Introduction to Computer Security

Chapter 9: Firewalls and Intrusion Prevention Systems

Chi-Yu Li (2020 Spring)
Computer Science Department
National Chiao Tung University

The Need for Firewalls

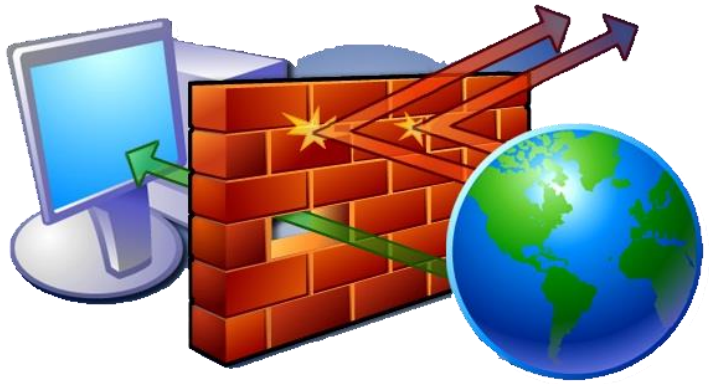
- Internet connectivity is essential
  - Threats: enabling the outside world to reach and interact with local network assets
- Why not just equip each workstation/server with strong security features?
  - Not sufficient; Not cost-effective
  - e.g., a security flow is discovered: each potentially affected system must be upgraded
    - The network may contain various OSes
    - Needs: scalable configuration management and aggressive patching
- A single choke point between the protected network and the Internet
  - Complement to host-based security services
  - Imposing security and auditing against Internet-based attacks
  - A single computer system or a set of two or more systems working together

Outline

- Firewall characteristics and access policy
- Types of firewalls
- Firewall basing
- Firewall location and configurations
- Intrusion prevention systems
- Example: Unified Threat Management Products

Firewall Characteristics

- Design goals
  - All traffic from inside to outside, and vice versa, 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



Firewall Access Policy

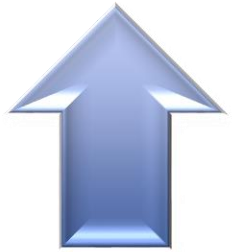
- A critical component in the planning and implementation: specifying a **suitable access policy**
  - Listing the types of traffic authorized
  - Being developed from the organization's information security risk assessment and policy

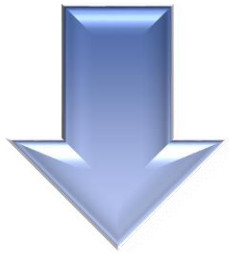
Characteristics for Control Access

- IP address and protocol values
  - Used by: packet filter and stateful inspection firewalls
  - Limiting access to specific services
- Application protocol
  - Used by: an app-level gateway
  - Relaying and monitoring the exchange of information for specific app protocols
    - e.g., checking SMTP email for spam
- User identity
  - Identifying inside users using secure authentication technology, e.g., IPSec
- Network activity
  - Considering time or request, e.g., only in business hours
  - Rate of requests or other activity patterns, e.g., detecting scanning attempts

Capabilities and Limitations

- Capabilities
  - A single choke point: keeping unauthorized traffic out and simplifying management
  - A location for monitoring security-related events
  - A convenient platform for Internet functions, e.g., NAT
  - The platform for IPSec: implementing VPN

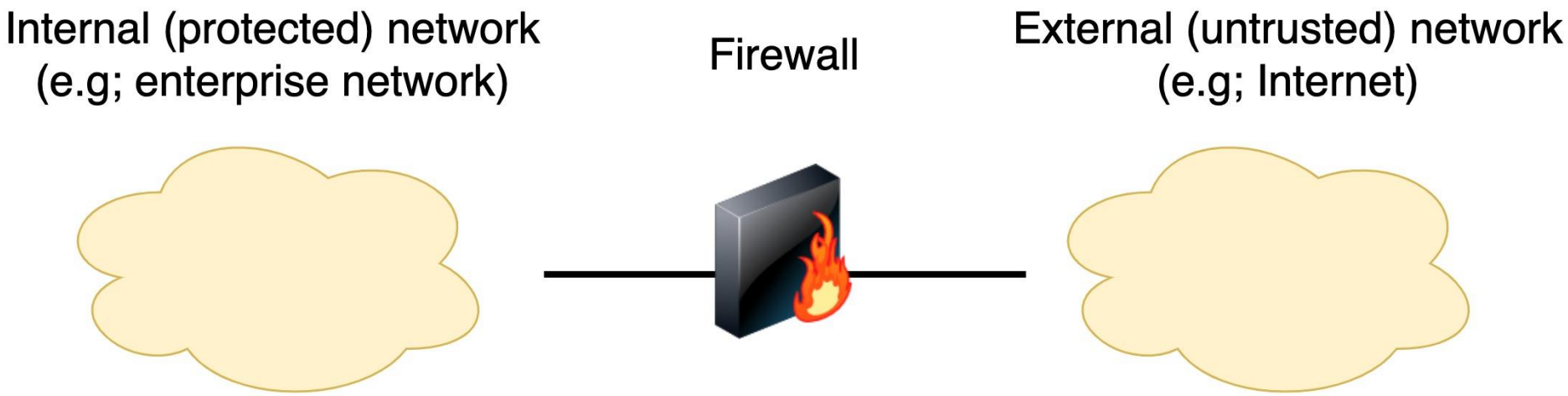




- Limitations
  - Cannot protect against attacks bypassing the firewall
  - May not protect fully against internal threats
  - An improperly secured wireless LAN may be accessed from outside
  - Devices infected outside are attached and used internally

Types of Firewalls

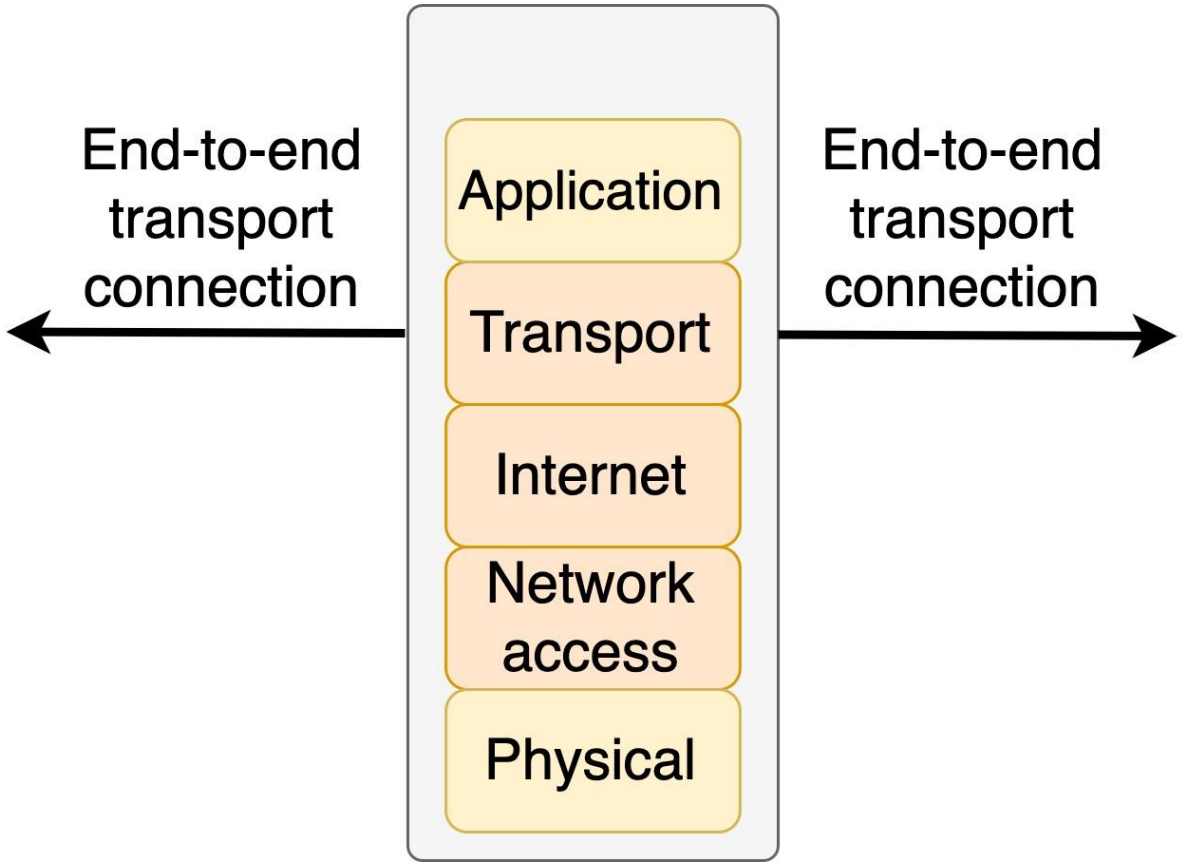
- General model



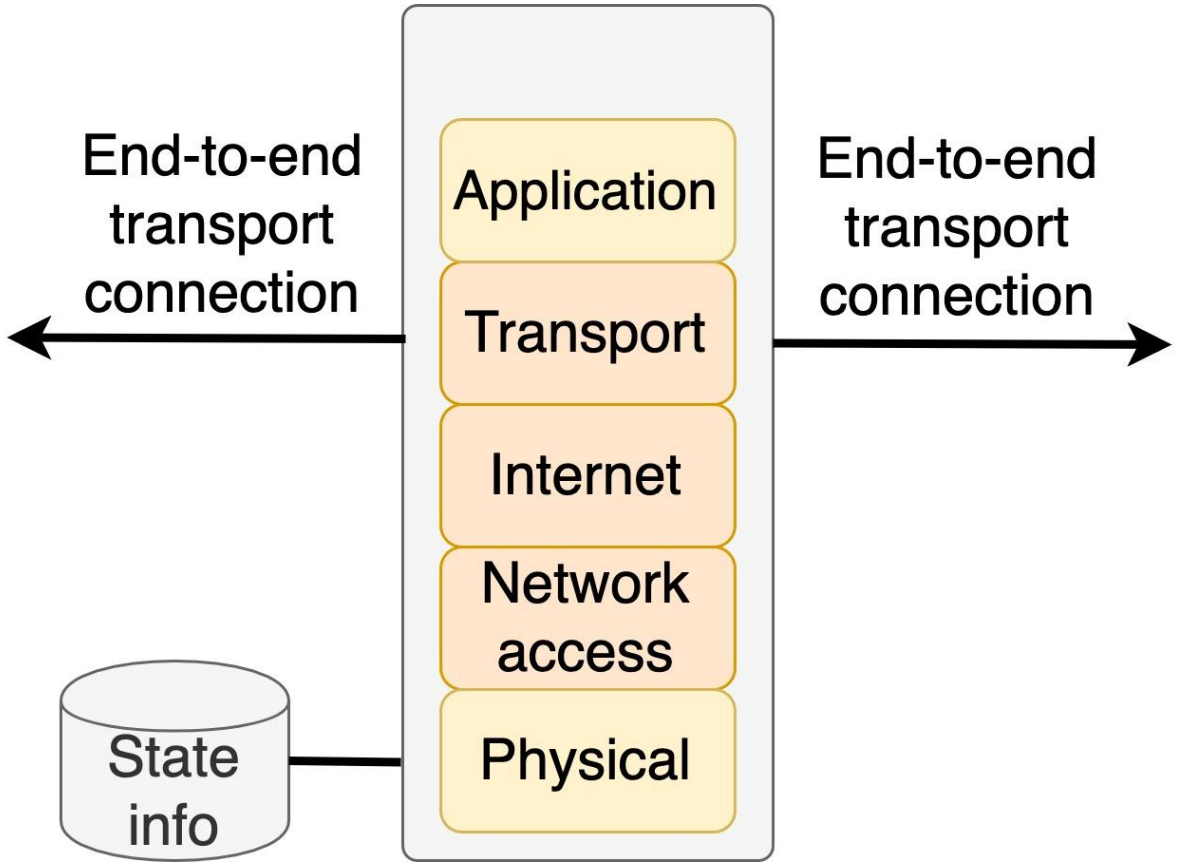
- Four major types
  - Packet filtering firewall
  - Stateful inspection firewall
  - Application proxy firewall
  - Circuit-level proxy firewall

Packet Filtering and Stateful Inspection Firewalls

Packet Filtering Firewall



Stateful Inspection Firewall



Packet Filtering Firewall

- Applying a set of rules to each incoming and outgoing IP packet
  - Rules based on matches in the IP or TCP header for packets in both directions
  - Matches: determining whether to forward or discard the packet
  - No match: a default action is taken
    - Discard: prohibit unless expressly permitted ➔ More conservative, controlled, visible to users
    - Forward: permit unless expressly prohibited ➔ Easier to manage and use but less secure

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

Packet Filtering Example

- Goal: allowing inbound and outbound email traffic but to block all other traffic
  - SMTP with port 25

Rule	Direction	Src address	Dest address	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

What problems exist in this rule set?

Packet Filtering Example (Cont.)

- Problem 1: Rule 4 allows external traffic to any destination port above 1023
- Problem 2: New Rule 4 allows an outside machine to send packets with source port 25 to internal machines
  - Intention of Rules 3 and 4: any inside host can send mail to the outside

Rule	Direction	Src address	Dest address	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filtering: Pros and Cons

- Pros
  - Simplicity
  - Transparent to users and are very fast
- Cons
  - Cannot prevent attacks that employ app specific vulnerabilities or functions
  - Limited logging functionality
  - Don’t support advanced user authentication, due to the lack of upper-layer functionality
  - Vulnerable to attacks on TCP/IP protocol issues
  - Susceptible to security breaches caused by improper configurations

Packet Filtering: Possible Attacks

- IP address spoofing
  - Attacker transmits packets from the outside with a source IP address of an internal host
  - Countermeasure: discarding incoming packets with an inside source address
- Source routing attacks
  - Attacker specifies the route that a packet should take
  - Countermeasure: discarding all packets that use this option
- Tiny fragment attacks
  - Attacker uses the IP fragmentation option to create extremely small fragments and force the TCP header info into a separate packet fragment
    - Circumventing filtering rules that depend on TCP header information
  - Countermeasure: enforcing the first fragment of a packet to contain a predefined minimum amount of the transport header

Traditional Packet Filtering: Weakness

- Making decisions on an individual packet basis
  - Doesn't take into consideration any higher-layer context
- Must permit inbound network traffic on all the ports ($\geqq$ 1024) for TCP-based traffic
  - Server port: < 1024 (well-known)
  - Client port: 1024 ~ 65535 ← a vulnerability

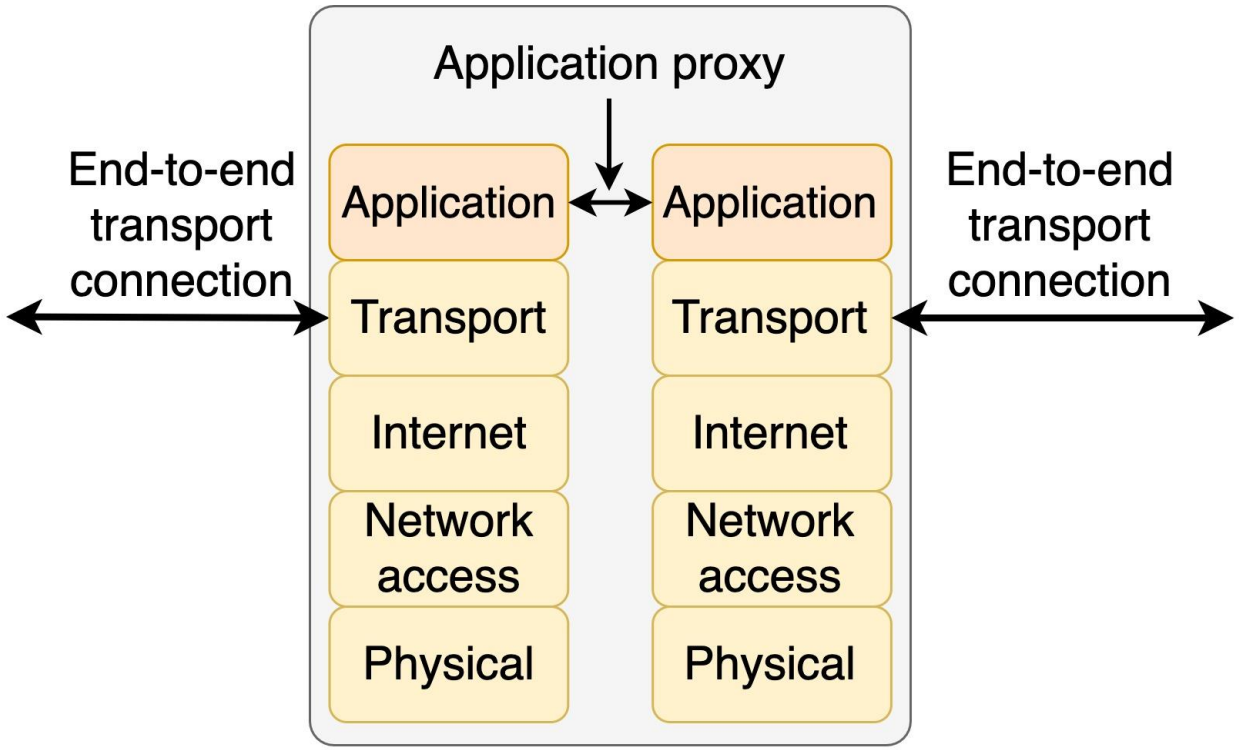
Stateful Inspection Firewalls

- Tightening rules for TCP traffic by creating a directory of outbound TCP connections
  - An entry for each currently established connection
  - Allowing incoming traffic to high numbered ports only for those entries
  - Keeping track of TCP sequence numbers
    - Preventing session hijacking attacks
- Some even inspect other protocols (FTP, SIPS, et.)

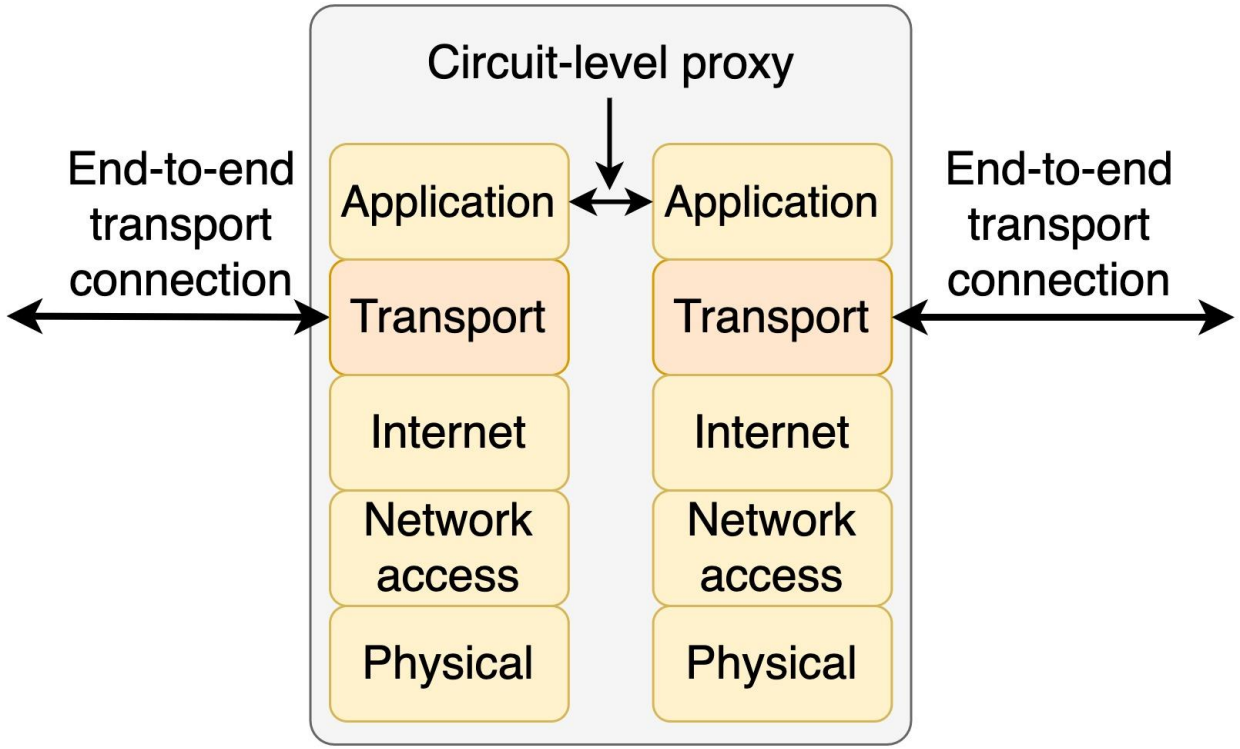
Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	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

Application and Circuit-level Proxy Firewalls

Application Proxy Firewall



Circuit-level Proxy Firewall



Application Proxy Firewall

- A relay of app-level traffic: an app proxy
  - User contacts it using a TCP/IP app (e.g., Telnet or FTP)
  - It contacts app on remote host and relays TCP segments between two ends
    - Two spliced connections
  - Must have proxy codes for specific apps
  - May restrict supported app features
- Pros: more secure than packet filters
  - Doesn’t rely on possible combinations at the TCP and IP level
- Cons: additional processing overhead on each connection

Circuit-level Proxy Firewall

- Splitting a TCP connection
  - Two TCP connections
    - One between itself and a TCP insider
    - One between itself and a TCP outsider
  - Relaying TCP segments from one connection to the other
  - Doesn't examine the contents
- Security: determining which connections are allowed
  - Typically used when inside users are trusted
- To reduce the overhead of the app-level proxy firewall
  - Inbound: app-level proxy firewall, outbound: circuit-level proxy

SOCKS: Circuit-level Gateway

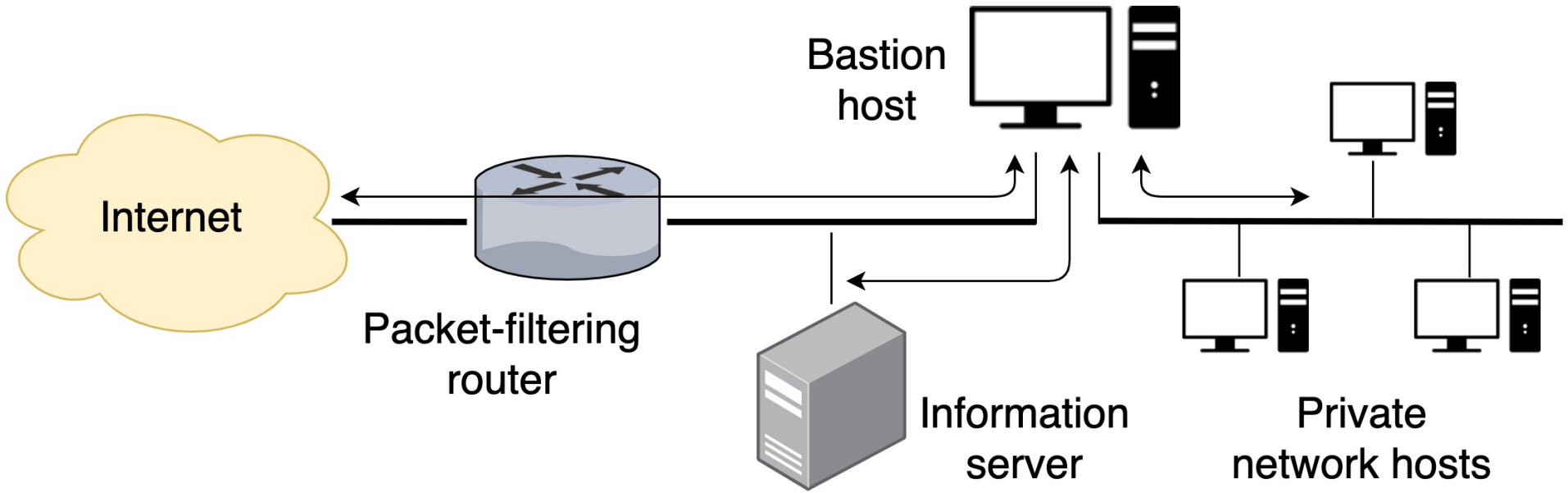
- A framework for client-server apps in TCP/UDP domains to conveniently and securely use the services of a network firewall
  - Client app contacts SOCKS server, authenticates, and sends a relay request
  - SOCKs server evaluates the request
    - Either establishes a connection or denies it
- Three components
  - SOCKS server: often running on a UNIX-based firewall; also on Windows
  - SOCKS client library: running on internal hosts protected by the firewall
  - SOCKS-ified versions of programs (e.g., FTP, TELNET)

Firewall Basing

- Stand-alone firewall (bastion host)
- Host-based (Server-based) firewall
- Personal firewall

Bastion Host

- A system identified by the firewall administrator as a critical strong point in the network's security
  - Serving as a platform for an app-level or circuit-level gateway



Bastion Hosts: Common Characteristics

- Running secure OS, only essential services ➔ a hardened system
- May require user authentication to access proxy or host
- Each proxy
  - Can restrict features, hosts accessed
  - Small, simple, checked for security
  - Independent, non-privileged
  - Limited disk use, hence read-only code

Host-based (Server-based) Firewalls

- Software modules: used to secure an individual host
  - Available in many OSes: add-on packages
  - Filtering and restricting the flow of packets
  - Common location: a server
- Pros
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of topology
  - Providing an additional layer of protection
    - Used in conjunction with stand-alone firewalls

Personal Firewalls

- Software modules on the personal computers
  - For both home and corporate uses
  - Can be housed in a router that connects all of the home computers
  - Much less complex than server-based and stand-alone firewalls
- Primary role: to deny unauthorized remote access
  - Can also monitor outgoing activity ➔ worms and other malware
- Practice
  - Linux: the *netfilter* package
  - Mac OS X: the *pf* package
  - All inbound connections are denied except for those the user explicitly permits
  - Outbound connections are usually allowed

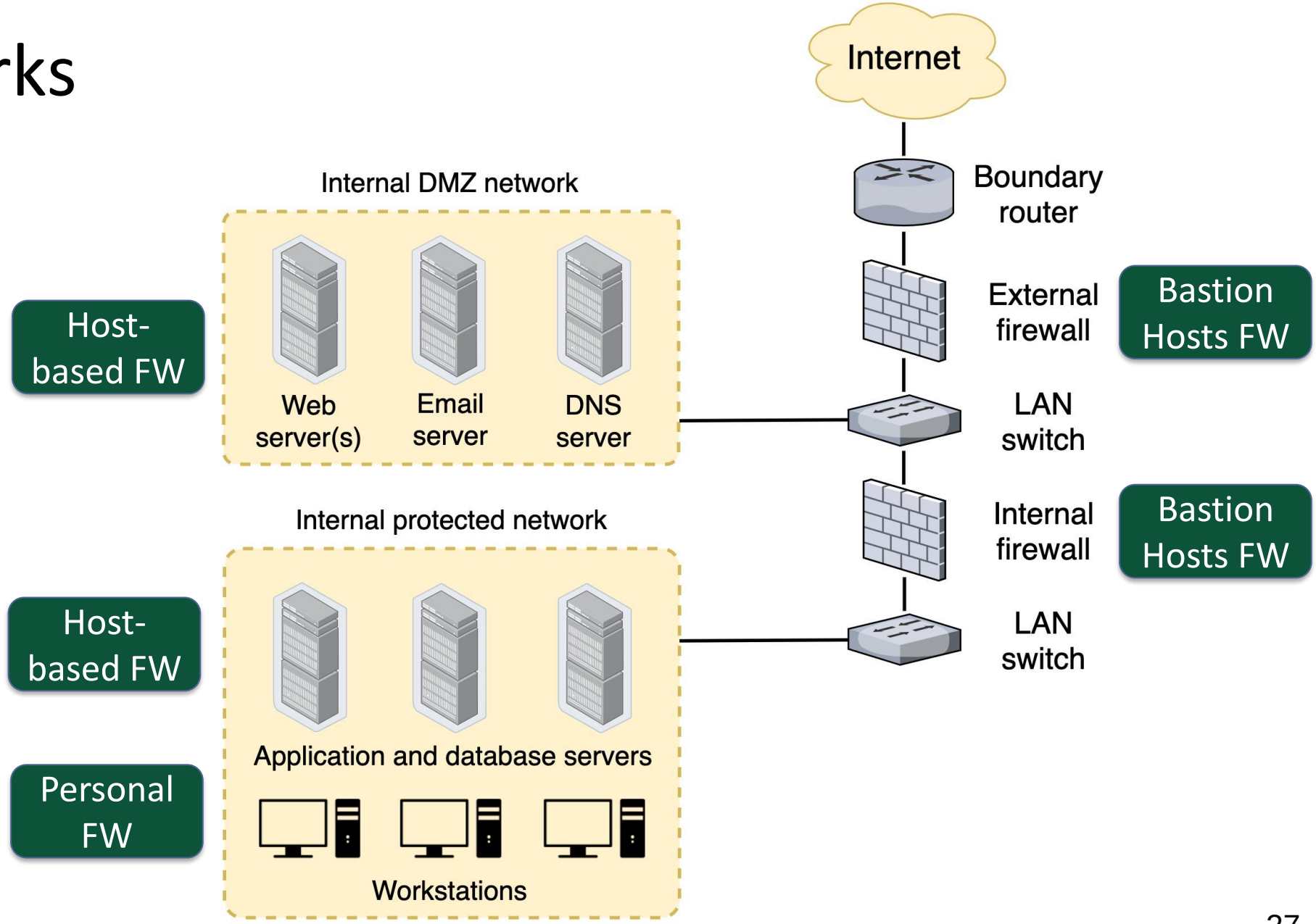
Firewall Location and Configurations

- DMZ networks
- Virtual private networks
- Distributed firewalls
- Summary of firewall locations and topologies

DMZ Networks

DMZ (Demilitarized Zone): A small network isolated from the private network.

Systems (e.g., a Web site) located on DMZ networks: externally accessible but need some protections

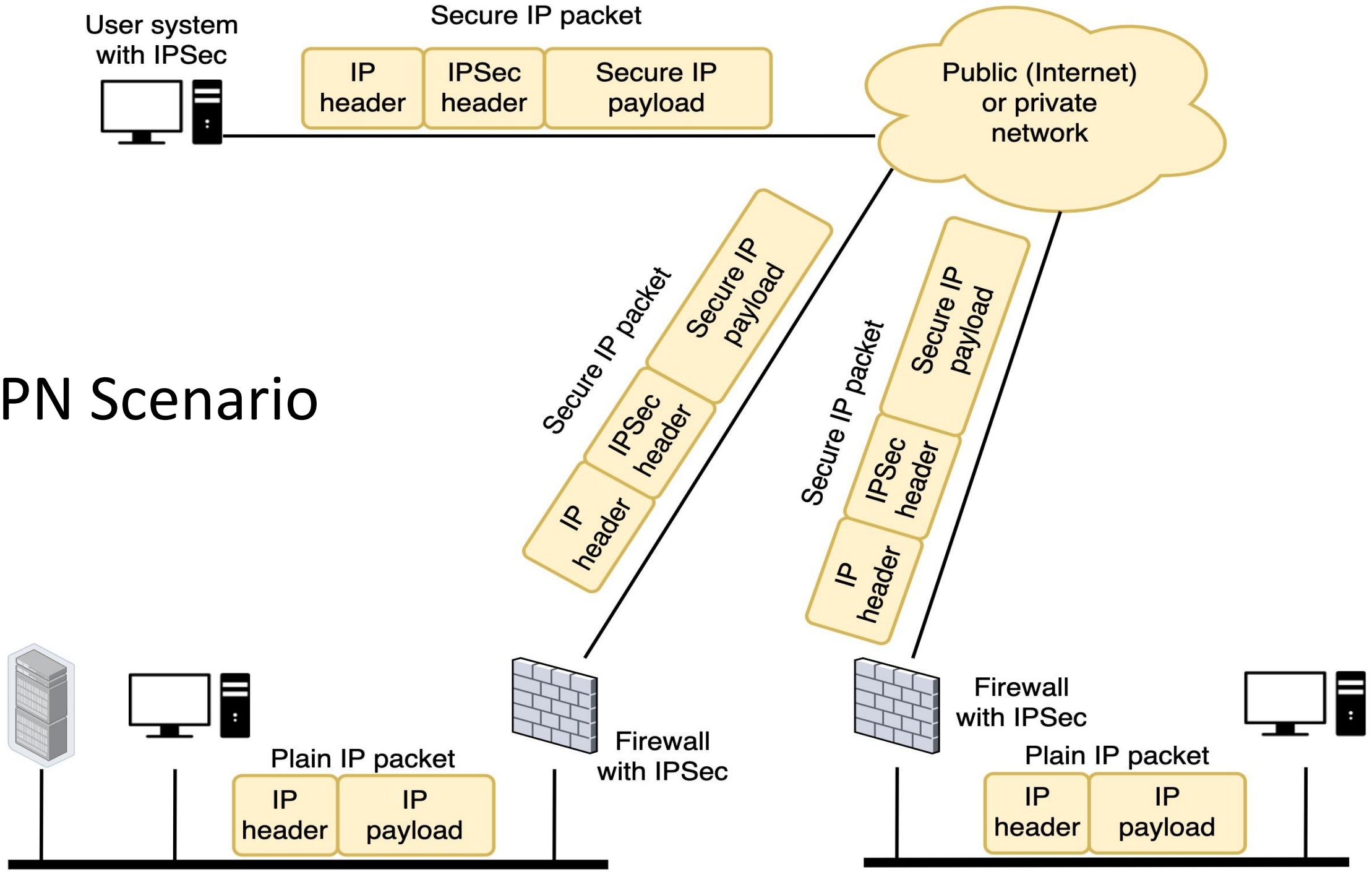


Virtual Private Networks (VPN)

- Containing a set of computers
  - Interconnecting by means of a relatively unsecure network
  - Making use of encryption and special protocols to provide security

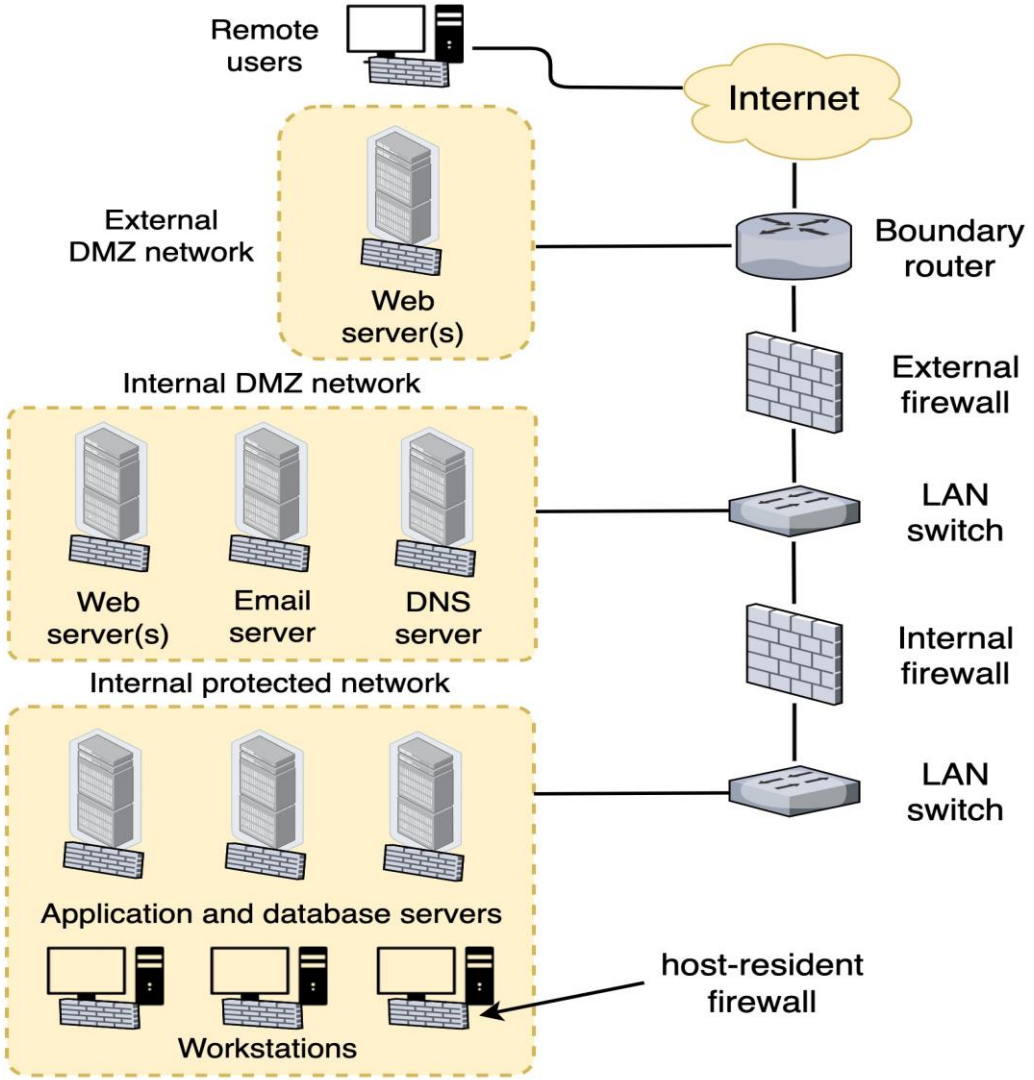
- Using encryption and authentication in the lower protocol layers to provide a secure connection through an insecure network
  - Most common protocol at the IP level: IPSec (Internet Protocol Security)

VPN Scenario



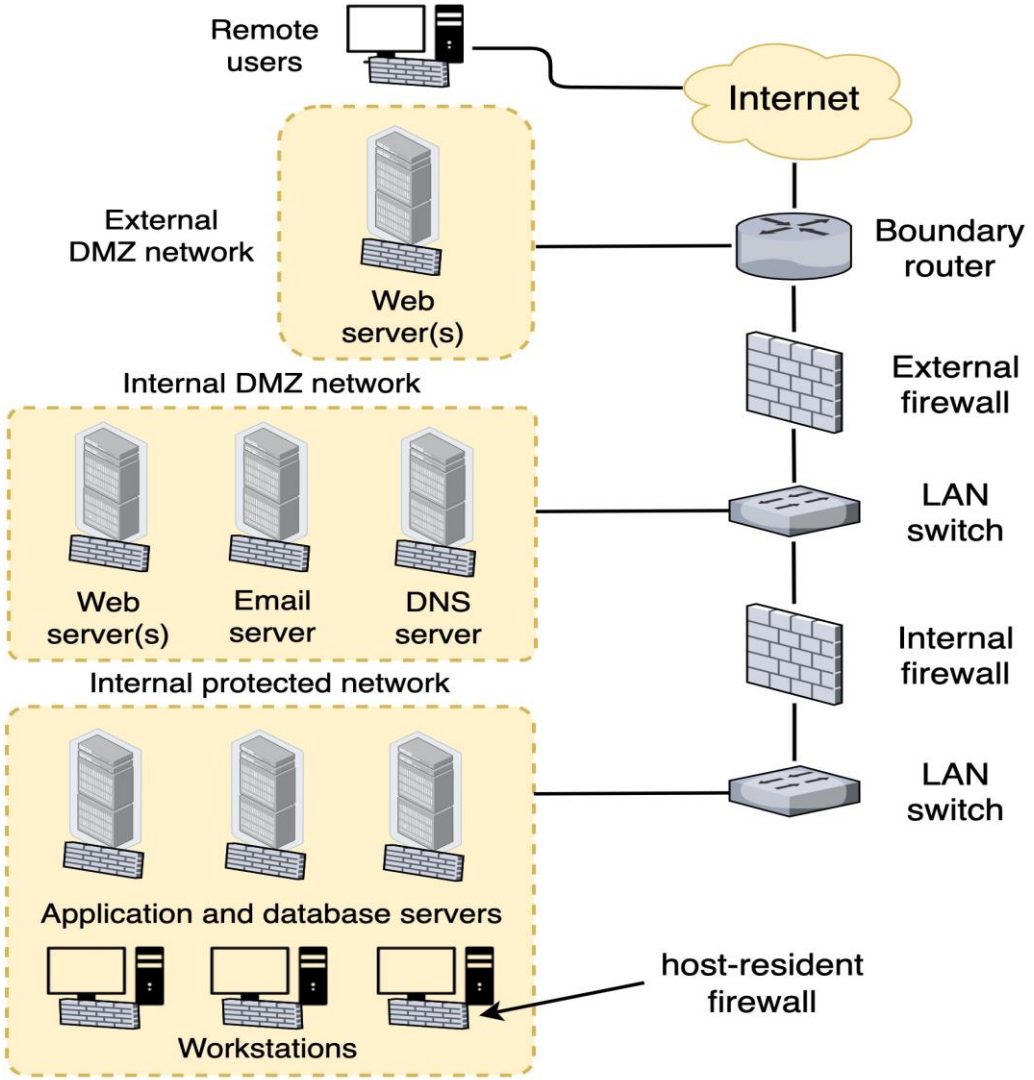
Distributed Firewalls

- Local protection: against internal attacks
  - Tailored to specific machines and apps
  - Host-based firewalls on hundreds of servers and workstation
  - Personal firewalls on local and remote user systems
- Global protection: against internal and external attacks
  - Stand-alone firewalls

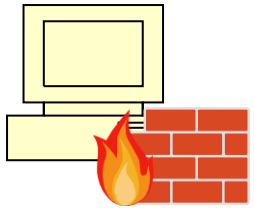


Distributed Firewalls (Cont.)

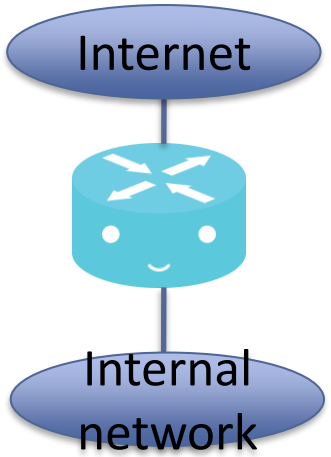
- May use both an internal and external DMZ
- External DMZ: less protection
  - e.g., Web servers
    - Have less critical information
    - Protected by host-based firewalls
- Security monitoring is also needed
  - log aggregation and analysis, firewall statistics, etc.



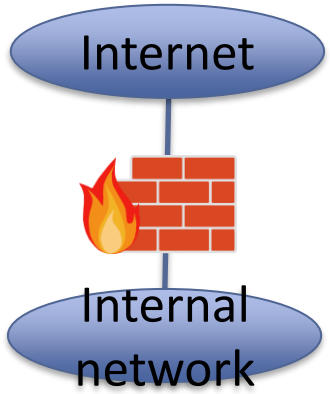
Summary of Firewall Locations and Topologies



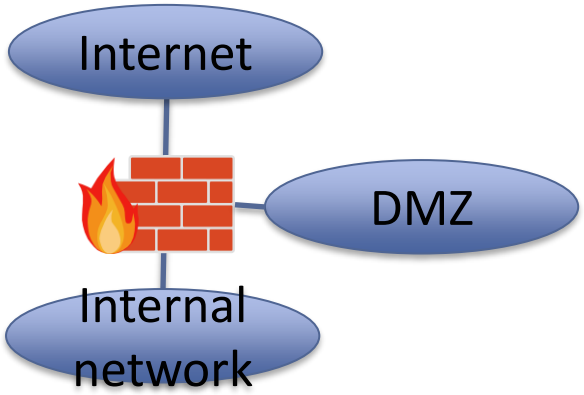
Host-resident firewall



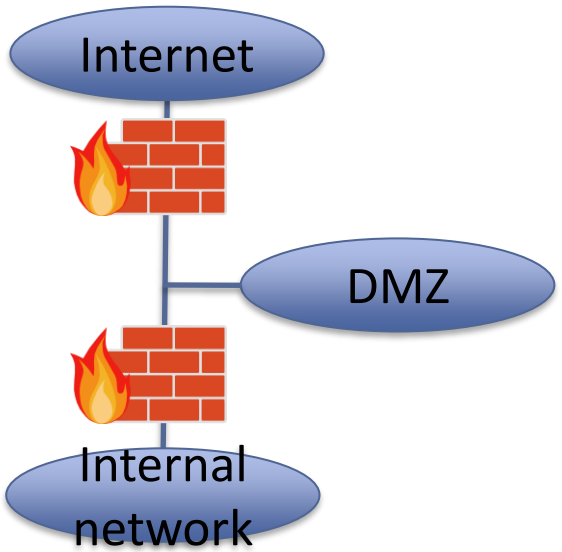
Screening router



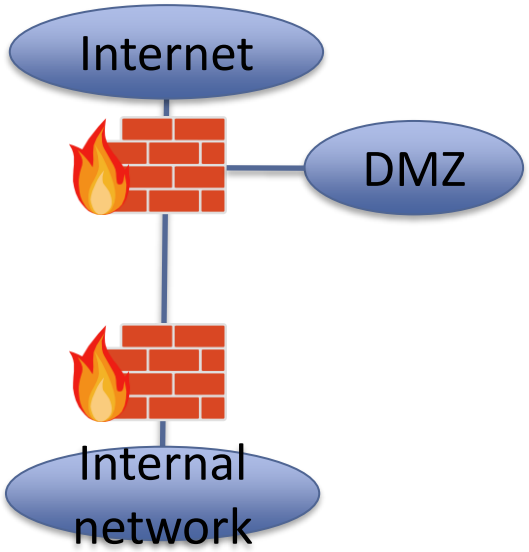
Single bastion inline



Single bastion T



Double bastion inline



Double bastion T

Intrusion Prevention System (IPS)

- An extension of an IDS: block or prevent detected malicious activity

- Like an IDS
  - Types: host-based, network-based, or distributed/hybrid
  - Approaches: anomaly detection, or signature/heuristic detection

Host-based IPS (HIPS)

- Anomaly detection
  - Behavior patterns that indicate malware
  - Or, not that of legitimate users
- Signature/heuristic detection
  - Specific content of app network traffic, sequences of system calls, etc.
  - Patterns that have been identified as malicious
- Examples of the types of malicious behavior addressed by a HIPS
  - Modification of system resources: Rootkits, Trojan horses, and backdoors
  - Privilege-escalation exploits
  - Buffer-overflow exploits
  - Access to e-mail contact list: many worms spread by mailing a copy of themselves
  - Directory traversal: hackers traverse directory and access files against Web servers

HIPS (Cont.)

- Capability can be tailored to the specific platform
  - General-purpose tools for a desktop or server system
  - Protection for specific types of servers: e.g., Web and database servers
- Alternative solution: a sandbox approach
  - Suited to mobile code, e.g., Java applets and scripting languages
  - Quarantining such code in an isolated system area
- Areas for desktop protection
  - System calls, file system access, system registry settings, host input/output

The Role of HIPS

- The main target for hackers and criminals: enterprise point
  - Including desktop and laptop systems
  - More popular than network devices to be attacked
- Security vendors focus more on the endpoint security products
  - An integrated, single-product suit of functions
    - E.g., antivirus, antispyware, antispam, and personal firewalls
- Pros: various tools work closely together
  - Threat prevention is more comprehensive
  - Management is easier

If HIPS is sophisticated enough, can we get rid of network-level devices?

Security Practice: Defense in Depth (DiD)

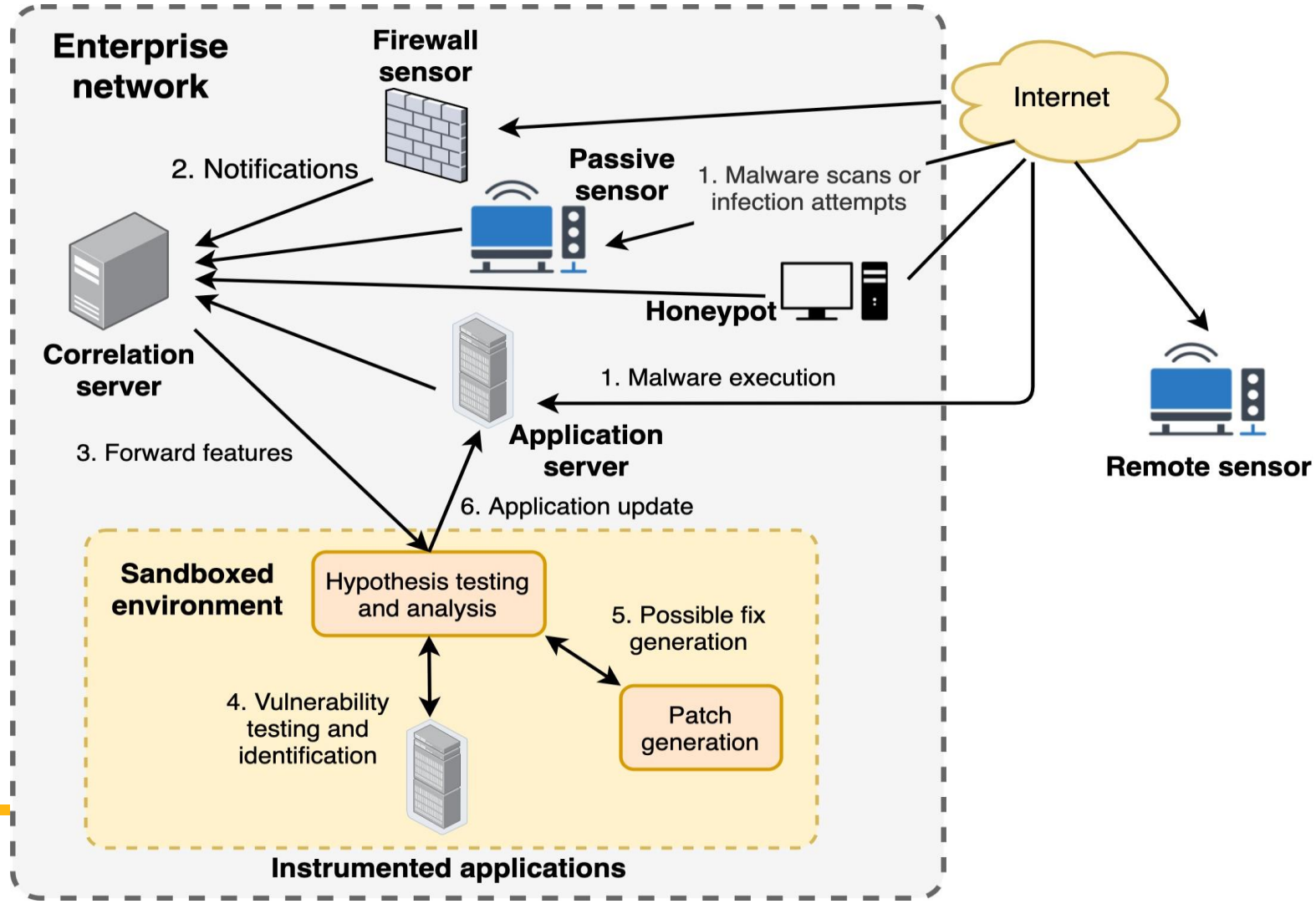
- A series of defensive mechanisms are layered to protect valuable data and information
  - Multi-layered approach with intentional redundancies
  - If one mechanism fails, another steps up immediately to thwart an attack
- Using HIPS as one element in a DiD strategy
  - Together with network-level devices, e.g., firewalls and network-based IPS

Network-based IPS (NIPS)

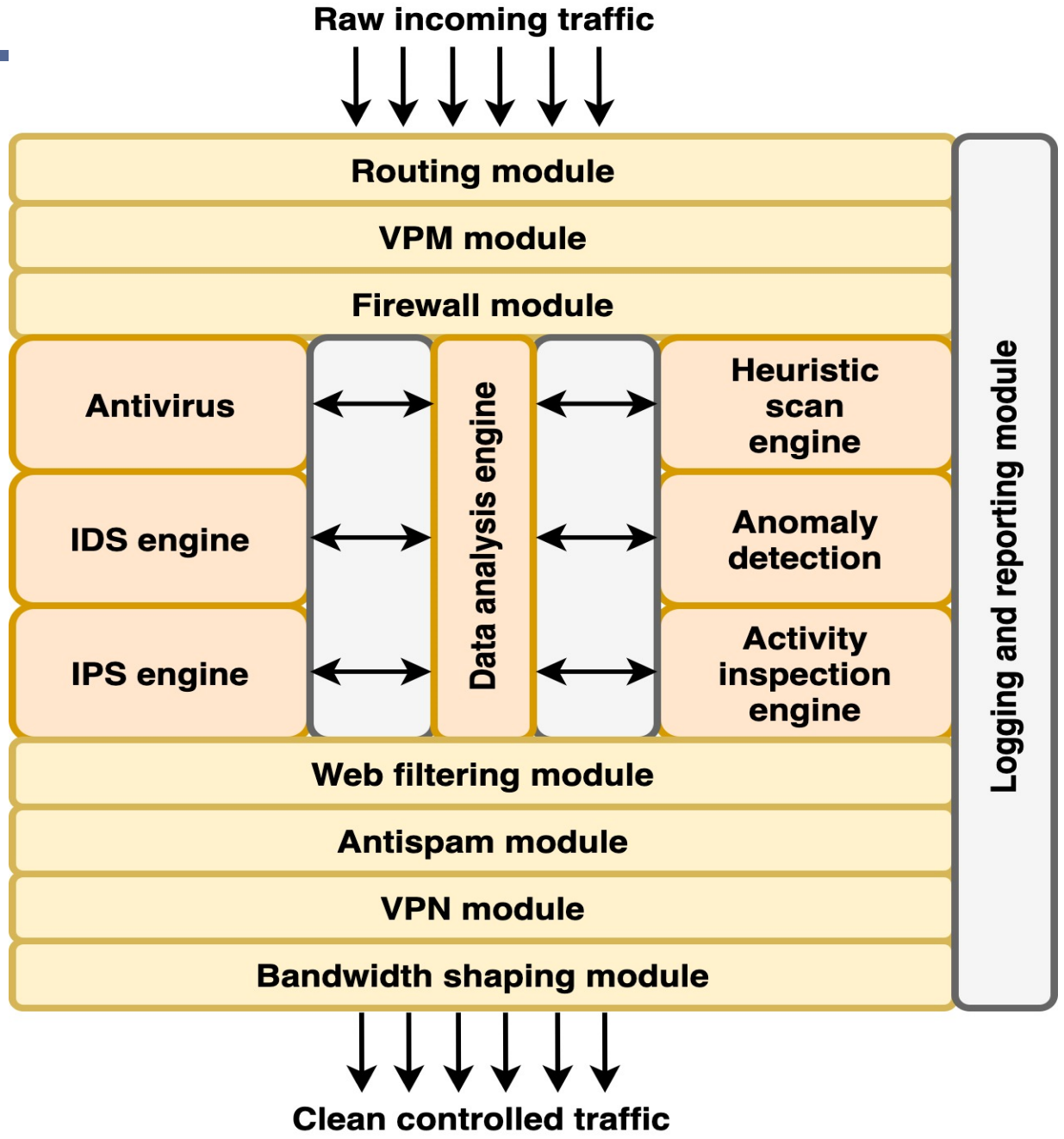
- Inline with NIDS: modifying or discarding packets and tearing down TCP connections
  - Approaches: anomaly detection, or signature/heuristic detection
- Typical methods used by a NIPS device to identify malicious packets
  - Pattern matching: e.g., specific byte sequences (the signature)
  - Stateful matching: attack signatures in the context of a traffic stream
  - Protocol anomaly: deviation from standards set in RFCs
  - Traffic anomaly
  - Statistical anomaly

Distributed or Hybrid IPS

- Example system: worms detection



Example: Unified Threat Management Appliance



www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.

Highlights

Compact, powerful, rack-mounted, and secure!

- **Multi-function UTM (Unified Threat Management) security appliance can replace five, six,**

Sidewinder G2 Security Appliance

Consolidating the widest variety of Internet security functions in one system

Sidewinder G2 Security Appliance

The Sidewinder G2® Security Appliance is the most comprehensive gateway security appliance in the world, with the strongest credentials of any leading all-in-one firewall or Unified Threat Management security appliance (as tracked by IDC). This market leading Internet security appliance delivers protections for your applications and networks against the entire threat matrix—*and* at Gigabit speeds. Our appliance consolidates the widest variety of gateway security functions in one system, reducing the complexity of managing a total perimeter security solution. These functions include our unprecedented Application Defenses™ firewall with embedded anti-virus, anti-spam, URL filtering, HTTPS/SSL accelerated termination, traffic anomaly detection, IDS/IPS, and a whole host of other critical protective features.

Sidewinder G2 includes the only firewall that has never had a CERT advisory posted against it in over 10 years—a truly remarkable accomplishment. It recently achieved the highest level of EAL4+ Common Criteria certification possible (far stronger than other vendors' EAL4 ratings). As a result, your Sidewinder G2 provides you with defense-in-depth protections against the entire threat matrix around the clock.

Application Defenses

Secure Computing's Application Defenses strategy is at the heart of the multi-layered defense-in-depth design of the Sidewinder G2 Security Appliance. The ability to face and defeat both known and unknown attacks is the strength of the Sidewinder G2 Application Defenses capabilities. This is achieved through a three-tiered defense-in-depth approach: 1) *Application awareness* ensures in-depth knowledge of a complete breadth of applications; 2) *Application control* enables granular policy controls on a per-rule basis; and 3) *Attack protection* provides in-depth detection of attacks from layer 3 through 7.

Sidewinder G2 Security Appliance Attack Protections Summary – Transport Level Examples

Full rack of Sidewinder G2 Security Appliance

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	

Sidewinder G2 Security Appliance Attack Protections Summary – Application Level Examples

Full rack of Sidewinder G2 Security Appliance

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)

Sidewinder G2 Security Appliance Attack Protections Summary – Application Level Examples (Cont.)

Full rack of Sidewinder G2 Security Appliance

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.

Questions?