Contenu

Introduction

Ce document décrit la configuration exigée pour passer le trafic AVC par un tunnel IPSEC au collecteur. Par défaut, les informations AVC ne peuvent pas être exportées à travers un tunnel IPSEC au collecteur

Conditions préalables

Cisco recommande que vous ayez la connaissance de base de ces thèmes :

- Visibilité d'application et contrôle (AVC)
- Moniteur de performances facile (EzPM)

Informations générales

La caractéristique de Cisco AVC est utilisée pour reconnaître, analyser et contrôler au-dessus des applications multiples. La connaissance d'application étant établi dans l'infrastructure réseau, plus la visibilité dans la représentation des applications s'exécutant sur le réseau, stratégie de par-application d'enables AVC pour le contrôle granulaire de l'utilisation de bande passante d'application, ayant pour résultat une meilleure expérience utilisateur. Voici que vous pouvez trouver plus de détails au sujet de cette technologie.

EzPM est une manière plus rapide et plus facile de configurer la configuration traditionnelle de

supervision des performances. Actuellement EzPM ne fait pas fournit la pleine flexibilité du modèle traditionnel de configuration de moniteur de performances. Voici que vous pouvez trouver plus de détails au sujet d'EzPM.

Limite

Actuellement AVC ne prend en charge pas le nombre de protocoles de Tunnellisation d'intercommunication, des détails peut être trouvé ici.

L'IPSec (IPSec) est l'un des protocoles non vérifiés de Tunnellisation d'intercommunication pour AVC et ce document adresse le contournement possible pour cette limite.

Configurez

Cette section décrit la configuration complète utilisée pour simuler la limite indiquée.

Diagramme du réseau

Dans ce schéma de réseau tous les Routeurs ont l'accessibilité entre eux utilisant les artères statiques. R1 est configuré avec la configuration d'EzPM et a un tunnel d'IPSec établi avec le routeur R2. R3 fonctionne comme exportateur ici, qui pourrait être perfection de Cisco ou n'importe quel autre genre d'exportateur qui est capable de collecter les données de performance.

Le trafic AVC est généré par R1 et il est envoyé à l'exportateur par l'intermédiaire de R2. R1 envoie le trafic AVC à R2 au-dessus d'une interface de tunnel d'IPSec.

Configuration initiale

Cette section décrit la configuration initiale pour R1 par R3.

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

 automatique duplex

 speed auto

!

artère 0.0.0.0 0.0.0.0 172.16.1.2 d'IP
```

!

R2

!

interface GigabitEthernet0/0/0

 IP address 172.16.2.2 255.255.255.0

 negotiation auto

 !

interface GigabitEthernet0/0/1

 IP address 172.16.1.2 255.255.255.0

 negotiation auto

!

R3

!

interface GigabitEthernet0/0

 IP address 172.16.2.1 255.255.255.0

 automatique duplex

 speed auto

!

artère 0.0.0.0 0.0.0.0 172.16.2.2 d'IP

!

Configuration IPSec

Cette section décrit la configuration IPSec pour le routeur R1 et R2.

R1

!

ip access-list IPSec_Match étendu

 IP quel d'autorisation hôte 172.16.2.1

```
!
crypto isakmp policy 1
 aes 256 d'encr
 MD5 d'informations parasites
 authentication pre-share
 groupe 2
adresse 172.16.1.2 du crypto isakmp key cisco123
!
!
ESP-SHA-hmac du l'ESP-aes 256 du crypto ipsec transform-set set2
 tunnel de mode
!
!
ipsec-ISAKMP du crypto map VPN 10
 placez le pair 172.16.1.2
 set transform-set set2
 adresse IPSec_Match de correspondance
!
interface GigabitEthernet0/1
 IP address 172.16.1.1 255.255.255.0
 automatique duplex
 speed auto
 crypto map VPN
!
```

R2

```
!
```

```
ip access-list IPSec_Match étendu
 hôte 172.16.2.1 d'IP d'autorisation
!
crypto isakmp policy 1
 aes 256 d'encr
 MD5 d'informations parasites
 authentication pre-share
 groupe 2
adresse 172.16.1.1 du crypto isakmp key cisco123
!
!
ESP-SHA-hmac du l'ESP-aes 256 du crypto ipsec transform-set set2
 tunnel de mode
!
!
ipsec-ISAKMP du crypto map VPN 10
 placez le pair 172.16.1.1
 set transform-set set2
 adresse IPSec_Match de correspondance
 reverse-route
!
interface GigabitEthernet0/0/1
 IP address 172.16.1.2 255.255.255.0
 negotiation auto
 cdp enable
 crypto map VPN
!
```

Pour vérifier, que le config d'IPSec fonctionne comme prévu ou pas, vérifiez **crypto isakmp SA de** sortie en démonstration

```
Crypto isakmp SA R1#show

Crypto isakmp SA d'ipv4

état de conn.-id d'état de src de dst

Crypto isakmp SA d'IPv6
```

Afin d'évoquer les associations de sécurité, cinglez l'exportateur (R3, 172.16.2.1) de R1.

```
R1#ping 172.16.2.1

Séquence d'échappement de type à abandonner.

Envoyant 5, les échos de l'ICMP 100-byte à 172.16.2.1, délai d'attente
est de 2 secondes :

!!!!!

Le taux de réussite est de 100 pour cent (5/5), min/moy/max aller-retour
= 1/1/4 ms

R1#
```

Maintenant, le routeur aura une association de sécurité active, qui confirme que le trafic étant provenu de R1 et destiné à l'exportateur est l'ESP encapsulé.

```
Crypto isakmp SA R1#show

Crypto isakmp SA d'ipv4

état de conn.-id d'état de src de dst

ACTIVE DE 172.16.1.2 172.16.1.1 QM_IDLE 1002

Crypto isakmp SA d'IPv6
```

Configuration d'EzPM

Cette section décrit la configuration d'EzPM pour le routeur R1.

R1

```
!

class-map correspondance-tout perforation-Lun-acl

 entité générée par PrimeAM de description - ne modifiez pas ou utilisez cette entité
```

IP de match protocol

!

application-expérience de profil de moniteur de performances de contexte de moniteur de performances

port 9991 de transport udp de la source GigabitEthernet0/1 de 172.16.2.1 de destination d'exportateur

application-trafic-stats de trafic-moniteur

ipv4 de conversation-trafic-stats de trafic-moniteur

ipv4 de temps de réponse des applications de trafic-moniteur

d'entrée d'ipv4 de medias de trafic-moniteur

de sortie d'ipv4 de medias de trafic-moniteur

l'ipv4 URL de trafic-moniteur classe-remplacent le perforation-Lun-acl

!

Appliquez le profil d'EzPM sur l'interface qui les besoins d'être surveillé ; ici nous surveillons le bouclage 0 interfaces.

R1

!

interface Loopback0

IP address 1.1.1.1 255.255.255.255

moniteur de performances de contexte de moniteur de performances

!

Contournement

Avec la configuration ci-dessus en place, prenez le **contextcontext-nameexporter de moniteur de performances de** sortie en démonstration.

Vérifiez le statut d'option de **caractéristiques de sortie**, par défaut il devrait être dans l'état **non utilisé**, qui est un comportement prévu et c'est pourquoi le trafic AVC n'est pas encapsulé ou est chiffré ici.

Afin de permettre le trafic AVC de traverser l'interface de tunnel d'IPsec, l'option de **caractéristiques de sortie** sera dans l'état utilisé. Et pour faire cela, il doit être activé explicitement dans le profil de flow exporter. Est ci-dessous la procédure pas à pas détaillée pour activer cette option.

Étape 1

Prenez la commande de **configuration de contexte-***nom de* **contexte de moniteur de performances de** sortie complète en démonstration et sauvegardez-la en Notepad. Est ci-dessous le bout pour cette sortie,

```
Configuration de moniteur de performances de contexte de moniteur de
performances R1#show

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

!            Configuration équivalente de moniteur de performances de
contexte !

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

! Exportateurs

! ==========

!

flow exporter Performance-Monitor-1

 exportateur de moniteur de performances de contexte de moniteur de
performances de description

 destination 172.16.2.1

 source GigabitEthernet0/1

 transport udp 9991

 ipfix d'export-protocol

 template data timeout 300

 délai d'attente 300 d'interface-table d'option

 délai d'attente 300 de vrf-table d'option

 délai d'attente 300 de l'option c3pl-class-table

 délai d'attente 300 de l'option c3pl-policy-table

 délai d'attente 300 d'échantillonneur-table d'option

 délai d'attente 300 d'application-table d'option
```

```
 délai d'attente 300 d'application-attributs d'option

 délai d'attente 300 de sous-titre-application-table d'option

----------------------bout-----------------------
```

Step-2

Ajoutez l'option d'**output-features** explicitement sous le profil de flow exporter. Après avoir ajouté l'option d'output-features le profil de flow exporter ressemblera à ceci,

flow exporter Performance-Monitor-1

exportateur de moniteur de performances de contexte de moniteur de performances de description

destination 172.16.2.1

source GigabitEthernet0/1

transport udp 9991

ipfix d'export-protocol

template data timeout 300

output-features

délai d'attente 300 d'interface-table d'option

délai d'attente 300 de vrf-table d'option

délai d'attente 300 de l'option c3pl-class-table

délai d'attente 300 de l'option c3pl-policy-table

délai d'attente 300 d'échantillonneur-table d'option

délai d'attente 300 d'application-table d'option

délai d'attente 300 d'application-attributs d'option

délai d'attente 300 de sous-titre-application-table d'option

Quittez le reste de la sortie comme elle est, ne modifient pas toute autre chose dans la sortie.

Step-3

Maintenant, retirez le profil d'EzPM de l'interface et du routeur aussi bien.

!

Bouclage 0 d'interface

aucun moniteur de performances de contexte de moniteur de performances

sortie

!

!

aucune application-expérience de profil de moniteur de performances de contexte de moniteur de performances

!

Step-4

Appliquez le config modifié sur le routeur R1. Assurez-vous que pas une commande simple n'est manquée, puisqu'elle peut entraîner n'importe quel comportement inhabituel.

Vérifiez

Cette section décrit la méthode de vérification utilisée dans ce document pour vérifier et comment ce contournement a aidé à surmonter la limite pour des paquets AVC mentionnés ici.

Avant d'appliquer le contournement, des paquets reçus par le routeur de pair d'IPSec (R2) seront lâchés. Au-dessous du message sera aussi bien généré :

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC : Paquet de Rec'd pas un paquet IPSEC,
dest_addr= 172.16.2.1, src_addr= 172.16.1.1, prot= 17
```

Ici R2 attend les paquets encapsulés de l'ESP qui sont destinés à 172.16.2.1, mais les paquets reçus sont les paquets UDP ordinaires (prot=17) et c'est un comportement prévu pour relâcher ces paquets. Au-dessous du paquet la capture prouve que le paquet reçu à R2 est un paquet UDP ordinaire au lieu de l'ESP encapsulé, qui est un comportement par défaut pour 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)
```

Après application du contournement, on ne le voit clairement de la capture ci-dessous de paquet que les paquets AVC reçus à R2 sont l'ESP encapsulé et de plus de messages d'erreur vus sur le

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
```

Dépannage

Actuellement il n'y a aucune information de dépannage spécifique disponible pour cette configuration.