Firewall Security

Chapter 8

Lecturer: Pei-yih Ting

Overview

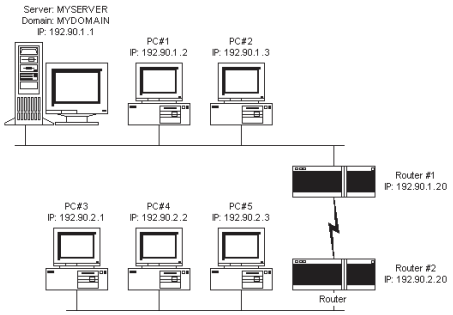
- Perimeter Security Devices
- H/W vs. S/W
- Packet Filtering vs. Stateful Inspection
- Firewall Topologies
- Firewall Rulebases

Perimeter Security Devices

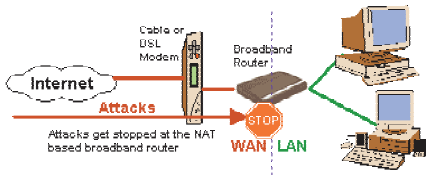
- Network devices that form the core of perimeter security include
  - Routers
  - Proxy servers
  - Firewalls
- A perimeter defense must be manageable
  - Balance financial, manpower, and other resources against the degree of security required

Routers

- Routers are used to interconnect networks
  - Usually bridge different physical networks
  - Route traffic from a source to a destination
  - Often the first device encountered as a packet enters a network from the Internet

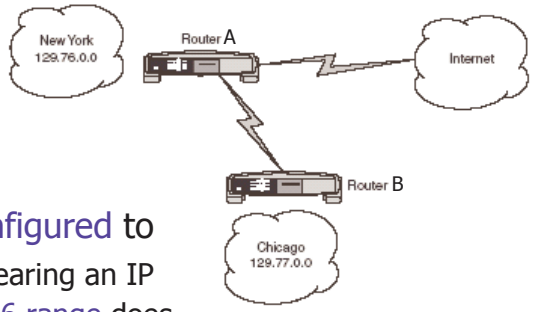


Routers (cont'd)



- Routers may implement some security functionalities
  - Packet filtering through the use of access control lists
  - Reducing load on other devices (ex. firewall, can protect from DOS attacks)
  - Screening traffic with suspicious IP addresses to protect against spoofing
  - Egress filtering: ensure traffic leaving your network bears a valid IP address, prevent hackers from launching spoofing attacks using your network

Routers: Spoofing Protection



- Router A can be configured to
  - Ensure that traffic bearing an IP address in the 129.76 range does not enter the protected New York network from either the Internet or the Chicago network
  - Reject any packets coming from the Internet connection with a source address in the 129.77 range

Proxies

- A proxy is an entity with the authorization to act on behalf of another
- Proxy servers sit between a client and an untrusted system in the Internet
  - Prevents the untrusted system from having any direct access to the client that would support malicious actions
    - Masks the client's identity
    - Limits network sniffing
  - Client requests are directed to the proxy
  - Proxy either responds from its cache or makes a request to the Web server on behalf of the client and then responds to the client
    - Limit type of the content (filtering)
    - Screen incoming data for malicious content

Proxies (cont'd)

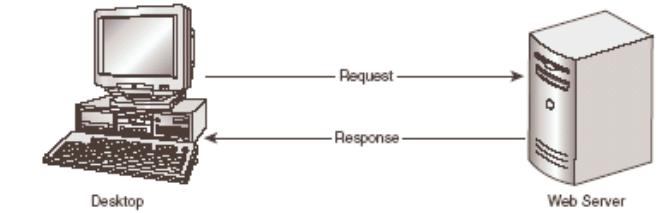


Figure 8.2
Normal client/server interaction

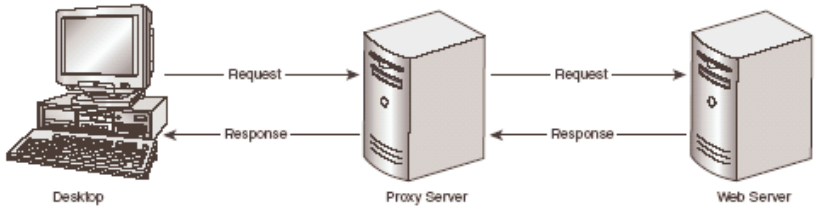


Figure 8.3
Client/server interaction using a proxy server

Firewalls

- Improve network security
- Cannot completely eliminate threats and attacks
- Responsible for screening traffic entering and/or leaving a computer network
- Each packet that passes is screened following a set of rules stored in the firewall rulebase
- Several types of firewalls
- Several common topologies for arranging firewalls

Types of Firewalls

- A diverse range of firewall solutions are available on the market today
  - Both hardware and software solutions
- Hardware-based firewalls (appliances)
  - Integrated solutions are standalone devices that contain all hardware and software required to implement the firewall
  - Similar to software firewalls in user interfaces, logging/audit, and remote configuration capabilities
  - More expensive than software firewalls
  - Faster processing possible for high-bandwidth environments

Types of Firewalls (cont'd)

- Software firewalls
  - Relatively inexpensive
  - Purchasing a license agreement will include media required to install and configure the firewall
  - Most firewalls are available for Windows, Unix, and Linux
  - Can also purchase design of the firewall rulebase with configuration, maintenance and support
    - Worthwhile unless you really understand what is needed, a mistake can negate the usefulness of the firewall

Packet Filtering

- An early basic technology for screening packets passing through a network
- Each packet is screened independently
- Firewall reads and analyzes the packet headers
- Offers considerable flexibility in what can be screened
  - Common fields: Source address, Destination address, Destination port, and Transport protocol
  - Can be used for performance enhancement by screening non-critical traffic by day or time for example

Stateful Inspection

- A next-generation firewall technology
- Overcomes the limitation of packet filtering that treats packets in isolation
- Treats packets as pieces of a connection
  - Maintains data about legitimate open connections that packets belong to
  - Keeps identity of ports being used for a connection
  - Traffic is allowed to pass until connection is closed or times out
  - Example: a typical Web page retrieving scenario

    client 1423 → server 80
    client 1423 ← server 2901
    client 1423 ↔ server 2901

Firewall Topologies

- Firewalls should be placed between the protected network (or subnet) and potential entry points
- Access points can include dial-up modems, wireless accesses, and broadband lines
- Three common firewall topologies
  - Bastion host (dual-home firewall)
  - Screened subnet
  - Dual firewalls
- Firewall installations can include combinations of these topologies for layered protection

Bastion Host

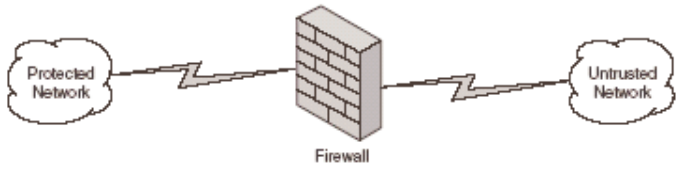


Figure 8.4
Bastion host

- Firewall is the sole link between the protected network and the untrusted network
- Firewall has two network interface cards
  - One to protected network
  - One to untrusted network
- Relatively inexpensive and easy to implement

Bastion Host (cont'd)

- If services are offered to clients outside of the protected network, there is a significant security risk
  - Port 80 has to stay open
  - Hackers can potentially compromise the Web server through this port and get access to full protected network (There is no protection between the Web server machine and other machines in the protected network.)

Screened Subnet

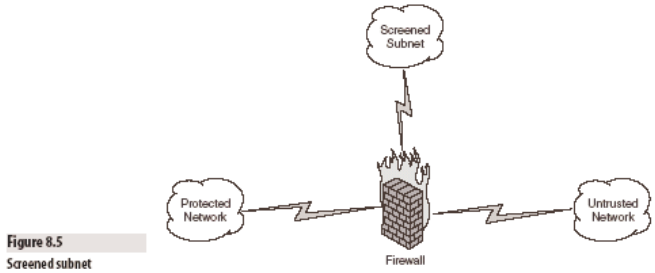


Figure 8.5
Screened subnet

- Also called demilitarized zone (DMZ)
- Single firewall, three network interface cards
  - One to protected network
  - One to screened subnet
  - One to untrusted network (the Internet)

Screened Subnet (cont'd)

- Screened subnet contains systems that provide services to external users (Web or SMTP servers etc.)
- If any machine in the DMZ is compromised, the whole DMZ might be attacked, but access is still kept out of the protected network

Dual Firewalls

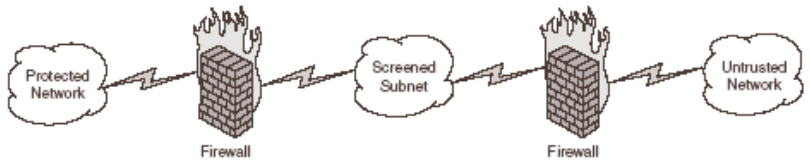


Figure 8.6
Dual firewalls

- Uses two firewalls, each with two network cards
  - One firewall connects to the untrusted network and the screened subnet
  - The other firewall connects to the screened subnet and the protected network

Dual Firewalls (cont'd)

- The screened subnet again provides a buffer between the networks
- Major advantage: minimize the possibility that a malicious individual could compromise the firewall itself
- For more security, use two different firewalls (H/W vs. S/W, vendors, different security certification levels)
  - Unlikely to have the same security vulnerabilities (apply patch as soon as possible)

Firewall Rulebases

- Rulebase is used to provide the definition of what traffic is allowable and what is not
- Firewall administrators spend most of their time on the rulebase
- Most firewalls have good user interfaces (GUI, remote configurable) to support rule definition
- General rule syntax is

  <action><protocol> from
  <source_address><source_port> to
  <destination_address><destination_port>
- Most firewalls have advanced functionality to supplement the basic fields above

Firewall Rules

- <action> may be either deny or allow
- <protocol> may be tcp, udp or icmp
- <source_address> and <destination_address> may be an IP address, an IP address range, or the keyword "any"
- <source_port> and <destination_port> may be a port number or the keyword "any"

- Advanced <action> could be drop inbound traffic. Dropped traffic is simply ignored, whereas the originator is notified when traffic is blocked
- Could integrate authentication to apply different security restrictions to different classes of users

Special Rules

- These are basic rules that should be included in all firewall installations
- Cleanup Rule Ex. deny any from any any to any any
  - "Deny everything that is not explicitly allowed."
  - Last rule in any firewall rulebase
  - Many firewalls include this rule implicitly in the installation
- Stealth Rule Ex. deny any from any any to firewall any
  - Prevents anyone from directly connecting to the firewall over the network (to protect from attacks)
  - First rule in the firewall rulebase (unless limited connections are explicitly allowed by previous rules)

Summary

- Perimeter security involves a combination of network devices including routers, proxy servers, and firewalls
- Routers are used for routing traffic
  - May have some security functionality
- Proxy servers sit between a protected client and an untrusted network, masking potentially dangerous interactions
- Firewalls screen traffic entering and leaving a network on a packet-by-packet basis

Summary (cont'd)

- Firewalls can be purchased as software or as integrated hardware packages
- There are two primary types of firewall filtering
  - Packet filtering examines each packet in isolation
  - Stateful inspection examines each packet within the context of a specific open connection
- There are three primary firewall topologies
  - Bastion host uses a single firewall with two interface cards
  - Screened subnet uses a single firewall with three interface cards
  - Dual firewalls uses two firewalls, each with two interface cards

Summary (cont'd)

- Firewalls rely on rulebases to configure the specific screening that will be done on packets
- Specific rules should be based on the business requirements for the particular organization
- There are two special rules that should be implemented by every firewall
  - Cleanup rule
  - Stealth rule

Assignments

- Reading: Chapter 8
- Practice 8.7 Challenge Questions
- Turn in Challenge Exercise 8.2 next week