İTÜ
Computer Security

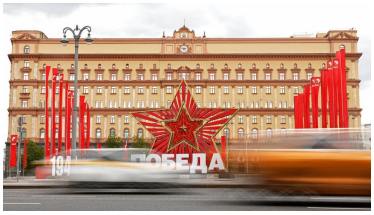
Firewalls and Intrusion Prevention Systems

Dr. Şerif Bahtiyar
bahtiyars@itu.edu.tr

1

Before Starting

Russia hacking: 'FSB in years-long cyber attacks on UK', says government



The UK is accusing Russia's Security Service, the FSB, of a sustained cyber-hacking campaign, targeting politicians and others in public life.

https://www.bbc.com/news/uk-politics-67647548

2

Outline

- Firewalls
- Intrusion Prevention Systems
- Unified Threat Management

3

Firewall

- The Need for Firewalls
- Firewall Characteristics
- Types of Firewalls
- Firewall Basing
- Firewall Location and Configurations

4

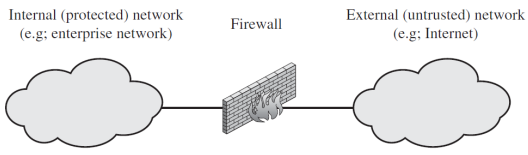
The Need for Firewalls

- Internet connectivity is essential for organizations and also for individuals.
- Internet access provides benefits for organizations by interacting with outside world -> create threats to the organization.
- Each system may be equipped with strong security features (host based security services) -> not cost effective.

5

The Need for Firewalls

- Alternative -> firewalls.
- Firewall is inserted between the premises network and the Internet.
- Protect local systems and network systems from network based threats.

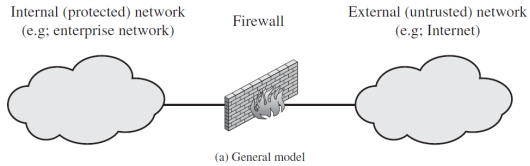


(a) General model

6

The Need for Firewalls

- Secure workstations and servers
- Provide a single choke point
- Be a single computer or a set of systems
- Provides additional layer of defense



(a) General model

7

Firewall Characteristics

Firewall design goals

- All traffic must pass through firewall
- Only authorized traffic are allowed to pass
- Immune to penetration (Trusted computer system are suitable for hosting)

8

Firewall Characteristics

Techniques to access control and policy enforcement

- Service control: determine services, such as IP address, port, web, mail,..
- Direction control
- User control
- Behavior control: controls how particular services are used.

9

Firewall Characteristics

Firewall capabilities

- Defines a single choke point
- Monitoring
- Platform for several non-security Internet functions, such as network address translator
- Platform for IPSec

10

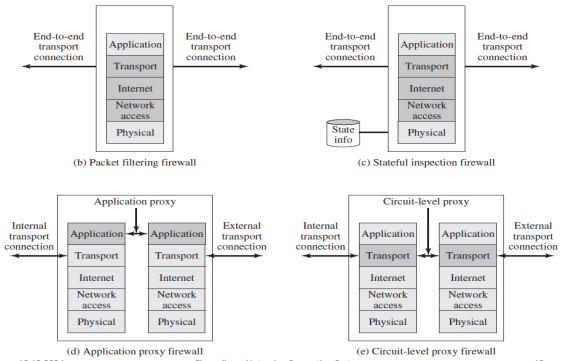
Firewall Characteristics

Firewall limitations

- Cannot protect against attacks that bypass firewall
- May not protect against internal threats
- Cannot guard against wireless communications
- Cannot provide protections to portable devices

11

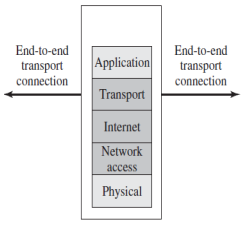
Types of Firewalls



12

Packet Filtering Firewall

- Applies a set of rules to each incoming and outgoing IP packets
- The packet filter is typically set up as a list of rules of matches on fields
  - If there is a match to one rule, the rule is invoked to determine whether to forward or discard the packet
  - If not apply default action



(b) Packet filtering firewall

13

Packet Filtering Firewall

Default policies

- Discard
  - More conservative
  - Preferred by business and government organizations
- Forward
  - Increases ease of use
  - Provides reduced security
  - May be used by open organizations, such as universities

14

Packet Filtering Firewall

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our host}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

15

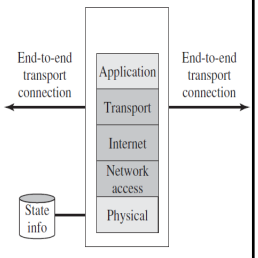
Packet Filtering Firewall

- Advantages of packet filter firewalls
  - Simple
  - Transparent to users
  - Very fast
- Weaknesses of packet filter firewalls
  - Cannot prevent attacks that employ application specific vulnerabilities
  - Limited logging functionality
  - No advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configurations can lead to breaches

16

Stateful Inspection Firewall

- A packet filter firewall must permit inbound network traffic on all high numbered ports for TCP traffic -> creates vulnerability.
- Stateful inspection packet firewall creates a directory of outbound TCP connections -> packet filter firewalls now allow incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory.



(c) Stateful inspection firewall

17

Stateful Inspection Firewall

Table 9.2 Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

- Review the same packet information as a packet filtering firewall
- Also records information about TCP connections
- May keep track of TCP sequence number
- May inspect limited amount of application data

18

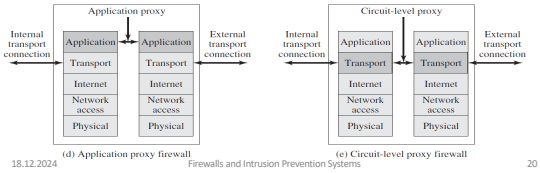
Application-Level Gateway

- Also called application proxy
- Acts as a relay of application level traffic
  - Users contact gateway with remote host name
  - Authenticate themselves
  - Gateway contacts application on remote host and relays TCP segments between server an user
- Must have proxy code for each application
- More secure than packet filters
- Have higher overhead

19

Circuit-Level Gateway

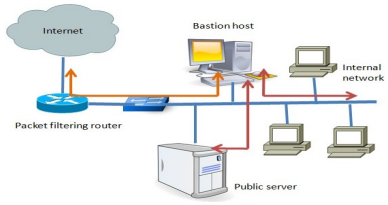
- Also known as circuit-level proxy
- Stand-alone system or specialized by an application-level gateway for certain applications
- Does not permit end-to-end TCP connection
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.



20

Firewall Basing - Bastion Host

- A critical **strong** point in the network's security
- Serves as a platform for an application or circuit level gateway.



Screened host firewall (single-homed bastion host)

Source: https://securitywing.com/types-of-firewall/

21

Firewall Basing - Bastion Host

Common characteristics

- Runs secure OS and only essential services
- May require additional user authentication to access to proxy
- Support only some applications
- Allow access only to specific host systems
- Maintains detailed audit information
- Very small software package
- Independent of other proxies on the bastion host
- Limited disk use
- Runs as a non-privileged user

22

Firewall Basing - Host-Based Firewalls

- Used to secure individual host
- Available add on for many OS
- Filter packet flows
- Generally used on servers
- Advantages
  - Security policies for servers can be implemented
  - Independent of topology (protection against both internal and external attacks)
  - Additional layer of protection to other firewalls

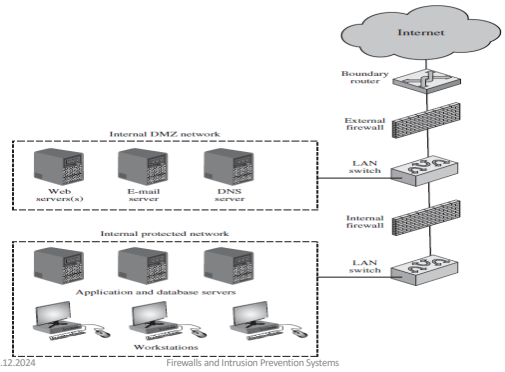
23

Firewall Basing - Personal Firewall

- Controls the traffic between a personal computer and the Internet
- Used in home environment or on corporate intranets
- A software module on the personal computer
- Much less complex
- Role is to deny unauthorized remote access to the computer
- Monitor outgoing activity to detect and block malware

24

Firewall Location and Configurations



25

Firewall Location and Configurations - DMZ

DMZ (Demilitarized zone) Networks

- External firewall
  - placed at the edge of a local network just inside boundary router
  - provides a basic level of protection
- Internal firewall
  - one or more internal firewalls protect the bulk of the enterprise network
  - adds more stringent filtering capability
  - two way protection
- Between external and internal firewalls are networked devices in a region referred to as a DMZ.

26

Firewall Location and Configurations - VPN

Virtual Private Network (VPN)

- Public networks like the Internet can be used to interconnect sites
  - Cost effective
  - Offloading WAN management tasks
- Problem-> Security-> VPN needed
- A VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through insecure network
  - Cheaper than real private networks using private lines
  - Operations are transparent to workstations and servers

27

Firewall Location and Configurations - VPN

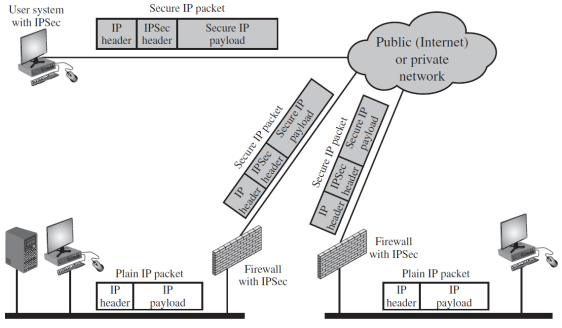


Figure 9.3 **A VPN Security Scenario**

28

Firewall Location and Configurations

Distributed Firewalls

- A distributed firewall configuration involves stand-alone firewalls devices plus host-based firewalls working together under a central administrative control.
- Security monitoring is an important aspect of distributed firewall configuration.

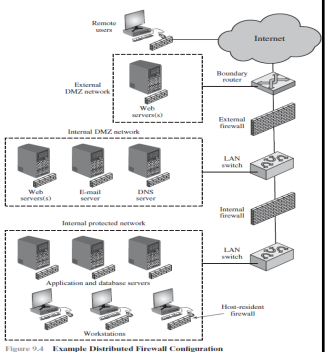
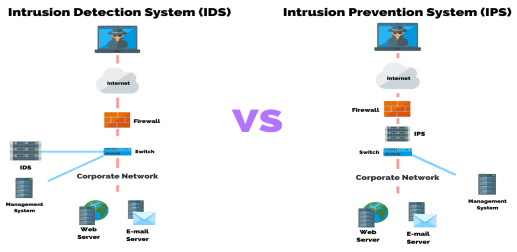


Figure 9.4 **Example Distributed Firewall Configuration**

29

Intrusion Prevention System (IPS)

Is a functional addition to a firewall that adds IDS types of algorithms to the repertoire of the firewall.



Source: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

30

Intrusion Prevention System (IPS)

- May be an inline network-based IDS (NIDS) that can block traffic
- May monitor ports on a switch and then send the appropriate command to a router or firewall to block traffic.
- May be either host based or network based

31

Intrusion Prevention System (IPS)

Host-Based IPS

- A host-based IPS (HIPS) makes use of both signature and anomaly detection techniques to identify attacks.
- Can be tailored to the specific platform
- Can use sandbox approaches to monitor behavior of specific code, such as mobile code, Java applets
- HIPS approach is an integrated single product suit of functions

32

Intrusion Prevention System (IPS)

Network-Based IPS

- A network-based IPS (NIPS) is an inline NIDS with the authority to discard packets and tear down TCP connections.
- Uses signature and anomaly detection techniques
- May provide flow data protection (monitor full application flow content)

33

Unified Threat Management

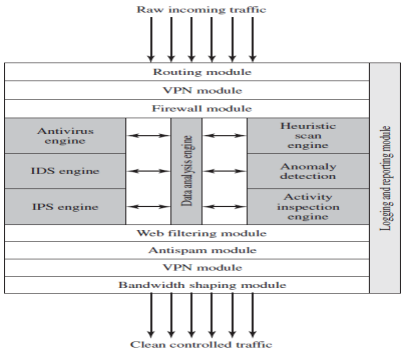


Figure 9.5 Unified Threat Management Appliance

34

Summary

- The Need for Firewalls
- Firewall Characteristics
- Types of Firewalls
- Firewall Basing
- Firewall location and Configurations
- Intrusion Prevention System
- Unified Threat Management

35