PALO ALTO NETWORKS PCNSE STUDY GUIDE

July 2018

Palo Alto Networks, Inc. www.paloaltonetworks.com

Contents

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 Palo Alto Networks next-generation firewall PAN-OS® 8.1 platform in any environment. This exam will *not* cover Aperture and Traps.

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

You should have three to five years' experience working in the Networking or Security industries and the equivalent of 6 months' experience working full-time with Palo Alto Networks Security Operating Platform.

You have at least one year of experience in Palo Alto Networks NGFW deployment and configuration.

Skills Required

- You can plan, deploy, configure, 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 e-Learning courses:

- Firewall Essentials: Configuration and Management (EDU-210) or e-Learning (EDU-110)
- Panorama: Managing Firewalls at Scale (EDU-220) or e-Learning (EDU-120)
- Optional training: Firewall: Debug and Troubleshoot (EDU-311)

When 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
- Prep 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 uses the resources and courses recommended in this guide where needed to gain that understanding.

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 8.1	
Domain	Weight (%)
Plan	16%
Deploy and Configure	23%
Operate	20%
Configuration Troubleshooting	18%
Core Concepts	23%
Total	100%

Exam Domain 1 – Plan

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

Preventing Successful Cyber-attacks

Palo Alto Networks® Security Operating Platform prevents successful cyberattacks by harnessing analytics to automate routine tasks and enforcement. Tight integration across the platform, and with partners, simplifies security so you can secure users, applications and data.

Operate efficiently to stop attacks that cause business disruption

The Security Operating Platform empowers you to confidently automate threat identification and enforcement across cloud, network and endpoints using data-driven approach and precise analytics. It blocks exploits, ransomware, malware, and fileless attacks to minimize infected endpoints and servers. The platform lets you easily adopt best practices and take a Zero Trust approach to reducing opportunities for attack.

Automate routine tasks to reduce response time and speed deployments

Chances are good that your operations teams and analysts are overburdened. The Security Operating Platform improves productivity – and lets them focus on higher value activities – using automation. Shared intelligence and consistent enforcement across network, cloud and endpoints strengthens prevention and speeds response. DevOps can speed multi-cloud deployment and simplify management through deep integrations with native cloud services and automation tools. Plus, your teams can continuously validate compliance of cloud deployments with customizable reports and controls that save time.

Improve security effectiveness and efficiency with tightly integrated innovations

Threats are dynamic. You need to keep evolving to stay ahead. New capabilities are tightly integrated, building on the value of what you already have. With Palo Alto Networks Application Framework, you can quickly consume innovative security apps, using your existing security data, sensors and enforcement points. Whether developed by us, our ecosystem of third parties or your own teams, these apps can detect and report on threats, or automate enforcement workflows, to reduce response time. This way, the Security Operating Platform enables you to get the most out of your existing Palo Alto Networks investment.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform consist of the following components:

Network Security
Our next-generation firewalls secure your business with a prevention-focused architecture and integrated innovations that are easy to deploy and use. Now, you can accelerate growth and eliminate risks at the same time.

- *Next-generation firewalls*

Advanced Endpoint Protection
Traps™ advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks.

- *Traps*

Cloud Security
Palo Alto Networks provides advanced protection for consistent security across all major clouds – Amazon® Web Services, Microsoft® Azure® and Google® Cloud Platform – and our automation features minimize the friction of app development and security. You can protect and segment applications, deliver continuous security and compliance, and achieve zero-day prevention. Cloud Security is delivered by:

- *VM-Series firewalls*
- *Evident*: The unique combination of continuous monitoring, cloud storage protection, and compliance validation and reporting will solve one of the most critical challenges in moving to public cloud.
- *Traps*

Cloud-Delivered Security Services
Our security subscriptions allow you to safely enable applications, users, and content by adding natively integrated protection from known and unknown threats both on and off the network.

These security subscriptions are purpose-built to share context and prevent threats at every stage of an attack, allowing you to enable singular policies and automated protection that secure your network and remote workforce while simplifying management and enabling your business. The Security Services consist

of:

- *AutoFocus* - The AutoFocus threat intelligence service enables security teams to prioritize their response to unique, targeted attacks and gain the intelligence, analytics and context needed to protect your organization. It provides context around an attack spotted in your traffic and threat logs, such as the malware family, campaign, or malicious actor targeting your organization. AutoFocus correlates and gains intelligence from:
    - WildFire® service – the industry's largest threat analysis environment
    - PAN-DB URL filtering service
    - MineMeld application for AutoFocus, enabling aggregation and correlation of any third-party threat intelligence source directly in AutoFocus
    - Traps advanced endpoint protection
    - Aperture SaaS-protection service
    - Unit 42 threat intelligence and research team
    - Intelligence from technology partners
    - Palo Alto Networks global passive DNS network
- *GlobalProtect* Secure Mobile Workforce - GlobalProtect cloud service reduces the operational burden associated with securing your remote networks and mobile users by leveraging a cloud-based security infrastructure managed by Palo Alto Networks. Based on the Palo Alto Networks Security Operating Platform, administrators can manage GlobalProtect cloud service with Panorama to create and deploy consistent security policies for all remote networks and mobile users. The GlobalProtect cloud service shared ownership model allows you to move your remote networks and mobile user security expenditures to a more efficient and predictable OPEX-based model.
- *URL Filtering Web Security* – A firewall subscription/license. Most attacks and exposure to malicious content occurs during the normal course of web browsing activities, which requires the ability to allow safe, secure web access for all users. URL Filtering with PAN-DB automatically prevents attacks that leverage the web as an attack vector, including phishing links in emails, phishing sites, HTTP-based command and control, malicious sites and pages that carry exploit kits.
- *Threat Prevention* – A firewall subscription/license. Threat Prevention leverages the visibility of our next-generation firewall to inspect all traffic, automatically preventing known threats, regardless of port, protocol or SSL encryption. Provides protection details for malware, vulnerability and spyware attacks.
- *WildFire® Malware Analysis* – Primary features available at no cost to firewalls. Advanced features available as a firewall subscription/license. Files being sent through the firewall can be evaluated by WildFire® for zero-day malware. WildFire® cloud-based threat analysis service is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The cloud-based service employs a unique multi-technique approach combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.
- *MineMeld Threat Intelligence Sharing* – An open-source application that streamlines the aggregation, enforcement and sharing of threat intelligence. MineMeld allows you to aggregate threat intelligence across public, private and commercial intelligence sources, including between government and commercial organizations. MineMeld natively integrates with Palo Alto Networks Security Operating Platforms to automatically create new prevention-based controls for URLs, IPs and domain intelligence derived from all sources feeding into the tool.
- *Logging Service* – Palo Alto Networks Logging Service is a cloud-based offering for context-rich enhanced network logs generated by our security offerings, including those of our next-generation firewalls and GlobalProtect cloud service. The cloud-based nature of the Logging Service allows customers to collect ever expanding rates of data, without needing to plan for local compute and storage.

  The Logging Service is the cornerstone of Palo Alto Networks Application Framework, which provides

a scalable ecosystem of security applications that can apply advanced analytics in concert with Palo Alto Networks enforcement points to prevent the most advanced attacks. You are no longer limited by how much hardware is available nor by how quickly the sensors can be deployed.

- *Magnifier Behavioral Analytics* – Magnifier behavioral analytics applies machine learning at cloud scale to rich network, endpoint and cloud data, so you can quickly find and stop targeted attacks, insider abuse and compromised endpoints. It is an application that uses the Application Framework and customer logging data stored by the Logging Service.

Application Framework

With the Palo Alto Networks Application Framework, we are ushering in the future of security innovation, reinventing how customers rapidly access, evaluate and adopt the most compelling new security technologies as an extension of the next-generation Security Operating Platform they already own and operate. The all-new framework is a culmination of over a decade of security disruption, providing customers with superior security through compelling cloud-based apps developed by Palo Alto Networks and today's most innovative security providers, large and small.

The Application Framework consists of the following parts:

- *Infrastructure* - A suite of cloud APIs, services, compute and native access to customer-specific data stores.
- *Customer-specific data store* - Palo Alto Networks Logging Service
- *Apps* – Are delivered from the cloud to extend the capabilities of the platform, including the ability to effortlessly collaborate between different apps, share threat context and intelligence, and drive automated response and enforcement.

Platform Integration

The Security Operating Platform's power often lies in the integration of services with their collective analytical capabilities. A next-generation firewall can directly integrate with several parts of the platform. WildFire®, and URL filtering are the most common. Greater levels of protection are available with other platform components. AutoFocus will add context to threat detected by your firewalls. Detected threats can now be characterized as a narrowly focused attack on your organization or part of a larger, non-targeted threat. This information supports a more informed priority decision about the allocation of finite remediation resources.

Applications implemented within the Application Framework can provide different, specialized analysis of data supplied by deployed firewall and Traps agents. The Logging Service provides the "Big Data" base of information these applications analyze. When a next-generation firewall is connected to the logging service an even greater depth of detail is supplied supporting a higher level of analysis. Magnifier is an example of an Application Framework application that analyses this data to find targeted attacks that would be harder to discern from individual firewall log analysis. This "Data Lake" is accessible through Application Framework APIs for any authorized application to evaluate providing an opportunity for complimentary product support.

Generally speaking, an approach that provides the maximum visibility of analyzed traffic and events, backed up with analysis to support the identification of target attacks enables the highest level of responsiveness to an organization's security teams.

In keeping with this approach, one might deploy Traps or a next-generation firewall as a standalone product initially utilizing their specific platform product support options and integrate other platform services over time. As more firewalls are implemented the integration of their logs in the Logging Service

creates an organization-wide set of enriched data that threat detection services can analyze to give you specific information on detected attacks and prescribe specific remediation.

Sample questions

1. Which component (or components) of the integrated Palo Alto Networks security solution limits access to a corporate z/OS (also known as MVS) mainframe?
    A. threat intelligence cloud
    B. advanced endpoint protection
    C. next-generation firewall
    D. advanced endpoint protection and next-generation firewall
2. Which Palo Alto Networks product is primarily designed to provide context with deeper information about attacks?
    A. MineMeld
    B. WildFire®
    C. AutoFocus
    D. Threat Prevention
3. Which Palo Alto Networks product is primarily designed 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 primarily designed to protect endpoints from successful Cyber-attacks?
    A. Global Protect
    B. Magnifier
    C. Traps
    D. Evident
5. The Palo Alto Networks Logging Service can accept logging data from which two products? (Choose two.)
    A. Traps
    B. next-generation firewalls
    C. Aperture
    D. MineMeld
    E. AutoFocus

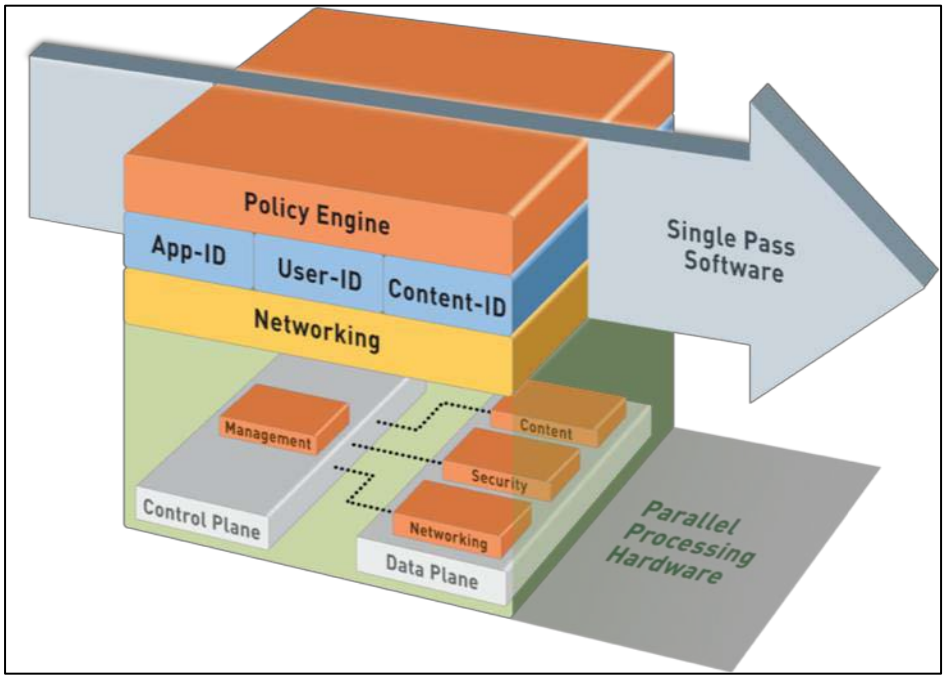
Given a scenario, identify how to design an implementation of the firewall to meet business requirements leveraging the Palo Alto Networks Security Operating Platform.

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 a much a selection of functions and services that drive proper sizing decisions to meet your needs.

The following link provides a features summary of all firewall models including throughput:
https://www.paloaltonetworks.com/resources/datasheets/product-summary-specsheet



The Single Pass Architecture means packets traverse the architecture only once

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

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

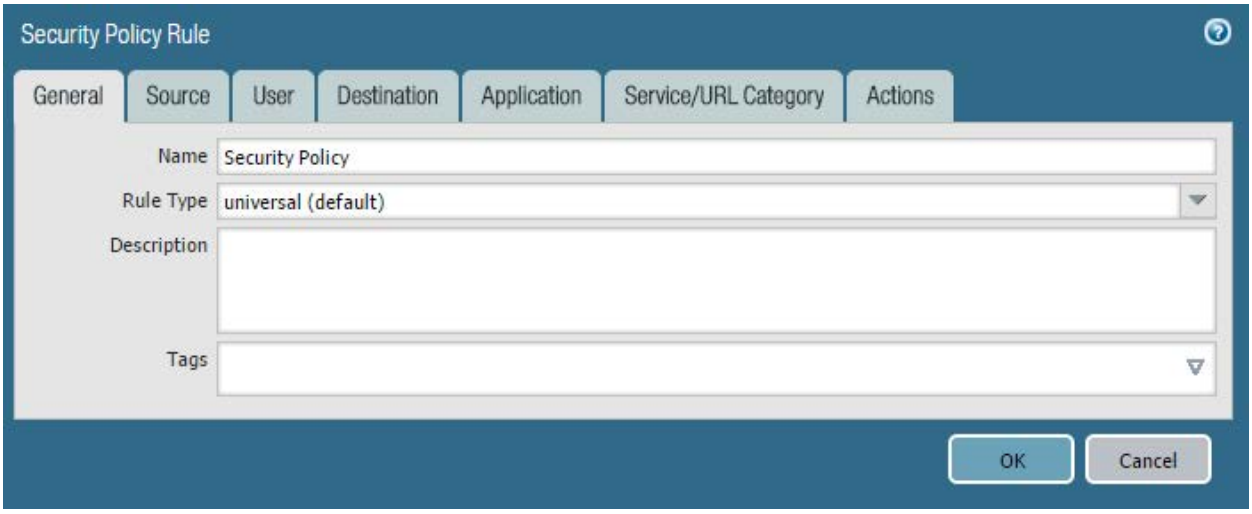
- App-ID: Scanning of traffic to identify the application that is involved, regardless of the protocol or port number used.
- Content-ID: Scanning of traffic for security threats (e.g., data leak prevention and URL filtering. virus, spyware, unwanted file transfers, specific data patterns, vulnerability 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

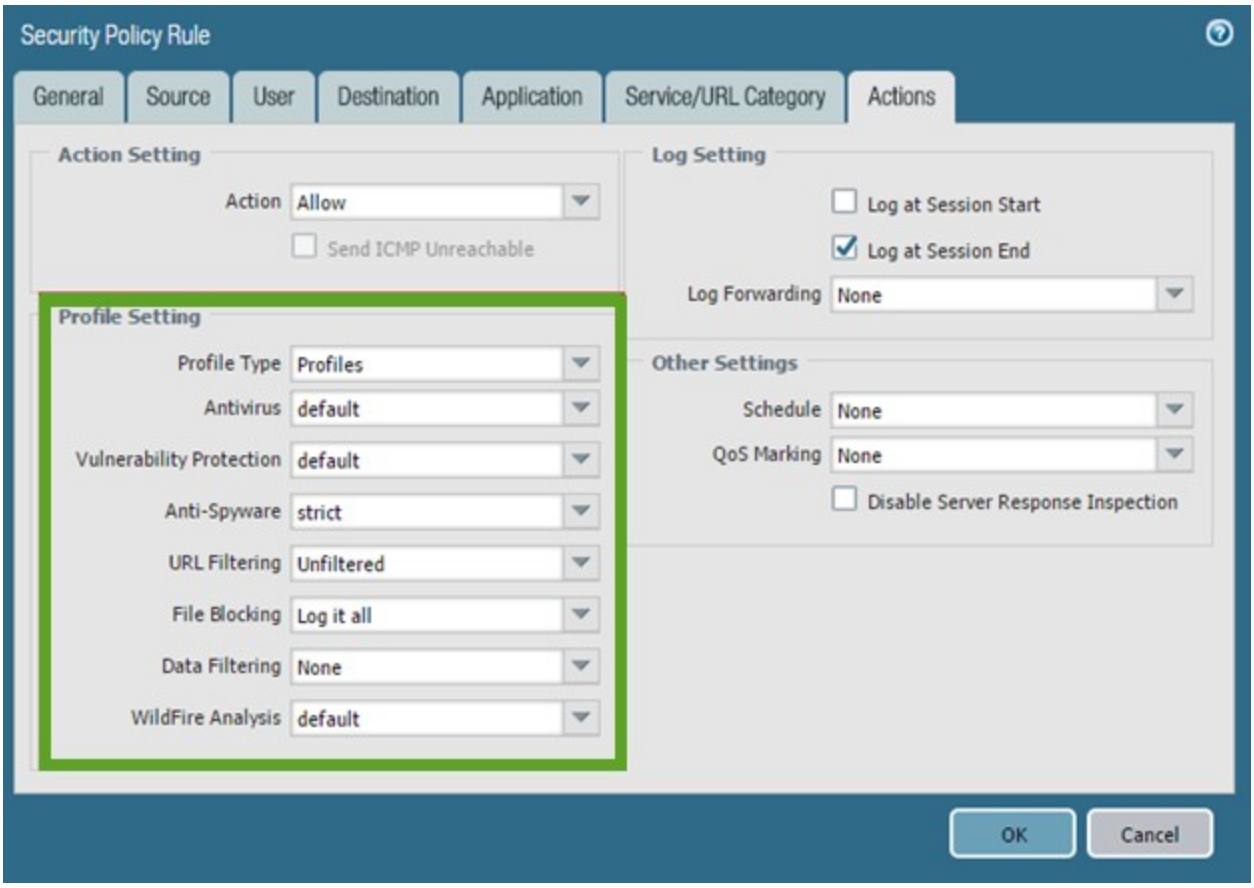
The Security policy consists of security rules that are the basis of the firewall’s ability to enable or block sessions. Multiple match conditions can be used when you create these rules. Security zones, source and destination IP address, application (App-ID), source user (User-ID), service (port), HIP match, and URL categories in the case of web traffic all can serve as traffic matching criteria for allow/block decision-making. 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 security rules and profile settings follow:



Creating a Security policy rule



Profile settings for a Security policy rule that enable Content-ID threat scanning

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, 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/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 only be assigned to one zone.

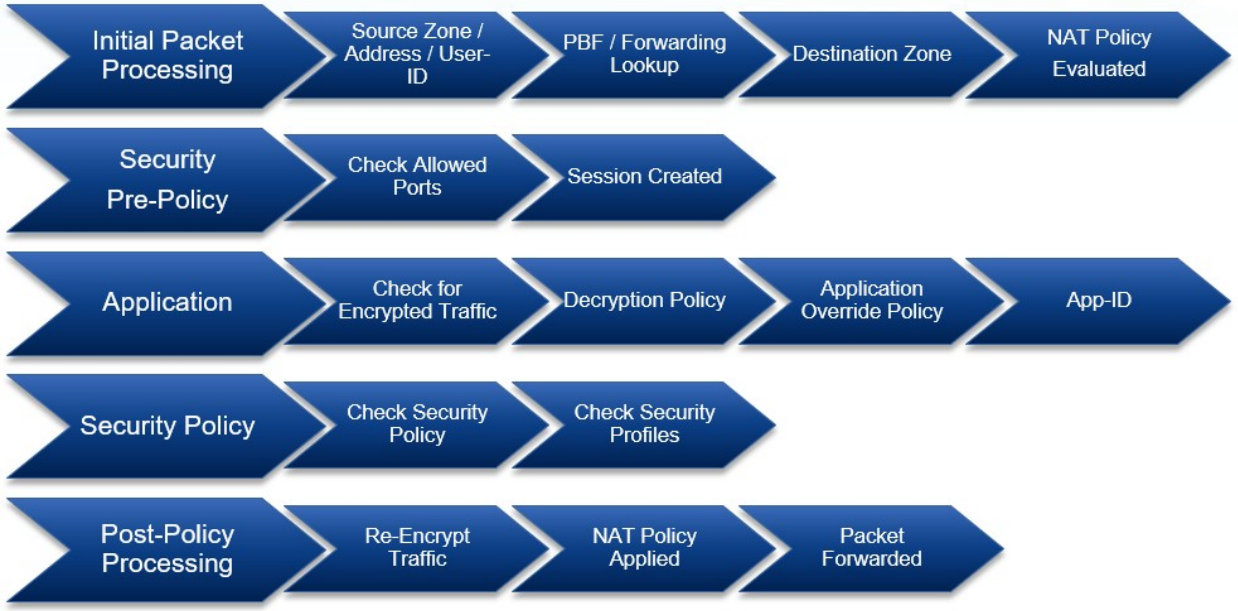
All sessions on the firewall are defined by the source and destination zones. Rules can use these defined zones to allow or deny traffic, apply QoS, or perform NAT. All traffic can flow freely within a zone and is referred to as *intrazone* traffic. Traffic between zones (called interzone traffic) is 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. The necessary security rules must be in place for the firewall to properly evaluate, configure, and maintain Security policies. 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 can be used to characterize traffic, providing specific use information and allowing precise policy creation and control. Log entries can be forwarded to external monitoring devices like Panorama, the Logging Service 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

Visualize the Palo Alto Networks firewall processes using the following graphical representation. Understanding 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.
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081



Session processing sequence

Enterprise Firewall Management

Palo Alto next-generation firewalls are managed individually and have no native ability to be managed as a whole. In these cases, it is an administrative responsibility to keep multiple firewalls' settings coordinated.

Panorama is the Palo Alto Networks enterprise management solution. Once Panorama and firewalls are linked, Panorama is the single interface to manage the entire enterprise.

Additional information on best practices in designing and deploying your Security policy when deploying as an edge device can be found here:
https://www.paloaltonetworks.com/documentation/81/best-practices/best-practices-internet-gateway

Other deployment best practices can be found here:
https://www.paloaltonetworks.com/documentation/best-practices

Sample question

6. A potential customer says they need a firewall to process 50Gbps of traffic. Which firewall, if any, do you recommend to the customer?
   A. PA-7080
   B. PA-7050
   C. PA-5260
   D. You don't recommend a firewall model at this point. Ask about the kind of traffic and how it needs to be processed. If the requirement is for 50Gbps IPsec VPN throughput, then the customer needs a PA-7050. For 50Gbps with threat prevention, you need a PA-7050. If only App-ID is used, a PA-5260 can fulfill the requirement.

Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements leveraging 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 making sure that an alternate firewall is available in the event that the peer firewall fails. HA pairs are made up of two firewalls of identical model, configuration and licensing. It is preferred that they are in physical proximity of 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 management interface IP address or administrator profiles, HA specific configuration, log data, and the Application Command Center (ACC) information is not shared between peers. For 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 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPsec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover.
- The VM-Series firewall in AWS 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 not support HA.

Active/Passive Clusters

Active/passive HA is the recommended deployment method in nearly every case. One firewall actively manages traffic while the other is synchronized and ready to transition to the active state, should a failure occur. 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 and takes over seamlessly and enforces the same policies to maintain network security. The firewalls synchronize the session state table allowing the passive partner to step into 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 is usually 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 does not support DHCP client. Furthermore, only the active-primary firewall can function as a DHCP Relay. If the active-secondary firewall receives DHCP broadcast packets, it drops them.

Physical and virtual firewall interfaces have unique addresses but can also have floating IP addresses assigned allowing both firewalls to support the single address at failover.

Important information on Floating IP Addresses and Virtual MAC Addresses for the Active/Active configuration can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address#ida3676d14-7d84-4389-b042-2c9b69ed3411.

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.
- Active/passive mode supports a VWire deployment; active/active mode does not.
- 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, and deploying floating IP addresses to provide proper failover. Because both firewalls are actively 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 are actively processing traffic.
- In active/active mode, the HA pair can be used to temporarily process more traffic than what one firewall can normally handle. However, this should not be the norm 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.

More details on designing an Active/Active cluster can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case

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), while 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 below.
- For firewalls without dedicated HA ports such as the PA-200, PA-220, PA-220R, and PA-500 firewalls, 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, implementing 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 on the purpose and setup of the HA links can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links#id1df2d565-1765-4666-83b0-87652318e06f

HA pair configuration synchronization is discussed here:
https://live.paloaltonetworks.com/t5/Learning-Articles/Information-Synchronized-in-an-HA-Pair/ta-p/57292

Sample questions

7. What would cause you to recommend an active/active cluster instead of an active/passive one?
    A. Active/action is the preferred solution when the firewall cluster is behind a load balancer that randomizes routing, requiring both firewalls to be active.
    B. Active/active is the preferred solution in most cases, because it allows for more bandwidth while both firewalls are up. Active/passive is available only for backward compatibility.

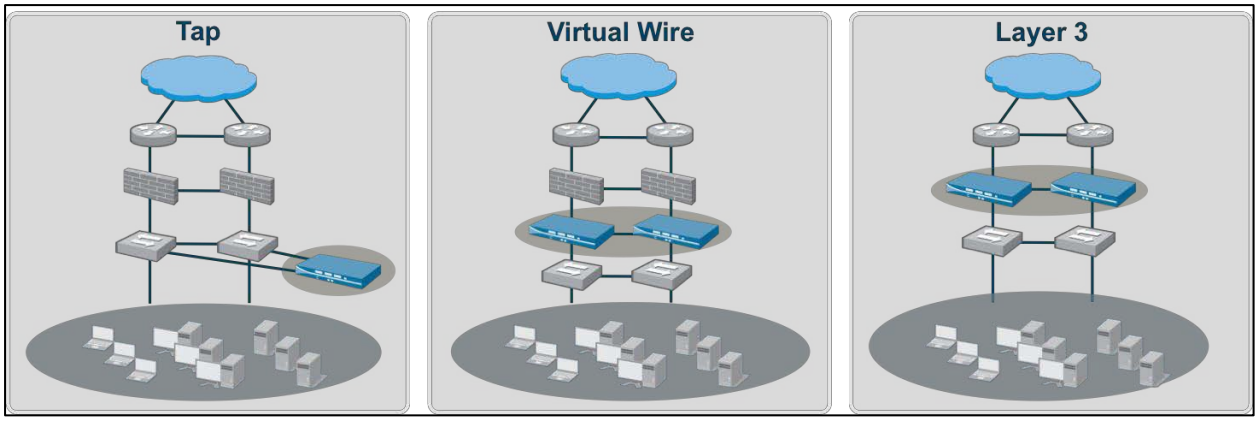
C. Active/active is the preferred solution when using the PA-7000 Series. When using the PA-5200 Series or smaller form factors, use active/passive.
D. Active/active is the preferred solution when using the PA-5200 Series or smaller form factors. When using the PA-7000 Series, use active/passive.

8. Which two of the following events can trigger an HA pair failover event? (Choose two.)
   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 destination address successfully
   D. OSPF implemented on the firewall determines an available route is now down
   E. RIP implemented on the firewall determines an available route is now down
9. Which of the following firewall models does not support active/passive HA pair?
   A. PA-200
   B. VM-Series in AWS
   C. VM-Series in Azure
   D. VM-Series in ESXi
10. 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
11. How do firewalls in an Active/Passive HA pair synchronize their configurations?
   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 and it automatically synchronizes with the other
   D. An administrator schedules an automatic sync frequency in the firewall configs

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

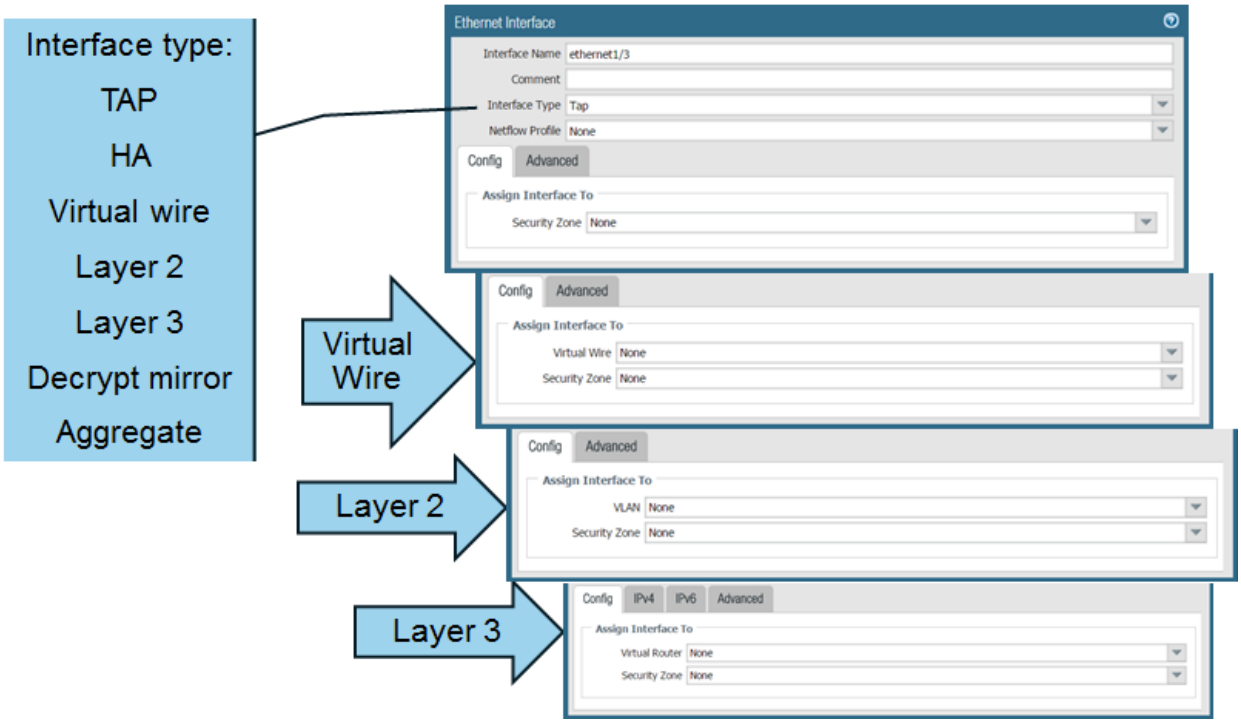
Types of Interfaces

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. A particular interface's configuration is chosen depending on functional need and existing network integration requirements. The following illustration shows the primary configuration options for integrating physical traffic ports. Layer 2 also is available but is not pictured.



Interface types are determined by functional needs.

The following screen capture shows primary configuration options for interfaces:



Possible interface configuration options to match your integration needs

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 key words and patterns that identify sensitive information.

Specific information is here:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-a-Decrypt-Mirror-Port-on-PAN-OS-6-0/ta-p/57440

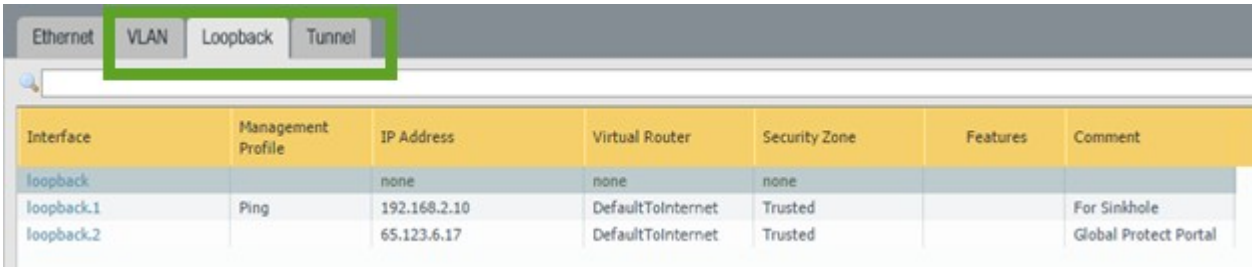
LACP Protocol / Aggregate Interfaces

Physical Layer 2 and 3 interfaces can be aggregated into single logical interfaces using the LACP protocol for multiplexing traffic.

Specific information is here:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-LACP/ta-p/65837

Virtual Interfaces

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



Loopback interfaces can be destination configs for DNS sinkholes and GlobalProtect service interfaces.

VLANs are logical interfaces specifically serving 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. This article is dated and has older WebUI screenshots, but the concepts are still current: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-a-Layer-2-to-Layer-3-Connection-on-the-Palo/ta-p/52787

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.

Tunnel Interfaces

Tunnel interfaces specifically serve VPN tunnels (both point to point and large-scale VPN solutions such as GlobalProtect) and are Layer 3 only. They serve as the entry and exit for traffic transiting a VPN tunnel. To configure a VPN tunnel, you must configure the Layer 3 interface at each end and 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. Each tunnel interface can have a maximum of 10 IPsec tunnels, which means that up to 10 networks can be associated with the same tunnel interface on the firewall. The encrypted tunnel traffic terminates on the VPN endpoint interface (an interface on the firewall) and cleartext traffic continues to the tunnel interface before it enters the routing environment of the firewall.

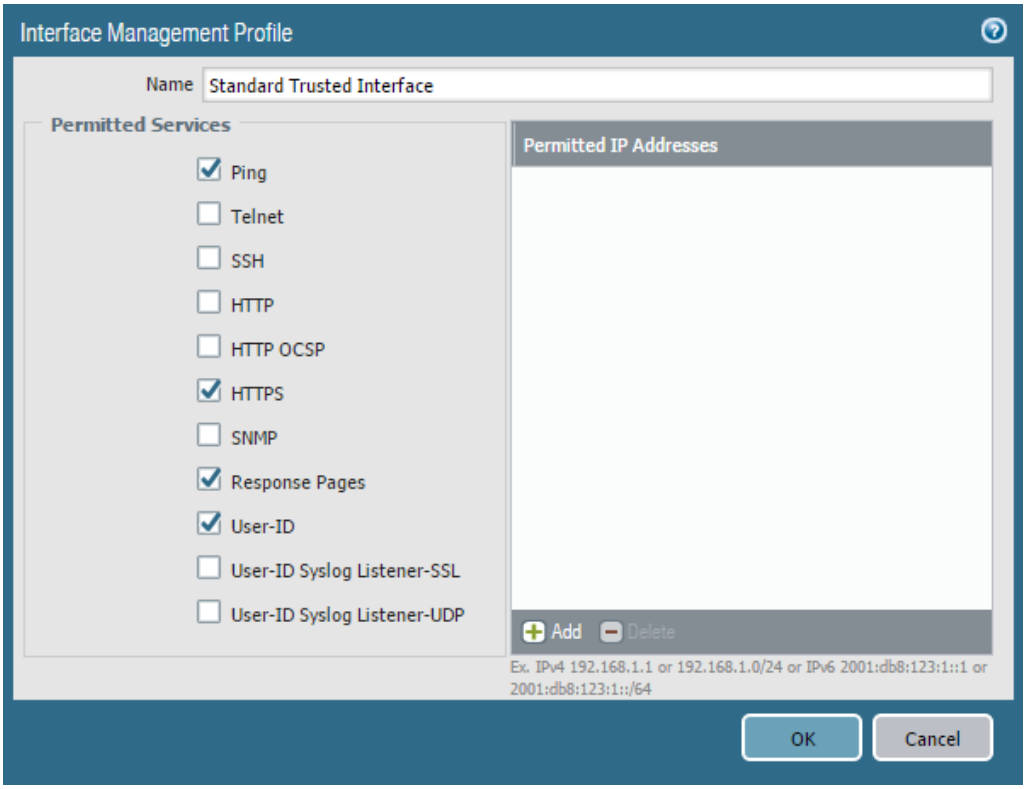
The tunnel interface must belong to a security zone to apply policy, and it must be assigned to a virtual router to use the existing routing infrastructure. Ensure that the tunnel interface and the physical interface are assigned to the same virtual router so that the firewall can perform a route lookup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

The Layer 3 interface to which the tunnel interface typically is attached 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 (for example, 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.

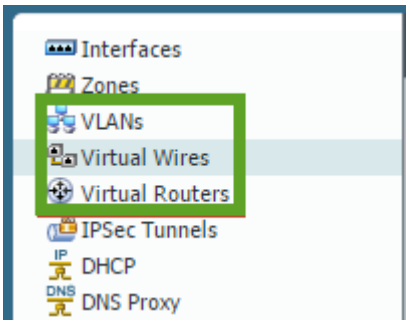
Interface Configurations

Each interface includes configurations for binding various services to them. HTTPS includes the WebUI service and should be included on at least one interface. The Permitted IP Addresses allow an Access Control List to be included, restricting access to any interface with this profile assigned.



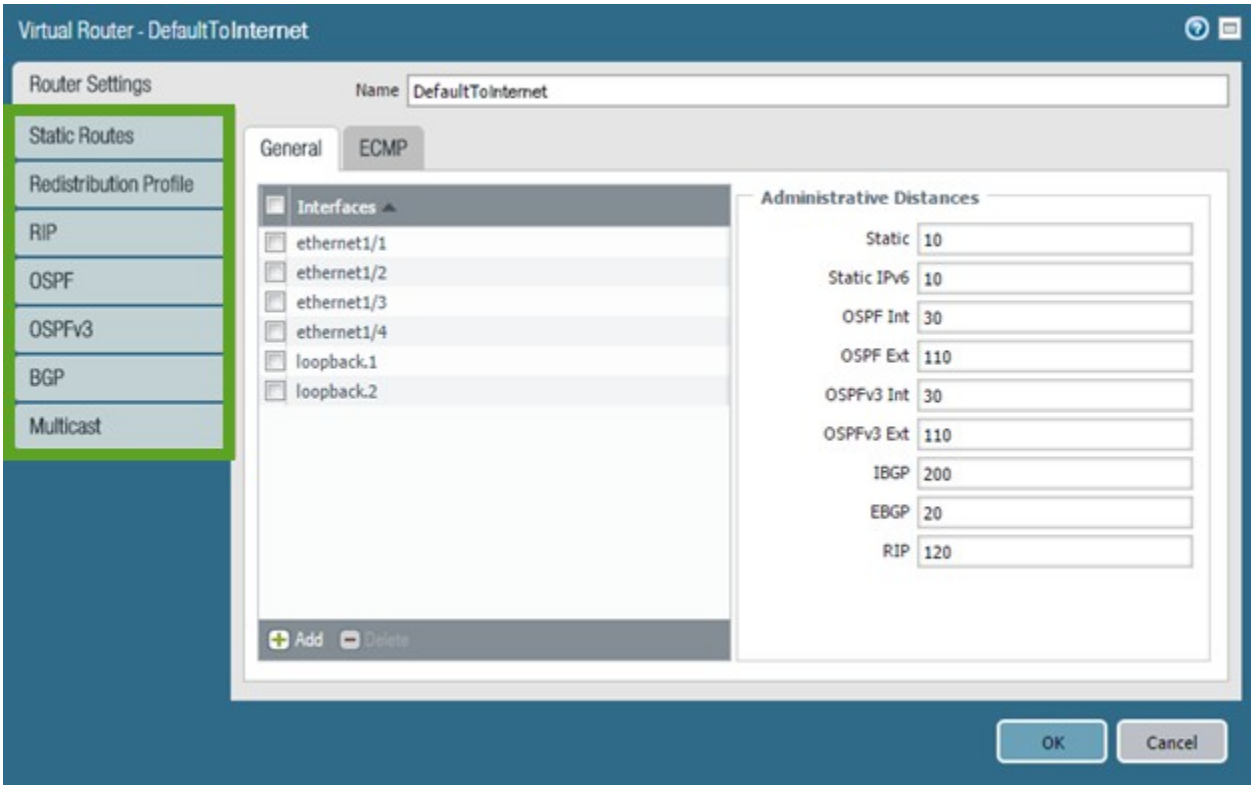
Protocol services and internal processes can be selectively bound to interfaces.

Palo Alto Networks firewalls provide several traffic-handling objects to move traffic between interfaces. The available types are: VLAN objects (VLANs) for Layer 2 traffic, virtual routers for Layer 3 traffic, and virtual wires for virtual wire interfaces.



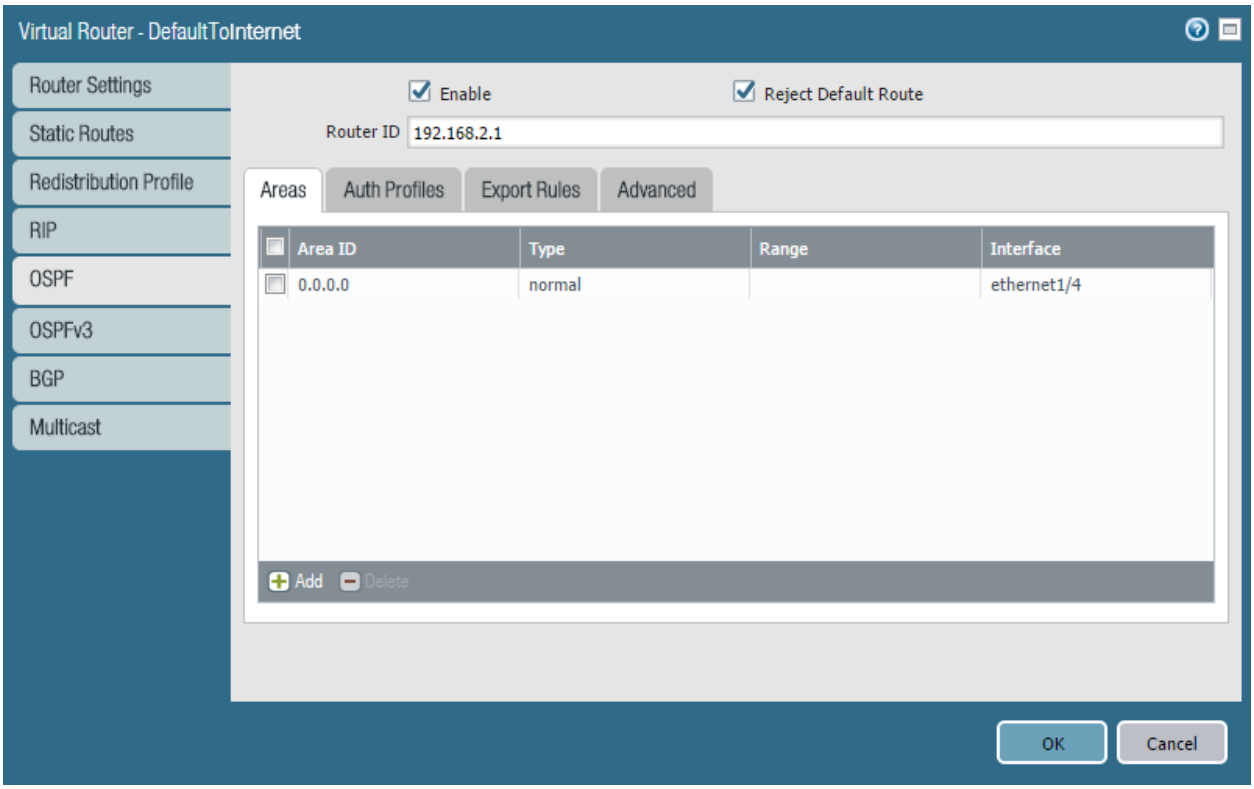
The available traffic-handling objects to move traffic from one interface to another

Simultaneous implementations of multiple 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.



Routing capabilities of a Layer 3 virtual router

Each Layer 3 dynamic routing protocol includes appropriate specific configuration options. An example of OSPFv2 follows.



An example of a dynamic routing configuration

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

References

- Network design (written for an older version of PAN-OS® software but still valid) https://live.paloaltonetworks.com/t5/Integration-Articles/Designing-Networks-with-Palo-Alto-Networks-Firewalls/ta-p/60868?attachment-id=1585
- Layer 2 interfaces https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Layer-2-Interfaces/ta-p/68229
- Layer 3 interfaces and related topics https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Layer-3-NAT-and-DHCP/ta-p/66999
- Layer 3 subinterfaces (VLAN tags) https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Layer-3-Subinterfaces/ta-p/67395
- Virtual wire interfaces
  Section 2 of https://live.paloaltonetworks.com/t5/Integration-Articles/Designing-Networks-with-Palo-Alto-Networks-Firewalls/ta-p/60868?attachment-id=1585

Sample questions

12. You want to put the NGFW in front of an existing firewall to begin providing better security while making the minimum required network changes. Which interface type to do you use?
    A. TAP
    B. Virtual Wire
    C. Layer 2
    D. Layer 3
13. Which kind of interface do you use to connect Layer 2 and Layer 3 interfaces?
    A. VLAN
    B. virtual router
    C. loopback
    D. tunnel
14. Which Dynamic Routing protocol cannot be configured on the firewall's virtual router(s)?
    A. RIP
    B. OSPF
    C. OSPFv3
    D. IGRP
    E. BGP
15. Which of the following are not compatible with Aggregate interface configuration?
    A. Aggregating 12, layer 3 interfaces together
    B. Aggregating 4, Virtual Wire interfaces together
    C. Using Aggregate interfaces in an HA pair
    D. 2 10Gps Optical and 2 10Gps copper ethernet ports aggregated together

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

Panorama Overview

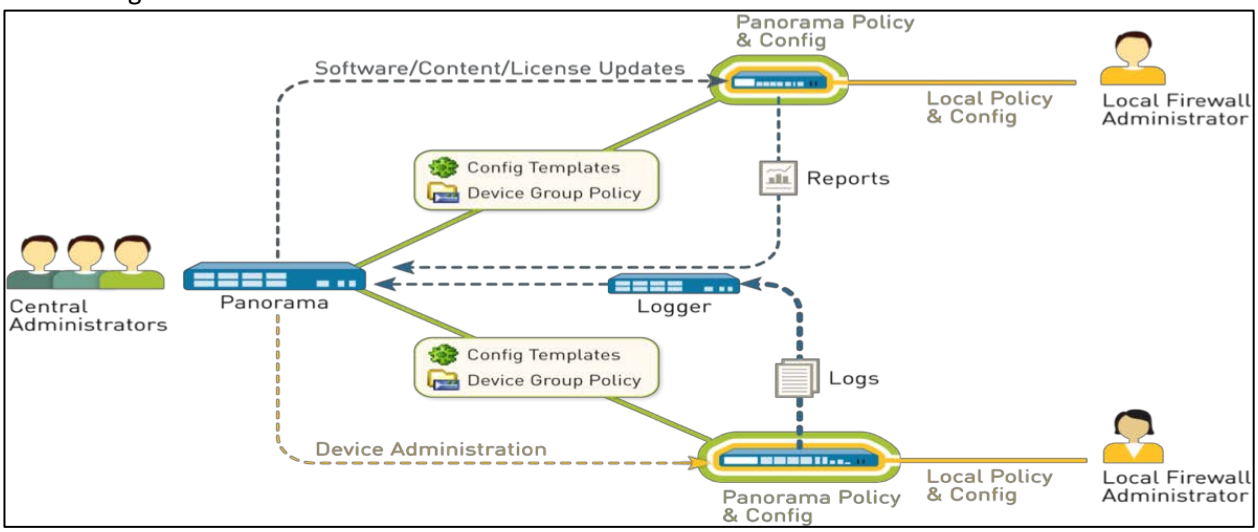
Without Panorama, Palo Alto Networks firewalls have no direct knowledge of each other and must be managed as independent entities. Panorama offers several important integration functions providing enterprise management for multiple firewalls.

Panorama is a separate Palo Alto Networks product supplied in either virtual or physical appliance form sized to match desired functions, number of firewalls, and level of firewall activity. Panorama should be implemented as a high availability cluster consisting of two identical platforms. Unlike firewalls, Panorama HA cluster members are often physically separated.

A functional overview of Panorama is here:
https://www.paloaltonetworks.com/products/management/panorama

A presentation of the different Panorama platforms and their capacities is here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/panorama-models

The following illustration outlines the main features of Panorama:



Panorama can provide centralized management, logging, reporting, software updates, and administrative control to multiple firewalls.

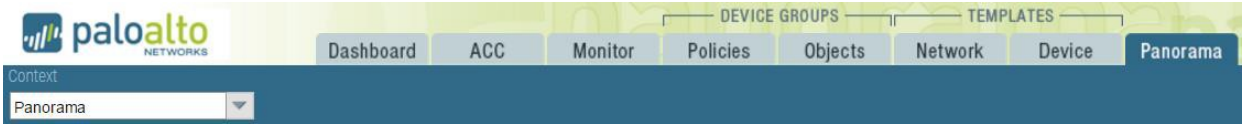
A brief description of these features can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/about-panorama#id52537f5d-4ddc-4701-b7e0-4d31476c2eb1

Log Aggregation

Log aggregation of events from firewalls to an enterprise-level log stored on Panorama requires specific design and scaling consideration. When log aggregation is implemented, copies of log events are forwarded from firewalls to Panorama as they are generated. Specific settings are created for each firewall that determine the specific event types to forward. This forwarding can be CPU- and disk-intensive on the Panorama platform and needs to be sized carefully. In high log volume situations, an intermediate level of log collecting servers can be implemented (Logger in the preceding diagram).

More discussion of this topic is here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/centralized-logging-and-reporting

Palo Alto Networks designed the Panorama WebUI to be as similar to the firewall WebUI as possible to simplify the transition to Panorama management. All menus (other than Panorama) are faithfully reproduced and mostly have identical menu options:



Top-level user interface for Panorama

Templates

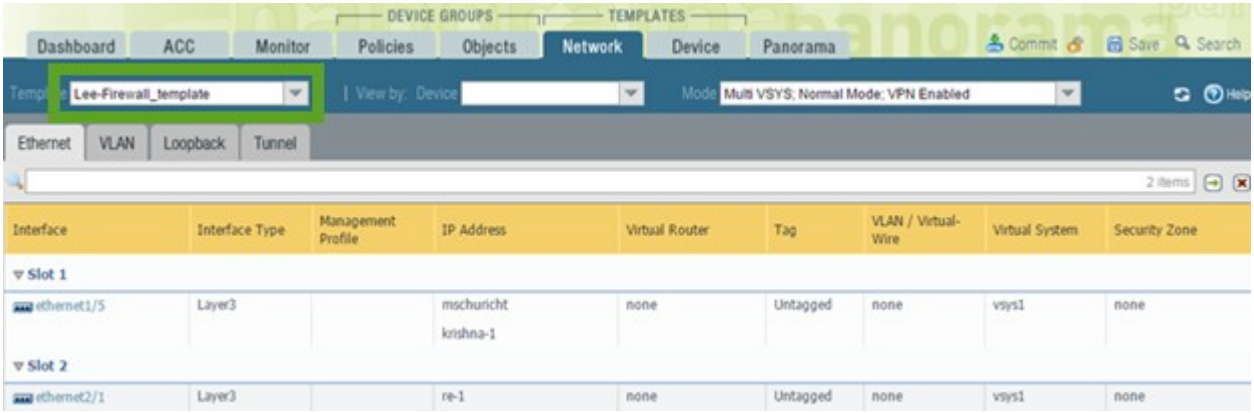
You use templates and template stacks to configure the settings that enable firewalls to operate on the network. Templates are the basic building blocks you use to configure the Network and Device tabs on

Panorama™. Template stacks give you the ability 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 give you the ability to layer templates to create a combined configuration. This enables you to define templates with location- 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.

Firewalls are assigned to template stacks. This link connects the template stack data with the specific firewalls and a particular template stack's data is pushed to its assigned firewalls with a Panorama push function.

Both templates and template stacks 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 you can override them to create a template stack variable specific to one or more firewalls. 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.

When defining 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. This enables you to avoid the redundancy of adding every setting to every template stack. 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.



Required device group object selection to receive network configuration settings

A firewall only can be assigned to one template stack at a time. The template stack can be an individual template or a collection of up to 16 individual templates.

An overview of Templates and Template Stacks can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks#id4ff18f85-9f4f-48fe-b6f9-e4b52a139d95

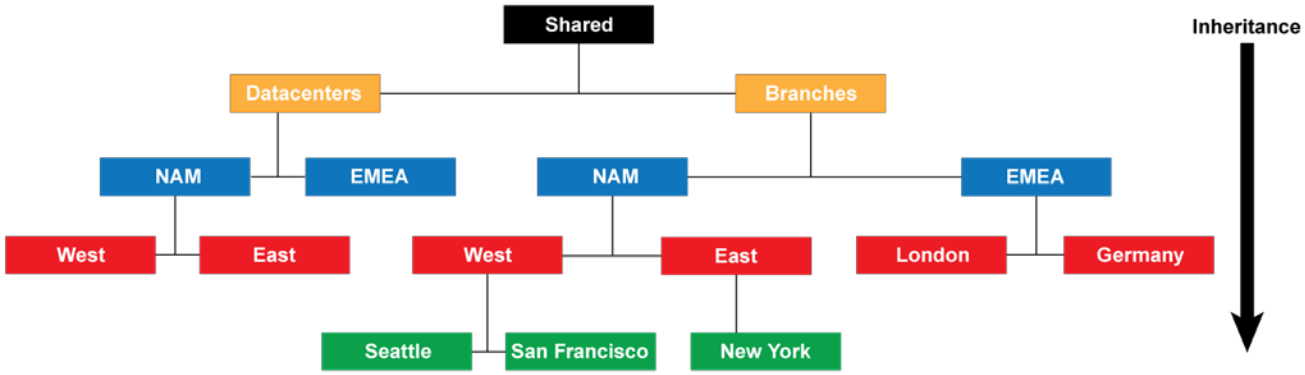
Sample questions

16. 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, can they share the same device group? Can they share the same template?
    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
17. A firewall is assigned to a Template stack of 2 templates. There is a common setting in each Template that has a different value. When Panorama pushes the template stack contents to the managed firewall which setting will the firewall receive?
    A. The value from the top template of the stack
    B. The value from the bottom template in the stack
    C. The value from the template designated as the Parent.
    D. The value an admin selects from the two available values.
18. 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
19. Which four firewall settings are stored in Panorama Templates? (Choose four.)
    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

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

Device Groups

Device Groups are Panorama objects used for storing firewall settings. Device Groups store settings found under the Policy and Objects tab of the firewall UI. Other than storing a different type of settings they behave like Templates except for the stacking concept. Device Groups are defined individually with their parent and ancestor device group specified at creation time for inheritance purposes. Instead of assigning firewalls to a stack they are assigned to an individual Device Group from which the firewall receives settings from it and all the others in a Parent relationship. Device Group inheritance always includes the pre-defined "Shared" group appearing in the senior position.



An example of Device Group inheritance

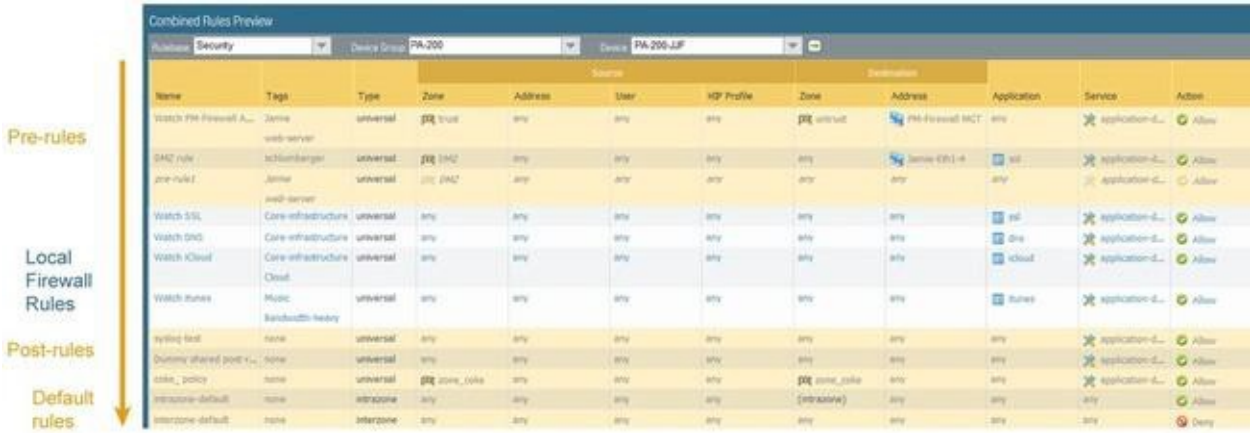
Information on Device Group design can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups#id72c6ff97-83c1-4aa8-a918-ea754a5a8887

A discussion of this hierarchy and inheritance can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy#id014f3417-fe14-4fdd-8fd7-c03ac8cb2e0b

Details about Device Groups and their use can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/manage-firewalls/manage-device-groups#id9b0560e8-e831-435e-a287-6a7970eae5d6

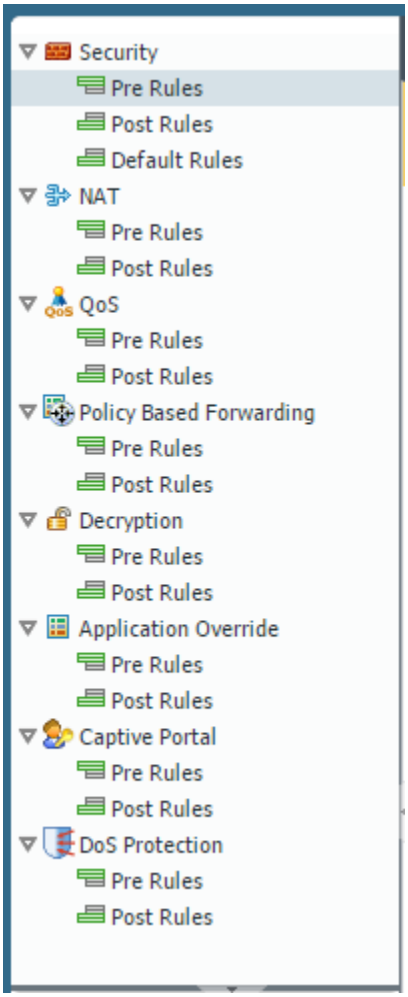
Configuration data from Panorama merges with the local firewall configuration (if any) at Panorama commit time. In the case of policies, the merged result is built from strict rules. Locally created firewall policies occupy the middle of the resulting list and Panorama-supplied policies occupy the top (Pre) or bottom (Post).

The Pre and Post designations are determined at policy creation time in Panorama by deliberately choosing the type during policy creation:



Panorama-supplied policies merge with local policies in this manner.

This image details options for Pre and Post position selections in Panorama



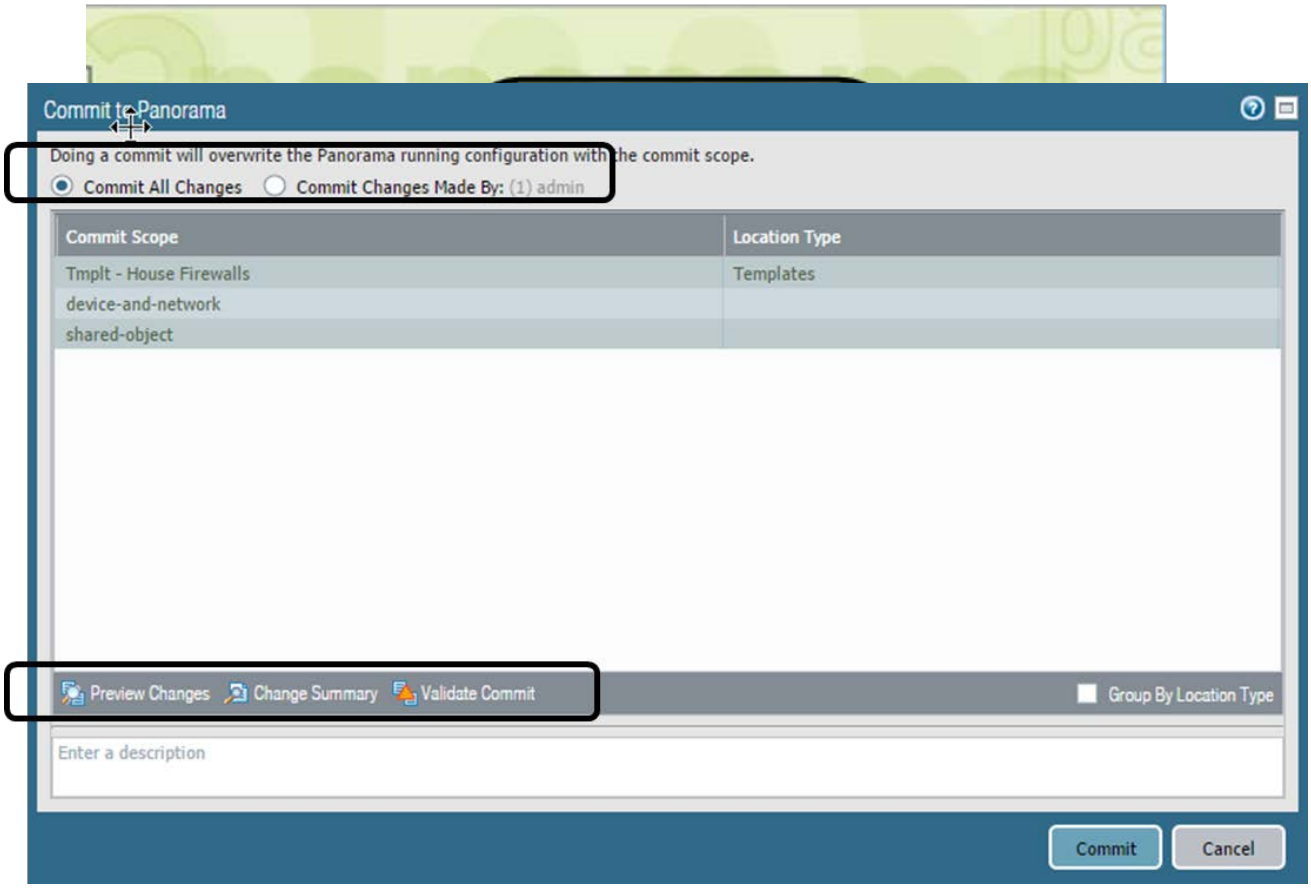
Panorama policy menu for Pre Rules and Post Rules

An administrator entering any information under the Panorama Policy or Objects tab *must* choose the Device Group to receive the settings. If settings are being entered into Policies a selection of pre-rules or post-rules must be made.

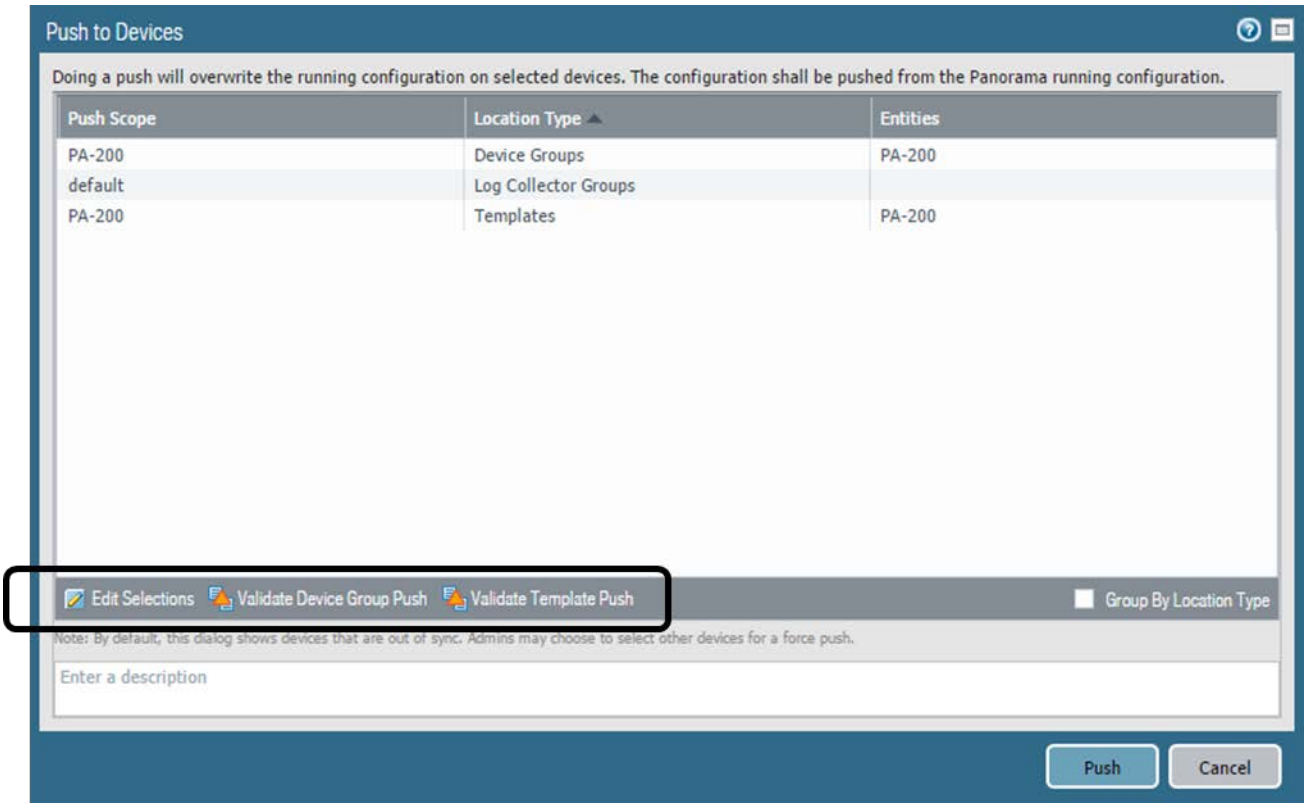
Committing Changes with Panorama

Panorama uses a similar Commit concept to firewalls but uses a process with multiple phases. When changes have been made in Panorama data it must first be committed to Panorama and then pushed to devices. Both of these processes provide methods to push partial data.

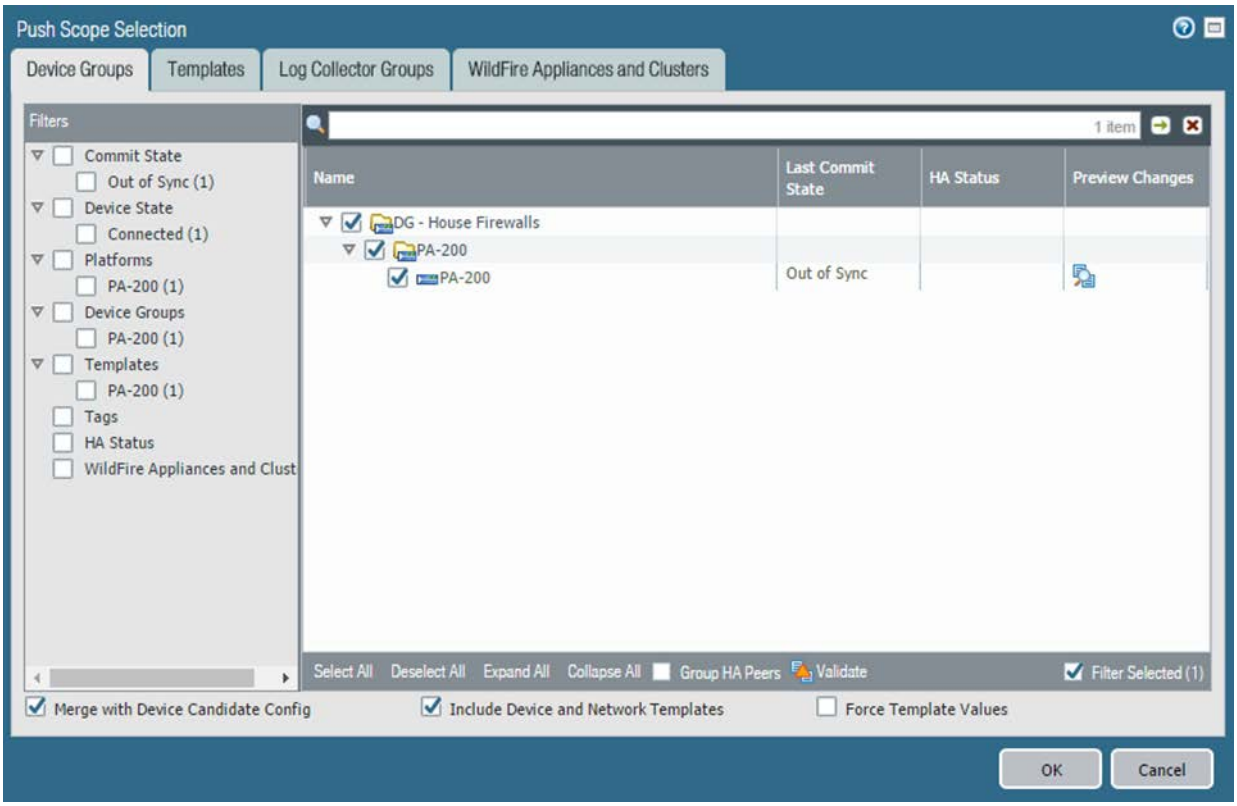
Committing to Panorama commits either the changes made by a chosen admin or all staged changes as illustrated below.



Once changes are committed to Panorama they are pushed to firewalls according to their assigned Device Groups and Template Stacks. This push process can either push all queued changes or be done selectively for specific Device Groups or Template Stacks. And specific firewalls can be chosen for the update.



Selecting the Edit Selections button at the bottom provides granular selection of the data to be pushed.



More information on the Commit and Push functions can be found here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/panorama-commit-validation-and-preview-operations#id1657d230-91b0-4ef0-99d2-dc344e5cf50f

Sample questions

20. When entering Security policy rules you want to ensure your new rules will take precedence over locally entered rules. Where do you put them in Panorama?
    A. In the Security policy rules with a targeted firewall.
    B. In the Default rules section of Security policy rules.
    C. In the Pre-rules section of Security policy rules.
    D. In the Post-rules section of Security policy rules.
21. Which three firewall settings are stored in Panorama Device Groups? Choose 3
    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

Identify options to deploy Palo Alto Networks firewalls in a private or public cloud (VM-Series)

Virtual Firewalls

The VM-Series is a virtualized form factor of our 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 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 virtual firewalls can be found in the public cloud "marketplaces" or uploaded as a virtual appliance into private clouds. There are several models available with the primary difference in them being the number of simultaneous sessions it can support.

Complete information about supported environments and locations can be found here:
https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/vm-series-firewalls

In both private and public cloud environments, the VM-Series can be deployed as a perimeter gateway, an IPsec VPN termination point, and a segmentation gateway, preventing threats from moving from workload to workload. These firewalls run the same PAN-OS® software as hardware appliance firewalls with the same feature set.

An overview of the available models is here:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

VM-Series firewalls deployed in cloud environments have special considerations for HA deployment, specific supported interface types, MAC address handling, Jumbo Frame use among others.

A complete description of these considerations can be found here:
https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization

Sample questions

22. A private cloud has 20 VLANs spread over 5 ESXi hypervisors, managed by single vCenter. How many firewall VMs are needed to implement microsegmentation?
    A. 1
    B. 4
    C. 5
    D. 20
23. When you deploy the Palo Alto Networks NGFW on NSX, do packets coming to an application VM from VMs running on different hardware go through the NSX firewall? If so, which modules do they go through?
    A. No, the Palo Alto Networks NGFW replaces the NSX firewall.
    B. Yes. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, application VM.
    C. Yes. The network, vSwitch, Palo Alto Networks NGFW, NSX firewall, application VM.
    D. Yes. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, NSX firewall, application VM.
24. Which option shows the interface types that ESX supports in the VM-Series firewalls?
    A. Tap, Layer 2, Layer 3, VWire
    B. Layer 3 only
    C. Tap, Layer 2, Layer 3
    D. Layer 3, VWire
25. Which option shows the circumstances in which High Availability is supported for Private Cloud VM-Series firewalls?
    A. ESX supports both active/active and active/passive HA, and KVM and Hyper-V support active/passive only.
    B. ESX, KVM, and Hyper-V support active/passive and active/active HA implementations.
    C. ESX, KVM, and Hyper-V support active passive HA-Lite configurations only, with no Active/Active support.
    D. ESX, KVM, and Hyper-V support active/passive implementations only.

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 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.

The types of administrative account roles are discussed here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-role-types

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.

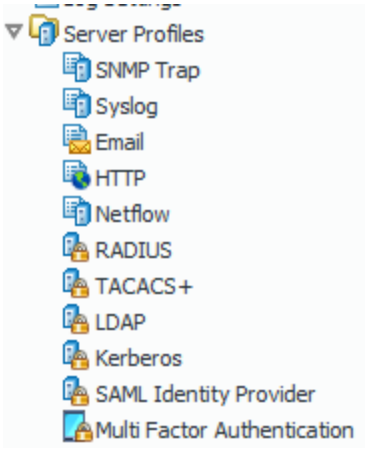
If you have a public key infrastructure, you can deploy certificates to enable authentication without users having to manually respond to login challenges. Alternatively, or in addition to certificates, you can implement interactive authentication, which requires users to authenticate using one or more 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication

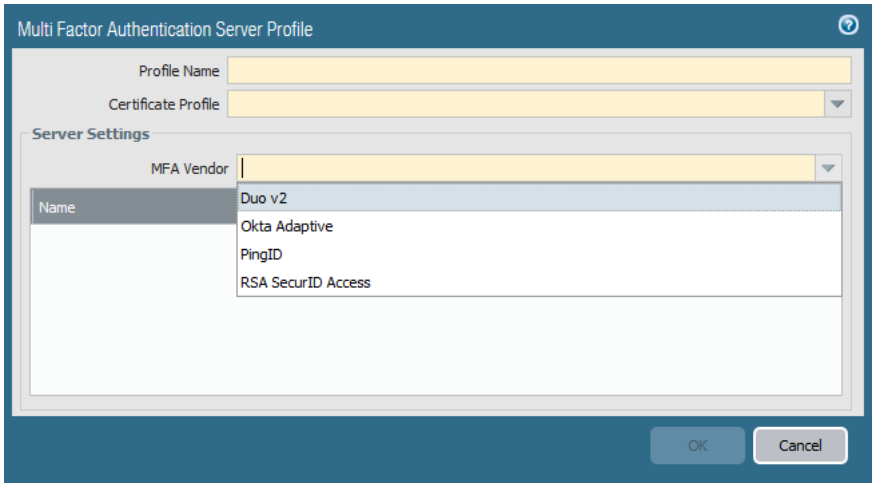
When user or administrative access is configured one or more authentication methods must be specified. A User/administrator definition typically requires an Authentication Profile which captures the desired authentication method. When more than one is desired, an Authentication Sequence can be used instead which is a list of Authentication Profiles. The first will be accessed and if not available will drop to the next option. Authentication Profiles are made up of an ordered list of Server Profiles that contain specific configuration and access information to the external authentication service.



Detailed information on creating Authentication Profiles and Sequences can be found here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication/configure-an-authentication-profile-and-sequence#idf258e497-4998-4a70-8676-aa9aba521a44

A special note on Multi-Factor Authentication.

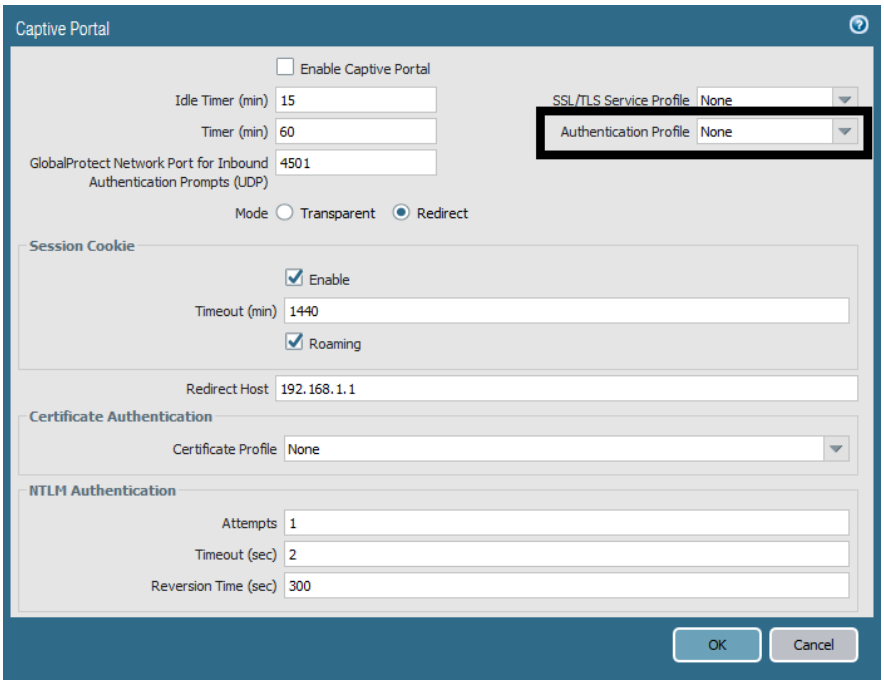
Palo Alto firewalls support multi-factor authentication. A Multi-factor Authentication Server Profile is used to integrate to external 3rd party MFA solution. The MFA factors that the firewall supports include Push, Short Message Service (SMS), Voice, and One-time password (OTP) authentication. This profile is where the specific product is chosen and configuration information for the product's integration is entered.



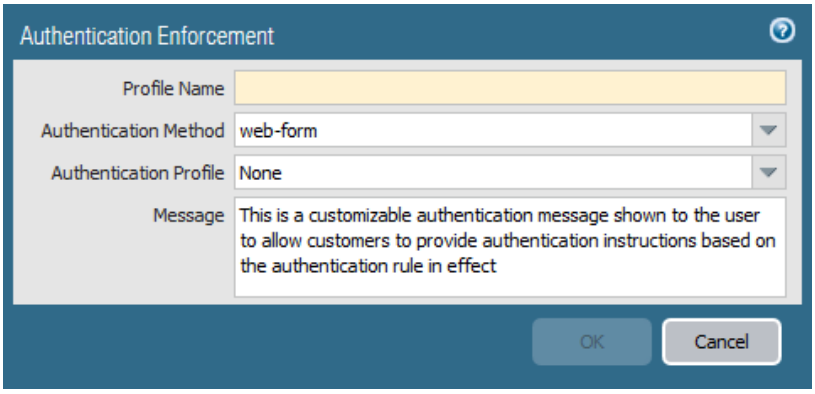
The Multi-factor Authentication Server Profile shown above can in turn be a part of multiple challenges a user must respond to. For example, you can force users to enter a login password and then enter a

verification code that they receive by phone before accessing critical financial documents.

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



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



Configuring base Captive Portal is discussed here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication/configure-multi-factor-authentication

Panorama Access Domains

Panorama implements an additional level of administration that through Access Domains. This optional configuration restricts Panorama administrator access to the settings for specific firewall(s).

More information about this can be found here:

https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/panorama-overview/role-based-access-control/access-domains#id3fcb9a8f-be36-4dd2-ace7-f82c20a90409

Sample questions

26. Which built-in Dynamic role would you give an auditor who is authorized to audit everything on the firewall?
    A. Superuser
    B. superuser (read-only)
    C. virtual system administrator
    D. virtual system administrator (read-only)
27. In order to configure Multi-Factor authentication for users accessing services through the firewall what primary configuration pieces need to be addressed? (Choose 5)
    A. GlobalProtect Portal
    B. Server Profile
    C. Captive Portal
    D. Authentication Enforcement Profile
    E. Authentication Policy
    F. Local User Database
    G. Authentication Profile
    H. Response Pages
28. Which of the following configuration components are NOT used for user authentication in the firewall?
    A. Local User Database
    B. Server Profiles
    C. Certificates
    D. Admin Roles
    E. Authentication policy rules
29. Which two firewall functions are reserved only for admins assigned the Superuser dynamic role? (Choose 2)
    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

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 are 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/profiles.

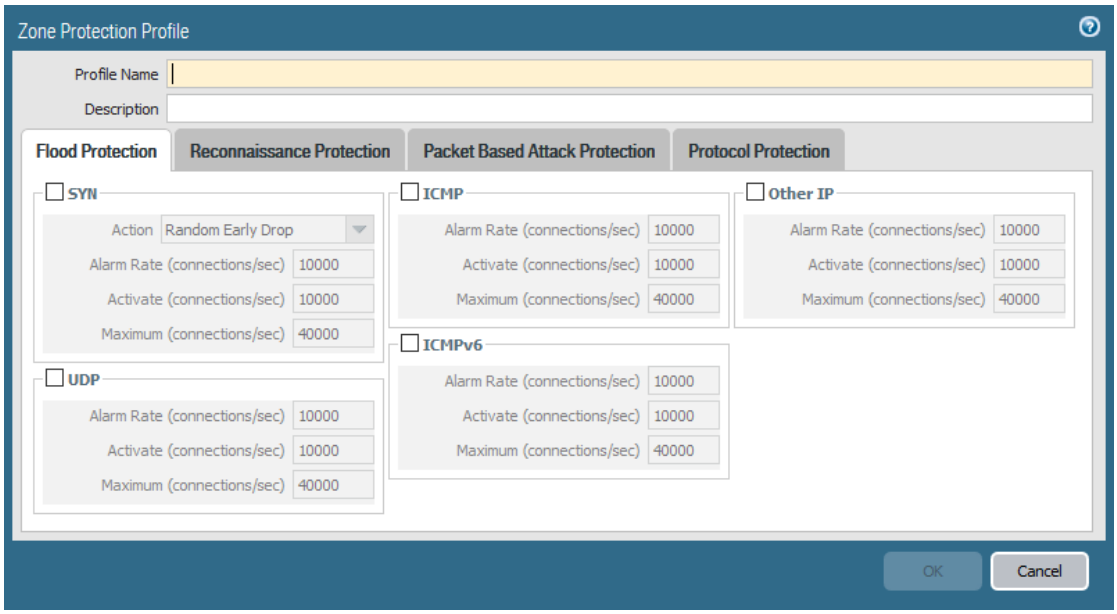
Zone Protection Profiles

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 against flood attacks by limiting the number of connections-per-second 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 broad defense of the entire zone based on the aggregate traffic entering the zone, 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 take individual IP addresses into account 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 minimizing firewall resource use.

A complete description of Zone Protection Profile settings appears here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles



A video tutorial about implementing Zone Protection Profiles is here:
https://live.paloaltonetworks.com/t5/Featured-Articles/Video-Tutorial-Zone-protection- profiles/ta-p/70687

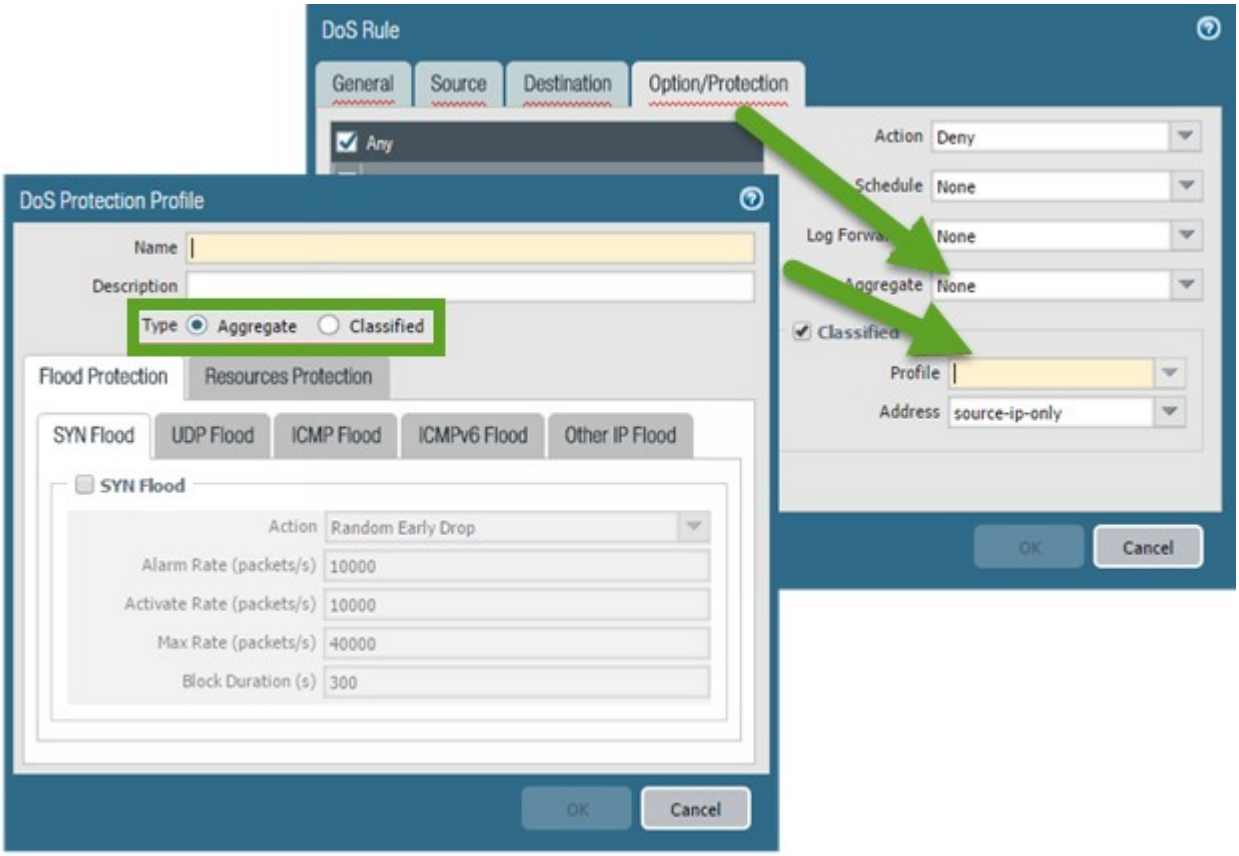
Recommendations for Zone Protection Profile settings are here:
https://live.paloaltonetworks.com/t5/Learning-Articles/Zone-Protection-Recommendations/ta-p/55850

DoS Protection Profile

DoS protection profiles and DoS protection policy rules combine to protect specific areas of your network against packet flood attacks (only, unlike Zone Protection Profiles) and to protect individual resources against session floods.

DoS protection profiles set the protection thresholds to provide DoS Protection Against Flooding of New Sessions for IP floods (connections-per-second 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 what 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 a zone protection profile, which supports only aggregate traffic, you can configure aggregate or classified DoS protection profiles and policy rules.



Implementation specifics for DoS Policy and Profile can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules

An important discussion of DoS protection in general and suggestions for protection can be found here:
https://live.paloaltonetworks.com/t5/Tech-Note-Articles/Understanding-DoS-Protection/ta-p/54562?attachment-id=1085

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

A discussion of the differences between Zone Protection Profiles and DoS Policies is here:
https://live.paloaltonetworks.com/t5/Learning-Articles/Differences-between-DoS-Protection-and-Zone-Protection/ta-p/57761

Sample questions

30. What are two reasons that denial-of-service protections are applied by zone? (Choose two.)
    A. Because denial-of-service protections are applied very early in the processing, before a lot of information is known about the connection – but the ingress interface is already known
    B. Because denial-of-service protections are only applied 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 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 those on virtual wires are yet another category.

31. To which protocol or protocols does the SYN flood protection?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
32. To which two protocols does port scan reconnaissance protection apply? (Choose two.)
    A. UDP
    B. TCP
    C. GRE
    D. ICMP
    E. IPX
33. In what two places do you configure flood protection? (Choose two.)
    A. DoS Profile
    B. QoS Profile
    C. Zone Protection Profile
    D. SYN Profile
    E. XOFF Profile
34. An administrator needs to provide tailored DoS protection to a specific address. Which two firewall features should be used? (Choose two.)
    A. Zone Protection Profiles
    B. Virtual Routers
    C. Server Profiles
    D. DoS protection policy rules
    E. DoS protection profiles

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, 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

Palo Alto Networks firewalls provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Decryption on a Palo Alto Networks firewall includes the capability to enforce

Security policies on encrypted traffic, where otherwise the encrypted traffic might not be blocked and shaped according to your configured security settings. Use decryption on a firewall to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted traffic. Enabling decryption on a Palo Alto Networks firewall can include preparing the keys and certificates required for decryption, creating a decryption policy, and configuring decryption port mirroring.

Traffic that has been encrypted using the protocols SSL and SSH can be decrypted to ensure that these protocols are being used for the intended purposes only, and not to conceal unwanted activity or malicious content.

Special Decryption Implementations

The Palo Alto Networks firewall can act as a Decryption Broker, decrypting traffic and then passing it through a designated interface to external security services providing access to the cleartext contents. These external services then return the traffic, which is re-encrypted by the Palo Alto Networks firewall and then sent to its original destination.

A discussion of this capability appears here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-broker

Palo Alto Networks firewalls can automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This is an option available 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring#idd86db0fc-4038-41bd-8098-f67ec9b27806

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 excluding servers 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. 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.

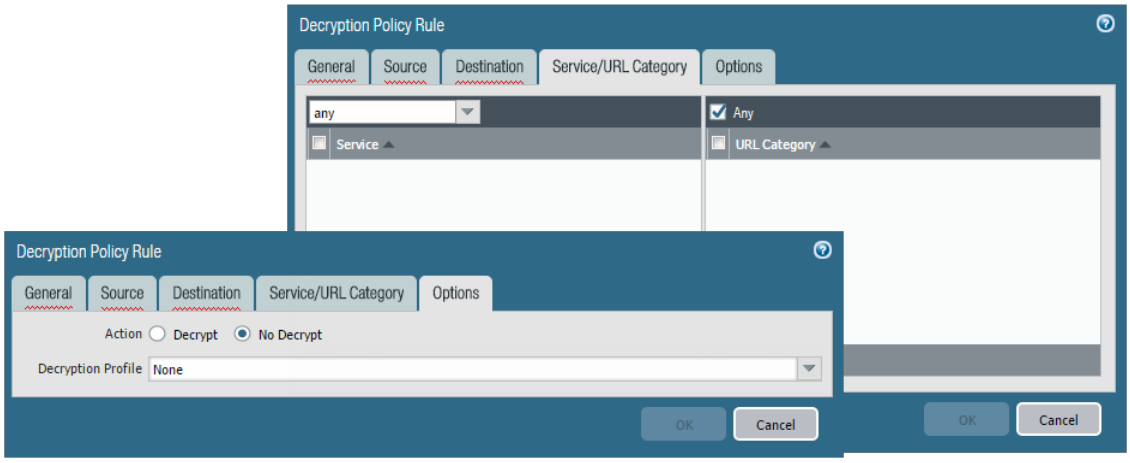
An overview of this capability is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies#idca90e9f4-2403-4907-8577-7d6d026cc2cb

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. To see the certificates in the user interface, click **Device > Certificate Management**. A discussion of certificate use for all purposes in the firewall is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/certificate-management/keys-and-certificates

Decryption Policies

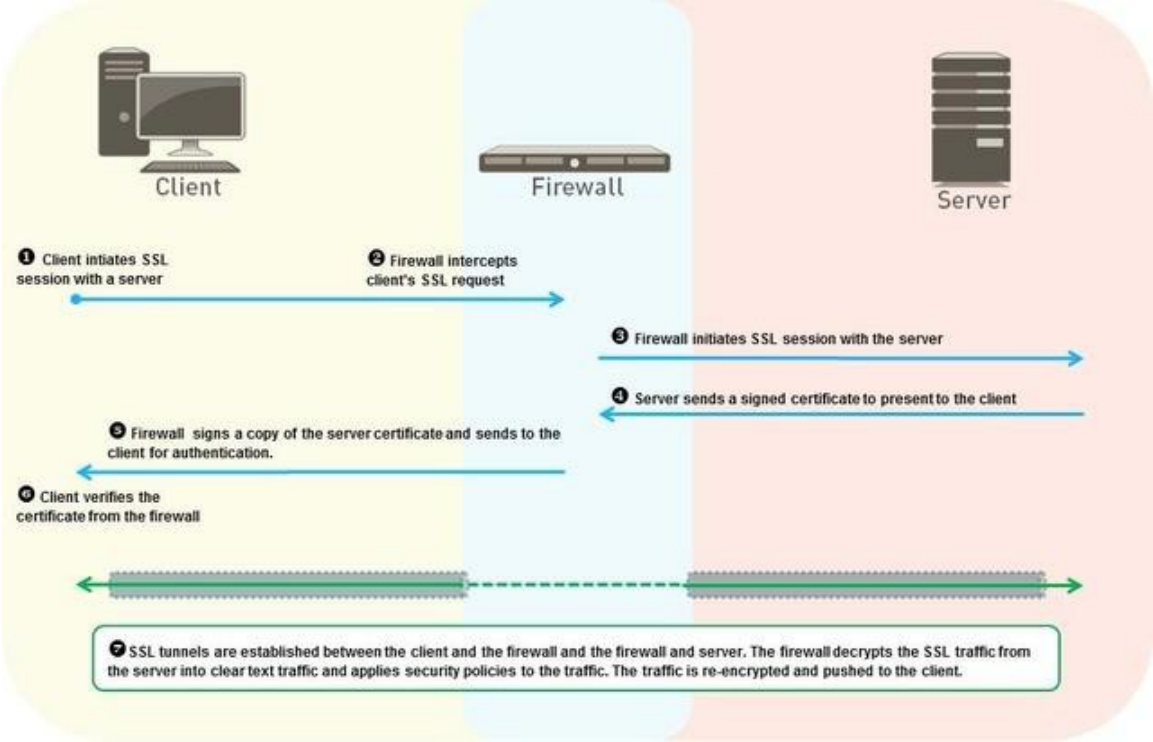
Ingress traffic decryption is controlled by Decryption policies. Palo Alto Networks firewalls automatically will detect encrypted traffic and react by evaluating the Decryption policies. If a matching policy is found, the firewall will attempt to decrypt the traffic according to the policy's specified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



A Decryption policy and its action under the Options tab

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 diagram shows this functionality.

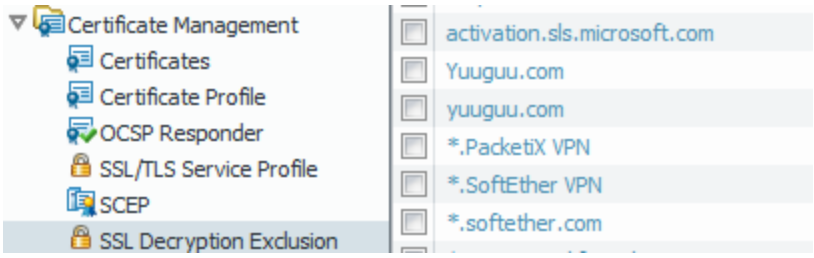


"Man in the Middle" deployment

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

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, considering 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.

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



A discussion of this topic and how to manage decryption exclusions is found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-

exclusions

Decryption policies typically contain other exceptions representing other applications with this behavior.

App-ID and Encryption

The App-ID scanning engine's effectiveness is often compromised by encrypted traffic that prevents scanning 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 elements, allowing the APP-ID engine to properly assign App-IDs without scanning contents. Details of this process are here:
https://live.paloaltonetworks.com/t5/Learning-Articles/How-Palo-Alto-Networks-Identifies-HTTPS-Applications-Without/ta-p/56284

Sample questions

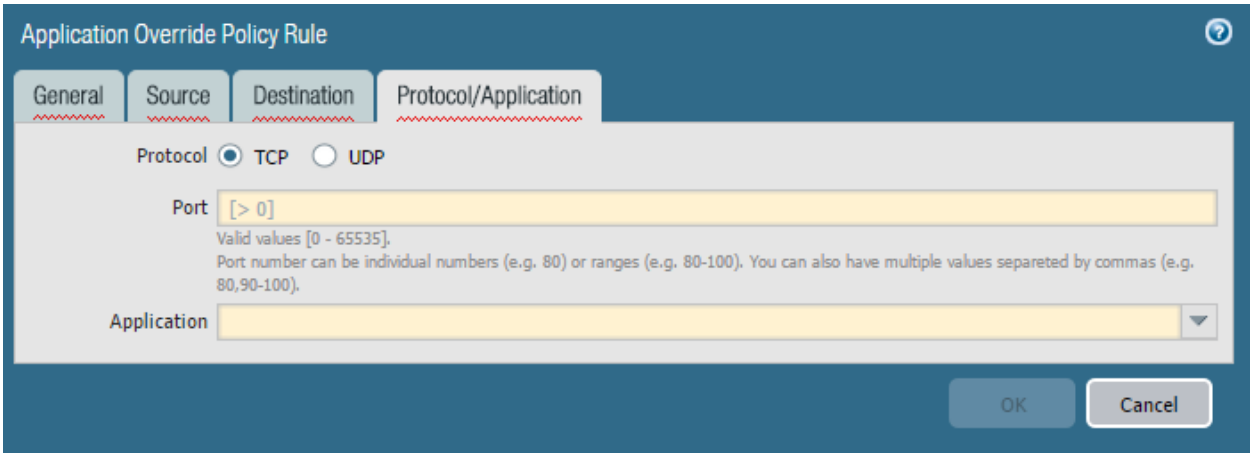
35. Which feature *never* requires a Decryption policy?
    A. antivirus
    B. App-ID
    C. file blocking
    D. network address translation
36. How can the NGFW inform web browsers that a web server's certificate is from an unknown certificate authority (CA)?
    A. Show a "the certificate is untrusted, are you SURE you want to go there" 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.
37. An organization that is decrypting user's browsing traffic has a compliance requirement to record all decrypted traffic. Which two firewall features can be used to directly support this requirement? (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

Answers to sample questions

1. D
2. D
3. A, D

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

Application override policies specify that certain traffic has a specific App-ID. An application override policy also bypasses layer 7 scanning. This means that no further App-ID and Content-ID scanning happens on that traffic.



Application Override policy

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 entry box. Choices are limited to applications currently in the App-ID database.

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 and QoS.

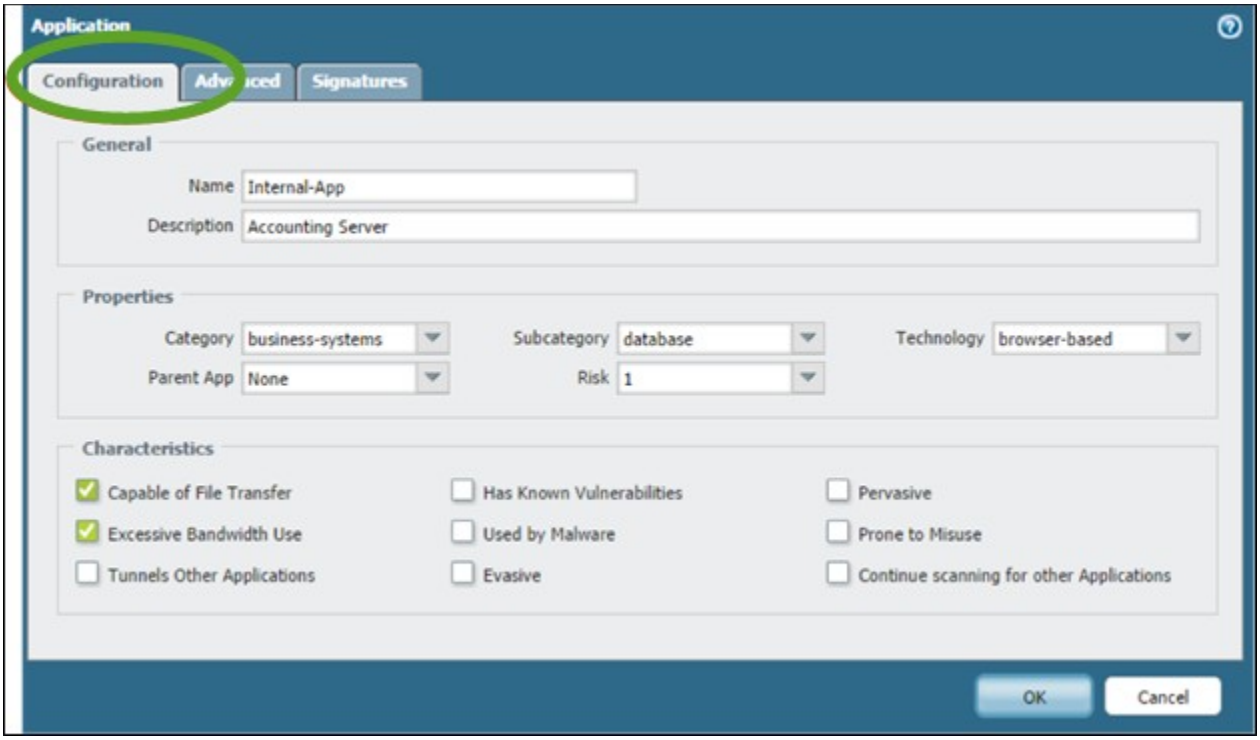
Use Cases

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

A discussion of typical uses of application override and specific implementation examples is here: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

The following illustrations document 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:



Application override should assign purpose-built custom application definitions.

Traffic matching Application Override policies will be identified elsewhere by the included App-ID.

Sample questions

38. Which type or types of identification is disabled by Application Override?
    A. Protocol-ID
    B. User-ID
    C. Content-ID
    D. User-ID and Content-ID
39. 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

Identify the methods of User--ID redistribution

User-ID works by mapping IP addresses to user identities. This information can come from Active

Directory, a Captive Portal, etc. When an organization uses multiple firewalls, it is useful to share the User-ID information between them. If the user must log on manually, usability is a lot better when the user only has to log on once. Even if the user's identity is available automatically (for example, from Active Directory), performance is better if the source of User-ID is queried only by a single firewall.

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

Sample question

40. How do layers facilitate the mapping (IP to User-ID) and the redistribution of that information?
    A. The IP to User-ID mapping is obtained by the lowest layer and is sent to the next lowest layer. That layer sends it to the next lowest, and the process repeats until the mapping reaches the top layer. Firewalls from each layer can receive information from multiple firewalls at a lower level. This algorithm allows some firewalls, such as those in remote offices and protecting regional applications, to have only the mappings for users they protect.
    B. The IP to User-ID mapping is obtained by the lowest layer and is sent to all the firewalls on the layer above. This algorithm ensures that all the firewalls (except those at the lowest layer) have all the mappings.
    C. The IP to User-ID mapping is obtained by the highest layer and is sent to the next highest layer. That layer sends it to the next highest, and the process repeats until the mapping reaches the bottom layer. Firewalls from each layer can receive information from multiple firewalls at a higher level. This algorithm allows some firewalls, such as those in remote offices and protecting regional applications, to have only the mappings for users they protect.
    D. The IP to User-ID mapping is obtained by the highest layer and is sent to all the firewalls on the layer below. This algorithm ensures that all the firewalls (except those at the highest layer) have all the mappings

Exam Domain 2 – Deploy and Configure

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 application knowledge allows you to create and enforce Security policy rules to enable, inspect, and shape desired applications and block unwanted applications. When you define policy rules to allow traffic, App-ID begins to classify traffic without any additional configuration.

App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, 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, 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 so that even when not using App-ID as a part of 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 HTTP protocol is recognized by the firewall as the App-ID “Web-Browsing” but when the http traffic belongs to a specific application (i.e., Facebook) it 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 are then 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 it is using a non-standard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.
3. If App-ID determines that encryption (SSL or SSH) is in use, and a Decryption policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow.
4. Decoders for known protocols are then 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 opening dynamic pinholes for applications such as SIP and FTP.

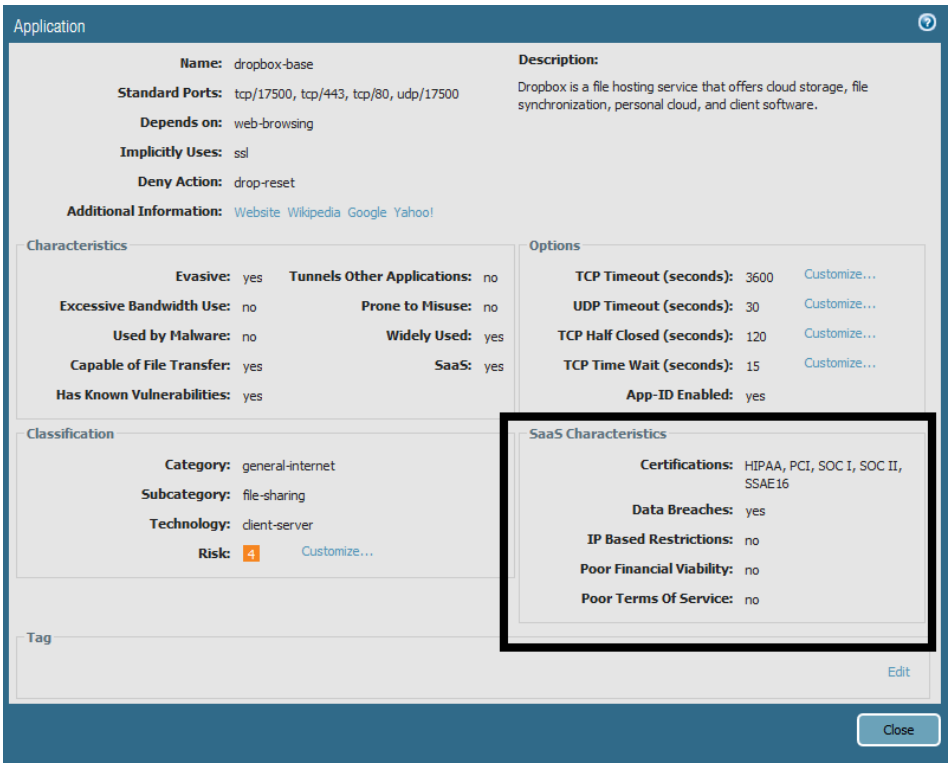
5. For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application.

When 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 the App-ID is being evaluated in every packet (that isn't encrypted) for its App-ID. The state of App-ID recognition changes as a session progresses and these states can be found in traffic logs. There might not have been payload data to scan (Insufficient data), or the session setup never completed (Incomplete), or perhaps the App-ID engine was not able to identify the traffic (unknown-tcp and unknown-udp). There are other states as well. For a full discussion of the App-ID types that might appear in a traffic log refer to this document:
https://live.paloaltonetworks.com/t5/Management-Articles/Not-Applicable-Incomplete-Insufficient-Data-in-the-Application/ta-p/65711

SaaS Applications

The App-ID engine identifies SaaS applications and provides additional functionality. There is a dedicated SaaS Application Usage report under Monitor > PDF Reports > SaaS Application Usage to 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 about sanctioning them at the organizational level.



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 particular SaaS application while having access to the organization's sanctioned environment. A discussion of this feature can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/app-id/http-header-insertion

Note on using App-ID

Because applications can often 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 port numbers it affords a much higher level of capability. When using Palo Alto Networks firewalls it is strongly recommended security rules use App-ID as selection criteria, not port numbers.

A general video about using App-ID can be found here:
https://youtu.be/Pm_hIhqknwk

Manage Custom or Unknown Applications:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/app-id/manage-custom-or-unknown-applications#id74b58a78-164f-4dc5-aa4e-31ce62f2af0d

Sample questions

41. Which option shows the type or types of application that can cause an incomplete value in the Application field in the Traffic log?
    A. UDP

B. TCP
C. ICMP
D. Both TCP and UDP

42. Session traffic being evaluated by a firewall is encrypted with SSL. Without decrypting it how does the firewall make an App-ID determination?
    A. Evaluating the HTTP headers
    B. Evaluating the SSL Hello exchange
    C. Evaluating certificate contents used for encryption
    D. Using information in the SSL Decryption Exclusion cache
43. During the firewall's App-ID scanning of an on-going session a change of application is detected. How does the firewall respond?
    A. Closes the session, opens a new one and evaluates all security policies again
    B. Closes the session, opens and 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

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

While 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) that are attached to the rule are applied for further content inspection rules 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 for 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 Profiles manage particular types of threat detection.

A detailed definition of these profiles and their use can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/security-profiles

A discussion of the application of Security Profiles to Security policy rules can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/set-up-a-basic-security-policy#idaf666d2e-b8eb-401d-a40a-668d93913154

Sample questions

44. Which profile do you use for DLP (data loss protection)?
    A. Antivirus
    B. URL Filtering
    C. File Blocking
    D. Data Filtering
45. A firewall admin is concerned about users entering user credentials into phishing sites. Which Security Profile can be configured to provide credential protection?
    A. WildFire® Analysis
    B. Tunnel Filtering
    C. Data Filtering
    D. URL Filtering

Identify the relationship between URL filtering and credential theft prevention

The Palo Alto Networks URL filtering solution compliments App-ID by enabling you to configure the firewall to identify and control access to web (HTTP and HTTPS) traffic and to protect 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 websites that have been categorized into categories. 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 can also 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 what 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 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 still allows them 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.

A discussion of this feature and how to implement can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/threat-prevention/prevent-credential-phishing#id743cc2df-382e-4d53-a74a-51f38be19ecf

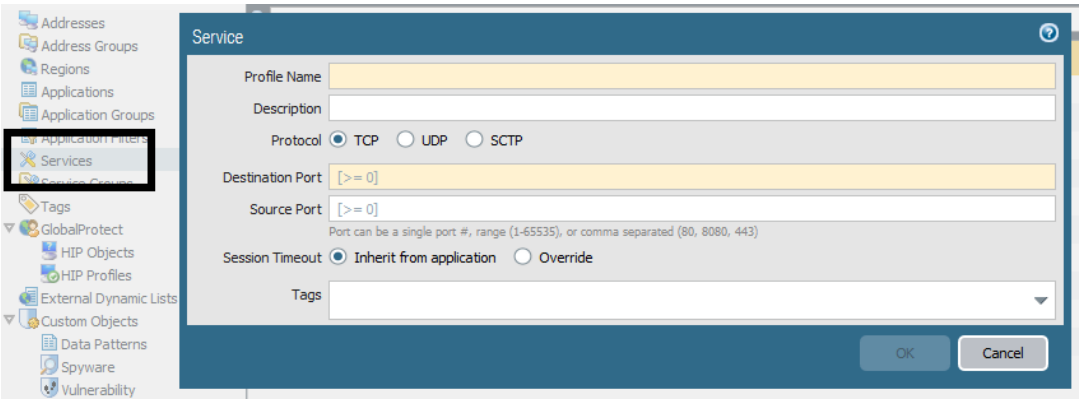
Sample questions

46. Which credential phishing prevention action allows users to decide to submit to a site anyway?
    A. Alert
    B. Allow
    C. Block
    D. Continue
47. 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.
48. A firewall administrator wished to enable Credential Phishing Prevention that blocks an attempt by a user to enter their organizations user ID and password. Which Type of User Credential Detection should be used?
    A. IP User Mapping
    B. Domain Credential Filter
    C. Group Mapping
    D. Citrix Mapping

Identify differences between services and applications

Applications identification (App-ID) is central to the operation of the NGFW. Port filters are no longer sufficient because multiple applications use the same ports, and applications can use ports that are different from their default. Services, however, are the objects that Palo Alto Networks uses to identify port numbers.

There are a few features in the firewall that might require the identification of port number (Services) as supplemental to the App-ID or as matching criteria for features that only scan packet headers (i.e., Application Override, NAT, etc.)



App-IDs are often found in Security policy rules and an application identified by App-ID might not be using its default port. The selection of "application-default" in the Service configuration of Security policy rules adds an enforcement condition that the detected App-ID must be using its default port(s) to match the App-ID condition. In situations where an App-ID might be using a non-standard port, or it does not have standard port number(s) at all the inclusion of a Service object to specify the ports or even the selection of "any" as a port number might be appropriate.

References

- **Objects > Applications** https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/objects/objects-applications#_96266
- **Objects > Application Groups** https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/objects/objects-application-groups
- **Objects > Services** https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/objects/objects-services

Sample question

49. Which two protocols are supported for services? (Choose two.)
    A. ICMP
    B. TCP
    C. IGP
    D. GRE
    E. UDP

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

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

Palo Alto Networks App-ID technology discussed in another section of this document provides for positive identification of applications regardless of port usage. This makes the safe access enablement for only

required access to only the users that require them possible. This practice reduces your attack surface by eliminating the potentially vulnerable traffic of unwanted applications. See the previous section for a discussion of the use of App-ID versus port number enforcement.

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.

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

A discussion of App-ID based policy can be found here:
https://www.paloaltonetworks.com/resources/datasheets/application-based-policies

Details of creating and managing Security policy rules and the use of App-ID appears here:
https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/policies/policies-security#ida067ab2f-c201-4411-9e51-c62e8e83935c

Sample questions

50. Which two applications cannot be identified by port number? (Choose two.)
    A. Microsoft Outlook Express email
    B. Google mail (Gmail)
    C. SSH
    D. Facebook
    E. FTP
51. An administrator creates a Security policy rule allowing office-on-demand traffic through the firewall. When the change is committed the firewall issues a warning saying,

    ```
    "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"
    ```

    What action should the administrator take?
    A. None is required, this is only a warning. Protection is still enabled
    B. The listed applications should be added to the same Security policy rule
    C. The Service action of the rule should be set to "dependent application default"
    D. Create a new Security policy rule for each listed application with an allow action higher in the rule list

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 of this link:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/activate-licenses-and-subscriptions#ide86db26b-258b-421f-9328-7aba83e734d4

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:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/install-content-and-software-updates#61072

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started

Sample questions

52. 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 for some reason.
D. Verify that the configuration is correct. You do not need to do anything else if it is correct, the configuration is updated automatically.

53. 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

Identify various methods for Authentication, Authorization, and Device Administration within a firewall.

See Identify methods for Authorization, Authentication, and Device Administration on p. 33.

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

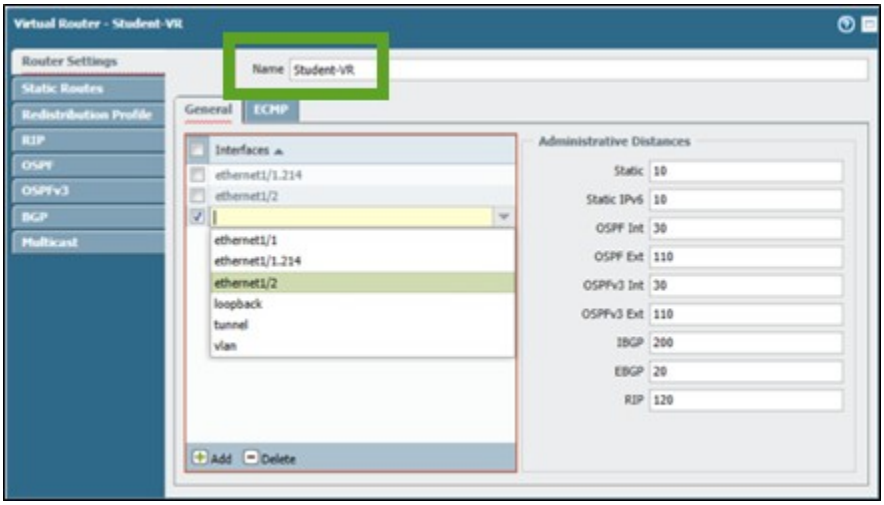
Sample questions

54. Which is *not* an application in which the NGFW and Panorama use certificates?
    A. Communication with Active Directory to obtain User-ID information
    B. Device authentication for the Captive Portal for User-ID information
    C. Device authentication for IPsec site-to-site VPN with Internet Key Exchange (IKE)
    D. Certificate to re-encrypt inbound SSL traffic
55. Administrators within the enterprise wish to replace the default certificate used by the firewall to secure the Web Management UI traffic with one generated by their existing certificate authority. Which of the following certificate properties 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. The CN must be set to the management port of the firewall

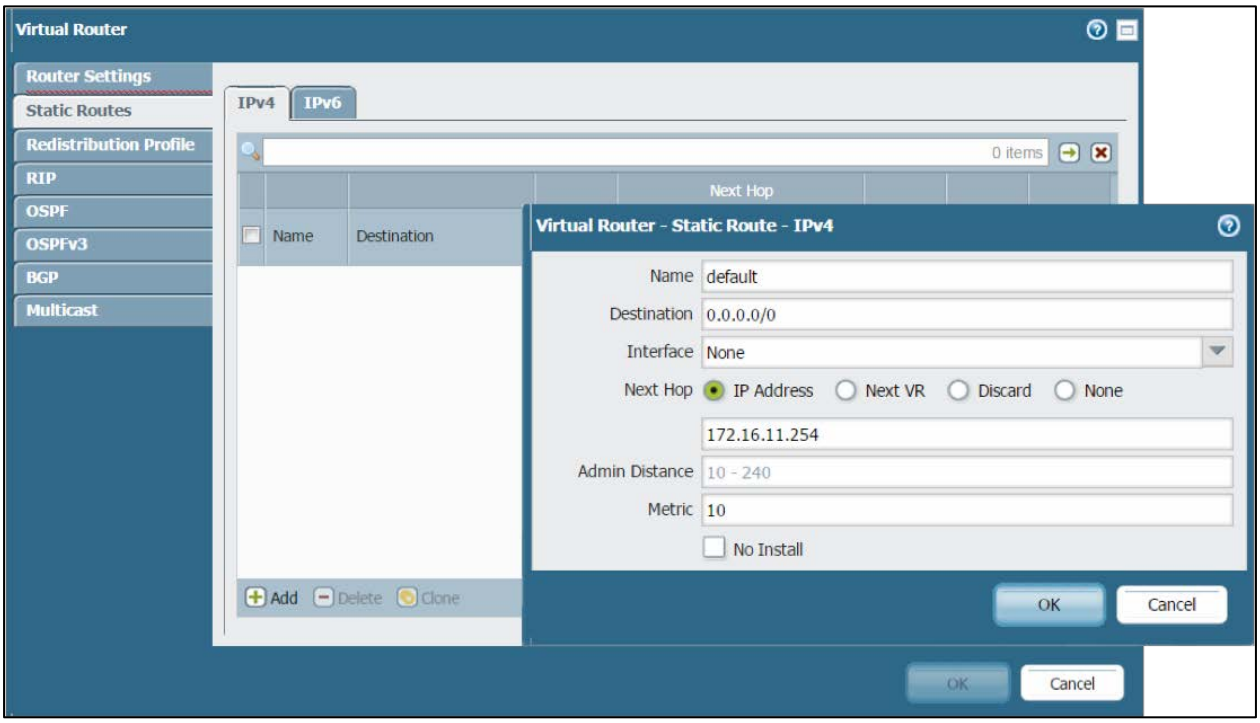
Identify how to configure a virtual router

Routing Configuration

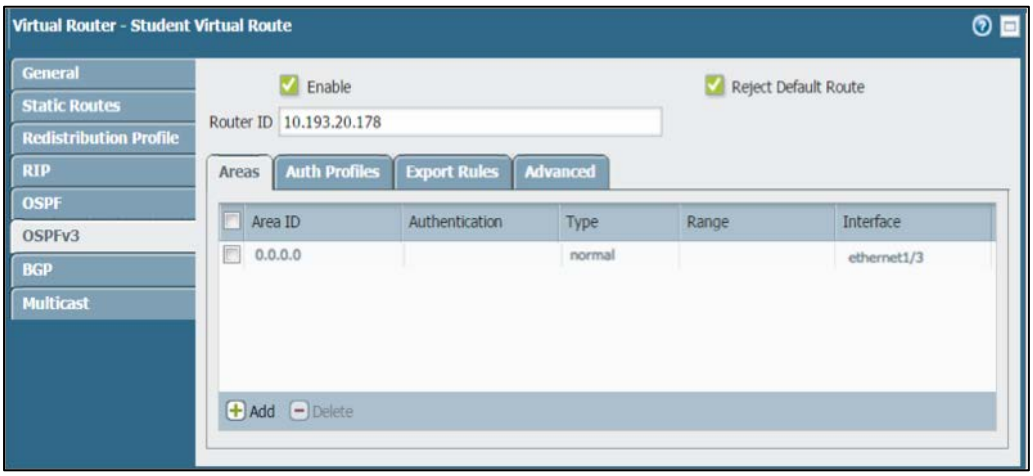
PAN-OS® software supports static routes, BGP, OSPF, RIP, and Multicast routing configured in the virtual router (VR). There are limitations for the number of entries in the forwarding and routing tables. Different platform levels also can support varying numbers of VRs. The VR configuration is meant to match the existing routing and routed infrastructure. In addition to protocol configuration, redistribution profiles can support protocol interoperability.



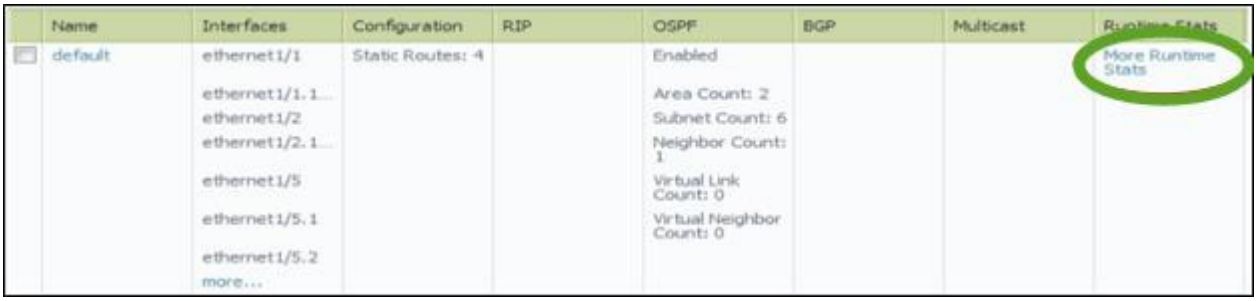
Virtual routers handle all Layer 3 forwarding decisions.



Static route creation in a virtual router



An example dynamic routing protocol configuration



The virtual router's routing and forwarding tables can be displayed.

A discussion of virtual routers and each of the supported dynamic routing protocols is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking

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

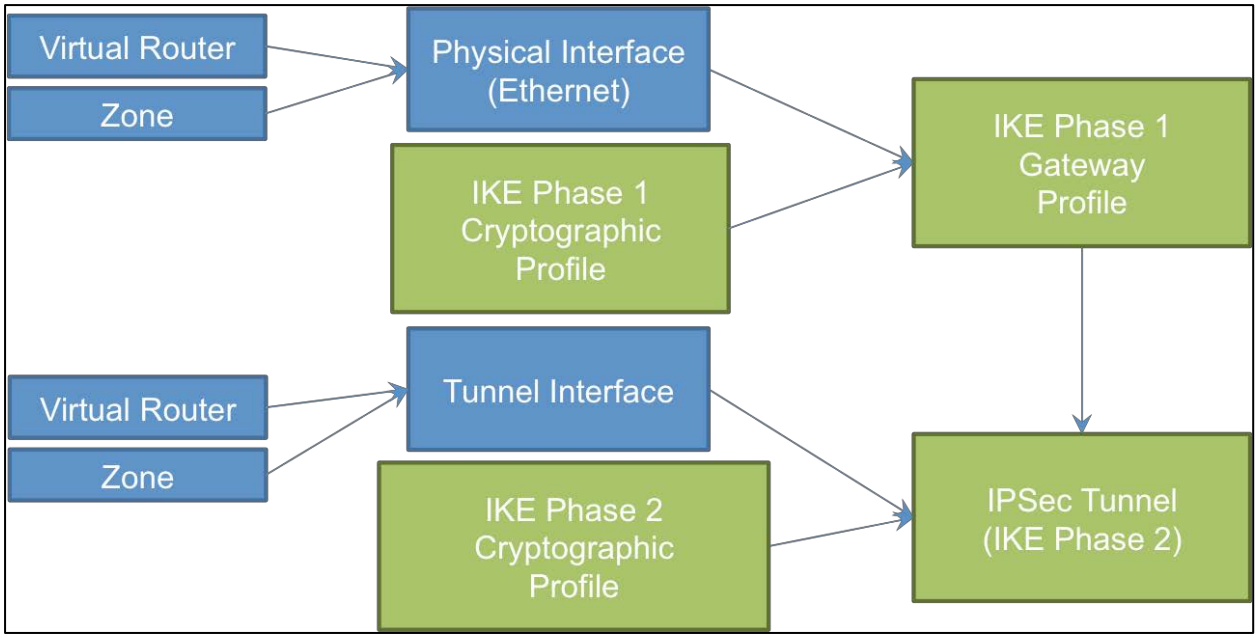
56. Can two Layer 3 interfaces have the same IP address. If so, under which conditions?
    A. Yes, but they must be connected to different virtual routers
    B. Yes, but they must be connected to the same Ethernet network through a switch. This configuration can be used only for high availability
    C. No, that is impossible
    D. Yes, but they must be subinterfaces of the same physical interface
57. A firewall's virtual router can connect to which three types of interfaces? (Choose three.)
    A. Virtual Wire Interface
    B. Management Interface
    C. Layer 3 traffic interface
    D. HA1 Interface

E. HA2 Interface
F. Loopback Interface
G. Tunnel Interface

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, 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 diagram illustrates the various objects involved in IPsec tunnel definitions.



There are multiple objects to configure to enable an IPsec tunnel.

A complete discussion of required settings is found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/vpns

CLI Troubleshooting Commands

The CLI offers 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.

Sample questions

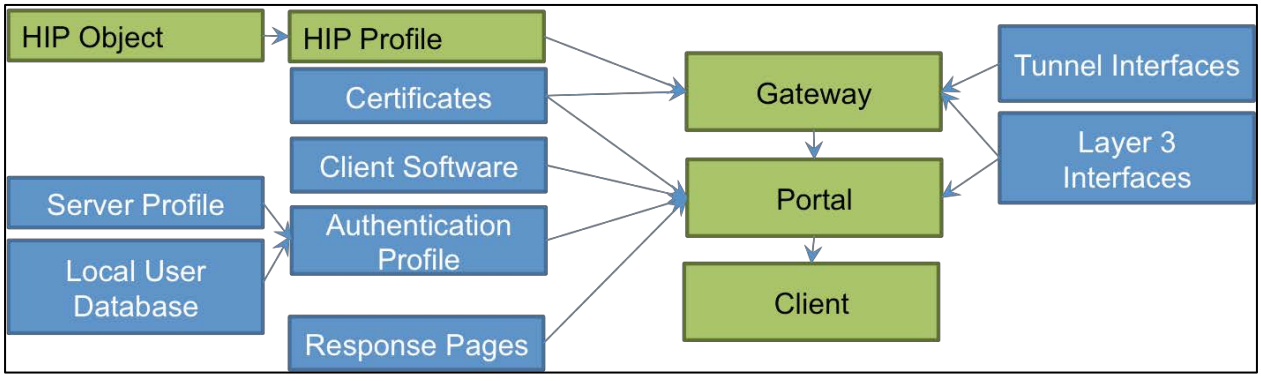
58. Which type is a tunnel interface?
    A. Tap
    B. Virtual wire
    C. Layer 2
    D. Layer 3
59. A firewall administrator is rolling out 50 Palo Alto Networks firewalls to protect remote sites. He wishes each to have a site-to-site IPsec VPN tunnel to each of the three campus locations. Which configuration function is the basis for automatic site-to-site IPsec tunnels setup 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 three campus' IPsec tunnel config
    C. Configuring the GlobalProtect Satellite settings of the campus and remote firewalls
    D. Entering campus IPsec tunnel settings for each remote firewall's IPsec Profile

Identify the configuration settings for GlobalProtect

GlobalProtect Overview

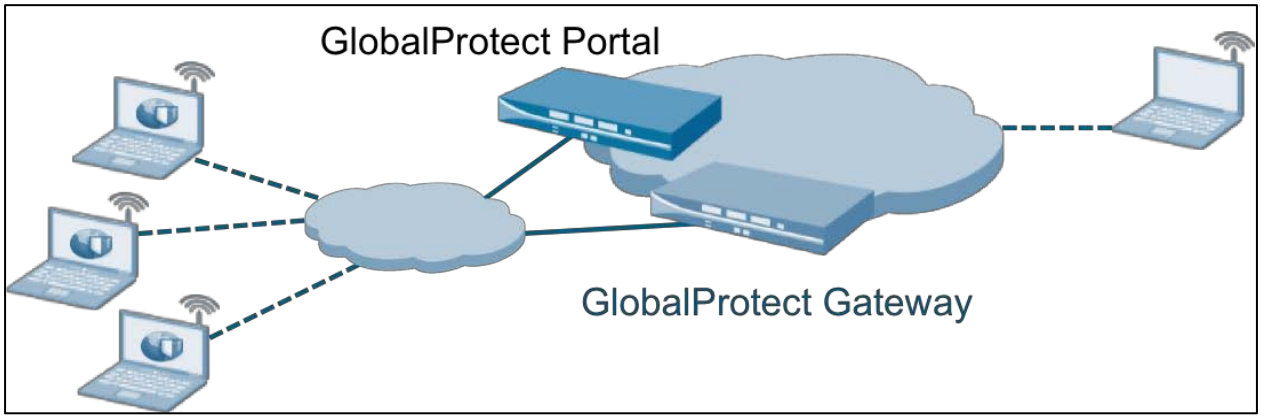
GlobalProtect solves the security challenges of roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located. GlobalProtect uses client software to build secure personal VPN tunnels to the firewall.

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/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/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:



There are multiple objects to configure to enable GlobalProtect.

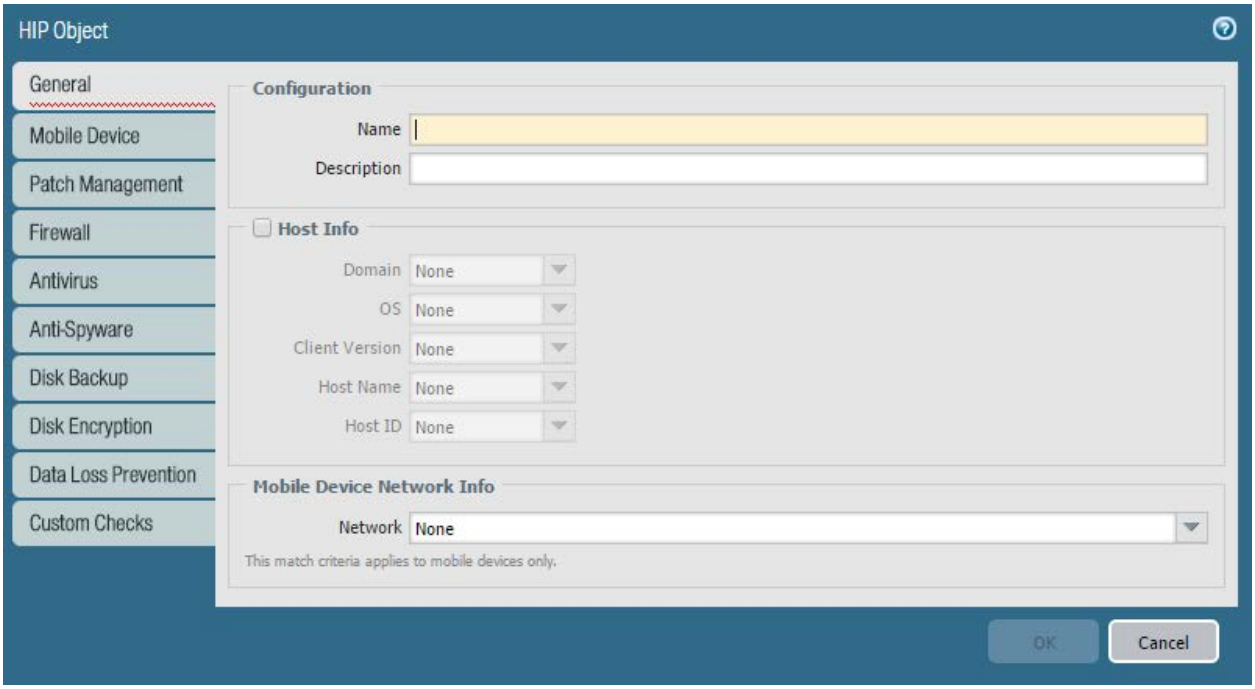
Every Palo Alto Networks firewall can provide GlobalProtect connectivity support to Windows and Mac clients with no additional license requirement. Client software can be downloaded directly from the Portal.



The GlobalProtect architectural components in a typical implementation.

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).

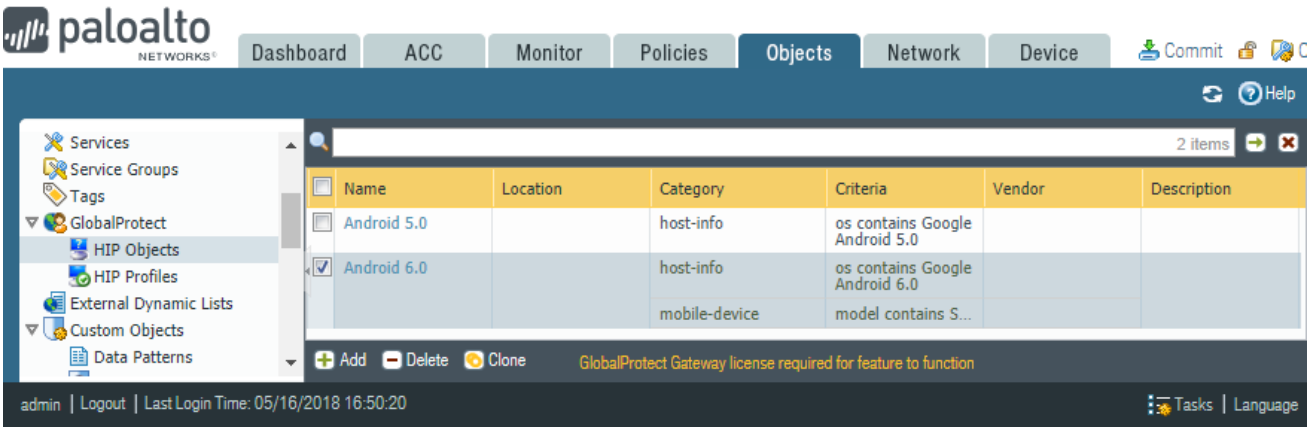
With the appropriate license, HIP checks can be performed by GlobalProtect agent software on the client platforms at connect time. The host information profile includes the OS version, patches installed, firewall and antivirus parameters, the process list, the registry, and other information that is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



HIP Object components

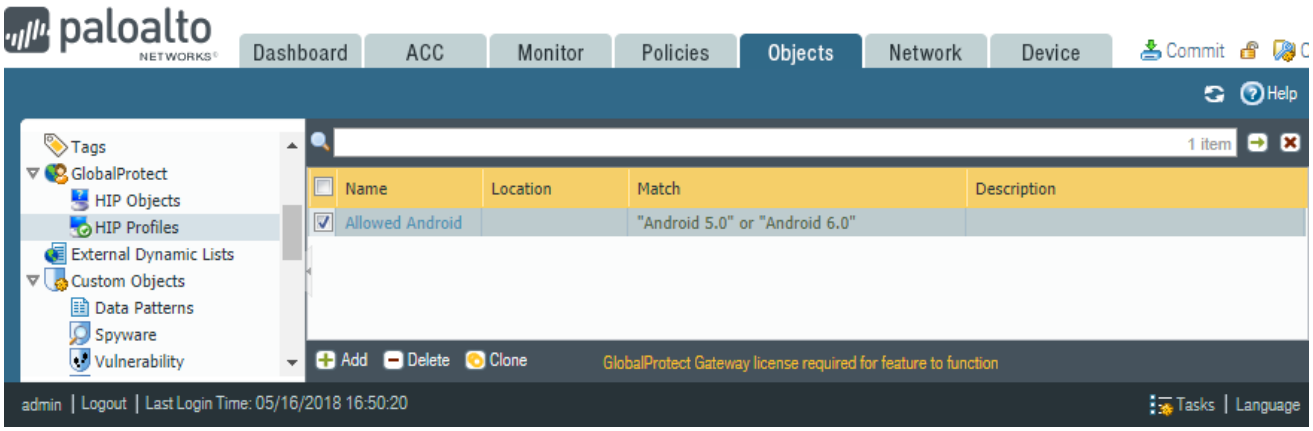
The firewall can extract information from these reports and use them as part of the Security policy. In this way the firewall provides appropriate access, depending on endpoint configuration.

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



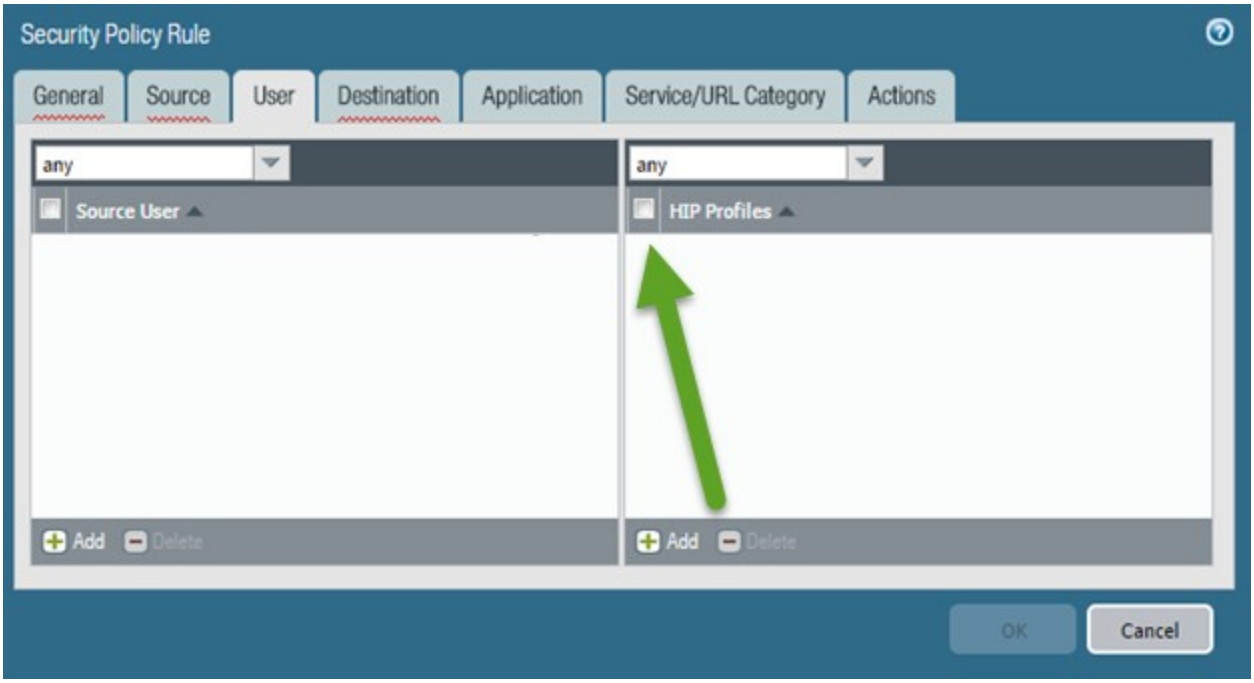
Examples of HIP Objects

These HIP objects are then used in HIP profiles.



An HIP Profile

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



HIP objects bring remote endpoint configuration to Security policy decision-making.

References

- Configuration of the firewall for GlobalProtect is discussed here: https://www.paloaltonetworks.com/documentation/81/globalprotect/globalprotect-admin-guide/get-started
- HIP checking implementation and use is explored in detail here: https://www.paloaltonetworks.com/documentation/81/globalprotect/globalprotect-admin-guide/host-information

Sample questions

60. Which operating system is not supported for use with GlobalProtect clients?
    A. iOS
    B. Android
    C. Windows
    D. z/OS
61. Which two functions is a GlobalProtect Gateway 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

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

See Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers on p. 37.

Identify how to configure features of the NAT rulebase

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 addresses, and application service (such as HTTP). As 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://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/policies/policies-nat#_38816

Sample questions

62. Which NAT type can be used to translate between IPv4 and IPv6?
    A. ipv4
    B. nat64
    C. nptv6
    D. ipv6
63. When a firewall has more than one NAT Policy rule that matches a packet how does it 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.

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://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/policies/policies-security#_54026

Sample questions

64. 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
65. 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). For a packet that has this rule applied what Security policy rule components are required 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

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 can also 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/service (or chain of devices) that examines the clear-text 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 on the use and configuration of this capability can be found here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-broker

See also Special Decryption Implementations on p. 42.

Special Decryption Implementations

The Palo Alto Networks firewall can act as a Decryption Broker, decrypting traffic and then passing it through a designated interface to external security services providing access to the cleartext contents. These external services then return the traffic which is re-encrypted by the Palo Alto Networks firewall

and sent to its original destination.

A discussion of this capability appears in the same link as above:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-broker

Palo Alto Networks firewalls can also automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This is an option available 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring#idd86db0fc-4038-41bd-8098-f67ec9b27806

References

- **Policies > Decryption** and https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/policies/policies-decryption#_56365
- SSL Forward Proxy
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/ssl-forward-proxy
- SSL Inbound Inspection
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/ssl-inbound-inspection
- SSH Proxy
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/ssh-proxy
- Configure SSL Forward Proxy
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/configure-ssl-forward-proxy
- Configure SSL Inbound Inspection
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/configure-ssl-inbound-inspection
- Configure SSH Proxy
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/configure-ssh-proxy

Sample questions

66. Which protocol is supported for traffic decryption?
    A. IPsec
    B. SP3
    C. SSH
    D. NLSP
67. 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

68. A firewall administrator is decrypting outbound SSL traffic and realizes certain traffic is sensitive and should not be decrypted. What feature must be configured to exclude the specific traffic from decryption?
    A. A Security policy rule that includes the specific URL with an “allow” action
    B. A Decryption policy rule with the specific URL and “no decrypt” action
    C. An Application Override policy that matches the application URL and port number
    D. A Decryption Profile that includes the site’s URL

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. This policy attaches 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://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/policies/policies-application-override#_81068
- **Objects > Applications** https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/objects/objects-applications/defining-applications

Sample questions

69. 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
70. If an Application Override policy rule matches traffic it assigns the indicated App-ID to the traffic. This assigned App-ID cannot be used in which firewall function?
    A. Security policy rule match conditions
    B. Policy Based Forwarding Policy rule match conditions
    C. QoS Policy rule match conditions
    D. NAT Policy rule match conditions

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® 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

71. 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
72. Which three items of information are required at a minimum to install and configure VM-Series firewalls? (Choose three.)
    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
73. VM-Series firewalls require which additional license step?
    A. Applying a “Base Capacity” license.
    B. Applying a “Cloud Services” license.
    C. Applying a “Site license” license.
    D. Applying a “VM Update” license.
74. A VM-Series firewall being deployed in Azure can be automatically configured by bootstrapping. Azure requires which of the following for Bootstrapping to work:
    A. A Storage Account configured for Azure Files Service
    B. A PowerShell script that feeds a configuration file to the firewall
    C. A xml configuration file included in the base firewall provisioning
    D. Azure Backup services configured with a config file and included in the firewall provisioning

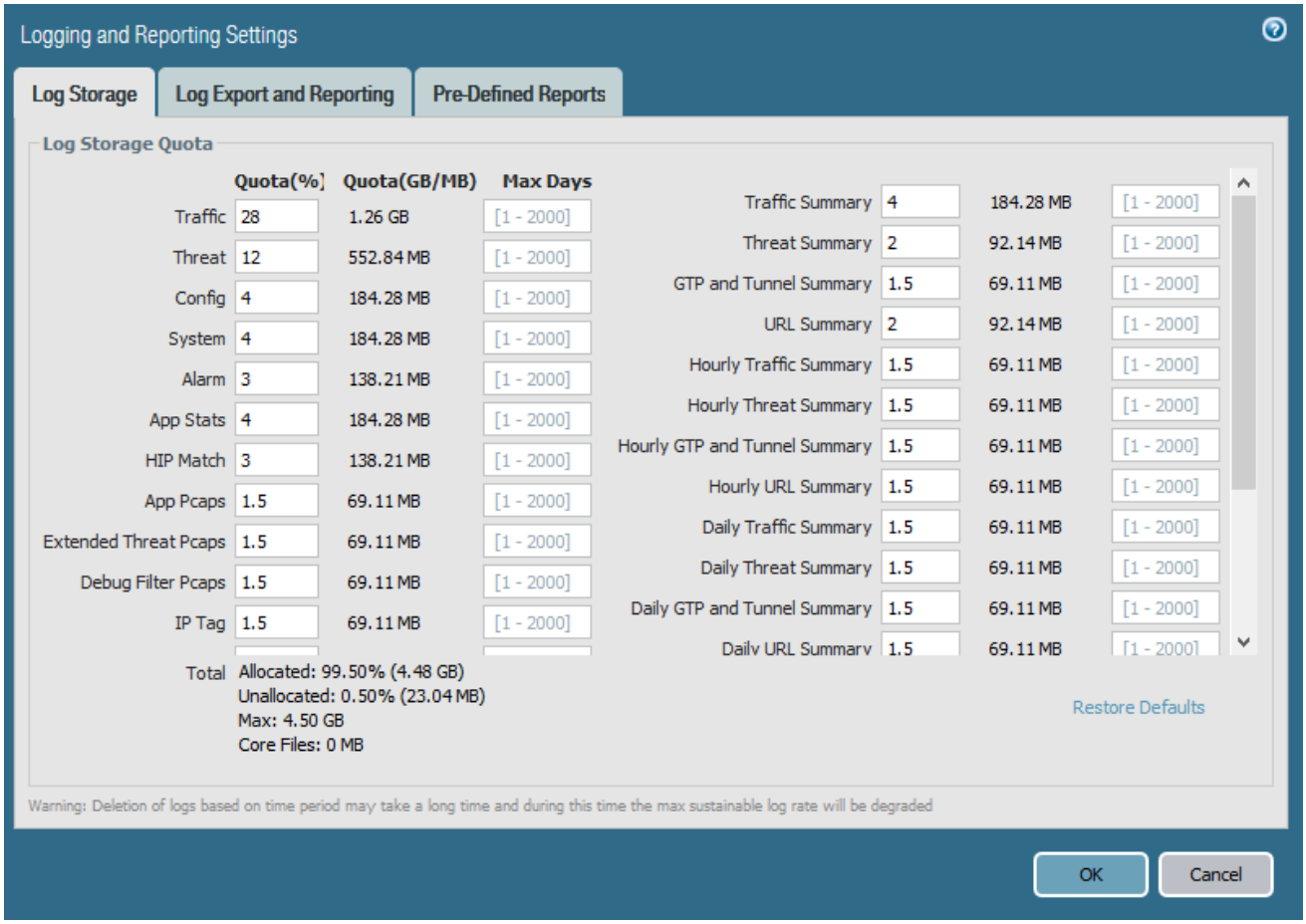
Exam Domain 3 – Operate

Identify considerations for configuring external log forwarding

Direct Firewall Log Forwarding

Using 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.



Device > Setup > Management > Logging and Reporting Settings

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

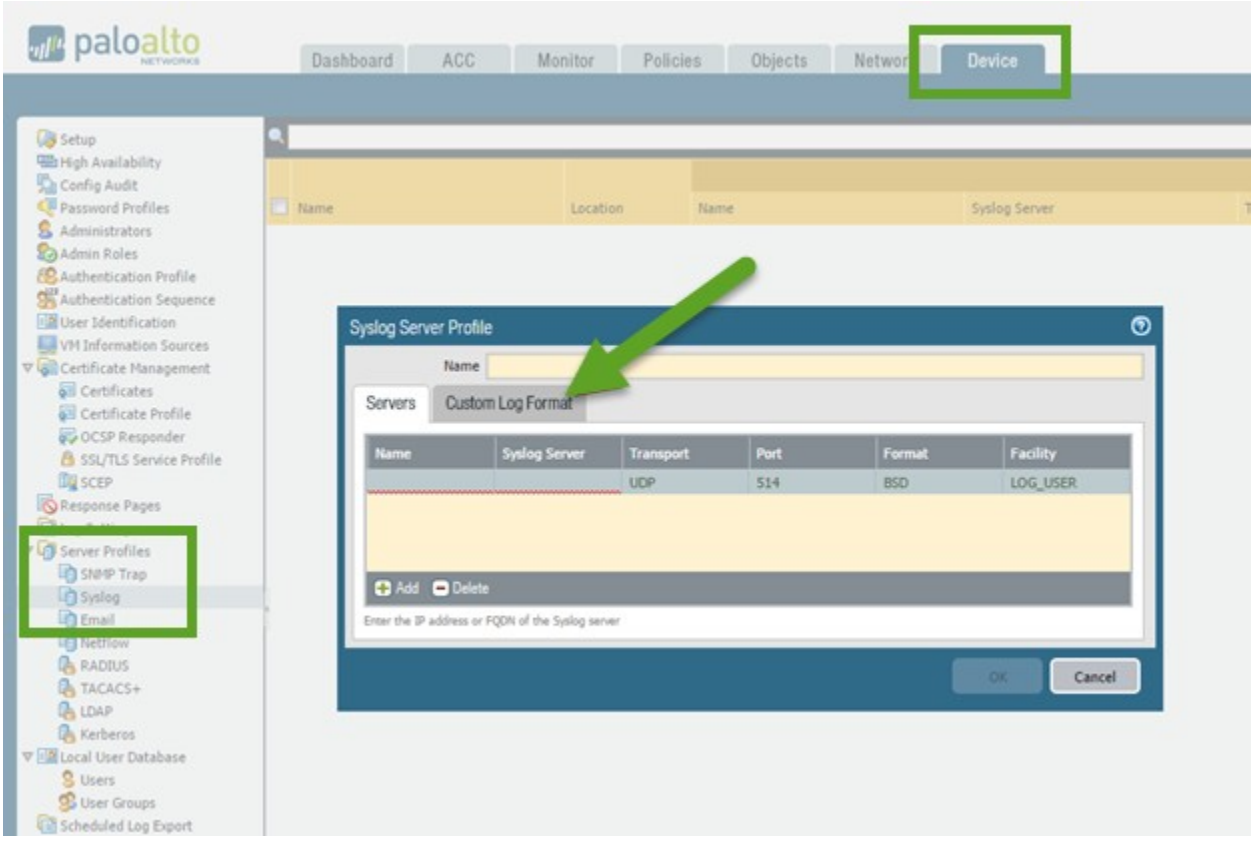
Before you can use Panorama or external systems to monitor the firewall, you must configure the firewall to forward its logs. Before forwarding to external services, the firewall automatically converts the logs to the necessary format: syslog messages, SNMP traps, HTTP, or email notifications. Before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

External forwarding supports the following types of destinations:

1. SNMP traps
2. syslog
3. HTTP server
4. Email

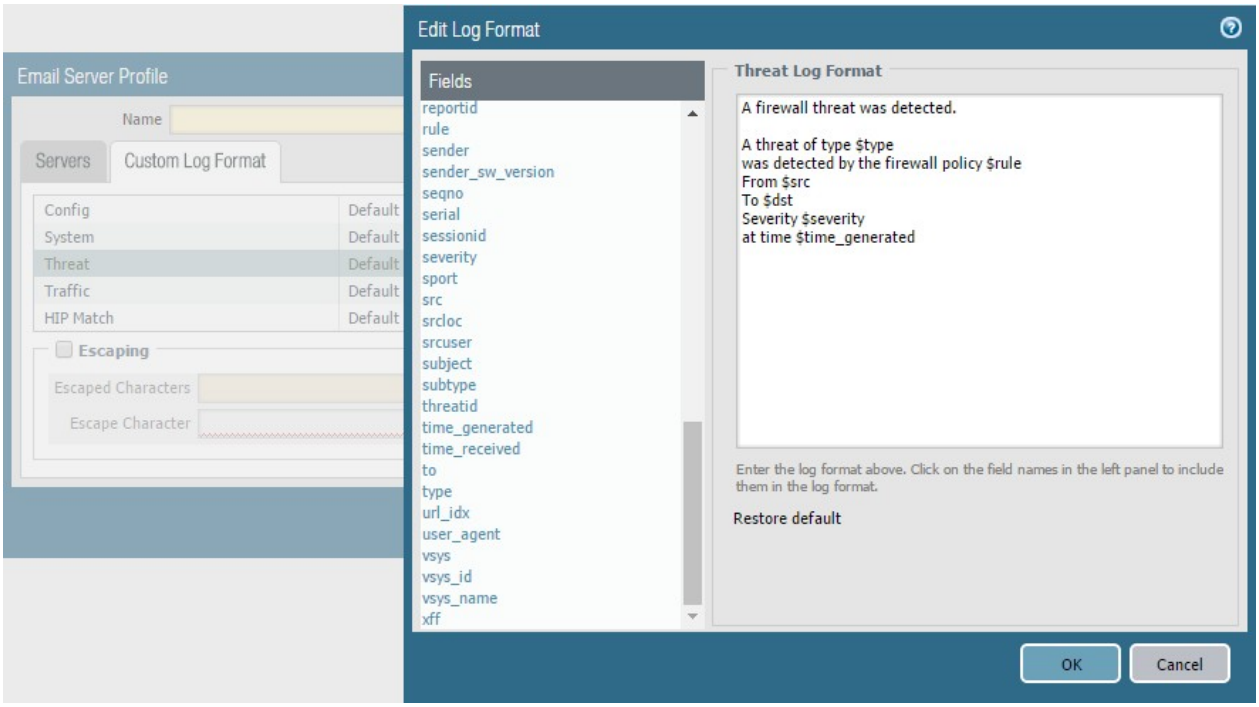
5. Panorama

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



Creating a syslog log forwarding destination

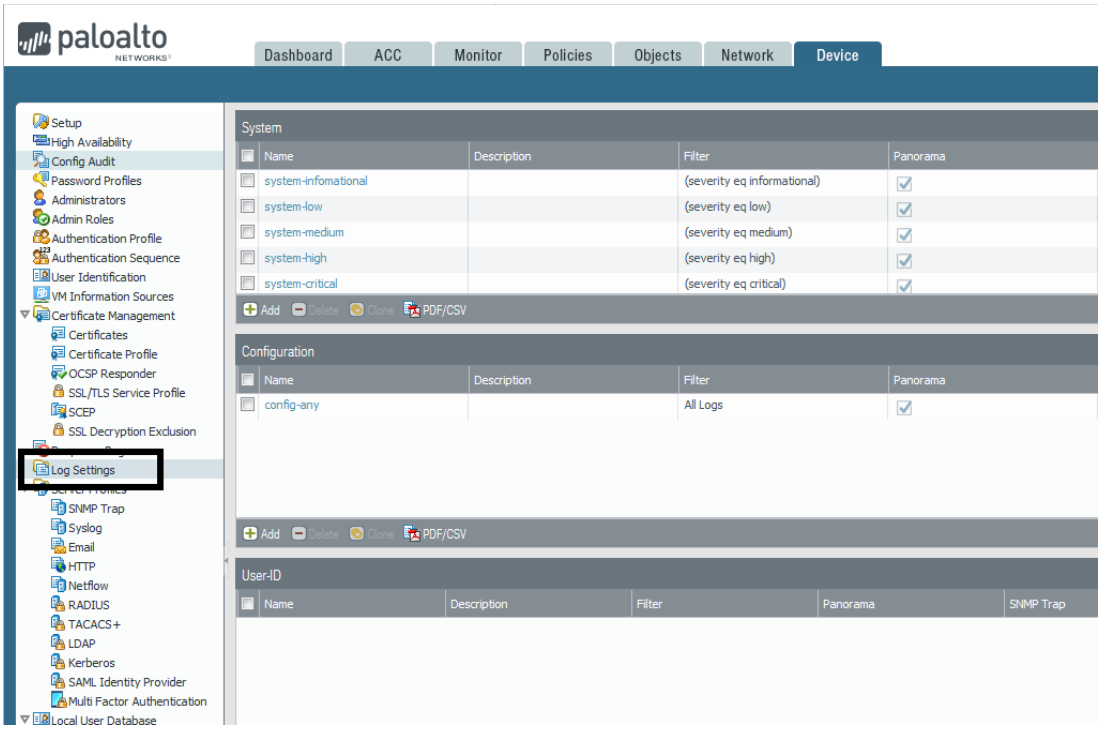
Email message formats can be customized. For example:



An example of a customized email message

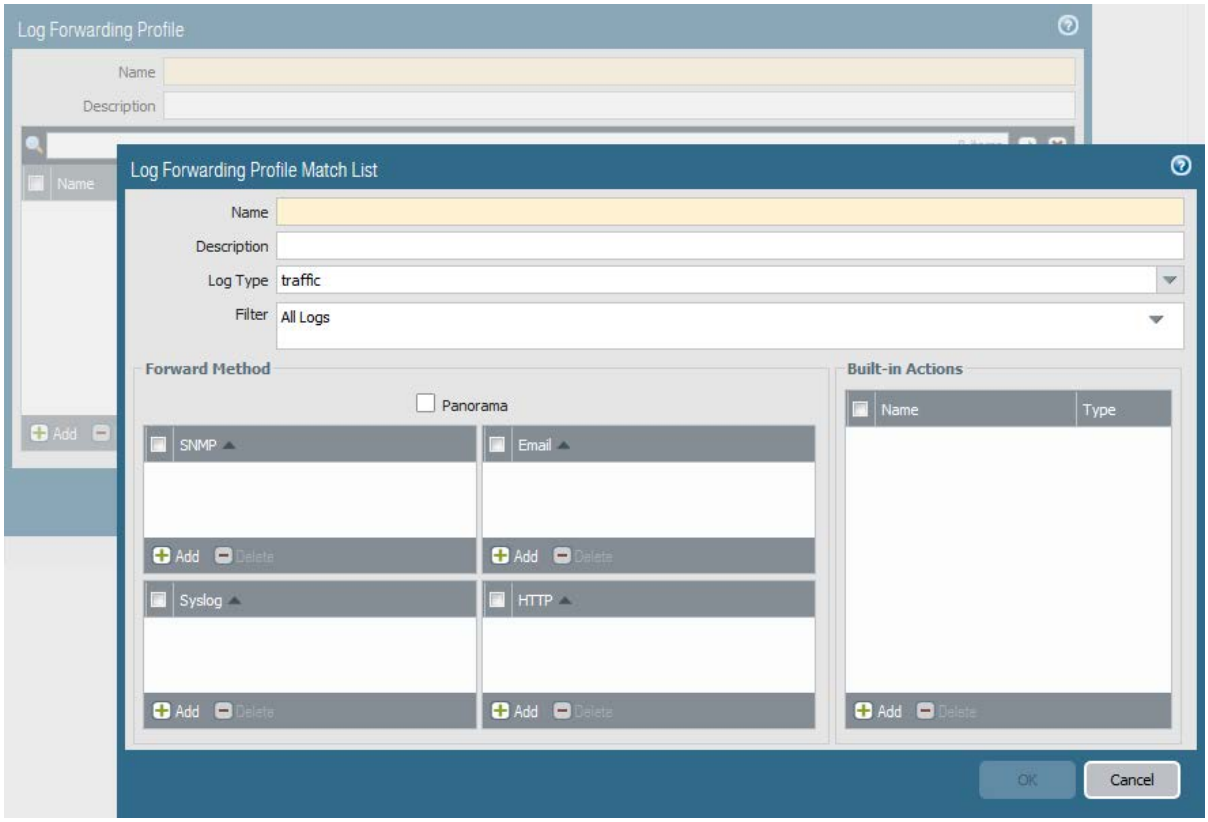
Any log event redirection causes a copy of the log event to be forwarded as specified. It is logged on the firewall as usual.

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



*Redirecting Log Events via **Device > Log Settings***

Use a Log Forwarding Profile to route Traffic, Threat, WildFire®, and other log events to other systems such as Panorama, SIEM products, syslog servers, and so on:



A Log Forwarding Profile

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/configure-log-forwarding

Palo Alto Networks also offer a cloud-based 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 Palo Alto Networks Application Framework API.

Further information about this service can be found here:
https://www.paloaltonetworks.com/documentation/10/cloud-services/logging-service-gsg

Sample questions

75. Which log format is not supported for log exports?
    A. SNMP trap
    B. syslog
    C. Apache log format
    D. HTTP
76. Which log type gets redirected using a Log Forwarding Profile?
    A. Config log
    B. Traffic log
    C. System log
    D. HIP Match log
77. Which of these enterprises cannot use the logging service?
    A. A top-secret NSA unit whose firewall protects them from the rest of a top secret government network.
    B. A mining operation in North Canada with intermittent Internet access.
    C. A data center with tens of millions of log entries per day
    D. A cruise ship with limited bandwidth most of the time (except when it is in port)

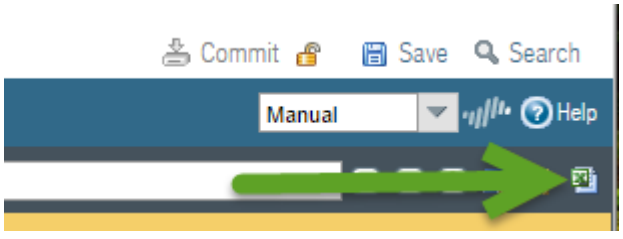
Interpret log files, reports, and graphs to determine traffic and threat trends

Logging and reporting are critical components of any security network. Being able 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 actionable information 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 WebUI. 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 divided into sections segmenting log data into related information. PAN-OS® 8.1 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.

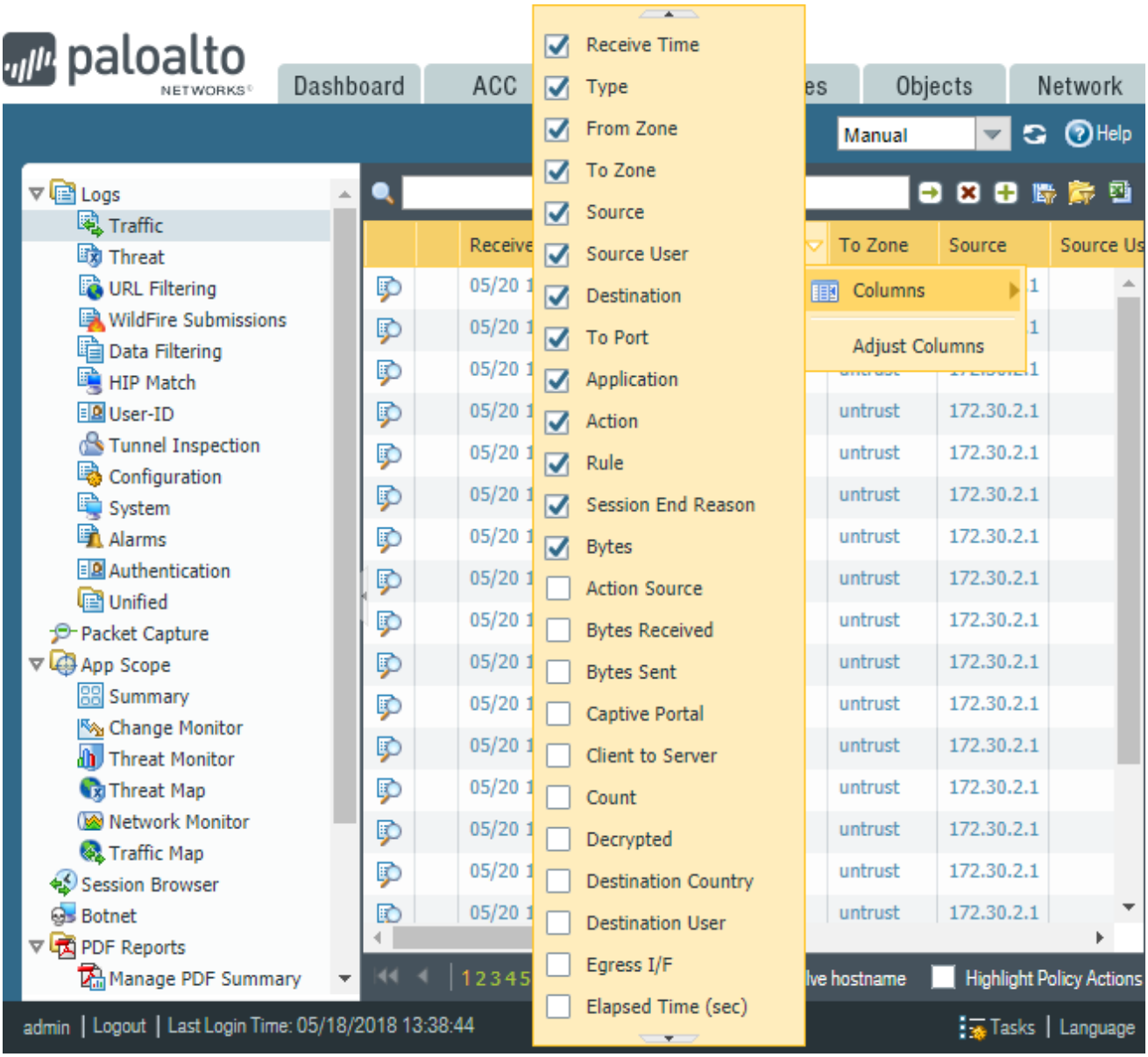
Each log provides similar features, making an organized presentation of desired data. Displayed log data can be exported in CSV format at any time.



The CSV export option available on any detailed log display

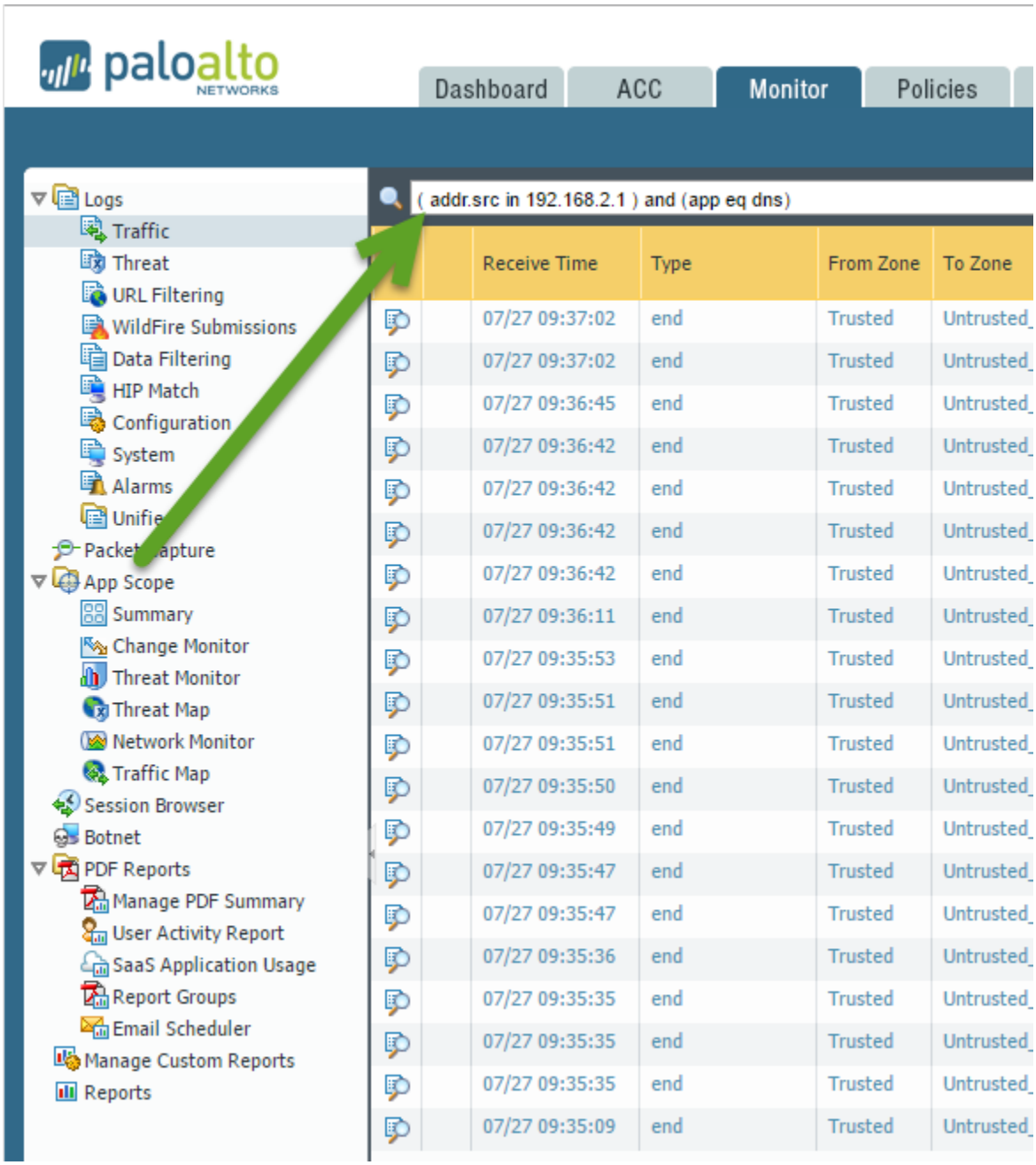
This export will include all detail for the displayed record even if it isn't visible in the chosen column displays.

You can see the entries in various logs using **Monitor > Logs**. You can configure which columns are displayed and their order and width.



Displayed columns can be chosen using the pull-down list appearing in any column header.

Each log display offers a powerful filtering capability facilitating the display of specific desired data.

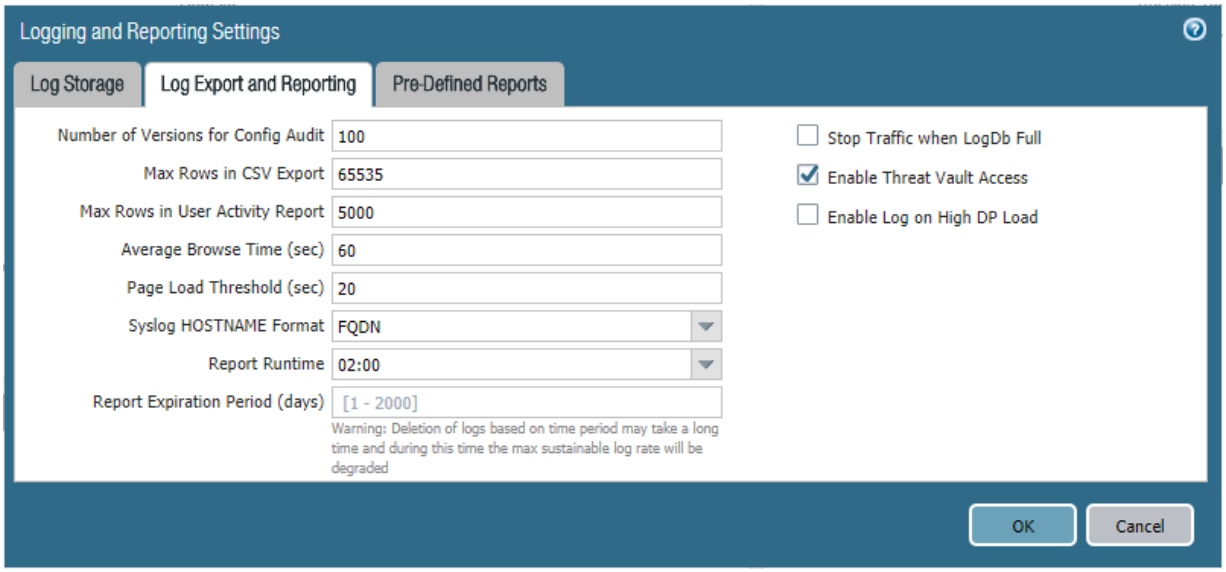


Filters can be added using two methods to eliminate the display of undesired entries.

Filters can be built and even stored for future use. Specific data on this functionality is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/view-and-manage-logs#_65083

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.

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

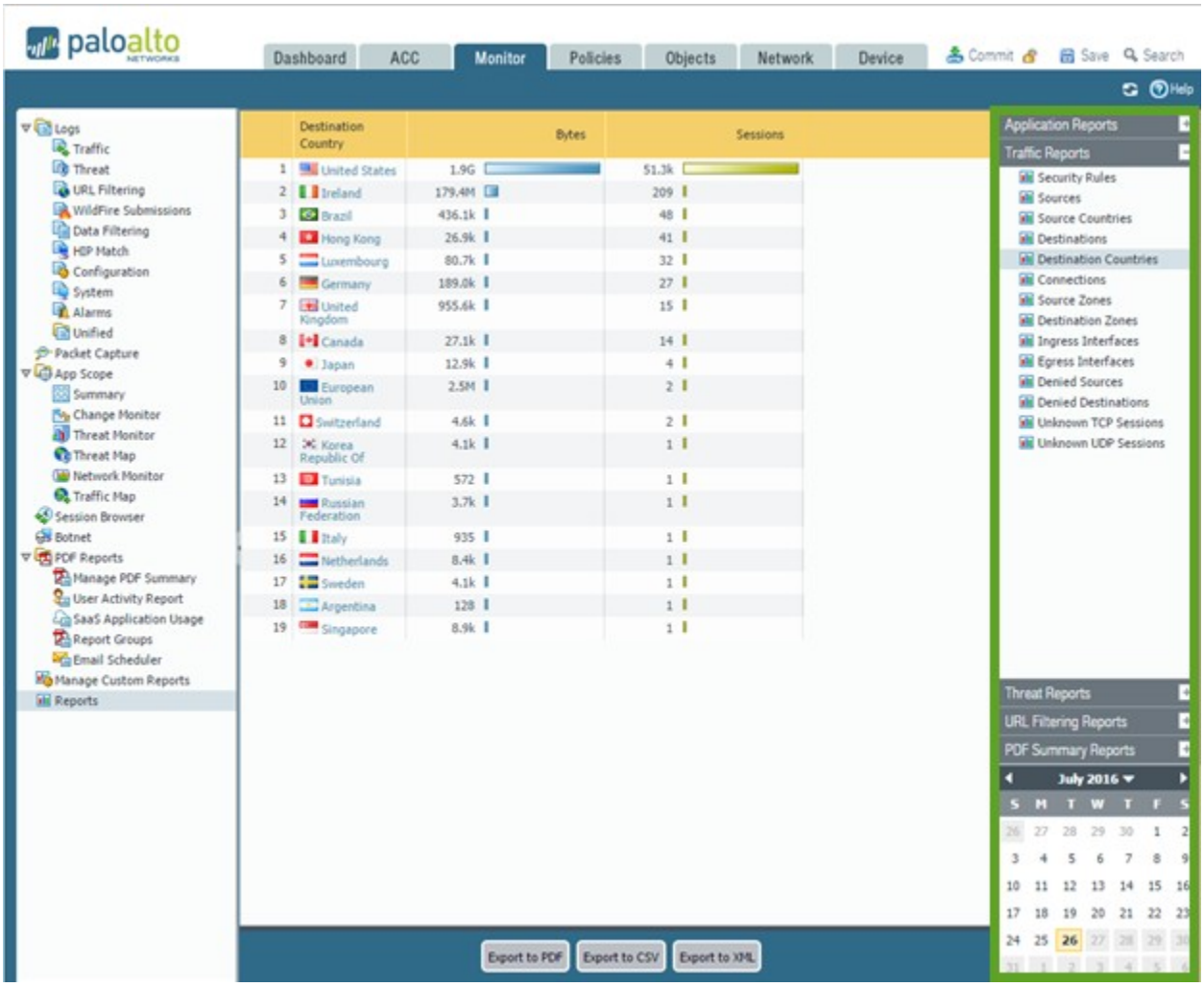


Settings for the repeating report database summarization process (two of the three tabs)

PDF Reports

The PDF Reports section offers many pre-defined 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. When these reports are chosen, they display their results for the previous day's traffic:



Predefined Report Browser showing choices of categories and specific reports on the right

The PDF Report 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/view-and-manage-reports/generate-custom-reports

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/view-and-manage-reports/generate-usergroup-activity-reports

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/view-and-manage-reports/manage-pdf-summary-reports#id5ffe964e-cb29-469d-911b-ed27f120e2cc

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 scheduled report output. Detailed information is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/use-the-app-scope-reports#_26529

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 also 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/use-the-application-command-center#73861

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, allowing 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: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/use-the-automated-correlation-engine#38973

Sample questions

78. 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)
79. 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

80. What product do you need to have to use event correlation?
    A. Next-generation firewall, PA-220
    B. Advanced endpoint protection
    C. Panorama
    D. GlobalProtect

Answers to sample questions

1. A
2. D, E
3. C

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

To 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/app-id/manage-custom-or-unknown-applications
- Create a Custom Application https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/app-id/use-application-objects-in-policy/create-a-custom-application

Sample questions

81. A customer's custom application uses DNS to transfer directory information, which needs to be filtered in a very different manner than normal DNS. How do you configure such 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 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.
82. 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

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

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 WebUI connection and then applied.

This process is discussed here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/install-content-and-software-updates#61072

PAN-OS® updates are managed in the **Device > Software** section of the WebUI. 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://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgrade-the-firewall-to-pan-os-81#ida59a23e6-923d-4fc7-abac-c7640d904e34

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 roll back (undo) PAN-OS® upgrades if required. Details are here:
https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/downgrade-from-pan-os-81

Updates to App-ID signature information can sometimes reclassify previously labeled traffic as something else 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/threat-prevention/best-practices-for-content-and-threat-content-updates

HA Firewalls
Dynamic updates are the responsibility of the individual firewalls to manage even when in passive mode. This task can be difficult if dynamic updates have no network path to the Palo Alto 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. Once 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://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgrade-the-firewall-to-pan-os-81/upgrade-an-ha-firewall-pair-to-pan-os-81#idab14f5f2-f662-4e5c-ba5b-2cc35993e2ec

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://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/manage-licenses-and-updates

Upgrading of Panorama-managed firewalls to PAN-OS® 8.1 is discussed here:
https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama

HA Cluster Firewall Updates Managed by Panorama
Panorama treats managed firewalls in HA pairs as individual firewalls for software update purposes.

Sample questions

84. If you need new dynamic content and the PAN-OS® version, in what order do you do it?
    A. It does not matter.

B. Update the PAN-OS® version first, then the dynamic content.
C. Update the dynamic content first, then the PAN-OS® version.
D. Update both at the same time.

85. In what order to you upgrade the different components of the firewall to a next version? (B)
    A. First the firewalls, then Panorama and the Log Collectors
    B. First Panorama and the Log Collectors, then the firewalls.
    C. The order does not matter.
    D. You manually upgrade Panorama, and doing so automatically upgrades the rest of the
86. How do you upgrade a high availability pair (A/P) to PAN-OS® 8.1? 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 have to upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

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. Making changes in the firewall WebUI stages these changes in the candidate configuration until a commit operation merges them, with the running configuration making them active.

Backing up versions of the running or candidate configuration enables you to later restore those versions on the firewall. A discussion about the basics is here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/firewall-administration/manage-configuration-backups#68133

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

Sample questions

87. What is the format of the configuration files?
    A. YAML
    B. JSON
    C. XML
    D. Some are in XML. Some in YAML

88. An organizatin has a QA network and a production network, each with its own firewalls. The change management policy dictates that any configuration change on the production firewalls has to be done by a script, which had been previously executed on the QA networks followed by extensive testing. What command do you use to copy a partial configuration file to the production firewalls?
    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.

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/ha-concepts
- What is HA-Lite on Palo Alto Networks PA-200 and VM-Series firewalls? 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links#id1df2d565-1765-4666-83b0-87652318e06f
- Set Up Active/Passive HA https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/set-up-activepassive-ha
- Set Up Active/Active HA https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/high-availability/set-up-activeactive-ha
- The information in section Given a scenario, identify how to design an implementation of firewalls in High Availability to meet business requirements leveraging the Palo Alto Networks Security Platform on p. 22.

Sample question

89. Which feature is not in active/active (A/A) mode?
    A. IPsec tunneling
    B. DHCP client
    C. link aggregation
    D. configuration synchronization

Identify the sources of information pertaining 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.

References

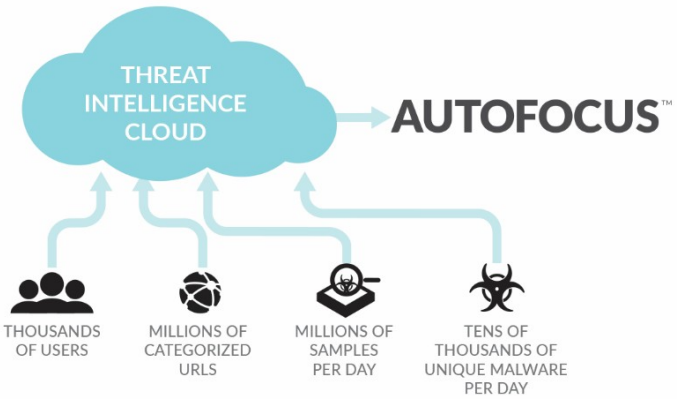
- SNMP Support https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/snmp-monitoring-and-traps/snmp-support
- Monitor Statistics Using SNMP https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/snmp-monitoring-and-traps/monitor-statistics-using-snmp
- Supported MIBs https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/snmp-monitoring-and-traps/supported-mibs

Sample question

90. 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

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. With AutoFocus, you can 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 keep up 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.

Enabling 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence.html

References

- AutoFocus at a glance
  https://www.paloaltonetworks.com/resources/datasheets/autofocus-at-a-glance
- AutoFocus Administrator's Guide, especially the dashboard
  https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/autofocus/autofocus_admin_guide.pdf

Sample question

91. Which ability does AutoFocus not have?
    A. distinguish between attacks that attempt to exfiltrate data (violate confidentiality) and attacks that attempt to modify it (violate integrity)
    B. display the processes started by specific malware
    C. display the network connections used by specific malware
    D. distinguish between commodity attacks and advanced persistent threats (APTs) directed against the customer's organization or industry

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, BrightCloud and PAN-DB database updates and lookups, 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.

References

- **Device > Dynamic Updates** https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/device/device-dynamic-updates
- Install Content and Software Updates
- Manage New App-IDs Introduced in Content Releases https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/install-content-and-software-updates
- See the New and Modified App-IDs in a Content Release https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-ids-since-last-content-version

Sample question

92. 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

Identify the relationship between Panorama and devices as it pertains 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 installing 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.

When deploying updates, 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, if you want to reduce the traffic load on the MGT interface by using another interface for devices to retrieve updates, you can configure Panorama to use multiple interfaces.

HA firewalls are expected to have the same version content updates. When firewalls are in a HA pair, they 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 will 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.

References

- Deploy Updates to Firewalls, Log Collectors and WildFire Appliances Using Panorama https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama#_76612
- Supported Updates https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/supported-updates

Sample questions

93. Which two types of device can receive the Antivirus content update? (Choose two.)
    A. Log Collector
    B. firewall
    C. WildFire®
    D. AutoFocus
    E. MindMeld
94. Within the 8.1 version, can a content update and a software version be incompatible? If so, in what way? (Choose the most accurate answer.)
    A. No, they are always compatible.
    B. Yes, newer content updates don't work with older versions of the software.
    C. Yes, newer versions of the software don't work with older versions of the content update.
    D. Yes, so you need to always update them at the same time.

Exam Domain 4 – Configuration Troubleshooting

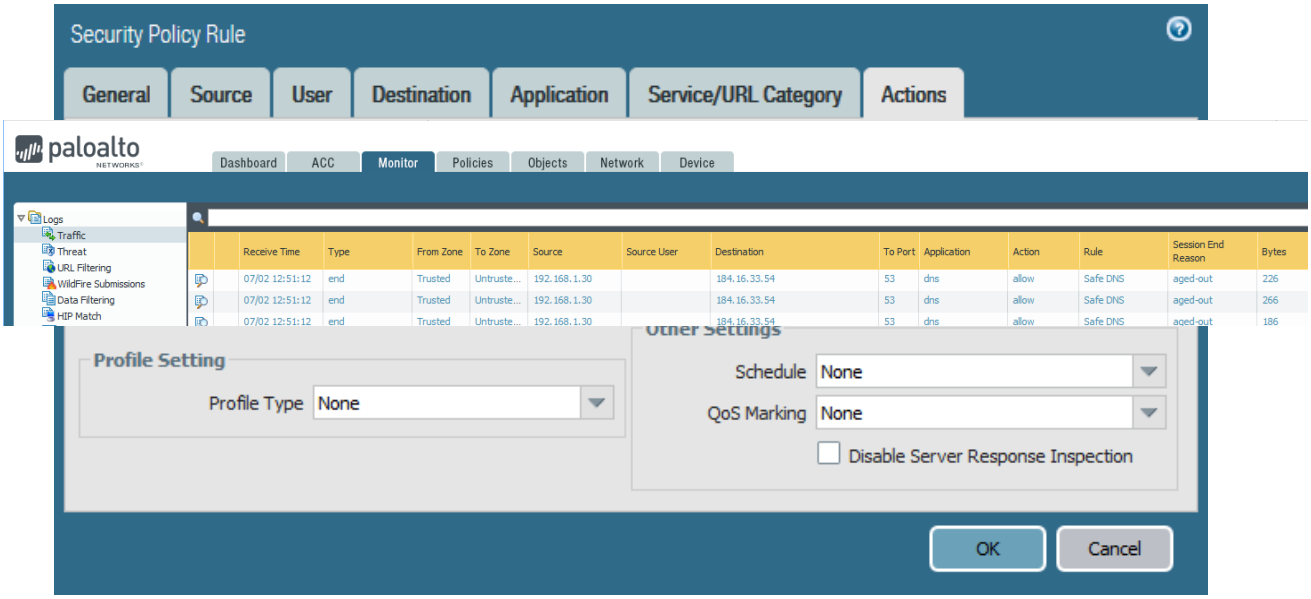
Identify system and traffic issues using WebUI and CLI tools.

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

Transit Traffic Not Passing Through as Expected

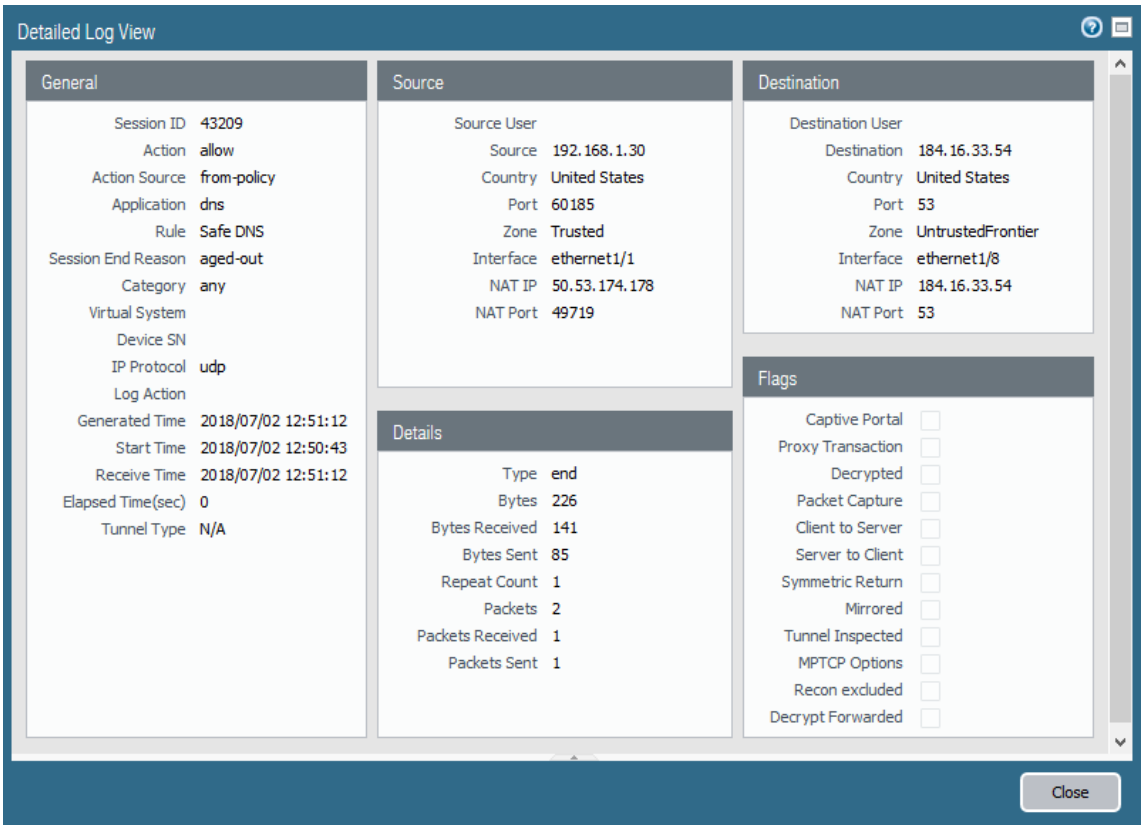
When traffic is not transiting a firewall when expected to do so there are three primary information sources available in the Web-based Management UI. There are many beyond these three but troubleshooting usually starts with these.

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.

The following capture shows the details of one of the entries listed .

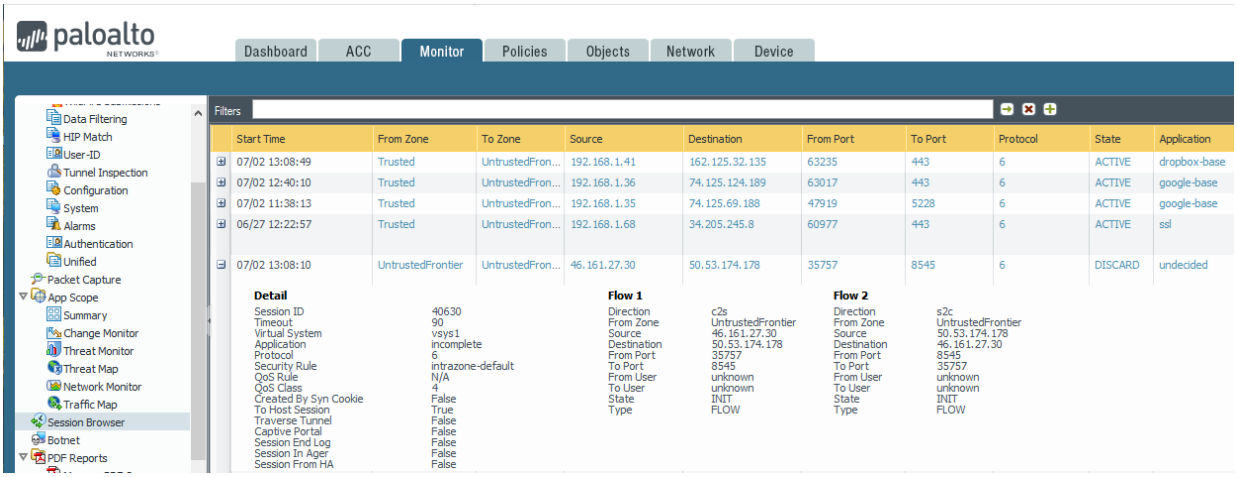


The presence of a log entry confirms that properly formed traffic has reached the firewall and has been evaluated by a Security policy rule. Traffic could be processed without reaching a session end, which would result in no log entry yet. The Session Browser allows troubleshooting of open sessions that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

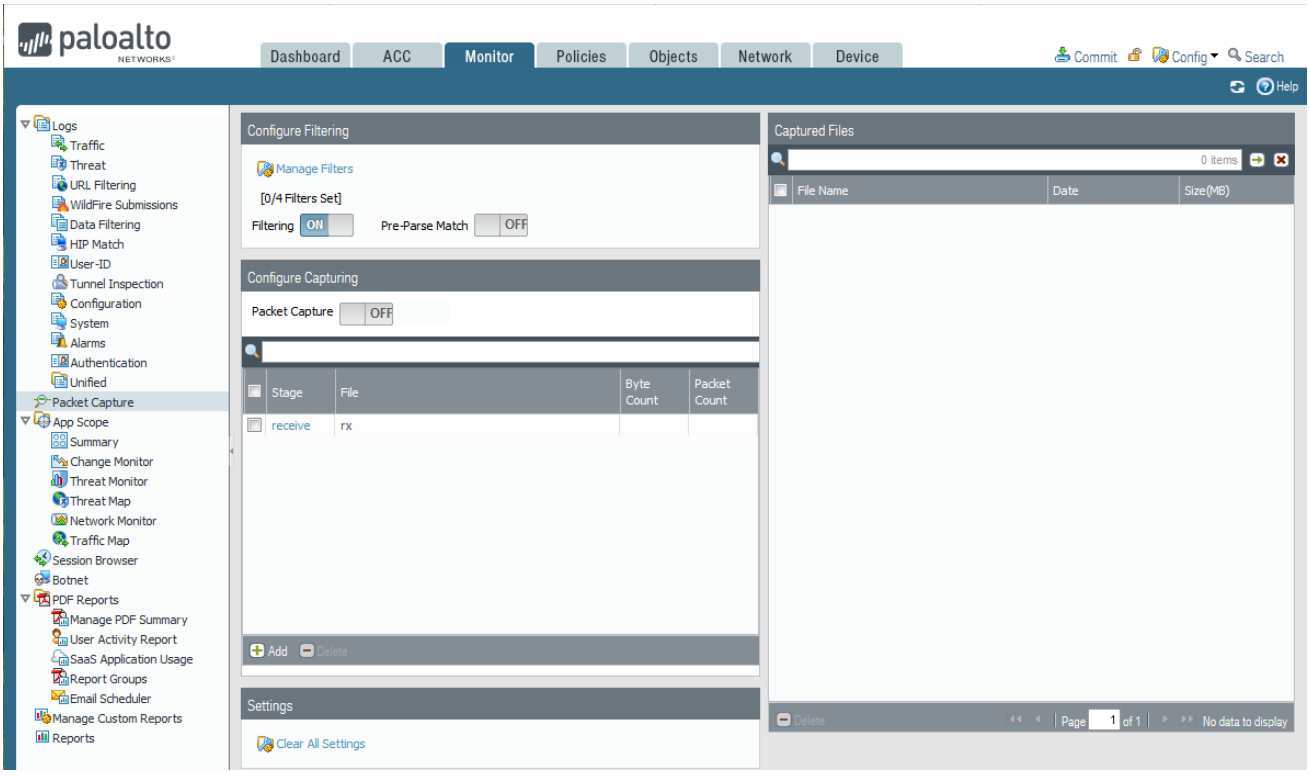
The detailed session information should be used to evaluate the handling of the traffic. The Source and Destination blocks display header data and confirm potential NATs being applied. The General block confirms the action taken by the Security policy rule and the rule's name, App-ID, protocol, time seen. and the reason the session ended. The Details block 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, the Session Browser can be used to display all open sessions currently known to the firewall. Each session can be expanded to allow you to examine details.



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 usage 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.

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 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.

  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- 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 are composed of 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/debug-log filters. For example, if a route lookup fails, a 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 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 is often used by experienced administrators for troubleshooting. This section provides only the briefest mention of basic CLI tools. The "Refences" section at the end of this section includes more complete information sources.

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 WebUI. 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 **s**how 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 WebUI can be accessed from the CLI. Each configuration step used in the WebUI has a command line equivalent. See the "References" section for the location of a detailed discussion.

References

- Log Types and Severity Levels
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/view-and-manage-logs/log-types-and-severity-levels
- **Monitor > Logs**
  https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/monitor/monitor-logs#_58165
- CLI Cheat Sheet: Device Management
  https://www.paloaltonetworks.com/documentation/81/pan-os/cli-gsg/cli-cheat-sheets/cli-cheat-sheet-device-management#_44428
- CLI Cheat Sheet: Networking
  https://www.paloaltonetworks.com/documentation/81/pan-os/cli-gsg/cli-cheat-sheets/cli-cheat-sheet-networking#_10944
- Interpret VPN Error Messages
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages

Sample questions

95. 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)

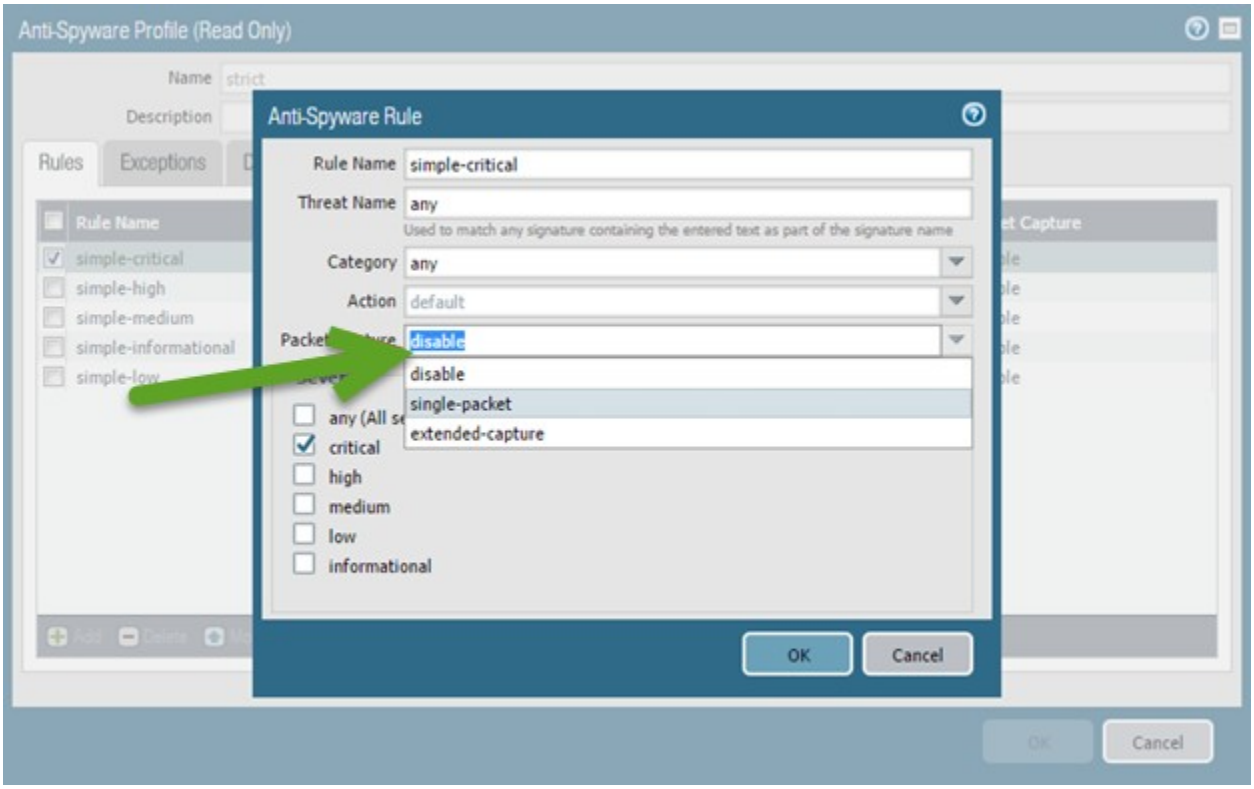
96. You can't get to the web interface. How do you check from the command line if it is running?
    A. ps -aux | grep appweb
    B. ps -aux | match appweb
    C. show system software status | grep appweb
    D. show system software status | match appweb
97. Which log file shows that a connection with an LDAP server was dropped?
    A. Traffic Log
    B. System Log
    C. User-ID Log
    D. Authentication Log

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 WebUI 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:



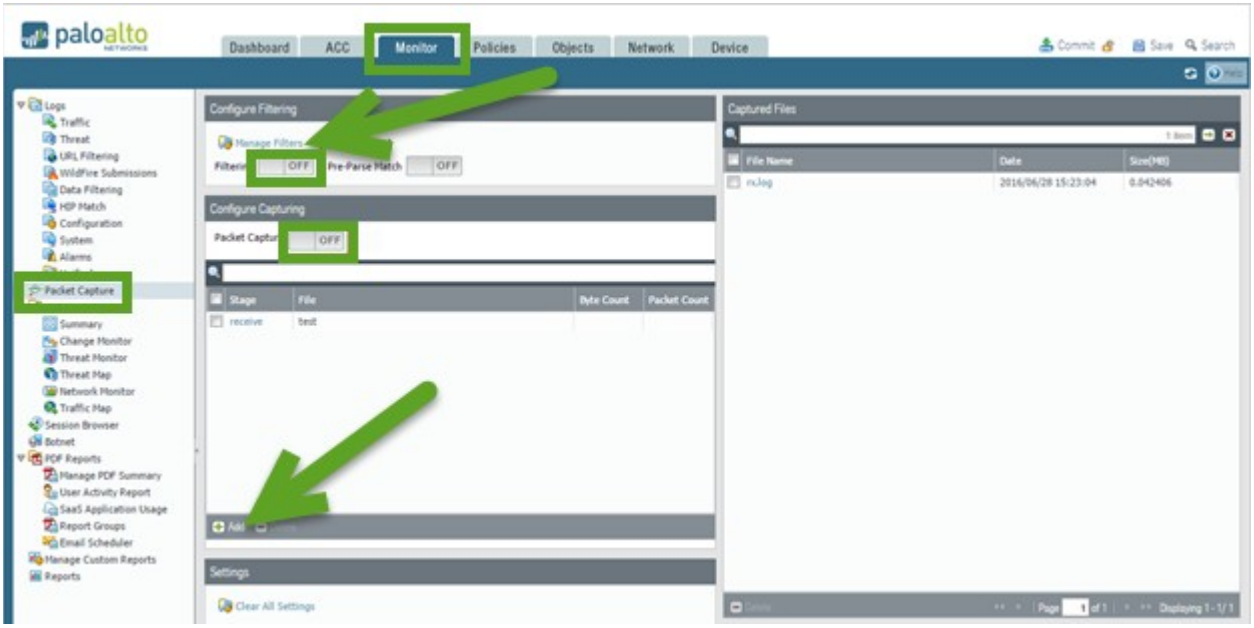
Configuring a packet capture response to the detection of spyware

Information about configuring threat detection captures and accessing the captured data is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/take-packet-captures/take-a-threat-packet-capture

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

Manual Packet Captures

Packet captures can be conducted on demand both from the WebUI and the CLI. WebUI 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 WebUI 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® WebUI 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/take-packet-captures/take-a-custom-packet-capture

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 WebUI 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

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.

Sample question

98. Which Security Profiles do not have a packet capture option?
    A. Antivirus
    B. Anti-spyware
    C. Vulnerability Protection
    D. URL Filtering
99. 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
100. Under which circumstances do you use tcpdump on the next-generation firewall?
    A. Never
    B. CLI capture of packets on traffic interfaces
    C. CLI capture of packets on the management interface
    D. It is the CLI command for the traffic interfaces and the management interface.

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

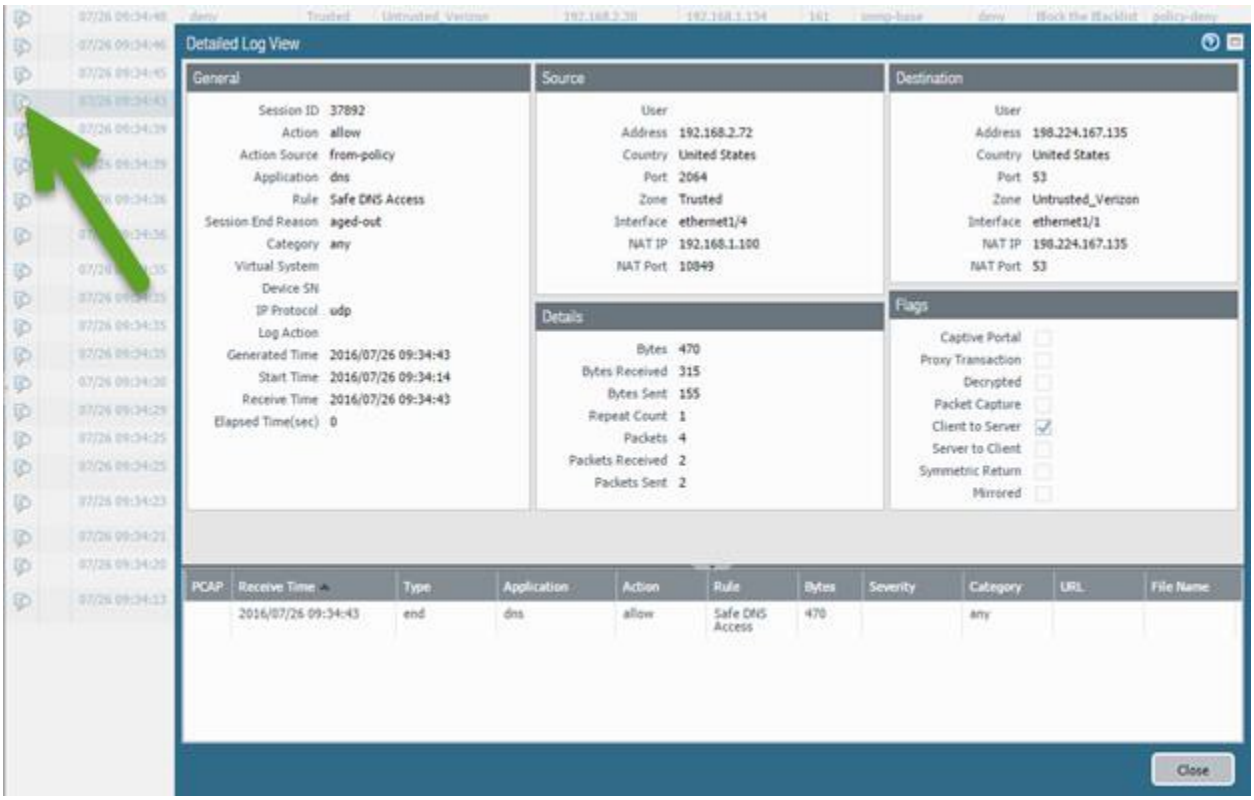
The Management port is isolated from internal connectivity for security purposes. If the Management port requires internet access, its traffic must be routed out of the firewall and through other network infrastructure that provides this connectivity. The traffic often is routed back to a traffic port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

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.

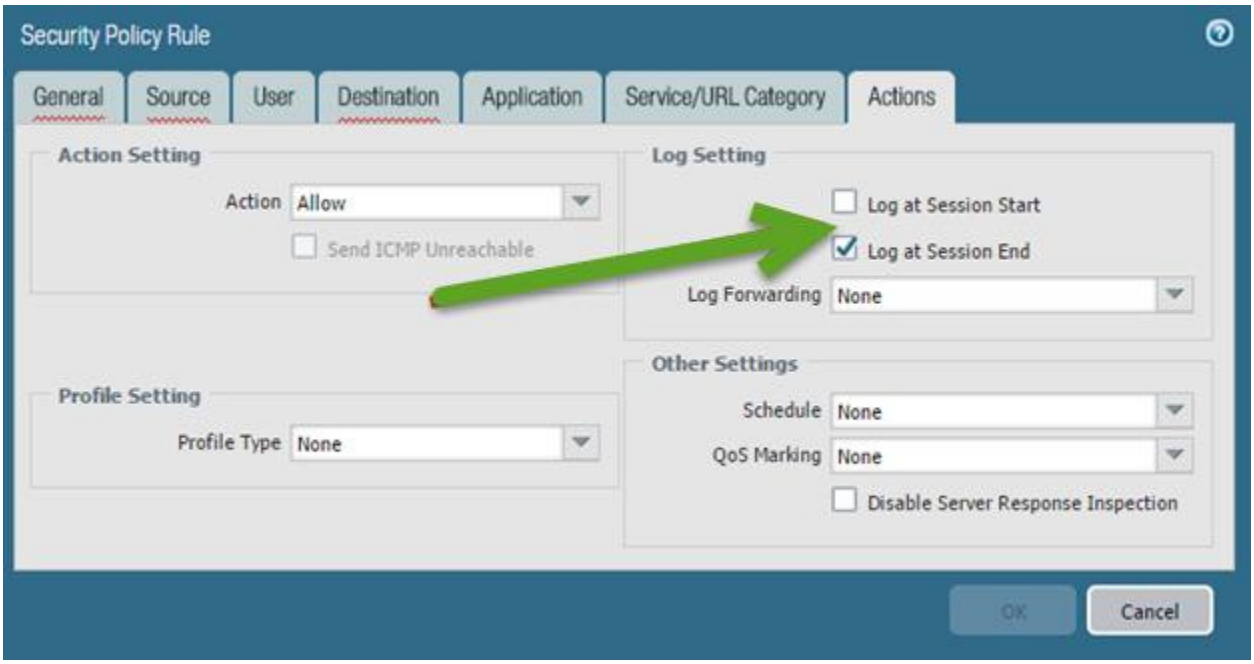
The WebUI provides several important tools. The path **Monitor > Logs > Traffic log** provides session summary information. Log entries for traffic are generated as specified in Security policies. The typical configuration specifies that log entries are created when a session ends. Use the magnifying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



Log entry detail

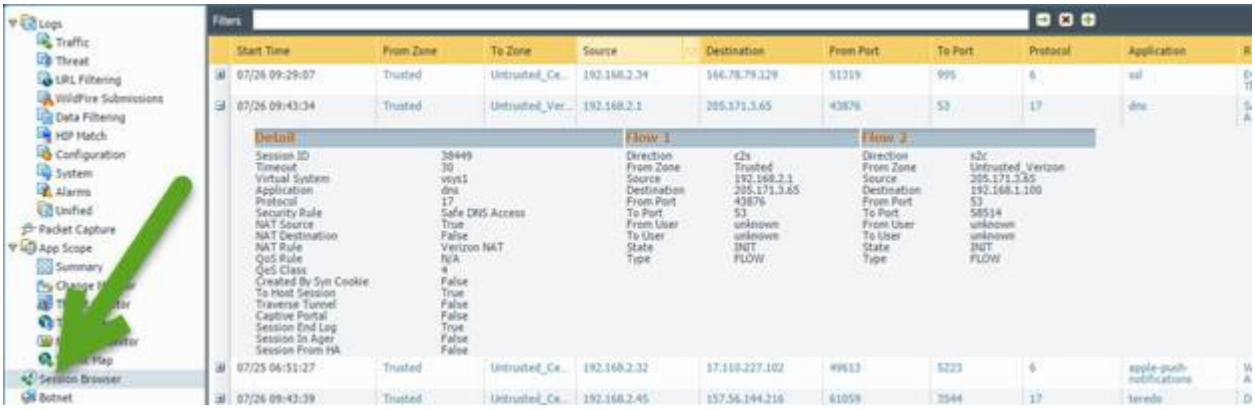
Details found here include much information for troubleshooting: the Security action, the firewall policy allowing it through, the assigned App-ID, zones, and the ingress and egress interfaces. NAT details and flags attesting to other handling details also appear. Examine this data to get valuable insight 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:

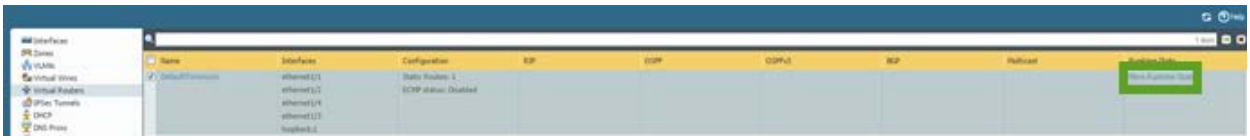


View open sessions within the session browser

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.

The CLI show commands will assist with troubleshooting. The WebUI 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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/monitoring/take-packet-captures#62168

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 WebUI:



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 question

101. 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
102. 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
103. 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

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-overview

- How to Implement and Test SSL Decryption
  https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719

Sample questions

104. 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.

105. 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.

106. Which of the following encryption algorithms 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

Identify certificate chain of trust issues

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies
- Certificate Management https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/certificate-management
- How to Install a Chained Certificate Signed by a Public CA https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Install-a-Chained-Certificate-Signed-by-a-Public-CA/ta-p/55523

Sample questions

107. 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.
108. Which field is mandatory in the subject field of a certificate?
    A. Organization
    B. Organizational Unit
    C. Common Name
    D. Locale
109. 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

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/virtual-routers
- Site-to-Site VPN with Static and Dynamic Routing
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-and-dynamic-routing
- Static Routes
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/static-routes/static-route-overview
- RIP
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/rip
- OSPF
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/ospf
- BGP
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/bgp

Sample questions

110. 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**

111. 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.

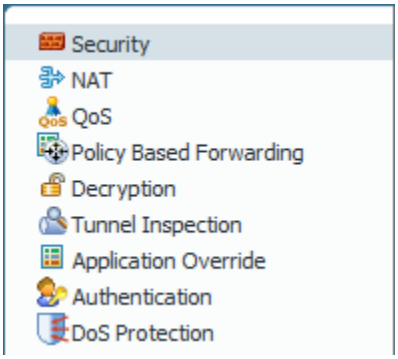
112. The organization has two links to the Internet, one 100Mbps and the other 10Mbps. The firewall balances them using equal-cost multi-path (ECMP) in the virtual router. Which load balancing ECMP setting does the organization need to use to optimize network resources?
    A. Balanced Round Robin
    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.

Exam Domain 5 – Core Concepts

Identify the correct order of the policy evaluation based on the packet flow architecture

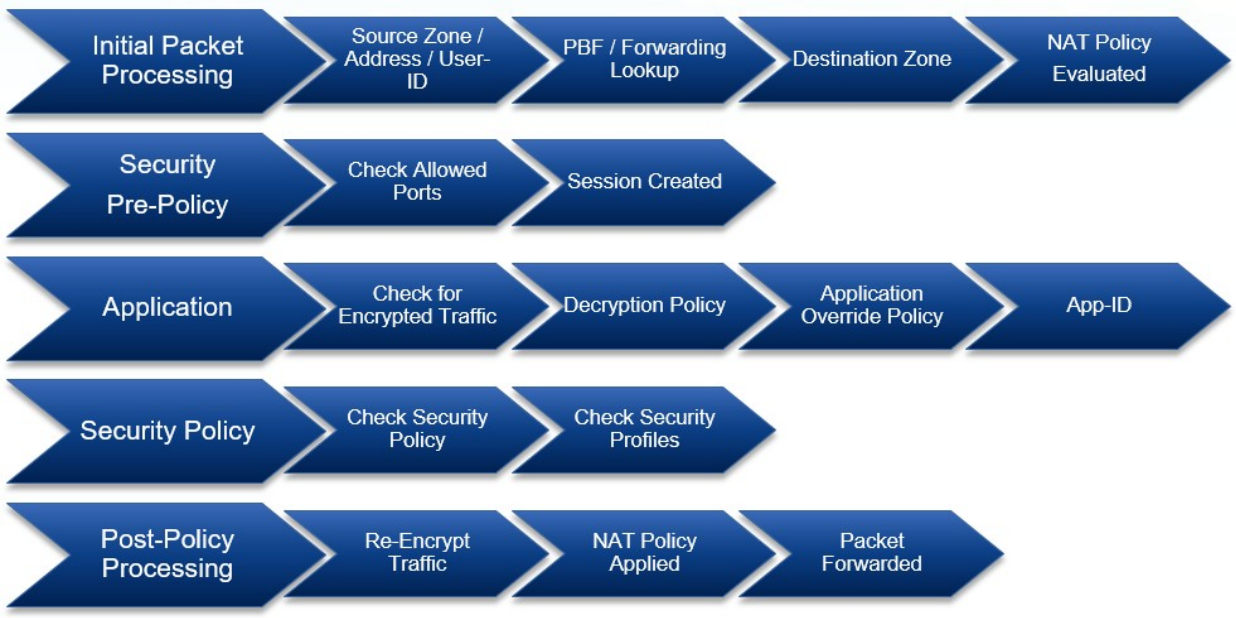
Policies

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:



All traffic processed by the firewall follows this sequence of events.

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/policy-types

CLI test Command

The firewall CLI includes an advanced traffic-handling prediction command, `test`. The `test` command includes a specification of the rulebase to test and a description of the traffic to present. The command result returns the processing outcome, including the policy that handles the traffic (if any) and the result.

A dated but still useful article with examples is here:
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Test-Security-NAT-and-PBF-Rules-via-the-CLI/ta-p/55911

Sample questions

113. 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
114. Which two statements are correct regarding policy evaluation? (Choose two.)
    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.
115. 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

Given an attack scenario, identify the Palo Alto Networks appropriate threat prevention component to prevent/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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/set-up-a-basic-security-policy#79320

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://www.paloaltonetworks.com/documentation/81/best-practices/best-practices-internet-gateway#60768

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://www.paloaltonetworks.com/documentation/81/best-practices/best-practices-internet-gateway/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles#48239

Sample questions

116. A URL Filtering Profile is part of which type of identification?
    A. App-ID
    B. Content-ID
    C. User-ID
    D. Service
117. 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
118. 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

Identify methods for identifying users

User-ID and Mapping Users

The User-ID feature of the Palo Alto NGFW enables you to create policies and perform reporting based on users and groups rather than on individual IP addresses.

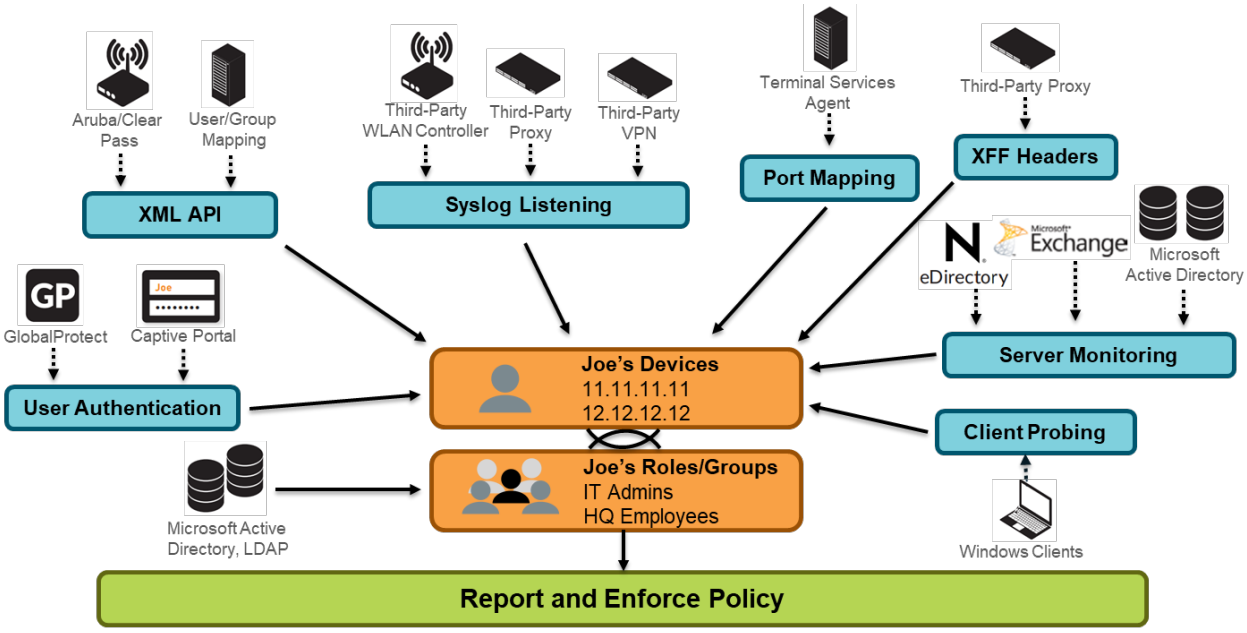
User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, enabling you to associate application activity and policy rules to users and groups—not just IP addresses. Furthermore, with User-ID enabled, the Application Command Center (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:



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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/user-id

Design and deployment considerations for complex environments are here:
https://live.paloaltonetworks.com/t5/Configuration-Articles/Architecting-User-Identification-

Deployments/ta-p/60904?attachment-id=2853

Best practices for User-ID implementations are here:
https://live.paloaltonetworks.com/t5/Configuration-Articles/User-ID-best-practices/ta-p/65756?attachment-id=3509
and here:
https://live.paloaltonetworks.com/t5/Learning-Articles/Best-practices-for-securing-User-ID-deployments/ta-p/61606

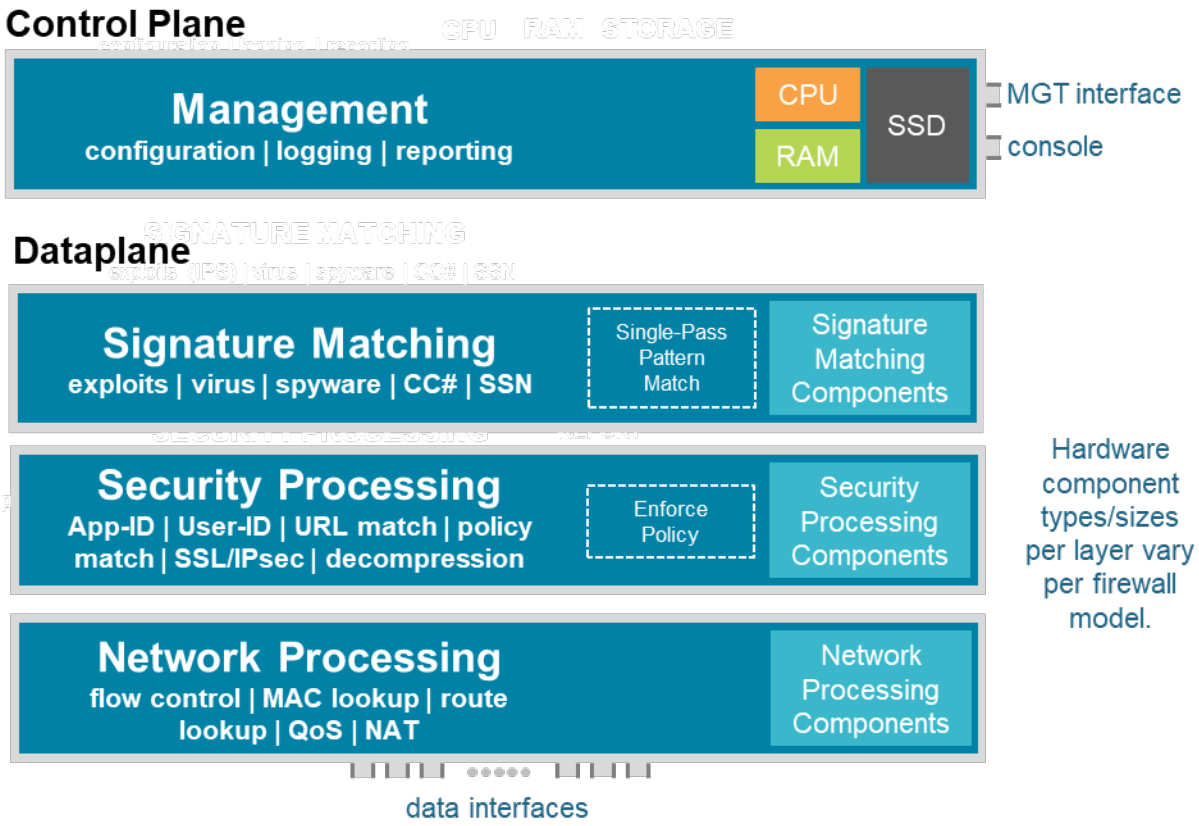
Sample questions

119. 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
120. 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
121. 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

Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks firewall

Management 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

The Management Network and Console connector terminates directly on this plane. The following functions are assigned to the data plane:

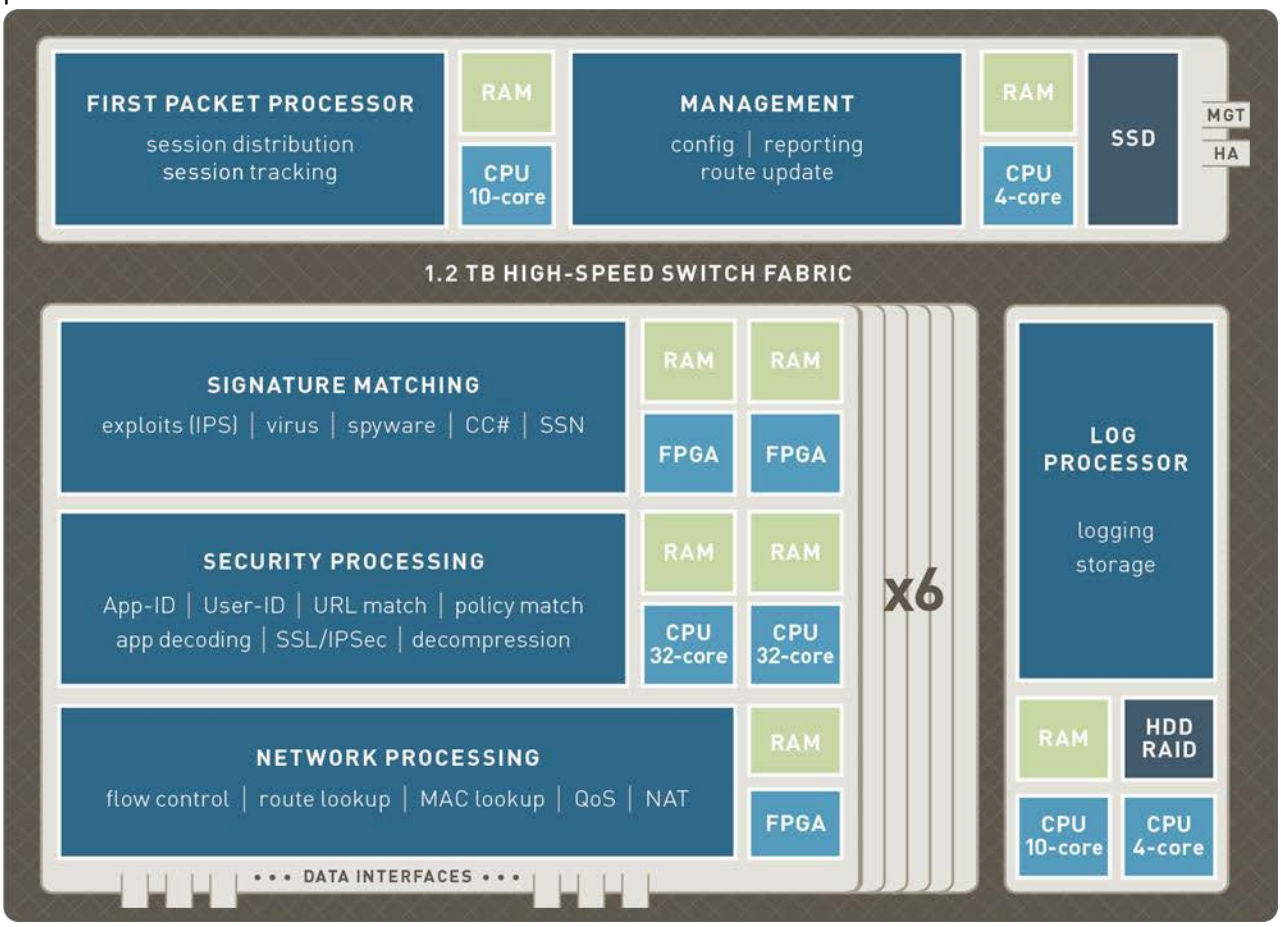
- Signature Match Processor:
  - All Content-ID and App-ID services
- Security Processors:
  - Session management
  - Encryption/decryption
  - Compression/decompression
  - Policy enforcement
- Network Processor:
  - Route
  - ARP
  - MAC lookup
  - QoS
  - NAT

- 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

Dedicated log collection and processing is implemented on a separate card. The following diagram provides an overview of the PA-7000 Series architecture:



PA-7000 Series architecture

Sample questions

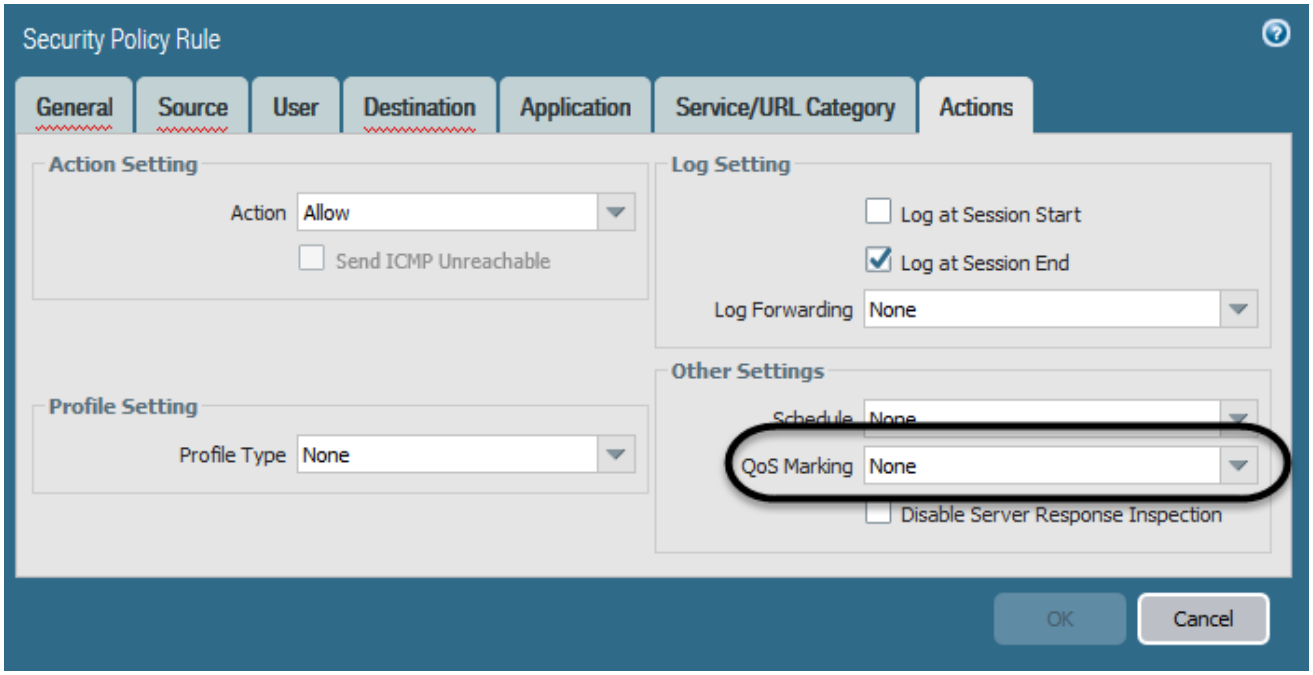
122. On a PA-7000, which management function runs on a separate card?
    A. configuration management
    B. logging
    C. reporting
    D. The web user interface
123. Does the next-generation firewall use FPGA? If so, in which plane or planes?
    A. No, never
    B. Yes, on the data plane, but only 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
124. Which of the following functions residents on the management place?
    A. App-ID matching
    B. Route lookup
    C. Policy match
    D. Logging

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.

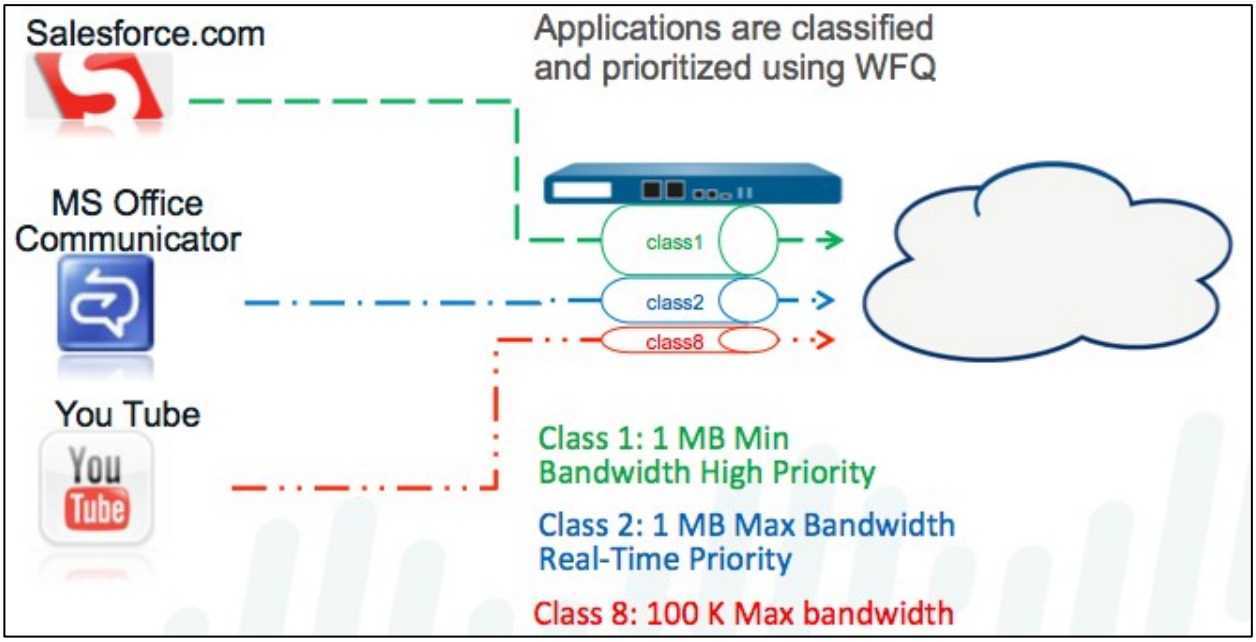
Palo Alto Networks QoS provides an “Application Aware” QoS service that can be driven by the traffic’s App-ID. The firewall’s QoS implementation is a self-contained system local to the firewall that can consider existing QoS packet markings but does not act directly on them. Traffic is evaluated against 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.



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.

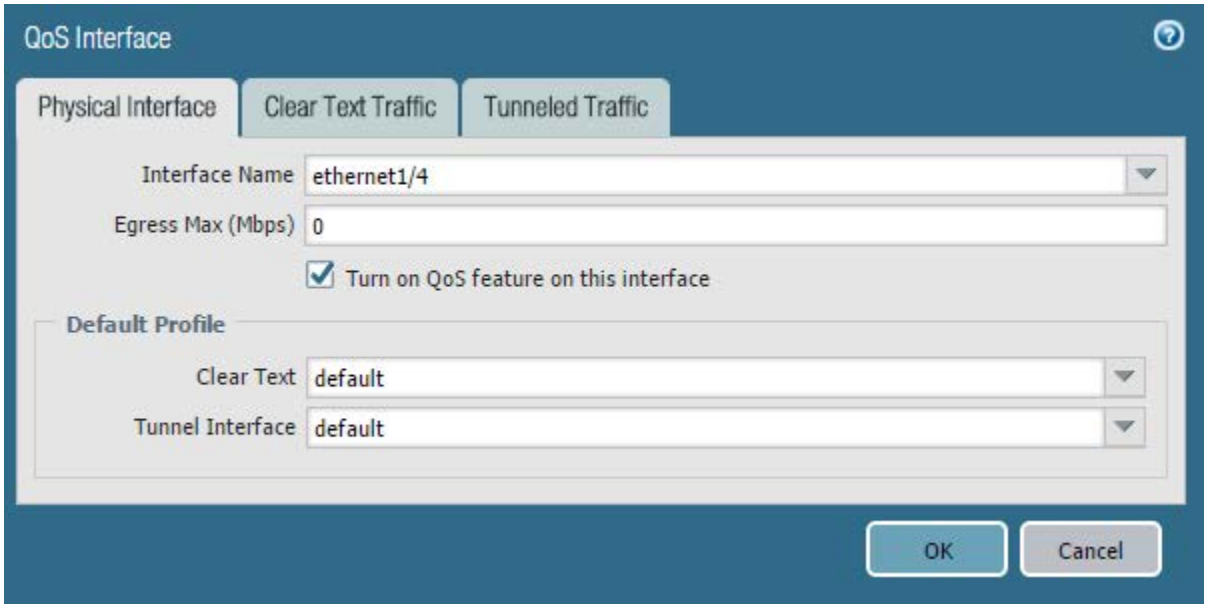
The number of packets dropped is determined by their assigned Priority. A real-time Priority setting means no packet dropping will be performed. High-, medium-, and low-priority settings indicate that greater levels of random packet dropping are performed during movement down the scale. No packets are 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

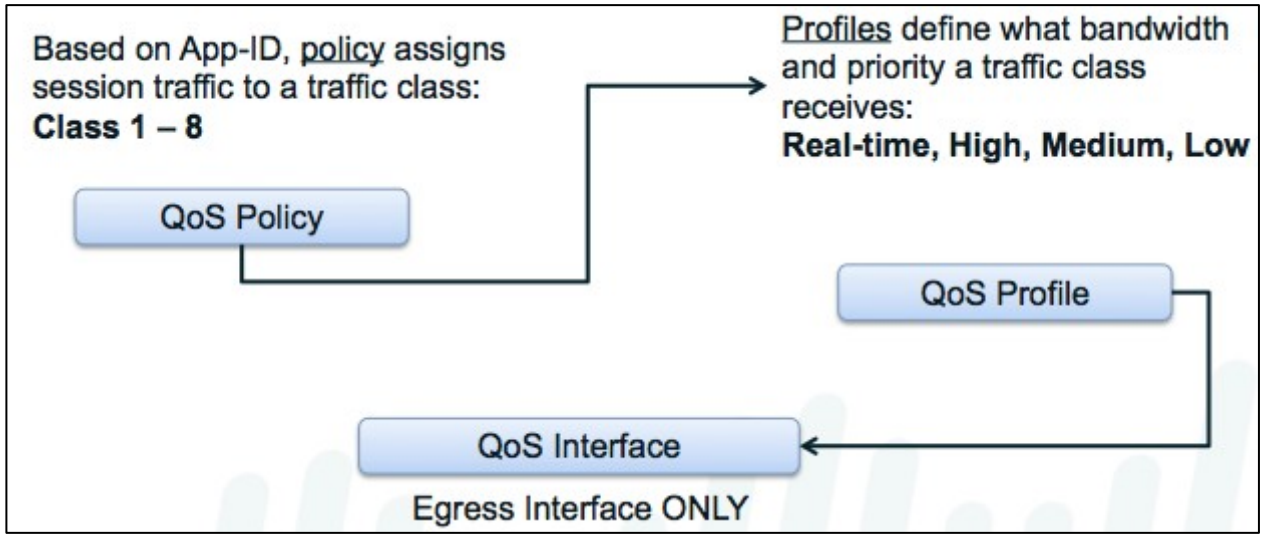
QoS Profiles prioritize specified traffic.

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.

References

A detailed discussion of QoS is here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/quality-of-service

Sample questions

125. 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
126. How many QoS classes does the next-generation firewall support?
    A. 4
    B. 8
    C. 16
    D. 32

127. 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).

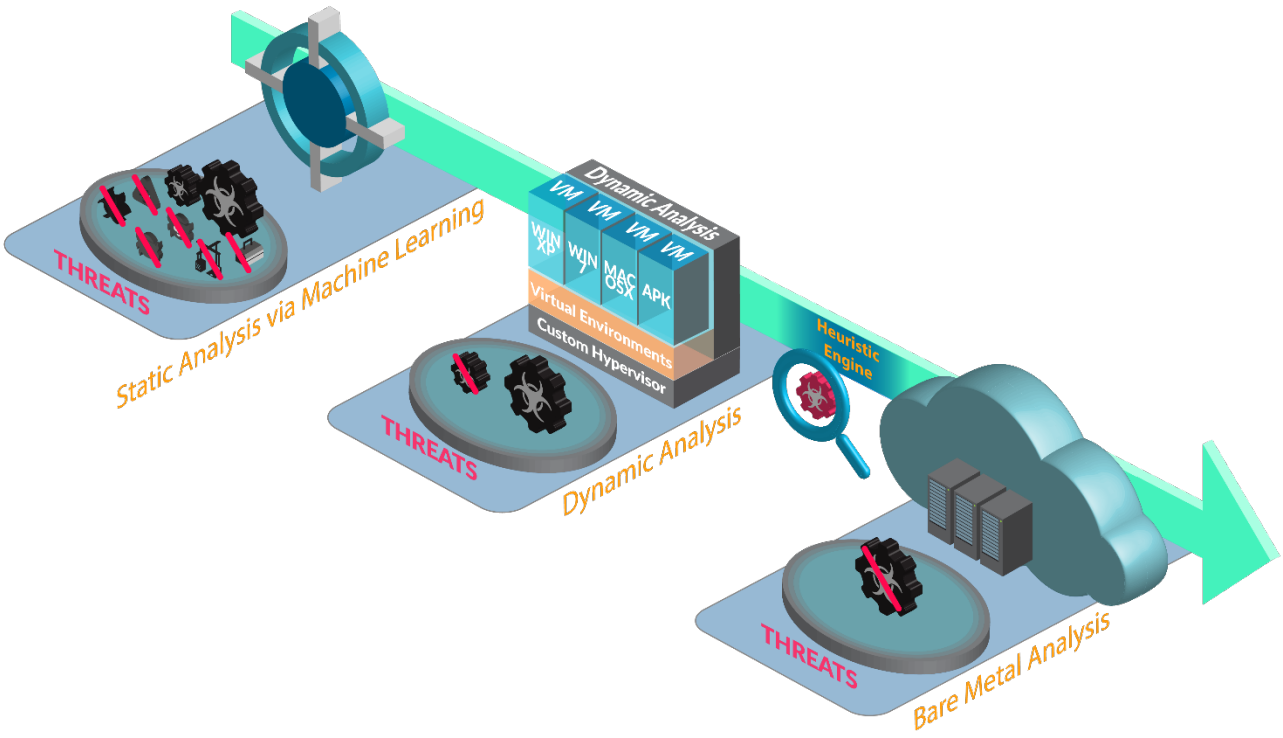
Identify the fundamental functions and concepts of WildFire

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 can then 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 diagram 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:

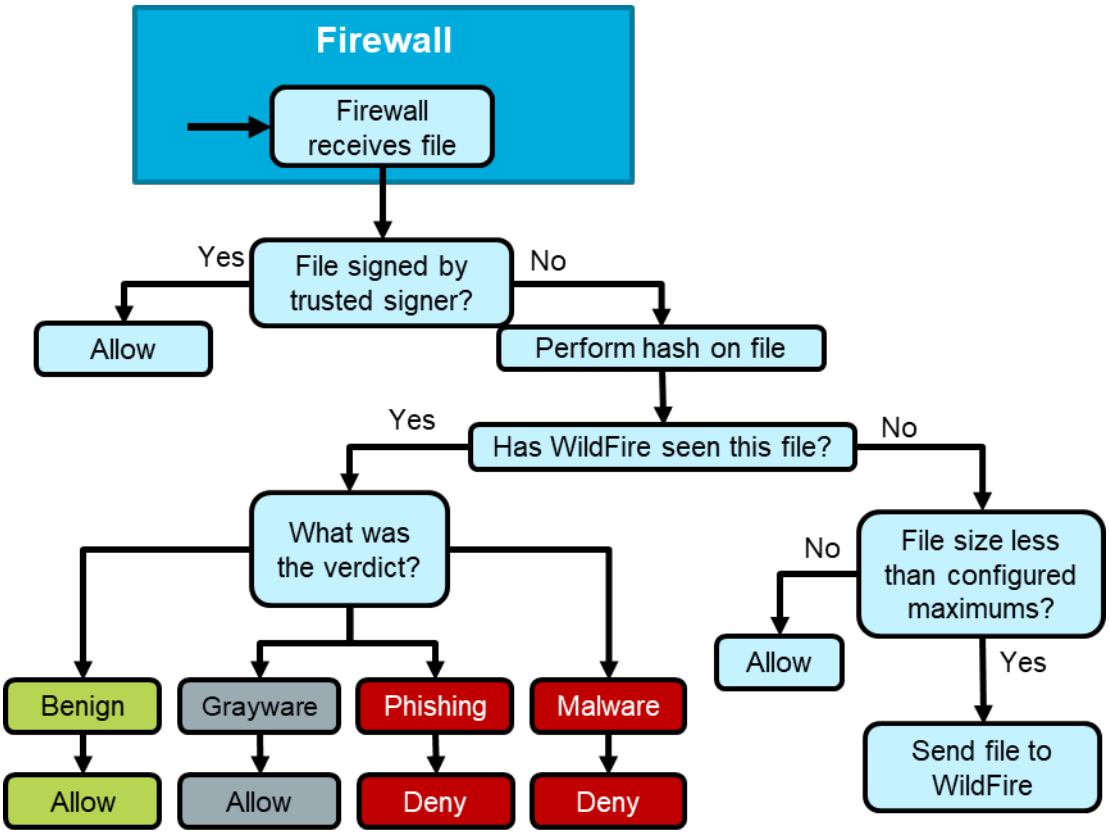
- Static analysis: Detects known threats by analyzing the characteristics of samples prior to execution
- Machine learning: Identifies variants of known threats by comparing malware feature sets against dynamically updated classification systems
- Dynamic analysis: A custom-built, evasion-resistant virtual 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.



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://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin
- The use of WildFire® in firewall profiles is outlined here: https://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin/submit-files-for-wildfire-analysis/forward-files-for-wildfire-analysis

Sample questions

128. Which file type is not supported by WildFire®?
    A. iOS applications
    B. Android applications
    C. Windows applications
    D. Microsoft Excel files

129. The firewall will skip the upload to WildFire® in which three cases? (Choose three.)
    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 10MB.
    F. The file is transferred through HTTPS.

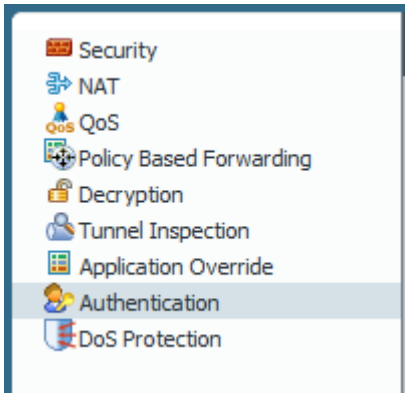
130. Which of these features is not supported on the WF-500 appliance?
    A. Bare metal analysis
    B. Microsoft Windows XP 32 bit analysis
    C. Microsoft Windows 7 64 bit analysis
    D. Static analysis

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.

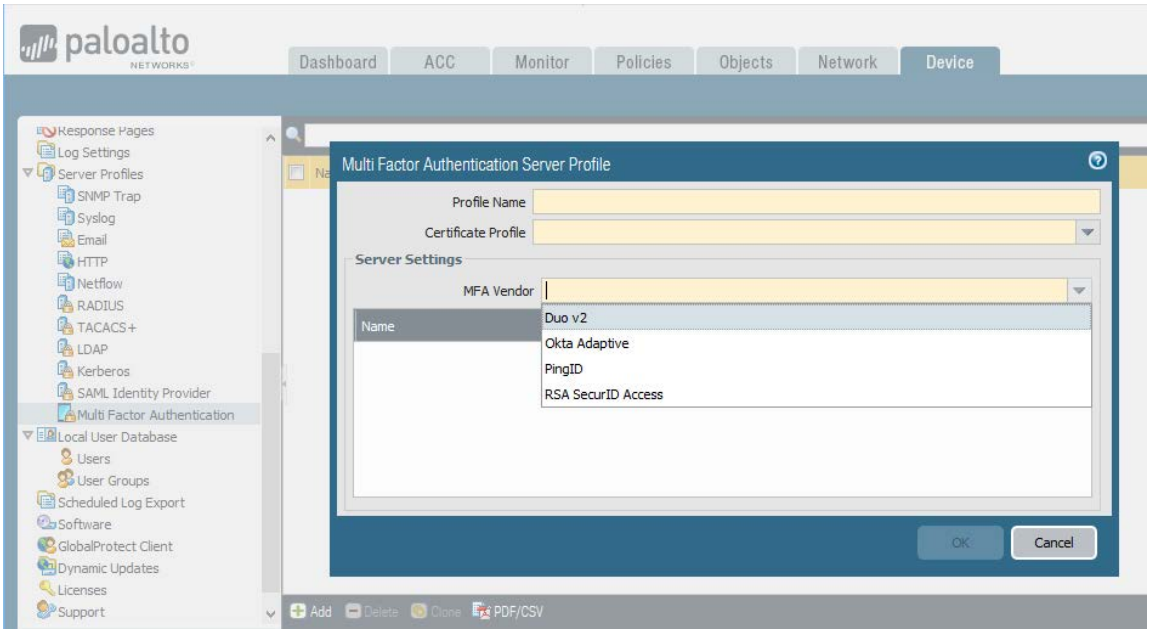
The firewall makes implementation of MFA in your network easy by integrating directly with several MFA platforms (Duo v2, Okta Adaptive, and PingID) and integrating through RADIUS with all other MFA platforms.

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.



References

- Multi-Factor Authentication https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication/authentication-types/multi-factor-authentication
- Authentication Policy https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication/authentication-policy

Note: You can see more information on this subject under the heading Identify methods for Authorization, Authentication, and Device Administration on p. 33.

Sample questions

131. What are the two purposes of multi-factor authentication? (Choose two.)
    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

132. Which of these MFA factors is not supported by the next-generation firewall?

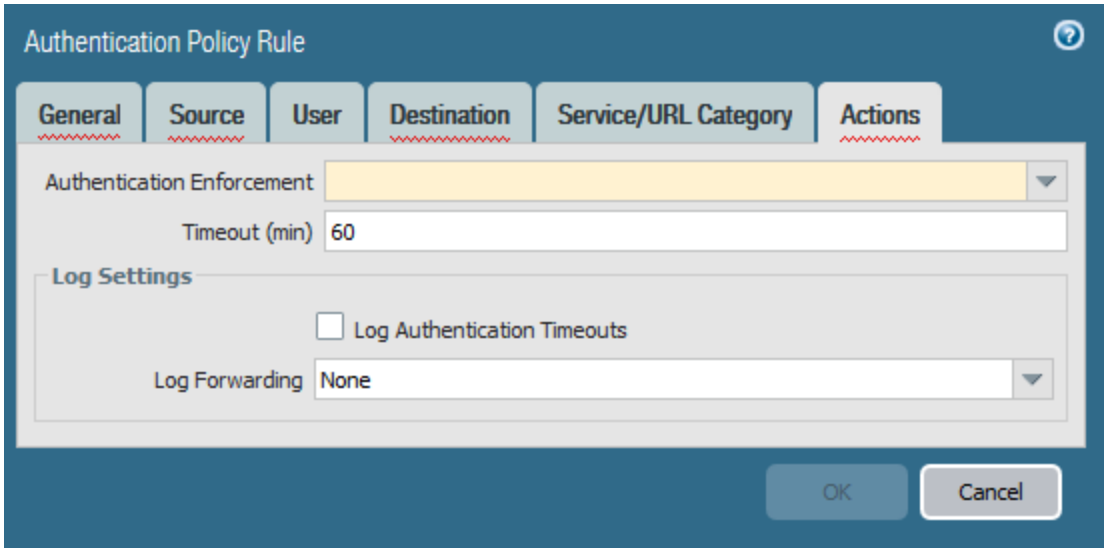
A. Voice
B. Push
C. SMS
D. S/Key

133. What is the meaning of setting the source user to known-user in an authentication policy rule?

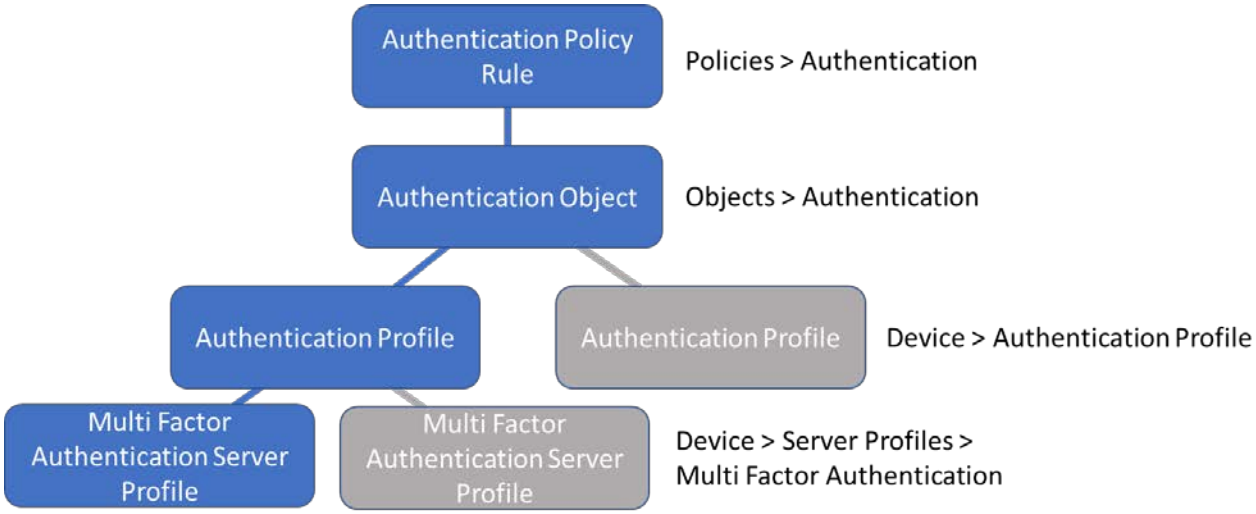
A. The user identity is known (tied to an IP address), but the resource is sensitive enough to require additional authentication.
B. The next-generation firewall will demand user authentication, and only then will the resource be available.
C. The source device is a known device, which is only used by a single person.
D. There is no such option. If the user identity is known, there is no need for an authentication policy rule.

Identify the dependencies for implementing MFA

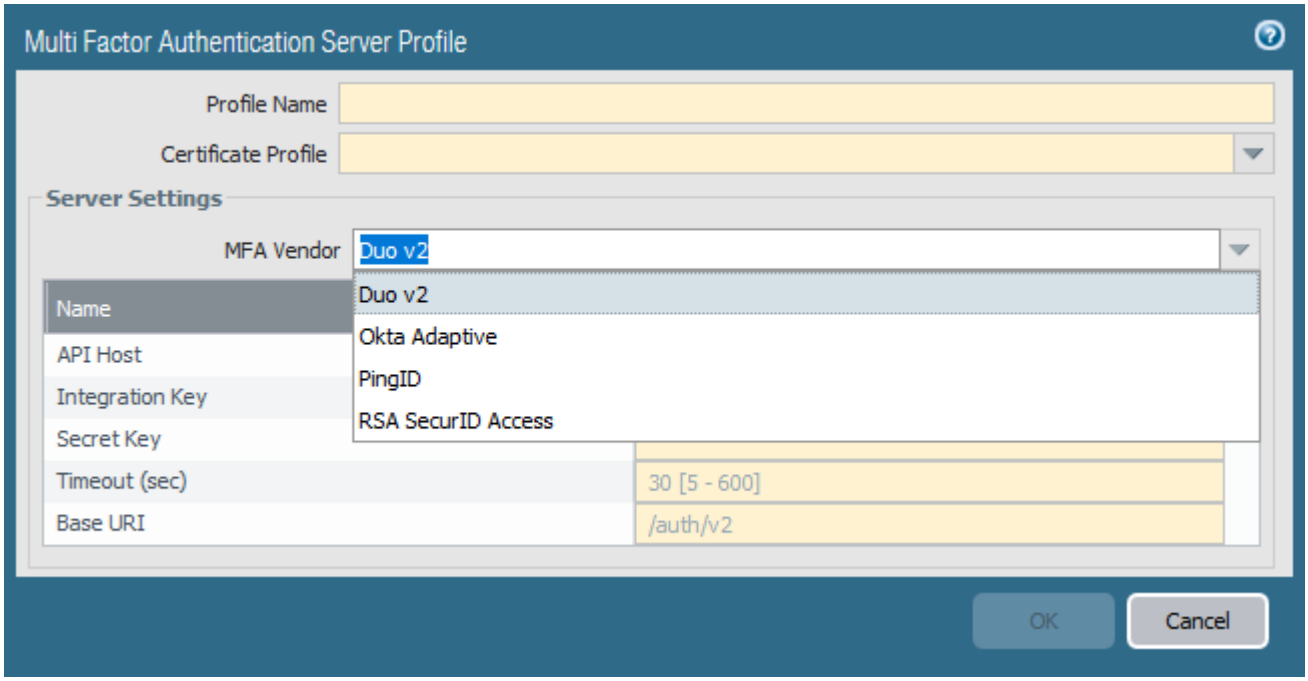
Before you can use multi-factor authentication (MFA) for protecting sensitive services and applications, you must configure several settings in the Palo Alto Networks firewall. MFA authentication is triggered when a user requests access to a service appearing in traffic that the firewall processes. The traffic is first evaluated by an Authentication policy rule. When a match is found, the authentication action of the rule is taken.



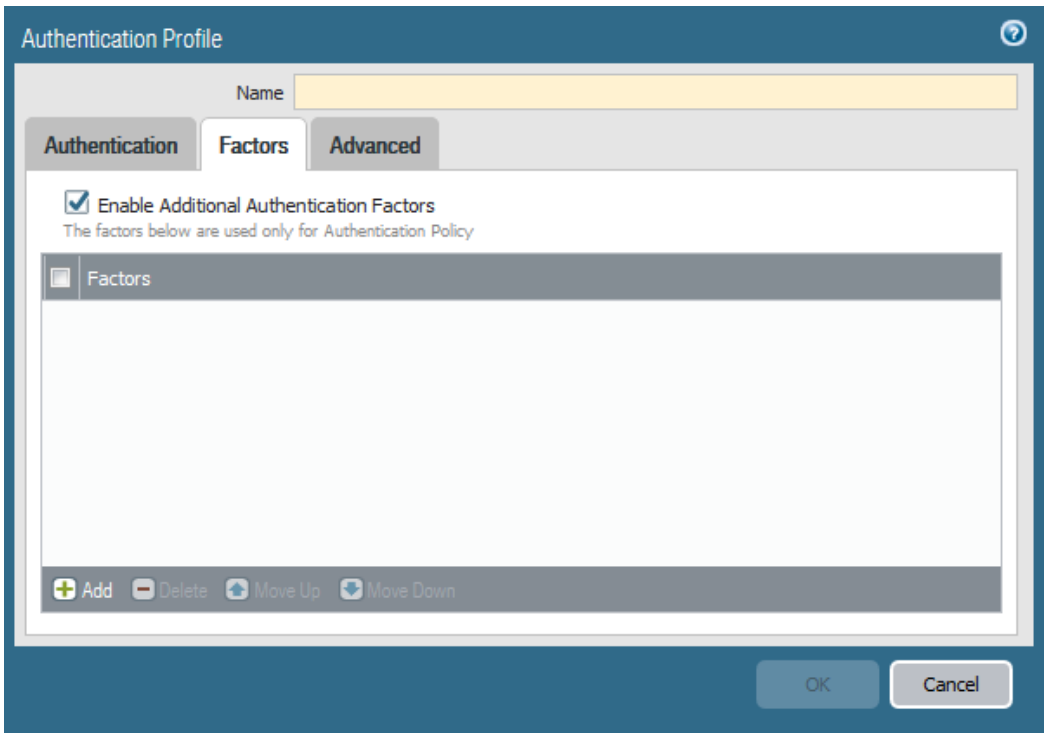
The following diagram shows the relationship of the required objects to configure the Authentication policy rule.



- 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.



- 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.

References

- Configure Multi-Factor Authentication https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/authentication/configure-multi-factor-authentication#_79409
- Map IP Addresses to Usernames Using Captive Portal https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal

Sample questions

134. What are the two Captive Portal modes? (Choose two.)
    A. Proxy
    B. Transparent
    C. Web form
    D. Certificate
    E. Redirect

135. 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.
136. An authentication policy rule has an 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

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/configure-interfaces/layer-2-interfaces
- Virtual Routers
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/networking/virtual-routers
- PBF (Policy-Based Forwarding)
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/policy-based-forwarding/pbf
- Use Case: PBF for Outbound Access with Dual ISPs
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/policy-based-forwarding/use-case-pbf-for-outbound-access-with-dual-isps

Sample question

137. Hypo Thetical, Inc. 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.
138. 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
139. 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.

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/set-up-a-basic-security-policy#79320

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://www.paloaltonetworks.com/documentation/81/best-practices/best-practices-internet-gateway#60768

Security Profiles are an important aspect of protection detection and prevention for specific types of threats. See the following document for more details:
https://www.paloaltonetworks.com/documentation/81/best-practices/best-practices-internet-gateway/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles#48239

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.

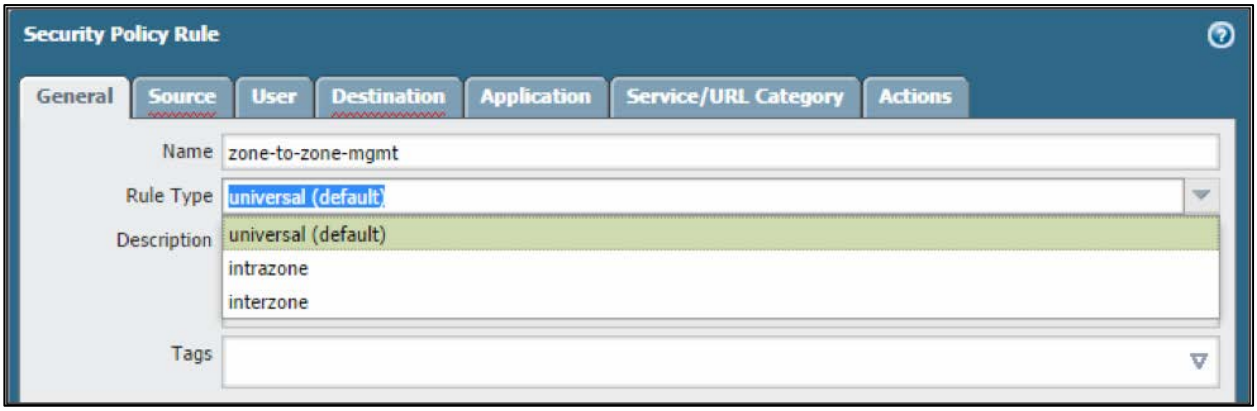
If Panorama device groups are used to push Security policy to one or more firewalls, the Security policy list is expanded to include rules before ("Pre") and after ("Post") the local firewall rules. Panorama rules are merged with local firewall policies in the position chosen during Panorama rule creation.

				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.

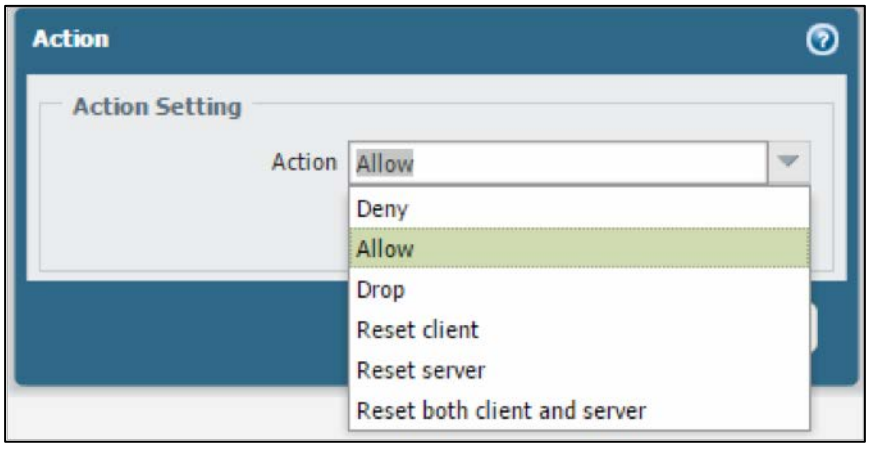


Security policy "rule type" selects the type of traffic the policy applies to.

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 continue to rely on the Palo Alto Networks specification by choosing "deny."

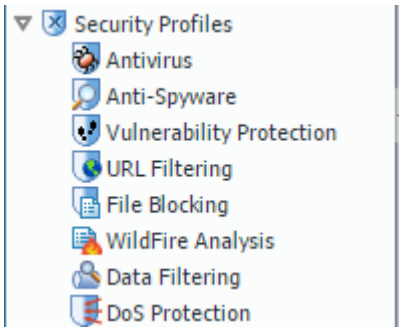


The actions available in security rules

Security Profile Overview

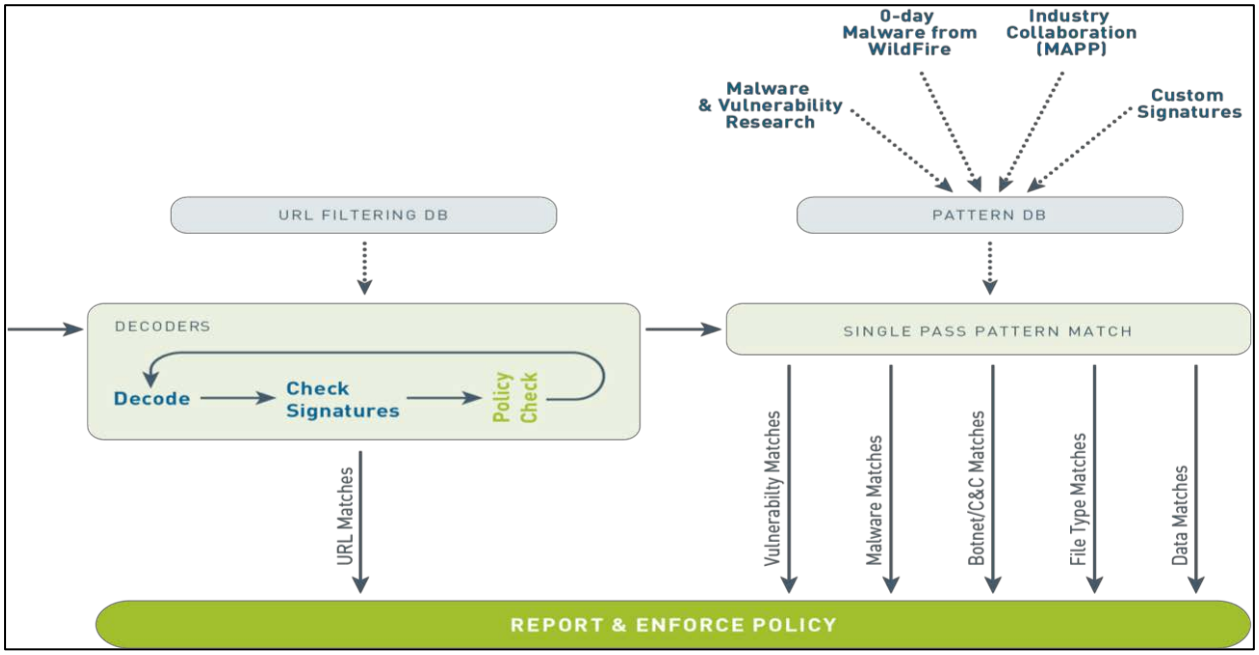
Security Profiles implement specific protections provided by the Palo Alto Networks Content-ID next-generation technology. After Security Profiles are created, they are attached to Security policies specifying Content-ID scans to be performed on traffic allowed by that policy. These profiles must be attached to Security policies to invoke their protections and will be applied only to the traffic handled by that particular policy.

Security Profiles include:



Configurable Security Profiles

An overview of each Security Profile is here:
https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/policy/security-profiles.html



Content-ID engine

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://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin/monitor-wildfire-activity/wildfire-analysis-reportsclose-up#90140

WildFire Profile setup details are here:
https://www.paloaltonetworks.com/documentation/81/pan-os/web-interface-help/objects/objects-security-profiles-wildfire-analysis

A complete review of WildFire® implementation considerations is here:
https://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin

An explanation of WildFire® subscription benefits is here:
https://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin/wildfire-overview/wildfire-subscription#25174

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/url-filtering/customize-the-url-filtering-response-pages

An overview of URL filtering is provided here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/url-filtering

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://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/url-filtering/url-filtering-overview/url-filtering-vendors

Specific information about implementing URL Filtering profiles and their allowed actions is here: https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/url-filtering/configure-url-filtering#74872

Sample questions

140. Which action specifies that Security Profiles are relevant in a policy rule?
    A. Deny
    B. Drop
    C. Reset
    D. Allow
141. 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.
142. 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

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 on this method appear here:

- https://www.paloaltonetworks.com/documentation/81/pan-os/xml-api/about-the-pan-os-xml-api
- https://www.paloaltonetworks.com/documentation/81/pan-os/xml-api/about-the-pan-os-xml-api/structure-of-a-pan-os-xml-api-request/xml-and-xpath
- https://www.paloaltonetworks.com/documentation/81/pan-os/xml-api/about-the-pan-os-xml-api/structure-of-a-pan-os-xml-api-request
- https://www.paloaltonetworks.com/documentation/81/pan-os/cli-gsg/use-the-cli/load-configurations/load-a-partial-configuration/load-a-partial-configuration-into-another-configuration-using-xpath-values

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://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/bootstrap-the-vm-series-firewall/prepare-the-bootstrap-package#_32401
- Bootstrap a Firewall using a USB Flash Drive https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive
- Bootstrap the VM-Series Firewall in Azure https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-azure
- Bootstrap the VM-Series Firewall in AWS https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws
- 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

Sample questions

143. 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
144. 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
145. Which environment supports a USB drive for the firewall bootstrap?
    A. VMware ESXi
    B. physical firewall
    C. Microsoft Hyper-V
    D. KVM

Further Resources

- Firewall 8.1 Essentials: Configuration and Management (EDU 210)
  https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/edu-210-8x-datasheet.pdf
- Panorama 8.1: Managing Firewalls at Scale (EDU-220)
  https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/edu-220-8x-datasheet.pdf
- PAN-OS 8.1 Admin Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os
- PAN-OS CLI Quick Start
  https://www.paloaltonetworks.com/documentation/81/pan-os/cli-gsg
- PAN-OS 8.1 New Features Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide
- Panorama 8.1 Admin Guide
  https://www.paloaltonetworks.com/documentation/81/panorama/panorama_adminguide
- Panorama 8.1 New Features Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/panorama-features
- GlobalProtect 8.1 Admin Guide
  https://www.paloaltonetworks.com/documentation/81/globalprotect/globalprotect-admin-guide
- GlobalProtect 8.1 New Features Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features
- WildFire 8.1 Admin Guide
  https://www.paloaltonetworks.com/documentation/81/wildfire/wf_admin
- WildFire 8.1 New Features Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/wildfire-features
- VM-Series Deployment Guide
  https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization
- Virtualization 8.1 New Features Guide
  https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/virtualization-features
- Live Community https://live.paloaltonetworks.com/
- Firewall In-Line Help

Appendix A: Sample test

The answers are on p. 145.

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, 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
    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 WebUI 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
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
    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.
    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 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?
    A. signature matching
    B. route lookup
    C. policy matching
    D. route updates
49. Which of the following User-ID methods 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

Appendix B: Answers to sample questions

Exam Domain 1 – Plan

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

1. Which component (or components) of the integrated Palo Alto Networks security solution limits access to a corporate z/OS (also known as MVS) mainframe?
    A. threat intelligence cloud
    B. advanced endpoint protection
    C. next-generation firewall
    D. advanced endpoint protection and next-generation firewall
2. Which Palo Alto Networks product is primarily designed to provide context with deeper information about attacks?
    A. MineMeld
    B. WildFire®
    C. AutoFocus
    D. Threat Prevention
3. Which Palo Alto Networks product is primarily designed 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 primarily designed to protect endpoints from successful Cyber-attacks?
    A. Global Protect
    B. Magnifier
    C. Traps
    D. Evident
5. The Palo Alto Networks Logging Service can accept logging data from which two products? (Choose two.)
    A. Traps
    B. next-generation firewalls
    C. Aperture
    D. MineMeld
    E. AutoFocus

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

6. A potential customer says they need a firewall to process 50Gbps of traffic. Which firewall, if any, do you recommend to the customer?
    A. PA-7080
    B. PA-7050
    C. PA-5260
    D. You don't recommend a firewall model at this point. Ask about the kind of traffic and how it needs to be processed. If the requirement is for 50Gbps IPsec VPN throughput, then the customer needs a PA-7080. For 50Gbps with threat prevention, you need a PA-7050. If only App-ID is used, a PA-5260 can fulfill the requirement.

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

7. What would cause you to recommend an active/active cluster instead of an active/passive one?
    A. Active/action is the preferred solution when the firewall cluster is behind a load balancer that randomizes routing, requiring both firewalls to be active.
    B. Active/active is the preferred solution in most cases, because it allows for more bandwidth while both firewalls are up. Active/passive is available only for backward compatibility.
    C. Active/active is the preferred solution when using the PA-7000 Series. When using the PA-5200 Series or smaller form factors, use active/passive.
    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.
8. Which two of the following events can trigger an HA pair failover event? (Choose two.)
    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 destination address successfully
    D. OSPF implemented on the firewall determines an available route is now down
    E. RIP implemented on the firewall determines an available route is now down
9. Which of the following firewall models does not support active/passive HA pair?
    A. PA-200
    B. VM-Series in AWS
    C. VM-Series in Azure
    D. VM-Series in ESXi
10. 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

11. How do firewalls in an Active/Passive HA pair synchronize their configurations?
    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 and it automatically synchronizes with the other
    D. An administrator schedules an automatic sync frequency in the firewall configs

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

12. You want to put the NGFW in front of an existing firewall to begin providing better security while making the minimum required network changes. Which interface type to do you use?
    A. TAP
    B. Virtual Wire
    C. Layer 2
    D. Layer 3
13. Which kind of interface do you use to connect Layer 2 and Layer 3 interfaces?
    A. VLAN
    B. virtual router
    C. loopback
    D. tunnel
14. Which Dynamic Routing protocol cannot be configured on the firewall's virtual router(s)?
    A. RIP
    B. OSPF
    C. OSPFv3
    D. IGRP
    E. BGP
15. Which of the following are not compatible with Aggregate interface configuration?
    A. Aggregating 12, layer 3 interfaces together
    B. Aggregating 4, Virtual Wire interfaces together
    C. Using Aggregate interfaces in an HA pair
    D. 2 10Gps Optical and 2 10Gps copper ethernet ports aggregated together

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

16. 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, can they share the same device group? Can they share the same template?
    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

17. A firewall is assigned to a Template stack of 2 templates. There is a common setting in each Template that has a different value. When Panorama pushes the template stack contents to the managed firewall which setting will the firewall receive?
    A. The value from the top template of the stack
    B. The value from the bottom template in the stack
    C. The value from the template designated as the Parent.
    D. The value an admin selects from the two available values.
18. 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
19. Which four firewall settings are stored in Panorama Templates? (Choose four.)
    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

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

20. When entering Security policy rules you want to ensure your new rules will take precedence over locally entered rules. Where do you put them in Panorama?
    A. In the Security policy rules with a targeted firewall.
    B. In the Default rules section of Security policy rules.
    C. In the Pre-rules section of Security policy rules.
    D. In the Post-rules section of Security policy rules.
21. Which three firewall settings are stored in Panorama Device Groups? Choose 3
    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

Identify options to deploy Palo Alto Networks firewalls in a private or public cloud (VM-Series)

22. A private cloud has 20 VLANs spread over 5 ESXi hypervisors, managed by single vCenter. How many firewall VMs are needed to implement microsegmentation?
    A. 1
    B. 4
    C. 5
    D. 20
23. When you deploy the Palo Alto Networks NGFW on NSX, do packets coming to an application VM from VMs running on different hardware go through the NSX firewall? If so, which modules do they go through?
    A. No, the Palo Alto Networks NGFW replaces the NSX firewall.
    B. Yes. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, application VM.
    C. Yes. The network, vSwitch, Palo Alto Networks NGFW, NSX firewall, application VM.
    D. Yes. The network, vSwitch, NSX firewall, Palo Alto Networks NGFW, NSX firewall, application VM.
24. Which option shows the interface types that ESX supports in the VM-Series firewalls?
    A. Tap, Layer 2, Layer 3, VWire
    B. Layer 3 only
    C. Tap, Layer 2, Layer 3
    D. Layer 3, VWire
25. Which option shows the circumstances in which High Availability is supported for Private Cloud VM-Series firewalls?
    A. ESX supports both active/active and active/passive HA, and KVM and Hyper-V support active/passive only.
    B. ESX, KVM, and Hyper-V support Active/Passive and Active/Active HA implementations.
    C. ESX, KVM, and Hyper-V support active passive HA-Lite configurations only, with no active/active support.
    D. ESX, KVM, and Hyper-V support active/passive implementations only.

Identify methods for Authorization, Authentication, and Device Administration

26. Which built-in Dynamic role would you give an auditor who is authorized to audit everything on the firewall?
    A. Superuser
    B. superuser (read-only)
    C. virtual system administrator
    D. virtual system administrator (read-only)

27. In order to configure Multi-Factor authentication for users accessing services through the firewall what primary configuration pieces need to be addressed? (Choose 5)
    A. GlobalProtect Portal
    B. Server Profile
    C. Captive Portal
    D. Authentication Enforcement Profile
    E. Authentication Policy
    F. Local User Database
    G. Authentication Profile
    H. Response Pages
28. Which of the following configuration components are NOT used for user authentication in the firewall?
    A. Local User Database
    B. Server Profiles
    C. Certificates
    D. Admin Roles
    E. Authentication policy rules
29. Which two firewall functions are reserved only for admins assigned the Superuser dynamic role? (Choose 2)
    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

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

30. What are two reasons that denial-of-service protections are applied by zone? (Choose two.)
    A. Because denial-of-service protections are applied very early in the processing, before a lot of information is known about the connection – but the ingress interface is already known
    B. **Because denial-of-service protections are only applied 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 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 those on virtual wires are yet another category.
31. To which protocol or protocols does the SYN flood protection?
    A. UDP
    B. TCP
    C. ICMP
    D. GRE
    E.

32. To which two protocols does port scan reconnaissance protection apply? (Choose two.)
    - **A. UDP**
    - **B. TCP**
    - C. GRE
    - D. ICMP
    - E. IPX
33. In what two places do you configure flood protection? (Choose two.)
    - **A. DoS Profile**
    - B. QoS Profile
    - **C. Zone Protection Profile**
    - D. SYN Profile
    - E. XOFF Profile
34. An administrator needs to provide tailored DoS protection to a specific address. Which two firewall features should be used? (Choose two.)
    - A. Zone Protection Profiles
    - B. Virtual Routers
    - C. Server Profiles
    - **D. DoS protection policy rules**
    - **E. DoS protection profiles**

Identify decryption deployment strategies

35. Which feature *never* requires a Decryption policy?
    - A. antivirus
    - B. App-ID
    - C. file blocking
    - **D. network address translation**
36. How can the NGFW inform web browsers that a web server's certificate is from an unknown certificate authority (CA)?
    - A. Show a "the certificate is untrusted, are you SURE you want to go there" 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.**
37. An organization that is decrypting user's browsing traffic has a compliance requirement to record all decrypted traffic. Which two firewall features can be used to directly support this requirement? (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

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

38. Which type or types of identification is disabled by Application Override?
    A. Protocol-ID
    B. User-ID
    C. Content-ID
    D. User-ID and Content-ID
39. 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

Identify the methods of User--ID redistribution

40. How do layers facilitate the mapping (IP to User-ID) and the redistribution of that information?
    A. The IP to User-ID mapping is obtained by the lowest layer and is sent to the next lowest layer. That layer sends it to the next lowest, and the process repeats until the mapping reaches the top layer. Firewalls from each layer can receive information from multiple firewalls at a lower level. This algorithm allows some firewalls, such as those in remote offices and protecting regional applications, to have only the mappings for users they protect.
    B. The IP to User-ID mapping is obtained by the lowest layer and is sent to all the firewalls on the layer above. This algorithm ensures that all the firewalls (except those at the lowest layer) have all the mappings.
    C. The IP to User-ID mapping is obtained by the highest layer and is sent to the next highest layer. That layer sends it to the next highest, and the process repeats until the mapping reaches the bottom layer. Firewalls from each layer can receive information from multiple firewalls at a higher level. This algorithm allows some firewalls, such as those in remote offices and protecting regional applications, to have only the mappings for users they protect.
    D. The IP to User-ID mapping is obtained by the highest layer and is sent to all the firewalls on the layer below. This algorithm ensures that all the firewalls (except those at the highest layer) have all the mappings

Exam Domain 2 – Deploy and Configure

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

41. Which option shows the type or types of application that can cause an incomplete value in the Application field in the Traffic log?
    A. UDP
    B. TCP
    C. ICMP
    D. Both TCP and UDP
42. Session traffic being evaluated by a firewall is encrypted with SSL. Without decrypting it how does the firewall make an App-ID determination?
    A. Evaluating the HTTP headers
    B. Evaluating the SSL Hello exchange
    C. Evaluating certificate contents used for encryption
    D. Using information in the SSL Decryption Exclusion cache
43. During the firewall's App-ID scanning of an on-going session a change of application is detected. How does the firewall respond?
    A. Closes the session, opens a new one and evaluates all security policies again
    B. Closes the session, opens and 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

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

44. Which profile do you use for DLP (data loss protection)?
    A. Antivirus
    B. URL Filtering
    C. File Blocking
    D. Data Filtering
45. A firewall admin is concerned about users entering user credentials into phishing sites. Which Security Profile can be configured to provide credential protection?
    A. WildFire Analysis
    B. Tunnel Filtering
    C. Data Filtering
    D. URL Filtering

Identify the relationship between URL filtering and credential theft prevention

46. Which credential phishing prevention action allows users to decide to submit to a site anyway?
    A. Alert
    B. Allow
    C. Block
    D. Continue
47. 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.
48. A firewall administrator wished to enable Credential Phishing Prevention that blocks an attempt by a user to enter their organizations user ID and password. Which Type of User Credential Detection should be used?
    A. IP User Mapping
    B. Domain Credential Filter
    C. Group Mapping
    D. Citrix Mapping

Identify differences between services and applications

49. Which two protocols are supported for services? (Choose two.)
    A. ICMP
    B. TCP
    C. IGP
    D. GRE
    E. UDP

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

50. Which two applications cannot be identified by port number? (Choose two.)
    A. Microsoft Outlook Express email
    B. Google mail (Gmail)
    C. SSH
    D. Facebook
    E. FTP

51. An administrator creates a Security policy rule allowing office-on-demand traffic through the firewall. When the change is committed the firewall issues a warning saying,

```
"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"
```

What action should the administrator take?

A. None is required, this is only a warning. Protection is still enabled
B. The listed applications should be added to the same Security policy rule
C. The Service action of the rule should be set to "dependent application default"
D. Create a new Security policy rule for each listed application with an allow action higher in the rule list

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

52. 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 for some reason.
    D. Verify that the configuration is correct. You do not need to do anything else if it is correct, the configuration is updated automatically.
53. 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

Identify how to configure and maintain certificates to support firewall features

54. Which is *not* an application in which the NGFW and Panorama use certificates?
    A. Communication with Active Directory to obtain User-ID information
    B. Device authentication for the Captive Portal for User-ID information
    C. Device authentication for IPsec site-to-site VPN with Internet Key Exchange (IKE)
    D. Certificate to re-encrypt inbound SSL traffic
55. Administrators within the enterprise wish to replace the default certificate used by the firewall to secure the Web Management UI traffic with one generated by their existing certificate authority. Which of the following certificate properties 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. The CN must be set to the management port of the firewall

Identify how to configure a virtual router

56. Can two Layer 3 interfaces have the same IP address. If so, under which conditions?
    A. Yes, but they must be connected to different virtual routers
    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. No, that is impossible
    D. Yes, but they must be subinterfaces of the same physical interface
57. A firewall's Virtual Router can connect to what three types of interfaces? (Choose three.)
    A. Virtual Wire Interface
    B. Management Interface
    C. Layer 3 traffic interface
    D. HA1 Interface
    E. HA2 Interface
    F. Loopback Interface
    G. Tunnel Interface

Identify the configuration settings for site-to-site VPN

58. Which type is a tunnel interface?
    A. Tap
    B. Virtual wire
    C. Layer 2
    D. Layer 3
59. A firewall administrator is rolling out 50 Palo Alto Networks firewalls to protect remote sites. He wishes each to have a site-to-site IPsec VPN tunnel to each of the three campus locations. Which configuration function is the basis for automatic site-to-site IPsec tunnels setup 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 three campus' IPsec tunnel config
    C. Configuring the GlobalProtect Satellite settings of the campus and remote firewalls
    D. Entering campus IPsec tunnel settings for each remote firewall's IPsec Profile

Identify the configuration settings for GlobalProtect

60. Which operating system is not supported for use with GlobalProtect clients?
    A. iOS
    B. Android
    C. Windows

D. z/OS

61. Which two functions is a GlobalProtect Gateway 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

Identify how to configure features of the NAT rulebase

62. Which NAT type can be used to translate between IPv4 and IPv6?
    A. ipv4
    B. nat64
    C. nptv6
    D. ipv6
63. When a firewall has more than one NAT Policy rule that matches a packet how does it 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.

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

64. 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
65. 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). For a packet that has this rule applied what Security policy rule components are required 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

Identify how to configure decryption

66. Which protocol is supported for traffic decryption?
    A. IPsec
    B. SP3
    C. SSH
    D. NLSP
67. 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
68. A firewall administrator is decrypting outbound SSL traffic and realizes certain traffic is sensitive and should not be decrypted. What feature must be configured to exclude the specific traffic from decryption?
    A. A Security policy rule that includes the specific URL with an "allow" action
    B. A Decryption policy rule with the specific URL and "no decrypt" action
    C. An Application Override policy that matches the application URL and port number
    D. A Decryption Profile that includes the site's URL

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

69. 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
70. If an Application Override policy rule matches traffic it assigns the indicated App-ID to the traffic. This assigned App-ID cannot be used in which firewall function?
    A. Security policy rule match conditions
    B. Policy Based Forwarding Policy rule match conditions
    C. QoS Policy rule match conditions
    D. NAT Policy rule match conditions

Identify how to configure VM-Series firewalls for deployment

71. 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

72. Which three items of information are required at a minimum to install and configure VM-Series firewalls? (Choose three.)
    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
73. VM-Series firewalls require which additional license step?
    A. Applying a "Base Capacity" license.
    B. Applying a "Cloud Services" license.
    C. Applying a "Site license" license.
    D. Applying a "VM Update" license.
74. A VM-Series firewall being deployed in Azure can be automatically configured by bootstrapping. Azure requires which of the following for Bootstrapping to work:
    A. A Storage Account configured for Azure Files Service
    B. A PowerShell script that feeds a configuration file to the firewall
    C. A xml configuration file included in the base firewall provisioning
    D. Azure Backup services configured with a config file and included in the firewall provisioning

Exam Domain 3 – Operate

Identify considerations for configuring external log forwarding

75. Which log format is not supported for log exports?
    A. SNMP trap
    B. syslog
    C. Apache log format
    D. HTTP
76. Which log type gets redirected using a Log Forwarding Profile?
    A. Config log
    B. Traffic log
    C. System log
    D. HIP Match log
77. Which of these enterprises cannot use the logging service?
    A. A top-secret NSA unit whose firewall protects them from the rest of a top secret government network.
    B. A mining operation in North Canada with intermittent Internet access.
    C. A data center with tens of millions of log entries per day
    D. A cruise ship with limited bandwidth most of the time (except when it is in port)

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

78. 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)
79. 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**
80. What product do you need to have to use event correlation?
    - A. Next-generation firewall, PA-220
    - B. Advanced endpoint protection
    - C. **Panorama**
    - D. GlobalProtect

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

81. A customer's custom application uses DNS to transfer directory information, which needs to be filtered in a very different manner than normal DNS. How do you configure such 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 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.
82. 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
83. Which two types of entities can have custom signatures? (Choose two.)
    - A. Services
    - B. URL categories
    - C. User groups
    - **D. Applications**
    - **E. Vulnerabilities**

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

84. If you need new dynamic content and the PAN-OS® version, in what order do you do it?
    A. It does not matter.
    B. Update the PAN-OS® version first, then the dynamic content.
    C. Update the dynamic content first, then the PAN-OS® version.
    D. Update both at the same time.
85. In what order to you upgrade the different components of the firewall to a next version? (B)
    A. First the firewalls, then Panorama and the Log Collectors
    B. First Panorama and the Log Collectors, then the firewalls.
    C. The order does not matter.
    D. You manually upgrade Panorama, and doing so automatically upgrades the rest of the
86. How do you upgrade a high availability pair (A/P) to PAN-OS® 8.1? 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 have to upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

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

87. What is the format of the configuration files?
    A. YAML
    B. JSON
    C. XML
    D. Some are in XML. Some are in YAML.
88. An organization has a QA network and a production network, each with its own firewalls. The change management policy dictates that any configuration change on the production firewalls has to be done by a script, which had been previously executed on the QA networks followed by extensive testing. What command do you use to copy a partial configuration file to the production firewalls?
    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.

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).

89. Which feature is not in active/active (A/A) mode?
    A. IPsec tunneling
    B. DHCP client
    C. link aggregation
    D. configuration synchronization

Identify the sources of information pertaining to HA functionality.

90. 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

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

91. Which ability does AutoFocus not have?
    A. distinguish between attacks that attempt to exfiltrate data (violate confidentiality) and attacks that attempt to modify it (violate integrity)
    B. display the processes started by specific malware
    C. display the network connections used by specific malware
    D. distinguish between commodity attacks and advanced persistent threats (APTs) directed against the customer's organization or industry

Identify the impact of deploying dynamic updates

92. 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

Identify the relationship between Panorama and devices as it pertains to dynamic updates versions and policy implementation and/or HA peers.

93. Which two types of device can receive the Antivirus content update? (Choose two.)
    A. Log Collector
    B. firewall
    C. WildFire®
    D. AutoFocus
    E. MindMeld
94. Within the 8.1 version, can a content update and a software version be incompatible? If so, in what way? (Choose the most accurate answer.)
    A. No, they are always compatible.
    B. Yes, newer content updates don't work with older versions of the software.
    C. Yes, newer versions of the software don't work with older versions of the content update.
    D. Yes, so you need to always update them at the same time.

Exam Domain 4 – Configuration Troubleshooting

Identify system and traffic issues using WebUI and CLI tools.

95. 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)
96. 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
97. 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

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

98. Which Security Profiles do not have a packet capture option?
    A. Antivirus
    B. Anti-spyware
    C. Vulnerability Protection
    D. URL Filtering
99. 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
100. Under which circumstances do you use tcpdump on the next-generation firewall?
    A. never
    B. CLI capture of packets on traffic interfaces
    C. CLI capture of packets on the management interface
    D. It is the CLI command for the traffic interfaces and the management interface.

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

101. 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
102. 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
103. 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

Identify how to troubleshoot SSL decryption failures

104. 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.

105. 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.

106. Which of the following encryption algorithms 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

Identify certificate chain of trust issues

107. 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.**

108. Which field is mandatory in the subject field of a certificate?
    - A. Organization
    - B. Organizational Unit
    - **C. Common Name**
    - D. Locale

109. 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

Given a scenario, identify how to troubleshoot traffic routing issues.

110. 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

111. What could be two reasons that some IP addresses get good performance when going to web sites, 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.

112. 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.

Exam Domain 5 – Core Concepts

Identify the correct order of the policy evaluation based on the packet flow architecture

113. 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
114. Which two statements are correct regarding policy evaluation? (Choose two.)
    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.
115. 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

Given an attack scenario, identify the Palo Alto Networks appropriate threat prevention component to prevent/mitigate the attack.

116. A URL Filtering Profile is part of which type of identification?
    A. App-ID
    B. Content-ID
    C. User-ID
    D. Service
117. 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
118. 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

Identify methods for identifying users

119. 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
120. 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
121. 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

Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks firewall

122. On a PA-7000, which management function runs on a separate card?
    A. configuration management
    B. logging
    C. reporting
    D. The web user interface
123. 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
124. Which of the following functions residents on the management place?
    A. App-ID matching
    B. Route lookup
    C. Policy match
    D. Logging

Given a scenario, determine how to control bandwidth use on a per-application basis

125. 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
126. How many QoS classes does the next-generation firewall support?
    A. 4
    B. 8
    C. 16
    D. 32
127. 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).

Identify the fundamental functions and concepts of WildFire®

128. Which file type is not supported by WildFire®?
    A. iOS applications
    B. Android applications
    C. Windows applications
    D. Microsoft Excel files
129. The firewall will skip the upload to WildFire® in which three cases? (Choose three.)
    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 10MB.**
    F. The file is transferred through HTTPS.
130. 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

Identify the purpose of and use case for MFA and the Authentication policy

131. What are the two purposes of multi-factor authentication? (Choose two.)
    - **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

132. Which of these MFA factors is not supported by the next-generation firewall?
    - A. Voice
    - B. Push
    - C. SMS
    - **D. S/Key**

133. 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.

Identify the dependencies for implementing MFA

134. What are the two Captive Portal modes? (Choose two.)
    - A. Proxy
    - **B. Transparent**
    - C. Web form
    - D. Certificate
    - **E. Redirect**

135. 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.

136. An authentication policy rule has an 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**

Given a scenario, identify how to forward traffic

137. Hypo Thetical, Inc. 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.
138. 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
139. 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.

Given a scenario, identify how to configure policies and related objects.

140. Which action specifies that Security Profiles are relevant in a policy rule?
    A. Deny
    B. Drop
    C. Reset
    D. Allow
141. 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.
142. What feature of the next-generation firewall allows you to block web sites that are not business-appropriate?
    A. App-ID
    B. File Blocking
    C. Exploit Protection
    D. URL Filtering

Identify the methods for automating the configuration of a firewall

143. 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

144. 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

145. Which environment supports a USB drive for the firewall bootstrap?
    A. VMware ESXi
    B. physical firewall
    C. Microsoft Hyper-V
    D. KVM

Appendix C: Answers to the sample test, p. 137

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, 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
    - **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 WebUI 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
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
    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.
    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 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?

A. signature matching

B. route lookup

C. policy matching

D. route updates

49. Which of the following User-ID methods 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.

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 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)*.

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 on 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 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 runtime. 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.

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.

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*.

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.

E-Learning

For those of you who want to keep up-to-date on our technology, a learning library of *free* e-Learning is available. These on-demand, self-paced e-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 e-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 42 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
- See what is trending
- Ask your security questions and get help from 87,000+ security professionals