ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

When identifying devices for IoT classification purposes, which two methods does Prisma SD-WAN use to discover devices that are not directly connected to the branch ION? (Choose two.)

A. LLDP

B. CDP

C. SNMP

D. Syslog

Answer: C, D

Explanation:

Comprehensive and Detailed Explanation

Prisma SD-WAN (formerly CloudGenix) integrates with Palo Alto Networks IoT Security to provide comprehensive visibility into all devices at a branch, including those that are not directly connected to the ION device. While the ION automatically detects and classifies devices connected directly to its interfaces via traffic inspection (DPI), DHCP, and ARP analysis, gaining visibility into off-branch devices (devices connected to downstream switches or access points) requires additional discovery mechanisms that can query the network infrastructure or ingest its logs.

1. SNMP (Simple Network Management Protocol): This is the primary active discovery method for off-branch devices. The Prisma SD-WAN ION device acts as a sensor that actively polls local network switches and wireless controllers using SNMP. By querying the ARP tables and MAC address tables (Bridge MIBs) of these intermediate network devices, the ION can identify endpoints that are connected to the switch ports, even if those endpoints are not currently sending traffic through the ION. This allows the system to map the topology and discover silent or lateral-traffic-only devices.

2. Syslog: In conjunction with SNMP, the IoT Security solution can utilize Syslog messages to discover and profile devices. Network infrastructure devices (like switches and WLAN controllers) can be configured to send Syslog messages to the collection point (which enables the IoT Security service) whenever a device connects or disconnects (e.g., port up/down events, DHCP snooping logs, or 802.1x authentication logs). These logs provide real-time data about device presence and identity (MAC/IP mappings) for devices that are not directly adjacent to the ION, ensuring 100% visibility across the branch network segments. LLDP (A) and CDP (B) are typically Link Layer discovery protocols used for discovering directly connected neighbors and do not propagate beyond the immediate link, making them unsuitable for discovering devices multiple hops away or behind a switch.

Question: 2

A network administrator is troubleshooting a critical SaaS application, "SuperSaaSApp", that is experiencing connectivity issues. Initially, the configured active and backup paths for the application were reported as completely down at Layer 3. The Prisma SD-WAN system attempted to route traffic for the application over an L3 failure path that was explicitly configured as a Standard VPN to Prisma Access.

However, users are still reporting a complete outage for the application and monitoring tools show application flows being dropped when attempting to use the Standard VPN L3 failure path, even though the tunnel itself appears to be up. The administrator suspects a policy misconfiguration related to how the Standard VPN path interacts with destination groups.

What is the most likely reason for flows being dropped when attempting to use the Standard VPN L3 failure path?

A. The "Move Flows Forced" action was not enabled in the performance policy for "SuperSaaSApp", preventing the system from actively shifting traffic to the L3 failure path.

B. The path policy rule for "SuperSaaSApp" has the "Required" checkbox selected for its Service & DC Group, but no direct paths were configured alongside it, creating a conflict.

C. The path policy rule explicitly designates a Standard VPN as the L3 failure path, but it does not include a designated Standard Services and DC Group, causing traffic to be dropped.

D. The Standard VPN in the path policy was not configured to "Minimize Cellular Usage", leading to the depletion of metered data and subsequent flow drops.

Answer: C

Explanation:

Comprehensive and Detailed Explanation

According to Palo Alto Networks Prisma SD-WAN administrator documentation regarding Path Policy configuration, specific rules apply when utilizing Standard VPNs (IPSec tunnels to non-ION devices, such as Prisma Access or third-party firewalls) as an L3 Failure Path.

When a Path Policy rule is configured, the administrator defines Active Paths, Backup Paths, and L3 Failure Paths. The L3 Failure Path is a "last resort" mechanism used when all Active and Backup paths are unavailable (Layer 3 down).

If Standard VPN is selected as the L3 Failure Path type, the system explicitly requires that the administrator also associates it with a specific Standard Services and DC Group within that same policy rule.

The ION device uses the Standard Services and DC Group to identify the specific remote endpoint (tunnel destination) where the traffic should be routed. Unlike a "Direct" (Internet) path which can simply route out to the WAN, a Standard VPN represents a logical tunnel. If the policy rule designates "Standard VPN" as the failure path but leaves the "Standard Services and DC Group" field empty or unselected, the ION effectively has a directive to "use a VPN" but lacks the instruction on which VPN group to use for this specific application context. Consequently, even if the IPSec tunnel to Prisma Access is physically up and stable, the policy engine cannot resolve the next hop for the "SuperSaaSApp" traffic, resulting in the packets being dropped. To resolve this, the administrator must edit the Path Policy rule to ensure the specific Standard Service/DC Group representing Prisma
Access is checked/selected for the L3 Failure Path.

Question: 3

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 SaaS application on direct internet and source User-ID based zone-based firewall rules on Branch-1 ION

B. User-1 accessing a private application within Branch-1, and source User-ID based zone-based firewall rules on

Branch-1 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 private application in Branch-2 via SD-WAN overlay, and destination User-ID based zone-based firewall rules on Branch-2 ION

Answer: A, B

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.

Question: 4

A site has two internet circuits: Circuit A with 500 Mbps capacity and Circuit B with 100 Mbps capacity.

Which path policy configuration will ensure traffic is automatically shifted from a saturated circuit to the circuit with available bandwidth?

A. Circuit A as an active, Circuit B as a backup

B. Circuit B as an active, Circuit A as a backup

C. Both circuits under active path

D. Circuit B as an L3 failure path

Answer: C

Explanation:

Comprehensive and Detailed Explanation

In Prisma SD-WAN (CloudGenix), Path Policies control how application traffic is steered across WAN links. To ensure that traffic is automatically shifted from a saturated circuit to another circuit with available bandwidth, both circuits must be configured as Active Paths within the policy rule.

When multiple paths are designated as "Active," the ION device treats them as a shared pool of available resources. The system continuously monitors the bandwidth utilization (capacity) and health (latency, jitter, loss) of all active links. If "Circuit A" (500 Mbps) becomes saturated or approaches its defined bandwidth limit, the ION's intelligent scheduler will automatically direct new application flows to "Circuit B" (100 Mbps) because it is a valid, healthy Active path with available capacity. This achieves effective load balancing and bandwidth aggregation.

In contrast, configuring "Circuit B" as a Backup Path (Option A or B) creates a strict priority relationship. Traffic would only move to the Backup path if the Active path completely failed or violated its configured SLA (Path Quality Profile) significantly enough to be considered "down." Mere bandwidth saturation might not trigger an SLA failure immediately, potentially leading to dropped packets on the saturated link while the backup link remains idle. Therefore, placing Both circuits under active path is the correct configuration for dynamic capacity management.

Question: 5

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).1

D. Raise an alarm.

Answer: B

Explanation:

Comprehensive and Detailed 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.

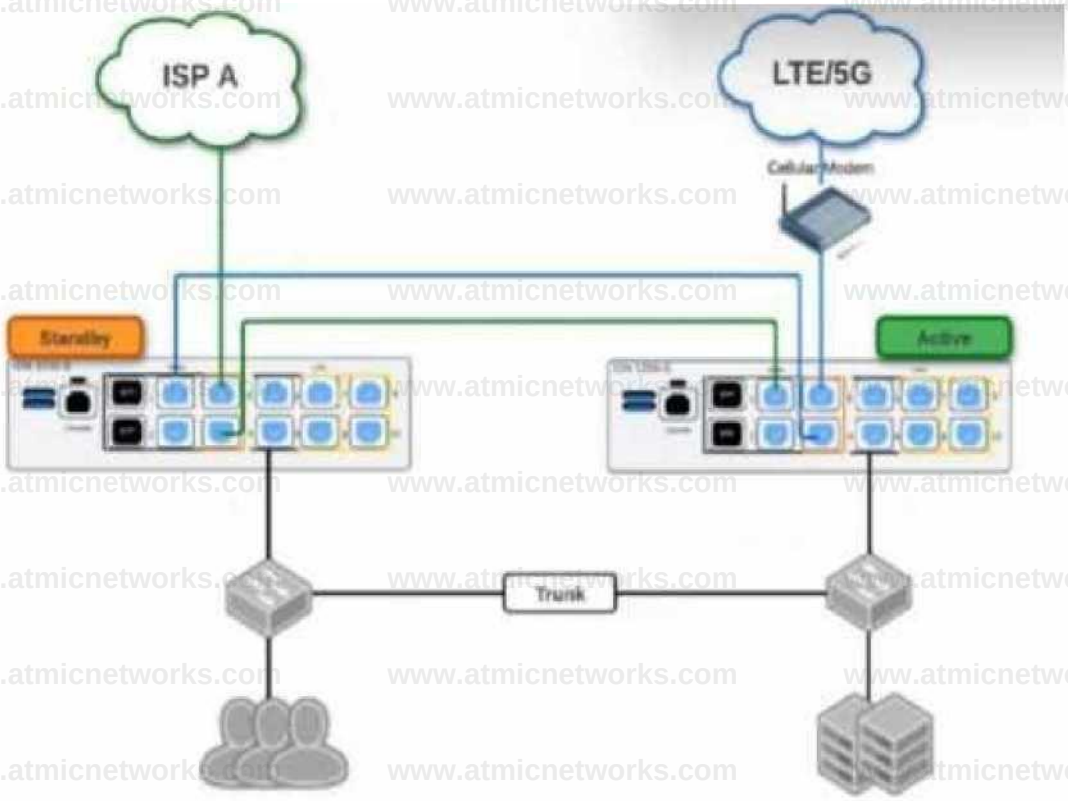
The Prisma SD-WAN ION device continuously monitors the health of all available paths. If the active path for a media application degrades and fails to meet the specified SLA, the default policy dictates that the traffic should be steered (moved) to an alternate, compliant path that meets the performance 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.

Reference: Prisma SD-WAN Administrator's Guide: Performance Policy Default Behavior

Question: 6

Based on the HA topology image below, which two statements describe the end-state when power is removed from the ION 1200-S labeled “Active”, assuming that the ION labeled “Standby” becomes the active ION? (Choose two.)



A. Both the connection to ISP A and the connection to LTE/5G will be usable.

B. The VRRP Virtual IP address assigned to any SVIs will be moved to the newly active ION.

C. The newly active ION will send a gratuitous ARP to the LAN for the IP address of any SVIs.

D. The connection to ISP A will be usable, but the connection to LTE/5G will not.

Answer: A, C

Explanation:

Comprehensive and Detailed Explanation

This scenario depicts a High Availability (HA) topology utilizing the ION 1200-S model's Fail-to-Wire (bypass) capabilities to share WAN links between two devices without needing external switches for every WAN connection.

1. WAN Link Availability (Statement A):

The diagram illustrates a "daisy-chain" cabling method supported by the ION 1200-S bypass pairs.

ISP A (Green): Connects directly to the "Standby" (Left) unit first. Since the Standby unit remains powered on, it maintains direct access to ISP A.

LTE/5G (Blue): Connects to the "Active" (Right) unit first. The connection then loops through a bypass pair on the Active unit to the Standby unit. When power is removed from the "Active" unit, the fail- to-wire relays on its Ethernet ports close physically. This creates a passive electrical bridge that connects the LTE modem directly to the Standby unit. The Standby unit (now becoming Active) will detect the link state change and successfully utilize the LTE connection. Therefore, both WAN links remain usable.

2. LAN Failover Mechanism (Statement C):

Prisma SD-WAN ION devices typically use a VRRP-like mechanism for LAN redundancy.

When the "Active" node fails (loses power), the "Standby" node stops receiving keepalives and promotes itself to the Active state.

To ensure downstream switches and clients immediately send traffic to the new Active unit, it must update their ARP tables. It does this by broadcasting a Gratuitous ARP (GARP) packet for the Virtual IP (VIP) address of the Switch Virtual Interfaces (SVIs). This action informs the network that the MAC address associated with the Gateway I1P is now reachable via the port connected to the new Active ION.234

Question: 7

In a data center (DC) with two ION devices, all of the remote branch Prisma SD-WAN VPNs are active only on DC ION-1.

Why are no VPNs active on DC ION-2?

A. The BGP core peer is down.

B. The static route to core as a next hop is missing.

C. The ION device is behind a NAT.

D. The DC and branches are in a different domain.

Answer: A

Explanation:

Comprehensive and Detailed Explanation

In a Prisma SD-WAN Data Center deployment, the operational state of the Secure Fabric VPNs (overlay tunnels) is directly tied to the health of the BGP Core Peer configuration.4

Core Peer Dependency: DC ION devices typically peer with the data center core switch (Core Router) via BGP to learn the subnets (prefixes) for the applications hosted in the DC. The Prisma SD-WAN controller monitors this BGP peering status.5

Controller Logic: If the BGP Core Peer on a DC ION goes down (or is not established), the controller automatically marks the VPN tunnels terminating at that specific ION as "Inactive".6 This is a fail-safe mechanism designed to prevent remote branches from sending traffic to a DC ION that has lost conne7ctivity to the internal data center network (and thus the applications).

Scenario Analysis: In this scenario, DC ION-1 has active VPNs, meaning its BGP Core Peer is UP and it is successfully advertising reachability. DC ION-2 has no active VPNs, which strongly indicates that its BGP Core Peer is down.8 Because the controller sees the peer is down, it suppresses the tunnel establishment or marks existing tunnels as inactive to ensure traffic is only directed to the healthy node (ION-1).

Question: 8

Which statement is valid when integrating Prisma SD-WAN with Prisma Access remote networks?

A. Security policies for remote networks are configured in Prisma Access and pushed to Prisma SD- WAN for enforcement on the branch ION devices.

B. Easy onboarding automatically recommends the closest preconfigured remote network security processing nodes and can be overridden manually.

C. A branch with multiple internet circuits will automatically connect to Prisma Access on each circuit and will be used in an active/standby manner for internet-bound traffic.

D. Bandwidth must be allocated to each Prisma Access remote network compute location, and this bandwidth is shared between all branches that terminate on this remote network node.

Answer: D

Explanation:

Comprehensive and Detailed Explanation

When deploying Prisma Access for Remote Networks (connecting branch offices), the licensing and throughput model is based on aggregate bandwidth allocated to specific compute locations (regions).

Bandwidth Allocation (Option D): Administrators must purchase and allocate a specific amount of bandwidth (e.g., 500 Mbps, 1 Gbps) to a Prisma Access "Compute Location" (e.g., US West, Europe Central). This allocated bandwidth is then shared as a pool among all the branch sites (Remote Networks) that onboard and terminate their IPSec tunnels at that specific location. The system does not allocate bandwidth on a strict per-site basis but rather enforces the limit on the aggregate throughput of the compute node itself.

Policy Enforcement (Option A): Security policies for Prisma Access are enforced in the cloud (at the Prisma Access Service Processing Node), not pushed down to the branch ION devices for local enforcement. The ION device handles local segmentation (ZBFW) and traffic steering, but the "Remote Network" security stack resides in the cloud.

Path Usage (Option C): Prisma SD-WAN is designed to utilize Active/Active paths. When a branch has multiple internet circuits connected to Prisma Access, the CloudBlade and ION automatically build tunnels on all compatible paths and can load-balance traffic across them based on application performance (SLA), rather than defaulting to a strict Active/Standby model for internet traffic.

Question: 9

What are two potential causes when a secondary public circuit has been added to the branch site, but the Prisma SD-WAN tunnel is not forming to the data center? (Choose two.)

A. Interface role is not selected as “internet.”

B. Circuit label is missing from interface type.

C. DNS is not configured.

D. Interface scope is set to “local.”

Answer: A, D

Explanation:

Comprehensive and Detailed Explanation

In Prisma SD-WAN (formerly CloudGenix), the establishment of Secure Fabric (VPN) tunnels is automated but relies heavily on the correct definition of the Network Context for each interface. If a tunnel fails to form on a newly added s2econdary circuit, it is typically due to a misconfiguration in how the interface is defined in the ION portal.

1. Interface Scope (Statement D):

The Scope setting on an interface determines its function in the network topology.

GIobal Scope: This defines the interface as a WAN-facing port. The ION device will only attempt to build VPN tunnels (overlay) on interfaces configured with Global scope.

Local Scope: This defines the interface as a LAN-facing port (for users, switches, or APs). If the administrator mistakenly sets the scope to "Local" for the new internet line, the ION treats it as a private LAN segment and will not initiate any tunnel negotiation or WAN signaling on that port.

2. Interface Role/Circuit Category (Statement A):

Prisma SD-WAN uses Circuit Categories (often referred to as Interface Roles in general networking terms, or specifically "Circuit Category" in the ION UI) to determine peering logic.

To form a tunnel over a public internet link to a Data Center, the circuit attached to the interface must be categorized as "Internet".

The controller uses this category to match compatible endpoints. It knows that a "Private WAN" (MPLS) link cannot directly tunnel to an "Internet" link without a gateway. If the new circuit is not correctly selected/categorized as "Internet" (e.g., left undefined or set to a different category), the system will not attempt to build the standard IPSec overlay to the Data Center's public IP address.

Question: 10

What is the number and structure of Prisma SD-WAN QoS queues supported per WAN interface?

A. 12 queues

4 classes1

3 application criteria within each class

B. 16 queues

4 classes

4 application criteria with each class

C. 8 queues

1 priority queue

7 non-priority queues

D. 8 queues

A. classes

B. application criteria within each class

Answer: B

Explanation:

Comprehensive and Detailed Explanation

The Prisma SD-WAN (ION) QoS engine utilizes a hierarchical queuing structure designed to provide granular control over application performance. Each WAN interface on an ION device supports a total of 16 QoS queues.

This 16-queue structure is derived from a matrix of 4 Classes (often referred to as Priority Classes) multiplied by 4 Application Criteria (Traffic Types).2

C. Priority Classes: The system defines four high-level business priority categories:3

Platinum (Highest priority)4

Gold

Silver

Bronze (Lowest priority/Best Effort)5

D. Application Criteria (Sub-queues): Within each of the four priority classes, the system further categorizes traffic into four specific application types to ensure proper handling (e.g., ensuring voice doesn't get stuck behind bulk data

even within the same priority level):6

Real-Time Video

Real-Time Audio

Transactional

Bulk7

Calculation: 4 Priority Classes × 4 Application Types = 16 Total Queues per interface. This structure allows the scheduler to ensure that a "Platinum" voice call is prioritized over "Platinum" bulk data, and both are prioritized over "Gold" traffic.

Question: 11

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. 1

B. 3

C. 5

D. 7

Answer: B

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.

Question: 12

A multinational company is deploying Prisma SD-WAN across North America, Europe, and Asi

a. The data centers in the North America region have served all regions, but regional policies are now being enforced that mandate each of the regions to build their own data centers and branch sites to

only connect to their respective regional data centers.

How can this regionalization be achieved so that new or existing branch sites only build tunnels to the regional DC IONs?

A. Create a new cluster for each regional DC ION and move the sites from the existing cluster to the new cluster.

B. Disable the auto-tunnel feature globally on the Prisma SD-WAN portal and manually create all necessary tunnels exclusively between IONs within their designated regions.

C. Remove the circuit labels and apply new circuit labels for in-region circuits only.

D. Assign WAN interfaces to distinct Virtual Routing and Forwarding (VRF) instances for each region on the DC IONs, ensuring that branches only connect to the WAN interfaces/VRFs designated for their region.

Answer: A

Explanation:

Comprehensive and Detailed Explanation

To achieve strict regional isolation where branch sites only form VPN tunnels with Data Centers in their specific region

(e.g., EU branches to EU DCs only), the correct architectural feature to utilize is VPN Clusters.

In Prisma SD-WAN (CloudGenix), a Cluster defines a logical security and topology boundary for the overlay network. By default, devices may be placed in a "Default" cluster where they attempt to form a mesh or hub-and-spoke topology with all other reachable devices in that context.

To enforce the new policy:

Logical Partitioning: The administrator should create separate VPN Clusters for each region (e.g., "Cluster-NA", "Cluster-EU", "Cluster-Asia").

Assignment: The Regional Data Center IONs and their corresponding Branch IONs must be moved into their respective clusters.

Result: The Prisma SD-WAN controller dictates that devices can only establish Secure Fabric (VPN) tunnels with other devices within the same cluster. This effectively segments the global network, ensuring that an Asian branch never attempts to build a tunnel to a North American DC, satisfying the compliance requirement without complex access lists or manual tunnel configuration.

Option B (Manual Tunnels) is administratively unscalable and negates the benefits of SD-WAN automation.

Option C (Circuit Labels) is primarily for path selection and traffic steering, not for hard topology segmentation.

Option D (VRFs) is used for local Layer 3 segmentation (routing isolation) within a device, not for controlling WAN overlay tunnel formation scope.

Question: 13

What are two requirements for implementing user/group-based path policies? (Choose two.)

A. Cloud Identity Engine
B. Internal host detection
C. Autonomous Digital Experience Manager (ADEM)
D. Data center ION

Answer: A, D

Explanation:

Comprehensive and Detailed Explanation

To implement User/Group-based policies (Path, QoS, or Security) in Prisma SD-WAN, the system requires two specific components to resolve user identities and map them to IP addresses within the fabric.

Cloud Identity Engine (CIE): This is the primary requirement for identity management. The Cloud Identity Engine connects the Prisma SD-WAN controller to your directory service (e.g., Active Directory, Azure AD/Entra ID). It allows the system to retrieve and resolve User and Group attributes (e.g., "Marketing Group," "User: john.doe") so they can be selected in policy rules. Without CIE, the controller cannot interpret the group names or user identities defined in the policies.

Data Center ION: In the standard deployment model for User-ID, a Data Center (DC) ION is required to act as the bridge or collector for IP-to-User mappings. The DC ION connects to the User-ID Agent (running on a PAN-OS firewall or Windows Server) to learn the mapping of IP addresses to usernames. It then redistributes this information to the controller or other branch IONs so they can identify which user is associated with the traffic flows originating from a specific private IP address.

Question: 14

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

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

Answer: C

Explanation:

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.

Question: 15

Site templates are to be used for the large-scale deployment of 100 Prisma SD-WAN branch sites across different regions.

Which two statements align with the capabilities and best practices for Prisma SD-WAN site templates? (Choose two.)

A. The use of Jinja conditional statements within a site template is not supported, thereby limiting dynamic customization options.

B. Mandatory variables for any site template include the site name, ION software version, and at least one ION serial number /device name pair.

C. Site templates offer the capability to pre-stage device configurations by creating a device shell.

D. Once a site has been deployed using a template, its configuration can be updated or modified by applying an updated version of the template.

Answer: B, C

Explanation:

Comprehensive and Detailed Explanation

Site Templates (often referred to as Site Configuration Templates) are a critical tool for the Zero Touch Provisioning (ZTP) of large-scale deployments in Prisma SD-WAN.

1. Device Pre-staging (Statement C):

One of the primary capabilities of Site Templates is the creation of Device Shells. A device shell is a configuration container that exists in the controller before the physical hardware is installed or connected. By using a template, an administrator can pre-provision the entire configuration (interfaces, routing, subnets) for the "Site" and "Element" (Device). When the physical ION device is later connected to the internet and claimed (associated with the shell via its Serial Number), it immediately inherits this pre-staged configuration, enabling a true "plug-and-play" deployment.

2. Mandatory Variables (Statement B):

To successfully instantiate a functional site from a generic template, specific unique identifiers are required in the variable data set (typically a CSV file).

Site Name: Identifies the location in the portal.

ION Software Version: Ensures the device boots to the specific validated code version required for the deployment, preventing inconsistencies.

ION Serial Number / Device Name: Required to bind the logical configuration (Shell) to the physical hardware. Even if the serial is added later during the claim process, the structure of the template and the deployment workflow mandates these variables to ensure the device can be uniquely identified and managed within the fabric.

Note on Option D: While it is technically possible to re-deploy a template, the Best Practice for "Day 2" operations (updating or modifying configuration after deployment) is to use Prisma SD-WAN Stacks (Network Stacks, Security Stacks, etc.). Stacks allow for granular, policy-based updates across multiple sites without the destructive or rigid nature of re-applying a full site initialization template. Therefore, D is not the aligned best practice.

Question: 16

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:

Comprehensive and Detailed 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: 17

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:

Comprehensive and Detailed 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: 18

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:

Comprehensive and Detailed 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: 19

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:

Comprehensive and Detailed 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: 20

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 ofline to trigger the dynamic failover.

D. The "Standard VPN" path policy must be selected.

Answer: A

Explanation:

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 ofloads 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: 21

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:

Comprehensive and Detailed 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: 22

A network engineer is troubleshooting an ION device that is showing as "Ofline" 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:

Comprehensive and Detailed 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 regionspecific 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 ofline in the portal.

Question: 23

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:

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.

Question: 24

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:

Comprehensive and Detailed 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: 25

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.

Question: 26

An administrator is configuring a High Availability (HA) pair of ION 3000 devices at a Data Center.

Which statement accurately describes the requirement for the HA Control Interface connection between the two devices?

A. The HA Control interface must be connected via a Layer 3 routed network to ensure reachability across different subnets.

B. The HA Control interface must be a direct physical connection or a Layer 2 adjacent connection on a dedicated VLAN, with no routing between them.

C. The HA Control connection is optional if both devices are managed by the same Cloud Controller.

D. The HA Control interface uses the management port and must be connected to the internet.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

In a Prisma SD-WAN High Availability (HA) deployment, the HA Control Interface is the critical lifeline used to synchronize state, heartbeats, and flow information between the Active and Standby ION devices.

The strict requirement for this connection is that it must be Layer 2 adjacent.

Best Practice: A direct physical cable connection between the designated HA ports of the two devices (e.g., Port 2 on Device A to Port 2 on Device B).

Alternative: Connectivity through a switch on a dedicated, isolated VLAN is supported, provided the devices are in the same broadcast domain and subnet.

Routing (Layer 3) is not supported for the HA Control link because the keepalive mechanism relies on low-latency, multicast/broadcast-level adjacency to detect failures instantly (sub-second failover). If the HA link were routed (Option A), network latency or router convergence issues could cause "SplitBrain" scenarios where both devices assume the Active role, leading to IP conflicts and traffic loops. Option C is incorrect because the Controller is too slow to manage real-time failover; the decision must be local.

Question: 27

A network administrator is viewing the Flow Browser to investigate a report that a specific user cannot access an internal web server. The flow entry for this traffic shows the "Flow State" as "INIT" and it remains in that state until it times out.

What does the "INIT" state indicate about the traffic flow?

A. The TCP 3-way handshake was completed successfully, and data is being transferred.

B. The ION device received the SYN packet from the client but never saw a SYN-ACK response from the server.

C. The flow was denied by a Zone-Based Firewall policy on the ION.

D. The traffic is being buffered while the ION waits for a dynamic VPN tunnel to establish.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

In the Prisma SD-WAN Flow Browser, the Flow State provides a real-time snapshot of the TCP/UDP session lifecycle.

INIT (Initialization): This state indicates that the ION device has seen the initial packet of a new session (typically a TCP SYN) originating from the client (Source), but it has not yet seen a return packet (such as a TCP SYN-ACK) from the destination server.

Diagnosis: A flow stuck in INIT is a classic indicator of a "Blackhole" or reachability issue downstream. It implies that the ION successfully routed the packet out toward the destination, but the destination did not reply. Common causes include:

The server is ofline.

A firewall in the path (or on the server itself) is dropping the traffic.

Routing is broken on the return path (asymmetric routing where the return traffic bypasses the ION).

If the flow had been denied by the ION's own firewall (Option C), the state would typically show as DENY or REJECT. If the handshake completed (Option A), the state would be ESTABLISHED. Therefore, INIT points to a lack of response from the remote end.

Question: 28

When integrating Prisma SD-WAN with Prisma Access, what is the specific role of the Service Connection (SC)?

A. It connects the Prisma Access cloud infrastructure back to the customer's Headquarters or Data Center for access

to internal private resources (e.g., AD, DNS, Intranet).

B. It is the IPSec tunnel that connects a Branch site to the Prisma Access gateway for internet access.

C. It is the SSL VPN portal used by mobile users to connect to the network.

D. It is the peering link between different Prisma Access regions to optimize global traffic.

Answer: A

Explanation:

Comprehensive and Detailed Explanation

In the Prisma Access architecture (integrated with SD-WAN), distinct connection types serve different purposes.

Remote Networks: These are the connections from your Branch sites (using ION devices) into the cloud. They allow branches to get to the internet or other branches.

Service Connections (SC): This is a specialized high-bandwidth connection used to bridge the Prisma Access Cloud to your Private Data Center or Headquarters.

The primary use case for a Service Connection (Option A) is to allow mobile users and branch users (who are connected to the Prisma cloud) to reach private, centralized resources that still reside onpremise, such as Active Directory controllers, legacy databases, or mainframes. Without a Service Connection, users in the cloud would be able to reach the internet and each other, but not the servers physically located in your HQ data center. The CloudBlade automates the creation of these tunnels, but architecturally, the "Service Connection" is the "cloud-to-HQ" bridge.

Question: 29

An administrator wants to configure a Path Policy that routes all "Guest Wi-Fi" traffic directly to the internet using the local broadband interface, bypassing all VPN tunnels.

Which Service & DC Group setting should be selected in the policy rule to achieve this "Direct Internet Access" (DIA) behavior?

A. Standard VPN

B. Direct

C. Any-Private

D. Default-Cluster

Answer: B

Explanation:

Comprehensive and Detailed Explanation

In Prisma SD-WAN Path Policies, the Service & DC Group (Destination) field determines where the traffic is sent.

Direct: This is the specific keyword/object used to instruct the ION to route traffic directly out to the local WAN interface (Local Breakout) towards the Internet, without encapsulation in a VPN tunnel. This is the correct setting for Guest Wi-Fi, SaaS applications (like Office 365), or any public web browsing that does not need to be backhauled.

Standard VPN / Default-Cluster: These options direct traffic into an IPSec overlay tunnel destined for a Data Center or another ION. Selecting these would "backhaul" the guest traffic, which contradicts the requirement for DIA.

When "Direct" is selected, the ION uses its available "Internet" category links. The policy can further specify which internet link to use (e.g., "Use Broadband, avoid LTE") via the path preference list, but the Destination type must be "Direct".

Question: 30

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.

Question: 31

An administrator needs to ensure that critical VoIP traffic is not dropped even when the branch's primary internet link is fully saturated with bulk file transfers.

Which QoS mechanism does Prisma SD-WAN automatically apply to the "Platinum" priority class to prevent starvation by lower-priority classes?

A. Strict Priority Queuing (SPQ)

B. Weighted Round Robin (WRR)

C. Hierarchical Token Bucket (HTB) with guaranteed bandwidth

D. First-In, First-Out (FIFO)

Answer: C

Explanation:

Comprehensive and Detailed Explanation

Prisma SD-WAN utilizes a hierarchical QoS model (typically based on Hierarchical Token Bucket or similar shaping algorithms) to manage bandwidth contention.

Guaranteed Bandwidth: The "Platinum" class (used for Real-Time voice/video) is assigned a guaranteed bandwidth percentage (floor) in the QoS profile. This ensures that even if "Gold" (Transactional) or "Silver" (Bulk) traffic is trying to consume 100% of the link, the scheduler reserves the specific portion (e.g., 30%) for Platinum traffic, preventing starvation.

Shaping, not Policing: Unlike simple policing which drops excess traffic hard, the ION device shapes the egress traffic. If the link is congested, the scheduler delays the lower-priority packets (buffering) to allow the high-priority Platinum packets to exit immediately.

Why not Strict Priority (A)? While Platinum behaves like a priority queue, pure Strict Priority can completely starve lower queues if the high-priority traffic is misbehaving or voluminous. Prisma SD- WAN typically uses bandwidth guarantees (floors) and limits (ceilings) to ensure fair sharing while protecting critical apps.

Question: 32

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.

Question: 33

Which component of the Prisma SD-WAN solution is responsible for the deep application identification (App-ID) and the generation of flow metrics (Network Transfer Time, Server Response Time) at the branch?

A. The CloudBlade container

B. The Prisma SD-WAN Controller

C. The ION Device Data Plane

D. The API Gateway

Answer: C

Explanation:

Comprehensive and Detailed Explanation

The ION Device Data Plane (the software running locally on the hardware appliance at the branch) is the component responsible for the heavy lifting of traffic analysis.

Edge Processing: Prisma SD-WAN uses an "Application-Defined" architecture. The ION device performs Deep Packet Inspection (DPI) on the first few packets of a flow to identify the application (e.g., distinguishing "Skype Video" from "Skype Chat").

Metric Calculation: The ION device timestamping engine calculates the performance metrics (RTT, NTT, SRT) in real-time as packets pass through its interfaces. It aggregates this metadata.

Role of Controller (B): The Controller collects and visualizes this data (Analytics), but it does not generate it. The Controller does not sit in the data path of the user traffic. If the ION relied on the controller for App-ID, latency would be unacceptably high. Therefore, all detection and metric generation happens locally on the ION Device.

Question: 34

An administrator has configured a Zone-Based Firewall (ZBFW) policy on a branch ION. They created a rule to "Allow" traffic from the "Guest" zone to the "Internet" zone. However, users in the "Guest" zone are reporting they cannot reach a specific public website, and the Flow Browser shows the flow state as "REJECT".

What is the most likely reason for this specific rejection, assuming the "Allow" rule is correctly placed at the top of the list?

A. The implicit default action at the bottom of the security policy is "Deny All".

B. The "Allow" rule does not have the specific "Application" defined (it is set to Any), causing a mismatch.

C. There is a "Deny" rule in the "Global" policy stack that is taking precedence over the "Local" site rule.

D. The ION device does not support firewalling for HTTP traffic.

Answer: C

Explanation:

Comprehensive and Detailed Explanation

In Prisma SD-WAN, security policies can be applied via Policy Stacks, which often have a hierarchy.

Stack Precedence: A common configuration involves a Global Security Stack (applied to all sites) and a Local/Site Security Stack (specific to one site). If the administrator configured a "Global" rule that says "Deny Access to Gambling Sites" (or a specific IP list), and that rule is higher in the binding order or part of a higher-priority stack, it will enforce the block before the local "Allow Guest to Internet" rule is processed.

Specifics of "REJECT": The state REJECT specifically implies a policy enforcement action (sending a TCP RST or ICMP Unreachable) rather than a silent drop or a routing failure.

Why not A? If the "Allow" rule is at the top and matches the traffic parameters (Zone/IP), the Default Deny at the bottom would never be reached. The issue implies a higher priority Deny exists.

Question: 35

When using the CloudBlade to integrate Prisma SD-WAN with Prisma Access, how does the system ensure that the IPSec tunnels between the branch ION and the Prisma Access Security Processing Node (SPN) are kept alive during periods of no user traffic?

A. The administrator must configure a continuous ping script on a branch PC.

B. The CloudBlade automatically configures the ION to send Synthetic Probes (ICMP/HTTP) across the tunnel.

C. The IPSec tunnel uses standard DPD (Dead Peer Detection) and the ION sends keepalives.

D. Prisma Access initiates the connection to the branch every 60 seconds.

Answer: C

Explanation:

Comprehensive and Detailed Explanation

The stability of VPN tunnels in the Prisma SD-WAN + Prisma Access integration relies on standard IPSec mechanisms.

Dead Peer Detection (DPD): The CloudBlade configuration automatically enables DPD on the IPSec tunnels it provisions.

Mechanism: DPD is a standard keepalive mechanism where the ION device sends periodic "R-U- THERE" messages to the Prisma Access gateway (and vice versa). If no acknowledgment is received after a specific count/timer, the ION marks the tunnel as down and attempts to re-key or switch to a backup path.

Synthetic Probes (B): While Synthetic Probes (part of ADEM or Path Quality monitoring) can be configured to measure latency/loss, the fundamental mechanism that keeps the IPSec security association (SA) active and detects link failure is DPD, not an application-layer probe.

Question: 36

An ION 3000 device at a remote branch has suffered a critical hardware failure and must be replaced via the RMA process. The administrator has received the replacement unit.

What is the correct procedure to transfer the configuration and license from the defective unit to the replacement unit to ensure minimal downtime and retention of historical data?

A. Manually configure the new device from scratch, then open a support ticket to transfer the license.

B. Use the "Replace Device" workflow in the Prisma SD-WAN portal, which automatically transfers the configuration (Device Shell) and re-associates the site to the new serial number.

C. Backup the configuration of the old device to a USB drive and restore it to the new device using the local console.

D. Delete the old device from the portal, create a new site for the replacement device, and rebuild the policies manually.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

The RMA replacement process in Prisma SD-WAN is designed to be seamless, leveraging the decoupling of logical configuration from physical hardware.

Replace Device Workflow: The administrator should use the "Replace Device" (or RMA) function within the portal. This workflow allows you to select the "Defective" device (old serial) and the "Replacement" device (new serial).

Configuration Transfer: Once executed, the system automatically binds the existing Device Shell (which contains all interface configs, routing policies, and site associations) to the new hardware's serial number. The new device, once connected to the internet, will "call home," identify itself, and download the exact configuration of the previous unit.

License Transfer: While the configuration moves automatically, the Support License transfer typically requires a specific step in the Customer Support Portal (CSP) or happens automatically if processed as a formal RMA order. Options A and D are incorrect because they involve manual reconfiguration, which is unnecessary and error-prone. Option C is incorrect as the ION platform relies on cloudbased config management, not local USB backups for hardware swaps.

Question: 37

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 sends Active Probes (synthetic UDP packets) across the Secure Fabric to measure path quality continuously.

B. It relies solely on Passive Monitoring of TCP retransmissions from other user traffic on that link.

C. It queries the ISP's router via SNMP to retrieve interface error counters.

D. It defaults to a static value of 0% loss until user traffic begins.

Answer: A

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.

Question: 38

In a Data Center deployment, what is the key functional difference between configuring a BGP neighbor as a "Core Peer" versus an "Edge Peer"?

A. A Core Peer is used for LAN-side routing to learn DC prefixes, while an Edge Peer is used for WAN- side routing to the Service Provider.

B. A Core Peer automatically redistributes learned routes into the SD-WAN fabric, whereas an Edge Peer does not.

C. A Core Peer supports eBGP only, while an Edge Peer supports iBGP only.

D. A Core Peer is used for connecting to the internet, while an Edge Peer connects to the MPLS provider.

Answer: A

Explanation:

Comprehensive and Detailed Explanation

In the Prisma SD-WAN Data Center (DC) model, the terminology for BGP peers defines their role in the topology and how the system generates route maps.

Core Peer: This peer type is designated for the LAN-side connection (facing the DC Core Switch or internal Routers). Its primary purpose is to learn the subnets/prefixes hosted in the data center so the ION can advertise them to the remote branches. The system automatically creates route maps to facilitate this redistribution into the fabric.

Edge Peer: This peer type is designated for the WAN-side connection (facing the Edge Router or MPLS PE). Its primary

purpose is to provide reachability to the underlay network.

Distinction: Selecting the correct type affects the default Route Maps and Prefix Lists generated by the controller. Configuring a Core Peer correctly ensures that the DC's internal subnets are properly learned and propagated to the overlay, whereas an Edge Peer configuration focuses on WAN nexthop reachability.

Question: 39

What is the default behavior of the Zone-Based Firewall (ZBFW) for traffic originating from the ION device itself (e.g., DNS queries, NTP sync, or Controller connectivity) destined for the "Internet" zone?

A. It is denied by the default "Deny All" rule unless explicitly allowed.

B. It is allowed by the implicit "Self-Zone" allow rule.

C. It is allowed only if the "Management" interface is used.

D. It is inspected by the "Global" security stack but bypasses local rules.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

The Self-Zone is a predefined security zone in the Prisma SD-WAN ZBFW that represents the ION device's own control plane and management traffic.

Default Rule: The security policy contains an implicit, uneditable default rule that Allows traffic originating from the Self-Zone to any destination zone (Internet, Private WAN, etc.).

Rationale: This ensures that the device can always perform essential critical functions—such as connecting to the Cloud Controller, resolving DNS, syncing time via NTP, and establishing VPN tunnels—without the administrator needing to manually create "Allow" rules for the device itself. If this traffic were blocked by a "Deny All" default, the device would become unmanageable (bricked) immediately after applying the policy.

Question: 40

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.

Question: 41

In the Prisma SD-WAN portal, an administrator is viewing the "Media" analytics for a branch site to troubleshoot complaints about poor voice quality.

When calculating the Mean Opinion Score (MOS) for voice traffic, which two metrics does the system prioritize active monitoring for, even when no user voice traffic is present on the link? (Choose two.)

A. Latency (One-Way)

B. Jitter

C. Throughput

D. Packet Loss

Answer: B, D

Explanation:

Comprehensive and Detailed Explanation

Prisma SD-WAN calculates the Mean Opinion Score (MOS) to provide a standardized metric (1-5) for voice quality. To ensure the system always knows the "voice readiness" of a path—even before a call starts—it uses Active Probes (synthetic UDP packets).

While latency is measured, the MOS calculation algorithm is most heavily penalized by Packet Loss (D) and Jitter (B).

Packet Loss: Even a small amount of loss (e.g., >1%) dramatically reduces voice clarity, causing dropouts.

Jitter: High variance in packet arrival time (jitter) causes the "robotic" voice effect and buffer underruns.

The system continuously measures these specific metrics on all WAN links using synthetic probes. If the packet loss or jitter exceeds the threshold defined in the "Path Quality Profile" (e.g., Voice Profile), the path is marked as non-compliant, and the MOS score drops, triggering a policy action to move the flow. Throughput (C) is less critical for voice as calls consume very little bandwidth (e.g., 64-100 Kbps), making congestion (loss/jitter) the primary enemy, not raw speed.

Question: 42

A customer wants to deploy Prisma SD-WAN ION devices at small home offices that use consumergrade broadband routers. These routers typically use Symmetric NAT and do not allow static port forwarding.

Which standard mechanism does Prisma SD-WAN utilize to successfully establish direct Branch-to- Branch (Dynamic) VPN tunnels through these Symmetric NAT devices?

A. UPnP (Universal Plug and Play)

B. STUN (Session Traversal Utilities for NAT)

C. Manual GRE Tunnels

D. SSL VPN encapsulation

Answer: B

Explanation:

Comprehensive and Detailed Explanation

Prisma SD-WAN utilizes STUN (Session Traversal Utilities for NAT) to facilitate NAT Traversal for its Secure Fabric overlay.

Discovery: When an ION device connects to the internet behind a NAT router, it reaches out to the Prisma SD-WAN Controller. The controller acts as a STUN server, identifying the public IP address and port that the ION's traffic is originating from.

Symmetric NAT Challenge: In Symmetric NAT, the mapping changes for every destination. However, the Prisma SD-WAN architecture is designed to handle this by having the controller coordinate the connection attempt.

Hole Punching: The controller shares the discovered public mapping information between two peer ION devices. They then simultaneously initiate traffic to each other's public IP/Port (a technique called "UDP Hole Punching"). This tricks the intermediate NAT devices into allowing the inbound traffic, establishing a direct P2P IPSec tunnel without requiring manual port forwarding or static IPs at the edge.

Question: 43

An administrator is configuring an ION 2000 device for a deployment where high availability is required, but the site has only a single internet circuit. The administrator configures a Bypass Pair (Fail-to-Wire) on ports 1 and 2 connecting the ISP modem to the legacy firewall.

If the ION device loses power, what is the resulting behavior of the traffic flowing through this Bypass Pair?

A. Traffic is blocked to prevent uninspected packets from entering the network (Fail-to-Block).

B. The internal relay closes, physically bridging Port 1 and Port 2, allowing traffic to flow transparently between the modem and firewall.

C. The device reboots into "Safe Mode" and acts as a Layer 2 switch.

D. Traffic is rerouted to the LTE modem automatically.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

The Bypass Pair feature on Prisma SD-WAN ION devices (specifically supported models like ION 2000, 3000, 7000, 9000) is a hardware-based resiliency mechanism known as Fail-to-Wire.

Operation: A "Bypass Pair" logically groups two physical interfaces (e.g., WAN 1 and LAN 1). Under normal operation, the ION processes traffic between them.

Power Loss: In the event of a total power loss (or critical software failure), a mechanical relay inside the device physically closes the circuit between the two ports.

Result: This creates a direct electrical connection (like a patch cable) between the upstream device (ISP Modem) and the downstream device (Legacy Firewall or Router). This ensures that internet connectivity is preserved for the site, even if the SD-WAN appliance is completely dead. This is critical for single-point-of-failure deployments where maintaining basic dial-tone is more important than SD-WAN optimization during a hardware outage.

Question: 44

An organization has created a custom internal application definition for "Inventory_App" on the Prisma SD-WAN controller based on its destination IP address and port (L3/L4 rule). The application server IP has just changed.

After updating the custom application definition on the controller, how is this change propagated to the branch ION devices?

A. The administrator must manually "Push" the policy to all sites.

B. The administrator must reboot the ION devices for the new object to load.

C. The controller automatically pushes the updated Application Definition (App-Def) to all ION devices immediately.

D. The change will only take effect after the daily "App-ID" scheduled update.

Answer: C

Explanation:

Comprehensive and Detailed Explanation

In Prisma SD-WAN, Custom Applications are global policy objects managed centrally on the controller.

Immediate Propagation: When an administrator creates or modifies a Custom Application definition (e.g., updating the IP subnet or port for an internal app), the Prisma SD-WAN controller automatically pushes this update to all connected ION devices in the tenant.

No Manual Push: Unlike some legacy firewall management paradigms (like Panorama "Commit and Push"), the Prisma SD-WAN architecture is "intent-based" and continuously synchronized. A change to a global object like an App Definition is considered a live configuration change and is distributed immediately via the secure control channel.

No Reboot: The ION data plane updates its classification engine dynamically without interrupting traffic or requiring a reboot. This ensures that policy enforcement (steering "Inventory_App" to the correct path) remains accurate in real-time.

Question: 45

When allocating Aggregate Bandwidth for a Prisma Access "Remote Network" deployment (connecting 50 branch sites), how is the bandwidth license enforced?

A. Each branch site is hard-capped at the specific bandwidth limit defined in its individual IPSec tunnel configuration.

B. The bandwidth is shared as a pool across all sites in a specific Compute Location (Region); individual sites can burst up to the available pool capacity.

C. The bandwidth is allocated per device serial number and cannot be shared.

D. The bandwidth license is only checked once during the initial onboarding; there is no ongoing enforcement.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

Prisma Access manages Remote Network bandwidth using an Aggregate Bandwidth licensing model.

Compute Locations: When you purchase bandwidth (e.g., 1 Gbps), you allocate it to specific Prisma Access Compute Locations (e.g., US West, Europe Central).

Shared Pool: All branch sites (Remote Networks) that connect to that specific Compute Location share the allocated bandwidth pool. For example, if you allocate 500 Mbps to "US West" and connect 10 branches to it, they compete for that 500 Mbps aggregate.

Bursting: An individual branch is not strictly rate-limited to a "slice" (e.g., 50 Mbps) unless you explicitly configure QoS guarantees. By default, a single branch can burst and consume a large portion of the aggregate pool if other branches are idle. The enforcement happens at the Region/Compute Node level, ensuring the total throughput does not exceed the licensed capacity for that region.

Question: 46

A network installer is attempting to claim a new ION device using the "Claim Code" method. The device is connected to the internet, but the status in the portal remains stuck at "Claimed" and does not transition to "Online". The installer connects a laptop to the LAN port of the ION and can successfully browse the internet, confirming the uplink is active.

What is the most likely cause of the device failing to reach the "Online" state?

A. The device is missing the "Site" assignment in the portal.

B. The upstream firewall is blocking outbound TCP port 443 or UDP port 123 (NTP).

C. The device has not yet downloaded the latest software image.

D. The "Circuit Label" has not been applied to the WAN interface.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

The transition from "Claimed" to "Online" depends entirely on the ION device's ability to establish a secure, persistent management tunnel to the Prisma SD-WAN Controller.

Connectivity Requirements: The ION device initiates an outbound connection to the controller on TCP Port 443 (HTTPS). It also requires accurate time synchronization to validate SSL certificates, necessitating access to NTP (UDP Port 123).

Scenario Analysis: Since the installer can browse the internet from the LAN, we know the physical link and basic routing/NAT are functional. The issue is specific to the management plane traffic.

Root Cause: If an upstream firewall (e.g., a corporate edge firewall or ISP filter) is inspecting SSL traffic or blocking specific FQDNs/Ports required by the ION, the device cannot complete the handshake. Consequently, it remains "Claimed" (registered in the database) but cannot go "Online"

(active management session). Options A, C, and D prevent provisioning (configuration push) but generally do not prevent the device from initially checking in and going "Online" if the pipe is open.

Question: 47

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.

Question: 48

When defining a Path Quality Profile (SLA) for a "Transactional" application group (e.g., Citrix, Oracle), the administrator sets the "Packet Loss" threshold to 1%.

What happens to the traffic for this application if all active paths currently exceed this 1% loss threshold?

A. The traffic is dropped to prevent data corruption.

B. The system selects the best available path (lowest loss) among the active paths, even if it violates the profile.

C. The traffic is queued indefinitely until a path recovers.

D. The system automatically enables a Backup path, even if the Active paths are technically "Up" but degraded.

Answer: B

Explanation:

Comprehensive and Detailed Explanation

This behavior describes the "Best Available Path" logic inherent in Prisma SD-WAN's availability design.

SLA Thresholds: Path Quality Profiles act as filters to identify compliant paths.

Total Violation: If all configured "Active" paths violate the SLA (e.g., Path A has 2% loss, Path B has 5% loss, and the threshold is 1%), the system does not drop the traffic (Option A) because maintaining connectivity is prioritized over perfect quality.

Selection Logic: The system enters a fallback state where it compares the available active paths and selects the "Least Bad" one—the path that is closest to meeting the SLA (in this case, Path A with 2% loss).

Backup Paths: Traffic would only move to a Backup path (Option D) if the policy explicitly configures the backup path to engage upon SLA violation of the active set. However, strictly speaking, if only active paths are considered and all fail, it picks the best of the active group rather than blackholing the traffic.

Question: 49

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.

Question: 50

A network engineer is troubleshooting a "Voice Quality" issue. They suspect that the DSCP markings are being stripped or altered by the ISP.

Which tool in the Prisma SD-WAN portal allows the engineer to capture live packets on the WAN interface and inspect the IP header ToS/DSCP field?

A. Flow Browser

B. Packet Capture (PCAP)

C. Path Quality Monitor

D. Event Logs

Answer: B

Explanation:

Comprehensive and Detailed Explanation

To validate specific packet-level details like DSCP (Differentiated Services Code Point) values, header checksums, or exact payload sizes, a Packet Capture (PCAP) is required.

PCAP Tool: Prisma SD-WAN provides a built-in PCAP utility accessible directly from the portal. The engineer can select the specific Interface (e.g., Internet 1), apply a Filter (e.g., port 5060 or host 1.2.3.4), and capture the traffic.

Analysis: The resulting .pcap file can be downloaded and opened in Wireshark. This allows the engineer to definitively see if the packets leaving the ION have DSCP EF (46) and if the packets arriving (if capturing on the other side) still retain that marking, or if the ISP has bleached it to CS0 (0).

Flow Browser (A): While it shows "Application" and metrics, the Flow Browser typically displays the assigned priority class, not necessarily the raw bit-level DSCP value present in the packet header on the wire.

Question: 51

A network administrator notices that a branch ION device is experiencing high CPU utilization due to a suspected TCP SYN Flood attack originating from a compromised host on the local LAN.

Which specific security feature should be configured and applied to the "LAN" zone to mitigate this Denial of Service (DoS) attack?

A. Zone-Based Firewall (ZBFW) Rule with a "Deny" action

B. Zone Protection Profile

C. Application Quality Profile (AQP)

D. Access Control List (ACL) on the WAN interface

Answer: B

Explanation:

Comprehensive and Detailed Explanation

To defend against volumetric attacks such as TCP SYN Floods, UDP Floods, or ICMP Floods, Prisma SD- WAN (like PAN-OS) utilizes Zone Protection Profiles.

Function: A Zone Protection Profile is a specific security object designed to screen traffic for protocol anomalies and flood behaviors before it is processed by the complex firewall policy engine. It sets thresholds (e.g., "Max 1000 SYNs/sec"). If the traffic rate exceeds this threshold, the system triggers an action (Alarm, Drop, or SYN Cookies) to protect the device's resources.

Application: Unlike a standard ZBFW Rule (A) which filters based on Source/Destination/App-ID (which might still allow the initial handshake packets that cause the flood), a Zone Protection Profile is applied to the Zone object itself (in this case, the LAN Zone). This ensures that the flood is mitigated at the ingress stage, preventing the ION's session table and CPU from being exhausted by the attack.

Question: 52

In the Prisma SD-WAN portal, the Application Health dashboard assigns a color-coded "Health Score" (Green, Yellow, Red) to applications.

Which three metrics are combined to calculate this composite AppX (Application Experience) score? (Choose three.)

A. Transaction Failure Rate

B. Network Transfer Time (NTT)

C. Server Response Time (SRT)

D. Bandwidth Utilization

E. Jitter

Answer: A, B, C

Explanation:

Comprehensive and Detailed Explanation

The AppX (Application Experience) score is a proprietary metric used by Prisma SD-WAN to provide a holistic view of user experience, rather than just network statistics. It is calculated based on three key components:

Transaction Failure Rate (A): The percentage of application transactions that failed (e.g., TCP resets, HTTP 500 errors). This indicates availability.

Network Transfer Time (B): The time taken for packets to traverse the network (WAN/LAN latency). This indicates network health.

Server Response Time (C): The time taken by the application server to respond to a request. This indicates backend performance.

Why not D or E?

Bandwidth Utilization (D) is a capacity metric, not a direct measure of quality. A link can be 90% full but still deliver packets quickly (good AppX), or 10% full but dropping packets (bad AppX).

Jitter (E) is a network-layer metric primarily relevant for UDP Real-Time media. While important, the high-level "AppX" score for general TCP apps focuses on the "Time-to-Glass" metrics (NTT/SRT) and success rates.

Question: 53

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

A. 1

B. 8

C. 24

D. 72

Answer: C

Explanation:

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 (InstantOn 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.

Question: 54

A network engineer is able to ping and traceroute from SD-WAN branch IP 192.168.1.123 to servers in primary data center – DC1, but is unable to ping or traceroute to a server 10.2.2.22 in the newly configured secondary data center, DC2.

The DC2 ION device is advertising the branch IP subnet 192.168.1.0/24 to the DC2 core via eBGP Core Peer. The DC2 data center site has site prefix 10.2.2.0/23 configured.

Which configuration will resolve the issue in this scenario?

A. The default 0.0.0.0/0 static route to the DC2 ION pointing to the DC2 next hop.

B. Reconfigure eBGP Core Peer to iBGP Core Peer.

C. Reconfigure eBGP Core Peer as Edge Peer type.

D. Remove site prefix 10.2.2.0/23 from DC2 site configuration.

Answer: A

Explanation:

Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:

In a Prisma SD-WAN deployment, the routing of traffic between branches and Data Centers (DCs) relies on the proper synchronization between the AppFabric (the overlay) and the local routing protocols (the underlay/LAN side). In this scenario, the branch can successfully reach DC1, indicating the branch ION is correctly participating in the fabric. However, traffic to DC2 (10.2.2.22) is failing.

The DC2 site has the site prefix 10.2.2.0/23 configured. In Prisma SD-WAN, defining a site prefix informs the Controller that this specific subnet "belongs" to that site, causing the Controller to advertise reachability for this prefix to all other ION devices in the fabric. Consequently, when the branch ION (192.168.1.123) attempts to reach 10.2.2.22, it correctly identifies DC2 as the destination and encapsulates the traffic toward the DC2 ION.

The bottleneck occurs once the packet arrives at the DC2 ION. While the ION is advertising the branch subnet (192.168.1.0/24) to the DC Core (ensuring the return path), the ION itself must know how to forward the incoming traffic from the branch to the internal DC network. If the DC2 ION does not have a specific route in its local routing table for the 10.2.2.0/23 subnet pointing to the DC Core's internal interface, the packet will be dropped.

According to Palo Alto Networks best practices for Data Center ION deployment, a static default route (0.0.0.0/0) should be configured on the ION device pointing toward the DC Core's next-hop IP address. This ensures that any traffic received from the AppFabric destined for internal DC resources—which are not directly connected to the ION—is successfully handed off to the core switching fabric for final delivery. Adding this default route (Option A) resolves the reachability issue by providing the "last-hop" routing instruction within the DC.

Question: 55

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:

(SNR Graph showing Carrier-1 in blue dropping to near 0 dB and Carrier-2 in green staying relatively stable between 4.5 dB and 6.5 dB)

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 theWAN path may have experienced some performance degradation.

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

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

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

Answer: A, D

Explanation:

Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:

In Prisma SD-WAN, the Signal-to-Noise Ratio (SNR) is a critical metric used to monitor the health and performance of cellular WAN interfaces. SNR measures the strength of the desired signal relative to the background noise level; higher values indicate a cleaner signal, while lower values suggest that

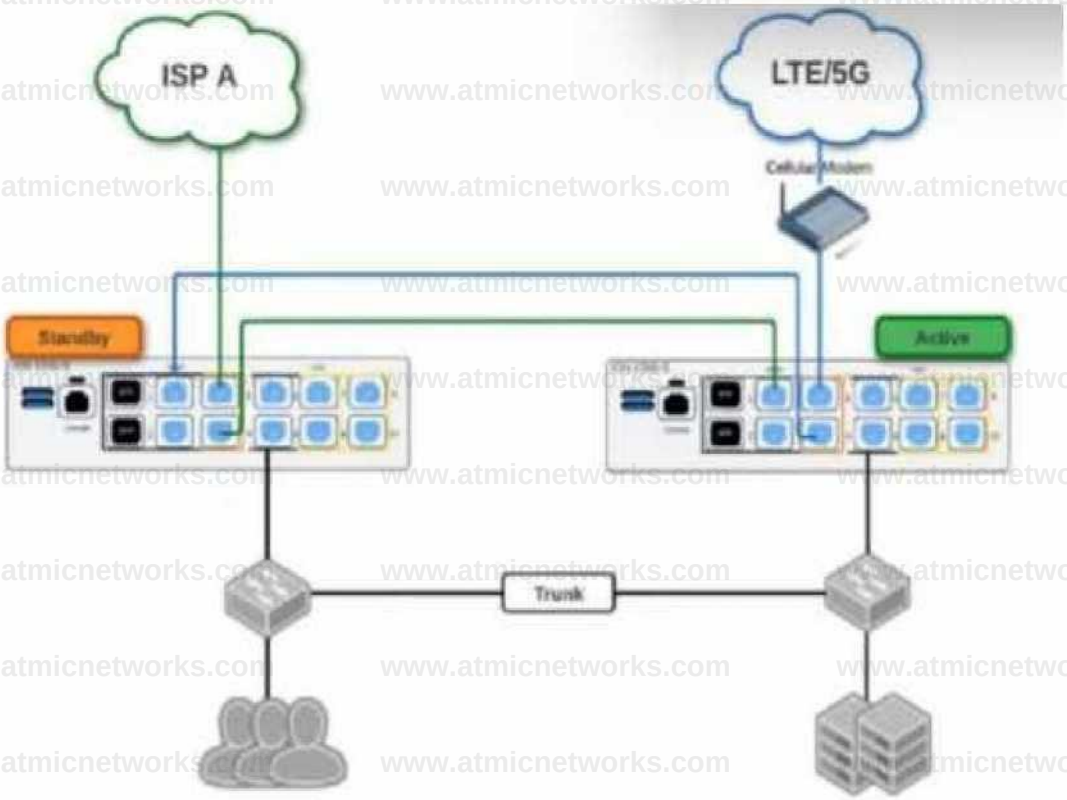
noise is overwhelming the signal, typically leading to increased packet loss, high latency, and reduced throughput.

Analyzing the provided graph, Carrier-1 (blue line) shows a severe drop in SNR, plummeting from approximately 4.5 dB to nearly 0.3 dB between 15:00 and 23:00. An SNR value this low is indicative of a failing or highly unstable link that cannot reliably sustain data traffic, directly supporting Inference A—that Carrier-1 experienced significant performance degradation. In contrast, Carrier-2 (green line) maintains a much higher and more consistent SNR throughout the same period.

Prisma SD-WAN's AppFabric uses application-based path selection and SLA monitoring to ensure the best possible user experience. When the system detects that a primary path (like Carrier-1) has degraded below acceptable thresholds—often triggered by high loss or latency resulting from poor signal quality—it will dynamically steer application flows to an alternative healthy path. Therefore, Inference D is correct: because Carrier-1's quality became untenable while Carrier-2 remained stable, the ION device would have likely initiated a path switchover to move traffic from the degraded Carrier-1 to the healthier Carrier-2.

Question: 56

Based on the HA topology image below, which two statements describe the end-state when power is removed from the ION 1200-S labeled "Active", assuming that the ION labeled "Standby" becomes the active ION? (Choose two.)



A. Both the connection to ISP A and the connection to LTE/5G will be usable.

B. The VRRP Virtual IP address assigned to any SVIs will be moved to the newly active ION.

C. The newly active ION will send a gratuitous ARP to the LAN for the IP address of any SVIs.

D. The connection to ISP A will be usable, but the connection to LTE/5G will not.

Answer: A, C

Explanation:

Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:

Prisma SD-WAN High Availability (HA) for branch ION devices, particularly the Gen-2 ION 1200-S, is designed to provide "100% WAN Capacity" preservation during a hardware or power failure. This is achieved through the use of Bypass Pairs (Fail-to-Wire). In the provided topology, the ISP A and LTE/5G circuits are cross-connected using the bypass ports (typically ports 3 and 4 on the ION 1200-

S).

When the "Active" ION device loses power, the internal physical relays in its bypass ports transition to a closed state, effectively creating a physical bridge between the ports. In this scenario, the LTE/5G signal—which enters the Active ION's port 4—is mechanically bridged to port 3, allowing it to pass through to port 4 of the Standby ION. Simultaneously, ISP A is already connected to the Standby ION. Consequently, once the Standby device completes its transition to the "Active" state, it has physical access to both WAN circuits, validating Statement A.

Regarding the LAN transition, Prisma SD-WAN does not use standard VRRP for ION-to-ION HA; instead, it uses a proprietary Control Plane HA mechanism. When the failover occurs, the newly active ION takes over the IP addresses of all configured Switch Virtual Interfaces (SVIs) and LAN interfaces. To ensure the downstream Layer 2 infrastructure (like the LAN switches shown in the diagram) updates its MAC address tables to point to the new physical hardware for those IPs, the newly active ION immediately broadcasts a Gratuitous ARP (GARP). This ensures that LAN traffic is correctly steered to the new device without a significant timeout, validating Statement C.

Question: 57

An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The application will be able to make any approved changes directly to devices via API.

What is a requirement for the application to create SD-WAN interfaces?

A. REST API's "sdwanInterfaceprofiles" parameter on a Panorama device

B. REST API's "sdwanInterfaces" parameter on a firewall device

C. XML API's "sdwanprofiles/interfaces" parameter on a Panorama device

D. XML API's "InterfaceProfiles/sdwan" parameter on a firewall device

Answer: B

Explanation:

Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer

documents:

In Palo Alto Networks PAN-OS SD-WAN environments, automation and orchestration are key components for service providers managing large-scale deployments. The PAN-OS REST API provides a modern, structured way to programmatically manage configuration objects, including those required for SD-WAN functionality.

When an application is designed to push changes directly to devices (individual firewalls) rather than through a centralized template in Panorama, it must interact with the firewall's local REST API. To successfully create a virtual SD-WAN interface, the application must target the correct resource URI. In the PAN-OS API schema, the logical SD-WAN interface—which groups physical links to enable application-based path selection—is managed via the sdwanInterfaces parameter within the REST API.

It is important to distinguish between the interface itself and the profiles that support it. Option A refers to sdwanInterfaceprofiles, which are the objects used to define the characteristics of a link (such as bandwidth, link type, and monitoring frequency), but not the interface itself. Furthermore, since the scenario specifies making changes "directly to devices," the target must be the firewall rather than Panorama. While Panorama can manage these objects via templates, a direct-to-device automation workflow necessitates using the firewall's REST API endpoint. Utilizing the REST API over the legacy XML API is the recommended standard for modern integrations due to its ease of use with JSON payloads and alignment with contemporary DevSecOps practices. By using the sdwanInterfaces parameter on the firewall, the MSP application can programmatically bind physical Layer 3 interfaces to the SD-WAN fabric.