

TŰZFAL/NAT átjárás

Hogyan megy át a tű fokán a tevé,
ezen fő a napkeleti bölcseknek a feje.

Kalandozás a NAT és a Valósídejű kommunikáció tűzfalátjárásának világában..

Mészáros Mihály

2018.05.04.

TŰZFAL/NAT átjárás

Hogyan megy át a tű fokán a tevé,
ezen fő a napkeleti bölcseknek a feje.

A Tűzfal kívül tartja a nem kívánatos forgalmat..





Cél: Szabványos NAT / Tűzfal-átjárás biztosítás az RTC szolgáltatások számára

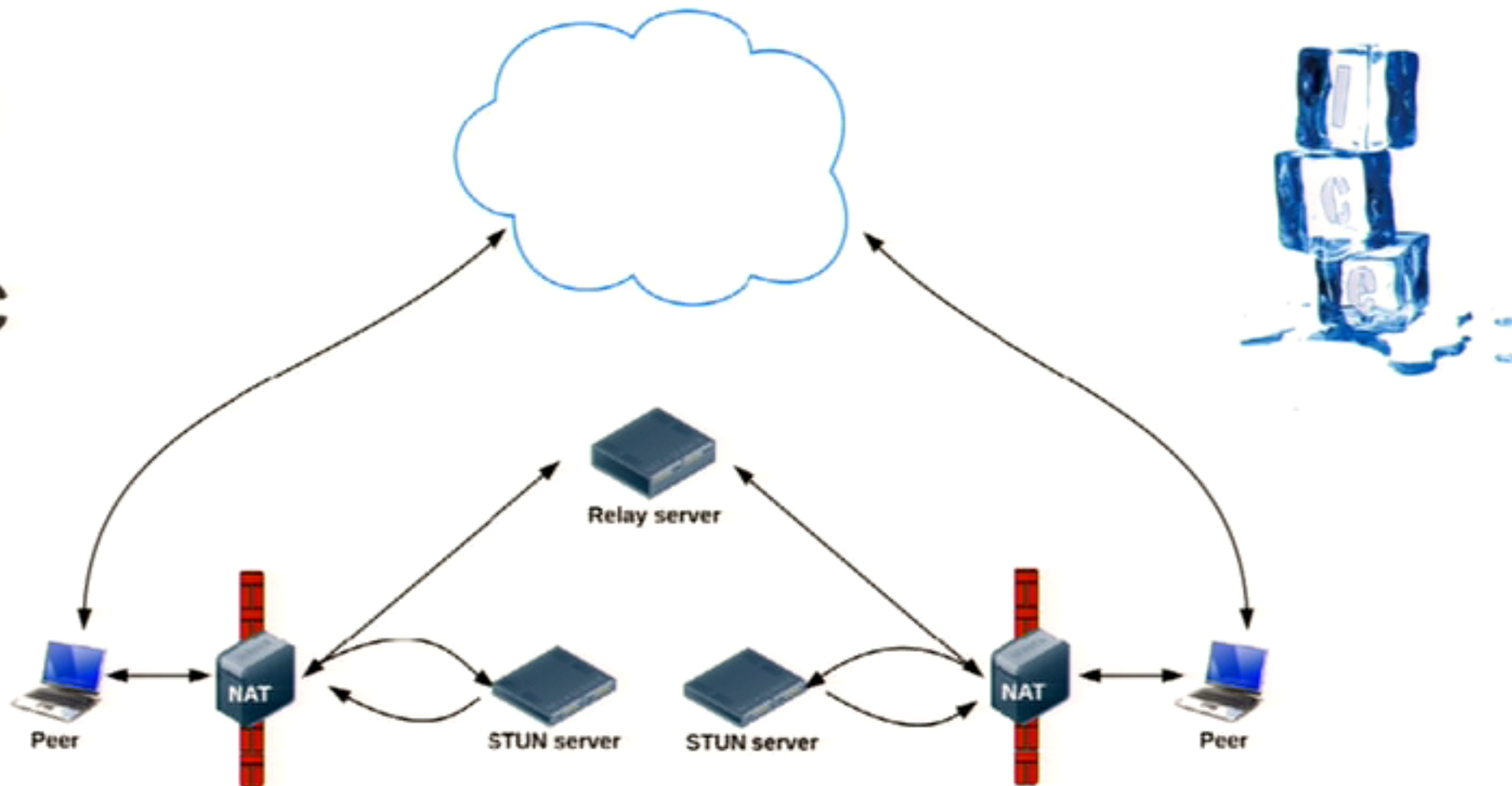


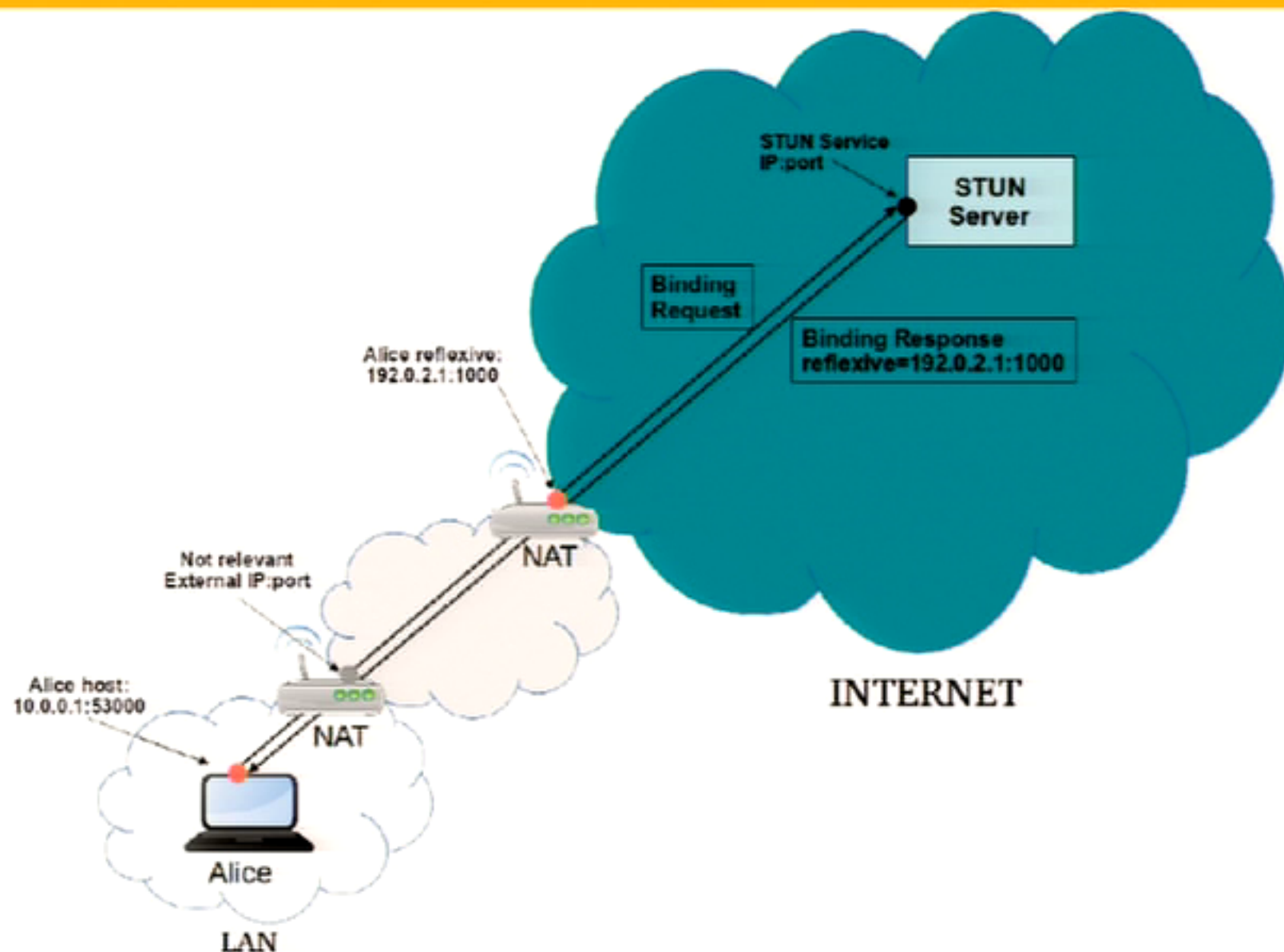
- Miért gond, ha befalazzuk az ajtót és az ablakot?
- Az Internet ma:
 - NAT (különböző fajtái),
 - Tűzfal (csomagszűrés),
 - IPv4 => IPv6 áttérés,
 - Multihomed eszközök, stb.
- TCP nem ideális valós idejű tartalmak számára.

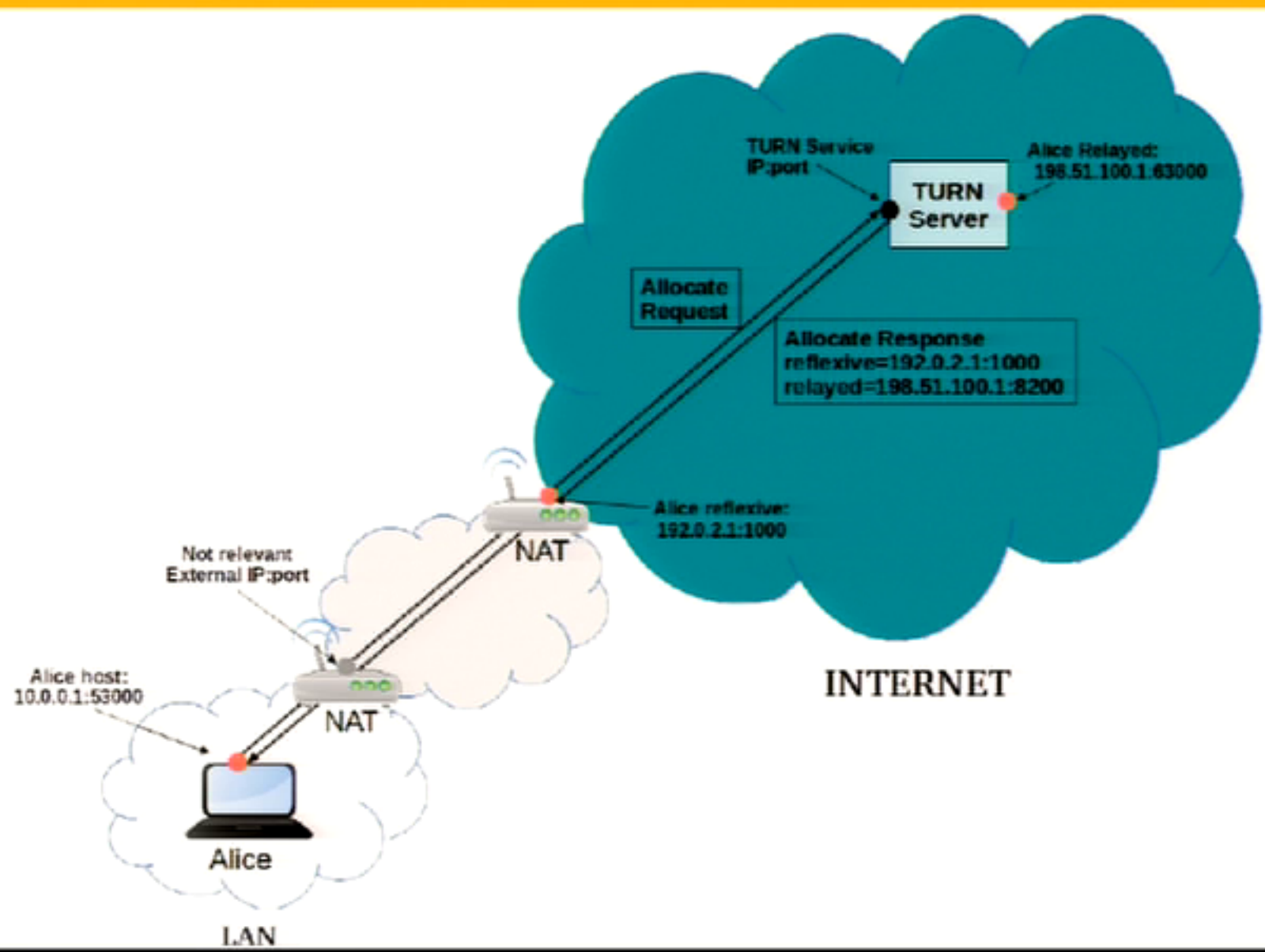


Rés a Pajzson: UDP hole punching



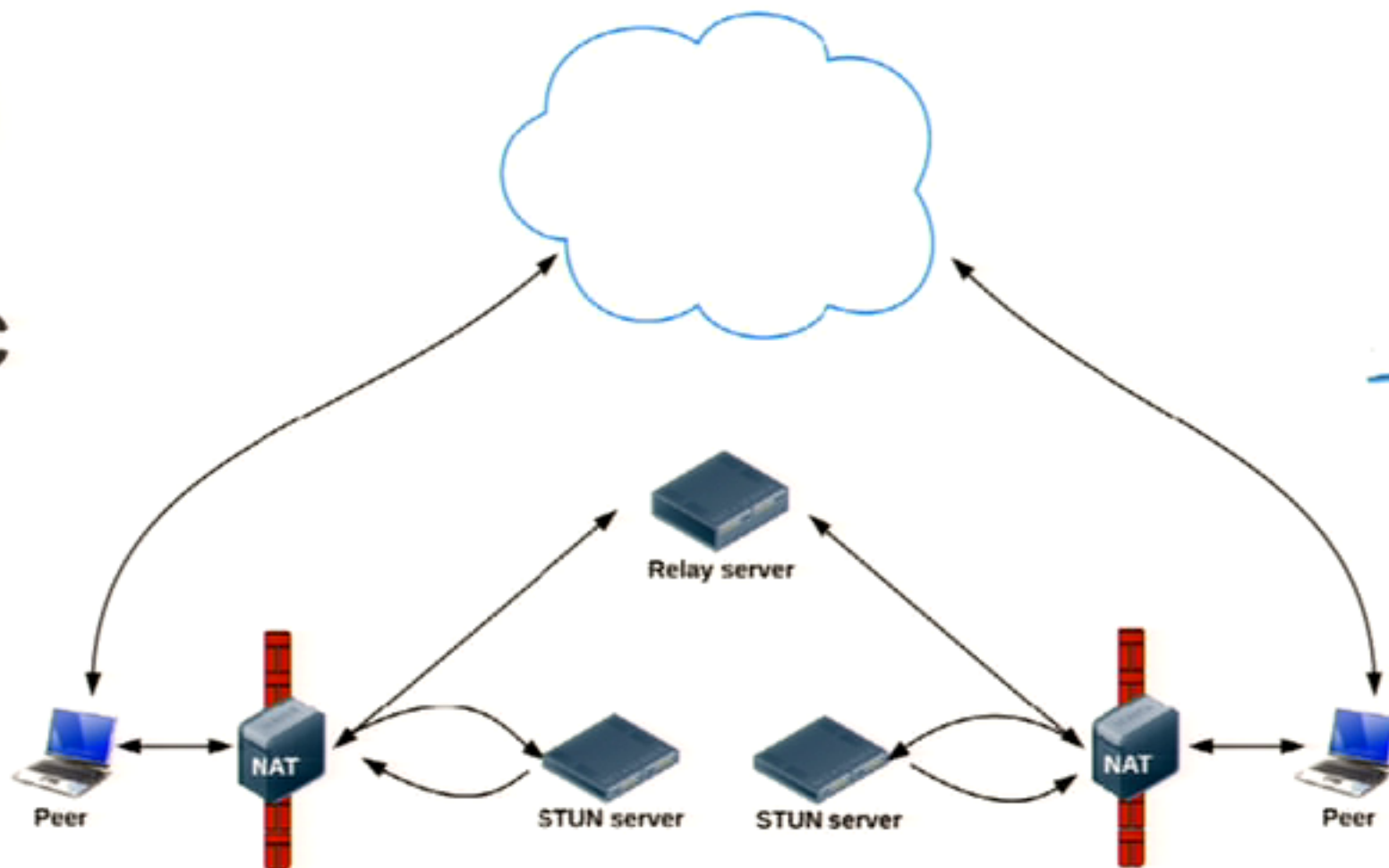




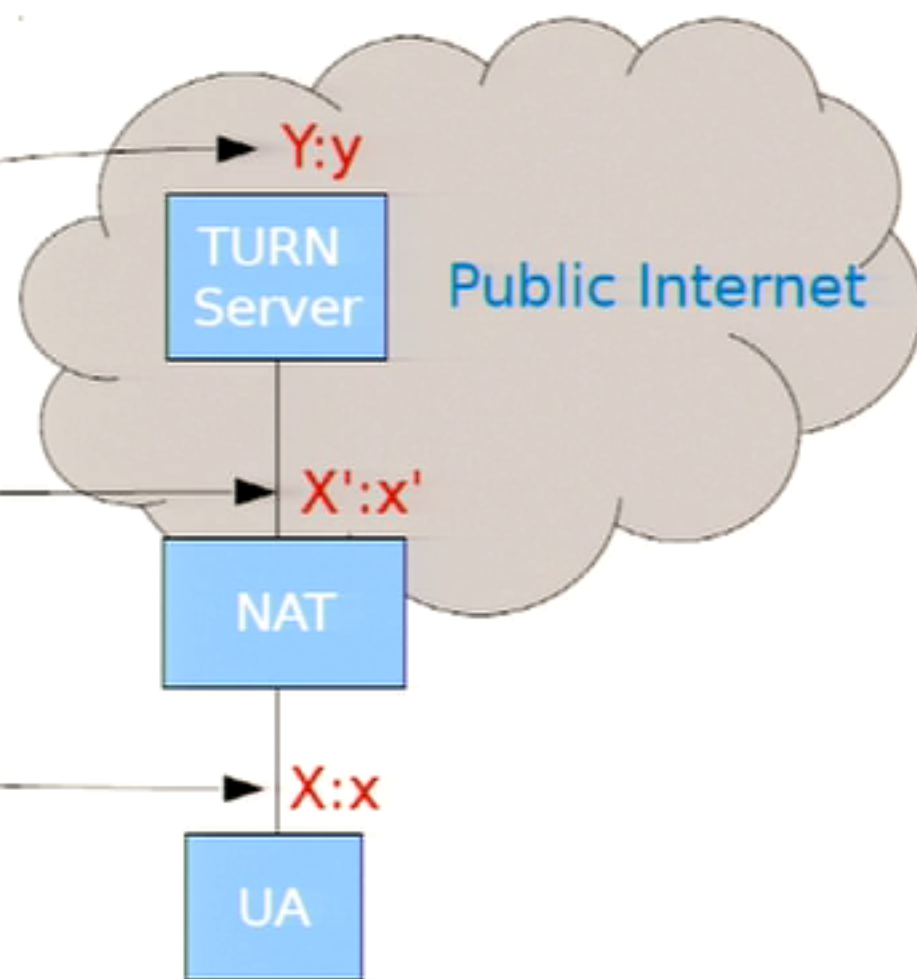




WebRTC



- Candidate pair
 - IP address, port, protocol
- Types
 - Relayed
 - Reflexive
 - Server, Peer
 - Host



- Discovery and Candidate gathering
 - Allocation
- Prioritisation
- Exchange
- Connectivity Check
 - Frozen Algorithm
- Coordination
- Communication



Bundle / rtcp-mux

Default

4
Connections

	RTP	RTCP
A		
V		

Bundle

2
Connections

	RTP	RTCP
A		
V		

a=group:BUNDLE

rtcp-mux

2
Connections

	RTP	RTCP
A		
V		

a=rtcp-mux

Both

1
Connection

	RTP	RTCP
A		
V		

- REQ-1:
 - A NAT MUST have an "**Endpoint-Independent Mapping**" behavior.
- REQ-8:
 - If application transparency is most important, it is RECOMMENDED that a NAT have "**Endpoint-Independent Filtering**" behavior. If a more stringent filtering behavior is most important, it is RECOMMENDED that a NAT have "**Address-Dependent Filtering**" behavior.
 - a) The filtering behavior MAY be an option configurable by the administrator of the NAT.

NAT főbb viselkedések: (mapping, filtering)

(port assignment, port parity, hairpinning,
mapping refresh, conflicting ip address
handling, etc.)

- REQ-1:
 - A NAT MUST have an "**Endpoint-Independent Mapping**" behavior.
- REQ-8:
 - If application transparency is most important, it is RECOMMENDED that a NAT have "**Endpoint-Independent Filtering**" behavior. If a more stringent filtering behavior is most important, it is RECOMMENDED that a NAT have "**Address-Dependent Filtering**" behavior.
 - a) The filtering behavior MAY be an option configurable by the administrator of the NAT.

- Mapping

- EIM
- ADM
- APDM

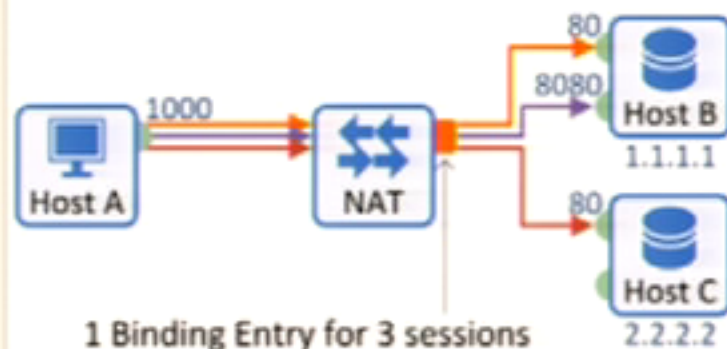
- Filtering

- EIF
- ADF
- APDF

	RFC 5780 definition		RFC 3489 definition
NAT Type 1	Endpoint-Independent Mapping	Endpoint-Independent Filtering	Full Cone
NAT Type 2	Endpoint-Independent Mapping	Address-Dependent Filtering	Restricted Cone
NAT Type 3	Endpoint-Independent Mapping	Address and Port-Dependent Filtering	Port Restricted Cone
NAT Type 4	Address-Dependent Mapping	Endpoint-Independent Filtering	
NAT Type 5	Address-Dependent Mapping	Address-Dependent Filtering	
NAT Type 6	Address-Dependent Mapping	Address and Port-Dependent Filtering	
NAT Type 7	Address and Port-Dependent Mapping	Endpoint-Independent Filtering	
NAT Type 8	Address and Port-Dependent Mapping	Address-Dependent Filtering	
NAT Type 9	Address and Port-Dependent Mapping	Address and Port-Dependent Filtering	Symmetric

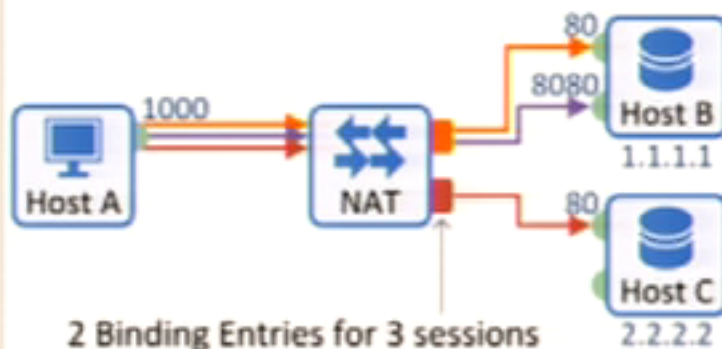
Endpoint-Independent Mapping

Endpoint-Independent Mapping

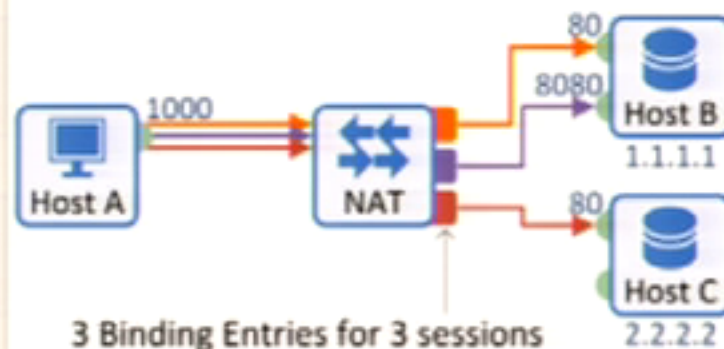


Endpoint-Dependent Mapping

Address-Dependent Mapping



Address and Port-Dependent Mapping

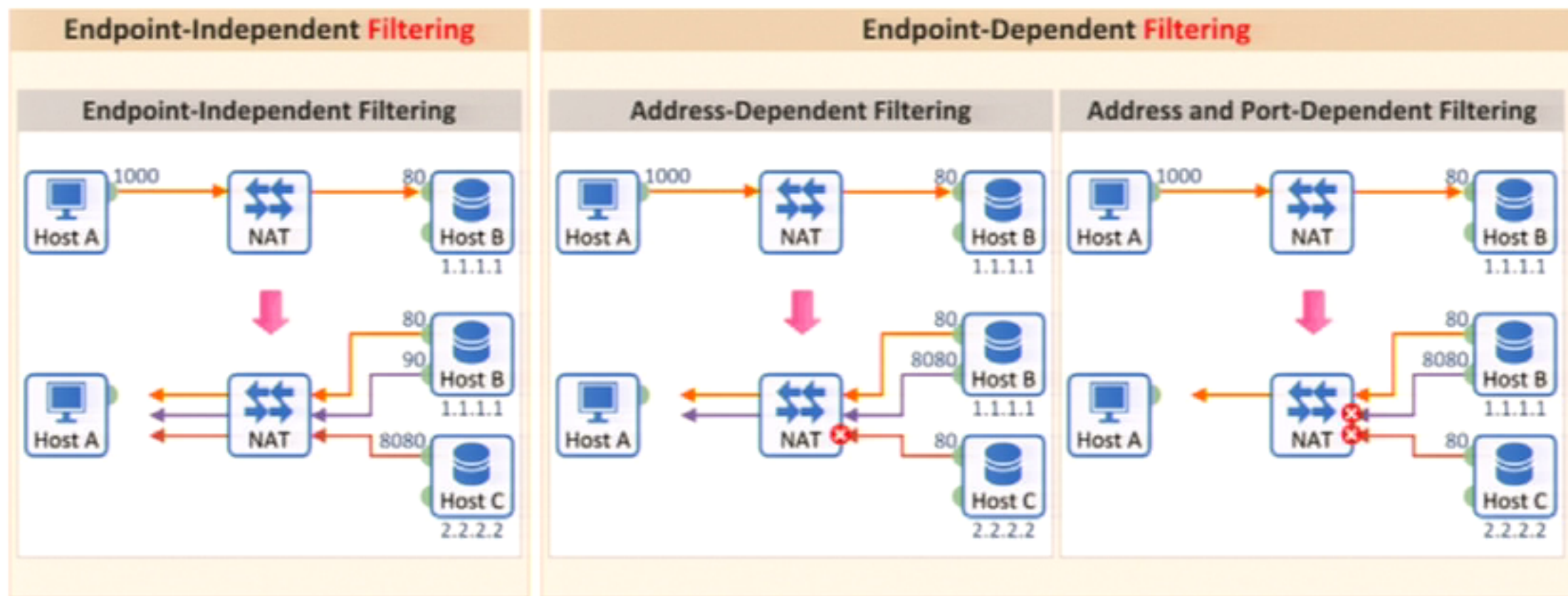


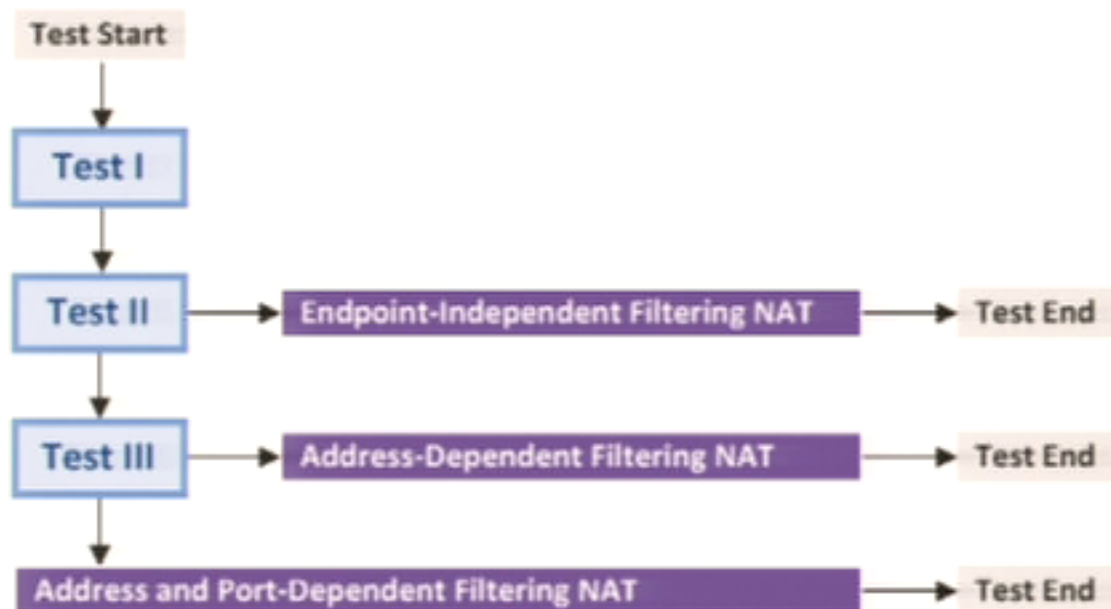


- TEST I
 - Primary IP, Primary Port
- TEST II
 - Alternate IP, Primary Port
- TEST III
 - Alternate IP, Alternate Port

Forrás:

<http://www.netmanias.com/en/post/techdocs/6067/nat-stun/nat-behavior-discovery-using-stun-rfc-5780>





- TEST I
 - Primary IP, Primary Port
- TEST II
 - Change Request IP and Port
- TEST III
 - Change Request Port

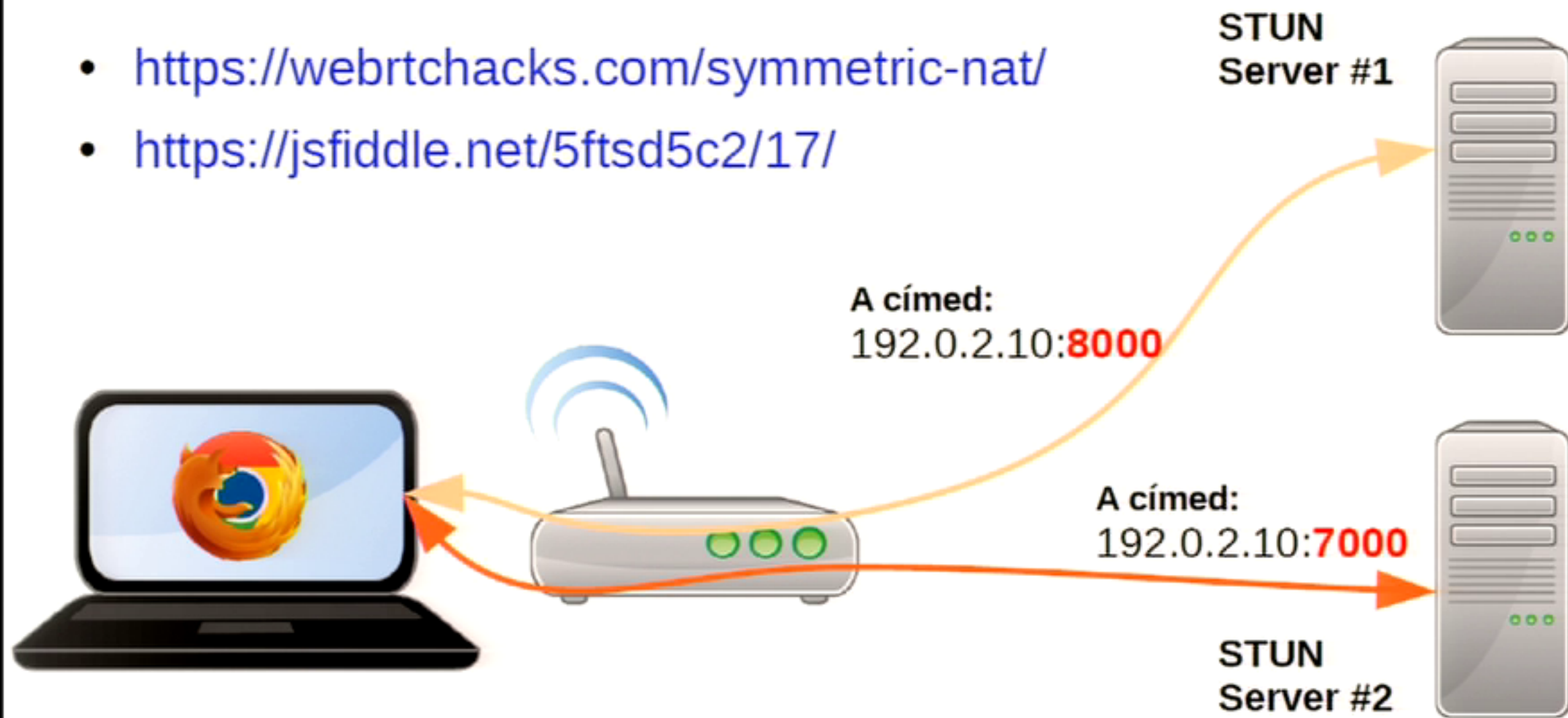
Forrás:

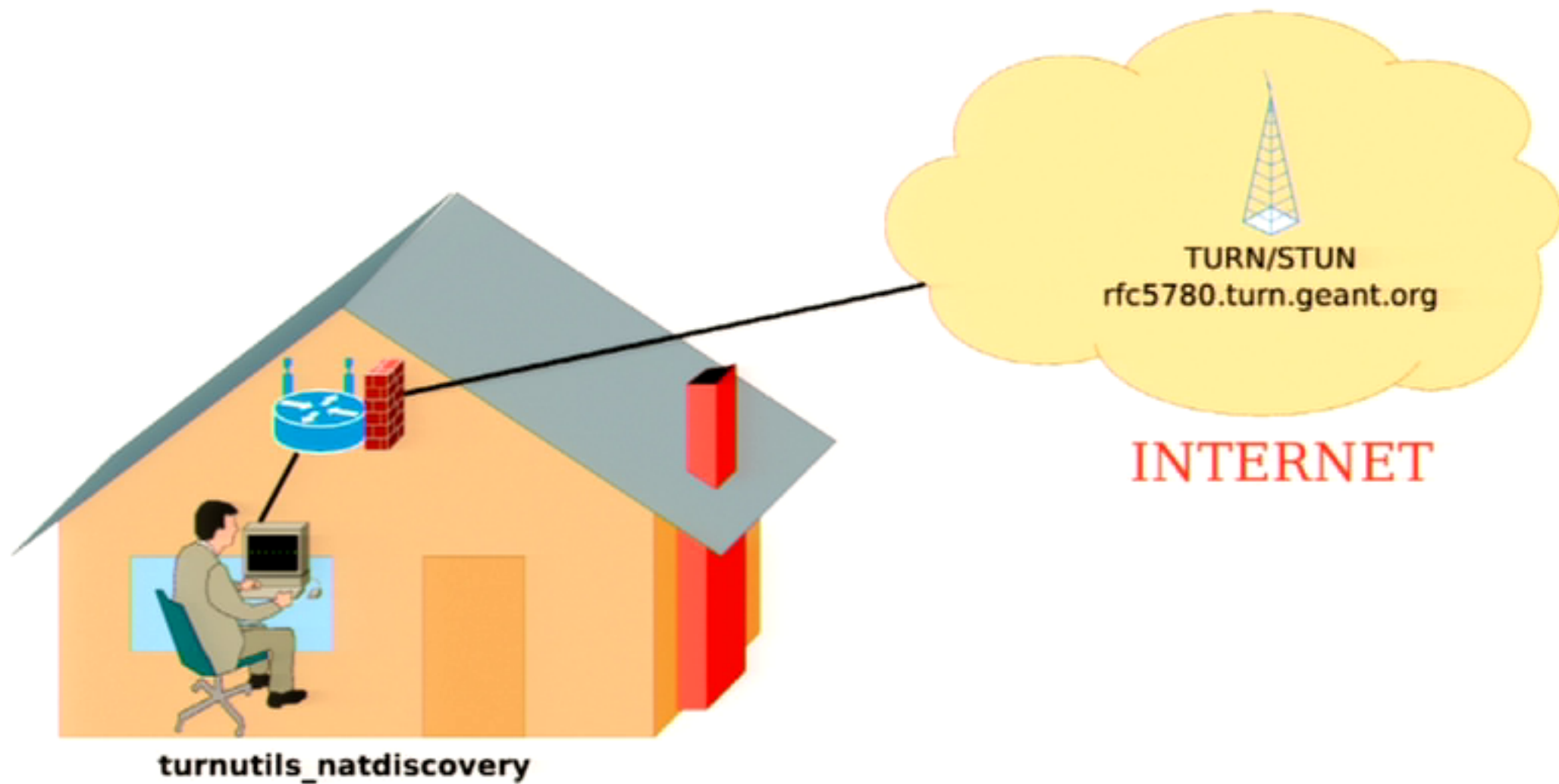
<http://www.netmanias.com/en/post/techdocs/6067/nat-stun/nat-behavior-discovery-using-stun-rfc-5780>

- Recommendations for Transport-Protocol Port Randomization
 - <https://tools.ietf.org/html/rfc6056>
- Updates to Network Address Translation (NAT) Behavioral Requirements (RFC4787++)
 - <https://tools.ietf.org/html/rfc7857>
- Min segít? pl. DNS cache mérgezés / Kaminsky támadás
 - <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>
- De még a port randomizálás sem véd minden támadás ellen.
 - <https://arxiv.org/pdf/1205.5190.pdf>

Szimmetrikus NAT felismerés böngészőből

- <https://webrtcchacks.com/symmetric-nat/>
- <https://jsfiddle.net/5ftsd5c2/17/>






```
$ turnutils_natdiscovery -f -m rfc5780.turn.geant.org
...
=====
NAT with Address and Port Dependent Mapping!
=====
...
=====
NAT with Address and Port Dependent Filtering!
=====
$
```

Campus NAT Behaviors

	EIM/EIF	EIM/ADF	EIM/APDF	APDM/APDF
Linux			Default	--random --random-fully
BSD			static-port	Default
Juniper vSRX	"persistent-nat any-remote-host"	"persistent-nat target-host"	"persistent-nat target-host- port"	Default
Cisco ios			Default	
Checkpoint 21400				Default

27%

of the sessions
use a TURN
relay server

4.1. TURN Relay Usage

The relay server usage is an important metric for applications and services that want to use the least amount of infrastructure servers. Without any TURN relay servers, these sessions would fail to setup, therefore, deploying TURN servers is important to establish connectivity. We observe that on average 27% of the sessions use a TURN relay server.

TABLE 4.1. TURN USAGE

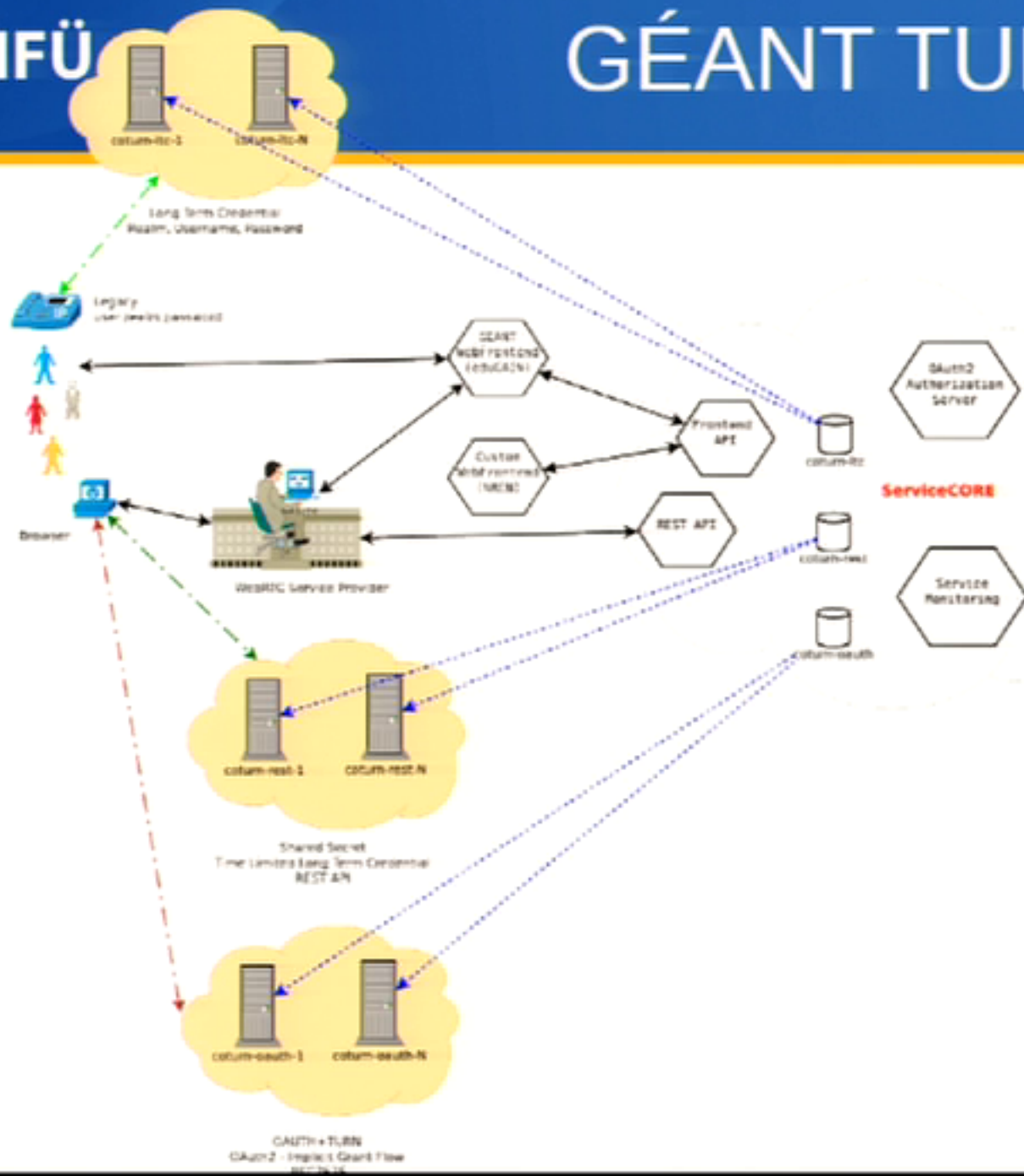
Nov	Dec	Jan	Feb
26,2 %	27,4 %	29,0 %	26,3 %

Usage metrics from real world WebRTC deployments.

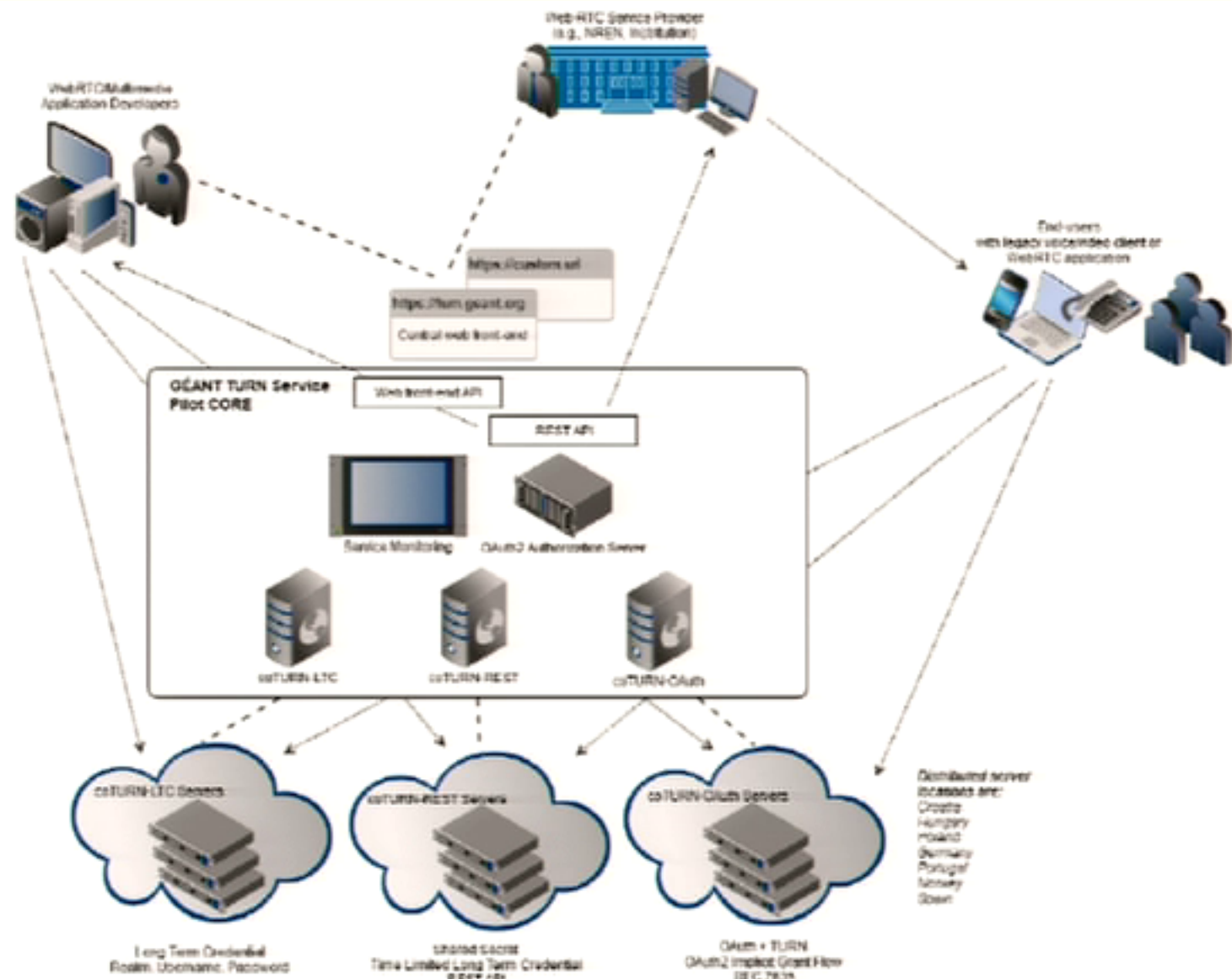


GÉANT

STUN/TURN pilot
Knockplop

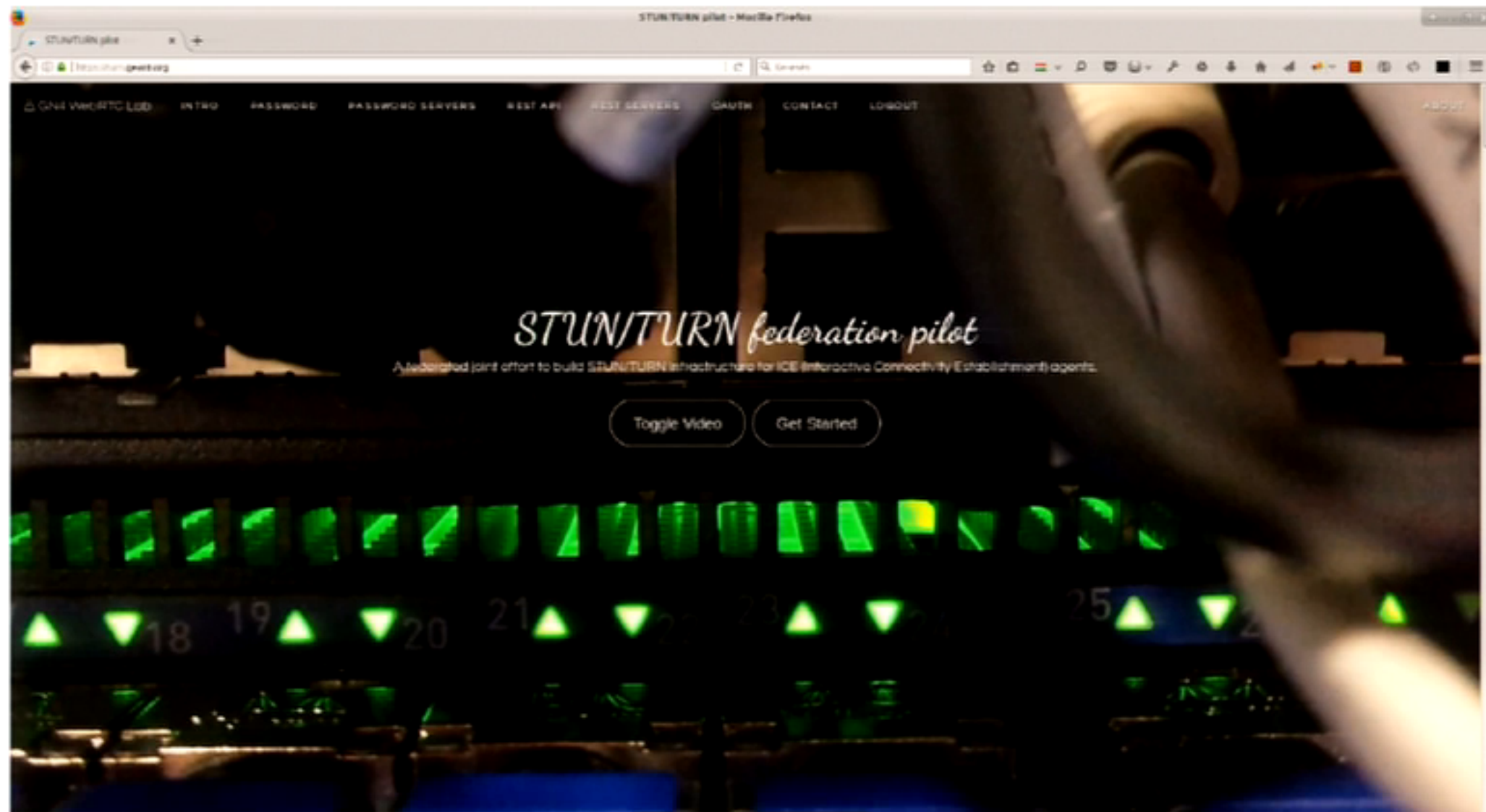


- <https://turn.geant.org>
- 3 féle autentikáció
- Elosztott infrastruktúra
- Európai közös erőfeszítés
- Szabványosítás (W3C, IETF)
- Cél
 - Legközelebbi szerver használata
 - Média forgalom GÉANT hálózaton belül tartása



Hol is?





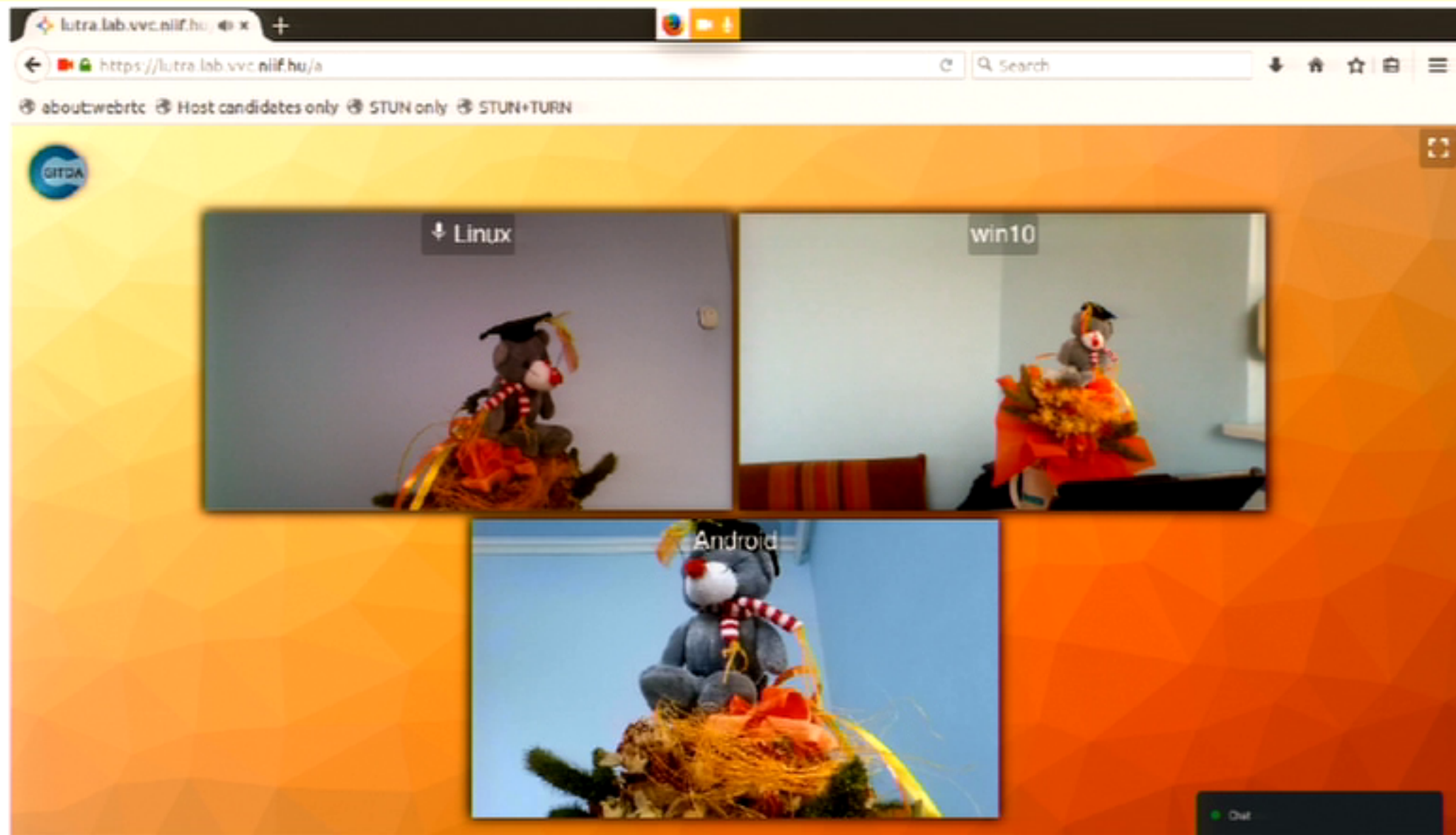
- Firefox TURN setup
 - `media.peerconnection.use_document_iceservers`
 - `media.peerconnection.default_iceservers`
- CSipSimple
 - <https://en.wikipedia.org/wiki/CSipSimple>
 - PJSIP



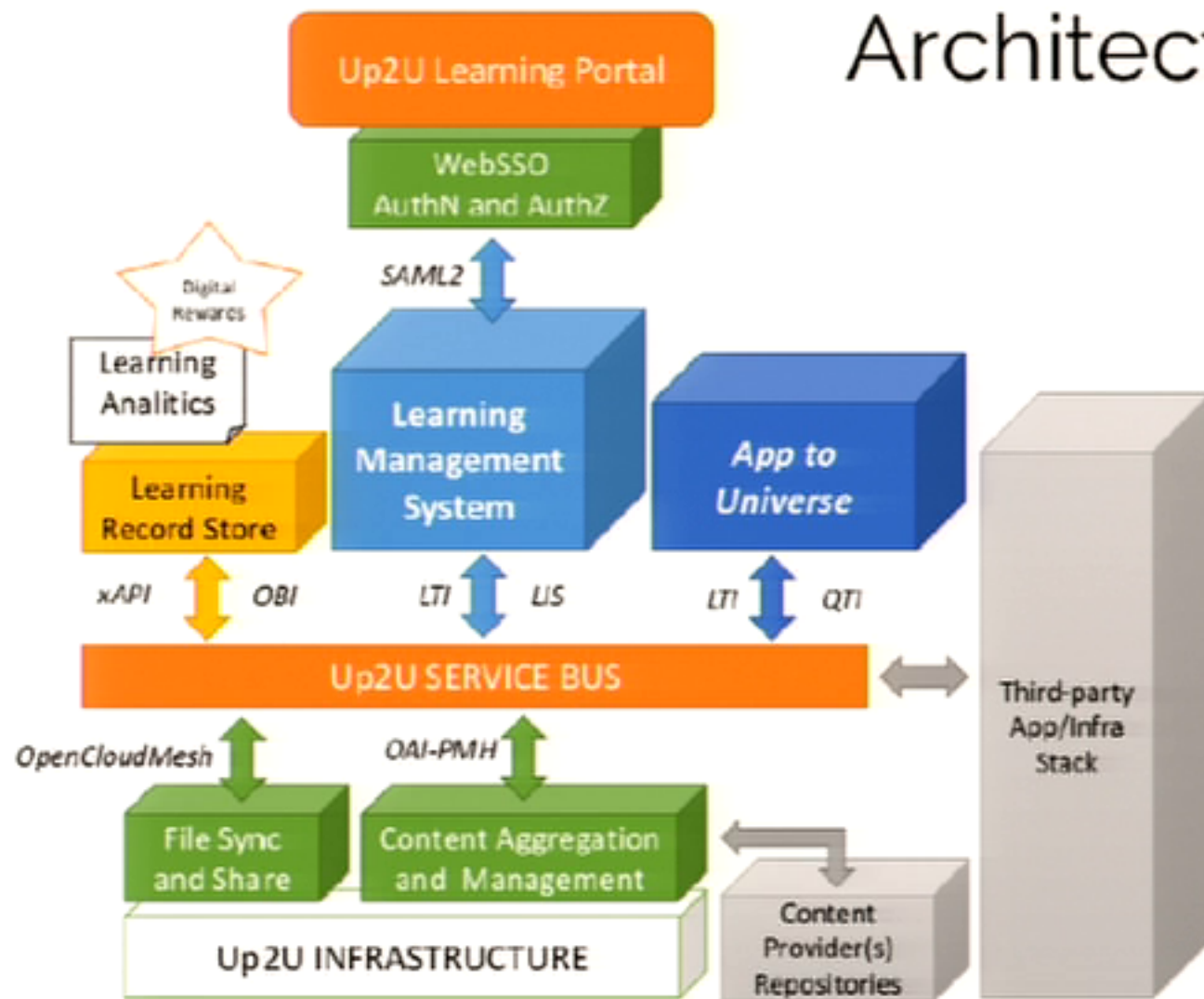
- Alap WebMeeting
- Szobák
 - Képernyő megosztás
 - Chat
- P2P
 - Teljes Összekapcsolt
 - Full Mesh
- Fogd és vidd rendezés
- MIT licenc

- node.js
 - web/https: express
 - signaling: socket.io
- Gulp
- GÉANT TURN
 - RTT TURN test
- Loopback tükör (TURN)
- Forrás:
 - <https://github.com/so010/knockplop>

UNINETT



Architecture



- Open Technology
- Standard APIs
- Value-add
- Scalable
- Modular
- Portable
- INTEROPERABILITY

- Példa WebRTC alkalmazás: **Knockplop** (moodle-plugin - UP2U)
 - RTC: WebRTC, VoIP, Vidkonf, Streaming, etc.
- **Tűzfalátjárás** mindenképp szükséges
 - Gáta: Csomagszűrés, NAT, IPv6 áttérés, multihoming, stb.
- Szabványos Tűzfalátjárás: **ICE**
 - **STUN / TURN** infrastruktúrára épül
- GÉANT: **STUN/TURN infrastruktúra**
 - Elosztott, tartalékkolt, monitorozott, Relay közel a klienshez, stb.
 - Forgalom az GÉANT hálózaton belül marad



39 / 39

80,8%



Köszönöm a Figyelmet!

PDF exportálása

Adobe Acrobat Pro DC

PDF fájlok Word-, illetve Excel fájlá alakítása

További tudnivalók

PDF létrehozása

PDF szerkesztése

Megjegyzés

Fájlok kombinálása

Kitöltés és aláírás

További eszközök

Fájlok tárolása és megosztása a Document Cloud szolgáltatásban

További információ