



Firewalls



What is a Firewall?

- A single point to control access to and from network based on admin policy
- Sits between the (secured) internal network and the (untrusted) external internet
- Imposes restrictions on network services ([Security policies](#))
 - only authorized traffic is allowed
- Auditing and controlling access
 - can implement alarms for abnormal behavior
- Is itself immune to penetration



Firewall Limitations

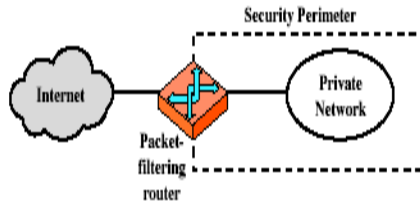
- cannot protect from attacks bypassing it
 - Ex. Dial-in from outside
- cannot protect against internal threats
 - Ex. – take private data out on CD
- cannot protect against transfer of all virus infected programs or files
 - Can co-locate antivirus software to scan all incoming traffic, costly



Types of Firewalls

- Packet Filters
 - Scans all packets and applies rules to forward or discard based on info in packet
 - IP address, port,...
- Application Level Gateways
 - Works at application level, similar to proxy servers
 - Relays application level traffic after examining and verifying content
- Circuit Level Gateways
 - Similar to application level gateway, but once connection is set up, simply relays and does not examine content

Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

- Simple and easy to implement
- Examine each IP packet and permit or deny according to rules
- Can filter packets in both directions
- Restrict access to services (ports)
- Possible default policies
 - that not expressly permitted is prohibited
 - that not expressly prohibited is permitted

Table 20.1 Packet-Filtering Examples

A	action	ourhost	port	theirhost	port	comment
	block	*	*	SPIGOT	*	we don't trust these people
	allow	OUR-GW	25	*	*	connection to our SMTP port

B	action	ourhost	port	theirhost	port	comment
	block	*	*	*	*	default

C	action	ourhost	port	theirhost	port	comment
	allow	*	*	*	25	connection to their SMTP port

D	action	src	port	dest	port	flags	comment
	allow	{our hosts}	*	*	25		our packets to their SMTP port
	allow	*	25	*	*	ACK	their replies

E	action	src	port	dest	port	flags	comment
	allow	{our hosts}	*	*	*		our outgoing calls
	allow	*	*	*	*	ACK	replies to our calls
	allow	*	*	*	>1024		traffic to nonservers

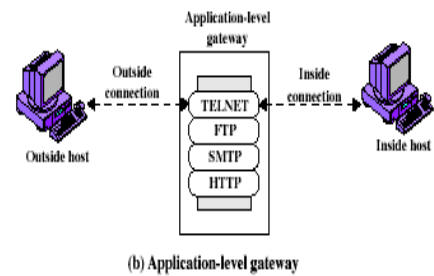
Attacks on Packet Filters

- IP address spoofing
 - fake source address to be trusted
 - add filters on router to block
- Source routing attacks
 - attacker sets a route other than default
 - block source routed packets
- Tiny fragment attacks
 - split header info over several tiny packets
 - either discard or reassemble before check

Firewalls – Stateful Packet Filters

- Examine each IP packet in context
 - keeps tracks of client-server sessions
 - checks each packet validly belongs to one
- Better able to detect bogus packets out of context
- More complex to implement

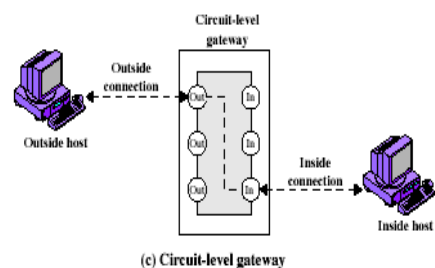
Firewalls - Application Level Gateway (or Proxy)



Firewalls - Application Level Gateway (or Proxy)

- Use an application specific gateway / proxy
- Has full access to protocol
 - user requests service from proxy
 - proxy validates request as legal
 - Forwards request to server and returns result to user
 - Can change part of the request
- Need separate proxies for each service
 - some services naturally support proxying
 - others are more problematic
 - custom services generally not supported

Firewalls - Circuit Level Gateway



Firewalls - Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting what connections are allowed
- Once created usually relays traffic without examining contents
- Typically used for allowing general outbound connections to trusted users inside. Verify user and then just relay messages with no further check
- SOCKS commonly used for this

SOCKS - Overview

- RFC 1928
- SOCKS server on firewall
- Client library on internal hosts
- Recompile/relink TCP based clients with SOCKS library
- Client opens TCP connection to appropriate SOCKS port on firewall
- SOCKS server acts as the circuit-level gateway
- Advantage – unified mechanism for all applications

Bastion Host

- Highly secure host system
- Potentially exposed to "hostile" elements
 - Hence is secured to withstand this
- May support 2 or more net connections
- May be trusted to enforce trusted separation between network connections
- Runs circuit / application level gateways or provides externally accessible services

Firewall Configurations

