NETWORK SECURITY ESSENTIALS

BCA – IV

Credits – 4

Evaluations – 5

The course is designed to build an understanding of various network security components, protocols and creating the awareness about the issues due to security.

Pre-requisites: An understanding of Basic Computer Networking and security

UNIT 4

Network defense tools: Firewalls, VPNs, Intrusion Detection, and filters

SPHERES OF SECURITY

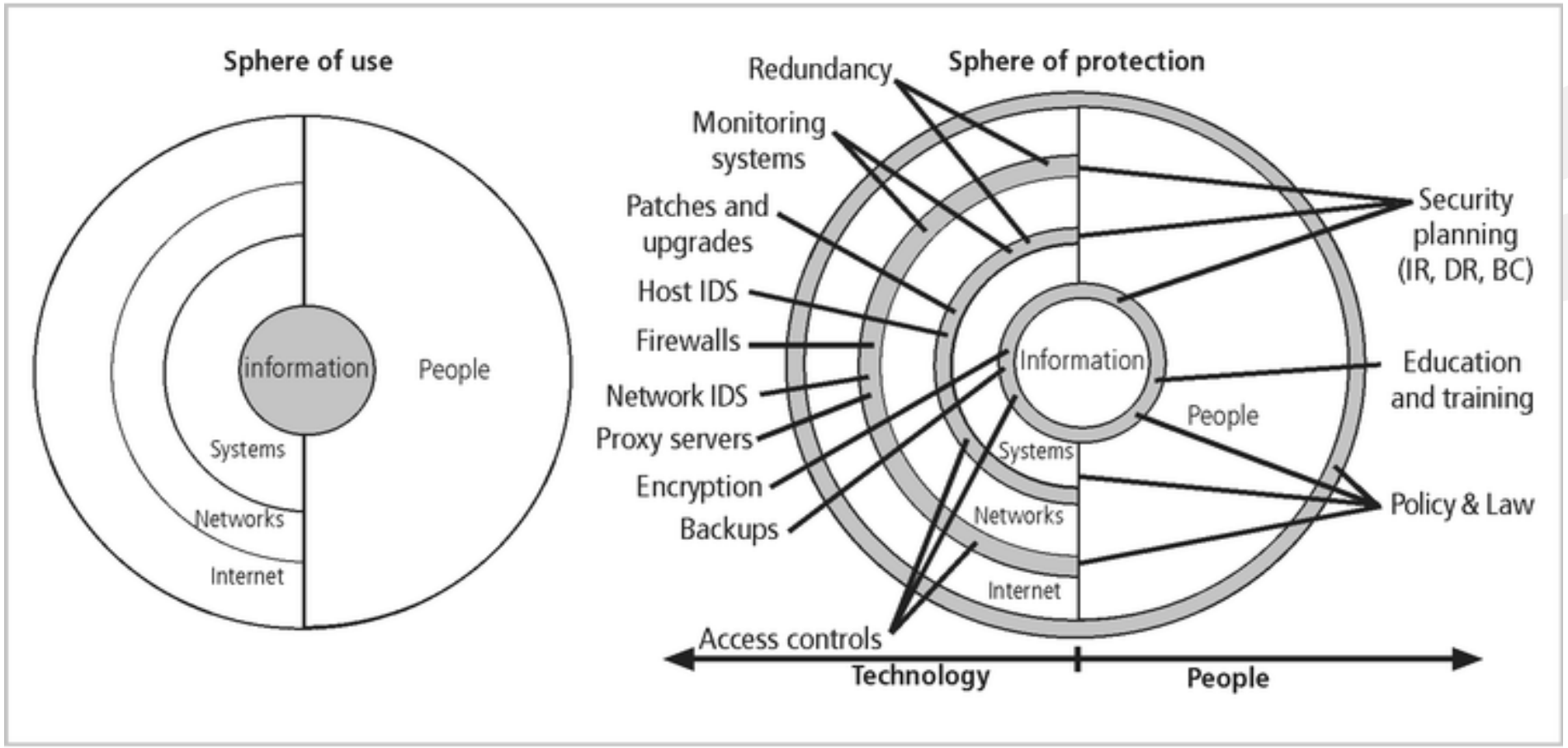


FIGURE 6-16 Spheres of Security

FIREWALLS

THE NATURE OF TODAY'S ATTACKERS

- Who are these "hackers" who are trying to break into your computer?

  Most people imagine someone at a keyboard late at night, guessing passwords to steal confidential data from a computer system.

  This type of attack does happen, but it makes up a very small portion of the total network attacks that occur.

  Today, worms and viruses initiate the vast majority of attacks. Worms and viruses generally find their targets randomly.

  As a result, even organizations with little or no confidential information need firewalls to protect their networks from these automated attackers.

WHAT IS A FIREWALL ?

- The term firewall has been around for quite some time and originally was used to define a barrier constructed to prevent the spread of fire from one part of a building or structure to another. Network firewalls provide a barrier between networks that prevents or denies unwanted or unauthorized traffic.

- **Definition**: A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted network -- using pre-configured rules or filters.

WHAT IS A FIREWALL ?

- Device that provides secure connectivity between networks (internal/external; varying levels of trust)
- Used to implement and enforce a security policy for communication between networks
- Firewalls can either be hardware and/or software based.

The terms "two-tier" and "three-tier" firewalls do not have a hard-and-fast definition. They are applied to two different ideas. First off (and in the most widely used terminology), the tiers refer to the number of interfaces the firewall has. A two-tier firewall would have two interfaces: the inside (protected) network and the outside (big, bad, scary) network. A three-tier firewall would have inside and outside as well, but also includes a side interface for a protected Demilitarized Zone (DMZ). On your DMZ, you can put servers that need to be publicly accessible (such as Web servers, mail servers and DNS servers), but also need to be protected.

DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well .

FIREWALLS HISTORY

- Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. The original idea was formed in response to a number of major internet security breaches, which occurred in the late 1980s.

FIREWALLS HISTORY

- First generation - packet filters
- The first paper published on firewall technology was in 1988, when Jeff Mogul from Digital Equipment Corporatin (DEC) developed filter systems known as packet filter firewalls.

- Second generation - circuit level
- From 1980-1990 two colleagues from AT&T Company, developed the second generation of firewalls known as circuit level firewalls.

- Third generation - application layer
- Publications by Gene Spafford of Purdue University, Bill Cheswick at AT&T Laboratories described a third generation firewall. also known as proxy based firewalls.

FIREWALLS HISTORY

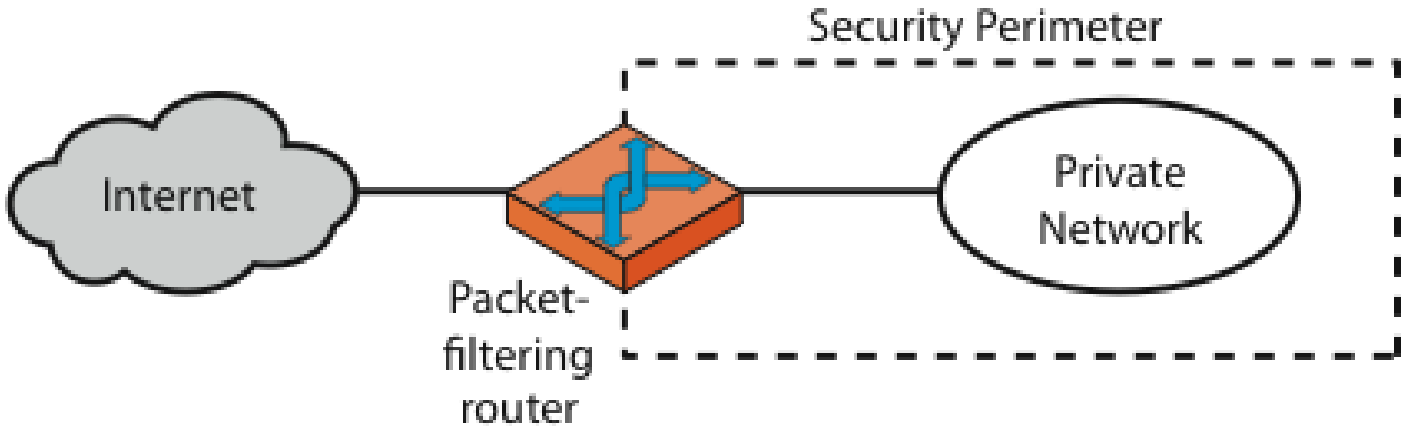
- Subsequent generations

- In 1992, Bob Braden and Annette DeSchon at the University of Southren California (USC) were developing their own fourth generation packet filter firewall system.

- In 1994 an Israeli company called Check Point Software Technologies built this into readily available software known as FireWall-1.

- Cisco, one of the largest internet security companies in the world released their PIX ” Private Internet EXchange ” product to the public in 1997.

FIREWALLS – PACKET FILTERS



(a) Packet-filtering router

FIREWALLS – PACKET FILTERS

- Simplest of components
- 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
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers

USAGE OF PACKET FILTERS

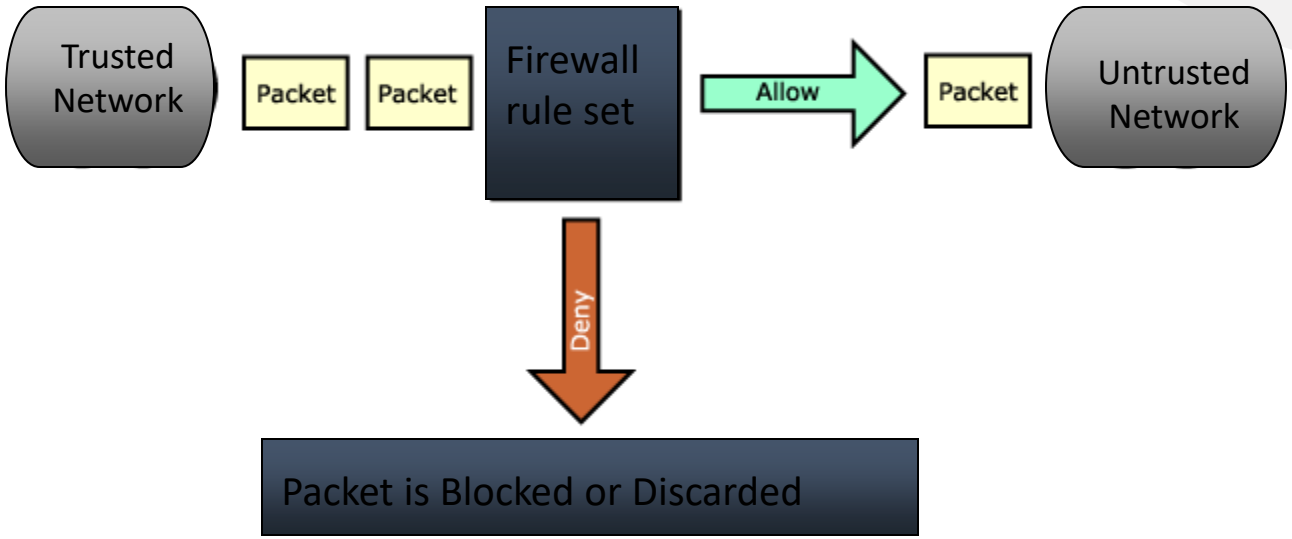
- Filtering with incoming or outgoing interfaces
  - E.g., Ingress filtering of spoofed IP addresses
  - Egress filtering
- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems

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 FILTERING FIREWALL

Packet Filtering Firewall



Every ruleset is followed by an implicit rule reading like this.

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

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.

Solution 1:

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

Example 2:

Now suppose that we want to implement the policy "any inside host can send mail to the outside".

Solution 2:

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

This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside. Simple enough…

So why is it wrong?

- Our defined restriction is based solely on the outside host’s port number, which we have no way of controlling.
- Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.

What can be a better solution ?

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

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

PACKET FILTERING

Strengths :

- Packet filtering is typically faster than other packet screening methods. Because packet filtering is done at the lower levels of the OSI model, the time it takes to process a packet is much quicker.

- Packet filtering firewalls can be implemented transparently. They typically require no additional configuration for clients.

- Packet filtering firewalls are typically less expensive. Many hardware devices and software packages have packet filtering features included as part of their standard package.

PACKET FILTERING

Weaknesses

- Packet filtering firewalls allow a direct connection to be made between the two endpoints. Although this type of packet screening is configured to allow or deny traffic between two networks, the client/server model is never broken.

- Packet filtering firewalls are fast and typically have no impact on network performance, but it's usually an all-or-nothing approach. If ports are open, they are open to all traffic passing through that port, which in effect leaves a security hole in your network.

- Defining rules and filters on a packet filtering firewall can be a complex task.

PACKET FILTERING (WEAKNESSES)

- Packet filtering firewalls are prone to certain types of attacks. Since packet inspection goes no deeper than the packet header information, There are three common exploits to which packet filtering firewalls are susceptible.

  - These are IP spoofing
    sending your data and faking a source address that the firewall will trust

  - ICMP ”Internet Control Message Protocol” tunneling
    ICMP tunneling allows a hacker to insert data into a legitimate ICMP packet.

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

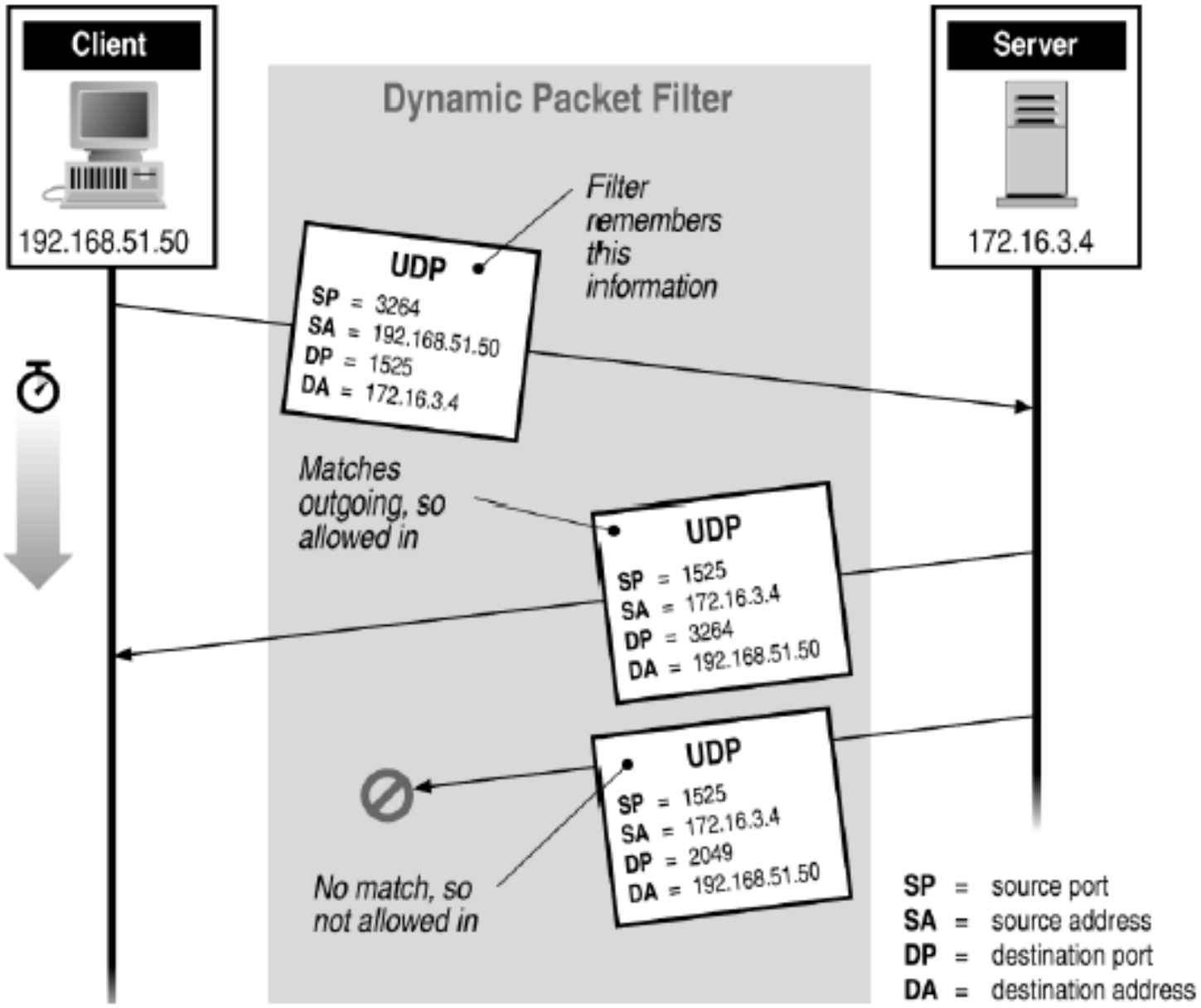
PORT NUMBERING

- TCP connection
  - Server port is number less than 1024
  - Client port is number between 1024 and 16383
- Permanent assignment
  - Ports <1024 assigned permanently
    - 20,21 for FTP 23 for Telnet
    - 25 for server SMTP 80 for HTTP
- Variable use
  - Ports >1024 must be available for client to make any connection
  - This presents a limitation for stateless packet filtering
    - If client wants to use port 2048, firewall must allow *incoming* traffic on this port
  - Better: stateful filtering knows outgoing requests

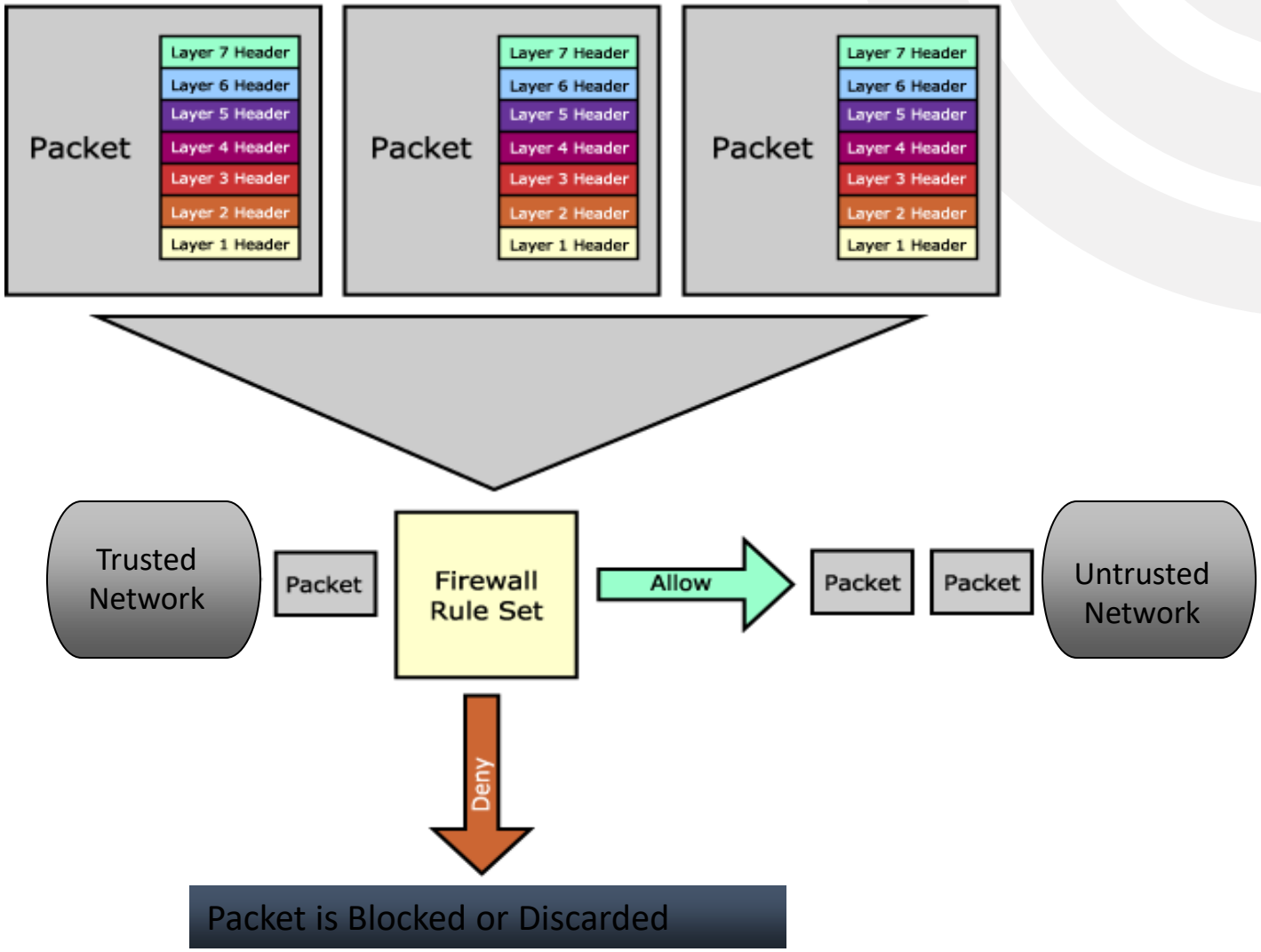
FIREWALLS – STATEFUL PACKET FILTERS

- Traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- Stateful packet filters address this need
- They examine each IP packet in context
  - Keep track of client-server sessions
  - Check each packet validly belongs to one
- Hence are better able to detect bogus packets out of context

STATEFUL FILTERING



STATEFUL PACKET INSPECTION FIREWALL



Firewall Outlines

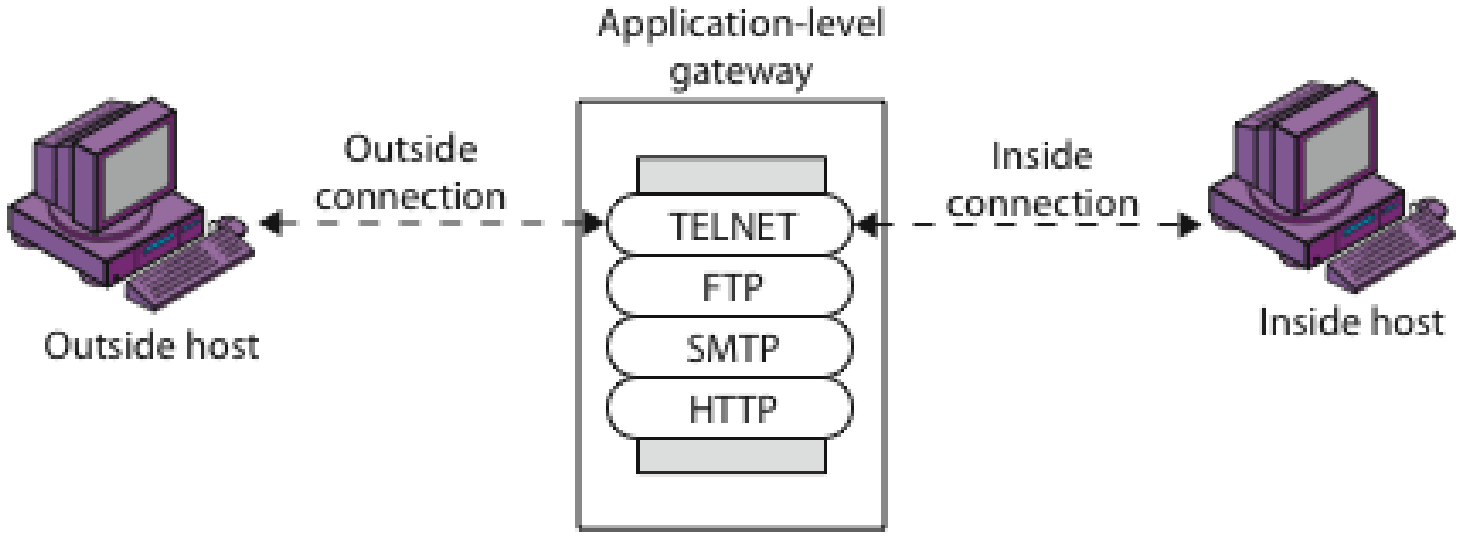
- Packet filtering
- Application gateways
- Circuit gateways

- Combination of above is dynamic packet filter

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
  - Application-level gateways/proxies
    - Tailored to http, ftp, smtp, etc.
  - Circuit-level gateways/proxies
    - Working on TCP level

FIREWALLS - APPLICATION LEVEL GATEWAY (OR PROXY)

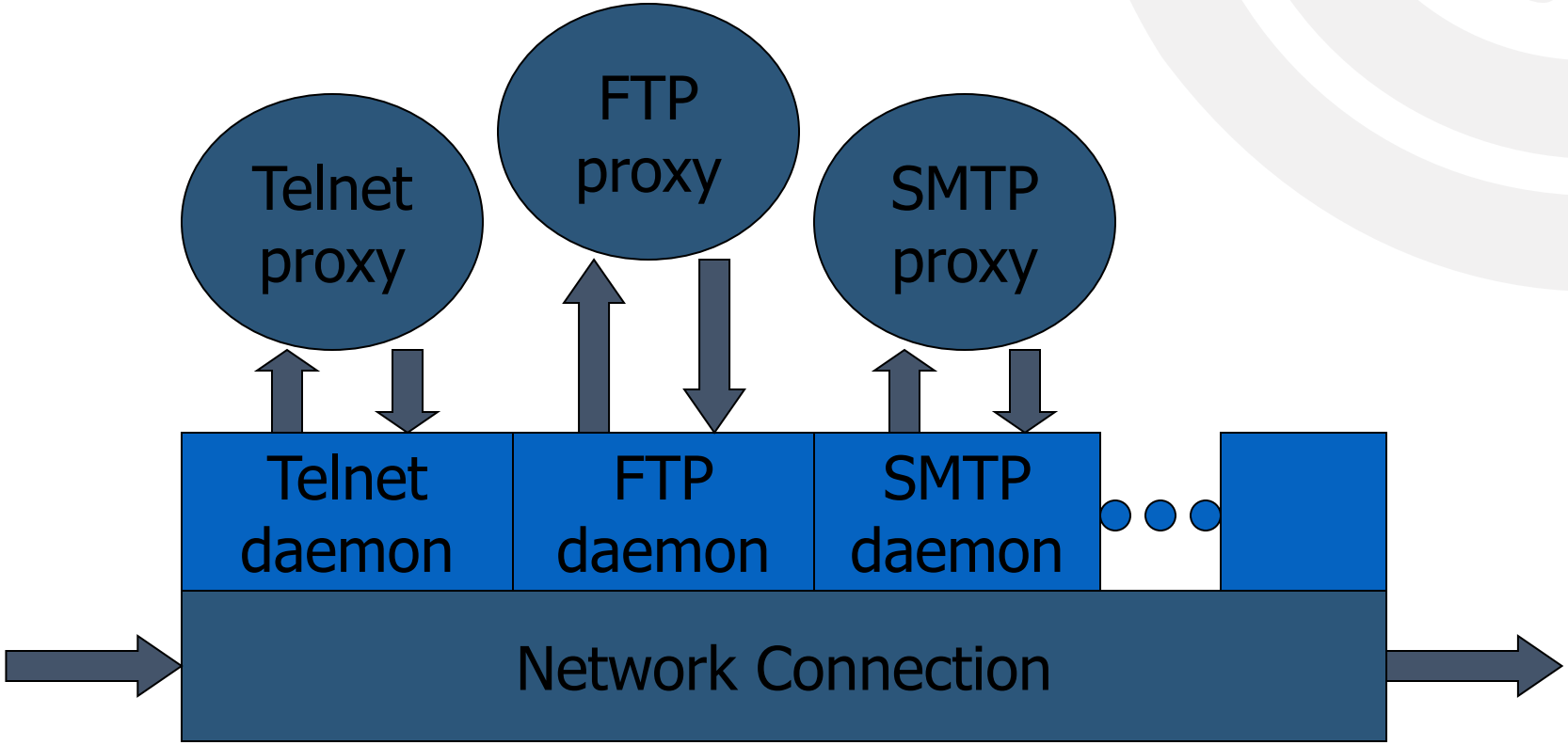


(b) Application-level gateway

APPLICATION-LEVEL FILTERING

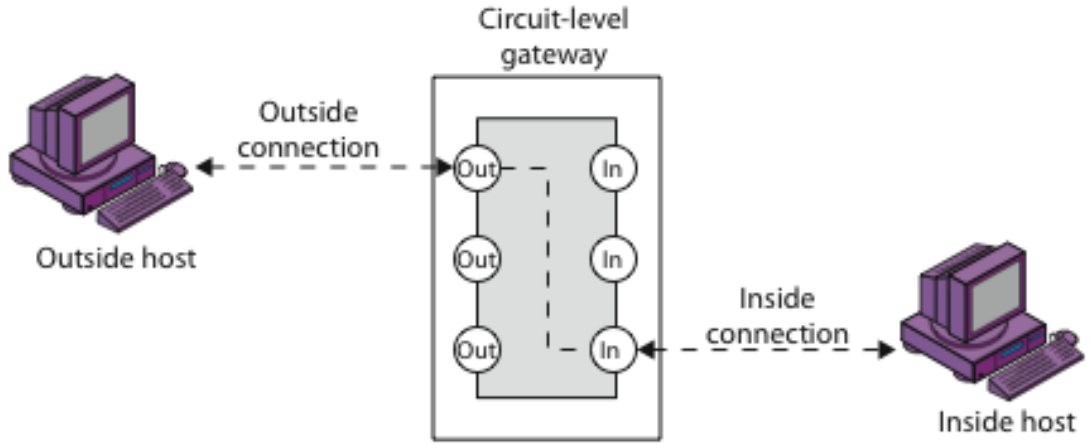
- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)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

APP-LEVEL FIREWALL ARCHITECTURE



Daemon spawns proxy when communication detected …

FIREWALLS - CIRCUIT LEVEL GATEWAY



(c) Circuit-level gateway

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies.

CIRCUIT-LEVEL GATEWAY

- Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions.

  Once a session has been established, it leaves the port open to allow all other packets belonging to that session to pass. The port is closed when the session is terminated.

  circuit-level gateways operate at the transport layer (layer 4) of the OSI model.

APPLICATION GATEWAYS/PROXIES FIREWALL

- The response is sent back to the application gateway/proxy, which determines if it is valid and then sends it on to the client.
- By breaking the client/server model, this type of firewall can effectively hide the trusted network from the untrusted network.
- It is important to note that the application gateway/proxy actually builds a new request, only copying known acceptable commands before sending it on to the destination.
- Unlike packet filtering and stateful packet inspection, an application gateway/proxy can see all aspects of the application layer so it can look for more specific pieces of information

APPLICATION GATEWAYS/PROXIES

Strengths

- Application gateways/proxies do not allow a direct connection to be made between endpoints. They actually break the client/server model.
- Typically have the best content filtering capabilities. Since they have the ability to examine the payload of the packet, they are capable of making decisions based on content.
- Allow the network administrator to have more control over traffic passing through the firewall. They can permit or deny specific applications or specific features of an application.

APPLICATION GATEWAYS/PROXIES

Weaknesses

- The most significant weakness is the impact they can have on performance.

  it requires more processing power and has the potential to become a bottleneck for the network.

- Typically require additional client configuration. Clients on the network may require specialized software or configuration changes to be able to connect to the application gateway/proxy.

To help you visualize the difference between a circuit-level gateway and other firewalls, here's a small chart of different firewall types:

Feature	Packet-Filtering Firewalls	Circuit-Level Gateways	Stateful Inspection Firewalls	Application-Level Gateways (Proxy Firewall)
Destination/IP Address Check	Yes	No	Yes	Yes
TCP Handshake Check	No	Yes	Yes	Yes
Deep-Layer Inspection	No	No	No	Yes
Virtualized Connection	No	No	No	Yes
Resource Impact	Minimal	Minimal	Small	Moderate

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 FIREWALLS DO (POSITIVE EFFECTS)

- Positive Effects

- User authentication.
- Firewalls can be configured to require user authentication. This allows network administrators to control, track specific user activity.

- Auditing and logging.
- By configuring a firewall to log and audit activity, information may be kept and analyzed at a later date.

WHAT FIREWALLS DO (POSITIVE EFFECTS)

- Anti-Spoofing - Detecting when the source of the network traffic is being "spoofed", i.e., when an individual attempting to access a blocked service alters the source address in the message so that the traffic is allowed.

- Network Address Translation (NAT) - Changing the network addresses of devices on any side of the firewall to hide their true addresses from devices on other sides. There are two ways NAT is performed:

- One-to-One - where each true address is translated to a unique translated address.
- Many-to-One - where all true addresses are translated to a single address, usually that of the firewall.

WHAT FIREWALLS DO (NEGATIVE EFFECTS)

Negative Effects

Although firewall solutions provide many benefits, negative effects may also be experienced.

- Traffic bottlenecks. By forcing all network traffic to pass through the firewall, there is a greater chance that the network will become congested.

- Single point of failure. In most configurations where firewalls are the only link between networks, if they are not configured correctly or are unavailable, no traffic will be allowed through.

WHAT FIREWALLS DO (NEGATIVE EFFECTS)

- **Increased management responsibilities.** A firewall often adds to network management responsibilities and makes network troubleshooting more complex.

- Many organizations need to use multiple firewalls to create strong network segmentation for a “defense in depth” strategy. Using firewalls with conflicting rules can cause legitimate traffic to be dropped, resulting in poor network performance and inefficiency.

WHAT FIREWALLS CANNOT DO

- The most common misconception about firewalls is that they guarantee security for your network.
- A firewall cannot and does not guarantee that your network is 100% secure.
- Firewalls cannot offer any protection against inside attacks. A high percentage of security incidents today come from inside the trusted network.

WHAT FIREWALLS CANNOT DO

- In most implementations, firewalls cannot provide protection against viruses or malicious code. Since most firewalls do not inspect the payload or content of the packet, they are not aware of any threat that may be contained inside.

- Finally, no firewall can protect against inadequate or mismanaged policies.

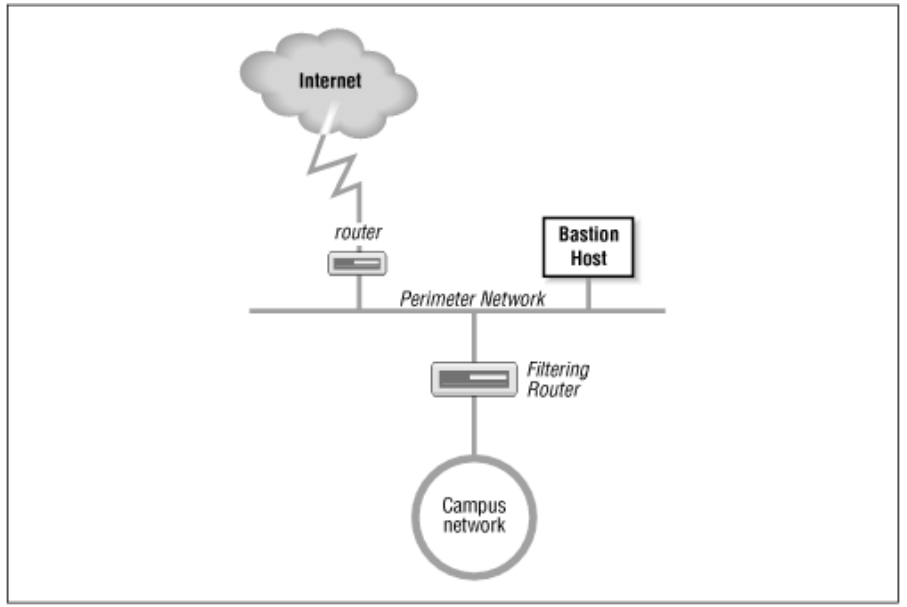
TYPES OF FIREWALLS

With regard to the scope of filtered communications the done between a single node and the network, or between two or more networks there exist :

- Personal Firewalls, a software application which normally filters traffic entering or leaving a single computer.
- Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks.

SCREENED SUBNET OR DEMILITARIZED ZONE (DMZ)

- Created between two packet filtering routers.
- The exterior router is the only connection between the enterprise network and the outside world
- The interior router does the bulk of the access control work. It filters packets
- The bastion host is a secure server. It provides an interconnection point between the enterprise network and the outside world for the restricted services
- The perimeter network connects the servers together and connects the exterior router to the interior router



DO YOU NEED A FIREWALL?

- The decision to implement a firewall solution should not be made without doing some research and analysis.

- **What does the firewall need to control or protect?**

  In order to make a sound decision, first identify what functions the firewall would need to perform. Will it control access to and from the network, or will it protect services and users?

  - What would the firewall control?
    - Access into the network
    - Access out of the network
    - Access between internal networks, departments, or buildings
    - Access for specific groups, users or addresses
    - Access to specific resources or services

DO YOU NEED A FIREWALL?

- **What would it need to protect?**
    - Specific machines or networks
    - Specific services
    - Information - private or public
    - Users

DO YOU NEED A FIREWALL?

- **What impact will a firewall have on your organization, network and users?**
  - What resources will be required to implement and maintain a firewall solution?
  - Who will do the work? Are experienced technical personnel available for the job or will someone need to be hired from outside your organization?
  - Is hardware available that meets the requirements to support a firewall solution?
  - Will existing services be able to function through a firewall?
  - What will the financial impact be on the organization? (Financial impact should include initial implementation costs, ongoing maintenance and upgrades, hardware and software costs, and technical support costs, whether the support is provided in-house or from an outside source.)

SECURITY POLICY

The success of any firewall solution's implementation is directly related to the existence of a well-thought-out and consistently-implemented security policy.

Some of the topics a security policy may address are:

- **Administrative Issues**

  - User access - Which users will be allowed access to and from the network?
  - Access to services - Which services will be allowed in and out of the network?
  - Access to resources - Which resources will be available to users?
  - User authentication - Will the organization require user authentication?
  - Logging and auditing - Will the organization want to keep log and audit files.
  - Policy violation consequences - What will be the consequences of policy violation?
  - Responsibilities - Who will oversee and administer the security policy? Who has final authority on decisions?

SECURITY POLICY

- **Technical Issues**
  - Remote access - Will the organization allow remote access to the network?
  - Physical security - How will physical security of machines, one of the most obvious security elements that is often overlooked, be achieve?
  - Virus protection - How will the organization handle virus protection?

INTRUSION DETECTION SYSTEMS - IDS

WHAT IS AN INTRUSION DETECTION SYSTEM?

- Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
- An IDS detects activity in traffic that may or may not be an intrusion.
- IDSes can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.

HOST BASED INTRUSION DETECTION

- Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
- It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.
- Host-based IDS are often critical in detecting internal attacks directed towards an organization’s servers such as DNS, Mail, and Web Servers.

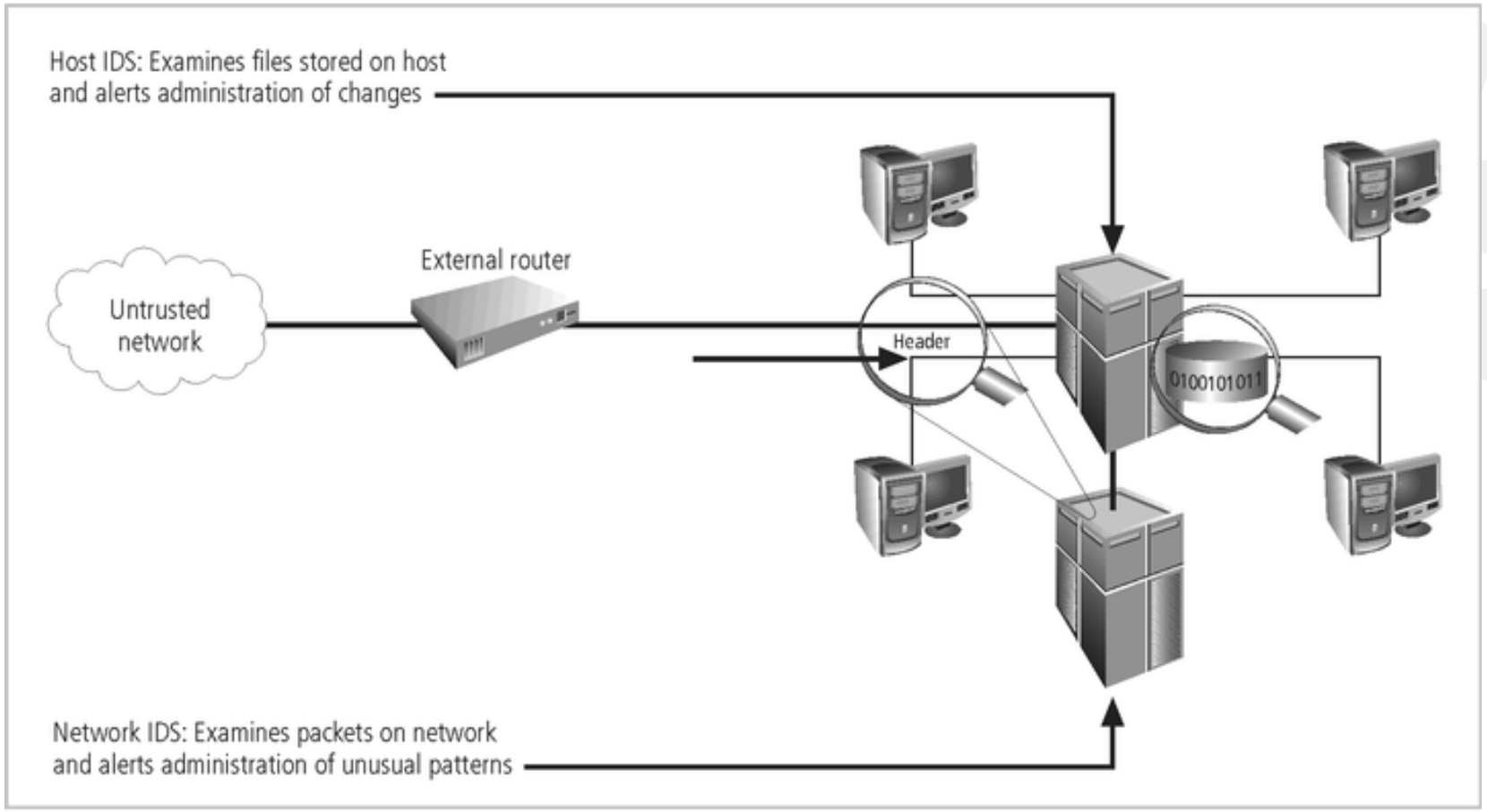


FIGURE 6-21 Intrusion Detection Systems

NETWORK BASED INTRUSION DETECTION

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
- Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
- Most Network-based IDS log their activities and report or alarm on questionable events.
- Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall.

HYBRID INTRUSION DETECTION

- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
- A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
- A Hybrid IDS is often deployed on an organization's most critical servers.

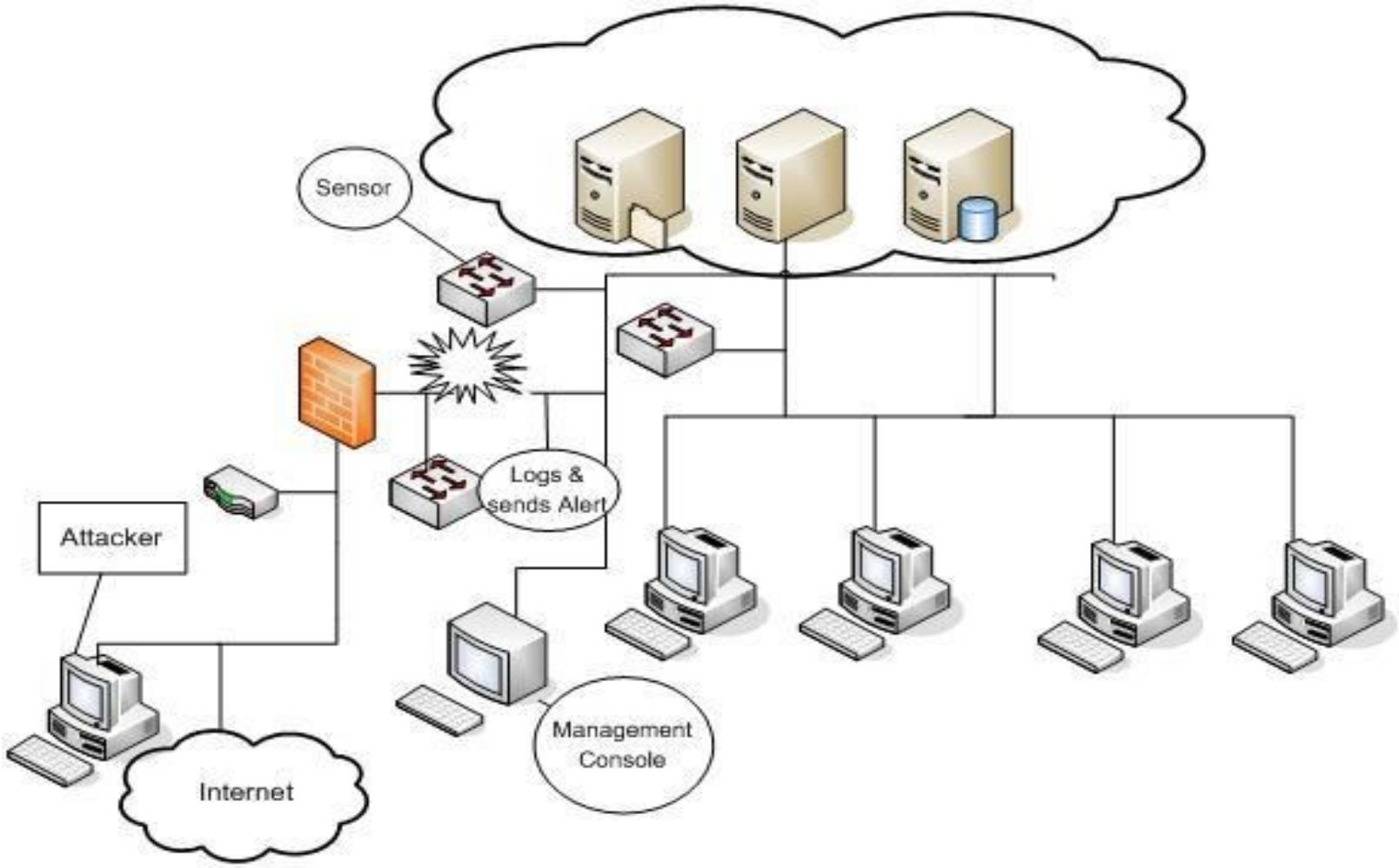
HONEYPOTS

- Are decoy servers or systems setup to gather information regarding an attacker of intruder into networks or systems.
- Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.
- Provide you early warning about new attacks and exploitation trends which allow administrators to successfully configure a behavioral based profile and provide correct tuning of network sensors.
- Can capture all keystrokes and any files that might have been used in the intrusion attempt.

PASSIVE SYSTEMS

- Detects a potential security breach
- Logs the information
- Signals an alert on the console
- Does not take any preventive measures to stop the attack

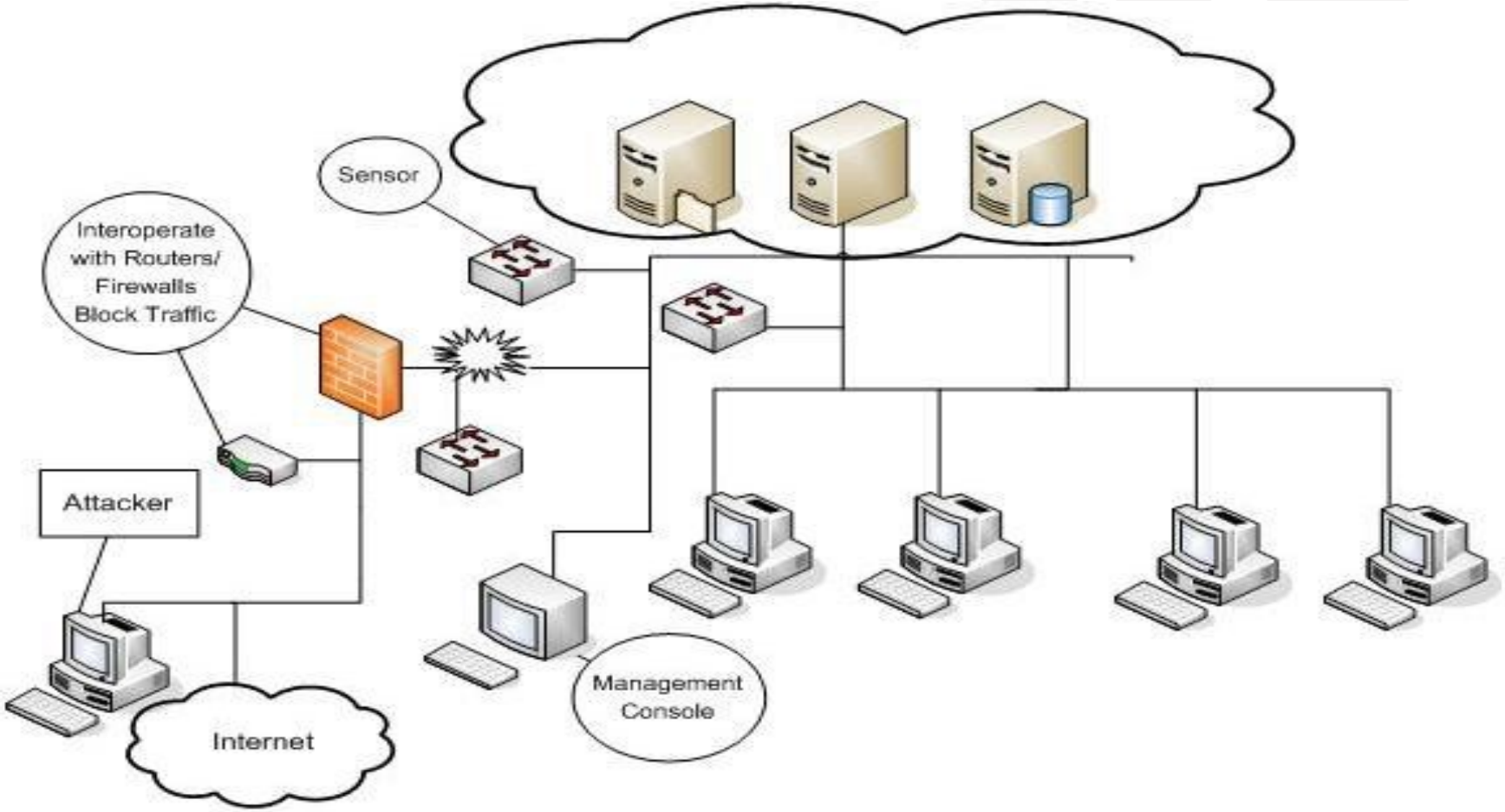
PASSIVE SYSTEMS



REACTIVE/ACTIVE SYSTEMS

- Responds to the suspicious activity like a passive IDS by logging, alerting and recording, but offers the additional ability to take action against the offending traffic.

REACTIVE/ACTIVE SYSTEMS



SIGNATURE BASED IDS

- Monitor network or server traffic and match bytes or packet sequences against a set of predetermined attack lists or signatures.
- Should a particular intrusion or attack session match a signature configured on the IDS, the system alerts administrators or takes other pre-configured action.
- Signatures are easy to develop and understand if you know what network behavior you're trying to identify.
- However, because they only detect known attacks, a signature must be created for every attack.
- New vulnerabilities and exploits will not be detected until administrators develop new signatures.
- Another drawback to signature-based IDS is that they are very large and it can be hard to keep up with the pace of fast moving network traffic.

PROS

- Can detect external hackers, as well as, internal network-based attacks
- Scales easily to provide protection for the entire network
- Offers centralized management for correlation of distributed attacks
- Provides defense in depth
- Gives administrators the ability to quantify attacks
- Provides an additional layer of protection

CONS

- Generates false positives and negatives
- Reacts to attacks rather than preventing them
- Requires full-time monitoring and highly skilled staff dedicated to interpreting the data
- Requires a complex incident response process
- Cannot monitor traffic at higher network traffic rates
- Generates an enormous amount of data to be analyzed
- Cannot deal with encrypted network traffic
- It is expensive