Firewalls

ITS335: IT Security

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 2 January 2015
its335y14s2l07, Steve/Courses/2014/s2/its335/lectures/firewalls.tex, r3503

Contents

Firewall Characteristics

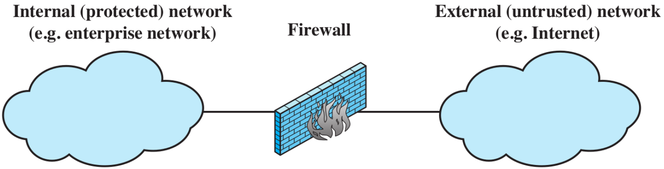
Types of Firewalls

Firewall Locations

Summary

The Need for Firewalls

- Internet connectivity is essential for organisations
    - However it creates a threat
- Firewalls are effective means of protecting LANs
    - Protection at single point, rather on every computer within LAN
- Inserted between the premises network and the Internet to establish a controlled link
- Used as a perimeter defense
    - Single choke point to impose security and auditing
    - Insulates the internal systems from external networks


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

Credit: Figure 9.1(a) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Firewall Characteristics

Design Goals

- All traffic from inside to outside must pass through the firewall
- Only authorised traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration

General Techniques

- Service control, e.g. filter based on IP address, port number
- Direction control, e.g. to internal LAN, to external Internet
- User control, e.g. student vs faculty
- Behaviour control, e.g. filter email with spam

Capabilities and Limitations

Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as platform for VPN end point

Limitations

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organisation
- Laptop, phone, or USB drive may be infected outside the corporate network then used internally

Contents

Firewall Characteristics

Types of Firewalls

Firewall Locations

Summary

Types of Firewalls

Packet Filtering accepts/rejects packets based on protocol headers

Stateful Packet Inspection adds state information on what happened previously to packet filtering firewall

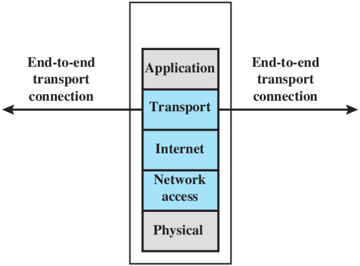
Application Proxy relay for application traffic

Circuit-level Proxy relay for transport connections

- Normally a firewall is implemented on a router
- That router may perform other (non-)security functions, e.g. VPN end-point, accounting, address and port translation (NAT)

Packet Filtering Firewall

- Security policy implemented by set of rules
- Rules define which packets can pass through the firewall
- Firewalls inspects each arriving packet (in all directions), compares against rule set, and takes action based on matching rule
- Default policies: action for packets for which no rule matches
  - Accept (allow, forward)
  - Drop (reject, discard) - recommended


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

Credit: Figure 9.1(b) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Packet Filtering Rules

Packet Information

- IP address: identifies host or network
- Port number: identifies server, e.g. web (80), email (25)
- Protocol number: identifies transport protocol, e.g. TCP or UDP
- Firewall interface: identifies immediate source/destination
- Other transport, network, data link packet header fields

Rules

- Conditions defined using packet information, direction
- Wildcards (*) support to match multiple values
- Actions typically accept or drop
- List of rules processed in order

Example Packet Filtering Firewalls

Software

- In operating systems: iptables (Linux), ipfw (Mac OSX), pf (BSD), Windows Firewall
- Standalone software: Comodo, Kaspersky, Norton, ZoneAlarm, Check Point, . . .

Appliances

- Firewall included in most consumer and enterprise routers
- Dedicated hardware: Cisco ASA/PIX, Dell SonicWALL, HP, Barracuda, Juniper, . . .
- Dedicated software distributions: pfSense, Monowall, Smoothwall, ClearOS, Untangle, IPCop, . . .

Issues with Packet Filtering Firewalls

Advantages

- Simplicity
- Transparent to users
- Very fast

Disadvantages

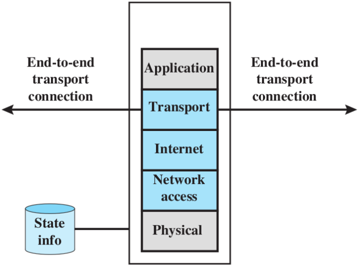
- Cannot prevent attacks that employ application specific vulnerabilities or functions
- Limited logging functionality
- Do not support advanced user authentication
- Vulnerable to attacks on TCP/IP protocol bugs
- Improper configuration can lead to breaches

Stateful Packet Inspection

- Traditional packet filtering firewall makes decisions based on individual packets; don't consider past packets (stateless)
- Many applications establish a connection between client/server; group of packets belong to a connection
- Often easier to define rules for connections, rather than individual packets
- Need to store information about past behaviour (stateful)
- Stateful Packet Inspection (SPI) is extension of traditional packet filtering firewalls
- Issues: extra overhead required for maintaining state information

Stateful Packet Inspection

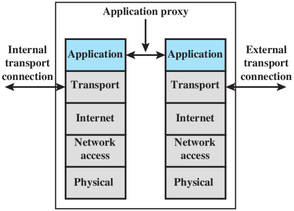
- For connections accepted by packet filtering firewall, record connection information
    - src/dest IP address, src/dest port, sequence numbers, connection state (e.g. Established, Closing)
- Packets arriving that belong to existing connections can be accepted without processing by firewall rules


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

Credit: Figure 9.1(c) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Application Proxy

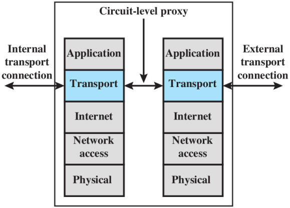
- Also called Application-level Gateway
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application; may restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection



Credit: Figure 9.1(e) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Circuit-level Proxy Firewall

- Also called Circuit-level Gateway
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed
- Typically used when inside users are trusted
- May use application-level gateway inbound and circuit-level gateway outbound; lower overheads



Credit: Figure 9.1(e) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Contents

Firewall Characteristics

Types of Firewalls

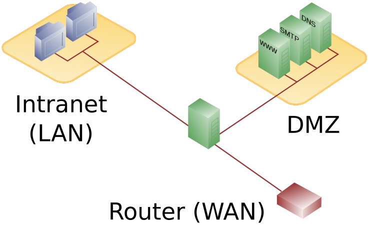
Firewall Locations

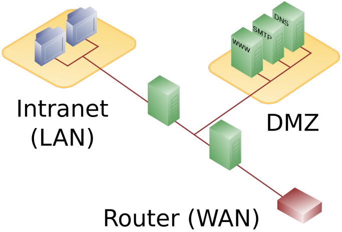
Summary

Firewall Locations

- Firewalls can be located on hosts: end-users computers and servers
- With large number of users, firewalls located on network devices that interconnect internal and external networks
- Common to separate internal network into two zones:
  1. Public-facing servers, e.g. web, email, DNS
  2. End-user computers and internal servers, e.g. databases, development web servers
- Public-facing servers put in De-Militarised Zone (DMZ)

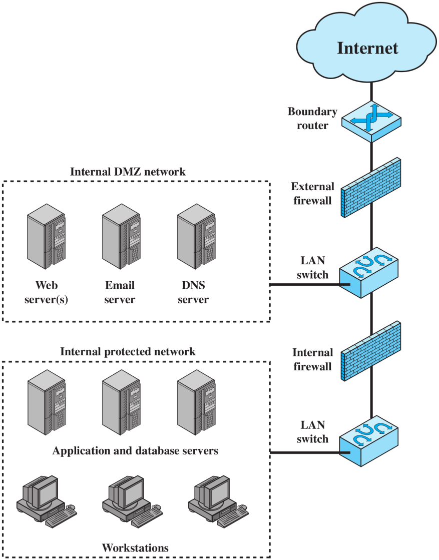
DMZ with 1 or 2 Firewalls





Credit: Pbroks13/Sangre Viento, Wikimedia Commons, Public Domain

Example DMZ with 2 Firewalls



Credit: Figure 9.3 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

Contents

Firewall Characteristics

Types of Firewalls

Firewall Locations

Summary

Key Points

- Firewall controls traffic into and out of a network (or computer)
- Control based on services, direction, user and behaviour
- Packet filtering: accept/reject packets based on headers
- Stateful packet inspection: keep track of past connections
- Proxy firewalls: relay application or connection traffic

Security Issues

- Complexity and human error: writing firewall rules that implement the security policy is difficult for large networks
- Bypassing security policies using tunnels
- Bypassing firewalls using other networks (WiFi, mobile) or devices (laptop, USB)

Areas To Explore

- Deep Packet Inspection