瞭解基於策略的VPN隧道內的加密ACL計數器

目錄

簡介

本檔案將說明基於原則的VPN通道中的密碼編譯存取控制清單(ACL)計數器的行為。

必要條件

需求

思科建議瞭解以下主題：

- Cisco IOS® /Cisco IOS® XE平台上的基於策略的站點到站點VPN
- Cisco IOS/Cisco IOS XE平台上的訪問控制清單

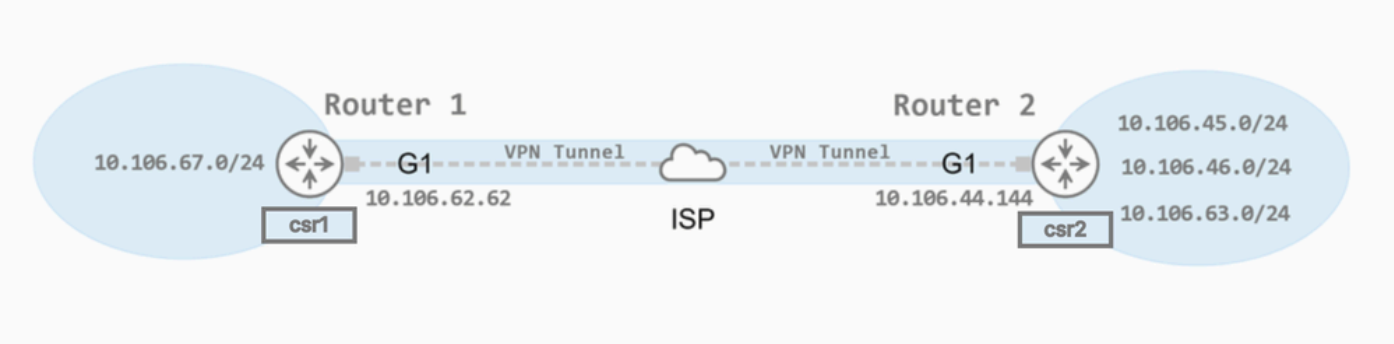
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco C8kv版本17.12.04(MD)

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

拓撲



拓撲

案例

通過研究兩種不同的方案，我們希望瞭解從不同對等體發起流量和重置隧道時ACL命中計數會受到什麼影響。

1. 情況一：在VPN隧道處於非活動狀態時從Router1發起的流量

   在此案例中，當VPN通道最初關閉且流量從Router1發起時，會分析ACL命中計數的變更。此分析有助於瞭解初始設定以及加密ACL計數器對第一次流量嘗試的反應。

2. 情況二：在VPN隧道處於活動狀態時從Router2發起的流量

   在此案例中，已建立VPN通道，並探索從Router2發起的流量。此案例深入瞭解ACL計數器在通道處於活動狀態且流量是從其他對等點引入時的行為。

通過比較這些場景，我們可以全面瞭解VPN隧道中ACL計數器在各種條件下的動態。

組態

我們已經在兩台Cisco C8kv路由器（指定為對等路由器）之間配置了一個基於策略的站點到站點VPN隧道。Router1命名為「csr1」，Router2命名為「csr2」。

Router1上的加密組態

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Router2上的加密組態

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
```

```
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

VPN通道內加密存取控制清單計數器的行為分析

最初，兩台裝置各自加密訪問清單的ACL命中計數均為零。

```
csr1#sh access-lists new_acl
Extended IP access list new_acl
    10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
    20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
    30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
```

```
csr2#sh access-lists new_acl
Extended IP access list new_acl
    20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
    30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
    40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
```

訪問控制清單對兩台對等裝置上的各自加密訪問清單的命中計數為零。

情況一：在VPN隧道處於非活動狀態時從Router1發起的流量

初始狀態：

連線Router1的VPN通道(IP:10.106.67.27)和Router2(IP:10.106.45.145)當前處於非活動狀態。

已採取的行動：

流量從Router1發起，旨在與Router2建立通訊。

意見：

1. ACL計數器行為：
   a.從Router1啟動流量時，Router1上的存取控制清單(ACL)計數器中會出現一個明顯的增量。此增量僅在通道嘗試建立時出現一次。
   b.ACL計數器的上升專門發生在發起路由器（在此案例中為Router1）上。Router2在此階段不會在其ACL計數器中反映任何變更。
2. 隧道建立：
   a.在流量發起對應的初始增量之後，第一個和Router2之間的通道成功建立。
   b.通道建立後，Router1上的ACL計數器會穩定下來，而且沒有進一步增加，這表示ACL規則已匹配，現在始終允許流量通過已建立的通道。

3. 通道重新啟動：
   只有當通道捨棄並需要重新建立時，Router1上的ACL計數器會再次增加。這表示ACL規則由嘗試建立通道的初始流量發起觸發，而不是在通道處於活動狀態後通過持續的資料傳輸觸發。

總而言之，此案例展示Router1上的ACL計數器對建立通道的初始流量嘗試是敏感的，但當VPN通道啟動並運作時仍保持靜態。

```
csr1#ping 10.106.45.145 source 10.106.67.27
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.106.45.145, timeout is 2 seconds:
Packet sent with a source address of 10.106.67.27
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
csr1#
csr1#
csr1#
csr1#sh acces
csr1#sh access-li
csr1#sh access-lists new_acl
Extended IP access list new_acl
    10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
    20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
    30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
csr1#
csr1#
csr1#
csr1#ping 10.106.45.145 source 10.106.67.27
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.106.45.145, timeout is 2 seconds:
Packet sent with a source address of 10.106.67.27
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
csr1#
csr1#sh access-lists new_acl
Extended IP access list new_acl
    10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
    20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
    30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
```

```
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#sh acces
csr2#sh access-li
csr2#sh access-lists new_acl
Extended IP access list new_acl
    20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
    30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
    40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#sh access-lists new_acl
Extended IP access list new_acl
    20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
    30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
    40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
csr2#
csr2#
csr2#
csr2#
```

案例1

場景二：VPN隧道處於活動狀態時從Router2發起的流量

初始狀態：

連線Router1的VPN通道(IP:10.106.67.27)和Router2(IP:10.106.45.145)當前處於活動狀態且運行正常。

已採取的行動：

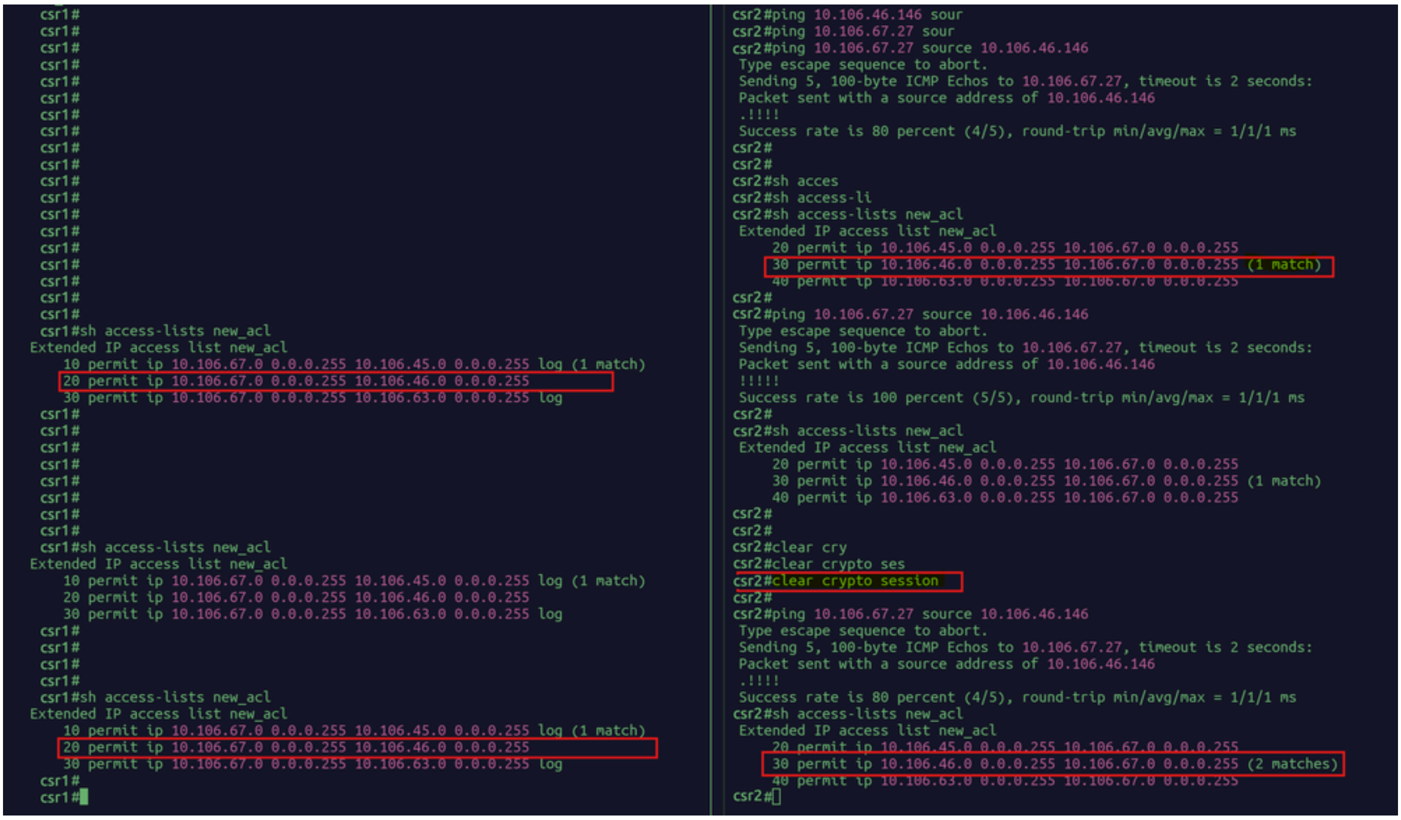
1. 通道開啟時，流量會從Router2向Router1發出。
2. 接下來，通道會故意清除（或重設）。
3. 清除通道後，Router2會再次啟動流量以重新建立連線。

意見：

1. 初始流量啟動：
   a.當流量首次從Router2啟動而通道已建立時，存取控制清單(ACL)計數器不會立即變更。
   b.這表示已建立通道中的持續流量不會觸發ACL計數器的增量。
2. 通道清除和重新啟動：
   a.清除通道後，第一個和Router2之間建立的連線會暫時中斷。這就需要針對任何後續流量執行重建過程。
   b.在清除通道後，從Router2重新發起流量時，Router2上的ACL計數器中有可觀察的增量。此增量表示正在再次使用ACL規則以方便建立通道。
3. ACL計數器特異性：

ACL計數器的增量僅發生在發起流量的那一端（本例中為Router2）。此行為突出顯示ACL在監控發起端流量發起過程方面的作用，而Router1的ACL計數器在此階段不受影響。

總而言之，此案例說明Router2上的ACL計數器在重新建立VPN通道時會對流量發起作出回應。計數器不會隨活動隧道內的常規流量增加，而是響應隧道重建的需要，確保精確跟蹤隧道啟動事件。



案例 2

結論:

加密ACL計數器的行為顯示它們在VPN隧道的啟動階段以獨佔方式註冊命中計數。

特定於啟動器的增量：從Router1啟動通道時，只會在Router1上看到命中次數的增加。同樣，如果從Router2啟動，則只會在Router2上增加命中次數。這突出說明了ACL在監控來源上的流量啟動流程方面的作用。

建立後的穩定性：成功建立通道後，兩個對等點上的ACL計數器會保持不變，表示沒有進一步的命中。此穩定性會一直持續，直到通道被清除或重置，然後再次嘗試流量啟動。
此行為強調了訪問控制清單在跟蹤和控制隧道建立的初始階段方面的功能，從而確保已建立的隧道內的後續資料流不會影響命中計數。

要點：

ACL計數器行為：在隧道啟動過程中，ACL計數器僅在發起方一側註冊增量。這表示計數器設計為監控觸發通道建立的初始流量。

靜態計數器建立後：一旦通道處於作用中且已建立，ACL計數器將保持不變。除非通道重設，否則

它們不會反映任何進一步的活動，且需要重新啟動，這突出表明需要關注初始流量事件。

流量啟動特異性：ACL命中計數特定於發起通道的對等體。這種專用性可確保準確跟蹤哪一方負責發起VPN連線，從而進行準確的監控和控制。

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）。