CS321: Computer Networks

Firewalls and IDS

Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Jodhpur
E-mail: manaskhatua@iitj.ac.in

Operational Security

- In man organizations, there is a single point of entry/exit where both good guys and bad guys entering and leaving the organization are security-checked.

- In a computer network, when traffic entering/leaving a network is security-checked, logged, dropped, or forwarded, it is done by operational devices
  - firewalls,
  - intrusion detection systems (IDSs), and
  - intrusion prevention systems (IPSs).

Firewalls

- A **firewall**
  - is a combination of hardware and software
  - that isolates an organization’s internal network from the Internet at large,
  - allowing some packets to pass and blocking others.

  - allows a network administrator to control access between the outside world and resources within the administered network by managing the traffic flow to and from these resources

- A firewall has three goals:
  - All traffic from outside to inside, and vice versa, passes through the firewall
    - a single point of access to the network makes it easier to manage and enforce a security-access policy
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
  - The firewall itself is immune to penetration
    - If the firewall is not designed or installed properly, it can be compromised

Cont…

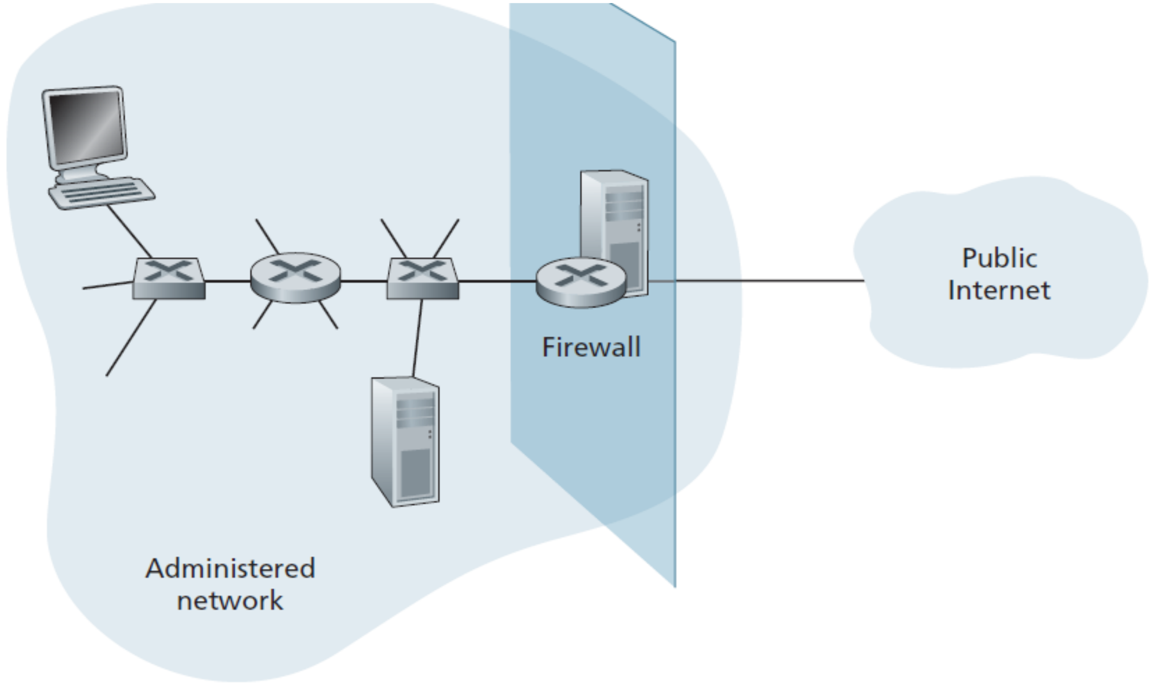


Figure 8.33 ♦ Firewall placement between the administered network and the outside world

- Firewalls can be classified in three categories
  - traditional packet filters,
  - stateful filters, and
  - application gateways.

Traditional Packet Filters

- All traffic leaving and entering the internal network passes through a gateway router
- it is at this router where **packet filtering** occurs

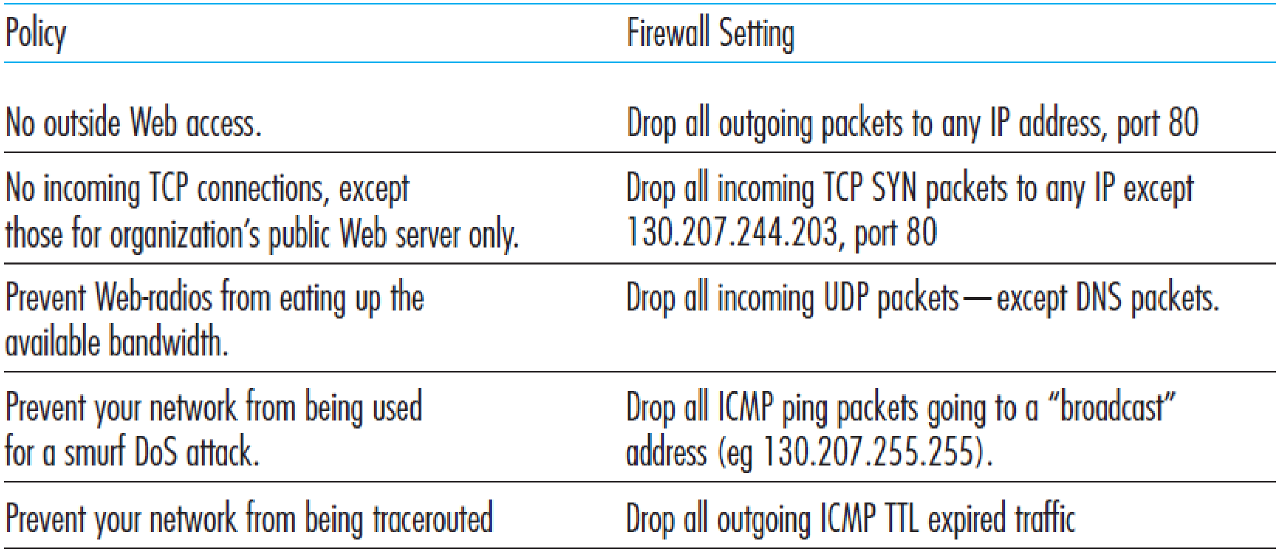
- A packet filter examines each datagram in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-specific rules.

- Filtering decisions are typically based on:
  - IP source or destination address
  - Protocol type in IP datagram field: TCP, UDP, ICMP, OSPF, and so on
  - TCP or UDP source and destination port
  - TCP flag bits: SYN, ACK, and so on
  - ICMP message type
  - Different rules for datagrams leaving and entering the network
  - Different rules for the different router interfaces

Example

- If the organization doesn’t want any incoming TCP connections except those for its public Web server, it can block all incoming TCP SYN segments except TCP SYN segments with destination port 80 and the destination IP address corresponding to the Web server.

- If the organization doesn’t want its internal network to be mapped (tracerouted) by an outsider, it can block all ICMP TTL expired messages leaving the organization’s network.

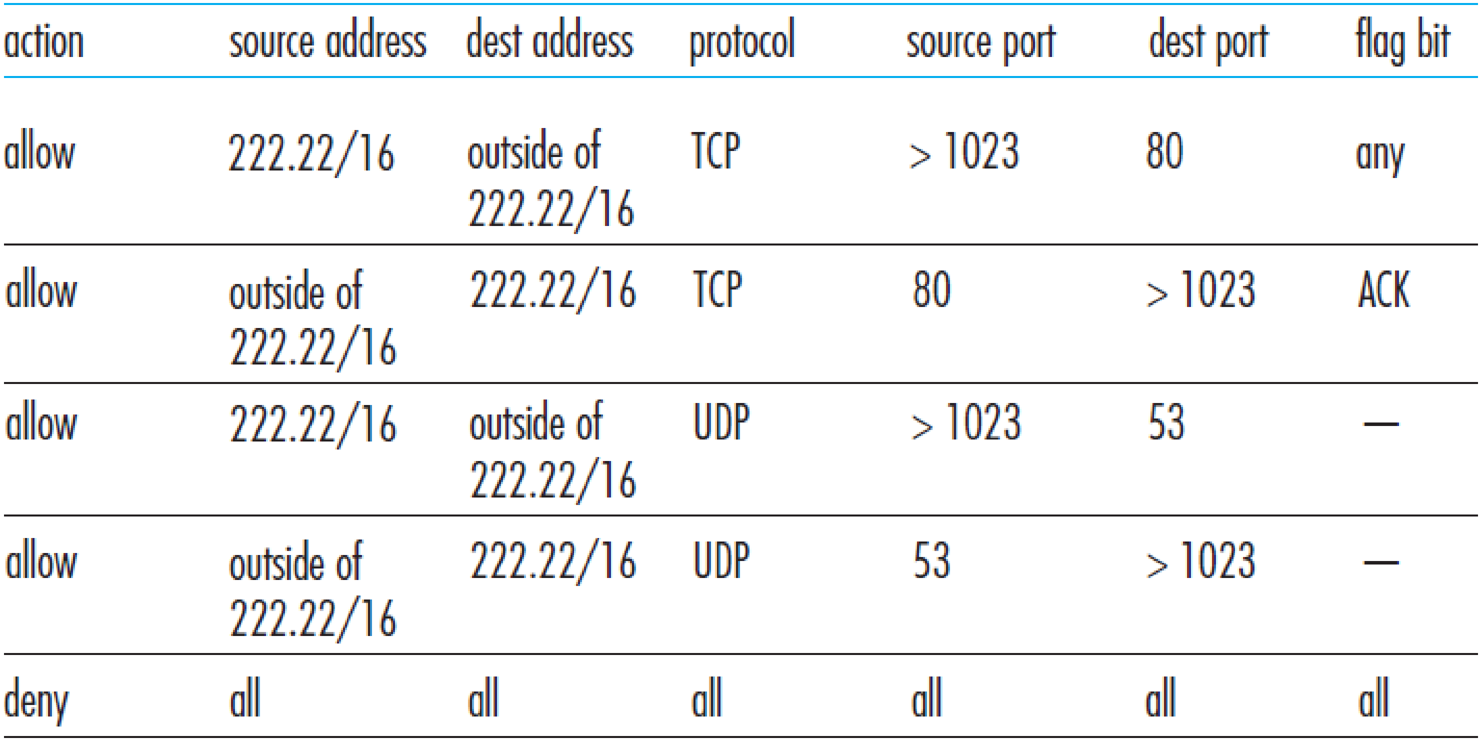


Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization’s public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a “broadcast” address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Table 8.5 ♦ Policies and corresponding filtering rules for an organization’s network 130.27/16 with Web server at 130.207.244.203

Access Control List

- Firewall rules are implemented in routers with access control lists,
- each router interface have its own list.



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

Table 8.6 ♦ An access control list for a router interface

- The first two rules together allow internal users to surf the Web; the second two rules together allow DNS packets to enter and leave the organization’s network

Stateful Packet Filters

- In a traditional packet filter, filtering decisions are made on each packet in isolation.

- Stateful filters actually track TCP connections, and use this knowledge to make filtering decisions.

- Why do we need this?
  - let’s reexamine the ACL
  - any packet arriving from the outside with ACK = 1 and source port 80 is allowed by the filter to pass into the internal network (see 2nd rule)

  - Such packets could be used by attackers in attempts to crash internal systems with malformed packets, carry out denial-of-service attacks, or map the internal network.
  - On the other hand, if the filtering does not allow such packets, then it would prevent the organization’s internal users from surfing the Web.

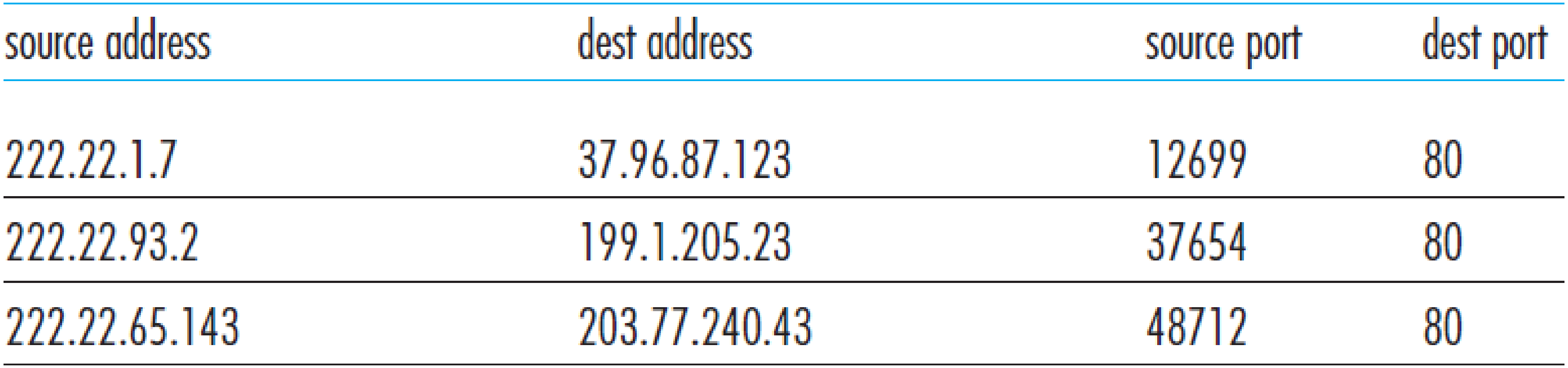
  - So, what to do?

Cont…

- Stateful filters solve this problem by tracking all ongoing TCP connections in a connection table.

- This is possible because the firewall can observe the beginning of a new connection and the end of a connection.

- the stateful filter includes a new column, “check connection,” in its access control list



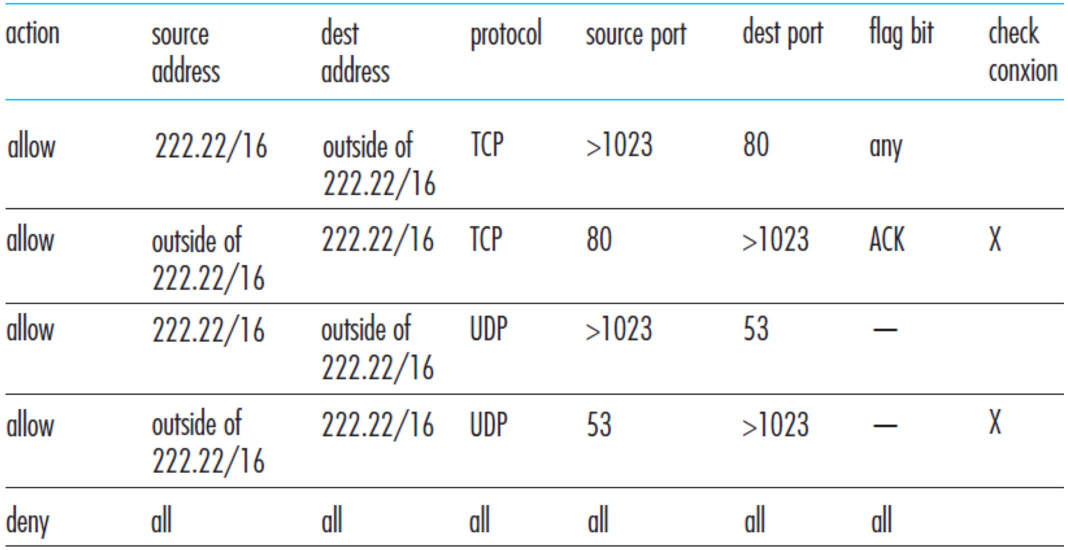
source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Table 8.7 ♦ Connection table for stateful filter

Example

- Suppose an attacker attempts to send a malformed packet into the organization’s network by sending a datagram with TCP source port 80 and with the ACK flag set
- Further suppose that this packet has source port number 12543 and source IP address 150.23.23.155.

- When this packet reaches the firewall, the firewall checks the ACL which indicates that the connection table must also be checked
- the connection table tells that this packet is not part of an ongoing TCP connection



action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
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	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

Table 8.8 ♦ Access control list for stateful filter

Application Gateway

- Packet-level filtering allows an organization to perform coarse-grain filtering on the basis of the contents of IP and TCP/UDP headers

- But what if an organization wants to provide a restricted set of internal users to create a Telnet session to the outside world ?

- Such tasks are beyond the capabilities of traditional and stateful filters.
  - Because, information about the identity of the internal users is application-layer data and is not included in the IP/TCP/UDP headers.

- To have finer-level security, firewalls must combine packet filters with application gateways.

- An **application gateway** is an application-specific server through which all application data (inbound and outbound) must pass.
- Application gateways look beyond the IP/TCP/UDP headers and make policy decisions based on application data.

Cont…

- Such a security policy is: combination of a packet filter (in a router) and a Telnet application gateway
- The router's filter is configured to block all Telnet connections except those that originate from the IP address of the application gateway.

- Note, the Telnet application gateway not only performs user authorization but also acts as a Telnet server and a Telnet client, relaying information between the user and the remote Telnet server.

- Internal networks often have multiple application gateways, for example, gateways for Telnet, HTTP, FTP, and e-mail.

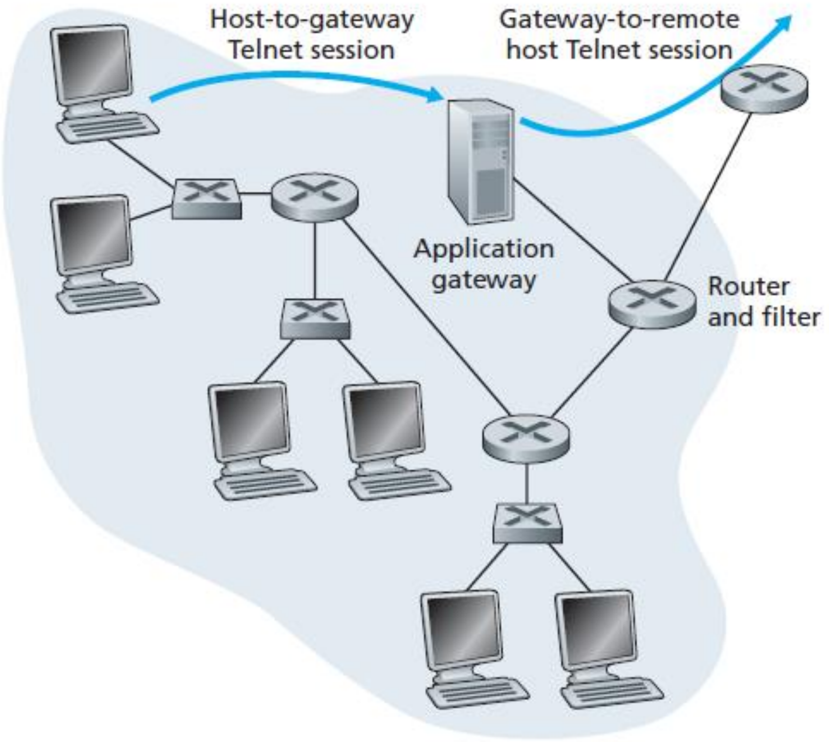


Figure 8.34 ♦ Firewall consisting of an application gateway and a filter

Intrusion Detection Systems

- Why IDS?
  - a packet filter (traditional and stateful) inspects IP, TCP, UDP, and ICMP header fields when deciding which packets to let pass through the firewall
  - an application gateway perform deep packet inspection (DPI) for a specific application only
  - How could we perform DPI for any application?
    - there is a need for yet another device—a device that not only examines the headers of all packets passing through it (like a packet filter), but also performs DPI (unlike a packet filter).

- A device that generates alerts when it observes potentially malicious traffic is called an intrusion detection system (IDS).
- A device that filters out suspicious traffic is called an intrusion prevention system (IPS).

- IDS can detect a wide range of attacks, including
  - network mapping, port scans, TCP stack scans,
  - DoS bandwidth-flooding attacks,
  - worms and viruses, OS vulnerability attacks, and
  - application vulnerability attacks.

Cont…

- An organization may deploy one or more IDS sensors

- they typically work in concert,
- send information about suspicious traffic activity to a central IDS processor,
- which collects and integrates the information
- and sends alarms to network administrators

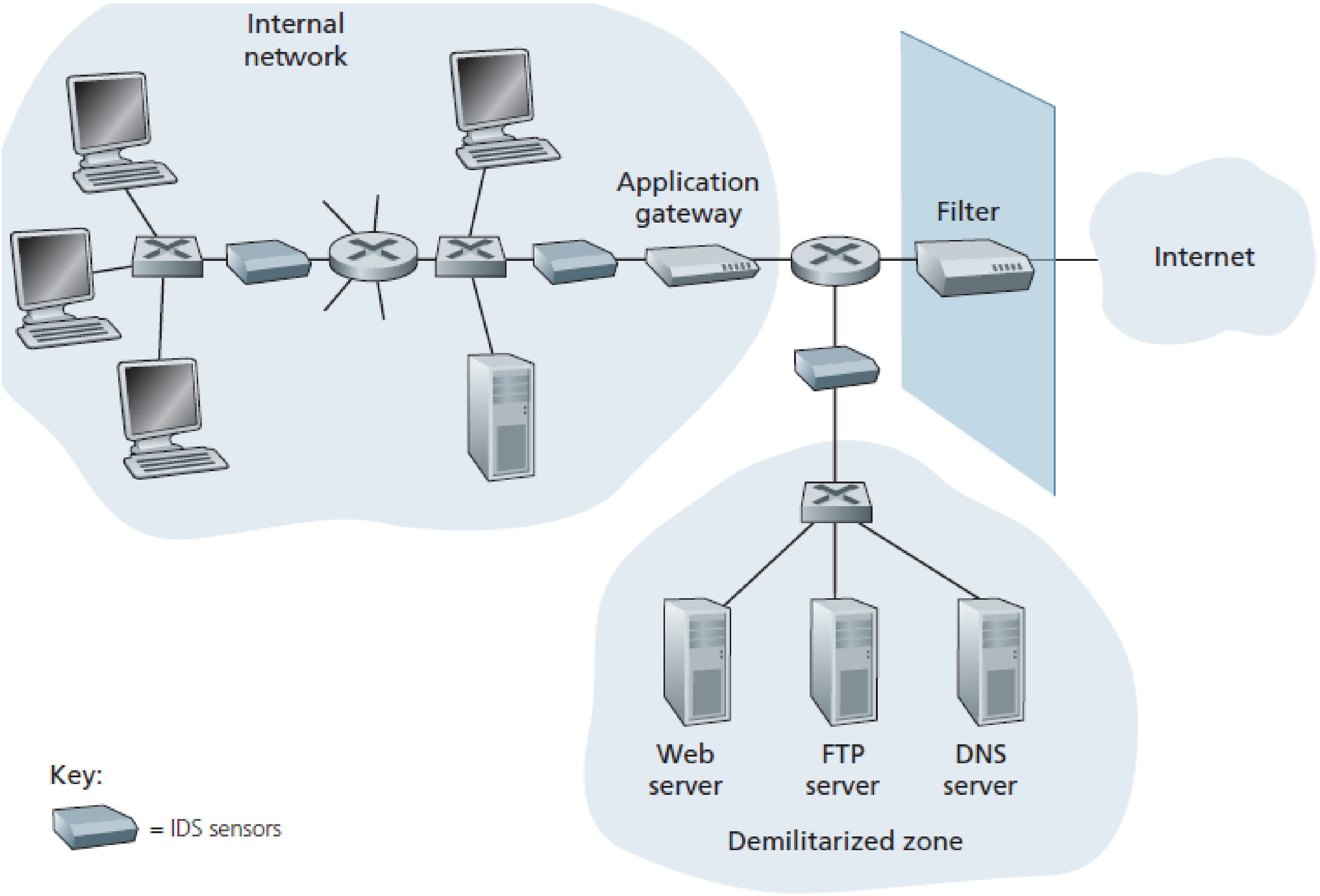


Figure 8.36 ♦ An organization deploying a filter, an application gateway, and IDS sensors

Cont…

- Why multiple IDS sensors?
  - as IDS not only needs to do deep packet inspection, but must also compare each passing packet with tens of thousands of “signatures”; this can be a significant amount of processing.

- IDS systems are broadly classified as
  - signature-based systems
    - maintains an extensive database of attack signatures.
    - A signature may simply be a list of characteristics about a single packet or may relate to a series of packets
    - Operationally, a signature-based IDS sniffs every packet passing by it, comparing each sniffed packet with the signatures in its database.
    - Limitations: (1) they require previous knowledge of the attack to generate an accurate signature. (2) need high computation power to compare with each signature
  - anomaly-based systems
    - creates a traffic profile as it observes
    - looks for packet streams that are statistically unusual (e.g., a sudden exponential growth in port scans and ping sweeps)
    - Advantage: they don’t rely on previous knowledge about existing attacks
    - Limitation: extremely challenging problem to distinguish between normal traffic and statistically unusual traffic.

Thanks!