NAT begrijpen om peer-to-peer communicatie mogelijk te maken op IOS en IOS XE routers

Inhoud

Inleiding

Dit document beschrijft de behoefte aan Session Traversal Utilities voor NAT (STUN) servers, de typen NAT-instellingen (Network Address Translation) met betrekking tot STUN-servers, hoe NAT een probleem bij deze installatie en de oplossing veroorzaakt.

Achtergrondinformatie

Het primaire doel van NAT-apparaten is om apparaten met privaat IP-adressen in een LAN-netwerk (Local Area Network) te laten communiceren met apparaten in openbare adresruimten, zoals het internet. Hoewel NAT-apparaten bedoeld zijn om interne hosts verbinding te laten maken met de openbare ruimte, biedt NAT problemen met het opzetten van die UDP-verbindingen wanneer het gaat om Point-to-Point (P2P)-toepassingen zoals VoIP, gaming, WebRTC en het delen van bestanden, waarbij de eindgebruikers als client en server moeten optreden om 2-voudige end-to-end communicatie te behouden. NAT-traversale technieken zijn doorgaans vereist om deze toepassingen te laten werken.

Behoefte aan NAT-transversale switch

Realtime spraak- en videocommunicatie op het internet zijn mainstream vandaag met verschillende populaire instant messengers (IM's) die VoIP-gesprekken ondersteunen. Een grote hindernis in de eerste toepassing van VoIP was het feit dat de meeste pc's of andere apparaten achter firewalls zitten en privé IP-adressen gebruiken. Meervoudige privé-adressen (IP-adres en poort) in het netwerk worden via een firewall toegewezen aan één openbaar adres. NAT. Maar het eindapparaat is zich niet bewust van zijn openbare adres, en kan daarom geen spraakverkeer van de verre partij op het privé adres ontvangen het in zijn communicatie van VoIP adverteert.

Unilateraal Self-Address Fixing (UNSAF) processen zijn processen waarbij een of ander voortkomend eindpunt probeert het adres (en de poort) te bepalen of te repareren waarmee het bekend is bij een ander eindpunt - bijvoorbeeld om in staat te zijn om uGebruik adresgegevens in de protocoluitwisseling of om een openbaar adres te adverteren waarvan het verbindingen ontvangt.

De onderhavige P2P-verbindingen zijn dus UNSAF-processen. Een veelvoorkomende manier waarop P2P-toepassingen peersessies opzetten en blijven NAT-vriendelijk is wanneer zij een openbare adresseerbare rendez-vous server gebruiken voor registratie en peer discovery.

Session Traversal Utilities voor NAT

Zoals per RFC 5389, biedt STUN een tool dat NAT's behandelt. Het voorziet in een middel voor een eindpunt om het IP adres en de haven te bepalen die door een NAT apparaat wordt toegewezen dat aan zijn privé IP adres en haven beantwoordt. Het verstrekt ook een manier voor een eindpunt om een NAT band levend te houden.

Typen NAT-implementaties

Er is vastgesteld dat de NAT-behandeling van UDP van implementatie tot uitvoering verschilt. De vier behandelingen die bij implementaties zijn waargenomen zijn:

Full Cone: Een full cone NAT is een waar alle verzoeken van hetzelfde interne IP adres en poort worden toegewezen aan hetzelfde externe IP adres en poort. Voorts kan om het even welke externe gastheer een pakket naar de interne gastheer verzenden, en het verzendt een pakket naar het in kaart gebrachte externe adres.

Restricted Cone: Een beperkte kegel NAT is een waarin alle verzoeken van hetzelfde interne IP-adres en dezelfde poort worden toegewezen aan hetzelfde externe IP-adres en dezelfde poort. In tegenstelling tot een volledige kegel NAT, kan een externe host (met IP-adres X) een pakket naar de interne host alleen sturen als de interne host eerder een pakket naar IP-adres X had verzonden.

Port Restricted Cone: Een port-limited cone NAT is als een beperkte kegel NAT, maar de beperking omvat poortnummers. Met name kan een externe host een pakket, met het IP-bronadres X en de bronpoort P, alleen naar de interne host sturen als de interne host eerder een pakket naar IP-adres X en poort P had verzonden.

Symmetrisch: Een symmetrische NAT is een NAT waarbij alle verzoeken van hetzelfde interne IP-adres en dezelfde poort naar een specifiek IP-adres en dezelfde poort naar hetzelfde externe IP-adres en dezelfde poort worden toegewezen. Als de zelfde gastheer een pakket met het zelfde bronadres en de haven, maar naar een verschillende bestemming verzendt, wordt een verschillende afbeelding gebruikt. Bovendien kan alleen de externe host die een pakket ontvangt een UDP-pakket terugsturen naar de interne host.

Overweeg een topologie waar de bron (A, Pa) (waar A het IP-adres is, en Pa de bronpoort is) communiceert met de bestemming (B, Pb) en (C, PC) via een NAT-apparaat.

Type NAT-implementatie	Public bron bij bestemd voor (B, Pb)	Publieke bron indien bestemd voor (C, PC)	Kan bestemming (bijvoorbeeld: (B, Pb) verkeer naar (A, Pa) te sturen?
Volle steen	(X1,PX1)	(X1,PX1)	Ja
Restricted Zone	(x)1,PX1)	(x)1,PX1)	Alleen als (A, Pa) eerst het verkeer naar B heeft verzonden
Poortbeperkt bereik	(x)1,PX1)	(x)1,PX1)	Alleen als (A, Pa) eerst het verkeer naar (B, Pb) had gestuurd
symmetrisch	(x)1,PX1)	(X2,PX2)	Alleen als (A, Pa) eerst het

verkeer naar (B, Pb) had gestuurd

Problemen met NAT dwars- en symmetrische NAT

STUN-servers reageren op STUN-bindende verzoeken die door STUN-clients worden verzonden en bieden de openbare IP/poort van de klant. Nu, dit adres/poort combinatie wordt gebruikt door de STUN-client in de peer-to-peer communicatie seinen. Echter, nu de endhost gebruikt hetzelfde privé-adres/poort (laten we ervan uitgaan dat dit zeker naar de openbare IP/poort verstrekt in de reactie van STUN) het NAT apparaat vertaalt het aan zelfde IP maar een verschillende haven als symmetrische NAT simpelmijnatie wordt gebruikt. Dit doorbreekt de UDP-communicatie omdat de seinen het verband gelegd op basis van hetvorige haven.

Cisco IOS® routers' NAT simpelmijnatie wanneer het PAT uitvoert is standaard symmetrisch. Therevoorstewordt echter verwacht dat u UDP-verbindingsproblemen met deze routers die NAT

De NAT-implementatie van de Cisco IOS-XE routers bij het uitvoeren van PAT is echter niet symmetrisch. Wanneer u twee verschillende streams met dezelfde bron IP en poort maar naar verschillende bestemmingen, de bron wordt NATED naar hetzelfde binnen wereldwijde IP en poort.

De oplossing voor het probleem

Uit deze beschrijving: het is duidelijk dat de probleem kan worden opgelost als u Endpoint-onafhankelijk in kaart brengen.

Volgens RCFC 4787: Met Endpoint-Independent Mapping (EIM), hergebruikt de NAT de poorttoewijzing voor verdere pakketten die vanaf hetzelfde interne IP-adres en dezelfde poort worden verzonden (X:x) naar een extern IP-adres en een externe poort.

Van een client, wanneer de endhost de opdrachten **nc -p 23456 10.0.0.4 40000** en **nc -p 23456 10.0.0.5 50000**, op twee verschillende terminalvensters uitvoert, zijn hier de resultaten van de NAT-vertalingen als u EIM gebruikt:

```
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 kunt u zien dat verschillende verkeersstromen met hetzelfde bronadres en dezelfde poort worden vertaald naar hetzelfde adres/poort, ongeacht de bestemmingshaven/het adres.

Op Cisco IOS-routers kunt u Endpoint Agnostic Port Allocation inschakelen met de opdracht **IP NAT-systeem voor inschakelen van services-haven.**

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

Samenvatting

Cisco IOS NAT-implementatie is standaard symmetrisch wanneer u poortadresomzetting (PAT) gebruikt en deze kan problemen opleveren bij het passeren van P2P UDP-verkeer waarvoor servers zoals STUN voor NAT-routing nodig zijn. U moet EIM op het NAT-apparaat expliciet configureren om dit te laten werken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.