Comprendre la NAT pour activer la communication peer-to-peer sur les routeurs IOS et IOS XE

Table des matières

Introduction

Ce document décrit le besoin d'utilitaires de traversée de session pour les serveurs NAT (STUN), les types de configurations de traduction d'adresses de réseau (NAT) par rapport aux serveurs STUN, comment la NAT cause un problème dans cette configuration et la solution.

Informations générales

L'objectif principal des périphériques NAT est de permettre aux périphériques dotés d'adresses IP privées dans un réseau local (LAN) de communiquer avec des périphériques dans des espaces d'adressage publics, tels qu'Internet. Cependant, bien que les périphériques NAT soient censés permettre aux hôtes internes de se connecter à l'espace public, lorsqu'il s'agit d'applications point à point (P2P) telles que la VoIP, les jeux, WebRTC et le partage de fichiers, où les utilisateurs finaux doivent agir à la fois comme client et comme serveur pour maintenir une communication bidirectionnelle de bout en bout, la NAT rend difficile l'établissement de ces connexions UDP. Les techniques de traversée NAT sont généralement requises pour que ces applications fonctionnent.

Nécessité de la traversée NAT

Communication vocale et vidéo en temps réel sur Internet sont courant dominant aujourd'hui avec plusieurs messageries instantanées (IM) populaires qui prennent en charge les appels VoIP. L'un des principaux obstacles à l'adoption initiale de la VoIP était le fait que la plupart des ordinateurs ou autres périphériques se trouvent derrière des pare-feu et utilisent des adresses IP privées. Plusieurs adresses privées (adresse IP et port) du réseau sont mappées à une adresse publique unique par un pare-feu avec NAT . Mais le périphérique final ne connaît pas son adresse publique et ne peut donc pas recevoir de trafic vocal de la partie distante sur l'adresse privée qu'il annonce dans sa communication VoIP.

Unilatéral Les processus UNSAF (Self Address Fixing) sont des processus par lesquels certains points d'extrémité d'origine tentent de déterminer ou de fixer l'adresse (et le port) par lesquels ils

sont connus d'un autre point d'extrémité, par exemple pour pouvoir uUtilisez les données d’adresse dans l’échange de protocoles ou pour annoncer une adresse publique à partir de laquelle il reçoit des connexions.

Les connexions P2P en cours de discussion sont donc des processus UNSAF. Une façon courante pour les applications P2P d'établir des sessions d'appairage et de rester NAT est compatible lorsqu'ils utilisent un serveur de rendez-vous adressable publiquement pour à des fins d'enregistrement et de découverte.

Utilitaires de traversée de session pour NAT

Conformément à la RFC 5389, STUN fournit un outil qui traite des NAT. Il permet à un point d'extrémité de déterminer l'adresse IP et le port attribués par un périphérique NAT qui correspondent à son adresse IP privée et à son port. Elle permet également à un point de terminaison de maintenir une liaison NAT active.

Types d'implémentations NAT

Il a été observé que le traitement NAT du protocole UDP varie selon les mises en oeuvre. Les quatre traitements observés dans les mises en oeuvre sont :

Full Cone : une NAT full cone est une NAT dans laquelle toutes les requêtes provenant de la même adresse IP interne et du même port sont mappées à la même adresse IP externe et au même port. En outre, tout hôte externe peut envoyer un paquet à l'hôte interne et il envoie un paquet à l'adresse externe mappée.

Restricted Cone : une fonction NAT de cône restreint est une fonction dans laquelle toutes les requêtes provenant de la même adresse IP interne et du même port sont mappées à la même adresse IP externe et au même port. Contrairement à une fonction NAT à cône plein, un hôte externe (avec l’adresse IP X) ne peut envoyer un paquet à l’hôte interne que si l’hôte interne a déjà envoyé un paquet à l’adresse IP X.

Port Restricted Cone : une NAT de cône à port restreint est similaire à une NAT de cône restreint, mais la restriction inclut des numéros de port. Plus précisément, un hôte externe peut envoyer un paquet, avec l'adresse IP source X et le port source P, à l'hôte interne uniquement si l'hôte interne a déjà envoyé un paquet à l'adresse IP X et au port P.

Symétrique : une NAT symétrique est une NAT dans laquelle toutes les requêtes provenant de la même adresse IP interne et du même port vers une adresse IP de destination et un port spécifiques, sont mappées vers la même adresse IP externe et le même port. Si le même hôte envoie un paquet avec la même adresse source et le même port, mais vers une destination différente, un mappage différent est utilisé. En outre, seul l’hôte externe qui reçoit un paquet peut renvoyer un paquet UDP à l’hôte interne.

Considérez une topologie dans laquelle la source (A, Pa) (où A est l'adresse IP et Pa est le port source) communique avec la destination (B, Pb) et (C, PC) via un périphérique NAT.

Type de mise en oeuvre NAT	Public source quand destiné à (B, Pb)	Source publique à destination de (C, Pc)	Destination possible (par exemple : (B, Pb)) envoyer du trafic vers (A, Pa) ?
Cône Plein	(X1, Px1)	(X1, Px1)	Oui
Cône Restreint	(X1,Px1)	(X1,Px1)	Uniquement si (A, Pa) avait

			envoyé le trafic à B
Cône à accès limité	(X1,Px1)	(X1,Px1)	Uniquement si (A, Pa) a envoyé le trafic à (B, Pb) pour la première fois
Symétrique	(X1,Px1)	(X2, Px2)	Uniquement si (A, Pa) a envoyé le trafic à (B, Pb) pour la première fois

Problèmes avec NAT Traversal et NAT symétrique

Les serveurs STUN répondent aux requêtes de liaison STUN envoyées par les clients STUN et fournissent l'adresse IP/le port public du client. Cette adresse/ce port est utilisée par le client STUN dans sa communication peer-to-peer signalisation. Cependant, maintenant que la hôte final utilise la même adresse/le même port privé (supposons qu'il est liaison à l'adresse IP/au port public fourni dans la réponse STUN) le périphérique NAT le traduit vers la même adresse IP mais un port différent si la NAT est symétrique simpletmoinote est utilisé. Cela interrompt la communication UDP car la signalisation avait établi la connexion sur la base de la pport précédent.

Cisco IOS® routeurs' NAT simpletmoinote lorsqu'il exécute PAT est symétrique par défaut. Làeà l'avant, vous devez voir des problèmes de connexion UDP avec ces routeurs qui exécutent NAT .

Cependant, l'implémentation NAT des routeurs Cisco IOS-XE lorsqu'il exécute la PAT n'est pas symétrique. Lorsque vous envoyez deux avec la même adresse IP source et le même port, mais vers des destinations différentes, la source obtient NATED vers la même adresse IP globale interne et le même port.

La solution au problème

À partir de cette description, il est clair que la peut être résolu si vous effectuez Indépendant des terminaux mappage.

Selon le RCFC 4787: Avec Endpoint-Independent Mapping (EIM), la NAT réutilise le mappage de port pour les paquets suivants envoyés depuis la même adresse IP interne et le même port (X:x) à toute adresse IP et à tout port externes.

Àpartir d'un client, lorsque l'hôte d'extrémité exécute les commandes **nc -p 23456 10.0.0.4 4000** et **nc -p 23456 10.0.0.5 5000**, sur deux fenêtres de terminal différentes, voici les résultats des traductions NAT si vous utilisez 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
```

Ici, vous pouvez voir que différents flux de trafic qui ont la même adresse source et le même port sont traduits vers la même adresse/port, quel que soit le port/l'adresse de destination.

Sur les routeurs Cisco IOS, vous pouvez activer l'allocation de ports agnostiques de terminal à l'aide de la commande **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

Résumé

L'implémentation NAT de Cisco IOS est symétrique par défaut lorsque vous utilisez la traduction d'adresses de port (PAT) et peut provoquer des problèmes lorsqu'elle transmet du trafic UDP P2P qui nécessite des serveurs tels que STUN pour la traversée NAT. Vous devez configurer explicitement EIM sur le périphérique NAT pour que cela fonctionne.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.