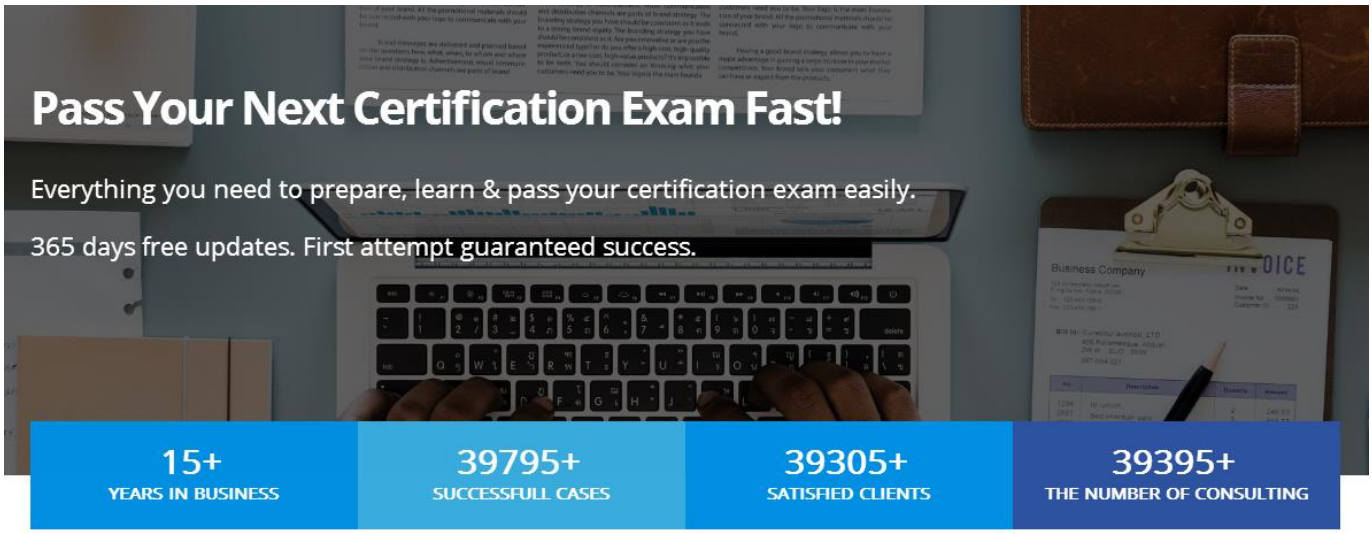
PracticeVCE



TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.practicevce.com

Professional Study Tool and Reliable Exam Practice Material

Exam : **SD-WAN-Engineer**

Title : Palo Alto Networks SD-WAN Engineer

Vendor : Palo Alto Networks

Version : DEMO

NO.1 A remote branch site is reporting intermittent connectivity to the Data Center. The administrator checks the System > Alarms page and sees a "VPN_DOWN" alarm for the tunnel to the DC. However, the internet circuit status is "Up".
Which specific log file or diagnostic tool in the Prisma SD-WAN portal would provide the IKE (Internet Key Exchange) error codes (e.g., "NO_PROPOSAL_CHOSEN" or "AUTH_FAILED") to pinpoint the cause of the tunnel failure?

A. Flow Browser

B. Event Logs > System

C. Site Summary > Topology

D. Link Quality Graphs

Answer: B

Explanation:
Comprehensive and Detailed Explanation
To diagnose specific VPN negotiation failures (Phase 1 or Phase 2 IPSec issues), the Event Logs (specifically filtered for System or VPN events) are the correct resource.
* Event Logs: This section records the control plane signaling messages. If a VPN tunnel fails to establish, the Event Log will generate an entry containing the specific IKE failure reason sent by the peer or generated locally. Common errors found here include INVALID_COOKIE, NO_PROPOSAL_CHOSEN (mismatch in encryption algorithms), or PRE_SHARED_KEY_MISMATCH.
* Flow Browser (A): This shows user traffic (TCP/UDP sessions). If the VPN is down, user traffic won't even enter the tunnel, so the Flow Browser will just show dropped flows or blackholes, but it won't explain why the tunnel itself is broken.
* Link Quality (D): This shows latency/loss graphs for established tunnels. It cannot diagnose why a tunnel failed to form in the first place.

NO.2 A network operator receives a critical SITE_CONNECTIVITY_DOWN alarm for a branch site in the Prisma SD-WAN portal.
What specific condition triggers this alarm type?

A. The device has lost power and rebooted.

B. One of the two internet circuits at the site has gone down.

C. All Secure Fabric Links (VPNs) to all remote peers are down, isolating the site from the overlay.

D. The site has exceeded its licensed bandwidth capacity.

Answer: C

Explanation:
Comprehensive and Detailed Explanation
The SITE_CONNECTIVITY_DOWN alarm is a high-severity alert indicating a total loss of overlay connectivity for a site.
* It does not trigger if just one circuit fails (Option B), provided that other circuits are still up and maintaining VPNs. A single link failure would typically trigger a "Link Down" or "VPN Down" alarm, but the Site connectivity would remain "Up" (degraded).
* It does not simply mean the device rebooted (Option A), although a reboot would cause it temporarily; the alarm specifically tracks the state of the VPN fabric.
The SITE_CONNECTIVITY_DOWN alarm specifically generates when all Secure Fabric Links (VPN tunnels) on the device are in the "Down" state. This means the branch is completely isolated from the rest of the SD-WAN network (Data Centers and other branches), even if the device itself might still be

powered on and reachable via the controller (management plane). It signifies a "Blackout" of the data plane for that location.

NO.3 Two branch sites, "Branch-A" and "Branch-B", are both behind active NAT devices (Source NAT) on their local internet circuits.
What requirement must be met for these two branches to successfully establish a direct Dynamic VPN (ION- to-ION) tunnel over the internet?

A. One of the sites must have a Static Public IP (1:1 NAT) to act as the initiator.

B. Both sites must disable NAT and use public IPs on the ION interface.

C. The ION devices automatically use STUN (Session Traversal Utilities for NAT) to discover their public IPs and negotiate the connection.

D. Dynamic VPNs are not supported if both sides are behind NAT.

Answer: C
Explanation:
Comprehensive and Detailed Explanation
Prisma SD-WAN supports Dynamic VPNs (Branch-to-Branch) even when both endpoints are behind Source NAT (e.g., typical broadband connections).
To achieve this, the ION devices utilize standard NAT Traversal techniques, specifically leveraging STUN (Session Traversal Utilities for NAT).
* Discovery: Each ION communicates with the Cloud Controller (which acts as a STUN server/signaling broker). Through this communication, the controller observes the public IP and Port that the ION's traffic is coming from (the post-NAT address).
* Signaling: The controller shares this public reachability information with the peer ION.
* Hole Punching: The IONs then attempt to initiate connections to each other's discovered public IP /Port. This "UDP Hole Punching" allows them to establish a direct IPSec tunnel through the NAT devices without requiring static 1:1 NAT mapping or manual port forwarding on the provider routers, enabling mesh connectivity in commodity internet environments.

NO.4 When planning a software upgrade for a large fleet of ION devices, what is the recommended best practice regarding the "Software Version" assigned in the Site Summary?

A. Manually log into each device and upload the new image file via USB.

B. Assign the new software version to the "Global" site configuration to upgrade all 1000+ sites simultaneously.

C. Use Site Tags to group sites (e.g., "Pilot", "Region-1", "Region-2") and assign the new software version incrementally to these tags to minimize risk.

D. The ION devices upgrade themselves automatically whenever a new version is released by Palo Alto Networks.

Answer: C
Explanation:
Comprehensive and Detailed Explanation
The best practice for managing upgrades in a large-scale Prisma SD-WAN environment is the Canary or Phased Rollout approach, utilizing Site Tags.
* Risk Mitigation: Upgrading all sites simultaneously (Option B) is highly risky. If the new software version has an unforeseen bug or compatibility issue with a specific circuit type, the entire network could face an outage.

* Tag-Based Management: Administrators should create tags such as "Upgrade-Phase-1" (Pilot sites) or
"Region-North". By assigning the specific Software Version to the Tag (rather than the individual site or the global default), the controller pushes the update only to that subset of devices.
* Procedure:
* Apply update to "Pilot" tag (5 sites). Monitor for 24-48 hours.
* Apply update to "Region-1" tag (50 sites). Monitor.
* Eventually, update the Global default once confidence is high.
Option A is unscalable, and Option D is incorrect as the administrator retains full control over when upgrades occur; they are not forced automatically without policy configuration.

NO.5 Which IONs can support Branch Gateway?
A. 3102V, 3200, 1200S, 5200
B. 1200, 3200, 9200, 7108V1
C. 3104V, 1200S, 5200, 7108V
D. 9200, 3200, 5200, 7116V
Answer: D
Explanation:
In the Prisma SD-WAN ecosystem, ION (Instant-On Network) devices are categorized based on their performance capabilities, throughput, and their specific role within the network architecture-namely, whether they function as a Branch device or a Data Center (DC) device.2 The "Branch Gateway" designation typically refers to high-capacity hardware or virtual instances designed to handle complex routing, massive throughput, and high-density connectivity requirements found in large branch offices or regional hubs.
The devices listed in option D represent the high-performance tier of the ION family. The ION 9200 and ION
5200 are flagship hardware appliances designed for large-scale deployments, offering multi-gigabit throughput and extensive port density.3 The ION 3200 serves as a robust mid-to-high range branch solution.4 The ION 7116V is a high-capacity virtual appliance (part of the 7000 series) designed to provide flexible, software-defined gateway capabilities in virtualized environments or public clouds (like AWS, Azure, or GCP).
Specifically, these models support advanced features such as Layer 3 hardware forwarding, integrated switching (in certain sub-models), and the processing power required to run deep packet inspection (DPI) for application-based path selection at scale. While smaller units like the 1200 series are excellent for small-to- medium branches, the 9200, 3200, 5200, and 7116V are the primary workhorses for organizations requiring
"Gateway" class performance to manage heavy traffic loads and maintain high availability in a Prisma SD- WAN fabric.

NO.6 Which specialized hardware feature is available on the ION 9000 series but NOT on the ION 3000 series, making it suitable for high-throughput Data Center deployments?
A. Support for LTE/5G SIM cards
B. Fail-to-Wire Bypass Pairs
C. 10 Gigabit Ethernet (SFP+) ports
D. PoE+ (Power over Ethernet) output ports

Answer: C
Explanation:
Comprehensive and Detailed Explanation
The ION 9000 is the flagship high-performance hardware model designed for large Data Centers and Campus Cores.
* 10GbE Connectivity (C): The defining hardware differentiator for the ION 9000 is its inclusion of multiple 10 Gigabit Ethernet (SFP+) interfaces. This allows it to interconnect with Data Center core switches at 10Gbps speeds, supporting the multi-gigabit aggregate throughput required for hub sites aggregating traffic from hundreds of branches.
* ION 3000: The ION 3000 is a branch-tier device limited to 1 Gigabit Ethernet (copper/SFP) interfaces.
* Bypass Pairs (B): Both models (and others like ION 2000/7000) support Bypass Pairs.
* LTE/PoE (A/D): These are typically features of smaller branch/edge models (like ION 1200), not the high-end DC concentrators.

NO.7 Network segmentation is required due to overlapping IP address space and M&A scenarios. Which Prisma SD-WAN feature will achieve the desired segmentation and end-to-end connectivity in this use case?

A. Virtual Routing and Forwarding (VRF) profiles with proper site bindings to achieve desired isolation across the underlay

B. Virtual Routing and Forwarding (VRF) profiles with proper site bindings to achieve desired isolation locally and across the secure fabric

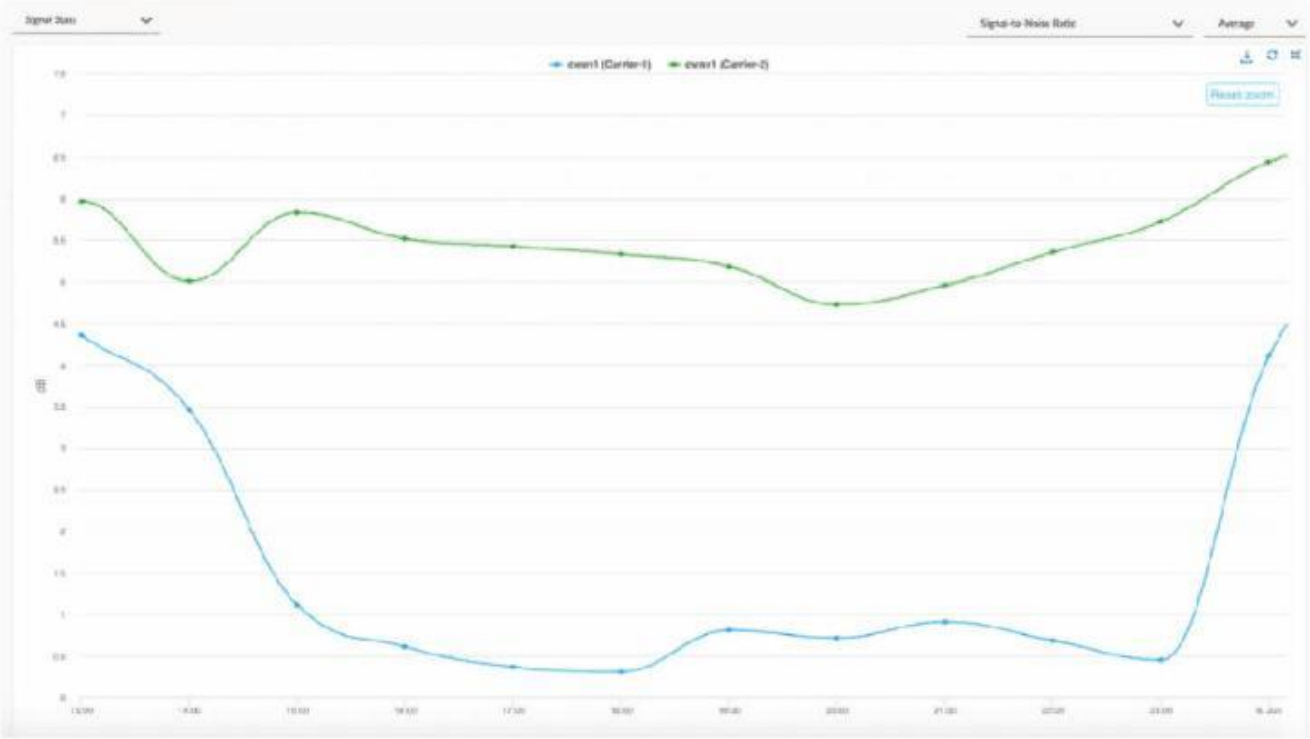
C. Multiple contexts with interface segmentation to achieve desired isolation across the underlay

D. Multiple virtual routers with interface segmentation to achieve desired isolation across the secure fabric

Answer: B
Explanation:
In modern enterprise environments, particularly those undergoing Mergers and Acquisitions (M&A), engineers often face the challenge of overlapping IP address space.4 Prisma SD-WAN addresses this by utilizing Virtual Routing and Forwarding (VRF) profiles.5 A VRF creates a separate routing table instance within the ION device, allowing multiple networks to coexist on the same physical hardware even if they use the same IP ranges.
To achieve end-to-end connectivity while maintaining strict segmentation, these VRF profiles must be correctly associated with site bindings.7 When a VRF is "bound" to a site, the ION device ensures that traffic belonging to that specific segment remains isolated not only locally (on the LAN) but also across the secure SD-WAN fabric. Prisma SD-WAN achieves this by encapsulating the traffic within the overlay tunnels and tagging it with a unique VRF identifier.8 This ensures that a "Corporate" VRF at Site A can only communicate with the "Corporate" VRF at Site B, effectively keeping "Guest" or "Acquisition" traffic completely separate.
This architectural approach is superior to traditional underlay segmentation (Option A) or simple interface- based virtual routers (Option D) because it provides a centralized, software-defined method to manage multi- tenancy. By using VRF profiles, administrators can define a global security and routing posture once and push it to all relevant sites.9 This simplifies the integration of new business units with conflicting IP schemes, as the Prisma SD-WAN controller handles the complex orchestration required to maintain path selection and security policies uniquely for each VRF across

the entire global network.

NO.8 When troubleshooting an issue at a site that is running on two cellular links from two carriers, the operations team shared some evidence shown in the graph below:



For the time duration shown in the graph, what are two inferences about the site's traffic that can be made?
(Choose two.)

A. Using Carrier-1 as the WAN path may have experienced some performance degradation.

B. Using Carrier-2 as the WAN path may have experienced some performance degradation.

C. Using Carrier-2 as the WAN path may have switched over to Carrier-1.

D. Using Carrier-1 as the WAN path may have switched over to Carrier-2.

Answer: A D

Explanation:

The provided graph displays the Signal-to-Noise Ratio (SNR) for two cellular carriers, Carrier-1 (blue line) and Carrier-2 (green line), over a specific period. In cellular communications, SNR is a critical metric used to determine the quality of a wireless signal. A higher SNR indicates a cleaner, stronger signal, while a lower SNR indicates that the signal is being "drowned out" by background noise or interference, which directly correlates to performance degradation, packet loss, and lower throughput.

Looking at the graph, Carrier-1 experiences a significant and sustained drop in SNR, falling from roughly

4.5 dB to nearly 0.5 dB for the majority of the time duration. This drastic reduction in signal quality strongly suggests that Carrier-1 may have experienced performance degradation (Option A). During this dip, the link quality would likely fall below the configured thresholds for business-critical application traffic.

Because Prisma SD-WAN is an application-defined fabric that continuously monitors path health, the ION device would detect this degradation on Carrier-1. If Carrier-2 maintains a significantly higher

and more stable SNR (as shown by the green line remaining between 4.5 dB and 6.5 dB), the ION device's Path Selection engine would automatically steer traffic away from the degraded link. Consequently, it is highly probable that Carrier-1 traffic switched over to Carrier-2 (Option D) to maintain the application SLA. This automated failover is a core strength of the Prisma SD-WAN architecture, ensuring that the best available path is utilized based on real-time link statistics rather than simple "up/down" states.

NO.9 An administrator needs to generate a monthly report showing the "Top Applications" by bandwidth usage across all branch sites to justify a bandwidth upgrade.
Which specific component of the Prisma SD-WAN interface is designed to create, schedule, and email these PDF summaries?

A. Activity Charts

B. Media Analytics

C. Reports

D. Flow Browser

Answer: C

Explanation:
Comprehensive and Detailed Explanation
Prisma SD-WAN separates real-time visibility from historical summarization.
* Reports (C): The Reports section is the dedicated engine for generating historical summaries. Administrators can create custom report templates (e.g., "Monthly Executive Summary") that include specific widgets like "Top Applications by Volume," "Site Availability," or "Circuit Utilization." Crucially, this feature allows for Scheduling, where the system automatically generates the PDF report at a set interval (e.g., first day of the month) and emails it to a distribution list.
* Activity Charts (A) / Media Analytics (B): These provide interactive, visual graphs for ad-hoc analysis but are not designed for generating downloadable, scheduled PDF summaries for management.
* Flow Browser (D): This is for deep-dive troubleshooting of individual sessions, not for high-level aggregate reporting.