# CIT 270: SYSTEMS SECURITY I

# CHAPTER 7: ADMINISTERING A SECURE NETWORK

BYU IDAHO

# INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

**Note**

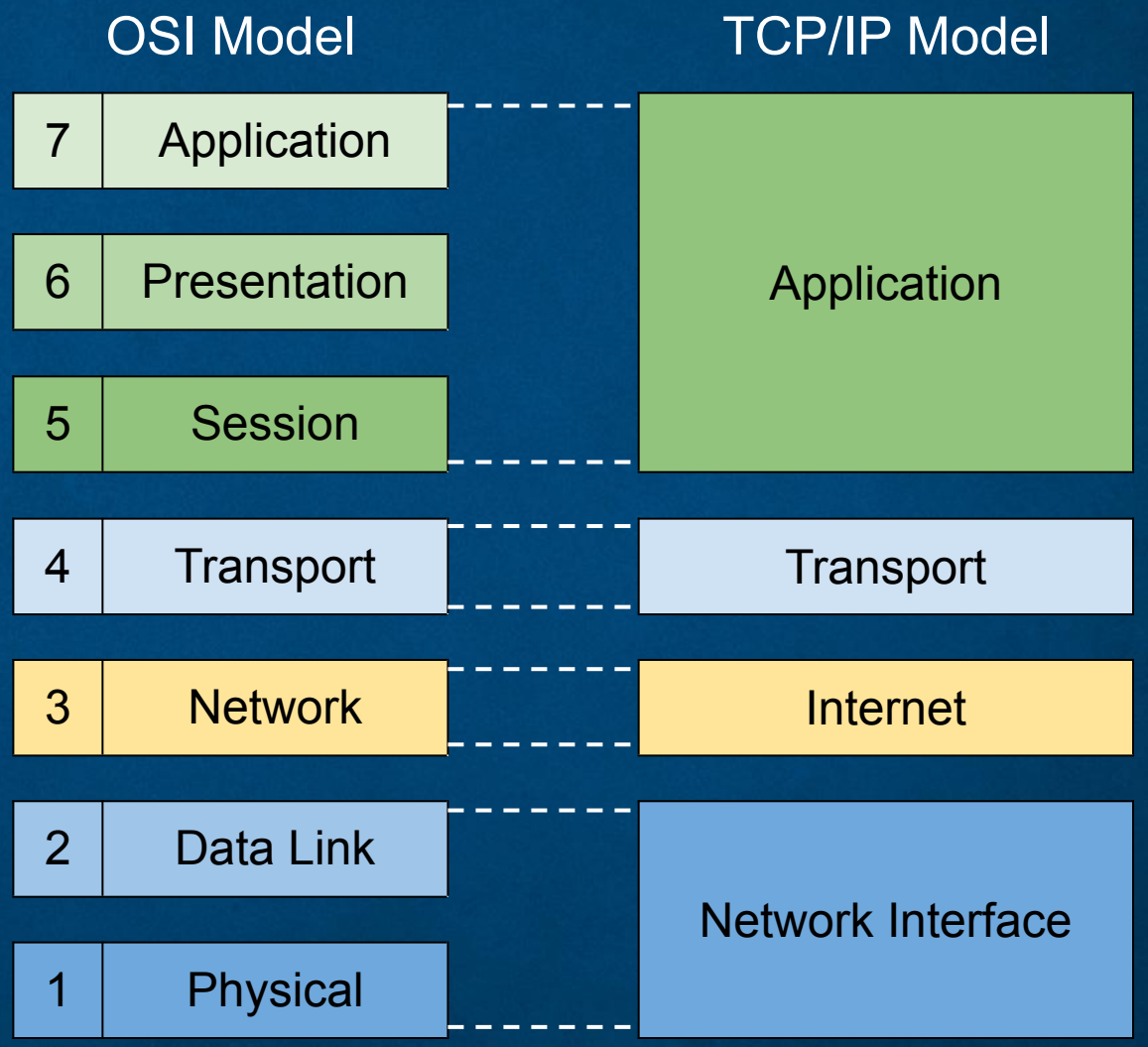
Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

# SECURE NETWORK PROTOCOLS

Computer networks have protocols or rules for communications. TCP/IP is the most common protocol used today and is comprised of several different protocols that all function together as a protocol suite.

IP is responsible for addressing packets and sending them on the correct route while TCP is responsible for reliable packet transmission.



# SECURE NETWORK PROTOCOLS

Simple Network Management Protocol (SNMP): used to manage network equipment allowing administrators to remotely monitor, manage, and configure devices; mixed public and private default settings.

SNMPv3: version 3 of SNMP that supports authentication and encryption.

SNMP is also in some printers, copiers, fax machines, uninterruptible power supplies (UPSs) and so on.

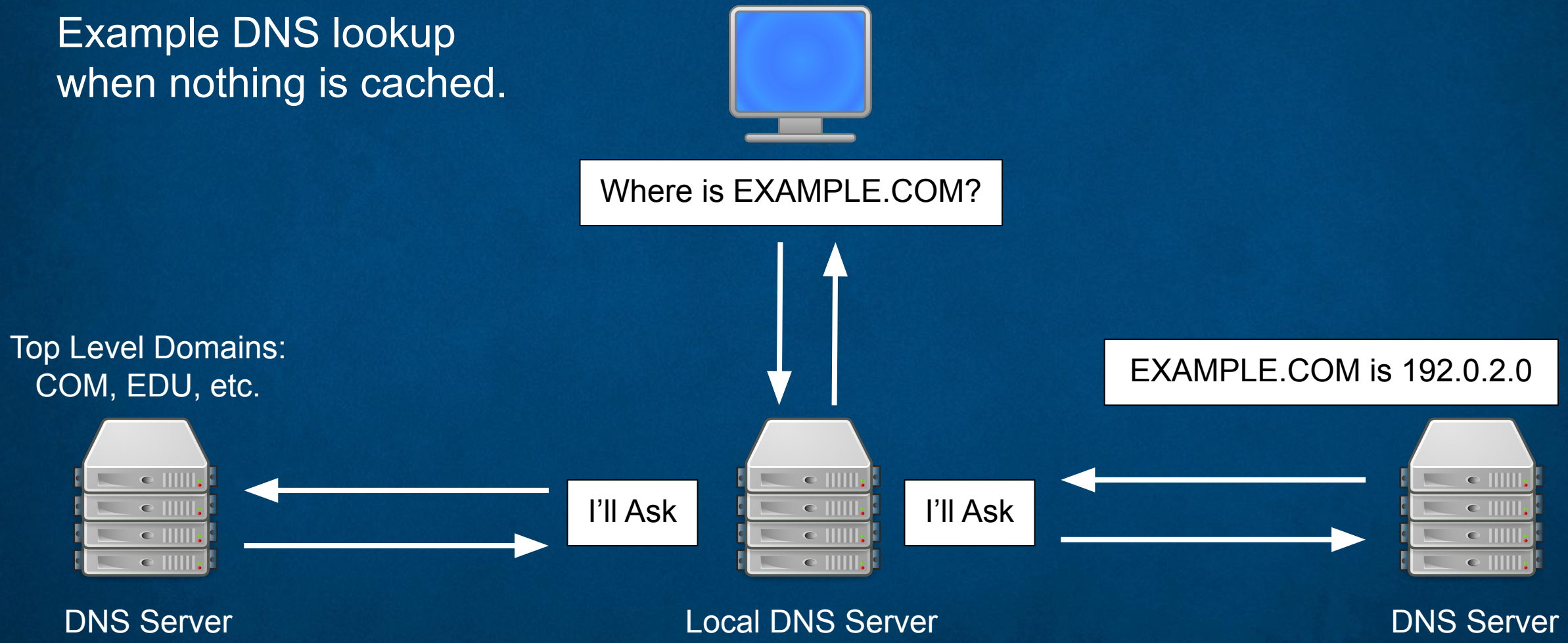
# SECURE NETWORK PROTOCOLS

Because of its importance DNS is often the focus of an attack. Domain Name System Security Extensions (DNSSEC) adds additional resource records and message header information to the DNS process which can be used to verify that requested data has not been altered in transmission.

When a client now request a DNS lookup they can also ask for a DNSSEC digital signature record to verify the response is trustworthy.

# SECURE NETWORK PROTOCOLS

Example DNS lookup
when nothing is cached.



# SECURE NETWORK PROTOCOLS

File Transfer Protocol (FTP): an unsecure TCP/IP protocol used to connect to an FTP server; similar to HTTP connecting to a web server.

FTP Secure (FTPS): uses SSL or TLS to encrypt commands sent over the control port (21) but may or may not encrypt the data port (20); might encrypt.

Secure FTP (SFTP): an entire protocol by itself using a single TCP port that encrypts and compresses all data and commands; will encrypt.

# SECURE NETWORK PROTOCOLS: PROTOCOL RECOMMENDATIONS

| Application or Technology | Recommended Secure Protocol |
|---|---|
| Voice and video | Secure Real-time Transport Protocol (SRTP) |
| Time synchronization | Network Time Protocol (NTP) |
| Email | Secure/ Multipurpose Internet Mail Extensions (S/MIME) |
| Web browsing | Hypertext Transport Protocol Secure (HTTPS) |
| File Transfer | Secure FTP (SFTP) |
| Remote access | Virtual Private Network (VPN) |
| Domain name resolution | DNS Security Extensions (DNSSEC) |
| Routing and switching | IP Security (IPsec) |
| Network address translation | IP Security (IPsec) |
| Subscription services | IP Security (IPsec) |

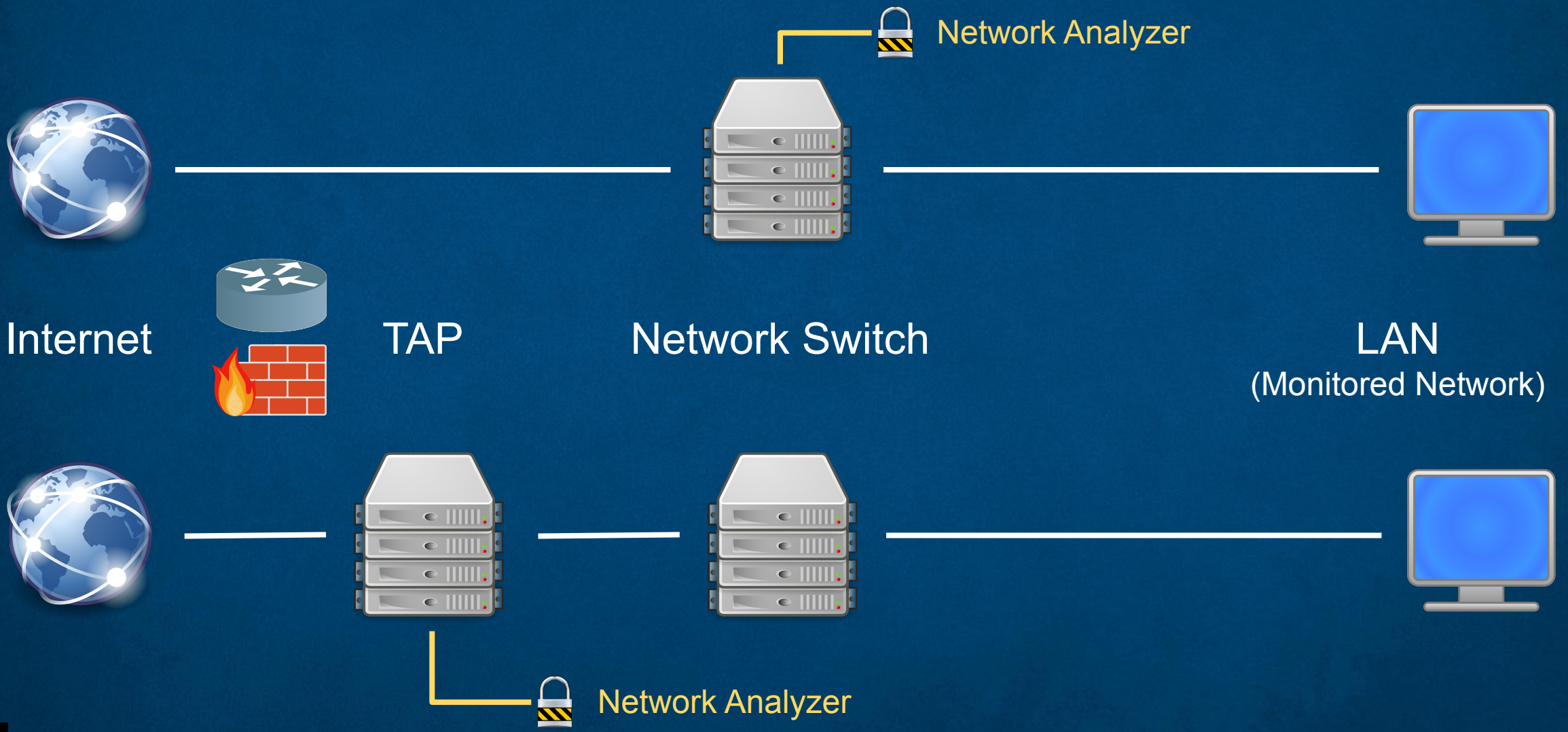
# PLACEMENT OF SECURITY DEVICES AND TECHNOLOGIES

It is important that networks are built properly to insure every security or monitoring device is not only configured properly but has been placed in the correct spot in the network.

Port Mirroring: copies traffic received from a port on a switch and sends it to a dedicated monitoring port on the switch; small scale.

Network Tap / Text Access Point: a separate device that receives a copy of all network traffic for monitoring purposes: large scale.

# PLACEMENT OF SECURITY DEVICES AND TECHNOLOGIES



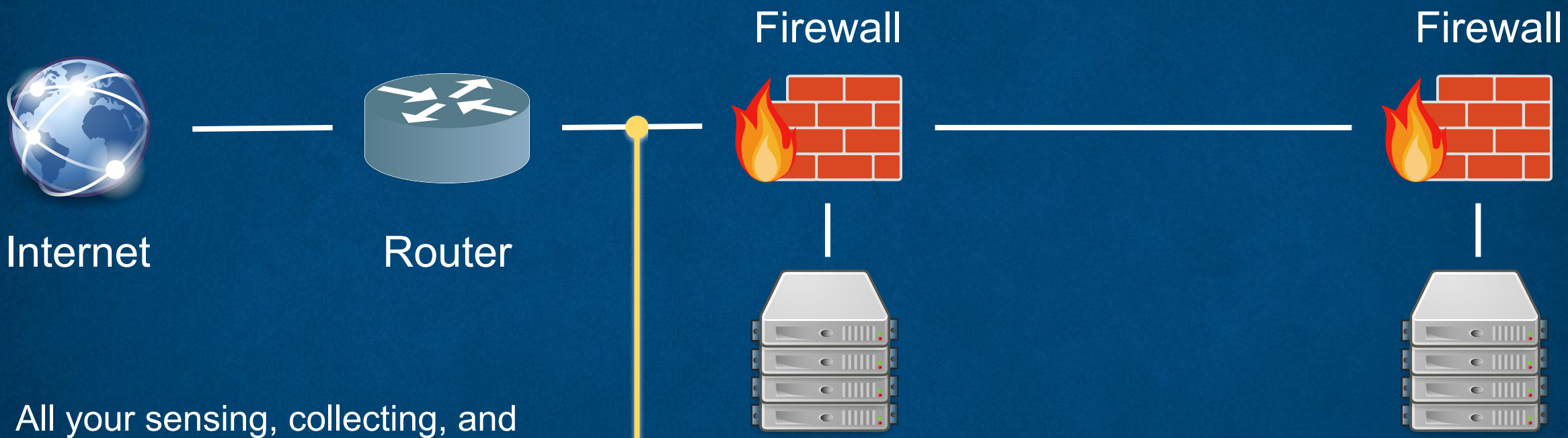
# PLACEMENT OF SECURITY DEVICES AND TECHNOLOGIES

Aggregation Switch: combines multiple network connections into a single link.

Correlation Engine: aggregates and correlates content from different sources to uncover an attack. This is similar to a Security Information and Event Management (SIEM) application but it's focus is on network events; should be protected and internal to your network. Reads logs.

DDoS Mitigator: a hardware device that identifies and blocks real-time distributed denial of service (DDoS) attacks.

# PLACEMENT OF SECURITY DEVICES AND TECHNOLOGIES




All your sensing, collecting, and filtering should happen here. This is the largest point of network traffic and is before any spitting out into your various network segments.

## DMZ

- Web Server
- Email Server

## Internal Network

- Database Server
- Application Server

# ANALYZING SECURITY DATA

Log: accumulated recorded events that have occured on a network or computer.

| Device | Beneficial Security Data |
|---|---|
| Firewalls | Logs inbound and outbound connections, denied traffic, permitted traffic, new IP address attempting to probe the network, and so on. |
| Web Servers | Can keep records of connections and can log or provide valuable information about an attack carried out against it. |
| DHCP Servers | Identify new systems that mysteriously appear and then disappear. Tracks which device had which IP address at specific times. |
| DNS Servers | Shows queries that have been received and can log errors. |
| Routers & Switches | Provide general information about all network traffic. |

# ANALYZING SECURITY DATA

Data Execution Prevention (DEP): a Microsoft Windows feature that prevents attackers from using buffer overflow to execute malware.

File Integrity Check (FIC): a service that can monitor any changes made to a computer's files such as OS files.

Application Whitelisting: an inventory of allowed applications that have been pre-approved to be active and present on a device or network.

Removable Media Control: a tool that can restrict which removable media can be attached to a system; sometimes be spoofed.

# ANALYZING SECURITY DATA

Advanced Malware Management: often a third-party service or tool that monitors a network for any unusual activity; behaviors, heuristic monitoring.

Question: What is Heuristic Analysis?

Malware Protection Techniques (Part 3): Heuristics

# MANAGING AND SECURING NETWORK PLATFORMS: VIRTUALIZATION

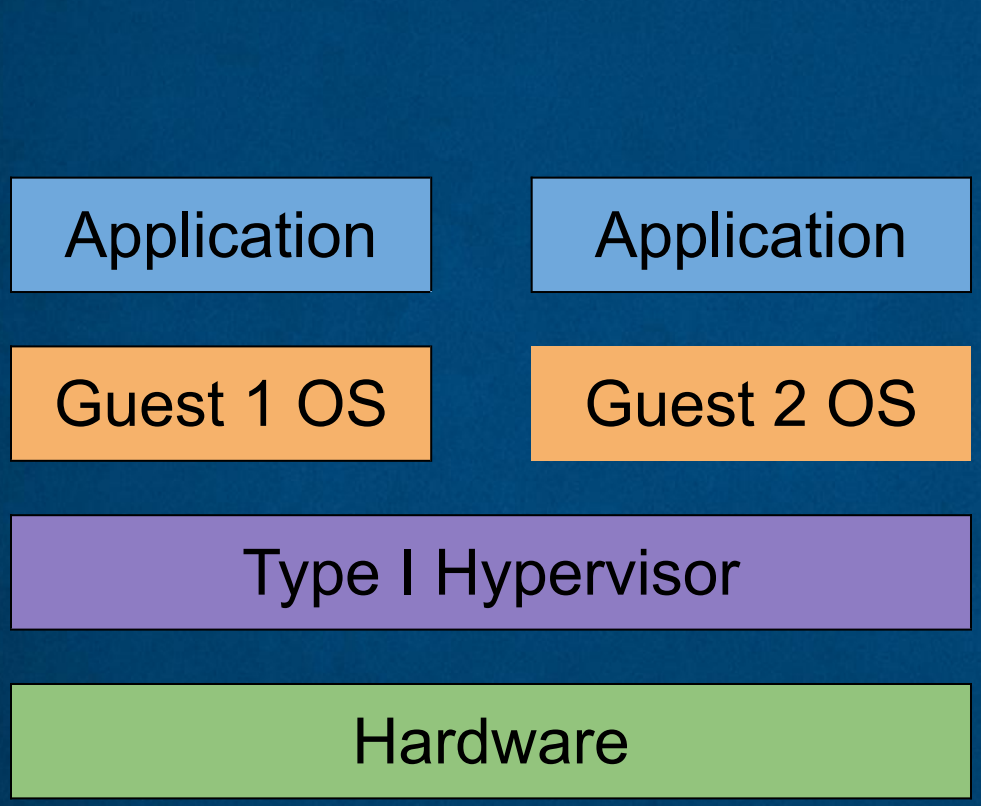
Virtualization: a means of managing and presenting computer resources by function without regard to their physical layout or location.

Hypervisor: the virtual machine monitoring program that manages the virtual machines (VMs) operating systems.

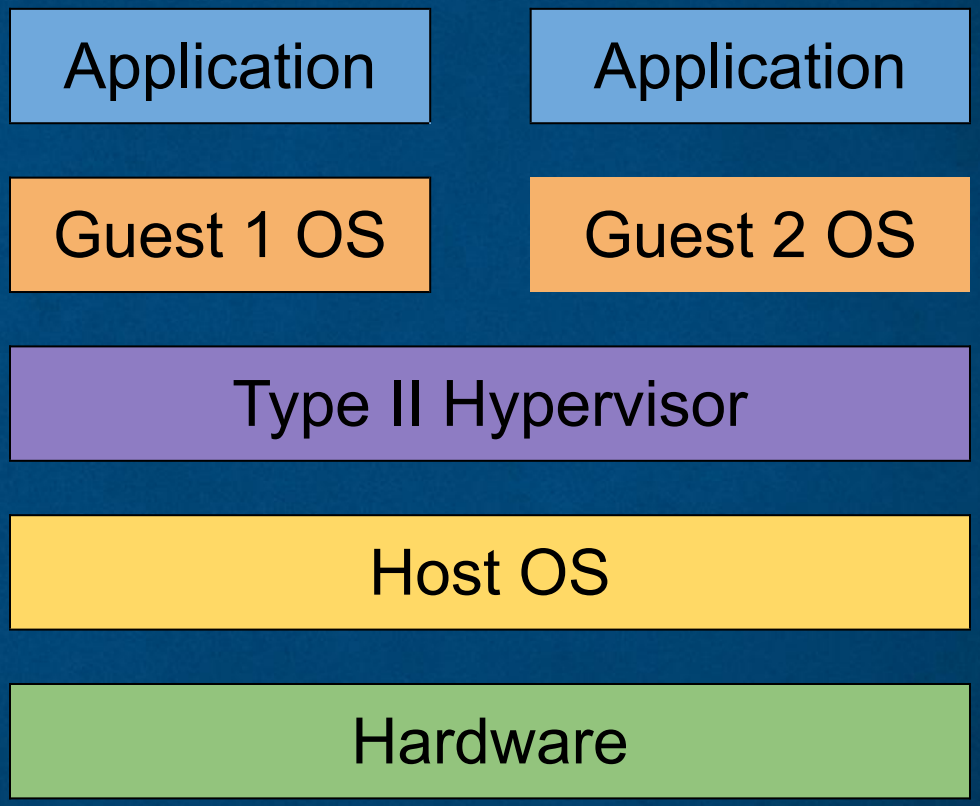
Type I Hypervisor: runs directly on the computer's hardware instead of the underlying operating system.

Type II Hypervisor: run on the host operating system much like a traditional computer application.

# MANAGING AND SECURING NETWORK PLATFORMS: VIRTUALIZATION




Type I Hypervisor




Type II Hypervisor

# MANAGING AND SECURING NETWORK PLATFORMS: VIRTUALIZATION

Virtual Desktop Infrastructure (VDI): the process of running a user's desktop inside a virtual machine on a server.

Virtual Distributed Ethernet (VDE): an Ethernet-compliant virtual network that can connect physical computers and/or virtual machines together.

Virtual Machine Escape Protection: protections that block a VM from directly interacting with the host OS and potentially infecting other VMs; break out.

Virtual Machine Sprawl: the widespread proliferation of virtual machines with little to no management or proper oversight.

# MANAGING AND SECURING NETWORK PLATFORMS: CLOUD COMPUTING

On-premises: a model for managing an enterprises technology where hardware and software is purchased and managed in-house.

Hosted Services: a model for managing an enterprises technology where hardware and software resources are shared (leased) by other enterprises.

Cloud Computing: a pay-per-use computing model where you pay for the amount of resources you use; fast scaling (up or down) of resources, AWS.

# MANAGING AND SECURING NETWORK PLATFORMS: CLOUD COMPUTING

Public Cloud: services and infrastructure are offered to all users with access provided remotely through the internet.

Community Cloud: a cloud open only to specific organizations that have common concerns or needs; hospitals and HIPAA.

Private Cloud: a cloud created and maintained on a private network.

Hybrid Cloud: a combination of public and private clouds.

Cloud Storage: a remote file storage; Google Drive, One Drive.

# MANAGING AND SECURING NETWORK PLATFORMS: CLOUD COMPUTING

Software as a Service (SaaS): the cloud computing vendor provides access to the vendors software applications running on a cloud infrastructure.

Platform as a Service (PaaS): consumers can install their own specialized applications on the cloud computing network; no infrastructure control.

Infrastructure as a Service (IaaS): a step above PaaS where the customer also controls what software is run and which operating system is used.

Security as a Service (SECaaS): all security services are delivered from the cloud to the enterprise; no expensive on-premise hardware needed.

# REFERENCES


Book [PNG]. Flat Icon. https://www.flaticon.com/free-icon/book-opened-outline-from-top-view_30169

“DMZ (Computing).” Wikipedia, Wikimedia Foundation, 13 May 2019, en.wikipedia.org/wiki/DMZ_(computing).

Firewall [PNG]. München: Pixabay GmbH. Free for commercial use. No attribution required.

Internet Globe [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

Lock [PNG]. München: Pixabay GmbH. Free for commercial use. No attribution required.

“Malware Protection Techniques (Part 3): Heuristics” Sourcefire, YouTube, 12 December 2012, https://youtu.be/d7boMCLmnaA

OSI model vs. TCP/IP model [Figure 7-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 284. Boston, MA: Cengage.

# REFERENCES


Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.

“Question: What is Heuristic Analysis?” The Thing of the Name, YouTube, 4 February 2015, https://youtu.be/hLdYx1od-0o

Router [PNG]. München: Pixabay GmbH. Free for commercial use. No attribution required.

Secure network protocol recommendations [Table 7-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 291. Boston, MA: Cengage.

Type I and Type II Hypervisors [Figure 7-8]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 301. Boston, MA: Cengage.