使用私有地址配置三台路由器之間的IPSec

目錄

簡介

本文檔介紹使用私有地址的三台路由器的全網狀配置。該示例說明了以下功能：

- 封裝安全性裝載(ESP) — 僅資料加密標準(DES)
- 預共用金鑰
- 每台路由器後面的專用網路：192.168.1.0、192.168.2.0和192.168.3.0
- isakmp策略和加密對映配置
- 使用**access-list**和**route-map**命令定義的隧道流量。除了連線埠位址轉譯(PAT)之外，路由對應還可以套用到Cisco IOS®軟體版本12.2(4)T2和更新版本上的一對一靜態網路位址轉譯(NAT)。有關詳細資訊，請參閱NAT — 能夠將路由對映與靜態轉換功能結合使用概述。

註：加密技術受出口管制約束。您有責任瞭解關於加密技術出口的法律。如果您對出口管制有任何疑問，請傳送電子郵件至export@cisco.com。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.3.(7)T。

- 配置了IPSec的Cisco路由器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

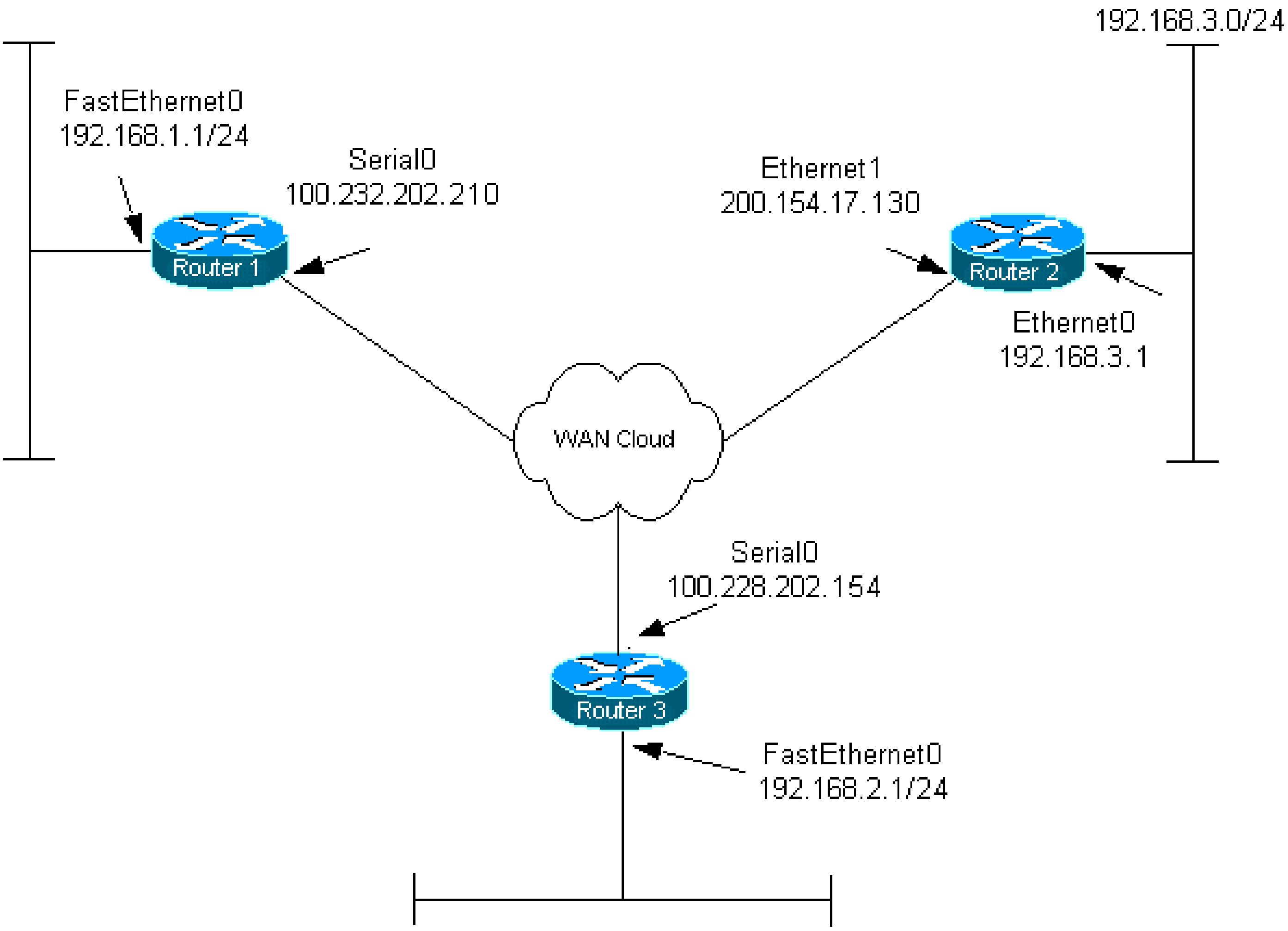
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- 路由器1

- 路由器2
- 路由器3

路由器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
```

路由器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
```

路由器3配置

```

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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto engine connections active** — 顯示IPSec對等體之間的加密和解密資料包。
- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(SA)。
- **show crypto ipsec sa** — 顯示當前(IPSec)SA使用的設定。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出**debug指令之前，請先參閱**有關Debug指令的重要資訊。

注意：以下調試必須在兩個IPSec路由器（對等體）上運行。 必須在兩個對等體上清除SA。

- **debug crypto isakmp** — 顯示階段1期間的錯誤。
- **debug crypto ipsec** — 顯示階段2期間的錯誤。
- **debug crypto engine** — 顯示來自加密引擎的資訊。
- **clear crypto connection** ***connection-id [slot*** *| rsm | vip]* — 終止當前正在執行的加密會話。加密的作業階段通常會在作業階段逾時終止。使用**show crypto cisco connections**命令獲取connection-id值。
- **clear crypto isakmp** — 清除第1階段SA。
- **clear crypto sa** — 清除第2階段SA。

相關資訊

- IPSec支援頁面
- 技術支援 - Cisco Systems