Network Security

Note Title

2/7/2011

Announcements

- Computer Security talk of interest (need to reserve a spot)
  evening of March 10 - extra credit
- Next DETER exercise won't be in class
  (I'll post it later today)
  - due in 2 weeks

OSI Model

high

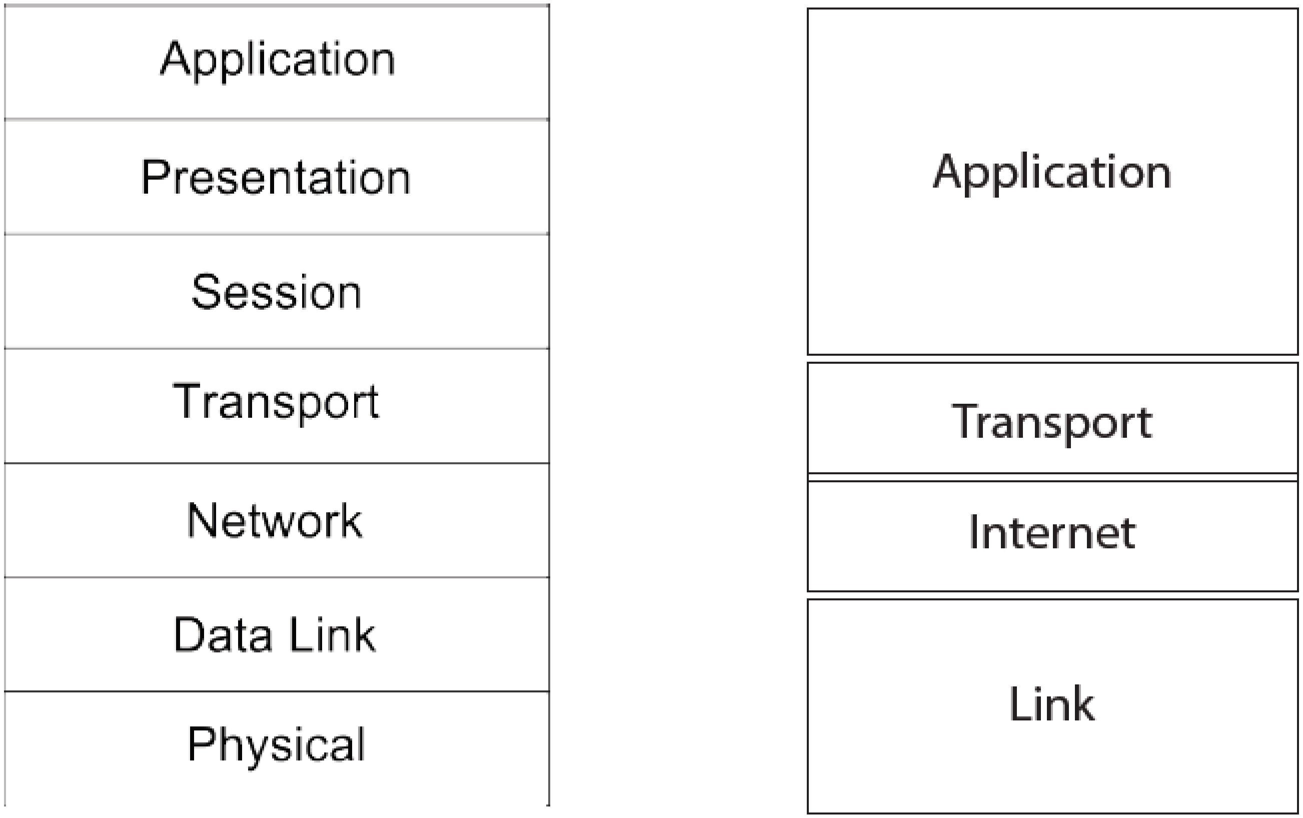
Application	user application interaction
Presentation	structure representation
Session	session checkpointing and recovery
Transport	reliability
Network	logical addressing, routing
Data Link	physical addressing, 802.11
Physical	media, signal, binary transmission

low

TCT/IP

The internet protocol suite, called TCP/IP, is an implementation of the OSI.

While it doesn't use as fine of a granularity as OSI, it does differentiate between "levels" of the computer.



Application

Presentation

Session

Transport

Network

Data Link

Physical

OSI Model

Application

Transport

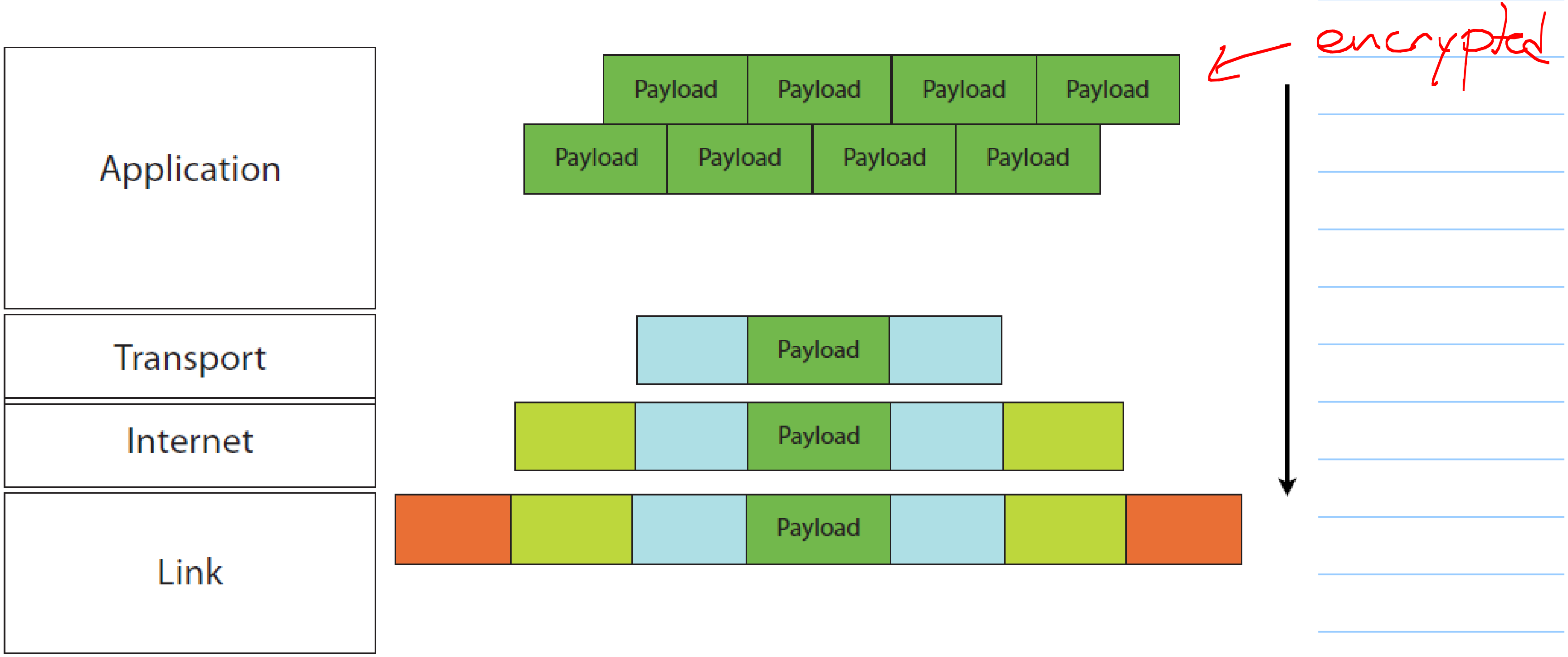
Internet

Link

TCP/IP

Transmitting Data

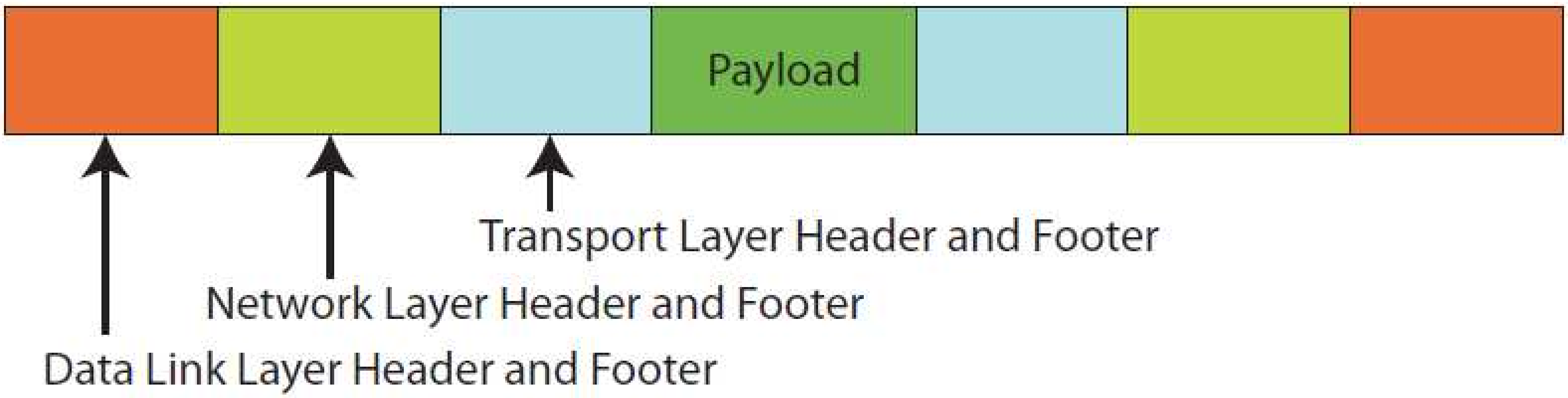
Data is divided into packets, and each layer adds its own headers & footers.



encrypted

Security view

- Certain areas of these headers and footers are more interesting from a security standpoint



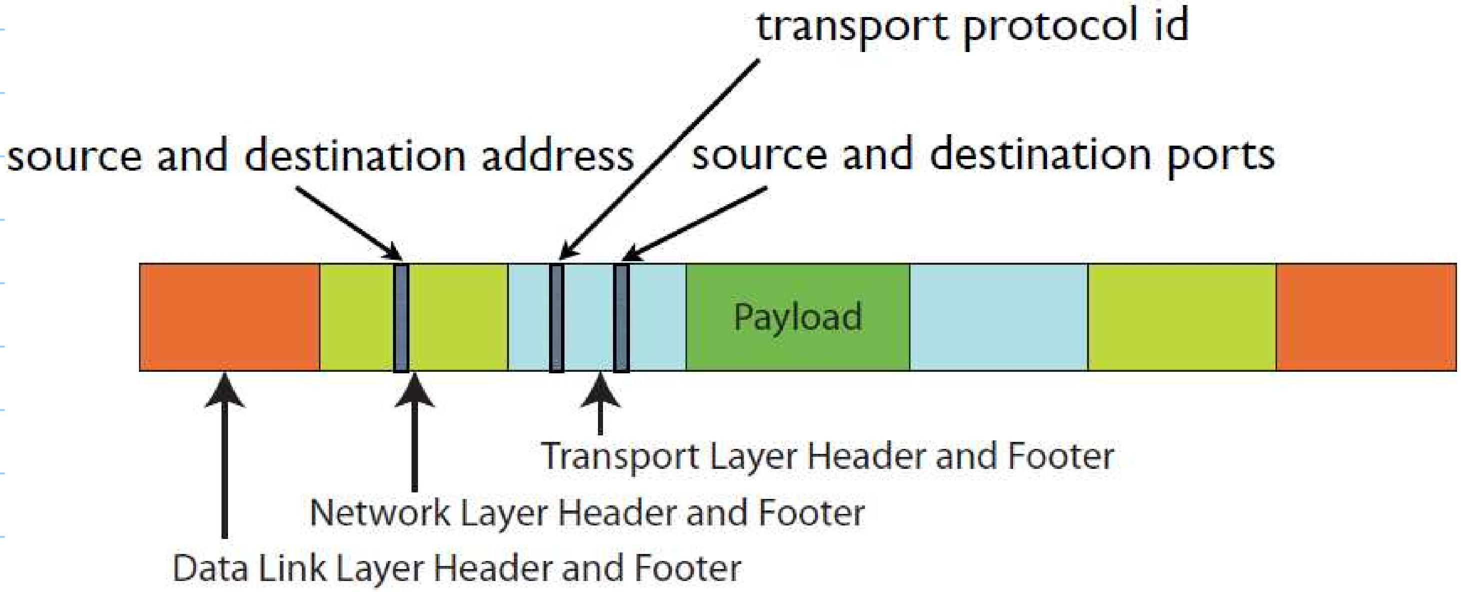
Payload

Transport Layer Header and Footer

Network Layer Header and Footer

Data Link Layer Header and Footer

Well, what information could a hacker use to interfere with this or gain access to illicet information?


transport protocol id
source and destination address
source and destination ports
Payload
Transport Layer Header and Footer
Network Layer Header and Footer
Data Link Layer Header and Footer

Two issues

① System Protection

Firewalls ✓

Want the computers to stay safe

② Hiding Information

IPSec ✓

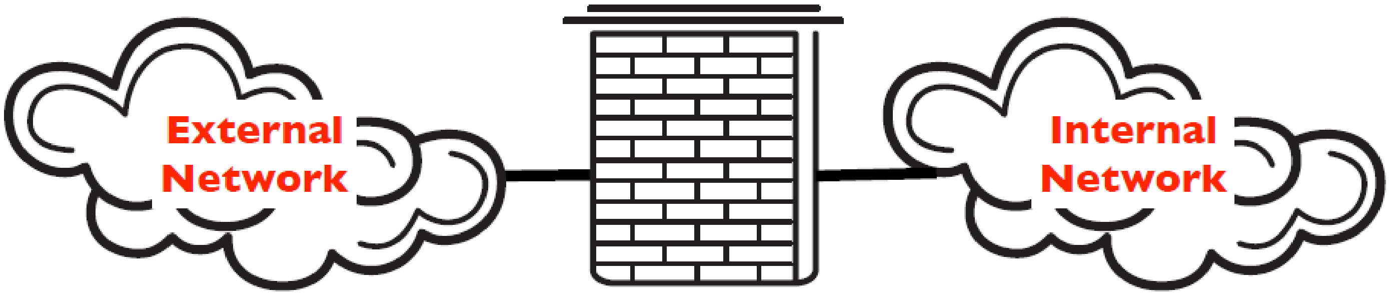
Want our connections + information to stay safe.

Firewalls

All traffic from the inside network to the outside must pass through the firewall computer.

Ideally: Firewall will protect internal computers from all sources of attacks.

single firewall



Packet Filtering Firewall

Rules are based on the packet headers.

Examples

Allow all traffic to port 23.

Allow traffic to port 23 only from a specific IP.

- Based on IP address, Port number, based on request authorizations.

(check text)

Proxy (or Stateful) Firewall

In general, TCP connections fix a port number for all communication.

Higher number ports are reallocated as needed for these connections.

Stateful firewalls track established TCP connections, and only allow traffic to specific ports for the duration of one connection.

Port numbers under 1024 are restricted,

Anything up to 65,535 are fair game

Gateway Servers

Proxies or gateway servers are often set up for / even stricter monitoring.

Applications are not allowed to connect directly to the internet.

Instead:

- computer requests a webpage
- All http connections get routed to a proxy
- The proxy computer connects to webpage for me, + forwards traffic

Proxy advantages:

- Allows much stronger control
- Can speed up webbrowsing & other services

Proxy disadvantages

- Slow
- User unfriendly

Additional options

- Host-based firewall
  - Dedicated servers
  - large set of machines to monitor
- Personal firewall
  - run on a single machine
  - come by default on any OS

Example : iptables

A native Linux firewall tool.

Can be run on an individual machine, or on a server to protect larger networks.

This is the focus of our next lab.

```
$ iptables -t filter -A INPUT -m state --state NEW -p tcp -s 192.168.0.1 --dport 23 -j REJECT
```

`iptables`

We're going to use the iptables tool to insert a new rule into netfilter.

`-t filter`

This rule is going to go in the filter table, which is the built-in packet filtering table. This rule will apply only to:

`-A INPUT`

packets that have been put into the `INPUT` *chain either by the kernel or by some previous rule and which:*

`-m state --state NEW`

represent a new connection,

`-p tcp`

are Transmission Control Protocol (TCP) packets,

`-s 192.168.0.1`

are from the host 192.168.0.1,

`--dport 23`

and are destined for port 23.

`-j REJECT`

Reject any matching packet. Processing of all packets matching this rule will instantly jump to the built-in target REJECT, which means that the packet will be rejected by the kernel with some kind of network error message.

Firewall Configurations

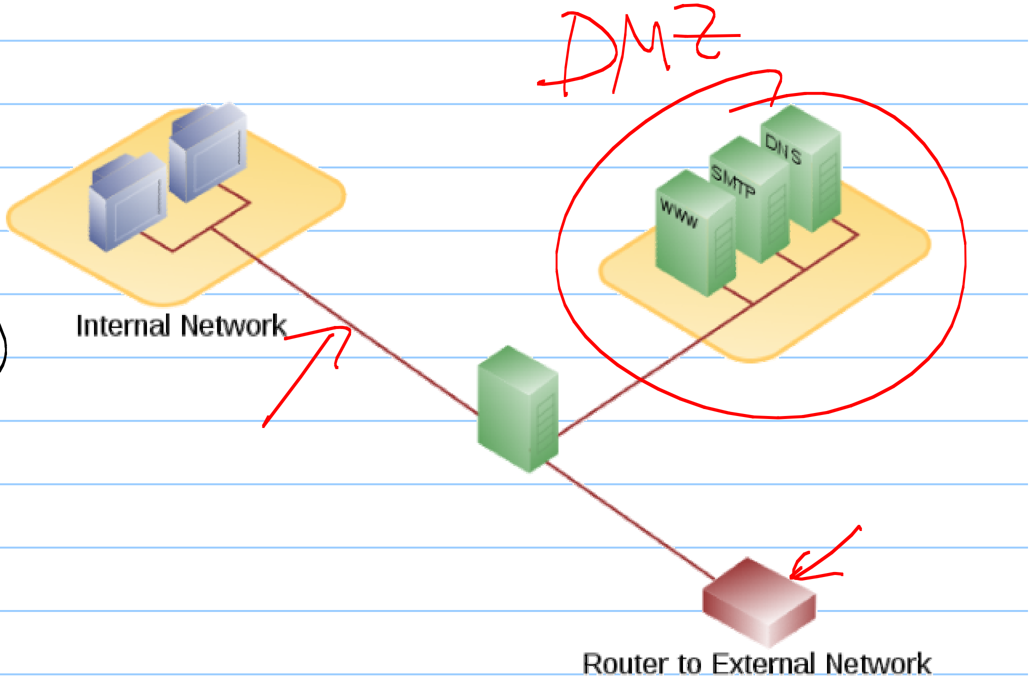
DMZ - "Demilitarized Zone"
A portion of the network between a secure internal network and external internet, with a firewall on each side

Typically contains:

- Web site hosting
- Email servers
- "High risk services"

Goal:

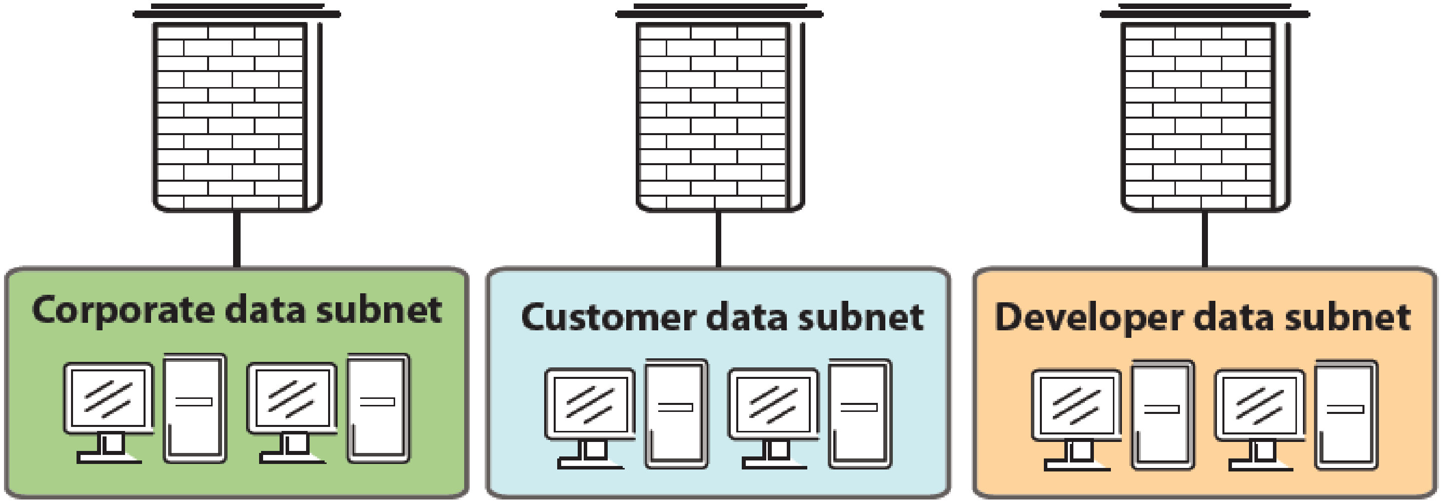
- Restrict & monitor communications to the DMZ (from both directions!)



(picture courtesy of Wikipedia)

Ideally: Even behind DMZ, each area is kept separate.

Why? Keep vulnerabilities separate.



Other Elements of Firewalls (& the DMZ)

- Intrusion Detection Systems (Ch. 6)

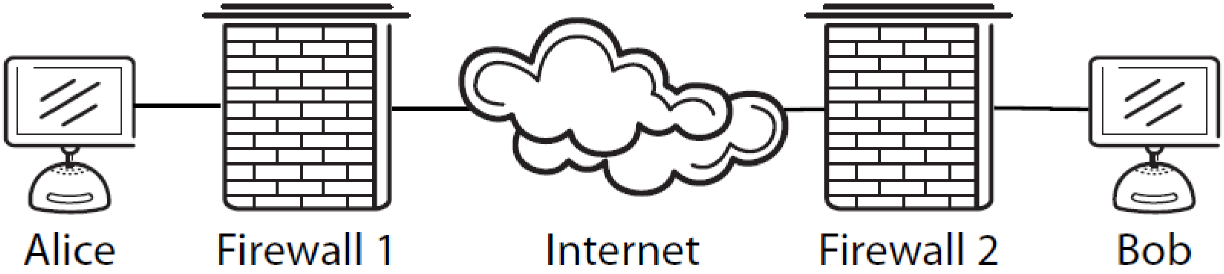
  Systems which look for unusual behavior
  NIDS

- Intrusion prevention systems

  IDS + authority to block or change traffic

IPSec

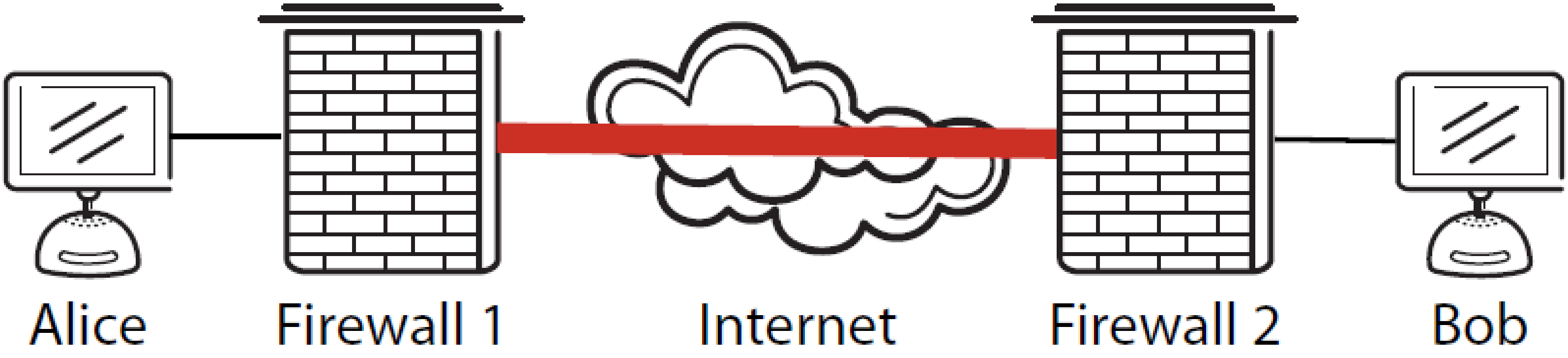
Have you ever sent a password over the wireless connection at a coffee shop?



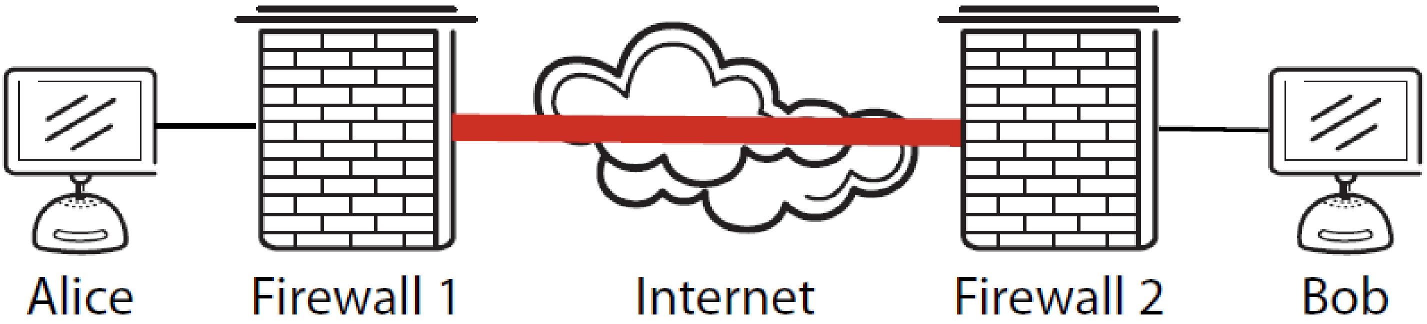
Related question: Ever heard of a packet sniffer?

IPSec

The goal of IPSec is to provide a cryptographically secure connection for data being sent over an insecure network.



How is this different from standard encryption?

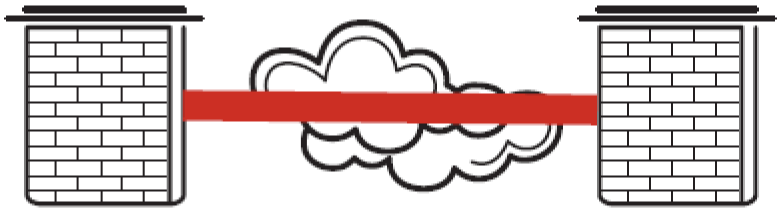


↑ encrypted

Application never knows about encryption.

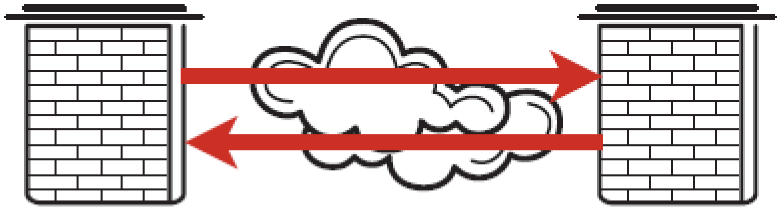
Associated with each end of the connection is:

- cryptographic key,
- identity of the opposite end,
- cryptographic services.



A security association is **unidirectional**:

a transmission between two parties requires an SA in each direction.



secure

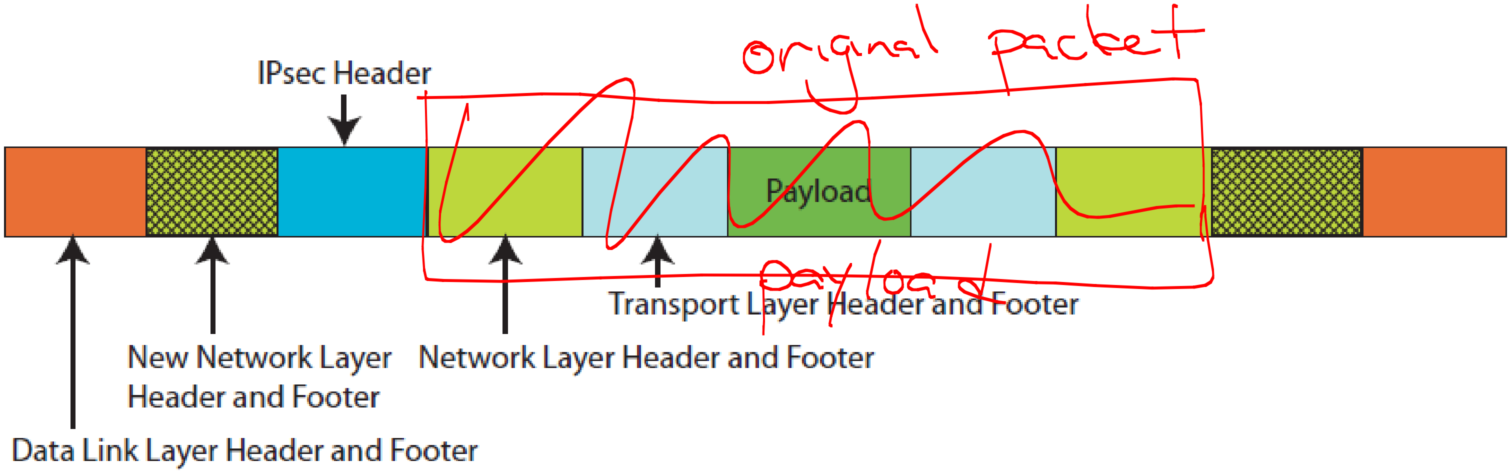
authentication

Two Modes

- Transport Mode
- Tunnel Mode ←

Tunnel Mode

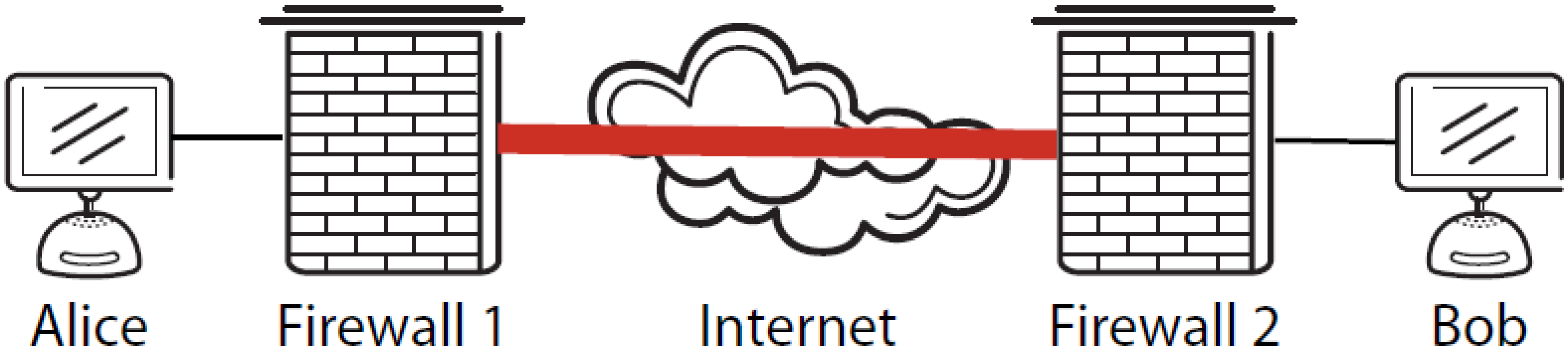
Works when connection is between firewalls


original packet
IPsec Header
Payload
payload
Transport Layer Header and Footer
New Network Layer Header and Footer
Network Layer Header and Footer
Data Link Layer Header and Footer

"Refers to keeping the original IP packet intact and adding a new IP header and IPsec information outside.

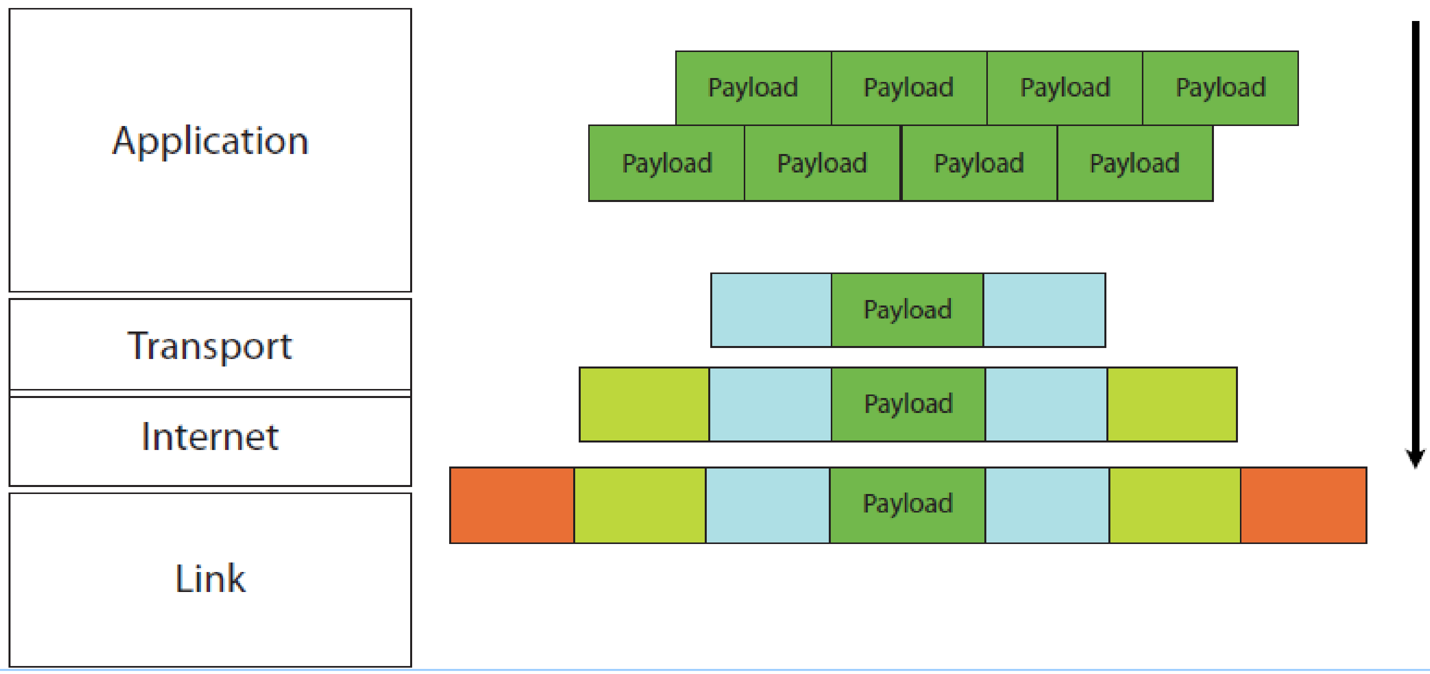
Content taken from "Network Security: Private Communication in a Public World."

Example :

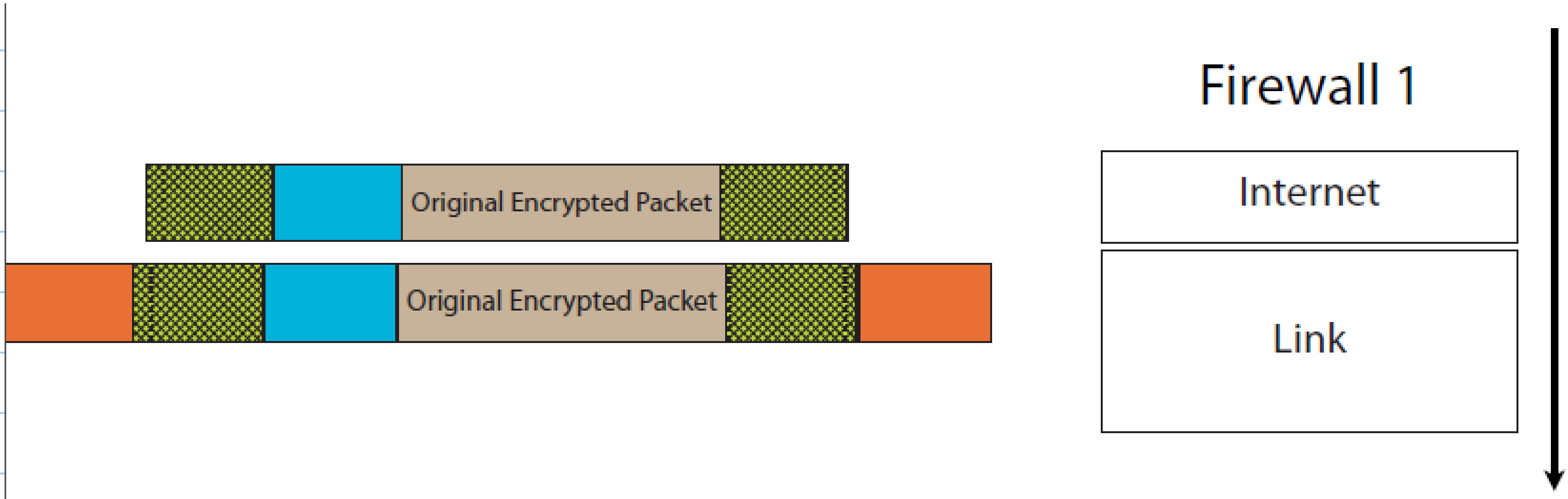


Alice wants to send a message to Bob using IPsec

Alice sends her packets as usual:



At the firewall:



The IPsec-enabled firewall encrypts the packet, adds a IPsec header and adds a new IP header.

From then on, routers will only see the IPSec headers added by the firewall.

At Bob's firewall, packets are decrypted & sent to him.

Alice & Bob never see the security.