Lecture 19: IPsec and VPN

COSC362 Data and Network Security

Book 1: Chapter 20 – Book 2: Chapters 9 and 22

Spring Semester, 2021

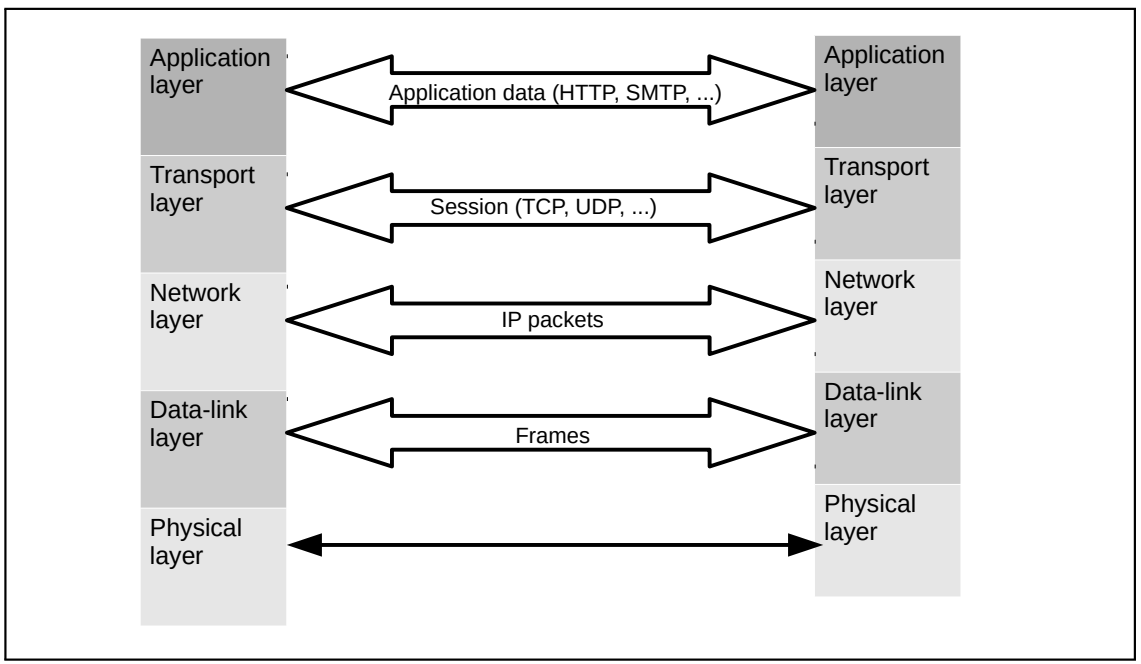
Motivation

- IP security (IPsec) is a framework for ensuring secure communications over IP (internet protocol) networks.
- Security services similar as TLS, but at a lower layer in the communication protocol stack.
- Security added to IPv4 and IPv6.
- Virtual private networks (VPNs) extend a private network across a public network and enable secure communication over the latter.

Outline

Outline

Cryptography in the TCP/IP Stack



- Application layer security: SSH, S-MIME, PGP, etc.
- Transport layer security: SSL, TLS.
- Network layer security: IPsec.
- Data-link layer security: WEP, WPA, WPA2, etc.

Introduction

- Standard: RFCs 4301-4305 (2005) with cryptographic algorithms updated in subsequent RFCs.
- Providing protection for any higher layer protocol, including arbitrary TCP and UDP sessions.
- Using encryption, authentication and key management algorithms.
- Commonly used to provide virtual private networks (VPNs).
- Providing a security architecture for both:
  - IPv4: RFC 791 (1981)
  - IPv6: RFC 8200 (2017)

Security Services

- *Message confidentiality:* Protecting against unauthorized data disclosure:
  - By using encryption mechanisms.
- *Message integrity:* Determining if data has been changed (either intentionally or unintentionally):
  - By using message authentication codes (MACs).
- *Limited traffic analysis protection:* Possibly difficult to know which parties are communicating, how often, or how much data is being sent when monitoring network traffic:
  - By concealing IP datagram details such as source and destination addresses.

Security Services

- *Message replay protection:* Data not delivered multiple times, and not delivered badly out of order.
- *Peer authentication:* Ensuring network traffic to be sent from the expected host:
  - Each IPsec endpoint confirms its identity of the other IPsec endpoint with which it wishes to communicate.

Gateway-to-Gateway Architecture

- Providing secure communications between 2 networks.
- Network traffic routed through IPsec connection, protecting it appropriately.
- Only protecting data between the 2 gateways.
- Often used when connecting 2 secured networks:
  - Example: Linking a branch office to headquarters over the Internet.
- Less costly than private wide area network (WAN) circuits.

Host-to-Gateway Architecture

- Commonly used to provide secure remote access:
  - Example: An organization deploys a VPN gateway onto its network.
- Each remote access user establishes a VPN connection between the local computer (host) and the gateway.
- The VPN gateway may be either a dedicated device or part of another network device.
- Often used when connecting hosts on unsecured networks to resources on secured networks.

Host-to-Host Architecture

- Typically used for special purpose needs:
  - Example: System administrators performing remote management of a single server.
- Providing protection for data throughout its transit (end-to-end).
- Resource-intensive to implement and maintain in terms of user and host management.
- All user systems and servers participating in VPNs need to have VPN software installed and/or configured.
- Key management through a manual process.

Types

- *Encapsulating security payload (ESP):* Providing confidentiality, authentication, integrity and replay protection.
- *Authentication header (AH):* Providing authentication, integrity and replay protection, but NOT confidentiality:
  - AH is now deprecated.
- *Internet key exchange (IKE):* Negotiating, creating and managing session keys in *security associations* (SAs).

IPsec Connection Setup

- Key exchange using IKEv2 protocol:
  - Standard: RFC 7296 (2014).
- IKEv2 uses a Diffie-Hellman protocol authenticated using signatures with public keys in X.509 certificates.
- Including *cookies* to mitigate denial-of-service (DoS) attacks:
  - Providing *Proof of Reachability* before any expensive cryptographic processing is completed.

Using cookies

RFC 7296 Section 2.6:

- Mechanism to mitigate the DoS attack called *stateless cookie*.
- When the server is under load, the initial request is responded with a calculated *stateless cookie*:
  - a value that can be re-calculated based on values in the initial request *without* storing responder-side state.
- The initial request is then expected to repeat, this time including the stateless cookie.

RFC 7296 Section 3:

- Addition of a *Proof of Work*:
  - by calculating a pre-image for a partial hash value.
- Setting an upper bound determined by the attacker's CPU to the number of negotiations it can initiate in a unit of time.

Security Associations

- Containing information needed by an IPsec endpoint to support an IPsec connection.
- Possibly including cryptographic keys and algorithms, key lifetimes, security parameter index (SPI), security protocol identifier (ESP and/or AH).
- SPI included in IPsec header to associate a packet with the appropriate SA.
- Telling the endpoint how to process inbound IPsec packets and/or how to generate outbound packets.
- Unidirectional: One SA for each direction of connection.
- IKEv2 to establish keys used in SAs.

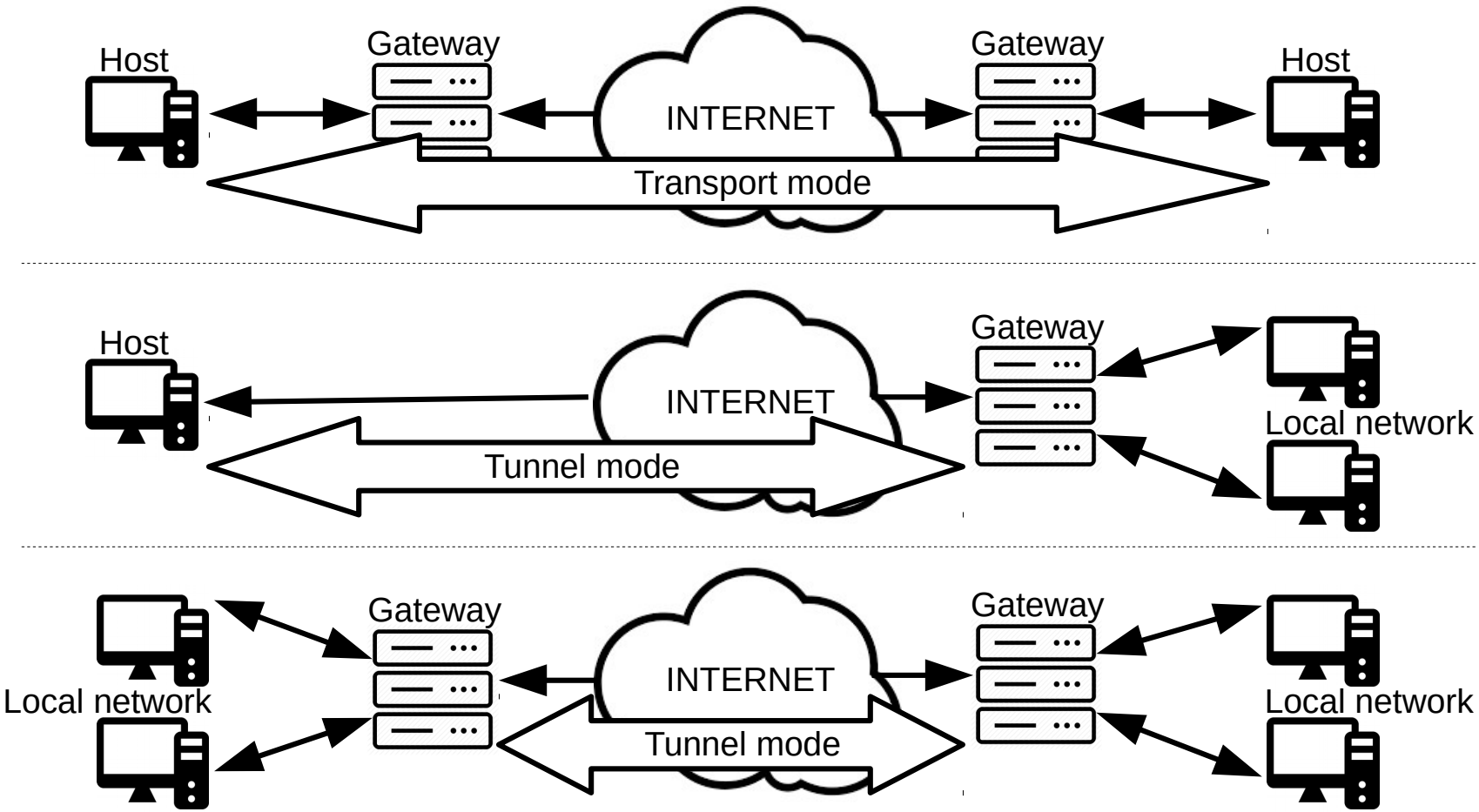
Cryptographic Suites

- Similar to TLS cipher suites:
  - Several standardised cryptographic suites, incorporating both public key and symmetric key algorithms.
- Specific groups are available for Diffie-Hellman (in finite fields and on elliptic curves).
- 3DES and AES used for encryption, either in CBC or GCM mode.
- HMAC or CMAC (variant) used for integrity if GCM mode is not used.

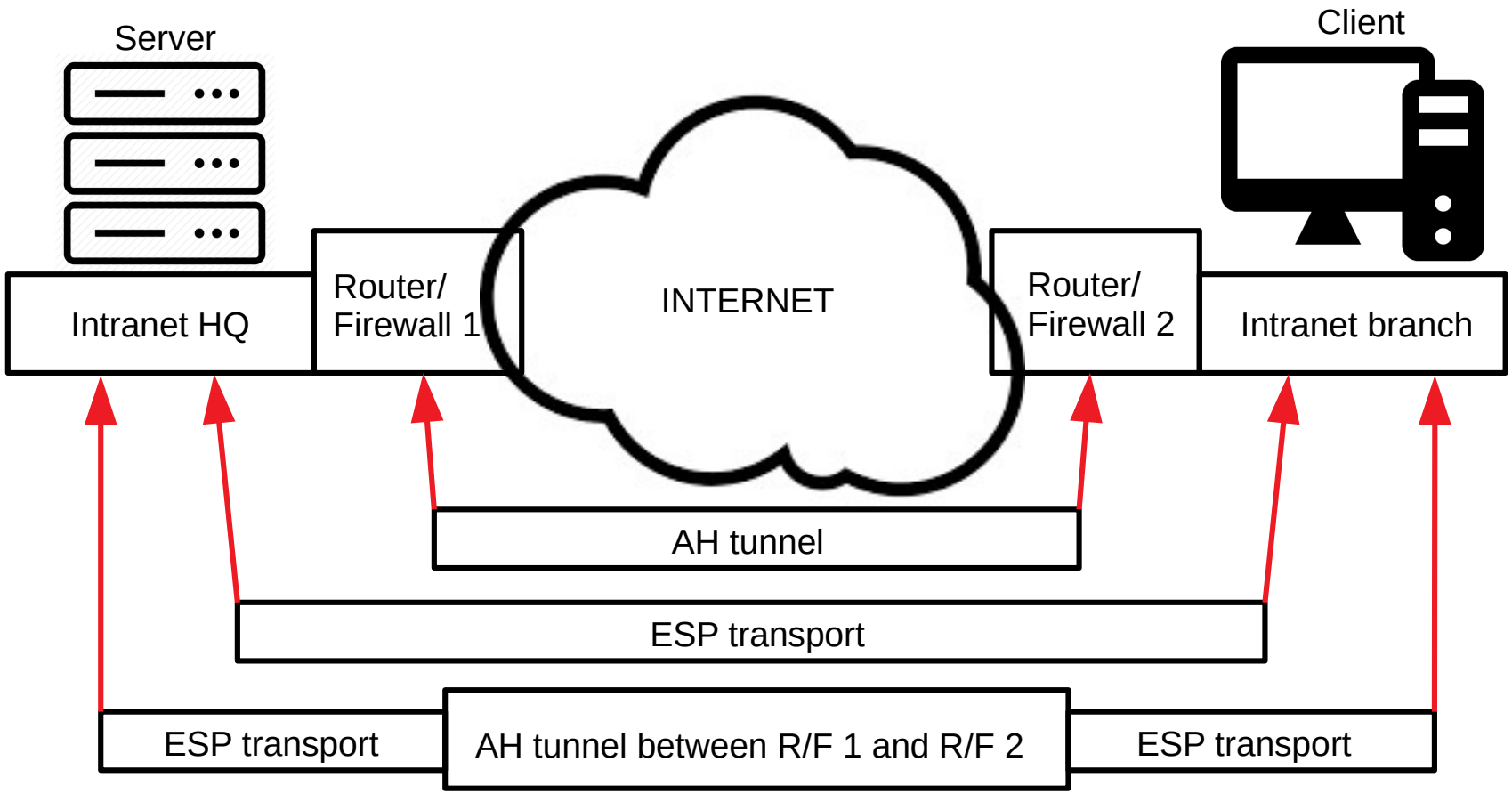
Modes of Operation

- Each protocol (either ESH or AH) can operate in either *transport* or *tunnel* mode.
- *Transport mode:* Maintaining IP header of the original packet and protecting the payload:
  - Generally used in host-to-host architectures.
- *Tunnel mode:* Encapsulating the original packet into a new one, and letting the payload be the original packet:
  - Generally used in gateway-to-gateway and host-to-gateway architectures.

Mode Overiew



Example

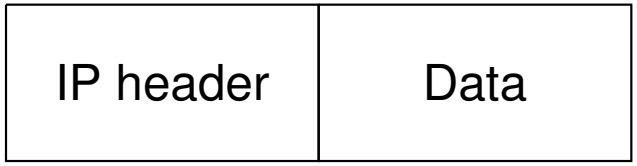

Server
Client
Intranet HQ
Router/
Firewall 1
INTERNET
Router/
Firewall 2
Intranet branch
AH tunnel
ESP transport
ESP transport
AH tunnel between R/F 1 and R/F 2
ESP transport

Components

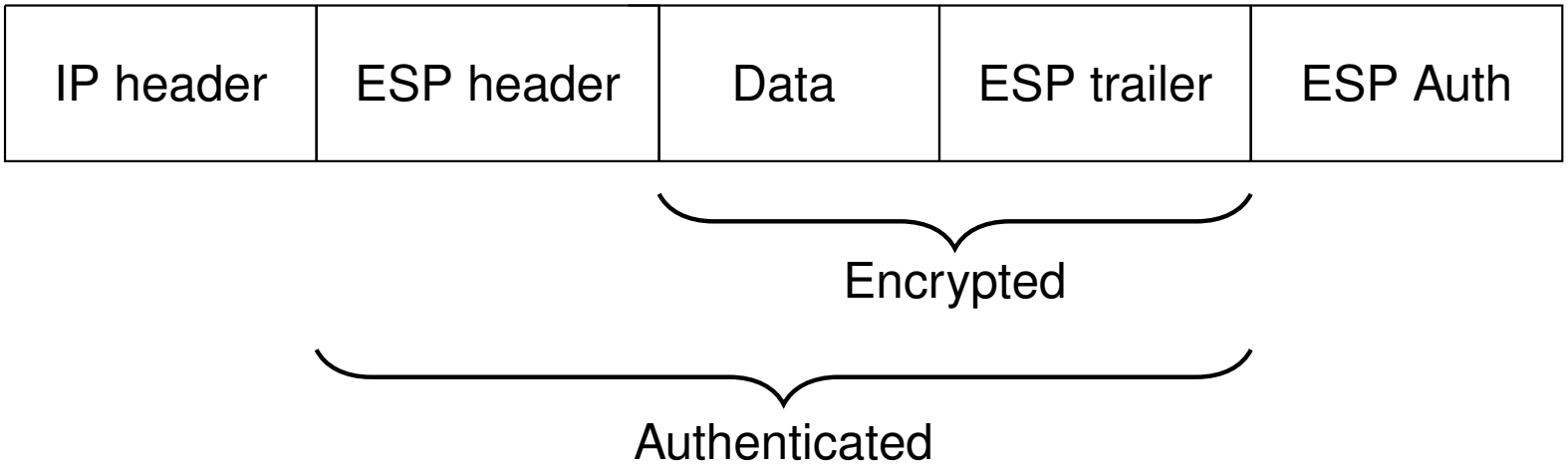
- *ESP header:* Containing the SPI identifying the SA and sequence numbers.
- *ESP trailer:* Containing padding and its length, and possibly including extra padding to enhance traffic flow confidentiality.
- *ESP auth:* Containing MAC of the encrypted data and ESP header:
  - Possibly not required if an authenticated encryption mode is used.

Transport Mode ESP

- Original IP packet:



- IP packet protected by transport mode ESP:



Pictures for IPv4 (slight differences for IPv6)

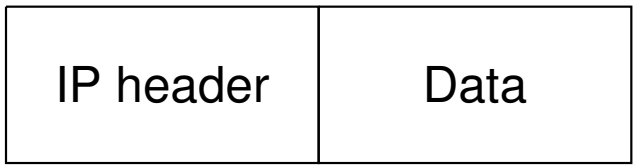
Transport Mode ESP

Outbound packet processing:

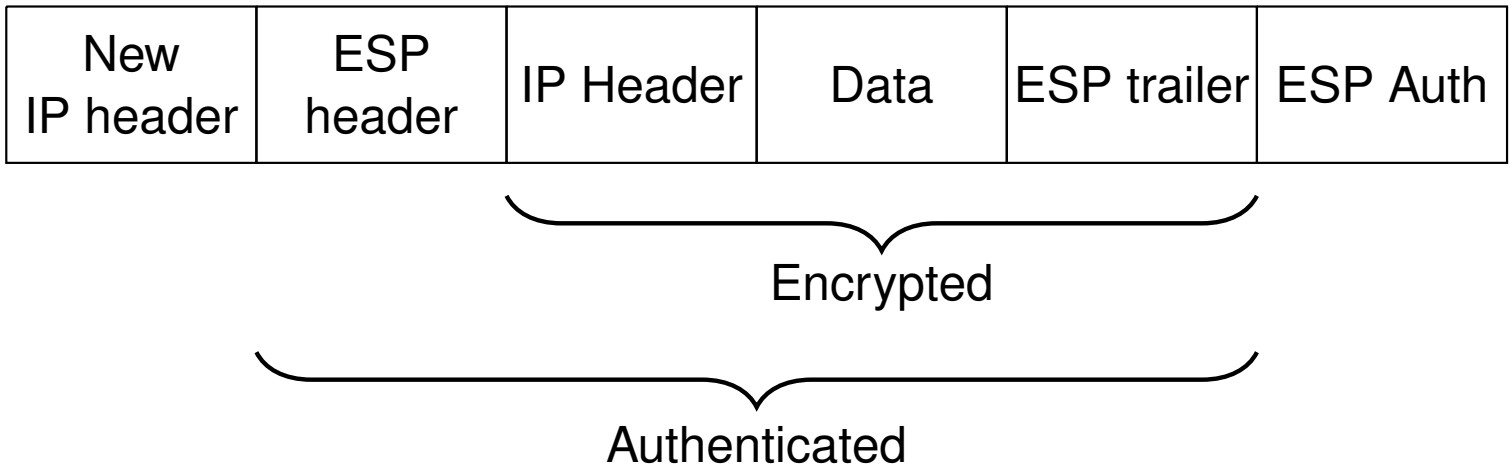
- Data after original IP header:
  - Padded by adding an ESP *trailer*.
  - Encrypted using symmetric cipher and key agreed in the SA.
- ESP *header* prepended.
- If SA uses the authentication service, then:
  - ESP MAC calculated over the data prepared so far and appended.
- Original IP header prepended BUT some fields must be changed:
  - Protocol field changed from TCP to ESP.
  - Total length field changed to reflect the addition of ESP header.
  - Checksums recalculated.

Tunnel Mode ESP

- Original IP packet:



- IP packet protected by tunnel mode ESP:



Pictures for IPv4 (slight differences for IPv6)

Tunnel Mode ESP

Outbound packet processing:

- Entire original packet:
  - Padded by adding an ESP *trailer*.
  - Encrypted using symmetric cipher and key agreed in the SA.
- ESP *header* prepended.
- If SA uses the authentication service, then:
  - ESP MAC calculated over the data prepared so far and appended.
- A new outer IP header prepended:
  - Inner IP header of original IP packet carrying the *ultimate* source and destination addresses.
  - Outer IP header may contain distinct IP addresses (e.g. addresses of security gateways).
  - Outer IP header protocol field set to ESP.

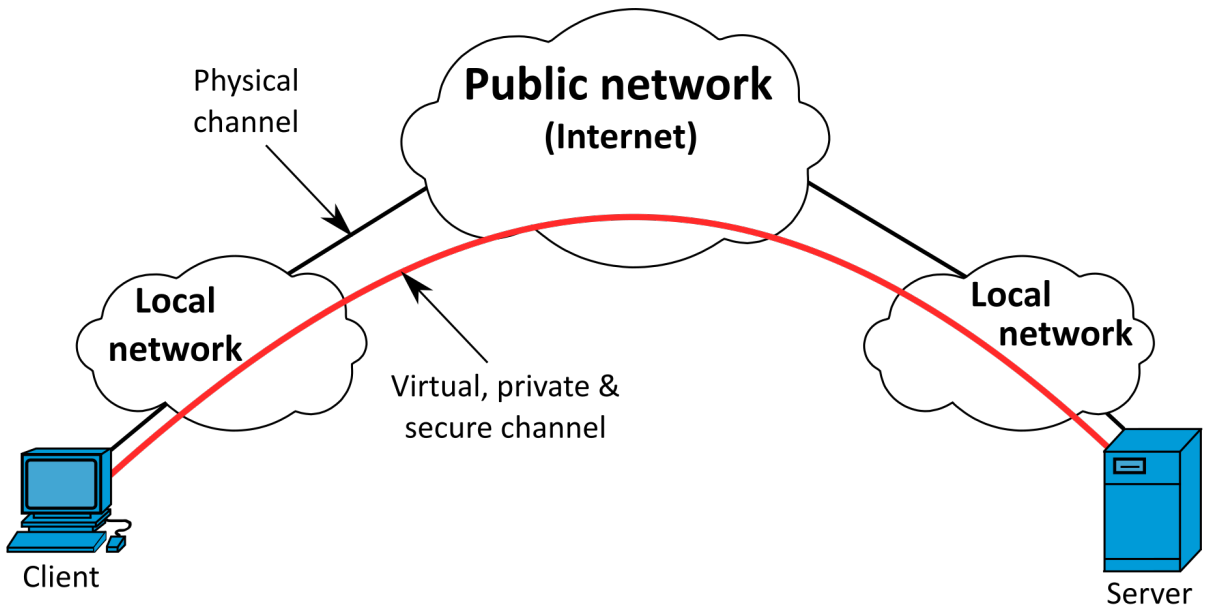
Security

- Active attacks exist for *encryption-only* mode of ESP protocol:
  - Providing encryption without integrity is known to be insecure.
  - Unlike earlier IPsec versions, the 2005 version does not require implementations to support encryption-only modes, but still allows it.
- Attacks due to MAC-then-encrypt configurations:
  - AH applies encryption *after* MAC (*MAC-then-encrypt*).
  - ESP applies encryption *before* MAC (*encrypt-then-MAC*).

Outline

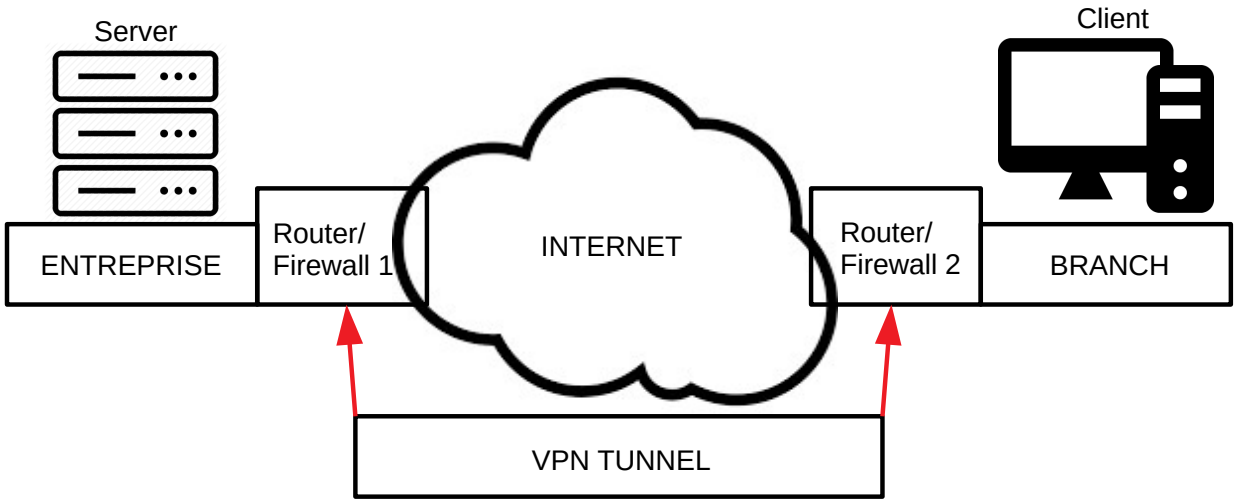
Introduction

- Providing a secure distributed network.
- Creating secure channels over the insecure Internet.
- Types:
  - Branch office interconnect (Intranet VPN)
  - Supplier/business partner access (Extranet VPN)
  - Remote access



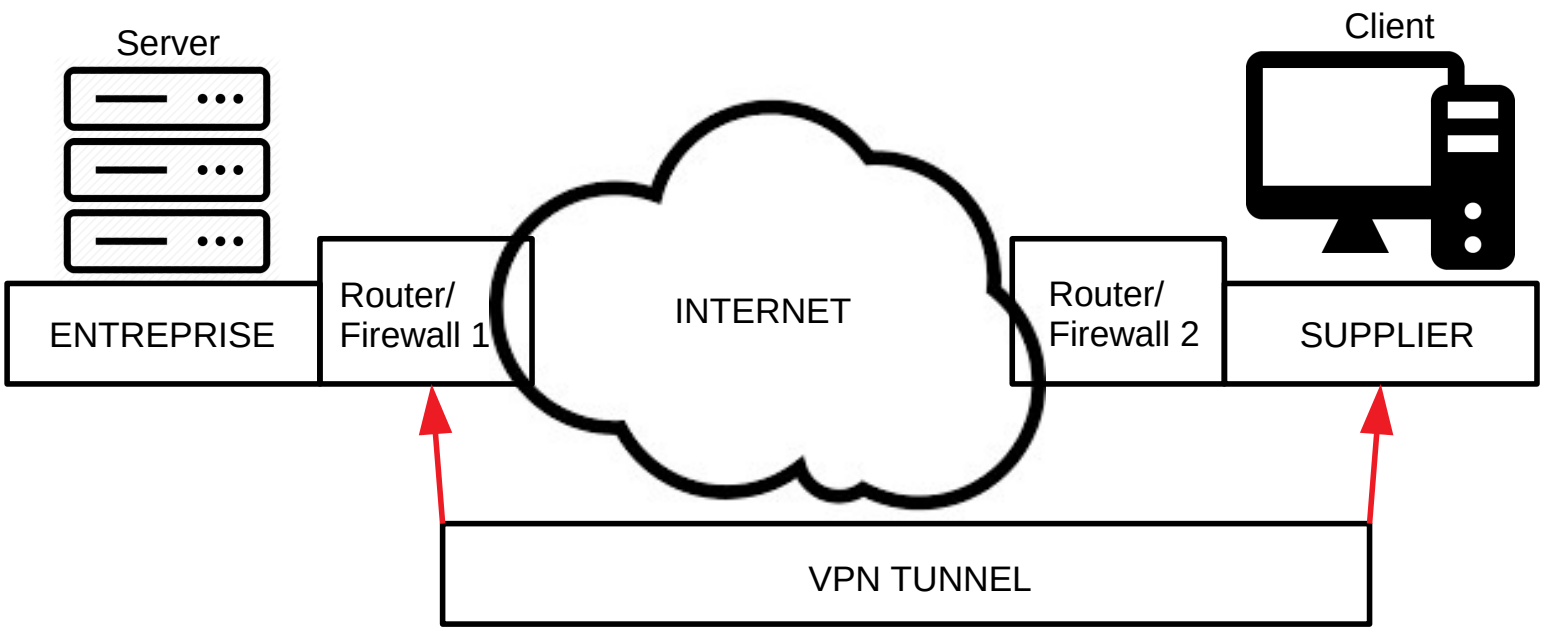
Branch Office Interconnect

- Establishing a VPN tunnel between router/firewall 1 and router/firewall 2:
  - Using AH to authenticate data from tunnel endpoints (routers/firewalls).
  - Using ESP to encrypt data over the Internet.
- Only routers/firewalls need to support IPsec:
  - No change to Intranet resources.



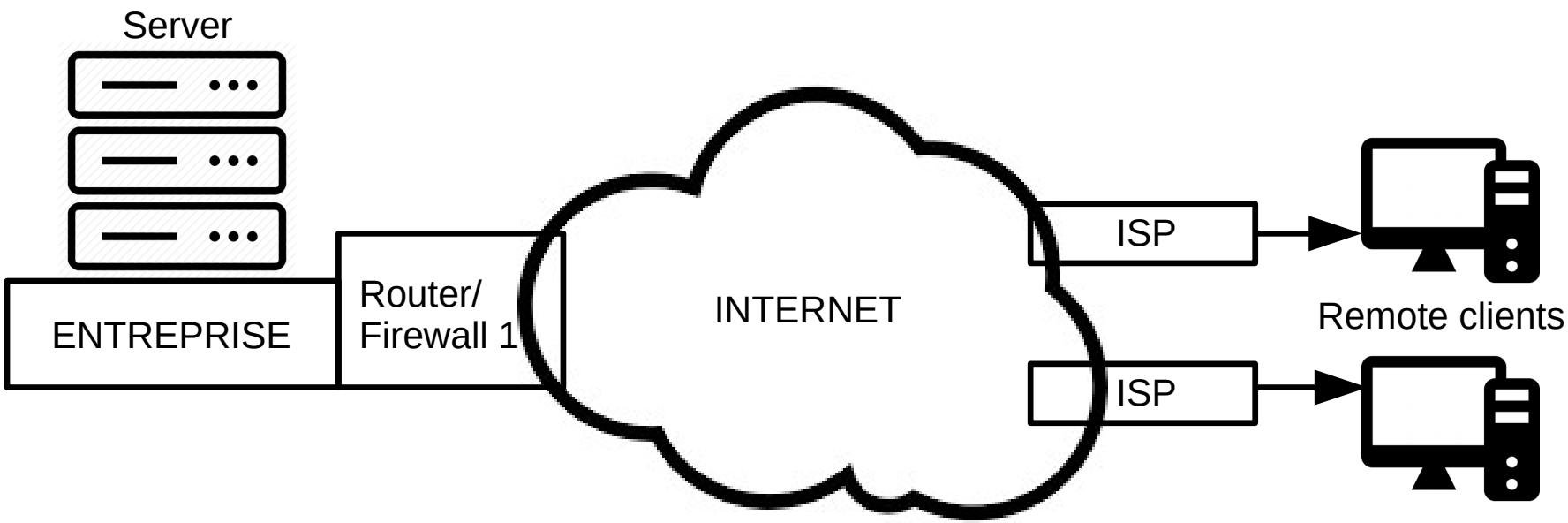
Supplier Network

- Supplier may not be part of the entreprise:
  - VPN extended to operate between router/firewall 1 and individual parts of supplier network.

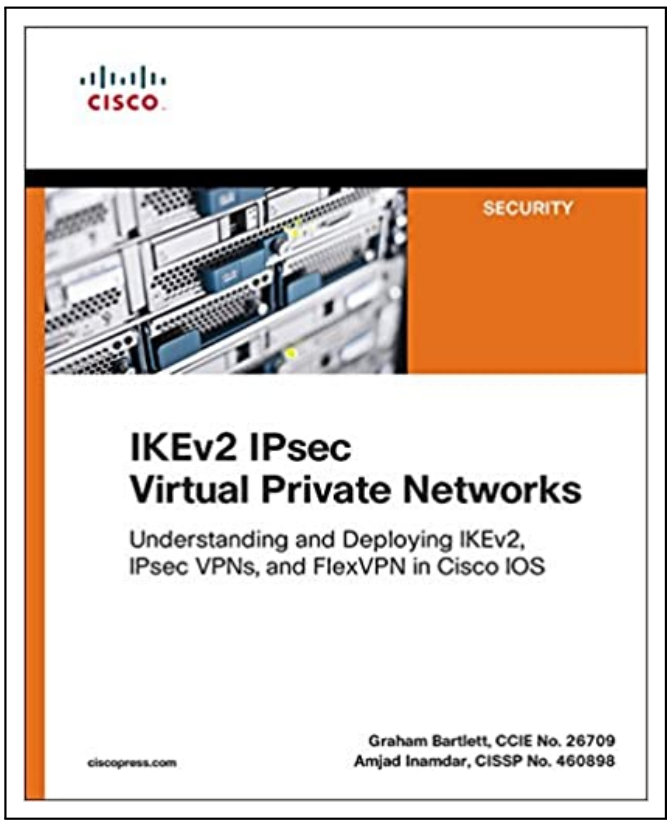


Remote Access

- Internet service providers (ISPs) can provide VPN services across the untrusted Internet.



IKEv2 VPN



- Most recent and now very common in commercial equipment.
- Simple configuration and use with modern Windows and Linux systems, as well as mobile phones.