使用NAT和靜態配置路由器IPsec隧道專用到專用網路

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[ACL中的Deny語句為何指定NAT流量？](#)
[但是，靜態NAT又如何呢？為什麼我無法通過IPsec隧道訪問該地址？](#)
[設定](#)
[網路圖表](#)
[組態](#)
[驗證](#)
[疑難排解](#)
[疑難排解指令](#)
[相關資訊](#)

簡介

此示例配置演示如何：

- 加密兩個私人網路（10.1.1.x和172.16.1.x）之間的流量。
- 將靜態IP地址（外部地址200.1.1.25）分配給位於10.1.1.3的網路裝置。

您使用存取控制清單(ACL)告知路由器不要對私人到私人網路流量執行網路位址轉譯(NAT)，該流量會進行加密並在離開路由器時放在通道上。在此示例配置中，也存在用於10.1.1.x網路上的內部伺服器的靜態NAT。此示例配置使用NAT命令上的route-map選項，在流向它的流量也通過加密隧道傳送時阻止它成為NAT。

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(14)T
- 兩台思科路由器

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。

ACL中的Deny語句為何指定NAT流量？

使用Cisco IOS IPsec或VPN時，在概念上將網路替換為隧道。在此圖中，您使用從200.1.1.1到100.1.1.1的Cisco IOS IPsec隧道替換網際網路雲。從透過通道連結在一起的兩個私人LAN的角度讓此網路變得透明。出於此原因，您通常不想對從一個專用LAN到遠端專用LAN的流量使用NAT。當資料包到達內部Router 3網路時，您希望看到來自Router 2網路且源IP地址來自10.1.1.0/24網路而不是200.1.1.1的資料包。

有關如何配置NAT的詳細資訊，請參閱NAT操作順序。本文檔顯示，當資料包從內部傳到外部時，NAT發生在加密檢查之前。這就是必須在配置中指定此資訊的原因。

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

注意：也可以構建隧道並仍然使用NAT。在此案例中，您將NAT流量指定為「IPsec的相關流量」（在本文檔的其他部分中稱為ACL 101）。有關如何在NAT處於活動狀態時構建隧道的詳細資訊，請參閱在帶有重複LAN子網的路由器之間配置IPsec隧道。

但是，靜態NAT又如何呢？為什麼我無法通過IPsec隧道訪問該地址？

此設定還包括一個靜態的一對一NAT ，用於位於10.1.1.3的伺服器。這是到200.1.1.25的NAT，以便Internet使用者可以訪問它。發出以下命令：

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

此靜態NAT禁止172.16.1.x網路上的使用者通過加密隧道訪問10.1.1.3。這是因為您需要使用ACL 122拒絕加密流量進行NAT。但是，對於與10.1.1.3之間的所有連線，靜態NAT命令優先於通用NAT語句。靜態NAT語句並不專門拒絕加密流量也進行NAT。當172.16.1.x網路上的使用者連線到10.1.1.3時，來自10.1.1.3的應答將通過NAT傳送到200.1.1.25，因此不會通過加密的隧道返回（加密之前會發生NAT）。

您必須對靜態NAT語句使用**route-map**命令拒絕加密流量進行NAT'd（甚至靜態一對一NAT'd）。

注意：只有Cisco IOS軟體版本12.2(4)T及更高版本才支援靜態NAT上的route-map選項。請參閱 NAT — 能夠將路由對應與靜態轉譯搭配使用以瞭解其他資訊。

您必須發出以下附加命令，以允許對靜態NAT主機10.1.1.3的加密訪問：

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

這些語句告知路由器僅將靜態NAT應用於與ACL 150匹配的流量。 ACL 150表示不要將該NAT應用於源自10.1.1.3並通過加密隧道發往172.16.1.x的流量。但是，請將其應用於來源為10.1.1.3的所有其他流量（基於網際網路的流量）。

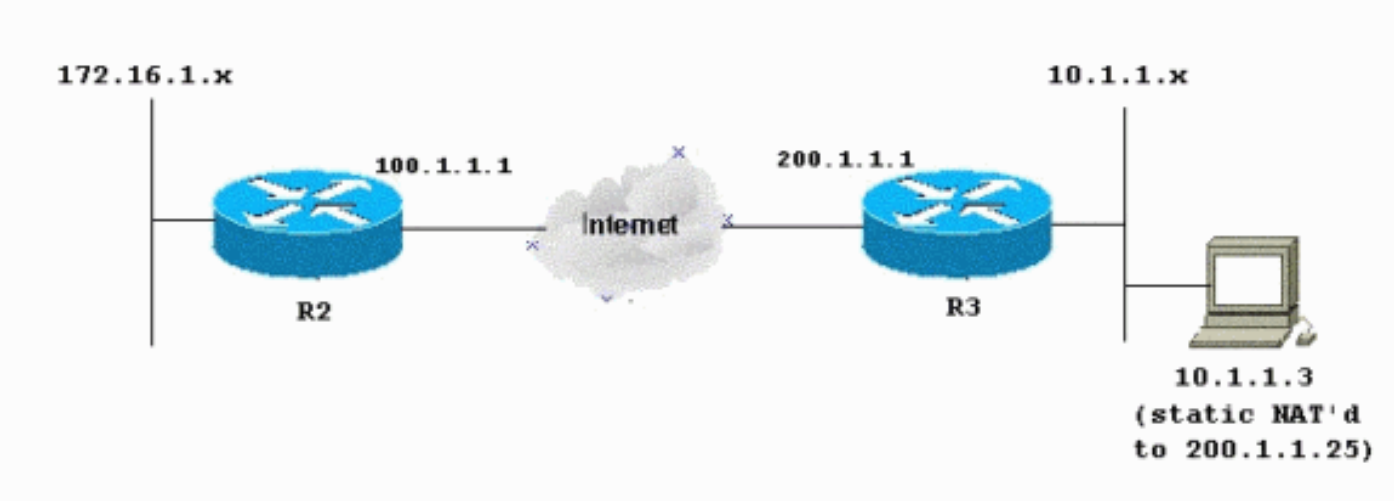
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

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2
- 路由器3

R2 — 路由器配置

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
```

```
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3 — 路由器配置

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
```

```
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

使用本節內容，對組態進行疑難排解。

請參閱IP安全性疑難排解 — 瞭解和使用debug命令以瞭解其他資訊。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug crypto ipsec sa** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp sa** — 請參見階段1的ISAKMP協商。
- **debug crypto engine** — 顯示加密會話。

相關資訊

- **IPsec協商/IKE通訊協定 — Cisco Systems**
- **技術支援與文件 - Cisco Systems**