# 使用NAT隱藏ONS 15454的實際IP地址以建立 CTC會話

### 目錄

簡介 必要條件 <u>需</u>求 <u>採用元件</u> 慣例 背景資訊 拓撲 設定 網路圖表 組態 Cisco ONS 15454組態 個人電腦配置 路由器配置 驗證 驗證程式 疑難排解 相關資訊

## <u>簡介</u>

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。

## <u>必要條件</u>

### <u>需求</u>

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。

### <u>採用元件</u>

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。

#### <u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

## <u>背景資訊</u>

本節提供基本的背景資訊。

#### <u>拓撲</u>

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。

## <u>設定</u>

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<u>命令查詢工具(僅限註</u>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

<u>Cisco ONS 15454組態</u>

請完成以下步驟:

 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<u>圖2中的箭頭A</u>),以及「Default Router(預設路由器)」欄位是否包含值10.89.238.1(請參見<u>圖2中的箭頭B</u>)。圖2 - ONS 15454配置

Alarms Conditions	History Circuits	Provisioning Inventory	Maintenance			
General	General Static Routing OSPF RIP Proxy Firewall					
Ether Bridge			<b>1</b> 4 0			
Network	IP Address:	10.89.238.56	Net/Subnet Mask Length: 24 🚔 Mask: 255.255.255.0			
Protection	MAC Address:	00-10-cf-d2-d7-c2	Default Router: 10.89.238.1			
BLSR	MAC AGGICSS.					
Security	LCD IP Setting:	Allow Configuration 🔽	Summers CTC IP Disnlay			
SNMP Comm Channels	Forward DHCP Requests to:     Gateway Settings     Current Settings: SOCKS proxy					
Timing Alarm Profiles Defaults WDM-ANS	⊙ Standard Cor ○ Other Consta	nstant (683)	E External Network Element (ENE)     Gateway Network Element (GNE)     SOCKS proxy only			

- 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<u>圖2中的箭頭C</u>),然後選擇「SOCKS代理」選項(請參見<u>圖2中的箭頭D</u>)。
- 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<u>圖</u> <u>2中的箭頭E</u>)。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<u>圖3中的箭頭</u>A)。 此外,請檢查172.16.1.1是否為 預設網關(請參見<u>圖3中的箭頭</u>B)。

#### 圖3 - PC配置

Internet Protocol (TCP/IP) Properti	es ?X				
General					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
Use the following IP address:					
IP address:	172 . 16 . 1 . 254 🗕 📥 A				
S <u>u</u> bnet mask:	255 . 255 . 255 . 0				
Default gateway:	172.16.1.1 🖊 📥 🖪				

### 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。
  1
  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
  1
  ! Allow CTC to access TCP Port 80 on ONS 15454
  !
  access-list 101 permit tcp any eq 1080 any
  1
  ! Allow CTC to access TCP Port 1080 on ONS 15454
  1
  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。

1

!

```
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<u>圖4</u>)。

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 --- 172.16.1.200 10.89.238.56

Outside local Outside global

### 驗證

本節提供的資訊可用於確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>註冊</u>客戶使用)支援某些show命令,此工具可讓您檢視<u>show</u>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。
- 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\*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55500] NAT\*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501] NAT\*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501] NAT\*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501] NAT\*: s=10.89.238.56->172.16.1.200, d=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\*: 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]

permit tcp any eq www any (56 matches)

permit tcp any eq 1080 any (330 matches)

permit tcp any any eq 683 (6 matches) <sub>如果訪</sub>

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** 

😫 CTC Alerts		
<u> 5</u> /5/05 3:02:34 PM	Lost connection to Pioneer-56, changing to Network View.	
📤 5/5/05 3:00:32 PM	Lost connection to Pioneer-56, changing to Network View.	
Auto-popup: All alerts	Close	Help

作為解決方法,您可以開啟CTC IIOP偵聽程式埠。思科錯誤ID <u>CSCeh96275</u>(僅限<u>註冊</u>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。

## <u>疑難排解</u>

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