KillTest

質量更高　服務更好



練習題

https://www.killtest.net

一年免費更新服務

Exam : **SD-WAN-Engineer**

Title : Palo Alto Networks SD-WAN Engineer

Version : DEMO

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.

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.

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.

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.

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