在VPN 3000集中器上為IPSec配置NAT透明模式

目錄

簡介

網路位址轉譯(NAT)是為了解決網際網路通訊協定第4版(IPV4)用盡位址空間的問題而開發的。如今，家庭使用者和小型辦公室網路使用NAT作為購買註冊地址的替代方案。公司單獨實施NAT或使用防火牆實施NAT以保護其內部資源。

最常用的NAT解決方案「多對一」將多個私有地址對映到單個可路由（公共）地址；這也稱為埠地址轉換(PAT)。 關聯在埠級別實施。PAT解決方案為不使用任何埠的IPSec流量帶來問題。

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 VPN 3000 Concentrator
- Cisco VPN 3000客戶端版本2.1.3及更高版本
- 適用於NAT-T的Cisco VPN 3000客戶端和集中器版本3.6.1及更高版本

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。

封裝安全性裝載

協定50（封裝安全負載[ESP]）處理IPSec的加密/封裝資料包。大多數PAT裝置不能與ESP配合使用，因為它們已被程式設計為僅與傳輸控制協定(TCP)、使用者資料包協定(UDP)和網際網路控制消息協定(ICMP)配合使用。 此外，PAT裝置無法對映多個安全引數索引(SPI)。 VPN 3000客戶端中的NAT透明模式通過將ESP封裝在UDP中並將其傳送到協商埠來解決此問題。要在VPN 3000集中器上啟用的屬性的名稱是通過NAT啟用的IPSec。

作為IETF標準的新協定NAT-T（截至本文撰寫時仍處於DRAFT階段）也將IPSec資料包封裝在UDP中，但它可在埠4500上運行。該埠不可配置。

NAT透明模式如何工作？

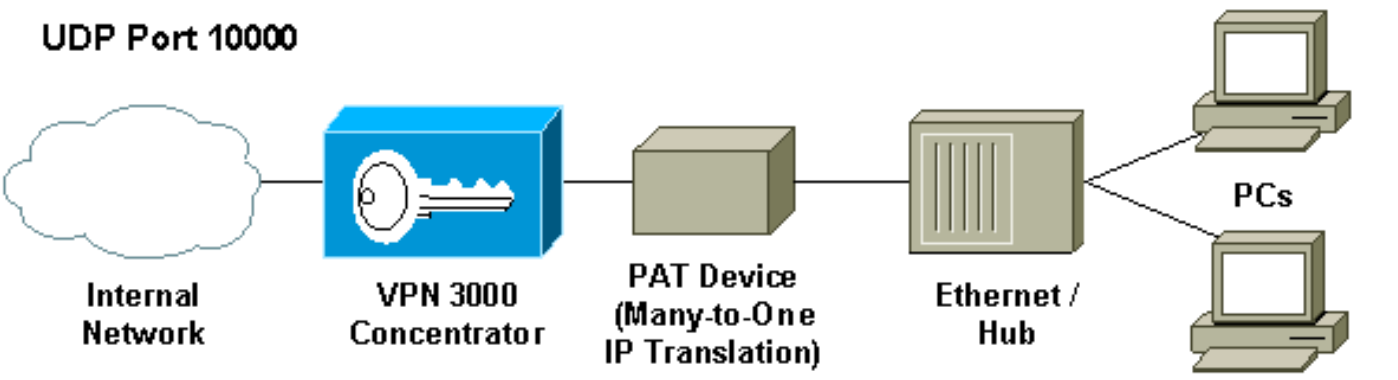
在VPN集中器上啟用IPSec透明模式會建立不可見的過濾器規則並將它們應用於公共過濾器。然後，當VPN客戶端連線時，配置的埠號透明地傳遞到VPN客戶端。在入站端，來自該埠的UDP入站流量直接傳遞到IPSec進行處理。流量經過解密和解除封裝，然後正常路由。在出站端，IPSec對一個UDP報頭進行加密、封裝並應用（如果已配置）。 在以下三種情況下，運行時篩選器規則將被取消啟用並從相應的篩選器中刪除：當組禁用IPSec over UDP時、組被刪除時，或者該埠上最後一個活動的IPSec over UDP SA被刪除時。傳送Keepalive以防止NAT裝置由於不活動而關閉埠對映。

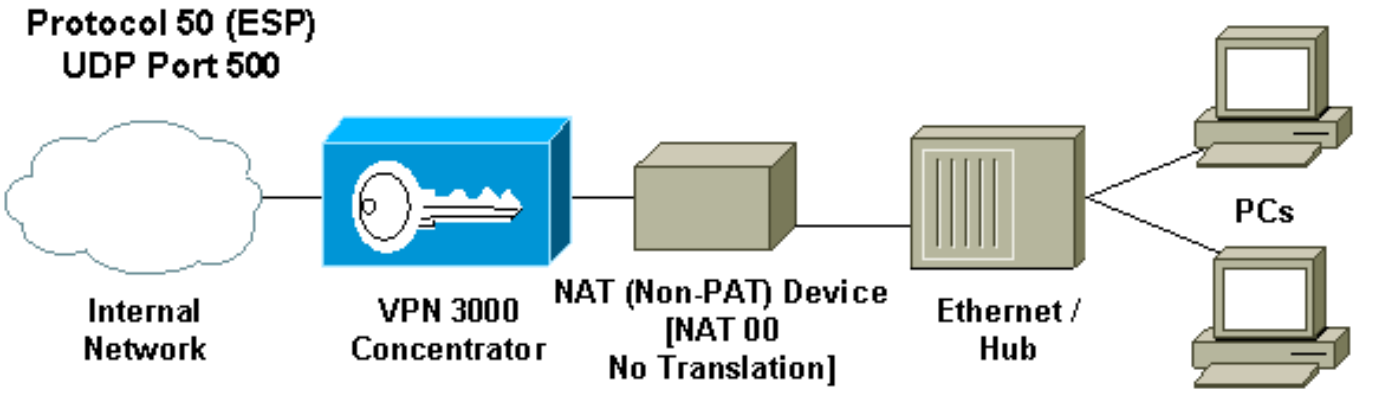
如果在VPN集中器上啟用了IPSec over NAT-T，則VPN集中器/VPN客戶端使用UDP封裝的NAT-T模式。NAT-T在IKE協商期間自動檢測VPN客戶端和VPN集中器之間的任何NAT裝置。您必須確保UDP埠4500在VPN集中器/VPN客戶端之間未被阻止，NAT-T才能正常工作。此外，如果您使用的是已經使用該埠的先前IPSec/UDP配置，則必須重新配置該先前IPSec/UDP配置以使用不同的UDP埠。由於NAT-T是IETF草案，因此如果其他供應商實施此標準，則使用多供應商裝置會有幫助。

NAT-T可同時與VPN客戶端連線和LAN到LAN連線配合使用，這與IPSec over UDP/TCP不同。此外，Cisco IOS®路由器和PIX防火牆裝置支援NAT-T。

您不需要啟用IPSec over UDP即可使NAT-T正常工作。

配置NAT透明模式





使用以下過程在VPN集中器上配置NAT透明模式。

注意：IPSec over UDP是基於每個組配置的，而IPSec over TCP/NAT-T是全域性配置的。

1. 配置IPSec over UDP:在VPN集中器上，選擇**Configuration > User Management > Groups**。要新增組，請選擇**Add**。要修改現有組，請選擇它並按一下**Modify**。按一下IPSec頁籤，檢查**通過NAT的IPSec**，並配置**通過NAT UDP埠的IPSec**。通過NAT的IPSec的預設埠為10000（源和目標），但此設定可能會更改。
2. 配置IPSec over NAT-T和/或IPSec over TCP:在VPN集中器上，選擇Configuration > **System > Tunneling Protocols > IPSec > NAT Transparency**。選中**IPSec over NAT-T和/或TCP**覈取方塊。

如果已啟用所有功能，請使用以下優先順序：

1. 使用TCP的IPSec。
2. 使用NAT-T的IPSec。
3. 使用UDP的IPSec。

使用NAT透明的Cisco VPN客戶端配置

要使用IPSec over UDP或NAT-T，您需要在Cisco VPN客戶端3.6及更高版本上啟用IPSec over UDP。在使用UDP的IPSec的情況下，UDP埠由VPN集中器分配，而對於NAT-T，該埠固定到UDP埠4500。

要使用IPSec over TCP，您需要在VPN客戶端上啟用它，並配置應手動使用的埠。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN 3000系列使用者端支援頁面
- IPSec支援頁面
- 技術支援 - Cisco Systems