

# Configurar o IPSEC ISE 2.2 para fixar uma comunicação NAD (ASA)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Arquitetura do IPsec ISE](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração ASA](#)

[Configurar as relações ASA](#)

[Configurar a política IKEv1 e permita IKEv1 na interface externa](#)

[Configurar o grupo de túneis \(o perfil da conexão de LAN para LAN\)](#)

[Configurar o ACL para o tráfego VPN do interesse](#)

[Configurar o IKEv1 transformam o grupo](#)

[Configurar um crypto map e aplique-o a uma relação](#)

[Configuração final ASA](#)

[Configuração ISE](#)

[Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT no ISE](#)

[Adicionar o NAD ao grupo IPsec no ISE](#)

[Permita o IPSEC no ISE](#)

[Verificar](#)

[ASA](#)

[ESR](#)

[ISE](#)

[Troubleshooting](#)

[Configurar a site para site de FlexVPN \(DVTI ao crypto map\) entre NAD e ISE 2.2](#)

[Configuração ASA](#)

[Configuração ESR no ISE](#)

[Considerações de projeto de FlexVPN](#)

## Introdução

Este documento descreve como configurar e pesquisar defeitos o IPSEC do RAI0 para fixar o motor do serviço da identidade de Cisco (ISE) 2.2 - uma comunicação do dispositivo do acesso de rede (NAD). O tráfego de radius deve ser cifrado dentro da versão 1 de site para site do intercâmbio de chave de Internet do IPsec (do LAN para LAN) e (IKEv1 e IKEv2) do túnel 2 entre a ferramenta de segurança adaptável (ASA) e o ISE. Este documento não cobre a divisória da configuração de VPN de AnyConnect SSL.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Cisco ASA
- Conceitos gerais do IPsec
- Conceitos gerais do RAIO

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5515-X Series ASA que executa a versão de software 9.4(2)11
- Versão 2.2 do motor do serviço da identidade de Cisco
- Pacote de serviços 1 de Windows 7

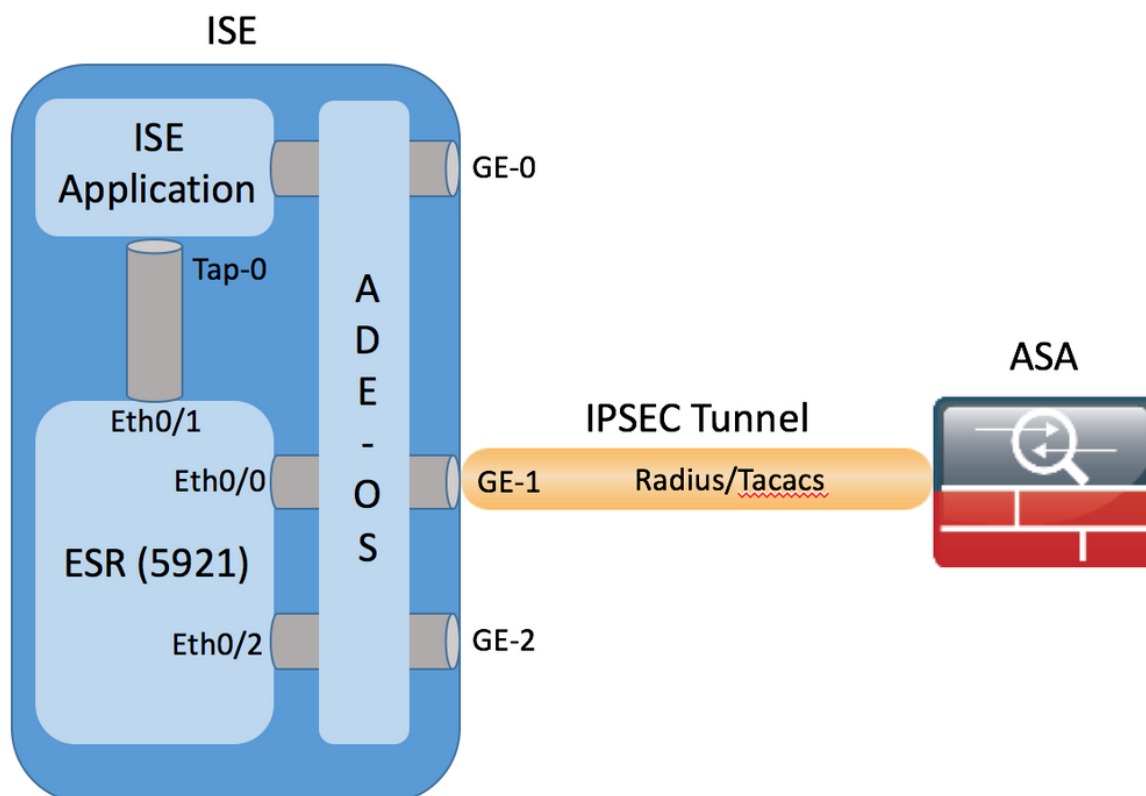
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Informações de Apoio

O objetivo é fixar os protocolos que usam a mistura MD5, o raio e o TACACS incertos com IPsec. Tome isto na consideração:

- Cisco ISE apoia o IPsec em modos do túnel e de transporte.
- Quando você permite o IPsec em uma relação de Cisco ISE, um túnel de IPsec está criado entre Cisco ISE e o NAD para fixar a comunicação.
- Você pode definir uma chave pré-compartilhada ou usar os Certificados X.509 para a autenticação IPsec.
- O IPsec pode ser permitido em Eth1 através das relações Eth5. Você pode configurar o IPsec em somente uma relação de Cisco ISE pelo PSN.

## Arquitetura do IPsec ISE



Uma vez que os pacotes criptografado são recebidos pela relação ESR GE-1 ISE os interceptam na relação Eth0/0.

```
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 10.48.26.170 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
```

O ESR decifra-os e de acordo com o NAT preconfigured as regras executam a tradução de endereços. (Para o NAD) os pacotes que parte RADIUS/TACACS são traduzidos ao endereço da relação do Ethernet0/0 e cifrados mais tarde.

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

Os pacotes que são destinados à relação Eth0/0 em portas RADIUS/TACACS devem ser forwarded através da relação Eth0/1 ao endereço IP 10.1.1.2, que é endereço interno do ISE. Configuração ESR de Eth0/1

```
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
```

Configuração ISE da relação Tap-0 interna:

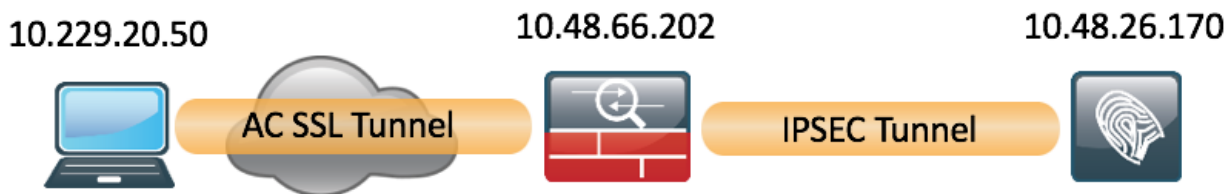
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.2 netmask 255.255.255.252 broadcast 10.1.1.3
    inet6 fe80::6c2e:37ff:fe5f:b609 prefixlen 64 scopeid 0x20<link>
    ether 6e:2e:37:5f:b6:09 txqueuelen 500 (Ethernet)
    RX packets 81462 bytes 8927953 (8.5 MiB)
    RX errors 0 dropped 68798 overruns 0 frame 0
    TX packets 105 bytes 8405 (8.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Configurar

Esta seção descreve como terminar as configurações ASA CLI e ISE.

## Diagrama de Rede

A informação neste documento usa esta instalação de rede:



## Configuração ASA

### Configurar as relações ASA

Se a relação/relações ASA não é configurada, assegure-se de que você configure pelo menos o endereço IP de Um ou Mais Servidores Cisco ICM NT, conecte-se o nome, e o nível de segurança:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
```

### Configurar a política IKEv1 e permita IKEv1 na interface externa

A fim configurar as políticas do Internet Security Association and Key Management Protocol (ISAKMP) para as conexões IKEv1, incorpore o comando `cripto do <priority>` da política `ikev1`:

```
cripto ikev1 policy 20
 authentication pre-share
 encryption aes
 hash sha
 group 5
 lifetime 86400
```

**Nota:** Um fósforo da política IKEv1 existe quando ambas as políticas dos dois pares contêm a mesma autenticação, criptografia, mistura, e valores de parâmetro de Diffie-Hellman. Para IKEv1, a política do peer remoto deve igualmente especificar uma vida inferior ou igual à vida na política que o iniciador envia. Se as vidas não são idênticas, a seguir o ASA usa a vida mais curto.

Você deve permitir IKEv1 na relação que termina o túnel VPN. Tipicamente, esta é a relação exterior (ou *público*). A fim permitir IKEv1, incorpore o **ikev1 cripto permitem** o comando do **<interface-name>** no modo de configuração global:

```
crypto ikev1 enable outside
```

### Configurar o grupo de túneis (o perfil da conexão de LAN para LAN)

Para um túnel de LAN para LAN, o tipo do perfil de conexão é **ipsec-l2l**. A fim configurar a chave IKEv1 preshared, incorpore o modo de configuração dos *IPsec-atributos do grupo de túneis*:

```
crypto ikev1 enable outside
```

### Configurar o ACL para o tráfego VPN do interesse

O ASA usa o Access Control Lists (ACLs) a fim diferenciar o tráfego que deve ser protegido com criptografia IPsec do tráfego que não exige a proteção. Protege os pacotes externos que combinam um motor do controle de aplicativo da licença (ACE) e assegura-se de que os pacotes de entrada que combinam uma licença ACE tenha a proteção.

```
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

**Nota:** Um ACL para o tráfego VPN usa os endereços IP de origem e de destino após o Network Address Translation (NAT). O único tráfego cifrado neste caso é tráfego entre o ASA e o ISE.

### Configurar o IKEv1 transformam o grupo

Um IKEv1 transforma o grupo é uma combinação de protocolos de segurança e os algoritmos que defina a maneira que o ASA protege dados. Durante negociações da associação de segurança IPsec (SA), os pares devem identificar uma transformação ajustada ou a proposta que sejam as mesmas para ambos os pares. O ASA aplica então combinado transforma o grupo ou a proposta a fim criar um SA que proteja fluxos de dados na lista de acessos para esse crypto map.

A fim configurar o IKEv1 transforme o grupo, incorporam o comando **cripto do conjunto de transformação do IPsec ikev1**:

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

### Configurar um crypto map e aplique-o a uma relação

Um crypto map define uma política de IPsec a ser negociada IPsec SA e inclui-a:

- Uma lista de acessos a fim identificar os pacotes que a conexão IPsec permite e protege
- Identificação do par
- Um endereço local para o tráfego de IPsec
- Os IKEv1 transformam grupos

Aqui está um exemplo:

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

Você pode então aplicar o crypto map à relação:

```
crypto map MAP interface outside
```

## Configuração final ASA

Está aqui a configuração final no ASA:

```
crypto map MAP interface outside
```

## Configuração ISE

### Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT no ISE

O endereço deve ser configurado no GE1-GE5 da relação do CLI, GE0 não é apoiado.

```
crypto map MAP interface outside
```

**Nota:** O aplicativo reinicia depois que o endereço IP de Um ou Mais Servidores Cisco ICM NT é configurado na relação:

% que mudam o endereço IP de Um ou Mais Servidores Cisco ICM NT puderam fazer com que os serviços ISE reiniciem

Continue com mudança do endereço IP de Um ou Mais Servidores Cisco ICM NT? [N] Y/N:

Y

### Adicionar o NAD ao grupo IPSec no ISE

Navegue à **administração > aos recursos de rede > aos dispositivos de rede**. Clique **adicionam** sobre. Assegure-se de que você configure o nome, endereço IP de Um ou Mais Servidores Cisco ICM NT, segredo compartilhado. Para terminar o túnel de IPsec do NAD selecione **YE** contra o grupo do dispositivo da rede IPsec.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > EK\_ASA

### Network Devices

Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

\* Shared Secret

CoA Port

Uma vez que o NAD é adicionado, a rota adicional deve ser criada no ISE, para assegurar-se de que o tráfego de radius atravesse o ESR e obtenha cifrado:

```
crypto map MAP interface outside
```

## Permita o IPSEC no ISE

Navegue à **administração > ao sistema > aos ajustes**. Clique sobre o **raio** e o further no **IPSEC**. Selecione o PSN (único/múltiplo/tudo) seletor permitem a opção, escolhem a relação e selecionam o método de autenticação. Clique em Salvar. Os serviços reiniciam no nó selecionado neste momento.

The screenshot shows the Cisco ISE Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The main content area is titled 'IPsec Deployment' and 'Activate ISE Nodes for IPsec'. It displays a table with one row selected: 'ISE22-1ek' with 'IPsec Status' set to 'Disabled'. Below the table, there are two notes: 'Note: Please be aware that the application server will restart on the selected nodes.' and 'Note: Proper licensing must be installed and configured on ESR. Please see IPsec documentation.' The configuration options include 'Enable/Disable IPsec for selected nodes' (set to 'Enable'), 'IPsec Interface for selected nodes' (set to 'Gigabit Ethernet 1'), and 'Authentication for selected nodes' (set to 'Pre-shared Key' with the value 'Krakow123'). There are 'Cancel' and 'Save' buttons at the bottom right.

Note, isso depois que a configuração de CLI do reinício ISE dos serviços mostra a interface configurada sem endereço IP de Um ou Mais Servidores Cisco ICM NT e no estado de fechamento, ele é esperado como o ESR (roteador encaixado dos serviços) toma o controle da relação ISE.

```
crypto map MAP interface outside
```

Uma vez que os serviços são reiniciados, a funcionalidade ESR está permitida. Para entrar ao ESR datilografe o esr na linha de comando:

```
crypto map MAP interface outside
```

O ESR é vem acima com a seguinte configuração de criptografia:

```
crypto map MAP interface outside
```

Devido ao ASA não apoia o algorithm do hashing sha256, a configuração adicional é exigida no ESR para combinar as políticas IKEv1 para a? a e? a fase de IPSEC. Configurar a política do isakmp e transforme o grupo, para combinar aqueles configurados no ASA:

```
crypto map MAP interface outside
```

Certifique-se que o ESR tem uma rota para enviar para fora pacotes criptografado:

```
crypto map MAP interface outside
```

## Verificar

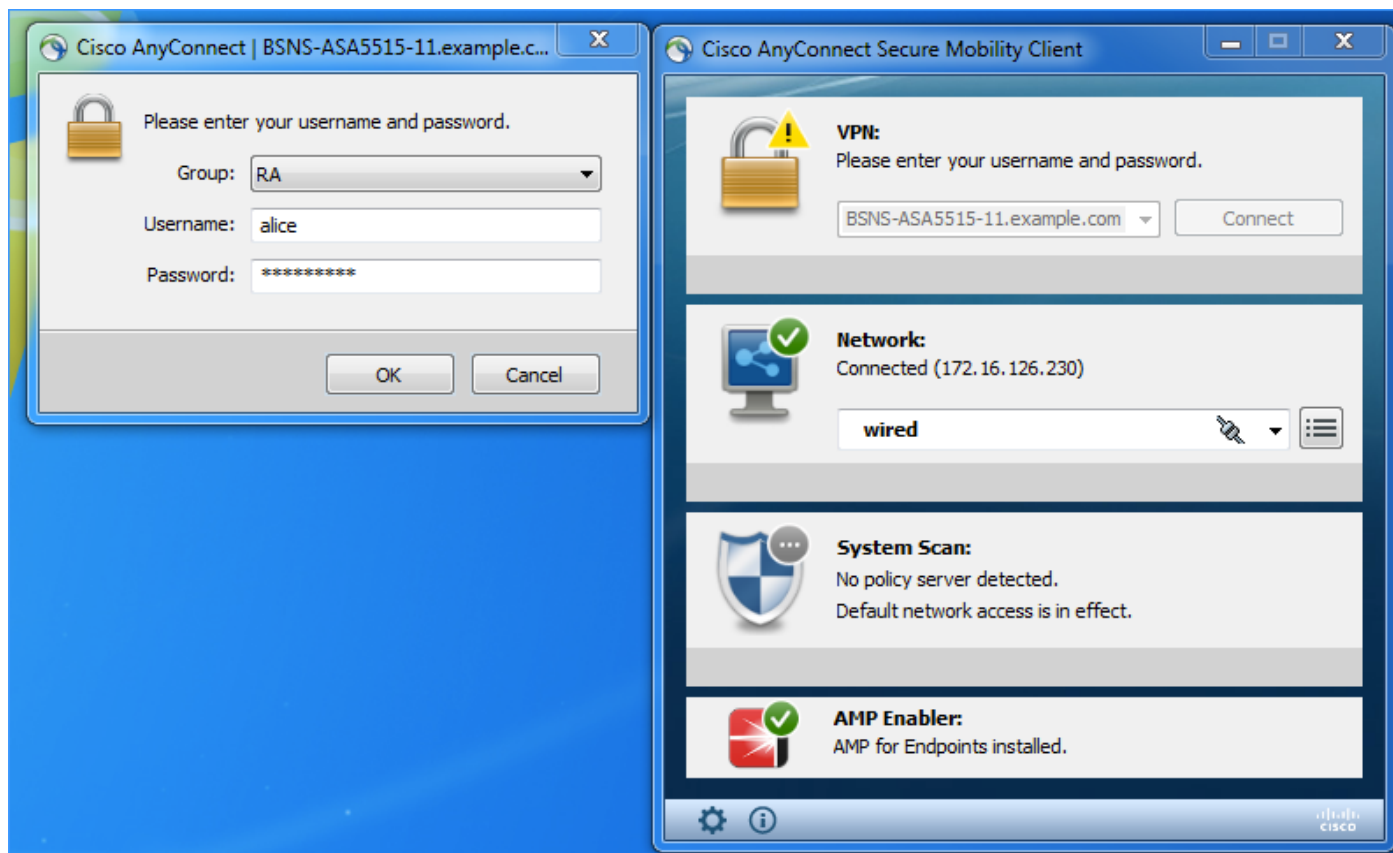
## ASA



Antes que os clientes de Anyconnect conectem, o ASA não tem nenhuma sessão de criptografia:

```
crypto map MAP interface outside
```

O cliente conecta através do cliente VPN de Anyconnect, porque uma fonte ISE 2.2 da autenticação é usada.



O ASA envia um pacote de informação de RADIUS, que provoque o estabelecimento da sessão de VPN, uma vez o túnel é acima da seguinte saída é visto no ASA e confirma que a fase 1 do túnel está acima:

```
crypto map MAP interface outside
```

A fase 2 está acima, e os pacotes são cifrados e decifrados:

```
crypto map MAP interface outside
```

## ESR

As mesmas saídas podem ser verificadas no ESR, fase um estão acima:

```
crypto map MAP interface outside
```

A fase 2 está acima, os pacotes são cifrados e decifrados com sucesso:

```
crypto map MAP interface outside
```

## ISE

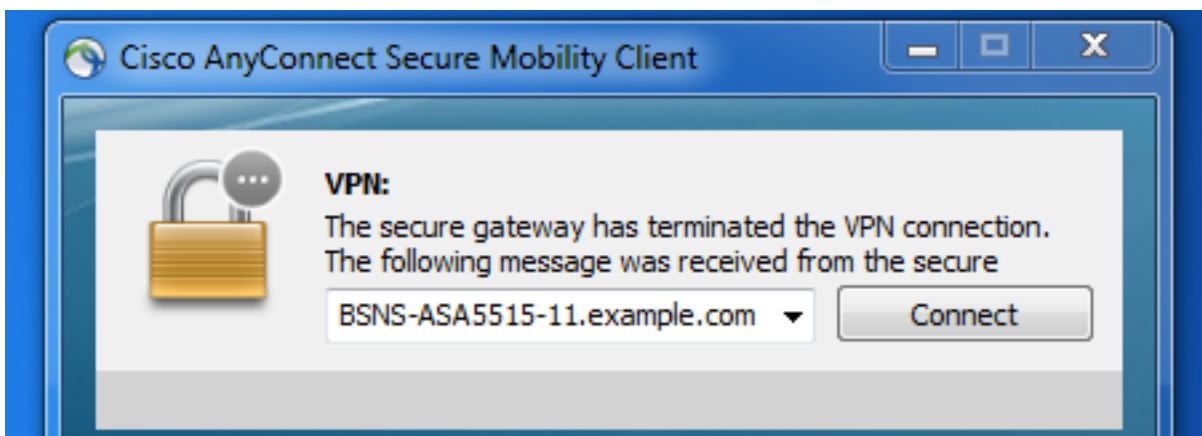
A autenticação viva indica a autenticação regular PAP\_ASCII:

As captações tomadas na relação GE1 do ISE e filtradas com ESP ou raio, confirmam que não há nenhum raio no texto claro, e todo o tráfego é cifrado:

No.	Time	Source	Destination	Protocol	Length	Info
42	2017-02-03 11:23:01.618220	10.48.66.202	10.48.26.170	ESP	694	ESP (SPI=0xd370da0e)
43	2017-02-03 11:23:01.665386	10.48.26.170	10.48.66.202	ESP	262	ESP (SPI=0x108bbceb)
44	2017-02-03 11:23:01.668335	10.48.66.202	10.48.26.170	ESP	742	ESP (SPI=0xd370da0e)
45	2017-02-03 11:23:01.680209	10.48.26.170	10.48.66.202	ESP	134	ESP (SPI=0x108bbceb)
60	2017-02-03 11:23:02.166469	10.48.66.202	10.48.26.170	ESP	774	ESP (SPI=0xd370da0e)
61	2017-02-03 11:23:02.179383	10.48.26.170	10.48.66.202	ESP	134	ESP (SPI=0x108bbceb)

É igualmente possível enviar pacotes criptografado do ISE - mudança da autorização (CoA) - uma vez que o túnel é em serviço:

Nesta sessão de exemplos a terminação foi emitida, e o cliente VPN obtido desligou em consequência:



## Troubleshooting

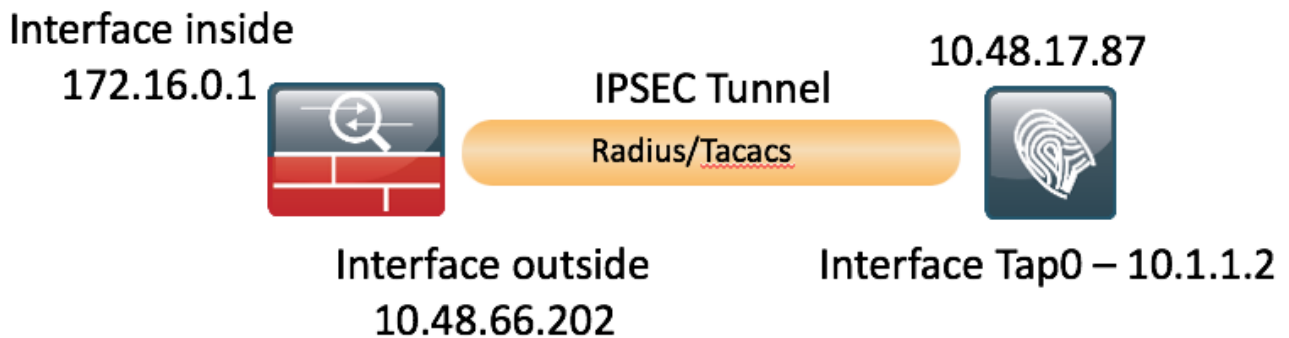
A técnica de Troubleshooting comum VPN pode ser aplicada para pesquisar defeitos as edições relativas ao IPSEC. Você pode encontrar documentos úteis abaixo:

[Os IO IKEv2 debugam para o VPN de Site-para-Site com os PSK que pesquisam defeitos TechNote](#)

[O ASA IKEv2 debuga para o VPN de Site-para-Site com PSK](#)

## Configurar a site para site de FlexVPN (DVTI ao crypto map) entre NAD e ISE 2.2

É igualmente possível proteger o tráfego de radius com FlexVPN. A seguinte topologia é usada no exemplo abaixo:



A configuração de FlexVPN é direta. Mais detalhes podem ser encontrados aqui:

<http://www.cisco.com/c/en/us/support/docs/security/flexvpn/116008-flexvpn-nge-config-00.html>

### Configuração ASA

```
crypto map MAP interface outside
```

### Configuração ESR no ISE

```
crypto map MAP interface outside
```

### Considerações de projeto de FlexVPN

- O túnel VPN é construído usando DVTI no lado ESR e o crypto map no lado ASA, com a configuração acima do ASA pode gerar o pacote de informação de RADIUS originado da interface interna, que assegurará a lista de acesso correta para que a criptografia provoque o estabelecimento da sessão de VPN.
- Note, esse neste caso ASA NAD deve ser definido no ISE com endereço IP de Um ou Mais Servidores Cisco ICM NT da interface interna.