啟用AVC流量通過IPSec隧道介面的解決方法

目錄

簡介

本檔案將說明將AVC流量通過IPSEC通道傳送到收集器所需的組態。預設情況下，無法通過IPSEC隧道將AVC資訊匯出到收集器

必要條件

思科建議您瞭解以下主題的基本知識：

- 應用可視性與可控性(AVC)
- 簡易效能監控器(EzPM)

背景資訊

Cisco AVC功能用於識別、分析和控制多個應用。AVC將應用感知功能內建到網路基礎設施中，並且可瞭解網路上運行的應用的效能，從而支援每個應用的策略，以精細控制應用頻寬的使用，從而提供更好的終端使用者體驗。在此處，您可以找到有關此技術的更多詳細資訊。

EzPM是配置傳統效能監控配置的更快且更簡單的方法。目前，EzPM無法提供傳統效能監控器配置模型的完全靈活性。在此您可以找到有關EzPM的更多詳細資訊。

限制

目前AVC不支援通道隧道協定的數量，您可以在此處找到詳細信息。

網際網路通訊協定安全(IPSec)是AVC不受支援的傳遞通道通訊協定之一，本檔案將說明針對此限制的可能因應措施。

設定

本節介紹用於模擬給定限制的完整配置。

網路圖表

在此網路圖中，所有路由器都可以使用靜態路由相互通訊。R1配置了EzPM配置，並且與R2路由器建立了一個IPSec隧道。R3在此處充當匯出器，匯出器可能是Cisco Prime或能夠收集效能資料的任何其他型別的匯出器。

AVC流量由R1生成，並通過R2傳送到匯出器。R1通過IPSec隧道介面將AVC流量傳送到R2。

初始配置

本節介紹R1到R3的初始配置。

R1

```
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!

interface GigabitEthernet0/1

 ip address 172.16.1.1 255.255.255.0

 雙工自動

 速度自動

!

ip route 0.0.0.0 0.0.0.0 172.16.1.2

!
```

R2

```
!

interface GigabitEthernet0/0/0
```

```
 ip address 172.16.2.2 255.255.255.0
 自動交涉
 !
interface GigabitEthernet0/0/1
 ip address 172.16.1.2 255.255.255.0
 自動交涉
!
```

R3

```
!
interface GigabitEthernet0/0
 ip address 172.16.2.1 255.255.255.0
 雙工自動
 速度自動
!
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
```

IPSec配置

本節介紹R1和R2路由器的IPSec配置。

R1

```
!
ip access-list extended IPSec_Match
 permit ip any host 172.16.2.1
!
crypto isakmp policy 1
 encr aes 256
 hash md5
```

身份驗證預共用

組2

```
crypto isakmp key cisco123 address 172.16.1.2
!
!
crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac
```

模式隧道

```
!
!
crypto map VPN 10 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set set2
 match address IPSec_Match
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
```

雙工自動

速度自動

密碼編譯對應VPN

```
!
```

R2

```
!
ip access-list extended IPSec_Match
 permit ip host 172.16.2.1 any
!
crypto isakmp policy 1
```

encr aes 256

hash md5

身份驗證預共用

組2

crypto isakmp key cisco123 address 172.16.1.1

!

!

crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac

模式隧道

!

!

crypto map VPN 10 ipsec-isakmp

set peer 172.16.1.1

set transform-set set2

match address IPSec_Match

反向路由

!

interface GigabitEthernet0/0/1

ip address 172.16.1.2 255.255.255.0

自動交涉

cdp enable

密碼編譯對應VPN

!

要驗證IPSec配置是否按預期工作，請檢查**show crypto isakmp sa**的輸出

```
R1#show crypto isakmp sa

IPv4ISAKMP SA

dst src state conn-id status
```

```
IPv6ISAKMP SA
```

為了建立安全關聯，請從R1 ping匯出器(R3, 172.16.2.1)。

```
R1#ping 172.16.2.1


172.16.2.15100ICMP2

!!!!!

100%(5/5)//= 1/1/4

R1#
```

現在，路由器將具有活動安全關聯，確認源自R1且目的地為匯出器的流量是ESP封裝的。

```
R1#show crypto isakmp sa

IPv4ISAKMP SA

dst src state conn-id status

172.16.1.2 172.16.1.1 QM_IDLE 1002

IPv6ISAKMP SA
```

EzPM配置

本節介紹R1路由器的EzPM配置。

R1

```
!
class-map match-all perf-mon-acl
 說明PrimeAM生成的實體 — 不要修改或使用此實體
 match protocol ip
!
performance monitor context Performance-Monitor profile application-experience
 匯出器目標172.16.2.1源GigabitEthernet0/1傳輸udp埠9991
 traffic-monitor application-traffic-stats
 traffic-monitor conversation-traffic-stats ipv4
```

```
 traffic-monitor application-response-time ipv4

 traffic-monitor media ipv4 ingress

 traffic-monitor media ipv4 egress

 traffic-monitor url ipv4 class-replace perf-mon-acl

!
```

在需要監控的介面上套用EzPM設定檔；此處我們監控loopback 0介面。

R1

```
!

interface Loopback0

 ip address 1.1.1.1 255.255.255.255

 performance monitor context Performance-Monitor

!
```

因應措施

在以上配置就緒的情況下，獲取**show performance monitor** *contextcontext-***nameexporter**的輸出。

檢查**輸出功能**選項的狀態，預設情況下它應該處於**Not Used**狀態，這是預期的行為，也是此處未封裝或加密AVC流量的原因。

為了讓AVC流量通過IPsec隧道介面，**Output Features**選項應處於使用狀態。為此，必須在流匯出器配置檔案中顯式啟用它。以下是啟用此選項的詳細逐步程式。

步驟1

執行**show performance monitor context** *context-name* configuration 命令的完整輸出，並將其儲存在記事本中。以下是此輸出的片段，

```
R1#show performance monitor context Performance-Monitor

!================================================================================
========

!            Context Performance-Monitor

!================================================================================
========



!==========
```

```
!
flow exporter Performance-Monitor-1
 description performance monitor context Performance-Monitor
 172.16.2.1
 GigabitEthernet0/1
 udp 9991
 export-protocol ipfix
 300
 option interface-table timeout 300
 vrf-table timeout 300
 c3pl-class-table timeout 300
 c3pl-policy-table timeout 300
 300
 option application-table timeout 300
 option application-attributes timeout 300
 300
------------------------snip-------------------------
```

步驟2

在流匯出器配置檔案下顯式新增**output-features**選項。新增輸出功能選項後，流匯出器配置檔案應如下所示，

```
flow exporter Performance-Monitor-1
 description performance monitor context Performance-Monitor匯出程式
 目的地172.16.2.1
 源GigabitEthernet0/1
 傳輸udp 9991
 export-protocol ipfix
 模板資料超時300
```

output-features

option interface-table timeout 300

選項vrf-table timeout 300

選項c3pl-class-table timeout 300

選項c3pl-policy-table timeout 300

選項取樣器表超時300

option application-table timeout 300

option application-attributes timeout 300

選項子應用程式表超時300

保留輸出的其餘部分，不要更改輸出中的任何其他內容。

步驟3

現在，從介面和路由器中刪除EzPM配置檔案。

!

Interface loopback 0

no performance monitor context Performance-Monitor

exit

!

!

no performance monitor context Performance-Monitor profile application-experience

!

步驟4

在R1路由器上應用修改後的配置。請確保沒有遺漏任何一個命令，因為它可能會導致任何意外行為。

驗證

本節介紹本文中所用的檢查驗證方法，以及此解決方法如何幫助克服此處提到的AVC封包限制。

在應用此解決方法之前，IPSec對等路由器(R2)收到的資料包將被丟棄。還將生成以下消息：

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC:IPSECdest_addr= 172.16.2.1,src_addr=
```

```
172.16.1.1= 17
```

這裡R2期望收到目的地為172.16.2.1的ESP封裝資料包，但收到的資料包是純UDP資料包(prot=17)，丟棄這些資料包的行為是預期的。下面的資料包捕獲顯示，在R2收到的資料包是純UDP資料包，而不是ESP封裝的資料包，這是AVC的預設行為。

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.2.1 (172.16.2.1)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1348
  Identification: 0x961a (38426)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
⊞ Header checksum: 0xc56b [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.2.1 (172.16.2.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50208 (50208), Dst Port: 9991 (9991)
  Source Port: 50208 (50208)
  Destination Port: 9991 (9991)
  Length: 1328
⊞ Checksum: 0xb7ec [validation disabled]
  [Stream index: 0]
Data (1320 bytes)
```

在應用此解決方法之後，從下面的資料包捕獲中可清楚地看到，在R2上收到的AVC資料包是ESP封裝的，在R2上不會再出現錯誤消息。

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1448
  Identification: 0x0114 (276)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: Encap Security Payload (50)
⊞ Header checksum: 0x5aec [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.1.2 (172.16.1.2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Encapsulating Security Payload
  ESP SPI: 0x804c46a3 (2152482467)
  ESP Sequence: 203
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。