SWITCH

The Swiss Education & Research Network

SIP security and the great fun with Firewall / NAT

Bernie Höneisen

SURA / ViDe, 29.03.2006, Atlanta, GA (USA)

Content

- SIP and Firewall
- SIP and NAT
- Privacy / Encryption
- SpIT / Authentication
- SIP Identity
- General Internet Security

Firewalls

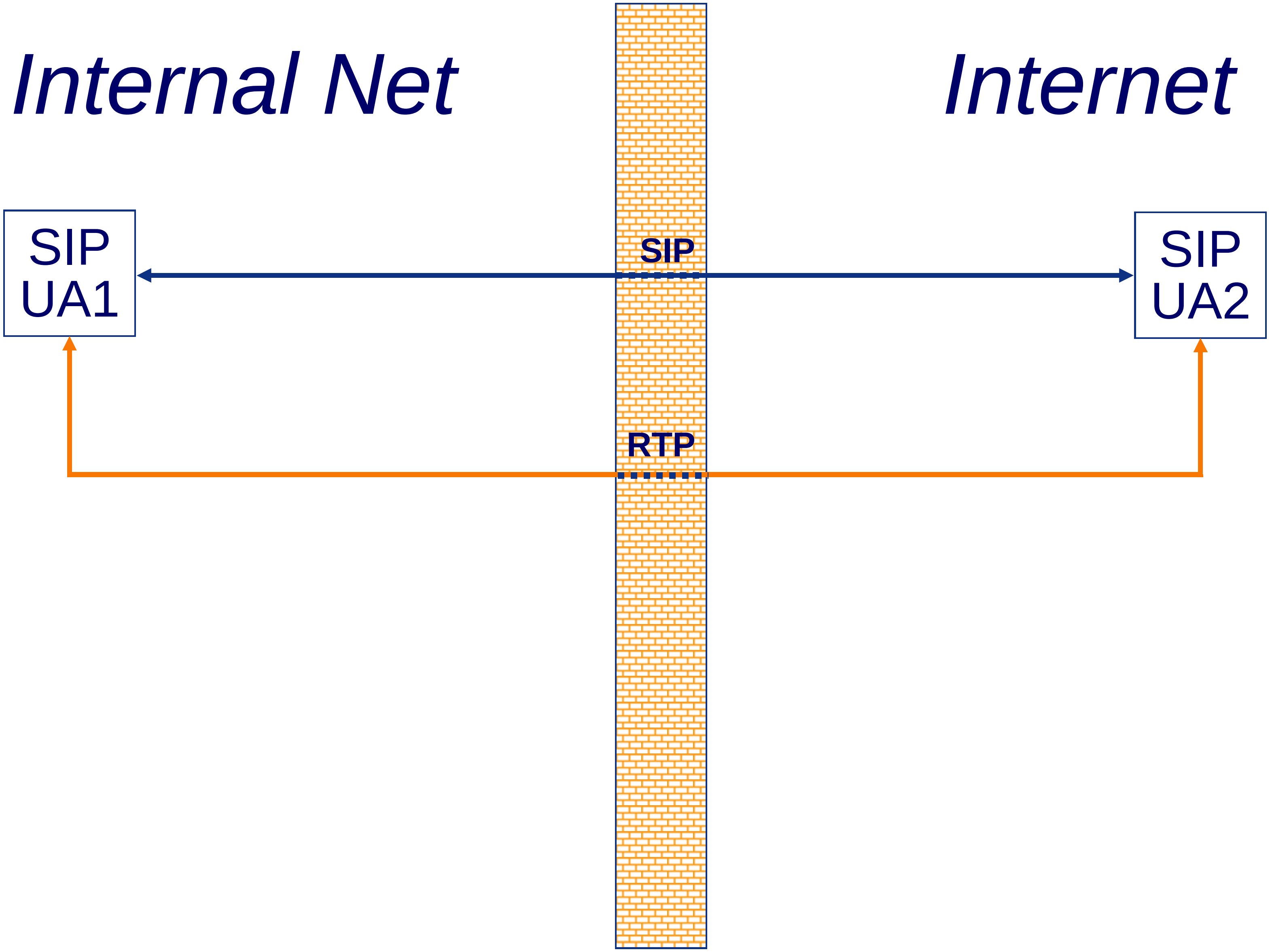
- SIP signalling and media transport is done peer-to-peer
- Media ports are negotiated per call
- The number of firewalls is growing (including personal FWs)
- Firewall rules get more restrictive

→ One has to take special measures to allow SIP communication through firewalls

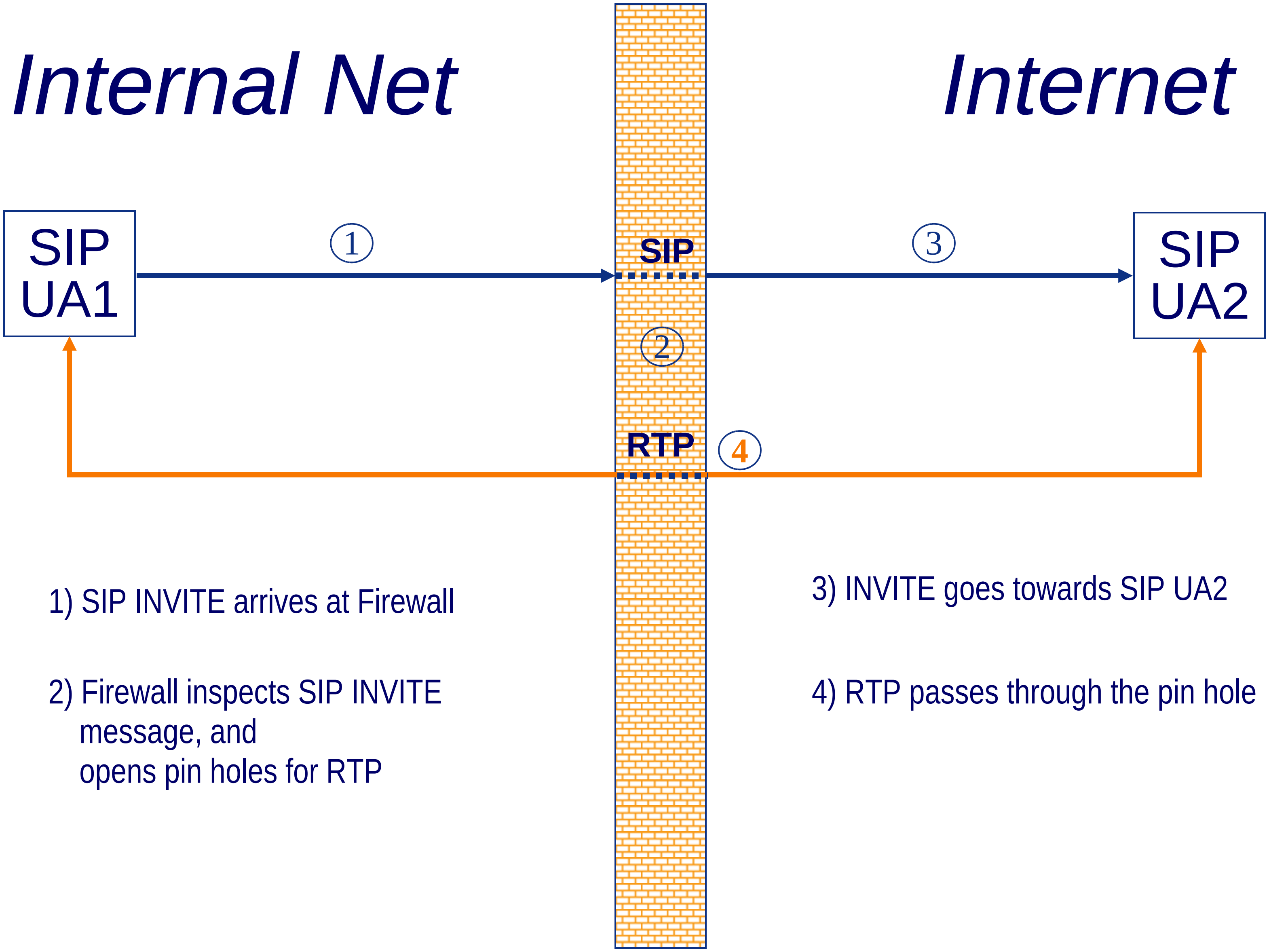
Some Ways to deal with Firewalls

- Open pin holes (statically)
- SIP aware firewall
  - dynamically open pin holes per session
- Stateful firewall
  - outgoing traffic opens pin holes for corresponding incoming traffic
  - Precondition: UA must support symmetric signalling and media
- Proxy Solution
  - open pin holes just to dedicated hosts e.g. in DMZ
    - » TURN Server
    - » Mediaproxy / B2BUA

Open Pin Holes in Firewall



SIP aware Firewall



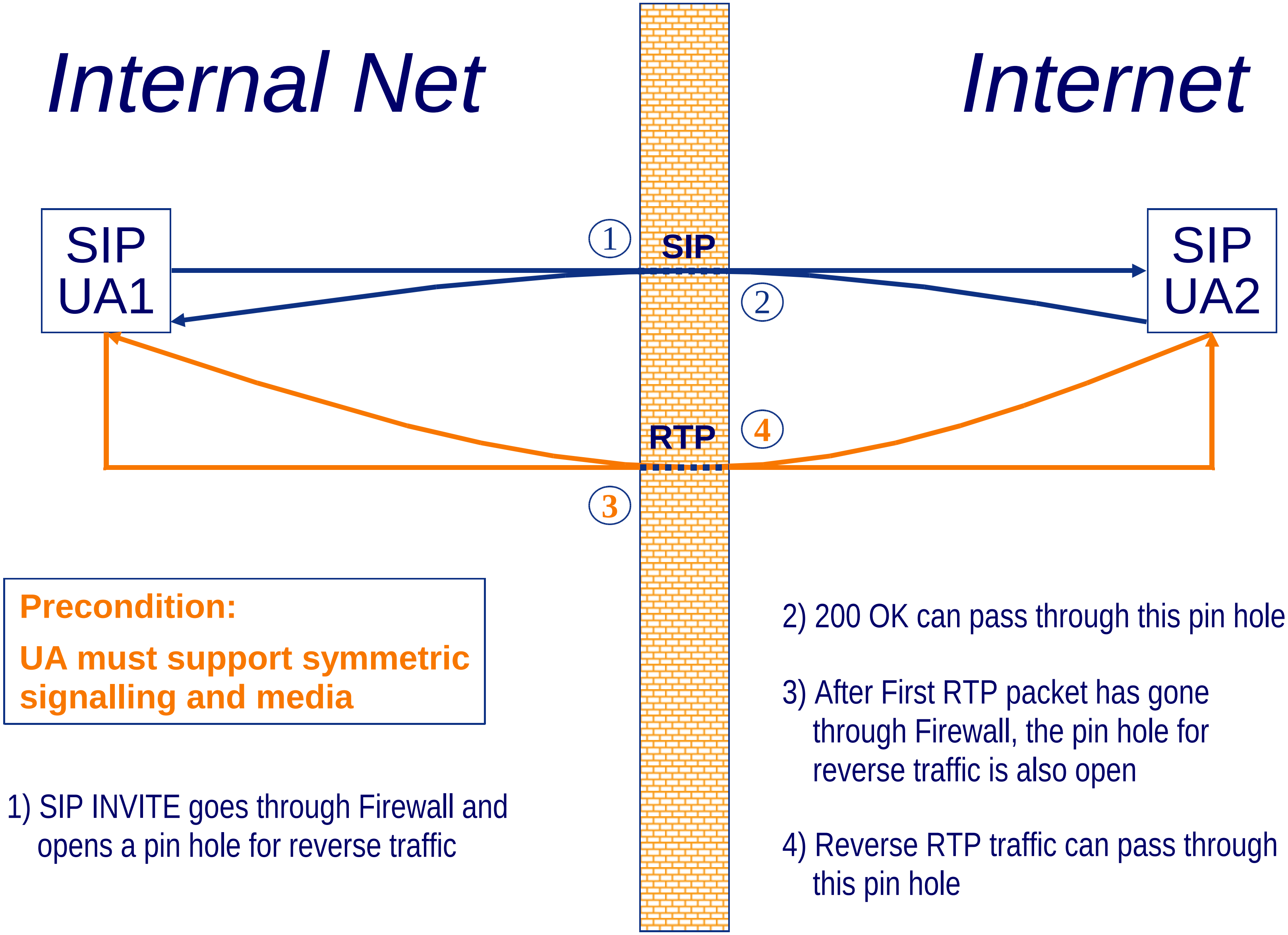
1) SIP INVITE arrives at Firewall

2) Firewall inspects SIP INVITE message, and
opens pin holes for RTP

3) INVITE goes towards SIP UA2

4) RTP passes through the pin hole

Stateful Firewall



Precondition:

UA must support symmetric signalling and media

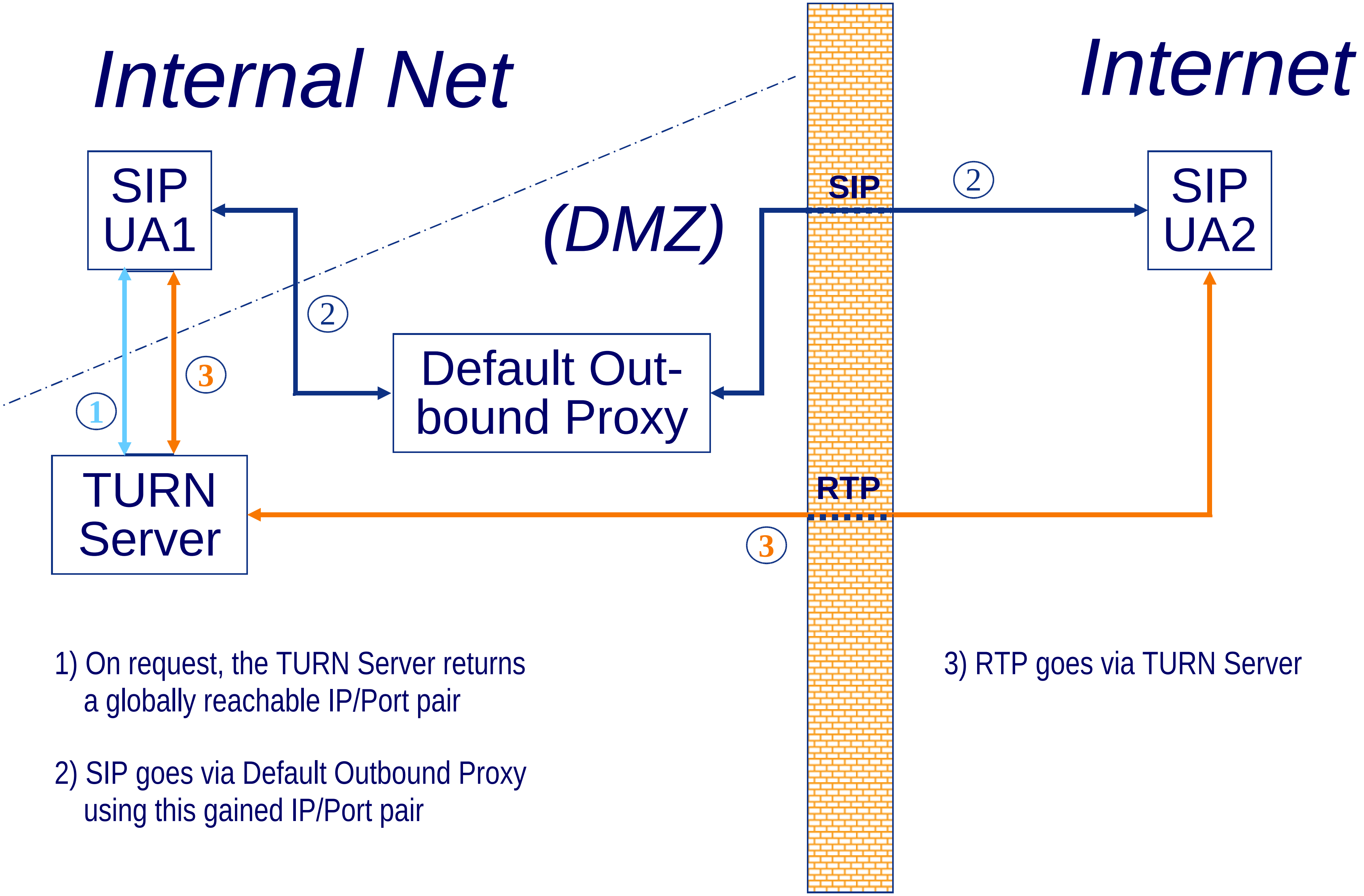
1) SIP INVITE goes through Firewall and opens a pin hole for reverse traffic

2) 200 OK can pass through this pin hole

3) After First RTP packet has gone through Firewall, the pin hole for reverse traffic is also open

4) Reverse RTP traffic can pass through this pin hole

TURN Server

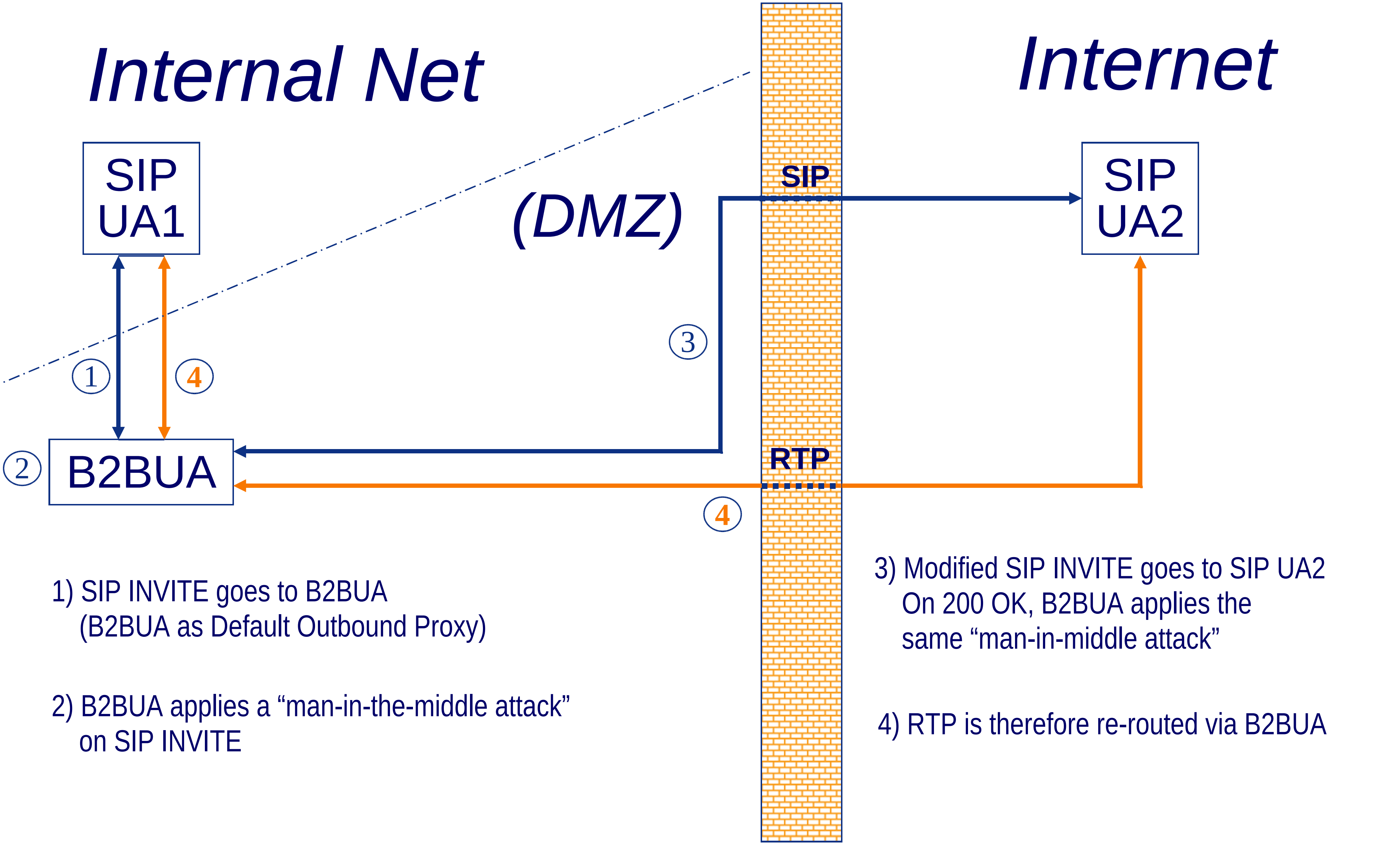


1) On request, the TURN Server returns a globally reachable IP/Port pair

2) SIP goes via Default Outbound Proxy using this gained IP/Port pair

3) RTP goes via TURN Server

Mediaproxy / B2BUA



1) SIP INVITE goes to B2BUA
(B2BUA as Default Outbound Proxy)

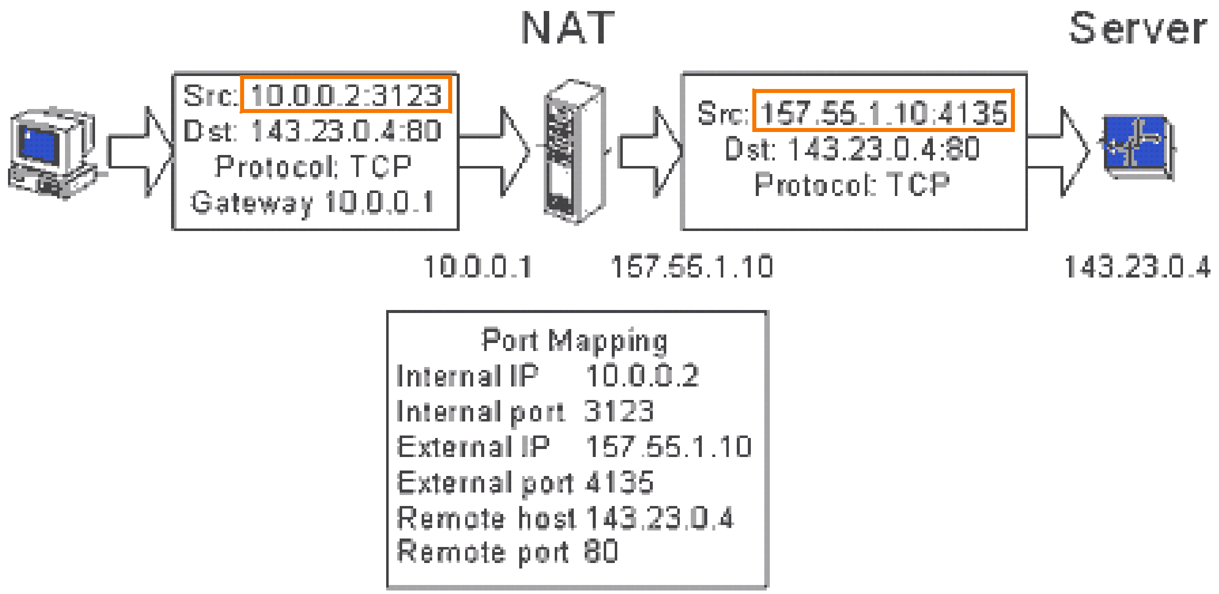
2) B2BUA applies a “man-in-the-middle attack” on SIP INVITE

3) Modified SIP INVITE goes to SIP UA2
On 200 OK, B2BUA applies the same “man-in-middle attack”

4) RTP is therefore re-routed via B2BUA

Network Address Translation (NAT)

- Many networks are "protected" with a NAT box (shortage of IP addresses, firewall functionality)
- With IPv6 we don't need NAT anymore
  - hopefully...
  - time scale?
- Basic NAT operation:



Src: 10.0.0.2:3123
Dst: 143.23.0.4:80
Protocol: TCP
Gateway 10.0.0.1

Src: 157.55.1.10:4135
Dst: 143.23.0.4:80
Protocol: TCP

Port Mapping

Internal IP	10.0.0.2
Internal port	3123
External IP	157.55.1.10
External port	4135
Remote host	143.23.0.4
Remote port	80

Some ways to overcome a NAT

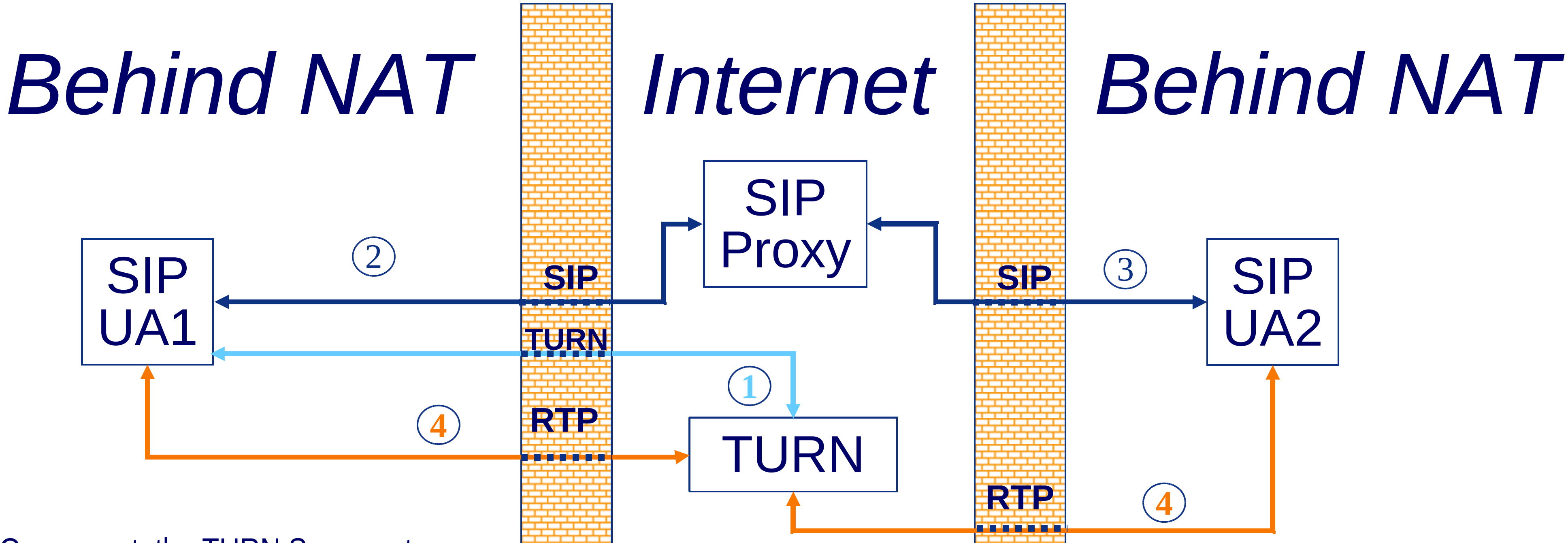
- STUN
  - – Discover NAT and Firewall situation between UA and Internet
  - – Discover public IP Address (and port mapping rules) of NAT
- TURN
  - – Request a public IP/Port pair to proxy RTP streams
- ICE
  - – Provide in SIP signalling many (ordered) alternatives, typically including also STUN and TURN
  - – The other side performs “trial and error”
- Mediaproxy / B2BUA
  - – “man-in-middle attack” to SIP signalling

→ **All these solutions require UA to support symmetric signalling and media**

More ways to overcome a NAT

- UPnP
  - Request NAT to open pin holes and return public IP/Port pair(s)
- Port forwarding
  - Statically configure NAT to keep certain pin holes and bindings open
- SIP aware NAT
  - Let NAT inspect signalling and dynamically open the Pin Holes

TURN Server



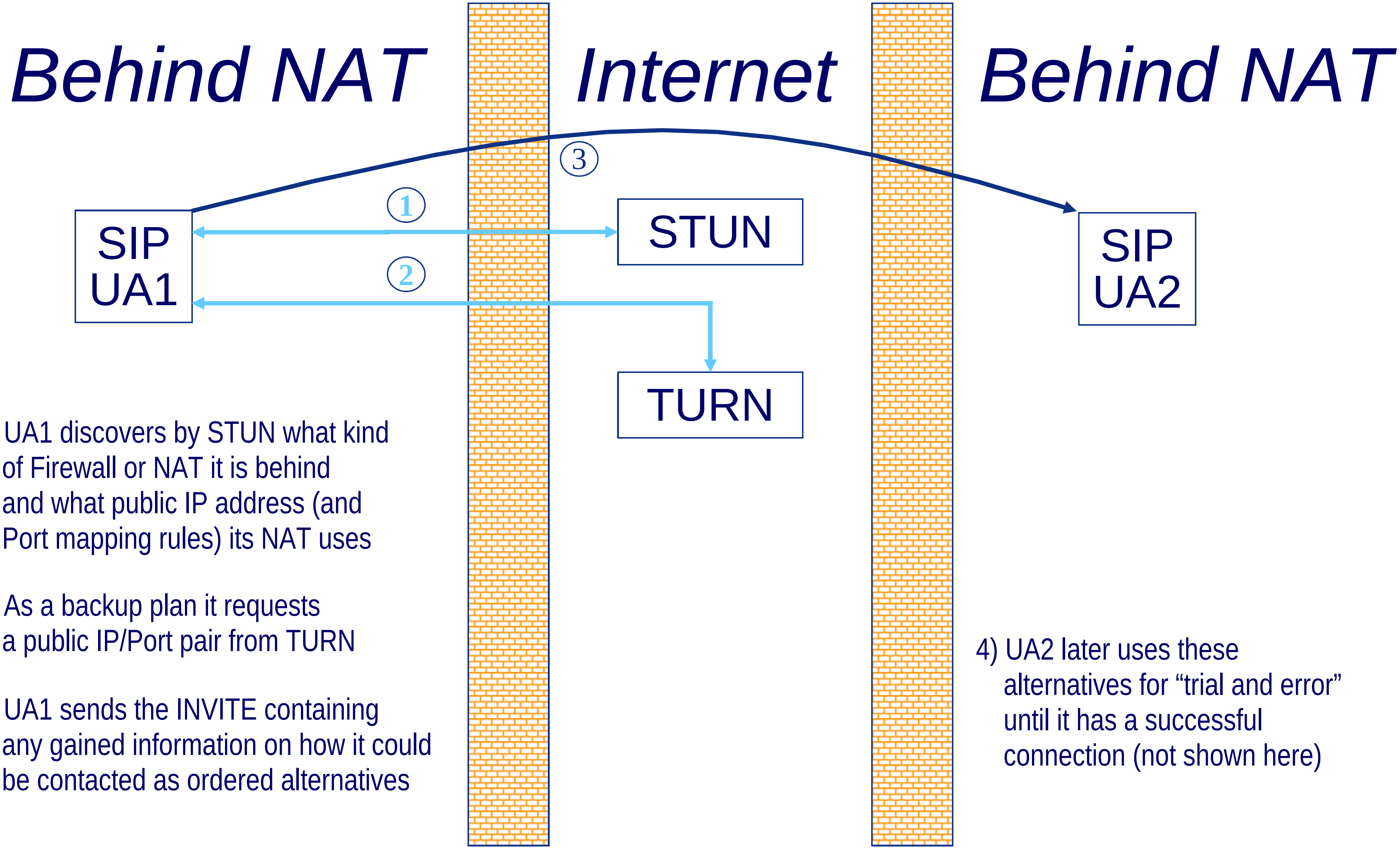
1) On request, the TURN Server returns a globally reachable IP/Port pair

2) SIP INVITE using this IP/Port pair goes to SIP Proxy

3) SIP INVITE goes to UA2 (Pin Hole has been kept open by SIP Proxy)

4) RTP is therefore re-routed via TURN Server
Pin holes on both sides are opened by first (RTP) packet

ICE / STUN / TURN



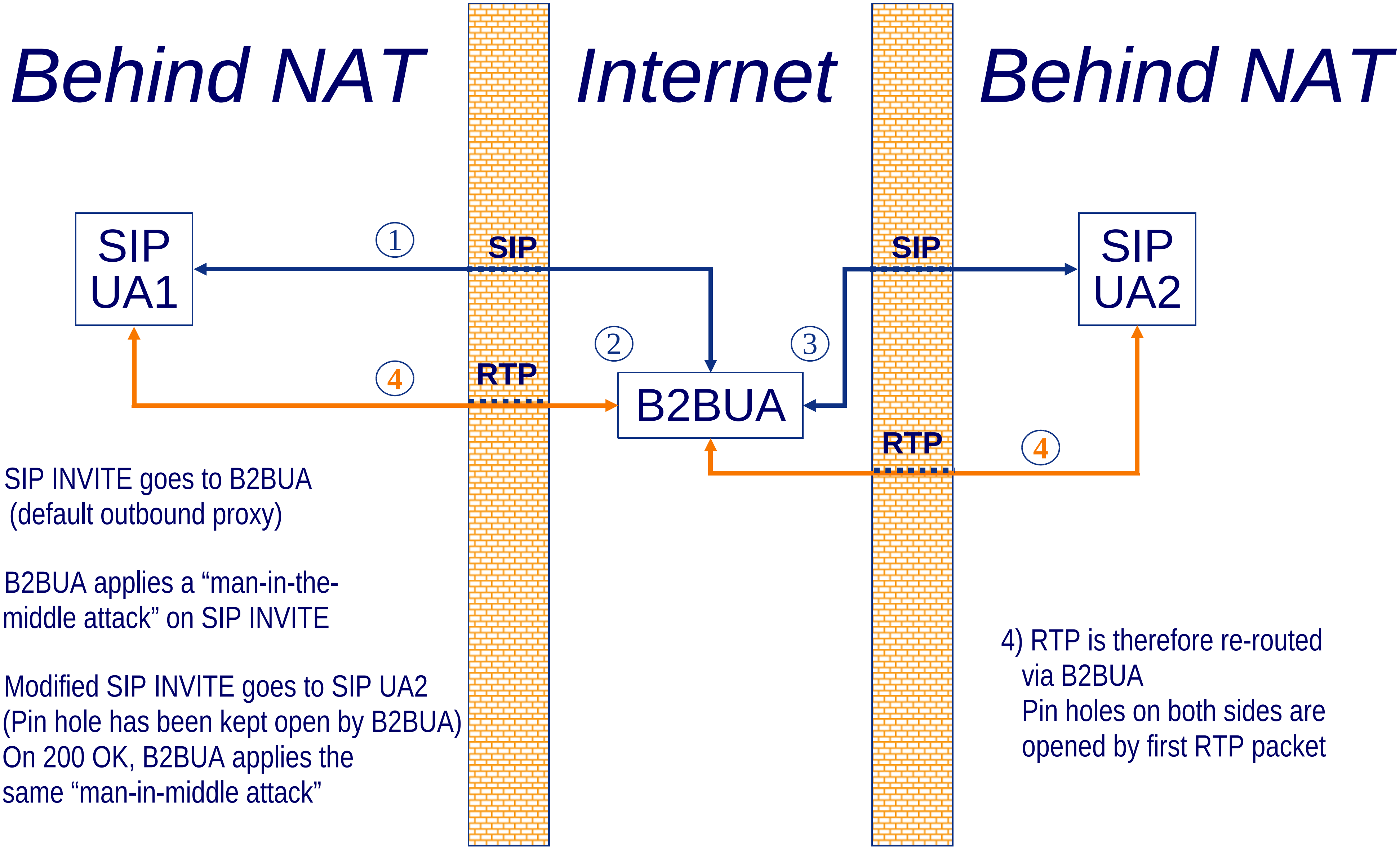
1) UA1 discovers by STUN what kind of Firewall or NAT it is behind and what public IP address (and Port mapping rules) its NAT uses

2) As a backup plan it requests a public IP/Port pair from TURN

3) UA1 sends the INVITE containing any gained information on how it could be contacted as ordered alternatives

4) UA2 later uses these alternatives for “trial and error” until it has a successful connection (not shown here)

Mediaproxy / B2BUA



1) SIP INVITE goes to B2BUA
 (default outbound proxy)

2) B2BUA applies a “man-in-the-middle attack” on SIP INVITE

3) Modified SIP INVITE goes to SIP UA2
(Pin hole has been kept open by B2BUA)
On 200 OK, B2BUA applies the same “man-in-middle attack”

4) RTP is therefore re-routed via B2BUA
Pin holes on both sides are opened by first RTP packet

Privacy, Encryption

- **Wiretapping a SIP based conversation is not easy**
- **As with PSTN, one needs physical access to the network**
- **But, gaining physical access to WLAN networks is easy**

Encryption (possible solutions)

- Signalling (SIP)
  - End-to-End
    - S/MIME
  - Hop-by-hop
    - SIPS (require TLS on whole signalling path)
- Streams (RTP)
  - SRTP
- Lower Layer solutions
  - VPN, IPSec, TLS
  - Wireless: WEP, WPA, 802.1X

Spam over Internet Telephony (SpIT)

- Many VoIP services are free of charge or charged flatrate
- Sending pre-recorded messages to thousands of VoIP users within seconds is possible
  - SpIT calls in the middle of the night
  - Answering machine is full with SpIT
- Spam IMs will be a problem too

SpIT Prevention (possible solutions)

- Client based solutions
  - Closed User Groups
    - » Trusted buddy lists
- Network based Solutions
  - Web of trust
  - Blacklisting
  - Charging
- Mixed approaches
  - SIP Identity

⇒ All solutions require some kind of trust relationship, e.g.

- CA (server and/or client certificates)
- shared secret

Authentication

- Call hijacking
  - – associate a user’s SIP URI with another IP address
    - » “Stealing” calls from someone else
- Identity theft
  - – Caller Identity faking
    - » pretend to be someone else
    - » Using (charged) services of someone else
- Man-in-the-middle attack

→ Registration, call signalling and media should be authenticated

Authentication (possible solutions)

- Signalling (SIP)
  - Basic Authentication (deprecated!)
  - Digest Authentication (challenge - response)
  - S/MIME
  - SIPS
  - SIP Identity
- Streams (RTP)
  - SRTP
- Lower Layer solutions
  - TLS
  - IPSec
- All solutions require some kind of trust relationship, e.g.
  - Shared secret
  - CA (server and/or client certificates)

SIP Identity (draft-ietf-sip-identity-06)

- IETF proposal (Standards Track) in RFC Editor queue
- SIP messages are signed by sending UA or local SIP (Outbound) Proxy
  - If Proxy signs the SIP message (on behalf of the user)
    - » the UA authenticates at Proxy
      e.g. with Digest Authentication over TLS
- Receiving party (Proxy or UA) verifies signature
- Certificate Authority (CA)

Internet security

- VoIP systems are challenged by the well known Internet security threats:
  - (Distributed) Denial-of-Service
  - Viruses, worms, …
  - Buffer overflow attacks
  - …

- VoIP will most probably not be as reliable as the PSTN

→ This is the price we pay for new functionality/services and lower costs

;-)

Questions / Discussion