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

内容

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。Port Address Translation（PAT；ポートアドレス変換）に加えて、ルートマップは、Cisco IOS®ソフトウェアリリース12.2T2以降で1対1のスタティックNetwork Address Translation（NAT；ネットワークアドレス変換）に適用できます。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、輸出規制の対象となります。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特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いています。

- 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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「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。

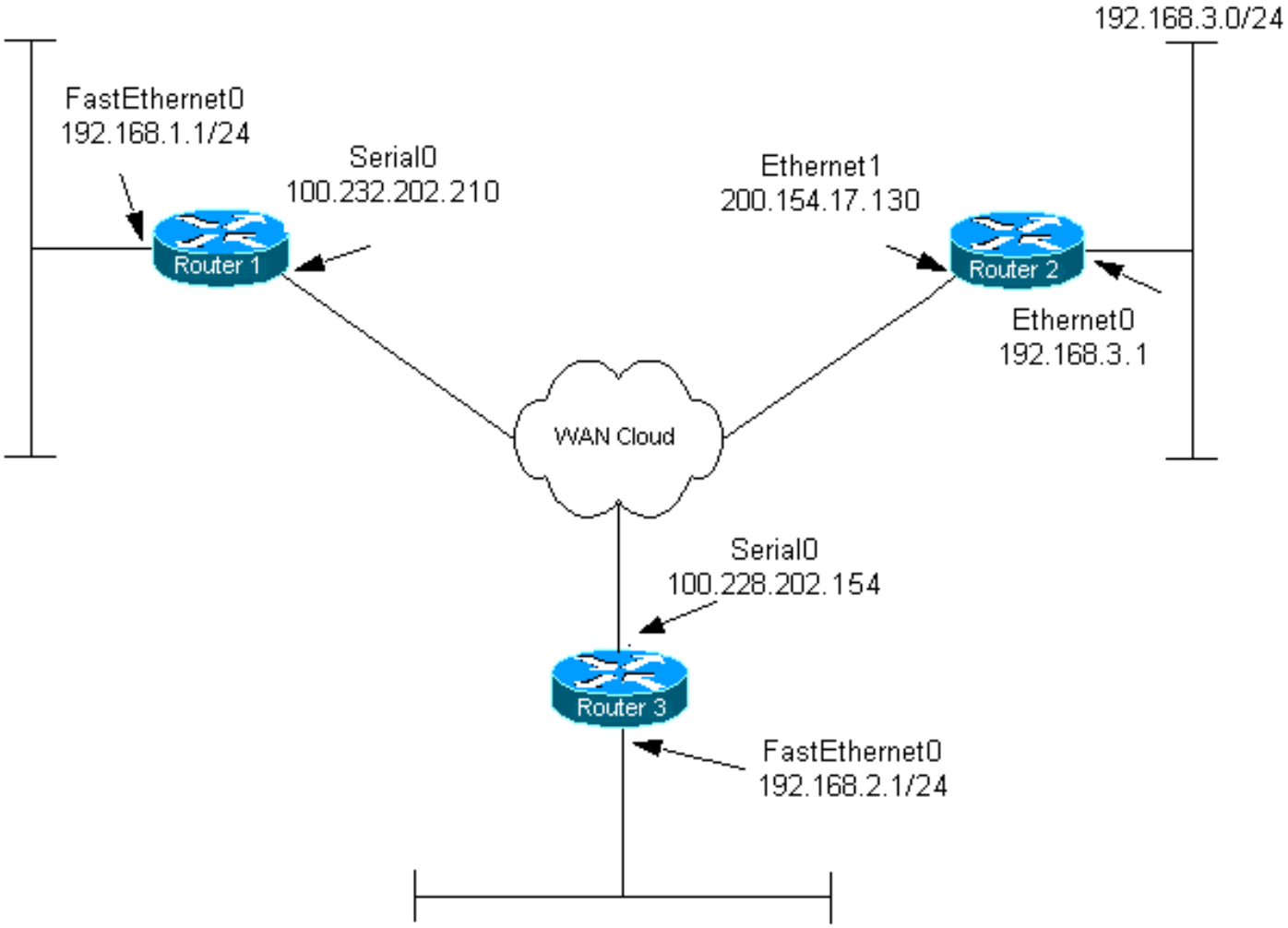
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

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 セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- ルータ 1
- ルータ 2
- Router 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

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- 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。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

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）で実行されている必要があります。 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