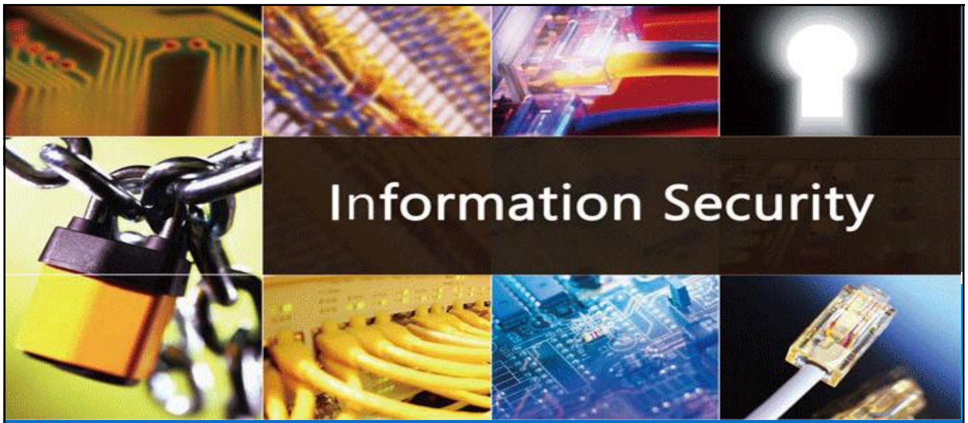


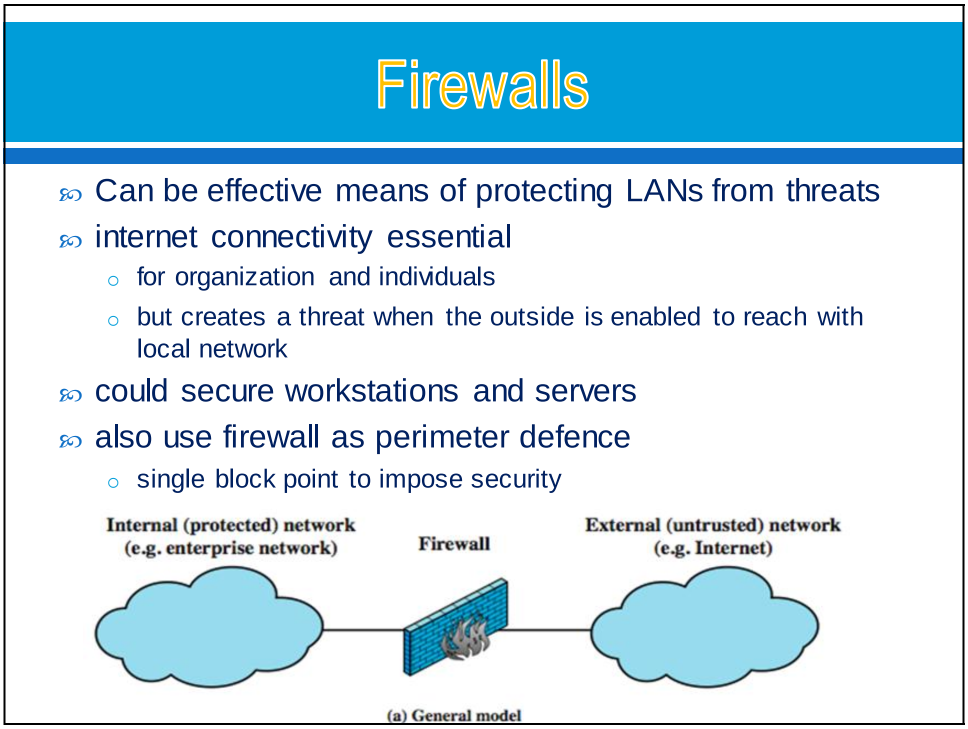
Information Security

Chapter 10: Firewall

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- Introduction
- Capabilities and Limits
- Firewall types
- Firewall basing
- Security: Defense in Depth
- Firewall locations
- Packet Filter Rules

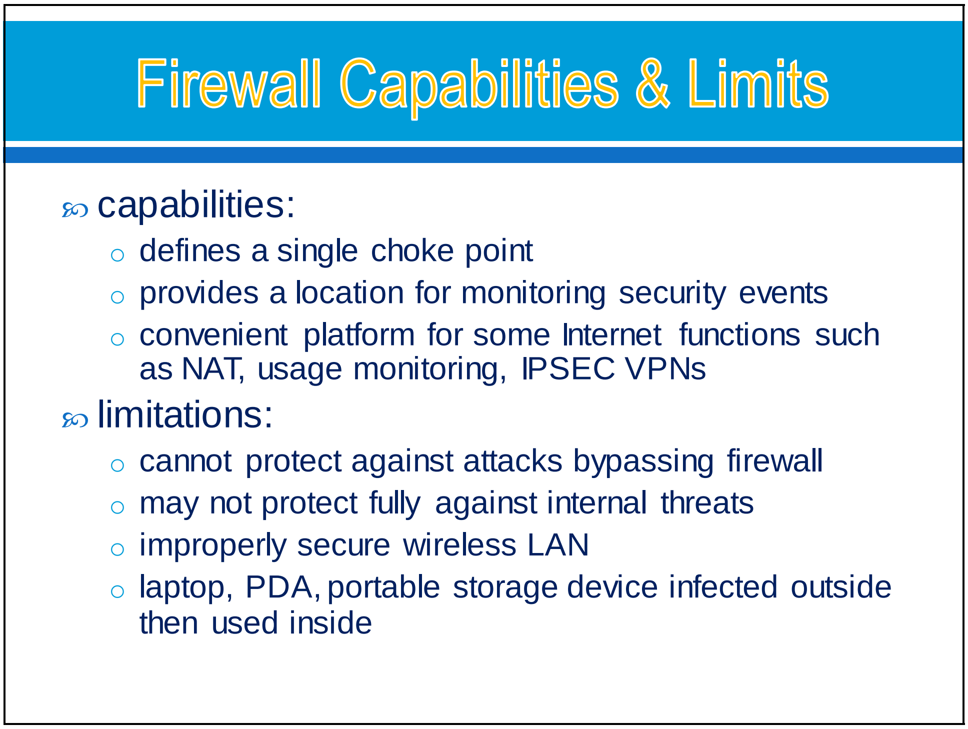


Firewalls

- Can be effective means of protecting LANs from threats
- internet connectivity essential
  - for organization and individuals
  - but creates a threat when the outside is enabled to reach with local network
- could secure workstations and servers
- also use firewall as perimeter defence
  - single block point to impose security

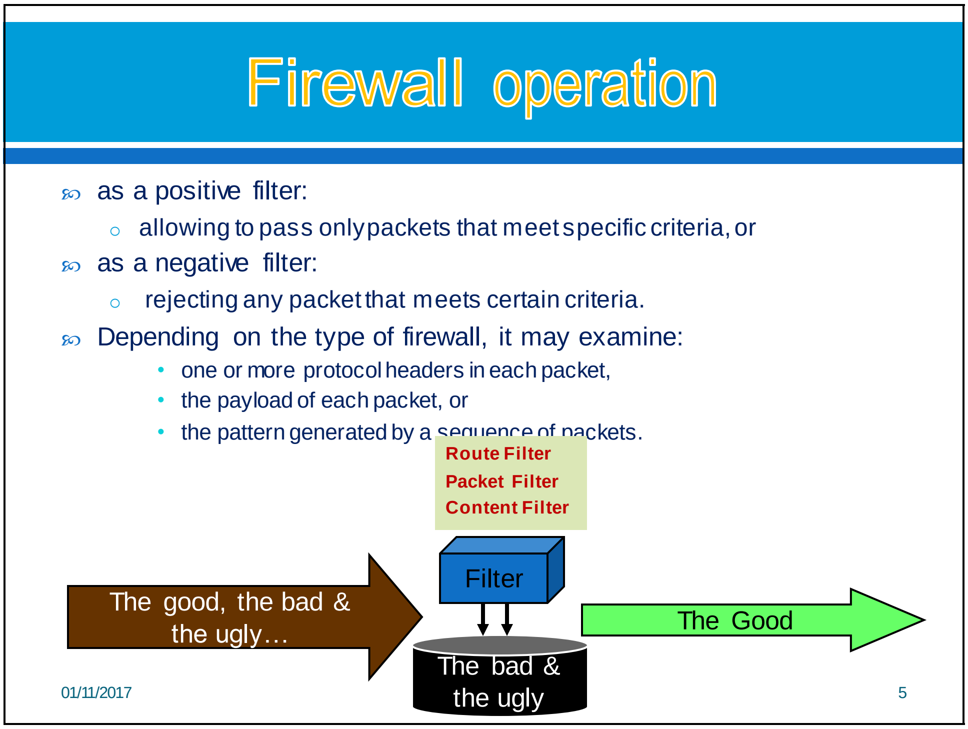
Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

(a) General model



Firewall Capabilities & Limits

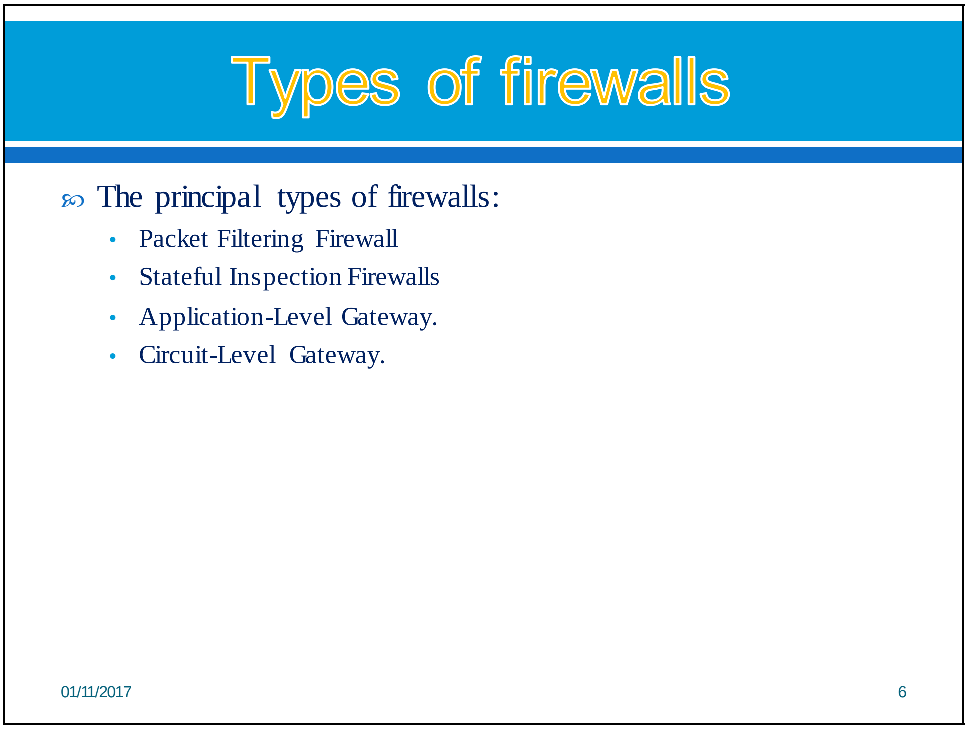
- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - improperly secure wireless LAN
  - laptop, PDA, portable storage device infected outside then used inside



Firewall operation

- as a positive filter:
  - allowing to pass only packets that meet specific criteria, or
- as a negative filter:
  - rejecting any packet that meets certain criteria.
- Depending on the type of firewall, it may examine:
  - one or more protocol headers in each packet,
  - the payload of each packet, or
  - the pattern generated by a sequence of packets.

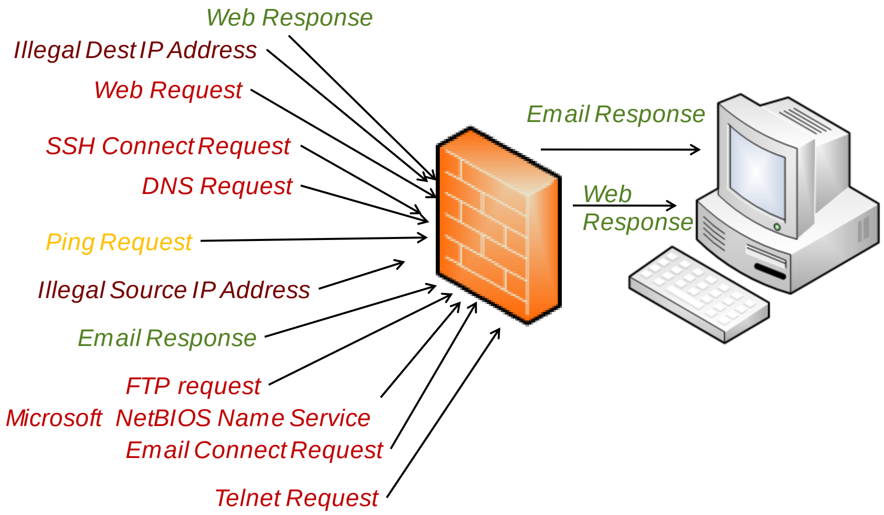
Route Filter
Packet Filter
Content Filter
Filter
The good, the bad & the ugly…
The bad & the ugly
The Good



Types of firewalls

- The principal types of firewalls:
  - Packet Filtering Firewall
  - Stateful Inspection Firewalls
  - Application-Level Gateway.
  - Circuit-Level Gateway.

Packet Filter Firewall

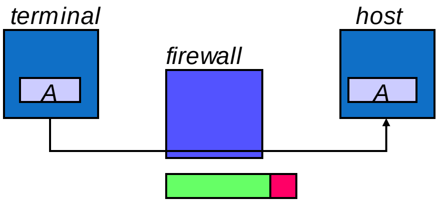


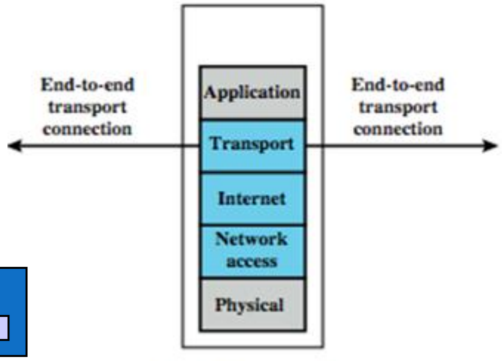
Web Response
Illegal Dest IP Address
Web Request
SSH Connect Request
DNS Request
Ping Request
Illegal Source IP Address
Email Response
FTP request
Microsoft NetBIOS Name Service
Email Connect Request
Telnet Request
Email Response
Web Response

Packet Filtering

Packet Filtering:

- Packet header is inspected
- Single packet attacks caught
- Very little overhead in firewall: very quick
- High volume filter





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

(b) Packet filtering firewall

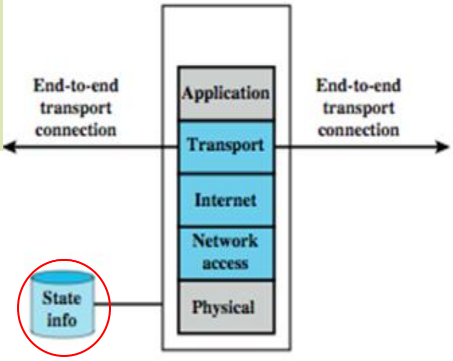
Packet Filter Weaknesses

- weaknesses
  - cannot prevent attack on application bugs (do not examine upper-layer data)
  - limited logging functionality
  - do no support advanced user authentication
  - vulnerable to attacks on TCP/IP protocol bugs
  - improper configuration can lead to breaches
- attacks
  - IP address spoofing,
  - source route attacks,
  - tiny fragment attacks

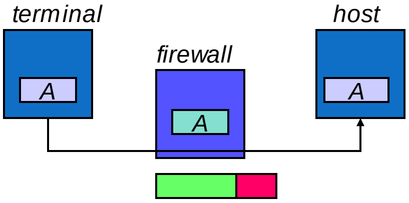
Stateful Inspection

Stateful Inspection

- State retained in firewall memory
- Most multi-packet attacks caught
- More fields in packet header inspected
- Little overhead in firewall: quick


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

(c) Stateful inspection firewall



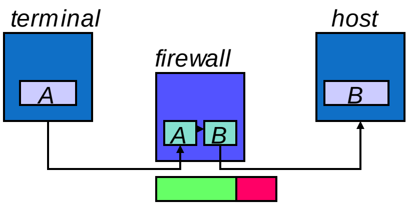
Stateful Inspection Firewall

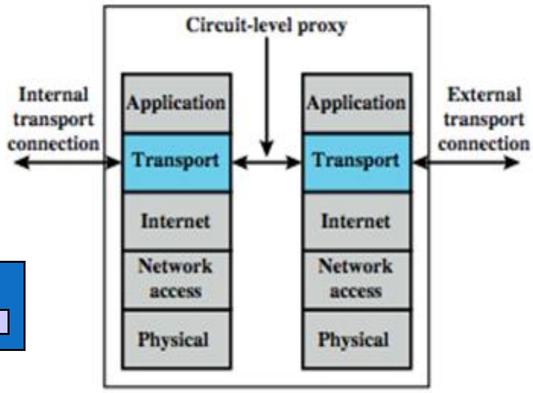
- reviews packet header information but also keeps info on TCP connections
  - typically have low, “known” port no for server
  - and high, dynamically assigned client port nº.
  - simple packet filter must allow all return high port numbered packets back in
  - stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  - only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  - may also track TCP seq numbers as well

Circuit-Level Firewall

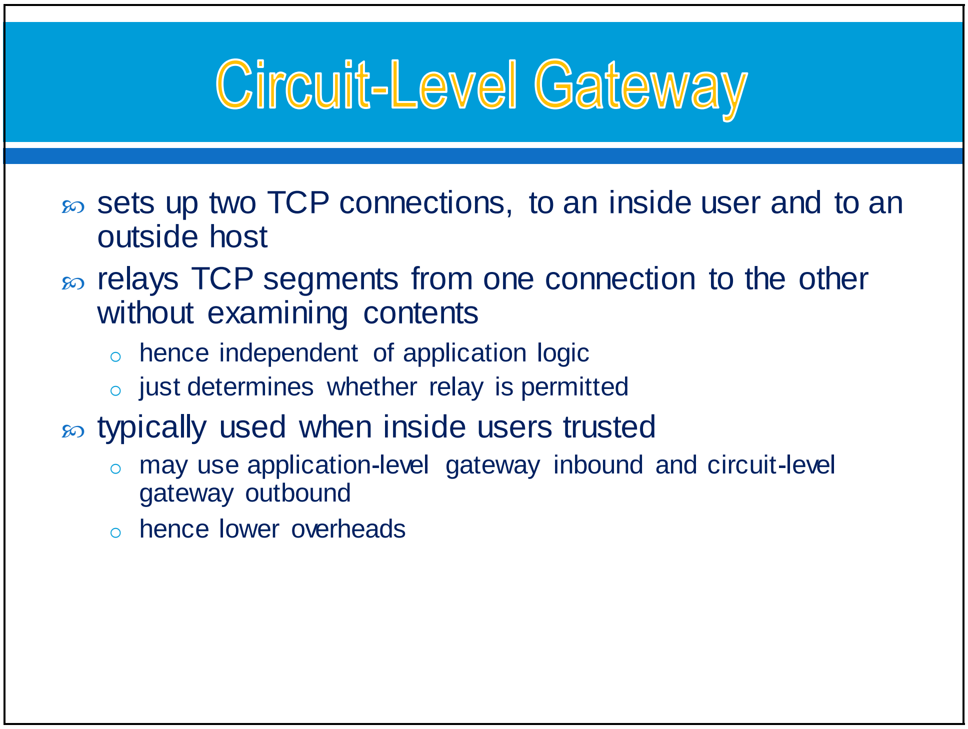
Circuit-Level Firewall:

- Packet session terminated and recreated via a Proxy Server
- All multi-packet attacks caught
- Packet header completely inspected
- High overhead in firewall: slow



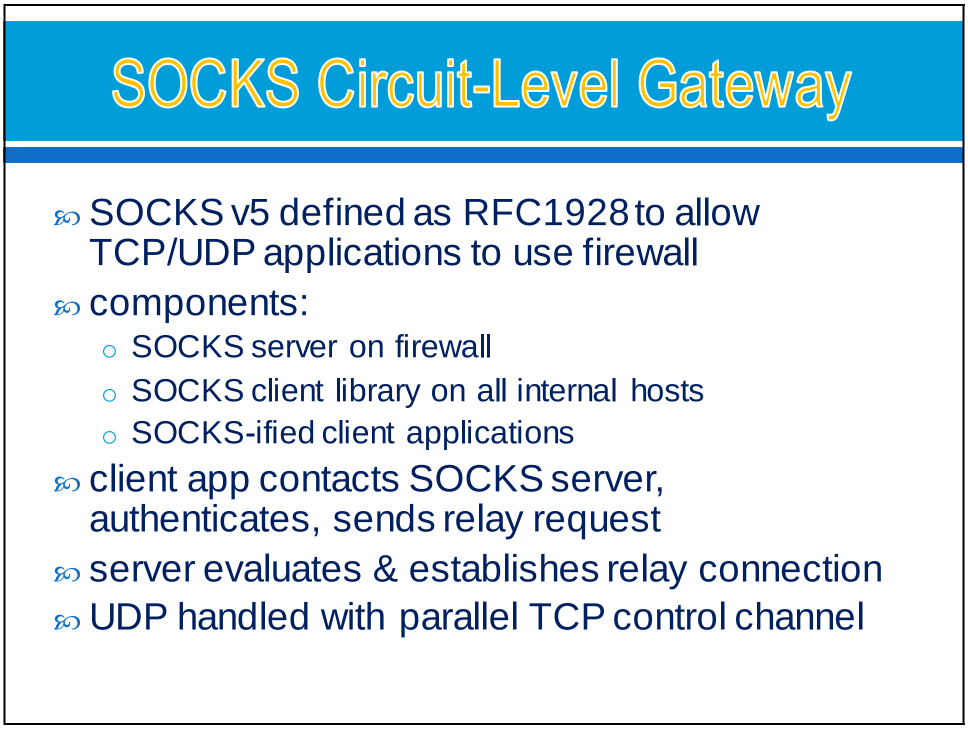


(e) Circuit-level proxy firewall



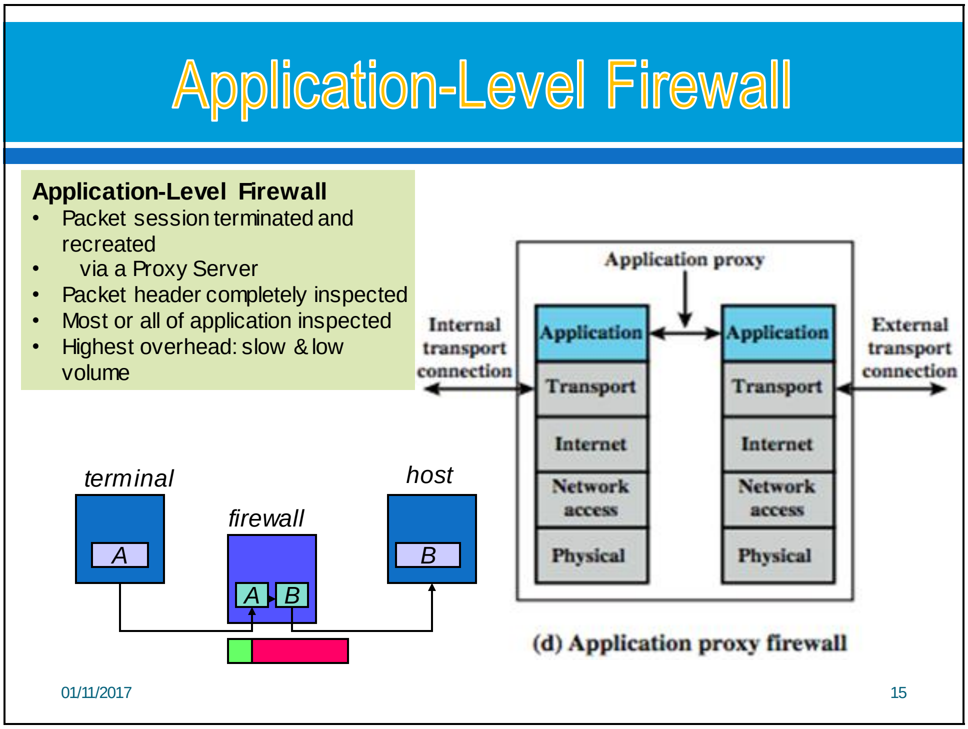
Circuit-Level Gateway

- sets up two TCP connections, to an inside user and to an outside host
- relays TCP segments from one connection to the other without examining contents
  - hence independent of application logic
  - just determines whether relay is permitted
- typically used when inside users trusted
  - may use application-level gateway inbound and circuit-level gateway outbound
  - hence lower overheads



SOCKS Circuit-Level Gateway

- SOCKS v5 defined as RFC1928 to allow TCP/UDP applications to use firewall
- components:
  - SOCKS server on firewall
  - SOCKS client library on all internal hosts
  - SOCKS-ified client applications
- client app contacts SOCKS server, authenticates, sends relay request
- server evaluates & establishes relay connection
- UDP handled with parallel TCP control channel

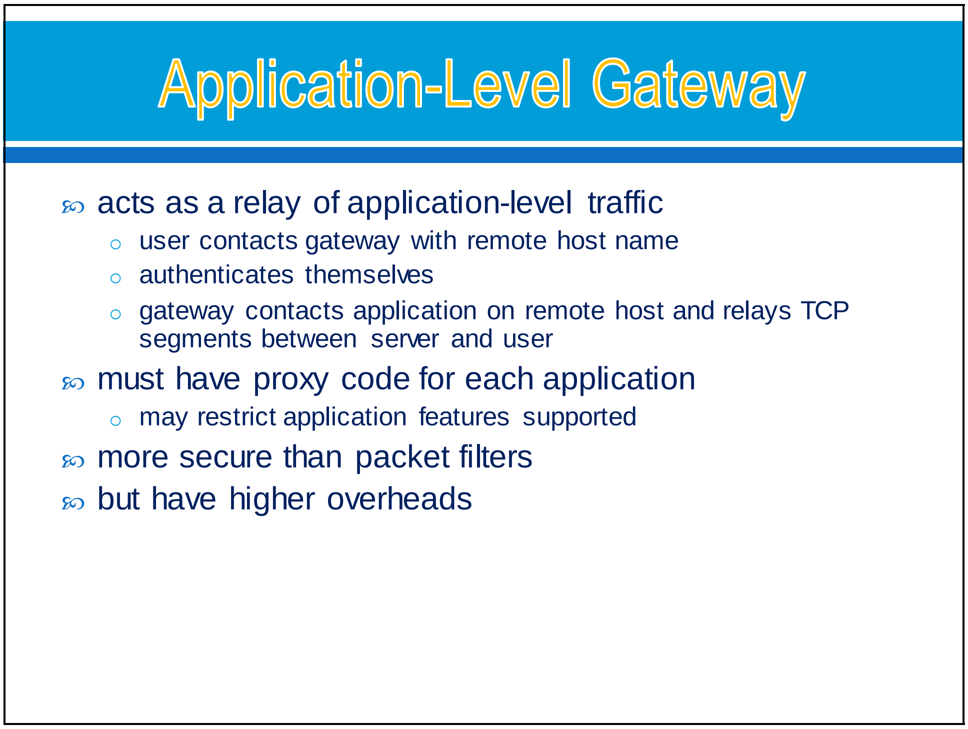


Application-Level Firewall

Application-Level Firewall

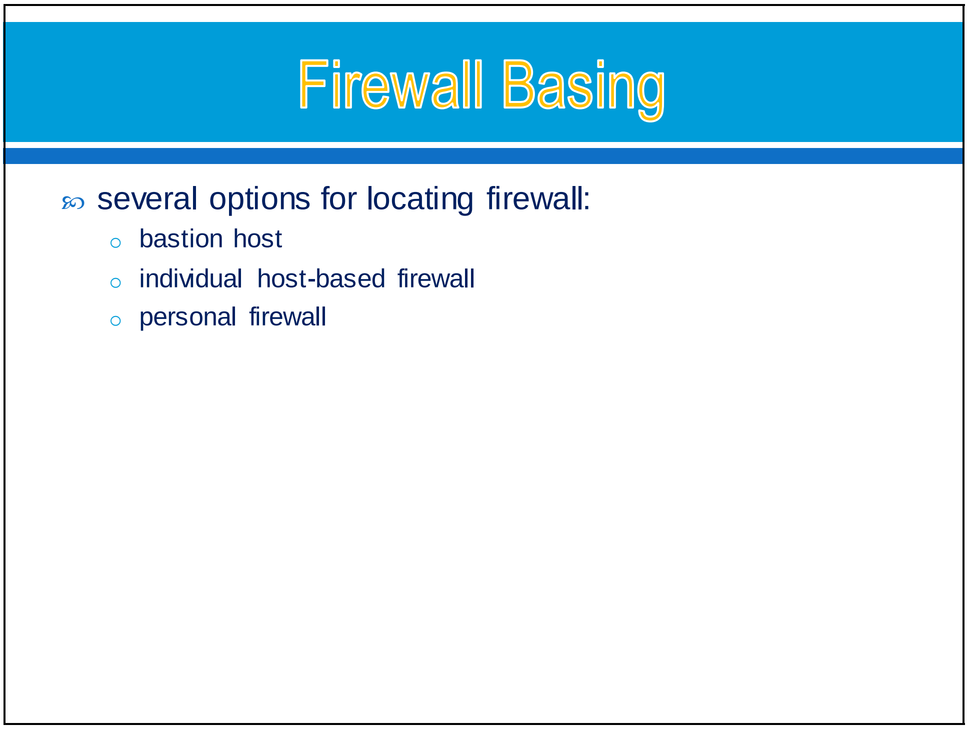
- Packet session terminated and recreated
- via a Proxy Server
- Packet header completely inspected
- Most or all of application inspected
- Highest overhead: slow & low volume

(d) Application proxy firewall



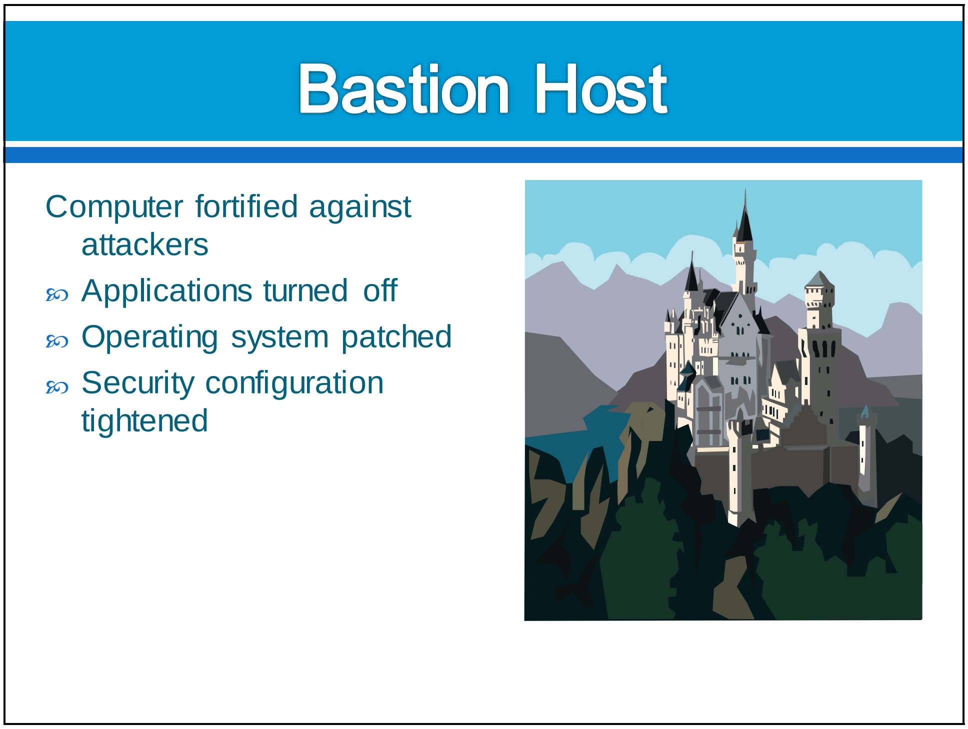
Application-Level Gateway

- acts as a relay of application-level traffic
  - user contacts gateway with remote host name
  - authenticates themselves
  - 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
- more secure than packet filters
- but have higher overheads



Firewall Basing

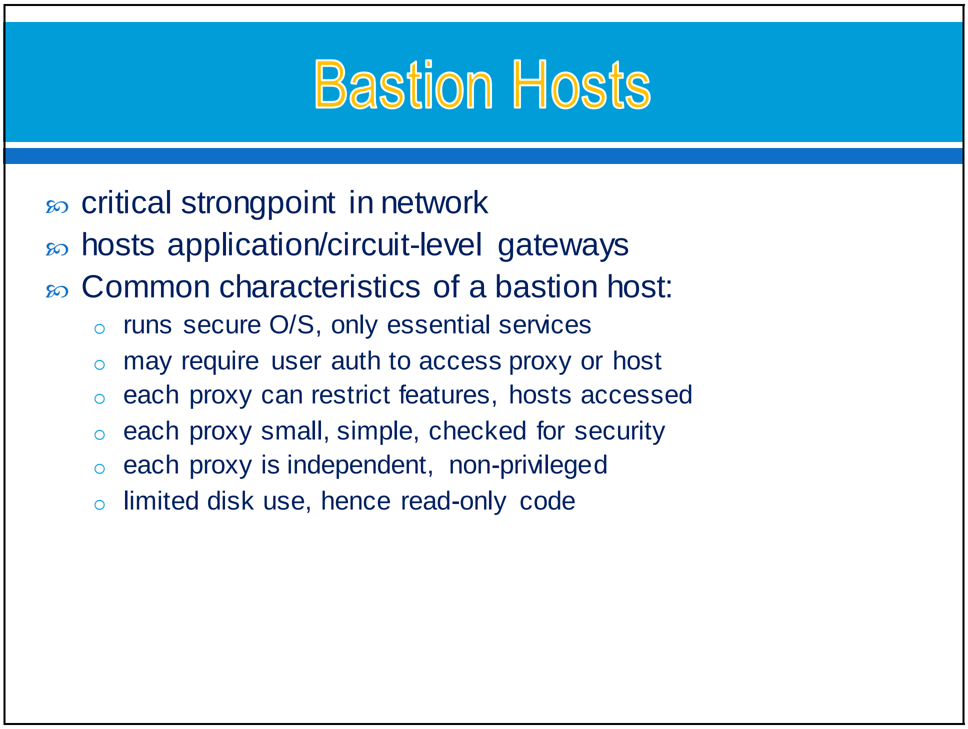
- several options for locating firewall:
  - bastion host
  - individual host-based firewall
  - personal firewall



Bastion Host

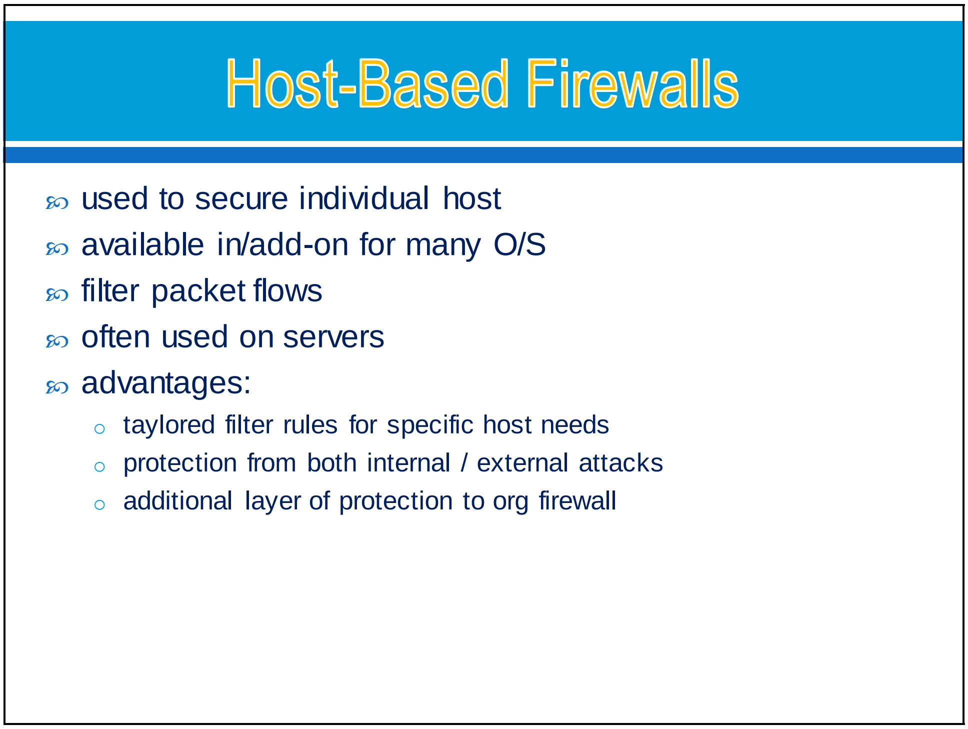
Computer fortified against attackers

- Applications turned off
- Operating system patched
- Security configuration tightened



Bastion Hosts

- critical strongpoint in network
- hosts application/circuit-level gateways
- Common characteristics of a bastion host:
  - runs secure O/S, only essential services
  - may require user auth to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code



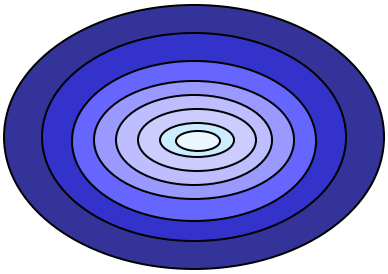
Host-Based Firewalls

- used to secure individual host
- available in/add-on for many O/S
- filter packet flows
- often used on servers
- advantages:
  - taylored filter rules for specific host needs
  - protection from both internal / external attacks
  - additional layer of protection to org firewall

Personal Firewall

- controls traffic flow to/from PC/workstation
- for both home or corporate use
- may be software module on PC
- or in home cable/DSL router/gateway
- typically much less complex
- primary role to deny unauthorized access
- may also monitor outgoing traffic to detect/block worm/malware activity

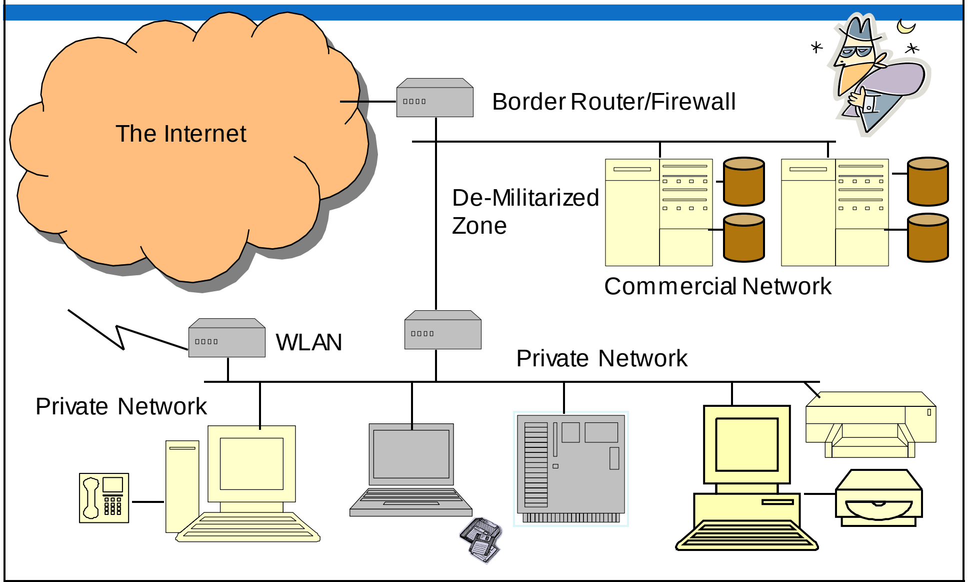
Security: Defense in Depth



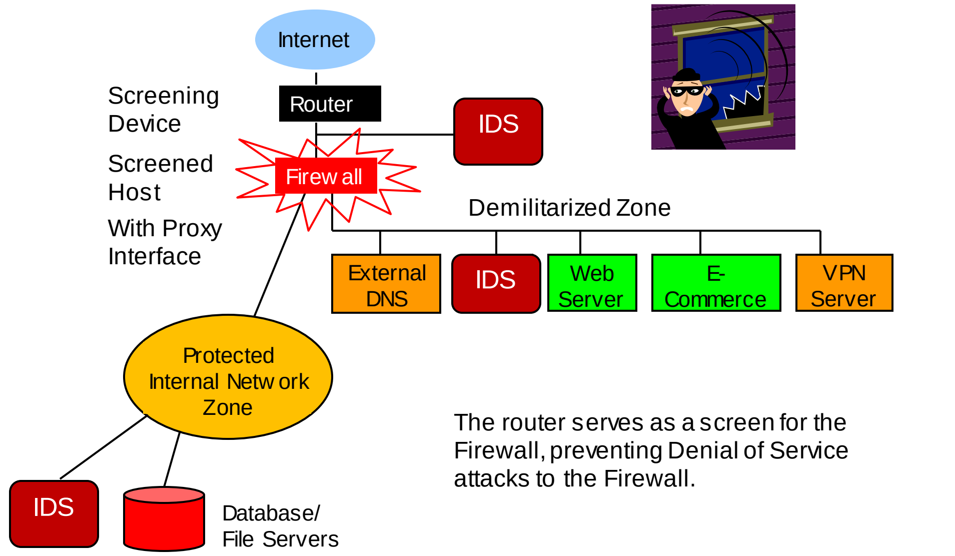
- Border Router
- Perimeter firewall
- Internal firewall
- Intrusion Detection System
- Policies & Procedures & Audits
- Authentication
- Access Controls

Attacking the Network

What ways do you see of getting in?

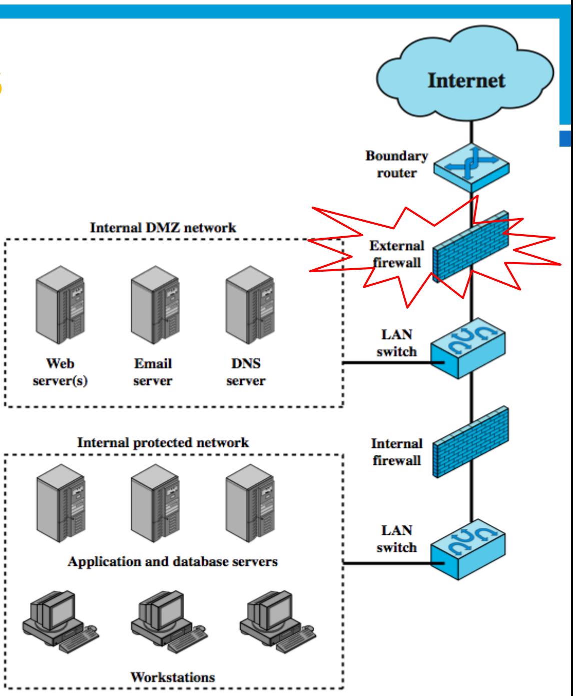


Multi-Homed Firewall: Separate Zones

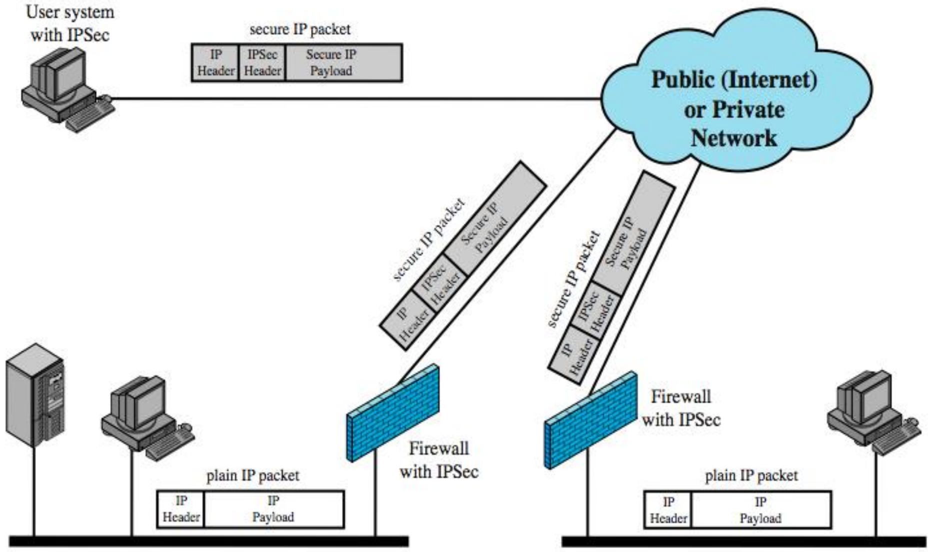


The router serves as a screen for the Firewall, preventing Denial of Service attacks to the Firewall.

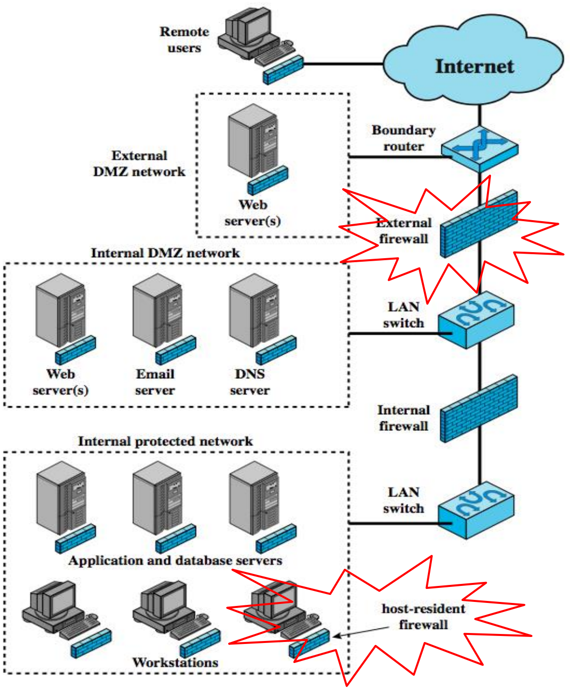
Firewall Locations



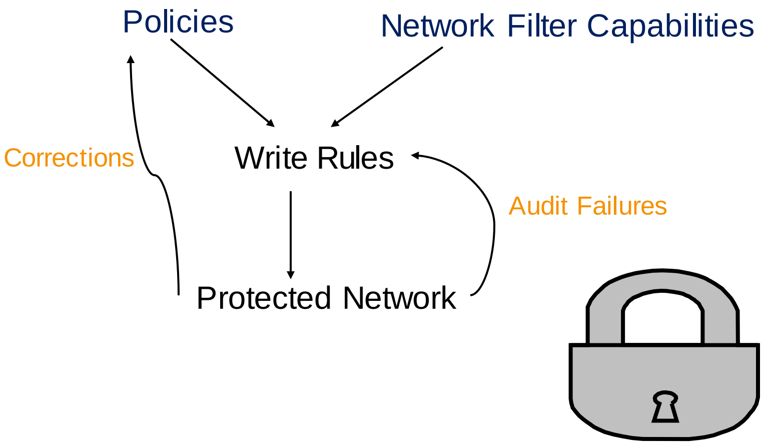
Firewall with Virtual Private Networks

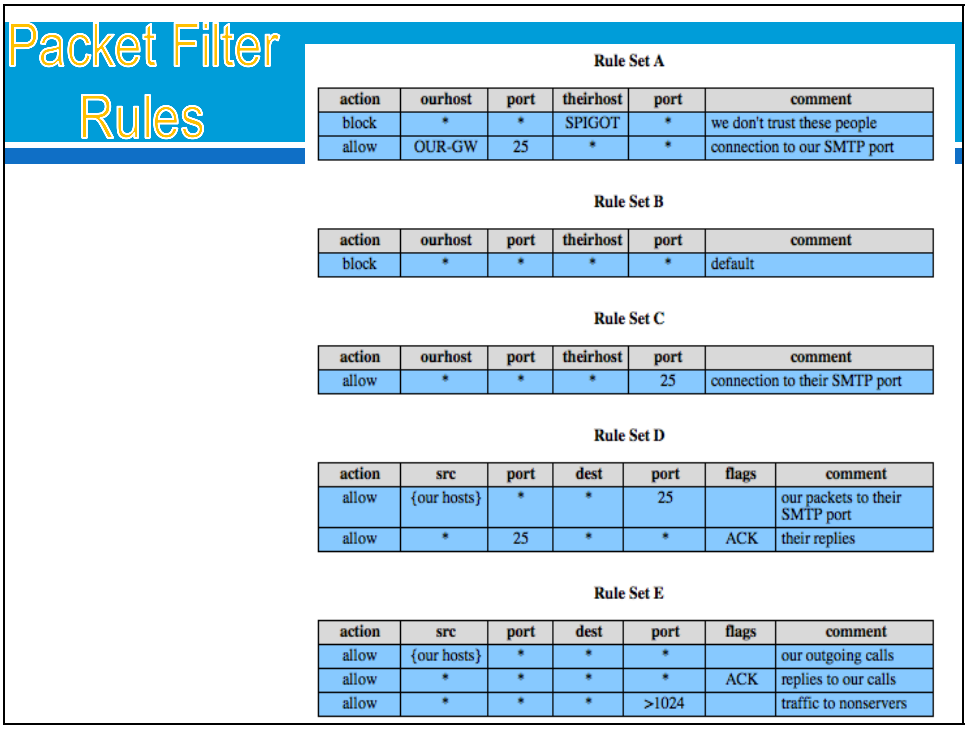


Distributed Firewalls



Firewall policy - Writing Rules





Packet Filter Rules

Rule Set A

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

Rule Set B

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

Rule Set C

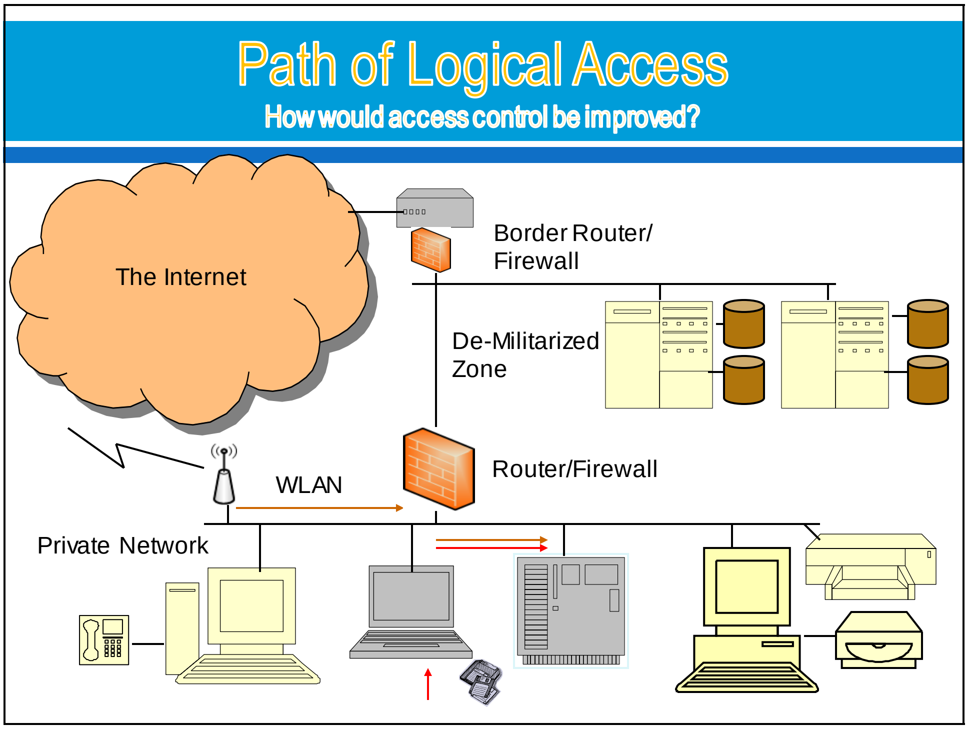
action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

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

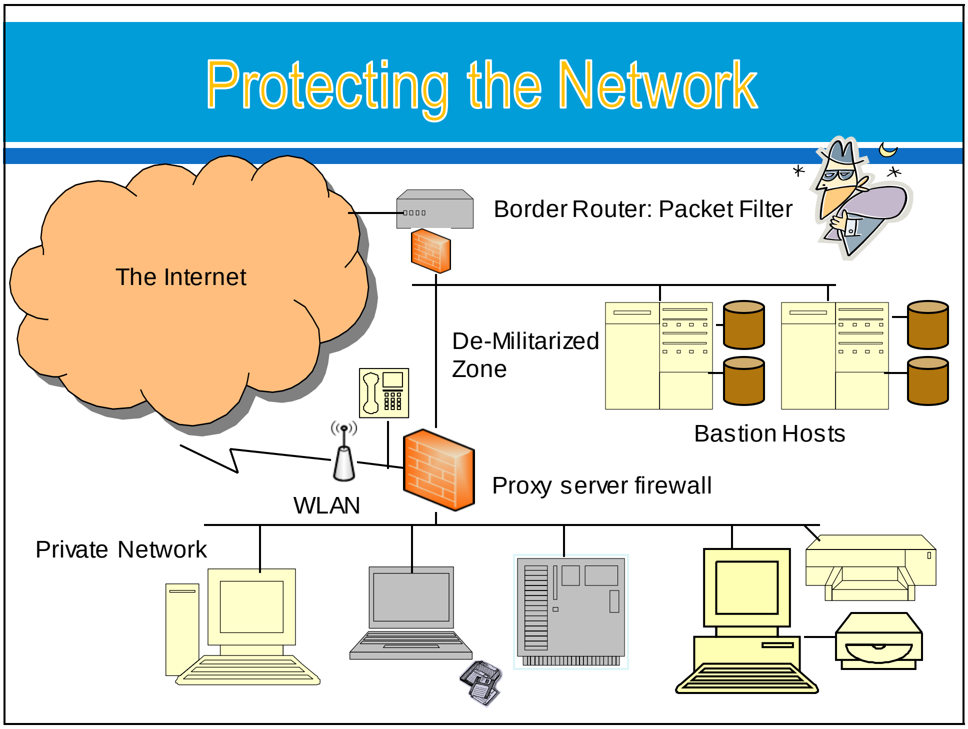
Rule Set E

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



Path of Logical Access

How would access control be improved?



Protecting the Network

The Internet

Border Router: Packet Filter

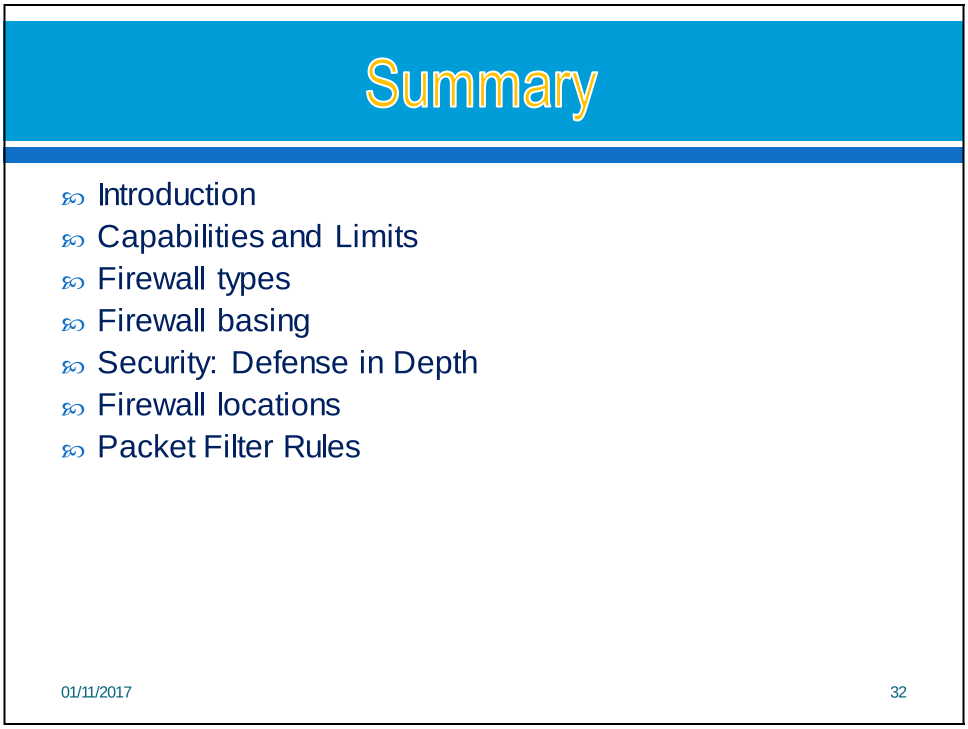
De-Militarized Zone

Bastion Hosts

Proxy server firewall

WLAN

Private Network



Summary

- Introduction
- Capabilities and Limits
- Firewall types
- Firewall basing
- Security: Defense in Depth
- Firewall locations
- Packet Filter Rules

Practice

- Set up a firewall
  - On windows: ISA, TMG
  - On Linux: IPtable, Pfsen, Endian, ClearOS…
- Configure rules in firewall

Q & A