

ASA : exemple de configuration de l'envoi du trafic réseau de l'ASA vers le module AIP SSM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Paramètres de configuration initiaux](#)

[Inspection du trafic au moyen d'AIP-SSM en mode en ligne ou en mode promiscuité](#)

[Inspection du trafic au moyen d'AIP-SSM doté d'ASDM](#)

[Inspection d'un trafic particulier au moyen d'AIP-SSM](#)

[Exclusion d'un trafic réseau particulier de l'analyse du module AIP-SSM](#)

[Vérifier](#)

[Dépannage](#)

[Problèmes de basculement](#)

[Messages d'erreur](#)

[Prise en charge de Syslog](#)

[Redémarrage du module AIP-SSM](#)

[Alerte par courriel du module AIP-SSM](#)

[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration sur la façon d'envoyer le trafic réseau qui traverse les dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 au module d'Advanced Inspection and Prevention Security Services Module (AIP SSM) (IPS). Des exemples de configuration sont fournis grâce à l'interface CLI.

Référez-vous à [Exemple de configuration d'ASA : Envoyer le trafic réseau de l'ASA vers le CSC-SSM](#) afin d'envoyer le trafic réseau de l'appliance de sécurité adaptative (ASA) de la gamme Cisco ASA 5500 au module de services de sécurité de contrôle et de sécurité de contenu (CSC-SSM).

Consultez la section sur [l'affectation des capteurs virtuels à un contexte de sécurité \(AIP-SSM seulement\) pour en savoir plus sur l'envoi du trafic réseau transitant par le Cisco ASA de série 5500 en mode multicontexte vers le module AIP-SSM \(Advanced Inspection and Prevention Security Services Module\).](#)

Remarque : le trafic réseau qui traverse l'ASA inclut les utilisateurs internes qui accèdent à Internet ou les utilisateurs Internet qui accèdent à des ressources protégées par l'ASA dans une zone démilitarisée (DMZ) ou dans un réseau interne. Le trafic réseau envoyé vers l'ASA ou provenant de l'ASA n'est pas envoyé au module IPS aux fins d'inspection. Comme exemples d'un trafic qui n'est pas envoyé vers le module IPS, citons les messages Ping (ICMP) transmis aux interfaces ASA ou les transmissions Telnet vers l'ASA.

Remarque : le cadre de stratégie modulaire utilisé par l'ASA afin de classer le trafic pour inspection ne prend pas en charge IPv6. Or, si vous redirigez le trafic du protocole IPv6 vers le module AIP-SSM par l'ASA, celui-ci ne sera pas pris en charge.

Remarque : pour plus d'informations sur la configuration initiale du module AIP-SSM, reportez-vous à [Configuration initiale du capteur AIP-SSM](#).

Conditions préalables

Exigences

Dans le présent document, nous présumons que les lecteurs ont une connaissance de base sur la configuration du logiciel Cisco ASA, version 8.x, et d'IPS, version 6.x.

- Les composants de configuration requis pour ASA 8.x comprennent notamment les interfaces, les listes d'accès, la traduction d'adresses réseau (NAT) et le routage.
- Parmi les composants de configuration nécessaires pour AIP-SSM (logiciel IPS 6.x), mentionnons la configuration du réseau, les hôtes autorisés, la configuration de l'interface, les définitions de signature, et les règles d'action d'événement.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5510 doté de la version 8.0.2 du logiciel
- AIP-SSM-10 doté de la version 6.1.2 du logiciel IPS

Remarque : cet exemple de configuration est compatible avec tout pare-feu de la gamme Cisco ASA 5500 avec OS 7.x et versions ultérieures et avec le module AIP-SSM avec IPS 5.x et versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisés dans un environnement de laboratoire.](#)

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Paramètres de configuration initiaux

Ce document utilise les configurations suivantes. ASA et AIP-SSM démarrent tous deux avec leur configuration par défaut, mais des modifications particulières ont été apportées à des fins d'essais. Les ajouts sont indiqués dans la configuration.

- [ASA 5510](#)
- [AIP-SSM \(IPS\)](#)

ASA 5510

```
<#root>
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 globa

prompt hostname context
.
: end

```

AIP-SSM (IPS)

<#root>

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

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#
```

Remarque : si vous ne parvenez pas à accéder au module AIP-SSM avec https, procédez comme suit :

- Configurez une adresse IP de gestion pour le module. Vous pouvez configurer la liste d'accès réseau dans laquelle vous indiquez les adresses IP et les réseaux IP autorisés à se connecter à l'adresse IP de gestion.
- Assurez-vous d'avoir bien connecté l'interface Ethernet externe du module AIP. L'accès de la gestion au module AIP est possible par cette interface seulement.

Pour en savoir plus, consultez la section [Initialisation d'AIP-SSM](#).

Inspection du trafic au moyen d'AIP-SSM en mode en ligne ou en mode promiscuité

Les administrateurs réseau et la direction de l'entreprise indiquent souvent que tout doit être surveillé. Cette configuration répond aux besoins en matière de surveillance. Outre la surveillance de tous les éléments, il faut prendre deux décisions concernant la façon dont ASA et AIP-SSM interagissent.

- Le module AIP-SSM peut-il fonctionner ou être déployé en mode promiscuité ou en mode en ligne?
 - Le mode promiscuité signifie qu'une copie des données est transmise à l'AIP-SSM, tandis que l'ASA transfère les données d'origine vers la destination. L'AIP-SSM en mode promiscuité peut être considéré comme un système de détection des intrusions (IDS). Dans ce mode, le paquet déclencheur (le paquet à l'origine de l'alarme) peut toujours atteindre sa destination. L'évitement peut alors être mis en œuvre et empêcher d'autres paquets d'atteindre la destination, mais le paquet déclencheur, lui, ne sera pas arrêté.
 - Le mode en ligne signifie que l'ASA transfère les données au module AIP-SSM aux fins d'inspection. Si les données réussissent l'inspection de l'AIP-SSM, celles-ci sont alors renvoyées à l'ASA, où elles seront traitées, puis envoyées vers la destination. L'AIP-SSM en mode en ligne peut être considéré comme un système de prévention des intrusions (IPS). Contrairement au mode promiscuité, le mode en ligne (IPS) peut en fait empêcher le paquet déclencheur d'atteindre la destination.
- Si l'ASA n'arrive pas à communiquer avec le module AIP-SSM, comment l'ASA doit-il gérer le trafic à inspecter? Par exemple, l'ASA ne peut pas communiquer avec un module AIP-SSM notamment lors de la recharge du module AIP-SSM ou si celui-ci tombe en panne et doit être remplacé. Dans un tel cas, l'ASA peut présenter une défaillance en position ouverte ou fermée.
 - Lors d'une défaillance en position ouverte, l'ASA continue de laisser passer le trafic à

inspecter vers la destination finale si l'AIP-SSM ne peut être atteint.

- Toutefois, en cas de défaillance en position fermée, le trafic à inspecter est bloqué lorsque l'ASA ne parvient pas à entrer en contact avec le module AIP-SSM.

Remarque : le trafic à inspecter est défini à l'aide d'une liste de contrôle d'accès. Dans cet exemple, la liste d'accès autorise le trafic IP en provenance de toute source vers n'importe quelle destination. Par conséquent, le trafic à inspecter peut être tout ce qui traverse l'ASA.

```
<#root>
```

```
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 acces
```

```
ciscoasa(config)#
```

```
policy-map global_policy
```

```
!--- Note that policy-map global_policy is a part of the !--- default configuration. In addition, polic
```

```
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
```

```
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.

Inspection du trafic au moyen d'AIP-SSM doté d'ASDM

Voici la marche à suivre pour inspecter le trafic si AIP-SSM utilise ASDM :

1. Allez à Configuration > IPS > Sensor Setup > Startup Wizard [configuration > IPS > réglage du capteur > assistant de démarrage] à la page d'accueil d'ASDM pour lancer la configuration, comme il est illustré ci-dessous :
2. Cliquez sur Launch Startup Wizard [lancer l'assistant de démarrage].
3. Cliquez sur Next (suivant) dans la fenêtre qui s'affiche après le lancement de l'assistant de démarrage.
4. Dans la nouvelle fenêtre, indiquez le nom de l'hôte, l'adresse IP, le masque de sous-réseau ainsi que l'adresse de la passerelle par défaut du module AIP-SSM dans l'espace à cette fin dans la section « Network Settings » (paramètres réseau). Cliquez ensuite sur Add [ajouter] pour ajouter les listes d'accès et ainsi autoriser le trafic avec le module AIP-SSM.
5. Dans la fenêtre Add ACL Entry [ajouter une entrée ACL], saisissez l'adresse IP et les détails du masque de réseau des hôtes et des réseaux qui doivent avoir accès au capteur. Cliquez OK.

Remarque : l'adresse IP hôte/réseau doit appartenir à la plage d'adresses du réseau de gestion.

6. Cliquez sur Next [suivant] après avoir fourni les détails dans les espaces correspondants.
7. Cliquez sur Add [ajouter] pour configurer les détails relatifs à la répartition du trafic.
8. Indiquez l'adresse réseau source et de destination ainsi que le type de service; par exemple, l'adresse IP est utilisée ici. Dans le présent exemple, la valeur any [n'importe quel] est utilisée pour la source et la destination lorsque vous inspectez le trafic au moyen du module AIP-SSM. Cliquez ensuite sur OK.
9. Les règles configurées pour la répartition du trafic s'affichent dans cette fenêtre; vous pouvez ajouter autant de règles que nécessaire si vous suivez la même procédure, expliquée aux étapes 7 et 8. Cliquez ensuite sur Finish [terminer] pour mettre fin à la

procédure de configuration d'ASDM.

Remarque : vous pouvez afficher l'animation du flux de paquets si vous cliquez sur Démarrer.

Inspection d'un trafic particulier au moyen d'AIP-SSM

Si l'administrateur réseau souhaite une surveillance de l'AIP-SSM comme sous-ensemble du trafic, l'ASA dispose de deux variables indépendantes pouvant être modifiées. D'abord, la liste d'accès peut être rédigée de sorte que le trafic nécessaire soit inclus ou exclu. Outre la modification aux listes d'accès, une politique de service peut être appliquée à une interface ou appliquée d'une manière générale pour que soit modifié le trafic inspecté par l'AIP-SSM.

D'après le [schéma du réseau présenté dans le présent document](#), l'administrateur réseau souhaite que l'AIP-SSM inspecte tout le trafic qui est acheminé entre le réseau externe et le réseau DMZ.

```
<#root>
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

```
service-policy
```

command is applied to the DMZ interface.

Ensuite, l'administrateur réseau souhaite que l'AIP-SSM surveille le trafic lancé depuis le réseau interne vers le réseau externe. Le trafic qui est transféré du réseau interne au réseau DMZ n'est pas surveillé.

Remarque : cette section particulière nécessite une compréhension intermédiaire de l'état, des protocoles TCP, UDP, ICMP, de la connexion et des communications sans connexion.

```
<#root>
```

```
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
```

La liste d'accès interdit le trafic lancé sur le réseau interne et destiné au réseau DMZ. La deuxième ligne de la liste d'accès autorise ou envoie le trafic lancé sur le réseau interne et destiné au réseau externe vers l'AIP-SSM. À ce stade, l'état de l'ASA entre en jeu. Par exemple, un

utilisateur interne établit une connexion TCP (Telnet) à un périphérique sur le réseau externe (routeur). L'utilisateur se connecte avec succès au routeur et établit la connexion. Il formule ensuite une commande de routeur qui n'est pas autorisée. Le routeur lui répond « Command authorization failed » [autorisation de la commande refusée]. Le paquet de données qui contient le segment « Command authorization failed » [autorisation de la commande refusée] détient une source du routeur externe et une destination de l'utilisateur interne. La source (externe) et la destination (interne) ne correspondent pas aux listes d'accès définies précédemment dans ce document. L'ASA fait le suivi des connexions dynamiques, ainsi le paquet de données qui est retourné (de l'extérieur à l'intérieur) est réacheminé à l'AIP-SSM aux fins d'inspection. La signature personnalisée 60000 0, qui est configurée sur le module AIP-SSM, envoie une alarme.

Remarque : par défaut, l'ASA ne conserve pas l'état du trafic ICMP. Dans l'exemple de configuration précédent, l'utilisateur interne envoie un message Ping (demande ECHO ICMP) au routeur externe. Le routeur répond par une réponse ECHO ICMP. L'AIP-SSM inspecte le paquet de demandes ECHO, sauf le paquet de réponses ECHO (ECHO-reply). Si l'inspection ICMP est activée sur l'ASA, le module AIP-SSM inspecte les paquets de demandes ECHO et de réponses ECHO.

Exclusion d'un trafic réseau particulier de l'analyse du module AIP-SSM

L'exemple généralisé fourni donne un aperçu de l'exemption d'un trafic précis que doit analyser l'AIP-SSM. Pour ce faire, vous devez créer une liste d'accès qui contient le flux de trafic à exclure de l'analyse de l'AIP-SSM dans l'énoncé du refus. Dans le présent exemple, IPS est le titre de la liste d'accès définissant le flux de trafic que doit analyser l'AIP-SSM. Le trafic entre <source> et <destination> est exclu de l'analyse ; tout autre trafic est inspecté.

```
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
```

Vérifier

Vérifiez que les événements d'alerte sont enregistrés dans l'AIP-SSM.

Connectez-vous au module AIP-SSM au moyen du compte utilisateur de l'administrateur. La commande `show events alert` [afficher les événements d'alerte] génère ce résultat.

Remarque : le résultat varie en fonction des paramètres de signature, du type de trafic envoyé au module AIP-SSM et de la charge réseau.

[L'Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show.](#) Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

<#root>

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 00t...+..^..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....60...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
```

Dans les exemples de configuration donnés, plusieurs signatures IPS sont réglées sur « alarme » pour le trafic de test. Les signatures 2000 et 2004 sont modifiées. La signature personnalisée 60000 est ajoutée. Dans un environnement pratique ou un réseau laissant passer peu de données par l'ASA, il peut être nécessaire de modifier les signatures afin que des événements soient déclenchés. Si l'ASA et l'AIP-SSM sont déployés dans un environnement où passe une grande quantité de trafic, les paramètres de signature par défaut sont susceptibles de générer un événement.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Exécutez ces commandes show à partir de l'ASA.

- show module : Cette commande affiche des informations à propos du SSM sur l'ASA ainsi que des informations système.

<#root>

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-S

- Commande show run

<#root>

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 : Cette commande affiche les compteurs d'une liste d'accès.

```
<#root>
```

```
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.

Avant que vous installiez et utilisiez l'AIP-SSM, le trafic réseau transite-t-il par l'ASA comme prévu? Si ce n'est pas le cas, il peut être nécessaire de procéder au dépannage des règles des politiques d'accès du réseau et de l'ASA.

Problèmes de basculement

- Si vous avez deux ASA dans une configuration de basculement et que chacun contient un module AIP-SSM, vous devez répliquer manuellement la configuration des AIP-SSM. Seule la configuration du ASA est répliquée par le mécanisme de basculement. Le module AIP-SSM n'est pas inclus dans le basculement. Consultez [l'exemple de configuration de basculement actif/en veille PIX/ASA 7.x pour en savoir plus sur le basculement](#).
- L'AIP-SSM ne participe pas au basculement avec état si ce dernier est configuré sur la paire de basculements ASA.

Messages d'erreur

Le module IPS (AIP-SSM) génère des messages d'erreur, comme illustré, sans toutefois déclencher d'événements.

```
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.
```

Ce message d'erreur apparaît parce que le capteur virtuel IPS n'a pas été attribué à l'interface de fond de panier d'ASA. L'ASA est correctement configuré pour envoyer le trafic au module SSM, mais vous devez attribuer le capteur virtuel à l'interface de fond de panier que crée l'ASA afin que le SSM puisse analyser le trafic.

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

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

Ces messages indiquent que la journalisation IP est activée, ce qui accapare toutes les ressources du système. Cisco recommande la désactivation de la journalisation IP, car il ne faut l'utiliser qu'à des fins de dépannage ou d'investigation.

Remarque : le message d'erreur `errWarning Inline data bypass has started` est un comportement attendu car le capteur redémarre momentanément le moteur d'analyse après la mise à jour de la signature, qui est une partie nécessaire du processus de mise à jour de la signature.

Prise en charge de Syslog

L'AIP-SSM ne prend pas en charge syslog comme format d'alerte.

La méthode utilisée par défaut pour recevoir des informations d'alerte de l'AIP-SSM est le protocole SDEE (Security Device Event Exchange). Une autre option consiste à configurer des signatures individuelles de manière à générer une alerte SNMP comme mesure si celles-ci sont déclenchées.

Redémarrage du module AIP-SSM

Le module AIP-SSM ne répond pas correctement.

Si le module AIP-SSM ne répond pas correctement, redémarrez-le sans redémarrer l'ASA. Utilisez la commande [hw-module module 1 reload](#) pour redémarrer le module AIP-SSM sans redémarrer l'ASA.

Alerte par courriel du module AIP-SSM

L'AIP-SSM peut-il envoyer des alertes aux utilisateurs par courriel?

Non. L'AIP-SSM ne prend pas en charge cette fonction.

Informations connexes

- [Référence des commandes des dispositifs de sécurité Cisco, version 7.2](#)
- [Messages du journal système des dispositifs de sécurité Cisco, version 7.2](#)
- [Référence de commande pour le système de prévention des intrusions Cisco 5.1](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.