NAT och ”NAT-traversal”

Tekniker för att hantera anslutningar in genom NAT

[8]

Olof Svensson

Innehållsförteckning

1. Introduktion

Målet med det här arbetet är att beskriva olika sätt att lösa problemen med att skapa direkta anslutningar från Internet till enheter som befinner sig bakom en Network Address Translator-router (NAT). Tanken är att presentera olika lösningar, hur de principiellt fungerar, vilka förutsättningar som krävs, lite om för- och nackdelar med respektive metod och att ge exempel på tillämpningar. Läsaren förväntas ha grundläggande kunskaper i datakommunikation och internetteknik.

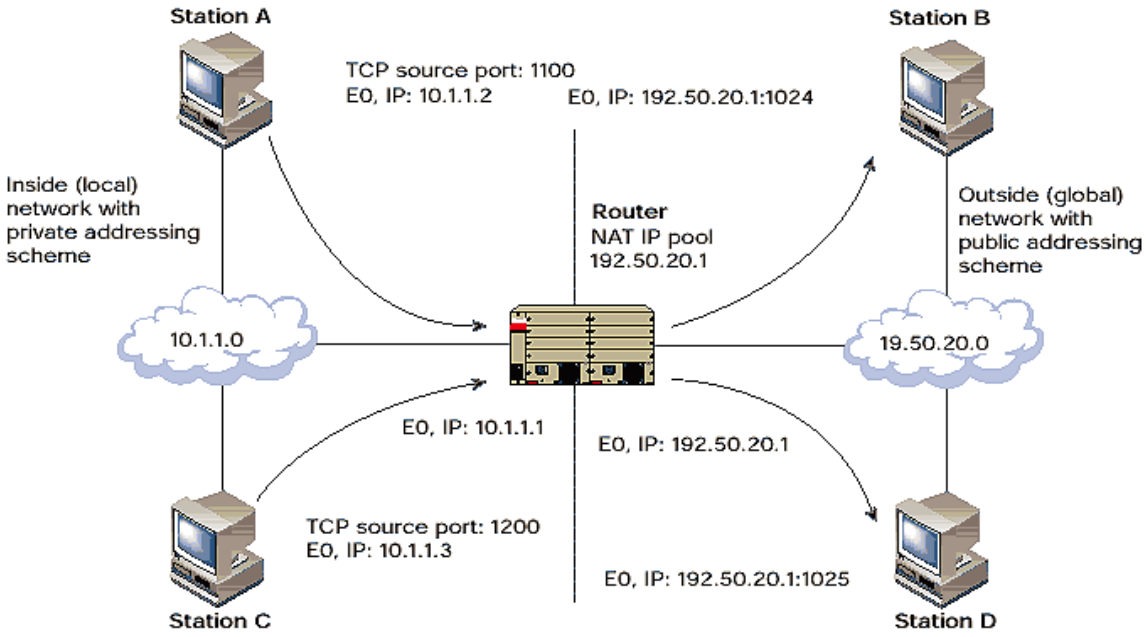
2. Kort om NAT

”the use of NATs is becoming widespread in the Internet. Some people are proclaiming NAT as both the short and long term solution to some of the Internet's address availability issues and questioning the need to continue the development of IPv6. [..] At the same time others see a myriad of difficulties caused by the increasing use of NAT.”
(RFC 2993, [1] Architectural Implications of NAT)

Allt fler elektroniska prylar (enheter) förses i dag med nätverkshårdvara och funktioner som kräver tillgång till Internet, och det blir allt vanligare att lokala nätverk på kontor eller i bostäder ansluts.
Ofta är möjligheterna att tilldela Internet-adresser till alla dessa nya enheter begränsade av avtal, kostnad eller teknik. De flesta mindre slutkunder förses med en Internet-adress per abonnemang. Ett behov av att dela upp en eller flera adresser på ett större antal enheter har skapats och den vanligaste lösningen är NAT.
Att ansluta ett lokalt nätverk genom en NAT-router till Internet är en enkel och billig lösning och Internetleverantören behöver oftast inte blandas in alls.

Bilden nedan [2] visar ett exempel på hur ett lokalt nätverk kan vara kopplat till ett annat nätverk, oftast Internet, genom en NAT-router. Notera att det för alla datorer utanför det lokala nätverket ser ut som att datorerna i det lokala nätverket har samma adress: NAT-routerns publika adress 192.50.20.1. Routerns funktion är att skapa bindningar (översätta) mellan de publika och de lokala adresserna för att anslutningar ska kunna upprättas mellan de båda näten.

Det finns lite olika typer av NAT men den vanligast förekommande typen är s.k. asymmetriska port-mappande NAT [3], och fungerar enligt principen på bilden. Den här texten behandlar bara sådana NAT.



Protokoll	Lokalt nät (LAN) Källaddress:Port	Internet (WAN) Källadress:Port	Måladress (WAN)
TCP (A till B)	10.1.1.2:1100	192.50.20.1:1024	192.50.20.2
TCP (C till D)	10.1.1.3:1200	192.50.20.1:1025	192.50.20.3

NAT-tabell för routern på bilden ovan [2]

3. Anslutningar in genom NAT

3.1 Problemet

”Network Address Translators (NATs), while providing many benefits, also come with many drawbacks. The most troublesome of those drawbacks is the fact that they break many existing IP applications, and make it difficult to deploy new ones. Guidelines have been developed that describe how to build "NAT friendly" protocols, but many protocols simply cannot be constructed according to those guidelines. Examples of such protocols include almost all peer-to peer protocols, such as multimedia communications, file sharing and games.” (RFC 3489, [3] STUN)

Ett problem med NAT är att när en anslutning ska upprättas till en enhet som befinner sig på insidan av NAT-routern, så kan inte routern av sig själv veta var den ska vidarebefordra trafiken.

När en anslutningsbegäran skickas till en port på routerns externa gränssnitt måste det finnas en regel för vidarebefordring av denna till någon enhet på det interna nätverket.

Applikationsprotokoll som skickar information om vilka adresser och portar som är öppna för andra enheter att ansluta till fungerar i allmänhet inte korrekt om inte routern konfigureras för att ta speciell hänsyn till dem. I och med P2P-protokollens växande popularitet har detta blivit en stor nackdel eftersom de bygger på direkta anslutningar mellan enskilda enheter.

3.2 Lösningar

3.2.1 Relaying

En anslutning kan upprättas indirekt med hjälp av en publik server, som två klienter ansluter till och som vidarebefordrar all trafik dem i mellan. Relaying är en mycket enkel lösning som fungerar oavsett vad för slags NAT klienterna sitter bakom. Ingen speciell konfiguration av klienterna eller deras lokala nät behöver göras. Säkerheten kan hållas på en hög nivå med krypterade anslutningar. Största problemet är dålig prestanda. För system som flyttar stora datamängder eller hanterar många anslutningar är detta en i regel en ganska dålig metod eftersom antalet klienter i regel är mycket större än antalet servrar, som har begränsad kapacitet och bandbredd.
Traversal Using Relay NAT (TURN) är ett protokoll för att vidarebefordra TCP- och UDP-trafik via en publik server [4].

Ex: Push- och POP-protokoll som E-mail via SMTP och POP. Prestandaproblem undviks genom att varje organisation har sin egen (eller flera) SMTP resp POP-servrar.

3.2.2 Manuell konfigurering

NAT-routern konfigureras statiskt att vidarebefordra all inkommande trafik på specifika portar till specifika adresser och portar på det lokala nätverket.
Detta kan bara göras om användaren av programvaran som kräver portöppningen också har kontroll över routern, och kan konfigurera den rätt.
Att manuellt konfigurera routern för forwarding är enkelt och bra för nätverk där administratören har kontroll över routern och de tjänster som behöver vara tillgängliga utifrån, t ex ett mindre kontorsnätverk.
Om programvaran av olika skäl måste använda en specifik port kan bara en enhet per publik adress (WAN IP) vara aktiv samtidigt.
En del tjänster använder slumpmässigt utvalda portar eller portar i relativt stora intervaller. Att skapa forwarding-regler för ett stort intervall innebär att antalet portar som kan användas av andra datorer på det lokala nätverket minskar drastiskt.
Att skapa en forwarding-regel för en port innebär också att den exponeras för det publika nätet vilket kan innebära en säkerhetsrisk.

Ex: Ett företag som vill ha en publik webbserver på sin externa adress kan konfigurera routern att vidarebefordra all inkommande trafik på port 80 till en webbserver på sitt lokala nätverk.

3.2.3 Tunneling, VPN och Callback

En VPN-lösning kan användas för att upprätta kommunikation med en enhet på det lokala nätverket och låta en gästdator utanför nätverket agera som om den vore lokalt ansluten. VPN kan vara ett bra sätt att undvika problem med NAT om avsikten är att anslutningarna ska främst ska ske inom det virtuella nätverket, t ex inom ett företag med geografiskt spridda kontor. En VPN-router måste finnas i båda ändar av anslutningen och NAT-routern måste stödja detta. VPN-förbindelsen kan krypteras för att höja säkerhetsnivån.

Ex: Ett företag med två mindre kontor i Zürich och Stockholm har ett IP-telefonisystem för interna samtal. Båda kontoren har ett LAN bakom NAT med var sin publika IP-adress. Det finns 20 telefoner på varje kontor och alla använder samma port. Situationen löses genom att koppla samman de båda kontorsnäten med VPN genom NAT-routern.

En port kan, om datorn som tillhandahåller tjänsten tillåter det, tunnlas via t ex SSH till en fjärrdator, för att möjliggöra kommunikation med godtycklig tjänst som är tillgänglig i det lokala nätverket. Den här tekniken lämpar sig bäst för när man kan lita på att portarna inte tunnlas till en osäker miljö eller att de tillgängliga tjänsterna är inherent säkra. SSH har annars hög säkerhet mot avlyssning och manipulering av det som överförs. Den här typen av tunneling varar bara medan det finns en aktiv SSH-session och är därför mer lämplig för tillfälliga aktiviteter.

Ex: Bob jobbar hemifrån. En ändring ska göras i en kunddatabas, men SQL-servern är bakom NAT och dessutom är det dubbla brandväggar i mellan. Det finns däremot en statiskt forwardad port på SQL-servern dit Bob kan ansluta med SSH. Bob tunnlar SQL-serverns port till sin egen dator hemma via SSH.

Callback kan se ut på olika sätt, men principen är att genom en öppen tjänst på det lokala nätverket, signalera ett klientprogram att ansluta till en given server. Den här tekniken kan användas även med ganska begränsade användarrättigheter.

Ex: Bob vill fjärrstyra sin dator på jobbet via VNC, men den är bakom NAT och det finns ingen forwarding. Bob har DSL och dynamisk IP, men kör en SSH-server hemma. Det finns ett script på Bobs dator på jobbet som regelbundet tömmer och scannar all inkommande e-post efter en speciell nyckel. Bob mailar sin nyckel och scriptet kör en SSH-klient mot Bobs hemmadator, och forwardar VNC-porten.

3.2.4 Application Layer Gateway (ALG)

En Application Layer Gateway är ett program som är skräddarsytt för att skapa kompatibilitet med ett specifikt applikationsprotokoll. Protokoll med information om adresser och öppna portar på en intern enhet (t ex FTP) kan fås att fungera genom att läsa av trafiken på applikationsnivå och modifiera adresser eller skapa forwarding-regler för varje session [6].

ALG används i huvudsak för att skapa kompatibilitet med etablerade protokoll eftersom den är specifikt skriven för varje protokoll och för den specifika routern.

3.2.5 Simple Traversal of UDP over NATs (STUN)

STUN är ett protokoll (RFC 3489) för att kartlägga vad för slags NAT som finns mellan en enhet på ett lokalt nätverk och Internet och vilka de motsvarande publika adresserna är.
Detta görs genom att en STUN-klient kontaktar en publik STUN-server, och utför ett antal tester för att kartlägga hur nätet mellan dem hanterar UDP-trafik. Servern ser den publika adressen, och genom att kategorisera olika typer av NAT efter hur testerna faller ut kan man välja olika sätt att hantera problemet.
Eftersom UDP-kommunikation är stateless sätter en NAT-router i regel upp en forwarding-regel med en timeout mellan två portar när den observerar inkommande UDP-trafik. All trafik in och ut på samma port vidarebefordras sedan mellan de två kommunikationsdeltagarna.
Med hjälp av STUN kartläggs den publika adressen av applikationen, och denna används sedan för att facilitera öppning av UDP-portar. Dessa kan sedan användas för trafik i båda riktningarna. Ingen speciell konfigurering behövs vilket förenklar administrationen av det lokala nätverket. STUN är inte kompatibelt med alla typer av NAT, alla NAT-routrar och garanterar inte att kompatibilitet med kommande varianter av NAT.

Ex: Google Talk använder STUN

3.2.6 UDP Hole Punching

UDP Hole Punching kallas också den princip som innebär öppnande av UDP-portar i en NAT-router med hjälp av en publik server [7]. Flera proprietära protokoll använder sig av UDP Hole Punching. Det är också denna princip som STUN bygger på. UDP Hole Punching fungerar inte med alla typer av NAT och inte heller med alla routrar. Kompatibiliteten ökar emellertid då användandet ökar och router-tillverkarna vill stödja metoden.

Ex: Skype använder sig av sin egen UDP Hole Punching-implementation.

3.2.7 UPnP

UPnP är en standard för att definiera och kontrollera enheter som kopplas in på ett nätverk. En kategori av dessa enheter är Internet Gateway Device (IGD). En IGD är en generell definition av en NAT-router [5]. Routern implementerar en server som exporterar de funktioner som krävs av definitionen. En UPnP-applikation som ansluter till en IGD kan bland annat få reda på den publika IP adressen, kontrollera vilka portar som används och till vad, eller lägga till tillfälliga eller permanenta forwarding-regler. På så sätt kan ett P2P-program som behöver öppna portar för inkommande anslutningar, också se till att NAT-routern vidarebefordrar dessa till rätt ställe.
UPnP är sprunget ur UPnP Forum, en sammanslutning av olika hård- och mjukvarutillverkare. UPnP gör administrationen av nätverket väldigt enkel, tanken är att den ska vara obefintlig. Säkerheten i UPnP kan emellertid diskuteras eftersom tekniken i princip gör det möjligt för vilken programvara som helst på det lokala nätverket att skapa godtyckliga forwarding-regler, som kan underminera säkerheten och stabiliteten i nätverket.

Ex: Tele2’s IP-telefonidosa använder UPnP för att skapa rätt forwarding-regler när den ansluts till ett nät innanför en NAT-router.

4. Källförteckning

[1] Architectural Implications of NAT
The Internet Society. T. Hain.
http://www.iptel.org/ietf/firewall/arch/rfc2993.txt
November 2000

[2] Enterasys White Paper on Network Address Translation
http://www.enterasys.com/products/whitepapers/ssr/network-trans

[3] STUN (RFC 3489)
The Internet Society. Rosenberg, et al.
http://www.ietf.org/rfc/rfc3489.txt
Mars 2003

[4] Traversal Using Relay NAT (TURN)
Rosenberg, et al.
http://www.jdrosen.net/papers/draft-rosenberg-midcom-turn-08.txt
September 2005

[5] Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0
UPnP Forum
http://www.upnp.org/standardizeddcps/documents/UPnP_IGD_1.0.zip
November 2001

[6] White Paper - NAT Traversal Solutions for Multimedia over IP Services
Newport Networks
http://www.newport-networks.com/whitepapers/nat-traversal2.html

[7] Peer-to-Peer Communication Across Network Address Translators
Ford, et al.
http://www.brynosaurus.com/pub/net/p2pnat
Februari 2005

[8] Bosco's Screen Share™
Hutchings Software
http://www.componentx.com/ScreenShare/router_setup.php