Firewalls, IDS and IPS

MIS5214

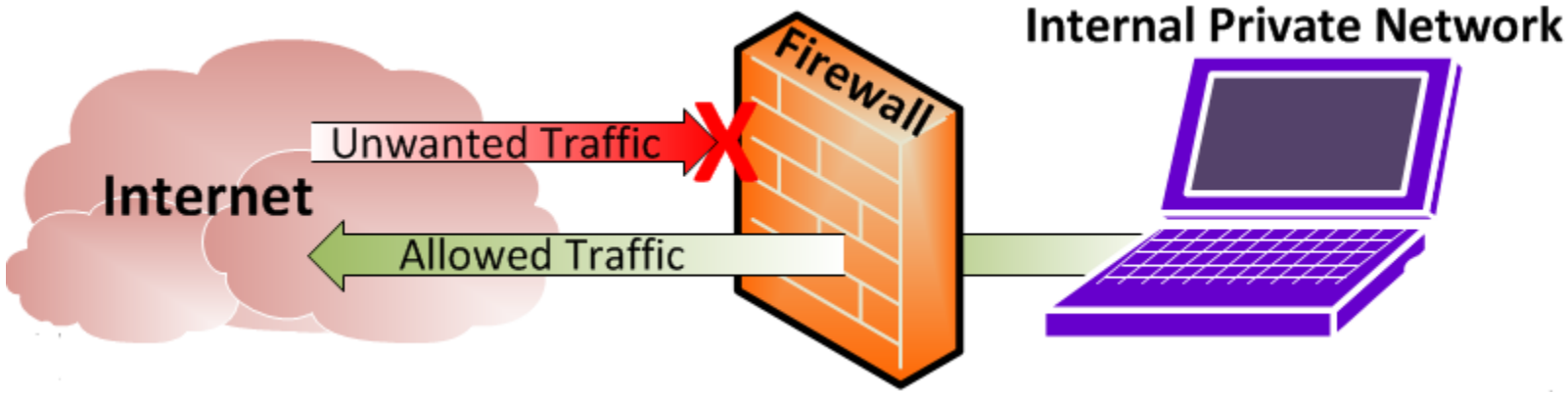
Midterm Study Support Materials

Agenda

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems

Firewalls are used to Implement Network Security Policy

- Firewalls support and enforce an organization's network security policy
- High-level directives on acceptable an unacceptable actions to protect critical assets
- Firewall security policy:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed

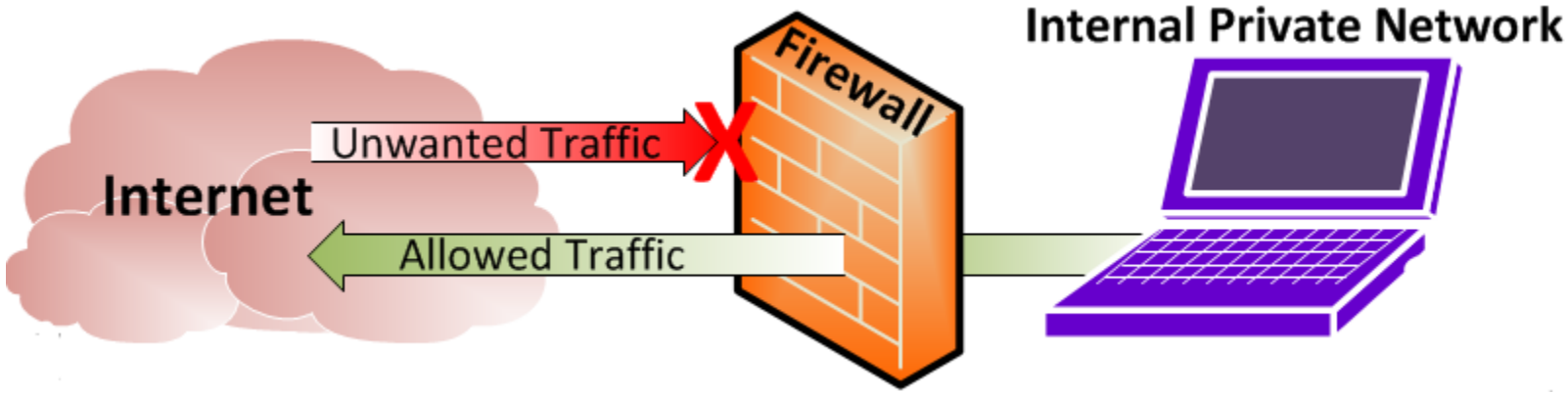


Firewalls are security architecture “choke points” in an IT network

- All communication should flow through and be inspected and restricted by firewalls
- Are used to restrict access to one network from another
  - Restrict access from the internet to access corporate networks
  - Restrict access between internal network segments
- Restrict access
  - Between origin and destination
  - Based on determination of acceptable traffic type(s)

Firewalls are used to Implement Network Security Policy

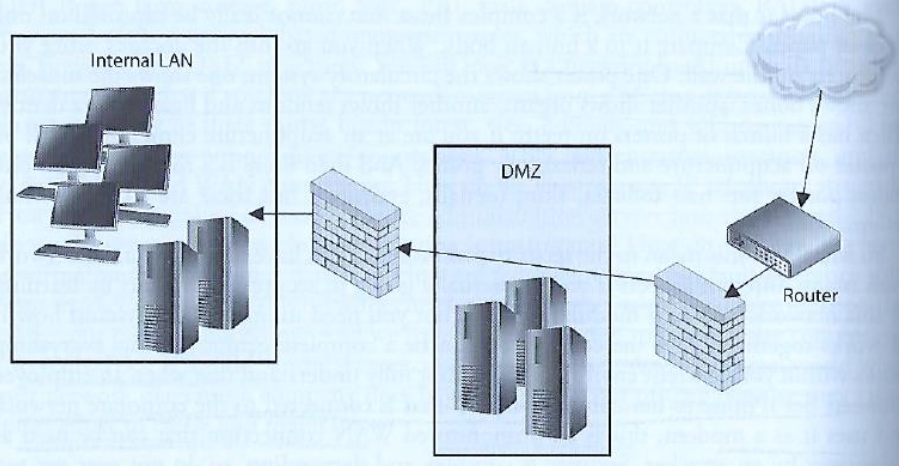
- Firewalls support and enforce an organization's network security policy
- High-level directives on acceptable and unacceptable actions to protect critical assets
- Firewall security policy identifies:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed



Firewall Technology

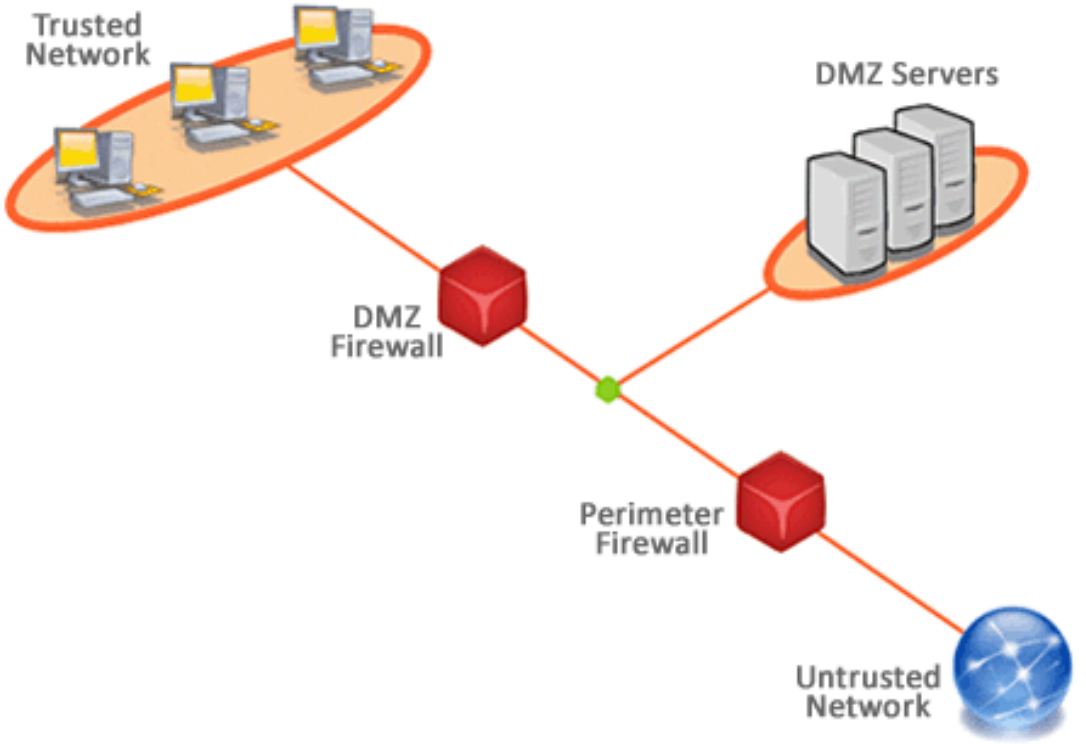
- May be implemented as a
  - Software product running on a server
  - Specialized hardware appliance
- Monitors data packets coming into and out of the network it is protecting
- Packets are filtered by:
  - Source and destination addresses and ports
  - Header information
  - Protocol type
  - Packet type
  - Service
  - Data content – i.e. application and file data content

Demilitarized Zone (DMZ)



Firewalls are installed to construct DMZ areas

- Network segments which are located between protected and unprotected networks
- Provides a buffer zone between the dangerous Internet and valuable assets the organization seeks to protect
- Usually 2 firewalls are installed to form a DMZ
  - May contain mail, file, and DNS (Domain Name System) servers
  - Usually contain an Intrusion Detection System sensor which listens for suspicious and malicious behavior
  - Servers in DMZ must be hardened to serve as the first line of protection against attacks coming from the internet

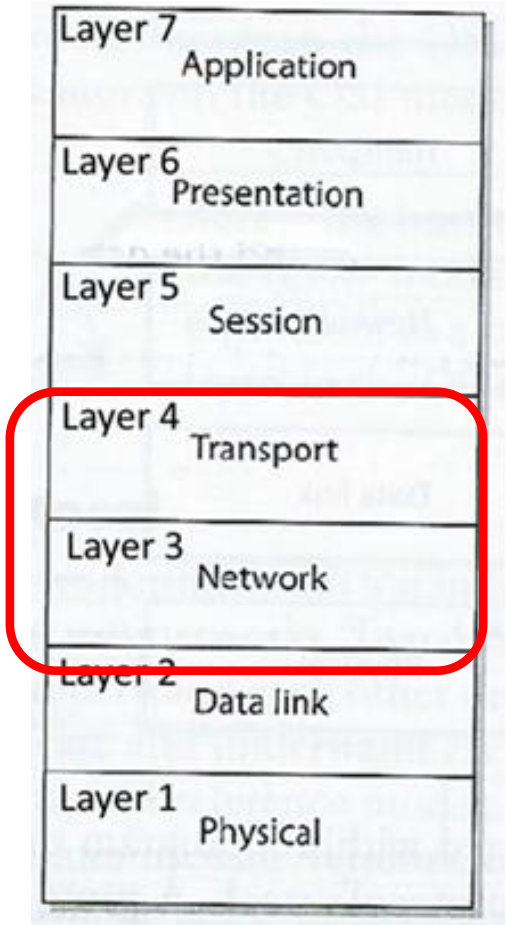


Types of Firewalls

1. Packet filtering
2. Dynamic packet filtering
3. Stateful inspection
4. Proxy Firewall
5. Kernal Proxy

Packet-filtering firewalls

- "First-generation" firewall technology – most basic and primitive
- Capabilities built into most firewalls and routers
- Configured with access control lists (ACLs) which dictate the type of traffic permitted into and out of the network
- Filters compare protocol header information from network and transport layers with ACLs

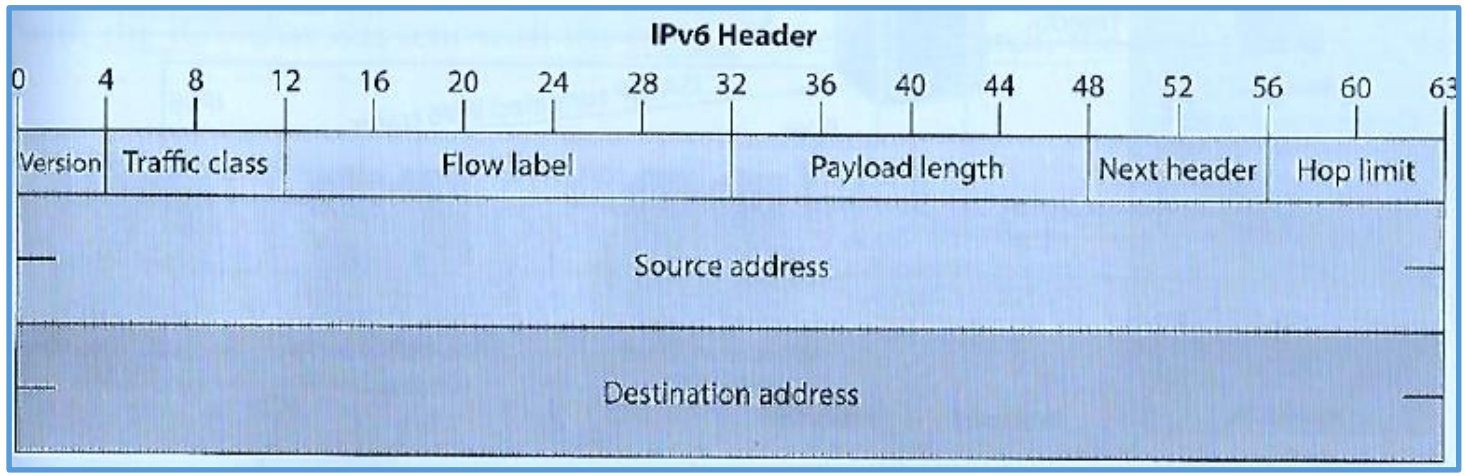


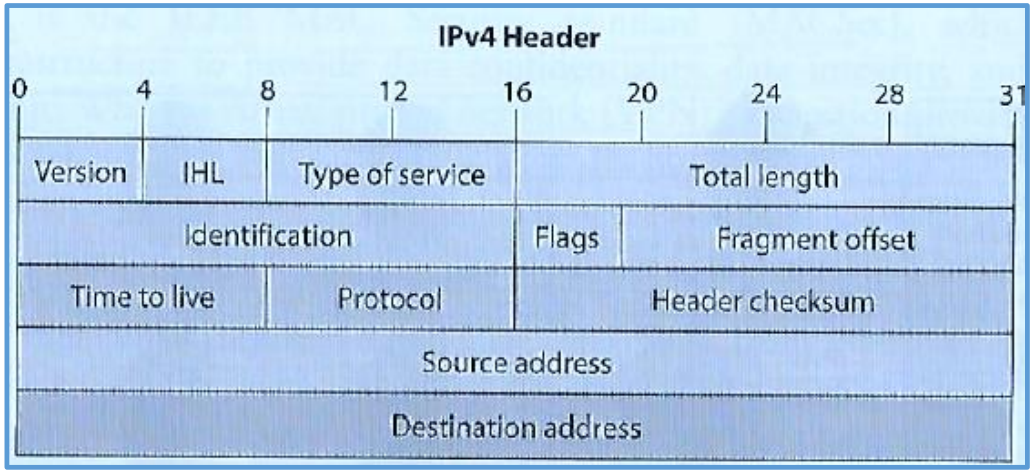
Packet-filtering Firewalls

Compares ACLS with network protocol header values to determine permit/deny network access based on:

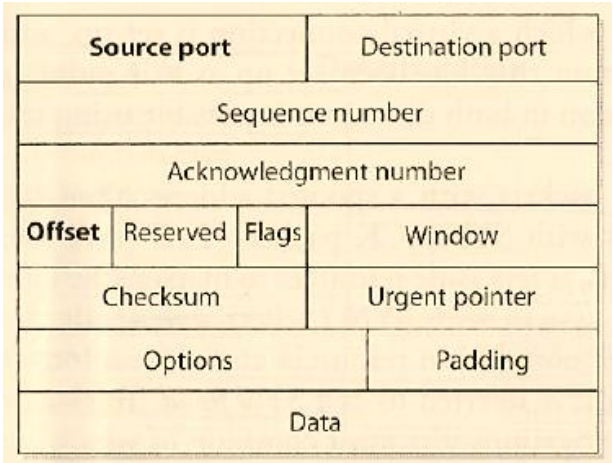
1. Source and destination IP addresses
2. Source and destination port numbers
3. Protocol types
4. Inbound and outbound traffic direction

Network Layer 3

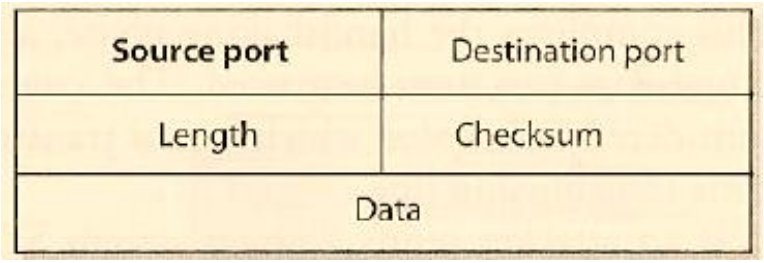




TCP format



UDP format



Transport Layer 4

TCP/IP Port numbers

Ports 0 to 1023 are Well-Known Ports

Ports 1024 to 49151 are Registered Ports – Often registered by a software developer to designate a particular port for their application

Ports 49152 to 65535 are Public Ports

Port # / Layer	Name	
1080	socks	SOCKS network application proxy services
1236	bvcontrol [rmtcfg]	Remote configuration server for Gracilis Packeten network switches[a]
1300	h323hostcallsc	H.323 telecommunication Host Call Secure
1433	ms-sql-s	Microsoft SQL Server
1434	ms-sql-m	Microsoft SQL Monitor
1494	ica	Citrix ICA Client
1512	wins	Microsoft Windows Internet Name Server
1524	ingreslock	Ingres Database Management System (DBMS) lock services
1525	prospero-np	Prospero non-privileged
1645	datametrics [old-radius]	Datametrics / old radius entry
1646	sa-msg-port [oldradacct]	sa-msg-port / old radacct entry
1649	kermit	Kermit file transfer and management service

Example ACL Rules

- Router configuration allowing SMTP (Simple Mail Transfer Protocol) traffic to travel from system 10.1.1.2 to system 172.16.1.1:

  permit tcp host 10.1.1.2 host 172.16.1.1 eq smtp

- Allow UDP traffic from 10.1.2 to 172.16.1.1:

  permit udp host 10.1.1.2 host 172.16.1.1

- Block all ICMP (Internet Control Message Protocol) i.e. router error messages and operational information traffic from entering through a certain interface:

  deny icmp any any

- Allow standard web traffic (to a web server listening on port 80) from system 1.1.1.1 to system 5.5.5.5:

  permit tcp host 1.1.1.1 host 5.5.5.5 eq www

Packet-filtering firewalls

Packet filtering firewalls: monitor traffic and provide “stateless inspection” of header attribute values (i.e. delivery information) of individual packets

and after the decision to permit or deny access to the network is made the firewall *forgets* about the packets

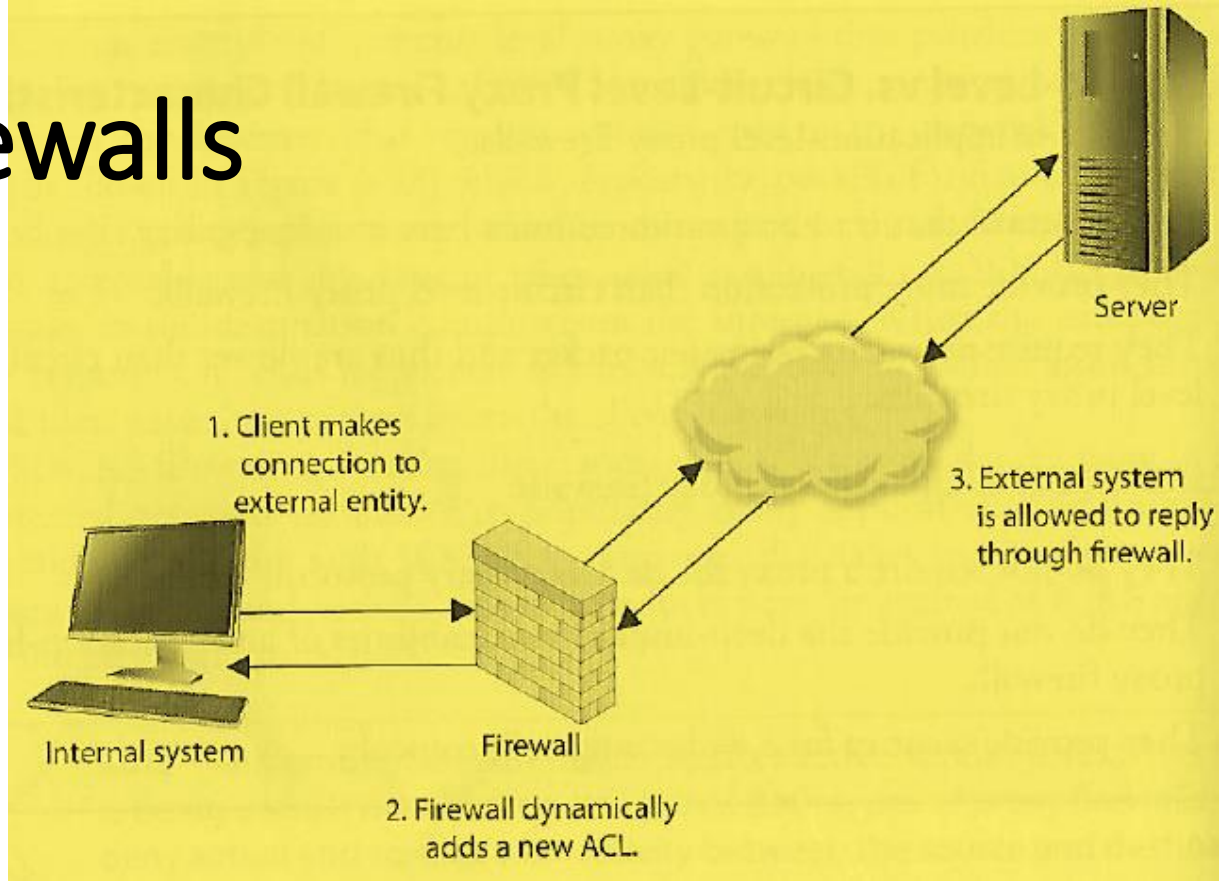
- **Weakness:** No knowledge of data moving between applications communicating across the network
  - Cannot protect against packet content, e.g. probes for specific software with vulnerabilities and exploit a buffer overflow for example
  - Should not be used to protect an organization’s infrastructure and information assets

- **Strengths:** Useful at the edge of a network to quickly and efficiently strip out obvious “junk” traffic
  - High performance and highly scalable because they do not carry out extensive processing on the packets and are not application dependent
  - First line of defense to block all network traffic that is obviously malicious or unintended for a specific network
  - Typically complemented with more sophisticated firewalls able to identify non-obvious security risks

Dynamic Packet-Filtering Firewalls

When an internal system needs to communicate with a computer outside its trusted network it needs to choose an identify its source port so the receiving system knows how/where to reply

- Ports up to 1023 are reserved for specific server-side services and are known as “well-known ports”
- Sending system must choose a randomly identified port higher than 1023 to use to setup a connection with another computer



- The dynamic packet-filtering firewall creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port
- The ACLs are dynamic in nature – once the connection is finished the ACL is removed
- The dynamic packet-filtering firewall offers the benefit of allowing any type of traffic outbound and permitting only response traffic inbound

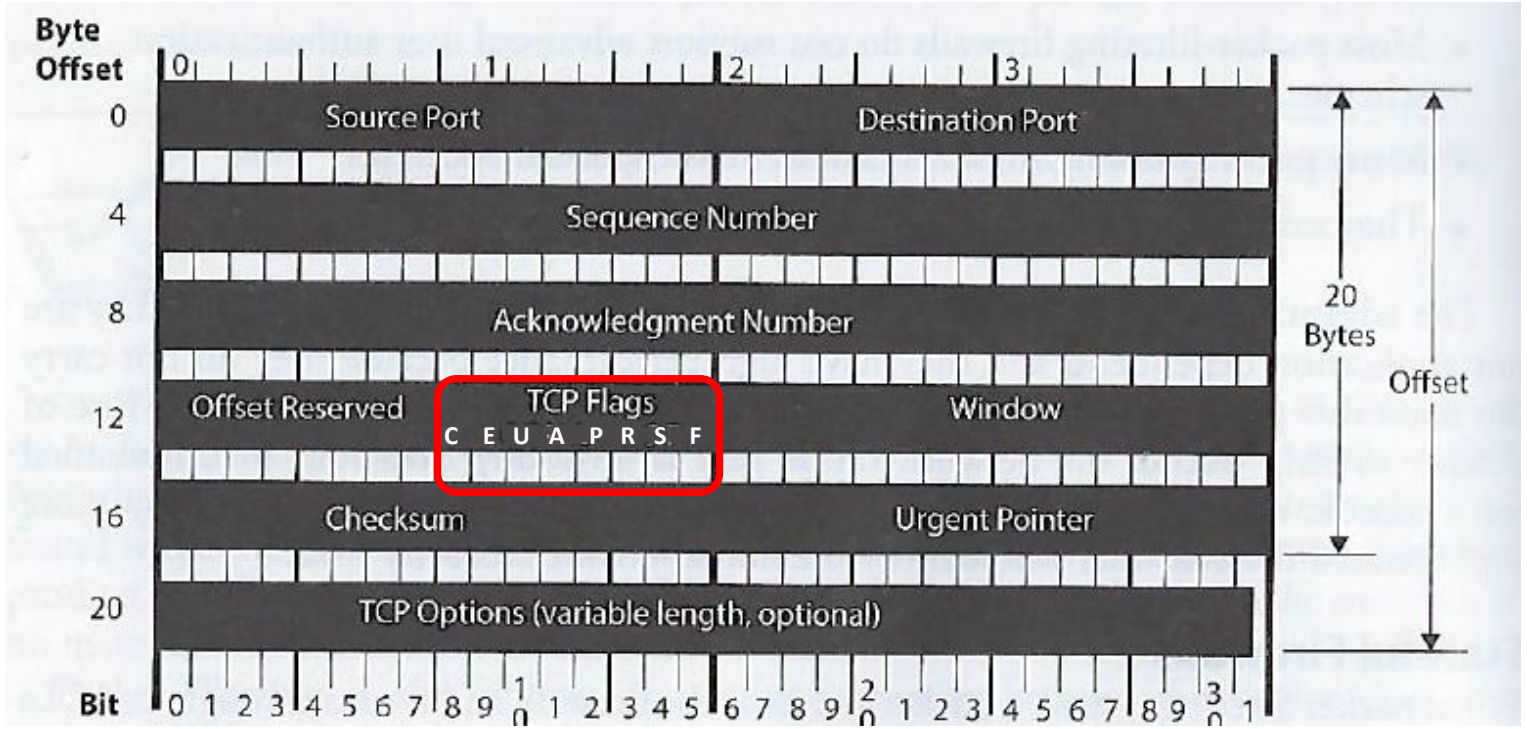
Stateful Inspection Firewall

- Remembers and keeps track of what computers say to each other
  - Tracks where packets went until each particular connection between computers is closed
- Uses a “state table” which it updates to track the contents of packets each computer sent to each other
  - Makes sure the sequential process of packet message interchange involved in connection-oriented protocols (e.g. TCP – transmission control protocol) are properly synchronized and formatted
    - *If not an attack is detected and blocked*

Stateful Inspection example

Determine if all TCP Flags set to 1

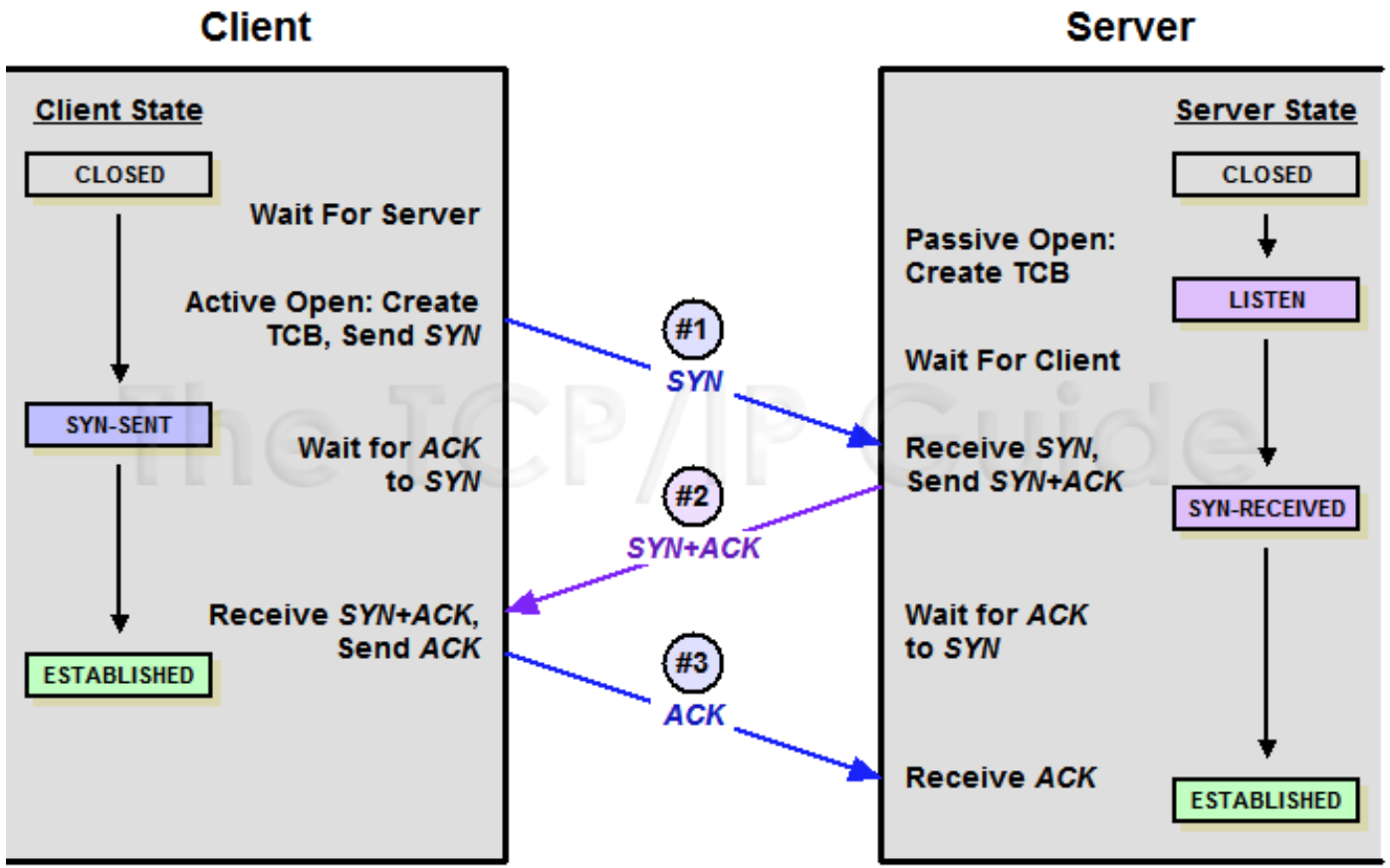
- Attackers send packets with all TCP flags set to 1 with hope that the firewall will not understand or check these values and forward them to the server
- Under no circumstances during legitimate TCP connections are all values turned to 1
- If detected connection is blocked



TCP Flags
CEUAPRSF
Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Stateful Inspection example

Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:



Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers

*Out of order acknowledgement and/or sequence numbers can imply a **replay attack** is underway and the firewall will protect internal systems from this activity*

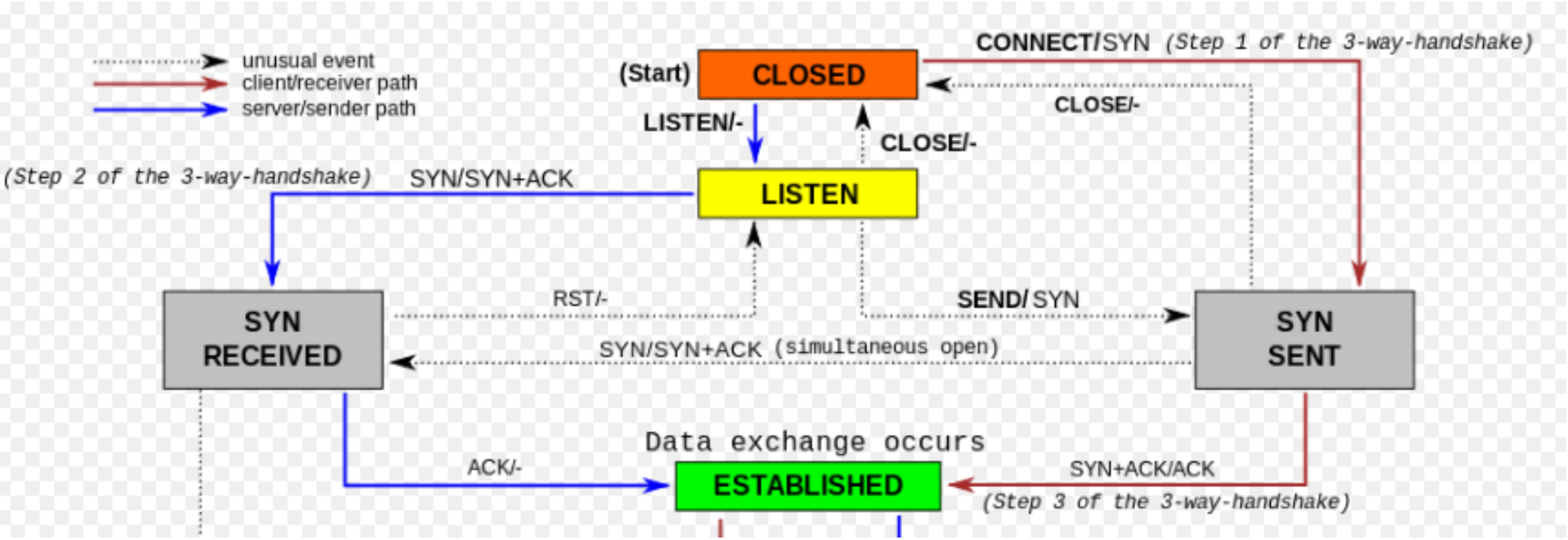
Stateful Inspection example

Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED

Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers

If a remote computer sends in a SYN/ACK packet without an internal computer first sending out a SYN packet, this is against protocol rules and the firewall will block the traffic



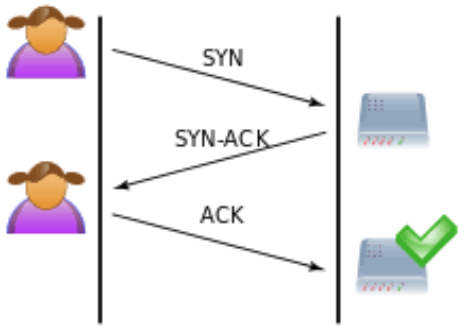
It knows how the protocols are supposed to work, and if something out of order (incorrect flag values, incorrect sequences, etc.) is detected the traffic is blocked

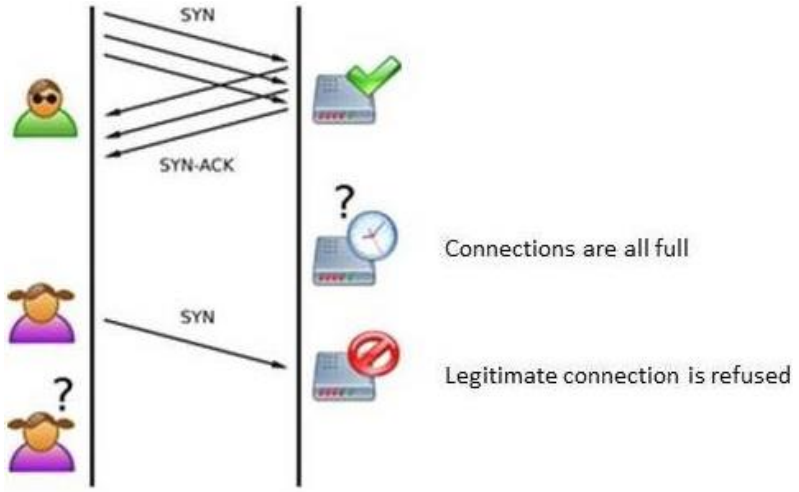
Stateful Inspection Firewalls

Strength: Maintains a state table that tracks each and every communication session to validate the session

- Provides high-degree of security, without introducing a huge performance hit
- Is scalable and transparent to users
- Tracks both connection-oriented protocols (e.g. TCP) and connectionless protocols (UDP and ICMP)

- **Weakness:** Succeptible to Denial of Service (DoS) attacks aided at flooding the state table with fake information
  - *Poorly designed stateful firewalls with state-tables filled with bogus information may freeze or reboot*

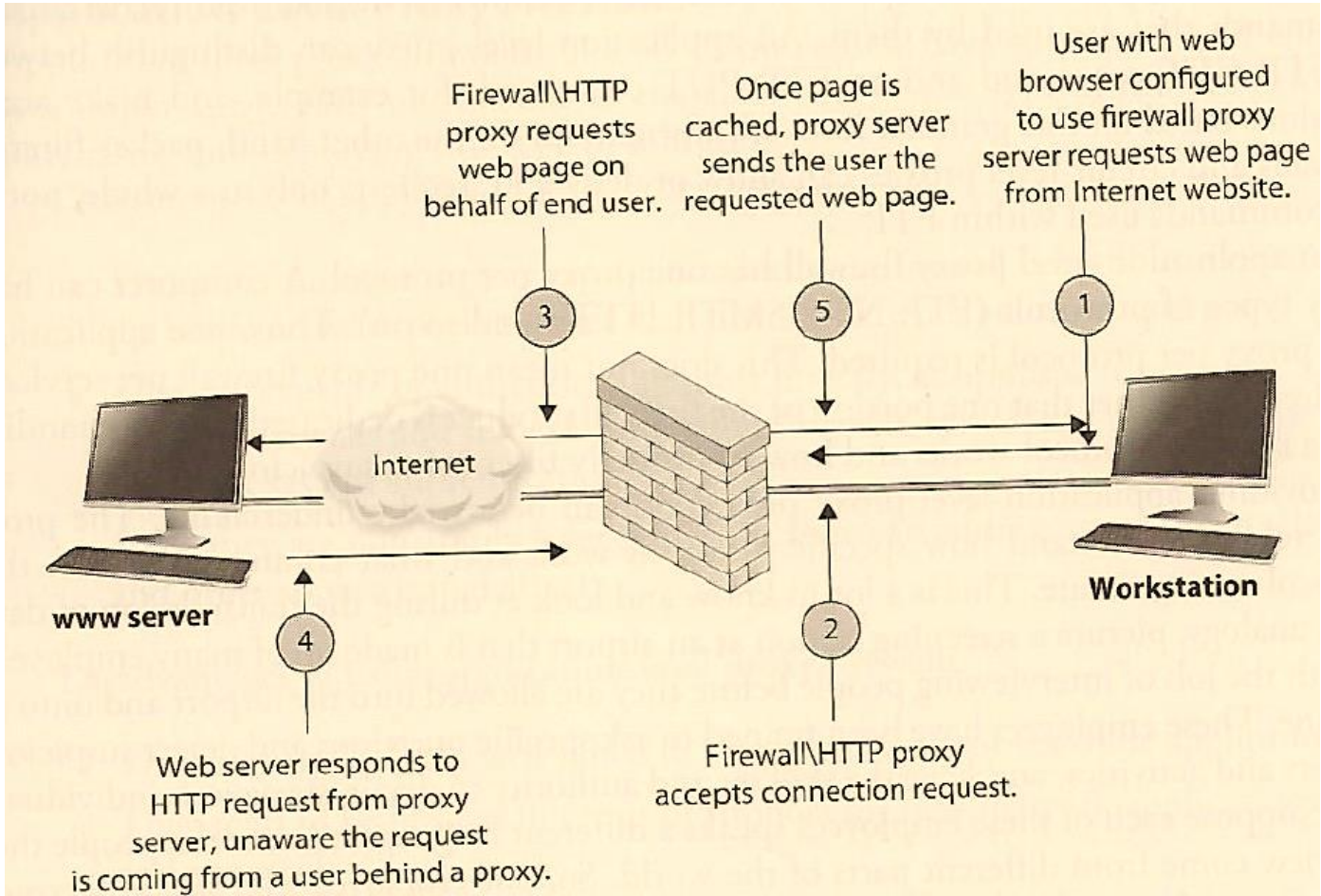




Proxy Firewall

- Is a “middleman” standing between a trusted and untrusted networks, denying end to end connectivity between source and destination computers – puts itself between the pair in both directions intercepting and inspecting each message before delivering it to the intended recipient

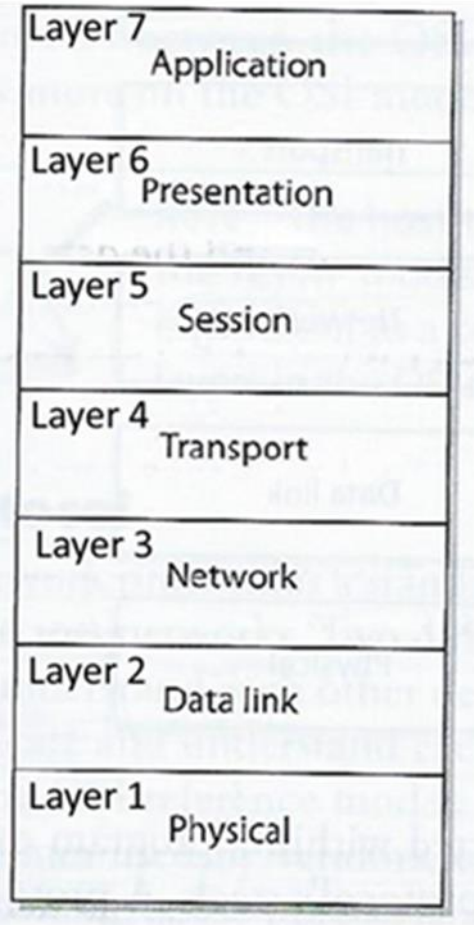
- Applies ACL rules, and also…
  - *Ends the communication session, breaking the communication channel between source and destination, so there is no direct connection between two communicating computers*
  - *Inspects the traffic*
  - *When traffic is “approved” the proxy firewall starts a new session from itself to the receiving system*



Proxy Firewall – two types working at different levels in the OSI model

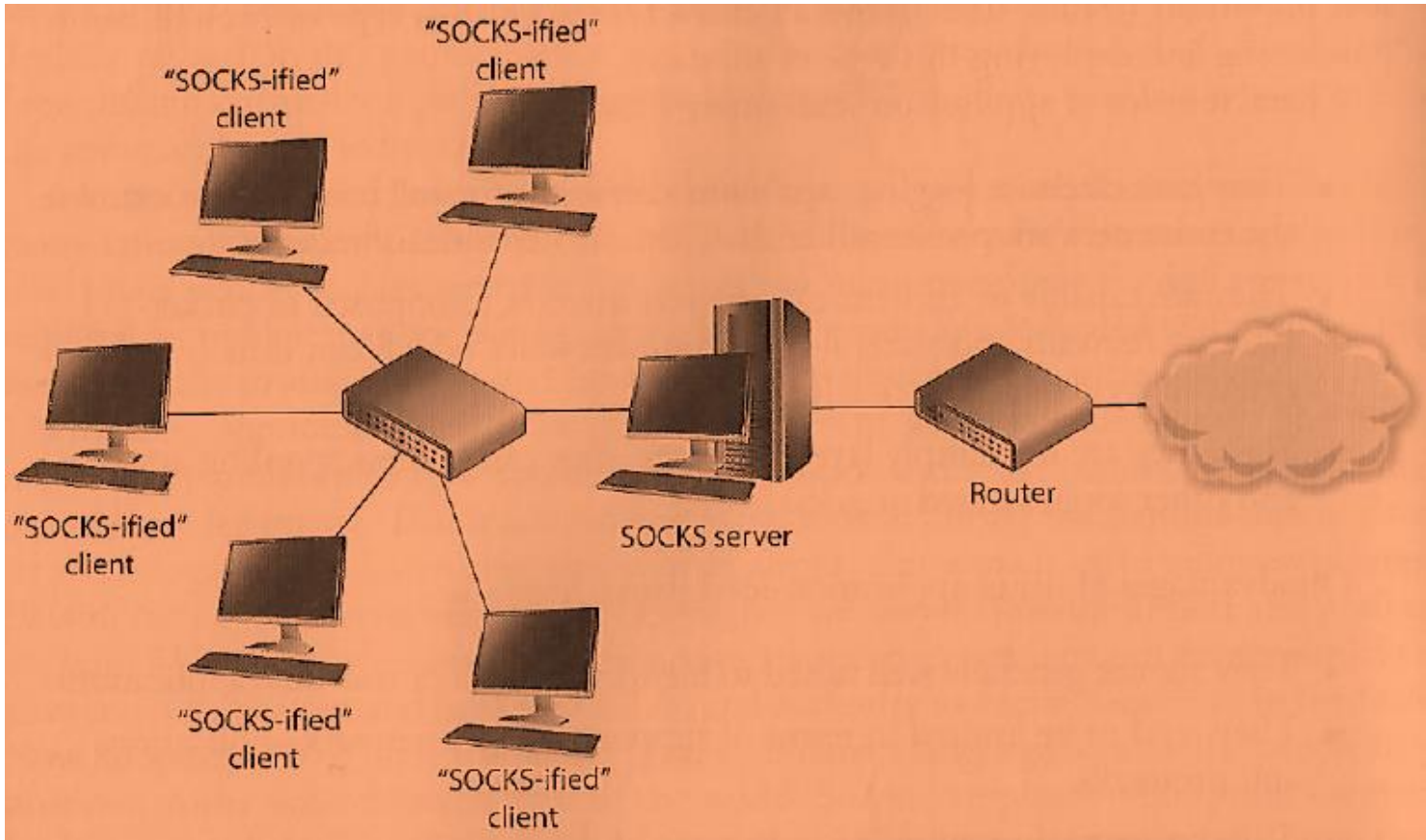
- **Circuit-level proxies** work at the lower levels of the OSI stack – up through the session layer
  - Creates a "circuit" connection between 2 computer systems
  - Cannot look into the contents of the packet to perform "deep inspection", does not understand application-level protocols and cannot determine if the packets are safe or unsafe
  - Works similar to a packet filter looking at header information, making decisions based on address, port and protocol header values

- **Application-level proxies** work up through the application layer
  - Understand entire contents of packets, making decisions based on API services, protocols and commands (e.g. FTP PUT and GET commands)
  - Each API protocol must have its own proxy able to understand the commands, how the protocol works, and how to detect suspicious data transmissions using the protocol
  - A Proxy Firewall will have a series of application-level proxies – one proxy per protocol (i.e. one for FTP, and different specific ones for NTP, SMTP, HTTP, …)



Circuit-level Proxy Firewalls

- Only examines network addresses and ports – similar to packet filtering firewalls, but provides proxy services insulating the internal identities and addresses of machines from external devices
- Can handle a much wider variety of protocols and services than an application proxy-level proxy firewall can
- Does not understand application-level protocols, and cannot provide more granular level control protecting from malicious transactions and content



Application-level Proxy Firewalls

Advantages

- Have extensive logging capabilities due to ability to examine contents of the entire network packet rather than just addresses and ports
- Capable of authenticating users directly
  - Packet-filtering and stateful-inspection firewalls only able to authenticate systems (not users)
- Functioning a higher levels in the OSI stack enable them to detect and address spoofing and other sophisticated attacks

Disadvantages

- May not be well suited for real-time or high-bandwidth applications
- Create performance issues due to processing needed to inspect and analyze “deep content” of packets
- Limited support for newer network applications and protocols

Application and Circuit Proxy Firewalls both

- Act as a proxy
- Deny actual end-to-end connectivity between the source and destination computers
- Clients attempting remote connection connects and communicates to the proxy; the proxy – in turn – establishes a connection to the destination system and makes requests to it on behalf of the client
- The proxy maintains 2 independent connections for every one network transmission, turning a 2-party session into a 4-party session – providing the middle processes emulating the 2 real systems

Application-level versus Circuit-level Proxy Firewalls

- **Application-level**
  - Need a unique proxy to monitor each API protocol
  - Provide more protection than circuit-level proxy firewalls
  - Require more processing per packet and are slower than circuit-level proxy firewalls
- **Circuit-level**
  - Provide security for a wider range of (lower level) protocols
  - Are more general purse as they function at lower levels in the OSI stack and do not require a proxy for each API protocol
  - Do not provide deep-inspection capabilities of an application-level proxy firewall

Kernal Proxy Firewalls

- Considered a “fifth generation” firewall
- Functions as a proxy – conducting network address translation so it function as a “middleman”
- Creates a dynamic, customized virtual network stacks for each packet that consists of only the protocol proxies needed to examine it
  - The packet is evaluated at every layer of the stack simultaneously
    - Data link header
    - Network header
    - Transport header
    - Session layer information
    - Application layer data
  - If anything is determined unsafe the packet is discarded
- Much faster than an application-level proxy because it is optimized to function at the lower level kernel level of the operating system

Next-Generation Firewalls (NGFW)

- Combines the best capabilities of the other firewalls
  - Ensures traffic is well-behaved and in accordance with applicable protocols
  - Breaks direct connection between internal and external systems (proxy)
  - Provides dynamic port assignment
- Also includes a signature-based Intrusion Detection System (IPS) engine
  - Able to look for specific indicators of attack even in traffic is well behaved
- Able to use centralized data sources
  - Able to be updated with new attack signatures from cloud aggregators
  - For consistent up to date whitelists, blacklists and policies
  - Can connect to Active Directory to provide URL to IP address translations
- Tend to be expensive – cost of ownership beyond small and medium sized organizations

Summary

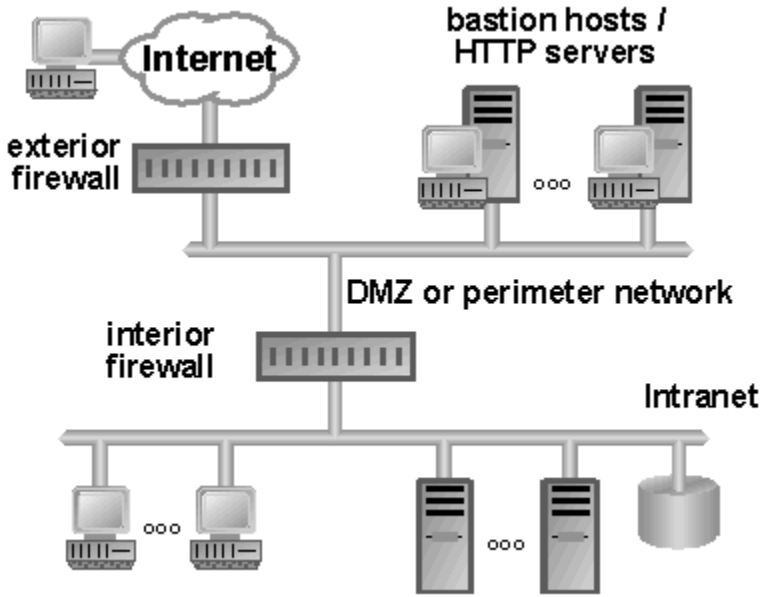
Firewall type	OSI Layer	Characteristics
Packet Filtering	Network Layer	Looks at destination and source addresses, ports, and services requested. Routers use ACLs monitor network traffic
Dynamic Packet Filtering	Network Layer	Allows any permitted type of traffic outbound and only response traffic inbound
Stateful	Network Layer	Looks at the state and context of packets. Keeps track of each conversation using state table
Circuit-level Proxy	Session Layer	Provides proxy services, but looks only at the header packet information (less detailed level of control that application-level proxy)
Application-level Proxy	Application Layer	Looks deep into packets and makes granular access control decisions, It requires one proxy per protocol
Kernal Proxy	Application Layer	Faster than application-level proxy because processing performed in operating system kernel. One network stack created for each packet
Next-generation	Multiple Layers	Very fast and supports high bandwidth. Built-in IPS, able to connect to external services like Active Directory

Main firewall architectures

1. Dual-homed Firewall
2. Screened host
3. Screened Subnet

Bastion Host

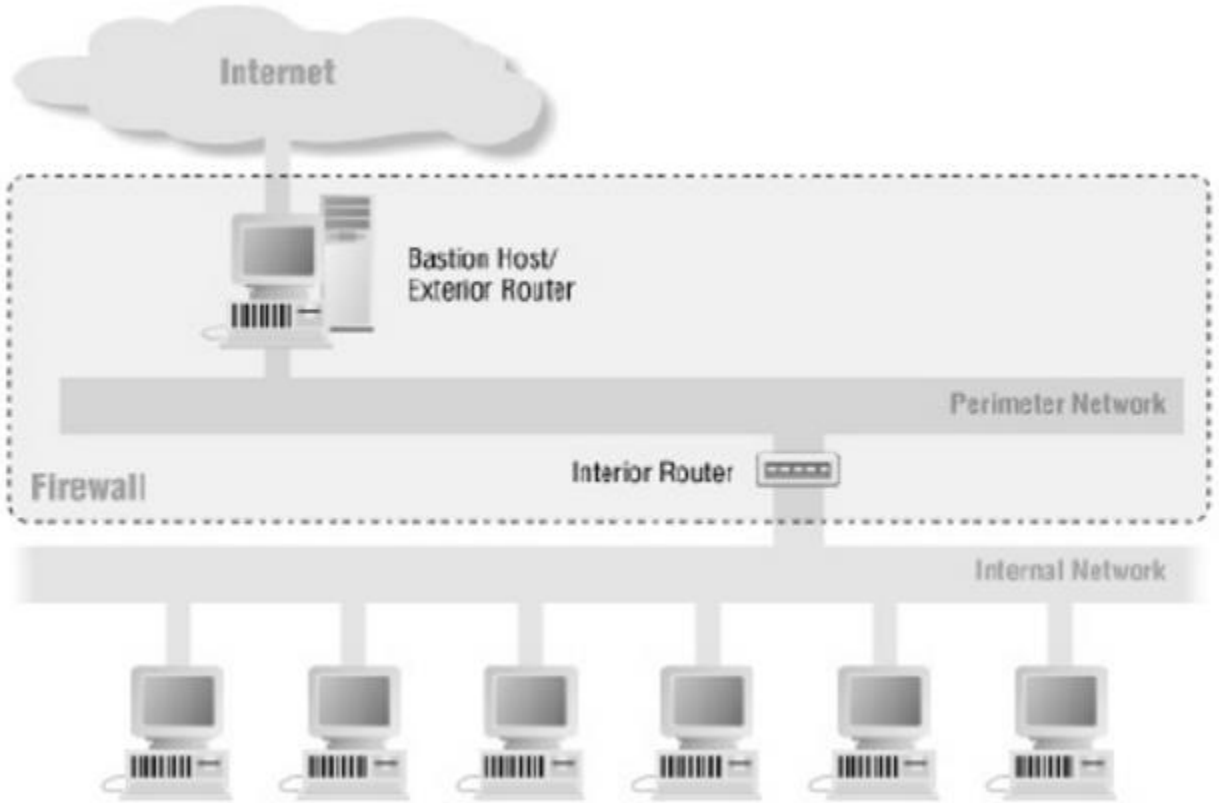
- Bastion host system is a highly exposed device closer than any other system to an untrusted network, that is most likely to be targeted by attacker
- Typically directly connected to an untrusted network, or placed on the public side of a DMZ
- Needs to be extremely locked down and hardened to reduce its attack surface (i.e. vulnerabilities reduced as much as possible):
  - All unnecessary:
    - Services disabled
    - Accounts removed
    - Applications removed
    - Subsystems and administrative tools removed



Dual-Homed Firewall Architecture

- A “dual-homed” device has two network interface cards (NICs)
  - Multi-homed devices have multiple NICs
- Firewall software running on a dual-homed device
  - Underlying operating system should have packet forwarding and routing turned off for security

- Packet comes to the external NIC from an untrusted network and is forwarded up through the firewall software and if not dropped forwarded to the internal NIC



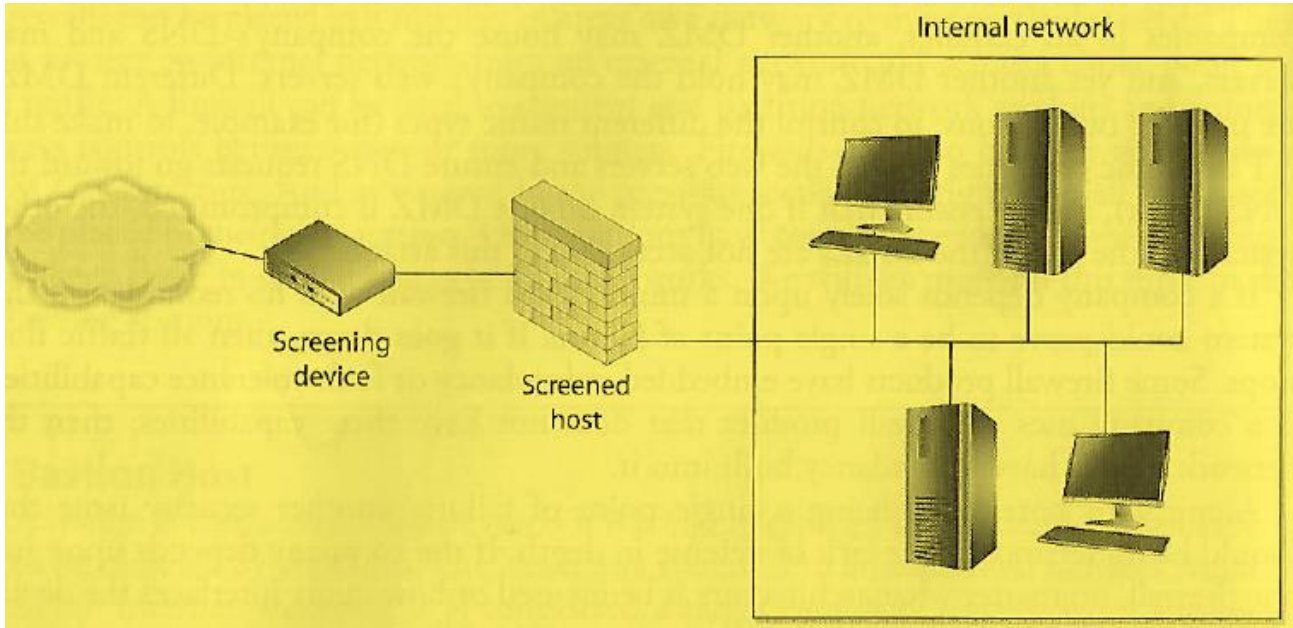
- Without redundancy, if this goes down the dual-homed firewall becomes a single point of failure
- On layer of protection lacks “defense in depth”
  If an attacker compromises one firewall they can gain direct access to the organizations network resources

Screened Host Firewall Architecture

- A firewall that communicates directly with a perimeter router and the internal network
  1. Traffic from the Internet first passes through a packet filtering router applying ACL rules which filters out (i.e. drops) junk packets
  2. Traffic that makes it past this phase is sent to the screen-host firewall which applies more rules to the traffic and drops the denied packets
  3. Remaining traffic moves to the internal network

- Router provides network-level packet filtering
- Application-based firewall provides packet filtering at the application layer
- Security level is higher than a bastion dual-homed firewall because attacker would need to compromise 2 systems to achieve success

"One-tier tiered configuration"



Screened Subnet Architecture

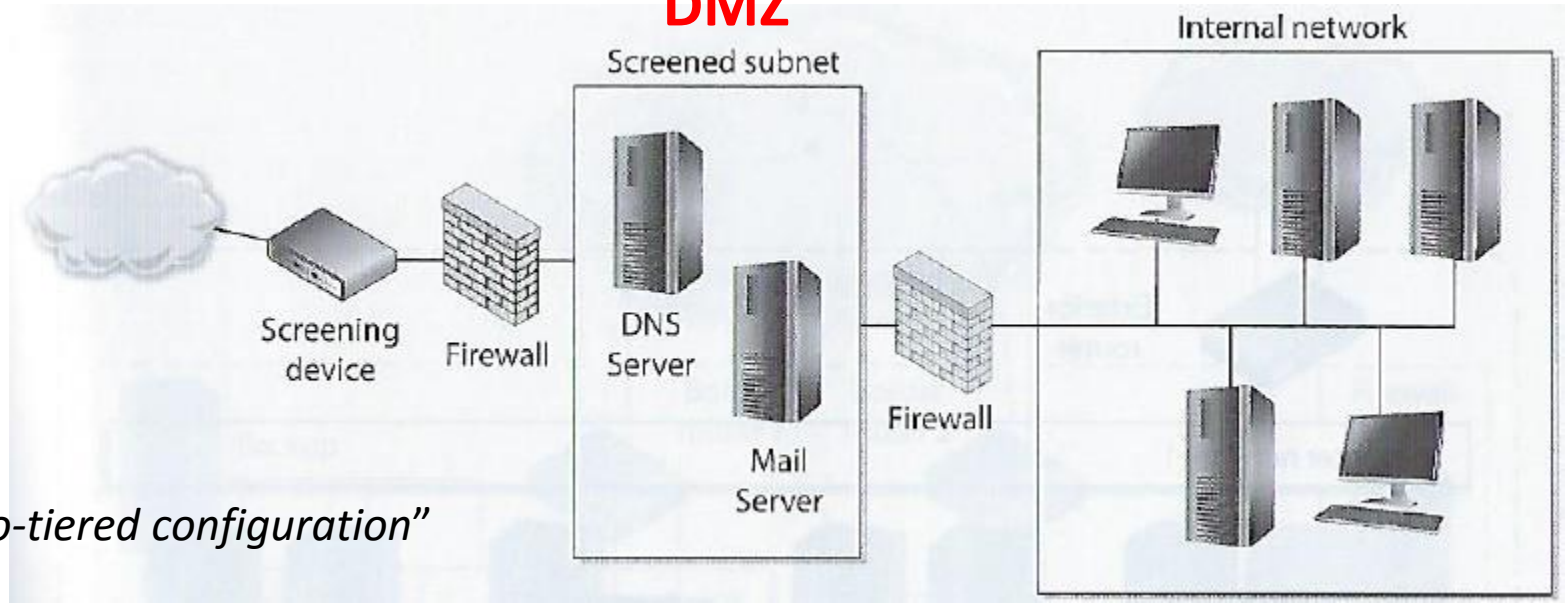
Adds another layer of depth to the security of the screened-host architecture

- The external firewall screens traffic entering the screened sub-network, instead of firewall redirecting traffic to the internal network
- The second interior firewall also filters the traffic – this creates a screened subnet (i.e. DMZ)

Creates a DMZ between 2 firewalls which functions as a small network isolated between trusted internal and untrusted external network

3-devices working together provides more protection than a stand-alone firewall or a screened-host firewall

All 3 need to be compromised by an attacker to gain access to the internal network



"Two-tiered configuration"

Characteristics of Firewall Architecture

- **Dual-homed**
  - A single computer with separate NICs connected to internal and external network
  - Used to divide an external untrusted network from an internal trusted network
  - Must harden and disable computer's forwarding and routing functionality so the two networks communicate through the computer's firewall software and are truly segregated
- **Screened host**
  - A router filters and screens traffic applying its ACL to drop 'junk' traffic before it is passed to the firewall
- **Screened subnet**
  - An external router filters/screens traffic before it enters the subnet, sending remaining traffic through two firewalls before making its way to the internal network

Good firewall behavior…

- The Firewall's ***default action is to deny*** any packets explicitly not allowed
  - If no rule in the ACL explicitly says the packet can come in, it is dropped
  - Any packet coming in from the Internet containing the source address of an internal host should be dropped
    - Spoofing or masquerading attack reflected in a modified packet header having the source address of a host inside the target network
  - No packet should be permitted to leave that does not contain a source address of an internal host – this is how DDoS zombies work
  - Many companies deny packets with source routing information in the headers which may circumnavigate internal routers and firewalls
- Firewalls ***not effective "out of the box"***
  - Need to understand internal default rules which may negate user provided rules
  - Can create bottlenecks
  - Need to effectively distribute them throughout the network to control network access points and provide appropriate "defense in depth"
  - Do not protect against malware, complex attack types, sniffers, rogue access points

Common firewall rules:

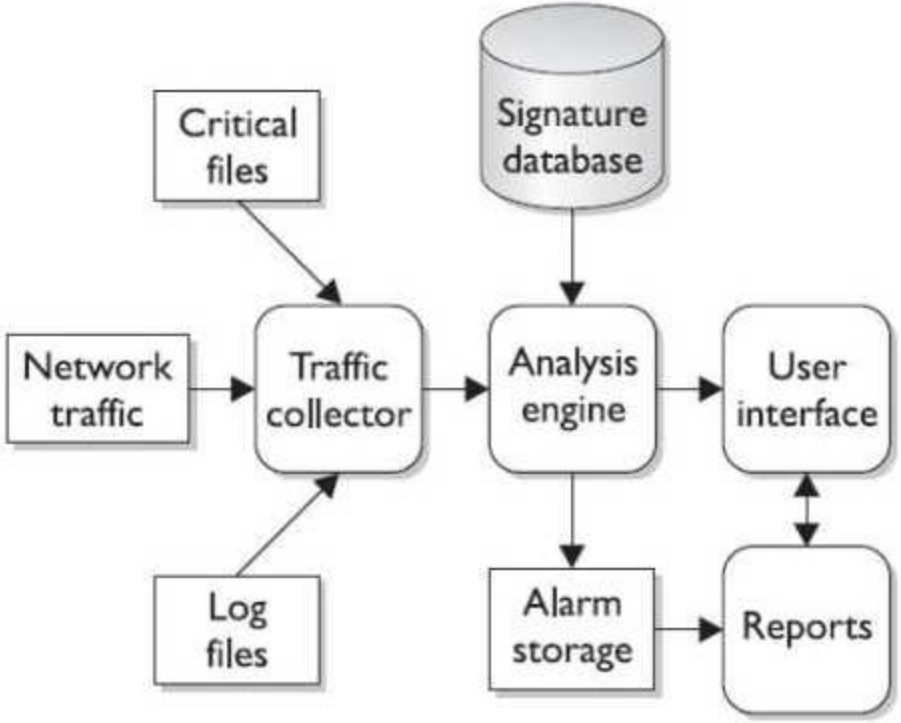
- Stealth rule
  - Disallow unauthorized systems from accessing to firewall software
- Silent rule
  - Identify and drop “noisy” traffic without logging it to reduce log sizes by not responding to unimportant packets
- Cleanup rule
  - Last rule in the rule base drops and logs remaining traffic that does not meet preceding rules
- Negate rule
  - Create tighter rules by specifying what system can be accessed and how (whitelisting), and do not use broad and permissive rules that default to any traffic (e.g. blacklisting)

Agenda

- **Firewalls**
- Intrusion Detection Systems
- Intrusion Prevention Systems

Intrusion Detection Systems (IDSs)

- While firewalls and antivirus are preventive controls, IDSs are access control monitoring devices designed to
  1. Detect a security breach
  2. Aid in mitigating damage caused by hackers breaking into sensitive computer and network systems
- IDS' components
  1. Sensors
     - Collect and send traffic and user activity data to analyzers
  2. Analyzers
     - Look for suspicious activity and if found sends alert to administrator's interface
  3. Administrative interfaces



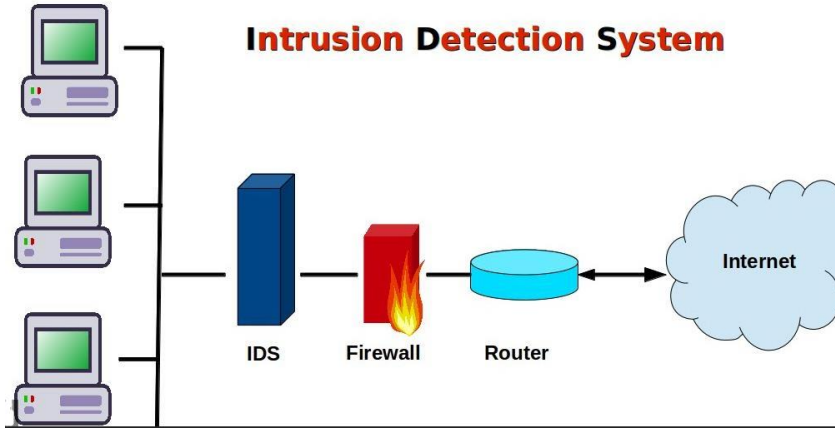
Intrusion Detection Systems (IDSs)

Two main types of IDS

1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

IDS can be configured to:

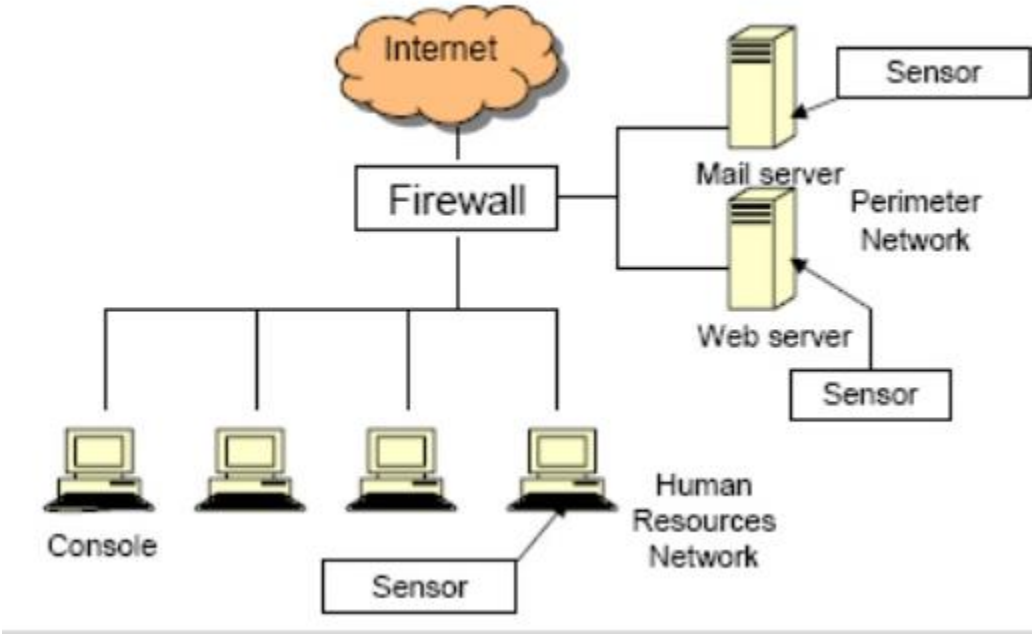
- Watch for attacks
- Parse audit logs
- Terminate a connection
- Alert administrator as attacks happen
- Expose a hacker and her/his techniques
- Illustrate which vulnerabilities need to be addressed



Intrusion Detection Systems (IDSs)

Host-based IDS (HIDS)

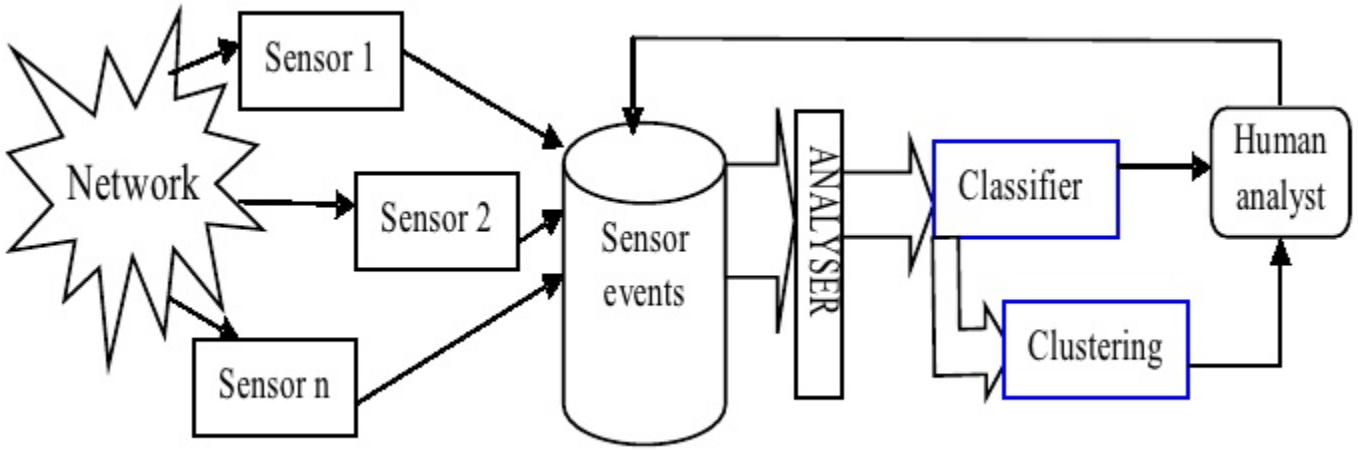
- Can be installed to look at the data packets within the higher levels of the OSI stack for anomalous or inappropriate activity on individual servers and/or workstations
- Usually installed on critical servers (too much administrative overhead to put them everywhere)
- Make sure users do not put the system at risk by activities such as deleting system files or reconfiguring important settings
- Does deeper inspection of the packets
- Does not understand network traffic



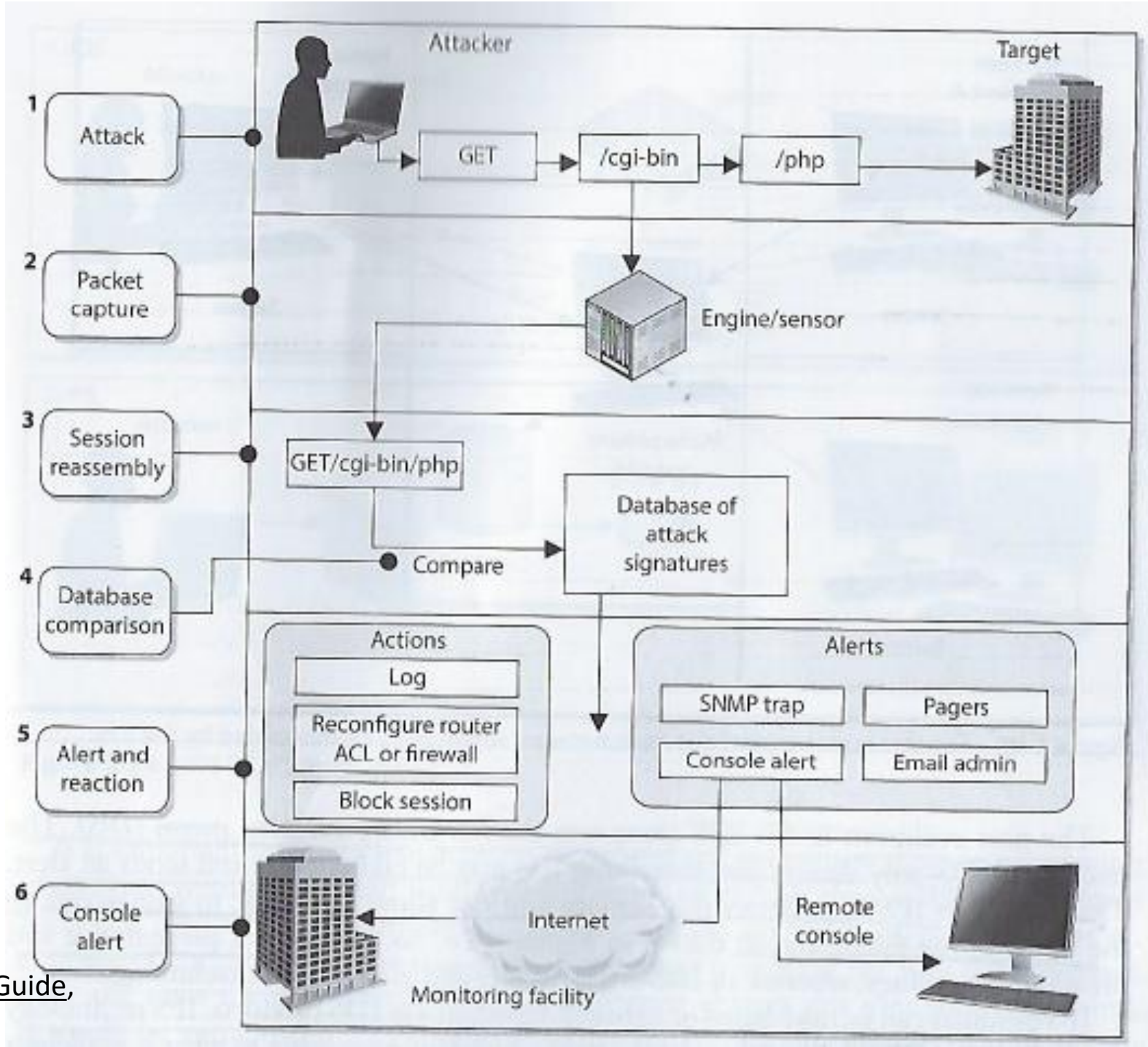
Intrusion Detection Systems (IDSs)

Network-based IDS (NIDS)

- Uses sensors which can be either host computers with specialized software installed or dedicated appliances
  - Each have a NIC (network interface card)
    - NIC is configured in promiscuous mode to capture all traffic (rather than packets addressed to the host computer
    - Copies packets – sending one copy up the TCP stack (for normal processing or possible analysis with a HIDS), and another copy to analyzer looking for specific patterns in the network traffic
- Monitors network traffic, cannot see the activity happening within the higher levels of the OSI stack (HIDS is used for this)

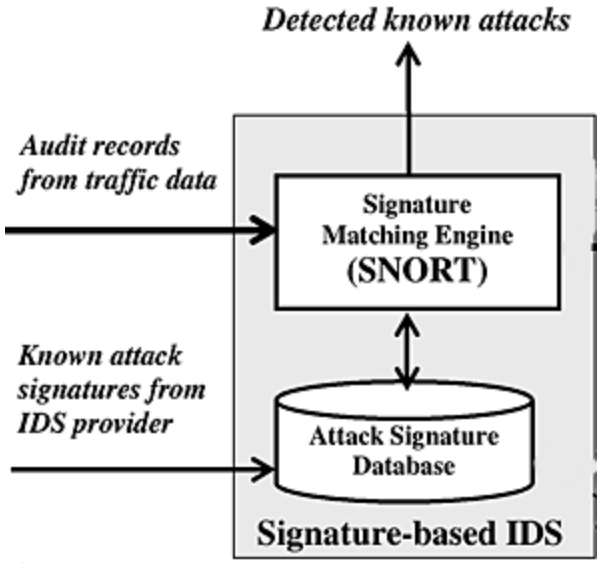


Basic architecture of a Network IDS



Harris, S. and Maymi, F. (2016) All In One CISSSP Exam Guide, Seventh Edition, McGraw-Hill Education

Intrusion Detection Systems (IDSs)



NIDS and HIDS can be one of the following types:

1. Signature-based:
   - Pattern matching, similar to antivirus software
   - Signatures must be continuously updated
   - Cannot identify new attacks
   - 2 types
     - Pattern matching: Compares individual packets to signatures
     - Stateful matching: Compares patterns among packets
2. Anomaly-based (a.k.a. Heuristic-based or Behavior-based):
   - Behavioral-based system able to learn from “normal activities”
   - Can detect new attacks
   - 3 Types:
     - Statistical anomaly-based – creates a normal profile used to compare sensed activities
     - Protocol anomaly-based – Identifies incorrect uses that violate protocols (e.g. TCP 3-way handshake)
     - Traffic anomaly-based – Identifies unusual activity in network traffic
3. Rule-based
   - Uses artificial intelligence expert systems that process rules in the form of “If *situation* then *action*” statements to identify combinations of activities within the data of the packets
     - *e.g. “IF a root user creates FileA AND FileB IN same directory and there is a call to Administrative ToolK THEN trigger alert”*
   - Cannot detect new attacks
   - The more complex the rules, the greater the need for processing power to support the software and hardware requirements so the IDS does not become a bottleneck and performance problem

Intrusion Prevention System (IPS)

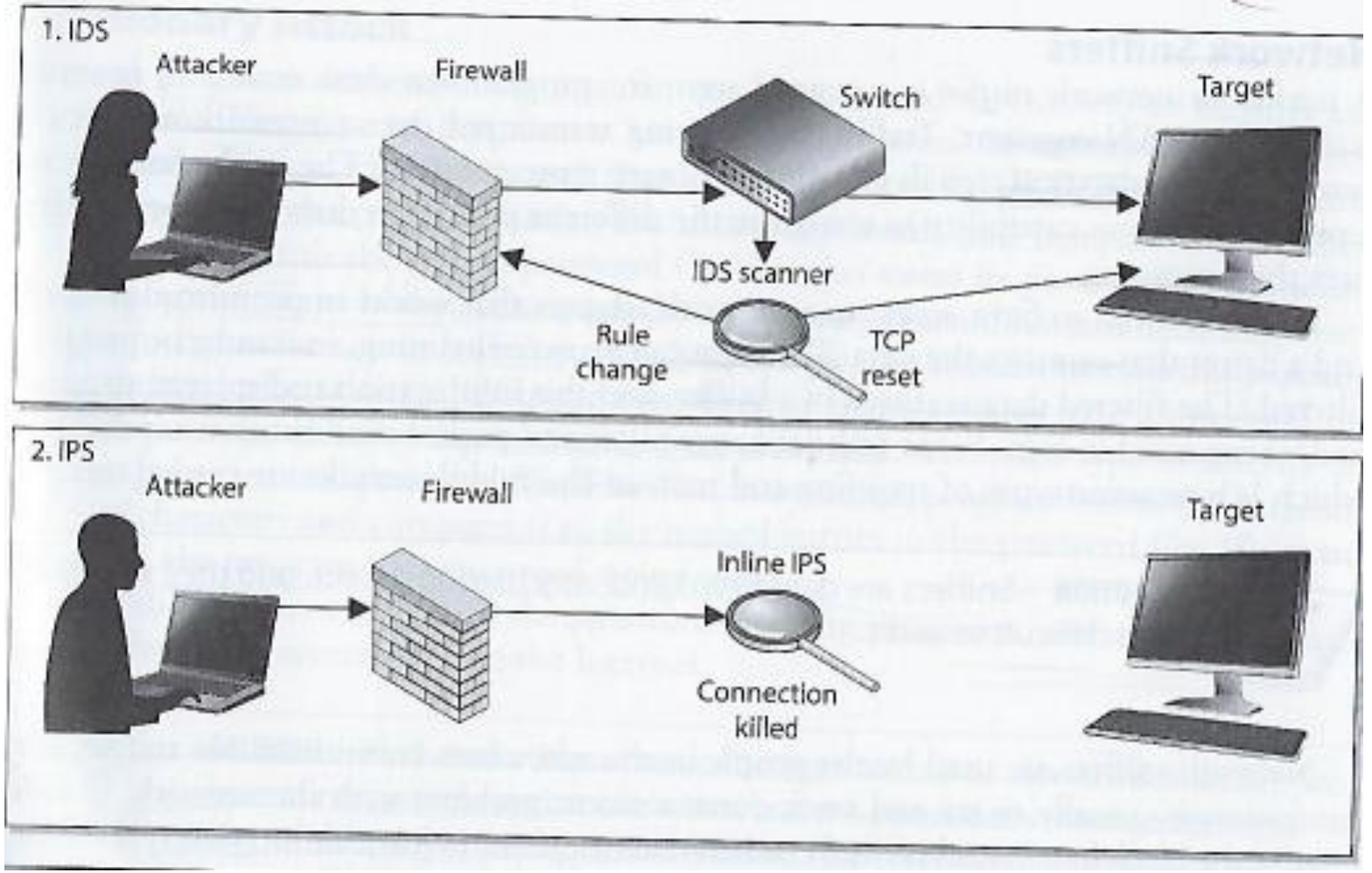
- IDS – Detect something bad may be taking place and send an alert
  - *Detective and "after the fact" response*
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
  - *Preventive and proactive response*

- *IPS can be host-based or network-based (like IDS)*
- *Can be content-based (looking deep into packets), conduct protocol analysis or be signature matching*
- *Also can use rate-based metrics to identify suspicious increases in volumes of traffic*
  - *E.g. DoS – flood attack*
  - *Traffic flow anomalies – "slow and low" stealth attack attempting to be undetected*

IDS versus IPS

Possible responses to a triggered event:

- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors and administrators



Agenda

- ✓Firewalls
- ✓Intrusion Detection Systems
- ✓Intrusion Prevention Systems