PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ADMINISTRATOR STUDY GUIDE

January 2020

http://education.paloaltonetworks.com

Palo Alto Networks, Inc. www.paloaltonetworks.com

Table of Contents

Palo Alto Networks PCNSA Study Guide

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

Overview

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

Successfully passing this exam certifies that the successful candidate has the knowledge and skills necessary to implement Palo Alto Networks next-generation firewall PAN-OS® 9.1 platform in any environment. This exam does not cover other products like Panorama, or the Prisma or Cortex suite of products.

Exam Details

- Certification Name: Palo Alto Networks Certified Network Security Administrator
- Delivered through Pearson VUE: www.pearsonvue.com/paloaltonetworks
- Exam Series: PCNSA
- Total Seat Time: 90 minutes
- Number of items: 50
- Time for exam items: 80 minutes
- Format: Multiple Choice, Scenarios with Graphics, and Matching
- Language: English

Intended Audience

The PCNSA 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 system administrators.

Qualifications

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

You have at least 6 months' experience in Palo Alto Networks NGFW deployment and configuration.

Skills Required

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

Recommended Training

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

- Firewall Essentials: Configuration and Management (EDU-210) or digital learning (EDU-110)
- PCNSA Practice Test: PCNSA Practice Test

About This Document

Efforts have been made to introduce all relevant information that might be found in a PCNSA Certification Test. However, other related topics also might appear on any delivery of the exam. This document should not be considered a definitive test preparation guide but an introduction to the knowledge required, and these guidelines might 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.

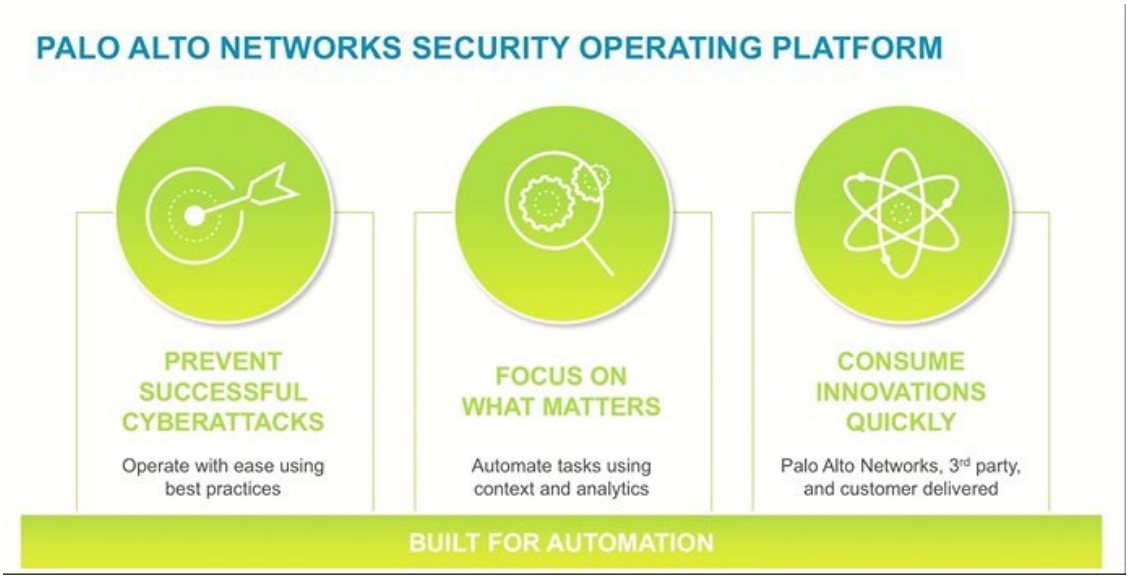
Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.1 Identify the components of the Palo Alto Networks Security Operating Platform.

The Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform is built for automation. The platform successfully prevents cyberattacks by utilizing accurate analytics, implementing automation, and delivering cloud-based applications. The platform integrates applications from Palo Alto Networks, third parties, and customers. The analytics-based automation enables IT personnel to operationalize their security easily and consistently using best practices. Security tools that weren't designed for automation require analysts to manually combine insights from many disconnected sources before they act. The Palo Alto Networks Security Operating Platform eliminates any disconnects by ensuring tight integration across the platform, thus simplifying security so you can secure computing resources, users, applications, and data consistently.

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks by focusing on what matters: leveraging cloud-based security data and applications (see the following figure).



Prevent Successful Cyberattacks: Operate with ease using best practices.

Organizations need to operate efficiently to stop attacks that cause business disruption. The Security Operating Platform empowers you to confidently automate threat identification and prevention across clouds, networks, servers, and endpoints with a data-driven approach utilizing accurate, cloud-delivered analytics. The platform blocks exploits, ransomware, malware, and fileless attacks. It enables you to easily adopt security best practices using application-, user-, and content-based policies. These policies take a Zero Trust approach to minimize opportunities for attack.

Focus on What Matters: Automate tasks, using context and analytics, to reduce response time and speed deployments.

Your operations teams and analysts likely are overburdened. The Security Operating Platform improves productivity via automation, thus allowing IT personnel the time to focus on higher-value activities.

Automation enables you to streamline routine tasks. Tight integration across the platform with ecosystem partners delivers consistent security across the cloud, networks, and endpoints (CNE). The shared intelligence and consistent enforcement across CNE strengthen prevention and reduces response time. DevOps can improve the speed of multi-cloud deployment and simplify management through deep integrations with native cloud services and automation tools. Plus, your teams can continuously validate compliance of cloud deployments with customizable reports and controls that save time. Security controls are automated with security policies that dynamically change to match your applications, users, and content.

Consume Innovations Quickly: Improve security effectiveness and efficiency with tightly integrated innovations.

Threats are dynamic. You need to keep evolving to stay ahead. The platform continually improves security effectiveness and efficiency with tightly integrated innovations. With Palo Alto Networks Cortex as part of the platform, you can get the most out of your existing investments, including your existing unified security data set, sensors and enforcement points, with custom and third- party security applications. Whether these apps are developed by Palo Alto Networks, our ecosystem of third parties, or your own teams (customer apps), they can detect and report on threats, or automate enforcement workflows, to reduce response time. Organizations now can deploy frictionless, seamlessly integrated security, delivered from the cloud as applications. These applications provide unlimited plug- and-play protection, with drag-and-drop innovation. Application developers everywhere have instant access to more than 10,000 organizations and more than a decade’s worth of aggregated threat data and telemetry.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform has the following components:

- Network Security
- Advanced Endpoint Protection
- Cloud Security
- Cloud-Delivered Security Services
- Cortex and Cortex Data Lake
- Palo Alto Networks Apps, Third-Party Apps, and Customer Apps

Network Security

Palo Alto Networks firewalls enable you to adopt best practices using application-, user-, and content-based policies to minimize opportunities for attack. Our next-generation firewalls are available as physical appliances, virtualized appliances, and cloud-delivered services, all managed consistently with Panorama. These next-generation firewalls secure your business with a prevention-focused architecture and integrated innovations that are easy to deploy and use. Palo Alto Networks next-generation firewalls detect known and unknown threats, including those within encrypted traffic, using intelligence generated across many thousands of customer deployments. The firewalls reduce risks and prevent a broad range of attacks. For example, they enable users to access data and applications based on business requirements and they stop credential theft and an attacker's ability touse stolen credentials.

With our next-generation firewalls, you can quickly create security rules that mirror business policy and are easy to maintain and adapt to your dynamic environment. They reduce response times with automated policy-based actions, and you can automate workflows via integration with administrative tools such as ticketing services, or any system with a RESTful API.

The family of next-generation firewalls includes:

- VM-Series: Our virtualized next-generation firewall protects your private and public cloud deployments by segmenting applications and preventing threats. For more information, see

https://www.paloaltonetworks.com/products/secure-the-cloud/vm-series.

- Prisma Access: Prisma Access cloud service provides next-generation firewall security delivered from the cloud globally in an operationally efficient manner. For more information, see https://www.paloaltonetworks.com/products/globalprotect/cloudservice.
- Physical firewalls: Physical firewalls currently being sold include the PA-220, PA-800, PA-3200, PA-5200, and PA-7000 series. Older models include the PA-200, PA-500, PA-3000 and PA-5000 series. For more information, see https://www.paloaltonetworks.com/products/secure-the-network/next-generation- firewall.

Advanced Endpoint Protection

Advanced Endpoint Protection blocks exploits, ransomware, malware, and fileless attacks to minimize infected endpoints and servers. Traps advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. Traps is the only solution that pre-emptively blocks security breaches such as ransomware attacks, using a unique multi-method approach that prevents known and unknown malware, exploits, and zero-day threats. Traps is being integrated into the Cortex product line in 2020 and will take the Cortex product name.

Traps is unique in the breadth and depth of its endpoint protections:

- Stops malware, exploits, and ransomware before they can compromise endpoints.
- Provides protection while endpoints are online and offline, on network and off network.
- Coordinates enforcement with network and cloud security to prevent successful attacks.
- Detects threats and automates containment to minimize impact.
- Includes WildFire® cloud-based threat analysis service with your Traps subscription.
- Integrates with the Palo Alto Networks Security Operating Platform.

For more information, see https://www.paloaltonetworks.com/products/secure-the-endpoint/traps.

Cloud Security

Cloud Security speeds up multi-cloud deployments, with continuous compliance validation, through deep integrations with native cloud services and automation tools. Palo Alto Networks provides advanced protection for consistent security across all major clouds: Amazon Web Services, Microsoft Azure and Google Cloud Platform.

Our cloud-based products protect and segment applications, deliver continuous security and compliance, and achieve zero-day prevention. Palo Alto Networks lets you deliver consistent, automated protections across public and private clouds so you can adopt SaaS applications, rapidly roll out cloud-delivered services and applications, and avoid business disruption.

Cloud security is delivered by:

- **Inline security (VM-Series firewalls):** The VM-Series protects your private and public cloud deployments by enabling applications and preventing threats.
- **API security (Cortex XDR, Prisma SaaS):** Continuously monitor and secure your cloud workloads via API to prevent data loss and enable compliance.
- **Host security (Traps):** Protect cloud workloads against zero-day threats with multiple methods of prevention and minimal impact on resources.

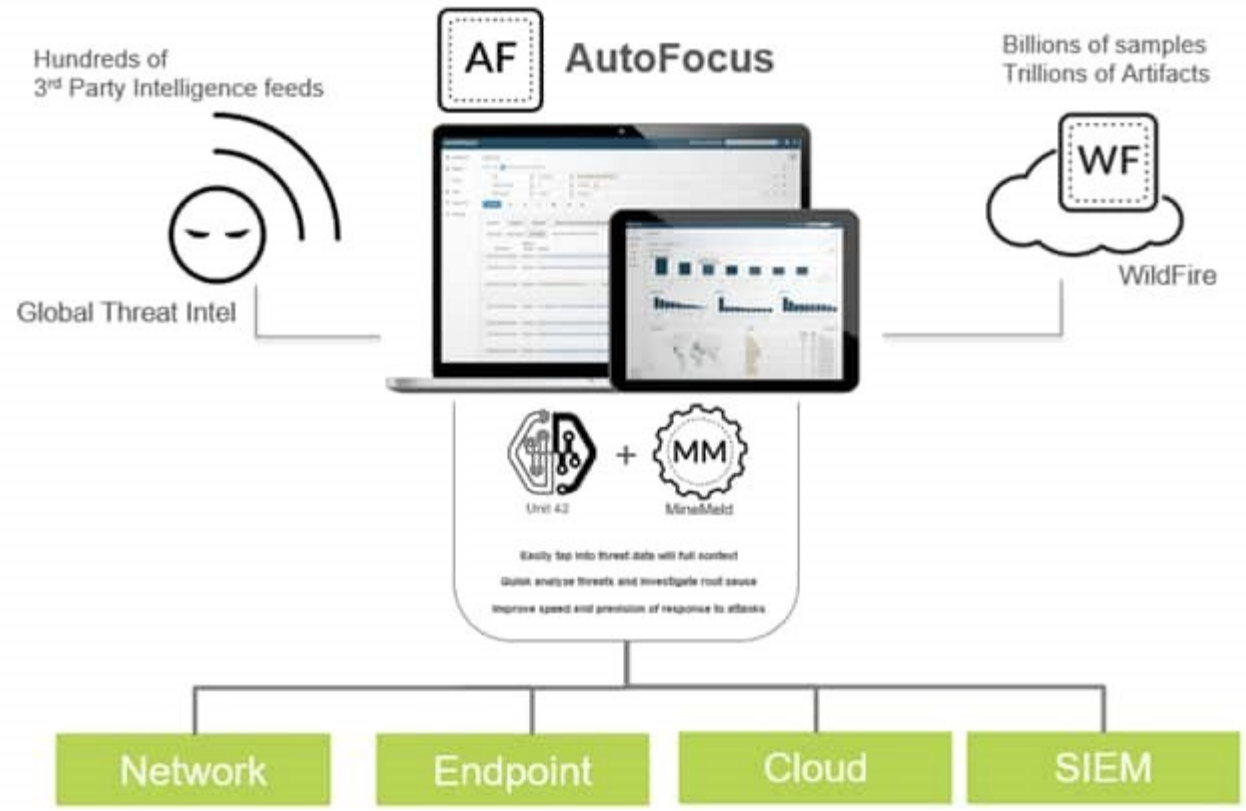
For more information, see https://www.paloaltonetworks.com/products/secure-the-cloud.

Cloud-Delivered Security Services

Confidently automate threat identification and prevention everywhere. Our security subscriptions allow you to safely enable applications, users, and content by adding natively integrated protection from known and unknown threats both on and off the network.

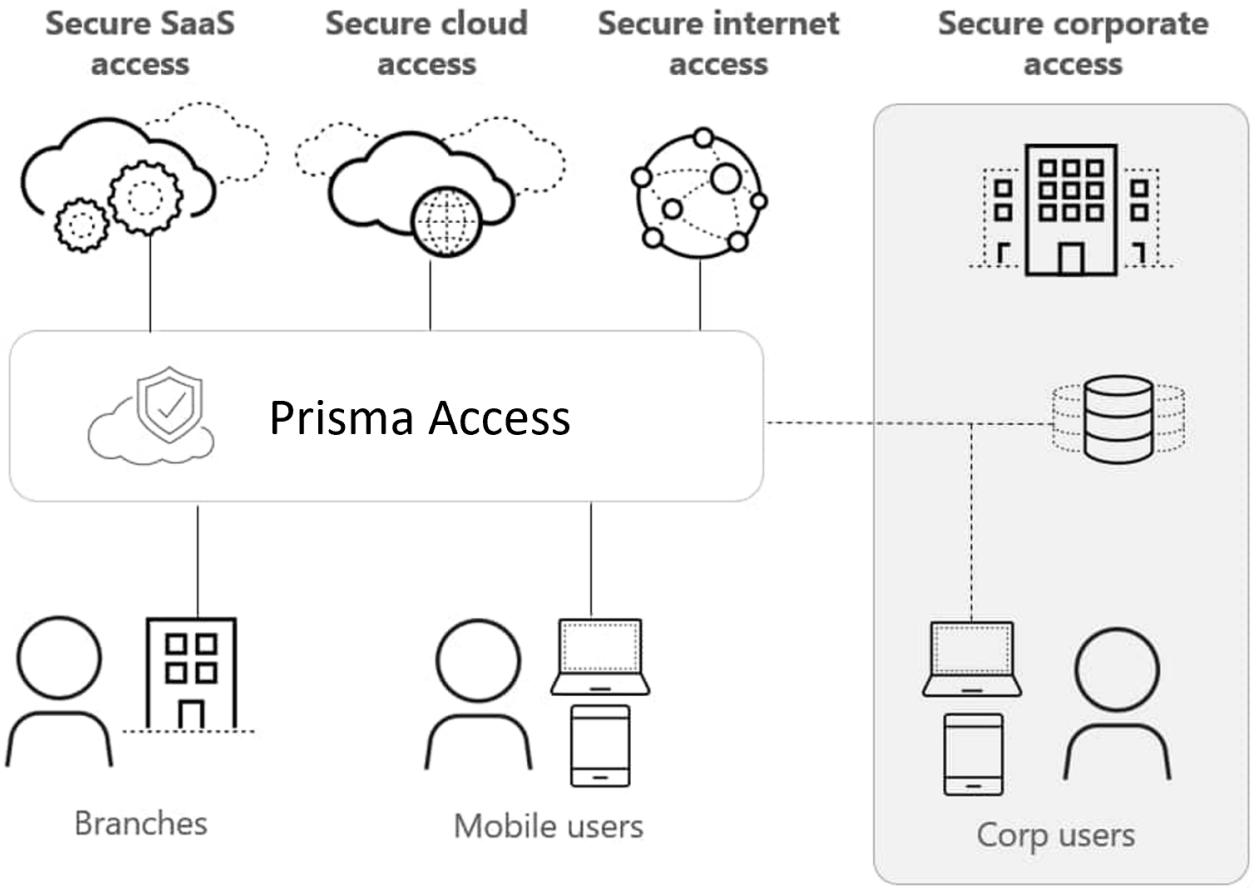
These security subscriptions are purpose-built to share context and prevent threats at every stage of an attack, enabling you to configure singular policies and automated protection that secure your network and remote workforce while simplifying management and enabling your business. The Security Services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

- **AutoFocus:** Disparate tools and data sources have made the jobs for security analysts more difficult to do quickly and effectively. AutoFocus contextual threat intelligence brings speed, consistency, and precision to threat investigation. It provides instant access to community-based threat data, enhanced with deep context and attribution from the Unit 42 threat research team, saving time and effort. Now your teams can quickly investigate, correlate, and pinpoint malware's root cause without adding dedicated malware researchers or additional tools. Plus, automated protections make raw intelligence simple to turn into protection across your environment.



For more information, see https://www.paloaltonetworks.com/products/secure-the-network/autofocus.html.

- **Prisma Access***:* You need to secure all users equally. But mobile, branch, and cloud expansion move applications and users beyond the perimeter, which makes traditional network security inefficient. Prisma Access provides the full security capabilities of the Palo Alto Networks next-generation firewall, delivered as a service. Now you can protect users across your organization and prevent successful cyberattacks with scale and simplicity, and without compromise. Prisma Access automates the orchestration and rollout of security services, reducing deployment time. You can deploy new features, increase coverage, and scale globally with cloud infrastructure, which gives you a new level of flexibility



For more information, see https://www.paloaltonetworks.com/products/globalprotect/cloudservice.html.

URL Filtering Web Security: Most attacks and exposure to malicious content occur during normal web browsing activities. URL filtering with PAN-DB automatically prevents attacks that leverage the web as an attack vector, including phishing links in emails, phishing sites, HTTP-based command-and-control, malicious sites, and pages that carry exploit kits.URL filtering provides:

- Reduction of the risk of infection from dangerous websites and protection of users and data from malware and credential-phishing pages.
- Protection across the attack lifecycle through integration with WildFire and the Security Operating Platform.
- Retention of protections synchronized with the latest threat intelligence through our cloud-based URL categorization for phishing, malware, and undesired content.
- Full visibility and threat inspection into normally opaque web traffic through granular control over SSL decryption.

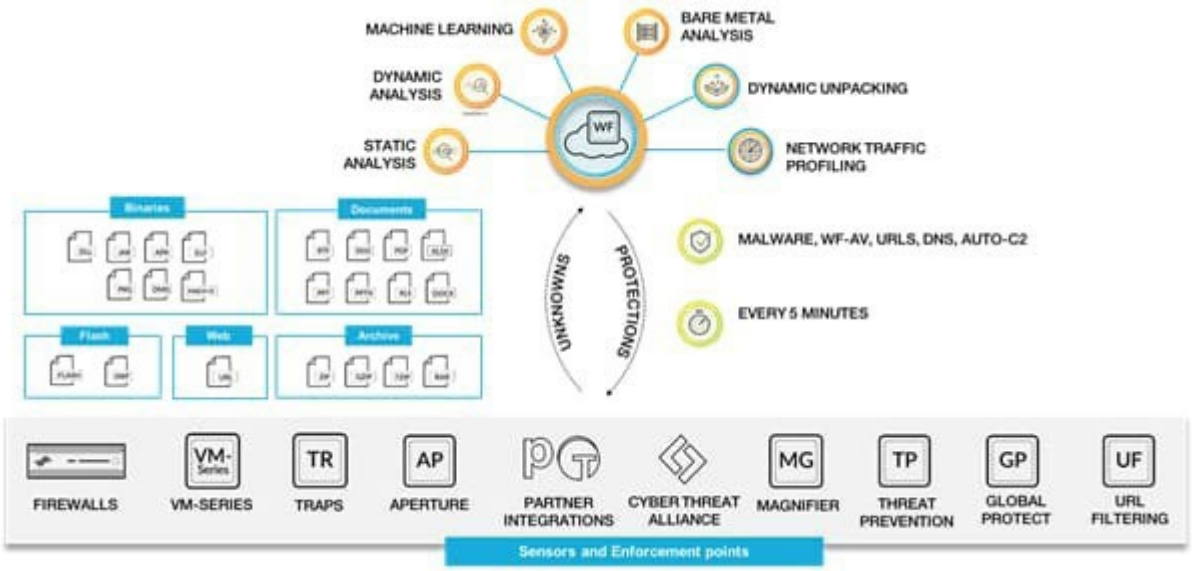
For more information, see https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb.

- **Threat Prevention:** Because threats do not discriminate between application delivery vectors, an approach to security is needed that has full visibility into all application traffic, including SSL encrypted content, with full user context. Threat Prevention leverages the visibility of our next-generation firewall to inspect all traffic, and thus automatically prevents known threats, regardless of port, protocol, or SSL encryption.

Threat Prevention automatically stops vulnerability exploits with IPS capabilities, offers inline malware protection, and blocks outbound command-and control traffic. When combined with WildFire and URL filtering, organizations are protected at every stage of the attack lifecycle, including both known and zero-day threats.

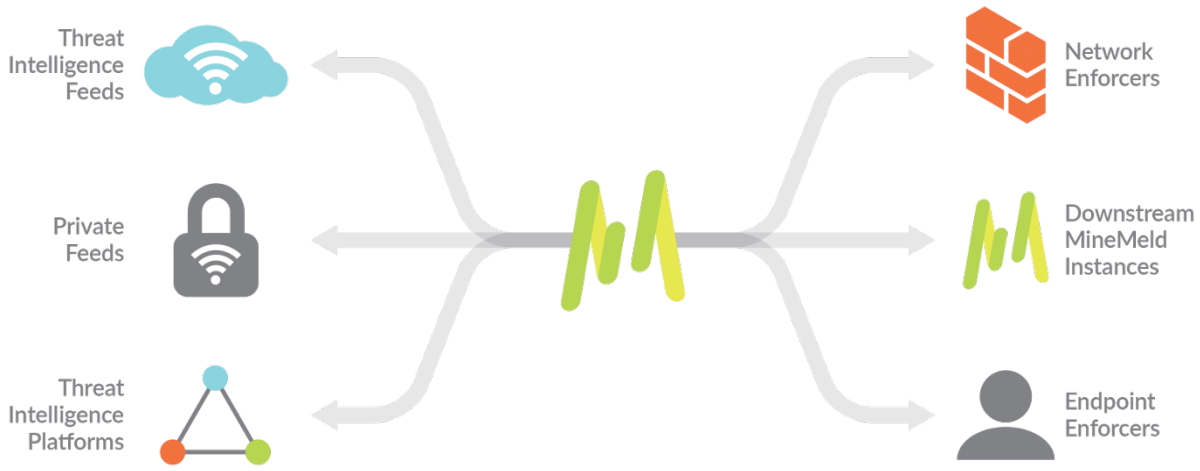
For more information, see https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/threat-prevention.

- **WildFire Malware Analysis:** WildFire automatically prevents zero-day exploits and malware. Traditional malware analysis and sandboxing techniques are not adequate and cannot keep pace with new exploits. WildFire uses shared community-sourced threat data and advanced analysis, and immediately shares protections across the network, endpoint, and cloud. WildFire automatically delivers protections about every five minutes (by accessing a database that is updated every 5 minutes), thus preventing successful cyberattacks. (Note that "Aperture" shown in the following figure now is called "Prisma SaaS." Also, Traps and Magnifier are now part of "Cortex XDR".)



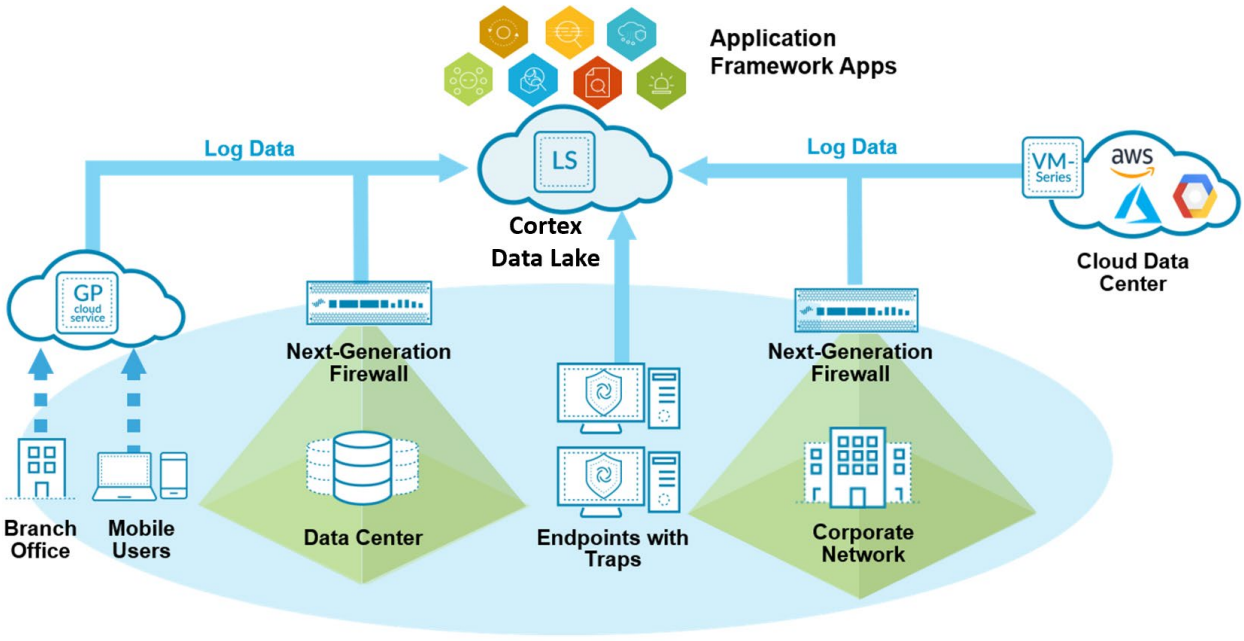
For more information, see https://www.paloaltonetworks.com/products/secure-the-network/wildfire.html.

MineMeld Threat Intelligence Sharing: To prevent successful cyberattacks, many organizations collect indicators of compromise (IOCs) from various threat intelligence providers with the intent of creating new controls for their security devices. Unfortunately, legacy approaches to aggregation and enforcement are highly manual in nature, and often create complex workflows that require the extension of the time needed to identify and validate which IOCs should be blocked. Now security organizations can leverage MineMeld, an open-source application that streamlines the aggregation, enforcement, and sharing of threat intelligence. MineMeld is available for all users directly on GitHub and pre-built virtual machines (VMs) for easy deployment. Customers with an AutoFocus subscription also receive access to a private instance of MineMeld as part of their AutoFocus subscription. With the proper software, anyone can add to the MineMeld functionality by contributing code to the open-source repository.



For more information, see [https://www.paloaltonetworks.com/products/secure-the- network/subscriptions/minemeld](https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld).

- **Cortex Data Lake:** On-premises log management traditionally has been a chore. Now the cloud-delivered Cortex Data Lake enables you to easily collect large volumes of log data, so innovative applications can gain insight from your environment. You can simplify your log infrastructure, automate log management, and use your data to prevent attacks more effectively.



For more information, see https://www.paloaltonetworks.com/products/management/logging-service.

- **Cortex XDR:** Cortex XDR applies machine learning at a cloud scale to network, endpoint, and cloud data so that you can quickly find and stop targeted attacks, insider abuse, and compromised endpoints. Cortex XDR uncovers the actions attackers cannot conceal, by profiling user and device behavior and identifying anomalies that indicate active attacks. Cortex XDR

integrates rich metadata collected from the Security Operating Platform with attack detection algorithms and enables you to detect post-intrusion activity with precision.

Cortex XDR stops these threats:

- Targeted attacks: Cortex XDR detects anomalous activities that attackers carry out as they move around the network looking for valuable data.
- Malicious insiders: By profiling behavior, Cortex XDR identifies behavioral anomalies such as internal reconnaissance and credential abuse to identify attacks.
- Risky behavior: Cortex XDR allows your organization to follow security best practices by monitoring user activity and identifying risky behavior.
- Compromised endpoints: Cortex XDR detects malware behavior and confirms infections using Pathfinder endpoint analysis and WildFire threat analysis services.

For more information, see https://www.paloaltonetworks.com/products/xdr.

Cortex and Cortex Data Lake

Put security innovations to work sooner and with less effort. Cybersecurity innovations come from many sources: Palo Alto Networks, third parties, and customers. With Palo Alto Networks Cortex, you can use applications from these sources right away, so you can stay a step ahead of attackers.

With Cortex, customers can rapidly access, evaluate, and adopt new security technologies as an extension of the next-generation Security Operating Platform they already own and operate. The all-new framework is a culmination of more than a decade of security disruption that has provided customers with superior security through cloud-based applications developed by Palo Alto Networks and today's most innovative security providers, large and small.

All threats are dynamic. Security needs to keep evolving to stay ahead of the latest threats. New capabilities are tightly integrated, building on the value of what you already have. With Palo Alto Networks Cortex, you can quickly consume innovative security applications, using your existing security data, sensors and enforcement points. Whether these applications are developed by Palo Alto Networks, our ecosystem of third parties, or your own teams, they can detect and report on threats or automate enforcement workflows to reduce response time. Thus the Security Operating Platform enables you to maximize your existing Palo Alto Networks investment.

Cortex consists of the following components:

- **Infrastructure:** A suite of cloud APIs, services, compute, and native access to customer-specific data stores
- **Customer-specific data store:** The Palo Alto Networks Cortex Data Lake
- **Apps:** Applications that are delivered from the cloud to extend the capabilities of the platform, including the ability to effortlessly collaborate between different applications, share threat context and intelligence, and drive automated response and enforcement.

For more information, see https://www.paloaltonetworks.com/products/application-framework.

Sample questions

1. The Palo Alto Networks Security Operating Platform is designed for which three purposes? (Choose three.)

    A. consume innovations quickly
    B. ensure compliance
    C. focus on what matters
    D. prevent successful cyberattacks

2. Which item is not one of the six primary components of the Palo Alto Networks Security Operating Platform?

    A. Applications (Palo Alto Networks applications, third-party applications, customer applications)
    B. Cloud-Delivered Security Services
    C. WildFire
    D. Cortex and Cortex Data Lake
    E. Network Security
    F. Advanced Endpoint Protection
    G. Cloud Security

3. Which cloud-delivered security service provides instant access to community-based threat data?

    A. Prisma SaaS
    B. AutoFocus
    C. Threat 42
    D. Cortex XDR

4. Which cloud-delivered security services provides security for branches and mobile users?

    A. MineMeld
    B. Cortex XDR
    C. AutoFocus
    D. Prisma Access

5. Which Palo Alto Networks Security Operating Platform component provides access to applications from Palo Alto Networks, third parties, and customers?

    A. Cloud-Delivered Security Services
    B. WildFire
    C. Cortex
    D. Network Security
    E. Advanced Endpoint Protection

6. Which Palo Alto Networks firewall feature provides all the following abilities?

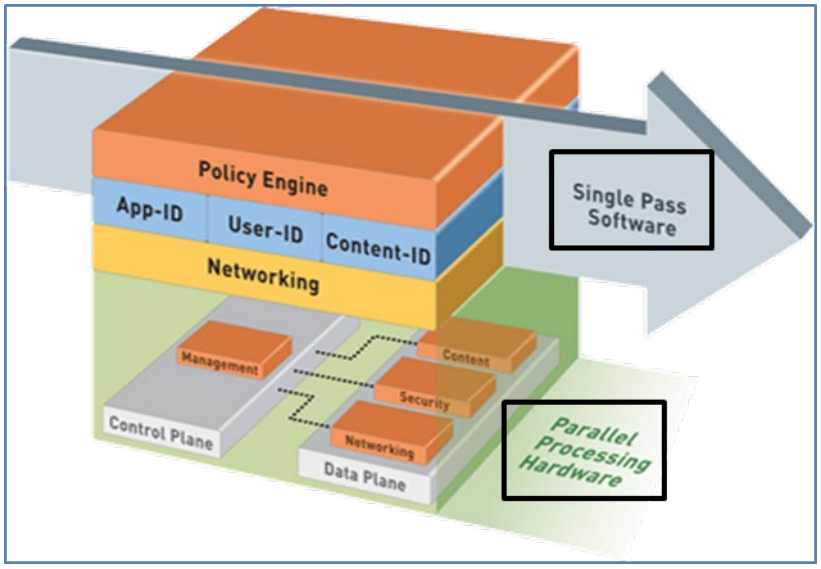
    - Stops malware, exploits, and ransomware before they can compromise endpoints
    - Provides protection while endpoints are online and offline, on network and off
    - Coordinates enforcement with network and cloud security to prevent

successful attacks

- Detects threats and automates containment to minimize impact
- Includes WildFire cloud-based threat analysis service with your Cortex XDR subscription
- Integrates with the Palo Alto Networks Security Operating Platform
  A. Cortex XDR
  B. Prisma SaaS
  C. URL Filtering
  D. WildFire
  E. GlobalProtect
  F. AutoFocus

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.2 Identify the components and operation of single-pass parallel processing architecture.



Palo Alto Networks has reduced latency enormously, using the Single-Pass Parallel Processing (SP3) architecture, which combines two complementary components:

- Single-Pass Software
- Parallel Processing Hardware

The SP3 architecture is the overall design approach for Palo Alto Networks next-generation firewalls. The architecture enables full, contextual classification of traffic, followed by a set of enforcement and threat prevention options. The architecture classifies and controls traffic in a “single pass” through the firewall using a variety of stream-based technology components. Each current protection feature in the device (antivirus, spyware, data filtering, and vulnerability protection) uses this stream-based signature format. The stream-based design of the architecture results in superior performance, especially when multiple security functions are enabled.

This architecture enables you to achieve superior security posture and efficiency. The SP3 architecture enables Palo Alto Networks to exceed competitors' firewall performance. In competitive approaches, next-generation features often are added in a sequence of separate engines that limit policy flexibility, negatively impact performance, and increase management complexity.

The software's "scan it all, scan it once" approach enables superior security posture and performance on both physical and virtual next-generation firewalls. The architecture incorporates advanced technologies (e.g., App-ID, User-ID, and WildFire) to provide superior classification and control capabilities to help secure your organization's network.

Management and Data Planes

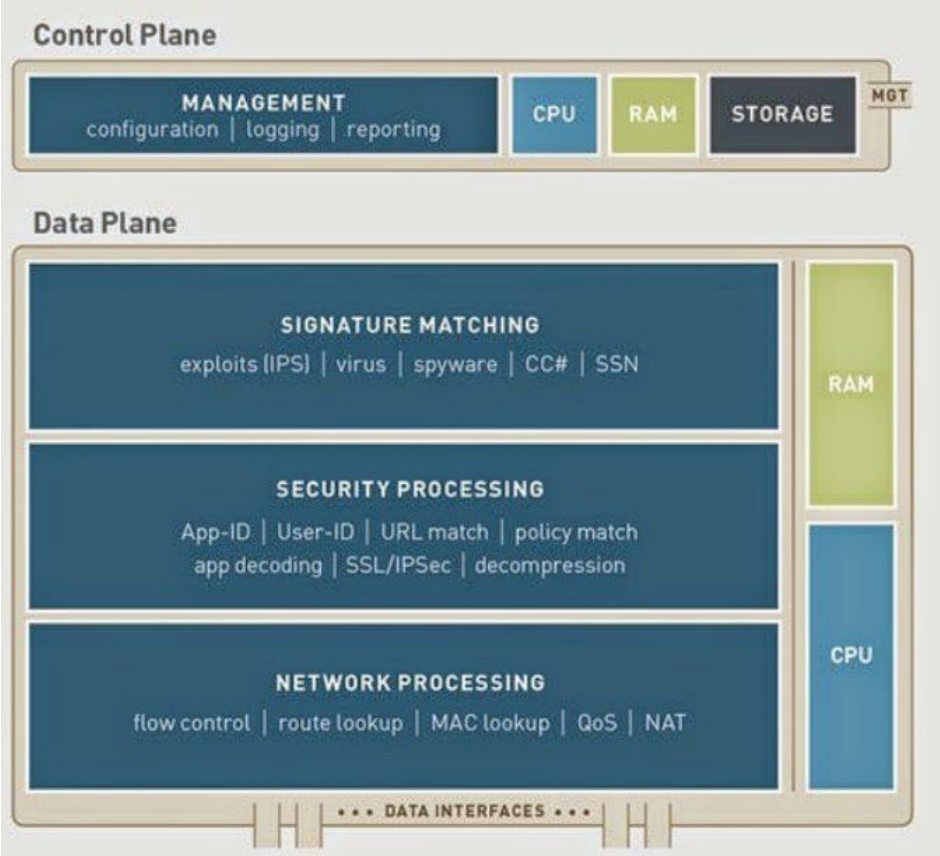
In addition to the Single Pass Software, hardware is the other critical piece of the Palo Alto Networks SP3 architecture. The management plane and data-plane functionality on both physical and virtual firewalls is integral to all Palo Alto Networks firewalls. These separate planes have dedicated hardware resources (CPU, RAM, and storage), making them independent of each other. This separation means that heavy use of one plane will not adversely impact the other plane's performance. For example, an administrator could be running a very processor-intensive report, and yet the ability to process packets would not be affected by this reporting job, because of the separation of the data and control planes.

The control plane provides the management features of the firewall:

- Firewall configuration
- Logging
- Reporting

The data plane provides the data processing features of the firewall:

- Signature matching
- Security processing
- Network processing



Sample questions

7. Which management features does the control plane provide? (Choose three.)

    A. security processing
    B. logging
    C. reporting
    D. firewall configuration
    E. signature matching
    F. network processing

8. Which three data processing features does the data plane provide? (Choose three.)

    A. network processing
    B. security processing
    C. signature matching
    D. firewall configuration
    E. logging
    F. reporting

9. What are three components of the Network Processing module? (Choose three.)
    A. QoS
    B. NAT
    C. App-ID
    D. flow control
    E. url match
    F. spyware
10. Which approach most accurately defines the Palo Alto Networks SP3 architecture?
    A. prioritize first
    B. sequential processing
    C. scan it all, scan it once
    D. zero trust segmentation platform
11. What is the result of using a stream-based design of architecture?
    A. superior performance
    B. increased latency
    C. superior latency
    D. increased functionality

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.3 Given a network design scenario, apply the Zero Trust security model and describe how it relates to traffic moving through your network.

In the traditional security model, internal users, devices, and applications, and the traffic they generated were trusted (authenticated and allowed access), but verification (monitoring and inspection of their traffic) was not implemented, because that traffic was "trusted." This traditional security model is not effective in combatting today's sophisticated cyberattacks. Most attacks today are caused by compromised endpoints such as computers and mobile devices. The endpoint traffic can then traverse the network laterally within the corporation to infect database servers and other high-value targets. The traditional perimeter-only security model is a broken security model.

Thus, internal traffic not only needs to be "trusted," it also needs to be continually monitored and inspected for any anomalies such as malware delivery, reconnaissance, exploitation, attacks, malware installation, and command-and-control (C2) activity.

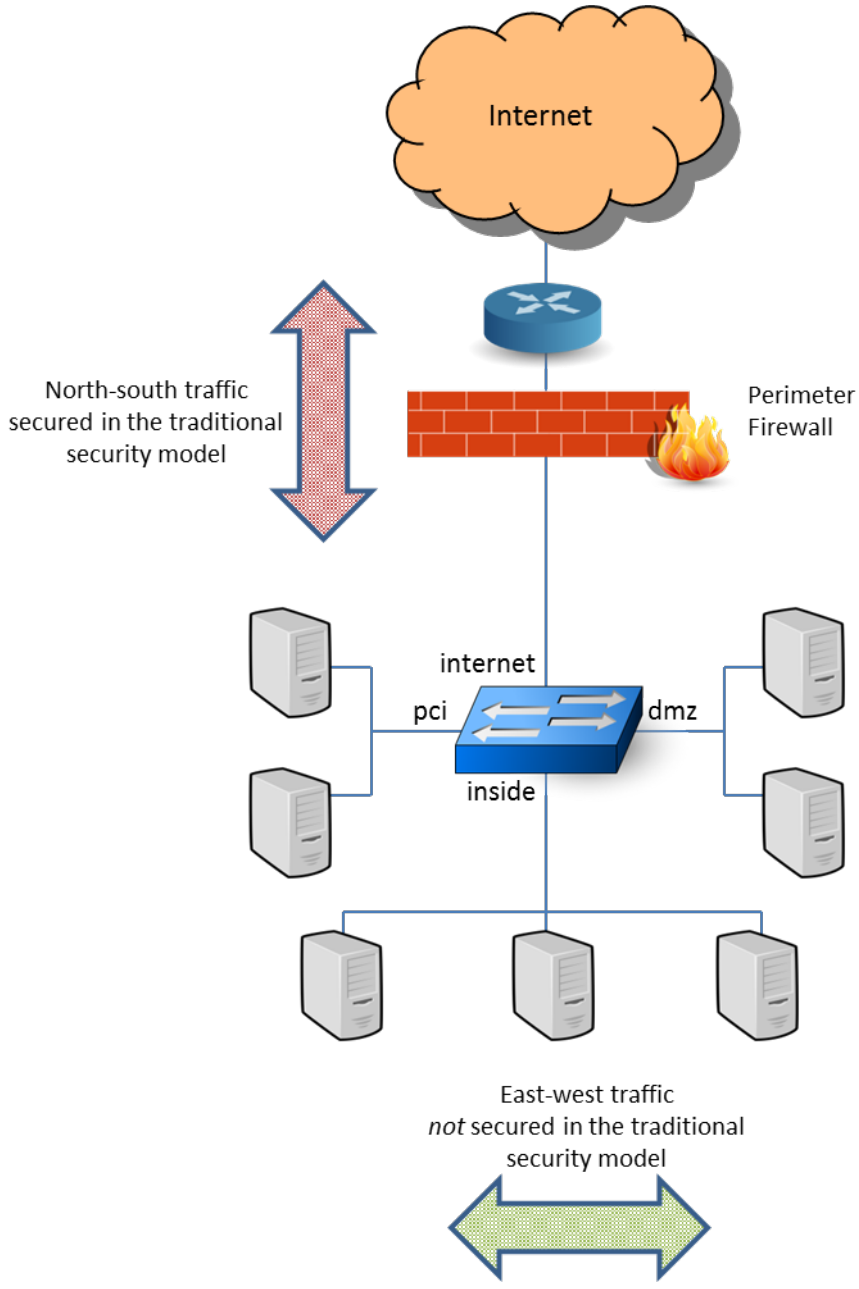
Note that internal users, devices, and applications do not include just those physically located at the corporate site; they also include those that access the company site via remote access technologies such as VPN, Citrix, remote desktop, SSH, HTTP, and HTTPS. Here are some examples of "internal" users.

- Remote employees
- Partners
- Wireless users

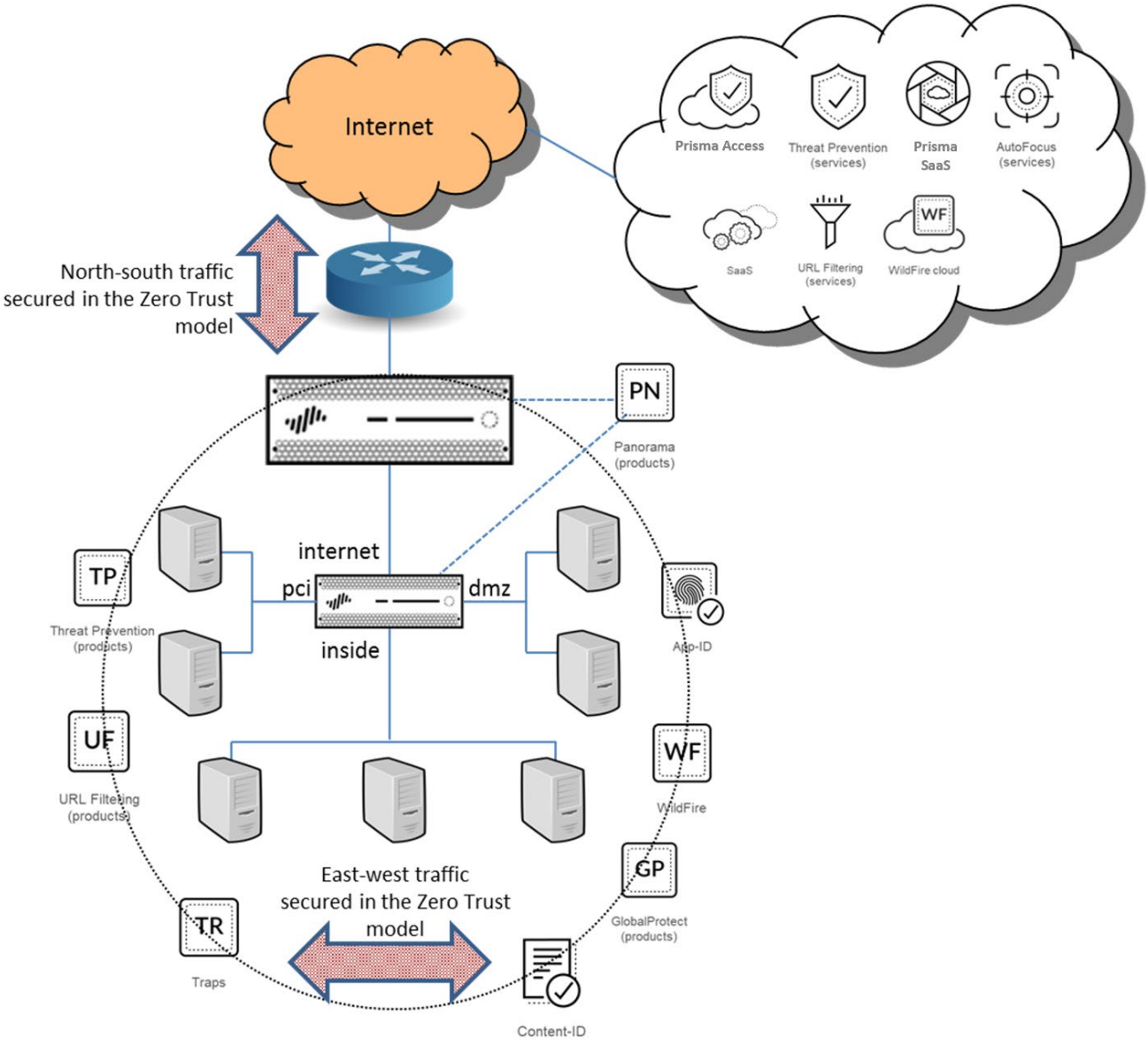
- Remote/branch offices
- Internal employees

Zero Trust is an alternative security model that addresses the shortcomings of the traditional, perimeter-centric strategies. A perimeter-centric strategy is one where all the security is enforced at the network juncture between the internal network and the internet (north-south traffic). Zero Trust is rooted in the principle of "never trust, always verify," and is designed to address lateral (east-west traffic) threat movement within a network by segmenting the network and applying security enforcement at each network boundary. For example, an attacker that infiltrates an endpoint still may need to move laterally throughout the environment to reach the data center where the targeted content resides.

Data Flow in the Traditional, Perimeter-Centric Network



Data Flow in the Zero Trust Network



Zero Trust has three main concepts.

All resources are accessed in a secure manner regardless of location:

- This concept is especially important as it relates to mobility. Zero Trust must secure the following use cases:
    - Tablet computers
    - Smartphones
    - Road warriors
    - Laptop users
    - Home workers
- Access control is on a “need-to-know” basis and is strictly enforced:
    - Access control must be done on a granular basis.

    - The WikiLeaks Attack is one example of an attack that was executed due to lack of enforcement)
- All traffic is logged and inspected:
    - Not just on perimeter (north-south) traffic
    - Include traffic that moves laterally (east-west) inside a network

In summary, both north-south and east-west traffic must be controlled, monitored, inspected, and logged to prevent today's sophisticated cyberattacks.

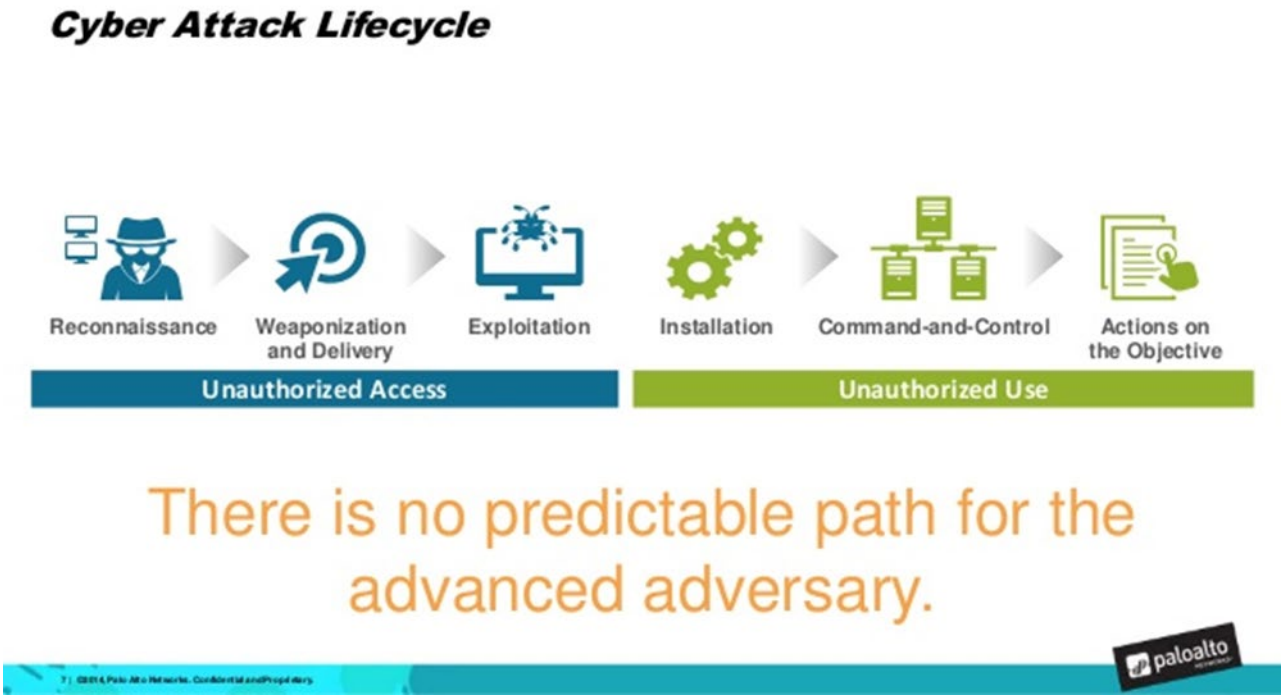
Sample questions

12. Which security model does Palo Alto Networks recommend that you deploy?
    A. separation-of-trust
    B. zero trust
    C. trust-then-verify
    D. never trust
13. The Zero Trust model is implemented to specifically inspect which type of traffic?
    A. east-west
    B. north-south
    C. left-right
    D. up-down
14. What are the three main concepts of Zero Trust? (Choose three.)
    A. All resources are accessed in a secure manner, regardless of location.
    B. Access control is on a "need-to-know" basis and is strictly enforced.
    C. Credentials need to be verified.
    D. All traffic is logged and inspected.
    E. Internal users are trusted implicitly.
    F. External users are trusted explicitly.
15. Which two statements are true about the Zero Trust model? (Choose two.)
    A. Traffic is inspected laterally.
    B. Traffic is inspected east-west.
    C. Internal traffic is implicitly trusted.
    D. External traffic is implicitly trusted.
16. Which three Palo Alto Networks products secure your network? (Choose three.)
    A. MineMerge
    B. Prisma SaaS
    C. URL filtering
    D. Containers
    E. TrapContent
    F. WildFire

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.4 Identify stages in the Cyber-Attack Lifecycle and firewall mitigations that can prevent attacks.

The Cyber-Attack Lifecycle is a sequence of events that an attacker goes through to successfully infiltrate a network and exfiltrate data from it. Blocking just a single stage in this lifecycle often is enough to protect a company's network from a successful attack. Palo Alto Networks products prevent advanced cyberattacks at every stage of the attack lifecycle. The Palo Alto Networks platform protects every part of the global enterprise network: it addresses vulnerabilities and malware arriving at the endpoint, mobile device, and network perimeter, or within the data center.



When cyberattackers strategize their way to infiltrate an organization's network and exfiltrate data, they follow the series of stages that comprise the attack lifecycle. They must progress through each stage to successfully complete an attack. Block cyberattacks at any point in the cycle to break the chain of attack. Note that the attacks can follow any order with the attack chain. The following sections describe the different stages of the attack lifecycle and steps that should be taken at each stage to prevent an attack.

1. Reconnaissance: During the first stage of the attack lifecycle, cyber adversaries carefully plan their method of attack. Attackers research, identify, and select targets within an organization such as human resources and financial personnel that will allow them to meet their objectives. Attackers can gather intelligence through publicly available sources such as Twitter, LinkedIn, and corporate websites – all the places where a company will share information about itself. Cyberattackers also will scan for vulnerabilities that can be exploited within the target network (services and applications) and map out areas that they can take advantage of.

Prevent by:

- Performing continuous inspection of network traffic flows to detect and prevent port scans and host sweeps.
- Implementing security awareness by limiting what should be posted on the internet: sensitive documents, customer lists, event attendees, job roles, and responsibilities.

2. Weaponization and Delivery: If any vulnerability has been detected by reconnaissance, attackers next determine which methods to use to deliver malicious payloads. Methods they might use include automated tools such as exploit kits, spear phishing attacks with malicious links, infected attachments, and malvertizing.

Prevent by:

- Gain full visibility into all traffic, including SSL traffic, by decrypting it and blocking high-risk applications
- Extending protections to remote and mobile devices
- Protecting against perimeter breaches by blocking malicious or risky websites using URL filtering
- Blocking known exploits, malware, and inbound command-and-control (C2) communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-C2, DNS monitoring, sinkholing, and file and content blocking
- Detecting unknown malware and automatically informing customers and third parties globally to thwart new attacks
- Providing ongoing education to users about spear phishing links, watering hole attacks, unknown emails, risky websites, malicious USB drives, and other attack methods

3. Exploitation: In this stage, attackers deploy an exploit against a vulnerable application or system, typically using an exploit kit or weaponized document such as a Microsoft Word .doc or Adobe Acrobat .pdf file. An exploit kit or weaponized document enables the attacker to gain an initial entry point into the organization.

Prevent by:

- Keep systems patched
- Educating users to recognize phishing attempts
- Blocking known and unknown vulnerability exploits on the endpoint
- Automatically delivering new protections globally to thwart follow-up attacks

4. Installation: After cyberattackers have established an initial foothold, they will install malware to conduct further operations, such as maintaining access, maintaining persistence, and escalating privileges. Off-the-shelf tools are the most common method of attack.

Prevent by:

- Preventing malware installation on the endpoint, network, and cloud services

- Establishing secure security zones with strictly enforced user access controls that provide ongoing monitoring and inspection of all traffic between zones (Zero Trust model)
- Limiting local administrator access for users
- Training users to identify the signs of a malware infection and know how to follow up if something occurs

5. Command and Control: With malware installed, attackers own both sides of the connection: their malicious infrastructure and the infected endpoint. They can actively control the system and proceed to the next stages of an attack. Attackers will establish a command channel to be able to communicate and pass data back and forth between the infected devices and their own infrastructure. Typical surveillance methods include key logging, audio capture, screen capture, and webcam capture.

Prevent by:

- Blocking outbound C2 communications
- Blocking uploads that match file and data pattern uploads
- Redirecting malicious outbound communication to internal sinkholes to identify and block compromised hosts
- Blocking outbound communication to known malicious URLs through URL filtering
- Creating a database of malicious domains to ensure global awareness and prevention through DNS monitoring
- Limiting the attacker's ability to move laterally within a network

6. Actions on the Objective: These actions are completed by an active attacker. After attackers have control, persistence, and ongoing communication between the endpoint and the attacker's infrastructure, they will act to achieve their goal. Their objective could be to exfiltrate data, destroy critical infrastructure, deface a website, or create fear or the means for extortion.

Prevent by:

- Using threat intelligence tools to proactively hunt for indicators of compromise (IoCs) on the network
- Monitoring and inspecting all traffic between security zones
- Enforcing user access controls across secure zones
- Blocking outbound C2 communications along with traffic that matches file and data pattern uploads
- Using URL filtering to block outbound communication to known malicious URLs
- Implementing granular control of applications and applying user control to enforce file transfer application policies on the enterprise
- Eliminating known archiving and transfer tactics and limiting the attacker's ability to move laterally within a network

As was mentioned, advanced attacks are very complex because an adversary can succeed only by progressing through every stage of the attack lifecycle. If they cannot successfully take advantage of vulnerabilities, then they cannot install malware and will not be able to obtain command and control over the system. Cyber-security is asymmetric warfare: An attacker must do everything correctly to succeed, but a network defender needs to do only one thing correctly among multiple opportunities to prevent an attack.

Disruption of the attack lifecycle relies not only on technology but also on people and processes in the organization. The people must receive ongoing security awareness training and be educated in best practices to minimize the likelihood of an attack progressing past the first stage. Processes and policies must be in place for remediation if an attacker successfully progress through the entire attack lifecycle.

Here is a link to an on-demand webinar that examines the anatomy of real attacks carried out by advanced adversaries: https://www.paloaltonetworks.com/resources/webcasts/defeat-pragmatic-adversary.html

Sample questions

17. True or false: Blocking just one stage in the Cyber-Attack Lifecycle is all that is neededto protect a company's network from attack.
    A. true
    B. false
18. What are two stages of the Cyber-Attack Lifecycle? (Choose two.)
    A. weaponization and delivery
    B. manipulation
    C. extraction
    D. command and control
19. Command and control be prevented through which two methods? (Choose two.)
    A. exploitation
    B. DNS Sinkholing
    C. URL filtering
    D. reconnaissance
20. Exploitation can be mitigated by which two actions? (Choose two.)
    A. keeping systems patched
    B. using local accounts
    C. blocking known and unknown vulnerability exploits on the endpoint
    D. providing admin credentials

Exam Domain 2 – Simply Passing Traffic

2.1 Identify and configure firewall management interfaces.

Management Access to the Palo Alto Networks Firewalls

Four methods are used to manage the Palo Alto Networks next-generation firewalls:

- Web interface
- CLI
- Panorama
- XML API

All Palo Alto Networks firewalls provide an out-of-band management port (MGT) that you can use to perform firewall administration functions. The MGT port uses the control plane, separating the management functions of the firewall from the network traffic processing functions (data plane). This separation between the control plane and data plane safeguards access to the firewall and enhances performance. When you use the web interface, you must perform all initial configuration tasks from the MGT port even if you plan to use an in-band data port for managing your firewall. A serial/console port also is available to accomplish initial configuration of the firewall using SSH or Telnet.

Some management tasks, such as retrieving licenses and updating the threat and application signatures on the firewall, require access to the internet, which typically is done via the MGT port. If you do not want to enable external access via your MGT port, you can set up an in-band data port on the data plane to provide access to required external services (using service routes). Service routes are explained in more detail in a following section.

Initial Steps to Gain Access to the Firewall

The first step to gain access to the firewall for the first time is to gather the following information for the MGT port. Note that if the firewall is set up as a DHCP client, this information will be included automatically via DHCP.

- IP address
- Netmask
- Default gateway
- At least one DNS server address

The second step is to connect a computer to the firewall using either an RJ-45 Ethernet cable or a serial cable.

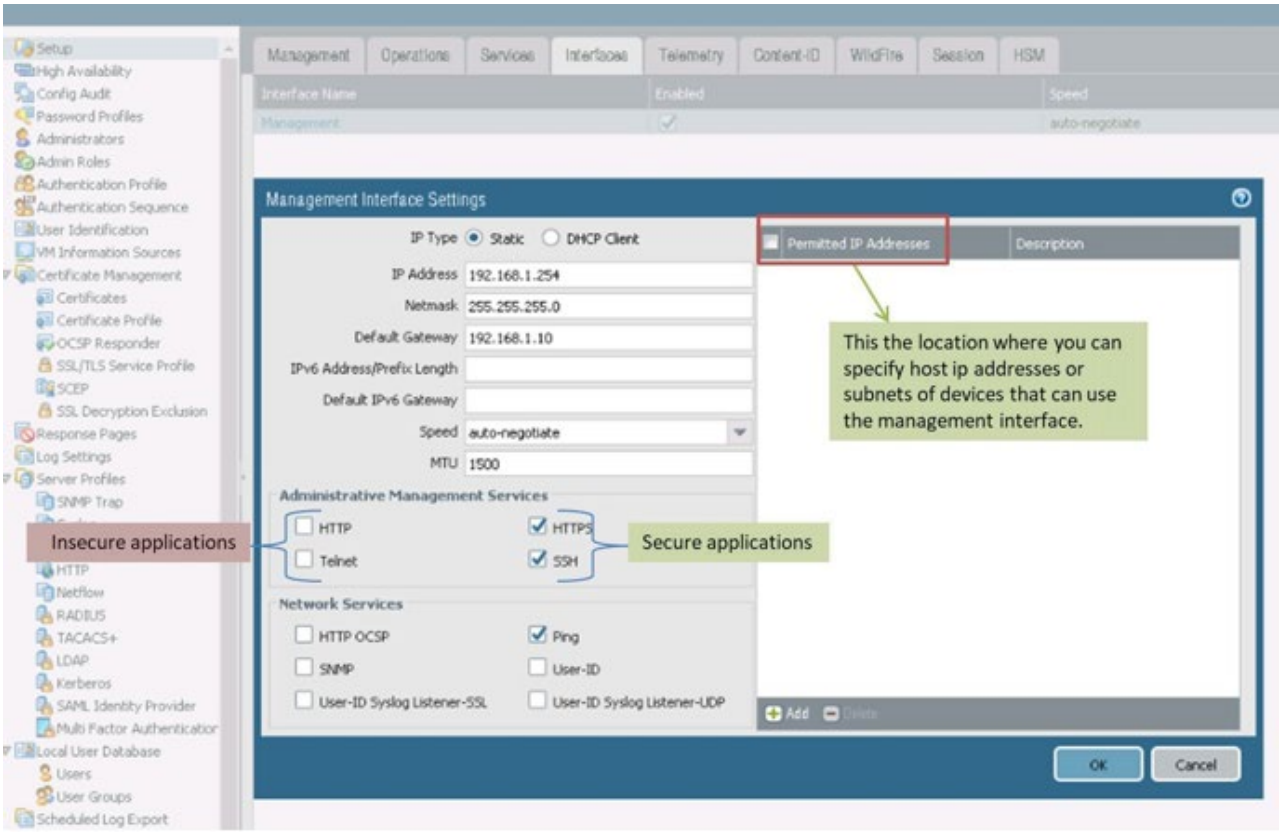
An RJ-45 Ethernet cable is connected from your computer to the firewall MGT port. From a browser, navigate to https://192.168.1.1. Note that you might need to change the IP address on your computer to an address in the 192.168.1.0/24 subnet, such as 192.168.1.2, to access this URL.

The serial cable is connected from your computer to the firewall console port using terminal emulation software such as SSH or Telnet. The default connection parameters are 9600-8-N-1.

The third step is to log in to the firewall. The default username is “admin” and the default password is “admin”. Starting with PAN-OS 9.1, you are forced to change the admin account password the first time you log in to the web interface.

Four Firewall Management Methods

Web interface: The web interface is used for configuration and monitoring over HTTP or HTTPS using a web browser. HTTPS is the default method; HTTP is available as a less secure method than HTTPS.



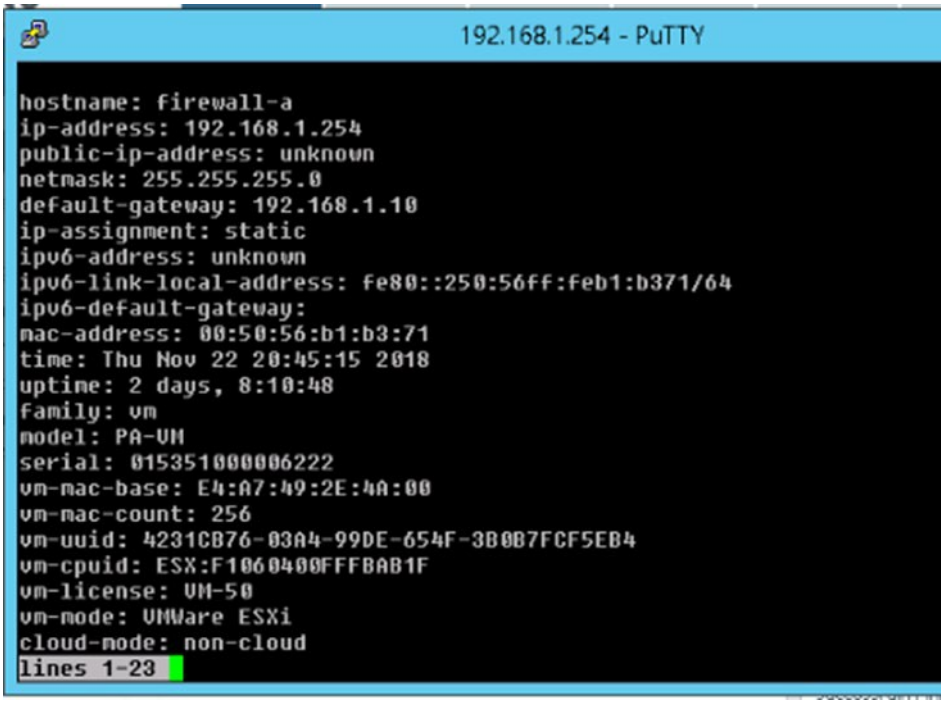
CLI: The CLI is text-based configuration and monitoring over the serial console port, or over the MGT port using Secure Shell (SSH) or Telnet. The Palo Alto Networks firewall CLI offers access to debugging information and often is used by experienced administrators for troubleshooting. The account used for authenticating into the CLI must have CLI access enabled.

The CLI command prompt will be in *operational mode* by default. The commands available within the context of operational mode include basic networking commands such as **`ping`** and **`traceroute`**, basic system commands such as **`show`**, and more advanced system commands such as **`debug`**. Commands to shut down and restart the system also are available from within operational mode.

Access configuration mode by typing the command **`configure`** while in operational mode.

Configuration mode enables you to display and modify the configuration parameters of the firewall, verify candidate configuration, and commit the config.

The following figure shows an example CLI screen with the first lines of **`show system state`** while in operational mode:



Panorama: Panorama is a Palo Alto Networks product that provides centralized web-based management, reporting, and logging for multiple firewalls. Use Panorama for centralized policy and firewall management to increase operational efficiency in managing and maintaining a distributed network of firewalls. If you have six or more firewalls deployed in your network, you should use Panorama to reduce the complexity and administrative overhead needed to manage configuration, policies, software, and dynamic content updates. The Panorama web interface is similar to the firewall web interface, but with additional management functions.

XML API: The XML API provides a representational state transfer (REST)-based interface to access firewall configurations, operational status, reports, and packet captures from the firewall. An API browser is available on the firewall at https://<firewall>/api, where <firewall> is the hostname or IP address of the firewall. You can use this API to access and manage your firewall through a third-party service, application, or script.

The PAN-OS XML API can be used to automate tasks such as:

- Create, update, and modify firewall and Panorama configurations
- Execute operational mode commands, such as restarting the system or validating configurations
- Retrieve reports
- Manage users through User-ID
- Update dynamic objects without having to modify or commit new configurations

Interface Management Profiles

Management of Palo Alto Networks firewalls is not limited to using a dedicated MGT interface or console port. Data interfaces on the data plane also can be used as management interfaces. If the MGT interface goes down, you can continue to manage the firewall by allowing management access over another data interface. Each data interface includes configurations for binding various services to them:

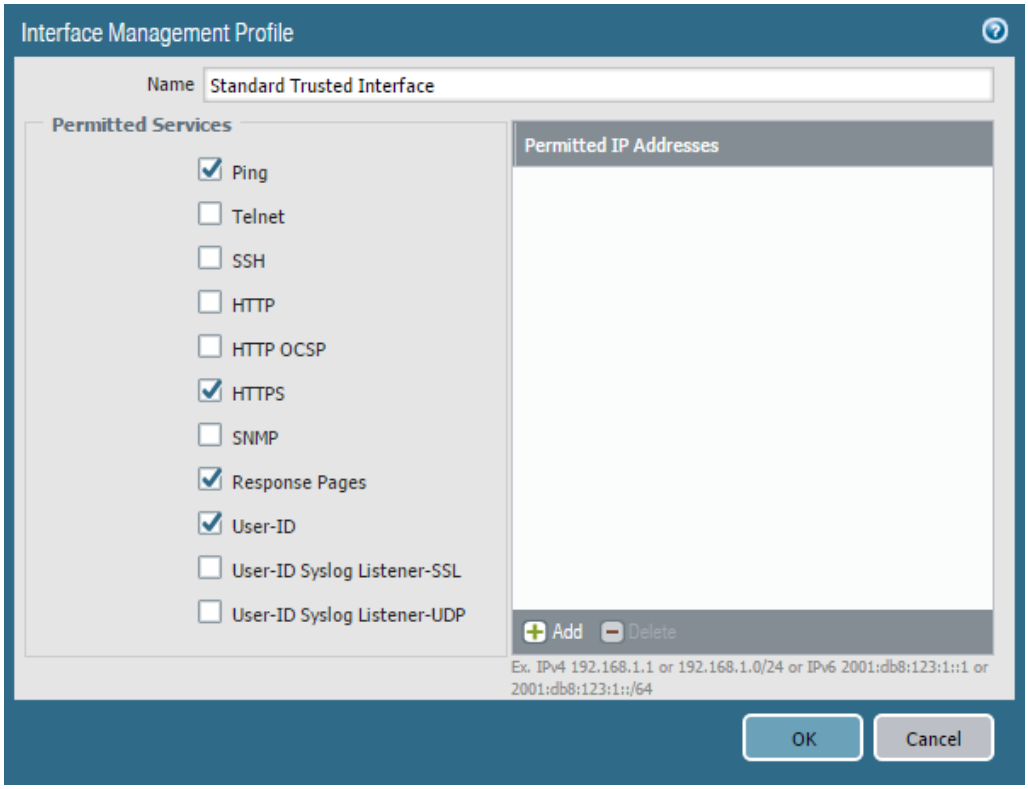
- HTTPS (default)
- SSH (default)
- Ping (default)
- Telnet
- HTTP
- SNMP
- Response Pages
- User-ID

An interface management profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that a firewall interface permits for management. For example, you might want to prevent users from accessing the firewall web interface over the ethernet1/1 interface but allow that interface to receive SNMP queries from your network monitoring system. In this case, you would enable SNMP and disable HTTP/HTTPS in an interface management profile and assign the profile to ethernet1/1.

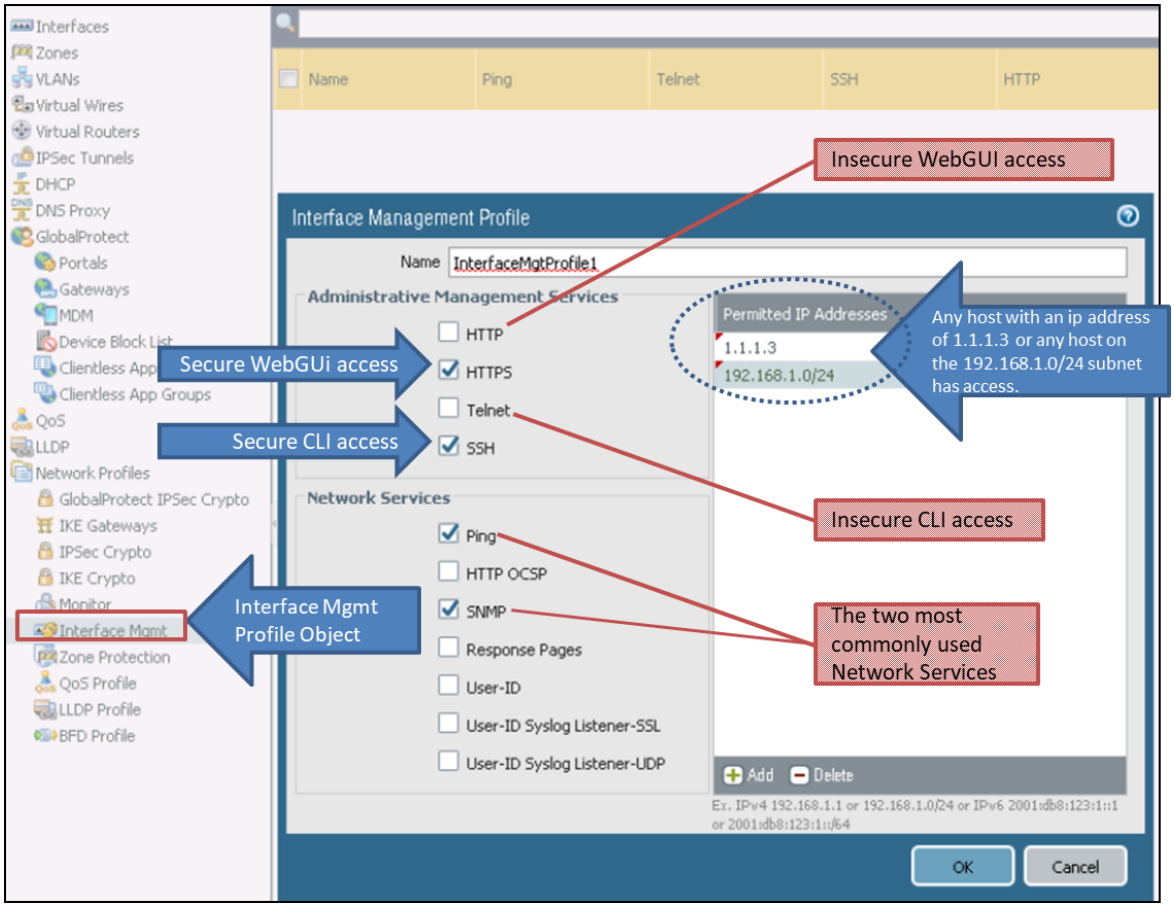
HTTPS includes the web interface service and should be included on at least one data interface. The **Permitted IP Addresses** field allows an Access Control List to be included, thus restricting access to only specified IP addresses for any interface with this profile assigned. If no IP addresses are added to the list of **Permitted IP Addresses**, then any IP address is allowed. After at least one IP address is added to the list, only those IP addresses are allowed access.

You can assign an interface management profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (aggregate group, VLAN, loopback, and tunnel interfaces). If you do not assign an interface management profile to an interface, the firewall denies management access for all IP addresses, protocols, and services by default.

Interface Management Profile Screenshot 1



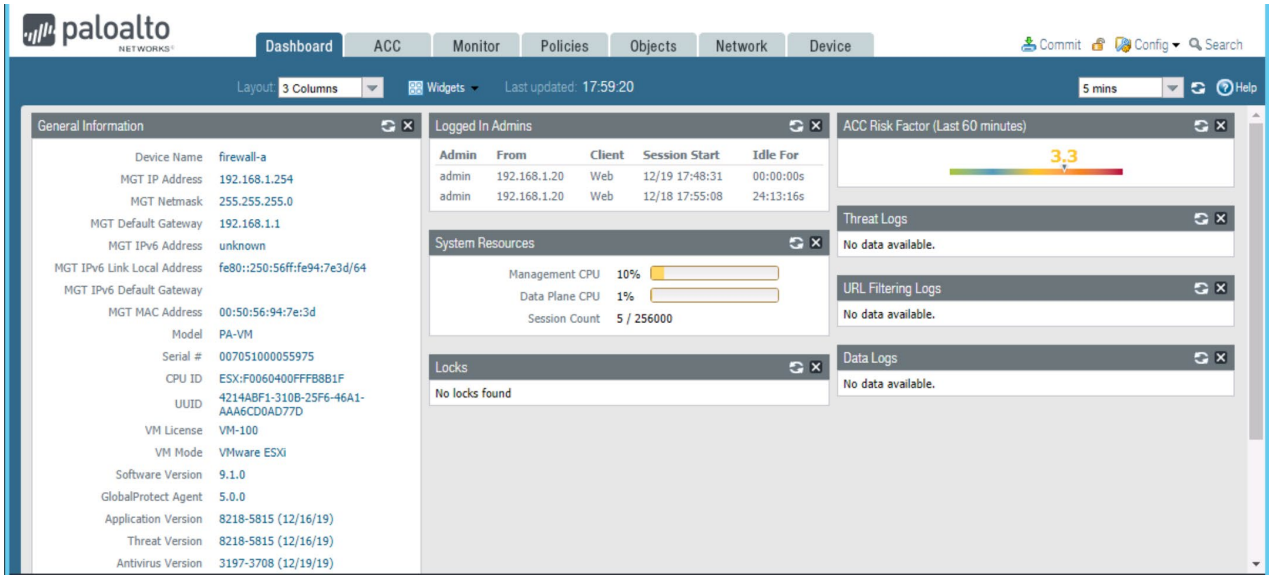
Interface Management Profile Screenshot 2



Firewall Web Interface – Dashboard

Firewall Dashboard

The firewall **Dashboard** provides information in a condensed format. It is the main screen for web interface management.



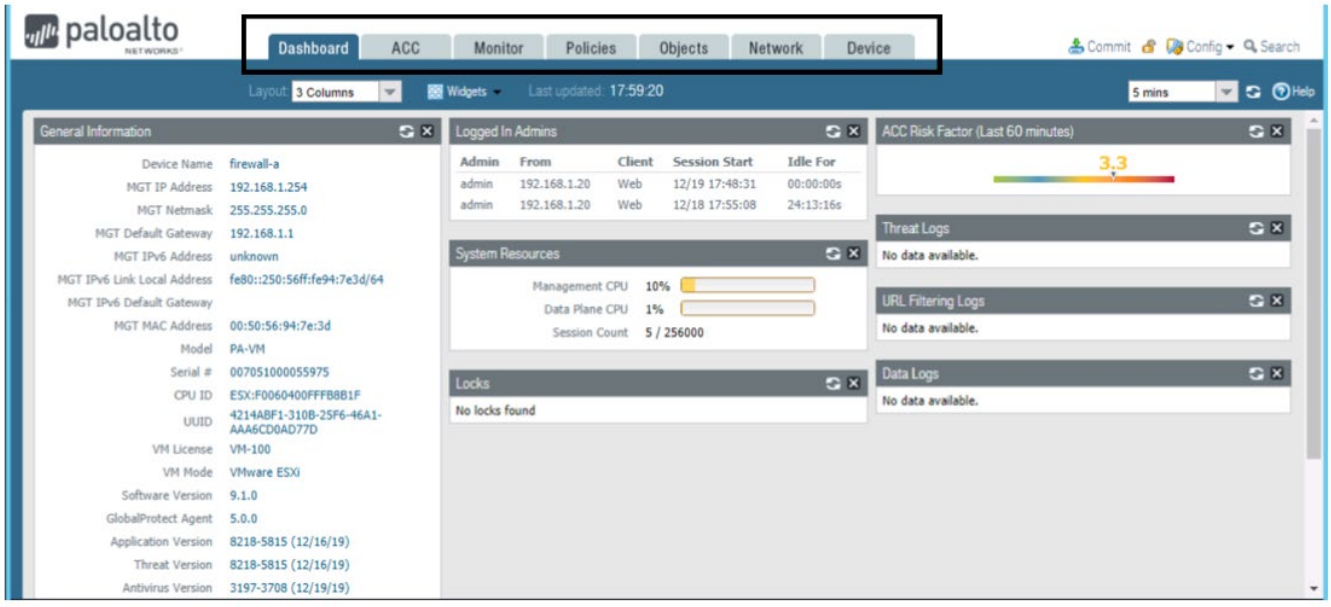
The **Dashboard** is customizable and allows you to determine which widgets to display:

- Application widgets:
  - ACC Risk Factor
  - Top Applications
  - Top High Risk Applications
- Logs widgets:
  - Config Logs
  - Data Filtering Logs
  - System Logs
  - Threat Logs
  - URL Filtering Logs
- System widgets:
  - General Information
  - High Availability
  - Interfaces
  - Locks
  - Logged In Admins
  - System Resources

Functional Category Tabs

Management of the firewall is conducted using seven category tabs, which are listed and briefly described as follows:

The Dashboard Page and Functional Categories Tabs

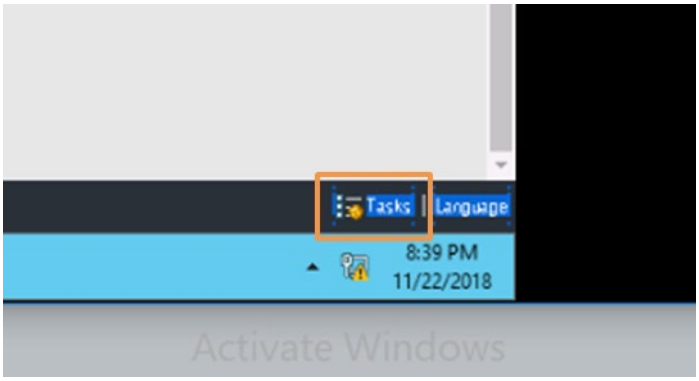


- **Dashboard**: Provides general information such as device name, MGT IP address, and licensing information. This page can be augmented by adding widgets.

- **ACC**: Uses the firewall logs to graphically depict traffic trends on your network
- **Monitor**: Provides logging visibility and the ability to run packet captures
- **Policies**: Allows the creation of policies such as security policy and NAT policy
- **Objects**: Allows the creation of objects such as Address objects
- **Network**: Allows the configuration of network parameters such as interfaces and zones
- **Device**: Allows the configuration of system information such as the hostname or certificates

Tasks Icon

The **Tasks** icon appears at the bottom right. Select it to display the tasks that you, other administrators, or the PAN-OS software has initiated since the last firewall reboot (for example, manual commits or automatic FQDN refreshes).

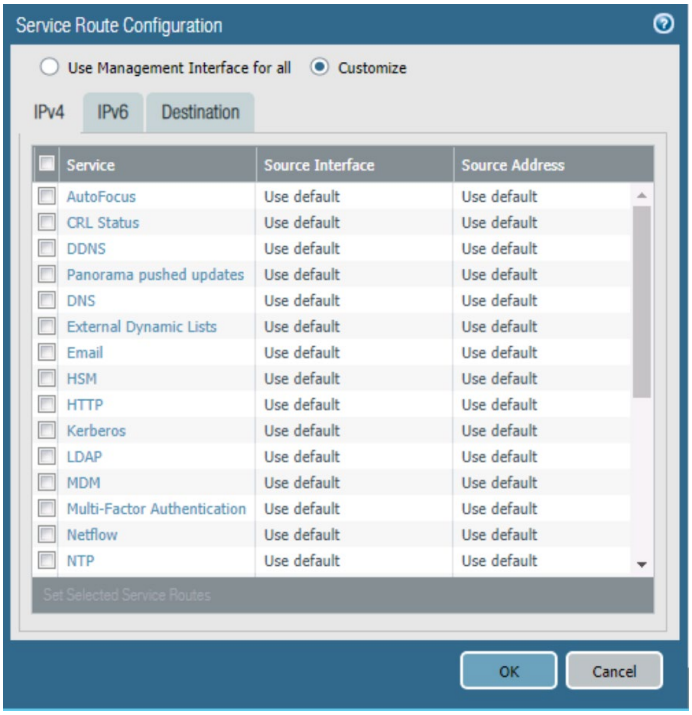


Service Routes

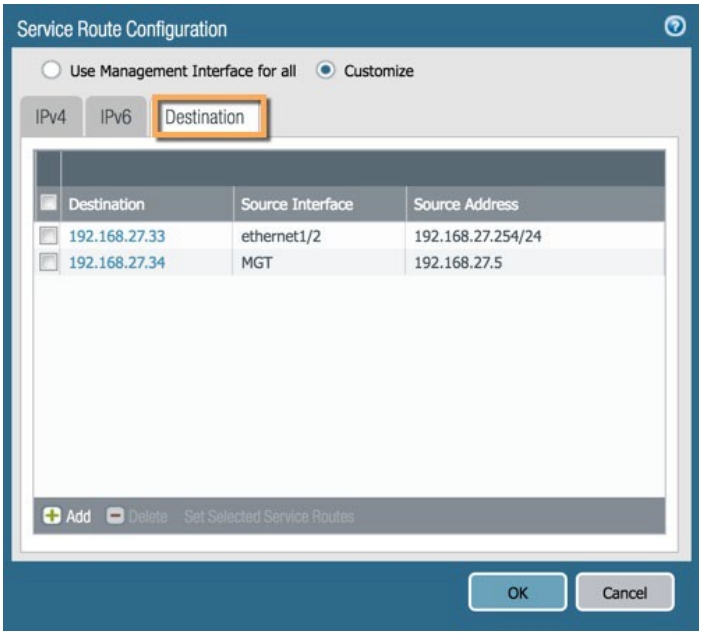
By default, the firewall uses the management interface to communicate with various servers including those for External Dynamic Lists, DNS, email, and Palo Alto Networks updates servers. The management interface also is used to communicate with Panorama. Service routes are used so that the communication between the firewall and servers goes through the data ports on the data plane. These data ports require appropriate security policy rules before external servers can be accessed.

Configuring Service Routes

Go to **Device > Setup > Services > Service Route Configuration > Customize** and configure the appropriate service routes. See the following figure:



To configure service routes for non-predefined services, you can manually enter the destination addresses on the **Destination** tab:



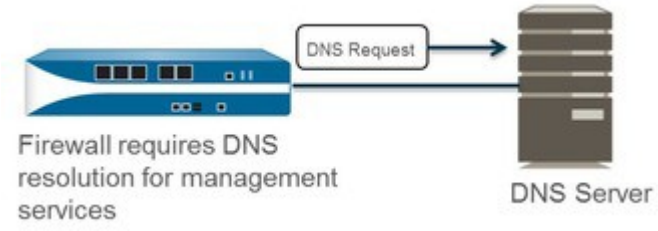
In the example shown, the service route for 192.168.27.33 is configured to source from the data plane's ethernet1/2 interface, which has a source IP address of 192.168.27.254.

Firewall Services

Palo Alto Networks firewalls integrate with three important services: DNS, DHCP, and NTP.

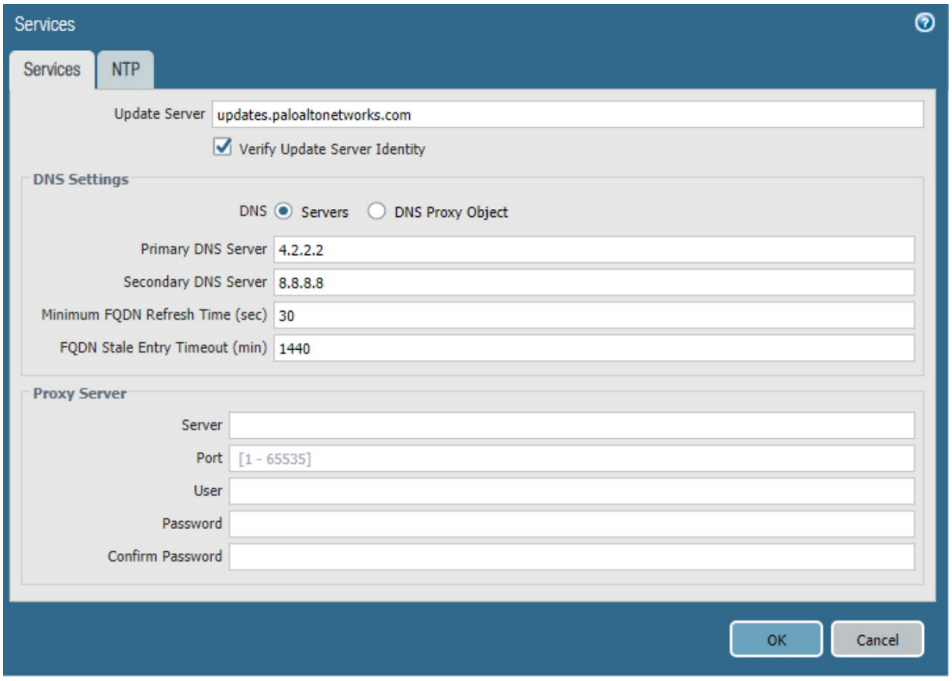
DNS

Domain Name System (DNS) is a protocol that translates (resolves) a user-friendly domain name such as www.paloaltonetworks.com to an IP address so that users can access computers, websites, services, or other resources on the internet or private networks. You must configure your firewall with at least one DNS server so it can resolve hostnames.



Configuring DNS

To configure DNS, select **Device > Setup > Services > Services_gear_icon**. On the **Services** tab, for DNS, click **Servers** and enter the **Primary DNS Server** address and **Secondary DNS Server** address. Click **OK** and **Commit**.



DHCP

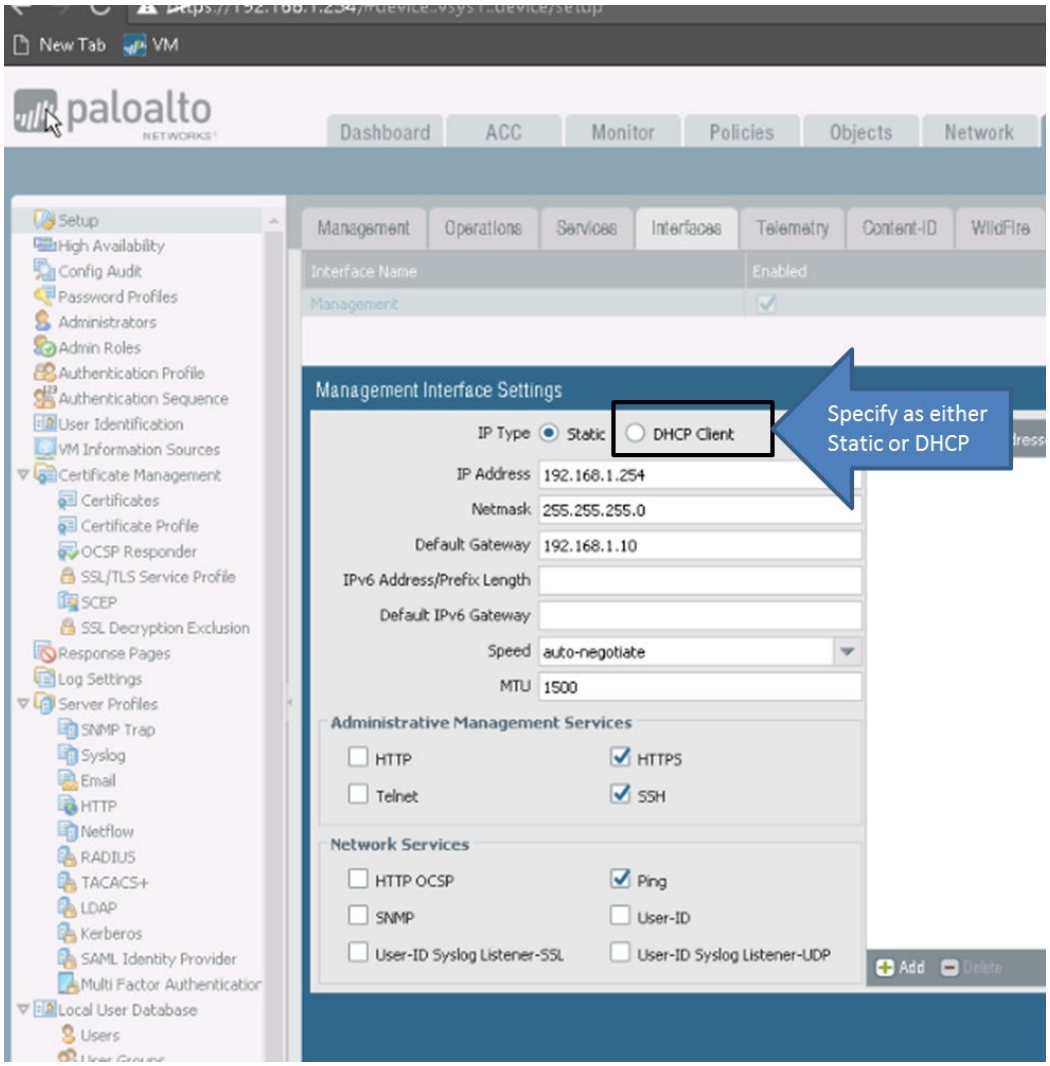
A Palo Alto Networks firewall acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. The use of DHCP saves time and effort because users need not know the network's addressing plan or other options, such as default gateway, they are inheriting from the DHCP server.

Some configuration parameters that DHCP can learn dynamically include:

- IP address for MGT port
- Netmask
- Default gateway

- At least one DNS server address

Management Interface DCHP Client Option

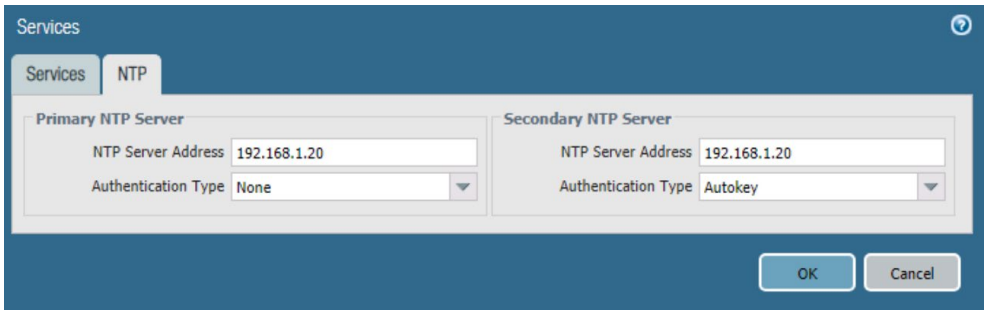


NTP

NTP client information is optional. The NTP information can be obtained via DHCP if the firewall is configured as a DHCP client.

Configuring NTP

Select **Device > Setup > Services > Services_gear_icon**.



Sample questions

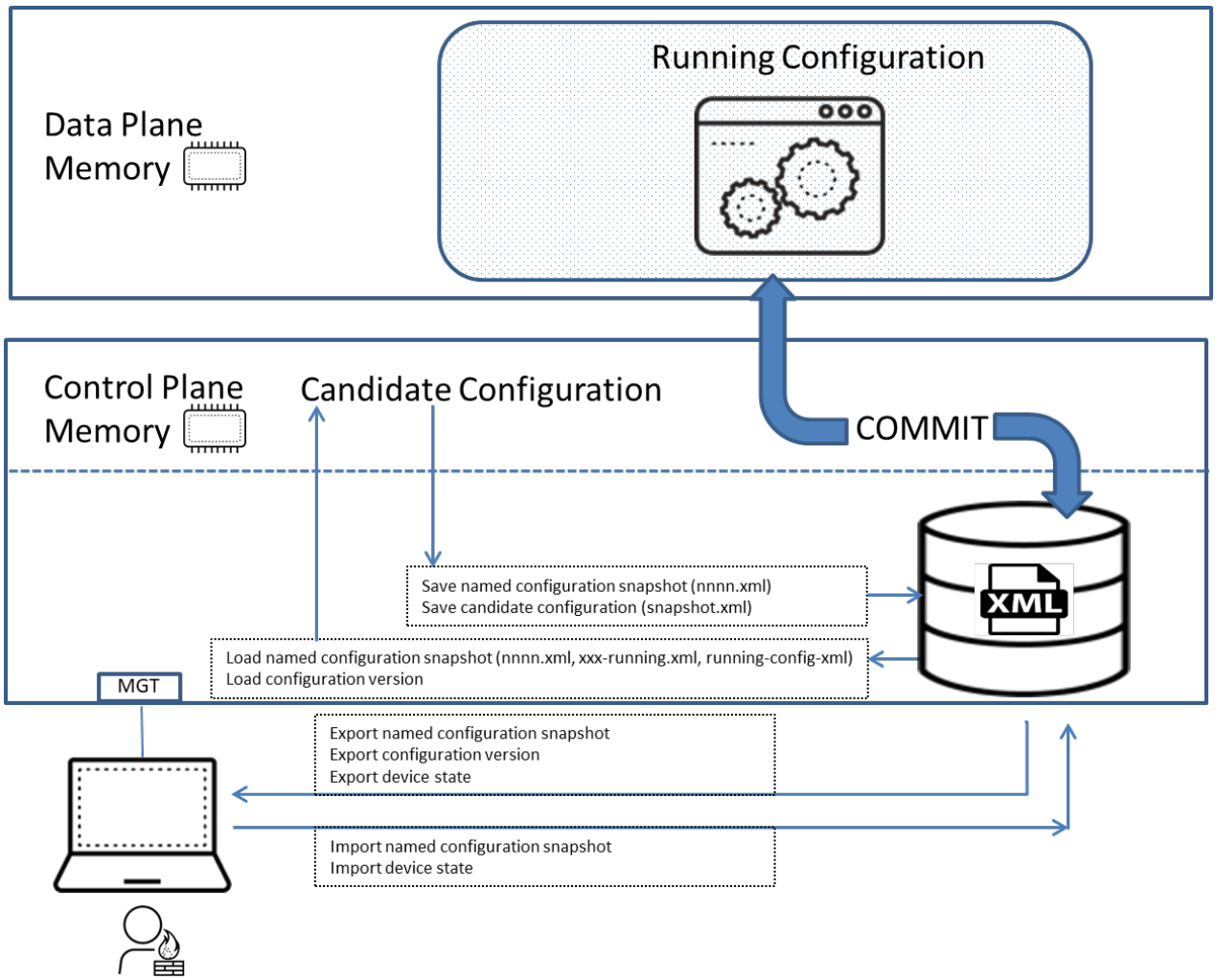
21. What are two firewall management methods? (Choose two.)
    A. CLI
    B. RDP
    C. VPN
    D. XML API
22. Which two devices are used to connect a computer to the firewall for management purposes? (Choose two.)
    A. rollover cable
    B. serial cable
    C. RJ-45 Ethernet cable
    D. USB cable
23. What is the default IP address on the MGT interfaces of a Palo Alto Networks firewall?
    A. 192.168.1.1
    B. 192.168.1.254
    C. 10.0.0.1
    D. 10.0.0.254
24. What are the two default services that are available on the MGT interface? (Choose two.)
    A. HTTPS
    B. SSH
    C. HTTP
    D. Telnet
25. True or false. Service route traffic has Security policy rules applied against it.
    A. true
    B. false
26. Service routes may be used to forward which two traffic types out a data port? Choose two.)
    A. External Dynamic Lists
    B. MineMeld
    C. Skype
    D. Palo Alto Networks updates

Exam Domain 2 – Simply Passing Traffic

2.2 Identify how to manage firewall configurations.

Manage Configurations Using Candidate and Running Configurations

All configuration changes in a Palo Alto Networks firewall are done to a *candidate configuration*, which resides in memory on the control plane. A commit activates the changes since the last commit and installs the running configuration on the data plane, where it will become the *running configuration*.



Candidate Configuration

The act of saving your changes to the candidate configuration does not activate those changes. A commit must be performed on the firewall to activate the changes and to cause the candidate configuration to become the running configuration. The commit can be done either via the web interface or the CLI.

The candidate configuration can be saved as either a default snapshot file (snapshot.xml) or as a custom-named snapshot file (<custom_name>.xml). However, a firewall does not automatically save the candidate configuration to persistent storage; you must manually save the candidate configuration. If the firewall reboots before you commit your changes, you can revert the candidate configuration to the current snapshot to restore changes you made between the last commit and the last snapshot, using the **Revert to last saved configuration** option.

Running Configuration

The running configuration is a configuration that is saved within a file named running-config.xml. The running configuration exists in data plane memory, where it is used to control firewall traffic and operate the firewall. A commit operation is necessary to write the candidate configuration to the running configuration.

After you commit changes, the firewall automatically saves a new *version* of the running configuration that is timestamped. You can load a previous version of the running-configuration using the **Load**

configuration version option. The firewall queues commit requests so that you can initiate a new commit while a previous commit is in progress. The firewall performs the commits in the order they are initiated but prioritizes commits that the firewall initiates automatically, such as FQDN refreshes.

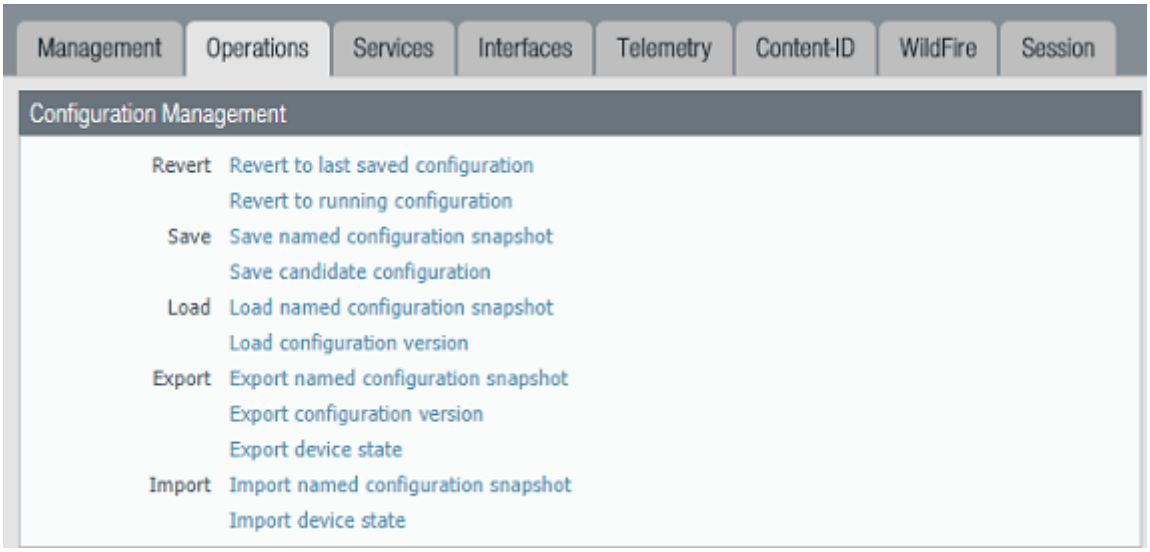
If a system event or administrator action causes a firewall to reboot, the firewall automatically reverts to the current version of the running configuration.

Manage Running and Candidate Configurations

Palo Alto Networks firewall configurations are managed using five categories, which are found under

Device > Setup > Operations and are described in the next sections:

- **Revert**
- **Save**
- **Load**
- **Export**
- **Import**

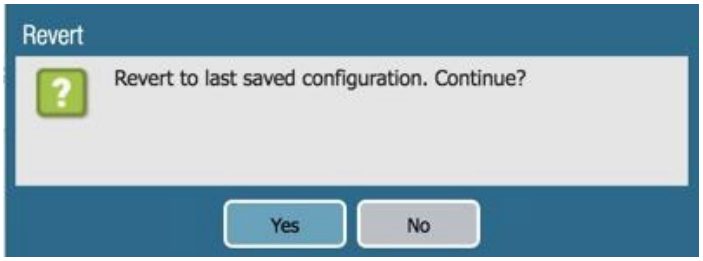


As a best practice, periodically save candidate configurations.

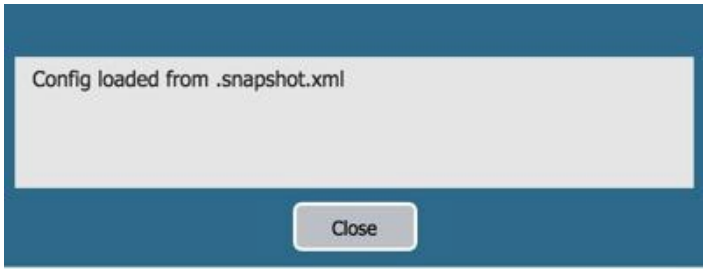
Revert to Last Saved Configuration

This option restores the default snapshot (snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click **Device > Setup > Operations > Save candidate configuration** or **Save** at the top right of the web interface). This option restores the last saved candidate configuration from the local drive. The current candidate configuration is overwritten. This quick restore is useful when you work on “hot” boxes.

The first message asks if you want to continue with the restore:



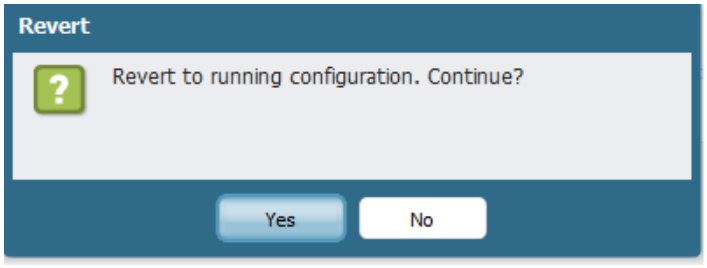
The second message informs you which file has been restored:



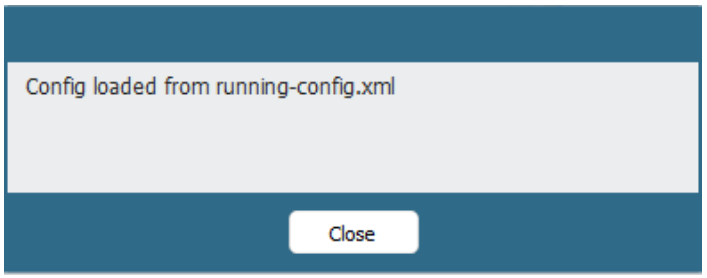
Revert to Running Configuration

This option restores the current running configuration. This operation undoes all the changes you made to the candidate configuration since the last commit and restores the config from the running-config.xml file.

The first message asks if you want to continue with the revert:

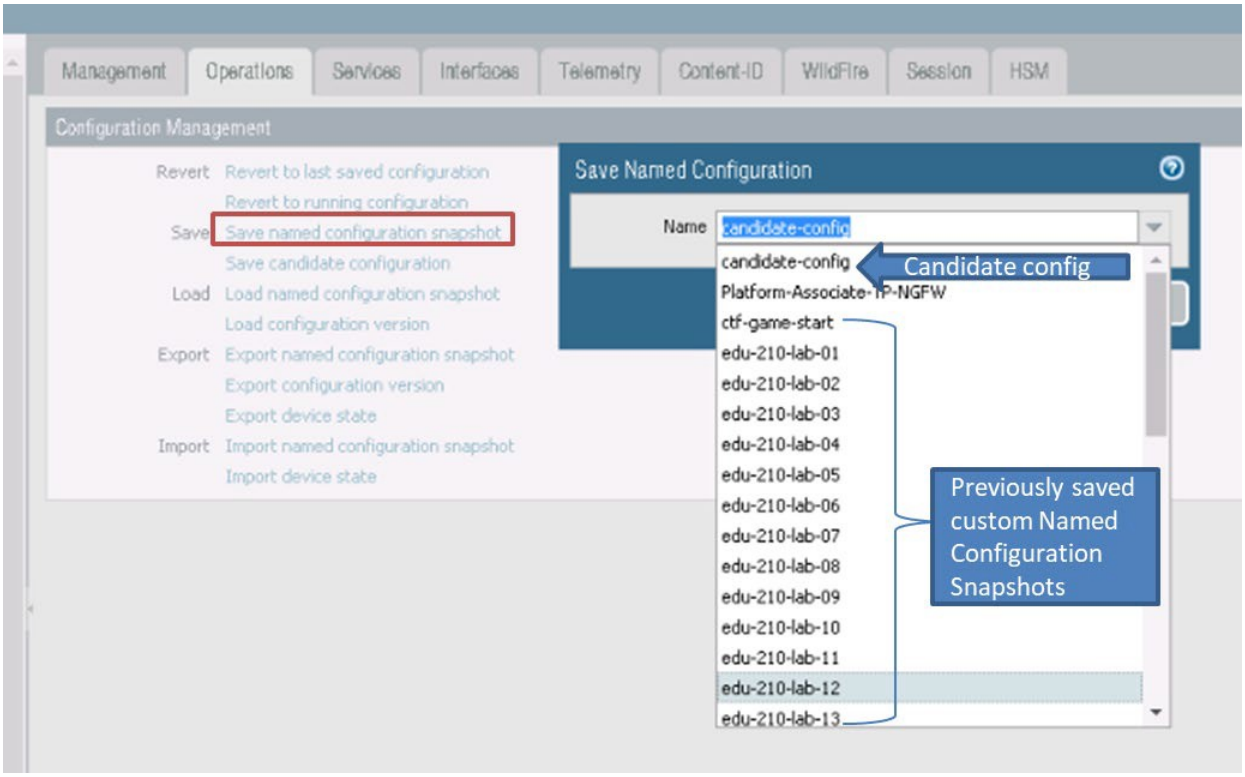


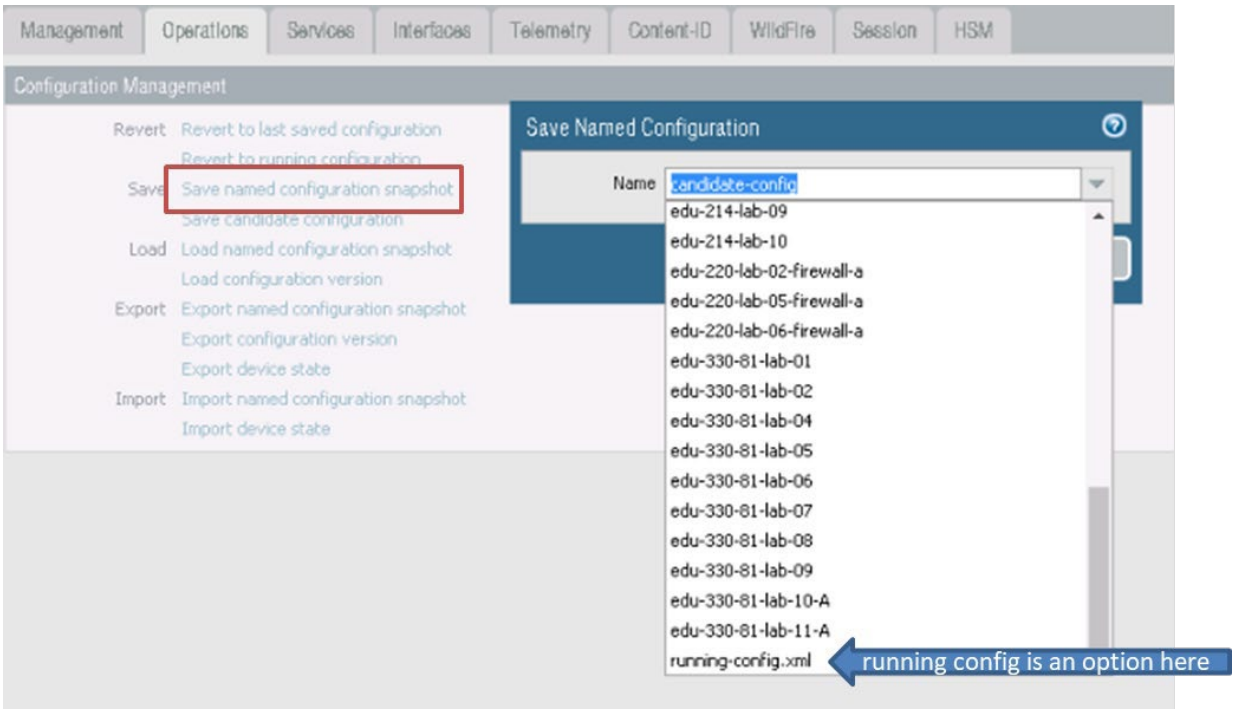
The second message informs you which file has been restored.



Save Named Configuration Snapshot

This option creates a candidate configuration snapshot that does not overwrite the default snapshot (snapshot.xml). Enter a custom name for the snapshot or select an existing snapshot to overwrite. This function is useful when you create a backup file or a test configuration file that could be downloaded for a further modification or testing in the lab environment.





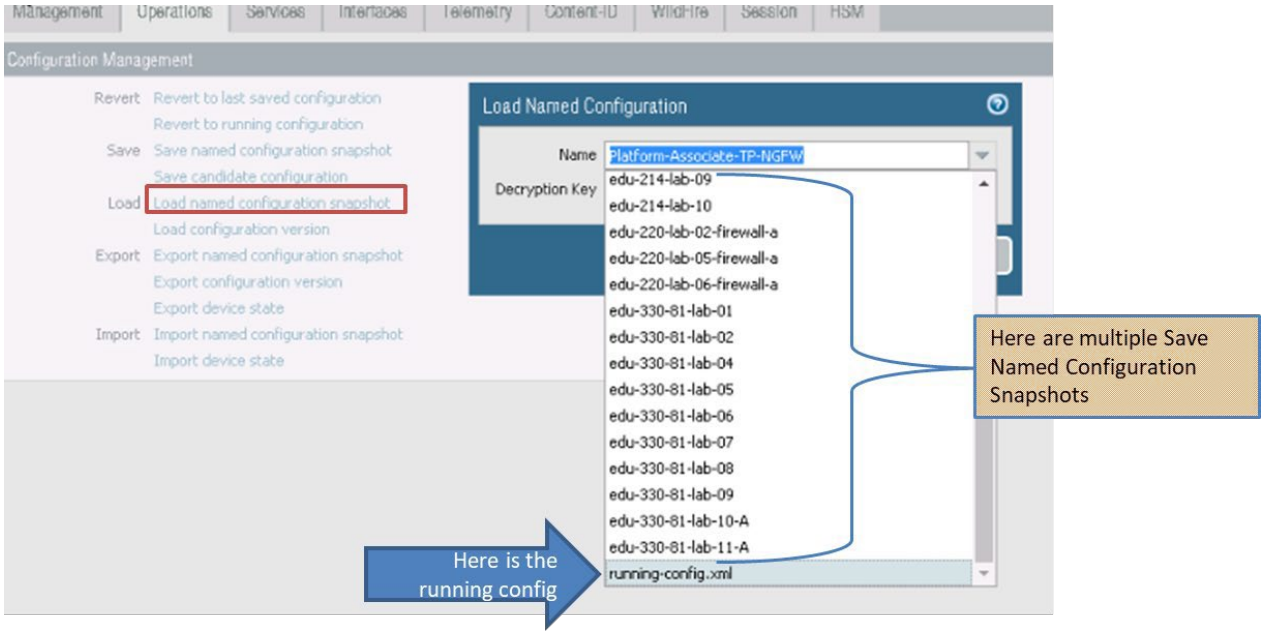
Save Candidate Configuration

This option creates or overwrites the default snapshot (snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click **Device > Setup > Operations > Save candidate configuration** or **Save** at the top right of the web interface).

Load Named Configuration Snapshot

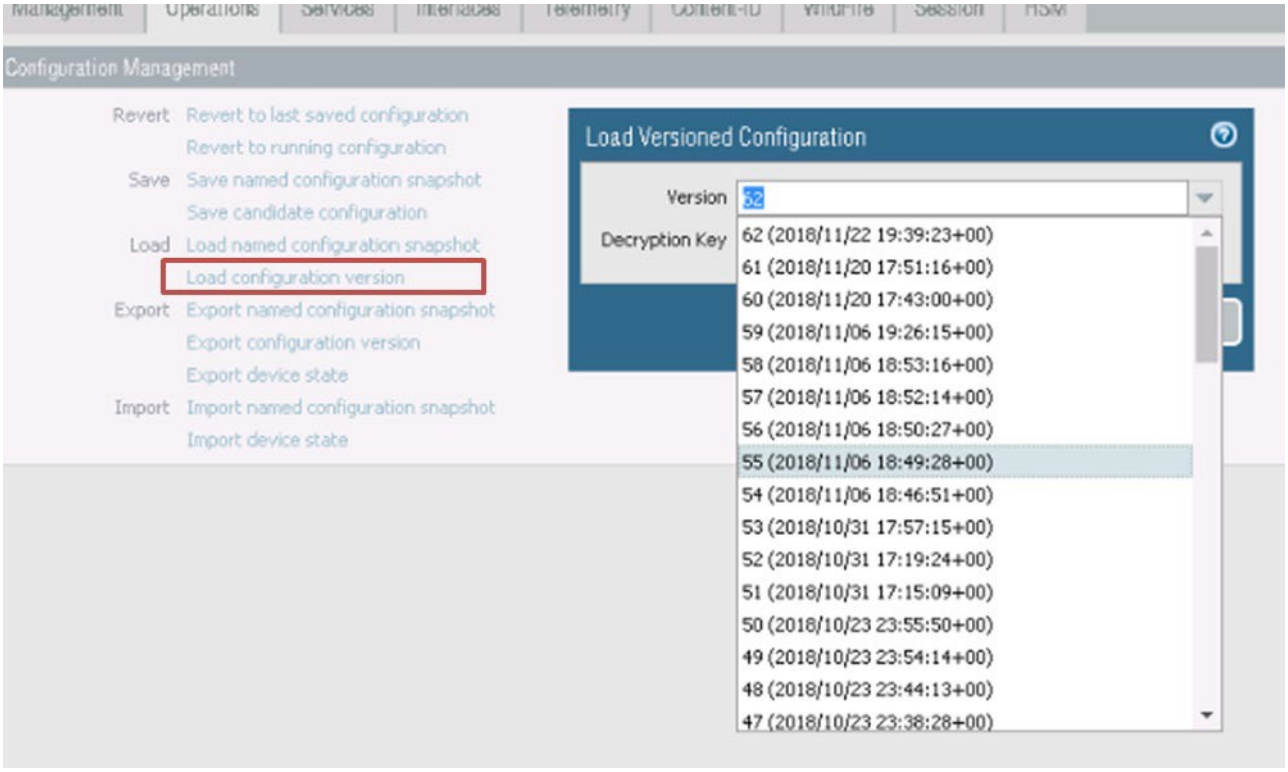
This option overwrites the current candidate configuration with one of the following:

- Custom-named candidate configuration snapshot (instead of the default snapshot)
- Custom-named running configuration that you imported
- Current running configuration (running-config.xml)



Load Configuration Version

This option overwrites the current candidate configuration with a previous version of the running configuration that is stored on the firewall. The firewall creates a timestamped version of the running configuration whenever a commit is made.



Export Named Configuration Snapshot

This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

Export Configuration Version

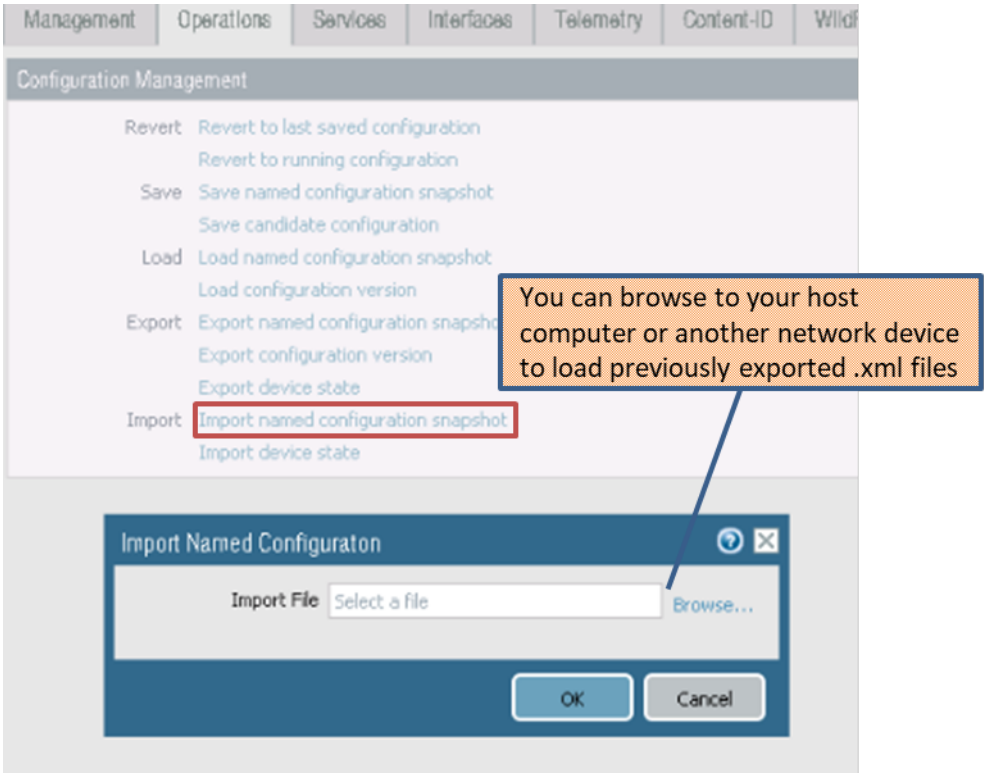
This option exports a version of the running configuration as an XML file.

Export Device State

This option exports the firewall state information as a file. In addition to the running configuration, the state information includes device group and template settings pushed from Panorama, if applicable. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites that the portal manages, and satellite authentication information. If you replace a firewall or portal, you can restore the exported information on the replacement by importing the state bundle.

Import Named Configuration Snapshot

This option imports a running or candidate configuration as an XML file from any network location such as a host computer. Click **Browse** and select the configuration file to be imported. The XML file then can be loaded as a candidate configuration and even ultimately loaded as the running configuration if required.



Import Device State

This option imports the state information file that you exported from a firewall using the **Export device state** option. The state information includes the running configuration and device group and template settings pushed from Panorama, if applicable. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites, and satellite authentication information. If you replace a firewall or portal, you can restore the information on the replacement by importing the state bundle.

Sample questions

27. Which firewall plane does the running configuration reside on?
    A. management
    B. control
    C. data
    D. security
28. Which firewall plane does the candidate configuration reside on?
    A. management
    B. control
    C. data
    D. security
29. Candidate config and running config files are saved as which file type?
    A. TXT
    B. HTML
    C. XML
    D. RAR

30. Which command must be performed on the firewall to activate any changes?
    A. commit
    B. save
    C. load
    D. save named
    E. import
    F. copy
31. Which command backs up configuration files to a remote network device?
    A. import
    B. load
    C. copy
    D. export
32. The command **`load named configuration snapshot`** overwrites the current candidate configuration with which three items? (Choose three.)
    A. custom-named candidate configuration snapshot (instead of the default snapshot)
    B. custom-named running configuration that you imported
    C. snapshot.xml
    D. current running configuration (running-config.xml)
    E. Palo Alto Networks updates

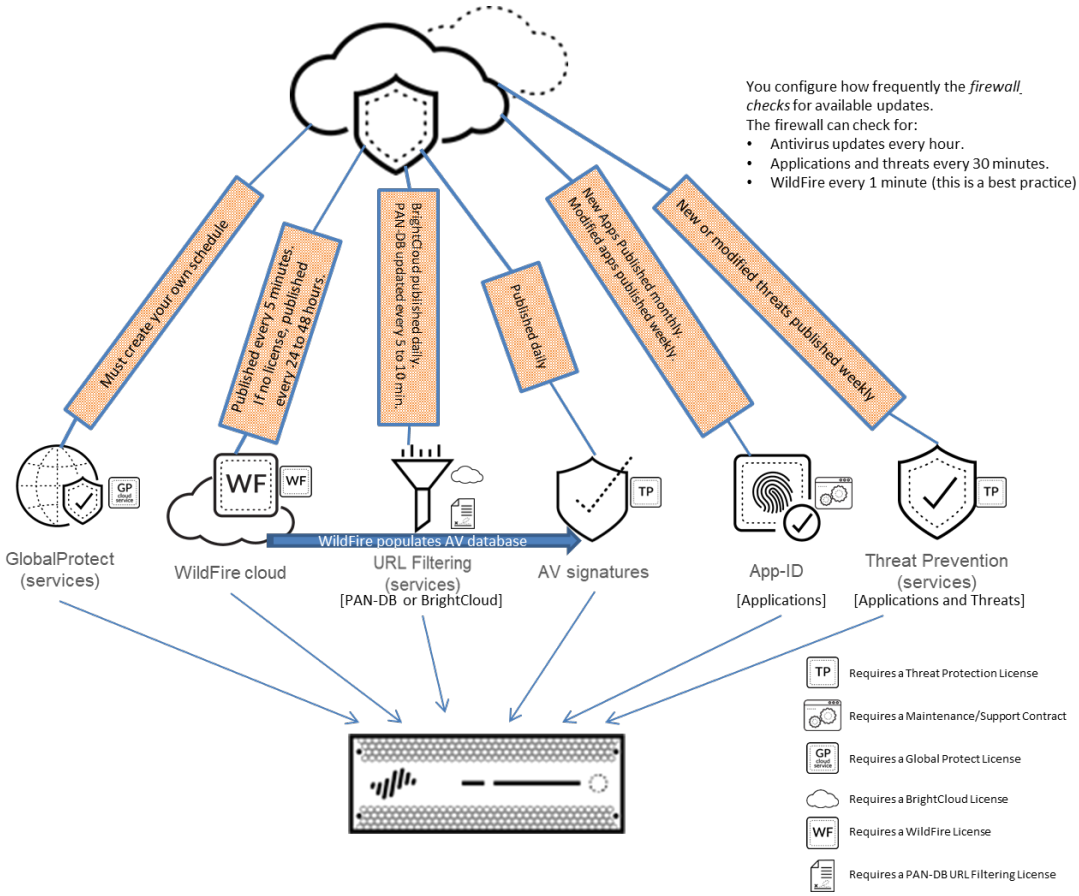
Exam Domain 2 – Simply Passing Traffic

2.3 Identify and schedule dynamic updates.

Dynamic Updates

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. Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates.

The following diagram illustrates how often updated information is made available to the firewall. Note that BrightCloud subscriptions are no longer being sold as of Feb 01, 2018. All deployments sold after Feb 01, 2018 use the PAN-DB database to perform URL filtering. Support for BrightCloud deployments will end on Jul 31, 2021.



The following content updates are available, depending on which subscriptions you have:

- **Antivirus:** Includes new and updated antivirus signatures, including WildFire signatures and automatically-generated command-and-control (C2) signatures. WildFire signatures detect malware seen first by firewalls from around the world. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.
- **Applications:** Includes new and updated application signatures. This update does not require any additional subscriptions, but it does require a valid maintenance support contract. New applications are published monthly, and modified applications are published weekly. To best deploy application updates to ensure application availability, be sure to follow the Best Practices for Application and Threat Content Updates.
- **Applications and Threats:** Includes new and updated application and threat signatures, including those that detect spyware and vulnerabilities. This update is available if you have a Threat Prevention subscription (and you get it instead of the Applications update). New and modified threat signatures and modified applications signatures are published weekly; new application signatures are published monthly. The firewall can retrieve the latest update within 30 minutes of availability. To best deploy application and threat updates based on your security and application availability needs, be sure to follow the Best Practices for Application and Threat Content Updates.
- **GlobalProtect Data File:** Contains vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect clients. You

must have a GlobalProtect license (subscription) and create an update schedule to receive these updates.

- **GlobalProtect Clientless VPN:** Contains new and updated application signatures to enable clientless VPN access to common web applications from the GlobalProtect portal. You must have a GlobalProtect license (subscription) and create an update schedule to receive these updates and enable clientless VPN to function.
- **Palo Alto Networks (PAN-DB) URL filtering:** Complements App-ID by enabling you to configure the firewall to identify and control access to web (HTTP and HTTPS) traffic and to protect your network from attack. If URL filtering is enabled, all web traffic is compared against the URL filtering database, which contains a listing of millions of websites that have been categorized into 60 to 80 categories.

Although the Palo Alto Networks URL filtering solution supports both BrightCloud and PAN-DB, only the PAN-DB URL filtering solution allows you to choose between the PAN-DB Public Cloud and the PAN-DB Private Cloud. Use the public cloud solution if the Palo Alto Networks next-generation firewalls on your network can directly access the internet. If the network security requirements in your enterprise prohibit the firewalls from directly accessing the internet, you can deploy a PAN-DB private cloud on one or more M-500 appliances that function as PAN-DB servers within your network. PAN-DB URL filtering requires a PAN-DB URL Filtering license.

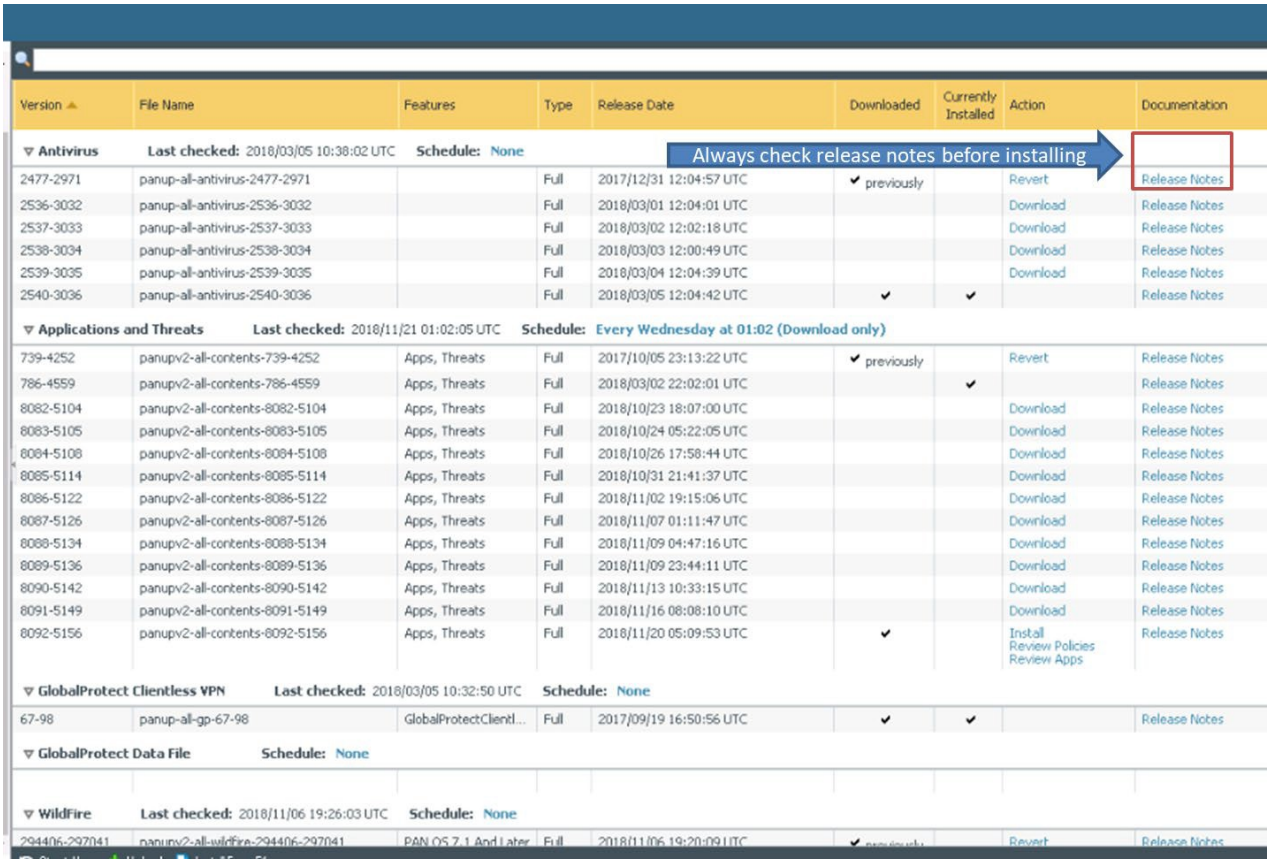
Every 5 to 10 minutes a new version is published that contains updated categorization data and an incremented version number. Each time the Palo Alto Networks firewall sends a request to the cloud, it checks the current version number. If the number is different, the firewall upgrades the device's version to the current cloud version. The primary purpose of the frequency of updates is to leverage native integration with WildFire, which creates new signatures and records malicious URLs every 5 minutes.

- **BrightCloud URL Filtering**: Provides updates to the BrightCloud URL filtering database only. You must have a BrightCloud subscription to get these updates. New BrightCloud URL database updates are published daily. End-of-sale was 01/01/2018 and end-of-support is 07-01-2021.
- **WildFire:** Available with a WildFire subscription, this update provides near-real-time malware and antivirus signatures created as a result of the analysis done by the WildFire cloud service. As a best practice, schedule the firewall to retrieve any WildFire updates every minute). If you have a Threat Prevention subscription and not a WildFire subscription, you must wait 24 to 48 hours for the WildFire signatures to be added into the antivirus update.
- **WF-Private:** Provides malware signatures generated by an on-premises WildFire appliance.

Downloading and Installing Updates

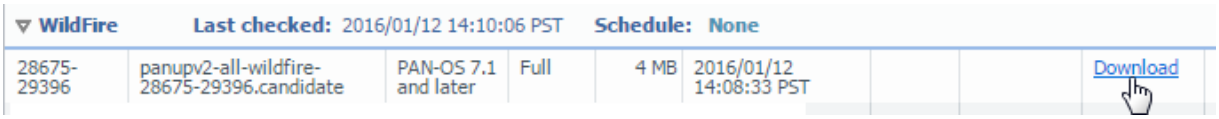
You can view the latest updates, read the release notes for each update, and then select the update you want to download and install. You also can revert to a previously installed version of an update.

Always review content Release Notes for the list of the newly identified and modified applications and threat signatures that the content release introduces.



You can download updates directly from the Palo Alto Networks update server. You also can download the updates to another system such as a user desktop or a Panorama management appliance and then upload them to the firewall. Whether you download an update through the web or upload an update from Panorama, the update will appear in the list of available updates at **Device > Dynamic Updates**. Click **Install** to install the updates.

Downloading Updates



Installing Updates

Software Updates

PAN-OS updates are managed in the **Device > Software** section of the web interface. 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.

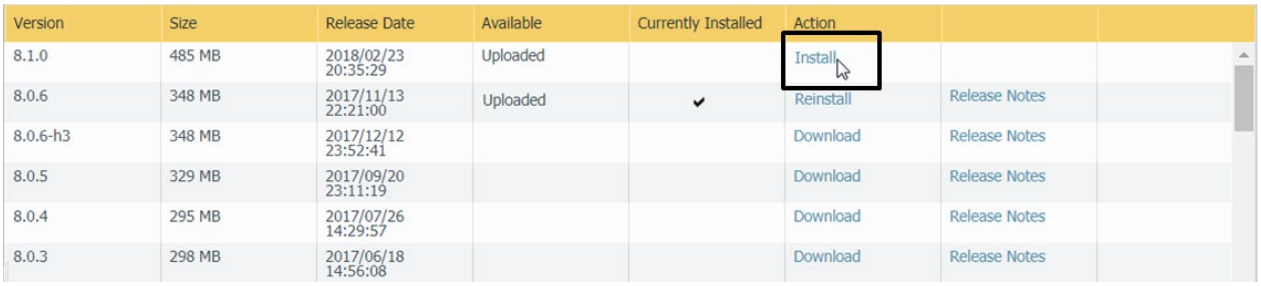
The software downloads are done over the MGT interface by default. A data interface can be used to download the software using a service route. The latest version of applications and threats must be installed to complete the software installation. If your firewall does not have internet access from the management port, you can download the software image from the Palo Alto Networks Customer Support Portal and then manually **Upload** it to your firewall.

Before you upgrade to a newer version of software:

- Always review the release notes to determine any impact of upgrading to a newer version of software.
- Ensure the firewall is connected to a reliable power source. A loss of power during an upgrade can make the firewall unusable.
- Although the firewall automatically creates a configuration backup, a best practice is to create and externally store a backup before you upgrade.

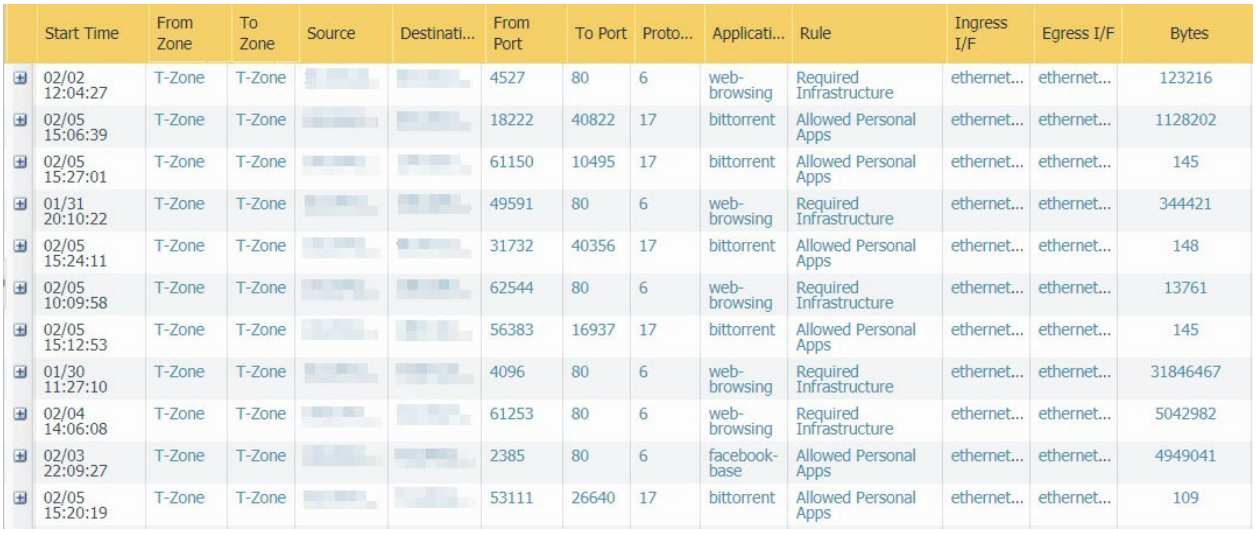
To upgrade to a newer version of software, complete the following steps:

1. Ensure you follow the correct upgrade path. When you upgrade, typically you must download the *x*.0 base release before you install the maintenance or feature release. For example, to upgrade from 7.*x*.*y* to 8.*x*.*y*, download both 8.0 and 8.*x*.*y*. 8.0 automatically is installed when you install 8.*x*.*y*.
2. Select **Device Software** and click **Check Now** to display the latest PAN-OS updates.
3. Locate and **Download** the applicable PAN-OS software
4. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.



Version	Size	Release Date	Available	Currently Installed	Action		
8.1.0	485 MB	2018/02/23 20:35:29	Uploaded		Install		
8.0.6	348 MB	2017/11/13 22:21:00	Uploaded	✔	Reinstall	Release Notes	
8.0.6-h3	348 MB	2017/12/12 23:52:41			Download	Release Notes	
8.0.5	329 MB	2017/09/20 23:11:19			Download	Release Notes	
8.0.4	295 MB	2017/07/26 14:29:57			Download	Release Notes	
8.0.3	298 MB	2017/06/18 14:56:08			Download	Release Notes	

5. After the installation completes successfully, reboot the firewall.
6. Verify that the firewall is passing traffic. Select **Monitor > Session Browser** and verify that you are seeing new sessions:



	Start Time	From Zone	To Zone	Source	Destinati...	From Port	To Port	Proto...	Applicati...	Rule	Ingress I/F	Egress I/F	Bytes
⊞	02/02 12:04:27	T-Zone	T-Zone			4527	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	123216
⊞	02/05 15:06:39	T-Zone	T-Zone			18222	40822	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	1128202
⊞	02/05 15:27:01	T-Zone	T-Zone			61150	10495	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	145
⊞	01/31 20:10:22	T-Zone	T-Zone			49591	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	344421
⊞	02/05 15:24:11	T-Zone	T-Zone			31732	40356	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	148
⊞	02/05 10:09:58	T-Zone	T-Zone			62544	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	13761
⊞	02/05 15:12:53	T-Zone	T-Zone			56383	16937	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	145
⊞	01/30 11:27:10	T-Zone	T-Zone			4096	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	31846467
⊞	02/04 14:06:08	T-Zone	T-Zone			61253	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	5042982
⊞	02/03 22:09:27	T-Zone	T-Zone			2385	80	6	facebook-base	Allowed Personal Apps	ethernet...	ethernet...	4949041
⊞	02/05 15:20:19	T-Zone	T-Zone			53111	26640	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	109

Sample questions

33. What is the shortest time interval that you can configure a Palo Alto Networks firewall to download WildFire updates?

    A. 1 minute
    B. 5 minutes
    C. 15 minutes
    D. 60 minutes

34. What is the publishing interval for WildFire updates, with a valid WildFire license?

    A. 1 minute
    B. 5 minutes
    C. 15 minutes
    D. 60 minutes

35. True or false. A Palo Alto Networks firewall automatically provides a backup of the configuration during a software upgrade.

    A. true
    B. false

36. If you have a Threat Prevention subscription but *not* a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

    A. 1 to 2 hours
    B. 2 to 4 hours
    C. 10 to 12 hours
    D. 12 to 48 hours

37. Which three actions should you complete before you upgrade to a newer version of software? (Choose three.)

    A. Review the release notes to determine any impact of upgrading to a newer version of software.
    B. Ensure the firewall is connected to a reliable power source.
    C. Export the device state.
    D. Create and externally store a backup before you upgrade.

38. What are five ways to download software? (Choose five.)

    A. over the MGT interface on the control plane
    B. over a data interface on the data plane
    C. upload from a computer
    D. from the Palo Alto Networks Customer Support Portal
    E. from the PAN-DB database
    F. from Panorama

Exam Domain 2 – Simply Passing Traffic

2.4 Configure internal and external services for account administration.

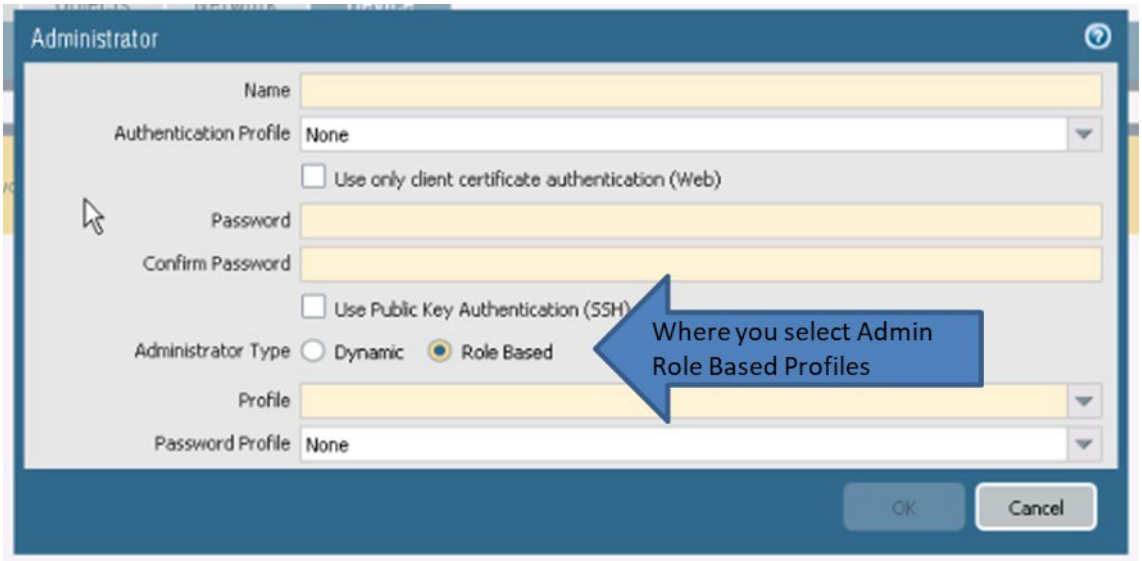
Administrator accounts control access to firewalls. By default, Palo Alto Networks firewalls have a predefined, default local admin account that has full access. Administrator accounts can be either local (internal) or non-local (external). Additional local or external administrator accounts can be created with customized administrative privileges by assigning them to **Role Based** admin role profiles, or you can assign administrator accounts to built-in account types using **Dynamic** admin roles.

Administrative Role Types

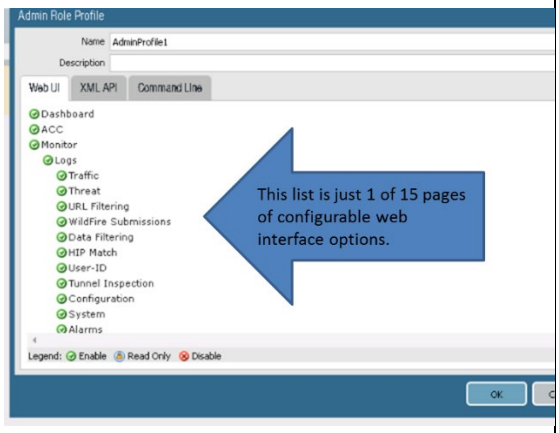
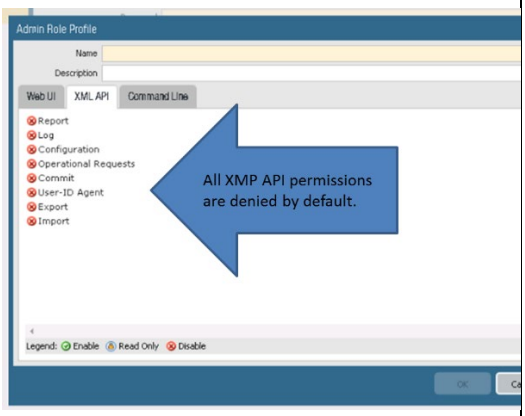
A *role* defines the type of access that an administrator has to the firewall. The two role types are **Role Based** profile roles and **Dynamic** roles:

- **Role Based** profile roles: These are custom roles you can configure for more granular access control over the functional areas of the web interface, CLI, and XML API. For example, you can create an Admin Role profile role for your operations staff that provides access to the firewall and network configuration areas of the web interface and a separate profile for your security administrators that provides access to security policy definitions, logs, and reports. On a firewall with multiple virtual systems, you can select whether the role defines access for all virtual systems or specific virtual systems. After new features are added to the product, you must update the roles with corresponding access privileges; the firewall does not automatically add new features to custom role definitions.

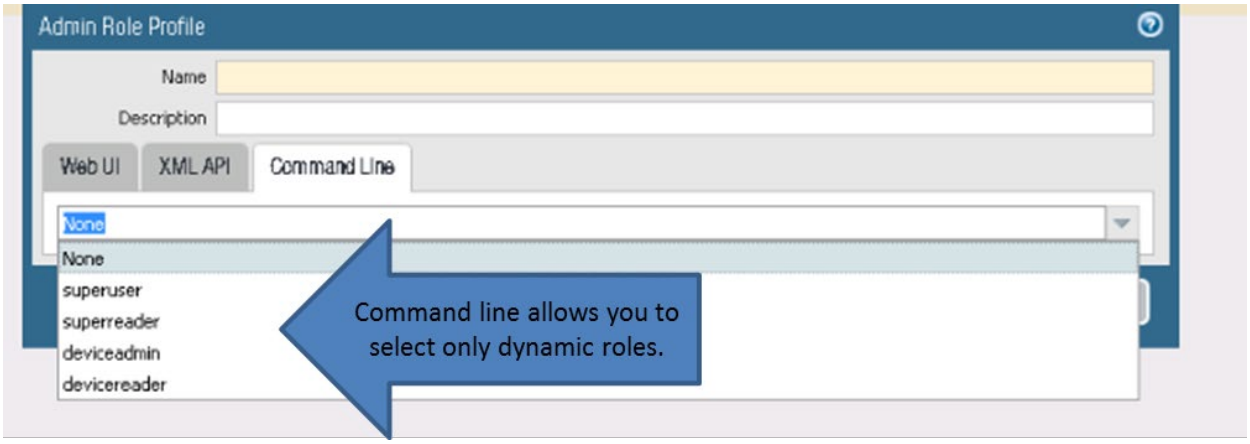
Administrator Account Configuration



Role Based Profile Types

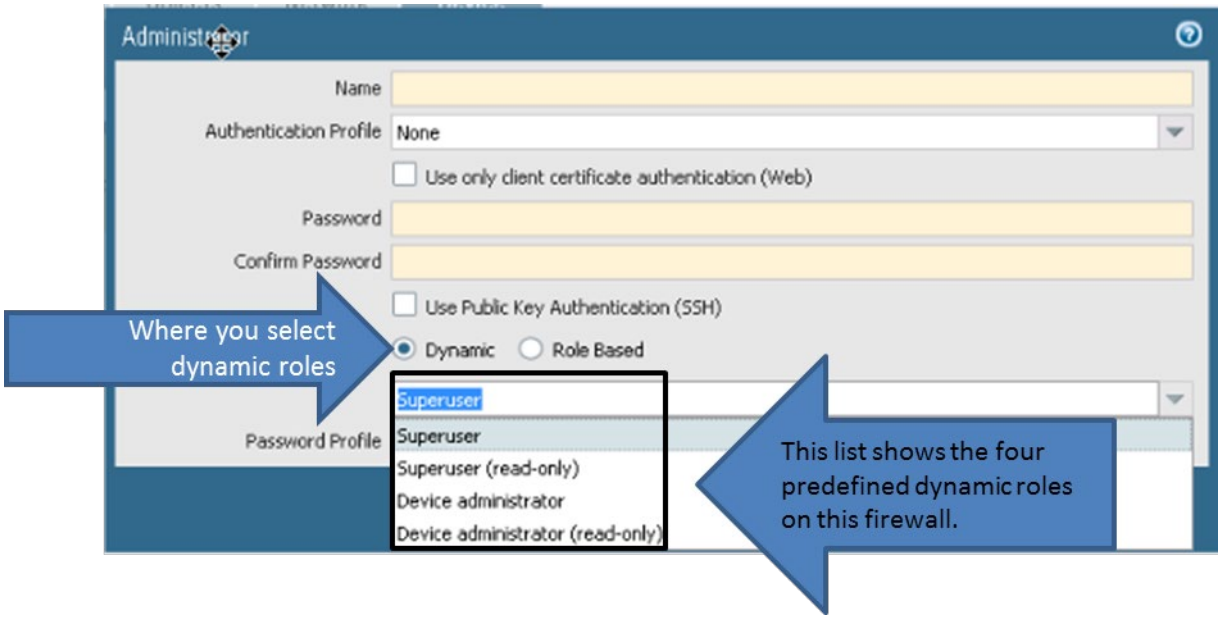
Web Interface	XML API
	

CLI

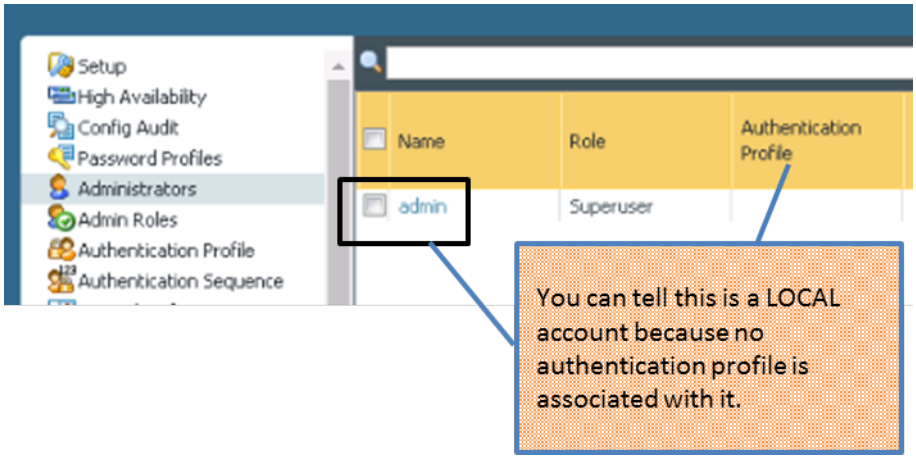


- **Dynamic** roles: These are built-in or predefined roles that provide access to the firewall. When new features are added, the firewall automatically updates the definitions of **Dynamic** roles; you never need to manually update them. The following list identifies the access privileges associated with dynamic roles.
  - **Superuser**: Full access to the firewall, including defining new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges.
  - **Superuser** (read-only): Read-only access to the firewall
  - **Virtual system administrator**: Full access to a selected virtual system (vsys)on the firewall, available on only firewalls that support virtual systems
  - **Virtual system administrator (read-only**): Read-only access to a selected vsys on thefirewall, available on only firewalls that support virtual systems
  - **Device administrator**: Full access to all firewall settings except for defining new accounts or virtual systems
  - **Device administrator (read-only):** Read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged-in account is visible)

Administrator Account Configuration



Local administrator accounts are authenticated using a local database.



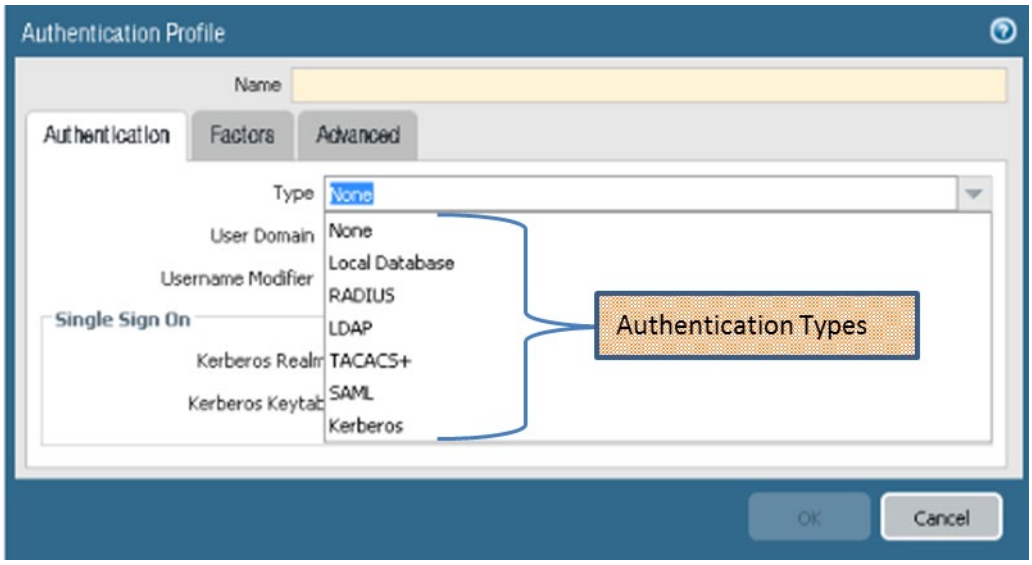
External administrator accounts require an external authentication service that is specified using an Authentication Profile.

PAN-OS software supports the following authentication types:

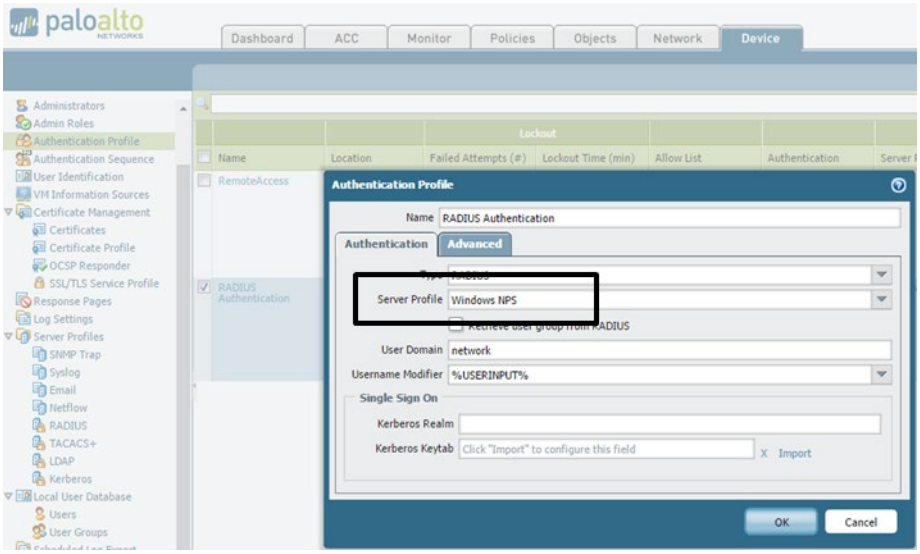
- None
- Local Database
- RADIUS
- LDAP
- TACACS+
- SAML
- Kerberos

Authentication Profiles provide authentication settings that you can apply to administrator accounts, SSL-VPN access, and Captive Portal. An Authentication Profile configuration screenshot follows:

Authentication Profiles

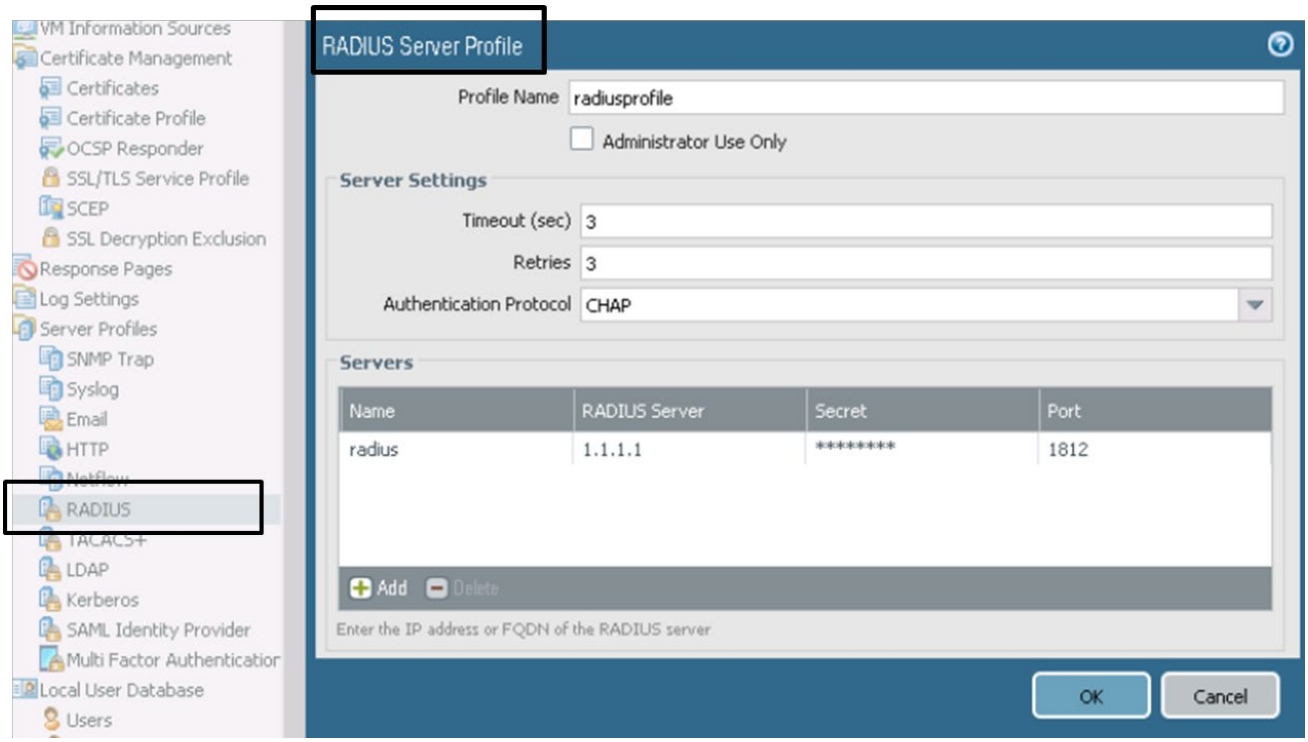


An Authentication Profile references a Server Profile.



A Server Profile includes the server name, its IP address, the service port that it is listening to, and other values. An example of a RADIUS Server Profile follows:

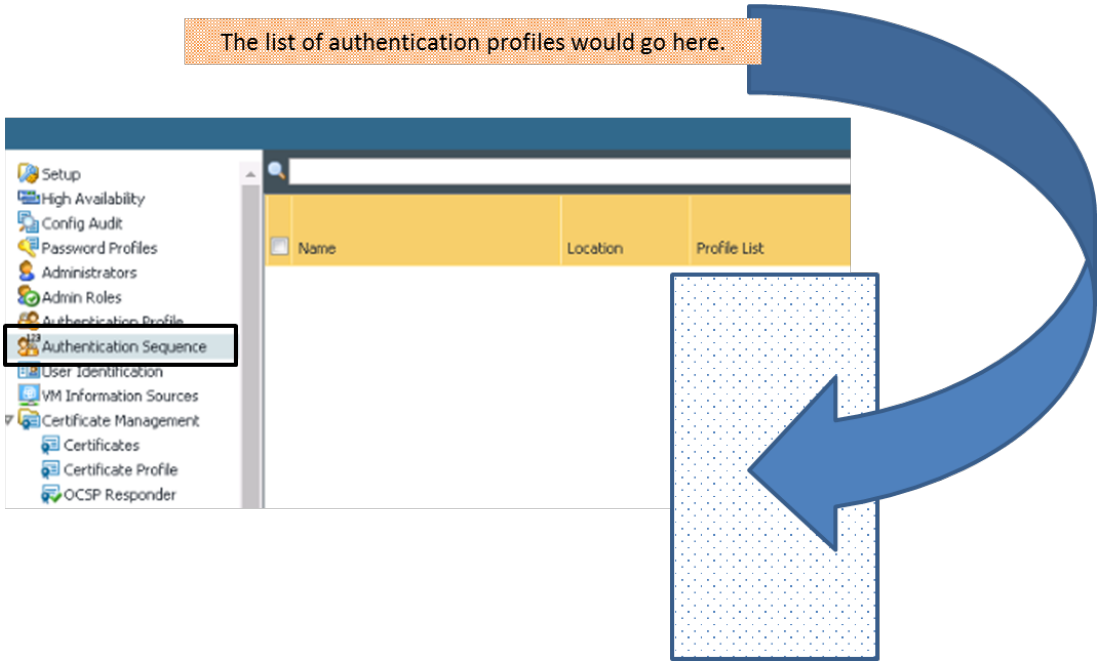
Server Profile



Authentication Sequence

Admin Roles for external administrator accounts can be assigned to an Authentication Sequence, which includes a sequence of one or more Authentication Profiles that are processed in a specific order. The firewall checks against each Authentication Profile within the Authentication Sequence until one Authentication Profile successfully authenticates the user. If an external administrator account does not reference an Authentication Sequence, it directly references an Authentication Profile instead. A user is denied access only if authentication fails for all the profiles in the Authentication Sequence. A depiction of an Authentication Sequence follows:

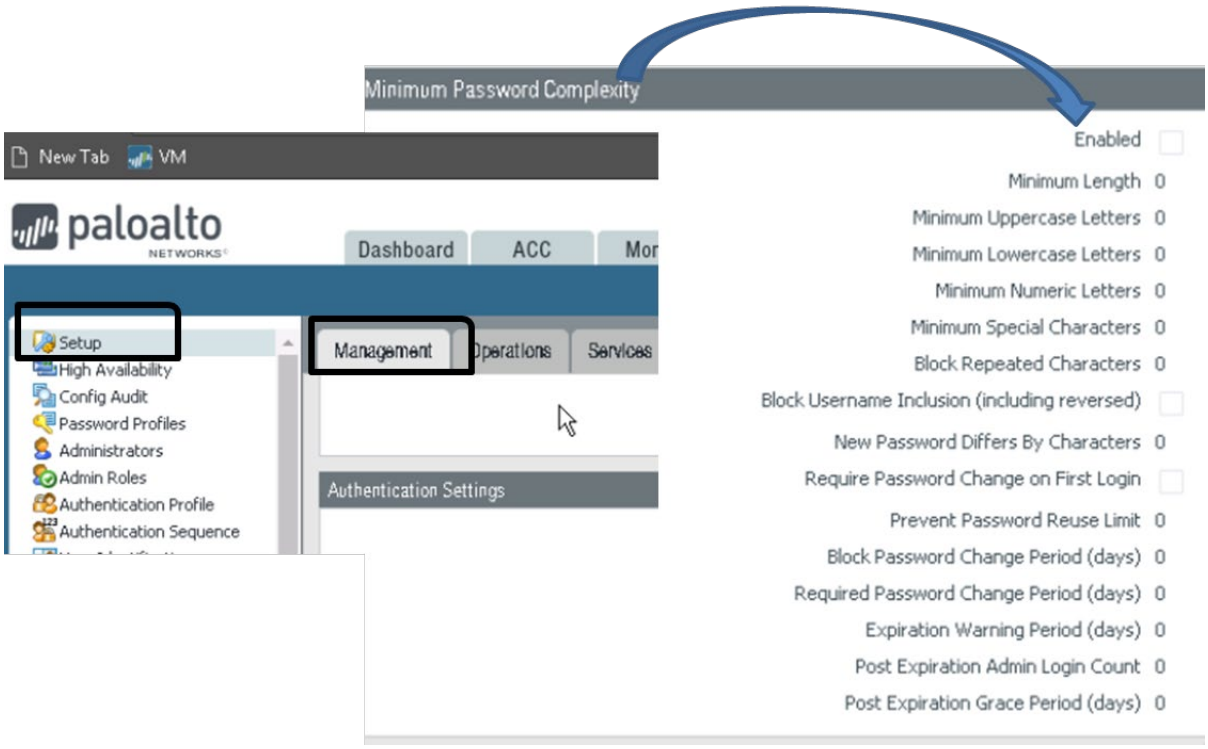
Authentication Sequence



Administrator Account Passwords

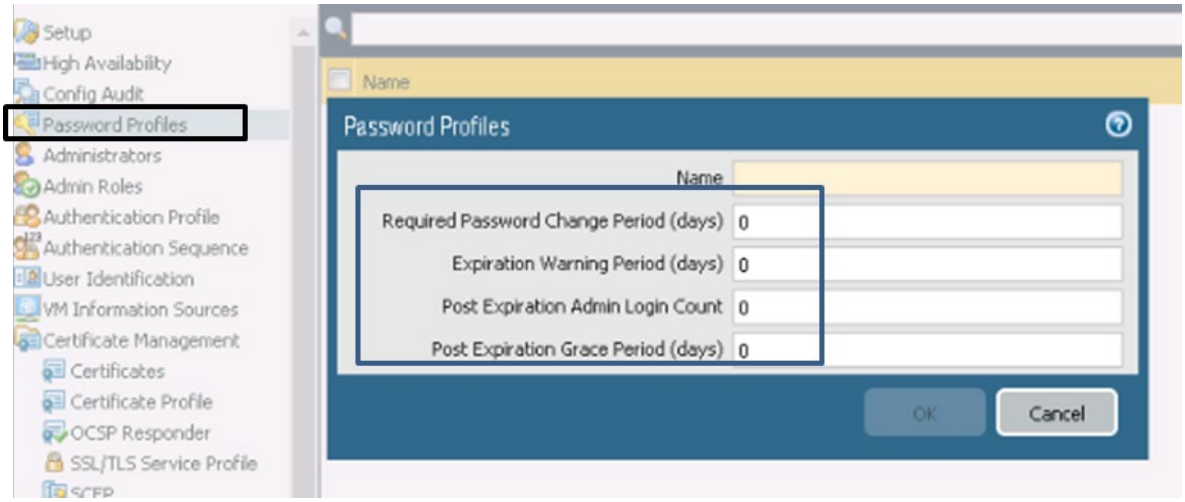
To ensure tighter security, you should enable Minimum Password Complexity Requirements. These global settings are applied to all local administrator accounts and help protect the firewall against unauthorized access for administrator accounts that require stricter complexity and aging requirements than do accounts for standard administrators.

Global Minimum Password Complexity Requirements



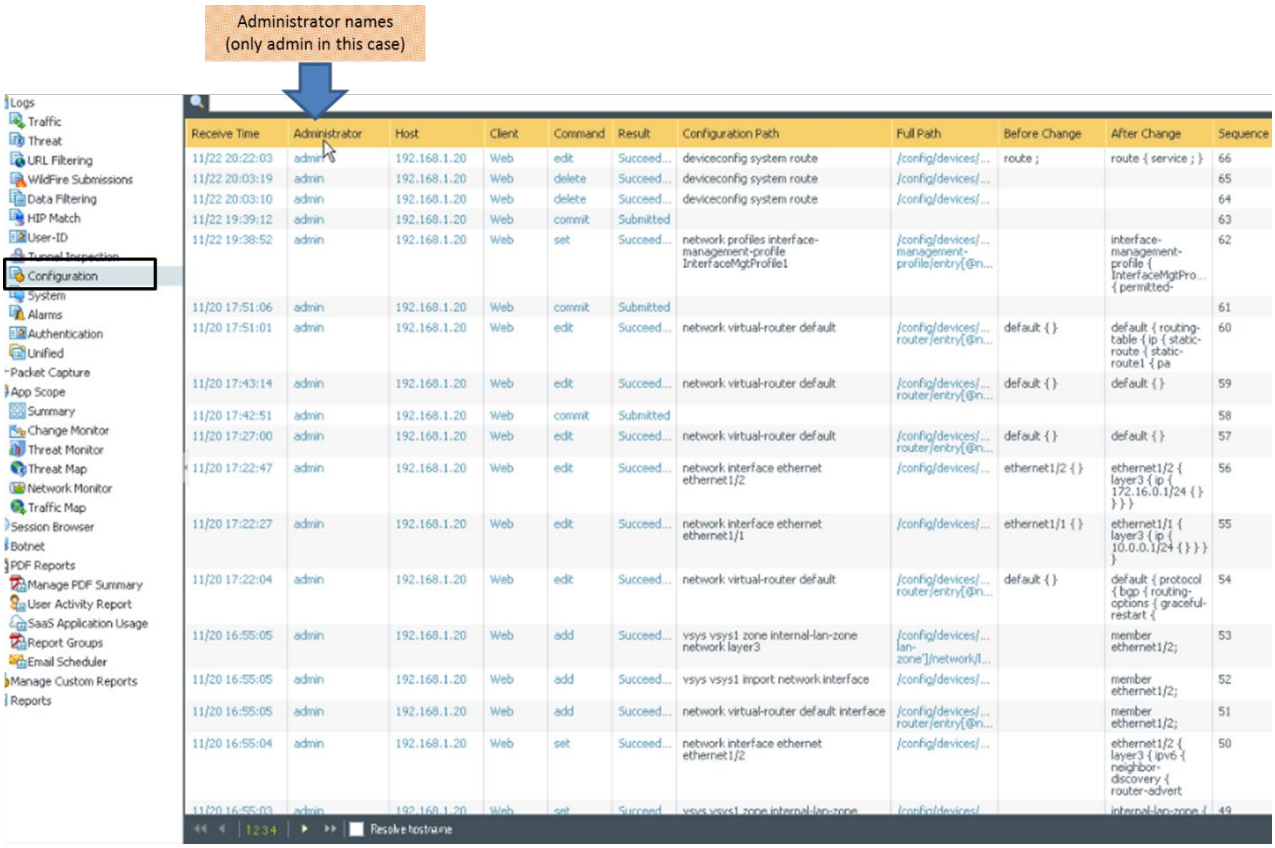
A password profile can be assigned to a local administrator account, which overrides the global password settings:

Password Profile



Configuration Logs

Configuration logs display entries for changes to the firewall configuration. Each entry includes the date and time, the administrator username, the IP address from where the administrator made the change, the type of client (web, CLI, or Panorama), the type of command executed, the command status (succeeded or failed), the configuration path, and the values before and after the change.



Sample questions

39. Which two statements are true about a Role Based Admin Role profile role? (Choose two.)
    A. It is a built-in role.
    B. It can be used for CLI commands.
    C. It can be used for XML API.
    D. Superuser is an example.
40. PAN-OS software supports which two authentication types? (Choose two.)
    A. RADIUS
    B. SMB
    C. TACACS+
    D. AWS
41. Which two Dynamic Admin Role types are available on the PAN-OS software? (Choose two.)
    A. superuser
    B. superuser (write only)
    C. device user

D. device administrator (read-only)

42. Which type of profile does an Authentication Sequence include?
    A. Security
    B. Authorization
    C. Admin
    D. Authentication
43. An Authentication Profile includes which other type of profile?
    A. Server
    B. Admin
    C. Customized
    D. Built-in
44. True or False: Dynamic Admin Roles are called “dynamic” because you can customize them.
    A. true
    B. false
45. What is used to override global Minimum Password Complexity Requirements?
    A. Authentication Profile
    B. Local Profile
    C. Password Role
    D. Password Profile

Exam Domain 2 – Simply Passing Traffic

2.5 Given a network diagram, create the appropriate security zones.

Security Zones

The Palo Alto Networks firewalls use security zones to analyze, control, and log network traffic as it traverses from one zone interface to another zone interface. Zones logically group networks that contain particular types of traffic that are contained within defined security classifications. Examples of such classifications are Internet, Data Center Applications, Users, IT Infrastructure, and Customer Data.

Security zones are divided into two broad categories: Intrazone and Interzone. Security zones contain one or more physical or virtual interfaces. An interface can belong to only one zone. Intrazone traffic, by default, allows traffic to flow between interfaces that exist in the same zone. Interzone traffic, by default, denies traffic from flowing between interfaces that exist in different zones.

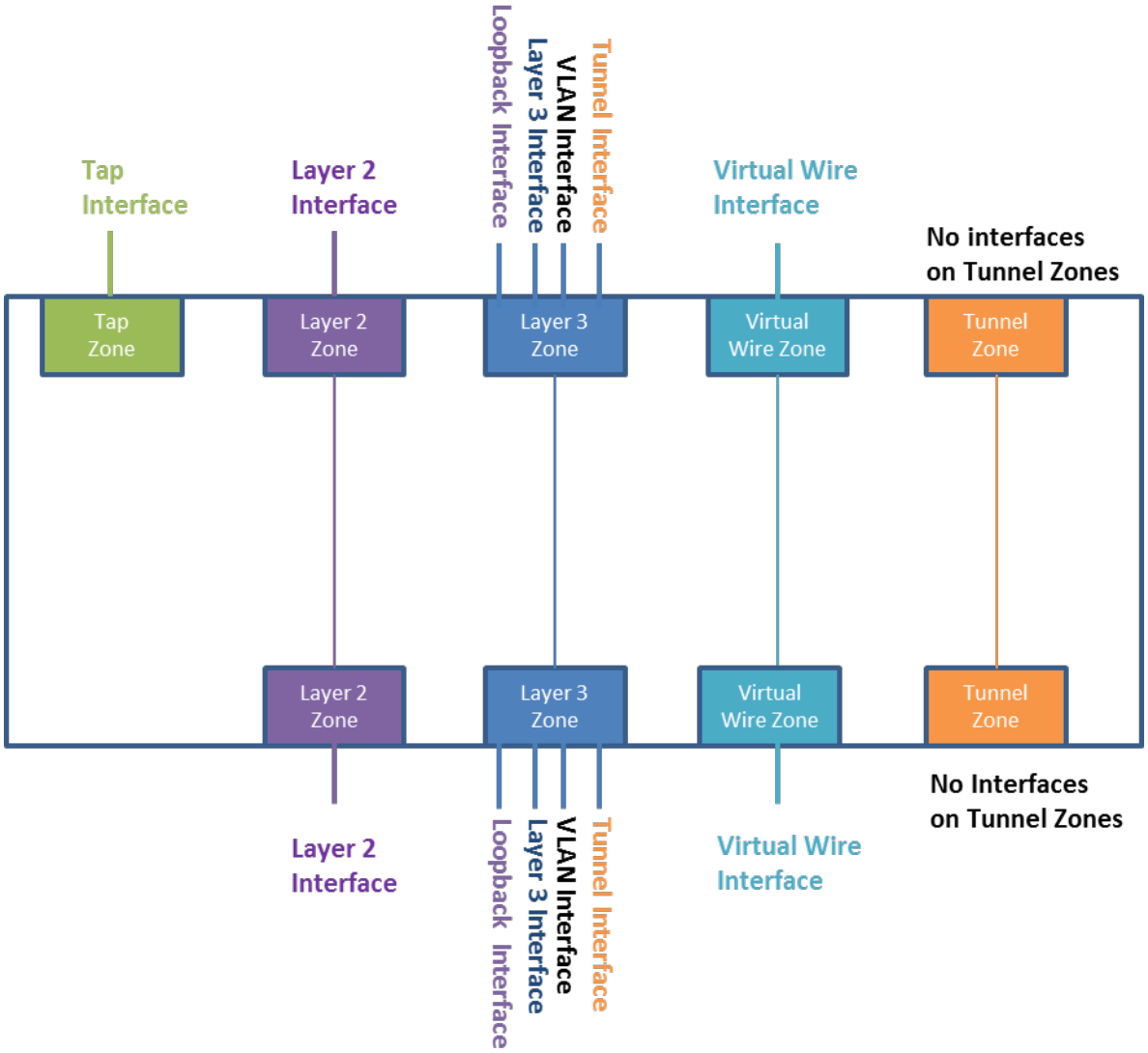
Security policy rules are applied to zones (not interfaces) to allow or deny traffic, apply QoS, perform NAT, apply security profiles, or set logging parameters. Security policy rules are described in another section of this study guide.

The following diagram is an example of network segments partitioned into multiple zones based on their security classification. The zones and the corresponding security policy rules should be made as definitive as possible to reduce your network’s attack surface. All zone names are custom names that are defined by the firewall administrator. There are five primary zone types (Tap, Layer 2, Layer 3, Tunnel, and Virtual

Wire) that support only specific interface types, also depicted in the following diagram. Different zone and interface types can be used simultaneously on different physical firewall interfaces. Tunnel zones became available in PAN-OS 8.0 and are used for a feature named tunnel content inspection.

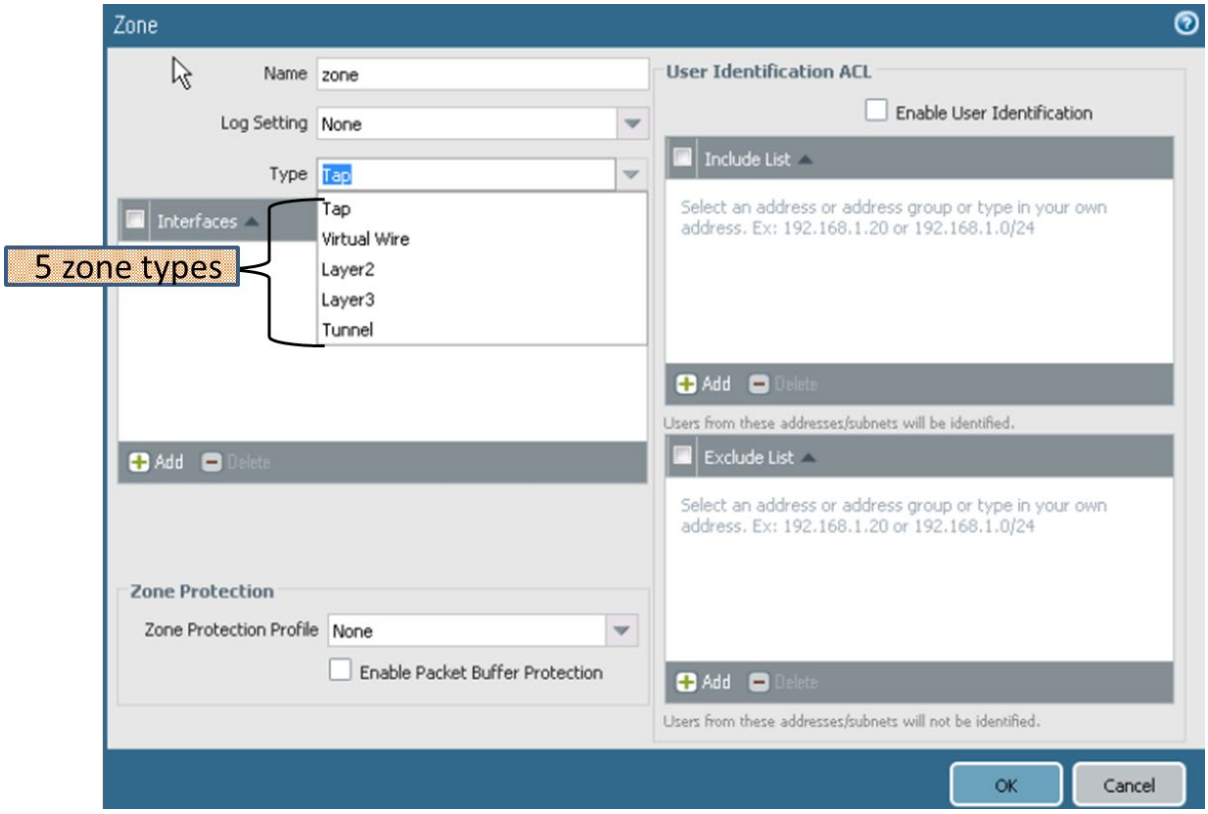
A sixth zone type named External is a special zone that is available only on some firewall models. The External zone allows traffic to pass between virtual systems when multiple virtual systems are configured on the same firewall. Virtual systems are supported only on the PA-2000, PA-3000, PA-4000, PA-5000, and PA-7000 Series firewalls. The External zone type is visible in the drop-down list only when it is supported by a firewall with the virtual systems feature enabled.

Note that MGT and HA interfaces are not assigned to a zone.

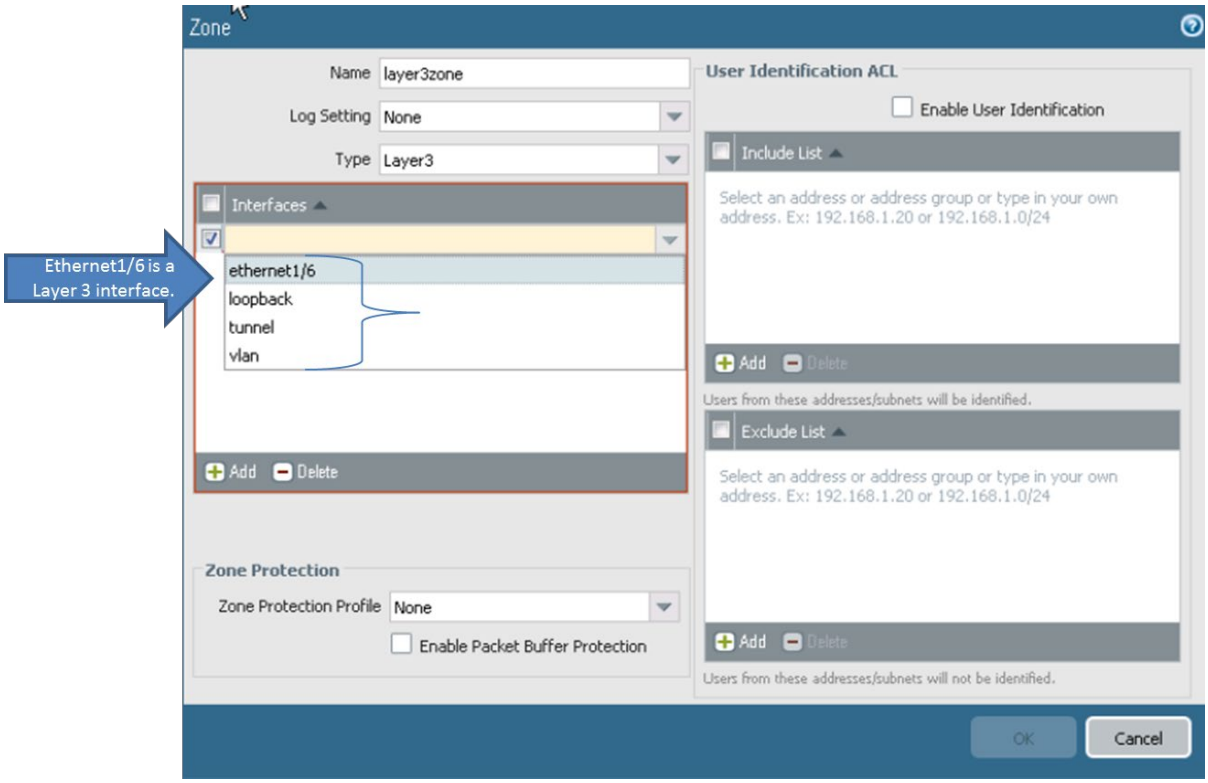


Zones need to be created and configured by assigning a zone name and specifying the zone type. Interfaces do not have to be configured prior to the zone's creation; they can be assigned to a zone later. Note that zone names are case-sensitive.

Five Zone Types



The following figure shows that the Layer 3 zone allows four interface types: Layer 3 (Ethernet1/6), loopback, tunnel, and vlan:



Sample questions

46. Which two default zones are included with the PAN-OS software? (Choose two.)
    A. Interzone
    B. Extrazone
    C. Intrazone
    D. Extranet
47. Which two zone types are valid? (Choose two.)
    A. trusted
    B. tap
    C. virtual wire
    D. untrusted
    E. dmz
48. The External zone type is used to pass traffic between which type of objects?
    A. Layer 2 interfaces
    B. Layer 3 interfaces
    C. virtual routers
    D. virtual systems
49. Which two statements about interfaces are correct? (Choose two.)
    A. Interfaces must be configured before you can create a zone.
    B. Interfaces do not have to be configured before you can create a zone.
    C. An interface can belong to only one zone.
    D. An interface can belong to multiple zones.
50. Which three interface types can belong in a Layer 3 zone? (Choose three.)
    A. loopback
    B. Layer 3
    C. tunnel
    D. virtual wire
51. What are used to control traffic through zones?
    A. access lists
    B. security policy lists
    C. security policy rules
    D. access policy rules

Exam Domain 2 – Simply Passing Traffic

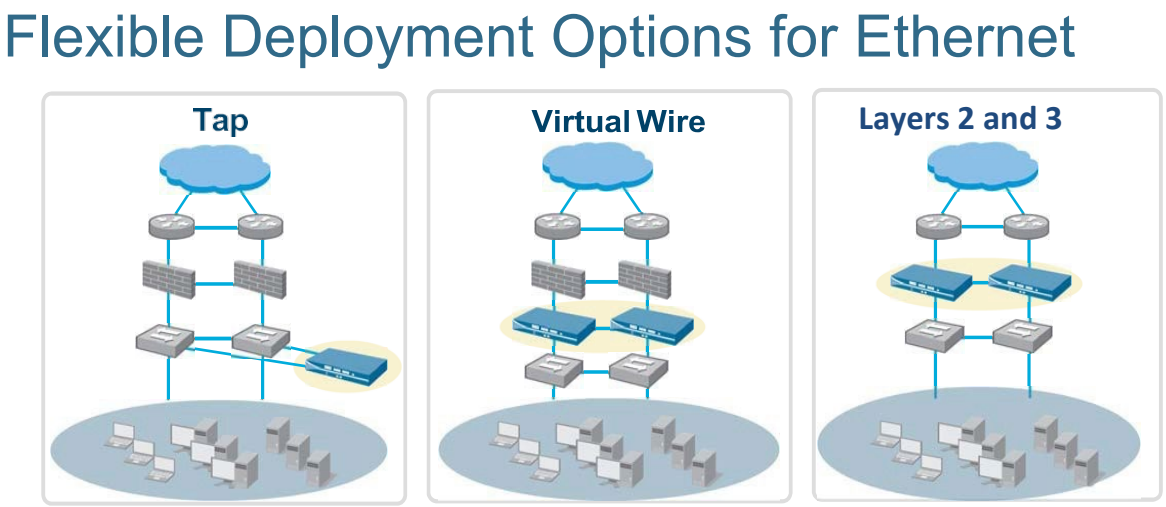
2.6 Identify and configure firewall interfaces.

Types of Ethernet Interfaces

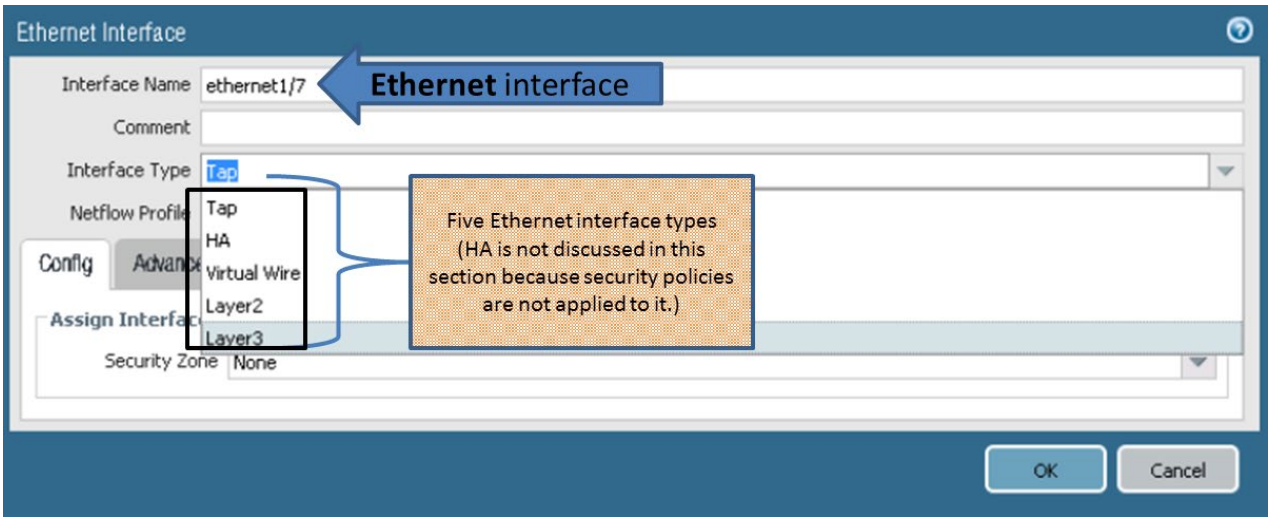
PAN-OS software has the following Ethernet interface types: Tap, Virtual Wire, Layer 2, Layer 3, and HA. (High Availability [HA] interfaces are not discussed in this section). A firewall can be configured with

multiple instances of each interface type to accommodate its functional requirements within a network. The following figure shows how a firewall can be used in Tap, Virtual Wire, Layer 2 or Layer 3 mode.

Ethernet Interface Types

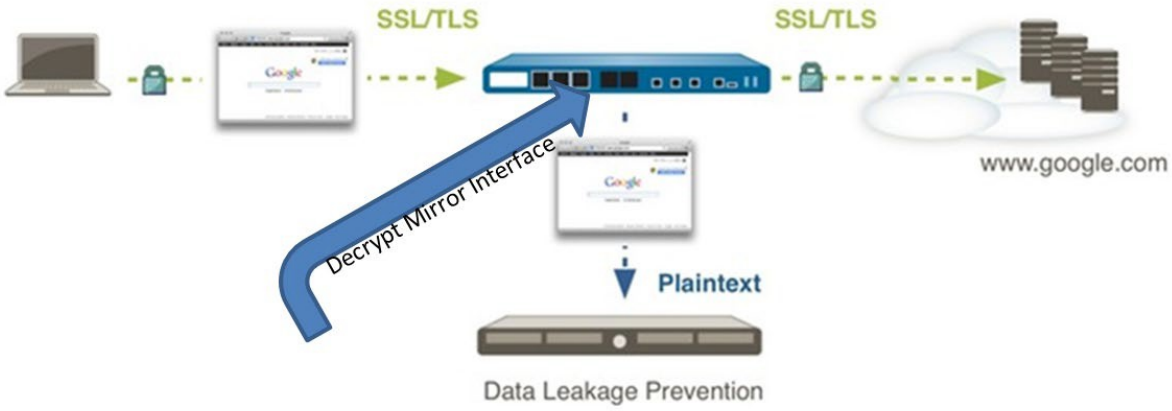


• App-ID, Content-ID, and User-ID visibility without inline deployment • Traffic logged to provide visibility	• SSL decryption (no encryption) • Allows NAT	• All the Virtual Wire mode capabilities including Layer 2 or Layer 3 services: virtual routers, VPN, and routing protocols



Other available interface types include the following:

- **Decrypt Mirror**: This feature enables decrypted traffic from a firewall to be copied and sent to a traffic collection tool that can receive raw packet captures, such as NetWitness or Solera, for archiving and analysis. Decrypt Mirror is often used to route decrypted traffic through an external interface to a data loss prevention (DLP) service. DLP is a product category for products that scan internet-bound traffic for keywords and patterns that identify sensitive information. Note that a free license is required to use this feature. This feature is not available on the VM-Series firewalls.

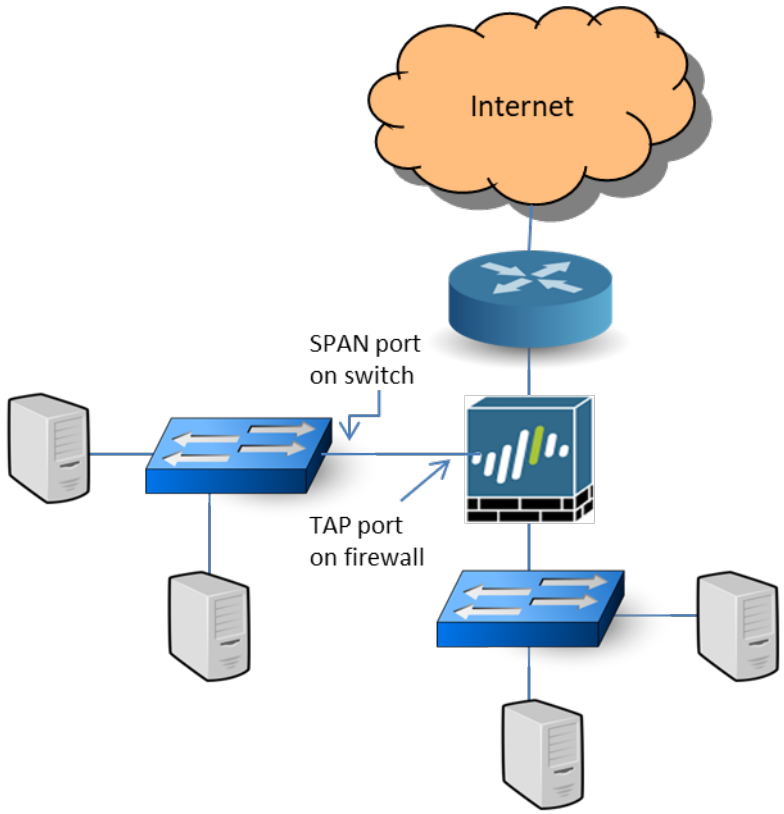


- **Log card:** For PA-7000 Series firewalls only. A log card data port performs log forwarding for syslog, email, Simple Network Management Protocol (SNMP), and WildFire fileforwarding. One data port on a PA-7000 must be configured as a log card interface because the MGT interface cannot handle all the logged traffic.
- **Aggregate:** Used to bundle multiple physical HA3, Virtual Wire, Layer 2, or Layer 3 interfaces into a logical interface for better performance (via load-balancing) and redundancy using IEEE 802.1AX (LACP) link aggregation. The interface types to be bundled must be the same. All Palo Alto Networks firewalls except the PA-200 and VM-Series models support Aggregate Ethernet (AE) interface groups.
- **HA interface:** Each high availability (HA) interface has a specific function. One HA interface is for configuration synchronization and heartbeats; the other HA interface is for state synchronization. If active/active high availability is enabled, the firewall also can use a third HA interface to forward packets.
- **Management:** MGT interfaces are used to manage a firewall using a network cable.
- **Loopback:** Loopback interfaces are Layer 3 virtual interfaces that 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:** A tunnel interface is a logical (virtual) interface used with VPN tunnels to deliver encrypted traffic between two endpoints. The tunnel interface must belong to a security zone to before policy can be applied, and it must be assigned to a virtual router to use the existing routing infrastructure. A tunnel interface does not require an IP address to route traffic between the sites. An IP address is only required if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel.

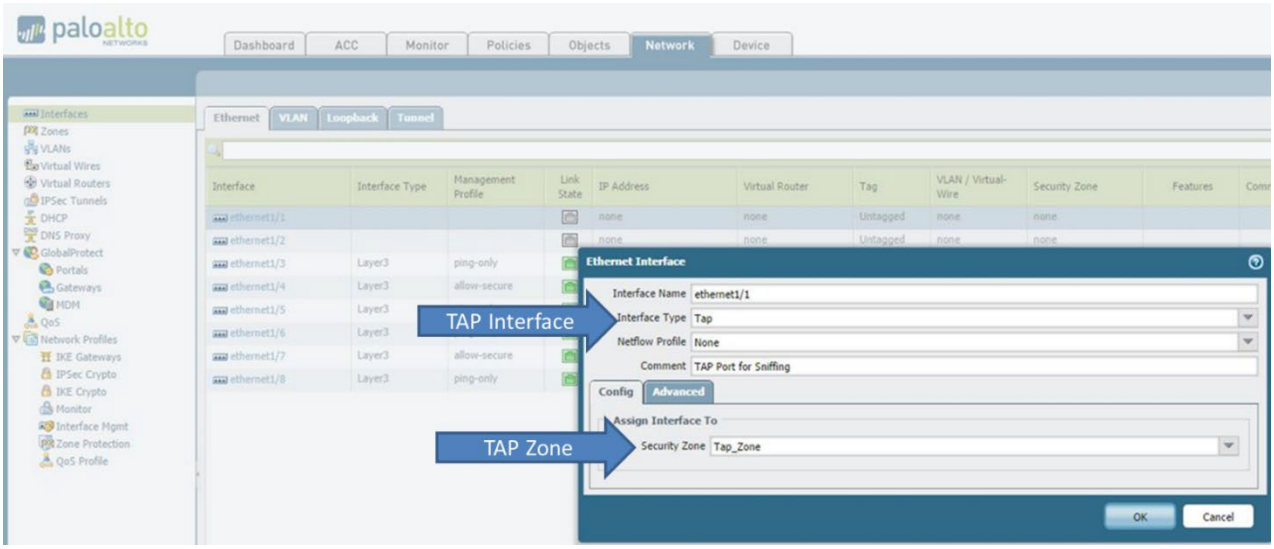
Tap, Virtual Wire, Layer 2, and Layer 3 interfaces

- **Tap**: A Tap interface monitors traffic that is connected to a network switch's MIRROR/SPAN port. This mirrored traffic is forwarded by a switch port to a firewall's Tap interface and is analyzed for App-ID, User-ID, Content-ID, and other traffic, just like any other normal data traffic that would pass through the firewall. Before traffic can be logged, a security policy must be configured that includes the Tap zone. Tap interfaces

are easy to deploy and can be implemented without disruption to your existing network. Tap mode offers visibility in the Traffic log and also in the **ACC** tab. The information can be used to help configure security policy rules, and to make other firewall configuration changes. Tap traffic is not managed (blocked, allowed, or shaped) TAP interfaces must be assigned to a Tap zone.



To configure a Tap interface, go to **Network > Interfaces > Ethernet > <select_interface>**.

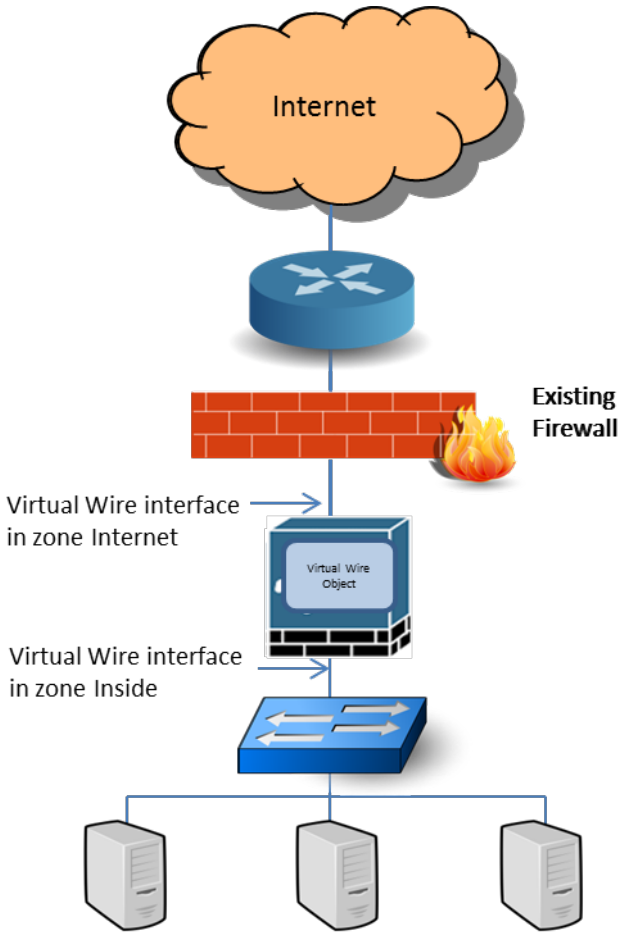


Virtual Wire

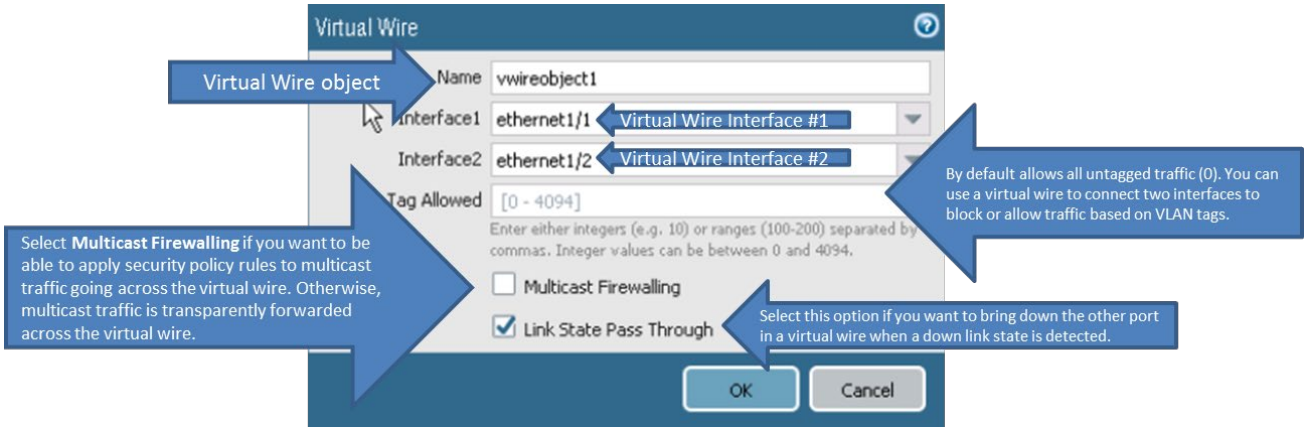
A Virtual Wire interface is used to pass traffic through a firewall by binding two Ethernet interfaces and allowing traffic to pass between them. Virtual Wire interfaces are often placed between an existing

firewall and a secured network to enable analysis of the traffic before actually migrating from a legacy firewall to a Palo Alto Networks firewall.

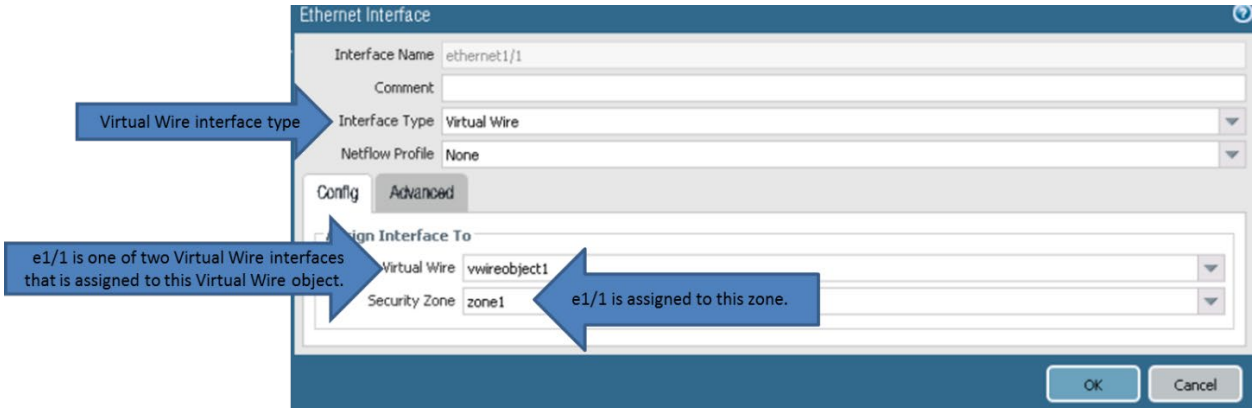
- No IP or MAC addresses are assigned to virtual wire interfaces. No routing or switching is done on a Virtual Wire interface. A virtual wire interface that receives a frame or packet ignores any Layer 2 or Layer 3 addresses for switching or routing purposes, but applies your security or NAT policy rules before passing an allowed frame or packet over the virtual wire to the second Virtual Wire interface and on to the network device connected to it. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet interfaces of the same medium (both either copper or fiber) or bind a copper interface to a fiber interface.
- Two Virtual Wire interfaces, each in a virtual wire zone (the zone can be the same or different), and a virtual wire object are required to complete a virtual wire configuration. The following figure shows one interface in one zone (Internet) and the other interface in another zone (Inside). If both interfaces are in different zones (interzone traffic), all traffic will be inspected by security policy rules until sessions can be established, and then you can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.
- If both interfaces are in the same zone (intrazone traffic), all the traffic would be allowed by default, and sessions can be easily established. However, you also can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.
- Virtual Wire interfaces can be subdivided into Virtual Wire subinterfaces that can be used to classify traffic according to VLAN tags, IP addresses, IP ranges, or subnets. Use of subinterfaces enables you to separate traffic into different zones for more granular control than regular (non-subinterface) Virtual Wire interfaces.



To configure a Virtual Wire object, go to **Network > Virtual Wires > Add**.

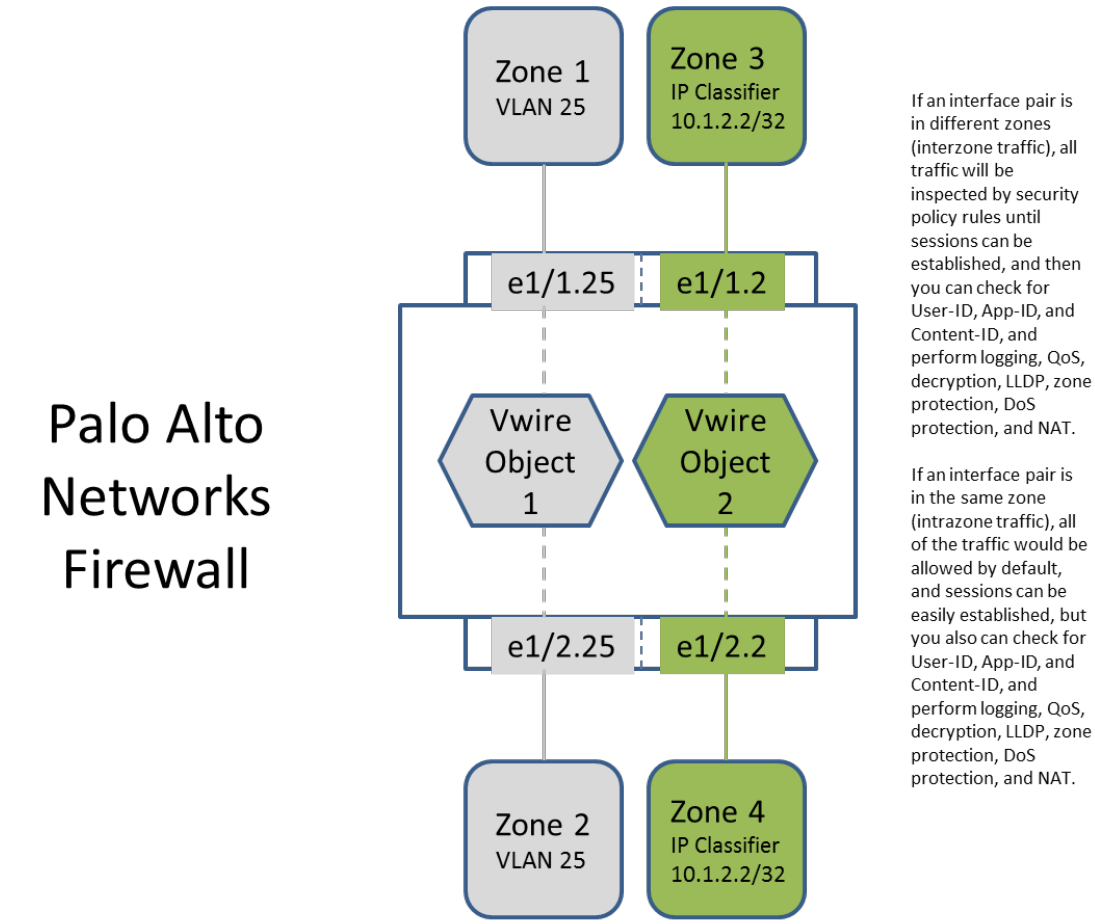


To configure a Virtual Wire interface, go to **Network > Interfaces > Ethernet > <select_interface>**.



Virtual Wire Subinterfaces

Virtual wire deployments can use Virtual Wire subinterfaces to separate traffic into different zones. Virtual Wire subinterfaces provide flexibility in enforcing distinct policies when you need to manage traffic from multiple customer networks. Virtual Wire subinterfaces enable you to control and separate traffic by specifying criteria such as VLAN tags and IP classifiers. IP classifiers consist of host IP addresses, IP subnets, and IP ranges. Assign each subinterface to a different zone, and then enforce security policy rules for the traffic that matches the defined criteria. Note that zones can belong to separate virtual systems.



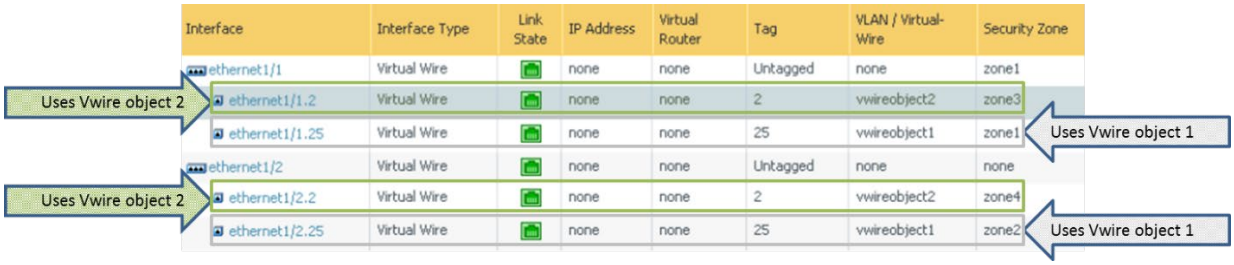
Security Policy #1

Source Zone	Destination Zone	Logging Profile
Zone 1	Zone 2	VLAN 25 information (which is a specific customer in this case)

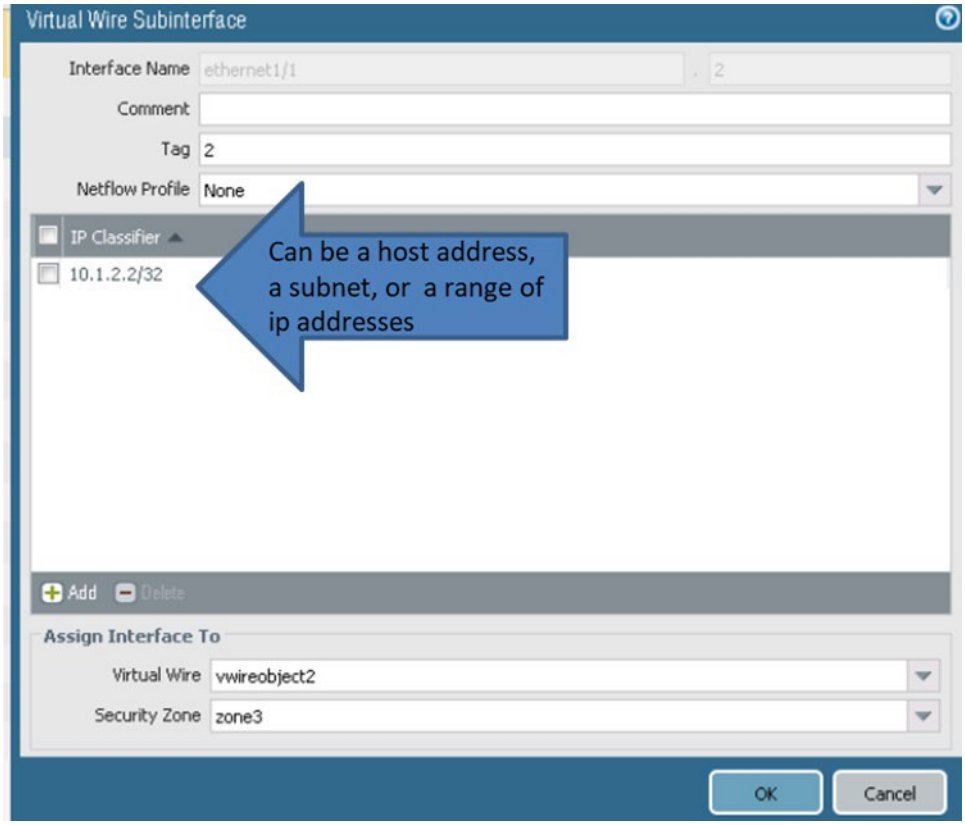
Security Policy #2

Source Zone	Destination Zone	Logging Profile
Zone 3	Zone 4	Host 10.1.2.2 information (which is a specific server in this case)

To configure a Virtual Wire subinterface, go to **Network > Interfaces > Ethernet** and select, but do not open, a Virtual Wire interface. Then click **Add Subinterfaces** as the bottom of the web interface window.

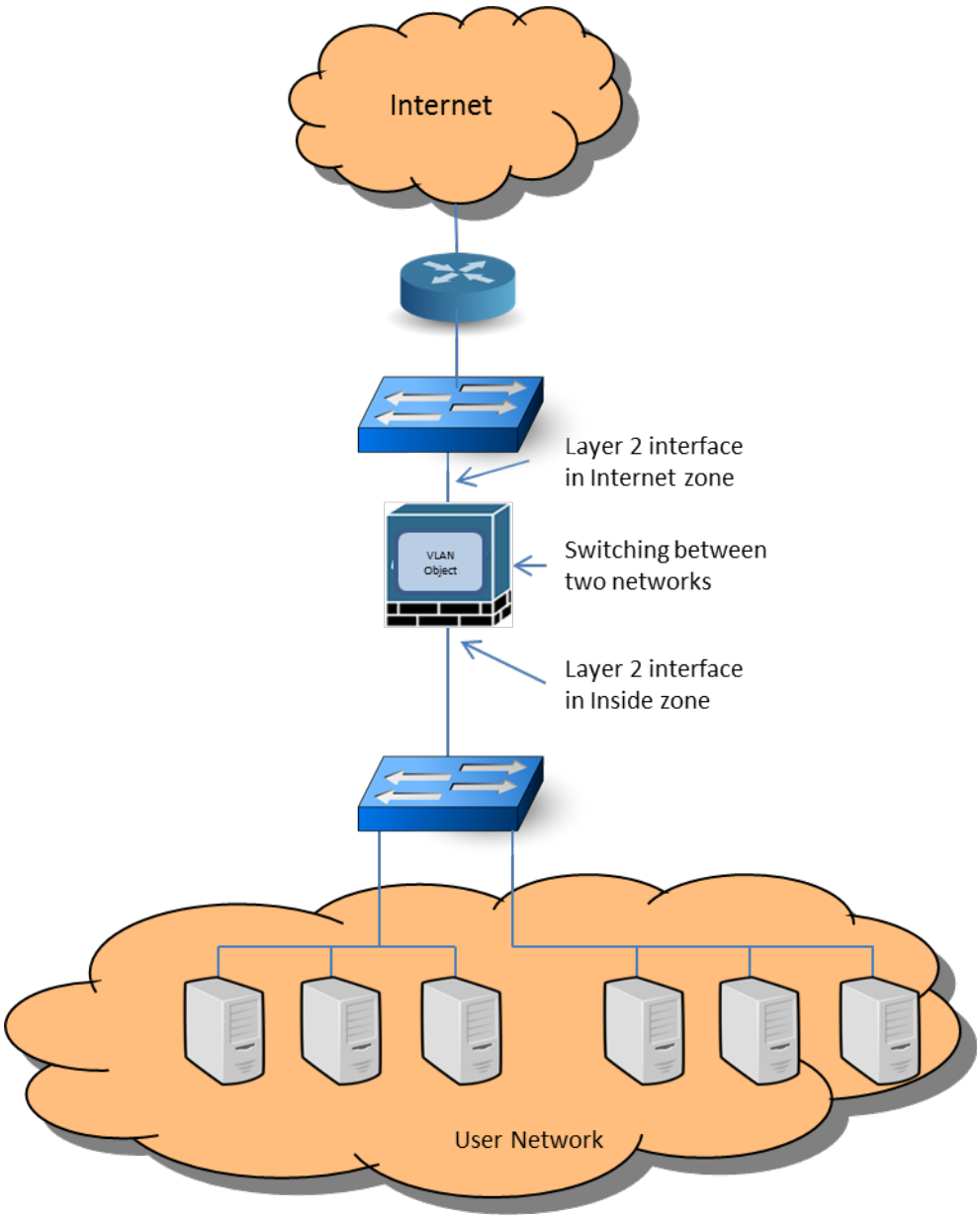


Virtual Wire Subinterface

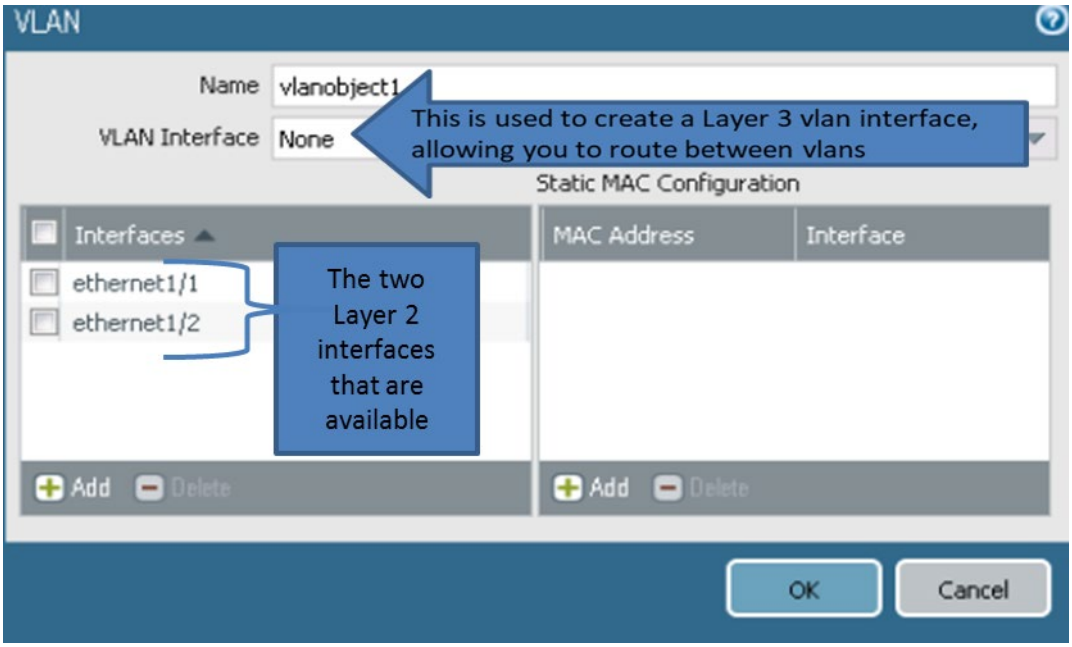


Layer 2 Interfaces

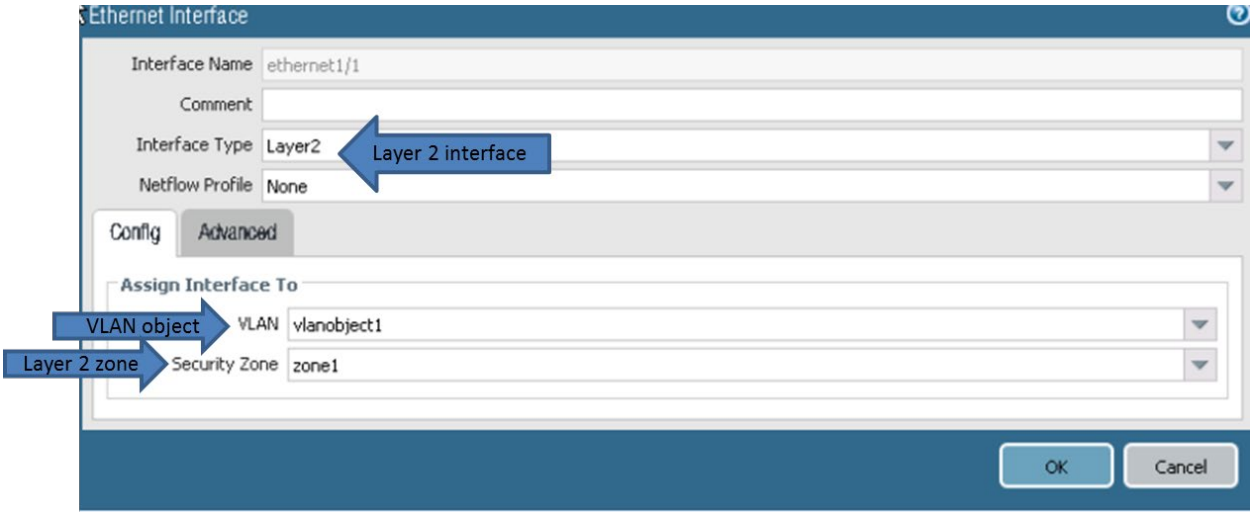
Layer 2 interfaces are used to switch traffic between other Layer 2 interfaces. Before switching can take place, each Layer 2 interface must be assigned to a VLAN object. Assignment of interfaces that belong to the same VLAN but exist in different Layer 2 zones enables you to analyze, shape, manage, and decrypt the traffic. Layer 2 traffic can route to other Layer 3 interfaces using a Layer 3 VLAN interface. Note that Layer 2 interfaces do not participate in spanning tree other than forward BPDUs.



To configure a VLAN object, go to **Network > VLAN > Add**.

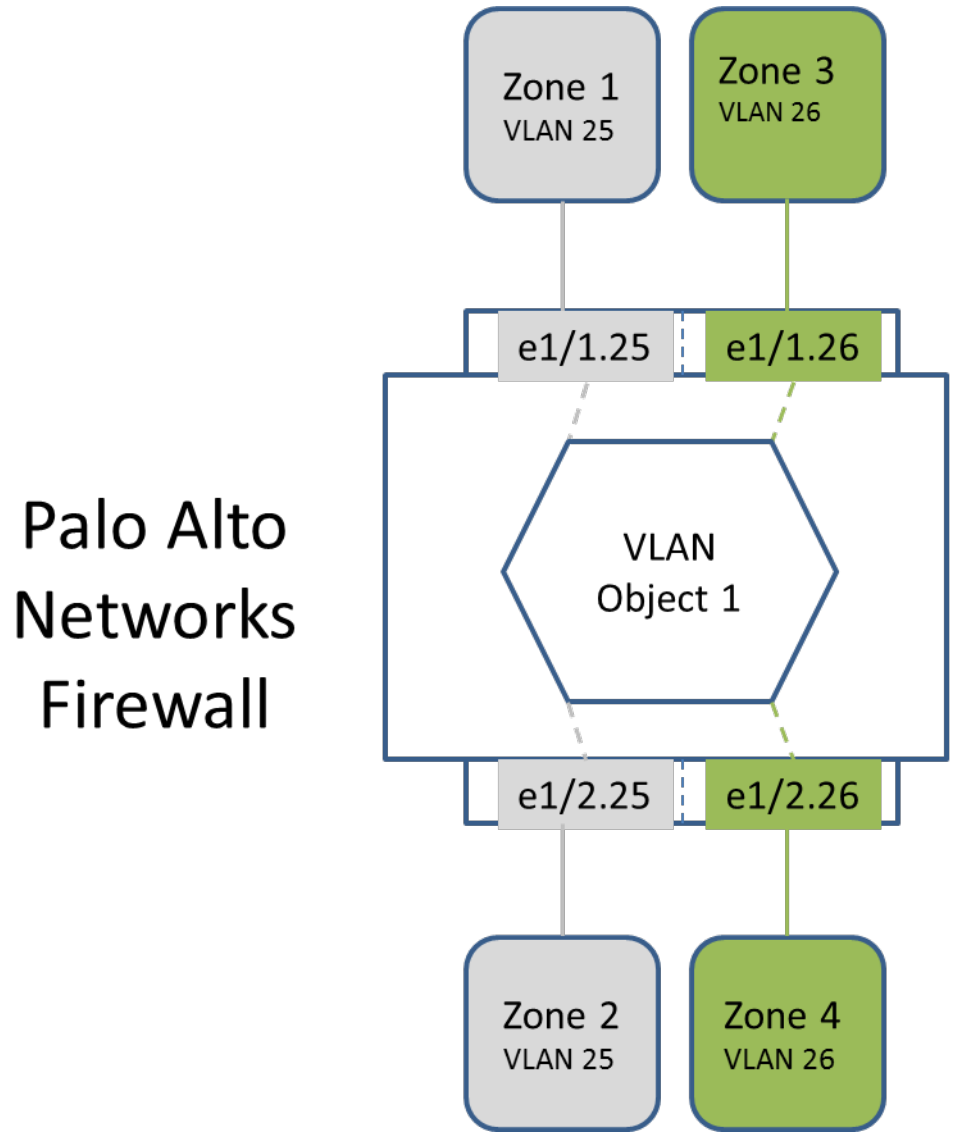


To configure a Layer 2 interface, go to **Network > Interfaces > Ethernet > <select_interface>**.



Layer 2 Subinterfaces

Layer 2 interfaces can be subdivided into Layer 2 subinterfaces. For each Ethernet port configured as a physical Layer 2 interface, you can define an additional logical Layer 2 interface (subinterface) for each VLAN tag assigned to the traffic that the port receives. The firewall enables Layer 2 switching between Layer 2 subinterfaces that are connected to the same VLAN object. To enable switching between Layer 2 subinterfaces, assign the same VLAN object to the subinterfaces. Even though Layer 2 subinterfaces are available on a Palo Alto Networks firewall, the best practice is to use Layer 3 subinterfaces. Use of Layer 3 subinterfaces isolates Layer 2 traffic, yet provides routing between subnets.



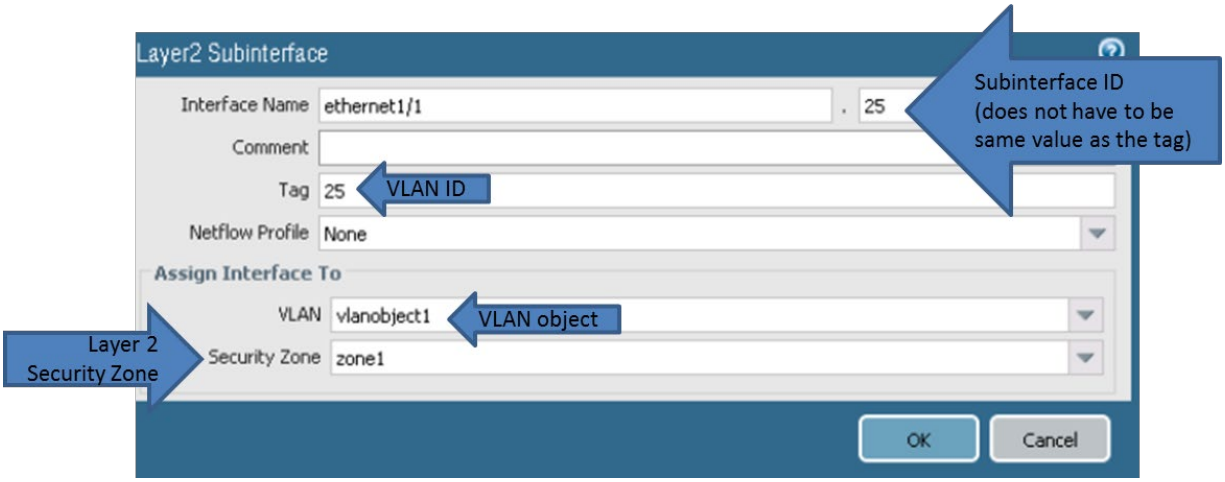
If interfaces in the same VLAN are in different zones (interzone traffic), all traffic will be inspected by security policy rules until sessions can be established, and then you can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, and DoS protection.

If interfaces in the same VLAN are in the same zone (intrazone traffic), all of the traffic would be allowed by default, and sessions can be easily established, but you also can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, and DoS protection.

To configure a Layer 2 subinterface, go to **Network > Interfaces > Ethernet > <select_interface>** and select, but do not open, a Layer 2 interface. Then click **Add Subinterfaces** as the bottom of the web interface window.

Interface	Interface Type	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer2		none	none	Untagged	vlanobject1	zone1
ethernet1/1.25	Layer2		none	none	25	vlanobject1	zone1
ethernet1/1.26	Layer2		none	none	26	vlanobject1	zone3
ethernet1/2	Layer2		none	none	Untagged	vlanobject1	none
ethernet1/2.25	Layer2		none	none	25	vlanobject1	zone2
ethernet1/2.26	Layer2		none	none	26	vlanobject1	zone4

Layer 2 Subinterface



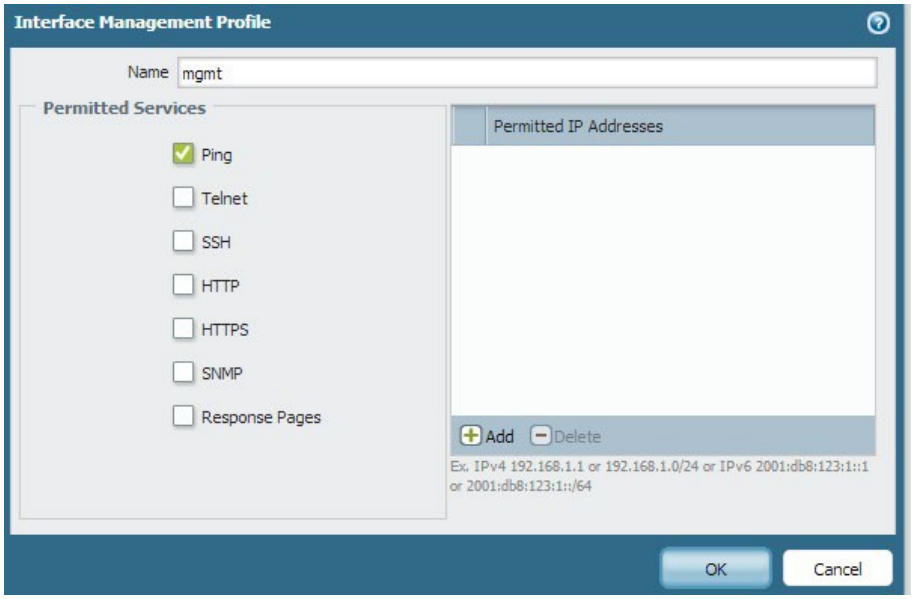
Layer 3 Interfaces

In a Layer 3 deployment, the firewall routes traffic between multiple interfaces. A Virtual Router object must exist for the firewall to route traffic between Layer 3 interfaces. Layer 3 interfaces are assigned IP addresses. PAN-OS software supports both IPv4 and IPv6 addressing. As is the case in most interface types, Layer 3 traffic can be monitored, analyzed, managed, shaped, translated, and encrypted or decrypted. If a tunnel is used for routing or if tunnel monitoring is turned on, the tunnel needs an IP address. The **Advanced** tab contains options that enable you to configure a variety of Layer 3 interface settings such as MTU, static ARP, LLDP, IPv6 NDP, link speed, and duplex settings. Both IPv4 and IPv6 addresses can be configured on a single interface.

Loopback interfaces are Layer 3 virtual interfaces that 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.

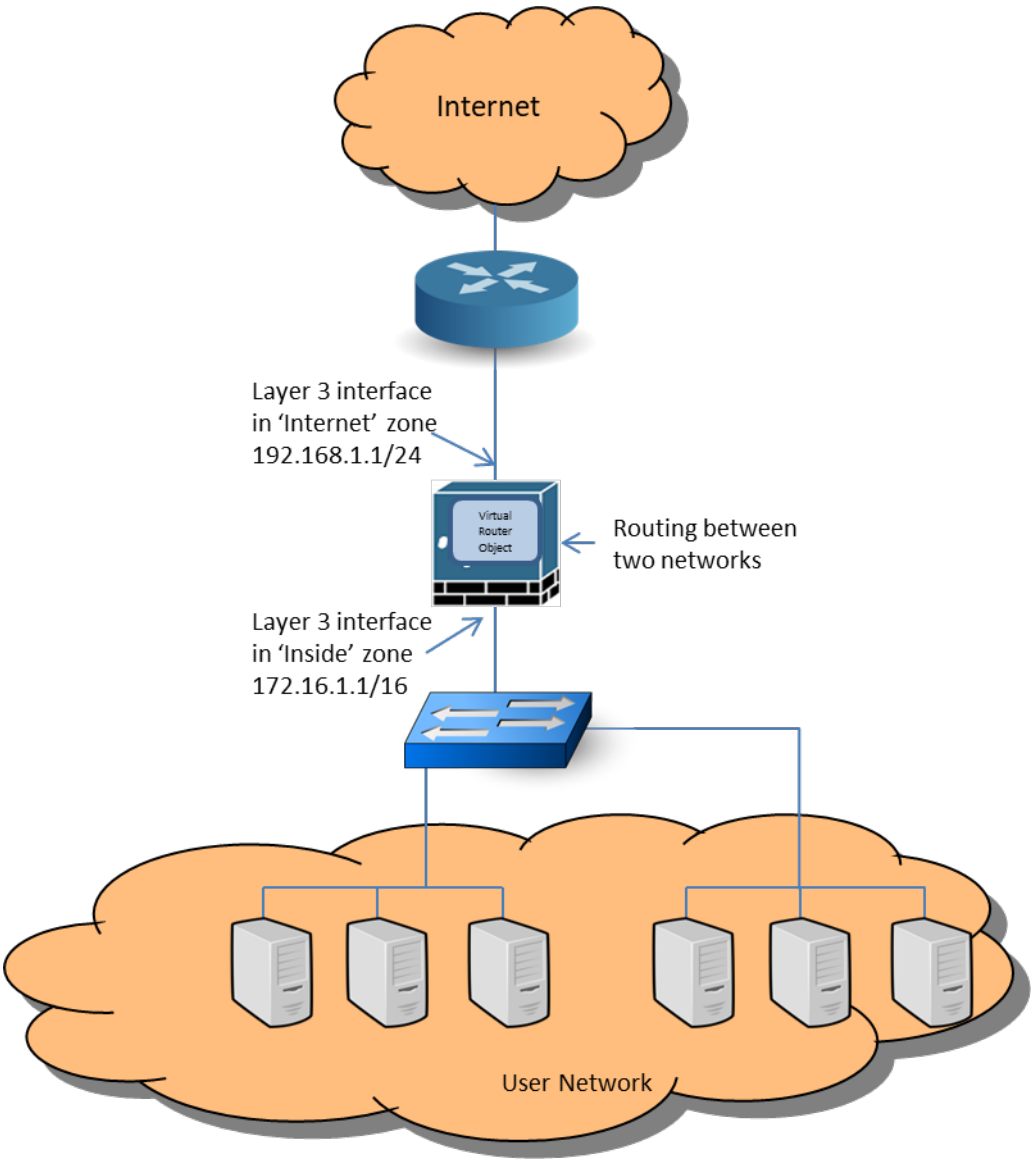
Unlike Tap, Virtual Wire, or Layer 2 interfaces, Layer 3 interfaces can be used to manage firewalls using an interface management profile. An interface management profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that a firewall Layer 3 interface permits for management traffic. Interface management profiles are discussed in more detail in a different section of this study guide.

Example of an Interface Management Profile

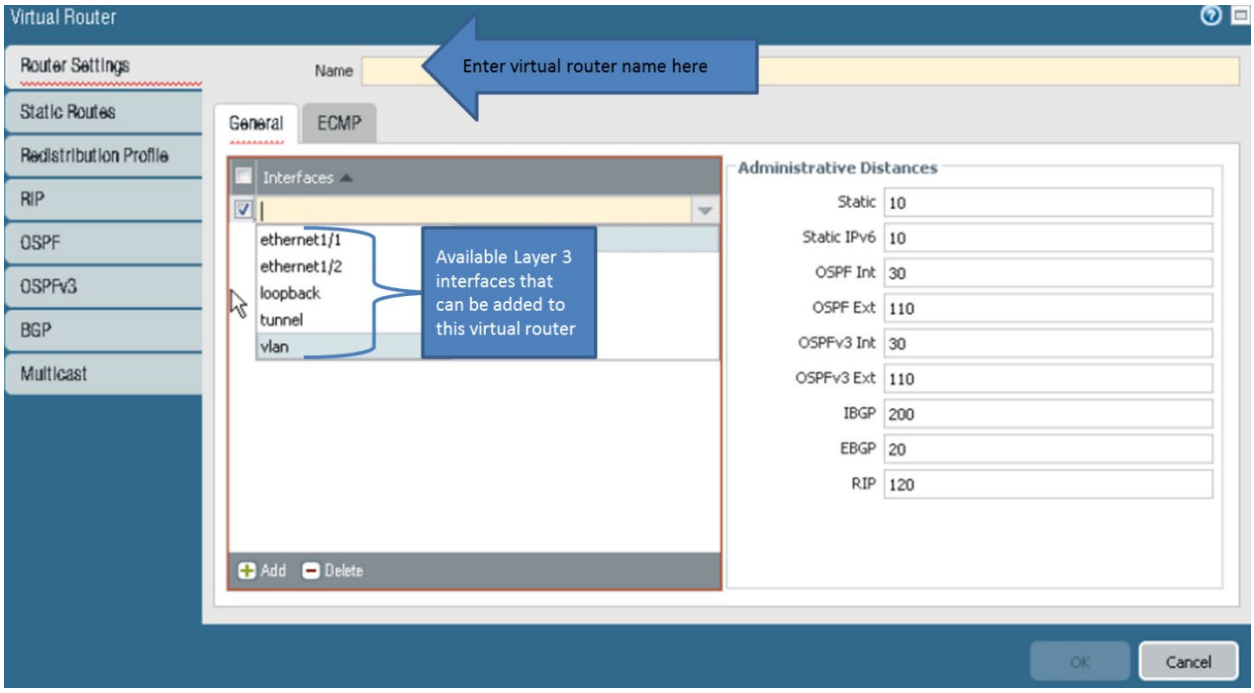


You can configure a Layer 3 interface with one or more static IPv4 addresses or as a DHCP client. A single Layer 3 interface can be assigned multiple IPv4 addresses, although they should not be in the same subnet. You can configure a Layer 3 interface with one or more IPv6 addresses, either as a link-local address or a Global address.

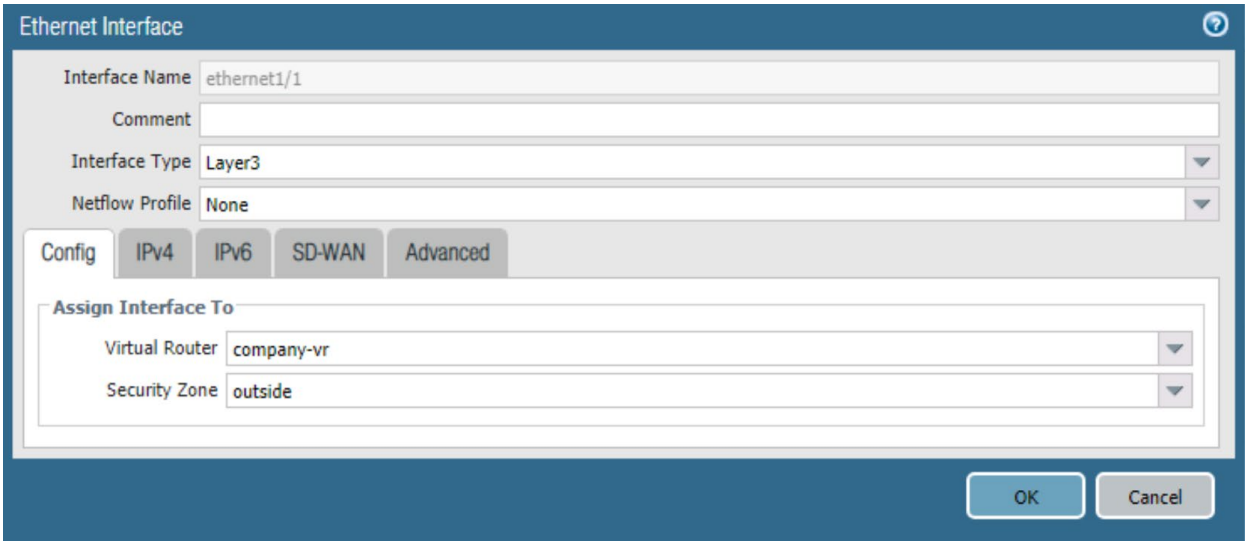
Layer 3 interfaces also can be configured as subinterfaces, where each subinterface is assigned a unique IP address.



To configure a virtual router object, go to **Network > Virtual Routers > Add**.

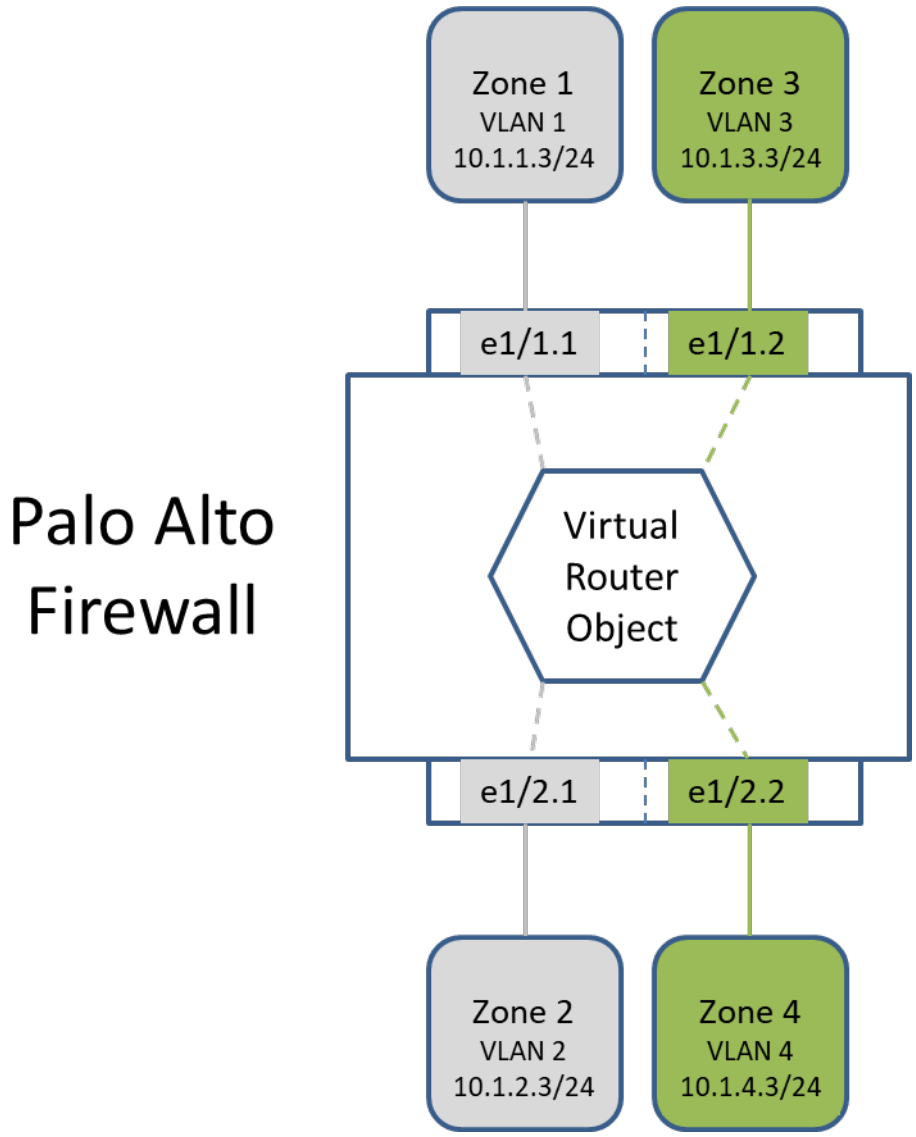


To configure a Layer 3 interface, go to **Network > Interfaces > Ethernet > <select_interface>**.

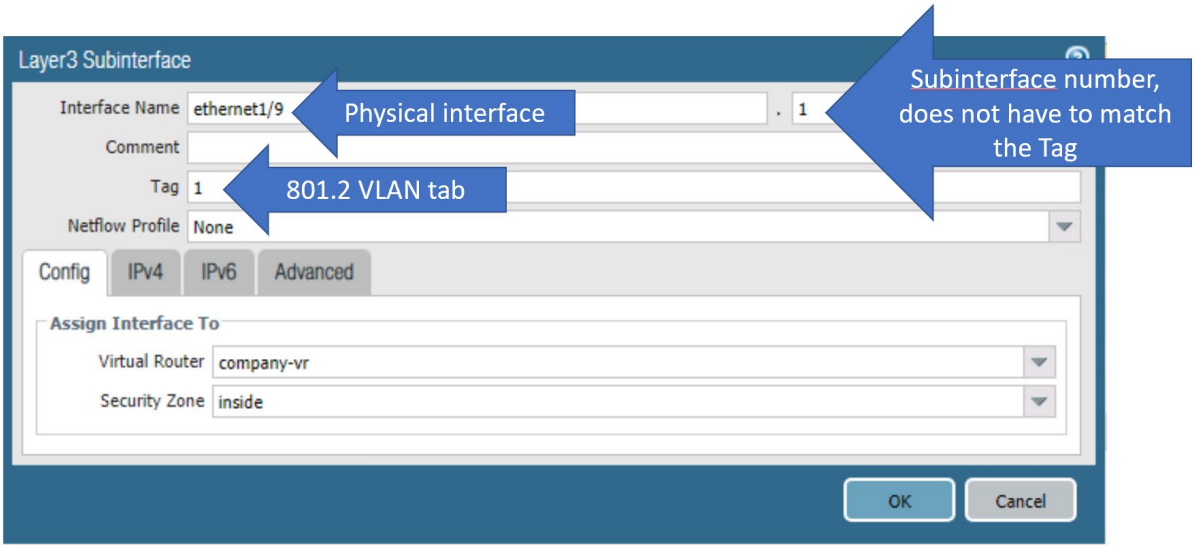


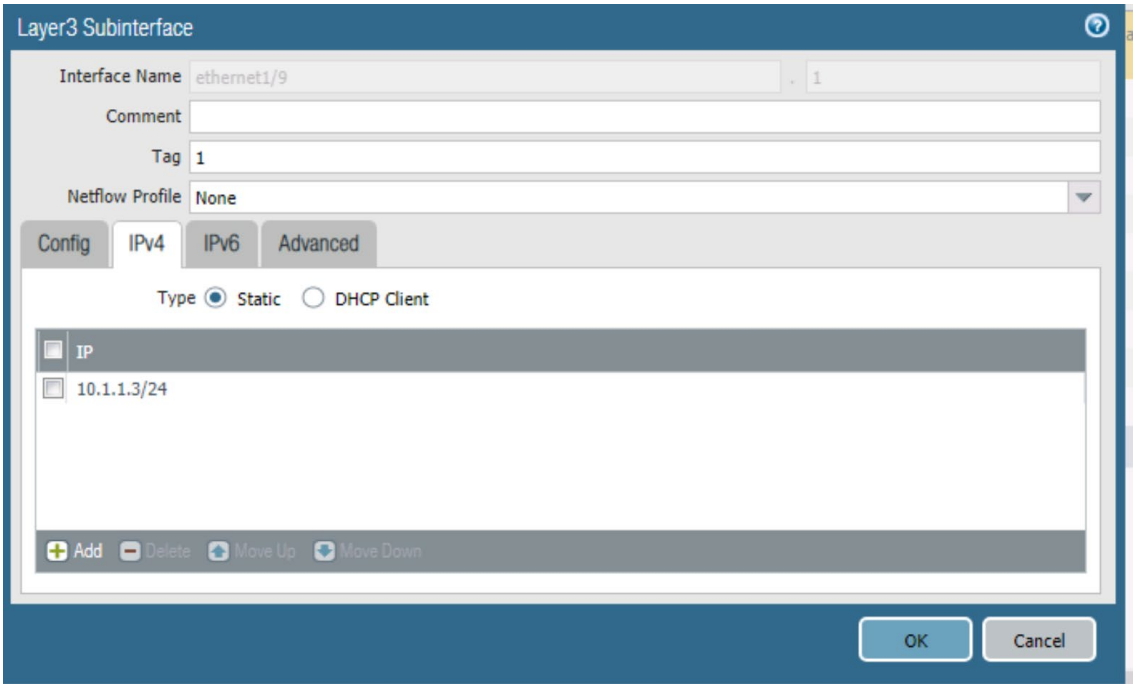
Layer 3 Subinterfaces

For each Ethernet port configured as a physical Layer 3 interface, you can define additional logical Layer 3 interfaces (subinterfaces). Layer 3 subinterfaces possess the same capabilities and features as Layer 3 interfaces, with a difference being that Layer 3 subinterfaces are assigned to 802.1Q VLANs. A Virtual Router object is required to route traffic between each VLAN.



To configure a Layer 3 subinterface, go to **Network > Interfaces > Ethernet**, select a Layer 3 interface, and click **Add Interface.**





Sample questions

52. Which two actions can be done with a Tap interface? (Choose two.)
    A. encrypt traffic
    B. decrypt traffic
    C. allow or block traffic
    D. log traffic
53. Which two actions can be done with a Virtual Wire interface? (Choose two.)
    A. NAT
    B. route
    C. switch
    D. log traffic
54. Which two actions can be done with a Layer 3 interface? (Choose two.)
    A. NAT
    B. route
    C. switch
    D. create a Virtual Wire object
55. Layer 3 interfaces support which two items? (Choose two.)
    A. NAT
    B. IPv6
    C. switching
    D. spanning tree
56. Layer 3 interfaces support which three advanced settings? (Choose three.)
    A. IPv4 addressing
    B. IPv6 addressing
    C. NTP configuration

D. NDP configuration
E. link speed configuration
F. link duplex configuration

57. Layer 2 interfaces support which three items? (Choose three.)
    A. spanning tree blocking
    B. traffic examination
    C. forwarding of spanning tree BPDUs
    D. traffic shaping via QoS
    E. firewall management
    F. routing
58. Which two interface types support subinterfaces? (Choose two.)
    A. virtual wire
    B. Layer 2
    C. loopback
    D. tunnel
59. Which two statements are true regarding Layer 3 interfaces? (Choose two.)
    A. You can configure a Layer 3 interface with one or more as a DHCP client.
    B. You can assign only one IPv4 addresses to the same interface.
    C. You can enable an interface to send IPv4 Router Advertisements by selecting the Enable Router Advertisement check box on the Router Advertisement tab.
    D. You can apply an interface management profile to the interface.

Exam Domain 2 – Simply Passing Traffic

2.7 Given a scenario, identify steps to create and configure a virtual router.

Virtual Routers

Virtual routers obtain routes to remote subnets either by the manual addition of static routes or the dynamic addition of routes using dynamic routing protocols. Each Layer 3 Ethernet, loopback, VLAN, and tunnel interface defined on the firewall must be associated with a virtual router. Although each interface can belong to only one virtual router, you can configure multiple routing protocols and static routes for a virtual router.

Dynamic routing protocols available on a Palo Alto Networks firewall are as follows:

- BGP4
- OSPFv2
- OSPVv3
- RIPv2

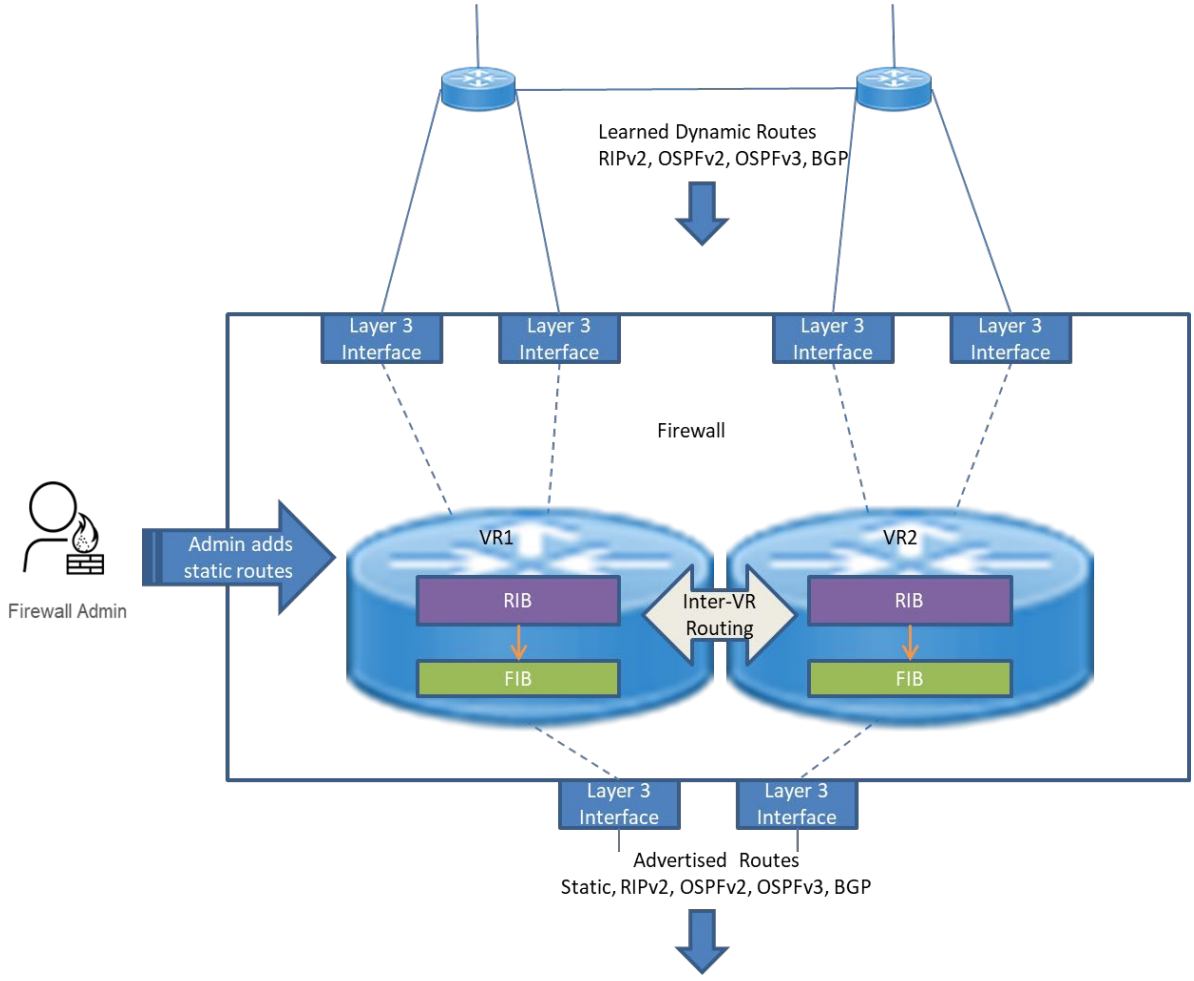
Multicast routing protocols available on a Palo Alto Networks firewall are as follows:

- IGMPv1, IGMPv2, IGMPv3
- PIM-SM, PIM-ASM, PIM-SSM

Dynamic routing protocols have administrative distances applied to them that are used to determine the best route to a destination when multiple routes are available from two different routing protocols. The default administrative distances can be modified.

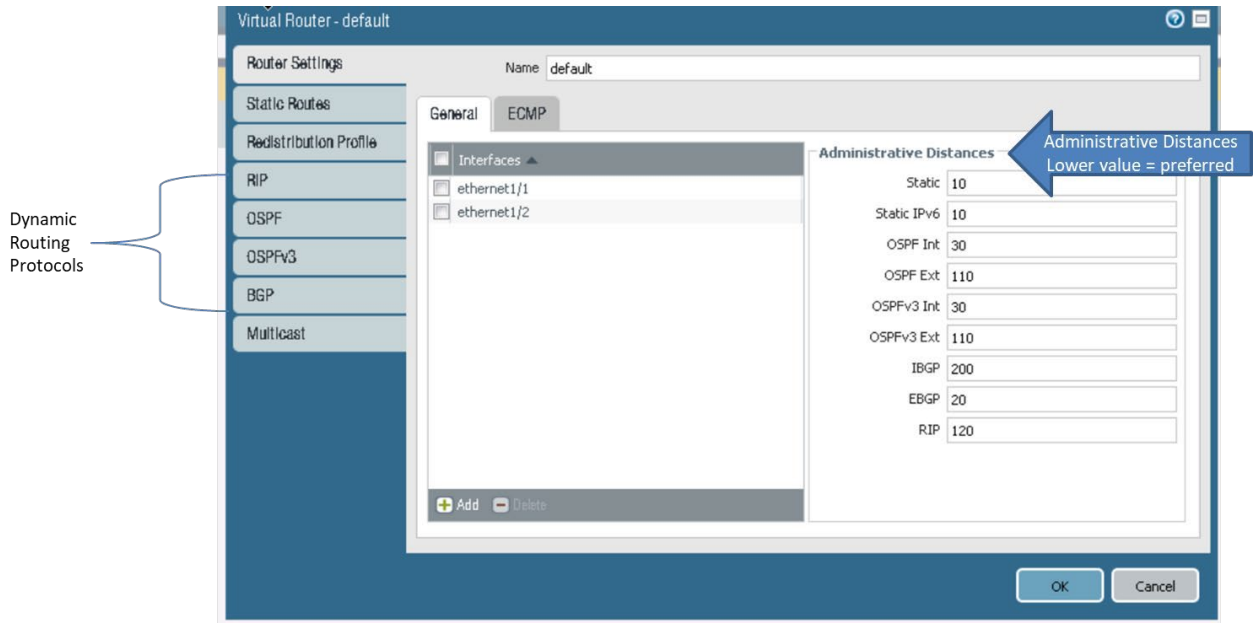
You can create multiple virtual routers, each of which maintains a separate set of routes that aren't shared between these virtual routers, thus enabling you to configure different routing behaviors for different interfaces. Virtual routers can route to other virtual routers within the same firewall if a next hop is specified to reach another virtual router.

The firewall initially populates its learned routes into the firewall's IP routing information base (RIB). The virtual router obtains the best route from the RIB, and then places it in the forwarding information base (FIB). Packets then are forwarded to the next hop router defined in the FIB.



Virtual Router General Configuration Settings

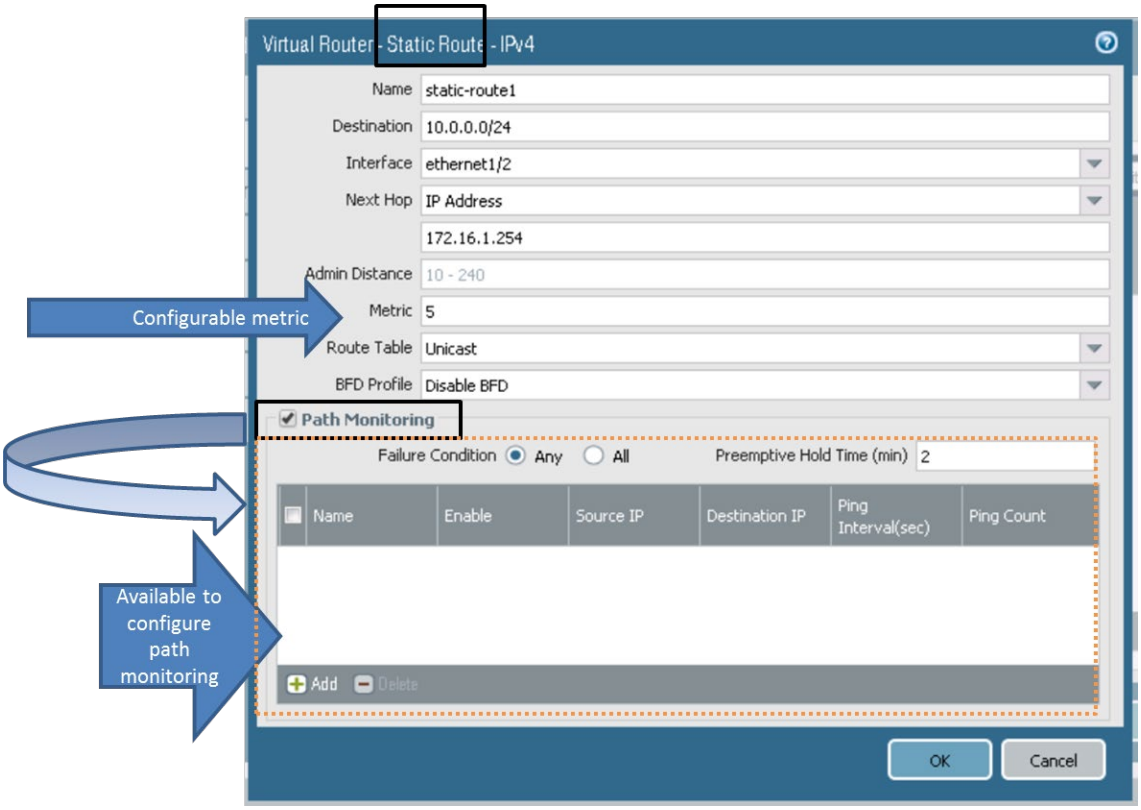
The administrative distances are shown on the right side of the following screencap. Most of these distances are consistent with the values in RFCs, but they can be modified to reflect the needs of your environment.

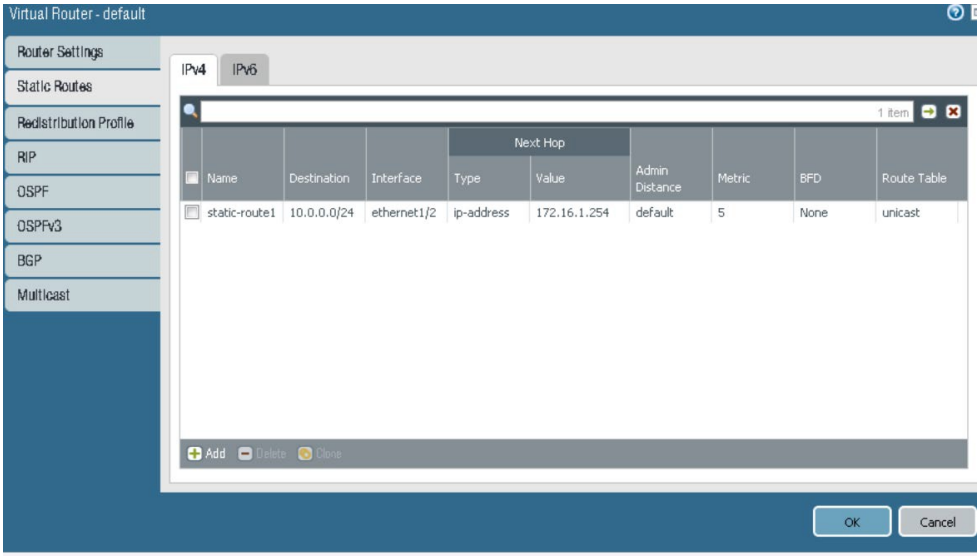


Static Route Configuration Settings

Static routes have the lowest administrative distances by default, other than locally connected routes. This default administrative distance value is 10, which can be changed.

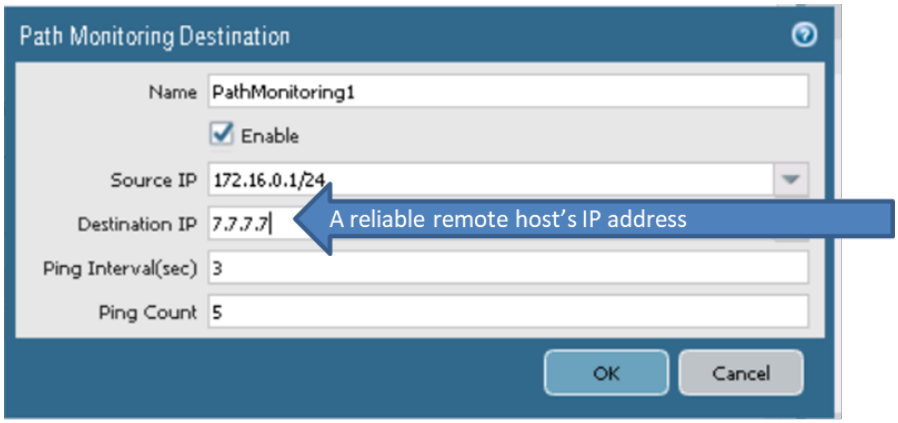
Static routes have a default metric value of 10, which also can be changed. If you have multiple static routes to the same destination, you can make one preferable over the other by changing the metric. The default metric in the following example was changed from its default value of 10 to 5:





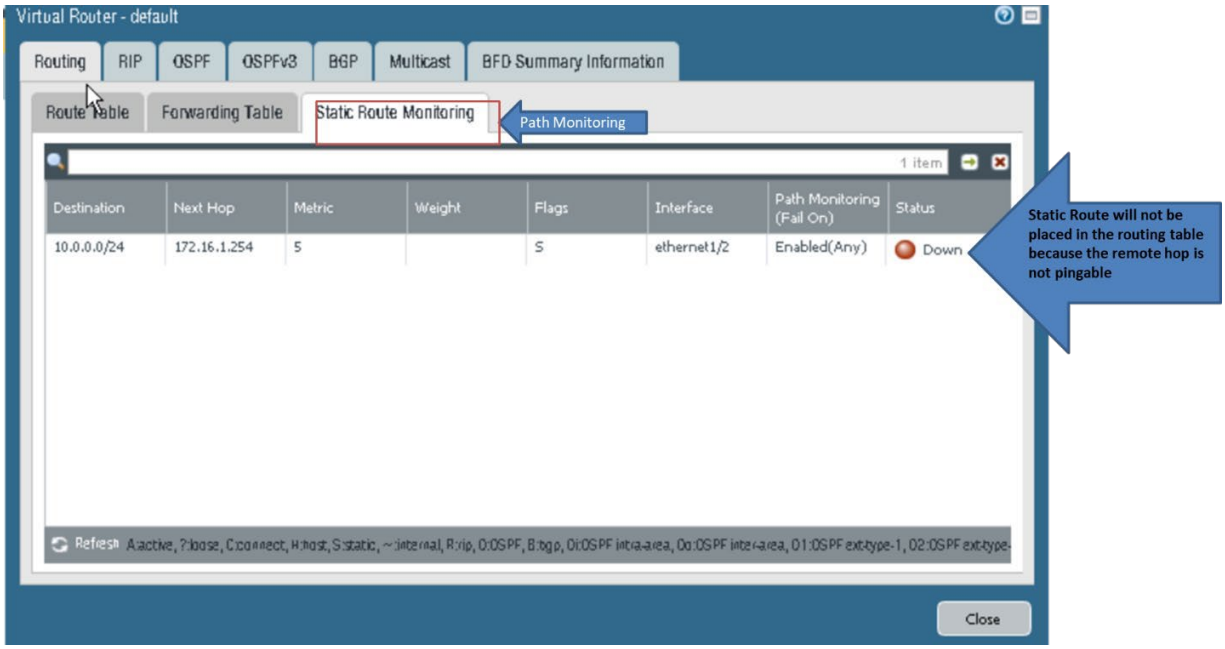
Path Monitoring for Static Routes Configuration Settings

Path monitoring monitors upstream interfaces on remote, reliable devices using ICMP pings. If the path monitoring fails, an associated static route is removed from the routing table. An alternative route then can be used to route traffic.



Path Monitoring	Select to enable path monitoring for the static route.
Failure Condition	Select the condition under which the firewall considers the monitored path down and thus the static route down: • **Any**—If any one of the monitored destinations for the static route is unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. • **All**—If all of the monitored destinations for the static route are unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. Select **All** to avoid the possibility of a single monitored destination signaling a static route failure when that monitored destination is simply offline for maintenance, for example.
Preemptive Hold Time (min)	Enter the number of minutes a downed path monitor must remain in Up state—the path monitor evaluates all of its member monitored destinations and must remain Up before the firewall reinstalls the static route into the RIB. If the timer expires without the link going down or flapping, the link is deemed stable, path monitor can remain Up, and the firewall can add the static route back into the RIB. If the link goes down or flaps during the hold time, path monitor fails and the timer restarts when the downed monitor returns to Up state. A **Preemptive Hold Time** of zero causes the firewall to reinstall the static route into the RIB immediately upon the path monitor coming up. Range is 0-1,440; default is 2.
Name	Enter a name for the monitored destination (up to 31 characters).
Enable	Select to enable path monitoring of this specific destination for the static route; the firewall sends ICMP pings to this destination.
Source IP	Select the IP address that the firewall will use as the source in the ICMP ping to the monitored destination: • If the interface has multiple IP addresses, select one. • If you select an interface, the firewall uses the first IP address assigned to the interface by default. • If you select **DHCP (Use DHCP Client address)**, the firewall uses the address that DHCP assigned to the interface. To see the DHCP address, select **Network** > **Interfaces** > **Ethernet** and in the row for the Ethernet interface, click on **Dynamic DHCP Client**. The IP Address appears in the Dynamic IP Interface Status window.
Destination IP	Enter a robust, stable IP address or address object for which the firewall will monitor the path. The monitored destination and the static route destination must use the same address family (IPv4 or IPv6)
Ping Interval (sec)	Specify the ICMP ping interval in seconds to determine how frequently the firewall monitors the path (pings the monitored destination; range is 1-60; default is 3).
Ping Count	Specify the number of consecutive ICMP ping packets that do not return from the monitored destination before the firewall considers the link down. Based on the **Any** or **All** failure condition, if path monitoring is in failed state, the firewall removes the static route from the RIB (range is 3-10; default is 5). For example, a Ping Interval of 3 seconds and Ping Count of 5 missed pings (the firewall receives no ping in the last 15 seconds) means path monitoring detects a link failure. If path monitoring is in failed state and the firewall receives a ping after 15 seconds, the link is deemed up; based on the **Any** or **All** failure condition, path monitoring to **Any** or **All** monitored destinations can be deemed up, and the Preemptive Hold Time starts.

This static route is removed from the routing table until reachability to the next hop is obtained.



Virtual Router Forwarding Information Base

The following screenshot shows the CLI output of the FIB. A GUI runtime display also is available.

```
admin@firewall-a> show routing fib

total virtual-router shown :              1


--------------------------------------------------------------------------------
virtual-router name: default
interfaces:
   ethernet1/1 ethernet1/2


route table:
flags: u - up, h - host, g - gateway, e - ecmp, * - preferred path

maximum of fib entries for device:                2500
maximum of IPv4 fib entries for device:           2500
maximum of IPv6 fib entries for device:           2500
number of fib entries for device:                 4
maximum of fib entries for this fib:              2500
number of fib entries for this fib:               4
number of fib entries shown:                      4

id      destination           nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
9       10.0.0.0/24           0.0.0.0            u      ethernet1/1        1500
8       10.0.0.1/32           0.0.0.0            uh     ethernet1/1        1500
4       172.16.0.0/24         0.0.0.0            u      ethernet1/2        1500
3       172.16.0.1/32         0.0.0.0            uh     ethernet1/2        1500
--------------------------------------------------------------------------------
```

Sample questions

60. What is the default administrative distance of a static route within the PAN-OS software?
    A. 1
    B. 5
    C. 10
    D. 100
61. Which two dynamic routing protocols are available in the PAN-OS software? (Choose two.)
    A. RIP1
    B. RIPv2
    C. OSPFv3
    D. EIGRP
62. Which value is used to distinguish the preference of routing protocols?
    A. metric
    B. weight
    C. distance
    D. cost
    E. administrative distance

63. Which value is used to distinguish the best route within the same routing protocol?
    A. metric
    B. weight
    C. distance
    D. cost
    E. administrative distance
64. In path monitoring, what is used to monitor remote network devices?
    A. ping
    B. SSL
    C. HTTP
    D. HTTPS
    E. link state

Exam Domain 2 – Simply Passing Traffic

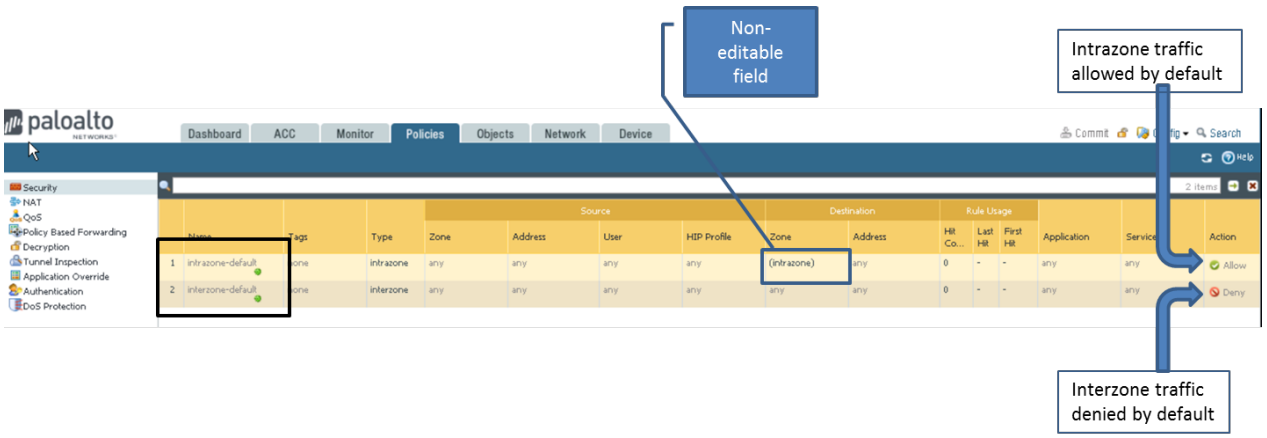
2.8 Identify the purpose of specific security rule types.

Security Rule Types

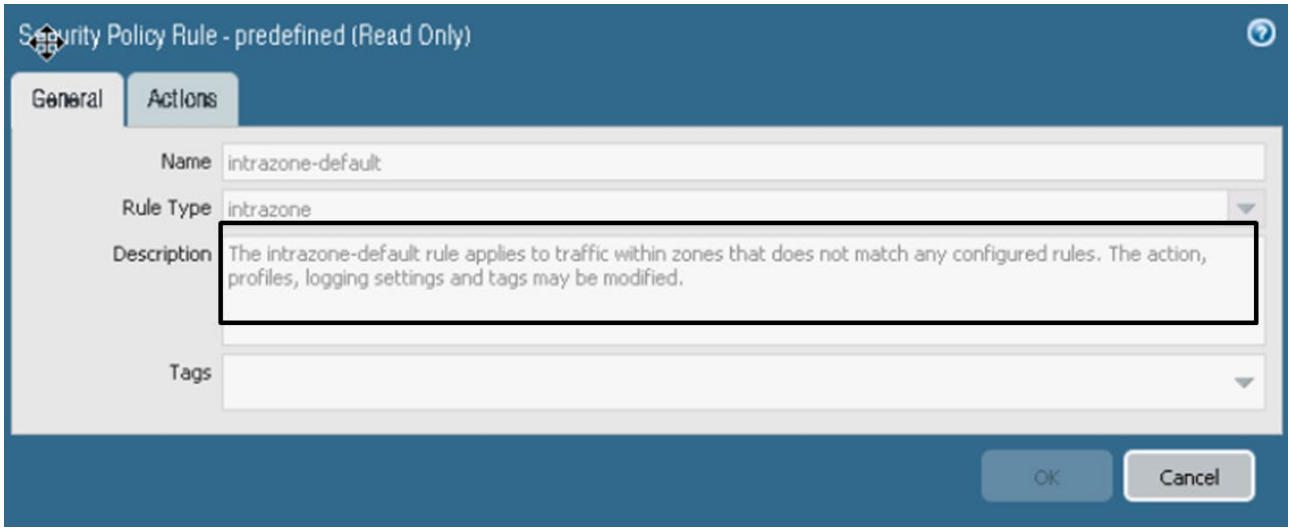
Security policies allow you to enforce rules and take action, and they can be as general or as specific as needed. The list of policy rules are compared from the top down against the incoming traffic. The more specific rules must precede the more general ones, because the first rule that matches the traffic is applied.

The default rules apply for traffic that doesn't match any user-defined rules. These default rules are displayed at the bottom of the security rulebase. The default rules are predefined rules that are part of the predefined configuration and are read-only by default; you can override them and change a limited number of settings, including the tags, action (allow or deny), log settings, and security profiles. The names for the two default rules are intrazone-default and interzone-default.

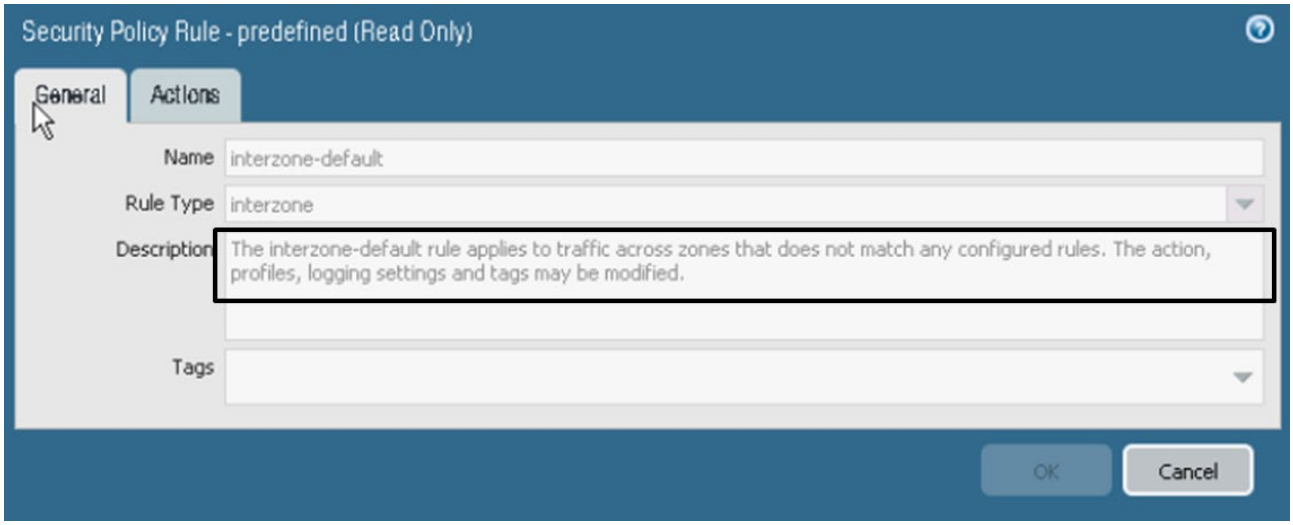
Default Rules: Intrazone Default and Interzone Default



Intrazone Security Policy



Interzone Security Policy



The following table describes the three types of security policy:

Rule Type	Description
Intrazone • Default rule • Displayed at the bottom of the security rulebase	A security policy rule allowing traffic within the same zone. Intrazone rule types apply to all matching traffic within the specified source zones (a destination zone cannot be specified for intrazone rules). For example, if the source zone is being set to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B. Traffic logging is not enabled by default. However, best practice is to log the end-of-session traffic.

Interzone • default rule • Displayed at the bottom of the security rulebase	A security policy rule allowing traffic between two different zones. However, the traffic within the same zone will not be allowed when the policy is created as type Interzone. Interzone rule types apply to all matching traffic between the specified source and destination zones. For example, if the source zone is being set to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not to traffic within zones A, B, or C. Traffic logging is not enabled by default. However, best practice is to log the traffic.
Universal • Exists above the intrazone and interzone security policies	By default, all the traffic destined between two zones, regardless of whether it is from the same zone or different zone. Universal rule types apply to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if a universal rule is being created with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A. Traffic logging is enabled by default.

Sample questions

65. What are the two default (predefined) security policy rule types in PAN-OS software? (Choose two.)
    A. Universal
    B. Interzone
    C. Intrazone
    D. Extrazone
66. True or false. Because the first rule that matches the traffic is applied, the more specific rules must follow the more general ones.
    A. true
    B. false
67. Which statement is true?
    A. For Intrazone traffic, traffic logging is enabled by default.
    B. For Interzone traffic, traffic logging is enabled by default.
    C. For Universal traffic, traffic logging is enabled by default.
    D. For any rule type, traffic logging is enabled by default.

Exam Domain 2 – Simply Passing Traffic

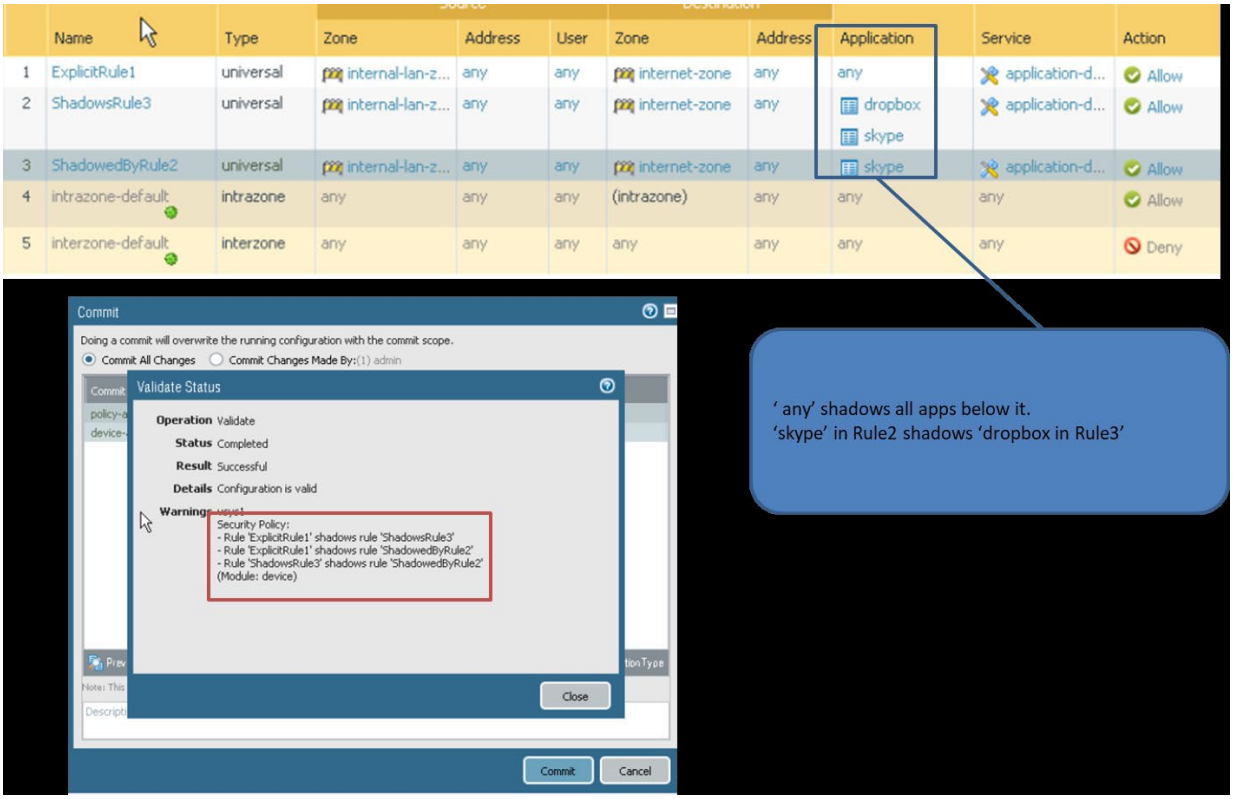
2.9 Identify and configure security policy match conditions, actions, and logging options.

Implicit and Explicit Rules

Two implicit (predefined) security policy rules come with the PAN-OS software: intrazone and interzone. The intrazone security policy rule allows traffic within a zone by default. The interzone security policy does not allow traffic between zones by default. These two predefined security policy rule types reside at the bottom of the security rulebase set, and are processed after all other preceding security policy rules are processed. All preceding security rules must be explicitly defined by an administrator. Note that traffic is not logged by default for the predefined rules and that traffic is logged by default for explicitly defined rules. Best practice is to log for all security policy rules, whether implicit or explicit.

A shadow rule warning indicates that a broader rule matching the criteria is configured above a more specific rule.

The following screenshot shows that no traffic ever will match the second rule, which specifically allows skype and dropbox, because all applications already have been allowed by the first rule. Rule 2's "skype" shadows rule 3's "skype."

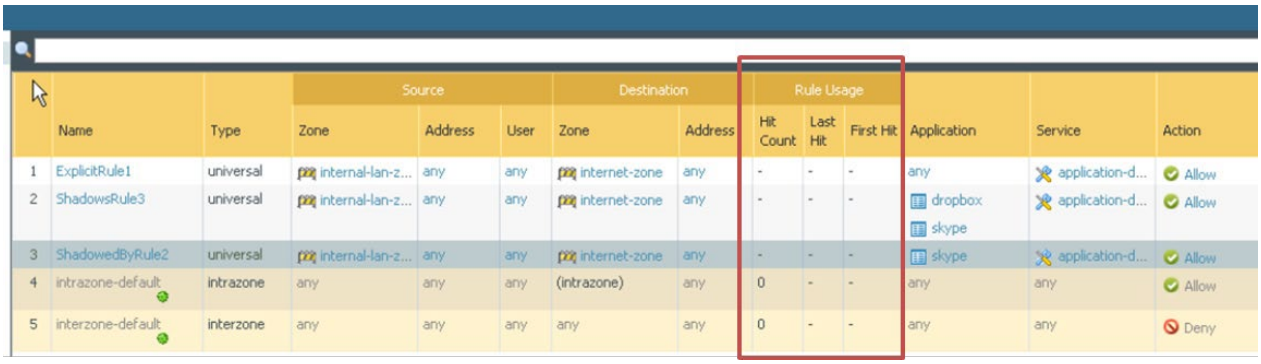


Security Rule Hit Count

The PAN-OS software enables you to monitor hit count. The three components of **Rule Usage** are as follows:

- **Hit Count:** The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, data-plane restarts, and upgrades unless you manually reset or rename the rule.
- **Last Hit:** The most recent timestamp for when traffic matched the rule
- **First Hit:** The first instance when traffic was matched to this rule

In the following screenshot, note that the hit counts have not incremented because this example has no live traffic:



Sample questions

68. What are the two default (predefined) security policy rule types in PAN-OS software? (Choose

two.)

A. Universal
B. Interzone
C. Intrazone
D. Extrazone

69. True or false? Best practice is to enable logging for the two predefined security policy rules.
    A. true
    B. false
70. What will be the result of one or more occurrences of shadowing?
    A. a failed commit
    B. an invalid configuration
    C. a warning
    D. an alarm window
71. Which type of security policy rules most often exist above the two predefined security policies?
    A. Intrazone
    B. Interzone
    C. Universal
    D. Global

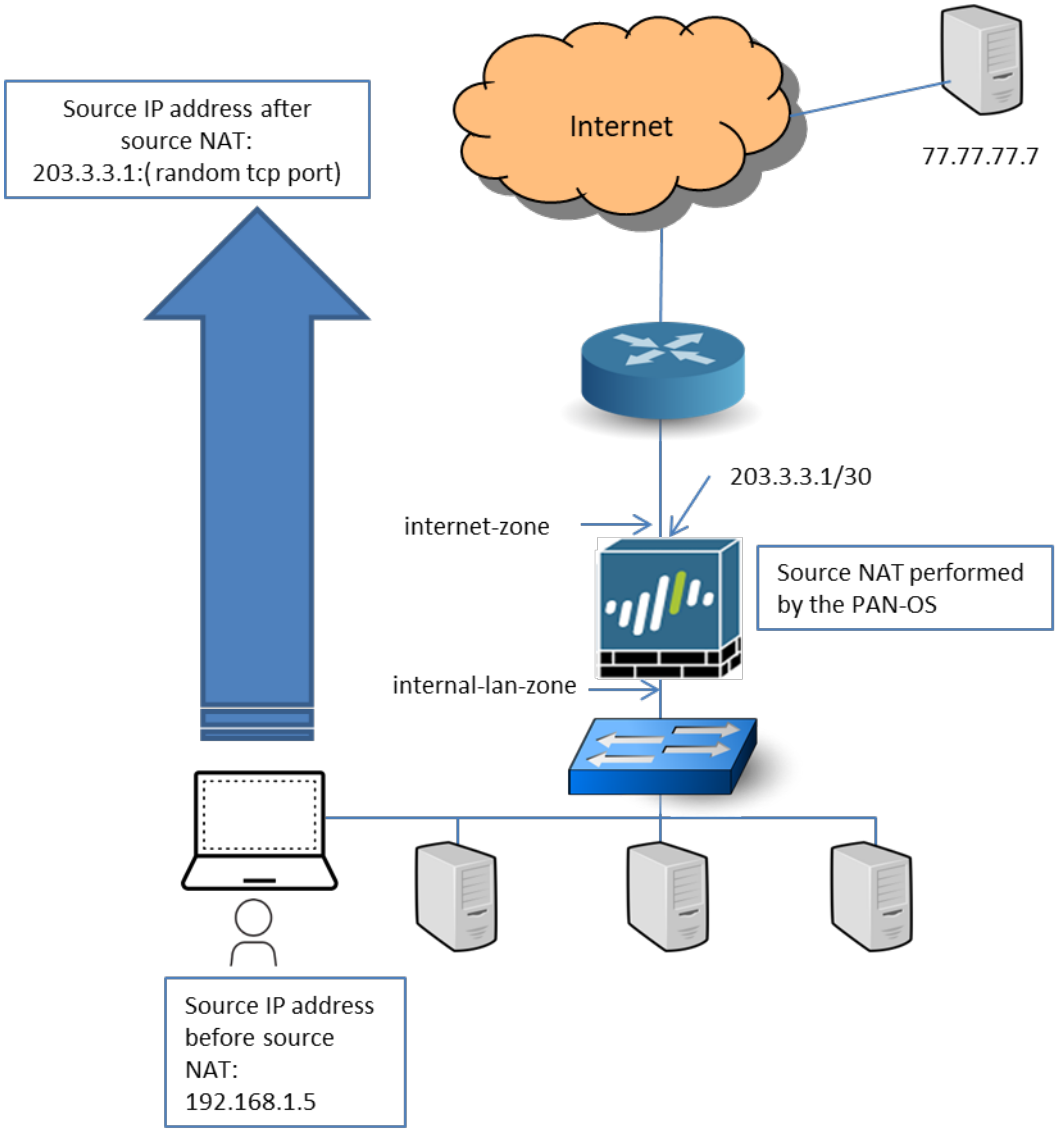
Exam Domain 2 – Simply Passing Traffic

2.10 Given a scenario, identify and implement the proper NAT solution.

NAT Types

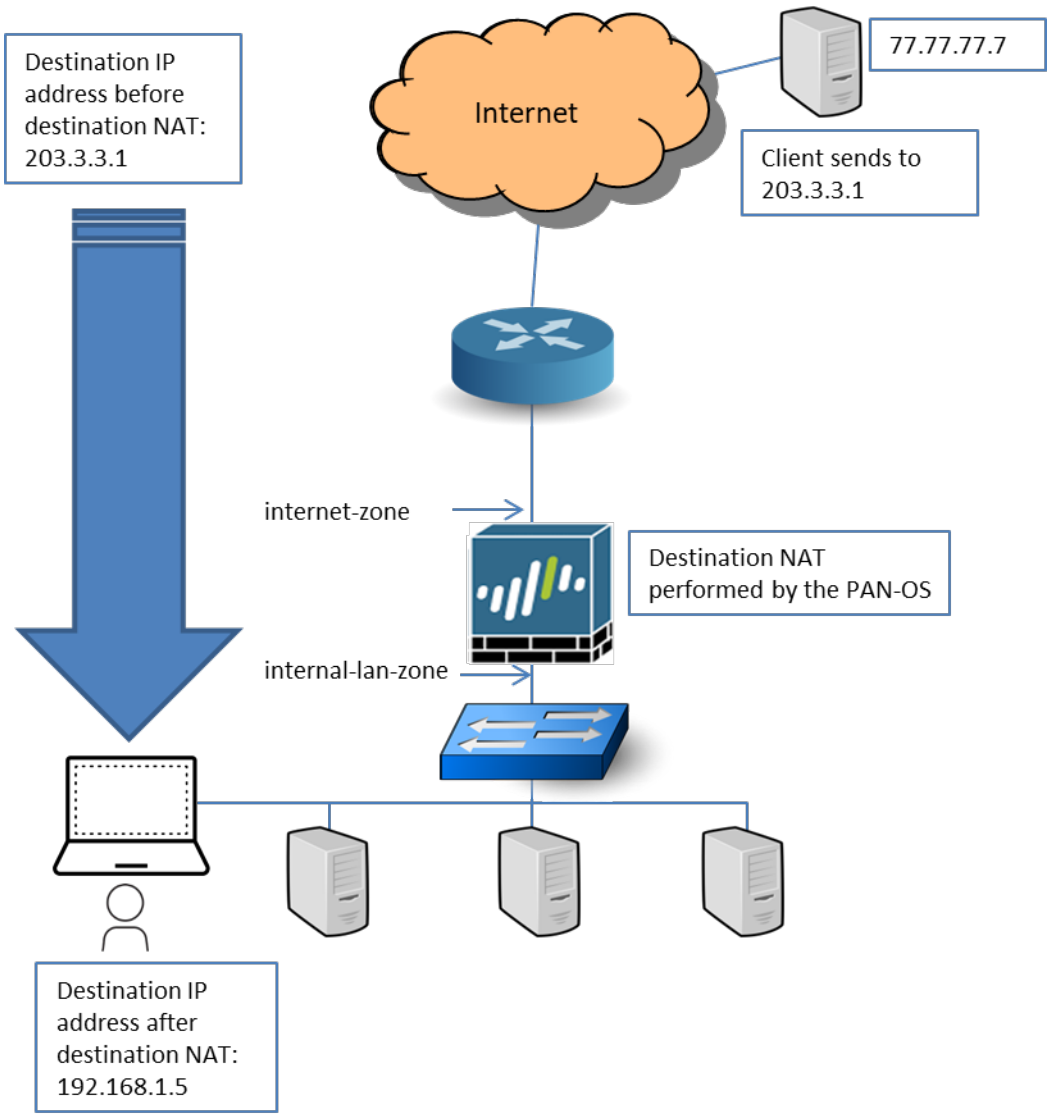
The two basic types of NAT are source NAT (SNAT) and destination NAT (DNAT).

SNAT is used to replace the original source IP address in a packet. A typical scenario for SNAT is when a packet is originated from within a company's network and then is forwarded out to the internet. The original source IP address usually is an RFC 1918 IP address that is not routable within the internet.



DNAT is used to replace the original destination IP address in a packet. A typical scenario for DNAT is when a packet is originated from the internet and then is forwarded to a company's internal network. The original destination IP is routable within the internet. When the packet arrives at the firewall, the routable IP address is replaced with the real IP address of the destination device (usually an RFC 1918 IP address) and then is forwarded to the destination device.

DNAT can be used in other scenarios such as when subnets overlap.

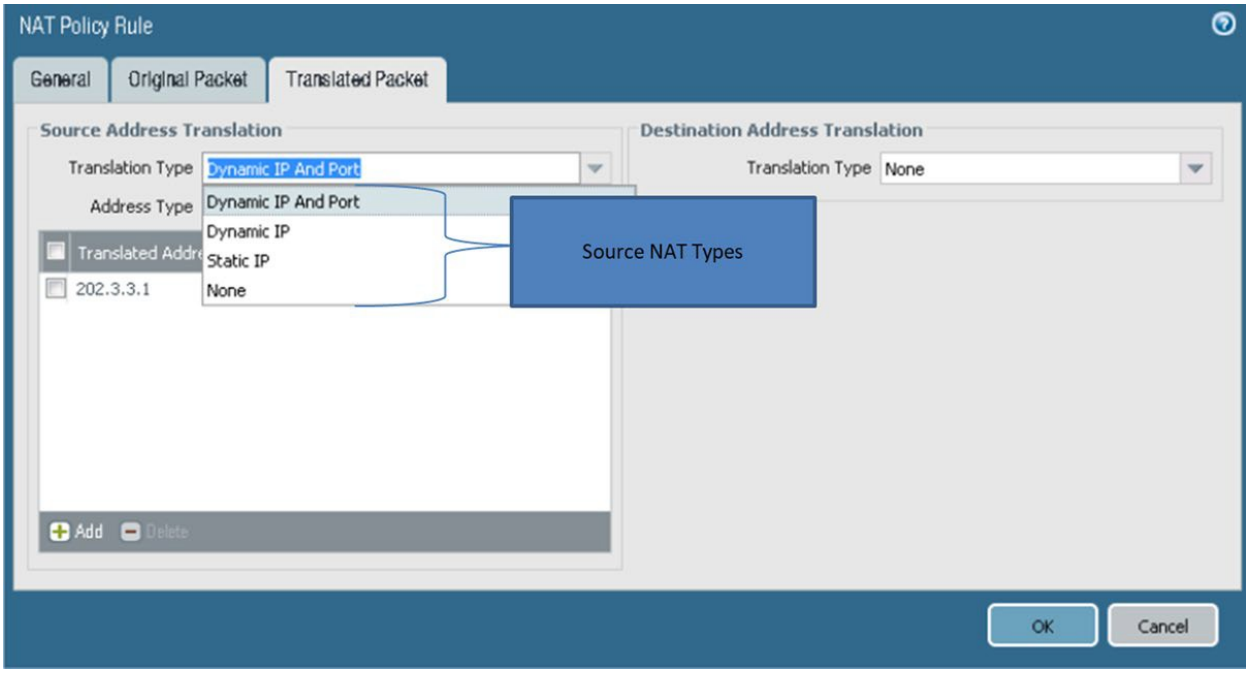


Source NAT Types

The following table describes the three source NAT types: static IP, dynamic IP, and dynamic IP and port:

Source NAT Type	Description
Static IP	The same address always is used for the translation and the port is unchanged. For example, if the source range is 192.168.0.1 – 192.168.0.10, and the translation range is 10.0.0.1 – 10.0.0.10, address 192.168.0.2 always is translated to 10.0.0.2. The address range usually is limited. This concept applies if only a host /32 IP address is used.
Dynamic IP	The original source IP address translates to the next available address in the specified range but the port number remains unchanged. Up to 32,000 consecutive IP address are supported. A dynamic IP pool can contain multiple subnets, so you can translate your internal network addresses to two or more separate public subnets.

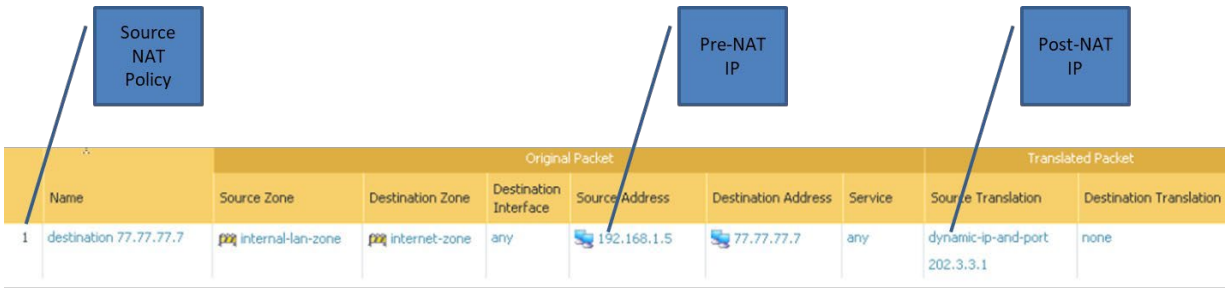
Source NAT Type	Description
Dynamic IP and port	This is the most commonly used source NAT type. Address selection is based on a hash of the source IP address. For a given source IP address, the firewall uses the same translated source address for all sessions.

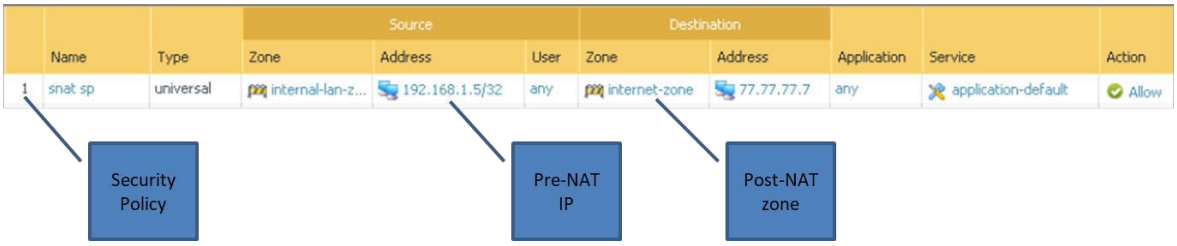


Source NAT and Security Policies

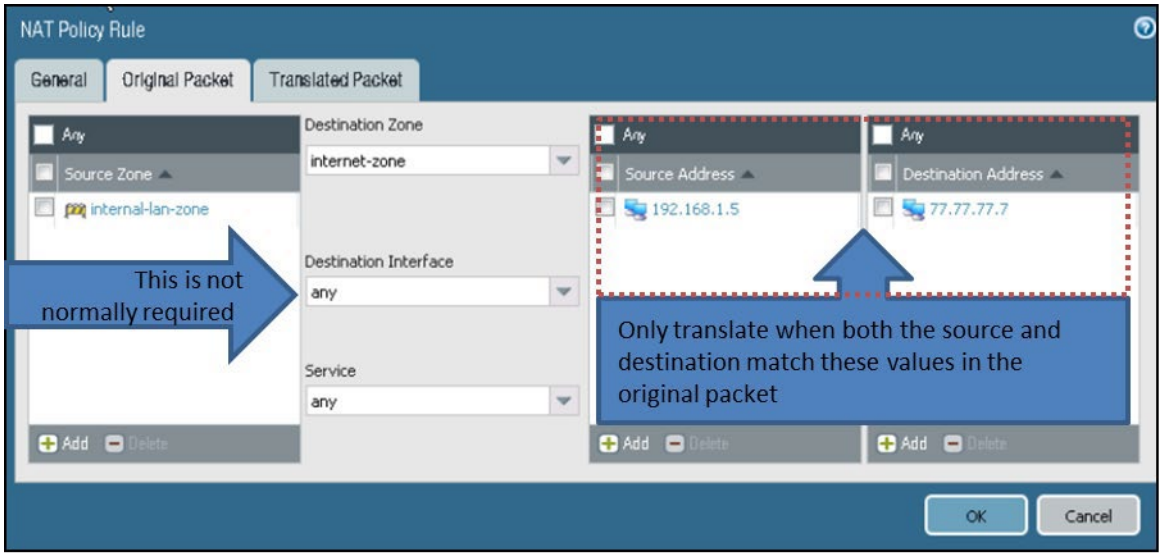
A security policy rule requires a source IP, destination IP, source zone, and destination zone. If you use an IP address in a security policy rule, you must add the IP address value that existed before NAT was implemented, which is called the pre-NAT IP. After the IP address is translated (post-NAT IP), determine the zone where the post-NAT IP address would exist. This post-NAT zone is used in the Security policy rule.

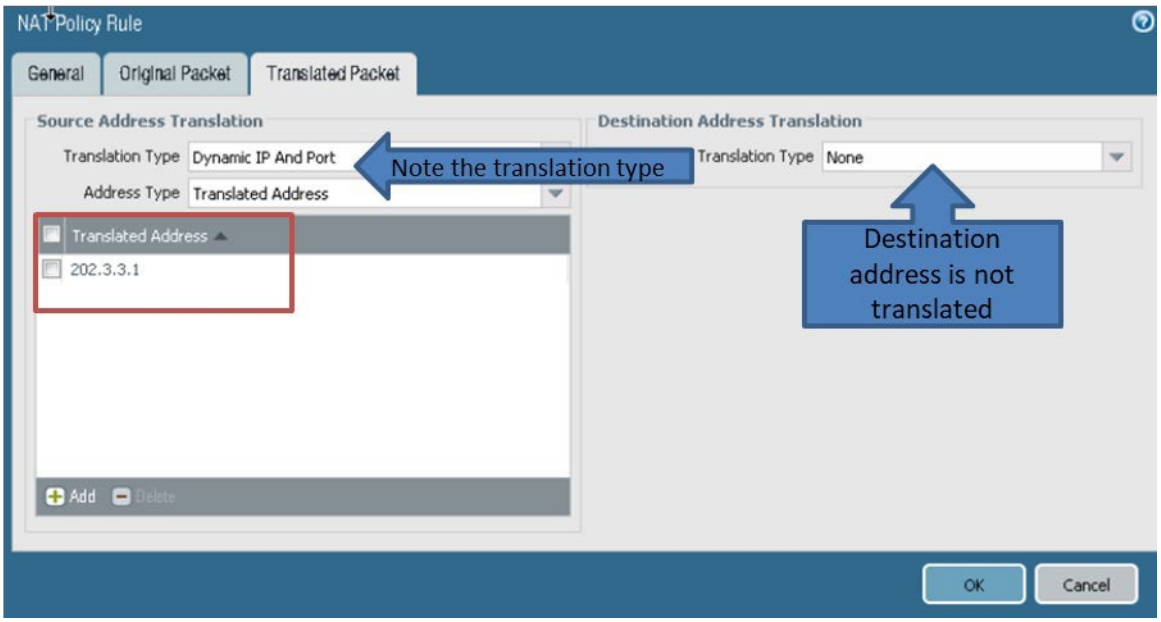
A simple way to remember how to configure security policy rules where NAT was implemented is to memorize the following: “pre-NAT IP; post-NAT zone.”





Configuring Source NAT





Configuring Bidirectional Source NAT

For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure. If you are configuring static source NAT, bidirectional NAT enables you to eliminate the need to create an additional NAT policy rule for the incoming traffic.

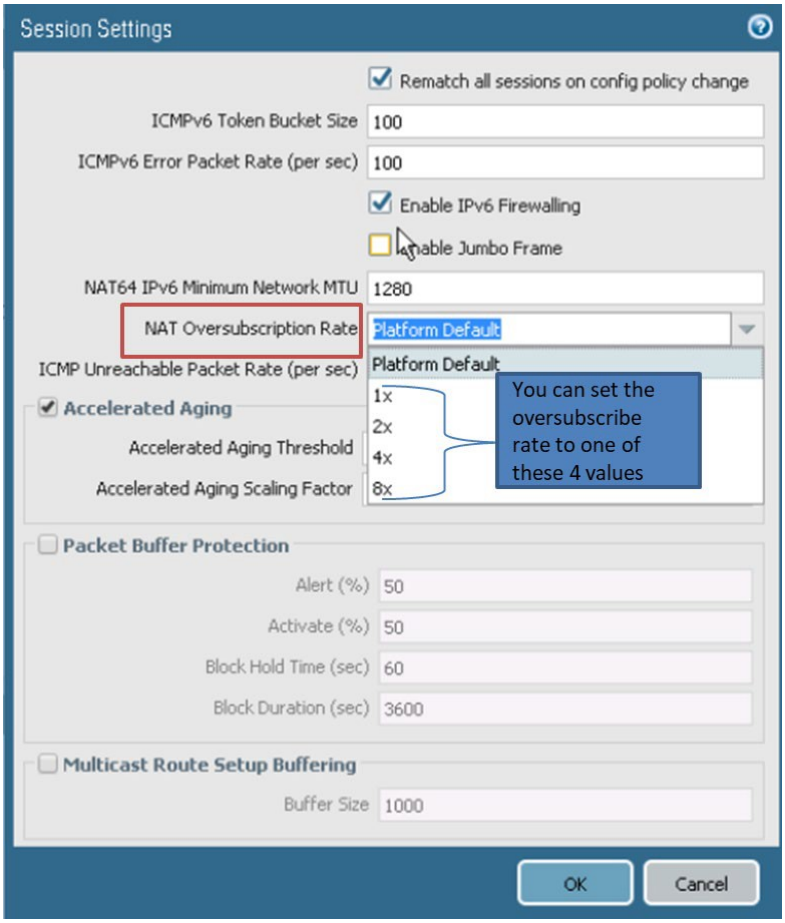
If you enable bidirectional translation, you must ensure that you have security policy rules in place to control the traffic in both directions. If there are no such rules, the bidirectional feature allows packets to be translated automatically in both directions.

DIPP NAT Oversubscription

The DIPP **NAT Oversubscription Rate** is the number of times that the same translated IP address and port pair can be used concurrently. Reduction of the oversubscription rate will decrease the number of source device translations but will provide higher NAT rule capacities. Oversubscription assumes that the destination is different in each translation.

Platform Default turns off oversubscription, whereby the default rate of the firewall model applies:

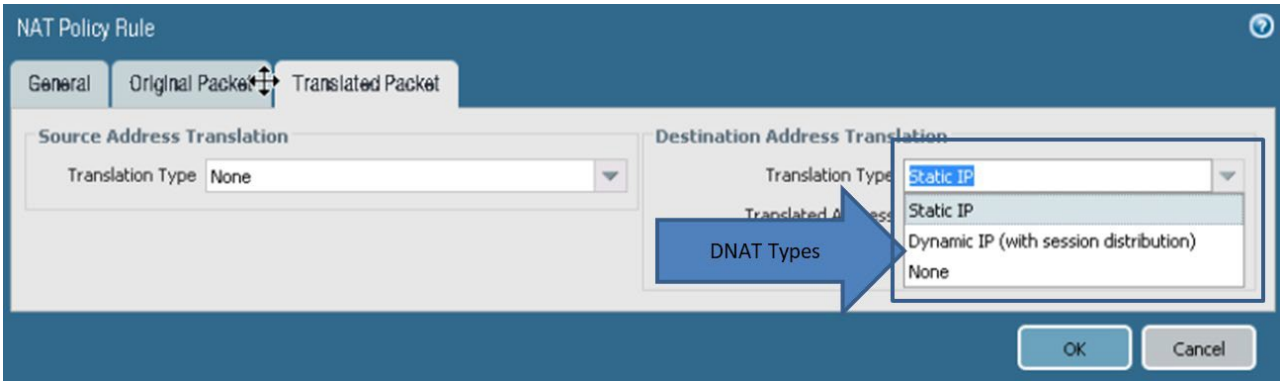
- 1x: means no oversubscription, where each IP address and port pair can be used only one time
- 2x: oversubscribed two times
- 4x: oversubscribed three times
- 8x: oversubscribed eight times



Destination NAT Types

Destination NAT (DNAT) typically is used to allow an external client to initiate access to an internal host such as a web server. The two types of destination NAT are as follows:

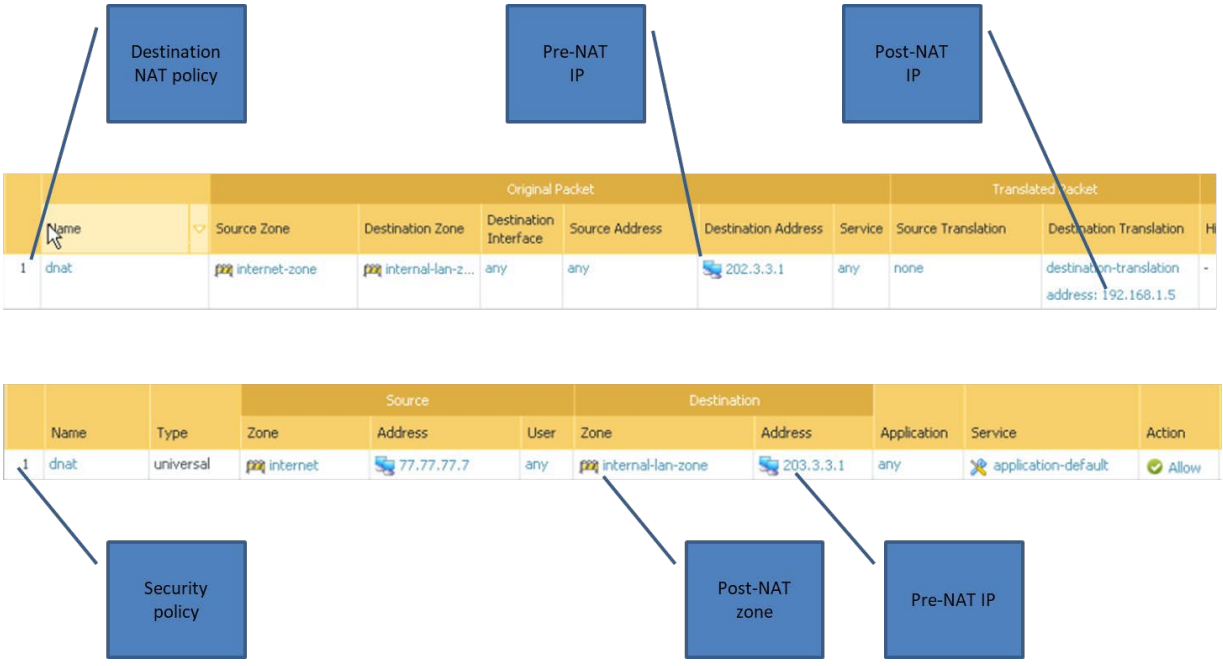
Destination NAT Type	Description
Static	You can set the translated address as an IP address or range of IP addresses and a translated port number (1 – 65,535), to which the original destination address and port number are translated. If the **Translated Port** field is blank, the destination port is not changed.
Dynamic IP (with session distribution)	You can enter a translated address that is an FQDN, an address object, or an address group from which the firewall selects the translated address. If the DNS server returns more than one address for an FQDN or if the address object or address group translates into more than one IP address, the firewall distributes sessions among those addresses using the specified session distribution method.



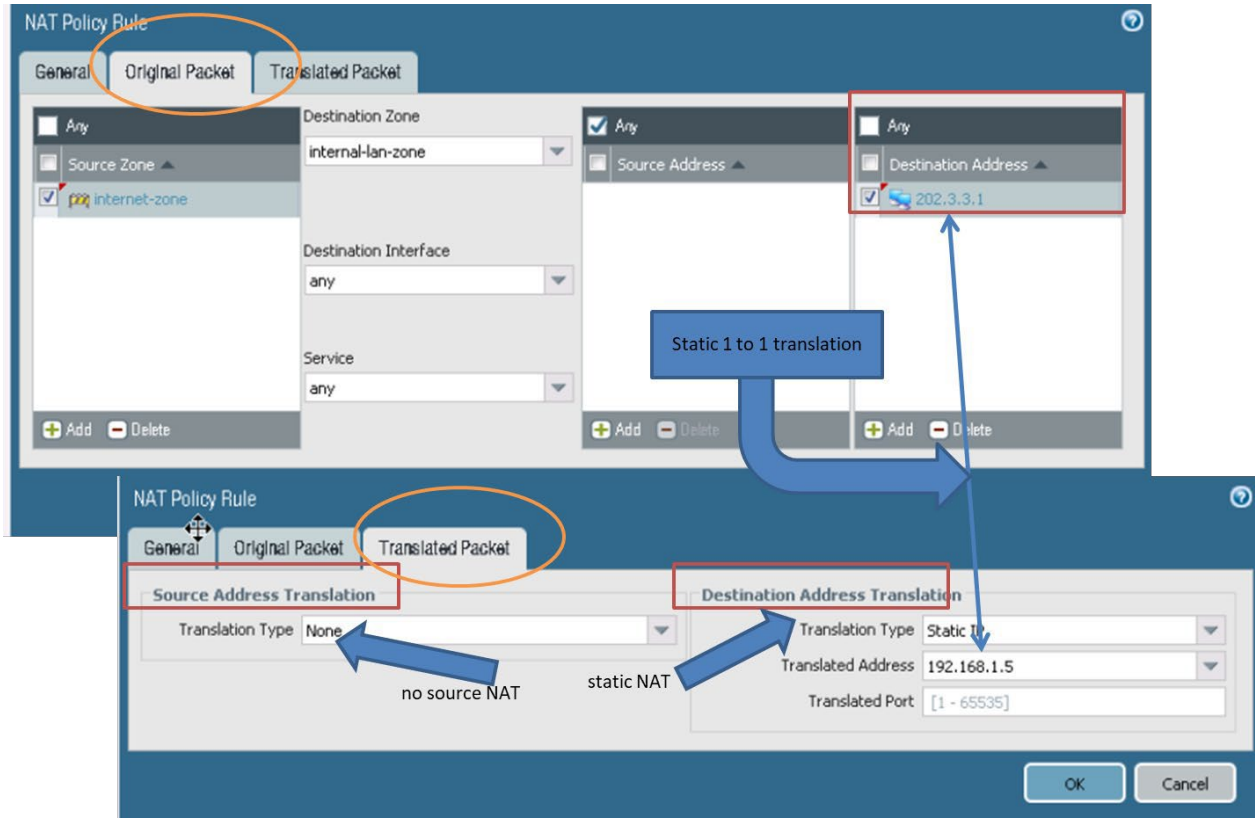
Destination NAT and Security Policies

A security policy rule requires a source IP, destination IP, source zone, and destination zone. If you use an IP address in a security policy rule, you must add the IP address value that existed before NAT was implemented, which is called the pre-NAT IP. After the destination IP address is translated (post-NAT IP), determine the zone where the post-NAT IP address would exist. This post-NAT zone is used in the security policy rule.

A simple way to remember how to configure security policy rules where NAT was implemented is to memorize the following: “pre-NAT IP; post-NAT zone.”

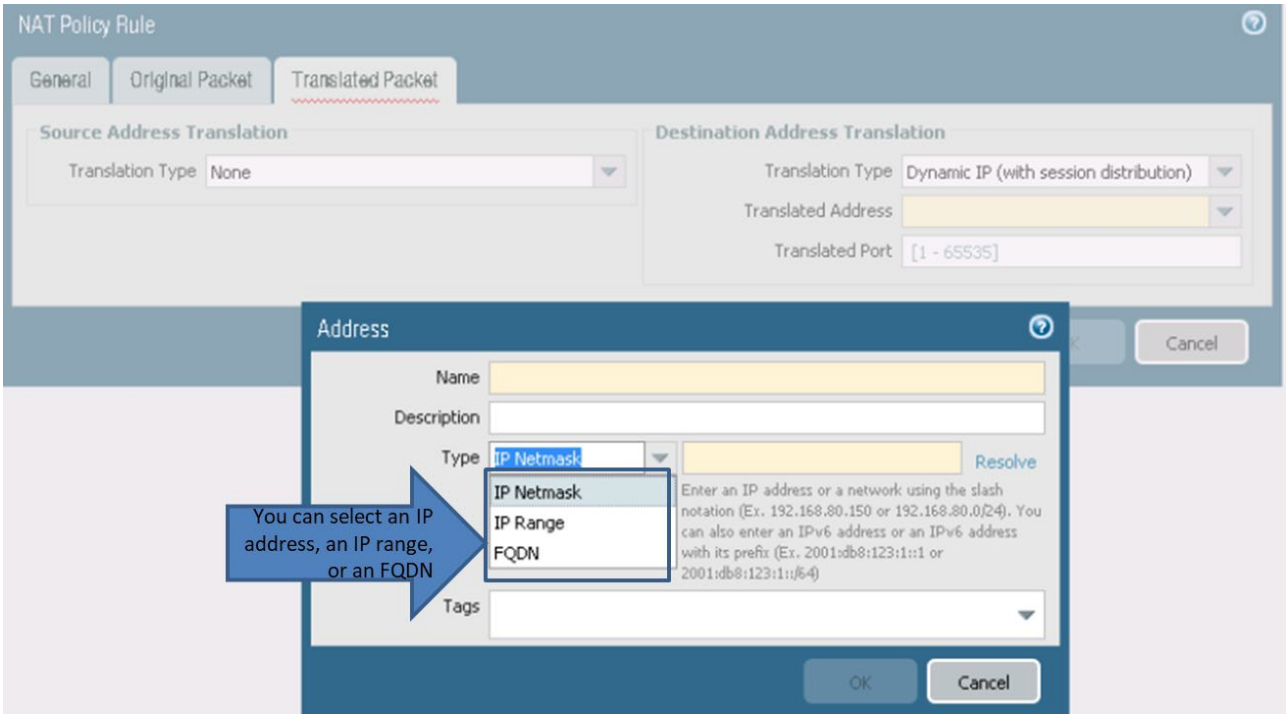


Configuring Destination NAT

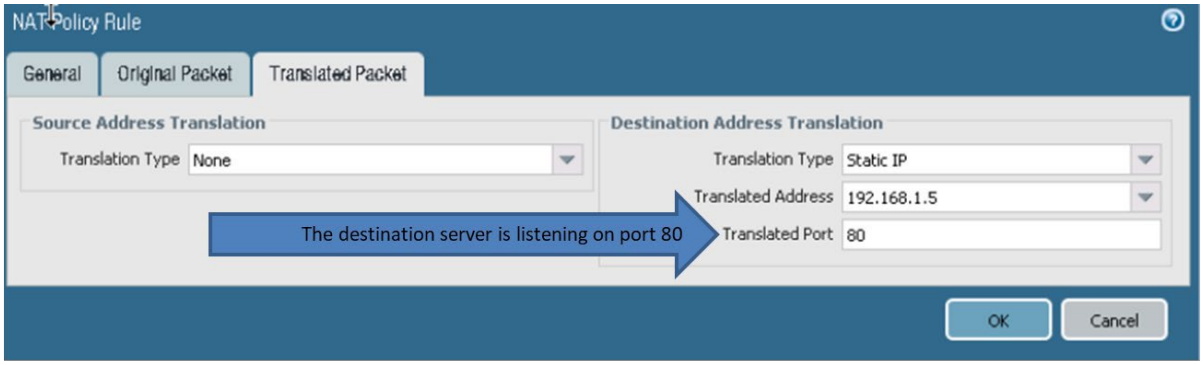


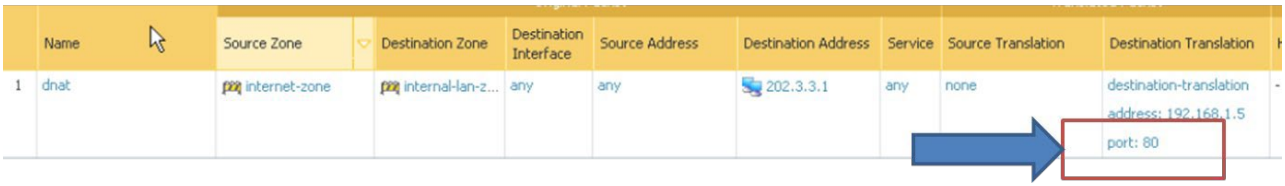
Configuring Dynamic IP Address Support for DNAT

You can enter a translated address that is an FQDN, an address object, or an address group from which the firewall selects the translated address. If the DNS server returns more than one address for an FQDN or if the address object or address group translates into more than one IP address, the firewall distributes sessions among those addresses using the specified session distribution method.



Configuring Destination NAT Port Forwarding





Sample questions

72. What are two source NAT types? (Choose two.)
    A. universal
    B. static
    C. dynamic
    D. extrazone
73. A simple way to remember how to configure security policy rules where NAT was implemented is to memorize the following:
    A. post-NAT zone, post-NAT zone
    B. post-NAT IP, post-NAT zone
    C. pre-NAT IP, post-NAT zone
    D. pre-NAT IP, pre-NAT zone
74. What are two types of destination NAT? (Choose two.)
    A. dynamic IP (with session distribution)
    B. DIPP
    C. global
    D. static
75. What are two possible values for DIPP NAT oversubscription? (Choose two.)
    A. 1x
    B. 4x
    C. 16x
    D. 32x
76. Which statement is true regarding bidirectional NAT?
    A. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
    B. For static translations, bidirectional NAT enables the firewall to create a corresponding

translation in the same direction of the translation you configure.

C. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.

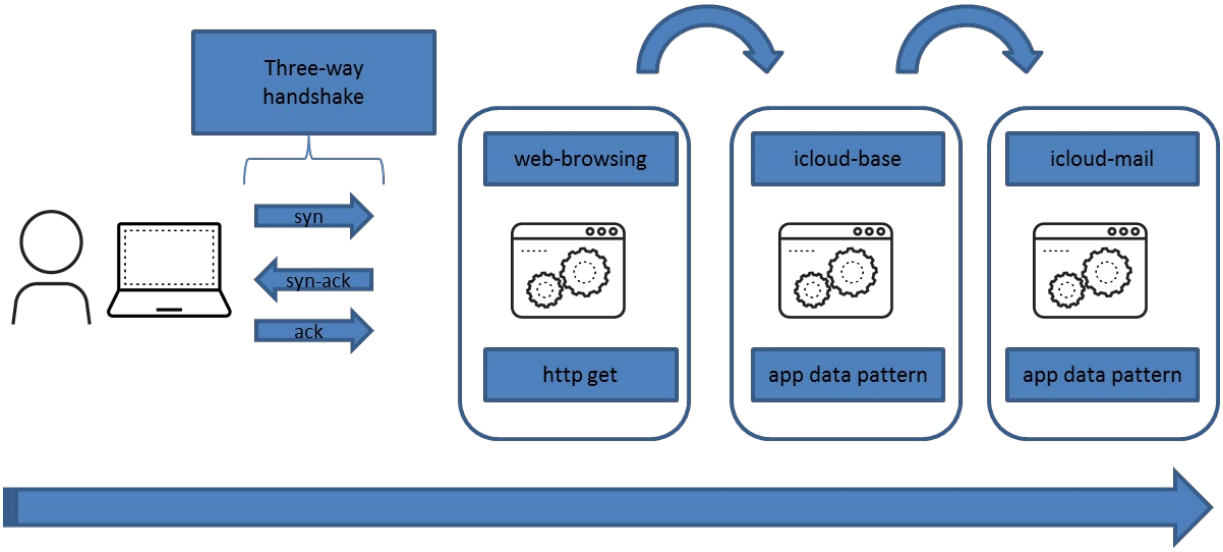
D. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction of the translation you configure.

Exam Domain 3 – Traffic Visibility

3.1 Given a scenario, select the appropriate application-based security policy rules.

Application Shifts

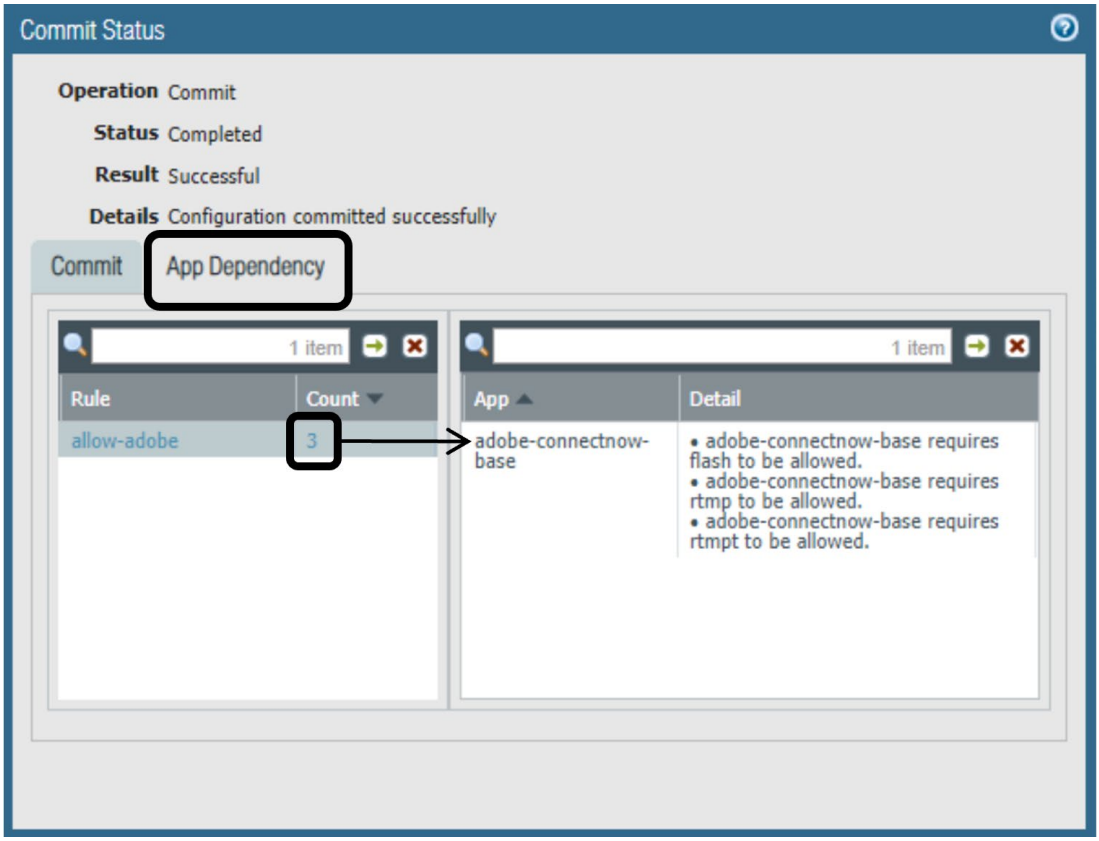
Applications can change during the lifetime of a session. This behavior is called an "application shift." For example, a user types **www.icloud.com** into a web browser to access their iCloud email. This initial request goes out as an HTTP request, and the application is recognized as web-browsing. After the HTTP request is completed, the application is changed to icloud-base. After the icloud-base application is processed, the application changes to icloud-mail.



Dependent Applications

Some applications within PAN-OS software are dependent on other applications, which means that if Application#1 is dependent on Application#2, then both Application#1 and Application#2 need to be allowed in the security policy. For example, icloud-mail is dependent on icloud-base, therefore both applications need to be allowed in the security policy. Also, icloud-base is dependent on web-browsing, so the web-browsing application also needs to be added to security policy. Additional dependent applications are shown in the following figure.

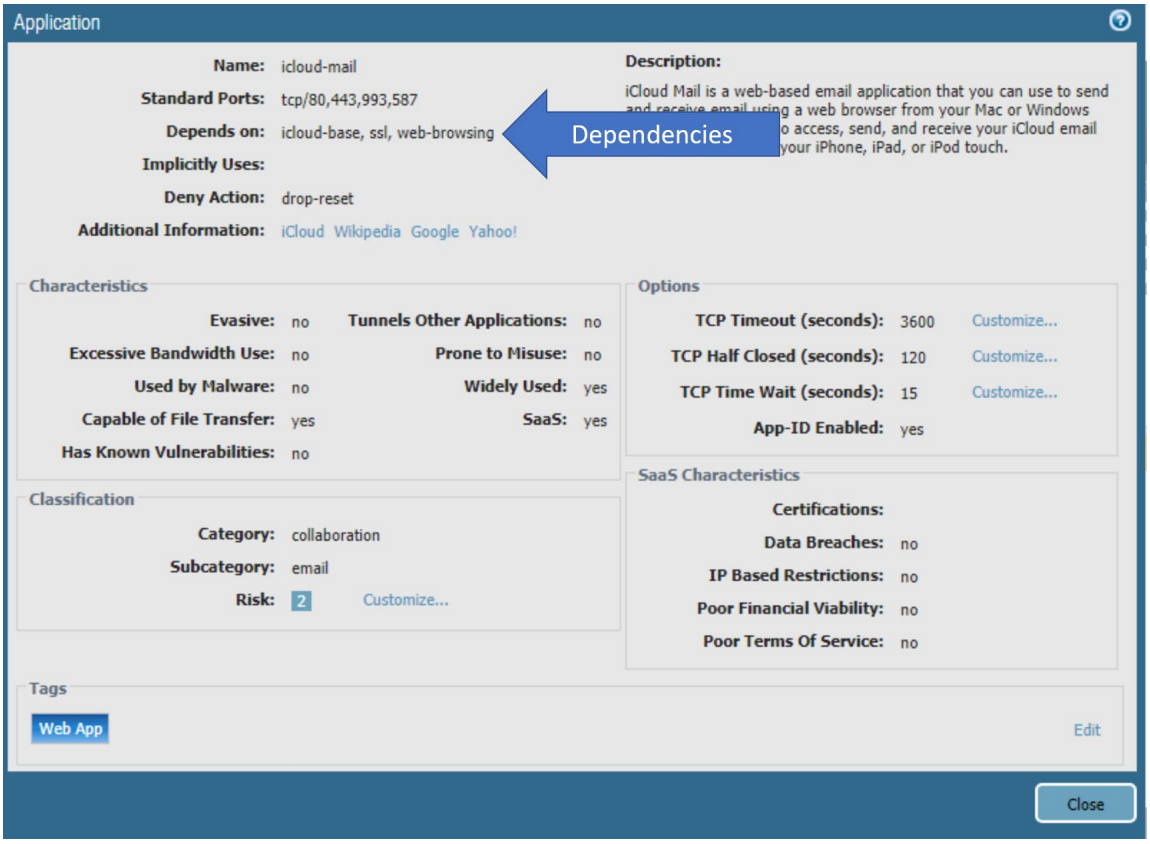
Commit Warnings Due to Missing Dependencies



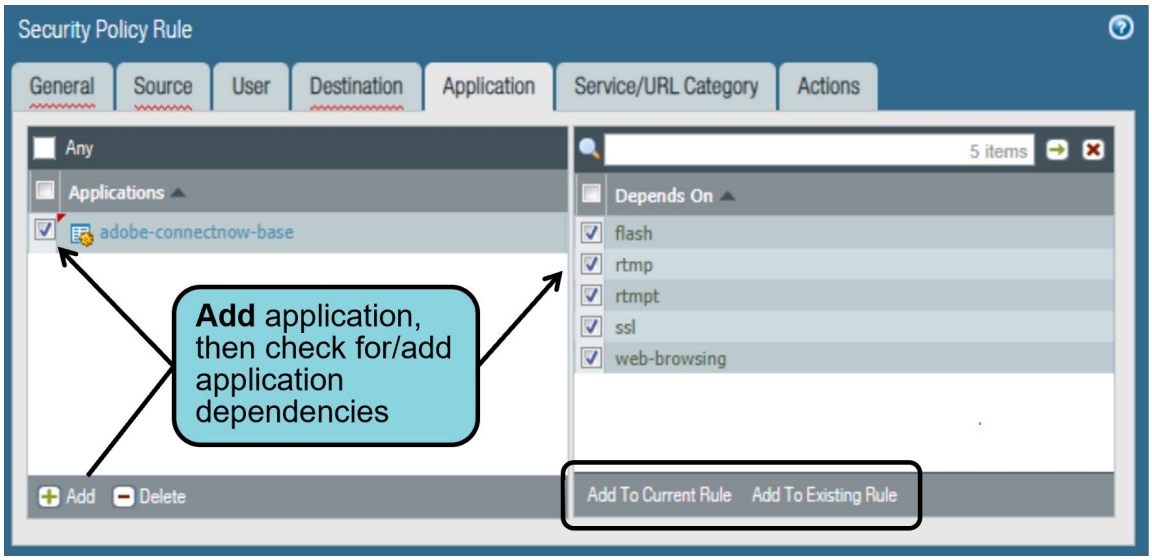
The App Dependency tab does not appear in the Commit Status window if there are no dependency warnings.

Determining Dependent Applications

To determine applications and their dependencies, navigate to **Objects > Applications**.



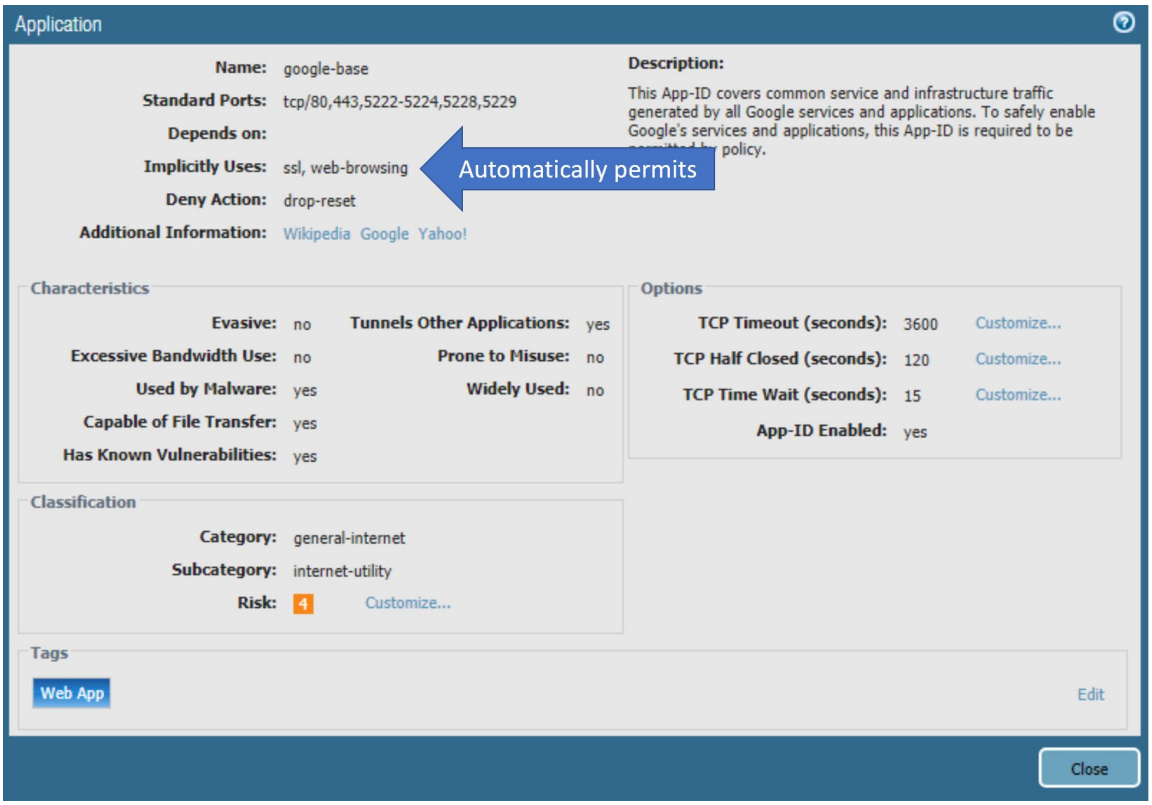
Another method to determine applications and their dependencies is to use the **Depends On** panel on the **Applications** tab while creating or updating a security policy rule.



Implicit Applications and Determining Implicit Applications

Some applications such as icloud are dependent on the web-browsing application to be specified in a security policy. Sometimes you do not have to explicitly allow access to the dependent applications for the traffic to flow because the firewall can determine the dependencies and allow them implicitly. One example is google-base. To be able to use google-base, you do not have to add ssl or web-browsing to a security policy.

To determine applications that specifically are used, navigate to **Objects > Applications**.



Sample question

77. What are two application dependencies for icloud-mail? (Choose two.)
    A. ssl
    B. skype
    C. google-base
    D. icloud-base

Exam Domain 3 – Traffic Visibility

3.2 Given a scenario, configure application filters or application groups.

Application Filters

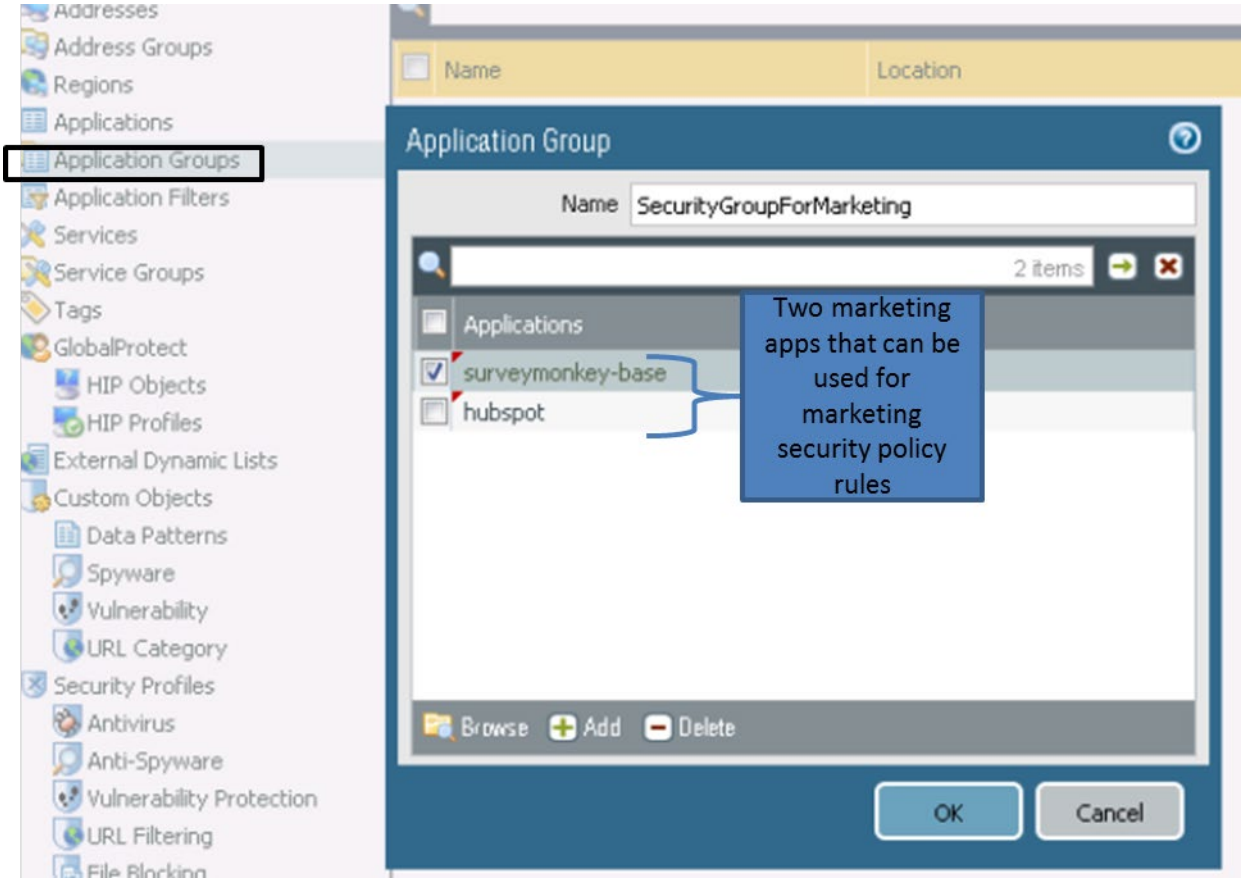
An administrator can dynamically categorize multiple applications into an application filter based on the specific attributes Category, Subcategory, Tags, Risk, and Characteristic. For example, if you want to allow all audio streaming applications, you could create an application filter that includes the subcategory of audio-streaming, which automatically would add all applications to the filter from the App-ID database that are subcategorized as audio-streaming. The filter then would be added as an application to a security policy rule. Application filters simplify the process of ensuring that all applications that meet any attribute automatically are added to a security policy.

Starting with PAN-OS 9.1, you can configure an Application Filter to filter for a group of applications based on their assigned application tags. Palo Alto Networks now assigns one or more predefined tags to some applications in the App-ID database. You also can create and assign your own custom tag to an application. You can build an Application Filter using these tags and then use the Application Filter in policy rules to control access to the applications. If application tags are updated and they are part of an Application Filter, then policy could begin to treat such applications differently.

Application Groups

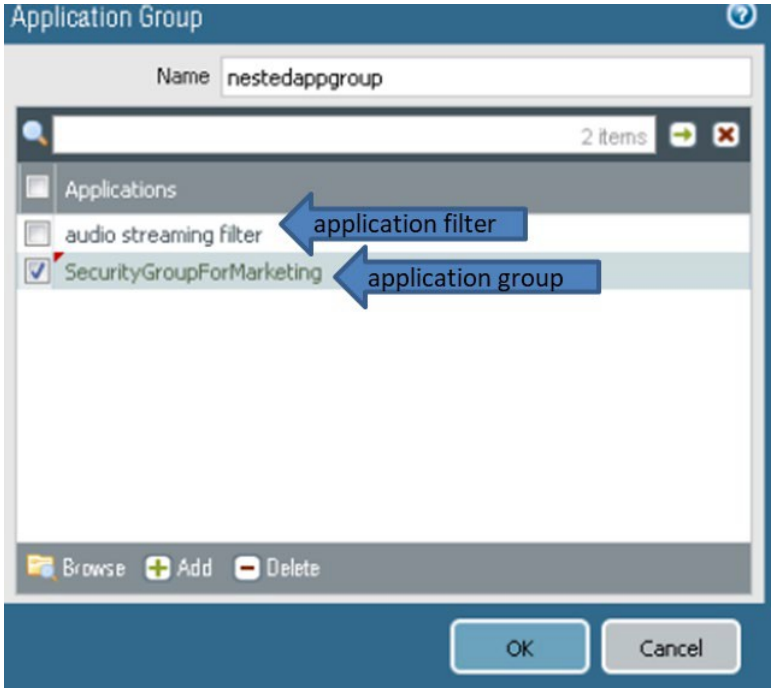
An administrator can manually categorize multiple applications into an application group based on App-ID. This application group then is added to one or more security policy rules as required, which streamlines firewall administration. Instead of a firewall administrator individually adding different applications into a security policy, only the application group needs to be added to the policy.

Application groups often are used to simplify security, QoS, and PBF policy rule implementation.



Nesting Application Groups and Filters

An administrator can nest application groups and filters. Multiple applications and multiple application filters can be combined into an application group. One or more application groups then also can be combined into one application group. The final application group then can be added to a security policy rule.



Sample questions

78. What does an Application Filter enable an administrator to do?
    A. manually categorize multiple service filters
    B. dynamically categorize multiple service filters
    C. dynamically categorize multiple applications
    D. manually categorize multiple applications
79. Which two items can be added to an application group? (Choose two.)
    A. application groups
    B. application services
    C. application filters
    D. admin accounts

Exam Domain 3 – Traffic Visibility

3.3 Identify the purpose of application characteristics as defined in the App-ID database.

Application Properties

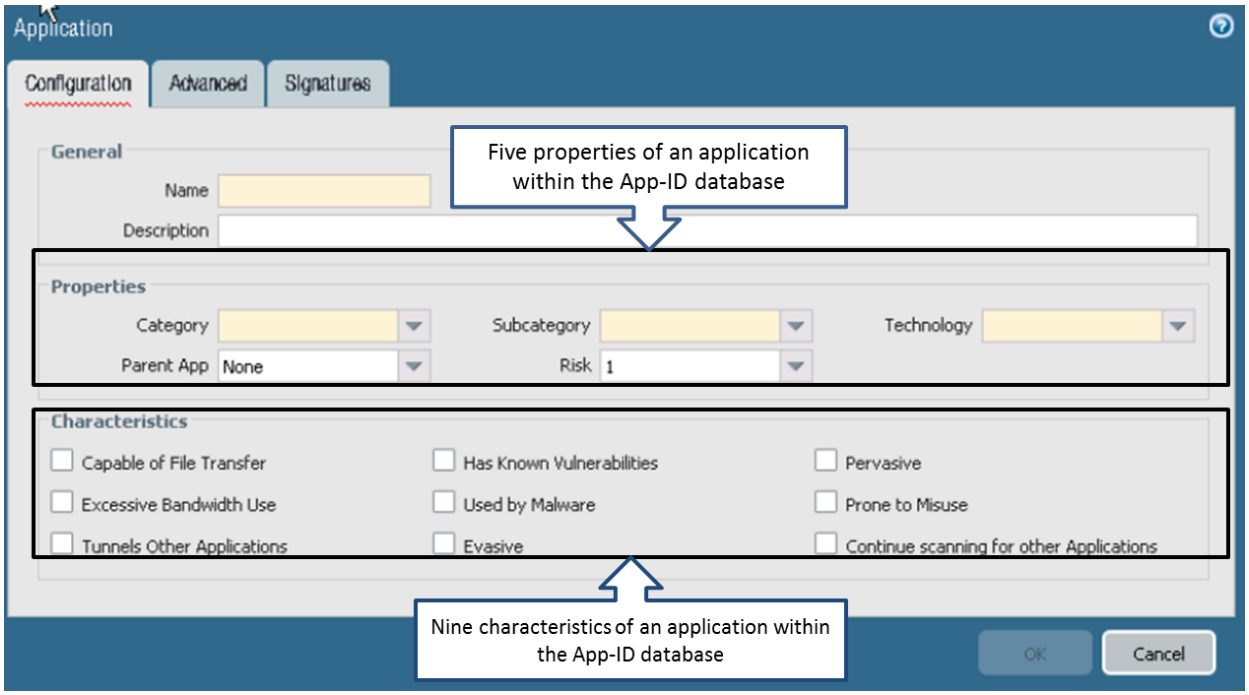
All applications in the App-ID database are defined by five properties:

Property	Definition
Category	Used to generate the Top Ten Application Categories chart within the ACC and is available for filtering

Subcategory	Also used to generate the Top Ten Application Categories chart within the ACC and is available for filtering
Risk	A relative risk rating, from 1 to 5, with 5 being the most risky
Tag	Either predefined or custom tags can be associated with an application
Characteristic	Identifies some application property or behavior, like certified for FEDRAMP, or can be used for evasion, or can use excessive bandwidth, and so on
Technology	Technology most closely associated with the application

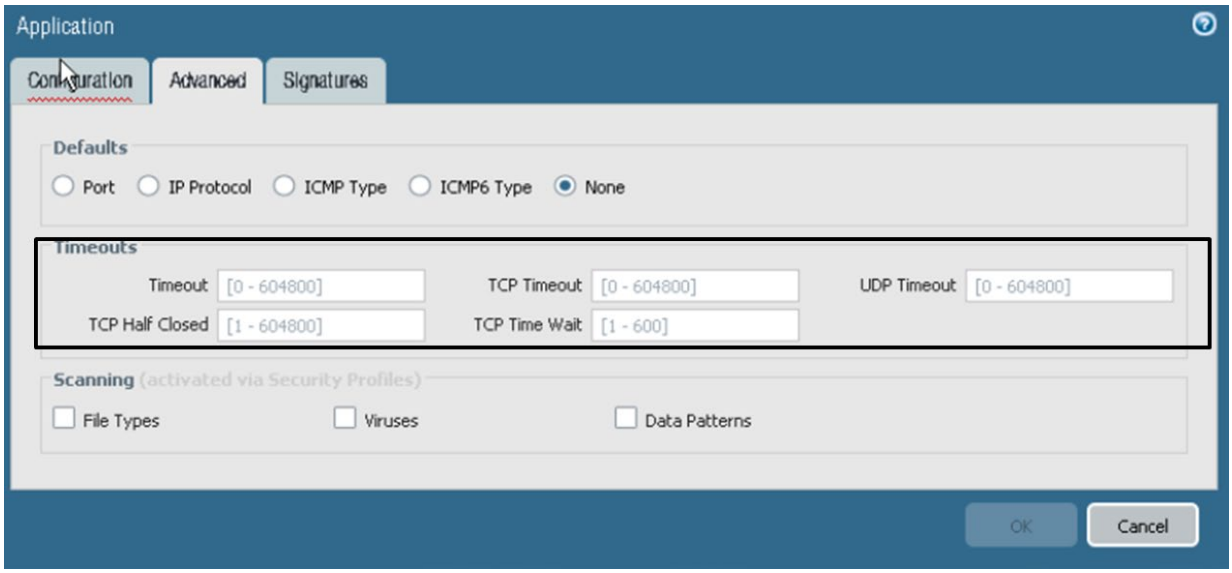
Application Characteristics

All applications in the App-ID database are defined by nine characteristics. The definitions are self-explanatory.



Application Timeouts

Item	Definition
Timeout	Number of seconds before an idle application flow is terminated. A zero indicates that the default timeout of the application will be used. This value is used for protocols other than TCP and UDP in all cases, and for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.
TCP Timeout	Number of seconds before an idle TCP application flow is terminated. A zero indicates that the default timeout of the application is used.
UDP Timeout	Number of seconds before an idle UDP application flow is terminated. A zero indicates that the default timeout of the application is used.
TCP Half Closed	Maximum length of time that a session remains in the session table between receiving the first FIN and receiving the second FIN or RST. If the timer expires, the session is closed.
TCP Time Wait	Maximum length of time that a session remains in the session table after receiving the second FIN or RST. If the timer expires, the session is closed. If this time is not configured at the application level, the global setting is used (range is 1 to 600 seconds). If this value is configured at the application level, it overrides the global TCP Time Wait setting.



Sample questions

80. What does the TCP Half Closed setting mean?
    A. maximum length of time that a session remains in the session table between receiving the first FIN and receiving the third FIN or RST.
    B. minimum length of time that a session remains in the session table between receiving the first FIN and receiving the second FIN or RST.
    C. maximum length of time that a session remains in the session table between receiving the first FIN and receiving the second FIN or RST.
    D. minimum length of time that a session remains in the session table between receiving the first FIN and receiving the third FIN or RST.
81. What are two application characteristics? (Choose two.)
    A. stateful
    B. excessive bandwidth use
    C. intensive
    D. evasive

Exam Domain 3 – Traffic Visibility

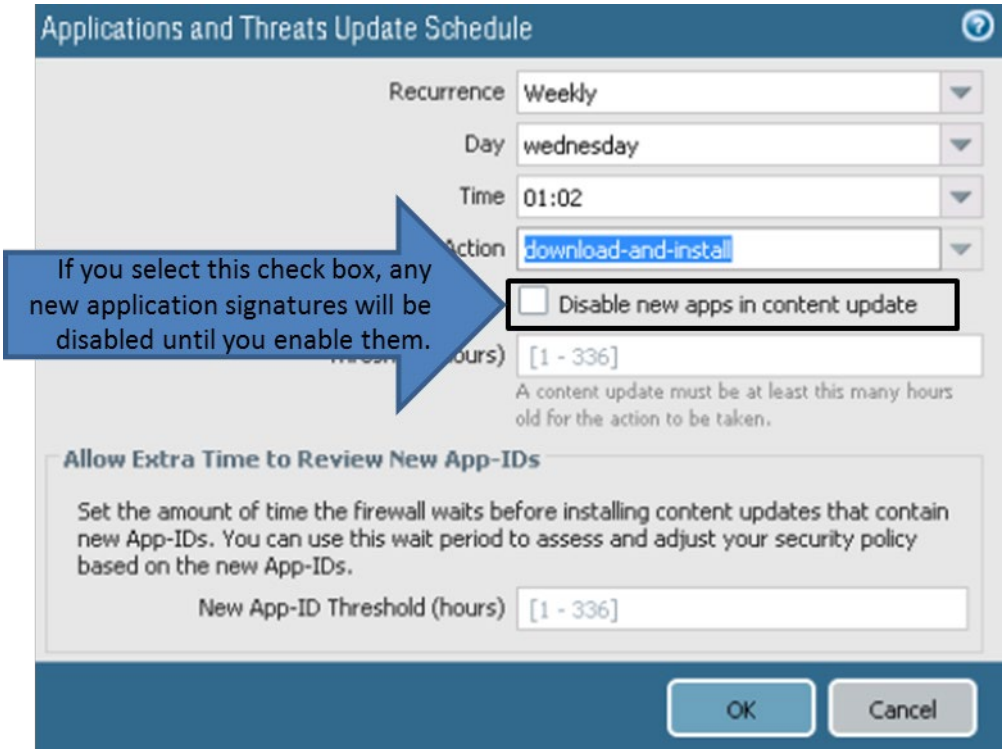
3.4 Identify the potential impact of App-ID updates to existing security policy rules.

App-ID Updates and Impact

A firewall administrator must be careful before they install any App-ID updates because some applications might have changed since the last App-ID update (content update). For example, an application that was previously categorized under web-browsing now might be categorized under its own unique App-ID. Categorization of applications into more specific applications enables more granularity and control of applications within security policy rules. Because the new App-ID no longer will be categorized as web-

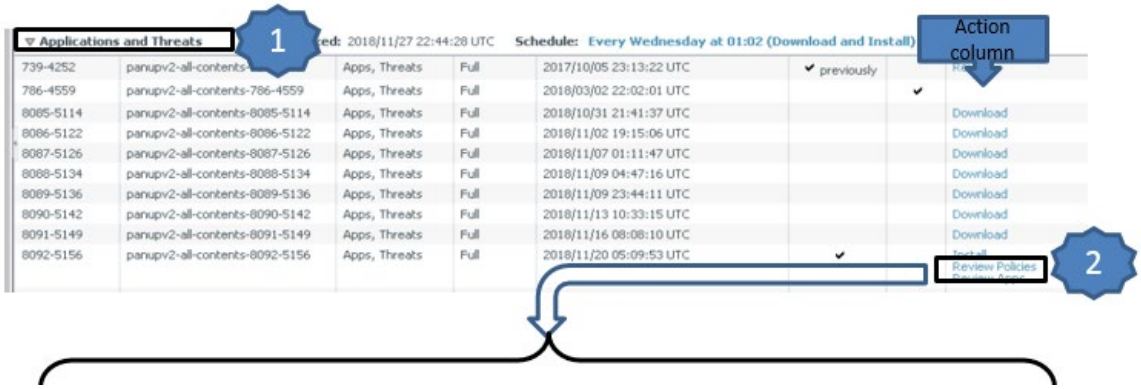
browsing, no security policy rule now will contain this new App-ID. Consequently, the new App-ID will be blocked.

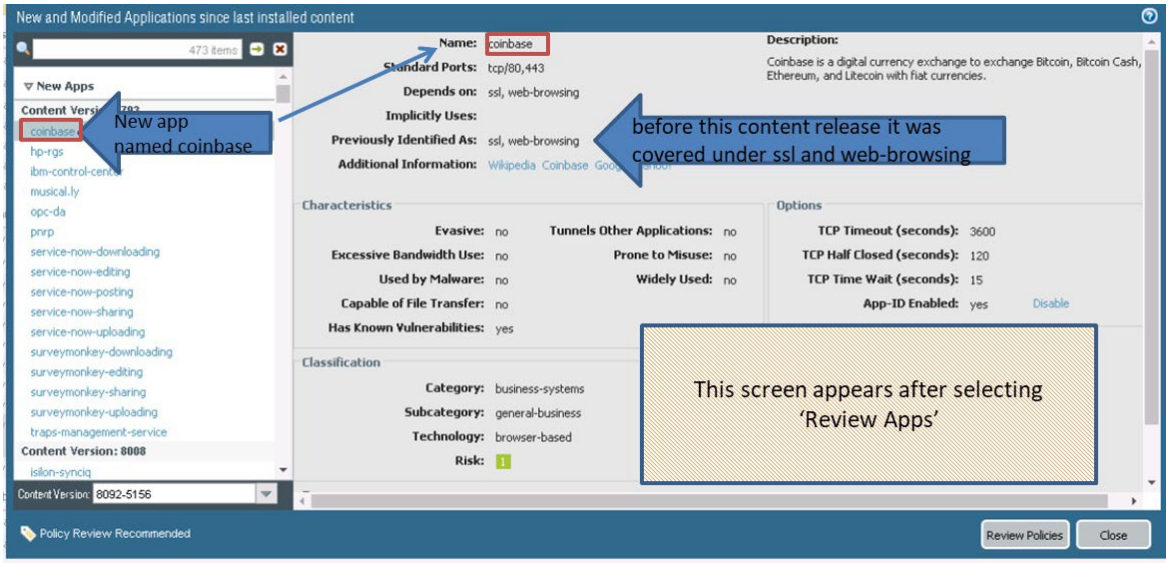
You can minimize this risk by using the **Disable new apps in content** update feature. New updates will be downloaded and installed according to the schedule, but they will be disabled until they are manually enabled. Be aware that this action will force you to keep track of disabled applications over time, which increases your administrative burden. It might be better to examine the effect of any new applications on your security policy and make any required policy updates without disabling new application signatures.



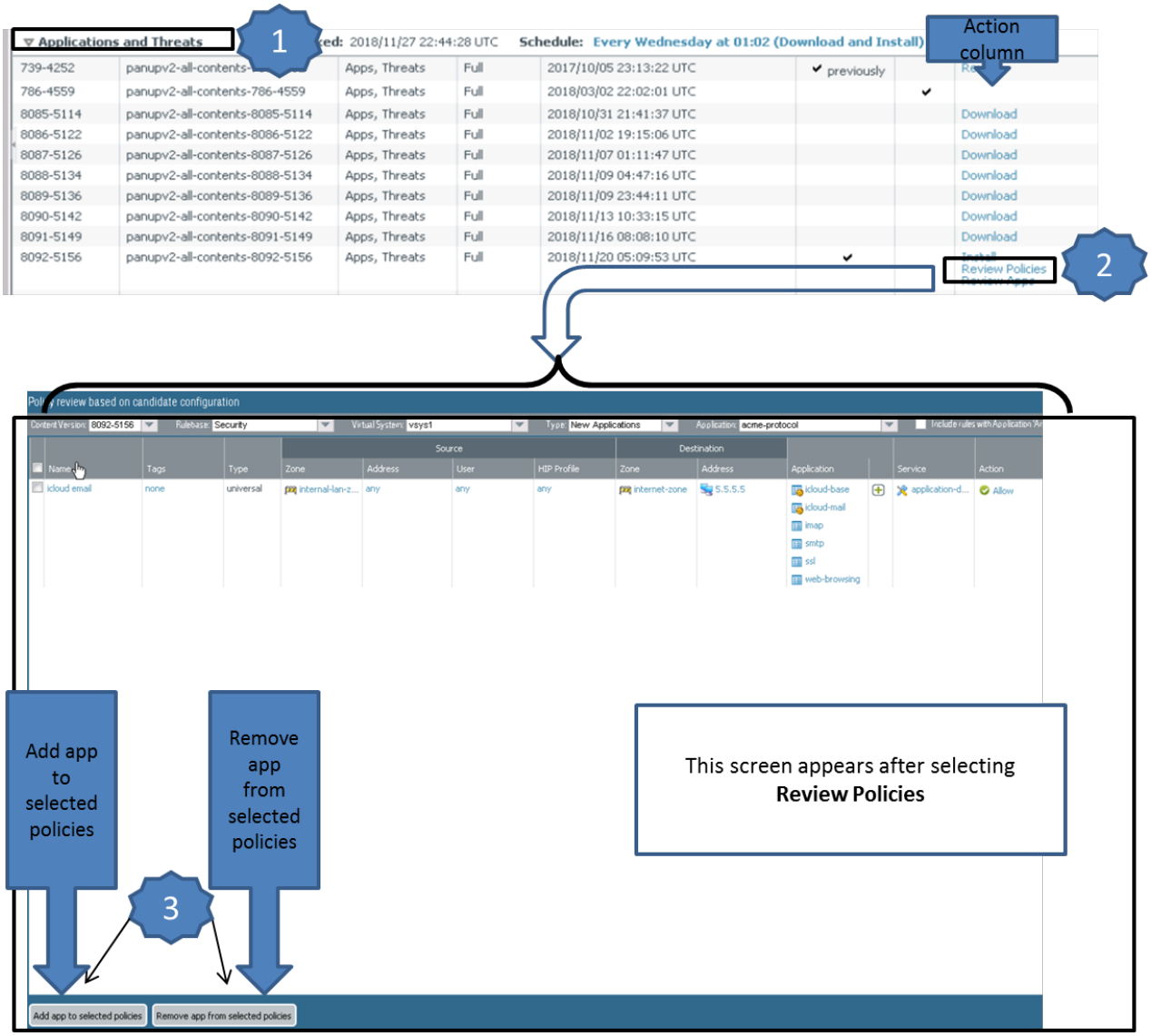
Content Update Absorption

To see the applications that have been modified since the last content release, select **Review Apps** in the **Action** column. The screen will display details about the modified application.

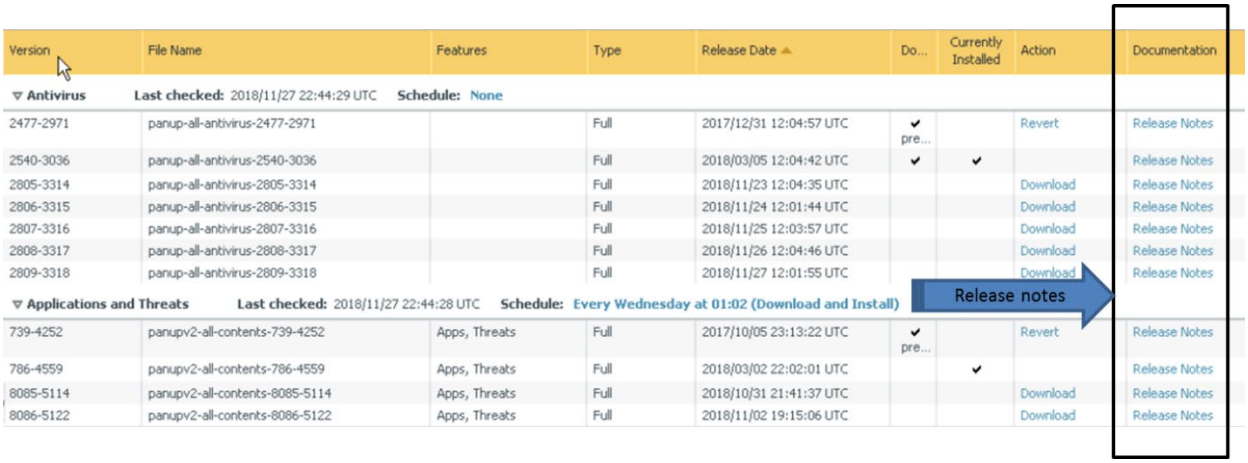




Select **Review Policies** to display the security policy rules that might enforce traffic differently once the application is modified.



Always review content release notes for the list of newly identified and modified applications and threat signatures that the content release introduces. Content release notes also describe how the update might impact existing security policy enforcement and provides recommendations about how you can modify your security policy to best leverage what's new. Installation of new App-IDs included in a content release version sometimes can cause a change in policy enforcement for the application that now is uniquely identified.



Version	File Name	Features	Type	Release Date	Do...	Currently Installed	Action	Documentation
▽ Antivirus	Last checked: 2018/11/27 22:44:29 UTC	Schedule: None						
2477-2971	panup-all-antivirus-2477-2971		Full	2017/12/31 12:04:57 UTC	✔ pre...		Revert	Release Notes
2540-3036	panup-all-antivirus-2540-3036		Full	2018/03/05 12:04:42 UTC	✔	✔		Release Notes
2805-3314	panup-all-antivirus-2805-3314		Full	2018/11/23 12:04:35 UTC			Download	Release Notes
2806-3315	panup-all-antivirus-2806-3315		Full	2018/11/24 12:01:44 UTC			Download	Release Notes
2807-3316	panup-all-antivirus-2807-3316		Full	2018/11/25 12:03:57 UTC			Download	Release Notes
2808-3317	panup-all-antivirus-2808-3317		Full	2018/11/26 12:04:46 UTC			Download	Release Notes
2809-3318	panup-all-antivirus-2809-3318		Full	2018/11/27 12:01:55 UTC			Download	Release Notes
▽ Applications and Threats	Last checked: 2018/11/27 22:44:28 UTC	Schedule: Every Wednesday at 01:02 (Download and Install)						
739-4252	panupv2-all-contents-739-4252	Apps, Threats	Full	2017/10/05 23:13:22 UTC	✔ pre...		Revert	Release Notes
786-4559	panupv2-all-contents-786-4559	Apps, Threats	Full	2018/03/02 22:02:01 UTC		✔		Release Notes
8085-5114	panupv2-all-contents-8085-5114	Apps, Threats	Full	2018/10/31 21:41:37 UTC			Download	Release Notes
8086-5122	panupv2-all-contents-8086-5122	Apps, Threats	Full	2018/11/02 19:15:06 UTC			Download	Release Notes

Sample questions

82. Which column in the Applications and Threats screen includes the options **Review Apps** and **Review Policies**?
    A. Features
    B. Type
    C. Version
    D. Action
83. Which link can you select in the web interface to minimize the risk using of installing new App-ID updates?
    A. Enable new apps in content
    B. Disable new apps in app-id database
    C. Disable new apps in content
    D. Enable new apps in App-ID database

Exam Domain 3 – Traffic Visibility

3.5 Identify the tools to optimize security policies.

See the Legacy Port-Based to App-ID Rule Converter feature in the PAN-OS 9.1 *Administrator's Guide at* https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/security-policy-rule-optimization.html#id257da3f7-bbab-4fdf-9399-73587d5cceff.

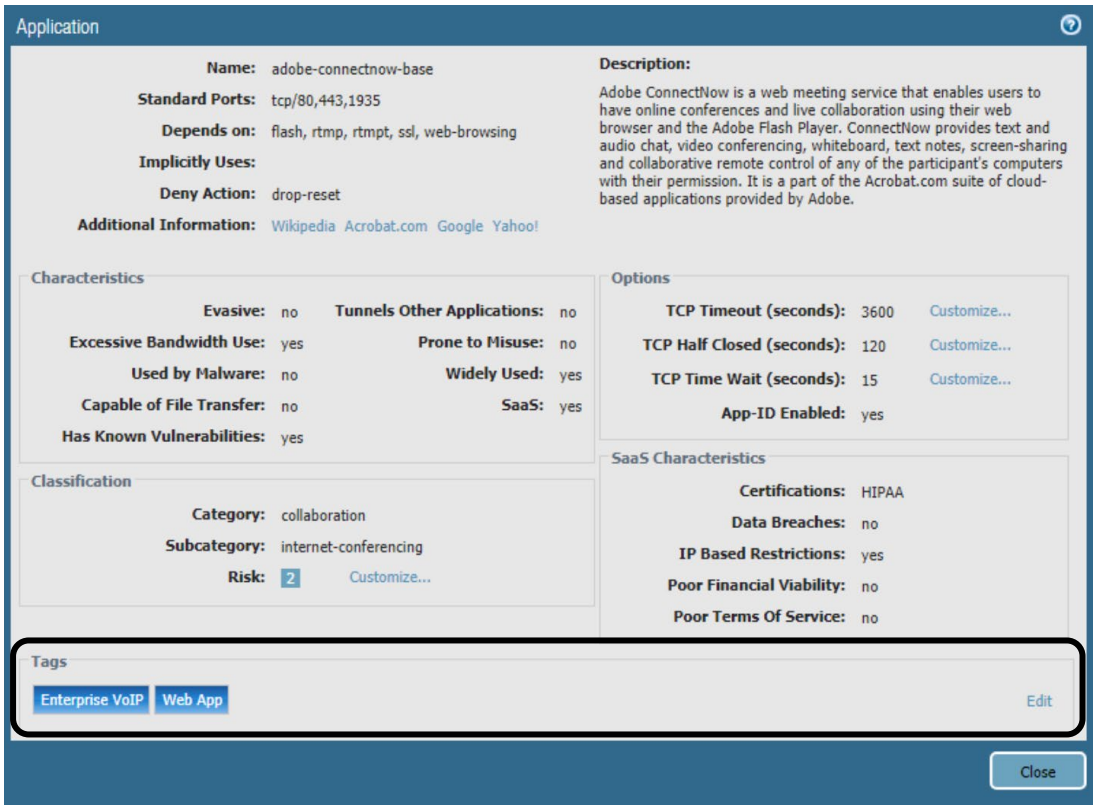
Exam Domain 3 – Traffic Visibility

3.6 Identify features used to streamline App-ID policy creation.

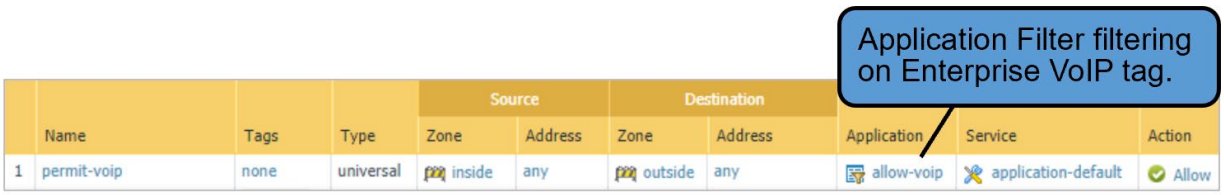
Application Tags

Starting with the release of PAN-OS 9.1, Palo Alto Networks adds predefined tags to many applications listed in the App-ID database. The predefined tags are assigned to applications based on the application's characteristics. For example, web-based applications are assigned the tag *Web App* and VoIP applications are assigned the tag *Enterprise VoIP*. Predefined tags are updated and maintained by the *Applications and Threats* dynamic updates.

You can view application tags in the web interface by browsing to **Objects > Applications** and then opening an application's details window (see the following image). You can create custom tags using **Objects > Tags** and then assign your custom tag to an application. To assign a custom tag to an application, use the **Edit** link in the application's details window, as shown in the following screenshot:



You can use application tags as policy rule match criteria. First, create an application filter using one or more application tags as filter criteria. Then add the application filter to a policy rule. If the tags associated with applications are updated, then the behavior of application filters and policy rules also will be automatically updated. An example Security policy rule with an application filter is shown in the following screenshot:

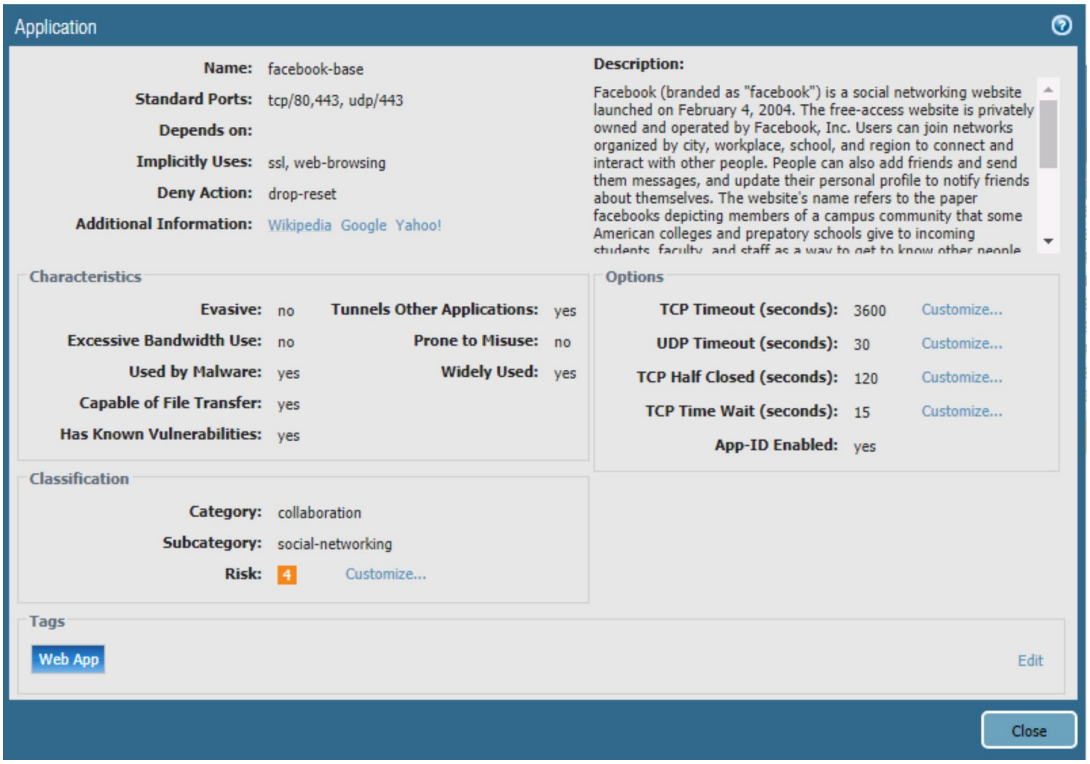


Application Dependencies

PAN-OS security controls are application-based rather than port-based and protocol-based. For example, rather than permit HTTP port 80 traffic to traverse the firewall, you permit the *web-browsing* application instead. The use of named applications to control network traffic rather than protocol and port number combinations reduces your attack surface.

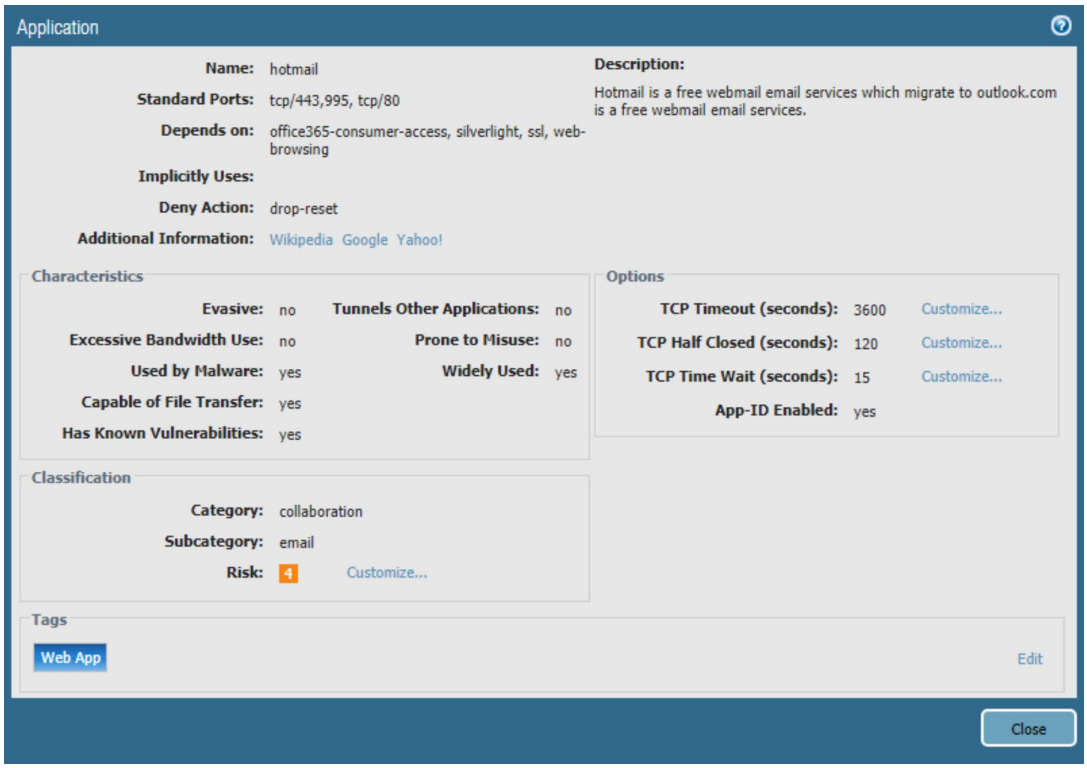
Because you must work with PAN-OS policies that are application based, you must be aware of concepts of implicit and explicit application dependencies. Some applications depend on other applications. For example, the facebook-base application depends on the web-browsing and ssl applications. To use Facebook in your environment, your firewall policy also must permit the ssl, web-browsing, and facebook-base applications. The applications that you must explicitly add to your policy rules depend on whether you are working with implicit application dependencies or explicit application dependencies.

The facebook-base application implicitly allows the ssl and web-browsing applications. This “implicit allow” means that you don’t have to explicitly add a policy rule that permits ssl and web-browsing. If you allow the facebook-base application, then the PAN-OS software will implicitly allow ssl and web-browsing too. In the web interface, browse to **Objects > Applications** and then open an application’s details window to view any implicitly allowed applications. Notice the **Implicitly Uses** field in the following screenshot:



Other dependent applications require that you explicitly add any other required applications to your policy rules. Such applications are said to have explicit application dependencies. For example, to permit the use of Hotmail in your environment, you must permit the hotmail, office365-consumer-access, silverlight, ssl, and web-browsing applications. However, the office365-consumer-access, silverlight, ssl, and web-browsing applications are not implicitly allowed by the hotmail application, which means that

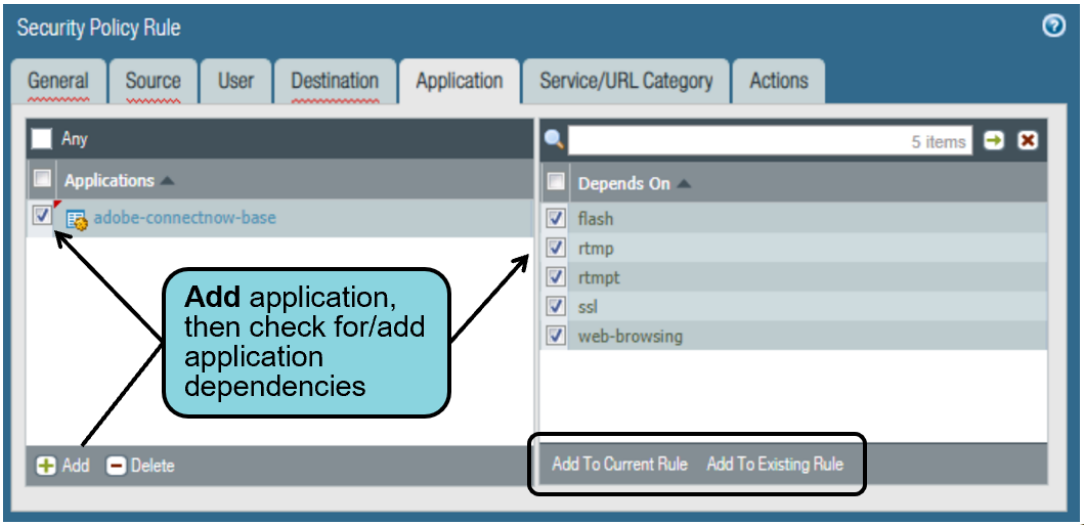
you must explicitly add them to your policy rules before your users would be able to use Hotmail. In the web interface, browse to **Objects > Applications** and then open an application's details window to view any explicit application dependencies. Notice the **Depends on** field in the following screenshot:



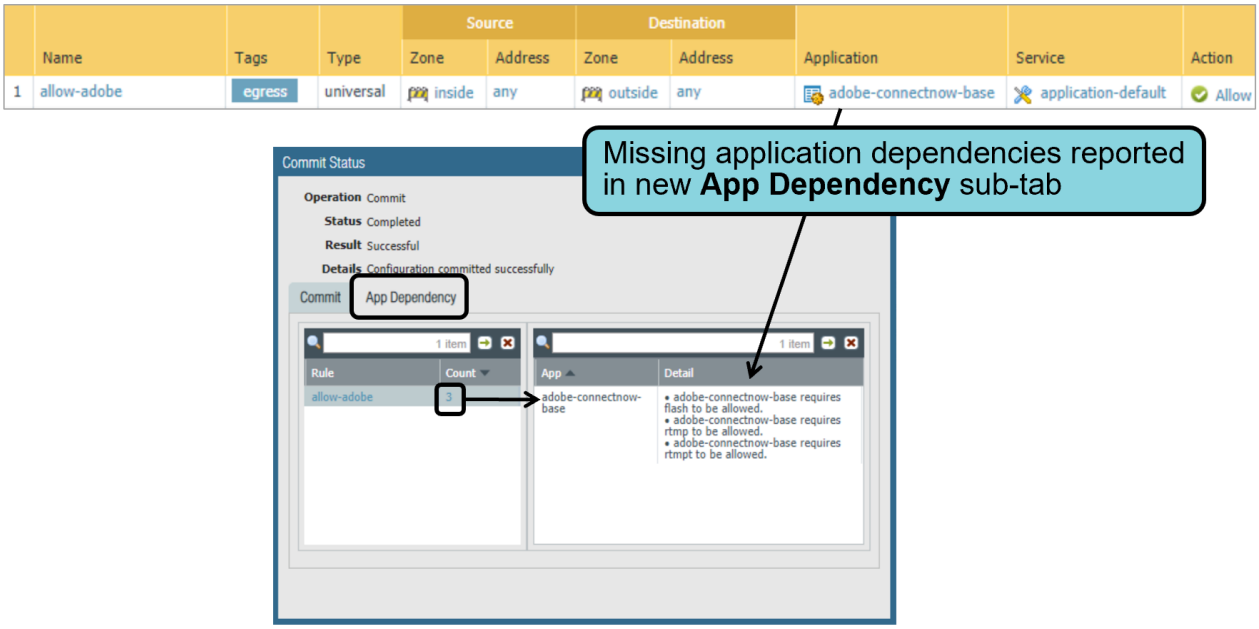
Explicit Application Dependency Resolution Workflows

PAN-OS 9.1 features three different workflows that enable you to configure your policy rules to include any explicit application dependencies. Some workflows are more efficient and streamlined than others.

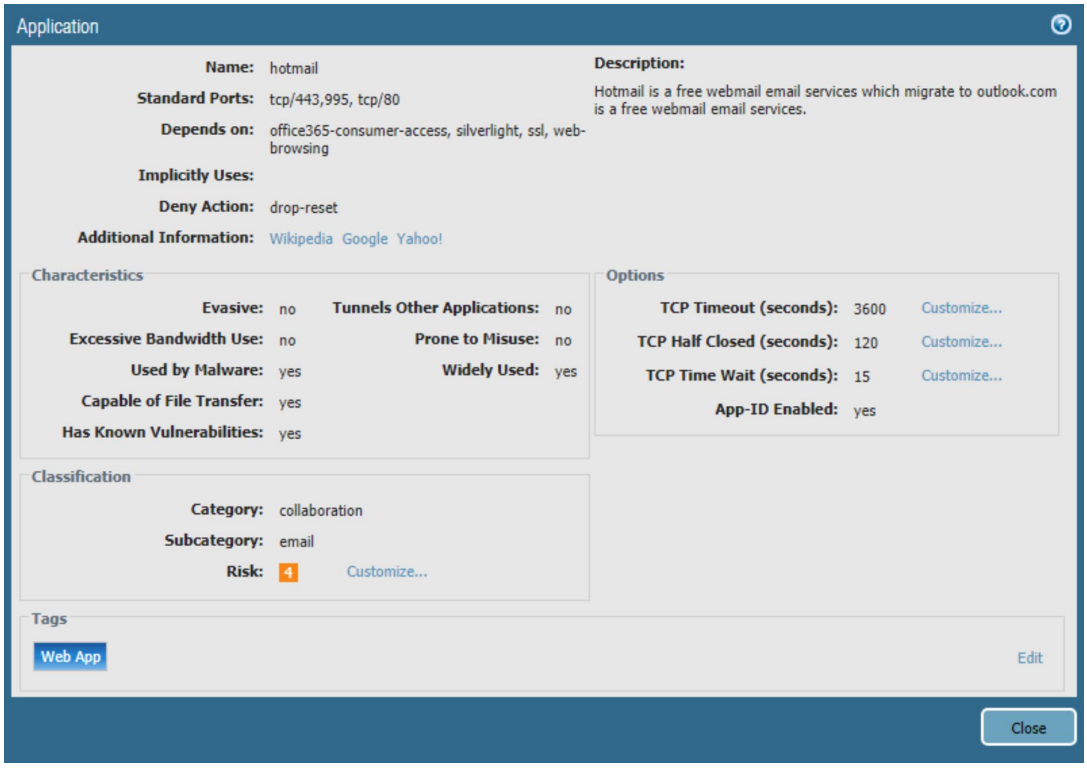
The most efficient workflow is to determine and resolve explicit application dependencies while you configure a new policy rule. This method is available starting with PAN-OS 9.1. For example, in the web interface, browse to **Policies > Security** and then click **Add** to create a new rule. As you are adding applications on the **Applications** tab, the new 9.1 **Depends On** subpanel lists any explicit application dependencies. You can add the listed applications to the current rule, or to another existing rule, in your policy. When you are finished, commit your configuration. The following screenshot is an example of the new **Depends On** subpanel:



You also can determine explicit application dependencies by updating your policy rules and then performing a commit. This workflow is not as efficient as the previous workflow. When you perform the commit in the web interface, the firewall finishes by presenting you with a **Commit Status** window. Starting with PAN-OS 9.1, the **Commit Status** window includes a new **App Dependency** tab if there are any applications in your policy rules with missing explicit application dependencies. In the example that follows, the "allow-adobe" policy rule permits the adobe-connectnow-base application but does not include the required application dependencies. The **Commit Status** window reports these missing applications. In the **Commit Status** window, you can "**click allow-adobe**," edit the rule to add the missing applications, and then commit again:



The final workflow is to research the App-ID information presented at **Objects > Applications** before you create or update a policy rule. For example, if you wanted to permit the use of Hotmail, then your App-ID research should tell you that you must add not only the hotmail application to your policy rule but also the office365-consumer-access, silverlight, ssl, and web-browsing applications. Notice the **Depends On** information for hotmail in the following screenshot:



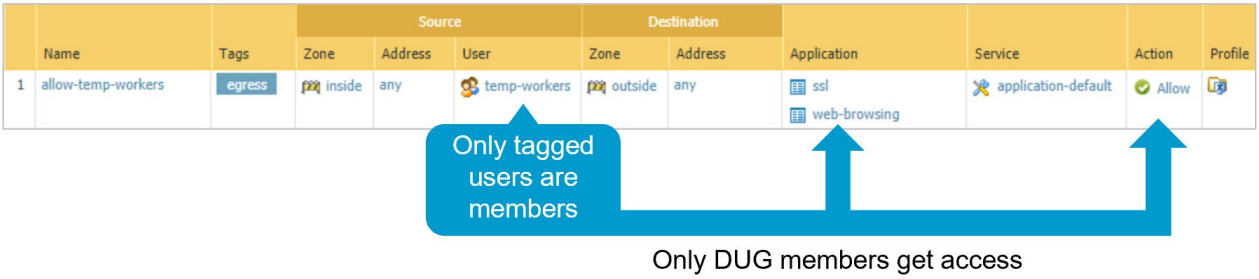
Exam Domain 3 – Traffic Visibility

3.7 Identify the benefits of using DUGs in policy rules.

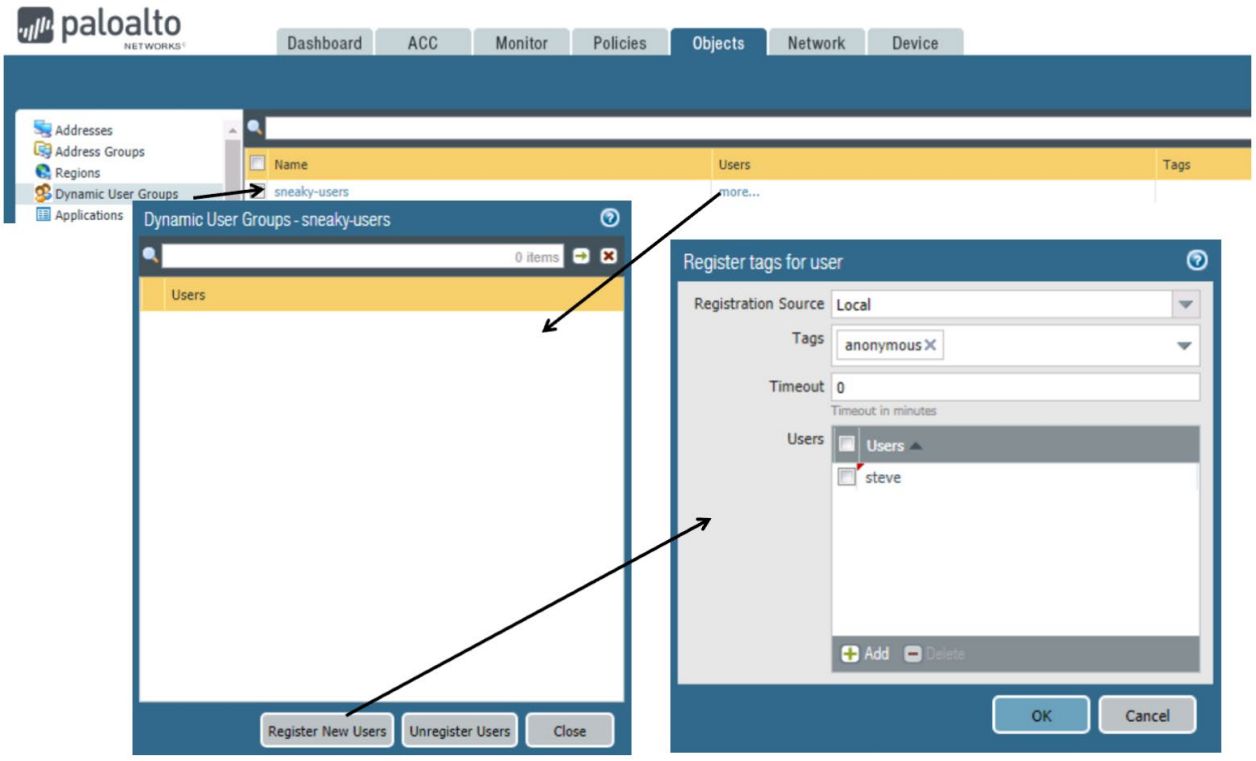
Dynamic User Groups

Dynamic user groups (DUGs) are a new feature in PAN-OS 9.1. DUGs control access to resources managed by firewall policies, including the Security policy, Authentication policy, and the Decryption policy. DUGs enable you to create policy rules that provide auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. When you create a policy rule, you can add a DUG to the **Source User** field as a match criterion. In past PAN-OS releases you would have been able to add only a username or a static groupname to the **Source User** field.

You must commit your firewall configuration after you have created a DUG and added it to a policy rule. However, you do not have to perform a commit when users are added to or removed from a DUG. User membership in a DUG is dynamic; it is controlled by tagging and untagging of usernames. Because updates to DUG membership are automatic, use of DUGs instead of a static group (such as an LDAP group) enables you to respond to changes in user behavior or potential threats without manual policy changes.



Several methods are available to tag or untag usernames. You can manually tag and untag usernames using the web interface, as shown in the following screenshot:



Usernames also can be tagged and untagged using the auto-tagging feature in a Log Forwarding Profile also can tag or untag usernames. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames. In the web interface, you can use logical AND or OR operators with the tags to better filter or match against. You also can configure a timeout value that determines when a username will be automatically untagged.

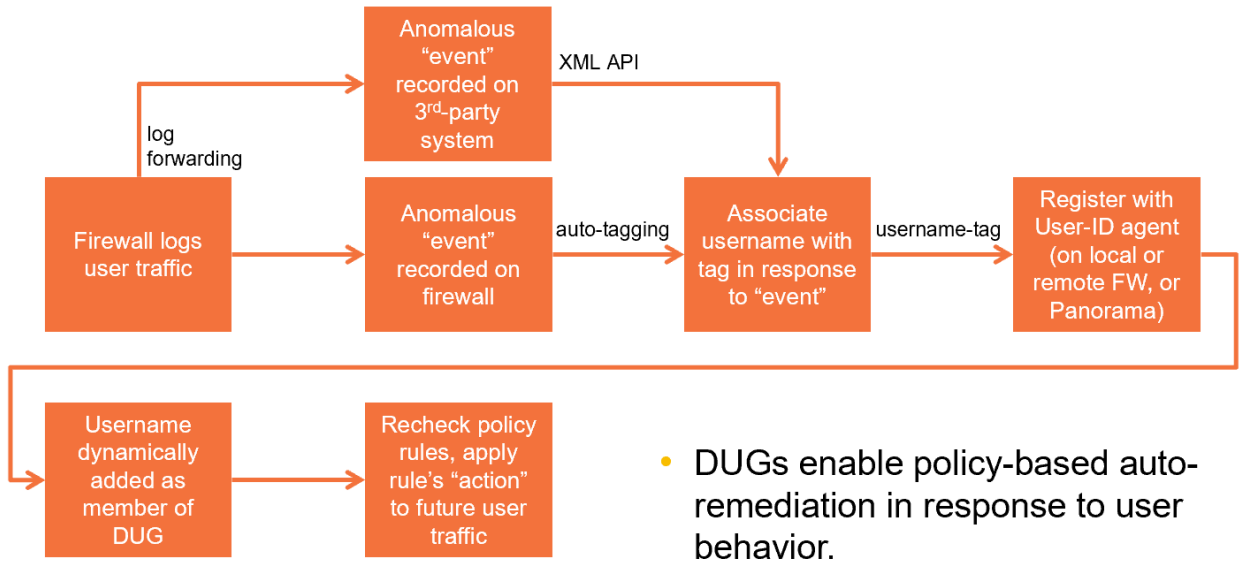
DUG Operation

DUGs enable you to create a Security policy that provides auto-remediation in response to user behavior and activity. Auto-remediation reduces administrative burden by automating the firewall's response to user activity. Auto-remediation using DUGs also reduces the firewall's response time to malicious activity, which provides better security for your environment.

In the illustration shown in the following screenshot, a user's traffic is recorded in the firewall logs. You can analyze these logs directly on the firewall or you can configure log forwarding to forward the logs to a third-party system for analysis. If logs are being analyzed locally on the firewall, the log forwarding configuration can invoke a new built-in action that will associate a tag with a username based on one or

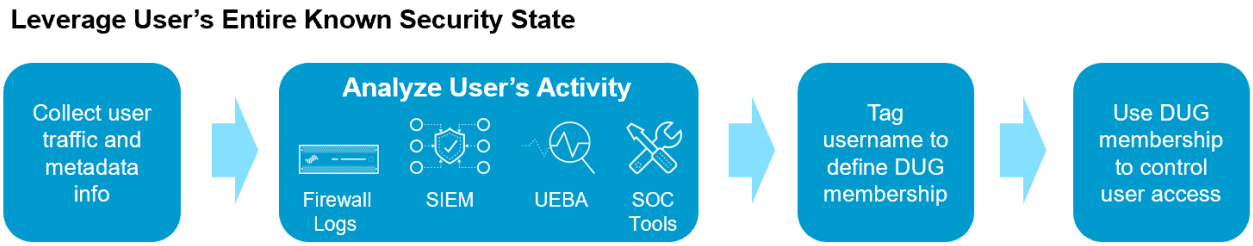
more events in a log. A third-party system also can associate a tag with a username using the PAN-OS XML API. Username-tag registrations are recorded in and maintained by a User-ID agent.

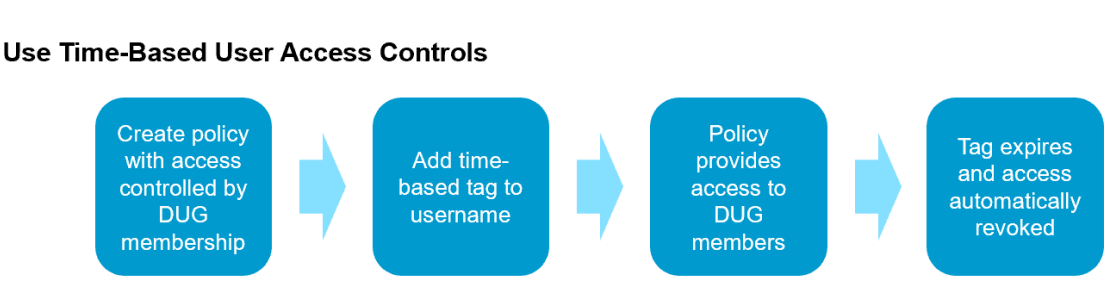
The firewall uses these username-tag pairs to determine which users are currently members of a DUG. When you configure a DUG you associate it with one or more tags. Any user that also is associated with a tag configured in a DUG becomes a member of the DUG. DUG membership is then used to determine future policy rule matches. As examples, a Security policy could block a user, an Authentication policy could force the user to use MFA, or a Decryption policy could force the user's traffic to be decrypted.



Example Use Cases

Here two DUG use case examples are shown:





The first example illustrates the use a user's entire known security state, which is derived from various sources, to determine how the firewall will control or affect the user's access to network resources. In this case, the user's network traffic is logged so that it can be analyzed. User metadata also might be collected from other resources such as an LDAP server.

All this data can be analyzed in the firewall's logs, or on a SIEM, or in a *user and entity behavior analytics* system, or using a variety of tools available to a SOC. Any of these tools can be configured to tag or untag a username, depending on the results of the analysis. Tagging and untagging of a username determines whether it is a member of a DUG. Then DUG membership and policy configuration determine how the firewall should treat the user's network traffic.

The second example illustrates how to use a DUG to implement time-based access controls for workers that might require only short-term access to network resources. In this case, you create a DUG and add it to policies that control user access to network resources. You then can add a time-based tag to a username. A tagged username is a member of the DUG and network access is permitted by the DUG. When the time-based tag expires, the user's membership in the DUG is terminated along with the network access that was provided by the DUG.

Exam Domain 3 – Traffic Visibility

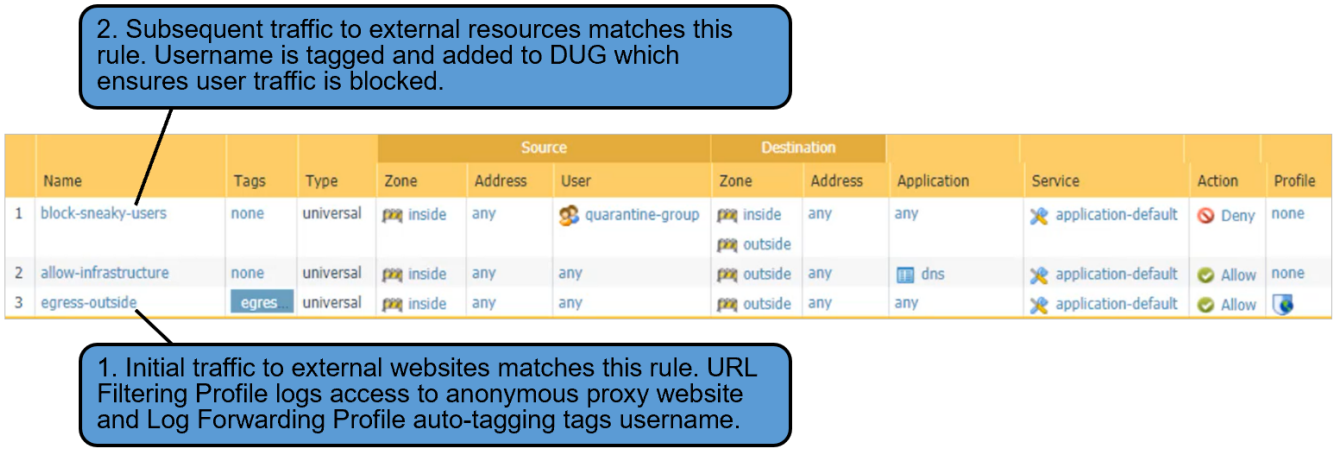
3.8 Identify the requirements to support dynamic user groups.

DUG Prerequisites

The dynamic user group feature was added to PAN-OS software starting with version 9.1. All firewalls must be upgraded to at least version 9.1 to use DUGs. If your firewalls will be managed by Panorama, then your Panorama device also must be upgraded to at least version 9.1.

You also must configure User-ID on your firewalls. The dynamic tags are registered and unregistered from the User-ID agent either on the local firewall, a remote firewall, or Panorama.

To use DUGs to invoke auto-remediation, you will need to create at least two Security policy rules: one to allow initial traffic to populate the DUG and another rule to deny traffic for the activity you want to prevent. To ensure that users are tagged, the rule to allow traffic must have a higher rule number in your rulebase than the rule that denies traffic. The following screenshot illustrates how the two rules would be configured. The application is "any" for illustration purposes, but this configuration is not a recommended best practice:



For additional information about configuring and using DUGs, see the *PAN-OS® 9.1 Administrator's Guide* at https://docs.paloaltonetworks.com.

Exam Domain 4 – Securing Traffic

4.1 Given a risk scenario, identify and apply the appropriate security profile.

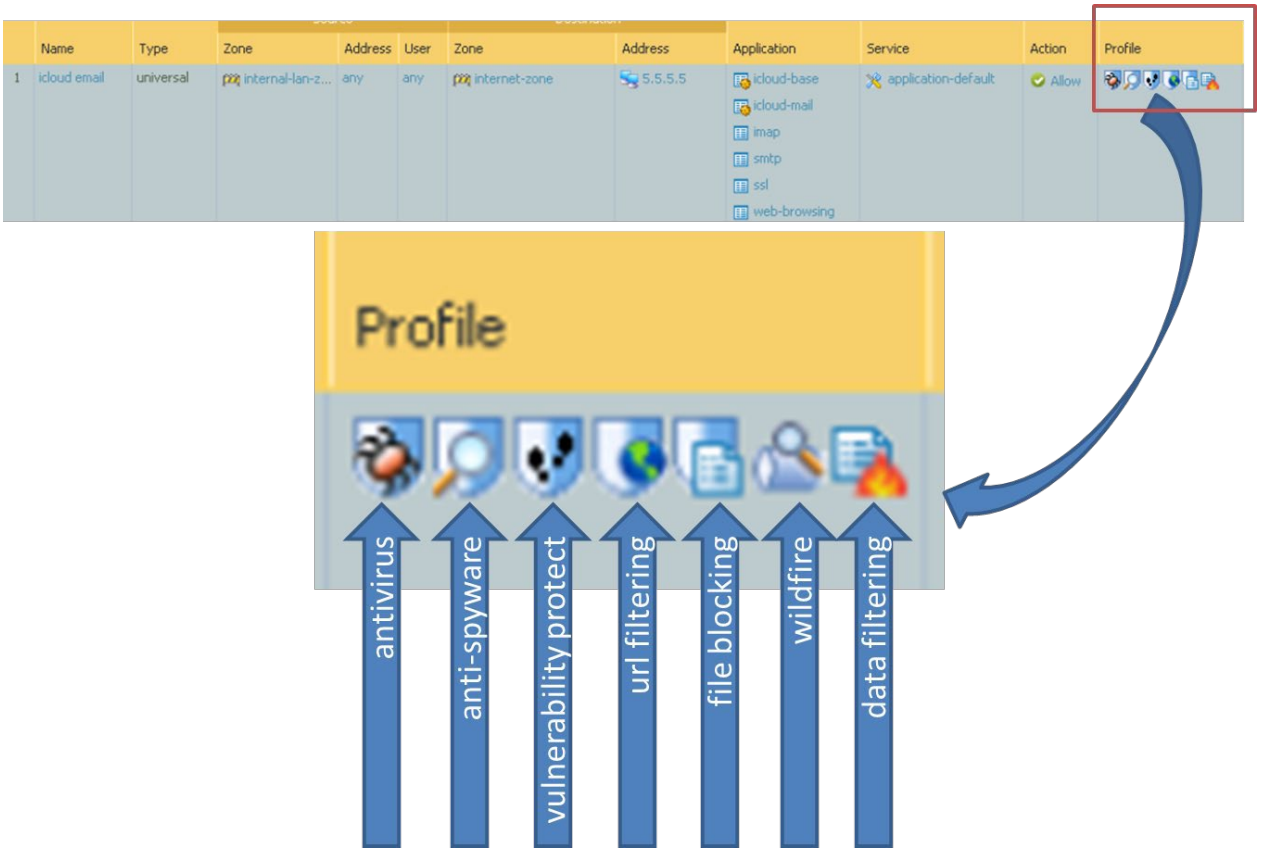
Security Profiles

Security profiles are added to the end of security policy rules. After a packet has been allowed by the security policy, security profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software. Traffic also can be scanned for suspicious file uploads.

A Security Profile Group can be created that includes one or more security profiles, which simplifies the task of adding security profiles to a security policy rule.

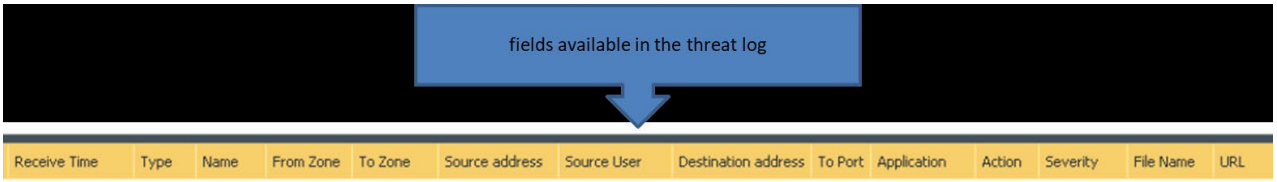
The following table describes the security profile types:

Type	Description
Antivirus	Detects infected files being transferred within the application or protocol
Anti-Spyware	Detects spyware downloads and command-and-control traffic from previously installed spyware
Vulnerability Protection	Detects attempts to exploit known software vulnerabilities
URL Filtering	Classifies and controls web browsing based on website content
File Blocking	Tracks and blocks file uploads and downloads based on file type and application
WildFire Analysis	Forwards unknown files and URL links to the WildFire® service for malware analysis. **Note:** This type will not be discussed further in this section.
Data Filtering	Identifies and blocks transfer of specific data patterns found in network traffic **Note:** This type will not be discussed further in this section.



Threat Logs

Threats are recorded and logged in the Threat log. A Threat log display entries when traffic matches one of the security profiles attached to a security policy rule on the firewall. Each entry includes the following information: date and time; type of threat (such as virus or spyware); threat description or URL (**Name** column); source and destination zones, addresses, and ports; application name; alarm action (such as allow or block); and severity level. The Threat log is used as the source of information that is displayed on the **ACC** tab (Application Control Center).



Threat levels are based on severity. There are five levels of severity:

- **Critical:** Critical threats are serious threats such as those that affect default installations of widely deployed software and result in the compromise of servers. Critical threats include those where the exploit code is widely available to attackers. The attacker usually does not need any special authentication credentials or knowledge about the individual victims, and the target does not need to be manipulated into performing any special functions.
- **High**: High threats are those that can become critical but have mitigating factors; for example, they might be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool.

- **Medium**: Medium threats are minor threats and those that pose minimal impact. Examples include DoS attacks that do not compromise the target or exploits that require an attacker to reside on the same LAN as the victim. Medium threats affect only non-standard configurations or obscure applications, or provide very limited access.
- **Low**: Low threats are warning-level threats that have little impact on an organization's infrastructure. They usually require local or physical system access and often might result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low.
- **Informational**: Informational threats are suspicious events that do not pose an immediate threat but that are reported to call attention to deeper problems that could exist. URL Filtering log entries are logged as Informational. Log entries with any verdict and an action set to block also are logged as Informational.

Antivirus Security Profiles

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

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

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

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

Anti-Spyware Security Profiles

Anti-Spyware security profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between security zones. For example, you might want to have custom Anti-Spyware profiles that minimize inspection between more trusted zones while maximizing inspection on traffic received from less trusted zone such as internet-facing zones.

Vulnerability Protection Security Profiles

Vulnerability Protection security profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware security profiles identify infected hosts as traffic leaves the network, but Vulnerability Protection security profiles protect against threats entering the network. For

example, Vulnerability Protection security profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The *default* Vulnerability Protection security profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

URL Filtering Security Profiles

The URL Filtering security profile determines web access and credential submission permissions for each URL category. By default, site access for all URL categories is set to "allow" when you create a new URL Filtering security profile. All allowed traffic will not be logged by default. You can customize the URL Filtering security profile with custom site access settings for each category, or use the predefined *default* URL Filtering security profile on the firewall to allow access to all URL categories except the following threat-prone categories, which it blocks: abused-drugs, adult, gambling, hacking, malware, phishing, questionable, and weapons.

For each URL category, select **User Credential Submissions** to allow or disallow users from submitting valid corporate credentials to a URL in that category. This action will prevent credential phishing.

Management of the sites to which users can submit credentials requires User-ID, and you must first set up credential phishing prevention. URL categories with the **Site Access** set to block automatically are set to also block user credential submissions.

File Blocking Security Profiles

A security policy can include specification of a File Blocking profile that blocks selected file types from being uploaded or downloaded, or generates an alert when the specified file types are detected.

Sample question

84. What are two benefits of Vulnerability Protection security profiles? (Choose two.)
    A. prevent compromised hosts from trying to communicate with external command-and- control (C2) servers
    B. protect against viruses, worms, and Trojans
    C. prevent exploitation of system flaws
    D. prevent unauthorized access to systems

Exam Domain 4 – Securing Traffic

4.2 Identify the difference between security policy actions and security profile actions.

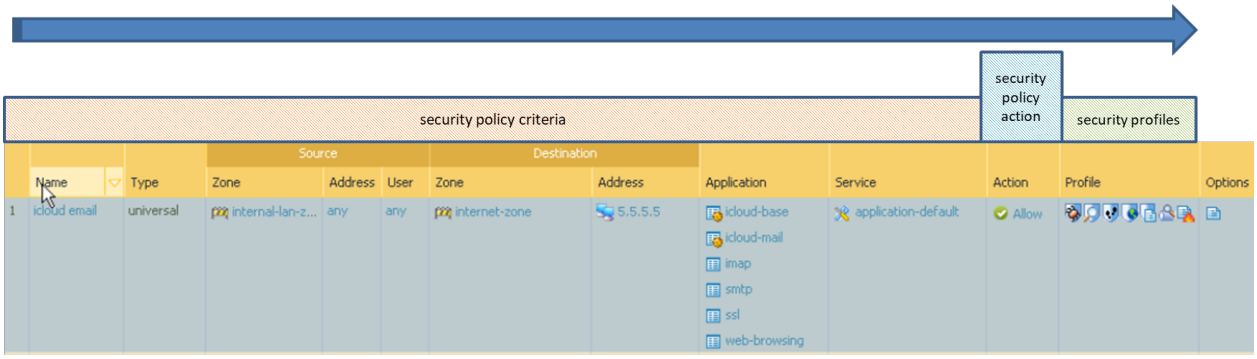
Security Policy Actions and Security Profile Actions

When packets traverse a firewall, they are inspected in two primary stages:

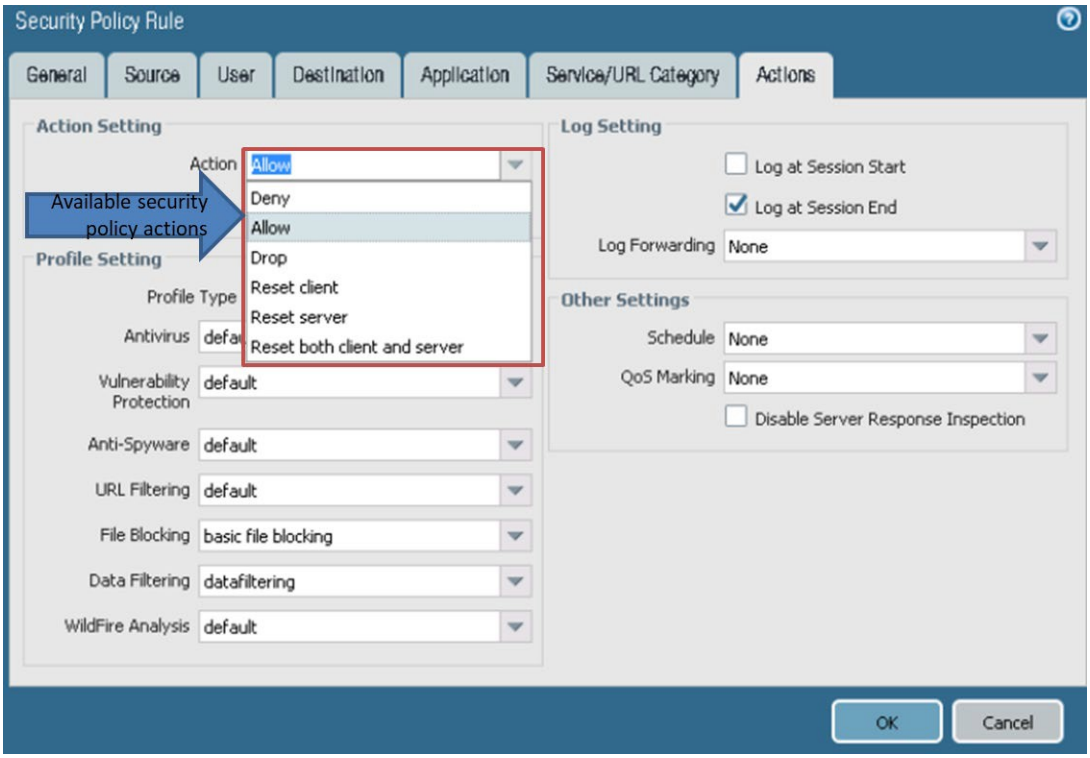
- Security Policy Stage
- Security Profile Stage

In the Security Policy Stage, packets must meet all the criteria in a security policy rule to match the security policy rule. If all the criteria match, the security policy rule's action is applied. If the security policy

action is “allow,” the packet is inspected by the security profiles attached to the security policy rule. If all the security profile criteria do not match, or the security policy is any action other than “allow,” the packet is evaluated against the next security policy rule, and so on. You can create a Security Profile Group that includes one or more security profiles, which simplifies the task of adding security profiles to a security policy rule.



The Available Security Policy Actions



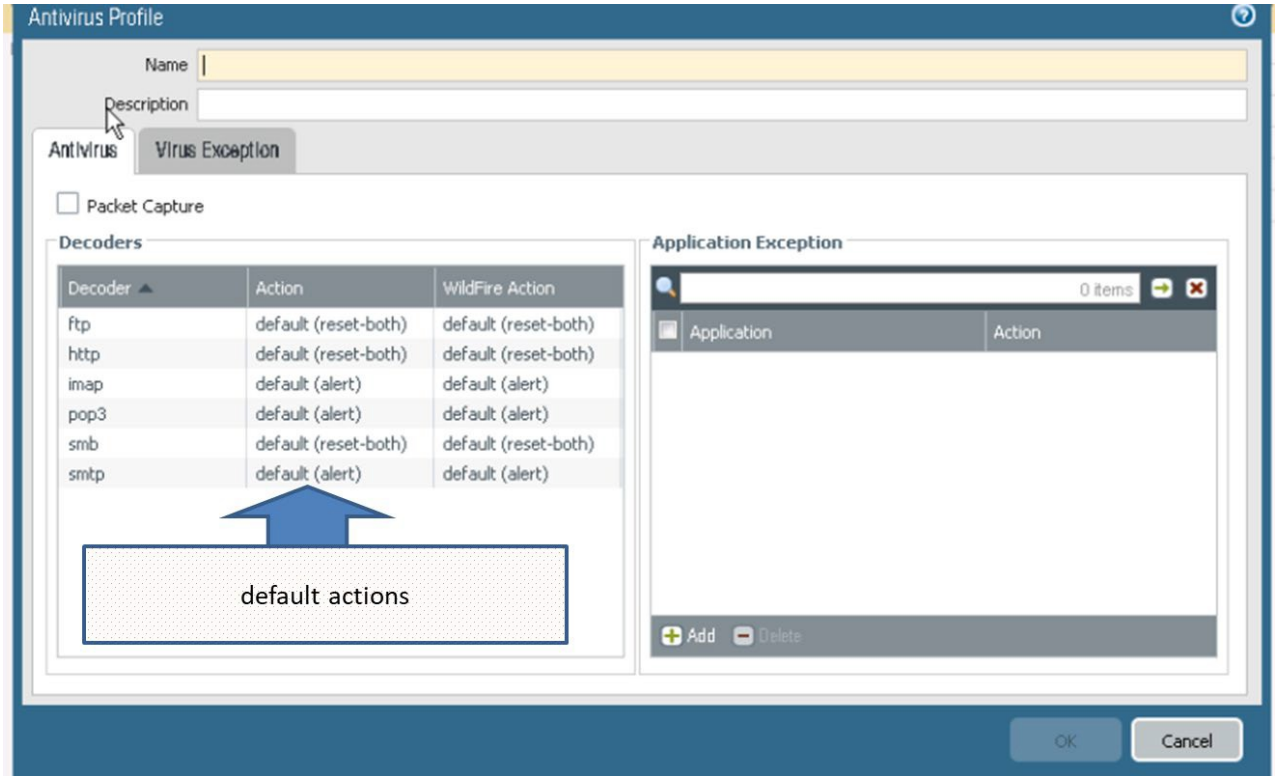
Antivirus Security Profile Actions

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

Action	Description
Default	For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. The default action typically is an “alert” or a “reset-both.” The default action is displayed in parentheses, for example, default (alert), in the threat or antivirus signature.

Allow	Permits the application traffic.
Alert	Generates an alert for each application traffic flow. The alert is saved in the Threat log.
Drop	Drops the application traffic.
Reset Client	For TCP, resets the client-side connection. For UDP, drops the connection.
Reset Server	For TCP, resets the server-side connection. For UDP, drops the Connection.
Reset Both	For TCP, resets the connection on both client and server ends. For UDP, drops the connection.

You also can use customized profiles to minimize antivirus inspection for traffic between trusted security zones. They also can be used to maximize the inspection of traffic received from more untrusted zones such as the internet and of traffic sent to highly sensitive destinations such as server farms. The Palo Alto Networks WildFire product also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded daily by Threat Prevention subscribers (sub-hourly for WildFire subscribers).



Anti-Spyware Security Profile Actions

You can create custom Anti-Spyware profiles, or one of the two following predefined profiles can be chosen when applying anti-spyware to a security policy rule:

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

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

Action	Description
Default	For each threat signature and anti-spyware signature that is defined by Palo Alto Networks, a default action is specified internally. The default action typically is an "alert" or a "reset-both." The default action is displayed in parentheses, for example, default (alert), in the threat or antivirus signature.
Allow	Permits the application traffic.
Alert	Generates an alert for each application traffic flow. The alert is saved in the Threat log.
Drop	Drops the application traffic.
Reset Client	For TCP, resets the client-side connection. For UDP, drops the connection.
Reset Server	For TCP, resets the server-side connection. For UDP, drops the connection.
Reset Both	For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
Block IP	Blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

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

Two Predefined Anti-Spyware Security Profiles

Vulnerability Protection Security Profile Actions

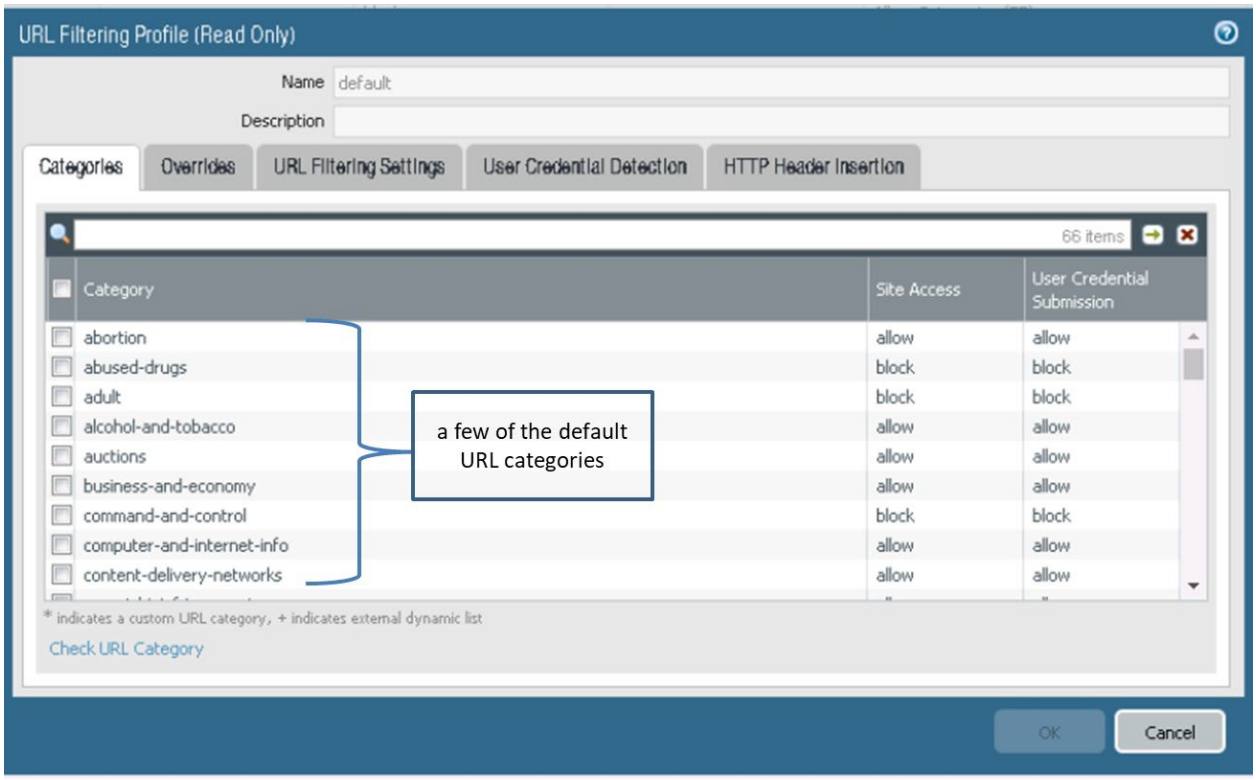
The *default* Vulnerability Protection security profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

Two Predefined Vulnerability Protection Security Profiles

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable

URL Filtering Security Profile Actions

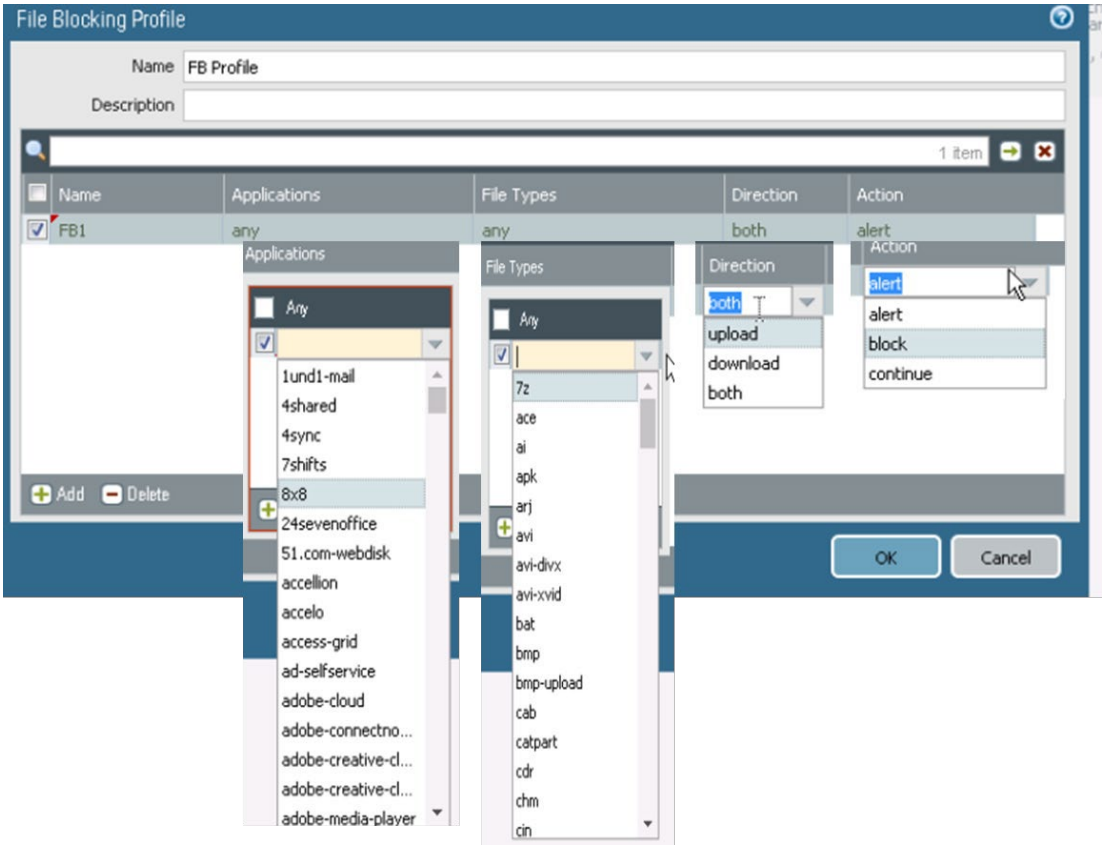
Action	Description
Alert	The website is allowed and a log entry is generated in the URL filtering log.
Allow	The website is allowed and no log entry is generated.
Block	The website is blocked and the user will see a response page and will not be able to continue to the website. A log entry is generated in the URL Filtering log. Blocking of site access for a URL category also sets **User Credential Submissions** for that URL category to "block."
Continue	The user will be prompted with a response page indicating that the site has been blocked due to company policy, but the user is prompted with the option to continue to the website. The "continue" action typically is used for categories that are considered benign and is used to improve the user experience by giving the user the option to continue if they consider the site to be incorrectly categorized. The response page message can be customized to contain details specific to your company. A log entry is generated in the URL Filtering log. The Continue webpage doesn't display properly on client systems configured to use a proxy server.
Override	The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or helpdesk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn't display properly on client systems configured to use a proxy server.
None	The "none" action applies only to custom URL categories. Select **none** to ensure that, if multiple URL Filtering profiles exist, the custom category will not have any impact on other profiles. For example, if you have two URL Filtering profiles and the custom URL category is set to block in one profile, if you do not want the "block" action to apply to the other profile, you must set the action to **none**. Also, to delete a custom URL category, the category must be set to **none** in any profile where it is used.



File Blocking Security Profile Actions

Field	Description
Name	Enter a rule name (up to 31 characters in length).
Applications	Select the applications the rule applies to or select **Any**.
File Types	Click in the field and then click **Add** to display a list of supported file types. Click a file type to add it to the profile and continue to add file types as needed. If you select **Any**, the defined action is taken on all supported file types.
Direction	Select the direction of the file transfer (**upload**, **download**, or **both**).
Action	Select the action taken when the selected file types are detected: • **alert:** An entry is added to the Threat log. • **block:** The file is blocked. • **continue:** A message to the user indicates that a download has been requested and asks the user to confirm whether to continue. The purpose is to warn the user of a possible unknown download (also known as a drive-by-download) and to give the user the option of continuing or stopping the download.

When you create a File Blocking profile with the action “continue,” you can choose only the application web-browsing. If you choose any other application, traffic that matches the security policy will not flow through the firewall because the users will not be prompted with a continue page.



Sample question

85. Which two actions are available for Antivirus security profiles? (Choose two.)
    A. continue
    B. allow
    C. block IP
    D. alert

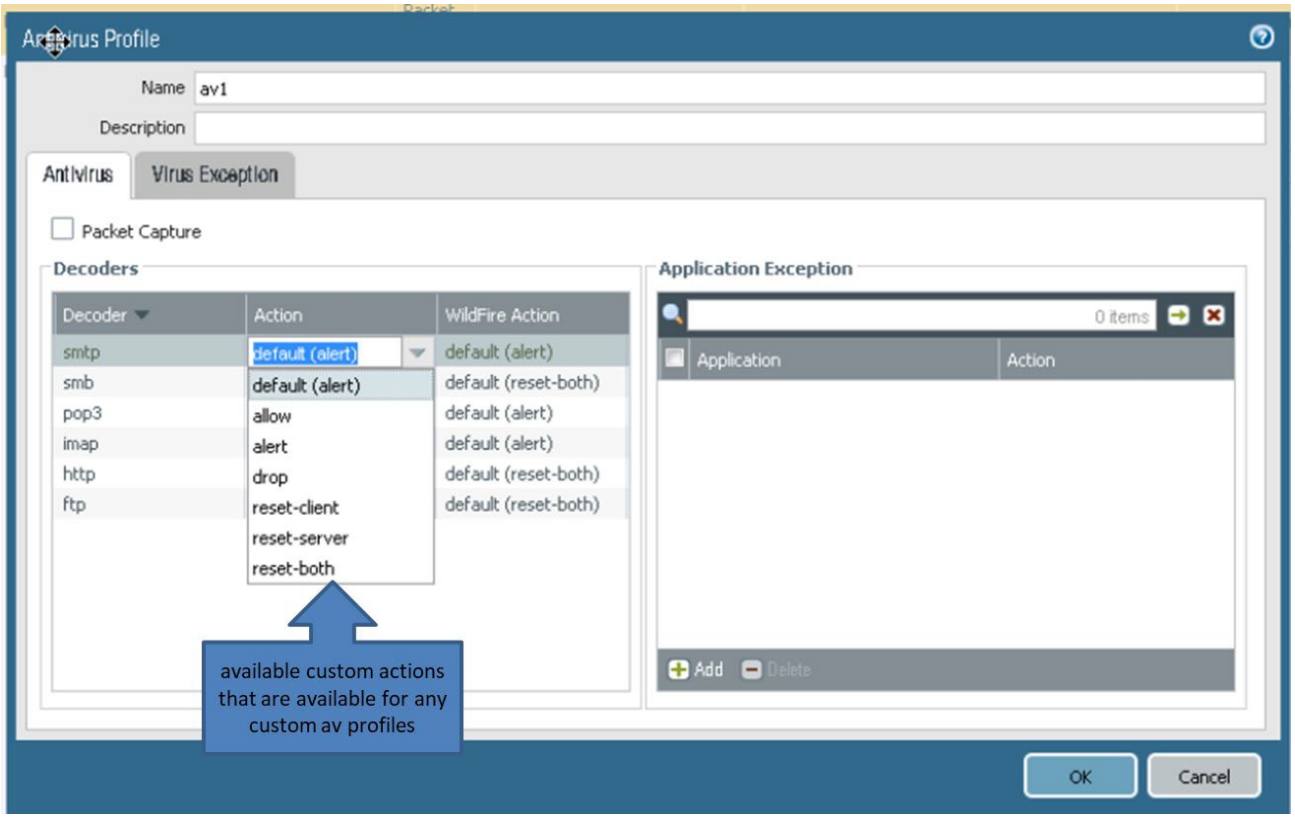
Exam Domain 4 – Securing Traffic

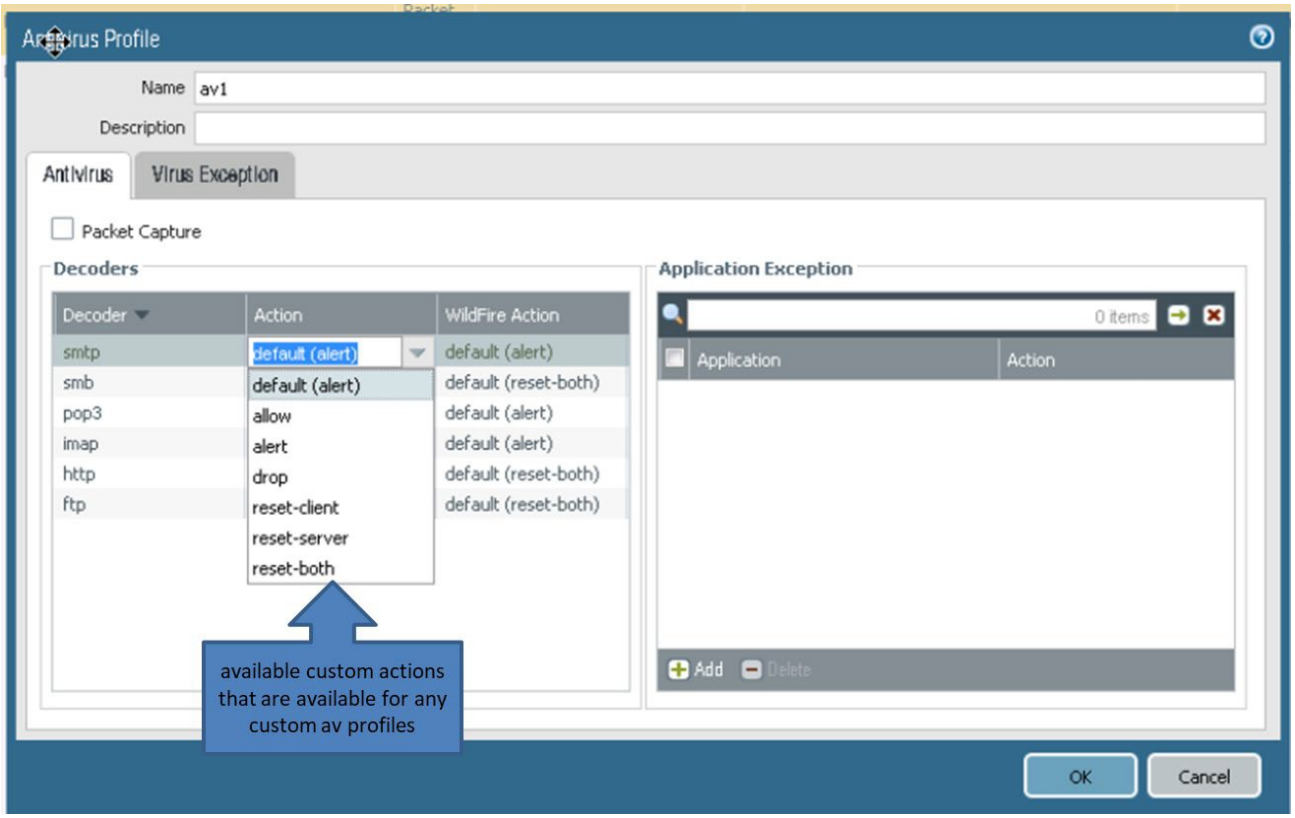
4.3 Given a network scenario, identify how to customize security profiles.

Antivirus Security Profile Customization

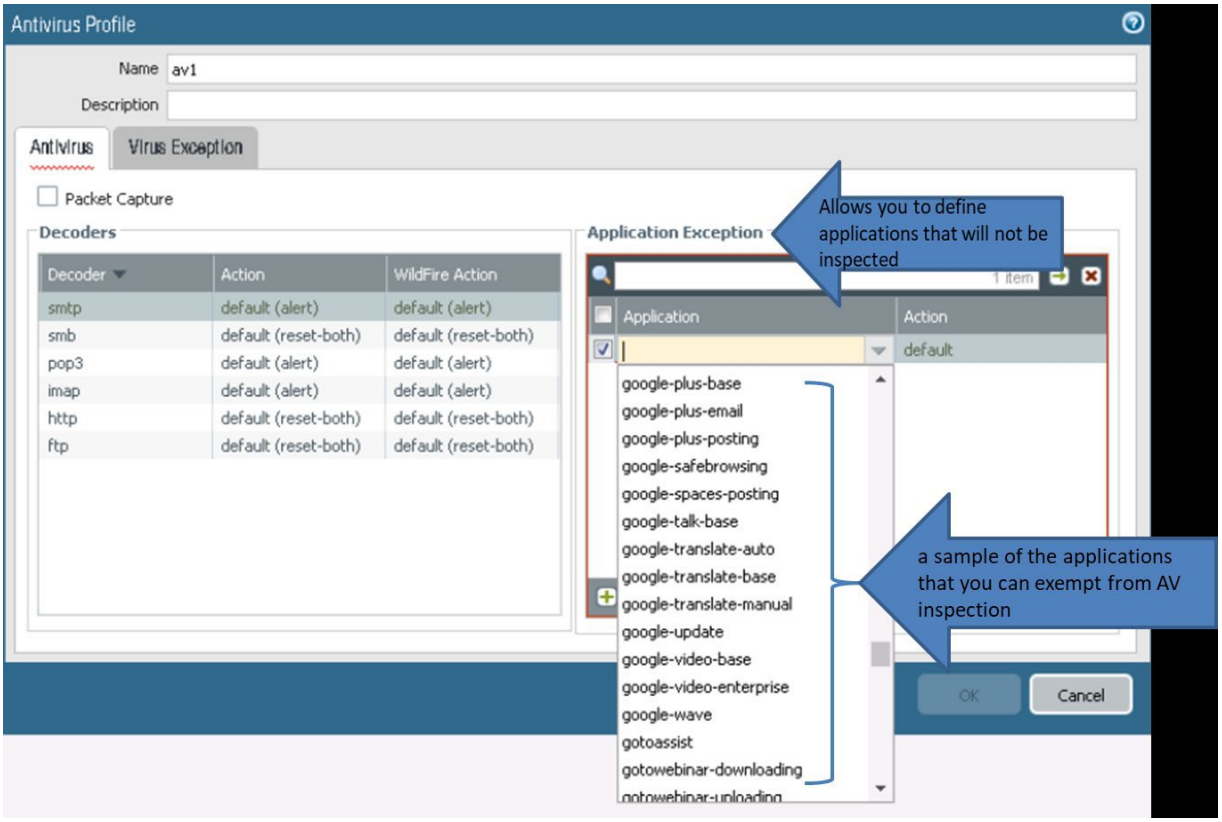
Customized profiles can be used to minimize antivirus inspection for traffic between more trusted security zones. They also can be used to maximize the inspection of traffic received from less trusted zones such as the internet and of traffic sent to highly sensitive destinations such as server farms. The Palo Alto Networks WildFire product also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded daily by Threat Prevention subscribers (sub-hourly for WildFire subscribers).

Antivirus Security Profile Customization for Decoder Actions

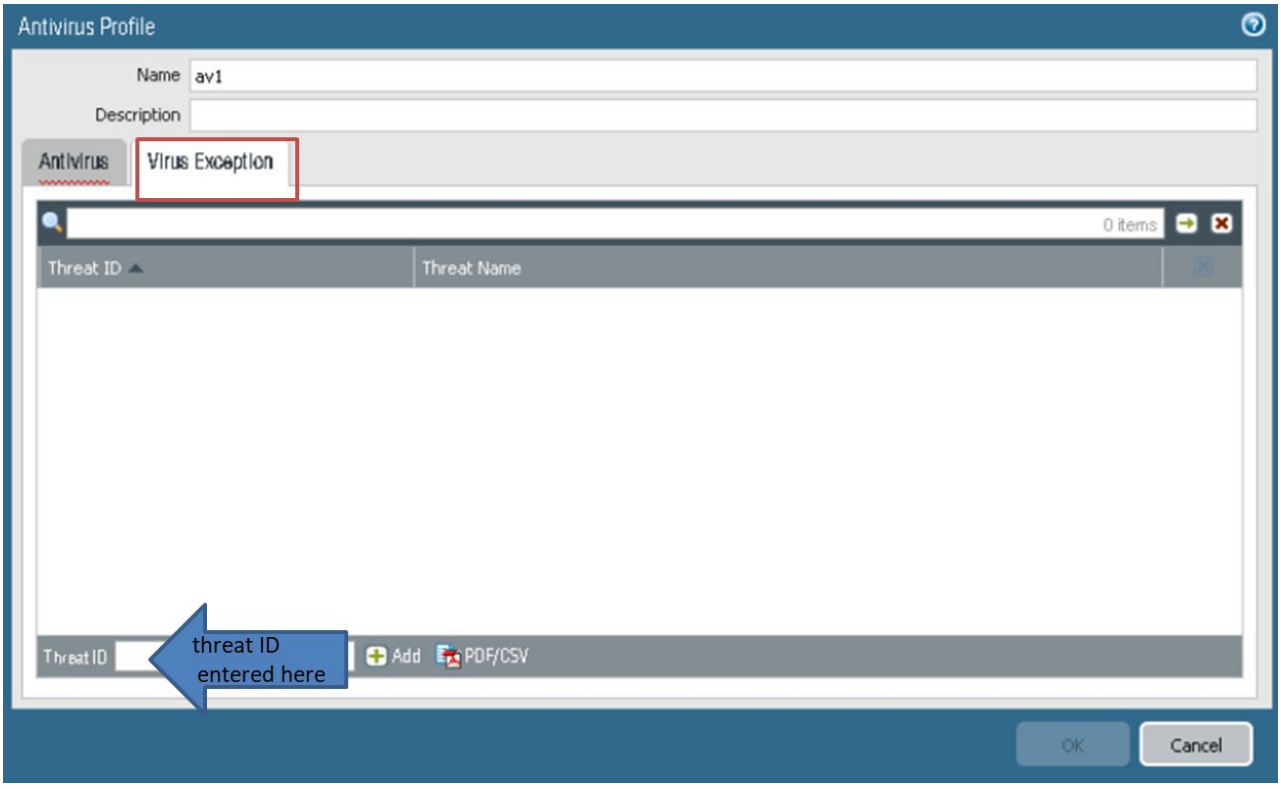

Antivirus Profile
Name av1
Description
Antivirus
Virus Exception
Packet Capture
Decoders
Decoder
Action
WildFire Action
smtp default (alert) default (alert)
smb default (reset-both)
pop3 default (alert)
imap default (alert)
http default (reset-both)
ftp default (reset-both)
default (alert)
allow
alert
drop
reset-client
reset-server
reset-both
Application Exception
0 items
Application
Action
Add
Delete
available custom actions that are available for any custom av profiles
OK
Cancel


Antivirus Profile
Name av1
Description
Antivirus
Virus Exception
Packet Capture
Decoders
Decoder
Action
WildFire Action
smtp default (alert) default (alert)
smb default (reset-both)
pop3 default (alert)
imap default (alert)
http default (reset-both)
ftp default (reset-both)
default (alert)
allow
alert
drop
reset-client
reset-server
reset-both
Application Exception
0 items
Application
Action
Add
Delete
available custom actions that are available for any custom av profiles
OK
Cancel

Antivirus Security Profile Customization to Exclude Specific Apps from AV Inspection



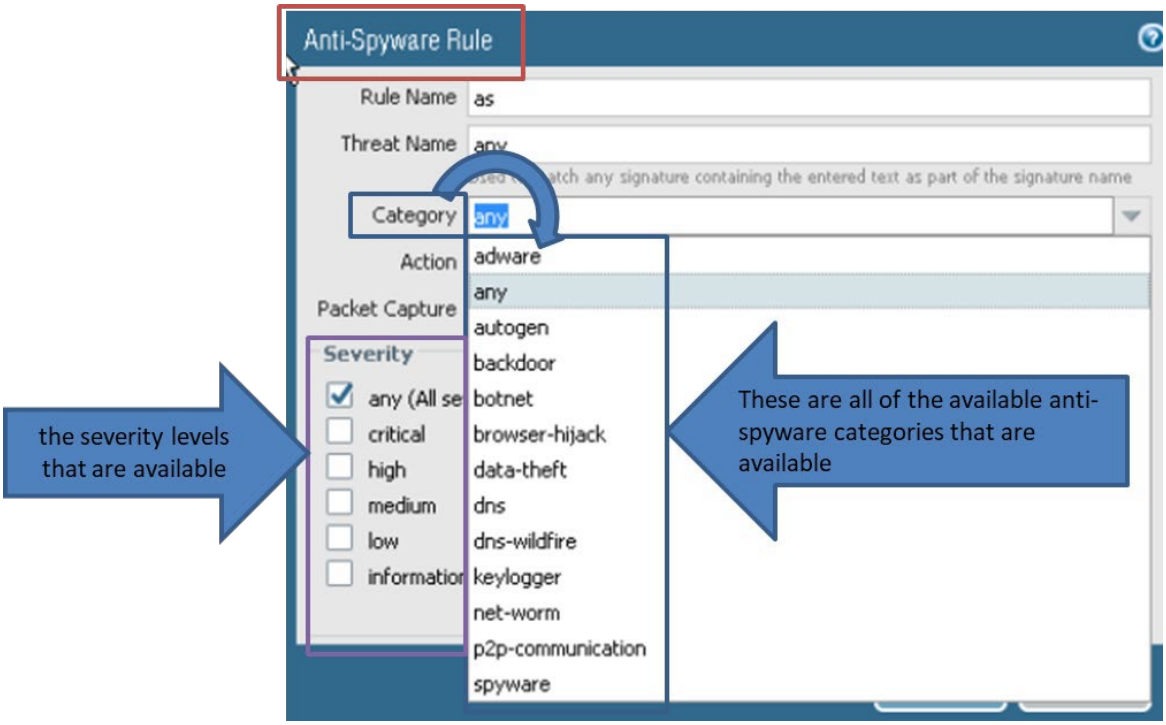
Antivirus Security Profile Customization to Exclude Threats from AV Inspection



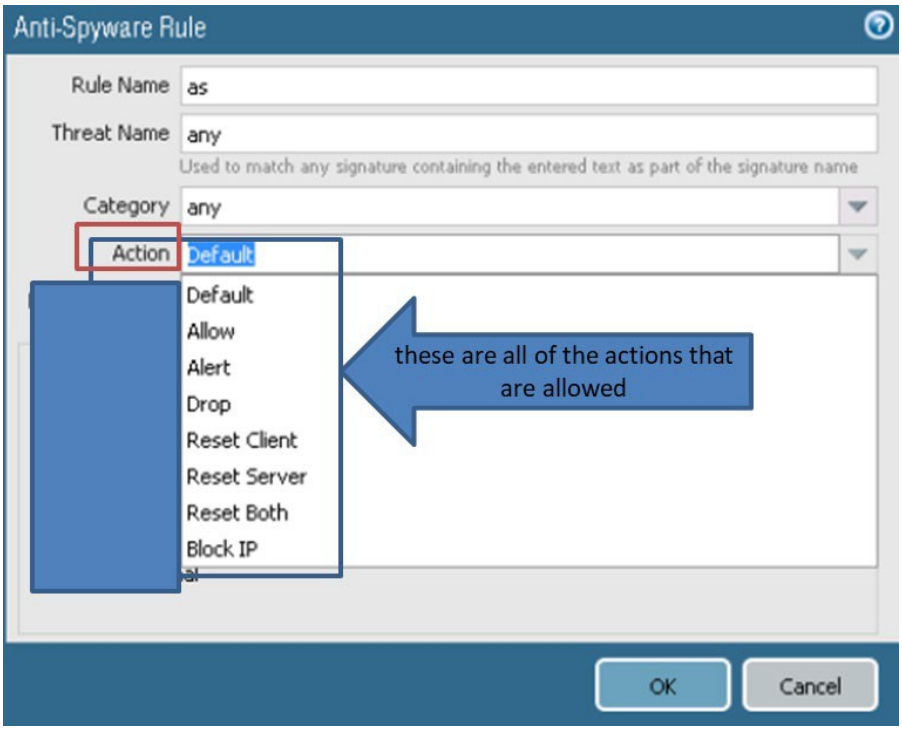
Anti-Spyware Security Profile Customization

Custom Anti-Spyware profiles can be created. For example, you can reduce the stringency for anti-spyware inspection for traffic between more trusted security zones and maximize the inspection of traffic received from the internet or traffic sent to protected assets such as server farms.

Anti-Spyware Security Profile Customization of Categories



Anti-Spyware Security Profile Customization of Actions

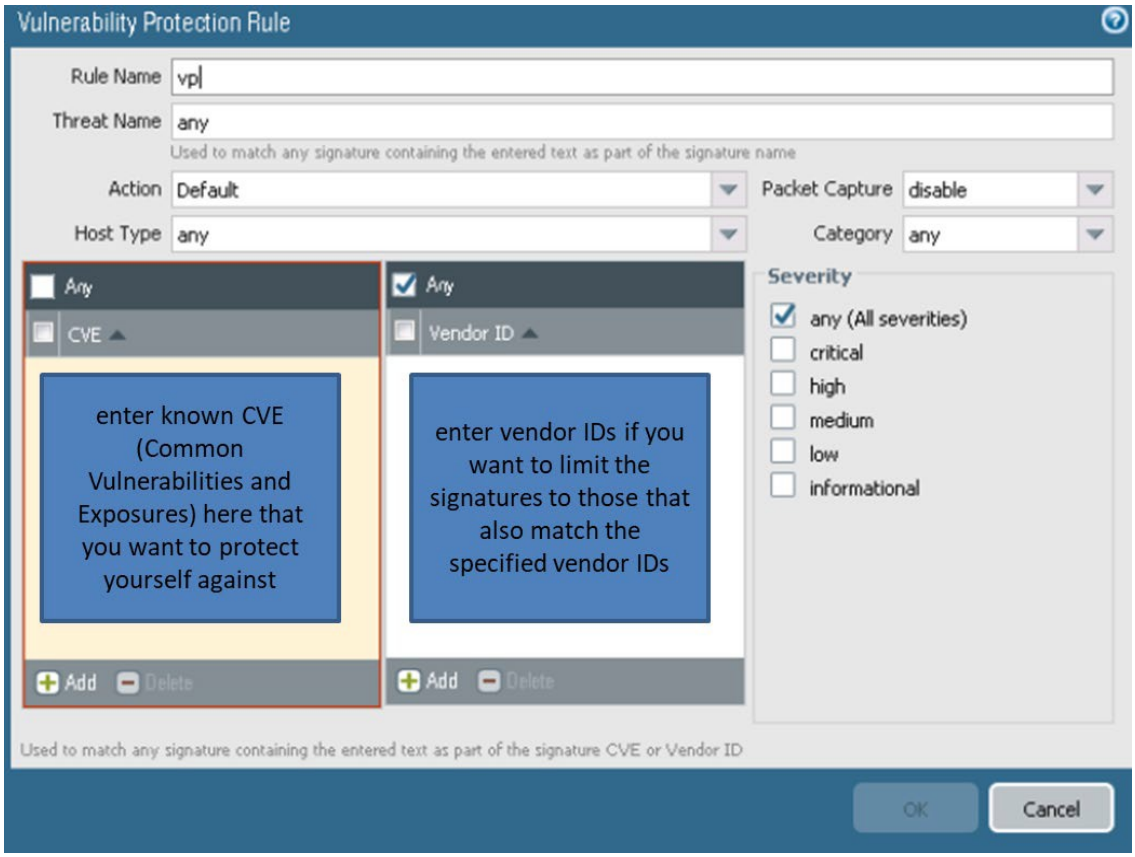


Vulnerability Protection Security Profile Customization

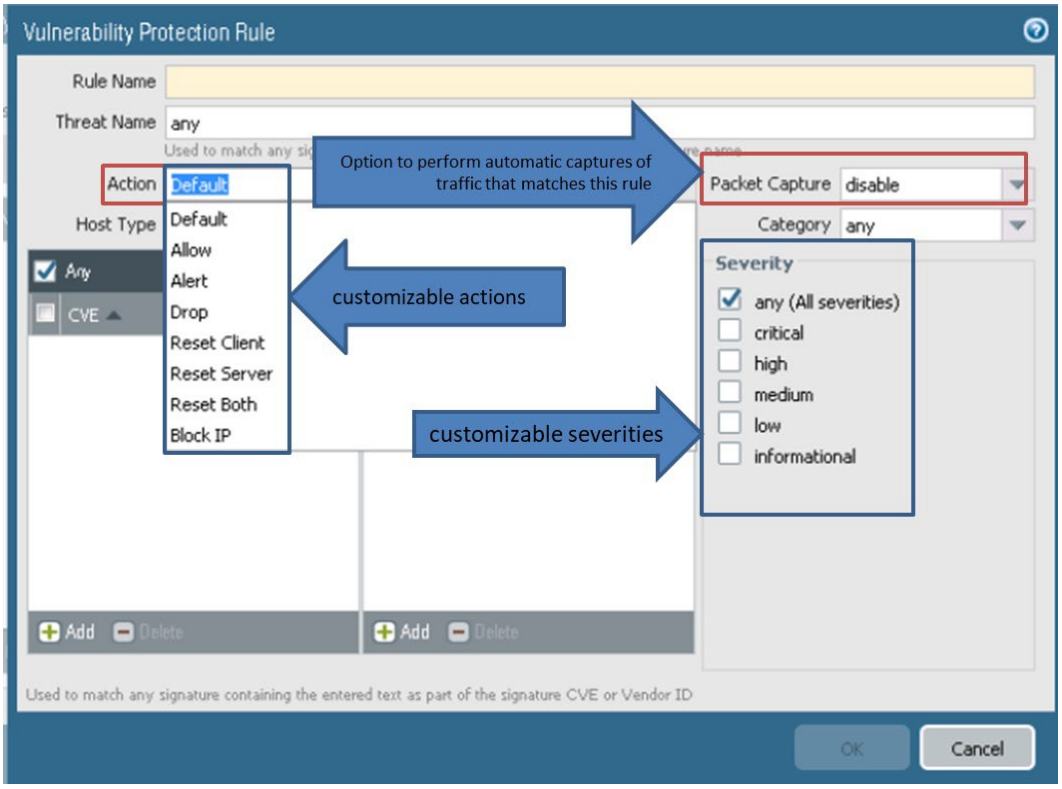
The *default* Vulnerability Protection security profile protects clients and servers from all known critical-, high-, and medium-severity threats. Customized profiles can be used to minimize vulnerability checking for traffic between more trusted security zones and to maximize protection for traffic received from less trusted zones such as the internet, along with traffic sent to highly sensitive destinations such as server farms.

The **Exceptions** setting found under the **Exceptions** tab enables you to change the response for a specific signature based on its Threat ID number or name. For example, you can block all packets that match specific signatures, except for the one(s) that you set up as exception(s), which could be set up as an action to generate only alerts.

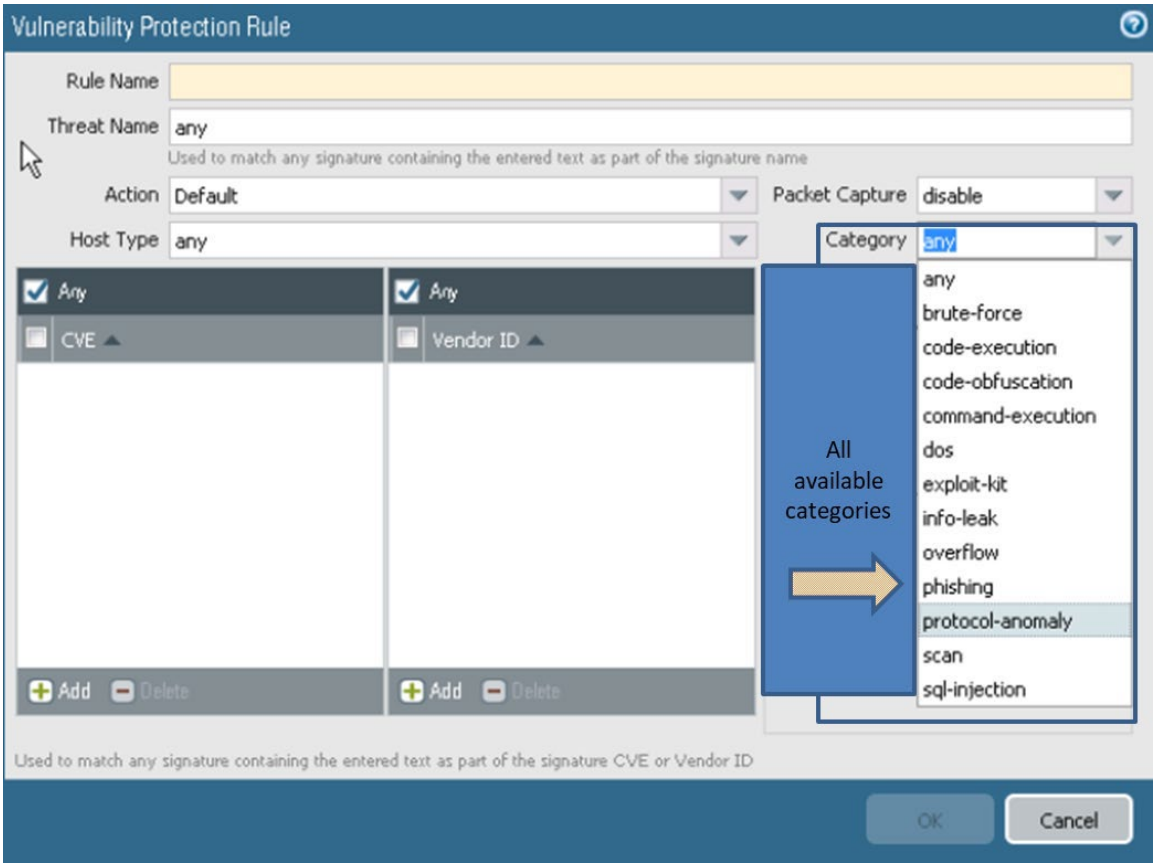
Vulnerability Protection Profile Customization of CVEs and Vendor IDs



Vulnerability Protection Profile Customization of Actions and Severity



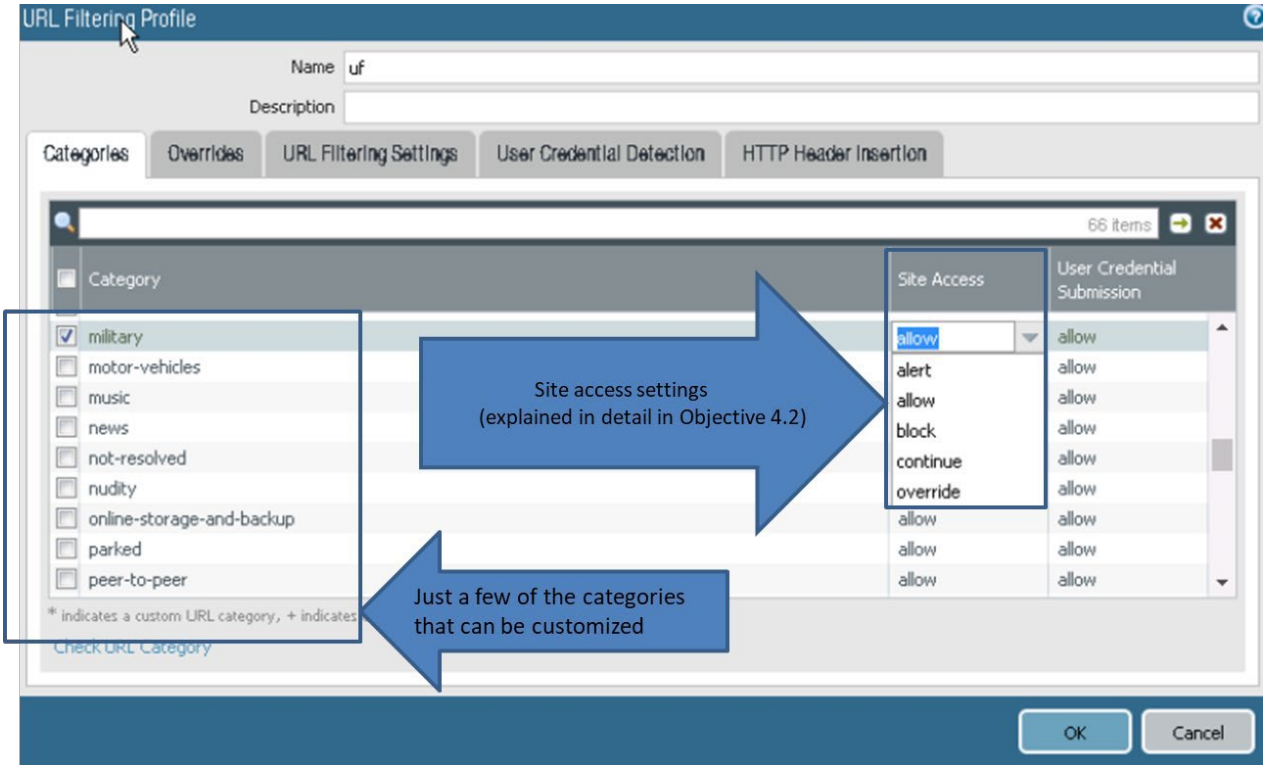
Vulnerability Protection Profile Customization of Categories



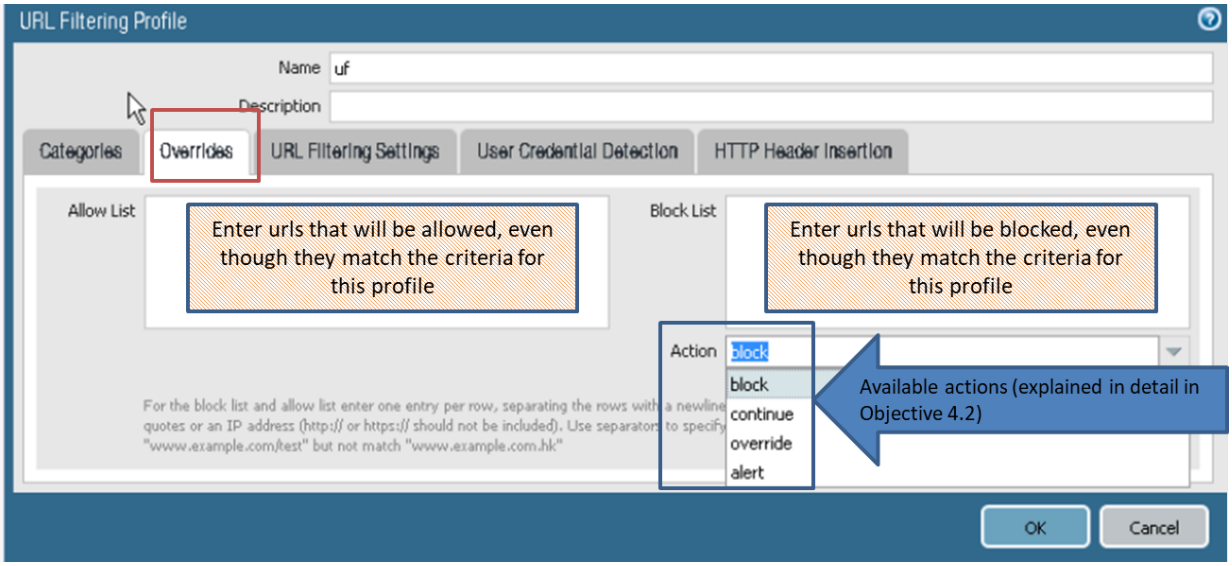
URL Filtering Security Profile Customization

URL Filtering security profiles should be customized to meet the unique needs of your organization.

URL Filtering Profile Customization of Categories and Site Access



URL Filtering Profile Customization Using Overrides



Safe Search

Many search engines have a safe search setting that filters out pornographic images and videos in search query return traffic. When **Safe Search Enforcement** is enabled, the firewall blocks search results if the end user is not using the strictest safe search settings in the search query. The firewall can enforce safe search for the following search providers: Google, Yahoo, Bing, Yandex, and YouTube. This is a best-effort setting and is not guaranteed by the search providers to work with every website.

HTTP Header Logging

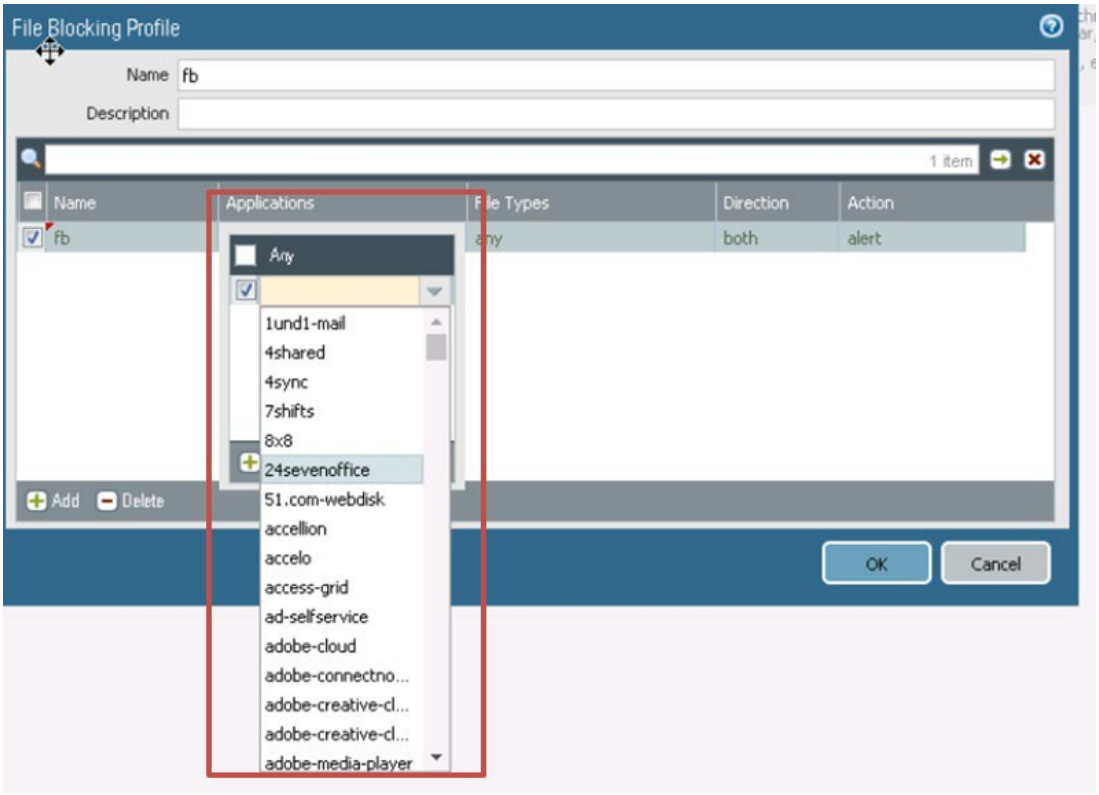
The **HTTP Header Logging** feature provides visibility into the attributes included in the HTTP request sent to a server. When HTTP Header Logging is enabled, one or more of the following attributes are recorded in the URL Filtering log:

- **User Agent:** The web browser that the user used to access the URL. This information is sent in the HTTP request to the server. For example, the User Agent can be Internet Explorer or Firefox.
- **Referrer:** The URL of the webpage that linked the user to another webpage. It is the source that redirected (referred) the user to the webpage that is being requested.
- **X-Forward-For**: The header field option that preserves the IP address of the user who requested the webpage. It enables you to identify the IP address of the user, which is particularly useful if you have a proxy server on you network or you have implemented source NAT that is masking the user's IP address such that all requests seem to originate from the proxy server's IP address or a common IP address.

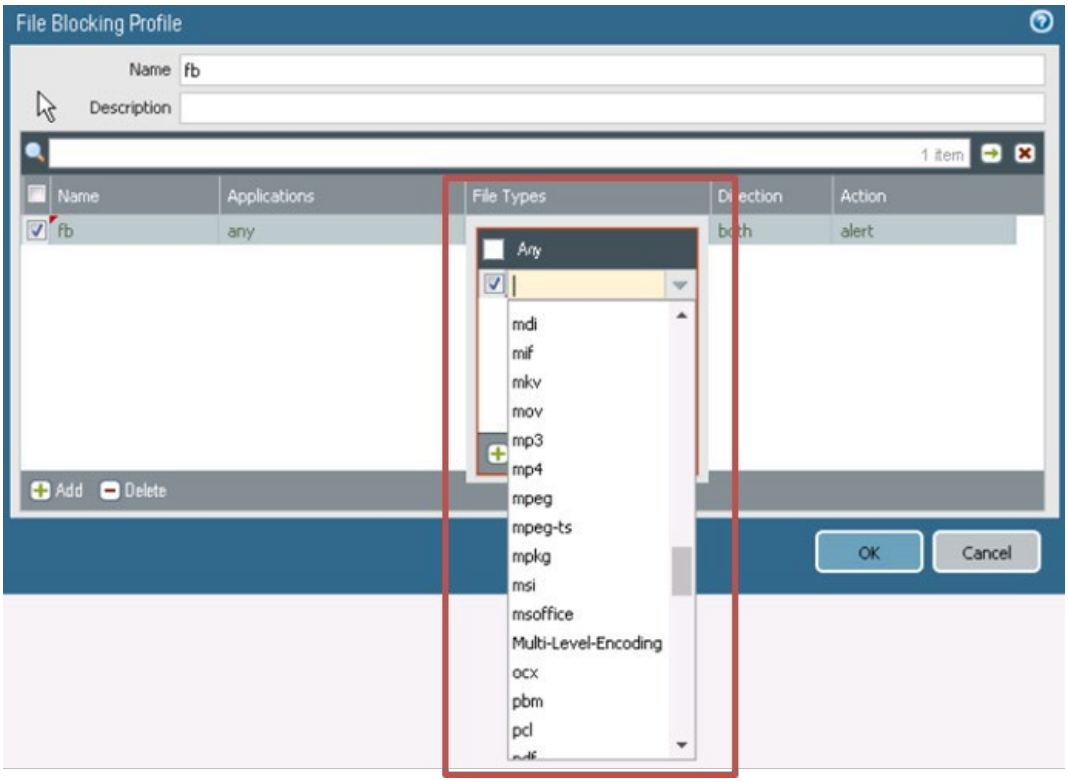
File Blocking Security Profile Customization

File blocking should be customized to meet the unique needs of your organization.

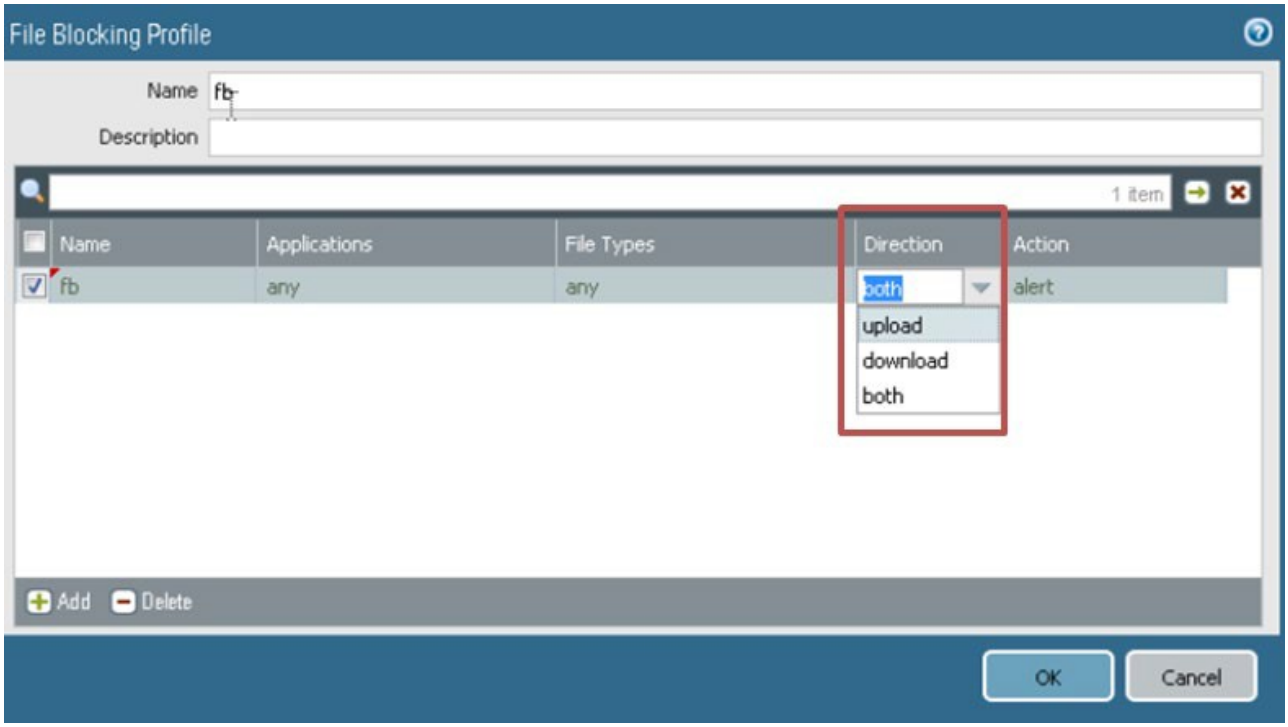
File Blocking Applications Customization



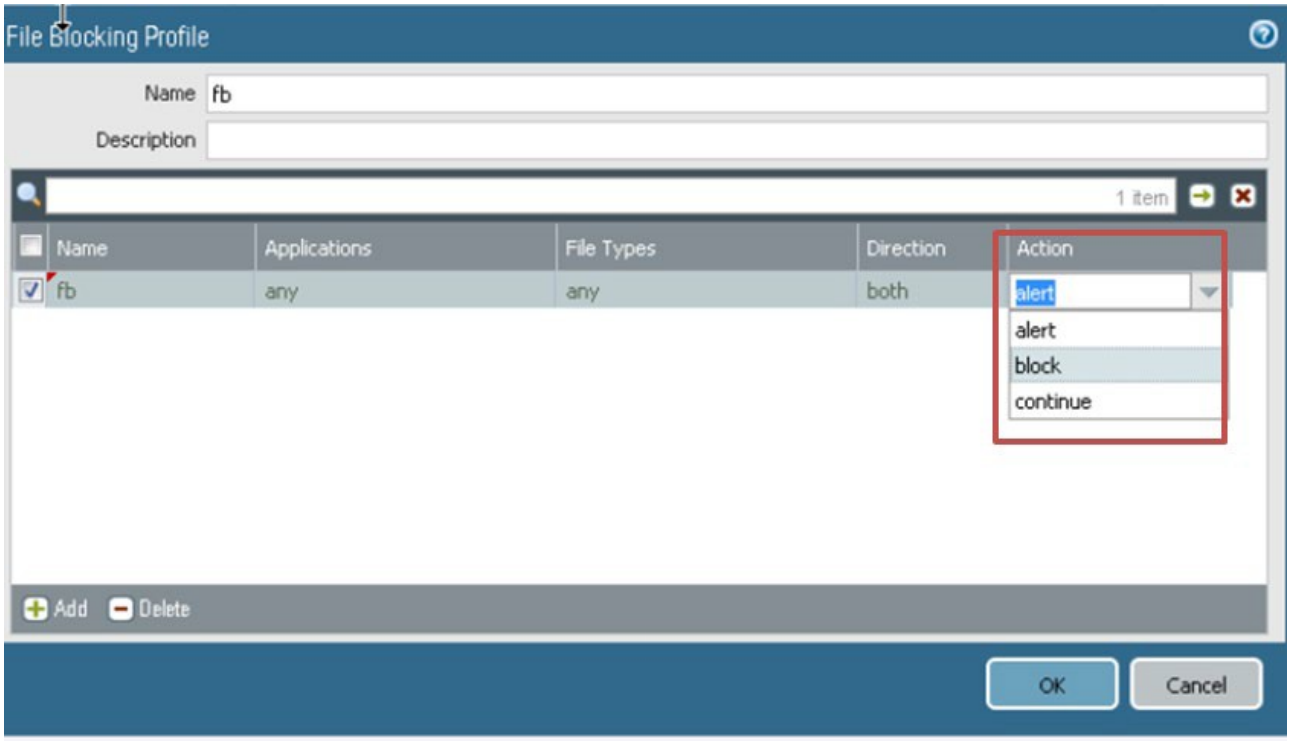
File Blocking File Types Customization



File Blocking Direction Customization



File Blocking Action Customization



Sample question

86. Which two HTTP Header Logging options are within a URL Filtering profile? (Choose two.)
    A. User-Agent
    B. Safe Search
    C. URL redirection
    D. X-Forwarded-For

Exam Domain 4 – Securing Traffic

4.4 Identify the firewall's protection against packet- and protocol-based attacks.

Denial-of-Service Protection

PAN-OS software does not only provide protection using security policy rule's and security profiles, which use signatures and heuristics to identify attacks. PAN-OS software also provides denial-of-service (DoS) protection, which is based on analysis of packet headers to detect threats rather than signatures.

A DoS attack attempts to make network devices unreachable by disrupting services. These attacks usually come from the internet but can come from misconfigured or compromised internal devices. The typical method is to flood the target with resource requests until the requests consume all the target's available resources: memory, CPU cycles, and bandwidth. Typical targets are internet-facing devices that users can access from outside the corporate network such as web servers and database servers. Palo Alto Networks firewalls provide the following three DoS attack mitigation tools as part of a layered approach to DoS protection. Note that packet buffer protection will not be described in this section.

- **Zone Protection profiles**: Apply only to new sessions in ingress zones and provide broad protection against flood attacks by limiting the connections-per-second (CPS) to the firewall, plus protection against reconnaissance (port scans and host sweeps), packet-based attacks, and Layer 2 protocol-based attacks.
- **DoS Protection profiles and policy rules**: Provide granular protection of specific, critical devices for new sessions. Classified profiles protect individual devices by limiting the CPS for a specific device or specific devices. Aggregate profiles limit the total CPS for a group of devices but don't limit the CPS for a particular device in the group to less than the total allowed for the group, so one device still might receive most of the connection requests.
- **Packet buffer protection:** Protects against single-session DoS attacks that attempt to overwhelm the firewall's packet buffer.

Zone Protection Profiles

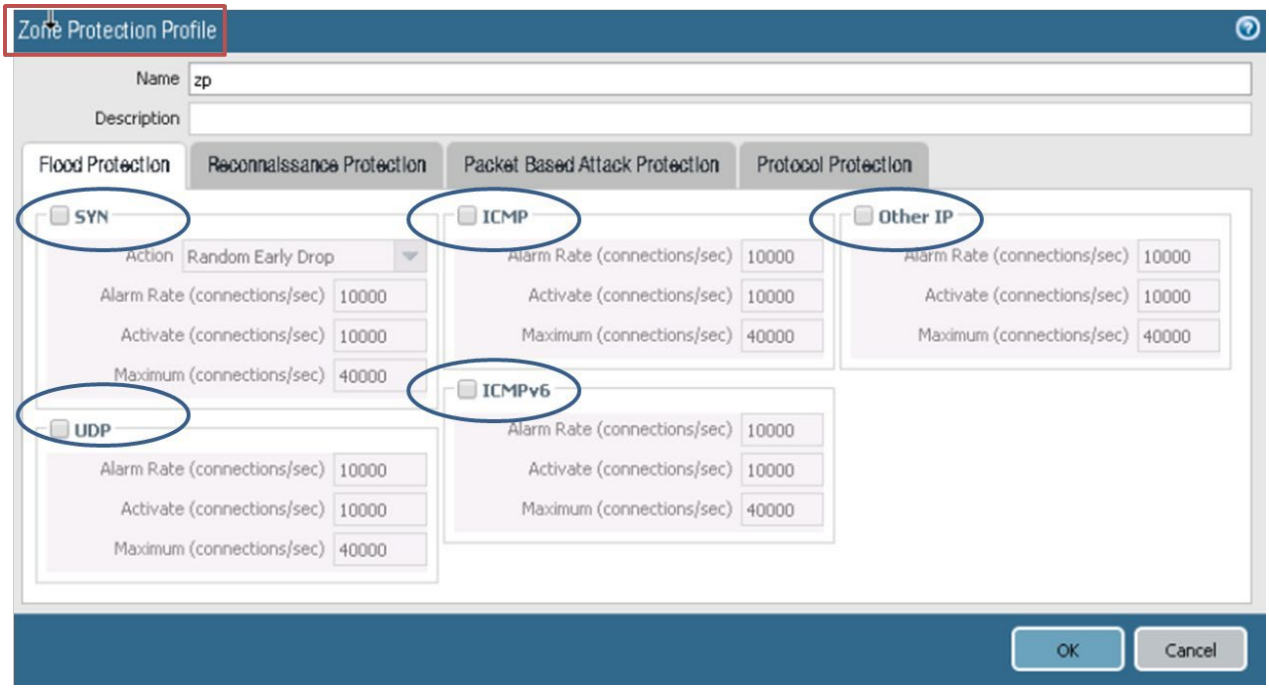
A Zone Protection profile is applied to an ingress zone. It offers protection against floods, reconnaissance attacks, and other packet-based attacks. Zone protection is broad-based protection and is not designed to protect a specific end host or traffic going to a particular destination zone. Only a single Zone Protection profile can be applied to a zone. Zone protection is enforced only when there is no session match for the packet because zone protection is based on new CPS, not on packets per second (pps). If the packet matches an existing session, it will bypass the Zone Protection profiles.

Flood Attack Protection

Zone Protection profiles protect against of five types of floods:

- SYN (TCP)
- UDP
- ICMP
- ICMPv6
- Other IP

Flood Protection Activate Rates



SYN Random Early Drop

This feature causes TCP SYN packets to be dropped to mitigate a flood attack. When the flow exceeds the **Activate** rate threshold, the firewall drops individual SYN packets randomly to restrict the flow. When the flow exceeds the **Maximum** rate threshold, 100% of incoming SYN packets are dropped.

SYN Cookies

This feature causes the firewall to act like a proxy, intercept the TCP SYN, generate a cookie on behalf of the server to which the SYN was directed, and send a SYN-ACK with the cookie to the original source. Only when the source returns an ACK with the cookie to the firewall does the firewall consider the source valid and forward the SYN to the server. This is the preferred configuration option.

UDP

UDP flood protection is activated when the number of UDP packets (not matching an existing session) the zone receives per second exceeds the **Activate** threshold. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the **Maximum** rate. The firewall stops dropping the UDP packets if the incoming rate drops below the **Activate** threshold.

ICMP

ICMP flood protection is activated when the number of ICMP packets (not matching an existing session) the zone receives per second exceeds the **Activate** threshold. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the **Maximum** rate. The firewall stops dropping the ICMP packets if the incoming rate drops below the **Activate** threshold.

ICMPv6

ICMPv6 flood protection is activated when the number of ICMPv6 packets (not matching an existing session) the zone receives per second exceeds the **Activate** threshold. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the **Maximum** rate. The firewall stops dropping the ICMPv6 packets if the incoming rate drops below the **Activate** threshold.

Other IP

Other IP flood protection is activated when number of non-IP packets (not matching an existing session) the zone receives per second exceeds the **Activate** threshold. The firewall uses an algorithm to progressively drop more packets as the attack rate increases, until the rate reaches the **Maximum** rate. The firewall stops dropping the Other IP packets if the incoming rate drops below the **Activate** threshold.

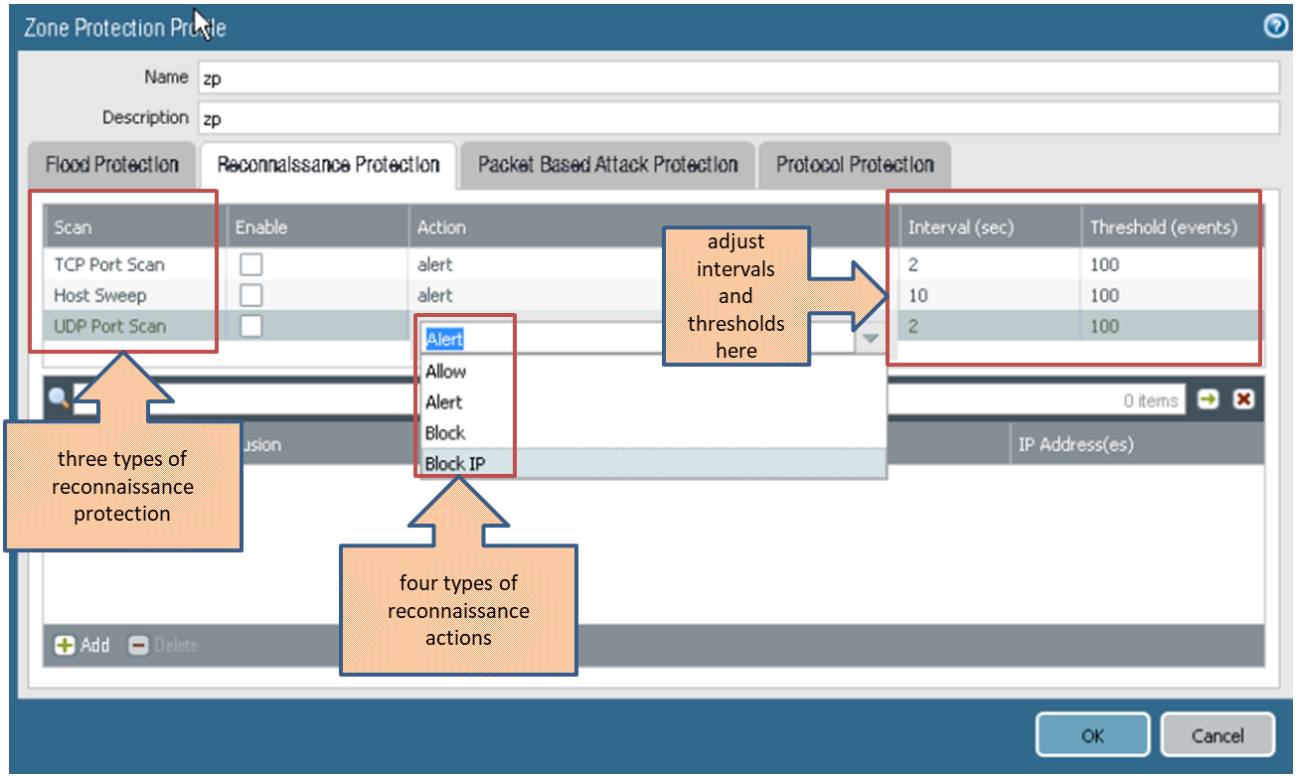
Reconnaissance Attack Protection

Reconnaissance protection protects against reconnaissance attacks, which are the first type of attacks within a Cyber-Attack Lifecycle. During the first stage of the attack lifecycle, cyberattackers carefully plan their method of attack. They research, identify, and select targets within an organization such as human resources and financial personnel that will enable them to meet their objectives. Attackers can gather intelligence through publicly available sources such as Twitter, LinkedIn, and corporate websites – all the places where a company will share information about itself. The cyberattackers also will scan for vulnerabilities that can be exploited within the target network (services and applications), and map out resources that they can take advantage of.

Prevent by:

- Performing continuous inspection of network traffic flows to detect and prevent port scans and host sweeps
- Implementing security awareness by limiting what should be posted on the internet: sensitive documents, customer lists, event attendees, job roles, and responsibilities

See Palo Alto Networks documentation for more detail about these complicated types of attacks.

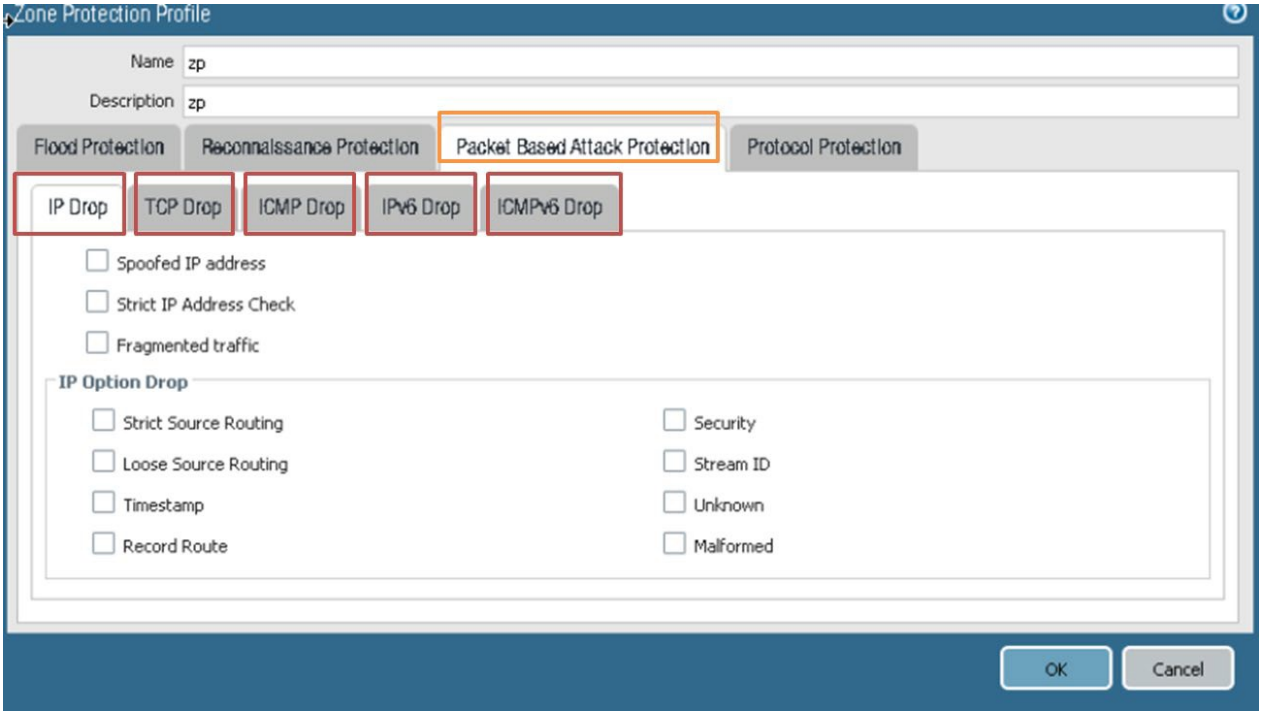


Packet-Based Attack Protection

There are many types of packet-based attack protection. Each one will not be covered in detail in this section. Please refer to Palo Alto Networks documentation to obtain more detail on these complicated types of attacks.

The five major categories of packet-based attack protection are:

- IP Drop
- TCP Drop
- ICMP Drop
- IPv6 Drop
- ICMPv6 Drop



Packet-based attacks take many forms. Zone Protection profiles check IP, TCP, ICMP, IPv6, and ICMPv6 packet headers and protect a zone by:

- Dropping packets with undesirable characteristics
- Stripping undesirable options from packets before admitting them to the zone

Select the drop characteristics for each packet type when you configure packet-based attack protection. The best practices for each IP protocol are:

- **IP Drop**: Drop **Unknown** and **Malformed** packets. Also drop **Strict Source Routing** and **Loose Source Routing** because allowing these options permits adversaries to bypass security policy rules that use the destination IP address as the matching criterion. For internal zones only, check **Spoofed IP Address** so only traffic with a source address that matches the firewall routing table can access the zone.
- **TCP Drop**: Retain the default **TCP SYN with Data** and **TCP SYNACK with Data** drops, drop **Mismatched overlapping TCP segment** and **Split Handshake** packets, and strip the **TCP Timestamp** from packets.

Enable the **Rematch Sessions** option as a best practice. It applies committed newly configured or edited security policy rules to existing sessions. However, if you configure **Tunnel Content Inspection** on a zone and **Rematch Sessions** is enabled, you also must disable **Reject Non-SYN TCP** (change the selection from **Global** to **No**). If you don't disable that option, when you enable or edit a **Tunnel Content Inspection** policy the firewall will drop all existing tunnel sessions. Create a separate Zone Protection profile to disable **Reject Non-SYN TCP** only on zones that have **Tunnel Content Inspection** policies and only when you enable **Rematch Sessions**.

- **ICMP Drop**: There are no standard best practice settings because dropping of ICMP packets depends on how you use ICMP (or if you use ICMP). For example, if you want to block ping activity, you can block **ICMP Ping ID 0**.

- **IPv6 Drop**: If compliance matters, ensure that the firewall drops packets with non-compliant routing headers, extensions, etc.
- **ICMPv6 Drop**: If compliance matters, ensure that the firewall drops certain packets if the packets don't match a security policy rule.

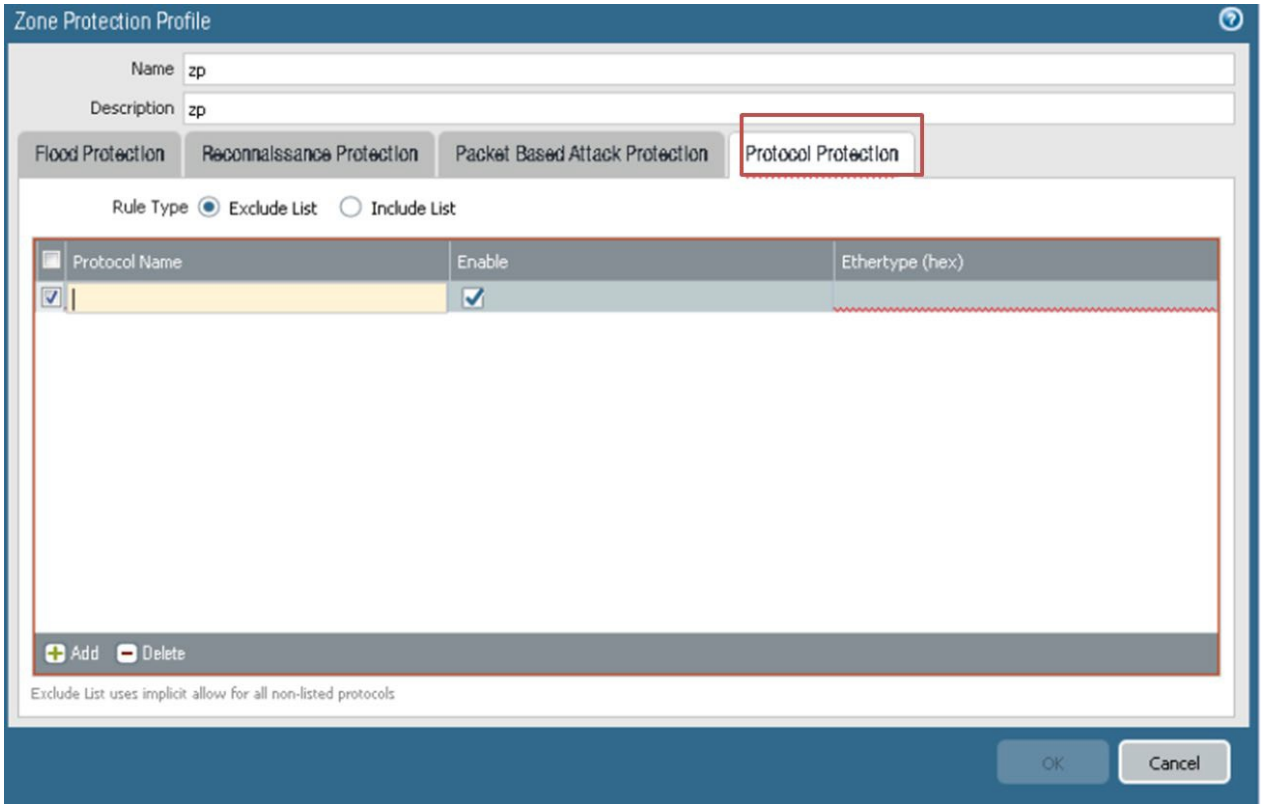
Protocol Attack Protection

In a Zone Protection profile, **Protocol Protection** defends against non-IP protocol-based attacks. Enable **Protocol Protection** to block or allow non-IP protocols between security zones on a Layer 2 VLAN or on a virtual wire, or between interfaces within a single zone on a Layer 2 VLAN (Layer 3 interfaces and zones drop non-IP protocols, so non-IP **Protocol Protection** doesn't apply).

Configure **Protocol Protection** to reduce security risks and facilitate regulatory compliance by preventing less secure protocols from entering a zone or an interface in a zone. If you don't configure a Zone Protection profile that prevents non-IP protocols in the same zone from going from one Layer 2 interface to another, the firewall allows the traffic because of the default intrazone allow security policy rule. You can create a Zone Protection profile that blocks protocols such as LLDP within a zone to prevent discovery of networks reachable through other zone interfaces.

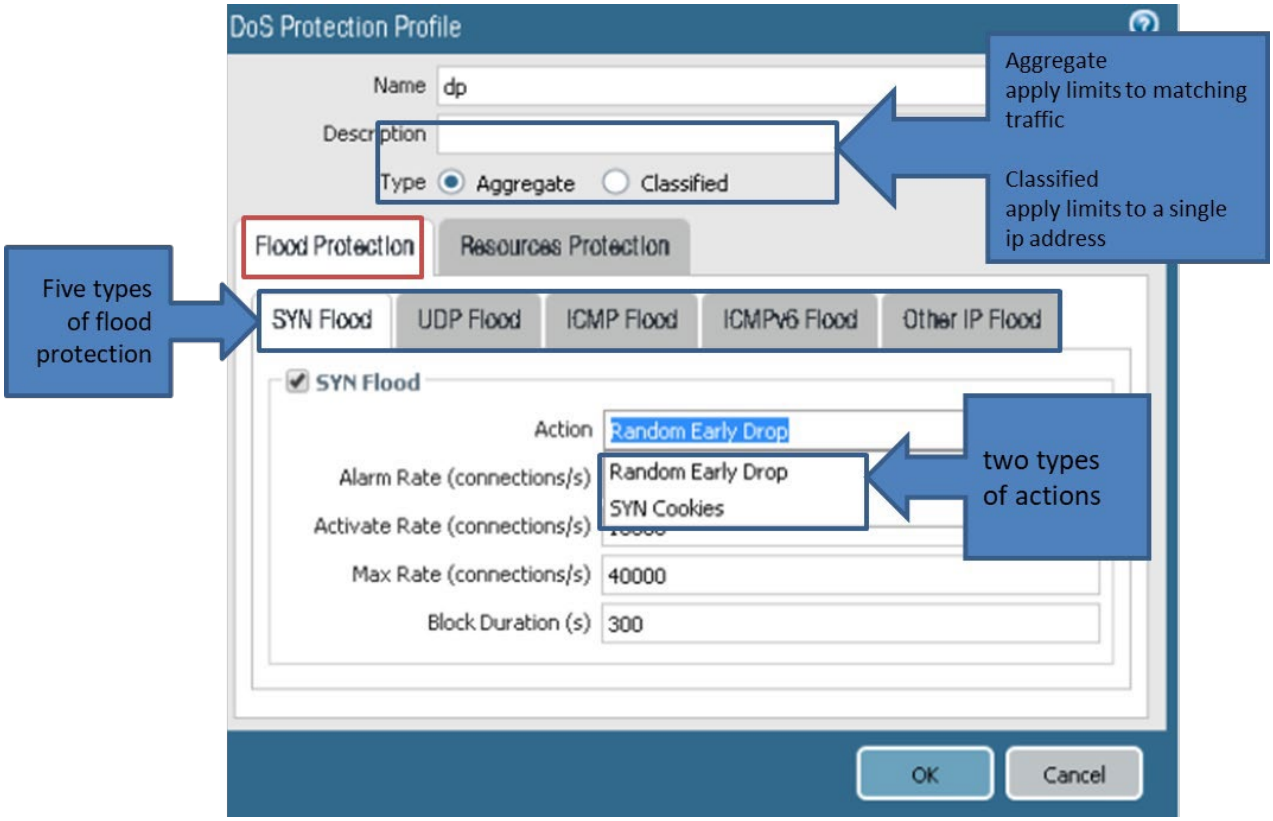
If you need to discover which non-IP protocols are running on your network, use monitoring tools such as NetFlow, Wireshark, or other third-party tools. Examples of non-IP protocols you can block or allow are LLDP, NetBEUI, Spanning Tree, and Supervisory Control and Data Acquisition (SCADA) systems such as Generic Object Oriented Substation Event (GOOSE), among many others.

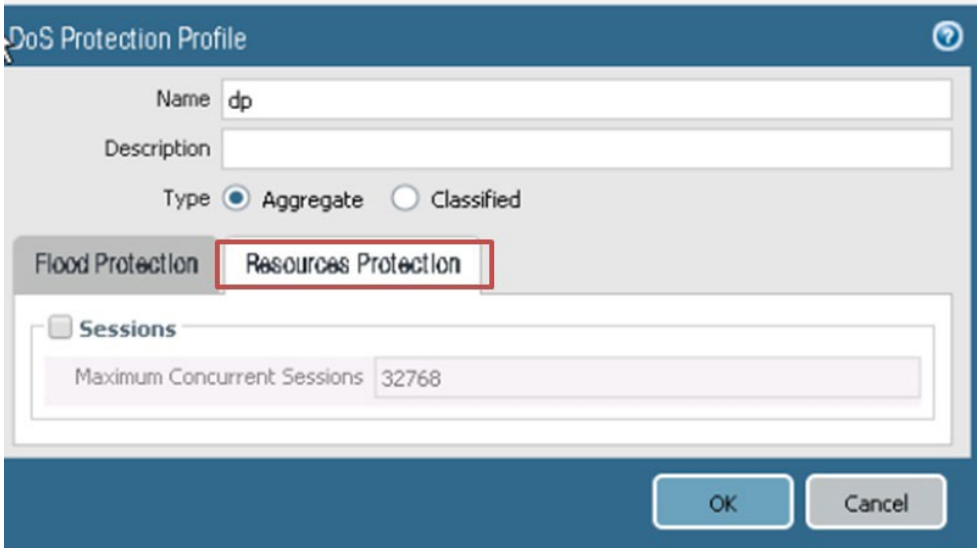
Create an **Exclude List** or an **Include List** to configure **Protocol Protection** for a zone. The **Exclude List** is a blacklist—the firewall blocks all the protocols you place in the **Exclude List** and allows all other protocols. The **Include List** is a whitelist—the firewall allows only the protocols you specify in the list and blocks all other protocols. Use include lists for **Protocol Protection** instead of exclude lists. Include lists specifically sanction only the protocols you want to allow and block the protocols you don't need or didn't know were on your network, which reduces the attack surface and blocks unknown traffic. A list supports up to 64 Ethertype entries, each identified by its IEEE hexadecimal Ethertype code. When you configure zone protection for non-IP protocols on zones that have Aggregated Ethernet (AE) interfaces, you can't block or allow a non-IP protocol on only one AE interface member because AE interface members are treated as a group.



DoS Protection Profiles and Policies

DoS Protection profiles and DoS Protection policy rules combine to protect specific groups of critical resources and individual critical resources against session floods. Compared to Zone Protection profiles, which protect entire zones from flood attacks, DoS protection provides granular defense for specific systems, especially critical systems that users access from the internet and often are attack targets, such as web servers and database servers. Apply both types of protection because if you only apply a Zone Protection profile, then a DoS attack that targets a particular system in the zone can succeed if the total CPS doesn't exceed the zone's **Activate** and **Maximum** rates. DoS protection is resource-intensive, so use it only for critical systems. DoS Protection profiles specify flood thresholds, similarly to Zone Protection profiles. DoS Protection policy rules determine the devices, users, zones, and services to which DoS Protection profiles apply. See Palo Alto Networks documentation for more detail about these complicated types of attacks.





Sample question

87. What are the two components of Denial-of-Service Protection? (Choose two.)

A. Zone Protection profile
B. DoS Protection profile and policy rules
C. load protection
D. reconnaissance protection

Exam Domain 4 – Securing Traffic

4.5 Identify how the firewall can use the cloud DNS database to control traffic based on domains.

See the Multi-Category and Risk-Based URL Filtering and the Real-Time Cloud DNS Signatures features in the PAN-OS 9.0 *New Features Guide at* https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features.html.

Exam Domain 4 – Securing Traffic

4.6 Identify how the firewall can use the PAN-DB database to control traffic based on websites.

Most attacks and exposure to malicious content occur during normal web browsing activities, which means that all users must have safe, secure web access. PAN-DB is a global URL and IP database, designed to fulfill an enterprise's web security needs. URL filtering with PAN-DB automatically prevents attacks that leverage the web as an attack vector, including phishing links in emails, phishing sites, HTTP-based command and control, malicious sites, and pages that carry exploit kits.

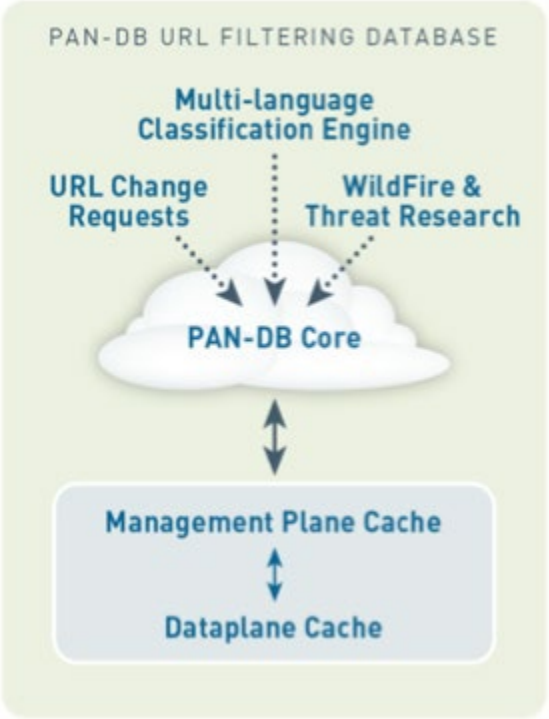
Granular policy enables the prevention of downloads, the automation of warning messages, or the restriction of access altogether. PAN-DB provides real-time protections from emerging attacks. PAN-DB receives updates from WildFire every five minutes to block malicious sites, in addition to other advanced identification techniques.

PAN-DB is tightly integrated into PAN-OS software, thus providing advanced persistent threat (APT) protection with high performance beyond traditional URL filtering. Traditional URL filtering is intended to control unwanted web surfing such as non-business or illegal sites, but it usually doesn't cover up-to-the-minute malicious websites such as newly discovered malware site, exploit site, or command-and-control (C2) sites.

How PAN-DB Maximizes URL Lookup Performance

The following sections describe the components shown in the following figure.

PAN-DB Classification and Cache System



PAN-DB Core

The PAN-DB core, located in the Palo Alto Networks threat intelligence cloud, has a full URL and IP database to cover web security needs.

Management Plane Cache

The PAN-DB database is placed into the management plane cache, which provides quick URL lookups. The management plane cache will pull more URLs and categories from the PAN-DB core as users access sites that are not currently in the management plane cache. Any URL requested by a user is “unknown” to Palo Alto Networks will be examined, categorized, and implemented as appropriate.

Data-Plane Cache

A data-plane cache contains the most frequently accessed sites, which enables quicker URL lookups. The Malicious URL database is delivered from WildFire.

Millions of URLs and IPs are classified in a variety of ways. The PAN-DB receives URLs and IP addresses from the “Multi-language Classification Engine” and from “URL Change Requests from users.” The PAN-DB also receives malicious URL and IP information from WildFire. Examples of malicious URL and the IP database follow:

- **Malware Download URL and IP address:** Prevent from downloading malware
- **C&C URL and IP address:** Disable malware communications

The malicious URLs are generated as WildFire identifies unknown malware, zero-day exploits and APTs by executing them in a virtual sandbox environment.

PAN-DB will block a malicious URL with low latency.

PAN-DB has a superior mechanism that increases the speed of URL lookups, which means that you will get URL category information without sacrificing throughput.

The malicious URLs are generated as WildFire identifies unknown malware, zero-day exploits, and APTs, and executes them in a virtual sandbox environment. The ongoing malicious URL updates to PAN-DB allows you to block malware downloads and disable malware C2 communications.

Use the malicious URL database to block a variety of malicious web access and communication without compromising web access performance.

Sample question

88. Which two types of attacks does the PAN-DB prevent? (Choose two.)
    A. phishing sites
    B. HTTP based command-and-control
    C. infected JavaScript
    D. flood attacks

Exam Domain 4 – Securing Traffic

4.7 Discuss how to control access to specific URLs using custom URL filtering categories.

Custom URL Filtering Categories

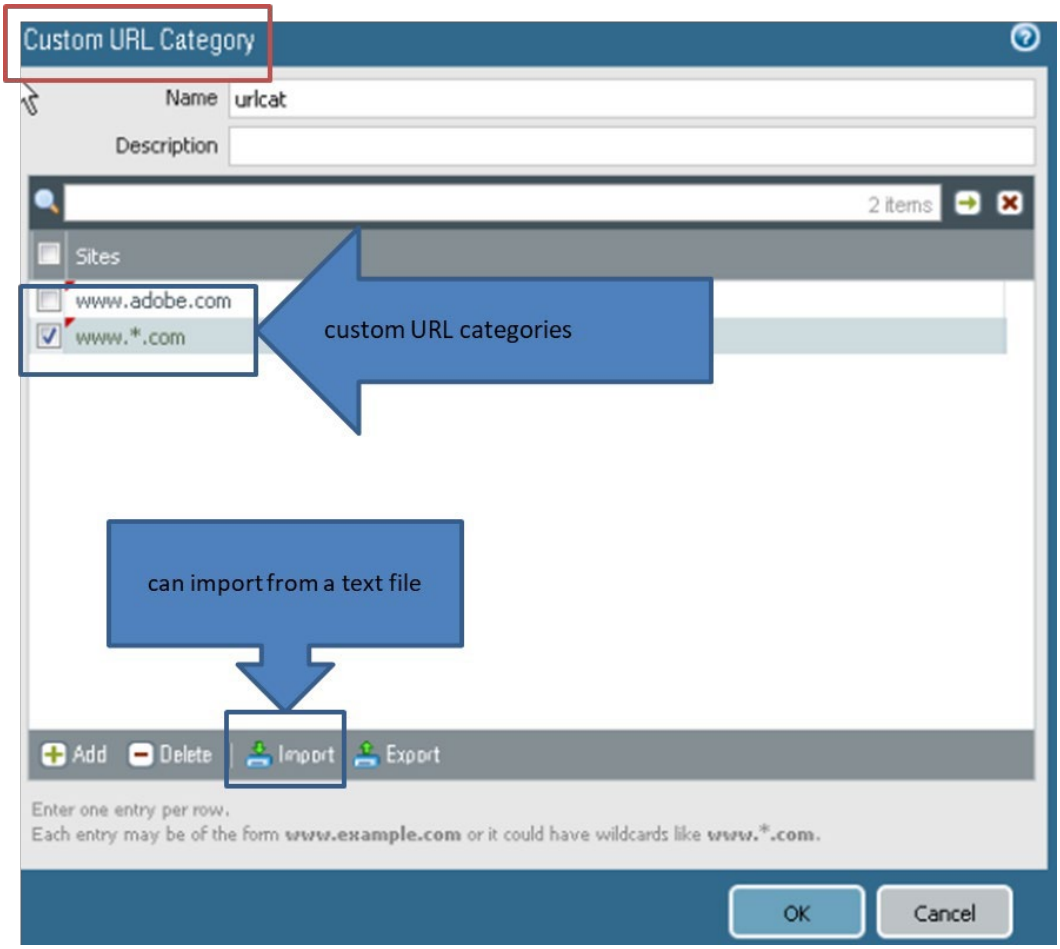
Use the **Custom URL Category** page to create your custom list of URLs and use it in a URL Filtering profile or as a match criterion in policy rules. In a custom URL category, you can add URL entries individually or import a text file that contains a list of URLs. URL entries added to custom categories are case-insensitive.

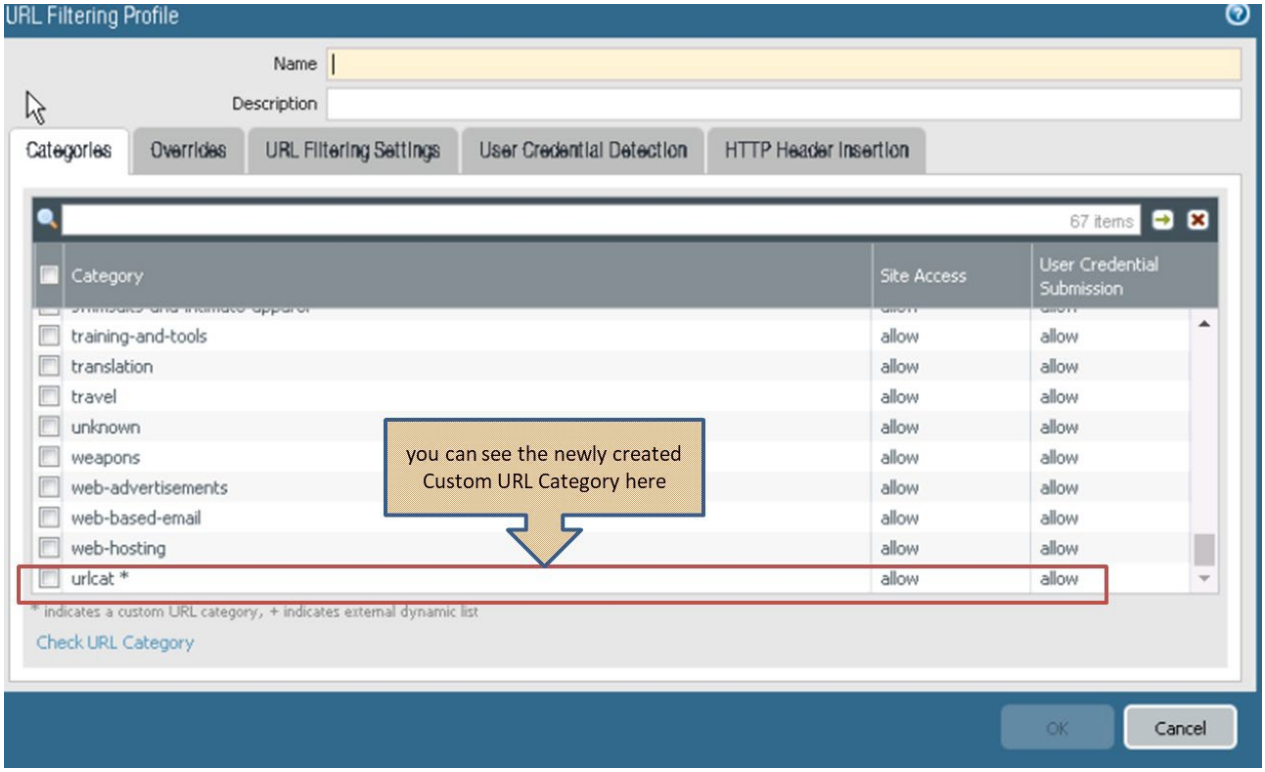
Custom URL category settings are as follows:

- **Name:** Enter a name to identify the custom URL category (up to 31 characters in length). This name displays in the category list when URL Filtering profiles are defined and in the match criteria for URL categories in policy rules. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
- **Description:** Enter a description for the URL category (up to 255 characters in length).
- **Shared:** Select this option if you want the URL category to be available to:
    - **Every virtual system (vsys) on a multi-vsys firewall**. If you clear this selection, the URL category will be available only to the virtual system selected in the **Objects** tab.
    - **Every device group on Panorama**. If you clear this selection, the URL category will be available only to the device group selected in the **Objects** tab.
- **Sites:**
    - Click **Add** to enter URLs, only one in each row. Each URL can be in the format

"www.example.com" or can include wildcards ("*.example.com").

- Click **Import** and browse to select the text file that contains the list of URLs. Enter only one URL per row. Each URL can be in the format "www.example.com" or can include wildcards ("*.example.com").
- Click **Export** to export the custom URL entries included in the list. The URLs are exported as a text file.
- Select an entry and click **Delete** to remove the URL from the list. Before you can delete a custom category that you have used in a URL Filtering profile, you must set the action to **None**. Go to **Category** actions in **Objects > Security Profiles > URL Filtering**.





Sample question

89. Which two valid URLs can be used in a custom URL category? (Choose two.)
    A. ww.youtube.**
    B. www.**.com
    C. www.youtube.com
    D. *.youtube.com

Exam Domain 5 – Identifying Users

5.1 Given a scenario, identify an appropriate method to map IP addresses to usernames.

Today's working environment is extremely dynamic. Users no longer are restricted to using just one device, a computer, on the network. A user may be using a smartphone, tablet, desktop, and a laptop. Each device is given an IP address dynamically by a DHCP server, which makes tracking the user difficult and almost impossible to control. Use of a username is easier than use of an IP address to control and log a user's activity. The process of mapping a username to an IP address is the function of User-ID.

A user's IP address constantly is changing because so many devices are used by users, and laptops provide so much mobility. Capture of that information often is difficult. The firewall needs to be able to monitor multiple sources simultaneously.

For instance, a user's cellphone usually is not in the corporate domain and doesn't require the user to log in to the domain. However, users often will have their corporate email on the phone. When the phone

checks for new email and authenticates with the Exchange server, the system can capture the IP address from the logs.

The user could be using an iPad or Linux workstation that also is not on the domain. The firewall has a service called Captive Portal that can be used to force the user to authenticate to use the internet. The firewall then has the user's name and IP address.

The firewall also has other ways to capture user information. The firewall can use server monitoring to monitor the security logs on a Windows server for successful authentication events. Syslog monitoring of login events can be used with LDAP and Linux, among others.

The different methods of user mapping are:

- Server Monitoring: A Windows-based User-ID agent, or the built-in PAN-OS integrated User-ID agent inside the PAN-OS firewall, monitors Security Event logs for successful login and logout events on Microsoft domain controllers, Exchange Servers, or Novell eDirectory servers.
- Port mapping: For Microsoft Terminal Services or Citrix environments, users might share the same IP address. To overcome this issue, the Palo Alto Networks Terminal Services agent must be installed on the Windows or Citrix terminal server. The Terminal Services Agent uses the source port of each client connection to map each user to a session. Linux terminal servers do not support the Terminal Services agent, and must use XML API to send user mapping information from login or logout events to User-ID.
- Syslog: The Windows-based User-ID agent and the PAN-OS integrated User-ID agent use Syslog Parse Profiles to interpret login and logout event messages that are sent to syslog servers from devices that authenticate users. Such devices include wireless controllers, 802.1*x* devices, Apple Open Directory servers, proxy servers, and other network access control (NAC) devices.
- XFF headers: If a proxy server exists between users and a firewall, the firewall might see the source IP address of the proxy server instead of the original source IP address of the host that originated the traffic. Most proxy servers have a feature that allows forwarding of the original source IP address of the host to the firewall within an XFF header. Use of the original client source IP address enables the firewall to map the IP address to a username.
- Authentication Policy and Captive Portal: There are some cases where the User-ID agent can't map an IP address to username using any of the methods previously described. In these cases, you can use an Authentication Policy and Captive Portal, whereby any web traffic (HTTP or HTTPS) that matches an Authentication policy rule forces the user to authenticate via one of the following three Captive Portal authentication methods:
    - Browser Challenge: Uses Kerberos or NT LAN Manager (NTLM)
    - Web Form: Uses multi-factor authentication, SAML single sign-on, Kerberos, TACACS+, RADIUS, LDAP, or local authentications
    - Client certificate authentication
- GlobalProtect: Mobile users have an application running on their endpoint for which they must enter login credentials for VPN access to the firewall. The login information is used for User-ID

mapping. GlobalProtect is the most recommended method to map device IP addresses to usernames.

- XML API: The PAN-OS XML API is used in cases where standard user mapping methods might not work, such as third-party VPNs or 802.1*x*-enabled wireless networks.
- Client Probing: Used in a Microsoft Windows environment where the User-ID agent probes client systems using Windows Management Instrumentation (WMI) and/or NetBIOS. Client probing is not a recommended method for user mapping.

For more information about the methods used to collect User-ID information, see the following information:

- "User-ID" module in the EDU-110 and EDU-210 training, *Firewall Essentials: Configuration and Management*
- User-ID in the *PAN-OS Administrator's Guide*: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html

Exam Domain 5 – Identifying Users

5.2 Given a scenario, identify the appropriate User-ID agent to deploy.

User-ID has two agents that can be used to monitor the servers and gather the User-ID information. One is the built-in agent, called the integrated agent, inside the PAN-OS firewall. The other agent is a Windows-based client that for 8.0 and later can be installed on any Windows server 2008 or higher system. Both agents have the same functionality. Several factors can determine which agent to use.

An organization might choose to use the Windows agent if it has more than 100 domain controllers because neither type of agent can monitor more than 100 domain controllers or 50 syslog servers. Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

However, if network bandwidth is an issue, you might want to use the PAN-OS integrated agent because it communicates directly with the servers, whereas the Windows agent communicates with the servers and then communicates the User-ID information to the firewall so that it can update the firewall database.

For more information about the different agents and how they are used, see the following information:

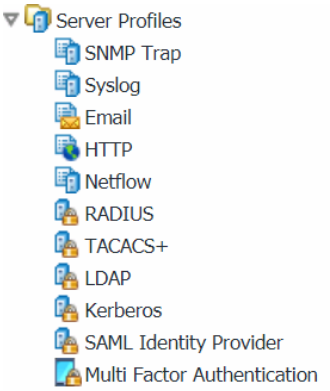
- "User-ID" module in the EDU-110 and EDU-210 training, *Firewall Essentials: Configuration and Management*
- User-ID in the *PAN-OS Administrator's Guide*: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html

Exam Domain 5 – Identifying Users

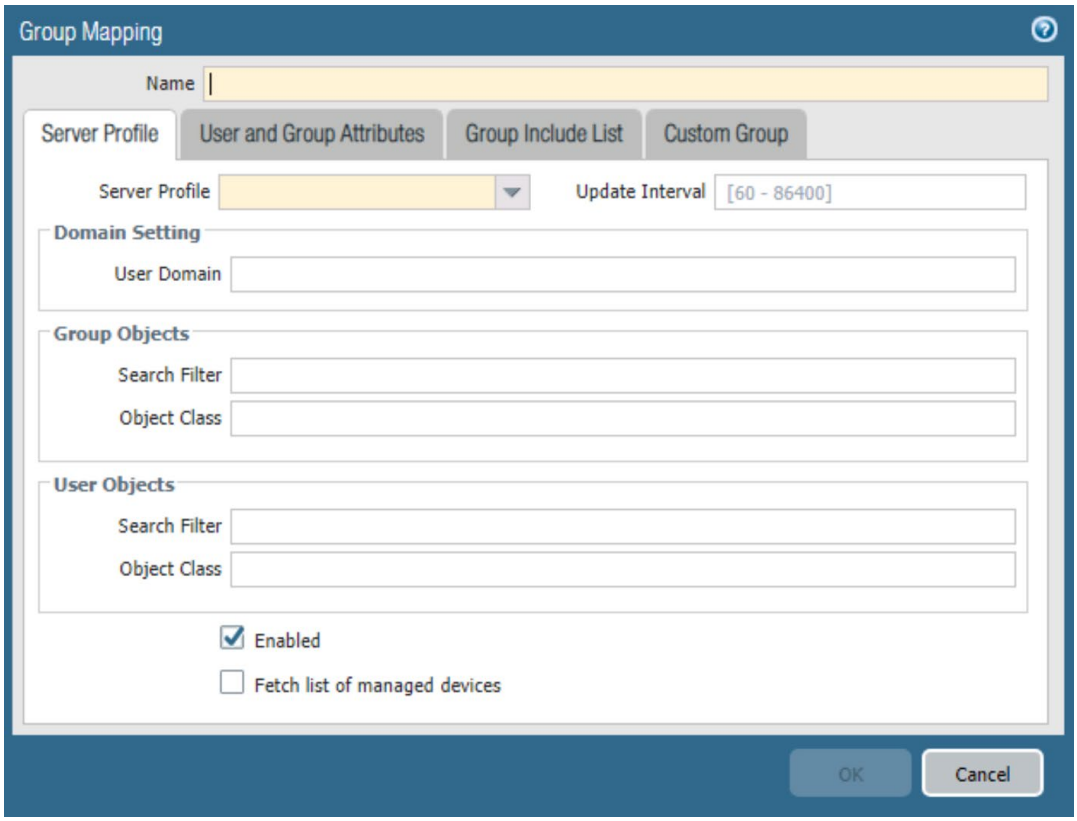
5.3 Identify how the firewall maps usernames to user groups.

Several options must be configured before User-ID can function. The LDAP Server Profile is the most important item to configure. The LDAP Server Profile is used to connect the firewall to an LDAP server and retrieve a list of usernames and groups.

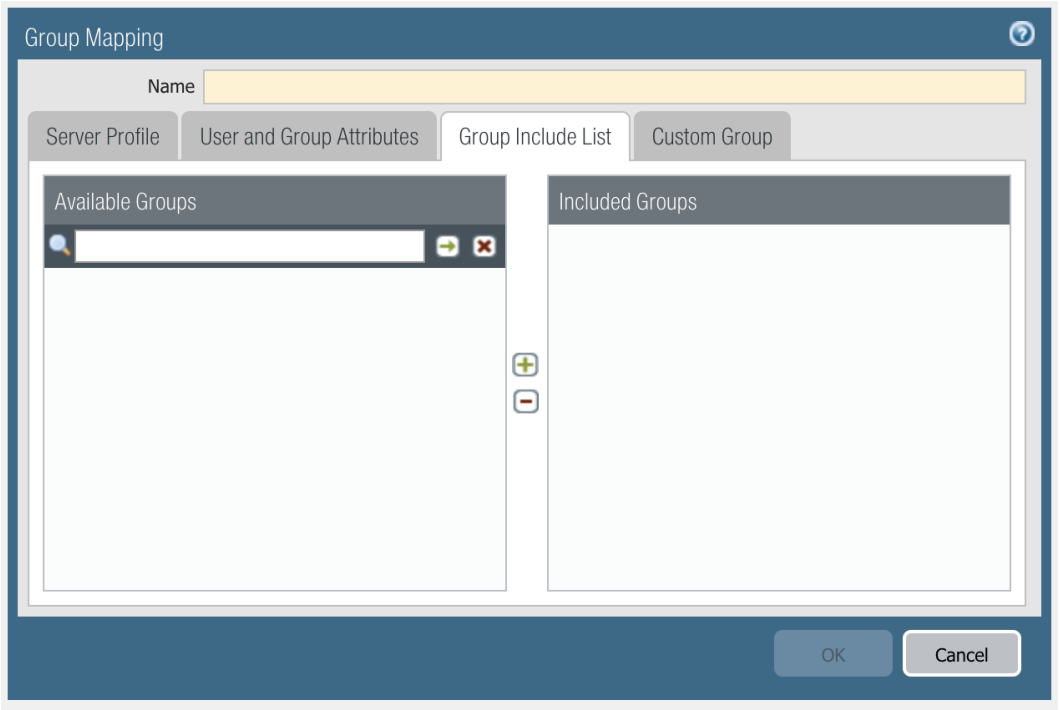
The LDAP Server Profile will require different information, depending on what is used.



After the LDAP Server Profile is configured, the group mapping needs to be configured:



The administrator should select the LDAP Server Profile they configured earlier and complete the domain settings. The **Group Include List** tab will show the available groups in the domain. The administrator can choose which group to monitor and which ones to ignore:



To learn more about the methods to map users and groups to collect User-ID information, see the following information:

- "User-ID" module in the EDU-110 and EDU-210 training, Firewall Essentials: Configuration and Management
- User-ID in the *PAN-OS Administrator's Guide*: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html

Exam Domain 5 – Identifying Users

5.4 Given a graphic, identify User-ID configuration options.

User-ID uses multiple technologies to map IP addresses to usernames. The method used depends on the operating system, applications used in the organization, and the network infrastructure used within the company.

For instance, if the company is using an Aruba system, the XML API can be used to retrieve the information from the Aruba system.

If the company is using Citrix or Microsoft terminal servers to deliver desktops to end users, then the Terminal Services agent is used to retrieve the User-ID information. The Terminal Services agent needs to be installed on the actual Citrix or Microsoft terminal server.

The firewall can use client probing to gather information from Windows clients. The User-ID agent will send requests to the Windows client to identify the user that is logged in to the system.

For more information about the different agents and how they are used, see the following:

- "User-ID" module in the EDU-110 and EDU-210 training, *Firewall Essentials: Configuration and Management*
- User-ID in the *PAN-OS Administrator's Guide*: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html

Sample questions

90. What are three methods of mapping usernames to IP addresses? (Choose three.)
    A. Server Monitoring
    B. Traps
    C. MineMeld
    D. syslog
    E. AutoFocus
    F. port mapping
91. Which type of Server Profile is used to create group mappings?
    A. RADIUS
    B. TACACS+
    C. Kerberos
    D. LDAP
92. The Server Monitoring user mapping method can monitor which three types of servers? (Choose three.)
    A. RADIUS
    B. Microsoft Domain Controllers
    C. Exchange Servers
    D. Novell eDirectory Servers
93. The Port Mapping user mapping method can monitor which two types of environments? (Choose two.)
    A. Citrix
    B. Microsoft terminal servers
    C. Exchange Servers
    D. Linux servers
94. The Windows User-ID Agent can be installed on which two operating systems? (Choose two.)
    A. Linux
    B. Server 2016
    C. XP
    D. Server 2008

Exam Domain 6 – Deployment Optimization

6.1 Identify the benefits and differences between the Heatmap and the BPA reports.

The Palo Alto Networks Customer Success team is focused on ensuring that customers use their products as effectively as possible. The free Best Practice Assessment (BPA) tool for Palo Alto Networks firewalls and Panorama evaluates a device's configuration by measuring the adoption rate of a firewall's capabilities, and by validating whether the policies adhere to best practices. The BPA tool provides recommendations and instructions about how to remediate failed best practice checks. The ultimate goal for running the BPA is to reduce your attack surface. The BPA tool should be run on a scheduled basis (for example, quarterly) to ensure continuous improvement.

The two components to the BPA tool are the Security Policy Adoption Heatmap component and the BPA assessment component. The Heatmap analyzes a Palo Alto Networks deployment, measuring the adoption rate of features and capabilities across a targeted network infrastructure. The Heatmap can filter the information by device groups, serial numbers, zones, areas of architecture, and other categories. The results chart the progress of security improvement toward a Zero Trust network.

The BPA compares a firewall or Panorama configuration against best practices and provides recommendations to strengthen your security posture by fully adopting Palo Alto Networks prevention capabilities. More than 200 security checks are performed on the firewall or Panorama configuration. A pass/fail score is provided for each check. If a check returns a failing score, the tool provides a justification for the failing score and recommendations about how to resolve the issue.

Both components require the Tech Support File from either Panorama or a firewall to be uploaded to the Palo Alto Networks Customer Support Portal. After the Tech Support File is imported, the user performs architecture mapping, which maps your existing zone names to predefined architecture classifications. Examples of architecture classifications are Enterprise – Perimeter – Internet, Internal – Core – Users, Mobility – Remote Users/VPN.

Heatmap Component

The Heatmap measures the adoption rate of the following features. The results display the adoption rate based on source zone to destination zone. Column filters are available to drill down to specific device groups, source zones, and destination zones.

The Heatmap measures the adoption rate of the following Palo Alto Networks firewall features:

- WildFire
- Threat Prevention (IPS)
    - Anti-Spyware
    - DNS Sinkhole
    - Antivirus
    - Vulnerability Protection
- URL Filtering
- File Blocking

- Data Filtering
- User-ID
- App-ID
- Service/Port
- Logging

paloalto NETWORKS | Trending | Serial Number & Vsys | **Zones** | Zone Type | Area of Architecture | Tags | Rule Detail | Go to Best Practice Assessment

Security Policy Capability Adoption Heatmaps

Documentation / Help

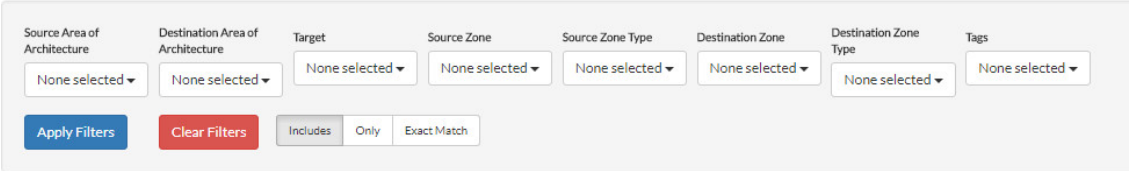
Column Filters

					WildFire	Threat Prevention (IPS)				URL-Filtering						
Source Zone	Destination Zone	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
Lokalnettet_L3, VPN	untrust_vr1	27	26	1	100.0	100.0	92.3	100.0	100.0	100.0	100.0	0.0	92.6	96.3	92.3	100.0
Lokalnettet_L3	untrust_vr1	18	16	2	100.0	100.0	56.3	93.8	100.0	93.8	100.0	0.0	38.9	55.6	100.0	100.0
Lokalnettet_L3, Trust_DC, VPN	untrust_vr1	6	6	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
any	untrust_vr1	5	0	5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	60.0	0.0	100.0
Kjeller, Kontor, Stue	Kjeller, Kontor, Stue	3	3	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	33.3	100.0
Clientless_VPN, Lokalnettet_L3, VPN	untrust_vr1	3	3	0	100.0	100.0	66.7	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
Clientless_VPN, Lokalnettet_L3, Trust_DC, VPN	untrust_vr1	2	2	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	50.0	100.0	100.0
Lokalnettet_L3, VPN, untrust_vr1	GP_Clientless_Portal, Management, untrust_vr1	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
untrust_GP	untrust_GP	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
untrust_GP, untrust_vr1	untrust_GP, untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
untrust_vr1	untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Garasje, Kjeller, Kontor, Stue	Garasje, Kjeller, Kontor, Stue	1	1	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0
Grand Total:		77	65	12	98.5	98.5	75.4	96.9	98.5	96.9	98.5	0.0	59.7	74.0	87.7	100.0

Some items cannot realistically be expected to reach 100%, such as DNS Sinkhole. DNS Sinkhole should be considered only for traffic that includes DNS queries. Another example is URL filtering, which typically is implemented only on the perimeter. Also, you should enable threat prevention only on rules that allow traffic; there is no point in enabling threat prevention on ”drop” or ”deny” rules. You should focus on yellow, orange, and red highlights, which indicate gaps in security.

Zone Mapping enables you to determine which traffic you want to analyze by selecting source zone and destination zone pairs, and source areas of architecture and destination areas of architecture. After you do the zone mapping, you can import it into the Customer Success tool to create a new Heatmap.

Zone Mapping Feature Section



Example Zone Mapping Report

Source Area of Architecture	Destination Area of Architecture	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire	Threat Prevention (IPS)					URL-Filtering						
					WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
Remote Users / VPN	Remote Users / VPN	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
Remote Users / VPN	Perimeter Internet	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0
Perimeter Internet, Remote Users / VPN	Perimeter Internet, Remote Users / VPN	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Perimeter Internet	Perimeter Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Perimeter Internet	3rd party / Vendors, Cloud, Data Center East West, Data Center North South, Guest / BYOD, Internal Core, Out-of-band Management, Perimeter Internet, Remote Office, Remote Users / VPN	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Out-of-band Management	Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0
Internal Core, Remote Users / VPN	Perimeter Internet	30	29	1	100.0	100.0	89.7	100.0	100.0	100.0	100.0	0.0	93.3	94.7	93.1	100.0
Internal Core, Remote Users / VPN	Internal Core	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
Internal Core, Perimeter Internet, Remote Users / VPN	Out-of-band Management, Perimeter Internet, Remote Users / VPN	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
Internal Core	Perimeter Internet	18	16	2	100.0	100.0	54.3	93.8	100.0	93.8	100.0	0.0	38.9	55.6	100.0	100.0
Data Center East West, Internal Core, Remote Users / VPN	Perimeter Internet	8	8	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	87.5	100.0	100.0
Data Center East West, Internal Core, Remote Users / VPN	Data Center East West, Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
Data Center East West, Internal Core, Out-of-band Management, Remote Users / VPN	Perimeter Internet	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
Data Center East West, Internal Core	Perimeter Internet	1	1	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0
Grand Total		**77**	**65**	**12**	**98.5**	**98.5**	**75.4**	**94.9**	**98.5**	**96.9**	**98.5**	**0.0**	**59.7**	**74.0**	**87.7**	**100.0**

The figure highlights the output of source architectures and destination architectures in the earlier Heatmap report after zone mapping has been performed. Examples of architectures are Internal, External, Internal Core, Data Center East, and Data Center West.

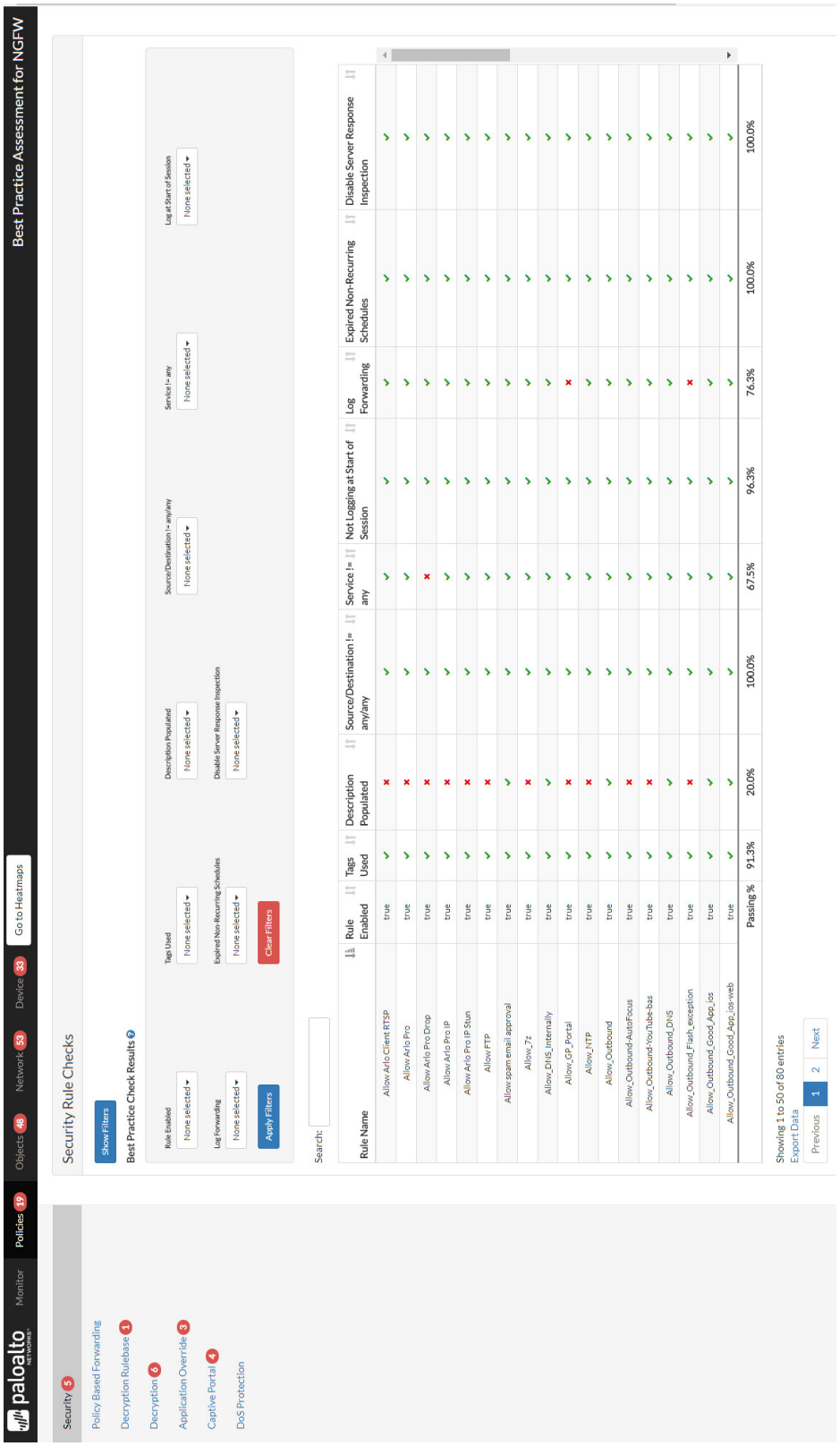
Best Practice Assessment Tool

The BPA tool enables you to create a firewall configuration that meets security best practices.

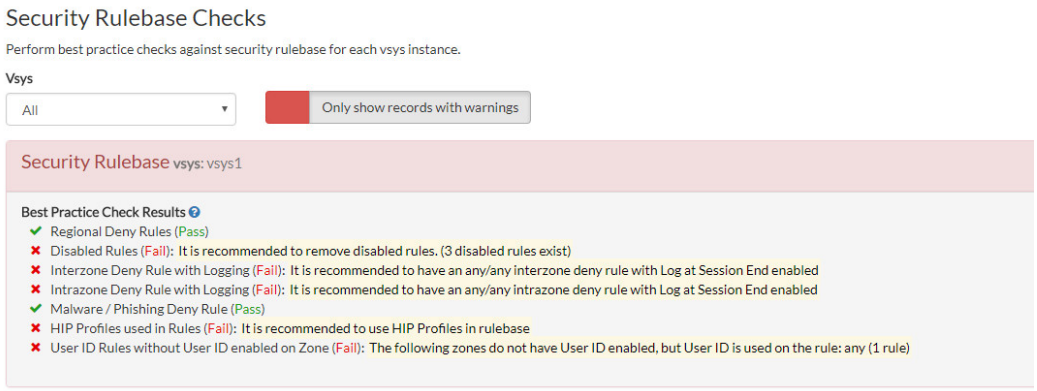
The seven primary categories of the Best Practice Assessment tool are as follows:

- Security
- Policy Based Forwarding
- Decryption Rulebase
- Decryption
- Application Override
- Captive Portal
- DoS Protection

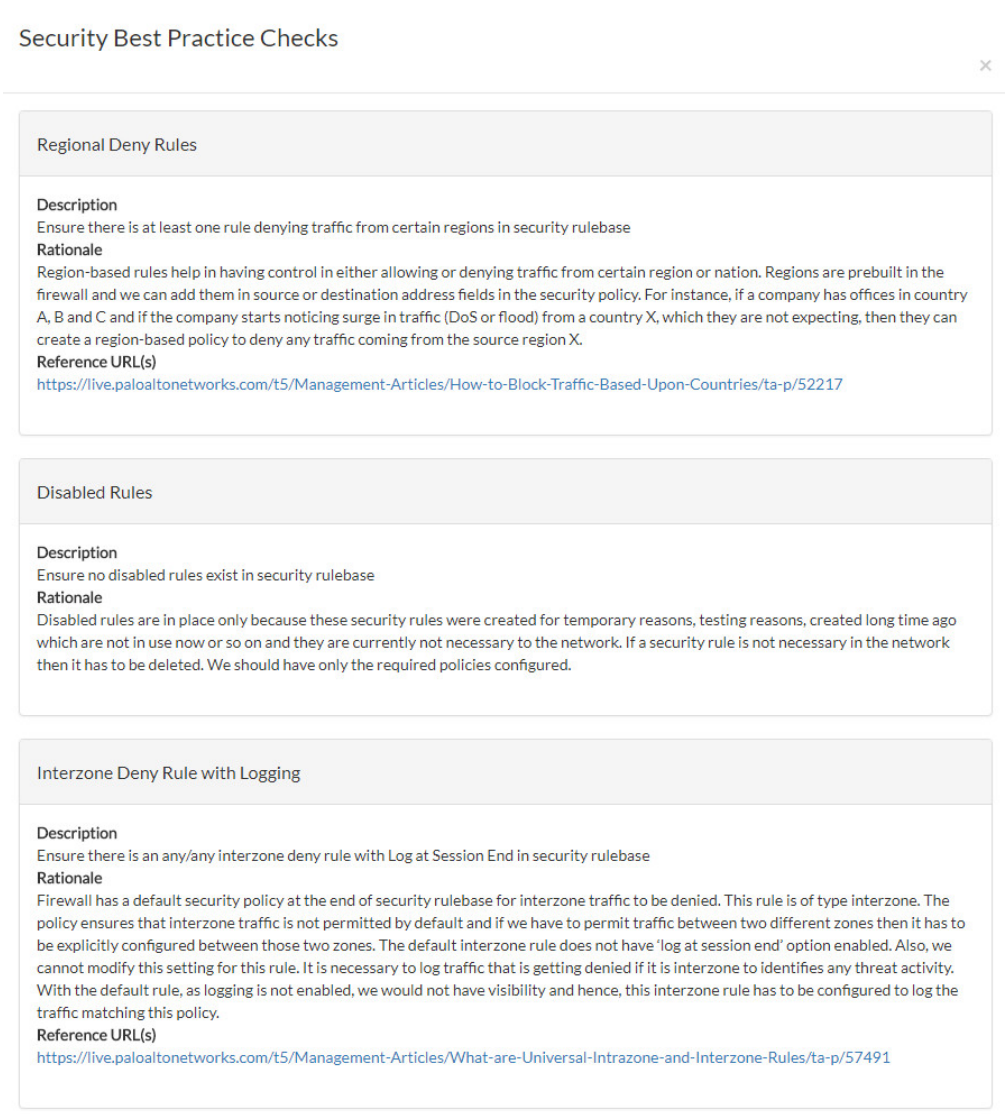
Example Best Practice Assessment Report



Example of Best Practices for Security Rulebase Checks



Example of Best Practices for Security Best Practice Checks



Sample questions

95. A Heatmap provides an adoption rate for which three features? (Choose three.)
    A. WildFire
    B. Traps
    C. File Blocking
    D. User-ID
    E. SSL certificates
    F. Authentication Profiles

96. What are three Best Practice Assessment tool primary categories? (Choose three.)
    A. User-ID
    B. Logging
    C. Vulnerability Protection
    D. Security
    E. Decryption
    F. DoS Protection

97. Which two security features normally do not achieve an adoption rate of 100%? (Choose two.)
    A. URL Filtering
    B. App-ID
    C. Logging
    D. DNS Sinkhole

98. Which type of file is used to generate the Heatmap report and the BPA report?
    A. Technical Support
    B. Configuration
    C. Statistics
    D. XML

99. What are two components of the BPA tool? (Choose two.)
    A. Security Policy Adoption Heatmap
    B. BPA
    C. XML
    D. Security Policy

Answers to the Sample Questions

Correct answers are indicated in **bold**.

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.1 Identify the components of the Palo Alto Networks Security Operating Platform.

1. The Palo Alto Networks Security Operating Platform is designed for which three purposes? (Choose three.)
   A. **consume innovations quickly**
   B. ensure compliance
   C. **focus on what matters**
   D. **prevent successful cyberattacks**
2. Which item is not one of the six primary components of the Palo Alto Networks Security Operating Platform?
   A. applications (Palo Alto Networks applications, third-party applications, customer applications)
   B. Cloud-Delivered Security Services
   C. **WildFire**
   D. Cortex and Cortex Data Lake
   E. Network Security
   F. Advanced Endpoint Protection
   G. Cloud Security
3. Which cloud-delivered security service provides instant access to community-based threat data?
   A. Prisma SaaS
   B. **AutoFocus**
   C. Threat 42
   D. Cortex XDR
4. Which cloud-delivered security services provides security for branches and mobile users?
   A. MineMeld
   B. Cortex XDR
   C. AutoFocus
   D. **Prisma Access**
5. Which Palo Alto Networks Security Operating Platform component provides access to applications from Palo Alto Networks, third parties, and customers?
   A. Cloud-Delivered Security Services
   B. WildFire
   C. **Cortex**
   D. Network Security

E. Advanced Endpoint Protection

6. Which Palo Alto Networks firewall feature provides all the following abilities?

- Stops malware, exploits, and ransomware before they can compromise endpoints
- Provides protection while endpoints are online and offline, on network and off
- Coordinates enforcement with network and cloud security to prevent successful attacks
- Detects threats and automates containment to minimize impact
- Includes WildFire cloud-based threat analysis service with your Cortex XDR subscription
- Integrates with the Palo Alto Networks Security Operating Platform

A. **Cortex XDR**
B. Prisma SaaS
C. URL Filtering
D. WildFire
E. GlobalProtect
F. AutoFocus

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.2 Identify the components and operation of single-pass parallel processing architecture.

7. Which management features does the Control Plane provide? (Choose three.)

A. security processing
B. **logging**
C. **reporting**
D. **firewall configuration**
E. signature matching
F. network processing

8. Which three data processing features does the data plane provide? (Choose three.)

A. **network processing**
B. **security processing**
C. **signature matching**
D. firewall configuration
E. logging
F. reporting

9. What are three components of the Network Processing module? (Choose three.)

A. **QoS**
B. **NAT**
C. App-ID
D. **flow control**
E. URL match

F. spyware

10. Which approach most accurately defines the Palo Alto Networks SP3 architecture?

A. prioritize first
B. sequential processing
C. **scan it all, scan it once**
D. zero trust segmentation platform

11. What is the result of using a stream-based design of architecture?

A. **superior performance**
B. increased latency
C. superior latency
D. increased functionality

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.3 Given a network design scenario, apply the Zero Trust security model and describe how it relates to traffic moving through your network.

12. Which security model does Palo Alto Networks recommend that you deploy?

A. separation-of-trust
B. **zero trust**
C. trust-then-verify
D. never trust

13. The Zero Trust model is implemented to specifically inspect which type of traffic?

A. **east-west**
B. north-south
C. left-right
D. up-down

14. What are the three main concepts of Zero Trust? (Choose three.)

A. **All resources are accessed in a secure manner, regardless of location.**
B. **Access control is on a "need-to-know" basis and is strictly enforced.**
C. Credentials need to be verified.
D. **All traffic is logged and inspected.**
E. Internal users are trusted implicitly.
F. External users are trusted explicitly.

15. Which two statements are true about the Zero Trust model? (Choose two.)

A. **Traffic is inspected laterally.**
B. **Traffic is inspected east-west.**
C. Internal traffic is implicitly trusted.
D. External traffic is implicitly trusted.

16. Which three Palo Alto Networks products secure your network? (Choose three.)

A. MineMerge
B. **Prisma SaaS**
C. **URL filtering**
D. Containers
E. TrapContent
F. **WildFire**

Exam Domain 1 – Palo Alto Networks Security Operating Platform Core Requirements

1.4 Identify stages in the Cyber-Attack Lifecycle and firewall mitigations that can prevent attacks.

17. True or false: Blocking just one stage in the Cyber-Attack Lifecycle is all that is neededto protect a company's network from attack.
    A. **true**
    B. false
18. What are two stages of the Cyber-Attack Lifecycle? (Choose two.)
    A. **weaponization and delivery**
    B. manipulation
    C. extraction
    D. **command and control**
19. Command and control be prevented through which two methods? (Choose two.)
    A. exploitation
    B. **DNS Sinkholing**
    C. **URL filtering**
    D. reconnaissance
20. Exploitation can be mitigated by which two actions? (Choose two.)
    A. **keeping systems patched**
    B. using local accounts
    C. **blocking known and unknown vulnerability exploits on the endpoint**
    D. providing admin credentials

Exam Domain 2 – Simply Passing Traffic

2.1 Identify and configure firewall management interfaces.

21. What are two firewall management methods? (Choose two.)

A. **CLI**
B. RDP
C. VPN
D. **XML API**

22. Which two devices are used to connect a computer to the firewall for management purposes? (Choose two.)
    A. rollover cable
    B. **serial cable**
    C. **RJ-45 Ethernet cable**
    D. USB cable
23. What is the default IP address on the MGT interfaces of a Palo Alto Networks firewall?
    A. 192.168.1.1
    B. 192.168.1.254
    C. 10.0.0.1
    D. 10.0.0.254
24. What are the two default services that are available on the MGT interface? (Choose two.)
    A. **HTTPS**
    B. **SSH**
    C. HTTP
    D. Telnet
25. True or false. Service route traffic has Security policy rules applied against it.
    A. **true**
    B. false
26. Service routes may be used to forward which two traffic types out a data port? Choose two.)
    A. **External Dynamic Lists**
    B. MineMeld
    C. Skype
    D. **Palo Alto Networks updates**

Exam Domain 2 – Simply Passing Traffic

2.2 Identify how to manage firewall configurations.

27. Which firewall plane does the running-configuration reside on?
    A. management
    B. control
    C. **data**
    D. security
28. Which firewall plane does the candidate configuration reside on?
    A. management

B. control

C. data

D. security

29. Candidate config and running config files are saved as which file type?

A. TXT

B. HTML

C. **XML**

D. RAR

30. Which command must be performed on the firewall to activate any changes?

A. commit

B. save

C. load

D. save named

E. import

F. copy

31. Which command backs up configuration files to a remote network device?

A. import

B. load

C. copy

D. **export**

32. The command **`load named configuration snapshot`** overwrites the current candidate configuration with which three items? (Choose three.)

A. **custom-named candidate configuration snapshot (instead of the default snapshot)**

B. **custom-named running configuration that you imported**

C. snapshot.xml

D. **current running configuration (running-config.xml)**

E. **Palo Alto Networks updates**

Exam Domain 2 – Simply Passing Traffic

2.3 Identify and schedule dynamic updates.

33. What is the shortest time interval that you can configure a Palo Alto Networks firewall to download WildFire updates?

A. **1 minute**

B. 5 minutes

C. 15 minutes

D. 60 minutes

34. What is the publishing interval for WildFire updates, with a valid WildFire license?

A. 1 minute

B. **5 minutes**

C. 15 minutes

D. 60 minutes

35. True or false. A Palo Alto Networks firewall automatically provides a backup of the configuration during a software upgrade.

    A. **true**
    B. false

36. If you have a Threat Prevention subscription but *not* a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

    A. 1 to 2 hours
    B. 2 to 4 hours
    C. 10 to 12 hours
    D. **12 to 48 hours**

37. Which three actions should you complete before you upgrade to a newer version of software? (Choose three.)

    A. **Review the release notes to determine any impact of upgrading to a newer version of software.**
    B. **Ensure the firewall is connected to a reliable power source.**
    C. Export the device state.
    D. **Create and externally store a backup before you upgrade.**

38. What are five ways to download software? (Choose five.)

    A. **over the MGT interface on the control plane**
    B. **over a data interface on the data plane**
    C. **upload from a computer**
    D. **from the Palo Alto Networks Customer Support Portal**
    E. from the PAN-DB database
    F. **from Panorama**

Exam Domain 2 – Simply Passing Traffic

2.4 Configure internal and external services for account administration.

39. Which two statements are true about a Role Based Admin Role profile role? (Choose two.)

    A. It is a built-in role.
    B. **It can be used for CLI commands.**
    C. **It can be used for XML API.**
    D. Superuser is an example.

40. PAN-OS software supports which two authentication types? (Choose two.)

    A. **RADIUS**
    B. SMB
    C. **TACACS+**
    E. AWS

41. Which two Dynamic Admin Role types are available on the PAN-OS software? (Choose two.)
    A. **superuser**
    B. superuser (write only)
    C. device user
    D. **device administrator (read-only)**
42. Which type of profile does an Authentication Sequence include?
    A. Security
    B. Authorization
    C. Admin
    D. **Authentication**
43. An Authentication Profile includes which other type of profile?
    A. **Server**
    B. Admin
    C. Customized
    D. Built-in
44. True or False: Dynamic Admin Roles are called “dynamic” because you can customize them.
    A. true
    B. **false**
45. What is used to override global Minimum Password Complexity Requirements?
    A. Authentication Profile
    B. Local Profile
    C. Password Role
    D. **Password Profile**

Exam Domain 2 – Simply Passing Traffic

2.5 Given a network diagram, create the appropriate security zones.

46. Which two default zones are included with the PAN-OS software? (Choose two.)
    A. **Interzone**
    B. Extrazone
    C. **Intrazone**
    D. Extranet
47. Which two zone types are valid? (Choose two.)
    A. trusted
    B. **tap**
    C. **virtual wire**
    D. untrusted
    E. dmz
48. The External zone type is used to pass traffic between which type of objects?
    A. Layer 2 interfaces
    B. Layer 3 interfaces

C. virtual routers
D. **virtual systems**

49. Which two statements about interfaces are correct? (Choose two.)

A. Interfaces must be configured before you can create a zone.
B. **Interfaces do not have to be configured before you can create a zone.**
C. **An interface can belong to only one zone.**
D. An interface can belong to multiple zones.

50. Which three interface types can belong in a Layer 3 zone? (Choose three.)

A. **loopback**
B. **Layer 3**
C. **tunnel**
D. virtual wire

51. What are used to control traffic through zones?

A. access lists
B. security policy lists
C. **security policy rules**
D. access policy rules

Exam Domain 2 – Simply Passing Traffic

2.6 Identify and configure firewall interfaces.

52. Which two actions can be done with a Tap interface? (Choose two.)

A. encrypt traffic
B. **decrypt traffic**
C. allow or block traffic
D. **log traffic**

53. Which two actions can be done with a Virtual Wire interface? (Choose two.)

A. **NAT**
B. route
C. switch
D. **log traffic**

54. Which two actions can be done with a Layer 3 interface? (Choose two.)

A. **NAT**
B. **route**
C. switch
D. create a Virtual Wire object

55. Layer 3 interfaces support which two items? (Choose two.)

A. **NAT**
B. **IPv6**

C. switching

D. spanning tree

56. Layer 3 interfaces support which three advanced settings? (Choose three.)

A. IPv4 addressing

B. IPv6 addressing

C. NTP configuration

D. **NDP configuration**

E. **link speed configuration**

F. **link duplex configuration**

57. Layer 2 interfaces support which three items? (Choose three.)

A. spanning tree blocking

B. **traffic examination**

C. **forwarding of spanning tree BPDUs**

D. **traffic shaping via QoS**

E. firewall management

F. routing

58. Which two interface types support subinterfaces? (Choose two.)

A. **virtual wire**

B. **Layer 2**

C. loopback

D. tunnel

59. Which two statements are true regarding Layer 3 interfaces? (Choose two.)

A. **You can configure a Layer 3 interface with one or more as a DHCP client.**

B. You can assign only one IPv4 addresses to the same interface.

C. You can enable an interface to send IPv4 Router Advertisements by selecting the Enable Router Advertisement check box on the Router Advertisement tab.

D. **You can apply an interface management profile to the interface.**

Exam Domain 2 – Simply Passing Traffic

2.7 Given a scenario, identify steps to create and configure a virtual router.

60. What is the default administrative distance of a static route within the PAN-OS software?

A. 1

B. 5

C. **10**

D. 100

61. Which two dynamic routing protocols are available in the PAN-OS software? (Choose two.)

A. RIP1

B. **RIPv2**

C. **OSPFv3**

D. EIGRP

62. Which value is used to distinguish the preference of routing protocols?
    A. metric
    B. weight
    C. distance
    D. cost
    E. **administrative distance**
63. Which value is used to distinguish the best route within the same routing protocol?
    A. **metric**
    B. weight
    C. distance
    D. cost
    E. administrative distance
64. In path monitoring, what is used to monitor remote network devices?
    A. **ping**
    B. SSL
    C. HTTP
    D. HTTPS
    E. link state

Exam Domain 2 – Simply Passing Traffic

2.8 Identify the purpose of specific security rule types.

65. What are the two default (predefined) security policy rule types in PAN-OS software? (Choose two.)
    A. Universal
    B. **Interzone**
    C. **Intrazone**
    D. Extrazone
66. True or false. Because the first rule that matches the traffic is applied, the more specific rules must follow the more general ones.
    A. true
    B. **false**
67. Which statement is true?
    A. For Intrazone traffic, traffic logging is enabled by default.
    B. For Interzone traffic, traffic logging is enabled by default.
    C. **For Universal traffic, traffic logging is enabled by default.**
    D. For any rule type, traffic logging is enabled by default.

Exam Domain 2 – Simply Passing Traffic

2.9 Identify and configure security policy match conditions, actions, and logging options.

68. What are the two default (predefined) security policy rule types in PAN-OS software? (Choose two.)
    A. Universal
    B. **Interzone**
    C. **Intrazone**
    D. Extrazone

69. True or false? Best practice is to enable logging for the two predefined security policy rules.
    A. **true**
    B. false

70. What will be the result of one or more occurrences of shadowing?
    A. a failed commit
    B. an invalid configuration
    C. **a warning**
    D. an alarm window

71. Which type of security policy rules most often exist above the two predefined security policies?
    A. intrazone
    B. interzone
    C. **universal**
    D. global

Exam Domain 2 – Simply Passing Traffic

2.10 Given a scenario, identify and implement the proper NAT solution

72. What are two source NAT types? (Choose two.)
    A. universal
    B. **static**
    C. **dynamic**
    D. extrazone

73. A simple way to remember how to configure security policy rules where NAT was implemented is to memorize the following: (Choose one.)
    A. post-NAT zone, post-NAT zone
    B. post-NAT IP, post-NAT zone
    C. **pre-NAT IP, post-NAT zone**
    D. pre-NAT IP, pre-NAT zone

74. What are two types of destination NAT? (Choose two.)

A. **dynamic IP (with session distribution)**
B. DIPP
C. global
D. **static**

75. What are two possible values for DIPP NAT oversubscription? (Choose two.)

A. **1x**
B. **4x**
C. 16x
D. 32x

76. Which statement is true regarding bidirectional NAT?

A. **For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.**
B. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction of the translation you configure.
C. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
D. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction of the translation you configure.

Exam Domain 3 – Traffic Visibility

3.1 Given a scenario, select the appropriate application-based security policy rules.

77. What are two application dependencies for icloud-mail? (Choose two.)

A. **ssl**
B. skype
C. google-base
D. **icloud-base**

Exam Domain 3 – Traffic Visibility

3.2 Given a scenario, configure application filters or application groups.

78. What does an application filter enable an administrator to do?

A. manually categorize multiple service filters
B. dynamically categorize multiple service filters
C. **dynamically categorize multiple applications**
D. manually categorize multiple applications

79. Which two items can be added to an application group? (Choose two.)

    A. application groups
    B. application services
    C. application filters
    D. admin accounts

Exam Domain 3 – Traffic Visibility

3.3 Identify the purpose of application characteristics as defined in the App-ID database.

80. What does the TCP Half Closed setting mean?

    A. maximum length of time that a session remains in the session table between receiving the first FIN and receiving the third FIN or RST.
    B. minimum length of time that a session remains in the session table between receiving the first FIN and receiving the second FIN or RST.
    C. maximum length of time that a session remains in the session table between receiving the first FIN and receiving the second FIN or RST.
    D. minimum length of time that a session remains in the session table between receiving the first FIN and receiving the third FIN or RST.

81. What are two application characteristics? (Choose two.)

    A. stateful
    B. excessive bandwidth use
    C. intensive
    D. evasive

Exam Domain 3 – Traffic Visibility

3.4 Identify the potential impact of App-ID updates to existing security policy rules.

82. Which column in the Applications and Threats screen includes the options **Review Apps** and **Review Policies**?

    A. Features
    B. Type
    C. Version
    D. **Action**

83. Which link can you select in the web interface to minimize the risk using of installing new App-ID updates?
    A. Enable new apps in content
    B. Disable new apps in app-id database
    C. **Disable new apps in content**
    D. Enable new apps in App-ID database

Exam Domain 4 – Securing Traffic

4.1 Given a risk scenario, identify and apply the appropriate security profile.

84. What are two benefits of Vulnerability Protection security profiles? (Choose two.)
    A. prevent compromised hosts from trying to communicate with external command-and-control (C2) servers
    B. protect against viruses, worms, and Trojans
    C. **prevent exploitation of system flaws**
    D. **prevent unauthorized access to systems**

Exam Domain 4 – Securing Traffic

4.2 Identify the difference between security policy actions and security profile actions.

85. Which two actions are available for Antivirus security profiles? (Choose two.)
    A. continue
    B. **allow**
    C. block IP
    D. **alert**

Exam Domain 4 – Securing Traffic

4.3 Given a network scenario, identify how to customize security profiles.

86. Which two HTTP Header Logging options are within a URL Filtering profile? (Choose two.)
    A. **User-Agent**
    B. Safe Search
    C. URL redirection
    D. **X-Forwarded-For**

Exam Domain 4 – Securing Traffic

4.4 Identify the firewall's protection against packet- and protocol- based attacks.

87. What are the two components of Denial-of-Service Protection? (Choose two.)

    A. **Zone Protection profile**
    B. **DoS Protection profile and policy rules**
    C. flood protection
    D. reconnaissance protection

Exam Domain 4 – Securing Traffic

4.6 Identify how the firewall can use the PAN-DB database to control traffic based on websites.

88. Which two types of attacks does the PAN-DB prevent? (Choose two.)

    A. **phishing sites**
    B. **HTTP based command-and-control**
    C. infected JavaScript
    D. flood attacks

Exam Domain 4 – Securing Traffic

4.7 Discuss how to control access to specific URLs using custom URL filtering categories.

89. Which two valid URLs can be used in a custom URL category? (Choose two.)

    A. ww.youtube.**
    B. www.**.com
    C. **www.youtube.com**
    D. ***.youtube.com**

Exam Domain 5 – Identifying Users

5.4 Given a graphic, identify User-ID configuration options.

90. What are three methods of mapping usernames to IP addresses? (Choose three.)

    A. **Server Monitoring**
    B. Traps
    C. MineMeld
    D. **syslog**
    E. AutoFocus

F. **port mapping**

91. Which type of Server Profile is used to create group mappings?

    A. RADIUS
    B. TACACS+
    C. Kerberos
    D. **LDAP**

92. The Server Monitoring user mapping method can monitor which three types of servers? (Choose three.)

    A. RADIUS
    B. **Microsoft Domain Controllers**
    C. **Exchange Servers**
    D. **Novell eDirectory Servers**

93. The Port Mapping user mapping method can monitor which two types of environments? (Choose two.)

    A. **Citrix**
    B. **Microsoft terminal servers**
    C. Exchange Servers
    D. Linux servers

94. The Windows User-ID Agent can be installed on which two operating systems? (Choose two.)

    A. Linux
    B. **Server 2016**
    C. XP
    D. **Server 2008**

Exam Domain 6 – Deployment Optimization

6.1 Identify the benefits and differences between the Heatmap and the BPA reports.

95. A Heatmap provides an adoption rate for which three features? (Choose three.)

    A. **WildFire**
    B. Traps
    C. **File Blocking**
    D. **User-ID**
    E. SSL certificates
    F. Authentication Profiles

96. What are three Best Practice Assessment tool primary categories? (Choose three.)
    A. User-ID
    B. Logging
    C. Vulnerability Protection
    D. **Security**
    E. **Decryption**
    F. **DoS Protection**

97. Which two security features normally do not achieve an adoption rate of 100%? (Choose two.)
    A. **URL Filtering**
    B. App-ID
    C. Logging
    D. **DNS Sinkhole**

98. Which type of file is used to generate the Heatmap report and the BPA report?
    A. **Technical Support**
    B. Configuration
    C. Statistics
    D. XML

99. What are two components of the BPA tool? (Choose two.)
    A. **Security Policy Adoption Heatmap**
    B. **BPA**
    C. XML
    D. Security policy