Retiisi

Reaaliaikaiset Internet-palvelut ja SIP

Palomuurit ja NAT SIP-palvelun rakentamisessa

Kirjoittajat:	Mika Mustikkamäki TYT/Wirlab
Kuvaus:	Palomuurien ja NAT:in toiminta SIP-palvelua rakennettaessa, ratkaisumahdollisuuksia
Tiedostonimi:	Retiisi-Palomuurit_ja_NAT.pdf
Dokumentin tila:	Julkaistu
Versio:	1.2
Päiväys:	13/12/2005

SISÄLLYSLUETTELO

1. Johdanto

Tässä Retiisi-projektin dokumentissa käsitellään SIP-palveluiden rakentamista verkkoympäristöihin, joissa on otettava huomioon palomuurien ja NAT-osoitekäännösten asettamat vaatimukset ja rajoitukset. Dokumentissa esiteltävät otsikot on tarkoitettu ensisijaisesti SIP-palveluita tarjoavien operaattoreiden käyttöön ympäristöjen suunnittelun ja rakentamisen tueksi. Dokumentti toimii kuitenkin myös yleisenä johdatuksena IP-puheluympäristöjen problematiikkaan silloin kun käytössä on IP-liikennettä rajoittavia ja määrittäviä tekijöitä kuten palomuurit tai NAT-osoitekäännökset.

Dokumentissa käydään ensin läpi keskeiset SIP-palvelussa esiintyvät protokollat ja niiden toiminta, sekä esitellään yleisimmät palomuuri- ja NAT-tyypit. Tämän jälkeen eritellään tarkemmin, millä eri tavoilla SIP-palvelun toiminta voi keskeytyä tai häiriintyä. Lopuksi tarkastellaan ohjelmistoympäristöjä ja -asetuksia, jotka mahdollistavat toimivan SIP-palvelun toteutumisen, sekä luodaan perussuositukset toimivan SIP-IP-puheluympäristön rakentamista varten.

2. Session Initiation Protocol (SIP)

SIP-protokolla määrittelee toimijoiden välisten istuntojen perustamiseen, ylläpitoon ja purkamiseen liittyvät viestit. Se on standardoitu IETF RFC:ssä 3261 [1], johon on lisäksi julkaistu päivitykset IETF RFC 3265 [2] ja IETF RFC 3853 [3]. Istunto on lähettäjistä ja vastaanottajista sekä niiden välisestä kommunikaatiosta muodostuva käsite, jolla voidaan tarkoittaa esimerkiksi internet-puheluita ja muita multimediaelementtejä sisältävää viestinvaihtoa [4]. IETF RFC 3261 määrittelee kuusi erilaista request-tapaa, joilla istuntoja hallitaan. Ne ovat INVITE, ACK, BYE, REGISTER, CANCEL ja OPTIONS. SIP-protokolla on suunniteltu kevyeksi, skaalautuvaksi ja helposti implementoitavaksi. Se on tekstipohjainen ja viestirakenteeltaan HTTP-protokollan kaltainen. SIP-protokolla nähdään ITU:n standardoiman H.323-protokollan korvaajana.

Edellä mainittujen keskeisten SIP-standardien lisäksi on olemassa useita täydentäviä standardeja, joilla määritellään mm. pikaviestien lähetys, salattu signalointi, erilaisia puhelunreitityssääntöjä ja monia muita. Tässä dokumentissa esiteltävät kokonaisuudet perustuvat pääosin IETF RFC:n 3261 määrityksiin.

2.1. SIP:in taustaa

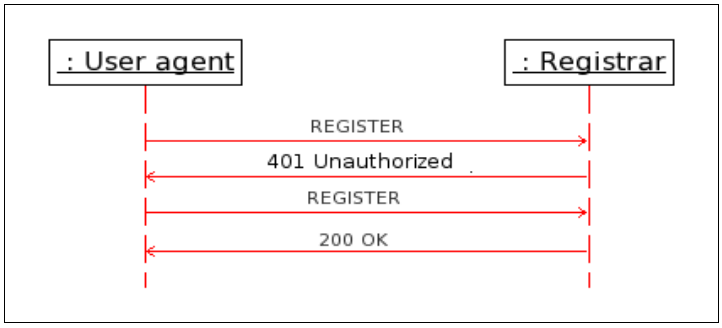
Ensimmäinen IETF:n SIP:iin liittyvä draft (luonnos) oli helmikuussa 1996 julkaistu draft-ietf-mmusic-sip-00 [5], johon julkaistiin kolmen seuraavan vuoden aikana yksitoista päivitystä ennen draft-versiosta draft-ietf-mmusic-sip-12 siirtymistä hyväksytyn RFC:n asteelle, silloin numerolla 2543. Keskeisiä henkilöitä SIP:in kehityksessä ovat olleet erityisesti Jonathan Rosenberg ja Henning Schulzrinne. SIP-protokollan alkutaival on ollut enemmän tai vähemmän hankalaa H.323-protokollan hallitessa nykyisiä tuotemarkkinoita. Kahden viime vuoden aikana SIP-protokollaa käyttävät laitteet ja ohjelmistot ovat kuitenkin yleistyneet niin paljon, että niiden

voidaan katsoa nouseen markkinoiden silmissä tasavertaiseen asemaan suurimman kilpailijansa kanssa.

Tärkeä voitto SIP:lle oli sen valinta kolmannen sukupolven matkapuhelinverkkojen keskeiseksi puhelujen signalointiprotokollaksi. Jo tällä hetkellä SIP:iä käytetään osassa matkaviestimien push-to-talk -ominaisuuksien toteutuksia, ja tuleva Nokian Presence Solution -versio lisää yhteensopivuutta OMA:n PoC-toteutuksen ja SIP/SIMPLE-toteutusten välillä.

2.2. Esimerkkejä SIP-signaloinnista

Ohessa esitellään SIP:in perussignalointia SIP-rekisteröinnissä ja puhelun muodostuksessa kahden osapuolen välillä. Kuvassa 1 nähdään signaloinnin eteneminen rekisteröitäessä käyttäjän SIP-identiteetti palvelimelle. User agent kuvaa käyttäjän päätelaitetta tai -ohjelmistoa ja Registrar on verkossa toimiva operaattorin SIP-välityspalvelin.



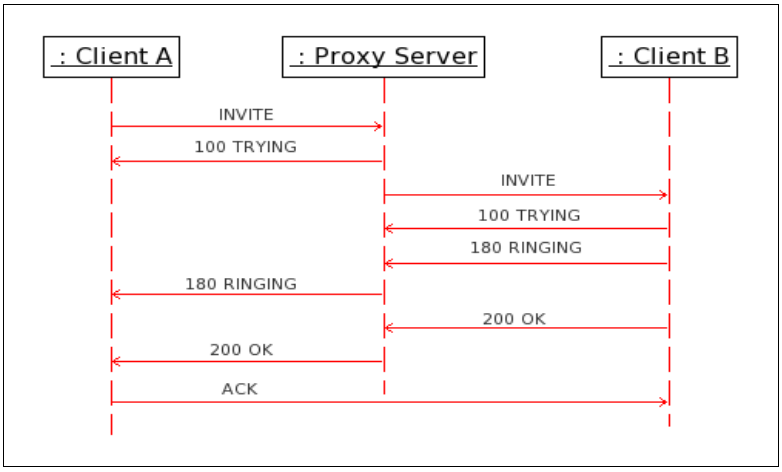
Kuva 1: SIP REGISTER

Kuvassa esitetyn REGISTER-tapahtuman signalointi etenee seuraavasti:

```
REGISTER sip:wirlab.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK25837588
CSeq: 3189 REGISTER
To: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Expires: 900
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Call-ID: 117525788@192.168.1.42
Content-Length: 0
User-Agent: kphone/4.1.1-pre2
Event: registration
Allow-Events: presence
Contact: "Mika Mustikkamaki" <sip:mika.mustikkamaki@192.168.1.42;transport=udp>;methods="INVITE, MESSAGE, INFO,
SUBSCRIBE, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER"

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK25837588
CSeq: 3189 REGISTER
To: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=452a782dfafe2eba1e0b092c27257495.cd1c
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Call-ID: 117525788@192.168.1.42
WWW-Authenticate: Digest realm="wirlab.net", nonce="4222d2ab637c1108cc58de4bdbedeafdbf774156", qop="auth"
Server: Wirlab Research Center SIP Router (0.9.0 (i386/linux))
Content-Length: 0

SipCall: Incoming response
SipTransaction: Incoming Response
SipRegister: Authentication required
getDigestResponse(): Remote endpoint supports Digest with qop=auth
WL: SipProtocol: HA1=029821d612d8e4a9497b4702fe783cfb (mika.mustikkamaki@wirlab.net:wirlab.net)
SipProtocol: Digest calculated.
SipRegister: Auth is 'Digest username="mika.mustikkamaki@wirlab.net", realm="wirlab.net",
nonce="4222d2ab637c1108cc58de4bdbedeafdbf774156", uri="sip:wirlab.net", qop=auth, cnonce="abcdefghi", nc=00000001,
response="065536033c97a56ca77b71d9a6542d61", opaque="", algorithm="MD5"'
```

```
SipRegister: Proxy Auth is '(null)'

REGISTER sip:wirlab.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK78B6938A
CSeq: 3190 REGISTER
To: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Authorization: Digest username="mika.mustikkamaki@wirlab.net", realm="wirlab.net",
nonce="4222d2ab637c1108cc58de4bdbedeafdbf774156", uri="sip:wirlab.net", qop=auth, cnonce="abcdefghi", nc=00000001,
response="065536033c97a56ca77b71d9a6542d61", opaque="", algorithm="MD5"
Expires: 900
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Call-ID: 117525788@192.168.1.42
Content-Length: 0
User-Agent: kphone/4.1.1-pre2
Event: registration
Allow-Events: presence
Contact: "Mika Mustikkamaki" <sip:mika.mustikkamaki@192.168.1.42;transport=udp>;methods="INVITE, MESSAGE, INFO,
SUBSCRIBE, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER"

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK78B6938A
CSeq: 3190 REGISTER
To: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=452a782dfafe2eba1e0b092c27257495.4742
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>
Call-ID: 117525788@192.168.1.42
Contact: <sip:mika.mustikkamaki@192.168.1.42;transport=udp>;q=0.5;expires=900
Server: Wirlab Research Center SIP Router (0.9.0 (i386/linux))
Content-Length: 0
```

Kuvassa 2 esitetään käyttäjältä A lähtevä istunnon aloituspyyntö (INVITE) käyttäjälle B. INVITE kulkee operaattorin välityspalvelimen kautta. Kuvassa esitetään puhelun kulku pisteeseen, jossa aloitetaan varsinaisen median (ääni) siirto.



Kuva 2: SIP INVITE

SIP INVITE:n signalointi kulkee seuraavasti:

```
INVITE sip:user@domain SIP/2.0

Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK56D2CCD8
CSeq: 2672 INVITE
To: <sip:user@domain>
Content-Type: application/sdp
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=6FFD5B78
Call-ID: 883050662@192.168.1.42
Subject: sip:mika.mustikkamaki@wirlab.net
Content-Length: 204
User-Agent: kphone/4.1.1-pre2
Contact: "Mika Mustikkamaki" <sip:mika.mustikkamaki@192.168.1.42;transport=udp>

(SDP information removed)

SIP/2.0 100 trying -- your call is important to us
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK56D2CCD8
CSeq: 2672 INVITE
To: <sip:user@domain>
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=6FFD5B78
Call-ID: 883050662@192.168.1.42
Server: Wirlab Research Center SIP Router (0.8.99-dev5 (i386/linux))
Content-Length: 0
```

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK56D2CCD8
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=6FFD5B78
To: <sip:user@domain>;tag=1959889910
Contact: <sip:mtm@192.168.1.44:5060>
Record-Route: <sip:192.98.81.153;lr>
Call-ID: 883050662@192.168.1.42
CSeq: 2672 INVITE
Server: X-Lite release 1103m
Content-Length: 0

SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK56D2CCD8
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=6FFD5B78
To: <sip:user@domain>;tag=1959889910
Contact: <sip:mtm@192.168.1.44:5060>
Record-Route: <sip:192.98.81.153;lr>
Call-ID: 883050662@192.168.1.42
CSeq: 2672 INVITE
Content-Type: application/sdp
Server: X-Lite release 1103m
Content-Length: 290

(SDP information removed)

ACK sip:mtm@192.168.1.44:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.42;branch=z9hG4bK56D2CCD8
CSeq: 2672 ACK
To: <sip:user@domain>;tag=1959889910
From: "Mika Mustikkamaki" <sip:mika.mustikkamaki@wirlab.net>;tag=6FFD5B78
Call-ID: 883050662@192.168.1.42
Route: <sip:192.98.81.153;lr>
Content-Length: 0
User-Agent: kphone/4.1.1-pre2
Contact: "Mika Mustikkamaki" <sip:mika.mustikkamaki@192.168.1.42;transport=udp>
```

3. Session Description Protocol (SDP)

Tämä standardi määritellään IETF RFC:ssä 2327 [6] ja IETF RFC:ssä 3266 [7]. SDP on protokolla jolla kuvaillaan multimediaistuntojen ominaisuuksia, mutta se ei ota kantaa istuntojen ominaisuuksien neuvotteluun. SIP:in yhteydessä tämä tarkoittaa yleisesti sitä, että istuntojen osapuolet käyttävät SDP-tietueita tukemiensa äänikodekkien mainostamiseen ja ilmoittavat SDP-kentissä mm. IP-osoitteensa. SDP ei ole itsessään siirtokerroksen protokolla, vaan SIP:in tapauksessa SDP:tä käytetään siirtämään tarvittava tieto kommunikoiville osapuolille. SDP:n yleisenä tarkoituksena on ilmoittaa istunnon nimi ja tarkoitus, aikavälin jolloin kyseinen istunto on aktiivisena, tietoa mediasta joka muodostaa istunnon sekä tarvittavat tiedot median vastaanottamiseksi [8].

SDP suunniteltiin alunperin multicast-neuvotteluiden välityksen avuksi. Tyypillisen SIP-istunnon SDP-tietueet koostuvat seuraavista kentistä:

```
v=0
o=username 0 0 IN IP4 192.168.1.42
s=The Funky Flow
c=IN IP4 192.168.1.42
t=0 0
m=audio 33068 RTP/AVP 0 97 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:97 iLBC/8000
a=fmtp:97 mode=30
```

Purettuna: `v` on protokollaversio, `o` omistaja- ja istunnon kuvaus, `s` istunnon nimi, `c` yhteyden tiedot, `t` istunnon aktiivisuus, `m` media ja tiedonsiirron tyyppi sekä `a`-kentät media-attribuutteja.

4. Realtime Transport Protocol (RTP)

RTP on varsinaisen median siirtoon tarkoitettu protokolla. Se määritetään IETF RFC:ssä 3550 [9] ja IETF RFC:ssä 3551 [10]. Nimensä mukaisesti se pyrkii tarjoamaan siirtoyhteyden reaaliaikaisuutta tarvitseville sovelluksille, kuten ääni ja video. RTP:tä voidaan käyttää sekä multi- että unicast-tyyppisissä ympäristöissä. RTP:tä käytetään yleensä yhdessä UDP:n kanssa, joten se on yhteydetön eikä tarjoa siten luotettavaa, sekventiaalista pakettien lähetystä. Täten RTP-protokolla itsessään ei myöskään takaa reaaliaikaisuutta itse mediansiirtopalvelussa. RTP-protokolla koostuu kahdesta lähekkäisestä ali-protokollasta, RTP:stä ja RTCP:stä. Jälkimmäinen on niinkutsuttu kontrolliprotokolla, joka valvoo palvelun laatua sekä välittää käynnissä olevasta istunnosta tietoa siihen osallistuville osapuolille [11]. RTCP tunnistaa myös mahdollisen pakettihävikin, jolloin median vastaanottaja voi kompensoida hävikistä aiheutuvaa viiveen vaihtelua.

RTP-paketti koostuu seuraavista osista: sekvenssinumero, hyötykuorman tunniste, kehyksen tunniste, lähteen tunniste sekä mediansisäinen synkronointi. RTCP-paketin osat ovat palvelunlaadun palaute (feedback), istunnonhallinta, tunniste sekä mediansisäinen synkronointi.

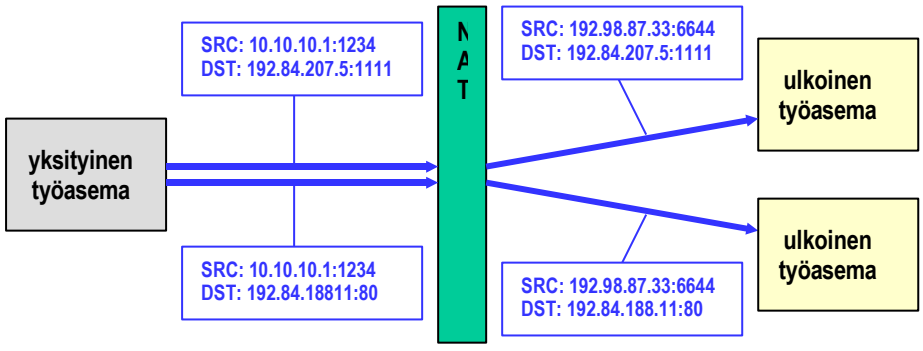
5. Network Address Translation (NAT)

NAT:ia, joka on standardoitu IETF RFC:ssä 3022 [12] käytetään yleisesti tilanteissa, joissa julkinen IP-osoiteavaruus on rajattu tai organisaation sisäverkko halutaan piilottaa julkiselta internetiltä yhden ulospäin näkyvän osoitteen suojaan. Kaikki liikenne kulkee tällöin yksityisistä osoitteista julkisiin osoitteisiin verkon reunalla olevan NAT:in toteuttavan laitteen läpi. NAT:illa voidaan toteuttaa myös käännös, jossa yksityisen puolen osoitteita voidaan kääntää samaan määrään julkisia osoitteita. Tällöin käyttötarkoitus on puhtaammin sisäverkon osoitteiden peittäminen julkiselta verkolta. Samalla kuitenkin mahdollistuu se, että sisäverkossa yksityisillä osoitteilla olevat koneet voivat tarjota palveluitaan julkiseen internetiin päin. Suurin syy NAT:in käyttöön tänä päivänä on kuitenkin IPv4-osoiteavaruuden rajallisuus. NAT:ia käyttämällä operaattorit voivat käyttää samoja yksityisiä osoiteavaruuksia usean asiakkaan verkoissa, ja kääntää sitten kunkin yhteyden terminointipisteessä koko asiakas-aliverkon yhteen julkiseen osoitteeseen.

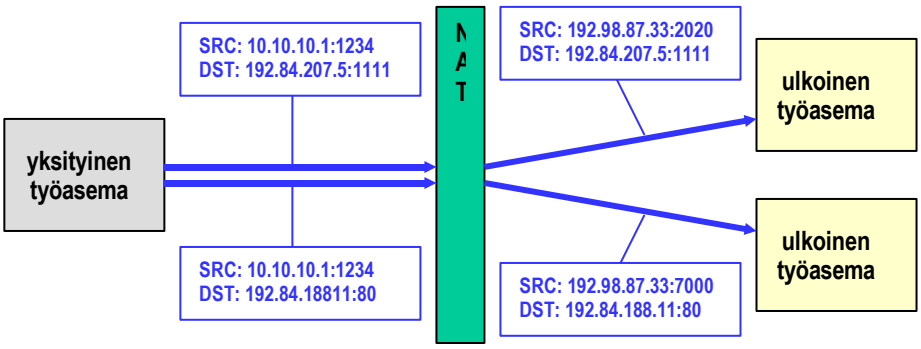
Yleisintä toteutusta, jossa koko yksityinen aliverkko käännetään yhdeksi julkiseksi osoitteeksi kutsutaan myös nimellä PAT. Tällä tarkoitetaan sitä, että erilliset yksityiset puolen osoitteet käännetään useiksi julkisiksi “virtuaaliosoitteiksi” muuttamalla julkisen osoitteen tietoliikenneporttia.

5.1. NAT-tyypit ja niiden erot

NAT-toteutukset voidaan jakaa karkeasti kahteen kategoriaan: cone-tyyppiset ja symmetriset. Cone-tyyppisissä NAT:eissa julkinen lähdeosoite (so. ulospäin näkyvä yhteysosoite) käännetään perustuen yksityiseen lähdeosoitteeseen ja -porttiin. Cone-tyypit jaotellaan vielä kolmeen eri ala-kategoriaan: Full Cone, Restricted Cone ja Port Restricted Cone. Näistä tarkemmin alla. Symmetrisessä toteutuksessa julkinen lähdeosoite käännetään sekä yksityisen lähdeosoitteen ja -portin että julkisen kohdeosoitteen ja -portin perusteella. Seuraavassa Cone- ja symmetrisen NAT:in peruseroavaisuudet.

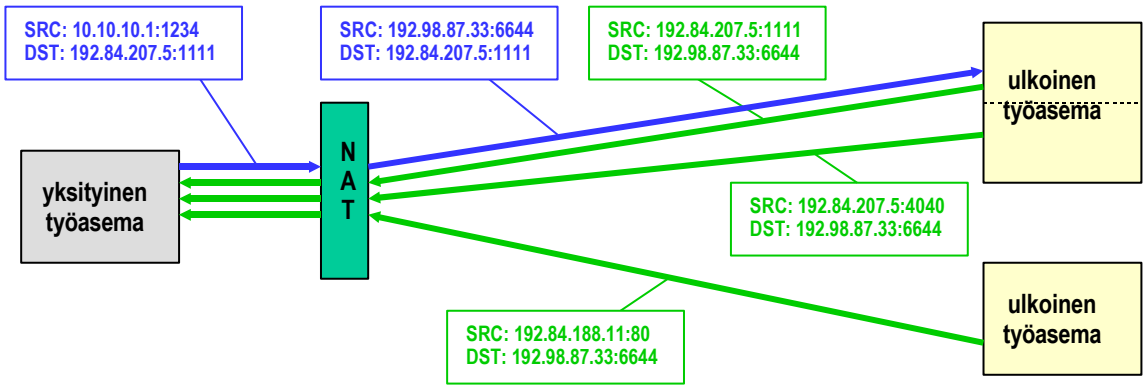


Kuva 3. Cone-tyyppinen NAT



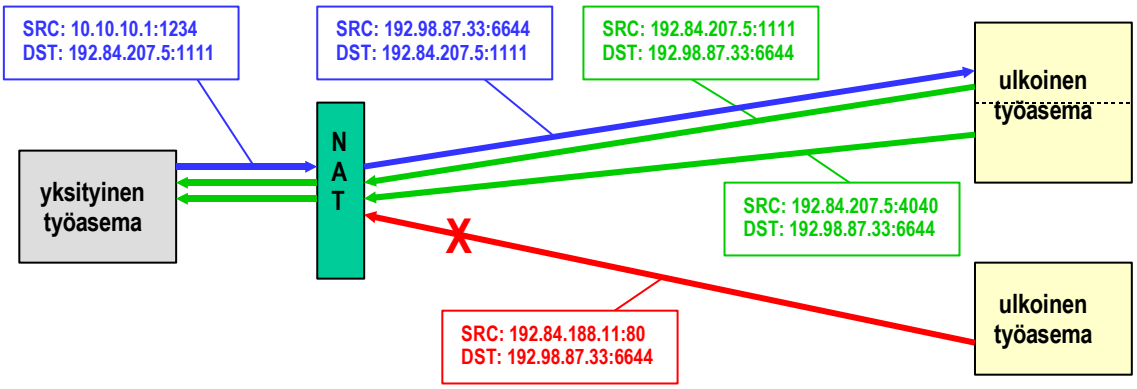
Kuva 4. Symmetrinen NAT

Cone-tyyppisten NAT:ien ala-kategorioissa Full Cone NAT toimii siten, että mistä tahansa ulkoisesta lähdeosoitteesta voidaan liikennöidä NAT:in läpi yksityisiin kohteisiin kuten kuvassa 5 esitetään.



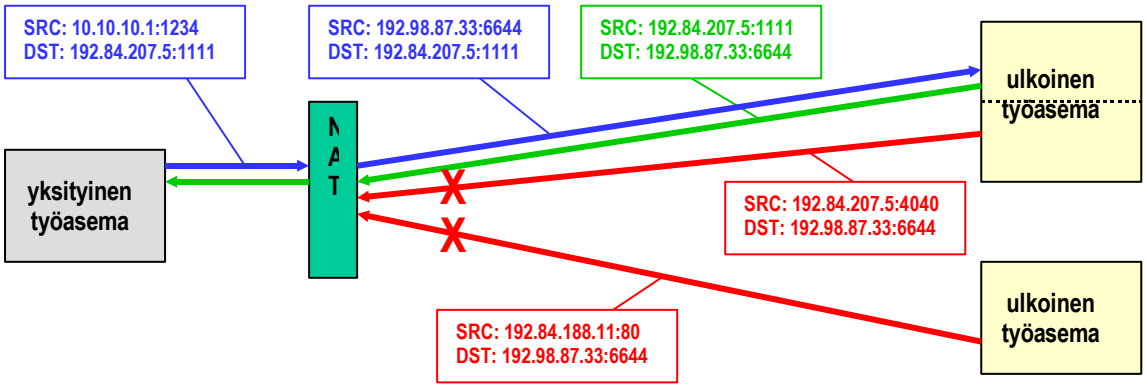
Kuva 5: Full Cone NAT

Restricted Cone NAT toimii puolestaan siten, että yksityisen puolen NAT-käännökset ovat avoimia ainoastaan niille ulkopuolisille kohteille, joihin yksityiseltä puolelta on ensin avattu tiedonsiirtoyhteys, kuten kuvassa 6.



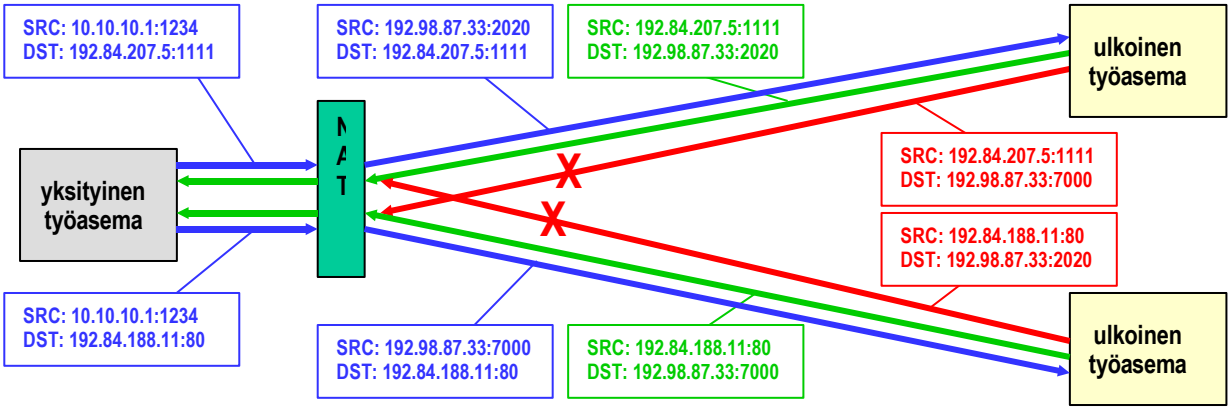
Kuva 6. Restricted Cone NAT

Viimeisenä cone-tyyppisenä NAT:ina on Port Restricted Cone, jossa toiminta on kuten Restricted Cone NAT:issa sillä erotuksella, että myös julkisen puolen portilla on merkitystä. Vain kohdeosoitteista ja *porteista*, jonne NAT:in takaa on ensin liikennöity, on oikeus lähettää paluupaketteja yksityisen puolen kohteeseen, kuten kuvassa 7.



Kuva 7. Port Restricted Cone NAT

Symmetrisen NAT:in tapauksessa NAT-käännökset ovat istuntokohtaisia, eli käännös on avoin ainoastaan sille julkiselle lähdeosoitteelle, jota varten käännös on alunperin luotu, kuten kuvassa 8.



Kuva 8. Symmetrinen NAT

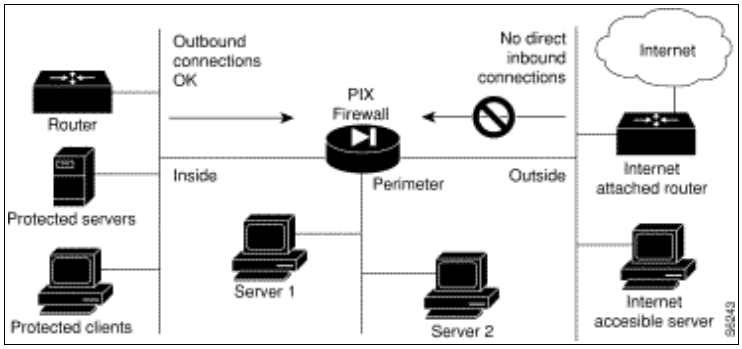
6. Palomuurit

Palomuurit ovat nykyisissä yritys- ja yksityisverkoissa enemmän sääntö kuin poikkeus. Palomuurien yleisesti käsitetty tehtävä on toiminnallisuutena yksinkertainen: estää internetistä tulevaa haitallista verkkoliikennettä pääsemästä läpi organisaation omaan verkkoon tai asiakkaille. Palomuuri jakaa verkon käyttäjänsä kannalta yleensä vähintään kahteen alueeseen: internetiin (ei-luotettu alue) ja sisäverkkoon (luotettu alue). Palomuurin tarkoitus on kontrolloida hallitusti näiden alueiden välistä liikennettä perustuen kulloinkin aktiiviseen tietoturvapolitiikkaan (policy). Palomuurilla voidaan estää esimerkiksi troijalaisten, palvelunestohyökkäysten, vakoiluohjelmistojen sekä luvattomien porttiskannauksien pääsy organisaation verkkoon. Palomuuriratkaisujen laajennukseksi hankitaan usein erillinen virusskanneri, mutta joissakin palomuurituotteissa sellainen on valmiiksi integroituna.

Palomuurit voidaan jakaa karkeasti kahteen tyyppiin: verkkokerroksen palomuurit ja sovelluskerroksen palomuurit. Verkkokerroksella toiminta perustuu suodattimiin (filter), jotka määrittävät millaiset IP-paketit saavat kulkea palomuurin läpi ja mitkä kielletään. Sovellustasolla palomuuri voi ottaa suoraan kantaa käytettävän sovelluksen oikeuksiin kuljettaa liikennettä palomuurin läpi. Tällaisia sovelluksia voivat olla esimerkiksi sähköposti ja www. Nykyään suurin osa palomuureista on nimenomaan sovelluskerroksen vartijoita, eli ne tarkastelevat läpi menevien pakettien hyötykuormaa ja toteuttavat tuloksiin perustuen konfiguroitujen sääntöjensä mukaisia toimenpiteitä.Hyötykuorman tarkkailusta käytetään käsitettä *stateful inspection [13]*.

Palomuurin sääntökanta koostuu säännöistä, joissa määritellään sallitut ja kielletyt lähde-/kohdeosoitteet ja -tietoliikenneportit ja tiedonsiirtoprotokollat (TCP, UDP, ICMP jne.).

Jos palomuuria käyttävä organisaatio tarjoaa palveluita julkiseen verkkoon, palomuurin avulla muodostetaan usein ns. DMZ-alue. Tällä tarkoitetaan sitä, että varsinainen organisaation sisäverkko, jossa sijaitsee työntekijöiden työasemat sekä muut toimistolaitteet, pidetään kokonaan palomuurin takana julkiselta verkolta piilossa, mutta tiettyjä palveluja (nimipalvelu, web, sähköposti) tarjoavia koneita varten palomuuriin tehdään erillinen, avoimempi aliverkko, josta liikenne julkisesta verkosta pääsee vuotamaan DMZ:ssa oleville palvelimille. Palomuurit pitävät usein sisällään myös NAT-ominaisuuksia, joista lisää seuraavassa kappaleessa. Kuvassa 3 Cisco PIX -esimerkkitoteutus.



Kuva 3: Esimerkkiympäristö Cisco PIX-palomuurilla [14]

7. SIP-ympäristön protokollien ongelmat palomuuri- ja NAT-ympäristöissä

Oletetaan, että SIP-välityspalvelin on joko julkisessa Internetissä tai DMZ-alueella. Tämä on lähtökohtainen suositus välityspalvelimen sijainniksi. SIP-signalointi kohtaa ongelmia palomuurien kanssa lähinnä estettyjen porttien myötä. SIP-palvelimet ja asiakasohjelmistot kuuntelevat SIP-pyyntöjä ja vasteita yleensä portissa `5060`. Mikäli tämän portin käyttö on estetty palomuurissa, mitkään SIP-sanomat eivät oletusasetuksilla pääse päätelaitteelta välityspalvelimelle tai toisin päin. Myös erilaiset voimassaoloajan asetukset palomuurissa määriteltynä aiheuttavat ongelmia – palomuuri saattaa estää päätelaitteen tai asiakasohjelmiston pakettilähetykset, mikäli kyseisestä lähdeosoitteesta ei tule määritellyn ajanjakson sisällä verkkoliikennettä palomuurille.

NAT on myös huomattava ongelmien aiheuttaja SIP:issä. Koska julkisen NAT-osoitteen takana käytetään useita yksityisiä, ei julkisesti reititettäviä IP-osoitteita, on SIP-proxyn normaaleissa olosuhteissa mahdotonta reitittää SIP-kutsuja NAT:in takana oleviin osoitteisiin. Proxy ei voi tietää kunkin NAT-yhteyden porttimäärityksiä ja siten yhteyksien avaaminen ulkoapäin NAT:in taakse estyy (esimerkiksi INVITE-viestissä). Myös NAT-käännöksen takana olevan päätelaitteen on joissain tapauksissa selvitettävä, minkälainen NAT sen edessä on (mikäli on) ja kirjoitettava vastaavasti omat julkisen IP-osoitteen kontaktitietonsa SIP-viesteihin. Tällainen päätelaitteen hoitaman NAT-tunnistuksen käyttö on viime aikoina kuitenkin vähentynyt huomattavasti siinä käytettyjen standardien ongelmien vuoksi.

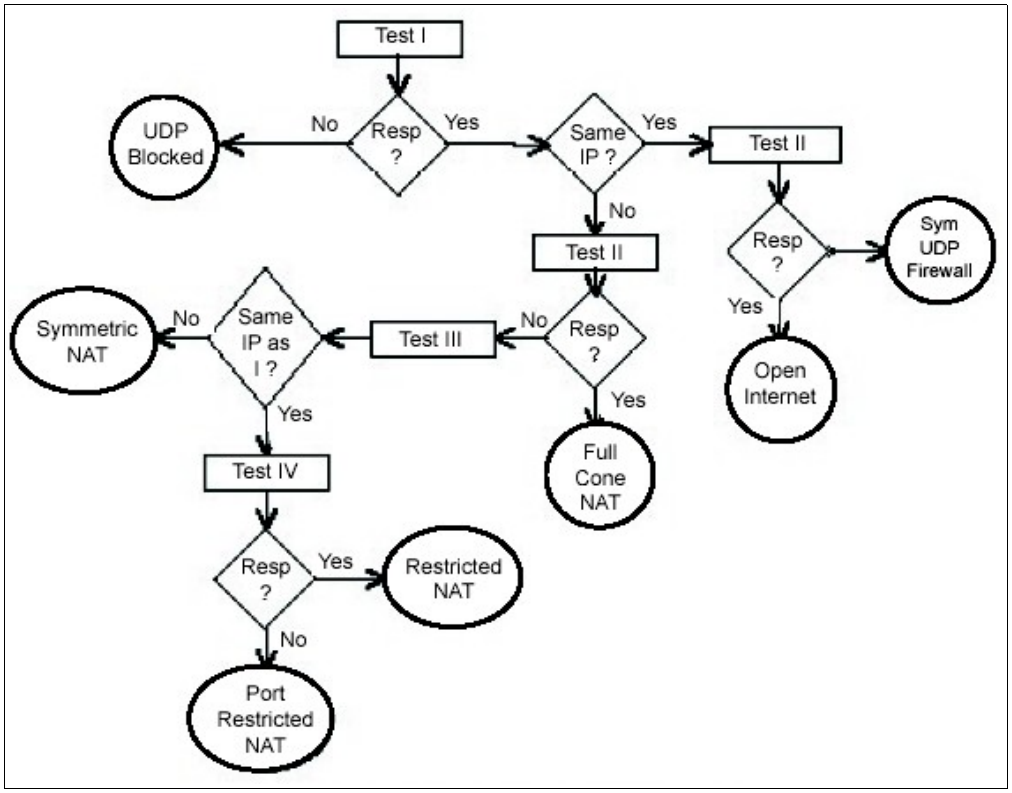
SDP:n kohdalla NAT-käännökset aiheuttavat ongelmia, koska SDP:n avulla neuvotellaan muiden median kuljettamiseen liittyvien asetusten lisäksi istuntoihin osallistuvien tahojen yhteystiedot. Ilman NAT-tunnistusta päätelaitteen muodostamaan SDP-viestiin sisältyy täten yksityinen IP-osoite (ks. esim. tietue edellä kohdassa 3), eikä SDP:n neuvottelema media pääse milloinkaan oikeaan kohteeseensa.

RTP-liikenteen läpimenoa estää sekä NAT että palomuurit. Yksityisen ja julkisen IP-osoitteen problematiikka signaloinnissa on sama kuin SIP-signaloinnin osalta ja läheisesti sidoksissa myös SDP-sanomissa välitettäviin tietueisiin. RTP käyttää yleensä korkeita tietoliikenneportteja väliltä `30000` – `60000`, mikä asettaa vaatimuksia palomuurin konfiguraatiolle. Palomuureissa ns. yläportit ovat poikkeuksetta suljettuja.

Yleisesti ottaen tämän päivän toteutuksissa palomuurit ovat huomattavasti suurempi ongelmien aiheuttaja kuin NAT:it.

8. Palomuurien ja NAT:in aiheuttamien ongelmien ratkaisumahdollisuuksia

Niin kauan kun käytössä ei ole symmetrinen NAT-käännös, voidaan signaloinnin kohtaamia ongelmia ohittaa käyttämällä esimerkiksi STUN-protokollaa [15]. STUN-protokollalla päätelaite voi selvittää edessään olevan NAT-osoitekäännöksen tyypin ja saamansa vastineen perusteella kirjoittaa oikein IP-osoitetietonsa. Useimmat tällä hetkellä markkinoilla olevat SIP-puhelimet tukevat STUN-protokollaa. Kuten kohdassa 7 mainittiin, STUN-toteutusten käyttö on viime aikoina vähentynyt sen toiminta- ja skaalautuvuusongelmien takia. STUN:illa ei yksinkertaisesti olla pystytty vastaamaan niihin monimutkaisiin päätelaite-, välityspalvelin-, ja NAT-ympäristöihin, joista yleisimmät SIP-järjestelmät muodostuvat. Kuvassa 4 on esitetty STUN-kyselyn toimintalogiikka.



Kuva 4: NAT-osoitekäännöstyypin selvittäminen [16].

Jos käytössä on symmetrinen NAT-osoitekäännös (ja käytännön toteutuksissa monimutkaisen STUN-ympäristön välttämiseksi) jää ainoaksi mahdollisuudeksi käyttää älykästä SIP-proxyä signaloinnissa, sekä erillistä RTP-välityspalvelinta, joka hoitaa RTP-liikenteen välittämisen istunnon osapuolien välillä. Yksi mahdollisuus tällaiseksi välityspalvelimeksi on MediaProxy [16, esim.]. Älykäs SIP-proxy tarkoittaa käytännössä sellaista SIP-proxyllä toimivaa rekisteröintipalvelua, jossa päätelaitteen IP-kontaktitiedoksi ei merkitä laitteen itsensä SIP-signaloinnissa välittämää informaatiota (yksityinen IP-osoite), vaan tallennetaan tietokantaan se nimenomainen IP-osoite ja portti (julkinen), josta päätelaitteen REGISTER-viesti saatiin. Tämän jälkeen riittää

yleensä se, että päätelaite konfiguroidaan lähettämään uudelleenrekisteröintisanomia (tai ns. Dummy NOTIFY-viestejä) tarpeeksi lyhyin väliajoin, jolloin alkuperäinen NAT-käännös pysyy voimassa.

Koska välityspalvelin käsittelee päätelaitteen kontaktitietoa erillisenä omana tietueenaan, päätelaite luulee silti keskustelevansa välityspalvelimen kanssa omalla ei-julkisella osoitteellaan, eikä sen toiminta siten häiriinny. Olennaista on päätelaitteen kyky lähettää ja vastaanottaa paketteja saman tietoliikenneportin kautta. Tätä ominaisuutta kutsutaan symmetriseksi signaloinniksi, ja se on käytössä useimmissa saatavilla olevissa päätelaitteissa ja ohjelmistoissa. Symmetrisen signaloinnin toteuttamisen voidaan katsoa olevan pakollinen ominaisuus päätelaitteelle, sillä ainoastaan tämän ominaisuuden avulla voidaan käyttää SIP-välityspalvelimen ja päätelaitteen yhteistoimintaa NAT:in ohittamiseksi.

Ympäristö, joka koostuu edellä mainituista osista, pystyy varmistamaan päätelaitteiden esteettömän toiminnan NAT-käännösten takaa useimmissa tapauksissa. Kun NAT:in aiheuttamat ongelmat on hoidettu, on enää jäljellä palomuurin konfigurointi. Mikäli käytetään MediaProxyä staattisesti kaikille yhteyksille, tarvitsee palomuuriin konfiguroida enää pääsy MediaProxyn IP-osoitteelle, sekä sen käyttämälle RTP-porttiavaruudelle. Jos kuitenkin kaikki RTP-liikenne kierrätetään yhden pisteen kautta, aiheutuu siitä helposti suorituskykyongelmia (MediaProxy on PC-palvelin, usein vielä samalla laitealustalla kuin SIP-proxy itse). Mittausten mukaan nyky-kellotaajuuksilla yksi palvelinkone voisi välittää jopa satojen yhtäaikaisten istuntojen RTP-mediaa [18], mutta tästä huolimatta kaiken median kierrättäminen MediaProxy:n läpi on huono lähtökohta SIP-ymäristön suunnittelulle.

Mikäli SIP-ympäristössä päätelaitteiden käytössä on sekä julkisia että NAT-käännettyjä lähdeosoitteita, on SIP-proxyssä syytä suorittaa NAT-testi päätelaitteen tekemän INVITE-sanoman yhteydessä. Mikäli voidaan päätellä, että jokin päätelaite ei ole NAT:in takana, ei sen RTP-liikennettä ole myöskään syytä kierrättää MediaProxyn kautta. Tällöin jäljelle jää ongelma, että palomuurin konfiguraatiossa täytyy ottaa huomioon päätelaitteet, jotka liikennöivät itsenäisesti. Tällaisessa tapauksessa kysymykseen tulee joko IP-osoite- tai aliverkkokohtaisesti avattava RTP-porttiavaruus.

Lopuksi vielä huomio ns. älykkäistä NAT-toteutuksista. Nämä ovat yleensä laitteita, jotka pyrkivät tunnistamaan NAT:in takana olevien päätelaitteiden käyttämät sovellukset, joiden toimintaa osoitekäännös mahdollisesti estää (tässä tapauksessa SIP). Valitettavan usein tilanne on kuitenkin se, että ongelmien ratkaisemisen sijaan älykkäät NAT:it tuovat niitä lisää. Usein älykkäät NAT-toteutukset laitteissa ovat vielä sellaisia, että toiminnallisuutta ei voi erikseen kytkeä pois päältä. Tällöin ainoa mahdollisuus ohittaa älykkyys on konfiguroida päätelaitteet käyttämään SIP-signalointiporttinaan muuta kuin `5060`:aa. Tällä yksinkertaisella muutoksella voidaan ohittaa suurin osa (pseudo)älykkäistä NAT:eista, sillä ne eivät yleensä tutki tietoliikennepakettien sisältöä, vaan tunnistavat esim. SIP-signaloinnin ainoastaan käytetystä oletusportista (`5060`).

9. Lähteet

[1] Rosenberg et al: “SIP: Session Initiation Protocol”, 2002.

[2] A. B. Roach: “Session Initiation Protocol (SIP)-Specific Event Notification”, 2002.

[3] J. Peterson: “S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)”, 2004

[4] Franzens et al: “IP Telephony Cookbook”, 2004

[5] M.Handley, Eve Schooler: “Session Initiation Protocol”, 1996

[6] M. Handley, V. Jacobson: “SDP: Session Description Protocol”, 1998

[7] Olson et al: “Support for IPv6 in Session Description Protocol (SDP)”, 2002

[8] SDP: Session Description Protocol, http://www.javvin.com/protocolSDP.html

[9] Schulzrinne et al: “RTP: A Transport Protocol for Real-Time Applications”, 2003

[10] Schulzrinne et al: “RTP Profile for Audio and Video Conferences with Minimal Control”, 2003

[11] RTP: Real-Time Transport Protocol: http://www.javvin.com/protocolRTP.html

[13] Staful Inspection, ks. esim. http://www.checkpoint.com/products/technologies/stateful_inspect.html

[12] P. Srisuresh, K. Egevang: “Traditional IP Network Address Translator”, 2001

[14] Cisco Systems: “Using PIX Firewall”, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/overvw.htm

[15] Rosenberg et al: “STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)”, 2003

[16] DeltaThree: “NAT Traversal In SIP', http://corp.deltathree.com/technology/networkaddress.asp

[17] MediaProxy, http://www.ag-projects.com/MediaProxy.html

[18] MediaProxy-suorituskyky, ks. esim. http://mediaproxy.ag-projects.com/INSTALL

10. Käsitteet ja lyhenteet

DMZ	Demilitarized Zone
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
OMA	Open Mobile Alliance
PAT	Port Address Translation
PoC	Push to talk over Cellular
RFC	Request For Comments
RTCP	Realtime Transport Control Protocol
RTP	Realtime Transport Protocol
SIP	Session Initiation Protocol
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
NAT	Network Address Translation
VPN	Virtual Private Network