Entender o NAT para permitir a comunicação ponto-a-ponto em roteadores IOS e IOS XE

Contents

Introduction

Este documento descreve a necessidade de utilitários de passagem de sessão para servidores NAT (STUN), os tipos de configurações de conversão de endereço de rede (NAT) com relação aos servidores STUN, como o NAT causa um problema nessa configuração e na solução.

Informações de Apoio

A finalidade principal dos dispositivos NAT é permitir que os dispositivos com endereços IP privados em uma rede local (LAN) se comuniquem com dispositivos em espaços de endereço público, como a Internet. No entanto, embora os dispositivos NAT devam permitir que os hosts internos se conectem com o espaço público, quando se trata de aplicações ponto-a-ponto (P2P) como VoIP, jogos, WebRTC e compartilhamento de arquivos, onde os usuários finais precisam agir como cliente e servidor para manter a comunicação de ponta a ponta bidirecional, a NAT oferece dificuldade para estabelecer essas conexões UDP. As técnicas de passagem NAT são normalmente necessárias para fazer com que esses aplicativos funcionem.

Necessidade de NAT Traversal

Comunicação de voz e vídeo em tempo real na Internet são mainstream hoje com vários IMs (Instant Messengers, mensagens instantâneas) populares que oferecem suporte a chamadas VoIP. Um grande obstáculo na adoção inicial do VoIP foi o fato de que a maioria dos PCs ou outros dispositivos ficam atrás de firewalls e usam endereços IP privados. Vários endereços privados (endereço IP e porta) na rede são mapeados para um único endereço público por um firewall com NAT. Mas o dispositivo final não está ciente de seu endereço público e, portanto, não pode receber tráfego de voz da parte remota no endereço privado que anuncia em sua comunicação VoIP.

Unilateral Os processos de Correção de Autoendereço (UNSAF) são processos em que algum endpoint de origem tenta determinar ou corrigir o endereço (e a porta) pelo qual é conhecido por outro endpoint, por exemplo, para poder uUse dados de endereço na troca de protocolo ou para anunciar um endereço público do qual ele recebe conexões.

As conexões P2P em discussão são, portanto, processos UNSAF. Uma maneira comum de as aplicações P2P estabelecerem sessões de peering e permanecerem amigável com NAT é quando eles usam um servidor de reunião publicamente endereçável para fins de registro e descoberta de pares.

Utilitários de passagem de sessão para NAT

De acordo com o RFC 5389, o STUN fornece uma ferramenta que lida com NATs. Ele fornece um meio para um endpoint determinar o endereço IP e a porta alocados por um dispositivo NAT que corresponde ao seu endereço IP privado e à sua porta. Ele também fornece uma maneira de um endpoint manter uma ligação NAT ativa.

Tipos de implementações de NAT

Observou-se que o tratamento NAT do UDP varia entre as implementações. Os quatro tratamentos observados nas implementações são:

Cone completo: um NAT de cone completo é aquele em que todas as solicitações do mesmo endereço IP interno e porta são mapeadas para o mesmo endereço IP externo e porta. Além disso, qualquer host externo pode enviar um pacote para o host interno e envia um pacote para o endereço externo mapeado.

Cone restrito: um NAT de cone restrito é aquele em que todas as solicitações do mesmo endereço IP interno e porta são mapeadas para o mesmo endereço IP externo e porta. Diferentemente de um NAT de cone completo, um host externo (com endereço IP X) pode enviar um pacote para o host interno somente se o host interno já tiver enviado um pacote para o endereço IP X.

Cone restrito de porta: um NAT de cone restrito de porta é como um NAT de cone restrito, mas a restrição inclui números de porta. Especificamente, um host externo pode enviar um pacote, com o endereço IP de origem X e a porta de origem P, para o host interno somente se o host interno tiver enviado previamente um pacote para o endereço IP X e para a porta P.

Simétrico: um NAT simétrico é aquele em que todas as solicitações do mesmo endereço IP interno e porta para um endereço IP destino específico e porta são mapeadas para o mesmo endereço IP externo e porta. Se o mesmo host enviar um pacote com o mesmo endereço de origem e porta, mas para um destino diferente, um mapeamento diferente será usado. Além disso, somente o host externo que recebe um pacote pode enviar um pacote UDP de volta ao host interno.

Considere uma topologia em que a origem (A, Pa) (onde A é o endereço IP e Pa é a porta origem) se comunica com o destino (B, Pb) e (C, PC) através de um dispositivo NAT.

Tipo de implementação de NAT	Público origem quando destinado a (B, Pb)	Fonte pública quando destinada a (C, Pc)	Destino da lata (por exemplo: (B, Pb) enviar tráfego para (A, Pa)?
Cone completo	(X1, Px1)	(X1, Px1)	Yes
Cone restrito	(X1,Px1)	(X1,Px1)	Apenas se (A, Pa) tivesse enviado primeiro o tráfego para B
Cone de porta restrita	(X1,Px1)	(X1,Px1)	Somente se (A, Pa) tiver enviado primeiro o tráfego para

			(B, Pb)
Simétrico	(X1,Px1)	(X2, Px2)	Somente se (A, Pa) tiver enviado primeiro o tráfego para (B, Pb)

Problemas com NAT Traversal e NAT simétrico

Os servidores STUN respondem às solicitações de vinculação STUN enviadas por clientes STUN e fornecem o IP/porta público do cliente. Agora, esse endereço/porta combinação é usada pelo cliente STUN em sua comunicação ponto-a-ponto sinalização. No entanto, agora que a host final usa o mesmo endereço/porta privada (vamos supor que seja limite para a porta/IP pública fornecido na resposta STUN), o dispositivo NAT o converte no mesmo IP, mas em uma porta diferente se o NAT simétrico simpleseuanotação é usado. Isso interrompe a comunicação UDP porque o sinalização tinha estabelecido a conexão com base no pporta anterior.

Cisco IOS® roteadores' NAT simpleseuanotação quando ele executa o PAT é simétrico por padrão. Háeantes, espera-se que você veja problemas de conexão UDP com esses roteadores que executam NAT .

No entanto, a implementação de NAT dos roteadores Cisco IOS-XE quando executa o PAT não é simétrica. Quando você envia duas mensagens fluxos com o mesmo IP e porta de origem, mas para destinos diferentes, a origem recebe NATED para o mesmo IP e porta globais internos.

A solução para o problema

A partir dessa descrição, é evidente que a o problema pode ser resolvido se você executar Independente de endpoint mapeamento.

Conforme RCFC 4787 : Com Endpoint-Independent Mapping (EIM), o NAT reutiliza o mapeamento de portas para pacotes subsequentes enviados do mesmo endereço IP interno e porta (X:x) para qualquer endereço IP externo e porta.

A partir de um cliente, quando o host final executa os comandos **nc -p 23456 10.0.0.4 40000** e **nc -p 23456 10.0.0.5 5000**, em duas janelas de terminal diferentes, aqui estão os resultados das conversões de NAT se você usar 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
```

Aqui você pode ver que diferentes fluxos de tráfego que têm o mesmo endereço origem e porta são convertidos para o mesmo endereço/porta, independentemente da porta/endereço destino.

Nos roteadores Cisco IOS, você pode habilitar a Alocação de Porta Independente de Ponto Final com o 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

Summary

A implementação de NAT do Cisco IOS é simétrica por padrão quando você usa a Conversão de Endereço de Porta (PAT - Port Address Translation) e pode causar problemas quando ela passa o tráfego UDP P2P que exige servidores como STUN para a passagem de NAT. Você precisa configurar explicitamente o EIM no dispositivo NAT para que isso funcione.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.