

Firewalls



Ahmad Almulhem

March 10, 2012

Outline

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

Firewalls



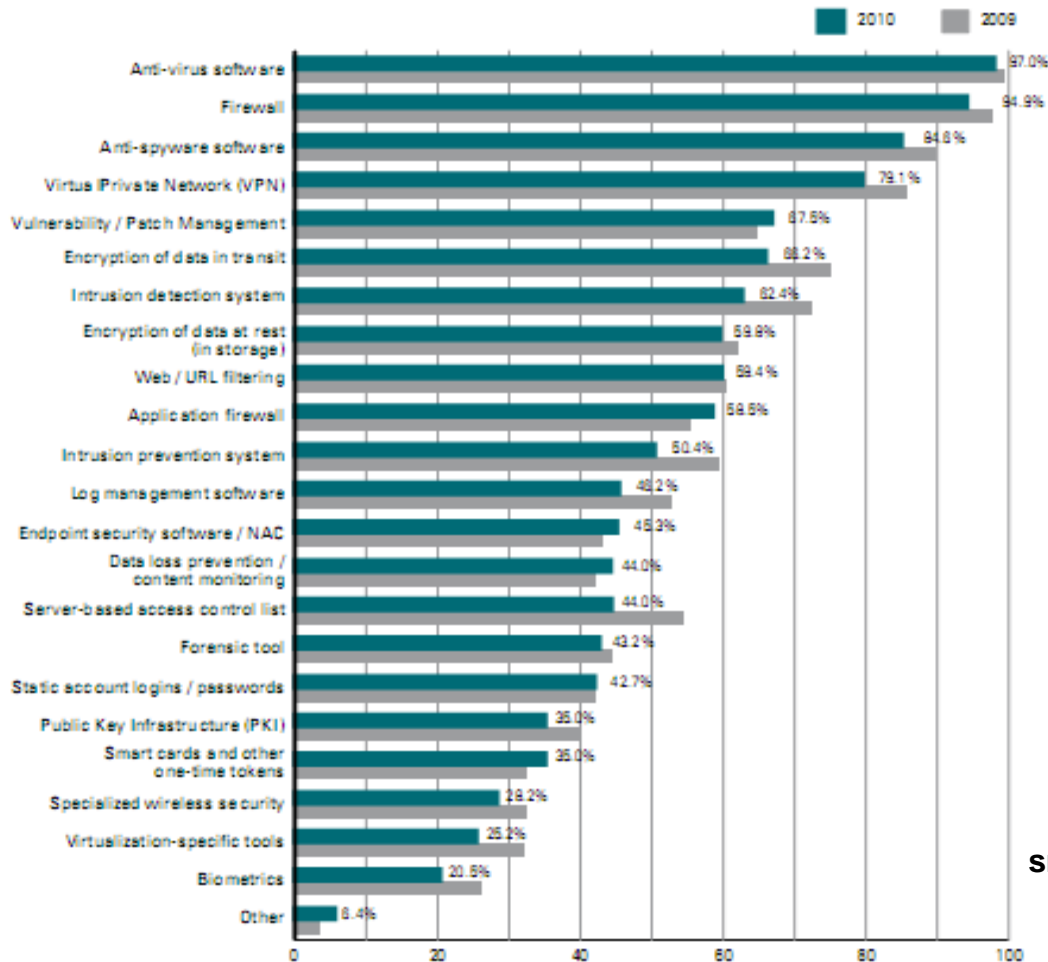
- Term originated from physical firewall
 - Designed to contain fires
 - Slow down the spread of fires
- Computing firewalls work a bit differently
 - Usually try to prevent “external fires”
 - More like the Great Wall of China
 - Does provide internal segmentation and protection
 - can be implemented in either hardware or software, or a combination of both.

The Need For Firewalls

- Internet connectivity is essential
 - however it creates a threat
- effective means of protecting a network while allowing Internet access
- inserted between the premises network and the Internet to establish a controlled link
 - can be a single computer system or a set of two or more systems working together
- used as a perimeter defense
 - single choke point to impose security and auditing
 - insulates the internal systems from external networks

The Need For Firewalls

Types of Security Technology Used
By Percent of Respondents



Major firewall vendors:
Checkpoint
Cisco PIX

src: CSI Computer Crime and Security Survey 2010/2011

Firewall Characteristics

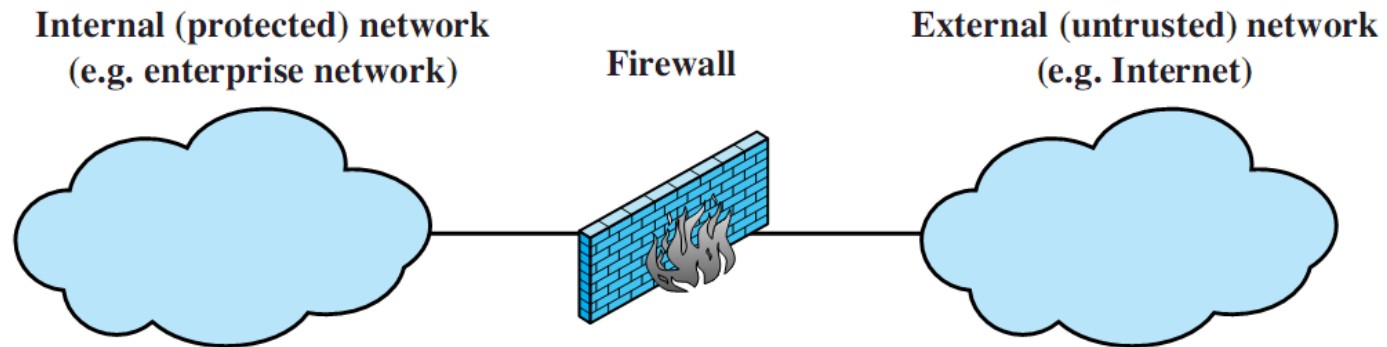
Design goals:

- all traffic from inside to outside must pass through the firewall
- only authorized traffic as defined by the local security policy will be allowed to pass
- the firewall itself is immune to penetration

Techniques used by firewalls to control access and enforce the site's security policy are:

- service control
- direction control
- user control
- behavior control

Types of Firewalls



- firewall acts as a packet filter
 - positive filter: allow only packets meeting certain criteria
 - negative filter: reject any packet that meets certain criteria
- may examine
 - one or more protocol headers in each packet
 - payload
 - sequence of packets

Types of Firewalls

- Traditional Packet filters (stateless)
- Stateful filters
- Application Gateway (proxy)

Traditional packet filters

Analyzes each packet going through it; makes drop decision based on:

- source IP address
- destination IP address
- source port
- destination port
- TCP flag bits
 - SYN bit set: datagram for connection initiation
 - ACK bit set: part of established connection
- TCP or UDP or ICMP
 - Firewalls often configured to block all UDP
- direction
 - Is the datagram leaving or entering the internal network?
- router interface
 - decisions can be different for different interfaces

Filtering Rules - Examples

<u>Policy</u>	<u>Firewall Setting</u>
No outside Web access.	Drop all outgoing packets to any IP address, port 80
External connections to public Web server only.	Drop all incoming TCP SYN packets to any IP except 222.22.44.203, port 80
Prevent IPTV from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a Smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 222.22.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP

Access control lists

Apply rules from top to bottom:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

a packet may not match any rule (default)

two default policies:

- discard – drop packet

 - more conservative, secure, visible to users

- forward – pass packet

 - easier to manage, friendlier to users, but less secure

Access control lists

- Each router/firewall interface can have its own ACL
- Most firewall vendors provide both command-line and graphical configuration interface

Advantages and disadvantages of traditional packet filters

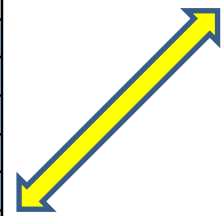
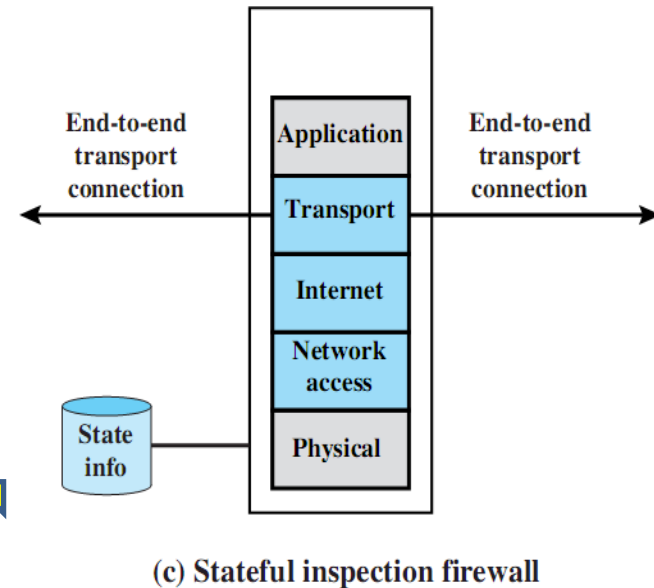
- Advantages
 - Simplicity: one firewall can protect entire network
 - Can be efficient if filtering rules are kept simple
 - Widely available. Almost any router, even Linux boxes
- Disadvantages
 - Can possibly be penetrated
 - IP address spoofing, fragmentation
 - Cannot enforce some policies. For example, permit certain users.
 - Rules can get complicated and difficult to test

Stateful Firewall

- considers a packet in series of packets (not individually)
 - packet context
- keeps info about each TCP connection
 - determines if a packet is a start of TCP connection, part of an existing connection, or invalid
- still has a set of static rules, but states of connection is part of matching a rule
- improve filtering based on TCP connections
- can be a target of DOS attack (how?)

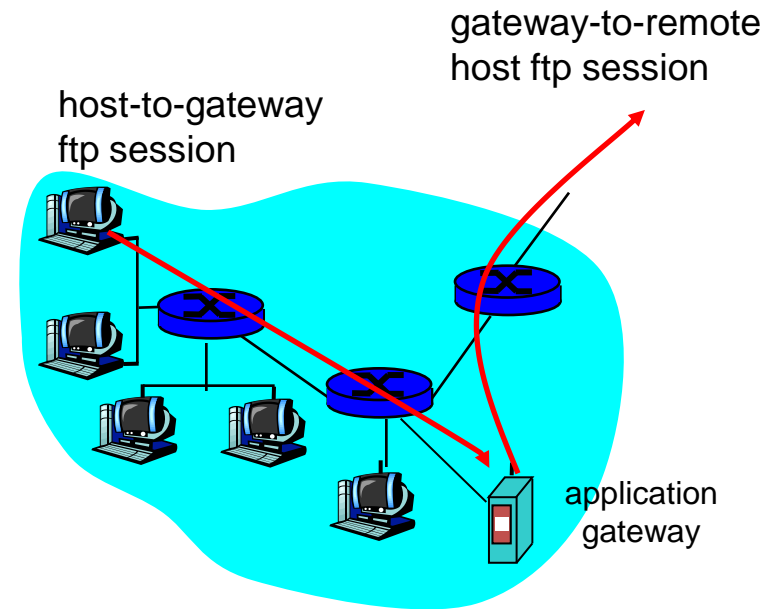
Table 9.2 Example Stateful Firewall Connection State Table [WACK02]

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



Application Gateways

- Gateway (proxies) sits between user on inside and server on outside. Instead of talking directly, user and server talk through proxy.
- Allows more fine grained and sophisticated control than packet filtering. For example, ftp server may not allow files greater than a set size.
- can authenticates users



Advantages and disadvantages of application gateways

- Advantages
 - Proxy can log all connections, activity in connections
 - Proxy can provide caching
 - Proxy can do intelligent filtering based on content
 - Proxy can perform user-level authentication
- Disadvantages
 - Not all services have proxied versions
 - May need different proxy server for each service
 - Requires modification of client
 - Performance

SOCKS Proxy protocol

- Generic proxy protocol
 - Don't have to redo all of the code when proxifying an application.
- Can be used by HTTP, FTP, telnet, SSL,...
 - Independent of application layer protocol
- Includes authentication, restricting which users/apps/IP addresses can pass through firewall.

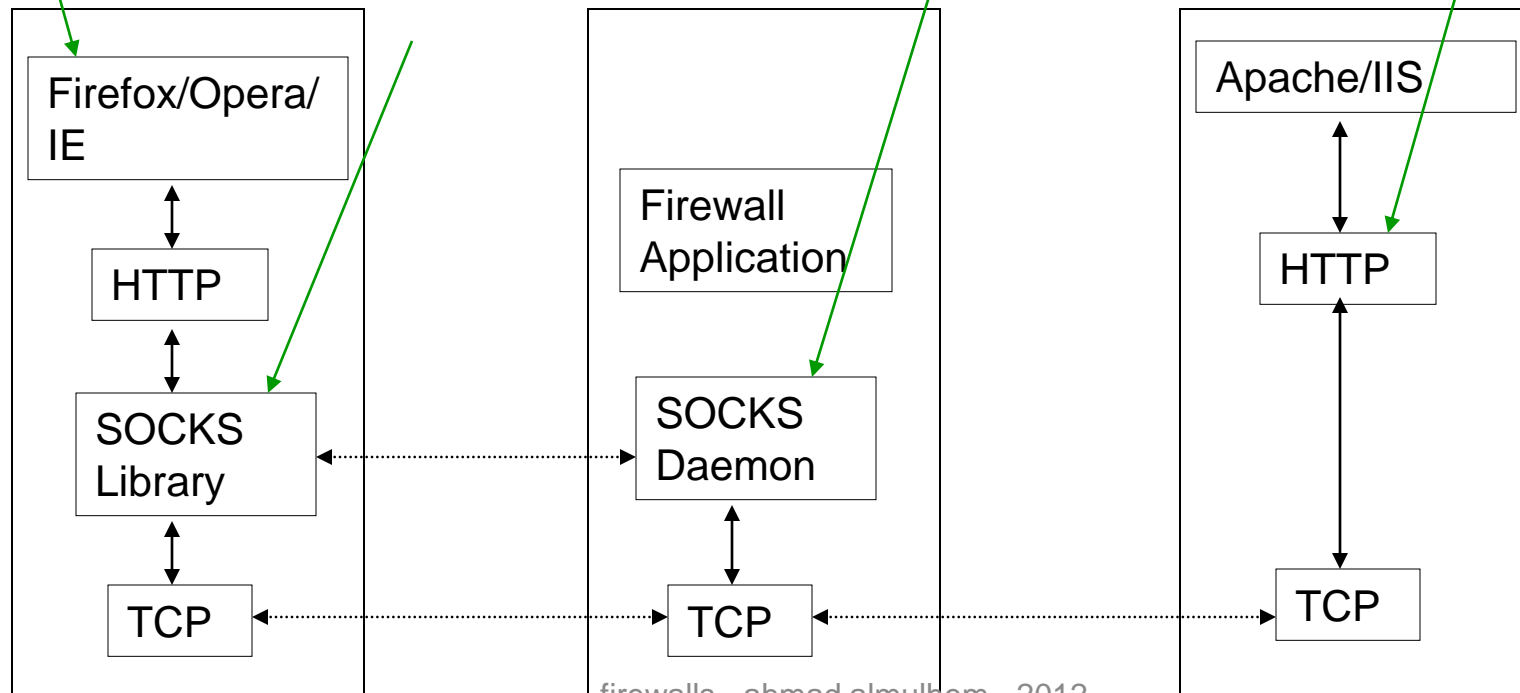
SOCKS proxy protocol

1. For example, let's assume that browser requests a page

2. SOCKS Library is a collection of procedures. It translates requests into a specific format and sends them to SOCKS Daemon

3. The SOCKS Daemon runs on the firewall host. The daemon authenticates the user and forwards all the data to the server.

4. The server receives requests as ordinary HTTP. It does not need a SOCKS library.



Firewall Basing

- it is common to base a firewall on a standalone machine running a common operating system, such as UNIX or Linux
- also may be implemented as a software modules in a router or LAN switch
- additional basing options:
 - bastion host
 - individual host-based firewall
 - personal firewall

Bastion Hosts

- a special purpose computer on a network specifically designed and configured to withstand attacks
- critical strongpoint in network
- fully exposed to attacks
- hosts application/circuit-level gateways
- common characteristics:
 - runs secure O/S,
 - only essential services (close all unneeded ports)
 - disable/remove unneeded users accounts
 - disable/remove any unneeded network protocols
 - limited disk use, hence read-only code

Host-Based Firewalls

- a software module used to secure individual host
- available by default or as an add-on for many O/S
- filter packet flows
- often used on servers
- advantages:
 - tailored filter rules for specific host needs
 - protection from both internal / external attacks
 - additional layer of protection to stand-alone firewalls

Personal Firewall

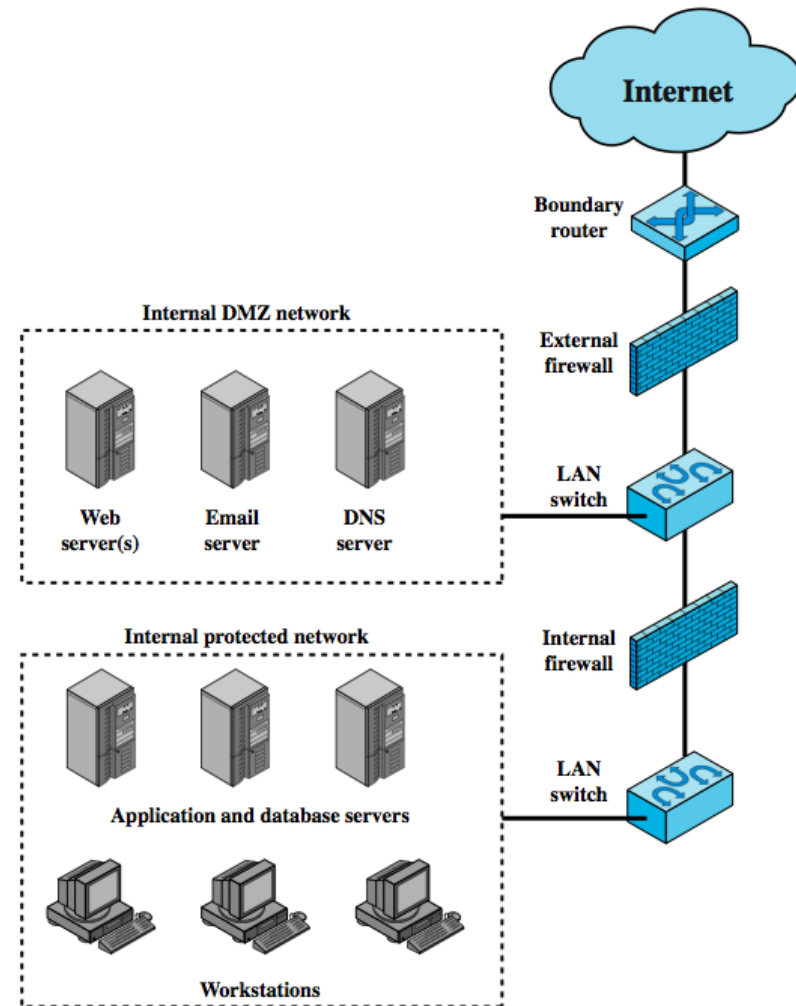
- controls traffic flow to/from PC/workstation
 - e.g. Firewall in MS Windows
- used for both home or corporate use
- may be software module on PC or embedded in home cable/DSL router/gateway
- typically much less complex than stand-alone firewalls and server-based firewalls
- primary role to deny unauthorized access
- may also monitor outgoing traffic to detect/block worm/malware activity

Firewall Configurations

- A firewall is positioned to provide a protective barrier between Internet and internal network
- a security administrator must decide on the location and on the number of firewalls needed.
- there are several options; we look at some common options next

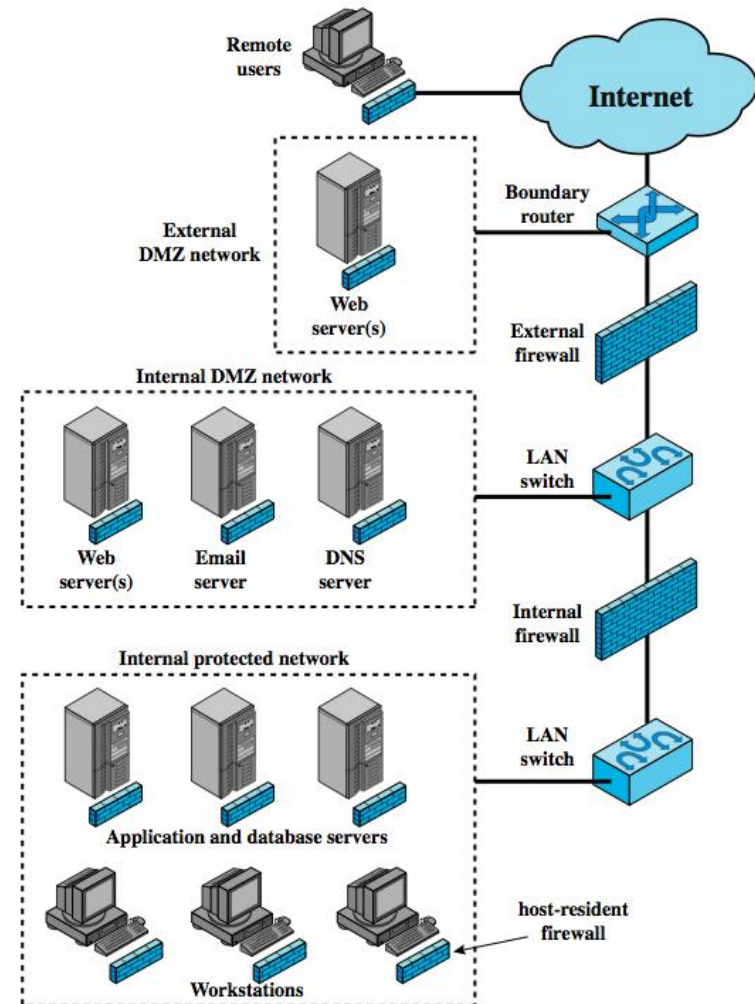
DMZ Network

- most common configuration
- DMZ short for demilitarized zone
- external firewall is placed at the edge of a local or enterprise network
- one or more internal firewalls protect the bulk of the enterprise network
- between the two types of firewalls is DMZ; contains server accessible from outside, like web server, DNS, e-mail servers
- external firewall provides protection of DMZ systems and basic protection for the whole enterprise
- internal firewall(s) provide more stringent filtering, and 2-way protection w.r.t. DMZ



Distributed Firewalls

- involves standalone firewall devices plus host-based firewalls working together under a central administrative control
- Administrators can configure host-based firewalls on hundreds of servers and workstation as well as configuring personal firewalls on local and remote user systems
- tools let the network administrator set policies and monitor security across the entire network
- may make sense to establish both an internal and an external DMZ
- advantage: strong, fine-grained monitoring

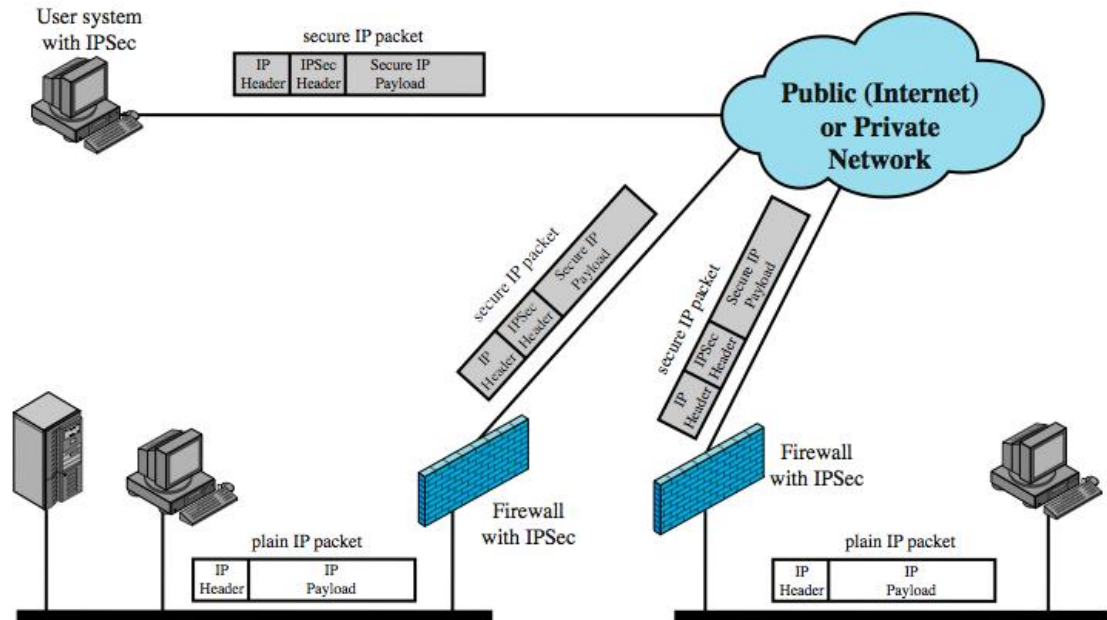


Virtual Private Networks

- virtual private network (VPN); set of networks interconnected through unsecure network (Internet)

- use encryption and special protocols to protect transmitted traffic

- VPN attractive solution; cheaper than real private networks
- IPSec is most common protocol used
- VPN functionality typically implemented in firewalls
- encryption/decryption (also compression) between end-points transparent to users



Firewall Policies

- A firewall policy is usually specified as a sequence of rules
- Each rule consists of a predicate and a decision.
 - A predicate typically includes five fields:
 - source IP, destination IP, source port, destination port, protocol type
 - Typical decisions are **accept** and **discard**.


Firewall Policy	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
r_1	1.2.3.*	192.168.1.1	*	25	TCP	Accept
r_2	1.2.3.9	192.168.1.1	*	25	*	Discard
r_3	*	*	*	*	*	Discard

Packet	Src IP	Dst IP	Src Port	Dst Port	Protocol	Payload
	1.2.3.5	192.168.1.1	78	25	TCP	


- Conflict Resolution: first-match

Firewall Policies Anomalies

(1) Wrong order: the order of firewall rules is wrong.

	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
 r ₁	1.2.3.*	192.168.1.1	*	25	TCP	Accept
r ₂	1.2.3.9	192.168.1.1	*	25	*	Discard

(2) Missing rules: some rules are missed in the firewall policy.

	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
 r ₁	1.2.3.*	192.168.1.1	*	25	TCP	Accept
r ₂	1.2.3.9	192.168.1.1	*	25	*	Discard

(3) Wrong predicates: the predicates of some rules are wrong.

	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
r ₁	1.2.3.*	192.168.1.1	*	25	TCP	Accept

Firewall Policies Anomalies

(4) Wrong decisions: the decisions of some rules are wrong.

	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
r ₁	1.2.3.*	192.168.1.1	*	25	TCP	Accept
r ₂	1.2.3.9	192.168.1.1	*	25	*	Discard

(5) Wrong extra rules: some rules are not needed in the policy.

	Src IP	Dst IP	Src Port	Dst Port	Protocol	Decision
r ₁	1.2.3.*	192.168.1.1	*	25	TCP	Accept
r₂	1.2.3.9	192.168.1.1	*	25	*	Discard
r ₃	*	*	*	*	*	Discard

References

- William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Pearson Education, Prentice Hall, 2008.
- JeeHyun Hwang, Tao Xie, Fei Chen, and Alex X. Liu. "Systematic Structural Testing of Firewall Policies", IEEE Transactions on Network and Service Management. 2012.