

Accès Internet d'enable pour le module ASA 5500-X IPS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Les informations de caractéristique](#)

[Dépannage de la méthodologie](#)

[Contournement](#)

[FORUM AUX QUESTIONS](#)

[Informations connexes](#)

[Introduction](#)

Selon la conception, les nouveaux modules des systèmes des préventions des intrusions 5500-X de l'appliance de sécurité adaptable (ASA) (IPS) ne permet pas le trafic d'à travers-le-case sur le port de la Gestion 0/0. Par conséquent, si l'IPS est placé pour utiliser l'adresse IP de l'interface de gestion de l'ASA comme passerelle par défaut, puis le capteur ne peut pas être géré ou accédé à des hôtes derrière d'autres interfaces. En outre, le capteur ne pourra pas atteindre l'Internet.

Ce document explique comment installer les nouveaux modules ASA 5500-X IPS pour accéder à l'Internet par l'intermédiaire de l'ASA.

[Conditions préalables](#)

[Conditions requises](#)

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modules ASA 5500-X IPS

[Composants utilisés](#)

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

- Modules ASA 5500-X IPS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Les informations de caractéristique

Les 5512-5555 appliances sont sans faille intégrées avec l'IPS, qui fonctionne comme module logiciel. L'interface de Gestion IPS partage l'interface de la Gestion 0/0 avec l'ASA. Actuellement, le port de la Gestion 0/0 ne permet pas le trafic d'à travers-le-case dans la gamme 5500-X ASA de périphériques. Cette question affecte la simplicité d'utilisation, particulièrement quand l'interface de la Gestion 0/0 est placée comme passerelle par défaut l'IPS.

Dépannage de la méthodologie

Conditions préalables :

Permis de caractéristique IPS installé sur l'ASA. Ceci est exigé pour activer le module IPS. Ceci peut être vérifié utilisant la commande de **show version** sur l'ASA. Vérifiez le **module IPS : Activé** dans la sortie de **show version**.

```
ASA(config)# show module
```

```
Mod Card Type                               Model                               Serial No.
-----
 0 ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC ASA5515                       FCH1549776V
ips ASA 5515-X IPS Security Services Processor ASA5515-IPS                   FCH1549776V

Mod MAC Address Range                       Hw Version   Fw Version   Sw Version
-----
 0 503d.e59d.90a0 to 503d.e59d.90a7 1.0          2.1(9)8     8.6(1)
ips 503d.e59d.909e to 503d.e59d.909e N/A         N/A         7.1(4)E4

Mod SSM Application Name                   Status       SSM Application Version
-----
ips IPS                                   Up          7.1(4)E4

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

Mod License Name   License Status   Time Remaining
-----
ips IPS Module    Enabled         perpetual
```

Contournement

Afin de permettre au module IPS d'accéder à l'Internet (par exemple pour des automatique-mises à jour, la corrélation globale, etc.), connectez le port de la Gestion 0/0 sur l'ASA à un périphérique

de la couche 3.

Par exemple, le port de la Gestion 0/0 peut être connecté à un port franc sur un routeur interne ou local à l'ASA. Le routeur, consécutivement, peut avoir la passerelle par défaut qui indique l'intérieur/interface interne de l'ASA. Procédez comme suit :

1. Connectez le port de la Gestion 0/0 de l'ASA au périphérique de la couche 3. En outre, établissez la Connectivité entre une interface interne de l'ASA et ce périphérique de la couche 3.
2. Configurez l'adresse IP de Gestion pour le module IPS. Assurez-vous que cette adresse est sur le même sous-réseau que l'adresse IP d'interface de gestion ASA. Dans l'exemple, 10.1.1.1 a été assigné à l'interface Management0/0 de l'ASA et de 10.1.1.2 à l'interface de Gestion IPS.
3. Configurez la passerelle par défaut sur le module IPS comme périphérique de la couche 3 mentionné ci-dessus. Des artères ou la passerelle par défaut appropriées doivent être placées en conséquence sur le périphérique de la couche 3 pour expédier le trafic nécessaire à l'intérieur/à interface interne de l'ASA.
4. Configurez une artère statique sur l'ASA de sorte que le trafic de retour accède le module IPS par ce périphérique de la couche 3.

Topologie :

Configuration d'échantillon :

Routeur :

```
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
end
!
interface GigabitEthernet0/1
 ip address 10.1.1.3 255.255.255.0
 duplex auto
 speed auto
end
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA 5515 :

```
ASA# show running-config
: Saved
:
ASA Version 8.6(1)2
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif internet
 security-level 0
 ip address 172.16.103.73 255.255.255.0
```

```

!
interface Management0/0
  nameif management
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!
object network obj-10.0.0.0
  subnet 10.1.0.0 255.255.0.0
!
object network obj-10.0.0.0
  nat (inside,internet) dynamic interface
!
route internet 0.0.0.0 0.0.0.0 172.16.103.64 1
!--- Route configured to reach the ips module through the internal router route inside 10.1.1.2
255.255.255.255 192.168.1.2 1

```

ASA 5515-IPS :

```

sensor#show configuration
! -----
! Current configuration last modified Sun Sep 18 00:06:25 2012
! -----
! Version 7.1(4)! Host:
!   Realm Keys          key1.0
! Signature Definition: Signature Update    S615.0    2012-01-03
! -----
service interface
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
!--- The management IP address is set. host-ip 10.1.1.2/24,10.1.1.3 !--- The access-list is set
to allow management from the 10.0.0.0/8 network. access-list 10.0.0.0/8 dns-primary-server
enabled !--- The DNS server IP address is set. address 8.8.8.8 exit exit exit

```

Une demande de caractéristique a été augmentée de permettre le trafic d'à travers-le-case sur le port de la Gestion 0/0 l'IPS.

Les détails peuvent être trouvés ici : ID de bogue Cisco [CSCua67798](#) (clients [enregistrés](#) seulement) : ENH ASA 5500-X - Pour permettre le trafic d'à travers-le-case sur le port de gestion

[FORUM AUX QUESTIONS](#)

Q : Je n'ai pas un périphérique de la couche 3 à l'intérieur du point de réseau la passerelle par défaut à. Comment l'IPS peut-il atteindre l'Internet ?

A : Référez-vous à ce document pour d'autres conceptions : [/c/en/us/support/docs/security/ips-sensor-software-version-71/113690-ips-config-mod-00.html](#).

[Informations connexes](#)

- [Support et documentation techniques - Cisco Systems](#)