Contenido

Introducción

Este documento describe la configuración requerida para pasar el tráfico AVC a través de un túnel IPsec al colector. Por abandono, la información AVC no se puede exportar a través de un túnel IPsec al colector

Prerrequisitos

Cisco recomienda que usted tiene el conocimiento básico de estos temas:

- Visibilidad y control (AVC) de la aplicación
- Monitor de rendimiento fácil (EzPM)

Antecedentes

La característica de Cisco AVC se utiliza para reconocer, para analizar y para controlar sobre las aplicaciones múltiples. Con la conciencia de la aplicación incorporada a la infraestructura de red, más la visibilidad al funcionamiento de las aplicaciones que se ejecutan en la red, directiva de la por-aplicación de los permisos AVC para el control granular del uso del ancho de banda de la aplicación, dando por resultado una mejor experiencia del usuario final. Aquí usted puede encontrar más detalles sobre esta tecnología.

EzPM es una manera más rápida y más fácil de configurar la configuración tradicional de la

supervisión de rendimiento. EzPM no hace actualmente proporciona la flexibilidad completa del modelo tradicional de la configuración del monitor de rendimiento. Aquí usted puede encontrar más detalles sobre EzPM.

Limitación

AVC no soporta actualmente el número de protocolos de túneles del paso, los detalles se puede encontrar aquí.

La seguridad de protocolos en Internet (IPSec) es uno de los protocolos de túneles sin apoyo del paso para AVC y este documento dirige la solución alternativa posible para esta limitación.

Configurar

Esta sección describe la configuración completa usada para simular la limitación dada.

Diagrama de la red

En este diagrama de la red todo el Routers tiene accesibilidad el uno al otro usando las Static rutas. El r1 se configura con la configuración de EzPM y tiene un túnel IPsec establecido con el router del r2. El R3 está trabajando como exportador aquí, que podría ser prima de Cisco o cualquier otra clase de exportador que es capaz de recoger los Datos del rendimiento.

El tráfico AVC es generado por el r1 y se envía al exportador vía el r2. El r1 envía el tráfico AVC al r2 sobre una interfaz del túnel IPsec.

Configuración inicial

Esta sección describe la configuración inicial para el r1 con el R3.

R1

```
¡!
loopback0 de la interfaz
dirección IP 1.1.1.1 255.255.255.255
¡!

interfaz GigabitEthernet0/1

 dirección IP 172.16.1.1 255.255.255.0

 auto dúplex

 auto de la velocidad

¡!

ruta de IP 0.0.0.0 0.0.0.0 172.16.1.2
```

¡!

R2

¡!

interfaz GigabitEthernet0/0/0

 dirección IP 172.16.2.2 255.255.255.0

 negotiation auto

 ¡!

interfaz GigabitEthernet0/0/1

 dirección IP 172.16.1.2 255.255.255.0

 negotiation auto

¡!

R3

¡!

interfaz GigabitEthernet0/0

 dirección IP 172.16.2.1 255.255.255.0

 auto dúplex

 auto de la velocidad

¡!

ruta de IP 0.0.0.0 0.0.0.0 172.16.2.2

¡!

Configuración IPSec

Esta sección describe la configuración IPSec para el router del r1 y del r2.

R1

¡!

lista de acceso IPSec_Match extendido del IP

 IP ninguno del permiso host 172.16.2.1

¡!

política isakmp crypto 1

aes 256 del encr

md5 del hash

authentication pre-share

group2

direccionamiento crypto 172.16.1.2 del cisco123 de la clave del isakmp

¡!

¡!

esp-sha-hmac crypto del ESP-aes 256 del transforme el conjunto set2 del IPSec

túnel del modo

¡!

¡!

correspondencia de criptografía VPN 10 IPSec-ISAKMP

fije al par 172.16.1.2

fije el transforme el conjunto set2

haga juego el direccionamiento IPSec_Match

¡!

interconecte GigabitEthernet0/1

dirección IP 172.16.1.1 255.255.255.0

auto dúplex

auto de la velocidad

correspondencia de criptografía VPN

¡!

R2

¡!

```
lista de acceso IPSec_Match extendido del IP
 host 172.16.2.1 del IP del permiso
¡!
política isakmp crypto 1
 aes 256 del encr
 md5 del hash
 authentication pre-share
 group2
direccionamiento crypto 172.16.1.1 del cisco123 de la clave del isakmp
¡!
¡!
esp-sha-hmac crypto del ESP-aes 256 del transforme el conjunto set2 del IPSec
 túnel del modo
¡!
¡!
correspondencia de criptografía VPN 10 IPSec-ISAKMP
 fije al par 172.16.1.1
 fije el transforme el conjunto set2
 haga juego el direccionamiento IPSec_Match
 reverso-ruta
¡!
interfaz GigabitEthernet0/0/1
 dirección IP 172.16.1.2 255.255.255.0
 negotiation auto
 permiso cdp
 correspondencia de criptografía VPN
¡!
```

Para verificar si el config del IPSec esté trabajando como se esperaba o no, marque la salida para **isakmp crypto sa de la demostración**

```
Isakmp crypto sa R1#show

ISAKMP Crypto SA del IPv4

estatus CONN-identificación del estado del src del dst

ISAKMP Crypto SA del IPv6
```

Para sacar a colación las asociaciones de seguridad, haga ping el exportador (R3, 172.16.2.1) del r1.

```
R1#ping 172.16.2.1

Ingrese escape sequence para abortar.

Enviando 5, el echos del 100-byte ICMP a 172.16.2.1, descanso es 2
segundos:

¡!!!!!

El índice de éxito es el 100 por ciento (5/5), minuto ida-vuelta/avg/=
1/1/4 ms máximo

R1#
```

Ahora, el router tendrá una asociación de la seguridad activa, que confirma que el tráfico que es originado del r1 y destinado al exportador es ESP encapsulado.

```
Isakmp crypto sa R1#show

ISAKMP Crypto SA del IPv4

estatus CONN-identificación del estado del src del dst

ACTIVE DEL QM_IDLE 1002 DE 172.16.1.2 172.16.1.1

ISAKMP Crypto SA del IPv6
```

Configuración de EzPM

Esta sección describe la configuración de EzPM para el router del r1.

R1

```
¡!

clase-mapa perforación-lunes-ACL corresponda con todos

 entidad generada PrimeAM de la descripción - no modifique ni utilice esta entidad
```

haga juego el protocol ip

¡!

aplicación-experiencia del perfil del monitor de rendimiento del contexto del monitor de rendimiento

puerto 9991 UDP del transporte de la fuente GigabitEthernet0/1 de 172.16.2.1 del destino del exportador

aplicación-tráfico-stats del control de tráfico

conversación-tráfico-stats ipv4 del control de tráfico

Application Response Time ipv4 del control de tráfico

ingreso de los media ipv4 del control de tráfico

salida de los media ipv4 del control de tráfico

clase-reemplace perforación-lunes-ACL URL ipv4 del control de tráfico

¡!

Aplique el perfil de EzPM en la interfaz que las necesidades de ser monitoreado; aquí estamos monitoreando la interfaz del loopback0.

R1

¡!

loopback0 de la interfaz

dirección IP 1.1.1.1 255.255.255.255

monitor de rendimiento del contexto del monitor de rendimiento

¡!

Solución Aternativa

Con la configuración antedicha en el lugar, tome la salida para el **contextcontext-nameexporter del monitor de rendimiento de la demostración**.

Marque para saber si hay el estatus de la opción de las **funciones de resultados**, por abandono debe estar en el estado **no usado**, que es una conducta esperada y por eso el tráfico AVC no se está encapsulando ni se está cifrando aquí.

Para dejar el tráfico AVC pase a través de la interfaz del túnel IPsec, las **funciones de resultados que la** opción estará en el estado usado. Y para hacer eso, tiene que ser habilitada explícitamente en el perfil del exportador del flujo. Abajo está el procedimiento paso a paso detallado para habilitar esta opción.

Step-1

Tome el resultado completo para el **comando configuration del** *nombre del contexto del* **contexto del monitor de rendimiento de la demostración** y sálvelo en la libreta. Abajo está el recorte para esta salida,

```
Configuración del monitor de rendimiento del contexto del monitor de
rendimiento R1#show

¡!
=============================================================================
=======

¡!            ¡Configuración equivalente del monitor de rendimiento del
contexto!

¡!
=============================================================================
=======

¡! Exportadores

¡! ==========

¡!

exportador Performance-Monitor-1 del flujo

 exportador del monitor de rendimiento del contexto del monitor de
rendimiento de la descripción

 destino 172.16.2.1

 fuente GigabitEthernet0/1

 UDP 9991 del transporte

 ipfix del exportación-protocolo

 plantilla se agotó el tiempo de espera de datos 300

 descanso 300 de la interfaz-tabla de la opción

 descanso 300 de la VRF-tabla de la opción

 descanso 300 de la opción c3pl-class-table

 descanso 300 de la opción c3pl-policy-table

 descanso 300 de la dechado-tabla de la opción

 descanso 300 de la aplicación-tabla de la opción
```

```
 descanso 300 de los aplicación-atributos de la opción

 descanso 300 de la sub-aplicación-tabla de la opción

----------------------recorte-----------------------
```

Step-2

Agregue la opción de las **funciones de resultados** explícitamente bajo perfil del exportador del flujo. Después de agregar la opción de las funciones de resultados el perfil del exportador del flujo parecerá esto,

```
exportador Performance-Monitor-1 del flujo

 exportador del monitor de rendimiento del contexto del monitor de rendimiento de la descripción

 destino 172.16.2.1

 fuente GigabitEthernet0/1

 UDP 9991 del transporte

 ipfix del exportación-protocolo

 plantilla se agotó el tiempo de espera de datos 300

funciones de resultados

 descanso 300 de la interfaz-tabla de la opción

 descanso 300 de la VRF-tabla de la opción

 descanso 300 de la opción c3pl-class-table

 descanso 300 de la opción c3pl-policy-table

 descanso 300 de la dechado-tabla de la opción

 descanso 300 de la aplicación-tabla de la opción

 descanso 300 de los aplicación-atributos de la opción

 descanso 300 de la sub-aplicación-tabla de la opción
```

Deje el resto de la salida como es, no alteran cualquier otra cosa en la salida.

Step-3

Ahora, quite el perfil de EzPM de la interfaz y del router también.

```
¡!

Loopback 0 de interfaz
```

ningún monitor de rendimiento del contexto del monitor de rendimiento

salida

¡!

¡!

ninguna aplicación-experiencia del perfil del monitor de rendimiento del contexto del monitor de rendimiento

¡!

Step-4

Aplique los config modificados en el router del r1. Aseegurese que no faltan a un comando único hacia fuera, puesto que puede causar cualquier conducta inesperada.

Verificación

Esta sección describe el método de verificación usado en este documento para marcar y cómo esta solución alternativa ha ayudado a superar la limitación para los paquetes AVC mencionados aquí.

Antes de aplicar la solución alternativa, los paquetes recibidos por el router de peer IPSec (r2) serán caídos. Debajo del mensaje será generado también:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Paquete de Rec'd no un paquete IPsec,
dest_addr= 172.16.2.1, src_addr= 172.16.1.1, prot= 17
```

Aquí el r2 está contando con los paquetes encapsulados ESP que son destinados para 172.16.2.1, pero los paquetes recibidos son los paquetes UDP llanos (prot=17) y es una conducta esperada para caer estos paquetes. Debajo de la captura de paquetes muestra que el paquete recibido en el r2 es un paquete UDP llano en vez del ESP encapsulado, que es un comportamiento predeterminado para 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)
```

Después de aplicar la solución alternativa, se ve claramente de la captura de paquetes abajo que los paquetes AVC recibidos en el r2 son ESP encapsulado y de no más de mensajes de error vistos en el r2.

```
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
```

Resolución de problemas

No hay actualmente información específica acerca de Troubleshooting disponible para esta configuración.