A

Virtual Internship Report on

Cyber Security

Submitted in partial fulfillment of the requirements
for the award of the degree of

Bachelor of Technology

In

Computer Science & Engineering

By

P Anjaneyulu (20B81A05D3)

Under the Esteemed Supervision of

Mr. Sravanan Rajagopal, Training Partner Manager

Edu Skills, Hyderabad

(Duration: September 2022 to November 2022)

DEPARTMENT OF COMPUTR SCIENCE & ENGINEERING

SIR C R REDDY COLLEGE OF ENGINEERING

Approved by AICTE, Permanently affiliated to JNTU, Kakinada

Eluru, Andhra Pradesh

2020-2024

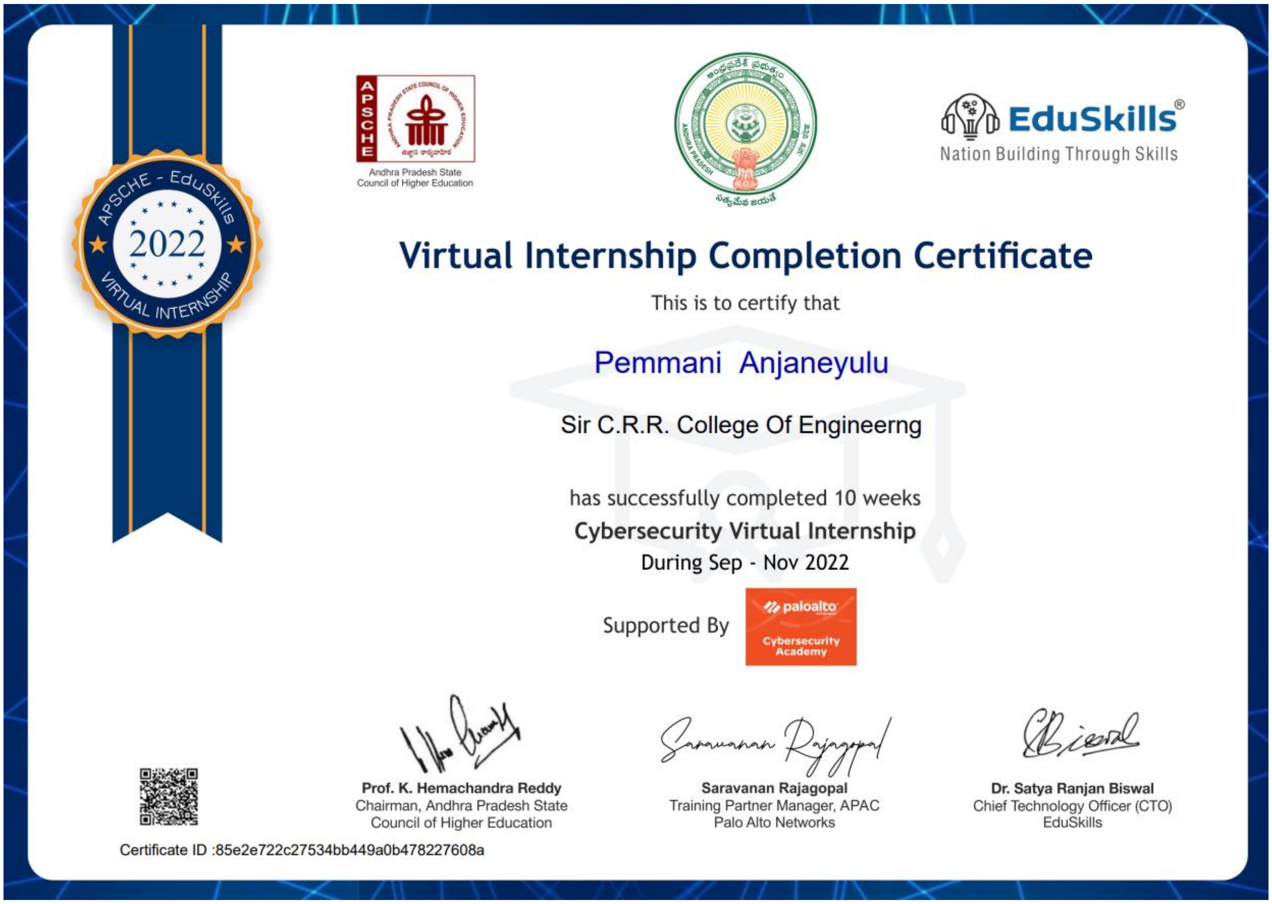
SIR C R REDDY COLLEGE OF ENGINEERING

CERTIFICATE

This is to certify that this Virtual Internship report entitled “**Cyber Security Internship”** submitted by **Pemmani Anjaneyulu (20B81A05D3),**in partial fulfillment for the award of degree of **BACHELOR OF TECHNOLOGY** in **COMPUTER SCIENCE AND ENGINEERING**, at **SIR C R REDDY College of Engineering**, Eluru affiliated to Jawaharlal Nehru Technological University, Kakinada.

Internship Internal Coordinator	**Head of the Department**
K.B.Vara Prasad, M.Tech	Dr. A Yesu Babu, M.Tech, Ph.D
Assistant Professor, CSE	Professor & Head, CSE

External Examiner



APSCHE - EduSkills 2022 VIRTUAL INTERNSHIP

APSCHE

Andhra Pradesh State Council of Higher Education

EduSkills®

Nation Building Through Skills

Virtual Internship Completion Certificate

This is to certify that

Pemmani Anjaneyulu

Sir C.R.R. College Of Engineerng

has successfully completed 10 weeks

Cybersecurity Virtual Internship

During Sep - Nov 2022

Supported By paloalto Cybersecurity Academy

Saravanan Rajagopal

Prof. K. Hemachandra Reddy
Chairman, Andhra Pradesh State
Council of Higher Education

Saravanan Rajagopal
Training Partner Manager, APAC
Palo Alto Networks

Dr. Satya Ranjan Biswal
Chief Technology Officer (CTO)
EduSkills

Certificate ID :85e2e722c27534bb449a0b478227608a

CERTIFICATE LINK:

https://drive.google.com/file/d/18xJpjYTletRVKvN6_7Phsj633D40F0Cw/view?usp=share_link

ABSTRACT

Computer security, **cybersecurity** (**cyber security**), or **information technology security** (**IT security**) is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

While most aspects of computer security involve digital measures such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering.

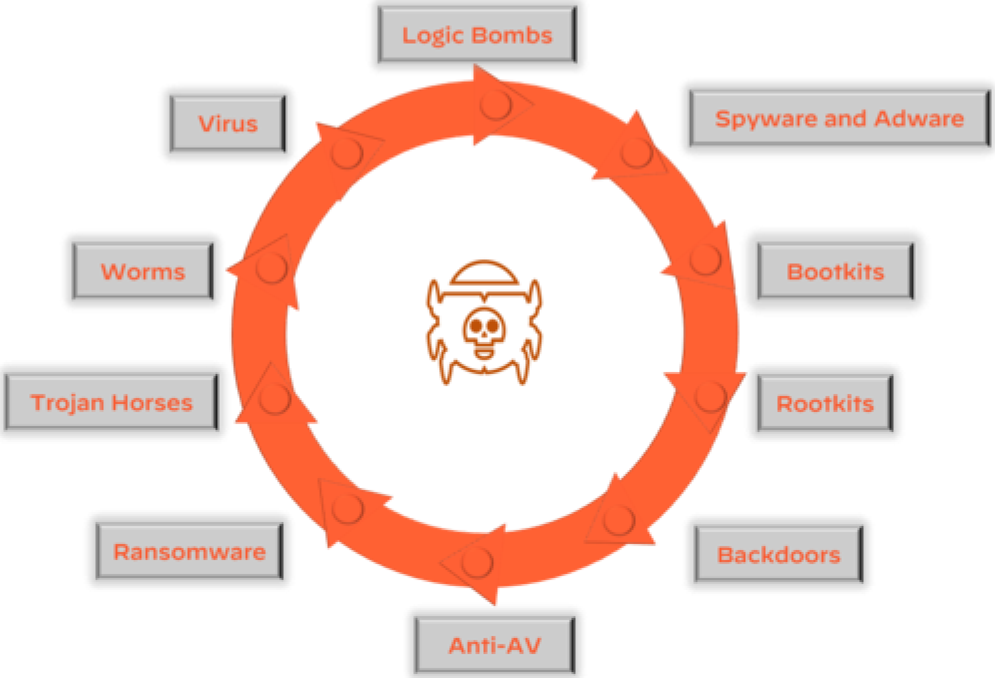
The field has become of significance due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to the complexity of information systems, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy.

.

Lesson 2: Cyberattack Types:

Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack strategy. This lesson describes the different malware types and properties, the relationship between vulnerabilities and exploits, and how modern malware plays a central role in a coordinated attack against a target. This lesson also explains the timeline of eliminating a vulnerability.

Malware Types:



Logic Bombs

A logic bomb is malware that is triggered by a specified condition, such as a given date or a particular user account being disabled.

Spyware and adware

Spyware and adware are types of malwares that collect information, such as internet surfing behavior, login credentials, and financial account information, on an infected endpoint. Spyware often changes browser and other software settings and slows computer and internet speeds on an infected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as pop-up banners.

Rootkits

A rootkit is malware that provides privileged (root-level) access to a computer. Rootkits organizations face today. The FBI Internet Crime Complaint Center (IC3) estimates that "in aggregate" BEC attacks cost organizations three times more than any other cybercrime and BEC incidents represented nearly a third of the incidents investigated by Palo Alto Networks Unit 42 Incident Response Team in 2021. According to the Verizon 2021 Data Breach Investigations Report (DBIR), BEC is the second most common form of social engineering today.

Phishing Attacks

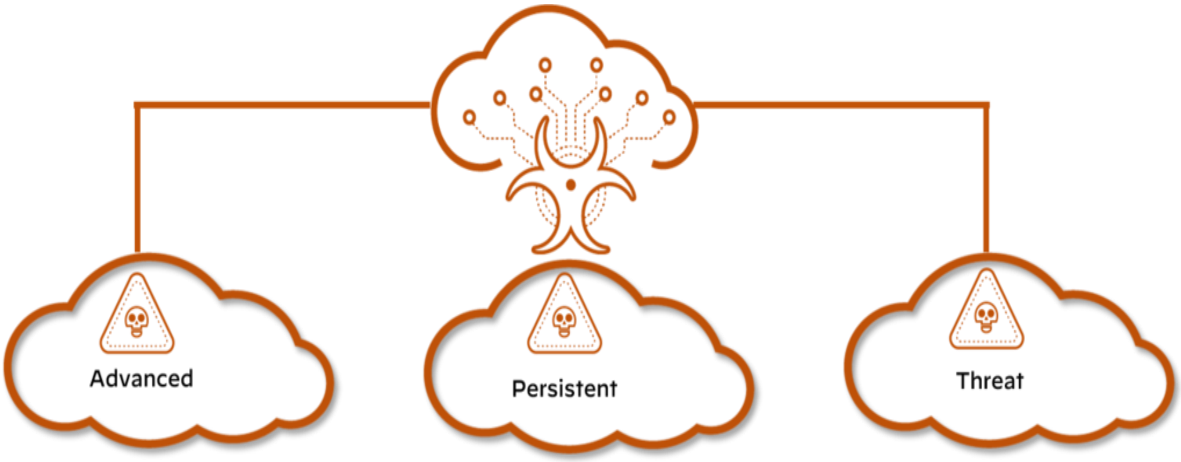
We often think of spamming and phishing as the same thing, but they are actually separate processes, and they each require their own mitigations and defenses. Phishing attacks, in contrast to spam, are becoming more sophisticated and difficult to identify and many more types of attacks

Lesson 4: Advanced Persistent Threats and Wi-Fi Vulnerabilities

With the explosive growth in fixed and mobile devices over the past decade, wireless (Wi-Fi) networks are growing exponentially—and so is the attack surface for advanced persistent threats (ATP). This lesson describes Wi-Fi vulnerabilities and attacks and APTs.

Advanced Persistent Threats

Advanced persistent threats, or APTs, are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. APTs are generally coordinated events that are associated with cybercriminal groups.



Lazarus

Attacks against nation-states and corporations are common, and the group of cybercriminals that may have done the most damage is Lazarus. The Lazarus group is known as an APT. The Lazarus group has been known to operate under different names, including Bluenoroff and Hidden Cobra. They were initially known for launching numerous attacks against government and financial institutions in South Korea and Asia. In more recent years, the Lazarus group has been targeting banks, casinos, financial investment software developers, and crypto-currency businesses. The malware attributed to this group recently has been found in 18 countries around the world.

Lesson 5:Security

Models

The goal of a security model is to provide measurable threat prevention through trusted and untrusted entities. This can be a complicated process, as every security model will have its own customizations and many variables need to be identified. This lesson describes the core concepts of a security model and why the model is important, the functions of a perimeter-based security model, the Zero Trust security model design principles, and how the principle of least privilege applies to the Zero Trust security model.

Perimeter-Based Security Model

Perimeter-based network security models date back to the early mainframe era (circa late 1950s), when large mainframe computers were located in physically secure “machine rooms.” These rooms could be accessed by a limited number of remote job entry (RJE) terminals directly connected to the mainframe in physically secure areas.

Relies on Physical Security

Today’s data centers are the modern equivalent of machine rooms, but perimeter-based physical security is no longer sufficient. Click the arrows for more information about several obvious but important reasons for the security issues associated with perimeter-based security.

Fundamentals of Network Security

This training introduces someone with no prior knowledge to the fundamentals of network security including concepts they must understand to recognize and potentially defend home networks and mission-critical infrastructure.

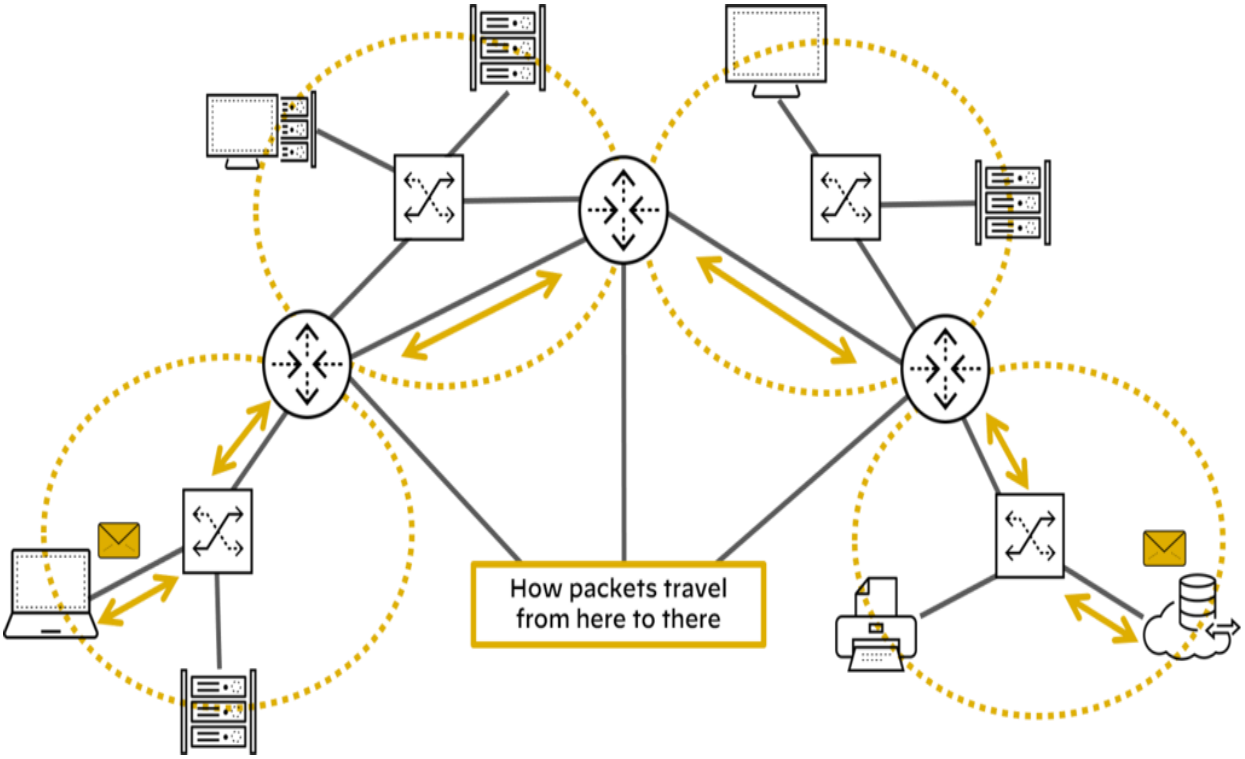
After completing this training, you should be able to:

- Describe basic operations of enterprise networks, common networking devices, routed and routing protocols, network types and topologies, and services such as DNS
- Explain IP addressing, subnetting, and packet encapsulation based on the Open Systems Interconnection (OSI) model
- Describe network security technologies such as packet filtering, stateful inspection, application firewalls, and IDS and IPS and web content filters
- Explain how to explore endpoint and mobile device security using technology such as personal firewalls, host-based IPS, and management features
- Describe how to properly secure enterprise networks through PAN-OS deployment templates and migration options and DNS, URL Filtering, Threat Prevention, and WildFire® subscription services

Lesson Topics

This training comprises five lessons and takes about two hours to complete.

- Lesson 1: The Connected Globe



Today billions of devices worldwide are connected to the Internet and use the transport communications protocol/internet protocol (TCP/IP) to communicate with each over packet-switched networks. Specialized devices and technologies such as routers, routing protocols, SD-WAN, the domain name system (DNS) and the world wide web (WWW) facilitate communications between connected devices.

Lesson 2: Addressing and Encapsulation

This lesson describes the functions of physical, logical, and virtual addressing in networking, IP addressing basics, subnetting fundamentals, OSI and the TCP/IP models, and the packet lifecycle.

TCP/IP Overview

In cybersecurity, you must understand that applications sending data from one host computer to another host computer will first segment the data into blocks and will then forward these data blocks to the TCP/IP stack for transmission.

TCP/IP Protocol Stack

The TCP stack places the block of data into an output buffer on the server and determines the maximum segment size of individual TCP blocks permitted by the server operating system. The TCP stack then divides the data blocks into appropriately sized segments, adds a TCP header, and sends the segment to the IP stack on the server.

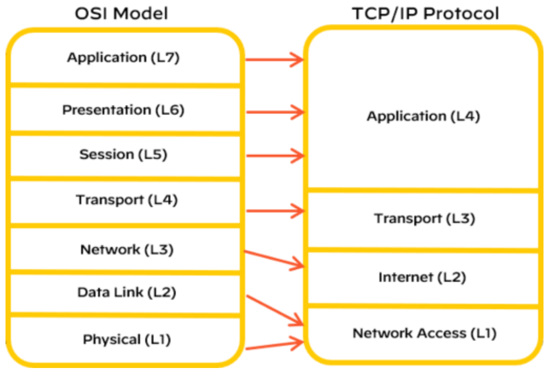
The IP stack adds source and destination IP addresses to the TCP segment and notifies the server operating system that it has an outgoing message that is ready to be sent across the network. When the server operating system is ready, the IP packet is sent to the network adapter

Introduction to Subnetting

Subnetting is a technique used to divide a large network into smaller, multiple subnetworks by segmenting an IP address into two parts: the network portion of the address and the host portion of the address.

OSI Model and TCP/IP Protocol Layers

The OSI model is defined by the International Organization for Standardization and consists of seven layers. This model is a theoretical model used to logically describe networking processes



Lesson 3: Network Security Technologies

In this lesson, we will discuss the basics of network security technologies such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), web content filters, virtual private networks (VPNs), data loss prevention (DLP), and unified threat management (UTM), which are deployed across the industry.

Legacy Firewalls

Firewalls have been central to network security since the early days of the internet. A firewall is a hardware platform or software platform or both that controls the flow of traffic between a trusted network (such as a corporate LAN) and an untrusted network (such as the internet).

Packet Filtering Firewalls

First-generation packet filtering (also known as port-based) firewalls have the following characteristics:

Operation

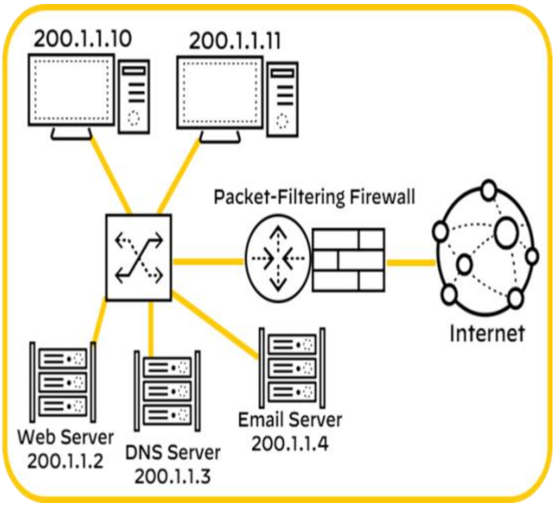
Packet filtering firewalls operate up to Layer 4 (Transport layer) of the OSI model and inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, ICMP), and port number.

Match

Packet filtering firewalls match source and destination IP address, protocol, and port number information contained within each packet header to a corresponding rule on the firewall that designates whether the packet should be allowed, blocked, or dropped.

Inspection

Packet filtering firewalls inspect and handle each packet individually, with no information about context or session.

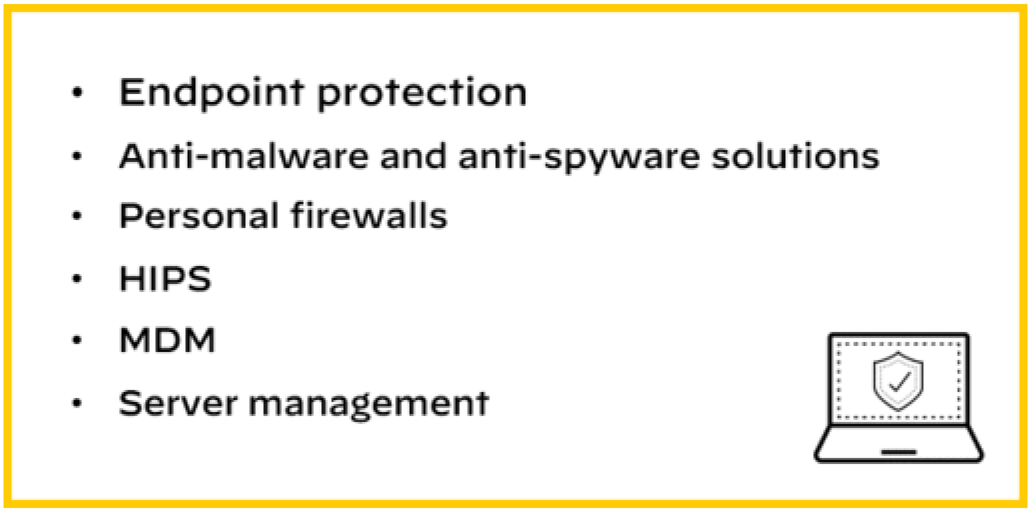


Lesson 4: Endpoint Security and Protection

In this lesson, we will explore endpoint security challenges and solutions, including malware protection, anti-malware software, personal firewalls, host-based intrusion prevention systems (HIPSs), and mobile device management (MDM) software. We will also introduce network operations concepts, including server and systems administration, directory services, and structured host and network troubleshooting.

Endpoint Security

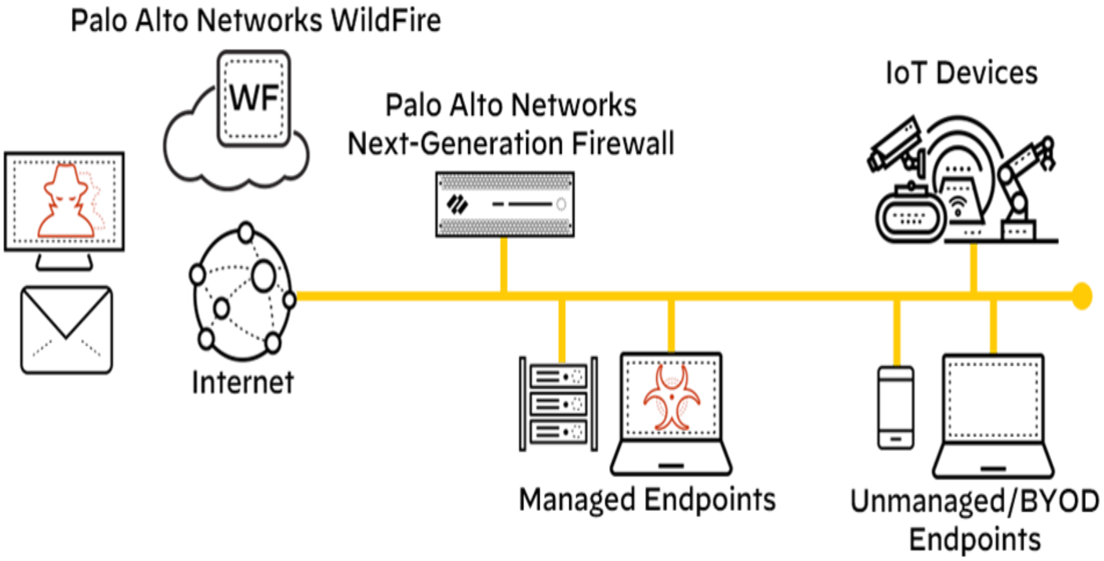
In 2022, there were more than 11.5 billion internet of things (IoT) devices worldwide, including machine-to-machine (M2M), wide-area IoT, short-range IoT, massive-and-critical IoT, and multi-access edge computing (MEC) devices. Traditional endpoint security encompasses numerous security tools



- Endpoint protection
- Anti-malware and anti-spyware solutions
- Personal firewalls
- HIPS
- MDM
- Server management

Endpoint Protection

Advanced malware and script-based attacks can bypass traditional antivirus solutions with ease and potentially wreak havoc on your business.


Palo Alto Networks WildFire
WF
Palo Alto Networks Next-Generation Firewall
IoT Devices
Internet
Managed Endpoints
Unmanaged/BYOD Endpoints

Lesson 5: Secure the Enterprise

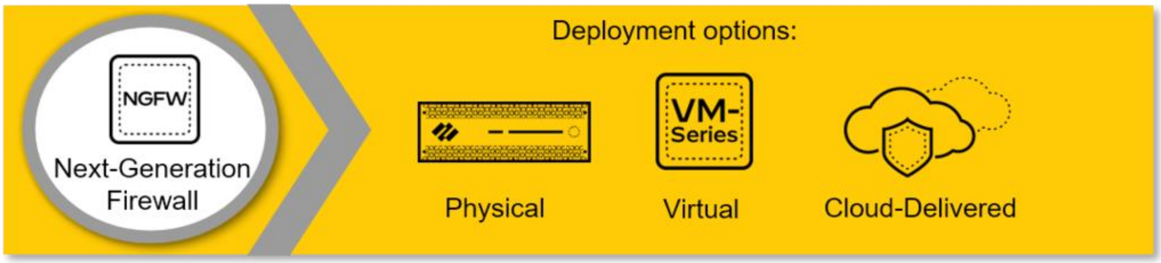
The networking infrastructure of an enterprise can be extraordinarily complex. The Palo Alto Networks prevention-first security architecture secures enterprises' perimeter networks

Prevention-First Architecture

Simplifying your security posture allows you to reduce operational costs and infrastructure while increasing your ability to prevent threats to your organization.

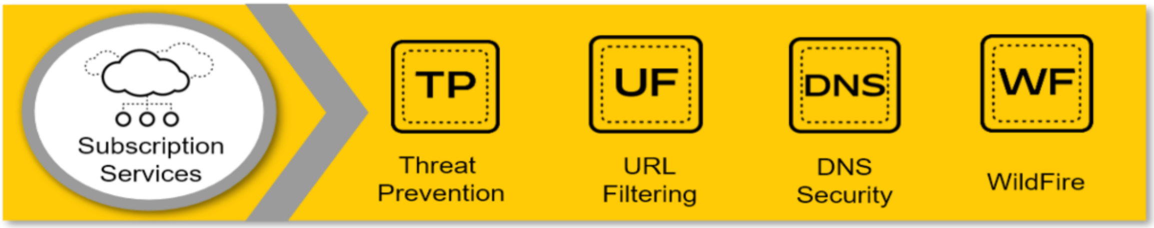
Next-Generation Firewall

The Palo Alto Networks Next-Generation Firewall is the foundation of our product portfolio. The firewall is available in physical, virtual, and cloud-delivered deployment options



Subscription Services

Subscription services add enhanced threat services and next-generation firewall capabilities, including DNS Security, URL Filtering, Threat Prevention, and WildFire malware prevention.



Panorama

Panorama provides centralized network security management. It simplifies administration while delivering comprehensive controls and deep visibility into network-wide traffic and security threats.

PN
Panorama
Centralized network security management and administration
Visibility into network-wide traffic and security threats

Lesson 1: Cloud Computing

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively.

Definition

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner. Read the quote below for the definition of cloud computing according to the U.S. National Institute of Standards and Technology.

Cloud Computing Ecosystem

The cloud computing ecosystem consists of service models, deployment models, responsibilities, and security challenges.

Service Models, Deployment Models, and Responsibilities

Virtualization is a critical component of a cloud computing architecture that, when combined with software orchestration and management tools that are covered in this course, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

Shared Responsibility Model

The security risks that threaten your network today do not change when you move from on-premises to the cloud. The shared responsibility model defines who (customer and/or provider) is responsible for what (related to security) in the public cloud.

Cloud Security Responsibilities

In general terms, the cloud provider is responsible for security of the cloud, including the physical security of the cloud data centres, and foundational networking, storage, compute, and virtualization services.

Lesson 2: Cloud Native Technologies

Like a new universe, the cloud native ecosystem has many technologies and projects quickly spinning off and expanding from the initial core of containers.

Cloud Native Technology Properties

A useful way to think of cloud native technologies is as a continuum spanning from virtual machines (VMs) to containers to serverless. On one end are traditional VMs operated as stateful entities, as we’ve done for over a decade now. On the other are completely stateless, serverless apps that are effectively just bundles of app code without any packaged accompanying operating system (OS) dependencies.

Virtualization

Virtualization is the foundation of cloud computing. You can use virtualization to create multiple virtual machines to run on one physical host computer.

Overview

You can think of virtual machines as separate computers running various operating systems on a physical host computer. Virtual machines and their associated operating systems often are referred to as “virtual guest operating systems.” These virtual guest operating systems all share the physical compute resources: processors, dynamic memory (RAM), and permanent storage media of a physical host machine.

Hypervisor

Hypervisor software allows multiple, virtual guest operating systems to run concurrently on a single physical host computer. The hypervisor functions between the computer operating system and the hardware kernel.

Lesson 3: Cloud Native Security

The speed and flexibility that are so desirable in today’s business world have led companies to adopt cloud technologies that require not just more security but new security approaches. In the cloud, you can have hundreds or even thousands of instances of an application, presenting exponentially greater opportunities for attack and data theft.

The Four Cs of Cloud Native Security

The CNCF defines a container security model for Kubernetes in the context of cloud native security. Each layer provides a security foundation for the next layer.

Cloud

The cloud (and data centres) provide the trusted computing base for a Kubernetes cluster. If the