

# ΕΠΛ 674: Εργαστήριο 5

## Firewalls

---

Παύλος Αντωνίου  
Εαρινό Εξάμηνο 2011



University of Cyprus  
Department of  
Computer Science

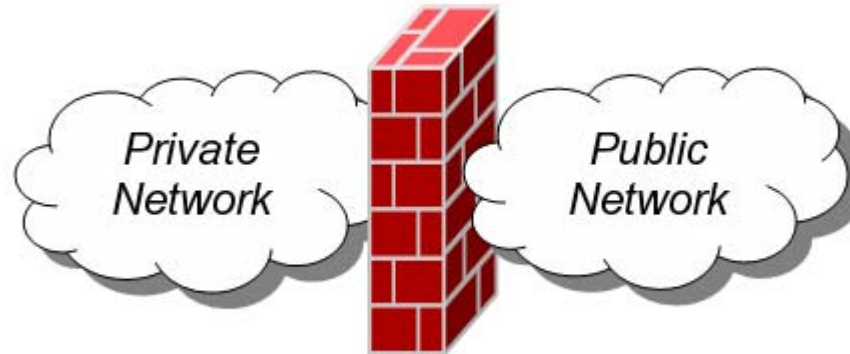
**NETR**<sup>works</sup><sub>research</sub>  
Laboratory

# Firewalls

- A firewall is hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network
- All information entering or leaving the network must pass through the firewall, which examines the information packets and blocks those that do not meet the security criteria.
- A firewall **implements** and **enforces** security policies for:
  - access
  - routing
  - application access

# Firewalls

- Internet : zone with no trust
- Internal network : zone with high trust



# What can a firewall do?

---

- A firewall is a focus for security decisions (choke point)
- A firewall can enforce a security policy
- A firewall can log network activity efficiently
- A firewall limits your exposure

# What can't a firewall do?

---

- Can't protect a subnet against malicious **insiders**
- Can't protect a subnet against **connections** that don't go through it
- Can't protect a subnet against completely **new threats**
- Can't protect a subnet fully against **viruses, worms**
- Can't work out of the box. Admin needs to **configure** it

# Personal vs Network firewalls

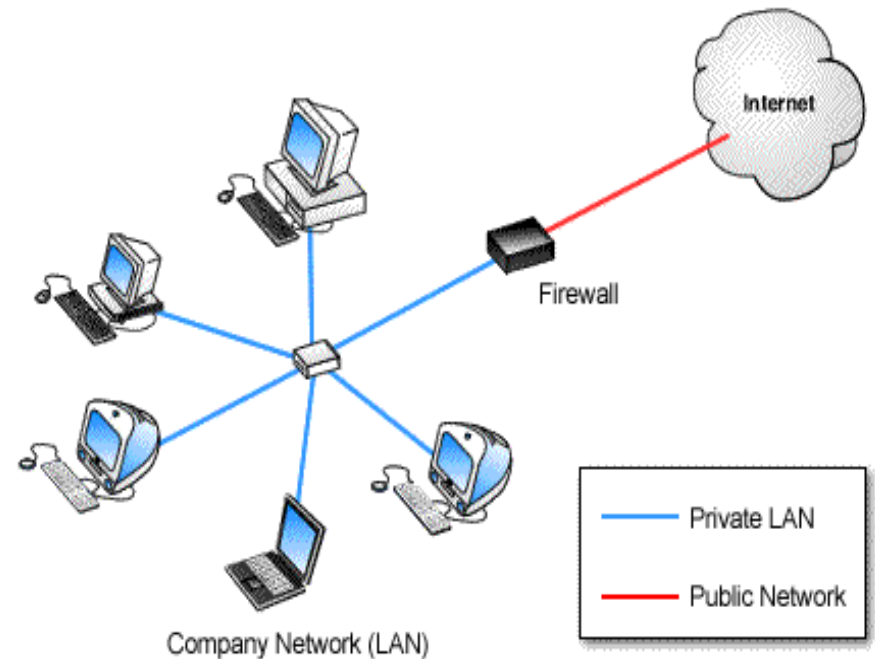
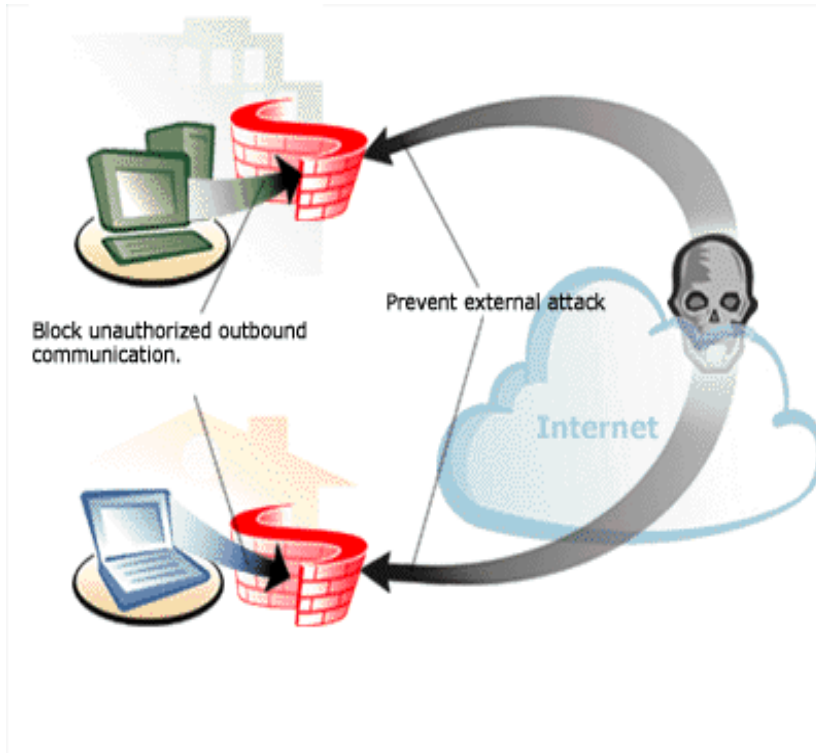
---

- Whether the communication is being done between a single node and the network, or between two or more networks:
  - **Personal firewalls**, a software application which normally filters traffic entering or leaving a single computer.
  - **Network firewalls**, normally running on a dedicated network device or computer positioned on the boundary of two or more networks. Such a firewall filters all traffic entering or leaving the connected networks.

# Personal vs Network firewalls



University of Cyprus



# Personal firewalls

- A **personal firewall** is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.
- A personal firewall differs from a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed.
- Many personal firewalls are able to control network traffic by prompting the user each time a connection is attempted and adapting security policy accordingly. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.



# Personal firewalls

---

- Alert the user about outgoing connection attempts
- Monitor applications that are listening for incoming connections
- Prevent unwanted network traffic from locally installed applications
- Provide the user with information about an application that makes a connection attempt.
- Provide information about the destination server with which an application is attempting to communicate

# Network vs Application layer firewalls

- Whether the communication is intercepted at the network layer, or at the application layer:
- **Network layer firewalls:** Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established ruleset. The firewall administrator may define the rules; or default rules may apply. They are very fast and tend to be very transparent to users.
- **Application layer firewalls:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgement to the sender). In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

# Network vs Application layer firewalls



University of Cyprus

Application layer  
firewalls

Network layer  
firewalls

Layer 7 - Application

Layer 6 - Presentation

Layer 5 - Session

Layer 4 - Transport

Layer 3 - Network

Layer 2 - MAC/DLC

Layer 1 - Physical

# Network layer firewalls

- A network layer firewall or a packet filters is a type of firewall techniques which looks at each packet entering or leaving the network and accepts or rejects it based on defined rules. More specifically:
  - operates on the network layer of OSI model
  - applies a set of rules to each incoming IP packet and then forward or discards a packet
  - rules are based on matches to fields in the IP or TCP header since filtering criteria are:
    - sender and receiver IP addresses
    - sender and receiver ports
    - protocol version
- Advantages: transparent to users since users are not burdened with setting up the firewall, simplicity, high-speed (especially hardware packets filters), low cost
- Disadvantages: it is difficult to configure (administrator), do not offer authentication services

# Network layer firewalls

- Every 'rule' consists of:
  - one or more 'match[es]' (rule executed if all matches are true)
  - and a 'target' (what to do, if the rule is matched → allow, deny ?)
- Rules are based on parameters:
  - source and destination IP addresses
  - source and destination port numbers
  - protocol
    - TCP
    - UDP
  - direction
    - incoming
    - outgoing

# Network layer firewalls

- **Example1:**
  - Deny from 195.209.34.64/28
  - Deny from 195.209.34.96/29
  - Allow from any
  - Packets with source IP addresses 195.209.34.78 and 195.209.34.89 will be allowed to pass from the firewall ?
- **Example2:**
  - Allow from 224.0.0.0/6
  - Deny from any
  - Packet with source IP address 228.52.34.8 will be allowed to pass from the firewall ?

# Network layer firewalls

- **Example1:**
  - Deny from 195.209.34.64/28
  - Deny from 195.209.34.96/29
  - Allow from any
  - Packets with source IP addresses 195.209.34.78 and 195.209.34.89 will be allowed to pass from the firewall ?
- **Solution → Rule 1:**
  - CIDR 28 → 28 stable bits and 4 variable. The section of IP address that varies is the last one ( $3 \times 8 = 24 + 4 = 28$ ). 64 → 01000000 where the 4 last bits are variable which means we have a range from 01000000 to 01001111 → 195.209.34.64 to 195.209.34.79. Rule 1 defines that firewall will reject packets with IP source addresses from 195.209.34.64 to 195.209.34.79
  - **So, the packet 195.209.34.78 will be denied**

# Network layer firewalls

- **Example1:**
  - Deny from 195.209.34.64/28
  - Deny from 195.209.34.96/29
  - Allow from any
  - Packets with source IP addresses 195.209.34.78 and 195.209.34.89 will be allowed to pass from the firewall ?
- **Example2:**
  - Allow from 224.0.0.0/6
  - Deny from any
  - Packet with source IP address 228.52.34.8 will be allowed to pass from the firewall ?

Policy: by default  
accept everything  
except if expressly be  
denied



# Network layer firewalls



University of Cyprus

- **Example1:**
  - Deny from 195.209.34.64/28
  - Deny from 195.209.34.96/29
  - Allow from any
  - Packets with source IP addresses 195.209.34.8 and 195.209.34.89 will be allowed to pass from the firewall ?
- **Example2:**
  - Allow from 224.0.0.0/6
  - Deny from any
  - Packet with source IP address 228.52.34.8 will be allowed to pass from the firewall ?

Policy: by default deny everything except if expressly be allowed

# Statefull vs Stateless firewalls

---

- Whether the communication state is being tracked or not a network layer firewall:
- **Statefull firewalls**: is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.
- **Stateless firewalls**: Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for.

# iptables firewall



University of Cyprus

Policy: by default  
accept everything  
except if expressly be  
denied

```
root@vmubuntu:~# iptables -v -L
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in      out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in      out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in      out     source               destination
```

# iptables firewall



University of Cyprus

Policy: by default deny  
everything except if  
expressly be allowed

```
root@vmubuntu:~# iptables -P INPUT DROP
root@vmubuntu:~# iptables -v -L
Chain INPUT (policy DROP, 0 packets, 0 bytes)
  pkts bytes target    prot opt in      out     source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in      out     source destination

Chain OUTPUT (policy ACCEPT 84 packets, 9198 bytes)
  pkts bytes target    prot opt in      out     source destination
```

# iptables firewall



University of Cyprus

```
root@vmubuntu:~# ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
^C
--- localhost ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24025ms

root@vmubuntu:~# iptables -A INPUT -i lo -j ACCEPT
root@vmubuntu:~# iptables -V -L
Chain INPUT (policy DROP 82 packets, 7608 bytes)
  pkts bytes target     prot opt in     out     source    destination
    0      0 ACCEPT     all  --  lo      any      anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 176 packets, 17748 bytes)
  pkts bytes target     prot opt in     out     source    destination
root@vmubuntu:~# ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.088 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.067 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.049 ms
^C
--- localhost ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.049/0.068/0.088/0.015 ms
```



# iptables firewall



University of Cyprus

insert  
rules

show  
rules

```
root@vmubuntu:~# iptables -A INPUT -i eth0 -p icmp -j ACCEPT
root@vmubuntu:~# iptables -A INPUT -i eth0 -p udp -m udp --sport 53 --dport 1024:65535 -j ACCEPT
root@vmubuntu:~# iptables -A INPUT -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
root@vmubuntu:~# iptables -A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
root@vmubuntu:~# iptables -A INPUT -i eth0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
root@vmubuntu:~# iptables -A INPUT -s 155.207.113.0/24 -j ACCEPT
root@vmubuntu:~# iptables -v -L
```

Chain INPUT (policy DROP 58 packets, 7688 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
26	2674	ACCEPT	all	--	lo	any	anywhere	anywhere	
0	0	ACCEPT	icmp	--	eth0	any	anywhere	anywhere	
0	0	ACCEPT	udp	--	eth0	any	anywhere	anywhere	udp spt:domain dpts:1024:65535
0	0	ACCEPT	tcp	--	eth0	any	anywhere	anywhere	state RELATED,ESTABLISHED
0	0	ACCEPT	tcp	--	eth0	any	anywhere	anywhere	tcp dpt:ssh state NEW
0	0	ACCEPT	tcp	--	eth0	any	anywhere	anywhere	tcp dpt:www state NEW
0	0	ACCEPT	all	--	any	any	csd-net/24	anywhere	

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

Chain OUTPUT (policy ACCEPT 121 packets, 12262 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------