PALO ALTO NETWORKS PCNSE STUDY GUIDE: EARLY ACCESS

Based on PAN-OS® 9.0
May 2019

©2016-2019, Palo Alto Networks, Inc.

Palo Alto Networks, Inc. www.paloaltonetworks.com
©2016-2019 Palo Alto Networks – all rights reserved. Aperture, AutoFocus, Demisto, GlobalProtect, Palo Alto Networks, PAN-OS, Panorama, RedLock, Traps, and WildFire are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners.

Contents

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

©2016-2019, Palo Alto Networks, Inc.

Palo Alto Networks PCNSE Study Guide

Welcome to the *Palo Alto Networks PCNSE Study Guide*. The purpose of this guide is to help you prepare for your PCNSE exam and achieve your PCNSE credential. This study guide is a summary of the key topic areas that you are expected to know to be successful at the PCNSE exam. It is organized based on the exam blueprint and key exam objectives.

Overview

The Palo Alto Networks Certified Network Security Engineer (PCNSE) is a formal, third-party proctored certification that indicates that those who have passed it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most implementations based on the Palo Alto Networks platform.

This exam will certify that the successful candidate has the knowledge and skills necessary to implement the Palo Alto Networks next-generation firewall PAN-OS® 9.0 platform in any environment.
More information is available from Palo Alto Networks at:
https://www.paloaltonetworks.com/services/education/pcnse

Exam Details

- Certification Name: Palo Alto Networks Certified Network Security Engineer
- Delivered through Pearson VUE: www.pearsonvue.com/paloaltonetworks
- Exam Series: PCNSE
- Seat Time: **80** minutes
- Number of items: **75**
- Format: Multiple Choice, Scenarios with Graphics, and Matching
- Languages: English and Japanese

Intended Audience

The PCNSE exam should be taken by anyone who wants to demonstrate a deep understanding of Palo Alto Networks technologies, including customers who use Palo Alto Networks products, value-added resellers, pre-sales system engineers, system integrators, and support staff.

Qualifications

Candidate should have three to five years' experience working in the Networking or Security industries and the equivalent of 6 to 12 months' experience deploying and configuring Palo Alto Networks NGFW within Palo Alto Networks Security Operating Platform.

©2016-2019, Palo Alto Networks, Inc.

Skills Required

- You can plan, deploy, configure, operate, and troubleshoot Palo Alto Networks Security Operating Platform components.
- You have product expertise and understand the unique aspects of the Palo Alto Networks Security Operating Platform and how to deploy one appropriately.
- You understand networking and security policies used by PAN-OS software.

Recommended Training

Palo Alto Networks strongly recommends that you attend the following instructor-led training courses or equivalent virtual digital learning courses:

- Firewall Essentials: Configuration and Management (EDU-210) or digital learning (EDU-110)
- Panorama: Managing Firewalls at Scale (EDU-220) or digital learning (EDU-120)
- Optional Training: Firewall: Optimizing Firewall Threat Prevention (EDU-214) or digital learning (EDU-114)
- Optional training: Firewall: Troubleshooting (EDU-330)

After you have completed the courses, practice on the platform to master the basics. Use the following resources to prepare for the exam. All resources can be found here: https://www.paloaltonetworks.com/services/education/pcnse

- Cybersecurity Skills Practice Lab
- PCNSE Study Guide and Practice Exam
- Administrator's Guide: specific configuration information and "best practice" settings
- Preparation videos and tutorials

About This Document

Efforts have been made to introduce all relevant information that might be found in a PCNSE Certification Test. However, other related topics also may appear on any delivery of the exam. This document should not be considered a definitive test preparation guide but an introduction to the knowledge required, and these guidelines may change at any time without notice. This document contains many references to outside information that should be considered essential to completing your understanding.

Disclaimer

This study guide is intended to provide information about the objectives covered by this exam, related resources, and recommended courses. The material contained within this study guide is not intended to guarantee that a passing score will be achieved on the exam. Palo Alto Networks recommends that a candidate thoroughly understand the objectives indicated in this guide and use the resources and courses recommended in this guide where needed to gain that understanding.

©2016-2019, Palo Alto Networks, Inc.

Preliminary Score Report

The score report notifies candidates that, regardless of pass or fail results, an exam score may be revised any time after testing if there is evidence of misconduct, scoring inaccuracies, or aberrant response patterns.

Palo Alto Networks Certified Network Security Engineer - PCNSE Based on PAN-OS Version 9.0	
Domain	Weight (%)
Plan	16%
Deploy and Configure	23%
Operate	20%
Configuration Troubleshooting	18%
Core Concepts	23%
Total	100%

©2016-2019, Palo Alto Networks, Inc.

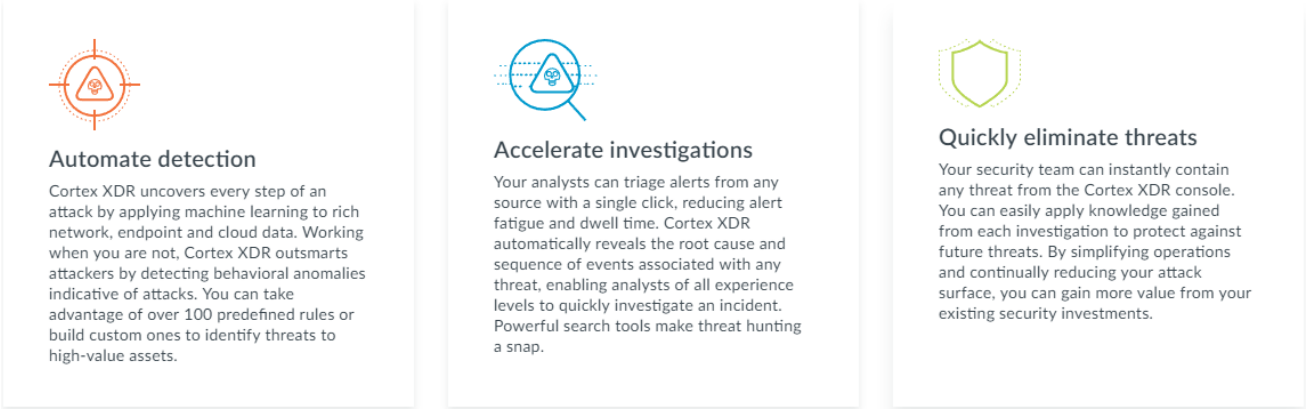
Exam Domain 1 – Plan

1.1 Identify how the Palo Alto Networks products work together to detect and prevent threats

Stop Sophisticated Attacks Across Your Network, Endpoint, and Cloud Assets

Tools in silos, such as endpoint detection and response (EDR) and network traffic analysis (NTA), force your analysts to manually piece together information, which slows investigations and increases complexity. The Cortex XDR cloud-based detection and response app removes security blind spots by stitching together network, endpoint, and cloud data.

Detect, Investigate, and Respond at Lightning Speed



Automate detection

Cortex XDR uncovers every step of an attack by applying machine learning to rich network, endpoint and cloud data. Working when you are not, Cortex XDR outsmarts attackers by detecting behavioral anomalies indicative of attacks. You can take advantage of over 100 predefined rules or build custom ones to identify threats to high-value assets.

Accelerate investigations

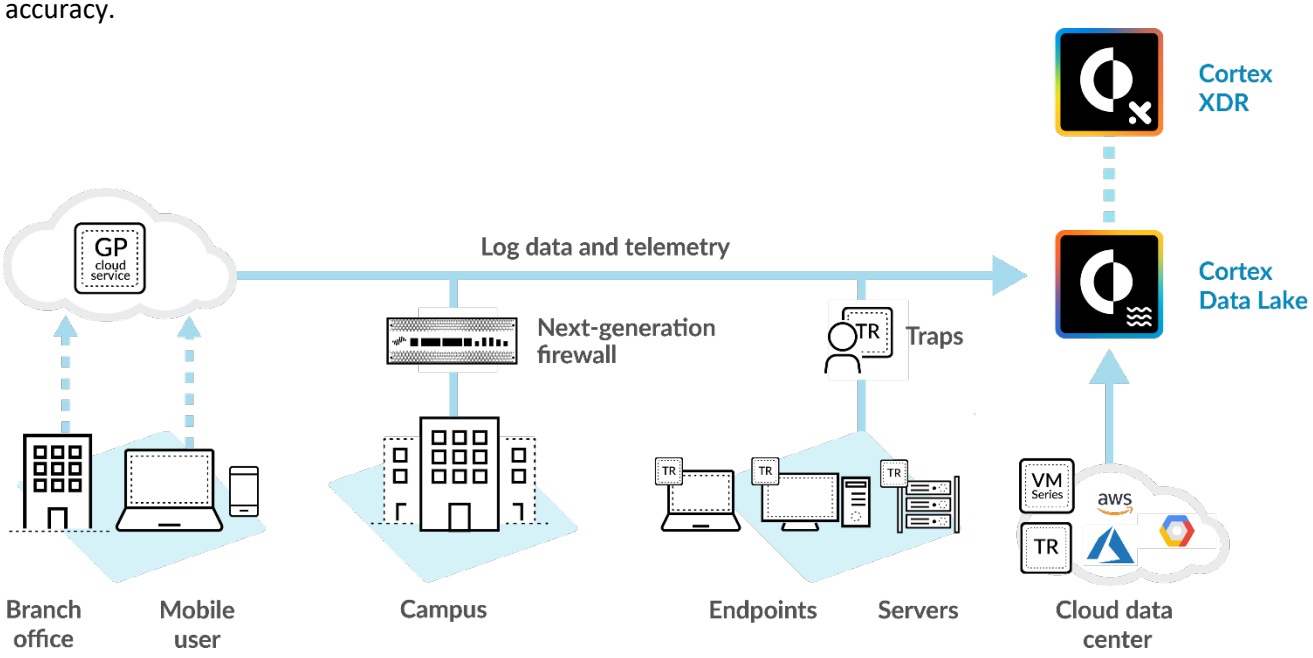
Your analysts can triage alerts from any source with a single click, reducing alert fatigue and dwell time. Cortex XDR automatically reveals the root cause and sequence of events associated with any threat, enabling analysts of all experience levels to quickly investigate an incident. Powerful search tools make threat hunting a snap.

Quickly eliminate threats

Your security team can instantly contain any threat from the Cortex XDR console. You can easily apply knowledge gained from each investigation to protect against future threats. By simplifying operations and continually reducing your attack surface, you can gain more value from your existing security investments.

Cortex and Cortex XDR

Cortex is the industry's only open and integrated AI-based continuous security platform. It delivers radical simplicity and significantly improves security outcomes through automation and unprecedented accuracy.



©2016-2019, Palo Alto Networks, Inc.

Overview

Cortex can integrate Palo Alto Networks products into a cohesive threat detection and response system. Products can run alone or in conjunction with others providing world-class security solutions. They can be unified with the Cortex subscription that aggregates their data for a holistic and comprehensive enterprise solution.

Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure. If your data is unified, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is augmented with data from Palo Alto Networks WildFire®, AutoFocus/MineMeld, and Unit 42 information sources.

Cortex XDR is a set of tools that works with Cortex Data Lake to identify threats manually. With AI, it determines root causes of security events and responds to threats by deploying response settings to enforcement products.

Palo Alto Networks products are organized into two areas of focus that are described in the following sections.

Securing the Enterprise

Grounded in the next-generation firewall and the services that enable it.

Next-generation firewalls: Next-generation firewalls secure your enterprise with a prevention-focused architecture and integrated innovations that are easy to deploy and use. Palo Alto Networks next-generation firewalls detect known and unknown threats, including those within encrypted traffic, using intelligence generated across many thousands of customer deployments. The firewalls reduce risks and prevent a broad range of attacks. For example, they enable users to access data and applications based on business requirements and they stop credential theft and an attacker's ability to use stolen credentials

DNS Security: DNS security service applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight integration with the next-generation firewall gives you automated protections and eliminates the need for independent tools. DNS Security service makes malicious domain information available to your NGFW collected from WildFire, Unit 42, URL filtering, and the Cyber Threat Alliance.

WildFire®: WildFire automatically prevents zero-day exploits and malware. Traditional malware analysis and sandboxing techniques are not adequate and cannot keep pace with new exploits. WildFire uses shared community-sourced threat data and advanced analysis, and immediately shares protections across the network, endpoint, and cloud. WildFire automatically delivers protections about every 5 minutes (by accessing a database that is updated every 5 minutes), thus preventing successful cyberattacks.

AutoFocus: AutoFocus contextual threat intelligence brings speed, consistency, and precision to threat investigation. It provides instant access to community-based threat data, enhanced with deep context and attribution from the Unit 42 threat research team, thus saving time and effort. Now your teams can quickly investigate, correlate, and pinpoint malware's root cause without adding dedicated malware

©2016-2019, Palo Alto Networks, Inc.

researchers or additional tools. Plus, automated protections make raw intelligence simple to turn into protection across your environment.

Traps: Traps advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. Traps is the only solution that pre-emptively blocks security breaches such as ransomware attacks. It uses a unique multi-method approach that prevents known and unknown malware, exploits, and zero-day threats.

Threat Prevention: Threat Prevention capitalizes on the next-generation firewall's capability to inspect all traffic, and can prevent known threats, regardless of port, protocol, or SSL encryption. Threat Prevention automatically stops vulnerability exploits with IPS capabilities, offers inline malware protection, and blocks outbound command-and control-traffic. When combined with WildFire and URL filtering, organizations are protected at every stage of the attack lifecycle, including both known and zero-day threats. This service is consumed by other products and integrated into others.

Panorama: An enterprise-level firewall management solution that simplifies, streamlines, and consolidates core tasks and capabilities, thus enabling you to use a single console to view all your firewall traffic, manage all aspects of device configuration, push global policies, and generate reports on traffic patterns or security incidents, all at enterprise scale.

MineMeld: MineMeld is an open-source application that streamlines the aggregation, enforcement, and sharing of threat intelligence. MineMeld is available for all users directly on GitHub and pre-built virtual machines (VMs) for easy deployment. Anyone using the proper software can add to the MineMeld functionality by contributing code to the open-source repository. MineMeld integrates information from disparate sources, normalizes it for consumption, and can automate settings on managed products.

Expedition: Expedition is a free, virtual appliance that helps convert firewall configurations from leading vendors to Palo Alto Networks next-generation firewalls.
The second area of focus is securing the cloud.

Securing the Cloud

VM-Series next-generation firewalls: Palo Alto Networks virtualized next-generation firewalls protect your private and public cloud deployments by segmenting applications and preventing threats. Available for many public and private cloud technologies and provide the same world-class level of detection and prevention of your physical next-generation firewalls.

Aperture: The use of software as a service (SaaS) applications is creating new risks and gaps in security visibility for malware propagation, data leakage, and regulatory non-compliance. Aperture provides complete visibility and granular enforcement across all user, folder, and file activity within sanctioned SaaS applications, thus providing detailed analysis and analytics about usage without requiring any additional hardware, software, or network changes.

GlobalProtect cloud service: GlobalProtect cloud service provides the full security capabilities of the Palo Alto Networks next-generation firewall *delivered as a service*. You can protect users across your organization and prevent successful cyberattacks with scale and simplicity, and without compromise.

©2016-2019, Palo Alto Networks, Inc.

GlobalProtect cloud service automates the orchestration and rollout of security services, thus reducing deployment time. You can deploy new features, increase coverage, and scale globally with cloud infrastructure, which gives you a new level of flexibility.

RedLock: The RedLock public cloud security and compliance service uses machine learning to understand the role and behavior of each cloud resource and enriches visibility by correlating data from external sources such as vulnerability scanners, threat intelligence tools, and SIEMS. Information provided by RedLock provide security personnel with unmatched insight into the threats detected in their environment.

Cortex Data Lake: The cloud-delivered Logging Service allows you to easily collect large volumes of log data, so innovative apps can gain insight from your environment. You can simplify your log infrastructure, automate log management, and use the insights gained from your data to prevent attacks more effectively. This service is used to populate the Cortex Data Lake.

Magnifier: Magnifier behavioral analytics applies machine learning at a cloud scale to network, endpoint, and cloud data so that you can quickly find and stop targeted attacks, insider abuse, and compromised endpoints. Magnifier uncovers the actions attackers cannot conceal, by profiling user and device behavior and identifying anomalies that indicate active attacks. Magnifier integrates rich metadata collected from the Security Operating Platform with attack detection algorithms and enables you to detect post-intrusion activity with precision.

Sample Questions

1. Which component of the integrated Palo Alto Networks security solution limits network-attached workstation access to a corporate mainframe?
   A. threat intelligence cloud
   B. advanced endpoint protection
   C. next-generation firewall
   D. tunnel inspection
2. Which Palo Alto Networks product is designed primarily to provide threat context with deeper information about attacks?
   A. RedLock
   B. WildFire
   C. AutoFocus
   D. Threat Prevention
3. Which Palo Alto Networks product is designed primarily to provide normalization of threat intelligence feeds with the potential for automated response?
   A. MineMeld
   B. WildFire
   C. AutoFocus
   D. Threat Prevention

©2016-2019, Palo Alto Networks, Inc.

4. Which Palo Alto Networks product is designed primarily to protect endpoints from successful cyberattacks?
   A. GlobalProtect
   B. Magnifier
   C. Traps
   D. RedLock
5. The Palo Alto Networks Cortex Data Lake can accept logging data from which products? (Choose two.)
   A. Traps
   B. next-generation firewalls
   C. Aperture
   D. MineMeld
   E. AutoFocus
6. Which Palo Alto Networks product is required to deliver your product log data to a central cloud base storage service managed by Palo Alto Networks?
   A. RedLock
   B. Traps
   C. next-generation firewall
   D. Cortex Data Lake
7. Which product is an example of an application designed to analyze Cortex Data Lake information?
   A. Cortex XDR - Analytics
   B. RedLock
   C. Cortex XDR – Automated Response
   D. AutoFocus

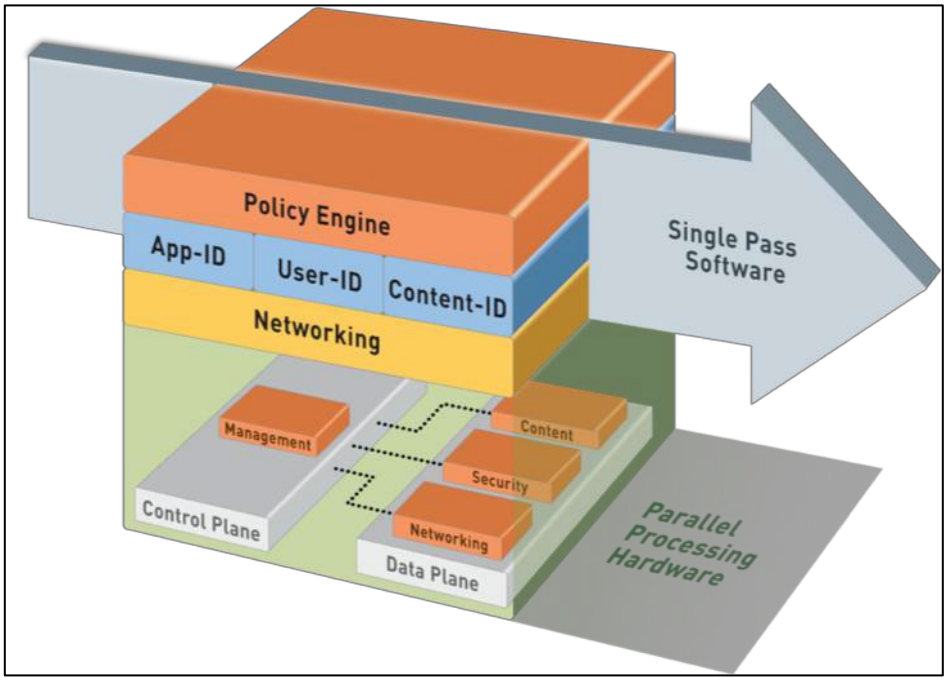
©2016-2019, Palo Alto Networks, Inc.

1.2 Given a scenario, identify how to design an implementation of the firewall to meet business requirements that leverage the Palo Alto Networks Security Operating Platform

Choosing the Appropriate Firewall

Feature and performance requirements impact the choice of firewall model. All Palo Alto Networks firewalls run the same version of PAN-OS® software, ensuring the same primary feature set. When you investigate which model fits a given need, evaluate throughput, maximum concurrent sessions, and connections per second with App-ID, threat prevention, and decryption features enabled. Note that there are two published throughput statistics: "firewall throughput" and "threat prevention throughput." "Threat prevention throughput" is the expected throughput with most of the defensive options (App-ID, User-ID, IPS, antivirus, and anti-spyware) enabled, and "firewall throughput" is the throughput with no Content-ID defense options enabled. Additional services might be available as integrated products or service licenses that enrich logging data analysis. Overall, choosing a firewall is as much a selection of functions and services that drive proper sizing decisions to meet your needs.

A few features, such as the Decryption Broker, are supported only on firewalls that have larger compute resources." The way it is currently written sounds odd. The following link provides a features summary of all firewall models, including throughput:
https://www.paloaltonetworks.com/resources/datasheets/product-summary-specsheet



The Palo Alto Networks firewall was designed to use an efficient system referred to as next-generation processing. Next-Generation Processing enables packet evaluation, application identification, policy decisions, and content scanning in a single efficient processing pass.

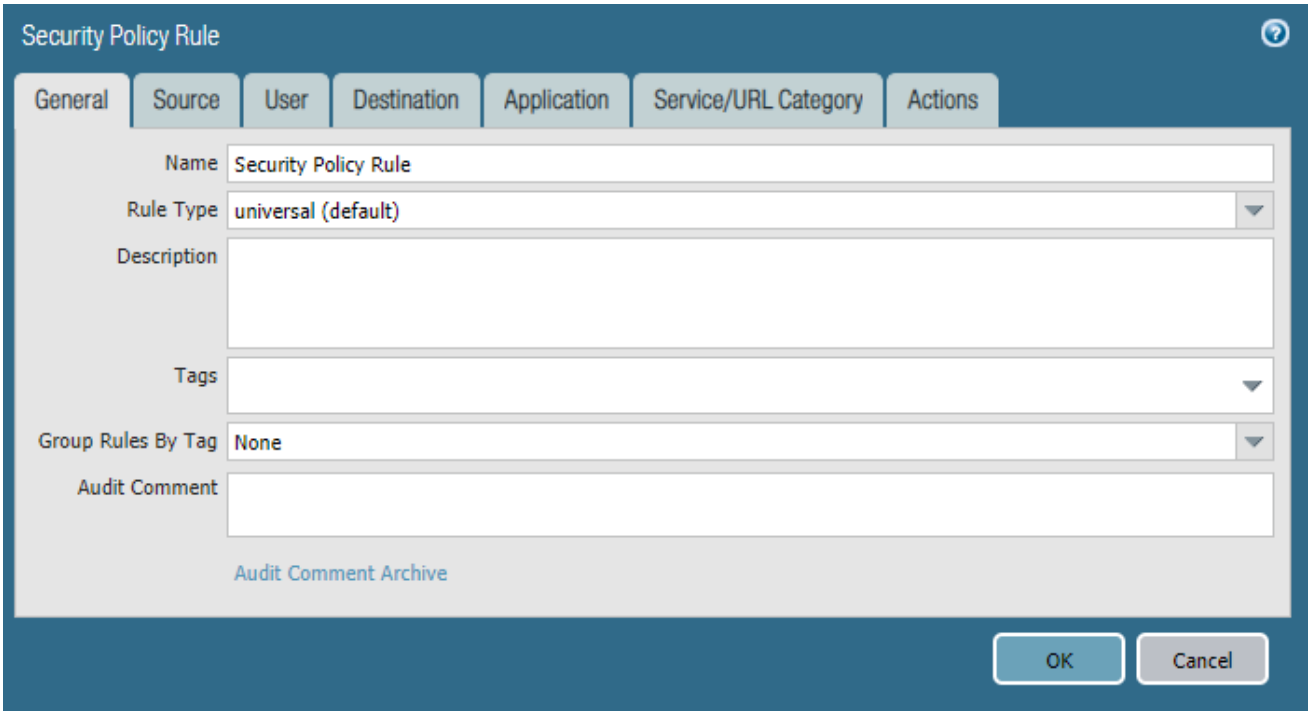
©2016-2019, Palo Alto Networks, Inc.

Palo Alto Networks firewalls contain the following primary next-generation features:

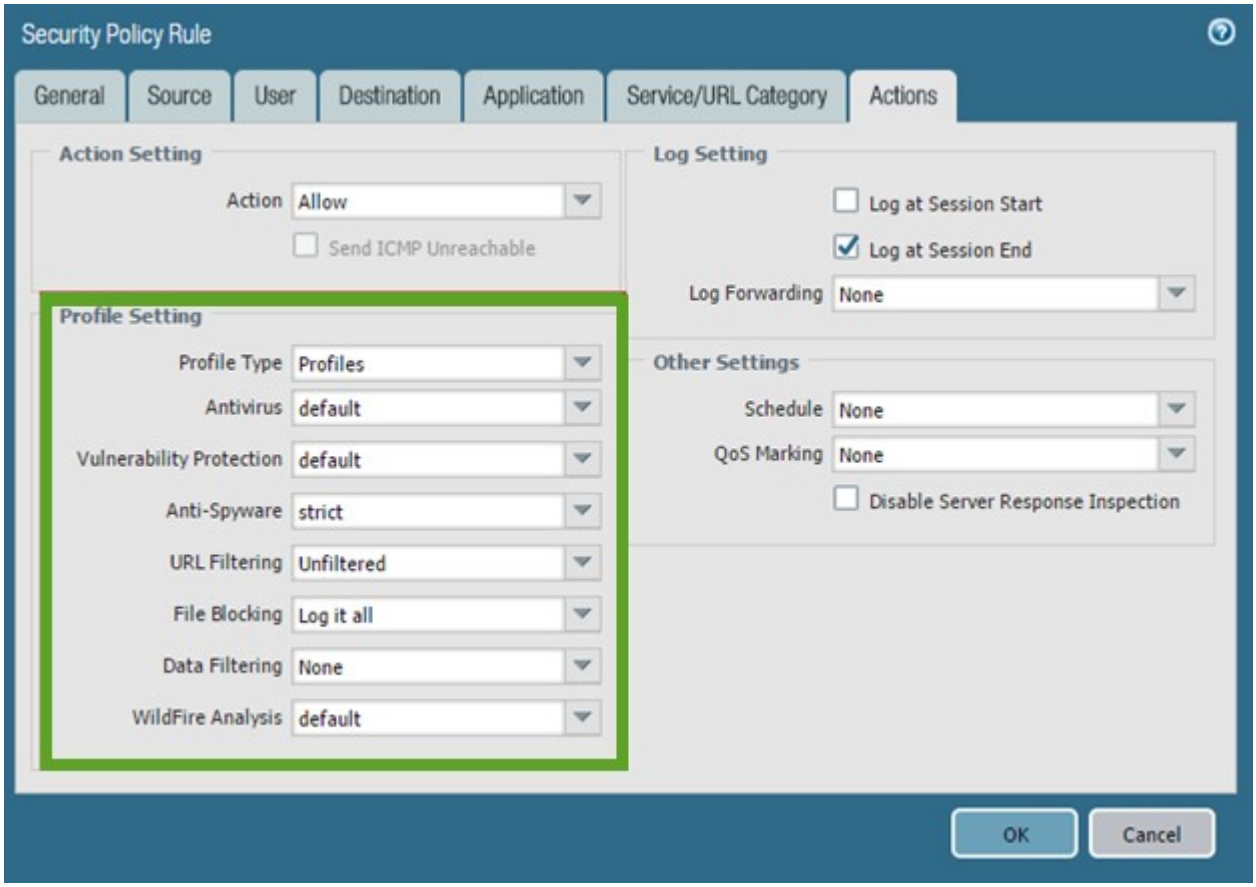
- App-ID: Scanning of traffic to identify the application that is involved, regardless of the protocol or port number used
- Content-ID: Scanning of traffic for security threats (e.g., data leak prevention and URL filtering, virus, spyware, unwanted file transfers, specific data patterns, vulnerability attacks, and appropriate browsing access
- User-ID: Matching of a user to an IP address (or multiple IP addresses), allowing your Security policy to be based on who is behind the traffic, not the device

Security Policy

The Security policy consists of security rules that are the basis of the firewall's ability to enable or block sessions. Multiple match conditions can be used when you create these rules. Security zones, source and destination IP address, application (App-ID), source user (User-ID), service (port), HIP match, and URL categories in the case of web traffic all can serve as traffic matching criteria for decisions to allow or block. App-ID ensures the positive identification of applications regardless of their attempts at evasiveness. Allowed session traffic can be scanned further based on Security Profiles (Content-ID) to identify unwanted traffic content. These profiles use signatures to identify known threats. Unknown threats are identified by WildFire, which creates signatures to turn them into known threats.
Examples of creating a policy rule security rules and profile settings follow:



©2016-2019, Palo Alto Networks, Inc.



Security Zones

Palo Alto Networks firewalls are zone-based. Zones designate a network segment that has similar security classification (i.e., Users, Data Center, DMZ Servers, and Remote Users). The firewall security model is focused on evaluating traffic as it passes from one zone to another. These zones act as a logical way to group physical and virtual interfaces. Zones are required to control and log the traffic that traverses the interfaces. All defined interfaces should be assigned a zone that marks all traffic coming to or from the interface. Zones are defined for specific interface types (TAP, Virtual Wire, Layer 2, or Layer 3) and can be assigned to multiple interfaces of the same type only. An interface can be assigned only to one zone.

All sessions on the firewall are defined by the source and destination zones. Rules can use these defined zones to allow or deny traffic, apply QoS, or perform NAT. All traffic can flow freely within a zone and is referred to as *intrazone* traffic. Traffic between zones (called *interzone* traffic) is denied by default. Security policy rules are required to modify these default behaviors. Traffic will be allowed to travel only between zones if a security rule is defined and the rule matches all conditions of the session. For interzone traffic, Security policy rules must reference a source zone and destination zone (not interfaces) to allow or deny traffic.

Security policies are used to create a positive (whitelist) and/or negative (blacklist) enforcement model for traffic flowing through the firewall. These rules are enumerated from the top down, and the first rules with the appropriate matching conditions will allow or deny the matching traffic. If the logging is enabled on the matching rule, and the traffic crosses a zone, the action for that session is logged. These logs are extremely useful for adjusting the positive/negative enforcement model. The log information

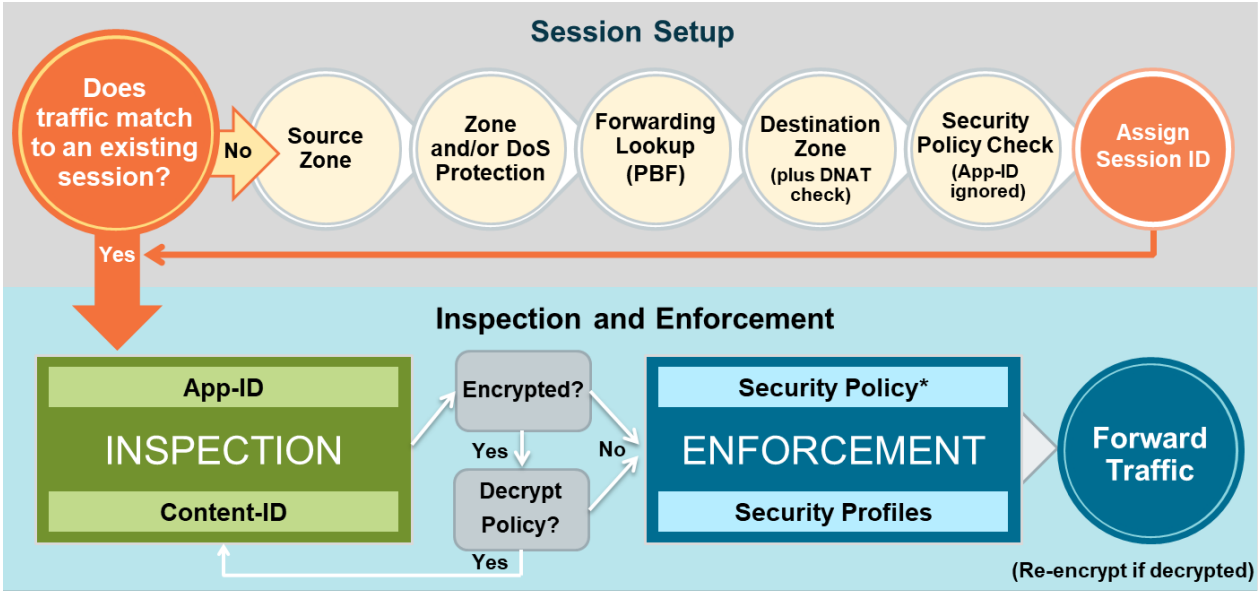
©2016-2019, Palo Alto Networks, Inc.

can be used to characterize traffic, thus providing specific use information and allowing precise policy creation and control. Log entries can be forwarded to external monitoring devices such as Panorama, the Cortex Data Lake, and/or a syslog server. Palo Alto Networks firewall logs, Application Command Center, App Scope, and other reporting tools all work to precisely describe traffic and use patterns.

Traffic Processing Sequence

Use the following graphical representation to visualize the Palo Alto Networks firewall processes. Your understanding of the linear version of the traffic flow can be useful when you create the initial configuration and when you adjust the rules after installation. Note that the graphical representation is a simplified version of the complete flow documented in the following article. Advanced analysis and discussion of the flow logic of the firewall is included in the *Firewall: Troubleshooting* (EDU-330) training class.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0



* Policy check relies on pre-NAT IP addresses

Enterprise Firewall Management

Palo Alto Networks next-generation firewalls are managed individually and have no native ability to be managed collectively from a single interface at an enterprise level. Panorama is the Palo Alto Networks enterprise management solution. Panorama can be scaled for the largest deployments when it is deployed in a "manager of managers" approach using the Panorama Interconnect plugin whereby Panorama is deployed to manage downstream Panoramas which, in turn, manage populations of firewalls.

©2016-2019, Palo Alto Networks, Inc.

Additional information about best practices in designing and deploying your Security policy when deploying a firewall as an edge device can be found here:
https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices.html
Other deployment best practices can be found here:
https://docs.paloaltonetworks.com/best-practices

Virtual Firewalls in Clouds

Palo Alto Networks products include the VM-Series virtual firewalls for implementation in both private and public cloud architectures. They run the same version of PAN-OS and support the same core features as do firewall appliances. Some features might not be supported or are implemented using alternate techniques, depending on the capabilities of the hosting environment. For example, most public cloud vendors support only Layer-3 types of interfaces for connection to their virtual networks. Another example is the varying level of HA support in public cloud deployments. Some support native High Availability connection and configuration of a pair of VM-Series firewalls and others support the scaling of parallel implementations of VM-Series firewalls that have no High Availability configuration. Consult cloud-specific documentation for these differences.

Sample Questions

8. A potential customer says it wants to maximize the threat detection capability of its next-generation firewall. Which three additional services should it consider implementing to enhance its firewall's capability to detect Threats?
   A. Traps
   B. WildFire
   C. URL Filtering
   D. Expedition
   E. DNS Security
9. Which product best secured east-west traffic within a public cloud implementation. Which product is best suited for this need?
   A. RedLock
   B. MineMeld
   C. VM-Series firewall
   D. Cortex

©2016-2019, Palo Alto Networks, Inc.

1.3 Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements that leverage the Palo Alto Networks Security Operating Platform

High Availability

You can set up two Palo Alto Networks firewalls as an HA pair. HA allows you to minimize downtime by ensuring that an alternate firewall is available if the peer firewall fails. HA pairs comprise two firewalls of identical model, configuration, and licensing. They should be physically close to each other, but geographical separation is supported. The firewalls in an HA pair use dedicated or in-band HA ports on the firewall to synchronize data—network, object, and policy configurations—and to maintain state information. Firewall-specific configuration such as the management interface IP address or administrator profiles, HA-specific configuration, log data, and the Application Command Center (ACC) information is not shared between peers. To get a consolidated application and log view across the HA pair, you must use Panorama, the Palo Alto Networks centralized management system. When a failure occurs on a firewall in an HA pair and the peer firewall takes over the task of securing traffic, the event is called a failover. The conditions that trigger a failover are:

- One or more of the monitored interfaces fail. (link monitoring)
- One or more of the destinations specified on the firewall cannot be reached. (path monitoring)
- The firewall does not respond to heartbeat polls. (heartbeat polling and Hello messages)
- A critical chip or software component fails. (known as packet path health monitoring)

HA Modes

Palo Alto Networks firewalls support stateful ***active/passive*** or ***active/active*** High Availability with session and configuration synchronization with a few exceptions:

- The PA-200 (a discontinued model) firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some run-time data synchronization such as IPsec security associations. It does not support session synchronization (HA2), and therefore does not offer stateful failover.
- The VM-Series firewall in AWS and GCP supports active/passive HA only; if it is deployed with Amazon Elastic Load Balancing (ELB), it does not support HA (in this case ELB provides the failover capabilities).
- The VM-Series firewall in Microsoft Azure does support HA in PAN-OS V9 only.
- The VM-Series firewall deployed in Google Cloud Platform supports both active/active and active/passive HA.

Public cloud deployments of VM-Series firewalls also are supported in each vendor's version of a "scaled" implementation, allowing virtual firewalls to share the traffic load through a deployment of parallel firewall instances and the option to create or remove firewall instances in response to changes in traffic loads. These deployments all include the cloud vendor's load balancer deployed in front of the firewall "scale set" to manage the spreading of the traffic across the available firewalls. This same deployment practice also creates a High-Availability scenario in the sense that failing firewall instances can be removed from the "scale" set automatically using various detection abilities within the load balancer. A trade-off for "scale set" methods of High Availability is there typically is no synchronization between firewalls, so failovers are disruptive in the sense that existing sessions are terminated.

Active/Passive Clusters

©2016-2019, Palo Alto Networks, Inc.

Active/passive HA usually is the recommended deployment method. One firewall actively manages traffic while the other is synchronized and ready to transition to the active state if a failure occurs. In this mode, both firewalls share the same configuration settings, and one actively manages traffic until a path, link, system, or network failure occurs. When the active firewall fails, the passive firewall transitions to the active state, takes over seamlessly, and enforces the same policies to maintain network security. The firewalls synchronize the session state table, thus allowing the passive partner to become active and continue servicing active sessions at failover. Active/passive HA is supported in the Virtual Wire, Layer 2, and Layer 3 deployments.

Because one firewall is handling traffic and both firewalls share the same traffic interface configuration, active/passive usually is much easier to manage.

Active/Active Clusters

Both firewalls in the pair are active and processing traffic and work synchronously to handle session setup and session ownership. Both firewalls individually maintain session tables and routing tables and synchronize to each other. Active/active HA is supported in Virtual Wire and Layer 3 deployments.

In active/active HA mode, the firewall HA interfaces cannot receive address via DHCP Furthermore, only the active-primary firewall's traffic interface can function as a DHCP relay. The active-secondary firewall that receives DHCP broadcast packets drops them.

In a Layer 3 deployment of HA active/active mode, you can assign floating IP addresses, which move from one HA firewall to the other if a link or firewall fails. The interface on the firewall that owns the floating IP address responds to ARP requests with a virtual MAC address.

Floating IP addresses are recommended when you need functionality such as the Virtual Router Redundancy Protocol (VRRP). Floating IP addresses also can be used to implement VPNs and source NAT, thus allowing for persistent connections when a firewall offering those services fails.

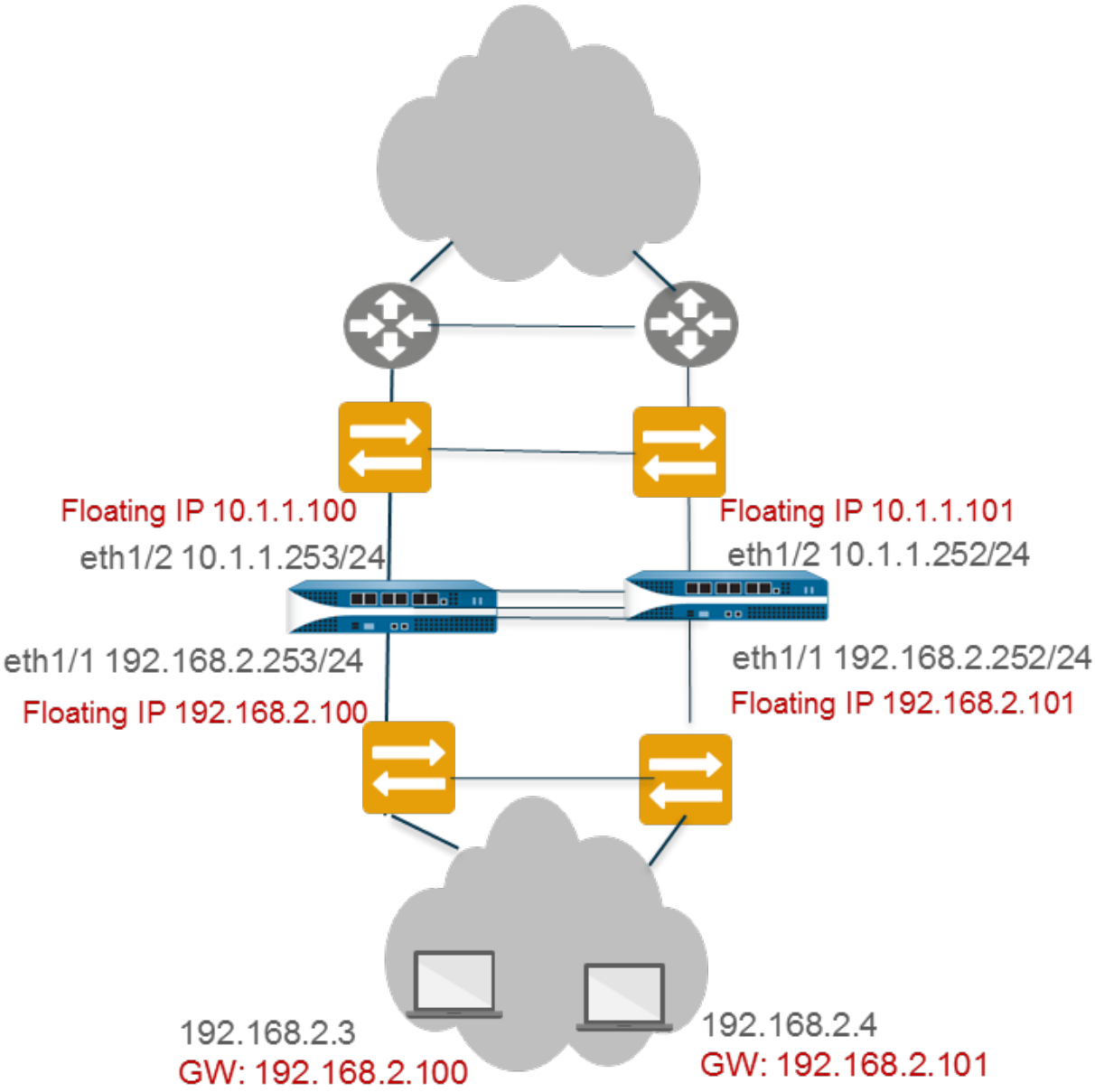
As shown in the figure that follows, each HA firewall interface has its own IP address and floating IP address. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure. You configure the end hosts to use a floating IP address as its default gateway, thus allowing you to load balance traffic to the two HA peers. You also can use external load balancers to load balance traffic.

If a link or firewall fails or a path monitoring event causes a failover, the floating IP address and virtual MAC address move over to the functional firewall. (In the figure that follows, each firewall has two floating IP addresses and virtual MAC addresses; they all move over if the firewall fails.) The functioning firewall sends a gratuitous ARP to update the MAC tables of the connected switches to inform them of the change in floating IP address and MAC address ownership to redirect traffic to itself.

After the failed firewall recovers, by default the floating IP address and virtual MAC address move back to firewall with the Device ID (0 or 1) to which the floating IP address is bound. More specifically, after the failed firewall recovers, it comes on line. The currently active firewall determines that the firewall is back online and checks whether the floating IP address it is handling belongs natively to itself or to the other

©2016-2019, Palo Alto Networks, Inc.

firewall. If the floating IP address originally was bound to the other Device ID, the firewall automatically gives it back. An example of a floating IP deployment follows:



Each firewall in the HA pair creates a virtual MAC address for each of its interfaces that has a floating IP address or ARP load-sharing IP address.

Choosing a Cluster Type

- Active/passive mode has simplicity of design; it is significantly easier to troubleshoot routing and traffic flow issues in active/passive mode.
- Both active/active and active/passive mode support a virtual wire deployment.
- Active/active mode requires advanced design concepts that can result in more complex networks. Depending on how you implement active/active HA, it might require additional configuration such as activating networking protocols on both firewalls, replicating NAT pools,

©2016-2019, Palo Alto Networks, Inc.

and deploying floating IP addresses to provide proper failover. Because both firewalls actively are processing traffic, the firewalls use additional concepts of session owner and session setup to perform Layer 7 content inspection.

- Active/active mode is recommended if each firewall needs its own routing instances and you require full, real-time redundancy out of both firewalls all the time. Active/active mode has faster failover and can handle peak traffic flows better than active/passive mode because both firewalls actively are processing traffic.
- In active/active mode, the HA pair can be used to temporarily process more traffic than what one firewall normally can handle. However, this situation should not be standard because a failure of one firewall causes all traffic to be redirected to the remaining firewall in the HA pair. Your design must allow the remaining firewall to process the maximum capacity of your traffic loads with content inspection enabled. If the design oversubscribes the capacity of the remaining firewall, high latency and/or application failure can occur.
- In cases of virtual firewall deployments, the cloud architecture might limit your deployment choices. Consult the design and deployment documentation specific to your chosen cloud vendor.

A use-case illustrating an active/active deployment can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-address-bound-to-active-primary-firewall.html

HA Links and Backup Links

The firewalls in an HA pair use HA links to synchronize data and maintain state information. Some models of the firewall have dedicated HA ports—Control link (HA1) and Data link (HA2)—and others require you to use the in-band ports as HA links.

- For firewalls with dedicated HA ports, use these ports to manage communication and synchronization between the firewalls. For details, see the link that follows.
- For firewalls without dedicated HA ports such as the PA-220, and PA-220R, as a best practice use a data-plane port for the HA port and use the management port as the HA1 backup.

Because the HA ports synchronize data critical to proper HA failover, implementation backup HA paths is a recommended best practice. In-band ports can be used for backup links for both HA1 and HA2 connections when dedicated backup links are not available. Consider the following guidelines when you configure backup HA links:

- The IP addresses of the primary and backup HA links must not overlap each other.
- HA backup links must be on a different subnet from the primary HA links.
- HA1-backup and HA2-backup ports must be configured on separate physical ports. The HA1-backup link uses ports 28770 and 28260.

More information about the purpose and setup of the HA links can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links

©2016-2019, Palo Alto Networks, Inc.

HA pair configuration synchronization is discussed here:
https://live.paloaltonetworks.com/t5/Learning-Articles/Information-Synchronized-in-an-HA-Pair/ta-p/57292
Information about data that is not synchronized between HA partners is at the following links:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/reference-ha-synchronization/what-settings-dont-sync-in-activepassive-ha
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/reference-ha-synchronization/what-settings-dont-sync-in-activeactive-ha

Sample Questions

10. Why would you recommend an active/active cluster instead of an active/passive one?
    A. Active/active is the preferred solution when the firewall cluster is behind a load balancer that randomizes routing, thus requiring both firewalls to be active.
    B. Active/active usually is the preferred solution because it allows for more bandwidth while both firewalls are up.
    C. Active/active is the preferred solution when the PA-7000 Series is used. Use active/passive with the PA-5200 Series or smaller form factors.
    D. Active/active is the preferred solution when using the PA-5200 Series or smaller form factors. When using the PA-7000 Series, use active/passive.
11. Which two events can trigger an HA pair failover event?
    A. An HA1 cable is disconnected from one of the firewalls.
    B. A Dynamic Update fails to download and install.
    C. The firewall fails to ping a path-monitored destination address successfully.
    D. OSPF implemented on the firewall determines that an available route is now down.
    E. RIP implemented on the firewall determines that an available route is now down.
12. Which two firewall features support floating IP addresses in an active/active HA pair? (Choose two.)
    A. data-plane traffic interfaces
    B. source NAT
    C. VPN endpoints
    D. loopback interfaces
    E. management port
13. How are configurations in firewalls in an active/passive HA pair synchronized?
    A. An administrator commits the changes to one, then commits them to the partner, at which time the changes are sent to the other.
    B. An administrator pushes the config file to both firewalls, then commits them.
    C. An administrator commits changes to one, which automatically synchronizes with the other.
    D. An administrator schedules an automatic sync frequency in the firewall configs.
14. How is an active/passive HA pair configured in virtual firewalls deployed in public clouds? (Choose two.)
    A. The virtual firewalls are deployed in a cloud “scale set” with a cloud-supplied load balancer in front to detect and manage failover.
    B. The virtual firewalls rely on a VM-Series plugin to map appropriate cloud functions to the

©2016-2019, Palo Alto Networks, Inc.

firewall's HA settings.

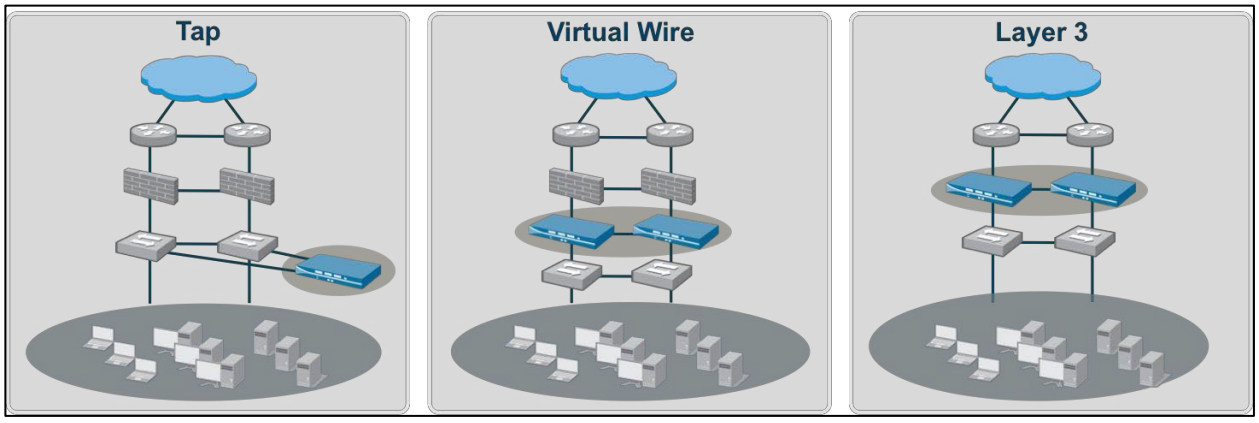
C. Virtual firewalls use PAN-OS HA configuration combined with appropriate cloud deployments of interfaces for HA use.
D. The virtual firewalls use an HA Compatibility module for the appropriate cloud technology

©2016-2019, Palo Alto Networks, Inc.

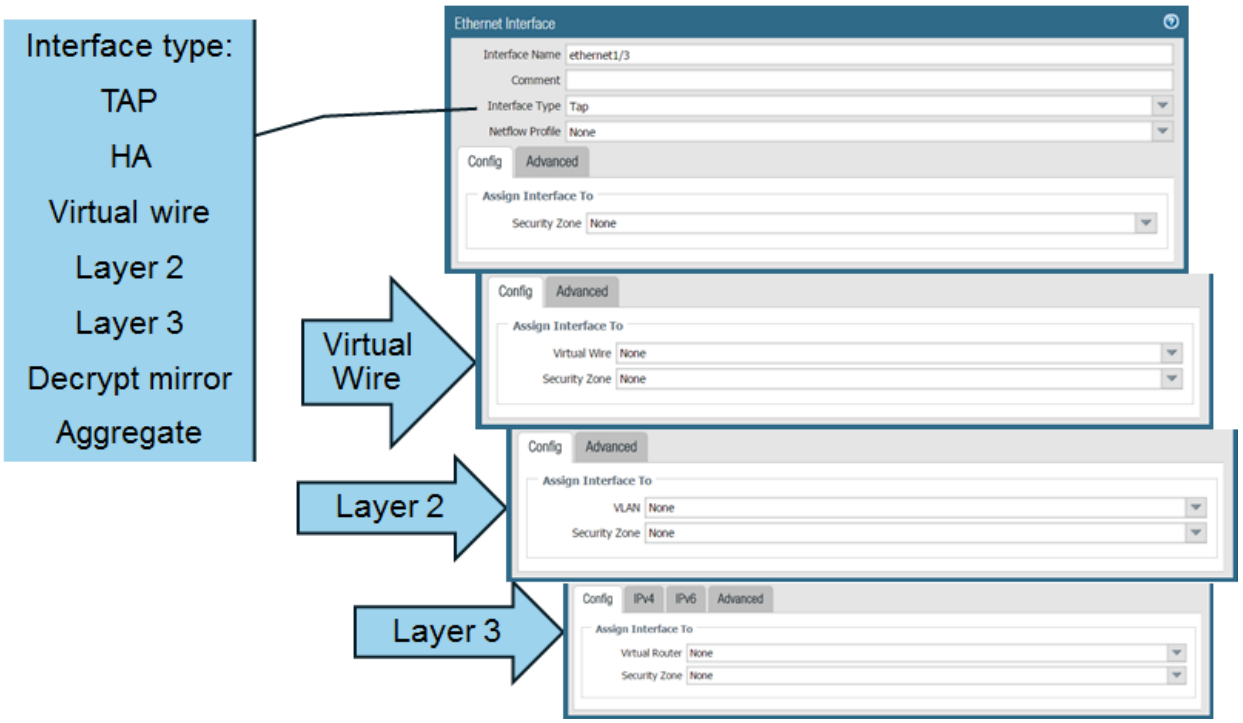
1.4 Identify the appropriate interface type and configuration for a specified network deployment

Types of Interfaces

Palo Alto Networks firewalls support several different interface types: TAP mode, virtual wire mode, Layer 2, Layer 3, and aggregate. A single firewall can freely intermix interface types to meet any integration need. The decision about which interface configuration to choose depends on functional need and existing network integration requirements. The following figure shows the primary configuration options for integration of physical traffic ports. Layer 2 also is available but is not pictured.



The following screenshot shows primary configuration options for interfaces:



©2016-2019, Palo Alto Networks, Inc.

Tap

A network tap is a device that provides a way to access data flowing across a computer network. TAP mode deployment allows you to passively monitor traffic flows across a network using a switch SPAN or mirror port.

A switch SPAN or mirror port permits the copying of traffic from other ports on the switch to the Tap interface of the firewall, providing a one-way flow of copied network traffic into the firewall. This configuration allows the firewall to perform detection of traffic and threats but prevents any enforcement action from taking place because the traffic does flow through the firewall back to the environment.

By deploying the firewall in TAP mode, you can get visibility into which applications are running on the network without having to make any changes to your network design. When the firewall is in TAP mode, it also can identify threats on your network. Remember, however, that the traffic is not running through the firewall when the firewall is in TAP mode, so no action can be taken on the traffic, including blocking traffic with threats or applying QoS traffic control.

Details about configuring Tap interfaces are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/tap-interfaces.html

Virtual Wire

In a virtual wire deployment, you install a firewall transparently on a network segment by binding two firewall ports (interfaces) together. The virtual wire logically connects the two interfaces; hence, the virtual wire is internal to the firewall.

Use a virtual wire deployment only when you want to seamlessly integrate a firewall into a topology and the two connected interfaces on the firewall need not do any switching or routing. For these two interfaces, the firewall is considered a bump in the wire.

A virtual wire deployment simplifies firewall installation and configuration because you can insert the firewall into an existing topology without assigning MAC or IP addresses to the interfaces, redesigning the network, or reconfiguring surrounding network devices. The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags. It also supports Security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active HA, QoS, zone protection (with some exceptions), non-IP protocol protection, DoS protection, packet buffer protection, tunnel content inspection, and NAT.

Each virtual wire interface is directly connected to a Layer 2 or Layer 3 networking device or host. The virtual wire interfaces have no Layer 2 or Layer 3 addresses. When one of the virtual wire interfaces receives a frame or packet, it ignores any Layer 2 or Layer 3 addresses for switching or routing purposes but applies your security or NAT policy rules before passing an allowed frame or packet over the virtual wire to the second interface and on to the network device connected to it.

You wouldn't use a virtual wire deployment for interfaces that need to support switching, VPN tunnels, or routing because they require a Layer 2 or Layer 3 address. A virtual wire interface doesn't use an

©2016-2019, Palo Alto Networks, Inc.

Interface Management Profile, which controls services such as HTTP and ping and therefore requires the interface to have an IP address.

All firewalls shipped from the factory have two Ethernet ports (ports 1 and 2) preconfigured as virtual wire interfaces, and these interfaces allow all untagged traffic.

Details about configuring virtual wire interfaces are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces.html

Layer 2

In a Layer 2 deployment, the firewall provides switching between two or more networks. Devices are connected to a Layer 2 segment; the firewall forwards the frames to the proper port, which is associated with the MAC address identified in the frame. Configure a Layer 2 interface when switching is required.

Details about configuring Layer 2 interfaces are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/layer-2-interfaces.html

Layer 3

In a Layer 3 deployment, the firewall routes traffic between multiple ports using TCP/IP addressing. Before you can configure Layer 3 interfaces, you must configure the virtual routers that you want the firewall to use to route the traffic for each Layer 3 interface.

Layer 3 deployments require more network planning and configuration preparation than do most other firewall interfaces but still are the most widely used in firewall deployments. Palo Alto Networks supports both IPv4 and IPv6 simultaneously through a *dual stack* implementation when IPv6 is required.

Each Layer 3 interface must be configured with an IPv4 and/or an IPv6 address, zone name assignment, and the attached virtual router that services the traffic on the interface. Options available to meet other connectivity requirements include:

- NetFlow integration
- MSS adjustment
- MTU adjustment
- Binding of firewall services (ping responses, web management interface availability, etc.)
- Neighbor discovery for IPv6
- Manual MAC address assignment
- LLDP enablement
- Dynamic DNS support
- Link negotiation settings

Details about configuring Layer 3 interfaces and its options can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/layer-3-interfaces/configure-layer-3-interfaces.html

©2016-2019, Palo Alto Networks, Inc.

Decrypt Mirror

Decrypt mirror is a special configuration supporting the routing of decrypted traffic copies through an external interface to a data loss prevention (DLP) service. Data loss prevention is a product category for products that scan internet-bound traffic for keywords and patterns that identify sensitive information. Specific information is here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGDCA0

Aggregate Interfaces

An aggregate Ethernet (AE) interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces into a single virtual interface that connects the firewall to another network device or another firewall. An AE interface group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy: When one interface fails, the remaining interfaces continue to support traffic.

Before you configure an AE interface group, you must configure its interfaces. Hardware media can differ among the interfaces assigned to any particular aggregate group. For example, you can mix fiber optic and copper. But the bandwidth (1Gbps, 10Gbps, 40Gbps, or 100GBps) and interface type (HA3, virtual wire, Layer 2, or Layer 3) must be the same. You can add up to eight AE interface groups per firewall, and each group can have up to eight interfaces.

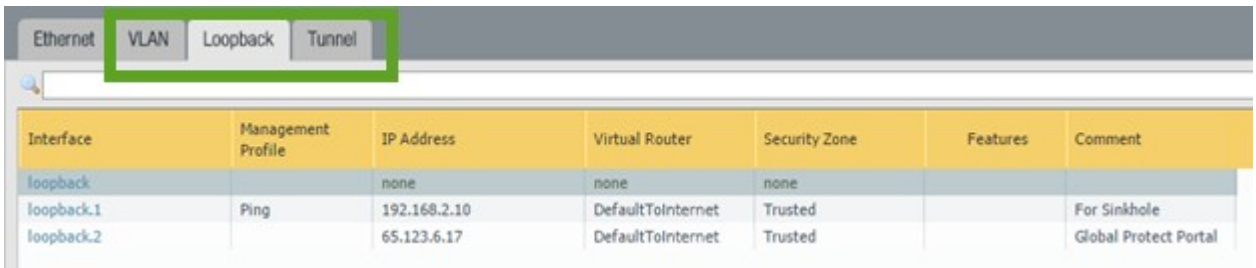
Aggregate interface creation begins with the definition of an Aggregate Interface group, after which individual interfaces are added to the group.

Information about the creation of the group can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html

Details about assigning interfaces to the group can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface

Virtual Interfaces

Palo Alto Networks firewalls also provide several virtual interface types for additional functionality:



©2016-2019, Palo Alto Networks, Inc.

VLAN Interfaces

VLANs are logical interfaces that specifically serve as interconnects between on-board virtual switches (VLANs) and virtual routers, which allows traffic to move from Layer 2 to Layer 3 within the firewall.

Specific information is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-interfaces-vlan

Loopback Interfaces

Loopback interfaces are Layer 3 interfaces that exist only virtually and connect to virtual routers in the firewall. Loopback interfaces are used for multiple network engineering and implementation purposes. They can be destination configurations for DNS sinkholes, GlobalProtect service interfaces (portals and gateways), routing identification, and more.

Specific information about configuring loopback Interfaces can be found in the reference for Layer 3 interfaces.

Tunnel Interfaces

In a VPN tunnel setup, the Layer 3 interface at each end must have a logical tunnel interface for the firewall to connect to and establish a VPN tunnel. A tunnel interface is a logical (virtual) interface that is used to deliver traffic between two endpoints. If you configure any proxy IDs, the proxy ID is counted toward any IPsec tunnel capacity.

The tunnel interface must belong to a security zone to apply policy and it must be assigned to a virtual router to use the existing routing infrastructure. Ensure that the tunnel interface and the physical interface are assigned to the same virtual router so that the firewall can perform a route lookup and determine the appropriate tunnel to use.

The Layer 3 interface that the tunnel interface is attached to typically belongs to an external zone, for example, the untrust zone. Although the tunnel interface can be in the same security zone as the physical interface, for added security and better visibility you can create a separate zone for the tunnel interface. If you create a separate zone for the tunnel interface, such as a VPN zone, you will need to create security policies to enable traffic to flow between the VPN zone and the trust zone.

A tunnel interface does not require an IP address to route traffic between the sites. An IP address is required only if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel. With dynamic routing, the tunnel IP address serves as the next hop IP address for routing traffic to the VPN tunnel.

If you are configuring the Palo Alto Networks firewall with a VPN peer that performs policy-based VPN, you must configure a local and remote proxy ID when setting up the IPsec tunnel. Each peer compares the proxy IDs configured on it with what actually is received in the packet to allow a successful IKE phase 2 negotiation. If multiple tunnels are required, configure unique proxy IDs for each tunnel interface; a tunnel interface can have a maximum of 250 proxy IDs. Each proxy ID counts toward the IPsec VPN tunnel

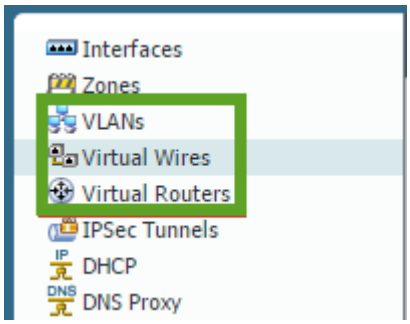
©2016-2019, Palo Alto Networks, Inc.

capacity of the firewall, and the tunnel capacity varies by the firewall model.

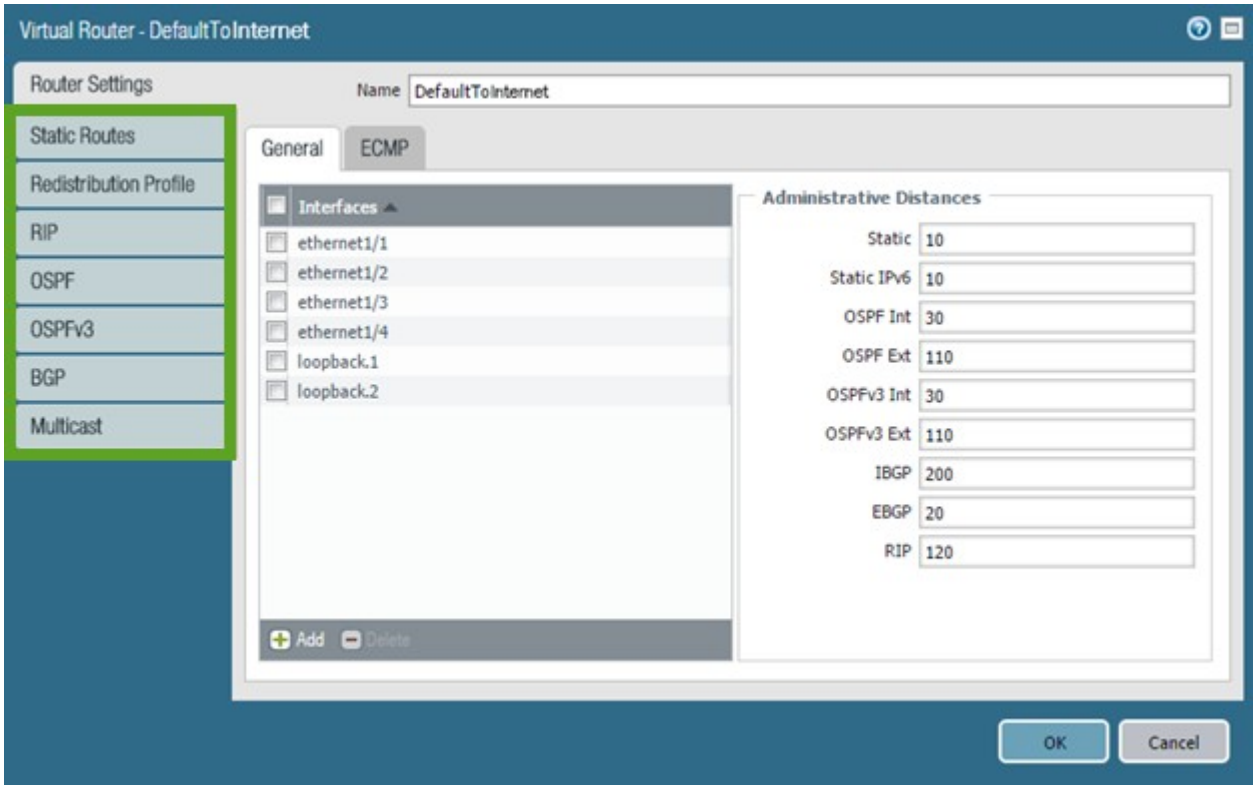
Specific information about configuring tunnel interfaces can be found in the references for Layer 3 interfaces.

Traffic Forwarding

All traffic that arrives at the firewall will be delivered either to an internal firewall process (destination traffic) or be passed through a traffic interface (transit traffic). All transit traffic must be handed off to the egress interface by a traffic handling object that matches the interface type. Examples of these objects are VLAN objects (VLANs) for Layer 2 traffic, virtual routers for Layer 3 traffic, and virtual wires for virtual wire interfaces.



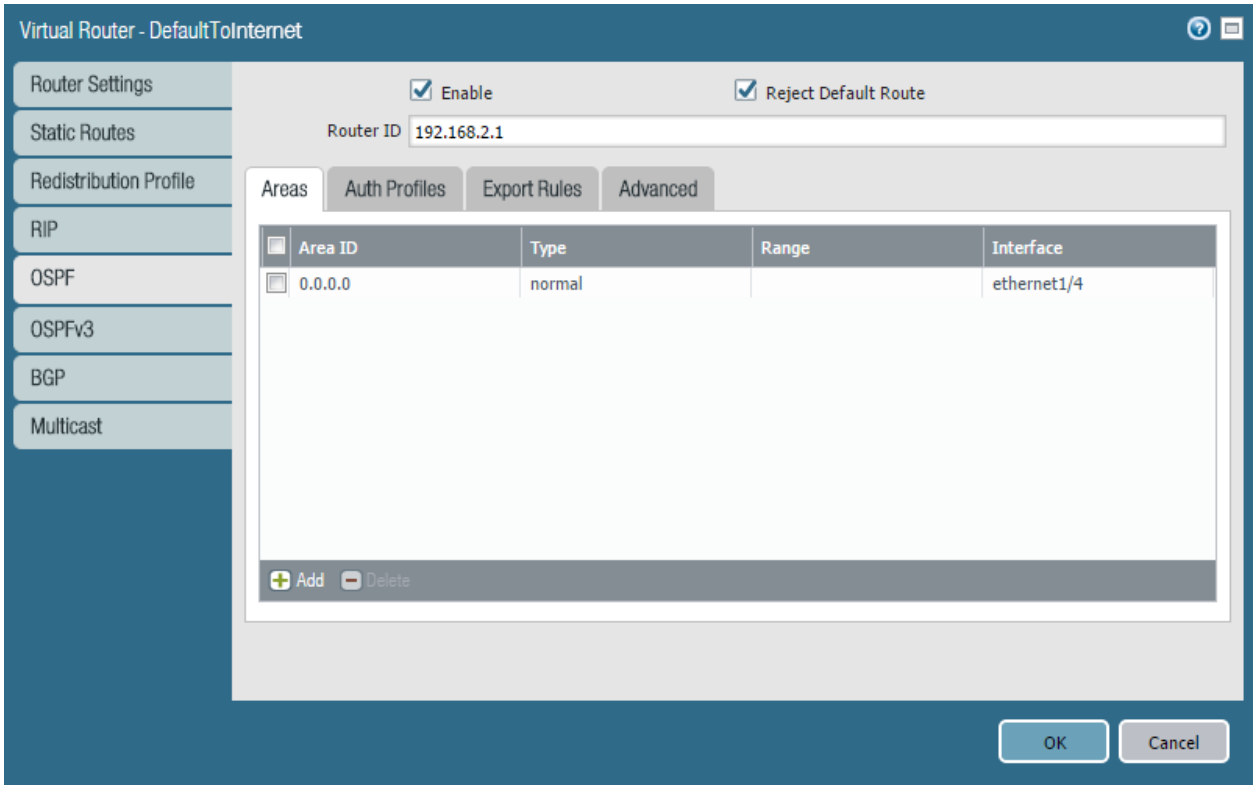
Simultaneous implementations of multiple traffic handler types in multiple quantities are possible. Each object contains configuration capability appropriate to its protocol-handling needs. Virtual routers implement various dynamic routing support if desired.



Each Layer 3 dynamic routing protocol includes appropriate specific configuration options. An example

©2016-2019, Palo Alto Networks, Inc.

of OSPFv2 follows.



IPsec tunnels are considered Layer 3 traffic segments for implementation purposes and are handled by virtual routers as is any other network segment. Forwarding decisions are made by destination address, not by VPN policy.

Virtual Routers

Because Layer 3 interfaces and their associated virtual routers are the most widely used deployment options, a review of virtual routers follows.

A virtual router is a function of the firewall that participates in Layer 3 routing. The firewall uses virtual routers to obtain routes to other subnets after you manually define static routes or through participation in one or more Layer 3 routing protocols (dynamic routes). The routes that the firewall obtains through these methods populate the IP routing information base (RIB) on the firewall. When a packet is destined for a different subnet than the one it arrived on, the virtual router obtains the best route from the RIB, places it in the forwarding information base (FIB), and forwards the packet to the next hop router defined in the FIB. The firewall uses Ethernet switching to reach other devices on the same IP subnet. (An exception to adding only a single optimal route to the FIB occurs if you are using ECMP, in which case all equal-cost routes go in the FIB.)

The Ethernet, VLAN, and tunnel interfaces defined on the firewall receive and forward Layer 3 packets. The destination zone is derived from the outgoing interface based on the forwarding criteria, and the firewall consults policy rules to identify the Security policies that it applies to each packet. In addition to routing to other network devices, virtual routers can route to other virtual routers within the same firewall if a next hop is specified to point to another virtual router.

©2016-2019, Palo Alto Networks, Inc.

You can configure Layer 3 interfaces on a virtual router to participate with dynamic routing protocols (BGP, OSPFv2, OSPFv3, or RIP) and add static routes. You also can create multiple virtual routers, each maintaining a separate set of routes that aren't shared between virtual routers, which enables you to configure different routing behaviors for different interfaces.

Each Layer 3 Ethernet, loopback, VLAN, and tunnel interface defined on the firewall must be associated with a virtual router. Although each interface can belong to only one virtual router, you can configure multiple routing protocols and static routes for a virtual router.

A firewall can have more than one router instance with each model supporting a different maximum. An interface can be attached to one virtual router at a time. Virtual routers can route directly to each other within the firewall.

Administrative Distance

Within the virtual router configuration, set administrative distances for types of routes as required for your network. A virtual router that has two or more different routes to the same destination uses administrative distance to choose the best path from different routing protocols and static routes, by preferring a lower distance.

Route Redistribution

Route redistribution on the firewall is the process of making routes that the firewall learned from one routing protocol (or a static or connected route) available to a different routing protocol, thereby increasing the number of reachable networks. Without route redistribution, a router or virtual router advertises and shares routes only with other routers that run the same routing protocol. You can redistribute IPv4 or IPv6 BGP, connected, or static routes into the OSPF RIB and redistribute OSPFv3, connected, or static routes into the BGP RIB.

Route distribution means, for example, you can make specific networks that were once available only by manual static route configuration on specific routers available to BGP autonomous systems or OSPF areas. You also can advertise locally connected routes, such as routes to a private lab network, into BGP autonomous systems or OSPF areas.

You might want to give users on your internal OSPFv3 network access to BGP so they can access devices on the internet. In this case you would redistribute BGP routes into the OSPFv3 RIB.

Conversely, you might want to give your external users access to some parts of your internal network, so you can make internal OSPFv3 networks available through BGP by redistributing OSPFv3 routes into the BGP RIB.

©2016-2019, Palo Alto Networks, Inc.

Equal-Cost Multi-Path Routing

Equal-cost multi-path (ECMP) processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination. Without this feature, the virtual router will choose multiple equal-cost routes to the same destination from the routing table and add it to its forwarding table; it will not use any of the other routes unless there is an outage in the chosen route.

Enablement of ECMP functionality on a virtual router allows the firewall to have up to four equal-cost paths to a destination in its forwarding table, which allows the firewall to:

- Load balance flows (sessions) to the same destination over multiple equal-cost links
- Efficiently use all available bandwidth on links to the same destination rather than leave some links unused.
- Dynamically shift traffic to another ECMP member to the same destination if a link fails, rather than having to wait for the routing protocol or RIB table to elect an alternative path/route. Dynamic failover can help reduce downtime when links fail.

Information about configuring ECMP can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/ecmp

GRE Tunnels

A GRE tunnel connects two endpoints (a firewall and another device) in a point-to-point, logical link. The firewall can terminate GRE tunnels; you can route or forward packets to a GRE tunnel. GRE tunnels are simple to use and often are the tunneling protocol of choice for point-to-point connectivity, especially to services in the cloud or to partner networks.

Create a GRE tunnel when you want to direct packets that are destined for an IP address to take a certain point-to-point path, for example, to a cloud-based proxy or to a partner network. The packets travel in the GRE tunnel (over a transit network such as the internet) to the cloud service while on their way to the destination address. Thus, the cloud service can enforce its services or policies on the packets.

After the firewall allows a packet (based on a policy match) and the packet egresses to a GRE tunnel interface, the firewall adds GRE encapsulation; it doesn't generate a session. The firewall does no Security policy rule lookup for the GRE-encapsulated traffic; therefore, you don't need a Security policy rule for the GRE traffic the firewall encapsulates. However, after the firewall receives GRE traffic, it generates a session and applies all policies to the GRE IP header in addition to the encapsulated traffic. The firewall treats the received GRE packet as it would any other packet.

If the firewall receives the GRE packet on an interface that has the same zone as the tunnel interface associated with the GRE tunnel (for example, tunnel.1), the source zone is the same as the destination zone. By default, traffic is allowed within a zone (intrazone traffic), so the ingress GRE traffic is allowed by default.

However, if you configured your own intrazone Security policy rule to deny such traffic, you must explicitly allow GRE traffic.

©2016-2019, Palo Alto Networks, Inc.

Likewise, if the zone of the tunnel interface associated with the GRE tunnel (for example, tunnel.1) is different from the zone of the ingress interface, you must configure a Security policy rule to allow the GRE traffic.

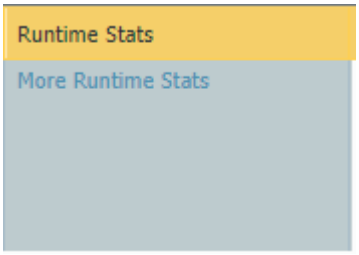
Because the firewall encapsulates the tunneled packet in a GRE packet, the additional 24 bytes of GRE header automatically result in a smaller maximum segment size (MSS) in the maximum transmission unit (MTU). If you don't change the IPv4 MSS Adjustment Size for the interface, by default the firewall reduces the MTU by 64 bytes (40 bytes of IP header + 24 bytes of GRE header).

This means if the default MTU is 1,500 bytes, the MSS will be 1,436 bytes (1,500 − 40 − 24 = 1436). If you configure an MSS adjustment size of 300 bytes, for example, the MSS will be only 1,176 bytes (1,500 − 300 − 24 = 1,176).

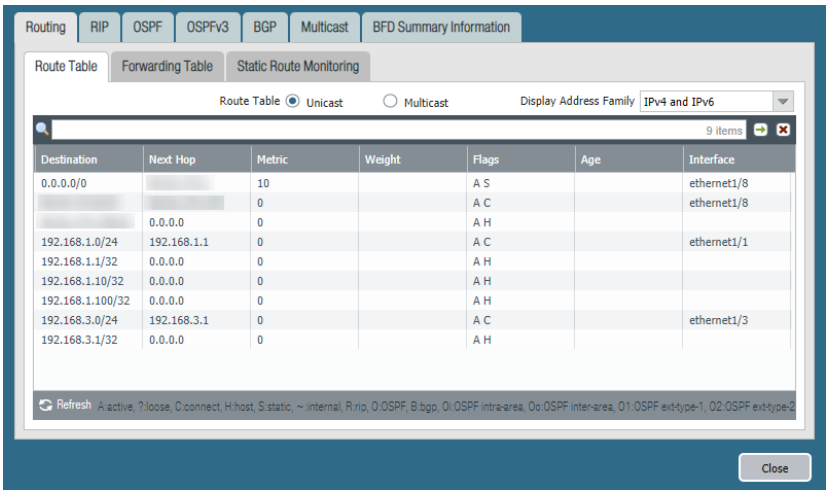
Routing of a GRE or IPsec tunnel to a GRE tunnel is not supported. However, you can route a GRE tunnel to an IPsec tunnel. A GRE tunnel does not support QoS. The firewall does not support a single interface acting as both a GRE tunnel endpoint and a decryption broker. GRE tunneling does not support NAT between GRE tunnel endpoints.

Routing Troubleshooting

Troubleshooting of the routing decisions made by a virtual router when it processes a packet can be diagnosed easily. A virtual router maintains a RIB and a FIB, which can be displayed any time in the management web interface using the **Runtime Stats** link displayed on the virtual router summary line:



Click the **More Runtime Stats** link to get access to the routing table (RIB) and the forwarding table (FIB) with additional displays that contain the status of any enabled dynamic routing protocols.



©2016-2019, Palo Alto Networks, Inc.

Sample Questions

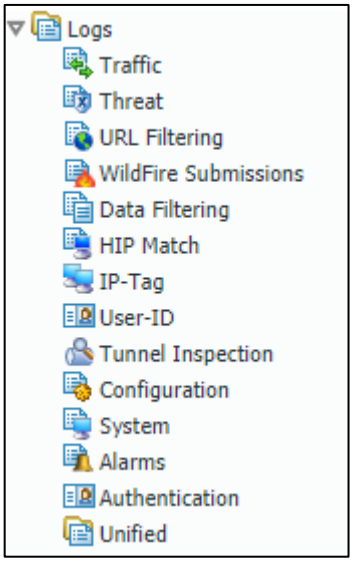
15. When a NGFW is in front of an existing firewall to provide better security while making the minimum required network changes, which interface type do you use?
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3
16. Which kind of interface do you use to connect Layer 2 and Layer 3 interfaces?
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3
17. Which three types of interfaces can the firewall's management web interface be bound to? (Choose three.)
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3
18. Which three types of interfaces connect to a virtual router?
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3
19. Which dynamic routing protocol is not supported by the Palo Alto Networks firewall?
    A. RIP
    B. OSPF
    C. OSPFv3
    D. IGRP
    E. BGP
20. Which action is not compatible with aggregate interface configuration?
    A. aggregating 12 Layer 3 interfaces
    B. aggregating 4 virtual wire interfaces
    C. aggregating interfaces in an HA pair
    D. aggregating two 10Gbps optical and two 10Gbps copper Ethernet ports

©2016-2019, Palo Alto Networks, Inc.

1.5 Identify strategies for retaining logs using Distributed Log Collection

Event Logging on NGFWs

Palo Alto Networks next-generation firewalls automatically generate local log entries through normal traffic processing.



A firewall's default behavior is to store these logs in locally available storage. Firewall appliances have fixed storage that can't be expanded (except the 7000 Series). This storage is used in a "circular" fashion, meaning that log entries are written until storage fills, at which point the oldest entries are overwritten. Because storage size is fixed and logging rates depend in part on Security policy rule settings and traffic rates, a firewall's log retention period before entries are overwritten is difficult to predict.

VM-Series virtual firewall logging behavior is the same, except that cloud storage resources often can be expanded for increased log retention.

Distributed Log Collection

For Centralized Logging and Reporting, you must forward the logs generated on the firewalls to your on-premises infrastructure that includes the Panorama management server or Log Collectors, or you must send the logs to the cloud-based Cortex Data Lake service. In addition to aggregating logs, Panorama can forward them as SNMP traps, email notifications, syslog messages, and HTTP payloads to an external server.

For centralized logging and reporting, you also can use the Cortex Data Lake that is designed to work seamlessly with Panorama. The Cortex Data Lake allows your managed firewalls to forward logs to the Cortex Data Lake infrastructure instead of to Panorama or to the managed Log Collectors, so you can augment your existing distributed log collection setup or scale your current logging infrastructure.

The Application Command Center (ACC) on Panorama provides a single pane for unified reporting across all the firewalls. It enables you to centrally monitor network activity to analyze, investigate, and report on traffic and security incidents. On Panorama, you can view logs and generate reports from logs forwarded to the Cortex Data Lake, to Panorama, or to the managed Log Collectors, if configured, or you can query

©2016-2019, Palo Alto Networks, Inc.

the managed firewalls directly.

For example, you can generate reports about traffic, threat, and/or user activity in the managed network based on logs stored on Panorama (and the managed collectors) or by accessing the logs stored locally on the managed firewalls, or on Cortex Data Lake.

If you don't configure Log Forwarding to Panorama or Cortex Data Lake, you can schedule reports to run on each managed firewall and forward the results to Panorama for a combined view of user activity and network traffic. Although reports don't provide a granular drill-down on specific information and activities, they provide a unified monitoring approach.

Panorama uses Log Collectors to aggregate logs from managed firewalls. When Panorama generates reports, it queries the Log Collectors for log information that provides you visibility into all the network activity that your firewalls monitor. Because you use Panorama to configure and manage Log Collectors, they also are known as managed collectors. Panorama can manage two types of Log Collectors:

- Local Log Collector: This type of Log Collector runs locally on the Panorama management server. Only an M-600, M-500 appliance, M-200, M-100 appliance, or Panorama virtual appliance in Panorama mode supports a local Log Collector.

Note: If you forward logs to a Panorama virtual appliance in Legacy mode, it stores the logs locally without a Log Collector.

- Dedicated Log Collector: This is an M-600, M-500, M-200, M-100 appliance, or Panorama virtual appliance in Log Collector mode. You can use an M-Series appliance in Panorama mode or a Panorama virtual appliance in Panorama or Legacy (ESXi and vCloud Air) mode to manage Dedicated Log Collectors. Before you can use the Panorama web interface for managing Dedicated Log Collectors, you must add them as managed collectors. Otherwise, administrative access to a Dedicated Log Collector is available only through its CLI using the predefined administrative user (admin) account. Dedicated Log Collectors don't support additional administrative user accounts.

You can use either or both types of Log Collectors to achieve the best logging solution for your environment.

A Collector Group is 1 to 16 managed collectors that operate as a single logical log collection unit. If the Collector Group contains Dedicated Log Collectors, Panorama uniformly distributes the logs across all the disks in each Log Collector and across all Log Collectors in the group. This distribution optimizes the available storage space. To enable a Log Collector to receive logs, you must add it to a Collector Group. You can enable log redundancy by assigning multiple Log Collectors to a Collector Group. The Collector Group configuration specifies which managed firewalls can send logs to the Log Collectors in the group.

If an HA pair of Panoramas is configured to include Log Collectors, the Log Collectors function independently from the HA relationship and both are independently active. They can be added to different Collector Groups or to the same Collector Group.

More information about this topic can be found here:https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/centralized-logging-and-reporting.html

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

21. How do you create and view enterprise-wide reports that include data from all managed firewalls?
    A. Run Panorama reports normally. Firewall summary reporting information is gathered automatically once Firewall are managed by Panorama.
    B. Configure log forwarding on the managed firewalls to forward logs to Panorama using syslog formatting.
    C. Run custom Panorama reports and select **remote log**s as the information source.
    D. Run custom Panorama reports and select **log collector** as the information source.
22. What must you configure to guarantee duplication of log data on Log Collectors to eliminate log data loss in cases of hardware failure?
    A. Log Collector settings to include “Replicate Data”
    B. Panorama HA settings to include “Duplicate Logs”
    C. Log Collector settings to include “Enable log redundancy”
    D. Log forwarding settings of firewalls for two Log Collector destinations
23. Which three devices can be used as Log Collectors?
    A. Virtual Panorama
    B. PA-220R
    C. M-600
    D. M-200
    E. VM-300LC
24. Which statement is true regarding Log Collecting in a Panorama HA pair?
    A. Both Panoramas cannot be configured to collect logs.
    B. Log collecting is handled by the active HA Panorama until a failover occurs.
    C. Both Panoramas collect independent logging traffic and are not affected by failover.
    D. Both Panoramas receive the same logging traffic and synchronize in case of HA failover.

©2016-2019, Palo Alto Networks, Inc.

1.6 Given a scenario, identify the strategy that should be implemented for Distributed Log Collection

Log Collection Platform Choices

When centralized logging is implemented, one design criterion is where log collection will occur. The options for log data collection are Panorama management platform, a Panorama-managed Log Collector and the Logging Service.

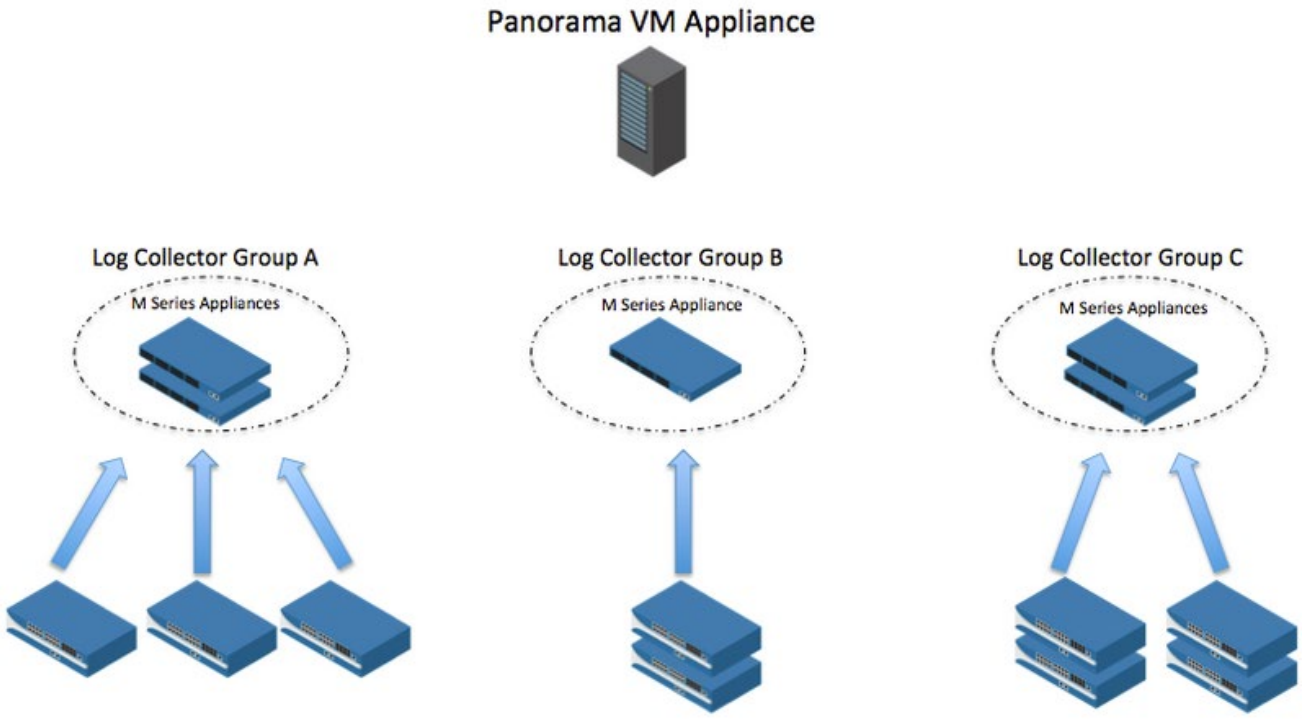
The choice of platform is driven by your anticipated logging volume and the network topology the logging data will traverse.

A complete discussions of log sizing and its impact on design can be found here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clc8CAC

On-Premises Log Collection

Log collection is collecting logs from one or multiple firewalls, either to a single Panorama or to a distributed log collection infrastructure. Reports can be generated based on that log data, whether it resides locally to the Panorama (e.g., single M-Series or VM appliance) or on a distributed logging infrastructure.

The Panorama solution allows for flexibility in design by assigning these functions to different physical pieces of the management infrastructure. For example, device management may be performed from a VM Panorama, while the firewalls forward their logs to collocated dedicated Log Collectors:



©2016-2019, Palo Alto Networks, Inc.

Cortex Data Lake

Palo Alto Networks Logging Service exists as a cloud-based storage mechanism for logs generated by the security platform. Log storage is an important consideration when you buy Palo Alto Networks devices or services. Sufficient log retention not only enables operations by ensuring data is available to administrators for troubleshooting and incident response, but it also enables the full suite services provided by the Cortex Data Lake.

Sample Questions

25. How are log retention periods on Palo Alto Networks firewalls increased?
    A. add storage to any firewall model
    B. increase the allocation for overall log storage within the firewall
    C. turn on log compression
    D. forward logs to external Log Collectors
26. How is firewall log data sent to the Cortex Data Lake accessed?
    A. direct viewing and searching with the Cortex gateway
    B. Panorama using a Log Collector configuration for access
    C. reporting in a firewall using a “remote data source” configuration
    D. reporting in a firewall equipped with a “Remote Logging” plugin
27. Log retention is increased when a Dedicated Log Collector is used to collect logs from firewalls in which two ways?
    A. turning on “Log Compression” in the Log Collector
    B. adding storage capacity to the Log Collector
    C. enabling “Log Storage Sharing” between the Log Collector and Panorama
    D. adding Log Collectors to the Log Collector Group

©2016-2019, Palo Alto Networks, Inc.

1.7 Identify how to use template stacks for administering Palo Alto Networks firewalls as a scalable solution using Panorama

Panorama Overview

Without Panorama, Palo Alto Networks firewalls have no direct knowledge of each other and must be managed as independent entities. Panorama offers several important integration functions that provide enterprise management for multiple firewalls.

The Panorama management server provides centralized monitoring and management of multiple Palo Alto Networks next-generation firewalls and of WildFire appliances and appliance clusters. It provides a single location from which you can oversee all applications, users, and content traversing your network, and then uses this knowledge to create application enablement policies that protect and control the network. Use of Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

The PCNSE certification requires the candidate taking the test to have knowledge of Panorama firewall management functions. The following information reviews these management concepts but does not cover the remaining Panorama features.

Panorama uses *device groups* and *templates* to group firewalls into logical sets that require similar configuration. You use device groups and templates to centrally manage all configuration elements, policies, and objects on the managed firewalls. Panorama also enables you to centrally manage licenses, software (PAN-OS software, SSL-VPN client software, GlobalProtect agent/app software), and content updates (Applications and threats, WildFire, and Antivirus).

Panorama's web interface management interface looks very much like the firewall's management web interface.

Firewall menus from management web interface:

Panorama menus from management web interface:

You can use the **Device** and **Network** tabs in Panorama to deploy a common base configuration to multiple firewalls that require similar settings using a template or a template stack (a combination of templates). When you manage firewall configurations with Panorama, you use a combination of device groups (to manage shared policies and objects) and templates (to manage shared device and network settings).

©2016-2019, Palo Alto Networks, Inc.

Templates and Template Stacks

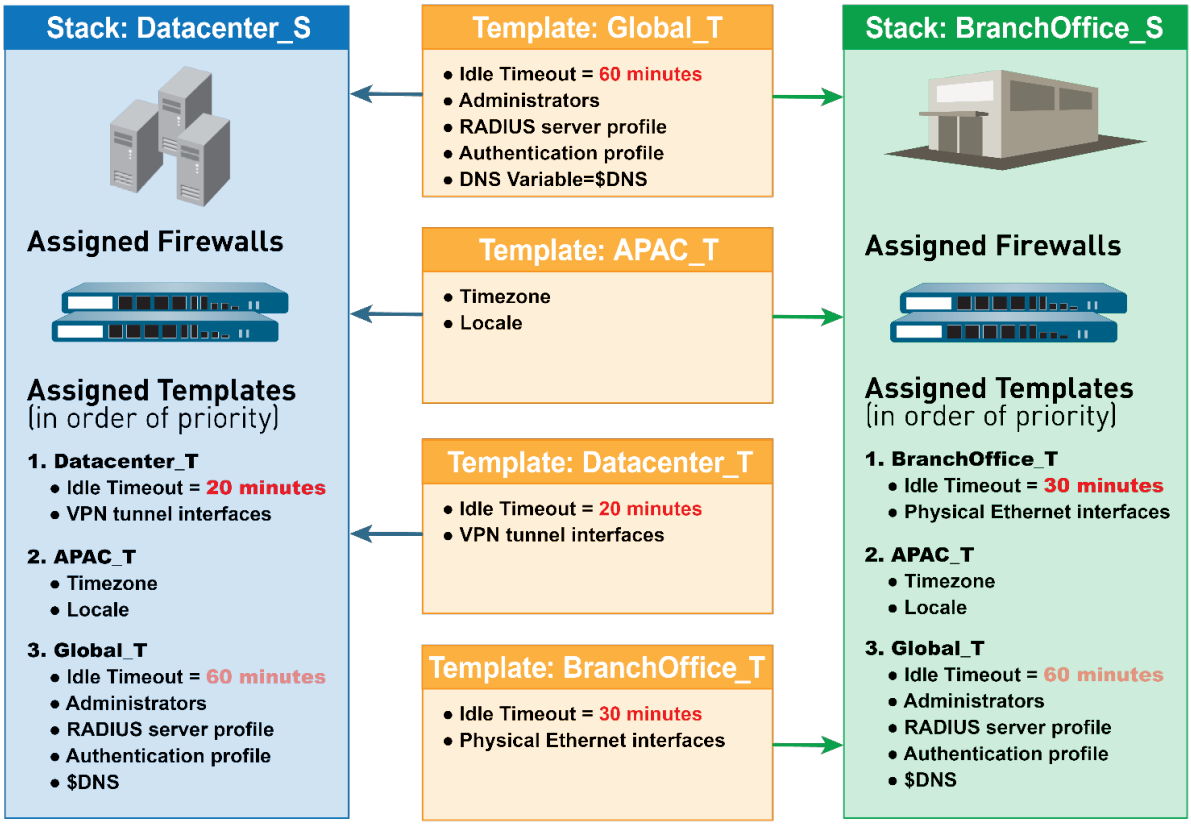
You use templates and template stacks to configure the settings that enable firewalls to operate on the network. Templates are the basic building blocks you use to configure the **Network** and **Device** tabs on Panorama. You can use templates to define interface and zone configurations, to manage the server profiles for logging and syslog access, or to define VPN configurations. Template stacks enable you to layer multiple templates and create a combined configuration. Template stacks simplify management because they allow you to define a common base configuration for all devices attached to the template stack and they enable you to layer templates to create a combined configuration. This enables you to define templates with location-specific or function-specific settings and then stack the templates in descending order of priority so that firewalls inherit the settings based on the order of the templates in the stack.

Templates and template stacks both support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, group IDs, and interfaces in your configurations. Template variables are inherited by the template stack and can be overridden to create a template stack variable. However, templates do not inherit variables defined in the template stack. When a variable is defined in the template or template stack and pushed to the firewall, the value defined for the variable is displayed on the firewall.

To accommodate firewalls that have unique settings, you can use templates to override the template stack configuration. Or you can push a broader, common base configuration and then override certain pushed settings with firewall-specific values on individual firewalls. When you override a setting on the firewall, the firewall saves that setting to its local configuration and Panorama no longer manages the setting.

When you define a template stack, consider assigning firewalls that are the same hardware model and require access to similar network resources, such as gateways and syslog servers. Grouping enables you to avoid the redundancy of adding every setting to every template stack. The following figure shows an example configuration in which you assign data center firewalls in the Asia-Pacific (APAC) region to a stack with global settings, one template with APAC-specific settings, and one template with data center-specific settings. To manage firewalls in an APAC branch office, you then can re-use the global and APAC-specific templates by adding them to another stack that includes a template with branch-specific settings. Templates in a stack have a configurable priority order that ensures Panorama pushes only one value for any duplicate setting. Panorama evaluates the templates listed in a stack configuration from top to bottom with higher templates having priority. The following figure also illustrates a data center stack in which the data center template has a higher priority than the global template: Panorama pushes the idle timeout value from the data center template and ignores the value from the global template.

©2016-2019, Palo Alto Networks, Inc.



Sample Questions

28. The Security policy for all of a customer's remote offices is the same, but because of different bandwidth requirements some offices can use a PA-220 and others require higher-end models (up to PA-5000 Series). If the firewalls for the offices are all managed centrally using Panorama, how might they share device groups and templates?
    A. same device group and same template stack
    B. same device group, different template stacks
    C. different device groups, same template stack
    D. different device groups and different template stacks
29. A firewall is assigned to a template stack of two templates. A setting common to each template has a different value. When Panorama pushes the template stack contents to the managed firewall, which setting will the firewall receive?
    A. value from the top template of the stack
    B. value from the bottom template in the stack
    C. value from the template designated as the parent
    D. value an admin selects from the two available values
30. Which two firewall settings are stored in Panorama templates?
    A. custom Application-ID signatures
    B. Server Profile for an external LDAP server
    C. services definitions
    D. DoS Protection Profiles
    E. traffic interface configurations

©2016-2019, Palo Alto Networks, Inc.

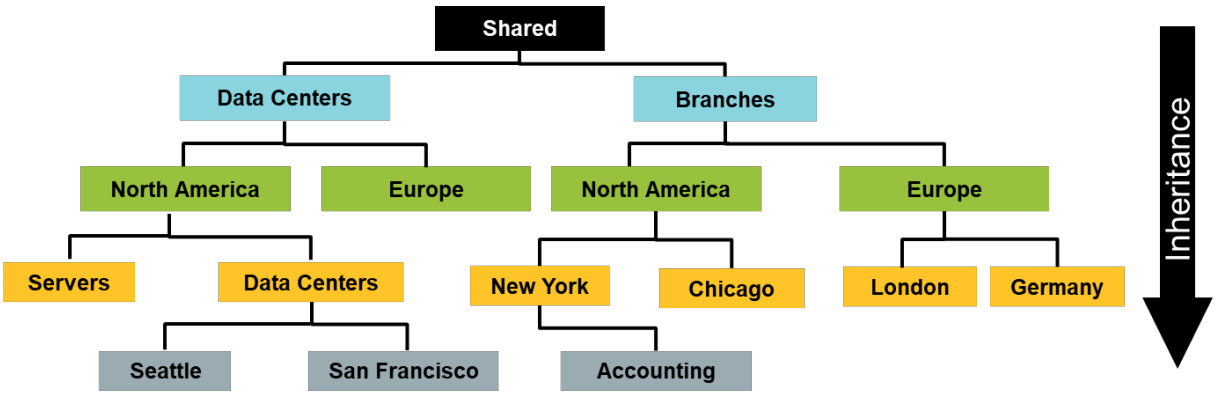
1.8 Identify how to use device group hierarchy for administering Palo Alto Networks firewalls as a scalable solution using Panorama

Device Groups

Before you can use Panorama effectively, you must group the firewalls in your network into logical units called device groups. A device group enables grouping based on network segmentation, geographic location, organizational function, or any other common aspect of firewalls that require similar policy configurations. You can use device groups to configure policy rules and the objects they reference. You can organize device group hierarchically, with shared rules and objects at the top and device group-specific rules and objects at subsequent levels. Organization enables you to create a hierarchy of rules that enforce how firewalls handle traffic. For example, you can define a set of shared rules as a corporate acceptable use policy. Then, to allow only regional offices to access peer-to-peer traffic such as BitTorrent, you can define a device group rule that Panorama pushes only to the regional offices (or define a shared security rule and target it to the regional offices).

You can create a device group hierarchy to nest device groups in a hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups (ancestors). At the top level, a device group can have child, grandchild, and great-grandchild device groups (descendants). All device groups inheriting settings from the Shared location, a container at the top of the hierarchy for configurations that are common to all device groups.

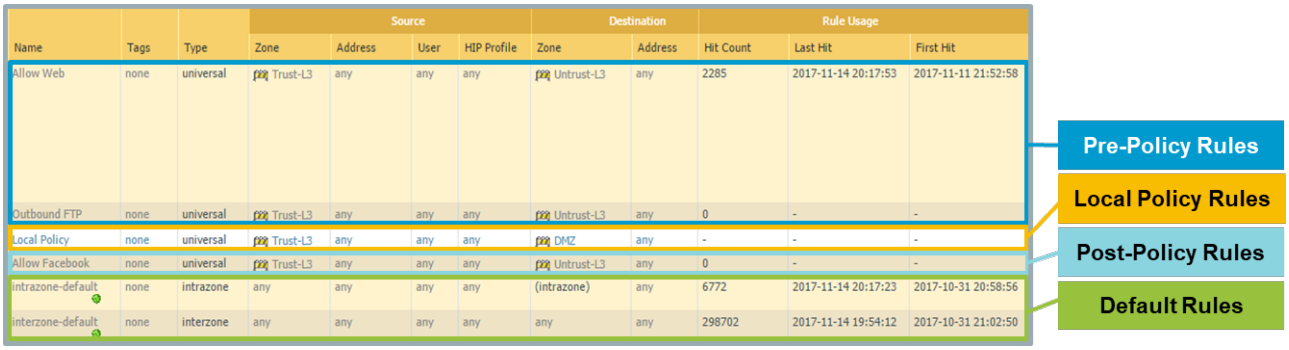
Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. For example, you could configure shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at lower levels. Without a hierarchy, you would have to configure both function-specific and location-specific settings for every device group in a single level under Shared.



Device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. A firewall evaluates policy rules by layer (shared, device group, and local) and by type (pre-rules, post-rules, and default rules) in the following order from top to bottom. When the firewall receives traffic, it performs the action defined in the first evaluated rule that matches the traffic and disregards all subsequent rules. To change the evaluation order for rules within a particular layer, type, and rule base (for example, shared Security pre-rules). Whether you view rules on a firewall or in

©2016-2019, Palo Alto Networks, Inc.

Panorama, the web interface displays them in evaluation order. All the shared, device group, and default rules that the firewall inherits from Panorama are shaded orange. Local firewall rules display between the pre-rules and post-rules. The rules with the orange shading in the following figure were provided by Panorama and can be managed only from Panorama. They are read-only in local firewall displays.



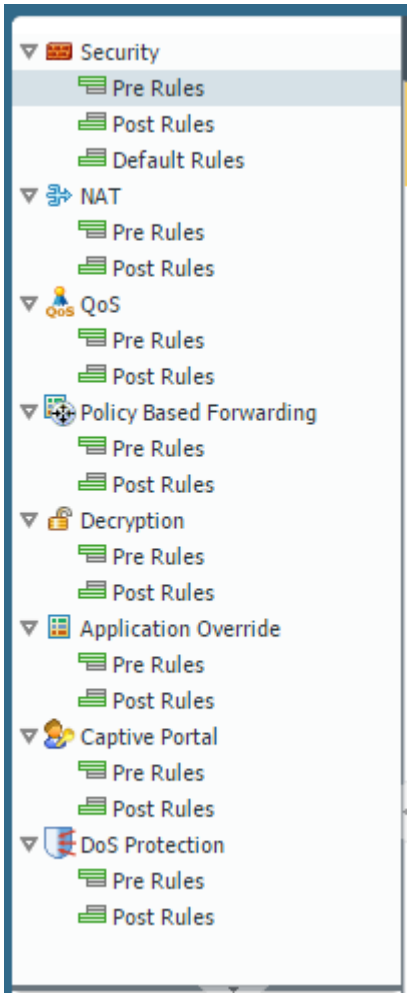
Objects are configuration elements that policy rules reference, for example: IP addresses, URL categories, Security Profiles, users, services, and applications. Rules of any type (pre-rules, post-rules, default rules, and rules locally defined on a firewall) and any rulebase (Security, NAT, QoS, Policy Based Forwarding, Decryption, Application Override, Captive Portal, and DoS Protection) can reference objects. You can reuse an object in any number of rules that have the same scope as that object in the device group hierarchy.

For example, if you add an object to the Shared location, all rules in the hierarchy can reference that shared object because all device groups inherit objects from Shared. If you add an object to a particular device group, only the rules in that device group and its descendant device groups can reference that device group object. If object values in a device group must differ from those inherited from an ancestor device group, you can override inherited object values. You also can revert to inherited object values at any time. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

When new policy rules are entered into a Panorama device group the device group and the pre or post designation must be decided. The pre and post designations are chosen through selection of the appropriate policy menu item, as shown in the following figure.

©2016-2019, Palo Alto Networks, Inc.

The image below details options for pre-position rules and post-position rules selections in Panorama



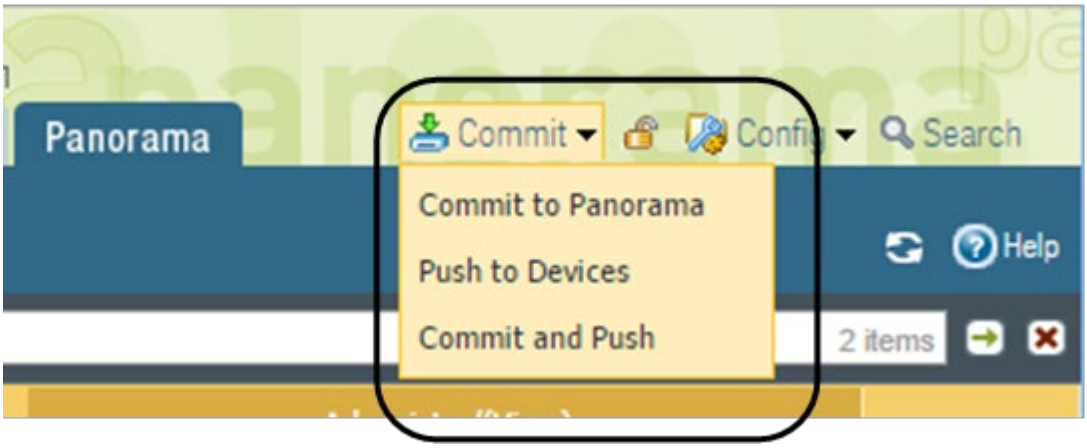
The *Panorama Administrator's Guide* can be found here:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin.html

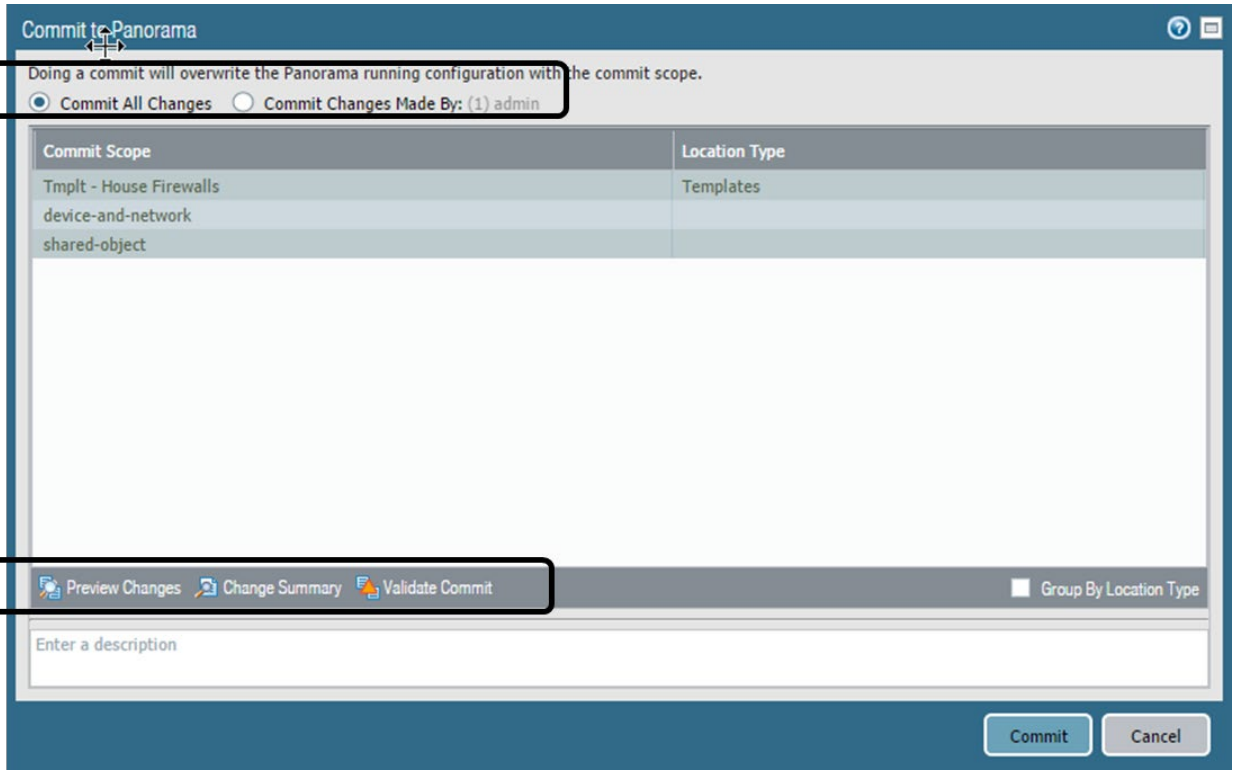
Committing Changes with Panorama

Panorama uses a similar commit concept to firewalls but uses a process with multiple phases. After changes have been made in Panorama data, users must first be committed to Panorama and then pushed to devices. Both processes provide methods to push partial data.

A commit to Panorama commits either the changes made by a chosen admin or all staged changes, as shown in the following figures.

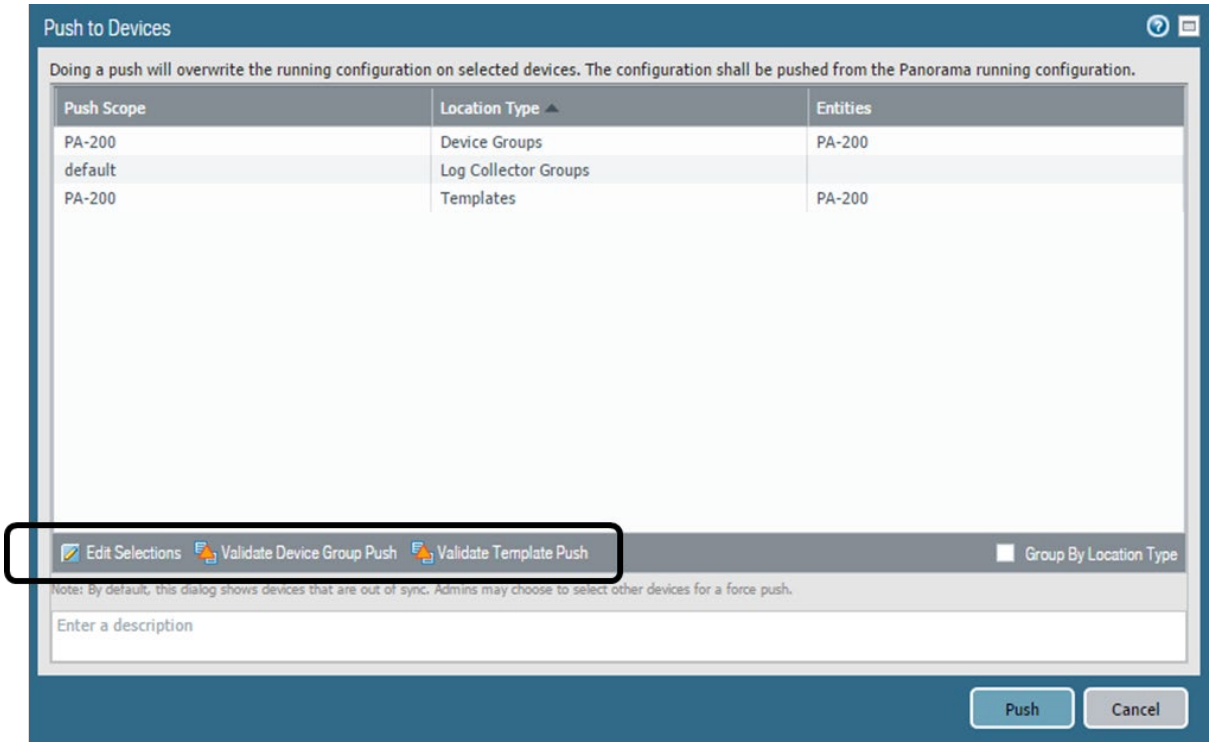
©2016-2019, Palo Alto Networks, Inc.



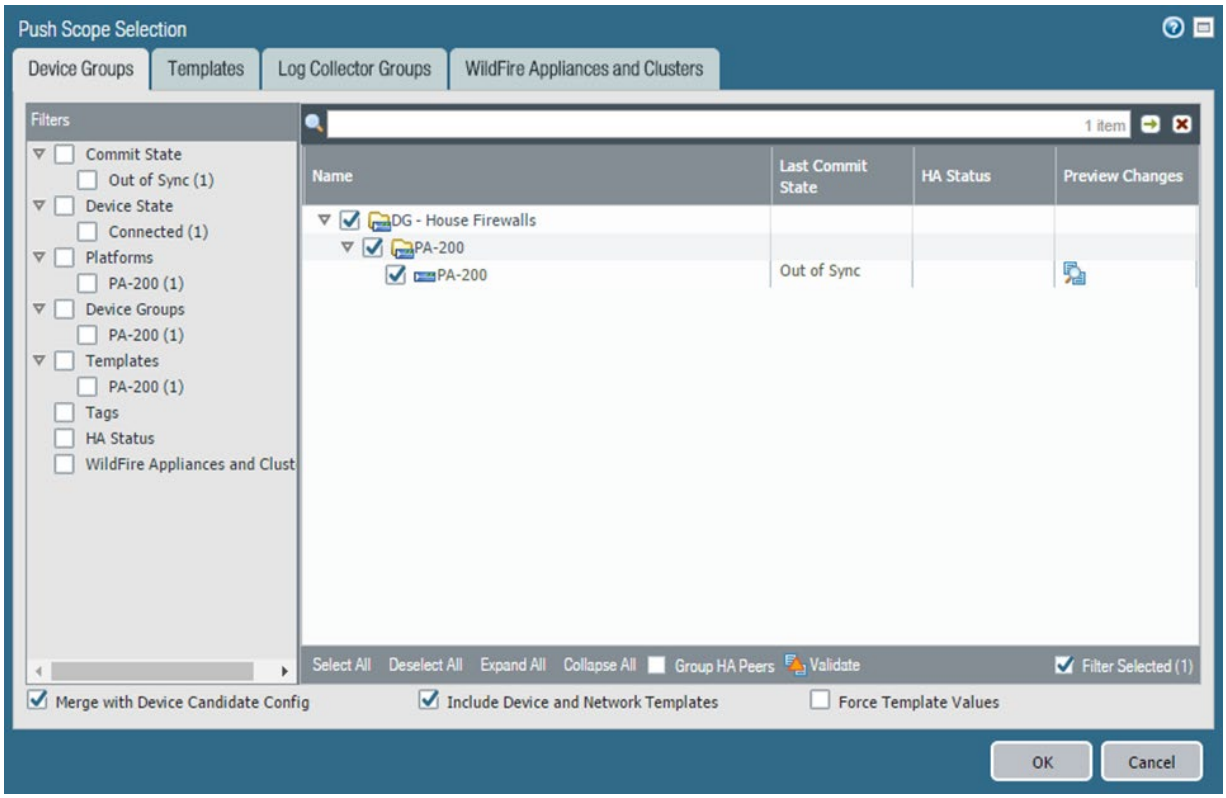


After changes are committed to Panorama, they are pushed to firewalls according to their assigned device groups and template stacks. This push process either can push all queued changes or be done selectively for specific device groups or template stacks. And specific firewalls can be chosen for the update.

©2016-2019, Palo Alto Networks, Inc.



Select **Edit Selections** at the bottom of the window to get a granular selection of the data to be pushed.



More information about the commit and push operations can be found here:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/panorama-commit-validation-and-preview-operations.html

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

31. Where in Panorama do you enter Security policy rules to ensure that your new rules will take precedence over locally entered rule?
    A. Security policy rules with a targeted firewall
    B. default rules section of Security policy rules
    C. pre-rules section of Security policy rules
    D. post-rules section of Security policy rules
32. How are changes made to Security policy rules seen in the Panorama web interface management window for a specific firewall configuration?
    A. log in to Panorama, clone the rule, modify the clone, and add a target firewall to the new rule
    B. select the rule, click the override button, and enter the changes
    C. create a new locally defined Security policy rule that is placed higher in the rule list than the rule to be overridden
    D. log in to Panorama and modify the original rule
33. Which three firewall settings are stored in Panorama device groups?
    A. User Identification configuration
    B. custom Application-ID signatures
    C. services definitions
    D. DoS Protection Profiles
    E. traffic interface configurations
    F. Zone Protection Profiles
    G. Server Profile for an external LDAP server

©2016-2019, Palo Alto Networks, Inc.

1.9 Identify planning considerations unique to deploying Palo Alto Networks firewalls in a public cloud

Virtual Firewalls

The VM-Series is a virtualized form factor of the Palo Alto Networks next-generation firewall that can be deployed in a range of public and private cloud computing environments. VM-Series firewalls run the same PAN-OS software as an appliance does, with the same features and capabilities. Each environment supports the full functionality of PAN-OS software with minor differences depending on the deployed cloud technology.

The VM-Series firewall is available in the VM-50 (Lite), VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, and VM-1000-HV.

All models can be deployed as guest virtual machines on VMware ESXi and vCloud Air, Citrix NetScaler SDX, KVM and KVM in OpenStack, and Microsoft Hyper-V. In the public cloud environments—Amazon Web Services, Azure, Google Cloud Platform, Oracle Cloud, Alibaba Cloud, and Cisco ACI—all models except the VM-50 are supported; on VMware NSX, only the VM-100, VM-200, VM-300, VM-500, and VM-1000-HV firewalls are supported. The software package (.xva, .ova, or .vhdx file) that is used to deploy the VM-Series firewall is common across all models.

All VM-Series firewalls require a capacity license to enable full firewall functionality. After you apply the capacity license on the VM-Series firewall, the model number and the associated capacities are implemented on the firewall. Capacity is defined in terms of the number of sessions, rules, security zones, address objects, IPsec VPN tunnels, and SSL VPN tunnels that the VM-Series firewall is optimized to handle. To make sure that you purchase the correct model for your network requirements, use the following table to learn the maximum capacity for each model and the capacity differences by model:

MODEL	SESSIONS	SECURITY RULES	DYNAMIC IP ADDRESSES	SECURITY ZONES	IPSEC VPN TUNNELS	SSL VPN TUNNELS
VM-50	50,000	• 250 • 200 in Lite mode	1,000	15	• 250 • 25 in Lite mode	• 250 • 25 in Lite mode
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

©2016-2019, Palo Alto Networks, Inc.

The standard VM-50 is the smallest model of the VM-Series and requires more resources than are available in some environments. The VM-50 Lite mode provides an alternative for environments where hardware resources are constrained. The VM-50 Lite requires 4.5GB of memory instead of the 5.5GB required by the standard VM-50. The VM-50 Lite uses the same license as the standard VM-50 but comes up in Lite mode when allocated 4.5GB of RAM.

Public Clouds

The virtual firewalls can be found in the public cloud marketplaces. Most public cloud marketplaces are populated with three virtual firewall choices that differ in their license requirements. A Bring Your Own License (BYOL) version is an unlicensed VM-Series firewall requiring the customer to provide their separately purchased capacity code and feature licenses after provisioning. The VM-Series Bundle 1 and 2 both are prelicensed versions of VM-300s. Bundle 1 is prelicensed for Threat Prevention only. Bundle 2 is pre-licensed for Threat Prevention, WildFire, URL Filtering, and GlobalProtect. Bundle 1 and 2 versions of the VM-300 incur a usage charge per hour of operation paid to the cloud vendor. The BYOL configuration contains no premium rates above the costs of the component cloud resources.

These pre-configured VM-Series firewalls provided by the cloud vendor application stores usually consist of three interfaces: one for management and one each for trusted and untrusted network traffic connections. Most cloud deployments provide a way to modify the configuration through addition of more interface connections subjected to the methods and capacities of the cloud vendor.

Each VM-Series virtual firewall has a VM-Series Plugin for the cloud vendor that implements certain functionality such as High Availability. See the deployment documentation specific to your cloud vendor for specific information:
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment.html

Sample Questions

34. Which two types of firewall interfaces are most likely to be supported in public cloud deployments?
    A. tap
    B. virtual wire
    C. Layer 3
    D. tunnel
    E. aggregate Ethernet
35. Where is the VM-Series virtual firewall appliance for public cloud deployments found?
    A. Palo Alto Networks Support Portal
    B. cloud vendor's "Solution Marketplace"
    C. Using the download link supplied on the same site as the license server
    D. Palo Alto Networks Product Download portal

©2016-2019, Palo Alto Networks, Inc.

1.10 Identify planning considerations unique to deploying Palo Alto Networks firewalls in a hybrid cloud

Hybrid Cloud

Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. The VM-Series firewall described in the previous section provides a fully featured next-generation firewall solution for cloud deployments in both environments.

Public and private cloud deployments each have their own design and deployment considerations (see the related sections in this guide) that must be considered individually. Regardless of the type of deployed environment, centralized monitoring, reporting, and management must be considered. The Panorama management solution can be deployed in either type of cloud and can manage across cloud boundaries if required communication channels are implemented.

Connectivity Considerations

Firewalls and Panorama each have connectivity requirements to reach outside services such as WildFire and to consume updates such as dynamic updates. When Panorama is used to manage firewalls, the devices must have a compatible communication channel between them. Hybrid deployments do not add any unique communication requirements of their own; each environment must be engineered to provide appropriate connectivity through its virtual networking environments as required. Engineering might include the use of the firewall to connect cloud environments with any required routing responsibility.

Site-to-site VPNs often are used to interconnect cloud-based virtual networks. The Palo Alto Networks firewalls can act as endpoints for these VPN connections and are subjected to VPN design and configuration considerations (see the VPN section in this guide).

©2016-2019, Palo Alto Networks, Inc.

1.11 Identify planning considerations unique to deploying Palo Alto Networks firewalls in a private cloud

Private Clouds

The VM-Series virtual firewall runs on the private cloud technologies listed in the previous section. In these cases, a compatible virtual appliance (OVA-format) is downloaded from the Palo Alto Networks Support Portal, uploaded to the cloud, and deployed and configured according to their requirements. These virtual firewalls are unlicensed and require both a capacity code and that feature licenses be applied after installation.

Specific information about private cloud deployments can be found here:
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment.html

Sample Questions

36. A private cloud has 20 VLANs spread over five ESXi hypervisors, managed by a single vCenter. How many firewall VMs are needed to implement microsegmentation?
    A. one
    B. four
    C. five
    D. 20
37. When you deploy the Palo Alto Networks NGFW on NSX, packets coming to an application VM from VMs running on different hardware go through which modules?
    A. network, vSwitch, NSX firewall, Palo Alto Networks NGFW, application VM
    B. network, vSwitch, Palo Alto Networks NGFW, NSX firewall, application VM
    C. network, vSwitch, NSX firewall, Palo Alto Networks NGFW, NSX firewall, application VM
    D. vSwitch, network, Palo Alto Networks NGFW, NSX firewall, application VM
38. Which option shows the interface types that ESXi supports in the VM-Series firewalls?
    A. tap, Layer 2, Layer 3, virtual wire
    B. Layer 3 only
    C. tap, Layer 2, Layer 3
    D. Layer 3, virtual wire

©2016-2019, Palo Alto Networks, Inc.

1.12 Identify methods for authorization, authentication, and device administration

Administrative Accounts and Roles

Administrators can configure, manage, and monitor Palo Alto Networks firewalls and Panorama using the web interface, CLI, and XML API management interface. You can customize role-based administrative access to the management interfaces to delegate specific tasks or permissions to certain administrators.

Administrative accounts specify roles and authentication methods for the administrators of Palo Alto Networks firewalls and Panorama. Each device has a predefined default administrative account (admin) that provides full read-write access (also known as superuser access) to the firewall. Other administrative accounts can be created as needed.

You configure administrator accounts based on the security requirements of your organization, any existing authentication services that your network uses, and the required administrative roles. A role defines the type of system access that is available to an administrator. You can define and restrict access as broadly or granularly as required, depending on the security requirements of your organization. For example, you might decide that a data center administrator can have access to all device and networking configurations, but a security administrator can control only Security policy definitions, while other key individuals can have limited CLI or XML API access. The role types are:

- Dynamic Roles: These are built-in roles that provide access to Panorama and managed firewalls. After new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. The following table lists the access privileges associated with dynamic roles.

DYNAMIC ROLE	PRIVILEGES
Superuser	Full read-write access to Panorama
Superuser (read-only)	Read-only access to Panorama
Panorama administrator	Full access to Panorama except for the following actions: • Create, modify, or delete Panorama or firewall administrators and roles. • Export, validate, revert, save, load, or import a configuration in the **Device > Setup > Operations** page. • Configure **Scheduled Config Export** functionality in the **Panorama** tab.

- Admin Role Profiles: To provide more granular access control over the functional areas of the web interface, CLI, and XML API, you can create custom roles. After new features are added to the product, you must update the roles with corresponding access privileges: Panorama does not automatically add new features to custom role definitions. You select one of the following profile types when you Configure an Admin Role Profile.

©2016-2019, Palo Alto Networks, Inc.

ADMIN ROLE PROFILE	DESCRIPTION
Panorama	For these roles, you can assign read-write access, read-only access, or no access to all the Panorama features that are available to the superuser dynamic role except the management of Panorama administrators and Panorama roles. For the latter two features, you can assign read-only access or no access, but you cannot assign read-write access. An example use of a Panorama role would be for security administrators who require access to security policy definitions, logs, and reports on Panorama.

Authentication

Authentication is a method for protecting services and applications by verifying the identities of users so that only legitimate users have access. Several firewall and Panorama features require authentication. Administrators authenticate to access the web interface, CLI, or XML API of the firewall and Panorama. End users authenticate through Captive Portal or GlobalProtect to access various services and applications. You can choose from several authentication services to protect your network and to accommodate your existing security infrastructure while ensuring a smooth user experience.

If you have a public key infrastructure, you can deploy certificates to enable authentication without users having to manually respond to login challenges. Alternatively, or in addition to certificates, you can implement interactive authentication, which requires users to authenticate using one or more methods.

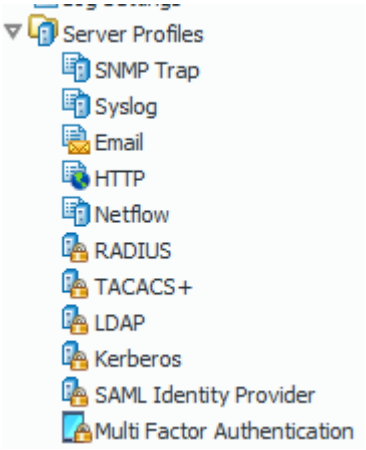
Supported authentication types include:

- Multi-factor
- SAML
- Single sign-on
- Kerberos
- TACACS+
- RADIUS
- LDAP
- Local

A complete discussion of these authentication types can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication.html

©2016-2019, Palo Alto Networks, Inc.

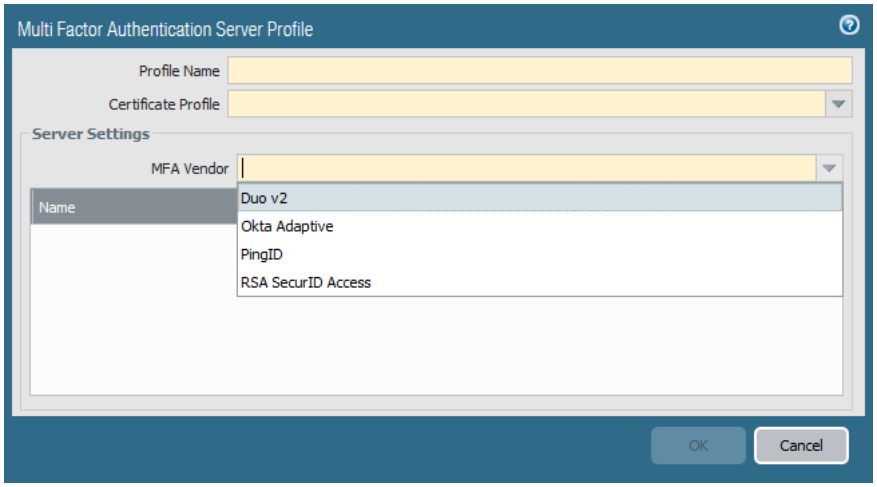
When user or administrative access is configured, one or more authentication methods must be specified. A user/administrator definition typically requires an Authentication Profile that captures the desired authentication method. When more than one is desired, you can instead use an Authentication Sequence, which is a list of Authentication Profiles. The first profile will be accessed. If it is not available, the next option will be tried. An Authentication Profile specifies a single Server Profile. Authentication Profiles comprise an ordered list of Server Profiles that contain specific configuration and access information to the external authentication service.



Detailed information about creating Authentication Profiles and sequences can be found here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence.html

Special Note About Multi-Factor Authentication

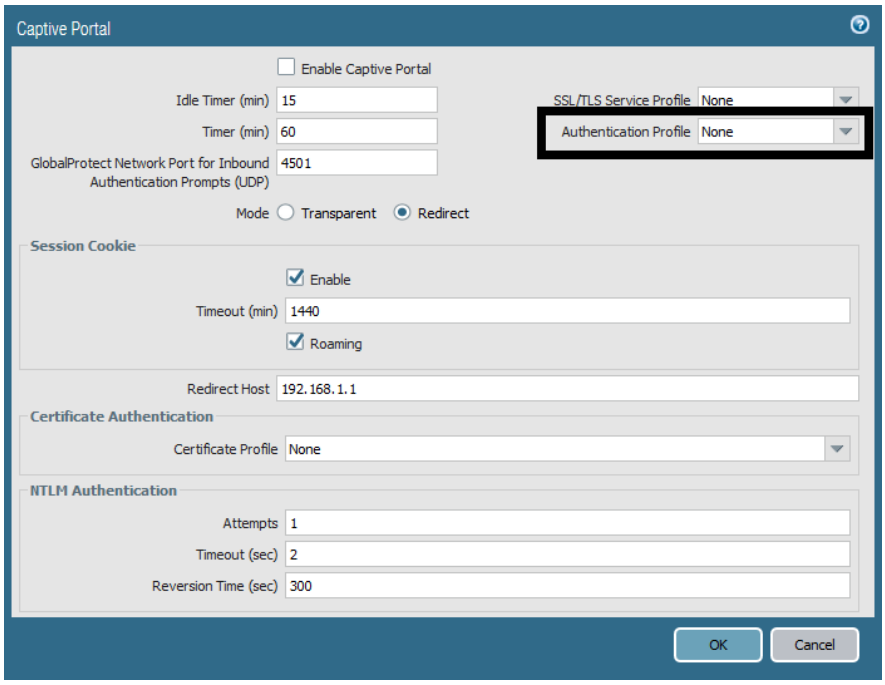
Palo Alto Networks firewalls support multi-factor authentication. A Multi-Factor Authentication Server Profile is used to integrate an external third-party MFA solution. MFA factors that the firewall supports include Push, Short Message Service (SMS), voice, and one-time password (OTP) authentication. This profile identifies the specific product with its configuration information.



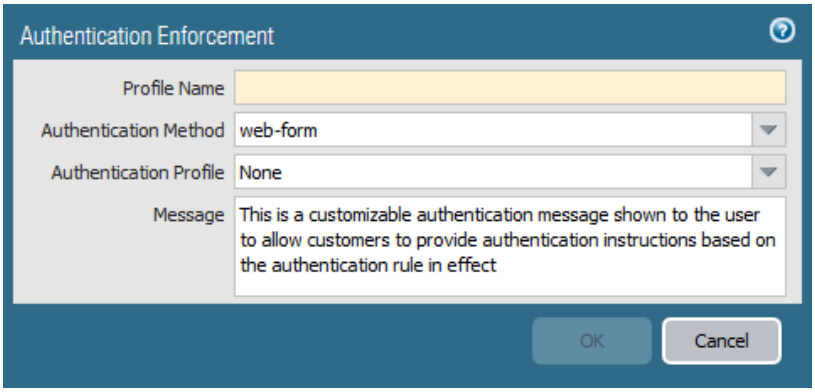
The Multi-Factor Authentication Server Profile shown can be a part of multiple challenges that a user must respond to. For example, you can force users to enter a login password and then enter a verification code that they receive by phone before they can access critical financial documents.

©2016-2019, Palo Alto Networks, Inc.

The firewall challenges a user with a Captive Portal. Captive Portal configuration includes an Authentication Profile selected for base configuration that represents the first challenge a user must negotiate.



An Authentication Enforcement policy then is used to join the MFA product as a second required authentication. Selection of the MFA product's Authentication Profile adds it as a second authentication requirement for users.



Configuration of base Captive Portal is discussed here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal/configure-captive-portal

The complete MFA implementation process is discussed here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-multi-factor-authentication

Panorama Access Domains

©2016-2019, Palo Alto Networks, Inc.

Panorama access domains control the access that device group and template administrators have to specific device groups (to manage policies and objects), to templates (to manage network and device settings), and to the web interface of managed firewalls (through context switching). You can define up to 4,000 access domains and manage them locally or by using RADIUS Vendor-Specific Attributes (VSAs), TACACS+ VSAs, or SAML attributes.

More information about access domains can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/panorama-web-interface/panorama-access-domains

Sample Questions

39. To configure multi-factor authentication for users accessing services through the firewall, which three configuration pieces need to be addressed?
    A. GlobalProtect Portal
    B. Captive Portal
    C. Authentication Enforcement Profile
    D. Authentication Profile
    E. Response pages
40. Which two configuration components can be used for external user authentication in the firewall?
    A. Local User Database
    B. Server Profiles
    C. VM Information source
    D. admin roles
    E. Authentication policy rules
41. Which two firewall functions are reserved only for admins assigned the superuser dynamic role?
    A. certificate management
    B. managing firewall admin accounts
    C. editing the management interface settings
    D. creating virtual systems within a firewall
    E. accessing the configuration mode of the CLI

©2016-2019, Palo Alto Networks, Inc.

1.13 Identify the methods of certificate creation on the firewall

Certificate Background

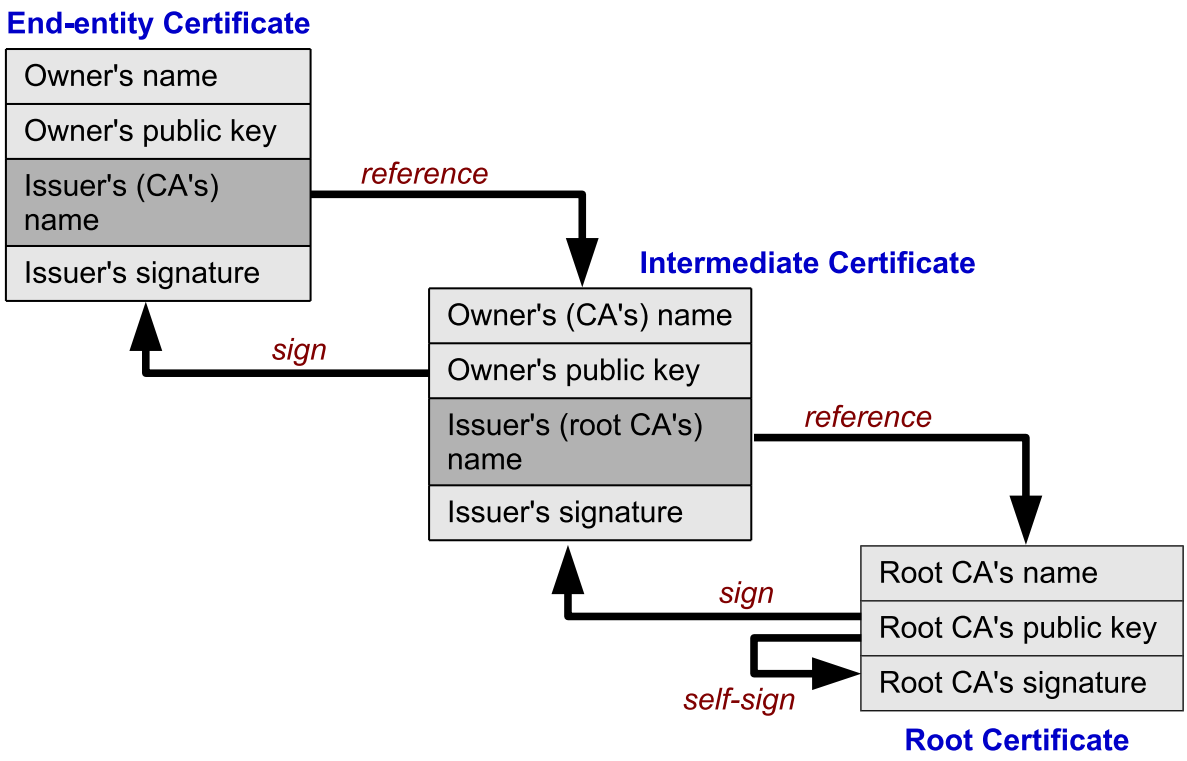
In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid and the software examining the certificate trusts the issuer, then the software can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject typically is a person or organization. However, in Transport Layer Security (TLS) a certificate's subject typically is a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.

In a typical public key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. Certificate authorities also can be created and managed by individuals and organizations requiring certificates for internal use.

A CA is responsible for signing certificates. These certificates act as an introduction between two parties, which means that a CA acts as a trusted third party. A CA processes requests from people or organizations requesting certificates (called subscribers), verifies the information, and potentially signs an end-entity certificate based on that information. To perform this role effectively, a CA needs to have one or more broadly trusted root certificates or intermediate certificates and the corresponding private keys. CAs may achieve this broad trust by having their root certificates included in popular software, or by obtaining a cross-signature from another CA delegating trust.

A receiving entity is responsible for validating the information contained in a certificate presented to it. Among the potential verification tests is a validation that the certificate was issued by the issuing CA information contained in the certificate. This verification requires the CA’s signing key contained in its Root Certificate used to sign all issued certificates. This certificate must be locally available to the receiving entity to run the validation test. These CA Root Certificates often are kept in locally stored certificate caches in the hosting OS or a browser or program-managed certificate cache.

©2016-2019, Palo Alto Networks, Inc.



Certificate authorities also are responsible for maintaining up-to-date revocation information about certificates they have issued that indicate whether certificates still are valid. They provide this information through Online Certificate Status Protocol (OCSP) and/or certificate revocation lists (CRLs).

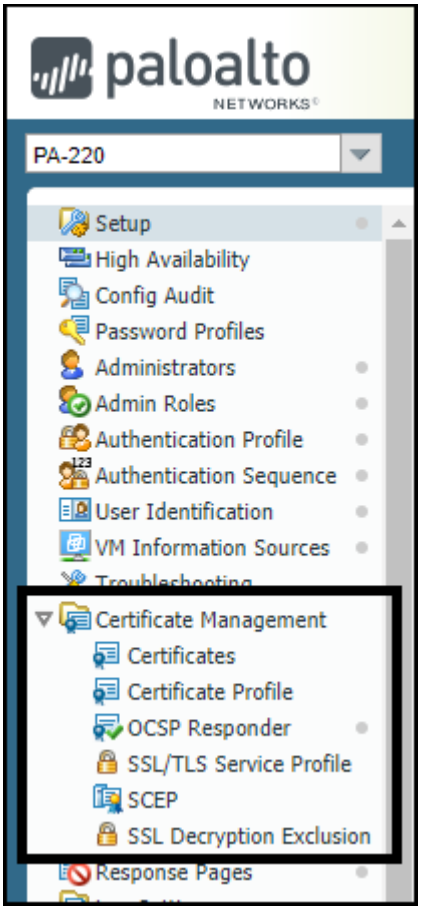
Certificates on the Firewall

Encryption and identity verification and their required certificates are used for many functions within the Palo Alto Networks firewall and Panorama. A partial list includes:

- SSL/TLS decryption
- Management (MGT) interface user authentication
- GlobalProtect
- Portal authentication
- Gateway authentication
- Mobile Security Manager authentication
- Captive Portal user authentication
- IPsec VPN IKE authentication
- High Availability authentication
- Secure syslog authentication

Because of this extensive use, certificate management functions are provided within the firewall's management web interface:

©2016-2019, Palo Alto Networks, Inc.

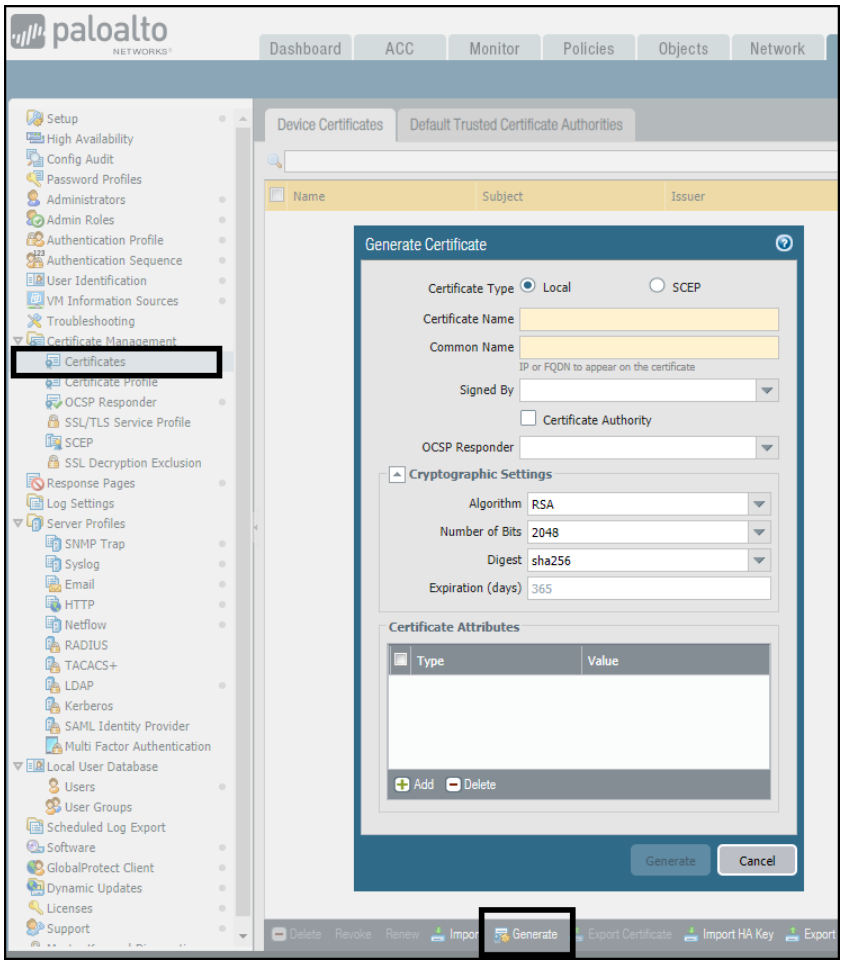


Certificate Creation and Import

The firewall's certificate management capability provides methods to create and manage certificates as a certificate authority and to import and manage certificates created by an external certificate authority. This includes their associate public and private keys. If your enterprise has a Simple Certificate Enrollment Protocol (SCEP) server, you can configure an SCEP Profile to automate the generation and distribution of unique client certificates. SCEP operation is dynamic in the sense that the enterprise PKI generates a user-specific certificate when the SCEP client requests it and sends the certificate to the SCEP client. The SCEP client then transparently deploys the certificate to the client device.

©2016-2019, Palo Alto Networks, Inc.

Basic required information must be provided when a new certificate is created directly on the firewall:

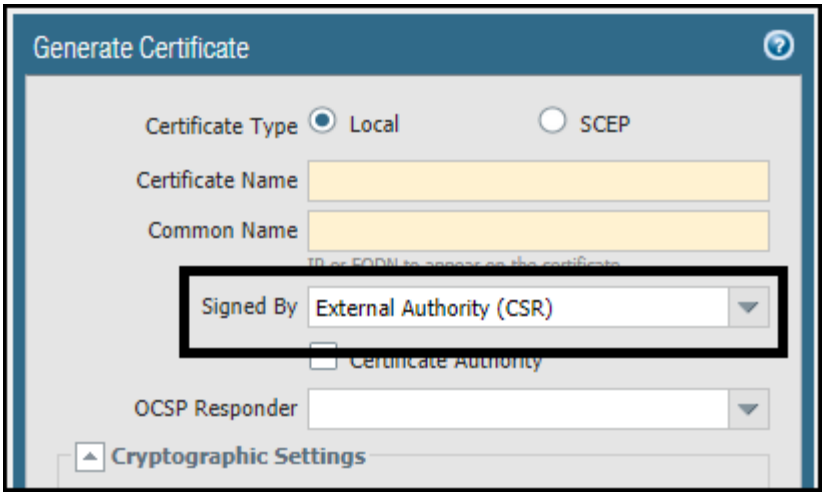


Included in this certificate information are settings that choose whether this certificate is self-signed or signed by another certificate stored in the firewall (the **Signed By** field). The **Certificate Authority** check box determines whether this certificate will have the rights to sign other certificates.

Once the appropriate data is entered and the **Generate** button is pressed, a new certificate will be created with its private and public keys and be added to the firewall's storage. The resultant certificate then can be exported with or without the private key for external use.

In cases where a certificate needs to be generated by an external CA, a certificate signing request (CSR) file can be created on the firewall that is exported and transferred to the CA. This file contains the required information for certificate creation. Select the **External Authority** option in the **Signed By** field to trigger this generation.

©2016-2019, Palo Alto Networks, Inc.



This creates the CSR file and adds it to firewall storage, from where it can be exported and transmitted to the external CA. The certificate generated by the CA can be imported into the firewall, at which point the CSR file is replaced by the certificate in the firewall's certificate storage and listings.

More details about certificate management can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/certificate-management.html

Sample Questions

42. A Palo Alto Networks firewall can obtain a certificate for its internal use through which three methods?
    A. importing a certificate file generated by an external CA
    B. referencing an externally stored certificate by a URL configured in an SSL/TLS Service Profile
    C. generating a certificate directly by manually entering certificate data
    D. obtaining a certificate from an SCEP server using an SCEP profile
    E. importing a certificate from an external CA by using an Authentication Profile
43. Which input simplifies a certificate request from an external CA?
    A. certificate signing request
    B. Certificate signing request with a separate private key
    C. certificate signing request with a separate public key
    D. certificate signing request with a separate public key and private key
44. Which two resources must also be available to successfully run certificate validation tests on a certificate received from an external source?
    A. Root Certificate of the issuing CA
    B. public key for the received certificate
    C. OCSP connection address
    D. existing Certificate Profile that matches the received certificate's CA identity

©2016-2019, Palo Alto Networks, Inc.

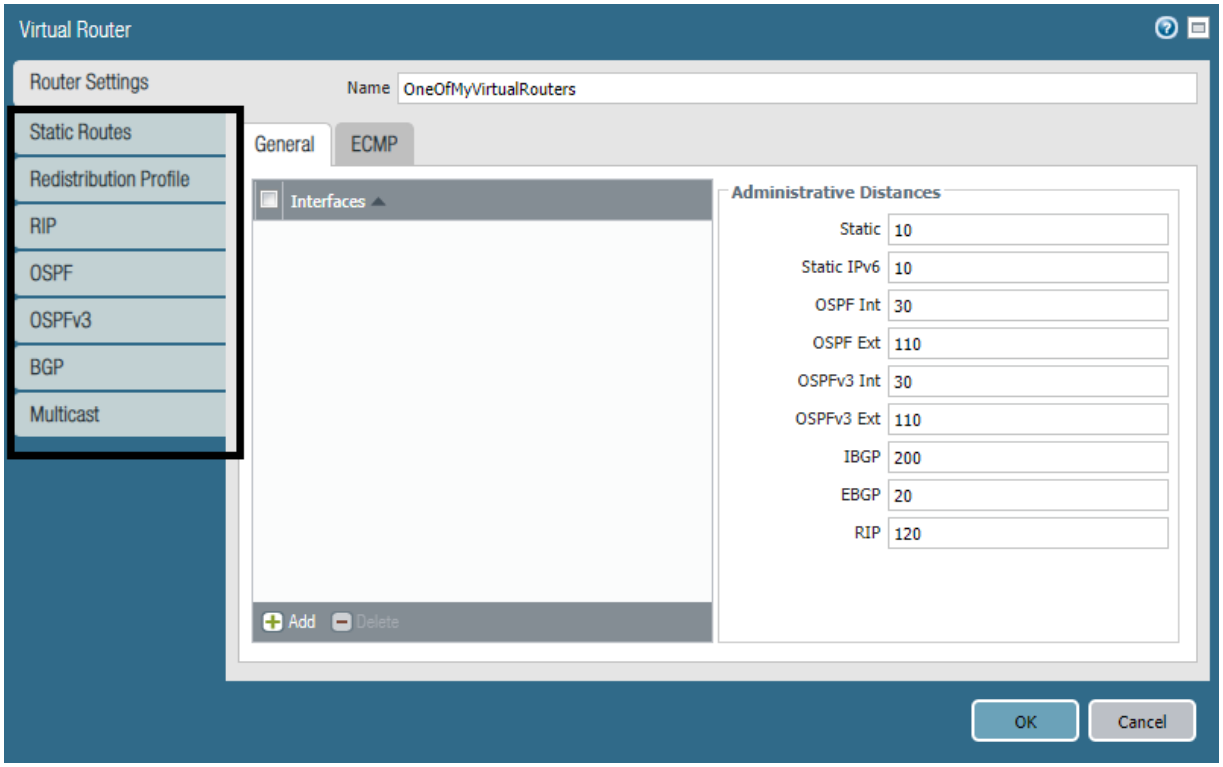
1.14 Identify options available in the firewall to support dynamic routing

Overview

All Palo Alto Networks firewalls provide a flexible networking architecture that includes support for dynamic routing, switching, and VPN connectivity, and enables you to deploy the firewall into nearly any networking environment. When you configure the Ethernet ports on your firewall, you can choose from Virtual Wire, Layer 2, or Layer 3 interface deployments. If you want to integrate into a variety of network segments, you can configure different types of interfaces on different ports. The firewalls also can participate in several routing protocols, including static routes. The dynamic routing protocols supported by the Palo Alto Networks firewalls are:

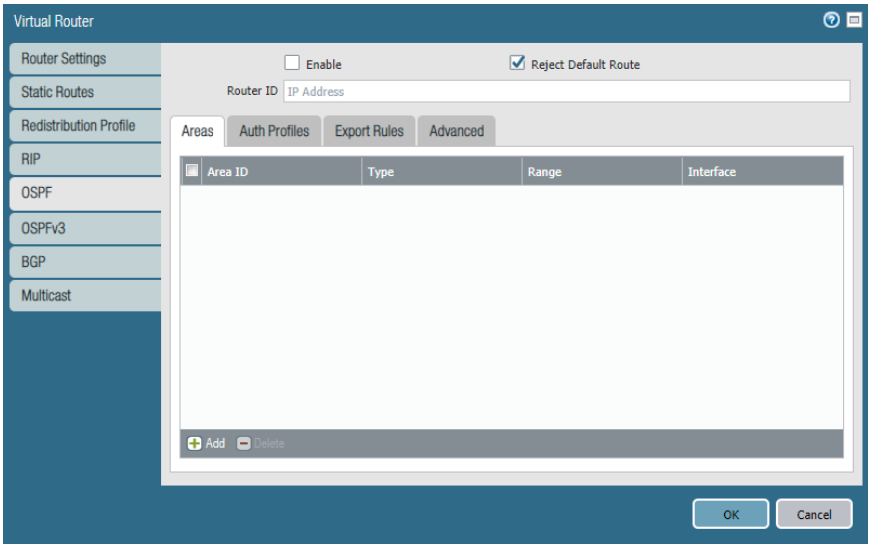
- RIP
- OSPF
- OSPFv3
- BGP
- Multicast

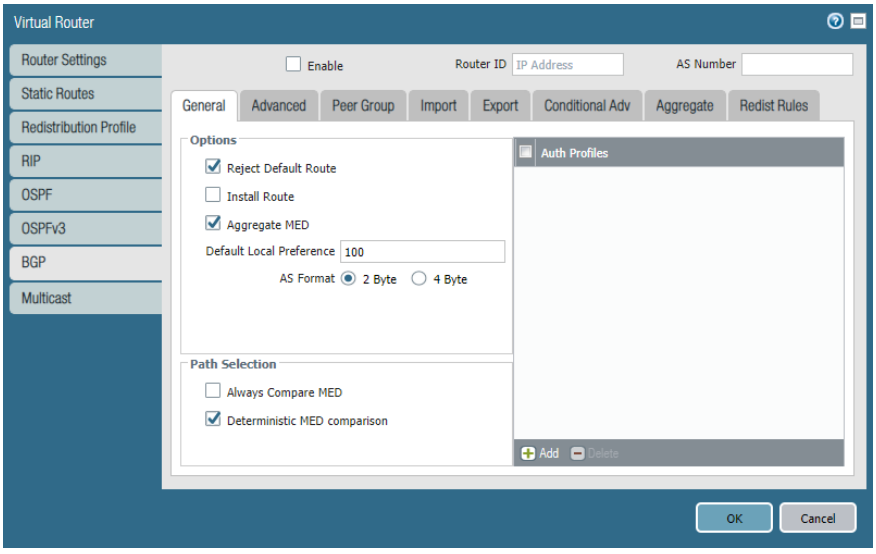
These routing protocols are implemented on TCP/IP networks and are supported as optional configurations in a firewall's virtual router.



Multiple router protocols can be enabled at the same time. Each routing protocol has its own configuration settings.

©2016-2019, Palo Alto Networks, Inc.





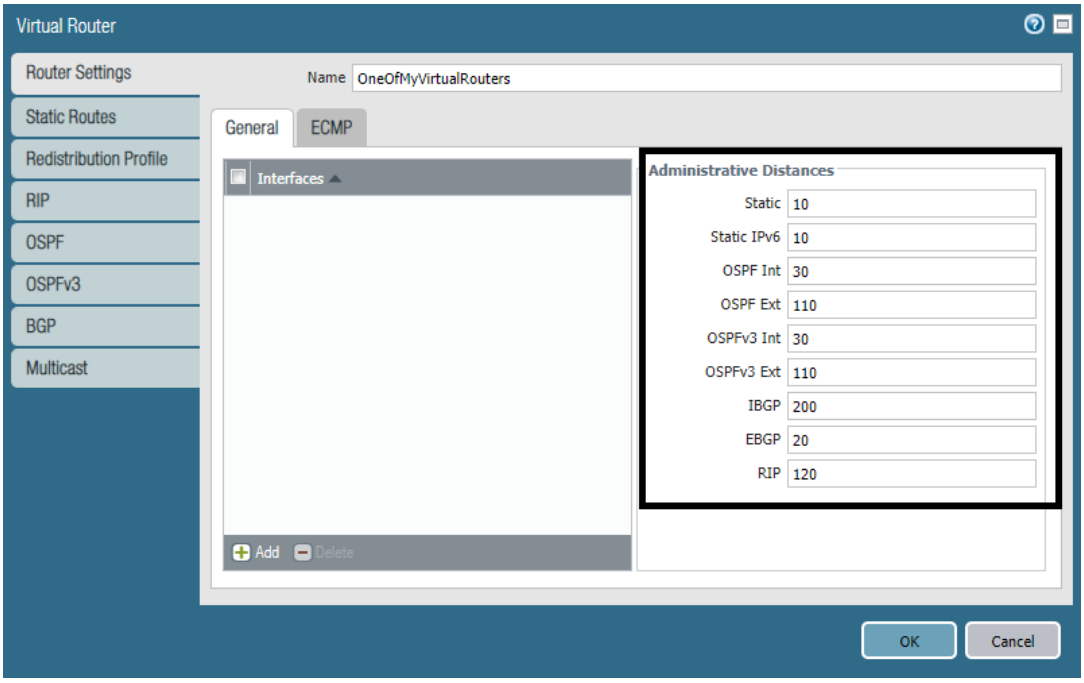
Each virtual router instance can be configured separately for dynamic routing, with each router maintaining separate routing tables (RIBs). Each router instance has a RIB and forwarding table (FIB) that are used during packet processing to identify the appropriate interface for packet egress.

A virtual router can share routes between router protocols using Redistribution Profiles. You can redistribute IPv4 or IPv6 BGP, connected, or static routes into the OSPF RIB and redistribute OSPFv3, connected, or static routes into the BGP RIB.

Administrative Distance

Within the virtual router configuration, set administrative distances for types of routes as required for your network. A virtual router that has two or more different routes to the same destination from different routing protocols uses administrative distance to choose the best path from different routing protocols and static routes by preferring a lower distance.

©2016-2019, Palo Alto Networks, Inc.



Sample Questions

45. The firewall uses which information to determine which interface to use for a packet's egress?
    A. manually configured static routes
    B. routing information base (RIB)
    C. appropriate Redistribution Profile
    D. ECMP destination monitoring results
46. A virtual router can use a Redistribution Profile to share routes between which routing protocols? (Choose three.)
    A. static routes
    B. IGRP
    C. RIP
    D. OSPF
    E. multicast
47. How does a firewall RIB with routes to the same destination in multiple router protocols determine the which route to use?
    A. according to the following precedence of route type: static, RIP, OSPF, BGP
    B. using the virtual router's FIB
    C. using the associated route's metric and choosing the lowest value
    D. using the route's administrative distance and choosing the lowest value

©2016-2019, Palo Alto Networks, Inc.

1.15 Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers

Resource Exhaustion

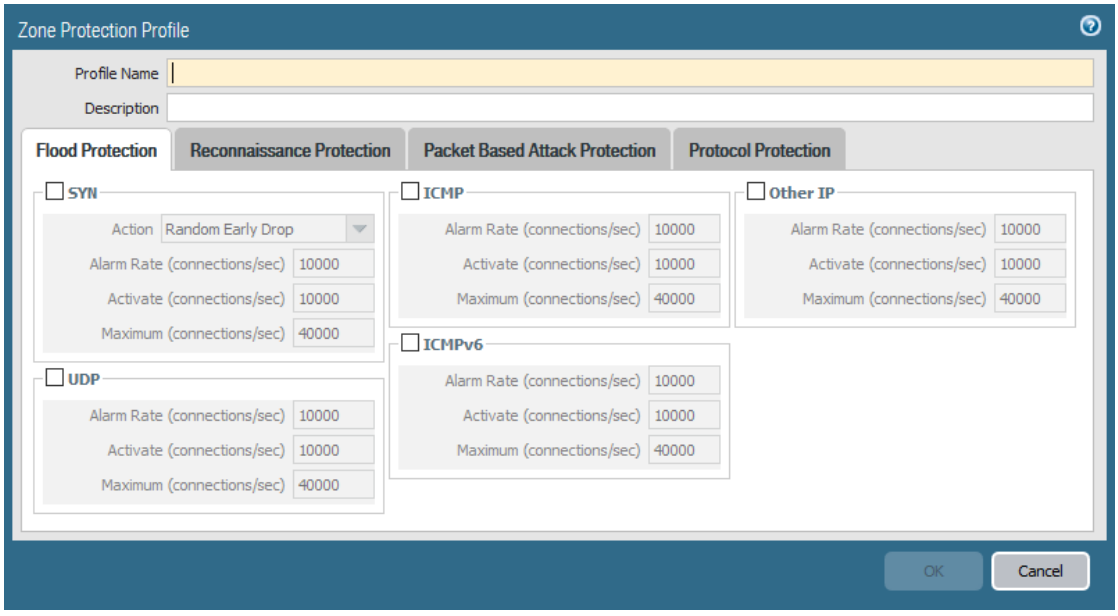
Port scans and floods are common causes of resource exhaustion at the interface and system level for protected devices and the firewall interfaces themselves. Although PAN-OS software does have powerful protections, none of them is turned on by default, which leaves a firewall exposed to these attacks until protections are configured. Palo Alto Networks provides two protection mechanisms for resource exhaustion caused by these attacks, Zone Protection Profiles and DoS Protection policies or profiles.

Zone Protection Profiles

Zone Protection Profiles defend the zone at the ingress zone edge against reconnaissance port scan and host sweep attacks, IP packet-based attacks, non-IP protocol attacks, and flood attacks by limiting the number of connections per second (CPS) of different packet types.

Zone design itself provides segmentation of networks, which magnifies the protection of Zone Protection Profiles. A discussion of zone design through the lens of protection can be found here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/zone-protection-and-dos-protection/how-do-zones-protect-the-network#iddd95afb5-16e3-491e-af0d-280511d3047c

Zone Protection Profiles provide a broad defense of the entire zone based on the aggregate traffic entering the zone, thus protecting against flood attacks and undesirable packet types and options. Zone Protection Profiles don't control traffic between zones, they control traffic only at the ingress zone. Zone Protection Profiles don't consider individual IP addresses because they apply to the aggregate traffic entering the zone (DoS Protection policy rules defend individual IP addresses in a zone). This protection is done early in the traffic processing flow, thus minimizing firewall resource use.



©2016-2019, Palo Alto Networks, Inc.

A complete description of Zone Protection Profiles and details for its configuration are here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection.html

Recommendations for Zone Protection Profile settings are here: https://live.paloaltonetworks.com/t5/Learning-Articles/Zone-Protection-Recommendations/ta-p/55850

DoS Protection Profile

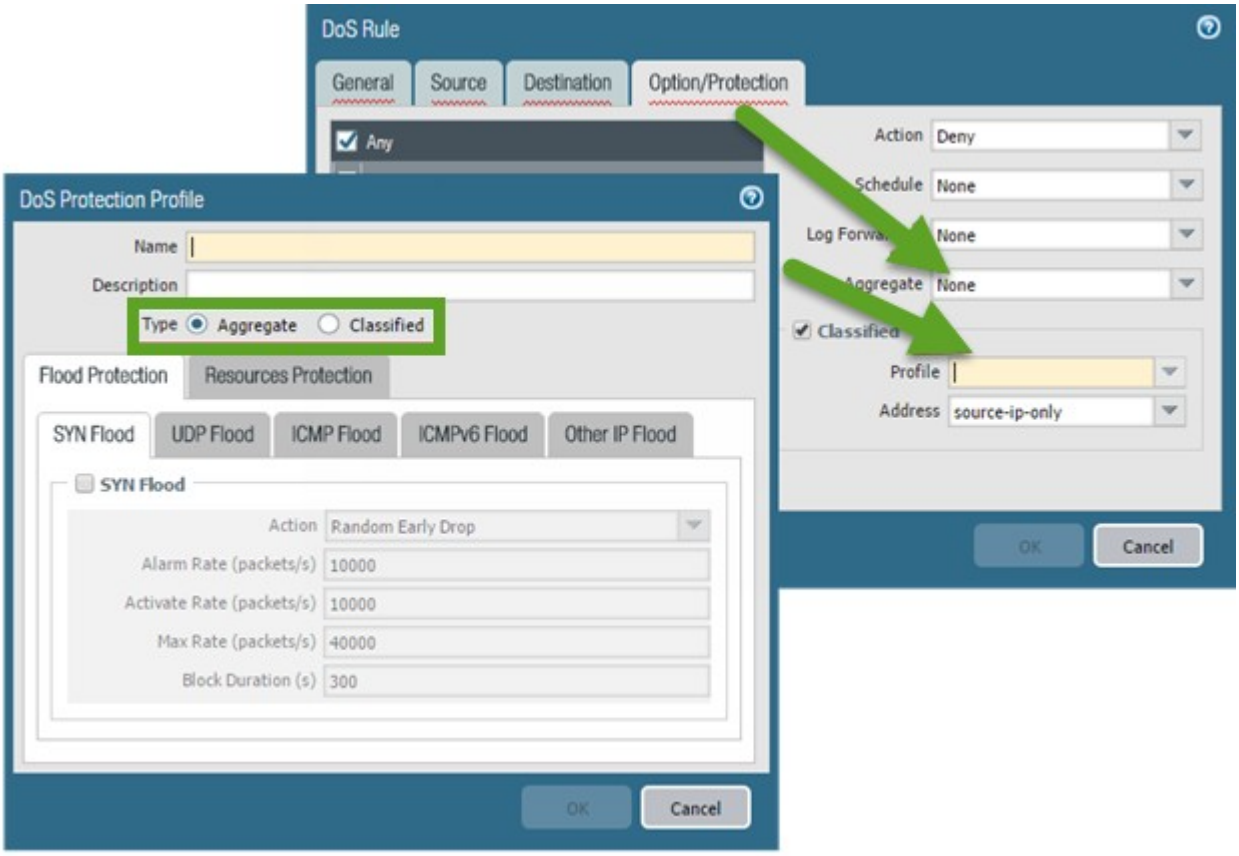
DoS Protection Profiles and DoS Protection policy rules combine to protect specific groups of critical resources and individual critical resources against session floods. Compared to Zone Protection Profiles, which protect entire zones from flood attacks, DoS protection provides granular defense for specific systems, especially critical systems that users access from the internet and often are attack targets, such as web servers and database servers. Apply both types of protection because if you apply only Zone Protection Profile, then a DoS attack that targets a particular system in the zone can succeed if the total CPS doesn't exceed the zone's **Activate** and **Maximum** rates.

DoS Protection is resource-intensive, so use it only for critical systems. As is the case with Zone Protection Profiles, DoS Protection Profiles specify flood thresholds. DoS Protection policy rules determine the devices, users, zones, and services to which DoS Profiles apply.

DoS Protection Profiles set the protection thresholds to provide DoS protection against flooding of new sessions for IP floods (CPS limits) to provide resource protection (maximum concurrent session limits for specified endpoints and resources) and to configure whether the profile applies to aggregate or classified traffic. DoS Protection policy rules control where to apply DoS protection and which action to take when traffic matches the criteria defined in the rule.

Unlike a Zone Protection Profile, which protects only the ingress zone, DoS Protection Profiles and policy rules can protect specific resources inside a zone and traffic flowing between different endpoints and areas. Unlike the case with a Zone Protection Profile, which supports only aggregate traffic, you can configure aggregate or classified DoS Protection Profiles and policy rules.

©2016-2019, Palo Alto Networks, Inc.



Differences Between DoS Protection and Zone Protection

A DoS Protection policy can be used to accomplish some of the same things a Zone Protection policy does, but there are a few key differences:

- A major difference is a DoS policy can be classified or aggregate. Zone Protection policies are aggregate.
- A classified profile allows the creation of a threshold that applies to a single source IP.

For example, a max session rate per IP can be created for all traffic matching the policy, then block that single IP address once the threshold is triggered.

- An Aggregate Profile allows the creation of a max session rate for all packets matching the policy. The threshold applies to a new session rate for all IPs combined. A triggered threshold would affect *all* traffic matching the policy.
- Zone Protection Policies allow the use of flood protection and can protect against port scanning and sweeps and packet-based attacks. A few examples are IP spoofing, fragments, overlapping segments, and reject tcp-non-syn.
- Zone Protection Profiles may have less performance impact because they are applied pre-session and don't engage the policy engine.

©2016-2019, Palo Alto Networks, Inc.

Specific implementation information for DoS policy and profiles can be found here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules

An exploration of DoS attacks and defending against them using Palo Alto Networks firewalls is here: https://live.paloaltonetworks.com/t5/Documentation-Articles/Understanding-DoS-Protection/ta-p/54562?attachment-id=1085

Sample Questions

48. For which two reasons are denial-of-service protections applied by zone?
    A. because denial-of-service protections are applied early in the processing, before much information is known about the connection but when the ingress interface already is known
    B. because denial-of-service protections are applied only when manually turned on to avoid quota overload (which would make denial of service easier)
    C. because denial-of-service protections can depend on only the zone, and never on port numbers or IP addresses
    D. because denial-of-service protections on a Layer 3 interface are different from the denial-of-service protections available on a Layer 2 interface, and interfaces on virtual wires
49. SYN flood protection provides flood protection from which protocol?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
50. To which two protocols does port scan reconnaissance protection apply?
    A. UDP
    B. TCP
    C. GRE
    D. ICMP
    E. IPX
51. In which two places do you configure flood protection?
    A. DoS Profile
    B. QoS Profile
    C. Zone Protection Profile
    D. SYN Profile
    E. XOFF Profile
52. Which two firewall features should be used to provide tailored DoS protection to a specific address?
    A. Zone Protection Profiles
    B. virtual routers
    C. Server Profiles
    D. DoS Protection policy rules
    E. DoS Protection Profiles

©2016-2019, Palo Alto Networks, Inc.

1.16 Identify decryption deployment strategies

Packet Visibility

The use of encryption for all network applications is growing at a rapid rate. When traffic is encrypted, the Palo Alto Networks firewall loses visibility into packet contents, thus making Content-ID impossible. Because of this, malware might be able to pass unchallenged to an endpoint, at which point it is decrypted and able to attack. Decryption policies maximize the firewall's visibility into packet content to allow for content inspection.

Decryption

The Secure Sockets Layer (SSL) and Secure Shell (SSH) encryption protocols secure traffic between two entities, such as a web server and a client. SSL and SSH encapsulate traffic, encrypting data so that it is meaningless to entities other than the client and server with the certificates to affirm trust between the devices and the keys to decode the data. Decrypt SSL and SSH traffic to:

- Prevent malware concealed as encrypted traffic from being introduced into your network. For example, an attacker compromises a website that uses SSL encryption. Employees visit that website and unknowingly download an exploit or malware. The malware then uses the infected employee endpoint to move laterally through the network and compromise other systems.
- Prevent sensitive information from moving outside the network
- Ensure the appropriate applications are running on a secure network
- Selectively decrypt traffic; for example, create a Decryption policy and profile to exclude traffic for financial or healthcare sites from decryption

Palo Alto Networks firewall decryption is policy-based, and can decrypt, inspect, and control inbound and outbound SSL and SSH connections. A Decryption policy enables you to specify traffic to decrypt by destination, source, service, or URL category, and to block, restrict, or forward the specified traffic according to the security settings in the associated Decryption Profile. A Decryption Profile controls SSL protocols, certificate verification, and failure checks to prevent traffic that uses weak algorithms or unsupported modes from accessing the network. The firewall uses certificates and keys to decrypt traffic to plaintext, and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, WildFire, and File-Blocking Profiles. After decrypting and inspecting traffic, the firewall re-encrypts the plaintext traffic as it exits the firewall to ensure privacy and security.

The firewall provides three types of Decryption policy rules: SSL Forward Proxy to control outbound SSL traffic, SSL Inbound Inspection to control inbound SSL traffic, and SSH Proxy to control tunneled SSH traffic. You can attach a Decryption Profile to a policy rule to apply granular access settings to traffic, such as checks for server certificates, unsupported modes, and failures.

SSL decryption (both forward proxy and inbound inspection) requires certificates to establish the firewall as a trusted third party, and to establish trust between a client and a server to secure an SSL/TLS connection. You also can use certificates when excluding servers from SSL decryption for technical reasons (the site breaks decryption for reasons such as certificate pinning, unsupported ciphers, or mutual authentication). SSH decryption does not require certificates.

©2016-2019, Palo Alto Networks, Inc.

A review of decryption concepts can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-concepts.html

A discussion of decryption best practices can be found here:
https://docs.paloaltonetworks.com/best-practices/9-0/decryption-best-practices

Decryption Broker

A firewall acting as a decryption broker uses dedicated decryption forwarding interfaces to send decrypted traffic to a security chain—a set of inline, third-party security appliances—for additional analysis. Two types of security chain networks are supported with a decryption broker (Layer 3 security chains and Transparent Bridge security chains), and you also can choose that the firewall direct traffic through the security chain unidirectionally or bidirectionally. A single firewall can distribute decrypted sessions among up to 64 security chains and can monitor security chains to ensure that they are effectively processing traffic.

A discussion of this capability is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts

Decryption Mirror

Palo Alto Networks firewalls can automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This option is available at no cost to middle and high-end firewalls that can automatically forward copies of decrypted traffic to external DLP products.

A description of this feature can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-concepts/decryption-mirroring.html

Keys and Certificates

Palo Alto Networks firewalls decrypt encrypted traffic by using keys to transform strings (passwords and shared secrets) from ciphertext to plaintext (decryption) and from plaintext back to ciphertext (re-encrypting traffic as it exits the device). Certificates are used to establish the firewall as a trusted third party and to create a secure connection. SSL decryption (both forward proxy and inbound inspection) requires certificates to establish trust between two entities to secure an SSL/TLS connection. Certificates also can be used when servers are excluded from SSL decryption. You can integrate a hardware security module (HSM) with a firewall to enable enhanced security for the private keys used in SSL Forward Proxy and SSL Inbound Inspection decryption.

Palo Alto Networks firewall decryption is policy-based and can be used to decrypt, inspect, and control both inbound and outbound SSL and SSH connections. Decryption policies allow you to specify traffic for decryption according to destination, source, or URL category and to block or restrict the specified traffic according to your security settings. The firewall uses certificates and keys to decrypt the traffic specified by the policy to plaintext, and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking Profiles.

©2016-2019, Palo Alto Networks, Inc.

After traffic is decrypted and inspected on the firewall, the plaintext traffic is re-encrypted as it exits the firewall to ensure privacy and security.

Central to this discussion is the role of digital certificates to secure SSL and SSH encrypted data. Your understanding of this role and planning for proper certificate needs and deployment are important considerations in decryption use.

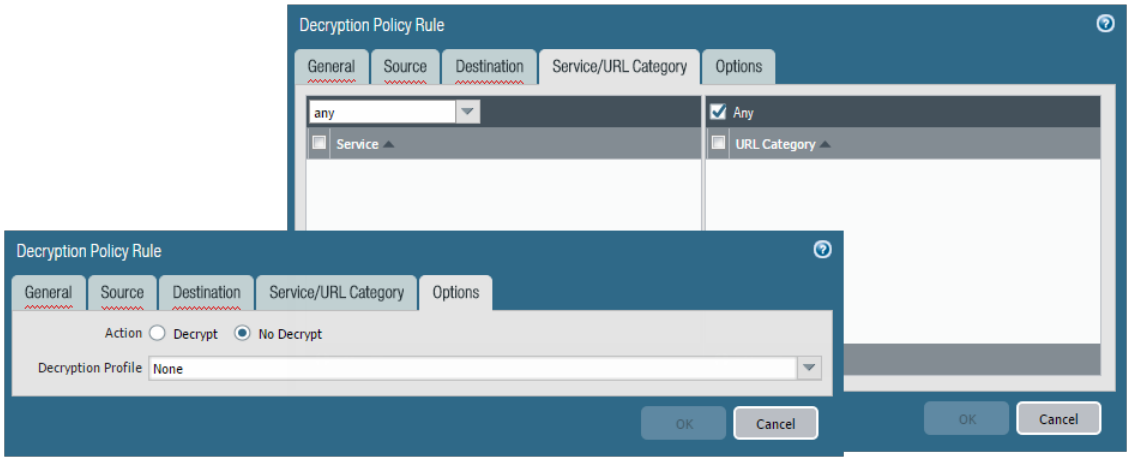
Concepts are discussed here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies.html

The use of certificates is central to other important firewall functions in addition to decryption. This need led to the implementation of extensive certificate management capabilities on the firewall.

A discussion of certificate use for all purposes in the firewall is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/certificate-management/keys-and-certificates.html

Decryption Policies

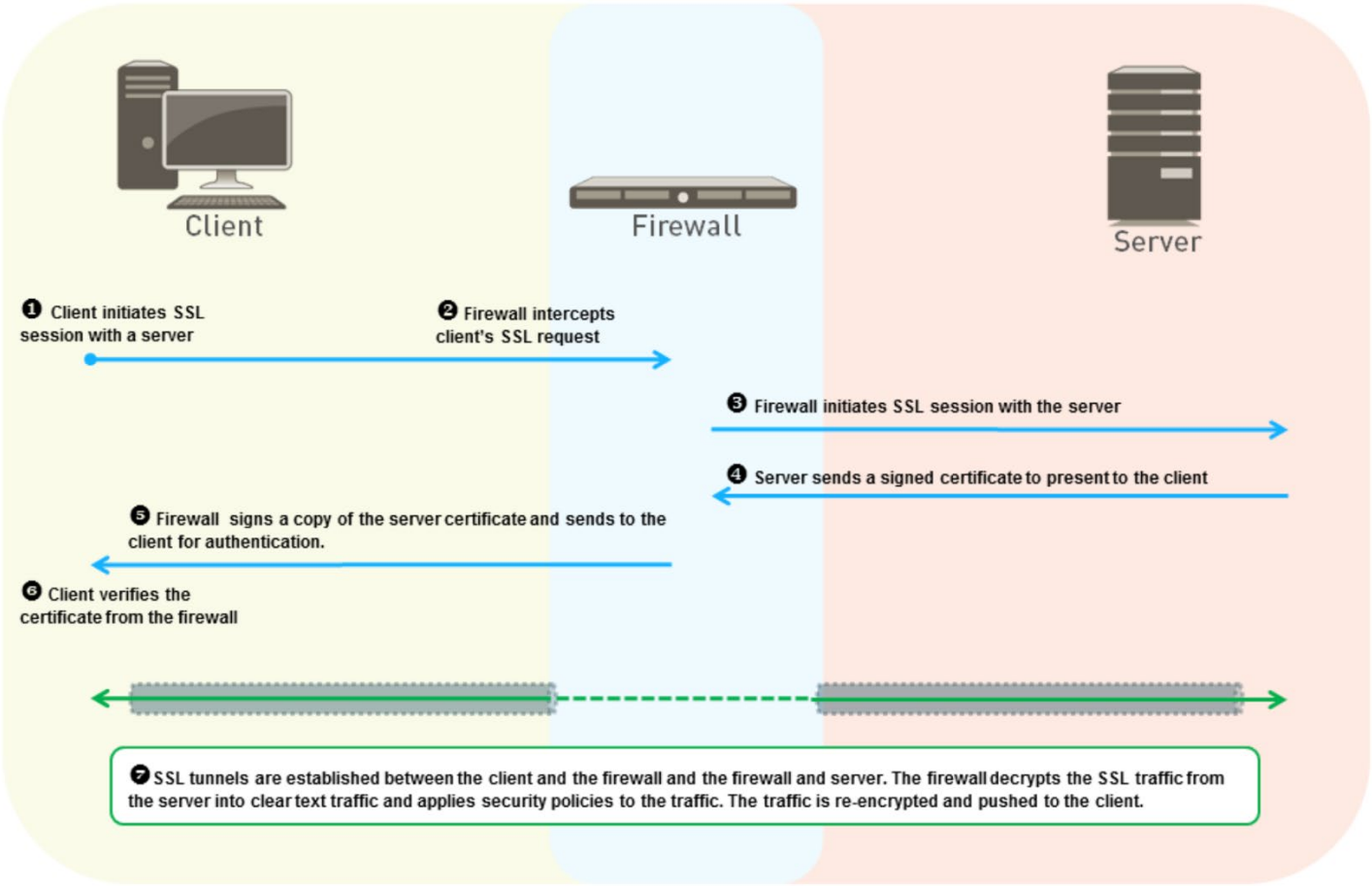
Ingress traffic decryption is controlled by Decryption policies. Palo Alto Networks firewalls automatically will detect encrypted traffic and react by evaluating the Decryption policies. If a matching policy is found, the firewall will attempt to decrypt the traffic according to the policy's specified decryption action. Normal packet processing resumes afterward.



SSL Forward Proxy

Decryption of outbound SSL traffic commonly is implemented and takes the form of SSL Forward Proxy, which features the firewall as an intermediate communication node. This deployment commonly is referred to as a "man in the middle." The following figure shows this functionality.

©2016-2019, Palo Alto Networks, Inc.

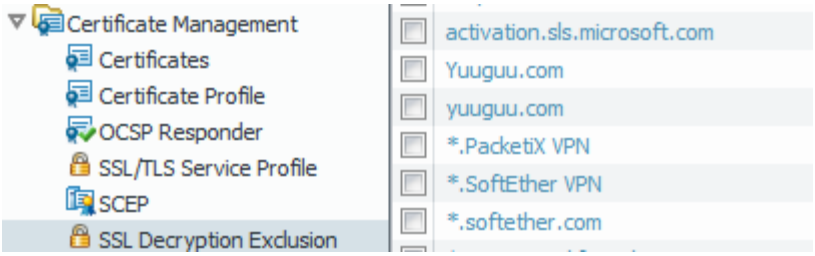


Note that SSL Forward Proxy replaces the original certificate from the server with one signed by a different key that then is delivered to the client.

Decryption Exclusions

A developer of a solution using SSL decryption can take extra programmatic steps to interrogate the certificate received at the client for specific characteristics present in the original certificate. When these characteristics are not found, the author often assumes that a decrypting process is in the middle of the conversation and may act to prevent full functionality and considers this presence a security risk. These products typically are not fully functional in a decrypting environment and must be added as exceptions to Decryption policies.

Palo Alto Networks recognizes this fact and provides a mechanism to mark certain encrypted traffic for decryption bypass. This is managed in part by Palo Alto Networks for known pinned traffic while allowing you administration capability for local requirements.



©2016-2019, Palo Alto Networks, Inc.

A discussion of this topic and how to manage decryption exclusions is found here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-exclusions

App-ID and Encryption

The App-ID scanning engine's effectiveness often is compromised by encrypted traffic that prevents scanning packet contents for identifying elements. This traffic typically is given the App-ID of SSL" In some cases, the App-ID engine can evaluate elements of the certificate that secures this data for specific identifying components, allowing the App-ID engine to properly assign App-IDs without scanning contents. Details about this process are here: https://live.paloaltonetworks.com/t5/Learning-Articles/How-Palo-Alto-Networks-Identifies-HTTPS-Applications-Without/ta-p/56284

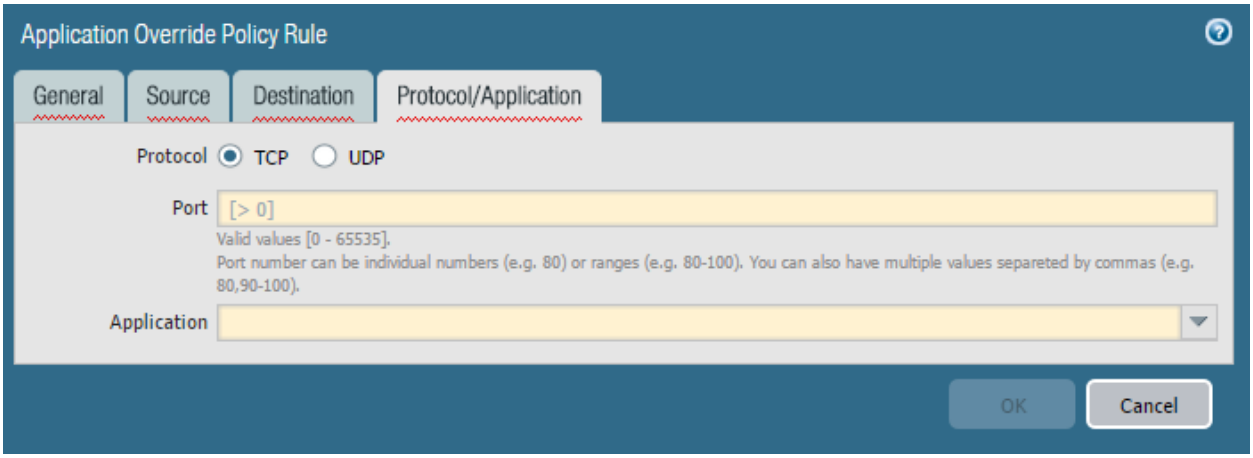
Sample Questions

53. Which feature does not require a Decryption policy?
    A. antivirus
    B. App-ID
    C. file blocking
    D. network address translation
54. How can the next-generation firewall inform web browsers that a web server's certificate is from an unknown CA?
    A. show a "the certificate is untrusted, are you SURE you want to go there" response page before accessing the website
    B. relay the untrusted certificate directly to the browser
    C. have two certificates in the firewall, one used for sites whose original certificate is trusted, and the other for sites whose original certificate is untrusted
    D. have two certificate authority certificates in the firewall, one is used to produce certificates for sites whose original certificate is trusted, and the other for certificates for sites whose original certificate is untrusted
55. Which firewall features can be used to support an organization's requirement of decrypting a user's browsing traffic for compliance and to record all decrypted traffic? (Choose two.)
    A. Decryption Broker
    B. Policy Based Forwarding
    C. Default Router setting of Forward Cleartext
    D. Interface setting of Decryption Port Mirroring
    E. Decryption policy rule action set to Forward Cleartext

©2016-2019, Palo Alto Networks, Inc.

1.17 Identify the impact of application override to the overall functionality of the firewall

Application Override policies specify the App-ID for certain traffic. An Application Override policy also bypasses Layer 7 scanning. This means that no further App-ID and Content-ID scanning happens on that traffic.



Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the **Application** field.

Choices are limited to applications currently in the App-ID database. Because an existing App-ID must be chosen for the policy, the admin should add a new App-ID to the database for this purpose.

Details about creating an App-ID entry for this purpose can be found here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0

Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer 4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy rules and QoS.

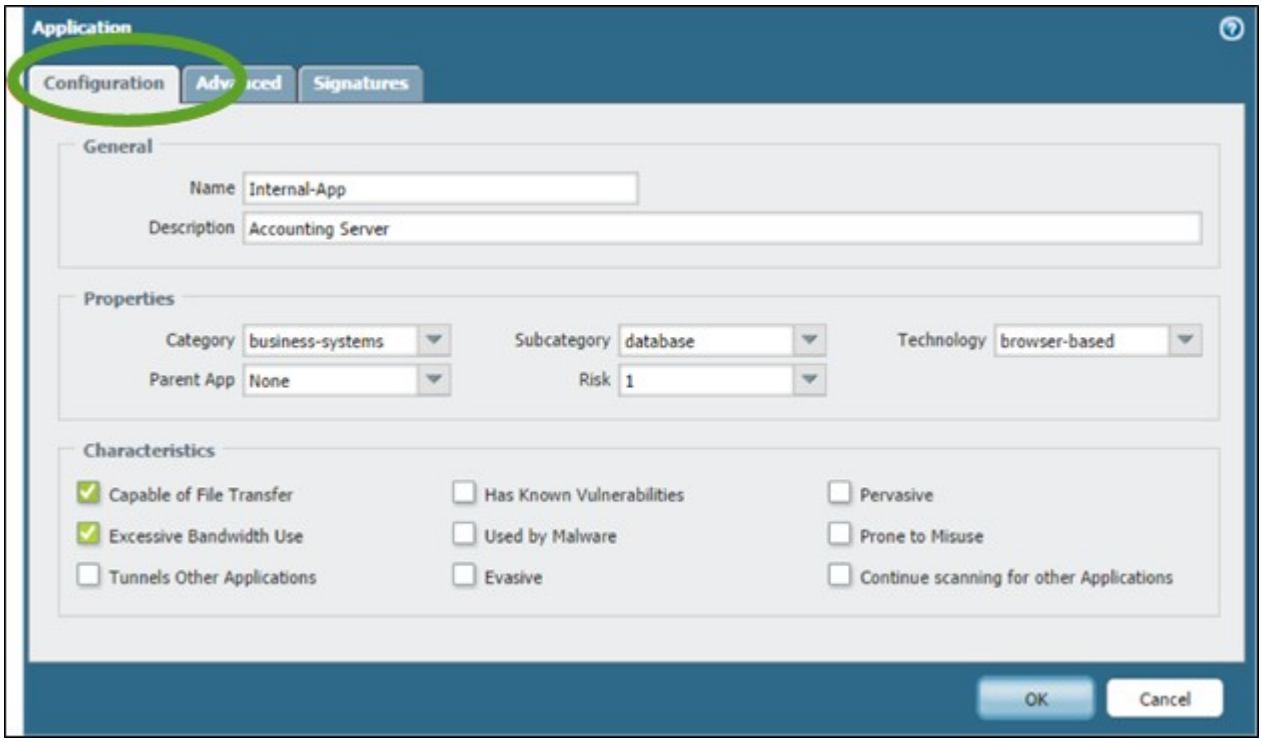
Use Cases

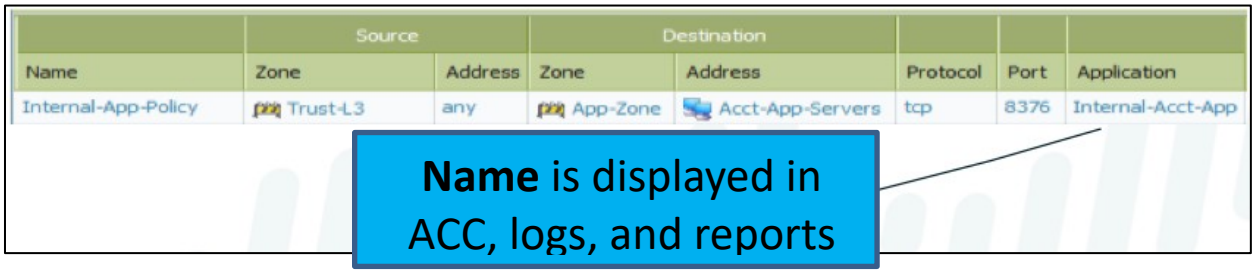
Three primary uses cases for Application Override policy are:

- To identify "Unknown" App-IDs with a different or custom application signature
- To re-identify an existing application signature
- To bypass the Signature Match Engine (within the SP3 architecture) to improve processing times

©2016-2019, Palo Alto Networks, Inc.

The following figures show the creation of a new App-ID for a custom internal application and its use in an Application Override policy that assigns it to appropriate traffic.





©2016-2019, Palo Alto Networks, Inc.

Sample Questions

56. Which type of identification is disabled by Application Override?
    A. Protocol-ID
    B. User-ID
    C. Content-ID
    D. URL Filtering
57. Application Override is triggered by which configuration setting?
    A. Custom App-ID
    B. Application Override policy rule
    C. Application Override definition in Custom Objects
    D. Application Filters

©2016-2019, Palo Alto Networks, Inc.

1.18 Identify the methods of User-ID redistribution

Every firewall that enforces user-based policy requires user mapping information. In a large-scale network, instead of configuring all your firewalls to directly query the mapping information sources, you can streamline resource usage by configuring some firewalls to collect mapping information through redistribution. Redistribution also enables the firewalls to enforce user-based policies when users rely on local sources for authentication (such as regional directory services) but need access to remote services and applications (such as global data center applications).

If you configure Authentication policy, your firewalls also must redistribute the authentication timestamps that are generated when users authenticate to access applications and services. Firewalls use the timestamps to evaluate the timeouts for Authentication policy rules. The timeouts allow a user who successfully authenticates to later request services and applications without authenticating again within the timeout periods. Redistribution of timestamps enables you to enforce consistent timeouts across all the firewalls in your network.

Firewalls share user mappings and authentication timestamps as part of the same redistribution flow; you don't have to configure redistribution for each information type separately.

User-ID Table Sharing

To enable a firewall or virtual system to serve as a User-ID agent that redistributes user mapping information along with the timestamps associated with authentication challenges, configure the collector name and pre-shared key.

Specific information about this configuration can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/user-id-agent-setup/user-id-agent-setup-redistribution.html

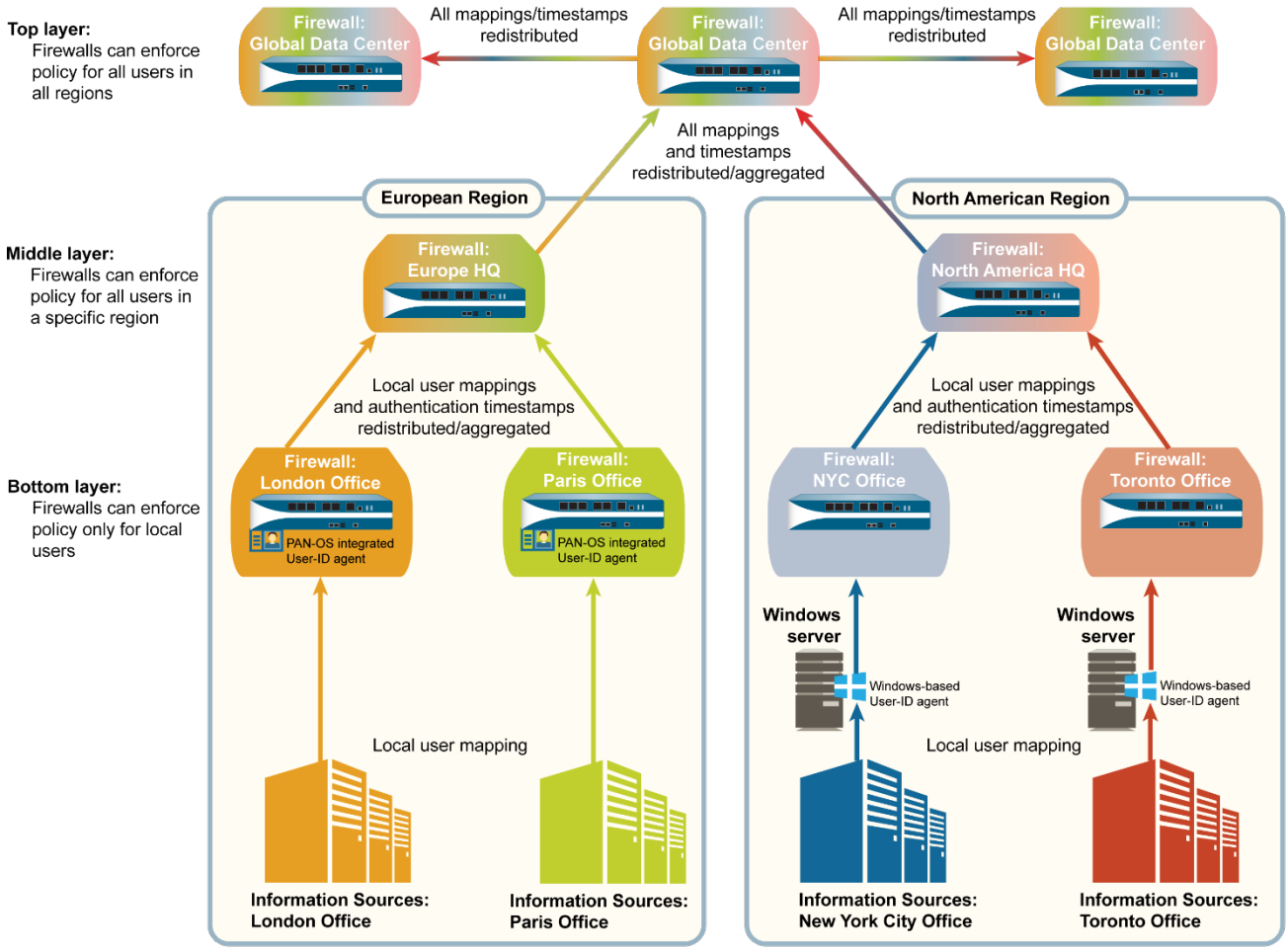
User-ID Table Consumption

To map usernames to IP addresses, User-ID agents monitor sources such as directory servers. The agents send the user mappings to firewalls, Log Collectors, or Panorama. Each appliance then can serve as redistribution points that forward the mappings to other firewalls, Log Collectors, or Panorama. Before a firewall or Panorama can collect user mappings, you must configure its connections to the User-ID agents or redistribution points.

More information about this topic can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/user-identification/device-user-identification-user-id-agents.

©2016-2019, Palo Alto Networks, Inc.

Use Case Example



References

- Redistribute User Mappings and Authentication Timestamps
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps
- User-ID Redistribution Using Panorama
  https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/user-id-redistribution-using-panorama

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

58. User-ID user-id-to-IP-address mapping tables can be read by which product or service?
    A. Traps
    B. Panorama Log Collector
    C. AutoFocus
    D. VM-Series firewall plugin

©2016-2019, Palo Alto Networks, Inc.

1.19 Identify VM-Series bootstrap components and their function

Bootstrapping

All Palo Alto Networks firewalls can automatically configure themselves during first boot using the bootstrapping feature. This feature provisions a specifically prepared storage volume (USB for physical appliances or storage accounts for the VM-Series) containing configuration data, licenses, dynamic updates, and PAN-OS updates that all are applied automatically during the boot process.

VM-Series Bootstrapping

Bootstrapping allows you to create a repeatable and streamlined process of deploying new VM-Series firewalls on your network because it allows you to create a package with the model configuration for your network and then use that package to deploy VM-Series firewalls anywhere. You can bootstrap the VM-Series firewall off an external device (such as a virtual disk, a virtual CD-ROM, or a storage bucket such as AWS S3 or Google Cloud bucket) to complete the process of configuring and licensing the VM-Series firewall. You can either bootstrap the firewall with basic initial configuration and licenses so that the firewall can register with Panorama and then retrieve its full configuration from Panorama, or you can bootstrap the complete configuration so that the firewall is fully configured on boot-up.

Bootstrap Package

The bootstrap process is initiated only when the firewall starts up in a factory default state. After you attach the virtual disk, virtual CD-ROM, or storage bucket to the firewall, the firewall scans for a bootstrap package and, if one exists, the firewall uses the settings defined in the bootstrap package. If you have included a Panorama server IP address in the file, the firewall connects with Panorama. If the firewall has internet connectivity, it contacts the licensing server to update the UUID and obtain the license keys and subscriptions. The firewall then is added as an asset in the Palo Alto Networks Support Portal. If the firewall does not have internet connectivity, it either uses the license keys you included in the bootstrap package or it connects to Panorama, which retrieves the appropriate licenses and deploys them to the managed firewalls.

The bootstrap package that you create must include the /config, /license, /software, and /content folders, even if empty:

- /config folder: Contains the configuration files. The folder can hold two files: init-cfg.txt and the bootstrap.xml.

  Note: If you intend to pre-register VM-Series firewalls with Panorama with bootstrapping, you must generate a VM auth key on Panorama and include the generated key in the init-cfg file.
- /license folder: Contains the license keys or auth codes for the licenses and subscriptions that you intend to activate on the firewalls. If the firewall does not have internet connectivity, you must either manually obtain the license keys from the Palo Alto Networks Support portal or use the Licensing API to obtain the keys and then save each key in this folder.

©2016-2019, Palo Alto Networks, Inc.

Note: You must include an auth code bundle instead of individual auth codes so that the firewall or orchestration service can simultaneously fetch all license keys associated with a firewall. If you use individual auth codes instead of a bundle, the firewall will retrieve only the license key for the first auth code included in the file.

- /software folder: Contains the software images required to upgrade a newly provisioned VM-Series firewall to the desired PAN-OS version for your network. You must include all intermediate software versions between the Open Virtualization Format (OVF) version and the final PAN-OS software version to which you want to upgrade the VM-Series firewall.
- /content folder: Contains the Applications and Threats updates, WildFire updates, and the BrightCloud URL filtering database for the valid subscriptions on the VM-Series firewall. You must include the minimum content versions required for the desired PAN-OS version. Without the minimum required content version associated with the PAN-OS version, the VM-Series firewall cannot complete the software upgrade.
- /plugins folder: Optional folder contains a single VM-Series plugin image.

The bootstrapping volume must be prepared according to the specific information outlined here: https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall.html

Sample Questions

59. When will a firewall check for the presence of bootstrap volume?
    A. each time it cold-boots
    B. each time it boots from a Factory Default state
    C. when a firewall is started in Maintenance Mode
    D. each time it warm-boots
60. Can a firewall's PAN-OS software be updated by the bootstrap process?
    A. Yes, by including a copy of the desired PAN-OS software in the /software folder of the bootstrap volume.
    B. Yes, by including a copy of the desired PAN-OS software in the /content folder of the bootstrap volume.
    C. No, it must be updated by an administrator after the firewall starts.
    D. No, the firewall must be licensed first.

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 2 — Deploy and Configure

2.1 Identify the application meanings in the Traffic log (incomplete, insufficient data, non-syn TCP, not applicable, unknown TCP, unknown UDP, and unknown P2P)

To safely enable applications on your network, the Palo Alto Networks next-generation firewalls provide both an application and web perspective—App-ID and URL filtering—to protect against a full spectrum of legal, regulatory, productivity, and resource utilization risks.

App-ID enables visibility into the applications on the network so you can learn how they work and understand their behavioral characteristics and their relative risk. This knowledge about applications allows you to create and enforce Security policy rules to enable, inspect, and shape desired applications and block unwanted applications. After you define policy rules to allow traffic, App-ID begins to classify traffic without any additional configuration.

App-ID is a patented traffic classification system available only in Palo Alto Networks firewalls. It determines what an application is, irrespective of port, protocol, encryption (SSH or SSL), or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

The App-ID engine is driven by pattern recognition features in the hardware and software of PAN-OS® firewalls. It is based on scanning payloads and application headers only. It does not use port number as a recognition tool; it uses it only for secondary enforcement.

The signature database used by the App-ID scanning engine is updated periodically by Palo Alto Networks through the Applications and Threat Updates.

The App-ID engine is fundamental to PAN-OS software and cannot be turned off. Even when App-ID is not being used as a part of Security policy rules, the Traffic logs show traffic classified by App-ID.

The App-ID engine also can look inside of protocols for “tunneling” applications. For example, the firewall recognizes the HTTP protocol as the App-ID “Web-Browsing.” But when HTTP traffic that belongs to a specific application (e.g., Facebook) will be identified as such by App-ID.

Here's how App-ID identifies applications traversing your network:

1. Traffic is matched against policy to check whether it is allowed on the network.
2. Signatures then are applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines if the application is being used on its default port or if it is using a non-standard port. Traffic that is allowed by policy then is scanned for threats and is further analyzed to identify the application more granularly.
3. If App-ID determines that encryption (SSL or SSH) is in use, and if a Decryption policy rule is in place, the session is decrypted, and application signatures are applied again on the decrypted flow.

©2016-2019, Palo Alto Networks, Inc.

4. Decoders for known protocols then are used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and for opening of dynamic pinholes for applications such as SIP and FTP.
5. For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application.

After the application is identified, the policy check determines how to treat the application, for example—block, or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS.

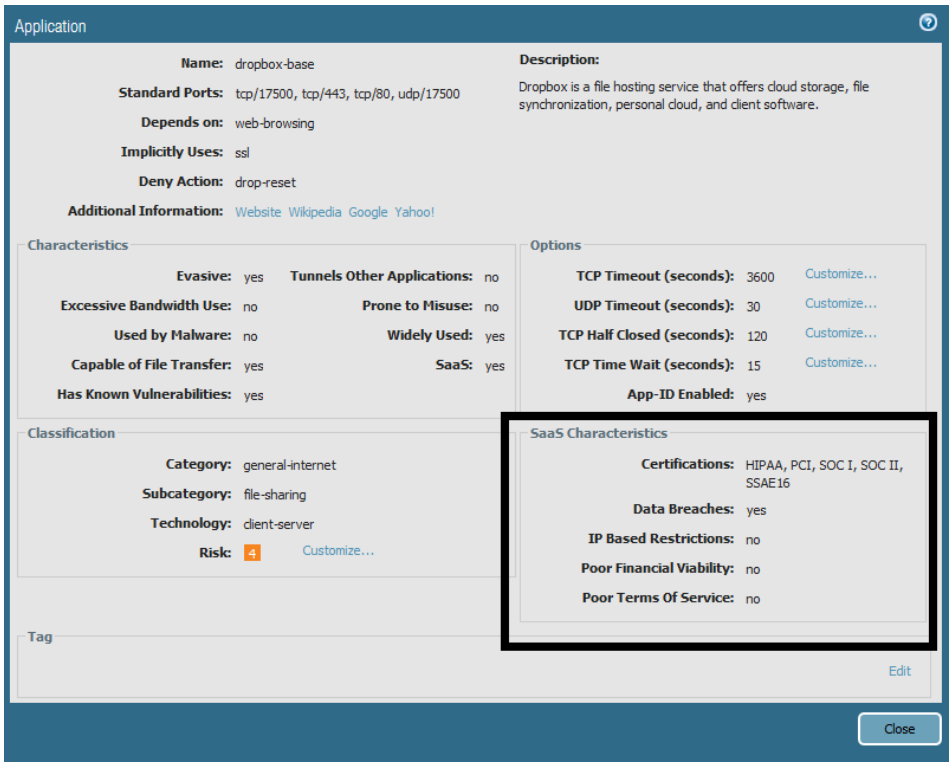
Over the course of a session each packet is being evaluated for its App-ID. The state of App-ID recognition changes as a session progresses, and these states can be found in Traffic logs:

- **incomplete:** Either the three-way TCP handshake did not complete or the three-way TCP handshake did complete but there was no data after the handshake to identify the application. Traffic being seen is not really an application.
  For example, if a client sends a server a syn and the Palo Alto Networks device creates a session for that syn, but the server never sends a SYN ACK back to the client, then that session is “incomplete.”
- **insufficient data:** Not enough data to identify the application. So, for example, if the three-way TCP handshake completed and there was one data packet after the handshake but was not enough to match any of our signatures, then the user will see “insufficient data” in the Application field of the Traffic log.
- **unknown-tcp:** The firewall captured the three-way TCP handshake, but the application was not identified, perhaps because of the use of a custom application for which the firewall does not have signatures.
- **unknown-udp:** Unknown UDP traffic
- **unknown-p2p:** Matches generic P2P heuristics
- **not-applicable:** The Palo Alto Networks device has received data that will be discarded because the port or service that the traffic is coming in on is not allowed, or no rule or policy allows that port or service.
  For example, if there was only one rule on the Palo Alto Networks device and that rule allowed the application of web-browsing only on port/service 80, and traffic (web-browsing or any other application) is sent to the Palo Alto Networks device on any other port/service besides 80, then the traffic is discarded or dropped and you'll see sessions with "not-applicable" in the Application field.

SaaS Applications

The App-ID engine identifies SaaS applications and provides additional functionality. A dedicated SaaS Application Usage report under **Monitor > PDF Reports > SaaS Application Usage** will help your organization identify applications storing your data in external locations. The App-IDs for SaaS application contain additional data about these applications and their providers to help you make decisions allowing access to them at the organizational level.

©2016-2019, Palo Alto Networks, Inc.



Palo Alto Networks firewalls include a feature within the URL Filtering engine that provides HTTP Header Insertion for certain SaaS applications that can prevent users from accessing private instances of a SaaS application while having access to the organization's sanctioned environment. A discussion of this feature can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-security-profiles-url-filtering/http-header-insertion

Note About Using App-ID

Because applications often can use non-standard ports for communication, a traffic enforcement technology based only on port numbers does not provide security administrators enough control over the actual application traffic entering their organizations. Because App-ID identifies applications strictly on packet contents and not on port numbers, it provides a much higher level of capability. When you use Palo Alto Networks firewalls, your security rules should use App-ID as selection criteria, not port numbers.

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

61. An application using which protocol can receive an **incomplete** value in the Application field in the Traffic log?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
62. Session traffic being evaluated by a firewall is encrypted with SSL. If the firewall does not decrypt the traffic, how does the firewall make an App-ID determination?
    A. evaluate the HTTP headers
    B. evaluate the SSL Hello exchange
    C. evaluate certificate contents used for encryption
    D. use information in the SSL Decryption Exclusion cache
63. How does the firewall respond to a change of application detected during the firewall's App-ID scanning of an on-going session.?
    A. closes the session, opens a new one, and evaluates all security policies again
    B. closes the session, opens a new one, and evaluates the original matching Security policy rule only
    C. updates the application in the existing session and evaluates all Security policies again
    D. updates the application in the existing session and continues to use the original action from the first Security policy rule match

©2016-2019, Palo Alto Networks, Inc.

2.2 Given a scenario, identify the set of Security Profiles that should be used

Although Security policy rules enable you to allow or block traffic on your network, Security Profiles help you define an allow-but-scan rule, which scans allowed applications for threats such as viruses, malware, spyware, and DDoS attacks. When traffic matches the allow rule defined in the Security policy, the Security Profile(s) attached to the rule are applied for further content inspection such as antivirus checks and data filtering. Security Profiles are the features that provide the services of the Content-ID feature of PAN-OS software.

Security Profiles are not used in the match criteria of a traffic flow. The Security Profile is applied to scan traffic after the application or category is allowed by the Security policy.

The firewall provides default Security Profiles that you can use out-of-the-box to begin protecting your network from threats. Security Profiles are attached to specific Security policy rules specifying that particular type of threat detection should be performed on traffic allowed by the rule.

You can add Security Profiles that are commonly applied together to create a Security Profile Group; this set of profiles can be treated as a unit and added to Security policies in one step (or included in Security policies by default, if you choose to set up a default Security Profile Group).

Security Profile Types

Security Profiles manage particular types of threat detection:

Antivirus Profiles

Antivirus Profiles protect against viruses, worms, trojans, and spyware downloads. The Palo Alto Networks antivirus solution uses a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, to provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML, and JavaScript viruses, and includes support for scanning inside compressed files and data encoding schemes. If you have enabled Decryption on the firewall, the profile also enables scanning of decrypted content.

The default profile inspects all the listed protocol decoders for viruses, and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for FTP, HTTP, and SMB protocols. You can configure the action for a decoder or Antivirus signature and specify how the firewall responds to a threat event:

- default: For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an “alert” or a “reset-both.”

©2016-2019, Palo Alto Networks, Inc.

The default action is displayed in parenthesis, for example, default (alert) in the threat or Antivirus signature.

- allow: Permits the application traffic
- alert: Generates an alert for each application traffic flow. The alert is saved in the threat log.
- drop: Drops the application traffic
- reset -client: For TCP, resets the client-side connection. For UDP, drops the connection.
- reset-server: For TCP, resets the server-side connection. For UDP, drops the connection.
- reset-both: For TCP, resets the connection on both client and server ends. For UDP, drops the connection.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the internet, long with the traffic sent to highly sensitive destinations, such as server farms.

The Palo Alto Networks WildFire® system also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard Antivirus signatures that can be downloaded daily by Threat Prevention subscribers (sub-hourly for WildFire subscribers).

Anti-Spyware Profiles

Anti-Spyware Profiles block spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, thus allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware Profiles that minimize inspection between trusted zones while maximizing inspection on traffic received from an untrusted zone such as an internet-facing zone. You can define your own custom Anti-Spyware Profiles or choose one of the following predefined profiles when applying anti-spyware to a Security policy rule:

- Default: Uses the “default” action for every signature, as specified by Palo Alto Networks when the signature is created
- Strict: Overrides the “default” action of critical, high, and medium-severity threats to the block action, regardless of the action defined in the signature file. This profile still uses the default action for low and informational severity signatures.

After the firewall detects a threat event, you can configure the following actions in an Anti-Spyware Profile:

- default: For each threat signature and Anti-Spyware signature that is defined by Palo Alto Networks, a “default” action is specified internally. Typically, the default action is an “alert” "or a “reset-both.” The “default” action is displayed in parenthesis, for example, “default” (alert) in the threat or Antivirus signature.
- allow: Permits the application traffic
- alert: Generates an alert for each application traffic flow. The alert is saved in the Threat log.
- drop: Drops the application traffic
- reset-client: For TCP, resets the client-side connection. For UDP, drops the connection.
- reset-server: For TCP, resets the server-side connection. For UDP, drops the connection.
- reset-both: For TCP, resets the connection on both client and server ends. For UDP, drops the

©2016-2019, Palo Alto Networks, Inc.

connection.

Note: In some cases, when the profile action is set to “reset-both,” the associated threat log might display the action as “reset-server.” This occurs when the firewall detects a threat at the beginning of a session and presents the client with a 503 block page. Because the block page disallows the connection, the client side does not need to be reset and only the server-side connection is reset.

- Block IP: Blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

You also can enable the DNS Sinkholing action in Anti-Spyware Profiles to enable the firewall to forge a response to a DNS query for a known malicious domain, thus causing the malicious domain name to resolve to an IP address that you define. This feature helps to identify infected hosts on the protected network using DNS traffic. Infected hosts then can be easily identified in the Traffic logs and Threat logs because any host that attempts to connect to the sinkhole IP address most likely is infected with malware.

Anti-Spyware Profiles and Vulnerability Protection Profiles are configured similarly.

Vulnerability Protection Profiles

Vulnerability Protection Profiles stop attempts to exploit system flaws or gain unauthorized access to systems. Although Anti-Spyware Profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection Profiles protect against threats entering the network. For example, Vulnerability Protection Profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Profile protects clients and servers from all known critical, high, and medium-severity threats. You also can create exceptions that allow you to change the response to a specific signature.

After the firewall detects a threat event, you can configure the following actions in an Anti-Spyware profile:

- default: For each threat signature and Anti-Spyware signature that is defined by Palo Alto Networks, a “default” action is specified internally. The “default” action typically is an “alert” or a “reset-both.” The “default” action is displayed in parenthesis, for example, “default” (alert) in the threat or Antivirus signature.
- allow: Permits the application traffic
- alert: Generates an alert for each application traffic flow. The alert is saved in the Threat log.
- drop: Drops the application traffic
- reset-client: For TCP, resets the client-side connection. For UDP, drops the connection.
- reset-server: For TCP, resets the server-side connection. For UDP, drops the connection.
- reset-both: For TCP, resets the connection on both client and server ends. For UDP, drops the connection.

Note: In some cases, when the profile action is set to “reset-both,” the associated Threat log might display the action as “reset-server.” This occurs when the firewall detects a threat at the beginning of a session and presents the client with a 503 block page. Because the block page disallows the connection, the client side does not need to be reset and only the server-side connection is reset.

- Block IP— This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

©2016-2019, Palo Alto Networks, Inc.

URL Filtering Profiles

URL Filtering Profiles enable you to monitor and control how users access the web over HTTP and HTTPS. The firewall comes with a default profile that is configured to block websites such as known malware sites, phishing sites, and adult content sites. You can use the default profile in a Security policy, clone it to be used as a starting point for new URL Filtering Profiles, or add a new URL Profile that will have all categories set to “allow” for visibility into the traffic on your network. You then can customize the newly added URL profiles and add lists of specific websites that always should be blocked or allowed, which provides more granular control over URL categories.

Data Filtering Profiles

Data Filtering Profiles prevent sensitive information such as credit card numbers or Social Security numbers from leaving a protected network. The Data Filtering Profile also allows you to filter on keywords, such as a sensitive project name or the word confidential. It should focus your profile on the desired file types to reduce false positives. For example, you may want to search only Word documents or Excel spreadsheets. You also may want to scan only web-browsing traffic or FTP.

You can create custom data pattern objects and attach them to a Data Filtering Profile to define the type of information about which you want to filter. Create data pattern objects based on:

- Predefined Patterns: Filter for credit card numbers and Social Security numbers (with or without dashes) using predefined patterns
- Regular Expressions: Filter for a string of characters
- File Properties: Filter for file properties and values based on file type
  Note: If you’re using a third-party, endpoint data loss prevention (DLP) solution to populate file properties to indicate sensitive content, this option enables the firewall to enforce your DLP policy.

File Blocking Profiles

The firewall uses File Blocking Profiles to block specified file types over specified applications and in the specified session flow direction (inbound/outbound/both). You can set the profile to “alert” or “block” on upload and/or download and you can specify which applications will be subject to the File Blocking Profile. You also can configure custom block pages that will appear when a user attempts to download the specified file type. This allows the user to pause to consider whether they want to download a file.

You can define your own custom File Blocking Profiles or choose one of the following predefined profiles when applying file blocking to a Security policy rule. The predefined profiles, which are available with content release version 653 and later, allow you to quickly enable best practice file blocking settings:

- Basic file blocking: Attach this profile to the Security policy rules that allow traffic to and from less sensitive applications to block files that commonly are included in malware attack campaigns or that have no real use case for upload or download. This profile blocks upload and download of PE files (.scr, .cpl, .dll, .ocx, .pif, .exe), Java files (.class, .jar), Help files (.chm, .hlp), and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. It also prompts users to acknowledge when they attempt to download encrypted-rar or encrypted-zip files. This rule alerts on all other file types to give you complete visibility into all file types entering and leaving your network.

©2016-2019, Palo Alto Networks, Inc.

- Strict file blocking: Use this stricter profile on the Security policy rules that allow access to your most sensitive applications. This profile blocks the same file types as the basic file blocking profile, and blocks flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

Configure a File Blocking Profile with the following actions:

- alert: After the specified file type is detected, a log is generated in the Data Filtering log.
- block: After the specified file type is detected, the file is blocked, and a customizable block page is presented to the user. A log also is generated in the Data Filtering log.
- continue: After the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log also is generated in the Data Filtering log. Because this type of forwarding action requires user interaction, it is applicable only for web traffic.

WildFire Analysis Profiles

Use a WildFire Analysis Profile to enable the firewall to forward unknown files or email links for WildFire analysis. This detection is for zero-day threats contained in files. The firewall's anti-virus threat detection finds known virus based on local resources. Specify files to be forwarded for analysis based on application, file type, and transmission direction (upload or download). Files or email links matched to the profile rule are forwarded to either the WildFire public cloud or the WildFire private cloud (hosted with a WF-500 appliance), depending on the analysis location defined for the rule. If a profile rule is set to forward files to the WildFire public cloud, the firewall also forwards files that match existing Antivirus signatures, in addition to unknown files.

You also can use the WildFire Analysis Profiles to set up a WildFire hybrid cloud deployment. If you are using a WildFire appliance to analyze sensitive files locally (such as PDFs), you can specify for less sensitive file types (such as PE files) or file types that are not supported for WildFire appliance analysis (such as APKs) to be analyzed by the WildFire public cloud. Use of both the WildFire appliance and the WildFire cloud for analysis allows you to benefit from a prompt verdict for files that already have been processed by the cloud and for files that are not supported for appliance analysis and frees the appliance capacity to process sensitive content.

DoS Protection Profiles

DoS Protection Profiles provide detailed control for DoS Protection Policies. DoS policies allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. The Palo Alto Networks firewalls support two DoS protection mechanisms:

- Flood Protection: Detects and prevents attacks where the network is flooded with packets, which results in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack usually is spoofed.
- Resource Protection: Detects and prevent session exhaustion attacks. In this type of attack, many hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources.

You can enable both types of protection mechanisms in a single DoS Protection Profile.

©2016-2019, Palo Alto Networks, Inc.

The DoS Profile is used to specify the type of action to take and the details on matching criteria for the DoS policy. The DoS Profile defines settings for SYN, UDP, and ICMP floods; can enable resource protection; and defines the maximum number of concurrent connections. After you configure the DoS Protection Profile, you then attach it to a DoS policy.

When you configure DoS protection, you should analyze your environment to set the correct thresholds based on your actual traffic rather than using the default values provided.

Sample Questions

64. Which profile do you use for DLP?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
65. Which profile do you use to monitor DNS resolution lookups for sites associated with threat activity?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
66. Which profile do you use to analyze files for zero-day malware?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering

©2016-2019, Palo Alto Networks, Inc.

67. Which profile do you use to examine browsing traffic for appropriate browsing policy enforcement?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
68. Which profile do you use to detect and block an executable file from being transferred through the firewall?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering

©2016-2019, Palo Alto Networks, Inc.

2.3 Identify the relationship between URL filtering and credential theft prevention

Phishing Prevention Overview

The Palo Alto Networks URL filtering solution complements App-ID by controlling access to web (HTTP and HTTPS) traffic and protecting your network from attack.

With URL filtering enabled, all web traffic is compared against the URL filtering database, which contains a listing of millions of categorized websites. You can use these URL categories as a match criterion to enforce Security policy and to safely enable web access and control the traffic that traverses your network. You also can use URL filtering to enforce safe search settings for your users and to prevent credential phishing based on URL category.

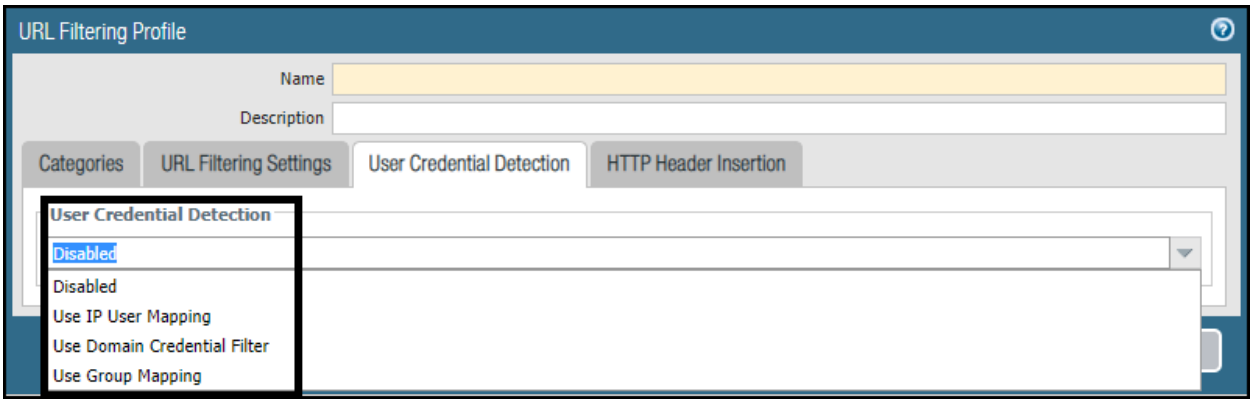
Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose which websites you want to either allow or block corporate credential submissions based on the URL category of the website. When the firewall detects a user credentials being transmitted to a site in a category you have restricted, it either displays a block response page that prevents the user from submitting credentials or presents a continue page that warns users against submitting credentials to sites classified in certain URL categories. But the firewall still allows the user to continue with the credential submission. You can customize these block pages to educate users against reusing corporate credentials, even on legitimate, non-phishing sites.

Credential Detection

Before you configure credential phishing prevention, decide which method you want the firewall to use to identify credentials. Each method requires the configuration of *User-ID* technology. The *IP-to-user mapping* and *group mapping* methods check for valid username submissions only. In these cases, the firewall blocks or allows the submission, based on your settings, regardless of the accompanying password submitted. The *domain credential filter* method checks for valid passwords submitted to a webpage:

- IP-to-user mapping: The firewall uses IP-address-to-user mappings that the PAN-OS integrated User-ID collects to check if a username submitted to a webpage matches the username of the logged-in user.
- Group mapping: The PAN-OS integrated User-ID agent collects group mapping information from a directory server and retrieves a list of groups and the corresponding group members. It compares usernames submitted to a webpage against the group member usernames.
- Domain credential filter: The Windows-based User-ID agent is installed on a Read-Only Domain Controller (RODC). The User-ID agent collects password hashes that correspond to users for which you want to enable credential detection and sends these mappings to the firewall. The firewall then checks if the source IP address of a session matches a username and if the password submitted to the webpage belongs to that username. With this mode, the firewall blocks or alerts on the submission only when the password submitted matches a user password.

©2016-2019, Palo Alto Networks, Inc.

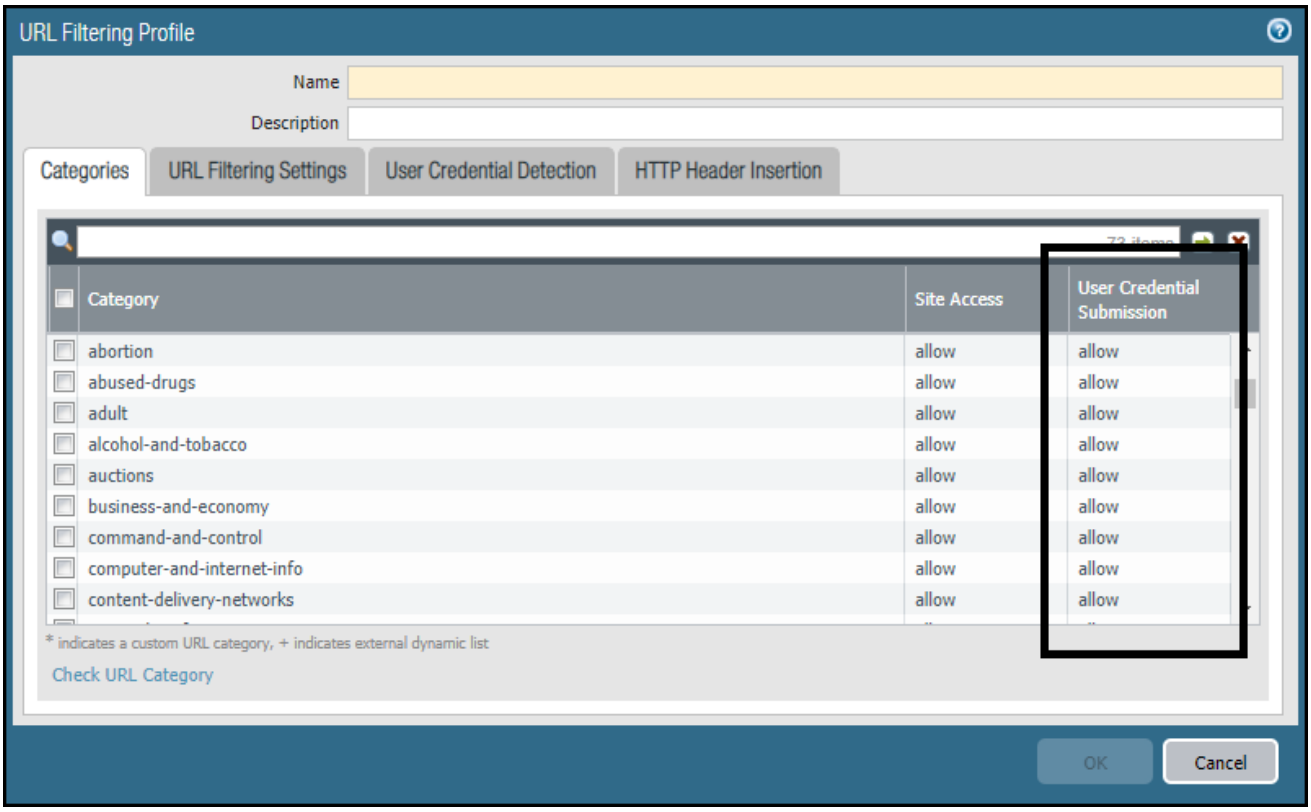


Category Selection for Enforcement

After the detection method is chosen for the URL Filtering Profile, the enforcement action must be chosen for each appropriate browsing category. Custom categories can be created when flexibility is required in identifying specific category members. For each category, select how you want to treat User Credential Submissions:

- alert: Allow users to submit credentials to the website but generate a URL Filtering log each time a user submits credentials to sites in this URL category
- allow: (default) Allow users to submit credentials to the website
- block: Block users from submitting credentials to the website. When a user tries to submit credentials, the firewall displays the **Anti Phishing Block** page, which prevents the credential submission.
- continue: Present the **Anti Phishing Continue** page response page when a user attempts to submit credentials. Users must select **Continue** on the response page to continue with the submission.

©2016-2019, Palo Alto Networks, Inc.



When the firewall detects a user attempting to submit credentials to a site in a category you have restricted, it either displays a block response page that prevents the user from submitting credentials or presents a continue page that warns users against submitting credentials to sites classified in certain URL categories. But the firewall still allows the user to continue with the credential submission. You can customize these block pages to educate users against reusing corporate credentials, even on legitimate, non-phishing sites.

Sample Questions

69. Which credential phishing prevention action allows users to choose to submit credentials to a site anyway?
    A. alert
    B. allow
    C. block
    D. continue

©2016-2019, Palo Alto Networks, Inc.

70. Which user credential detection method would work if multiple users share the same client IP address (for example, because of dynamic address translation done by a device on the internal side of the firewall)?
    A. IP-to-user mapping
    B. group mapping
    C. domain credential filter
    D. IP-and-port-to-user mapping
    E. identify the relationship between URL filtering and credential theft prevention
71. Which type of user credential detection should be used by a firewall administrator that wants to enable Credential Phishing Prevention that blocks an attempt by a user to enter the organization's user ID and password?
    A. IP-to-user mapping
    B. domain credential filter
    C. group mapping
    D. Citrix mapping

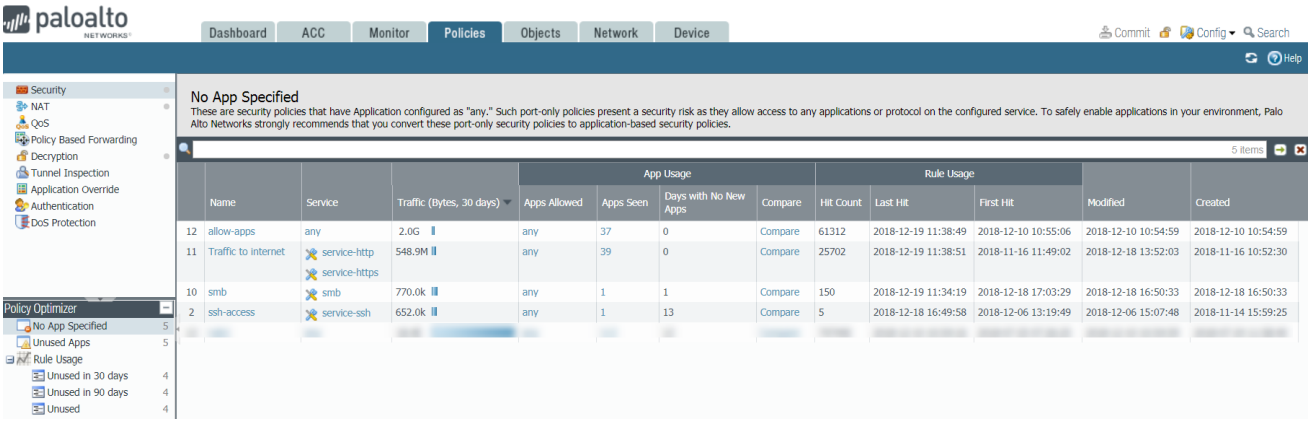
©2016-2019, Palo Alto Networks, Inc.

2.4 Implement and maintain the App-ID lifecycle

When you transition from a legacy firewall to a Palo Alto Networks next-generation firewall, you inherit a large number of port-based rules that allow any application on the ports, which increases the attack surface because any application can use an open port. Policy Optimizer identifies all applications seen on any legacy port-based Security policy rule and provides an easy workflow for selecting the applications you want to allow on that rule. Migrate port-based rules to application-based whitelist rules to reduce the attack surface and safely enable applications on your network. Use Policy Optimizer to maintain the rulebase as you add new applications.

Step 1: Identify Port-Based Rules

Port-based rules have no configured (whitelisted) applications. **Policies > Security > Policy Optimizer > No App Specified** displays all port-based rules (**Apps Allowed** is **any**).



Step 2: Prioritize Which Port-Based Rules to Convert First

Policies > Security > Policy Optimizer > No App Specified enables you to sort rules without affecting their order in the rulebase and provides other information that helps you prioritize rules for conversion based on your business goals and risk tolerance.

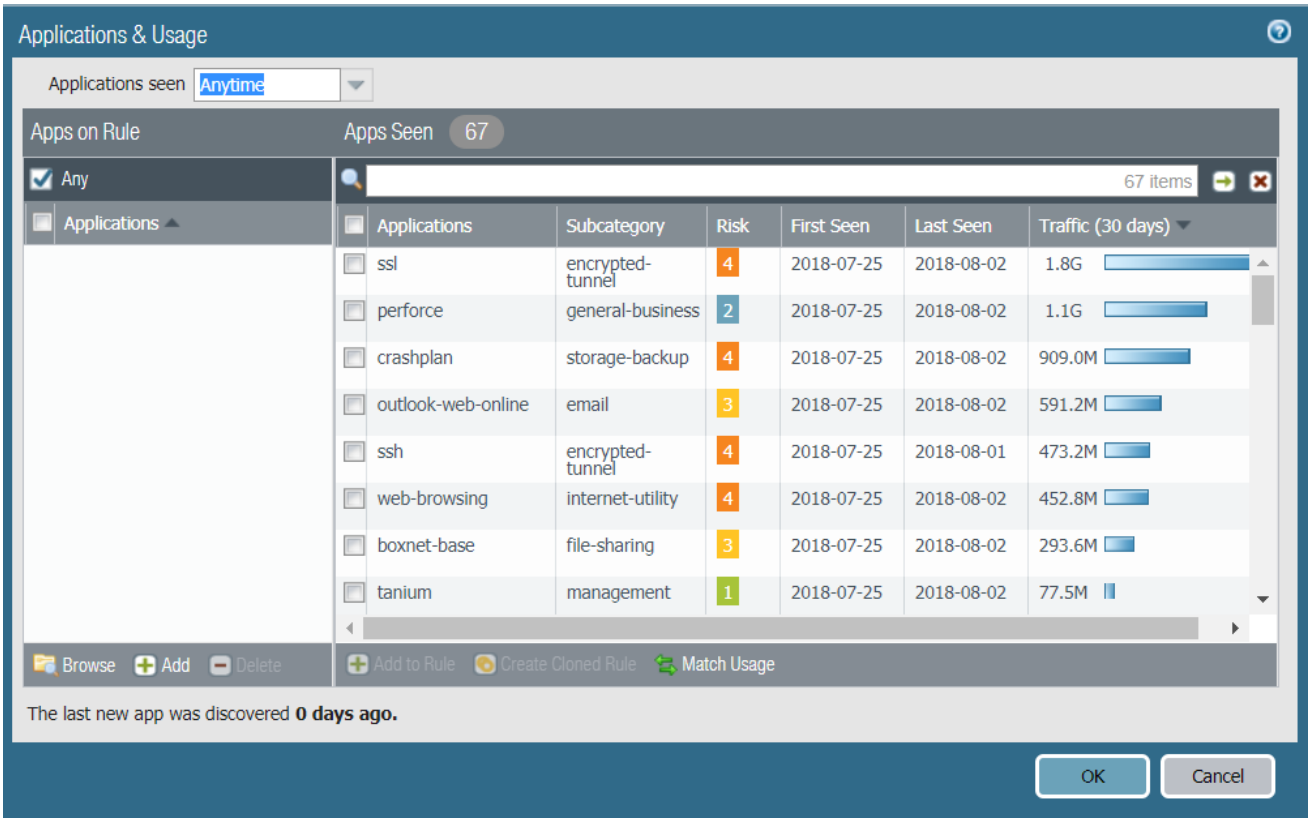
- Traffic (Bytes, 30 days): (Click to sort.) Rules that currently match the most traffic are at the top of the list. This is the default sorting order.
- Apps Seen: (Click to sort.) A large number of legitimate applications matching a port-based rule may indicate you should replace it with multiple application-based rules that tightly define the applications, users, and sources and destinations. For example, if a port-based rule controls traffic for multiple applications for different user groups on different sets of devices, create separate rules that pair applications with their legitimate users and devices to reduce the attack surface and increase visibility. (Click the **Apps Seen** number or **Compare** to display the applications that have matched the rule.)
- Days with No New Apps: (Click to sort.) When the applications seen on a port-based rule stabilize, you can be more confident the rule is mature, conversion won't accidentally exclude legitimate applications, and no more new applications will match the rule. The **Created** and **Modified** dates help you evaluate a rule's stability because older rules that have not been modified recently may also be more stable.
- Hit Count: Displays rules with the most matches over a selected time frame. You can exclude rules for which you reset the hit counter and specify the exclusion time period in days. Exclusion

©2016-2019, Palo Alto Networks, Inc.

of rules with recently reset hit counters prevents misconceptions about rules that show fewer hits than you expect because you didn't know the counter was reset.

Step 3: Review the Apps Seen on Port-Based Rules, Starting with the Highest Priority Rules

On **No Apps Specified**, click **Compare** or the number in **Apps Seen** to open **Applications & Usage**, which lists applications that matched a port-based rule over a specified time frame, with each application's **Risk**, the date it was **First Seen**, the date it was **Last Seen**, and the amount of traffic over the last 30 days.



You can check **Applications seen** on port-based rules over the past 7, 15, or 30 days, or over the rule's lifetime (**Anytime**). For migrating rules, **Anytime** provides the most complete assessment of applications that matched the rule.

You can search and filter the **Apps Seen**, but remember that an hour or more is required to update **Apps Seen**. You also can order the **Apps Seen** by clicking the column headers. For example, you can click **Traffic (30 days)** to bring the applications with the most recent traffic to the top of the list or click **Subcategory** to organize the applications by subcategory.

©2016-2019, Palo Alto Networks, Inc.

Step 4: Clone or Add Applications to the Rule to Specify the Applications You Want to Allow on the Rule

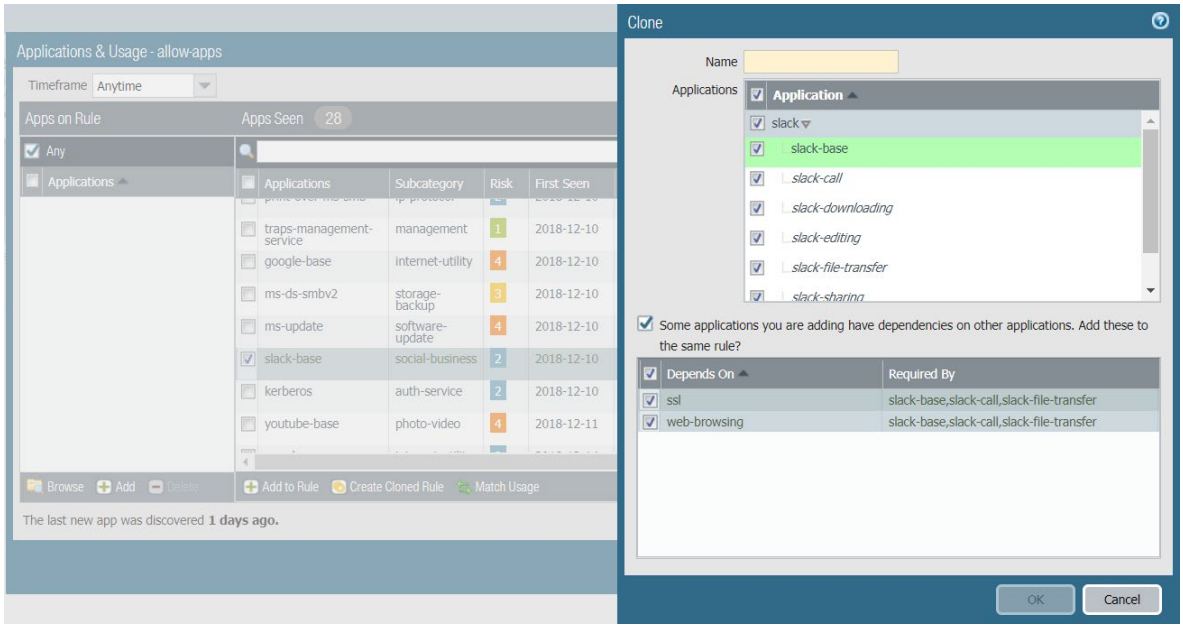
On **Applications & Usage**, convert a port-based rule to an application-based rule by:

- Cloning the rule: Preserves the original port-based rule and places the cloned application-based rule directly above it in the rulebase
- Adding applications to the rule: Replaces the original port-based rule with the new application-based rule and deletes the original rule

Cloning is the safest way to migrate rules, especially when **Applications & Usage** shows more than a few well-known applications matching the rule. Cloning preserves the original port-based rule and places it below the cloned application-based rule, which eliminates the risk of losing application availability because traffic that doesn't match the cloned rule flows through to the port-based rule. When traffic from legitimate applications hasn't hit the port-based rule for a reasonable period of time, you can remove it to complete that rule's migration.

To **clone** a port-based rule:

1. In **Apps Seen**, click the check box next to each application you want in the cloned rule. Remember that an hour or more is required to update **Apps Seen**.
2. Click **Create Cloned Rule**. In the **Clone** dialog, **Name** the cloned rule and add other applications in the same container and application dependencies, if required. This figure shows how to clone a rule by selecting the slack-base application:



In the **Clone** window, the green row is the selected application to clone. The container application (**slack**) is in the gray row. The applications listed in italics are applications in the same container as the selected application but that have not been seen on the rule. Individual applications that have been seen on the rule are in normal font. All the applications are included in the cloned rule by default to help prevent the rule from breaking.

3. If the container app is a tolerated application (not an application sanctioned for business purposes) and you want to constrain access to some of the individual functional applications in

©2016-2019, Palo Alto Networks, Inc.

the container, uncheck the box next to each individual application you don't want users to access. If the container app is a sanctioned business application, add the container app and its individual applications.

4. Leave the application dependencies checked, in this example, **ssl** and **web-browsing** (these are applications that the selected application requires).
5. Click **OK** to add the new application-based rule directly above the port-based rule in the rulebase.
6. **Commit** the configuration.

After you clone a rule and **Commit** the configuration, the applications you select for the cloned rule are removed from the original port-based rule's **Apps Seen** list. For example, if a port-based rule has 16 **Apps Seen** and you select two individual applications and one dependent application for the cloned rule, after cloning, the port-based rule shows 13 **Apps Seen** because the three selected applications have been removed from the port-based rule (16 − 3 = 13). The cloned rule shows the three added applications in **Apps on Rule**.

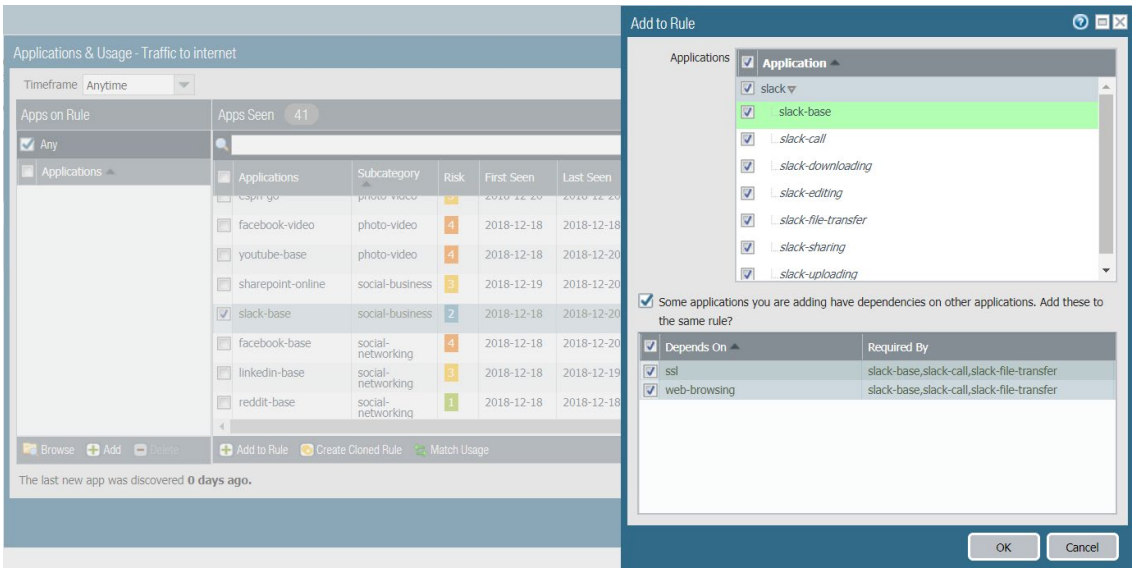
Creation of a cloned rule with a container app works a bit differently. For example, a port-based rule has 16 **Apps Seen** and you select one individual application and a container app for the cloned rule. The container app has five individual applications and has one dependent application. After cloning, the cloned rule shows seven **Apps on Rule**—the individual application, the five individual applications in the container app, and the dependent application for the container app. However, in the original port-based rule, **Apps Seen** shows 13 applications because only the individual application, the container app, and the container app's dependent application are removed from the port-based rule.

Unlike with cloning, addition of applications to a port-based rule replaces the rule with the resulting application-based rule. Addition of applications to a rule is simpler than cloning, but riskier because you may inadvertently miss applications that should be on the rule, and the original port-based rule isn't in the rulebase to identify accidental omissions. However, addition of applications to port-based rules that apply to only a few well-known applications migrates the rule quickly to an application-based rule. For example, for a port-based rule that controls only traffic to TCP port 22, the only legitimate application is SSH, so it's safe to add applications to the rule.

There are three ways to **add** applications to replace a port-based rule with an application-based rule: **Add to Rule**, **Match Usage** in **Apps Seen**, and **Add** in **Apps on Rule**:

- **Add to Rule** applications from **Apps Seen** (applications that matched the rule). Remember that an hour or more is required to update **Apps Seen**.
    1. Select applications from **Apps Seen** on the rule.
    2. Click **Add to Rule**. In the **Add to Rule** dialog, add other applications in the same container app and application dependencies, if required. For example, to add slack-base to a rule:

©2016-2019, Palo Alto Networks, Inc.



As is the case with the **Clone** dialog, the green row in the **Add to Rule** dialog is the selected application to add to the rule. The container app (**slack**) is in the gray row. The applications listed in italics are applications in the same container but that have not been seen on the rule. Individual applications that have been seen on the rule are in normal font. All the applications are included in the new rule by default to help prevent the rule from breaking.

3. If you are sure any of the italicized applications in the container that have not been seen on the rule will never be seen on the rule, you can uncheck the box next to them, so they aren't included in the rule. If you uncheck a container app, its individual applications also are unchecked.
4. Leave the application dependencies checked, in this example **ssl** and **web-browsing** (these are applications that the selected application requires).
5. Click **OK** to replace the port-based rule with the new application-based rule.

   When you **Add to Rule** and **Commit** the configuration, the applications you didn't add are removed from **Apps Seen** because the new application-based rule no longer allows them. For example, if a rule has 16 **Apps Seen** and you **Add to Rule** three applications, the resulting new rule shows only those three added applications in **Apps Seen**.

   Add to Rule with a container app works a bit differently. For example, a port-based rule has 16 **Apps Seen** and you select one individual application and a container app to add to the new rule. The container app has five individual applications and has one dependent application. After you add the applications to the rule, the new rule shows seven **Apps on Rule**—the individual application, the five individual applications in the container app, and the dependent application for the container app. However, **Apps Seen** shows 13 applications because the individual application, the container app, and the container app's dependent application are removed from that list.

- Add all of the **Apps Seen** on the rule to the rule at one time with one click (**Match Usage**):

  1. In **Apps Seen**, click **Match Usage**. Remember that an hour or more is required to update **Apps Seen**. All the applications in **Apps Seen** are copied to **Apps on Rule**.
  2. Click **OK** to create the application-based rule and replace the port-based rule.

©2016-2019, Palo Alto Networks, Inc.

- If you know the applications you want on the rule, you can **Add** applications manually in **Apps on Rule**. However, this method is equivalent to using the traditional Security policy rule **Application** tab and does not change **Apps Seen** or **Apps on Rule**. To preserve accurate application usage information, convert rules using **Add to Rule**, **Create Cloned Rule**, or **Match Usage** in **Apps Seen**.
    1. In **Apps on Rule**, **Add** (or **Browse**) and select applications to add to the rule. This is equivalent to adding applications on the **Application** tab.
    2. Click **OK** to add the applications to the rule and replace the port-based rule with the new application-based rule.

Step 5: For Each Application-Based Rule, Set the Service to application-default

If business needs require you to allow applications (for example, internal custom applications) on non-standard ports between particular clients and servers, restrict the exception to only the required application, sources, and destinations. Consider rewriting custom applications so they use the application default port.

Step 6: Commit the Configuration

Step 7: Monitor the Rules

- **Cloned rules:** Monitor the original port-based rule to ensure the application-based rule matches the desired traffic. If applications you want to allow match the port-based rule, add them to the application-based rule or clone another application-based rule for them. When only applications that you don't want on your network match the port-based rule for a reasonable period of time, the cloned rule is robust (it catches all the application traffic you want to control) and you can safely remove it.
- **Rules with added applications:** Because you convert only port-based rules that have a few well-known applications directly to application-based rules, in most cases the rule is solid from the start. Monitor the converted rule to see if the expected traffic matches the rule. If there's less traffic than expected, the rule may not allow all of the necessary applications. If there's more traffic than expected, the rule may allow unwanted traffic. Listen to user feedback. If users can't access applications they need for business purposes, the rule (or another rule) may be too tight.

Sample Questions

72. Which security risks are elevated when port-based Security policy rules are used?
    A. The firewall's resources will be negatively impacted by processing unwanted traffic.
    B. Unwanted applications can get through the firewall, bringing their vulnerabilities with them.
    C. A greater range of threats can be included in packet payloads.
    D. The firewall is more vulnerable to DoS attacks.

©2016-2019, Palo Alto Networks, Inc.

73. What is the Palo Alto Networks suggested process for converting port-based Security policies to use App-ID?
    A. Use the Expedition tool to analyze Traffic logs against Security policy to suggest policy changes.
    B. Use the built-in firewall reports to identify applications found in the traffic and update policy based on desired traffic.
    C. Use the Policy Optimizer feature of the firewall to identify applications and update policy rules.
    D. Use the firewall's New Applications Seen feature to identify applications and update policy rules.
74. If App-ID is implemented in Security policy rules, should port numbers also be included?
    A. No, App-ID-based Security policy rules detect and allow or block any desired application using the included port number values in the App-ID database.
    B. Yes, including the port numbers as a *service*-matching condition can eliminate some traffic before App-ID processing, conserving firewall resources.
    C. Yes, including an *application-default* setting in the *service*-matching condition requires that applications use only known or typical port numbers.
    D. No, App-ID based Security policy rules detect and allow or block any desired application using the edited port number values in the App-ID database.

©2016-2019, Palo Alto Networks, Inc.

2.5 Identify how to create security rules to implement App-ID without relying on port-based rules

App-ID vs. Port-Based Security

Security policy rules based on evaluation of protocol type and port numbers are not accurate enough to effectively control application access through your firewall. Many applications use alternate or even multiple port numbers, which makes their detection even more difficult. For instance, allowing TCP port 80 provides access for all web-based applications with their associated vulnerabilities.

Palo Alto Networks App-ID technology provides for positive identification of applications regardless of port usage. This makes possible the safe access enablement for only required access to only the users that require them. This practice reduces your attack surface by eliminating the potentially vulnerable traffic of unwanted applications.

Moving from Port-Based to App-ID Security

Moving from a port-based Security policy to an application-based Security policy may seem like a daunting task. However, the security risks of staying with a port-based policy far outweigh the effort required to implement an application-based policy. And, although legacy port-based Security policies may have thousands of rules (many of which have an unknown purpose), a best practice policy has a streamlined set of rules that align with your business goals, simplifying administration and reducing the chance of error. Because the rules in an application-based policy align with your business goals and acceptable use policies, you can quickly scan the policy to understand the reason for every rule.

As with any technology, there usually is a gradual approach to a complete implementation that consists of carefully planned deployment phases to make the transition as smooth as possible, with minimal impact to your end users. The general workflow for implementing a best practice internet gateway Security policy is as follows:

- Assess your business and identify what you need to protect: The first step in deploying a security architecture is to assess your business and identify your most valuable assets and the greatest threats to those assets. For example, if you are a technology company, your intellectual property is your most valuable asset. In this case, one of your biggest threats would be source code theft.
- Segment your network using interfaces and zones: Traffic cannot flow between zones unless there is a Security policy rule to allow it. One of the easiest defenses against lateral movement of an attacker that has made its way into your network is to define granular zones and allow access only to the specific user groups that need to access an application or resource in each zone. By segmenting your network into granular zones, you can prevent an attacker from establishing a communication channel within your network (either via malware or by exploiting legitimate applications), thereby reducing the likelihood of a successful attack on your network.
- Identify whitelist applications: Before you can create an internet gateway best practice Security policy, you must have an inventory of the applications you want to allow on your network and you must distinguish between those applications you administer and officially sanction and those that you want users to be able to use safely. After you identify the applications (including general types of applications) you want to allow, you can map them to specific best practice rules.
- Create user groups for access to whitelist applications: After you identify the applications you plan to allow, you must identify the user groups that require access to each one. Because

©2016-2019, Palo Alto Networks, Inc.

compromising an end user's system is one of the cheapest and easiest ways for an attacker to gain access to your network, you can greatly reduce your attack surface by allowing access only to applications to the user groups that have a legitimate business need.

- Decrypt traffic for full visibility and threat inspection: You can't inspect traffic for threats if you can't see it. And today SSL/TLS traffic flows account for 40 percent or more of the total traffic on a typical network. This is precisely why encrypted traffic is a common way for attackers to deliver threats. For example, an attacker may use a web application such as Gmail, which uses SSL encryption, to email an exploit or malware to employees accessing that application on the corporate network. Or, an attacker may compromise a website that uses SSL encryption to silently download an exploit or malware to site visitors. If you are not decrypting traffic for visibility and threat inspection, you are leaving a very large surface open for attack.
- Create best practice Security Profiles for the internet gateway: Command-and-control traffic, CVEs, drive-by downloads of malicious content, phishing attacks, APTs all are delivered via legitimate applications. To protect against known and unknown threats, you must attach stringent Security Profiles to all Security policy allow rules.
- Define the initial internet gateway Security policy: Using the application and user group inventory you conducted, you can define an initial policy that allows access to all of the applications you want to whitelist by user or user group. The initial policy rulebase you create also must include rules for blocking known malicious IP addresses, temporary rules to prevent other applications you might not have known about from breaking, and identification of policy gaps and security holes in your existing design.
- Monitor and fine-tune the policy rulebase: After the temporary rules are in place, you can begin monitoring traffic that matches to them so that you can fine-tune your policy. Because the temporary rules are designed to uncover unexpected traffic on the network, such as traffic running on non-default ports or traffic from unknown users, you must assess the traffic matching these rules and adjust your application allow rules accordingly.
- Remove the temporary rules: After a monitoring period of several months, you should see less and less traffic hitting the temporary rules. When you reach the point where traffic no longer hits the temporary rules, you can remove them to complete your best practice internet gateway Security policy.
- Maintain the rulebase: Because the nature of applications is dynamic, you must continually monitor your application whitelist and adapt your rules to accommodate new applications that you decide to sanction and to determine how new or modified App-IDs impact your policy. Because the rules in a best practice rulebase align with your business goals and leverage policy objects for simplified administration, adding support for a new sanctioned application or new or modified App-ID often is as simple as adding or removing an application from an application group or modifying an application filter.

©2016-2019, Palo Alto Networks, Inc.

Palo Alto Networks has developed an innovative approach to securing networks that identifies all traffic by applications using a variety of techniques. This approach replaces conventional approaches that attempt to control traffic based on port numbers.

See the previous section, *2.4 Implement and maintain the App-ID lifecycle*, for a complete description of features and their usage for converting port-based rules to use App-ID.

A web-based App-ID listing of all the existing App-IDs can be found here:
https://applipedia.paloaltonetworks.com/

Sample Questions

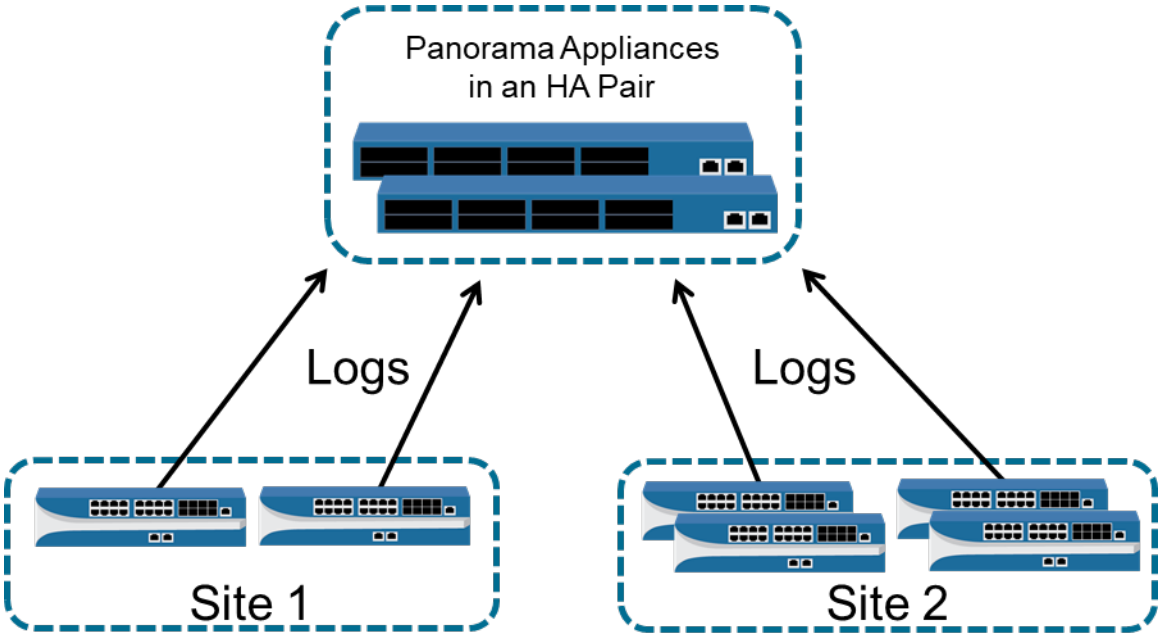
75. Which two applications cannot be identified by port number?
    A. Microsoft Outlook Express email
    B. Google mail (Gmail)
    C. SSH
    D. Facebook
    E. FTP
76. An administrator creates a Security policy rule that allows office-on-demand traffic through the firewall. When the change is committed the firewall issues the following warning:
    "vsys1: Rule 'Allow Office apps' application dependency warning:
    Application 'office-on-demand' requires 'ms-office365-base' be allowed
    Application 'office-on-demand' requires 'sharepoint-online' be allowed
    Application 'office-on-demand' requires 'ssl' be allowed
    Application 'office-on-demand' requires 'web-browsing' be allowed"
    Which action should the administrator take?
    A. Create an application chain that include the dependencies
    B. Add the listed applications to the same Security policy rule
    C. set the Service action of the rule to "dependent application default"
    D. create a new Security policy rule for each listed application with an "allow" action higher in the rule list

©2016-2019, Palo Alto Networks, Inc.

2.6 Identify configurations for distributed Log Collectors

Simple Log Collection Deployment

Logs are forwarded to the Panorama appliances in an HA pair.
The secondary Panorama appliance in HA can be used to store logs.



Note: In an HA pair, when both the Panorama VMs are operating in Panorama mode, the same log (from the firewalls) is sent to the active and passive Panorama appliances. Therefore, the log basically is replicated between the active and the passive appliances of the HA pair. This deployment option is recommended if the firewalls generate up to 10,000 logs per second.

Log Collector Deployment

Dedicated Log Collectors are M-600, M-500, M-200, or M-100 appliances in Log Collector mode. Because they perform only log collection, not firewall management, Dedicated Log Collectors allow for a more robust environment than local Log Collectors. Dedicated Log Collectors provide the following benefits:

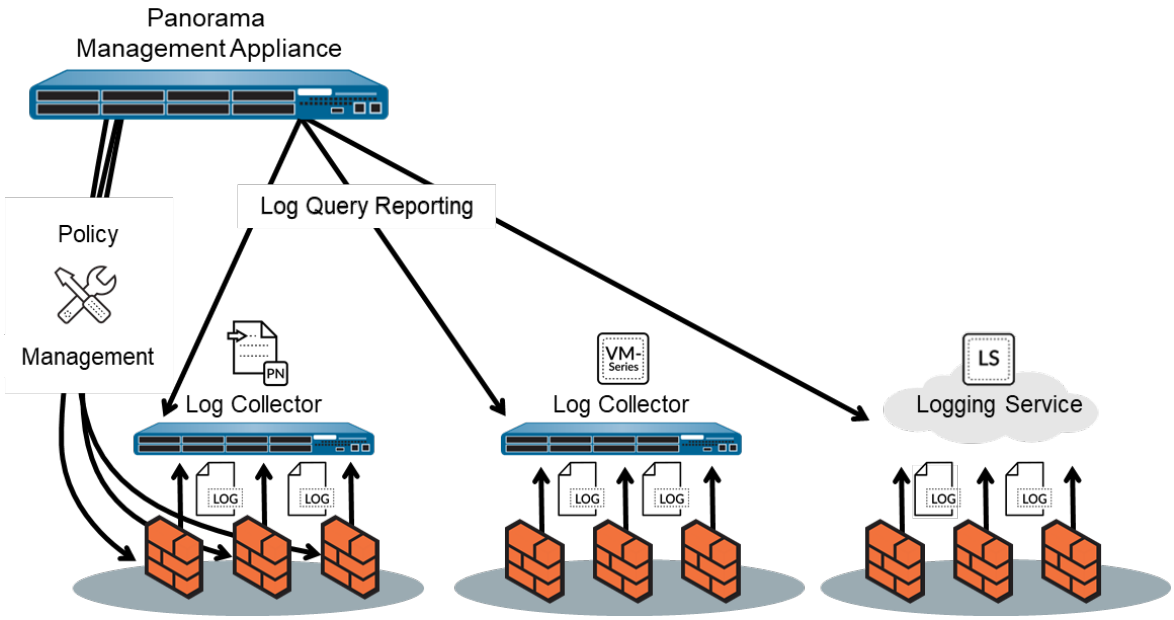
- Enable the Panorama management server to use more resources for management functions instead of logging
- Provide high-volume log storage on a dedicated hardware appliance
- Enable higher logging rates
- Provide horizontal scalability and redundancy with RAID 1 storage
- Optimize bandwidth resources in networks where more bandwidth is available for firewalls to send logs to nearby Log Collectors than to a remote Panorama management server
- Enable you to meet regional regulatory requirements (for example, regulations might not allow logs to leave a particular region)

The Panorama management appliance always maintains management responsibility of the managed firewalls. Firewalls are configured to forward their logs to specific Log Collectors, where they are aggregated. The Panorama management appliance then sends queries to the Log Collectors to gather the

©2016-2019, Palo Alto Networks, Inc.

data that is required for centralized log views and reporting purposes. Logging data remains in the Log Collectors and never is transmitted to the Panorama management appliance.

Log Collectors must be made a member of a Log Collector Group to be configured and receive forwarded log events.



Log Collector Groups

Log Collectors are members of *Log Collector Groups*. A Log Collector Group can have more than one Log Collector device as a member. Log Collectors must meet the following requirements before they can become members of the same group:

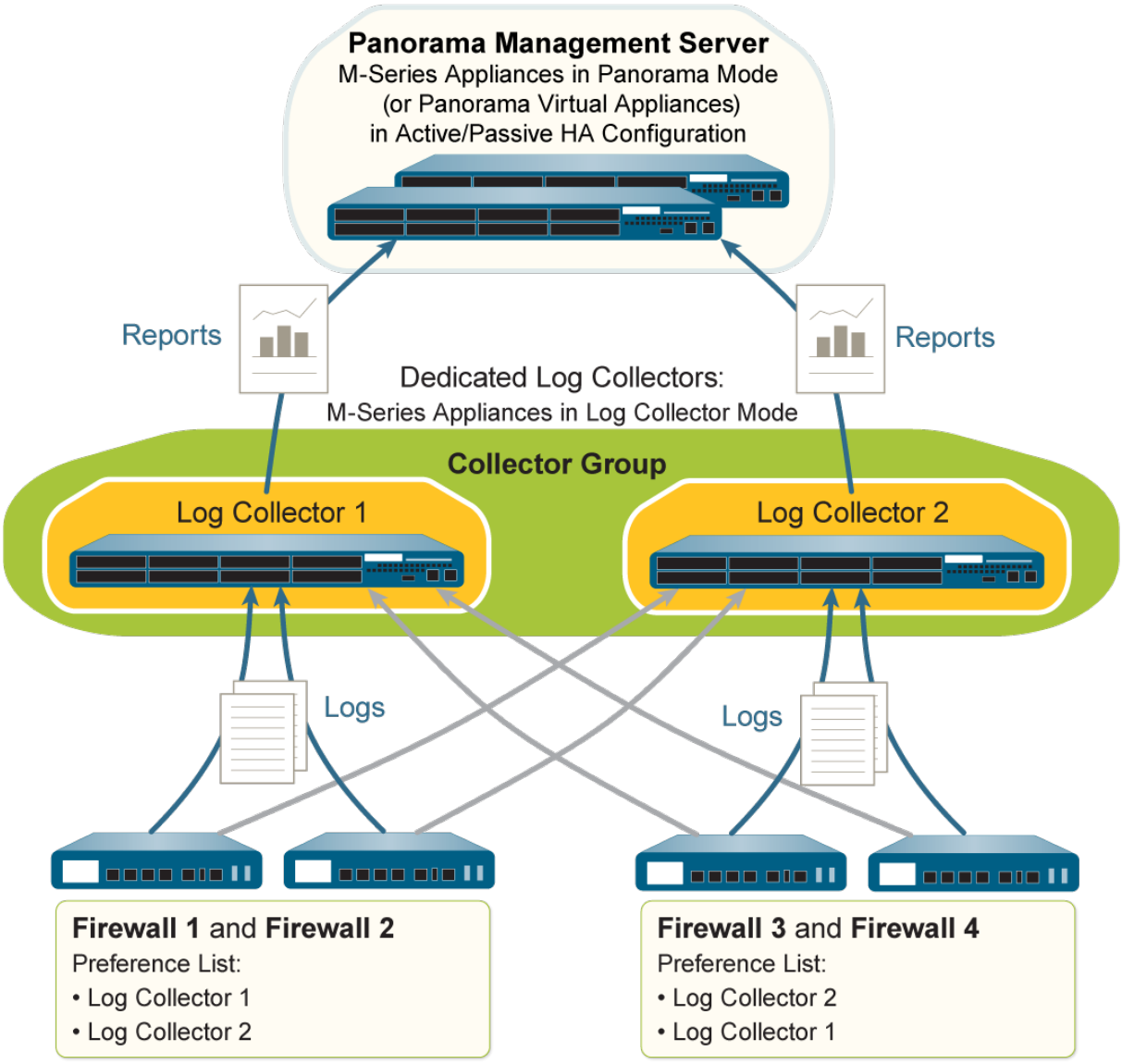
- In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-600 appliances, all M-500 appliances, all M-200, all M-100 appliances, or all Panorama virtual appliances.
- Log redundancy is available only if each Log Collector has the same number of logging disks. Disks can be added to Log Collectors with remaining expansion capacity.
- (Best Practice) All Log Collectors in the same Collector Group should be in the same local-area network (LAN). Avoid adding Log Collectors in the same or different wide-area networks (WANs) to the same Collector Group because network disruption is much more common and may result in log data loss. Additionally, it is recommended that Log Collectors in the same Collector Group should be physically near each other to allow Panorama to quickly query the Log Collectors when needed.

Log Collectors in a Log Collector group appear as a single logical entity to devices forwarding logs. The Log Collector Group makes local log storage location decisions when multiple platforms are present, thus eliminating the need for an administrator to configure specific log storage behavior other than the optional use of *log redundancy* within the collector group.

When a Log Collector Group contains more than one Log Collector, firewalls can be configured to use a priority-based list of specific collectors within the group to use as logging destinations. The firewall automatically fails over to the next entry on the list when it cannot reach the preferred Log Collector.

©2016-2019, Palo Alto Networks, Inc.

Firewalls also can be configured to use alternate collector groups as logging destinations when all Log Collectors of a preferred Log Collector Group become unavailable.



Cortex Data Lake (Formerly Logging Service)

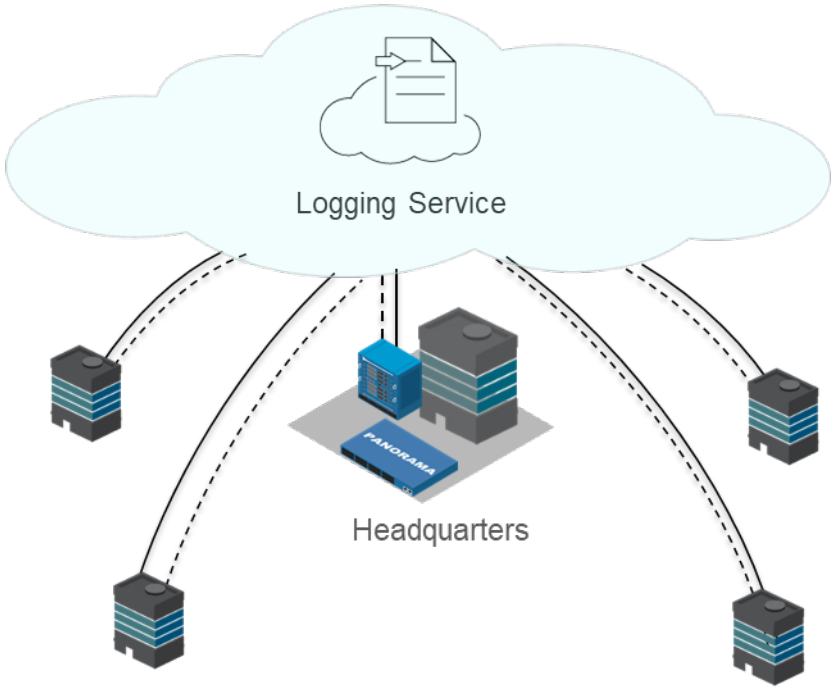
The Logging Service provides cloud-based, centralized log storage and aggregation for your on-premises and virtual (private cloud and public cloud) firewalls that can augment existing Log Collectors or function as deployed Log Collectors. Panorama provides the interface for the logs stored in the Logging Service, and it can show you an aggregated view of all logs stored there. You can generate reports and perform log analysis and forensics on the log data.

Cortex Data Lake is the central repository of all the logs generated from firewalls and the Traps endpoint server. It initiates queries, generates reports, and analyzes logs stored in the cloud via Panorama. It also enables reporting, log viewing, and many other analytics-based applications on your logs. The Logging Service offers you flexible options to expand storage and log ingestion rates on demand, without the need for you to buy new hardware or manually provision new virtual machines.

©2016-2019, Palo Alto Networks, Inc.

The Logging Service provides the following functionality:

- Isolation: Your data is isolated to avoid any cross-contamination from the data of other customers.
- Redundancy: Multiple copies of your log database are stored to ensure redundancy.
- Regionalization: Logging facilities are in the Americas and Europe. You choose where to forward your data.
- Scalability: You can start with storage you need now and scale up as your storage needs grow.



©2016-2019, Palo Alto Networks, Inc.

Sample Question

77. Which two options will provide an enterprise-wide log that can be viewed from Panorama?
    A. Select firewalls are designated as Log Collectors and add logs forwarded from other firewalls to their own.
    B. Panorama devices are configured as Dedicated Log Collectors that then are added to Log Collector Groups. Firewalls forward logs to a designated Log Collector within a Collector Group.
    C. Cortex Data Lake is configured as a Log Collector in Panorama. Firewalls forward logs to Cortex Data Lake.
    D. A Panorama device is configured in Management Mode and a Log Collector is defined on the Panorama appliance, which then is added to a Log Collector Group. Firewalls forward logs to a designated Log Collector within a Collector Group.

©2016-2019, Palo Alto Networks, Inc.

2.7 Identify the required settings and steps necessary to provision and deploy a next-generation firewall

By default, the firewall has an IP address of 192.168.1.1 and a username/password of admin/admin. For security reasons, you must change these settings before continuing with other firewall configuration tasks. You must perform these initial configuration tasks either from the MGT interface, even if you do not plan to use this interface for your firewall management, or by using a direct serial connection to the console port on the device.

Steps to Connect the Firewall

You can connect to the firewall in one of the following ways:

- Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete. When the device is ready, the prompt changes to the name of the firewall, for example, PA-500 login.
- Connect an RJ-45 Ethernet cable from your computer to the MGT port on the firewall. From a browser, go to https://192.168.1.1. Note that you may need to change the IP address on your computer to an address in the 192.168.1.0 network, such as 192.168.1.2, to access this URL.

For more information, see the initial sections at this link:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started

Installing and Activating Licenses

The next configuration steps involve installing the proper licenses and activating subscriptions on the firewall. Use the resulting access to update PAN-OS software and dynamic update files as required.

You can activate licenses first on the Palo Alto Networks website and then communicate them to the firewall (assuming internet connectivity from the Management port). If connectivity is not available, you can enter licenses directly.

See this information for details:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/register-the-firewall.html

Dynamic Updates

These activated licenses provide access to PAN-OS software updates and Subscription data files (dynamic updates). The following information explains these licenses and the process for updating files and PAN-OS software:

Dynamic updates are explained here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html

Downloading and configuring them for automatic update is discussed here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/install-

©2016-2019, Palo Alto Networks, Inc.

content-and-software-updates.html

Firewall Configuration

After these initial deployment steps are taken, configuration becomes a task of implementing network connectivity and security settings to meet your specific requirements. These next steps can vary widely. A complete discussion with implementation guidance is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/register-the-firewall.html

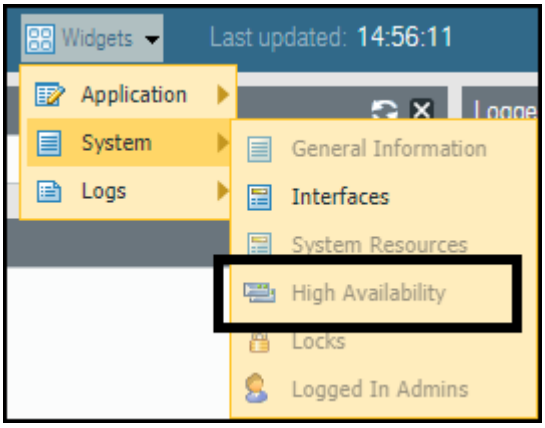
Sample Questions

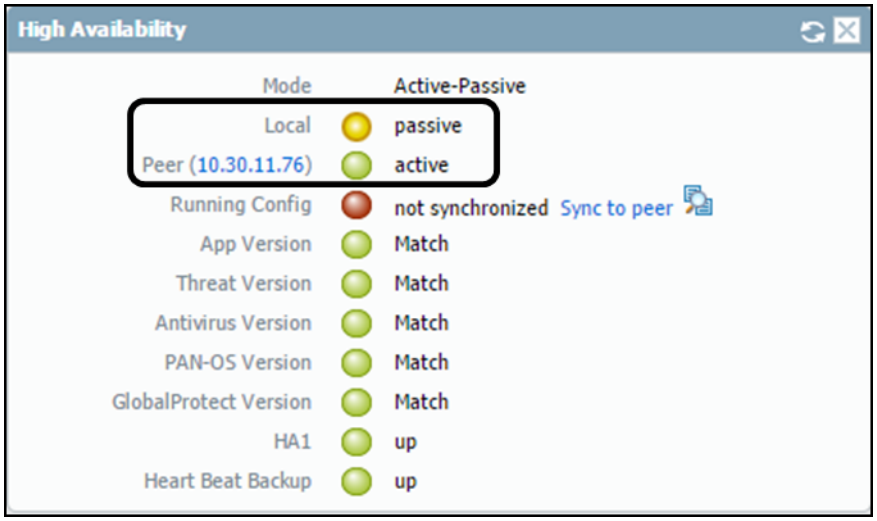
78. You finished configuring the firewall's basic connectivity in the lab and are ready to put it in the data center. What do you have to remember to do before you power down the firewall?
    A. Save the changes.
    B. Commit the changes.
    C. Create a restore thumb drive in case the configuration is deleted.
    D. Verify that the configuration is correct. You do not need to do anything else if it is correct; the configuration is updated automatically.
79. The Management port on a firewall can be configured as which type of interface?
    A. Layer 2
    B. Layer 3
    C. virtual wire
    D. serial

©2016-2019, Palo Alto Networks, Inc.

2.8 Identify which device of an HA pair is the active partner

Two Palo Alto Networks firewalls are configured as a *High Availability* (HA) pair can be deployed in an *active/passive* or *active/active* configuration. Palo Alto Networks provides an easy-to-use widget on the web interface **Dashboard** tab to monitor the status of the HA pair. Regardless of the deployment type, this widget will identify which firewalls of the HA pair are active and processing traffic.





The preceding figure identifies the firewall being viewed as the passive partner of an active/passive HA configuration.

©2016-2019, Palo Alto Networks, Inc.

Sample Question

80. Which two steps must be completed to enable the display of the High Availability widget?
    A. Log in to the firewall management web interface and configure HA for active/active or active/passive.
    B. Log in to the firewall management web interface and press the **Sync to peer** link in the firewall HA configuration settings.
    C. Log in to the firewall's CLI and enter the **`get management-server logging on`** command.
    D. Select and enable the **High Availability** widget in the firewall's management web interface **Dashboard** display.

©2016-2019, Palo Alto Networks, Inc.

2.9 Identify various methods for authentication, authorization, and device administration within PAN-OS software for connecting to the firewall

See section *1.12 Identify methods for authorization, authentication, and device administration*.

©2016-2019, Palo Alto Networks, Inc.

2.10 Identify various methods for authentication, authorization, and device administration within PAN-OS software for connecting to services through the firewall

Protecting Service Access Through the Firewall

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a webpage), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or one-time password (OTP) authentication. For the first factor, users authenticate through a Captive Portal web form. For any additional factors, users authenticate through a multi-factor authentication (MFA) login page.

After the user authenticates for all factors, the firewall evaluates Security policy to determine whether to allow access to the service or application.

To reduce the frequency of authentication challenges that interrupt the user workflow, you can specify a timeout period during which a user authenticates only for initial access to services and applications, not for subsequent access. Authentication policy integrates with Captive Portal to record the timestamps used to evaluate the timeout and to enable user-based policies and reports.

Based on user information that the firewall collects during authentication, User-ID creates a new IP address-to-username mapping or updates the existing mapping for that user (if the mapping information has changed). The firewall generates User-ID logs to record the additions and updates. The firewall also generates an Authentication log for each request that matches an Authentication rule. If you favor centralized monitoring, you can configure reports based on User-ID or Authentication logs and forward the logs to Panorama or external services as you would for any other log types.

Configuring Authentication Policy

Perform the following steps to configure Authentication policy for end users who access services through Captive Portal. Before starting, ensure that your Security Policy allows users to access the services and URL categories that require authentication.

1. Configure Captive Portal. If you use MFA services to authenticate users, you must set the **Mode** to **Redirect**.
2. Configure the firewall to use one of the following services to authenticate users.
    - External Authentication Services: Configure a Server Profile to define how the firewall connects to the service.
    - Local database authentication: Add each user account to the local user database on the firewall.
    - Kerberos single sign-on (SSO)—Create a Kerberos keytab for the firewall. You can configure the firewall to use Kerberos SSO as the primary authentication service and, if SSO failures occur, fall back to an external service or local database authentication.

©2016-2019, Palo Alto Networks, Inc.

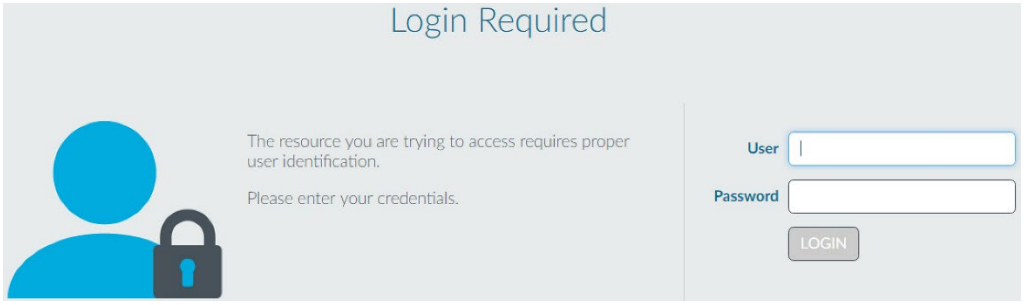
3. Configure an Authentication Profile and sequence for each set of users and Authentication policy rules that require the same authentication services and settings.
   Select the **Type** of authentication service and related settings:
   - **External service:** Select the **Type** of external server and select the **Server Profile** you created for it.
   - **Local database authentication:** Set the **Type** to **Local Database**. In the **Advanced** settings, **Add** the Captive Portal users and user groups you created.
   - **Kerberos SSO:** Specify the **Kerberos Realm** and **Import** the **Kerberos Keytab**.
4. Configure an Authentication Enforcement object.
   The object associates each Authentication Profile with a Captive Portal method. The method determines whether the first authentication challenge (factor) is transparent or requires a user response.
   - Select **Objects > Authentication** and **Add** an object.
   - Enter a **Name** to identify the object.
   - Select an **Authentication Method** for the authentication service **Type** you specified in the Authentication Profile:
     - **browser-challenge:** Select this method if you want the client browser to respond to the first authentication factor instead of having the user enter login credentials. For this method, you must have configured Kerberos SSO in the Authentication Profile or NT LAN Manager (NTLM) authentication in the Captive Portal settings. If the browser challenge fails, the firewall falls back to the web-form method.
     - **web-form:** Select this method if you want the firewall to display a Captive Portal web form for users to enter login credentials.
   - Select the **Authentication Profile** you configured.
   - Enter the **Message** that the Captive Portal web form will display to tell users how to authenticate for the first authentication factor.
   - Click **OK** to save the object.
5. Configure an Authentication policy rule.
   Create a rule for each set of users, services, and URL categories that require the same authentication services and settings.
   - Select **Policies > Authentication** and **Add** a rule.
   - Enter a **Name** to identify the rule.
   - Select **Source** and **Add** specific zones and IP addresses or select **Any** zones or IP addresses.
     The rule applies only to traffic coming from the specified IP addresses or from interfaces in the specified zones.
   - Select **User** and select or **Add** the source users and user groups to which the rule applies (default is **any**).
   - Select or **Add** the **Host Information Profiles** to which the rule applies (default is **any**).
   - Select **Destination** and **Add** specific zones and IP addresses or select **any** zones or IP

©2016-2019, Palo Alto Networks, Inc.

addresses.
The IP addresses can be resources (such as servers) for which you want to control access.

- Select **Service/URL Category** and select or **Add** the **services and service groups** for which the rule controls access (default is **service-http**).
- Select or **Add** the **URL Categories** for which the rule controls access (default is **any**). For example, you can create a custom URL category that specifies your most sensitive internal sites.
- Select **Actions** and select the **Authentication Enforcement** object you created.
- Specify the **Timeout** period in minutes (default 60) during which the firewall prompts the user to authenticate only once for repeated access to services and applications.
- Click **OK** to save the rule.

6. (MFA only) Customize the MFA login page.
   - The firewall displays this page so that users can authenticate for any additional MFA factors.
7. Verify that the firewall enforces Authentication policy.
   - Log in to your network as one of the source users specified in an Authentication policy rule.
   - Request a service or URL category that matches one specified in the rule.
     The firewall displays the Captive Portal web form for the first authentication factor. For example:



   - End the session for the service or URL you just accessed.
   - Start a new session for the same service or application. Be sure to perform this step within the **Timeout** period you configured in the Authentication rule.
     The firewall allows access without re-authenticating.
   - Wait until the **Timeout** period expires and request the same service or application.
     The firewall prompts you to re-authenticate.
8. (Optional) Redistribute user mappings and authentication timestamps to other firewalls that enforce Authentication policy to ensure they all apply the timeouts consistently for all users.

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

81. Which objects ties together Captive Portal method with an authentication profile when configuring multifactor authentication?
    A. Multi-Factor Authentication Server Profile
    B. Authentication policy rule
    C. authentication sequence
    D. Authentication Enforcement object
82. Which four firewall Server Profiles can provide first factor authentication for multi-factor authentication configurations? (Choose four.)
    A. HTTP
    B. Okta
    C. PingID
    D. Kerberos
    E. RADIUS
    F. SAML
    G. LDAP
    H. RSA SecureID Access

©2016-2019, Palo Alto Networks, Inc.

2.11 Identify how to configure and maintain certificates to support firewall features

Certificate Management

Certificates are used for a variety of purposes in Palo Alto Networks firewalls: securing SSL encryption, authenticating connections, and authenticating other SSL certificates. To augment certificate handling, the Palo Alto Networks firewall provides certificate management functions including import, export, and certificate creation.

A discussion of certificate use and management is here:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management

An exploration of many SSL certificate-related technical issues, including implementation and troubleshooting, is here:
https://live.paloaltonetworks.com/t5/Management-Articles/SSL-certificates-resource-list/ta-p/53068

Sample Question

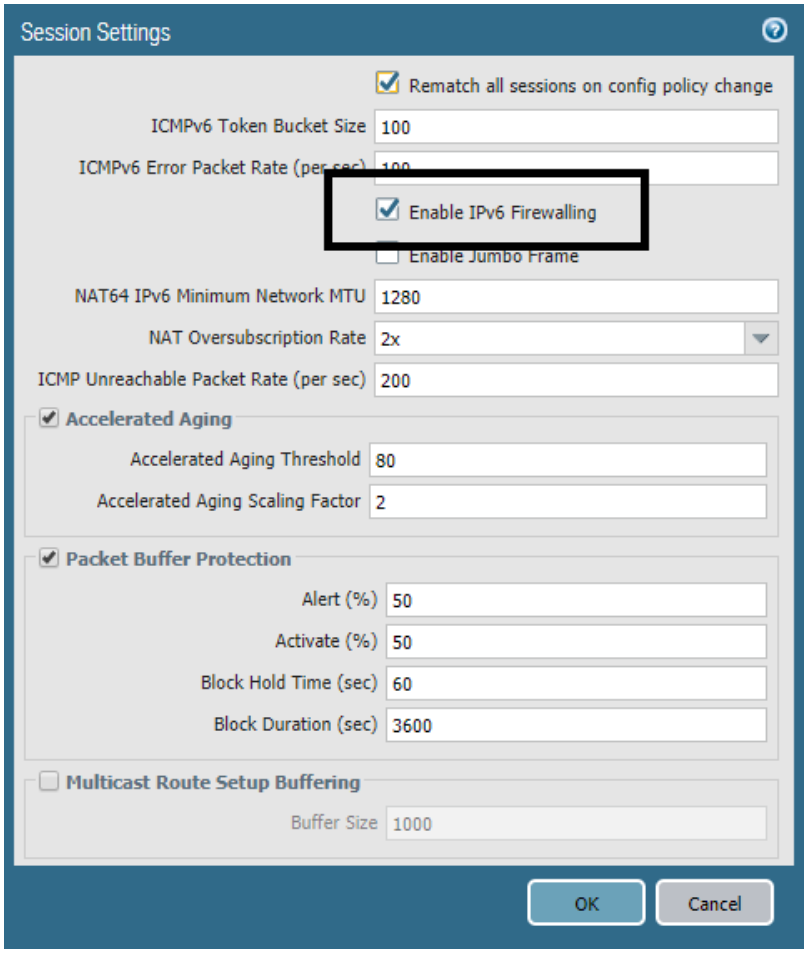
83. Administrators within the enterprise want to replace the default certificate used by the firewall to secure the management web interface traffic with a certificate generated by their existing certificate authority. Which certificate property must be set for their new certificate to function?
    A. Certificate CN set to a domain name that resolves to any traffic port address of the firewall.
    B. Certificate must be signed by the firewall root certificate.
    C. Certificate must have the **Forward Trust Certificate** property set.
    D. CN must be set to the management port of the firewall.

©2016-2019, Palo Alto Networks, Inc.

2.12 Identify the features that support IPv6

Firewall Support of IPv6

Palo Alto Networks firewalls support IPv6 addressing by implementing dual protocol stacks (IPv4 and IPv6) that simultaneously service many features of the firewall. Each firewall has a master switch that enables IPv6 support that is on by default. Navigate to **Device > Setup > Session > Session Settings** to find the following:



©2016-2019, Palo Alto Networks, Inc.

The following table lists the features that supports IPv6 when IPv6 is enabled on a firewall:

PAN-OS FEATURE	PAN-OS 7.1	PAN-OS 8.0	PAN-OS 8.1	PAN-OS 9.0
Security				
App-ID and firewalling in Layer 2 and Layer 3	✓	✓	✓	✓
User-ID	✓	✓	✓	✓
Content-ID	✓	✓	✓	✓
Block IPv6 in IPv4 tunneling (via App-ID)	✓	✓	✓	✓
Zone protection	✓	✓	✓	✓
Packet-based attack protection	—	✓	✓	✓
Reconnaissance protection	✓	✓	✓	✓
URL filtering	✓	✓	✓	✓
SSL decryption	✓	✓	✓	✓
SSH decryption	✓	✓	✓	✓
DoS rulebase	✓	✓	✓	✓
IPv6 access to PAN-DB	✓	✓	✓	✓
DNS Sinkhole	✓	✓	✓	✓
External Dynamic List (EDL)	✓	✓	✓	✓
Management and Panorama				
SSH management (dedicated MGMT port)	✓	✓	✓	✓
Web interface management (dedicated MGMT port)	✓	✓	✓	✓
Interface management (ping, telnet, ssh, http, https: all ports)	✓	✓	✓	✓
Device to Panorama SSL TCP connection	✓	✓	✓	✓
Panorama HA connection between peers	—	✓	✓	✓
DNS	✓	✓	✓	✓

©2016-2019, Palo Alto Networks, Inc.

PAN-OS FEATURE	PAN-OS 7.1	PAN-OS 8.0	PAN-OS 8.1	PAN-OS 9.0
Dynamic DNS support for firewall interfaces (DHCP-based interfaces)	—	—	—	✓
RADIUS	✓	✓	✓	✓
LDAP	✓	✓	✓	✓
SYSLOG	✓	✓	✓	✓
SNMP	✓	✓	✓	✓
NTP	✓	✓	✓	✓
Device DNS (device only)	✓	✓	✓	✓
DNS proxy	✓	✓	✓	✓
Reporting and visibility into IPv6	✓	✓	✓	✓
IPv6 address objects	✓	✓	✓	✓
IPv6 FQDN address objects	✓	✓	✓	✓
Networking				
IPv6 static routes	✓	✓	✓	✓
PBF	✓	✓	✓	✓
PBF next hop monitor (v6 endpoint)	✓	✓	✓	✓
OSPFv3	✓	✓	✓	✓
MP-BGP	—	✓	✓	✓
GRE tunneling support	—	—	—	✓
ECMP	✓	✓	✓	✓
Dual stack support for L3 interfaces	✓	✓	✓	✓
QoS policy	✓	✓	✓	✓
QoS marking	✓	✓	✓	✓
DSCP (session based)	✓	✓	✓	✓
Neighbor discovery and duplicate address detection	✓	✓	✓	✓
Tunnel content inspection	—	✓	✓	✓
Virtual wires	✓	✓	✓	✓
NPTv6 (stateless prefix translation)	✓	✓	✓	✓
NAT64 (IP-IPv6 protocol translation)	✓	✓	✓	✓

©2016-2019, Palo Alto Networks, Inc.

PAN-OS FEATURE	PAN-OS 7.1	PAN-OS 8.0	PAN-OS 8.1	PAN-OS 9.0
Link Layer Discovery Protocol (LLDP)	✓	✓	✓	✓
Bidirectional Forwarding Detection (BFD)	✓	✓	✓	✓
VPN				
GlobalProtect	—	✓	✓	✓
IKE/IPsec	✓	✓	✓	✓
IKEv2	✓	✓	✓	✓
IPv6 over IPv4 IPsec tunnel	✓	✓	✓	✓
Large Scale VPN (LSVPN)	—	✓	✓	✓
Host Dynamic Address Configuration				
DHCPv6 relay	✓	✓	✓	✓
SLAAC (router advertisements)	✓	✓	✓	✓
SLAAC (router preference)	✓	✓	✓	✓
SLAAC (RDNSS)	—	✓	✓	✓
Device				
High Availability (HA) - active/active	✓	✓	✓	✓
High Availability (HA) - active/passiv	✓	✓	✓	✓
High Availability (HA): IPv6 transport for HA1 and HA2	✓	✓	✓	✓
High Availability (HA) path monitoring (IPv6 Endpoint)	✓	✓	✓	✓
User-ID				
Map IPv6 address to users	✓	✓	✓	✓
Captive Portal for IPv6	✓	✓	✓	✓
Connection to User-ID agents over IPv6	✓	✓	✓	✓
User-ID XML API for IPv6	✓	✓	✓	✓

©2016-2019, Palo Alto Networks, Inc.

PAN-OS FEATURE	PAN-OS 7.1	PAN-OS 8.0	PAN-OS 8.1	PAN-OS 9.0
Terminal Servers agent IPv6	✓	✓	✓	✓

Sample Question

84. Which two configuration conditions must be met for a Palo Alto Networks firewall to send and receive IPv6 traffic?
    A. **Enable IPv6** check box in the Virtual Router configuration is checked.
    B. An Ethernet interface is configured for virtual wire.
    C. An Ethernet interface is configured for Layer 3.
    D. **Enable IPv6 Firewalling** check box under **Session Settings** is turned on.

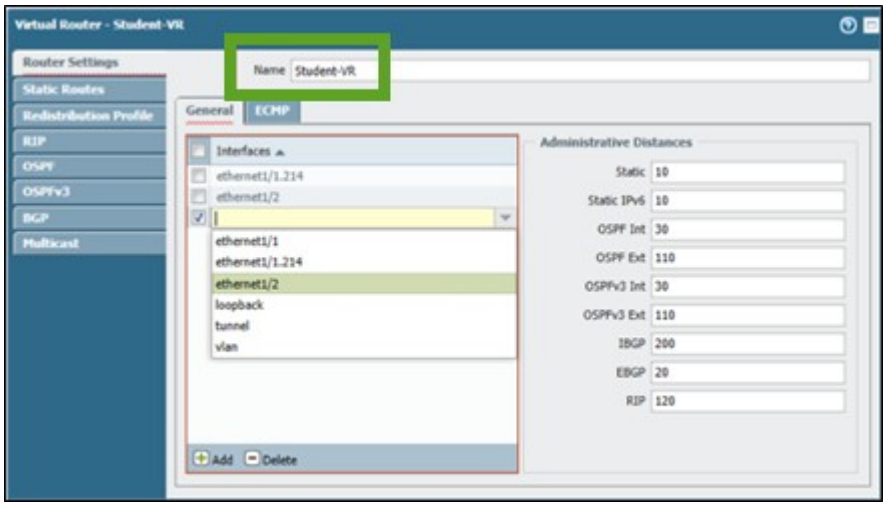
©2016-2019, Palo Alto Networks, Inc.

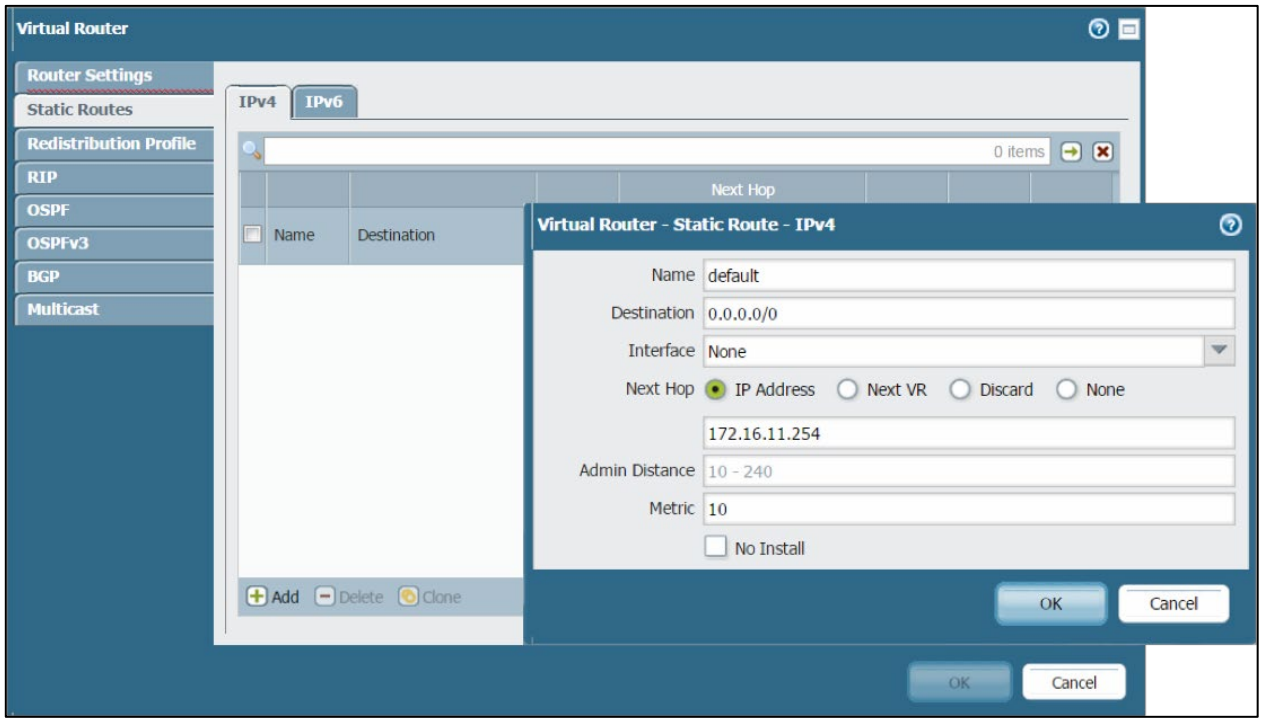
2.13 Identify how to configure a virtual router

Routing Configuration

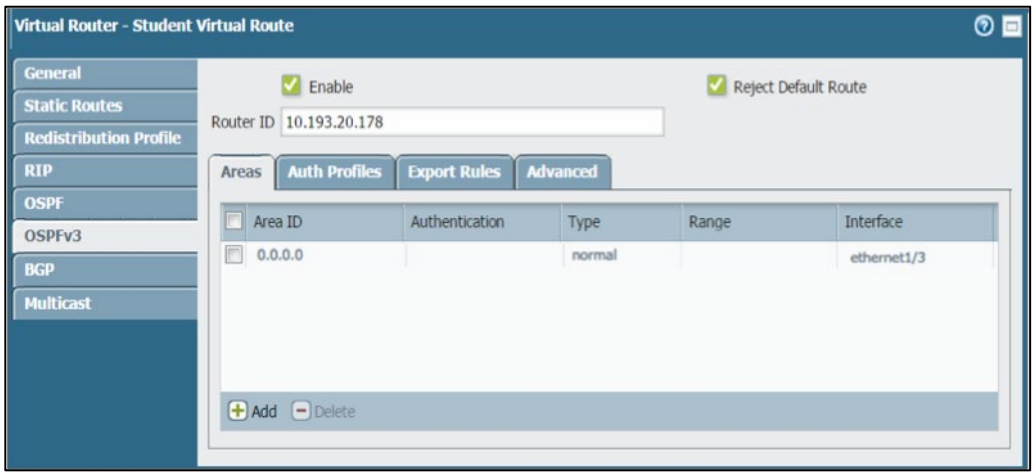
PAN-OS software supports static routes, BGP, OSPF, RIP, and multicast routing configured in the virtual router (VR). There are limitations for the number of entries in the forwarding tables (FIBs) and routing tables (RIBs).

Different platform levels also can support varying numbers of virtual routers. The virtual router configuration is meant to match the existing routing and routed infrastructure. In addition to protocol configuration, Redistribution Profiles can support protocol interoperability.





©2016-2019, Palo Alto Networks, Inc.



A discussion of virtual routers and each of the supported dynamic routing protocols is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-virtual-routers.html

Troubleshooting Routing

The CLI has advanced troubleshooting of routing functions. Output from the **`debug routing`** … command provides insight into router processing, including advanced debugging logs and routing-specific packet captures.

Sample Questions

85. Under which condition can layer 3 interfaces in the same firewall have the same IP address?
    A. they must be connected to different virtual routers.
    B. they must be connected to the same Ethernet network through a switch.
    C. they must be subinterfaces of the same physical interface.
    D. They must be in different zones.

©2016-2019, Palo Alto Networks, Inc.

86. A firewall's virtual router can connect to which three types of interfaces?
    A. virtual wire
    B. management
    C. Layer 3 traffic
    D. HA1
    E. HA2
    F. loopback
    G. tunnel

©2016-2019, Palo Alto Networks, Inc.

2.14 Given a scenario, identify how to configure an interface as a DHCP relay agent

DHCP Overview

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP or IP networks where a DHCP server dynamically assigns an IP address and other network configuration parameters to subscribing devices on a network so they can communicate with other IP networks. DHCP operates in a client-server model where a client broadcasts a DHCP request that then is responded to by the server with previously configured settings. Because the service communication uses network broadcasts, a DHCP server can receive client requests from the local network segment only; DHCP queries cannot normally transit through a router to another network segment.

DHCP and DHCP Relay on the Firewall

A Palo Alto Networks firewall can function as a DHCP server on assigned interfaces. Interfaces also can be configured to listen for DHCP broadcasts and forward them (relay) to other network segments bypassing the broadcast limitation DHCP. This feature ensures that a client needing DHCP services can find them even when connected on other network segments.

Before you can enable a firewall interface to transmit DHCP messages between clients and servers, you must configure the firewall as a DHCP relay agent. The interface can forward messages to a maximum of eight external IPv4 DHCP servers and eight external IPv6 DHCP servers. A client DHCPDISCOVER message is sent to all configured servers, and the DHCPOFFER message of the first server that responds is relayed back to the requesting client.

Before you can configure a DHCP relay agent, make sure that you have configured a Layer 3 Ethernet or Layer 3 VLAN interface, and the interface is assigned to a virtual router and a zone.

1. Select **DHCP Relay**.
   Select **Network > DHCP > DHCP Relay**.
2. Specify the IP address of each DHCP server with which the DHCP relay agent will communicate.
   - In the **Interface** field, select the interface you want to be the DHCP relay agent.
   - Select either **IPv4** or **IPv6**, which indicates the type of DHCP server address you will specify.
   - If you checked **IPv4**, in the **DHCP Server IP Address** field, **Add** the address of the DHCP server to and from which you will relay DHCP messages.
   - If you checked **IPv6**, in the **DHCP Server IPv6 Address** field, **Add** the address of the DHCP server to and from which you will relay DHCP messages. If you specify a multicast address, also specify an outgoing **Interface**.
   - (Optional) Repeat the prior three sub-bullets to enter a maximum of eight DHCP server addresses per IP address family.
3. Commit the configuration.
   Click **OK** and **Commit**.

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

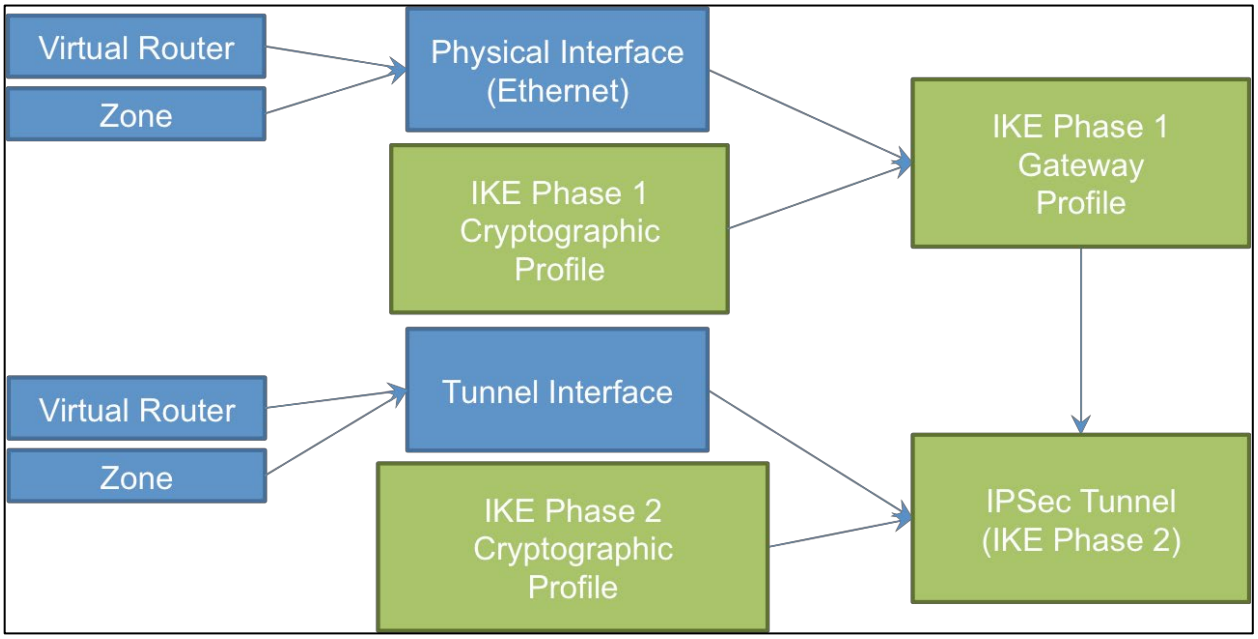
87. A Palo Alto Networks firewall can forward DHCP broadcasts from one network to another?
    A. True
    B. False
88. A Palo Alto Networks firewall can forward DHCP packets to servers connected to which two kinds of networks? (Choose two.)
    A. virtual wire
    B. Layer 2
    C. Layer 3
    D. aggregate
89. How does a Palo Alto Networks firewall configured to forward DHCP packets to multiple server destinations choose which reply to forward to the sender?
    A. The first server listed in the “Server Priority” DHCP configuration is forwarded until it fails to respond, then the next one is chosen.
    B. A request is sent to all servers on the list, and the first responder is forwarded.
    C. All DHCP server responses are forwarded, and the receiving client chooses which to accept.
    D. The server that is the fewest network hops from the requesting client is chosen. When more than one server has the same hop count, all packets from the servers are forwarded to the client.

©2016-2019, Palo Alto Networks, Inc.

2.15 Identify the configuration settings for site-to-site VPN

IPsec Tunnel Interfaces

IPsec VPNs are terminated on Layer 3 tunnel interfaces. (These tunnel interfaces can be put into separate zones, thus allowing specific Security policy per zone.) These tunnels require IPsec and Crypto Profiles for Phase 1 and Phase 2 connectivity. PAN-OS® software supports route-based VPNs, which means that the decision to route traffic through the VPN is made by the virtual router. Palo Alto Networks firewalls support connection to alternate policy-based VPNs requiring the use of proxy IDs for compatibility. The following figure shows the various objects involved in IPsec tunnel definitions.



A complete discussion of required settings is found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/set-up-site-to-site-vpn

CLI Troubleshooting Commands

The CLI has additional **`test`** and **debug** commands for troubleshooting required for configuring and maintaining one or more tunnels. VPN events including errors are posted to the System log. The message quality is more thorough when the firewall is the recipient of VPN negotiation requests from other endpoints.

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

90. Which type is a tunnel interface?
    A. Tap
    B. virtual wire
    C. Layer 2
    D. Layer 3
91. A firewall administrator is rolling out 50 Palo Alto Networks firewalls to protect remote sites. Each firewall must have a site-to-site IPsec VPN tunnel to each of three campus locations. Which configuration function is the basis for automatic site-to-site IPsec tunnels set up from each remote location to the three campuses?
    A. import of a settings table into the remote firewall's IPsec tunnel config
    B. import of a settings table into the IPsec tunnel config of the three campuses
    C. configuration of the GlobalProtect satellite settings of the campus and remote firewalls
    D. entering of campus IPsec tunnel settings for each remote firewall's IPsec Profile

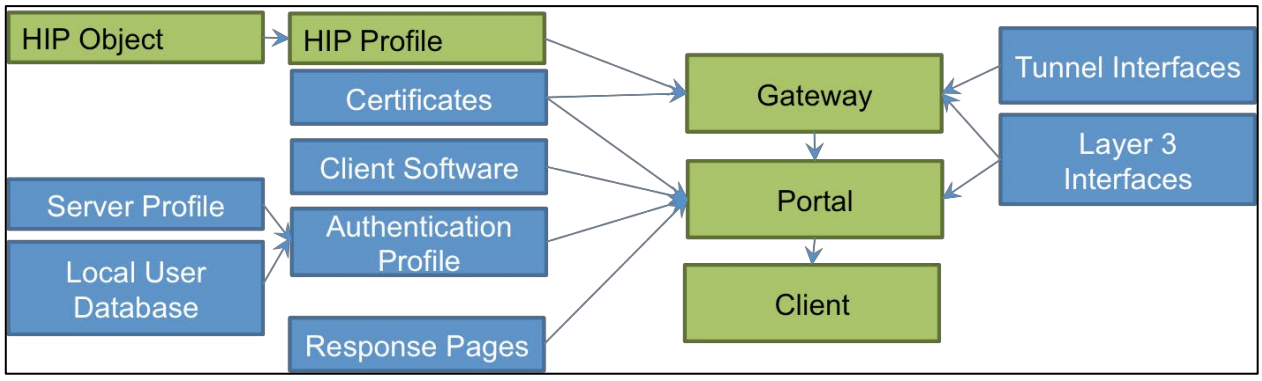
©2016-2019, Palo Alto Networks, Inc.

2.16 Identify the configuration settings for GlobalProtect

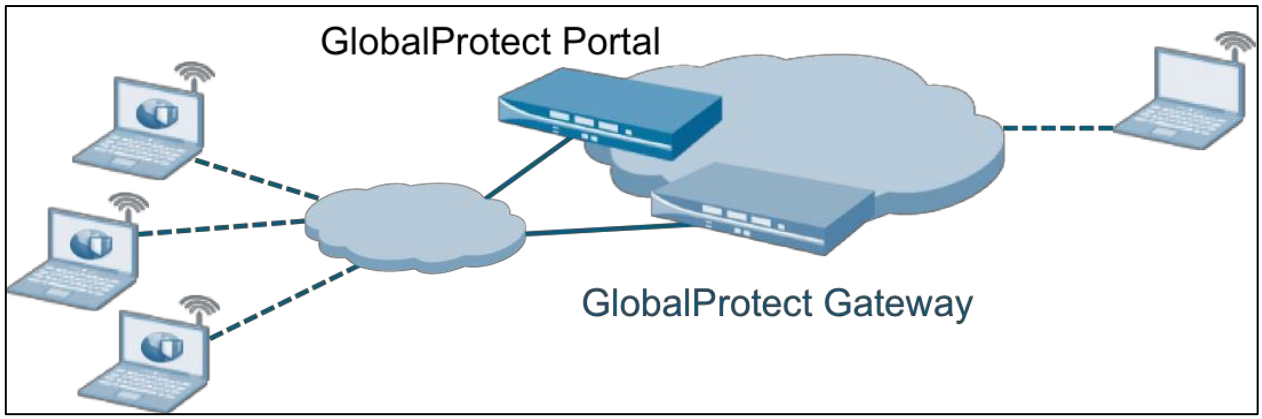
GlobalProtect Overview

GlobalProtect solves the security challenges of roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located. GlobalProtect uses client software to build secure personal VPN tunnels to the firewall.

GlobalProtect comprises many different components. An understanding of those basic components is the starting point for a successful deployment. The GlobalProtect Portal performs the initial authentication of a client, downloads and upgrades the GlobalProtect Client, performs a host information profile (HIP) check (if licensed), and provides a list of GlobalProtect Gateways for user traffic. The GlobalProtect Portal must be enabled on a Layer 3 interface with a reachable IP address. The GlobalProtect Gateway creates and maintains the VPN tunnels for user traffic in SSL or IPsec forms. The GlobalProtect Gateway distributes an IP address to each authenticated user. (This IP-to-username address mapping can be used for effective User-ID in Security policy.) A diagram of the configuration elements follows:



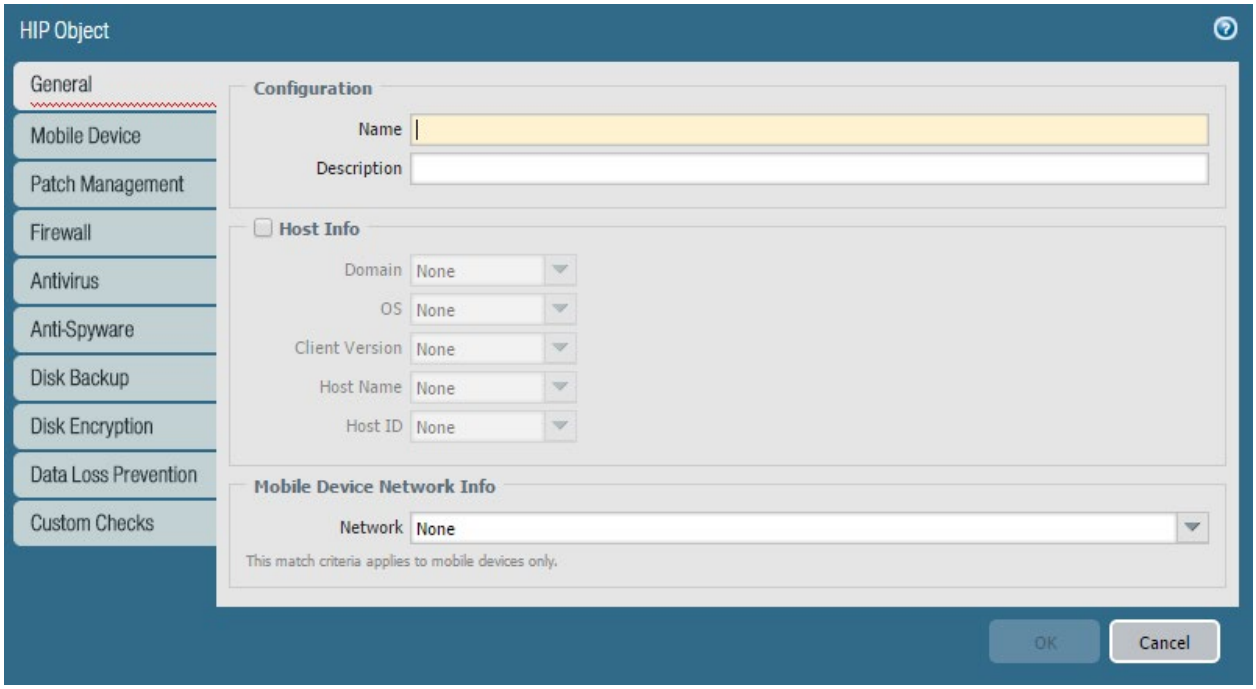
Every Palo Alto Networks firewall can provide GlobalProtect connectivity support to Windows and Mac clients with no additional license requirement. Client software can be downloaded directly from the Portal.



Gateway traffic (SSL or IPsec encryption) can be terminated on a tunnel interface in a separate zone, which allows for specific policies to be enabled for that zone and user(s).

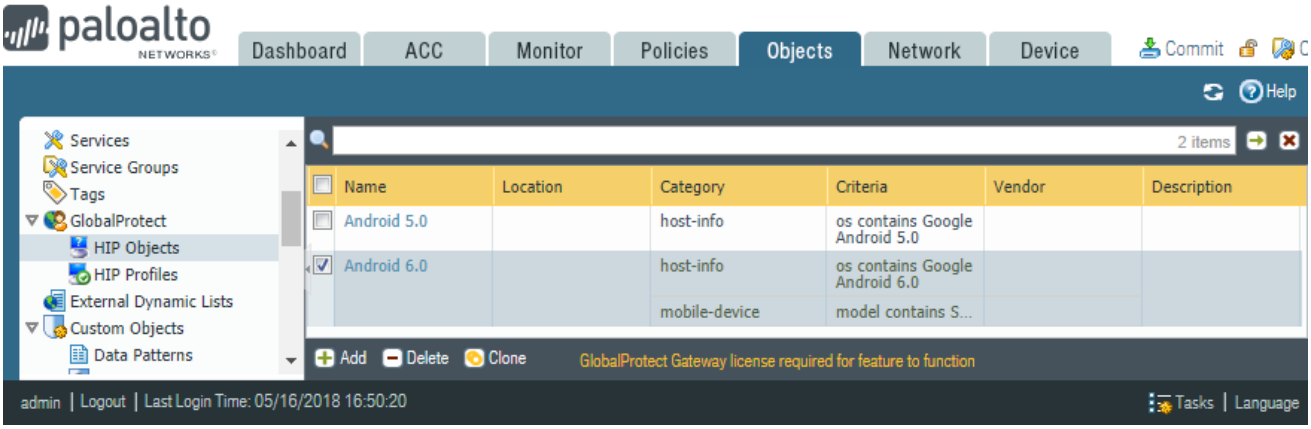
©2016-2019, Palo Alto Networks, Inc.

If you have the appropriate license, HIP checks can be performed by GlobalProtect agent software on the client platforms at connect time. The HIP Profile includes the OS version, patches installed, firewall and antivirus parameters, the process list, the registry, and other information that is useful to assess the security of an endpoint.



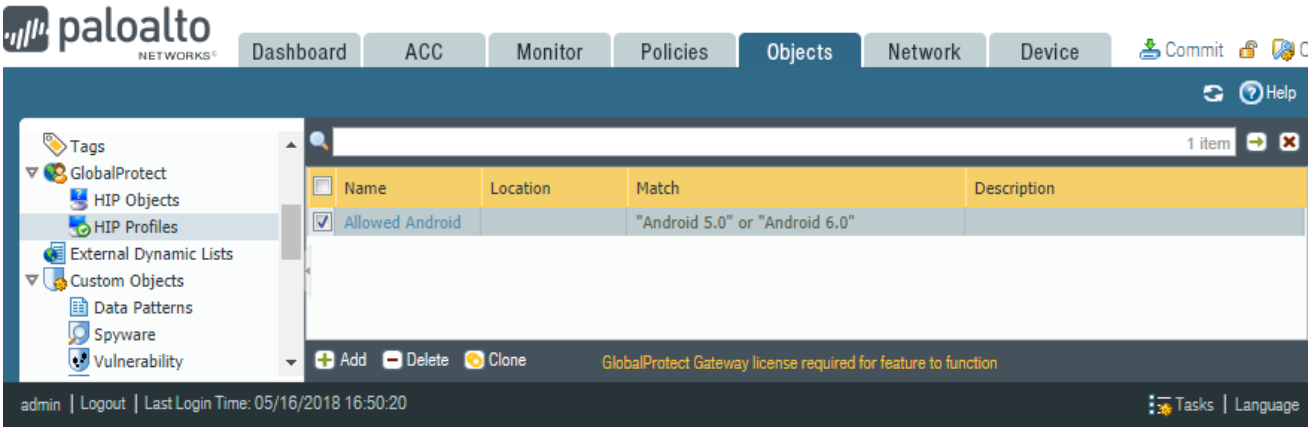
The firewall can extract information from these reports and use them as part of the Security policy. In this way the firewall provides appropriate access, depending on endpoint configuration.

HIP fields are used to define HIP objects. For example, a HIP object might apply to all devices using Android 5.0, or all Samsung devices using Android 6.0.

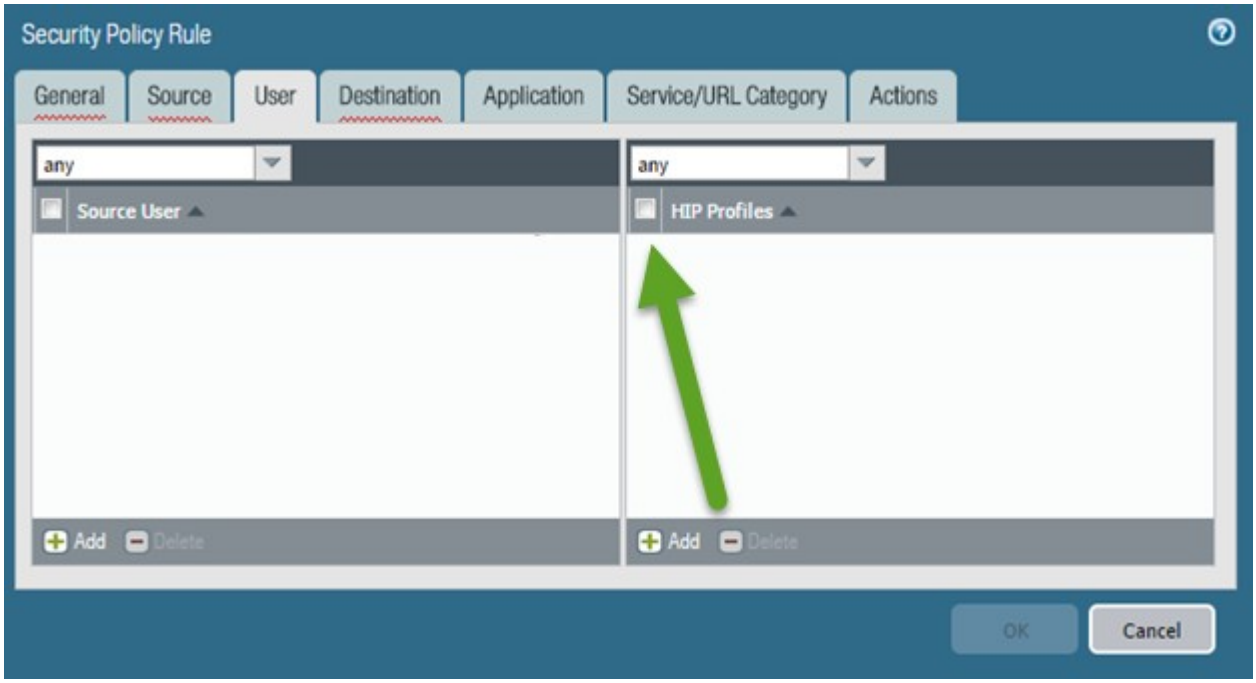


These HIP objects then are used in HIP Profiles.

©2016-2019, Palo Alto Networks, Inc.



These HIP Profiles then can be required by Security policy rules:



References

- A discussion of GlobalProtect with links to configuration specifics can be found here: https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/globalprotect-overview
- HIP checking implementation and use is explored in detail here: https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/host-information/about-host-information

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

92. Which configuration or service is required for an iOS device using the GlobalProtect license to connect to a local GlobalProtect Gateway?
    A. X-Auth configuration in the gateway settings
    B. global protect gateway license
    C. firewall authentication policy with an iOS setting
    D. GlobalProtect client downloaded from the GlobalProtect Portal
93. GlobalProtect Gateway is uniquely responsible for which function?
    A. terminating SSL tunnels
    B. authenticating GlobalProtect users
    C. creating on-demand certificates to encrypt SSL
    D. managing and updating GlobalProtect client configurations
    E. managing GlobalProtect Gateway configurations

©2016-2019, Palo Alto Networks, Inc.

2.17 Identify how to configure items pertaining to denial-of-service protection and zone protection

See *1.15 Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers*.

©2016-2019, Palo Alto Networks, Inc.

2.18 Identify how to configure features of NAT policy rules

Network address translation (NAT) allows the organization to use internal IP addresses that are not exposed to the internet. NAT rules are based on source and destination zones, source and destination address, and application service (such as HTTP). As is the case with Security policies, NAT policy rules are compared against incoming traffic in sequence, and the first rule that matches the traffic is applied.

Reference

- **Policies > NAT**
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-nat

Sample Questions

94. Which NAT type can be used to translate between IPv4 and IPv6?
    A. ipv4
    B. nat64
    C. nptv6
    D. ipv6
95. How does a firewall that has more than one NAT policy rule that matches a packet process the packet?
    A. Each matching rule in the list is applied from the top down, with cumulative changes being processed at the end of the list.
    B. The first rule matching the packet is applied and processed, skipping the others.
    C. The firewall issues an error when committing NAT policy rules that can affect the same packet.
    D. The last matching rule in the list is applied and processed.

©2016-2019, Palo Alto Networks, Inc.

2.19 Given a configuration example including DNAT, identify how to configure security rules

Security policies allow you to enforce rules and actions and can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same.

Reference

- **Policies > Security**
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security.html

Sample Questions

96. An internal web browser sends a packet to a server. The browser's connection has the source IP address 192.168.5.3, port 31415. The destination is 209.222.23.245, port 80. The firewall translates the source to 75.22.21.54, port 27182. Which three of these source IP addresses would cause a rule to apply to this traffic? (Choose three.)
    A. 192.168.5.0/24
    B. 75.22.21.0/24
    C. 192.168.4.0/23
    D. 192.168.0.0/16
    E. 75.22.0.0/17
    F. 75.22.128.0/17
97. A NAT policy rule is created to change the destination address of any packets with a source of any address and a destination address of 10.10.10.10 (in the DMZ zone) to 192.168.3.45 (in the Trust zone). Which Security policy rule components are required for a packet that has this rule applied to match and allow this traffic?
    A. source address any, source zone any, destination address 192.168.3.45, destination zone Trust, action = allow
    B. source address any, source zone any, destination address 10.10.10.10, destination zone Trust, action = allow
    C. source address any, source zone any, destination address 192.168.3.45, destination zone DMZ, action = allow
    D. source address any, source zone any, destination address 10.10.10.10, destination zone DMZ, action = allow

©2016-2019, Palo Alto Networks, Inc.

2.20 Identify how to configure decryption

You can configure the firewall to decrypt traffic for visibility, control, and granular security. Decryption policies can apply to Secure Sockets Layer (SSL) including SSL encapsulated protocols (such as IMAP(S), POP3(S), SMTP(S), FTP(S)) and to Secure Shell (SSH) traffic. SSH decryption can be used to decrypt outbound and inbound SSH traffic to assure that secure protocols are not being used to tunnel disallowed applications and content.

A Palo Alto Networks firewall also can act as a decryption broker for other external security services. This feature will decrypt traffic and forward it out of the selected interface to a specific security device or service (or chain of devices) that examines the cleartext traffic. The last service in the chain returns the packet to the firewall, which then encrypts it and forward it to the original destination.

Information about the use and configuration of this capability can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts

Special Decryption Implementations

Palo Alto Networks firewalls also can automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This option available is at no cost to middle and high-end firewalls that automatically forward copies of decrypted traffic to external DLP products. A description of this feature can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-concepts/decryption-mirroring.html

Sample Questions

98. Which protocol is supported for traffic decryption matching a Decryption policy rule??
    A. IPsec
    B. SP3
    C. SSH
    D. NLSP
99. Where do you specify that a certificate is to be used for SSL Forward Proxy?
    A. Certificate properties
    B. Decryption Profile
    C. Decryption policy
    D. Security policy
100. Which feature must be configured to exclude sensitive traffic from decryption?
    A. Security policy rule that includes the specific URL with an “allow” action
    B. Decryption policy rule with the specific URL and “no decrypt” action
    C. Application Override policy that matches the application URL and port number
    D. Decryption Profile that includes the site’s URL

©2016-2019, Palo Alto Networks, Inc.

2.21 Given a scenario, identify an application override configuration and use case

To change how the firewall classifies network traffic into applications, you can specify Application Override policies. These policies attach the configured App-ID to matching traffic and bypasses the normal App-ID processing steps in the firewall. This assigned application functions identically to an App-ID supplied application name and can be used in the same way. For example, if you want to control one of your custom applications, you can use an Application Override policy to identify traffic for that application according to zone, source, and destination address, port, and protocol.

Note that the App-ID bypass characteristic of Application Override also skips essential Content-ID processing, which could result in undetected threats. This feature should be used for trusted traffic only.

References

- **Policies > Application Override**
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-application-override.html
- **Objects > Applications**
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-applications/defining-applications

Sample Questions

101. Which option is not a parameter used to identify applications in an Application Override policy?
   A. protocol
   B. port number
   C. first characters in the payload
   D. destination IP address

102. When an Application Override policy matches traffic and assigns an App-ID which firewall process is bypassed?
   A. QOS
   B. IP-Sec
   C. Content-ID
   D. User-ID

©2016-2019, Palo Alto Networks, Inc.

2.22 Identify how to configure VM-Series firewalls for deployment

The VM-Series of virtual firewalls can be deployed to several public and private cloud technologies. Each environment has different deployment characteristics and requirements. Some require the uploading of the firewall's virtual appliance. Others provide it in an "Application Store" that is provisioned and configured.

Regardless of the deployed environment, every VM-Series firewall runs the same PAN-OS software supporting the same set of features. Some environments have specific limits and requirements (i.e., supported interface types).

Supported virtual technologies are outlined here:
https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/vm-series-firewalls

Details for implementation in each of these environments and a review of their specific requirements and limitations are here:
https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization

Sample Questions

103. Which virtual interface is the management on a VM-Series firewall running on ESXi?
    A. vNIC #1
    B. vNIC #2
    C. vNIC #9
    D. vNIC #10
104. Which three items of information are required at a minimum to install and configure VM-Series firewalls?
    A. VLANs to be connected through the firewall
    B. management port IP address
    C. IP addresses for the data interfaces
    D. management port default gateway
    E. management port netmask
    F. IP address for the external (internet-facing) interface
105. VM-Series firewalls require which additional license step?
    A. Apply a Base Capacity license
    B. Apply a Cloud Services license
    C. Apply a Site license
    D. Apply a VM Update license
106. A VM-Series firewall being deployed in Azure can be automatically configured by bootstrapping. Azure requires which features for Bootstrapping to work?
    A. Storage Account configured for Azure Files Service
    B. PowerShell script that feeds a configuration file to the firewall
    C. XML configuration file included in the base firewall provisioning
    D. Azure Backup services configured with a config file and included in the firewall provisioning

©2016-2019, Palo Alto Networks, Inc.

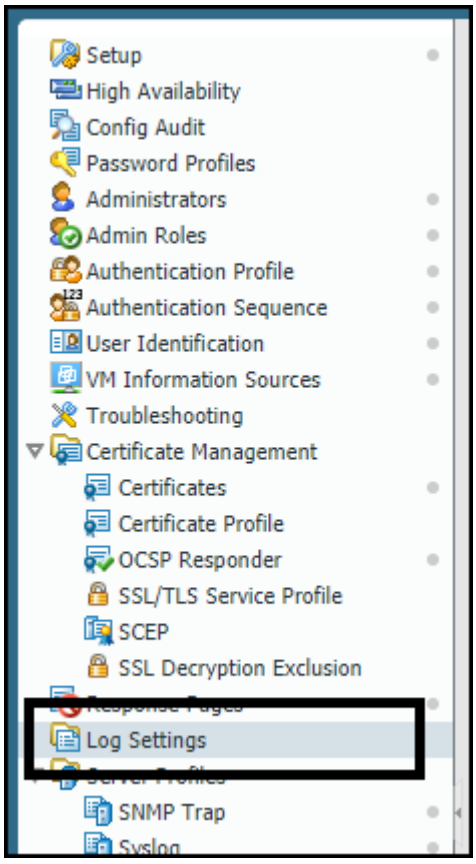
2.23 Identify how to configure firewalls to use tags and filtered log forwarding for integration with network automation

Log Forwarding, Filtering, and Tagging

The Palo Alto Networks firewall contains several important features to identify log events of interest and to forward the events in various formats to outside monitoring technology. The firewall also can extract IP addresses from the events and add tags to them, which could then include them in Dynamic Address Groups managed by the firewall. These groups can be used in Security policy rules to provide a higher level of security treatment.

Filtering and Forwarding Log Events

The Palo Alto Networks firewall has two primary methods to forward log events, depending on the log message type. Events associated with examined traffic use Log Forwarding Profiles. Events generally related to non-traffic specific firewall activity (e.g. Authentication, System, and HIP Match) can be filtered and forwarded using **Log Settings**. Navigate to **Device > Log Settings**.



©2016-2019, Palo Alto Networks, Inc.

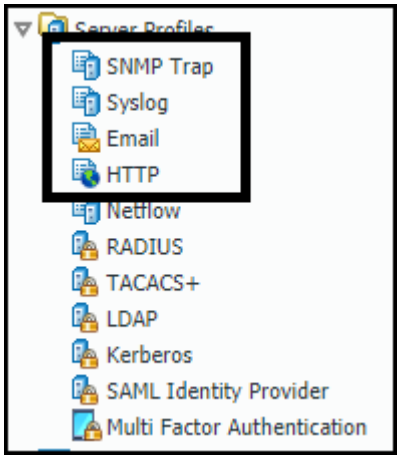
Log Forwarding Profiles can be used to filter and forward logs from the following firewall logs:

- Traffic
- Threat
- Tunnel
- URL Filtering
- WildFire Submissions
- Authentication
- Data Filtering

Log forwarding of any event type can send copies of log events to destinations supporting the following data formats:

- SNMP
- Email
- Syslog
- HTTP

Each log forwarding destination is configured in the firewall with a Server Profile of the appropriate type. Navigate to **Device > Log Settings** and create a profile for each specific destination.



After the destination's Server Profile is created, it can be used in a Log Forwarding Profile.

Log Forwarding Profiles

To maximize the efficiency of your incident response and monitoring operations, you now can create custom log forwarding filters based on any log attributes (such as threat type or source user). Instead of forwarding all logs or all logs of specific severity levels, you can use the filters to forward only the information you want to monitor or act on. For example, a security operations analyst that investigates malware attacks might be interested only in Threat logs with the type attribute set to wildfire-virus.

Steps:

1. Configure a Server Profile for each external service that will receive logs from the firewall. The profiles define how the firewall connects to the services.

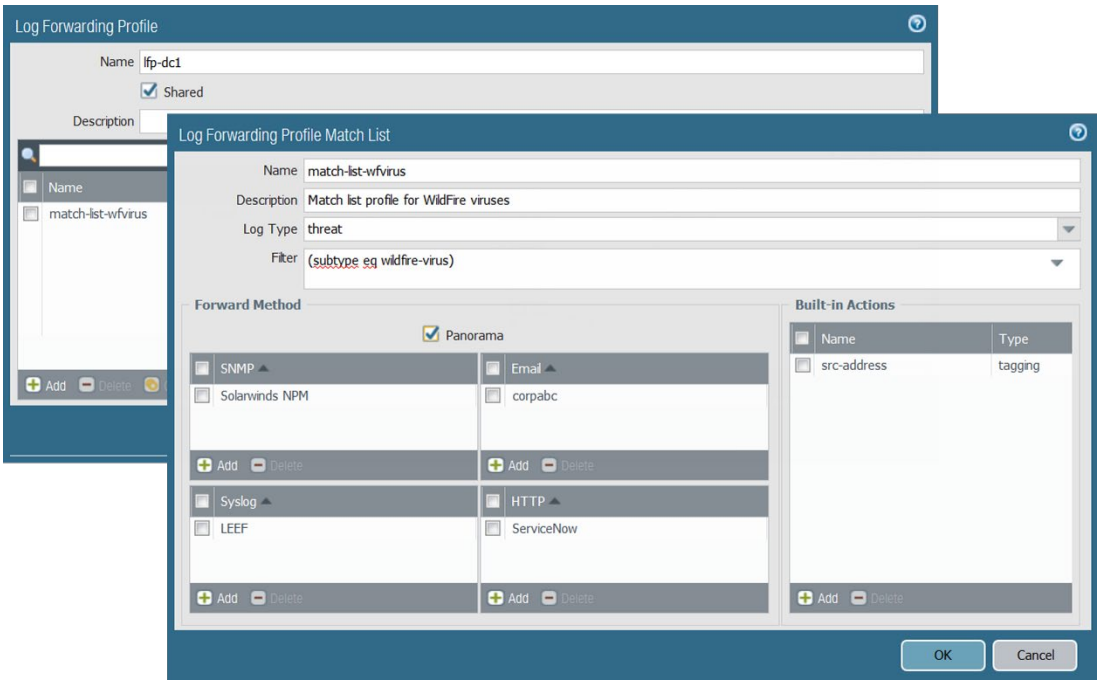
   For example, to configure an HTTP Server Profile, select **Device > Server Profiles > HTTP** and **Add**

©2016-2019, Palo Alto Networks, Inc.

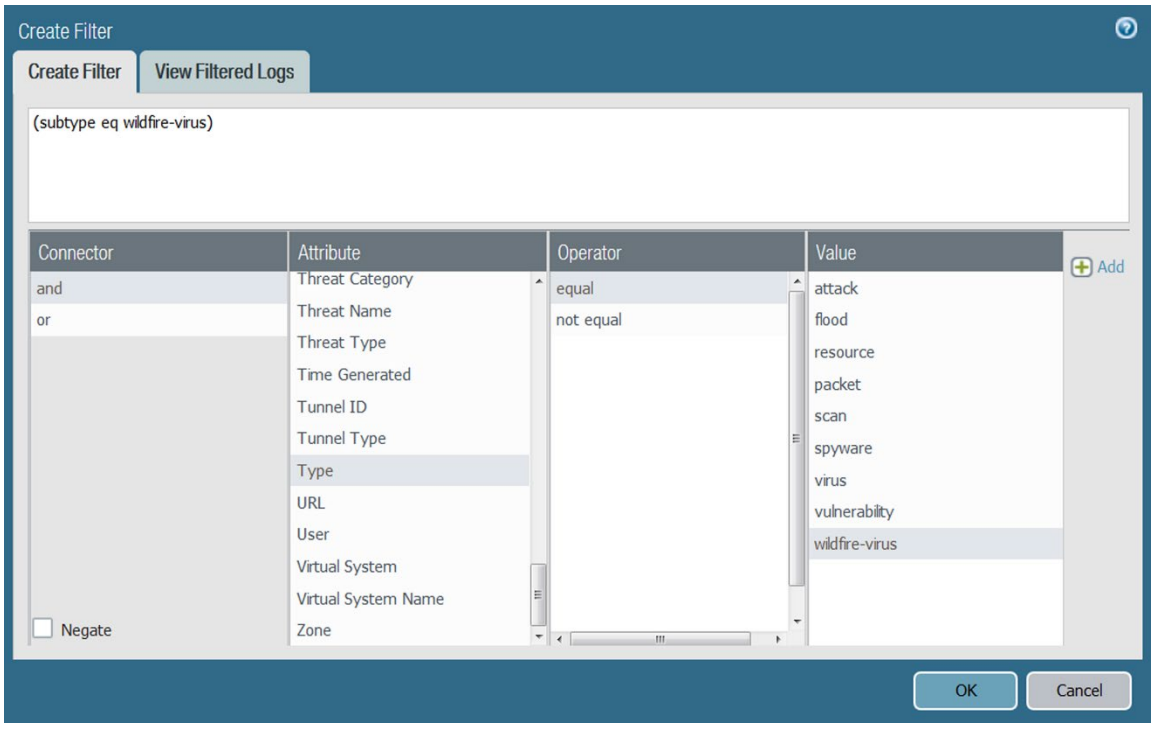
the profile.

2. Select **Objects > Log Forwarding** and **Add** a Log Forwarding Profile to define the destinations for Traffic, Threat, WildFire Submissions, URL Filtering, Data Filtering, Tunnel, and Authentication logs.

   In each Log Forwarding profile, **Add** one or more match list profiles to specify log query filters, forwarding destinations, and automatic actions such as tagging.



   In each match list profile, select **Filter > Filter Builder** and **Add** filters based on log attributes.

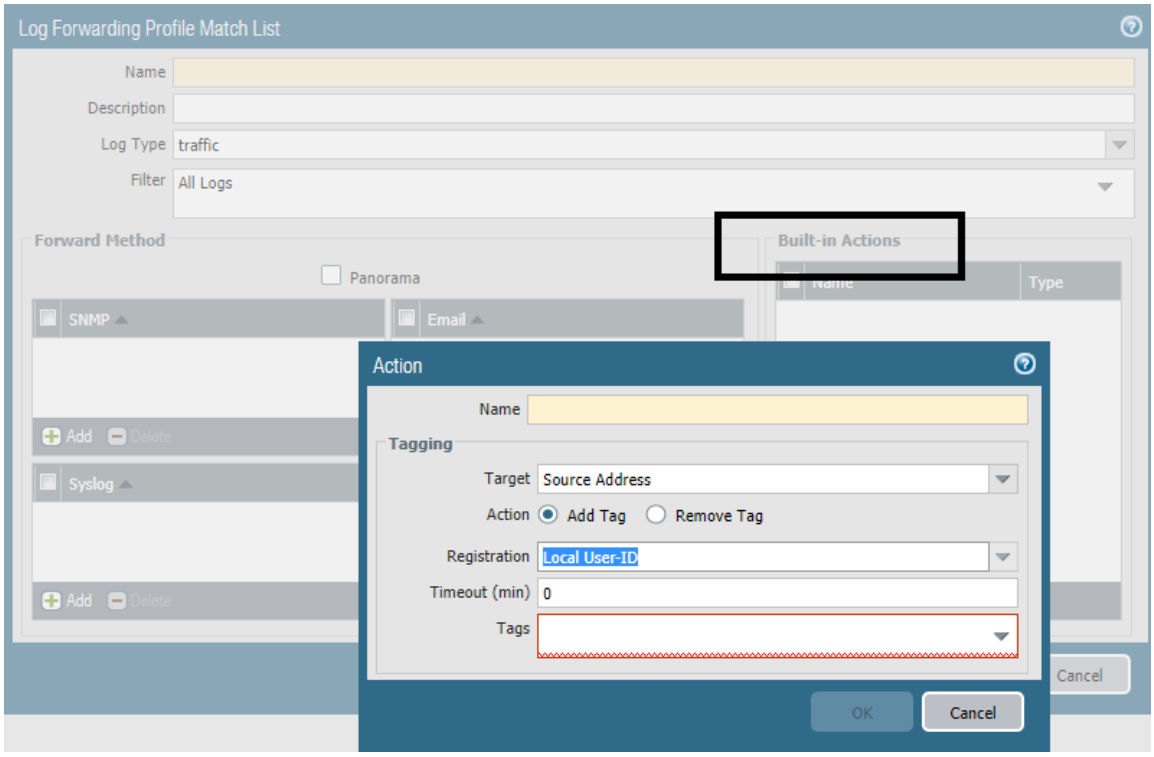


©2016-2019, Palo Alto Networks, Inc.

3. Assign the Log Forwarding profile to policy rules and network zones.
   The firewall generates and forwards logs based on traffic that matches the rules and zones. Security, authentication, and DoS protection rules support log forwarding. For example, to assign the profile to a Security rule, select **Policies > Security**, edit the rule, select **Actions**, and select the **Log Forwarding** profile you created.
4. Select Device > Log **Settings** and configure the destinations for System, Configuration, User-ID, HIP Match, and Correlation logs. For each log type that the firewall will forward, **Add** one or more match list profiles as you did in the Log Forwarding Profile.
5. **Commit** your changes.

Automated Actions and Tagging with Log Forwarding

Log Forwarding Profiles also provide a mechanism to collect the source or destination IP address of the event and add it to a Tag list. The Tag then can be used to assign the address to a Dynamic Group that is used in a Security Policy Rule.



Add the action to perform.
Add or remove a tag to the source or destination IP address in a log entry automatically and register the IP address and tag mapping to a User-ID agent on the firewall or Panorama, or to a remote User-ID agent so that you can respond to an event and dynamically enforce Security policy. The ability to tag an IP address and dynamically enforce policy using Dynamic Address Groups gives you better visibility, context, and control for consistently enforcing Security policy irrespective of where the IP address moves across your network.

Configure the following settings:

©2016-2019, Palo Alto Networks, Inc.

- **Add** an action and enter a name to describe it.
- Select the target IP address you want to tag: **Source Address** or **Destination Address**.
  You can take an action for all log types that include a source or destination IP address in the log entry. You can tag the source IP address only, in Correlation logs and HIP Match logs; you cannot configure an action for System logs and Configuration logs because the log type does not include an IP address in the log entry.
- Select the action: **Add Tag** or **Remove Tag**.
- Select whether to register the IP address and tag mapping to the **Local User-ID** agent on this firewall or Panorama, or to a **Remote User-ID** agent.
- To register the IP address and tag mapping to a **Remote User-ID** agent, select the HTTP Server Profile (**Device > Server Profiles > HTTP**) that will enable forwarding.
- Configure the IP-Tag **Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting of the timeout to 0 means that the IP-Tag mapping does not time out (range is 0 to 43200 (30 days); default is 0).
- Enter or select the **Tags** you want to apply or remove from the target source or destination IP address. Within the Log Forwarding Profile, you can define a **Built-in Action**.

Sample Questions

107. Dynamic tags can be assigned to which kind of data in a log event?
    A. source and destination address, source and destination zone name
    B. source and destination address
    C. interface, zone name
    D. DNS name, zone name

108. How can the firewall use Dynamically Tagged objects to block traffic?
    A. The object is added to an enforcement list of a Data Filtering Object that then is attached to a Security policy rule.
    B. The object is assigned to a Dynamic List, which then is included in the destination address matching condition of a Security policy rule.
    C. The object is assigned to a Dynamic Address Group object, which then is added to the destination address matching condition of a Security policy rule.

109. A dynamic tag can be assigned to data in which four types of log events? (Choose four.)
    A. Traffic
    B. Threat
    C. URL Filtering
    D. HIP Match
    E. Tunnel Inspection
    F. Configuration
    G. System

110. Dynamic tagging activity is recoded in which log?
    A. System
    B. Configuration
    C. IP-Tag
    D. Data Filtering

©2016-2019, Palo Alto Networks, Inc.

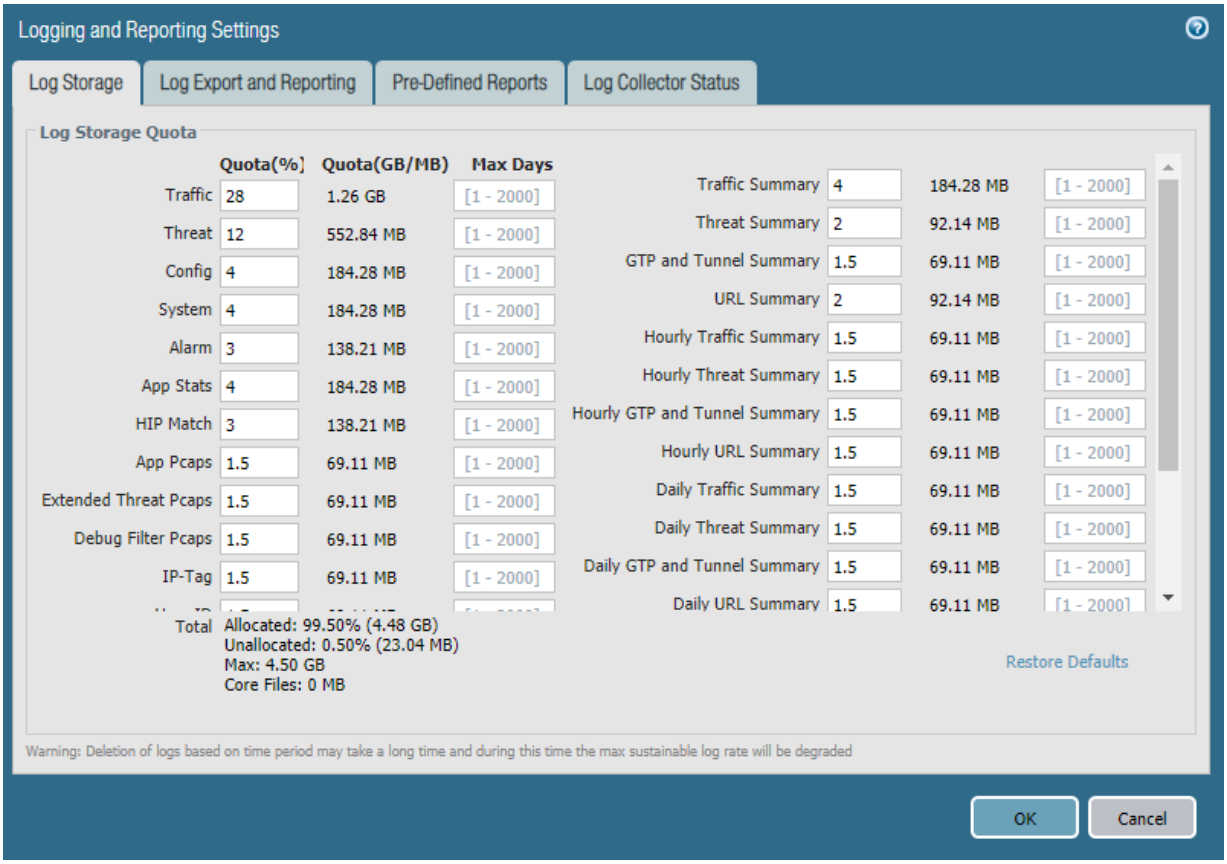
Exam Domain 3 – Operate

3.1 Identify considerations for configuring external log forwarding

Direct Firewall Log Forwarding

Use of an external service to monitor the firewall enables you to receive alerts for important events, archive monitored information on systems with dedicated long-term storage, and integrate with third-party security monitoring tools.

Local log storage on Palo Alto Networks firewalls is strictly allocated between different log files to ensure that no particular log is overrun by another. This allocation is user-controlled. Navigate to **Device > Setup > Management > Logging and Reporting Settings** for access to the following configuration settings:



Each storage area typically acts as circular logs in the sense that, when filled, new entries will overwrite old ones. Space is cleared in blocks and messages added to the System log.

Before you can use Panorama or external systems to monitor the firewall, you must configure the firewall to forward its logs. Before the firewall forwards to external services, it automatically converts the logs to the necessary format: syslog messages, SNMP traps, HTTP, or email notifications. Before you start this procedure, ensure that Panorama or the external server that will receive the log data is running and can receive this traffic.

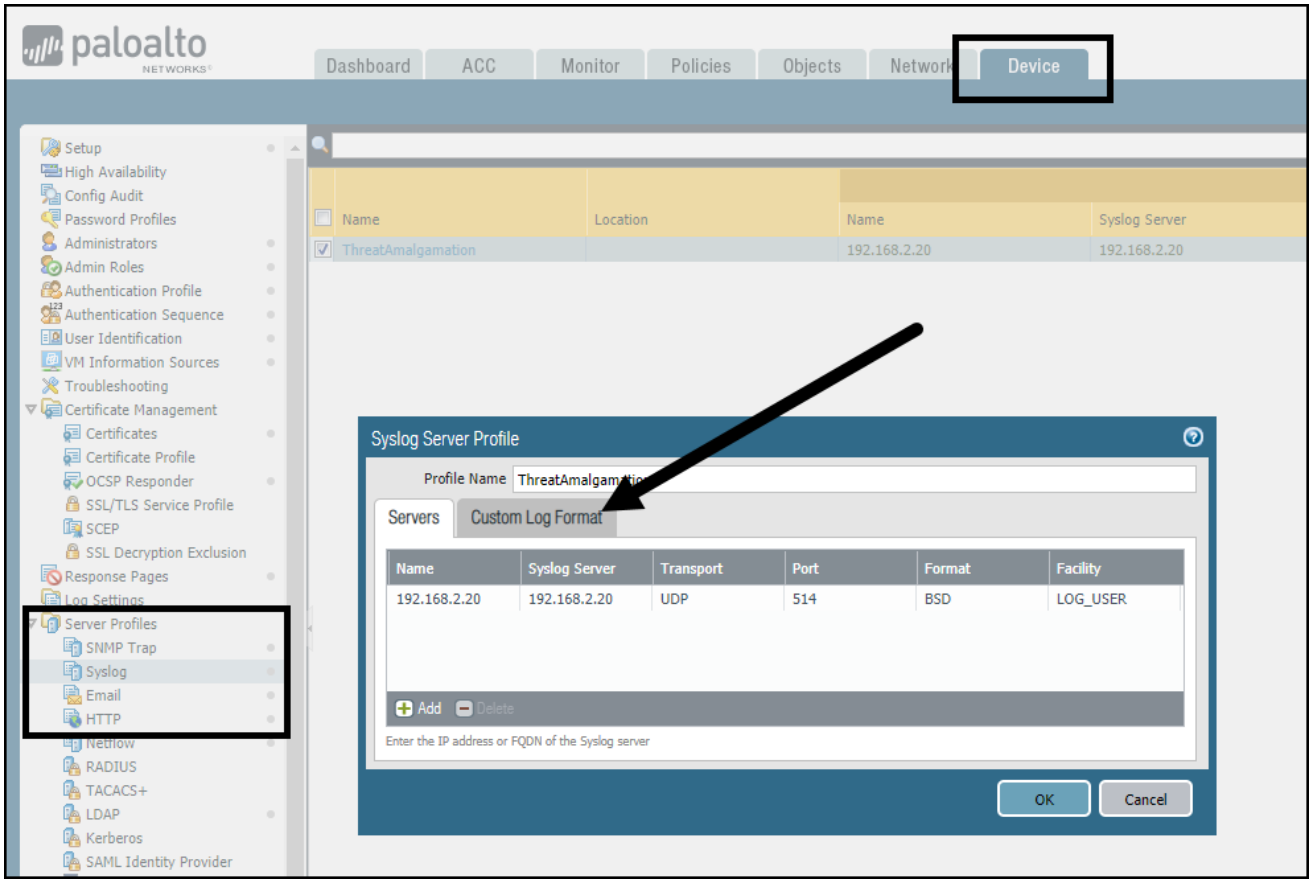
©2016-2019, Palo Alto Networks, Inc.

Destination Log Types and Formatting

External forwarding supports the following types of destinations:

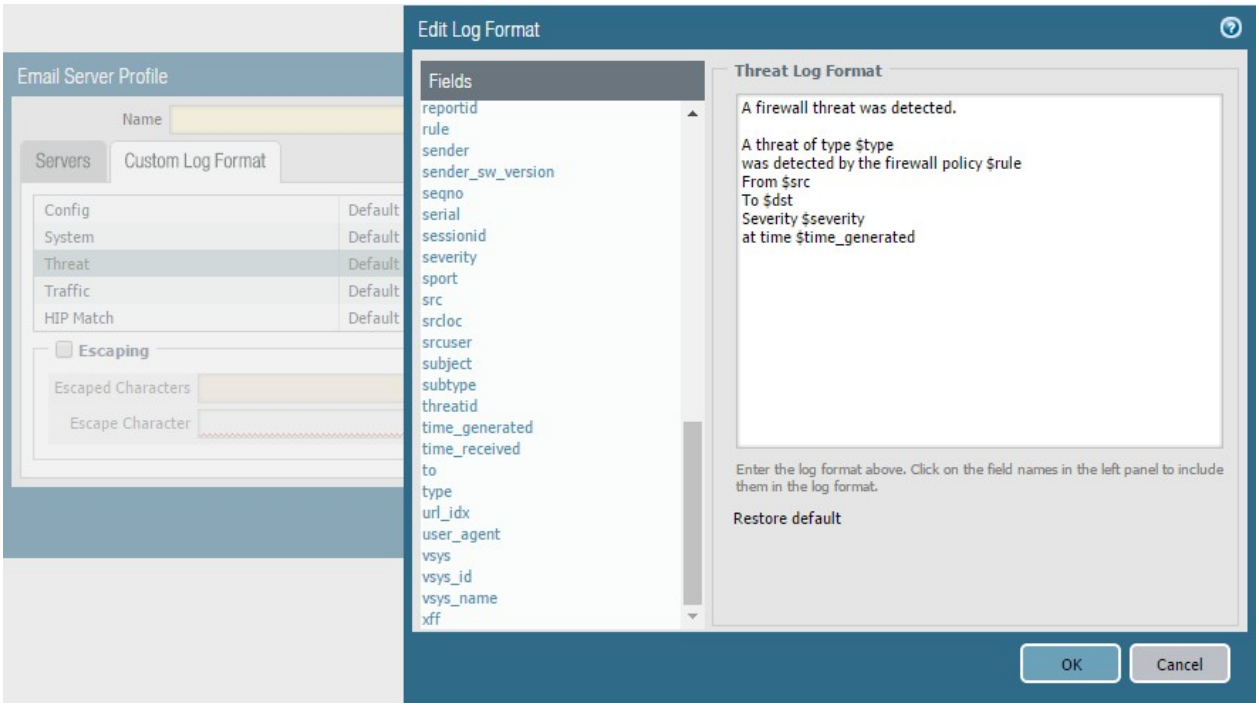
1. SNMP traps
2. Syslog
3. HTTP server
4. Email
5. Panorama

All types (other than Panorama) support customization of the message format. A typical destination configuration follows:



©2016-2019, Palo Alto Networks, Inc.

Email message formats can be customized. For example:

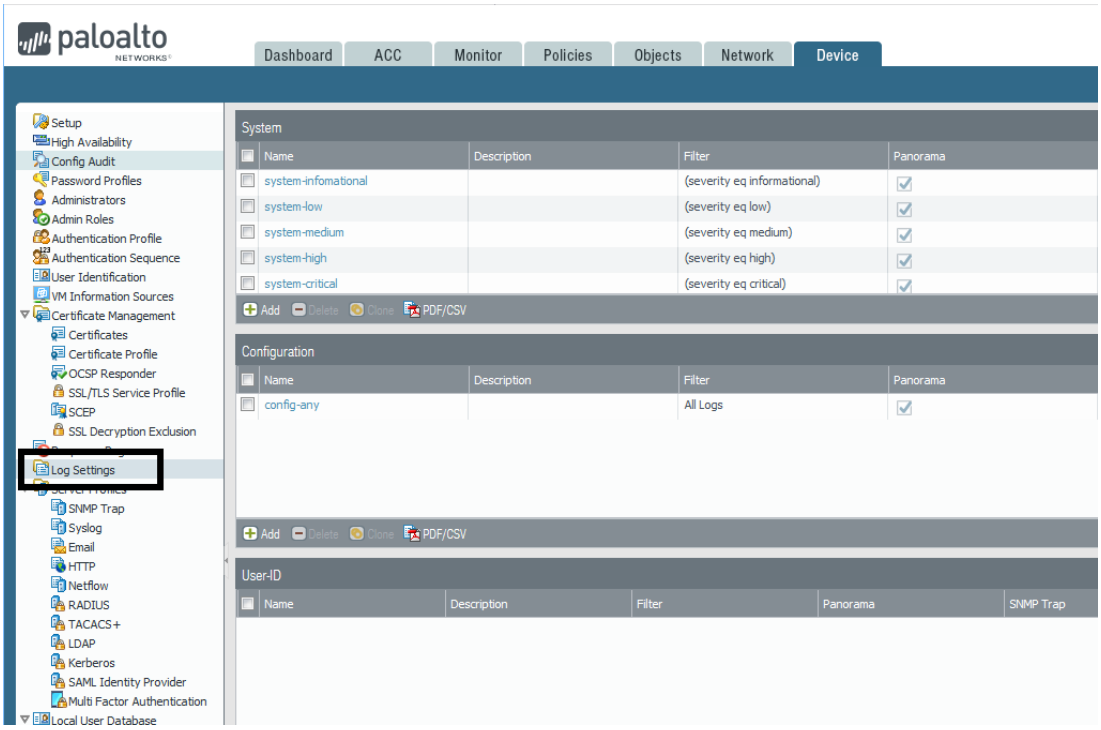


Any log event redirection causes a copy of the log event to be forwarded as specified. It is logged on the firewall as usual.

©2016-2019, Palo Alto Networks, Inc.

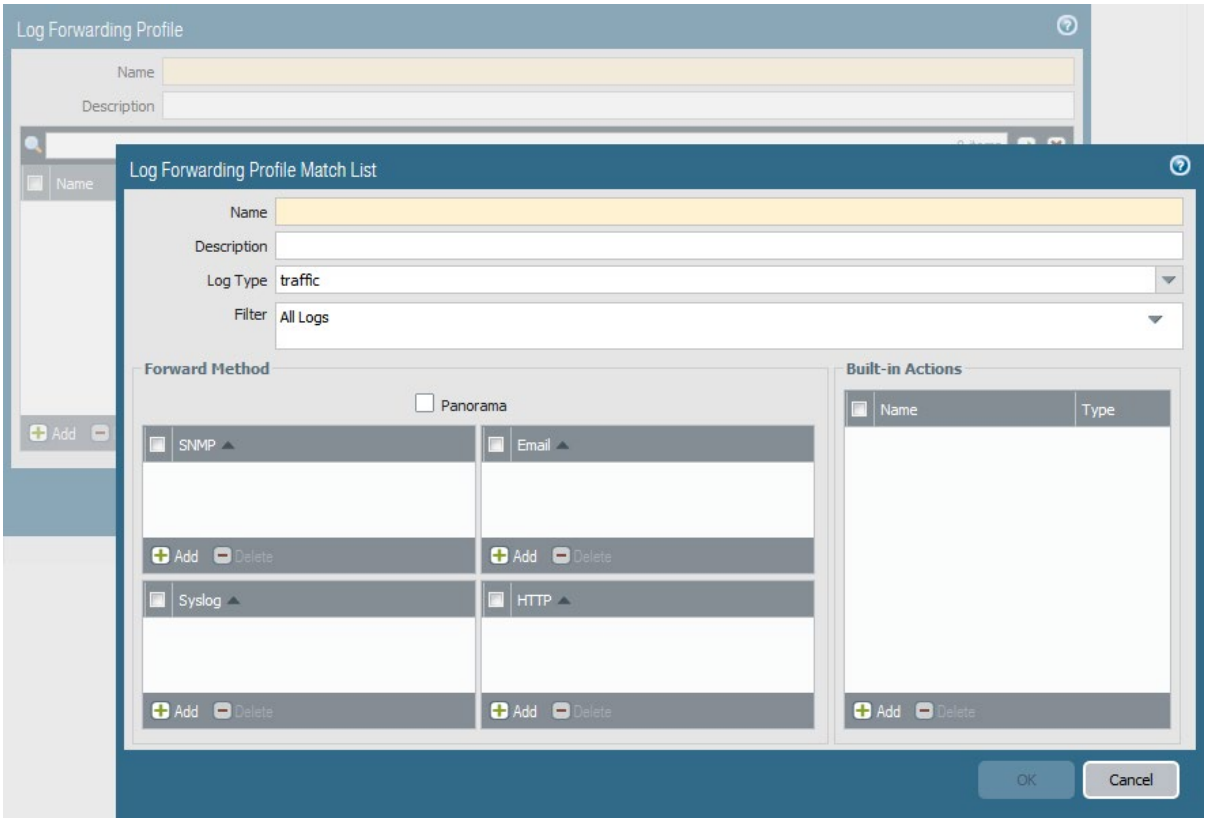
Methods Used to Forward Logs

Two main methods are used to forward log events, depending on the log message type. Log events destined for the System, Config, User-ID, and HIP Match logs are redirected using **Device > Log Settings** to choose event destination(s) for specific event types:



©2016-2019, Palo Alto Networks, Inc.

The second method is the use of a Log Forwarding Profile to route Traffic, Threat, WildFire®, and other log events to other systems such as Panorama, SIEM products, syslog servers:



Log Forwarding Profiles are attached to individual firewall Security policies to enable forwarding of the events associated with the processing of the specific policy. These profiles include one or more Log Forwarding Profile Match Lists. This granularity allows administrators specific control of forwarding and the potential of different forwarding for policies of differing importance.

All forwarded events are sent to their destination as they are generated on the firewall. A complete discussion of log forwarding configuration is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/configure-log-forwarding

Palo Alto Networks also offers a cloud-based Cortex XDR Data Lake (formerly Logging Service) that can be a central repository for forwarded logs from multiple Palo Alto Networks devices. This central pool of log data is fully accessible to the owner and acts as an optional base for further third-party security applications through the Palo Alto Networks Cortex API.

Further information about this service can be found here:
https://docs.paloaltonetworks.com/cortex/cortex-data-lake

©2016-2019, Palo Alto Networks, Inc.

Sample Question

111. Which two firewall logs can be exported using the Scheduled Log Export function? (Choose two.)

A. Configuration
B. System
C. Traffic
D. URL

©2016-2019, Palo Alto Networks, Inc.

3.2 Interpret log files, reports, and graphs to determine traffic and threat trends

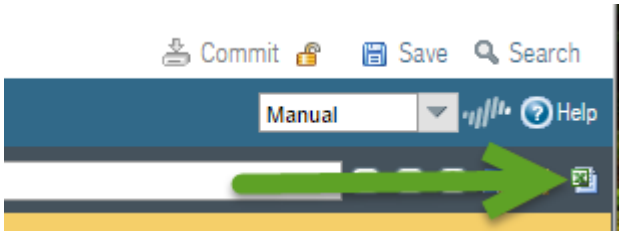
Logging and reporting are critical components of any security network. The ability to log all network activity in a logical, organized, and easily segmented way makes logging even more valuable. Rapid, thorough, and accurate interpretation of events is critical to security. Security practitioners often suggest that security is only as good as the visibility it is built on. These reasons contribute to Palo Alto Networks information collection and display design.

A discussion of available log data and making it into information that can be acted on is here: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/actionable-threat-intelligence

Log information generally is in the **Monitor** tab of the web interface. The reporting sections align with the general use of these reports. The Log section presents detailed, real-time data with the ability to recall previous data (subjected to available storage). It is subdivided into sections that segment log data into related information. PAN-OS® 9.0 includes a Unified log that collects copies of events from the Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs into a single location for easy parsing of related data.

Each log provides similar features, which results in an organized presentation of desired data. Displayed log data can be exported in CSV format at any time.

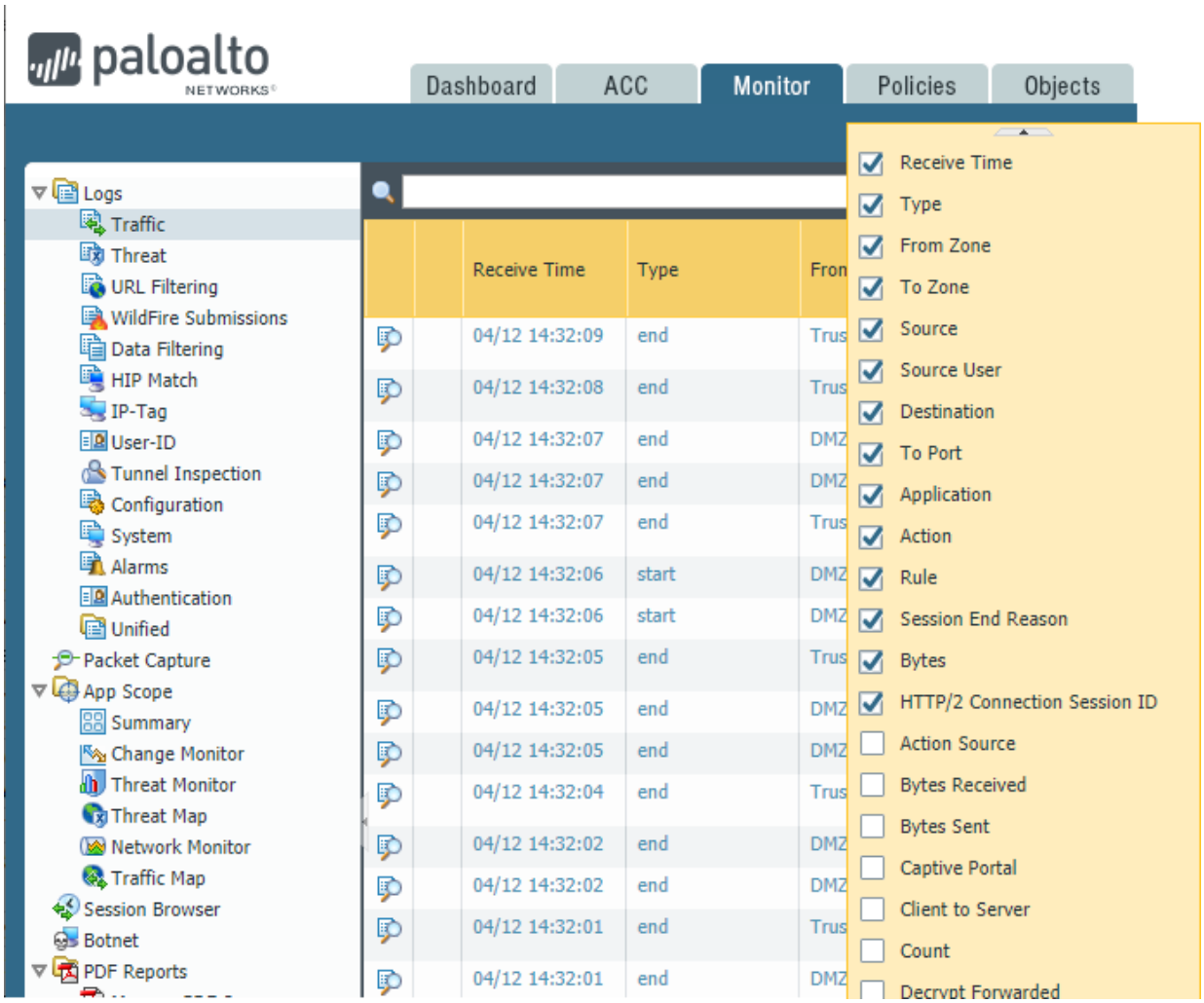
The following figure shows the CSV export option available on any detailed log display:



This export will include all detail for the displayed record even if it isn't visible in the chosen column displays.

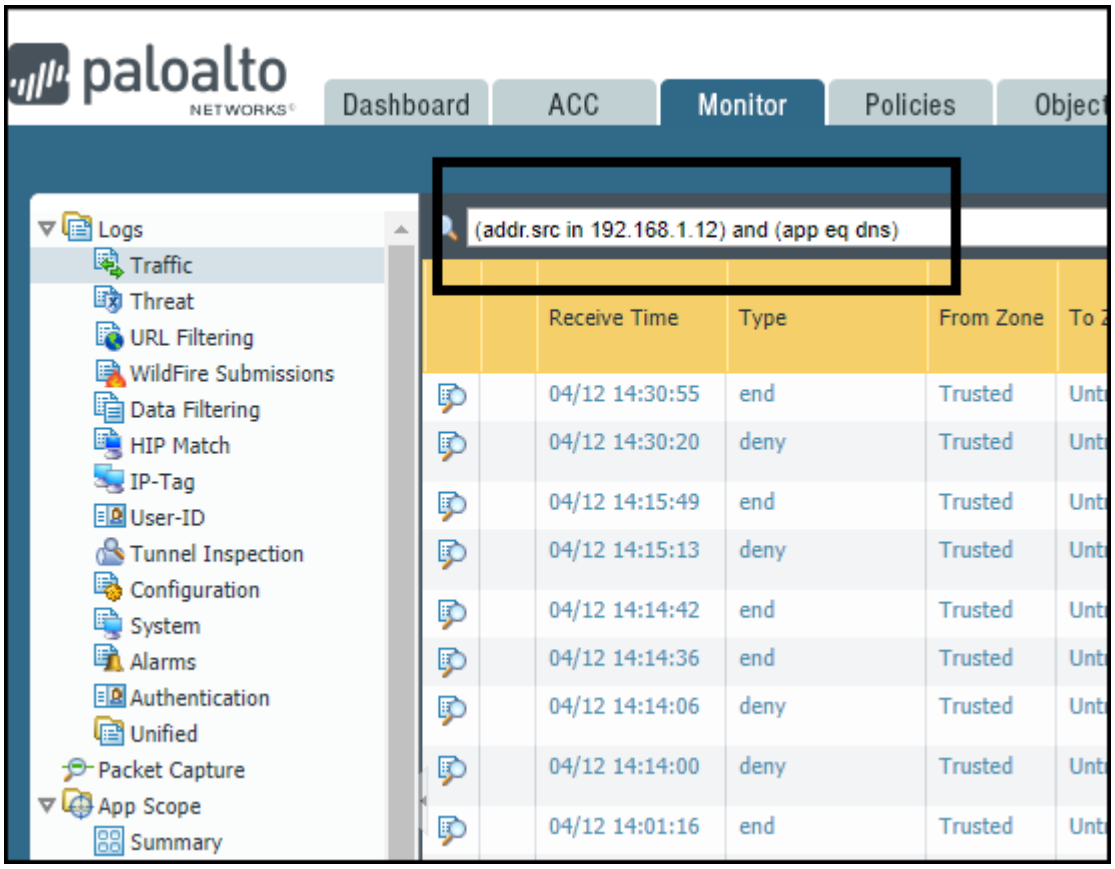
You can see the entries in various logs using **Monitor > Logs**. You can configure the columns to display and their order and width:

©2016-2019, Palo Alto Networks, Inc.



Each log display offers a powerful filtering capability that facilitates the display of specific desired data:

©2016-2019, Palo Alto Networks, Inc.



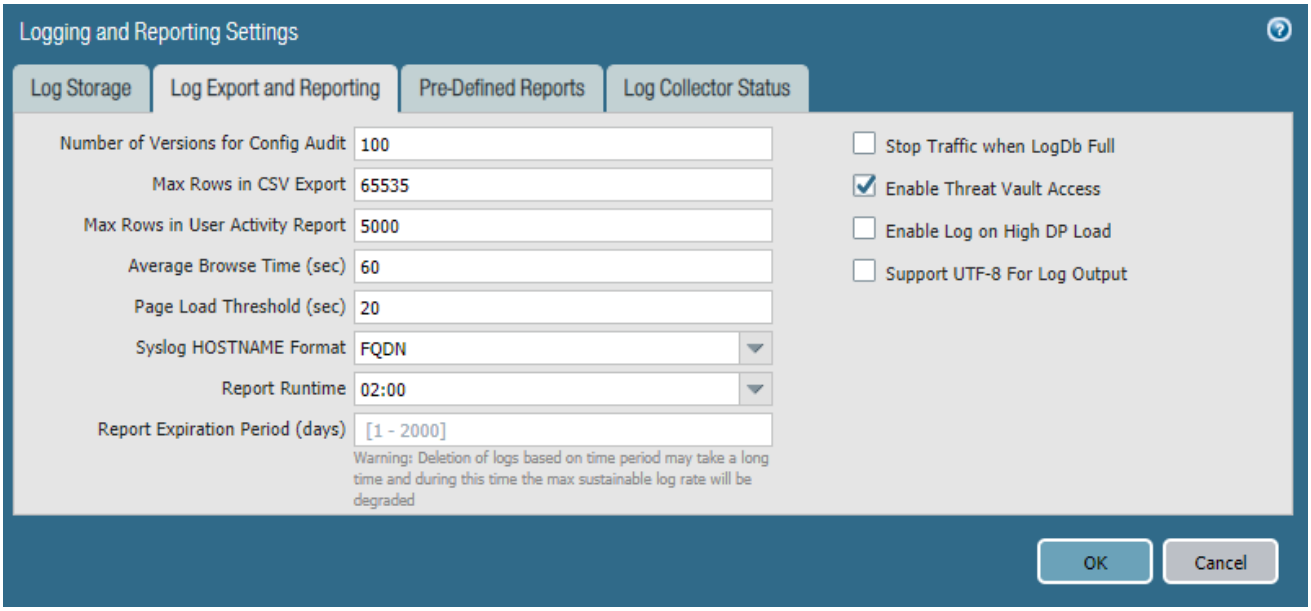
Filters can be added to eliminate the display of undesired entries.

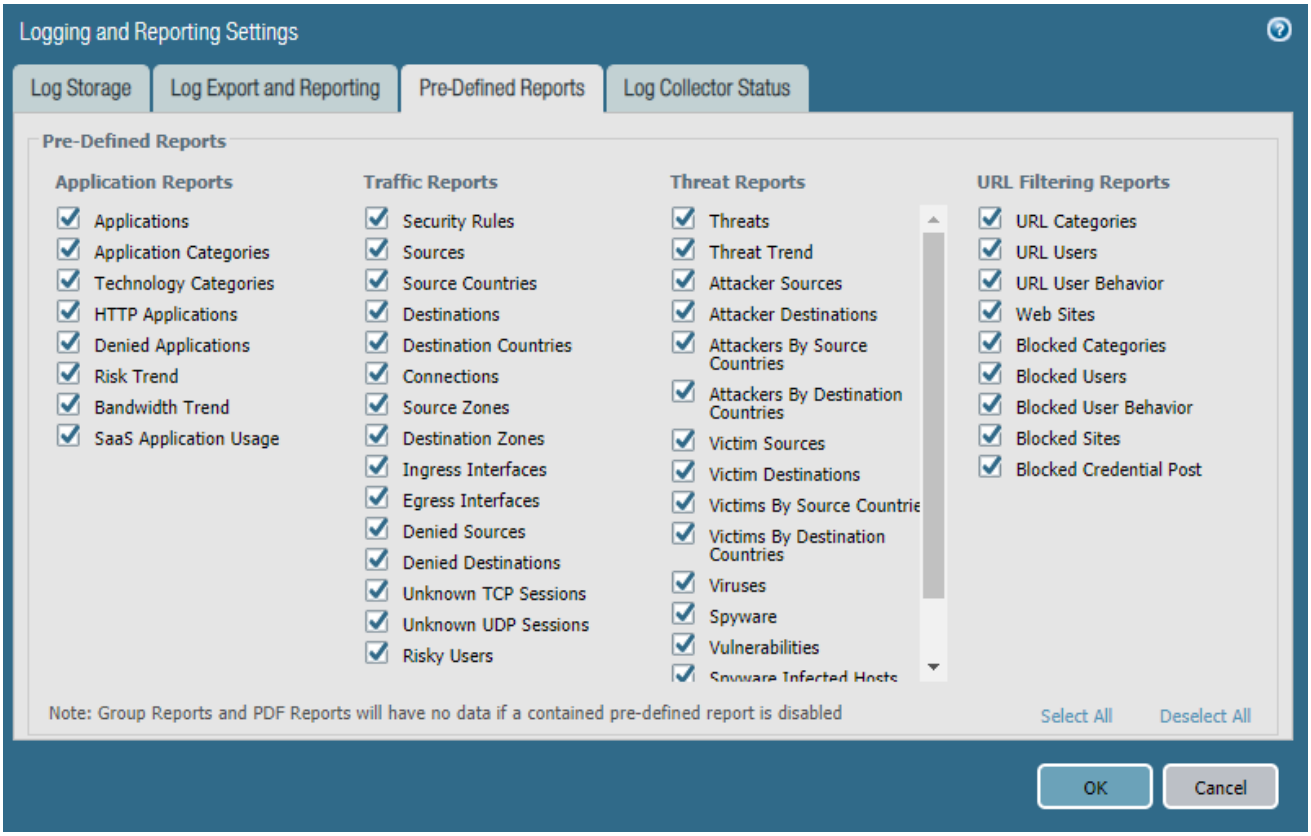
Filters can be built and even stored for future use. Specific data about this functionality is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/view-and-manage-logs

While this log data is stored in detail in log storage, a firewall summarizes new log entries and adds the results to separate on-board reporting databases used as default sources by Application Command Center (ACC), App Scope, PDF Reports, and Custom Reports.

©2016-2019, Palo Alto Networks, Inc.

The scope of this summarization process can be controlled with settings on **Device > Setup > Management > Logging and Reporting Settings**:



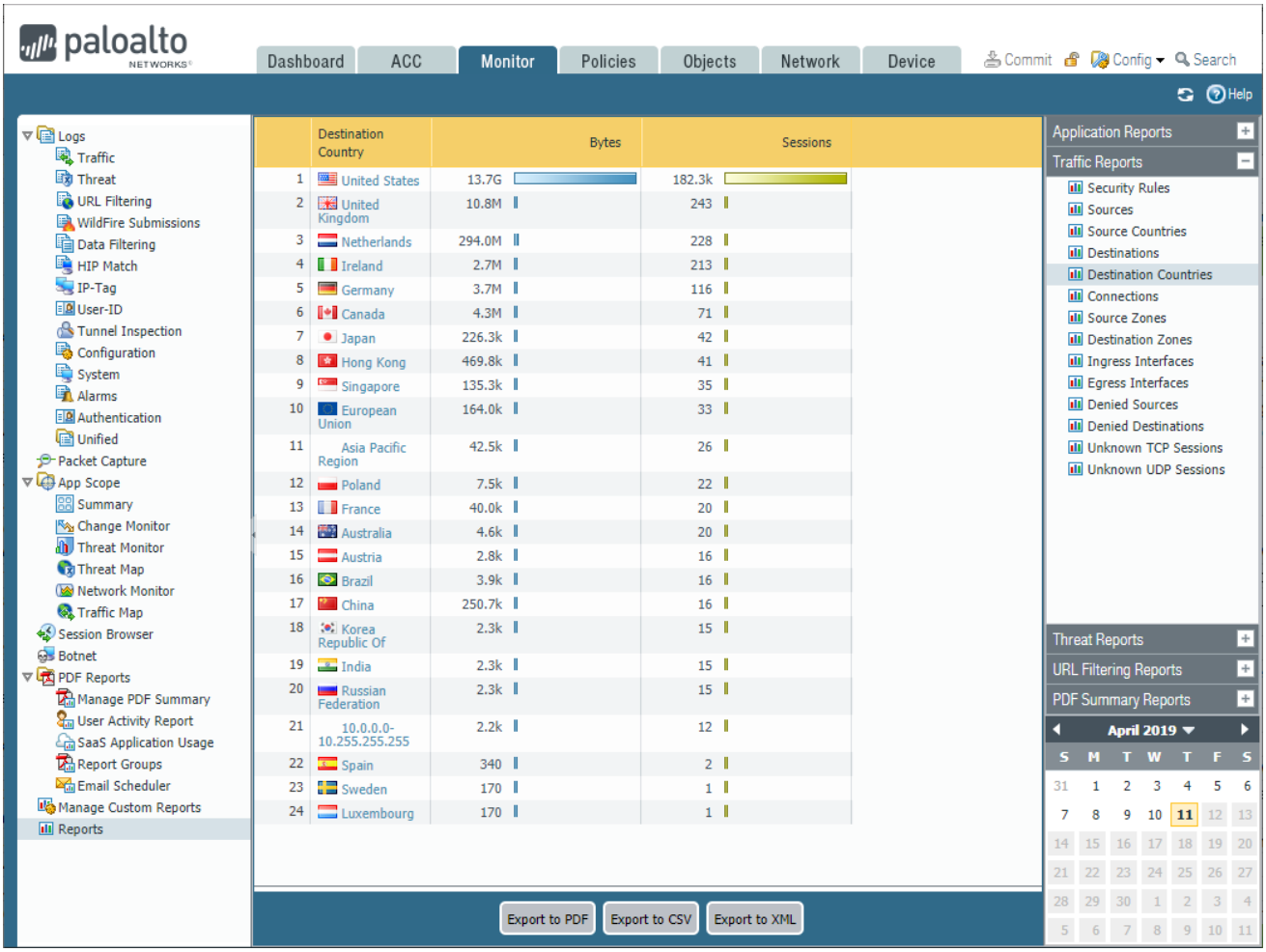


©2016-2019, Palo Alto Networks, Inc.

PDF Reports

The PDF Reports section offers many predefined PDF reports that can be run as a group on a scheduled basis and delivered through email daily or weekly.

These reports typically run once per day and summarize all activity on the firewall. A report browser of predefined reports appears on the right. In the following figure, chosen reports display their results for the previous day's traffic. The Predefined Report Browser shows choices of categories and specific reports on the right:



The PDF Reports section offers other important reporting tools. Custom reports can be created, stored, and run on-demand and/or a schedule basis. More information is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports

©2016-2019, Palo Alto Networks, Inc.

User/Group Activity Report

A predefined User/Group Activity report provides complete application use and browsing activity reports for individuals or group. Information is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports.html

PDF Summary Report

A PDF Summary Report includes several top-5-oriented reports grouped to provide a general representation of the firewall's traffic during the previous day. Details are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports

App Scope reports focus on base-line performance comparisons of firewall use. These reports provide power tools to characterize changes in detected use patterns. They were designed for ad-hoc queries more than for scheduled report output. Detailed information is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-the-app-scope-reports.html

Application Command Center

The Application Command Center (ACC) is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network. The ACC uses the firewall logs to provide visibility into traffic patterns and information about threats that can be acted on. The ACC layout includes a tabbed view of network activity, threat activity, and blocked activity. Each tab includes pertinent widgets for better visualization of network traffic. The graphical representation allows you to interact with the data and to see the relationships between events on the network so that you can uncover anomalies or find ways to enhance your network security rules. For a personalized view of your network, you can add a custom tab and include widgets that allow you to find the information that is most important to you.

Other reports and displays on the firewall often support click-through of data items to enable you to uncover more detail. This practice often results in a switch to the ACC with preset filters to focus only on the previously displayed data. Detailed use data is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-the-application-command-center.html

Automated Correlation Engine

The Automated Correlation Engine is an analytics tool that uses the logs on the firewall to detect events on your network that can be acted on. The engine correlates a series of related threat events that, when combined, indicate a likely compromised host on your network or some other higher-level conclusion. It pinpoints areas of risk, such as compromised hosts on the network, which allows you to assess the risk and act to prevent exploitation of network resources. The Automated Correlation Engine uses Correlation objects to analyze the logs for patterns, and when a match occurs it generates a correlated event.

Detailed information is here:

©2016-2019, Palo Alto Networks, Inc.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-the-automated-correlation-engine.html

Sample Questions

112. Which filter finds all log entries for traffic that originates from the internal device whose IP address is 172.17.1.3 and according to the header appears to be HTTP or HTTPS?
   A. (addr.src in 172.17.1.3) and ((port.dst eq 80) or (port.dst eq 443))
   B. ((addr.src in 172.17.1.3) and (port.dst eq 80)) or (port.dst eq 443)
   C. (src.addr in 172.17.1.3) and ((dst.port eq 80) or (dst.port eq 443))
   D. ((src.addr in 172.17.1.3) and (dst.port eq 80)) or (dst. port eq 443)

113. Which two log files would you use if you suspect that a rogue administrator is modifying the firewall's rulebase to allow and hide illicit traffic? (Choose two.)
   A. Traffic
   B. Threat
   C. Data Filtering
   D. Configuration
   E. System

114. Which product is required to use event correlation?
   A. next-generation firewall, PA-220
   B. Advanced Endpoint Protection
   C. Panorama
   D. GlobalProtect

©2016-2019, Palo Alto Networks, Inc.

3.3 Identify scenarios in which there is a benefit from using custom signatures

Before you can create a custom application, you must define the application attributes: its characteristics, category and subcategory, risk, port, and timeout. You also must define patterns or values that the firewall can use to match to the traffic flows themselves (the signature). Finally, you can attach the custom application to a Security policy that allows or denies the application (or add it to an application group or match it to an application filter). You also can create custom applications to identify ephemeral applications of a topical interest.

References

- Manage Custom or Unknown Applications
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-custom-or-unknown-applications
- Create a Custom Application
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application

Sample Questions

115. How is a custom application configured that uses DNS to transfer directory information and needs to be filtered in a very different manner than normal DNS?
   A. You cannot do it with the NGFW. You need to manually configure a proxy.
   B. Create specific rules for the sources and destinations that run this application.
   C. Create a custom signature and specify the DNS fields that are different from normal DNS use and patterns to identify when it is the custom application.
   D. Create an Application Override policy and specify the sources and destinations that run this application.

116. What are two results of using Application Override policies? (Choose two.)
   A. prevent matching traffic from entering VPN tunnels
   B. apply a specified App-ID label to matching traffic
   C. prevent matching traffic from being logged
   D. cause matching traffic to bypass Content-ID processing
   E. route traffic to WildFire for scanning

117. Which two types of entities can have custom signatures?
   A. Services
   B. URL categories
   C. User groups
   D. Applications
   E. Vulnerabilities

©2016-2019, Palo Alto Networks, Inc.

3.4 Given a scenario, identify the process to update a Palo Alto Networks system to the latest version of the software

Standalone Firewalls

For non-HA firewalls, software updates fall into two categories: subscription updates and PAN-OS upgrades.

Subscription updates are enabled through application of various licenses to the firewall. These updates are managed under **Device > Dynamic Updates**. Updates can be transferred directly from Palo Alto Networks on demand or by schedule control. In cases where no network connectivity is present, these updates can be downloaded from the Palo Alto Networks Dynamic Update section of the Support portal site onto an administrator's system and uploaded through a Management web interface connection and then applied.

This process is discussed here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates.html

PAN-OS updates are managed in the **Device > Software** section of the web interface. New PAN-OS versions can be downloaded and even installed without user disruption. A final system reboot must be performed to put the new PAN-OS software into production. This reboot is disruptive and should be done during a change control window.

A firewall does not need to upgrade to each released PAN-OS software in sequence. Considerations for skipping releases are outlined here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/upgrade-the-firewall-to-pan-os-90/determine-pan-os-upgrade-path.html

Make note of the requirement that dynamic updates be upgraded to the latest versions before PAN-OS software is upgraded to ensure compatibility.

You can undo PAN-OS upgrades if required. Details are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/downgrade-from-pan-os-90.html

Updates to App-ID signature information sometimes can reclassify previously labeled traffic, which might impact user access to critical applications. The firewall provides several mechanisms to review changes to App-IDs prior to or immediately after their installation.

A discussion of this issue and deployment techniques can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases

HA Firewalls

Dynamic updates are the responsibility of the individual firewalls to manage, even when they are in passive mode. This task can be difficult if dynamic updates have no network path to the Palo Alto

©2016-2019, Palo Alto Networks, Inc.

Networks update servers. Dynamic updates in HA clusters include an option to “Sync-to-peer” for use when the secondary firewall has no network route to the update server. Further discussion is here: https://live.paloaltonetworks.com/t5/Management-Articles/Scheduled-Dynamic-Updates-in-an-HA-Environment/ta-p/60449

Firewalls in HA clusters must upgrade PAN-OS software individually. In active/passive clusters a firewall typically is put into Suspend mode and then upgraded. After the upgrade is complete, the firewall is made active with the partner then going to Suspend mode and being upgraded.

A detailed discussion of this process appears here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/upgrade-the-firewall-to-pan-os-90/upgrade-an-ha-firewall-pair-to-pan-os-90

Upgrading Firewalls Under Panorama Management

Firewalls managed by Panorama can get dynamic updates from Panorama including scheduled updates. PAN-OS upgrades also can be managed from Panorama. A complete discussion is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates

Upgrading of Panorama-managed firewalls to PAN-OS 9.0 is discussed here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/upgrade-the-firewall-to-pan-os-90/upgrade-firewalls-using-panorama.html

HA Cluster Firewall Updates Managed by Panorama

Panorama treats managed firewalls in HA pairs as individual firewalls for software update purposes.

Sample Questions

118. In which order do you update dynamic content and the PAN-OS version?
    A. Update the PAN-OS version first, then the dynamic content.
    B. Update the dynamic content first, then the PAN-OS version.
    C. Update both at the same time.
119. In which order do you upgrade the different components of the firewall to a next version?
    A. firewalls, then Panorama, then Log Collectors
    B. Panorama and the Log Collectors, then the firewalls
    C. Log Collectors, Panorama and the firewall
120. How do you upgrade a High Availability pair (A/P) to PAN-OS 9.0? Assume you need to keep internet access up during the upgrade.
    A. Upgrade the active firewall first, then the passive one.
    B. Upgrade the passive firewall first, then the active one.
    C. Run the upgrade on the active firewall. It will manage the process and upgrade the passive firewall.
    D. You must upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

©2016-2019, Palo Alto Networks, Inc.

3.5 Identify how configuration management operations are used to ensure desired operational state of stability and continuity

Firewall settings are stored in XML config files that can be archived, restored, and otherwise managed.

Running Configuration and Candidate Configuration

A firewall contains both a running configuration that contains all settings currently active, and a candidate configuration. The candidate configuration is a copy of the running configuration that also includes settings changes not yet committed. changes made in the firewall web interface stages these changes in the candidate configuration until a commit operation merges them, with the running configuration making them active.

If you back up versions of the running or candidate configuration, you can later restore those versions on the firewall. A discussion about the basics is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-configuration-backups

Guidelines for configuration management are here:
https://live.paloaltonetworks.com/t5/Featured-Articles/Backing-Up-and-Restoring-Configurations/ta-p/65781

Sample Questions

121. What is the format of the configuration files?
    A. YAML
    B. JSON
    C. XML
    D. Some are in XML. Some in YAML
122. Which CLI command do you use to copy a partial configuration file to a firewall?
    A. **scp** from a different device. The firewall serves as the file server.
    B. **ssh** from a different device. The firewall serves as the file server.
    C. **scp** from the firewall's CLI. A different computer serves as the file server.
    D. **ssh** from the firewall's CLI. A different computer serves as the file server.

©2016-2019, Palo Alto Networks, Inc.

3.6 Identify the settings related to critical HA functions (link monitoring; path monitoring; HA1, HA2, and HA3 functionality; HA backup links; and differences between A/A and A/P)

High Availability (HA) is when two firewalls are placed in a group and have their configuration synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover if a peer goes down. Configure two firewalls in an HA pair to provide redundancy and allow you to ensure business continuity.

References

- HA Concepts (including the subtopics)
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/ha-concepts
- What is HA-Lite on Palo Alto Networks PA-200?
  https://live.paloaltonetworks.com/t5/Learning-Articles/What-is-HA-Lite-on-Palo-Alto-Networks-PA-200-and-VM-Series/ta-p/62553
- HA Links and Backup Links
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links
- Set Up Active/Passive HA
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activepassive-ha.html
- Set Up Active/Active HA
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activeactive-ha.html
- See additional information in *section 1.3 Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements that leverage the Palo Alto Networks Security Operating Platform*

Sample Question

123. Which option is an intended advantage of an active/active HA pair vs. an active/passive pair?
   A. increased throughput
   B. support of asynchronous routing
   C. increased session count
   D. shared dynamic updates

©2016-2019, Palo Alto Networks, Inc.

3.7 Identify the sources of information that pertain to HA functionality

Network monitoring applications use SNMP to query network components such as the NGFW. The firewall has additional information specific to HA. You now can monitor the dedicated HA2 interfaces of firewalls, in addition to the HA1, HA2 backup, and HA3 interfaces. Use the IF-MID and the interfaces MIB to see SNMP statistics for dedicated HA2 interfaces.

Panorama includes *Managed Device Health Monitoring* which displays limited HA status information in the summary display in the Panorama management web interface.

References

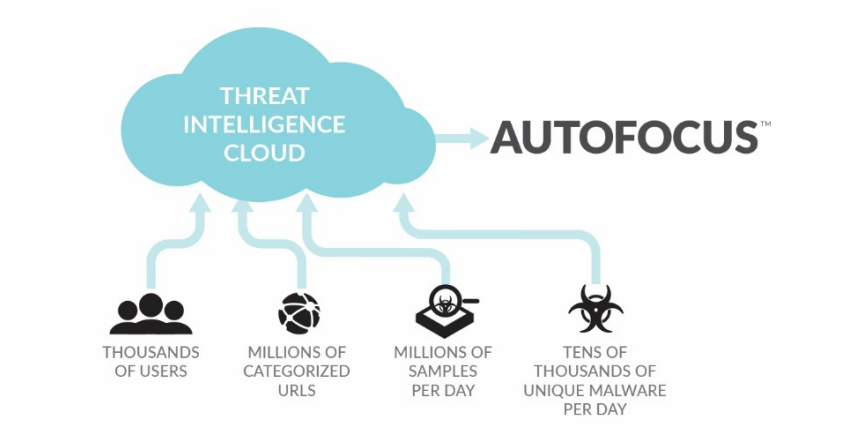
- SNMP Support
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps/snmp-support
- Monitor Statistics Using SNMP
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps/monitor-statistics-using-snmp
- Supported MIBs
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps/supported-mibs
- Using Device Health Monitoring from Panorama
  https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-device-health.html

Sample Question

124. Which MIB specifies the fields for information about the High Availability interfaces?
   A. MIB-II
   B. IF-MIB
   C. PAN-COMMON-MIB.my
   D. PAN-PRODUCT-MIB.my

©2016-2019, Palo Alto Networks, Inc.

3.8 Identify how to configure the firewall to integrate with AutoFocus and verify its functionality



AutoFocus is a threat intelligence service that provides an interactive, graphical interface for analyzing threats in your network. You can use AutoFocus to compare threats in your network to threat information collected from other networks in your industry or across the globe, within specific time frames. AutoFocus statistics are updated to include the most recent threat samples analyzed by Palo Alto Networks. Access to this information allows you to stay current with threat trends and to take a preventive approach to securing your network.

AutoFocus is a separately licensed product that is accessed in two primary ways: directly through the AutoFocus Portal, or by viewing AutoFocus-provided data in a firewall's web interface. The AutoFocus Portal is the primary access method for the evaluation of overall trends and characteristics of historical and current threats. This data can be used to characterize traffic seen on your network(s). Threats found by the firewall can be enriched by AutoFocus-provided contextual data. Additional threat context can be displayed for threats reported in your firewall logs.

Enablement of AutoFocus is a three-step process:

1) Enter your AutoFocus authorization code into the firewall's License Management.
2) Ensure that the correct URL to access AutoFocus is configured in the firewall.
3) Log in to the AutoFocus Portal and add information about your firewalls.

Details about this process can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence

References

- AutoFocus at a glance
  https://www.paloaltonetworks.com/resources/datasheets/autofocus-at-a-glance
- *AutoFocus Administrator's Guide*, especially the dashboard
  https://docs.paloaltonetworks.com/autofocus/autofocus-admin

©2016-2019, Palo Alto Networks, Inc.

Sample Question

125. A principle benefit of the AutoFocus product is:

A. Provide additional threat detection data to the firewall
B. Manage access to SaaS applications through the firewall
C. Provide additional context to previously discovered threats
D. Examine Cortex Data Lake log data for undetected threats

©2016-2019, Palo Alto Networks, Inc.

3.9 Identify the impact of deploying dynamic updates

Palo Alto Networks maintains a Content Delivery Network (CDN) infrastructure for delivering content updates to Palo Alto Networks firewalls. The firewalls access the web resources in the CDN to perform various App-ID and Content-ID functions. By default, the firewalls use the management port to access the CDN infrastructure for application updates, threat and antivirus signature updates, and access to the Palo Alto Networks WildFire® cloud. To ensure that you are always protected from the latest threats (including those that have not yet been discovered), you must keep your firewalls up-to-date with the latest content and software updates published by Palo Alto Networks.

App-ID updates have a special impact because new application definitions might affect current Security policy rules. PAN-OS software provides features to review the App-ID updates and modify the Security policy rules.

If your firewalls are managed by Panorama, the Panorama device can be the source of dynamic updates for managed firewalls and can configure the update schedule.

References

- Configure Content and Software Updates
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/app-and-threat-content-updates/configure-app-threat-updates
- Manage New App-IDs Introduced in Content Releases
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases.html#
- Managing dynamic updates from Panorama
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates

Sample Question

126. Which field in a new App-ID facilitates the determination of the App-ID's impact on policy enforcement?
   A. Name
   B. Depends on
   C. Previously Identified As
   D. App-ID Enabled

©2016-2019, Palo Alto Networks, Inc.

3.10 Identify the relationship between Panorama and devices as pertaining to dynamic updates versions and policy implementation and/or HA peers

You can use Panorama to qualify software and content updates by deploying them to a subset of firewalls, Dedicated Log Collectors, or WildFire appliances and appliance clusters before you install the updates on the rest of the firewalls. If you want to schedule periodic content updates, Panorama requires a direct internet connection. To deploy software or content updates on demand (unscheduled), the procedure differs based on whether Panorama is connected to the internet. Panorama displays a warning if you manually deploy a content update when a scheduled update process has started or will start within five minutes.

Panorama notifies the devices (firewalls, Log Collectors, and WildFire) that updates are available. The devices then retrieve the update packages from Panorama. By default, devices retrieve updates over the management (MGT) interface on Panorama. However, you can configure Panorama to use multiple interfaces if you want to reduce the traffic load on the MGT interface by using another interface for devices to retrieve updates.

HA firewalls are expected to have the same version content updates. Firewalls that are in an HA pair each implement an update process. In cases of Panorama management of update files, Panorama should schedule an update for both HA peers individually.

Firewalls in an HA configuration normally automatically sync their configurations with each other. When one firewall performs a commit, the changes are communicated to the other firewall and a commit is automatically triggered, thus keeping them in sync. When Panorama manages an HA firewall set, this automatic update is disabled, with the sync responsibility now belonging to Panorama. An administrator must include the HA pair in any changes made and committed on Panorama.

Reference

- Managing dynamic updates from Panorama https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates

Sample Questions

127. Which type of device can receive the Antivirus content update?
    A. Log Collector
    B. firewall
    C. AutoFocus
    D. MindMeld
128. What requirement must a Panorama meet to update a managed firewall's antivirus file?
    A. The PAN-OS versions on the firewall and Panorama must be the same
    B. Panorama and the firewall must be able to connect to Palo Alto Network's update server
    C. The update must be installed on Panorama before any firewalls
    D. Panorama must download an antivirus file version compatible with the target firewall's PAN-OS version

©2016-2019, Palo Alto Networks, Inc.

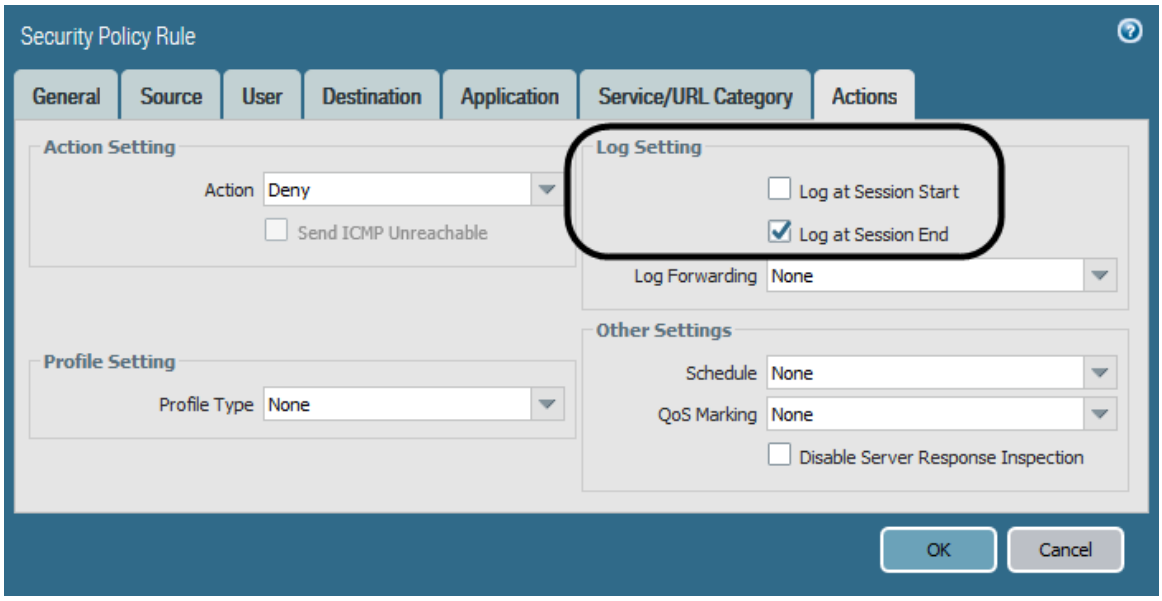
Exam Domain 4 – Configuration Troubleshooting

4.1 Identify system and traffic issues using the web interface and CLI tools

Palo Alto Networks firewall troubleshooting involves a wide range of specific knowledge that depends on the type of issue being presented. This section introduces a few principle tools and methods available for troubleshooting. The end of this section includes references for other tools and topics. Dedicated training classes for firewall troubleshooting also are available from Palo Alto Networks and Training Partners.

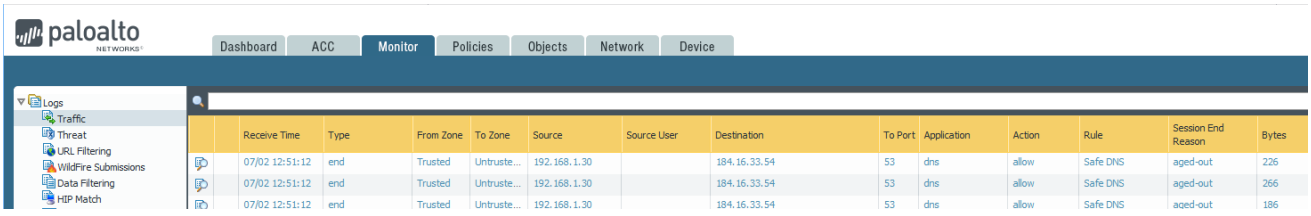
Transit Traffic Not Passing Through as Expected

If traffic is not transiting a firewall as expected, three primary information sources are available in the management web interface: the **traffic log**, the **session browser**, and **traffic capture** features.



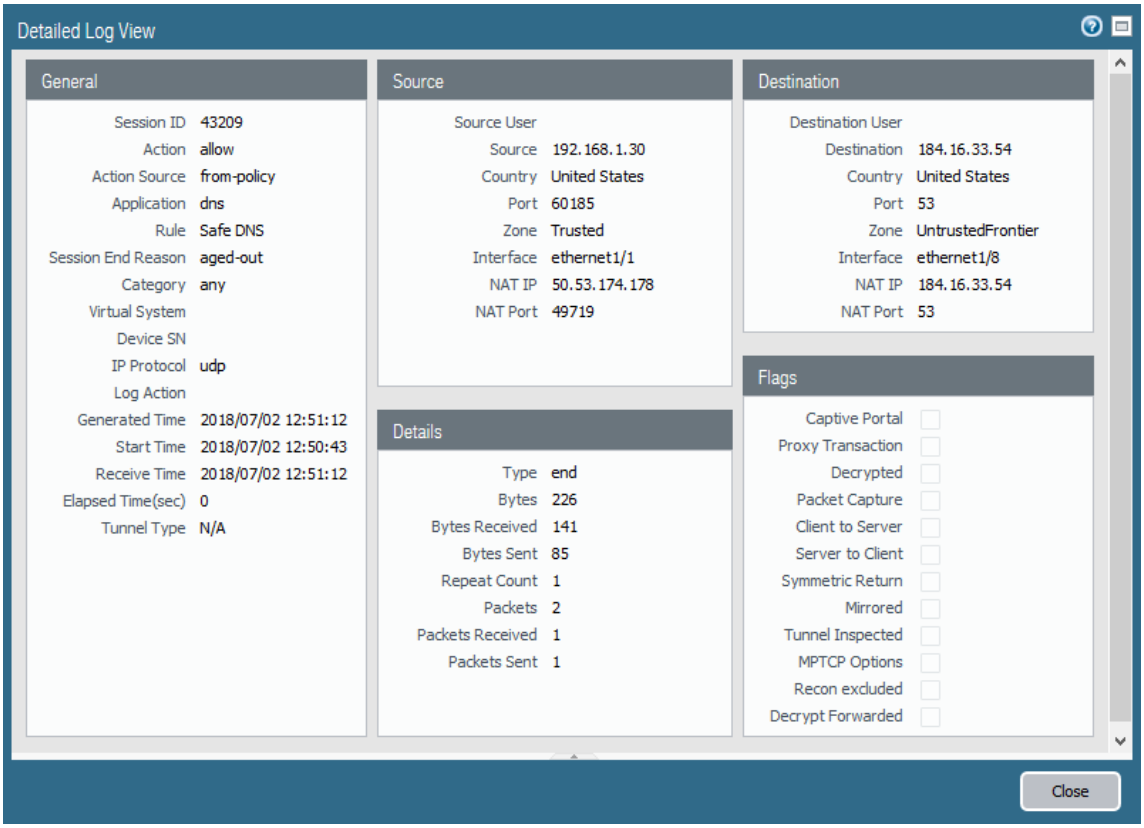
If you believe that the traffic to be evaluated has been received by the firewall, initial investigation should begin with the Traffic log. The Traffic log can be found at **Monitor > Logs > Traffic**. The default behavior of the firewall is to create a summary entry for each session when it ends. This behavior is controlled by the **Log Setting** included in the **Actions** tab of each Security policy rule. This setting controls the logging behavior of traffic handled by that rule only allowing different logging behavior for different traffic.

If the traffic in question includes at least one closed session an entry for it should appear. You can see detailed information about that session by clicking the **magnifying glass** icon in the left column:



©2016-2019, Palo Alto Networks, Inc.

The following screenshot shows the details of one of the entries listed:



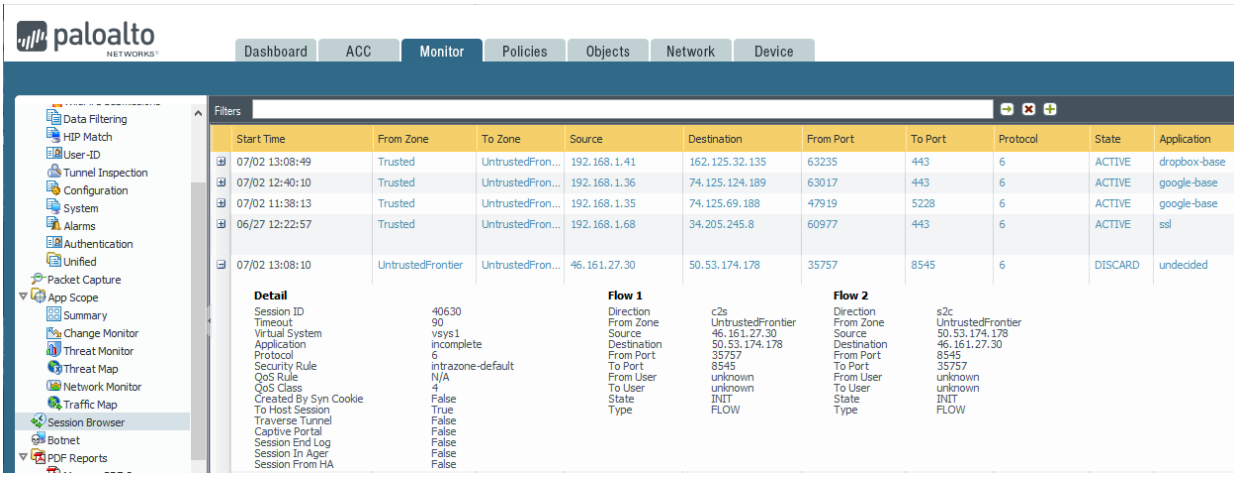
The presence of a log entry confirms that properly formed traffic has reached the firewall and has been evaluated by a Security policy rule. Traffic could be processed without reaching a session end, which would result in no log entry yet. The Session Browser allows troubleshooting of open sessions that might not have been logged yet.

The detailed session information should be used to evaluate the handling of the traffic. The Source and Destination sections display header data and confirm potential NATs being applied. The General section confirms the action taken by the Security policy rule and the rule's name, App-ID, protocol, time seen. and the reason the session ended. The Details section shows the packet summary for the reported session, including counts and size.

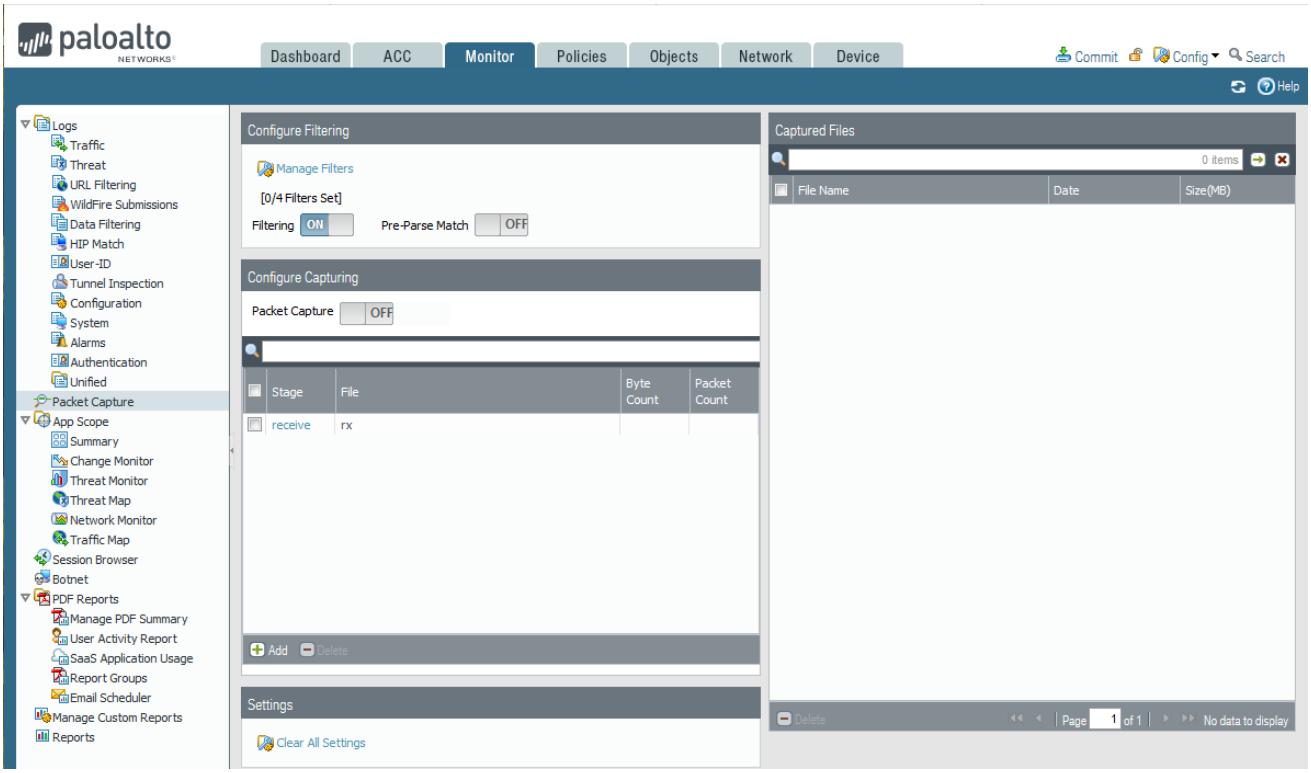
Examination of this information often confirms the firewall's handling of the traffic and might show unexpected behavior to correct as required.

When a session has not ended and no Traffic log entry has been made, you can use the session browser to display all open sessions currently known to the firewall. You can expand each session and examine details.

©2016-2019, Palo Alto Networks, Inc.



When troubleshooting requires the examination of actual packet contents, a packet capture can be performed on the firewall and subsequently downloaded as a pcap formatted file ready for external software consumption. Packet capture settings are found under **Monitor > Packet Capture**.



Following is a description of a suggested package capture use sequence.

Clearing Existing Settings

The **Clear All Settings** option turns off packet capture and clears all packet capture settings, including filters and capture stages. It also clears settings for any advanced debug-level packet-diagnostics features, such as flow basic, for which there are no controls or status indicators in the web interface. Use of **Clear All Settings** does not turn off automated packet captures associated with any active Security Profiles.

©2016-2019, Palo Alto Networks, Inc.

Warning: If you manually clear just the filters while another firewall administrator is actively running a capture, the running capture will start to capture all packets, with no filters. Before you clear any existing filters, confirm that the filters are not being used. If another administrator has saved filters that are meant to be used later, you can disable those filters rather than delete them. Use of **Clear All Settings** will clear all filters and turn off all capture.

Configuring and Turning on the Filters

You must turn on filtering and then turn on packet capture before any sessions that you want to capture have been initiated. Existing sessions will not be marked for capture.

Adding Stages and Filenames

Filtering alone is not resource-intensive, whereas turning on packet capture and/or turning on debug-level logging is resource-intensive. Therefore, the decision whether to configure your capture stages before or after turning on filtering generally is not that important.

You can, for example, configure your filters, turn them on, and then monitor them using CLI commands for session volume before you complete the rest of the configuration. To monitor the number of marked sessions, use the CLI command **`show counter global filter delta yes packet-filter yes`**. Execute the command once and then a second time to see the difference (the delta) from the prior execution of the command.

Tip: To analyze "inside" and "outside" sessions within a single file, you can configure the receive and transmit stages to write to the same filename, which will result directly in a merged pcap file.
When you configure a capture stage, you can specify the maximum number of bytes and/or the maximum number of packets, after which capturing stops.

A brief description of the four available capture stages follows:

- **Receive stage**: The firewall produces receive-stage packet captures by applying the capture filter(s) on a packet-per-packet basis. Receive-stage captures include all packets captured by the firewall's logical interfaces. Receive-stage captures can help you determine whether a packet is reaching the firewall.

  However, because of potential hardware offloading and pre-parse discards, a receive-stage capture may not produce exactly the same results as would physically tapping the wire just outside the correct physical ingress port of the firewall.

  The receive stage will not capture both flows of a session unless the filter configuration matches to traffic in each direction.

- **Firewall stage**: On firewalls running PAN-OS 8.0 and earlier, packets captured at the firewall and transmit stages will be captured when the corresponding session has been matched to a capture-filter statement. Firewalls running PAN-OS 8.1 and later capture packets at the firewall and transmit stages by the same effective logic (though not exactly the same) as the receive stage, that is, only if the individual flow (c2s or s2c) matches the filter configuration.

©2016-2019, Palo Alto Networks, Inc.

Firewall-stage capture shows you what is inside the box. The firewall-stage capture point is post-ingress, post-session-setup, and pre-NAT.

The flow logic of the firewall stage itself applies NAT as the last or nearly last step of Layer 2-to-Layer 4 packet processing and before any Layer 7 packet-payload content analysis begins. The IP addresses of packets captured by the firewall stage will match the pre-NAT addressing as defined in the session table. Also, packets that the firewall drops because of Layer 2-to-Layer 4 processing (such as packets dropped because of a session-closed status) will appear in the drop-stage pcap with pre-NAT addressing.

Packets that the firewall drops because of a "deny" action triggered by an App-ID policy or Security Profile will appear in the drop-stage pcap with post-NAT addressing.

If NAT is involved, the packet-threading features or flow-following or stream-following features of packet analyzers will not work for firewall-stage pcaps. With NAT, packet threading is possible only if you configure the receive-stage and transmit-stage pcaps and then merge them. You can make the firewall automatically merge receive-stage and transmit-stage pcaps by configuring them with the same filename.

- **Drop stage**: The drop-stage packet capture is perhaps best thought of as the result of a logging event, instead of a traditional off-the-wire packet capture. Packets in the drop-stage capture are captured after the capture point of the stage that drops the packet. Thus, packets in the drop-stage capture also will be found in the pcap for the stage from which the packet was dropped.

  A packet dropped in the receive stage will appear in both the drop-stage pcap and the receive-stage pcap. Typically you also will find packets that fail the initial session setup process in both the receive-stage and drop-stage pcaps. Packets dropped by or subsequent to the firewall stage will be found in both the drop-stage and firewall-stage pcaps.

  Drop-stage pcaps comprise copies of individual packets that are dropped. Drop-stage pcaps do not include prior or subsequent packets for contextual analysis. Drop-stage pcaps include only the exact packets dropped. If you want to better understand why a packet has been dropped, query the global counters, review log data, and run additional debug-level packet-diagnostic features such as flow basic.

- **Transmit stage**: Capture of packets at the transmit stage shows you packets as they egress from the firewall's logical interface. In transmit-stage pcaps you can see block pages, resets, TCP MSS adjustments, and any other packets or packet transformations created by the firewall itself, including post-NAT addressing.

Pre-Parse-Match Option

After a packet enters the ingress port, the firewall performs several basic pre-processing tests to ensure that the packet is viable before it is received for subsequent session setup and/or additional firewall processing. The firewall discards packets that fail these basic tests before the packet reaches the point where it is matched against the capture and debug-log filters. For example, if a route lookup fails, a

©2016-2019, Palo Alto Networks, Inc.

packet never will reach even the initial (receive) capture filter.

To capture packets that normally would be discarded before the filter match, the system emulates an initial, "pre-parse" positive match for every packet entering the system. This initial "match" allows all packets to be filtered subsequently by the normal receive-stage filtering process. The pre-parse match option is resource-intensive. You should consider using it only for advanced or otherwise rare troubleshooting purposes. Palo Alto Networks recommends that you use this option only under direct advice and guidance from technical support.

Troubleshooting of route-lookup failures is the typical use case that may require use of the pre-parse option. However, such errors typically are easy to identify using the firewall's interface counters.

To enable the pre-parse match option in the CLI, use the command debug **`dataplane packet-diag set filter pre-parse-match yes`**.

Turning On Capture

- After you turn on packet capture, you can monitor the capture in other ways to see if you are actively capturing any traffic:
- Refresh the Packet Capture page in the web interface and look first for the existence of new capture files, and then for their file size. You can refresh the page repetitively to monitor any growth in the file size.
- Use the CLI to show the current packet-diagnostics settings by running the debug **`dataplane packet-diag show setting`** command. The bottom of the settings summary includes the same data displayed in the "Captured Files" section of the Packet Capture page in the web interface.
- Monitor currently marked sessions, in addition to verifying that the capture-stage files are growing.

Turning Off Capture and Then Filtering

Turn off the packet capture before turning off filtering to avoid suddenly capturing all packets. You also may want to monitor any currently marked sessions using the CLI to ensure that the session(s) that you want to capture have finished. To show marked sessions, use the CLI command `show counter` **`global filter delta yes packet-filter yes.`** To show the detailed status of a session, use the command **`show session id [number]`**.

Exporting and Downloading pcaps

Exporting of pcaps from the web interface is a simple matter of clicking the hyperlink associated with the filename of the pcap you want to export. You can export pcaps from the CLI and display them in a similar way as you would use tcpdump within a Linux console.

The Palo Alto Networks firewall CLI offers access to more debugging information and often is used by experienced administrators for troubleshooting. This section provides only the briefest mention of basic CLI tools. The "References" section at the end of this section includes more complete information sources.

©2016-2019, Palo Alto Networks, Inc.

Connecting to the CLI is possible using a Serial console emulator or SSH connecting through the Management port. The account used for authenticating into the CLI must have CLI access enabled.

After you log in to the CLI, the command prompt by default will be in *operational mode*. The commands available within the context of operational mode include basic networking commands such as `ping` and `traceroute`, basic system commands such as `show`, and more advanced system commands such as `debug`. Debug commands allow you to set parameters that, if improperly used, can cause system failure. Commands to shut down and restart the system also are available from within operational mode.

Configuration mode enables you to display and modify the configuration parameters of the firewall, verify candidate configuration, and commit the config. Access it by typing the command `configure` while in operational mode.

CLI mode offers access to data not available in the web interface. Additional log files written by various subsystems of the firewall are available. Large files, i.e., log files, can be displayed with four principle commands: **`show`**, **`tail`**, **`less`**, and **`grep`**. A partial list of useful log files for troubleshooting can be found in the reference section at the end of this section.

The `show` command is the main method to display values and settings. In operational mode begin by typing show, a space, and then press the Tab key to invoke the autocomplete function showing all available options for the show command. Examine this list and explore options to become familiar with accessing settings and values for troubleshooting. The command **`show interface all`** displays a summary of all configured interfaces, their link status, and assigned zones. The command **`show system resources`** displays the overall resources utilization status of the firewall. For troubleshooting purposes, the **`test`** command shows the results when a simulated packet is presented to various subsystems. For example, the command **`test security-policy-match…`** shows the security processing of the simulated packet described at the end of the command. The command **`test routing…`** predicts the virtual router's handling of the simulated packet. Many **`test`** commands are available that can be found by entering **`test`** followed by a space and then the Tab key for the autocomplete listing of options.

Packet captures also can be performed at the command line level. The same packet capture engine explored earlier through the web interface can be accessed from the CLI. Each configuration step used in the web interface has a command line equivalent. See the "References" section for the location of a detailed discussion.

References

- Log Types and Severity Levels https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels.html
- **Monitor > Logs https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/monitor/monitor-logs.html**
- CLI Cheat Sheet: Device Management https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-device-management.html

©2016-2019, Palo Alto Networks, Inc.

- CLI Cheat Sheet: Networking https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking.html
- Interpret VPN error messages https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages.html

Sample Questions

129. Users cannot access their Gmail accounts through the firewall. Which log do you look in, and which filter do you use?
   A. Traffic, (app eq gmail)
   B. Traffic, (app in gmail)
   C. Configuration, (app eq gmail)
   D. Configuration, (app in gmail)

130. You can't get to the web interface. How do you check from the command line if it is running?
   A. ps -aux | grep appweb
   B. ps -aux | match appweb
   C. show system software status | grep appweb
   D. show system software status | match appweb

131. Which log file shows that a connection with an LDAP server was dropped?
   A. Traffic Log
   B. System Log
   C. User-ID Log
   D. Authentication Log

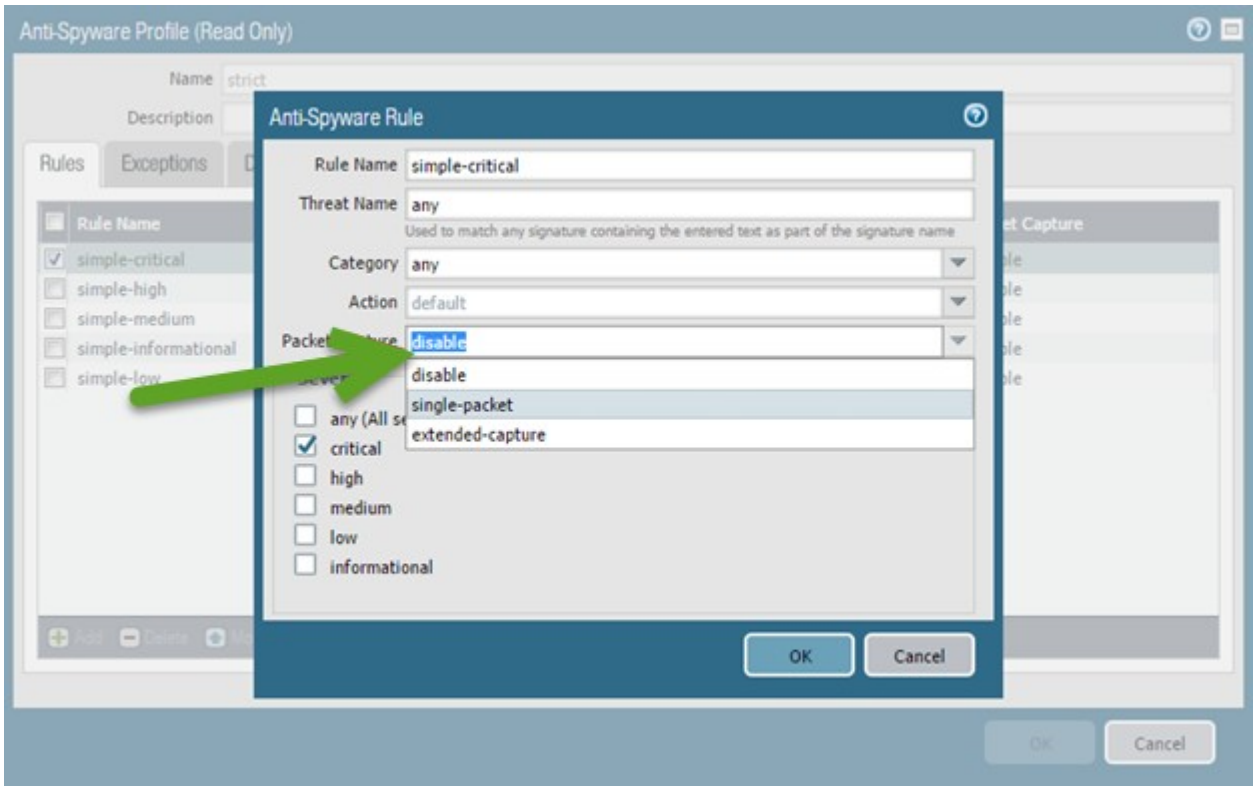
©2016-2019, Palo Alto Networks, Inc.

4.2 Given a session output, identify the configuration requirements used to perform a packet capture

Palo Alto Networks firewalls can capture traffic automatically in response to threat detection or can capture it manually. Capture tools are available in the web interface and CLI.

Automatic Threat Detection Captures

Automatic captures can be triggered as a response to threat detection. When Security Profiles are created, configuration settings can include a detection response of an automatic packet capture of the event. All threat-detecting Security Profiles have this capability. An example follows:



Configuring a packet capture response to the detection of spyware

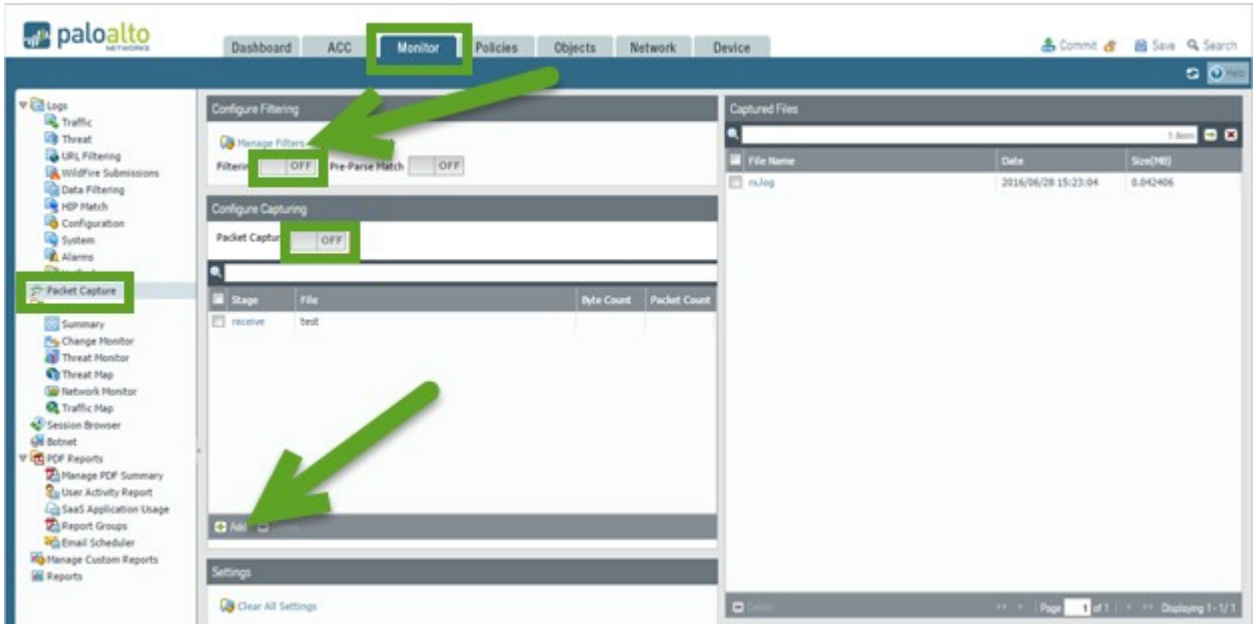
Information about configuring threat detection captures and accessing the captured data is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/take-packet-captures/take-a-threat-packet-capture.html

Data Filtering Security Profiles can take captures of configured patterns. Because this data might be highly valuable, special password protections are provided for these stored captures. Details are here: https://live.paloaltonetworks.com/t5/Management-Articles/Enable-data-capture-for-data-filtering-and-manage-data/ta-p/65934

©2016-2019, Palo Alto Networks, Inc.

Manual Packet Captures

Packet captures can be conducted on demand both from the web interface and the CLI. Web interface captures are configured in the **Monitor > Packet Capture** option. This packet capture process will *not* capture management interface traffic. The following image shows configuration options to create a web interface capture and turn it on/off. Captured traffic is stored on the firewall and is available for download as a pcap file usable by many protocol analysis software packages. The capture configuration follows:



The PAN-OS web interface provides access to traffic packet captures. Additional pcap and debug tools are available through the CLI.

Complete information about the configuration and use of this feature is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/take-packet-captures/take-a-custom-packet-capture.html

Note: Some Palo Alto Networks firewalls include a Hardware Offload feature that optimizes the handling of traffic. Offloaded traffic will not appear in packet captures in either the web interface or the CLI. PA-3050, PA-3060, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls have this feature. To guarantee that all packets are available for capture, a CLI command must be run to temporarily disable Hardware Offload. See the following information for details and disclosures about CPU impact. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/take-packet-captures/disable-hardware-offload.html

Note: Management interface traffic cannot be captured by the previously mentioned CLI tools. The **`tcpdump`** command is the only tool with visibility to this traffic.

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

132. Which Security Profiles do not have a packet capture option?
    A. Antivirus
    B. Anti-spyware
    C. Vulnerability Protection
    D. URL Filtering
133. On a PA-7080, which feature (if any) do you need to disable to use packet capture?
    A. None
    B. Hardware offload
    C. Hardware acceleration
    D. Decryption
134. Under which circumstance must you use tcpdump on the next-generation firewall?
    A. CLI capture of tunnel interface traffic
    B. CLI capture of packets on traffic interfaces
    C. CLI capture of packets on the management interface
    D. CLI capture of IPsec negotiation traffic

©2016-2019, Palo Alto Networks, Inc.

4.3 Given a scenario, identify how to troubleshoot and configure interface components

PAN-OS software supports a variety of interface configuration options. The network interfaces on a firewall fall into two general types: Traffic ports and the Management port.

Traffic Ports

Traffic ports provide multiple configuration options with the ability to pass traffic through to other ports via traffic-handling objects (virtual routers, virtual wires, and VLANs).

Management Port

The Management port is isolated from internal connectivity for security purposes. If the Management port requires internet access, its traffic must be routed out of the firewall and through other network infrastructure that provides this connectivity. The traffic often is routed back to a traffic port on the firewall requiring appropriate Security Policies for access. This traffic then is treated like any other and must be allowed through by Security policies.

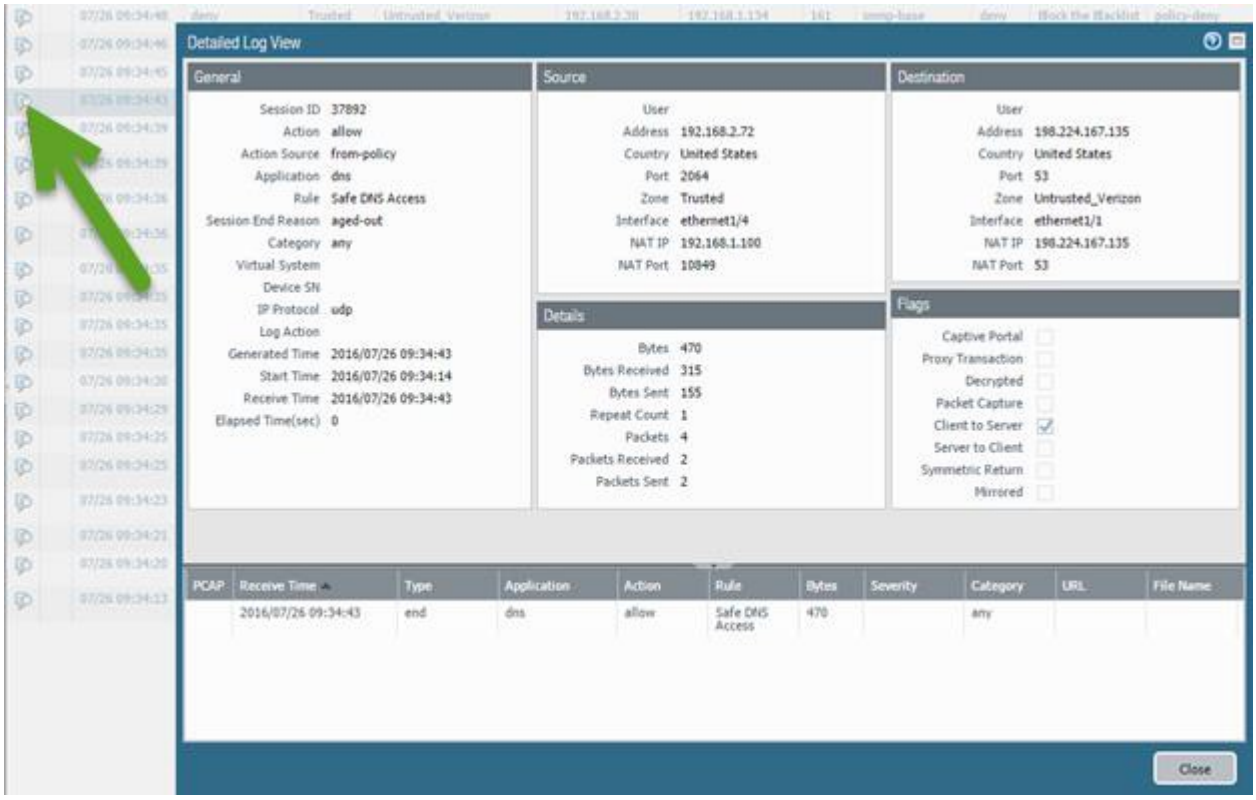
This management traffic can be routed through alternate ports. A discussion is here: https://live.paloaltonetworks.com/t5/Configuration-Articles/Setting-a-Service-Route-for-Services-to-Use-a-Dataplane/ta-p/59433

©2016-2019, Palo Alto Networks, Inc.

Troubleshooting Tools

There are several important tools for troubleshooting traffic flow through the firewall. A best practice in troubleshooting is to separate general connectivity issues from those of security. Connectivity issues should be resolved before security processing is evaluated.

The web interface provides several important tools. The path **Monitor > Logs > Traffic log** provides session summary information. Log entries for traffic are generated as specified in Security policies. The typical configuration specifies that log entries are created when a session ends. Use the magnifying glass icon to examine this log entry for detail:

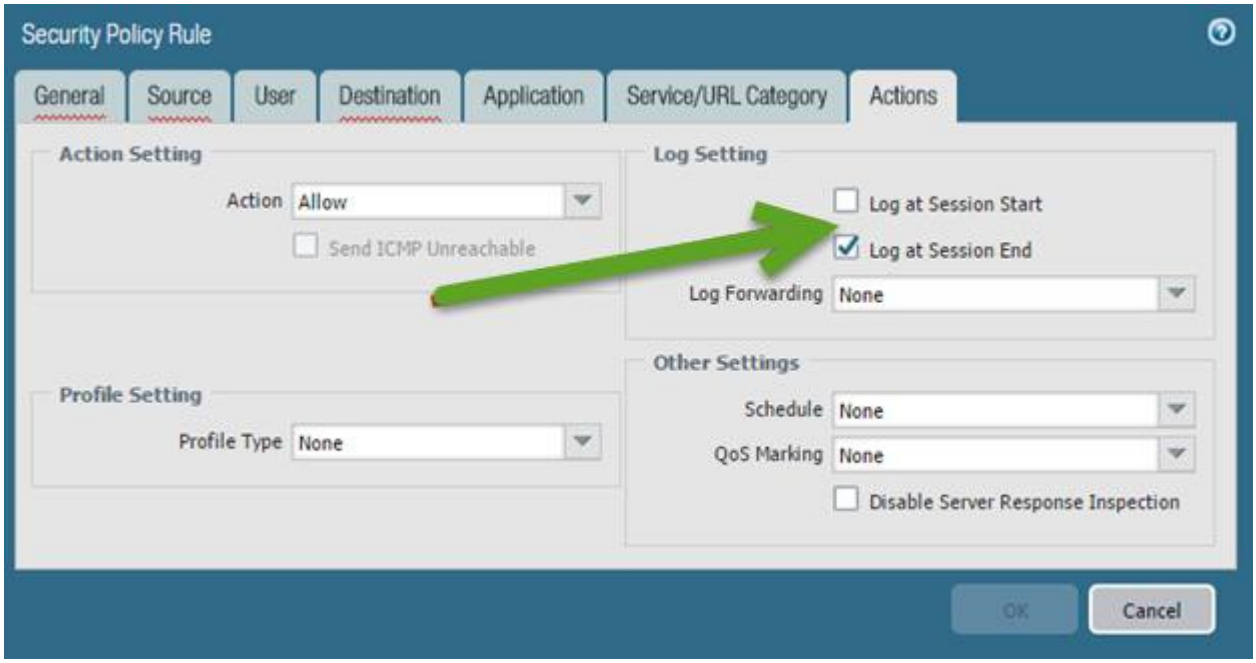


©2016-2019, Palo Alto Networks, Inc.

Log Entry Detail

Details found here include much information for troubleshooting: the Security action, the firewall policy allowing it through, the assigned App-ID, zones, and the ingress and egress interfaces. NAT details and flags attesting to other handling details also appear. Examine this data to get valuable insight into the firewall's processing of this traffic from both connectivity and security processing views.

This data typically is written at session end, but logging settings can specify log entries be created at session initiation time. This practice drives more log volume, but it can provide critical data in certain situations. Turn on Log at Session Start temporarily during troubleshooting to provide more information and gain insight:



Turning on entry creation at session initiation time temporarily can aid in troubleshooting.

View open sessions using the **Monitor > Session Browser** display:

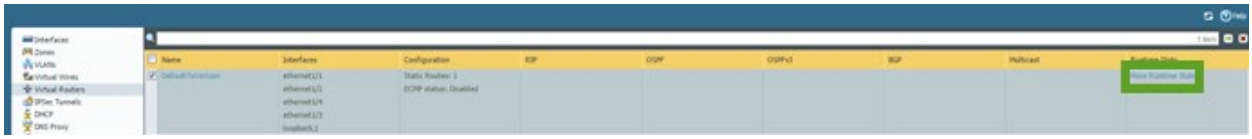
View open sessions within the session browser

The Clear check box at the end of a session summary line can be used to end the session immediately, often generating the desired log entry.

©2016-2019, Palo Alto Networks, Inc.

The CLI **show** commands will assist with troubleshooting. The web interface traffic capture and CLI pcap and debug functions give greater visibility to system-level operation for troubleshooting. A complete discussion about packet captures is here: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/take-packet-captures.html

Connectivity issues often arise from unexpected traffic forwarding decisions. You can view forwarding decisions by displaying the Layer 3 routing and forwarding tables in the web interface:



Display the specific virtual router's routing and forwarding tables with this link.

Note that policy-based forwarding (PBF) policies can override routing decisions and must be considered when you troubleshoot connectivity. The routing and forwarding tables mentioned do *not* show the effects of existing PBF policies. PBF troubleshooting is best done on the CLI; **show** commands can display existing PBF policies and whether they are active. The **test pbf-policy-match** command will show the application of existing PBF policies on modeled traffic.

Sample Questions

135. Where in the user interface can you see if any sessions are going through a specific interface?
    A. dashboard
    B. Application Control Center (ACC)
    C. session log node in the Monitor tab
    D. The session browser node in the Monitor tab
136. Communication through a specific interface works most of the time but fails when traffic is at its highest. In which policy do you look to identify the problem?
    A. Security policy
    B. DoS Protection Policy
    C. QoS Policy
    D. Application Override Policy
137. Which interface mode allows you to add firewall protection to a network with the least disruption?
    A. Tap
    B. Layer 3
    C. Layer 2
    D. Virtual Wire

©2016-2019, Palo Alto Networks, Inc.

4.4 Identify how to troubleshoot SSL decryption failures

PAN-OS software can decrypt and inspect inbound and outbound SSL connections going through the Palo Alto Networks firewall. SSL decryption can occur on interfaces in Virtual Wire, Layer 2, or Layer 3 mode by using the SSL rulebase to configure which traffic to decrypt. Decryption can be based on URL categories and source user and source/target addresses. Once traffic is decrypted, tunneled applications can be detected and controlled, and the decrypted data can be inspected for threats, URL filtering, file blocking, or data filtering. Decrypted traffic is never sent off the device.

References

- Decryption Overview
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-overview.html
- How to Implement and Test SSL Decryption
  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEZCA0

Sample Questions

138. SSL decryption has been working for the customer but suddenly it stopped. What could be a possible reason?
   A. The firewall's CA certificate expired. By default, those certificates are valid for one year.
   B. The firewall's IP address, which is encoded in the certificate, changed.
   C. The firewall has been upgraded to a different model.
   D. The firewall's decryption subscription expired.

139. The company uses a small SaaS provider for some specialized need. This SaaS is provided through HTTPS. Suddenly, it stopped working through the firewall. When accessed from home, users receive an error about the certificate. Which two situations would explain this?
   A. The SaaS's certificate had expired. The firewall's decryption policy is configured to block connections with expired certificates.
   B. The SaaS's certificate had expired. The firewall's decryption policy is configured to use the untrusted CA with expired certificates.
   C. The SaaS's certificate was replaced with one whose Certificate Authority is not known to the firewall. The firewall's decryption policy is configured to block connections with certificates whose CA is not trusted.
   D. The SaaS's certificate was replaced with one whose Certificate Authority is not known to the firewall. The firewall's decryption policy is configured to use the untrusted certificate for certificates whose CA is not trusted.
   E. The firewall's own CA certificate needs to be updated.

140. Which encryption algorithm is not supported, and if the settings specify it using it causes the firewall to stop the connection?
   A. DES
   B. 3DES
   C. AES252-CBC
   D. AES256-GCM

©2016-2019, Palo Alto Networks, Inc.

4.5 Identify issues with the certificate chain of trust

Keys are strings of numbers that typically are generated using a mathematical operation involving random numbers and large primes. Keys are used to transform other strings (such as passwords and shared secrets) from plaintext to ciphertext (a process called encryption) and from ciphertext to plaintext (a process called decryption). Keys can be symmetric (the same key is used to encrypt and decrypt) or asymmetric (one key is used for encryption and a mathematically related key is used for decryption). Any system can generate a key.

X.509 certificates are used to establish trust between a client and a server to establish an SSL connection. The certificate contains either the FQDN of the server or its IP address in the common name (CN) field. All certificates must be issued by a certificate authority (CA). After the CA verifies a client or server, the CA issues the certificate and signs it with the CA's a private key. The client already has the CA's public key to verify those signatures.

With a Decryption policy configured, a session between the client and the server is established only if the firewall trusts the CA that signed the server certificate. To establish trust, the firewall must have the server root CA certificate in its certificate trust list (CTL) and use the public key contained in that root CA certificate to verify the signature. The firewall then presents a copy of the server certificate signed by the Forward Trust certificate for the client to authenticate. You also can configure the firewall to use an enterprise CA as a forward trust certificate for SSL Forward Proxy. If the firewall does not have the server root CA certificate in its CTL, the firewall will present a copy of the server certificate signed by the Forward Untrust certificate to the client. The Forward Untrust certificate ensures that clients are prompted with a certificate warning when they attempt to access sites hosted by a server with untrusted certificates.

References

- Keys and Certificates for Decryption Policies
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies.html
- Certificate Management
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/certificate-management.html
- How to Install a Chained Certificate Signed by a Public CA
  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkoCAC

Sample Questions

141. Which condition could be a symptom of a chain of trust issue?
    A. The firewall no longer decrypts HTTPS traffic.
    B. The firewall no longer decrypts HTTPS traffic from a specific site.
    C. The firewall still decrypts HTTPS traffic from all sites, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.
    D. The firewall still decrypts HTTPS traffic from a specific site, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.

©2016-2019, Palo Alto Networks, Inc.

142. Which field is mandatory in the subject field of a certificate?

A. Organization
B. Organizational Unit
C. Common Name
D. Locale

143. Which field in a certificate has to include a value known to the firewall for the certificate to be considered valid by the firewall?

A. Issuer
B. Subject
C. Key
D. Object

©2016-2019, Palo Alto Networks, Inc.

4.6 Given a scenario, identify how to troubleshoot traffic routing issues

There are several methods to route traffic using the NGFW:

- Static routes require manual configuration on every router in the network, rather than the firewall entering dynamic routes in its route tables. Even though static routes require that configuration on all routers, such routes may be desirable in small networks rather than having an administrator configure a routing protocol.
- Routing Information Protocol (RIP) is an interior gateway protocol (IGP) that was designed for small IP networks. RIP relies on hop count to determine routes; the best routes have the fewest number of hops. RIP is based on UDP and uses port 520 for route updates. By limiting routes to a maximum of 15 hops, the protocol helps prevent the development of routing loops, but also limits the supported network size. If more than 15 hops are required, traffic is not routed. RIP also can take longer to converge than OSPF and other routing protocols.
- Open Shortest Path First (OSPF) is an IGP that is most often used to dynamically manage network routes in large enterprise network. It determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The information gathered from the LSAs is used to construct a topology map of the network. This topology map is shared across routers in the network and is used to populate the IP routing table with available routes.
- Changes in the network topology are detected dynamically and are used to generate a new topology map within seconds. A shortest path tree is computed of each route. Metrics associated with each routing interface are used to calculate the best route. These metrics can include distance, network throughput, and link availability. These metrics also can be configured statically to direct the outcome of the OSPF topology map.
- **Border Gateway Protocol (BGP)** is the primary internet routing protocol. BGP determines network reachability based on IP prefixes that are available within autonomous systems (AS), where an AS is a set of IP prefixes that a network provider has designated to be part of a single routing policy.

References

- Virtual Routers
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/virtual-routers.html
- Site-to-Site VPN with Static and Dynamic Routing
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-and-dynamic-routing.html
- Static Routes
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/static-routes/static-route-overview.html
- RIP
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/rip.html
- OSPF
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/ospf.html
- BGP
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/bgp.html

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

144. Where do you find the dynamic routing configuration for data in the NGFW's web interface?
   A. Device > Network > Virtual Router
   B. Network > Virtual Router
   C. Device > Network > Interfaces
   D. Network > Interfaces

145. What could be two reasons that some IP addresses get good performance when going to websites, and others IP addresses in the same network get bad performance (with the same sites)? This is happening consistently; the same IP addresses always get the bad performance. The organization has redundant connections to the internet, and all three of them are up. (Choose two.)
   A. The organization uses equal-cost multi-path (ECMP) routing to the internet and selects which path to use based on the source IP address, and some IP addresses get routed through a slower ISP.
   B. The organization uses Policy Based Forwarding (PBF) and selects which route to use for the internet based on source IP address, and some IP addresses get routed through a slower ISP.
   C. The organization uses the Routing Information Protocol (RIP), and some IP addresses get routed through a slower ISP.
   D. The organization uses Border Gateway Protocol (BGP), and some IP addresses get routed through a slower ISP.
   E. The organization uses Open Shortest Path First (OSPF), and some IP addresses get routed through a slower ISP.

146. The organization has two links to the internet, one 100Mbps and the other 10Mbps. The firewall balances them using equal-cost multi-path (ECMP) in the virtual router. Which load balancing ECMP setting does the organization need to use to optimize network resources?
   A. Balanced Round Robin
   B. Weighted Round Robin, with a weight of 10 for the fast connection and 100 for the slow one.
   C. IP Hash
   D. Weighted Round Robin, with a weight of 100 for the fast connection and 10 for the slow one.

4.7 Given a scenario, identify how to troubleshoot a bootstrap install process

Bootstrapping speeds up the process of configuring and licensing a physical or VM-Series firewall to make it operational on the network, with or without internet access. Bootstrapping enables you to configure the firewall using an init-cfg.txt configuration file that enables the firewall to connect to the network and Panorama, and then obtain its complete configuration from Panorama. You can also fully configure the firewall with the basic init-cfg-txt configuration file and a bootstrap.xml file. Information from these two files is combined and fully configures the firewall.

Bootstrapping enables you to create a repeatable and streamlined process of deploying new firewalls on your network because it enables you to create a package and then use that package to deploy firewalls anywhere. You can bootstrap a physical or VM-Series firewall off an external device to complete the

©2016-2019, Palo Alto Networks, Inc.

process of configuring and licensing the firewall. External devices include a USB thumb drive, virtual disk, virtual CD-ROM, or a storage bucket such as AWS S3 or Google Cloud bucket.

For security reasons, you can bootstrap a firewall only when it is in factory default state. If your firewall will not bootstrap, ensure that it is in factory default mode. The procedure to reset a firewall to its factory default settings is at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/reset-the-firewall-to-factory-default-settings.html.

If you intend for the firewall to receive a complete configuration at boot-up rather than only a partial network configuration, ensure that you have created the optional bootstrap.xml file in the /config directory along with the init-cfg.txt file. The init-cfg.txt file contains only a partial firewall configuration that provides the basic information the firewall needs to connect to your network.

If any of the required network parameters is missing in the init-cfg.txt file, the firewall exits the bootstrap process and boots up using the default IP address, 192.168.1.1.

If you intend for Panorama to manage the bootstrapped firewall, then generate the VM auth key on Panorama and ensure that you place the key in the init-cfg.txt file. Otherwise Panorama will not be able to connect to and configure the bootstrapped firewall.

If your firewall is not licensed properly after bootstrapping, then ensure that you have used an auth code bundle in the /license directory instead of individual auth codes. Use of a bundle enables the firewall or orchestration service to simultaneously fetch all license keys associated with a firewall. If you use individual auth codes instead of a bundle, the firewall will retrieve only the license key for the first auth code included in the file.

If you are bootstrapping a VM-Series firewall in KVM using the user-data method and a tar ball, then ensure that your version of OpenStack Platform 5 (Icehouse based) has been patched appropriately. Without the patch, use of a tar ball with the user-data method causes the nova boot command to fail. The patch is located at https://bugs.launchpad.net/python-novaclient/+bug/1419859.

Bootstrap troubleshooting reference information can be found at https://docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-errors.html.

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 5 – Core Concepts

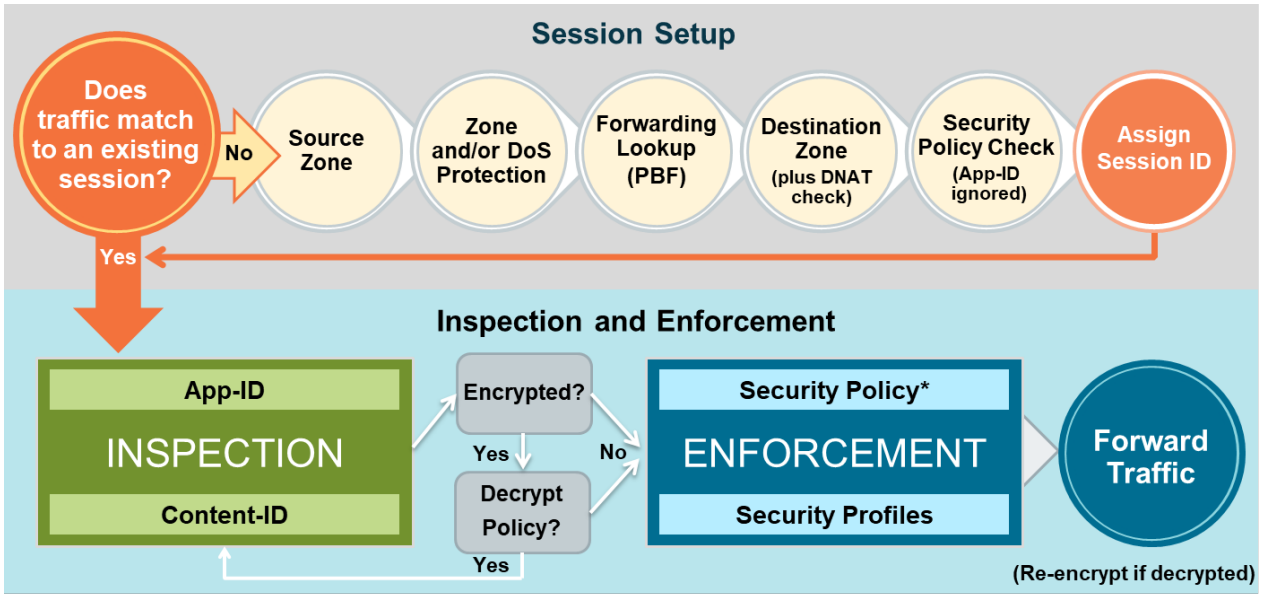
5.1 Identify the correct order of the policy evaluation based on the packet flow architecture

Policies

Palo Alto Networks firewalls implement several types of policies:

Types of Policies in a Palo Alto Networks Firewall

Every policy type is a list of policies. For every connection, policies are matched from the top down and the first match policy is applied – and that is the only policy of that type that is applied to that connection. The order in which policy types are applied is based on the packet processing order:



* Policy check relies on pre-NAT IP addresses

All traffic processed by the firewall follows this sequence of events.

©2016-2019, Palo Alto Networks, Inc.

Evaluation Order

An example of the importance of evaluation order can be found with NAT and Security policies. NAT policies change TCP/IP addresses in packet headers. Security policies are required to allow the traffic in question to transit the firewall. The processing order indicates that addresses changed by NAT policies are done *after* Security policies are evaluated, resulting in Security policies being written for pre-NAT packet addresses.

An overview of the different policy types is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/policy-types.html

Policy Match and Connectivity Tests

In PAN-OS® 9.0, you can perform policy match and connectivity tests for firewalls from the web interface rather than the CLI. You can easily test the running configuration of your firewalls and verify traffic and connectivity to ensure policy are matching policy rules as expected to allow or deny traffic, and that firewalls can connect to network resources and external services such as WildFire®, Log Collectors, or the Update Server.

Details about using the management web UI for testing can be found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/management-features/policy-match-and-connectivity-tests-from-the-web-interface.html

A dated but still useful article with examples for running the **`test`** command form the CLI is here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClQSCA0

Sample Questions

147. What is the correct order of operations between the Security policy and the NAT policy?
    A. NAT policy evaluated, Security policy evaluated, NAT policy applied, Security policy applied
    B. NAT policy evaluated, NAT policy applied, Security policy evaluated, Security policy applied
    C. NAT policy evaluated, Security policy evaluated, Security policy applied, NAT policy applied
    D. Security policy evaluated, NAT evaluated, NAT policy applied, Security policy applied
148. Which two statements are correct regarding policy evaluation?
    A. All policies are evaluated, and the most specific policy will match.
    B. Policies are evaluated from the top down, and the first match processes the traffic.
    C. Interzone traffic is allowed by default.
    D. Intrazone traffic is allowed by default.
    E. Outbound traffic is allowed by default. Only inbound traffic is evaluated.

©2016-2019, Palo Alto Networks, Inc.

149. In which of these operations is the order correct?

A. Decryption, check allowed ports, app-ID identification, check Security policy
B. Decryption, app-ID identification, check allowed ports, check Security policy
C. Check allowed ports, decryption, app-ID identification, check Security policy
D. Decryption, app-ID identification, check Security policy, check allowed ports

©2016-2019, Palo Alto Networks, Inc.

5.2 Given an attack scenario, identify the appropriate Palo Alto Networks threat prevention component to prevent or mitigate the attack

Advance Persistent Threats

Threats to your organization are growing in complexity and capability. Advanced persistent threats represent the most difficult challenge to the security professional.
An overview of APTs as they relate to Palo Alto Networks firewalls is here:
https://www.paloaltonetworks.com/features/apt-prevention

Security Policies and Profiles

The primary firewall tools protecting users from threats are Security policies combined with Security Profiles implementing specific protections.

The first steps in creating a Security policy are found here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/set-up-a-basic-security-policy.html

The completion of these steps provides only a basic setup that is not comprehensive enough to protect your network. The next phase is here:
https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices.html

The previous review includes a review of Security Profiles, which is an important aspect of protection detection and prevention for specific types of threats. See the following document for more details:
https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles.html

Sample Questions

150. A URL Filtering Profile is part of which type of identification?
   A. App-ID
   B. Content-ID
   C. User-ID
   D. Service

151. Which stage of the kill chain is most likely to be stopped by dividing the network into separate security zones and making sure all inter-zone traffic is inspected by a firewall?
   A. Reconnaissance
   B. Execution
   C. Lateral movement
   D. Data exfiltration

152. Which component can tell you if an attack is an advanced persistent threat (APT) or a broad attack designed to produce a botnet for future abuse?
   A. next-generation firewall
   B. WildFire
   C. MindMeld
   D. AutoFocus

©2016-2019, Palo Alto Networks, Inc.

5.3 Identify methods for identifying users

User-ID and Mapping Users

The User-ID feature of the Palo Alto Networks NGFW enables you to create policies and perform reporting based on users and groups rather than on individual IP addresses.

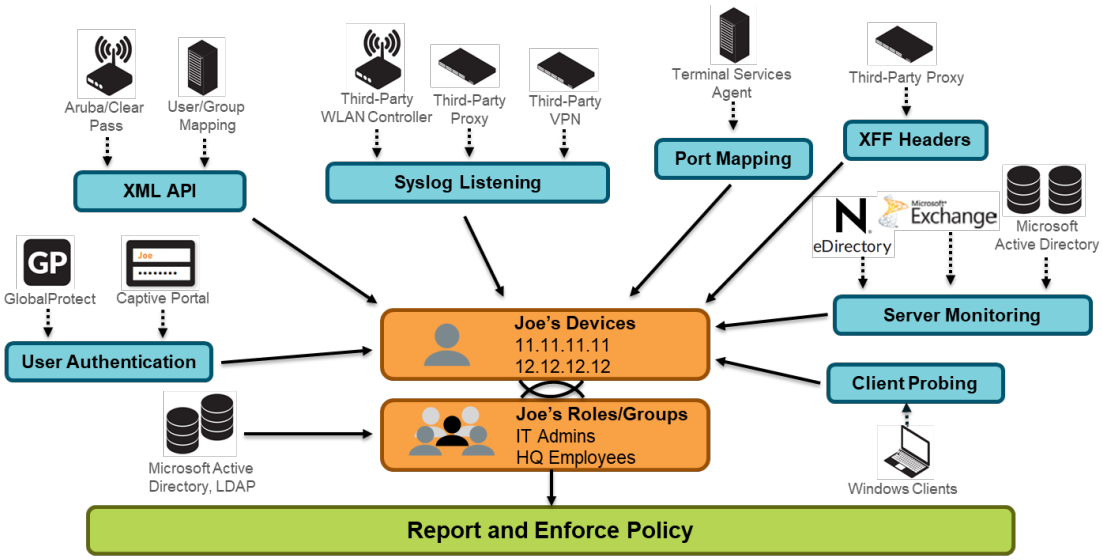
User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, enabling you to associate application activity and policy rules to users and groups—not just IP addresses. Furthermore, with User-ID enabled, the Application Command Center (ACC), App Scope, reports, and logs all include usernames in addition to user IP addresses.

For user- and group-based policies, the firewall requires a list of all available users and their corresponding group mappings that you can select when defining your policies. The firewall collects group mapping information by connecting directly to your LDAP directory server.

Before it can enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this user mapping information.

A User-ID agent process runs either on the firewall (Agentless implementation) or is installed as a separate process on a Windows OS machine. This User-ID agent monitors various network technologies for authentication events and gathers the data, creating a master IP-address-to-user mapping table stored in the firewall. For example, the User-ID agent monitors server logs for login events, probes clients, and listens for syslog messages from authenticating services. To identify mappings for IP addresses that the agent didn't map, you can configure the firewall to redirect HTTP requests to a Captive Portal login. You can customize the user mapping mechanisms to suit your environment, and even use different mechanisms at different sites.

In complex environments, multiple User-ID agents can be deployed to work collaboratively on a master User-ID-to-address mapping table. The following diagram illustrates the main functionality of the User-ID agent:



©2016-2019, Palo Alto Networks, Inc.

PAN-OS software can use multiple information sources to map usernames to the IP address of a session.

References

A complete overview of User-ID is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id.html
Design and deployment considerations for complex environments are here:
https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000D8S7AAK&field=Attachment_1__Body__s
Best practices for User-ID implementations are here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClF7CAK
and here:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVPCA0

Sample Questions

153. User-ID maps users to what type of information? (Choose the most accurate answer.)
   A. MAC addresses
   B. IP addresses
   C. IP address/port number combinations
   D. IP addresses in the case of single-user devices (tablets, PCs, etc.), IP address / port number combinations in the case of Linux and UNIX servers

154. What protocol or protocols does User-ID use to map between user identities and groups?
   A. NetBIOS
   B. LDAP
   C. syslog
   D. It can use both LDAP and syslog

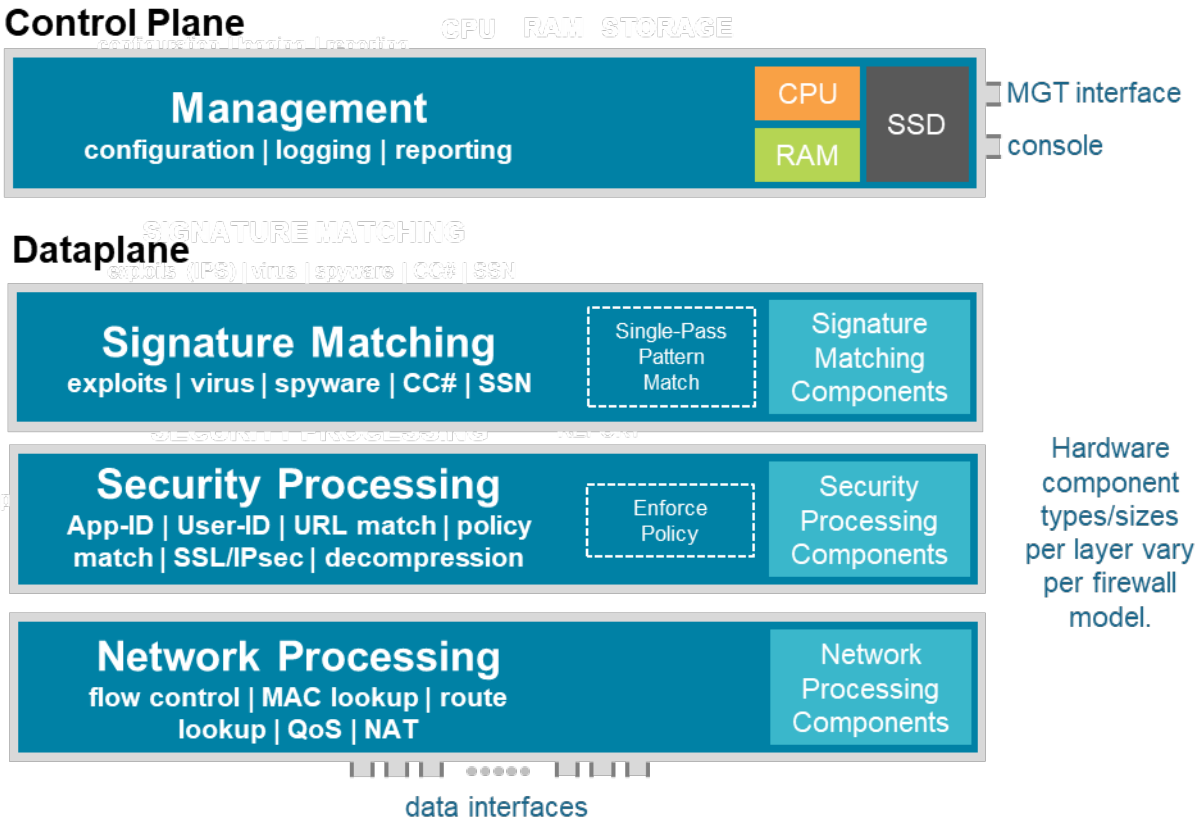
155. What format do you use when calling the API to inform the firewall of a new IP to user ID mapping?
   A. XML
   B. JSON
   C. YAML
   D. Base64

©2016-2019, Palo Alto Networks, Inc.

5.4 Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks firewall

Management Planes and Data Planes

Whether physical or virtual, the management plane and data-plane functionality is integral to all Palo Alto Networks firewalls. These functions have dedicated hardware resources, making them independent of each other. The following diagram details the architecture of a PA-220 firewall:



Palo Alto Networks maintains the management plane and data-plane separation to protect system resources.

Every Palo Alto Networks firewall assigns a minimum of these functions to the management plane:

- Configuration management
- Logging
- Reporting functions
- User-ID agent process
- Route updates

©2016-2019, Palo Alto Networks, Inc.

The Management Network and Console connector terminates directly on this plane. The following functions are assigned to the data plane:

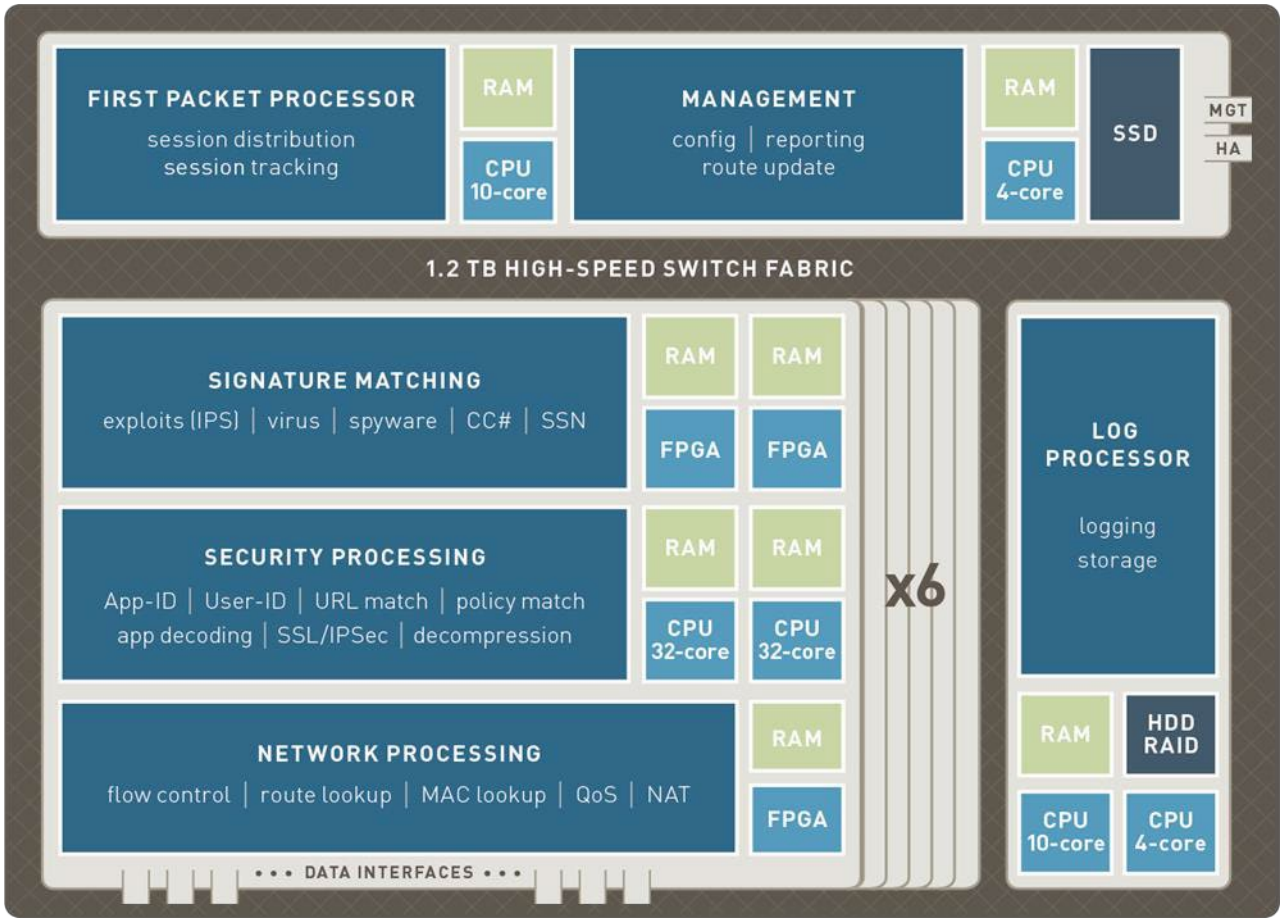
- Signature Match Processor:
  - All Content-ID and App-ID services
- Security Processors:
  - Session management
  - Encryption/decryption
  - Compression/decompression
  - Policy enforcement
- Network Processor:
  - Route
  - ARP
  - MAC lookup
  - QoS
  - NAT
  - Flow control

The data plane connects directly to the traffic interfaces. As more computing capability is added to more powerful firewall models, the management and data planes gain other functionality as required, sometimes implemented on dedicated cards. Several core functions gain FPGAs (field-programmable gate arrays) for flexible high-performance processing. Additional management plane functions might include:

- First packet processing
- Switch fabric management

©2016-2019, Palo Alto Networks, Inc.

Dedicated log collection and processing is implemented on a separate card. The following figure provides an overview of the PA-7000 Series architecture:



©2016-2019, Palo Alto Networks, Inc.

Sample Questions

156. On a PA-7000, which management function runs on a separate card?
    A. configuration management
    B. logging
    C. reporting
    D. The web user interface
157. Does the next-generation firewall use FPGA? If so, in which plane or planes?
    A. no, never
    B. yes, on the data plane, but only on higher-end models
    C. yes, on the management plane, but only on higher end models
    D. on both data the data plane and the management plane, but only on higher end models
158. Which function resides on the management plane?
    A. App-ID matching
    B. Route lookup
    C. Policy match
    D. Logging

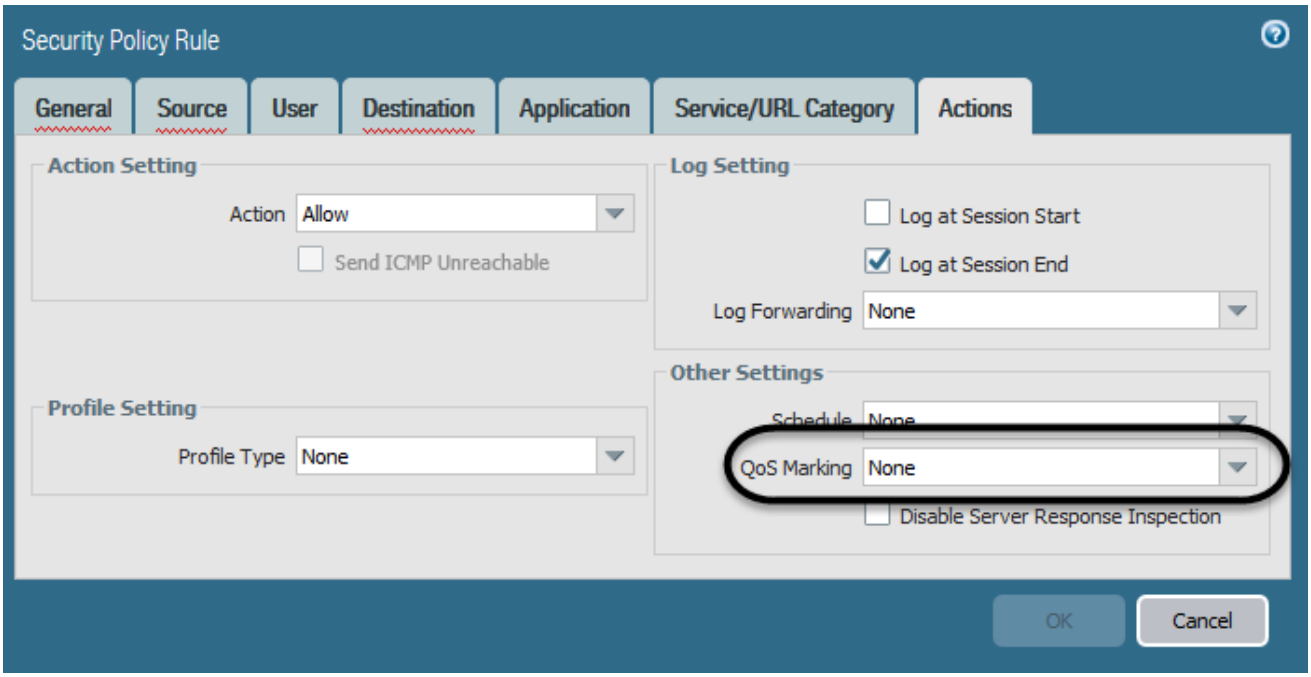
©2016-2019, Palo Alto Networks, Inc.

5.5 Given a scenario, determine how to control bandwidth use on a per-application basis

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish these tasks by providing differentiated handling and capacity allocation to specific flows in network traffic, which enables the network administrator to assign the order in which traffic is handled and the amount of bandwidth provided to traffic.

Palo Alto Networks QoS provides an "Application Aware" QoS service that can be driven by the traffic's App-ID. The firewall's QoS implementation is a self-contained system local to the firewall that can consider existing QoS packet markings but does not act directly on them. Traffic is evaluated against QoS policies that include existing QoS packet markings, App-ID, and other matching conditions to assign a traffic classification value of 1 through 8. These values are the basis for QoS decision making. QoS control of traffic is limited to egress traffic for the configured interface(s) only. Ingress traffic cannot be managed.

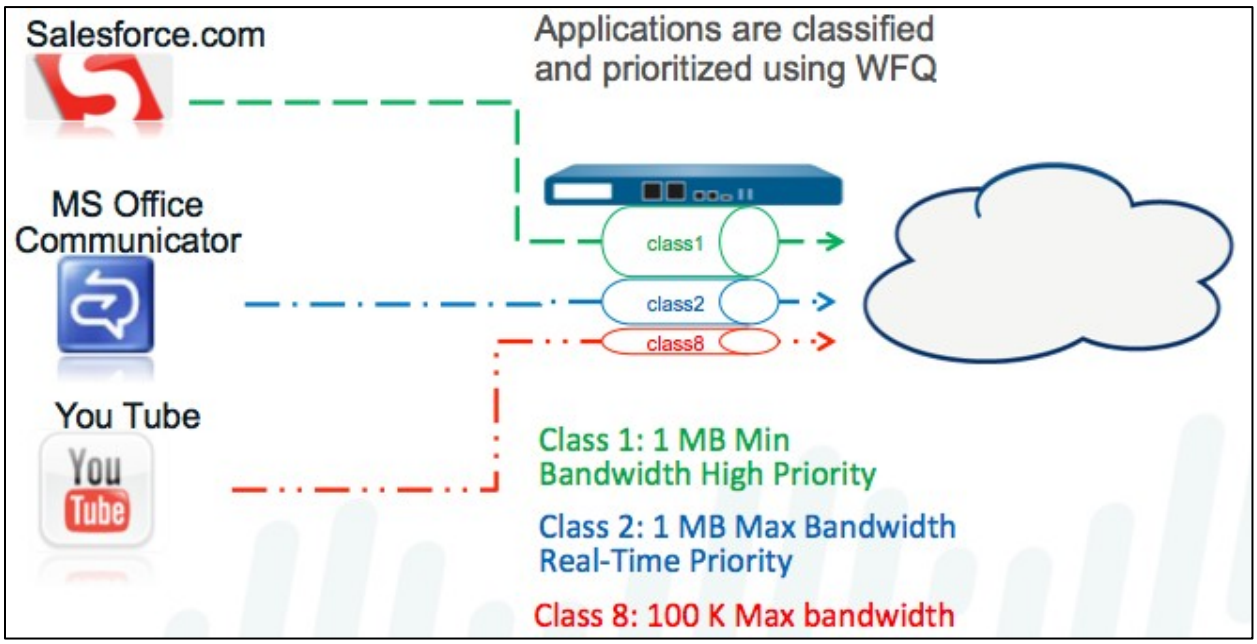
The method available to write QoS marking into packet headers is an additional action found in Security policy rules that applies to traffic that they process. This marking is not directly related to QoS processing in the firewall.



QoS implementation on a Palo Alto Networks firewall begins with three primary configuration components that support a full QoS solution: a QoS policy, a QoS Profile, and configuration of the QoS egress interface. Each option in the QoS configuration task facilitates a broader process that optimizes and prioritizes the traffic flow and allocates and ensures bandwidth according to configurable parameters.

QoS policies assign traffic classes (1-8) to traffic that matches the policy conditions.

©2016-2019, Palo Alto Networks, Inc.



PAN-OS QoS functionality can use App-ID for specific bandwidth reservation.

QoS Profiles describe the priority to be given to the specified traffic when the interface becomes constrained. As priority decreases, more packets are randomly dropped until the constraint is cleared. The number of packets dropped is determined by their assigned Priority. A real-time Priority setting means no packet dropping will be performed. High-, medium-, and low-priority settings indicate that greater levels of random packet dropping are performed during movement down the scale. No packets are dropped until the egress traffic on the managed interface becomes constrained, meaning that outbound traffic queues for the interface are filling faster than they can be emptied.

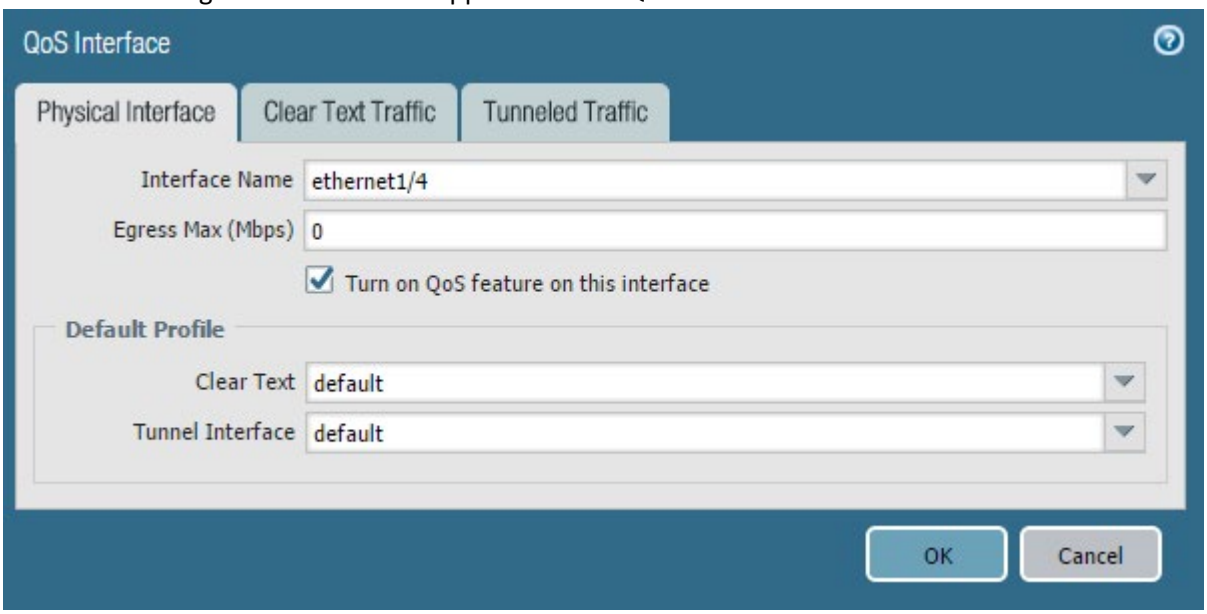
Profiles also specify maximum bandwidth enforcement applied at all times. Bandwidth configured as guaranteed can be used by all traffic until the interface becomes constrained, at which point traffic will be dropped to ensure that the specified traffic can reach its guaranteed bandwidth.

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
default			
class1			real-time
class2			high
class3			high
class4			medium
class5			medium
class6			low
class7			low
class8			low

©2016-2019, Palo Alto Networks, Inc.

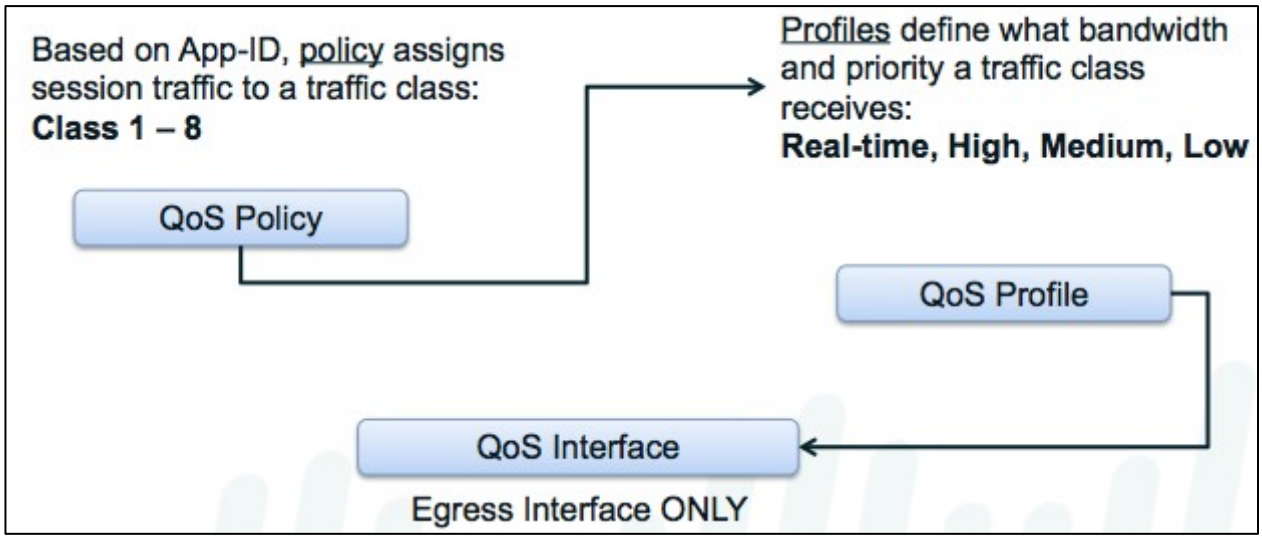
QoS Profiles prioritize specified traffic.

To apply a QoS Profile, assign it to an interface. All traffic on an interface is split between VPN (Tunnel Interface) and everything else (Clear Text). Each requires a QoS Profile assignment when present. Other tabs are available for optional QoS management that includes source interface, source subnet, and tunnel interface as matching conditions for the application of a QoS Profile.



Profiles are applied to interfaces to control their egress traffic.

The interrelationship between the QoS Policies, traffic classes, QoS Profiles, and interfaces is shown in the following image:



QoS is configured at the policy, profile, and interface level for granular control.

©2016-2019, Palo Alto Networks, Inc.

References

A detailed discussion of QoS is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/quality-of-service.html

Sample Questions

159. What parameter whose value is known to NGFW is important for QoS decisions?
   A. App-ID
   B. Content-ID
   C. User-ID
   D. Ingress interface

160. How many QoS classes does the next-generation firewall support?
   A. 4
   B. 8
   C. 16
   D. 32

161. Which additional information about an established connection cannot change its QoS class?
   A. App-ID
   B. URL category
   C. User-ID (if allowed for all users, and then the firewall gets the User-ID for a different reason)
   D. Content-type (for example, downloading an executable can have a different QoS class from downloading a PDF).

©2016-2019, Palo Alto Networks, Inc.

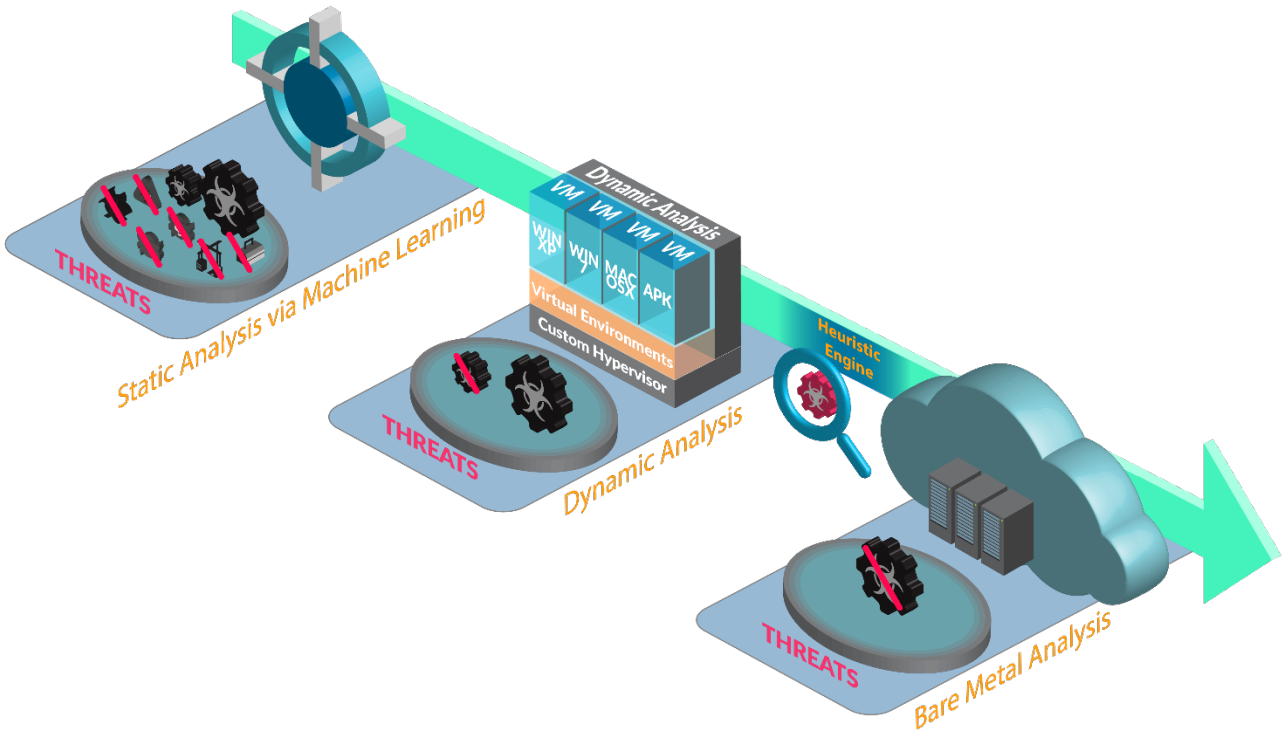
5.6 Identify the fundamental functions and concepts of WildFire

WildFire Overview

The WildFire Analysis Environment identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block the malware. When a Palo Alto Networks firewall is instructed to forward files vis a WildFire Analysis Profile, the firewall can automatically forward the sample for WildFire analysis. Based on the properties, behaviors, and activities that the sample displays when analyzed and executed in the WildFire sandbox, WildFire determines the sample to be benign, grayware, phishing, or malicious. WildFire then generates signatures to recognize the newly discovered malware and makes the latest signatures globally available every five minutes. Free WildFire users get the signature updates the following day, whereas WildFire license holders gain access to it within five minutes of generation. All Palo Alto Networks firewalls then can compare incoming samples against these signatures to automatically block the malware first detected by a single firewall.

WildFire is implemented in a Palo Alto Networks managed public cloud *or* a WF-500 appliance installed on a user's network.

The following figure outlines the principal workflow of WildFire:



WildFire looks within files for malicious activities and renders a verdict with an analysis report. WildFire analyzes files using the following methods:

- Static analysis: Detects known threats by analyzing the characteristics of samples prior to execution
- Machine learning: Identifies variants of known threats by comparing malware feature sets against dynamically updated classification systems

©2016-2019, Palo Alto Networks, Inc.

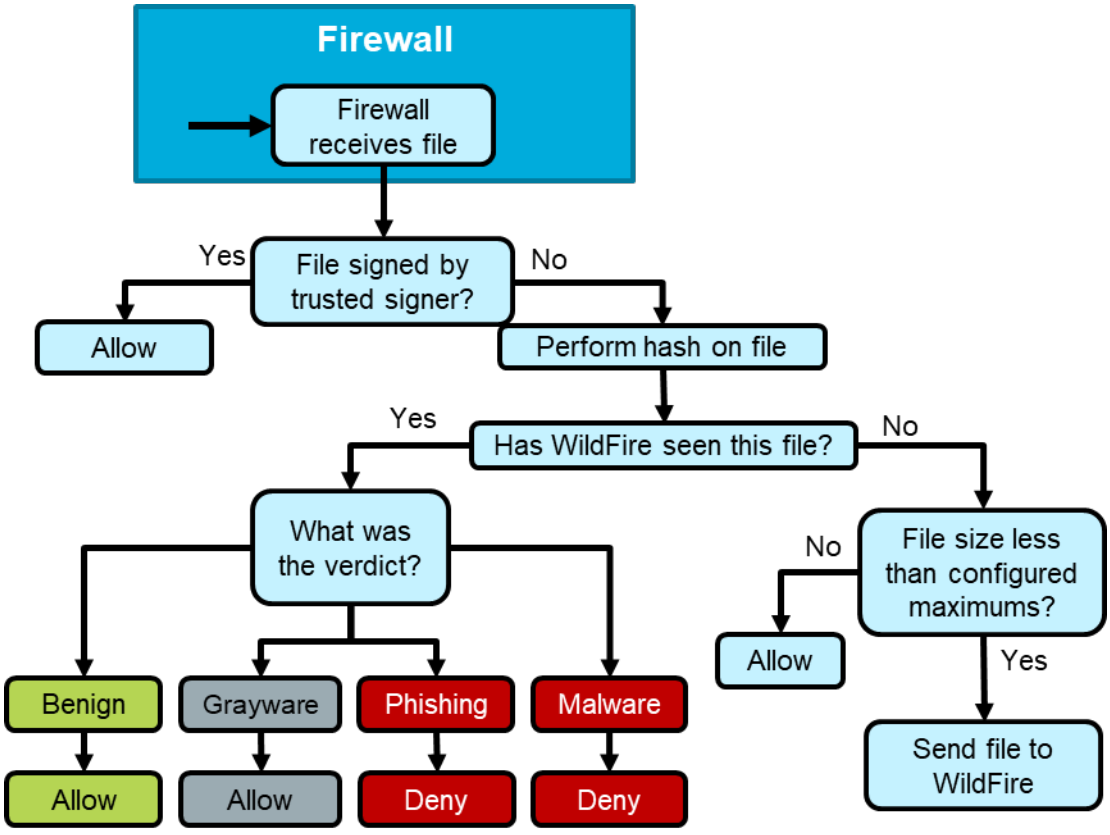
- Dynamic analysis: A custom-built, evasion-resistant virtual environment in which previously unknown submissions are detonated to determine real-world effects and behavior
- Bare metal analysis (WildFire cloud analysis only): A fully hardware-based analysis environment specifically designed for advanced VM-aware threats. Samples that display the characteristics of an advanced VM-aware threat are steered toward the bare metal appliance by the heuristic engine.

WildFire operates analysis environments that replicate the following operating systems:

- Microsoft Windows XP 32-bit
- Microsoft Windows 7 64-bit
- Microsoft Windows 7 32-bit (supported as an option for WildFire appliance only)
- Microsoft Windows 10 64-bit (WildFire cloud analysis only)
- Mac OSX (WildFire cloud analysis only)
- Android (WildFire cloud analysis only)
- Linux (WildFire cloud analysis only)

The WildFire public cloud also analyzes files using multiple versions of software to accurately identify malware that targets specific versions of client applications. The WildFire® private cloud does not support multi-version analysis and does not analyze application-specific files across multiple versions.

WildFire analysis of files is configured as WildFire Analysis Profiles attached to a Security policy rule allowing file transfer traffic. A file matching the policy then is evaluated by the WildFire Analysis Profile. If it matches, the firewall applies the following WildFire forwarding evaluation.



©2016-2019, Palo Alto Networks, Inc.

Files that are sent to WildFire for analysis are *not* quarantined in the firewall during the analysis process. They are forwarded normally to their destination. If WildFire detects malware, a notification can be sent which should then be treated as an Incident Response appropriate to your organization's policies.

WildFire is available to every Palo Alto Networks firewall for use at no charge. A WildFire license is available that provides additional WildFire features.

References

- A detailed description of WildFire is here: https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html
- The use of WildFire in firewall profiles is outlined here: https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/forward-files-for-wildfire-analysis.html

Sample Questions

162. Which file type is not supported by WildFire?
   A. iOS applications
   B. Android applications
   C. Windows applications
   D. Microsoft Excel files

163. The firewall will skip the upload to WildFire in which three cases?
   A. The file has been signed by a trusted signer.
   B. The file is being uploaded rather than downloaded.
   C. The file is an attachment in an email.
   D. The file hash matches a previous submission.
   E. The file is larger than 50MB.
   F. The file is transferred through HTTPS.

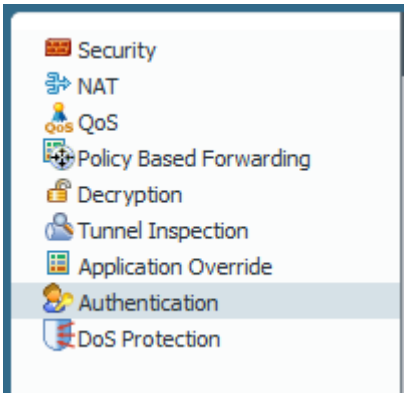
164. Which of these features is not supported on the WF-500 appliance?
   A. Bare Metal Analysis
   B. Microsoft Windows XP 32-bit analysis
   C. Microsoft Windows 7 64-bit analysis
   D. static analysis

©2016-2019, Palo Alto Networks, Inc.

5.7 Identify the purpose of and use case for MFA and the Authentication policy

You can configure multi-factor authentication (MFA) to ensure that each user authenticates using multiple methods (factors) when accessing highly sensitive services and applications. For example, you can force users to enter a login password and then enter a verification code that they receive by phone before allowing access to important financial documents. This approach helps to prevent attackers from accessing every service and application in your network just by stealing passwords.

The firewall makes implementation of MFA in your network easy by integrating directly with several MFA platforms (Duo v2, Okta Adaptive, and PingID) and integrating through RADIUS with all other MFA platforms.

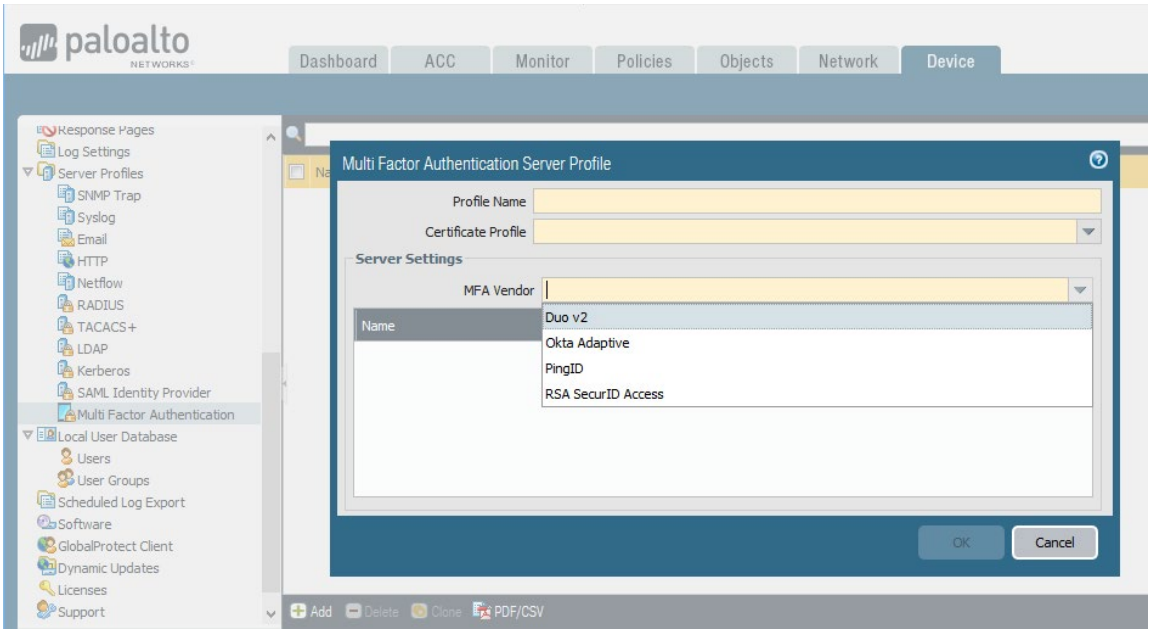


For end-user authentication via Authentication policy, the firewall directly integrates with several MFA platforms (Duo v2, Okta Adaptive, PingID, and RSA SecurID), and integrates through RADIUS or SAML for all other MFA platforms.

MFA is driven by an Authentication policy that allows precise application of appropriate authentication. These policies can invoke simple Captive Portal challenge pages for one-time authentication or can include one (or more) integrated MFA vendor Server Profiles that are included in Authentication Profiles for additional challenges.

Once a user successfully completes all challenges, an appropriate Security policy rule will be evaluated that allows access to that protected service.

©2016-2019, Palo Alto Networks, Inc.



References

- Multi-Factor Authentication https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/multi-factor-authentication.html
- Authentication Policy https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-policy.html

Sample Questions

165. What are the two purposes of multi-factor authentication?
   A. reduce the value of stolen passwords
   B. simplify password resets
   C. reduce/prevent password sharing
   D. ensure strong passwords
   E. provide single sign-on functionality

166. Which of these MFA factors is not supported by the next-generation firewall?
   A. Voice
   B. Push
   C. SMS
   D. S/Key

©2016-2019, Palo Alto Networks, Inc.

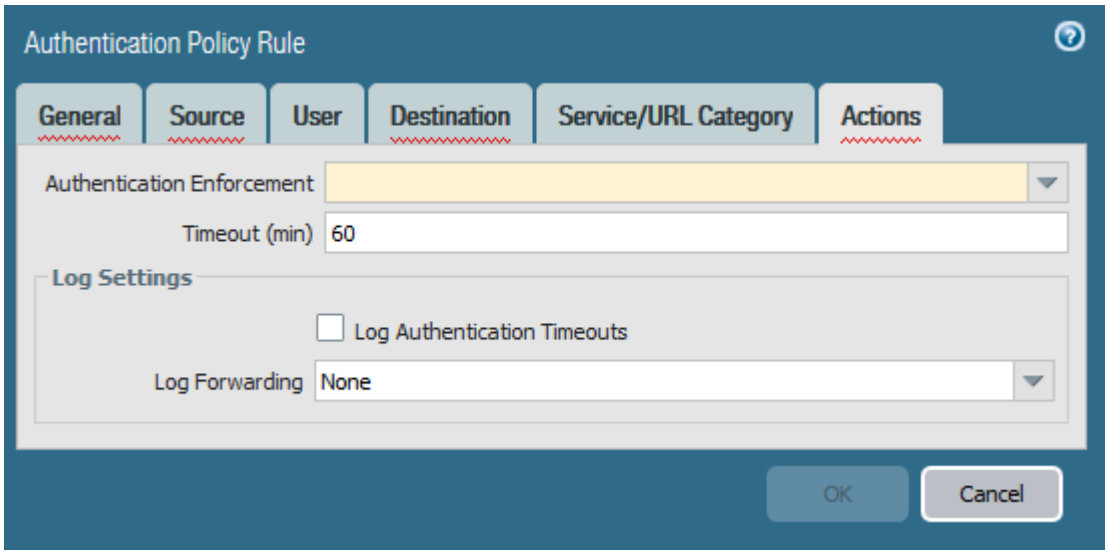
167. What is the meaning of setting the source user to known-user in an authentication policy rule?

A. The user identity is known (tied to an IP address), but the resource is sensitive enough to require additional authentication.
B. The next-generation firewall will demand user authentication, and only then will the resource be available.
C. The source device is a known device, which is only used by a single person.
D. There is no such option. If the user identity is known, there is no need for an authentication policy rule.

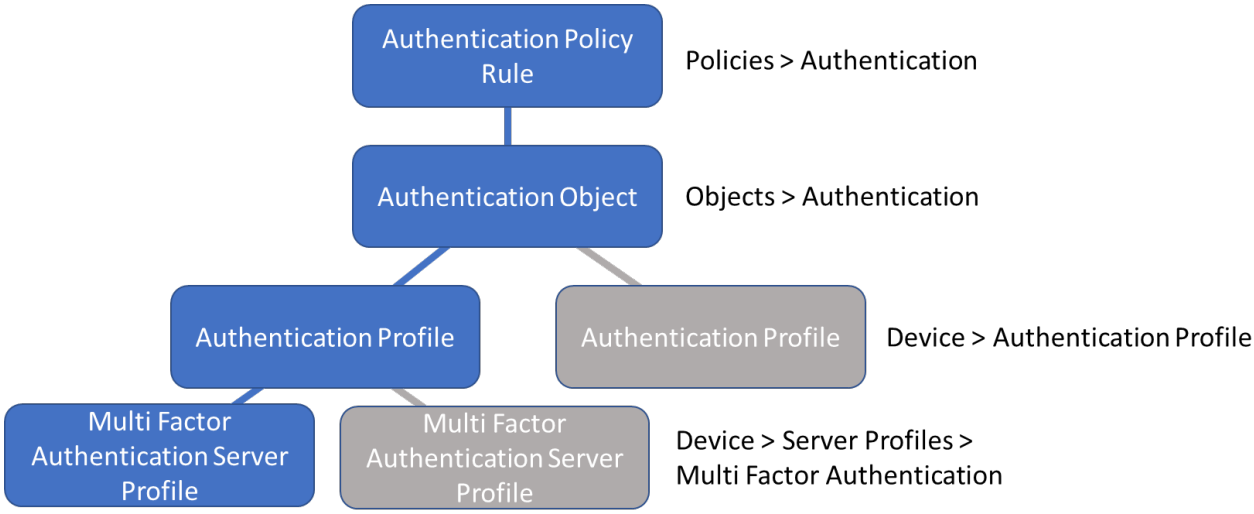
©2016-2019, Palo Alto Networks, Inc.

5.8 Identify the dependencies for implementing MFA

Before you can use multi-factor authentication (MFA) for protecting sensitive services and applications, you must configure several settings in the Palo Alto Networks firewall. MFA authentication is triggered when a user requests access to a service appearing in traffic that the firewall processes. The traffic is first evaluated by an Authentication policy rule. When a match is found, the authentication action of the rule is taken.

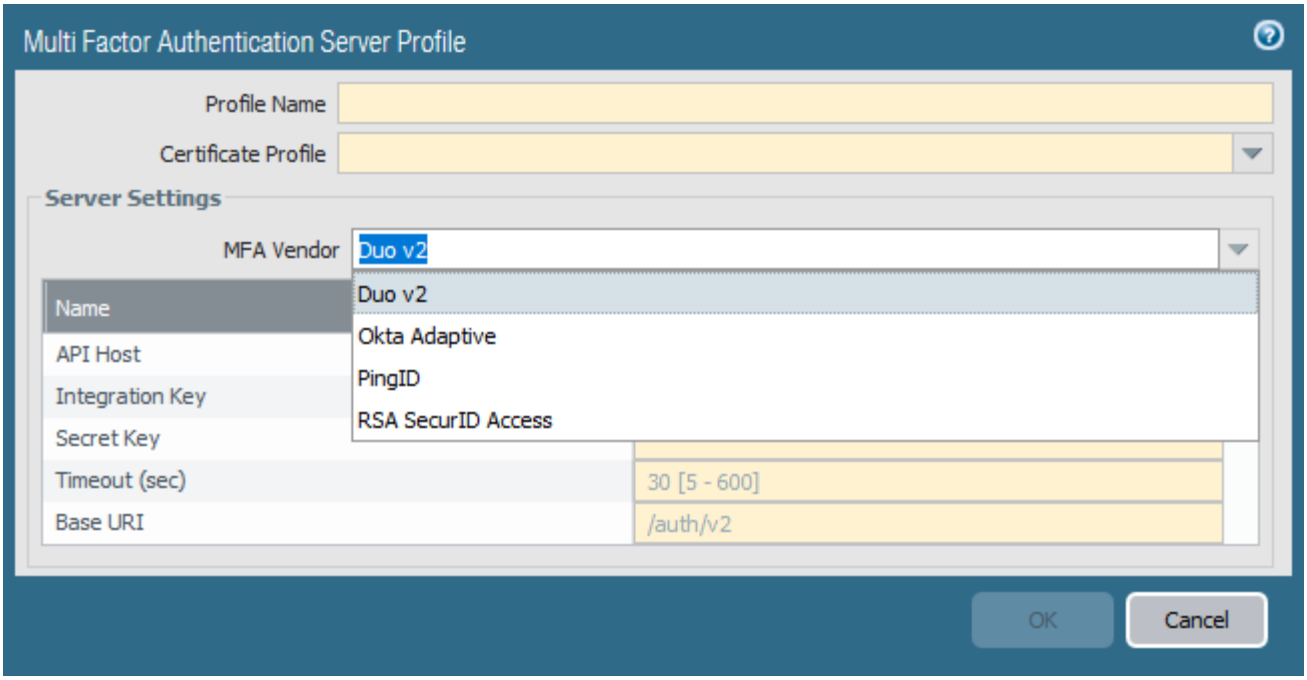


The following figure shows the relationship of the required objects to configure the Authentication policy rule.

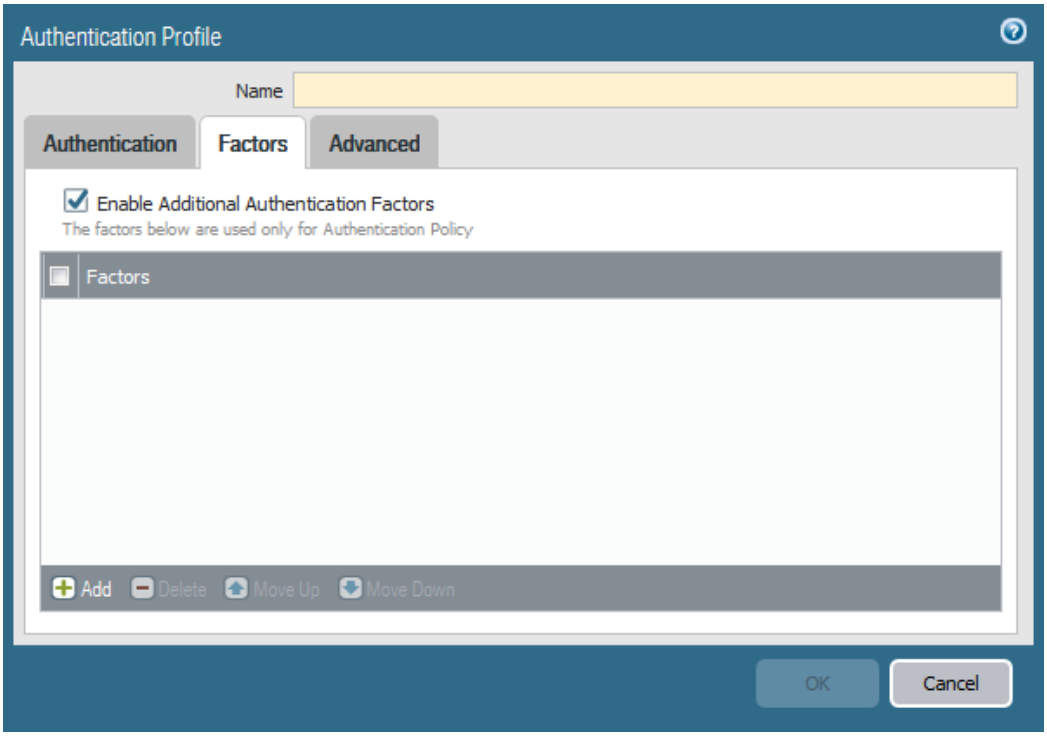


- Multi-Factor Authentication Server Profile: Defines the access method, location, and authentication for integrated MFA vendors. The MFA Vendor drop-down list shows supported vendors. A Certificate Profile is required to support the certificate used to validate the certificate used by the MFA solution to secure its communication with the firewall.

©2016-2019, Palo Alto Networks, Inc.



- Authentication Profile: Specifies the authentication type and Server Profile for the first Captive Portal-driven authentication. The Factors tab incorporates the integrated MFA vendor defined in the Multi Factor Authentication Server Profile. Multiple factors can be added that require the user to pass each challenge from the top down.



- Authentication Enforcement Object: Specifies the specific Authentication Profile to use and is assigned to an Authentication Policy rule. A Captive Portal Authentication Method also must be specified. A custom message can be included for the user that explains how to respond to the challenge.

©2016-2019, Palo Alto Networks, Inc.

References

- Configure Multi-Factor Authentication
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-multi-factor-authentication.html
- Map IP Addresses to Usernames Using Captive Portal
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html

Sample Questions

168. What are the two Captive Portal modes? (Choose two.)
   A. Proxy
   B. Transparent
   C. Web form
   D. Certificate
   E. Redirect

169. Which of these actions is not required to configure Multi-factor authentication using SAML and an Identity Provider (IdP)?
   A. Create an authentication policy rule.
   B. Configure NTLM settings.
   C. Create an authentication object.
   D. Create an authentication profile.

170. An Authentication policy rule has a HIP profile. Where are the users being authenticated coming from?
   A. internal devices, such as Linux workstations
   B. external devices belonging to customers of the organization
   C. internal servers running UNIX (Solaris, HPUX, AIX, etc.)
   D. GlobalProtect connections through the internet

©2016-2019, Palo Alto Networks, Inc.

5.9 Given a scenario, identify how to forward traffic

In a Layer 2 deployment, the firewall provides switching between two or more networks. Devices are connected to a Layer 2 segment; the firewall forwards the frames to the proper port, which is associated with the MAC address identified in the frame. The firewall uses virtual routers to obtain routes to other subnets by manually defining static routes or through participation in one or more Layer 3 routing protocols (dynamic routes). The routes that the firewall obtains through these methods populate the firewall's IP routing information base (RIB). An interface configured as Virtual Wire will forward all traffic that meets the optional VLAN filter to its partner Virtual Wire interface. This packet handling is done invisibly to the packet (aka Bump in the Wire). This allows a firewall to be placed in an existing traffic path without requiring traffic engineering of the infrastructure.

Palo Alto Networks firewalls also support Policy Based Forwarding. A Policy Based Forwarding rule can be created that identifies specific traffic to forward to a specified interface bypassing any virtual router lookup.

References

- Layer 2 Interfaces
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/layer-2-interfaces.html
- Virtual Routers
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/virtual-routers.html
- PBF (Policy-Based Forwarding)
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/policy-based-forwarding/pbf.html
- Use Case: PBF for Outbound Access with Dual ISPs
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/policy-based-forwarding/use-case-pbf-for-outbound-access-with-dual-isps.html

Sample Questions

171. A company has strict security requirements that require every connection between two internal computers to be inspected. Those internal computers are connected and disconnected by non-technical users. How do you forward traffic between those internal computers?
    A. Use a switch.
    B. Use an NGFW configured as a switch, with Layer 2 interfaces.
    C. Use an NGFW configured as a router, with Layer 3 interfaces.
    D. Use an NGFW in TAP or Virtual Mirror mode.

©2016-2019, Palo Alto Networks, Inc.

172. You have two links to the internet, going through two ISPs (for backup purposes). Link A has a lower latency, and link B supports a higher bandwidth. Which link would you use for VoIP, and how will you specify to use it?
   A. Link A, specify in a Policy Based Forwarding policy
   B. Link B, specify in a Policy Based Forwarding policy
   C. Link A, specify in a Virtual Router
   D. Link B, specify in a Virtual Router

173. Can you put devices on two sides of a VPN tunnel on the same Ethernet segment?
   A. No, because this requirement never happens.
   B. No, because Ethernet at layer 2 is a lower layer than a layer 3 VPN tunnel
   C. Yes, if you tunnel Ethernet over IP.
   D. Yes, because VPN tunnels can be layer 2 tunnels.

©2016-2019, Palo Alto Networks, Inc.

5.10 Given a scenario, identify how to configure policies and related objects

Security Policy Overview

The firewall will not allow any traffic to flow from one zone to another unless there is a Security policy rule to allow it. When a packet enters a firewall interface, the firewall matches the attributes in the packet against the Security policy rules to determine whether to block or allow the session based on attributes such as the source and destination security zone, the source and destination IP address, the application, the user, and the service. The firewall evaluates incoming traffic against the Security policy rulebase from left to right and from top to bottom and then takes the action specified in the first security rule that matches (for example, whether to allow, deny, or drop the packet). Because processing goes from the top to bottom, you must order the rules in your Security policy rulebase so that more specific rules are at the top of the rulebase and more general rules are at the bottom to ensure that the firewall is enforcing policy as expected.

The first steps in creating a Security policy are here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/set-up-a-basic-security-policy.html

The completion of these steps provides only a basic setup that is not comprehensive enough to protect your network. The next phase is here:
https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices.html

Security Profiles are an important aspect of protection detection and prevention for specific types of threats. See the following document for more details:
https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles.html

Security policies are a top-down first match and exit. Up to two processing steps are in each Security policy match. Step 1 confirms that a match has been made based on the matching conditions provided in the Security policy. If a match is found in Step 1, the traffic is logged (based on that policy's configuration) and the chosen action (deny, allow, drop, reset) is performed. Once processing is complete, there will be no further matching in the Security policy list.

Security Policy: Allow

If the action is "allow," Step 2 of the policy is evaluated. Step 2 is the application of configured Security Profiles. In Step 2, the content of sessions is scanned for various threat signatures, URLs can be scanned for unauthorized destinations, and files can be scanned for malware.

If Panorama device groups are used to push Security policy to one or more firewalls, the Security policy list is expanded to include rules before ("Pre") and after ("Post") the local firewall rules. Panorama rules are merged with local firewall policies in the position chosen during Panorama rule creation.

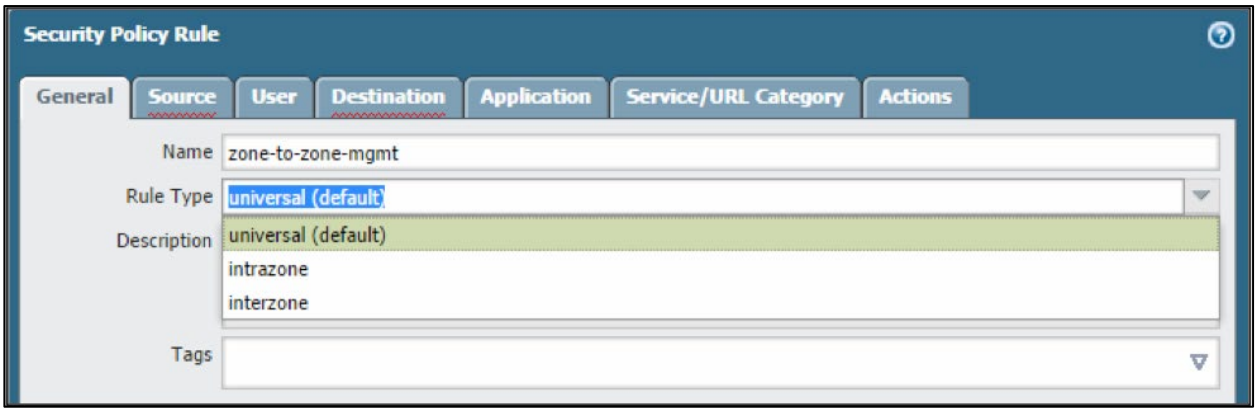
©2016-2019, Palo Alto Networks, Inc.

				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	Inbound FTP	none	universal	Untrust-L3	any	any	any	Trust-L3	172.16.11.1	ftp	application-d...	Allow	none
2	General Internet	none	universal	Trust-L3	any	any	any	Untrust-L3	any	dns flash ftp ping ssl web-browsing	application-d...	Allow	none
3	Allow YouTube	none	universal	Trust-L3	any	any	any	Untrust-L3	any	youtube	application-d...	Allow	none
4	Allow Facebook	none	universal	Trust-L3	any	any	any	Untrust-L3	any	facebook	application-d...	Allow	none
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none

Security policy should use App-ID for match criteria.

At the end of the list are two default policy rules: one for an Intrazone Allow and one for an Interzone Deny. Taken together they implement the default security behavior of the firewall to block interzone traffic and allow Intrazone traffic. The default logging is off for both.

Security policies in PAN-OS software are set by type: Universal (default), Interzone, and Intrazone. (All policies – regardless of type – are evaluated top-down, first match, then exit.) The Universal type covers both Interzone and Intrazone.



Security policy “rule type” selects the type of traffic the policy applies to.

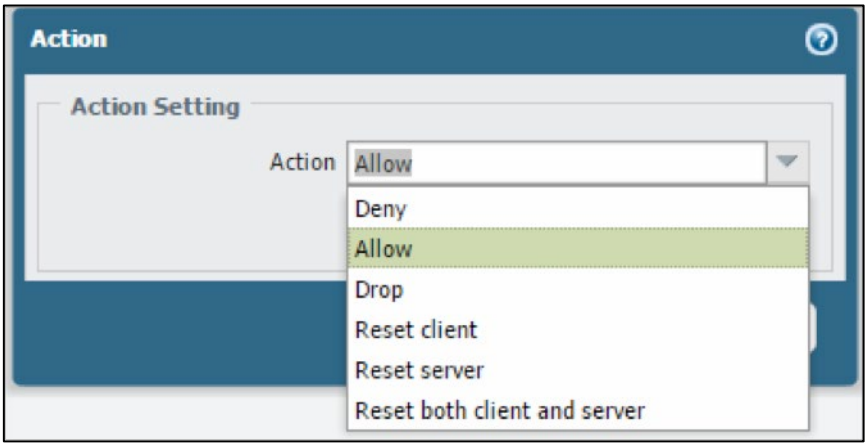
Throughput performance is not changed based on how quickly a match is made. Because evaluation is top-down first match then exit, exceptions to policies must appear before the general policy. Beyond this policy, order is based on administrative preference. Use Administrative Tags, a Policy search bar, and a Global Find to quickly navigate to the policy or policies needed for moves, adds, changes, deletes, clones, and troubleshooting.

Security Policy: Deny

Among Security policy actions the “deny” choice requires an explanation. This is a legacy setting from prior versions of PAN-OS® software that was the only choice to stop traffic. Prior to PAN-OS® 7, a reference was made to the App-ID database for the matching session’s application to find the preferred method of stopping traffic, which ranged from blocking to reset. These choices now have been added directly to the Action choices. The settings continue to be present in the App-ID database and are now exposed for viewing. Firewall administrators now can choose the desired blocking action directly or can

©2016-2019, Palo Alto Networks, Inc.

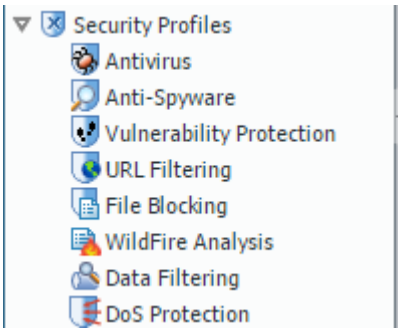
continue to rely on the Palo Alto Networks specification by choosing **deny**.



Security Profile Overview

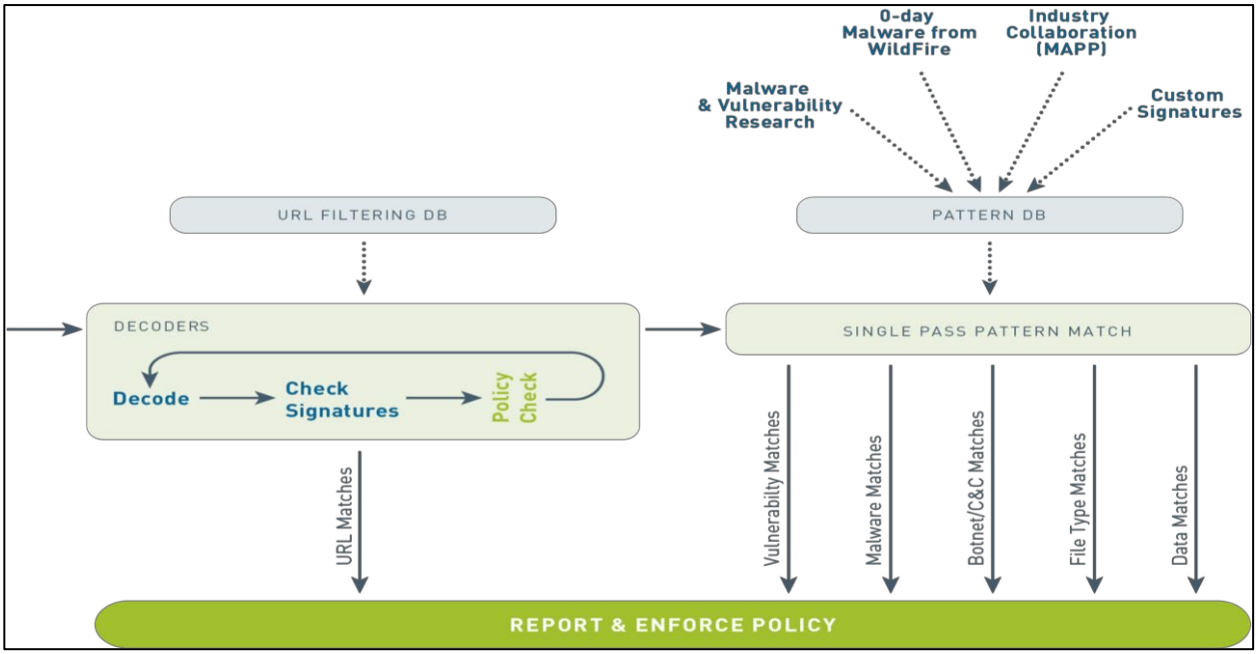
Security Profiles implement specific protections provided by the Palo Alto Networks Content-ID next-generation technology. After Security Profiles are created, they are attached to Security policies specifying Content-ID scans to be performed on traffic allowed by that policy. These profiles must be attached to Security policies to invoke their protections and will be applied only to the traffic handled by that particular policy.

Security Profiles include:



An overview of each Security Profile is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

©2016-2019, Palo Alto Networks, Inc.



All scanning is done by signature matching on a streaming basis (not file basis). These signatures are updated based on the configuration and licensing options. For example, with a WildFire® license, new virus and malware signatures can be installed as quickly as every 5 minutes. If the firewall has a Threat Prevention license but no WildFire® license, signatures from WildFire® would be updated only every 24 hours.

Once enabled, content scanning does consume firewall resources. Consult a firewall comparison chart to identify the model with appropriate "Threat Enabled" throughput.

WildFire Analysis Profiles

WildFire cloud can scan your organization's files using an appropriately configured WildFire Analysis Profile. A profile includes match conditions describing file characteristics you want to forward to WildFire for analysis. As files matching these conditions are transferred through your firewall, a copy is sent to WildFire for analysis.

Note: Files are *not* quarantined pending WildFire evaluation. In cases of positive malware findings, the security engineer must use information collected on the firewall and by WildFire to locate the file internally for remediation.

WildFire Profiles indicate which files are to be forwarded according to system-wide WildFire configuration settings. WildFire typically renders a verdict on a file within 5 to 10 minutes of receipt. WildFire analysis results in a detailed report including all aspects of the original file and the contained malware. This report is a valuable tool that describes the exact nature of the detected threat. Discussion of the report is here:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/monitor-wildfire-activity/wildfire-analysis-reportsclose-up.html

WildFire Profile setup details are here:

©2016-2019, Palo Alto Networks, Inc.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-security-profiles-wildfire-analysis.html

A complete review of WildFire implementation considerations is here:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html

An explanation of WildFire subscription benefits is here:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-subscription.html

URL Filtering Profiles

A URL Filtering Profile is a collection of URL filtering controls that are applied to individual Security policy rules to enforce your web access policy. The firewall comes with a default profile that is configured to block threat-prone categories such as malware, phishing, and adult. You can use the default profile in a Security policy, clone it to be used as a starting point for new URL Filtering Profiles, or add a new URL Filtering Profile that will have all categories set to allow for visibility into the traffic on your network. You then can customize the newly added URL Filtering Profiles and add lists of specific websites that always should be blocked or allowed. This information provides more granular control over URL categories. For example, you may want to block social-networking sites but allow some websites that are part of the social-networking category.

URL filtering requires a URL filtering subscription that keeps URL data type information current. This subscription provides descriptive data as to which type of information is at a given URL. Profiles can implement various actions against categories that reflect the organization's use policies and risk posture.

When URL Filtering Profiles invoke an action, the user can be notified directly, reducing user confusion as to the cause. These pages can be modified to meet an organization's particular need:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/customize-the-url-filtering-response-pages.html

An overview of URL filtering is provided here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering.html

Update services from two vendors are available for the firewall, but only one can be active at a given moment. Although they provide similar support to URL Filtering Profiles, the way each approach works within the firewall differs. A brief discussion of the two methods is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-overview/url-filtering-vendors.html

Specific information about implementing URL Filtering profiles and their allowed actions is here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/configure-url-filtering.html

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

174. Which action specifies that Security Profiles are relevant in a policy rule?
    A. Deny
    B. Drop
    C. Reset
    D. Allow
175. Are files quarantined while WildFire checks if they are malware or legitimate?
    A. Yes
    B. No
    C. By default, yes, but you can change the settings.
    D. By default, no, but you can change the settings.
176. What feature of the next-generation firewall allows you to block websites that are not business-appropriate?
    A. App-ID
    B. File Blocking
    C. Exploit Protection
    D. URL Filtering

©2016-2019, Palo Alto Networks, Inc.

5.11 Identify the methods for automating the configuration of a firewall

Automated configuration of Palo Alto Networks firewalls can be accomplished with several options. A running firewall can be accessed through its API from which configurations can be altered by an authenticated sender.

Details about this method appear here:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/about-the-pan-os-xml-api.html

A complete firewall configuration can be read and applied via the Bootstrapping feature. You create a package with the model configuration for your network and then use that package to deploy firewalls (physical or virtual) anywhere. For physical firewalls, you use a USB drive. For virtual firewalls, you can use a virtual disk, a virtual CD-ROM, an Azure Storage Account or an AWS S3 bucket. You either can bootstrap the firewall with basic initial configuration and licenses so that the firewall can register with Panorama and then retrieve its full configuration from Panorama, or you can bootstrap the complete configuration so that the firewall is fully configured on bootup.

References

- Prepare the Bootstrap Package
  https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall/prepare-the-bootstrap-package.html
- Bootstrap a Firewall using a USB Flash Drive
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html
- Bootstrap the VM-Series Firewall in Azure
  https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-azure.html
- Bootstrap the VM-Series Firewall in AWS
  https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws.html
- AWS CloudFormation
  https://aws.amazon.com/cloudformation/
- Working with Managed Policies
  http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-using.html#_create-managed-policy-console

©2016-2019, Palo Alto Networks, Inc.

Sample Questions

177. Which operating system do you select to use for a Palo Alto Networks NGFW running in Microsoft Azure?
   A. Windows
   B. BSD
   C. Linux
   D. Linux or BSD

178. What are the four component directories of a Palo Alto Networks bootstrap container?
   A. software, config, license, and content
   B. software, config, lic, and content
   C. software, configuration, license, and content
   D. software, configuration, lic, and content

179. Which environment supports a USB drive for the firewall bootstrap?
   A. VMware ESXi
   B. physical firewall
   C. Microsoft Hyper-V
   D. KVM

©2016-2019, Palo Alto Networks, Inc.

Appendix A: Sample Test

1. What is the last step of packet processing in the firewall?
    A. check allowed ports
    B. check Security Profiles
    C. check Security policy
    D. forwarding lookup
2. Which interface type requires you to configure where the next hop is for various addresses?
    A. TAP
    B. Virtual Wire
    C. Layer 2
    D. Layer 3
3. Can you allow the firewall to be managed through a data interface? Where do you specify it?
    A. You specify **Web UI** in the interface properties.
    B. You specify **Management** in the interface properties.
    C. You specify **HTTPS** in the Interface Management Profile, and then specify in the interface properties to use that profile.
    D. You specify **Management** in the Interface Management Profile, and then specify in the interface properties to use that profile.
4. Some devices managed by Panorama have their external interface on ethernet1/1, some on ethernet1/2. However, the zone definitions for the external zone are identical. What is the recommended solution in this case?
    A. Create two templates: One for the ethernet1/1 devices, one for the ethernet1/2 devices. Use the same external zone definitions in both. Apply those two templates to the appropriate devices.
    B. Create three templates: One for the ethernet1/1 device, one for the ethernet1/2 devices, and one with the external zone definitions. Use those templates to create two template stacks, one with the ethernet1/1 and external zone, another with the ethernet1/2 and external zone. Apply those two template stacks to the appropriate devices.
    C. Create three templates: One for the ethernet1/1 device, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
    D. Create three template stacks: One for the ethernet1/1 device, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
5. Which two options have the correct order of policy evaluation? (Remembering that not all rule types exist in all policies.) (Choose two.)
    A. device group pre-rules, shared pre-rules, local firewall rules, intrazone-default, interzone-default
    B. device group pre-rules, local firewall rules, shared post-rules, device group post-rules, intrazone-default, interzone-default
    C. device group pre-rules, local firewall rules, device group post-rules, shared post-rules,

©2016-2019, Palo Alto Networks, Inc.

intrazone-default, interzone-default

D. device group pre-rules, local firewall rules, intrazone-default, interzone-default, device group post-rules, shared post-rules
E. shared pre-rules, device group pre-rules, local firewall rules, intrazone-default, interzone-default

6. When you deploy the Palo Alto Networks NGFW on NSX, how many virtual network interfaces does a VM-Series firewall need?
   A. two, one for traffic input and output and one for management traffic
   B. four, two for traffic input and output and two for management traffic (for High Availability)
   C. three, one for traffic input, one for traffic output, and one for management traffic
   D. six, two for traffic input, two for traffic output, and two for management traffic (for High Availability)
7. Which source of user information is *not* supported by the NGFW?
   A. RACF
   B. LDAP
   C. Active Directory
   D. SAML
8. What is the main mechanism of packet-based attacks?
   A. malformed packets that trigger software bugs when they are received
   B. excess packets that fill up buffers, preventing legitimate traffic from being processed
   C. packets that get responses that leak information about the system
   D. packets that either fill up buffers or get responses that leak information
9. Which method is *not* a decryption method?
   A. SSH Proxy
   B. SSL Proxy
   C. SSL Forward Proxy
   D. SSL Inbound Inspection
10. Which type of identification does an Application Override policy override?
    A. App-ID
    B. User-ID
    C. Content-ID
    D. Service
11. Which two types of application can cause an insufficient data value in the Application field in the Traffic log? (Choose two.)
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
    E. IGP
12. Which three profile types are used to prevent malware from entering the network? (Choose three.)
    A. Antivirus
    B. Anti-spyware

©2016-2019, Palo Alto Networks, Inc.

C. WildFire analysis
D. File blocking
E. Vulnerability Protection
F. Zone Protection

13. Which user credential detection method does not require access to an external directory?
    A. group mapping
    B. domain credential filter
    C. LDAP
    D. Certificate
14. Which object type(s) has a property to specify whether it can transfer files?
    A. Application
    B. Service
    C. User
    D. User group
15. When destination NAT rules are configured, the associated security rule is matched using which parameters?
    A. pre-NAT source zone and post-NAT destination zone
    B. post-NAT source zone and pre-NAT destination zone
    C. pre-NAT source zone and post-NAT destination IP address
    D. post-NAT source zone and post-NAT destination zone
16. What is the initial IP address for the management interface?
    A. 10.0.0.1
    B. 172.16.0.1
    C. 192.168.1.1
    D. 192.168.255.254

17. In a new firewall, which port provides web interface access by default?
    A. Data port #1
    B. any data port
    C. Management port
    D. Console port
18. Which application requires you to import private keys?
    A. Capital Portal
    B. Forward Trust
    C. SSL Inbound Inspection
    D. SSL Exclude Certificate

©2016-2019, Palo Alto Networks, Inc.

19. Can two Layer 3 interfaces have the same IP address. If so, under which conditions?
    A. No, that is impossible.
    B. Yes, but they must be connected to the same Ethernet network through a switch. This configuration can be used only for High Availability.
    C. Yes, but they must be connected to different virtual routers.
    D. Yes, but they must be subinterfaces of the same physical interface.
20. Which two protocols are supported for site-to-site VPNs? (Choose two.)
    A. Authentication header (AH)
    B. Secure Socket Layer (SSL)
    C. Encapsulating Security Payload (ESP)
    D. Transport Layer Security (TLS)
    E. Secure Shell (SSH)
21. Which two functions is a GlobalProtect Portal responsible for? (Choose two.)
    A. terminating SSL tunnels
    B. authenticating GlobalProtect users
    C. creating on-demand certificates to encrypt SSL
    D. managing and updating GlobalProtect client configurations
    E. managing GlobalProtect Gateway configurations
22. What is the preferred SYN flood action?
    A. Random Drop
    B. Random Early Drop
    C. SYN Proxy
    D. SYN Cookies
23. What, if anything, would be a valid reason to allow non-SYN TCP packets at the start of a connection?
    A. Such packets could happen legitimately in the case of asymmetric routing.
    B. Such packets could happen legitimately if there is load balancing across firewalls.
    C. Such packets could happen legitimately because of either asymmetric routing or load balancing across firewalls.
    D. Such packets could happen because of router bugs
24. Where do you configure protection from malformed IP and TCP headers?
    A. DoS Profile
    B. QoS Profile
    C. Zone Protection Profile
    D. Application Profile
25. Which parameter is *not* a valid criterion for the original packet in address translation?
    A. source zone
    B. application
    C. service
    D. destination address
26. Which parameter do you use to apply a rule to traffic coming in from a specific interface?
    A. source zone
    B. source address
    C. User

©2016-2019, Palo Alto Networks, Inc.

D. source interface

27. Where do you specify that certain URL categories are not to be decrypted (to avoid the liability of holding information such as employees' personal bank credentials)?
    A. certificate properties
    B. Decryption Profile
    C. Decryption policy
    D. Security policy
28. Where do you specify how the firewall should treat invalid certificates?
    A. certificate properties
    B. Decryption Profile
    C. Decryption policy
    D. Security policy
29. Which two public cloud environments support pay-as-you-go (PAYG) firewall licensing? (Choose two.)
    A. Microsoft Azure
    B. Microsoft Hyper-V
    C. Amazon AWS
    D. VMware NSX
    E. VMware ESXi
30. Which log type gets redirected in **Device > Log Settings**?
    A. Config log
    B. Traffic log
    C. Threat log
    D. WildFire Submission log
31. Which tab of the user interface gives you a consolidated picture of the security situation and the top-level threats?
    A. Dashboard
    B. ACC
    C. Monitor
    D. Devices
32. A customer's custom application uses SMTP (email) to transfer directory information, which needs to be filtered in a very different manner than normal DNS. How do you configure this filtering?
    A. You cannot do it with the NGFW. You need to manually configure a proxy.
    B. Create specific rules for the sources and destinations that run this application.
    C. Create a custom signature and specify the SMTP fields that are different from normal DNS use and patterns to identify when it is the custom application.
    D. Create an Application Override policy and specify the sources and destinations that run this application.

©2016-2019, Palo Alto Networks, Inc.

33. Which kind of update (or updates) requires a disruption in connectivity?
    A. There never is a need to disrupt connectivity.
    B. Only dynamic content updates require a brief disruption while the firewall integrates them with the Security policy.
    C. Only PAN-OS updates require a reboot to apply.
    D. Both dynamic content updates and PAN-OS updates cause disruption in connectivity.
34. Which High Availability port (or ports) is used for which plane?
    A. HA1 for the data plane, HA2 for the management plane.
    B. HA1 for the management plane, HA2 for the data plane.
    C. If HA1 works, it is used for both data and management. HA2 is a backup.
    D. HA1 for the management plane, HA2 for the data plane in the 7000 Series. The less costly models have only an HA1, which is used for both management and data.
35. Which two protocols can AutoFocus use to retrieve log information from an NGFW? (Choose two.)
    A. syslog
    B. Log transfer protocol, a Palo Alto Networks proprietary protocol
    C. HTTP
    D. HTTPS
    E. SNMP
36. How often does Palo Alto Networks publish new applications?
    A. every 30 minutes
    B. hourly
    C. daily
    D. weekly
37. Which type of device can receive the GlobalProtect data files content update?
    A. Log Collector
    B. firewall
    C. WildFire®
    D. Antivirus
38. An administrator claims to be unable to log in to the firewall. In which log will you see evidence of this problem?
    A. Traffic
    B. System
    C. Configuration
    D. Authentication
39. How do you reboot the firewall from the command line?
    A. restart system
    B. reboot
    C. request restart system
    D. request reboot

©2016-2019, Palo Alto Networks, Inc.

40. Where in the user interface do you configure how many packets to capture?
    A. In the Device tab, as part of the Setup node.
    B. In the Security Profiles, because the desired number of captured packets can vary between profiles.
    C. You configure a default in the Device tab, as part of the Capture node. Then, you can configure exceptions in the Security Profiles.
    D. You don't, you can only configure the number of packets to capture on the command line interface
41. You are preparing a bootstrap template for use with either Microsoft Azure or Amazon AWS. You don't want to include the Content-ID files because the firewall will download the latest version when it is booted anyway. What do you do?
    A. Leave the content directory empty.
    B. Do not create a content directory.
    C. Either leave the content directory empty or do not create it.
    D. Create a content directory, but put in a placeholder file, download latest.
42. Which format do you use for an AWS CloudFormation Template?
    A. XML
    B. CSV
    C. JSON
    D. JSON or XML
43. When are security rules from Panorama processed, compared to local firewall rules?
    A. The question is incorrect, because a firewall can either have local rules or Panorama rules.
    B. Panorama rules are processed first, so they take precedence.
    C. Local rules are processed first, so they take precedence.
    D. Some Panorama rules are processed before the firewall's local rules, and some are processed after the local rules.
44. Which statement about Security Profiles is correct?
    A. They are evaluated from top down, with the first match processing the traffic.
    B. They are applied to all inbound traffic when they are enabled.
    C. They enable a specific type of scanning (e.g., Virus, Spyware).
    D. They can specify actions based on the username.
45. Which authentication method can be handled by the browser without affecting the user experience?
    A. web-challenge
    B. browser-challenge
    C. web-form
    D. browser-form

©2016-2019, Palo Alto Networks, Inc.

46. The R&D network of the defense contractor is not connected to the internet. However, it is connected to SIPRNet (https://en.wikipedia.org/wiki/SIPRNet), which is used to transfer classified information. The contractor is concerned about getting malware files and infected PDFs through that network. Can this company use WildFire for protection?
    A. No, because there is no network path to the WildFire server.
    B. No, but no protection is needed because everybody with SIPRnet access has a security clearance and is trustworthy.
    C. Yes, but only if they can get approval to have a gateway to the public internet.
    D. Yes. They can use a WF-500 appliance.
47. How does the NGFW handle excess packets when there are QoS constraints?
    A. It buffers them until there is bandwidth to send them.
    B. It drops a percentage of them randomly.
    C. It replaces them with packets that tell the computer on the other side to slow down.
    D. It sends a portion instead of the whole packet.
48. Which function is performed by the control plane?
    A. signature matching
    B. route lookup
    C. policy matching
    D. route updates
49. Which User-ID method is *not* transparent to the user?
    A. Captive Portal
    B. User-ID agent connected to Active Directory
    C. User-ID agent monitoring server logs for login events
    D. User-ID agent connected to a Cisco WLAN controller
50. Which feature of the NGFW lets you identify attempts to tunnel SSH over other ports?
    A. App-ID
    B. Content-ID
    C. User-ID
    D. Content-ID and User-ID
51. What is the correct order of operations?
    A. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security policy, check Security Profiles, re-encrypt traffic.
    B. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security Profiles, check Security policy, re-encrypt traffic.
    C. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security policy, re-encrypt traffic.
    D. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security Profiles, check Security policy, re-encrypt traffic

©2016-2019, Palo Alto Networks, Inc.

Appendix B: Answers to Sample Questions

Exam Domain 1 – Plan

1.1 Identify how the Palo Alto Networks products work together to detect and prevent threats

1. Which component of the integrated Palo Alto Networks security solution limits network-attached workstation access to a corporate mainframe?
    A. threat intelligence cloud
    B. advanced endpoint protection
    C. next-generation firewall
    D. tunnel inspection
2. Which Palo Alto Networks product is designed primarily to provide threat context with deeper information about attacks?
    A. RedLock
    B. WildFire
    C. AutoFocus
    D. Threat Prevention
3. Which Palo Alto Networks product is designed primarily to provide normalization of threat intelligence feeds with the potential for automated response?
    A. MineMeld
    B. WildFire
    C. AutoFocus
    D. Threat Prevention
4. Which Palo Alto Networks product is designed primarily to protect endpoints from successful cyberattacks?
    A. GlobalProtect
    B. Magnifier
    C. Traps
    D. RedLock
5. The Palo Alto Networks Cortex Data Lake can accept logging data from which products? (Choose two.)
    A. Traps
    B. next-generation firewalls
    C. Aperture
    D. MineMeld
    E. AutoFocus
6. Which Palo Alto Networks product is required to deliver your product log data to a central cloud base storage service managed by Palo Alto Networks?
    A. RedLock
    B. Traps
    C. next-generation firewall
    D. Cortex data lake

©2016-2019, Palo Alto Networks, Inc.

7. Which product is an example of an application designed to analyze Cortex Data Lake information?
    A. Cortex XDR - Analytics
    B. RedLock
    C. Cortex XDR – Automated Response
    D. AutoFocus

1.2 Given a scenario, identify how to design an implementation of the firewall to meet business requirements that leverage the Palo Alto Networks Security Operating Platform

8. A potential customer says it wants to maximize the threat detection capability of its next-generation firewall. Which three additional services should it consider implementing to enhance its firewall's capability to detect Threats?
    A. Traps
    B. WildFire
    C. URL Filtering
    D. Expedition
    E. DNS Security
9. Which product best secured east-west traffic within a public cloud implementation. Which product is best suited for this need?
    A. RedLock
    B. MineMeld
    C. VM-Series firewall
    D. Cortex

1.3 Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements that leverage the Palo Alto Networks Security Operating Platform

10. Why would you recommend an active/active cluster instead of an active/passive one?
    A. Active/active is the preferred solution when the firewall cluster is behind a load balancer that randomizes routing, thus requiring both firewalls to be active.
    B. Active/active usually is the preferred solution because it allows for more bandwidth while both firewalls are up.
    C. Active/active is the preferred solution when the PA-7000 Series is used. Use active/passive with the PA-5200 Series or smaller form factors.
    D. Active/active is the preferred solution when using the PA-5200 Series or smaller form factors. When using the PA-7000 Series, use active/passive.
11. Which two events can trigger an HA pair failover event?
    A. An HA1 cable is disconnected from one of the firewalls.
    B. A Dynamic Update fails to download and install.
    C. The firewall fails to ping a path-monitored destination address successfully.
    D. OSPF implemented on the firewall determines that an available route is now down.
    E. RIP implemented on the firewall determines that an available route is now down.

©2016-2019, Palo Alto Networks, Inc.

12. Which two firewall features support floating IP addresses in an active/active HA pair? (Choose two.)
    A. data-plane traffic interfaces
    B. source NAT
    C. VPN endpoints
    D. loopback interfaces
    E. management port
13. How are configurations in firewalls in an active/passive HA pair synchronized?
    A. An administrator commits the changes to one, then commits them to the partner, at which time the changes are sent to the other.
    B. An administrator pushes the config file to both firewalls, then commits them.
    C. An administrator commits changes to one, which automatically synchronizes with the other.
    D. An administrator schedules an automatic sync frequency in the firewall configs.
14. How is an active/passive HA pair configured in virtual firewalls deployed in any public clouds? Choose two
    A. The virtual firewalls are deployed in a cloud "scale set" with a cloud-supplied load balancer in front to detect and manage failover.
    B. The virtual firewalls rely on a VM-Series plugin to map appropriate cloud functions to the firewall's HA settings.
    C. Virtual firewalls use PAN-OS HA configuration combined with appropriate cloud deployments of interfaces for HA use.
    D. The virtual firewalls use an HA Compatibility module for the appropriate cloud technology

1.4 Identify the appropriate interface type and configuration for a specified network deployment

15. When a NGFW is in front of an existing firewall to provide better security while making the minimum required network changes. Which interface type do you use?
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3
16. Which kind of interface do you use to connect Layer 2 and Layer 3 interfaces?
    A. VLAN
    B. tunnel
    C. tap
    D. virtual wire
    E. Layer 2
    F. Layer 3

©2016-2019, Palo Alto Networks, Inc.

17. Which three types of interfaces can the firewall's management web interface be bound to? (Choose three.)
    - **A. VLAN**
    - **B. tunnel**
    - C. tap
    - D. virtual wire
    - E. Layer 2
    - **F. Layer 3**
18. Which three types of interfaces connect to a virtual router?
    - **A. VLAN**
    - **B. tunnel**
    - C. tap
    - D. virtual wire
    - E. Layer 2
    - **F. Layer 3**
19. Which dynamic routing protocol is not supported by the Palo Alto Networks firewall?
    - A. RIP
    - B. OSPF
    - C. OSPFv3
    - **D. IGRP**
    - E. BGP
20. Which action is not compatible with aggregate interface configuration?
    - **A. aggregating 12 Layer 3 interfaces**
    - B. aggregating 4 virtual wire interfaces
    - C. aggregating interfaces in an HA pair
    - D. aggregating two 10Gbps optical and two 10Gbps copper Ethernet ports

1.5 Identify strategies for retaining logs using Distributed Log Collection

21. How do you create and view enterprise-wide reports that include data from all managed firewalls?
    - **A. Run Panorama reports normally. Firewall summary reporting information is gathered automatically once Firewall are managed by Panorama.**
    - B. Configure log forwarding on the managed firewalls to forward logs to Panorama using syslog formatting.
    - C. Run custom Panorama reports and select **remote log**s as the information source.
    - D. Run custom Panorama reports and select **log collector** as the information source.
22. What must you configure to guarantee duplication of log data on Log Collectors to eliminate log data loss in cases of hardware failure?
    - A. Log Collector settings to include "Replicate Data"
    - B. Panorama HA settings to include "Duplicate Logs"
    - C. Log Collector settings to include "Enable log redundancy"
    - D. Log forwarding settings of firewalls for two Log Collector destinations

©2016-2019, Palo Alto Networks, Inc.

23. Which three devices can be used as Log Collectors?
    - **A. Virtual Panorama**
    - B. PA-220R
    - **C. M-600**
    - **D. M-200**
    - E. VM-300LC
24. Which statement is true regarding Log Collecting in a Panorama HA pair?
    - A. Both Panoramas cannot be configured to collect logs.
    - B. Log collecting is handled by the active HA Panorama until a failover occurs.
    - **C. Both Panoramas collect independent logging traffic and are not affected by failover.**
    - D. Both Panoramas receive the same logging traffic and synchronize in case of HA failover.

1.6 Given a scenario, identify the strategy that should be implemented for Distributed Log Collection

25. How are log retention periods on Palo Alto Networks firewalls increased?
    - A. add storage to any firewall model
    - B. increase the allocation for overall log storage within the firewall
    - C. turn on log compression
    - **D. forward logs to external Log Collectors**
26. How is firewall log data sent to the Cortex Data Lake accessed?
    - A. direct viewing and searching with the Cortex gateway
    - **B. Panorama using a Log Collector configuration for access**
    - C. reporting in a firewall using a “remote data source” configuration
    - D. reporting in a firewall equipped with a “Remote Logging” plugin
27. Log retention is increased when a Dedicated Log Collector is used to collect logs from firewalls in which two ways?
    - A. turning on “Log Compression” in the Log Collector
    - **B. adding storage capacity to the Log Collector**
    - C. enabling “Log Storage Sharing” between the Log Collector and Panorama
    - **D. adding Log Collectors to the Log Collector Group**

1.7 Identify how to use template stacks for administering Palo Alto Networks firewalls as a scalable solution using Panorama

28. The Security policy for all of a customer’s remote offices is the same, but because of different bandwidth requirements some offices can use a PA-220 and others require higher-end models (up to PA-5000 Series). If the firewalls for the offices are all managed centrally using Panorama, how might they share device groups and templates?
    - **A. same device group and same template stack**
    - B. same device group, different template stacks
    - C. different device groups, same template stack
    - D. different device groups and different template stacks

©2016-2019, Palo Alto Networks, Inc.

29. A firewall is assigned to a template stack of two templates. A setting common to each template has a different value. When Panorama pushes the template stack contents to the managed firewall, which setting will the firewall receive?
    - **A. value from the top template of the stack**
    - B. value from the bottom template in the stack
    - C. value from the template designated as the parent
    - D. value an admin selects from the two available values
30. Which two firewall settings are stored in Panorama templates?
    - A. custom Application-ID signatures
    - **B. Server Profile for an external LDAP server**
    - C. services definitions
    - D. DoS Protection Profiles
    - **E. traffic interface configurations**

1.8 Identify how to use device group hierarchy for administering Palo Alto Networks firewalls as a scalable solution using Panorama

31. Where in Panorama do you enter Security policy rules to ensure that your new rules will take precedence over locally entered rule?
    - A. Security policy rules with a targeted firewall
    - B. default rules section of Security policy rules
    - **C. pre-rules section of Security policy rules**
    - D. post-rules section of Security policy rules
32. How are changes made to Security policy rules seen in the Panorama web interface management window for a specific firewall configuration?
    - **A. log in to Panorama, clone the rule, modify the clone, and add a target firewall to the new rule**
    - B. select the rule, click the override button, and enter the changes
    - C. create a new locally defined Security policy rule that is placed higher in the rule list than the rule to be overridden
    - D. log in to Panorama and modify the original rule
33. Which three firewall settings are stored in Panorama device groups?
    - A. User Identification configuration
    - **B. custom Application-ID signatures**
    - **C. services definitions**
    - **D. DoS Protection Profiles**
    - E. traffic interface configurations
    - F. Zone Protection Profiles
    - G. Server Profile for an external LDAP server

©2016-2019, Palo Alto Networks, Inc.

1.9 Identify planning considerations unique to deploying Palo Alto Networks firewalls in a public cloud

34. Which two types of firewall interfaces are most likely to be supported in public cloud deployments?
    A. tap
    B. virtual wire
    C. Layer 3
    D. tunnel
    E. aggregate Ethernet
35. Where is the VM-Series virtual firewall appliance for public cloud deployments found?
    A. Palo Alto Networks Support Portal
    B. cloud vendor's "Solution Marketplace"
    C. Using the download link supplied on the same site as the license server
    D. Palo Alto Networks Product Download portal

1.11 Identify planning considerations unique to deploying Palo Alto Networks firewalls in a private cloud

36. A private cloud has 20 VLANs spread over five ESXi hypervisors, managed by a single vCenter. How many firewall VMs are needed to implement microsegmentation?
    A. one
    B. four
    C. five
    D. 20
37. When you deploy the Palo Alto Networks NGFW on NSX, packets coming to an application VM from VMs running on different hardware go through which modules?
    A. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, application VM.
    B. The network, vSwitch, Palo Alto Networks NGFW, NSX firewall, application VM.
    C. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, NSX firewall, application VM.
    D. The vSwitch, network, Palo Alto Networks NGFW, NSX firewall, application VM.
38. Which option shows the interface types that ESXi supports in the VM-Series firewalls?
    A. tap, Layer 2, Layer 3, virtual wire
    B. Layer 3 only
    C. tap, Layer 2, Layer 3
    D. Layer 3, virtual wire

©2016-2019, Palo Alto Networks, Inc.

1.12 Identify methods for authorization, authentication, and device administration

39. To configure multi-factor authentication for users accessing services through the firewall, which three configuration pieces need to be addressed?
    A. GlobalProtect Portal
    B. Captive Portal
    C. Authentication Enforcement Profile
    D. Authentication Profile
    E. Response pages
40. Which two configuration components can be used for external user authentication in the firewall?
    A. Local User Database
    B. Server Profiles
    C. VM Information source
    D. admin roles
    E. Authentication policy rules
41. Which two firewall functions are reserved only for admins assigned the superuser dynamic role?
    A. certificate management
    B. managing firewall admin accounts
    C. editing the management interface settings
    D. creating virtual systems within a firewall
    E. accessing the configuration mode of the CLI

1.13 Identify the methods of certificate creation on the firewall

42. A Palo Alto Networks firewall can obtain a certificate for its internal use through which three methods?
    A. importing a certificate file generated by an external CA
    B. referencing an externally stored certificate by a URL configured in an SSL/TLS Service Profile
    C. generating a certificate directly by manually entering certificate data
    D. obtaining a certificate from an SCEP server using an SCEP profile
    E. importing a certificate from an external CA by using an Authentication Profile
43. Which input simplifies a certificate request from an external CA?
    A. certificate signing request
    B. Certificate signing request with a separate private key
    C. certificate signing request with a separate public key
    D. certificate signing request with a separate public key and private key
44. Which two resources must also be available to successfully run certificate validation tests on a certificate received from an external source?
    A. Root Certificate of the issuing CA
    B. public key for the received certificate
    C. OCSP connection address
    D. existing Certificate Profile that matches the received certificate's CA identity

©2016-2019, Palo Alto Networks, Inc.

1.14 Identify options available in the firewall to support dynamic routing

45. The firewall uses which information to determine which interface to use for a packet's egress?
    A. manually configured static routes
    B. routing information base (RIB)
    C. appropriate Redistribution Profile
    D. ECMP destination monitoring results
46. A virtual router can use a Redistribution Profile to share routes between which three routing protocols?
    A. static routes
    B. IGRP
    C. RIP
    D. OSPF
    E. multicast
47. How does a firewall RIB with routes to the same destination in multiple router protocols determine the which route to use?
    A. according to the following precedence of route type: static, RIP, OSPF, BGP
    B. using the virtual router's FIB
    C. using the associated route's metric and choosing the lowest value
    D. using the route's administrative distance and choosing the lowest value

1.15 Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers

48. For which two reasons are denial-of-service protections applied by zone?
    A. because denial-of-service protections are applied early in the processing, before much information is known about the connection but when the ingress interface already is known
    B. because denial-of-service protections are applied only when manually turned on to avoid quota overload (which would make denial of service easier)
    C. because denial-of-service protections can depend on only the zone, and never on port numbers or IP addresses
    D. because denial-of-service protections on a Layer 3 interface are different from the denial-of-service protections available on a Layer 2 interface, and interfaces on virtual wires
49. SYN flood protection provides flood protection from which protocol?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
50. To which two protocols does port scan reconnaissance protection apply?
    A. UDP
    B. TCP
    C. GRE
    D. ICMP
    E. IPX

©2016-2019, Palo Alto Networks, Inc.

51. In which two places do you configure flood protection?
    - **A. DoS Profile**
    - B. QoS Profile
    - **C. Zone Protection Profile**
    - D. SYN Profile
    - E. XOFF Profile
52. Which two firewall features should be used to provide tailored DoS protection to a specific address?
    - A. Zone Protection Profiles
    - B. virtual routers
    - C. Server Profiles
    - **D. DoS Protection policy rules**
    - **E. DoS Protection Profiles**

1.16 Identify decryption deployment strategies

53. Which feature does not require a Decryption policy?
    - A. antivirus
    - B. App-ID
    - C. file blocking
    - **D. network address translation**
54. How can the next-generation firewall inform web browsers that a web server's certificate is from an unknown CA?
    - A. show a "the certificate is untrusted, are you SURE you want to go there" response page before accessing the website
    - B. relay the untrusted certificate directly to the browser
    - C. have two certificates in the firewall, one used for sites whose original certificate is trusted, and the other for sites whose original certificate is untrusted
    - **D. have two certificate authority certificates in the firewall, one is used to produce certificates for sites whose original certificate is trusted, and the other for certificates for sites whose original certificate is untrusted**
55. Which firewall features can be used to support an organization's requirement of decrypting a user's browsing traffic for compliance and to record all decrypted traffic? (Choose two.)
    - **A. Decryption Broker**
    - B. Policy Based Forwarding
    - C. Default Router setting of Forward Cleartext
    - **D. Interface setting of Decryption Port Mirroring**
    - E. Decryption policy rule action set to Forward Cleartext

©2016-2019, Palo Alto Networks, Inc.

1.17 Identify the impact of application override to the overall functionality of the firewall

56. Which type of identification is disabled by Application Override?
    A. Protocol-ID
    B. User-ID
    C. Content-ID
    D. URL Filtering
57. Application Override is triggered by which configuration setting?
    A. Custom App-ID
    B. Application Override policy rule
    C. Application Override definition in Custom Objects
    D. Application Filters

1.18 Identify the methods of User-ID redistribution

58. User-ID user-id-to-IP-address mapping tables can be read by which product or service?
    A. Traps
    B. Panorama Log Collector
    C. AutoFocus
    D. VM-Series firewall plugin

1.19 Identify VM-Series bootstrap components and their function

59. When will a firewall check for the presence of bootstrap volume?
    A. each time it cold-boots
    B. each time it boots from a Factory Default state
    C. when a firewall is started in Maintenance Mode
    D. each time it warm-boots
60. Can a firewall's PAN-OS software be updated by the bootstrap process?
    A. Yes, by including a copy of the desired PAN-OS software in the /software folder of the bootstrap volume.
    B. Yes, by including a copy of the desired PAN-OS software in the /content folder of the bootstrap volume.
    C. No, it must be updated by an administrator after the firewall starts.
    D. No, the firewall must be licensed first.

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 2 — Deploy and Configure

2.1 Identify the application meanings in the Traffic log (incomplete, insufficient data, non-syn TCP, not applicable, unknown TCP, unknown UDP, and unknown P2P)

61. An application using which protocol can receive an **incomplete** value in the Application field in the Traffic log?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
62. Session traffic being evaluated by a firewall is encrypted with SSL. If the firewall does not decrypt the traffic, how does the firewall make an App-ID determination?
    A. evaluate the HTTP headers
    B. evaluate the SSL Hello exchange
    C. evaluate certificate contents used for encryption
    D. use information in the SSL Decryption Exclusion cache
63. How does the firewall respond to a change of application detected during the firewall's App-ID scanning of an on-going session.?
    A. closes the session, opens a new one, and evaluates all security policies again
    B. closes the session, opens a new one, and evaluates the original matching Security policy rule only
    C. updates the application in the existing session and evaluates all Security policies again
    D. updates the application in the existing session and continues to use the original action from the first Security policy rule match

2.2 Given a scenario, identify the set of Security Profiles that should be used

64. Which profile do you use for DLP?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
65. Which profile do you use to monitor DNS resolution lookups for sites associated with threat activity?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering

©2016-2019, Palo Alto Networks, Inc.

66. Which profile do you use to analyze files for zero-day malware?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
67. Which profile do you use to examine browsing traffic for appropriate browsing policy enforcement?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering
68. Which profile do you use to detect and block an executable file from being transferred through the firewall?
    A. Antivirus
    B. Anti-Spyware
    C. Vulnerability Protection
    D. URL Filtering
    E. File Blocking
    F. WildFire Analysis
    G. Data Filtering

2.3 Identify the relationship between URL filtering and credential theft prevention

69. Which credential phishing prevention action allows users to choose to submit credentials to a site anyway?
    A. alert
    B. allow
    C. block
    D. continue
70. Which user credential detection method would work if multiple users share the same client IP address (for example, because of dynamic address translation done by a device on the internal side of the firewall)?
    A. IP-to-user mapping
    B. group mapping
    C. domain credential filter
    D. IP-and-port-to-user mapping
    E. identify the relationship between URL filtering and credential theft prevention

©2016-2019, Palo Alto Networks, Inc.

71. Which type of user credential detection should be used by a firewall administrator that wants to enable Credential Phishing Prevention that blocks an attempt by a user to enter the organization's user ID and password?
    A. IP-to-user mapping
    B. domain credential filter
    C. group mapping
    D. Citrix mapping

2.4 Implement and maintain the App-ID lifecycle

72. Which security risks are elevated when port-based Security policy rules are used?
    A. The firewall's resources will be negatively impacted by processing unwanted traffic.
    B. Unwanted applications can get through the firewall, bringing their vulnerabilities with them.
    C. A greater range of threats can be included in packet payloads.
    D. The firewall is more vulnerable to DoS attacks.
73. What is the Palo Alto Networks suggested process for converting port-based Security policies to use App-ID?
    A. Use the Expedition tool to analyze Traffic logs against Security policy to suggest policy changes.
    B. Use the built-in firewall reports to identify applications found in the traffic and update policy based on desired traffic.
    C. Use the Policy Optimizer feature of the firewall to identify applications and update policy rules.
    D. Use the firewall's New Applications Seen feature to identify applications and update policy rules.
74. If App-ID is implemented in Security policy rules, should port numbers also be included?
    A. No, App-ID-based Security policy rules detect and allow or block any desired application using the included port number values in the App-ID database.
    B. Yes, including the port numbers as a *service*-matching condition can eliminate some traffic before App-ID processing, conserving firewall resources.
    C. Yes, including an *application-default* setting in the *service*-matching condition requires that applications use only known or typical port numbers.
    D. No, App-ID based Security policy rules detect and allow or block any desired application using the edited port number values in the App-ID database.

2.5 Identify how to create security rules to implement App-ID without relying on port-based rules

75. Which two applications cannot be identified by port number?
    A. Microsoft Outlook Express email
    B. Google mail (Gmail)
    C. SSH
    D. Facebook
    E. FTP

©2016-2019, Palo Alto Networks, Inc.

76. An administrator creates a Security policy rule that allows office-on-demand traffic through the firewall. When the change is committed the firewall issues the following warning:
"vsys1: Rule 'Allow Office apps' application dependency warning:
Application 'office-on-demand' requires 'ms-office365-base' be allowed
Application 'office-on-demand' requires 'sharepoint-online' be allowed
Application 'office-on-demand' requires 'ssl' be allowed
Application 'office-on-demand' requires 'web-browsing' be allowed"
Which action should the administrator take?
    A. Create an application chain that include the dependencies
    B. Add the listed applications to the same Security policy rule
    C. set the Service action of the rule to "dependent application default"
    D. create a new Security policy rule for each listed application with an "allow" action higher in the rule list

2.6 Identify configurations for distributed Log Collectors

77. Which two options will provide an enterprise-wide log that can be viewed from Panorama?
    A. Select firewalls are designated as Log Collectors and add logs forwarded from other firewalls to their own.
    B. Panorama devices are configured as Dedicated Log Collectors that then are added to Log Collector Groups. Firewalls forward logs to a designated Log Collector within a Collector Group.
    C. Cortex Data Lake is configured as a Log Collector in Panorama. Firewalls forward logs to Cortex Data Lake.
    D. A Panorama device is configured in Management Mode and a Log Collector is defined on the Panorama appliance, which then is added to a Log Collector Group. Firewalls forward logs to a designated Log Collector within a Collector Group.

2.7 Identify the required settings and steps necessary to provision and deploy a next-generation firewall

78. You finished configuring the firewall's basic connectivity in the lab and are ready to put it in the data center. What do you have to remember to do before you power down the firewall?
    A. Save the changes.
    B. Commit the changes.
    C. Create a restore thumb drive in case the configuration is deleted.
    D. Verify that the configuration is correct. You do not need to do anything else if it is correct; the configuration is updated automatically.
79. The Management port on a firewall can be configured as which type of interface?
    A. Layer 2
    B. Layer 3
    C. virtual wire
    D. serial

©2016-2019, Palo Alto Networks, Inc.

2.8 Identify which device of an HA pair is the active partner

80. Which two steps must be completed to enable the display of the High Availability widget?
    A. Log in to the firewall management web interface and configure HA for active/active or active/passive.
    B. Log in to the firewall management web interface and press the **Sync to peer** link in the firewall HA configuration settings.
    C. Log in to the firewall's CLI and enter the **`get management-server logging on`** command.
    D. Select and enable the High Availability widget in the firewall's management web interface Dashboard display.

2.10 Identify various methods for authentication, authorization, and device administration within PAN-OS software for connecting to the firewall

81. Which object ties together Captive Portal method with an authentication profile when configuring multifactor authentication?
    A. Multi-Factor Authentication Server Profile
    B. Authentication policy rule
    C. authentication sequence
    D. Authentication Enforcement object
82. Which four firewall Server Profiles can provide first factor authentication for multi-factor authentication configurations? (Choose four.)
    A. HTTP
    B. Okta
    C. PingID
    D. Kerberos
    E. RADIUS
    F. SAML
    G. LDAP
    H. RSA SecureID Access

2.11 Identify how to configure and maintain certificates to support firewall features

83. Administrators within the enterprise want to replace the default certificate used by the firewall to secure the management web interface traffic with a certificate generated by their existing certificate authority. Which certificate property must be set for their new certificate to function?
    A. Certificate CN set to a domain name that resolves to any traffic port address of the firewall.
    B. Certificate must be signed by the firewall root certificate.
    C. Certificate must have the Forward Trust Certificate property set.
    D. CN must be set to the management port of the firewall.

©2016-2019, Palo Alto Networks, Inc.

2.12 Identify the features that support IPv6

84. Which two configuration conditions must be met for a Palo Alto Networks firewall to send and receive IPv6 traffic?
    A. **Enable IPv6** check box in the Virtual Router configuration is checked.
    B. An Ethernet interface is configured for virtual wire.
    C. An Ethernet interface is configured for Layer 3.
    D. Enable IPv6 Firewalling check box under Session Settings is turned on.

2.13 Identify how to configure a virtual router

85. Under which condition can layer 3 interfaces in the same firewall have the same IP address?
    A. they must be connected to different virtual routers.
    B. they must be connected to the same Ethernet network through a switch.
    C. they must be subinterfaces of the same physical interface.
    D. They must be in different zones.
86. A firewall's virtual router can connect to which three types of interfaces?
    A. virtual wire
    B. management
    C. Layer 3 traffic
    D. HA1
    E. HA2
    F. loopback
    G. tunnel

2.14 Given a scenario, identify how to configure an interface as a DHCP relay agent

87. A Palo Alto Networks firewall can forward DHCP broadcasts from one network to another?
    A. True
    B. False
88. A Palo Alto Networks firewall can forward DHCP packets to servers connected to which two kinds of networks? (Choose two.)
    A. virtual wire
    B. Layer 2
    C. Layer 3
    D. aggregate
89. How does a Palo Alto Networks firewall configured to forward DHCP packets to multiple server destinations choose which reply to forward to the sender?
    A. The first server listed in the "Server Priority" DHCP configuration is forwarded until it fails to respond, then the next one is chosen.
    B. A request is sent to all servers on the list, and the first responder is forwarded.
    C. All DHCP server responses are forwarded, and the receiving client chooses which to accept.
    D. The server that is the fewest network hops from the requesting client is chosen. When more than one server has the same hop count, all packets from the servers are forwarded to the client.

©2016-2019, Palo Alto Networks, Inc.

2.15 Identify the configuration settings for site-to-site VPN

90. Which type is a tunnel interface?
    A. Tap
    B. virtual wire
    C. Layer 2
    D. Layer 3
91. A firewall administrator is rolling out 50 Palo Alto Networks firewalls to protect remote sites. Each firewall must have a site-to-site IPsec VPN tunnel to each of three campus locations. Which configuration function is the basis for automatic site-to-site IPsec tunnels set up from each remote location to the three campuses?
    A. import of a settings table into the remote firewall's IPsec tunnel config
    B. import of a settings table into the IPsec tunnel config of the three campuses
    C. configuration of the GlobalProtect satellite settings of the campus and remote firewalls
    D. entering of campus IPsec tunnel settings for each remote firewall's IPsec Profile

2.16 Identify the configuration settings for GlobalProtect

92. Which configuration or service is required for an iOS device using the GlobalProtect license to connect to a local Global Protect Gateway?
    A. X-Auth configuration in the gateway settings
    B. GlobalProtect gateway license
    C. firewall authentication policy with an iOS setting
    D. GlobalProtect client downloaded from the GlobalProtect portal
93. GlobalProtect Gateway is uniquely responsible for which function?
    A. terminating SSL tunnels
    B. authenticating GlobalProtect users
    C. creating on-demand certificates to encrypt SSL
    D. managing and updating GlobalProtect client configurations
    E. managing GlobalProtect Gateway configurations

2.18 Identify how to configure features of NAT policy rules

94. Which NAT type can be used to translate between IPv4 and IPv6?
    A. ipv4
    B. nat64
    C. nptv6
    D. ipv6
95. How does a firewall that has more than one NAT policy rule that matches a packet process the packet?
    A. Each matching rule in the list is applied from the top down, with cumulative changes being processed at the end of the list.
    B. The first rule matching the packet is applied and processed, skipping the others.
    C. The firewall issues an error when committing NAT policy rules that can affect the same packet.
    D. The last matching rule in the list is applied and processed.

©2016-2019, Palo Alto Networks, Inc.

2.19 Given a configuration example including DNAT, identify how to configure security rules

96. An internal web browser sends a packet to a server. The browser's connection has the source IP address 192.168.5.3, port 31415. The destination is 209.222.23.245, port 80. The firewall translates the source to 75.22.21.54, port 27182. Which three of these source IP addresses would cause a rule to apply to this traffic? (Choose three.)
    - **A. 192.168.5.0/24**
    - B. 75.22.21.0/24
    - **C. 192.168.4.0/23**
    - **D. 192.168.0.0/16**
    - E. 75.22.0.0/17
    - F. 75.22.128.0/17
97. A NAT policy rule is created to change the destination address of any packets with a source of any address and a destination address of 10.10.10.10 (in the DMZ zone) to 192.168.3.45 (in the Trust zone). Which Security policy rule components are required for a packet that has this rule applied to match and allow this traffic?
    - A. source address any, source zone any, destination address 192.168.3.45, destination zone Trust, action = allow
    - **B. source address any, source zone any, destination address 10.10.10.10, destination zone Trust, action = allow**
    - C. source address any, source zone any, destination address 192.168.3.45, destination zone DMZ, action = allow
    - D. source address any, source zone any, destination address 10.10.10.10, destination zone DMZ, action = allow

2.20 Identify how to configure decryption

98. Which protocol is supported for traffic decryption matching a Decryption policy rule?
    - A. IPsec
    - B. SP3
    - **C. SSH**
    - D. NLSP
99. Where do you specify that a certificate is to be used for SSL Forward Proxy?
    - **A. Certificate properties**
    - B. Decryption Profile
    - C. Decryption policy
    - D. Security policy
100. Which feature must be configured to exclude sensitive traffic from decryption?
    - A. Security policy rule that includes the specific URL with an "allow" action
    - **B. Decryption policy rule with the specific URL and "no decrypt" action**
    - C. Application Override policy that matches the application URL and port number
    - D. Decryption Profile that includes the site's URL

©2016-2019, Palo Alto Networks, Inc.

2.21 Given a scenario, identify an application override configuration and use case

101. Which option is not a parameter used to identify applications in an Application Override policy?
    A. protocol
    B. port number
    C. first characters in the payload
    D. destination IP address

102. When an Application Override policy matches traffic and assigns an App-ID which firewall process is bypassed?
    A. QOS
    B. IP-Sec
    C. Content-ID
    D. User-ID

2.22 Identify how to configure VM-Series firewalls for deployment

103. Which virtual interface is the management on a VM-Series firewall running on ESXi?
    A. vNIC #1
    B. vNIC #2
    C. vNIC #9
    D. vNIC #10

104. Which three items of information are required at a minimum to install and configure VM-Series firewalls?
    A. VLANs to be connected through the firewall
    B. management port IP address
    C. IP addresses for the data interfaces
    D. management port default gateway
    E. management port netmask
    F. IP address for the external (internet-facing) interface

105. VM-Series firewalls require which additional license step?
    A. Apply a Base Capacity license
    B. Apply a Cloud Services license
    C. Apply a Site license
    D. Apply a VM Update license

106. A VM-Series firewall being deployed in Azure can be automatically configured by bootstrapping. Azure requires which features for Bootstrapping to work?
    A. Storage Account configured for Azure Files Service
    B. PowerShell script that feeds a configuration file to the firewall
    C. XML configuration file included in the base firewall provisioning
    D. Azure Backup services configured with a config file and included in the firewall provisioning

©2016-2019, Palo Alto Networks, Inc.

2.23 Identify how to configure firewalls to use tags and filtered log forwarding for integration with network automation

107. Dynamic tags can be assigned to which kind of data in a log event?
    A. source and destination address, source and destination zone name
    B. source and destination address
    C. interface, zone name
    D. DNS name, zone name

108. How can the firewall use dynamically tagged objects to block traffic?
    A. The object is added to an enforcement list of a Data Filtering Object that then is attached to a Security policy rule.
    B. The object is assigned to a Dynamic List, which then is included in the destination address matching condition of a Security policy rule.
    C. The object is assigned to a Dynamic Address Group object, which then is added to the destination address matching condition of a Security policy rule.

109. A dynamic tag can be assigned to data in which four types of log events?
    A. Traffic
    B. Threat
    C. URL Filtering
    D. HIP Match
    E. Tunnel Inspection
    F. Configuration
    G. System

110. Dynamic tagging activity is recoded in which log?
    A. System
    B. Configuration
    C. IP-Tag
    D. Data Filtering

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 3 – Operate

3.1 Identify considerations for configuring external log forwarding

111. Which two firewall logs can be exported using the Scheduled Log Export function?

A. Configuration
B. System
C. Traffic
D. URL

3.2 Interpret log files, reports, and graphs to determine traffic and threat trends

112. Which filter finds all log entries for traffic that originates from the internal device whose IP address is 172.17.1.3 and according to the header appears to be HTTP or HTTPS?

A. (addr.src in 172.17.1.3) and ((port.dst eq 80) or (port.dst eq 443))
B. ((addr.src in 172.17.1.3) and (port.dst eq 80)) or (port.dst eq 443)
C. (src.addr in 172.17.1.3) and ((dst.port eq 80) or (dst.port eq 443))
D. ((src.addr in 172.17.1.3) and (dst.port eq 80)) or (dst. port eq 443)

113. Which two log files would you use if you suspect that a rogue administrator is modifying the firewall's rulebase to allow and hide illicit traffic? (Choose two.)

A. Traffic
B. Threat
C. Data Filtering
D. Configuration
E. System

114. Which product is required to use event correlation?

A. next-generation firewall, PA-220
B. Advanced Endpoint Protection
C. Panorama
D. GlobalProtect

3.3 Identify scenarios in which there is a benefit from using custom signatures

115. How is a custom application configured that uses DNS to transfer directory information and needs to be filtered in a very different manner than normal DNS?

A. You cannot do it with the NGFW. You need to manually configure a proxy.
B. Create specific rules for the sources and destinations that run this application.
C. Create a custom signature and specify the DNS fields that are different from normal DNS use and patterns to identify when it is the custom application.
D. Create an Application Override policy and specify the sources and destinations that run this application.

©2016-2019, Palo Alto Networks, Inc.

116. What are two results of using Application Override policies? (Choose two.)

A. prevent matching traffic from entering VPN tunnels

B. apply a specified App-ID label to matching traffic

C. prevent matching traffic from being logged

D. cause matching traffic to bypass Content-ID processing

E. route traffic to WildFire for scanning

117. Which two types of entities can have custom signatures?

A. Services

B. URL categories

C. User groups

D. Applications

E. Vulnerabilities

3.4 Given a scenario, identify the process to update a Palo Alto Networks system to the latest version of the software

118. In which order do you update dynamic content and the PAN-OS version?

A. Update the PAN-OS version first, then the dynamic content.

B. Update the dynamic content first, then the PAN-OS version.

C. Update both at the same time.

119. In which order do you upgrade the different components of the firewall to a next version?

A. firewalls, then Panorama, then Log Collectors

B. Panorama and the Log Collectors, then the firewalls

C. Log Collectors, Panorama and the firewall

120. How do you upgrade a High Availability pair (A/P) to PAN-OS 9.0? Assume you need to keep internet access up during the upgrade.

A. Upgrade the active firewall first, then the passive one.

B. Upgrade the passive firewall first, then the active one.

C. Run the upgrade on the active firewall. It will manage the process and upgrade the passive firewall.

D. You must upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

3.5 Identify how configuration management operations are used to ensure desired operational state of stability and continuity

121. What is the format of the configuration files?

A. YAML

B. JSON

C. XML

D. Some are in XML. Some in YAML

©2016-2019, Palo Alto Networks, Inc.

122. Which CLI command do you use to copy a partial configuration file to a firewall?
    A. **scp** from a different device. The firewall serves as the file server.
    B. **ssh** from a different device. The firewall serves as the file server.
    C. scp from the firewall's CLI. A different computer serves as the file server.
    D. **ssh** from the firewall's CLI. A different computer serves as the file server.

3.6 Identify the settings related to critical HA functions (link monitoring; path monitoring; HA1, HA2, and HA3 functionality; HA backup links; and differences between A/A and A/P)

123. Which option is an intended advantage of an active/active HA pair vs. an active/passive pair?
    A. increased throughput
    B. support of asynchronous routing
    C. increased session count
    D. shared dynamic updates

3.7 Identify the sources of information that pertain to HA functionality

124. Which MIB specifies the fields for information about the High Availability interfaces?
    A. MIB-II
    B. IF-MIB
    C. PAN-COMMON-MIB.my
    D. PAN-PRODUCT-MIB.my

3.8 Identify how to configure the firewall to integrate with AutoFocus and verify its functionality

125. A principle benefit of the AutoFocus product is:
    A. Provide additional threat detection data to the firewall
    B. Manage access to SaaS applications through the firewall
    C. Provide additional context to previously discovered threats
    D. Examine Cortex Data Lake log data for undetected threats

3.9 Identify the impact of deploying dynamic updates

126. Which field in a new App-ID facilitates the determination of the App-ID's impact on policy enforcement?
    A. Name
    B. Depends on
    C. Previously Identified As
    D. App-ID Enabled

©2016-2019, Palo Alto Networks, Inc.

3.10 Identify the relationship between Panorama and devices as pertaining to dynamic updates versions and policy implementation and/or HA peers

127. Which type of device can receive the Antivirus content update?
    A. Log Collector
    B. firewall
    C. AutoFocus
    D. MindMeld

128. What requirement must a Panorama meet to update a managed firewall's antivirus file?
    A. The PAN-OS versions on the firewall and Panorama must be the same
    B. Panorama and the firewall must be able to connect to Palo Alto Network's update server
    C. The update must be installed on Panorama before any firewalls
    D. Panorama must download an antivirus file version compatible with the target firewall's PAN-OS version

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 4 – Configuration Troubleshooting

4.1 Identify system and traffic issues using the web interface and CLI tools

129. Users cannot access their Gmail accounts through the firewall. Which log do you look in, and which filter do you use?
    - **A. Traffic, (app eq gmail)**
    - B. Traffic, (app in gmail)
    - C. Configuration, (app eq gmail)
    - D. Configuration, (app in gmail)

130. You can't get to the web interface. How do you check from the command line if it is running?
    - A. ps -aux | grep appweb
    - B. ps -aux | match appweb
    - C. show system software status | grep appweb
    - **D. show system software status | match appweb**

131. Which log file shows that a connection with an LDAP server was dropped?
    - A. Traffic Log
    - **B. System Log**
    - C. User-ID Log
    - D. Authentication Log

4.2 Given a session output, identify the configuration requirements used to perform a packet capture

132. Which Security Profiles do not have a packet capture option?
    - A. Antivirus
    - B. Anti-spyware
    - C. Vulnerability Protection
    - **D. URL Filtering**

133. On a PA-7080, which feature (if any) do you need to disable to use packet capture?
    - A. None
    - **B. Hardware offload**
    - C. Hardware acceleration
    - D. Decryption

134. Under which circumstance must you use tcpdump on the next-generation firewall?
    - A. CLI capture of tunnel interface traffic
    - **B. CLI capture of packets on traffic interfaces**
    - C. CLI capture of packets on the management interface
    - D. CLI capture of IPsec negotiation traffic

©2016-2019, Palo Alto Networks, Inc.

4.3 Given a scenario, identify how to troubleshoot and configure interface components

135. Where in the user interface can you see if any sessions are going through a specific interface?
    A. dashboard
    B. Application Control Center (ACC)
    C. session log node in the Monitor tab
    D. The session browser node in the Monitor tab

136. Communication through a specific interface works most of the time but fails when traffic is at its highest. In which policy do you look to identify the problem?
    A. Security policy
    B. DoS Protection Policy
    C. QoS Policy
    D. Application Override Policy

137. Which interface mode allows you to add firewall protection to a network with the least disruption?
    A. Tap
    B. Layer 3
    C. Layer 2
    D. Virtual Wire

4.4 Identify how to troubleshoot SSL decryption failures

138. SSL decryption has been working for the customer but suddenly it stopped. What could be a possible reason?
    A. The firewall's CA certificate expired. By default, those certificates are valid for one year.
    B. The firewall's IP address, which is encoded in the certificate, changed.
    C. The firewall has been upgraded to a different model.
    D. The firewall's decryption subscription expired.

139. The company uses a small SaaS provider for some specialized need. This SaaS is provided through HTTPS. Suddenly, it stopped working through the firewall. When accessed from home, users receive an error about the certificate. Which two situations would explain this?
    A. The SaaS's certificate had expired. The firewall's decryption policy is configured to block connections with expired certificates.
    B. The SaaS's certificate had expired. The firewall's decryption policy is configured to use the untrusted CA with expired certificates.
    C. The SaaS's certificate was replaced with one whose Certificate Authority is not known to the firewall. The firewall's decryption policy is configured to block connections with certificates whose CA is not trusted.
    D. The SaaS's certificate was replaced with one whose Certificate Authority is not known to the firewall. The firewall's decryption policy is configured to use the untrusted certificate for certificates whose CA is not trusted.
    E. The firewall's own CA certificate needs to be updated.

©2016-2019, Palo Alto Networks, Inc.

140. Which encryption algorithm is not supported, and if the settings specify it using it causes the firewall to stop the connection?

A. DES

B. 3DES

C. AES252-CBC

D. AES256-GCM

4.5 Identify issues with the certificate chain of trust

141. Which condition could be a symptom of a chain of trust issue?

A. The firewall no longer decrypts HTTPS traffic.

B. The firewall no longer decrypts HTTPS traffic from a specific site.

C. The firewall still decrypts HTTPS traffic from all sites, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.

D. The firewall still decrypts HTTPS traffic from a specific site, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.

142. Which field is mandatory in the subject field of a certificate?

A. Organization

B. Organizational Unit

C. Common Name

D. Locale

143. Which field in a certificate has to include a value known to the firewall for the certificate to be considered valid by the firewall?

A. Issuer

B. Subject

C. Key

D. Object

4.6 Given a scenario, identify how to troubleshoot traffic routing issues

144. Where do you find the dynamic routing configuration for data in the NGFW's web interface?

A. Device > Network > Virtual Router

B. Network > Virtual Router

C. Device > Network > Interfaces

D. Network > Interfaces

©2016-2019, Palo Alto Networks, Inc.

145. What could be two reasons that some IP addresses get good performance when going to websites, and others IP addresses in the same network get bad performance (with the same sites)? This is happening consistently; the same IP addresses always get the bad performance. The organization has redundant connections to the internet, and all three of them are up. (Choose two.)

A. The organization uses equal-cost multi-path (ECMP) routing to the internet and selects which path to use based on the source IP address, and some IP addresses get routed through a slower ISP.

B. The organization uses Policy Based Forwarding (PBF) and selects which route to use for the internet based on source IP address, and some IP addresses get routed through a slower ISP.

C. The organization uses the Routing Information Protocol (RIP), and some IP addresses get routed through a slower ISP.

D. The organization uses Border Gateway Protocol (BGP), and some IP addresses get routed through a slower ISP.

E. The organization uses Open Shortest Path First (OSPF), and some IP addresses get routed through a slower ISP.

146. The organization has two links to the internet, one 100Mbps and the other 10Mbps. The firewall balances them using equal-cost multi-path (ECMP) in the virtual router. Which load balancing ECMP setting does the organization need to use to optimize network resources?

A. Balanced Round Robin

B. Weighted Round Robin, with a weight of 10 for the fast connection and 100 for the slow one.

C. IP Hash

D. Weighted Round Robin, with a weight of 100 for the fast connection and 10 for the slow one.

©2016-2019, Palo Alto Networks, Inc.

Exam Domain 5 – Core Concepts

5.1 Identify the correct order of the policy evaluation based on the packet flow architecture

147. What is the correct order of operations between the Security policy and the NAT policy?
    A. NAT policy evaluated, Security policy evaluated, NAT policy applied, Security policy applied
    B. NAT policy evaluated, NAT policy applied, Security policy evaluated, Security policy applied
    C. NAT policy evaluated, Security policy evaluated, Security policy applied, NAT policy applied
    D. Security policy evaluated, NAT evaluated, NAT policy applied, Security policy applied

148. Which two statements are correct regarding policy evaluation?
    A. All policies are evaluated, and the most specific policy will match.
    B. Policies are evaluated from the top down, and the first match processes the traffic.
    C. Interzone traffic is allowed by default.
    D. Intrazone traffic is allowed by default.
    E. Outbound traffic is allowed by default. Only inbound traffic is evaluated.

149. In which of these operations is the order correct?
    A. Decryption, check allowed ports, app-ID identification, check Security policy
    B. Decryption, app-ID identification, check allowed ports, check Security policy
    C. Check allowed ports, decryption, app-ID identification, check Security policy
    D. Decryption, app-ID identification, check Security policy, check allowed ports

5.2 Given an attack scenario, identify the appropriate Palo Alto Networks threat prevention component to prevent or mitigate the attack

150. A URL Filtering Profile is part of which type of identification?
    A. App-ID
    B. Content-ID
    C. User-ID
    D. Service

151. Which stage of the kill chain is most likely to be stopped by dividing the network into separate security zones and making sure all inter-zone traffic is inspected by a firewall?
    A. Reconnaissance
    B. Execution
    C. Lateral movement
    D. Data exfiltration

152. Which component can tell you if an attack is an advanced persistent threat (APT) or a broad attack designed to produce a botnet for future abuse?
    A. next-generation firewall
    B. WildFire
    C. MindMeld
    D. AutoFocus

©2016-2019, Palo Alto Networks, Inc.

5.3 Identify methods for identifying users

153. User-ID maps users to what type of information? (Choose the most accurate answer.)
    A. MAC addresses
    B. IP addresses
    C. IP address/port number combinations
    D. IP addresses in the case of single-user devices (tablets, PCs, etc.), IP address / port number combinations in the case of Linux and UNIX servers
154. What protocol or protocols does User-ID use to map between user identities and groups?
    A. NetBIOS
    B. LDAP
    C. syslog
    D. It can use both LDAP and syslog
155. What format do you use when calling the API to inform the firewall of a new IP to user ID mapping?
    A. XML
    B. JSON
    C. YAML
    D. Base64

5.4 Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks firewall

156. On a PA-7000, which management function runs on a separate card?
    A. configuration management
    B. logging
    C. reporting
    D. The web user interface
157. Does the next-generation firewall use FPGA? If so, in which plane or planes?
    A. No, never
    B. Yes, on the data plane, but only on higher end models
    C. Yes, on the management plane, but only on higher end models
    D. On both data the data plane and the management plane, but only on higher end models
158. Which function resides on the management plane?
    A. App-ID matching
    B. route lookup
    C. policy match
    D. logging

©2016-2019, Palo Alto Networks, Inc.

5.5 Given a scenario, determine how to control bandwidth use on a per-application basis

159. What parameter whose value is known to NGFW is important for QoS decisions?
    - **A. App-ID**
    - B. Content-ID
    - C. User-ID
    - D. Ingress interface

160. How many QoS classes does the next-generation firewall support?
    - A. 4
    - **B. 8**
    - C. 16
    - D. 32

161. Which additional information about an established connection cannot change its QoS class?
    - A. App-ID
    - B. URL category
    - C. User-ID (if allowed for all users, and then the firewall gets the User-ID for a different reason)
    - **D. Content-type (for example, downloading an executable can have a different QoS class from downloading a PDF).**

5.6 Identify the fundamental functions and concepts of WildFire

162. Which file type is not supported by WildFire?
    - **A. iOS applications**
    - B. Android applications
    - C. Windows applications
    - D. Microsoft Excel files

163. The firewall will skip the upload to WildFire in which three cases?
    - **A. The file has been signed by a trusted signer.**
    - B. The file is being uploaded rather than downloaded.
    - C. The file is an attachment in an email.
    - **D. The file hash matches a previous submission.**
    - E. The file is larger than 50MB.
    - F. The file is transferred through HTTPS.

164. Which of these features is not supported on the WF-500 appliance?
    - **A. Bare metal analysis**
    - B. Microsoft Windows XP 32-bit analysis
    - C. Microsoft Windows 7 64-bit analysis
    - D. Static analysis

©2016-2019, Palo Alto Networks, Inc.

5.7 Identify the purpose of and use case for MFA and the Authentication policy

165. What are the two purposes of multi-factor authentication?
    - **A. reduce the value of stolen passwords**
    - B. simplify password resets
    - **C. reduce/prevent password sharing**
    - D. ensure strong passwords
    - E. provide single sign-on functionality

166. Which of these MFA factors is not supported by the next-generation firewall?
    - A. Voice
    - B. Push
    - C. SMS
    - **D. S/Key**

167. What is the meaning of setting the source user to known-user in an authentication policy rule?
    - **A. The user identity is known (tied to an IP address), but the resource is sensitive enough to require additional authentication.**
    - B. The next-generation firewall will demand user authentication, and only then will the resource be available.
    - C. The source device is a known device, which is only used by a single person.
    - D. There is no such option. If the user identity is known, there is no need for an authentication policy rule.

5.8 Identify the dependencies for implementing MFA

168. What are the two Captive Portal modes? (Choose two.)
    - A. Proxy
    - **B. Transparent**
    - C. Web form
    - D. Certificate
    - **E. Redirect**

169. Which of these actions is not required to configure Multi-factor authentication using SAML and an Identity Provider (IdP)?
    - A. Create an authentication policy rule.
    - **B. Configure NTLM settings.**
    - C. Create an authentication object.
    - D. Create an authentication profile.

170. An authentication policy rule has a HIP profile. Where are the users being authenticated coming from?
    - A. Internal devices, such as Linux workstations
    - B. External devices belonging to customers of the organization
    - C. Internal servers running UNIX (Solaris, HPUX, AIX, etc.).
    - **D. GlobalProtect connections through the internet**

©2016-2019, Palo Alto Networks, Inc.

5.9 Given a scenario, identify how to forward traffic

171. A company has strict security requirements that require every connection between two internal computers to be inspected. Those internal computers are connected and disconnected by non-technical users. How do you forward traffic between those internal computers?
    A. Use a switch.
    B. Use an NGFW configured as a switch, with Layer 2 interfaces.
    C. Use an NGFW configured as a router, with Layer 3 interfaces.
    D. Use an NGFW in TAP or Virtual Mirror mode.
172. You have two links to the internet, going through two ISPs (for backup purposes). Link A has a lower latency, and link B supports a higher bandwidth. Which link would you use for VoIP, and how will you specify to use it?
    A. Link A, specify in a Policy Based Forwarding policy
    B. Link B, specify in a Policy Based Forwarding policy
    C. Link A, specify in a Virtual Router
    D. Link B, specify in a Virtual Router
173. Can you put devices on two sides of a VPN tunnel on the same Ethernet segment?
    A. No, because this requirement never happens.
    B. No, because Ethernet at layer 2 is a lower layer than a layer 3 VPN tunnel
    C. Yes, if you tunnel Ethernet over IP.
    D. Yes, because VPN tunnels can be layer 2 tunnels.

5.10 Given a scenario, identify how to configure policies and related objects

174. Which action specifies that Security Profiles are relevant in a policy rule?
    A. Deny
    B. Drop
    C. Reset
    D. Allow
175. Are files quarantined while WildFire checks if they are malware or legitimate?
    A. Yes
    B. No
    C. By default, yes, but you can change the settings.
    D. By default, no, but you can change the settings.
176. What feature of the next-generation firewall allows you to block websites that are not business-appropriate?
    A. App-ID
    B. File Blocking
    C. Exploit Protection
    D. URL Filtering

©2016-2019, Palo Alto Networks, Inc.

5.11 Identify the methods for automating the configuration of a firewall

177. Which operating system do you select to use for a Palo Alto Networks NGFW running in Microsoft Azure?

    A. Windows
    B. BSD
    C. Linux
    D. Linux or BSD

178. What are the four component directories of a Palo Alto Networks bootstrap container?

    A. software, config, license, and content
    B. software, config, lic, and content
    C. software, configuration, license, and content
    D. software, configuration, lic, and content

179. Which environment supports a USB drive for the firewall bootstrap?

    A. VMware ESXi
    B. physical firewall
    C. Microsoft Hyper-V
    D. KVM

©2016-2019, Palo Alto Networks, Inc.

Appendix C: Answers to the Sample Test

1. What is the last step of packet processing in the firewall?
    A. check allowed ports
    B. check Security Profiles
    C. check Security policy
    D. forwarding lookup
2. Which interface type requires you to configure where the next hop is for various addresses?
    A. TAP
    B. Virtual Wire
    C. Layer 2
    D. Layer 3
3. Can you allow the firewall to be managed through a data interface? Where do you specify it?
    A. You specify **Web UI** in the interface properties.
    B. You specify **Management** in the interface properties.
    C. You specify HTTPS in the Interface Management Profile, and then specify in the interface properties to use that profile.
    D. You specify **Management** in the Interface Management Profile, and then specify in the interface properties to use that profile.
4. Some devices managed by Panorama have their external interface on ethernet1/1, some on ethernet1/2. However, the zone definitions for the external zone are identical. What is the recommended solution in this case?
    A. Create two templates: One for the ethernet1/1 devices, one for the ethernet1/2 devices. Use the same external zone definitions in both. Apply those two templates to the appropriate devices.
    B. Create three templates: One for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Use those templates to create two template stacks, one with the ethernet1/1 and external zone, another with the ethernet1/2 and external zone. Apply those two template stacks to the appropriate devices.
    C. Create three templates: One for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
    D. Create three template stacks: One for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
5. Which two options have the correct order of policy evaluation? (Remembering that not all rule types exist in all policies.) (Choose two.)
    A. device group pre-rules, shared pre-rules, local firewall rules, intrazone-default, interzone-default
    B. device group pre-rules, local firewall rules, shared post-rules, device group post-rules, intrazone-default, interzone-default
    C. device group pre-rules, local firewall rules, device group post-rules, shared post-rules,

©2016-2019, Palo Alto Networks, Inc.

intrazone-default, interzone-default

D. device group pre-rules, local firewall rules, intrazone-default, interzone-default, device group post-rules, shared post-rules

E. shared pre-rules, device group pre-rules, local firewall rules, intrazone-default, interzone-default

6. When you deploy the Palo Alto Networks NGFW on NSX, how many virtual network interfaces does a VM-Series firewall need?
   A. two, one for traffic input and output and one for management traffic
   B. four, two for traffic input and output and two for management traffic (for High Availability)
   C. three, one for traffic input, one for traffic output, and one for management traffic
   D. six, two for traffic input, two for traffic output, and two for management traffic (for High Availability)
7. Which source of user information is *not* supported by the NGFW?
   A. RACF
   B. LDAP
   C. Active Directory
   D. SAML
8. What is the main mechanism of packet-based attacks?
   A. malformed packets that trigger software bugs when they are received
   B. excess packets that fill up buffers, preventing legitimate traffic from being processed
   C. packets that get responses that leak information about the system
   D. packets that either fill up buffers or get responses that leak information
9. Which method is *not* a decryption method?
   A. SSH Proxy
   B. SSL Proxy
   C. SSL Forward Proxy
   D. SSL Inbound Inspection
10. What type of identification does an Application Override policy override?
    A. App-ID
    B. User-ID
    C. Content-ID
    D. Service
11. Which two types of application can cause an insufficient data value in the Application field in the Traffic log? (Choose two.)
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
    E. IGP
12. Which three profile types are used to prevent malware from entering the network? (Choose three.)
    A. Antivirus
    B. Anti-spyware

©2016-2019, Palo Alto Networks, Inc.

C. WildFire® analysis

D. File blocking

E. Vulnerability Protection

F. Zone Protection

13. Which user credential detection method does not require access to an external directory?

A. group mapping

B. domain credential filter

C. LDAP

D. Certificate

14. Which object type(s) has a property to specify whether it can transfer files?

A. Application

B. Service

C. User

D. User group

15. When destination NAT rules are configured, the associated security rule is matched using which parameters?

A. pre-NAT source zone and post-NAT destination zone

B. post-NAT source zone and pre-NAT destination zone

C. pre-NAT source zone and post-NAT destination IP address

D. post-NAT source zone and post-NAT destination zone

16. What is the initial IP address for the management interface?

A. 10.0.0.1

B. 172.16.0.1

C. **192.168.1.1**

D. 192.168.255.254

17. In a new firewall, which port provides web interface access by default?

A. Data port #1

B. any data port

C. Management port

D. Console port

18. Which application requires you to import private keys?

A. Capital Portal

B. Forward Trust

C. SSL Inbound Inspection

D. SSL Exclude Certificate

©2016-2019, Palo Alto Networks, Inc.

19. Can two Layer 3 interfaces have the same IP address. If so, under which conditions?
    A. No, that is impossible.
    B. Yes, but they must be connected to the same Ethernet network through a switch. This configuration can be used only for High Availability.
    C. Yes, but they must be connected to different virtual routers.
    D. Yes, but they must be subinterfaces of the same physical interface.
20. Which two protocols are supported for site-to-site VPNs? (Choose two.)
    A. Authentication header (AH)
    B. Secure Socket Layer (SSL)
    C. Encapsulating Security Payload (ESP)
    D. Transport Layer Security (TLS)
    E. Secure Shell (SSH)
21. Which two functions is a GlobalProtect Portal responsible for? (Choose two.)
    A. terminating SSL tunnels
    B. authenticating GlobalProtect users
    C. creating on-demand certificates to encrypt SSL
    D. managing and updating GlobalProtect client configurations
    E. managing GlobalProtect Gateway configurations
22. What is the preferred SYN flood action?
    A. Random Drop
    B. Random Early Drop
    C. SYN Proxy
    D. SYN Cookies
23. What, if anything, would be a valid reason to allow non-SYN TCP packets at the start of a connection?
    A. Such packets could happen legitimately in the case of asymmetric routing.
    B. Such packets could happen legitimately if there is load balancing across firewalls.
    C. Such packets could happen legitimately because of either asymmetric routing or load balancing across firewalls.
    D. Such packets could happen because of router bugs
24. Where do you configure protection from malformed IP and TCP headers?
    A. DoS Profile
    B. QoS Profile
    C. Zone Protection Profile
    D. Application Profile
25. Which parameter is *not* a valid criterion for the original packet in address translation?
    A. source zone
    B. application
    C. service
    D. destination address
26. Which parameter do you use to apply a rule to traffic coming in from a specific interface?
    A. source zone
    B. source address
    C. User

©2016-2019, Palo Alto Networks, Inc.

D. source interface

27. Where do you specify that certain URL categories are not to be decrypted (to avoid the liability of holding information such as employees' personal bank credentials)?
    A. certificate properties
    B. Decryption Profile
    C. Decryption policy
    D. Security policy
28. Where do you specify how the firewall should treat invalid certificates?
    A. certificate properties
    B. Decryption Profile
    C. Decryption policy
    D. Security policy
29. Which two public cloud environments support pay-as-you-go (PAYG) firewall licensing? (Choose two.)
    A. Microsoft Azure
    B. Microsoft Hyper-V
    C. Amazon AWS
    D. VMware NSX
    E. VMware ESXi
30. Which log type gets redirected in **Device > Log Settings**?
    A. Config log
    B. Traffic log
    C. Threat log
    D. WildFire Submission log
31. Which tab of the user interface gives you a consolidated picture of the security situation and the top-level threats?
    A. Dashboard
    B. ACC
    C. Monitor
    D. Devices
32. A customer's custom application uses SMTP (email) to transfer directory information, which needs to be filtered in a very different manner than normal DNS. How do you configure this filtering?
    A. You cannot do it with the NGFW. You need to manually configure a proxy.
    B. Create specific rules for the sources and destinations that run this application.
    C. Create a custom signature and specify the SMTP fields that are different from normal DNS use and patterns to identify when it is the custom application.
    D. Create an Application Override policy and specify the sources and destinations that run this application.
33. Which kind of update (or updates) requires a disruption in connectivity?
    A. There never is a need to disrupt connectivity.
    B. Only dynamic content updates require a brief disruption while the firewall integrates them with the Security policy.
    C. Only PAN-OS® updates require a reboot to apply.

©2016-2019, Palo Alto Networks, Inc.

D. Both dynamic content updates and PAN-OS® updates cause disruption in connectivity.

34. Which High Availability port (or ports) is used for which plane?
    A. HA1 for the data plane, HA2 for the management plane.
    B. HA1 for the management plane, HA2 for the data plane.
    C. If HA1 works, it is used for both data and management. HA2 is a backup.
    D. HA1 for the management plane, HA2 for the data plane in the 7000 Series. The less costly models have only an HA1, which is used for both management and data.
35. Which two protocols can AutoFocus use to retrieve log information from an NGFW? (Choose two.)
    A. syslog
    B. Log transfer protocol, a Palo Alto Networks proprietary protocol
    C. HTTP
    D. HTTPS
    E. SNMP
36. How often does Palo Alto Networks publish new applications?
    A. every 30 minutes
    B. hourly
    C. daily
    D. weekly
37. Which type of device can receive the GlobalProtect data files content update?
    A. Log Collector
    B. firewall
    C. WildFire®
    D. Antivirus
38. An administrator claims to be unable to log in to the firewall. In which log will you see evidence of this problem?
    A. Traffic
    B. System
    C. Configuration
    D. Authentication
39. How do you reboot the firewall from the command line?
    A. restart system
    B. reboot
    C. request restart system
    D. request reboot
40. Where in the user interface do you configure how many packets to capture?
    A. In the Device tab, as part of the Setup node.
    B. In the Security Profiles, because the desired number of captured packets can vary between profiles.
    C. You configure a default in the Device tab, as part of the Capture node. Then, you can configure exceptions in the Security Profiles.
    D. You don't, you can only configure the number of packets to capture on the command line interface
41. You are preparing a bootstrap template for use with either Microsoft Azure or Amazon AWS. You

©2016-2019, Palo Alto Networks, Inc.

don't want to include the Content-ID files because the firewall will download the latest version when it is booted anyway. What do you do?

A. Leave the content directory empty.

B. Do not create a content directory.

C. Either leave the content directory empty or do not create it.

D. Create a content directory, but put in a placeholder file, download latest.

42. Which format do you use for an AWS CloudFormation Template?

A. XML

B. CSV

C. JSON

D. JSON or XML

43. When are security rules from Panorama processed, compared to local firewall rules?

A. The question is incorrect, because a firewall can either have local rules or Panorama rules.

B. Panorama rules are processed first, so they take precedence.

C. Local rules are processed first, so they take precedence.

D. Some Panorama rules are processed before the firewall's local rules, and some are processed after the local rules.

44. Which statement about Security Profiles is correct?

A. They are evaluated from top down, with the first match processing the traffic.

B. They are applied to all inbound traffic when they are enabled.

C. They enable a specific type of scanning (e.g., Virus, Spyware).

D. They can specify actions based on the username.

45. Which authentication method can be handled by the browser without affecting the user experience?

A. web-challenge

B. browser-challenge

C. web-form

D. browser-form

46. The R&D network of the defense contractor is not connected to the internet. However, it is connected to SIPRNet (https://en.wikipedia.org/wiki/SIPRNet), which is used to transfer classified information. The contractor is concerned about getting malware files and infected PDFs through that network. Can this company use WildFire® for protection?

A. No, because there is no network path to the WildFire® server.

B. No, but no protection is needed because everybody with SIPRnet access has a security clearance and is trustworthy.

C. Yes, but only if they can get approval to have a gateway to the public internet.

D. Yes. They can use a WF-500 appliance.

47. How does the NGFW handle excess packets when there are QoS constraints?

A. It buffers them until there is bandwidth to send them.

B. It drops a percentage of them randomly.

C. It replaces them with packets that tell the computer on the other side to slow down.

D. It sends a portion instead of the whole packet.

48. Which function is performed by the control plane?

©2016-2019, Palo Alto Networks, Inc.

A. signature matching
B. route lookup
C. policy matching
D. route updates

49. Which User-ID methods is *not* transparent to the user?
A. CaptivePortal
B. User-ID agent connected to Active Directory
C. User-ID agent monitoring server logs for login events
D. User-ID agent connected to a Cisco WLAN controller

50. Which feature of the NGFW lets you identify attempts to tunnel SSH over other ports?
A. App-ID
B. Content-ID
C. User-ID
D. Content-ID and User-ID

51. What is the correct order of operations?
A. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security policy, check Security Profiles, re-encrypt traffic.
B. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security Profiles, check Security policy, re-encrypt traffic.
C. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security policy, re-encrypt traffic.
D. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security Profiles, check Security policy, re-encrypt traffic.

©2016-2019, Palo Alto Networks, Inc.

Appendix D: Glossary

Advanced Encryption Standard (AES): A symmetric block cipher based on the Rijndael cipher.
AES: See Advanced Encryption Standard (AES).
API: See application programming interface (API).
application programming interface (API): A set of routines, protocols, and tools for building software applications and integrations.
application whitelisting: A technique used to prevent unauthorized applications from running on an endpoint. Authorized applications are manually added to a list that is maintained on the endpoint. If an application is not on the whitelist, it cannot run on the endpoint. However, if it is on the whitelist the application can run, regardless of whether vulnerabilities or exploits are present within the application.
attack vector: A path or tool that an attacker uses to target a network.
BES: See bulk electric system (BES).
boot sector: Contains machine code that is loaded into an endpoint's memory by firmware during the startup process, before the operating system is loaded.
boot sector virus: Targets the boot sector or master boot record (MBR) of an endpoint's storage drive or other removable storage media. See also *boot sector* and *master boot record (MBR)*.
bot: Individual endpoints that are infected with advanced malware that enables an attacker to take control of the compromised endpoint. Also known as a zombie. See also *botnet*.
botnet: A network of bots (often tens of thousands or more) working together under the control of attackers using numerous command and control (CnC) servers. See also *bot*.
bring your own apps (BYOA): Closely related to BYOD, BYOA is a policy trend in which organizations permit end users to download, install, and use their own personal apps on mobile devices, primarily smartphones and tablets, for work-related purposes. See also *bring your own device (BYOD)*.
bring your own device (BYOD): A policy trend in which organizations permit end users to use their own personal devices, primarily smartphones and tablets, for work-related purposes. BYOD relieves organizations from the cost of providing equipment to employees, but creates a management challenge due to the vast number and type of devices that must be supported. See also *bring your own apps (BYOA)*.
bulk electric system (BES): The large interconnected electrical system, consisting of generation and transmission facilities (among others), that comprises the "power grid."
BYOA: See bring your own apps (BYOA).
BYOD: See bring your own device (BYOD).
child process: In multitasking operating systems, a sub-process created by a parent process that is currently running on the system.
CIP: See Critical Infrastructure Protection (CIP).
consumerization: A computing trend that describes the process that occurs as end users increasingly find personal technology and apps that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use, than enterprise IT solutions.
covered entity: Defined by HIPAA as a healthcare provider that electronically transmits PHI (such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies), a health plan (such as a health insurance company, health maintenance organization, company health plan, or government program including Medicare, Medicaid, military and veterans' healthcare), or a healthcare clearinghouse. See also *Health Insurance Portability and Accountability Act (HIPAA)* and *protected health information (PHI)*.
Critical Infrastructure Protection (CIP): Cybersecurity standards defined by NERC to protect the physical

©2016-2019, Palo Alto Networks, Inc.

and cyber assets necessary to operate the bulk electric system (BES). See also *bulk electric system (BES)* and *North American Electric Reliability Corporation (NERC)*.

data encapsulation: A process in which protocol information from the OSI layer immediately above is wrapped in the data section of the OSI layer immediately below. See also *open systems interconnection (OSI) reference model*.

DDOS: See distributed denial-of-service (DDOS).

distributed denial-of-service (DDOS): A type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable.

EAP: See extensible authentication protocol (EAP).

EAP-TLS: See extensible authentication protocol Transport Layer Security (EAP-TLS).

EHR: See electronic health record (EHR).

electronic health record (EHR): As defined by HealthIT.gov, an EHR "goes beyond the data collected in the provider's office and include[s] a more comprehensive patient history. EHR data can be created, managed, and consulted by authorized providers and staff from across more than one healthcare organization."

electronic medical record (EMR): As defined by HealthIT.gov, an EMR "contains the standard medical and clinical data gathered in one provider's office."

EMR: See electronic medical record (EMR).

endpoint: A computing device such as a desktop or laptop computer, handheld scanner, point-of-sale (POS) terminal, printer, satellite radio, security or videoconferencing camera, self-service kiosk, server, smart meter, smart TV, smartphone, tablet, or Voice over Internet Protocol (VoIP) phone. Although endpoints can include servers and network equipment, the term is generally used to describe end user devices.

Enterprise 2.0: A term introduced by Andrew McAfee and defined as "the use of emergent social software platforms within companies, or between companies and their partners or customers." See also *Web 2.0*.

exclusive or (XOR): A Boolean operator in which the output is true only when the inputs are different (for example, TRUE and TRUE equals FALSE, but TRUE and FALSE equals TRUE).

exploit: A small piece of software code, part of a malformed data file, or a sequence (string) of commands, that leverages a vulnerability in a system or software, causing unintended or unanticipated behavior in the system or software.

extensible authentication protocol (EAP): A widely used authentication framework that includes approximately 40 different authentication methods.

extensible authentication protocol Transport Layer Security (EAP-TLS): An Internet Engineering Task Force (IETF) open standard that uses the Transport Layer Security (TLS) protocol in Wi-Fi networks and PPP connections. See also *point-to-point protocol (PPP)* and *Transport Layer Security (TLS)*.

extensible markup language (XML): A programming language specification that defines a set of rules for encoding documents in a human- and machine-readable format.

false negative: In anti-malware, malware that is incorrectly identified as a legitimate file or application. In intrusion detection, a threat that is incorrectly identified as legitimate traffic. See also *false positive*.

false positive: In anti-malware, a legitimate file or application that is incorrectly identified as malware. In intrusion detection, legitimate traffic that is incorrectly identified as a threat. See also *false negative*.

favicon ("favorite icon"): A small file containing one or more small icons associated with a particular website or webpage.

Federal Information Security Management Act (FISMA): See *Federal Information Security Modernization Act (FISMA)*.

Federal Information Security Modernization Act (FISMA): A U.S. law that implements a comprehensive framework to protect information systems used in U.S. federal government agencies. Known as the Federal Information Security Management Act prior to 2014.

Financial Services Modernization Act of 1999: See *Gramm-Leach-Bliley Act (GLBA)*.

©2016-2019, Palo Alto Networks, Inc.

FISMA: See Federal Information Security Modernization Act (FISMA).
floppy disk: A removable magnetic storage medium commonly used from the mid-1970s until approximately 2007, when they were largely replaced by removable USB storage devices.
generic routing encapsulation (GRE): A tunneling protocol developed by Cisco Systems® that can encapsulate various network layer protocols inside virtual point-to-point links.
GLBA: See Gramm-Leach-Bliley Act (GLBA).

Gramm-Leach-Bliley Act (GLBA): A U.S. law that requires financial institutions to implement privacy and information security policies to safeguard the non-public personal information of clients and consumers. Also known as the Financial Services Modernization Act of 1999.
GRE: See generic routing encapsulation (GRE).
hacker: Originally used to refer to anyone with highly specialized computing skills, without connoting good or bad purposes. However, common misuse of the term has redefined a hacker as someone that circumvents computer security with malicious intent, such as a cybercriminal, cyberterrorist, or hacktivist.
hash signature: A cryptographic representation of an entire file or program's source code.
Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that defines data privacy and security requirements to protect individuals' medical records and other personal health information. See also *covered entity* and *protected health information (PHI).*
heap spraying: A technique used to facilitate arbitrary code execution by injecting a certain sequence of bytes into the memory of a target process.
HIPAA: See Health Insurance Portability and Accountability Act (HIPAA).
indicator of compromise (IOC): A network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.
initialization vector (IV): A random number used only once in a session, in conjunction with an encryption key, to protect data confidentiality. Also known as a nonce.
IOC: See indicator of compromise (IOC).
IV: See initialization vector (IV).
jailbreaking: Hacking an Apple® iOS device to gain root-level access to the device. This is sometimes done by end users to allow them to download and install mobile apps without paying for them, from sources, other than the App Store®, that are not sanctioned and/or controlled by Apple®. Jailbreaking bypasses the security features of the device by replacing the firmware's operating system with a similar, albeit counterfeit version, which makes it vulnerable to malware and exploits. See also *rooting*.
least privilege: A network security principle in which only the permission or access rights necessary to perform an authorized task are granted.
malware: Malicious software or code that typically damages, takes control of, or collects information from an infected endpoint. Malware broadly includes viruses, worms, Trojan horses (including Remote Access Trojans, or RATs), anti-AV, logic bombs, backdoors, rootkits, bootkits, spyware, and (to a lesser extent) adware.
master boot record (MBR): Contains information about how the logical partitions (or file systems) are organized on the storage media, and an executable boot loader that starts up the installed operating system.
MBR: See master boot record (MBR).

metamorphism: A programming technique used to alter malware code with every iteration, to avoid detection by signature-based anti-malware software. Although the malware payload changes with each iteration – for example, by using a different code structure or sequence, or inserting garbage code to change the file size – the fundamental behavior of the malware payload remains unchanged.
Metamorphism uses more advanced techniques than polymorphism. See also *polymorphism*.
Microsoft® Challenge-handshake authentication protocol (MS-CHAP): A protocol used to authenticate

©2016-2019, Palo Alto Networks, Inc.

Microsoft® Windows®-based workstation, using a challenge-response mechanism to authenticate PPTP connections without sending passwords.

MS-CHAP: See Microsoft® Challenge-handshake authentication protocol (MS-CHAP).

mutex: A program object that allows multiple program threads to share the same resource, such as file access, but not simultaneously.

NERC: See North American Electric Reliability Corporation (NERC).

Network and Information Security (NIS) Directive: A European Union (EU) directive that imposes network and information security requirements – to be enacted by national laws across the EU within two years of adoption in 2016 – for banks, energy companies, healthcare providers and digital service providers, among others.

NIS: See Network and Information Security (NIS) Directive.

nonce: See initialization vector (IV).

North American Electric Reliability Corporation (NERC): A not-for-profit international regulatory authority responsible for assuring the reliability of the bulk electric system (BES) in the continental U.S., Canada, and the northern portion of Baja California, Mexico. See also *bulk electric system (BES)* and *Critical Infrastructure Protection (CIP)*.

obfuscation: A programming technique used to render code unreadable. It can be implemented using a simple substitution cipher, such as an *exclusive or* (XOR) operation, or more sophisticated encryption algorithms, such as the *Advanced Encryption Standard* (AES). See also *Advanced Encryption Standard (AES)*, *exclusive or (XOR)*, and *packer*.

one-way (hash) function: A mathematical function that creates a unique representation (a hash value) of a larger set of data in a manner that is easy to compute in one direction (input to output), but not in the reverse direction (output to input). The hash function can't recover the original text from the hash value. However, an attacker could attempt to guess what the original text was and see if it produces a matching hash value.

open systems interconnection (OSI) reference model: Defines standard protocols for communication and interoperability using a layered approach in which data is passed from the highest layer (application) downward through each layer to the lowest layer (physical), then transmitted across the network to its destination, then passed upward from the lowest layer to the highest layer. See also *data encapsulation*.

OSI model: See open systems interconnection (OSI) reference model.

packer: A software tool that can be used to obfuscate code by compressing a malware program for delivery, then decompressing it in memory at run time. See also *obfuscation*.

packet capture (PCAP): A traffic intercept of data packets that can be used for analysis.

PAP: See password authentication protocol (PAP).

password authentication protocol (PAP): An authentication protocol used by PPP to validate users with an unencrypted password. See also *point-to-point protocol (PPP)*.

Payment Card Industry Data Security Standards (PCI DSS): A proprietary information security standard mandated and administered by the PCI Security Standards Council (SSC), and applicable to any organization that transmits, processes, or stores payment card (such as debit and credit cards) information. See also *PCI Security Standards Council (SSC)*.

PCAP: See packet capture (PCAP).

PCI: See Payment Card Industry Data Security Standards (PCI DSS).

PCI DSS: See Payment Card Industry Data Security Standards (PCI DSS).

PCI Security Standards Council (SSC): Comprised of Visa, MasterCard, American Express, Discover, and JCB, the SSC maintains, evolves, and promotes PCI DSS. See also *Payment Card Industry Data Security Standards (PCI DSS)*.

Personal Information Protection and Electronic Documents Act (PIPEDA): A Canadian privacy law that defines individual rights with respect to the privacy of their personal information, and governs how private sector organizations collect, use, and disclose personal information during business.

©2016-2019, Palo Alto Networks, Inc.

Personally Identifiable Information (PII): Defined by the U.S. National Institute of Standards and Technology (NIST) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity… and (2) any other information that is linked or linkable to an individual…."

PHI: See protected health information (PHI).

PII: See Personally Identifiable Information (PII).

PIPEDA: See Personal Information Protection and Electronic Documents Act (PIPEDA).

PKI: See public key infrastructure (PKI).

point-to-point protocol (PPP): A Layer 2 (data link) protocol layer used to establish a direct connection between two nodes.

polymorphism: A programming technique used to alter a part of malware code with every iteration, to avoid detection by signature-based anti-malware software. For example, an encryption key or decryption routine may change with every iteration, but the malware payload remains unchanged. See also *metamorphism*.

PPP: See point-to-point protocol (PPP).

pre-shared key (PSK): A shared secret, used in symmetric key cryptography which has been exchanged between two parties communicating over an encrypted channel.

promiscuous mode: Refers to Ethernet hardware used in computer networking, typically a network interface card (NIC), that receives all traffic on a network segment, even if the traffic is not addressed to the hardware.

protected health information (PHI): Defined by HIPAA as information about an individual's health status, provision of healthcare, or payment for healthcare that includes identifiers such as names, geographic identifiers (smaller than a state), dates, phone and fax numbers, email addresses, Social Security numbers, medical record numbers, or photographs, among others. See also *Health Insurance Portability and Accountability Act (HIPAA)*.

public key infrastructure (PKI): A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.

QoS: See quality of service (QoS).

quality of service (QoS): The overall performance of specific applications or services on a network including error rate, bit rate, throughput, transmission delay, availability, jitter, etc. QoS policies can be configured on certain network and security devices to prioritize certain traffic, such as voice or video, over other, less performance-intensive traffic, such as file transfers.

RADIUS: See Remote Authentication Dial-In User Service (RADIUS).

rainbow table: A pre-computed table used to find the original value of a cryptographic hash function.

Remote Authentication Dial-In User Service (RADIUS): A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize access to a system or service.

remote procedure call (RPC): An inter-process communication (IPC) protocol that enables an application to be run on a different computer or network, rather than the local computer on which it is installed.

representational state transfer (REST): An architectural programming style that typically runs over HTTP, and is commonly used for mobile apps, social networking websites, and mashup tools.

REST: See representational state transfer (REST).

rooting: The Google Android equivalent of jailbreaking. See *jailbreaking*.

RPC: See remote procedure call (RPC)**. SaaS:** See Software as a Service (SaaS).

salt: Randomly generated data that is used as an additional input to a one-way has function that hashes a password or passphrase. The same original text hashed with different salts results in different hash values.

Sarbanes-Oxley (SOX) Act: A U.S. law that increases financial governance and accountability in publicly traded companies.

script kiddie: Someone with limited hacking and/or programming skills that uses malicious programs (malware) written by others to attack a computer or network.

©2016-2019, Palo Alto Networks, Inc.

Secure Sockets Layer (SSL): A cryptographic protocol for managing authentication and encrypted communication between a client and server to protect the confidentiality and integrity of data exchanged in the session.

service set identifier (SSID): A case sensitive, 32-character alphanumeric identifier that uniquely identifies a Wi-Fi network.

Software as a Service (SaaS): A cloud computing service model, defined by the U.S. National Institute of Standards and Technology (NIST), in which "the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

SOX: See Sarbanes-Oxley (SOX) Act.

spear phishing: A highly targeted phishing attack that uses specific information about the target to make the phishing attempt appear legitimate.

SSID: See service set identifier (SSID).

SSL: See Secure Sockets Layer (SSL).

STIX: See structured threat information expression (STIX).

structured threat information expression (STIX): An XML format for conveying data about cybersecurity threats in a standardized format. See also *extensible markup language (XML)*.

threat vector: See *attack vector.*

TLS: See Transport Layer Security (TLS).

Tor ("The Onion Router"): Software that enables anonymous communication over the internet.

Transport Layer Security (TLS): The successor to SSL (although it is still commonly referred to as SSL). See also *Secure Sockets Layer (SSL)*.

uniform resource locator (URL): A unique reference (or address) to an internet resource, such as a webpage.

URL: See uniform resource locator (URL).

vulnerability: A bug or flaw that exists in a system or software, and creates a security risk.

Web 2.0: A term popularized by Tim O'Reilly and Dale Dougherty, unofficially referring to a new era of the World Wide Web, which is characterized by dynamic or user-generated content, interaction, and collaboration, and the growth of social media. See also *Enterprise 2.0*.

XML: See extensible markup language (XML).

XOR: See exclusive or (XOR).

zero-day threat: The window of vulnerability that exists from the time a new (unknown) threat is released until security vendors release a signature file or security patch for the threat.

zombie: See *bot*.

©2016-2019, Palo Alto Networks, Inc.

Continuing Your Learning Journey with Palo Alto Networks

Training from Palo Alto Networks and our Authorized Training Centers delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Palo Alto Networks Security Operating Platform knowledge necessary to prevent successful cyberattacks and to safely enable applications.

Digital Learning

For those of you who want to keep up-to-date on our technology, a learning library of *free* digital learning is available. These on-demand, self-paced digital learning classes are a helpful way to reinforce the key information for those who have been to the formal hands-on classes. They also serve as a useful overview and introduction to working with our technology for those unable to travel to a hands-on, instructor-led class.

Simply register in our Learning Center and you will be given access to our digital learning portfolio. These online classes cover foundational material and contain narrated slides, knowledge checks, and, where applicable, demos for you to access.

New courses are being added often, so check back to see new curriculum available.

Instructor-Led Training

Looking for a hands-on, instructor-led course in your area?

Palo Alto Networks Authorized Training Centers (ATCs) are located globally and offer a breadth of solutions from onsite training to public, open environment classes. There are about 38 authorized training centers at more than 80 locations worldwide. For class schedule, location, and training offerings see https://www.paloaltonetworks.com/services/education/atc-locations.

Learning Through the Community

You also can learn from peers and other experts in the field. Check out our communities' site https://live.paloaltonetworks.com, where you can:

- Discover reference material
- Learn best practices
- Learn what is trending

©2016-2019, Palo Alto Networks, Inc.