Firewalls and Intrusion Detection Systems: Part 3

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

Types of Firewalls

1) Traditional Packet Filters
2) Stateful Packet Filters
3) Application Gateways

Traditional Packet Filters

- Examines *each packet in isolation* and determines whether the packet should be allowed to pass or should be dropped
  - based on rules configured by network administrator
- Filtering decisions typically based on:
  - IP source and/ or destination address
  - Protocol type in IP header: 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
- Often, different rules are used for:
  - packets entering and leaving the network
  - the different router interfaces

Examples

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	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent audio-video traffic from eating up the available bandwidth	Drop all UDP packets, except DNS packets
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Examples (contd.)

- Suppose we want to permit internal hosts to initiate or accept Telnet connections to/ from only external hosts from a pre-specified list
- How can we configure this policy?
  - Packet filter forwards only those Telnet packets (those with a port number of 23) initiated by or to the external hosts from the list
- Note that this filtering policy is based on a combination of IP addresses and port numbers

Examples (contd.)

- Suppose an organization:
  - wants to allow its internal hosts to initiate TCP connections to external hosts
  - but wants to prevent external hosts from initiating TCP connections to internal hosts
- How can we configure this policy?
  - We can use the fact that the first packet in every TCP connection has the ACK bit set to 0, but all the other packets have the ACK bit set to 1
  - Hence, the packet filter can drop all incoming TCP packets with the ACK bit set to 0

Examples (contd.)

- Consider an organization whose hosts have IP addresses of the form 222.22/16
- What types of traffic are allowed and blocked by the access control list in the figure?
- Note that first rule from top to bottom that matches is applied

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

Examples (contd.)

- The first two rules together allow internal users to surf the Web
  - ❑ but external sources are not allowed to establish a TCP connection with a Web server inside the organization
- The third and fourth rules together allow DNS packets to enter and leave the organization's network
- In summary, this access control list blocks all traffic except Web traffic initiated from within the organization and DNS traffic

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