使用NAT隱藏ONS 15454的實際IP地址以建立CTC會話

目錄

簡介

本文提供網路位址轉譯(NAT)的範例組態，以便在思科傳輸控制器(CTC)和ONS 15454之間建立作業階段。當ONS 15454位於私人網路中，CTC使用者端位於公共網路中時，此組態會使用NAT和存取清單。

出於安全考慮，應用NAT和訪問清單。NAT隱藏ONS 15454的實際IP地址。訪問清單用作防火牆，以控制進出該ONS 15454的IP流量。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 具有Cisco ONS 15454基礎知識。
- 請注意哪些Cisco路由器支援NAT。

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12.1(11)及更新版本
- Cisco ONS 15454 5.X及更新版本

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。

背景資訊

本節提供基本的背景資訊。

拓撲

測試拓撲包括：

- 一個Cisco ONS 15454，充當伺服器。
- 一台PC，用作CTC客戶端。
- 一台Cisco 2600系列路由器，提供NAT支援。

註：Cisco ONS 15454位於內部網路中，而PC位於外部網路中。

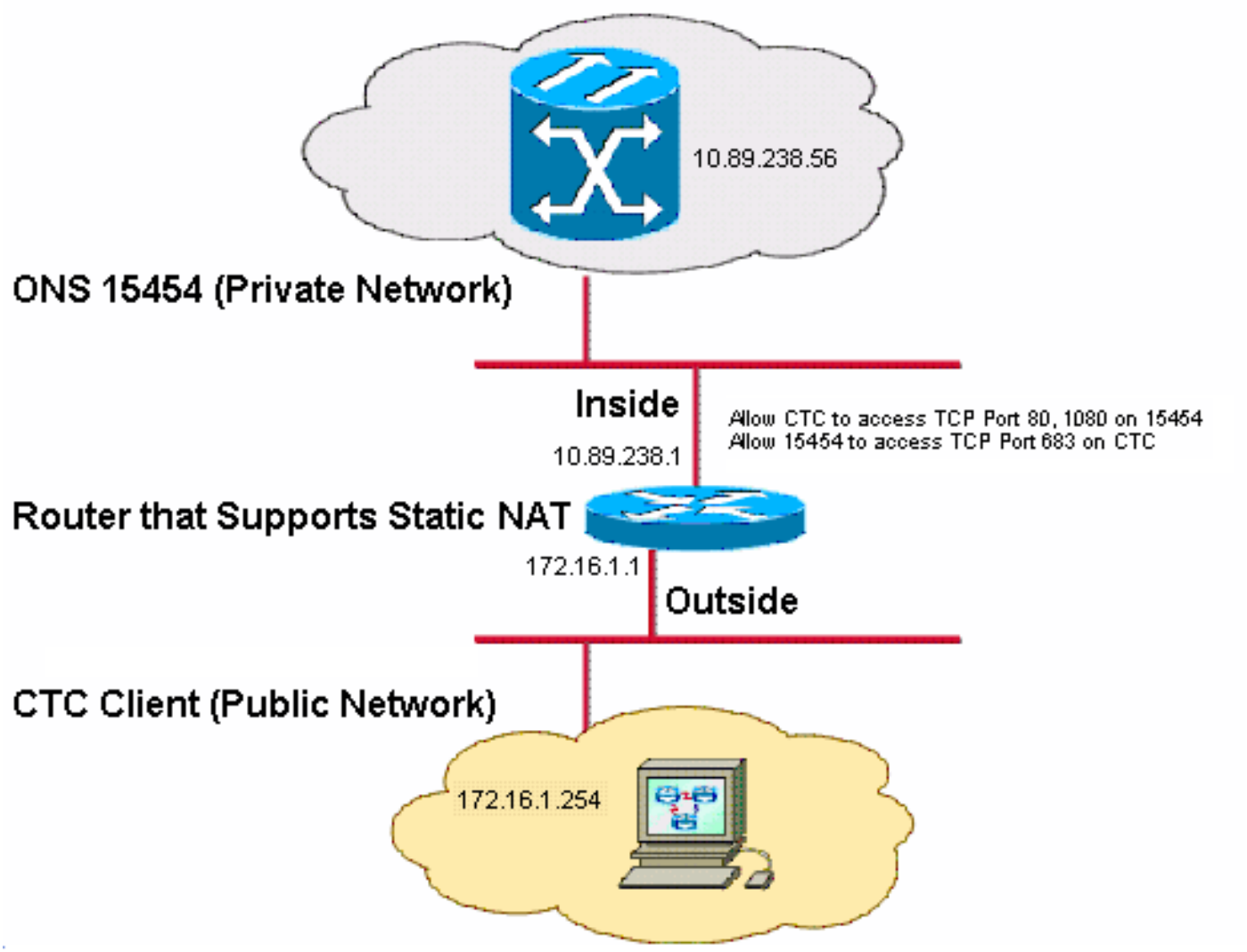
設定

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：



注意：假設172.16.0.0可在公共網路中路由。

組態

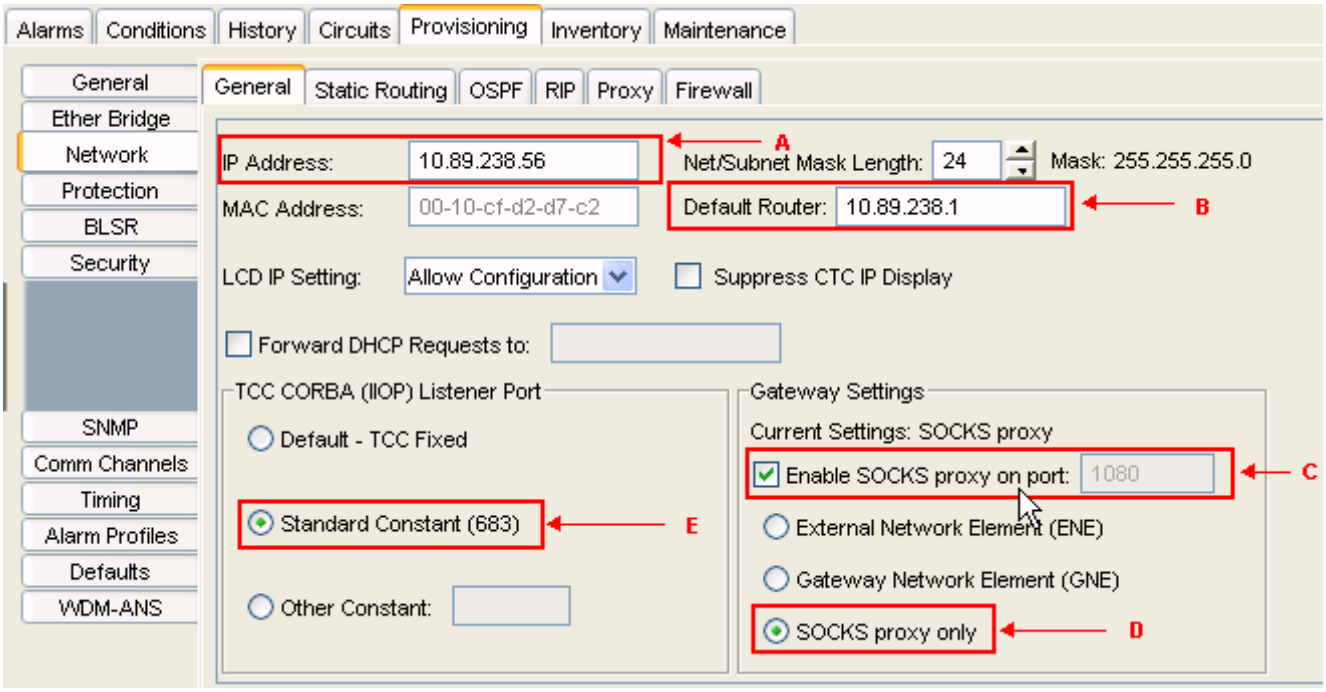
本檔案會使用以下設定：

- ONS 15454
- PC
- 路由器

Cisco ONS 15454組態

請完成以下步驟：

1. 在節點檢視中，按一下**Provisioning > General > Network**。驗證ONS 15454的IP地址在「IP Address（IP地址）」欄位中是否顯示為10.89.238.56(請參見圖2中的箭頭A)，以及「Default Router（預設路由器）」欄位是否包含值10.89.238.1(請參見圖2中的箭頭B)。**圖2 - ONS 15454配置**

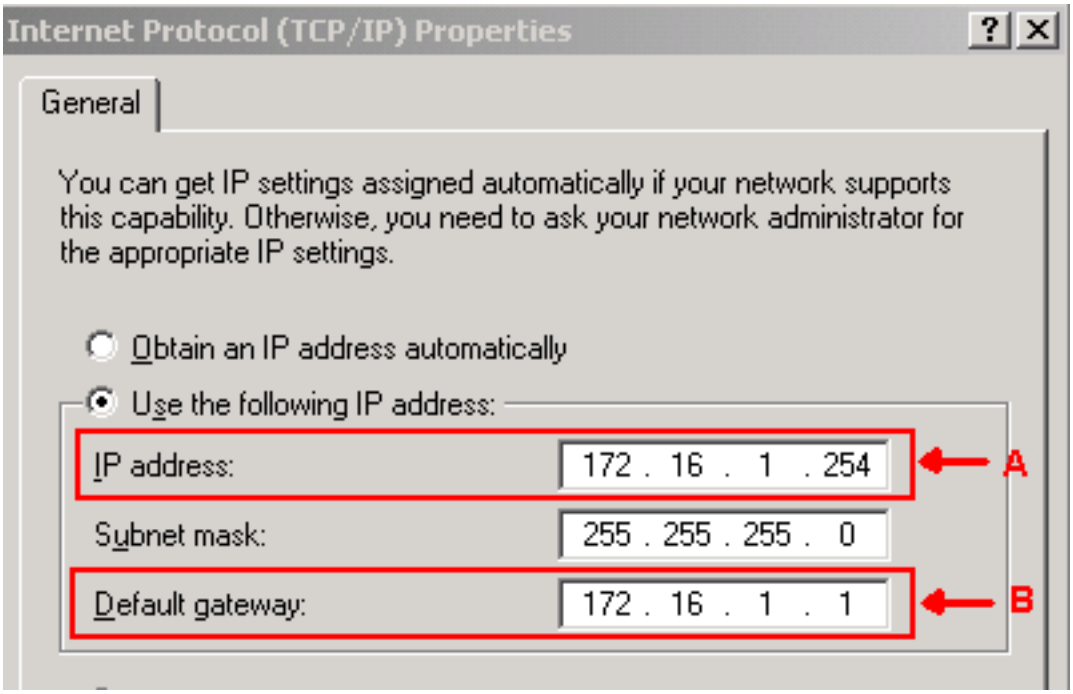


2. 選中「網關設定」部分中的**在埠上啟用SOCKS代理**覈取方塊(請參見圖2中的箭頭C)，然後選擇「**SOCKS代理**」選項(請參見圖2中的箭頭D)。
3. 在「TCC CORBA(IIOP)監聽程式埠」部分中選擇所需的監聽程式埠選項。您有以下三個選項：**Default - TCC Fixed** — 如果ONS 15454與CTC電腦位於防火牆同一側，或者沒有防火牆（預設），則選擇此選項。 此選項將ONS 15454監聽程式埠設定為埠57790。如果埠57790開啟，則可以使用預設 — TCC固定選項通過防火牆進行訪問。**標準常數** — 選擇此選項可使用埠683（CORBA預設埠號）作為ONS 15454監聽程式埠。此示例使用標準常數(683)(請參見圖2中的箭頭E)。**Other Constant** — 如果不使用埠683，請選擇此選項。鍵入防火牆管理員指定的IIOP埠。

個人電腦配置

在「Internet Protocol(TCP/IP)Properties(Internet協定(TCP/IP)屬性)」對話方塊中，驗證IP地址欄位是否表示172.16.1.254作為PC的IP地址(請參見圖3中的箭頭A)。 此外，請檢查172.16.1.1是否為預設網關(請參見圖3中的箭頭B)。

圖3 - PC配置



路由器配置

請完成以下步驟：

1. 配置Cisco ONS 15454所在的內部介面。

```
!
interface Ethernet1/0
 ip address 10.89.238.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
!
```

2. 配置訪問清單101。

```
access-list 101 permit tcp any eq www any
!
! Allow CTC to access TCP Port 80 on ONS 15454
!
access-list 101 permit tcp any eq 1080 any
!
! Allow CTC to access TCP Port 1080 on ONS 15454
!
access-list 101 permit tcp any any eq 683
!
! Allow ONS 15454 to access TCP Port 683 on the PC
!
```

3. 配置PC所在的外部介面。

```
interface Ethernet1/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
!
```

4. 配置靜態NAT。此組態會將IP位址10.89.238.56（內部本地）轉換為IP位址172.16.1.200（外部全域）。 在路由器上發出**show ip nat translation**命令以檢視轉換表(請參見圖4)。

```
!
ip nat inside source static 10.89.238.56 172.16.1.200
!
```

圖4 - IP NAT轉換

```
2600-4#show ip nat translation
Pro Inside global  Inside local   Outside local  Outside global
--- 172.16.1.200   10.89.238.56   ---            ---
```

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 access-list** — 顯示通過訪問清單的資料包計數。

驗證程式

完成以下步驟以驗證設定：

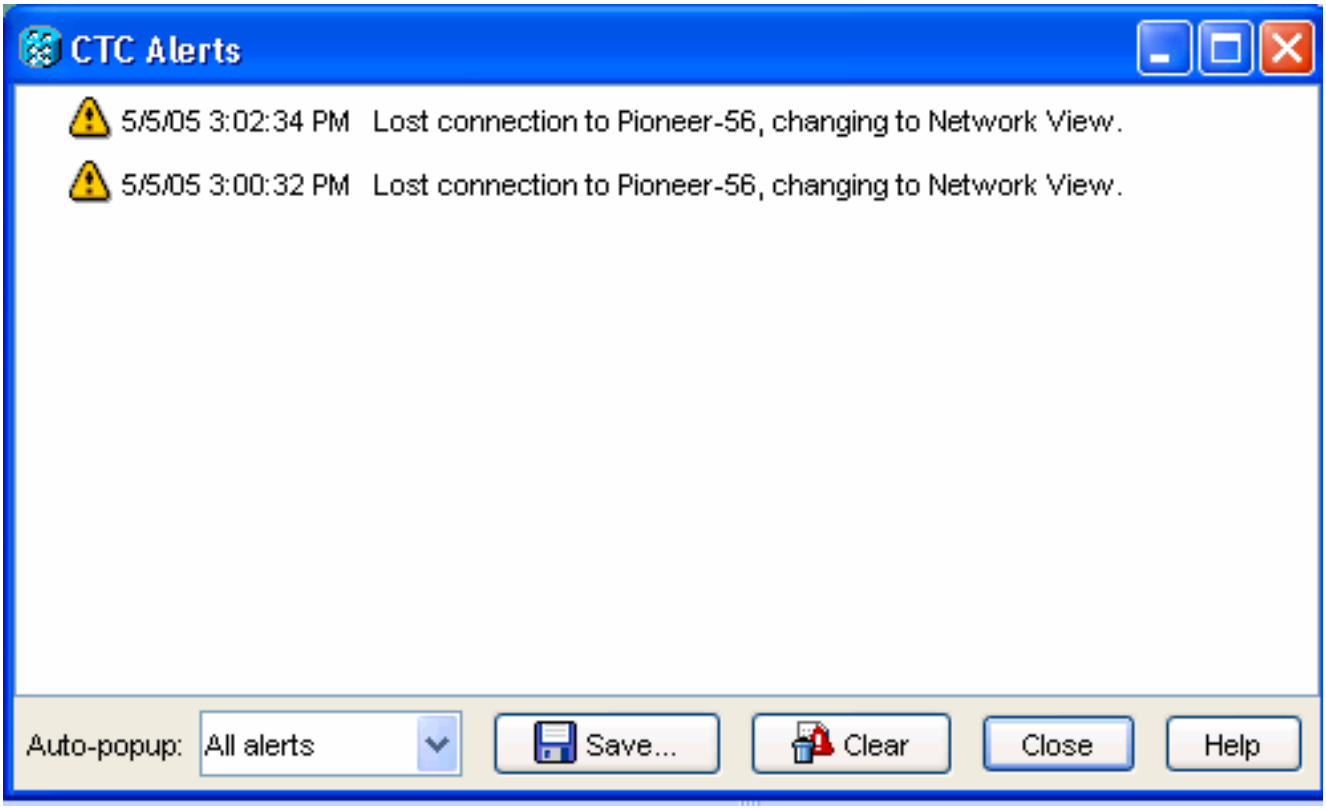
1. 運行Microsoft Internet Explorer。
2. 在瀏覽器視窗的Address欄位中鍵入**http://172.16.1.200**，然後按ENTER鍵。172.16.1.200是內部全域性地址。在公共網路中，CTC使用者只能訪問172.16.1.200，這是內部本地地址為10.89.238.56的ONS 15454的內部全域性地址。出現CTC登入視窗。
3. 鍵入要登入的使用者名稱和密碼。CTC客戶端成功連線到ONS 15454。
4. 發出**debug ip nat detailed**命令以開啟IP NAT詳細跟蹤。您可以在跟蹤檔案中檢視地址轉換。例如，從10.89.238.56到172.16.1.200(請參見圖5中的箭頭A)和從172.16.1.200到10.89.238.56(請參見圖5中的箭頭B)。**圖5 — 詳細調試IP NAT**

```
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55499]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55499]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55500]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55500]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55501]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32895]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32895]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32897]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897]
```

5. 在路由器上發出**show access-list**命令，以檢視通過訪問清單的資料包數量。**圖6 - show access-list命令**

```
2600-4#show access-list
Extended IP access list 101
    permit tcp any eq www any (56 matches)
    permit tcp any eq 1080 any (330 matches)
    permit tcp any any eq 683 (6 matches)
```

如果訪問清單阻止TCC CORBA(IIOP)偵聽器埠，則與ONS 15454的CTC會話會定期超時，並且每兩分鐘出現一次警報消息，如下所示：**圖7 - CTC警報：TCC CORBA(IIOP)埠被阻止**



作為解決方法，您可以開啟CTC IIOP偵聽程式埠。思科錯誤ID CSCeh96275(僅限註冊客戶)可解決此問題。將來，在防火牆上為TCP埠80和1080建立管道足以支援隱藏ONS 15454的實際IP地址。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems