Firewalls and Intrusion Detection Systems: Part 1

Gaurav S. Kasbekar

Dept. of Electrical Engineering

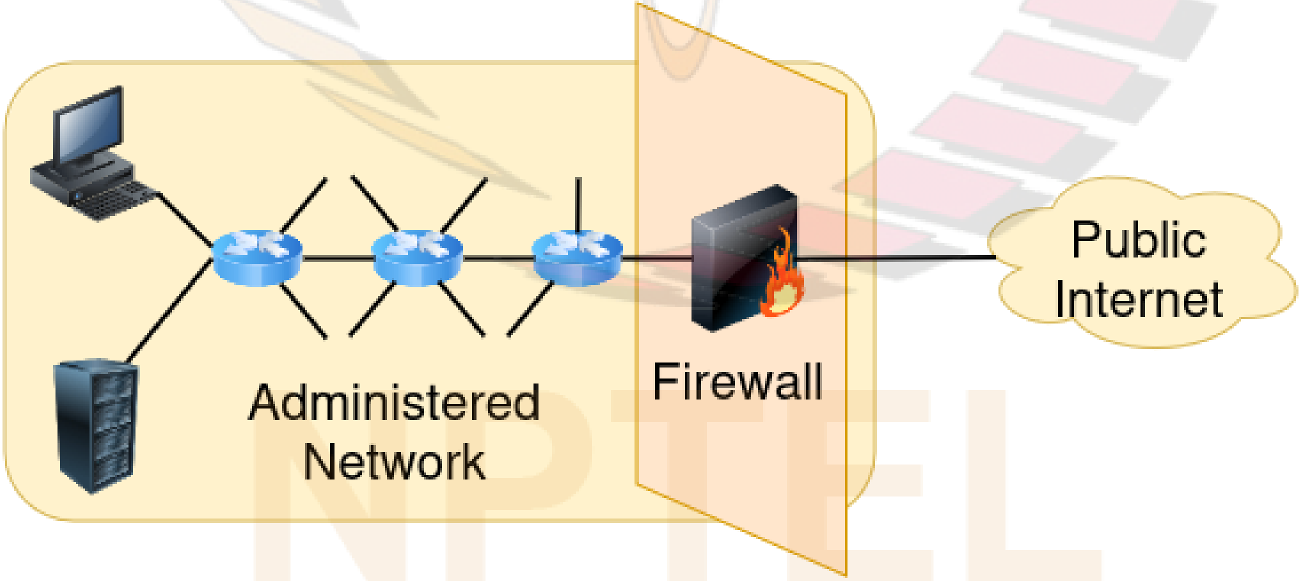
IIT Bombay

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

Introduction

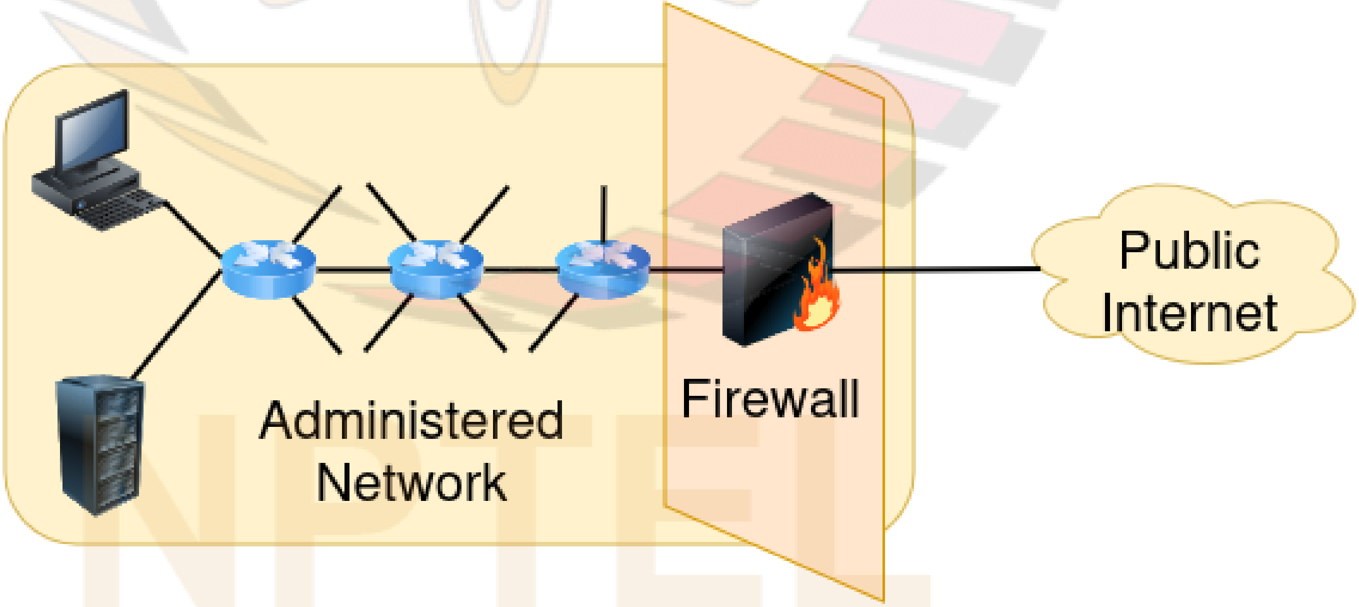
- Most organizations (e.g., universities, companies) have networks connected to the public Internet
- Attackers may attempt to:
  - ❑ infect machines with malware
  - ❑ obtain corporate secrets
  - ❑ map the internal network configurations
  - ❑ launch Denial of Service attacks, etc.
- We will discuss *firewalls* and *intrusion detection systems*, which can be used to detect and/ or prevent such attacks



Firewalls

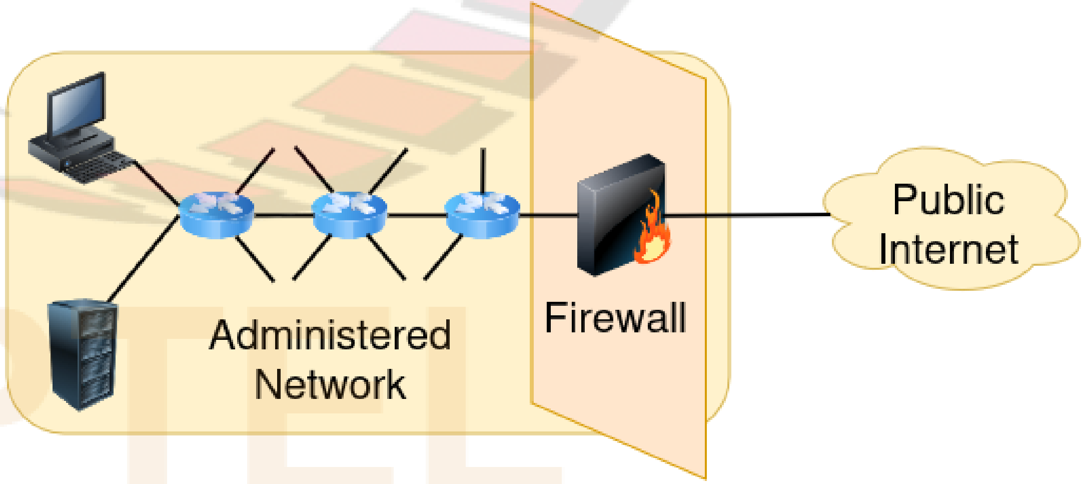
Firewall

- A firewall is a combination of hardware and software that controls access between an organization's internal network and the Internet
- Allows some packets to pass and blocks others, based on a given security policy
- Prevents intruders from attacking internal network
- Also prevents confidential internal data from getting out



Properties of a Firewall

- All traffic from outside to inside and vice versa passes through the firewall
- Only authorized traffic, as defined by the security policy configured by network administrator, allowed to pass
  - ❑ other traffic blocked
- Firewall itself is designed and maintained in such a way that it is hard to compromise, e.g.:
  - ❑ unnecessary services on the machine removed and newly available security patches installed expeditiously
- A firewall may be implemented:
  - ❑ in hardware as a stand-alone device
  - ❑ or in software on a PC
- Also, many routers support basic firewall functionality



Internet Control Message Protocol (ICMP)

- ICMP is a protocol used by hosts and routers to communicate network-layer information to each other
- A typical use of ICMP is for error reporting
    - e.g., while forwarding a packet, if an IP router is unable to find a path to the destination address, then it sends an ICMP packet to source indicating the error
    - may result in display of “Destination host unreachable” or “Destination network unreachable” message to end user
- ICMP packets have the “Protocol” field in the IP header equal to 1
    - note: this field equals “6” for TCP packets and “17” for UDP packets
- Examples of ICMP packets:
    - a “*redirect*” packet, which tells source host to use a particular router for forwarding to a particular destination, presumably because the router the source chose on a previous packet was not the best path to the destination
    - a “*ping*” packet, which is supposed to be echoed back by the system that receives it
        - useful for seeing if a system is alive and reachable

Examples of Attacks Using ICMP Messages

- ICMP ping can be exploited by attacker to:
  - ❑find machines to break into
- Sending an ICMP message to an internal host, say Alice, falsely claiming that some range of addresses is unreachable will cause:
  - ❑Alice to end its connections to machines in the range specified by that ICMP message
- ICMP redirects can be used to cause a host to:
  - ❑send traffic in a different direction, possibly towards a compromised machine
  - ❑allowing man-in-the-middle attacks to take place

Traceroute

- A program that can be used to trace a route from a host to any other host in the world
  - ❑ provides IP addresses of all the routers on path
- Implemented using ICMP messages
- Sends a series of ordinary UDP packets to the destination
  - ❑ each packet contains an unlikely UDP port number
- The first of these UDP packets has a TTL of 1, the second of 2, the third of 3, and so on
- When the n’th packet arrives at the n’th router:
  - ❑ the n’th router observes that the TTL has just expired
  - ❑ according to the rules of the IP protocol, the router discards the packet and sends an ICMP message to the source
  - ❑ this message includes the IP address of the router
- When this ICMP message arrives at the source host, it obtains the IP address of the n’th router on the path to the destination host
- This process continues until one of the UDP packets sent by source host reaches the destination host
- However, the traceroute program can be used by an attacker to attack an organization’s network as follows:
  - ❑ it can map the internal configuration of the organization’s network
  - ❑ It can use the configuration obtained to later attack the organization’s network