IPS 6.X et versions ultérieures/IDSM2 : exemple de configuration du mode de paires d'interfaces en ligne à l'aide d'IDM

Table des matières

Introduction

Le fonctionnement en mode Inline Interface Pair place le système de prévention des intrusions (IPS) directement dans le flux de trafic et affecte les taux de transfert de paquets, ce qui les ralentit lorsque la latence est ajoutée. Cela permet au capteur d'arrêter les attaques et donc d'abandonner le trafic malveillant avant qu'il n'atteigne la cible prévue, offrant ainsi un service de protection. Non seulement le périphérique en ligne traite les informations sur les couches 3 et 4, mais il analyse également le contenu et la charge utile des paquets pour détecter des attaques intégrées plus sophistiquées (couches 3 à 7). Cette analyse plus approfondie permet au système d'identifier et d'arrêter et/ou de bloquer les attaques qui transitent normalement par un pare-feu classique.

En mode Inline Interface Pair, un paquet arrive par la première interface de la paire sur le capteur et sort par la seconde interface de la paire. Le paquet est envoyé à la seconde interface de la paire, sauf si ce paquet est refusé ou modifié par une signature.

Remarque : vous pouvez configurer AIM-IPS et AIP-SSM pour qu'ils fonctionnent en ligne, même si ces modules n'ont qu'une seule interface de détection.

Remarque : si les interfaces jumelées sont connectées au même commutateur, vous devez les configurer sur le commutateur en tant que ports d'accès avec des VLAN d'accès différents pour

les deux ports. Sinon, le trafic ne passe pas par l'interface en ligne.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco IPS Sensor qui utilise Command Line Interface 6.0 et Intrusion Prevention System Device Manager (IDM) 6.0.

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.

Produits connexes

Les informations contenues dans ce document s'appliquent également au module de services IDSM-2 (Intrusion Detection System).

Conventions

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

Configuration des paires d'interfaces en ligne

Utilisez la commande inline-interfaces name dans le sous-mode d'interface de service afin de créer des paires d'interfaces en ligne.

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

Remarque : AIP-SSM est configuré pour le mode d'interface en ligne à partir de l'interface de ligne de commande Cisco ASA et non à partir de l'interface de ligne de commande Cisco IPS.

Ces options s'appliquent :

- inline-interfaces name : nom de la paire d'interfaces en ligne logique

  Remarque : sur toutes les interfaces de détection de fond de panier de tous les modules (IDSM-2 NM-CIDS et AIP-SSM), l'état admin est activé et protégé (vous ne pouvez pas modifier ce paramètre). L'état admin n'a aucun effet (et est protégé) sur l'interface de commande et de contrôle. Elle affecte uniquement les interfaces de détection. Il n'est pas nécessaire d'activer l'interface de commande et de contrôle, car elle ne peut pas être

surveillée.

- default : rétablit la valeur par défaut du système
- description : description de la paire d'interfaces en ligne
- interface1 interface_name : première interface de la paire d'interfaces en ligne
- interface2 interface_name : deuxième interface de la paire d'interfaces en ligne
- no : supprime une entrée ou un paramètre de sélection
- admin-state {enabled | disabled} : état de la liaison administrative de l'interface, qu'elle soit activée ou désactivée.

Configuration CLI

Complétez ces étapes afin de configurer les paramètres de paire VLAN en ligne sur le capteur :

1. Connectez-vous à l'interface de ligne de commande avec un compte disposant de privilèges d'administrateur.
2. Passez en sous-mode interface :

```
<#root>

sensor#

configure terminal

sensor(config)#

service interface


sensor(config-int)#
```

3. Vérifiez si des interfaces en ligne existent. Le type de sous-interface devrait être `none` si aucune interface en ligne n'a été configurée :

```
<#root>

sensor(config-int)#

show settings

   physical-interfaces (min: 0, max: 999999999, current: 2)
   ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
```

```
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
<protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
```

```
            description: <defaulted>
            admin-state: disabled <defaulted>
            duplex: auto <defaulted>
            speed: auto <defaulted>
            alt-tcp-reset-interface
            ------------------------------------------------
               none
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            subinterface-type
            ------------------------------------------------
               none
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         <protected entry>
         name: Management0/0 <defaulted>
         ------------------------------------------------
            media-type: tx <protected>
            description: <defaulted>
            admin-state: disabled <protected>
            duplex: auto <defaulted>
            speed: auto <defaulted>
            alt-tcp-reset-interface
            ------------------------------------------------
               none
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            subinterface-type
            ------------------------------------------------
               none
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      command-control: Management0/0 <protected>
      inline-interfaces (min: 0, max: 999999999, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      bypass-mode: auto <defaulted>
      interface-notifications
      ------------------------------------------------
         missed-percentage-threshold: 0 percent <defaulted>
         notification-interval: 30 seconds <defaulted>
         idle-interface-delay: 30 seconds <defaulted>
      ------------------------------------------------
   sensor(config-int)#
```

4. Nommez la paire en ligne :

```
<#root>

sensor(config-int)#
```

```
inline-interfaces PAIR1
```

5. Affichez la liste des interfaces disponibles :

```
<#root>

sensor(config-int)#

physical-interfaces ?

GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)#

physical-interfaces
```

6. Configurez deux interfaces en une paire :

```
<#root>

sensor(config-int)#

interface1 GigabitEthernet0/0
```

```
<#root>

sensor(config-int-inl)#

interface2 GigabitEthernet0/1
```

Vous devez affecter l'interface à un capteur virtuel et l'activer avant qu'il puisse surveiller le trafic. Reportez-vous à l'étape 10 pour plus d'informations.

7. Ajoutez une description de cette interface :

```
<#root>

sensor(config-int-phy)#

description PAIR1 Gig0/0 and Gig0/1
```

8. Répétez les étapes 4 à 7 pour toutes les autres interfaces que vous souhaitez configurer en paires d'interfaces en ligne.

9. Vérifiez les paramètres :

```
<#root>

sensor(config-int-inl)#

show settings

   name: PAIR1
   ----------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   ----------------------------------------------
```

10. Activez les interfaces attribuées à la paire d'interfaces :

```
<#root>

sensor(config-int)#

exit

sensor(config-int)#

physical-interfaces GigabitEthernet0/0

sensor(config-int-phy)#

admin-state enabled

sensor(config-int-phy)#

exit

sensor(config-int)#

physical-interfaces GigabitEthernet0/1

sensor(config-int-phy)#

admin-state enabled

sensor(config-int-phy)#

exit

sensor(config-int)#
```

11. Vérifiez que les interfaces sont activées :

```
<#root>

sensor(config-int)#

show settings
```

```
physical-interfaces (min: 0, max: 999999999, current: 5)
-----------------------------------------------
   <protected entry>
   name: GigabitEthernet0/0
   ------------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      subinterface-type
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   <protected entry>
   name: GigabitEthernet0/1
   ------------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      subinterface-type
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   <protected entry>
   name: GigabitEthernet0/2 <defaulted>
   ------------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: disabled <defaulted>
      duplex: auto <defaulted>
      speed: auto <defaulted>
      default-vlan: 0 <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      subinterface-type
```

```
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
--MORE--
```

12. Émettez cette commande afin de supprimer une paire d'interfaces en ligne et de retourner les interfaces au mode proche :

<#root>

```
sensor(config-int)#
```

no inline-interfaces PAIR1

Vous devez également supprimer la paire d'interfaces en ligne du capteur virtuel auquel elle est attribuée.

13. Vérifiez que la paire d'interfaces en ligne a été supprimée :

<#root>

```
sensor(config-int)#
```

show settings

```
  ------------------------------------------------
  command-control: Management0/0 <protected>
  inline-interfaces (min: 0, max: 999999999, current: 0)
  ------------------------------------------------
  ------------------------------------------------
  bypass-mode: auto <defaulted>
  interface-notifications
  ------------------------------------------------
```

14. Quittez le sous-mode de configuration interface :

<#root>

```
sensor(config-int)#
```

exit

```
Apply Changes:?[yes]:
```

15. Appuyez sur Entrée afin d'appliquer les modifications ou entrez no afin de les ignorer.

Configuration IDM

Complétez ces étapes afin de configurer les paramètres de paire VLAN en ligne sur le capteur à l'aide de l'IDM :

1. Ouvrez votre navigateur et entrez https://<Management_IP_Address_of_IPS> pour accéder à l'IDM sur l'IPS.
2. Cliquez sur Download IDM Launcher et Start IDM pour télécharger le programme d'installation de l'application.
3. Accédez à la page d'accueil afin d'afficher les informations relatives au périphérique, telles que le nom d'hôte, l'adresse IP, la version et le modèle.
4. Accédez à Configuration > Sensor Setup et cliquez sur Network. Vous pouvez spécifier ici le nom d'hôte, l'adresse IP et la route par défaut.
5. Accédez à Configuration > Interface Configuration et cliquez sur Summary.

   Cette page présente le résumé de la configuration de l'interface de détection :
6. Accédez à Configuration > Interface Configuration > Interfaces et sélectionnez le nom de l'interface. Cliquez ensuite sur Enable afin d'activer l'interface de détection. Configurez également les informations relatives au mode bidirectionnel, à la vitesse et au VLAN.
7. Accédez à Configuration > Interface Configuration > Interface Pairs et cliquez sur Add afin de créer la paire en ligne.
8. Affichez le résumé de la configuration des paires en ligne et appliquez-le.
9. Accédez à Configuration > Analysis Engine > Virtual Sensor et cliquez sur Edit afin de créer le nouveau capteur virtuel.
10. Attribuez la paire en ligne INLINE au capteur virtuel vs0.
11. Affichez le résumé des informations de capteur virtuel attribuées.

Configuration du commutateur pour IDSM-2 en mode en ligne

Référez-vous à la section Configuration du commutateur de la gamme Catalyst 6500 pour IDSM-2 en mode en ligne de Configuration d'IDSM-2 afin de configurer le commutateur pour IDSM-2 en mode en ligne.

Dépannage

Problème

Si l'IPS échoue et qu'il est configuré en ligne, les interfaces ne sont-elles pas ouvertes (le trafic continue à passer) ou fermées (le trafic est abandonné) ?

Solution

Vous pouvez configurer IPS en mode fail-open. Ainsi, si l'IPS échoue, il continuera à transmettre le trafic, mais il ne surveillera pas le trafic.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Système de prévention des intrusions Cisco
- Détecteurs Cisco, série IPS 4200
- 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.