Содержание

[Введение](#)
[Предварительные условия](#)
[Общие сведения](#)
[Ограничение](#)
[Настройка](#)
[Схема сети](#)
[Начальная конфигурация](#)
[_____ M1](#)
[R2](#)
[R3](#)
[--- Конфигурация IPSec](#)
[_____ M1](#)
[R2](#)
[Конфигурация EzPM](#)
[_____ M1](#)
[Обходной путь](#)
[Проверка](#)
[Устранение неисправностей](#)
[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает конфигурацию, требуемую для мимолетного трафика AVC через Туннель IPSec к коллектору. По умолчанию информация о AVC не может быть экспортирована через Туннель IPSec в коллектор

Предварительные условия

Cisco рекомендует иметь базовые знания об этих темах:

- Видимость приложения и контроль (AVC)
- Легкий монитор производительности (EzPM)

Общие сведения

Функция AVC Cisco использована, чтобы распознать, проанализировать и управлять по составным приложениям. С осведомленностью приложения, встроенной в инфраструктуру сети, плюс видимость в производительность приложений, работающих на сети, AVC включает на правило приложений для гранулированного контроля использования пропускной способности приложения, приводящего к лучшему опыту конечного пользователя. [Здесь](#) можно найти больше подробных данных об этой технологии.

EzPM является более быстрым и более легким способом настроить традиционную

конфигурацию мониторинга производительности. В настоящее время EzPM не делает предоставляет полную гибкость традиционной модели конфигурации монитора производительности. Здесь можно найти больше подробных данных о EzPM.

Ограничение

В настоящее время AVC не поддерживает количество транзитных протоколов туннелирования, подробные данные могут быть найдены здесь.

Протокол IPSEC (Internet Protocol Security) (IPSec) является одним из неподдерживаемых транзитных протоколов туннелирования для AVC, и этот документ обращается к возможному обходной пути для этого ограничения.

Настройка

В этом разделе описываются завершенную конфигурацию, используемую для моделирования данного ограничения.

Схема сети

В этой схеме сети все маршрутизаторы имеют достижимость друг другу использующему статические маршруты. R1 настроен с конфигурацией EzPM и установил один Туннель IPSec с маршрутизатором R2. R3 работает как средство экспорта здесь, которое могло быть Главной Cisco или любой другой вид средства экспорта, которое способно к сбору производительности данных.

Трафик AVC генерируется R1, и это передается средству экспорта через R2. R1 передает трафик AVC к R2 по интерфейсу Туннеля IPSec.

Начальная конфигурация

В этом разделе описываются начальную конфигурацию для R1 через R3.

_____ M1

```
!
interface Loopback0
IP-адрес 1.1.1.1 255.255.255.255
!

интерфейсный GigabitEthernet0/1

 ip address 172.16.1.1 255.255.255.0

 duplex auto

 speed auto

!
```

ip route 0.0.0.0 0.0.0.0 172.16.1.2

!

R2

!

интерфейс GigabitEthernet0/0/0

IP-адрес 172.16.2.2 255.255.255.0

negotiation auto

!

интерфейс GigabitEthernet0/0/1

ip address 172.16.1.2 255.255.255.0

negotiation auto

!

R3

!

интерфейсный GigabitEthernet0/0

IP-адрес 172.16.2.1 255.255.255.0

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 172.16.2.2

!

--- Конфигурация IPSec

В этом разделе описываются Конфигурацию IPSec для R1 и маршрутизатора R2.

_____ M1

!

ip access-list расширил IPSec_Match

```
 разрешите ip любой хост 172.16.2.1
!
crypto isakmp policy 1
 encr aes 256
 hash md5
 authentication pre-share
 group 2
cisco123 crypto isakmp key обращается 172.16.1.2
!
!
crypto ipsec transform-set set2 aes ESP 256 esp-sha-hmac
 туннель режима
!
!
isakmp ipsec VPN 10 криптокарты
 узел набора 172.16.1.2
 set transform-set set2
 совпадите обращаются к IPSec_Match
!
интерфейсный GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 VPN криптокарты
!
```

R2

```
!
ip access-list расширил IPSec_Match
 permit ip host 172.16.2.1 любой
!
crypto isakmp policy 1
 encr aes 256
 hash md5
 authentication pre-share
 group 2
cisco123 crypto isakmp key обращается 172.16.1.1
!
!
crypto ipsec transform-set set2 aes ESP 256 esp-sha-hmac
 туннель режима
!
!
isakmp ipsec VPN 10 криптокарты
 узел набора 172.16.1.1
 set transform-set set2
 совпадите обращаются к IPSec_Match
 reverse-route
!
интерфейс GigabitEthernet0/0/1
 ip address 172.16.1.2 255.255.255.0
 negotiation auto
 cdp enable
 VPN криптокарты
```

!

Чтобы проверить, работает ли config IPSec как ожидалось или нет, проверьте выходные данные для **show crypto isakmp sa**

```
Crypto isakmp R1#show sa

IPv4 Crypto ISAKMP SA

            src dst             сообщает         статус conn-id

IPv6 Crypto ISAKMP SA
```

Для внедрения сопоставлений безопасности пропингуйте средство экспорта (R3, 172.16.2.1) от R1.

```
R1#ping 172.16.2.1

Для завершения введите последовательность для выхода.

Передавая 5, 100-байтовое Эхо - сигналы ICMP к 172.16.2.1, таймаут
составляет 2 секунды:

!!!!!

Доля успешных попыток составляет 100 процентов (5/5), min/avg/Max. туда
и обратно = 1/1/4 мс

_____ M1
```

Теперь, маршрутизатор будет иметь ассоциацию активной безопасности, которая подтверждает, что ESP инкапсулируется трафик, инициируемый из R1 и предназначенный к средству экспорта.

```
Crypto isakmp R1#show sa

IPv4 Crypto ISAKMP SA

            src dst             сообщает         статус conn-id

172.16.1.2                   АКТИВНЫЙ 172.16.1.1 QM_IDLE 1002

IPv6 Crypto ISAKMP SA
```

Конфигурация EzPM

В этом разделе описываются конфигурацию EzPM для маршрутизатора R1.

_____ M1

!

match-all class-map perf-mon-acl

описание PrimeAM генерировал объект - не модифицирует или использует этот объект

ip match protocol

!

Монитор производительности контекста монитора производительности представляет опыт приложения

назначение средства экспорта 172.16.2.1 источника порт 9991 transport udp GigabitEthernet0/1

stats трафика приложения монитора трафика

ipv4 stats трафика диалога монитора трафика

ipv4 Application Response Time монитора трафика

вход ipv4 сред монитора трафика

выход ipv4 сред монитора трафика

замена класса ipv4 URL монитора трафика perf-mon-acl

!

Примените профиль EzPM на интерфейс, который должен быть проверен; здесь мы контролируем loopback 0 интерфейсов.

_____ M1

!

interface Loopback0

IP-адрес 1.1.1.1 255.255.255.255

Монитор производительности контекста монитора производительности

!

Обходной путь

С вышеупомянутой конфигурацией на месте, возьмите выходные данные для **монитора производительности показа contextcontext-nameexporter**.

Проверьте для статуса опции **Output Features**, по умолчанию это должно быть в **Не Используемое** состояние, которое является нормальным поведением, и именно поэтому трафик AVC не инкапсулируется или шифруется здесь.

Чтобы позволить трафику AVC пройти через интерфейс Туннеля IPSec, опция **Output Features** должна быть в используемом состоянии. И сделать это, это должно быть включено явно в профиле flow exporter. Ниже детализированное действие процедурой шага для включения этой опции.

Шаг 1

Возьмите завершение вывода для **команды настройки** *названия контекста* **контекста монитора производительности показа** и сохраните его в блокноте. Ниже надрез для этих выходных данных,

```
Конфигурация Монитора производительности контекста монитора
производительности R1#show

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

!           Эквивалентная конфигурация монитора производительности
контекста          !

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

! Средства экспорта

!==========

!

Монитор Производительности flow exporter 1

 средство экспорта Монитора производительности контекста монитора
производительности описания

 назначение 172.16.2.1

 источник GigabitEthernet0/1

 transport udp 9991

 export-protocol ipfix

 template data timeout 300

 таймаут интерфейсной таблицы опции 300

 таймаут таблицы VRF опции 300

 таймаут опции c3pl-class-table 300

 таймаут опции c3pl-policy-table 300

 таймаут таблицы образца опции 300
```

```
 таймаут таблицы приложения опции 300

 таймаут атрибутов приложения опции 300

 опция sub-application-table таймаут 300

фрагмент-----------------------
```

Шаг 2

Добавьте **опцию output-features** явно под профилем flow exporter. После добавления опции output-features профиль flow exporter должен быть похожим на это,

Монитор Производительности flow exporter 1

средство экспорта Монитора производительности контекста монитора производительности описания

назначение 172.16.2.1

источник GigabitEthernet0/1

transport udp 9991

export-protocol ipfix

template data timeout 300

output-features

таймаут интерфейсной таблицы опции 300

таймаут таблицы VRF опции 300

таймаут опции c3pl-class-table 300

таймаут опции c3pl-policy-table 300

таймаут таблицы образца опции 300

таймаут таблицы приложения опции 300

таймаут атрибутов приложения опции 300

опция sub-application-table таймаут 300

Остаток выхода выходных данных, как это, НЕ изменяет ничто больше в выходных данных.

Шаг 3

Теперь, удалите профиль EzPM из Интерфейса и из маршрутизатора также.

!

Interface Loopback0

никакой Монитор производительности контекста монитора производительности

exit

!

!

никакой Монитор производительности контекста монитора производительности не представляет опыт приложения

!

Шаг 4

Примените модифицированный config на маршрутизатор R1. Удостоверьтесь, что ни одна команда не пропущена, так как она может вызвать любое неожиданное поведение.

Проверка

В этом разделе описываются метод подтверждения, используемый в этом документе для проверки и как этот обходной путь помог преодолевать ограничение для пакетов AVC, упомянутых здесь.

Прежде, чем применить обходной путь, пакеты, полученные Одноранговым маршрутизатором IPSec (R2), будут отброшены. Ниже сообщения будет генерироваться также:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: пакет Rec'd не Пакет ipsec, dest_addr =
172.16.2.1, src_addr = 172.16.1.1, prot = 17
```

Здесь R2 ожидает инкапсулированные пакеты ESP, которые предназначены для 172.16.2.1, но полученные пакеты являются простыми пакетами UDP (prot=17), и это - нормальное поведение для отбрасывания этих пакетов. Ниже захвата пакета показывает, что пакет, полученный в R2, является простым пакетом UDP вместо инкапсулировавшего ESP, который является поведением по умолчанию для 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)
```

После применения обходного пути это ясно замечено по ниже захвата пакета, что пакеты AVC, полученные в R2, ESP инкапсулируются и больше сообщений об ошибках, замеченных на 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
```

Устранение неисправностей

В настоящее время нет никаких сведений по устранению проблем для данной конфигурации.