FIREWALL 10.2 ESSENTIALS: CONFIGURATION AND MANAGEMENT

LET'S GET STARTED!

- Welcome and introductions
- Intended audience and course focus
- Course objectives and modules
- Course exam and certification information
- Beacon learning tasks

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Class Introductions

- Welcome to the class!
- Important facts:
  - Times (start, end, lunch, breaks)
  - Places (lunch/break room, restrooms, emergency exits)
- Please introduce yourself:
  - Name
  - Company and position
  - Relevant experience
  - What are you are hoping to learn?

Intended Audience

- This course is designed for:
  - Security engineers
  - Security administrators
  - Security operators
  - Security analysts
  - Security architects
- This course assumes a working knowledge of:
  - Routing and switching
  - IP addressing
  - Basic security concepts

The course is intended for security engineers, administrators, operators, analysts, and architects.

Students must have a basic familiarity with networking concepts including routing, switching, and IP addressing, and with security concepts.

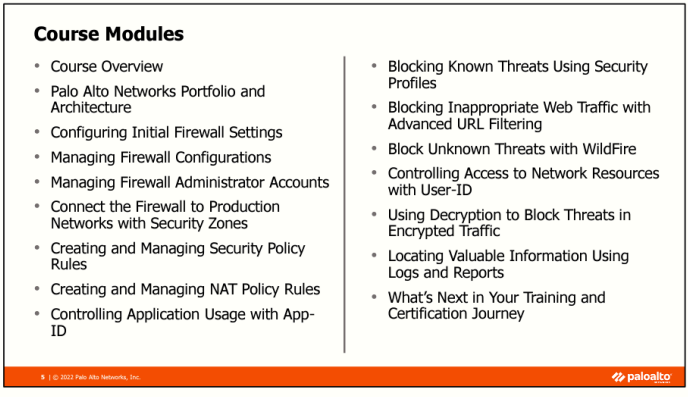
Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

Learning Objectives

After you complete this module,
you should be able to:

- Use network segmentation to reduce your attack surface
- Use App-ID to block threats by identifying applications
- Use Content-ID to block threats from known bad sources
- Use User-ID to block threats by identifying users
- Use firewall logs to view threats and traffic information

The course objectives are listed here.

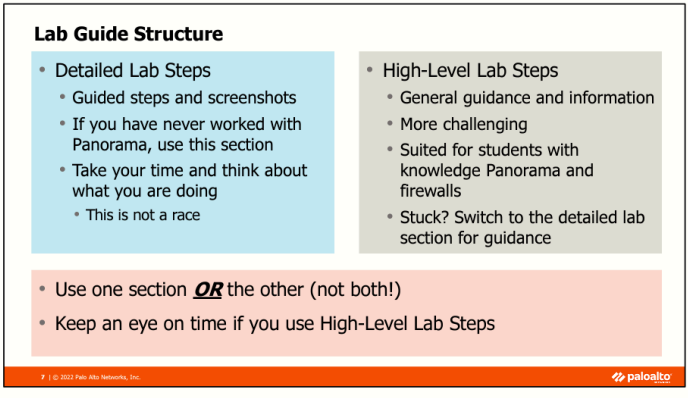


The module titles are listed here.

Blended Learning Modules

- Appendix A - Securing Endpoints with GlobalProtect
- Appendix B - Providing Firewall Redundancy with High Availability
- Appendix C - Connecting Remotes Sites using VPNs
- Appendix D – Configuring the User-ID Windows Agent

The module titles are listed here.



There are two sections for each lab in this guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with the firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

You do not need to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Use either one or the other.

Informal Post-Class Assessment

Evaluate your post-class knowledge and skills with a free, online assessment.

- Take the assessment within one week of course completion.
- To access the assessment:
  - Browse to
    - https://beacon.paloaltonetworks.com (external students)
    - https://flexlearn.paloaltonetworks.com (internal students)
  - Log in, search for the course number (i.e., "210"), click the course link, then select the assessment.
- Format: Open-book, true/false and multiple-choice questions (four to six questions per module)

Use your results to evaluate what you have learned so far and to refine your study plan for technical certification.

8 | © 2022 Palo Alto Networks, Inc.

paloalto

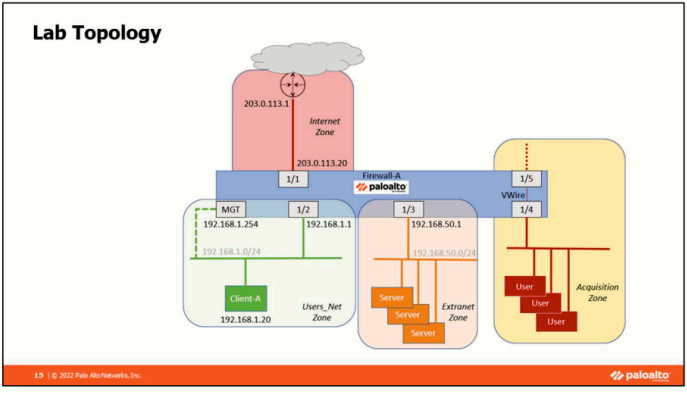
Palo Alto Networks offers students an opportunity to self-evaluate their post-class knowledge and skills in this free assessment in Beacon. Completion of this assessment is a useful way to self-evaluate what you learned from the course.

The post-class assessment exam should be attempted by all students who have completed the course. Post-class assessments are available for all instructor-led courses or their corresponding digital-learning course equivalents.

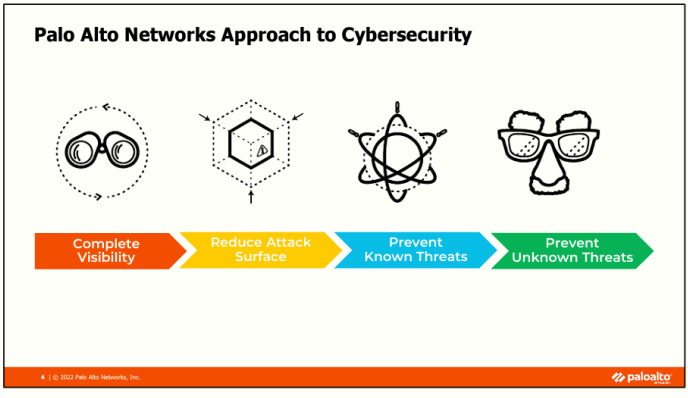
The assessment tests your knowledge of the features, functions, and tasks described in the course, and it serves as an objective indication of your comprehension of the course content.

The assessment is free, and you take it over the internet using a web browser. To access the assessment, first log in to Beacon at https://beacon.paloaltonetworks.com (for external students) and https://flexlearn.paloaltonetworks.com (for internal students). Then use your course number as the search word to find the link to launch your assessment.

The questions are true/false or multiple choice and consist of four to six questions per course module. It is an open-book assessment that also tests your ability to locate useful reference material.

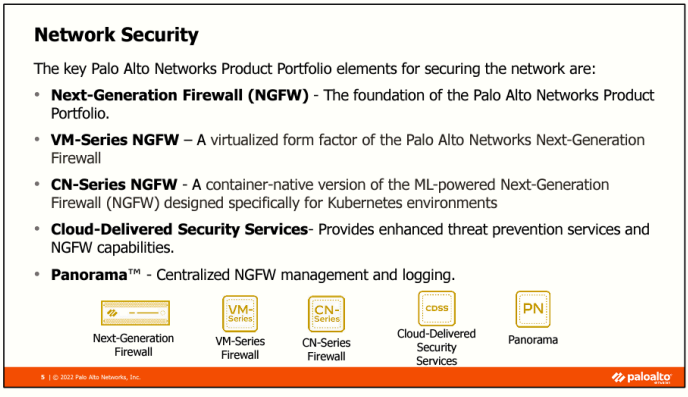


By the time you finish this course, you will have built this architecture. Your firewall will have four Security Zones and provide secure access to the Internet and to internal application servers from the lab client workstation.



The critical elements of the Palo Alto Networks approach to cybersecurity:

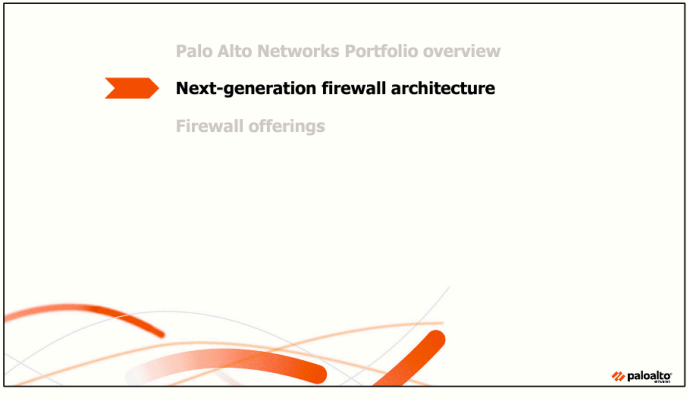
- **Provide visibility**: An organization cannot protect against what it cannot see. Visibility requires the complete visibility of users, applications, and content traversing corporate networks, the cloud, and endpoints. Only then is it possible to implement security policies and take actions, such as blocking unknown traffic, identifying advanced attacks, or permitting only applications with a valid business purpose.
- **Reduce the attack surface**: An attacker has more difficulty compromising an organization when the attack surface is reduced. A variety of actions and tactics are available to reduce the attack surface, including implementing an allowed application list to enable only critical business applications, inspecting unknown traffic and activity against acceptable use policies, and implementing multi-factor authentication to ensure that compromised credentials cannot be used to access applications and data.
- **Prevent known threats**: Preventing known threats is a foundational capability of any security program, but to do so effectively, your organization must be able to consume, and process threat intelligence and have a well-organized defense that can be reconfigured rapidly and automatically, based on new intelligence.
- **Prevent unknown threats**: Although vitally essential, signature-based prevention is limited to blocking only what it knows. Preventing unknown threats is a crucial capability consisting of making known threats, developing controls to stop them, and automatically reprogramming security technologies to incorporate the new rules. Palo Alto Networks technologies use data analytics and machine learning on collected datasets to detect behavioral anomalies indicative of a breach or attack and then provide detailed, actionable alerts. An organization can use automated processes and event correlation to make it easier to identify and address critical threats.



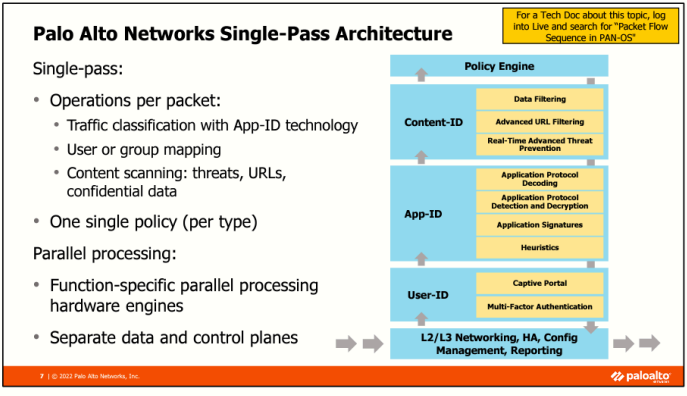
The networking infrastructure of an enterprise can be extraordinarily complex. The Product Portfolio secures the enterprise networks' perimeter, data center, and retail/branch offices with a fully integrated and automated platform that simplifies security. Simplifying your security posture enables you to reduce operational costs and support infrastructure while increasing your ability to prevent threats to your organization and quickly adjust to your dynamic environment. The key Product Portfolio elements for securing the network are:

- **Next-Generation Firewall (NGFW):** The Palo Alto Networks Product Portfolio foundation.
- **VM-Series NGFW** - Provides all the capabilities of the Palo Alto Networks Next-Generation hardware firewall in a virtual machine form factor
- **CN-Series NGFW** – A container-native version of the ML-powered Next-Generation Firewall (NGFW) designed explicitly for Kubernetes environments.
- **Cloud-Delivered Security Services:** Provides enhanced threat detection and prevention services and NGFW capabilities.
- **Panorama**: Centralized next-generation firewall management and logging.

For information about securing the enterprise, log into Live and search for "Product Selection" or see the documentation at https://www.paloaltonetworks.com/network-security.

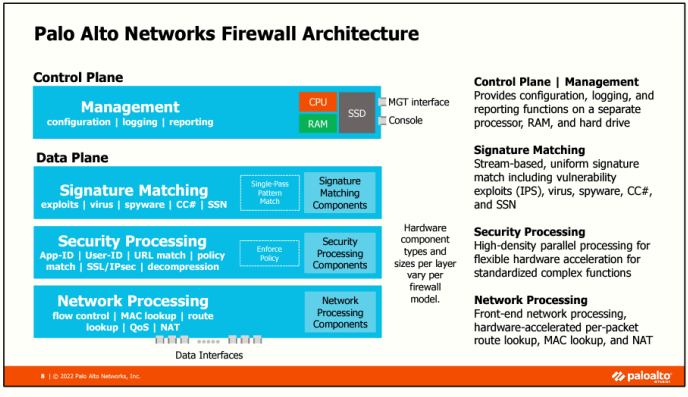


This section introduces architectural features of Palo Alto Networks firewalls.



The strength of the Palo Alto Networks firewall is its single-pass parallel processing (SP3) engine. The single-pass software performs operations once per packet. As a packet is processed, networking functions, policy lookup, application identification, decoding, and signature matching for any threats and content are performed just once. The parallel processing hardware is designed with separate data and control planes. The separation of the data and control planes means that heavy utilization of one plane will not negatively impact the other plane.

The advantage of providing the SP3 engine is that traffic is scanned with a minimal amount of buffering as it traverses the firewall. This speed lets you configure advanced features, such as scanning for viruses and malware, without slowing the firewall's performance.

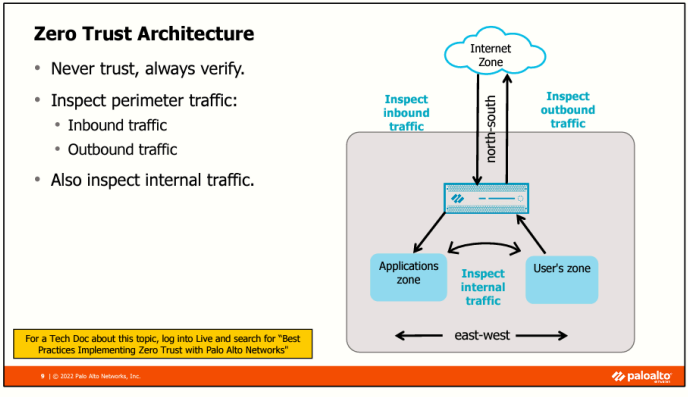


Palo Alto Networks has processors dedicated to specific security functions that work in parallel. These components can be implemented in hardware or software.

On the higher-end hardware models, the data plane contains three types of processors that are connected by high-speed 1Gbps buses:

- Signature Match Processor scans traffic and detects:
  - vulnerability exploits (intrusion protection system)
  - viruses
  - spyware
  - credit card numbers
  - Social Security numbers
- Security Processors: Multicore processors that handle security tasks such as Secure Sockets Layer decryption.
- Network Processor: Responsible for routing, network address translation, and network-layer communication.

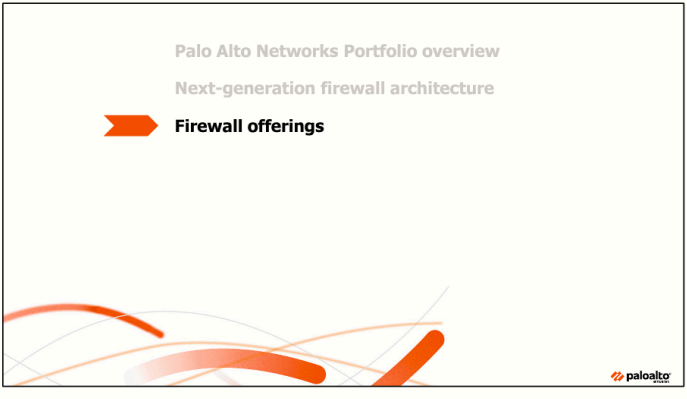
The control plane has its own dual-core processor, RAM, and hard drive on the higher-end hardware models. This processor is responsible for management UI, logging, and route updates.



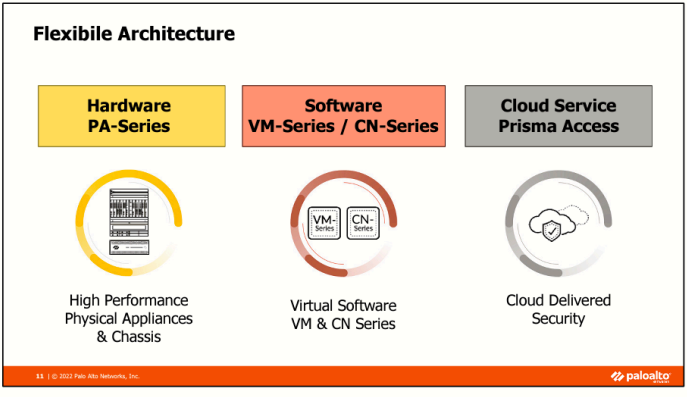
Conventional security models operate on the outdated assumption that everything inside an organization's network can be trusted. These models are designed to protect the perimeter. Meanwhile, threats that get inside the network go unnoticed and are left free to compromise sensitive, valuable business data. In the digital world, trust is nothing but a vulnerability.

The Zero Trust architecture model remedies the deficiencies of the perimeter-only architecture. Zero Trust is based on the principle "never trust, always verify" rather than on principle "trust but verify." In Zero Trust, each step a user makes through the infrastructure must be validated and authenticated across all locations.

In complex network architectures, you can simplify traffic flows to inbound traffic from the internet, outbound traffic to the internet, and internal traffic between nodes in your data center. You accomplish inbound and outbound inspection by locating a firewall between your internal network segments and the internet. You achieve an internal traffic inspection by locating a firewall between your internal subnets and VLANs.

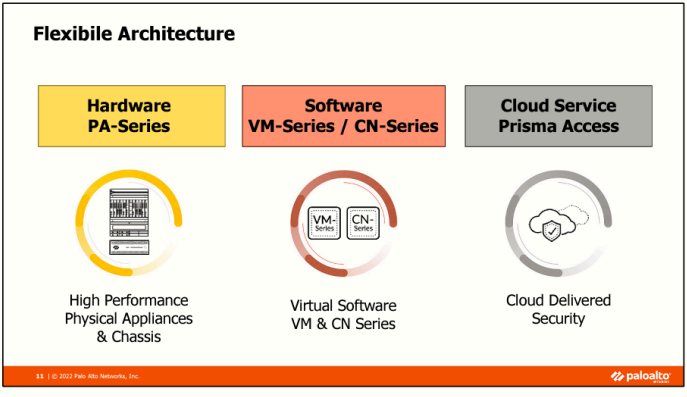


This section introduces the physical and virtual firewall models available from Palo Alto Networks. For the latest information about available Palo Alto Networks firewall models, log into Live and search for “Product Selection” or see https://www.paloaltonetworks.com/products/product-selection.html.



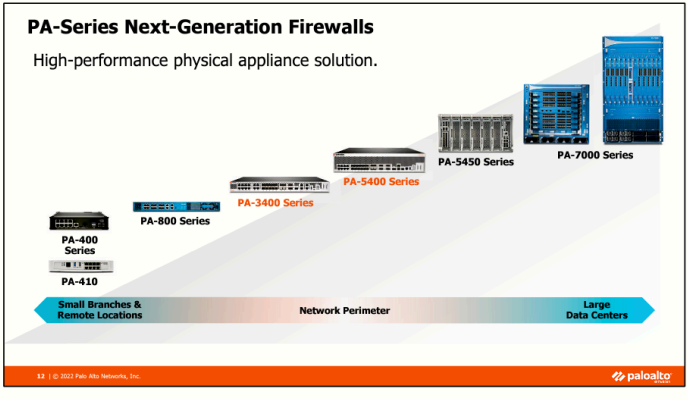
The foundation of the Strata Network Security Platform is the ML-Powered Next-Generation Firewall. Strata is designed to not only protect the perimeter of your network (north-south traffic), regardless of where that perimeter may be, but also traffic that moves internally (east-west) within your network. The flexibility of the Strata platform currently has 3 form factors of the firewall that can be used independently or combined for different uses cases to match your requirements by location, and you can manage all deployments centrally through Panorama network security management.

The PA-Series is a physical appliance that provides a blend of power, intelligence, simplicity, and versatility. The PA-Series protects enterprise and service provider deployments at headquarters, data centers, and branch offices. The VM- and CN-Series are Virtual Next-Generation Firewalls that protect your hybrid cloud and branch deployments by segmenting applications and preventing threats. And Prisma™ Access is a secure access service edge (SASE) offering that delivers security globally from the cloud.



The foundation of the Strata Network Security Platform is the ML-Powered Next-Generation Firewall. Strata is designed to not only protect the perimeter of your network (north-south traffic), regardless of where that perimeter may be, but also traffic that moves internally (east-west) within your network. The flexibility of the Strata platform currently has 3 form factors of the firewall that can be used independently or combined for different uses cases to match your requirements by location, and you can manage all deployments centrally through Panorama network security management.

The PA-Series is a physical appliance that provides a blend of power, intelligence, simplicity, and versatility. The PA-Series protects enterprise and service provider deployments at headquarters, data centers, and branch offices. The VM- and CN-Series are Virtual Next-Generation Firewalls that protect your hybrid cloud and branch deployments by segmenting applications and preventing threats. And Prisma™ Access is a secure access service edge (SASE) offering that delivers security globally from the cloud.



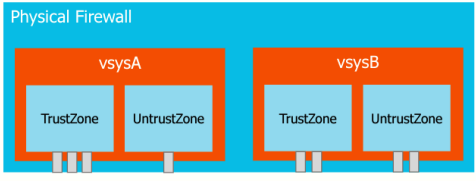
The PA-Series firewall is a high-performance physical appliance solution. The PA-Series is available in different sizes, from a desktop-size form factor for your small offices to large chassis form factors for your datacenters. The operating system is consistent across all hardware platforms, so the look and feel of the web-based management interface are the same.

The PA-7000 Series provides power, intelligence, and versatility for enterprise and service provider deployments. The PA-5450 series offers a versatile platform built for Hyper-Scale Data Centers, Internet Edge deployments, and Campus segmentation deployments. With the release of PAN-OS 10.2, two new PA-Series firewalls were introduced. The PA-5400 series provides no-compromise security and high performance for data centers and service providers, and the PA-3400 series provides broad threat coverage at the internet edge. The PA-800 Series provides security for branch offices and mid-sized businesses. The PA-400 series is optimized to meet your distributed enterprise branch requirements, while the PA-220 delivers visibility, control, and the power to prevent network threats in a small form factor. The PA-220R provides network security in a ruggedized form factor for severe environments.

To compare the capabilities of the various firewall models, log into Live and search for “Product Selection” or see https://www.paloaltonetworks.com/products/product-selection.html.

Virtual Systems

- Separate, logical firewalls within a single physical firewall
- Creates an administrative boundary
- Use case: multiple customers or departments



13 | © 2022 Palo Alto Networks, Inc.

A virtual system (vsys) is a separate, logical firewall instance within a single physical Palo Alto Networks firewall. Managed service providers and enterprises can use a single pair of firewalls (for high availability) and enable virtual systems on them, rather than use multiple firewalls. Each virtual system is an independent, separately managed firewall with its traffic kept separate from the traffic of other virtual systems.

A vsys consists of physical and logical interfaces and subinterfaces, virtual routers, and security zones. You choose the deployment modes, consisting of any combination of virtual wire, Layer 2, and Layer 3 interfaces on each virtual system. When you use virtual systems, you can segment any of the following:

- administrative access
- management of all policies (Security, NAT, QoS, Policy-Based Forwarding, Decryption, Application Override, Authentication, and DoS Protection)
- all objects (such as address objects, application groups, filters, external dynamic lists, Security Profiles, Decryption Profiles, and Custom objects)
- User-ID
- certificate management
- Server Profiles
- logging, reporting, and visibility functions

Virtual systems are supported on the PA-3x00, PA-5x00, and PA-7x00 Series firewalls. Each firewall series supports a base number of virtual systems; the number varies by platform. A Virtual Systems license is required to support multiple virtual systems on the PA-3x00 Series firewalls and create more than the base number of virtual systems supported on a platform.

For more information about Virtual Systems, log into Live and search for “Virtual Systems” or see https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems.html.

VM-Series Models and Capacities

Example Performance and Capacities	VM-50/ Lite	VM-100	VM-300	VM-500	VM-700
Firewall throughput (App-ID enabled)	**200Mbps**	**2Gbps**	**4Gbps**	**8Gbps**	**16Gbps**
Advanced Threat prevention throughput	**100Mbps**	**1Gbps**	**2Gbps**	**4Gbps**	**8Gbps**
New sessions per second	3,000	15,000	30,000	60,000	120,000
Dedicated CPU cores	2	2	2, 4	2, 4, 8	2, 4, 8, 16
Dedicated memory (minimum)	5.5GB/4.5GB	6.5GB	9GB	16GB	56GB
Dedicated disk drive capacity (minimum)	32GB	60GB	60GB	60GB	60GB

The VM-Series virtual firewalls provide all the capabilities of the Palo Alto Networks next-generation hardware firewall in a virtual machine form factor, so you can secure the environments that are vital to your organization. The VM-Series firewall can be deployed either on-premises or in a public cloud. For public cloud deployment, the VM-Series firewall can be deployed on either Alibaba Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, or Oracle Cloud to protect your cloud perimeter and your east-west traffic. More and more organizations are quickly adopting multi-cloud architectures to distribute risk and take advantage of the core competencies of different cloud vendors.

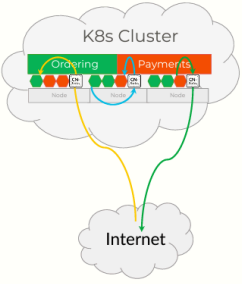
To ensure your applications and data are protected across public clouds and virtualized data centers, the VM-Series has been designed to deliver up to 16 Gbps of App-ID-enabled firewall performance across five models:

- VM-50/VM-50 Lite models are engineered to consume minimal resources and support CPU oversubscription yet deliver up to 200 Mbps of App-ID-enabled firewall performance for scenarios from virtual branch office/customer-premises equipment to high-density, multi-tenant environments.
- VM-100 and VM-300 models are optimized to deliver 2 Gbps and 4 Gbps of App-ID-enabled performance, respectively, for hybrid cloud, segmentation, and internet gateway use cases.
- VM-500 and VM-700 models can deliver 8 Gbps and 16 Gbps of App-ID-enabled firewall performance, respectively. They can be deployed as Network Functions Virtualization (NFV) security components in fully virtualized data center and service provider environments.

For more information about the VM-Series Firewall, log into Live and search for “VM-Series” or see https://www.paloaltonetworks.com/prisma/vm-series.

CN-Series Firewall

- CN-Series provides visibility and security to containerized application workloads.
- Natively integrates into Kubernetes clusters.
- Delivers the same capabilities as the PA-Series and VM-Series firewalls.
- Provides Layer 7 visibility, application-level segmentation, DNS security, and advanced threat protection.
- Protects traffic across trusted zones in public cloud or data center environments.



The Container Native or CN-Series firewalls deliver the same capabilities as the PA-Series and VM-Series firewalls, but in a container form factor. You can deploy the same cloud-delivered security services on top of the CN-Series firewalls, just like you would other firewall form factors. The CN-Series firewall natively integrates into Kubernetes to provide complete Layer 7 visibility, application-level segmentation, DNS security, and advanced threat protection for traffic going across trusted zones in public cloud and data center environments.

The CN-Series firewall provides containerized traffic visibility. For instance, the CN-Series firewall identifies the specific pod traffic that originates from, unlike a firewall deployed at the edge. This means that you can write more granular security policies defined at the application level rather than at the cluster level. Management of the CN-Series firewall is done through Panorama using the Kubernetes plugin. The Kubernetes plugin continuously pulls information from Kubernetes and feeds that information into Panorama.

For more information about the CN-Series Firewall, log into Live and search for “CN-Series” or see https://www.paloaltonetworks.com/network-security/cn-series.

Module Summary

Now that you have completed this module, you should be able to:

- Describe the three Pillars of the Palo Alto Networks Portfolio
- Define the single-pass architecture
- Define Zero Trust Concept
- Describe the physical and virtual firewall models available from Palo Alto Networks

Now that you have completed the module, you should be able to perform the tasks listed.

Review Questions

1. Which two planes are found in the Palo Alto Networks single-pass platform architecture? (Choose two.)
   a. control
   b. application
   c. data
   d. parallel processing
2. Which object cannot be segmented using virtual systems on a firewall?
   a. network security zone
   b. data plane interface
   c. administrative access
   d. MGT interface
3. Which series of firewalls is a high-performance physical appliance solution?
   a. CN
   b. PA
   c. VM
4. Which Strata product provides centralized firewall management and logging?
   a. WildFire
   b. Panorama
   c. GlobalProtect
   d. Prisma Access
5. True or false? The CN-Series firewalls deliver the same capabilities as the PA-Series and VM-Series firewalls.
   a. true
   b. False

Lab 1 Overview

- There is no lab for this module

Answers to Review Questions

1. a, c
2. d
3. b
4. b
5. a (true)