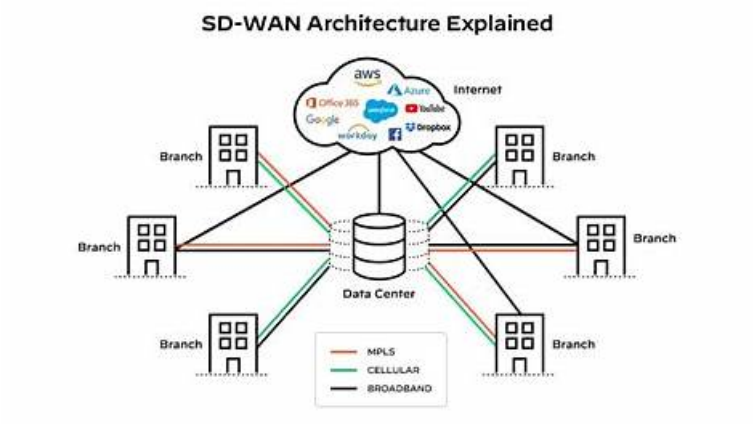
最新的Palo Alto Networks SD-WAN-Engineer熱門考題是行業領先材料＆權威的SD-WAN-Engineer：Palo Alto Networks SD-WAN Engineer



從Google Drive中免費下載最新的KaoGuTi SD-WAN-Engineer PDF版考試題庫：https://drive.google.com/open?id=10g5y_mYLRGkjxMfaF3d8rSLQMZo7xM-z

Palo Alto Networks SD-WAN-Engineer 認證考試是個檢驗IT專業知識的認證考試。KaoGuTi是個能幫你快速通過Palo Alto Networks SD-WAN-Engineer 認證考試的網站。在您考試之前使用我們提供的針對性培訓和測試練習題和答案，短時間內你會有很大的收穫。

我們KaoGuTi Palo Alto Networks的SD-WAN-Engineer考試的試題及答案，為你提供了一切你所需要的考前準備資料，關於Palo Alto Networks的SD-WAN-Engineer考試，你可以從不同的網站或書籍找到這些問題，但關鍵是邏輯性相連，我們的試題及答案不僅能第一次毫不費力的通過考試，同時也能節省你寶貴的時間。

>> SD-WAN-Engineer熱門考題 <<

有幫助的SD-WAN-Engineer熱門考題，最新的考試指南幫助妳快速通過SD-WAN-Engineer考試

KaoGuTi 考題網覆蓋了真實的 SD-WAN-Engineer 考試指南，並根據其編定適合全球考生都能通用的 SD-WAN-Engineer 題庫，讓每一位考生都能順利通過 Palo Alto Networks SD-WAN-Engineer 考試。我們承諾使用 SD-WAN-Engineer 考題的考生可以一次通過相關認證考試，對于一次不過的全額退款，避免您的後顧之憂。你現在就可以去網上可以免費下載我們提供的部分關於 Palo Alto Networks SD-WAN-Engineer 題庫的模擬測試題和答案作為嘗試。

Palo Alto Networks SD-WAN-Engineer 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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.
主題 3	• 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.

主題 4	• 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.
主題 5	• 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.

最新的 Network Security Administrator SD-WAN-Engineer 免費考試真題 (Q63-Q68):

問題 #63
For how many hours are Prisma SD-WAN VPN shared secrets valid?

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

答案：A

解題說明：
Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:
In the Prisma SD-WAN architecture, security is built directly into the AppFabric using a centralized, controller-led approach to key management. Unlike traditional VPNs that rely on manual Internet Key Exchange (IKE) or static Pre-Shared Keys (PSKs) which can be administratively burdensome and security-vulnerable, Prisma SD-WAN automates the entire lifecycle of encrypted tunnels. The Prisma SD-WAN Controller acts as the central authority for identity and key distribution for all ION (Instant-On Network) devices within the tenant's fabric.
Specifically, the VPN shared secrets used to secure these tunnels are ephemeral and are valid for exactly 24 hours. This 24-hour validity period is a security best practice implemented by Palo Alto Networks to limit the "blast radius" or window of exposure in the unlikely event that a key is compromised. The controller automatically handles the generation, distribution, and rotation of these secrets. Before the 24-hour timer expires, the controller pushes new keys to the ION devices, which then perform a hitless rollover. This ensures that the data plane remains active and encrypted without requiring manual intervention from a network administrator. If an ION device loses its control plane connection to the controller, it will maintain its existing tunnels using the current keys until they expire, at which point it must re-authenticate with the controller to receive a new set of valid secrets. This automated rotation is a core component of the Prisma SD-WAN Zero-Trust security model.

問題 #64
In which modes can a Prisma SD-WAN branch be deployed?

- A. Production, Control, Disabled
- B. POV, Production, Analytics
- C. Disabled, Analytics, Control
- D. Testing, Control, POV

答案：C

解題說明：
Comprehensive and Detailed Explanation
Prisma SD-WAN (formerly CloudGenix) defines three distinct Operational Modes for a branch site, which determine how the ION device processes traffic and interacts with the network.
Analytics Mode (Monitor): In this mode, the ION device is typically deployed inline or in a "promiscuous" monitor state to gain visibility into network traffic without actively enforcing path selection policies.1 It "learns" applications, bandwidth usage, and network characteristics (auditing) but does not steer traffic or block flows.2 This is often used during Proof of Concepts (POVs) or the initial "burn-in" phase of a deployment to generate reports without risking network disruption.
Control Mode: This is the full production state. In Control Mode, the ION device actively enforces Path Policies, QoS Policies, and Security Policies. It builds Secure Fabric VPN tunnels, steers traffic based on application SLAs (e.g., sending voice over MPLS and bulk data over Broadband), and handles failover events.3 This is the required mode for a fully functional SD-WAN site.
Disabled Mode: This mode effectively shuts down the site's SD-WAN functionality from the controller's perspective. It is an

administrative state used when a site is being decommissioned, provisioned but not yet live, or isolated for troubleshooting. In this state, the device does not participate in the fabric.

問題 #65
Where is route leaking configured between VRFs?

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

答案：D

解題說明：
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.

問題 #66
Which configuration requirement must be met to allow two branch ION devices to automatically establish a direct Dynamic VPN (branch-to-branch) connection for traffic flow, bypassing the Data Center?

- A. A static "Gre Tunnel" must be manually configured between the two sites.
- B. The Data Center ION must be offline to trigger the dynamic failover.
- C. The "Standard VPN" path policy must be selected.
- D. Both ION devices must be members of the same VPN Cluster.

答案：D

解題說明：
Comprehensive and Detailed Explanation
Dynamic VPNs (also known as ION-to-ION or Branch-to-Branch VPNs) allow Prisma SD-WAN devices to establish direct, on-demand secure tunnels between branch sites to optimize latency for peer-to-peer traffic (e.
g., VoIP calls between offices).
To enable this capability, the primary architectural requirement is the configuration of VPN Clusters.
A VPN Cluster defines a logical group of devices that are authorized to communicate with one another.
* By default, or if devices are in different clusters without peering, the topology typically defaults to Hub- and-Spoke, where branches only talk to the Data Center.
* When two branch ION devices are placed into the same VPN Cluster (or peered clusters), the controller shares the necessary reachability and cryptographic information between them.
Once in the same cluster, the ION devices monitor traffic. If a user at Branch A tries to contact a server at Branch B, the ION devices detect this interest. If a direct path is available (e.g., via public internet), they will dynamically negotiate a direct VPN tunnel, bypassing the Data Center hub. This offloads the hub and reduces latency. Option B is incorrect because SD-WAN eliminates manual GRE config. Option C is incorrect because dynamic VPNs are a performance feature, not just a disaster recovery feature.

問題 #67

In a Prisma SD-WAN deployment, what is the defining characteristic of a "Standard VPN" compared to a "Secure Fabric Link"?

- A. Standard VPNs are automatically built between ION devices, while Secure Fabric Links require manual configuration.
- B. Standard VPNs support BGP, whereas Secure Fabric Links only support static routing.
- C. Standard VPNs use GRE encapsulation, while Secure Fabric Links use VXLAN.
- D. Standard VPNs are manually configured IPSec tunnels to non-ION endpoints, while Secure Fabric Links are automated tunnels between ION devices.

答案：D

解題說明：
Comprehensive and Detailed Explanation
In the Prisma SD-WAN architecture, the terminology distinguishes between "Native" automation and "Legacy" interoperability.
Secure Fabric Links: These are the proprietary, automated overlay tunnels created between two Prisma SD-WAN ION devices (e.g., Branch ION to Data Center ION). The controller automatically manages the IP addressing, key rotation, and routing for these links. You do not manually configure "Phase 1" or "Phase 2" parameters for Secure Fabric links.
Standard VPNs: These are traditional, standards-based IPSec tunnels configured to connect an ION device to a Non-ION endpoint (Third-Party Peer). This is used for "Data Center to Data Center" connections where one side is a legacy firewall (e.g., Cisco ASA, Palo Alto Networks NGFW) or for connecting to cloud security services (SSE) that do not have a specific CloudBlade integration. For a Standard VPN, the administrator must manually define the IKE/IPSec profiles, pre-shared keys, and peer IP addresses to match the third-party device's configuration.

問題 #68
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, indianagriexam.com, englishprep.sarvanimmigration.ca, myportal.utt.edu.tt, bbs.x7cq.vip, Disposable vapes

從Google Drive中免費下載最新的KaoGuTi SD-WAN-Engineer PDF版考試題庫：https://drive.google.com/open?id=10g5y_mYLRGkjxMfaF3d8rSLQMZo7xM-z