Dr. Ammar Haider
Assistant Professor
School of Computing

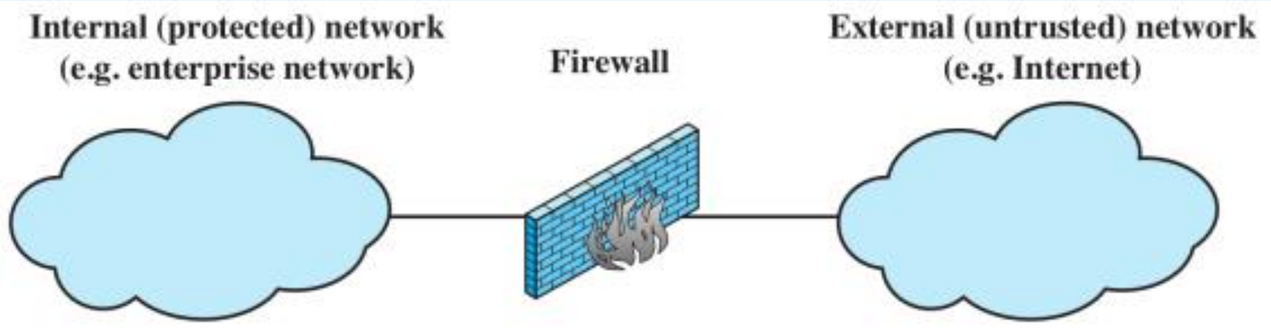
CS3002 Information Security

Firewalls

Reference: Stallings SPP chap 9

Firewalls

- Internet connectivity is essential for organizations
  - However it creates a threat
- Firewalls are effective means of protecting LANs
  - Protection at single point, rather on every computer within LAN
- Inserted between the premises network and the Internet to establish a controlled link
- Used as a perimeter defense
  - Single choke point to impose security and auditing
  - Insulates the internal systems from external networks


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

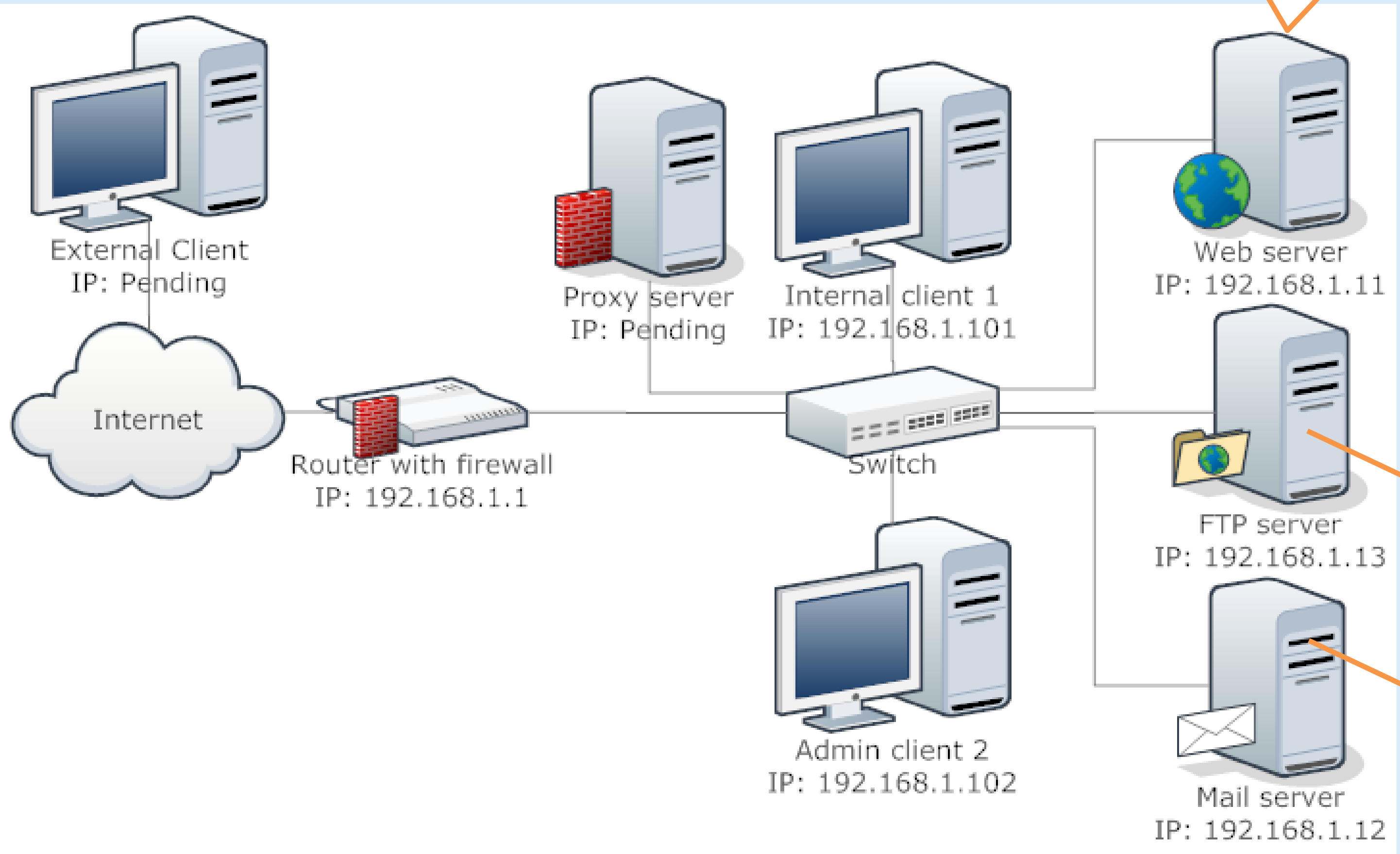
Firewall Design Goals

- All traffic inside to outside and opposite, 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

Firewall Security Policies

- Service control, e.g. filter based on IP address, port number
- Direction control, e.g. to internal LAN, to external Internet
- User control, e.g. student vs faculty
- Behaviour control, e.g. filter too frequent requests, email with spam

Example Firewall Jobs



Accessible to external users

Only accessible within company

Accessible to external users

Firewall Types

- Packet Filtering: accepts/rejects packets based on L3 & L4 protocol headers
- Stateful Packet Inspection: like packet filtering firewall, but considers state information (what happened previously)
- Circuit-level Proxy: relay for transport connections
- Application Proxy: relay for application traffic

Packet Filtering Firewall

- Security policy implemented by set of rules
  - Rules define which packets can pass through the firewall
- Firewalls inspects each arriving packet (in all directions), compares against rule set, and takes action based on matching rule
- Default policies: action for packets for which no rule matches
  - Accept (allow, forward)
  - Drop (reject, discard) - recommended

Packet Filtering Rules

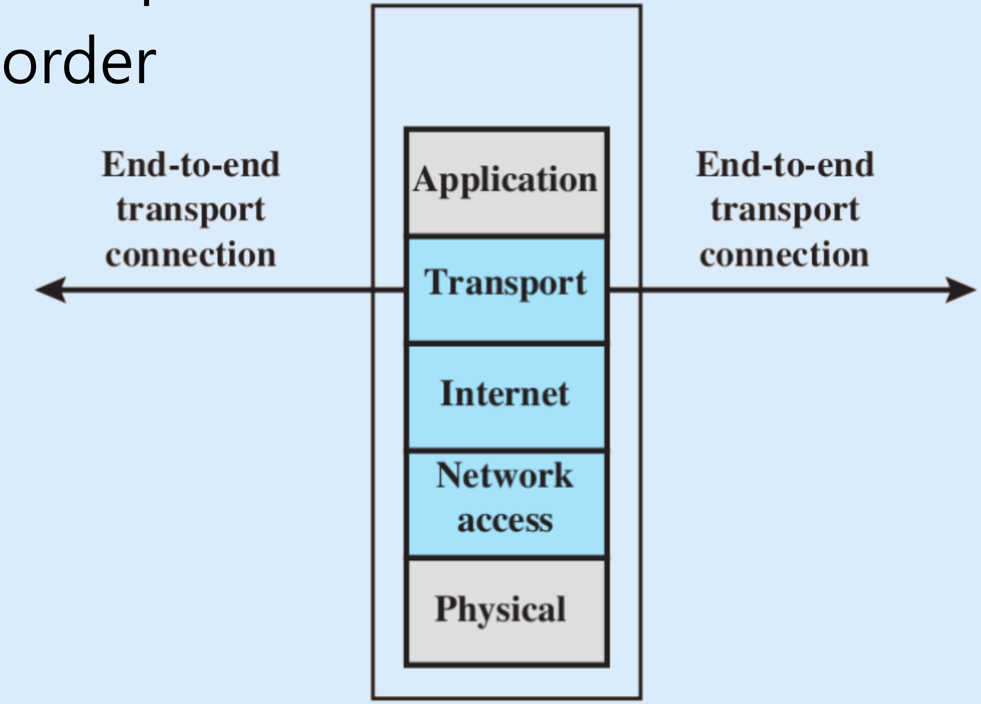
Packet Information (parameters to consider)

- IP address: identifies host or network
- Port number: identifies applications, e.g. web (80), email (25)
- Protocol number: identifies transport protocol, e.g. TCP or UDP
- Direction (or firewall interface): which way packet is coming in, which way going out
- Other transport, network, data link packet header fields (e.g. ICMP data types)

Packet Filtering Rules

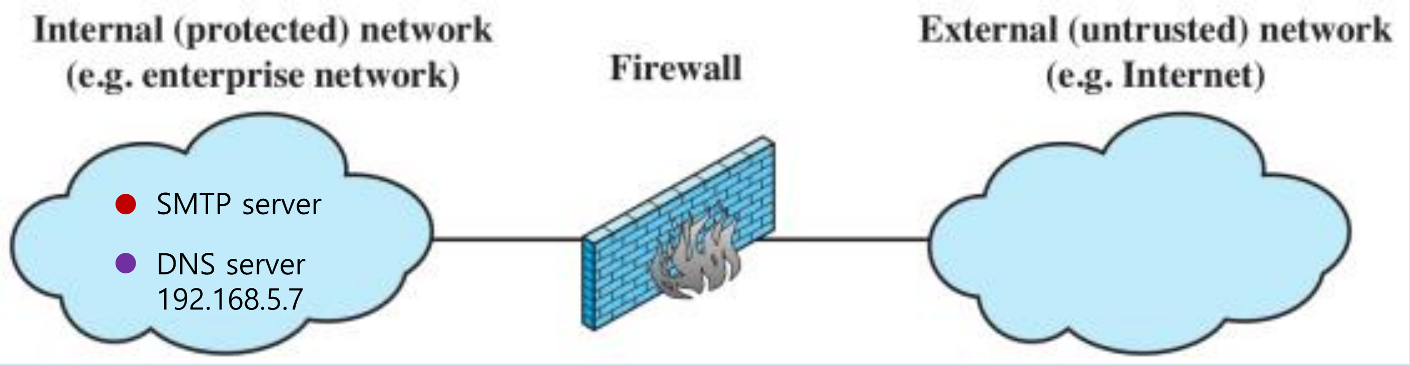
Rules

- Conditions defined using packet information, direction
- Wildcards (*) support to match multiple values
- Actions typically accept or drop
- List of rules processed in order



Packet Filtering: Example Rules

#	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	ACTION
1	In	External	SMTP-server IP	TCP	≥1024	25	Permit
2	Out	SMTP-server IP	External	TCP	25	≥1024	Permit
3	Out	Internal	External	TCP	≥1024	25	Permit
4	In	External	Internal	TCP	25	≥1024	Permit
5	In	External	192.168.5.7	UDP	≥1024	53	Permit
6	Out	192.168.5.7	External	UDP	53	≥1024	Permit
7	Either	Any	Any	Any	Any	Any	DROP


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
● SMTP server
● DNS server
192.168.5.7

Packet Filtering: Example Rules

#	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	ACTION
1	In	External	SMTP-server IP	TCP	≥1024	25	Permit
2	Out	SMTP-server IP	External	TCP	25	≥1024	Permit
3	Out	Internal	External	TCP	≥1024	25	Permit
4	In	External	Internal	TCP	25	≥1024	Permit
5	In	External	192.168.5.7	UDP	≥1024	53	Permit
6	Out	192.168.5.7	External	UDP	53	≥1024	Permit
7	Either	Any	Any	Any	Any	Any	DROP

Rules 1-2: Allow incoming emails (port 25 = SMTP) and associated TCP ACKs

Rules 3-4: Allow outgoing emails and associated TCP ACKs

Rules 5-6: Allow DNS requests (inbound) and responses (outbound)

Rule 7: Default rule when no other rule matches

Reminder: port numbers 1024 and greater are used by client applications.

Packet Filtering Firewall

Advantages

- Simplicity and speed
- Transparent to users

Disadvantages

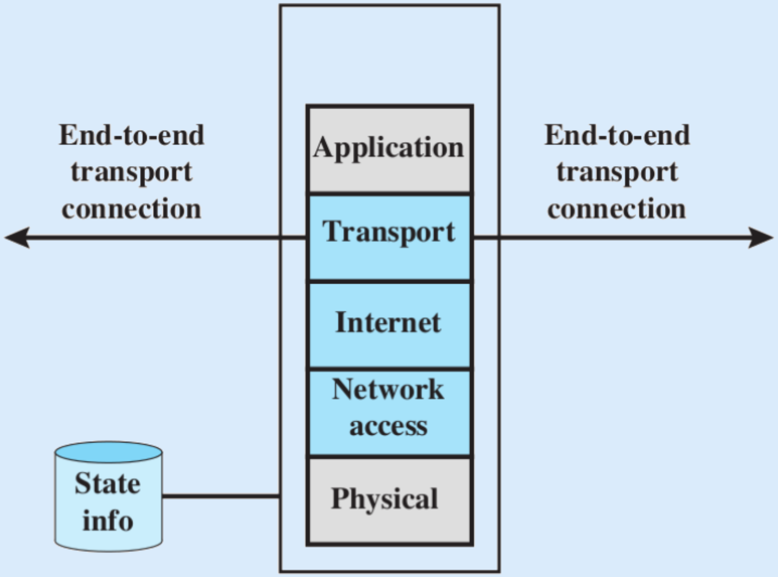
- Cannot prevent attacks that employ application specific vulnerabilities or functions
- Limited logging functionality
- Do not support advanced user authentication
- Can’t prevent attacks using IP spoofing
- Improper configuration can lead to breaches

Stateful Packet Inspection

- Traditional packet filtering firewall makes decisions based on individual packets; without considering past packets (stateless)
- Many applications establish a connection between client/server; so a group of consecutive packets belong to same connection
- Often easier to define rules for connections, rather than individual packets
- Need to store information about past behavior (state)
- Stateful Packet Inspection (SPI) is extension of traditional packet filtering firewalls
  - extra overhead required for maintaining state information
  - but faster processing of most packets

Stateful Packet Inspection

- For packets accepted by packet filtering firewall, record connection information
  - src/dest IP address, src/dest port, sequence numbers, connection state (e.g. new, established, closing)
- Packets arriving that belong to existing connections can be accepted without processing by firewall rules


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

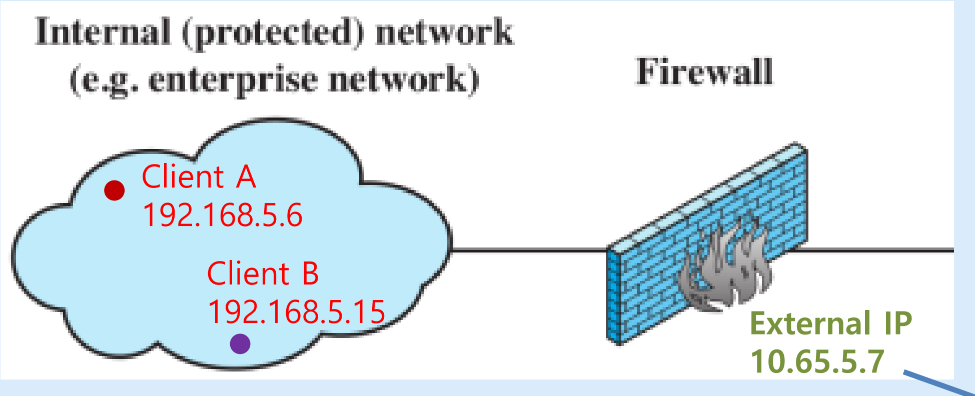
Stateful Packet Inspection

- Simplifies the rule set by being more permissive on existing connections

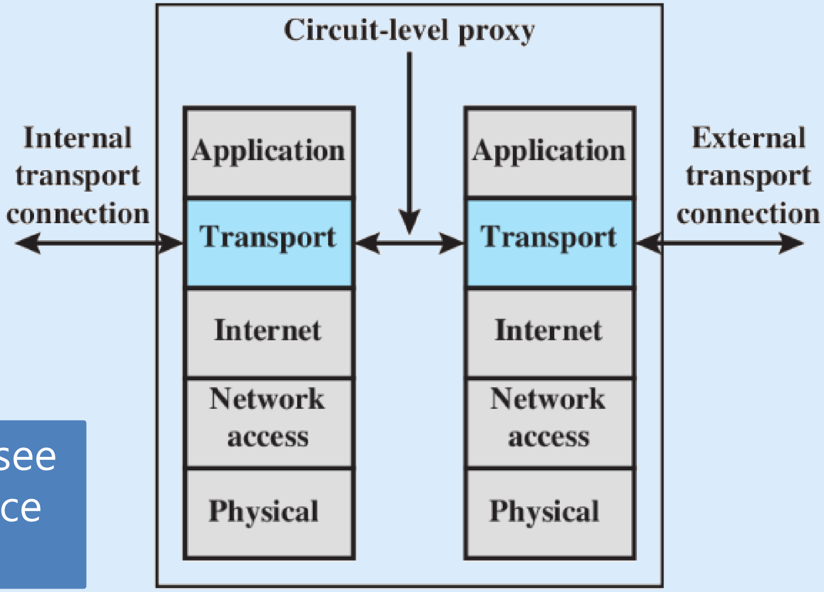
#	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Connection	ACTION
1	Either	Any	Any	TCP	Any	Any	Established	Permit
2	In	External	SMTP-IP	TCP	≥1024	25	New	Permit
3	Out	Internal	External	TCP	≥1024	25	New	Permit
4	Either	Any	Any	Any	Any	Any	Any	DROP

Circuit-level Proxy

- Also called Circuit-level Gateway
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
  - For incoming data
    - Proxy is server to internal network clients
  - For outgoing data
    - Proxy is client sending out data to the internet



External users see this IP as source of all traffic

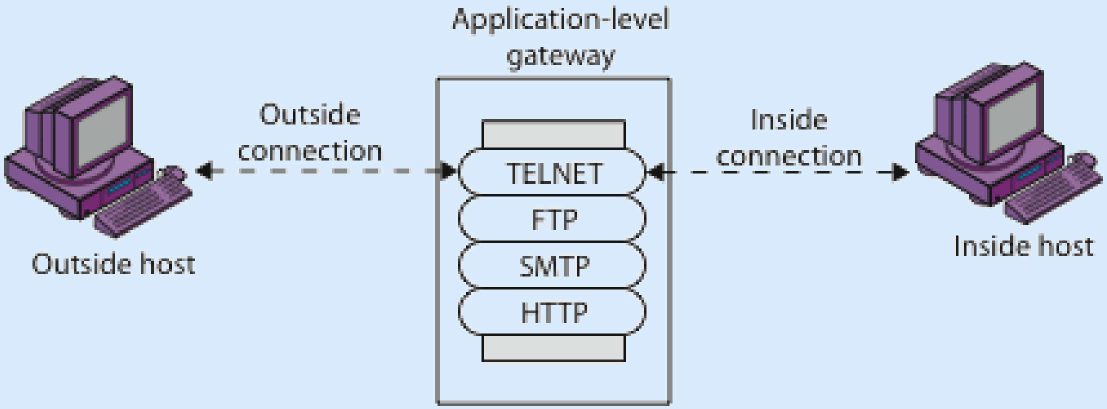


Circuit-level Proxy

- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed
- Does not examine application layer payload
- Typically used for outbound connections when inside users are trusted
  - Any (external) data that is requested by internal users is allowed in.
  - Incoming data that was never requested is blocked.

Application-level Gateway

- Inspects the application level operations (e.g. HTTP response contents, email contents) and allows/denies them based on predefined rules.
- Also logs attempted-access and allowed-access events
- Mostly implemented as a proxy, i.e. like a circuit-level gateway it maintains separate connections
  - client ↔ proxy, proxy ↔ server



Application-level Gateway

- Advantage
  - Tend to be more secure than packet filters

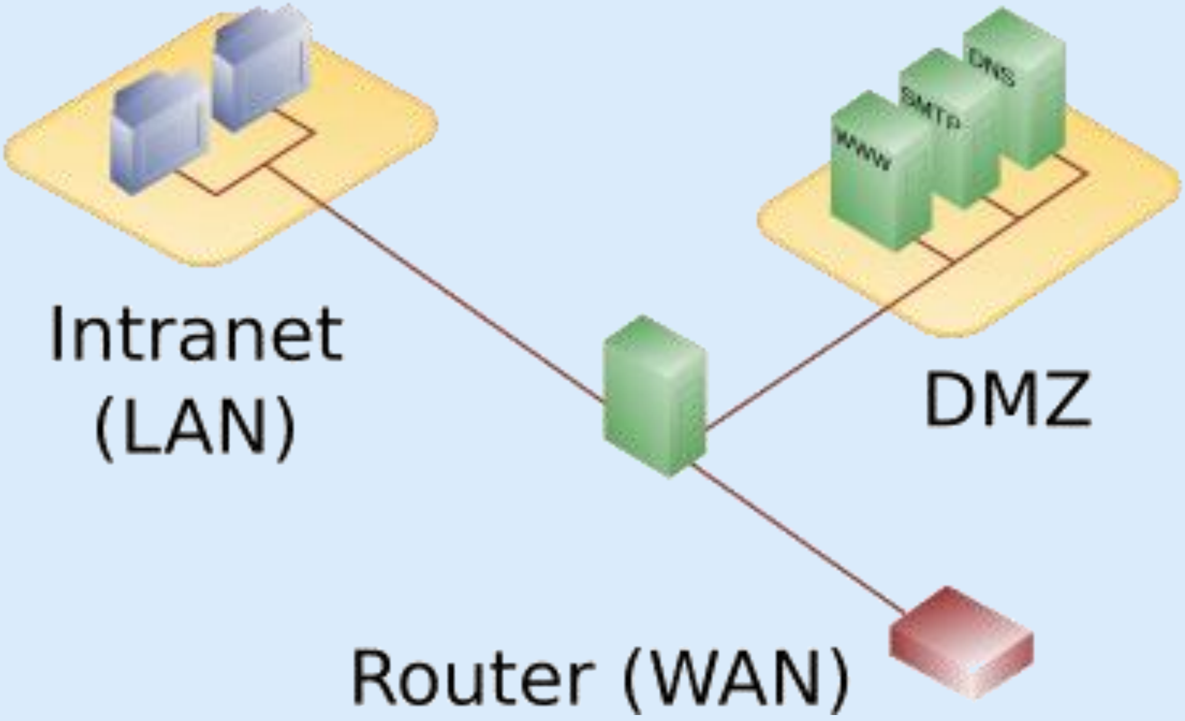
- Disadvantages
  - additional processing overhead on each connection
  - can become a bottleneck
  - No end-to-end encryption due to MITM like behavior

Firewall Location

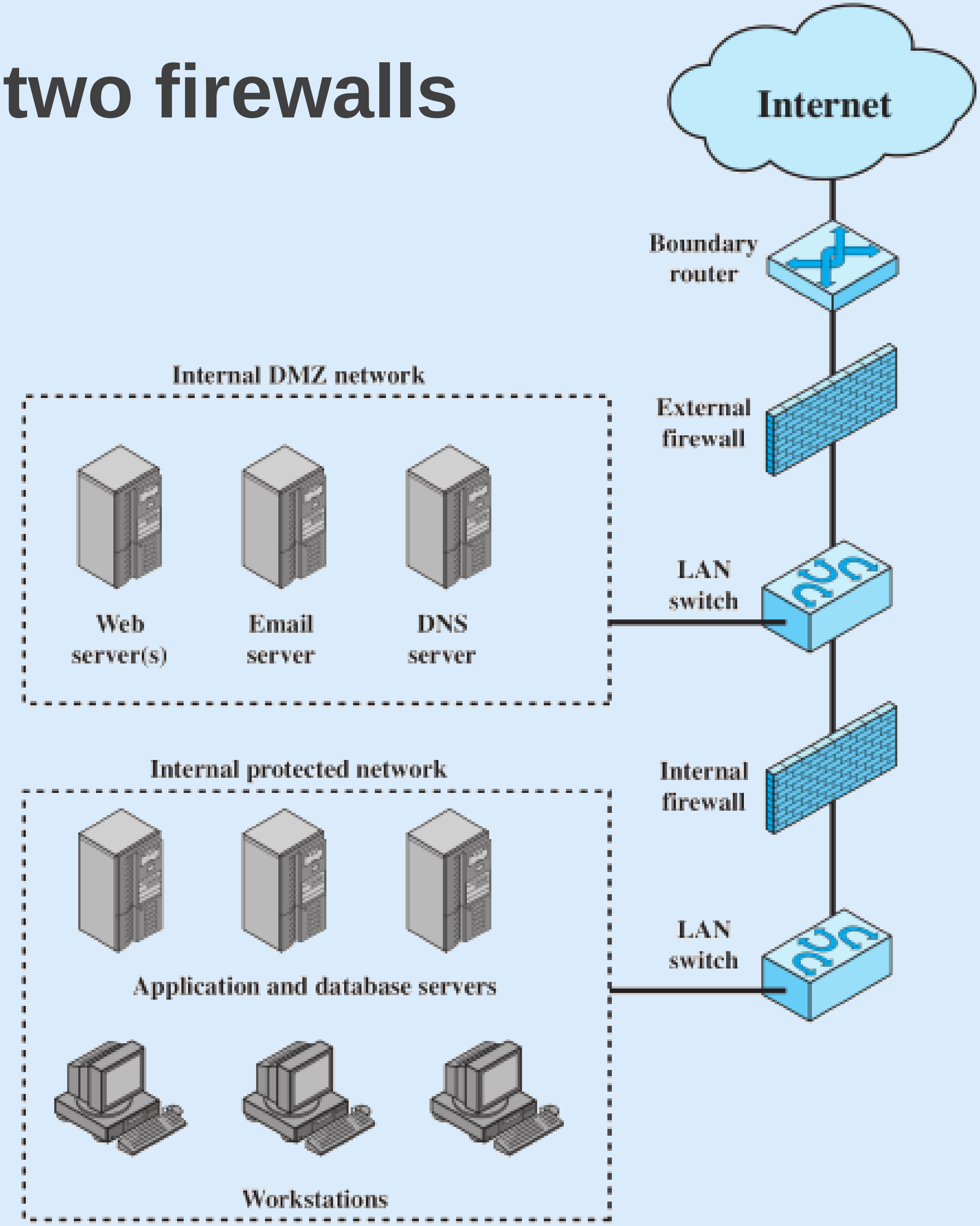
- Firewalls can be located on hosts: end-users computers and servers
- With large number of users, firewalls located on network devices that interconnect internal and external networks

- Common to separate internal network into two zones:
  1. Public-facing servers, e.g. web, email, DNS
  2. End-user computers and internal servers, e.g. databases, development web servers
- Public-facing servers put in De-Militarized Zone (DMZ)

DMZ with one firewall



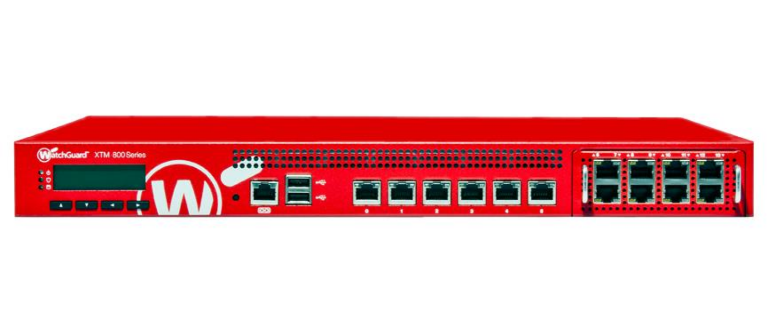
DMZ with two firewalls



Firewall: Additional Capabilities

Normally a firewall is implemented on the gateway router. Since it is a single choke point, it can also offer additional features:

- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related, e.g. accounting, address and port translation (NAT)
- Can serve as platform for VPN endpoint



Firewall Limitations

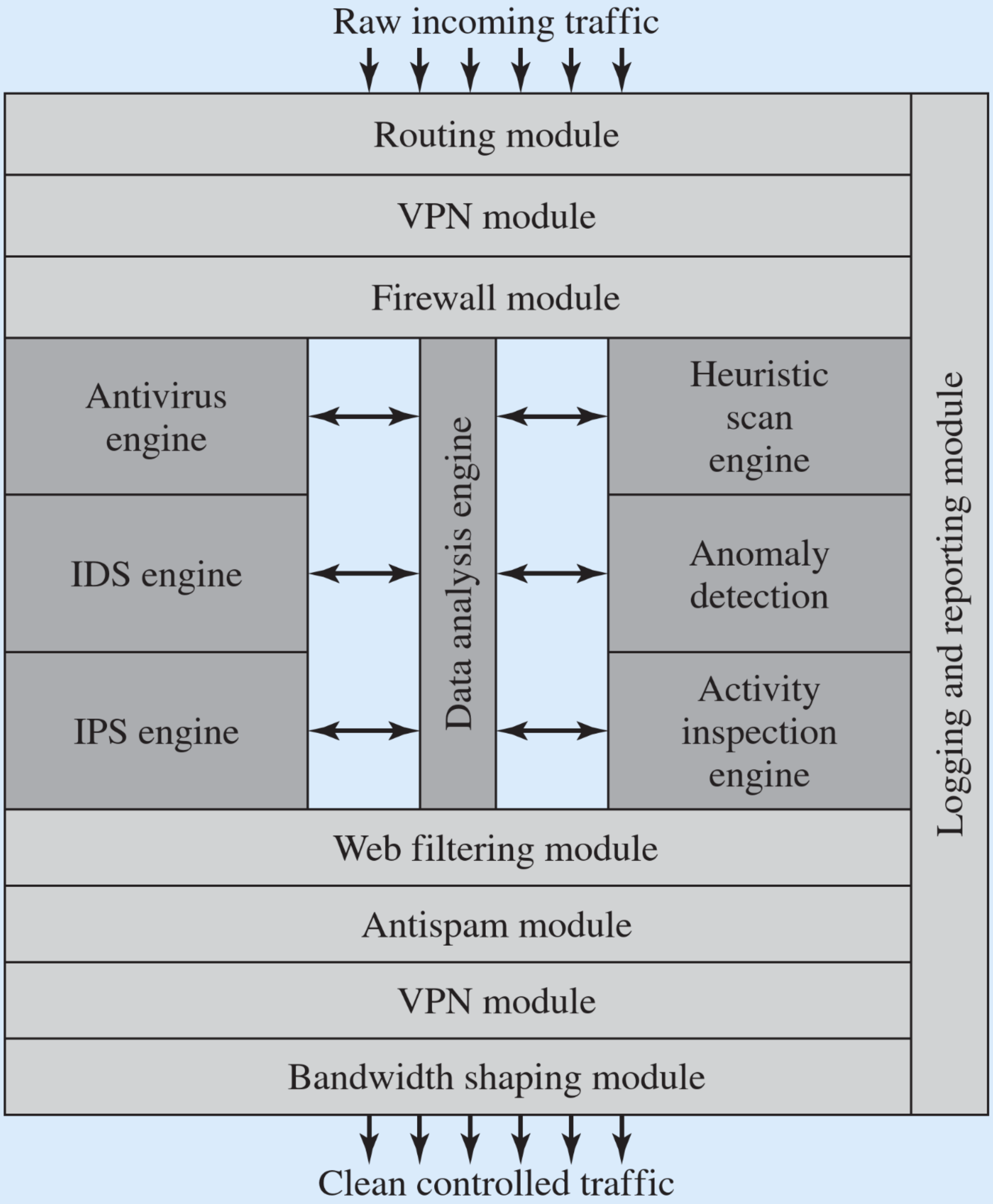
- Cannot protect against attacks bypassing firewall (mobile data connections, direct connections to peer organizations)
- May not protect fully against internal threats (e.g. rogue employees)
- Laptop, phone, or USB drive may be infected outside the corporate network then used internally
- Complexity and human error: writing firewall rules that implement the security policy is difficult for large networks
- Cannot inspect (encrypted) tunneled packets

Integrated Security Products

- An organization typically needs several layers of defense, like:
  - Anti-malware service
  - Intrusion detection & prevention system
  - VPN server
  - Firewall
  - Anti spam
- Configuring, managing and deploying several different security softwares can become a chore, not to mention performance degradation

Integrated Security Products

- To reduce this administrative & performance burden, several vendors now supply all-in-one products.
- Typically, these are called Unified Threat Management (UTM) appliances.
- A UTM product will perform (at least) network firewalling, network intrusion detection & prevention and gateway anti-virus.



UTM Architecture