***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
* Lesson 2: Addressing and Encapsulation
* Lesson 3: Network Security Technologies
* Lesson 4: Endpoint Security and Protection
* Lesson 5: Secure the Enterprise

***Lesson 1: The Connected Globe***

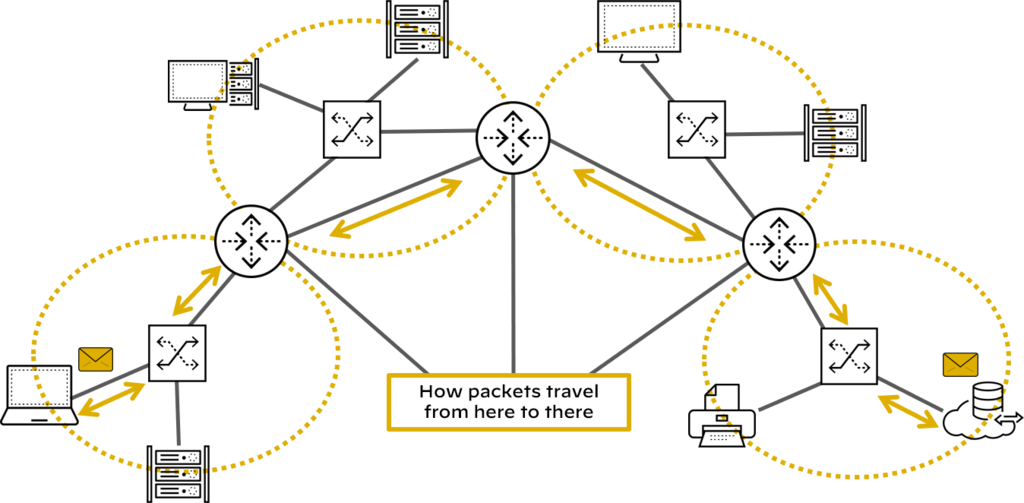
In this lesson, we will discuss how hundreds of millions of routers deliver Transmission Control Protocol/Internet Protocol (TCP/IP) packets using various routing protocols across local-area networks and wide-area networks. We also will discuss how the Domain Name System (DNS) enables internet addresses, such as www.paloaltonetworks.com, to be translated into routable IP addresses.

**The Net**

In the 1960s, the U.S. Defense Advanced Research Projects Agency (DARPA) created ARPANET, the precursor to the modern internet. ARPANET was the first packet-switched network. A packet-switched network breaks data into small blocks (packets), transmits each individual packet from node to node toward its destination, and then reassembles the individual packets in the correct order at the destination.

**How Things Connect**

The ARPANET evolved into the internet (often referred to as the network of networks) because the internet connects multiple local area networks (LAN) to a worldwide wide area network (WAN) backbone.



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.

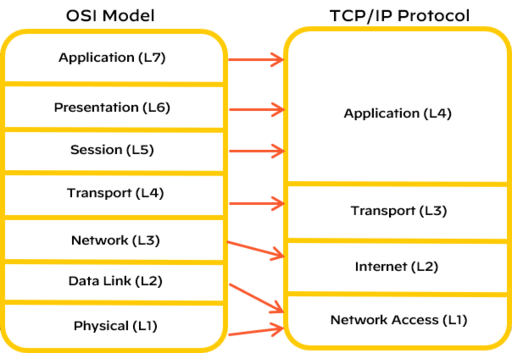
The IP stack adds source and destination IP addresses to the TCP segment and notifies the server operating system that it has an outgoing message that is ready to be sent across the network. When the server operating system is ready, the IP packet is sent to the network adapter

**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**

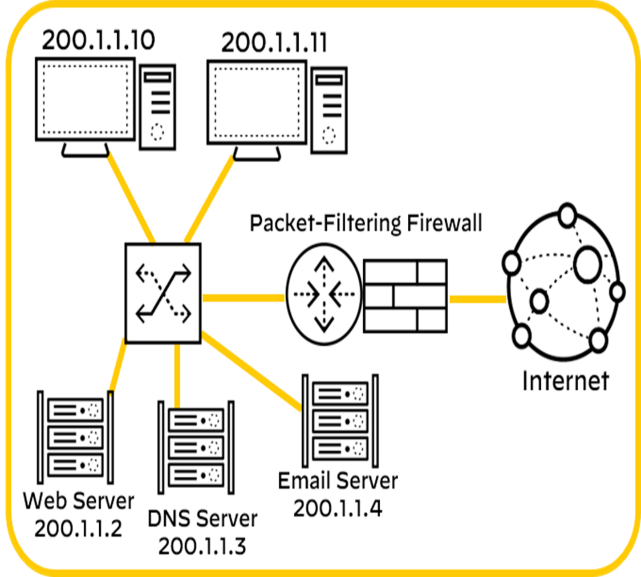
Packet filtering firewalls operate up to Layer 4 (Transport layer) of the OSI model and inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, ICMP), and port number.

**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.

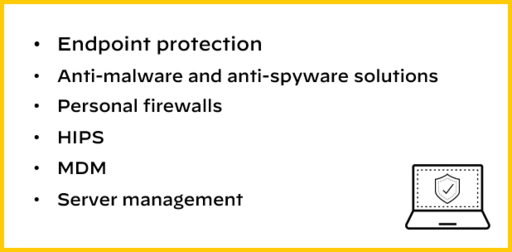


***Lesson 4: Endpoint Security and Protection***

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.

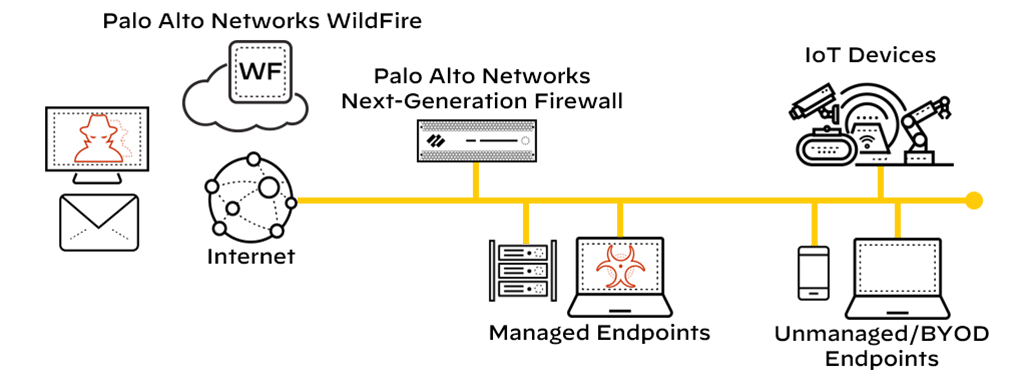
**Endpoint Security**

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**

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



***Lesson 5: Secure the Enterprise***

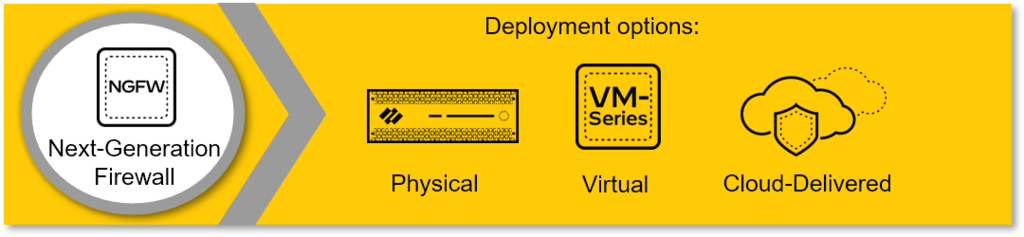
The networking infrastructure of an enterprise can be extraordinarily complex. The Palo Alto Networks prevention-first security architecture secures enterprises' perimeter networks

**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.

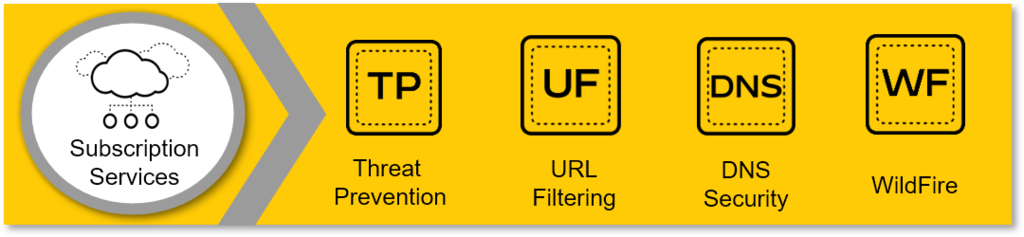
**Next-Generation Firewall**

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.