# プライベート アドレスを使用する 3 つのルータ間での IPSec の設定

## 目次



## 概要

このドキュメントでは、プライベート アドレスを使用する 3 つのルータ間のフルメッシュ構成について説明しています。 この例では、次の機能について説明しています。

- Encapsulating Security Payload（ESP）：Data Encryption Standard（DES; データ暗号規格）のみ
- 事前共有キー
- 各ルータの背後のプライベート ネットワーク： 192.168.1.0、192.168.2.0、および 192.168.3.0
- isakmp ポリシーおよびクリプトマップの設定
- **access-list** および **route-map** コマンドで定義されるトンネル トラフィック。 ポート アドレス変換（PAT）に加えて、ルート マップはに IOS® ソフトウェアリリース 12.2(4)T2 およびそれ以降 1 対 1 静的なネットワークアドレス変換（NAT） on Cisco 加えることができます。 詳細については、『NAT：ルート マップを使用したスタティック変換』を参照してください。

**注:** 暗号化テクノロジーは輸出規制の対象になります。 暗号化テクノロジーの輸出に関連する法規を理解することは、お客様の責任となります。 輸出規制に関する詳細については、電子メールで export@cisco.com までお問い合わせください。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.3.(7)T
- IPSec が設定された Cisco ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

## 設定

このドキュメントでは、次の設定を使用します。

- ルータ 1
- ルータ 2
- ルータ 3

**ルータ 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
```

**ルータ 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
```

## ルータ 3 の設定

```
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
```

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto engine connections active**：IPSec ピア間の暗号化および復号化されたパケットを表示します。
- **show crypto isakmp sa**：ピアにおける現在の IKE セキュリティ アソシエーション（SA）をすべて表示します。
- **show crypto ipsec sa**：現在の（IPSec）SA で使用されている設定を表示します。

# トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

## トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

**注:** debug コマンドを使用する前に、『debug コマンドに関する重要な情報』を参照してください。

**注:** 次のデバッグは両方の IPSec ルータ（ピア）で実行する必要があります。 SA のクリアは両方のピアで行う必要があります。

- **debug crypto isakmp**：フェーズ 1 のエラーを表示します。
- **debug crypto ipsec**：フェーズ 2 のエラーを表示します。
- **debug crypto engine**：暗号化エンジンからの情報を表示します。
- **clear crypto connection connection-id [slot** / *rsm* / **vip]**：現在進行中の暗号化セッションを終了します。 通常、暗号化セッションは、タイムアウトになると終了します。 connection-id 値を調べるには、**show crypto cisco connections** コマンドを使用します。
- **clear crypto isakmp**：フェーズ 1 SA をクリアします。
- **clear crypto sa**：フェーズ 2 SA をクリアします。

## 関連情報

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems