HERVÉ SCHAUER CONSULTANTS
Network Security Consulting Agency since 1989
Specialized in Unix, Windows, TCP/IP and Internet

IPv6

Network Security Threats

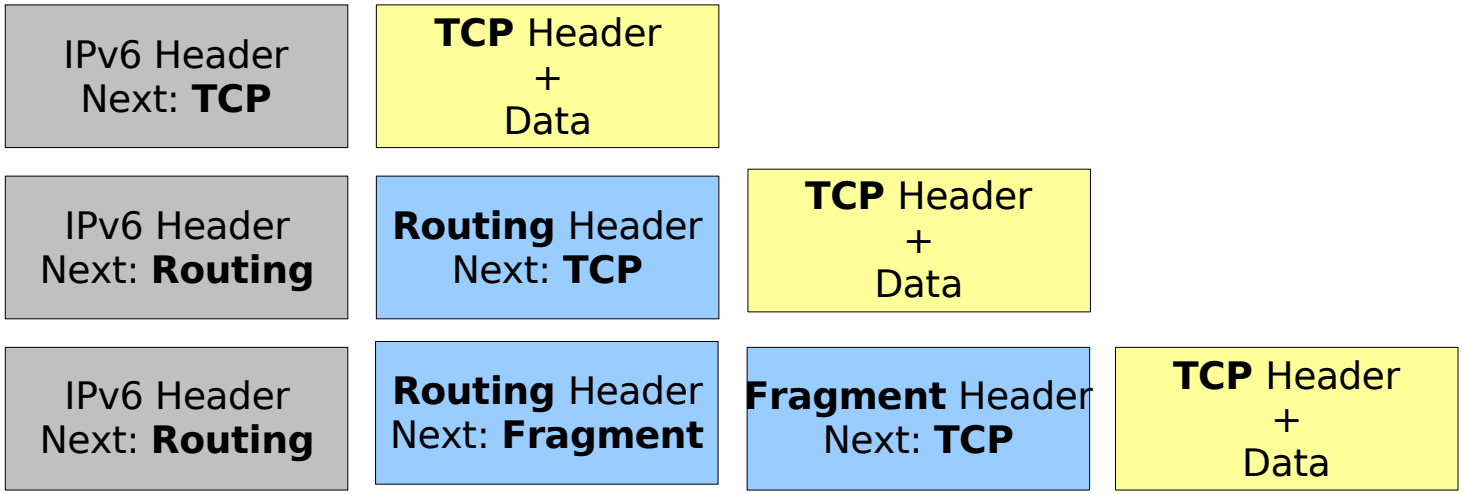
Nicolas Collignon
nicolas.collignon@hsc.fr - www.hsc.fr

Agenda

1. Covert channels
2. Application-level impacts
3. IDS impacts
4. Firewall / ACL bypassing
5. Mobiles Networks considerations

Covert Channels

- IPv6 extensions : Hop-by-Hop, Fragmentation, Routing ...



- TLV Options (Type-Length-Value)
- parallel streams hiding possibilities:
  - Specially crafted IPv6 extensions
  - « Home maid » TLV options

Applications impacts

- Low impacts on simple application-level protocols
- High impacts on application-level protocol carrying IP addresses
- A different IP addressing approach
  - Temporary Addresses, Privacy extensions
  - Session identification using IP addresses : authentication, statistics

An IDS nightmare :)

- Big addresses spaces
  - **/64 =~ 2 000 000 000** TCP+UDP scans with unique addresses

- Increasing use of IPsec
  - Skip encrypted traffic and miss attacks ?
  - Decrypt all IPsec traffic is not always possible
- Very modular IPv6 header's structure
  - Hard to design attacks signatures
  - More covert channel possibilities

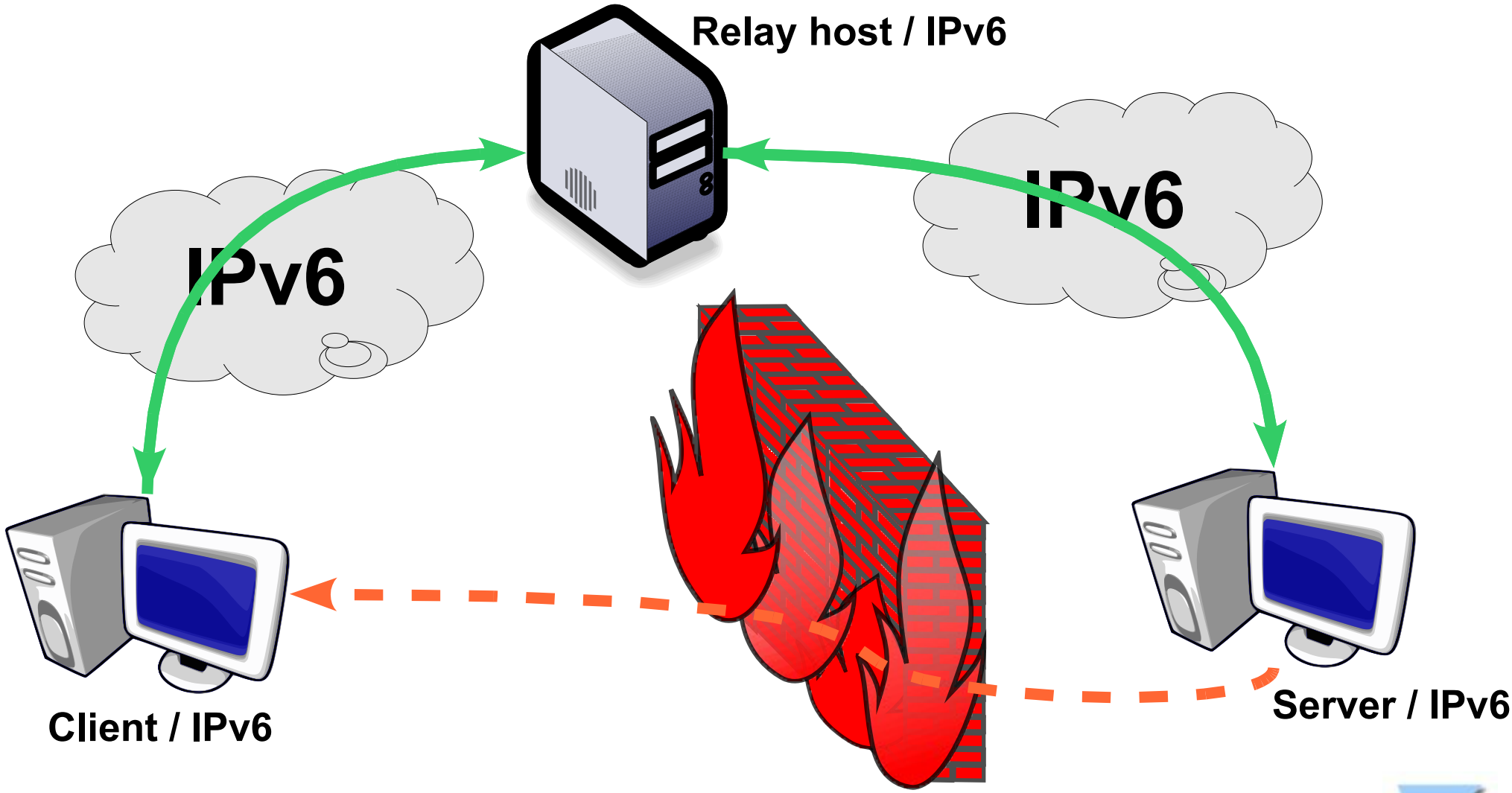
- Multiple packets routing methods
- How to handle dual protocol sessions ?

Routing Header type 0

- Concept similar to « *source routing* »
- Destination address changes at every hop
  - Complete header inspection needed to setup black-listing filtering 
- Most IPv6 enabled (including Internet connected) hosts support Routing Header type 0 and permit relaying 

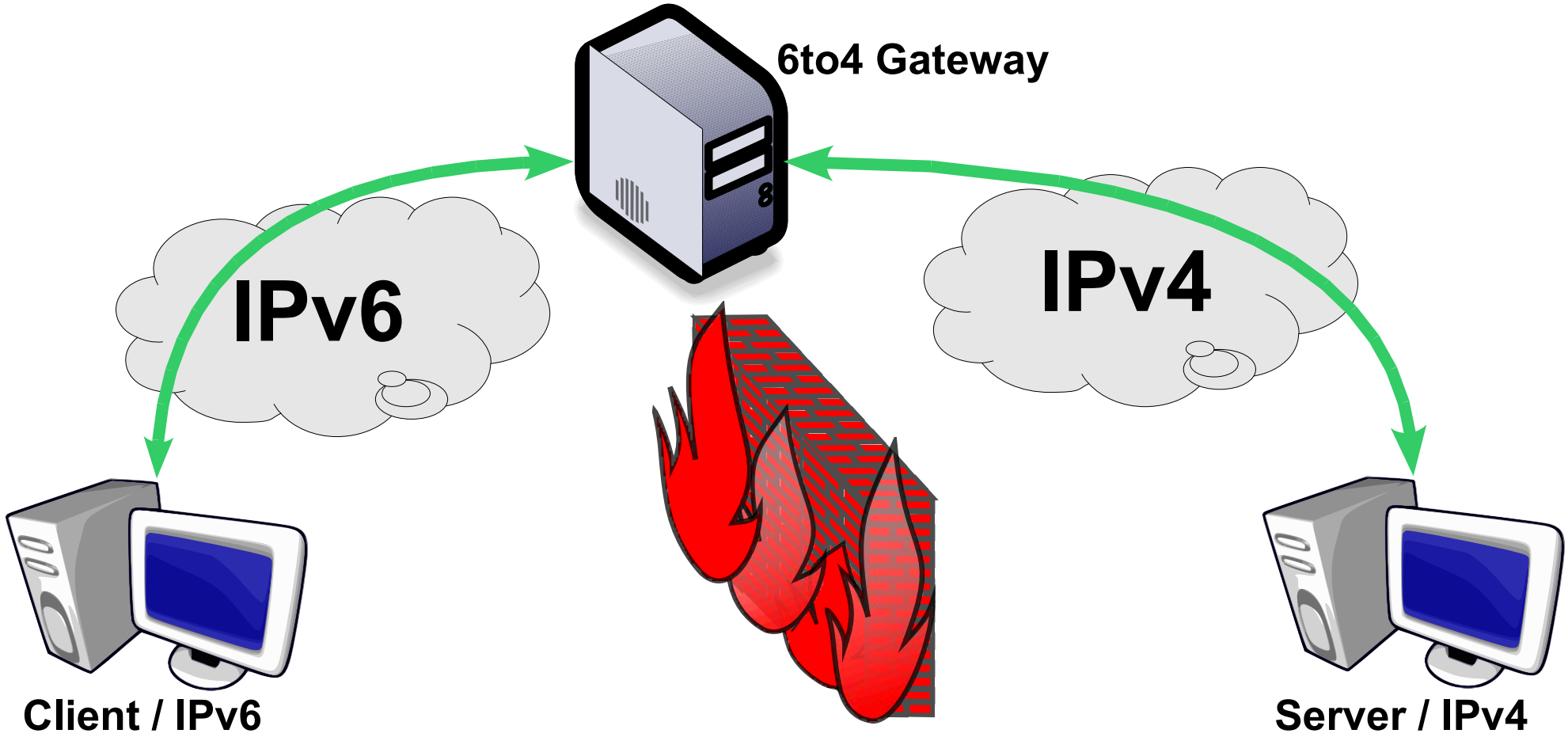
ACL bypass : Routing Headers

- Establish bidirectional tunnels



ACL bypass : 6to4 tunnels

- Use 6to4 gateways to bypass IPv4 ACLs
- A lot of 6to4 gateways open on Internet



Mobiles networks considerations

- Mobile to Mobile uncontrolled data streams
- 3GPP specifications say one /48 network per mobile

- Volume based accounting vs. Routing Headers
- IPv6 Mobility
  - may be dangerous: DoS
  - complex Routing Header filtering

IPv6 myths

- Scanning IPv6 networks take a very long time ? ***Yes but ...***
  - Increasing use of DNS, Sequential IP allocations (DHCP, GGSN)
  - Routing Headers may be used to speed up scan
  - Worms won't take longer to propagate: Multicast, EUI-64
- IPv6 is more secure than IPv4 ? ***No***
  - No standardized built-in key exchange protocol
  - Only 1 SEND implementation available
- Is it hard to define ACLs on an IPv6 network ? ***Yes***
  - Huge address space
  - IPv6 protocol and architecture complexity

Questions ?

...