

ASA:從ASA向AIP SSM傳送網路流量配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[初始配置](#)

[在內聯或承諾模式下使用AIP-SSM檢查所有流量](#)

[使用ASDM檢查AIP-SSM的所有流量](#)

[使用AIP-SSM檢查特定流量](#)

[從AIP-SSM掃描中排除特定網路流量](#)

[驗證](#)

[疑難排解](#)

[故障切換問題](#)

[錯誤消息](#)

[Syslog 支援](#)

[AIP-SSM重新引導](#)

[AIP-SSM電子郵件警報](#)

[相關資訊](#)

簡介

本文提供如何傳送通過Cisco ASA 5500系列自適應安全裝置(ASA)的網路流量到高級檢測和防禦安全服務模組(AIP-SSM)(IPS)模組的示例配置。配置示例隨命令列介面(CLI)提供。

請參閱[ASA:將網路流量從ASA傳送到CSC-SSM配置示例](#)，以便將網路流量從Cisco ASA 5500系列自適應安全裝置(ASA)傳送到內容安全和控制安全服務模組(CSC-SSM)。

有關如何將多情景模式下通過Cisco ASA 5500系列自適應安全裝置(ASA)的網路流量傳送到高級檢測和防禦安全服務模組(AIP-SSM)(IPS)模組的詳細資訊，請參閱[將虛擬感測器分配到安全情景 \(僅限AIP SSM \)](#)。

注意：通過ASA的網路流量包括訪問網際網路的內部使用者或訪問非軍事區(DMZ)或內部網路中受ASA保護的資源的網際網路使用者。傳送到ASA和從ASA傳送的網路流量不會傳送到IPS模組進行檢測。未傳送到IPS模組的流量示例包括ASA介面的ping(ICMP)或Telnet到ASA。

注意：ASA用於對流量進行分類以進行檢測的模組化策略框架不支援IPv6。因此，如果通過ASA將IPv6流量轉移到AIP SSM，則不支援該框架。

註：有關AIP-SSM初始配置的詳細資訊，請參閱[AIP-SSM感測器的初始配置](#)。

必要條件

需求

本文檔假設受眾對如何配置Cisco ASA軟體版本8.x和IPS軟體版本6.x有基本瞭解。

- ASA 8.x的必要配置元件包括介面、訪問清單、網路地址轉換(NAT)和路由。
- AIP-SSM (IPS軟體6.x) 的必要配置元件包括網路設定、允許的主機、介面配置、特徵碼定義和事件操作規則。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5510，軟體版本8.0.2
- 採用IPS軟體版本6.1.2的AIP-SSM-10

注意：此配置示例與OS 7.x及更高版本的任何Cisco ASA 5500系列防火牆和IPS 5.x及更高版本的AIP-SSM模組相容。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

設定

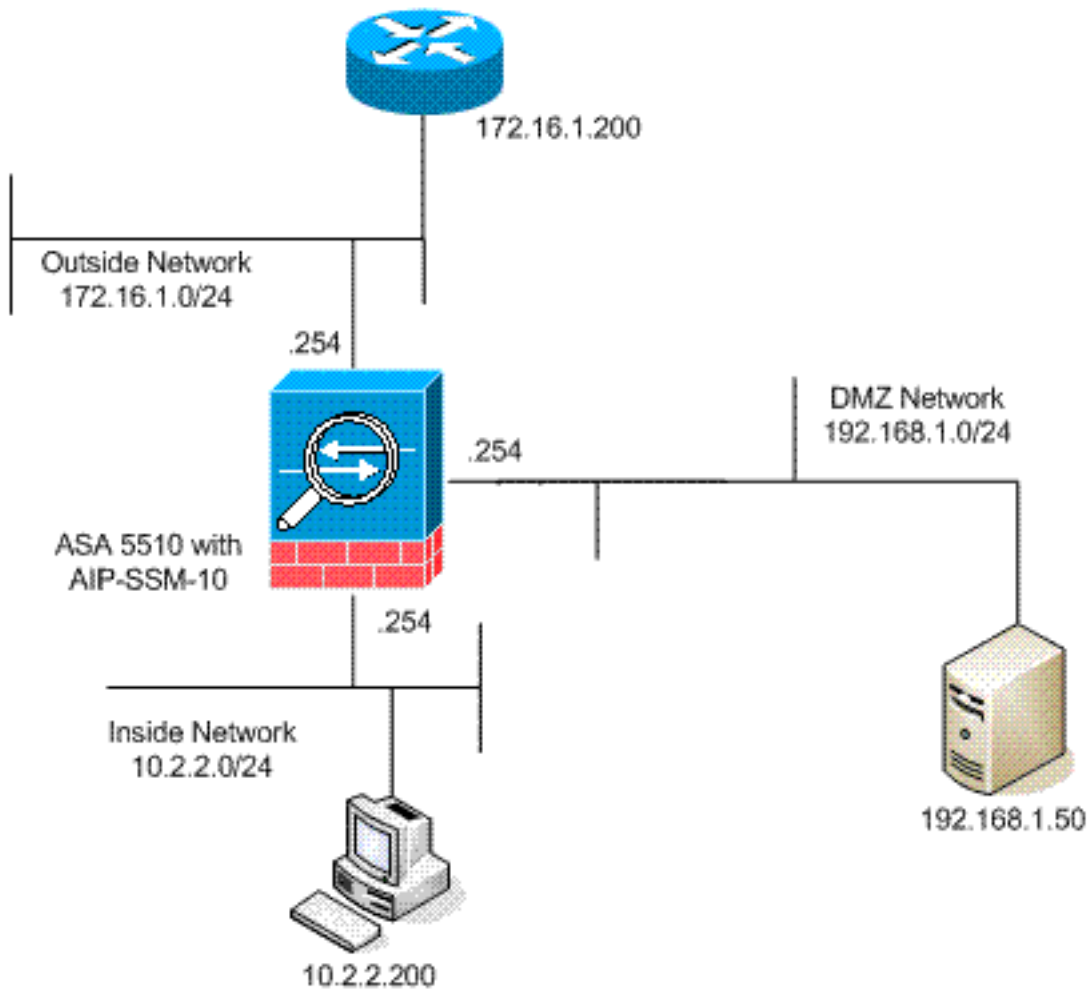
本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

此配置中使用的IP編址方案在Internet上不能合法路由。它們是[RFC 1918](#)，已在實驗室環境中使用。

網路圖表

本檔案會使用以下網路設定：



初始配置

本檔案會使用這些設定。ASA和AIP-SSM均以預設配置開始，但出於測試目的進行了特定更改。配置中註明了新增內容。

- [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：如果無法使用https訪問AIP-SSM模組，請完成以下步驟：

- 為模組配置管理IP地址。而且您可以配置network access list，在其中指定允許連線到管理IP的IP/IP網路。
 - 確保已連線AIP模組的外部乙太網介面。只能通過此介面對AIP模組進行管理訪問。
- 有關詳細資訊，請參閱[初始化AIP-SSM](#)。

在內聯或承諾模式下使用AIP-SSM檢查所有流量

網路管理員和公司高級管理層經常指出需要監控一切。此配置符合監控所有內容的要求。除了監控一切外，還需要就ASA和AIP-SSM如何互動做出兩個決策。

- AIP-SSM模組是否正常工作或以混雜或內聯模式部署？混雜模式是指當ASA將原始資料轉發到目的地時，資料副本被傳送到AIP-SSM。混雜模式下的AIP-SSM可視為入侵檢測系統(IDS)。在此模式下，觸發資料包（導致警報的資料包）仍然可以到達目的地。可以發生迴避，並阻止其他封包到達目的地，但不會停止觸發封包。內聯模式表示ASA將資料轉發到AIP-SSM以進行檢測。如果資料通過AIP-SSM檢測，則資料會返回到ASA以繼續處理並傳送到目的地。內嵌模式中的AIP-SSM可視為入侵防禦系統(IPS)。與混雜模式不同，內嵌模式(IPS)實際上可以阻止觸發封包到達目的地。
- 如果ASA無法與AIP-SSM通訊，ASA應如何處理待檢查流量？ASA無法與AIP-SSM進行通訊的例項包括AIP-SSM重新載入，或者模組出現故障需要更換的情況。在這種情況下，ASA可以失效開放或失效關閉。如果無法訪問AIP-SSM，失效開放允許ASA繼續將待檢查流量傳遞到最終目標。當ASA無法與AIP-SSM通訊時，失效關閉阻止要檢查的流量。**注意：**使用訪問清單定義要檢查的流量。在此範例輸出中，存取清單允許從任何來源到任何目的地的所有IP流量。因此，要檢查的流量可以是通過ASA的任何流量。

```
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 promiscuous fail-open
!--- If AIP-SSM is in promiscuous mode, issue !--- the no ips promiscuous fail-open command !---
in order to negate the command and then use !--- the ips inline fail-open command.
```

使用ASDM檢查AIP-SSM的所有流量

完成以下步驟，以便使用使用ASDM的AIP-SSM檢查所有流量：

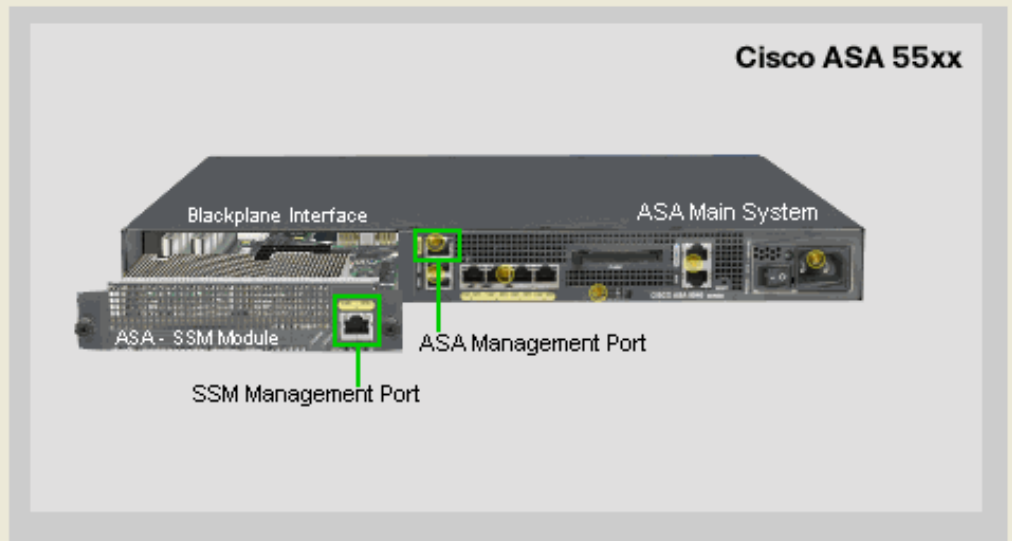
1. 在ASDM首頁中選擇Configuration > IPS > Sensor Setup > Startup Wizard以啟動配置，如下所示：

The screenshot displays the Cisco ASDM 6.1 for ASA interface. The top menu bar includes File, View, Tools, Wizards, Window, and Help. Below the menu is a navigation bar with Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help buttons. The left sidebar shows a tree view under 'IPS' with sub-items: Sensor Setup, Startup Wizard (highlighted), Network, Allowed Hosts/Networks, Time, Users, Interfaces, Policies, and Sensor Management. Below the sidebar are buttons for Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, IPS, and Device Management. The main content area is titled 'Configuration > IPS > Sensor Setup > Startup Wizard'. It contains introductory text about the wizard and a diagram of a Cisco ASA 55xx hardware unit. The diagram labels the Backplane Interface, ASA Main System, ASA-SSM Module, ASA Management Port, and SSM Management Port. A 'Launch Startup Wizard' button is located at the bottom of the main content area.

2. 按一下啟動啟動嚮導。

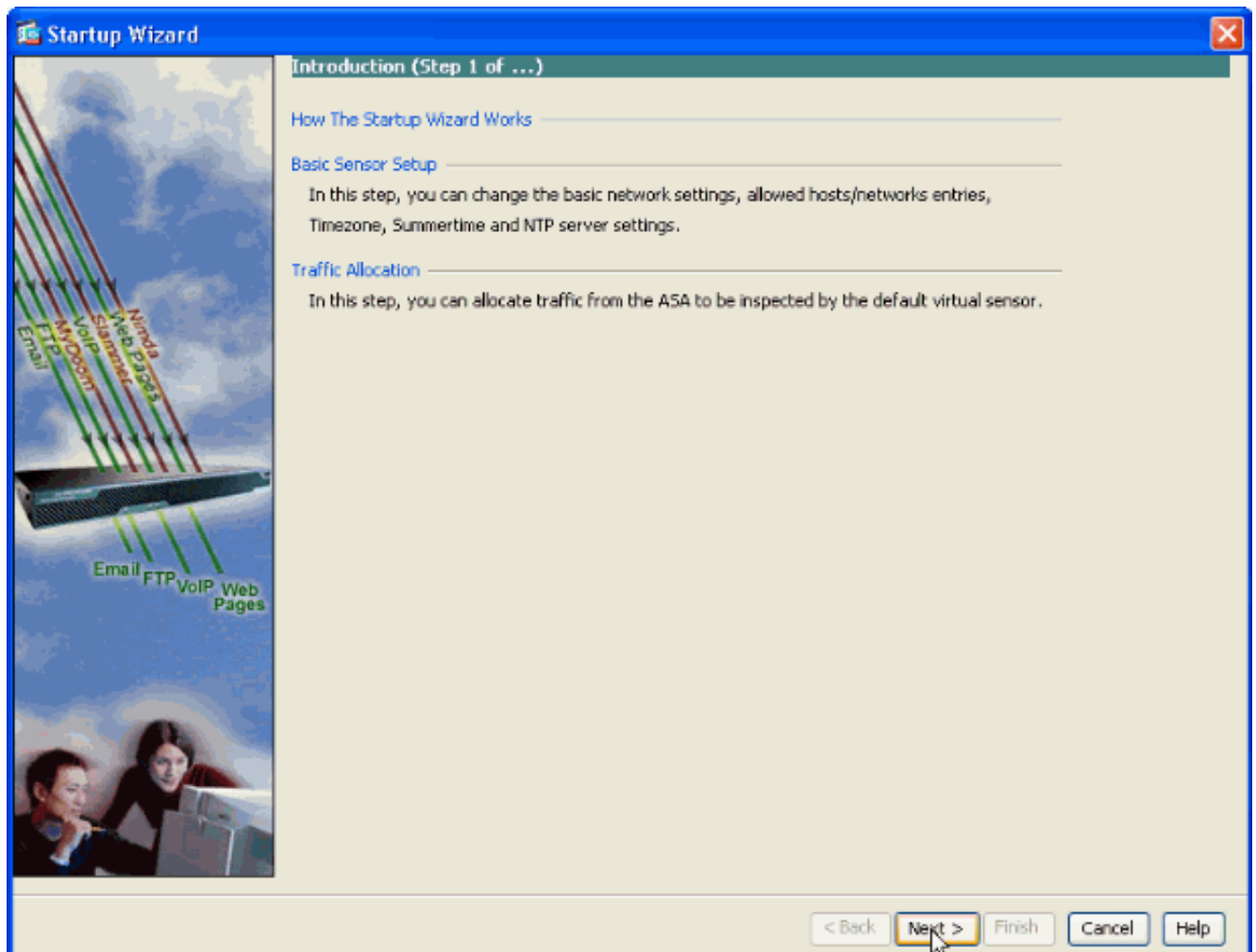
The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.

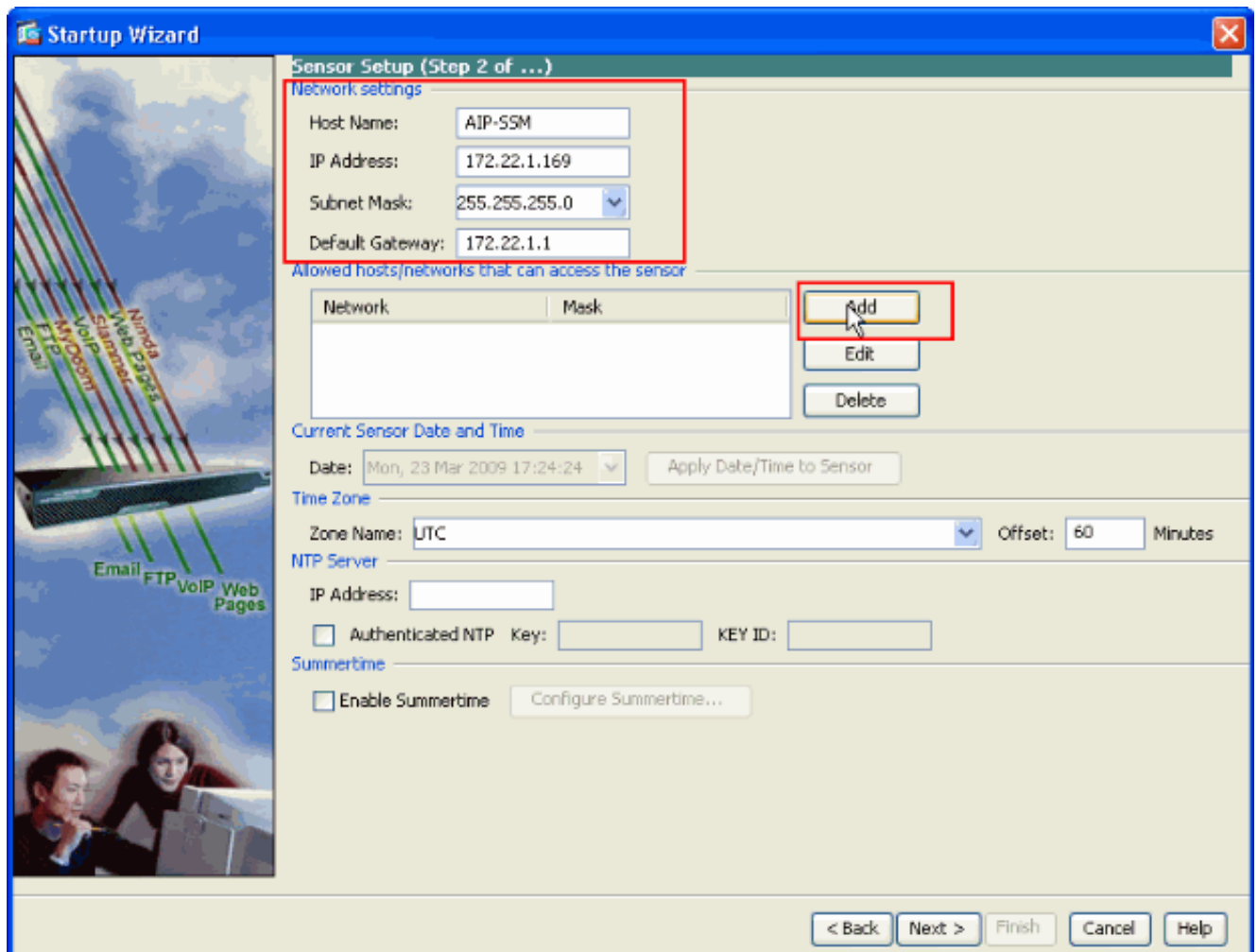


Launch Startup Wizard

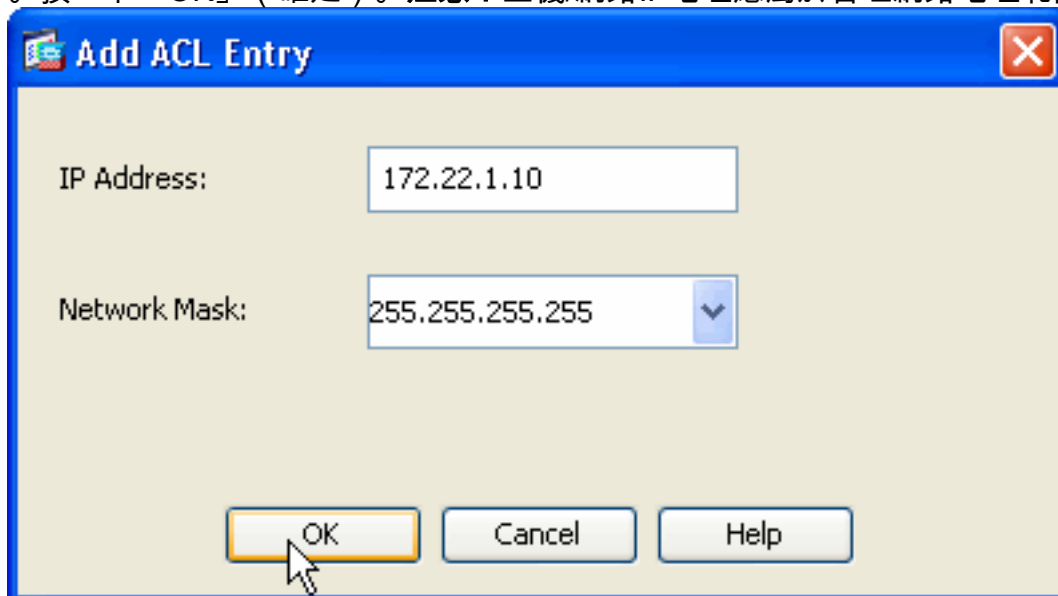
3. 在啟動嚮導後出現的新視窗中按一下下一步。



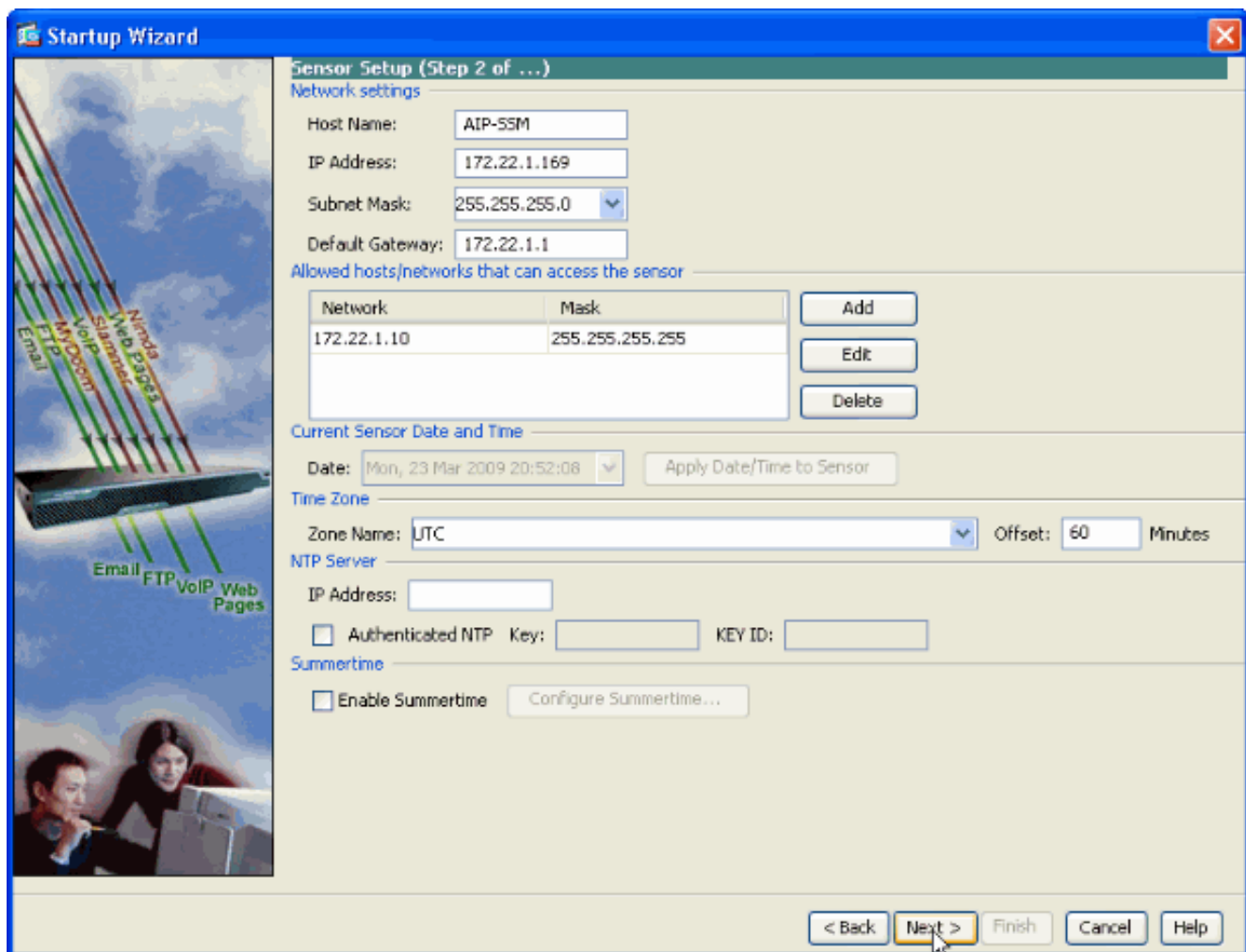
4. 在新視窗中，在Network settings部分下提供的相應空間中提供AIP-SSM模組的主機名、IP地址、子網掩碼和預設網關地址。然後按一下**Add**以新增存取清單，以允許使用AIP-SSM的所有流量。



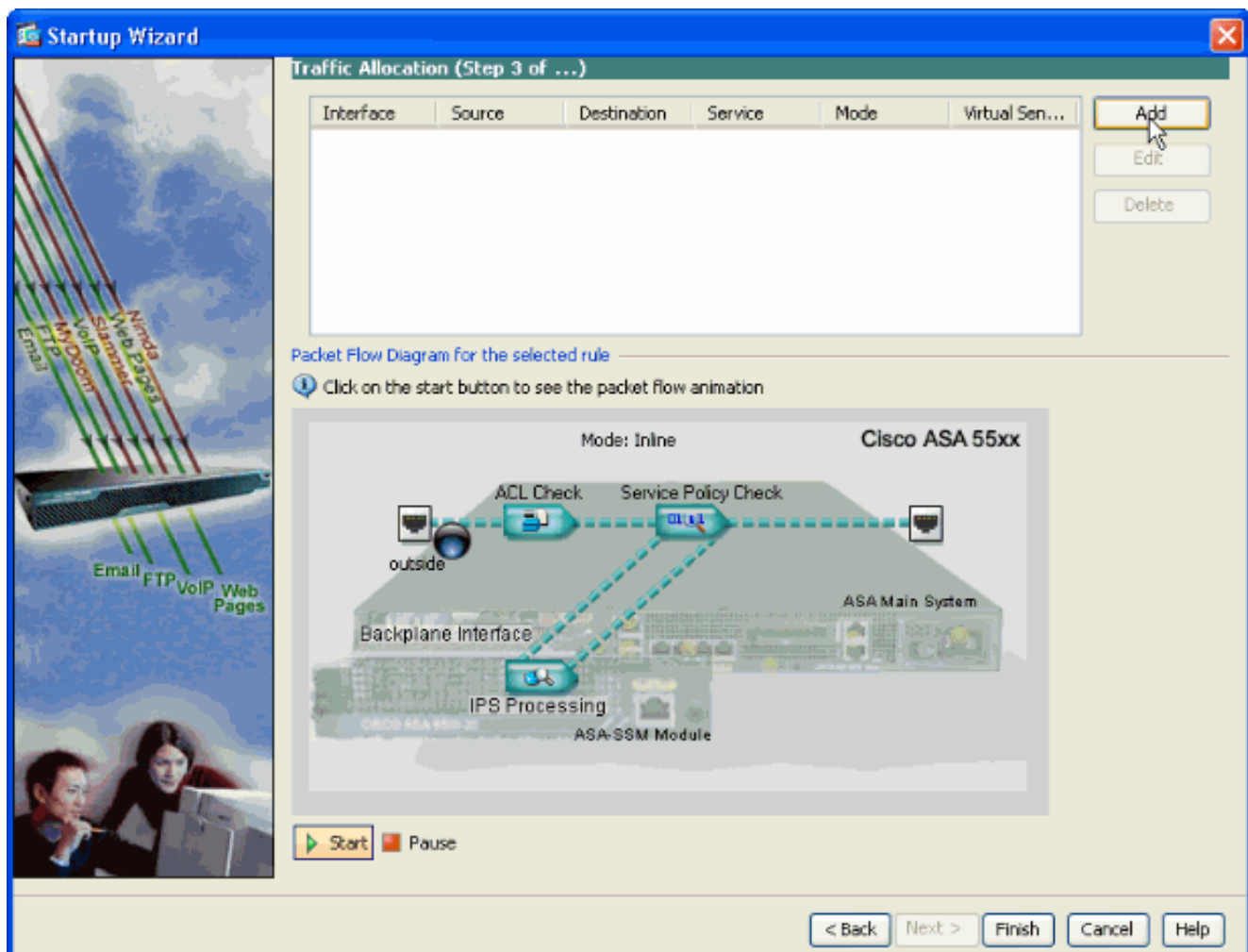
5. 在「Add ACL Entry」視窗中，提供允許訪問感測器的主機/網路的IP地址和網路掩碼詳細資訊。按一下「OK」（確定）。**注意：**主機/網路IP地址應屬於管理網路地址範圍。



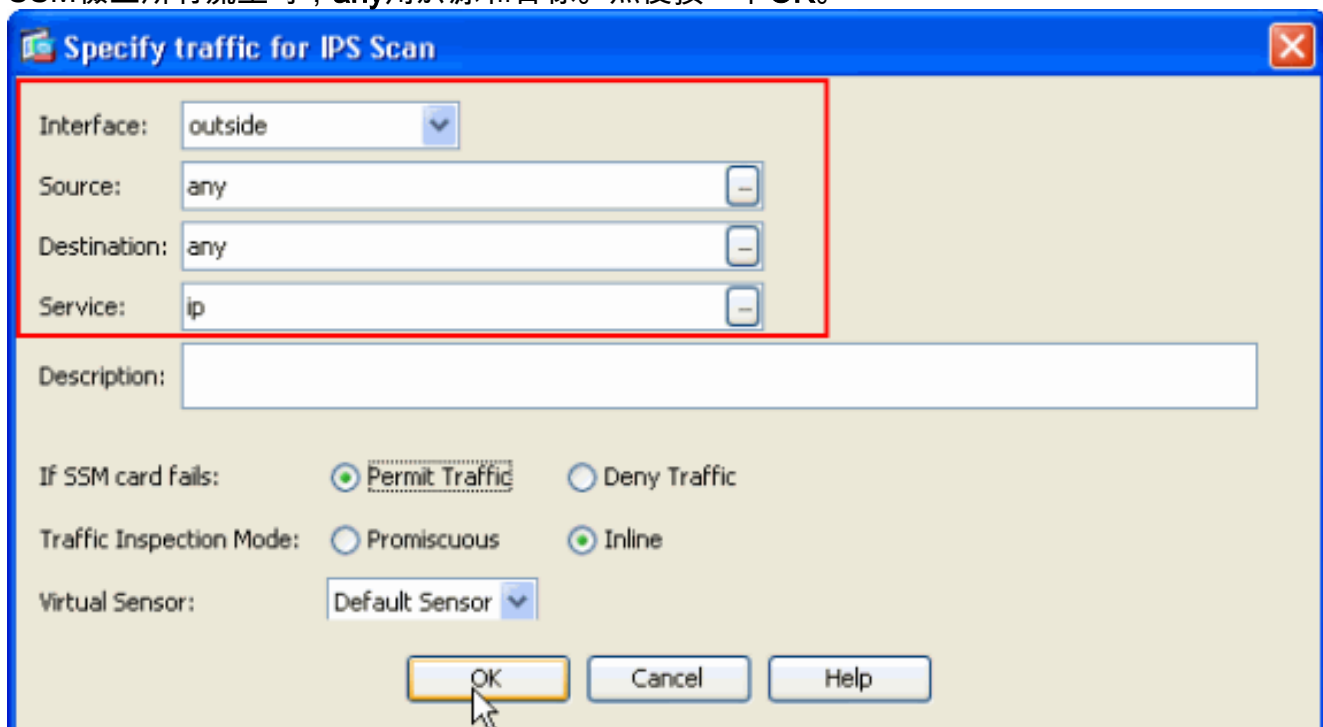
6. 在提供的相應空白處提供詳細資訊後，按一下下一步。



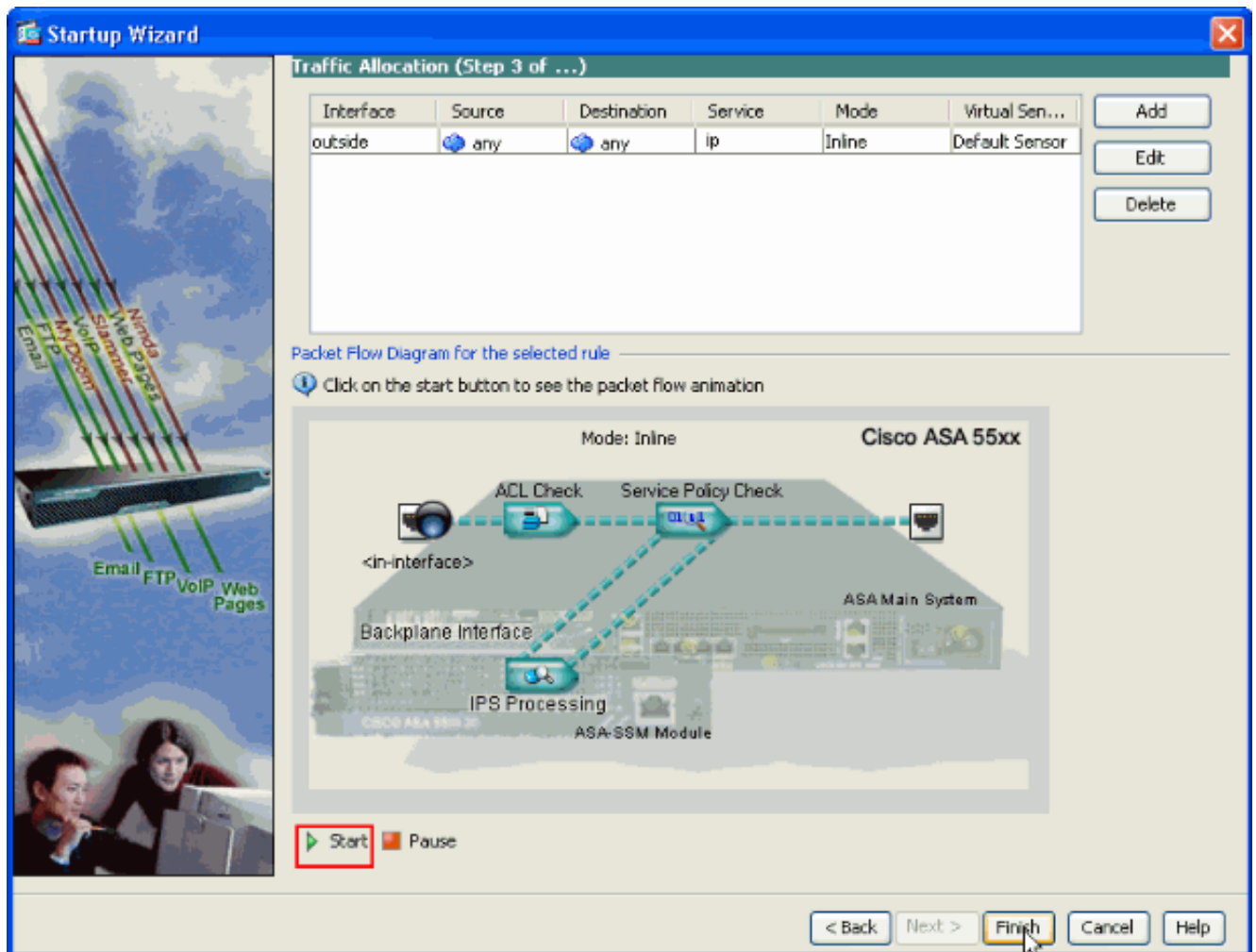
7. 按一下Add以設定流量分配詳細資訊。



8. 請提供來源和目的地網路位址以及服務型別，例如此處使用IP。在本示例中，當您使用AIP-SSM檢查所有流量時，any用於源和目標。然後按一下OK。



9. 已配置的流量分配規則將顯示在此視窗中，如果您完成了步驟7和8中所述的相同過程，可以根據需要新增多個規則。然後按一下完成，即可完成ASDM配置過程。注意：如果按一下Start（開始），可以檢視資料包流動畫。



使用AIP-SSM檢查特定流量

如果網路管理員希望將AIP-SSM監控器作為所有流量的子集，則ASA有兩個可以修改的獨立變數。首先，可以寫入存取清單以包含或排除所需的流量。除了修改訪問清單外，還可以將**service-policy**應用於介面或全域性來更改AIP-SSM檢查的流量。

參照本檔案的[網路圖表](#)，網路管理員希望AIP-SSM檢查外部網路和DMZ網路之間的所有流量。

```

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.

```

接下來，網路管理員希望AIP-SSM監控從內部網路發起到外部網路的流量。內部網路到DMZ網路不

受監控。

注意：此特定部分要求對狀態性、TCP、UDP、ICMP、連線和無連線通訊有中等程度的瞭解。

```
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
```

存取清單會拒絕在內部網路中發起且目的地為DMZ網路的流量。第二條訪問清單行允許或傳送從內部網路發起、目的地為外部網路的流量到AIP-SSM。此時，ASA的狀態性開始發揮作用。例如，內部使用者發起到外部網路（路由器）上裝置的TCP連線(Telnet)。使用者已成功連線到路由器並登入。然後使用者發出未經授權的路由器命令。路由器響應命令。包含Command authorization failed字串的資料包具有外部路由器的源和內部使用者的目標。來源（外部）和目的地（內部）與本檔案先前定義的存取清單不相符。ASA會跟蹤有狀態連線，因此，返回的資料包（從外部到內部）將傳送到AIP-SSM以供檢查。在AIP60000SSM上配置的自定義特徵碼0會發出警報。

注意：預設情況下，ASA不保留ICMP流量的狀態。在先前的範例組態中，內部使用者ping（ICMP回應請求）外部路由器。路由器使用ICMP echo-reply做出響應。AIP-SSM會檢查回應要求封包，但不會檢查回應要求封包。如果在ASA上啟用ICMP檢測，AIP-SSM會同時檢查回應請求和回應回複資料包。

[從AIP-SSM掃描中排除特定網路流量](#)

給定的通用示例提供了免除AIP-SSM要掃描的特定流量的檢視。為此，您需要建立一個訪問清單，該清單包含要在deny語句中從AIP-SSM掃描中排除的流量。在本示例中，IPS是定義要由AIP-SSM掃描的通訊流的訪問清單的名稱。<source>和<destination>之間的流量不會進行掃描；會檢查所有其他流量。

```
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
```

[驗證](#)

驗證警報事件是否記錄在AIP-SSM中。

使用管理員使用者帳戶登入AIP-SSM。**show events alert**命令將生成此輸出。

注意：輸出根據特徵碼設定、傳送到AIP-SSM的流量型別以及網路負載而變化。

[輸出直譯器工具\(僅供已註冊客戶使用\)\(OIT\)](#)支援某些show命令。使用OIT檢視show指令輸出的分析

o

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

```

在示例配置中，對多個IPS特徵碼進行調整以針對測試流量發出警報。對2000和2004簽名進行了修改。新增了自60000簽名屬性。在實驗室環境或幾乎沒有資料通過ASA的網路中，可能需要修改特徵碼以觸發事件。如果ASA和AIP-SSM部署在傳遞大量流量的環境中，則預設簽名設定可能會生成事件。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show指令輸出的分析。

從ASA發出以下show命令。

- **show module** — 顯示有關ASA上的SSM的資訊以及系統資訊。

```

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** — 顯示存取清單的計數器。

```
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.
```

在安裝並使用AIP-SSM之前，網路流量是否按預期通過ASA?否則，可能需要排除網路和ASA訪問策略規則的故障。

故障切換問題

- 如果您有兩個ASA處於故障切換配置中，並且每個都有一個AIP-SSM，則必須手動複製AIP-SSM的配置。故障切換機制只複製ASA的配置。故障切換中不包括AIP-SSM。有關故障切換問題的詳細資訊，請參閱[PIX/ASA 7.x主用/備用故障切換配置示例](#)。
- 如果在ASA故障切換對上配置了狀態故障切換，則AIP-SSM不會參與狀態故障切換。

錯誤消息

IPS模組(AIP-SSM)會生成如圖所示的錯誤消息，而不是激發事件。

```
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.
```

此錯誤消息的原因是IPS虛擬感測器未分配給ASA的背板介面。ASA的設定方式正確，以便將通訊量傳送到SSM模組，但您需要將虛擬感測器分配給ASA建立的背板介面，以便SSM掃描通訊量。

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

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

這些消息表示啟用了IP日誌記錄，從而佔用了所有系統資源。Cisco建議禁用IP日誌記錄，因為它只應用於故障排除/調查目的。

註：當感測器在特徵碼更新（特徵碼更新過程的一個必要部分）後立即重新啟動分析引擎時，errWarning Inline data bypass has started錯誤消息是預期行為。

Syslog 支援

AIP-SSM不支援將系統日誌作為警報格式。

從AIP-SSM接收警報資訊的預設方法是通過安全裝置事件交換(SDEE)。另一種方法是配置各個特徵碼，以生成SNMP陷阱，作為觸發時採取的操作。

[AIP-SSM重新引導](#)

AIP-SSM模組未正確響應。

如果AIP-SSM模組未正確響應，則重新啟動AIP-SSM模組而不重新啟動ASA。使用[hw-module module 1 reload](#) 命令重新啟動AIP-SSM模組並且不重新啟動ASA。

[AIP-SSM電子郵件警報](#)

AIP-SSM能否向使用者傳送電子郵件警報？

不支援。

[相關資訊](#)

- [思科安全裝置命令參考7.2版](#)
- [思科安全裝置系統日誌消息版本7.2](#)
- [思科入侵防禦系統5.1的命令參考](#)
- [技術支援與文件 - Cisco Systems](#)