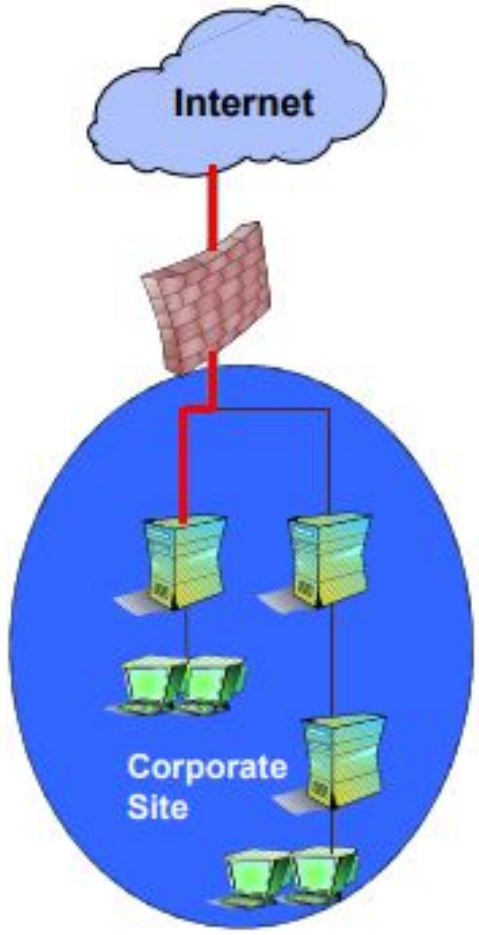
Firewalls & Network Defense

Day 1: Firewall Fundamentals

What Is a Firewall?

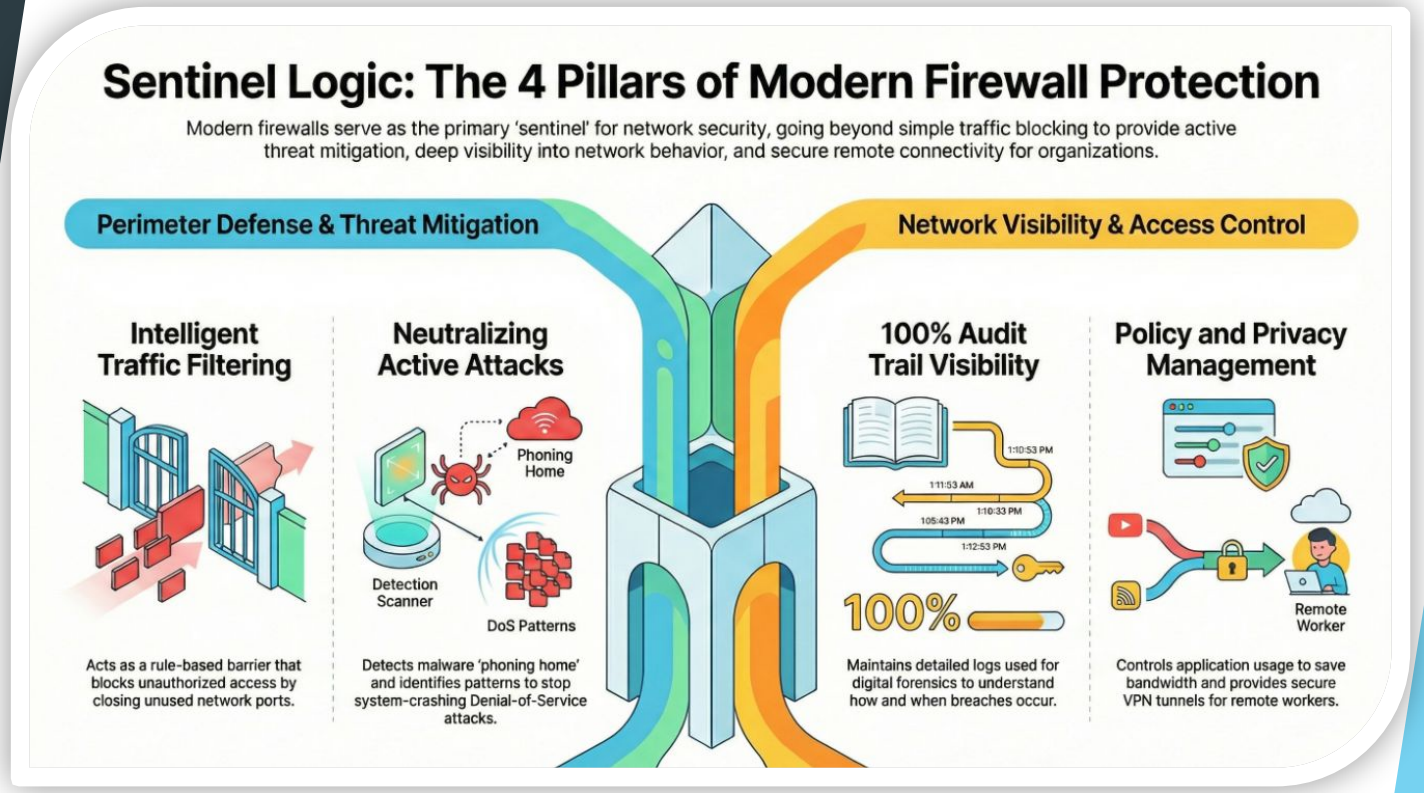
Your Digital Security Guard

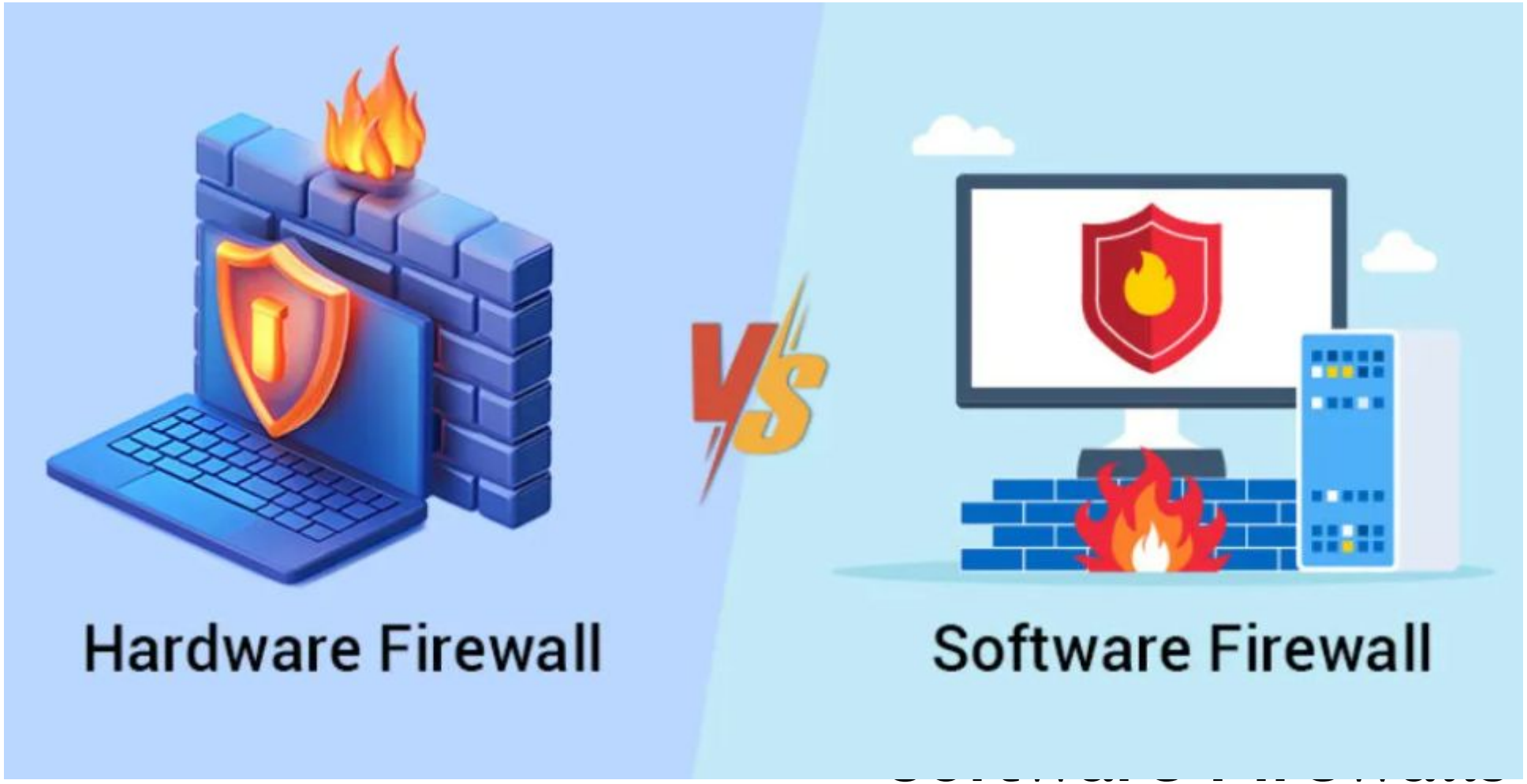
- Acts as a security gateway between two networks
- Tracks and controls network communications.
  - Decides whether to pass, reject, encrypt, or log communications (Access Control)



Why Are Firewalls Needed?

- Protection Against Malware.
- Safeguarding Sensitive Data.
- Maintaining System Integrity.





Protect an entire network ◦
Implemented on the router level ◦
Usually more expensive, harder to configure

Protect a single computer ◦
Usually less expensive, easier to configure

Host-Based vs. Network Firewalls

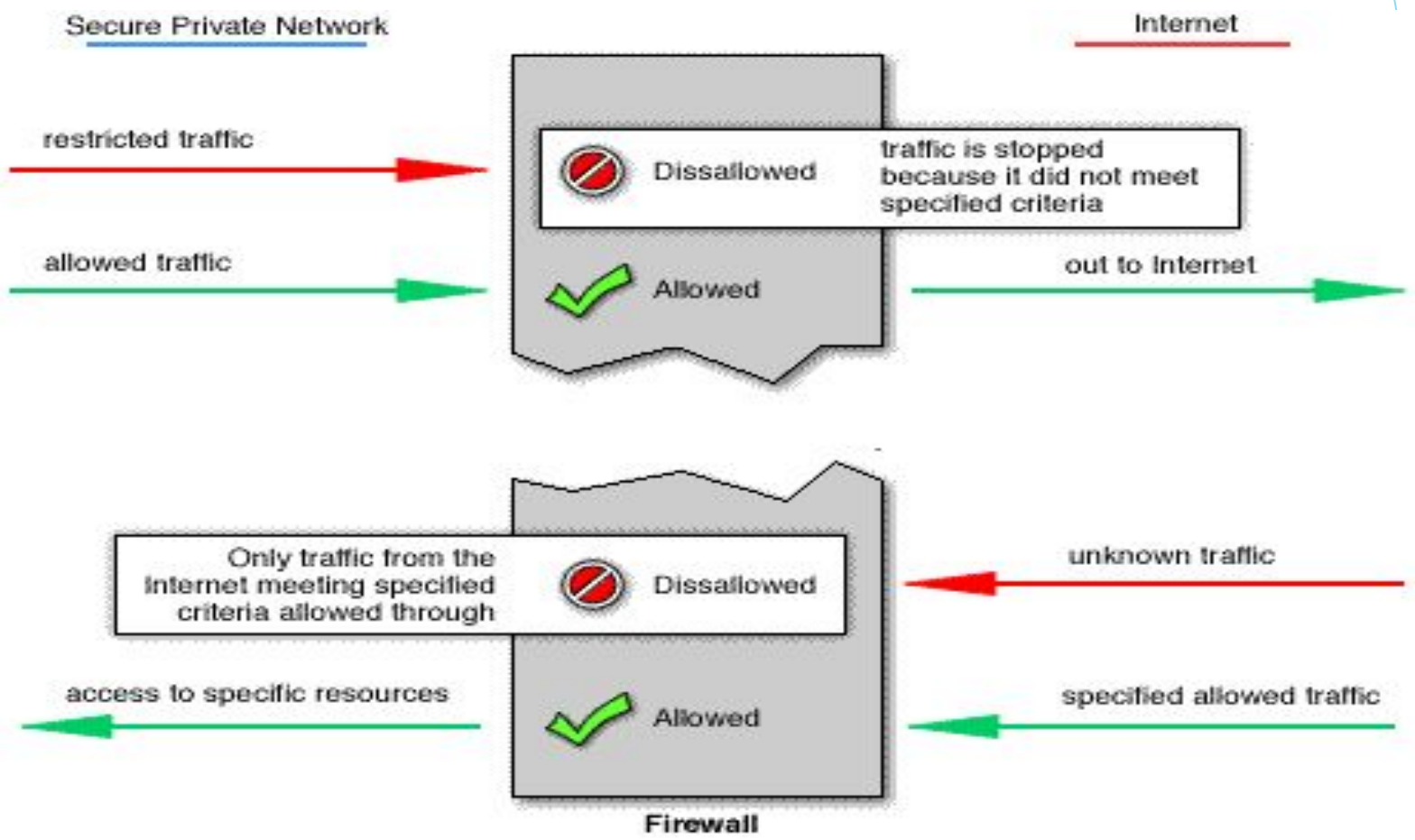
Host-Based Firewall

- Installed on **individual computers**.
- Protects **one device only**, providing a granular layer of security for that specific machine.
- Examples include Windows Defender Firewall for Windows systems and iptables/ufw on Linux distributions.

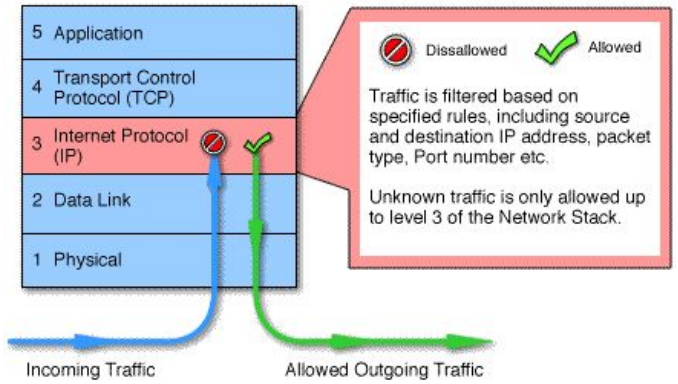
Network Firewall

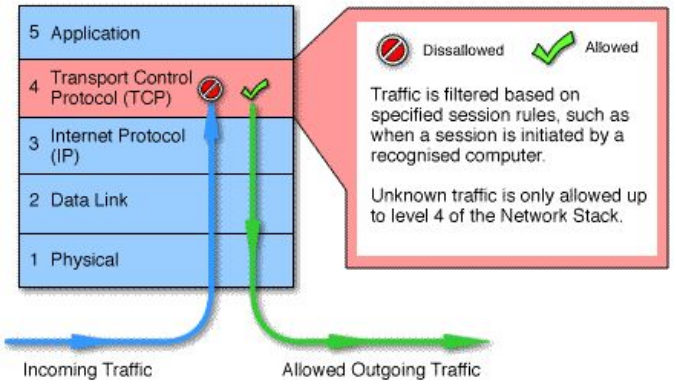
- Installed on a **network device**, typically at the perimeter of a network.
- Protects **all devices on the network**, acting as a centralized security checkpoint.
- Examples include pfSense, FortiGate, and Cisco Adaptive Security Appliance (ASA).

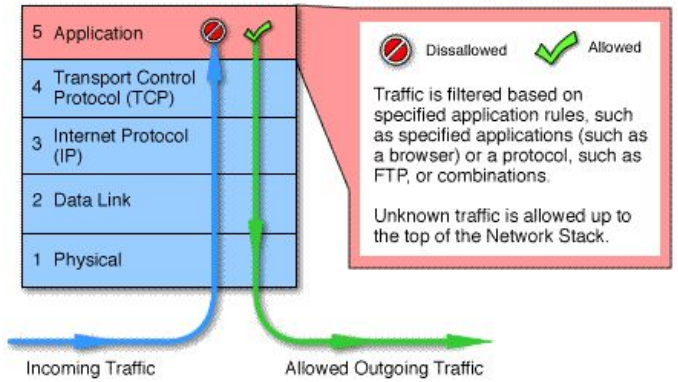
How It Works

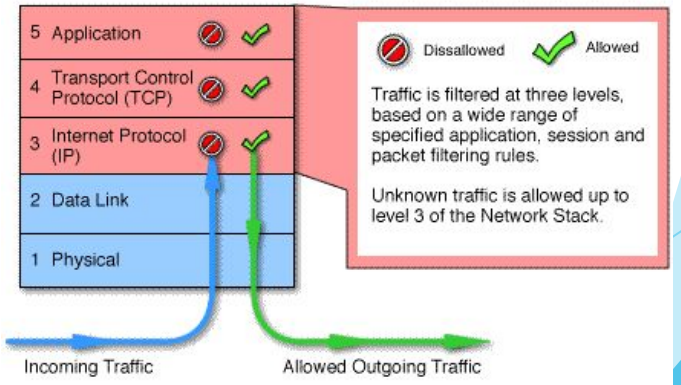

Secure Private Network
Internet
restricted traffic
Dissallowed
traffic is stopped
because it did not meet
specified criteria
allowed traffic
Allowed
out to Internet
Only traffic from the
internet meeting specified
criteria allowed through
Dissallowed
unknown traffic
access to specific resources
Allowed
specified allowed traffic
Firewall

Firewalls & the OSI









Classification /Types of Firewall

Characterized by protocol level it controls in

Packet filter	Circuit gateways	Application gateways

Combination of above is dynamic packet filter

The Four Generations of Firewall Evolution

1990s: Packet Filtering Firewalls

The first generation focused on basic packet filtering.

Early 2000s: Stateful Firewalls

The second generation introduced stateful traffic inspection.

2008: Next-Generation Firewalls

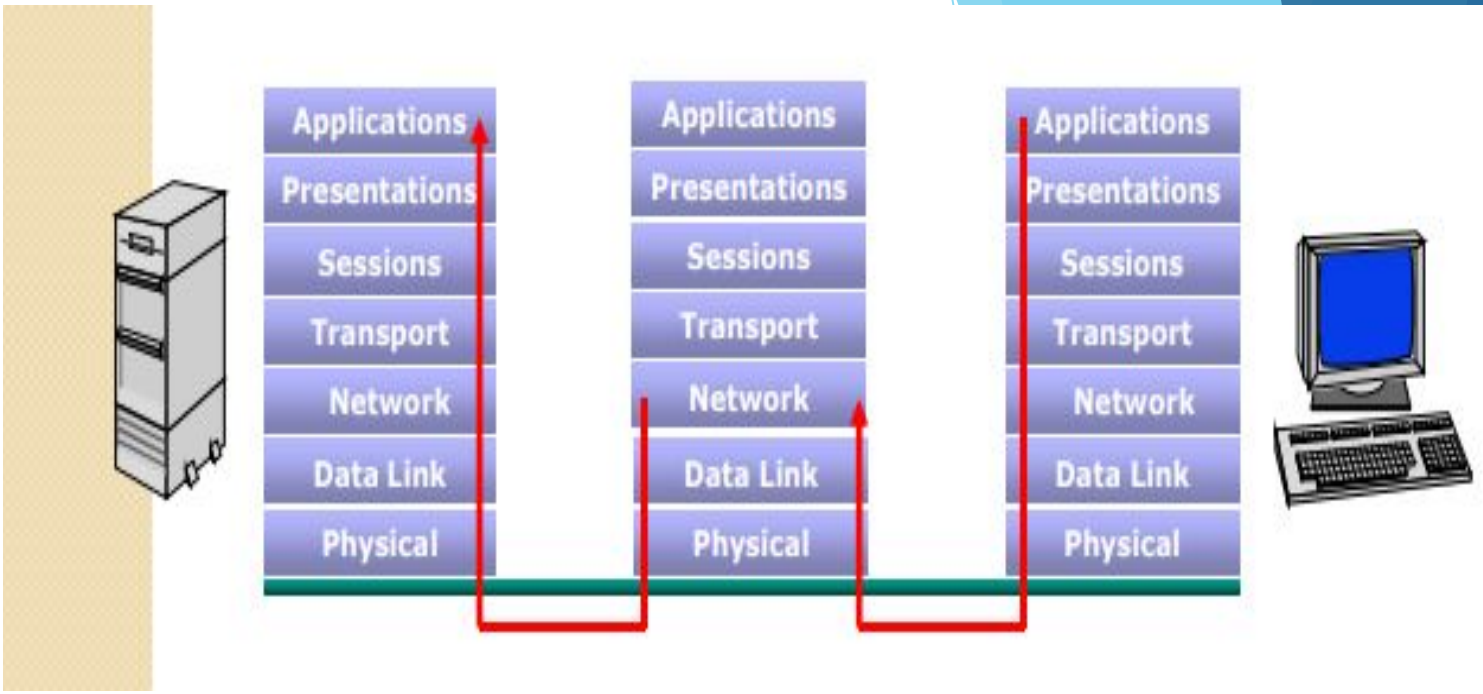
The third generation established the industry standard for NGFWs.

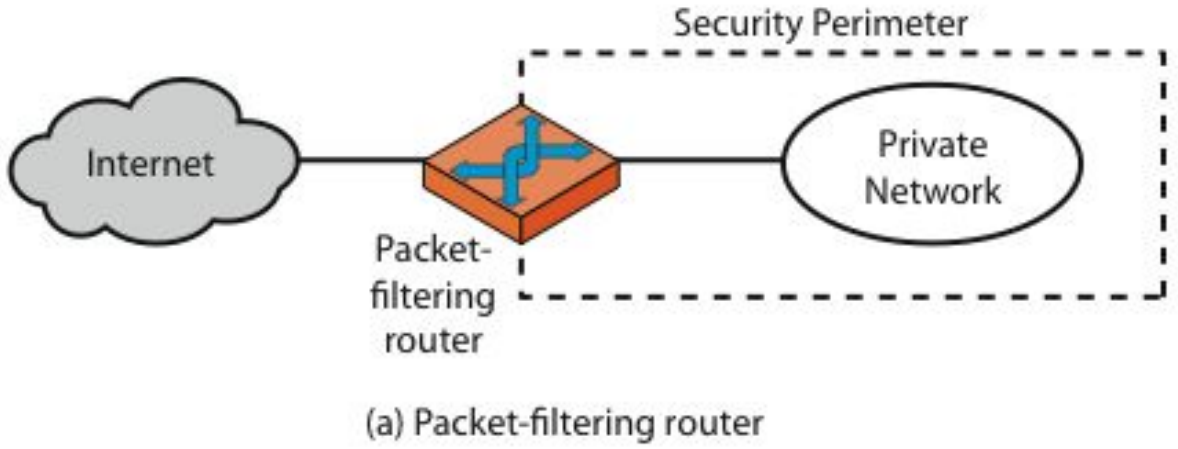
2020: ML-Powered NGFWs

The fourth generation incorporates machine leaming for advanced threat detection.

Packet-Filtering

- Packets examined at the network layer
- Useful “first line” of defense
  - commonly deployed on routers
- Simple accept or reject decision model
- No awareness of higher protocol layer
- Stateless Operation:
  - examine each packet in isolation, without remembering any prior packets or the context of a connection.

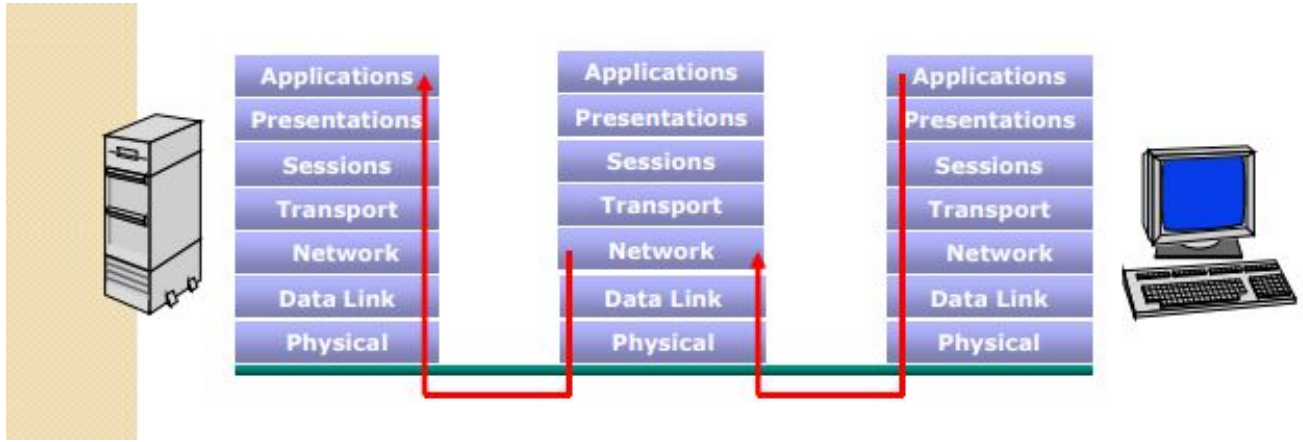




(a) Packet-filtering router

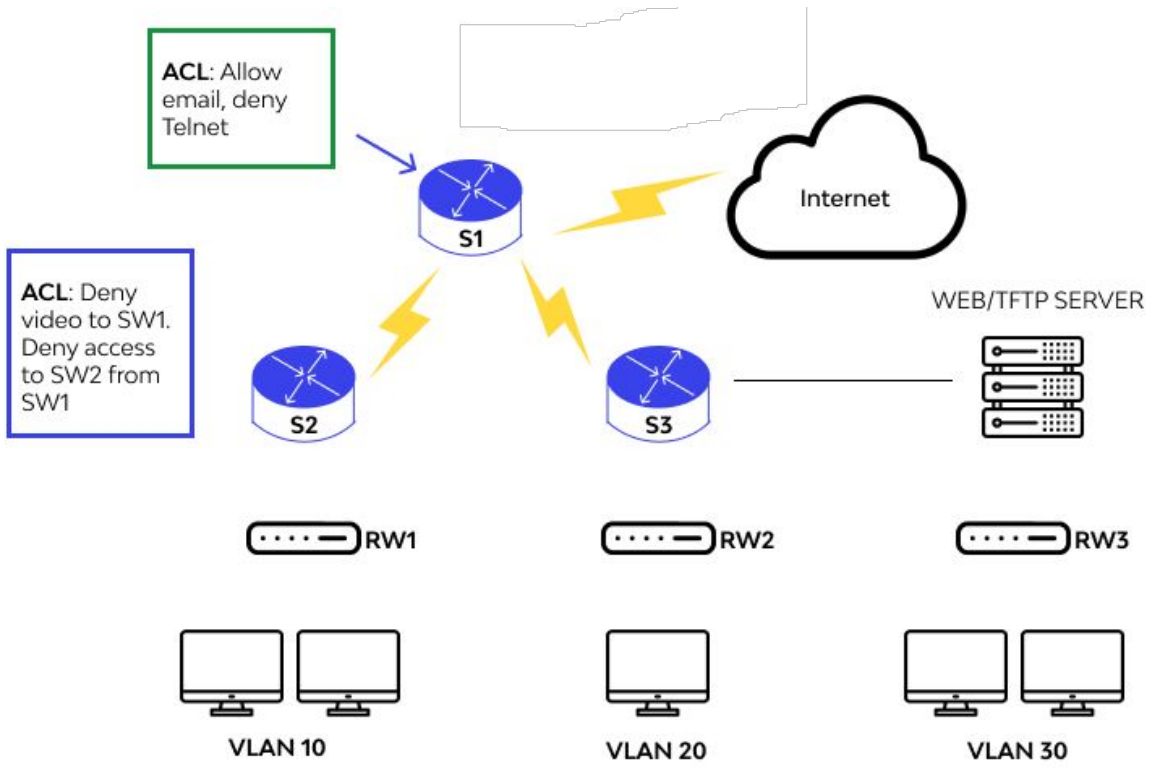
Packet-Filtering

- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
    - tracert
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers packets or the context of a connection.



Access Control List (ACL)

- Packet filtering firewalls use Access Control Lists (ACLs) to decide which traffic to permit or deny.
  - examines the header of every incoming and outgoing packet.
  - compares the packet against the ACL rules in order (top to bottom).
- **Filtering Criteria** (What the ACL looks at):
  - Source IP Address: Where is it coming from?
  - Destination IP Address: Where is it going?
  - Protocol: Is it TCP, UDP, or ICMP?
  - Port Numbers: Is it Web (80), Mail (25), or DNS (53)?
- **Implicit Deny:** The last rule of every ACL is an invisible "Deny All."
- Very fast (low latency) and low cost.
- Stateless



Security & Performance of Packet Filters

- IP address spoofing
  - Fake source address to be trusted
  - Add filters on router to block
- Tiny fragment attacks
  - Split TCP header info over several tiny packets
  - Either discard or reassemble before check
- Degradation depends on number of rules applied at any point
- Order rules so that most common traffic is dealt with first
- Correctness is more important than speed

How to Configure a Packet Filter

Start with a security policy.

Specify allowable packets in terms of logical expressions on packet fields.

Rewrite expressions in syntax supported by your vendor.

General Rules (Least Privilege):

All that is not expressly permitted is prohibited.

If you do not need it, eliminate it.

Packet Filter Configuration - 1

- Every ruleset is followed by an implicit rule: e.g. Block All.

action	src	port	dest	port	flags	comment
block	*	*	*	*	*	default

Packet Filter Configuration - 2

- Example 1:Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine. Also suppose that mail from some particular site SPIGOT is to be blocked.

action	src	port	dest	port	flags	comment
block	SPIGOT	*	*	*	*	We don't trust these site
allow	*	*	OUR-GW	25	*	Connection to our SMTP port

Packet Filter Configuration – 3 (The Flaw)

- Example 2:Now suppose that we want to implement the policy “any inside host can send mail to the outside”.

action	src	port	dest	port	flags	comment
allow	*	*	*	25	*	Connection to outside SMTP port

- This solution allows calls from any port on an inside machine and will direct them to port 25 on an outside machine.
- So why is it wrong?

Packet Filter Configuration - 4 (The Risk)

If our defined restriction is based solely on the destination's port number.

With this rule, an enemy can access any internal machines on port 25 from an outside machine.

We need a better solution that checks the direction/state.

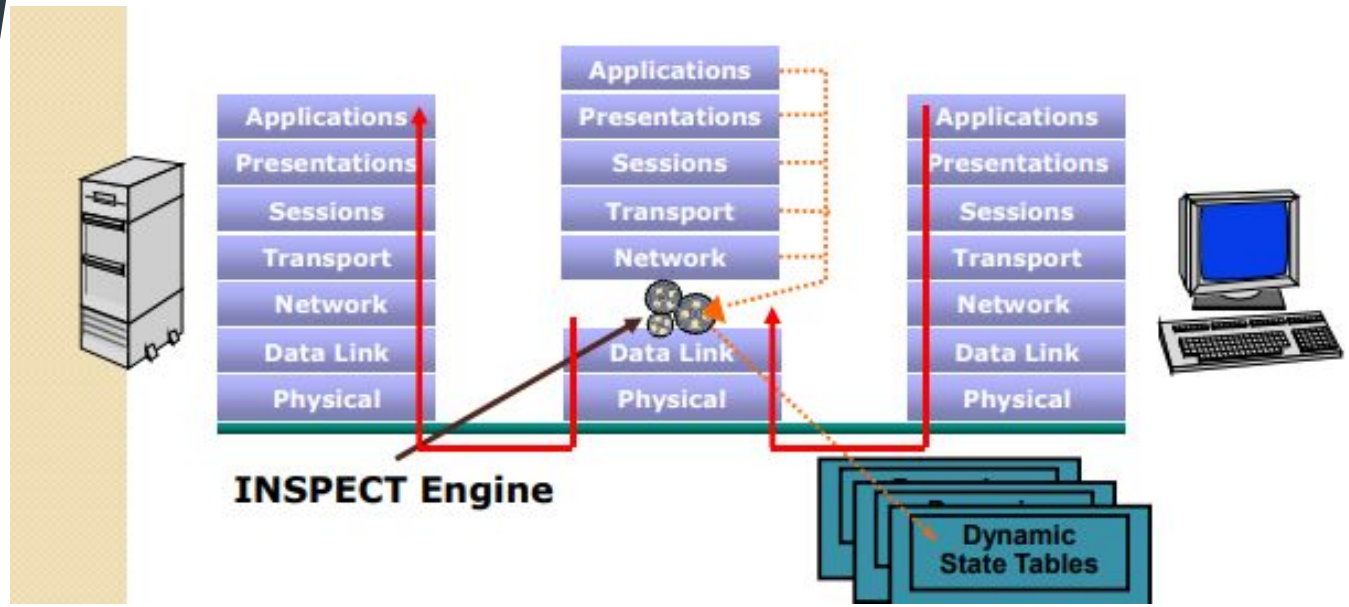
Packet Filter Configuration – 5 (The Solution)

- Rule 1: Only inside machines can access outside machines on port 25.
- Rule 2:The ACK signifies the packet is part of an ongoing conversation.
- Packets without ACK (connection establishment) are dropped unless they match Rule 1.
- Allows replies to come back in.

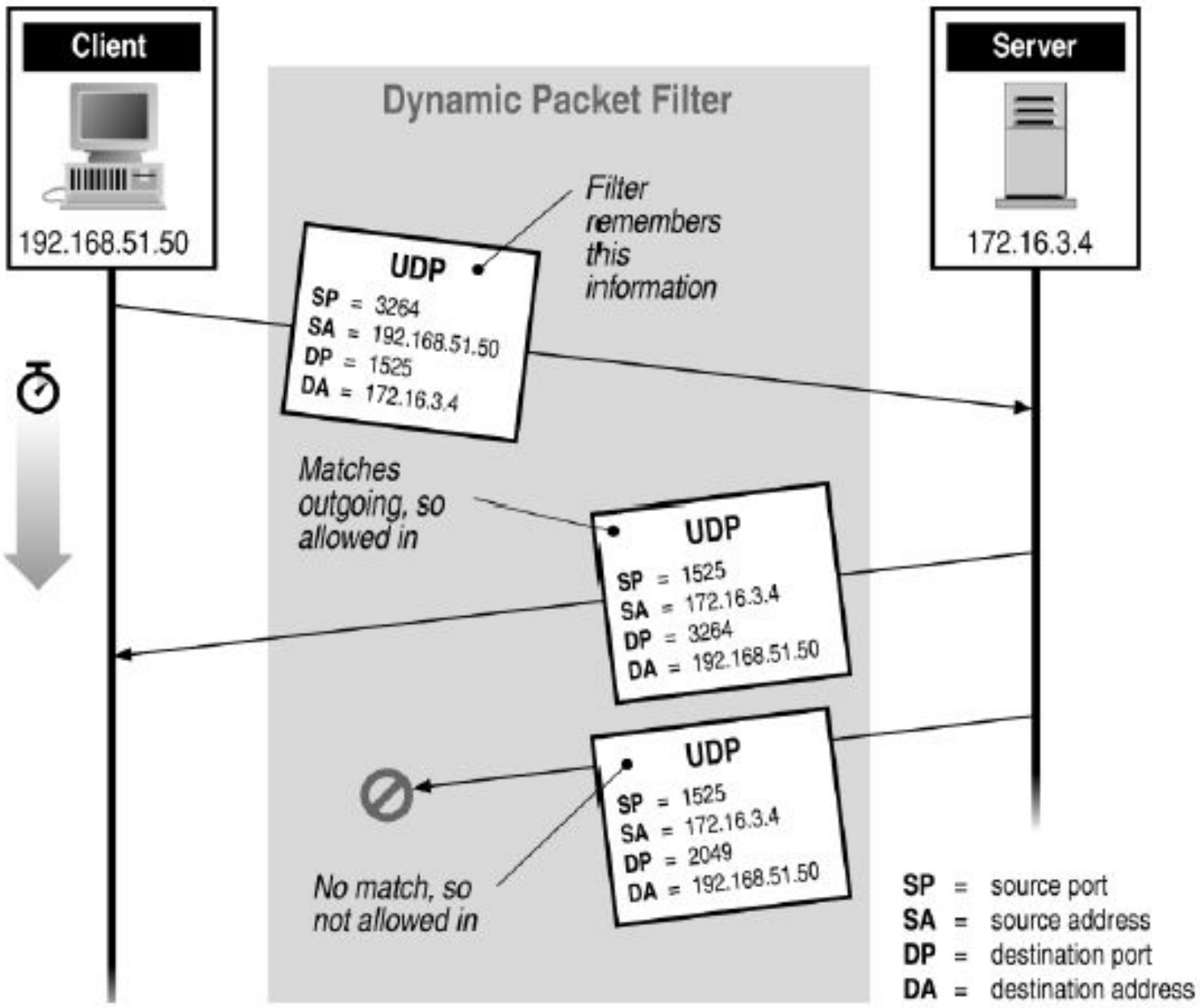
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25	*	Connection to outside SMTP port
allow	*	25	*	*	ACK	SMTP replies

Stateful Inspection

- Packets inspected between Data Link and Network layer (in OS kernel).
- Uses 'Dynamic State Tables’.
  - Memory makes decisions smarter.
- State tables are created to maintain connection context.
- Invented by Check Point (1993)



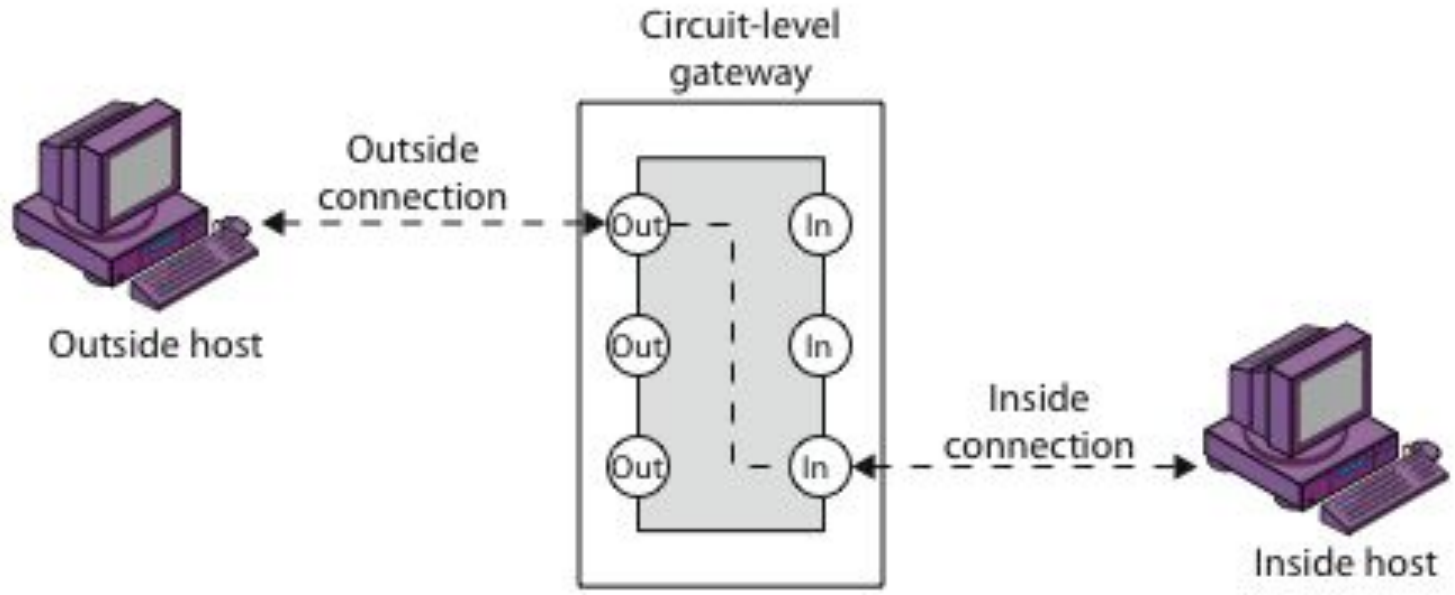
Stateful Filtering



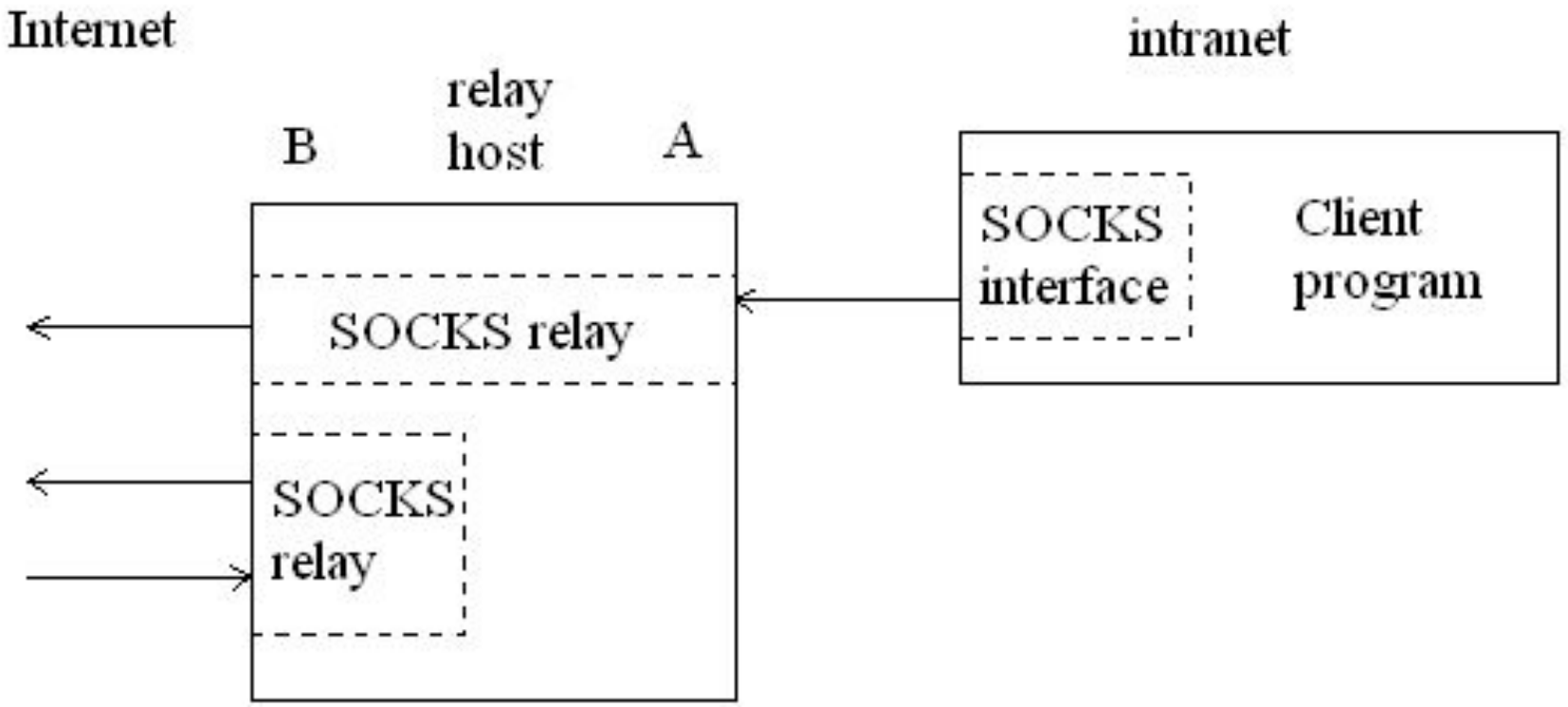
Firewall Gateways

- Firewall runs set of proxy programs
  - Proxies filter incoming, outgoing packets
  - All incoming traffic directed to firewall
  - All outgoing traffic appears to come from firewall
- Policy embedded in proxy programs
- Two kinds of proxies
  - Circuit-level gateways/proxies
    - Working on TCP level
  - Application-level gateways/proxies
    - Tailored to http, ftp, smtp, etc.

Firewalls - Circuit Level Gateway (Session Guard)



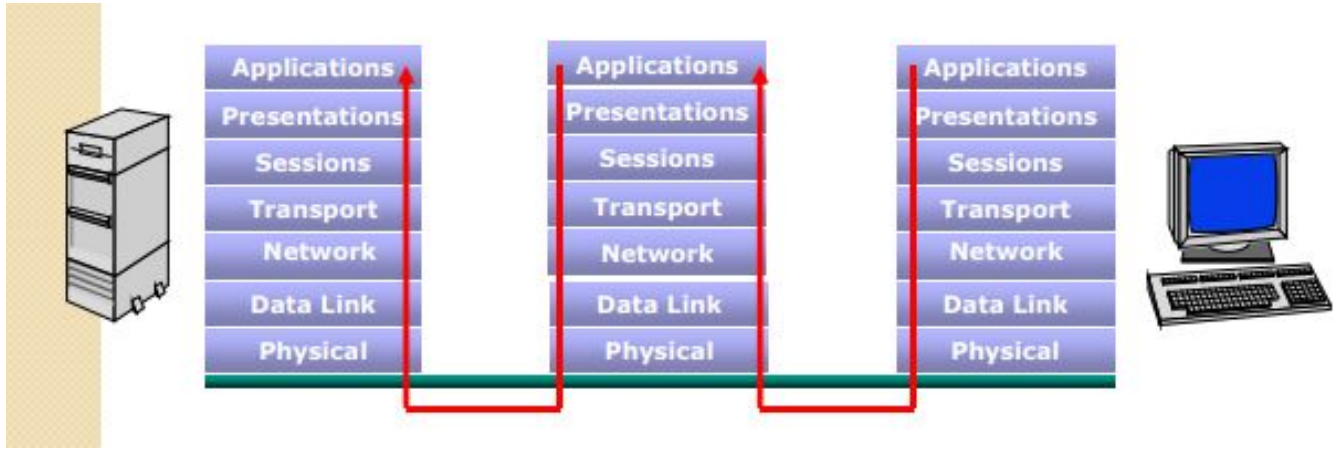
(c) Circuit-level gateway



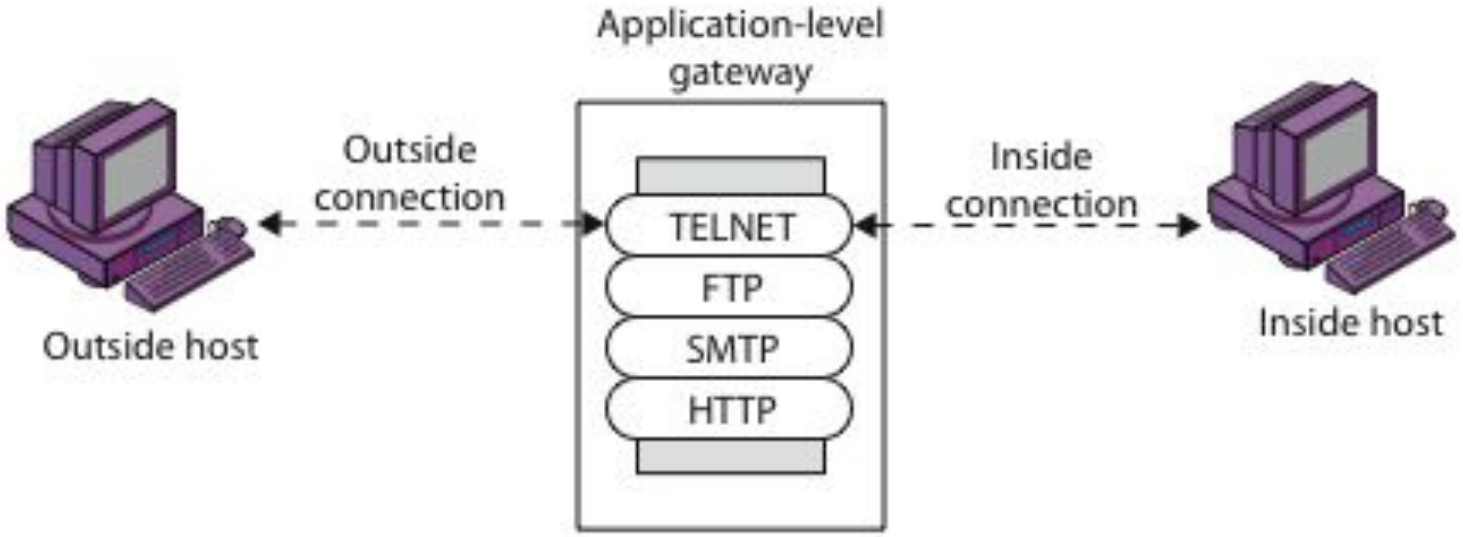
A typical SOCKS connection through interface A, and rogue connection through the external interface, B.

Application Gateway or Proxy

- Packets examined at the application layer.
- Application/Content filtering possible
  - e.g. prevent FTP 'put' commands).
- Modest performance
  - slower than packet filtering.
- Scalability limited due to processing overhead



Firewalls - Application-Level Gateway (or Proxy)

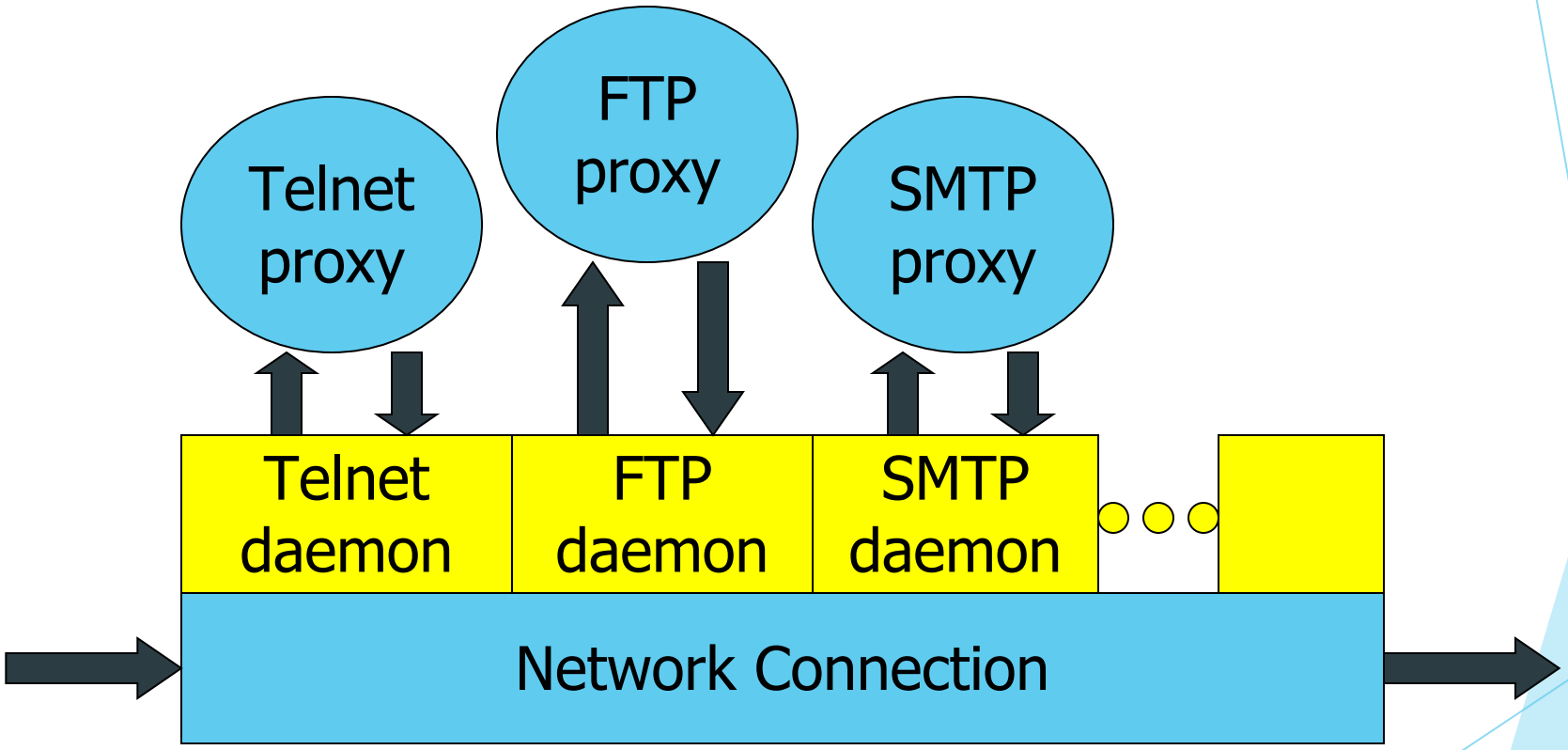


(b) Application-level gateway

Application-Level Filtering

- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
  - custom services generally not supported

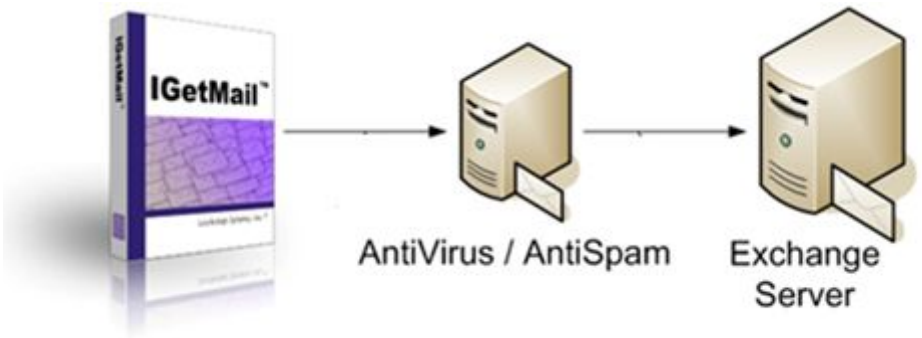
Application-level Firewall Architecture



Daemon spawns (creates) proxy when communication detected …

Application Level Enforce policy for specific protocols

- E.g., Virus scanning for SMTP
  - Need to understand MIME, encoding, Zip archives

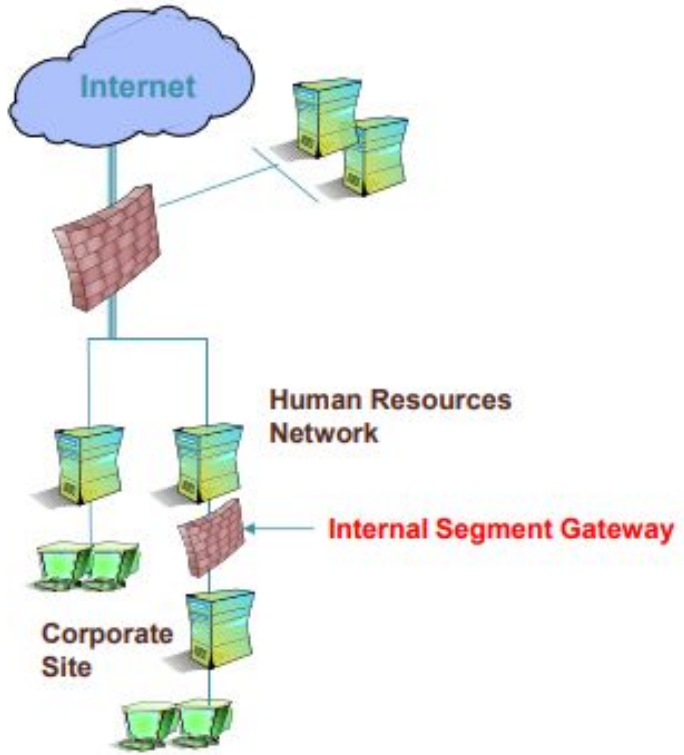


***MIME (Multipurpose Internet Mail Extensions)**

- An image, a document, or a script

Firewall Deployment Strategies

- Corporate Network Gateway (Perimeter).
- Internal Segment Gateway:
  - Protect sensitive segments (Finance, HR, R&D).
  - Provide second layer of defense.
  - Ensure protection against internal attacks.



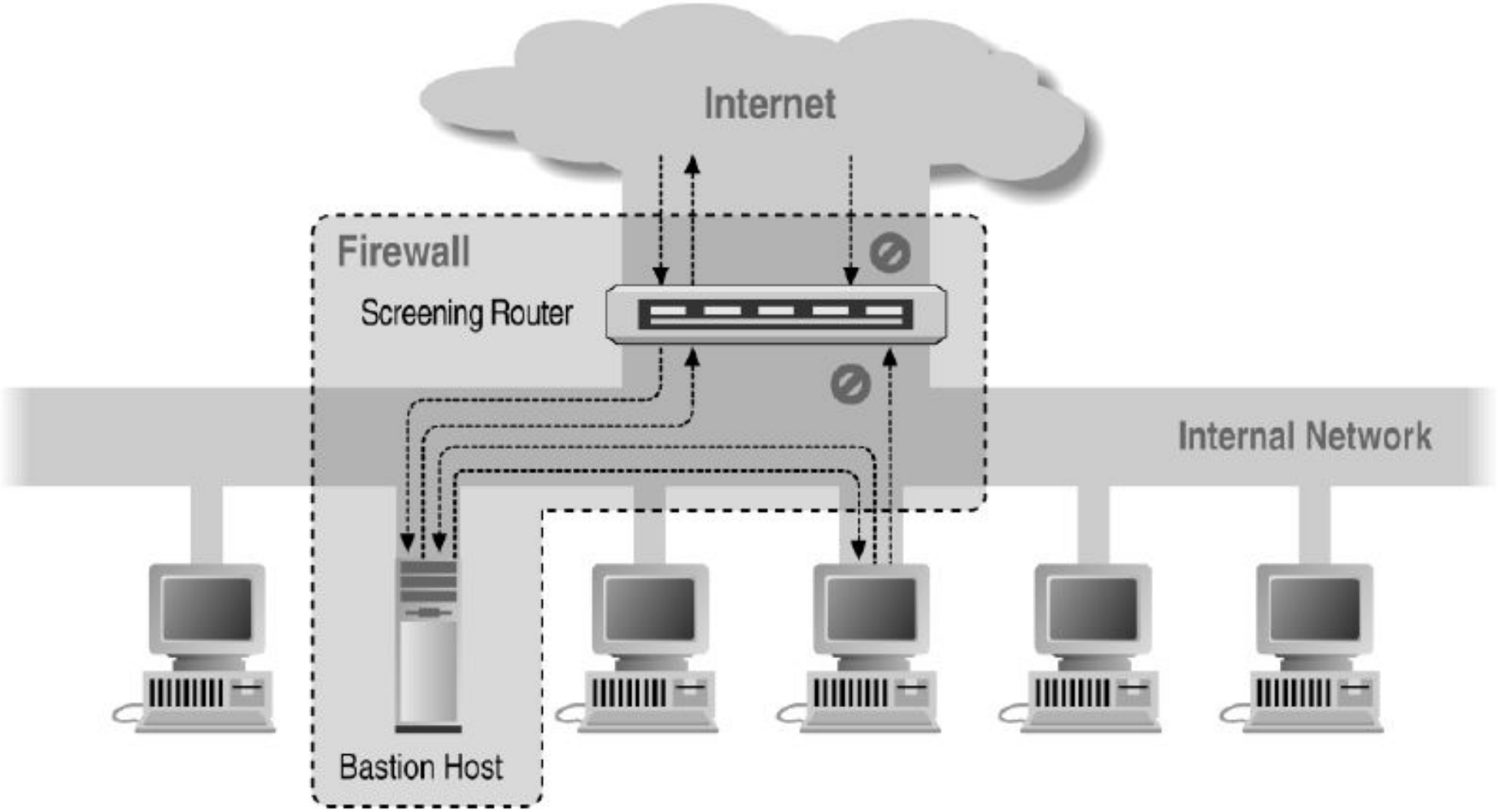
Network Address Translation (NAT)

- Converts a network's private (illegal) IP addresses to legal public IP addresses.
- Benefits:
  - Hides the true addresses of individual hosts (Security).
  - Allows more devices to be connected to the network (Scalability).

Bastion Host

- Highly secure host system
- Potentially exposed to "hostile" elements
- Hence is secured to withstand this
  - Disable all non-required services; keep it simple
- Enforces trusted separation between network connections
- Runs circuit / application-level gateways
  - Install/modify services you want
- Or provides externally accessible services

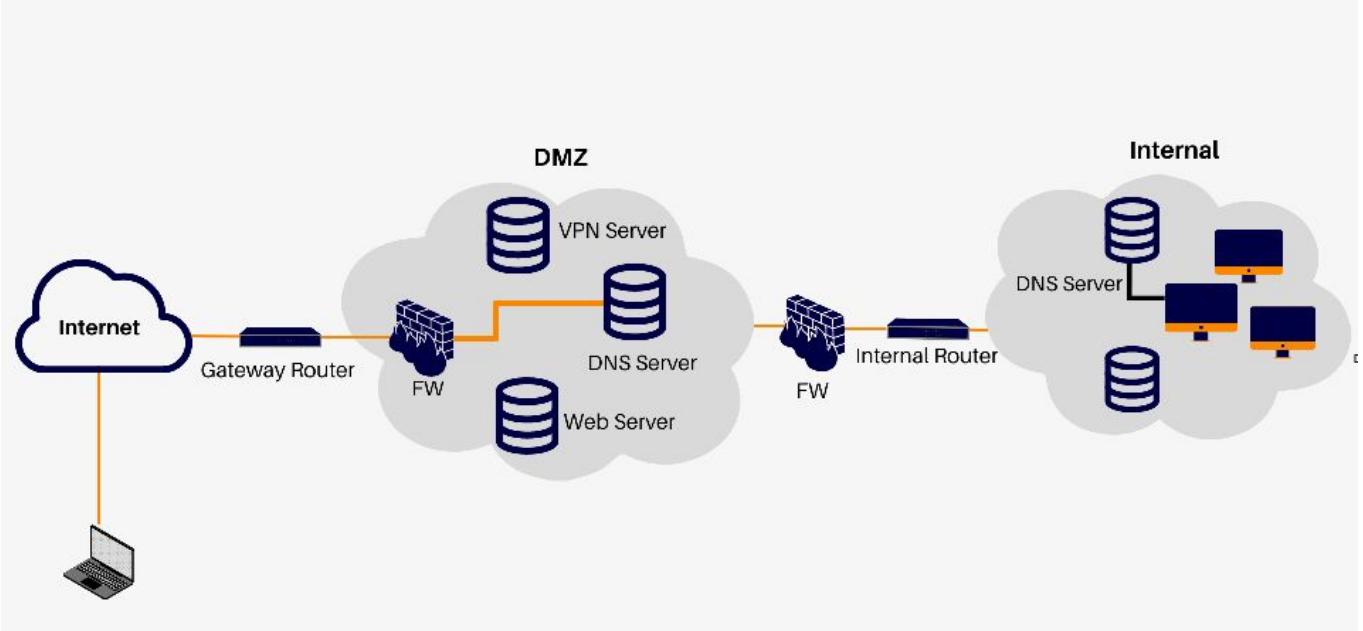
Screened Host Architecture



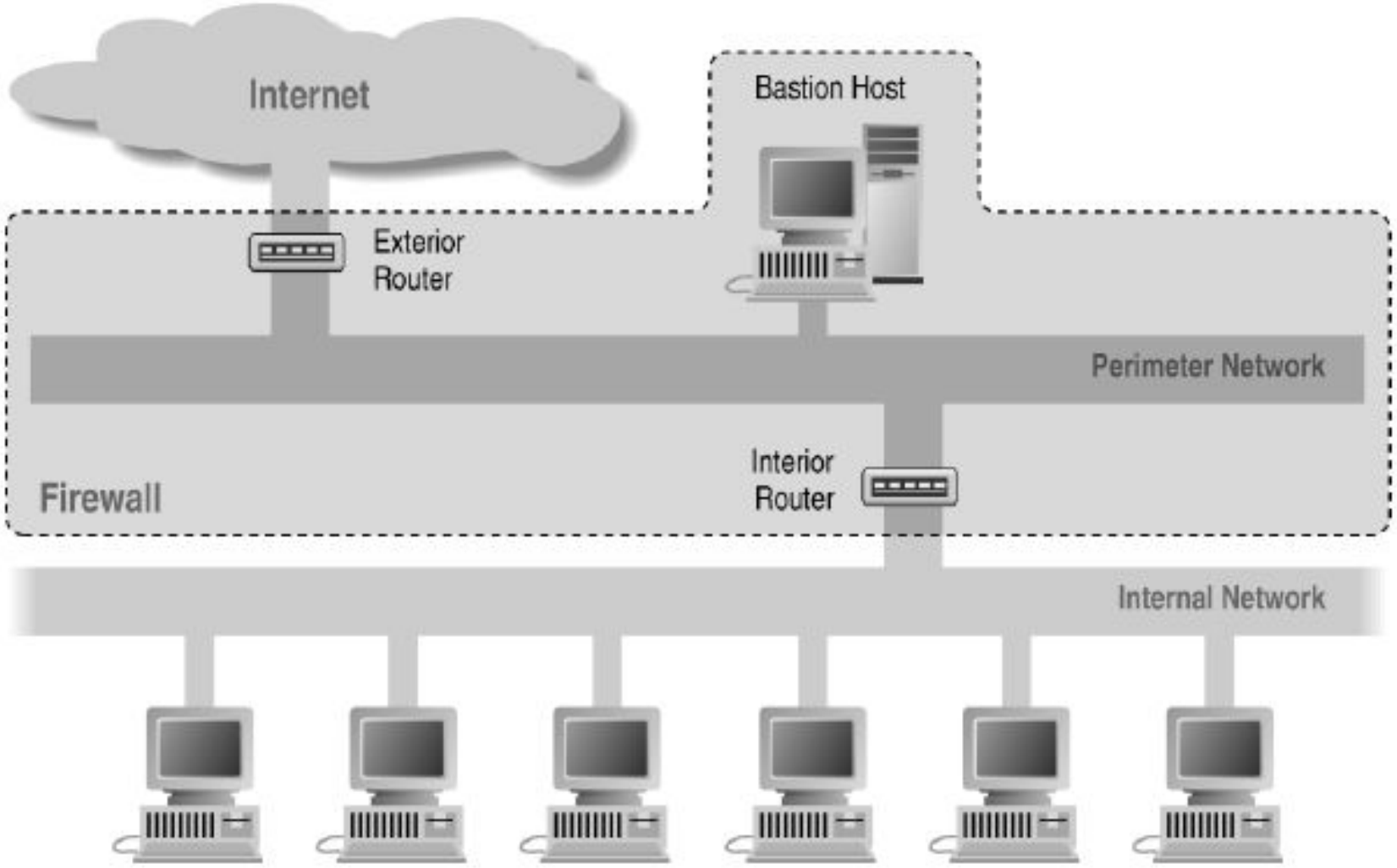
Demilitarized Zone (DMZ)

A physical or logical subnetwork that acts as an intermediate layer between a trusted internal network (LAN) and an untrusted external network (Internet).

- It hosts services that must be accessible from the outside (like Web, Email, and DNS servers) while keeping the rest of the internal network hidden and protected.
- ***The Buffer Zone or No Man's Land***.
- External users can reach the DMZ but are strictly blocked from moving deeper into the private corporate network.
- If an attacker successfully hacks a web server in the DMZ, they are still trapped behind an internal firewall, preventing them from accessing sensitive company data or databases.
- External Firewall: Sits between the Internet and the DMZ.
- Internal Firewall: Sits between the DMZ and the private network.



Screened Subnet Using Two Routers

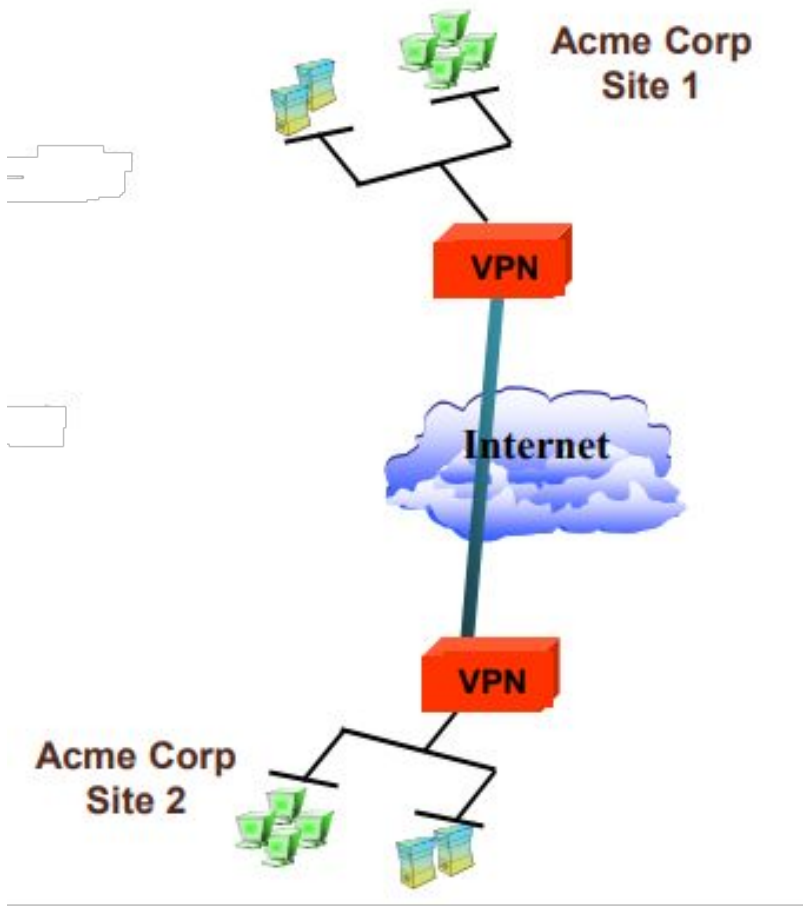


Firewalls Aren’t Perfect?

- Useless against attacks from the inside
  - Evildoer exists on inside
  - Malicious code is executed on an internal machine
- Organizations with greater insider threat
  - Banks and Military
- Protection must exist at each layer
  - Assess risks of threats at every layer
- Cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

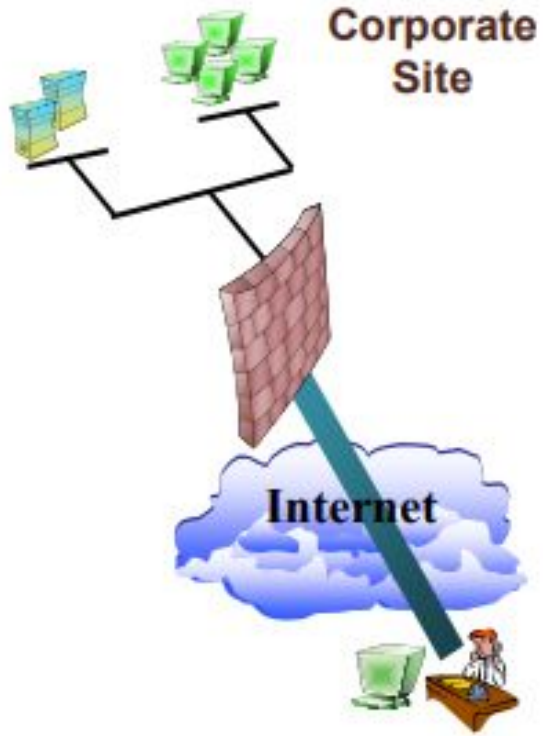
What is a VPN?

- VPN (Virtual Private Network) is a private connection over an open network (Internet).
- Includes authentication and encryption to protect data integrity and confidentiality.



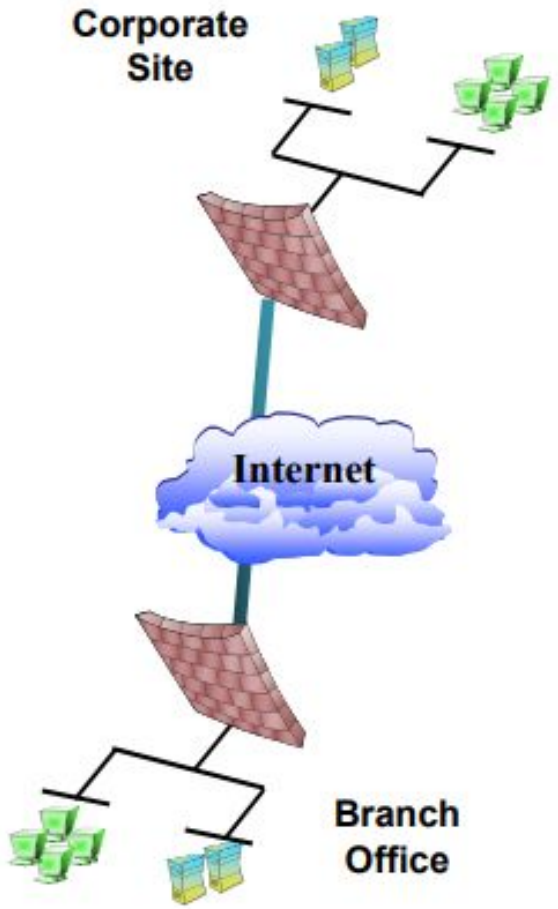
Types of VPNs: Remote Access

- Provides access to internal corporate network over the Internet.
- Reduces long distance, modem bank, and technical support costs.
- Uses protocols like PAP, CHAP, RADIUS.
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Handshake Authentication Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)



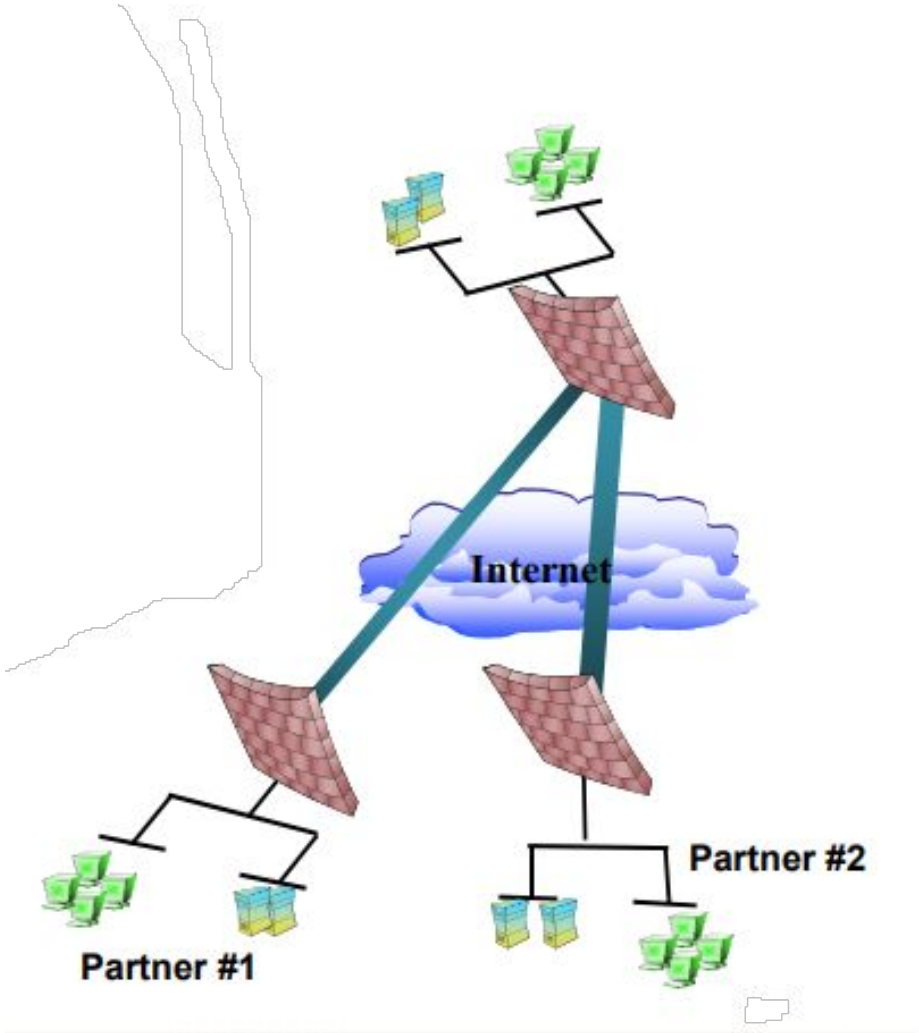
Types of VPNs: Site-to-Site

- Connects multiple offices over the Internet.
- Reduces dependencies on frame relay and leased lines.



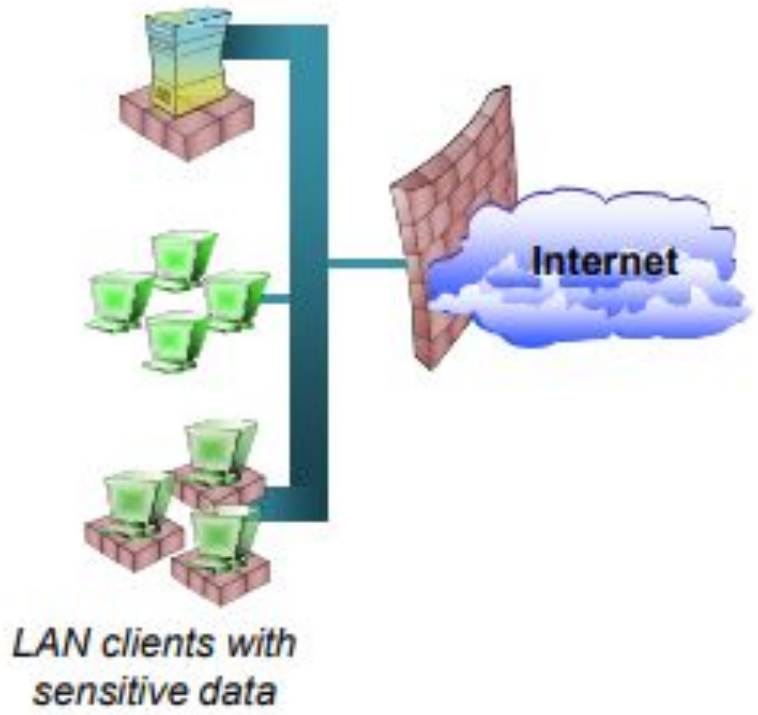
Types of VPNs: Extranet

- Provides business partners access to critical information (leads, sales tools, etc).
- Reduces transaction and operational costs.



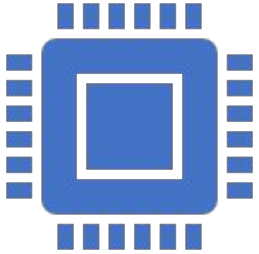
Types of VPNs: Client/Server

- Protects sensitive internal communications.
- Example: Encrypting traffic between LAN clients and a Database Server.



Intrusion Detection and Prevention Systems

Intrusion Detection/Prevention System (IDS/IPS)



Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitor network traffic to detect and prevent malicious activities

These systems are either implemented on a dedicated hardware or implemented as applications on a general-purpose server

IDS and IPS are placed at strategic points in the network to be able to monitor traffic from all devices

Intrusion Detection/Prevention System (IDS/IPS)

IDS and IPS leverage a database of attacks' signatures to detect malicious traffic

Signature-based IDS/IPS are popular and effective, but cannot detect zero-day attacks

Machine learning can be leveraged to create a model of the normal behavior of the network

Thus, the normal model can be used as a baseline to detect any abnormalities in the network

Intrusion Detection System (IDS)

An IDS monitors the traffic of a network *passively*

i.e., the IDS is not deployed inline in the topology

A network device (e.g., switch, router) duplicates and forwards the traffic to the IDS

The IDS analyzes the traffic offline (promiscuous mode) and matches the traffic stream with known malicious signatures

Advantages of IDS:

It does not negatively impact the performance of the network

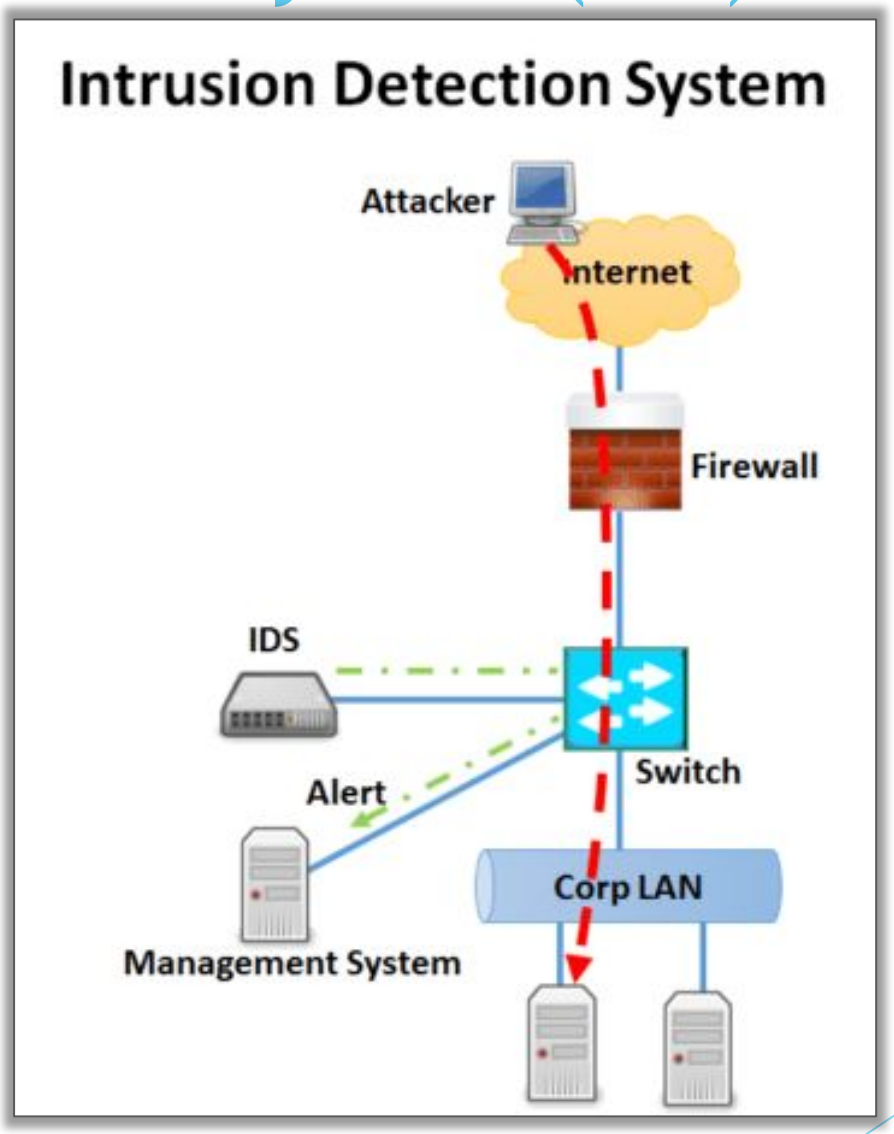
It does not affect the network if a problem or misconfiguration of the IDS occurs

Disadvantages of IDS:

It cannot stop malicious single-packet attacks from reaching the target

It requires assistance from other networking devices to respond to the attack

Intrusion Detection System (IDS)



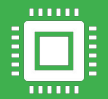
Intrusion Prevention System (IPS)

An IPS device monitors the network traffic *actively*

i.e., the IPS is deployed inline in the topology

The IPS analyzes traffic online, thus, all ingress and egress traffic must flow through the IPS for processing

Advantages of IPS:



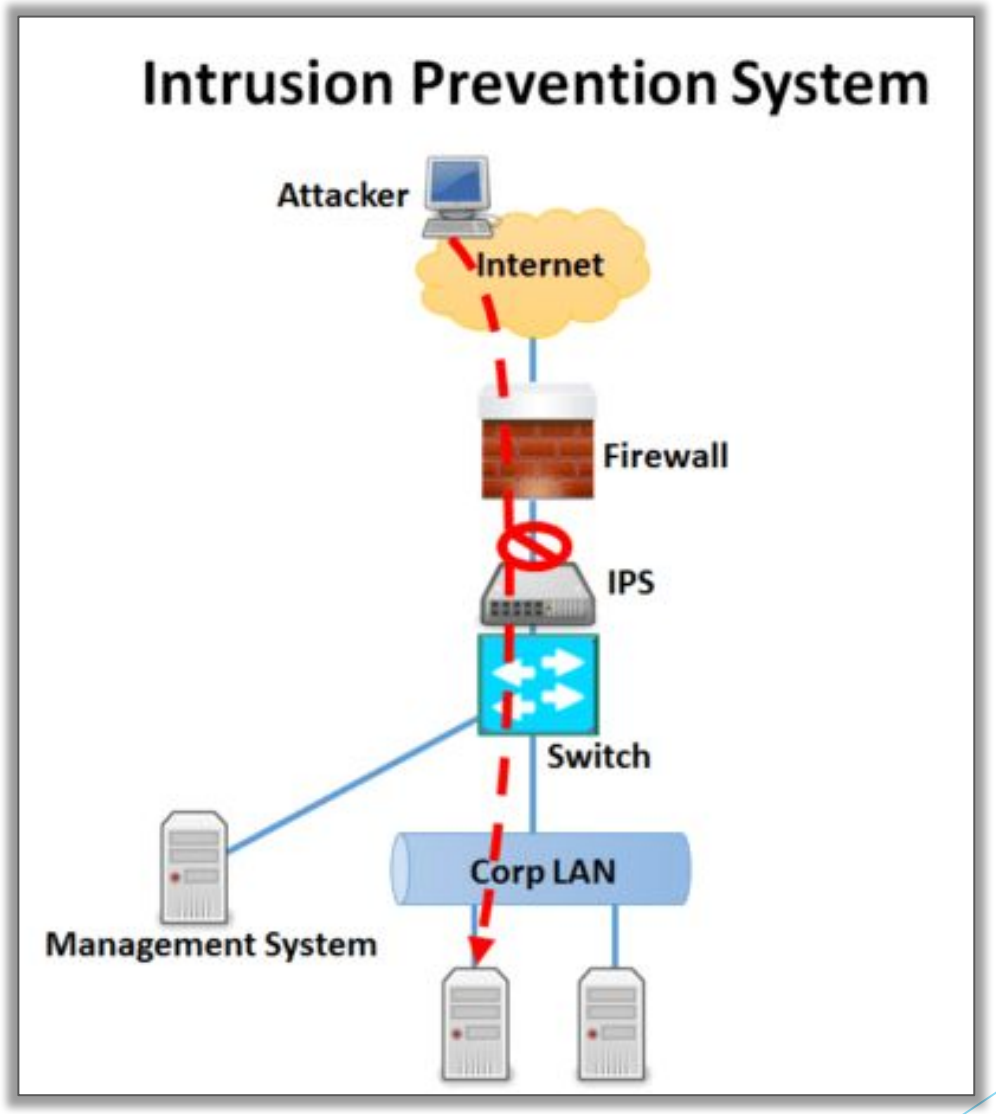
It can stop single packet attacks

Disadvantages of IPS:

It can negatively affect the performance of the network

It can disrupt the network if a problem or misconfiguration of the IPS occurs

Intrusion Prevention System (IPS)



Identifying Malicious Traffic on the Network

Signature-based IPS/IDS

- Set of rules looking for some specific pattern in a packet or stream of packets
- Most significant method used on today's IPS/IDS

Policy-based IPS/IDS

- Traffic is matched based on the security policy implemented in the network. e.g. No one should use Telnet.

Anomaly-based IPS/IDS

- A baseline of normal and malicious behavior is modeled and compared to the traffic flowing in the network. e.g. traffic spike at 4:00 AM from different country.

Reputation-based IPS/IDS

- A collection of inputs from various sources is gathered, including the reputation of a certain IP address, domain, URL, etc.

IPS/IDS Evasion Techniques

Traffic fragmentation	• Malicious traffic is split into multiple parts
Traffic substitution and insertion	• Data payload characters are substituted into different formats
Timing attacks	• Malicious traffic is sent at slow time intervals
Encryption and tunneling	• Malicious traffic is encrypted and cannot be easily inspected
Resource exhaustion	• Thousands of alerts are generated

The Security Toolkit: Choosing the Right Network Defense

Distinguishing between different network security tools by explaining their specific roles, scopes, and unique strengths.

pfSense

The Network's "Grand Central Station"

A complete open-source OS that handles routing and firewalling for an entire network.

UFW

The "Simple Lock" for Single Hosts

A host-based Linux tool designed to easily manage open ports on one computer.

Snort

The "Reliable Veteran" Detective

Uses signature-based detection to compare packet patterns against a massive database of known threats.

Suricata

High-Speed Multi-Threading

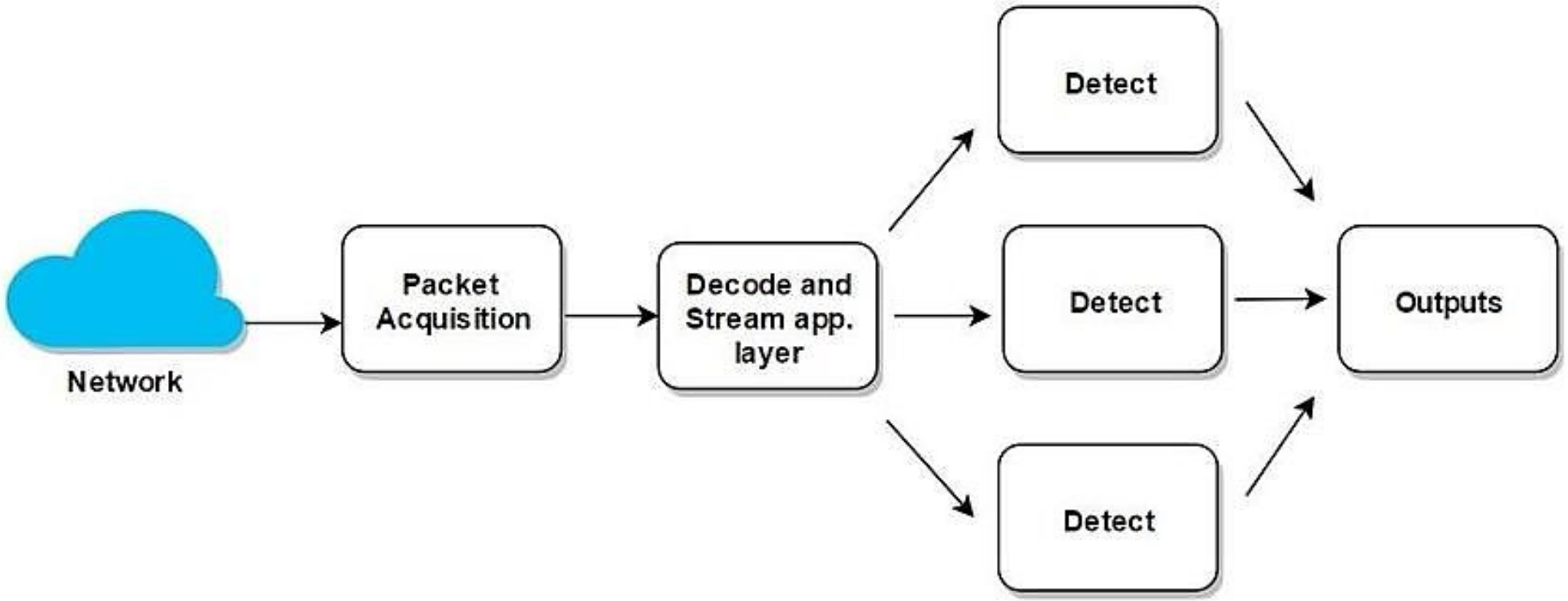
Modern engine capable of Deep Packet Inspection across multiple CPU cores for high-traffic networks.

QUICK-REFERENCE COMPARISON

Tool	Scope	Primary Category
pfSense	The Whole Network	Firewall Distribution
UFW	A Single Computer	Host Firewall
Suricata	High-Speed Traffic	IDS/IPS Engine

Multi-threading Engine

- Networks today process traffic in the order of tens and hundreds of Gigabytes per second
- Multithreading allows scaling horizontally on a single appliance



The Layered Defense

- **The Perimeter:** A **pfSense** box acts as the gateway.
- **The Intelligence:** Inside that pfSense box, you run **Suricata** to scan for viruses.
- **The Last Stand:** On the actual web server itself, you run **UFW** to make sure that even if the perimeter is breached, the server only talks to authorized ports.