

Configuración de IPSec de IOS a IOS mediante encriptación AES

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento provee una configuración de ejemplo para un túnel IOS-a-IOS IPSec mediante el encriptación del Estándar de encriptación avanzado (AES).

[prerrequisitos](#)

[Requisitos](#)

El soporte de la encriptación AES se ha introducido en Cisco IOS® 12.2(13)T.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Configuraciones

Este documento usa las configuraciones detalladas aquí.

- [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#

```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- show crypto isakmp sa—Muestra el estado de la Asociación de seguridad en Internet y el Protocolo de administración de claves (ISAKMP) SA.
- show crypto ipsec sa — Muestra las estadísticas en los túneles activos.
- **active del show crypto engine connections** — Visualiza el total cifra/descripta por el SA.

[Troubleshooting](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

[Comandos para resolución de problemas](#)

Note: Antes de ejecutar un comando debug, consulte [Información Importante sobre Comandos Debug](#).

- debug crypto ipsec — Muestra eventos de IPSec.
- debug crypto isakmp — Muestra mensajes acerca de eventos IKE.
- debug crypto engine — Muestra información del motor de criptografía.

[Puede encontrar información adicional sobre la resolución de problemas de IPSec en Resolución de problemas de seguridad IP – Introducción y uso de los comandos de depuración.](#)

[Información Relacionada](#)

- [Software Cisco IOS 12.2T – Norma de encriptación avanzado \(AES\)](#)
- [Configuración de seguridad de red IPSec](#)
- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)