ASA/PIX/IOS路由器的IPS迴避/攔截配置示例

目錄

簡介

本文檔介紹如何使用Cisco IPS在PIX/ASA/Cisco IOS路由器上配置迴避。感測器上的阻塞應用程式ARC啟動和停止路由器、Cisco 5000 RSM和Catalyst 6500系列交換機、PIX防火牆、FWSM和ASA上的阻塞。ARC向受管裝置發出針對惡意IP地址的阻止或迴避。ARC將相同的塊傳送到感測器管理的所有裝置。如果配置了主阻塞感測器，則向此裝置轉發並發出該阻塞。ARC監視塊的時間，並在時間到期後刪除塊。

使用IPS 5.1時，在多情景模式下回退到防火牆時必須特別小心，因為不會隨回退請求一起傳送VLAN資訊。

> **附註**：多情景FWSM的管理上下文中不支援阻止。

有三種型別的塊：

- 主機塊 — 阻止來自給定IP地址的所有流量。
- 連線塊 — 阻止從給定源IP地址到給定目標IP地址和目標埠的流量。從同一源IP地址到不同目標IP地址或目標埠的多個連線塊會自動將該塊從連線塊切換到主機塊。**附註**：安全裝置不支援連線塊。安全裝置僅支援具有可選埠和協定資訊的主機塊。
- 網路塊 — 阻止來自給定網路的所有流量。您可以在觸發簽名時手動或自動啟動主機和連線塊。您只能手動啟動網路塊。

對於自動塊，必須選擇「請求塊主機」或「請求塊連線」作為特定簽名的事件操作，以便SensorApp在觸發簽名時向ARC傳送塊請求。ARC收到來自SensorApp的阻止請求後，將更新裝置配置以阻止主機或連線。請參閱將操作分配給簽名，第5-22頁，瞭解有關將請求塊主機或請求塊連線事件操作新增到簽名的過程的詳細資訊。請參閱配置事件操作覆蓋，第7-15頁，瞭解有關將請求塊主機或請求塊連線事件操作新增到特定風險等級警報的覆蓋配置過程的詳細資訊。

在Cisco路由器和Catalyst 6500系列交換機上，ARC通過應用ACL或VACL建立塊。ACL和VACL會

分別對介面應用過濾器，包括方向和VLAN，以便允許或拒絕流量。.PIX防火牆、FWSM和ASA不使用ACL或VACL。使用內建的**shun**和**no shun**命令。

配置ARC時需要以下資訊：

- 如果裝置配置了AAA，則登入使用者ID
- 登入密碼
- 啟用密碼，如果使用者具有啟用許可權，則不需要此密碼
- 要管理的介面，例如ethernet0、vlan100
- 您希望在建立的ACL或VACL的開始（預阻止ACL或VACL）或結束（預阻止ACL或VACL）應用的任何現有ACL或VACL資訊。這不適用於PIX防火牆、FWSM或ASA，因為它們不使用ACL或VACL進行阻止。
- 使用Telnet或SSH與裝置通訊
- 您永遠不想被阻止的IP地址（主機或主機範圍）
- 你想讓這些塊持續多久

必要條件

需求

在配置ARC以阻止或速率限制之前，必須完成以下任務：

- 分析網路拓撲，瞭解哪些裝置應該被哪個感測器阻塞，哪些地址永遠不應阻塞。
- 收集登入每台裝置所需的使用者名稱、裝置密碼、啟用密碼和連線型別（Telnet或SSH）。
- 瞭解裝置上的介面名稱。
- 如果需要，請知道預阻止ACL或VACL以及後阻止ACL或VACL的名稱。
- 瞭解哪些介面應該被阻止，哪些介面不應該被阻止，以及哪些介面朝哪個方向被阻止（傳入或傳出）。

採用元件

本檔案中的資訊是根據思科入侵防禦系統5.1及更新版本。

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。

> **附註**：預設情況下，ARC配置為限製為250個塊條目。有關ARC支援的阻塞裝置清單的詳細資訊，請參閱支援的裝置。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

使用Blocking頁可配置啟用阻止和速率限制所需的基本設定。

ARC控制受管裝置上的阻塞和速率限制操作。

必須調整感測器以識別永遠不應被阻止的主機和網路。受信任裝置的流量可能會發出簽名。如果此簽名配置為阻止攻擊者，合法的網路流量可能會受到影響。裝置的IP地址可以列在Never Block清單中，以防止出現這種情況。

在Never Block條目中指定的網路掩碼將應用於Never Block地址。如果未指定網路掩碼，則應用預設的/32掩碼。

> **附註**：預設情況下，不允許感測器為自己的IP地址發出阻塞，因為這樣會干擾感測器與阻塞裝置之間的通訊。但是，此選項可由使用者配置。

一旦將ARC配置為管理阻塞裝置，則用於阻塞的阻塞裝置的分流和ACL/VACL不應手動更改。這會導致ARC服務中斷，並可能導致將來無法頒發塊。

> **附註**：預設情況下，Cisco IOS裝置僅支援阻塞。如果選擇速率限制或阻塞加速率限制，可以覆蓋阻塞預設值。

若要發出或修改阻止，IPS使用者必須具有Administrator或Operator角色。

配置感測器以管理Cisco路由器

本節介紹如何將感測器配置為管理Cisco路由器。包含以下主題：

- 配置使用者配置檔案
- 路由器和ACL
- 使用CLI配置Cisco路由器

配置使用者配置檔案

感測器使用**user-profiles** profile_name命令管理其他裝置，以便設定使用者配置檔案。使用者配置檔案包含使用者ID、密碼和啟用密碼資訊。例如，所有共用相同密碼和使用者名稱的路由器都可以使用一個使用者配置檔案。

> **附註**：在配置阻止裝置之前，必須**建立使用者配置檔案**。

完成以下步驟以設定使用者配置檔案：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入網路訪問模式。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. 建立使用者配置檔名稱。
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```

4. 鍵入該使用者配置檔案的使用者名稱。
```
sensor(config-net-use)#username username
```
5. 指定使用者的密碼。
```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

6. 指定使用者的啟用密碼。
```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

7. 驗證設定。
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. 退出網路訪問子模式。
```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```
9. 按**Enter**以應用更改，或輸入no以放棄更改。

路由器和ACL

當ARC設定有使用ACL的封鎖裝置時，ACL的構成方式如下：

1. 包含感測器IP地址或感測器NAT地址的允許行（如果指定）**附註**：如果允許封鎖感應器，ACL中不會出現此行。
2. 預封鎖ACL（如果已指定）：此ACL必須已存在於裝置上。**附註**：ARC會讀取預配置ACL中的行，並將這些行複製到塊ACL的起始位置。
3. 任何活動塊
4. **封鎖後ACL**或**permit ip any**:**封鎖後ACL(**如果已指定):此ACL必須已存在於裝置上。**附註**：ARC會讀取ACL中的行，並將這些行複製到ACL的末尾。**附註**：如果要允許所有不匹配的資料包，請確保ACL的最後一行是permit ip any any。**permit ip any any**（如果指定了後阻止ACL，則不使用）

   附註：ARC設定的ACL絕不應由您或任何其他系統修改。這些ACL是臨時的，感測器會不斷建立新的ACL。您唯一可以做的修改是修改預阻止ACL和後阻止ACL。

如果需要修改預阻止或後阻止ACL，請完成以下步驟：

1. 禁用感測器上的阻塞。
2. 更改裝置的配置。
3. 重新啟用感測器上的阻塞。

重新啟用阻塞後，感測器會讀取新的裝置配置。

附註：單個感測器可以管理多個裝置，但是多個感測器無法管理單個裝置。如果從多個感測器

發出的資料塊用於單個阻塞裝置，則必須在設計中合併主阻塞感測器。主阻塞感測器接收來自多個感測器的阻塞請求，並向阻塞裝置發出所有阻塞請求。

在路由器配置中建立並儲存預阻止和預阻止後ACL。這些ACL必須是擴展IP ACL，可以是命名的，也可以是編號的。有關如何建立ACL的詳細資訊，請參閱路由器文檔。

附註：預阻止和阻止後ACL不適用於速率限制。

ACL會自上而下進行評估，並執行第一個匹配操作。預先封鎖型ACL可能包含允許許可權，優先於封鎖產生的deny。

後阻塞ACL用於說明未由前阻塞ACL或阻塞處理的任何情況。如果介面上有現有的ACL且其方向與區塊發出方向相同，則該ACL可用作封包後ACL。如果沒有後阻止ACL，感測器會在新ACL的末尾插入permit ip any any。

當感測器啟動時，它會讀取兩個ACL的內容。接下來會使用以下專案建立第三個ACL:

- 感測器IP地址的允許行
- 預阻止ACL的所有配置行的副本
- 感測器阻塞的每個地址的拒絕線路
- 阻止後ACL的所有配置行的副本

感測器將新ACL應用到您指定的介面和方向。

附註：當新的塊ACL應用於路由器的介面時（在特定方向上），它將替換該介面上在該方向上的任何先前存在的ACL。

使用CLI配置Cisco路由器

完成以下步驟，將感測器配置為管理思科路由器以執行阻塞和速率限制：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入網路訪問子模式。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. 指定ARC控制的路由器的IP地址。
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. 輸入配置使用者配置檔案時建立的邏輯裝置名稱。
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   附註：ARC接受您輸入的任何內容。它不會檢查使用者配置檔案是否存在。
5. 指定用於訪問感測器的方法。
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```
   如果未指定，則使用SSH 3DES。**附註**：如果使用DES或3DES，則必須使用**ssh host-key ip_address**命令以接受來自裝置的SSH金鑰。
6. 指定感測器NAT地址。
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   附註：這會將ACL第一行中的IP地址從感測器地址更改為NAT地址。NAT地址是感測器地址

，即NAT之後的地址，由位於感測器和阻塞裝置之間的中間裝置轉換。

7. 指定路由器是執行阻塞、速率限制還是同時執行兩者。**附註**：預設設定為阻止。如果希望路由器僅執行阻塞，則無需配置響應功能。僅速率限制
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

   阻塞和速率限制
   ```
   sensor(config-net-rou)#response-capabilities block|rate-limit
   ```

8. 指定介面名稱和方向。
   ```
   sensor(config-net-rou)#block-interfaces interface_name {in | out}
   ```

   附註：介面名稱必須是路由器在interface命令後使用時識別的縮寫。
9. （可選）新增pre-ACL名稱（僅阻止）。
   ```
   sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
   ```
10. （可選）新增後ACL名稱（僅阻止）。
    ```
    sensor(config-net-rou-blo)#post-acl-name post_acl_name
    ```
11. 驗證設定。
    ```
    sensor(config-net-rou-blo)#exit

    sensor(config-net-rou)#show settings

       ip-address: 10.89.127.97
       ------------------------------------------------
          communication: ssh-3des default: ssh-3des
          nat-address: 19.89.149.219 default: 0.0.0.0
          profile-name: PROFILE1
          block-interfaces (min: 0, max: 100, current: 1)
          ------------------------------------------------
             interface-name: GigabitEthernet0/1
             direction: in
             ------------------------------------------------
                pre-acl-name: <defaulted>
                post-acl-name: <defaulted>
             ------------------------------------------------
          ------------------------------------------------
          response-capabilities: block|rate-limit default: block
       ------------------------------------------------
    sensor(config-net-rou)#
    ```
12. 退出網路訪問子模式。
    ```
    sensor(config-net-rou)#exit
    sensor(config-net)#exit
    sensor(config)#exit
    Apply Changes:?[yes]:
    ```
13. 按Enter以應用更改，或輸入no放棄更改。

配置感測器以管理思科防火牆

完成以下步驟，將感測器設定為管理思科防火牆：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入網路訪問子模式。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. 指定ARC控制的防火牆的IP地址。
   ```
   sensor(config-net)#firewall-devices ip_address
   ```

4. 輸入配置使用者配置檔案時建立的使用者配置檔名稱。
   ```
   sensor(config-net-fir)#profile-name user_profile_name
   ```
   附註：ARC接受您鍵入的任何內容。它不會檢查邏輯裝置是否存在。
5. 指定用於訪問感測器的方法。
   ```
   sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
   ```

   如果未指定，則使用SSH 3DES。**附註**：如果使用DES或3DES，則必須使用**ssh host-key ip_address**命令接受該金鑰，否則ARC無法連線到裝置。
6. 指定感測器NAT地址。
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   附註：這會將ACL第一行中的IP地址從感測器的IP地址更改為NAT地址。NAT地址是感測器地址，即NAT之後的地址，由位於感測器和阻塞裝置之間的中間裝置轉換。
7. 退出網路訪問子模式。
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. 按**Enter**以應用更改，或輸入**no**以放棄更改。

在PIX/ASA中阻止具有SHUN

發出**shun**命令可阻止來自攻擊主機的連線。與命令中的值匹配的資料包將被丟棄並記錄，直到刪除阻止功能。無論具有指定主機地址的連線當前是否處於活動狀態，都會應用**shun**。

如果指定目的地位址、來源和目的地連線埠以及通訊協定，則會將shun範圍縮小到與這些引數相符的連線。每個來源IP位址只能有一個**shun**命令。

由於**shun**命令用於動態阻止攻擊，因此它不會顯示在安全裝置配置中。

每當刪除介面時，也會刪除連線到該介面的所有分流。

此範例顯示有問題的主機(10.1.1.27)建立與受害者(10.2.2.89)的TCP連線。安全裝置連線表中的連線如下所示：

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

要阻止來自攻擊主機的連線，請在特權EXEC模式下使用**shun**命令。使用以下選項套用**shun**命令：

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

該命令刪除安全裝置連線表中的連線，並阻止來自10.1.1.27:555到10.2.2.89:666(TCP)的資料包通過安全裝置。

相關資訊

- 配置感測器以管理Catalyst 6500系列交換機和Cisco 7600系列路由器
- 技術支援與文件 - Cisco Systems