Problemumgehung zur Aktivierung des AVC-Datenverkehrs durch die IPSec-Tunnelschnittstelle

Inhalt

Einführung

Dieses Dokument beschreibt die erforderliche Konfiguration für die Weiterleitung von AVC-Datenverkehr über einen IPSEC-Tunnel an den Collector. AVC-Informationen können standardmäßig nicht über einen IPSEC-Tunnel in den Collector exportiert werden.

Voraussetzungen

Cisco empfiehlt, dass Sie über die folgenden grundlegenden Kenntnisse verfügen:

- Application Visibility and Control (AVC)
- Easy Performance Monitor (EzPM)

Hintergrundinformationen

Die Cisco AVC-Funktion dient der Erkennung, Analyse und Steuerung mehrerer Anwendungen.

Dank der in die Netzwerkinfrastruktur integrierten Anwendungserkennung sowie der Transparenz der Leistung von im Netzwerk ausgeführten Anwendungen ermöglicht AVC eine anwendungsspezifische Richtlinie für eine präzise Kontrolle der Bandbreitennutzung von Anwendungen, was zu einer besseren Endbenutzererfahrung führt. Hier finden Sie weitere Informationen zu dieser Technologie.

EzPM ist eine schnellere und einfachere Möglichkeit, die herkömmliche Konfiguration der Leistungsüberwachung zu konfigurieren. EzPM bietet derzeit nicht die volle Flexibilität des herkömmlichen Konfigurationsmodells für den Leistungsmonitor. Hier finden Sie weitere Informationen über EzPM.

Einschränkung

Derzeit unterstützt AVC nicht die Anzahl der Pass-Through-Tunneling-Protokolle. Einzelheiten hierzu finden Sie hier.

Internet Protocol Security (IPSec) ist eines der nicht unterstützten Pass-Through-Tunneling-Protokolle für AVC. Dieses Dokument behandelt die mögliche Problemumgehung für diese Einschränkung.

Konfigurieren

In diesem Abschnitt wird die vollständige Konfiguration beschrieben, die zur Simulation der gegebenen Einschränkung verwendet wird.

Netzwerkdiagramm

In diesem Netzwerkdiagramm sind alle Router untereinander über die statischen Routen erreichbar. R1 ist mit der EzPM-Konfiguration konfiguriert und hat einen IPSec-Tunnel mit dem R2-Router eingerichtet. R3 ist hier als Exporteur tätig, was Cisco Prime oder jeder andere Exporteur sein könnte, der in der Lage ist, die Leistungsdaten zu erfassen.

AVC-Datenverkehr wird von R1 generiert und über R2 an den Exporteur gesendet. R1 sendet den AVC-Datenverkehr über eine IPSec-Tunnelschnittstelle an R2.

Erstkonfiguration

In diesem Abschnitt wird die Erstkonfiguration für R1 bis R3 beschrieben.

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
```

```
 Duplexauto
 Geschwindigkeitsauto
!
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
 Verhandlungsauto
 !
interface GigabitEthernet0/0/1
 ip address 172.16.1.2 255.255.255.0
 Verhandlungsauto
!
```

R3

```
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
 Duplexauto
 Geschwindigkeitsauto
!
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
```

IPSec-Konfiguration

In diesem Abschnitt wird die IPSec-Konfiguration für R1- und R2-Router beschrieben.

R1

```
!
ip access-list erweitertes IPSec_Match
 permit ip any host 172.16.2.1
!
crypto isakmp-Richtlinie 1
 encr aes 256
 Hash md5
 Authentifizierung Pre-Share
 Gruppe 2
crypto isakmp key cisco123 address 172.16.1.2
!
!
crypto ipsec-Transformations-Set2 esp-aes 256 esp-sha-hmac
 Modustunnel
!
!
crypto map VPN 10 ipsec-isakmp
 set peer 172.16.1.2
 Set-Transformationssatz2
 Match-Adresse IPSec_Match
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 Duplexauto
 Geschwindigkeitsauto
```

```
 Crypto Map VPN
!
```

R2

```
!
ip access-list erweitertes IPSec_Match
 permit ip host 172.16.2.1 any
!
crypto isakmp-Richtlinie 1
 encr aes 256
 Hash md5
 Authentifizierung Pre-Share
 Gruppe 2
crypto isakmp key cisco123 address 172.16.1.1
!
!
crypto ipsec-Transformations-Set2 esp-aes 256 esp-sha-hmac
 Modustunnel
!
!
crypto map VPN 10 ipsec-isakmp
 set peer 172.16.1.1
 Set-Transformationssatz2
 Match-Adresse IPSec_Match
 Umleitung
!
interface GigabitEthernet0/0/1
```

ip address 172.16.1.2 255.255.255.0

Verhandlungsauto

cdp enable

Crypto Map VPN

!

Um zu überprüfen, ob die IPSec-Konfiguration wie erwartet funktioniert oder nicht, überprüfen Sie die Ausgabe für **show crypto isakmp sa**

```
R1#show crypto isakmp sa

IPv4-Verschlüsselung ISAKMP SA

dst src state conn-id status

IPv6 Crypto ISAKMP SA
```

Um die Sicherheitsverknüpfungen zu aktivieren, pingen Sie den Exporteur (R3, 172.16.2.1) von R1.

```
R1#ping 172.16.2.1

Geben Sie die Escape-Sequenz ein, um abzubrechen.

Beim Senden von 5 100-Byte-ICMP-Echos an 172.16.2.1 beträgt die
Zeitüberschreitung 2 Sekunden:

!!!!!

Die Erfolgsrate beträgt 100 Prozent (5/5), Round-Trip
min/durchschn./max. = 1/1/4 ms

R1#
```

Der Router verfügt nun über eine aktive Sicherheitszuordnung, die bestätigt, dass der vom R1 stammende und für den Exporteur bestimmte Datenverkehr ESP-gekapselt ist.

```
R1#show crypto isakmp sa

IPv4-Verschlüsselung ISAKMP SA

dst src state conn-id status

172.16.1.2 172.16.1.1 QM_IDLE 1002 AKTIV

IPv6 Crypto ISAKMP SA
```

EzPM-Konfiguration

In diesem Abschnitt wird die EzPM-Konfiguration für den R1-Router beschrieben.

R1

!

class-map match-all perf-mon-acl

Beschreibung von PrimeAM generierter Einheit - Diese Entität darf nicht geändert oder verwendet werden.

Übereinstimmungsprotokoll IP

!

Performance Monitor Context Performance Monitor-Profil Anwendungsumgebung

Export Ziel 172.16.2.1 Quelle GigabitEthernet0/1 Transport udp port 9991

Datenverkehrsstatistiken für Anwendungen

Verkehrsüberwachung - Verkehrsstatus - IPv4

Datenverkehrsüberwachung Anwendungs-Reaktionszeit IPv4

Datenverkehrsüberwachungsmedium IPv4-Eingang

Datenverkehrsüberwachungsmedium IPv4-Ausgang

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

!

Wenden Sie das EzPM-Profil auf die zu überwachende Schnittstelle an. hier wird die Loopback 0-Schnittstelle überwacht.

R1

!

interface Loopback0

ip address 1.1.1.1 255.255.255.255

Performance Monitor Context Performance Monitor

!

Problemumgehung

Wenn die obige Konfiguration vorhanden ist, übernehmen Sie die Ausgabe für den Show

Performance Monitor *Context*-**Name Exporteur**.

Überprüfen Sie den Status der Option **Output Features** (**Ausgabefunktionen**). Der Status sollte standardmäßig im Zustand **Nicht verwendet** sein. Dies ist ein erwartetes Verhalten, weshalb der AVC-Datenverkehr hier nicht gekapselt oder verschlüsselt wird.

Damit der AVC-Datenverkehr die IPsec-Tunnelschnittstelle passieren kann, muss die Option **Output Features** verwendet werden. Dazu muss sie explizit im Flow Exporter-Profil aktiviert werden. Im Folgenden finden Sie eine detaillierte schrittweise Anleitung zum Aktivieren dieser Option.

Schritt 1

Speichern Sie die vollständige Ausgabe für den **Konfigurationsbefehl show performance monitor** *context-name* und speichern Sie sie in notepad. Im Folgenden sehen Sie den Snip für diese Ausgabe.

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

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

! Entsprechende Konfiguration von Context Performance Monitor !

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

!Exporter

!=========

!

Flow Exporter Performance-Monitor-1

 description performance monitor context Performance Monitor exporteur

 Ziel 172.16.2.1

 source GigabitEthernet0/1

 Transportudp 9991

 export-protokoll ipfix

 Timeout für Vorlagendaten 300

 option interface-table timeout 300

 Option VRF-Tabelle Timeout 300

 Option c3pl-class-table timeout 300
```

```
 Option c3pl-policy-table timeout 300

 Zeitüberschreitung der Samplertabelle der Option 300

 Option Zeitüberschreitung der Anwendungstabelle 300

 Option Anwendungs-Attribute Timeout 300

 Option sub-application-table timeout 300

—snip—
```

Schritt 2

Fügen Sie die Option **Output-Features** explizit unter dem Flow Exporter-Profil hinzu. Nach dem Hinzufügen der Option "Output features" muss das Flow Exporter-Profil wie folgt aussehen:

Flow Exporter Performance-Monitor-1

description performance monitor context Performance Monitor exporteur

Ziel 172.16.2.1

source GigabitEthernet0/1

Transportudp 9991

export-protokoll ipfix

Timeout für Vorlagendaten 300

Ausgabefunktionen

option interface-table timeout 300

Option VRF-Tabelle Timeout 300

Option c3pl-class-table timeout 300

Option c3pl-policy-table timeout 300

Zeitüberschreitung der Samplertabelle der Option 300

Option Zeitüberschreitung der Anwendungstabelle 300

Option Anwendungs-Attribute Timeout 300

Option sub-application-table timeout 300

Belassen Sie den Rest der Ausgabe so, wie er ist, und ändern Sie KEINE anderen Elemente in der Ausgabe.

Schritt 3

Entfernen Sie jetzt das EzPM-Profil von der Schnittstelle und auch vom Router.

!

Schnittstellen-Loopback 0

Kein Performance Monitor Context Performance Monitor

Ausgang

!

!

Keine Leistungsüberwachung Kontext Performance Monitor-Profil Anwendungsumgebung

!

Schritt 4

Wenden Sie die geänderte Konfiguration auf dem R1-Router an. Vergewissern Sie sich, dass nicht ein einziger Befehl ausgelassen wird, da er ein unerwartetes Verhalten verursachen kann.

Überprüfen

In diesem Abschnitt wird die in diesem Dokument verwendete Überprüfungsmethode beschrieben. Außerdem wird erläutert, wie diese Problemumgehung dazu beigetragen hat, die hier genannten Einschränkungen bei AVC-Paketen zu überwinden.

Vor der Anwendung der Problemumgehung werden vom IPSec-Peer-Router (R2) empfangene Pakete verworfen. Die folgende Nachricht wird ebenfalls generiert:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Rec'd-Paket kein IPSEC-Paket, dest_addr=
172.16.2.1, src_addr= 172.16.1.1, prot= 17
```

Hier erwartet R2 gekapselte ESP-Pakete, die für 172.16.2.1 bestimmt sind, aber bei den empfangenen Paketen handelt es sich um reine UDP-Pakete (Port=17). Es wird erwartet, dass diese Pakete verworfen werden. Die unten dargestellte Paketerfassung zeigt, dass es sich bei dem bei R2 empfangenen Paket um ein reines UDP-Paket anstatt um ein gekapseltes ESP handelt. Dies ist ein Standardverhalten für AVC.

```
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)
```

Nach der Anwendung der Problemumgehung wird aus der folgenden Paketerfassung deutlich, dass die bei R2 empfangenen AVC-Pakete ESP-gekapselt sind und auf dem R2 keine weiteren Fehlermeldungen mehr angezeigt werden.

```
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
```

Fehlerbehebung

Derzeit sind für diese Konfiguration keine spezifischen Informationen zur Fehlerbehebung verfügbar.