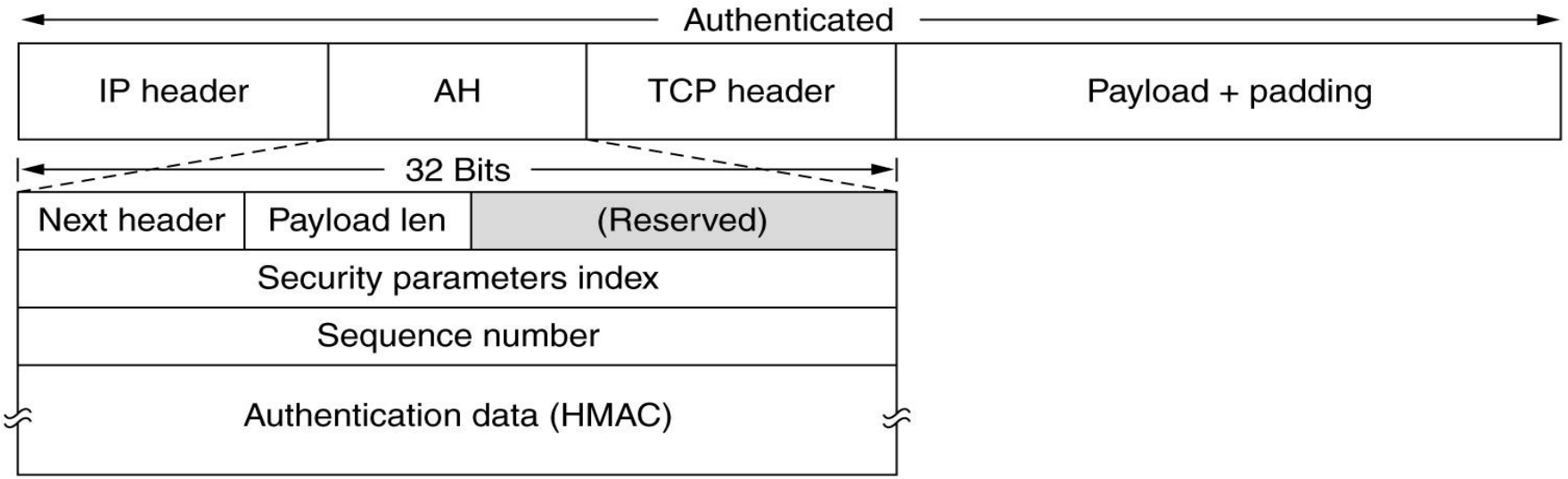
Sécurité des Réseaux, Master CSI 2
J.Bétréma, LaBRI, Université Bordeaux 1

IPSec

- RFC 2401 (novembre 1998)
- AH (Authentication Header, RFC 2402)
- ESP (Encapsulating Security Payload, RFC 2406)

AH en mode transport



The IPsec authentication header in transport mode for IPv4.

HMAC = Hashed Message Authentication Code (standard)

The protocol header (IPv4, IPv6, or Extension) immediately preceding the AH header will contain the value 51 in its Protocol (IPv4) or Next Header (IPv6, Extension) field.

Authentication data

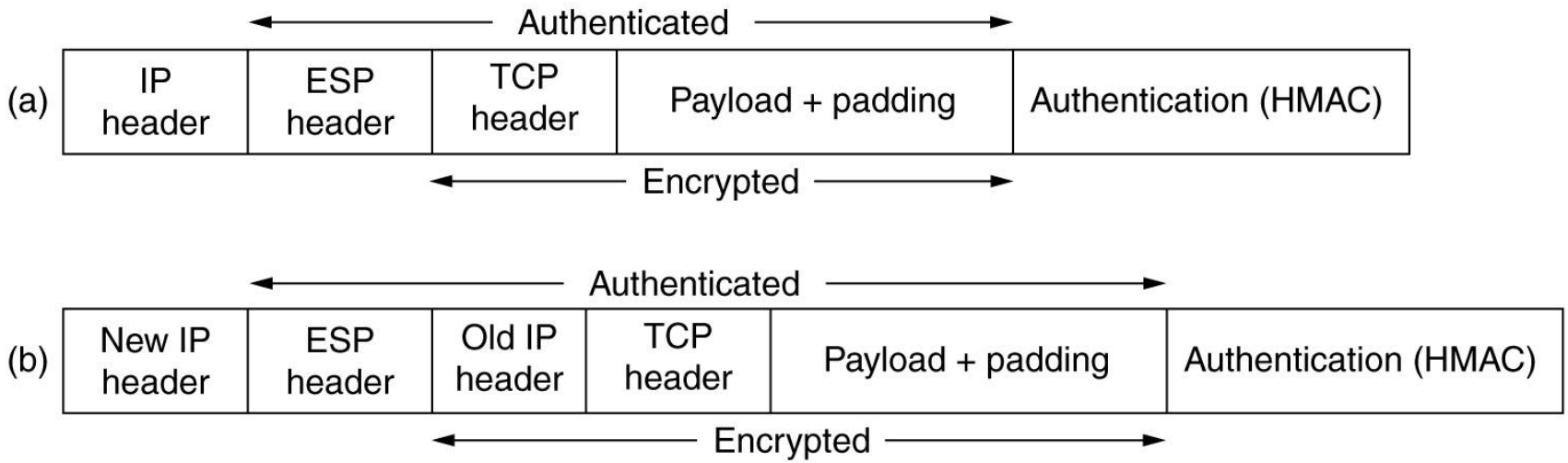
- This is a variable-length field that contains the Integrity Check Value (ICV) for this packet. The field must be an integral multiple of 32 bits in length.

- The authentication algorithm employed for the ICV computation is specified by the SA.

- For point-to-point communication, suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., DES) or on one-way hash functions (e.g., MD5 or SHA-1).

- The Use of HMAC-MD5-96 within ESP and AH, RFC 2403.
- The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404.

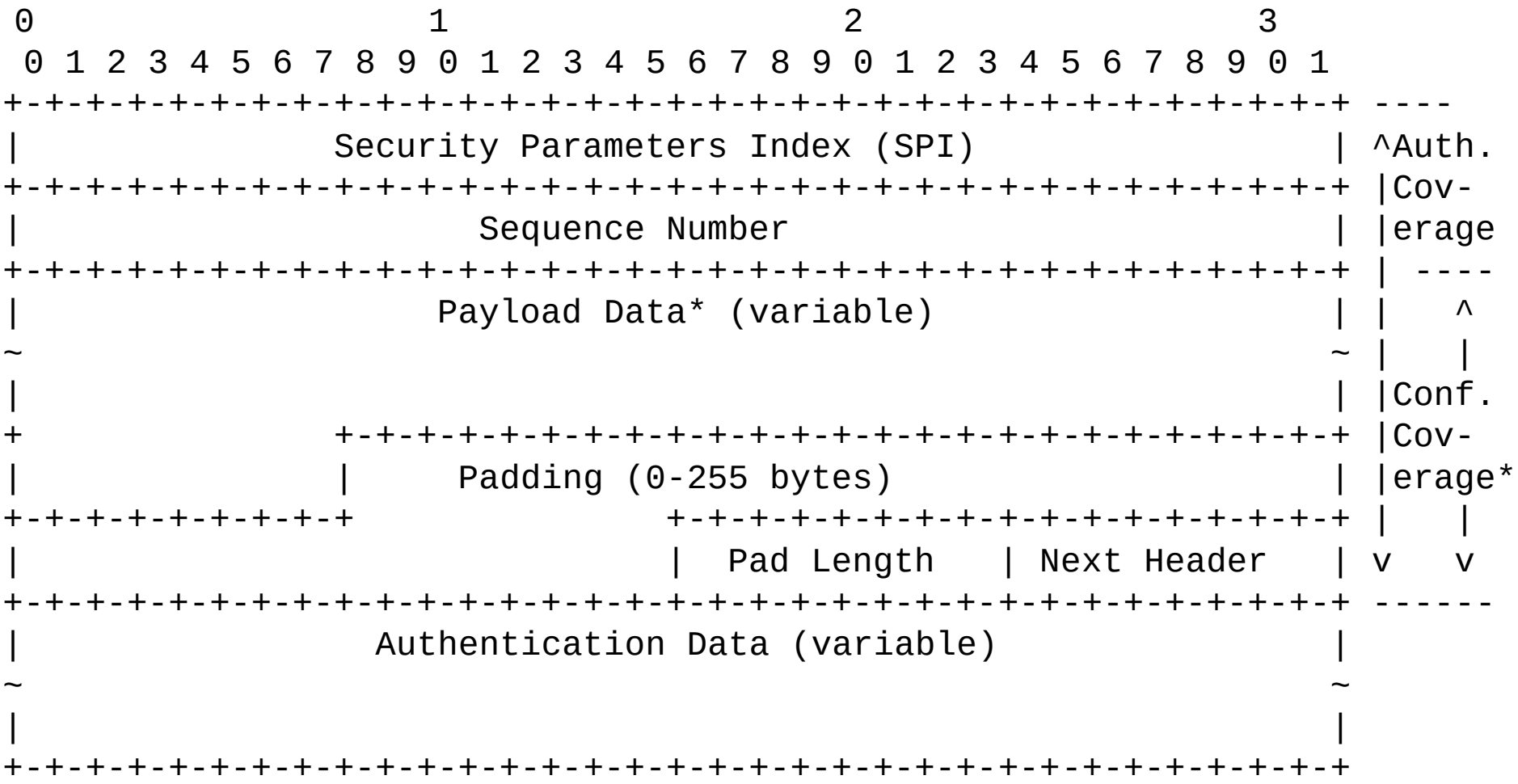
ESP : mode transport et mode tunnel



a) mode transport b) mode tunnel

The protocol header (IPv4, IPv6, or Extension) immediately preceding the ESP header will contain the value 50 in its Protocol (IPv4) or Next Header (IPv6, Extension) field.

ESP « header »


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Security Parameters Index (SPI)
Sequence Number
Payload Data* (variable)
Padding (0-255 bytes)
Pad Length
Next Header
Authentication Data (variable)
^Auth.
|Cov-
|erage
Conf.
Cov-
erage*

Politique de sécurité

• An SPD (Security Policy Database) must discriminate among traffic that is afforded IPsec protection and traffic that is allowed to bypass IPsec. For any *outbound* or *inbound* datagram, three processing choices are possible: discard, bypass IPsec, or apply IPsec.

• For traffic that is afforded IPsec protection, the SPD must specify the security services to be provided, protocols to be employed, algorithms to be used, etc.

• A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it.

• La politique de sécurité associe donc une SA à un certain type de trafic ; mais la RFC 2401 spécifie qu'on peut enchaîner plusieurs traitements (SA bundle), ce qui complique considérablement la norme…

Politique de sécurité (2)

• Les *sélecteurs* permettent d'identifier, dans la SPD, les différents types de trafic.

• Principaux sélecteurs : adresses IP source et destination, protocole de transport, ports source et destination, noms (DNS ou X.500) (?)

• Selectors may include *wildcard* or *range* entries and hence the selectors for two entries may overlap. (This is analogous to the overlap that arises with ACLs or filter entries in routers or packet filtering firewalls.) Thus, to ensure consistent, predictable processing, SPD entries MUST be ordered and the SPD MUST always be searched in the same order, so that the first matching entry is consistently selected. (This requirement is necessary as the effect of processing traffic against SPD entries must be deterministic) More detail on matching of packets against SPD entries is provided in Section 5…

SAD (Security Association Database)

- In each IPsec implementation there is a nominal Security Association Database, in which each entry defines the parameters associated with one SA. Each SA has an entry in the SAD.

- For outbound processing, entries are pointed to by entries in the SPD. Note that if an SPD entry does not currently point to an SA that is appropriate for the packet, the implementation creates an appropriate SA (or SA Bundle) and links the SPD entry to the SAD entry (see Section 5.1.1).

- For inbound processing, each entry in the SAD is indexed by a destination IP address, IPsec protocol type, and SPI.

SAD (2)

• For each of the selectors defined in Section 4.4.2, the SA entry in the SAD MUST contain the value or values which were negotiated at the time the SA was created.

• For the sender, these values are used to decide whether a given SA is appropriate for use with an outbound packet. This is part of checking to see if there is an existing SA that can be used.

• For the receiver, these values are used to check that the selector values in an inbound packet match those for the SA (and thus indirectly those for the matching policy). For the receiver, this is part of verifying that the SA was appropriate for this packet.

• These fields can have the form of specific values, ranges, wildcards, or "OPAQUE" as described in section 4.4.2, "Selectors".

• Note that for an ESP SA, the encryption algorithm or the authentication algorithm could be "NULL". However they MUST not both be "NULL".

SAD (3)

The following SAD fields are used in doing IPsec processing:

• Sequence Number Counter: a 32-bit value used to generate the Sequence Number field in AH or ESP headers. [REQUIRED for all implementations, but used only for outbound traffic.]

• Anti-Replay Window: a 32-bit counter and a bit-map (or equivalent) used to determine whether an inbound AH or ESP packet is a replay.

• AH Authentication algorithm, keys, etc.

• ESP Encryption algorithm, keys, IV mode, IV, etc.

• Lifetime of this Security Association: a time interval after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur.

IPSec et IPv6

• 1992 : the IAB (Internet Advisory Board) recommended replacing IP with the CLNP packet format, very similar to IP, standardized by ISO, with larger addresses.

• Certain very vocal IETF members wanted to invent their own header format.

• The new header format designed by IETF is IPv6, and because they've been designing it for so long, it is unfortunately not at all clear wether the world will ever migrate to IPv6.

• The IPv6 designers were frustrated that the world did'nt immediately deploy IPv6, after they spent 10 years designing it.

IPSec et IPv6 (2)

• Although bigger addresses are good for you, people don’t get excited about learning something new and doing radical changes to all their software if things are working. It just does’nt motivate people to turn their environment inside out.

• Especially when you consider the other thing you get by converting to IPv6, which is noninteroperability with the 600 million current Internet nodes.

• The IPv6 proponents hoped that IPSec would be the motivator for moving to IPv6.

• Some IPv6 advocates proposed making it illegal to make any improvements (including IPSec) to IPv4, so that if the world wanted any of the stuff IETF designed in the last 10 years, it would have to move to IPv6.

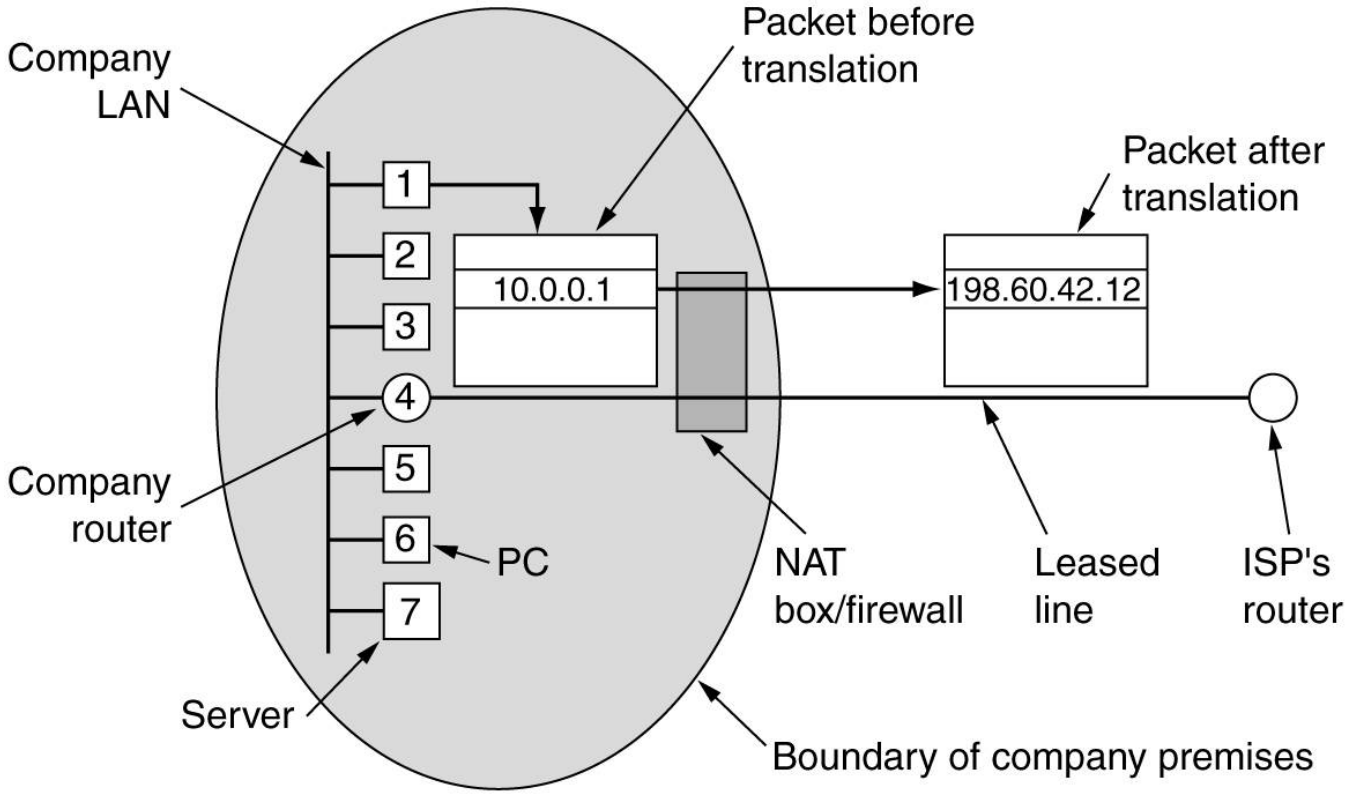
IPSec et IPv6 (3)

• The IPSec designers were more interested in security, and did’nt care wether it was deployed with 4-octet or 16-octet addresses, so they designed it to work with either format.

• The IPv6 specification says that IPSec is mandatory, so sometimes people claim that « Security is built into IPv6, whereas it’s an add-on to IPv4 ».

• In reality, IPSec works just as well with IPv4 and IPv6.

NAT – Network Address Translation



Placement and operation of a NAT box.

RFC 1918

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks.

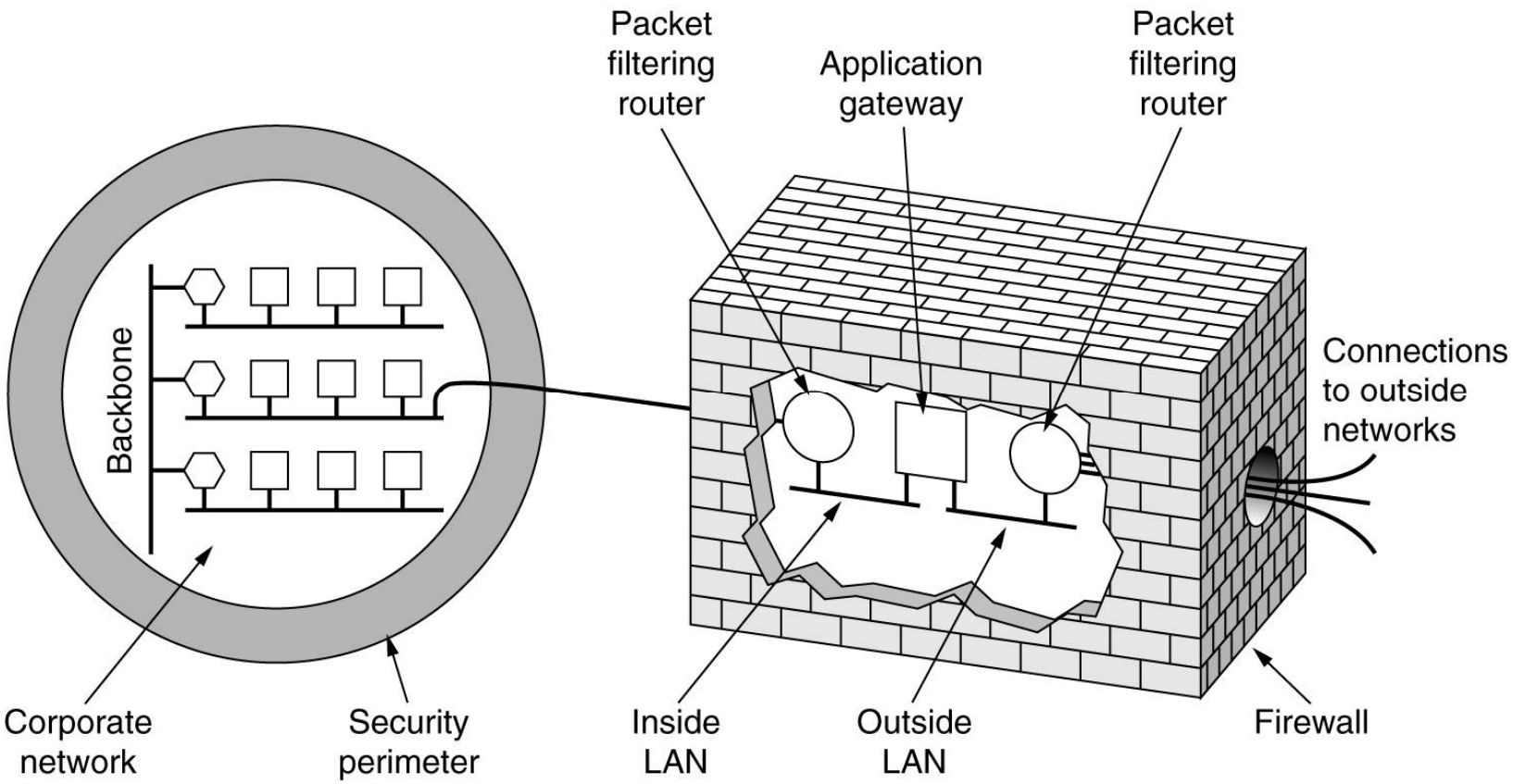
NAT (2)

• Everyone hates NAT, but NAT boxes are very popular because really what users want is for things to work and they don't care about architectural purity.

• NAT particularly infuriates the IPv6 proponents because it makes it possible for the world to delay migrating to IPv6.

• That is one reason they like AH, because the AH integrity check will fail if a NAT box modifies the IP header.

Firewalls



A firewall consisting of two packet filters and an application gateway.

Firewalls (2)

• Un pare-feu inspecte une partie du contenu des paquets (numéro de port, etc.), ce que le chiffrement empêche.

• IPSec *de bout en bout* (mode transport) souvent impossible (paquets détruits par les pare-feux).

• As much as people would like their traffic to be protected in transit, they’re even more anxious for their traffic to be delivered at all…

AH inutile ?

• At one of the final IETF meetings before AH and ESP were finalized, someone from Microsoft got up and gave an impassioned speech about how AH was useless given the existence of ESP, cluttered up the spec, and could’nt be implemented efficiently (because of the MAC in front of the data).

• Our impression of what happened next was that everyone in the room looked around at each other and said: « Hmm. He’s right, and we hate AH also, but if it annoys Microsoft let’s leave it, since we hate Microsoft more than we hate AH ».