



Vendor: Palo Alto Networks

Exam Code: SD-WAN-Engineer

Exam Name: Palo Alto Networks SD-WAN Engineer

Version: DEMO

QUESTION 1

A network installer is at a remote branch site to deploy a new ION 3000 device. The device has been racked, cabled to the internet, and powered on. The installer has the "Claim Code" displayed on the email sent by the administrator. When the administrator enters this Claim Code into the Prisma SD-WAN portal, what is the immediate status of the device before the configuration is fully pushed?

- A. Online
- B. Claimed
- C. Provisioned
- D. Active

Answer: B

Explanation:

In the Prisma SD-WAN (CloudGenix) Zero Touch Provisioning (ZTP) lifecycle, the device status transitions through specific stages that indicate its readiness and connectivity.

When an administrator enters the Claim Code (or Serial Number/Claim Code pair) into the portal, the device status immediately updates to "Claimed".

This status confirms that the portal has registered the device's unique identity and associated it with the customer's tenant. However, "Claimed" does not necessarily mean the device is fully operational or passing traffic yet. It simply signifies that the ownership is verified.

Once the physical device at the site successfully connects to the internet and reaches the Prisma SD-WAN Controller (using the call-home function), it will authenticate using its installed certificate. Upon successful authentication and the establishment of the secure control channel, the status will transition from "Claimed" to "Online".

Only after the device is "Online" can the controller push the specific site configuration (Device Shell), policies, and IP addressing required for the device to become "Provisioned" and eventually "Active" in the data path. If the device remains in the "Claimed" state for an extended period, it indicates that the hardware has not yet successfully contacted the controller, which prompts troubleshooting of the physical internet circuit or firewall rules upstream.

QUESTION 2

An administrator has configured a Path Policy for "ERP_Traffic". The policy allows two public internet links, "ISP-A" and "ISP-B", both marked as "Active". The Path Quality Profile (SLA) requires a latency of less than 150ms. Currently, both ISP-A and ISP-B have a latency of 40ms, well within the SLA. How does the Prisma SD-WAN ION determine which link to use for a new flow of "ERP_Traffic" when both active paths meet the SLA requirements?

- A. It selects the path with the lowest numerical latency (e.g., if ISP-A drops to 39ms).
- B. It selects the path with the highest available bandwidth capacity.
- C. It duplicates the packets across both paths (Packet Duplication) to ensure delivery.
- D. It selects the path that appears first in the interface configuration list.

Answer: B

Explanation:

Prisma SD-WAN utilizes a sophisticated decision engine for Application-Based Path Selection that goes beyond simple failover. When configuring a Path Policy, the administrator defines "Active" paths and a "Path Quality Profile" (SLA).

SLA Compliance (The Filter): First, the system filters the available paths based on the Path Quality Profile. In this scenario, both ISP-A and ISP-B have 40ms latency against a 150ms threshold. Both are "green" or compliant paths.

Selection Criteria (The Tie-Breaker): When multiple paths are configured as "Active" and all meet the performance SLA, the ION device aims to optimize the overall user experience and network utilization. The default behavior for load balancing across healthy, compliant active paths is to select the path with the highest available bandwidth capacity.

By steering new flows to the link with the most "headroom" (available Mbps), the system prevents the saturation of a smaller link (e.g., a 20Mbps DSL line) while a larger link (e.g., 1Gbps Fiber) sits underutilized. This maximizes the aggregate throughput for the site. While latency is the qualifier, bandwidth availability is often the selector for compliant paths. Note that if the application was defined as "Real-Time" and configured for packet duplication, behavior would differ, but for standard traffic, capacity-based distribution is the standard active/active logic.

QUESTION 3

What is the primary function of the "CloudBlade" platform in a Prisma SD-WAN deployment when integrating with third-party services or Prisma Access?

- A. It acts as a physical line card on the ION device to provide additional 10Gbps interfaces.
- B. It is a containerized application running on the ION device that performs Deep Packet Inspection (DPI).
- C. It is a cloud-based API integration layer that automates the configuration of the ION devices and the remote service.
- D. It is a monitoring dashboard used exclusively for viewing flow records.

Answer: C

Explanation:

The CloudBlade platform is a distinguishing architectural component of the Prisma SD-WAN solution. It is not a physical piece of hardware, nor is it software that runs directly on the branch ION device's CPU.

Instead, the CloudBlade platform is a cloud-based API integration layer hosted by Palo Alto Networks. It functions as an intelligent broker or "translator" between the Prisma SD-WAN Controller and external third-party services (such as Prisma Access, Amazon Web Services, Azure, ServiceNow, or Zscaler).

When an administrator configures the Prisma Access CloudBlade, for example, they input their API credentials and intent (e.g., "Connect all US branches to US West"). The CloudBlade engine then:

Communicates with the Prisma Access API to provision the remote IPSec termination nodes (Security Processing Nodes).

Translates this configuration into specific instruction sets for the Prisma SD-WAN Controller.

The Controller then pushes the necessary VPN tunnel configurations, IKE parameters, and routing rules to the relevant ION devices.

This architecture eliminates the need for manual IPSec configuration on every branch device. It ensures that if the third-party service changes its IP addresses or settings, the CloudBlade can detect the change via API and automatically update the branch fleet, maintaining connectivity without manual administrator intervention.

QUESTION 4

A network engineer is troubleshooting a user complaint regarding "slow application performance" for an internal web application. While viewing the Flow Browser in the Prisma SD-WAN portal, the engineer notices that the Server Response Time (SRT) is consistently high (over 500ms), while the Network Transfer Time (NTT) and Round Trip Time (RTT) are low (under 50ms). What does this data indicate about the root cause of the issue?

- A. The issue is likely caused by congestion on the WAN circuit, requiring a QoS policy adjustment.
- B. The issue is likely on the application server itself (e.g., high CPU, slow database query), not the network.
- C. The issue is caused by a high packet loss rate on the internet path.
- D. The issue is due to a misconfigured DNS server at the branch.

Answer: B

Explanation:

The Flow Browser and App Response Time metrics in Prisma SD-WAN are critical tools for isolating the fault domain--determining whether a problem lies in the "Network" or the "Application."

Network Transfer Time (NTT) / Round Trip Time (RTT): These metrics measure the time it takes for packets to traverse the network (WAN/LAN) and for acknowledgments to return. A low NTT (e.g., <50ms) confirms that the network pipes (SD-WAN overlay, Underlay circuits) are healthy and transporting packets quickly.

Server Response Time (SRT): This metric specifically measures the time between the server receiving a request and the server sending the first byte of the response. It essentially measures the "processing time" of the backend server.

In the scenario described, the network metrics (NTT/RTT) are excellent, effectively ruling out WAN congestion, packet loss, or latency (Option A and C). However, the Server Response Time (SRT) is very high (500ms). This signature is a definitive indicator that the network delivered the request instantly, but the application server took a long time to process it. This points the troubleshooting effort toward the server infrastructure (e.g., a slow SQL query, an overloaded web server, or lack of compute resources) rather than the SD-WAN environment.

QUESTION 5

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

Answer: A

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.

QUESTION 6

During the Zero Touch Provisioning (ZTP) process of a new ION device at a branch site, which interface ports are supported by default to request an IP address via DHCP and reach the Prisma SD-WAN controller for claiming?

- A. Only the dedicated Controller port (if available)
- B. Any LAN or WAN port on the device
- C. The dedicated Controller port, or Port 1 / Internet 1 if a dedicated port is absent
- D. Only the USB port via a cellular modem

Answer: C

Explanation:

For a successful Zero Touch Provisioning (ZTP) experience, the ION device must be able to obtain an IP address and reach the internet immediately upon boot-up.

According to Palo Alto Networks hardware guides, the Controller Port (often labeled specifically as "CONTROLLER" on models like the ION 3000/7000/9000) is pre-configured to act as a DHCP client by default. It is the preferred interface for the initial "call home" process.

However, for smaller desktop models (like the ION 1000/2000/1200 series) or scenarios where a dedicated management network is not available, the device firmware is also configured to attempt DHCP client requests on Port 1 (often labeled as Internet 1 or simply 1).

Connecting the ISP circuit to any random port (like Port 4 or a LAN port) will not work for ZTP because those interfaces are not pre-configured as DHCP clients in the factory default state. Therefore, the installer must ensure the internet uplink is connected to either the dedicated Controller port or Port 1/Internet 1 to ensure the device can resolve the controller FQDN and download its configuration.

QUESTION 7

A network engineer is troubleshooting an ION device that is showing as "Offline" in the Prisma SD-WAN portal, despite the site reporting that local internet access is working. The engineer has console access to the device. Which CLI command should be used to specifically validate the device's ability to resolve the controller's hostname and establish a secure connection to it over a

specific interface?

- A. ping <controller-ip>
- B. debug controller reachability <interface>
- C. show system connectivity
- D. dump vpn summary

Answer: B

Explanation:

The CLI command debug controller reachability <interface> (e.g., debug controller reachability 1) is the specific diagnostic tool designed to verify the entire connectivity chain required for management plane availability.

Unlike a simple ICMP ping (Option A), which only tests Layer 3 connectivity to an IP address, the debug controller reachability command performs a sequential set of tests:

DNS Resolution: It attempts to resolve the specific Locator service URL (locator.cgnx.net or region-specific FQDN) to verify DNS functionality.

TCP Connectivity: It tests the ability to establish a TCP connection to the controller on port 443 (HTTPS).

SSL/TLS Handshake: It validates that the device can successfully negotiate the secure tunnel required for authentication.

If this command fails at the DNS step, the issue is likely a missing DNS server in the interface config. If it fails at the TCP step, it implies an upstream firewall is blocking outbound port 443. This targeted output allows the engineer to pinpoint exactly why the device is offline in the portal.

QUESTION 8

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

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

Answer: C

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.

QUESTION 9

An administrator is configuring a BGP peer on a Data Center ION to learn routes from the core switch. The goal is to have the ION learn these prefixes and then advertise them to all remote branch sites across the SD-WAN overlay. Which setting must be configured on the BGP Peer to ensure these learned routes are redistributed into the SD-WAN fabric?

- A. Set the "Admin Distance" to 20.
- B. Enable "Graceful Restart".
- C. Set the "Scope" to "Global".
- D. Configure a "Prefix List" to deny all.

Answer: C

Explanation:

In Prisma SD-WAN routing configuration, the Scope setting on a BGP Peer (or a Static Route) controls the redistribution logic for the prefixes learned from that source.

Local Scope: If a BGP peer is configured with "Local" scope, the ION device will install the learned routes into its local routing table for its own reachability, but it will not advertise (redistribute) these routes to other ION devices via the Secure Fabric. They remain local to the site.

Global Scope: To advertise reachability to the rest of the network, the BGP peer must be configured with "Global" scope. This tells the ION that any prefixes learned from this specific neighbor (e.g., the DC Core Switch) should be propagated across the SD-WAN overlay to remote branches. This is the critical setting for enabling branch-to-DC communication for applications hosted behind that BGP peer. Without "Global" scope, the branches would never learn the routes to the data center subnets.

QUESTION 10

What is the default action for real-time media applications if link performance is poor?

- A. Drop the flow.
- B. Move flows.
- C. Apply Forward Error Correction (FEC).
- D. Raise an alarm.

Answer: B

Explanation:

According to the Prisma SD-WAN Performance Policy Default Behavior documentation, the default action configured for applications (including real-time media) when a path experiences poor performance (violates the SLA thresholds for latency, jitter, or packet loss) is to Move Flows. The Prisma SD-WAN ION device continuously monitors the health of all available paths. If the active path for a media application degrades and fails to meet the specified SLA, the default policy dictates that the traffic should be steered (moved) to an alternate, compliant path that meets the performance criteria.

While Forward Error Correction (FEC) is a powerful feature available in Prisma SD-WAN to mitigate packet loss for real-time applications, it is an optional action that must be explicitly enabled or configured within the performance policy rules. It is not the default action in the base

system configuration; the primary default mechanism for handling performance issues is to leverage the multi-path fabric to switch to a better link.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14