在具有重複LAN子網的路由器之間配置IPSec隧道

目錄

簡介

本文提供一個網路範例，該範例模擬兩個採用相同IP定址方案的合併公司。兩台路由器通過VPN隧道連線，並且每台路由器後面的網路相同。為使一個站點訪問另一個站點的主機，路由器上使用網路地址轉換(NAT)將源地址和目標地址更改為不同的子網。

注意：建議不要將此配置作為永久設定，因為從網路管理的角度來看，這會造成混亂。

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：

- 路由器A:執行Cisco IOS®軟體版本12.3(4)T的Cisco 3640路由器
- 路由器B:運行Cisco IOS®軟體版本12.3(5)的Cisco 2621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。

背景資訊

在本示例中，當站點A的主機172.16.1.2訪問站點B的相同IP地址主機時，它會連線到172.19.1.2地址而不是實際的172.16.1.2地址。當站點B的主機訪問站點A時，它會連線到一個172.18.1.2地址。路由器A上的NAT將任何172.16.x.x地址轉換為類似於匹配的172.18.x.x主機條目。路由器B上的NAT將172.16.x.x更改為類似172.19.x.x。

每台路由器的加密功能會加密串列介面上的已轉換流量。請注意，NAT在路*由器*加密之前進行。

注意：此配置僅允許兩個網路通訊。它不允許Internet連線。您需要額外的路徑連線到Internet，以便連線到這兩個站點以外的其他位置；換句話說，您需要在兩端新增另一個路由器或防火牆，並在主機上配置多個路由。

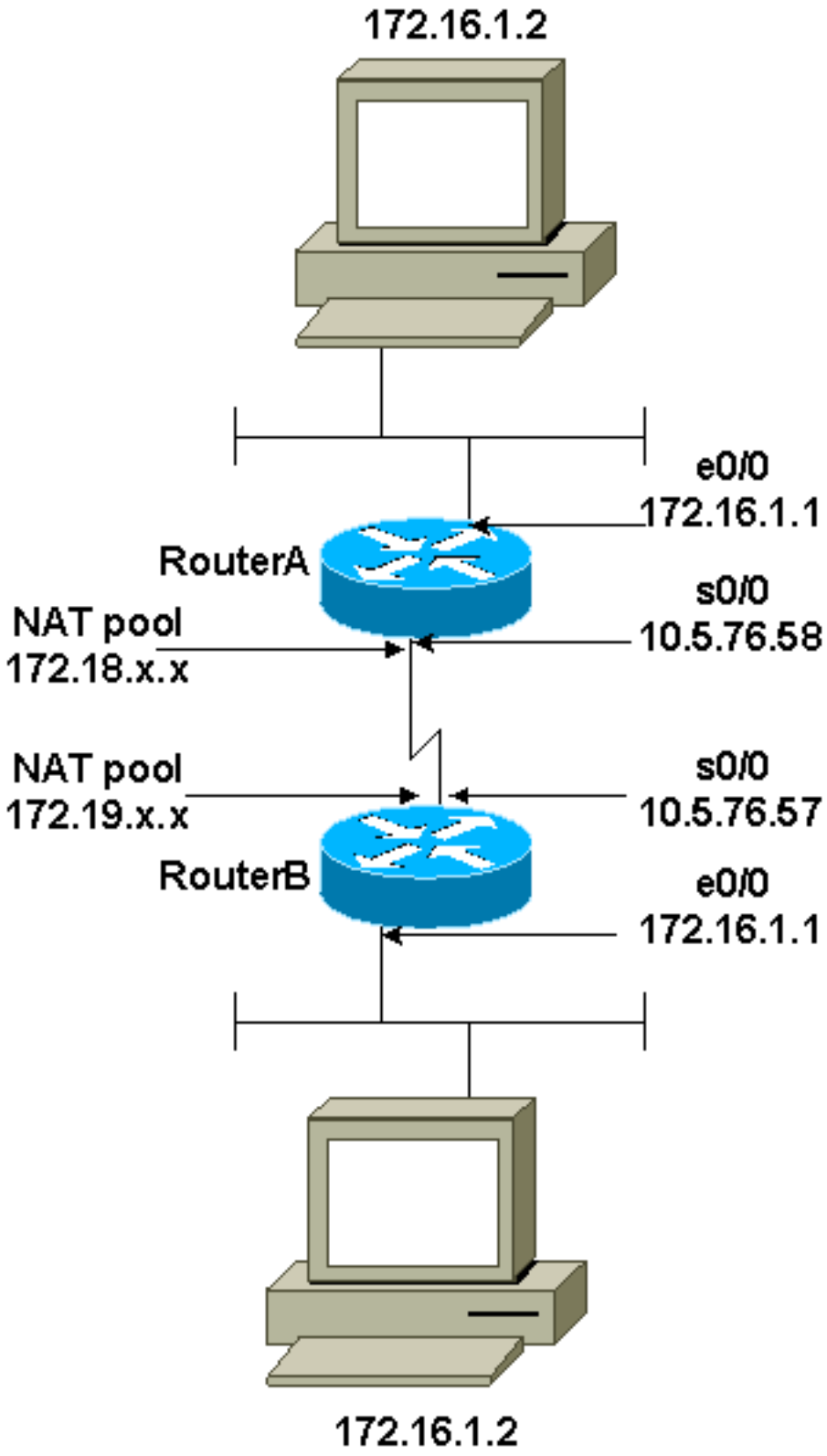
設定

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A
- 路由器B

路由器A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.57
 set transform-set myset1
  !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
 description Interface to Internet
 ip address 10.5.76.58 255.255.0.0
 ip nat outside
 clockrate 128000
 crypto map mymap
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

路由器B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.58
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.58
 set transform-set myset1
!--- Encrypt traffic to the other side.  match address
100
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 description Interface to Internet
```

```
 ip address 10.5.76.57 255.255.0.0
 ip nat outside
 crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
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 ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 顯示第1階段安全關聯。
- show ip nat translation — 顯示當前使用的NAT轉換。

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命令之前，請參閱**有關Debug命令的重要資訊**。**

- debug crypto ipsec — 顯示第2階段的IPSec協商。
- debug crypto isakmp — 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- debug crypto engine — 顯示加密的流量。

相關資訊

- IPSec支援頁面
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定

- 技術支援 - Cisco Systems