ASA: إرسال حركة مرور الشبكة من ASA إلى AIP SSM مثال تكوين

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين كيفية إرسال حركة مرور الشبكة التي تمر عبر جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco ASA 5500 Series إلى وحدة خدمات الأمان والفحص والمنع المتقدم (IPS) (AIP-SSM) النمطية. يتم توفير أمثلة التكوين مع واجهة سطر الأوامر (CLI).

ارجع إلى ASA: إرسال حركة مرور الشبكة من ASA إلى مثال تكوين CSC-SSM لإرسال حركة مرور بيانات الشبكة من جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco ASA 5500 Series إلى الوحدة النمطية Content Security and Control Security Services Module (CSC-SSM).

راجع تعيين أجهزة الاستشعار الظاهرية لسياق أمان (AIP SSM فقط) للحصول على مزيد من المعلومات حول كيفية إرسال حركة مرور الشبكة التي تمر عبر جهاز الأمان القابل للتكيف (ASA 5500 Series) من Cisco ASA في وضع سياق متعدد إلى وحدة خدمات الأمان والفحص والمنع المتقدم (IPS) (AIP-SSM) النمطية.

ملاحظة: تتضمن حركة مرور الشبكة التي تجتاز ASA المستخدمين الداخليين الذين يصلون إلى الإنترنت أو مستخدمي الإنترنت الذين يصلون إلى الموارد المحمية بواسطة ASA في منطقة منزوعة السلاح (DMZ) أو داخل الشبكة. لا يتم إرسال حركة مرور الشبكة التي يتم إرسالها إلى وحدة ASA ومنها إلى وحدة IPS للتفتيش. يتضمن مثال حركة المرور

التي لم يتم إرسالها إلى وحدة IPS النمطية إدخال (ICMP) واجهات ASA أو إنشاء شبكة telnet إلى ASA.

ملاحظة: لا يدعم إطار السياسات النمطي الذي يستخدمه مكتب الدعم التقني من أجل تصنيف حركة مرور البيانات للتفتيش IPv6. لذلك إذا قمت بتحويل حركة مرور IPv6 إلى AIP SSM من خلال ASA، فإنها غير مدعومة.

ملاحظة: للحصول على مزيد من المعلومات حول التكوين الأولي لدليل AIP-SSM، ارجع إلى التكوين الأولي لمستشعر AIP-SSM.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن الجمهور لديه فهم أساسي لكيفية تكوين برنامج Cisco ASA الإصدار x.8 و IPS Software الإصدار x.6.

- تتضمن مكونات التكوين الضرورية ل ASA 8.x الواجهات وقوائم الوصول وترجمة عنوان الشبكة (NAT) والتوجيه.
- تتضمن مكونات التكوين الضرورية لبروتوكول AIP-SSM (برنامج IPS 6.x) إعداد الشبكة والأجهزة المضيفة المسموح بها وتكوين الواجهة وتعريفات التوقيع وقواعد إجراء الحدث.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA 5510 مع برنامج صيغة 8.0.2
- AIP-SSM-10 مع برنامج IPS نسخة 6.1.2

ملاحظة: يتوافق مثال التكوين هذا مع أي جدار حماية من سلسلة Cisco ASA 5500 مع نظام التشغيل x.7 والإصدارات الأحدث ووحدة AIP-SSM النمطية مع IPS 5.x والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

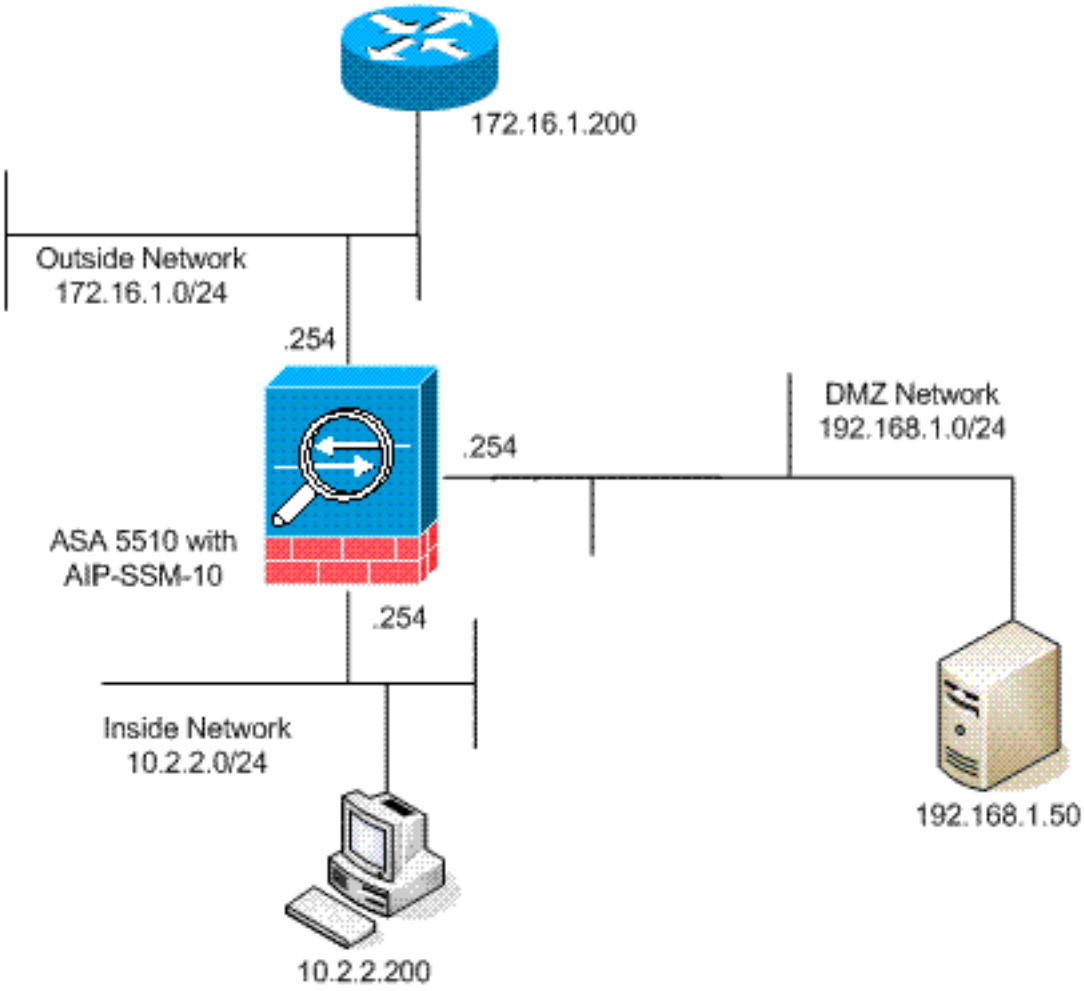
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

مخططات عنونة IP المستخدمة في هذا التكوين غير قابلة للتوجيه من الناحية القانونية على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



عمليات التهيئة الأولية

يستخدم هذا المستند هذه التكوينات. يبدأ كلا من ASA و AIP-SSM بتكوين افتراضي ولكن له تغييرات محددة تم إجراؤها لأغراض الاختبار. وتتم ملاحظة الإضافات في التكوين.

- 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
```

SSM دليل IPS (AIP)

```
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 ! --------
---------------------- service ssh-known-hosts exit ! --
           ---------------------------- service trusted-
      certificates exit ! ------------------------------
        #service web-server enable-tls true exit AIP-SSM
```

ملاحظة: إذا لم تكن قادرا على الوصول إلى وحدة AIP-SSM النمطية باستخدام HTTPS، فأكمل الخطوات التالية:

- قم بتكوين عنوان IP للإدارة للوحدة النمطية. ويمكنك تكوين ، والتي تحدد فيها شبكات IP/IP المسموح لها بالاتصال ب IP الخاص بالإدارة.
- تأكد من توصيل واجهة إيثرنت الخارجية لوحدة AIP النمطية. وصول الإدارة إلى وحدة AIP النمطية ممكن من خلال هذه الواجهة فقط.

راجع تهيئة AIP-SSM للحصول على مزيد من المعلومات.

افحص جميع حركات المرور باستخدام AIP-SSM في الوضع المضمن أو المختلط

غالبا ما يشير مسؤولو الشبكة وكبار مسؤولي الشركة إلى أن كل شيء يحتاج إلى المراقبة. تفي هذه التهيئة بمتطلبات مراقبة كل شيء. وبالإضافة إلى رصد كل شيء، لا بد من إتخاذ قرارين بشأن كيفية التفاعل بين وكالة الفضاء الأوروبية ومعهد الطيران الدولي - إدارة المواد الصلبة.

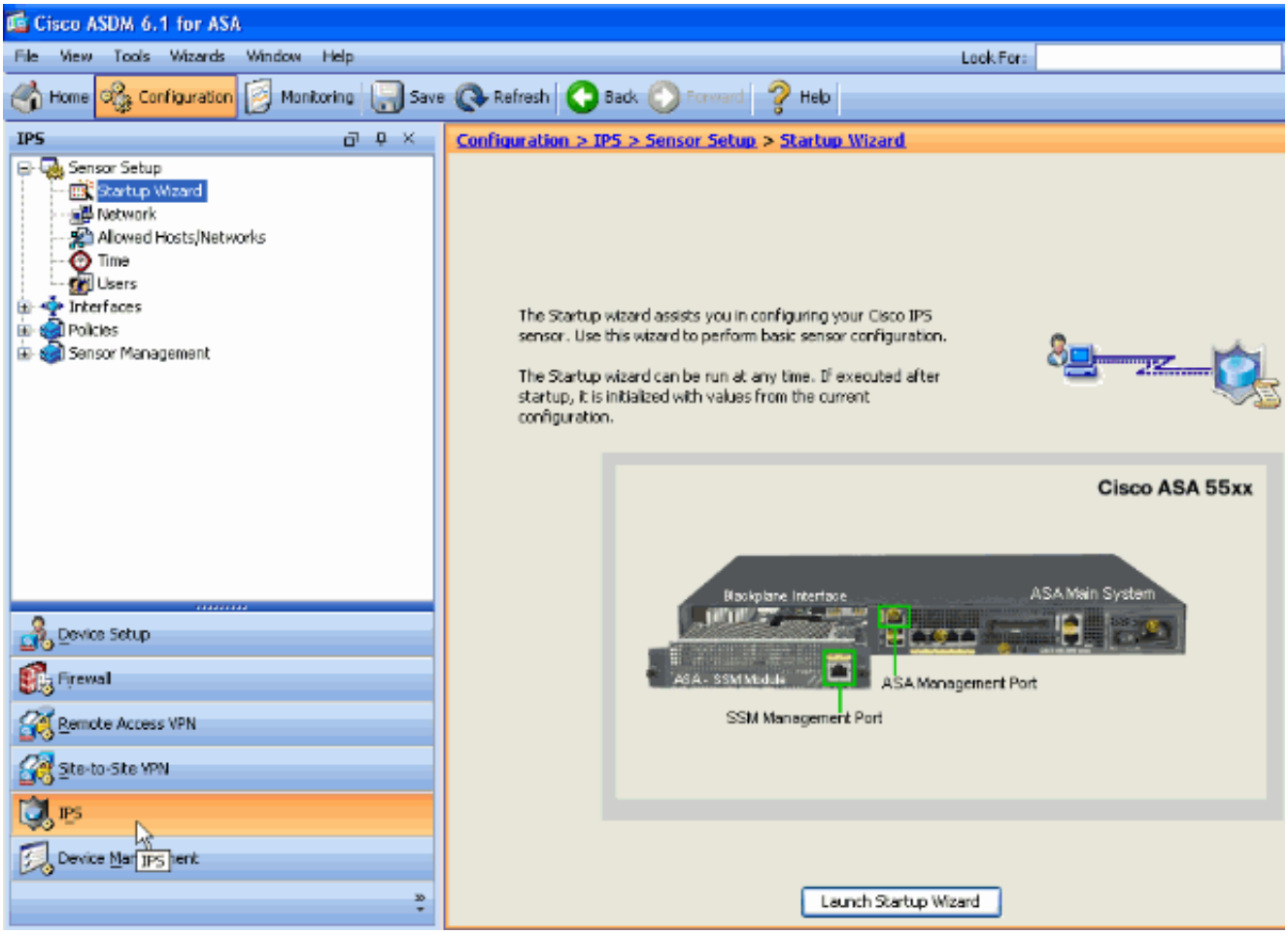
- هل تعمل وحدة AIP-SSM النمطية أو يتم نشرها في الوضع المختلط أو المضمن؟الوضع المختلط يعني أن نسخة من البيانات يتم إرسالها إلى AIP-SSM بينما يقوم ASA بإعادة توجيه البيانات الأصلية إلى الوجهة. يمكن إعتبار AIP-SSM في الوضع المختلطة نظام كشف التسلل (IDS). في هذا أسلوب، المشغل ربط (الربط أن يسبب التنبيه) يستطيع بعد وصلت الغاية. يمكن أن يحدث التجنب ويوقف الحزم الإضافية من الوصول إلى الوجهة، ومع ذلك لا يتم إيقاف حزمة المشغل.الوضع المضمن يعني أن ASA يرسل البيانات إلى AIP-SSM للفحص. إذا مرت البيانات بفحص AIP-SSM، ترجع البيانات إلى ASA للاستمرار في معالجتها وإرسالها إلى الوجهة. يمكن إعتبار AIP-SSM في الوضع المضمن كنظام لمنع الاقتحام (IPS). على عكس الوضع المختلطة، يمكن للوضع المضمن (IPS) إيقاف حزمة المشغل فعليا من الوصول إلى الوجهة.
- في حالة عدم قدرة ASA على الاتصال ب AIP-SSM، كيف يجب أن يعالج ASA حركة المرور التي يتم فحصها؟ وتتضمن أمثلة الحالات التي لا يتمكن فيها مساعد الأمين العام من الاتصال بمعالج AIP-SSM عمليات إعادة تحميل AIP-SSM أو إذا فشلت الوحدة النمطية وكانت بحاجة إلى إستبدال. في هذه الحالة، يمكن أن يفشل ASA في الفتح أو أن يقفل.يسمح فتح الفشل ل ASA أن يستمر أن يمر أن يكون فحصت حركة مرور إلى الغاية النهائية إن ال AIP-SSM يستطيع لا يكون بلغت.كتل معطلة بحيث يتم فحصها حركة المرور عندما لا يتمكن ASA من الاتصال ب AIP-SSM.**ملاحظة:** يتم تحديد حركة المرور التي سيتم فحصها باستخدام قائمة وصول. في هذا المثال الإخراج، تسمح قائمة الوصول لجميع حركة مرور IP من أي مصدر إلى أي وجهة. وبالتالي، فإن حركة المرور التي سيتم فحصها يمكن أن تكون أي شيء يمر عبر ASA.

```
ciscoasa(config)#access-list traffic_for_ips permit ip any any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
The match any command can be used in place of !--- the match access-list [access-list name] ---!
 command. !--- In this example, access-list traffic_for_ips permits !--- all traffic. The match
    any command also !--- permits all traffic. You can use either configuration. !--- When you
                                                .define an access-list, it can ease troubleshooting

                                                ciscoasa(config)#policy-map global_policy
     Note that policy-map global_policy is a part of the !--- default configuration. In ---!
.addition, policy-map global_policy !--- is applied globally with the service-policy command

                                                ciscoasa(config-pmap)#class ips_class_map
                                              ciscoasa(config-pmap-c)#ips inline fail-open
  Two decisions need to be made. !--- First, does the AIP-SSM function !--- in inline or ---!
promiscuous mode? !--- Second, does the ASA fail-open or fail-closed? ciscoasa(config-pmap-
                                                                                  c)#ips promiscous fail-open
If AIP-SSM is in promiscous mode, issue !--- the no ips promiscous fail-open command !--- ---!
                                              .in order to negate the command and then use !--- the ips inline fail-open command
```

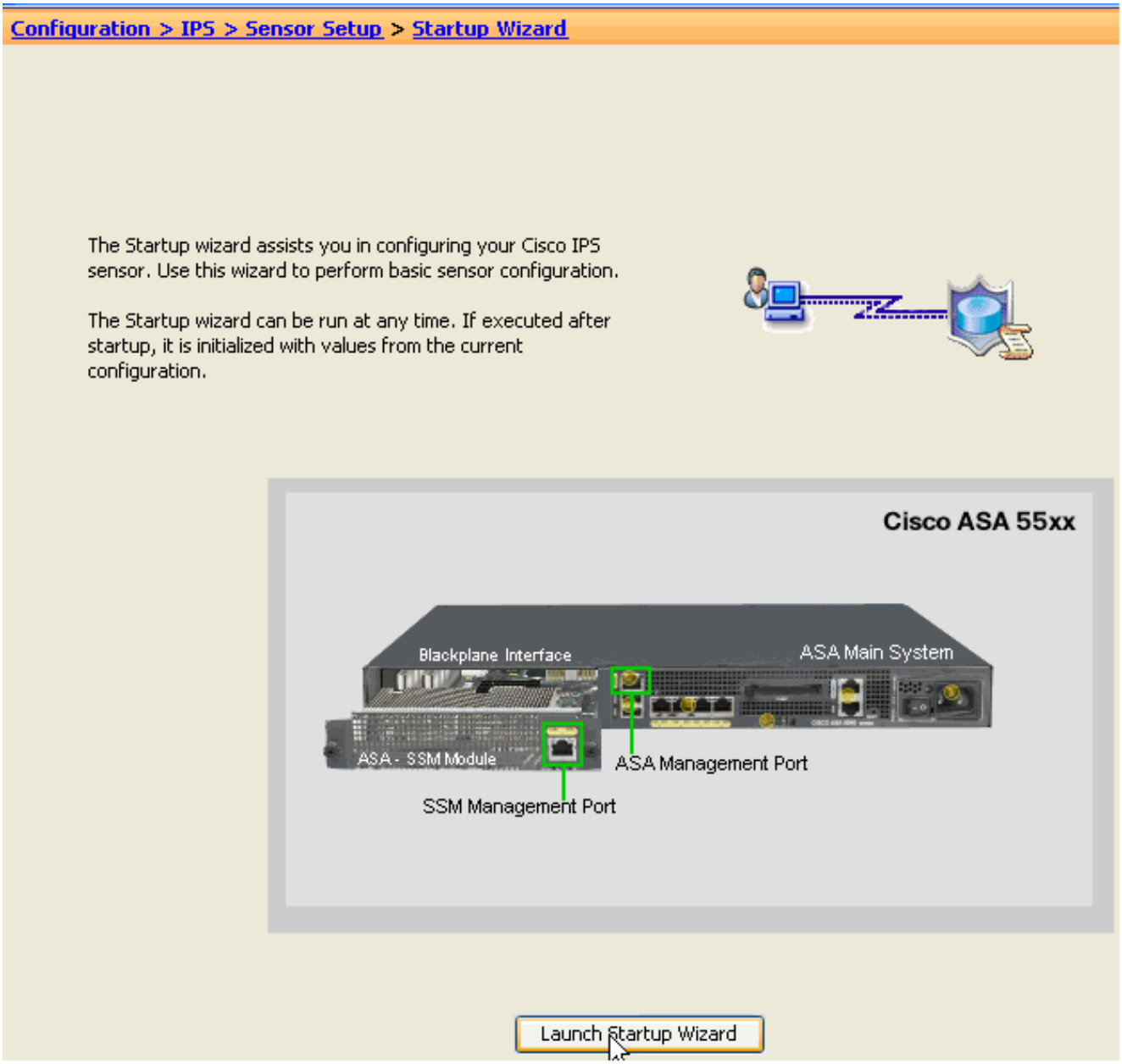
افحص كل حركة المرور باستخدام AIP-SSM باستخدام ASDM

أتمت هذا steps in order to فحصت كل حركة مرور مع AIP-SSM أن يستعمل ASDM:.

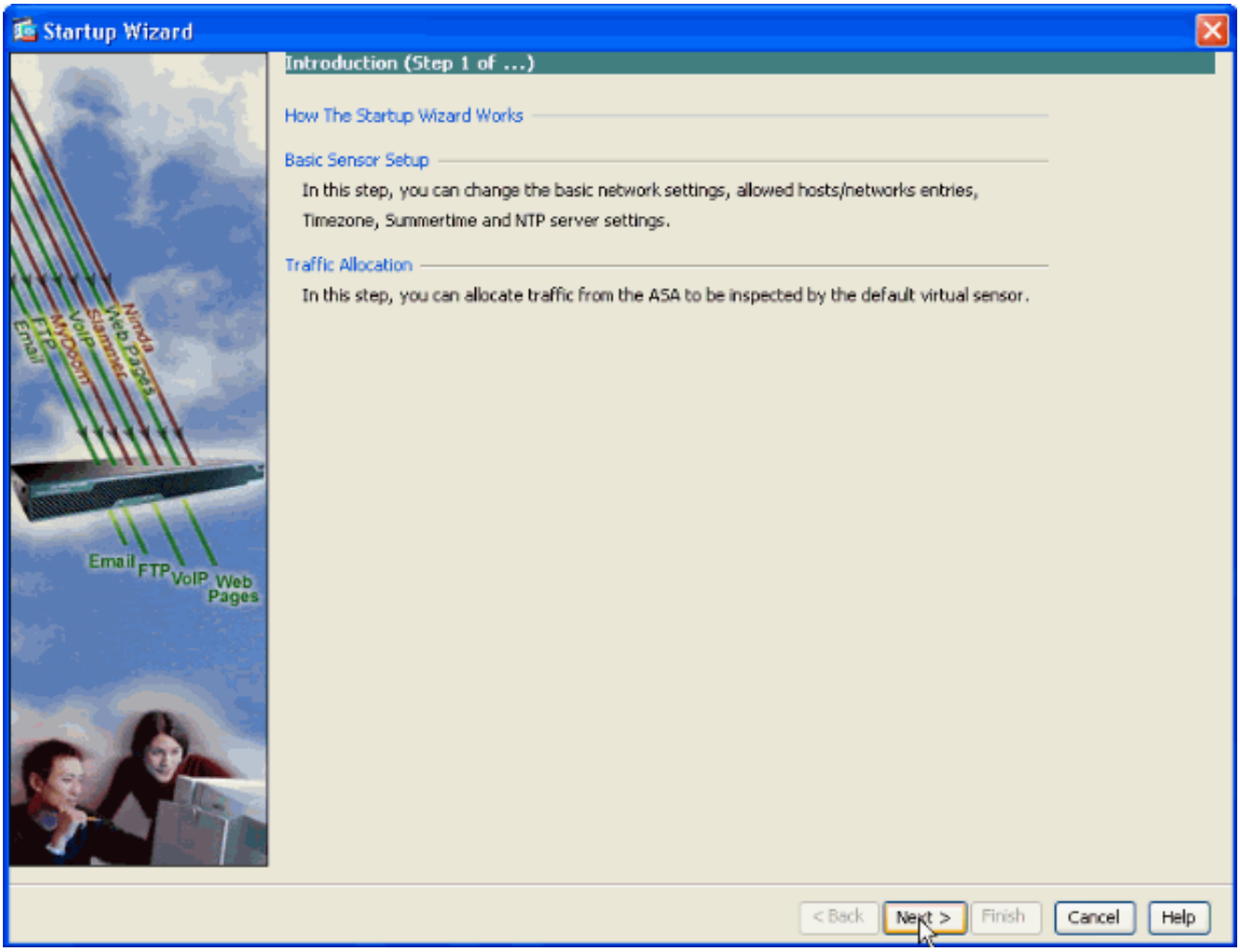
1. أختر **التكوين > IPS > إعداد المستشعر > معالج بدء التشغيل** في الصفحة الرئيسية ASDM لبدء التكوين، كما هو
موضح:



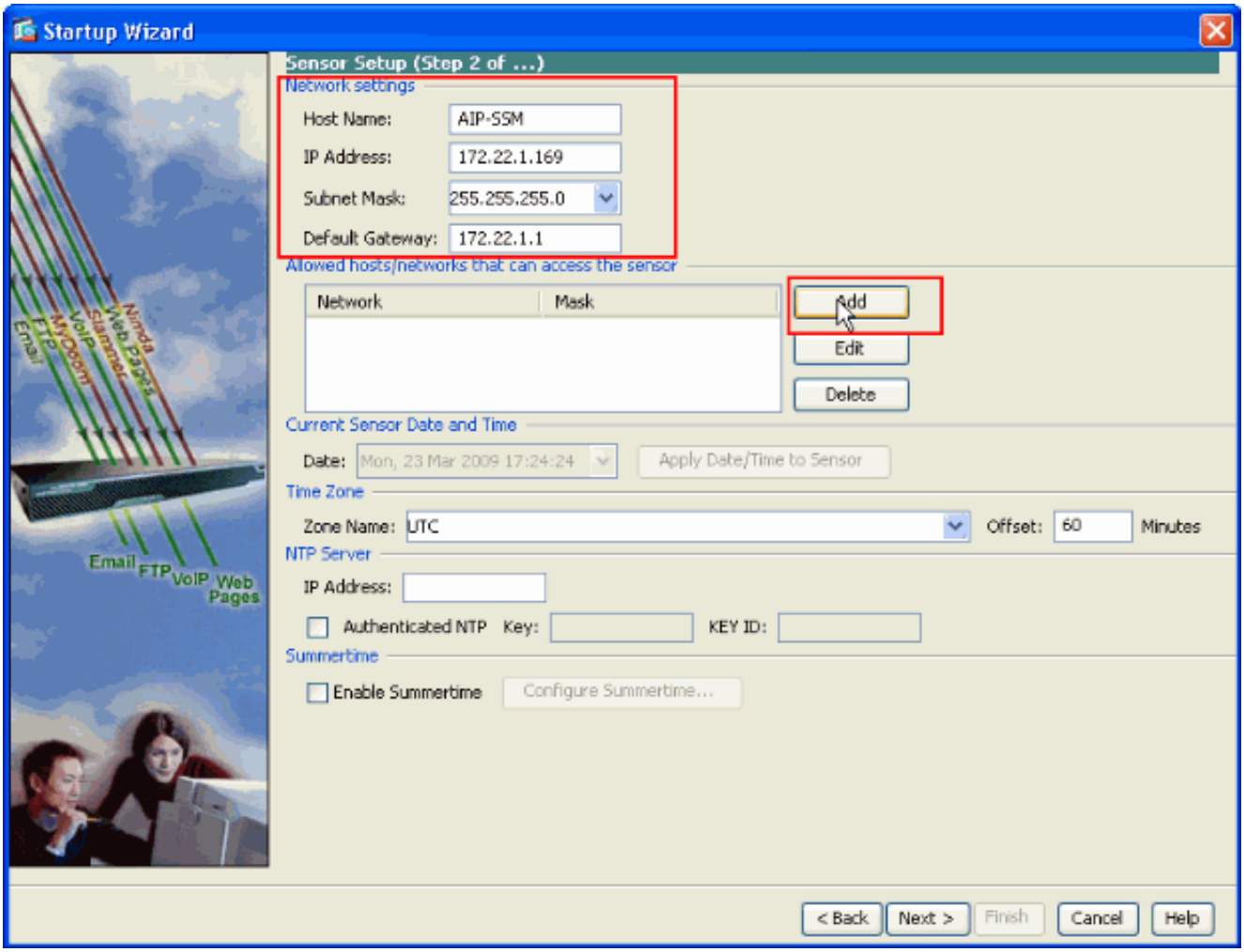
2. انقر على **معالج بدء التشغيل**.



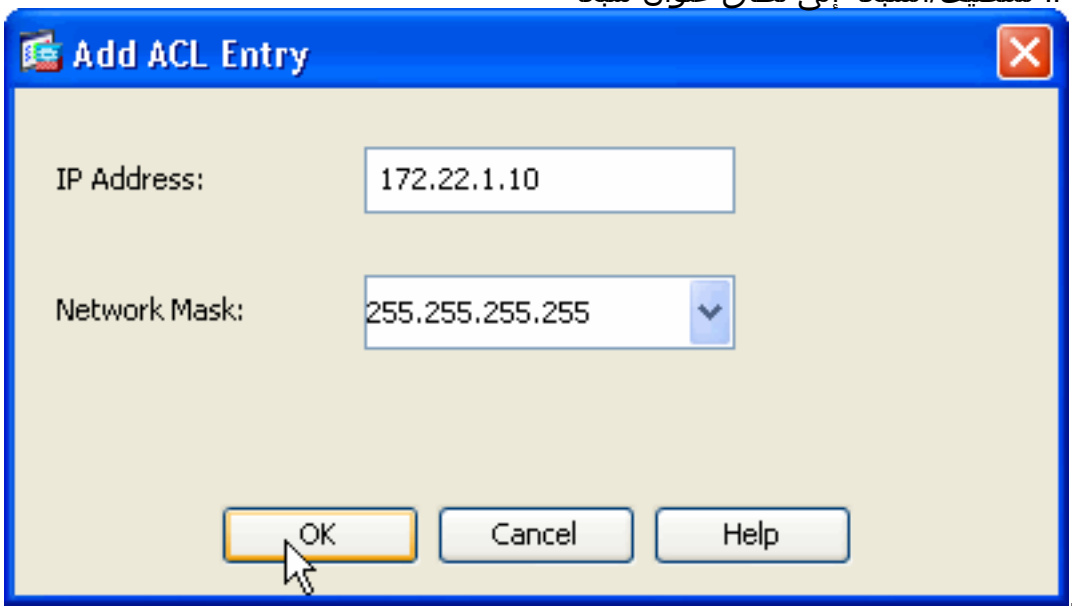
3. انقر فوق **التالي** في الإطار الجديد الذي يظهر بعد تشغيل معالج بدء التشغيل.



4. في النافذة الجديدة، قم بتوفير اسم المضيف وعنوان IP وقناع الشبكة الفرعية وعنوان العبارة الافتراضي لوحدة AIP-SSM النمطية في المساحة المقابلة المتوفرة ضمن قسم إعدادات الشبكة. ثم انقر فوق **إضافة** لإضافة قوائم الوصول للسماح لكل حركة المرور باستخدام AIP-SSM.

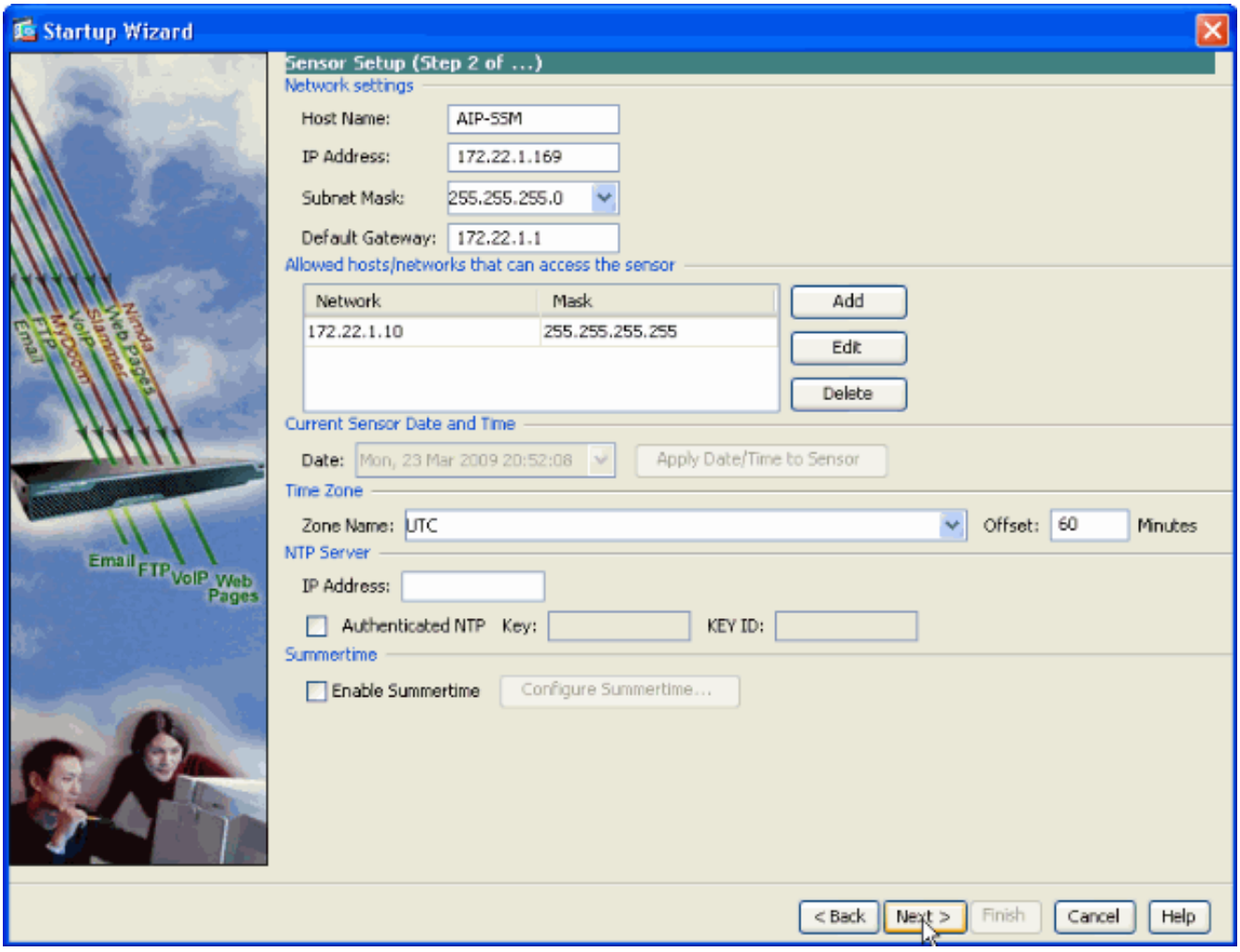


5. في نافذة **إضافة إدخال قائمة التحكم في الوصول (ACL)** ، يوفر **عنوان IP** وتفاصيل **قناع الشبكة** للمضيفين/الشبكات التي سيتم السماح لها بالوصول إلى المستشعر. وانقر فوق OK.**ملاحظة:** يجب أن ينتمي عنوان IP للمضيف/الشبكة إلى نطاق عنوان شبكة

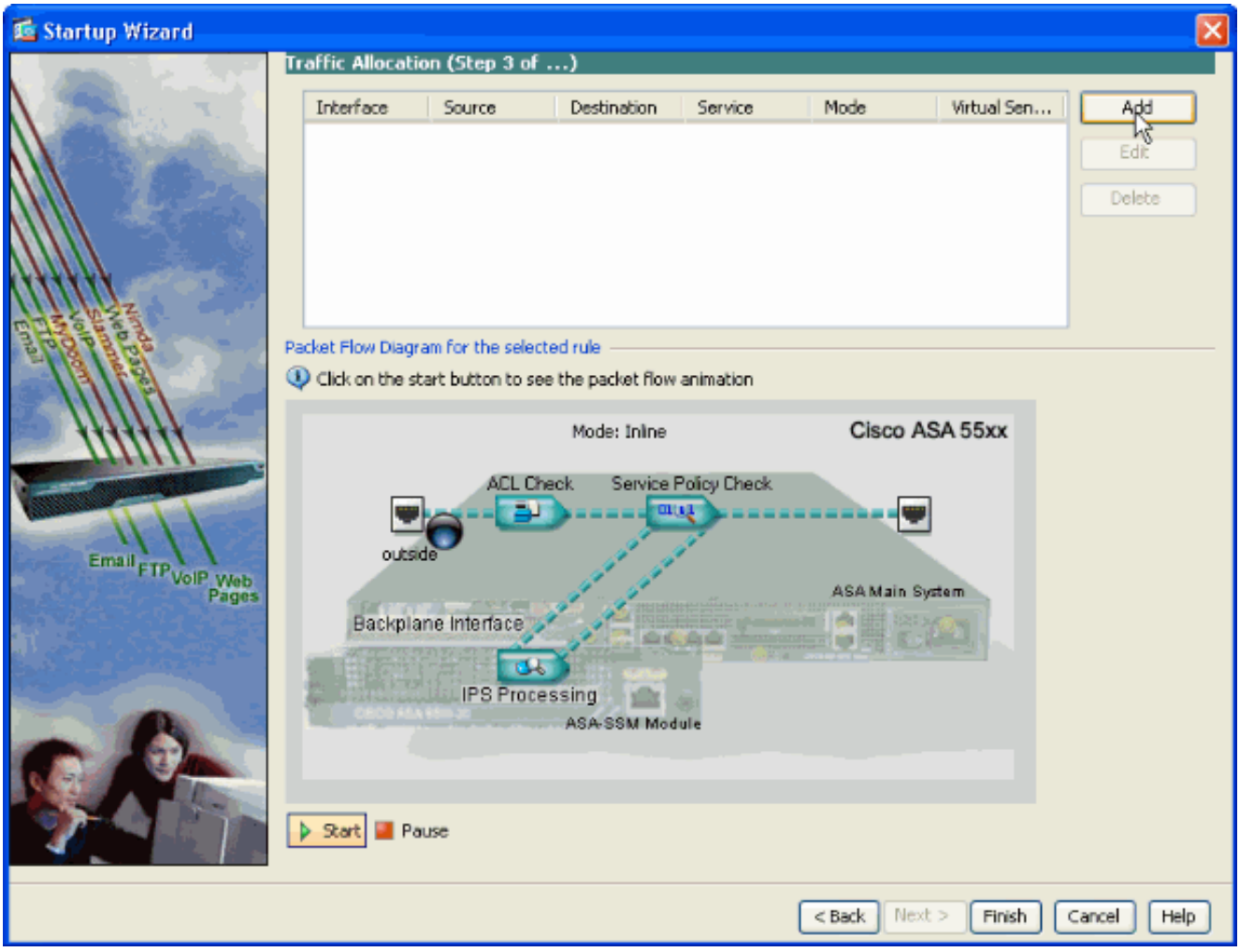


الإدارة.

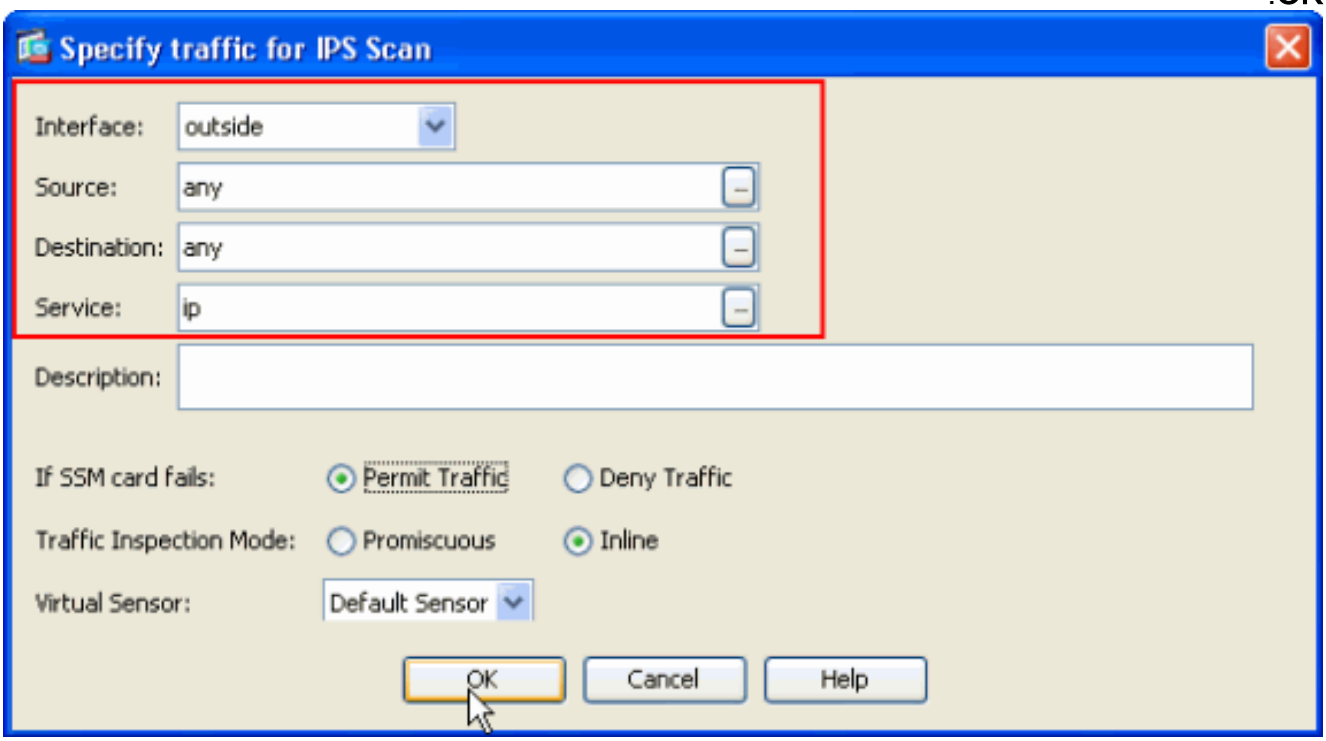
6. طقطقت **بعد ذلك** بعد أن يزود أنت التفاصيل في فراغات الشخصي يزود.



7. انقر فوق **إضافة** لتكوين تفاصيل توزيع حركة المرور.

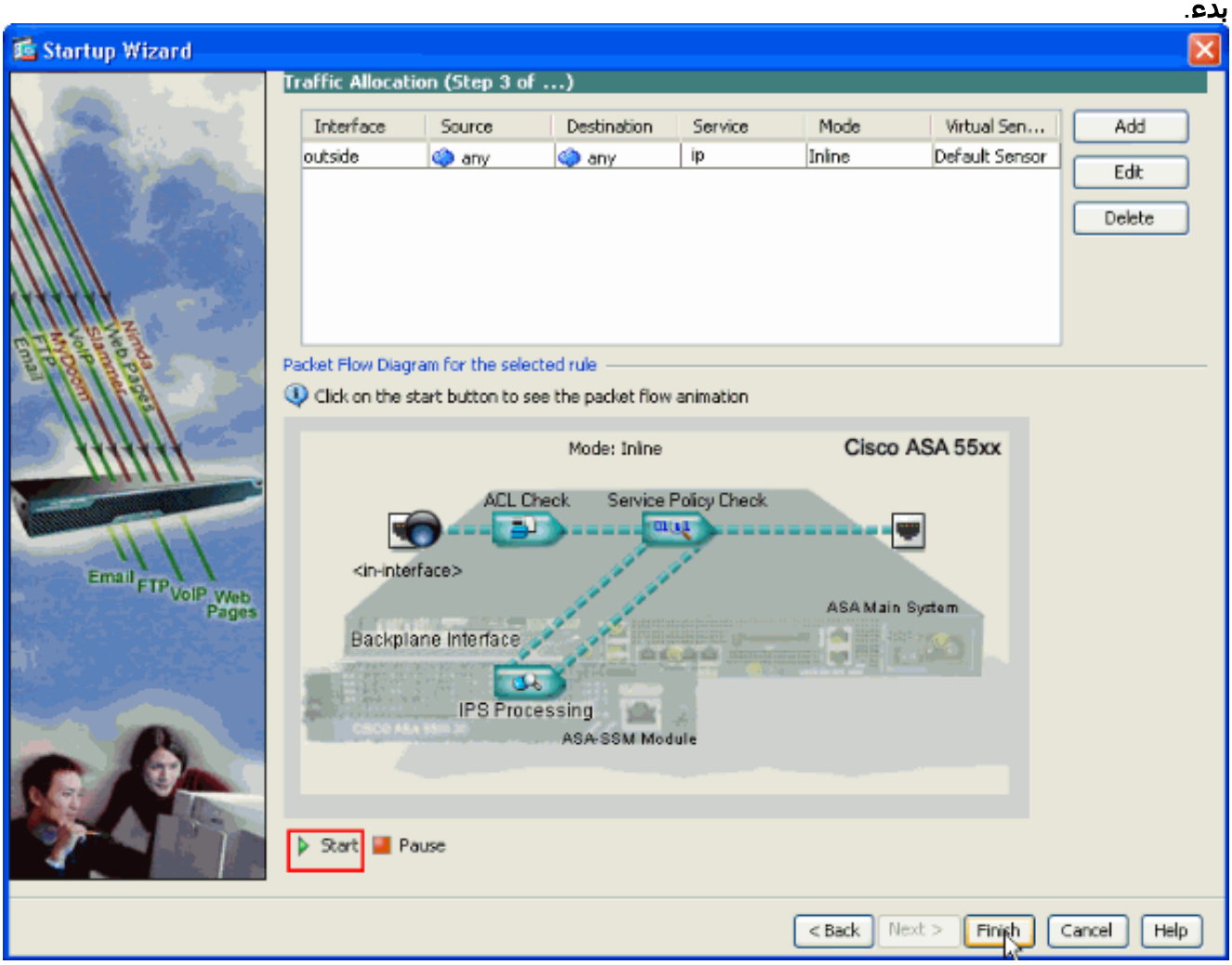


8. توفر عنوان الشبكة المصدر والوجهة ونوع الخدمة أيضا، على سبيل المثال، يتم إستخدام IP هنا. في هذا المثال، يتم إستخدام **أي** من أجل المصدر والوجهة بينما تقوم بفحص كل حركة المرور باستخدام AIP-SSM. ثم انقر فوق
.**OK**



9. يتم عرض قواعد تخصيص حركة المرور التي تم تكوينها في هذا الإطار ويمكنك إضافة العديد من القواعد حسب الحاجة إذا قمت بإكمال الإجراء نفسه كما هو موضح في الخطوات 7 و 8. ثم انقر فوق **إنهاء** ويؤدي هذا إلى اكتمال إجراء تكوين ASDM.**ملاحظة:** يمكنك عرض الرسم المتحرك لتدفق الحزمة إذا قمت بالنقر على

بدء.



افحص حركة مرور معينة باستخدام AIP-SSM

إذا كان مسؤول الشبكة يريد أن يتلقى ال AIP-SSM مدرب كمجموعة فرعية من كل حركة مرور، ال ASA يتلقى إثنان متغير مستقل أن يستطيع كنت عدلت. أولا، يمكن كتابة قائمة الوصول لتضمين حركة المرور الضرورية أو إستبعادها. وبالإضافة إلى تعديل قوائم الوصول، يمكن تطبيق **سياسة الخدمة** على واجهة أو بشكل عام لتغيير حركة المرور التي تم فحصها بواسطة AIP-SSM.

بالإشارة إلى الرسم التخطيطي للشبكة في هذا المستند، يريد مسؤول الشبكة أن يقوم AIP-SSM بفحص *كل* حركة المرور بين الشبكة الخارجية وشبكة DMZ.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip any 192.168.1.0 255.255.255.0
ciscoasa(config)#access-list traffic_for_ips deny ip 192.168.1.0 255.255.255.0 10.2.2.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 192.168.1.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface dmz
The access-list denies traffic from the inside network to the DMZ network !--- and traffic ---!
to the inside network from the DMZ network. !--- In addition, the service-policy command is
.applied to the DMZ interface
```

بعد ذلك، يريد مدير الشبكة AIP-SSM أن يراقب حركة مرور *يبدأ* من الشبكة الداخلية إلى الشبكة الخارجية. لا تتم مراقبة الشبكة الداخلية لشبكة DMZ.

ملاحظة: يتطلب هذا القسم تحديدا فهما متوسط المستوى لصلاحية الاتصال و TCP و UDP و ICMP والاتصال والاتصالات غير المتصلة.

```
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
```

ترفض قائمة الوصول حركة المرور التي تم بدؤها على الشبكة الداخلية الموجهة لشبكة DMZ. بينما يسمح خط قائمة الوصول الثاني لحركة مرور البيانات التي تبدأ على الشبكة الداخلية الموجهة للشبكة الخارجية أو يرسلها إلى AIP-SSM. وعند هذه النقطة، تلعب قيمة ال ASA دورا في ذلك. على سبيل المثال، يقوم مستخدم داخلي بتهيئة اتصال TCP (Telnet)) إلى جهاز على الشبكة الخارجية (الموجه). نجح المستخدم في الاتصال بالموجه وتسجيل الدخول. يصدر المستخدم بعد ذلك أمر موجه غير مصرح به. يستجيب الموجه مع . تحتوي حزمة البيانات التي تحتوي على سلسلة على مصدر للموجه الخارجي ووجهة للمستخدم الداخلي. لا يتطابق المصدر (الخارجي) والوجهة (في الداخل) مع قوائم الوصول المحددة مسبقا في هذا المستند. يتتبع ASA الاتصالات المعبرة، ولهذا السبب، يتم إرسال حزمة البيانات التي ترجع (من الخارج إلى الداخل) إلى AIP-SSM للفحص. التوقيع المخصص 60000 0، الذي تم تكوينه على AIP-SSM، تنبيهات.

ملاحظة: لا يحتفظ ASA بشكل افتراضي بالحالة لحركة مرور ICMP. في تكوين العينة السابق، يقوم المستخدم الداخلي بتجارب (طلب صدى ICMP) للموجه الخارجي. يستجيب الموجه باستخدام ICMP Echo-response. يفحص AIP-SSM حزمة طلب echo ولكنه لا يفحص حزمة صدى-رد. إذا تم تمكين فحص ICMP على ASA، يتم فحص كل من طلب echo وحزم echo-reply بواسطة AIP-SSM.

إستبعاد حركة مرور شبكة معينة من مسح AIP-SSM الضوئي

يقدم المثال المعمم المعطى رأيا بشأن إعفاء حركة مرور معينة يتعين مسحها ضوئيا بواسطة AIP-SSM. ولإجراء ذلك، يلزمك إنشاء قائمة وصول تحتوي على تدفق حركة المرور الذي سيتم إستبعاده من الفحص AIP-SSM في عبارة الرفض. في هذا المثال، IPS هو اسم قائمة الوصول التي تحدد تدفق حركة المرور الذي سيتم مسحه بواسطة AIP-SSM. يتم إستبعاد حركة المرور بين <source> و<destination> من المسح الضوئي، ويتم فحص جميع حركات المرور الأخرى.

```
<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
```

التحقق من الصحة

تحقق من تسجيل أحداث التنبيه في AIP-SSM.

قم بتسجيل الدخول إلى AIP-SSM باستخدام حساب مستخدم المسؤول. يقوم الأمر **show events alert** بإنشاء هذا الإخراج.

ملاحظة: يختلف المخرج بناء على إعدادات التوقيع، ونوع حركة المرور المرسلة إلى AIP-SSM، وتحميل الشبكة.

تدعم [أداة مترجم الإخراج (للعملاءالمسجلين فقط)](#) بعض أوامر **show**. استعملت الـ OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

```
                                                                    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
                        .C7 9F 74 8C 00 15  2B 95 F9 5E 08 00 45 00  ....t...+..^..E 16 00  000000
                        .......!....3C 2A 57 00 00 FF 01  21 B7 AC 10 01 C8 C0 A8  .<*W 00  000010
                        ........$.....F5 DA 11 24  00 00 00 01 02 03 04 05  .2 00 08 32 01  000020
                        ................  0A 0B 0C 0D  0E 0F 10 11 12 13 14 15 09 08 07 06  000030
                              ..........                  1A 1B 1C 1D  1E 1F 19 18 17 16  000040
                                                                    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
.C7 9F 74 8E 00 03  E3 02 6A 21 08 00 45 00  ....t.....j!..E 16 00  000000
..3C 2A 57 00 00 FF 01  36 4F AC 10 01 32 AC 10  .<*W....6O...2 00  000010
........$.......  C8 00 00 FD DA 11 24  00 00 00 01 02 03 04 05 01  000020
................  0A 0B 0C 0D  0E 0F 10 11 12 13 14 15 09 08 07 06  000030
      ..........                    1A 1B 1C 1D  1E 1F 19 18 17 16  000040
                                                 riskRatingValue: 100
                                                  interface: ge0_1
                                                   protocol: icmp
```

في التكوينات العينة، يتم ضبط العديد من توقيعات IPS للتنبيه عند حركة مرور الاختبار. تم تعديل التوقيع 2000 و 2004. يتم إضافة التوقيع المخصص 60000. في بيئة معملية أو شبكة حيث تمر بيانات قليلة عبر ال ASA، يمكن أن يكون من الضروري تعديل التوقيعات من أجل تشغيل الأحداث. إذا تم نشر ASA و AIP-SSM في بيئة تجتاز كمية كبيرة من حركة المرور، فإن إعدادات التوقيع الافتراضية من المحتمل أن تولد حدثا.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

أصدرت هذا **عرض** أمر من ال ASA.

- **show module** — يعرض معلومات حول SSM على ASA بالإضافة إلى معلومات النظام.

```
                                                ciscoasa#show module
 .Mod Card Type                                    Model              Serial No
---------- ------------------ ---------------------------------------- ---
ASA 5510 Adaptive Security Appliance        ASA5510            JMX0935K040 0
ASA 5500 Series Security Services Module-10 ASA-SSM-10         JAB09440271 1

     Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--------------- ------------ ------------ ------------------------------- ---
         (d948.e912 to 0012.d948.e916  1.0          1.0(10)0     8.0(2.0012 0
       c480.cc18 to 0013.c480.cc18  1.0          1.0(10)0     6.1(2)E3.0013 1

    Mod SSM Application Name           Status           SSM Application Version
 ------------------------- ---------------- ------------------------------ ---
                  IPS                        Up                 6.1(2)E3 1

                    Mod Status             Data Plane Status     Compatibility
                    ------------ --------------------- ------------------ ---
                                        Up Sys             Not Applicable 0
```

```
                                                    Up                Up 1
Each of the areas highlighted indicate that !--- the ASA recognizes the AIP-SSM and the ---!
                                                                .AIP-SSM status is up
```

- **تشغيل العرض**

```
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**— يعرض العدادات الخاصة بقائمة الوصول.

```
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 ---!
```

قبل أن تقوم بتثبيت واستخدام AIP-SSM، هل تمر حركة مرور الشبكة من خلال ASA كما هو متوقع؟ وإذا لم تكن كذلك، فقد يكون من الضروري أستكشاف أخطاء الشبكة وقواعد سياسة الوصول إلى ASA وإصلاحها.

مشكلات تجاوز الفشل

- إذا كان لديك إثنان من ASAs في تكوين تجاوز الفشل وكان لكل منهما AIP-SSM، **فيجب عليك** نسخ تكوين AIP-SSMs يدويا. يتم نسخ تكوين ASA فقط بواسطة آلية تجاوز الفشل. لا يتم تضمين AIP-SSM في تجاوز الفشل. ارجع إلى مثال تكوين التغلب على الأعطال في وضع الاستعداد/النشط ASA 7.x للحصول على مزيد من المعلومات حول مشاكل تجاوز الأعطال.
- لا تشارك AIP-SSM في تجاوز الفشل ذو الحالة إذا تم تكوين تجاوز الفشل ذو الحالة على زوج تجاوز الفشل ASA.

رسائل الخطأ

تنتج وحدة IPS النمطية (AIP-SSM) رسائل الخطأ كما هو موضح ولا تقوم بتشغيل الأحداث.

```
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
```

سبب رسالة الخطأ هذه هو أن مستشعر IPS الظاهري لم يتم تعيينه لواجهة اللوحة الخلفية ل ASA. يتم إعداد ASA بالطريقة الصحيحة لإرسال حركة مرور البيانات إلى وحدة SSM النمطية، ولكن يلزمك تعيين المستشعر الظاهري إلى واجهة اللوحة الخلفية التي ينشئها ASA لكي تقوم SSM بمسح حركة مرور البيانات.

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

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

هذه الرسائل تشير إلى تمكين تسجيل IP، والذي بدوره قام بتعبئة جميع موارد النظام. توصي Cisco بتعطيل تسجيل IP لأنه يجب إستخدامه فقط لأغراض أستكشاف الأخطاء وإصلاحها/التحقيق فقط.

ملاحظة: بدأ رسالة الخطأ Error Message `ErrWarning InLine` (خطأ) حيث يقوم المستشعر بإعادة تشغيل محرك التحليل مؤقتا بعد تحديث التوقيع، وهو جزء ضروري من عملية تحديث التوقيع.

دعم Syslog

لا يدعم AIP-SSM syslog كتنسيق تنبيه.

الطريقة الافتراضية لتلقي معلومات التنبيه من AIP-SSM هي من خلال تبادل حدث جهاز الأمان (SDEE). خيار آخر هو تكوين توقيعات منفردة لإنشاء ملائمة SNMP كإجراء يجب إتخاذه عند تشغيل تلك التوقيعات.

إعادة تمهيد AIP-SSM

لا تستجيب وحدة AIP-SSM النمطية بشكل صحيح.

إذا لم تستجب وحدة AIP-SSM النمطية بشكل صحيح، فأعد تشغيل وحدة AIP-SSM النمطية دون إعادة تمهيد ASA. أستخدم الأمر hw-module 1 reload لإعادة تمهيد وحدة AIP-SSM النمطية ولا تعيد تمهيد ASA.

تنبيه البريد الإلكتروني ل AIP-SSM

هل يمكن لبروتوكول AIP-SSM إرسال تنبيهات بالبريد الإلكتروني إلى المستخدمين؟

لا، إنه غير مدعوم.

معلومات ذات صلة

- مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2
- رسائل سجل نظام جهاز الأمان من Cisco، الإصدار 7.2
- مرجع أوامر نظام Cisco لمنع الاقتحام، الإصدار 5.1
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).