

COMPUTER SECURITY

Chapter 6: Network Security

NETWORK HARDENING

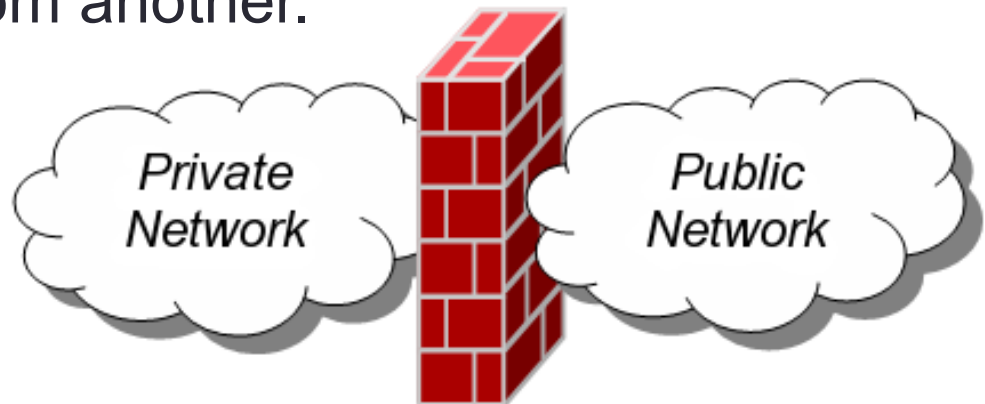
FIREWALLS

Firewalls

- [What is a Firewall?](#)

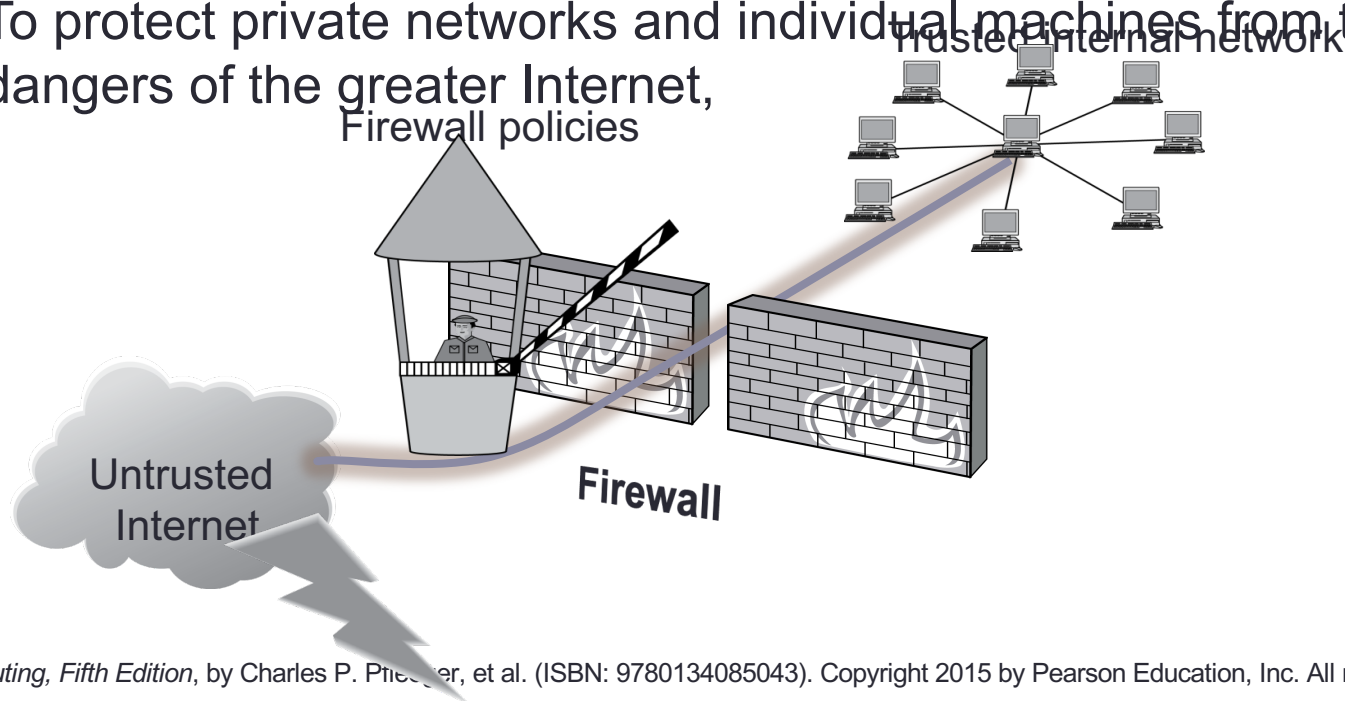
Firewalls

- A **firewall** is an integrated collection of security measures
 - designed to prevent unauthorized electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction
 - in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Policies

- A firewall can be employed to filter incoming or outgoing traffic
 - based on a predefined set of rules called firewall policies.
 - To protect private networks and individual machines from the dangers of the greater Internet,



Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
 - **Accepted:** permitted through the firewall
 - **Dropped:** not allowed through with no indication of failure
 - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected

Policy Actions

- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
 - TCP or UDP
 - the source and destination IP addresses
 - the source and destination ports
 - the application-level payload of the packet (e.g., whether it contains a virus).

Firewall Security Policy Example

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

- External traffic can reach the entire internal network on TCP/25 and UDP/69.
- Internal traffic can go out to port 80 on the external network.
- External traffic can reach TCP/80 on one internal server.
- All other traffic from external to internal is disallowed

Blacklisting and Whitelisting

- Two fundamental approaches to creating firewall policies (or rulesets)
 - to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines
 - in the trusted internal network (or individual computer):



Blacklists and White Lists



- **Blacklist** approach
 - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
 - This type of configuration is more flexible in ensuring that service to the internal network is not disrupted by the firewall
 - naïve from a security perspective - assumes the network administrator can enumerate all properties of malicious traffic.



Blacklists and White Lists

- **Whitelist** approach
 - A safer approach to defining a firewall ruleset is the default-deny policy
 - packets are dropped or rejected unless they are specifically allowed by the firewall.
 - Rules are created for traffic that is allowed
 - Much more secure configuration
 - Before a new service will work, a new rule has to be defined to it
 - Slightly less convenient.

Types of Firewalls

- Packet filtering (stateless) gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

Flood Guard

- Flood guards serve as preventive control
 - against denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
 - Protect availability
- Flood guards are available either as standalone devices or as firewall components
- Capable of monitoring network traffic to identify DoS attacks in progress
 - generated through packet flooding.

Flood Guard

- A sophisticated firewall
- like an application proxy, can interpret data at the protocol level and respond
- The distinction between a guard and an application proxy can be fuzzy;
 - the more protection features an application proxy implements, the more it becomes like a guard

Flood Guard

- Guards may implement any programmable set of rules; for example:
 - Limit the number of email messages a user can receive
 - Limit users' web bandwidth
 - Filter documents containing the word "Secret"
 - Pass downloaded files through a virus scanner

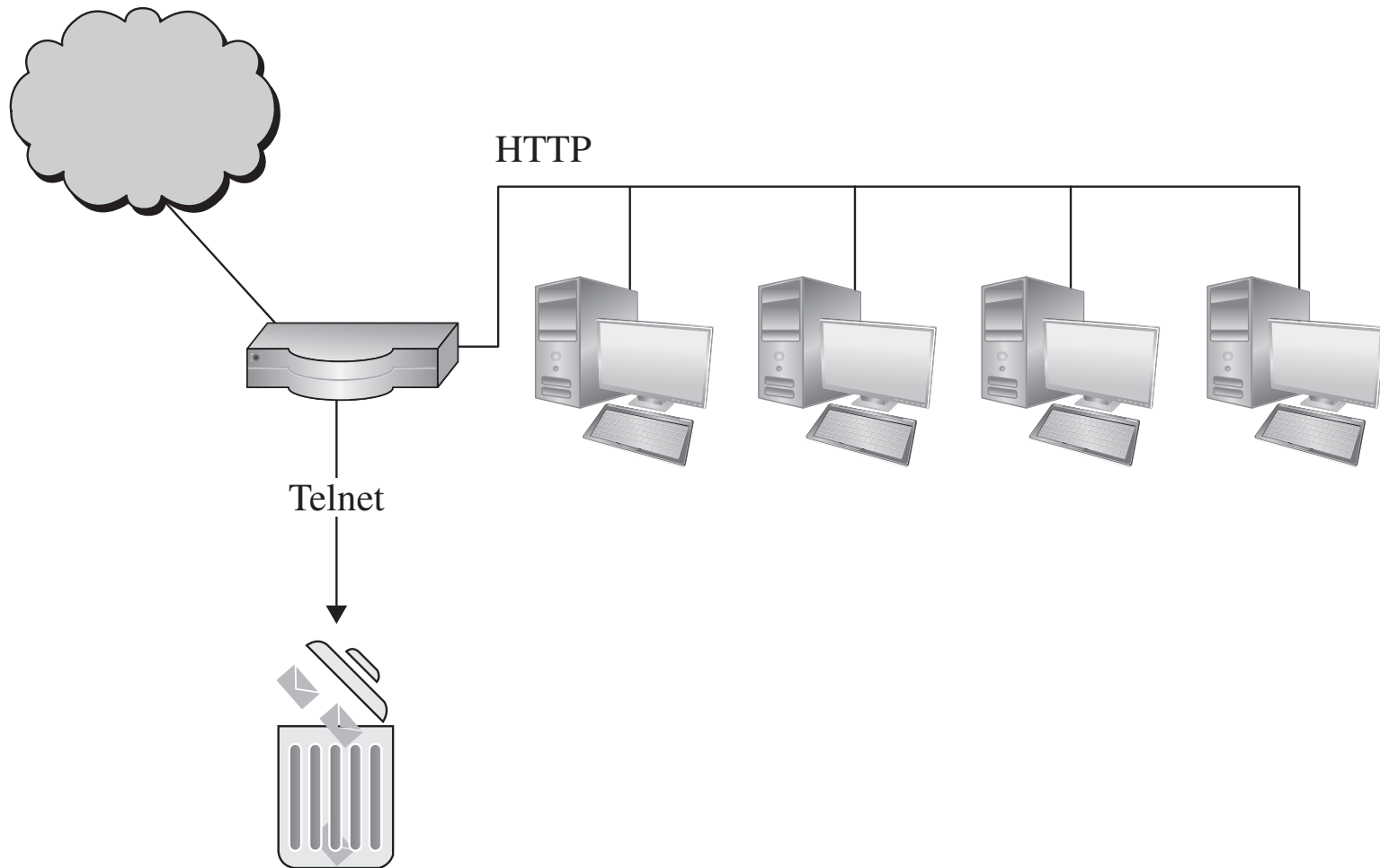
Flood Guard

- A security concept
- A form of Intrusion Detection System

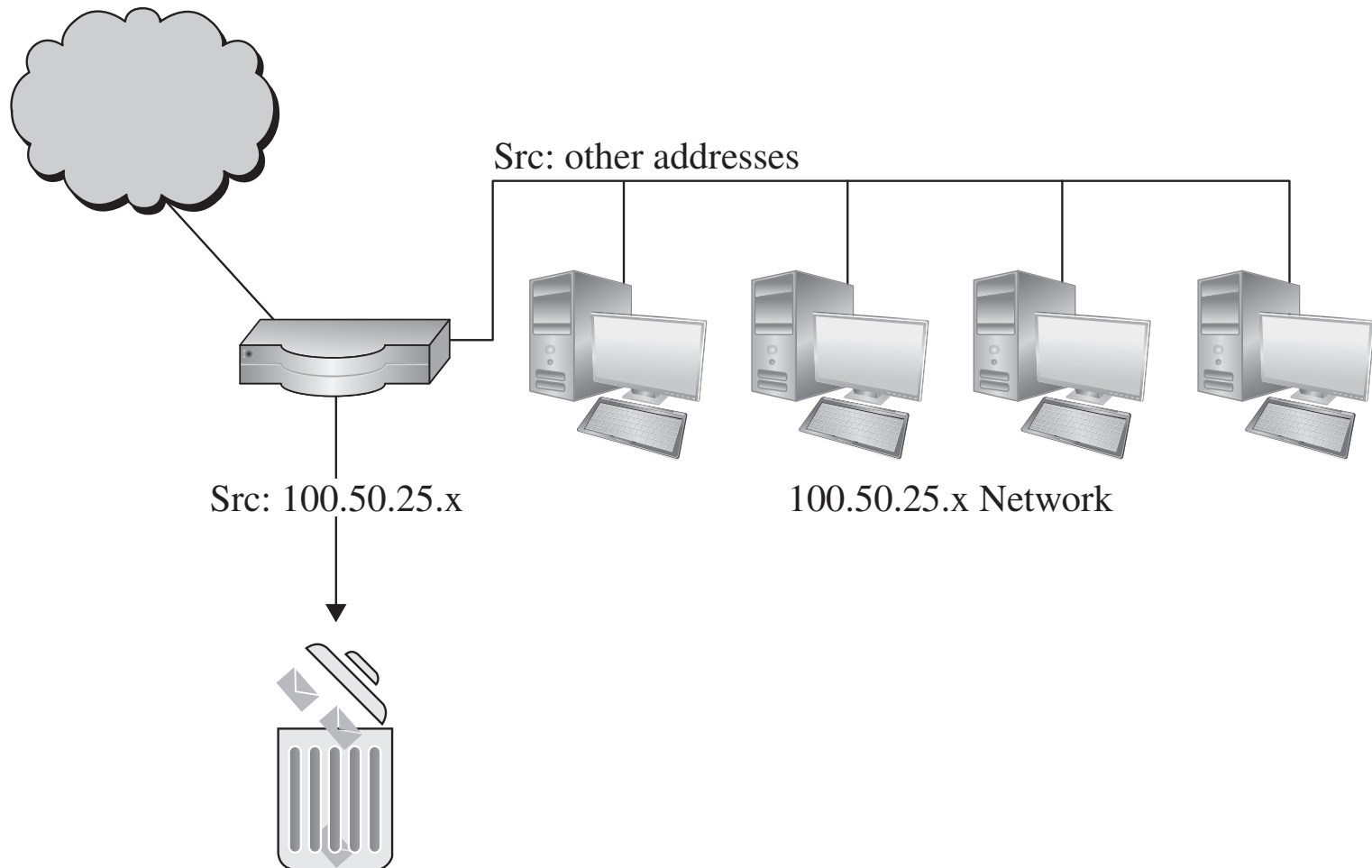
Packet-Filtering Gateways

- A packet-filtering gateway controls access on the basis of packet address and specific transport protocol type
 - e.g., HTTP traffic.
- If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- Packet-filtering gateways maintain no state from one packet to the next
 - They simply look at each packet's IP addresses and ports and compare them to the configured policies

Packet-Filtering Gateways

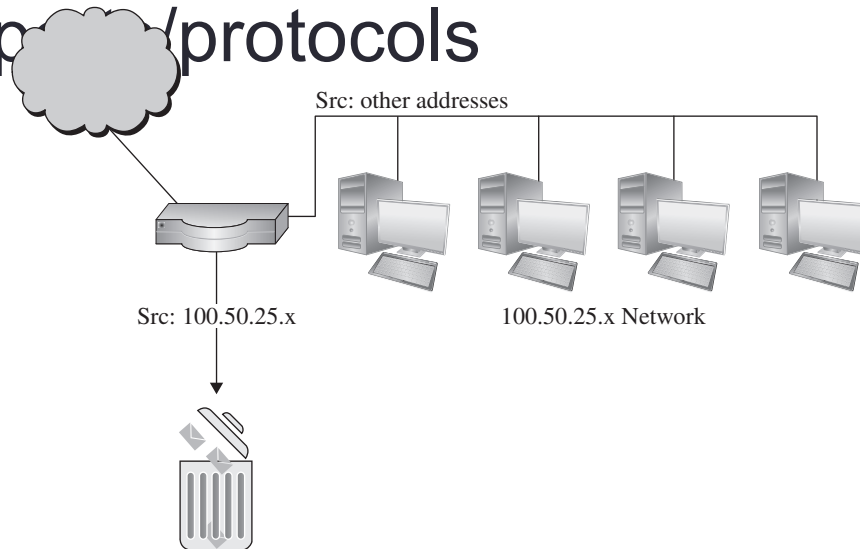


Packet-Filtering Gateways Example



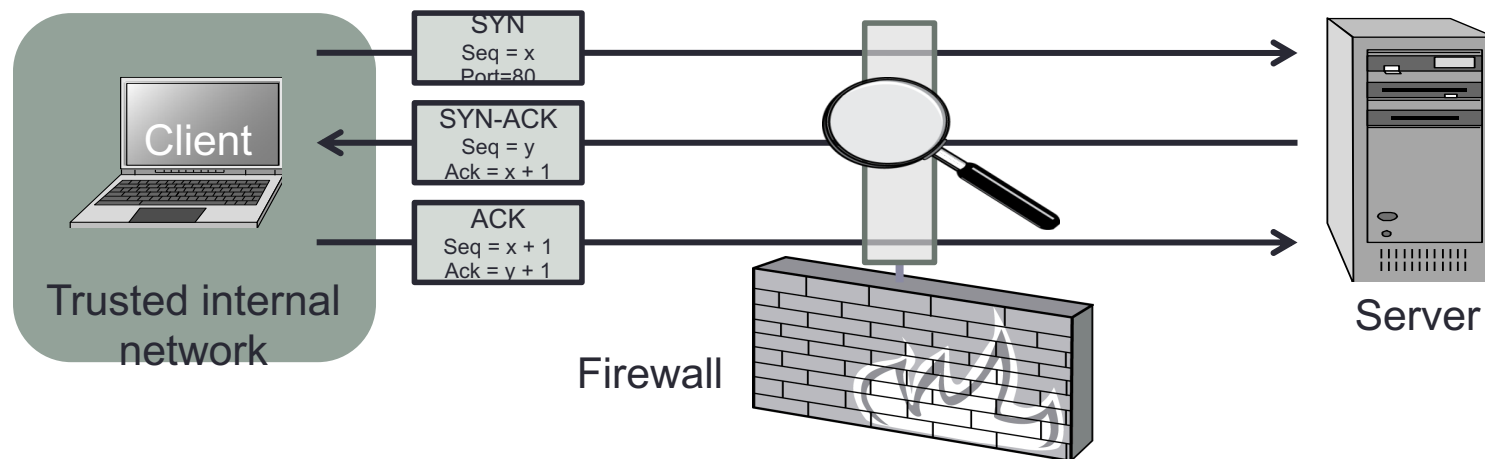
Packet-Filtering Gateways - Example

- Here, firewall is filtering traffic on the basis of source IP
 - rather than port.
- Filtering rules can also be based on combinations of addresses and p/protocols



Packet-Filtering (Stateless) Gateways

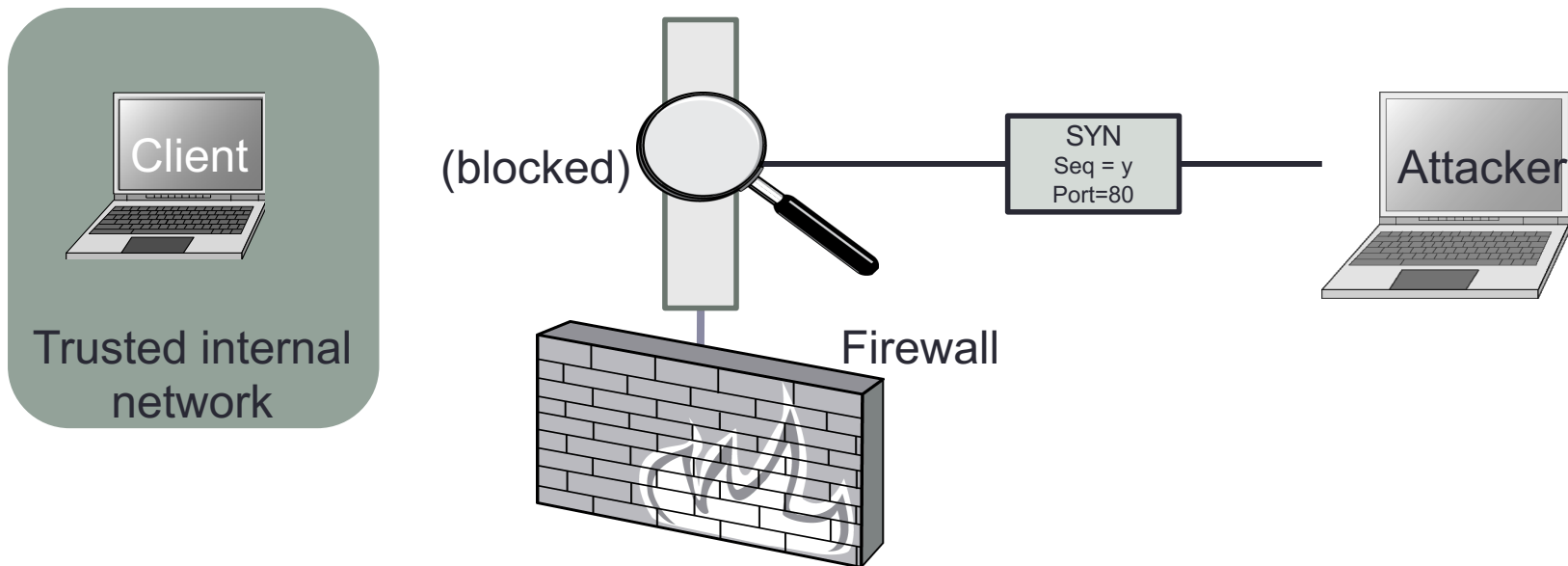
- A stateless firewall doesn't maintain any remembered context ("state") with respect to the packets it is processing
 - treats each packet attempting to travel through it in isolation
 - without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.

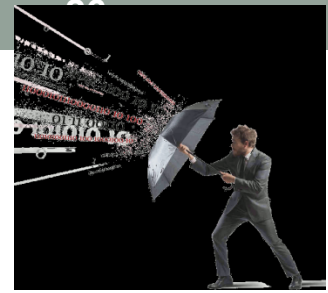


Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Stateful Inspection Firewall

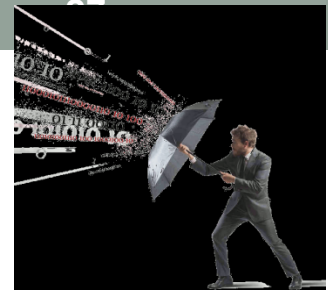
- Stateful inspection firewalls maintain state information from one packet to the next
 - In contrast to packet-filtering gateways
- It maintains records of all connections passing through it
- Can determine packet designation:
 - if a packet is the start of a new connection, a part of an existing connection, or is an invalid packet.

Statefull Firewalls



- **Stateful firewalls** can tell when packets are part of legitimate sessions
 - originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection
 - including IP addresses, ports, and sequence numbers of packets

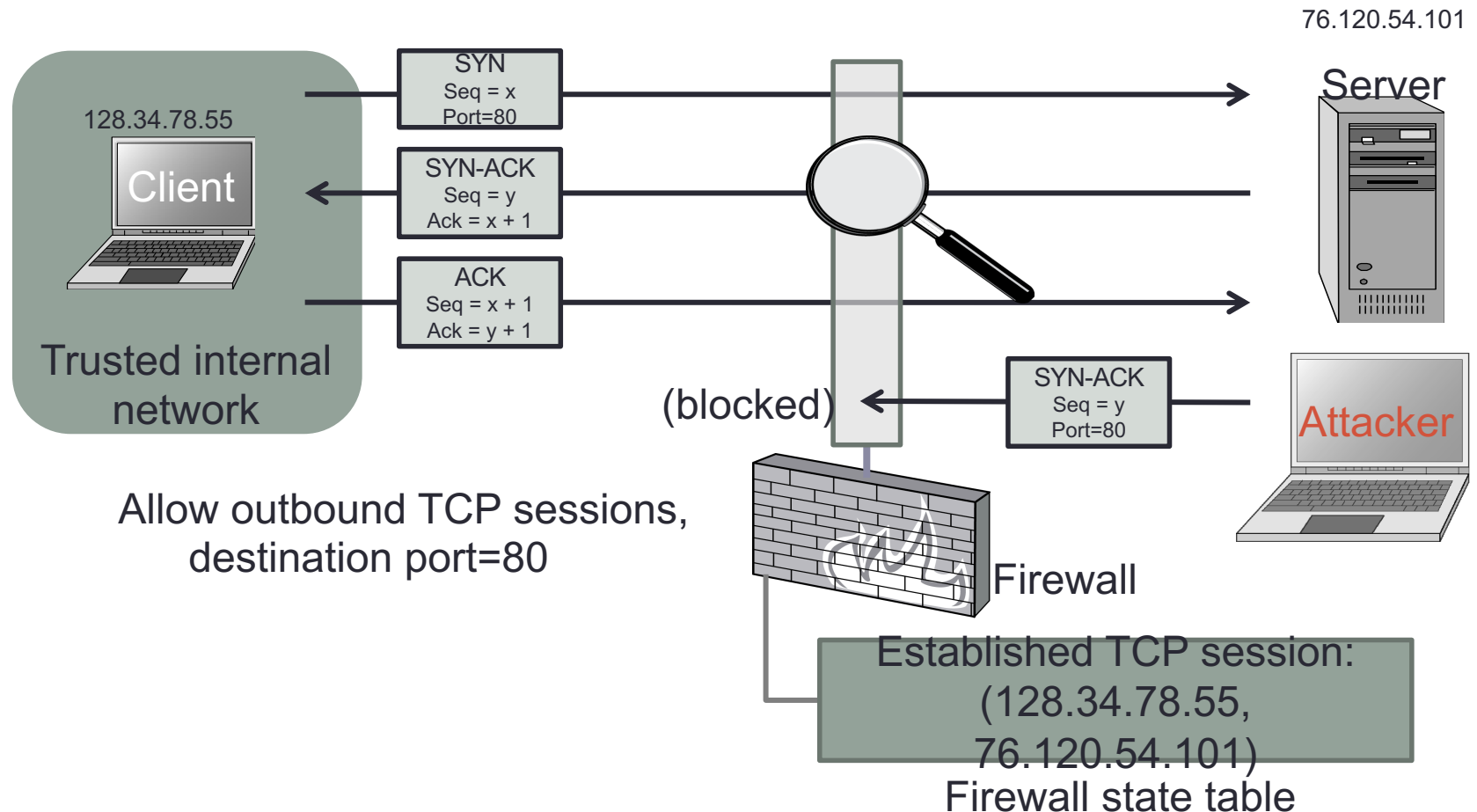
Statefull Firewalls



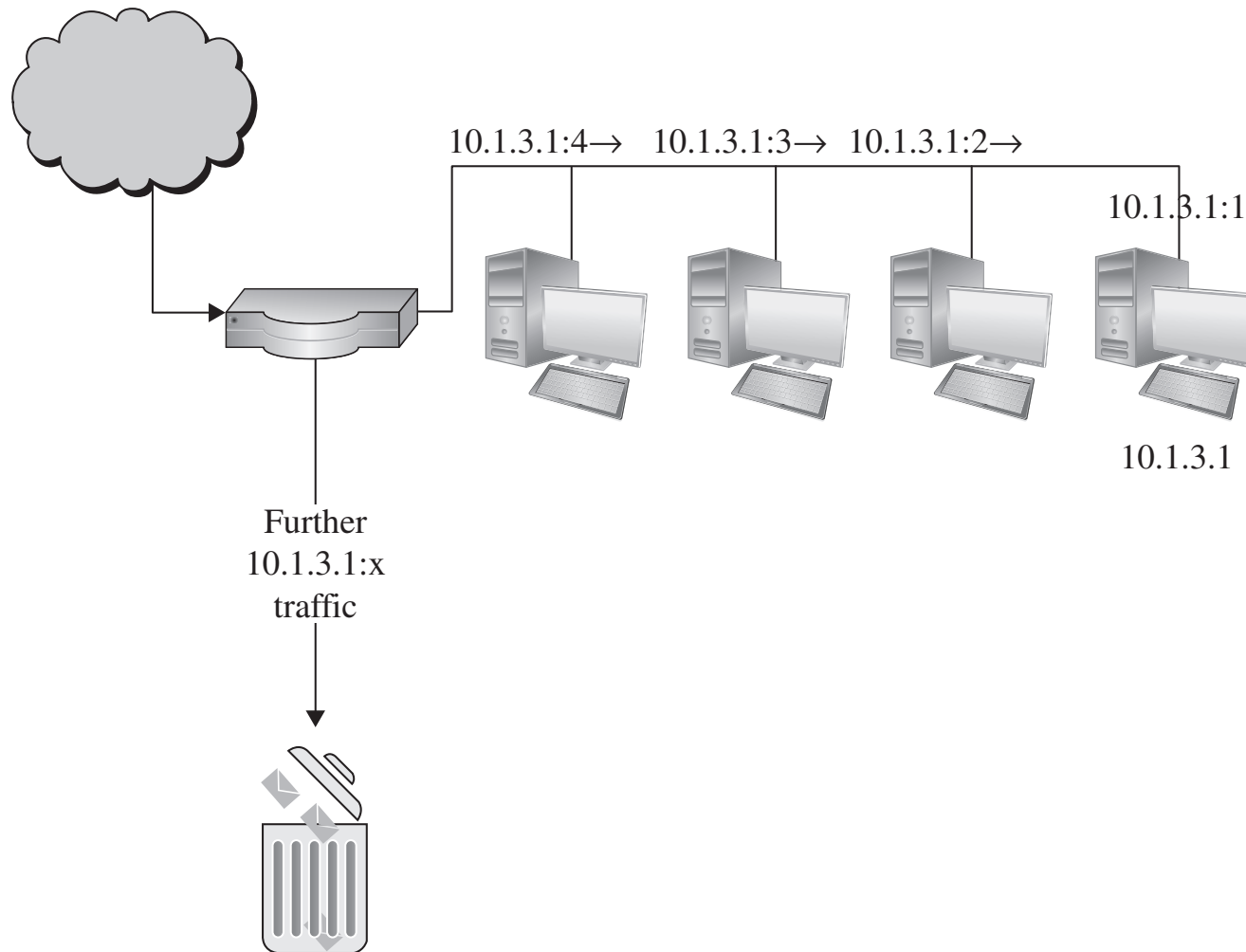
- Example: can allow only inbound TCP packets that respond to a connection initiated within internal network
 - Using these tables

Statefull Firewall Example

- Allow only requested TCP connections:

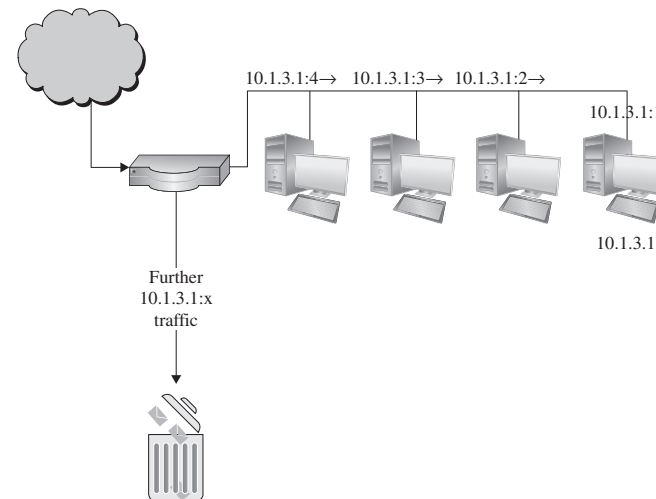


Stateful Inspection Firewall Example



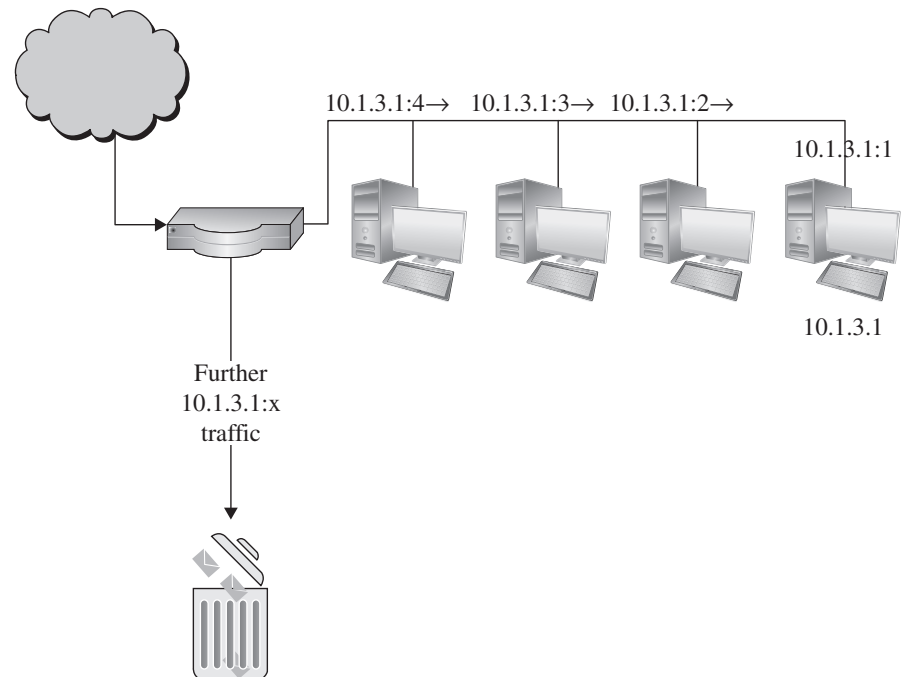
Stateful Inspection Firewall Example

- Firewall is counting the number of systems coming from external IP 10.1.3.1
- After the external system reaches out to a fourth computer, the firewall hits a configured threshold
 - begins filtering packets from that address.

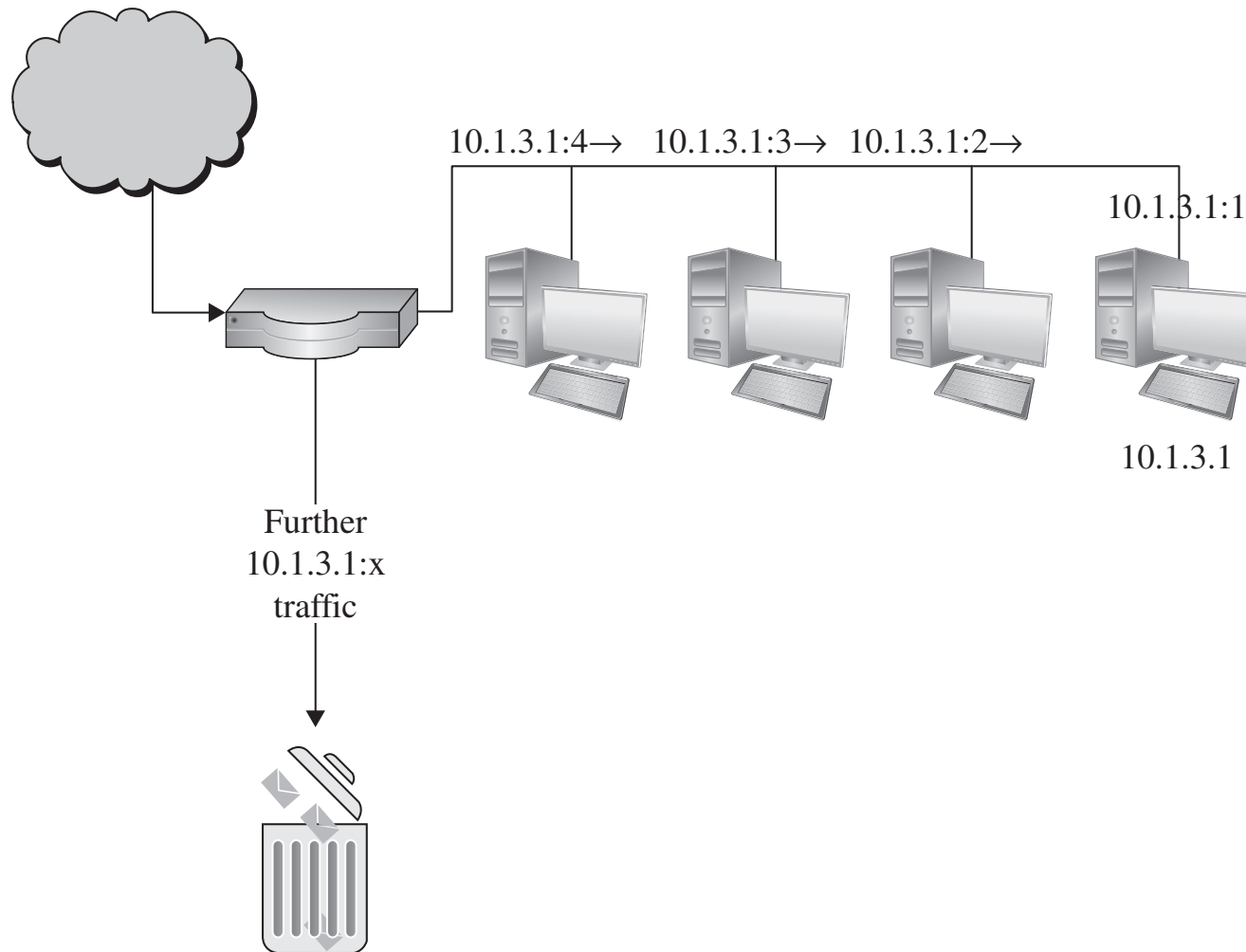


Stateful Inspection Firewall Example

- In real life, it can be difficult to define rules that require state/context
 - and that attackers cannot circumvent



Stateful Inspection Firewall Example



Application Layer Firewall

- Application layer firewall works like a **proxy**
 - can “understand” certain applications and protocols.
- It may inspect the contents of the traffic,
 - blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

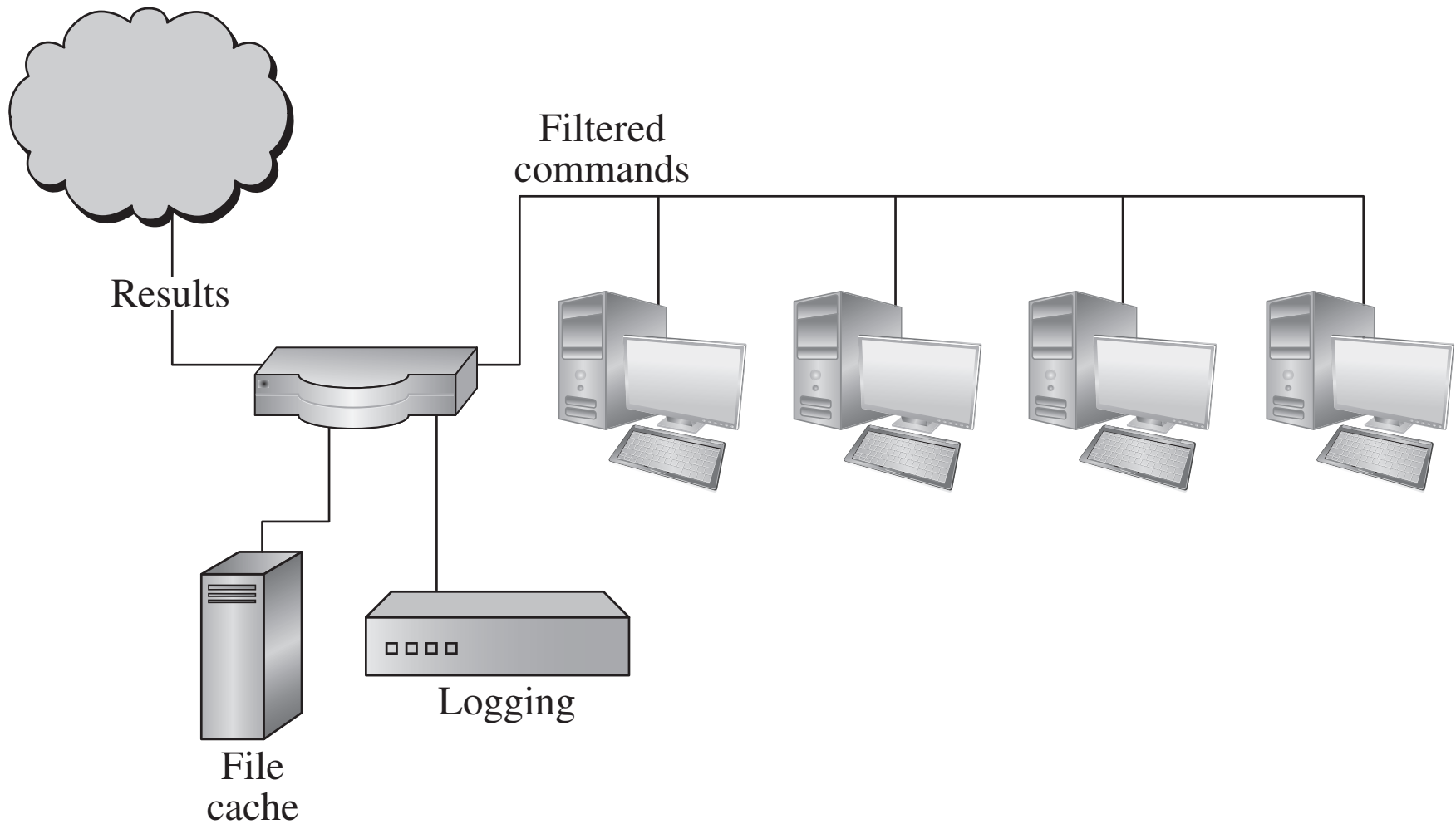
Application Proxy Firewall

- An application proxy simulates the behavior of an application at OSI layer 7
 - so that the real application receives only requests to act properly

Application Proxy Firewall

- Application proxies can serve a number of purposes:
 - Filtering potentially dangerous application-layer requests
 - Log requests/accesses
 - Cache results to save bandwidth
- For example, web proxy is used by companies often to monitor and filter employee internet use

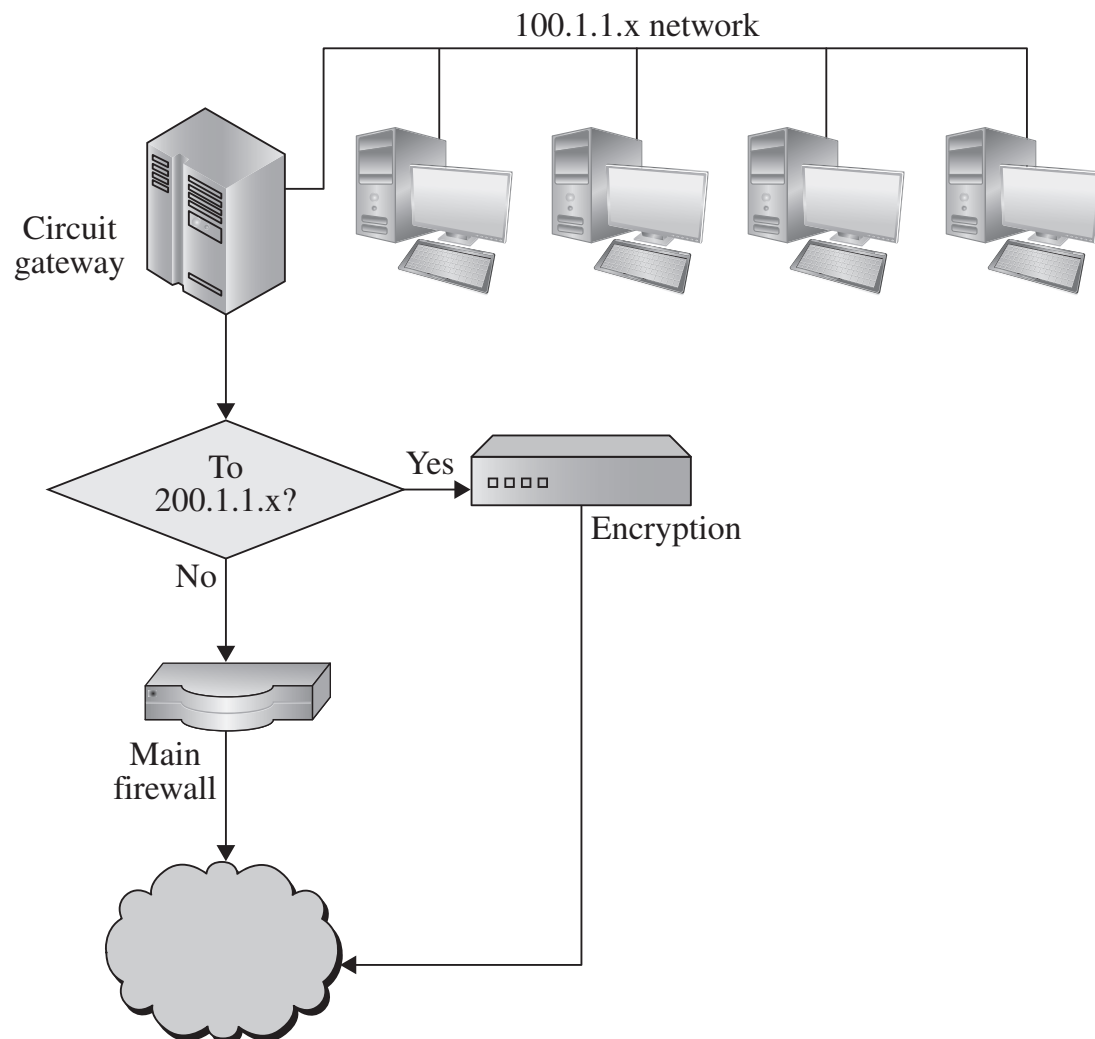
Application Proxy



Circuit-Level Gateway

- A firewall that essentially allows one network to be an extension of another.
- Operates at OSI layer 5, the session layer
- Functions as a virtual gateway between two networks
- One use of a circuit-level gateway is to implement a VPN

Circuit-Level Gateway



Personal Firewalls

- A personal firewall runs on a workstation or server
 - can enforce security policy like other firewalls.
- Restricts traffic by source IP and destination port
- Can also restrict which applications are allowed to use the network.

Personal Firewalls



Personal Firewalls

- Example: Windows firewall configuration dialog
 - an administrator can select which protocols and applications should be allowed to communicate
 - to and from the host



What Firewalls Can and Cannot Do

- Firewalls can protect an environment only if they control the entire perimeter
- Firewalls do not protect data outside the perimeter
- Firewalls are the most visible part of an installation to the outside
 - so they are an attractive target for attack

What Firewalls Can and Cannot Do

- Firewalls must be correctly configured
 - configuration must be updated as the environment changes,
 - firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion

Firewalls - summary

- Device that filters traffic between a protected “inside” network and less trustworthy “outside” network
- Most firewalls run as dedicated devices
 - Easier to design correctly and inspect for bugs
 - Easier to optimize for performance
- Firewalls implement security policies
 - or set of rules that determine what traffic can or cannot pass through

Firewalls – summary (cont.)

- A firewall is an example of a reference monitor, which means it should have three characteristics:
 - Always invoked (cannot be circumvented)
 - Tamperproof
 - Small and simple enough for rigorous analysis

Comparison of Firewall Types

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

MONITORING YOUR NETWORKS

Security Principles

- Network Separation/Segmentation
 - Using Virtual Devices (VLANs)
 - Creating dedicated virtual networks
 - Example:
 - Create one network for the employees of the company
 - A separate network for handling the printers
 - Printers do not need access to the same network resources that employees do
 - Enables easier monitoring of traffic between networks
 - Routers will be configured between both networks
 - To allow employees to print

Network Monitoring

- Creating ***baseline*** of your network
 - Can be achieved through traffic monitoring
 - Knowing how the network works typically will allow detecting of atypical activity

Network Monitoring

- Analyzing logs
 - The practice of collecting logs from different networks
 - Also client services
 - Performing automated analysis on them
 - This can result in network intrusions and malicious activities detection
 - Things that may be analyzed:
 - Firewall logs
 - Authentication logs

Analyzing Logs

- External devices and services should be closely monitored
 - They may be subject to more malicious traffic
 - Increases risk of compromise
 -

Analyzing Logs

- Analysis of logs:
 - Look for specific network messages
 - Like a firewall log
 - Attempted connection to internal service from an untrusted source address
 - Connections from internal network to known botnet addresses
 - May show a compromised machine on the network
 -

Analyzing Logs

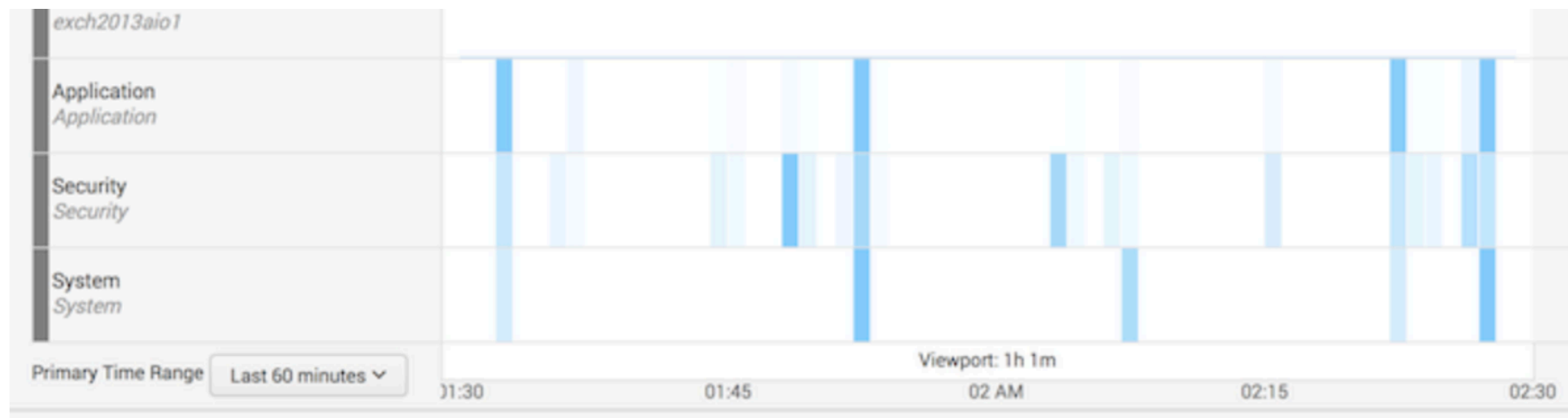
- Log Analysis systems are configured using user-defined rules
 - To match interesting or atypical log entries
- Alerts would be sent to security engineers
 - For further investigation
- Log data needs to be normalized
 - Different devices and systems may not be formatted in a common way.
 - Make it easier for analysts to further process the data

Analysis Logs

- Post-Fail analysis:
 - Investigating a compromised happened after a breach has been detected

Log Analyzer - example

- Splunk data analyzer:
- Shows various components associated with the host
 - User can add and delete components to track



IDS/IPS

INTRUSION DETECTION/ PREVENTION SYSTEMS (IDS/IPS)

- Operate by monitoring network traffic and analyzing it
- Look for behavior/characteristics that may indicate malicious traffic

Intrusion Detection Systems

- Intrusion
 - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing/networking resources)



<https://gbhackers.com/intrusion-detection-system-ids-2/>

Intrusion Detection System

- Security controls we covered so far:
 - Perimeter controls, firewall, and authentication and access controls
 - Block certain actions
 - Most of these controls are preventive
 - They block known bad things from happening
- After using those controls, some users are admitted to use a computing system

Intrusion Detection System

- Studies show that most computer security incidents are caused by insiders
 - or people impersonating them
 - people who would not be blocked by a firewall
- Insiders require access with significant privileges to do their daily jobs

Intrusion Detection System

- Harm from insiders may not be malicious
 - it is honest people making honest mistakes
- Harm can also result from potential malicious outsiders
 - who have somehow passed the screens of firewalls and access controls exist
- Prevention, although necessary, is not a complete computer security control
 - Detection during an incident copes with harm that cannot be prevented in advance

Intrusion Detection Systems



- Intrusion detection (IDS)
 - The identification through intrusion signatures and report of intrusion activities
- Intrusion prevention (IPS)
 - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network



IDS

- Can be host based or network based
- Network Intrusion Detection System (NIDS):
 - Deployed on the network
 - Monitors traffic for network segment or subnet
- Resemble firewalls
 - However, firewalls alerts of outside threats
 - NIDS alert from threats inside the network

IDS

- Host based IDS:
 - Deployed on a host
 - Software that monitors traffic to and from that host only
 - Monitors system files for unauthorized changes

Host-based IDS

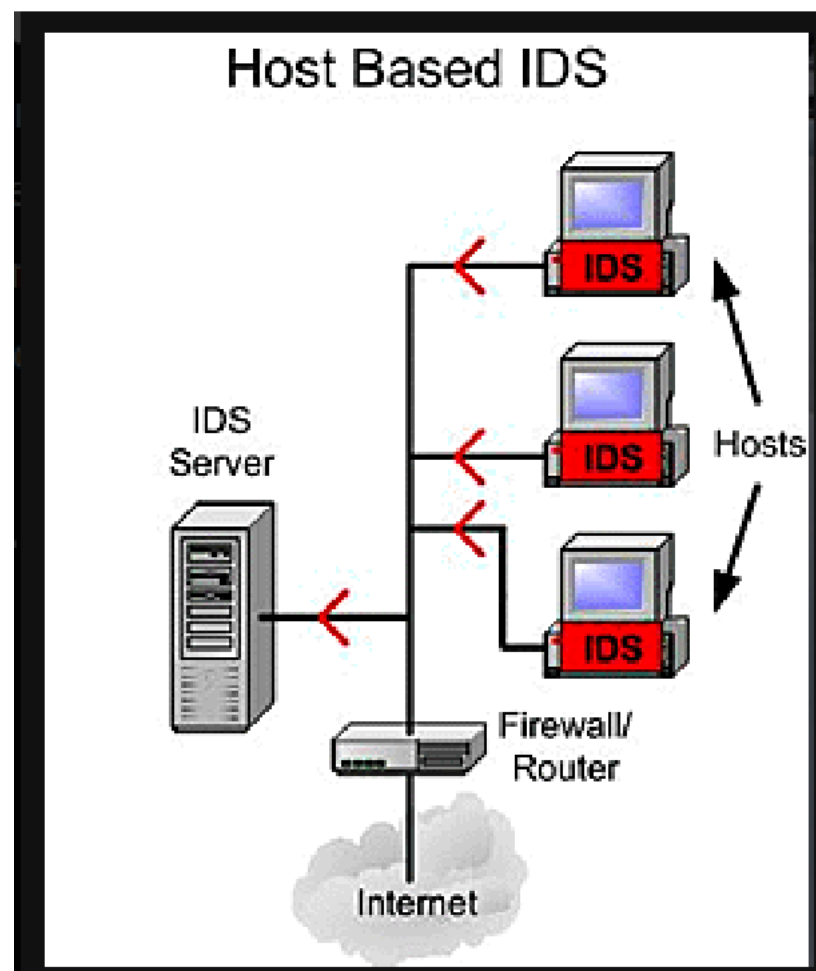
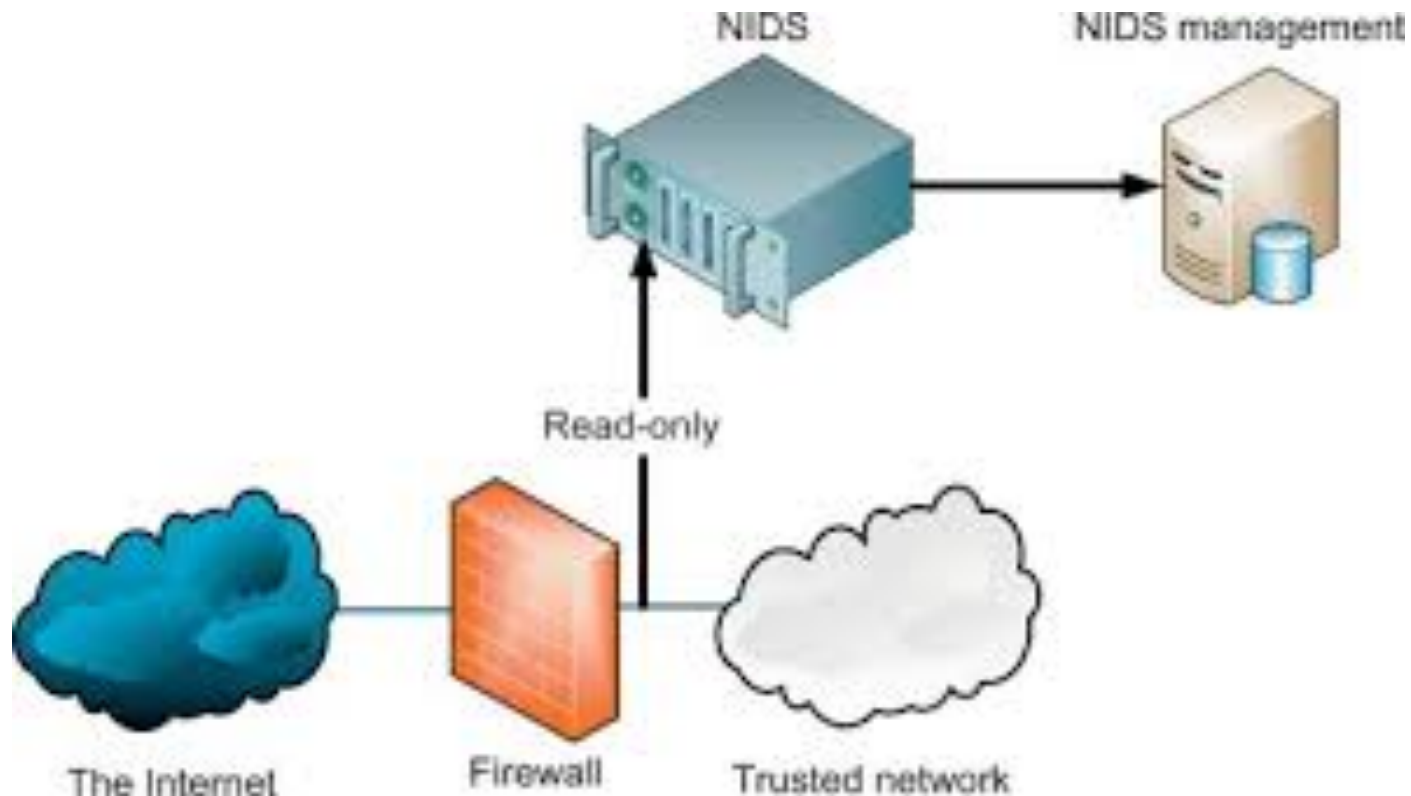
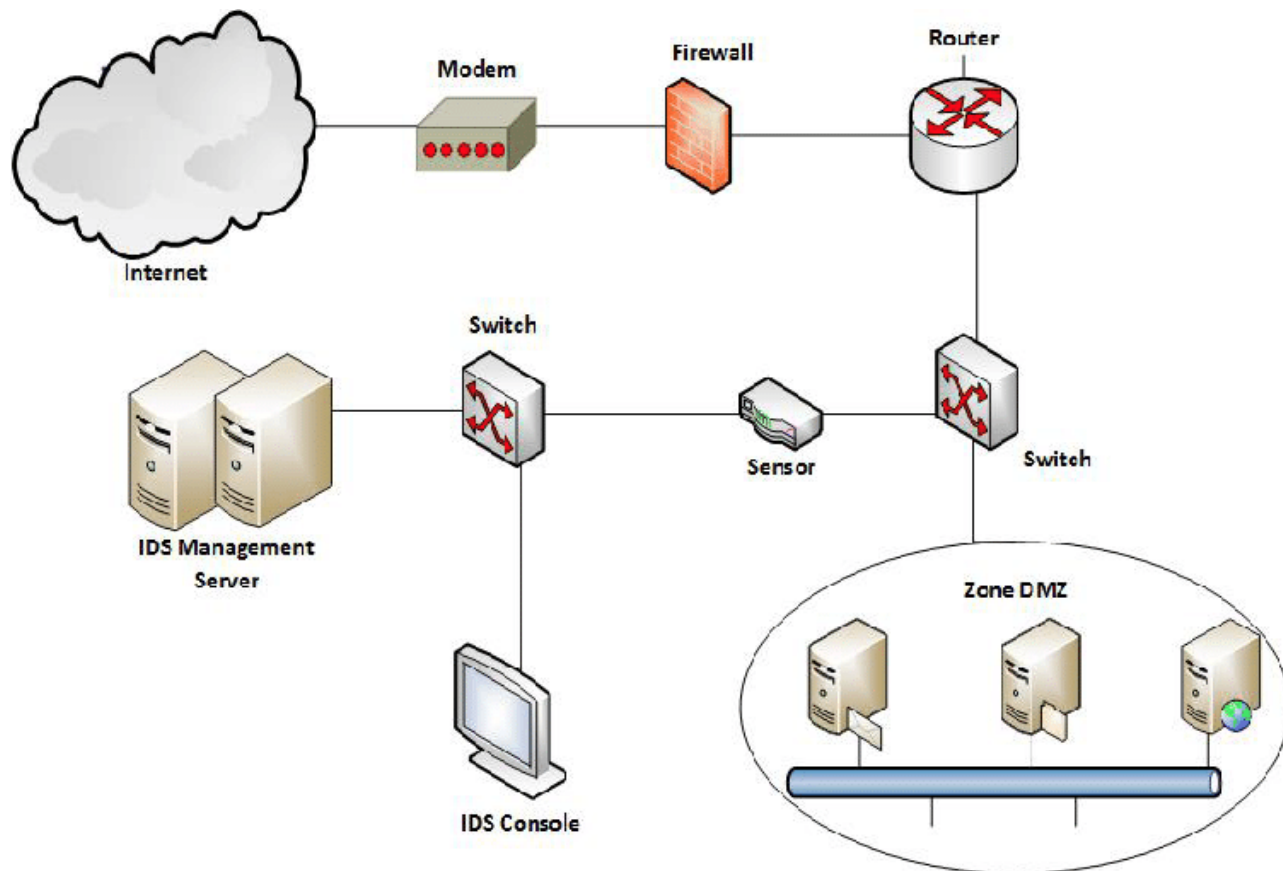


Fig. 2. Architecture of Host based IDS

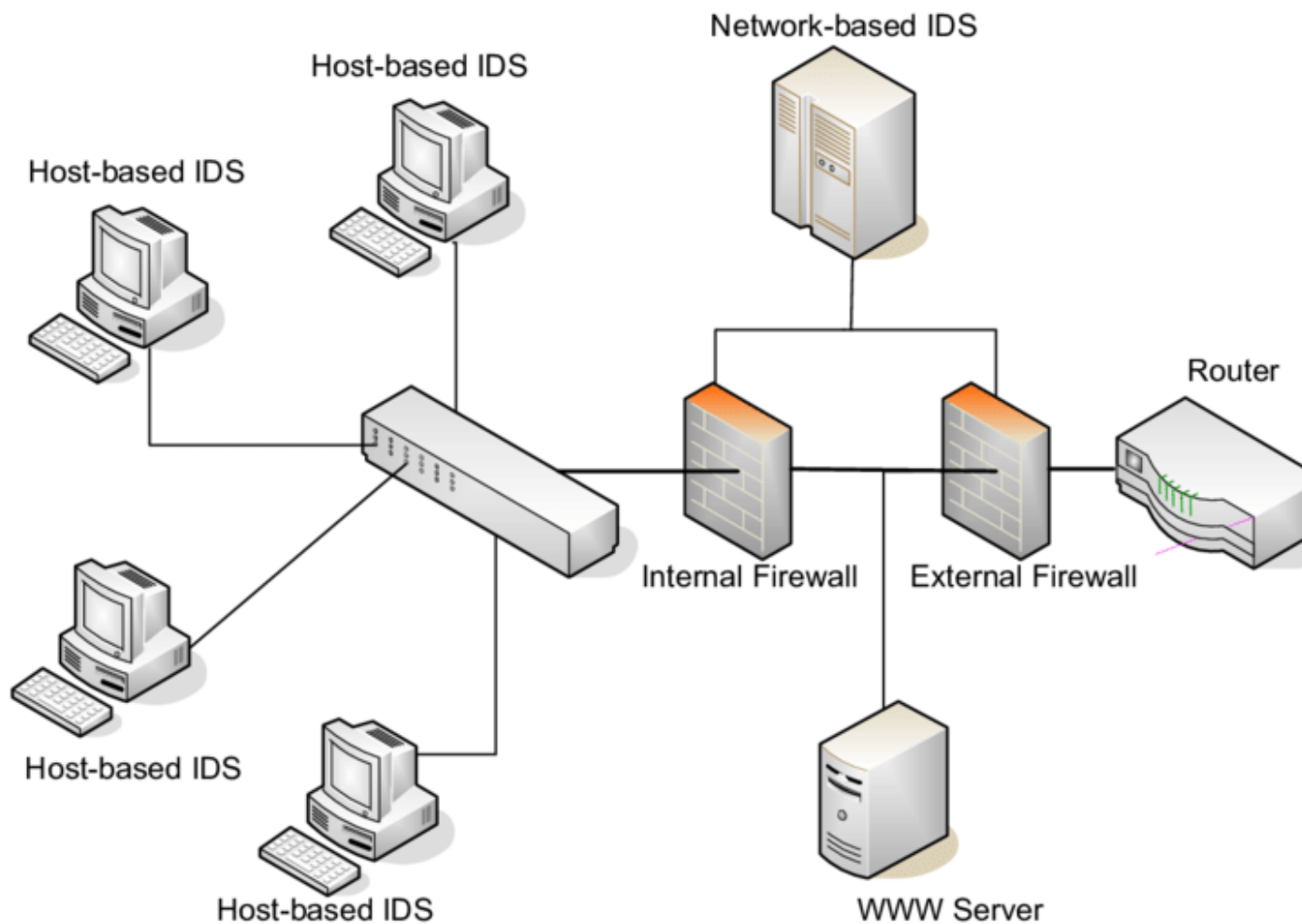
Network based NIDS



Network based NIDS



NIDS and Host-based IDS



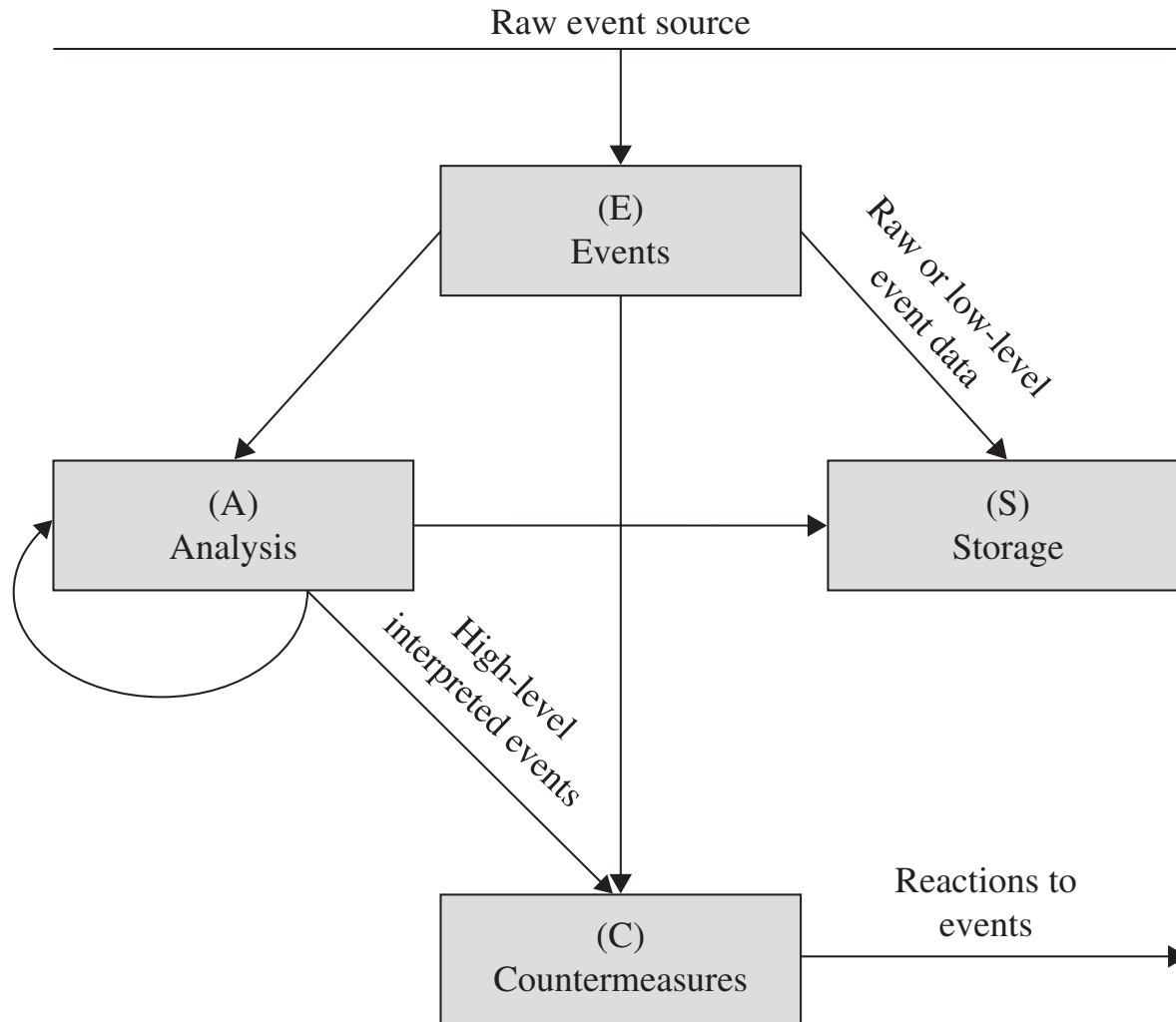
Popular NIDS systems

- Snort
 - Open source NIDS system
 - <https://www.snort.org/>
- Suricata
 - Open source IDS/IPS system
 - <https://suricata-ids.org/>
- Zeek (Bro) NIDS
 - Open-source software network analysis framework
 - <https://www.zeek.org/>

Systems Location

- NIDS:
 - Needs access to all traffic
 - Analyzing traffic between hosts
 - Using port mirroring functionality
 - Send a copy of network packets seen on one switch port to the NIDS port
 - Passive observer that only watches traffic
- NIPS (Network Intrusion Prevention System):
 - Has to be placed in line with traffic
 - So it can take action on the traffic
 - Active observer, can block or drop packets

Intrusion Detection Systems (IDS)



Intrusion Detection Systems (IDS)

- IDSs complement preventative controls as a next line of defense
 - monitor activity to identify malicious or suspicious events.

Intrusion Detection Systems (IDS)

- IDSs may:
 - Monitor user and system activity
 - Audit system configurations for vulnerabilities and misconfigurations
 - Assess integrity of critical system and data files
 - Recognize known attack patterns in system activity
 - Identify abnormal activity through statistical analysis
 - Manage audit trails and highlight policy violations
 - Install and operate traps to record information about intruders

Types of IDS

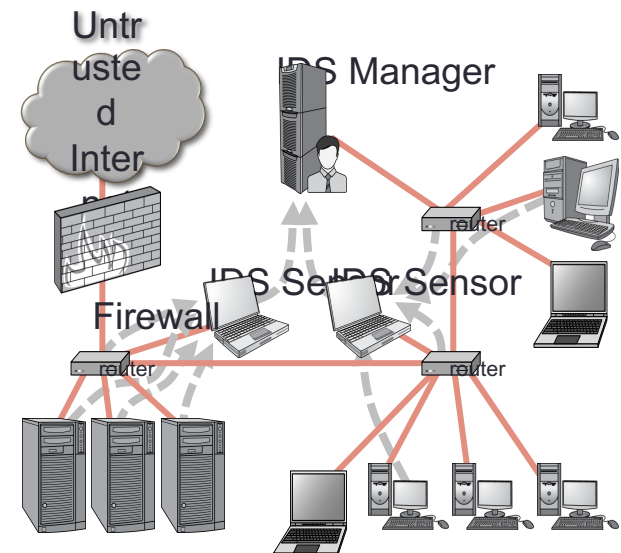
- Detection method
 - Signature-based
 - can only detect known patterns
 - Heuristic
 - for patterns of behavior that are out of the ordinary
- Location
 - Front end
 - looks at traffic as it enters the network
 - Internal
 - monitors traffic within the network

Types of IDS

- Scope
 - Host-based IDS (HIDS)
 - protects a single host by monitoring traffic from the OS
 - Network-based IDS (NIDS)
 - a server or appliance that monitors network traffic
- Capability
 - Passive
 - Active, also known as intrusion prevention systems (IPS)
 - tries to block or otherwise prevent suspicious or malicious behavior once it is detected

IDS Components

- The **IDS manager** compiles data from the IDS sensors to determine if an intrusion has occurred.
- This determination is based on a set of **site policies**, which are rules and conditions that define probable intrusions.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.



IDS Data

- Dorothy Denning identified several fields that should be included in IDS event records [1987]
 - Subject: the initiator of an action on the target
 - Object: the resource being targeted, such as a file, command, device, or network protocol
 - Action: the operation being performed by the subject towards the object

IDS Data

- Dorothy Denning identified several fields that should be included in IDS event records [1987] (cont.):
 - Exception-condition: any error message or exception condition that was raised by this action
 - Resource-usage: quantitative items that were expended by the system performing or responding to this action
 - Time-stamp: a unique identifier for the moment in time when this action was initiated

Intrusions

- An IDS is designed to detect a number of threats, including the following:
 - **masquerader:** an attacker who is falsely using the identity and/or credentials of a legitimate user
 - to gain access to a computer system or network
 - **Misfeasor:** a legitimate user who performs actions he is not authorized to do
 - **Clandestine user:** a user who tries to block or cover up his actions by deleting audit files and/or system logs

Intrusions



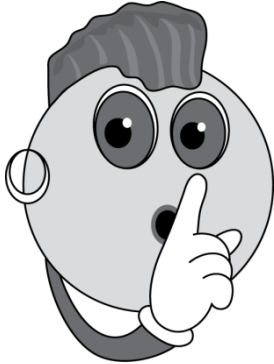
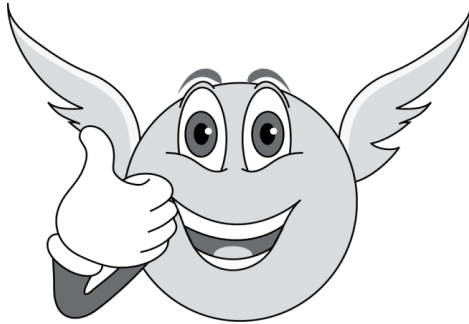
- In addition, an IDS is designed to detect automated attacks and threats, such as:
 - **port scans**: determine which ports on a host are open for TCP connections
 - **Denial-of-service attacks**: network attacks meant to overwhelm a host and shut out legitimate accesses
 - **Malware attacks**: replicating malicious software attacks, such as Trojan horses, computer worms, viruses, etc.
 -

Intrusions

- In addition, an IDS is designed to detect automated attacks and threats, such as (cont.):
 - **ARP spoofing**: an attempt to redirect IP traffic in a local-area network
 - **DNS cache poisoning**: a pharming attack directed at changing a host's DNS cache
 - to create a falsified domain-name/IP-address association

Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative)

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	 NYPD 03539480 True Positive	 NYPD 03539480 False Positive
No Alarm Sounded	 False Negative	 True Negative

The Base-Rate Fallacy

- Desirable properties for intrusion detection system:
 - a high true-positive rate and a low false-negative rate
 - Difficult to create in practice
 - Trade-off between these two properties exists
- If number of actual intrusions is relatively small compared to the amount of data being analyzed
 - => the effectiveness of an intrusion detection system can be reduced.

The Base-Rate Fallacy

- The effectiveness of some IDSs can be misinterpreted
 - due to a statistical error known as the **base-rate fallacy**.
- This occurs when the probability of some conditional event is assessed
 - without considering the “base rate” of that event.

Base-Rate Fallacy Example

- Suppose an IDS is 99% accurate
 - having a 1% chance of false positives or false negatives.
- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.

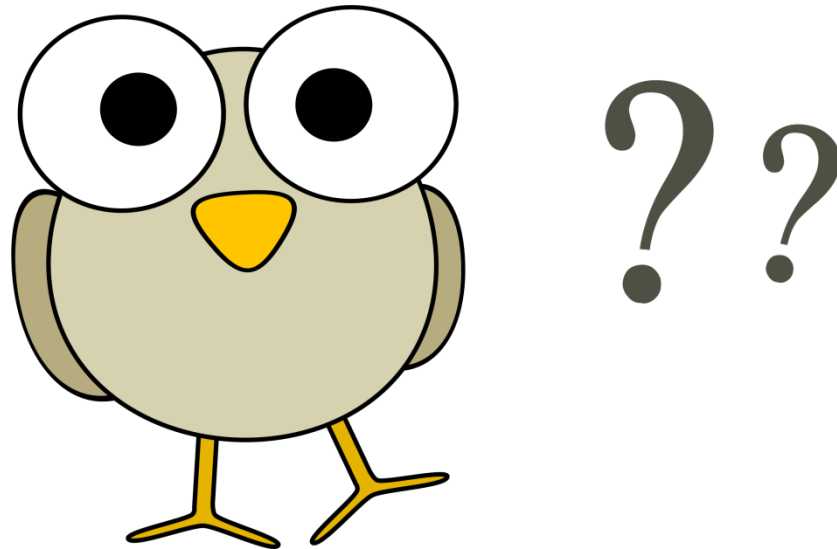
Base-Rate Fallacy Example

- Of the 100 malicious events, 99 will be detected as malicious
 - => we have **1 false negative**.
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious
 - => we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms
 - That is, roughly 99% of our alarms are false alarms.

IDS

- IDs

- Questions?



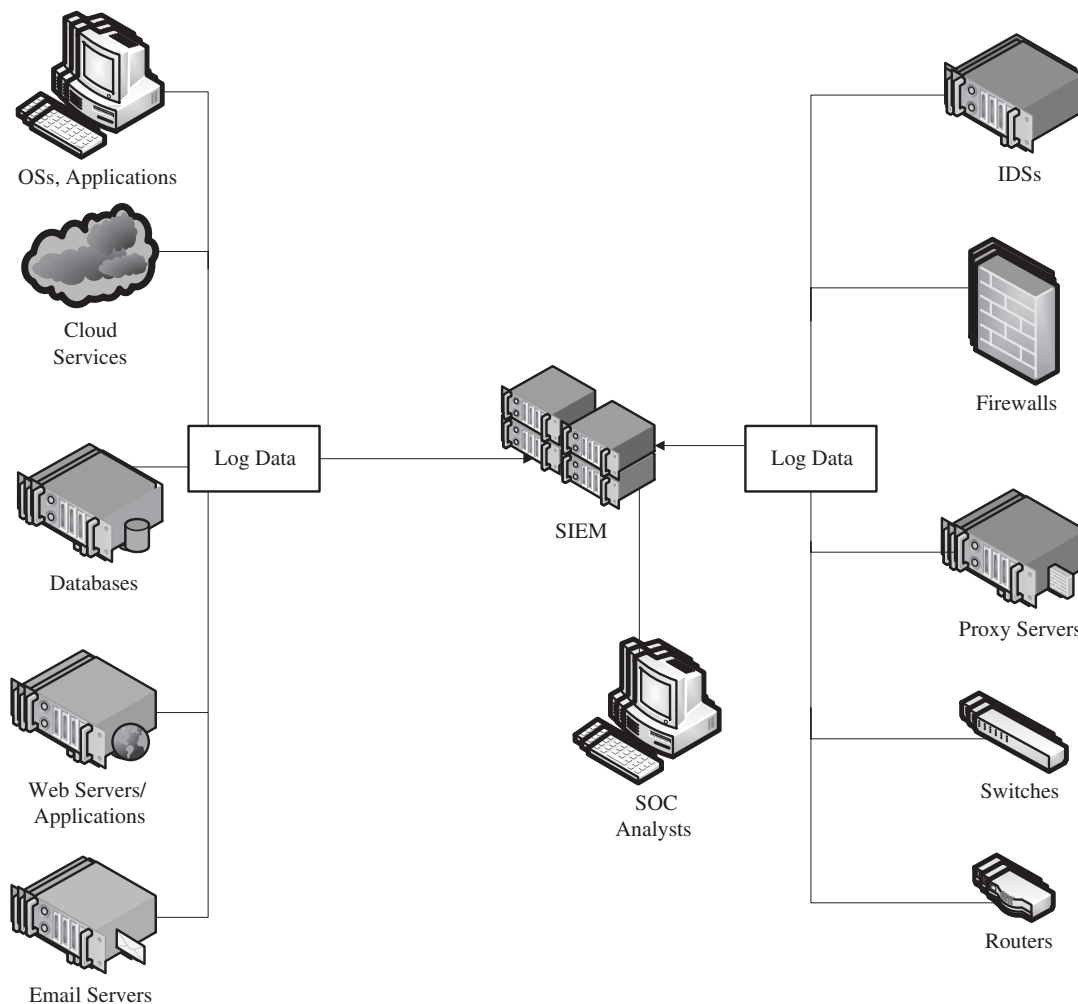
Security Information and Event Management (SIEM)

- Software systems that collect security-relevant data from a variety of products
 - hardware and software products
 - usually audit logs
- Create a unified security dashboard for security operations center personnel.
- SIEMs range in functionality
 - Simple ones allow for basic search and alerting
 - Complex platforms allow for completely custom dashboards, reports, alerts, and correlation

Security Information and Event Management (SIEM)

- <https://www.youtube.com/watch?v=ZuLazPgFtBE>

Security Information and Event Management (SIEM)

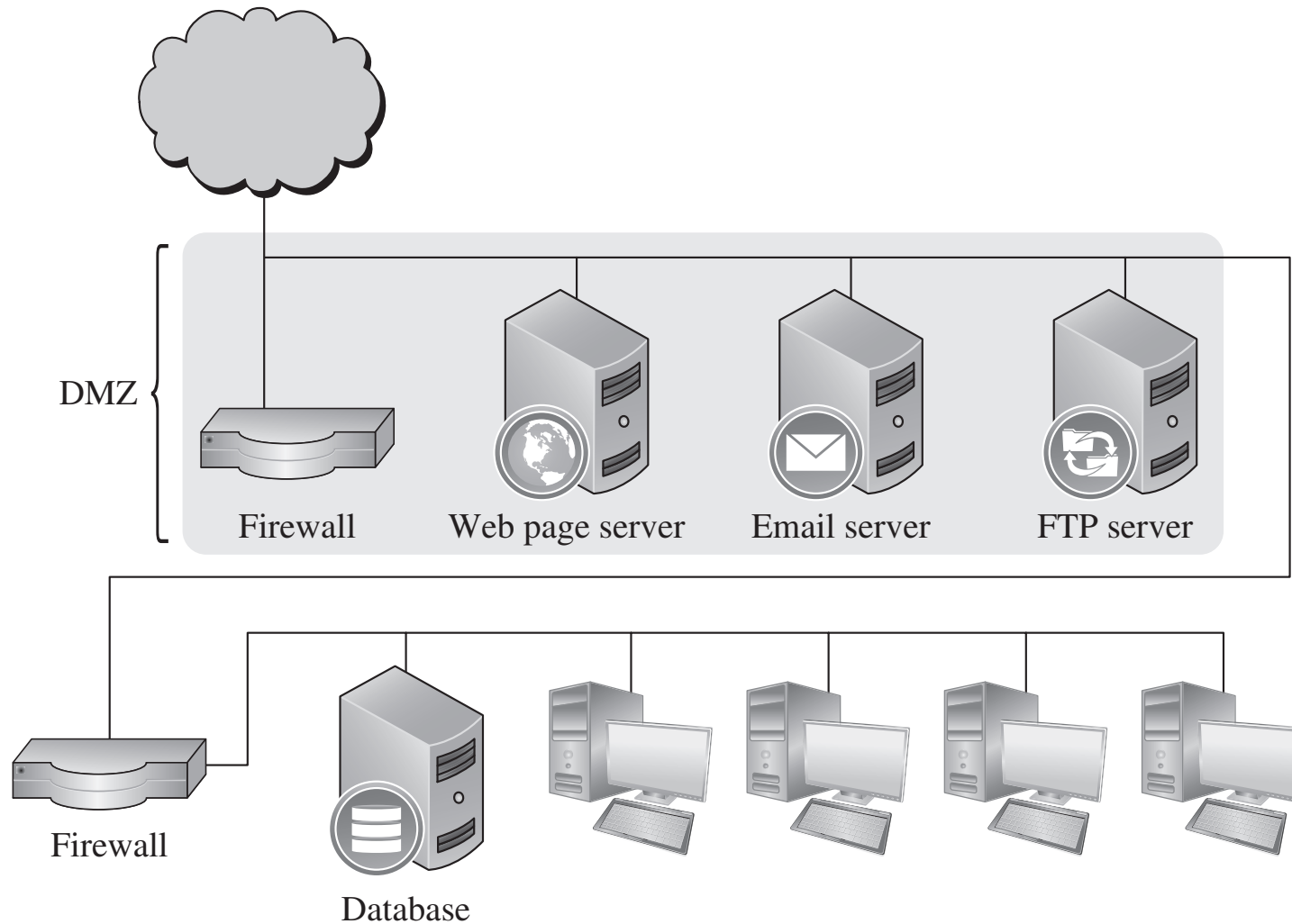


Security Information and Event Management (SIEM)

- Without an SIEM, analysts would need to:
 - log into each device individually on a constant basis
 - manually correlate events on one system against events on another
- This is impossible on any reasonably sized system.

NETWORK ARCHITECTURES

Demilitarized Zone (DMZ)



Demilitarized Zone (DMZ)

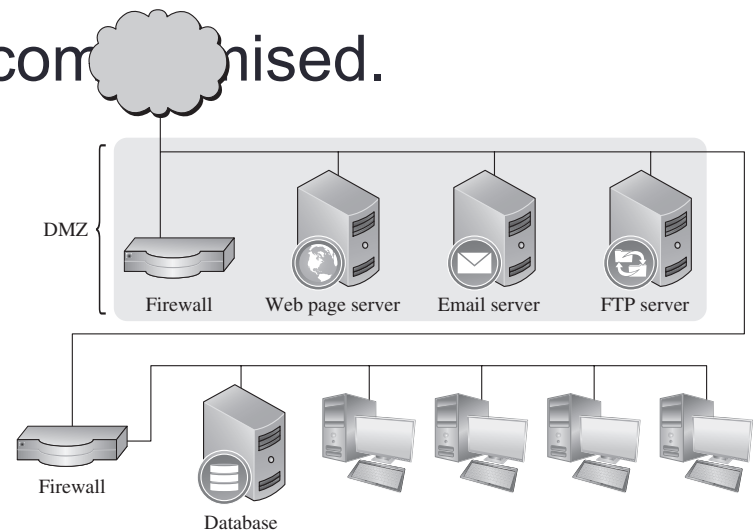
- A form of network architecture
 - A network enclave is dedicated to services that should be somewhat accessible from the outside.

DMZ

- DMZ

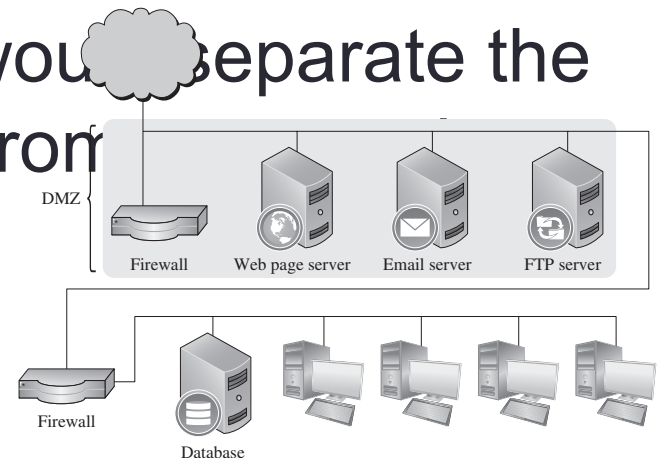
Demilitarized Zone (DMZ) Example

- A firewall protects a DMZ that contains web, email, and FTP servers
- A second firewall protects an internal network—that should not be reachable from the Internet—from the DMZ
 - in case a DMZ host becomes compromised.



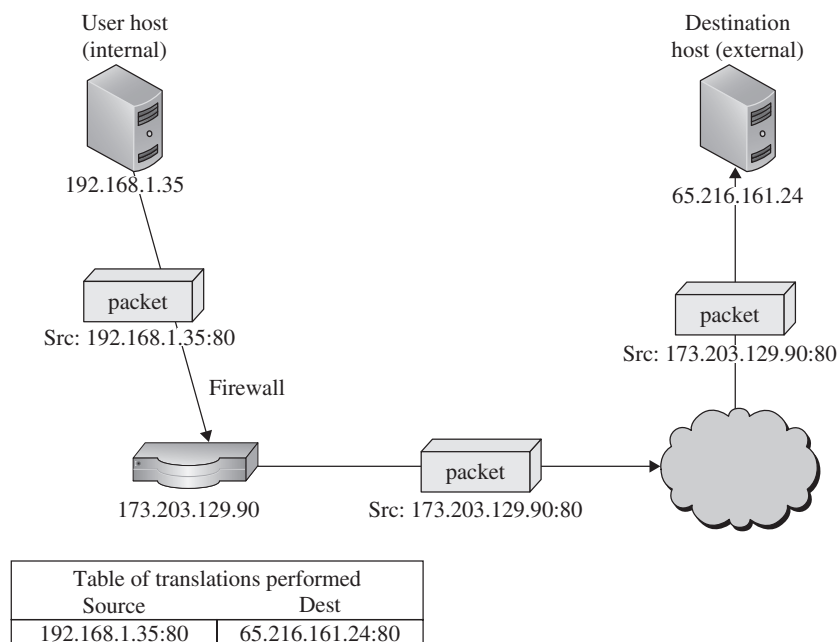
Demilitarized Zone (DMZ) Example

- The hosts that need to be accessible from the Internet are typically the most at risk from outside attacks
- With DMZ, they can only do limited damage
 - to internal hosts that do not need to be reachable from the Internet
- An even more careful option would be to separate the web, email, and FTP servers from
 - with further firewalls



Network Address Translation (NAT)

- A process that can be used by firewalls to prevent IP addresses leakage
 - For example, if internal host sends it to external host it asks for a reply from



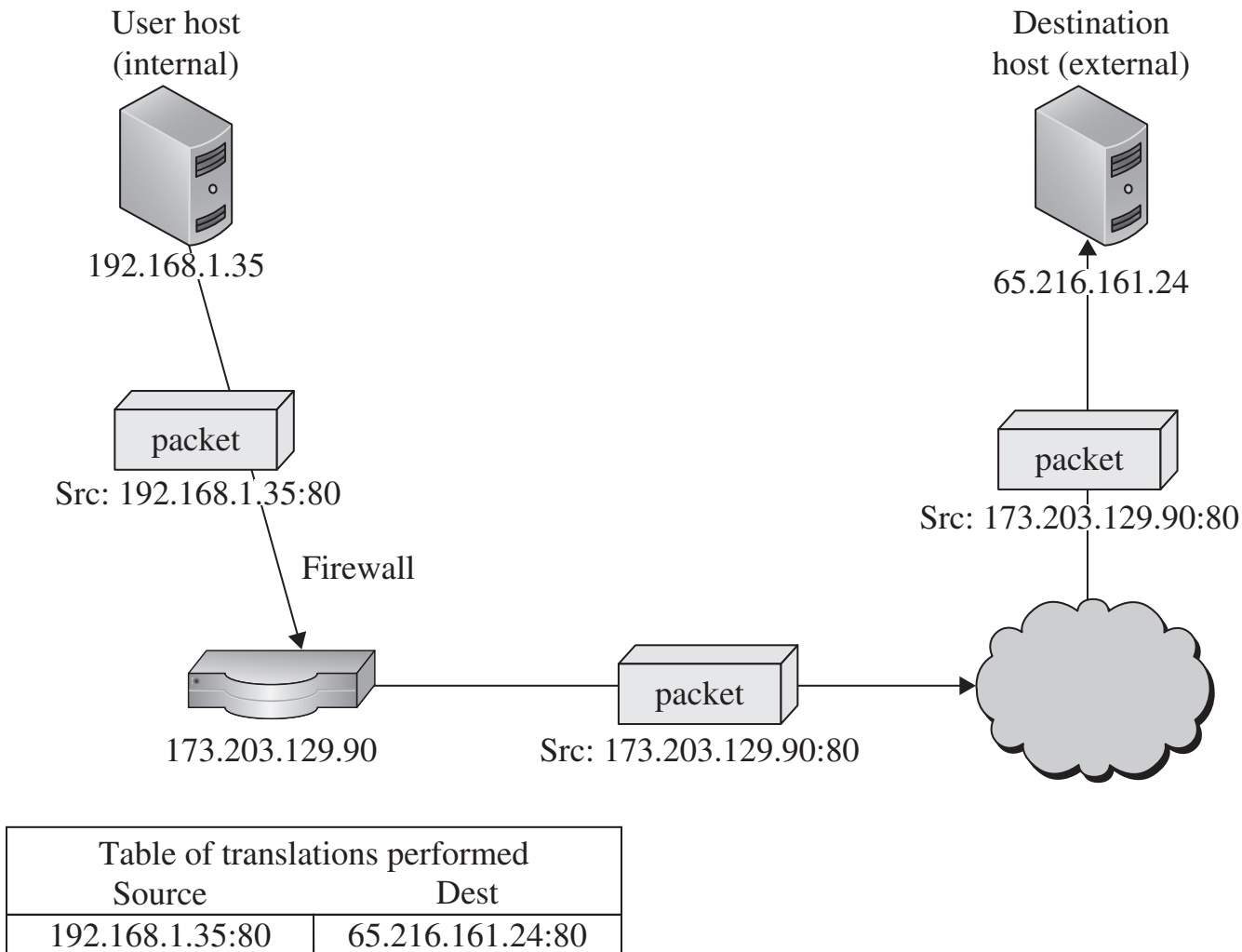
Network Address Translation (NAT)

- The source firewall converts the source address in the packet into the firewall's own address.
- The firewall makes an entry in a translation table
 - Showing the destination address, the source port, and the original source address
 - Enables forwarding replies to the original source address.

Network Address Translation (NAT)

- The firewall converts address back on any return packets
 - This has the effect of concealing the true address of the internal host
 - prevents the internal host from being reached directly

Network Address Translation (NAT)



NAT Firewall

- Allow internet traffic to pass through the gateway only if a device on the private network requested it
- Any unsolicited requests or data packets are discarded
 - preventing communication with potentially dangerous devices on the internet
- If inbound internet traffic does not have a private IP address to forward to beyond the gateway => data should be discarded
 - the NAT firewall then knows the traffic is unsolicited

Data Loss Prevention (DLP)

- Approach similar to firewall or guard
- DLP is a set of technologies that can:
 - Detect (and possibly prevent) attempts to send sensitive data where it is not allowed to go



Data Loss Prevention (DLP)

- Can be implemented as
 - Agent installed as an OS rootkit
 - Network-based solutions
 - Monitor connections and file transfers
 - Applications specific
 - E.g., software for monitoring email
- Indicators DLP looks for:
 - Keywords
 - Traffic patterns
 - Encoding/encryption



Data Loss Prevention (DLP)

- DLP is best for preventing accidental incidents, as malicious users will often find ways to circumvent it



Summary

- Networks are threatened by attacks aimed at interception, modification, fabrication, and interruption
- WPA2 has many critical security advantages over WEP
- Malicious DoS attacks are usually either volumetric in nature or exploit a bug

Summary

- Network encryption can be achieved using specialized tools
 - some for link encryption and some for end-to-end
 - such as VPNs, SSH, and the SSL/TLS protocols

Summary

- A wide variety of firewall types exist
 - ranging from very basic IP-based functionality to complex application-layer logic, and both on networks and hosts
- There are many flavors of IDS
 - each detects different kinds of attacks in very different parts of the network

- Questions?

