

# Índice

[Introdução](#)

[Pré-requisitos](#)

[Informações de Apoio](#)

[Limitação](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração inicial](#)

[R1](#)

[R2](#)

[R3](#)

[Configuração IPsec](#)

[R1](#)

[R2](#)

[Configuração de EzPM](#)

[R1](#)

[Solução](#)

[Verificar](#)

[Troubleshooting](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento descreve a configuração exigida passando o tráfego AVC através de um túnel de IPsec ao coletor. À revelia, a informação AVC não pode ser exportada através de um túnel de IPsec para o coletor

## Pré-requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Visibilidade do aplicativo e controle (AVC)
- Monitoramento de desempenho fácil (EzPM)

## Informações de Apoio

A característica de Cisco AVC é usada para reconhecer, analisar e controlar sobre aplicativos múltiplos. Com a conscientização do aplicativo construída na infraestrutura de rede, mais a visibilidade no desempenho dos aplicativos que são executado na rede, AVC permite a política do por-aplicativo para o controle granulado do uso da largura de banda do aplicativo, tendo por resultado uma experiência de usuário final melhor. [Aqui](#) você pode encontrar mais detalhes sobre esta tecnologia.

EzPM é uma maneira mais rápida e mais fácil de configurar a configuração tradicional do

monitoramento de desempenho. Atualmente EzPM não faz fornecer a flexibilidade completa do modelo tradicional da configuração do monitoramento de desempenho. [Aqui](#) você pode encontrar mais detalhes sobre EzPM.

## Limitação

Atualmente AVC não apoia o número de passagem-atraves de protocolos de tunelamento, detalhes pode ser encontrado [aqui](#).

A segurança de protocolo do Internet (IPsec) é um dos unsupported passagens-atraves dos protocolos de tunelamento para AVC e este documento endereça a alternativa possível para esta limitação.

## Configurar

Esta seção descreve a configuração completa usada para simular a limitação dada.

### Diagrama de Rede

Neste diagrama da rede todos os roteadores tem a alcançabilidade entre si que usa as rotas estáticas. O r1 é configurado com a configuração de EzPM e tem um túnel de IPsec estabelecido com o roteador R2. O R3 está trabalhando como um exportador aqui, que poderia ser prima de Cisco ou qualquer outro tipo de exportador que é capaz de recolher os dados de desempenho.

O tráfego AVC é gerado pelo r1 e é enviado ao exportador através do R2. O r1 envia o tráfego AVC ao R2 sobre uma relação do túnel de IPsec.

### Configuração inicial

Esta seção descreve a configuração inicial para o r1 com o R3.

#### R1

```
!  
relação Loopback0  
endereço IP 1.1.1.1 255.255.255.255  
!
```

```
relação GigabitEthernet0/1
```

```
endereço IP 172.16.1.1 255.255.255.0
```

```
automóvel frente e verso
```

```
automóvel da velocidade
```

```
!
```

```
rota 0.0.0.0 0.0.0.0 172.16.1.2 IP
```

!

## R2

!

relação GigabitEthernet0/0/0

endereço IP 172.16.2.2 255.255.255.0

negociação automática

!

relação GigabitEthernet0/0/1

endereço IP 172.16.1.2 255.255.255.0

negociação automática

!

## R3

!

relação GigabitEthernet0/0

endereço IP 172.16.2.1 255.255.255.0

automóvel frente e verso

automóvel da velocidade

!

rota 0.0.0.0 0.0.0.0 172.16.2.2 IP

!

## Configuração IPSec

Esta seção descreve a configuração IPSec para o r1 e o roteador R2.

## R1

!

lista de acesso IPSec\_Match prolongado IP

licença IP algum host 172.16.2.1

!  
política cripto 1 do isakmp  
aes 256 do encr  
mistura md5  
Pré-compartilhamento de autenticação  
grupo2  
endereço cripto 172.16.1.2 do cisco123 da chave do isakmp

!  
!  
esp-sha-hmac 256 cripto do conjunto de transformação set2 ESP-aes do IPsec

túnel do modo

!  
!  
crypto map VPN 10 IPsec-ISAKMP  
ajuste o par 172.16.1.2  
ajuste o conjunto de transformação set2  
combine o endereço IPsec\_Match

!  
conecte GigabitEthernet0/1  
endereço IP 172.16.1.1 255.255.255.0  
automóvel frente e verso  
automóvel da velocidade  
crypto map VPN

!  
**R2**

!

lista de acesso IPSec\_Match prolongado IP

host 172.16.2.1 da licença IP

!

política cripto 1 do isakmp

aes 256 do encr

mistura md5

Pré-compartilhamento de autenticação

grupo2

endereço cripto 172.16.1.1 do cisco123 da chave do isakmp

!

!

esp-sha-hmac 256 cripto do conjunto de transformação set2 ESP-aes do IPsec

túnel do modo

!

!

crypto map VPN 10 IPsec-ISAKMP

ajuste o par 172.16.1.1

ajuste o conjunto de transformação set2

combine o endereço IPSec\_Match

reverso-rota

!

relação GigabitEthernet0/0/1

endereço IP 172.16.1.2 255.255.255.0

negociação automática

o cdp permite

crypto map VPN

!

Para verificar se a configuração do IPsec está trabalhando como esperado ou não, verifique a saída para ver se há **isakmp cripto sa de mostra**

```
Isakmp cripto sa R1#show
```

```
ISAKMP cripto SA do IPv4
```

```
estado CONN-identificação do estado do src do dst
```

```
ISAKMP cripto SA do IPv6
```

A fim trazer acima as associações de segurança, sibile o exportador (R3, 172.16.2.1) do r1.

```
R1#ping 172.16.2.1
```

```
Digite a seqüência de escape para cancelar.
```

```
Enviando 5, os ecos do 100-byte ICMP a 172.16.2.1, intervalo são 2 segundos:
```

```
!!!!!
```

```
A taxa de sucesso é 100 por cento (5/5), minuto do round trip/médio/= 1/1/4 de Senhora máxima
```

```
R1#
```

Agora, o roteador terá uma associação da segurança ativa, que confirme que o tráfego que está sendo originado do r1 e destinado ao exportador é ESP encapsulado.

```
Isakmp cripto sa R1#show
```

```
ISAKMP cripto SA do IPv4
```

```
estado CONN-identificação do estado do src do dst
```

```
ACTIVE DE 172.16.1.2 172.16.1.1 QM_IDLE 1002
```

```
ISAKMP cripto SA do IPv6
```

## Configuração de EzPM

Esta seção descreve a configuração de EzPM para o roteador do r1.

**R1**

!

mapa de classe perf-segundo--ACL compatível com todos

entidade gerada PrimeAM da descrição - não altere nem use esta entidade

combine o protocolo IP

!

aplicativo-experiência do perfil do monitoramento de desempenho do contexto do monitoramento de desempenho

porta 9991 UDP do transporte da fonte GigabitEthernet0/1 de 172.16.2.1 do destino do exportador

aplicativo-tráfego-stats do monitor de tráfego

IPv4 conversação-tráfego-stats do monitor de tráfego

IPv4 do Application Response Time do monitor de tráfego

ingresso do IPv4 dos media do monitor de tráfego

saída do IPv4 dos media do monitor de tráfego

o IPv4 do monitor de tráfego URL classe-substitui o perf-segundo--ACL

!

Aplicar o perfil de EzPM na relação que necessitates de ser monitorado; aqui nós estamos monitorando a relação do laço de retorno 0.

R1

!

relação Loopback0

endereço IP 1.1.1.1 255.255.255.255

monitoramento de desempenho do contexto do monitoramento de desempenho

!

## Solução

Com a configuração acima no lugar, tome a saída para o `contextcontext-nameexporter` do **monitoramento de desempenho da mostra**.

Verifique para ver se há o estado da opção dos **recursos de emissor**, à revelia deve estar no estado **não usado**, que é um comportamento esperado e o tráfego AVC não está sendo encapsulado nem está sendo cifrado é por isso aqui.

A fim de deixar a passagem do tráfego AVC através da relação do túnel de IPsec, a opção dos **recursos de emissor** estará no estado usado. E para fazer isso, tem que ser permitida explicitamente no perfil do exportador do fluxo. Está abaixo o procedimento passo a passo detalhado para permitir esta opção.

## Step-1

Tome as saídas completas para o **comando configuration do nome de contexto do contexto do monitoramento de desempenho da mostra** e salvar as no bloco de notas. Está abaixo o pique para esta saída,

Configuração do monitoramento de desempenho do contexto do monitoramento de desempenho R1#show

```
!  
=====
```

```
!           Configuração equivalente do monitoramento de desempenho do  
contexto!
```

```
!  
=====
```

```
! Exportadores
```

```
! =====
```

```
!
```

```
exportador Performance-Monitor-1 do fluxo
```

```
exportador do monitoramento de desempenho do contexto do monitoramento  
de desempenho da descrição
```

```
destino 172.16.2.1
```

```
fonte GigabitEthernet0/1
```

```
UDP 9991 do transporte
```

```
ipfix do exportação-protocolo
```

```
intervalo 300 dos dados do molde
```

```
intervalo 300 da relação-tabela da opção
```

```
intervalo 300 da VRF-tabela da opção
```

```
intervalo 300 da opção c3pl-class-table
```

```
intervalo 300 da opção c3pl-policy-table
```

```
intervalo 300 da demonstrador-tabela da opção
```

```
intervalo 300 da aplicativo-tabela da opção
```



intervalo 300 dos aplicativo-atributos da opção

intervalo 300 da secundário-aplicativo-tabela da opção

-----pique-----

## Step-2

Adicionar a opção dos **recursos de emissor** explicitamente sob o perfil do exportador do fluxo. Após ter adicionado a opção dos recursos de emissor o perfil do exportador do fluxo olhará como este,

exportador Performance-Monitor-1 do fluxo

exportador do monitoramento de desempenho do contexto do monitoramento de desempenho da descrição

destino 172.16.2.1

fonte GigabitEthernet0/1

UDP 9991 do transporte

ipfix do exportação-protocolo

intervalo 300 dos dados do molde

### *recursos de emissor*

intervalo 300 da relação-tabela da opção

intervalo 300 da VRF-tabela da opção

intervalo 300 da opção c3pl-class-table

intervalo 300 da opção c3pl-policy-table

intervalo 300 da demonstrador-tabela da opção

intervalo 300 da aplicativo-tabela da opção

intervalo 300 dos aplicativo-atributos da opção

intervalo 300 da secundário-aplicativo-tabela da opção

Deixe o resto da saída como é, não alteram qualquer outra coisa na saída.

## Step-3

Agora, remova o perfil de EzPM da relação e do roteador também.

!

Interface loopback 0

nenhum monitoramento de desempenho do contexto do monitoramento de desempenho

saída

!

!

nenhuma aplicativo-experiência do perfil do monitoramento de desempenho do contexto do monitoramento de desempenho

!

#### Step-4

Aplice a configuração alterada no roteador do r1. Certifique-se de que não um comando único está faltado para fora, desde que pode causar todo o comportamento inesperado.

## Verificar

Esta seção descreve o método de verificação usado neste documento para verificar e como esta ação alternativa ajudou a superar a limitação para os pacotes AVC mencionados aqui.

Antes de aplicar a ação alternativa, os pacotes recebidos pelo roteador de IPsec peer (R2) serão deixados cair. Abaixo da mensagem será gerado também:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Pacote de Rec'd não um pacote de IPsec,  
dest_addr= 172.16.2.1, src_addr= 172.16.1.1, prot= 17
```

Aqui o R2 está esperando os pacotes encapsulado ESP que são destinados para 172.16.2.1, mas os pacotes recebidos são os pacotes de UDP lisos (prot=17) e é um comportamento esperado para deixar cair estes pacotes. Abaixo da captura de pacote de informação mostra que o pacote recebido no R2 é um pacote de UDP liso em vez do ESP encapsulado, que é um comportamento padrão 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)
```

Após ter aplicado a ação alternativa, vê-se claramente da captura de pacote de informação abaixo que os pacotes AVC recebidos no R2 são ESP encapsulado e de não mais Mensagens de Erro vistos no 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
```

## Troubleshooting

Atualmente não há nenhuma informação de Troubleshooting específica para esta configuração.