Soluzione per consentire al traffico AVC di passare attraverso l'interfaccia del tunnel IPSec

Sommario

Introduzione

In questo documento viene descritta la configurazione richiesta per il passaggio del traffico AVC al sistema di raccolta attraverso un tunnel IPSEC. Per impostazione predefinita, le informazioni AVC non possono essere esportate in un tunnel IPSEC al collector

Prerequisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Visibilità e controllo delle applicazioni (AVC)
- EzPM (Easy Performance Monitor)

Premesse

La funzione Cisco AVC viene utilizzata per riconoscere, analizzare e controllare più applicazioni. Grazie al riconoscimento delle applicazioni integrato nell'infrastruttura di rete e alla visibilità delle prestazioni delle applicazioni in esecuzione sulla rete, AVC consente di definire regole per singola

applicazione per il controllo granulare dell'utilizzo della larghezza di banda delle applicazioni, migliorando l'esperienza dell'utente finale. Qui puoi trovare ulteriori dettagli su questa tecnologia.

EzPM è un modo più semplice e veloce per configurare la configurazione tradizionale di monitoraggio delle prestazioni. Attualmente EzPM non offre la completa flessibilità del modello di configurazione tradizionale di Performance Monitor. Qui puoi trovare ulteriori dettagli su EzPM.

Limitazione

Attualmente AVC non supporta il numero di protocolli di tunneling pass-through. I dettagli sono disponibili qui.

IPSec (Internet Protocol Security) è uno dei protocolli di tunneling pass-through non supportati per AVC e in questo documento viene illustrata la possibile soluzione alternativa per questa limitazione.

Configurazione

Questa sezione descrive la configurazione completa utilizzata per simulare il limite specificato.

Esempio di rete

In questo diagramma di rete tutti i router sono raggiungibili l'uno con l'altro utilizzando le route statiche. R1 è configurato con la configurazione EzPM e dispone di un tunnel IPSec stabilito con il router R2. R3 lavora qui come esportatore, che potrebbe essere Cisco Prime o qualsiasi altro tipo di esportatore in grado di raccogliere i dati sulle prestazioni.

Il traffico AVC viene generato da R1 e inviato all'esportatore tramite R2. R1 invia il traffico AVC a R2 tramite un'interfaccia del tunnel IPSec.

Configurazione iniziale

In questa sezione viene descritta la configurazione iniziale per R1-R3.

R1

```
!
interfaccia Loopback0
indirizzo ip 1.1.1.1 255.255.255.255
!

interfaccia Gigabit Ethernet0/1

 indirizzo ip 172.16.1.1 255.255.255.0

 auto duplex

 speed auto
```

!

ip route 0.0.0.0 0.0.0.0 172.16.1.2

!

R2

!

interfaccia Gigabit Ethernet0/0/0

indirizzo ip 172.16.2.2 255.255.255.0

negoziazione automatica

!

interfaccia Gigabit Ethernet0/0/1

indirizzo ip 172.16.1.2 255.255.255.0

negoziazione automatica

!

R3

!

interfaccia Gigabit Ethernet0/0

indirizzo ip 172.16.2.1 255.255.255.0

auto duplex

speed auto

!

ip route 0.0.0.0 0.0.0.0 172.16.2.2

!

configurazione IPSec

In questa sezione viene descritta la configurazione IPSec per i router R1 e R2.

R1

!

```
ip access-list extended IPSec_Match
 allow ip any host 172.16.2.1
!
criterio crypto isakmp 1
 encr aes 256
 hash md5
 pre-condivisione di autenticazione
 gruppo 2
chiave crypto isakmp indirizzo cisco123 172.16.1.2
!
!
crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac
 tunnel in modalità
!
!
mappa crittografica VPN 10 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set set2
 corrispondenza indirizzo IPSec_Match
!
interfaccia Gigabit Ethernet0/1
 indirizzo ip 172.16.1.1 255.255.255.0
 auto duplex
 speed auto
 mappa crittografica VPN
!
```

R2

```
!
ip access-list extended IPSec_Match
 allow ip host 172.16.2.1 any
!
criterio crypto isakmp 1
 encr aes 256
 hash md5
 pre-condivisione di autenticazione
 gruppo 2
chiave crypto isakmp indirizzo cisco123 172.16.1.1
!
!
crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac
 tunnel in modalità
!
!
mappa crittografica VPN 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set set2
 corrispondenza indirizzo IPSec_Match
 invertire il percorso
!
interfaccia Gigabit Ethernet0/0/1
 indirizzo ip 172.16.1.2 255.255.255.0
 negoziazione automatica
```

```
 cdp enable

 mappa crittografica VPN

!
```

Per verificare se la configurazione IPSec funziona come previsto, controllare l'output del comando **show crypto isakmp sa**

```
R1#show crypto isakmp sa

SA IPv4 Crypto ISAKMP

stato conn-id stato src dst

SA IPv6 Crypto ISAKMP
```

Per richiamare le associazioni di sicurezza, eseguire il ping dell'esportatore (R3, 172.16.2.1) da R1.

```
R1#ping 172.16.2.1

Digitare la sequenza di escape da interrompere.

Invio di 5 echo ICMP da 100 byte a 172.16.2.1, il timeout è di 2
secondi:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#
```

Ora, il router avrà un'associazione di sicurezza attiva, che conferma che il traffico in provenienza dalla R1 e destinato all'esportatore è ESP incapsulato.

```
R1#show crypto isakmp sa

SA IPv4 Crypto ISAKMP

stato conn-id stato src dst

172.16.1.2 172.16.1.1 QM_IDLE 1002 ATTIVO

SA IPv6 Crypto ISAKMP
```

Configurazione EzPM

In questa sezione viene descritta la configurazione EzPM per il router R1.

R1

```
!
class-map match-all perf-mon-acl
 descrizione entità generata da PrimeAM - non modificare o utilizzare questa entità
 corrispondenza protocollo ip
!
contesto di monitoraggio prestazioni Performance-Monitor profilo esperienza applicazione
 destinazione dell'esportatore 172.16.2.1 origine Gigabit Ethernet0/1 trasporto udp port 9991
 monitoraggio del traffico applicazioni-statistiche
 traffic-monitor conversation-traffic-stats ipv4
 monitoraggio del traffico applicazione-tempo di risposta ipv4
 ingresso ipv4 media monitor di traffico
 uscita ipv4 media traffic-monitor
 traffic-monitor url ipv4 class-replace perf-mon-acl
!
```

applicare il profilo EzPM sull'interfaccia che deve essere monitorata; in questa sezione viene monitorata l'interfaccia 0 di loopback.

R1

```
!
interfaccia Loopback0
 indirizzo ip 1.1.1.1 255.255.255.255
 contesto di monitoraggio prestazioni Monitoraggio prestazioni
!
```

Soluzione alternativa

Con la configurazione precedente, utilizzare l'output per **show performance monitor** *contextcontext*-**name export**.

Verificare lo stato dell'opzione **Output Features**. Per impostazione predefinita, lo stato dell'opzione deve essere **Not Used**; si tratta di un comportamento previsto e pertanto il traffico AVC non viene incapsulato o crittografato.

Affinché il traffico AVC possa passare attraverso l'interfaccia del tunnel IPsec, l'opzione **Output Features** deve essere in stato utilizzato. E per farlo, deve essere abilitato esplicitamente nel profilo di esportazione del flusso. Di seguito viene riportata la procedura dettagliata che consente di attivare questa opzione.

Passaggio 1

Salvare nel blocco note l'output completo del **comando di configurazione show performance monitor context** *-name*. Di seguito è riportato l'elemento di cattura per questo output,

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

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

!            Configurazione equivalente di Monitoraggio prestazioni
contesto !

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

!Esportatori

!==========

!

Performance-Monitor-1 dell'utilità di esportazione del flusso

 descrizione contesto di Performance Monitor Esportatore Performance
Monitor

 destinazione 172.16.2.1

 origine Gigabit Ethernet0/1

 transport udp 9991

 export-protocol ipfix

 template data timeout 300

 option interface-table timeout 300

 option vrf-table timeout 300

 option c3pl-class-table timeout 300

 opzione c3pl-policy-table timeout 300

 option sampler-table timeout 300

 option application-table timeout 300
```

```
 option application-attributes timeout 300

 option sub-application-table timeout 300

—cattura—
```

Passaggio 2

Aggiungere l'opzione **output-features** in modo esplicito nel profilo di esportazione del flusso. Dopo aver aggiunto l'opzione relativa alle caratteristiche di output, il profilo dell'esportatore di flusso avrà questo aspetto,

Performance-Monitor-1 dell'utilità di esportazione del flusso

descrizione contesto di Performance Monitor Esportatore Performance Monitor

destinazione 172.16.2.1

origine Gigabit Ethernet0/1

transport udp 9991

export-protocol ipfix

template data timeout 300

caratteristiche-output

option interface-table timeout 300

option vrf-table timeout 300

option c3pl-class-table timeout 300

opzione c3pl-policy-table timeout 300

option sampler-table timeout 300

option application-table timeout 300

option application-attributes timeout 300

option sub-application-table timeout 300

Lasciare inalterato il resto dell'output, NON alterare altro nell'output.

Passaggio 3

A questo punto, rimuovere il profilo EzPM dall'interfaccia e anche dal router.

!

Loopback interfaccia 0

nessun contesto di Performance Monitor Performance-Monitor

esci

!

!

nessun contesto di monitoraggio prestazioni Performance-Monitor profilo esperienza applicazione

!

Passaggio 4

Applicare la configurazione modificata sul router R1. Assicurarsi che non venga omesso un singolo comando, poiché potrebbe causare un comportamento imprevisto.

Verifica

In questa sezione viene descritto il metodo di verifica usato in questo documento per verificare e in che modo questa soluzione ha contribuito a superare le limitazioni per i pacchetti AVC qui menzionate.

Prima di applicare la soluzione, i pacchetti ricevuti dal router peer IPSec (R2) verranno scartati. Verrà generato anche il seguente messaggio:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Reg. pacchetto non un pacchetto IPSEC,
dest_addr= 172.16.2.1, src_addr= 172.16.1.1, port= 17
```

In questo caso R2 si aspetta i pacchetti incapsulati ESP destinati alla versione 172.16.2.1, ma i pacchetti ricevuti sono pacchetti UDP semplici (port=17) ed è previsto che scartino questi pacchetti. L'acquisizione seguente mostra che il pacchetto ricevuto in R2 è un pacchetto UDP semplice anziché ESP incapsulato, il che è un comportamento predefinito per 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)
```

Dopo aver applicato la soluzione alternativa, dall'acquisizione dei pacchetti indicata di seguito si evince chiaramente che i pacchetti AVC ricevuti all'indirizzo R2 sono incapsulati tramite ESP e

non vengono più visualizzati messaggi di errore sull'indirizzo 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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche sulla risoluzione dei problemi per questa configurazione.