ASA:ASA에서 AIP SSM 컨피그레이션으로 네트워크 트래픽 전송 예시

목차

소개

이 문서에서는 Cisco ASA 5500 Series ASA(Adaptive Security Appliance)를 통과하는 네트워크 트래픽을 AIP-SSM(Advanced Inspection and Prevention Security Services Module)(IPS) 모듈로 전송하는 방법에 대한 샘플 컨피그레이션을 제공합니다.컨피그레이션 예제는 CLI(Command Line Interface)와 함께 제공됩니다.

ASA 참조:Cisco ASA 5500 Series ASA(Adaptive Security Appliance)에서 CSC-SSM(Content Security and Control Security Services Module)으로 네트워크 트래픽을 전송하려면 ASA에서 CSC-SSM 컨피그레이션 예로 네트워크 트래픽 전송

다중 상황 모드에서 Cisco ASA 5500 Series ASA(Adaptive Security Appliance)를 통과하는 네트워크 트래픽을 AIP-SSM(Advanced Inspection and Prevention Security Services Module) (IPS) 모듈로 전송하는 방법에 대한 자세한 내용은 보안 컨텍스트에 가상 센서 할당(AIP SSM전용)을 참조하십시오.

참고: ASA를 통과하는 네트워크 트래픽에는 DMZ(Demilitarized Zone) 또는 내부 네트워크에서

ASA로 보호되는 리소스에 액세스하는 인터넷 또는 인터넷 사용자에 액세스하는 내부 사용자가 포함됩니다.ASA에서 보내고 받는 네트워크 트래픽은 검사를 위해 IPS 모듈로 전송되지 않습니다.IPS 모듈로 전송되지 않는 트래픽의 예에는 ASA 인터페이스에 ping(ICMP) 또는 ASA에 텔넷팅이 포함됩니다.

참고: 검사를 위해 트래픽을 분류하기 위해 ASA에서 사용하는 모듈식 정책 프레임워크는 IPv6를 지원하지 않습니다. 따라서 ASA를 통해 IPv6 트래픽을 AIP SSM으로 전환하면 지원되지 않습니다.

참고: AIP-SSM의 초기 컨피그레이션에 대한 자세한 내용은 AIP-SSM 센서의 초기 컨피그레이션을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에서는 청중이 Cisco ASA 소프트웨어 버전 8.x 및 IPS 소프트웨어 버전 6.x를 구성하는 방법에 대한 기본적인 지식을 가지고 있다고 가정합니다.

- ASA 8.x에 필요한 컨피그레이션 구성 요소에는 인터페이스, 액세스 목록, NAT(Network Address Translation) 및 라우팅이 포함됩니다.
- AIP-SSM(IPS 소프트웨어 6.x)에 필요한 컨피그레이션 구성 요소에는 네트워크 설정, 허용된 호스트, 인터페이스 컨피그레이션, 시그니처 정의, 이벤트 작업 규칙이 포함됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0.2이 포함된 ASA 5510
- AIP-SSM-10(IPS 소프트웨어 버전 6.1.2 포함)

참고: 이 컨피그레이션 예는 OS 7.x 이상이 포함된 모든 Cisco ASA 5500 Series Firewall 및 IPS 5.x 이상이 포함된 AIP-SSM 모듈과 호환됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

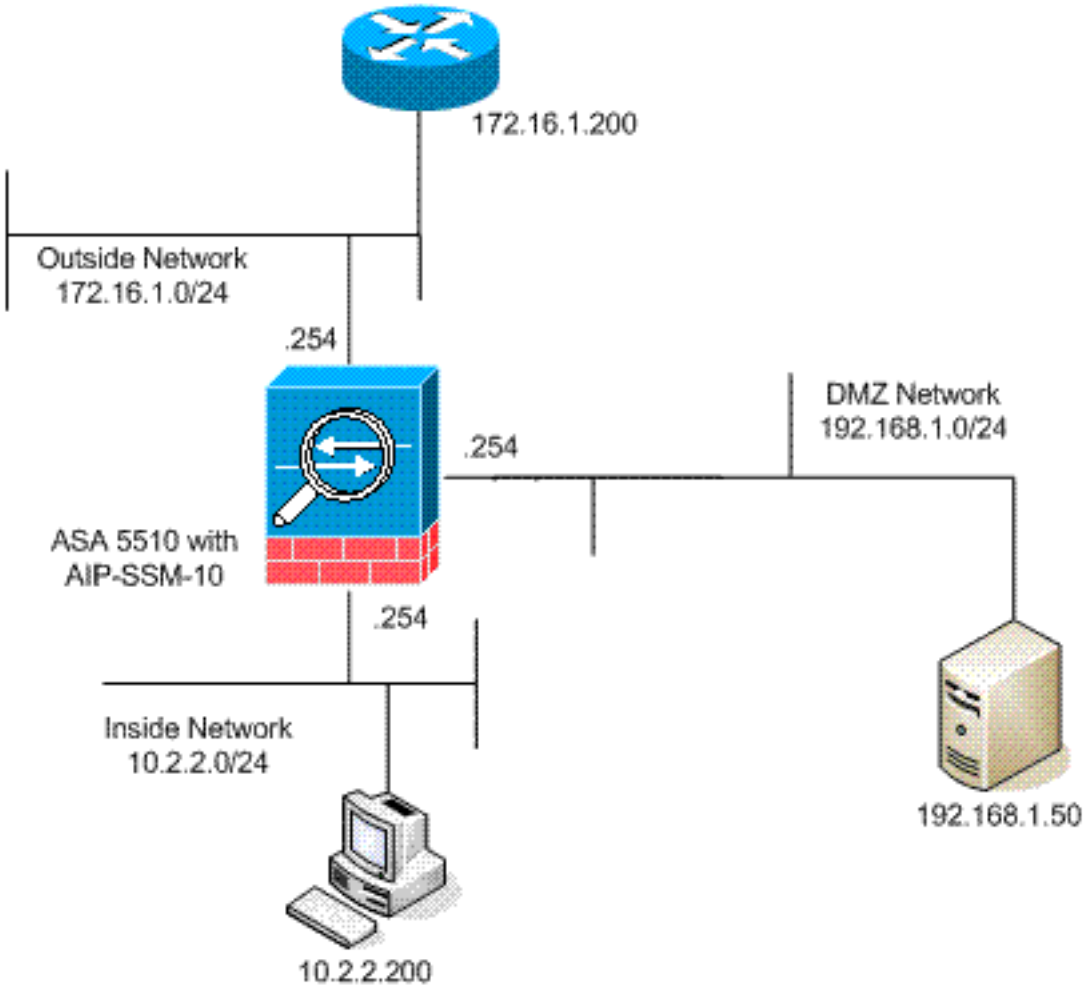
이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

이 컨피그레이션에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



초기 컨피그레이션

이 문서에서는 이러한 구성을 사용합니다.ASA와 AIP-SSM 모두 기본 컨피그레이션으로 시작하지만 테스트 목적으로 특정 변경 사항이 있습니다.추가는 컨피그레이션에 표시됩니다.

- 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#
```

참고: https로 AIP-SSM 모듈에 액세스할 수 없는 경우 다음 단계를 완료하십시오.

- 모듈의 관리 IP 주소를 구성합니다.관리 IP에 연결할 수 있는 IPs/IP 네트워크를 지정하는 을 구성할 수 있습니다.
- AIP 모듈의 외부 이더넷 인터페이스를 연결했는지 확인합니다.AIP 모듈에 대한 관리 액세스는 이 인터페이스에서만 가능합니다.

자세한 내용은 AIP-SSM 초기화를 참조하십시오.

인라인 또는 무차별 모드에서 AIP-SSM으로 모든 트래픽 검사

네트워크 관리자와 회사 고위 경영진은 모든 것을 모니터링해야 한다고 종종 말합니다.이 컨피그레이션은 모든 것을 모니터링하는 요구 사항을 충족합니다.모든 것을 모니터링하는 것 외에도 ASA와 AIP-SSM의 상호 작용 방식에 대해 두 가지 결정을 내려야 합니다.

- AIP-SSM 모듈이 작동하거나 프로미스큐어스 또는 인라인 모드에서 구축됩니까?프로미스큐어스 모드는 ASA가 원래 데이터를 대상에 전달하는 동안 데이터의 복사본이 AIP-SSM에 전송됨을 의미합니다.프로미스큐어스 모드의 AIP-SSM은 IDS(Intrusion Detection System)로 간주할 수 있습니다. 이 모드에서는 트리거 패킷(경보를 발생시키는 패킷)이 여전히 대상에 도달할 수 있습니다.차단은 발생하며 추가 패킷이 대상에 도달하는 것을 중지할 수 있지만 트리거 패킷은 중지되지 않습니다.인라인 모드는 ASA가 검사를 위해 AIP-SSM에 데이터를 전달함을 의미합니다.데이터가 AIP-SSM 검사를 통과하면 데이터가 ASA로 반환되어 계속 처리되고 대상으로 전송됩니다.인라인 모드의 AIP-SSM은 IPS(Intrusion Prevention System)로 간주할 수 있습니다. 무차별 모드와 달리 인라인 모드(IPS)는 트리거 패킷이 목적지에 도달하는 것을 실제로 중지할 수 있습니다.
- ASA가 AIP-SSM과 통신할 수 없는 경우, ASA는 검사할 트래픽을 어떻게 처리합니까?ASA가 AIP-SSM과 통신할 수 없는 경우 또는 AIP-SSM이 다시 로드되거나 모듈에 오류가 발생하여 교체가 필요한 경우의 인스턴스 예이 경우 ASA가 fail-open 또는 fail-closed일 수 있습니다.Fail-open을 사용하면 AIP-SSM에 연결할 수 없는 경우 ASA가 최종 대상으로 검사 대상 트래픽을 계속 전달할 수 있습니다.ASA가 AIP-SSM과 통신할 수 없는 경우 fail-closed blocks to-be-inspected traffic.**참고:** 검사할 트래픽은 access-list를 사용하여 정의됩니다.이 예제 출력에서 access-list는 모든 소스에서 모든 대상으로의 모든 IP 트래픽을 허용합니다.따라서 검사할 트래픽은 ASA를 통과하는 모든 것이 될 수 있습니다.

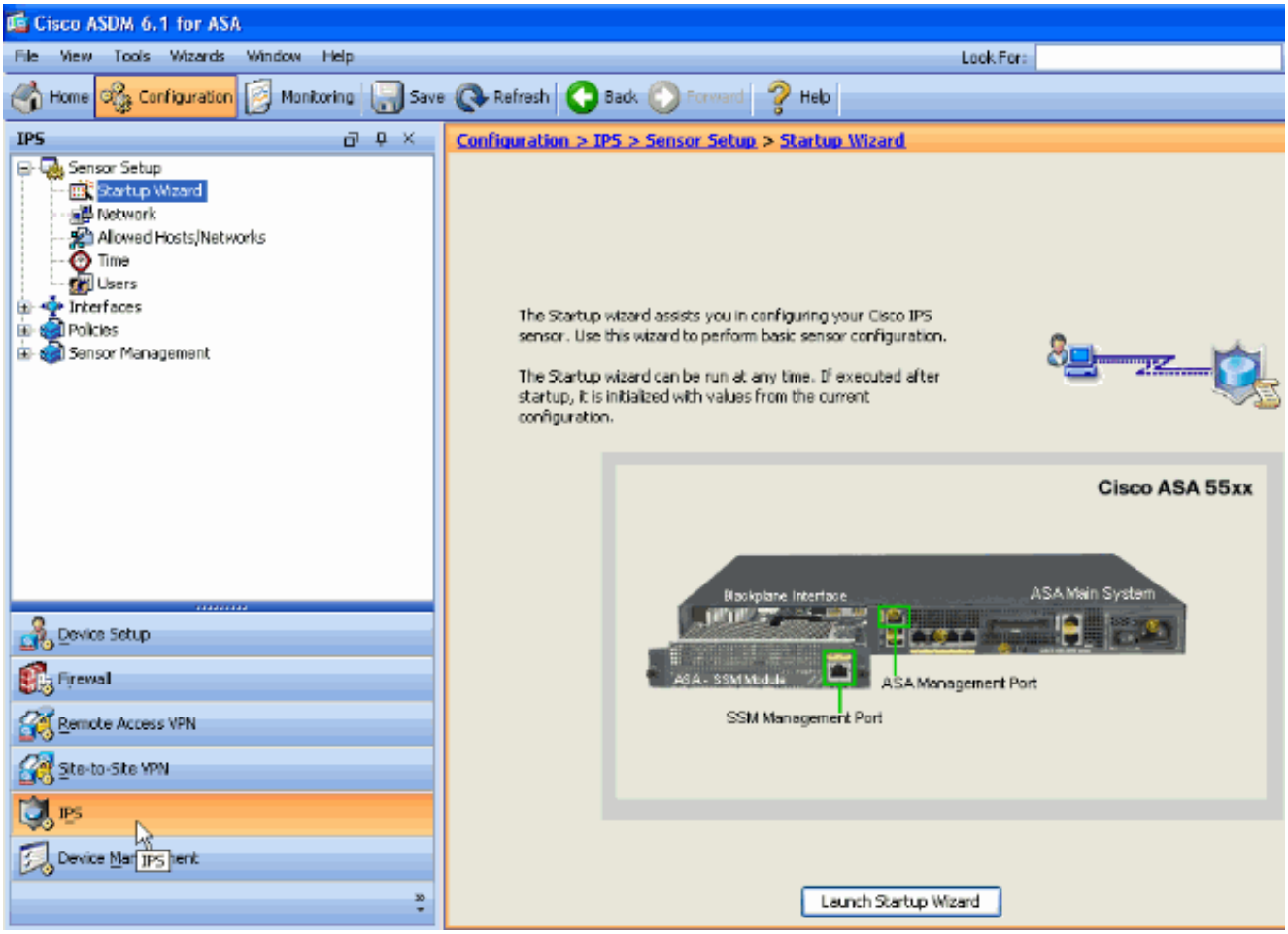
```
ciscoasa(config)#access-list traffic_for_ips permit ip any any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
!--- The match any command can be used in place of !--- the match access-list [access-list name]
command. !--- In this example, access-list 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.
```

ASDM을 사용하여 AIP-SSM으로 모든 트래픽 검사

ASDM을 사용하는 AIP-SSM을 사용하여 모든 트래픽을 검사하려면 다음 단계를 완료합니다.

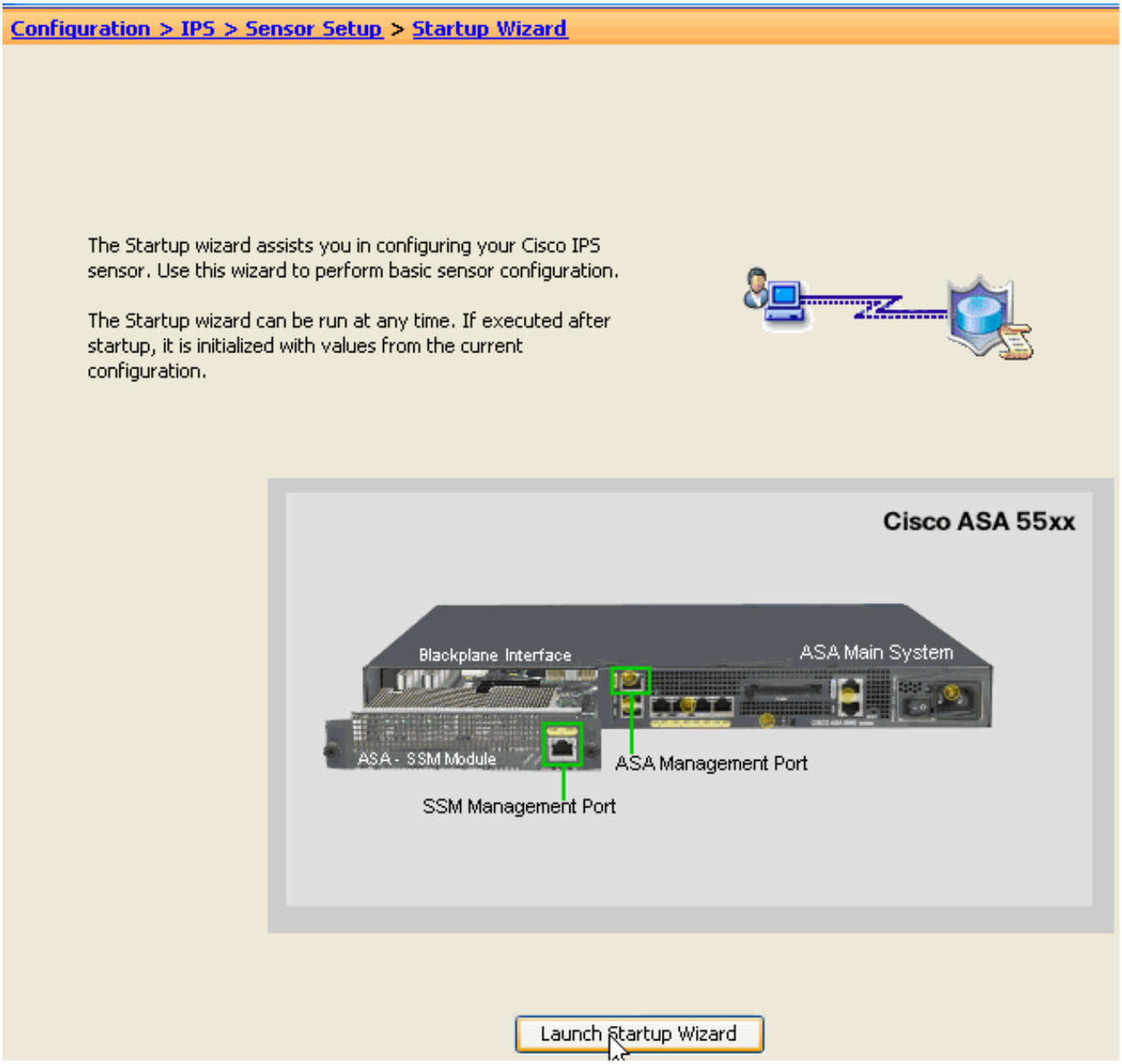
1. 다음과 **같이** 컨피그레이션 **> IPS > Sensor Setup > ASDM** 홈 페이지에서 시작 마법사를 선택하여 컨피그레이션을 시작합니다

.



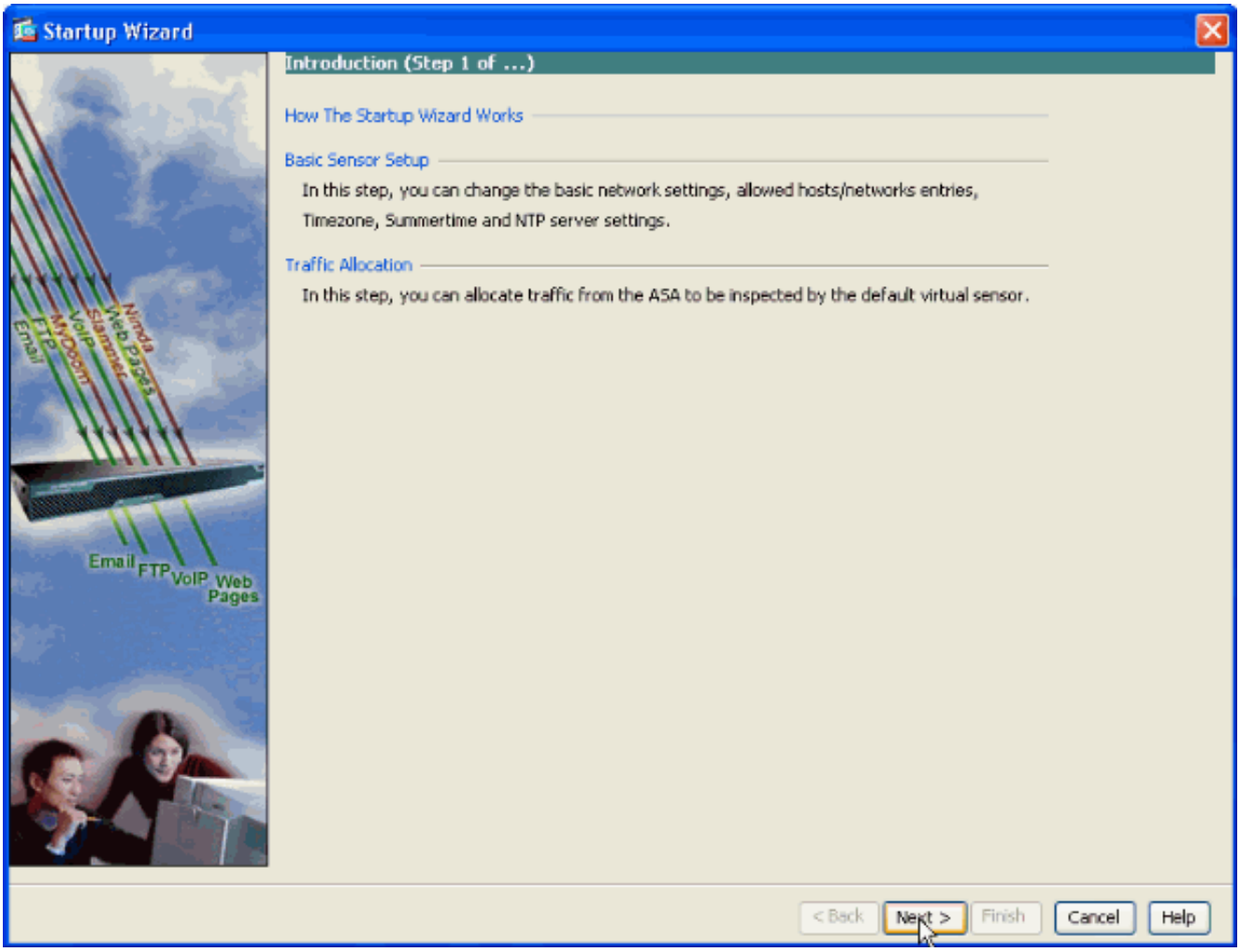
2. 시작 **마법사 시작을 클릭합니다**

.

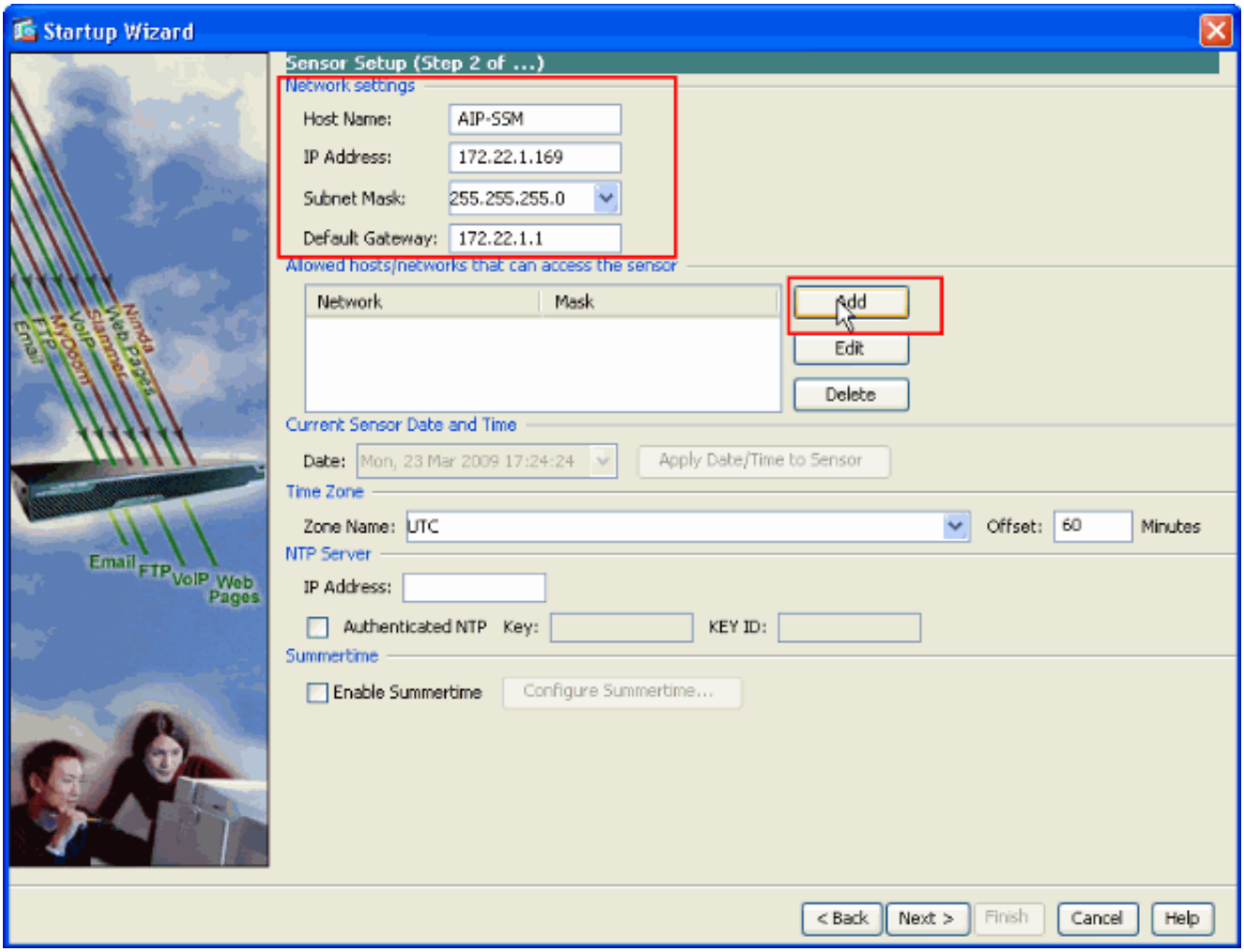


3. 시작 마법사를 시작한 후 나타나는 새 창에서 Next를 클릭합니다

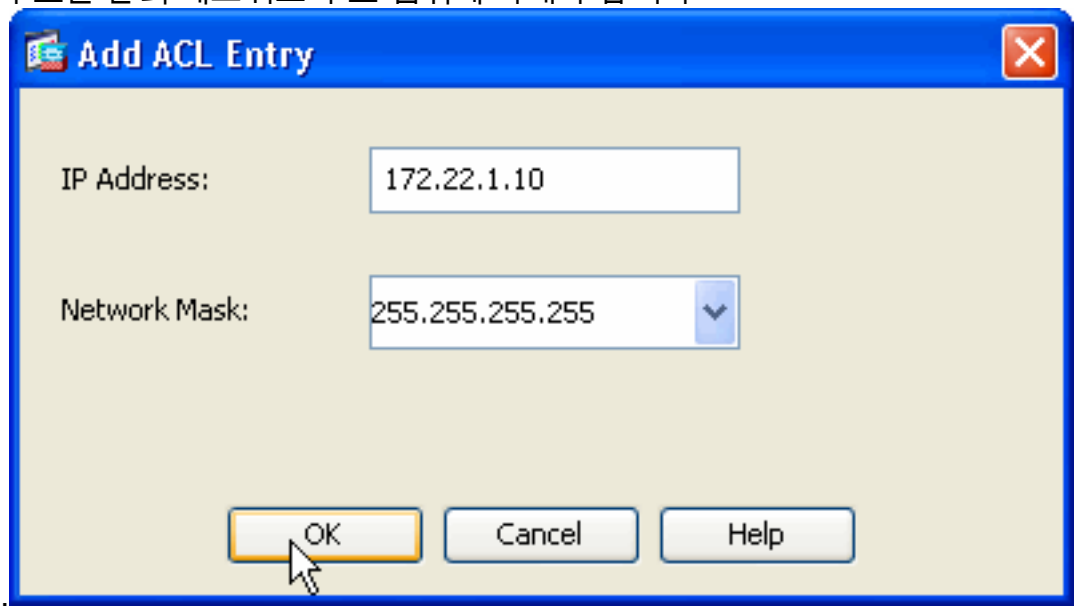
.



4. 새 창에서 Network settings(네트워크 설정) 섹션에 제공된 각 공간에 AIP-SSM 모듈에 대한 호스트 이름, IP 주소, 서브넷 마스크 및 기본 게이트웨이 주소를 입력합니다.그런 다음 **Add(추가)**를 클릭하여 AIP-SSM을 사용하는 모든 트래픽을 허용하도록 액세스 목록을 추가합니다
.



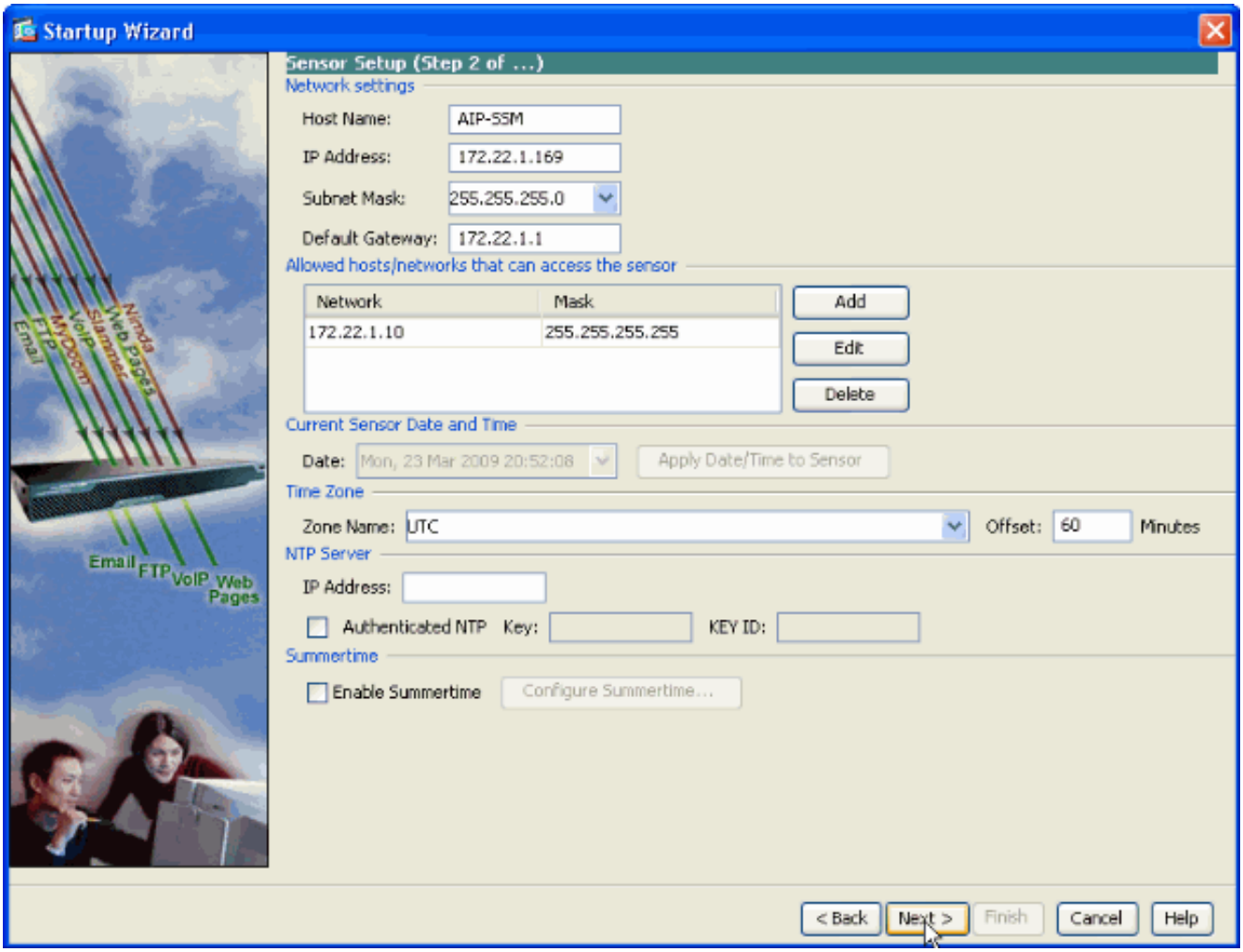
5. Add **ACL Entry(ACL 항목 추가)** 창에서 **IP 주소** 및 센서에 액세스할 수 있는 호스트/네트워크의 네트워크 마스크 세부사항을 제공합니다.OK(확인)**를 클릭합니다.참고:** 호스트/네트워크 IP 주소는 관리 네트워크 주소 범위에 속해야 합니다



.

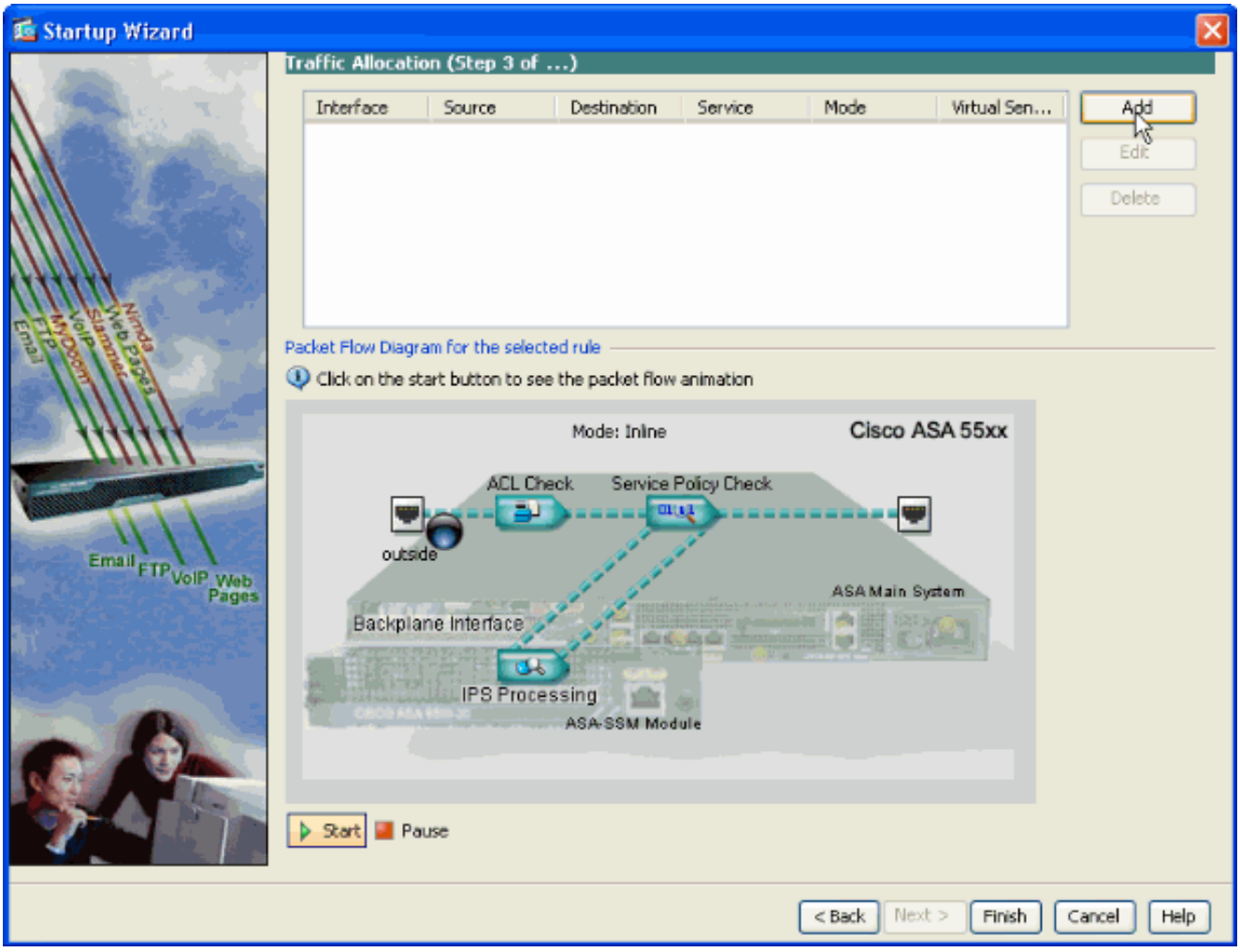
6. 제공된 각 공간에 세부사항을 입력한 후 Next(다음)를 클릭합니다

.



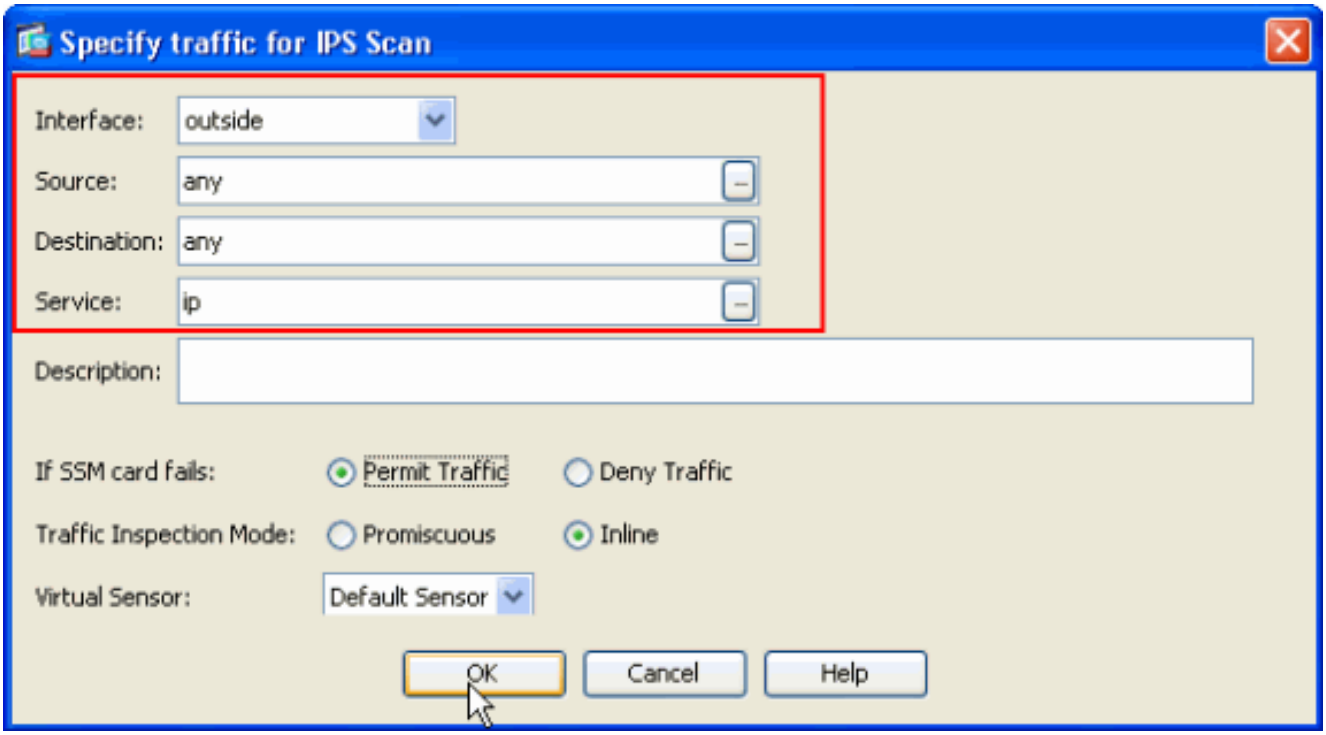
7. Add(**추가**)를 클릭하여 트래픽 할당 세부사항을 구성합니다

.



8. 소스 및 대상 네트워크 주소 및 서비스 유형(예: IP가 여기에 사용됨)을 제공합니다.이 예에서 **any**는 AIP-SSM을 사용하여 모든 트래픽을 검사할 때 소스 및 대상에 사용됩니다.그런 다음 **확인**을 클릭합니다

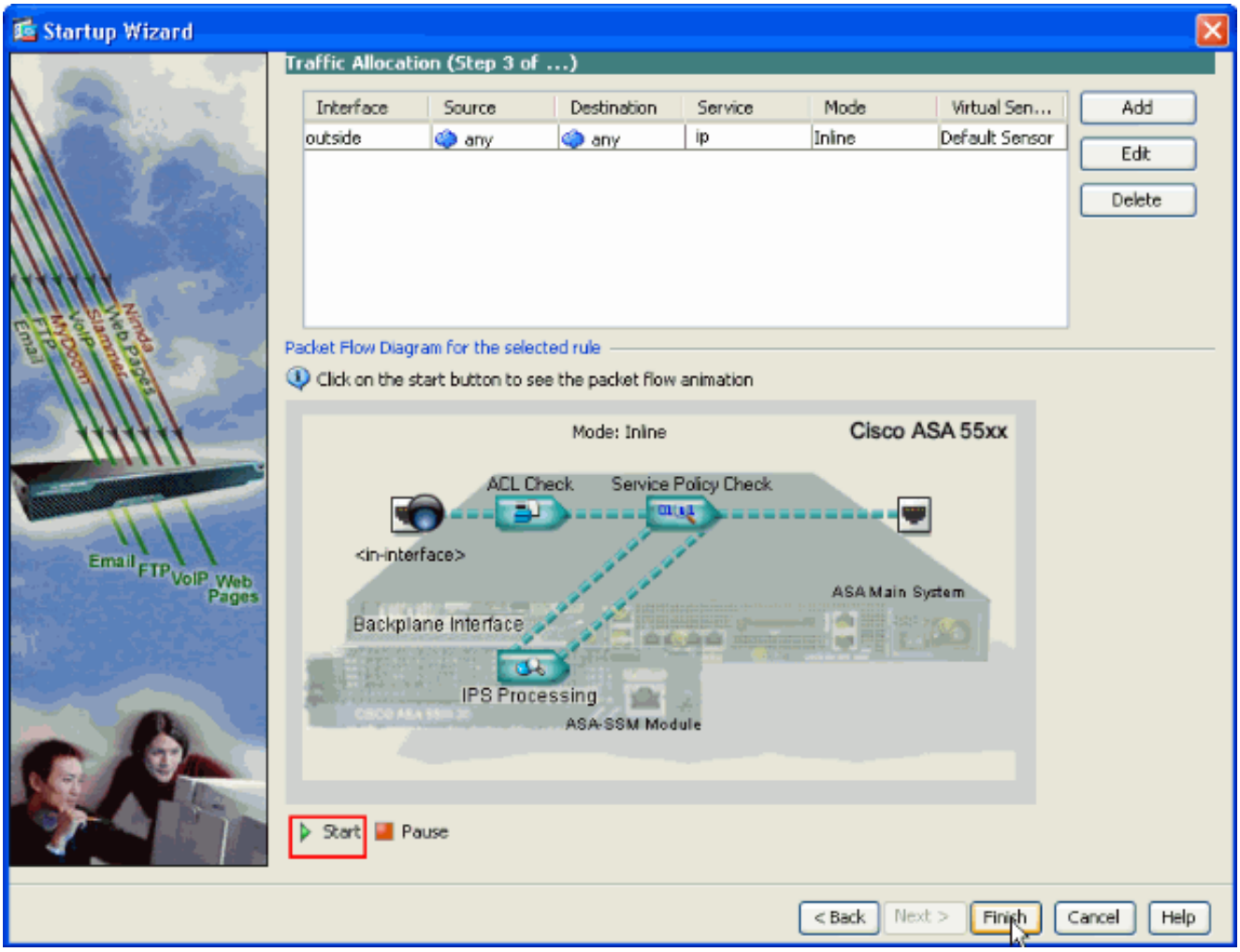
.



9. 구성된 트래픽 할당 규칙이 이 창에 표시되며, 7단계와 8단계에서 설명한 것과 동일한 절차를 완료한 경우 필요에 따라 규칙을 최대한 많이 추가할 수 있습니다. 그런 다음 **마침을** 클릭합니다. 그러면 ASDM 구성 절차가 완료됩니다.**참고: 시작**을 클릭하면 패킷 흐름 애니메이션을 볼

수 있습니다

.



AIP-SSM으로 특정 트래픽 검사

네트워크 관리자가 AIP-SSM 모니터를 모든 트래픽의 하위 집합으로 사용하려는 경우 ASA에는 수정할 수 있는 두 가지 독립 변수가 있습니다.먼저 필요한 트래픽을 포함하거나 제외하도록 access-list를 작성할 수 있습니다.액세스 목록 수정 외에도 AIP-SSM에서 검사한 트래픽을 변경하기 위해 **서비스 정책**을 인터페이스에 적용하거나 전역적으로 적용할 수 있습니다.

이 문서의 네트워크 다이어그램에 대한 참조를 통해 네트워크 관리자는 AIP-SSM이 외부 네트워크와 DMZ 네트워크 간의 *모든* 트래픽을 검사하도록 요청합니다.

```
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.

다음으로, 네트워크 관리자는 AIP-SSM이 내부 네트워크에서 외부 네트워크로 *시작된* 트래픽을 모니터링하기를 원합니다.내부 네트워크-DMZ 네트워크는 모니터링되지 않습니다.

참고: 이 특정 섹션에서는 상태, TCP, UDP, ICMP, 연결 및 연결 없는 통신에 대한 중간 이해가 필요합니다.

```
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
```

access-list는 DMZ 네트워크로 향하는 내부 네트워크에서 시작된 트래픽을 거부합니다.두 번째 액세스 목록 라인은 외부 네트워크로 향하는 내부 네트워크에서 시작된 트래픽을 AIP-SSM으로 허용하거나 전송합니다.이 시점에서 ASA의 상태가 실제로 나타납니다.예를 들어 내부 사용자는 외부 네트워크(라우터)의 디바이스에 대한 TCP 연결(텔넷)을 시작합니다. 사용자가 라우터에 성공적으로 연결하고 로그인합니다.그러면 사용자는 권한이 없는 라우터 명령을 실행합니다.라우터가 명령 권한 부여에 . 문자열이 포함된 데이터 패킷에는 외부 라우터의 소스와 내부 사용자의 대상이 있습니다.소스(외부) 및 대상(내부)이 이 문서에 이전에 정의된 액세스 목록과 일치하지 않습니다 .ASA는 상태 저장 연결을 추적하므로 (외부로) 반환하는 데이터 패킷이 검사를 위해 AIP-SSM에 전송됩니다.AIP-SSM에 구성된 사용자 지정 서명 60000 0, 경보

참고: 기본적으로 ASA는 ICMP 트래픽의 상태를 유지하지 않습니다.이전 샘플 컨피그레이션에서는 내부 사용자 ping(ICMP 에코 요청)이 외부 라우터를 ping합니다.라우터는 ICMP 에코 응답으로 응답합니다.AIP-SSM은 에코 요청 패킷을 검사하지만 에코 응답 패킷은 검사하지 않습니다.ASA에서 ICMP 검사가 활성화된 경우 에코 요청과 에코 응답 패킷 모두 AIP-SSM에서 검사합니다.

AIP-SSM 검사에서 특정 네트워크 트래픽 제외

지정된 일반 예제는 AIP-SSM에서 검사할 특정 트래픽을 제외하는 보기를 제공합니다.이를 수행하려면 deny 문에서 AIP-SSM 스캐닝에서 제외할 트래픽 흐름이 포함된 액세스 목록을 생성해야 합니다.이 예에서 IPS는 AIP-SSM에서 검사할 트래픽 흐름을 정의하는 액세스 목록의 이름입니다 .<source>와 <destination> 사이의 트래픽은 스캐닝에서 제외됩니다.다른 모든 트래픽은 검사됩니다.

```
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
```

다음을 확인합니다.

경고 이벤트가 AIP-SSM에 기록되는지 확인합니다.

관리자 사용자 계정으로 AIP-SSM에 로그인합니다.show events **alert** 명령**은** 이 출력을 생성합니다 .

참고: 출력은 시그니처 설정, AIP-SSM으로 전송되는 트래픽 유형 및 네트워크 로드에 따라 달라집니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

```
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
```

샘플 컨피그레이션에서는 테스트 트래픽에 대한 경보에 여러 IPS 시그니처가 조정됩니다.서명 2000 및 2004가 수정되었습니다.사용자 지정 서명 60000이 추가됩니다.적은 데이터가 ASA를 통과하는 랩 환경 또는 네트워크에서 이벤트를 트리거하려면 서명을 수정해야 할 수 있습니다.많은 양의 트래픽을 전달하는 환경에 ASA 및 AIP-SSM이 구축된 경우 기본 시그니처 설정이 이벤트를 생성할 가능성이 높습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

ASA에서 이러한 **show** 명령을 실행합니다.

- **show module** - ASA의 SSM 정보와 시스템 정보를 표시합니다.

```
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.
```

- **실행 표시**

```
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** - access-list에 대한 카운터를 표시합니다.

```
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-SSM을 설치하고 사용하기 전에 네트워크 트래픽이 예상대로 ASA를 통과합니까?그렇지 않은 경우 네트워크 및 ASA 액세스 정책 규칙의 문제를 해결해야 합니다.

장애 조치 문제

- 장애 조치 컨피그레이션에 두 개의 ASA가 있고 각각 AIP-SSM이 있는 경우 AIP-SSM의 컨피그레이션을 수동으로 복제해야 **합니다**.ASA의 컨피그레이션만 장애 조치 메커니즘에 의해 복제됩니다.AIP-SSM은 장애 조치에 포함되지 않습니다.장애 조치 문제에 대한 자세한 내용은 PIX/ASA 7.x Active/Standby Failover Configuration Example을 참조하십시오.
- ASA 장애 조치 쌍에 상태 저장 장애 조치가 구성된 경우 AIP-SSM은 상태 저장 장애 조치에 참여하지 않습니다.

오류 메시지

IPS 모듈(AIP-SSM)은 표시된 대로 오류 메시지를 생성하며 이벤트를 실행하지 않습니다.

```
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.
```

이 오류 메시지의 원인은 IPS 가상 센서가 ASA의 백플레인 인터페이스에 할당되지 않았기 때문입니다.SSM 모듈로 트래픽을 전송하기 위해 ASA가 올바른 방식으로 설정되었지만 SSM이 트래픽을 스캔하기 위해 ASA가 생성하는 백플레인 인터페이스에 가상 센서를 할당해야 합니다.

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

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

이러한 메시지는 IP LOGGING이 활성화되고 있으며, 이 경우 모든 시스템 리소스가 호스팅됩니다 .문제 해결/조사 목적으로만 사용해야 하므로 IP 로깅을 비활성화하는 것이 좋습니다.

참고: 서명 업데이트 프로세스에 필요한 부분인 서명 업데이트 후 센서가 분석 엔진을 잠시 재시작하면 오류 시작되었다는 오류 메시지가 나타날 것으로 예상됩니다.

Syslog 지원

AIP-SSM은 syslog를 경고 형식으로 지원하지 않습니다.

AIP-SSM에서 알림 정보를 수신하는 기본 방법은 SDEE(Security Device Event Exchange)를 사용하는 것입니다. 또 다른 옵션은 SNMP 트랩을 트리거될 때 수행할 작업으로 생성하기 위해 개별 서명을 구성하는 것입니다.

AIP-SSM 재부팅

AIP-SSM 모듈이 제대로 응답하지 않습니다.

AIP-SSM 모듈이 제대로 응답하지 않으면 ASA를 재부팅하지 않고 AIP-SSM 모듈을 재부팅합니다 .AIP-SSM 모듈을 재부팅하고 ASA를 재부팅하지 않으려면 hw-module module 1 reload 명령을 사용합니다.

AIP-SSM 이메일 알림

AIP-SSM에서 사용자에게 이메일 알림을 보낼 수 있습니까?

아니요, 지원되지 않습니다.

관련 정보

- Cisco Security Appliance 명령 참조, 버전 7.2
- Cisco Security Appliance 시스템 로그 메시지, 버전 7.2
- Cisco Intrusion Prevention System 5.1에 대한 명령 참조
- 기술 지원 및 문서 – Cisco Systems