CSCI262 : System Security

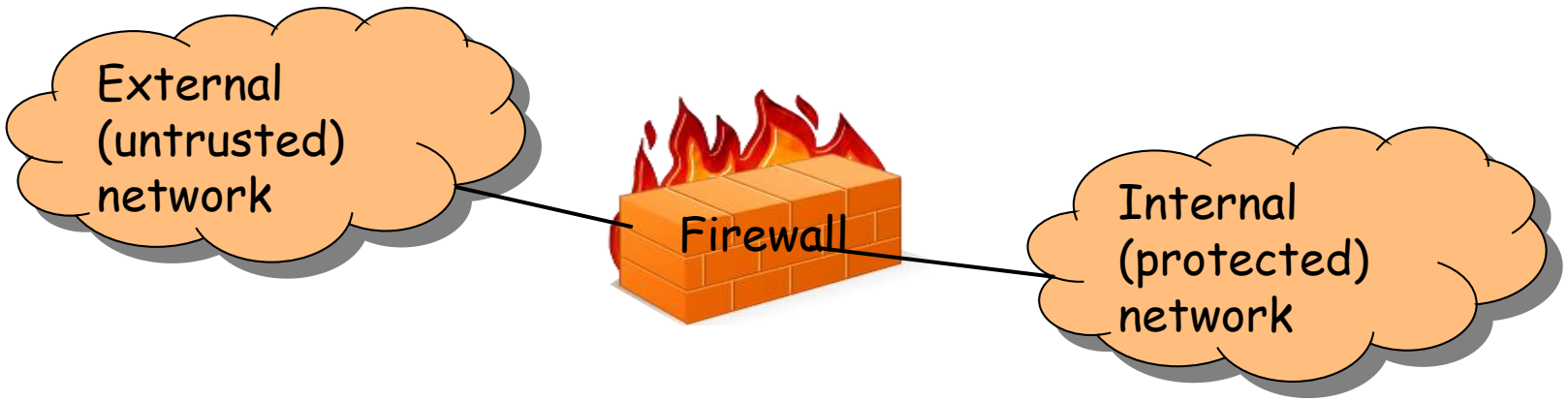
Week 9: Firewalls and Intrusion Prevention Systems (IPS)

Schedule

- What is a firewall?
- Firewall characteristics and Access Policy
- Types of firewalls
- Firewall architectures
- Intrusion Prevention Systems (IPS)

What is a firewall?

- A mechanism or device for controlling connections/traffic between networks.
  - The control can be at different levels, by IP address or content, for example.
- They can effectively enforce some access control and implement security policies.
  - Generally, they are designed to distinguish between the “trusted” internal network and the “distrusted” external network.



Infrastructure motivates firewall use

- There are certain common types of infrastructures:
  - A Centralized data processing system, with a central mainframe supporting a number of directly connected terminals.
  - Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.
  - Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two.
  - Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN).

- Consider equipping each workstation and server on the such networks with strong security features, including intrusion protection?
- This could be very expensive, and not necessarily efficient.
- So, the firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter.
- It is an effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet.
- The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

Design goals for a firewall

- Access to the network, either in or out, should be through the firewall.
  - Physically the firewall should be the only access point in/out of the network.
- Only authorised traffic should be allowed through the firewall.
  - Authorisation is defined with respect to the security policies implemented on the firewall.
- The firewall needs to be “invulnerable”.
- The firewall needs to be trusted.

General control techniques

- Basically: “What can filtering be based on?”:
  - **Service control:** Determines the type of services accessible, based, for example, on IP address and TCP port numbers.
  - **Direction control:** Determines which direction particular services may be requested in.
  - **User control:** Tailors usage to particular users. This is more likely to be applied to internal users, for it to apply to external users appropriate authentication mechanisms would be needed.
  - **Behaviour control:** Within an allowed service particular patterns or structures can be disallowed. This can prevent spam for example.

What can a firewall do?

- Provide a choke point to protect a network from outside. This simplifies security management and deployment.
- Monitor traffic, in particular for attempted security breaches.
- Provide a platform for some non-security functions, such as Network Address Translators.
  - That’s network layer functionality.

What can’t a firewall do?

- A firewall cannot:
  - Protect against internal attackers.
  - Practically protect against malware or programs infected with malware.
  - Protect against services that bypass the firewall. For example, a dial-in service to a local area network may not pass through the firewall.

NAT and PAT

- These aim to hide internal network addresses (TCP/IP) from the outside world.
- **N**etwork **A**ddress **T**ranslation:
  - Has a collection of valid external IP addresses which are mapped to internal computers.
- **P**ort **A**ddress **T**ranslation:
  - One external address as the proxy for all internal systems.
    - Everything seems to be sourced there.
  - Random and high order ports assigned to internal computers.

Types of firewalls

- Common types of Firewalls:
  - **Packet-filtering firewalls**:
    - Static (1st generation) or dynamic (4th generation).
  - **Stateful inspection firewalls** or **stateful packet filtering** (3rd generation).
  - **Application-level gateway** (2nd generation).
    - Also called proxy servers.
  - **Circuit-level gateway**.
- Firewall solutions may be a mix …

Packet-filtering firewall

- A packet filtering firewall has a collection of rules.
  - Each incoming and outgoing IP packet is weighed up with respect to the rules, and then either forwarded or discarded.
- The rules are typically based on IP or TCP header fields.
  - If a rule is matched, we determine whether to forward or discard the packet.
  - If there is no match to any rule, then a default action is taken.

The default security policy

- Default discard/reject/deny:
  - If there isn’t an explicit rule allowing something, it is blocked.
  - This is a conservative approach. ☺
- Default forward/accept/allow:
  - If there isn’t an explicit rule blocking something, it is allowed.
  - This is a liberal approach.☹

Problems with default allow

- How do you know where problems are going to occur?
- How do you protect new applications?
  - Can people just install anything they like and have it run through the firewall?
- On what basis do you restrict access?
  - The security administrator would need to be very up-to-date to keep this secure.

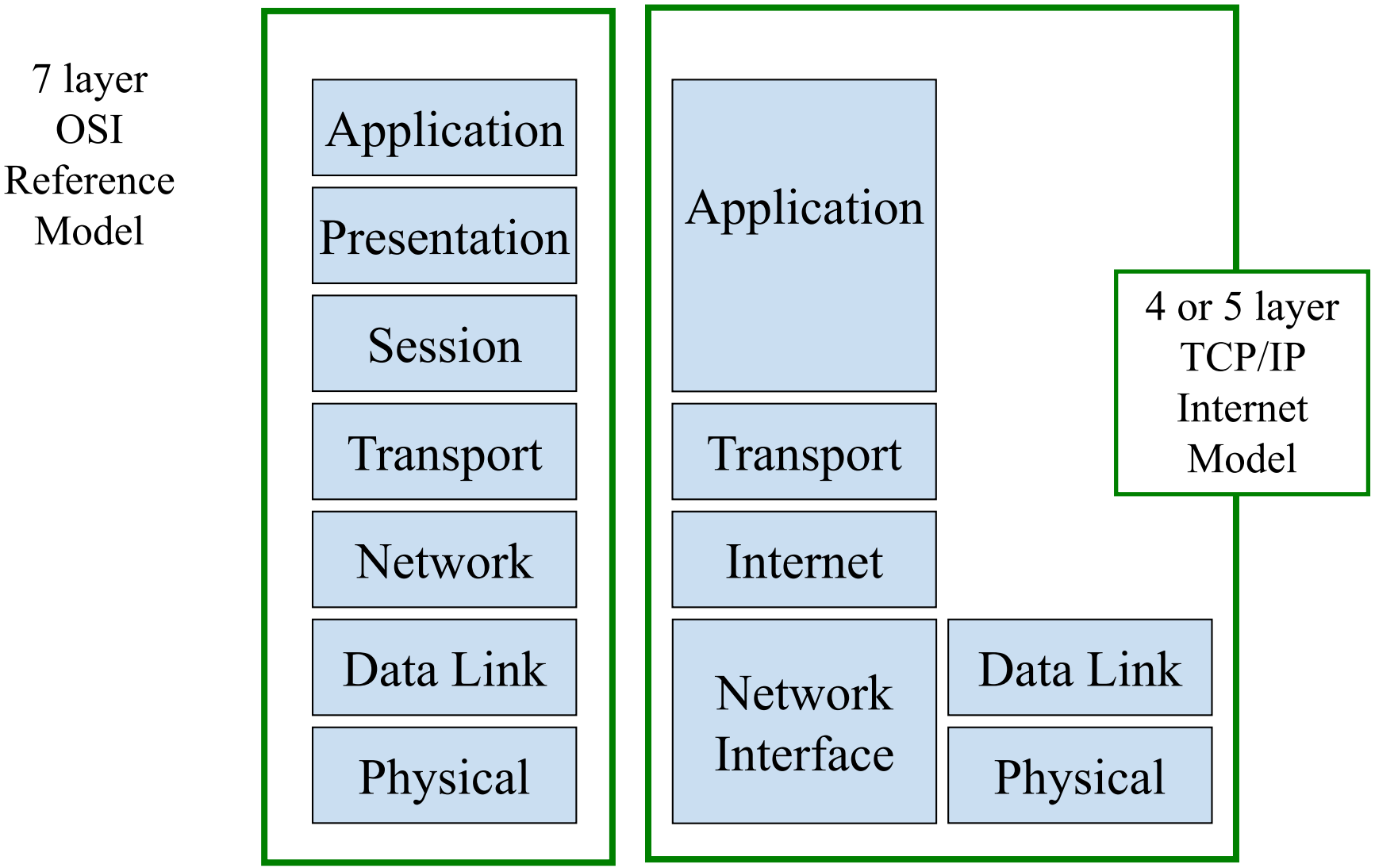
Packet-filtering firewall: Pros and cons

- Packet filtering firewalls are simple and fast.
- They are transparent to users.

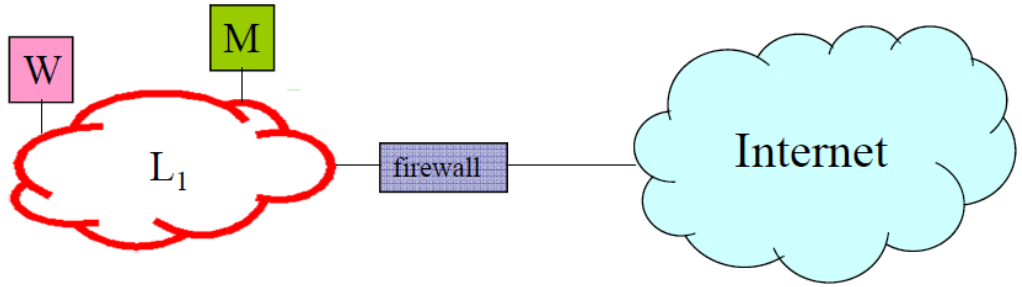
But…

- They don’t examine upper-layer data, so cannot prevent, for example, application layer attacks.
  - Logging is limited since there is limited access to the data, which will primarily be upper layer.
  - The lack of upper layer access also typically means they don’t support very substantial user authentication, even though it’s possible for there to be some
- They are generally vulnerable to TCP/IP based attacks, such as network layer address spoofing.
- Improper configuration can cause security breaches. They are not easy to configure.

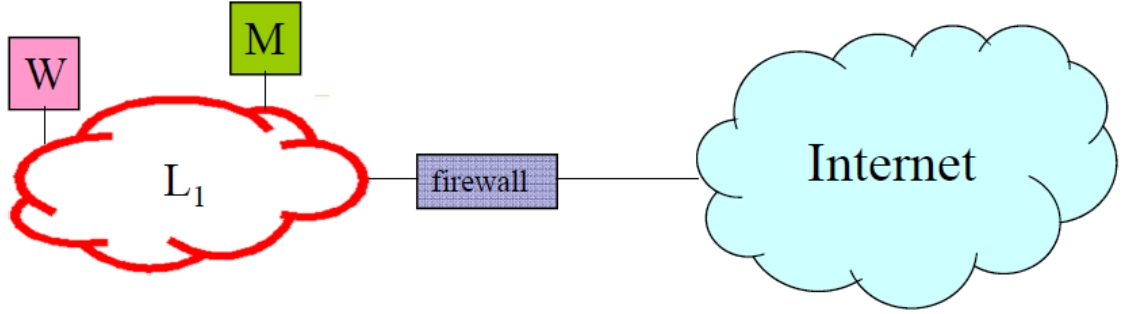
OSI versus TCP/IP Model



Filtering example:



- For network L_1, we would like to allow outsiders to:
  1. Access the web server running on W.
  2. Access the SMTP (email) server on M.
  3. Access the DNS server on M.
- We would also like users/programs on L_1 to:
  4. Send e-mail through the SMTP server on M, i.e. allow the SMTP server on M to access external SMTP servers.
  5. Access an external NTP (Network time protocol) server;
- Finally …
  6. We assume that the DNS server on L_1 can make DNS queries to external DNS servers.
  7. No other traffic is allowed between L_1 and outside.

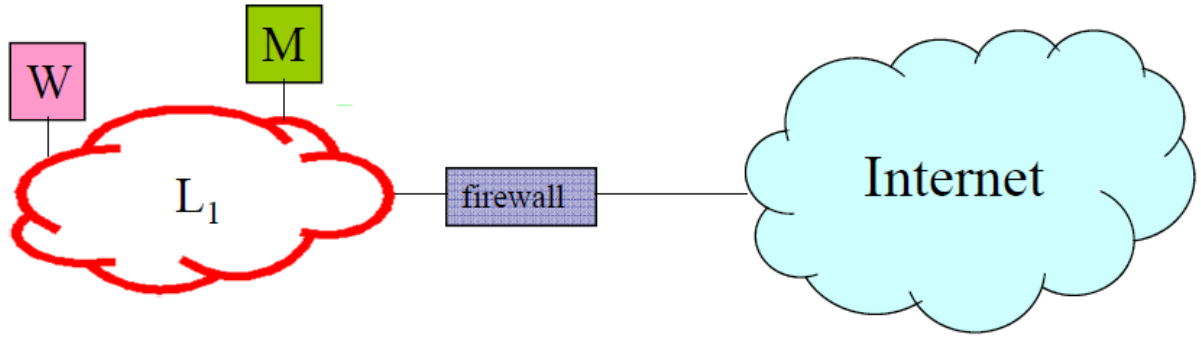


Aim	Inbound	Outbound
1	Request to Web server on W	Response from Web server on W
2	Request to SMTP server on M	Response from SMTP server on M
3	Request to DNS server on M	Response from DNS server on M
4	Response from external SMTP server from SMTP server on M	Request from SMTP server on M to external SMTP server
5	Response from external NTP server	Request to external NTP server
6	Response from external DNS server to DNS server on M	Request from DNS server on M to external DNS server

L1=10.21.*.*

W=10.21.5.9

M=10.21.5.7



To achieve Aim 1 we use the following rules …

Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	ACK Set	Action
A	In	Any	10.21.5.9	TCP	>1023	80	Either	Permit
B	Out	10.21.5.9	Any	TCP	80	>1023	Yes	Permit
C	Either	Any	Any	Any	Any	Any	Either	Deny

Port 80 is associated with http traffic.

Rule C is default deny so we might not explicitly include it.

Static vs dynamic packet filtering

- In static packet filtering rules are developed prior to installation and installed with the firewall, and subsequently changed by direct human input.
- In dynamic packet filtering, the firewall is able to respond to events and change the rules as appropriate.
  - So while static might allow all authentication packets through, dynamic might only allow that in response to a specific request.
    - Effectively a particular packet with a particular source, destination and port address.

Attacks on packet-filtering firewall

- **IP address spoofing**:
  - The intruder transmits packets from outside with a source IP address field containing a (hopefully) trusted address, such as that of an internal host.
- **Source routing attacks:**
  - The source station specifies a particular route that a packet should take as it crosses the Internet.
    - The attacker hopes the source routing information won't be analysed.
    - So source routed packets will normally be dropped.
- **Tiny fragment attacks**:
  - The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment.
    - So the fragment isn't treated in the same way as it normally would be.

Stateful inspection firewall …

- Traditional packet filters are stateless, that is they deal with packets independently.
- Stateful inspection firewalls allow a more dynamic structure, based on context.
  - Some sort of user authentication can be required before an “allow” entry for a particular connection is established.
    - Typically supporting client/server interaction.
  - Communication within a session can be allowed through identifying the source and destination details.

For a stateful inspection firewall …

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	1035	173.66.32.122	25	Established
223.43.21.231	1990	192.168.1.6	80	Established
24.102.32.22	1025	192.168.0.1	80	Established

Stateful Inspection firewalls

- **Advantages:**
  - They only allow packets belonging to an allowed session.
  - They can authenticate the user when the session is established.
  - They can determine whether the packets really carry HTTP, and it can enforce constraints at the application layer (e.g., filtering URLs to deny access to black-listed sites).
  - They can check the packet against the firewall's rule set, which can be extensive.

- **Disadvantages:**
  - Additional cost when the firewall's rule set is updated.
- The concept of deep packet inspection is unrelated to stateful firewalls.
  - With deep packet inspection it’s possible to inspect the user data in the, and as such it is an application layer firewall.

Application-level gateway (or proxy servers)

- These act as relays for application level traffic, often of limited types, such as web traffic.
  - These act on the application layer of the TCP/IP stack, application, session or presentation in OSI.
- End-to-end connections between server and client are not formed.
- Outgoing and incoming traffic are both inspected.
  - Checks application content for appropriateness, such as restricting particular websites.
  - Checks the format for protocol data.
    - In particular it can protect against malformed IP or TCP packets.
  - The latter can be difficult to do for complex protocols though.

- **Advantages:**
  - Higher security than packet filters.
  - Only need scrutinize a few allowable applications.
  - Easy to log and audit all incoming traffic.
- **Disadvantages:**
  - Additional processing overhead on each connection.

Circuit-level gateway

- This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications
- A circuit-level gateway does not permit an end-to-end TCP connection
  - The gateway 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
  - Once connected, the gateway typically relays TCP segments from one connection to the other without examining the contents
- The security function consists of determining which connections will be allowed.

- **Advantages:**
  - comparatively inexpensive and provide Anonymity to the private network.
- **Disadvantages:**
  - do not filter Individual Packets.

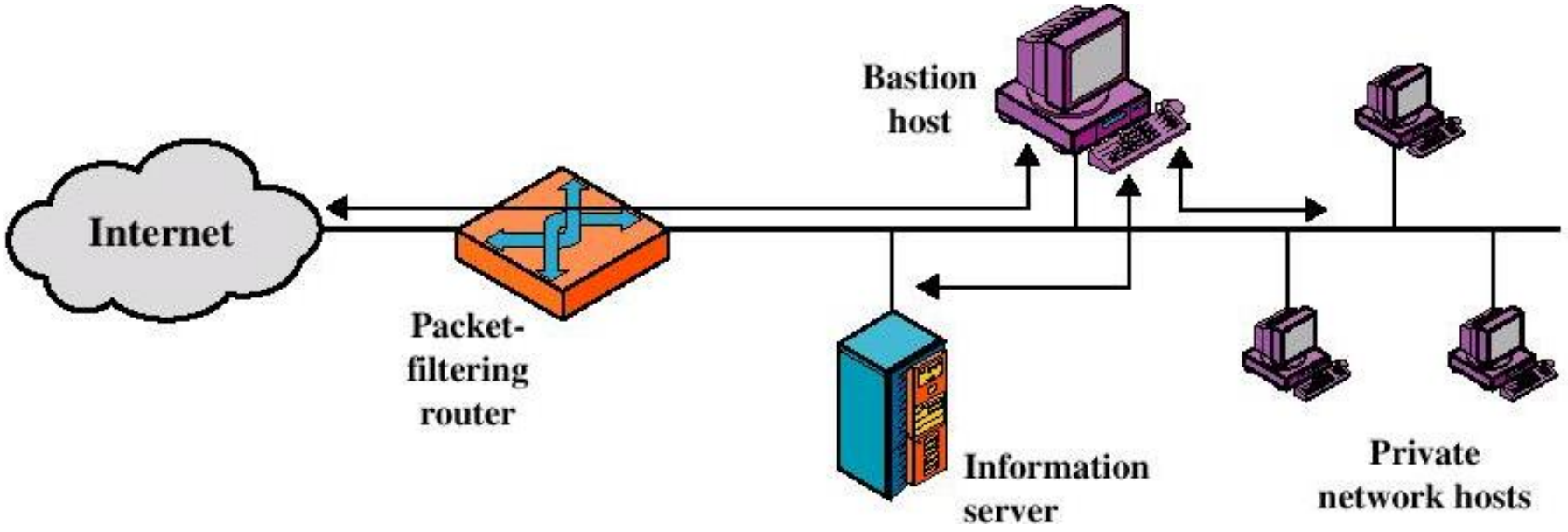
Firewall Architecture

- Packet-filtering routers:
  - Add firewall functionality to a border router.
- Single homed bastion host, or screened host firewall.
- Double or dual-homed bastion hosts.
- Screened subnet firewall with a DMZ.

Bastion Hosts

- These are hosts identified by the firewall administrator as critical points in the security of a network.
  - A bastion is a particular strong point on the outside of a fortification, and the bastion host obtains it's name by performing somewhat similar functionality.
- They typically have limited functionality, to reduce exposure to vulnerabilities and improve performance, and serve as a platform for an application-level gateway.
- The way in which the bastion host performs, and is fitted with other parts of the system, determines the firewall architecture.

Single-homed bastion host

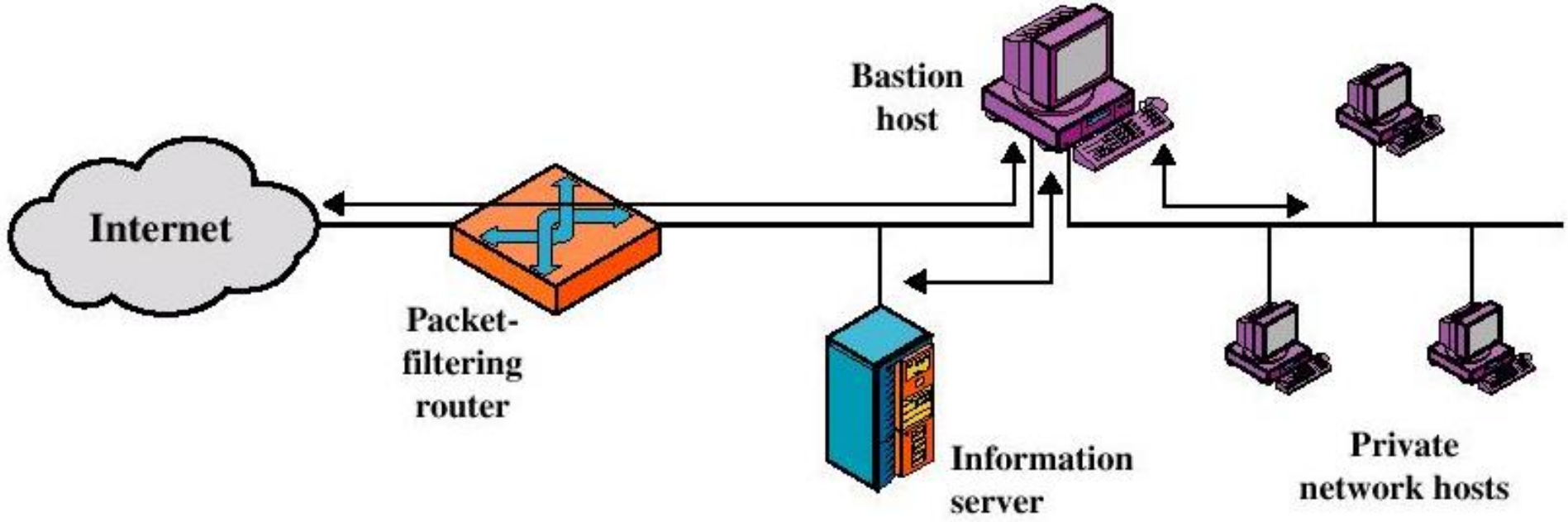


- The firewall is a composite of two systems:
  - A packet-filtering router which pre-filters to reduce the load on the second unit.
    - It allows proxy approved traffic through.
  - A bastion host (probably an application-layer firewall).
    - Provides proxy access for the inside.

- The bastion host can perform authentication and proxy functions that the packet-filtering router (firewall) cannot, because the proxy can see the application level information.
- This improves on single configurations:
  - We have both packet-level and application-level filtering.
    - This gives flexibility in defining security policies.
  - An intruder will needed to get through two separate systems.
- There is also flexibility in providing direct Internet access to, for example, a web server with public information.

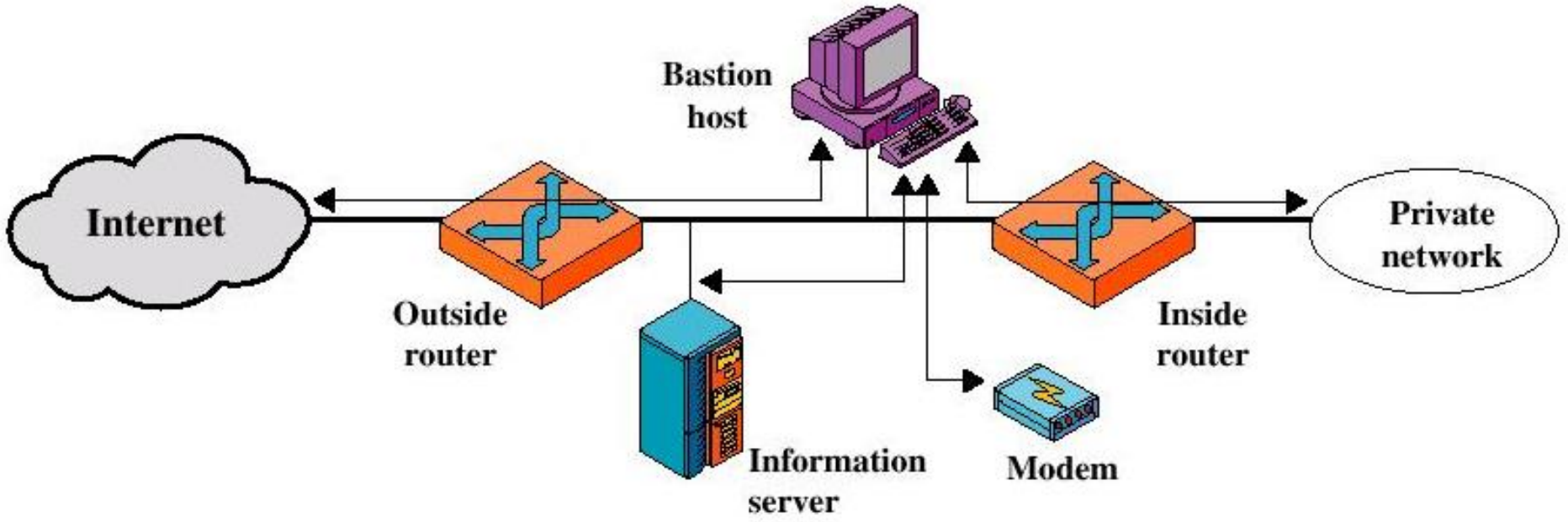
Dual-homed bastion host

This architecture is built around a dual-homed host, i.e. something with at least two network interfaces.



- One interface connects to the external network, another to the internal network.
- Everything (in/out) goes through the bastion host now.
- Will typically use NAT.

Screened-subnet firewall system



- Screened subnet firewall configuration.
  - This is the most common setting.
  - Two packet-filtering routers are used.
  - Creation of an isolated sub-network, the DMZ.

DMZ

- **D**e**M**ilitarised **Z**ones… or screened subnets.
- This is an area between the internal network and the big bad outside world of the internet.
- It will often contain interface servers for, for example, mail and web.

DMZ networks

External firewall:

- provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity
- Provides a basic level of protection for the remainder of the enterprise network

Internal firewall:

- adds more stringent filtering capability to protect enterprise servers and workstations from external attack.
- provides two-way protection with respect to the DMZ
- Multiple internal firewalls can be used to protect portions of the internal network from each other.

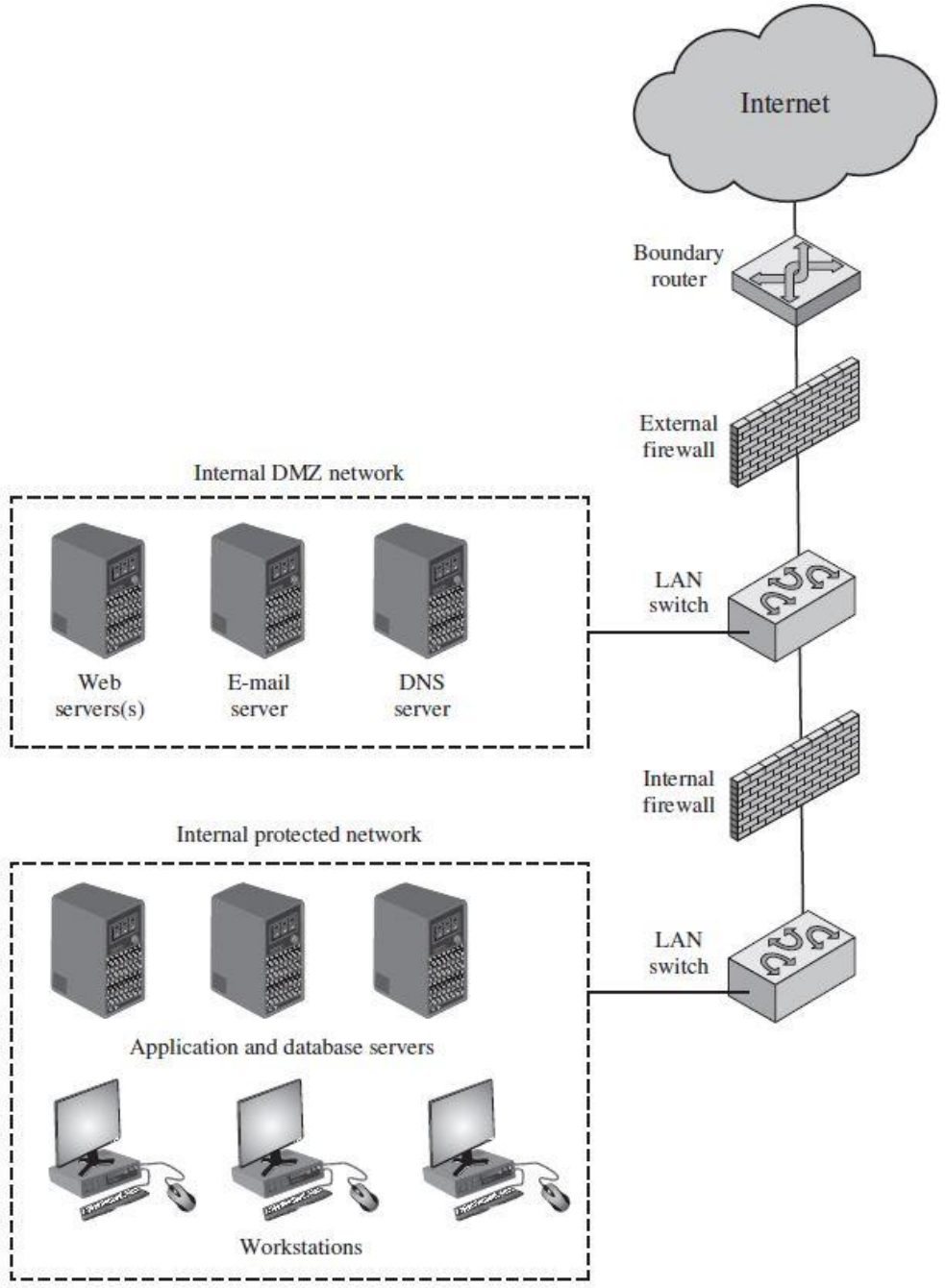


Figure 9.2 **Example Firewall Configuration**

Virtual Private Networks (VPN)

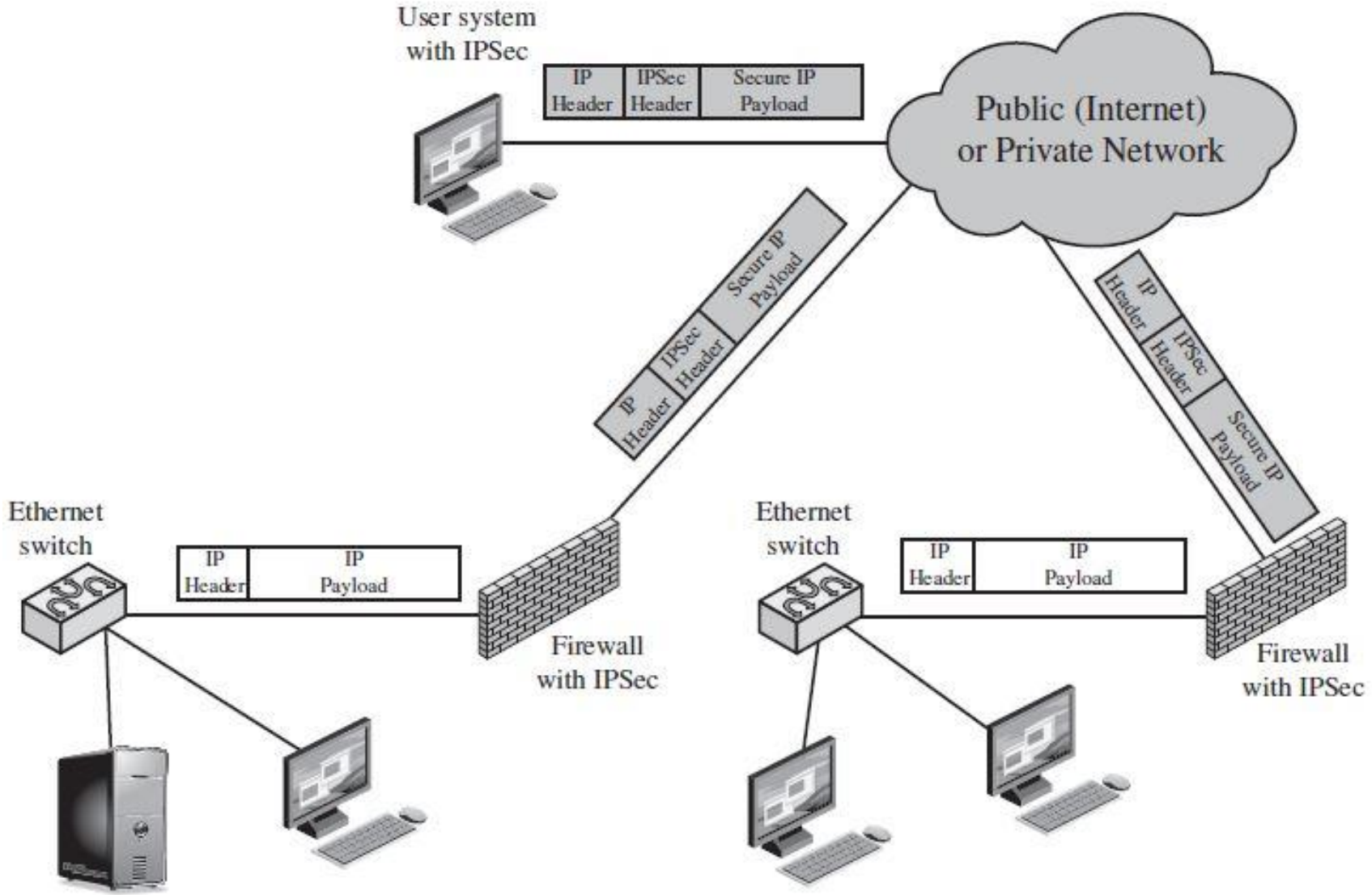


Figure 9.3 A VPN Security Scenario

Distributed Firewalls

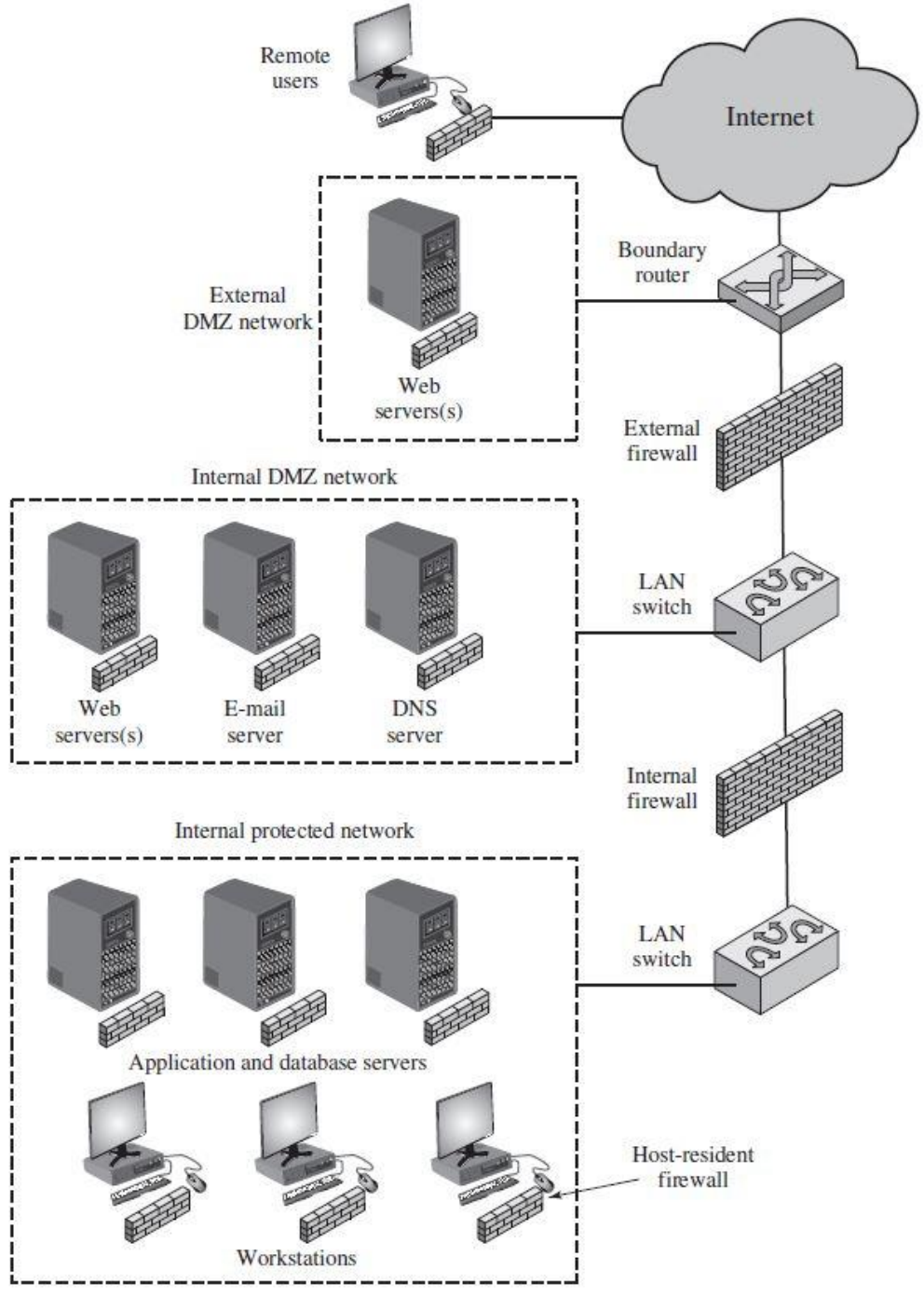


Figure 9.4 **Example Distributed Firewall Configuration**

Firewall limitations

- A firewall cannot protect against attacks that bypass the firewall.
  - Internal systems may have dial-out capability to connect to an ISP.
  - An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- A firewall may not protect fully against internal threats, such as:
  - Disgruntled employees.
  - An employee who unwittingly cooperates with external attacker.

- An improperly secured wireless LAN may be accessed from outside the organization.
  - An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
- A laptop or portable storage device may be used and infected outside the corporate network and then attached and used internally.

IDPS and firewalls …

- While we have been considering IDS/IPS systems and firewalls independently, the design of a security system should really consider all such components together.

Example: Unified Threat Management Products

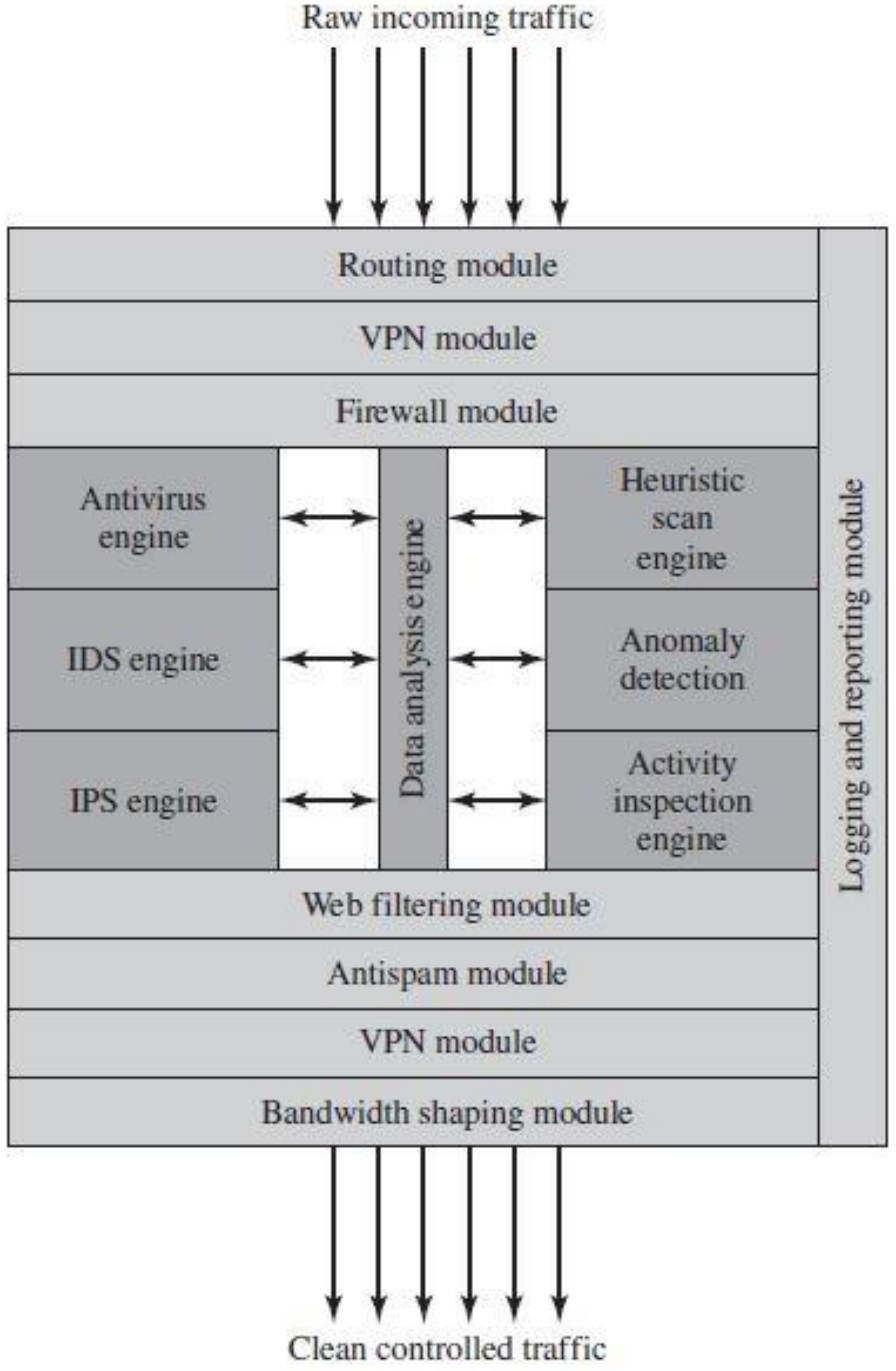


Figure 9.6 **Unified Threat Management Appliance**