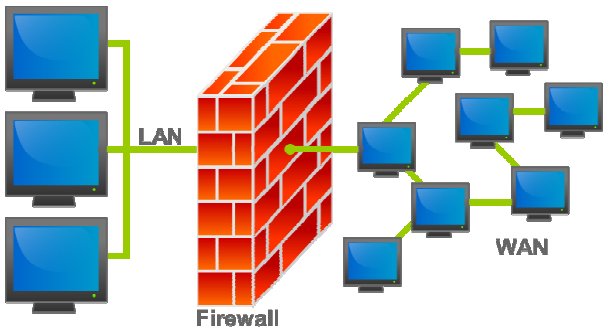
Firewall, VPN, IDS/IPS

Ahmet Burak Can
Hacettepe University
abc@hacettepe.edu.tr

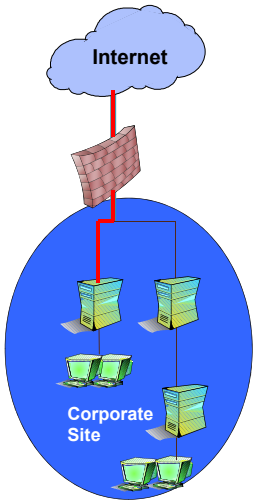
What is a Firewall?

- A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer



What is a Firewall ?

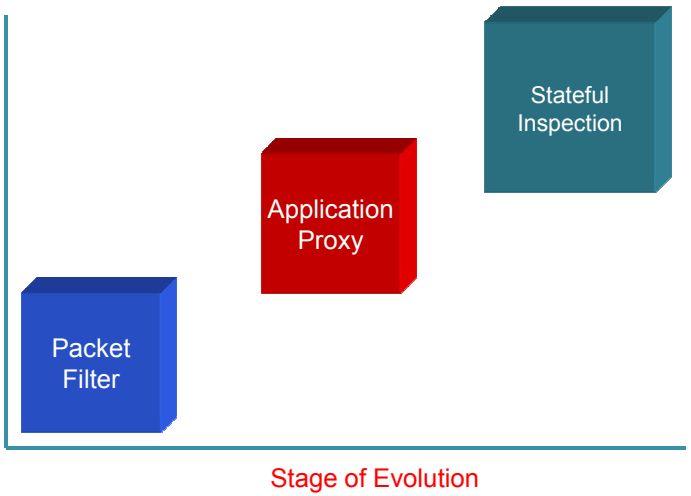
- A firewall :
  - Acts as a security gateway between two networks
  - Tracks and controls network communications
    - Decides whether to pass, reject, encrypt, or log communications (Access Control)



Hardware vs. Software Firewalls

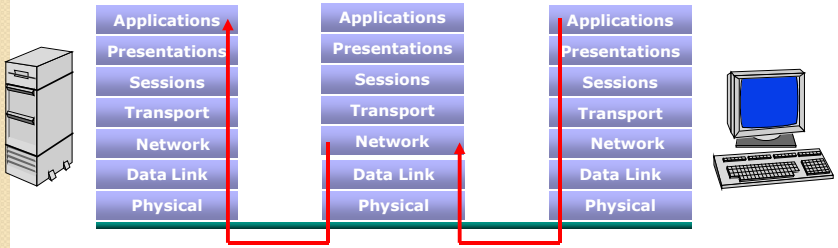
- Hardware Firewalls
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure
- Software Firewalls
  - Protect a single computer
  - Usually less expensive, easier to configure

Evolution of Firewalls



Packet Filter

- Packets examined at the network layer
- Useful "first line" of defense - commonly deployed on routers
- Simple accept or reject decision model
- No awareness of higher protocol layers



Packet Filter

- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples:
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers

How to Configure a Packet Filter

- Start with a security policy
- Specify allowable packets in terms of logical expressions on packet fields
- Rewrite expressions in syntax supported by your vendor
- General rules - least privilege
  - All that is not expressly permitted is prohibited
  - If you do not need it, eliminate it

Packet Filter Configuration - 1

Every ruleset is followed by an implicit rule reading like this.

action	src	port	dest	port	flags	comment
block	*	*	*	*	*	default

- Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine.
- Also suppose that mail from some particular site MORDOR is to be blocked.

Packet Filter Configuration - 2

action	src	port	dest	port	flags	comment
block	MORDOR	*	*	*	*	We don't trust these site
allow	*	*	OUR-GW	25	*	Connection to our SMTP port

- Now suppose that we want to implement the policy "any inside host can send mail to the outside".

Packet Filter Configuration - 3

action	src	port	dest	port	flags	comment
allow	*	*	*	25	*	Connection to outside SMTP port

- This solution allows calls from any port on an inside machine, and will direct them to port 25 on an outside machine.
- So why is it wrong?

Packet Filter Configuration - 4

- Our defined restriction is based solely on the destination's port number.
- With this rule, an enemy can access any internal machines on port 25 from an outside machine.
- What can be a better solution ?

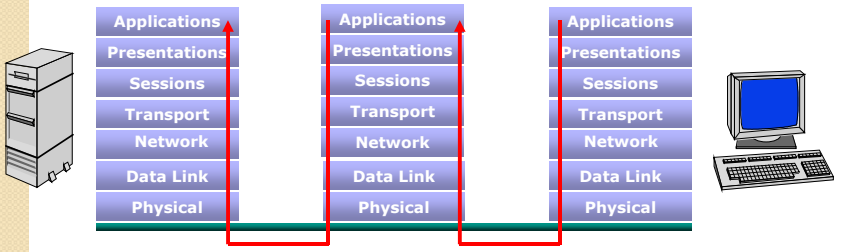
Packet Filter Configuration - 5

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25	*	Connection to outside SMTP port
allow	*	25	*	*	ACK	SMTP replies

- The first rule restricts that only inside machines can access to outside machines on port 25.
- In second rule, the ACK signifies that the packet is part of an ongoing conversation.
  - Packets without ACK are connection establishment messages, which are only permited from internal hosts by the first rule.
  - With the second rule, outside hosts can send back packets to inside hosts on port 25.

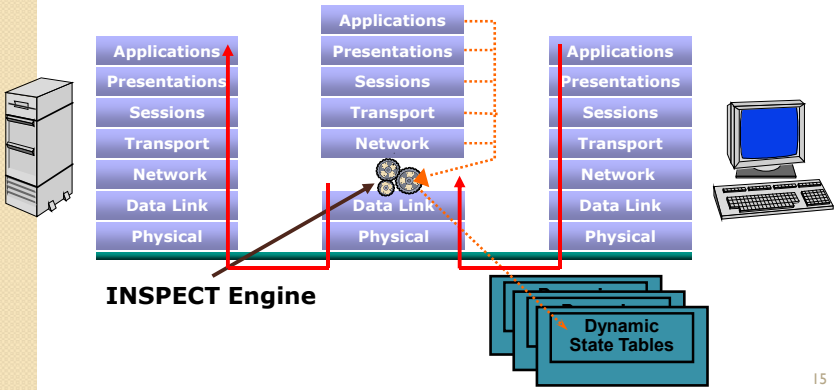
Application Gateway or Proxy

- Packets examined at the application layer
- Application/Content filtering possible - prevent FTP "put" commands, for example
- Modest performance
- Scalability limited

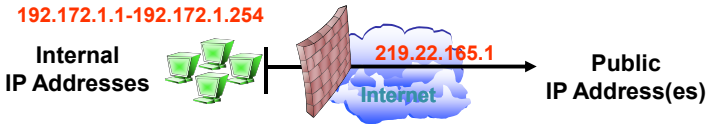


Stateful Inspection

- Packets Inspected between data link layer and network layer in the OS kernel
- State tables are created to maintain connection context
- Invented by Check Point



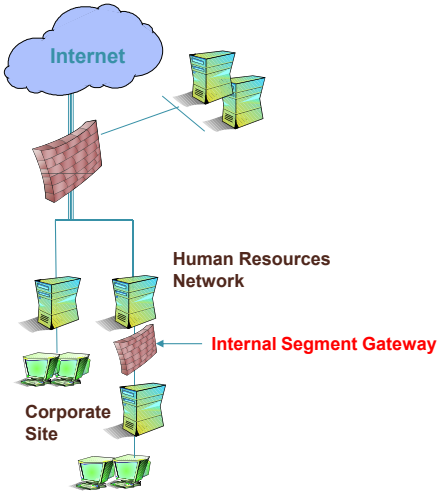
Network Address Translation (NAT)



- Converts a network's illegal IP addresses to legal or public IP addresses
  - Hides the true addresses of individual hosts, protecting them from attack
  - Allows more devices to be connected to the network

Firewall Deployment

- Corporate Network Gateway
- Internal Segment Gateway
  - Protect sensitive segments (Finance, HR, Product Development)
  - Provide second layer of defense
  - Ensure protection against internal attacks and misuse

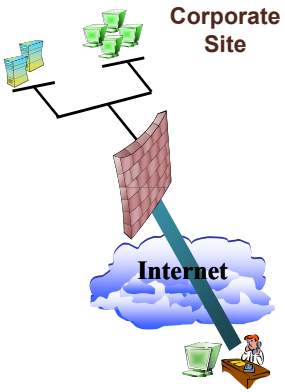


What is a VPN?

- A VPN is a private connection over an open network
- A VPN includes authentication and encryption to protect data integrity and confidentiality
- Types:
  - Remote Access VPN
  - Site-to-Site VPN
  - Extranet VPN
  - Client/Server VPN

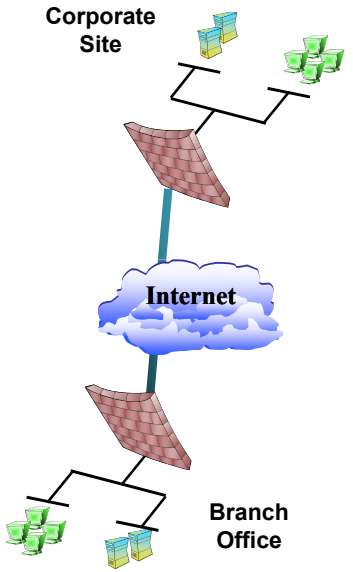
Types of VPNs

- Remote Access VPN
  - Provides access to internal corporate network over the Internet
  - Reduces long distance, modem bank, and technical support costs
  - PAP, CHAP, RADIUS



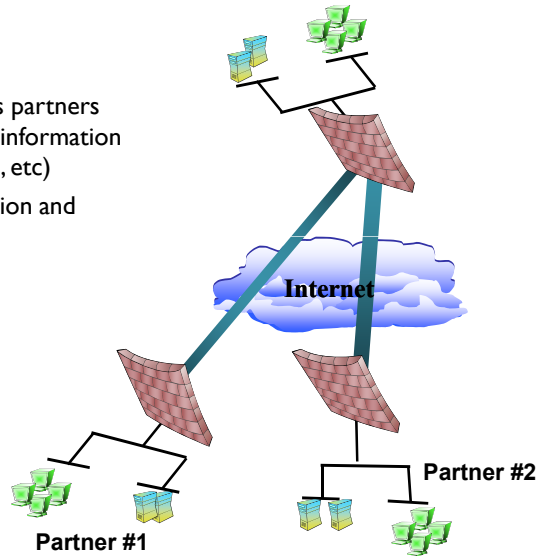
Types of VPNs

- Site-to-Site VPN
  - Connects multiple offices over Internet
  - Reduces dependencies on frame relay and leased lines



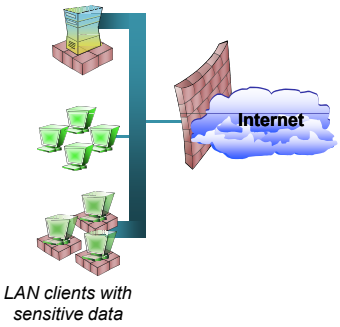
Types of VPNs

- Extranet VPN
  - Provides business partners access to critical information (leads, sales tools, etc)
  - Reduces transaction and operational costs



Types of VPNs

- Client/Server VPN
  - Protects sensitive internal communications



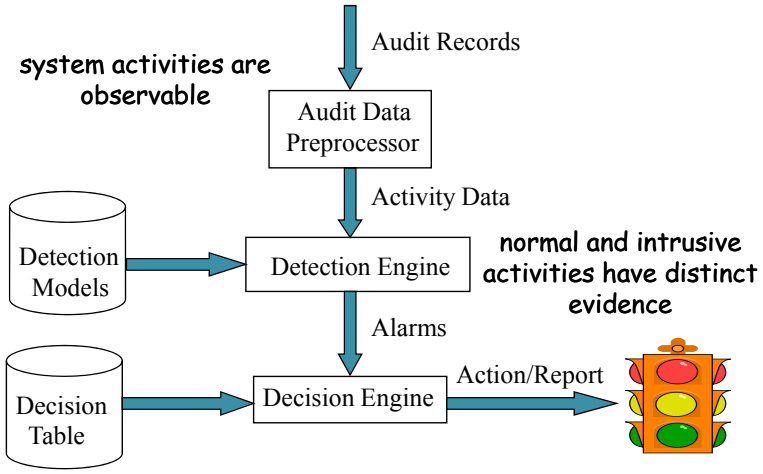
Overview of IDS/IPS

- Intrusion
  - A set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource)
- Intrusion detection
  - The process of identifying and responding to intrusion activities
- Intrusion prevention
  - The process of both detecting intrusion activities and managing responsive actions throughout the network.

Overview of IDS/IPS

- Intrusion detection system (IDS)
  - A system that performs automatically the process of intrusion detection.
- Intrusion prevention system (IPS)
  - A system that has an ambition to both detect intrusions and manage responsive actions.
  - Technically, an IPS contains an IDS and combines it with preventive measures (firewall, antivirus, vulnerability assessment) that are often implemented in hardware.

Components of Intrusion Detection System



Intrusion Detection Approaches

- Modeling
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (a.k.a. signature-based)
    - Anomaly detection (a.k.a. statistical-based)
- Deployment: Network-based or Host-based
  - Network based: monitor network traffic
  - Host based: monitor computer processes