PaloAltoNetworks.SD-WAN-Engineer.v2026-02-19.q28

Exam Code:	SD-WAN-Engineer
Exam Name:	Palo Alto Networks SD-WAN Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	28
Version:	v2026-02-19
# of views:	108
# of Questions views:	280
https://www.freepdfdumps.com/PaloAltoNetworks.SD-WAN-Engineer.v2026-02-19.q28.html	

NEW QUESTION: 1
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 SSL VPN portal used by mobile users to connect to the network.
C. It is the IPSec tunnel that connects a Branch site to the Prisma Access gateway for internet access.
D. It is the peering link between different Prisma Access regions to optimize global traffic.
Answer: (SHOW ANSWER)
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 on-premise, 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.

NEW QUESTION: 2

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 (LEAVE A REPLY)
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.

NEW QUESTION: 3
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 (LEAVE A REPLY)
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 offline.
* 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.

NEW QUESTION: 4
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 (LEAVE A REPLY)
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.

NEW QUESTION: 5
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 (LEAVE A REPLY)
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.

NEW QUESTION: 6
For how many hours are Prisma SD-WAN VPN shared secrets valid?
A. 1
B. 8
C. 24
D. 72
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:
In the Prisma SD-WAN architecture, security is built directly into the AppFabric using a centralized, controller-led approach to key management. Unlike traditional VPNs that rely

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

NEW QUESTION: 7
A customer wants to deploy Prisma SD-WAN ION devices at small home offices that use consumer-grade 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: (SHOW ANSWER)
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.

NEW QUESTION: 8
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: (SHOW ANSWER)
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.

NEW QUESTION: 9
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: (SHOW ANSWER)
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.

NEW QUESTION: 10
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 (LEAVE A REPLY)
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.

NEW QUESTION: 11
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: (SHOW ANSWER)
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.

NEW QUESTION: 12
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: (SHOW ANSWER)
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.

NEW QUESTION: 13

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: (SHOW ANSWER)
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).

NEW QUESTION: 14
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 (LEAVE A REPLY)
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.

NEW QUESTION: 15
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 (LEAVE A REPLY)
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.

NEW QUESTION: 16
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 (LEAVE A REPLY)
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".

NEW QUESTION: 17
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 (LEAVE A REPLY)
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.

NEW QUESTION: 18
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 (LEAVE A REPLY)
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.

NEW QUESTION: 19
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 (LEAVE A REPLY)
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.

NEW QUESTION: 20

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 (LEAVE A REPLY)
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.

NEW QUESTION: 21
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: (SHOW ANSWER)
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.

NEW QUESTION: 22
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 (LEAVE A REPLY)
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.

NEW QUESTION: 23
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: (SHOW ANSWER)
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.

NEW QUESTION: 24
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 (LEAVE A REPLY)
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 next-hop reachability.

NEW QUESTION: 25
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 (LEAVE A REPLY)
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.

NEW 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 (LEAVE A REPLY)
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 "Split-Brain" 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.

NEW QUESTION: 27
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. Event Logs
B. Flow Browser
C. Packet Capture (PCAP)
D. Path Quality Monitor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
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 (LEAVE A REPLY)
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.

dumps, the Actual4test.com SD-WAN-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SD-WAN-Engineer dumps with Test Engine here: https://www.actual4test.com/SD-WAN-Engineer_examcollection.html (**88** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)