

# Túnel IPSec de LAN para LAN entre um Cisco VPN 3000 Concentrator e um roteador com exemplo de configuração AES

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar o concentrador VPN](#)

[Verificar](#)

[Verifique a configuração de roteador](#)

[Verifique a configuração do concentrador VPN](#)

[Troubleshooting](#)

[Pesquise defeitos o roteador](#)

[Pesquise defeitos o concentrador VPN](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento mostra como configurar um túnel de IPsec entre um concentrador Cisco VPN 3000 e um roteador Cisco com padrão de codificação avançado (AES) como o algoritmo de criptografia.

O AES é uma publicação nova do padrão de processamento de informação federal (FIP) criada pelo National Institute of Standards and Technology (NIST) a ser usado como um método de criptografia. Este padrão especifica um algoritmo de criptografia simétrica AES que substitua o Data Encryption Standard (DES) enquanto uma privacidade transforma para o IPsec e o Internet Key Exchange (IKE). O AES tem três comprimentos chaves diferentes, uma chave do 128-bit (o padrão), uma chave do 192-bit, e uma chave do 256-bit. A característica AES em Cisco IOS® adiciona o apoio para o padrão de codificação novo AES, com modo do Cipher Block Chaining (CBC), ao IPsec.

Refira a [site do centro de recursos de segurança de computador nist](#) para obter mais informações sobre do AES.

Refira o [túnel IPSec de LAN para LAN entre o Cisco VPN 3000 Concentrator e o exemplo de](#)

[configuração do PIX Firewall](#) para obter mais informações sobre da configuração de túnel de Rede-para-Rede entre um VPN 3000 concentrator e o PIX Firewall.

Refira o [túnel de IPsec entre PIX 7.x e exemplo de configuração do VPN 3000 concentrator](#) para mais informação quando o PIX tem a versão de software 7.1.

## Pré-requisitos

### Requisitos

Este documento exige uma compreensão básica do protocolo IPsec. Refira uma [introdução à criptografia IPsec](#) para aprender mais sobre o IPsec.

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- **Requisitos do roteador** - A característica AES foi introduzida no Cisco IOS Software Release 12.2(13)T. A fim permitir o AES, seu roteador deve apoiar o IPsec e executar uma imagem IOS com chaves longas de "k9" (o subsistema de "k9").**Note:** O suporte a hardware para o AES está igualmente disponível 2691, 3725, e 3745 nos módulos VPN de aceleração de AES do Cisco 2600XM. Esta característica não tem nenhuma implicação de configuração e o módulo de hardware é selecionado automaticamente se ambos estão disponíveis.
- **Exigências do concentrador VPN** - O suporte de software para a característica AES foi introduzido na liberação 3.6. O suporte a hardware é fornecido pela aumentada nova, o processador de criptografia escalável (SEP-E). Esta característica não tem nenhuma implicação de configuração.**Note:** Na liberação 3.6.3 do Cisco VPN 3000 Concentrator, os túneis não negociam a AES devido à identificação de bug Cisco [CSCdy88797](#) ([clientes registrados somente](#)). Isto foi resolvido da liberação 3.6.4.**Note:** O Cisco VPN 3000 Concentrator usa um ou outro setembro ou setembro - Módulos E, não ambos. Não instale ambos no mesmo dispositivo. Se você instala um módulo SEP-E em um concentrador VPN que já contenha um módulo SEP, o concentrador VPN desabilita o módulo SEP e usa somente o módulo SEP-E.

### Componentes Utilizados

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

- Cisco 3600 Series Router com Cisco IOS Software Release 12.3(5)
- Concentrador Cisco VPN 3060 com Software Release 4.0.3

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.

### Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Note:** Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

## Configurações

Este documento utiliza as seguintes configurações:

- [Roteador de IPsec](#)
- [Concentrador de VPN](#)

### configuração do ipsec\_router

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
```

```

crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. !!--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end

```

**Note:** Embora a sintaxe ACL seja inalterada, os significados são levemente diferentes para ACLs cript. Nos ACLs cript., a **licença** específica aqueles pacotes de harmonização deve ser cifrada, visto que **negue** especifica os pacotes de harmonização não precisam de ser cifrados.

## [Configurar o concentrador VPN](#)

Os concentradores VPN PRE-não são programados com endereços IP de Um ou Mais Servidores

Cisco ICM NT em suas configurações de fábrica. Você tem que usar a porta de Console para configurar as configurações inicial que são um comando line interface(cli) menu-baseado. Refira [configurar concentradores VPN através do console](#) para obter informações sobre de como configurar através do console.

Após o endereço IP de Um ou Mais Servidores Cisco ICM NT em Ethernet1 a relação (privada) é configurada, o resto pode ser configurado ou usando o CLI ou através da interface de navegador. A interface de navegador apoia o HTTP e o HTTPS sobre o Secure Socket Layer (SSL).

Estes parâmetros são configurados através do console:

- **Hora/data** - As horas correta e a data são muito importantes. Ajudam a assegurar-se de que o registro e as entradas de relatório sejam exatos, e que o sistema pode criar um Security Certificate válido.
- **Relação (privada) de Ethernet1** - O endereço IP de Um ou Mais Servidores Cisco ICM NT e a máscara (de nossa topologia de rede 172.16.1.1/24).

Neste momento, o concentrador VPN é acessível com um navegador de HTML da rede interna. Para obter informações sobre de configurar o concentrador VPN no modo de CLI, refira a [configuração rápida usando o CLI](#).

1. Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface confidencial do navegador da Web para permitir a interface GUI. Clique sobre o ícone **necessário salvaguarda** para salvar mudanças à memória. O nome de usuário e senha do padrão de fábrica é o "admin" que é diferenciando maiúsculas e minúsculas.
2. Depois que você traz acima o GUI, selecione o **Configuração > Interfaces > Ethernet 2 (público)** para configurar a relação dos Ethernet 2.
3. O > IP Routing seletor > os **gateways padrão do Configuration > System** configuram o gateway do padrão (Internet) e o gateway do padrão do túnel (para dentro) para que o IPsec alcance as outras sub-redes na rede privada. Nesta encenação, há somente uma sub-rede disponível na rede interna.
4. Selecione o > Add do **Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Listas de Rede** para criar os listas de redes que definem o tráfego a ser cifrado. As redes mencionadas na lista são alcançáveis à rede remota. As redes mostradas na lista abaixo são redes local. Você pode igualmente gerar a lista de redes local automaticamente através do RASGO quando você clique **gerencie a lista local**.
5. As redes nesta lista são redes remotas e precisam de ser configuradas manualmente. A fim fazer isto, entre na rede/convite para cada sub-rede alcançável. Quando concluídas, estas são as duas listas de rede:
6. Selecione o **Configuration > System > Tunneling Protocols > > Add do LAN para LAN do IPsec** e defina o túnel de LAN para LAN. Este indicador tem três seções. A seção superior é para a informação de rede e as duas seções inferiores são para as lista da rede remota e local. Na seção de informação de rede, selecione a criptografia de AES, tipo do autenticação, proposta IKE, e datilografe a chave pré-compartilhada. Nas seções inferiores, aponte aos listas de redes que você já criou, lista locais e remotas respectivamente.
7. Depois que você clique **adiciona**, se sua conexão está correta, você é apresentado com o indicador LAN-à-LAN-adicionar-feito IPsec. Este indicador apresenta um sumário da informação de configuração de túnel. Igualmente configura automaticamente o nome do grupo, o nome SA, e o nome do filtro. Você pode editar todos os parâmetros nesta tabela. Neste momento o túnel de LAN para LAN de IPsec estabeleceu-se e você pode

começar trabalhar. Se, por qualquer motivo, o túnel não funciona, você pode verificar para ver se há configurações incorretas.

8. Você pode ver ou alterar previamente os parâmetros IPsec LAN-a-LAN criados quando você seleciona o **Configuration > System > Tunneling Protocols > LAN para LAN do IPsec**. Este gráfico mostra o “teste” porque o nome do túnel e da interface pública da extremidade remota é 30.30.30.1 conforme a encenação.
9. Às vezes, seu túnel não pôde vir acima se sua proposta IKE está na lista das Propostas Inativas. Selecione o **configuração > sistema > protocolos de tunelamento > IPSEC > propostas de IKE** para configurar a proposta do IKE ativo. Se sua proposta IKE está no as “Propostas Inativas” alistam-no podem permiti-lo quando você seleciona a proposta IKE e clica sobre o botão da **ativação**. Neste gráfico a proposta selecionada "IKE-AES256-SHA" está na lista dos propósitos ativo.
10. Selecione o **Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança** para verificar se os parâmetros SA estão corretos.
11. Clique o nome SA (neste caso, **L2L: o teste**), e clica então **altera** para verificar os SA. Se alguns dos parâmetros não combinam com a configuração do peer remoto, podem ser mudados aqui.

## Verificar

### Verifique a configuração de roteador

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto isakmp sa** – Exibe todas as SAs de IKE atuais em um correspondente. O estado QM\_IDLE denota que as sobras SA autenticadas com seu par e pode ser usado para trocas subsequentes do Quick Mode. Está em um estado quieto.

```
ipsec_router#show crypto isakmp sa
```

dst	src	state	conn-id	slot
20.20.20.1	30.30.30.1	QM_IDLE	1	0

- **mostre IPsec cripto sa** — Indica os ajustes usados por SA atuais. Verifique para ver se há os endereços IP do peer, as redes acessíveis no local e em extremidades remotas, e a transformação ajustada que é usada. Há dois ESP SA, um em cada sentido. Desde que o AH transforma os grupos são usados, ele estão vazios.

```
ipsec_router#show crypto ipsec sa
```

```
interface: Ethernet1/0
```

```
  Crypto map tag: vpn, local addr. 30.30.30.1
```

```
  protected vrf:
```

```
    local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
```

```
    remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
```

```

current_peer: 20.20.20.1:500

    PERMIT, flags={origin_is_acl,}

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

#pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

path mtu 1500, media mtu 1500

current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

sa timing: remaining key lifetime (k/sec): (4471883/28110)

IV size: 16 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x54FA9805(1425709061)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

sa timing: remaining key lifetime (k/sec): (4471883/28110)

IV size: 16 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

- **active do show crypto engine connections** — Indica as conexões de sessão de criptografia ativas atuais para todas as crypto-engines. Cada identificador de conexão é original. O

número de pacotes que são cifrados e decifrados é indicado nas últimas duas colunas.

```
ipsec_router#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0

## [Verifique a configuração do concentrador VPN](#)

Termine estas etapas para verificar a configuração do concentrador VPN.

1. Similar aos **comandos show crypto ipsec sa e show crypto isakmp sa** no Roteadores, você pode ver o IPsec e as estatísticas IKE quando você seleciona a **monitoração > as estatísticas > o IPsec nos** concentradores VPN.
2. Similar ao **comando show crypto engine connections active** no Roteadores, você pode usar o indicador das Administração-sessões no concentrador VPN para ver os parâmetros e as estatísticas para todas as conexões de LAN para LAN ou túneis do IPsec ativo.

## [Troubleshooting](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### [Pesquise defeitos o roteador](#)

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Note:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debug crypto engine** — Exibe o tráfego que está criptografado. A crypto-engine é o mecanismo real que executa a criptografia e a descryptografia. Uma crypto-engine pode ser um software ou um acelerador de hardware.
- **isakmp do debug crypto** — Indica as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1. IKE.
- **IPsec do debug crypto** — Indica as negociações de IPsec da fase 2. IKE.

Refira o [Troubleshooting de IPsec - Compreendendo e usando comandos debug](#) para mais informação detalhada e exemplo de saída.

### [Pesquise defeitos o concentrador VPN](#)

Similar aos **comandos debug nos** roteadores Cisco, você pode configurar classes de evento para ver todos os alarmes.

1. Selecione o **configuração > sistema > eventos > classes > adicionar** para girar sobre o registro das classes de evento. Estas classes estão disponíveis para o



IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

2. Ao adicionar, você pode igualmente selecionar o nível de seriedade para cada classe, com base no nível de seriedade que o alarme está enviado. Os alarmes podem ser segurados por um destes métodos:  
Pelo logIndicado no consoleEnviado ao servidor de Syslog  
UNIXEnviado como um emailEnviado como uma armadilha a um server do Simple Network Management Protocol (SNMP)
3. Selecione a **monitoração** > o **log filtrável de eventos** para monitorar os alarmes permitidos.

## Informações Relacionadas

- [Advanced Encryption Standard \(AES\)](#)
- [Módulo de criptografia DES/3DES/AES VPN](#)
- [Upgrade de software do concentrador VPN](#)
- [Concentrador VPN - Release Note](#)
- [Concentrador VPN que configura interfaces IP](#)
- [Configurações de amostra do IPsec](#)
- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de Suporte de Negociação IPSec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)