Firewalls and Intrusion Detection Systems: Part 4

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

Recall: Example Access Control List

- Consider an organization whose hosts have IP addresses of the form 222.22/16
- 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

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

Stateful Packet Filters

- Recall: in a traditional packet filter, filtering decisions are made on each packet in isolation
- Stateful packet filters:
  - track TCP connections
  - use this knowledge to make filtering decisions
- Recall the access control list on previous slide:
  - it allows any packet arriving from the outside with ACK bit set to 1 and source port 80 to pass through the filter
- This fact can be used by an attacker:
  - by sending malformed packets to internal systems, which may crash when they see unexpected header values
- One solution:
  - Modify the access control list so that it now blocks incoming packets with ACK bit set to 1 and source port 80
- Shortcoming:
  - This will prevent the organization's internal users from surfing the Web

Stateful Packet Filters (contd.)

- Stateful packet filters solve the above problem by tracking all ongoing TCP connections in a connection table
- Possible because firewall can observe:
  - the beginning of a new connection by observing a three-way handshake (SYN, SYNACK and ACK)
  - the end of a connection when it sees a FIN packet for the connection
- An example connection table of a firewall is shown in fig. below
  - indicates that there are three ongoing TCP connections, all Web connections initiated from within the organization

Source Address	Destination Address	Source Port	Destination 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

Stateful Packet Filters (contd.)

- Also, the stateful filter includes a new column, “check connection”, in its access control list as shown in fig. below
  - ❑indicates that the connection should be checked for two of the rules
- We study some examples to see how the connection table and the extended access control list can be used together

Action	Source Address	Destination Address	Protocol	Source Port	Destination Port	Flag Bit	Check Connection
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	

Example 1

- Suppose an attacker attempts to send a malformed packet into the organization's network by sending a packet with:
  - ❑TCP source port 80 and with the ACK bit set
  - ❑destination port 12543 and source IP address 150.23.23.155
- When this packet reaches the firewall, the latter checks the above access control list, which indicates that the connection table must be checked
- The firewall checks the connection table, sees that this packet is not part of an ongoing TCP connection, and drops the packet

Source Address	Destination Address	Source Port	Destination 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

Example 2

- Suppose an internal user wants to surf an external website
- First, the user's host sends a TCP SYN packet to the Web server
- Hence, this TCP connection gets recorded in the connection table
- When the Web server subsequently sends packets to the user's host (with the ACK bit set), the firewall :
  - ❑checks the table and sees that a corresponding connection is in progress
  - ❑lets these packets pass, thereby not interfering with the internal user's surfing activity

Handling UDP Traffic

- Recall: easy to maintain a connection table for TCP connections since connection:
  - ❑ starts when three-way handshake takes place and
  - ❑ ends when FIN packets sent
- However, UDP traffic not connection-based
  - ❑ so above approach cannot be used
- To handle UDP traffic, a stateful packet filter tracks state using:
  - ❑ only source and destination addresses and source and destination port numbers
- E.g.: recall the rows corresponding to DNS traffic in extended access control list discussed earlier (see fig.)

Action	Source Address	Destination Address	Protocol	Source Port	Destination Port	Flag Bit	Check Connection
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	

Application Gateway

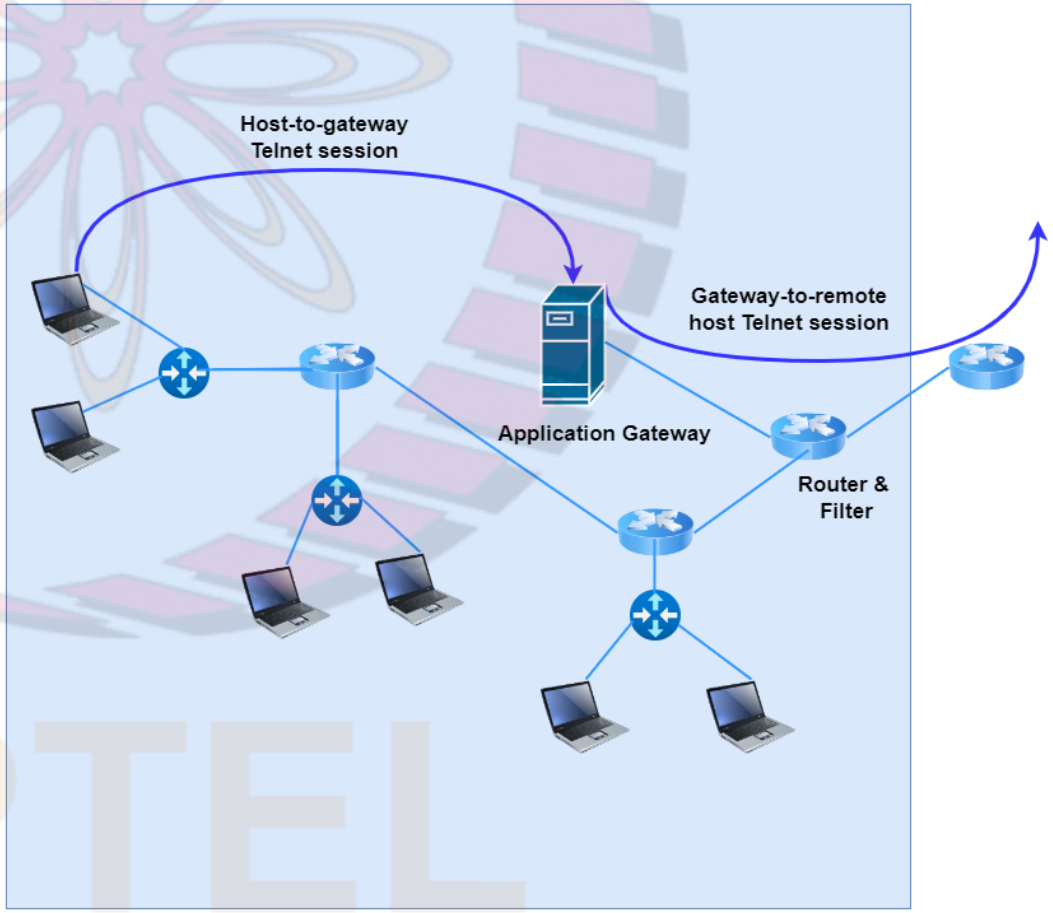
- Recall that traditional packet filters and stateful packet filters perform filtering on the basis of:
  - the contents of IP, TCP/UDP and ICMP headers
- Suppose an organization wants to implement the following policies:
  - It wants to allow Telnet to external hosts to a restricted set of internal *users* (as opposed to *IP addresses*)
  - Wants such privileged users to authenticate themselves first before being allowed to create Telnet sessions to external hosts
- How can above policies be implemented using packet filters?
  - cannot be implemented using packet filters since information about identities of users is application-layer data and is not included in the IP/TCP/UDP/ICMP headers
- To implement above policies, application gateways are needed
- Application gateways make policy decisions based on application data

Application Gateway (contd.)

- Application gateway:
  - is an application-specific server
  - through which all application data (inbound and outbound) must pass
- Multiple application gateways (corresponding to different applications) can run on the same host
  - but each gateway is a separate server with its own process

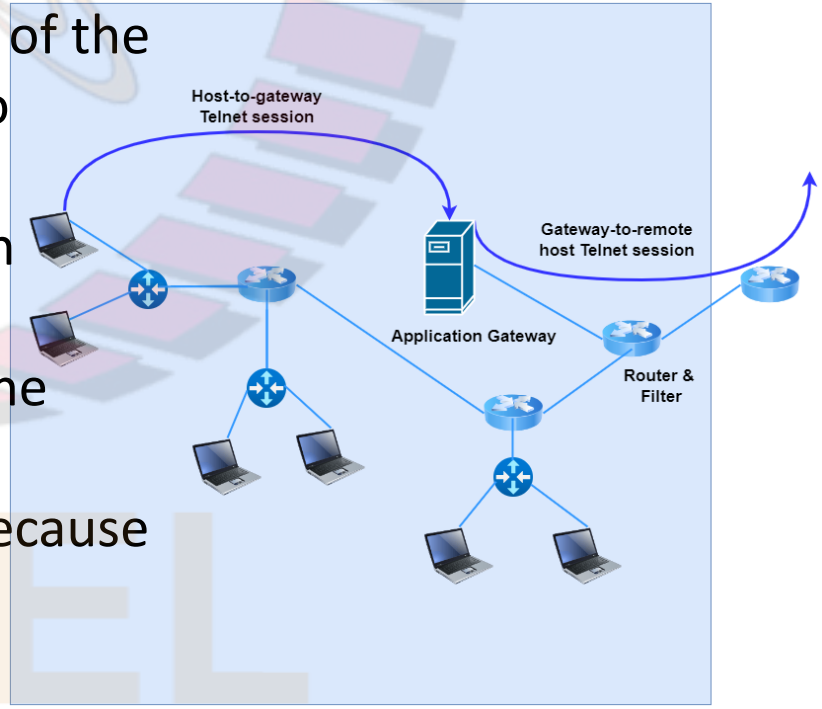
Example

- Suppose we want to design a firewall that:
  - ❑ allows only a restricted set of internal users to Telnet to external hosts
  - ❑ prevents all external clients from Telneting to an internal host
- This policy can be implemented using (see fig.) a 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
  - ❑ hence, inbound Telnet connections are blocked



Example (contd.)

- Consider an internal user who wants to Telnet to an external host
- The user must first set up a Telnet connection with the application gateway
- The application gateway prompts user for username and password:
  - when this information is supplied, gateway checks to see if the user has permission to Telnet to an external host
  - if not, then the Telnet connection from the internal user to the application gateway is terminated by the gateway
- If the user has permission, then gateway:
  1) prompts the user for the host name of the external host to which user wants to connect
  2) sets up a Telnet connection between gateway and external host
  3) subsequently relays data between the external host and user
- Note that packet filter permits step 2 because *gateway* initiates Telnet connection to external host



Application Gateway (contd.)

- Networks of organizations often have multiple application gateways, e.g., gateways for:
  - Telnet
  - HTTP
  - FTP
- The HTTP gateway often:
  - includes a Web cache
    - recently visited Webpages are cached so that they do not have to be repeatedly fetched from external websites
  - scans incoming webpages for virus signatures and objectionable content
- Disadvantages of application gateways:
  - A different application gateway is needed for each application
  - A performance penalty needs to be paid, since all data is relayed via the gateway
    - becomes a concern, especially when a large number of users or applications use the same gateway machine