IPS 6.X及更高版本/IDSM2：使用IDM的內聯介面對模式配置示例

目錄

簡介

在內嵌介面配對模式下運作時，會將入侵防禦系統(IPS)直接放入流量中，並會影響封包轉送速率，因此會在新增延遲時降低轉送速率。這使得感測器可以停止攻擊，從而在惡意通訊量到達預定目標之前將其丟棄，從而提供保護服務。內聯裝置不僅處理第3層和第4層上的資訊，還分析資料包的內容和負載，以發現更複雜的嵌入式攻擊（第3層至第7層）。這種更深入的分析可讓系統辨識並阻止通常透過傳統防火牆裝置的攻擊。

在內聯介面對模式下，資料包透過感測器上的該對的第一介面進入，並從該對的第二介面發出。資料包被傳送到該對的第二個介面，除非該資料包被簽名拒絕或修改。

注意：即使這些模組只有一個感應介面，您也可以將AIM-IPS和AIP-SSM配置為線上運行。

注意：如果成對介面連線到同一交換機，則您應在交換機上將它們配置為兩個埠具有不同接入VLAN的接入埠。否則，流量不會流經內聯介面。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於使用命令列介面6.0和入侵防禦系統裝置管理器(IDM) 6.0的Cisco IPS感測器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本文檔中的資訊也適用於入侵檢測系統(IDSM-2)服務模組。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

內聯介面對配置

在服務介面子模式下使用inline-interfaces name 命令以建立內聯介面對。

注意：使用命令查詢工具(僅限註冊客戶)可以獲取有關本部分使用的命令的更多資訊。

注意：AIP-SSM是從Cisco ASA CLI而非從Cisco IPS CLI配置為內聯介面模式。

這些選項適用：

- inline-interfaces name — 邏輯內聯介面對的名稱

  註：在所有模組（IDSM-2 NM-CIDS和AIP-SSM）上的所有背板感應介面上，admin-state設定為enabled並且受到保護（您無法更改該設定）。admin-state（處於保護狀態）對於命令和控制介面沒有影響。它只影響感應介面。由於無法監控命令和控制介面，因此不需要啟用該介面。

- default -將值設定回系統預設設定
- description — 內聯介面對的說明
- interface1 interface_name -內聯介面對的第一個介面
- interface2 interface_name— 內聯介面對的第二個介面
- no -刪除條目或選擇設定
- admin-state {enabled | disabled} —介面的管理鏈路狀態，啟用或停用介面。

CLI配置

要配置感測器上的內聯VLAN對設定，請完成以下步驟：

1. 使用具有管理員許可權的帳戶登入到CLI。

2. 進入介面子模式：

```
<#root>

sensor#

configure terminal

sensor(config)#

service interface


sensor(config-int)#
```

3. 驗證是否存在任何內聯介面。如果尚未配置任何內聯介面，子介面型別應顯示none：

```
<#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. 命名內嵌配對：

```
<#root>

sensor(config-int)#

inline-interfaces PAIR1
```

5. 顯示可用介面的清單：

```
<#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. 將兩個介面配置成對：

```
<#root>

sensor(config-int)#

interface1 GigabitEthernet0/0
```

```
<#root>

sensor(config-int-inl)#

interface2 GigabitEthernet0/1
```

您必須將介面分配給虛擬感測器並啟用該介面，虛擬感測器才能監視通訊量。有關詳細資訊，請參閱步驟10。

7. 增加此介面的說明：

```
<#root>

sensor(config-int-phy)#

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

8. 對於要配置到內聯介面對的任何其他介面，重複步驟4到7。
9. 驗證設定：

```
<#root>

sensor(config-int-inl)#

show settings

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

10. 啟用分配給介面對的介面：

```
<#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. 驗證是否已啟用介面：

<#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. 發出以下命令以刪除內嵌介面配對並將介面返回到混合模式：

```
<#root>

sensor(config-int)#

no inline-interfaces PAIR1
```

還必須從分配了內聯介面對的虛擬感測器中刪除該內聯介面對。

13. 驗證內嵌介面配對是否已刪除：

```
<#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. 退出介面配置子模式：

```
<#root>

sensor(config-int)#

exit

Apply Changes:?[yes]:
```

15. 按Enter 以應用更改或輸入no 以放棄更改。

IDM配置

要使用IDM配置感測器上的內聯VLAN對設定，請完成以下步驟：

1. 打開瀏覽器並輸入https:// <Management_IP_Address_of_IPS>以訪問IPS上的IDM。
2. 按一下Download IDM Launcher和Start IDM以下載應用程式的安裝程式。
3. 移至[首頁]檢視裝置資訊，例如主機名稱、IP位址、版本和型號。
4. 轉到Configuration > Sensor Setup，然後按一下Network。您可以在此處指定主機名、IP地址和預設路由。
5. 轉到Configuration > Interface Configuration，然後按一下Summary。

   此頁面顯示感應介面的組態摘要：

6. 轉到Configuration > Interface Configuration > Interfaces 並選擇介面名稱。然後，按一下Enable以啟用感測器介面。此外，配置雙工、速度和VLAN資訊。
7. 轉到Configuration > Interface Configuration > Interface Pairs，然後按一下Add以建立內聯對

。

8. 檢視內嵌配對組態的摘要並加以套用。
9. 轉到Configuration > Analysis Engine > Virtual Sensor 並按一下Edit 以建立新的虛擬感測器。
10. 將內聯對INLINE分配給虛擬感測器vs0。
11. 檢視分配的虛擬感測器資訊的摘要。

為內聯模式IDSM-2配置交換機

要為內聯模式IDSM-2配置交換機，請參閱配置IDSM-2 的為內聯模式IDSM-2配置Catalyst系列6500交換機部分。

疑難排解

問題

如果IPS發生故障且已內聯配置，則介面是失效開放（流量繼續透過）還是關閉（流量被丟棄）。

解決方案

可以將IPS配置為失效開放狀態。因此，如果IPS發生故障，它將繼續傳遞流量，但不會監控流量。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 思科入侵防禦系統
- Cisco IPS 4200系列感應器
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。