瞭解NAT以在IOS和IOS XE路由器上啟用對等通訊

目錄

簡介

本檔案介紹NAT(STUN)伺服器對作業階段穿越公用程式的需求、有關STUN伺服器的網路位址轉譯(NAT)設定的類型、NAT如何導致此設定中的問題以及解決方案。

背景資訊

NAT裝置的主要用途是允許區域網(LAN)中具有私有IP地址的裝置與公共地址空間（例如Internet）中的裝置通訊。但是，雖然NAT裝置應該允許內部主機與公共空間連線，但是當涉及到點對點(P2P)應用程式(例如VoIP、遊戲、WebRTC和檔案共用，終端使用者需要同時充當客戶端和伺服器來維持雙向端到端通訊時，NAT為建立這些UDP連線提供了困難。通常需要NAT遍歷技術才能使這些應用程式正常運行。

需要NAT穿越

Internet上的即時語音和影片通訊 是 主流 現在，支援網路電話(VoIP)呼叫的即時消息收發器(IM)非常流行。VoIP最初採用的一個巨大障礙是，大多數PC或其他裝置都位於防火牆後面，並使用私有IP地址。網路中的多個私有地址（IP地址和埠）由防火牆對映到單個公有地址，該防火牆具有 NAT. 但終端裝置不知道其公有地址，因此無法在其VoIP通訊中通告的私有地址上接收來自遠端方的語音流量。

單方面 自地址固定(UNSAF)過程是一些始發端點嘗試確定或修復另一個端點已知的地址（和埠）的過程，例如，要能夠 u使用協定交換中的地址資料或通告其接收連線的公有地址。

因此，正在討論的P2P連線是UNSAF進程。 一種常見的P2P應用建立對等會話並保留的方法 NAT友好型是指使用可公開定址的集結伺服器 註冊和對等體發現。

適用於NAT的作業階段遍歷公用程式

根據RFC 5389,STUN提供了處理NAT的工具。它為端點提供了一種方法，可確定由NAT裝置分配的IP地址和埠，該IP地址和埠與其私有IP地址和埠相對應。它還為端點提供保持NAT繫結活動狀態的

方法。

NAT實施型別

已經觀察到，UDP的NAT處理方法因實施而異。實施中觀察到的四種處理方法是：

全錐：全錐NAT是指將來自相同內部IP地址和埠的所有請求對映到相同外部IP地址和埠的NAT。此外，任何外部主機都可以向內部主機傳送資料包，並將資料包傳送到對映的外部地址。

受限錐：受限錐NAT是指將來自相同內部IP地址和埠的所有請求對映到相同外部IP地址和埠的NAT。與全錐NAT不同，外部主機（IP地址為X）只有在內部主機之前向IP地址為X傳送資料包時，才能向內部主機傳送資料包。

埠限制錐：埠限制錐NAT類似於限制錐NAT，但限制包括埠號。具體來說，只有當內部主機之前向IP地址X和埠P傳送了資料包時，外部主機才能將包含源IP地址X和源埠P的資料包傳送到內部主機。

對稱：在對稱NAT中，來自同一內部IP地址和埠到特定目標IP地址和埠的所有請求對映到同一外部IP地址和埠。 如果同一主機傳送的資料包具有相同的源地址和埠，但目的地不同，則使用不同的對映。 此外，只有接收資料包的外部主機才能將UDP資料包傳送回內部主機。

考慮源(A、Pa)（其中A是IP地址，Pa是源埠）通過NAT裝置與目標(B、Pb)和(C、PC)通訊的拓撲。

NAT實施型別	公用 源時間 目的地為(B、Pb)	公共源，目標為(C、Pc)	可以目標(例如： (B、Pb)將流量傳送到(A， Pa)?
全圓錐面	(X1,Px1)	(X1,Px1)	是
受限圓錐體	(X)1，畫素1)	(X)1，畫素1)	僅當(A， Pa)首先將流量傳送到B
埠限制圓錐體	(X)1，畫素1)	(X)1，畫素1)	僅當(A， Pa)首先將流量傳送到(B， Pb)時
對稱	(X)1，畫素1)	(X2,Px2)	僅當(A， Pa)首先將流量傳送到(B， Pb)時

NAT穿越和對稱NAT問題

STUN伺服器響應STUN客戶端傳送的STUN繫結請求，並提供客戶端的公共IP/埠。現在，此地址/埠 組合由STUN客戶端在其對等通訊中使用 訊號. 但是，現在， 終端主機 使用相同的私有地址/埠(假定為 繫結 到公共IP/埠 在STUN響應中提供)NAT裝置將其轉換為同一個IP，但如果是對稱NAT，則轉換為不同的埠 示例我ntation 已使用。這將中斷UDP通訊，因為 訊號 已根據p上一個埠。

Cisco IOS® routers' NAT 示例我ntation 當它執行PAT時，預設情況下是對稱的。 其他efore中，您會看到這些UDP連線問題 執行ping操作的路由器 NAT。

但是，Cisco IOS-XE路由器執行PAT時的NAT實施不對稱。當您傳送兩個不同的 如果流具有相同的源IP和埠，但流向不同的目標，則源會被NATED到相同的內部全域性IP和埠。

問題的解決方案

根據此描述， 很顯然， 如果執行 獨立於端點 對映。

根據RCFC 4787: 使用 端點獨立對映(EIM),NAT對從同一內部IP地址和埠(X:x)，傳送到任何外部IP地址和埠。

從客戶端上，當終端主機在兩個不同的終端視窗上運行命令**nc -p 23456 10.0.0.4 4000**和**nc -p 23456 10.0.0.5 5000**時，如果使用EIM，以下是NAT轉換的結果：

```
Pro Inside global       Inside local            Outside local        Outside global

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.4:40000 10.0.0.4:40000

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.5:50000 10.0.0.5:50000
```

在這裡，您可以看到，無論目的地連線埠/位址如何，具有相同來源位址和連線埠的不同流量都會轉換為相同位址/連線埠。

在Cisco IOS路由器上，可以使用命令啟用端點不相關的埠分配 **ip nat service enable-sym-port。**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html

摘要

當您使用埠地址轉換(PAT)時，Cisco IOS NAT實施預設情況下是對稱的，當它通過P2P UDP流量時，可能會引起問題，該流量需要伺服器（如STUN）進行NAT穿越。您需要在NAT裝置上顯式配置EIM才能使此工作正常進行。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。