Firewalls and Intrusion Detection Systems: Part 5

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2012
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt. Ltd., 2018
- C. Kaufman, R. Perlman, M. Speciner, "*Network Security: Private Communication in a Public World*", Pearson Education, 2nd edition, 2002

Intrusion Detection Systems

Motivation

- Recall: a packet filter (traditional or stateful):
  - inspects IP, TCP, UDP and ICMP header fields
  - to decide whether to let a packet pass or block it
- However, to detect several kinds of attacks:
  - we need to perform *deep packet inspection*
  - i.e., look at the application data that packets carry, in addition to header fields
- E.g. of such an attack:
  - packets carrying viruses or worms
- Recall: application gateways perform deep packet inspection
  - however, they only do this for a single application
- Hence, there is a need for another kind of device which:
  - examines the headers of all packets passing through it
  - as well as examines application data contained in them (i.e., performs deep packet inspection)

Intrusion Detection Systems

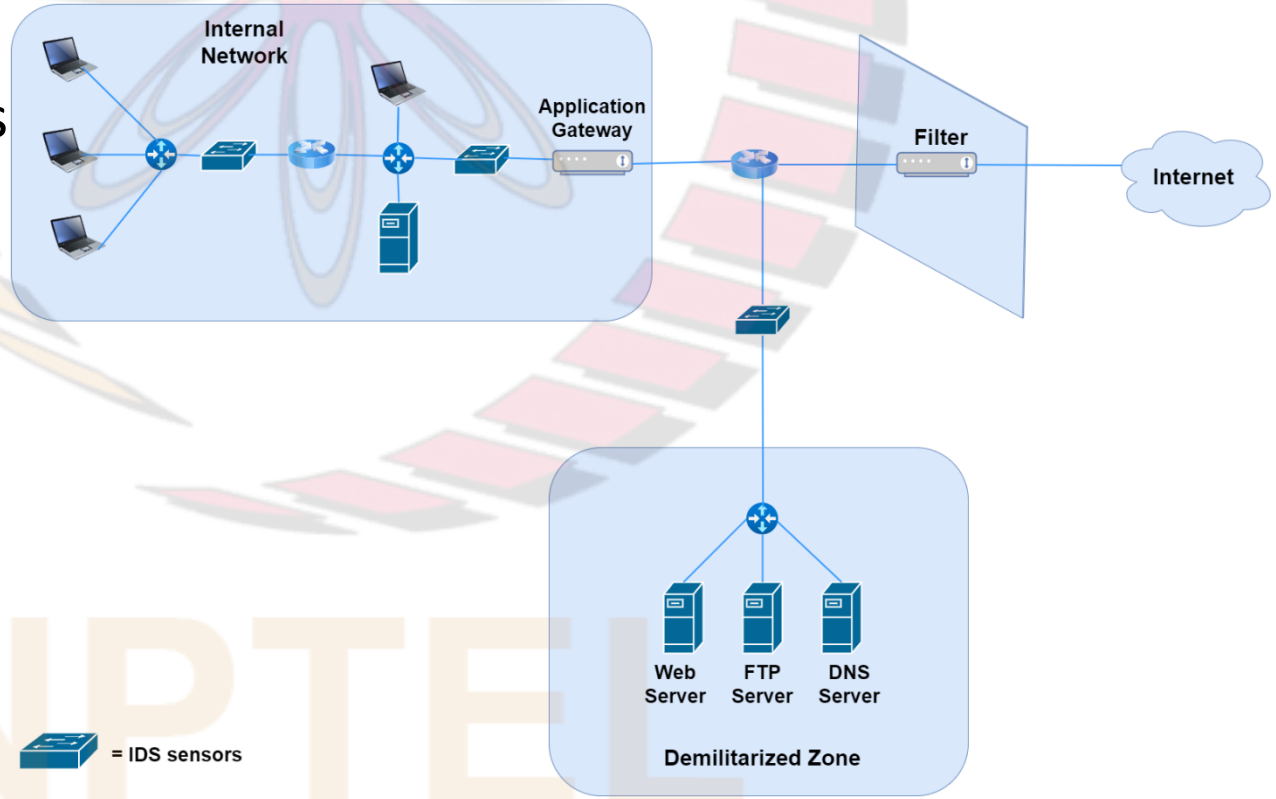
- Recall: there is a need for a device which:
  - examines the headers of all packets passing through it
  - as well as examines application data contained in them (i.e., performs deep packet inspection)
- When such a device observes a suspicious packet or a suspicious series of packets, it:
  - either prevents the packets from passing through it
  - or lets the packets pass, but sends alerts to a network administrator
    - network administrator later examines logs of those packets and takes appropriate actions
- A device that:
  - generates alerts when it observes potentially malicious traffic is called an *Intrusion Detection System* (IDS)
  - filters out suspicious traffic is called an *Intrusion Prevention System* (IPS)
- We now study both IDS and IPS together since the challenging part is to *detect* suspicious traffic
  - once this is done, sending alerts or dropping packets is straightforward
- We collectively refer to both IDS and IPS as IDS

Example Attacks That can be Detected Using IDS

- Network scanning
  - ❑ discovery of hosts, services and vulnerabilities on a computer network by sending probe packets into the network and analyzing the responses
  - ❑ can be performed using software such as “nmap”
  - ❑ E.g. of network scanning:
    1) Host Discovery:
       - identifying hosts on a network
       - e.g., listing the hosts that respond to TCP and/ or ICMP requests
    2) Port Scanning:
       - listing the open ports on target hosts
    3) Operating System (OS) and Hardware Detection:
       - determining the operating system and hardware deployed in hosts
    4) Network Vulnerability Scanning
       - e.g., the Security Administrator’s Integrated Network Tool (SAINT) is a computer software that detects the TCP and UDP services running on every host of a network
       - for each service that it finds running, it sends a series of probe packets designed to detect weaknesses that could allow an attacker to gain unauthorized access, launch a DoS attack or gain confidential information
- OS vulnerability attacks
- Application vulnerability attacks
- Injection of malware (e.g., worms, viruses) into hosts of the network
- Application-layer DoS or DDoS Attacks
  - ❑ e.g., attacker sends a large number of requests to log into an online account such as a Gmail account
  - ❑ lot of server resources consumed in the process of loading the relevant user data from a database, checking login credentials and sending a response containing the requested webpage

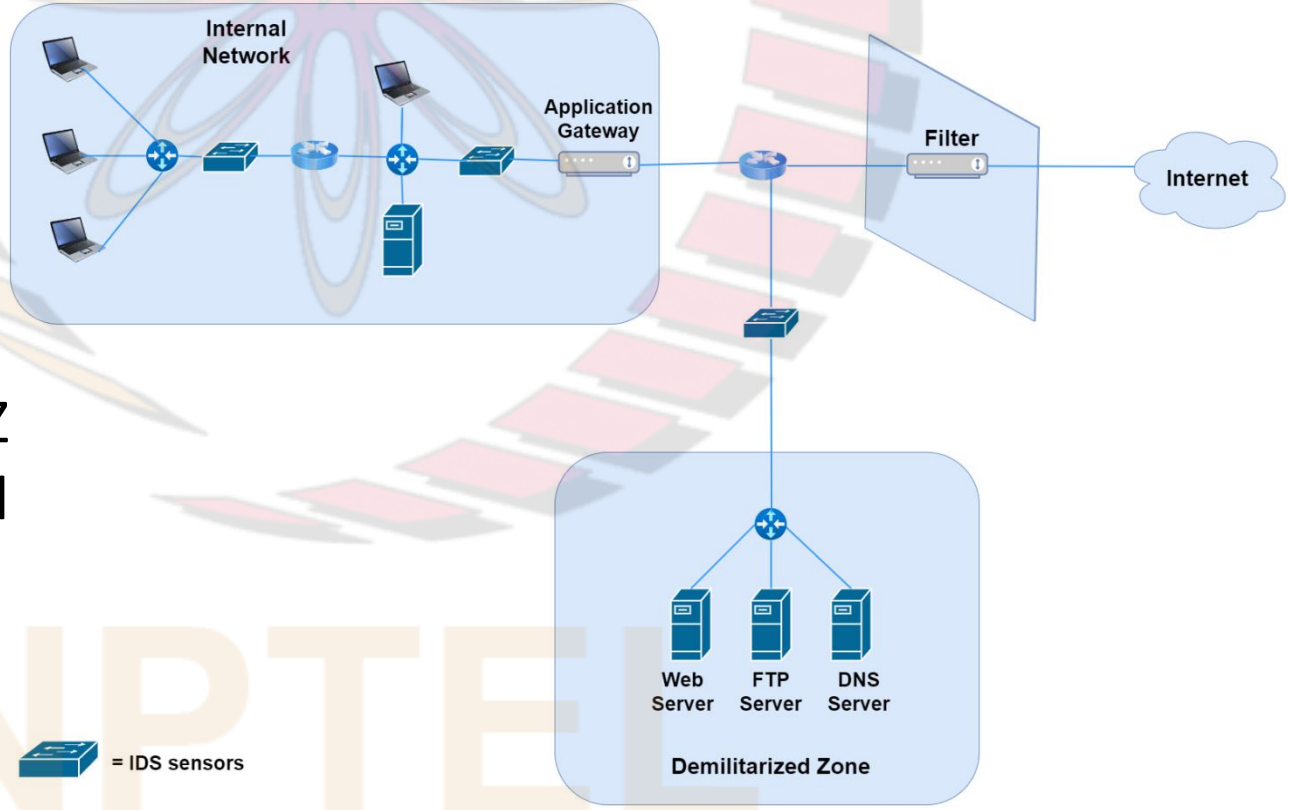
Example Network Architecture

- An organization may deploy one or more IDS sensors in its organization's network
- Fig. shows an organization that has three IDS sensors
- When multiple sensors are deployed:
  - each sends information about suspicious traffic activity to a central IDS processor
  - central IDS processor collects and analyzes the information and sends alarms to network administrator when considered appropriate



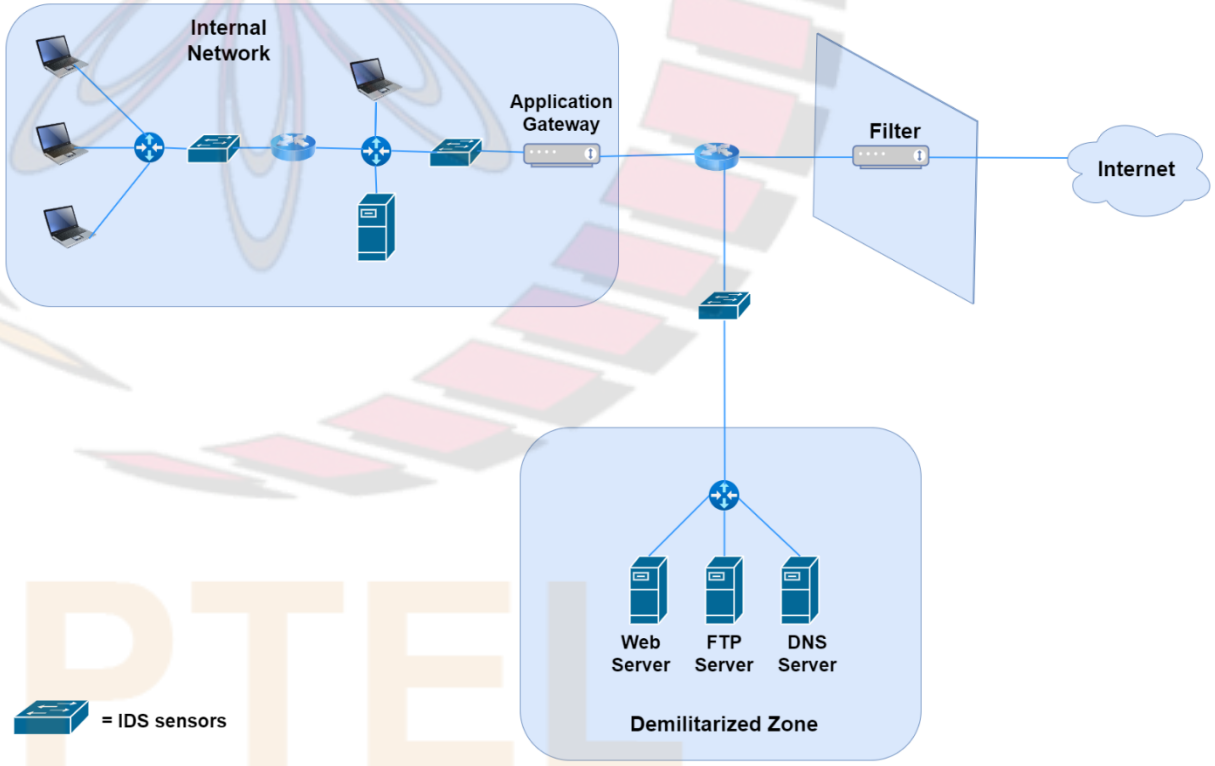
Example Network Architecture (contd.)

- In fig., organization's network is partitioned into two regions:
  - a high-security region protected by a packet filter, an application gateway and monitored by two IDS sensors
  - a low-security region (called "*demilitarized zone*" (DMZ)), protected by packet filter and monitored by one IDS sensor
- DMZ contains the organization's servers that need to communicate with external users
- A node in external network can only access nodes in DMZ
  - firewall blocks all access to high-security region



Demilitarized Zone (DMZ)

- A DMZ contains and exposes an organization's external facing services (e.g., Web server) to the public Internet
- Isolated from the rest of the internal network using IDSs
- Reason:
  - since machines in the DMZ are accessible to the public, they are the most likely machines to be compromised in the entire network
  - IDSs can protect machines in rest of internal network from being compromised if a machine in DMZ is compromised



Need for Multiple IDS Sensors

- Recall: in example organization's network, there are three IDS sensors
- Why not use only one IDS sensor, which could be placed just behind the packet filter or combined with it?
- Reason:
  - ❑ often an IDS needs to compare each passing packet with tens of thousands of "signatures"
  - ❑ this requires significant amount of processing, especially if the organization's network receives large amount of traffic from Internet
  - ❑ by placing the IDS sensors further downstream, each sensor only sees a fraction of the organization's traffic and can more easily keep up