

Configurando IPSec de IOS para IOS usando criptografia de AES

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.

Note: 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 run
Building 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 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-A
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
```

```

!
!

!--- Define Internet Key Exchange (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 10.48.66.146
!
!

!--- Define the IPSec transform set. crypto ipsec
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).
crypto map 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. crypto map
aesmap
!
ip nat inside source list acl_nat interface
FastEthernet0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.48.66.1
ip route 192.168.200.0 255.255.255.0 FastEthernet0
no ip http server
no 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 0
line aux 0
line vty 0 4
!
end

R-1721-A#
```

Router 1721-B

```
R-1721-B#show run
Building configuration...

Current configuration : 1492 bytes
!
! Last configuration change at 14:11:41 UTC Wed Sep 8
2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-B
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no 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 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.48.66.1
ip route 192.168.100.0 255.255.255.0 FastEthernet0
no ip http server
no 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 0
line aux 0
line vty 0 4
!
end
R-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.

- `show crypto isakmp sa`—Exibe o estado do SA do protocolo ISAKMP.
- `show crypto ipsec sa` — Exibe as estatísticas nos túneis ativos.
- **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](#)

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

- `debug crypto ipsec` — Exibe eventos de IPSec.
- `debug crypto isakmp` - Exibe mensagens sobre eventos IKE.
- `debug crypto engine` — Exibe informações a partir do cripto mecanismo.

[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](#)