

# Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento fornece um exemplo de configuração de um túnel IPSec IOS a IOS usando Padrão de criptografia avançado (AES).

## [Pré-requisitos](#)

### [Requisitos](#)

O apoio da criptografia de AES foi introduzido em Cisco IOS® 12.2(13)T.

### [Componentes Utilizados](#)

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

- Cisco IOS Software Release 12.3(10)
- Cisco 1721 Router

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](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## [Configurar](#)

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

**Nota:** Para localizar informações adicionais sobre os comandos usados neste documento, utilize a

Ferramenta Command Lookup (somente clientes [registrados](#)).

## [Configurações](#)

Este documento utiliza as configurações mostradas aqui.

- [Router 1721-A](#)
- [Router 1721-B](#)

### Router 1721-A

```
R-1721-A#show runBuilding configuration...Current
configuration : 1706 bytes!! Last configuration change at
00:46:32 UTC Fri Sep 10 2004! NVRAM config last updated at
00:45:48 UTC Fri Sep 10 2004!version 12.3service timestamps
debug datetime msecservice timestamps log datetime msecno
service password-encryption!hostname R-1721-A!boot-start-
markerboot-end-marker!!memory-size iomem 15mmpi polling-
interval 60no mmi auto-configureno mmi pvcmmi snmp-timeout
180no aaa new-modelip subnet-zeroip cef!!!ip audit po max-
events 100no ip domain lookupno ftp-server write-enable!!!
!!--- Define Internet Key Exchange (IKE) policy.cryptoisakmp
policy 10!--- Specify the 256-bit AES as the !--- encryption
algorithm within an IKE policy. encr aes 256!--- Specify that
pre-shared key authentication is used. authentication pre-
share!--- Specify the shared secret.cryptoisakmp key
cisco123 address 10.48.66.146!--- Define the IPSec
transform set.cryptoisec transform-set aasset esp-aes 256
esp-sha-hmac !!--- Define crypto map entry name "aesmap" that
will use !--- IKE to establish the security associations
(SA).cryptomap aesmap 10 ipsec-isakmp !--- Specify remote
IPSec peer. set peer 10.48.66.146!--- Specify which transform
sets !--- are allowed for this crypto map entry. set
transform-set aasset !--- Name the access list that
determines which traffic !--- should be protected by IPSec.
match address acl_vpn!!!interface ATM0 no ip address shutdown
no atm ilmi-keepalive dsl equipment-type CPE dsl operating-
mode GSHDSL symmetric annex A dsl linerate AUTO!interface
Ethernet0 ip address 192.168.100.1 255.255.255.0 ip nat
inside half-duplex!interface FastEthernet0 ip address
10.48.66.147 255.255.254.0 ip nat outside speed auto!---
Apply crypto map to the interface. cryptomap aesmap!ip nat
inside source list acl_nat interface FastEthernet0 overloadip
classlessip route 0.0.0.0 0.0.0.0 10.48.66.1ip route
192.168.200.0 255.255.255.0 FastEthernet0no ip http serverno
ip http secure-server!ip access-list extended acl_nat!---
Exclude protected traffic from being NAT'ed. deny ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 permit ip
192.168.100.0 0.0.0.255 any!--- Access list that defines
traffic protected by IPSec.ip access-list extended acl_vpn
permit ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255!!line con 0 exec-timeout 0 0line aux 0line vty 0
4!endR-1721-A#
```

### Router 1721-B

```
R-1721-B#show runBuilding configuration...Current
configuration : 1492 bytes!! Last configuration change at
14:11:41 UTC Wed Sep 8 2004!version 12.3service timestamps
debug datetime msecservice timestamps log datetime msecno
service password-encryption!hostname R-1721-B!boot-start-
markerboot-end-marker!!memory-size iomem 15mmpi polling-
```

```

interval 60no mmi auto-configureno mmi pvcmmi snmp-timeout
180no aaa new-modelip subnet-zeroip cef!!!ip audit po max-
events 100no ip domain lookupno ftp-server write-enable!!!
!!--- Define IKE policy.crypto isakmp policy 10!--- Specify
the 256-bit AES as the !--- encryption algorithm within an
IKE policy. encr aes 256!--- Specify that pre-shared key
authentication is used. authentication pre-share!--- Specify
the shared secret.crypto isakmp key cisco123 address
10.48.66.147!--- Define the IPsec transform set.crypto
ipsec transform-set aasset esp-aes 256 esp-sha-hmac !!---
Define crypto map entry name "aesmap" that uses !--- IKE to
establish the SA.crypto map aesmap 10 ipsec-isakmp !---
Specify remote IPsec peer. set peer 10.48.66.147!--- Specify
which transform sets !--- are allowed for this crypto map
entry. set transform-set aasset !--- Name the access list
that determines which traffic !--- should be protected by
IPsec. match address acl_vpn!!!interface Ethernet0 ip address
192.168.200.1 255.255.255.0 ip nat inside half-
duplex!interface FastEthernet0 ip address 10.48.66.146
255.255.254.0 ip nat outside speed auto!--- Apply crypto map
to the interface. crypto map aesmap!ip nat inside source list
acl_nat interface FastEthernet0 overloadip classlessip route
0.0.0.0 0.0.0.0 10.48.66.1ip route 192.168.100.0
255.255.255.0 FastEthernet0no ip http serverno ip http
secure-server!ip access-list extended acl_nat!--- Exclude
protected traffic from being NAT'ed. deny ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 permit ip 192.168.200.0
0.0.0.255 any!--- Access list that defines traffic protected
by IPsec.ip access-list extended acl_vpn permit ip
192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255!!line con 0
exec-timeout 0 0line aux 0line vty 0 4!endR-1721-B#

```

## Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando 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.

- **mostre isakmp cripto sa?** Indica o estado para Internet Security Association and Key Management Protocol (ISAKMP) SA.
- **mostre IPsec cripto sa?** Indica as estatísticas nos túneis ativo.
- **active do show crypto engine connections?** Indica o total cifra/decifra pelo SA.

## Troubleshooting

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

### Comandos para Troubleshooting

**Nota:** Antes de emitir comandos debug, consulte [Informações importantes sobre comandos debug](#).

- **IPsec do debug crypto?** Eventos de IPsec dos indicadores.
- **isakmp do debug crypto?** Indica mensagens sobre eventos IKE.
- **motor do debug crypto?** Indica a informação da crypto-engine.

[Informações adicionais sobre Troubleshooting de IPsec podem ser encontradas em Troubleshooting de Segurança de IP - Compreendendo e Utilizando os comandos debug.](#)

## Informações Relacionadas

- [Software Cisco IOS versões 12.2T AES \(Padrão de criptografia avançado\)](#)
- [Configurando a segurança da rede IPsec](#)
- [Página de suporte do IPsec](#)
- [Suporte Técnico - Cisco Systems](#)