Comprendere il NAT per abilitare la comunicazione peer-to-peer sui router IOS e IOS XE

Sommario

Introduzione

Questo documento descrive la necessità di Session Traversal Utilities per i server NAT (STUN), i tipi di configurazione di Network Address Translation (NAT) rispetto ai server STUN, il modo in cui NAT causa un problema in questa configurazione e nella soluzione.

Premesse

Lo scopo principale dei dispositivi NAT è quello di consentire ai dispositivi con indirizzi IP privati in una rete locale (LAN) di comunicare con i dispositivi negli spazi degli indirizzi pubblici, come Internet. Tuttavia, sebbene i dispositivi NAT debbano consentire agli host interni di connettersi allo spazio pubblico, quando si tratta di applicazioni Point-to-Point (P2P) come VoIP, videogame, WebRTC e condivisione di file in cui gli utenti finali devono agire sia come client che come server per mantenere la comunicazione bidirezionale, NAT fornisce difficoltà a stabilire tali connessioni UDP. Le tecniche di attraversamento NAT sono in genere necessarie per il funzionamento di queste applicazioni.

Necessità di NAT Traversal

Comunicazioni voce e video in tempo reale su Internet sono mainstream con i più diffusi instant messenger (IM) che supportano le chiamate VoIP. Un grande ostacolo nell'adozione iniziale del VoIP è stato il fatto che la maggior parte dei PC o altri dispositivi si trovano dietro i firewall e utilizzano indirizzi IP privati. Più indirizzi privati (indirizzo IP e porta) nella rete sono mappati a un singolo indirizzo pubblico da un firewall con NAT. Il dispositivo terminale, tuttavia, non è in grado di rilevare l'indirizzo pubblico e, di conseguenza, non può ricevere traffico vocale dalla parte remota sull'indirizzo privato pubblicizzato nella comunicazione VoIP.

Unilaterale I processi UNSAF (Self-Address Fixing) sono processi in cui alcuni endpoint di origine tentano di determinare o correggere l'indirizzo (e la porta) con cui sono noti a un altro endpoint, ad esempio per essere in grado di uUtilizzare i dati relativi all'indirizzo nello scambio di protocolli o

per annunciare un indirizzo pubblico da cui riceve le connessioni.

Le connessioni P2P in discussione sono quindi processi UNSAF. Un modo comune per le applicazioni P2P di stabilire sessioni di peering e rimanere NAT-friendly è quando utilizzano un server rendezvous indirizzabile pubblicamente per a scopo di registrazione e peer discovery.

Utilità di attraversamento sessione per NAT

Come indicato nella RFC 5389, STUN fornisce uno strumento che si occupa dei NAT. Fornisce un mezzo per un endpoint per determinare l'indirizzo IP e la porta allocati da un dispositivo NAT che corrisponde al suo indirizzo IP privato e alla sua porta. Consente inoltre a un endpoint di mantenere attivo un binding NAT.

Tipi di implementazioni NAT

È stato osservato che il trattamento NAT di UDP varia tra le implementazioni. I quattro trattamenti osservati nelle implementazioni sono:

Coni completi: un NAT conico completo è un nodo in cui tutte le richieste provenienti dallo stesso indirizzo IP interno e dalla stessa porta sono mappate allo stesso indirizzo IP esterno e alla stessa porta. Inoltre, ogni host esterno può inviare un pacchetto all'host interno e inviare un pacchetto all'indirizzo esterno mappato.

Coni limitati: un NAT con coni limitati è un nodo in cui tutte le richieste provenienti dallo stesso indirizzo IP interno e dalla stessa porta sono mappate allo stesso indirizzo IP esterno e alla stessa porta. A differenza di un NAT a cono intero, un host esterno (con indirizzo IP X) può inviare un pacchetto all'host interno solo se l'host interno ha già inviato un pacchetto all'indirizzo IP X.

Coni con restrizioni di porta: un NAT con coni con restrizioni di porta è simile a un NAT con coni con restrizioni, ma la restrizione include i numeri di porta. In particolare, un host esterno può inviare un pacchetto, con indirizzo IP di origine X e porta di origine P, all'host interno solo se l'host interno aveva precedentemente inviato un pacchetto all'indirizzo IP X e alla porta P.

Simmetrico: per NAT simmetrico si intende una NAT in cui tutte le richieste provenienti dallo stesso indirizzo IP interno e dalla stessa porta verso una destinazione IP e un indirizzo IP specifici vengono mappate alla stessa porta e allo stesso indirizzo IP esterno. Se lo stesso host invia un pacchetto con lo stesso indirizzo di origine e la stessa porta, ma a una destinazione diversa, viene utilizzato un mapping diverso. Inoltre, solo l'host esterno che riceve un pacchetto può inviare un pacchetto UDP all'host interno.

Si consideri una topologia in cui l'origine (A, Pa) (dove A è l'indirizzo IP e Pa è la porta di origine) comunica con la destinazione (B, Pb) e (C, PC) tramite un dispositivo NAT.

Tipo di implementazione NAT	Public origine quando destinato a (B, Pb)	Origine pubblica se destinata a (C, Pc)	Destinazione Can (ad esempio: (B, Pb)) inviare traffic a (A, Pa)?
Coni completi	(X1,Px1)	(X1,Px1)	Sì
Cono con restrizioni	(X1.Px1)	(X1.Px1)	Solo se (A, Pa) ha inviato il traffico a B
Cono con restrizioni della porta	(X1.Px1)	(X1.Px1)	Solo se (A, Pa) ha inviato il traffico a (B, Pb)
Simmetrico	(X1.Px1)	(X2,Px2)	Solo se (A, Pa) ha inviato il

traffico a (B, Pb)

Problemi di NAT Traversal e NAT simmetrico

I server STUN rispondono alle richieste di binding STUN inviate dai client STUN e forniscono l'IP/porta pubblica del client. Ora, questo indirizzo/porta viene utilizzata dal client STUN nelle comunicazioni peer-to-peer segnalazione. Tuttavia, ora che il host finale utilizza lo stesso indirizzo/porta privato (supponiamo che sia rilegato alla porta/indirizzo IP pubblico fornito nella risposta STUN) il dispositivo NAT lo converte nello stesso indirizzo IP ma su una porta diversa se il protocollo NAT è simmetrico semplicemeannotazione viene utilizzato. In questo modo si interrompe la comunicazione UDP perché segnalazione ha stabilito il collegamento sulla base delporta precedente.

Cisco IOS® router NAT semplicemeannotazione quando esegue PAT, per default l'opzione è simmetrica. Ci sonosprima, sono previsti problemi di connessione UDP con questi router che eseguono NAT.

Tuttavia, l'implementazione NAT dei router Cisco IOS-XE quando esegue il PAT non è simmetrica. Quando invii due messaggi diversi flussi con lo stesso IP di origine e la stessa porta, ma a destinazioni diverse, l'origine ottiene NATED allo stesso IP globale e porta interna.

La soluzione al problema

Da questa descrizione è chiaro che la è possibile risolvere il problema eseguendo Indipendente dagli endpoint mapping.

Come per RCFC 4787: Con EIM (Endpoint-Independent Mapping), il NAT riutilizza il mapping delle porte per i pacchetti successivi inviati dallo stesso indirizzo IP interno e dalla stessa porta (X:x) a qualsiasi indirizzo IP e porta esterni.

Da un client, quando l'host finale esegue i comandi **nc -p 23456 10.0.0.4 40000** e **nc -p 23456 10.0.0.5 50000**, su due diverse finestre del terminale, di seguito sono riportati i risultati delle traduzioni NAT se si utilizza 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
```

Come si può notare, i diversi flussi di traffico con lo stesso indirizzo di origine e la stessa porta vengono convertiti nello stesso indirizzo/porta indipendentemente dalla porta/indirizzo di destinazione.

Sui router Cisco IOS, è possibile abilitare l'allocazione delle porte agnostiche dell'endpoint con il comando **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

Riepilogo

L'implementazione NAT di Cisco IOS è simmetrica per impostazione predefinita quando si utilizza Port Address Translation (PAT) e può causare problemi quando passa il traffico UDP P2P che richiede server come STUN per l'attraversamento NAT. Per eseguire questa operazione, è necessario configurare in modo esplicito EIM sul dispositivo NAT.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).