VoIP biztonság

BME - TMIT
Médiabiztonság
feher.gabor@tmit.bme.hu

VoIP támadások

- Támadás a VoIP szoftveren keresztül
  - OS támadása
    - Windows és Linux/UNIX alapok - szerverek
    - Hardphone hibák
  - Konfigurációs hibák kihasználása
    - Gyenge jelszavak
    - SNMP hozzáférés
    - TFTP boot

    - VOMIT: voice over misconfigured internet telephones
- Támadás a VoIP hálózaton keresztül
  - Layer 2 támadások
    - ARP támadás – Gratuitous ARP -> MiM
    - DHCP támadás (rouge DHCP, DHCP starvation)
  - Layer3 támadások
    - DDoS
    - TCP/UDP támadások
  - Lehallgatás

VoIP támadások 2.

- Támadás VoIP protokollon keresztül
  - Nem specifikált működés
  - DoS
    - Hamisított SIP – H.323 üzenetek
      - CANCEL vagy BYE
    - ICMP port unreachable üzenet küldése
  - Hívásrablás
    - SIP üzenet, hogy a másik fél mozog

VoIP telefon tanúsítványok

- Tanúsítványok (Cisco)
  - Certificate Trust List (CTL)
    - A megbízható kiszolgálók tanúsítványának listája
      - Identity, PK, role
    - Boot idején töltődik le. (tyúk-tojás)
    - Az adminisztrátor írja alá
      - Saját PKI
      - Cisco aláírás eToken segítségével
  - A telefon is azonosítja magát
    - MIC (7970): Manufacturing Installed Certificate (Cisco root CA)
    - LSC (7960/7940): Locally Significant Certificate
      - CAPF által telepített
      - Jelszó, pin kód

VoIP telefon védelem

- Firmware védelme (Cisco)
  - A firmware boot idején töltődhet le. A firmware-t a tftp szerver szolgáltatja.
  - Hitelesített firmware
    - A firmware a Cisco-tól származik (Cisco root aláírás)
    - Egy adott verziótól már csak ezt lehet használni
- Konfiguráció védelme (Cisco)
  - Konfiguráció hitelesítése
    - Tanúsítványok használata
  - TLS védett kapcsolatok
    - CCM: Cisco Call Manager (most Unity)
    - CAPF: Certificate Authority Proxy Function

VoIP hálózat védelem

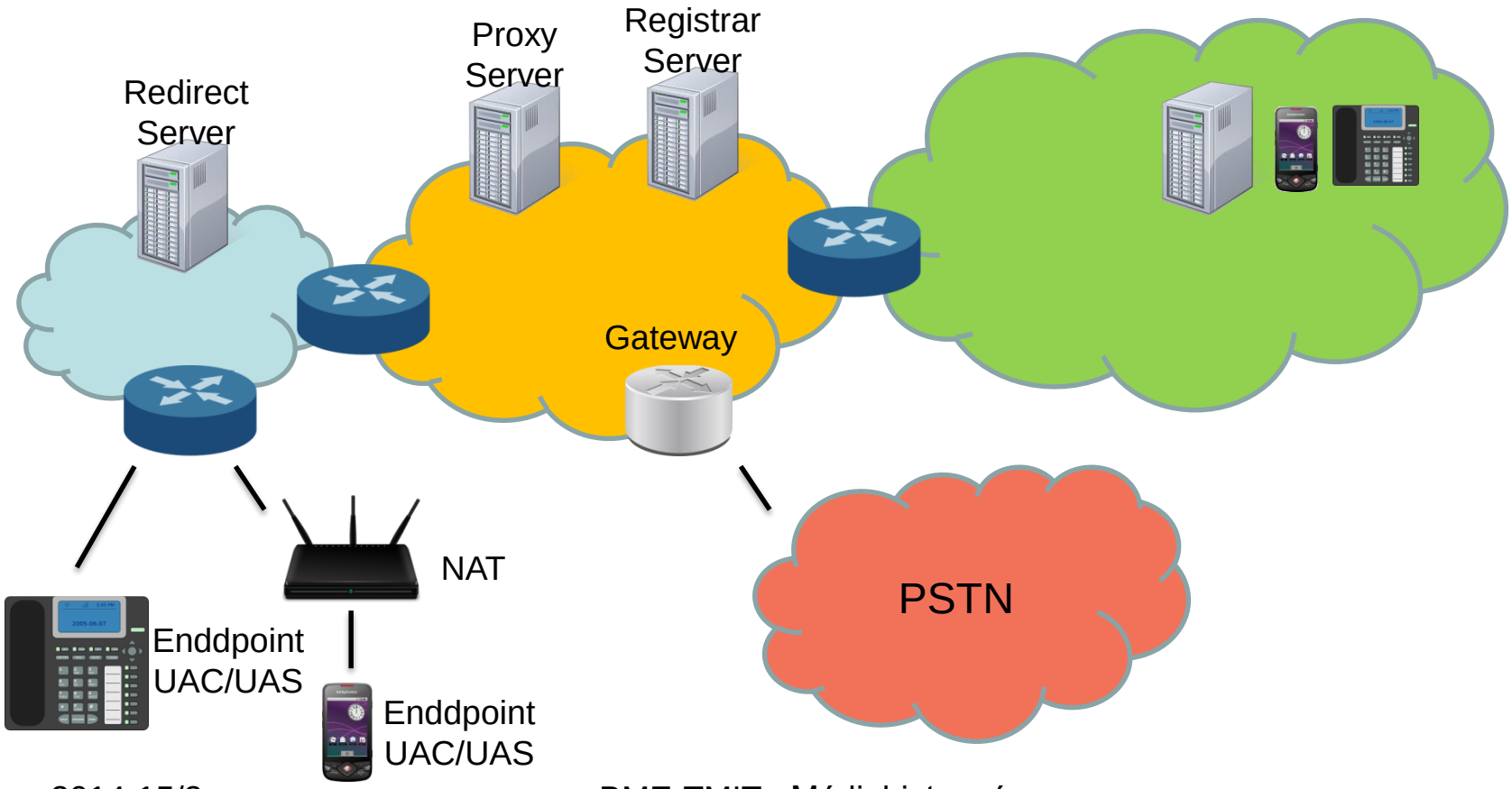
- Layer 2
  - MAC flooding (lehallgatás): MAC limit, 802.1X
  - Rouge DHCP, starvation:
    - DHCP snooping: Kliens proton nincs DHCP szerver (uplink is lehet megbízható)
    - DHCP starvation: DHCP limit, 802.1X
    - A DHCP szervernek közel kell lennie a kliensekhez
  - Gratuitous ARP:
    - Dynamic ARP inspection: Minden nem DHCP által rendelt MAC:IP páros blokkolása (IP is: IP Source Guard)
    - Ignore Gratuitous ARP: A telefon nem frissíti az ARP cache-t
  - VLAN
    - Hang és adat LAN elválasztása
- Layer 3
  - Tűzfalak alkalmazása
    - Alkalmazás proxy a VoIP protokoll értelmezésével
      - Médiafolyamok számára az UDP csatornák felnyitása és zárása
    - Titkosított adatok???
  - DoS
    - Egyidejű kérések számának maximálása (rate limit)

VoIP forgalom védelme

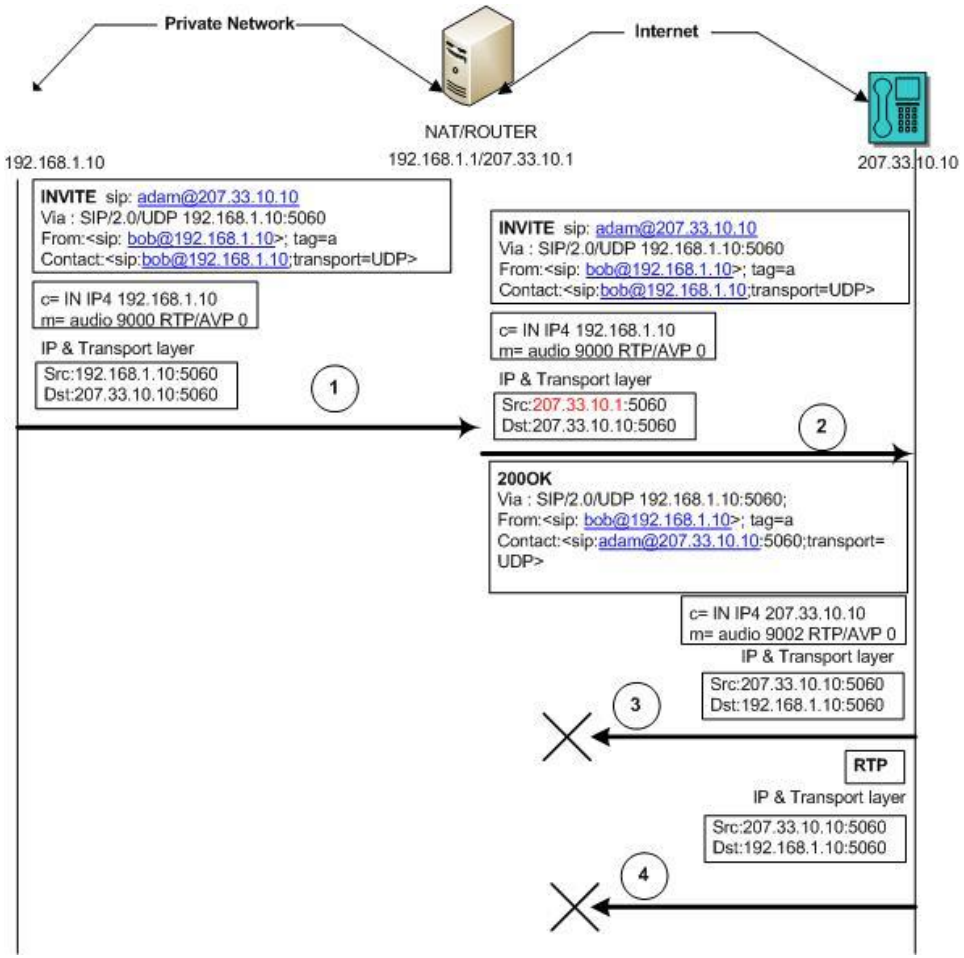
- Hangátvitel védelme
  - Tartalom titkosítás
    - Egyedi algoritmusok
  - IPSec, DTLS – Datagram Transport Layer Security
    - DTLS esetén meg kell oldani az újraküldéseket, időzítéseket, mivel UDP felett megy
  - SRTP
    - MIKEY (DH is), SDescription, ZRTP, (DTLS-SRTP)

Session Initiation Protocol

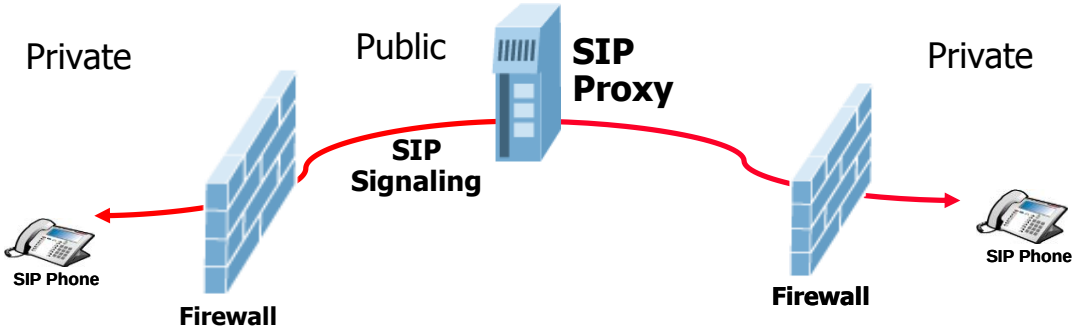
- Alapelemek



SIP és NAT


Private Network
Internet
NAT/ROUTER
192.168.1.1/207.33.10.1
192.168.1.10
207.33.10.10
INVITE sip: adam@207.33.10.10
Via : SIP/2.0/UDP 192.168.1.10:5060
From:<sip: bob@192.168.1.10>; tag=a
Contact:<sip:bob@192.168.1.10;transport=UDP>
c= IN IP4 192.168.1.10
m= audio 9000 RTP/AVP 0
IP & Transport layer
Src:192.168.1.10:5060
Dst:207.33.10.10:5060
1
INVITE sip: adam@207.33.10.10
Via : SIP/2.0/UDP 192.168.1.10:5060
From:<sip: bob@192.168.1.10>; tag=a
Contact:<sip:bob@192.168.1.10;transport=UDP>
c= IN IP4 192.168.1.10
m= audio 9000 RTP/AVP 0
IP & Transport layer
Src:207.33.10.1:5060
Dst:207.33.10.10:5060
2
200OK
Via : SIP/2.0/UDP 192.168.1.10:5060;
From:<sip: bob@192.168.1.10>; tag=a
Contact:<sip:adam@207.33.10.10:5060;transport=
UDP>
c= IN IP4 207.33.10.10
m= audio 9002 RTP/AVP 0
IP & Transport layer
Src:207.33.10.10:5060
Dst:192.168.1.10:5060
3
RTP
IP & Transport layer
Src:207.33.10.10:5060
Dst:192.168.1.10:5060
4

VoIP és Firewall/NAT

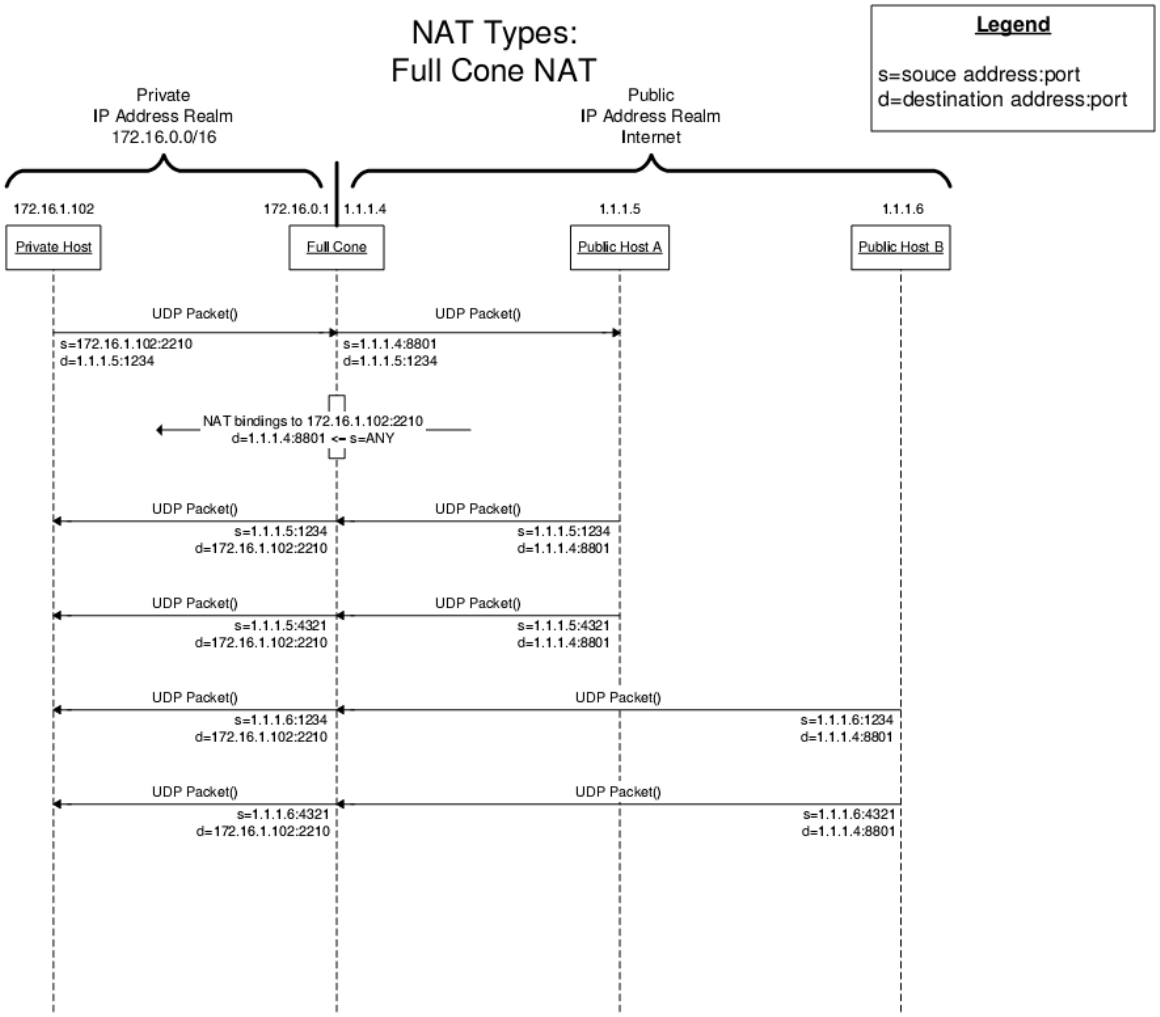


- Jelzés probléma
  - A SIP proxy nem tud kommunikálni a kliensekkel
  - A felnyitott portok ha nincs forgalom, akkor megszűnnek
- Média probléma
  - A SIP INVITE –ban küldött cím csak lokális
  - SDP nem tudja leírni a médiaforgalom címét
  - Az inicializálásnak a privát -> publikus irányba kell történnie
  - RTCP = RTP + 1
  - A felnyitott portok ha nincs forgalom, akkor megszűnnek

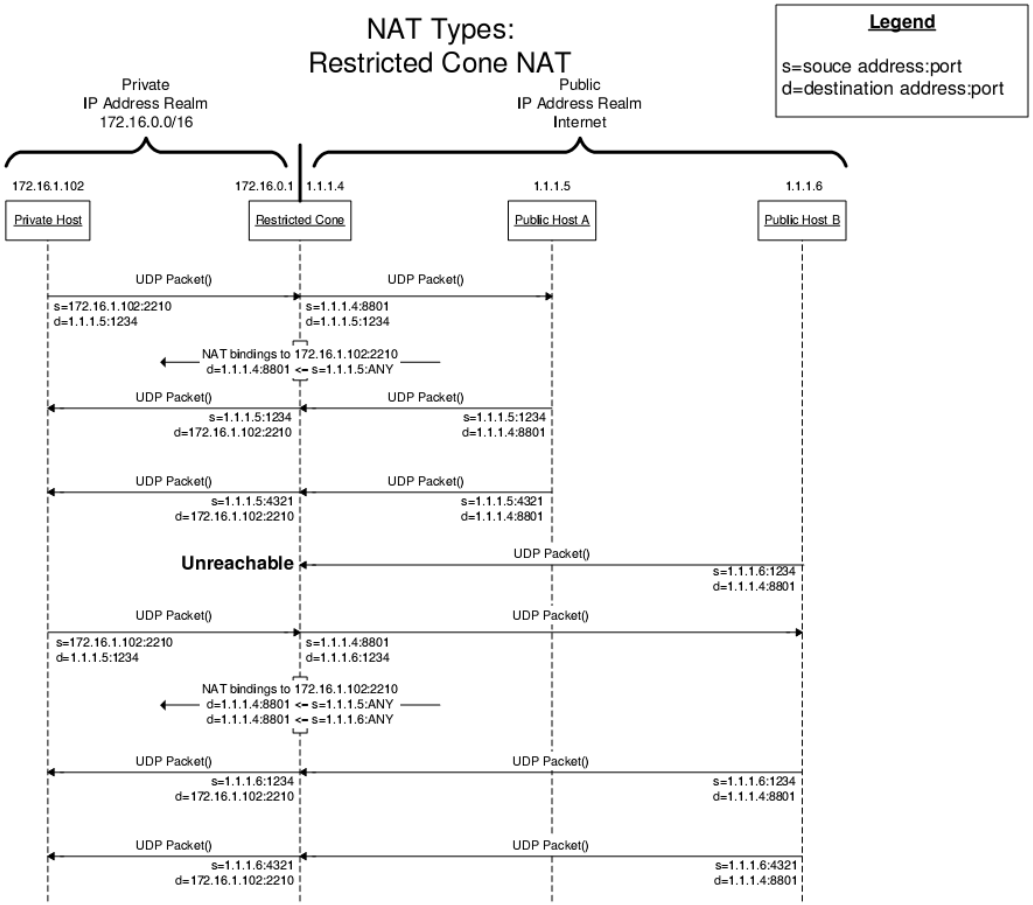
NAT

- Full Cone NAT
  - A belső cím:port 1:1 –ben külső cím:port –ra irányítva
  - Visszafelé irányban is így működik, tetszőleges küldő/port lehet
- Restricted Cone NAT
  - Hasonló a Full Cone –hoz, de visszafelé irányban az IP cím korlátozva van az eredeti címzettre (a port nem)
- Port Restricted Cone NAT
  - Hasonló a Rescrited Cone –hoz, de a port is korlátozva van az eredetileg megcímzett portra.
- Symmetric NAT
  - Hasonló a Port Restricted Cone –hoz, de itt minden új kapcsolathoz új külső IP:port lesz rendelve

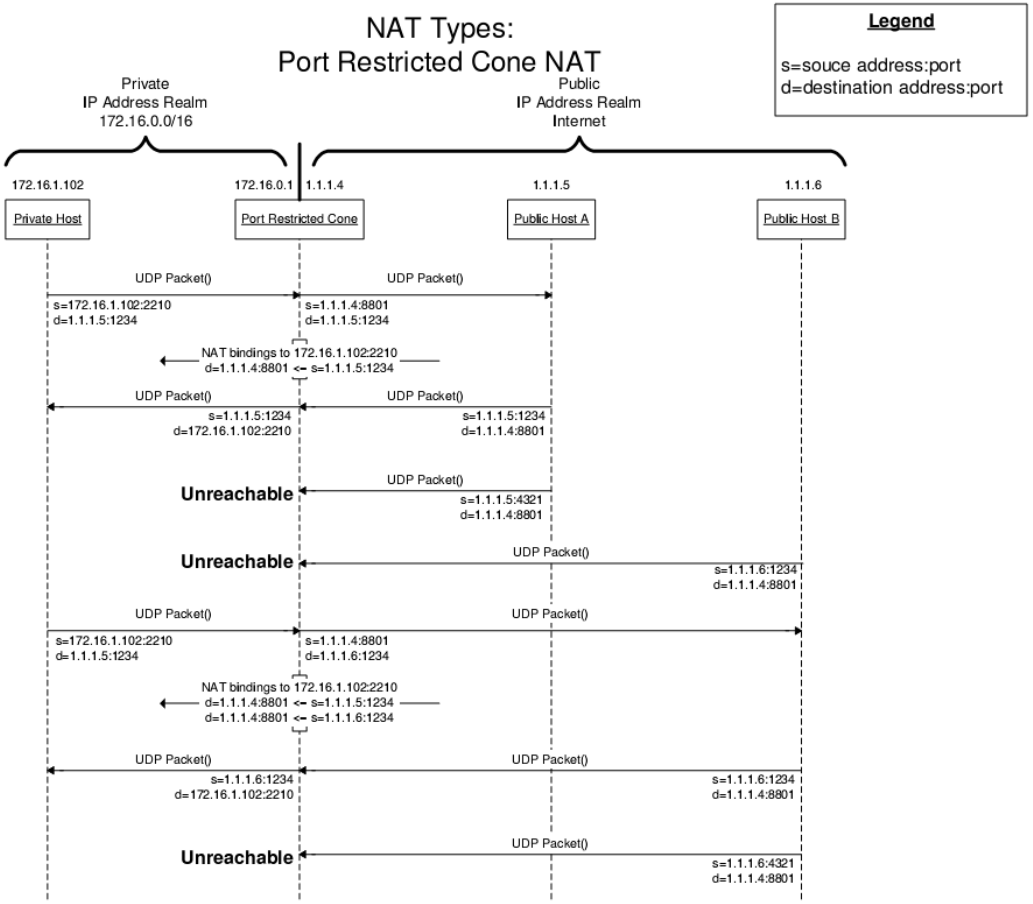
Full cone


NAT Types:
Full Cone NAT
Legend
s=souce address:port
d=destination address:port
Private
IP Address Realm
172.16.0.0/16
Public
IP Address Realm
Internet
172.16.1.102
172.16.0.1
1.1.1.4
1.1.1.5
1.1.1.6
Private Host
Full Cone
Public Host A
Public Host B
UDP Packet()
s=172.16.1.102:2210
d=1.1.1.5:1234
UDP Packet()
s=1.1.1.4:8801
d=1.1.1.5:1234
NAT bindings to 172.16.1.102:2210
d=1.1.1.4:8801 <- s=ANY
UDP Packet()
s=1.1.1.5:1234
d=172.16.1.102:2210
UDP Packet()
s=1.1.1.5:1234
d=1.1.1.4:8801
UDP Packet()
s=1.1.1.5:4321
d=172.16.1.102:2210
UDP Packet()
s=1.1.1.5:4321
d=1.1.1.4:8801
UDP Packet()
s=1.1.1.6:1234
d=172.16.1.102:2210
UDP Packet()
s=1.1.1.6:1234
d=1.1.1.4:8801
UDP Packet()
s=1.1.1.6:4321
d=172.16.1.102:2210
UDP Packet()
s=1.1.1.6:4321
d=1.1.1.4:8801

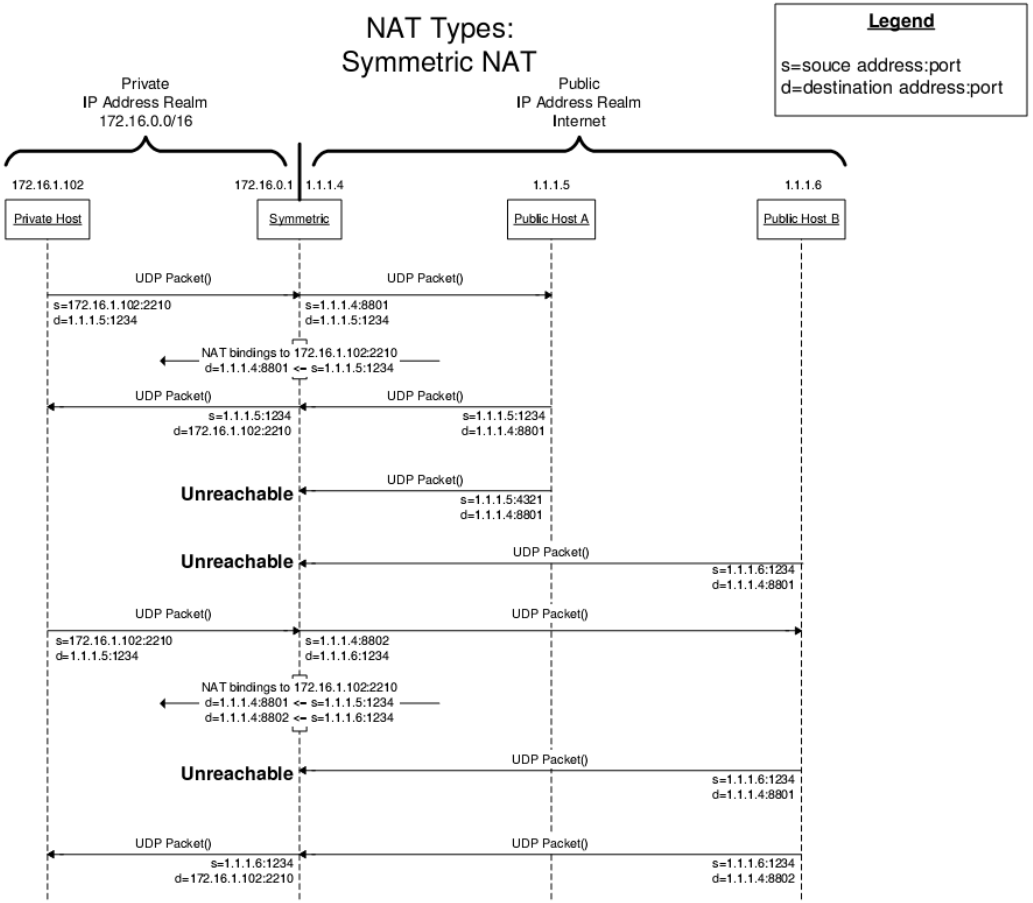
Restricted cone



Port restricted cone



Symmetric NAT



NAT/Tűzfal átjárás

- A hívó fél nem ismeri a saját publikus címét
  - Esetleg nem tudja, hogy NAT mögött van
- A hívott felet nem érik el a jelzésüzenetek/médiaforgalom

- Dedikált jelzésport
  - SIP: 5060
- Szimmetrikus RTP
  - A küldésre/vételre használt port megegyezik

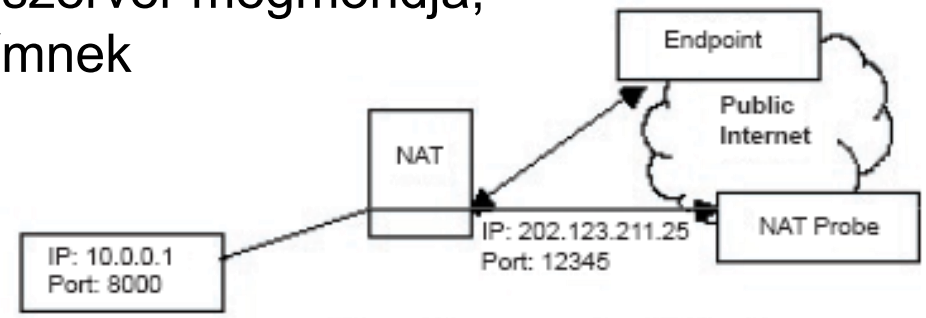
IGD

- Internet Gateway Device (IGD) Protocol
  - UPnP fórum
- Képességek
  - Külső cím megmutatása
  - Portok felsorolása, új port nyitás, zárás
    - Kérésre nyit egy portot, amin be lehet jönni
- Problémák
  - Nem minden NAT és OS támogatja
  - Feltételezzük, hogy a lokális hálózat biztonságos
    - Nem feltételezhető!
- Léteznek hasonló protokollok is
  - Realm-Specific IP (RSIP), Middlebox Communications (MIDCOM), NAT Port Mapping Protocol (NAT PMP)

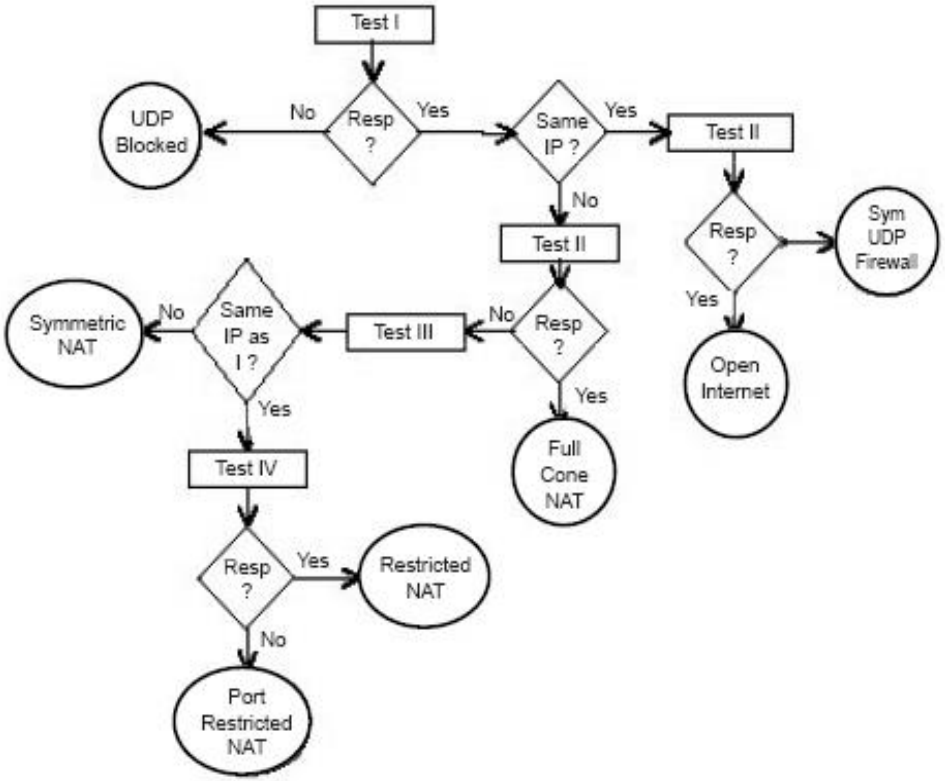
STUN

- Simple Traversal of UDP Through NATs

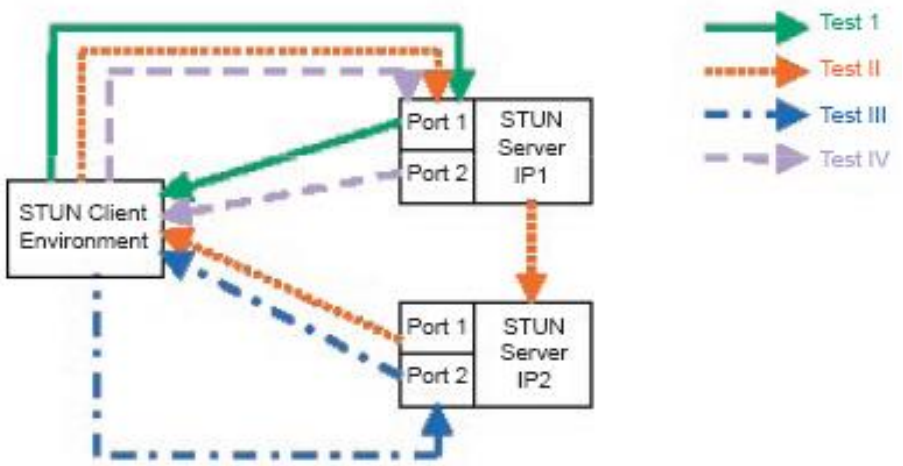
- A VoIP kliensnek tudnia kellene a saját NAT címét! (+port)
  - NAT Probe: A külső cím lekérdezése
    - Egy külső, publikus szerver megmondja, hogy mit lát küldő címnek



STUN felderítés



Test	Destination	Change IP	Change Port	Return IP:port
Test I	*IP1:1*	*N*	*N*	*IP1:1*
Test II	*IP1:1*	*Y*	*Y*	*IP2:2*
Test III	*IP2:1*	*N*	*N*	*IP2:1*
Test IV	*IP1:1*	*N*	*Y*	*IP1:2*



STUN és VoIP

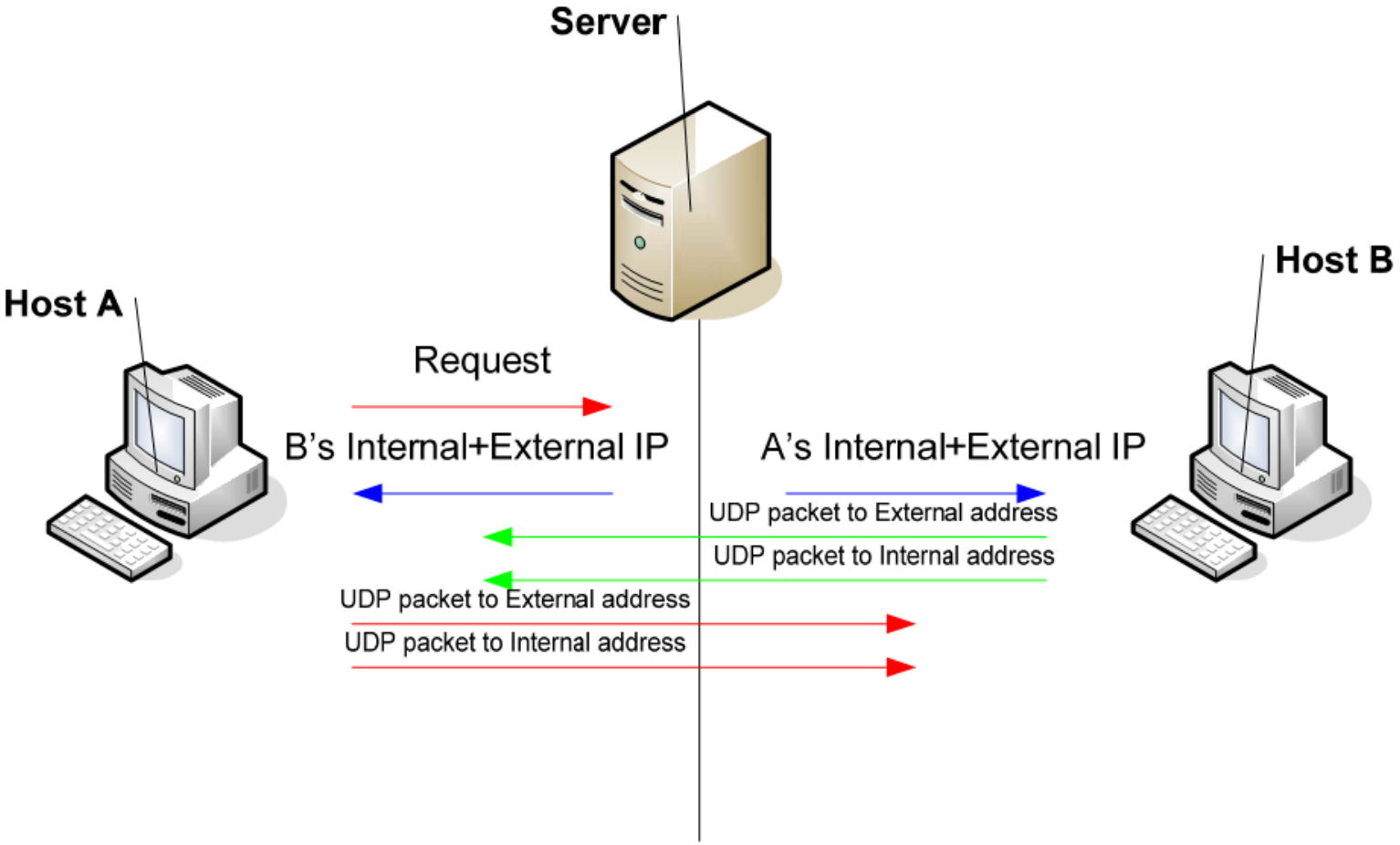
- Hívásfelépítés előtt STUN teszt ugyanarról a cím:port –ról, mint ahonnan a kapcsolat fel fog épülni.
  - Megtudom a szükséges IP címeket/portokat
  - Megtudom a NAT típusát

- Feltételek
  - Szimmetrikus NAT esetén nem működik!
    - A célcím és STUN szerver cím különbözik -> különböző NAT publikus címek a NAT táblában
    - Szerencsére a legtöbb SOHO NAT nem szimmetrikus
  - Működik, ha a VoIP szoftver ugyanazon a porton fogad és küld adatokat
    - A másik féllel a NAT címét kell közölni
    - A NAT probe után hamarosan indítani kell a kommunikációt, nehogy más címre álljon a NAT

UDP hole punching

- Egy külső szerver visszaküldi az IP címeket és portokat (belső és külső is) a kommunikáló feleknek
  - Aktív kapcsolat kell a hoszt és a külső szerver között, amin keresztül a hoszt adatot tud fogadni
  - A felek mindkét címen próbálkoznak
    - NATon belüli és kívüli kapcsolatok is lehetnek
- Amennyiben Full Cone akkor tud működni
- Restricted Cone esetben is működhet, ha elérik egymást a gépek

UDP hole punching

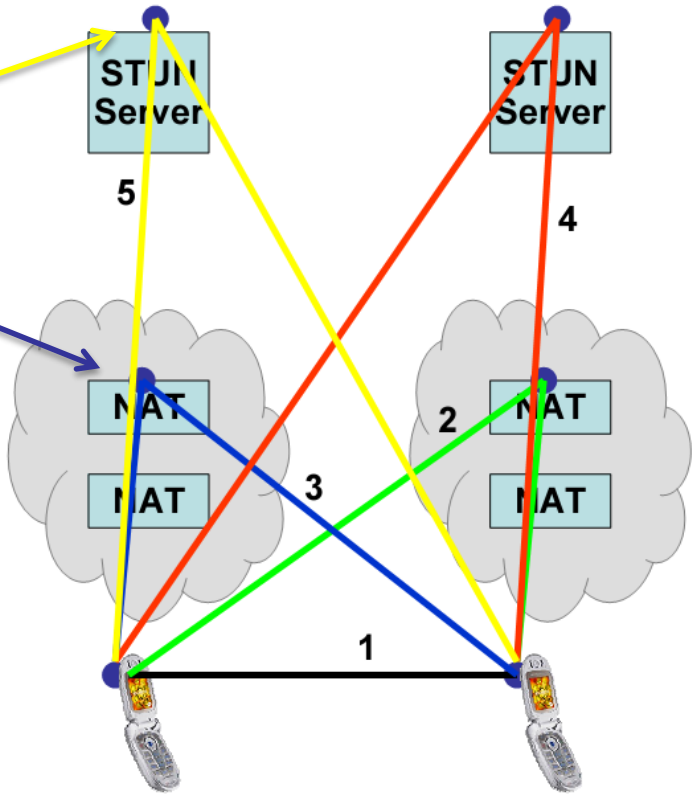


TURN

- Traversal Using Relay NAT
  - Egy külső szerver továbbítja a csomagokat
  - Ehhez mindkét fél csatlakozik, az adatokat ide címzik
    - Mivel mindkét fél eléri a TURN szervert, a visszirányú kapcsolaton megkapják a másik fél által küldött adatokat is
  - Költséges
    - Hosszú utak (idő)
    - Terhelt szerver
    - Csak végső esetben!

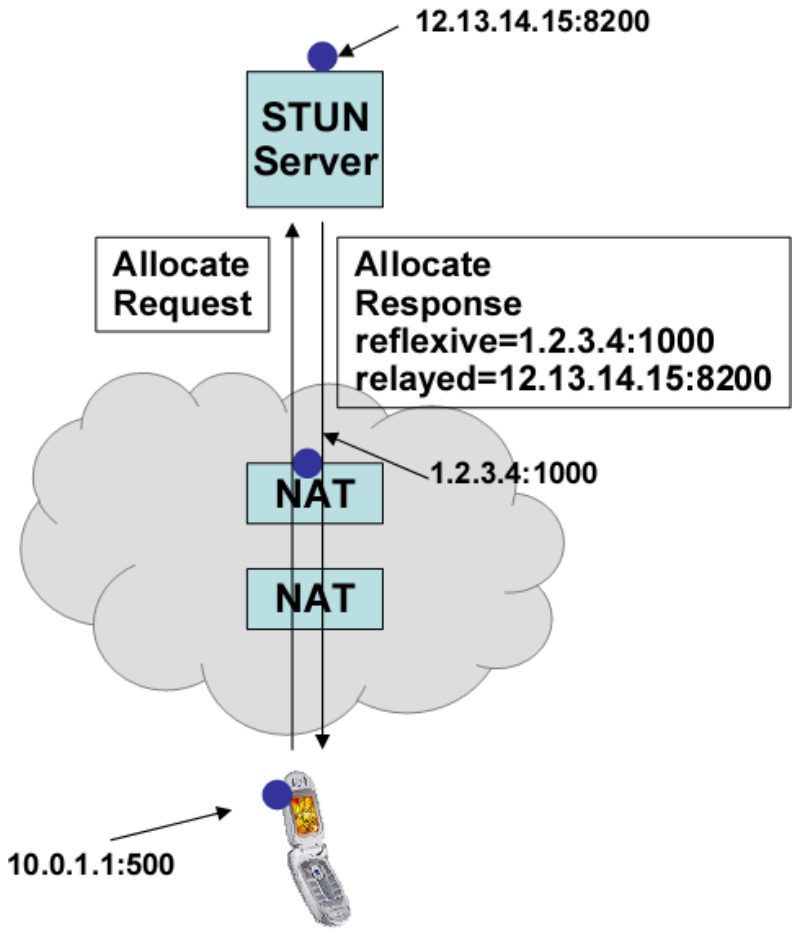
ICE

- Interactive Connectivity Establishment
  - STUN és TURN használata
    - Potenciális IP címek gyűjtése
      - Lokális
      - Server reflexive
      - Realyed
    - Prioritás
  - Kapcsolatépítés előtt a címek tesztelése (STUN)
  - Peer reflexive címek
    - A címek tesztelése közben keletkező új címek (szimmetrikus NAT)
  - A legjobb kapcsolat használata



ICE címgyűjtés

- Relay címhez üzenet
  - Egyben STUN szerver
  - Megmondja a reflexív címet



Session Border Controller - SBC

- A hálózat határain helyezkednek el
  - Biztonságot is nyújt
- Minden forgalom rajta megy keresztül (jelzés + média)
  - Mintha mindkét fél az SBC-n lenne (back-to-back user agent)
  - Átkódolhatja a forgalmat (jelzés + média)
- Titkosítás?

VoIP jelzések védelme

- Titkosított és hitelesített jelzés üzenetek
  - TLS (Pl.: SIPS), DTLS és IPSec
    - PKI-n alapul
    - Széles körben támogatott (TLS és IPSec)
    - De csak szakaszok védelme megoldott!
      - A hangforgalom titkosításához ez kevés lehet
      - A titkosító kulcsot e2e kéne egyeztetni
        - » SDescriptions nem az igazi, itt a kulcs az üzenetben van és a TLS az üzenettel együtt titkosítja
  - S/MIME
    - PKI-n alapul
    - Csak az SDP van titkosítva
    - E2e biztonság a forgalom számára
    - De nincs visszajátszás elleni védelem!
- Nem lehet teljesen e2e titkosítás, mert néhány mezőnek láthatónak kell lennie!
- A SIP proxyk megváltoztathatják az üzeneteket

Hamis SIP üzenetek

- From, via mezők hamisítása

INVITE sip:bob@atlanta.com SIP/2.0
Via: SIP/2.0/UDP evilsite.com
To: Bob sip:bob@atlanta.com
From: Alice <sip:lice@atlanta.com>
Call-ID: ae4356ef781a
Cseq: 100 INVITE
…

SIP Authentication

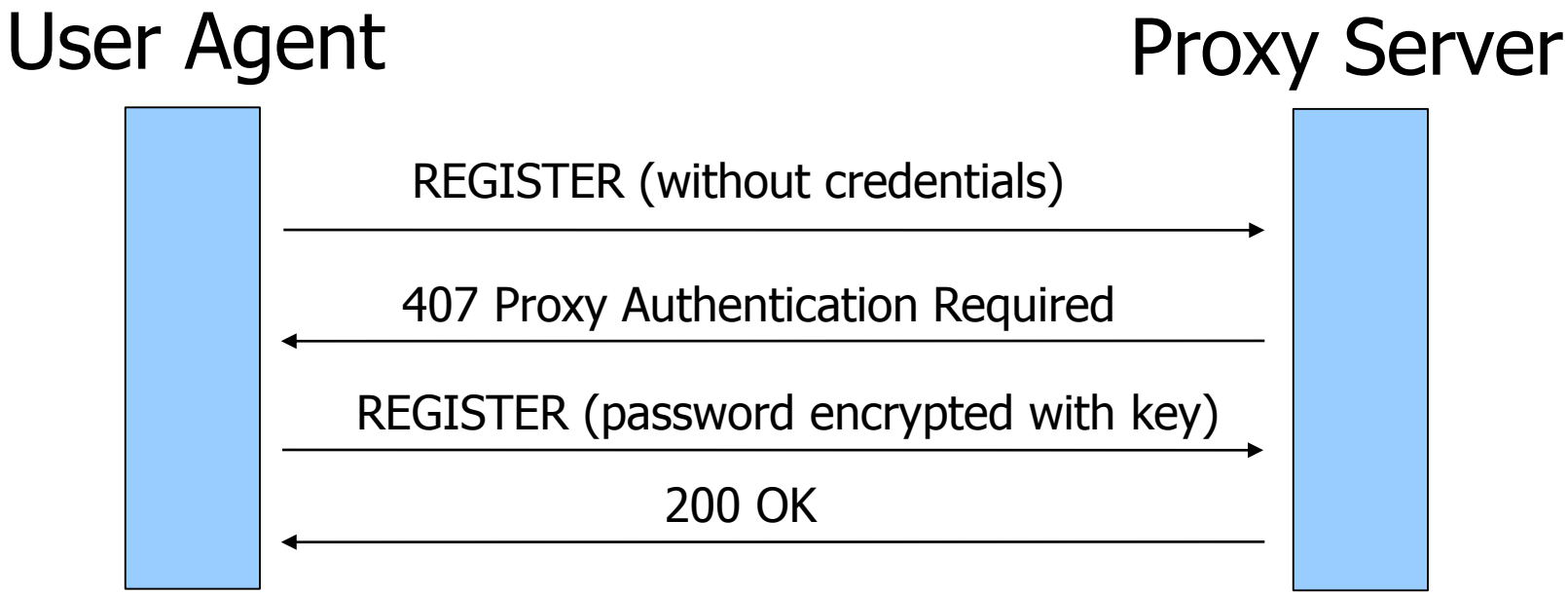
- A felhasználó hitelesítése
  - HTTP digest (RFC 3261)
    - Közös titok a felhasználónál és hitelesítőnél
  - TLS
  - S/MIME

SIP Authentication – HTTP digest

- A proxy szerver kér hitelesítést
  - INVITE vagy REGISTER üzenetnél
  - Kihívás alapú: (tartomány, nonce, hash algoritmus)
    - A kihívás a hitelesítés kéréssel együtt érkezik
    - A felhasználó is küldhet saját nonce értéket
- Csak a kérdés van hitelesítve, más mezőt nem titkosít/hitelesít

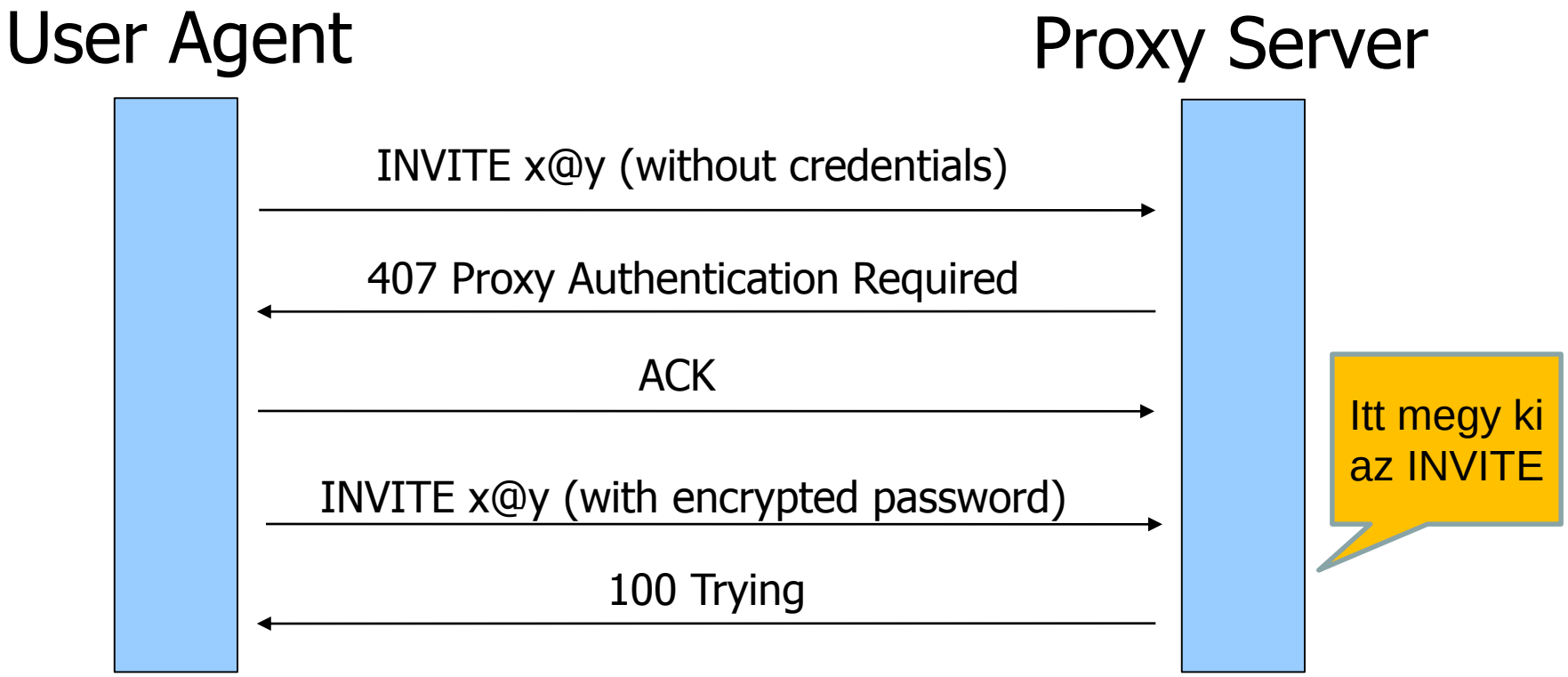
SIP Authentication – HTTP digest 2.

- Regisztrációval



SIP Authentication – HTTP digest 3.

- INVITE üzenetnél



SIPS Authentication

- Hasonlóan a HTTP-HTTPS-hez,TLS használata
- A szerverek egymás között és a távoli végponton is TLS felett alakítanak ki kapcsolatot
  - Elvileg ha nem tud kialakítani kapcsolatot, akkor nem épül fel
- Hop by hop titkosítás

SIP Authentication – S/MIME

- RFC 3261: Az SIP fejléceket megismétli a törzsben, MIME formátumban, titkosítva
  - Digitális aláírással (PKI)
  - Gond, hogy bizonyos mezők megváltozhatnak a továbbító proxyk miatt
    - Nehezen ellenőrizhető, hogy ez legitim vagy támadó változás
- RFC 3893: Authenticated Identity Body (AIB)
  - SIP válasz is használhatja
- PKI miatt gondok lehetnek

SIP Identity

- RFC 4474: Identity + Indetity info fejlécek
  - HTTPS vagy SIPS URI, az identitást lehet ellenőrizni segítségével
  - Csak SIP kérések
  - Digitális aláírással
- Az AIB továbbvitele, így az AIB nincs is elterjedve

P-Asserted-Identity (PAI)

- SIP hálózatban, ahol megbízható az együttműködés
  - A Proxy elhelyezi a felhasználó azonosítóját a továbbított üzenetekben
    - Kivéve, ha az üzenet nem megbízható félnek megy
    - Kivéve, ha a felhasználó annak eltávolítását kéri
  - SIP URI és opcionális *display name*