

# Konfigurieren von IOS zu IOS IPSec mithilfe der AES-Verschlüsselung

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Dieses Dokument enthält eine Beispielkonfiguration für einen IOS-zu-IOS IPSec-Tunnel unter Verwendung der AES-Verschlüsselung (Advanced Encryption Standard).

## [Voraussetzungen](#)

### [Anforderungen](#)

AES-Verschlüsselungsunterstützung wurde in Cisco IOS® 12.2(13)T eingeführt.

### [Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Softwareversion 12.3(10)
- Cisco 1721-Router

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### [Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#).

## [Konfigurieren](#)

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

## [Konfigurationen](#)

In diesem Dokument werden die hier gezeigten Konfigurationen verwendet.

- [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#

```

## Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto isakmp sa**: Zeigt den Status für die Internet Security Association and Key Management Protocol (ISAKMP) SA an.
- **show crypto ipsec sa**: Zeigt die Statistiken der aktiven Tunnel an.
- **show crypto engine connections active** - Zeigt die Gesamtzahl der Verschlüsselungen/Entschlüsselungen pro SA an.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

### Befehle zur Fehlerbehebung

**Hinweis:** Bevor Sie **Debugbefehle** ausgeben, lesen Sie [Wichtige Informationen über Debug-Befehle](#).

- **debug crypto ipsec**: Zeigt IPSec-Ereignisse an.
- **debug crypto isakmp**: Zeigt Meldungen über IKE-Ereignisse an.
- **debug crypto engine**: Zeigt Informationen vom Crypto Engine an.

Weitere Informationen zur Fehlerbehebung für IPSec finden Sie unter [IP Security Troubleshooting - Understanding and Using Debug Commands](#).

## Zugehörige Informationen

- [Cisco IOS Software Releases 12.2T - Advanced Encryption Standard \(AES\)](#)
- [Konfigurieren der IPSec-Netzwerksicherheit](#)
- [IPSec-Support-Seite](#)
- [Technischer Support - Cisco Systems](#)