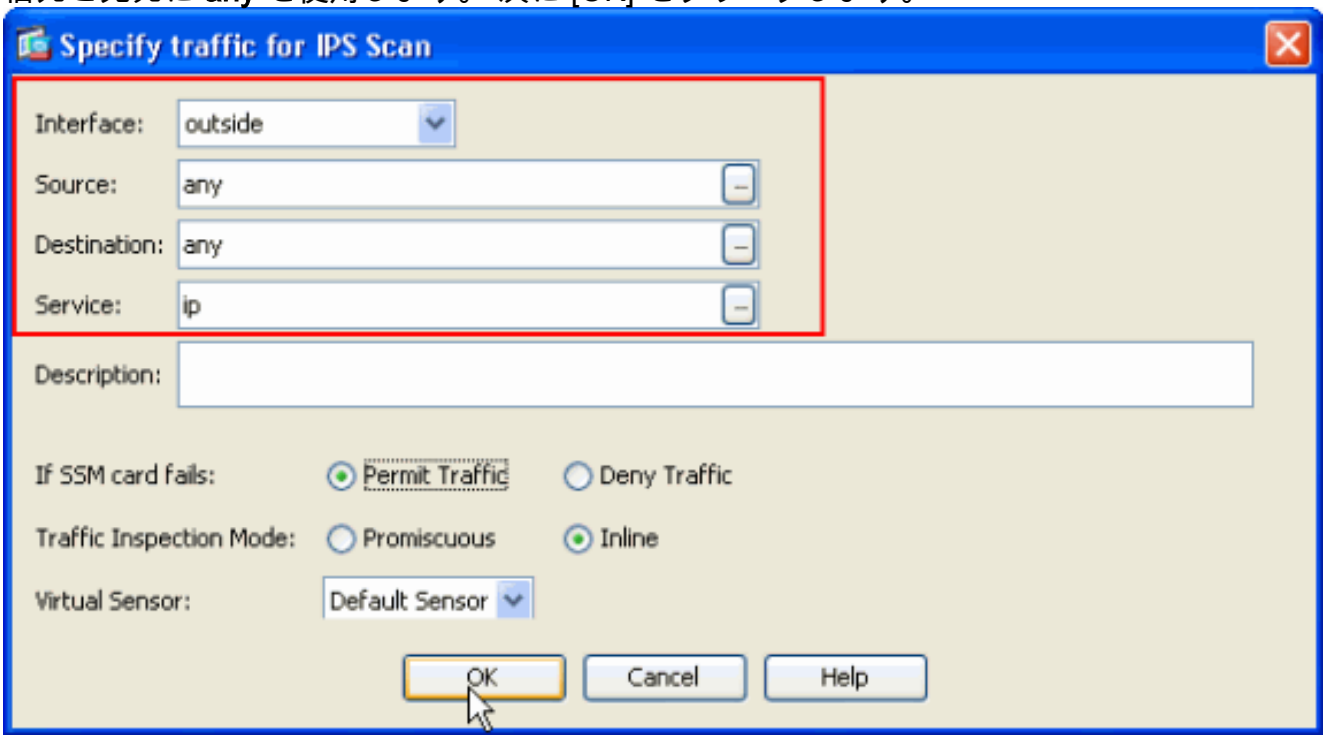
6. 提供されるそれぞれの領域で詳細を指定したら、[Next] をクリックします。



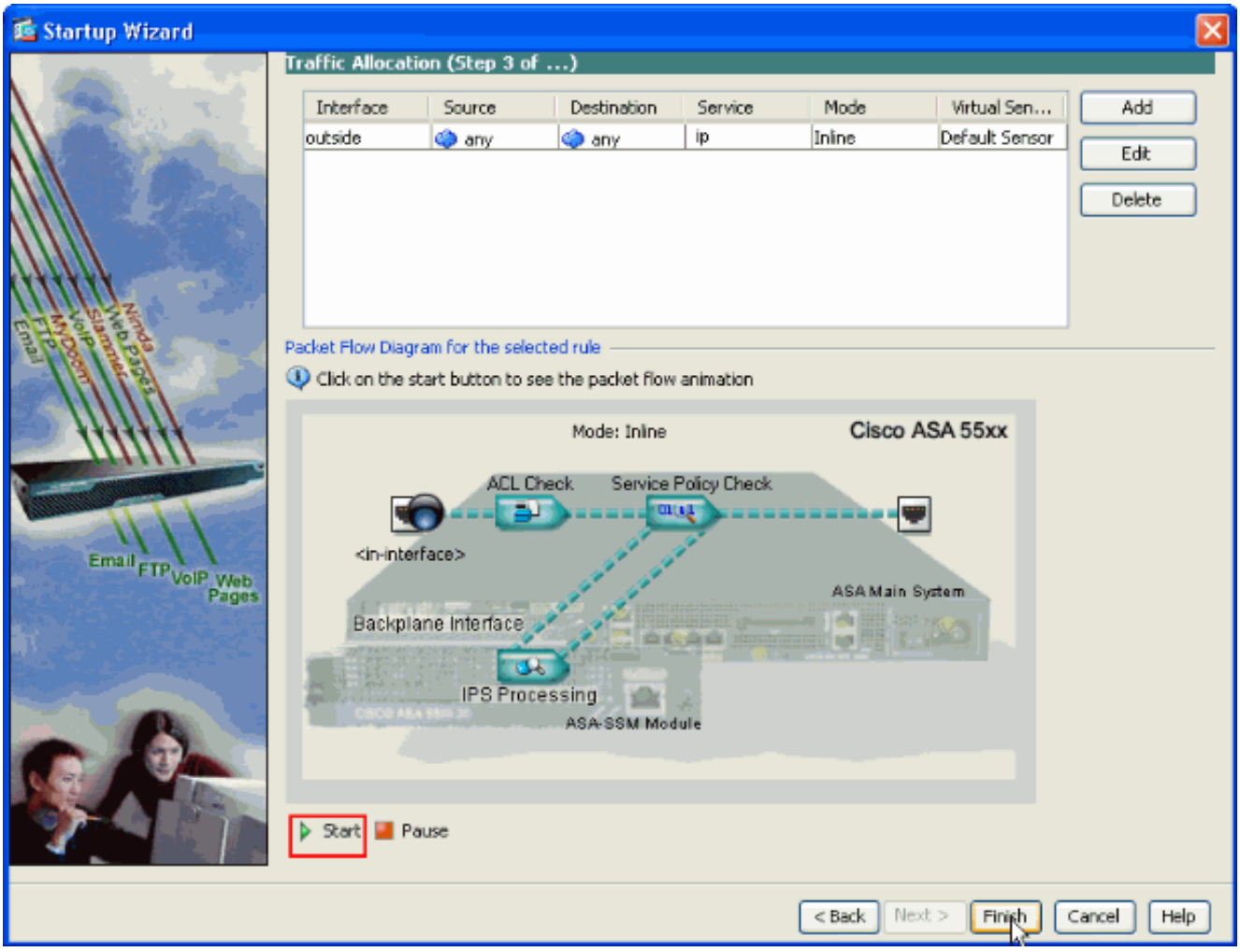
7. [Add] をクリックして、トラフィックの割り当ての詳細を設定します。



8. 送信元および宛先ネットワーク アドレスを入力し、サービスの種類、たとえばここで使用する IP も入力します。 この例では、AIP-SSM ですべてのトラフィックを検査するため、送信元と宛先に **any** を使用します。 次に [OK] をクリックします。



9. 設定されたトラフィックの割り当てルールがこのウィンドウに表示されます。ステップ 7 と 8 で説明したのと同じ手順を完了したら、必要なだけルールを追加できます。 次に、[Finish]をクリックし、ASDM の設定手順を完了します。**注:** [Start] をクリックすると、パケット フローのアニメーションを表示できます。



AIP-SSM による特定のトラフィックの検査

ネットワーク管理者が AIP-SSM モニタをすべてのトラフィックのサブネットとして設定する場合、ASA には設定可能な 2 つの独立した変数があります。 まず、必要なトラフィックを含めたり除外したりするように、アクセス リストを記述できます。 アクセス リストの修正に加えて、**サービス ポリシー**を特定のインターフェイスに適用したり、AIP-SSM によって検査されるトラフィックを変更するためにグローバルに適用できたりします。

ネットワーク管理者は、このドキュメント内のネットワーク図を参照して、外部ネットワークおよび DMZ ネットワーク間の すべてのトラフィックを AIP-SSM で検査することを必要としています。

```
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.

次に、このネットワーク管理者は、内部ネットワークから外部ネットワークへと*開始された*トラフィックを AIP-SSM でモニタすることを必要としています。 Inside ネットワークから DMZ ネットワークへのトラフィックは監視されません。

注: この特定のセクションでは、ステートフルネス、TCP、UDP、ICMP、接続、およびコネクションレス型通信に関する中程度の知識が必要です。

```
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
```

このアクセス リストでは、Inside ネットワークから発信され、DMZ ネットワークに宛てられたトラフィックが拒否されます。 2 番目のアクセス リストの行では、Inside ネットワークから発信され、AIP-SSM への Outside ネットワークに宛てられたトラフィックが許可または拒否されます。 この時点で、ASA のステートフルネスがその機能を発揮します。 たとえば、内部ユーザが Outside ネットワーク（ルータ）上のデバイスへの TCP 接続（Telnet）を開始します。 ユーザは、ルータへの接続とログインに成功します。 次に、ユーザは承認されていないルータ コマンドを発行します。 ルータは Command authorizaton failed を返します。 Command authorization failed という文字列を含むデータ パケットには、Outside ルータの発信元および Inside ユーザの宛先が含まれています。 発信元（Outside）および宛先（Inside）は、このドキュメントですでに定義されているアクセス リストには一致しません。 ASA では、ステートフルな接続が追跡されるため、（Outside から Inside へ）返されるデータ パケットは、検査のために AIP-SSM へ送信されます。 AIP-SSM で設定されたカスタム シグニチャ 60000 0 がアラームを発行します。

注: デフォルトでは、ASA では ICMP トラフィックの状態は保持されません。 上述の設定例では、内部ユーザが Outside ルータに対して PING（ICMP エコー要求）を実行します。 ルータは ICMP エコー応答を返します。 AIP-SSM では、エコー要求パケットは検査されますが、エコー応答パケットは検査されません。 ASA で ICMP 検査が有効になっている場合、エコー要求とエコー応答のどちらのパケットも AIP-SSM によって検査されます。

AIP-SSM スキャンからの特定のネットワーク トラフィックの除外

既定の一般化された例では、AIP-SSM でスキャンする特定のトラフィックを免除する際のビューが示されます。 これを実行するには、トラフィック フローが含まれているアクセスリストを作成する必要があります。このフローは、拒否のステートメントで AIP-SSM スキャンから除外されます。 この例では、IPS は、AIP-SSM でスキャンされるトラフィック フローを定義するアクセスリストの名前です。 <source> および <destination> 間のトラフィックは、スキャンから除外されます。 その他のすべてのトラフィックは検査されます。

```
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
```

確認

アラート イベントが AIP-SSM に記録されていることを確認します。

管理者ユーザ アカウントを使用して、AIP-SSM にログインします。 **show events alert** コマンドはこの出力を生成します。

注: 出力は、シグネチャ設定、AIP-SSM に送信されるトラフィックの種類、およびネットワーク負荷に基づいて異なります。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

```
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
```

この設定例では、複数の IPS シグニチャがテスト トラフィックに対してアラームを発行するように調整されています。 シグニチャ 2000 および 2004 は設定変更が行われています。 カスタム シグニチャ 60000 が追加されてます。 ラボ環境またはほとんどのデータが ASA を通過しないネットワークにおいては、イベントをトリガーするためにシグニチャの設定変更が必要になる場合があります。 ASA および AIP-SSM が大量のトラフィックが通過する環境に展開される場合、デフォルトのシグニチャ設定によってイベントが生成される可能性があります。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

ASA から **show** コマンドを発行します。

- **show module**：システム情報および ASA 上の SSM に関する情報を表示します。

```
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**：アクセス リストのカウンタを表示します。

```
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.
```

AIP-SSM を設置して使用する以前に、ネットワーク トラフィックは正常に ASA を通過していますか。 正常に通過しない場合、ネットワークおよび ASA アクセス ポリシー ルールにトラブルシューティングを行うことが必要な場合があります。

フェールオーバーの問題

- フェールオーバーが設定されている 2 台の ASA があり、それぞれが AIP-SSM を備えている場合は、AIP-SSM の設定を手動で複製する**必要があります**。 フェールオーバー メカニズムによって複製されるのは、ASA の設定だけです。 AIP-SSM はフェールオーバーに含まれません。 フェールオーバーの問題の詳細については、「PIX/ASA 7.x アクティブ/スタンバイ フェールオーバーの設定例 」を参照してください。
- ASA フェールオーバー ペアでステートフル フェールオーバーが設定されている場合、AIP-SSM はステートフル フェールオーバーに参加しません。

エラー メッセージ

次に示すように、IPS モジュール (AIP-SSM) によってエラー メッセージが生成され、イベントは発行されません。

```
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.
```

IPS バーチャル センサーが ASA のバックプレーン インターフェイスに割り当てられていないことがこのエラー メッセージの原因です。 SSM モジュールへトラフィックを送信するために ASA は適切な方法で設定されますが、SSM によってトラフィックがスキャンされるためには、ASA によって作成されたバックプレーン インターフェイスにバーチャル センサーを割り当てる必要が

あります。

```
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.
```

これらのメッセージは、すべてのシステム リソースを次々に占有する IP LOGGING が有効になっていることを示しています。 トラブルシューティングや調査を目的とする場合にだけ IP LOGGING を使用する必要があるため、Cisco では IP LOGGING を無効にすることをお勧めします。

注: errWarning インライン データのバイパスが開始され、エラー メッセージが表示されることが予測されます。シグネチャの更新後にセンサーによって分析エンジンがただちに再起動されるためで、これはシグネチャの更新プロセスの必要な部分です。

Syslog のサポート

AIP-SSM は syslog をアラート形式としてサポートしていません。

AIP-SSM からアラート情報を受け取るデフォルトの方法には、Security Device Event Exchange（SDEE）を介する方式があります。 他には、個々のシグネチャがトリガーされたときに取るアクションとして、SNMP トラップを生成するためにそれらを設定するオプションがあります。

AIP-SSM の再起動

AIP-SSM モジュールが正常に応答しません。

AIP-SSM モジュールが正しく応答しない場合は、ASA を再起動せずに AIP-SSM モジュールを再起動します。 AIP-SSM モジュールを再起動し、ASA を再起動しないためには、hw-module module 1 reload コマンドを使用します。

AIP-SSM の電子メール アラート

AIP-SSM はユーザに電子メール アラートを送信できますか。

いいえ。これはサポートされていません。

関連情報

- Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2
- Cisco セキュリティ アプライアンス システム ログ メッセージ、バージョン 7.2
- シスコ侵入防御システムのためのコマンド リファレンス 5.1
- テクニカル サポートとドキュメント – Cisco Systems