[2026-January-NewBraindump2go SD-WAN-Engineer VCE Free Download[Q1-Q20

2026/January Latest Braindump2go SD-WAN-Engineer Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go SD-WAN-Engineer Real Exam Questions!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. LLDPB. CDPC. SNMPD. SyslogAnswer: 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 PrismaAccess 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 IONB. User-1 accessing a private application within Branch-1, and source User-ID based zone-based firewall rules on Branch-1 IONC. User-1 accessing a private application in data center via SD-WAN overlay, and destination User-ID based zone-based firewall rules on DC IOND. 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 IONAnswer: A, B Explanation:Comprehensive and Detailed ExplanationIn 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 thedestination. 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 backupB. Circuit B as an active, Circuit A as a backupC. Both circuits under active pathD. Circuit B as an L3 failure path Answer: C Explanation:Comprehensive and Detailed ExplanationIn 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).1D. Raise an alarm.Answer: B Explanation:Comprehensive and Detailed ExplanationAccording 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 BehaviorQuestion: 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 ExplanationThis 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.234Question: 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 ExplanationIn 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.4Core 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.5Controller 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 ExplanationWhen 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 ExplanationIn 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.Global 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 classes13 application criteria within each classB. 16 queues 4 classes 4 application criteria with each classC. 8 queues 1 priority queue 7 non-priority queuesD. 8 queues 2 classes 4 application criteria within each classAnswer: B Explanation:Comprehensive and Detailed ExplanationThe 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).24 Priority Classes: The system defines four high-level business priority categories:3 Platinum (Highest priority)4Gold SilverBronze (Lowest priority/Best Effort)54 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):6Real-Time Video Real-Time Audio Transactional Bulk7Calculation: 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. 1B. 3C. 5D. 7Answer: B Explanation:Comprehensive and Detailed ExplanationThe 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.2However, 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).4If 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 Asia.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 toonly 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 ExplanationTo 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 EngineB. Internal host detectionC. Autonomous Digital Experience Manager (ADEM)D. Data center IONAnswer: A, D Explanation:Comprehensive and Detailed ExplanationTo 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, POVB. Production, Control, DisabledC. Disabled, Analytics, ControlD. POV, Production, AnalyticsAnswer: C Explanation:Comprehensive and Detailed ExplanationPrisma 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 enforcesPath 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 ExplanationSite 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. OnlineB. ClaimedC. ProvisionedD. ActiveAnswer: B Explanation:Comprehensive and Detailed ExplanationIn 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: 17An 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 ExplanationPrisma 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 ExplanationThe 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 interventionQuestion: 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 ExplanationThe 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 offline to trigger the dynamic failover.D. The "Standard VPN" path policy must be selected.Answer: A Explanation:Comprehensive and Detailed ExplanationDynamic VPNs (also known as ION-to-ION or Branch-to-Branch VPNs) allow Prisma SD-WAN devices to establish direct, on-demand secure tunnels between branch sites to optimize latency for peer-to-peer traffic (e.g., VoIP calls between offices).To enable this capability, the primary architectural requirement is the configuration of VPN Clusters.A VPN Cluster defines a logical group of devices that are authorized to communicate with one another.By default, or if devices are in different clusters without peering, the topology typically defaults to Hub-and-Spoke, where branches only talk to the Data Center.When two branch ION devices are placed into the same VPN Cluster (or peered clusters), the controller shares the necessary reachability and cryptographic information between them.Once in the same cluster, the ION devices monitor traffic. If a user at Branch A tries to contact a server at Branch B, the ION devices detect this interest. If a direct path is available (e.g., via public internet), they will dynamically negotiate a direct VPN tunnel, bypassing the Data Center hub. This offloads the hub and reduces latency. Option B is incorrect because SD-WAN eliminates manual GRE config. Option C is incorrect because dynamic VPNs are a performance feature, not just a disaster recovery feature.Resources From:1.2026 Latest Braindump2go SD-WAN-Engineer Exam Dumps (PDF & VCE) Free Share:**https://www.braindump2go.com/sd-wan-engineer.html**2.2026 Latest Braindump2go SD-WAN-Engineer PDF and SD-WAN-Engineer VCE Dumps Free Share:
https://drive.google.com/drive/folders/1NSNlefZUgKV9GNfEVa0zNYr9fXbSZfgc?usp=sharing3.2026 Free Braindump2go SD-WAN-Engineer Exam Questions Download:
https://www.braindump2go.com/free-online-pdf/SD-WAN-Engineer-PDF-Dumps(1-20).pdf Free Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!