IPS 6.X en hoger/IDSM2: Inline interfacemodus met behulp van IDM-configuratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Configuratie van inline-interfaceprocessors CLI-configuratie IDM-configuratie IDM-configuratie Configureer de switch voor IDSM-2 in inline modus Problemen oplossen Probleem Oplossing Gerelateerde informatie

Inleiding

Wanneer u in de modus Inline Interface air werkt, wordt het inbraakpreventiesysteem (IPS) rechtstreeks in de verkeersstroom gezet en heeft het effect op pakketsnelheden, waardoor deze trager worden wanneer er latentie wordt toegevoegd. Dit stelt de sensor in staat om aanvallen te stoppen zodat het kwaadaardig verkeer daalt voordat het doel bereikt, en het biedt dus bescherming. Niet alleen is de informatie over de verwerking van het inline apparaat op Lagen 3 en 4, maar het analyseert ook de inhoud en lading van de pakketten voor geavanceerdere ingebedde aanvallen (Lagen 3 tot 7). Deze diepere analyse laat het systeem aanvallen identificeren en stoppen en/of blokkeren die normaal door een traditioneel firewallapparaat lopen.

In de modus Inline-interface wordt een pakje ingevoerd in de eerste interface van het paar op de sensor en in de tweede interface van het paar. Het pakket wordt naar de tweede interface van het paar verzonden, tenzij het pakket wordt ontkend of gewijzigd door een handtekening.

Opmerking: U kunt AIM-IPS en AIP-SSM configureren om inline te werken, ook al hebben deze modules slechts één detecterende interface.

Opmerking: Als de gekoppelde interfaces op dezelfde schakelaar zijn aangesloten, dient u deze op de schakelaar te configureren als toegangspoorten met verschillende toegang VLAN's voor de twee poorten. Anders stroomt het verkeer niet door de inline interface.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IPS Sensor die de Opdracht Line Interface 6.0 en Inbraakpreventiesysteem Manager (IDM) 6.0 gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

De informatie in dit document is ook van toepassing op de servicesmodule voor inbraakdetectiesysteem (IDSM-2).

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Configuratie van inline-interfaceprocessors

Gebruik de opdracht *naam van inline-interfaces in de submodus van de servicinterface om inline interfaceparen te maken.*

Opmerking: Gebruik het <u>Opdrachtupgereedschap</u> (alleen<u>geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Opmerking: AIP-SSM is ingesteld voor inline interfacemodus vanuit Cisco ASA CLI en niet vanuit Cisco IPS CLI.

Deze opties zijn van toepassing:

- Naam van inline-interfaces Naam van het logische inline interfacepaarOpmerking: Op alle backplane sensorinterfaces op alle modules (IDSM-2 NM-CIDS en AIP-SSM) is de adminstatus ingeschakeld en beschermd (u kunt de instelling niet wijzigen). De admin-status heeft geen effect (en wordt beschermd) op de commando en controle interface. Het beïnvloedt alleen sensatieinterfaces. De opdracht en de bedieningsinterface hoeven niet te worden ingeschakeld omdat deze niet kan worden bewaakt.
- standaard: Hiermee stelt u de waarde weer in op de standaardinstelling van het systeem
- beschrijving Uw beschrijving van het online interfacepaar
- interface1 interface_name De eerste interface in het inline interfacepaar
- interface2 interface_name—De tweede interface in het inline interfacepaar
- no-Verwijdert een invoer of selectie-instelling
- beheerder {ingeschakeld | --- de administratieve verbindingsstaat van de interface, of de

interface is ingeschakeld of uitgeschakeld.

CLI-configuratie

Voltooi deze stappen om de instellingen van het paar inline VLAN op de sensor te configureren:

- 1. Meld u aan bij de CLI met een account met beheerrechten.
- 2. Geef de submodus interface op: sensor#configure terminal sensor(config)#service interface sensor(config-int)#
- 3. Controleer of er interfaces bestaan. Het subinterfacetype zou geen moeten lezen als er geen inline interfaces zijn geconfigureerd:

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. Geef het inline paar een naam:
  sensor(config-int)#inline-interfaces PAIR1
Toont de lijst met beschikbare interfaces:
  sensor(config-int)#physical-interfaces ?
  GigabitEthernet0/0 GigabitEthernet0/0 physical interface.
  GigabitEthernet0/1GigabitEthernet0/1physical interface.GigabitEthernet0/2GigabitEthernet0/2physical interface.GigabitEthernet0/3GigabitEthernet0/3physical interface.Management0/0Management0/0physical interface.
```

sensor(config-int)#physical-interfaces

Configuratie van twee interfaces in een paar: sensor(config-int)#interface1 GigabitEthernet0/0

sensor(config-int-inl)#interface2 GigabitEthernet0/1

U moet de interface aan een virtuele sensor toewijzen en deze activeren voordat het verkeer kan bewaken. Zie stap 10 voor meer informatie.

```
7. Voeg een beschrijving van deze interface toe:
  sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
```

8. Herhaal stappen 4 door 7 voor andere interfaces die u wilt configureren tot inline interfaceparen.

```
9. Controleer de instellingen:
  sensor(config-int-inl)#show settings
    name: PAIR1
     _____
       description: PAIR1 Gig0/0 & Gig0/1 default:
       interface1: GigabitEthernet0/0
       interface2: GigabitEthernet0/1
     _____
10. Schakel de interfaces in die aan het interfacepaar zijn toegewezen:
   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. Controleer dat de interfaces zijn ingeschakeld:
   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. Geef deze opdracht uit om een inline interfacepaar te verwijderen en de interfaces terug te sturen naar de veelbelovende modus:

sensor(config-int)#no inline-interfaces PAIR1

U moet ook het inline-interfacepaar uit de virtuele sensor verwijderen waaraan het is toegewezen.

13. Controleer of het inline interfacepaar is verwijderd:

sensor(config-int)#show settings

- 14. Submodus interface-configuratie afsluiten: sensor(config-int)#exit Apply Changes:?[yes]:
- 15. Druk op Voer in om de wijzigingen toe te passen of ga het niet in om ze weg te gooien.

IDM-configuratie

Voltooi deze stappen om de instellingen van het paar inline VLAN op de sensor te configureren met behulp van de IDM:

- 1. Open uw browser en voer https://<Management_IP_Address_of_IPS>in om de IDM op de IPS te gebruiken.
- 2. Klik op **Download IDM Launcher** en **Start IDM** om het installatieprogramma voor de toepassing te downloaden.
- 3. Ga naar de startpagina om de apparaatinformatie zoals Host Name, IP Address, versie en het model te

| e Help | | | | | | | | | | |
|----------------|---------------|---------------------|--------------|--------------|------------------|--------|---------|-------|----------|----|
| Home | Configuration | Monitoring | Back Forward | @ Refresh | ? Help | | | | CIS | |
| Device Informa | tion | | | Interface | Status | | | | | |
| Host Name: | ips | IP Address: | 10.10.10.11 | Interface | R. | Link | Enabled | Speed | Mode | 10 |
| IPS Version: | 6.0(4a)E1 | Device Type: | IDS-4215-K9 | FastEthen | net2/2 | Down | Yes | N/A | Unpaired | - |
| IDM Version | 6.0.202.35 | Total Memory: | 479 MB | FastEthen | net2/1 | Down | Yes | N/A | Unpaired | 1 |
| Bypass Mode: | Auto_off | Total Data Storage: | 166.8 MB | FastEthen | net2/0 | 🙆 Down | Yes | N/A | Unpaired | 1 |
| Missed Packets | | Total Sensing | | FastEthen | net0/1 | Down | Yes | N/A | Unpaired | |
| Percentage: | 0 | Interface | 5 | FastEthen | net2/3 | Down | Yes | NGA | Unpaired | |

 Ga naar Configuration > Sensor Setup en klik op Network. Hier kunt u de Hostnaam, IPadres en standaardroute instellen.

| Da cisco ioni oro i orioriori | 11 | | | | | | |
|---|--|---|----------------|---|---|-----------|---------|
| File Help | | | | | | | |
| Home Configuration | Montoring | Back | O Forward | Refresh | 🤗 Help | | cisco |
| Sersor Setue Network Network Authorized Keys Known Host Keys Sensor Key Certificates Trusted Hosts Server Certificate Time Users Interface Configuration Summary Interface Pairs VLAN Pairs VLAN Pairs VLAN Pairs VLAN Oroups Sylam Server Definitions Signature Defini | Ietwork Specify the netw Hostname: IP Address: Network Mask: Default Route: FTP Timeout I Allow Passw Web Server Se U Enable TLS Web server po | rork and c IPS 10.10.10 255.0.0.0 10.10.10 300 vord Recor ttings //SSL rt: 443 | ommunication y | Parameters for Remote Telnet is disabled Enet | the sensor. Access not a secure access servic by default. Ile Teinet Reset | ce and is | seconds |

5. Ga naar **Configuration > Interface Configuration** en klik op **Summary**.Op deze pagina wordt de samenvatting van de configuratie van de sensorinterface

| File Help | | | | | | | | |
|---|---|--|---------------------------|-------------------------------------|--------------------------------|---|---|-----------------|
| Home | Configuration | Monitoring | Back | Forward | @ Retresh | 🤣 Help | | cisco |
| Sensor Sel Network Alowe SSH | tup rk d Hosts thorized Keys | Summery The following is t promiscuous, inli | he contigu ne interfac | uration summar e pair, or inline | y of the sensi VLAN pair mo | ng interfaces. You ca ade, but no combinatio | n configure any single physics on of these modes is allowed. Assigned | l interface for |
| Ser Ser | nsor Key | Name EastPharpat0.0 | | Detais | Interface | | Virtual Sensor | Description |
| Certific | ates | FastPhernet2.0 | | Promiscuous | Interface | | -None | |
| S Sa | rsted Hosts | FastEthernet2/1 | | Promiscuous | Interface | | None | - |
| Time | rer commodie | FastEthernet2/2 | | Promiscuous | Interface | | None | |
| Users | - | FastEthernet2/3 | | Promiscuous | Interface | | None | |
| Contractions Contr | entourstion ny se Pairs Pairs Groups s | | | | | | | |

6. Ga naar **Configuration > Interface Configuration > Interfaces** en selecteer de interfacenaam. Klik vervolgens op **Inschakelen** om de detecterende interface in te schakelen. Configureer ook de informatie Duplex, Speed en VLAN.

| Cisco IDM 6.0 - 10.10.10 | -11 | | | | | | _ |
|---|---|---|---|-------------------------------------|---------------------------------------|--|------------|
| e Help | | | | | | | |
| Home Configuration | Montoring E | Back Forward | Refresh Hel | p | | | cisco |
| Sensor Setup Network Allowed Hosts SSH Authorized Keys | Interfaces A sensing interface can enable/disable t | must be enabled and he available sensing in | assigned to a virtual Iterfaces by selectin | sensor before th g the row(s) an | he sensor will m d clicking Enable | onitor that inte or Disable. Default | rface. You |
| Sensor Keys | Interface Name | Enabled | Media Type | Duplex | Speed | VLAN | CONCOLUMN |
| Q. Certificates | FastEthernet0/1 | Yes | TX (copper) | Auto | Auto | | Edit |
| Trusted Hosts | FastEthernet2/0 | Yes | TX (copper) | Auto | Auto | | - |
| Server Certificate | FastEthernet2/1 | Yes | TX (copper) | Auto | Auto | | Enable |
| 🛱 Time | FastEthernet2/2 | Yes | TX (copper) | Auto | Auto | | Linders |
| N Users | FastEthernet2/3 | Edit In | terface | | | | |
| Interfaces Interface Inte | <. | Enabled: Media Typ Duplex: Speed: Default VI Olise AU Selection | e TX (coppe Auto Auto Auto Auto IAN: 0 Iternate TCP Reset in riteriace FastEther n: | No r) M terface | | | |

7. Ga naar **Configuration > Interface Configuration > Interface Parks** en klik op **Add** om het inline paar te maken.

| File Helo | | | | | | Carbon Car |
|---|---|--|---|---|---------------------------|------------------|
| Home | Configuration | Monitoring Back | Forward Refres | 🤗 h Help | | cisco |
| Sensor Set Networ Alowe | up 🏠 🕺 | Interface Pairs You can create logical inte pair(s) by selecting the ro- | rface pair(s) for the avai w(s) and clicking Edit or D | lable sensing interfaces. Yo velete. | ou can edit/delete the ex | isting interface |
| - Aut | horized Keys | Interface Pair Name | Paired Interfaces | | Description | Select All |
| Ser Q Certific S Tru | ates sted Hosts | 6 | | | | Add |
| Ser Ser | ver Certificate | | C Add Interface Pa | ir | | Edt 🕹 |
| B Users | = | | Interface Pair Name: | INLINE | | Delete |
| Interface C Summa Differiat VLAN (| e Pairs Rains Shoups | | Select two interfaces: | FastEthernet0/1 FastEthernet2/0 FastEthernet2/1 | | |
| Analysis Er | Flow Notificatic ngine Sensors Variables | | Description | FastEthernet2/3 | | |
| Signatu Signatu Event A Sand Sand Blocking Blocking | re Definitions 0 loction Rules ISD ly Detections 1 g Properties | ٤] | ОК | Cencel | Help | |

8. Bekijk de samenvatting van de configuratie van het inline paar en pas deze toe.

| File Help | | | | | | | | Called Call |
|---|--|--|---------------------------------------|----------------------------------|-------------------------------------|----------------------------|--------------------------------|----------------------|
| Home | Configuration | Monitoring | Back | Forward | @ Refresh | 🤗 Help | | cisco |
| Sensor Set Networ Allower | inp At K k Hosts | Interface Pairs You can cre pair(s) by s | ate logical inter electing the row | face pair(s) f (s) and clicki | or the svailable ng Edit or Dele | e sensing interface le. | se. You can edit/delete the ex | disting interface |
| Aut | horized Keys | Interface I | Pair Name | Paired In | nterfaces | | Description | Select All |
| Certification Certification True Ser True Ser True Ser True Ser True Ser Users Interface Cr Summa Interface VLAN VLAN | sor Key ites sted Hosts ver Certificate artiguration ry es e Pairs iairs iairs Pow Notificatic gine Sensors /ariables re Definitions) ction Rules s0 y Detections g Properties | < | | rosiciter | III Apply | R | eset | Add Edt Delete |
| The license key | on the sensor has a | expired on 4/7/0 | 7 12:00 AM UT | | | | cisco admi | inistrator |

9. Ga naar **Configuration > Analysis Engine > Virtual Sensor** en klik op **Bewerken** om de nieuwe virtuele sensor te maken.

| e Help | | | | | | | | | |
|--|--|---|--|-------------------------------------|------------------------------------|----------------------------------|--|--|----------------------------|
| Home | Configuration | Monitoring | Back | Forward | Refresh | ? Help | | | cisco |
| Sensor Sel Networ Allowed SSH | up k 3 Hosts horized Keys | Virtual Senso The sensor create a ne clicking Edit | nonitors traffi w virtual sense or Delete. | c that traverse or by clicking A | s interfaces, in add. You can e | terface pairs dit or delete s | s, or VLAN pairs assign an existing virtual sense | ed to a virtual sen or by selecting the | sor. You car row(s) and |
| Ser | wn Host Keys Isor Key | Name | Assigned In | terfaces (or Pr | airs) | | Sig Definition Policy | Event Act Poll | Select All |
| Certifica | ates sted Hosts | vs0 | 1 | | | | sigD | | Add |
| A Summa Dinterface A Interface VLAN (VLAN (Dypass VLAN (Dypass Traffic I A Googn Virtual 3 Coognature Sign | ry es e Pairs airs Flow Notifications Flow Notification Sensors reflections cetton Rules s0 y Detections | ٤] | | <u>11</u> | Annix | | Reset | • | |
| Blocking | Properties | | | | Apply | | Reset | | |

10. Wijs de INLINE-paar toe aan de virtuele sensor vs0.

| Help | | | |
|---------------------|---------------------------------------|--|---------------------|
| Home Configu | aration Monitorina Back |) 🚫 🔞 🢡 K Forward Refresh Help | cisco |
| Sensor Setup | 🕼 Edit Virtual Sensor | | |
| Network | Vidual Sensor Name | vel | |
| SSH | Virtual Scribb Name. | Yau | |
| Authorized Ke | Signature Definition Policy: | sig0 💌 | |
| Known Host H | | | |
| Sensor Key | Event Action Rules Policy: | rules0 M | |
| Centricates | Anomaly Detection Policy: | ad0 at | |
| Server Certific | contracting accession of a sector | 300. Y | |
| Time | AD Operational Mode: | Detect 💌 | |
| AJ Users | | | |
| Summary | Inline TCP Session Tracking Mode | Virtual Sensor | |
| D Interfaces | Description: | destant state and second | |
| Interface Pairs | Provingeron. | default virtual sensor | |
| VLAN Pairs | -Available Interfaces | | |
| Bypass | Name | Details | Assigned Select All |
| Traffic Flow Notifi | FastEthernet0/1 | Promiscuous Interface | No |
| Analysis Engine | FastEthernet2/2 | Promiscuous Interface | No Assign |
| Global Variables | FastEthernet2/3 | Promiscuous Interface | No |
| olicies | INLINE | Inline Interface Pair: FastEthernet2/0<->FastEthernet2/1 | Yes Remove |
| Signature Definitio | | | |
| jps] sig0 | | | |
| - Dirules0 | 1 | 1 | |
| Anomaly Detection | 1-0 | | |
| Blocking | | | |
| Blocking Propertie | | Carcer (nep | |
| - III I | · · · · · · · · · · · · · · · · · · · | | |

11. Bekijk de samenvatting van de toegewezen virtuele sensorinformatie.

| Home Configuration | Montoring | Back | Forward | @ Refresh | 🤗 Help | | | cisco |
|--|---|--|-----------------------------------|------------------------------------|------------------------------------|--|--|-------------------------------|
| Sensor Setup Network Allowed Hosts SSH Authorized Keys | Virtual Senso The senso create a n clicking Ed | ors r montors traffic ew virtual senso t or Delete. | that traverses r by clicking A | : interfaces, in dd. You can ei | terface pairs, dit or delete an | or YLAN pairs assign existing virtual sense | ed to a virtual ser or by selecting the | nsor. You can e row(s) and |
| Sensor Key | Name | Assigned Int | ertaces (or Pa | irs) | | Sig Definition Policy | Event Act Poli | Select All |
| Trusted Hosts | vs0 | INLINE.0 (Inir | e Interface Pai | r: FastEtherne | 12/0<->FastEth | sig0 | | Add |
| Interface Configuration Summery Interfaces VLAN Pairs VLAN Pairs VLAN Groups Bypass Traffic Flow Notification Applyois Engine Virtual Sensors Policies Signature Definitions Signature Definitions | | | | | | | | Delete |

Configureer de switch voor IDSM-2 in inline modus

Raadpleeg het <u>gedeelte Catalyst Series 6500 switch voor IDSM-2 in</u> het gedeelte <u>Inline modus</u> van <u>IDSM-2 configureren</u> om de schakelaar voor IDSM-2 inline modus te configureren.

Problemen oplossen

Probleem

Als IPS mislukt en inline wordt geconfigureerd falen de interfaces open (verkeer blijft doorlopen) of gesloten (verkeer wordt laten vallen).

Oplossing

U kunt IPS in een openstaande toestand configureren. Dus als IPS faalt zal het het verkeer blijven doorgeven maar het zal het verkeer niet controleren.

Gerelateerde informatie

<u>Cisco ASA 5500 Series adaptieve security applicaties</u>

- <u>Cisco-inbraakpreventiesysteem</u>
- <u>Cisco IPS 4200 Series sensoren</u>
- Technische ondersteuning en documentatie Cisco Systems