Firewalls and Tunnels

Presented by
Group: 07

Group Members:

Saima Jahan Sultana (18701005)
Sadia Tahsin (18701014)
Nuzat Tasnim (18701024)
Sultana Tasnim Jahan (18701051)
Afrin Sultana (17701007)

Department of Computer Science & Engineering
University of Chittagong

August 11, 2022

Outline

- Firewalls
- Packet-Filter Rules And Actions
- Proxy Firewalls and Firewall Architectures
- SSH: Secure Shell
- VPNs And Encrypted Tunnels
- VPN(Virtual Private Networks)
- VPN Designs
- IPsec: IP Security Suite
- IPsec Operation Modes

Firewalls

A Firewall is a network security device that **monitors and filters incoming and outgoing network traffic** based on an organization's previously established security policies. Mainly, a firewall is essentially the barrier that sits between a private and the public Internet.

A **network security firewall** is a gateway providing access control functionality that can allow or deny, and optionally modify, data passing between two networks, or a network and a device.

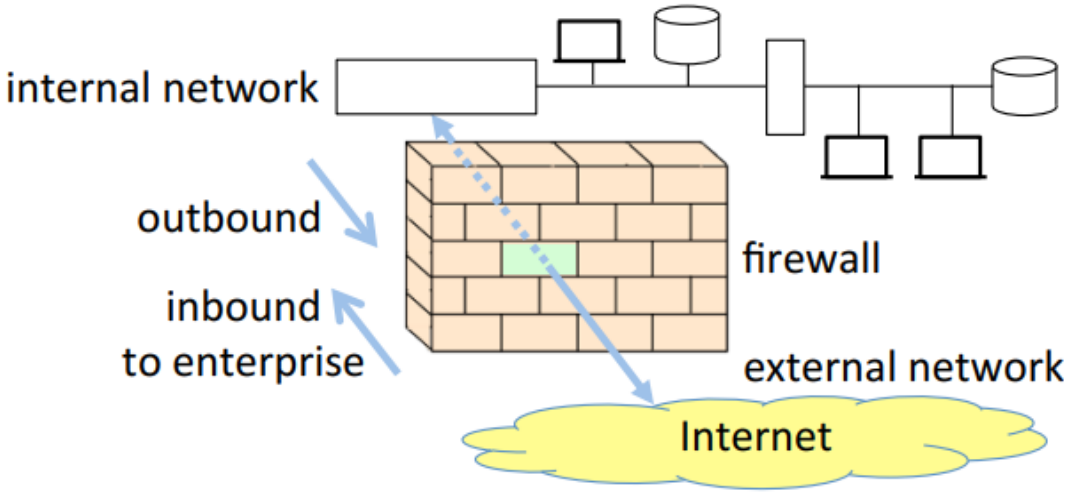

Figure: Network firewall (basic model)

Packet-Filter Rules And Actions

A packet-filter firewall contains a list of rules. The action is taken if rule satisfies. The primary actions are:

- **ALLOW (permit packet to pass)**: It supports **host-to-host** packet pass.
- **DROP (silently discard)**: the packet—a type-1 deny.
- **REJECT (drop but also try to inform the source)**: the packet—a type-2 deny.

Stateless And Stateful Filters:

- In a simple **stateless packet filter**, each packet is processed **independently** of others (with no dependency on prior packets).
- A **stateful packet filter** keeps track of selected details. It also called **dynamic packet filters**

Proxy Firewalls and Firewall Architectures

Two critical properties in firewall proxies:

- Transparency: The user experience is unchanged
- Performance: Performance degradation must be limited.

Packet-filtering

- Examine IP and TCP header
- Less secure

Packet-filter often combined with:

- Circuit-level proxy
- Application-level filters

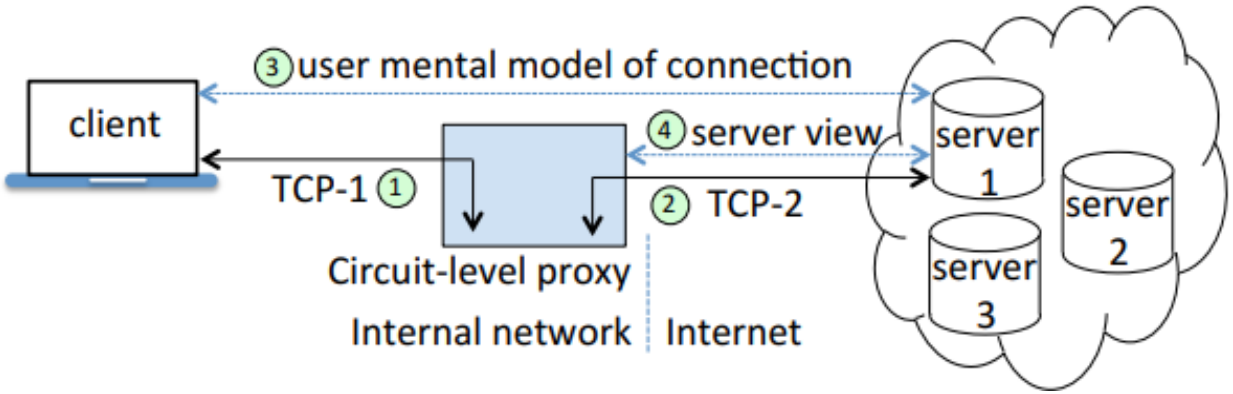

Figure: Circuit-level proxy firewall

Proxy Firewalls and Firewall Architectures (Cont.)

Circuit-level firewall:

- Work at the session layer
- Monitor TCP handshaking
- No end-to-end TCP connection
- No content checking

Application-level gateways:

- Work at application layer
- Filter traffic
- Include blocking packets
- Alter payloads

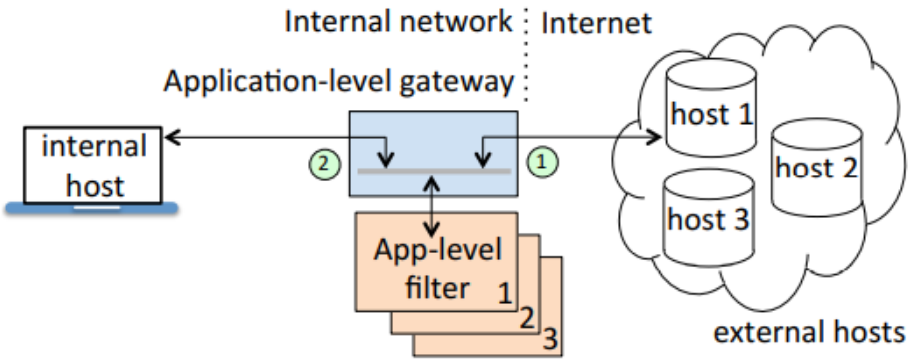

Figure: Application-level gateway filters

SSH: Secure Shell

The Secure Shell Protocol is a cryptographic network protocol. SSH provides a **security tunnel** by its own transport layer protocol, protecting both login passwords sent to remote services, and other data to be transported by TCP.

SSH is implemented in three parts:

- Transport layer protocol
- User authentication protocol
- Connection protocol

SSH: Secure Shell(Cont.)

Some **Client authentication methods** the clients of an SSH server may use:

- Client password (static, or OTP)
- Kerberos ticket obtained from a Kerberos server
- Client public key (described next)

SSH Port Forwarding: SSH port forwarding is a mechanism in SSH for tunneling application ports from the client machine to the server machine, or vice versa.

VPNs And Encrypted Tunnels

TCP/IP packets are plaintext.The existing networking protocols rely on plaintext header fields.Thus, to encrypt entire packets is not possible. An alternative is to encrypt the payload data only. A common strategy for this is tunneling.

Tunneling means one data stream's journey (the inner) being facilitated by another. It is a process encapsulation of one protocol by another — first protocol (header plus payload) is the payload of a second, the second prefixing a new (outer) header.

Two widely used technologies often viewed as security tunnels are:

- SSH, and
- IPsec

Encrypted tunnels are used to secure data that transits untrusted networks, and for VPNs.

VPN(Virtual Private Networks)

A **private network** is a network intended for access only by trusted users, with security (e.g., confidentiality, integrity) relying on a network architecture providing physical isolation.

A **virtual private network** is a private network typically uniting physically distant users or subnetworks, secured by not physical isolation but use of encrypted tunnels and special-purpose protocols software, and hardware including firewalls or gateways

VPN Designs

VPN design is of two types.

- **Transport mode**: It supports **host-to-host** architecture and provides end-to-end security.
- **Tunnel mode**: Tunnel mode involves network gateways.It supports two types of architecture.

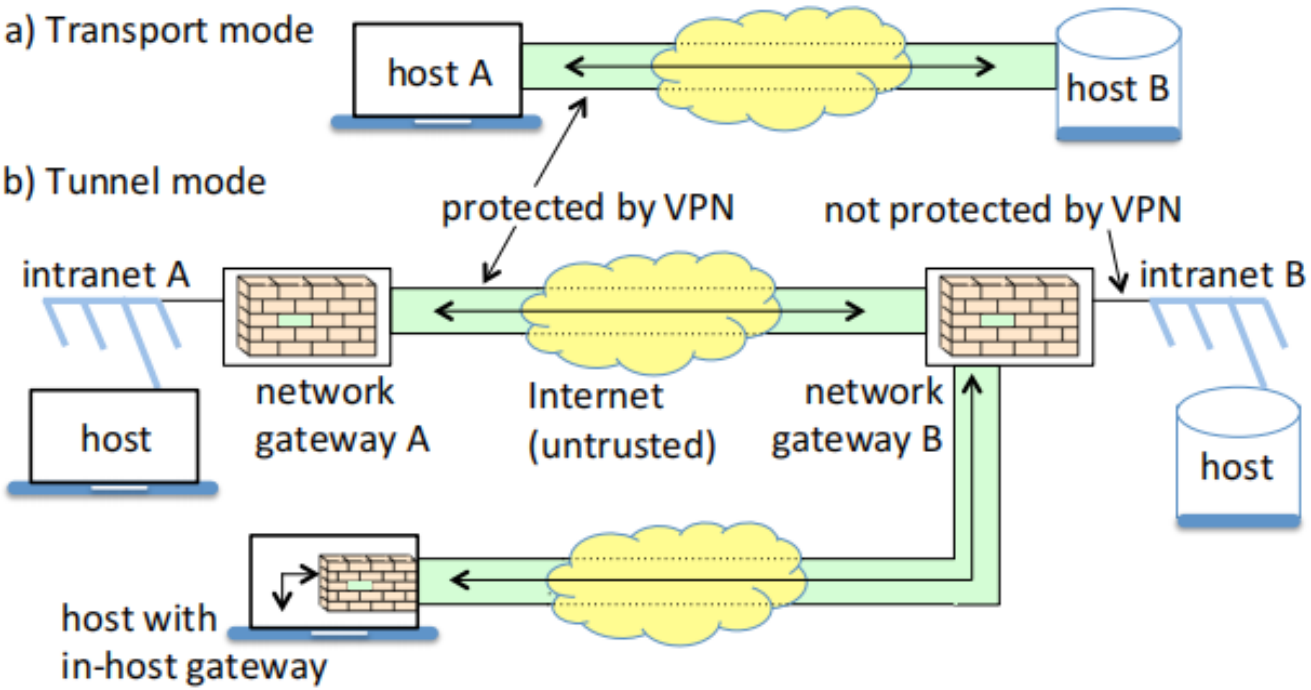

Figure: VPN designs

IPsec: IP Security Suite

The IPsec(IP Security suite) protocols provide network-layer security services that are inherited by transport and application layer protocols

IPsec enables VPNs through a broad and flexible suite of security services delivered by following three protocols

- **IKE:** Internet Key Exchange
- **AH:** Authentication Header
- **ESP:** Encapsulating Security Payload

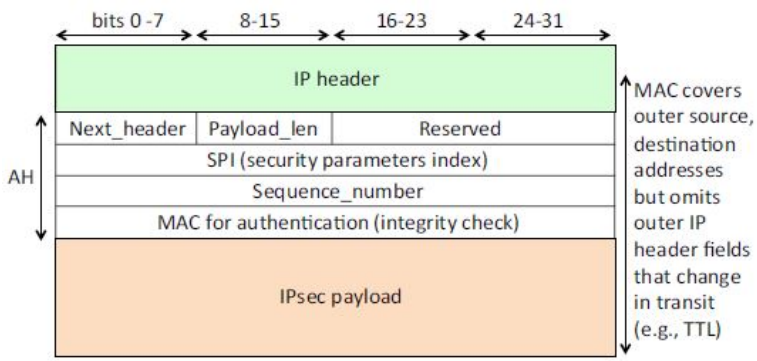

Figure: IPsec AH field view

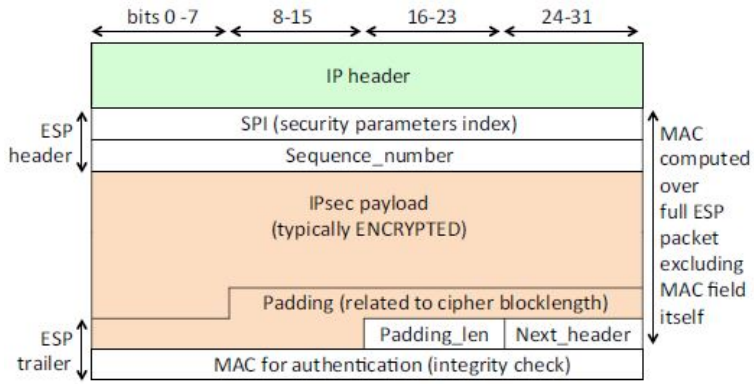

Figure: IPsec ESP field view

IPsec Operation Modes

Transport Mode

IPsec transport mode is used to provide an **end-to-end** VPN from one host to another host

Tunnel Mode

IPsec tunnel mode has two VPN use cases **network-to-network** VPNs, and **host-to-network** VPNs

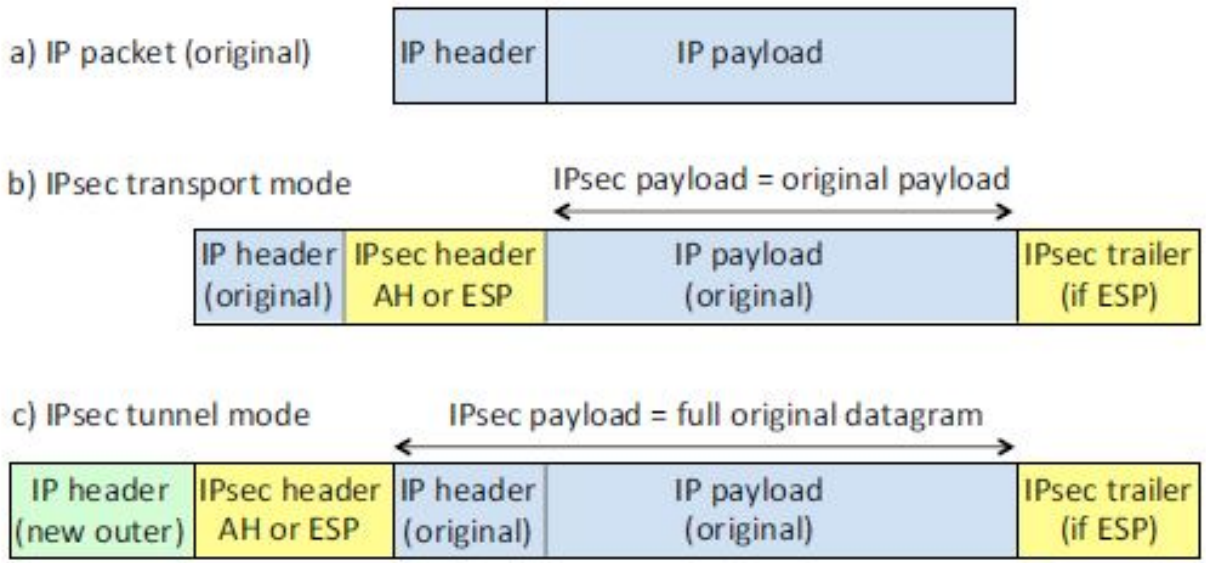

Figure: IPsec transport mode vs. tunnel mode (structural views)