SD-WAN-Engineer Training Tools | SD-WAN-Engineer Testking

BONUS!!! Download part of ITexamReview SD-WAN-Engineer dumps for free: https://drive.google.com/open?id=10j1snaaX9TNP6Q9al3axpKxq-BcBipE5

In fact, in real life, we often use performance of high and low to measure a person's level of high or low, when we choose to find a good job, there is important to get the SD-WAN-Engineer certification as you can. Our society needs to various comprehensive talents, rather than a man only know the book knowledge but not understand the applied to real bookworm, therefore, we need to get the SD-WAN-Engineer Certification, obtain the corresponding certifications. What a wonderful news it is for everyone who wants to pass the certification exams. There is a fabulous product to prompt the efficiency--the SD-WAN-Engineer exam prep, as far as concerned, it can bring you high quality learning platform to pass the variety of exams.

Palo Alto Networks SD-WAN-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Operations and Monitoring: This domain addresses monitoring device statistics, controller events, alerts, WAN Clarity reports, real-time network visibility tools, and SASE-related event management.
Topic 2	• Unified SASE: This domain covers Prisma SD-WAN integration with Prisma Access, ADEM configuration, IoT connectivity via Device-ID, Cloud Identity Engine integration, and User • Group-based policy implementation.
Topic 3	• Planning and Design: This domain covers SD-WAN planning fundamentals including device selection, bandwidth and licensing planning, network assessment, data center and branch configurations, security requirements, high availability, and policy design for path, security, QoS, performance, and NAT.
Topic 4	• Troubleshooting: This domain focuses on resolving connectivity, routing, forwarding, application performance, and policy issues using co-pilot data analysis and analytics for network optimization and reporting.
Topic 5	• Deployment and Configuration: This domain focuses on Prisma SD-WAN deployment procedures, site-specific settings, configuration templates for different locations, routing protocol tuning, and VRF implementation for network segmentation.

>> SD-WAN-Engineer Training Tools <<

SD-WAN-Engineer Testking, SD-WAN-Engineer Reliable Dumps Pdf

In our study, we found that many people have the strongest ability to use knowledge for a period of time at the beginning of their knowledge. As time goes on, memory fades. Our SD-WAN-Engineer study materials are designed to help users consolidate what they have learned, will add to the instant of many training, the user can test their learning effect in time after finished the part of the learning content, have a special set of wrong topics in our SD-WAN-Engineer Study Materials, enable users to find their weak spot of knowledge in this function, iterate through constant practice, finally reach a high success rate.

Palo Alto Networks SD-WAN Engineer Sample Questions (Q85-Q90):

NEW QUESTION # 85
By default, how many days will Prisma SD-WAN VPNs stay operational before the keys expire when an ION device loses connection with the controller?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:
Comprehensive and Detailed Explanation
The Prisma SD-WAN (CloudGenix) solution is designed with a separation of the control plane (Controller) and the data plane (ION devices).1 In the event that an ION device loses connectivity to the Cloud Controller (often referred to as running in "headless mode"), the device continues to forward traffic and maintain existing VPN tunnels using the keys it currently holds.2 However, for security purposes, the VPN session keys (shared secrets) used for the Secure Fabric have a finite validity period. The system is designed such that these keys are rotated regularly.3 If the controller is unreachable, the ION device can continue to rotate keys locally and maintain the VPNs for a maximum default period of 72 hours (exactly 3 days).4 If the connection to the controller is not restored within this 72-hour window, the keys will eventually expire, and the ION will be unable to retrieve new authorized key material from the controller.5 Consequently, the VPN tunnels will go down, and the "out of shared secret key" error will be observed in the VPN status logs.
This mechanism ensures that a permanently compromised or stolen device cannot maintain network access indefinitely without central authorization.

NEW QUESTION # 86
When configuring a Path Policy rule for a "Real-Time Video" application, the administrator wants to ensure the traffic uses the path with the lowest packet loss.
How does the Prisma SD-WAN ION determine the "Packet Loss" metric for a given path when there is no active user traffic flowing on that link?

- A. It relies solely on Passive Monitoring of TCP retransmissions from other user traffic on that link.
- B. It defaults to a static value of 0% loss until user traffic begins.
- C. It sends Active Probes (synthetic UDP packets) across the Secure Fabric to measure path quality continuously.
- D. It queries the ISP's router via SNMP to retrieve interface error counters.

Answer: C

Explanation:
Comprehensive and Detailed Explanation
Prisma SD-WAN utilizes Link Quality Monitoring (LQM) to maintain a real-time health score for every WAN path.
To ensure the system knows the quality of a path before sending critical user traffic onto it, the ION device uses Active Probing.
Mechanism: The ION sends synthetic probe packets (typically UDP) across the Secure Fabric (VPN tunnels) and Direct Internet paths to its peers. These probes measure Latency, Jitter, and Packet Loss.
Active vs. Passive: While the system does use Passive Monitoring (observing actual user flows) when traffic is present to reduce overhead, Active Probes are essential for idle links or backup paths. Without active probing, the ION would have no data to make an intelligent steering decision for the first packet of a new video call. This ensures that "Real-Time" policies always have up-to-date metrics to select the best path immediately.

NEW QUESTION # 87
What is the purpose of Secure Group Tag (SGT) propagation in Prisma SD-WAN?

- A. To integrate with external identity-based security solutions
- B. To clarify the intent of rules or configuration objects and improve rule organization
- C. To enable or disable SGT settings at the interface level and initiate services like NTP, DHCP, and App Probes
- D. To manage QoS policies for traffic based on user and application type

Answer: A

Explanation:
In modern enterprise environments, maintaining a consistent security posture across disparate network domains is a major challenge. Prisma SD-WAN addresses this by supporting Secure Group Tag (SGT) propagation. SGTs are a key component of Cisco's TrustSec architecture, used to classify traffic based on the identity of the source (users, devices, or groups) rather than just IP addresses. By supporting SGT propagation, Prisma SD-WAN allows organizations to integrate with external identity-based security solutions seamlessly.
When traffic enters an ION device from a LAN segment where SGTs are already applied (typically by an access layer switch or an Identity Services Engine), the ION device can be configured to preserve or
"propagate" these tags as the traffic traverses the SD-WAN fabric.6 This ensures that the identity context remains intact even after the traffic has crossed the WAN.7 When the traffic reaches its destination-whether that is a data center, another branch, or a security gateway-the receiving device can use the SGT to enforce granular security policies.
This integration is vital for organizations moving toward a Zero Trust architecture. Instead of rewriting complex firewall rules at every hop, the SGT acts as a portable identity badge. Prisma SD-WAN's ability to handle these tags allows it to participate in a larger security ecosystem, ensuring that a "Finance" user is treated with the same security restrictions at a remote branch as they would be at the corporate headquarters.
This eliminates the need for manual IP-to-Group mapping across the WAN, reducing administrative overhead and minimizing the risk of security gaps during lateral movement of traffic.

NEW QUESTION # 88
Where is route leaking configured between VRFs?

- A. BGP peer
- B. VRF definition
- C. Site configuration
- D. VRF profile

Answer: D

Explanation:
In the Prisma SD-WAN solution, multi-tenancy and network isolation are achieved through the use of Virtual Routing and Forwarding (VRF) instances. However, there are many operational scenarios-such as providing shared access to a common service (e.g., DNS, NTP) or a central Internet gateway-where traffic must transition between these isolated routing domains. This process is known as route leaking.
In the Prisma SD-WAN management interface, route leaking is specifically configured within the VRF Profile. Unlike traditional CLI-based routers where route leaking might be configured under a global routing table or individual VRF definitions via import/export targets, Prisma SD-WAN utilizes a profile-based approach to ensure scalability and consistency across multiple sites. A VRF Profile acts as a template that defines the routing behavior for specific VRFs across the fabric.
When an administrator navigates to the VRF Profile settings, they can define "Leaking Rules." These rules specify the "From VRF" (source) and "To VRF" (destination) parameters, along with the specific prefixes or default routes that should be shared. By placing this configuration within the VRF Profile rather than a site- specific configuration, Palo Alto Networks allows for a "configure once, apply many" workflow. Once the VRF Profile is updated with the leaking rules, any ION device associated with that profile will automatically update its local routing table to allow the specified inter-VRF communication. This centralized orchestration simplifies the management of complex segmentation requirements in large-scale SD-WAN deployments.

NEW QUESTION # 89
User-ID integration is configured for a Prisma SD-WAN deployment. Branch-1 has the user-to-IP mappings available, and User-1 is mapped to IP-1.
To which two use cases can User-ID based zone-based firewall policies be applied? (Choose two.)

- A. User-1 accessing a private application within Branch-1, and source User-ID based zone-based firewall rules on Branch-1 ION
- B. User-1 accessing a private application in Branch-2 via SD-WAN overlay, and destination User-ID based zone-based firewall rules on Branch-2 ION
- C. User-1 accessing a private application in data center via SD-WAN overlay, and destination User-ID based zone-based firewall rules on DC ION
- D. User-1 accessing a SaaS application on direct internet and source User-ID based zone-based firewall rules on Branch-1 ION

Answer: A,D

Explanation:
Comprehensive and Detailed Explanation
In Prisma SD-WAN (CloudGenix), Zone-Based Firewall (ZBFW) policies rely on the device's ability to map an IP address to a User-ID to enforce identity-based rules. The key to this question is understanding where the mapping exists and which direction the policy attributes (Source User vs. Destination User) apply to.
1. Mapping Location (Branch-1): The prompt states that Branch-1 has the user-to-IP mapping for User-1. For the most effective and scalable security enforcement, policies should be applied at the source (ingress) device where the traffic originates and where the user identity is known. This prevents unauthorized traffic from consuming WAN bandwidth only to be dropped at the destination. Therefore, the Branch-1 ION is the correct enforcement point for User-1's traffic.
2. Source vs. Destination User:
User-1 is the Source: In all scenarios, User-1 is the initiator of the traffic. Therefore, the security rule must match on Source User-ID.
Options C and D are incorrect because they suggest using Destination User-ID based rules to control User-1. Destination User-ID rules are used when the target of the traffic is a known user (e.g., VoIP calls to a specific user's phone), not when filtering based on the sender. Furthermore, relying on the DC or Branch-2 ION to enforce policies for User-1 would require the propagation of User-ID mappings across the overlay, whereas local enforcement at Branch-1 is the standard architectural model.
3. Valid Use Cases (A and B):
Option A (SaaS/Internet): The Branch-1 ION acts as the internet gateway. It can use the local mapping (IP-1 = User-1) to allow or deny access to specific SaaS applications (Direct Internet Access) based on the user's identity (e.g., "Allow Marketing Group to access Social Media").
Option B (Internal Segmentation): The Branch-1 ION can enforce policies for traffic moving between local zones (e.g., from a "Users" VLAN to a "Servers" VLAN within the branch). Since the ION routes this traffic and holds the mapping, it can enforce Source User-ID policies to secure local private applications.

NEW QUESTION # 90
.....

Engineer PDF Question

- Palo Alto Networks SD-WAN-Engineer Realistic Training Tools Pass Guaranteed □ Copy URL □ www.practicevce.com □ open and search for 《 SD-WAN-Engineer 》 to download for free □SD-WAN-Engineer Pdf Demo Download
- 100% Pass Quiz SD-WAN-Engineer - Newest Palo Alto Networks SD-WAN Engineer Training Tools □ ➠ www.pdfvce.com □ is best website to obtain ⇛ SD-WAN-Engineer ⇚ for free download □Exam SD-WAN-Engineer Answers
- Pass-Sure SD-WAN-Engineer Training Tools | Easy To Study and Pass Exam at first attempt - Perfect SD-WAN-Engineer: Palo Alto Networks SD-WAN Engineer □ Download ➡ SD-WAN-Engineer □□□ for free by simply entering ⇛ www.verifieddumps.com ⇚ website □Real SD-WAN-Engineer Question
- abelgslc606954.onzeblog.com, lewisffje315219.blogdosaga.com, gorillasocialwork.com, yeepdirectory.com, prestonthil314353.blog-ezine.com, www.stes.tyc.edu.tw, ammarvvew383123.mysticwiki.com, pasteldirectory.com, dawudhapu760103.techionblog.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

What's more, part of that ITexamReview SD-WAN-Engineer dumps now are free: https://drive.google.com/open?id=10j1snaaX9TNP6Q9al3axpKxq-BcBipE5