NAT zur Ermöglichung der Peer-to-Peer-Kommunikation auf IOS- und IOS XE-Routern

Inhalt

[Einleitung](#)
[Hintergrundinformationen](#)
[NAT-Traversal erforderlich](#)
[Session Traversal-Dienstprogramme für NAT](#)
[Arten von NAT-Implementierungen](#)
[Probleme mit NAT Traversal und Symmetric NAT](#)
[Die Lösung des Problems](#)
[Zusammenfassung](#)

Einleitung

Dieses Dokument beschreibt die Notwendigkeit von Session Traversal Utilities für NAT-Server (STUN), die Arten von Network Address Translation (NAT)-Konfigurationen in Bezug auf STUN-Server, wie NAT ein Problem in dieser Konfiguration verursacht und die Lösung.

Hintergrundinformationen

NAT-Geräte dienen in erster Linie dazu, Geräten mit privaten IP-Adressen in einem LAN die Kommunikation mit Geräten in öffentlichen Adressräumen, z. B. dem Internet, zu ermöglichen. Obwohl NAT-Geräte internen Hosts ermöglichen sollen, sich mit dem öffentlichen Raum zu verbinden, bietet NAT bei Point-to-Point (P2P)-Anwendungen wie VoIP, Gaming, WebRTC und Filesharing, bei denen die Endbenutzer sowohl als Client als auch als Server agieren müssen, um eine bidirektionale End-to-End-Kommunikation aufrechtzuerhalten, Schwierigkeiten beim Aufbau dieser UDP-Verbindungen. Damit diese Anwendungen funktionieren, sind in der Regel NAT-Überbrückungstechniken erforderlich.

NAT-Traversal erforderlich

Sprach- und Videokommunikation in Echtzeit über das Internet sind Mainstream derzeit mit mehreren beliebten Instant Messaging-Systemen (IMs), die VoIP-Anrufe unterstützen. Eine große Hürde bei der anfänglichen Einführung von VoIP war die Tatsache, dass die meisten PCs oder andere Geräte hinter Firewalls sitzen und private IP-Adressen verwenden. Mehrere private Adressen (IP-Adresse und Port) im Netzwerk werden einer einzigen öffentlichen Adresse durch eine Firewall mit NAT. Das Endgerät kennt jedoch seine öffentliche Adresse nicht und kann daher keinen Sprachdatenverkehr von der Gegenstelle über die private Adresse empfangen, die es in seiner VoIP-Kommunikation ankündigt.

einseitig Self-Address Fixing (UNSAF)-Prozesse sind Prozesse, bei denen ein Ursprungsendpunkt versucht, die Adresse (und den Port) zu bestimmen oder zu reparieren, über die er einem anderen Endpunkt bekannt ist, z. B. um uAdressdaten im Protokollaustausch verwenden oder eine öffentliche Adresse ankündigen, von der sie Verbindungen empfängt.

Bei den hier diskutierten P2P-Verbindungen handelt es sich somit um UNSAF-Prozesse. Eine gängige Methode für P2P-Anwendungen, Peering-Sitzungen einzurichten und zu behalten NAT-freundlich, wenn ein öffentlich adressierbarer Rendezvous-Server für Registrierung und Peer Discovery.

Session Traversal-Dienstprogramme für NAT

Gemäß RFC 5389 stellt STUN ein Tool bereit, das NATs verarbeitet. Es bietet einem Endpunkt die Möglichkeit, die von einem NAT-Gerät zugewiesene IP-Adresse und den zugewiesenen Port zu bestimmen, die mit der privaten IP-Adresse und dem Port übereinstimmen. Sie bietet einem Endpunkt auch die Möglichkeit, eine NAT-Bindung am Leben zu erhalten.

Arten von NAT-Implementierungen

Es wurde beobachtet, dass die NAT-Behandlung von UDP bei den einzelnen Implementierungen unterschiedlich ist. Bei den Implementierungen wurden die folgenden vier Behandlungen beobachtet:

Full Cone: Ein Full-Kegel-NAT ist ein NAT, bei dem alle Anfragen von derselben internen IP-Adresse und demselben Port derselben externen IP-Adresse und demselben externen Port zugeordnet werden. Darüber hinaus kann jeder externe Host ein Paket an den internen Host senden, und dieser sendet ein Paket an die zugeordnete externe Adresse.

Restricted Cone (Eingeschränkter Kegel): Eine NAT mit eingeschränktem Kegel ist eine Anforderung, bei der alle Anforderungen von derselben internen IP-Adresse und demselben Port derselben externen IP-Adresse und demselben externen Port zugeordnet werden. Im Gegensatz zu einer Full-Kegel-NAT kann ein externer Host (mit der IP-Adresse X) ein Paket nur dann an den internen Host senden, wenn der interne Host zuvor ein Paket an die IP-Adresse X gesendet hatte.

Port Restricted Cone: Ein Port Restricted Kegel NAT ist wie ein Restricted Kegel NAT, aber die Einschränkung umfasst Portnummern. Insbesondere kann ein externer Host ein Paket mit der Quell-IP-Adresse X und dem Quell-Port P nur dann an den internen Host senden, wenn der interne Host zuvor ein Paket an die IP-Adresse X und den Port P gesendet hat.

Symmetrisch: Eine symmetrische NAT besteht darin, dass alle Anforderungen von derselben internen IP-Adresse und demselben Port an eine bestimmte Ziel-IP-Adresse und einen bestimmten Port derselben externen IP-Adresse und demselben externen Port zugeordnet sind. Wenn derselbe Host ein Paket mit derselben Quelladresse und demselben Port, jedoch an ein anderes Ziel sendet, wird eine andere Zuordnung verwendet. Außerdem kann nur der externe Host, der ein Paket empfängt, ein UDP-Paket zurück an den internen Host senden.

Betrachten wir eine Topologie, in der die Quelle (A, Pa) (wobei A die IP-Adresse und Pa der Quell-Port ist) über ein NAT-Gerät mit dem Ziel (B, Pb) und (C, PC) kommuniziert.

Typ der NAT-Implementierung	Öffentlich Quelle wann bestimmt für (B, Pb)	Öffentliche Quelle für (C, PC)	Can-Ziel (z. B. (B, Pb) Datenverkehr an (A, Pa) senden?
Voller Ton	(X1,PX1)	(X1,PX1)	Ja
Restricted Cone	(X1.Px1)	(X1.Px1)	Nur wenn (A, Pa) den Datenverkehr zuerst an B gesendet hat

Port Restricted Cone	(X1.Px1)	(X1.Px1)	Nur wenn (A, Pa) den Datenverkehr zuerst an (B, Pb) gesendet hat
Symmetrisch	(X1.Px1)	(X2, Px2)	Nur wenn (A, Pa) den Datenverkehr zuerst an (B, Pb) gesendet hat

Probleme mit NAT Traversal und Symmetric NAT

STUN-Server reagieren auf STUN-Bindungsanfragen, die von STUN-Clients gesendet werden, und stellen die öffentliche IP/Port des Clients bereit. Diese Adresse/dieser Port wird vom STUN-Client in seiner Peer-to-Peer-Kommunikation verwendet. Signalisierung. Allerdings, nun da die Endhost verwendet dieselbe private Adresse/denselben privaten Port (setzen wir voraus, dass gebunden zu öffentlichen IP/Port bereitgestellt in der STUN-Antwort), wird sie vom NAT-Gerät in dieselbe IP, bei symmetrischer NAT jedoch in einen anderen Port übersetzt. eintönigichNation wird verwendet. Dies unterbricht die UDP-Kommunikation, da der Signalisierung hatte die Verbindung auf der Grundlage vonfrüherer Hafen.

Cisco IOS® Router" NAT eintönigichNation wenn PAT durchgeführt wird, ist standardmäßig symmetrisch. DerenoVorderseitewird erwartet, dass Sie UDP-Verbindungsprobleme mit diesen Router, die NAT:

Die NAT-Implementierung der Cisco IOS-XE-Router bei der PAT-Ausführung ist jedoch nicht symmetrisch. Wenn Sie zwei verschiedene Streams mit derselben Quell-IP und demselben Port, aber zu verschiedenen Zielen, wird die Quelle innerhalb der globalen IP-Adresse und des Ports mit derselben NATED versehen.

Die Lösung des Problems

Aus dieser Beschreibung geht hervor, es ist klar, dass die Problem kann behoben werden, wenn Sie Endgeräteunabhängig Zuordnung.

Gemäß RCFC 4787: Mit Endpoint-Independent Mapping (EIM): Die NAT verwendet die Portzuordnung für nachfolgende Pakete, die von derselben internen IP-Adresse und demselben Port gesendet werden (X:x) an eine beliebige externe IP-Adresse und einen beliebigen Port.

Wenn der Endhost auf einem Client die Befehle **nc -p 23456 10.0.0.4 4000** und **nc -p 23456 10.0.0.5 50000** ausführt, werden die Ergebnisse der NAT-Übersetzungen bei Verwendung von EIM:

```
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
```

Hier können Sie sehen, dass verschiedene Datenverkehrsflüsse, die dieselbe Quelladresse und denselben Port haben, in dieselbe Adresse/denselben Port umgewandelt werden, unabhängig vom Zielport bzw. von der Zieladresse.

Auf Cisco IOS-Routern können Sie die endpunktunabhängige Portzuweisung mithilfe des folgenden Befehls aktivieren: **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

Zusammenfassung

Die Cisco IOS NAT-Implementierung ist standardmäßig symmetrisch, wenn Sie Port Address Translation (PAT) verwenden. Sie kann Probleme verursachen, wenn P2P-UDP-Datenverkehr weitergeleitet wird, für den Server wie STUN für NAT-Traversal erforderlich sind. Damit dies funktioniert, müssen Sie EIM auf dem NAT-Gerät explizit konfigurieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.