

# Konfigurieren von IPSec zwischen drei Routern mithilfe von privaten Adressen

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In diesem Dokument wird eine vollständig vernetzte Konfiguration mit drei Routern beschrieben, die private Adressen verwenden. Im Beispiel werden folgende Features veranschaulicht:

- Encapsulating Security Payload (ESP) - nur Data Encryption Standard (DES)
- Vorinstallierte Schlüssel
- Private Netzwerke hinter jedem Router: 192.168.1.0, 192.168.2.0 und 192.168.3.0
- isakmp-Richtlinie und Konfiguration der Crypto Map
- Tunnel-Datenverkehr definiert mit den Befehlen **access-list** und **route-map**. Neben Port Address Translation (PAT) können Routing-Karten auch auf eine statische Network Address Translation (NAT) in Cisco IOS® Software, Version 12.2(4)T2 und höher, angewendet werden. Weitere Informationen finden Sie unter [Übersicht über die Funktion Routenzuordnungen mit statischen Übersetzungen](#).

**Hinweis:** Verschlüsselungstechnologie unterliegt Exportkontrollen. Es liegt in Ihrer Verantwortung, das Gesetz über den Export von Verschlüsselungstechnologien zu kennen. Wenn Sie Fragen zur Exportkontrolle haben, senden Sie eine E-Mail an [export@cisco.com](mailto:export@cisco.com).

## [Voraussetzungen](#)

### [Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

## Verwendete Komponenten

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

- Cisco IOS Softwareversion 12.3.(7)T.
- Cisco Router, die mit IPSec konfiguriert wurden.

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](#).

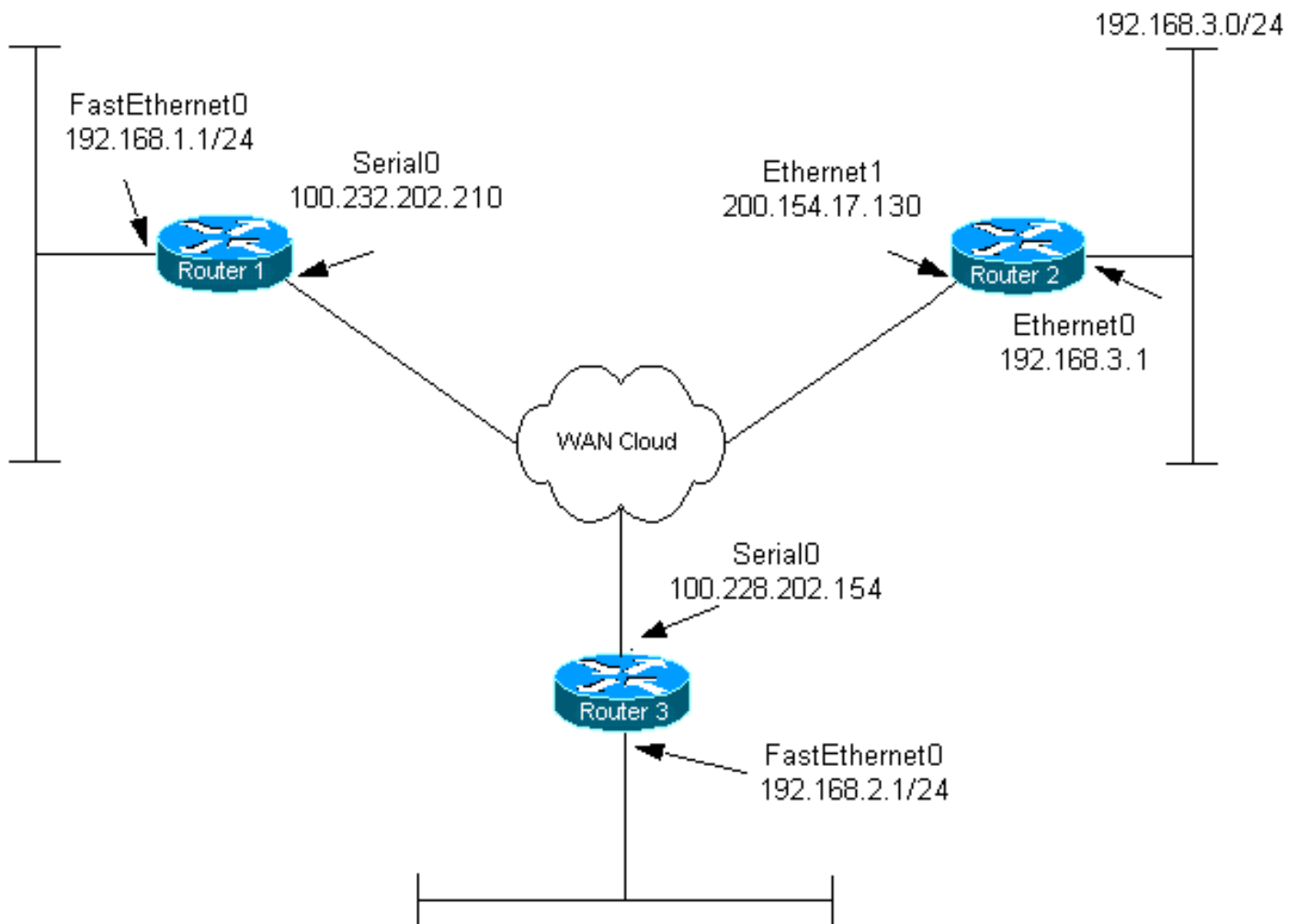
## Konfigurieren

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).

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- [Router 1](#)
- [Router 2](#)
- [Router 3](#)

### Router 1

```

Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!

```

```
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4
authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Serial0

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 20 ipsec-isakmp
    set peer 100.228.202.154
    set transform-set encrypt-des
    match address 106
crypto map combined 30 ipsec-isakmp
    set peer 200.154.17.130
    set transform-set encrypt-des
    match address 105
!
!
interface Serial0
    ip address 100.232.202.210 255.255.255.252
    ip nat outside
    serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
interface FastEthernet0
    ip address 192.168.1.1 255.255.255.0
    ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- Access control list (ACL) that shows traffic to
encrypt over the tunnel. access-list 105 permit ip
192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

```
!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.1.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

## Router 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 100.232.202.210
!
!

!--- IPSec policies. crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Ethernet1

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 7 ipsec-isakmp
set peer 100.232.202.210
```

```

    set transform-set encrypt-des
    match address 105

crypto map combined 8 ipsec-isakmp
    set peer 100.228.202.154
    set transform-set encrypt-des
    match address 106
!
!
!
interface Ethernet0
    ip address 192.168.3.1 255.255.255.0
    ip nat inside
!
interface Ethernet1
    ip address 200.154.17.130 255.255.255.224
    ip nat outside

!--- Apply the crypto map to the interface. crypto map
combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Ethernet1 overload

!--- ACL shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 106 permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip any any

!--- Do not perform NAT on the IPsec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

## Router 3-Konfiguration

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.232.202.210
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined local-address
Serial0
crypto map combined 7 ipsec-isakmp
  set peer 100.232.202.210
  set transform-set encrypt-des
  match address 106
crypto map combined 8 ipsec-isakmp
  set peer 200.154.17.130
  set transform-set encrypt-des
  match address 105
!
!
interface Serial0
  ip address 100.228.202.154 255.255.255.252
  ip nat outside
  serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
  interface FastEthernet0
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- ACL that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.2.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
    login
!
!
end

```

## 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 engine connections active** - Zeigt verschlüsselte und entschlüsselte Pakete zwischen IPSec-Peers an.
- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa**: Zeigt die von aktuellen (IPSec) SAs verwendeten Einstellungen.

## Fehlerbehebung



Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

## Befehle zur Fehlerbehebung

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

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

**Hinweis:** Die folgenden Debug-Prozesse müssen auf beiden IPSec-Routern (Peers) ausgeführt werden. Das Löschen von SAs muss auf beiden Peers erfolgen.

- **debug crypto isakmp:** Zeigt Fehler in Phase 1 an.
- **debug crypto ipsec:** Zeigt Fehler in Phase 2 an.
- **debug crypto engine:** Zeigt Informationen vom Crypto Engine an.
- **clear crypto connection *connection-id* [*Steckplatz* | *rsm* | *vip*]** —Beendet eine aktuell laufende verschlüsselte Sitzung. Verschlüsselte Sitzungen enden normalerweise, wenn die Sitzung das Zeitlimit überschreitet. Verwenden Sie den Befehl **show crypto cisco connections**, um den Wert *connection-id* zu ermitteln.
- **clear crypto isakmp** - Löscht die SAs der Phase 1.
- **clear crypto sa:** Löscht die SAs der Phase 2.

## Zugehörige Informationen

- [IPSec-Support-Seite](#)
- [Technischer Support - Cisco Systems](#)