PALO ALTO NETWORKS PCNSE STUDY GUIDE

February 2018

Palo Alto Networks, Inc.
www.paloaltonetworks.com
© 2016-2018 Palo Alto Networks – all rights reserved. Aperture, AutoFocus, GlobalProtect, Palo Alto Networks, PAN-OS, Panorama, Traps, and WildFire are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners.

Contents

© 2018 Palo Alto Networks, Inc.

© 2018 Palo Alto Networks, Inc.

Palo Alto Networks PCNSE Study Guide

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

Overview

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

This exam will certify that the successful candidate has the knowledge and skills necessary to implement Palo Alto Networks Next-Generation Firewall PAN-OS® 8.0 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
- Language: English

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 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 platform components.
- You have product expertise and understand the unique aspects of the Next-Generation Security Platform and how to deploy one appropriately.
- You understand Networks networking and security policies used by PAN-OS® software.

Recommended Training

Palo Alto Networks strongly recommends that the candidate attend the following courses: Firewall 8.0 Essentials: Configuration and Management (EDU-210), Panorama: Manage Multiple Firewalls (EDU-221), and Firewall: Debug and Troubleshoot (EDU-311) classes. Courses do not cover everything that a PCNSE needs to know, but they're the most efficient way to start learning. When you have the basics mastered, you should spend time on our platform practicing using the information in the 8.0 version of the Administrator's Guide. Find the guide here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os

The Administrator's Guide contains specific configuration information and some "best practice" configuration settings. Remember that many supplemental documents also are on the learning site. All candidates should take advantage of this free resource.

About This DocumentEfforts 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 require, 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 8.0	
Domain	Weight (%)
Plan	16%
Deploy and Configure	23%
Operate	20%
Configuration Troubleshooting	18%
Core Concepts	23%
Total	100%

Exam Domain 1 – Plan

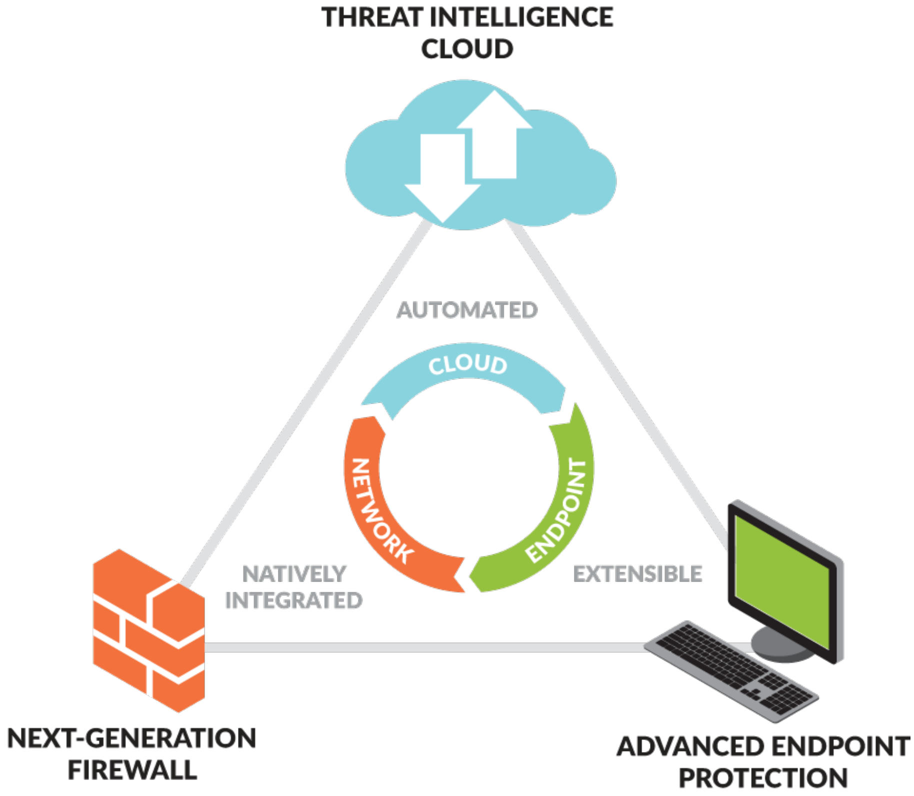
Identify how the Palo Alto Networks products work together to detect and prevent threats.

Preventing Successful Cyber-attacks.
The goals of security are to keep your information safe, and your organization's reputation intact. These goals can be met by reducing the attack surface and thus reducing the likelihood of a successful attack. By focusing on preventing successful attacks, the Palo Alto Networks Next-Generation Security Platform reduces the likelihood of a successful cybersecurity issue so that it is manageable and quantifiable, allowing organizations to compartmentalize their biggest threats and to focus on business operations.

The Palo Alto Networks Next-Generation Security Platform protects our digital way of life by safely enabling applications and preventing known and unknown threats across the network, cloud, and endpoints. The native integration of the platform delivers a prevention architecture that can provide superior security at lower total cost of ownership.

Our platform has four major components that enable the prevention of successful cyber-attacks:

1. **Natively integrated** technologies that:
    - Leverage a single-pass prevention architecture to exert positive control based on applications, users, and content to reduce the organizational attack surface
    - Support open communication, orchestration, and visibility
    - Enable a consistent security posture from the network, to the cloud, to the endpoint
2. **Automated** creation and delivery of protection mechanisms against new threats to network, cloud, and endpoint environments
3. **Extensibility and flexibility** that allows for protection of customers as they expand, move off their physical network, or adopt new technologies
4. **Threat intelligence sharing** that provides protection by leveraging a community of comprehensive global threat data sources to minimize the spread of attacks



By employing the Palo Alto Networks Threat Intelligence Cloud, businesses leverage the global threat community to detect unknown threats and to convert them into known, stoppable threats.

Sample question

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

Answer under the heading Answer to Identify how the Palo Alto Networks products work together to detect and prevent threats. on p. 116.

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

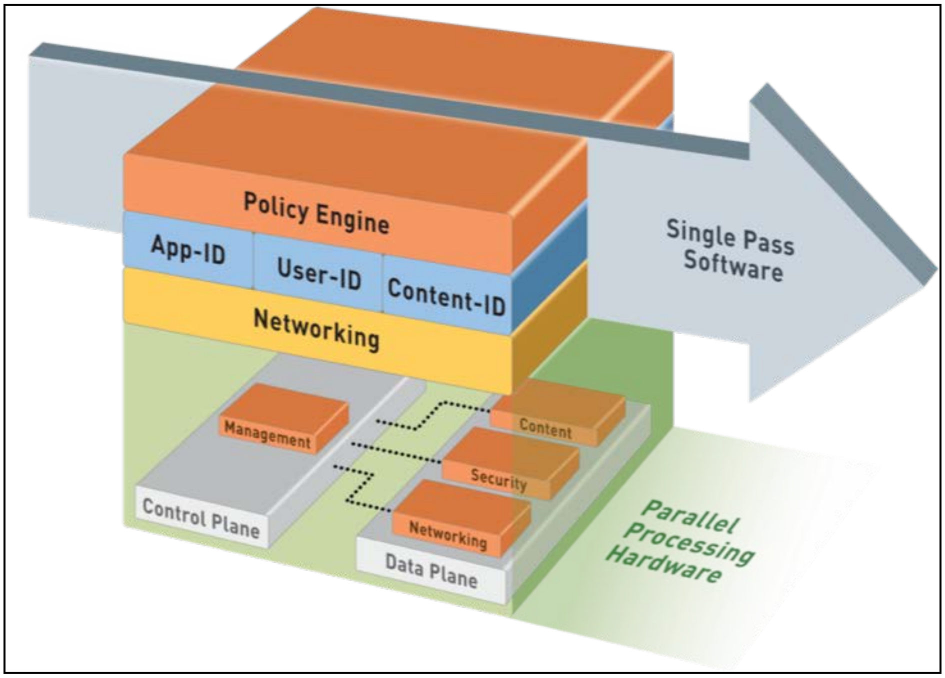
© 2018 Palo Alto Networks, Inc.

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 all defensive options enabled, and "firewall throughput" is the throughput with no Content-ID defense options enabled.

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 should have to 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 the the use of packet evaluation, application identification, policy decisions, and content scanning in a single efficient processing pass.

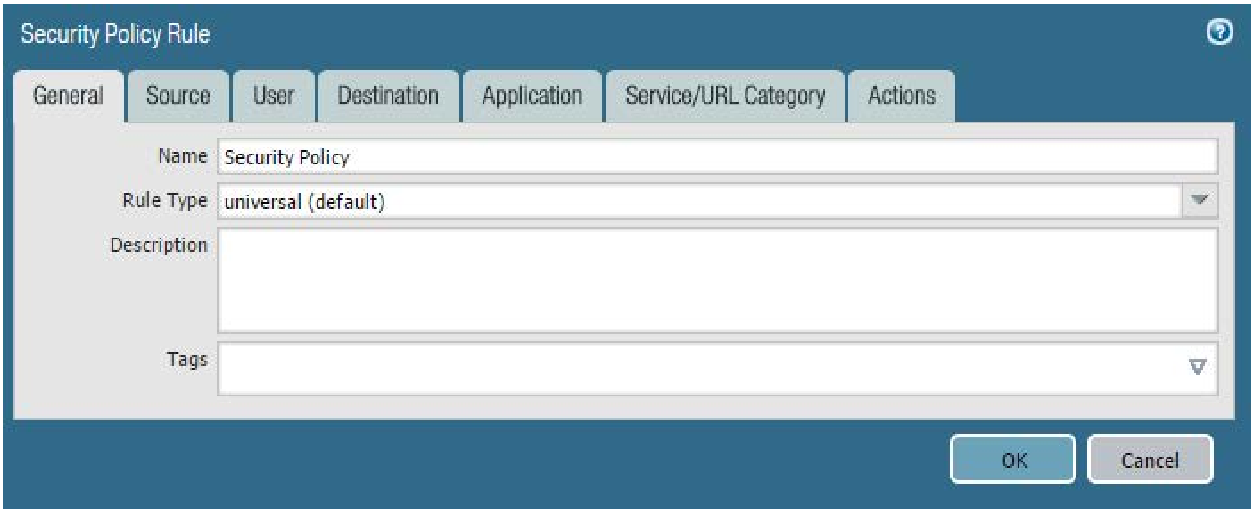
Palo Alto Networks firewalls contain the following next-generation features:

- App-ID: Scanning of traffic to identify the application that is involved, regardless of the protocol
- Content-ID: Scanning of indicated 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)

© 2018 Palo Alto Networks, Inc.

Security Policy

The Security policy consists of numerous security rules that are the basis of the firewall's ability to enable or block sessions. Numerous 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. Allowed sessions can be scanned further based on Security Profiles (Content-ID) to identify unwanted packet content. These profiles use known threat signatures and a mechanism (WildFire) to identify unknown threats, automatically generating new threat signatures. Examples of security rules and profile settings follow:



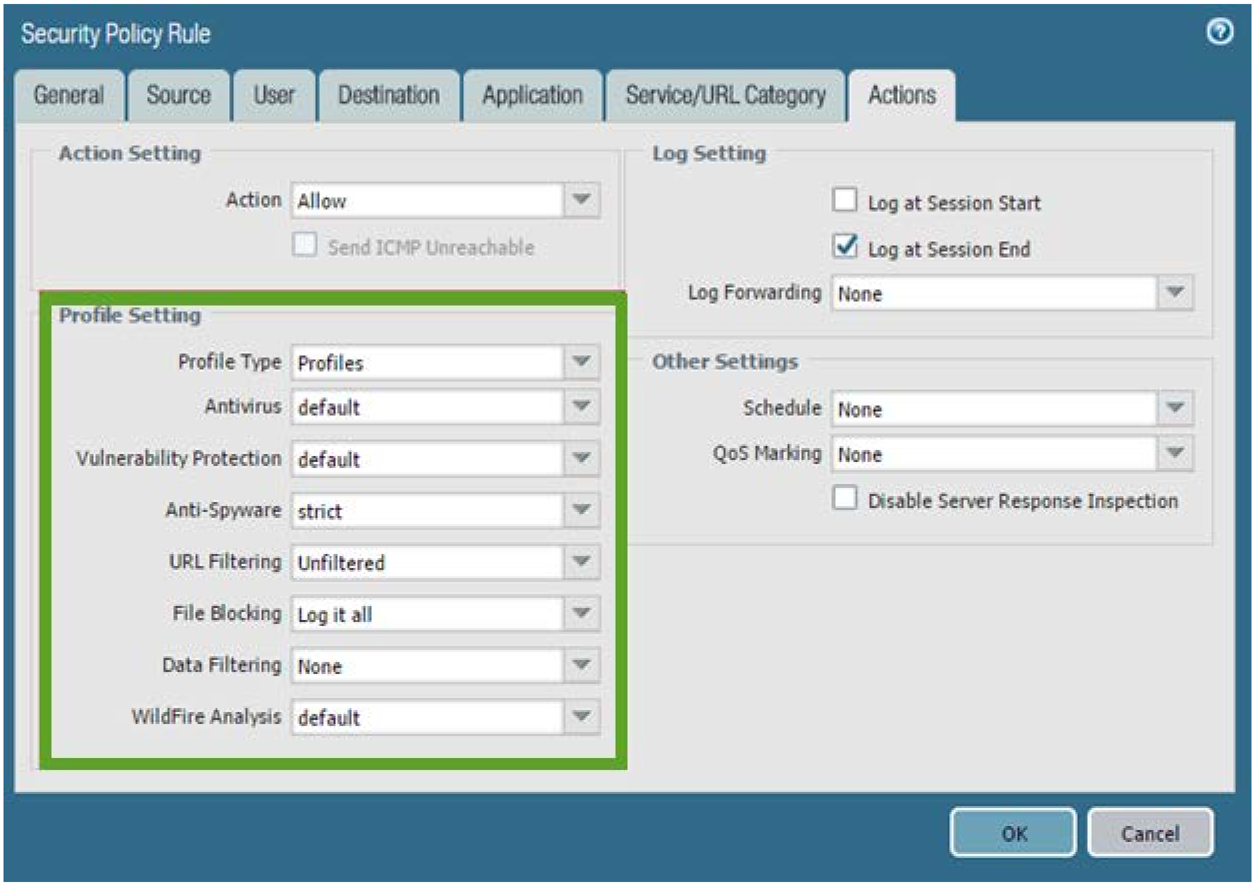
Name: Security Policy

Rule Type: universal (default)

Description:

Tags:

Creating a Security policy rule



Action Setting

Action: Allow

☐ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles
Antivirus: default
Vulnerability Protection: default
Anti-Spyware: strict
URL Filtering: Unfiltered
File Blocking: Log it all
Data Filtering: None
WildFire Analysis: default

Log Setting

☐ Log at Session Start
☑ Log at Session End
Log Forwarding: None

Other Settings

Schedule: None
QoS Marking: None
☐ Disable Server Response Inspection

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

Security Zones

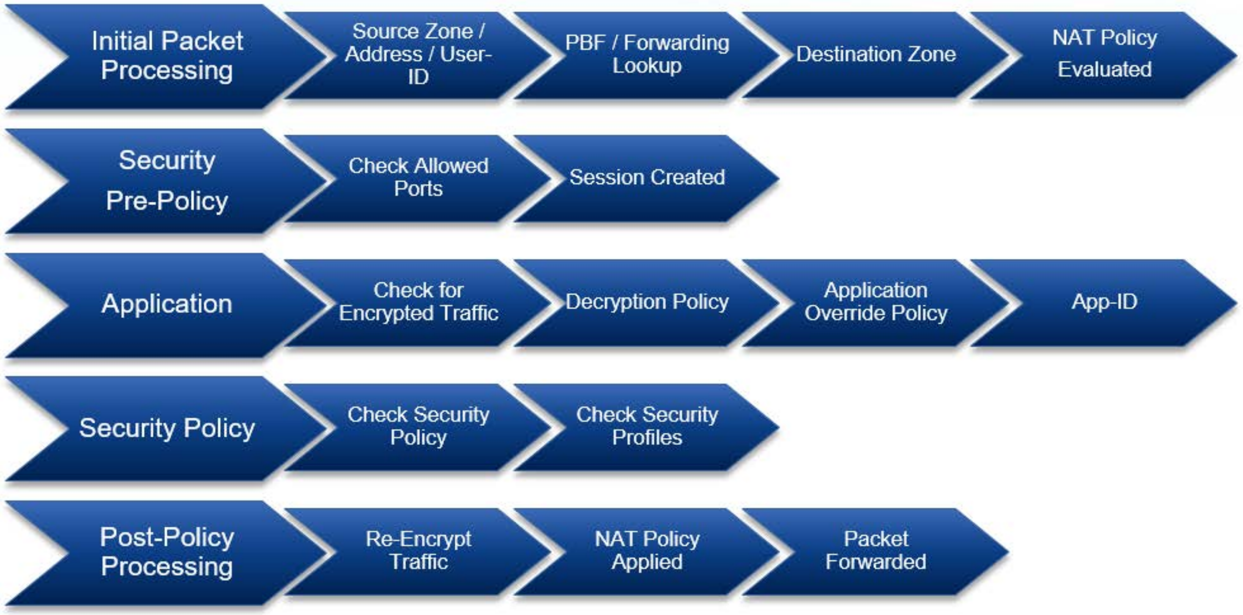
Palo Alto Networks firewalls are zone based. For traffic to pass, the deployment requires that security zones be implemented. These zones act as a logical way to group physical and virtual interfaces. Zones also are required to control and log the traffic that traverses the interfaces. You must assign an interface of the same type as the zone it is assigned (TAP, Virtual Wire, Layer 2 or Layer 3). To pass traffic through an interface, the traffic must be assigned to a zone. A zone can have multiple interfaces of the same type assigned to it, but an interface can belong to only 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. 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. 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, which is in document #1628: “The Life of a Packet”: https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081?attachment-id=4427.



Session processing sequence

Sample question

1. 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, but 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.

Answer under the heading Answer to Given a scenario, identify how to design an implementation of the firewall to meet business requirements leveraging the Palo Alto Networks Security Platform. on p. 116.

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.

High Availability

PAN-OS® software supports High Availability cluster deployments. Clusters consist of two firewalls of identical configuration and licensing. The members of the HA cluster can be directly attached via network cables or deployed a distance from each other if the two can be attached via a routable, or switchable, network. Clusters can be designed with active/passive or active/active configurations.

Active/Passive Clusters

Active/passive HA is the recommended deployment method in nearly every case. It consists of a single firewall configuration synchronized between two firewalls with only one being active and handling traffic at a given time. The synchronization of the configuration data occurs across the HA1 connection. The session data is kept on both firewalls via the HA2 connection. This synchronization process allows the passive firewall to take control of the existing session with little to no loss of data flow.

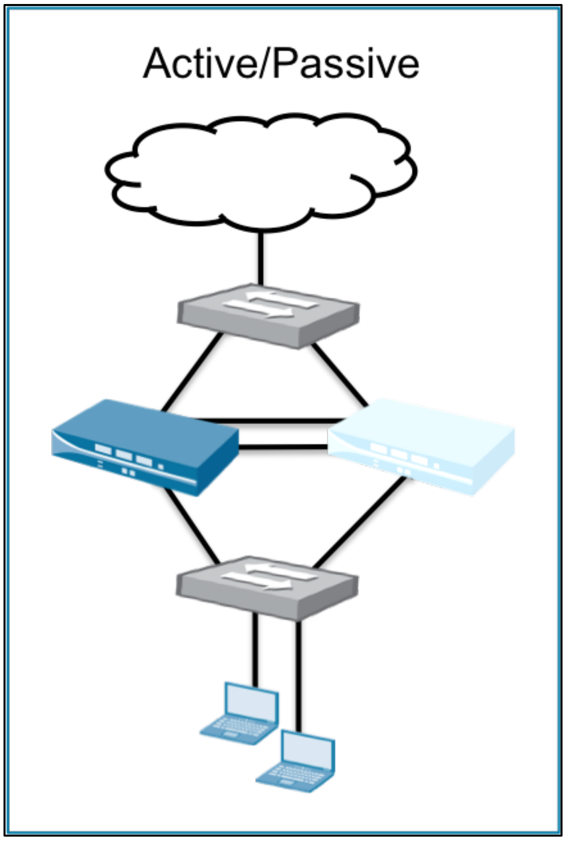
Active/Active Clusters

Active/active HA consists of a cluster of two firewalls attached with three cables: HA1, HA2, and HA3. We recommended it only when load balancing technology randomizes the routing of traffic between the firewalls. Please see additional documentation for Active/Active. For more information, see https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/set-up-active-active-ha.html.

Failover

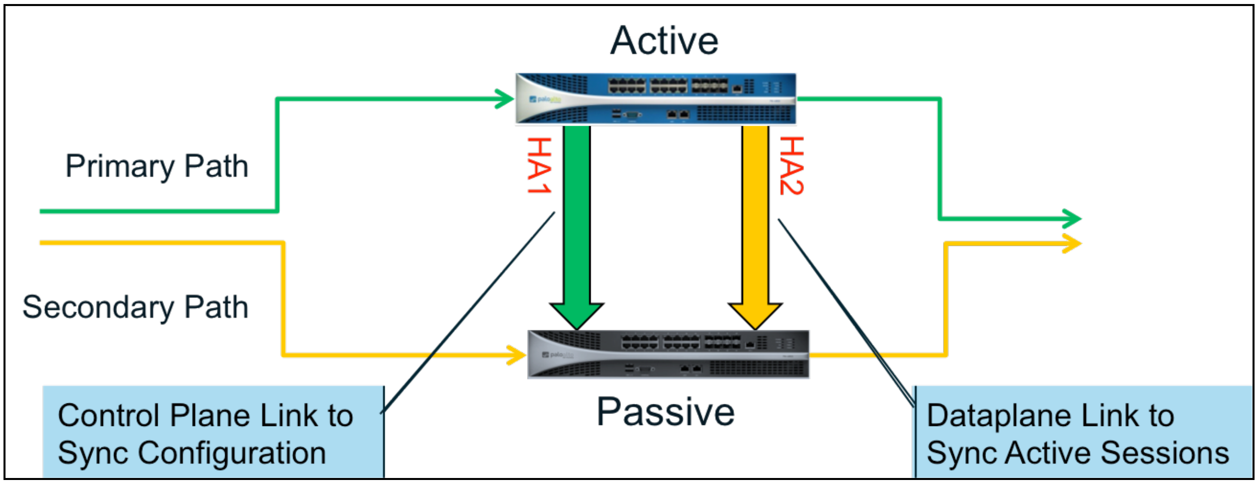
The high availability process can be monitored and triggered by several different methods. To avoid a split brain scenario, you should use all the methods. These methods include the use of a simple heartbeat, path monitoring, and link monitoring.

© 2018 Palo Alto Networks, Inc.



In an active/passive HA pair, only the active firewall processes traffic.

High Availability failover support in both active/active and active/passive clusters includes all firewall features and is non-disruptive to user sessions. Active/passive clusters include two interconnections between firewalls to synchronize all data required for failover support.


Active
Primary Path
Secondary Path
HA1
HA2
Passive
Control Plane Link to Sync Configuration
Dataplane Link to Sync Active Sessions

The HA1 and HA2 links work together to keep the HA firewalls perfectly syncronized.

Additional High Availability Information

Active/passive High Availability configuration details are here:

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-High-Availability-on-PAN-OS/ta-p/54086

Configuration synchronization is discussed here:

https://live.paloaltonetworks.com/t5/Learning-Articles/Information-Synchronized-in-an-HA-Pair/ta-p/57292

Sample question

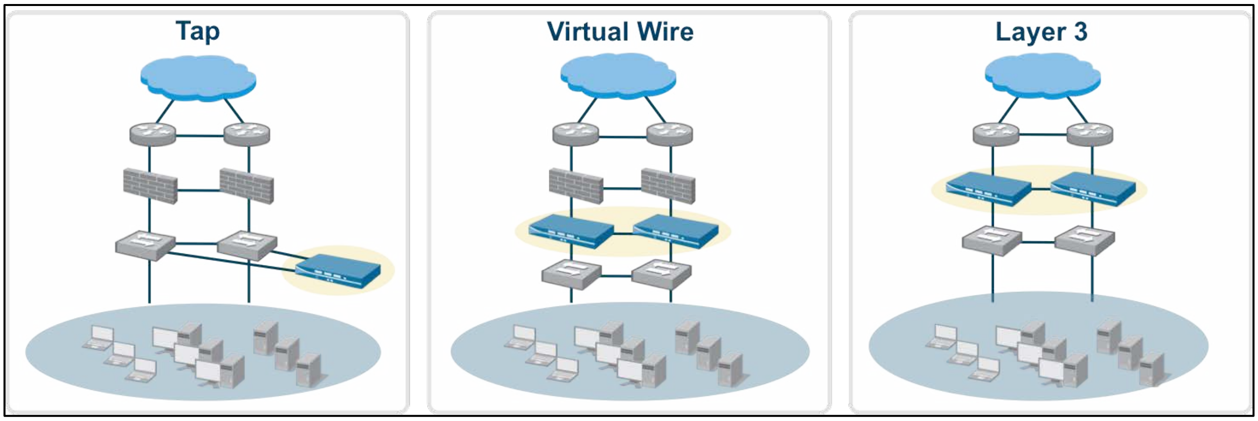
1. What would cause you to recommend an active/active cluster instead of an active/passive one?
    A. Active/active is the preferred solution when the firewall cluster is behind a load balancer that randomizes routing, requiring both firewalls to be active.
    B. Active/active is the preferred solution 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.

Answer under the heading Answer to Given a scenario, identify how to design an implementation of the firewall to meet business requirements leveraging the Palo Alto Networks Security Platform. on p. 116.

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

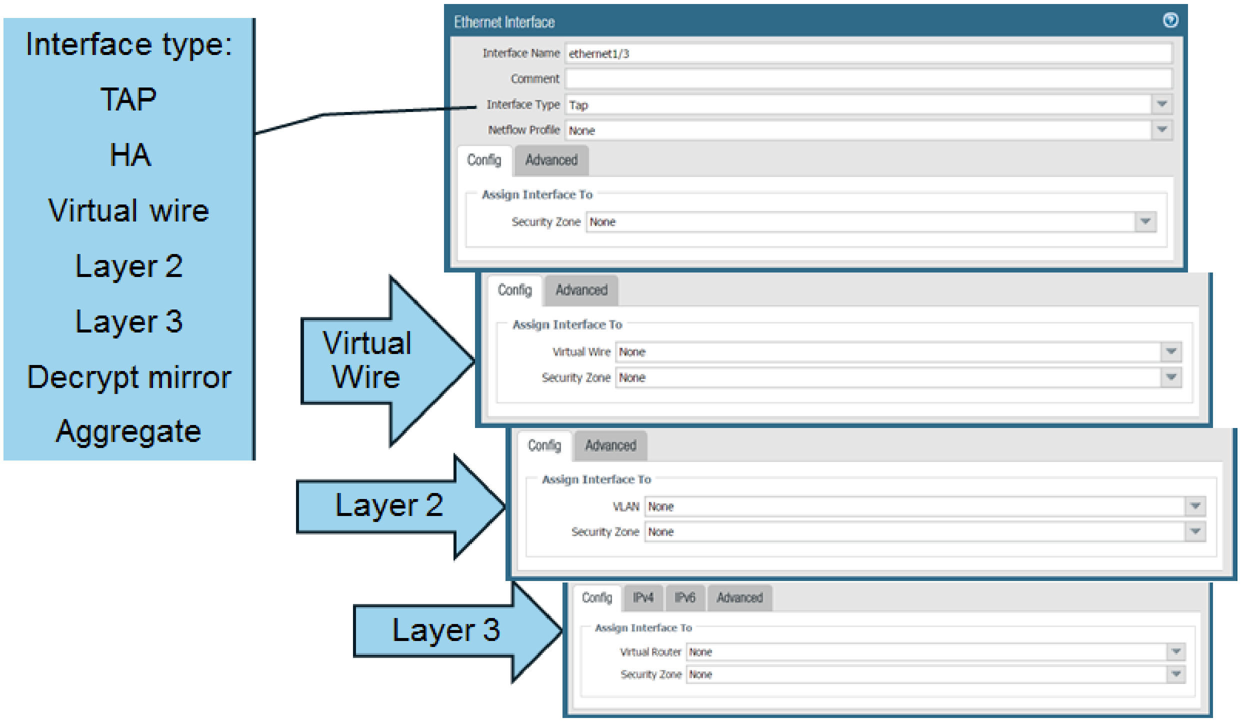
Types of Interfaces

Palo Alto Networks firewalls support several different interface types: TAP mode, Virtual Wire mode, Layer 2, and Layer 3. 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 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:


Interface type:

TAP

HA

Virtual wire

Layer 2

Layer 3

Decrypt mirror

Aggregate

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Tap

Netflow Profile: None

Config | Advanced

Assign Interface To

Security Zone: None

Virtual Wire

Config | Advanced

Assign Interface To

Virtual Wire: None

Security Zone: None

Layer 2

Config | Advanced

Assign Interface To

VLAN: None

Security Zone: None

Layer 3

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: None

Security Zone: None

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 DLP services.

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

© 2018 Palo Alto Networks, Inc.

LACP Protocol

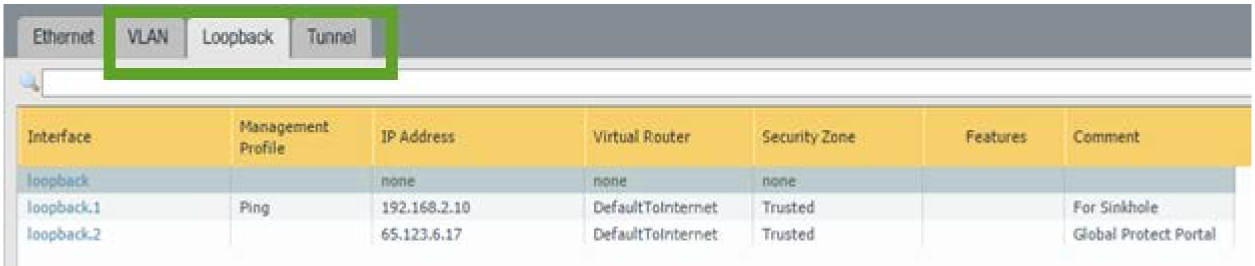
Physical Layer 2 and 3 interfaces can be aggregated into single logical interfaces using the LACP protocol for multiplexing traffic.

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:



Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
loopback		none	none	none		
loopback.1	Ping	192.168.2.10	DefaultToInternet	Trusted		For Sinkhole
loopback.2		65.123.6.17	DefaultToInternet	Trusted		Global Protect Portal

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 and are Layer 3 only.

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 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.

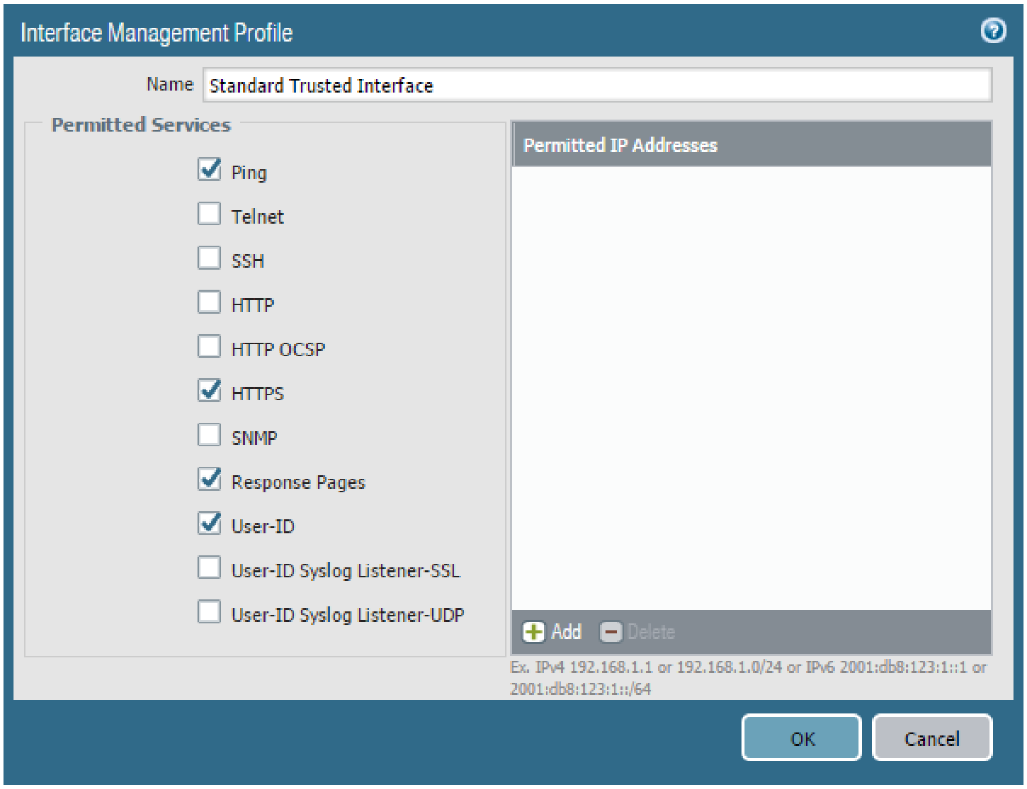
© 2018 Palo Alto Networks, Inc.

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.



Interface Management Profile

Name: Standard Trusted Interface

Permitted Services

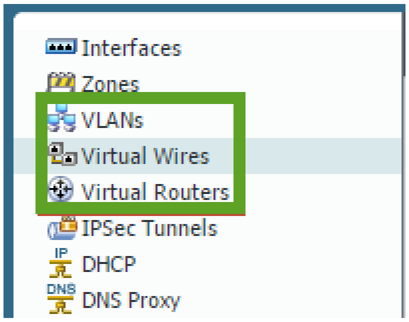
☑ Ping
□ Telnet
□ SSH
□ HTTP
□ HTTP OCSP
☑ HTTPS
□ SNMP
☑ Response Pages
☑ User-ID
□ User-ID Syslog Listener-SSL
□ User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

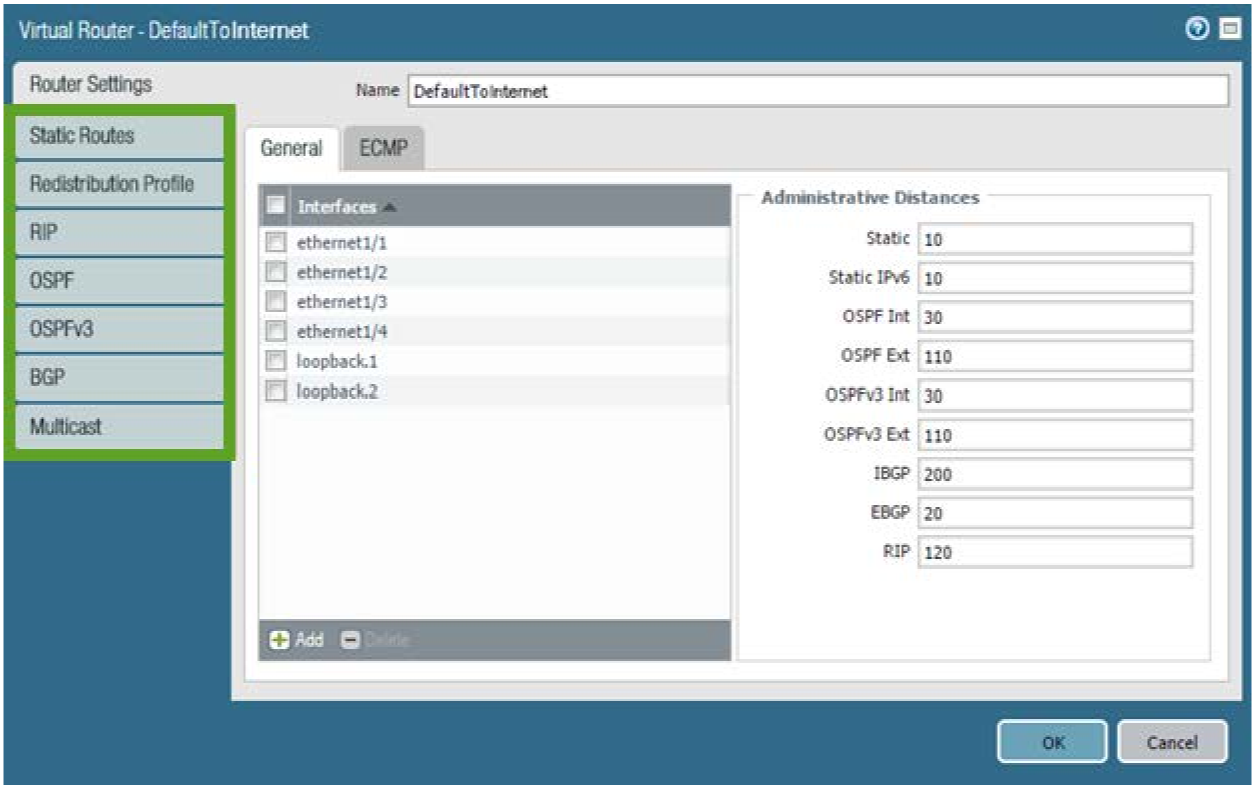
Protocol services and internal processes can be selectively bound to interfaces.

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.



Virtual Router - DefaultToInternet

Name: DefaultToInternet

□ Interfaces
□ ethernet1/1
□ ethernet1/2
□ ethernet1/3
□ ethernet1/4
□ loopback.1
□ loopback.2

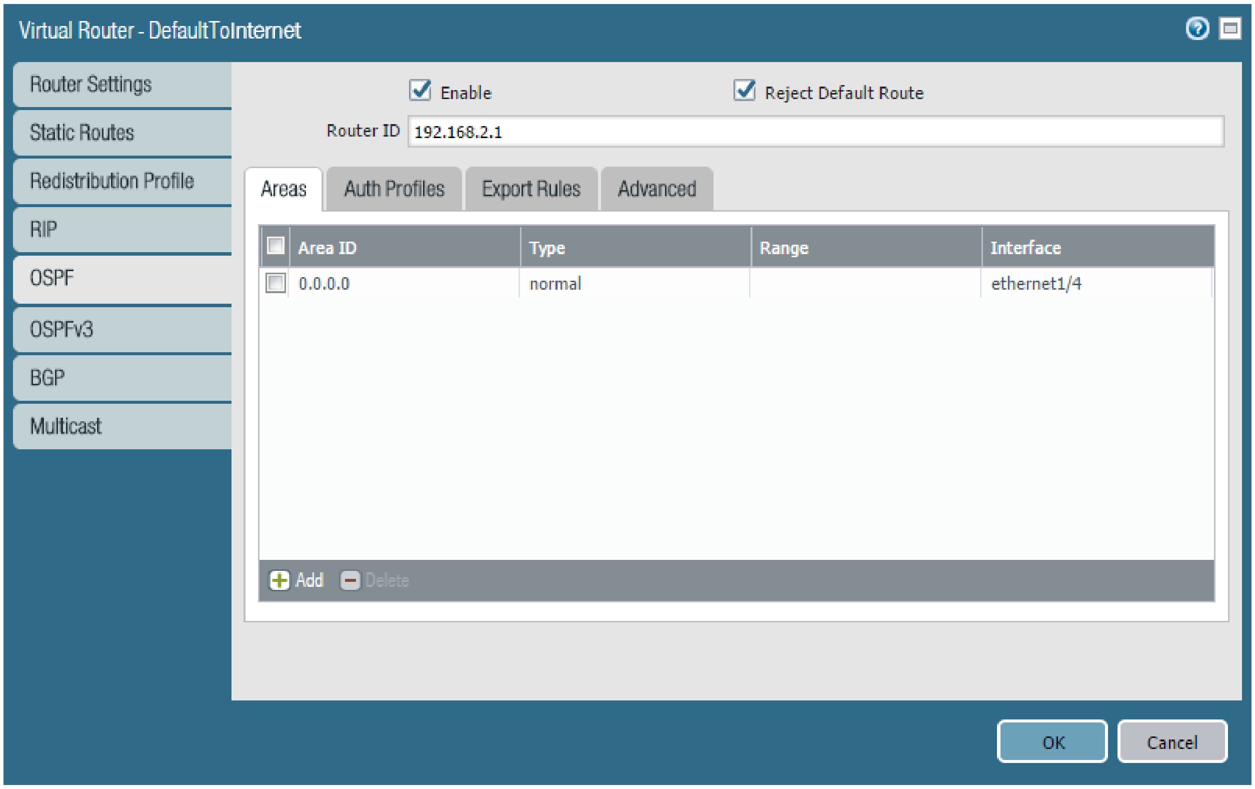
Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Routing capabilities of a Layer 3 virtual router

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

© 2018 Palo Alto Networks, Inc.



☑ Enable ☑ Reject Default Route

Router ID 192.168.2.1

□	Area ID	Type	Range	Interface
□	0.0.0.0	normal		ethernet1/4

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
  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

1. 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
2. Which kind of interface do you use to connect Layer 2 and Layer 3 interfaces?
   A. VLAN
   B. virtual router
   C. loopback
   D. tunnel
   E.

Answer under the heading Answers to Identify the appropriate interface type and configuration for a specified network deployment. on p. 116.

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 can be physically separated.

A functional overview of Panorama is here:

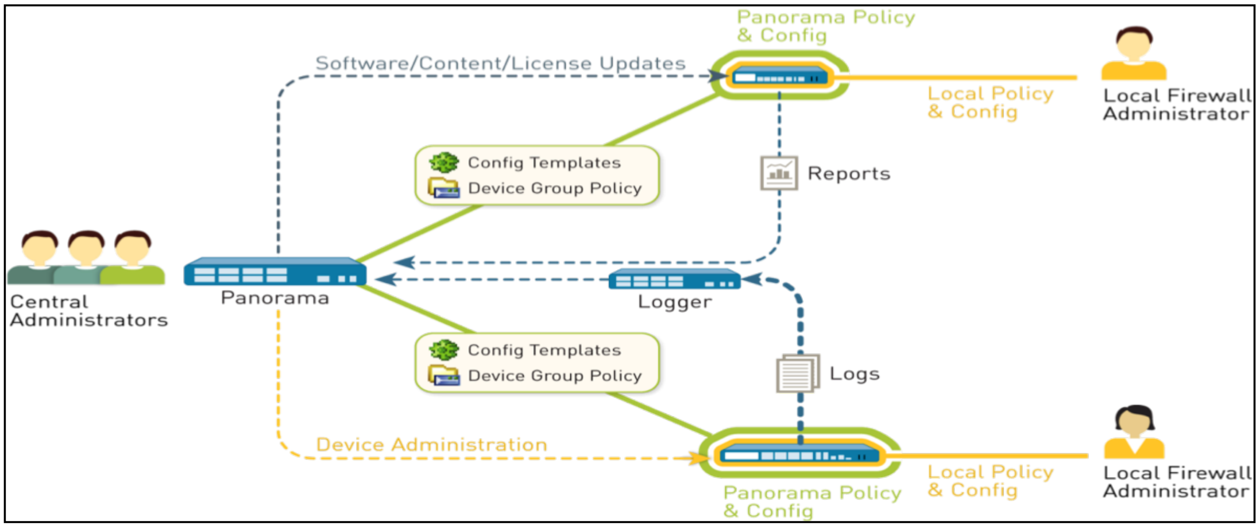
https://www.paloaltonetworks.com/products/secure-the-network/management/panorama

A presentation of the different Panorama platforms and their capacities is here:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/panorama-models

The following illustration outlines the main features of Panorama:

© 2018 Palo Alto Networks, Inc.



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

A brief description of these features is here:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/about-panorama#74210

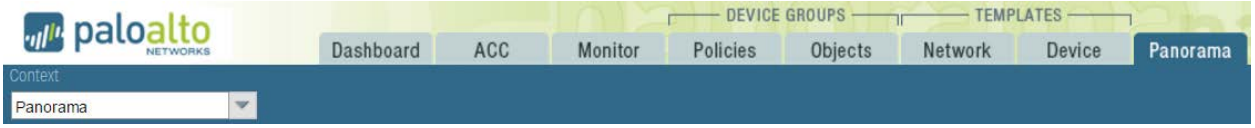
Log Aggregation

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 appliances can be implemented (Logger in the preceding diagram).

More discussion of this topic is here:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/centralized-logging-and-reporting#82482

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:

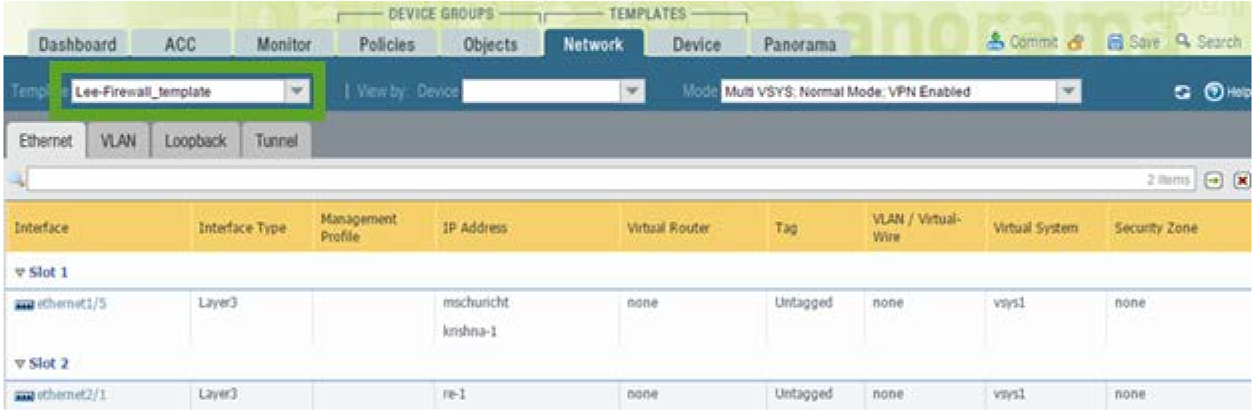


Top-level user interface for Panorama

Templates

To provide Enterprise Management of multiple firewalls, Palo Alto Networks implemented Template and Device Group data objects within Panorama that store firewall settings. These objects are specifically created and managed in Panorama under the Panorama menu. They then are assigned to specific firewalls, forming the link to configuration settings in Panorama. When a Panorama commit is performed, this stored data is pushed from these objects only to their linked firewalls.

Template objects store settings appear in the Panorama UI under the Device and Network menus, and are created in Panorama. An administrator that enters any information under the Panorama Device or Network tab *must* choose the Template to receive the settings.



Templ e: Lee-Firewall_template | View by: Device | Mode: Multi VSYS; Normal Mode; VPN Enabled

Interface	Interface Type	Management Profile	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
▾ Slot 1								
ethernet1/5	Layer3		mschuricht krishna-1	none	Untagged	none	vsys1	none
▾ Slot 2								
ethernet2/1	Layer3		re-1	none	Untagged	none	vsys1	none

Required device group object selection to receive network configuration settings

A firewall only can be assigned one template at a time. The template can be an individual template or a template stack of up to 16 individual templates. In the case of a Stack, the settings are inherited down the stack, ultimately reaching the firewall at the bottom. Duplicates at different levels will override others with a user-selectable inheritance setting. Stacks can be created and broken on demand from constituent templates.

See this link for a further discussion of templates:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/templates-and-template-stacks#12545

Sample question

1. 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-3000 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
    B. same device group, different templates
    C. different device groups, same template
    D. different device groups and different templates

© 2018 Palo Alto Networks, Inc.

Answer under the heading Answer to Identify how to use template stacks for administering Palo Alto Networks firewalls as a scalable solution using Panorama. on p. 116.

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

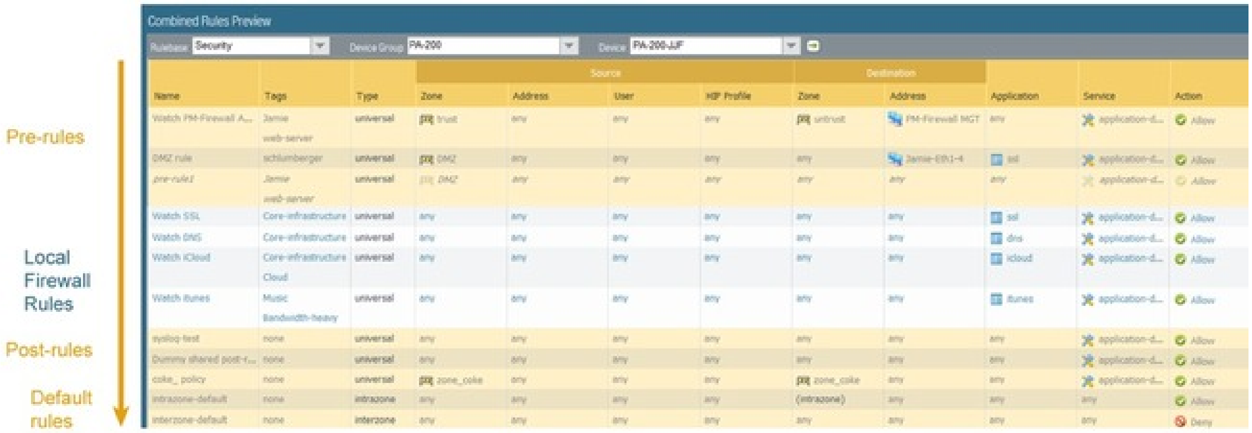
Device Groups

Device Group objects storage settings are found in the Policies and Objects tabs. As with templates, they are deliberately created by Panorama administrators and assigned to firewalls. Firewalls can be attached to only one Device Group object or Hierarchy. Device Group hierarchies can be modified after they are created. In these cases, settings are inherited down the hierarchy, ultimately reaching the firewall at the bottom.

See this link for further discussion of device groups:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/device-groups#78831

Panorama-supplied data 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:



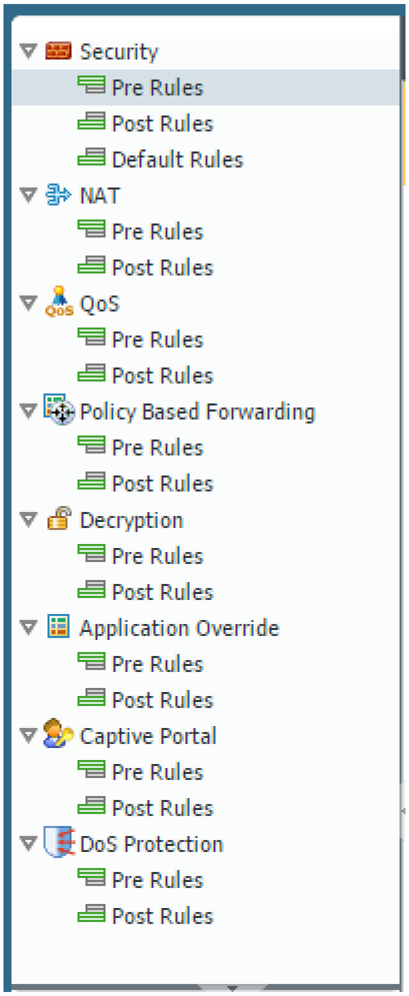
Rulebase: Security · Device Group: PA-200 · Device: PA-200-JJF

			Source				Destination				
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Watch PM-Firewall A...	Jamie web-server	universal	trust	any	any	any	untrust	PM-Firewall MGT	any	application-d...	Allow
DMZ rule	schlumberger	universal	DMZ	any	any	any	any	Jamie-Eth1-4	ssl	application-d...	Allow
pre-rule1	*Jamie* *web-server*	universal	*DMZ*	*any*	*any*	*any*	*any*	*any*	*any*	*application-d...*	*Allow*
Watch SSL	Core-infrastructure	universal	any	any	any	any	any	any	ssl	application-d...	Allow
Watch DNS	Core-infrastructure	universal	any	any	any	any	any	any	dns	application-d...	Allow
Watch iCloud	Core-infrastructure Cloud	universal	any	any	any	any	any	any	icloud	application-d...	Allow
Watch itunes	Music Bandwidth-heavy	universal	any	any	any	any	any	any	itunes	application-d...	Allow
syslog-test	none	universal	any	any	any	any	any	any	any	application-d...	Allow
Dummy shared post-r...	none	universal	any	any	any	any	any	any	any	application-d...	Allow
coke_ policy	none	universal	zone_coke	any	any	any	zone_coke	any	any	application-d...	Allow
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

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

See the following image for the Policy menu on Panorama featuring the Pre and Post position selections:

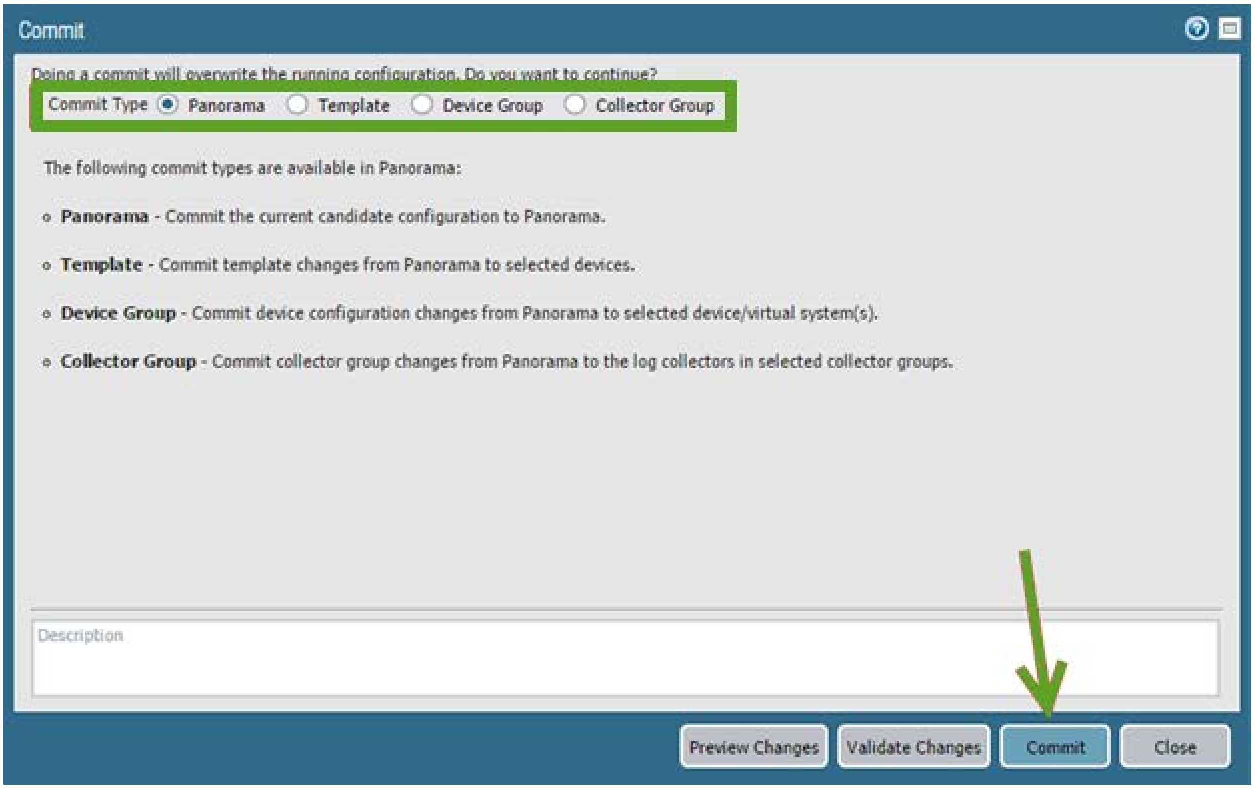
© 2018 Palo Alto Networks, Inc.



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.

The Commit process on Panorama consists of multiple phases. Newly entered data first must be committed to Panorama, followed by a Template and/or Device Group Commit as required.



Doing a commit will overwrite the running configuration. Do you want to continue?

Commit Type ● Panorama ○ Template ○ Device Group ○ Collector Group

The following commit types are available in Panorama:

- **Panorama** - Commit the current candidate configuration to Panorama.
- **Template** - Commit template changes from Panorama to selected devices.
- **Device Group** - Commit device configuration changes from Panorama to selected device/virtual system(s).
- **Collector Group** - Commit collector group changes from Panorama to the log collectors in selected collector groups.

Panorama has different types of Commits. Pushing new data to firewalls typically requires several types to be executed simultaneously.

More information on this process is here:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/panorama-commit-validation-and-preview-operations

Panorama implements a new level of Enterprise Administrator. These roles are fully configured by roles and scopes of accessible firewalls (Access Domain). They can work in conjunction to support a decentralized management model.

More information is here:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/role-based-access-control#93635

Sample question

1. If you want the rules that apply to more-specific device groups to override those that apply to more general groups, where do you put them?
    A. anywhere (the default behavior)
    B. in the pre-rules
    C. in the post-rules

© 2018 Palo Alto Networks, Inc.

D. for security, in the pre-rules. For all the other policies, in the post-rules.

Answer under the heading Answer to Identify how to use device group hierarchy for administering Palo Alto Networks firewalls as a scalable solution using Panorama. on p. 116.

Identify options to deploy Palo Alto Networks firewalls in a private 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 based on technologies from VMware, Amazon Web Services, Microsoft, Citrix, and KVM.

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

Implementation and use the same design and deployment principles as hardware appliance firewalls, with a few exceptions because of the hosting virtual environment.

Sample questions

1. 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
2. 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.

Answers under the heading Answer to Identify how to use device group hierarchy for administering Palo Alto Networks firewalls as a scalable solution using Panorama. on p.116. Identify methods for authorization, authentication, and device administration.

Administrative Accounts

Administrators can configure, manage, and monitor Palo Alto Networks firewalls 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. Every Palo Alto Networks firewall 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 accounts and their creation are discussed here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators#72624

Authentication

Many of the services that Palo Alto Networks firewalls and Panorama provide require authentication, including administrator access to the web interface and end user access to Captive Portal, GlobalProtect portals, and GlobalProtect gateways. The authentication methods that you can configure vary by service, and can include Kerberos single sign-on (SSO), external authentication services, certificates and certificate profiles, local database accounts, RADIUS Vendor-Specific Attributes (VSAs), and NT LAN Manager (NTLM).

A discussion of this topic with configuration details is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication

Sample question

1. Which permission level 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)

Answer under the heading Answer to Identify methods for authorization, authentication, and device administration. on p. 116.

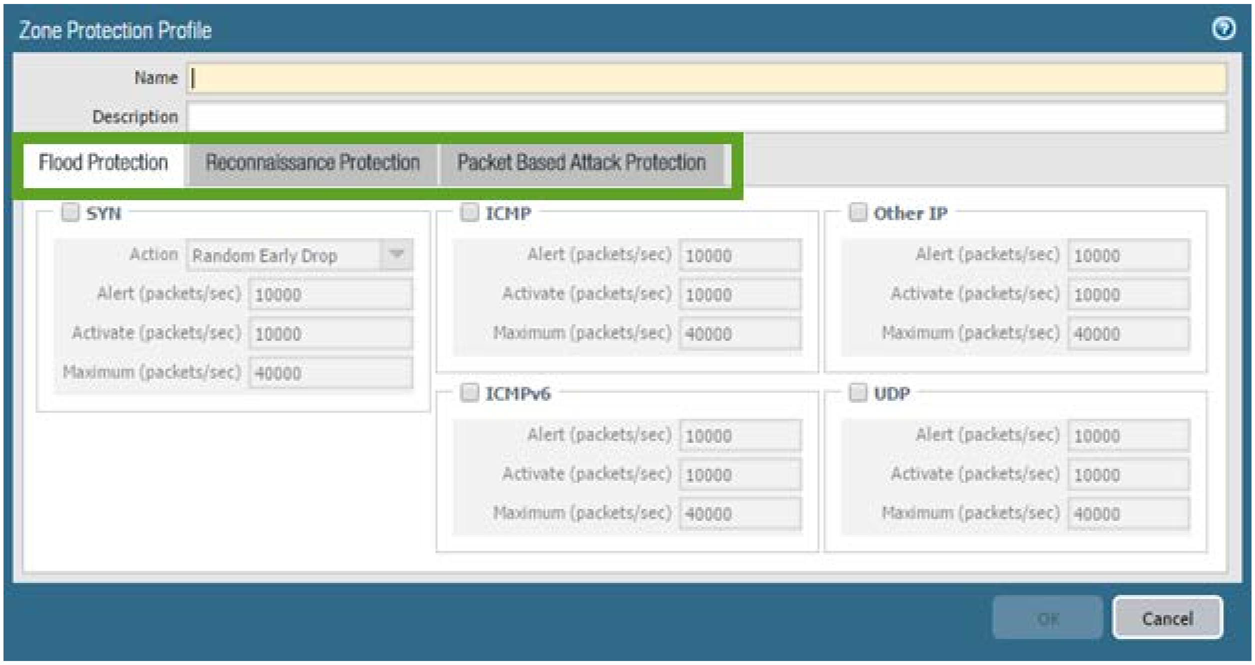
Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers.

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.

DoS and ZPP

PAN-OS® software provides denial-of-service (DoS) policy (associated with Denial of Service Profiles) and Zone Protection profiles (ZPP). As the name suggests, ZPP is applied at the zone level. All (sub)interfaces in that zone are covered by that ZPP as an aggregate protection.



Name

Description

□ SYN
Action: Random Early Drop
Alert (packets/sec): 10000
Activate (packets/sec): 10000
Maximum (packets/sec): 40000

□ ICMP
Alert (packets/sec): 10000
Activate (packets/sec): 10000
Maximum (packets/sec): 40000

□ Other IP
Alert (packets/sec): 10000
Activate (packets/sec): 10000
Maximum (packets/sec): 40000

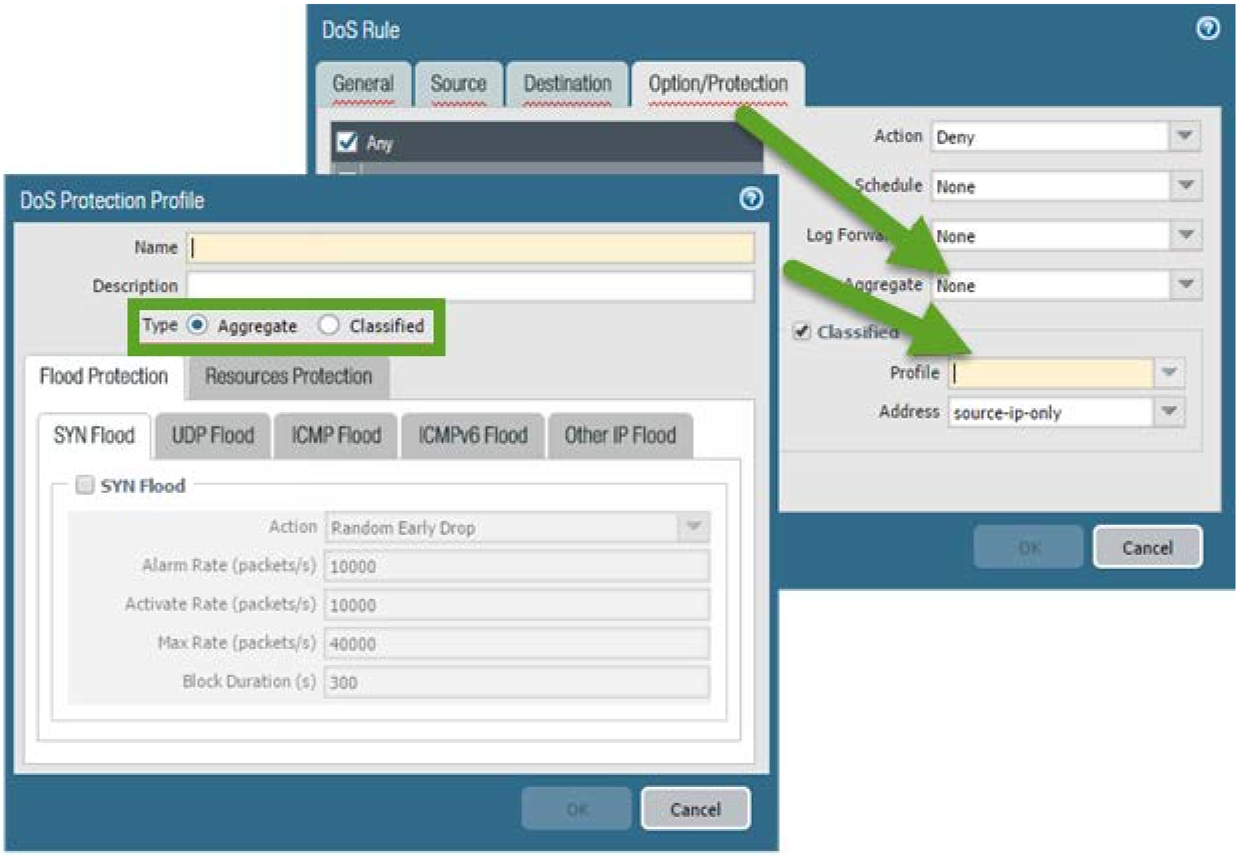
□ ICMPv6
Alert (packets/sec): 10000
Activate (packets/sec): 10000
Maximum (packets/sec): 40000

□ UDP
Alert (packets/sec): 10000
Activate (packets/sec): 10000
Maximum (packets/sec): 40000

Zone Protection Profiles provide multiple types of attack defenses.

Denial of Service policies can provide more granular flood attack protections to internal resources and operate at the same time as ZPPs. ZPPs operate on aggregate traffic totals at the zone level to measure traffic and invoke protections. DoS policies can be targeted as specifically as desired in the policy matching conditions. These policies invoke DoS Protection Security Profiles, which specify which defenses to implement.

© 2018 Palo Alto Networks, Inc.



☑ Any

Action: Deny

Schedule: None

Log Forwa: None

Aggregate: None

☑ Classified

Profile:

Address: source-ip-only

Name:

Description:

Type ● Aggregate ○ Classified

□ SYN Flood

Action: Random Early Drop

Alarm Rate (packets/s): 10000

Activate Rate (packets/s): 10000

Max Rate (packets/s): 40000

Block Duration (s): 300

DoS policies invoke protections specified in DoS Protection Profiles.

Rerefernces

- A video tutorial about implementing ZPP is here: https://live.paloaltonetworks.com/t5/Featured-Articles/Video-Tutorial-Zone-protection-profiles/ta-p/70687
- 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
- Recommendations for ZPP settings are here https://live.paloaltonetworks.com/t5/Learning-Articles/Zone-Protection-Recommendations/ta-p/55850
- A discussion of the differences between ZPP and DoS is here: https://live.paloaltonetworks.com/t5/Learning-Articles/Differences-between-DoS-Protection-and-Zone-Protection/ta-p/57761

Sample question

1. Why 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.

Answer under the heading Answer to Given a scenario, identify ways to mitigate resource exhaustion (because of denial-of-service) in application servers. on p. 116.

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 scanning difficult or impossible. As security practitioners, we are strongly motivated to implement Decryption policies to maximize the firewalls' visibility of packet contents.

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.

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/80/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:

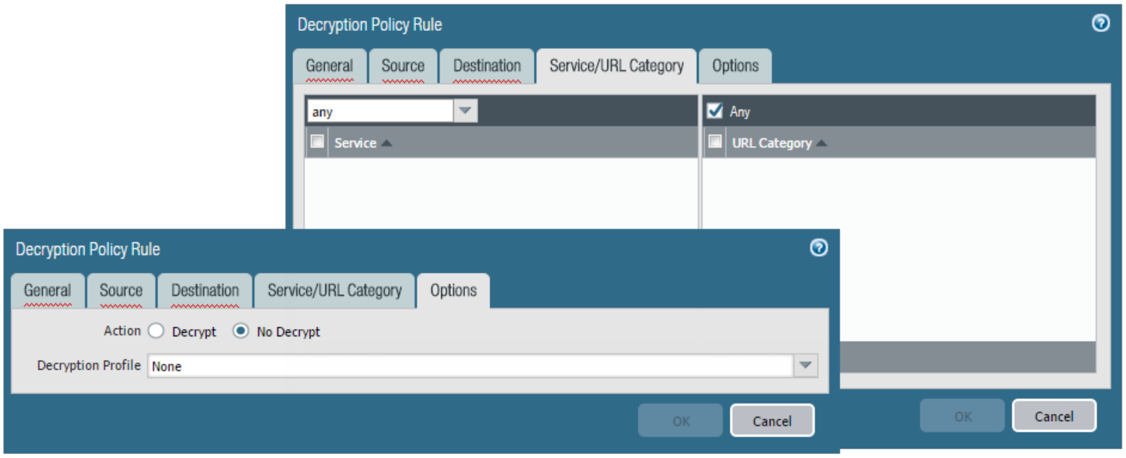
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/keys-and-certificates-for-decryption-policies#40372

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. D**evice > Certificate Management** is the central certificate work and storage area. A discussion of certificate use for all purposes in the firewall is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management/keys-and-certificates#61436

Decryption Policies

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.



any

☑ Any

Action ○ Decrypt ● No Decrypt

Decryption Profile None

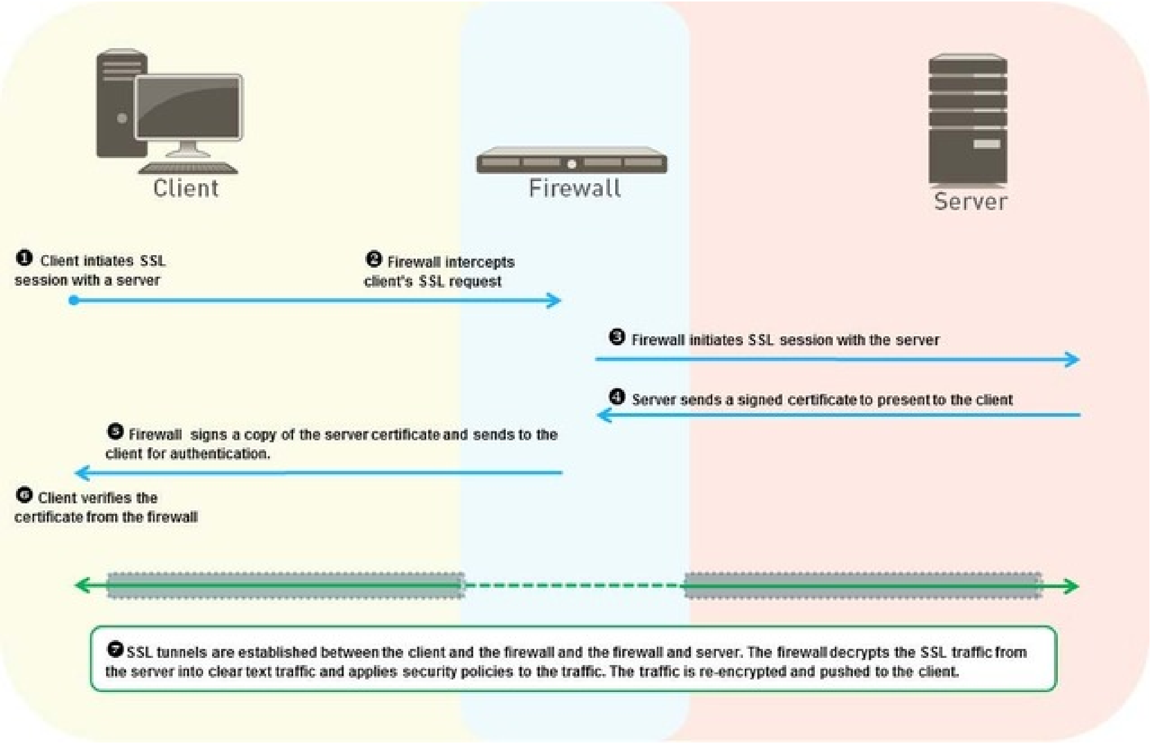
A Decryption policy and its action under the Options tab

A complete discussion of decryption concepts and detailed implementation topics is presented here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption

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.


Client
Firewall
Server
❶ Client intiates SSL session with a server
❷ Firewall intercepts client's SSL request
❸ Firewall initiates SSL session with the server
❹ Server sends a signed certificate to present to the client
❺ Firewall signs a copy of the server certificate and sends to the client for authentication.
❻ Client verifies the certificate from the firewall
❼ SSL tunnels are established between the client and the firewall and the firewall and server. The firewall decrypts the SSL traffic from the server into clear text traffic and applies security policies to the traffic. The traffic is re-encrypted and pushed to the client.

"Man in the Middle" deployment

Note that SSL Forward Proxy replaces the original certificate from the final destination 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 aren't 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 includes a list of these applications in a Decryption Bypass list embedded in PAN-OS® software. This list and its effects are explained here:

https://live.paloaltonetworks.com/t5/Configuration-Articles/List-of-Applications-Excluded-from-SSL-Decryption/ta-p/62201

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

App-ID and Encryption

The App-ID scanning engine's effectiveness often is compromised by encrypted traffic that prevents the 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

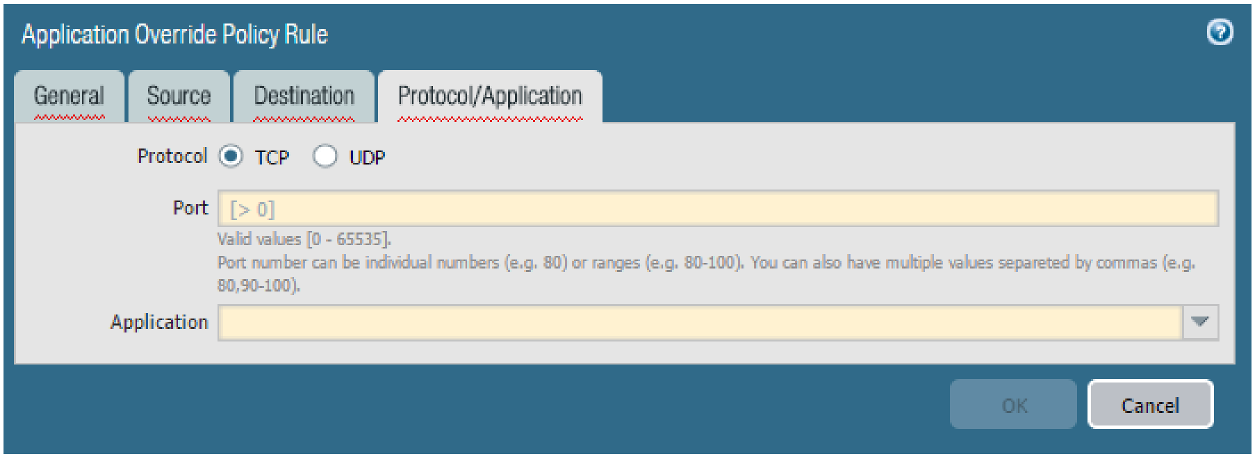
1. Which feature *never* requires a Decryption policy?
   A. antivirus
   B. App-ID
   C. file blocking
   D. network address translation
2. How can the NGFW inform web browsers that a web server's certificate is from an unknown certificate authority (CA)?
   A. Show a "the certificate is untrusted, 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.

© 2018 Palo Alto Networks, Inc.

Answers under the heading Answers to Identify decryption deployment strategies. on p. 116.

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

Application Override policies allow the firewall to identify traffic as that of a specified App-ID while bypassing all Layer 7 scanning, including App-ID and Content-ID.



Protocol ● TCP ○ UDP

Port [> 0]

Valid values [0 - 65535].
Port number can be individual numbers (e.g. 80) or ranges (e.g. 80-100). You can also have multiple values separeted by commas (e.g. 80,90-100).

Application

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:

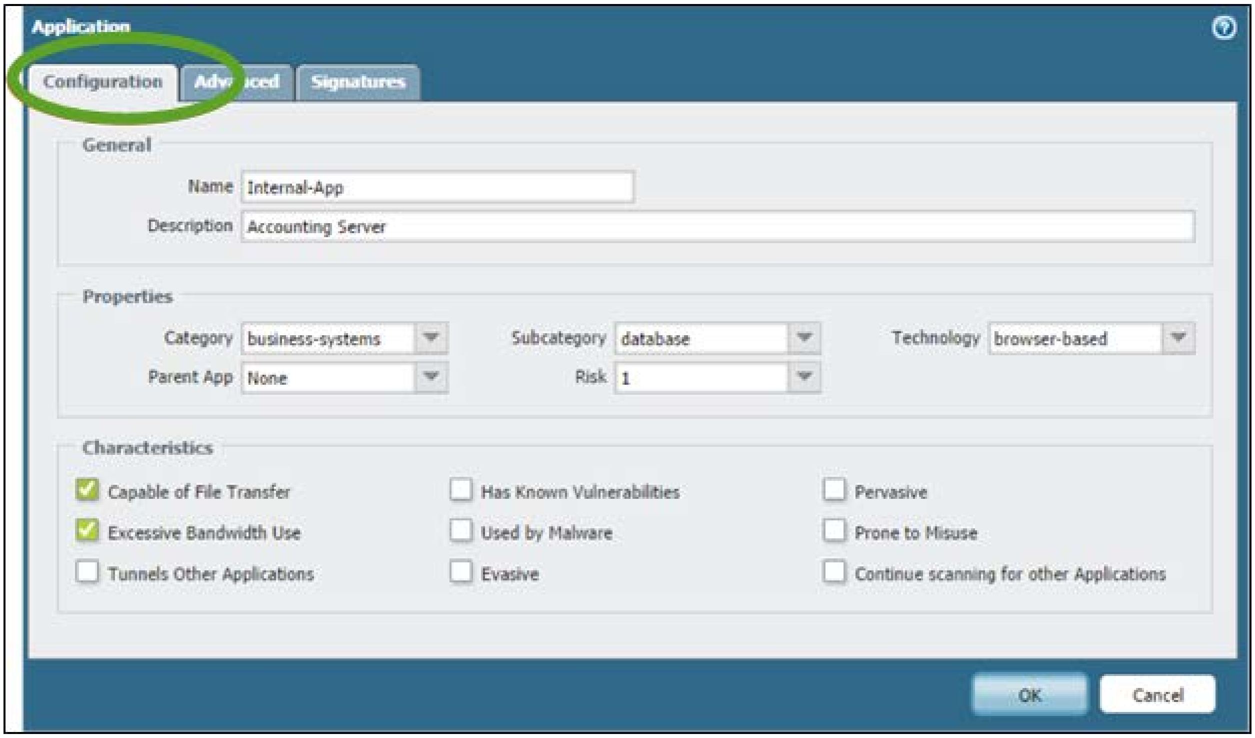
- To identify "Unknown" App-IDs with a different or custom application signature
- To re-identify an existing application signature
- To bypass the Signature Match Engine (within the SP3 architecture) to improve processing times

A discussion of typical application override uses 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:

© 2018 Palo Alto Networks, Inc.



General

Name: Internal-App

Description: Accounting Server

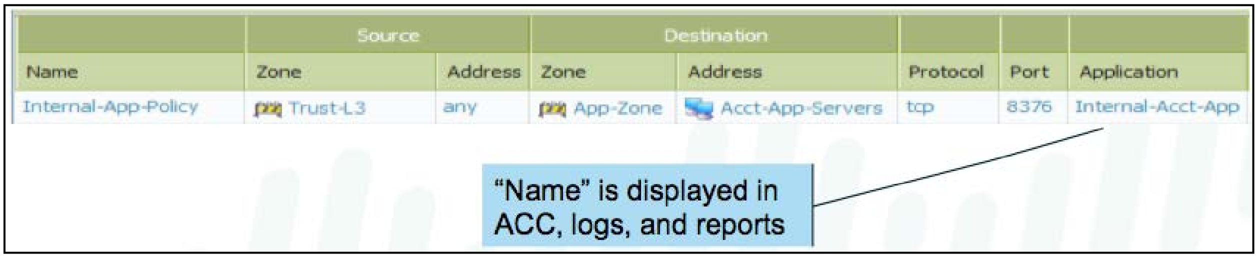
Properties

Category	business-systems	Subcategory	database	Technology	browser-based
Parent App	None	Risk	1		

Characteristics

☑ Capable of File Transfer	□ Has Known Vulnerabilities	□ Pervasive
☑ Excessive Bandwidth Use	□ Used by Malware	□ Prone to Misuse
□ Tunnels Other Applications	□ Evasive	□ Continue scanning for other Applications

Application override should assign purpose-built custom application definitions.



	Source		Destination				
Name	Zone	Address	Zone	Address	Protocol	Port	Application
Internal-App-Policy	Trust-L3	any	App-Zone	Acct-App-Servers	tcp	8376	Internal-Acct-App

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

Sample question

1. Which type of identification is disabled by Application Override?
    A. App-ID
    B. User-ID
    C. Content-ID

Answer under the heading Answers Identify the impact of application override to the overall functionality of the firewall on p. 117.

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 has to 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-IDs is only queried by a single firewall.

References

- Redistribute User Mappings and Authentication Timestamps https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/redistribute-user-mappings-and-authentication-timestamps
- User-ID Redistribution Using Panorama https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/user-id-redistribution-using-panorama

Sample question

1. How do layers facilitate the mapping (IP to user-ID) and the redistribution of that information?
   A. lThe 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 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 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 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).

Applications are identified by the information they transfer. If an application does not transfer enough information, it cannot be identified. If it transfers information, but is not known to Palo Alto Networks, it also cannot be identified. Several application "values" mean that the application cannot be identified.

References

- Manage Custom or Unknown Applications
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applications
- Not-Applicable, Incomplete, Insufficient Data in the Application Field
  https://live.paloaltonetworks.com/t5/Management-Articles/Not-Applicable-Incomplete-Insufficient-Data-in-the-Application/ta-p/65711

Sample question

1. Which type or types of application can cause an incomplete value in the Application field in the Traffic log?
   A. UDP
   B. TCP
   C. ICMP

Answer under the heading Answe to Identify the application meanings in the Traffic log (incomplete, insufficient data, non-syn TCP, not applicable, unknown TCP, unknown UDP, and unknown P2P). on p. 117.

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

Most Security Profiles are attached to rules to implement Content-ID to scan for and prevent harmful content of various kinds.

References

- Security Profiles
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles
- Create Best Practice Security Profiles
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/create-best-practice-security-profiles#_48239

Sample question

1. Which profile do you use for DLP (data loss protection)?

© 2018 Palo Alto Networks, Inc.

A. Antivirus
B. URL Filtering
C. File Blocking
D. Data Filtering

Answer under the heading Answers to Given a scenario, identify the set of Security Profiles that should be used. on p. 117.

Identify the relationship between URL filtering and credential theft prevention.

Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose which websites you want to either allow, alert on, or block corporate credential submissions based on the URL category of the website. Or you can present a page that warns users against submitting credentials to sites classified in certain URL categories. Having such a page presented gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. If corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate.

References

- Credential Phishing Prevention
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/credential-phishing-prevention
- PAN-OS 8.0: Preventing Credential-Based Attacks
  https://researchcenter.paloaltonetworks.com/2017/02/pan-os-8-0-preventing-credential-based-attacks/

Sample questions

1. Which credential phishing prevention action allows users to decide to submit to a site anyway?
   A. Alert
   B. Allow
   C. Block
   D. Continue
2. 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

Answers under the heading Answers to Identify the relationship between URL filtering and credential theft prevention. on p. 117.

Identify differences between services and applications

Applications identification (App-ID) is central to the operation of the NGFW. Port filters no longer are 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.

References

- Objects > Applications https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-applications#_96266
- Objects > Application Groups https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-application-groups
- Objects > Services https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-services

Sample question

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

Answer under the heading Answer to Identify differences between services and applications on p. 117.

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

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.

References

- Policies > Security https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/policies/policies-security#_67396
- Application Based Policies https://www.paloaltonetworks.com/resources/datasheets/application-based-policies

Sample question

1. Which two applications cannot be distinguished by port number? (Choose two.)

A. Microsoft Outlook Express email
B. Google mail (Gmail)
C. SSH
D. Facebook
E. FTP

Answer under the heading Answer to Identify how to create security rules to implement App-ID without relying on port-based rules. on p. 117.

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.

Note: Virtual firewalls must be licensed after initial configuration is performed. See this information for an explanation:

https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/license-the-vm-series-firewall/activate-the-license

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/80/pan-os/pan-os

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/80/pan-os/pan-os/getting-started/activate-licenses-and-subscriptions#75905

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/80/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/80/pan-os/pan-os

Sample questions

1. 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.
2. 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

Answers under the heading Answers to Identify the required settings and steps necessary to provision and deploy a next-generation firewall. on p. 117.

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

See Identify methods for authorization, authentication, and device administration. above.

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

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

A discussion of certificate use and management is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management

An exploration of many SSL certificate-related technical issues, including implementation and troubleshooting, is here:

https://live.paloaltonetworks.com/t5/Management-Articles/SSL-certificates-resource-list/ta-p/53068

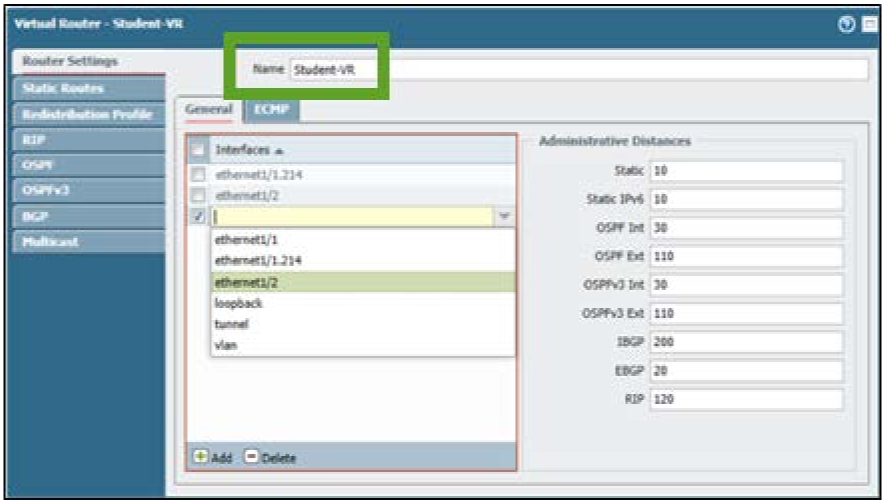
Sample question

1. 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

Answer under the heading Answer to Identify how to configure and maintain certificates to support firewall features. on p. 117.

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.



Name: Student-VR

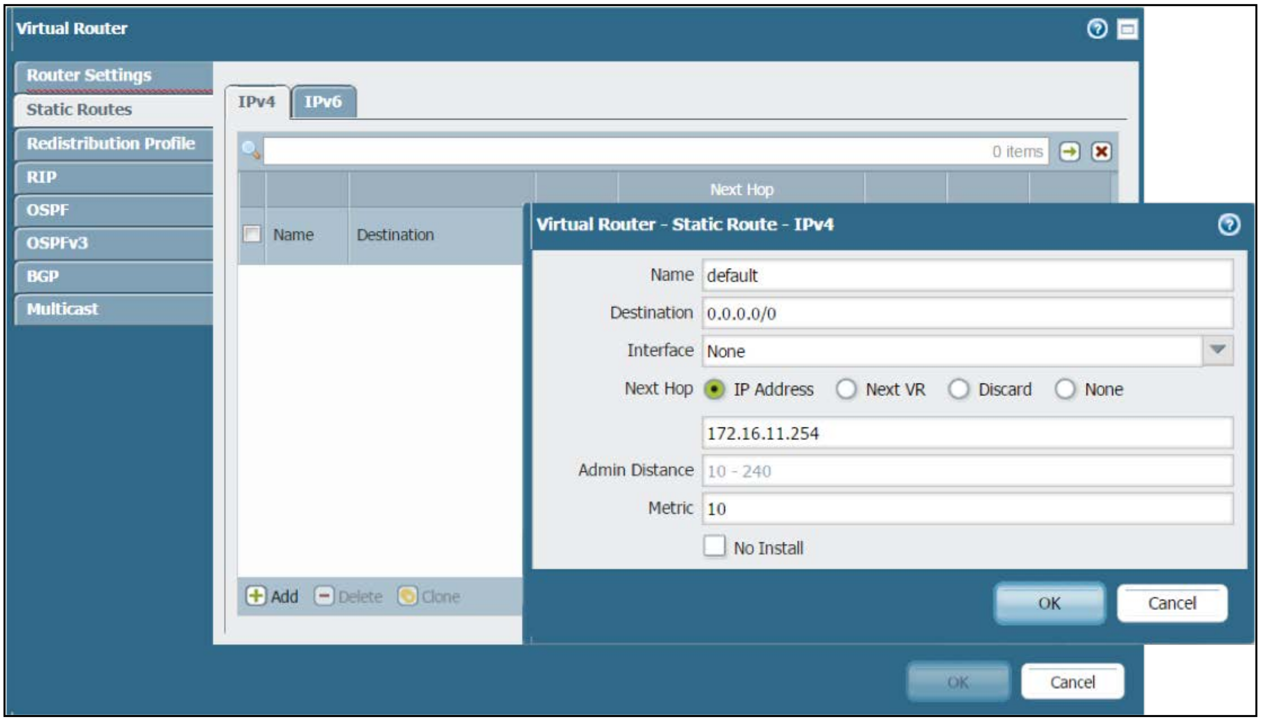
□	Interfaces ▲
□	ethernet1/1.214
□	ethernet1/2
☑	

ethernet1/1
ethernet1/1.214
ethernet1/2
loopback
tunnel
vlan

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Virtual routers handle all Layer 3 forwarding decisions.

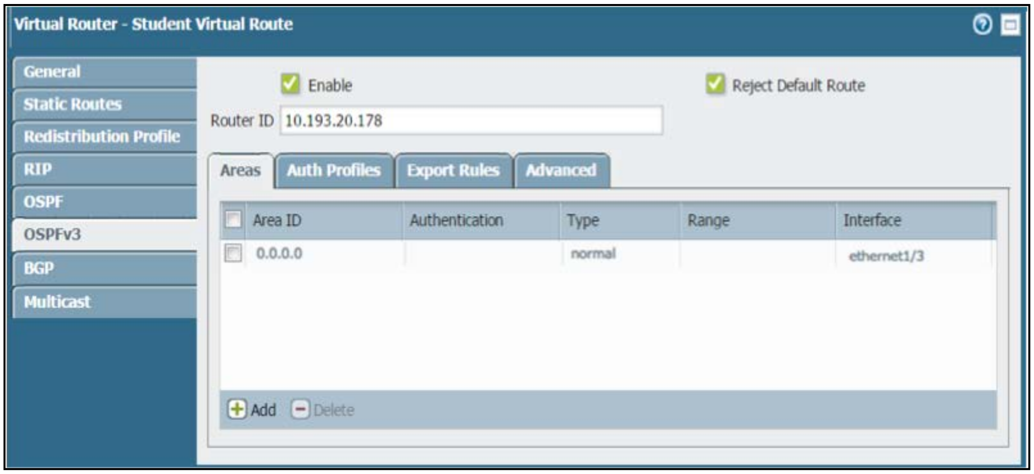


Virtual Router - Static Route - IPv4

Name: default
Destination: 0.0.0.0/0
Interface: None
Next Hop: ● IP Address ○ Next VR ○ Discard ○ None
172.16.11.254
Admin Distance: 10 - 240
Metric: 10
□ No Install

Static route creation in a virtual router

© 2018 Palo Alto Networks, Inc.



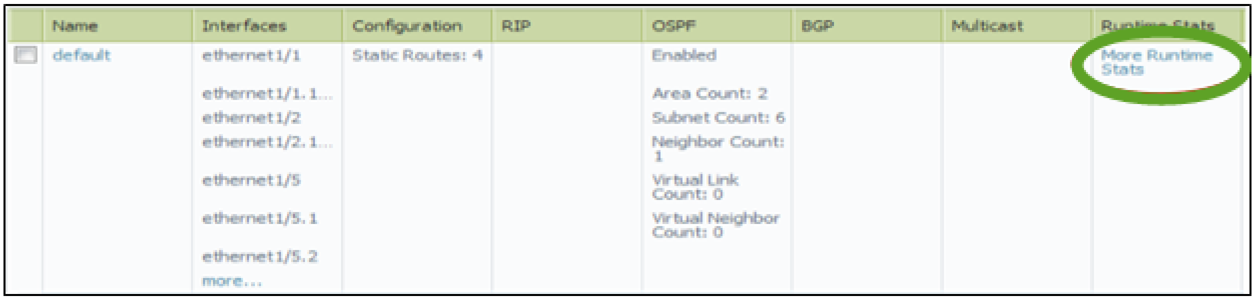
Virtual Router - Student Virtual Route

☑ Enable ☑ Reject Default Route

Router ID 10.193.20.178

□ Area ID	Authentication	Type	Range	Interface
□ 0.0.0.0		normal		ethernet1/3

An example dynamic routing protocol configuration



	Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
□	default	ethernet1/1 ethernet1/1.1... ethernet1/2 ethernet1/2.1... ethernet1/5 ethernet1/5.1 ethernet1/5.2 more...	Static Routes: 4		Enabled Area Count: 2 Subnet Count: 6 Neighbor Count: 1 Virtual Link Count: 0 Virtual Neighbor Count: 0			More Runtime Stats

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/80/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 question

1. You finished configuring the firewall's basic connectivity in the lab, and are ready to put it in the data center. What, if anything, do you have to remember to do before you power down the firewall?
   A. Save the changes.
   B. Commit the changes.
   C. Apply the changes.
   D. There is nothing you need to do – the changes are saved and applied automatically.

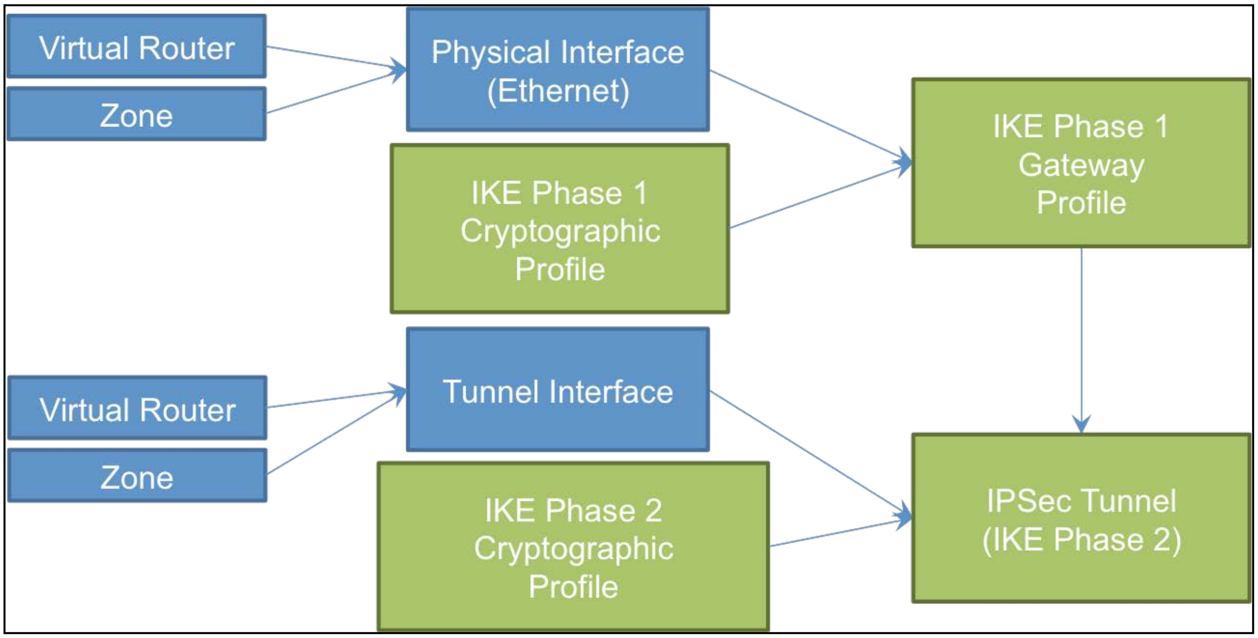
© 2018 Palo Alto Networks, Inc.

Answer under the heading Answer to Identify how to configure a virtual router. on p. 117.

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.


Virtual Router
Zone
Physical Interface (Ethernet)
IKE Phase 1 Cryptographic Profile
IKE Phase 1 Gateway Profile
Virtual Router
Zone
Tunnel Interface
IKE Phase 2 Cryptographic Profile
IPSec Tunnel (IKE Phase 2)

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/80/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 question

1. Which type is a tunnel interface?
    A. Tap
    B. virtual wire
    C. Layer 2
    D. Layer 3

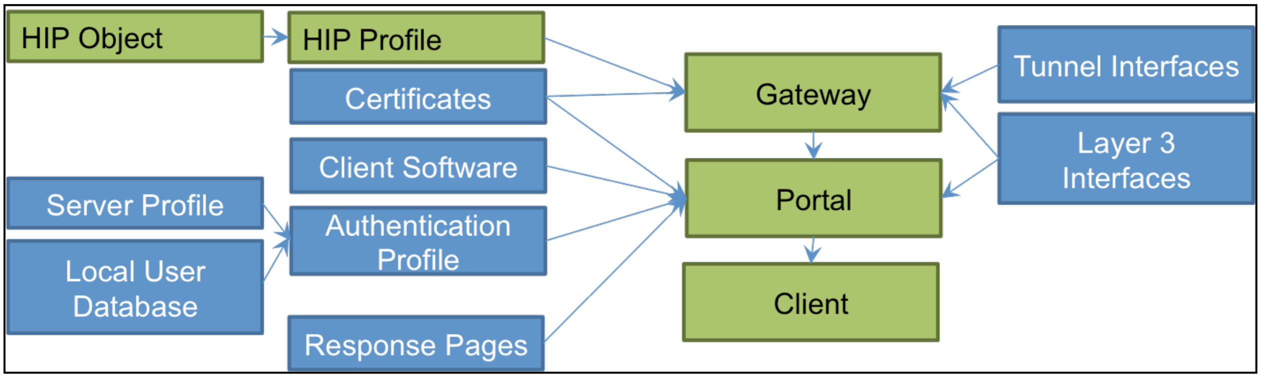
Answer under the heading Answer to Identify the configuration settings for site-to-site VPN. on p. 117.

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.

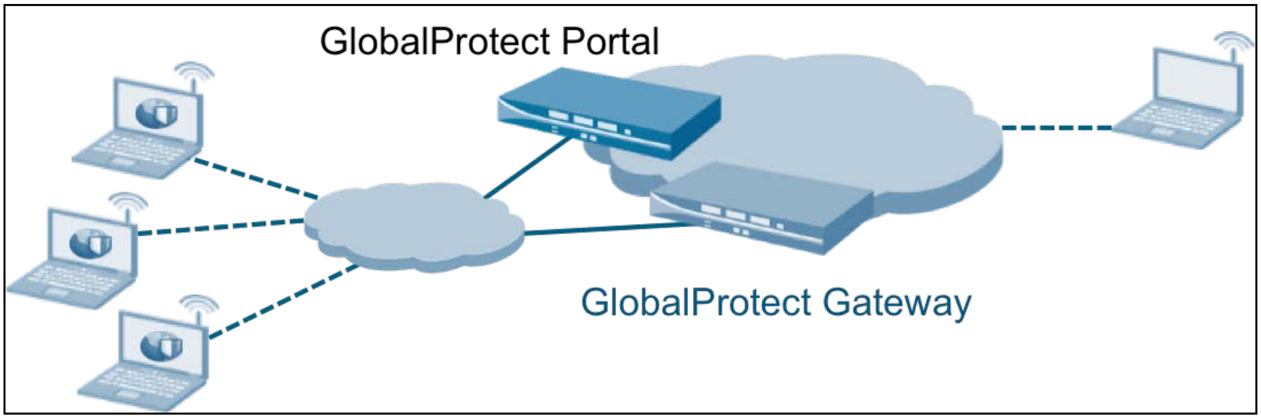
GlobalProtect comprises many different components. An understanding of those basic components is the starting point for a successful deployment. The GlobalProtect Portal performs the initial authentication of a client, downloads/upgrades the GlobalProtect Client, performs a host information profile (HIP) 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.

© 2018 Palo Alto Networks, Inc.

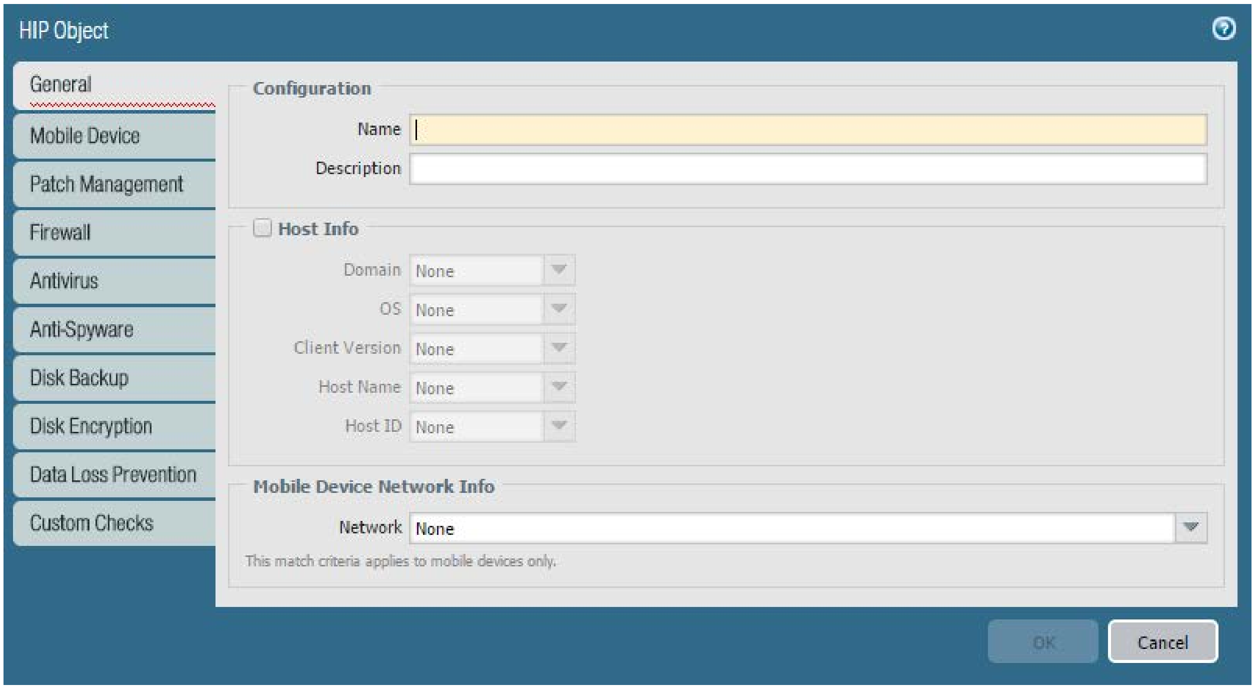


The GlobalProtect architectural components in a typical implementation.

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).

iOS and Android devices can access GlobalProtect client software at no cost in their application stores. Connection to the firewall, however, requires an extra-cost license.

With the appropriate license, HIP checks can be performed by GlobalProtect agent software on the client platforms at connect time. This information is a “security-oriented” inventory of the endpoint environment.


HIP Object

General
Mobile Device
Patch Management
Firewall
Antivirus
Anti-Spyware
Disk Backup
Disk Encryption
Data Loss Prevention
Custom Checks

Configuration

Name
Description

□ Host Info

Domain: None
OS: None
Client Version: None
Host Name: None
Host ID: None

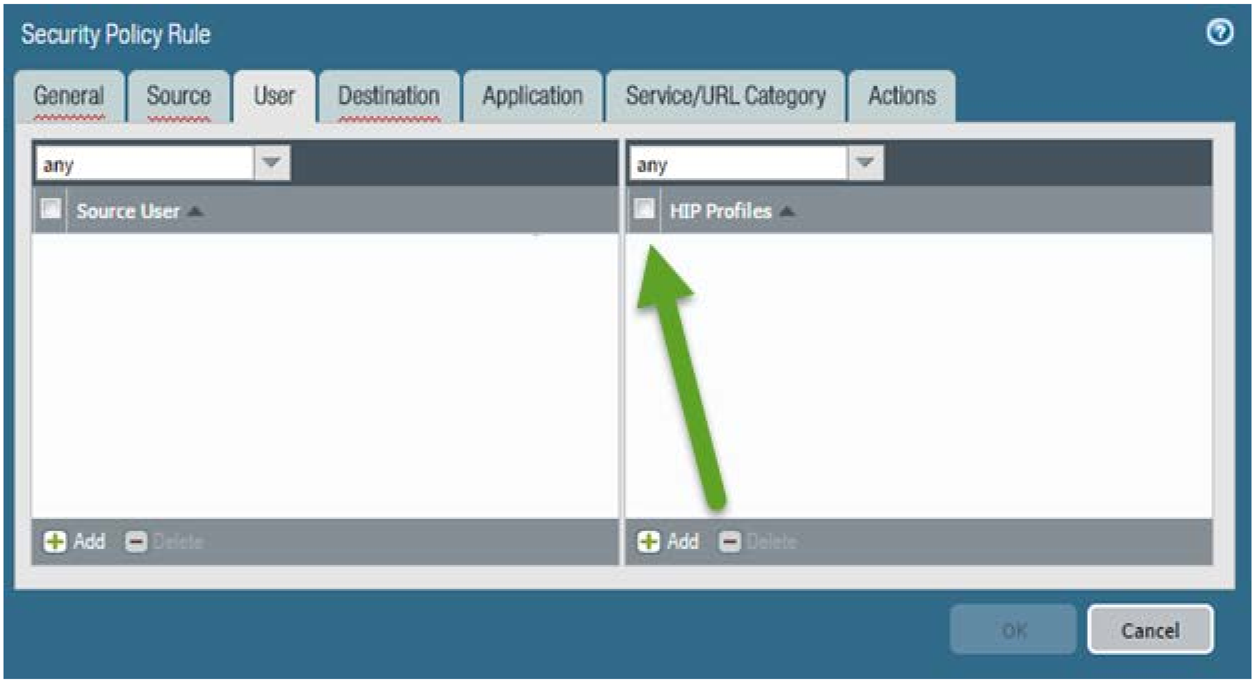
Mobile Device Network Info

Network: None

This match criteria applies to mobile devices only.

HIP Object components

Information from these reports can be extracted and made into logical true/false objects for use in Security policies, thus providing appropriate access, depending on endpoint configuration.



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

References

- Configuration of the firewall for GlobalProtect is discussed here: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/get-started
- HIP checking implementation and use is explored in detail here: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/host-information

Sample questions

1. Which operating system is not supported for use with GlobalProtect clients?
   A. iOS
   B. Android
   C. Windows
   D. z/OS
2. 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

Answers under the heading Answers to Identify the configuration settings for GlobalProtect. on p. 117.

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

Most denial-of-service (DoS) attacks rely on sending so many packets that some component cannot process all of them (that component can be the firewall or the server behind it). The NGFW makes such attacks more difficult through several mechanisms that quickly precheck and discard packets that are likely to be DoS attacks.

References

- Network > Network Profiles > Zone Protection
  https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-network-profiles-zone-protection
- Policies > DoS Protection
  https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/policies/policies-dos-protection#_89647

Sample questions

1. To which protocol or protocols does the SYN flood protection?
   A. UDP
   B. TCP
   C. ICMP
   D. GRE
2. To which two protocols does port scan reconnaissance protection apply? (Choose two)
   A. UDP
   B. TCP
   C. GRE
   D. ICMP
   E. IPX
3. 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

Answers under the heading Answers to Identify how to configure items pertaining to denial-of-service protection and zone protection. on p. 118.

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/80/pan-os/web-interface-help/policies/policies-nat#_38816

Sample question

1. Which NAT type can be used to translate between IPv4 and IPv6?
   A. ipv4
   B. nat64
   C. nptv6

Answer under the heading Answers to Identify how to configure features of the NAT rulebase. on p. 118.

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

Security Policies allow you to enforce rules and act, 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/80/pan-os/web-interface-help/policies/policies-security#_54026

Sample question

1. 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. 192.168.4.0/26
   D. 192.168.0.0/16
   E. 75.22.0.0/17
   F. 75.22.128.0/17

Answer under the heading Answer to Given a configuration example including DNAT, identify how to configure security rules. on p. 118.

© 2018 Palo Alto Networks, Inc.

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.

References

- Policies > Decryption
  https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/policies/policies-decryption#_56365
- SSL Forward Proxy
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/ssl-forward-proxy
- SSL Inbound Inspection
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/ssl-inbound-inspection
- SSH Proxy
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/ssh-proxy)
- Configure SSL Forward Proxy
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-forward-proxy
- Configure SSL Inbound Inspection
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection
- Configure SSH Proxy
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy#_46345

Sample questions

1. Which protocol is supported for traffic decryption?
   A. IPsec
   B. SP3
   C. SSH
   D. NLSP
2. 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

Answers under the heading Answers to Identify how to configure decryption. on p. 118.

© 2018 Palo Alto Networks, Inc.

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. 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.

References

- Policies > Application Override
  https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/policies/policies-application-override#_81068
- Create a Custom Application
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/create-a-custom-application

Sample question

1. 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

Answer under the heading Answer to Given a scenario, identify an application override configuration and use case. on p. 118.

Identify how to configure VM-Series firewalls for deployment.

To install a VM-Series firewall you must have access to the Open Virtualization Alliance format (OVA) template. Use the auth code you received in your order fulfillment email to register your VM-Series firewall and gain access to the OVA template. The OVA is downloaded as a zip archive that is expanded into three files: the .ovf extension is for the OVF descriptor file that contains all metadata about the package and its contents; the .mf extension is for the OVF manifest file that contains the SHA-1 digests of individual files in the package; and the .vmdk extension is for the virtual disk image file that contains the virtualized version of the firewall.

References

- Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi)
  https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-a-vm-series-firewall-on-an-esxi-server/install-a-vm-series-firewall-on-vmware-vsphere-hypervisor-esxi#_96904

- Install the VM-Series Firewall on Hyper-V https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-hyper-v/install-the-vm-series-firewall-on-hyper-v#_88880
- Set Up the VM-Series firewall on AWS https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-aws

Sample questions

1. 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
2. Which three items of information are required 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

Answer under the heading Answers to Identify how to configure VM-Series firewalls for deployment. on p. 118.

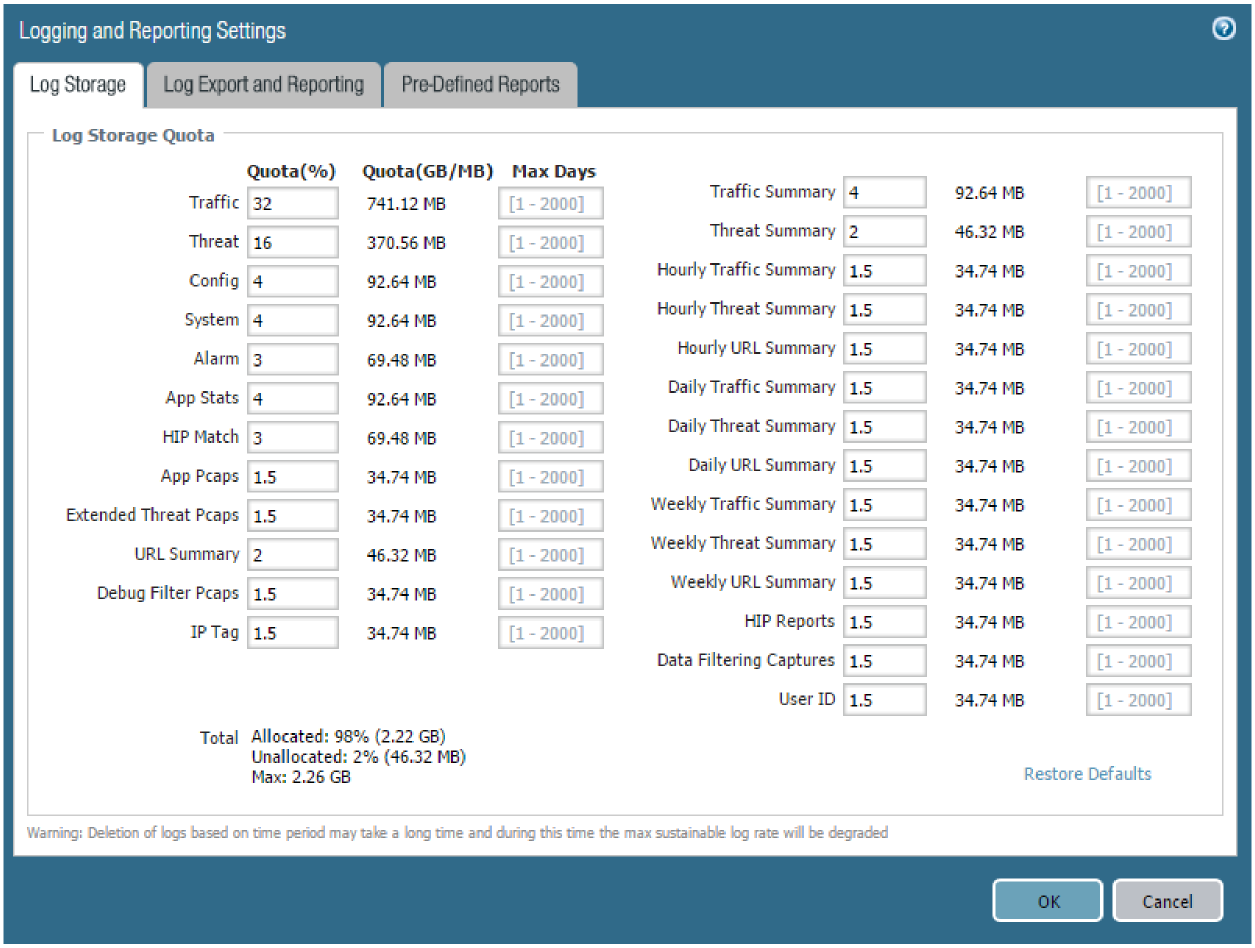
Exam Domain 3 – Operate

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.

Log storage on Palo Alto Networks firewalls is strictly allocated between different log and other storage types to ensure that no particular log is overrun by another. This allocation is user-controlled.



Log Storage Quota

	Quota(%)	Quota(GB/MB)	Max Days
Traffic	32	741.12 MB	[1 - 2000]
Threat	16	370.56 MB	[1 - 2000]
Config	4	92.64 MB	[1 - 2000]
System	4	92.64 MB	[1 - 2000]
Alarm	3	69.48 MB	[1 - 2000]
App Stats	4	92.64 MB	[1 - 2000]
HIP Match	3	69.48 MB	[1 - 2000]
App Pcaps	1.5	34.74 MB	[1 - 2000]
Extended Threat Pcaps	1.5	34.74 MB	[1 - 2000]
URL Summary	2	46.32 MB	[1 - 2000]
Debug Filter Pcaps	1.5	34.74 MB	[1 - 2000]
IP Tag	1.5	34.74 MB	[1 - 2000]

Traffic Summary	4	92.64 MB	[1 - 2000]
Threat Summary	2	46.32 MB	[1 - 2000]
Hourly Traffic Summary	1.5	34.74 MB	[1 - 2000]
Hourly Threat Summary	1.5	34.74 MB	[1 - 2000]
Hourly URL Summary	1.5	34.74 MB	[1 - 2000]
Daily Traffic Summary	1.5	34.74 MB	[1 - 2000]
Daily Threat Summary	1.5	34.74 MB	[1 - 2000]
Daily URL Summary	1.5	34.74 MB	[1 - 2000]
Weekly Traffic Summary	1.5	34.74 MB	[1 - 2000]
Weekly Threat Summary	1.5	34.74 MB	[1 - 2000]
Weekly URL Summary	1.5	34.74 MB	[1 - 2000]
HIP Reports	1.5	34.74 MB	[1 - 2000]
Data Filtering Captures	1.5	34.74 MB	[1 - 2000]
User ID	1.5	34.74 MB	[1 - 2000]

Total Allocated: 98% (2.22 GB)
Unallocated: 2% (46.32 MB)
Max: 2.26 GB

Restore Defaults

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

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.

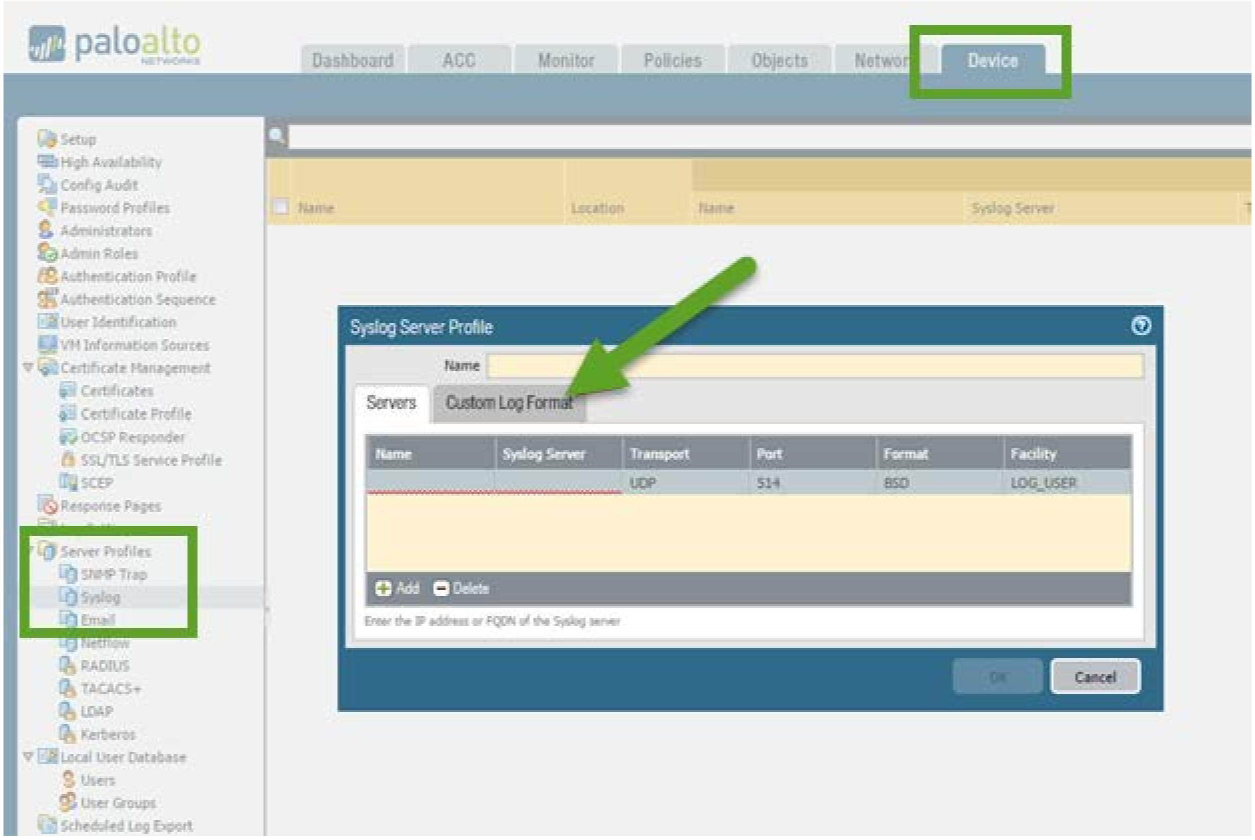
Before you can use Panorama or external systems to monitor the firewall, you must configure the firewall to forward its logs. Before forwarding to external services, the firewall automatically converts the logs to the necessary format: syslog messages, SNMP traps, HTTP, or email notifications. Before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

External forwarding supports the following types of destinations:

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

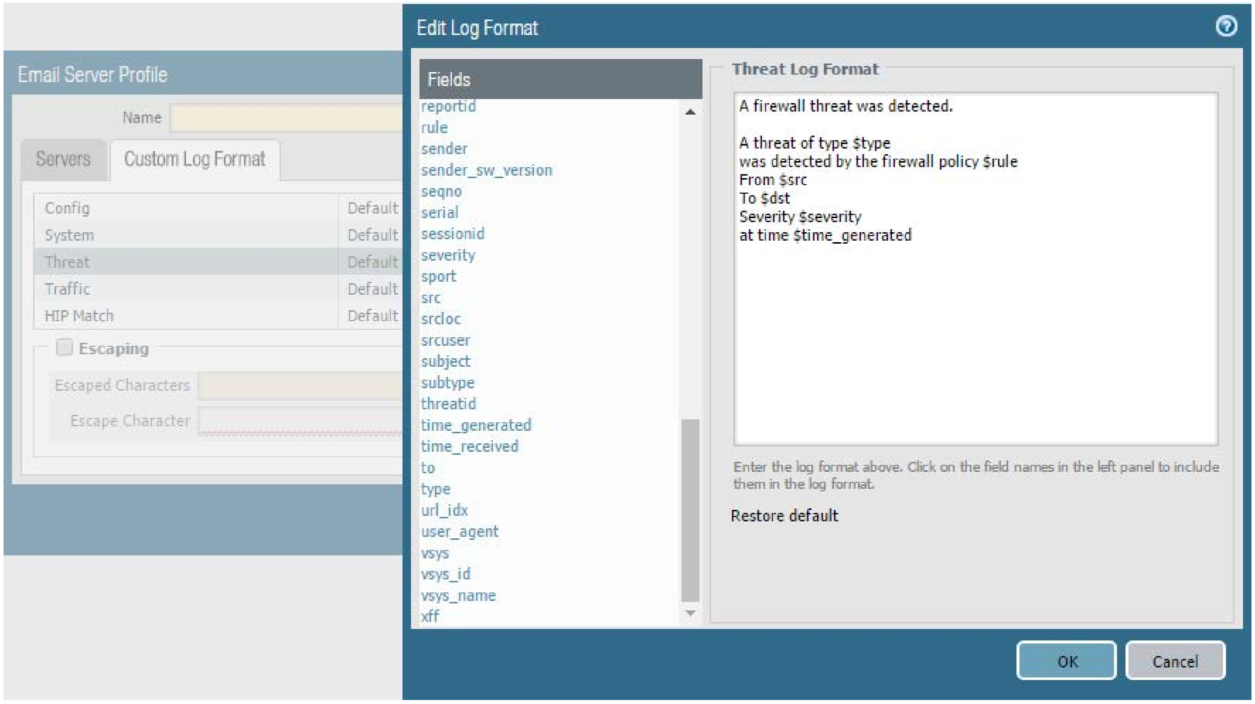
All types (other than Panorama) support customization of the message format. A typical destination configuration follows:

© 2018 Palo Alto Networks, Inc.



Creating a Syslog log forwarding destination

An example of a customized message format for an email destination follows.



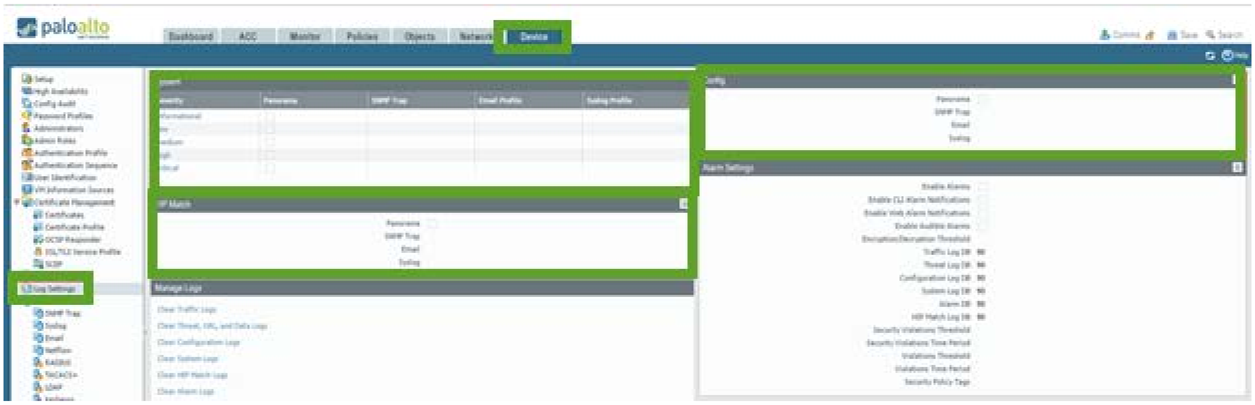
```
A firewall threat was detected.

A threat of type $type
was detected by the firewall policy $rule
From $src
To $dst
Severity $severity
at time $time_generated
```

An example of a customized email message

© 2018 Palo Alto Networks, Inc.

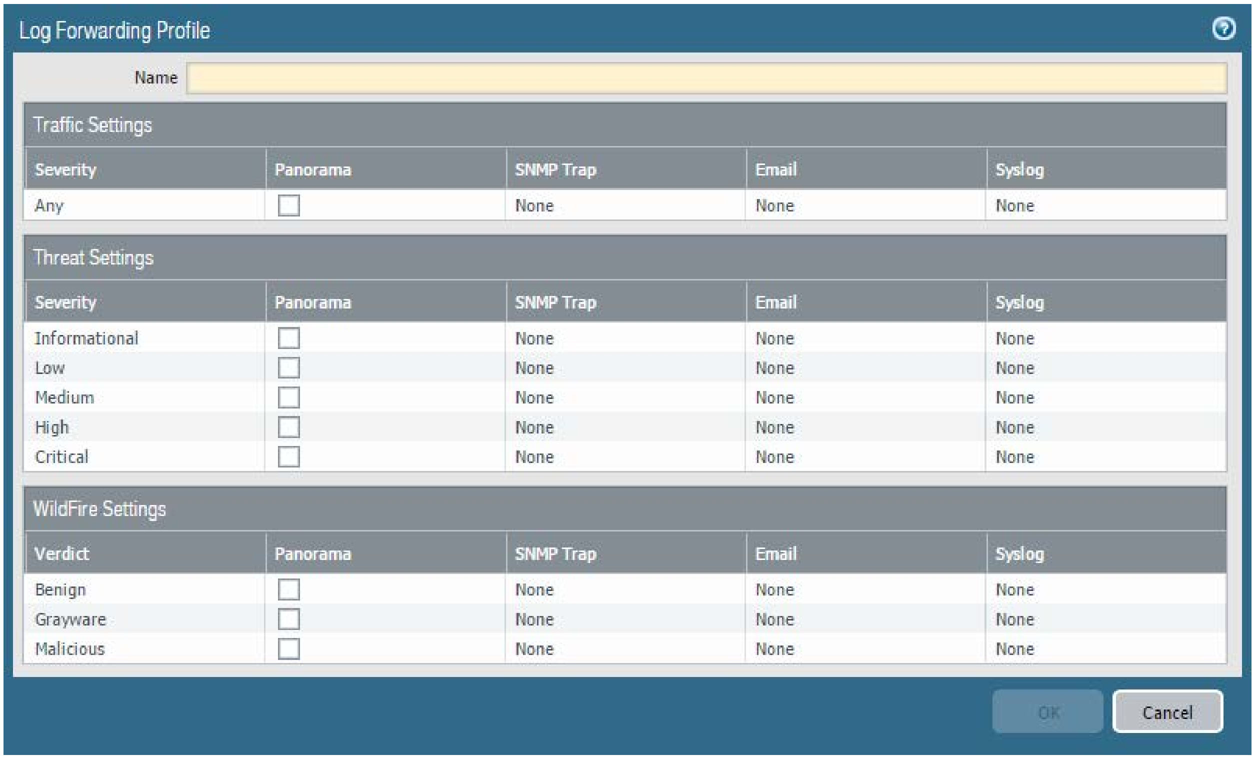
Any log event redirection causes a copy of the log event to be forwarded as specified. It is logged on the firewall as usual.

There are two main methods to forward log events, depending on the log message type. Log events destined for the System, Config, 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

Events normally written to the Traffic, Threat, and WildFire Submission logs are routed via a Log Forwarding Profile:



Name

Traffic Settings

Severity	Panorama	SNMP Trap	Email	Syslog
Any	□	None	None	None

Threat Settings

Severity	Panorama	SNMP Trap	Email	Syslog
Informational	□	None	None	None
Low	□	None	None	None
Medium	□	None	None	None
High	□	None	None	None
Critical	□	None	None	None

WildFire Settings

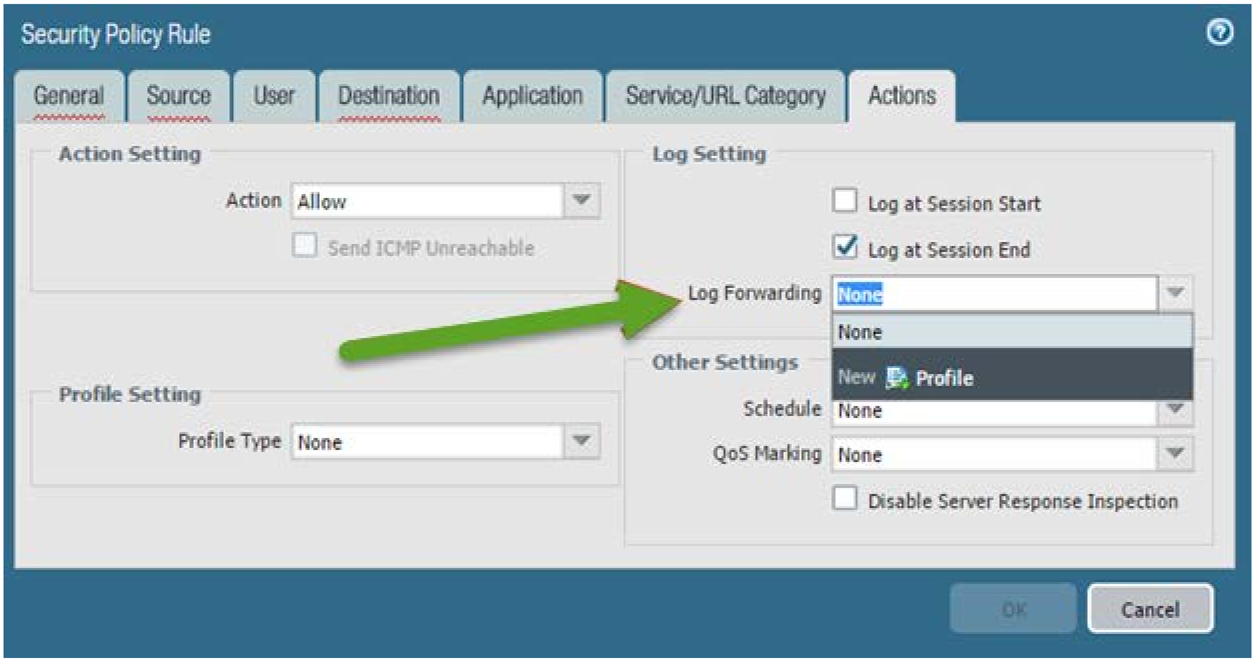
Verdict	Panorama	SNMP Trap	Email	Syslog
Benign	□	None	None	None
Grayware	□	None	None	None
Malicious	□	None	None	None

A Log Forwarding Profile specifying which log events are to be forwarded to which predefined destinations.

Log Forwarding Profiles are attached to individual firewall Security policies to enable forwarding of the events associated with the processing of the specific policy. This granularity allows administrators

© 2018 Palo Alto Networks, Inc.

specific control of forwarding and the potential of different forwarding for policies of differing importance:



Action: Allow

□ Send ICMP Unreachable

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Type: None

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Assigning a Log Forwarding Profile to a Security policy

All forwarded events are delivered as they are generated on the firewall.

A complete discussion of log forwarding configuration is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/configure-log-forwarding

Sample questions

1. Which log format is *not* supported for log exports? (C)
   A. SNMP trap
   B. Syslog
   C. Apache log format
   D. HTTP
2. Which log type gets redirected using a Log Forwarding Profile? (B)
   A. Config log
   B. Traffic log
   C. System log
   D. HIP Match log

Answers under the heading Answers to Identify considerations for configuring external log forwarding. on p. 118.

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

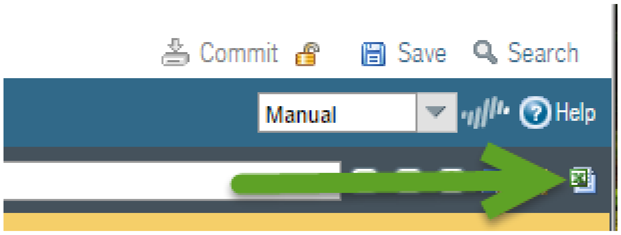
Logging and reporting are critical components of any security network. Being able to log all network activity in a logical, organized, and easily segmented way makes logging even more valuable. Rapid, thorough, and accurate interpretation of events is critical to security. Security practitioners often 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® 8.0 includes a Unified log that collects copies of events from the Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs into a single location for easy parsing of related data.

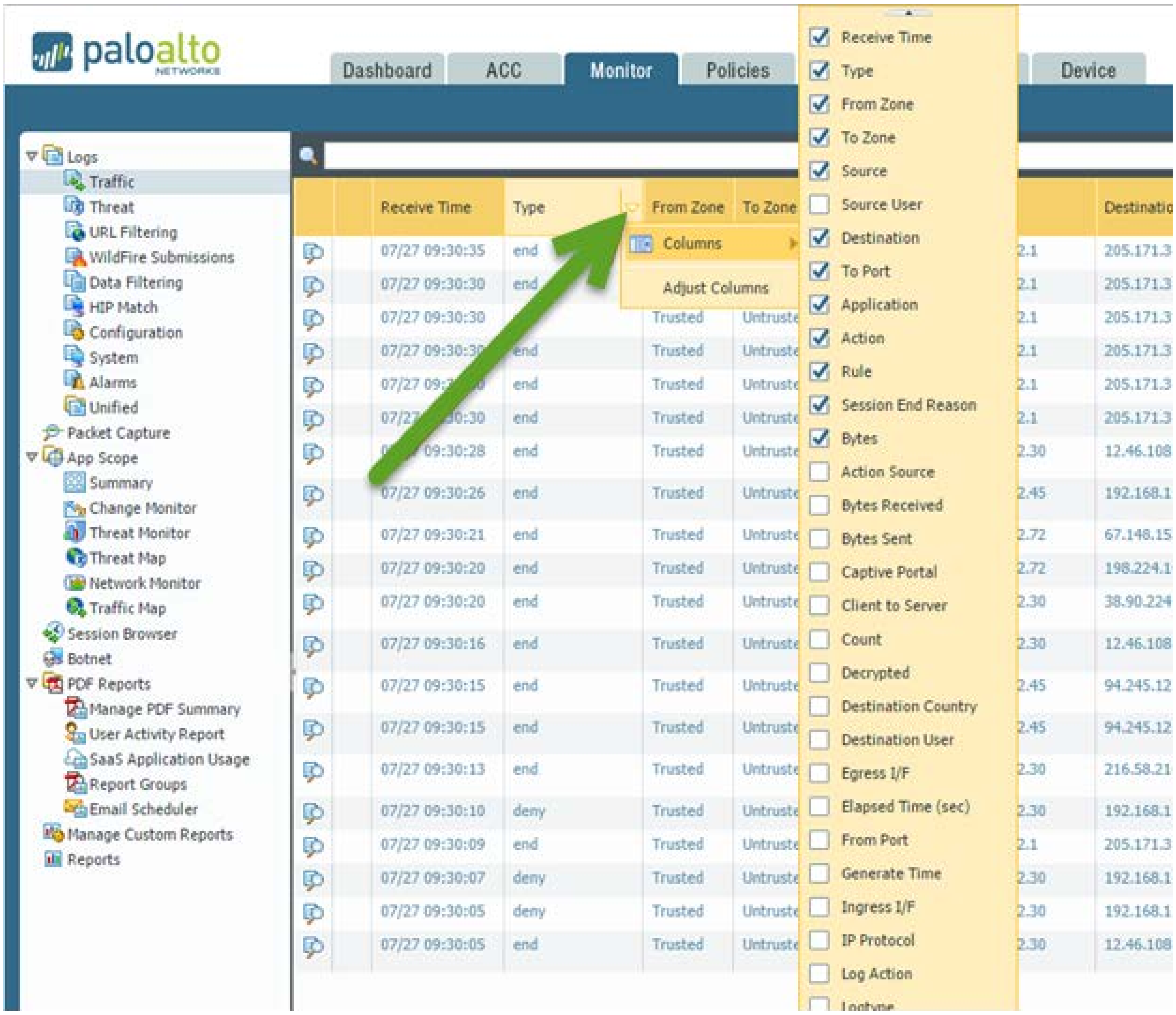
Each log provides similar features, making an organized presentation of desired data. Displayed log data can be exported in CSV format at any time.



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.

Displayed columns can be configured to present desired data.

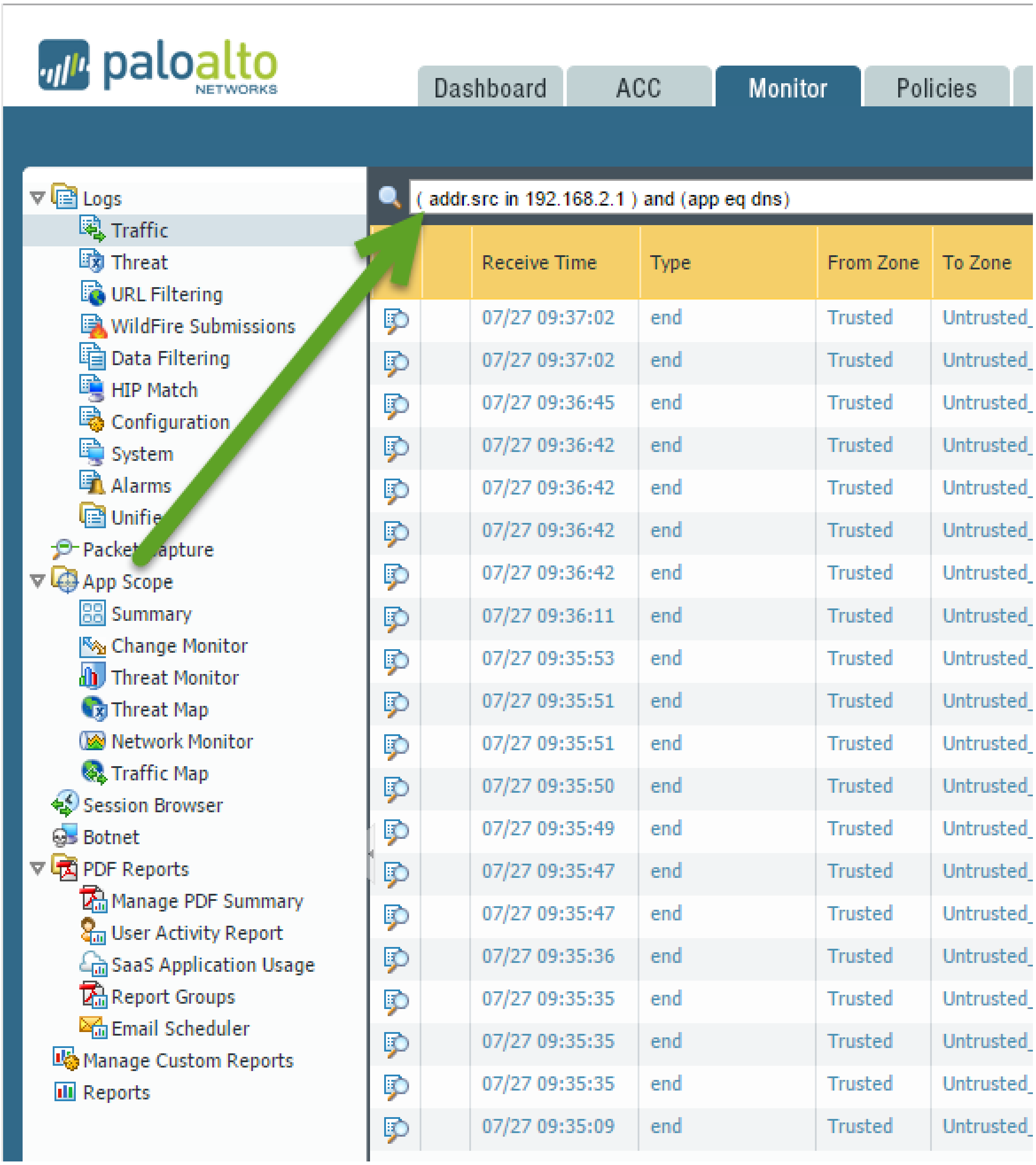


Receive Time	Type	From Zone	To Zone		Destinatio
07/27 09:30:35	end			2.1	205.171.3
07/27 09:30:30	end			2.1	205.171.3
07/27 09:30:30		Trusted	Untruste	2.1	205.171.3
07/27 09:30:3	end	Trusted	Untruste	2.1	205.171.3
07/27 09:[illegible]	end	Trusted	Untruste	2.1	205.171.3
07/2[illegible]0:30	end	Trusted	Untruste	2.1	205.171.3
[illegible] 09:30:28	end	Trusted	Untruste	2.30	12.46.108
07/27 09:30:26	end	Trusted	Untruste	2.45	192.168.1
07/27 09:30:21	end	Trusted	Untruste	2.72	67.148.15
07/27 09:30:20	end	Trusted	Untruste	2.72	198.224.1
07/27 09:30:20	end	Trusted	Untruste	2.30	38.90.224
07/27 09:30:16	end	Trusted	Untruste	2.30	12.46.108
07/27 09:30:15	end	Trusted	Untruste	2.45	94.245.12
07/27 09:30:15	end	Trusted	Untruste	2.45	94.245.12
07/27 09:30:13	end	Trusted	Untruste	2.30	216.58.21
07/27 09:30:10	deny	Trusted	Untruste	2.30	192.168.1
07/27 09:30:09	end	Trusted	Untruste	2.1	205.171.3
07/27 09:30:07	deny	Trusted	Untruste	2.30	192.168.1
07/27 09:30:05	deny	Trusted	Untruste	2.30	192.168.1
07/27 09:30:05	end	Trusted	Untruste	2.30	12.46.108

- ☑ Receive Time
- ☑ Type
- ☑ From Zone
- ☑ To Zone
- ☑ Source
- □ Source User
- ☑ Destination
- ☑ To Port
- ☑ Application
- ☑ Action
- ☑ Rule
- ☑ Session End Reason
- ☑ Bytes
- □ Action Source
- □ Bytes Received
- □ Bytes Sent
- □ Captive Portal
- □ Client to Server
- □ Count
- □ Decrypted
- □ Destination Country
- □ Destination User
- □ Egress I/F
- □ Elapsed Time (sec)
- □ From Port
- □ Generate Time
- □ Ingress I/F
- □ IP Protocol
- □ Log Action
- □ Logtype

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.



(addr.src in 192.168.2.1) and (app eq dns)

Receive Time	Type	From Zone	To Zone
07/27 09:37:02	end	Trusted	Untrusted_
07/27 09:37:02	end	Trusted	Untrusted_
07/27 09:36:45	end	Trusted	Untrusted_
07/27 09:36:42	end	Trusted	Untrusted_
07/27 09:36:42	end	Trusted	Untrusted_
07/27 09:36:42	end	Trusted	Untrusted_
07/27 09:36:42	end	Trusted	Untrusted_
07/27 09:36:11	end	Trusted	Untrusted_
07/27 09:35:53	end	Trusted	Untrusted_
07/27 09:35:51	end	Trusted	Untrusted_
07/27 09:35:51	end	Trusted	Untrusted_
07/27 09:35:50	end	Trusted	Untrusted_
07/27 09:35:49	end	Trusted	Untrusted_
07/27 09:35:47	end	Trusted	Untrusted_
07/27 09:35:47	end	Trusted	Untrusted_
07/27 09:35:36	end	Trusted	Untrusted_
07/27 09:35:35	end	Trusted	Untrusted_
07/27 09:35:35	end	Trusted	Untrusted_
07/27 09:35:35	end	Trusted	Untrusted_
07/27 09:35:09	end	Trusted	Untrusted_

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

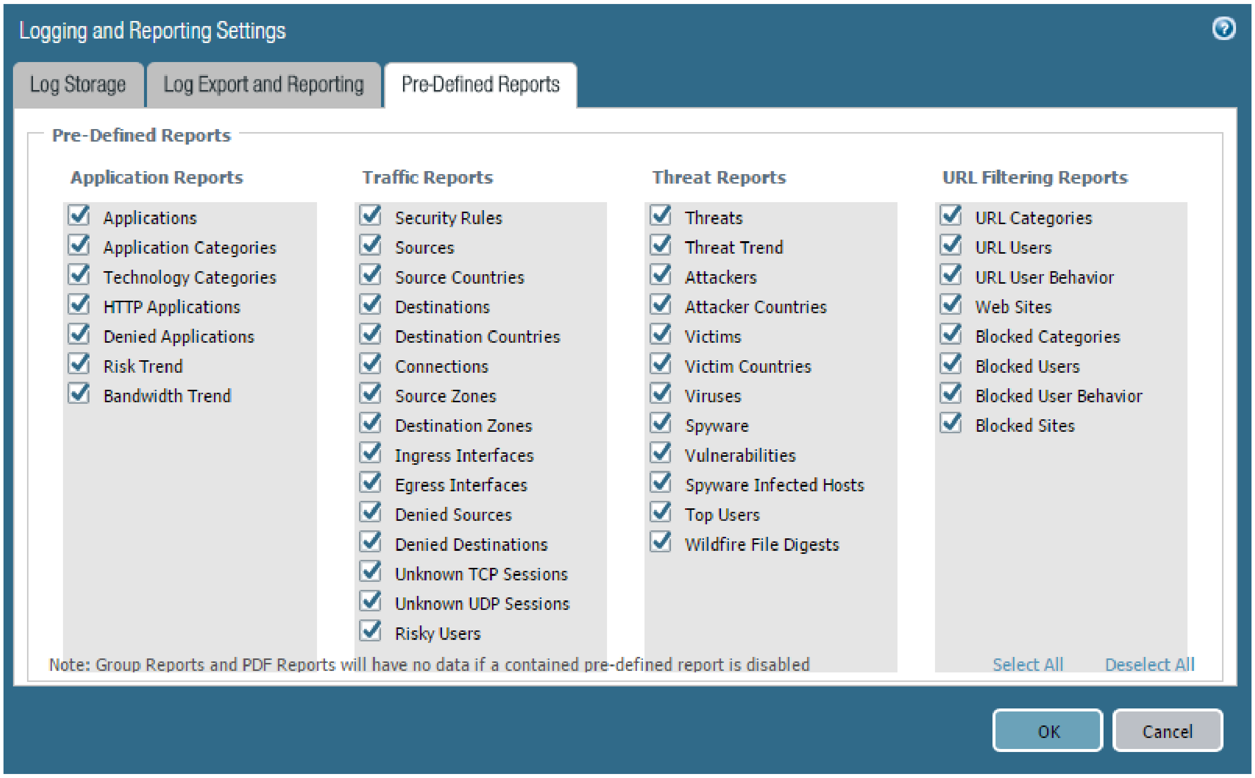
Filters can be built and even stored for future use. Specific data on this functionality is here:

https://www.paloaltonetworks.com/documentation/80/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 every 15 minutes 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.

© 2018 Palo Alto Networks, Inc.

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



Pre-Defined Reports

Application Reports

- ☑ Applications
- ☑ Application Categories
- ☑ Technology Categories
- ☑ HTTP Applications
- ☑ Denied Applications
- ☑ Risk Trend
- ☑ Bandwidth Trend

Traffic Reports

- ☑ Security Rules
- ☑ Sources
- ☑ Source Countries
- ☑ Destinations
- ☑ Destination Countries
- ☑ Connections
- ☑ Source Zones
- ☑ Destination Zones
- ☑ Ingress Interfaces
- ☑ Egress Interfaces
- ☑ Denied Sources
- ☑ Denied Destinations
- ☑ Unknown TCP Sessions
- ☑ Unknown UDP Sessions
- ☑ Risky Users

Threat Reports

- ☑ Threats
- ☑ Threat Trend
- ☑ Attackers
- ☑ Attacker Countries
- ☑ Victims
- ☑ Victim Countries
- ☑ Viruses
- ☑ Spyware
- ☑ Vulnerabilities
- ☑ Spyware Infected Hosts
- ☑ Top Users
- ☑ Wildfire File Digests

URL Filtering Reports

- ☑ URL Categories
- ☑ URL Users
- ☑ URL User Behavior
- ☑ Web Sites
- ☑ Blocked Categories
- ☑ Blocked Users
- ☑ Blocked User Behavior
- ☑ Blocked Sites

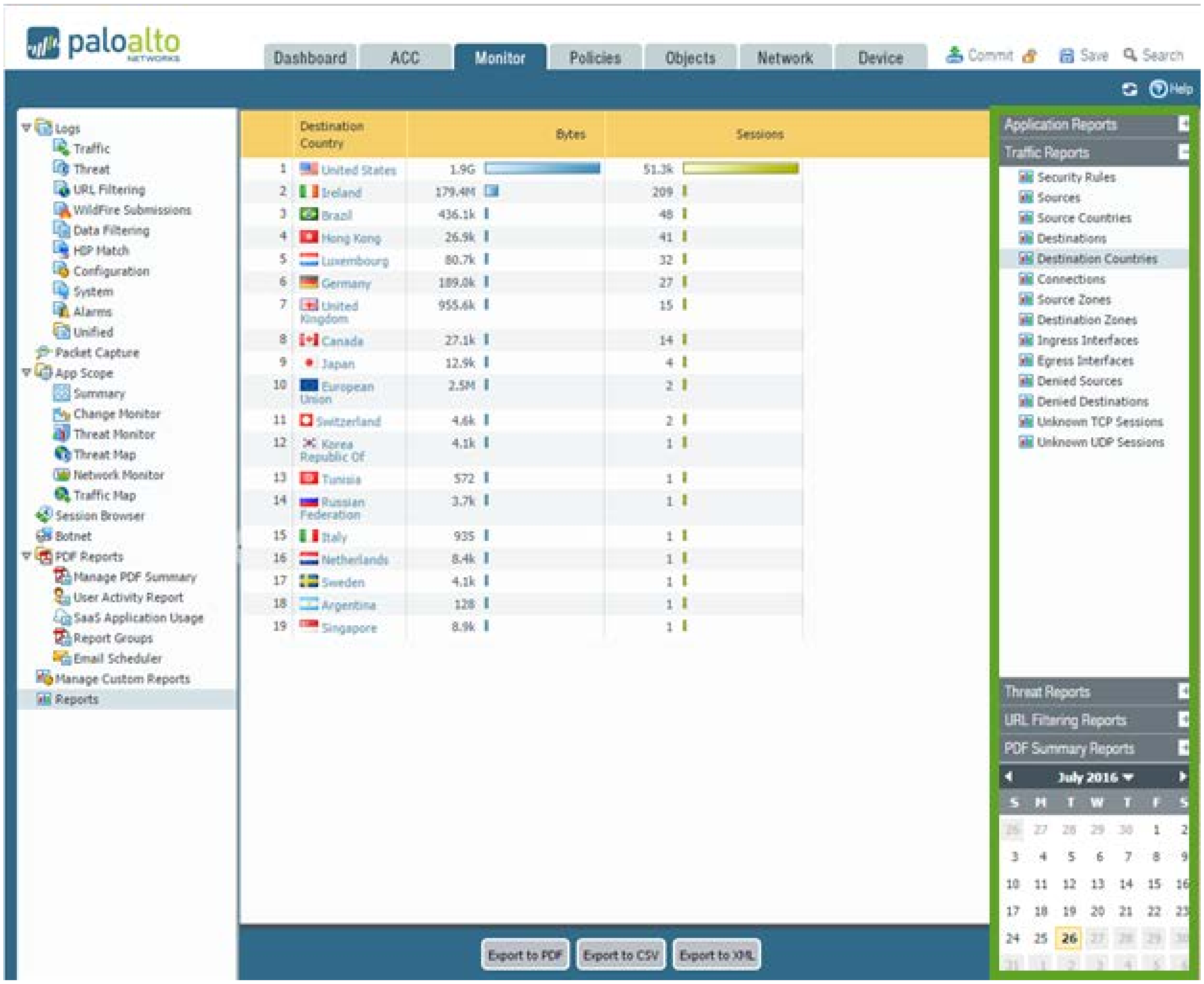
Note: Group Reports and PDF Reports will have no data if a contained pre-defined report is disabled

Settings for the repeating report database summarization process

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 via 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:



	Destination Country	Bytes	Sessions
1	United States	1.9G	51.3k
2	Ireland	179.4M	209
3	Brazil	436.1k	48
4	Hong Kong	26.9k	41
5	Luxembourg	80.7k	32
6	Germany	189.0k	27
7	United Kingdom	955.6k	15
8	Canada	27.1k	14
9	Japan	12.9k	4
10	European Union	2.5M	2
11	Switzerland	4.6k	2
12	Korea Republic Of	4.1k	1
13	Tunisia	572	1
14	Russian Federation	3.7k	1
15	Italy	935	1
16	Netherlands	8.4k	1
17	Sweden	4.1k	1
18	Argentina	128	1
19	Singapore	8.9k	1

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/80/pan-os/pan-os/monitoring/generate-custom-reports#35712

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/80/pan-os/pan-os/monitoring/generate-user-group-activity-reports#91388

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:

© 2018 Palo Alto Networks, Inc.

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/manage-pdf-summary-reports#24063

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/80/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/80/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/80/pan-os/pan-os/monitoring/use-the-automated-correlation-engine#38973

Sample questions

1. 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)

2. 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

Answers under the heading Answers to Interpret log files, reports, and graphs to determine traffic and threat trends. on p. 119.

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/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applications
- Create a Custom Application
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/create-a-custom-application#_33572

Sample questions

1. 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 cofigure 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.
2. 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

Answers under the heading Answers to Identify scenarios in which there is a benefit from using custom signatures. on p. 119.

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.

A discussion of this process is here:

https://www.paloaltonetworks.com/documentation/80/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/80/pan-os/newfeaturesguide/upgrade-to-pan-os-8-0/upgrade-the-firewall-to-pan-os-8-0#_17982

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® updates if required. Details are here:

https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-8-0/downgrade-from-pan-os-8-0#_97027

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/80/pan-os/newfeaturesguide/upgrade-to-pan-os-8-0/upgrade-an-ha-firewall-pair-to-pan-os-8-0#_60928

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/80/panorama/panorama_adminguide/manage-licenses-and-updates

Upgrading of Panorama-managed firewalls to PAN-OS® 8.0 is discussed here:

https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-8-0/upgrade-firewalls-using-panorama#_58633

HA Cluster Firewall Updates Managed by Panorama

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

Sample question

1. 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.

Answer under the heading Answer to Given a scenario, identify the process to update a Palo Alto Networks system to the latest version of the software. on p. 119.

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/80/pan-os/pan-os/firewall-administration/manage-configuration-backups#68133

Guidelines for configuration management are here:

https://live.paloaltonetworks.com/t5/Configuration-Articles/Configuration-Management-Guidelines/ta-p/65781

Sample question

1. What is the action that specifies that Security Profiles are relevant in a policy rule?
    A. Deny
    B. Reject
    C. Drop
    D. Accept

Answer under the heading Answer to Identify how configuration management operations are used to ensure desired operational state of stability and continuity. on p. 119.

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/80/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/80/pan-os/pan-os/high-availability/ha-links-and-backup-links
- Set Up Active/Passive HA
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/set-up-active-passive-ha
- Set Up Active/Active HA
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/set-up-active-active-ha

Sample question

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

Answer under the heading Answer to 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). on p. 119.

Identify the sources of information pertaining to HA functionality.

Network monitoring applications use SNMP to query network components, such as the NGFW. Version 8.0 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. To see SNMP statistics for dedicated HA2 interfaces, use the IF-MIB and interfaces MIB.

References

- SNMP Support
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/snmp-support
- Monitor Statistics Using SNMP
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/monitor-statistics-using-snmp
- Supported MIBs
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/supported-mibs

© 2018 Palo Alto Networks, Inc.

- Extended SNMP Supporthttps://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/management-features/extended-snmp-support#_37052

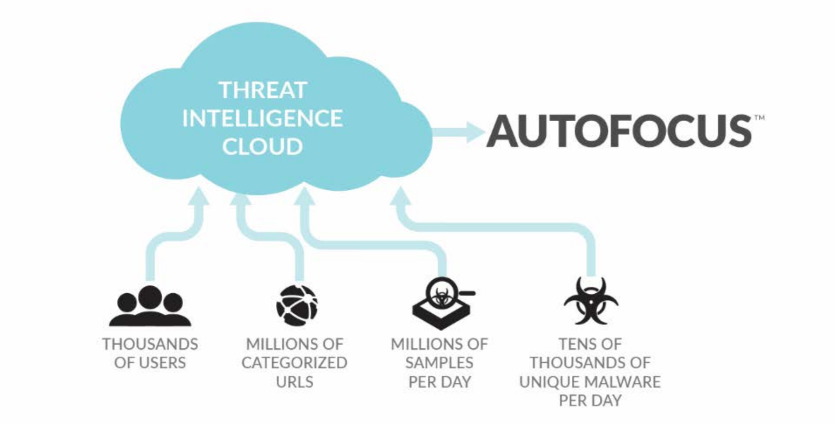
Sample question

1. 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

Answer under the heading Answer to Identify the sources of information pertaining to HA functionality. on p. 119.

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

AutoFocus, a Palo Alto Networks threat intelligence service, accelerates analysis and response efforts for the most damaging, unique, and targeted attacks. The hosted security service is natively integrated with the Palo Alto Networks Next-Generation Security Platform, thus extending your threat analysis and hunting capabilities without additional IT security resources. AutoFocus provides the visibility and threat context required to respond more quickly to critical attacks.


THREAT INTELLIGENCE CLOUD
AUTOFOCUS™
THOUSANDS OF USERS
MILLIONS OF CATEGORIZED URLS
MILLIONS OF SAMPLES PER DAY
TENS OF THOUSANDS OF UNIQUE MALWARE PER DAY

References

- At a Glance: AutoFocus
  https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/autofocus-at-a-glance

© 2018 Palo Alto Networks, Inc.

- AutoFocus Administrator's Guide, especially p. 17-20, 55-57 https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/autofocus/autofocus_admin_guide.pdf

Sample question

1. 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

Answer under the heading Answer to Identify how to configure the firewall to integrate with AutoFocus and verify its functionality. on p. 120.

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/80/pan-os/web-interface-help/device/device-dynamic-updates
- Install Content and Software Updates https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/install-content-and-software-updates
- Manage New App-IDs Introduced in Content Releases https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-new-app-ids-introduced-in-content-releases#_29763
- Review New App-IDs https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/review-new-app-ids#_53319

Sample question

1. 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

Answer under the heading Answer to Identify the impact of deploying dynamic updates. on p. 120.

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.

References

- Deploy Updates to Firewalls, Log Collectors and WildFire Appliances Using Panorama
  https://www.paloaltonetworks.com/documentation/80/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/80/panorama/panorama_adminguide/manage-licenses-and-updates/supported-updates#_97041

Sample questions

1. Which two types of device can receive the Antivirus content update? (Choose two)
    A. Log Collector
    B. Firewall
    C. WildFire
2. Within the 8.0 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.

Answers under the heading Answers to Identify the relationship between Panorama and devices as it pertains to dynamic updates versions and policy implementation and/or HA peers. on p. 120.

Exam Domain 4 – Configuration Troubleshooting

Identify system and traffic issues using WebUI and CLI tools.

There is no simple reference list to include in this section because being able to troubleshoot the firewall requires a thorough understanding of how it works. The references are for the main troubleshooting tools.

References

- Log Types and Severity Levels
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/log-types-and-severity-levels#_51096
- Monitor > Logs
  https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/monitor/monitor-logs#_58165
- CLI Cheat Sheet: Device Management
  https://www.paloaltonetworks.com/documentation/80/pan-os/cli-gsg/cli-cheat-sheets/cli-cheat-sheet-device-management#_44428
- CLI Cheat Sheet: Networking
  https://www.paloaltonetworks.com/documentation/80/pan-os/cli-gsg/cli-cheat-sheets/cli-cheat-sheet-networking#_10944
- Interpret VPN Error Messages
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/interpret-vpn-error-messages

Sample questions

1. 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)
2. You can’t get to the web interface. How do you check from the command line if it is running? (D)

```
A. ps -aux | grep appweb
B. ps -aux | match appweb
C. show system software status | grep appweb
D. show system software status | match appweb
```

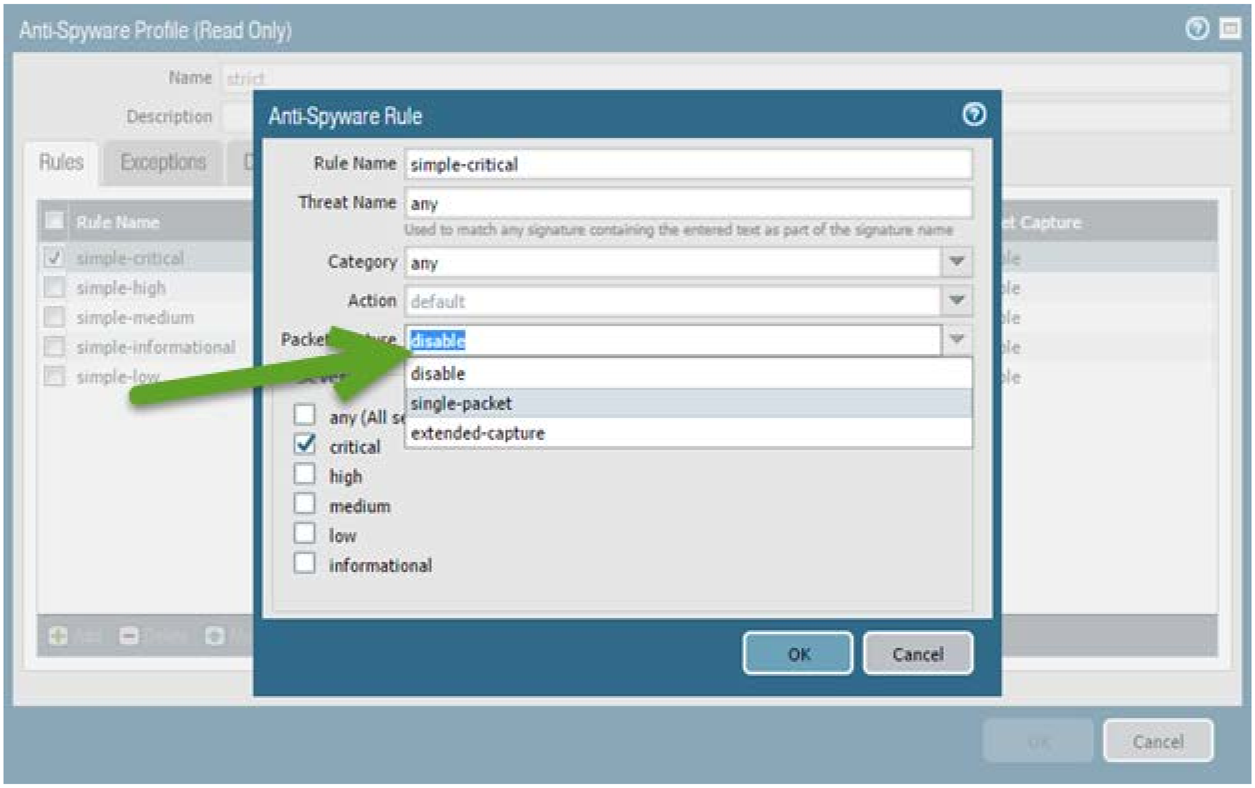
Answers under the heading Answers to Identify system and traffic issues using WebUI and CLI tools. on p. 120.

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:



Anti-Spyware Profile (Read Only)

Name: strict

Description:

Rule Name
- simple-critical
- simple-high
- simple-medium
- simple-informational
- simple-low

Anti-Spyware Rule

Rule Name: simple-critical

Threat Name: any

Used to match any signature containing the entered text as part of the signature name

Category: any

Action: default

Packet Capture: disable

Severity
- ☐ any (All se
- ☑ critical
- ☐ high
- ☐ medium
- ☐ low
- ☐ informational

Configuring a packet capture response to the detection of spyware

Information about configuring threat detection captures and accessing the captured data is here:

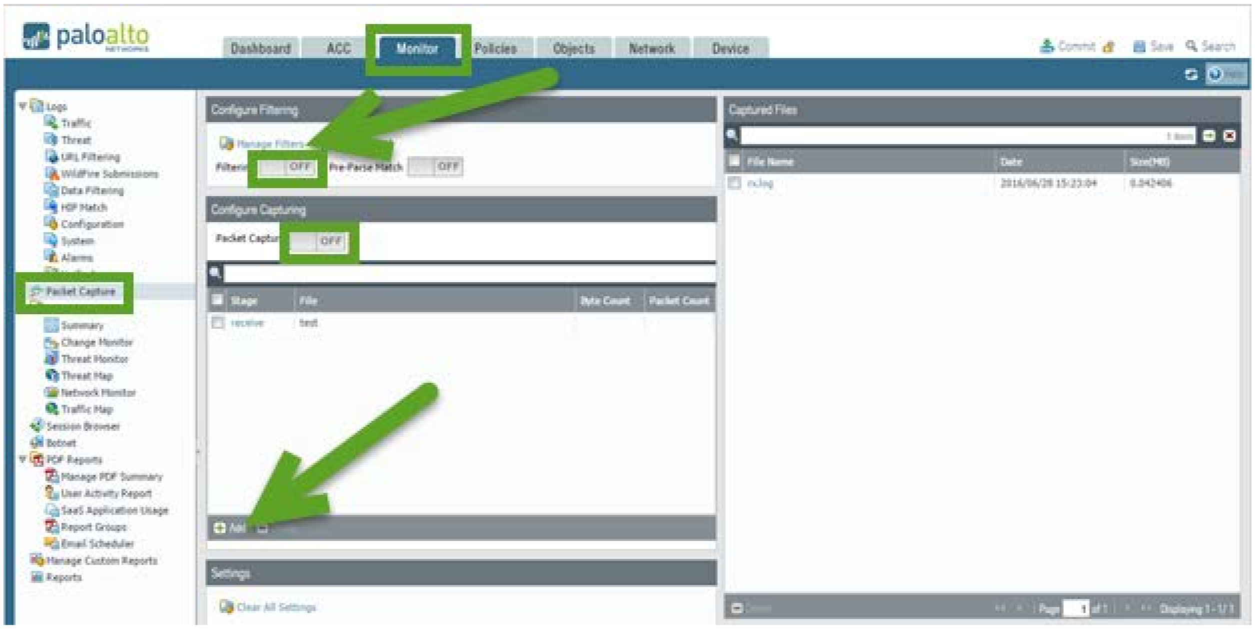
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-a-threat-packet-capture

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. 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:



Filtering OFF Pre-Parse Match OFF

Packet Capture OFF

Stage	File	Byte Count	Packet Count
receive	test		

File Name	Date	Size(MB)
rx.log	2016/06/28 15:23:04	0.042406

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/80/pan-os/pan-os/monitoring/take-a-custom-packet-capture#17879

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. All PA-2000 Series, PA-3050, PA-3060, PA-4000 Series, PA-5000 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/80/pan-os/pan-os/monitoring/disable-hardware-offload#85899

Note: WebUI packet captures cannot be used for traffic crossing the management interface.

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.

© 2018 Palo Alto Networks, Inc.

Sample question

1. Which Security Profiles do *not* have a packet capture option? (D)
    A. Antivirus
    B. Anti-spyware
    C. Vulnerability Protection
    D. URL Filtering

Answer under the heading Answers to Given a session output, identify the configuration requirements used to perform a packet capture. on p. 120.

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.

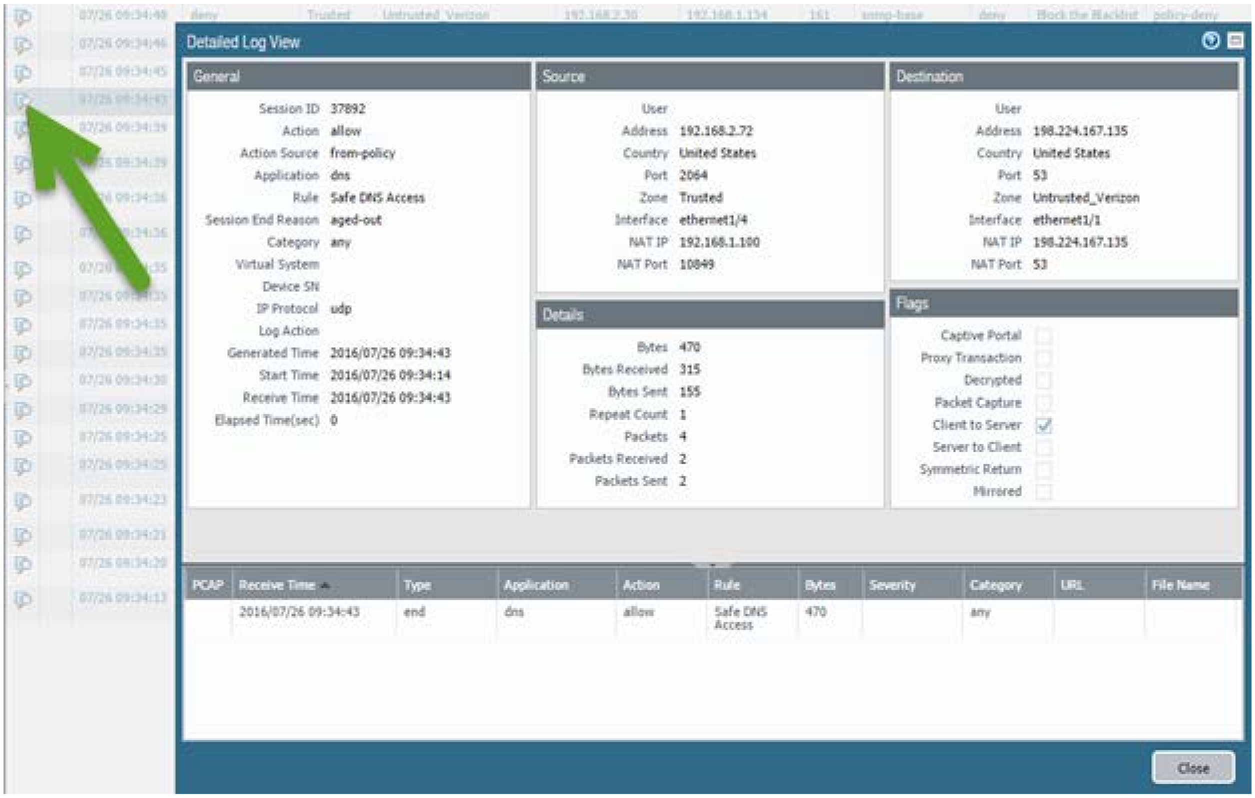
This management traffic can be routed through alternate ports. A discussion is here:

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:



Detailed Log View

General

Session ID 37892
Action allow
Action Source from-policy
Application dns
Rule Safe DNS Access
Session End Reason aged-out
Category any
Virtual System
Device SN
IP Protocol udp
Log Action
Generated Time 2016/07/26 09:34:43
Start Time 2016/07/26 09:34:14
Receive Time 2016/07/26 09:34:43
Elapsed Time(sec) 0

Source

User
Address 192.168.2.72
Country United States
Port 2064
Zone Trusted
Interface ethernet1/4
NAT IP 192.168.1.100
NAT Port 10849

Details

Bytes 470
Bytes Received 315
Bytes Sent 155
Repeat Count 1
Packets 4
Packets Received 2
Packets Sent 2

Destination

User
Address 198.224.167.135
Country United States
Port 53
Zone Untrusted_Verizon
Interface ethernet1/1
NAT IP 198.224.167.135
NAT Port 53

Flags

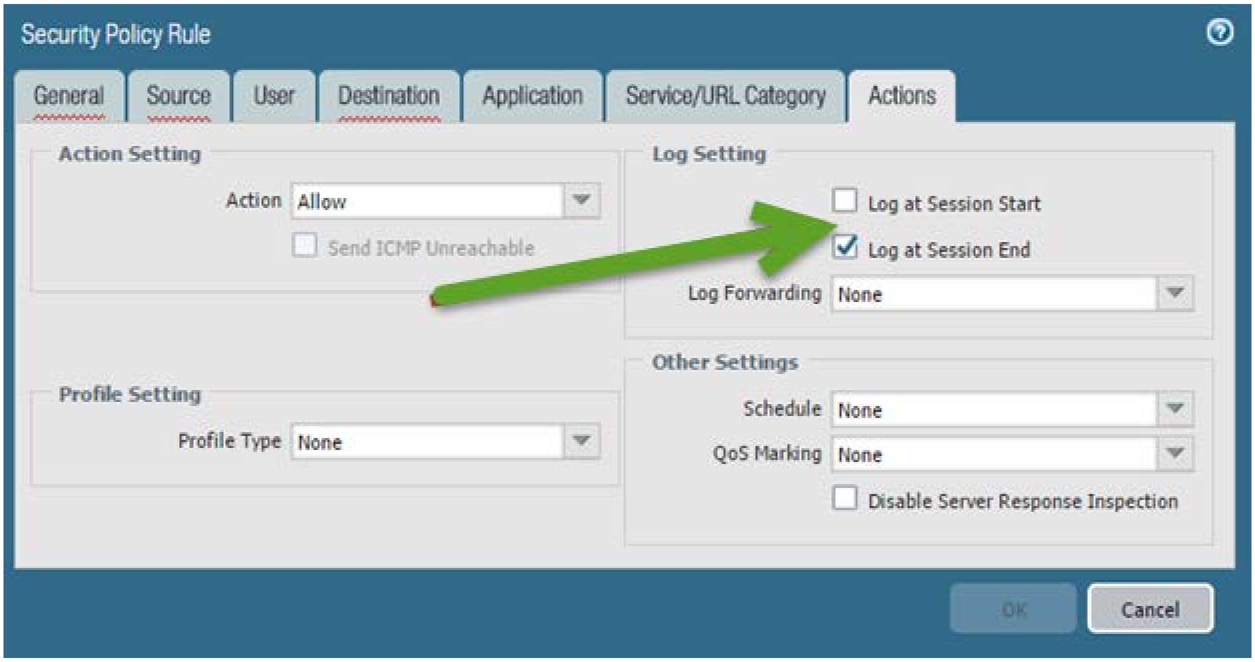
Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server ☑
Server to Client □
Symmetric Return □
Mirrored □

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	URL	File Name
	2016/07/26 09:34:43	end	dns	allow	Safe DNS Access	470		any		

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:



Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

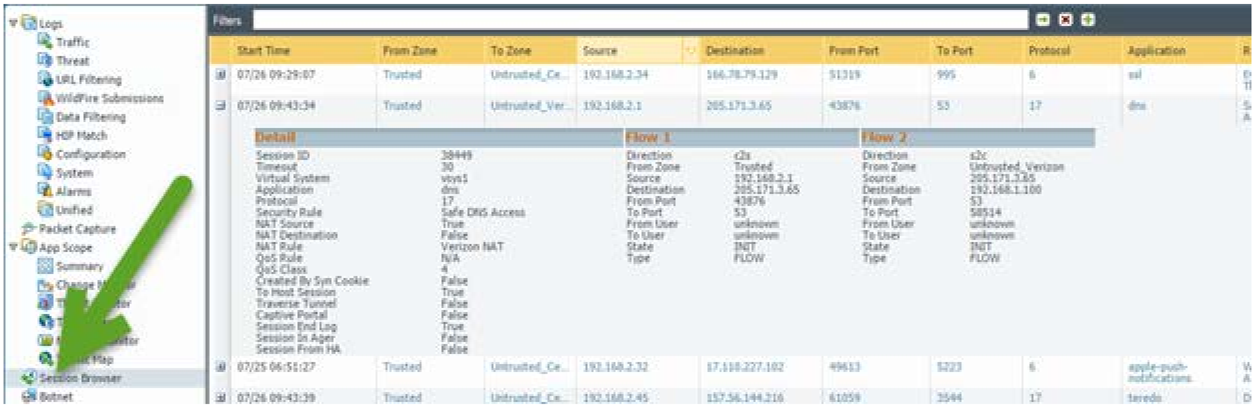
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

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

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



Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application
07/26 09:29:07	Trusted	Untrusted_Ce...	192.168.2.34	166.78.79.129	51319	995	6	ssl
07/26 09:43:34	Trusted	Untrusted_Ver...	192.168.2.1	205.171.3.65	43876	53	17	dns
07/25 06:51:27	Trusted	Untrusted_Ce...	192.168.2.32	17.110.227.102	49613	5223	6	apple-push-notifications
07/26 09:43:39	Trusted	Untrusted_Ce...	192.168.2.45	157.56.144.216	61059	3544	17	teredo

```
Detail                                          Flow 1                        Flow 2
Session ID               38449                  Direction     c2s             Direction     s2c
Timeout                  30                     From Zone     Trusted         From Zone     Untrusted_Verizon
Virtual System           vsys1                  Source        192.168.2.1     Source        205.171.3.65
Application              dns                    Destination   205.171.3.65    Destination   192.168.1.100
Protocol                 17                     From Port     43876           From Port     53
Security Rule            Safe DNS Access        To Port       53              To Port       58514
NAT Source               True                   From User     unknown         From User     unknown
NAT Destination          False                  To User       unknown         To User       unknown
NAT Rule                 Verizon NAT            State         INIT            State         INIT
QoS Rule                 N/A                    Type          FLOW            Type          FLOW
QoS Class                4
Created By Syn Cookie    False
To Host Session          True
Traverse Tunnel          False
Captive Portal           False
Session End Log          True
Session In Ager          False
Session From HA          False
```

View open sessions within the session browser

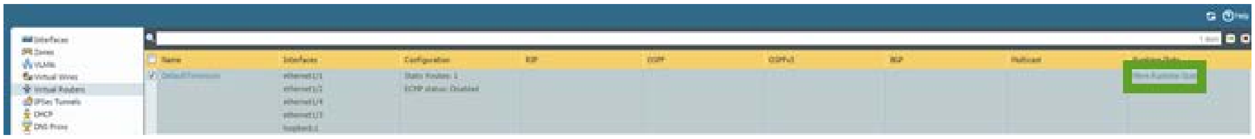
The Clear check box at the end of a session summary line can be used to end the session immediately, often generating the desired log entry.

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:

© 2018 Palo Alto Networks, Inc.

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures#62168

Connectivity issues often arise from unexpected traffic forwarding decisions. Find the simplest view into forwarding decisions by displaying the Layer 3 routing and forwarding tables in the WebUI:



Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runtime Stats
default	ethernet1/1 ethernet1/2 ethernet1/4 ethernet1/3 loopback.1	Static Routes: 1 ECMP status: Disabled						More Runtime Stats

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

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

1. 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. Th session browser node in the Monitor tab

Answer under the heading Answer to Given a scenario, identify how to troubleshoot and configure interface components. on p. 120.

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/80/pan-os/pan-os/decryption/decryption-overview
- How to Implement and Test SSL Decryptionhttps://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719

© 2018 Palo Alto Networks, Inc.

Sample question

1. 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.

Answer under the heading Answer to Identify how to troubleshoot SSL decryption failures. on p. 120.

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/80/pan-os/pan-os/decryption/keys-and-certificates-for-decryption-policies#_40372
- Certificate Management
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management#_19363

- 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 question

1. 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.

Answer under the heading Answers to Identify certificate chain of trust issues. on p. 121.

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 confoigure 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/80/pan-os/pan-os/networking/virtual-routers
- Site-to-Site VPN with Static and Dynamic Routing
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/site-to-site-vpn-with-static-and-dynamic-routing
- Static Routes
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/static-routes#_99987
- RIP
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/rip#_61661
- OSPF
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/ospf#_29900
- BGP
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/bgp

Sample question

1. 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**

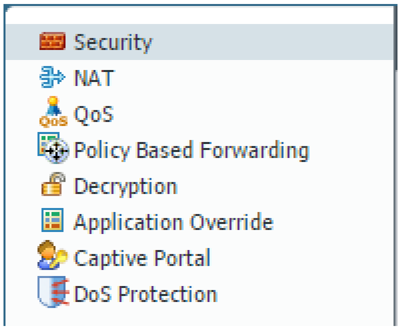
Answer under the heading Answer to Given a scenario, identify how to troubleshoot traffic routing issues. on p. 121.

Exam Domain 5 – Core Concepts

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

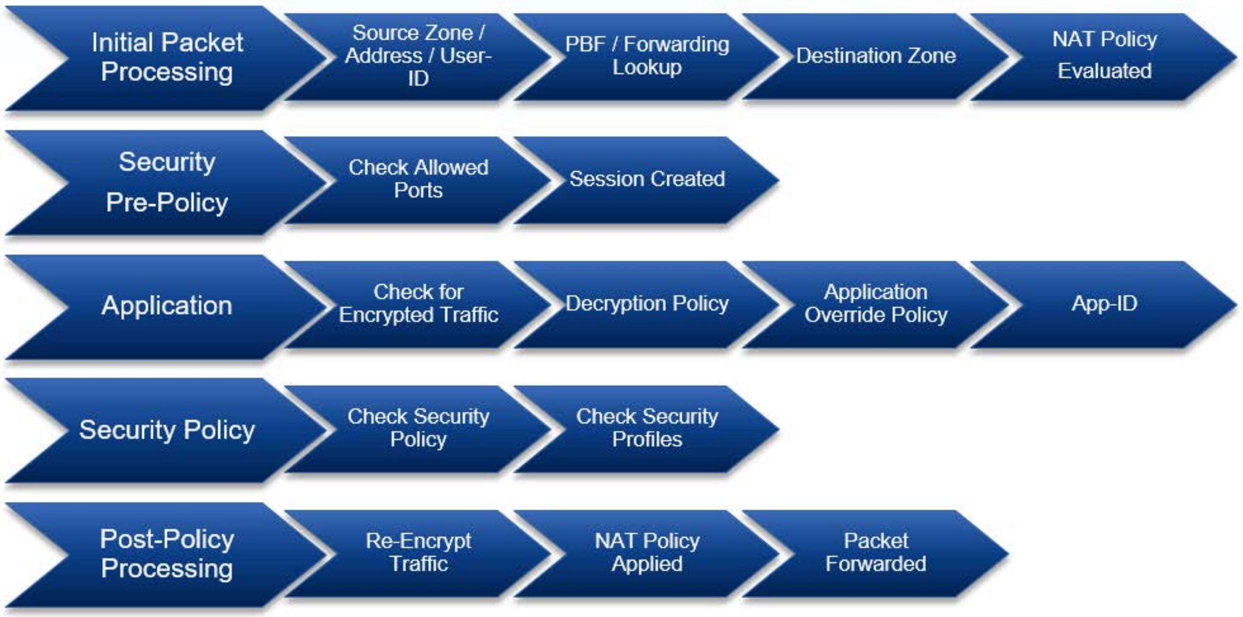
Policies

Palo Alto Networks firewalls implement several types of policies:



Types of policies in a Palo Alto Networks firewall

Each type of policy is implemented as a list in which match processing against traffic is performed from the top of the list down. The first policy matching the traffic in question is executed, with no other policy processing of that type performed. Each type of policy is reviewed in the order indicated in the following process flow:



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/70/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

1. 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
2. Which two statements are correct regarding policy evaluation? (Choose two.)
   A. All rules are searched and the most specific rule 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.

Answers under the heading Answers to Identify the correct order of the policy evaluation based on the packet flow architecture. on p. 121.

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/80/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/80/pan-os/pan-os/policy/best-practice-internet-gateway-security-policy#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/80/pan-os/pan-os/policy/create-best-practice-security-profiles#48239

Sample Question

1. A URL Filtering Profile is part of which type of identification?
   A. App-ID
   B. Content-ID
   C. User-ID

Answer under the heading Answer to Given an attack scenario, identify the Palo Alto Networks appropriate threat prevention component to prevent/mitigate the attack. on p. 121.

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.

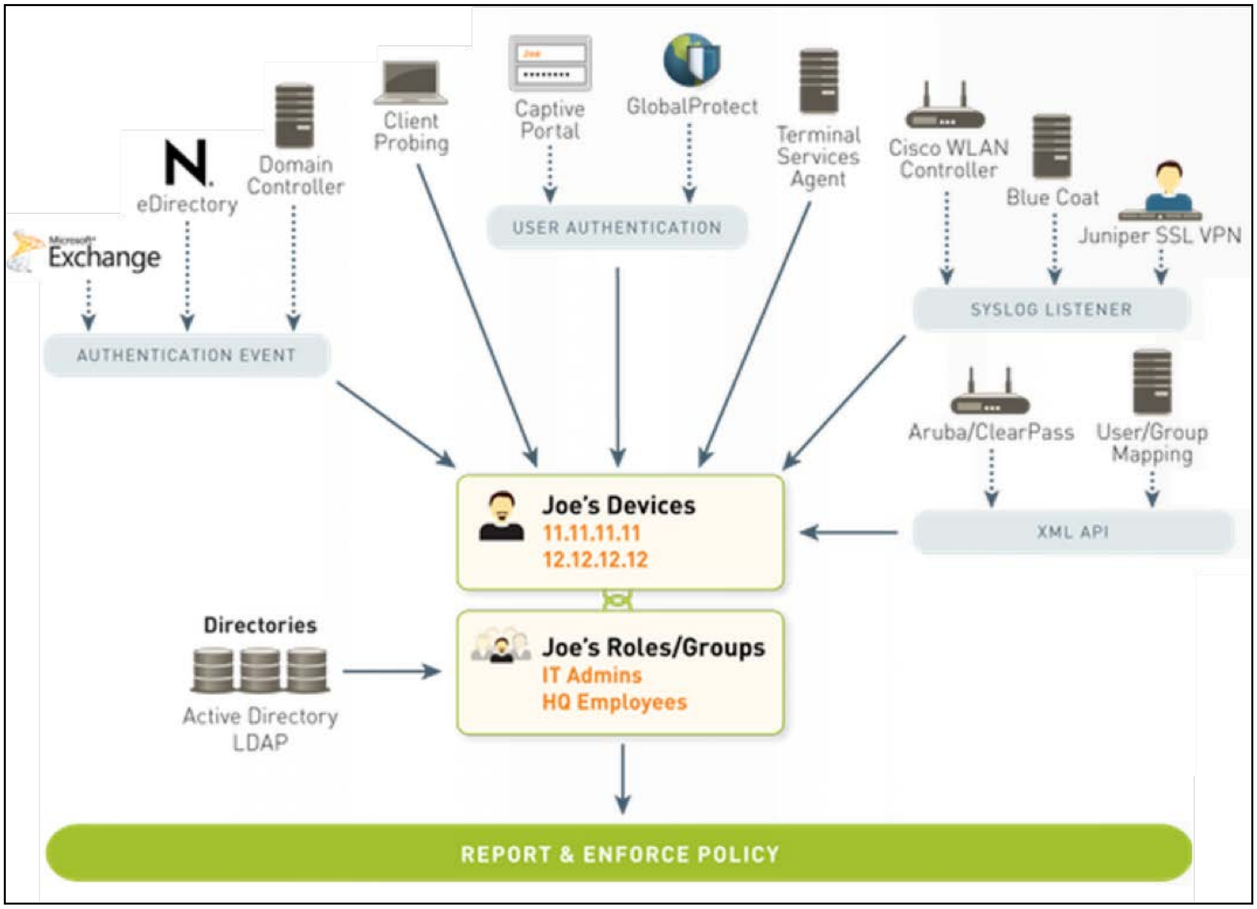
User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, enabling you to associate application activity and policy rules to users and groups—not just IP addresses. Furthermore, with User-ID enabled, the Application Command Center (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/70/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:

https://live.paloaltonetworks.com/t5/Learning-Articles/Best-practices-for-securing-User-ID-deployments/ta-p/61606

Sample Question

1. User-ID maps users to what type of information? (Choose the most accurate answer.) (B)
   - 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 multi-user devices (such as servers)

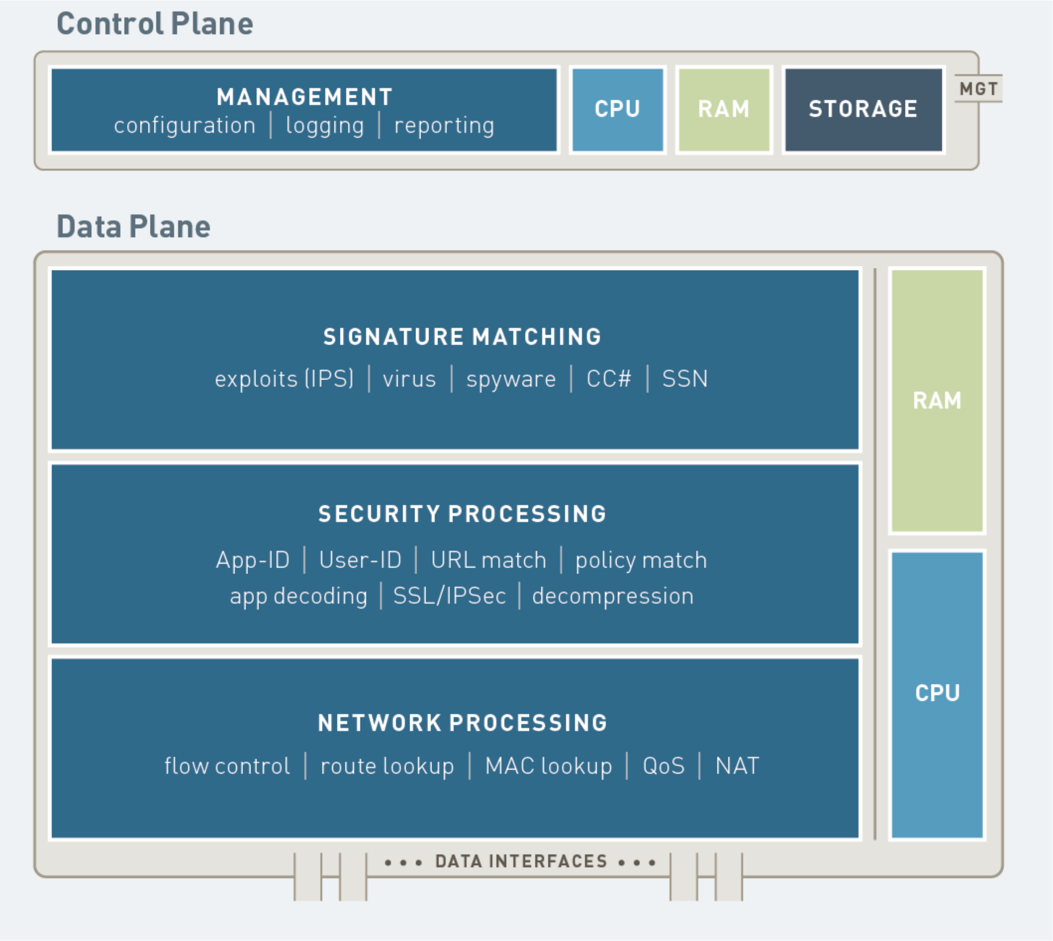
Answer under the heading Answer to Identify methods for identifying users. on p. 121.

Identify the fundamental functions residing on the management and dataplanes of a Palo Alto Networks firewall.

Management and Dataplanes

Whether physical or virtual, the management plane and dataplane 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:

© 2018 Palo Alto Networks, Inc.


Control Plane
MANAGEMENT
configuration | logging | reporting
CPU
RAM
STORAGE
MGT
Data Plane
SIGNATURE MATCHING
exploits (IPS) | virus | spyware | CC# | SSN
SECURITY PROCESSING
App-ID | User-ID | URL match | policy match
app decoding | SSL/IPSec | decompression
NETWORK PROCESSING
flow control | route lookup | MAC lookup | QoS | NAT
RAM
CPU
• • • DATA INTERFACES • • •

Palo Alto Networks maintains the management plane and dataplane 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 dataplane:

- 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

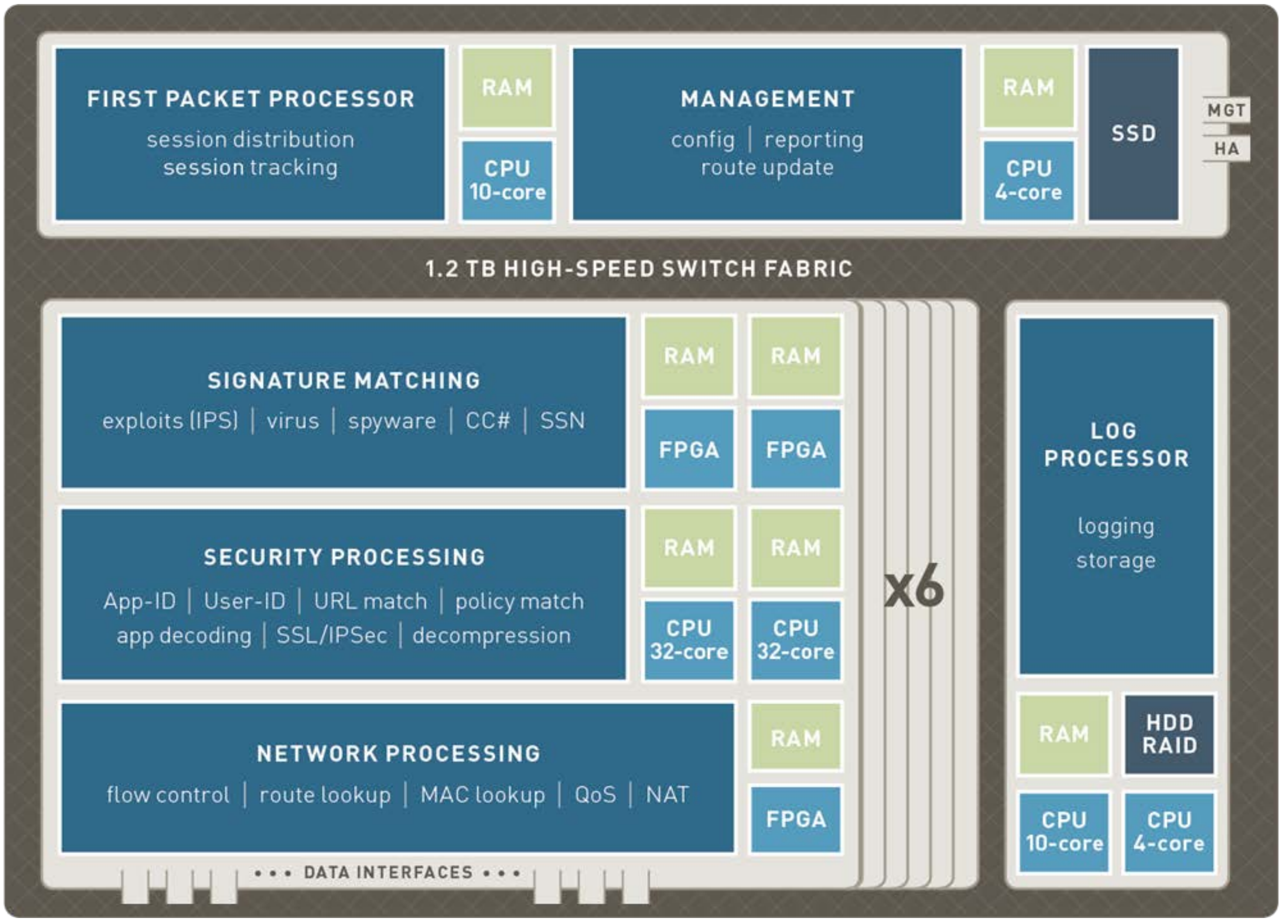
The dataplane connects directly to the traffic interfaces.

As more computing capability is added to more powerful firewall models, the management and dataplanes 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 Question

1. On a PA-7000, which management function runs on a separate card?
   A. configuration management
   B. logging
   C. reporting
   D. The web user interface

Answer under the heading Answer to Identify methods for identifying users. on p. 121.

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

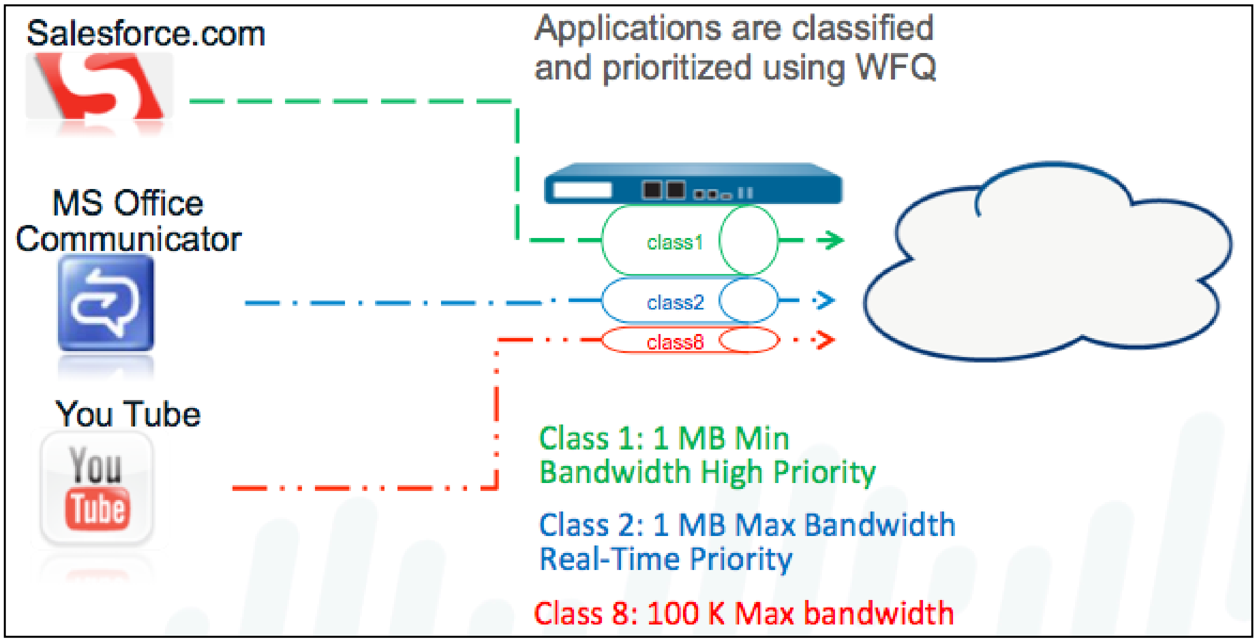
Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish these tasks by providing differentiated handling and capacity allocation to specific flows 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 basic QoS applied to networks and extends it to provide QoS to applications and users.

Palo Alto Networks QoS provides an “Application Aware” QoS service that can be driven by the traffic’s App-ID. Existing QoS packet markings can be used as input in QoS decisions. QoS markings can be written back to packets for consumption on other network nodes.

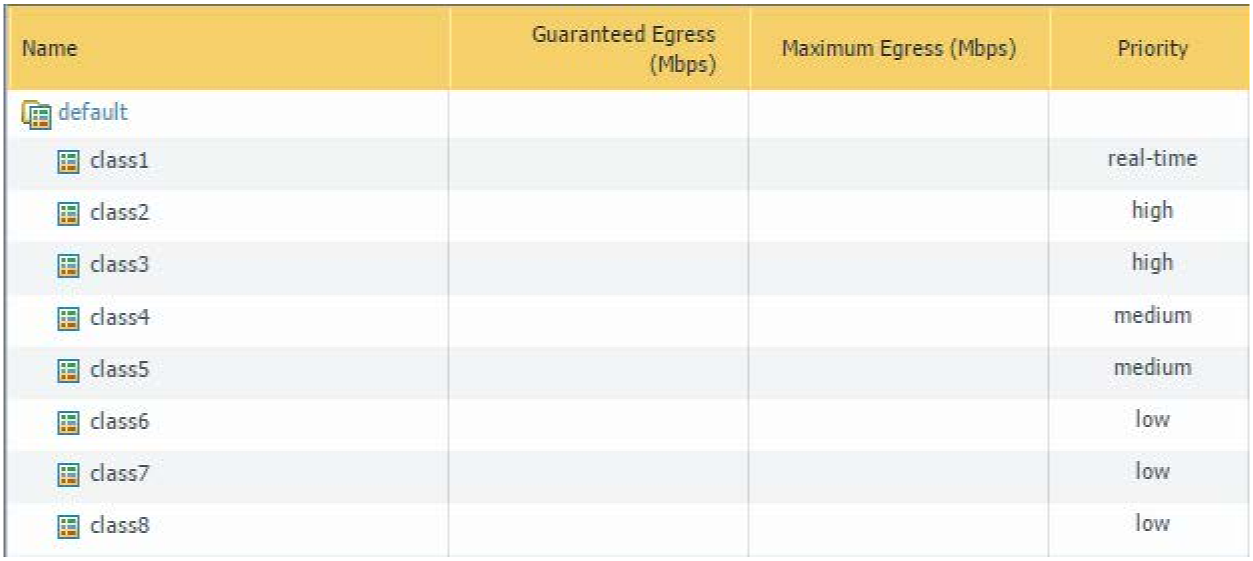
QoS implementation on a Palo Alto Networks firewall begins with three primary configuration components that support a full QoS solution: a QoS policy, a QoS Profile, and configuration of the QoS egress interface. Each option in the QoS configuration task facilitates a broader process that optimizes and prioritizes the traffic flow and allocates and ensures bandwidth according to configurable parameters.

QoS policies assign traffic classes (1-8) to the described traffic.


Salesforce.com
Applications are classified and prioritized using WFQ
MS Office Communicator
You Tube
class1
class2
class8
Class 1: 1 MB Min Bandwidth High Priority
Class 2: 1 MB Max Bandwidth Real-Time Priority
Class 8: 100 K Max bandwidth

PAN-OS® QoS functionality can use App-ID for specific bandwidth reservation.

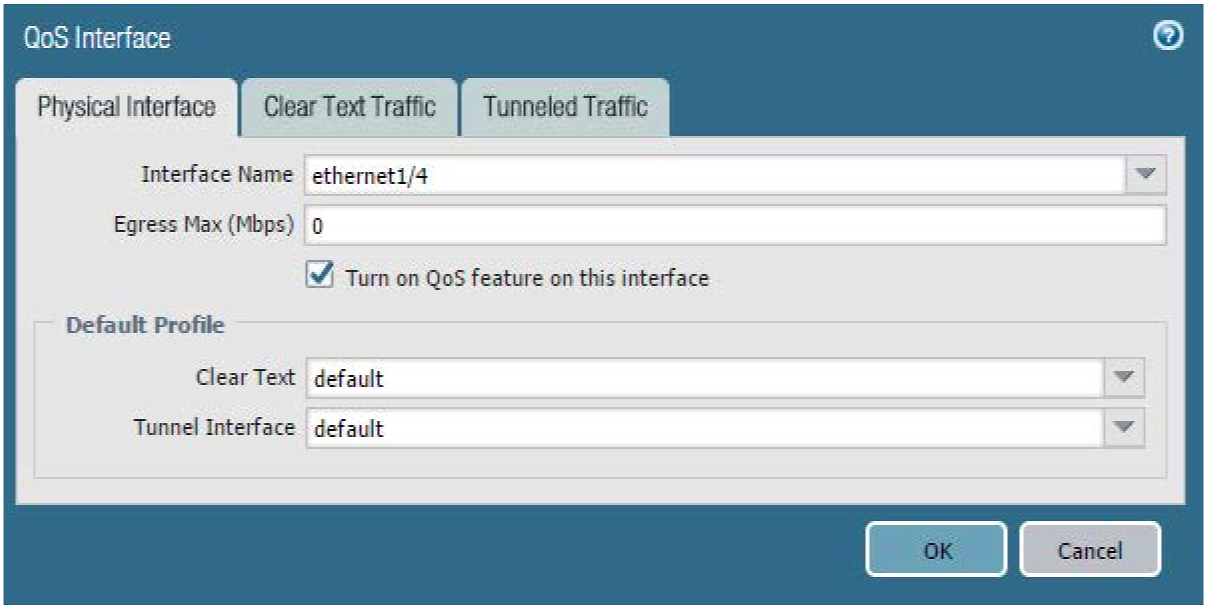
QoS Profiles describe the priority to be given to the specified traffic when the interface becomes constrained. As priority decreases, more packets are randomly dropped until the constraint is cleared. Profiles also specify bandwidth enforcement applied at all times.



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. Note that this assignment *shapes only egress traffic* on the interface.



Interface Name: ethernet1/4

Egress Max (Mbps): 0

☑ Turn on QoS feature on this interface

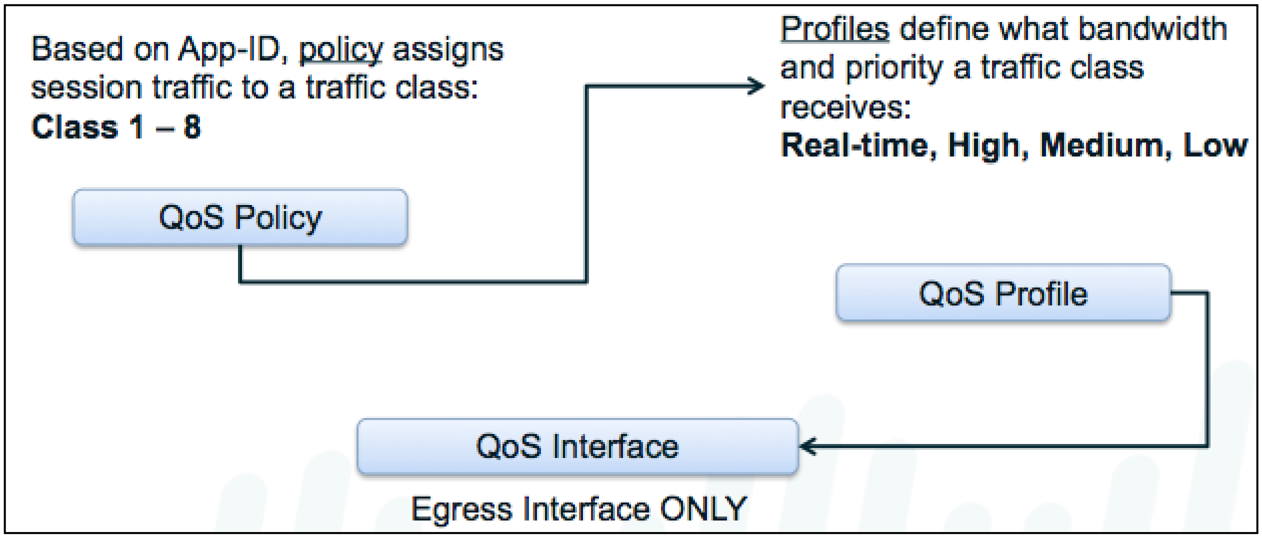
Default Profile

Clear Text: default

Tunnel Interface: default

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:



Based on App-ID, policy assigns session traffic to a traffic class: **Class 1 – 8**

Profiles define what bandwidth and priority a traffic class receives: **Real-time, High, Medium, Low**

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/70/pan-os/pan-os/quality-of-service

© 2018 Palo Alto Networks, Inc.

Sample Question

1. What parameter whose value is known to NGFW is important for QoS decisions?
    - A. App-ID
    - B. Content-ID
    - C. User-ID

Answer under the heading Answer to Given a scenario, determine how to control bandwidth use on a per-application basis. on p. 121.

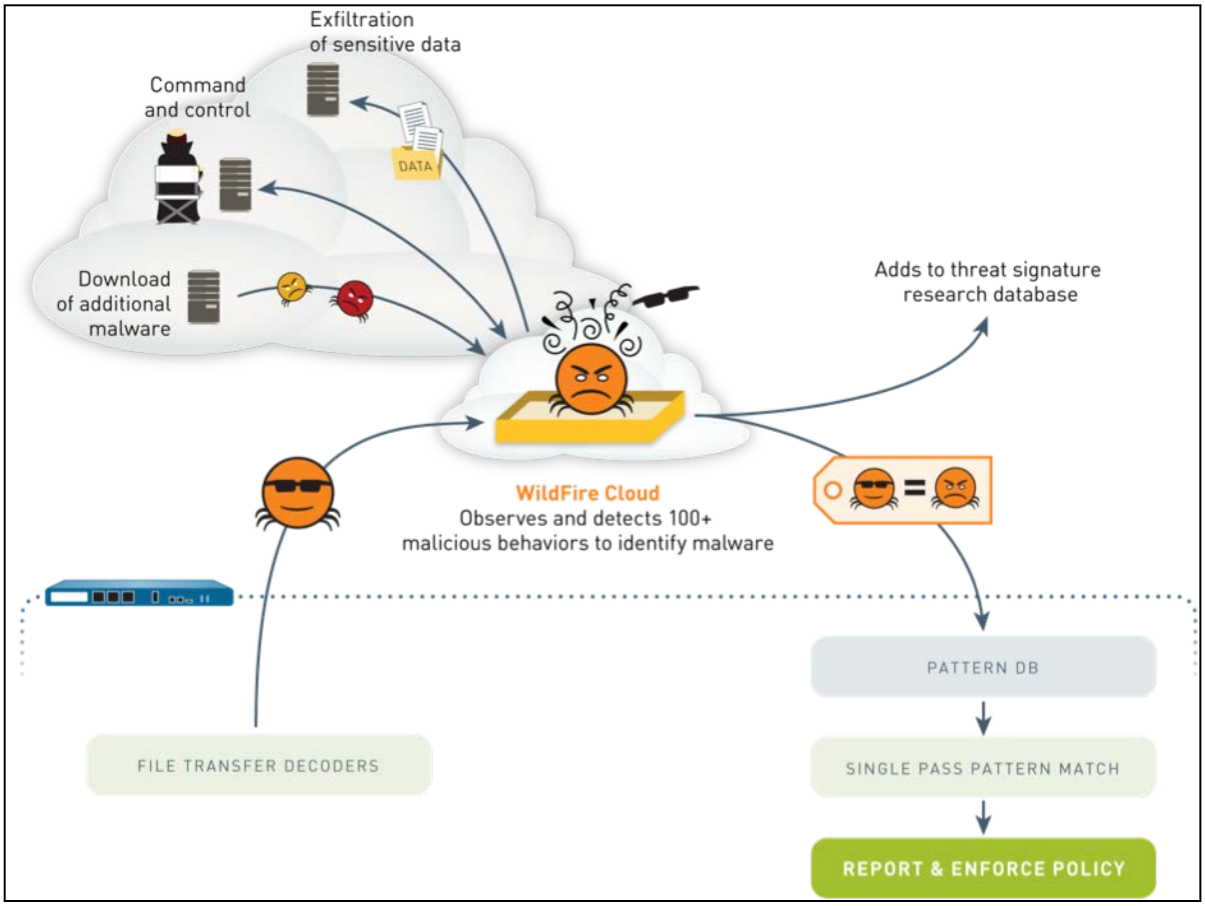
Identify the fundamental functions and concepts of WildFire

Wildfire Overview

WildFire is a sandbox analysis service that examines files for zero-day malware. A firewall administrator can submit copies of files transferred through the firewall to WildFire for analysis. Typically, within 5 minutes WildFire will process the file and provide a malware verdict plus a detailed analysis report. This service is available to all firewall owners for free with a license available for advanced features.

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 functions of WildFire:


Exfiltration of sensitive data
Command and control
DATA
Download of additional malware
Adds to threat signature research database
WildFire Cloud
Observes and detects 100+ malicious behaviors to identify malware
PATTERN DB
SINGLE PASS PATTERN MATCH
FILE TRANSFER DECODERS
REPORT & ENFORCE POLICY

WildFire looks within files for malicious activities and renders a verdict with an analysis report.

WildFire malware findings result in a new detection signature being created and added to the worldwide Antivirus update for all firewalls within 24 to 48 hours. WildFire license holders can receive these new signatures in as little as 5 minutes.

References

A detailed description of WildFire is here:

https://www.paloaltonetworks.com/documentation/80/wildfire/wf_adminThe use of WildFire in firewall profiles is outlined here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/wildfire-analysis-profiles

Sample questions

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

© 2018 Palo Alto Networks, Inc.

2. 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.

Answers under the heading Answers to Identify the fundamental functions and concepts of WildFire on p. 122.

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.

References

- Multi-Factor Authentication
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/multi-factor-authentication
- Authentication Policy
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/authentication-policy#_84422

Sample question

1. 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

Answer under the heading Answer to Identify the purpose of and use case for MFA and the Authentication policy. on p. 122.

Identify the dependencies for implementing MFA.

To use multi-factor authentication (MFA) for protecting sensitive services and applications, you must configure Captive Portal to display a web form for the first authentication factor and to record authentication timestamps. The firewall uses the timestamps to evaluate the timeouts for Authentication policy rules. To enable additional authentication factors, you can integrate the firewall with MFA vendors through RADIUS or vendor APIs. After evaluating the Authentication policy, the firewall evaluates the Security policy, so you must configure rules for both policy types.

References

- Configure Multi-Factor Authentication
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication#_79409
- Map IP Addresses to Usernames Using Captive Portal
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/map-ip-addresses-to-usernames-using-captive-portal#_65651

Sample question

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

Answer under the heading Answer to Identify the dependencies for implementing MFA. on p. 122.

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).

References

- Layer 2 Interfaces
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/layer-2-interfaces
- Virtual Routers
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/virtual-routers#_64633
- PBF (Policy-Based Forwarding)
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/pbf
- Use Case: PBF for Outbound Access with Dual ISPs
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/use-case-pbf-for-outbound-access-with-dual-isps

Sample question

1. An organization 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.

Answer to heading Answer to Given a scenario, identify how to forward traffic on p. 122.

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/80/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/80/pan-os/pan-os/policy/best-practice-internet-gateway-security-policy#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/80/pan-os/pan-os/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

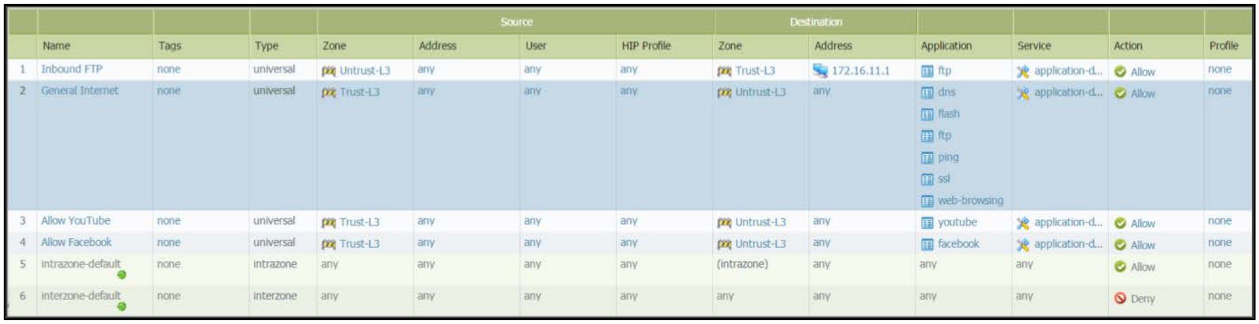
© 2018 Palo Alto Networks, Inc.

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.

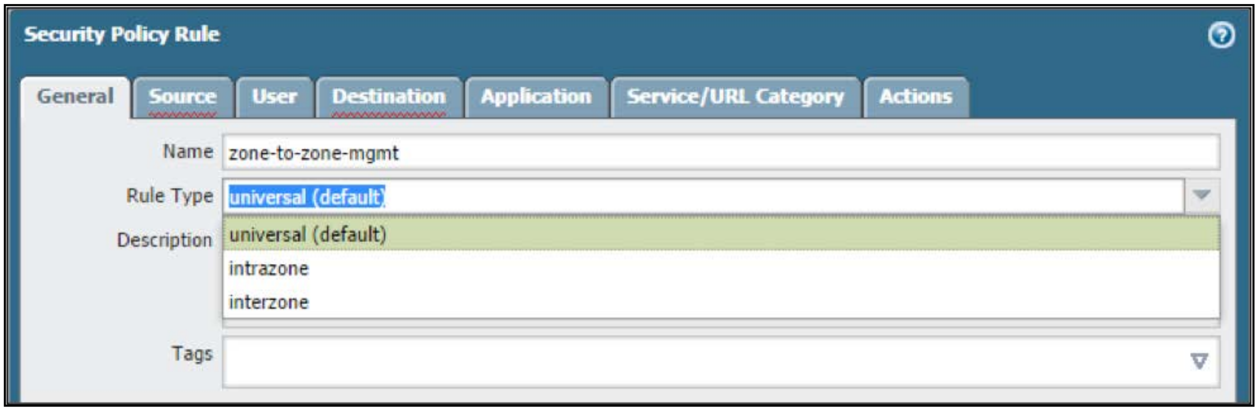


				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	Inbound FTP	none	universal	Untrust-L3	any	any	any	Trust-L3	172.16.11.1	ftp	application-d...	✓ Allow	none
2	General Internet	none	universal	Trust-L3	any	any	any	Untrust-L3	any	dns 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 policies: 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.



Name: zone-to-zone-mgmt

Rule Type: universal (default)

- universal (default)
- intrazone
- interzone

Description

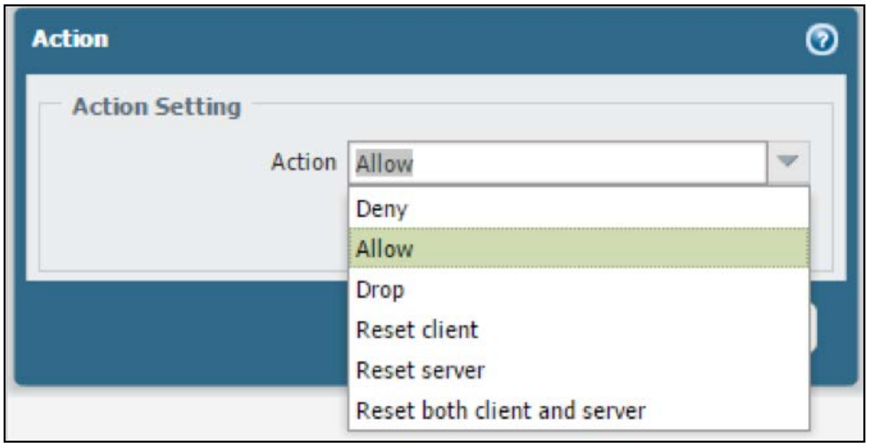
Tags

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."



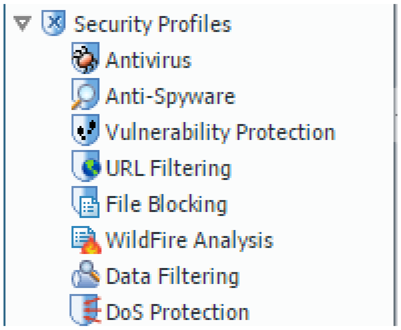
The actions available in security rules

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:

© 2018 Palo Alto Networks, Inc.

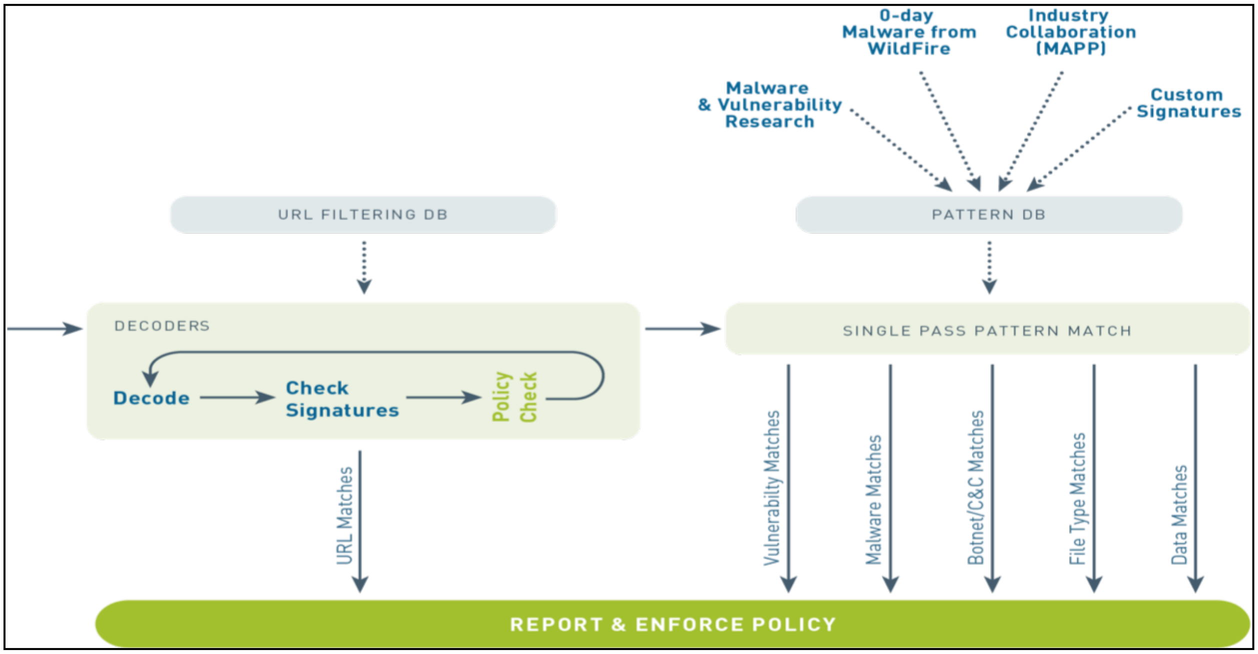


Configurable Security Profiles

An overview of each Security Profile is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles.html

The following diagram outlines the Content-ID engine that is responsible for Security Profile actions:



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 WildFie 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's 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/80/wildfire/wf_admin/monitor-wildfire-activity/wildfire-analysis-reports-close-up#90140

WildFire Profile setup details are here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/wildfire-analysis-profiles#75179

A complete review of WildFire implementation considerations is here:

https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin

An explanation of WildFire subscription benefits is here:

https://www.paloaltonetworks.com/documentation/80/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 FilteringProfiles 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. Thissubscription 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/80/pan-os/pan-os/url-filtering/url-filtering-response-pages

An overview of URL filtering is provided here:

https://www.paloaltonetworks.com/documentation/80/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/80/pan-os/pan-os/url-filtering/url-filtering-vendors

Specific information about implementing URL Filtering profiles and their allowed actions is here:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/url-filtering/configure-url-filtering#74872

Sample Questions

1. Which action specifies that Security Profiles are relevant in a policy rule? (D)
   A. Deny
   B. Drop
   C. Reset
   D. Allow
2. Are files quarantined while WildFire checks if they are malware or legitimate? (B)
   A. yes
   B. no
   C. By default yes, but you can change the settings.
   D. By default no, but you can change the settings.

Answers under the heading Answers to Given a scenario, identify how to configure policies and related objects. on p. 122.

Identify the methods for automating the configuration of a firewall

Bootstrapping is the process of configuring a firewall automatically. . 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, 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/80/virtualization/virtualization/bootstrap-the-vm-series-firewall/prepare-the-bootstrap-package#_32401Prepare a USB Flash Drive for Bootstrapping a Firewall https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/prepare-a-usb-flash-drive-for-bootstrapping-a-firewall
- Bootstrap the VM-Series Firewall in Azure https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-azure#_46161
- Bootstrap the VM-Series Firewall in AWS (https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws#_75110
- 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

1. Which operating system do you select to use for a Palo Alto Networks NGFW running in Microsoft Azure? (C)
   A. Windows
   B. BSD
   C. Linux
   D. Linux or BSD
2. What are the four component directories of a Palo Alto Networks bootstrap container? (A)
   A. software, config, license, and content
   B. software, config, lic, and content
   C. software, configuration, license, and content
   D. software, configuration, lic, and content

Answers under the heading Answers to Identify the methods for automating the configuration of a firewall on p. 122.

Further Resources

- Firewall 8.0 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 Essentials (221) Course for PAN-OS® 8.0
  https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/edu-221-8x-datasheet.pdf
- PAN-OS 8.0 Admin Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os
- PAN-OS CLI Quick Start
  https://www.paloaltonetworks.com/documentation/80/pan-os/cli-gsg
- PAN-OS 8.0 New Features Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide
- Panorama 8.0 Admin Guide
  https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide
- Panorama 8.0 New Features Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/panorama-features
- GlobalProtect 8.0 Admin Guide
  https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide
- GlobalProtect 8.0 New Features Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/globalprotect-features
- WildFire 8.0 Admin Guide
  https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin
- WildFire 8.0 New Features Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/wildfire-features
- VM-Series Deployment Guide
  https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization
- Virtualization 8.0 New Features Guide
  https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/virtualization-features
- Live Community
  https://live.paloaltonetworks.com/
- Firewall In-Line Help

Appendix A: Sample test

1. Which step happens last to a packet?
   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.)

© 2018 Palo Alto Networks, Inc.

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
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

© 2018 Palo Alto Networks, Inc.

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
14. Which object type(s) has a property to specify whether it can transfer files?
    A. Application
    B. Service
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)

© 2018 Palo Alto Networks, Inc.

    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.
24. Where do you configure protection from malformed IP and TCP headers?
    A. DoS Profile
    B. QoS Profile
    C. Zone Protection 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 platforms 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 confiogure 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 requires a disruption in connectivity?
    A. There never is a need to disrupt connectivity.
    B. Dynamic content updates require a brief disruption while the firewall integrates them with the Security policy.
    C. PAN-OS® updates require a reboot to apply.
34. Which high availability port (or ports) is used for which plane?
    A. HA1 for the dataplane, HA2 for the management plane.
    B. HA1 for the management plane, HA2 for the dataplane.
    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 dataplane 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?
    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
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.
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.
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.

© 2018 Palo Alto Networks, Inc.

    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.

Answers under the heading Answers to the sample test on p. 122.

Appendix B: Answers to sample questions

Answers to Exam Domain 1 – PlanAnswer to Identify how the Palo Alto Networks products work together to detect and prevent threats.

1. C

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

1. D

Answer to 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.

1. A

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

1. B
2. A

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

1. B

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

1. C

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

1. C
2. D

Answer to Identify methods for authorization, authentication, and device administration.

1. B

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

1. A, B

Answers to Identify decryption deployment strategies.

1. D
2. D

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

1. C

© 2018 Palo Alto Networks, Inc.

Answers to Identify the methods of User-ID redistribution

1. A

Answers to Exam Domain 2 – Deploy and Configure

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

1. B

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

1. D

Answers to Identify the relationship between URL filtering and credential theft prevention.

1. D
2. B

Answer to Identify differences between services and applications

1. B, E

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

1. B, D

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

1. B
2. B

Answer to Identify how to configure and maintain certificates to support firewall features.

1. A

Answer to Identify how to configure a virtual router.

1. B

Answer to Identify the configuration settings for site-to-site VPN.

1. D

Answers to Identify the configuration settings for GlobalProtect.

1. D
2. A, B

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

1. B
2. A, B
3. A, C

Answer to Identify how to configure features of the NAT rulebase.

1. B

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

1. A, C, D

Answers to Identify how to configure decryption.

1. C
2. A

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

1. C

Answers to Identify how to configure VM-Series firewalls for deployment.

1. A
2. B, D, E

Answers to Exam Domain 3 – Operate

Answers to Identify considerations for configuring external log forwarding.

1. C
2. B

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

1. A
2. D, E

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

1. C
2. B, D

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

1. C

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

1. D

Answer to 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).

1. B

Answer to Identify the sources of information pertaining to HA functionality.

1. B

© 2018 Palo Alto Networks, Inc.

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

1. A

Answer to Identify the impact of deploying dynamic updates.

1. C

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

1. A, B
2. C

Answers to Exam Domain 4 – Configuration Troubleshooting

Answers to Identify system and traffic issues using WebUI and CLI tools.

1. A
2. D

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

1. D

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

1. D

Answer to Identify how to troubleshoot SSL decryption failures.

1. A

© 2018 Palo Alto Networks, Inc.

Answers to Identify certificate chain of trust issues.

1. D

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

1. B

Answers to Exam Domain 5 – Core Concepts

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

1. C
2. B, D

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

1. B

Answer to Identify methods for identifying users.

1. B

Answer to Identify the fundamental functions residing on the management and dataplanes of a Palo Alto Networks firewall.

1. B

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

1. A

Answers to Identify the fundamental functions and concepts of WildFire

1. A
2. A, D, E

Answer to Identify the purpose of and use case for MFA and the Authentication policy.

1. A, C

Answer to Identify the dependencies for implementing MFA.

1. B, E

Answer to Given a scenario, identify how to forward traffic

1. B

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

1. D
2. B

Answers to Identify the methods for automating the configuration of a firewall

1. C
2. A

Answers to the sample test

1. B
2. D
3. C
4. B
5. C, E
6. C
7. A

8. A
9. B
10. A
11. A, B
12. A, C, D
13. A
14. A
15. A
16. C
17. C
18. C
19. C
20. A, C
21. B, D
22. D
23. B
24. C
25. B
26. A
27. C
28. B
29. A, C
30. A
31. B
32. C
33. C
34. B
35. C, D
36. D
37. B
38. B
39. C
40. A
41. A
42. C
43. D
44. C
45. B
46. D
47. B
48. D
49. A
50. A
51. A

© 2018 Palo Alto Networks, Inc.

Appendix C: 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).*

© 2018 Palo Alto Networks, Inc.

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

© 2018 Palo Alto Networks, Inc.

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 Next-Generation Security 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 great way of reinforcing the key information for those who have been to the formal hands-on classes. They also serve as a great 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 53 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 30,000+ security professionals

© 2018 Palo Alto Networks, Inc.