COMPUTER SECURITY

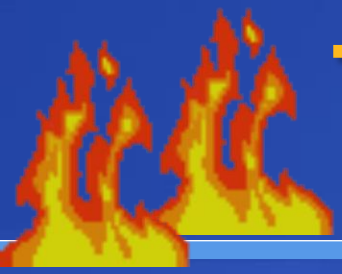
PRINCIPLES AND PRACTICE

SECOND EDITION

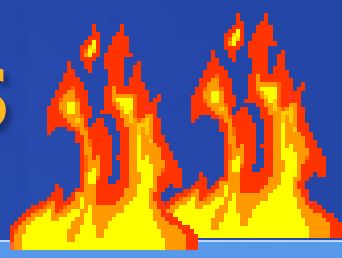
William Stallings | Lawrie Brown

Chapter 9

Firewalls and Intrusion Prevention Systems



The Need For Firewalls



- internet connectivity is essential
  - however it creates a threat
- effective means of protecting LANs
- inserted between the premises network and the Internet to establish a controlled link
  - can be a single computer system or a set of two or more systems working together
- used as a perimeter defense
  - single choke point to impose security and auditing
  - insulates the internal systems from external networks

Firewall Characteristics

design goals

- all traffic from inside to outside must pass through the firewall
- only authorized traffic as defined by the local security policy will be allowed to pass
- the firewall itself is immune to penetration

techniques used by firewalls to control access and enforce the site's security policy are:

- service control
- direction control
- user control
- behavior control

Firewall Capabilities And Limits

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 the platform for IPSec

limitations:

- cannot protect against attacks bypassing firewall
- may not protect fully against internal threats
- improperly secured wireless LAN can be accessed from outside the organization
- laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Types of Firewalls

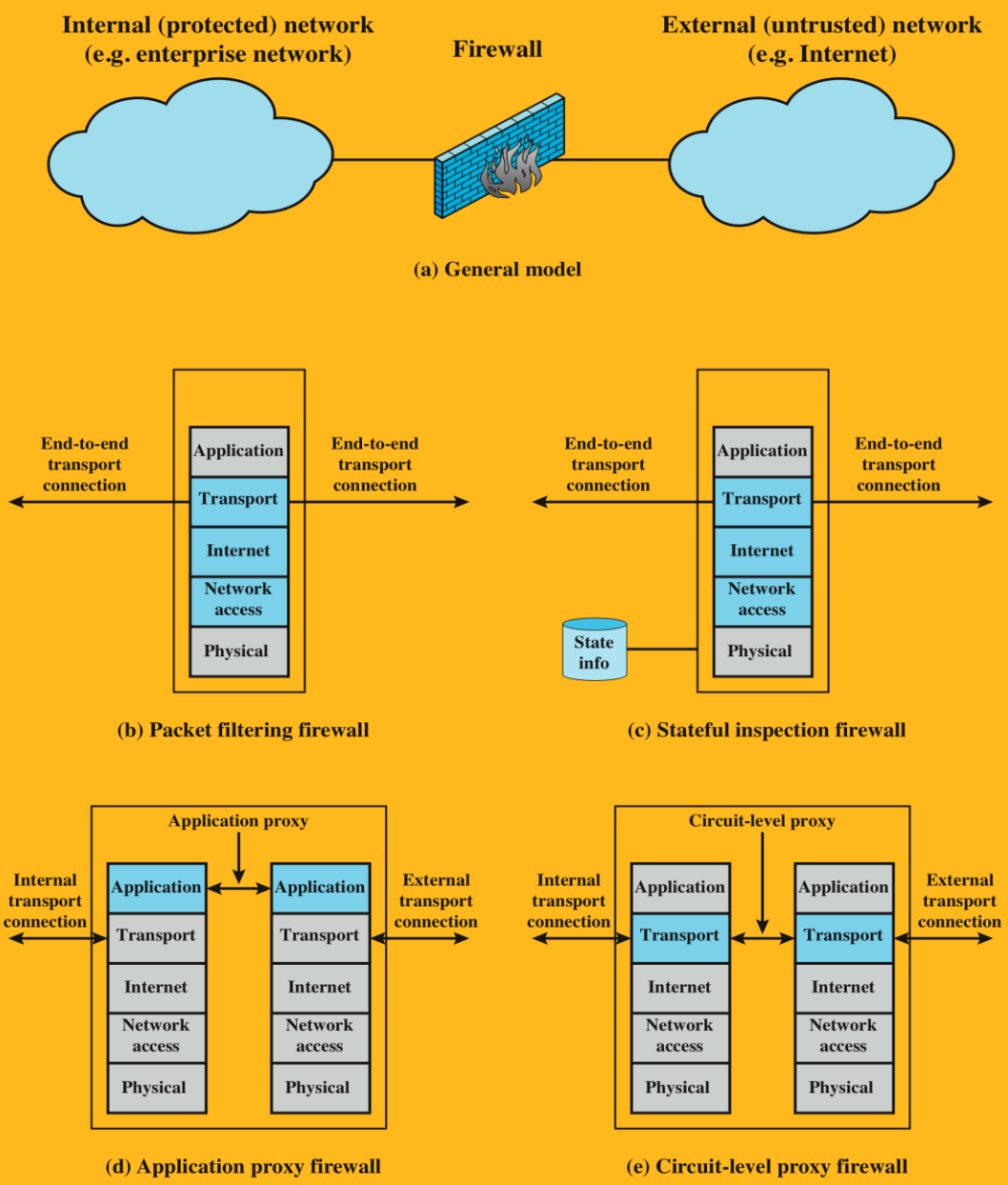


Figure 9.1 Types of Firewalls

Packet Filtering Firewall

- applies rules to each incoming and outgoing IP packet
  - typically a list of rules based on matches in the IP or TCP header
  - forwards or discards the packet based on rules match

filtering rules are based on information contained in a network packet
• source IP address • destination IP address • source and destination transport-level address • IP protocol field • interface

- two default policies:
  - discard - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - forward - permit unless expressly prohibited
    - easier to manage and use but less secure

Table 9.1

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

Packet Filter Advantages And Weaknesses

- advantages
  - simplicity
  - typically transparent to users and are very fast
- weaknesses
  - 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 Inspection Firewall

tightens rules for TCP traffic by creating a directory of outbound TCP connections

- there is an entry for each currently established connection
- packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

reviews packet information but also records information about TCP connections

- keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- inspects data for protocols like FTP, IM and SIPS commands

Example
Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Table 9.2 Example Stateful Firewall Connection State Table [WACK02]

Application-Level Gateway

- also called an application proxy
- acts as a relay of application-level traffic
  - user contacts gateway using a TCP/IP application
  - user is authenticated
  - 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

Circuit-Level Gateway

circuit level proxy

- 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

SOCKS Circuit-Level Gateway

- SOCKS v5 defined in RFC1928
- designed to provide a framework for client-server applications in TCP/UDP domains to conveniently and securely use the services of a network firewall
- client application contacts SOCKS server, authenticates, sends relay request
  - server evaluates and either establishes or denies the connection

components

Bastion Hosts

- system identified as a critical strong point in the network's security
- serves as a platform for an application-level or circuit-level gateway
- common characteristics:
  - runs secure O/S, only essential services
  - may require user authentication to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy is small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code

Host-Based Firewalls

- used to secure an individual host
- available in operating systems or can be provided as an add-on package
- filter and restrict packet flows
- common location is a server

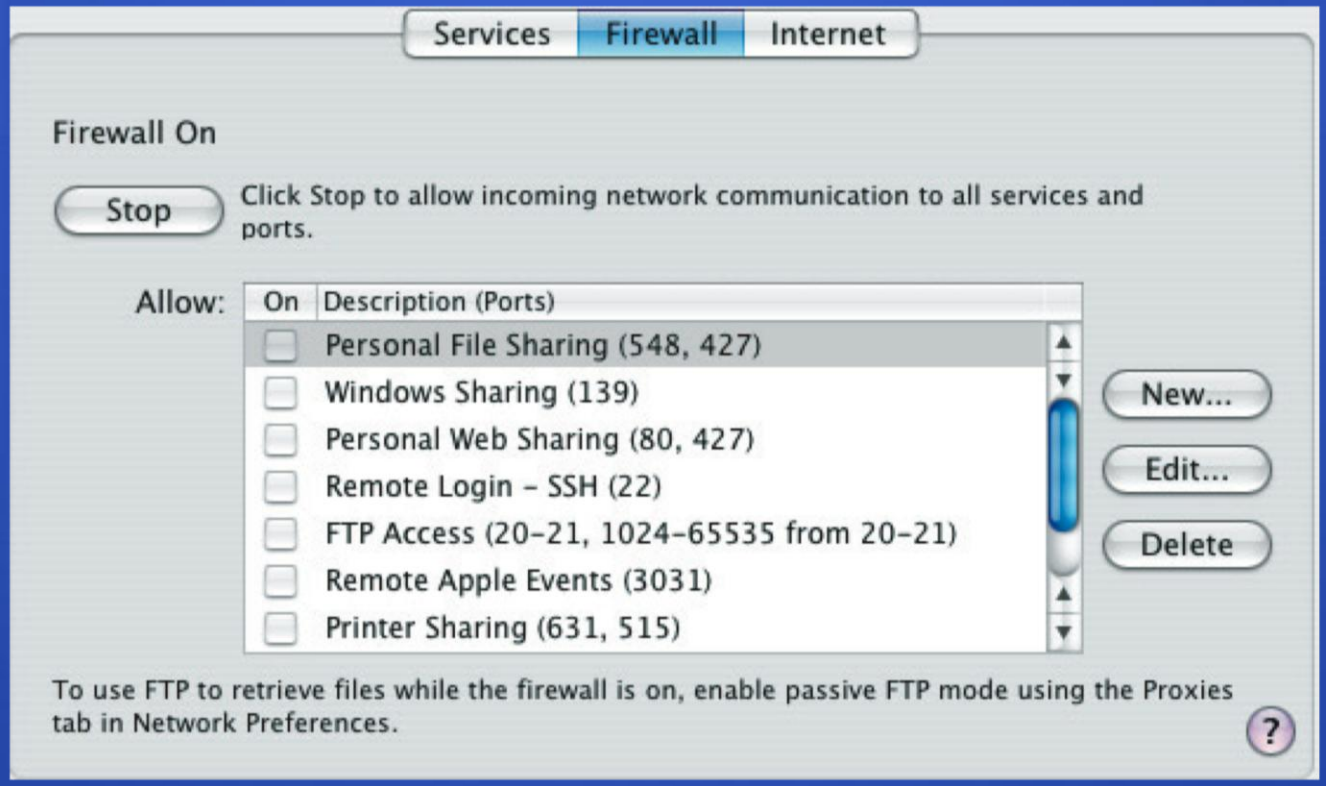
advantages:

- filtering rules can be tailored to the host environment
- protection is provided independent of topology
- provides an additional layer of protection

Personal Firewall

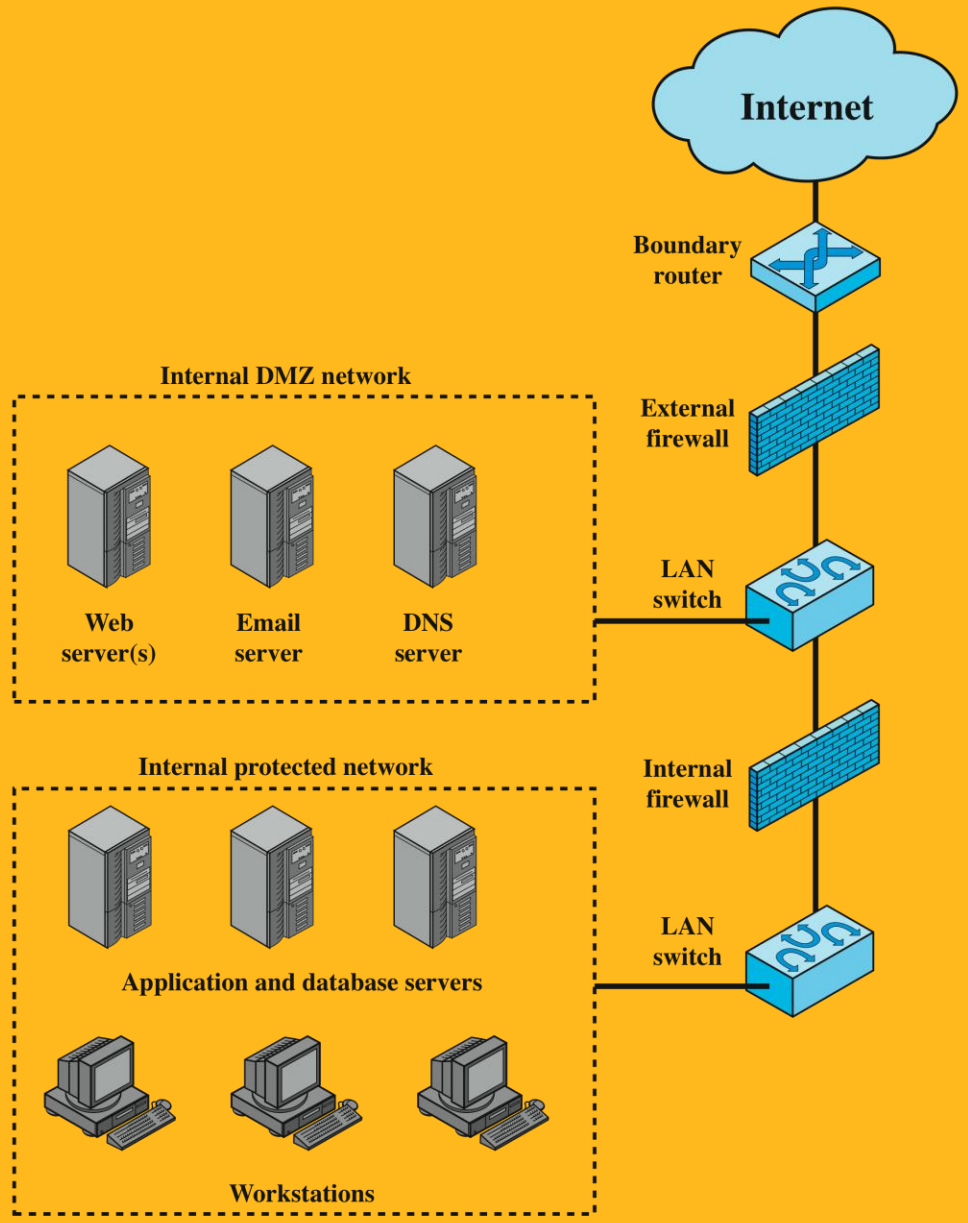
- controls traffic between a personal computer or workstation and the Internet or enterprise network
- for both home or corporate use
- typically is a software module on a personal computer
- can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- typically much less complex than server-based or stand-alone firewalls
- primary role is to deny unauthorized remote access
- may also monitor outgoing traffic to detect and block worms and malware activity

Example
Personal Firewall Interface

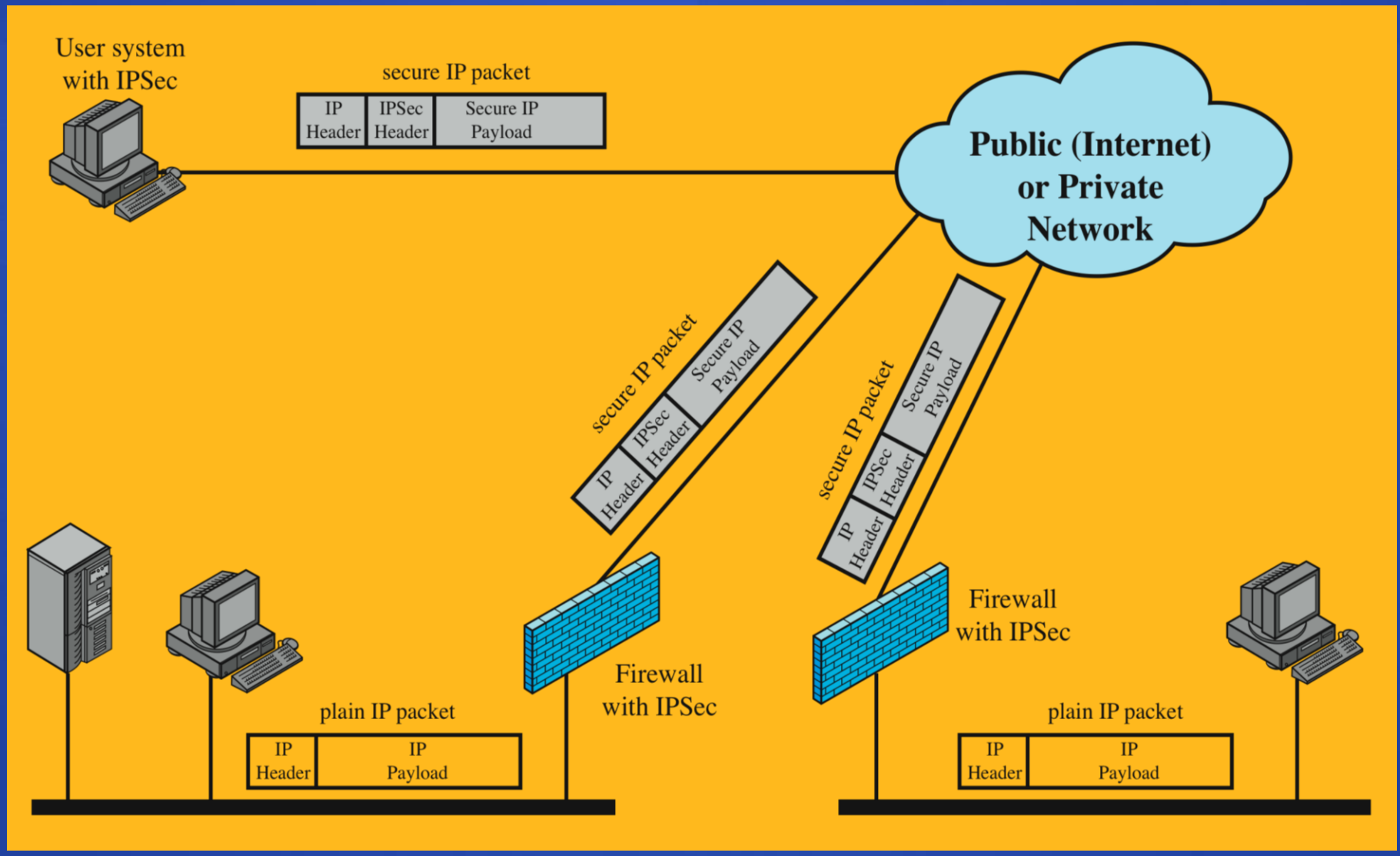


Example

Firewall Configuration

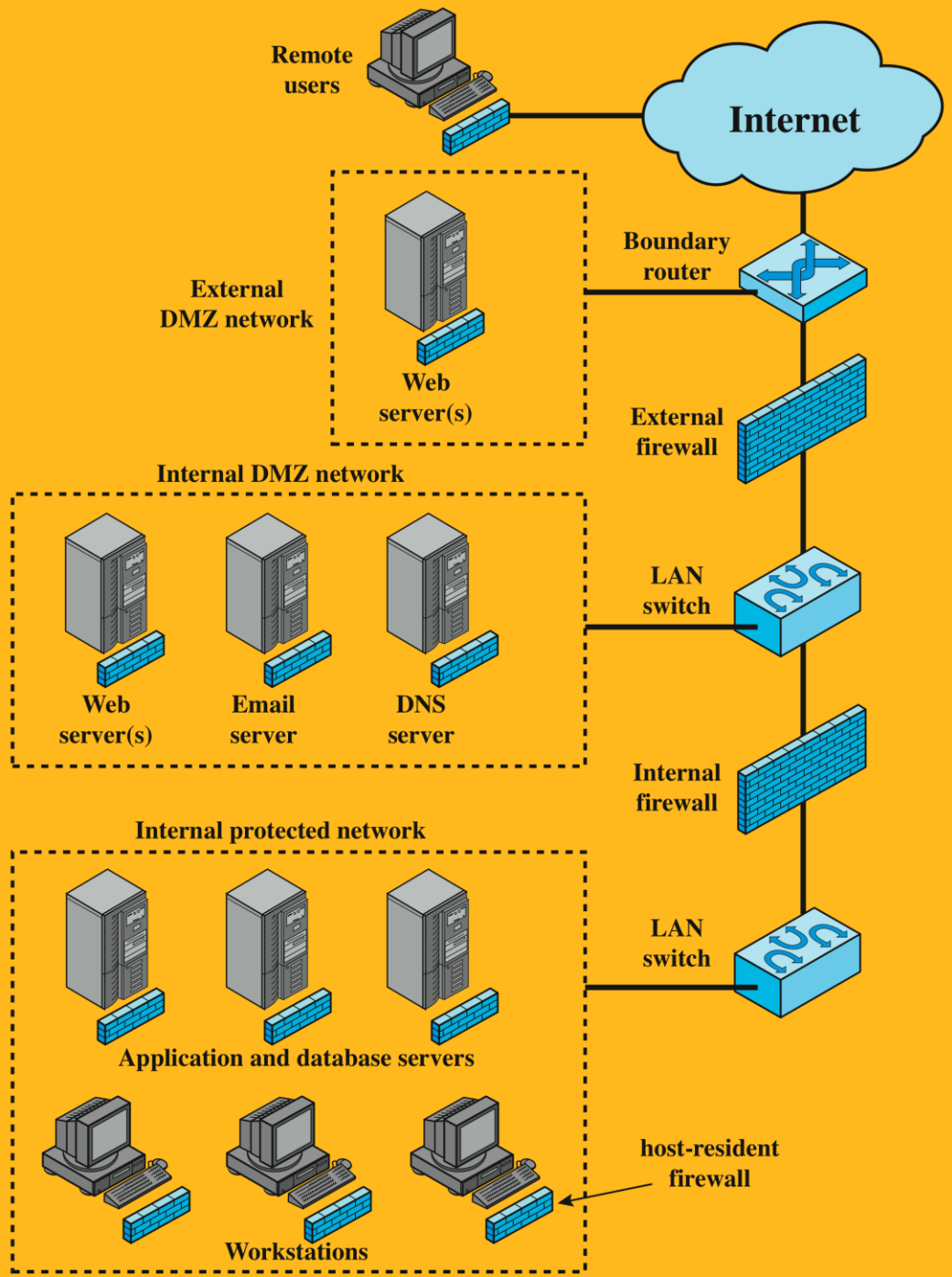


Virtual Private Networks (VPNs)



Example

Distributed Firewall Configuration



Firewall Topologies

host-resident firewall	• includes personal firewall software and firewall software on servers
screening router	• single router between internal and external networks with stateless or full packet filtering
single bastion inline	• single firewall device between an internal and external router
single bastion T	• has a third network interface on bastion to a DMZ where externally visible servers are placed
double bastion inline	• DMZ is sandwiched between bastion firewalls
double bastion T	• DMZ is on a separate network interface on the bastion firewall
distributed firewall configuration	• used by large businesses and government organizations

Intrusion Prevention Systems (IPS)

- recent addition to security products
  - inline network-based IDS that can block traffic
  - functional addition to firewall that adds IDS capabilities
- can block traffic like a firewall
- makes use of algorithms developed for IDSs
- may be network or host based

Host-Based IPS (HIPS)

- identifies attacks using both signature and anomaly detection techniques
  - signature: focus is on the specific content of application payloads in packets, looking for patterns that have been identified as malicious
  - anomaly: IPS is looking for behavior patterns that indicate malware
- can be tailored to the specific platform
- can also use a sandbox approach to monitor behavior

advantages

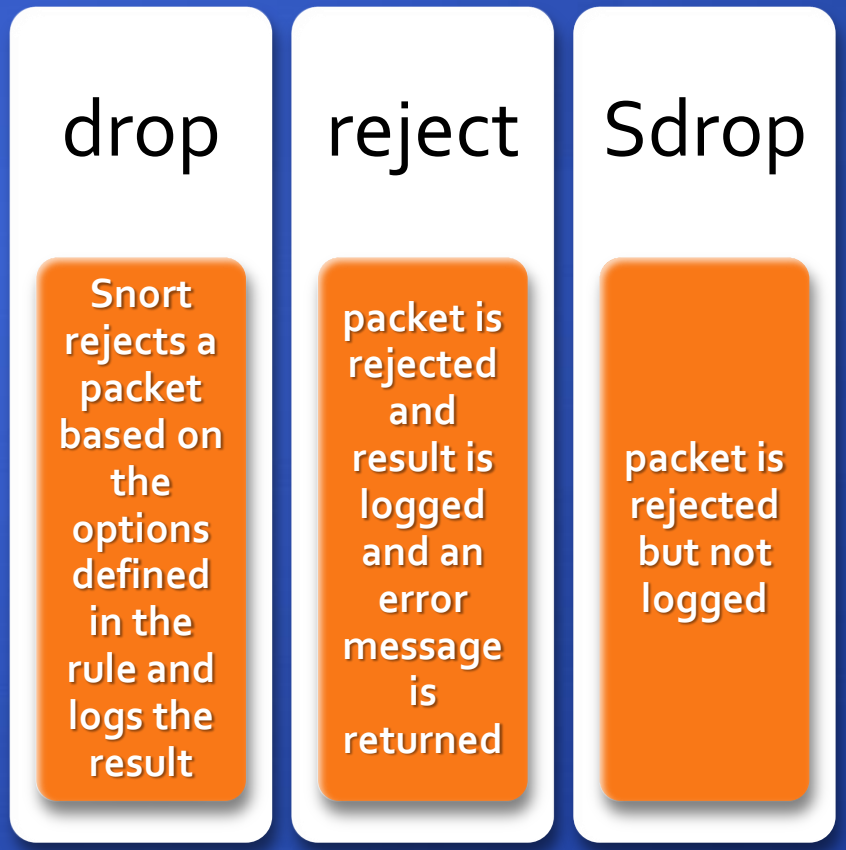
- the various tools work closely together
- threat prevention is more comprehensive
- management is easier

Network-Based IPS (NIPS)

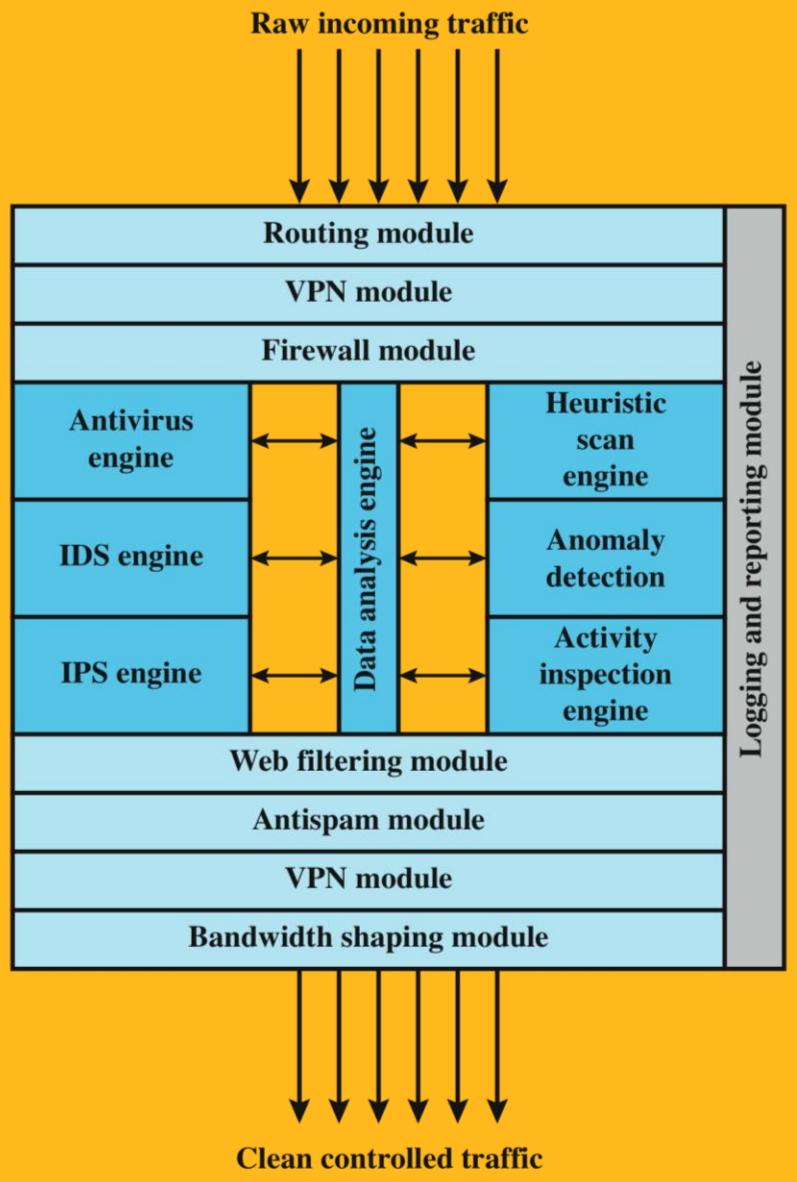
- inline NIDS with the authority to discard packets and tear down TCP connections
- uses signature and anomaly detection
- may provide flow data protection
  - monitoring full application flow content
- can identify malicious packets using:
  - pattern matching
  - stateful matching
  - protocol anomaly
  - traffic anomaly
  - statistical anomaly

Snort Inline

- enables Snort to function as an intrusion prevention capability
- includes a replace option which allows the Snort user to modify packets rather than drop them
  - useful for a honeypot implementation
  - attackers see the failure but can't figure out why it occurred



Unified Threat Management Products



Unified Threat Management Appliance (based on [JAME06])

Table 9.3

Sidewinder G2 Security Appliance Attack Protections Summary - Transport Level Examples

Attacks and Internet Threats		Protections	
TCP			
•Invalid port numbers •Invalid sequence •numbers •SYN floods •XMAS tree attacks •Invalid CRC values •Zero length •Random data as TCP •header	•TCP hijack attempts •TCP spoofing attacks •Small PMTU attacks •SYN attack •Script Kiddie attacks •Packet crafting: different TCP options set	•Enforce correct TCP flags •Enforce TCP header length •Ensures a proper 3-way handshake •Closes TCP session correctly •2 sessions, one on the inside and one on the outside •Enforce correct TCP flag usage •Manages TCP session timeouts •Blocks SYN attacks	•Reassembly of packets ensuring correctness •Properly handles TCP timeouts and retransmits timers •All TCP proxies are protected •Traffic Control through access lists •Drop TCP packets on ports not open •Proxies block packet crafting
UDP			
•Invalid UDP packets •Random UDP data to bypass rules	•Connection prediction •UDP port scanning	•Verify correct UDP packet •Drop UDP packets on ports not open	

Table 9.4

Sidewinder G2 Security Appliance Attack Protections Summary - Application Level Examples (page 1 of 2)

Attacks and Internet Threats	Protections
DNS	
Incorrect NXDOMAIN responses from AAAA queries could cause denial-of-service conditions.	•Does not allow negative caching •Prevents DNS Cache Poisoning
ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL.	•Sidewinder G2 prevents malicious use of improperly formed DNS messages to affect firewall operations. •Prevents DNS query attacks •Prevents DNS answer attacks
DNS information prevention and other DNS abuses.	•Prevent zone transfers and queries •True split DNS protect by Type Enforcement technology to allow public and private DNS zones. •Ability to turn off recursion
FTP	
•FTP bounce attack •PASS attack •FTP Port injection attacks •TCP segmentation attack	•Sidewinder G2 has the ability to filter FTP commands to prevent these attacks. •True network separation prevents segmentation attacks.
SQL	
SQL Net man in the middle attacks	•Smart proxy protected by Type Enforcement Technology •Hide Internal DB through nontransparent connections
Real-Time Streaming Protocol (RTSP)	
•Buffer overflow •Denial of service	•Smart proxy protected by Type Enforcement technology •Protocol validation •Denies multicast traffic •Checks setup and teardown methods •Verifies PNG and RTSP protocol, discards all others •Auxiliary port monitoring
SNMP	
•SNMP flood attacks •Default community attack •Brute force attack •SNMP put attack	•Filter SNMP version traffic 1, 2c •Filter Read, Write, and Notify messages •Filter OIDs •Filter PDU (Protocol Data Unit)

Table 9.4

Sidewinder G2 Security Appliance Attack Protections Summary - Application Level Examples (page 2 of 2)

SSH	
•Challenge-Response buffer overflows •SSHD allows users to override "Allowed Authentications" •OpenSSH buffer_append_space buffer overflow •OpenSSH/PAM challenge Response buffer overflow •OpenSSH channel code offer-by-one	Sidewinder G2 v6.x's embedded Type Enforcement technology strictly limits the capabilities of Secure Computing's modified versions of the OpenSSH daemon code.

SMTP			
•Sendmail buffer overflows •Sendmail denial of service attacks •Remote buffer overflow in sendmail	•Sendmail address parsing buffer overflow •SMTP protocol anomalies	•Split Sendmail architecture protected by Type Enforcement technology •Sendmail customized for controls	•Prevents buffer overflows through Type Enforcement technology •Sendmail checks SMTP protocol anomalies
•SMTP worm attacks •SMTP mail flooding •Relay attacks •Viruses, Trojans, worms	•E-mail Addressing spoofing •MIME attacks •Phishing e-mails	•Protocol validation •Anti-spam filter •Mail filters – size, keyword •Signature antivirus	•Anti-relay •MIME/Antivirus filter •Firewall antivirus •Anti-phishing through virus scanning

Spyware Applications		
•Adware used for collecting information for marketing purposes •Stalking horses •Trojan horses	•Malware •Backdoor Santas	•SmartFilter® URL filtering capability built in with Sidewinder G2 can be configured to filter Spyware URLs, preventing downloads.

Summary

- firewalls
  - need for
  - characteristics of
  - techniques
  - capabilities/limitations
- types of firewalls
  - packet filtering firewall
  - stateful inspection firewalls
  - application proxy firewall
  - circuit level proxy firewall
- bastion host
- host-based firewall
- personal firewall
- firewall location and configurations
  - DMZ networks
  - virtual private networks
  - distributed firewalls
- intrusion prevention systems (IPS)
- host-based IPS (HIPS)
- network-based IPS (NIPS)
- Snort Inline
- UTM products