PaloAltoNetworks.SD-WAN-Engineer.v2026-03-25.q46

Exam Code:	SD-WAN-Engineer
Exam Name:	Palo Alto Networks SD-WAN Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	46
Version:	v2026-03-25
# of views:	126
# of Questions views:	460
https://www.dumpsdb.com/dumps/Palo-Alto-Networks/SD-WAN-Engineer/PaloAltoNetworks.SD-WAN-Engineer.v2026-03-25.q46	

NEW QUESTION: 1
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: 2
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 (LEAVE A REPLY)
Comprehensive and Detailed Explanation
The Flow Browser and App Response Time metrics in Prisma SD-WAN are critical tools for isolating the fault domain-determining whether a problem lies in the "Network" or the "Application."
* Network Transfer Time (NTT) / Round Trip Time (RTT): These metrics measure the time it takes for packets to traverse the network (WAN/LAN) and for acknowledgments to return. A low NTT (e.g.,
<50ms) confirms that the network pipes (SD-WAN overlay, Underlay circuits) are healthy and transporting packets quickly.
* Server Response Time (SRT): This metric specifically measures the time between the server receiving a request and the server sending the first byte of the response. It essentially measures the "processing time" of the backend server.
In the scenario described, the network metrics (NTT/RTT) are excellent, effectively ruling out WAN congestion, packet loss, or latency (Option A and C). However, the Server Response Time (SRT) is very high (500ms). This signature is a definitive indicator that the network delivered the request instantly, but the application server took a long time to process it. This points the troubleshooting effort toward the server infrastructure (e.g., a slow SQL query, an overloaded web server, or lack of compute resources) rather than the SD-WAN environment.

NEW QUESTION: 3
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: 4

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: 5

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

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

A. Transaction Failure Rate

B. Network Transfer Time (NTT)

C. Server Response Time (SRT)

D. Bandwidth Utilization

E. Jitter

Answer: A,B,C (LEAVE A REPLY)

Comprehensive and Detailed Explanation

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

Transaction Failure Rate (A): The percentage of application transactions that failed (e.g., TCP resets, HTTP 500 errors). This indicates availability.
Network Transfer Time (B): The time taken for packets to traverse the network (WAN/LAN latency). This indicates network health.
Server Response Time (C): The time taken by the application server to respond to a request. This indicates backend performance.
Why not D or E?
Bandwidth Utilization (D) is a capacity metric, not a direct measure of quality. A link can be 90% full but still deliver packets quickly (good AppX), or 10% full but dropping packets (bad AppX).
Jitter (E) is a network-layer metric primarily relevant for UDP Real-Time media. While important, the high-level "AppX" score for general TCP apps focuses on the "Time-to-Glass" metrics (NTT/SRT) and success rates.

NEW QUESTION: 6
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: (SHOW ANSWER)
Comprehensive and Detailed Explanation
Site Templates (often referred to as Site Configuration Templates) are a critical tool for the Zero Touch Provisioning (ZTP) of large-scale deployments in Prisma SD-WAN.
1. Device Pre-staging (Statement C):
One of the primary capabilities of Site Templates is the creation of Device Shells. A device shell is a configuration container that exists in the controller before the physical hardware is installed or connected. By using a template, an administrator can pre-provision the entire configuration (interfaces, routing, subnets) for the "Site" and "Element" (Device). When the physical ION device is later connected to the internet and claimed (associated with the shell via its Serial Number), it immediately inherits this pre-staged configuration, enabling a true "plug-and-play" deployment.
2. Mandatory Variables (Statement B):

To successfully instantiate a functional site from a generic template, specific unique identifiers are required in the variable data set (typically a CSV file).
Site Name: Identifies the location in the portal.
ION Software Version: Ensures the device boots to the specific validated code version required for the deployment, preventing inconsistencies.
ION Serial Number / Device Name: Required to bind the logical configuration (Shell) to the physical hardware. Even if the serial is added later during the claim process, the structure of the template and the deployment workflow mandates these variables to ensure the device can be uniquely identified and managed within the fabric.
Note on Option D: While it is technically possible to re-deploy a template, the Best Practice for "Day 2" operations (updating or modifying configuration after deployment) is to use Prisma SD-WAN Stacks (Network Stacks, Security Stacks, etc.). Stacks allow for granular, policy-based updates across multiple sites without the destructive or rigid nature of re-applying a full site initialization template. Therefore, D is not the aligned best practice.

NEW QUESTION: 7
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 that appears first in the interface configuration list.
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 with the lowest numerical latency (e.g., if ISP-A drops to 39ms).
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.

NEW QUESTION: 8
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: (SHOW ANSWER)
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: 9
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 (LEAVE A REPLY)
Comprehensive and Detailed Explanation

Dynamic VPNs (also known as ION-to-ION or Branch-to-Branch VPNs) allow Prisma SD-WAN devices to establish direct, on-demand secure tunnels between branch sites to optimize latency for peer-to-peer traffic (e.
g., VoIP calls between offices).
To enable this capability, the primary architectural requirement is the configuration of VPN Clusters.
A VPN Cluster defines a logical group of devices that are authorized to communicate with one another.
* By default, or if devices are in different clusters without peering, the topology typically defaults to Hub- and-Spoke, where branches only talk to the Data Center.
* When two branch ION devices are placed into the same VPN Cluster (or peered clusters), the controller shares the necessary reachability and cryptographic information between them.
Once in the same cluster, the ION devices monitor traffic. If a user at Branch A tries to contact a server at Branch B, the ION devices detect this interest. If a direct path is available (e.g., via public internet), they will dynamically negotiate a direct VPN tunnel, bypassing the Data Center hub. This 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.

NEW QUESTION: 10
Which troubleshooting action should be taken when resources at one branch site can reach the internet but cannot be reached from the data center (DC)?
A. Create static route with DC ION as a next hop.
B. Ensure the LAN branch prefixes are set to "global."
C. Set the site in a control mode.
D. Admin up the Prisma SD-WAN DC endpoints.
Answer: B (LEAVE A REPLY)
In the Prisma SD-WAN architecture, reachability between sites is managed by the Control Plane, which automatically advertises prefixes across the secure fabric based on their scope. If a branch site has successful Direct Internet Access (DIA) but is invisible to the Data Center (DC), it indicates that while the local ION is online, its internal network information has not been propagated to the rest of the SD-WAN fabric.
The most common cause for this behavior is that the LAN interfaces or static routes at the branch are configured with a Local scope rather than a Global scope. When a prefix is set to "Local," the ION device treats that network as reachable only within that specific site; it will not advertise that prefix to the Controller for distribution to other ION devices, such as those at the Data Center. By ensuring the LAN branch prefixes are set to "global" (Option B), the administrator instructs the ION device to share these routes with the global fabric. Once the prefix is marked as global, the Prisma SD-WAN Controller identifies it as a reachable destination and updates the routing tables of all peer ION devices in the same

domain, including the DC gateways. This allows the Data Center to build a valid path to the branch resources over the secure VPN tunnels. Options like creating static routes (Option A) or changing site modes (Option C) do not address the fundamental requirement of prefix advertisement within the software-defined fabric, which relies on correctly defined metadata like route scope.

NEW QUESTION: 11
An administrator has configured a Zone-Based Firewall (ZBFW) policy on a branch ION. They created a rule to "Allow" traffic from the "Guest" zone to the "Internet" zone. However, users in the "Guest" zone are reporting they cannot reach a specific public website, and the Flow Browser shows the flow state as "REJECT".
What is the most likely reason for this specific rejection, assuming the "Allow" rule is correctly placed at the top of the list?
A. The implicit default action at the bottom of the security policy is "Deny All".
B. The "Allow" rule does not have the specific "Application" defined (it is set to Any), causing a mismatch.
C. There is a "Deny" rule in the "Global" policy stack that is taking precedence over the "Local" site rule.
D. The ION device does not support firewalling for HTTP traffic.
Answer: C (LEAVE A REPLY)
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: 12
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: 13
When an ION device has been claimed, the cloud-based controller generates and communicates with the device by which method?
A. Manufacturer Installed Certificate (MIC)
B. Existing customer public key infrastructure (KPI)
C. Self-signed certificate
D. Customer Installed Certificate (CIC)
Answer: A (LEAVE A REPLY)
In the Prisma SD-WAN (formerly CloudGenix) architecture, the security and authenticity of device-to- controller communication are paramount. When a new ION (Instant-On Network) device is powered on and connected to the internet, it initiates a secure "phone home" process to the Prisma SD-WAN Cloud Controller.
To ensure that the controller is communicating with a genuine Palo Alto Networks hardware or software instance, the system utilizes a Manufacturer Installed Certificate (MIC).
The MIC is a unique digital certificate burned into the hardware's Trusted Platform Module (TPM) or secure storage during the manufacturing process. This certificate acts as the device's foundational identity. When a customer "claims" a device in the Prisma SD-WAN portal using its serial number, the controller maps that serial number to the specific MIC associated with that unit.
Once the device is claimed and attempts to connect, a mutual TLS (mTLS) handshake occurs. The ION device presents its MIC to the controller to prove its identity, and the controller validates this against its records. This method eliminates the need for manual

staging, pre-configuration, or the complexity of managing a Customer Installed Certificate (CIC) or a private Public Key Infrastructure (PKI) during the initial deployment phase. By leveraging the MIC, Prisma SD-WAN achieves true Zero Touch Provisioning (ZTP), ensuring that only authorized, authentic devices can join the fabric and receive configuration policies, thereby maintaining a secure and automated onboarding workflow.

NEW QUESTION: 14
Return traffic for an application from the branch is being dropped on the branch ION. Application traffic arrives via SD-WAN internet overlay at the branch, and path policy for the application at the branch has the following settings:
Active = MPLS Overlay
Backup = Prisma Access on internet
Which branch configuration is the probable cause of this behavior?
A. It has Prisma Access tunnel over MPLS circuit but not on the internet circuit.
B. It has one MPLS and one internet circuit.
C. It has two internet circuits and no MPLS circuit.
D. It has no MPLS circuit, and the Prisma Access tunnel is down.
Answer: C (LEAVE A REPLY)
In Prisma SD-WAN, path selection and traffic symmetry are governed by the Path Policy and the available physical/virtual circuits at a site. The scenario describes a situation where return traffic is dropped on the branch ION after arriving via an Internet overlay. To understand why, we must analyze the "Active" and
"Backup" paths defined in the policy.
The policy specifies Active = MPLS Overlay and Backup = Prisma Access on internet. In a healthy environment, the ION device expects to send and receive traffic based on these defined paths. If the site actually has two internet circuits and no MPLS circuit (Option C), a critical mismatch occurs. Because there is no MPLS circuit available to satisfy the "Active" path, the device will fall back to the "Backup" path for initiated traffic.
However, the core issue here relates to how Prisma SD-WAN handles asymmetric routing and session state.
If traffic arrives at the branch via an "Internet Overlay" path that is not explicitly defined or allowed as a valid path for that specific application in the Path Policy, the ION device's flow integrity checks may drop the packets. Specifically, if the ION is configured with only Internet circuits but the policy is looking for an MPLS overlay that doesn't exist, the device may fail to correctly associate the return packets with the session state if the paths are perceived as "unbound" or "invalid" per the policy. This behavior is a security feature designed to ensure that traffic only traverses paths that meet the administrator's defined performance and security criteria. Without an MPLS circuit present, the policy cannot be fully realized, leading to potential drops for traffic arriving on paths not intended for that specific application flow.

NEW QUESTION: 15
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.

NEW QUESTION: 16
Which component of the Prisma SD-WAN solution is responsible for the deep application identification (App-ID) and the generation of flow metrics (Network Transfer Time, Server Response Time) at the branch?
A. The CloudBlade container
B. The Prisma SD-WAN Controller
C. The ION Device Data Plane
D. The API Gateway
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation

The ION Device Data Plane (the software running locally on the hardware appliance at the branch) is the component responsible for the heavy lifting of traffic analysis.
Edge Processing: Prisma SD-WAN uses an "Application-Defined" architecture. The ION device performs Deep Packet Inspection (DPI) on the first few packets of a flow to identify the application (e.g., distinguishing "Skype Video" from "Skype Chat").
Metric Calculation: The ION device timestamping engine calculates the performance metrics (RTT, NTT, SRT) in real-time as packets pass through its interfaces. It aggregates this metadata.
Role of Controller (B): The Controller collects and visualizes this data (Analytics), but it does not generate it. The Controller does not sit in the data path of the user traffic. If the ION relied on the controller for App-ID, latency would be unacceptably high. Therefore, all detection and metric generation happens locally on the ION Device.

NEW QUESTION: 17
During the Zero Touch Provisioning (ZTP) process of a new ION device at a branch site, which interface ports are supported by default to request an IP address via DHCP and reach the Prisma SD-WAN controller for claiming?
A. Only the dedicated Controller port (if available)
B. Any LAN or WAN port on the device
C. The dedicated Controller port, or Port 1 / Internet 1 if a dedicated port is absent
D. Only the USB port via a cellular modem
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
For a successful Zero Touch Provisioning (ZTP) experience, the ION device must be able to obtain an IP address and reach the internet immediately upon boot-up.
According to Palo Alto Networks hardware guides, the Controller Port (often labeled specifically as "CONTROLLER" on models like the ION 3000/7000/9000) is pre-configured to act as a DHCP client by default. It is the preferred interface for the initial "call home" process.
However, for smaller desktop models (like the ION 1000/2000/1200 series) or scenarios where a dedicated management network is not available, the device firmware is also

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

NEW QUESTION: 18
In the Prisma SD-WAN portal, the Application Health dashboard assigns a color-coded "Health Score" (Green, Yellow, Red) to applications.
Which three metrics are combined to calculate this composite AppX (Application Experience) score? (Choose three.)
A. Transaction Failure Rate
B. Network Transfer Time (NTT)
C. Server Response Time (SRT)
D. Bandwidth Utilization
E. Jitter
Answer: A,B,C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
The AppX (Application Experience) score is a proprietary metric used by Prisma SD-WAN to provide a holistic view of user experience, rather than just network statistics. It is calculated based on three key components:
* Transaction Failure Rate (A): The percentage of application transactions that failed (e.g., TCP resets, HTTP 500 errors). This indicates availability.
* Network Transfer Time (B): The time taken for packets to traverse the network (WAN/LAN latency).
This indicates network health.
* Server Response Time (C): The time taken by the application server to respond to a request. This indicates backend performance.
Why not D or E?
* Bandwidth Utilization (D) is a capacity metric, not a direct measure of quality. A link can be 90% full but still deliver packets quickly (good AppX), or 10% full but dropping packets (bad AppX).
* Jitter (E) is a network-layer metric primarily relevant for UDP Real-Time media. While important, the high-level "AppX" score for general TCP apps focuses on the "Time-to-Glass" metrics (NTT/SRT) and success rates.

NEW QUESTION: 19
By default, how many days will Prisma SD-WAN VPNs stay operational before the keys expire when an ION device loses connection with the controller?

A. 1
B. 3
C. 5
D. 7
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation
The Prisma SD-WAN (CloudGenix) solution is designed with a separation of the control plane (Controller) and the data plane (ION devices).1 In the event that an ION device loses connectivity to the Cloud Controller (often referred to as running in "headless mode"), the device continues to forward traffic and maintain existing VPN tunnels using the keys it currently holds.2 However, for security purposes, the VPN session keys (shared secrets) used for the Secure Fabric have a finite validity period. The system is designed such that these keys are rotated regularly.3 If the controller is unreachable, the ION device can continue to rotate keys locally and maintain the VPNs for a maximum default period of 72 hours (exactly 3 days).4 If the connection to the controller is not restored within this 72-hour window, the keys will eventually expire, and the ION will be unable to retrieve new authorized key material from the controller.5 Consequently, the VPN tunnels will go down, and the "out of shared secret key" error will be observed in the VPN status logs. This mechanism ensures that a permanently compromised or stolen device cannot maintain network access indefinitely without central authorization.

NEW QUESTION: 20
What are two requirements for implementing user/group-based path policies? (Choose two.)
A. Cloud Identity Engine
B. Internal host detection
C. Autonomous Digital Experience Manager (ADEM)
D. Data center ION
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
To implement User/Group-based policies (Path, QoS, or Security) in Prisma SD-WAN, the system requires two specific components to resolve user identities and map them to IP addresses within the fabric.
* Cloud Identity Engine (CIE): This is the primary requirement for identity management. The Cloud Identity Engine connects the Prisma SD-WAN controller to your directory service (e.g., Active Directory, Azure AD/Entra ID). It allows the system to retrieve and resolve User and Group attributes (e.g., "Marketing Group," "User: john.doe") so they can be selected in policy rules. Without CIE, the controller cannot interpret the group names or user identities defined in the policies.
* Data Center ION: In the standard deployment model for User-ID, a Data Center (DC) ION is required to act as the bridge or collector for IP-to-User mappings. The DC ION connects

to the User-ID Agent (running on a PAN-OS firewall or Windows Server) to learn the mapping of IP addresses to usernames. It then redistributes this information to the controller or other branch IONs so they can identify which user is associated with the traffic flows originating from a specific private IP address.

NEW QUESTION: 21
During the Zero Touch Provisioning (ZTP) process of a new ION device at a branch site, which interface ports are supported by default to request an IP address via DHCP and reach the Prisma SD-WAN controller for claiming?
A. Only the dedicated Controller port (if available)
B. Any LAN or WAN port on the device
C. The dedicated Controller port, or Port 1 / Internet 1 if a dedicated port is absent
D. Only the USB port via a cellular modem
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
For a successful Zero Touch Provisioning (ZTP) experience, the ION device must be able to obtain an IP address and reach the internet immediately upon boot-up.
According to Palo Alto Networks hardware guides, the Controller Port (often labeled specifically as
"CONTROLLER" on models like the ION 3000/7000/9000) is pre-configured to act as a DHCP client by default. It is the preferred interface for the initial "call home" process.
However, for smaller desktop models (like the ION 1000/2000/1200 series) or scenarios where a dedicated management network is not available, the device firmware is also configured to attempt DHCP client requests on Port 1 (often labeled as Internet 1 or simply 1).
Connecting the ISP circuit to any random port (like Port 4 or a LAN port) will not work for ZTP because those interfaces are not pre-configured as DHCP clients in the factory default state. Therefore, the installer must ensure the internet uplink is connected to either the dedicated Controller port or Port 1/Internet 1 to ensure the device can resolve the controller FQDN and download its configuration.

NEW QUESTION: 22
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 (LEAVE A REPLY)
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: 23
By default, how many days will Prisma SD-WAN VPNs stay operational before the keys expire when an ION device loses connection with the controller?
A. 1
B. 3
C. 5
D. 7
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
The Prisma SD-WAN (CloudGenix) solution is designed with a separation of the control plane (Controller) and the data plane (ION devices).1 In the event that an ION device loses connectivity to the Cloud Controller (often referred to as running in "headless mode"), the device continues to forward traffic and maintain existing VPN tunnels using the keys it currently holds.2 However, for security purposes, the VPN session keys (shared secrets) used for the Secure Fabric have a finite validity period. The system is designed such that these keys are rotated regularly.3 If the controller is unreachable, the ION device can continue to rotate keys locally and maintain the VPNs for a maximum default period of 72 hours (exactly 3 days).4 If the connection to the controller is not restored within this 72-hour window, the keys will eventually expire, and the ION will be unable to retrieve new authorized key material from the controller.5 Consequently, the VPN tunnels will go down, and the "out of shared secret key" error will be observed in the VPN status logs.
This mechanism ensures that a permanently compromised or stolen device cannot maintain network access indefinitely without central authorization.

NEW QUESTION: 24

An ION 3000 device at a remote branch has suffered a critical hardware failure and must be replaced via the RMA process. The administrator has received the replacement unit. What is the correct procedure to transfer the configuration and license from the defective unit to the replacement unit to ensure minimal downtime and retention of historical data?
A. Manually configure the new device from scratch, then open a support ticket to transfer the license.
B. Use the "Replace Device" workflow in the Prisma SD-WAN portal, which automatically transfers the configuration (Device Shell) and re-associates the site to the new serial number.
C. Backup the configuration of the old device to a USB drive and restore it to the new device using the local console.
D. Delete the old device from the portal, create a new site for the replacement device, and rebuild the policies manually.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation
The RMA replacement process in Prisma SD-WAN is designed to be seamless, leveraging the decoupling of logical configuration from physical hardware.
* Replace Device Workflow: The administrator should use the "Replace Device" (or RMA) function within the portal. This workflow allows you to select the "Defective" device (old serial) and the
"Replacement" device (new serial).
* Configuration Transfer: Once executed, the system automatically binds the existing Device Shell (which contains all interface configs, routing policies, and site associations) to the new hardware's serial number. The new device, once connected to the internet, will "call home," identify itself, and download the exact configuration of the previous unit.
* License Transfer: While the configuration moves automatically, the Support License transfer typically requires a specific step in the Customer Support Portal (CSP) or happens automatically if processed as a formal RMA order. Options A and D are incorrect because they involve manual reconfiguration, which is unnecessary and error-prone. Option C is incorrect as the ION platform relies on cloud-based config management, not local USB backups for hardware swaps.

NEW QUESTION: 25
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: (SHOW ANSWER)
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: 26
A network installer is attempting to claim a new ION device using the "Claim Code" method. The device is connected to the internet, but the status in the portal remains stuck at "Claimed" and does not transition to "Online". The installer connects a laptop to the LAN port of the ION and can successfully browse the internet, confirming the uplink is active. What is the most likely cause of the device failing to reach the "Online" state?

A. The device is missing the "Site" assignment in the portal.
B. The upstream firewall is blocking outbound TCP port 443 or UDP port 123 (NTP).
C. The device has not yet downloaded the latest software image.
D. The "Circuit Label" has not been applied to the WAN interface.
Answer: B (LEAVE A REPLY)
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: 27
Which troubleshooting step should be taken when users at a branch site are experiencing a maximum throughput of 200 Mbps for Direct Internet Access (DIA) traffic on a 1 Gbps internet connection?
A. Ensure QoS policy is applies to the site.
B. Ensure the WAN interface is set to 1 Gbps or auto mode.
C. Ensure performance policy is applied to the site.
D. Ensure the circuit configuration at the site level is properly set.
Answer: D (LEAVE A REPLY)
In Prisma SD-WAN, the effective throughput for any given circuit is fundamentally dictated by the Circuit Configuration defined at the site level. When a branch experiences a "throughput ceiling" (e.g., traffic capped at 200 Mbps on a 1 Gbps physical link), the most likely cause is that the software-defined bandwidth limit for that circuit has been set incorrectly in the Prisma SD-WAN Controller.
Prisma SD-WAN ION devices do not simply forward traffic at the maximum physical line rate by default; they rely on the administrator-defined Upstream and Downstream bandwidth values to perform traffic shaping, policing, and path selection. If a circuit is physically capable of 1 Gbps but is configured in the portal as having only 200 Mbps, the ION device will enforce this 200 Mbps limit to prevent oversubscribing the link and to

ensure that Quality of Service (QoS) and path selection calculations remain accurate based on the assumed capacity.
To resolve this, an engineer must navigate to the Site Configuration, locate the specific WAN circuit, and verify that the bandwidth settings match the actual service provider's handoff. If these values are set lower than the actual link speed, the device will artificially throttle the traffic. While ensuring the WAN interface is set to the correct speed/duplex (Option B) is a valid physical layer check, and QoS/Performance policies (Options A and C) manage how that bandwidth is used, it is the Circuit Configuration that defines the total available bandwidth for the SD-WAN fabric to utilize. Correcting this configuration allows the ION device to scale its throughput to match the full 1 Gbps capability of the broadband connection.

NEW QUESTION: 28
When configuring a Path Policy rule for a "Real-Time Video" application, the administrator wants to ensure the traffic uses the path with the lowest packet loss.
How does the Prisma SD-WAN ION determine the "Packet Loss" metric for a given path when there is no active user traffic flowing on that link?
A. It sends Active Probes (synthetic UDP packets) across the Secure Fabric to measure path quality continuously.
B. It relies solely on Passive Monitoring of TCP retransmissions from other user traffic on that link.
C. It queries the ISP's router via SNMP to retrieve interface error counters.
D. It defaults to a static value of 0% loss until user traffic begins.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
Prisma SD-WAN utilizes Link Quality Monitoring (LQM) to maintain a real-time health score for every WAN path.
To ensure the system knows the quality of a path before sending critical user traffic onto it, the ION device uses Active Probing.
* Mechanism: The ION sends synthetic probe packets (typically UDP) across the Secure Fabric (VPN tunnels) and Direct Internet paths to its peers. These probes measure Latency, Jitter, and Packet Loss.
* Active vs. Passive: While the system does use Passive Monitoring (observing actual user flows) when traffic is present to reduce overhead, Active Probes are essential for idle links or backup paths. Without active probing, the ION would have no data to make an intelligent steering decision for the first packet of a new video call. This ensures that "Real-Time" policies always have up-to-date metrics to select the best path immediately.

NEW QUESTION: 29
Full discovery and classification of IoT devices by the IoT Security service is failing. Which Prisma SD- WAN ION device configuration will cause this behavior?

A. The ION devices are missing DHCP Configuration. If ION devices are not explicitly configured as either a DHCP relay agent or a DHCP server, DHCP traffic logs will not be sent to the Strata Logging Service, resulting in incomplete device profiles for IoT Security.
B. The Prisma SD-WAN ION devices lack properly configured or enabled Service Health Probes specifically targeting the IoT device subnets. Without these active probes, the system cannot gather critical real-time reachability and performance metrics essential for dynamic device profiling and classification.
C. The Syslog export configuration on the ION devices to the Strata Logging Service has filters that are too restrictive, potentially excluding logs vital for IoT Security's device identification and classification engine. This prevents comprehensive event data, including device discovery messages, from reaching the portal.
D. The ION devices are not configured to explicitly enable and export IPFIX flow records, especially those containing Layer 2 and Layer 7 context, to the Strata Logging Service for IoT Security. While ARP data is sent by default, comprehensive device classification relies on these detailed flow records, which are not being captured.
Answer: A (LEAVE A REPLY)
Palo Alto Networks IoT Security relies on rich metadata and traffic logs to identify, classify, and secure devices across the network. A critical component of this discovery process is the ingestion of DHCP (Dynamic Host Configuration Protocol) traffic. DHCP packets contain vital information about a device, such as the MAC address, vendor-specific identifiers (Option 60), and hostnames, which are used by the machine learning engine to create a precise device profile.
In a Prisma SD-WAN environment, if the ION devices are not involved in the DHCP process, the necessary logs cannot be forwarded to the Strata Logging Service (SLS) for analysis by the IoT Security cloud. To ensure successful discovery, the ION device at the branch must be explicitly configured as either the DHCP Server for the local segment or as a DHCP Relay Agent. When the ION handles DHCP traffic, it automatically extracts and sends the relevant metadata to the cloud.
If the ION is bypassed-for example, if a local Layer 3 switch is handling DHCP internally without relaying it to the ION-the IoT Security service will lack the context needed to move beyond basic IP-level visibility.
Without these DHCP-derived "fingerprints," the system cannot perform the full classification required to apply granular security policies or identify potential vulnerabilities. Therefore, verifying that the ION device is correctly integrated into the DHCP lifecycle is the primary troubleshooting step for incomplete IoT device discovery in the Prisma SD-WAN portal.

NEW QUESTION: 30
A network installer is at a remote branch site to deploy a new ION 3000 device. The device has been racked, cabled to the internet, and powered on. The installer has the "Claim Code" displayed on the email sent by the administrator.

When the administrator enters this Claim Code into the Prisma SD-WAN portal, what is the immediate status of the device before the configuration is fully pushed?

A. Online

B. Claimed

C. Provisioned

D. Active

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation

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

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

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

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

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

NEW QUESTION: 31

When deploying a branch gateway, secure fabric VPN tunnels are automatically established between which two site types? (Choose two.)

A. Branch to branch gateway (same domain)

B. Branch gateway to data center

C. Branch gateway to branch gateway

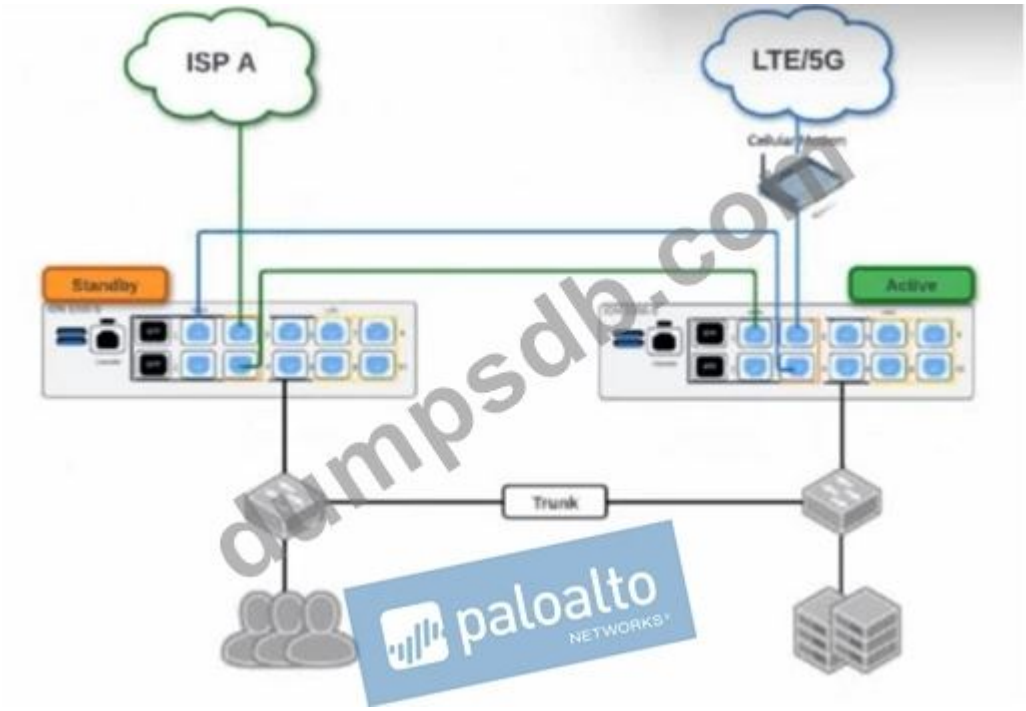
D. Branch to branch gateway (different domain)

Answer: (SHOW ANSWER)

In the Prisma SD-WAN (Instant-On Network) architecture, the "Secure Fabric" is a key feature that simplifies VPN orchestration through automation. When an ION device is deployed at a site and associated with a specific role, the Prisma SD-WAN Controller automatically manages the establishment of encrypted VPN tunnels without requiring manual IPsec configuration.

The most fundamental tunnel type is Branch gateway to data center (Option B). By default, the system follows a hub-and-spoke model where every branch ION device automatically attempts to build secure tunnels to all available Data Center clusters within its domain. This ensures that branch locations have immediate, redundant connectivity to centralized corporate resources and applications as soon as they are brought online.
Additionally, Prisma SD-WAN supports automated Branch gateway to branch gateway connectivity (Option C). Unlike traditional architectures that backhaul all traffic through a central hub, the Prisma SD- WAN fabric can dynamically establish "spoke-to-spoke" tunnels between branch gateways to facilitate direct communication. This is particularly useful for latency-sensitive applications like Voice over IP (VoIP) or video conferencing. While this can be configured as a "full mesh" where all sites build tunnels to all other sites, the controller intelligently manages these connections based on the defined site roles and domain configurations to optimize resource usage and performance. Options A and D are incorrect because the fabric orchestration logic is primarily focused on the functional roles of the gateways (Branch vs. Data Center) rather than "domains" in the context of tunnel initiation.

NEW QUESTION: 32
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 (LEAVE A REPLY)
Comprehensive and Detailed Explanation at least 150 to 250 words each from Palo Alto Networks SD-WAN Engineer documents:
Prisma SD-WAN High Availability (HA) for branch ION devices, particularly the Gen-2 ION 1200-S, is designed to provide "100% WAN Capacity" preservation during a hardware or power failure. This is achieved through the use of Bypass Pairs (Fail-to-Wire). In the provided topology, the ISP A and LTE/5G circuits are cross-connected using the bypass ports (typically ports 3 and 4 on the ION 1200-S).
When the "Active" ION device loses power, the internal physical relays in its bypass ports transition to a closed state, effectively creating a physical bridge between the ports. In this scenario, the LTE/5G signal-which enters the Active ION's port 4-is mechanically bridged to port 3, allowing it to pass through to port 4 of the Standby ION. Simultaneously, ISP A is already connected to the Standby ION. Consequently, once the Standby device completes its transition to the "Active" state, it has physical access to both WAN circuits, validating Statement A.
Regarding the LAN transition, Prisma SD-WAN does not use standard VRRP for ION-to-ION HA; instead, it uses a proprietary Control Plane HA mechanism. When the failover occurs, the newly active ION takes over the IP addresses of all configured Switch Virtual Interfaces (SVIs) and LAN interfaces. To ensure the downstream Layer 2 infrastructure (like the LAN switches shown in the diagram) updates its MAC address tables to point to

the new physical hardware for those IPs, the newly active ION immediately broadcasts a Gratuitous ARP (GARP). This ensures that LAN traffic is correctly steered to the new device without a significant timeout, validating Statement C.

NEW QUESTION: 33
When using the CloudBlade to integrate Prisma SD-WAN with Prisma Access, how does the system ensure that the IPSec tunnels between the branch ION and the Prisma Access Security Processing Node (SPN) are kept alive during periods of no user traffic?
A. The administrator must configure a continuous ping script on a branch PC.
B. The CloudBlade automatically configures the ION to send Synthetic Probes (ICMP/HTTP) across the tunnel.
C. The IPSec tunnel uses standard DPD (Dead Peer Detection) and the ION sends keepalives.
D. Prisma Access initiates the connection to the branch every 60 seconds.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
The stability of VPN tunnels in the Prisma SD-WAN + Prisma Access integration relies on standard IPSec mechanisms.
Dead Peer Detection (DPD): The CloudBlade configuration automatically enables DPD on the IPSec tunnels it provisions.
* Mechanism: DPD is a standard keepalive mechanism where the ION device sends periodic "R-U- THERE" messages to the Prisma Access gateway (and vice versa). If no acknowledgment is received after a specific count/timer, the ION marks the tunnel as down and attempts to re-key or switch to a backup path.
* Synthetic Probes (B): While Synthetic Probes (part of ADEM or Path Quality monitoring) can be configured to measure latency/loss, the fundamental mechanism that keeps the IPSec security association (SA) active and detects link failure is DPD, not an application-layer probe.

NEW QUESTION: 34
While designing a greenfield Prisma SD-WAN solution for a retailer, the risk management group requires segmentation of the retail network to avoid one large fault domain.
The following data points are provided:
* Two data centers and all sites need to access applications in both data centers
* 1000 retail branches with stores concentrated in multiple metropolitan areas
* Data Center 1 and Data Center 2 have different sets of applications that are not replicated
* Maintaining application availability is the primary goal
Which action will segment the retail network and reduce regional outages?
A. Implement a single, large data center cluster spanning both data centers to centralize management and optimize resource use.

B. Create more than one data center cluster for a larger pool of resources and resiliency.
C. Create more than one data center cluster in each data center and assign sites to clusters so nearby retail locations can be spread on separate clusters.
D. Add more data center aggregation devices within the same cluster to enhance the scalability and resilience.
Answer: (SHOW ANSWER)
In large-scale Prisma SD-WAN deployments, such as a retail network with 1,000 branches, architectural resilience is achieved through a strategy known as Hub Clustering. A Data Center Cluster is a logical grouping of ION devices at a hub site that provides termination for branch-to-DC VPN tunnels. To prevent the creation of a massive, single fault domain, Palo Alto Networks best practices recommend segmenting the branch population across multiple clusters.
By creating more than one data center cluster in each data center and strategically assigning sites to these clusters, an administrator can effectively isolate failure events. In a metropolitan area where stores are concentrated, spreading nearby retail locations across different clusters ensures that a localized resource failure or a cluster-specific misconfiguration only impacts a subset of the stores in that region rather than causing a complete regional outage.
This design directly addresses the requirement for maintaining application availability. Since Data Center 1 and Data Center 2 host different applications, each branch site must maintain active paths to both DCs. By using multiple clusters at each DC, the risk management group's goal of avoiding a large fault domain is met through "blast radius" containment. If Cluster A at Data Center 1 fails, the 1,000 sites are not all affected simultaneously; instead, only the specific sites bound to Cluster A lose connectivity to that hub, while their neighbors bound to Cluster B remain functional. This approach provides the highest level of regional resiliency and operational stability for high-density retail environments.

NEW QUESTION: 35
Which component of Prisma SD-WAN is responsible for distributing User-IP and user-group mappings to branch devices that match the corresponding source IPs?
A. DC ION
B. Cloud Identity Engine
C. Controller
D. NGFW
Answer: C (LEAVE A REPLY)
In the Prisma SD-WAN architecture, the Controller serves as the centralized management and control plane for the entire fabric. While the Cloud Identity Engine (CIE) is the component responsible for collecting and consolidating user-to-IP mappings from various identity providers (such as Active Directory, Okta, or Azure AD), it does not directly

manage the distribution of this operational data to the individual ION devices at the branch level.
Instead, the Prisma SD-WAN Controller integrates with the Cloud Identity Engine to ingest these identity mappings. Once the Controller has synchronized the User-IP and user-group information, it acts as the primary orchestrator. It is responsible for distributing these mappings down to the ION devices across all sites. This distribution ensures that when an ION device sees traffic from a specific source IP, it can accurately associate that traffic with a specific user or group based on the metadata provided by the Controller.
By centralizing this distribution through the Controller, Prisma SD-WAN ensures consistency across the network. Branch ION devices can then apply Application-Based Path Selection and security policies based on user identity rather than just IP addresses.
This architectural design offloads the processing requirements of maintaining direct connections to identity providers from the branch hardware, allowing the Controller to handle the heavy lifting of orchestration and global synchronization of identity data.

NEW QUESTION: 36
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: 37
In the Prisma SD-WAN portal, an administrator is viewing the "Media" analytics for a branch site to troubleshoot complaints about poor voice quality.
When calculating the Mean Opinion Score (MOS) for voice traffic, which two metrics does the system prioritize active monitoring for, even when no user voice traffic is present on the link? (Choose two.)
A. Latency (One-Way)
B. Jitter
C. Throughput
D. Packet Loss
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
Prisma SD-WAN calculates the Mean Opinion Score (MOS) to provide a standardized metric (1-5) for voice quality. To ensure the system always knows the "voice readiness" of a path-even before a call starts-it uses Active Probes (synthetic UDP packets).
While latency is measured, the MOS calculation algorithm is most heavily penalized by Packet Loss (D) and Jitter (B).
Packet Loss: Even a small amount of loss (e.g., >1%) dramatically reduces voice clarity, causing dropouts.
Jitter: High variance in packet arrival time (jitter) causes the "robotic" voice effect and buffer underruns.
The system continuously measures these specific metrics on all WAN links using synthetic probes. If the packet loss or jitter exceeds the threshold defined in the "Path Quality Profile" (e.g., Voice Profile), the path is marked as non-compliant, and the MOS score drops, triggering a policy action to move the flow. Throughput (C) is less critical for voice as calls consume very little bandwidth (e.g., 64-100 Kbps), making congestion (loss/jitter) the primary enemy, not raw speed.

NEW QUESTION: 38
When planning a software upgrade for a large fleet of ION devices, what is the recommended best practice regarding the "Software Version" assigned in the Site Summary?
A. Manually log into each device and upload the new image file via USB.
B. Assign the new software version to the "Global" site configuration to upgrade all 1000+ sites simultaneously.
C. Use Site Tags to group sites (e.g., "Pilot", "Region-1", "Region-2") and assign the new software version incrementally to these tags to minimize risk.

D. The ION devices upgrade themselves automatically whenever a new version is released by Palo Alto Networks.

Answer: C (LEAVE A REPLY)

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: 39

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

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

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

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

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

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

Answer: C (LEAVE A REPLY)

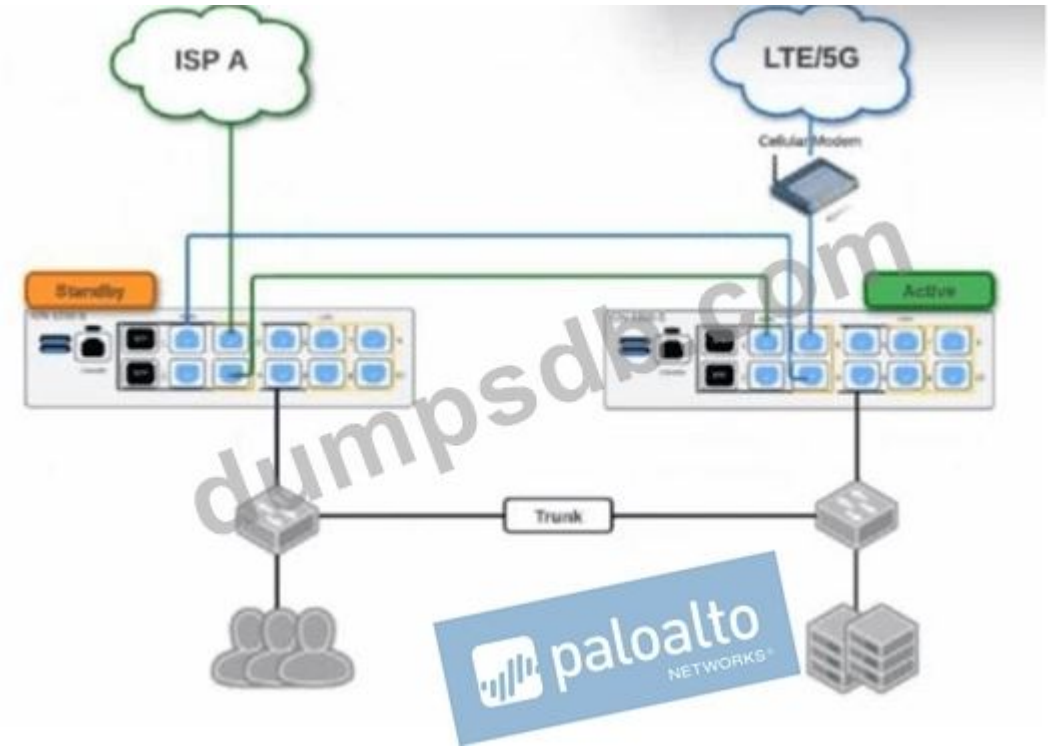
Comprehensive and Detailed Explanation

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: 40
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 (LEAVE A REPLY)
Comprehensive and Detailed Explanation

This scenario depicts a High Availability (HA) topology utilizing the ION 1200-S model's Fail-to-Wire (bypass) capabilities to share WAN links between two devices without needing external switches for every WAN connection.
1. WAN Link Availability (Statement A):
The diagram illustrates a "daisy-chain" cabling method supported by the ION 1200-S bypass pairs.
* ISP A (Green): Connects directly to the "Standby" (Left) unit first. Since the Standby unit remains powered on, it maintains direct access to ISP A.
* LTE/5G (Blue): Connects to the "Active" (Right) unit first. The connection then loops through a bypass pair on the Active unit to the Standby unit. When power is removed from the "Active" unit, the fail-to-wire relays on its Ethernet ports close physically. This creates a passive electrical bridge that connects the LTE modem directly to the Standby unit. The Standby unit (now becoming Active) will detect the link state change and successfully utilize the LTE connection. Therefore, both WAN links remain usable.
2. LAN Failover Mechanism (Statement C):
Prisma SD-WAN ION devices typically use a VRRP-like mechanism for LAN redundancy.
* When the "Active" node fails (loses power), the "Standby" node stops receiving keepalives and promotes itself to the Active state.
* To ensure downstream switches and clients immediately send traffic to the new Active unit, it must update their ARP tables. It does this by broadcasting a Gratuitous ARP (GARP) packet for the Virtual IP (VIP) address of the Switch Virtual Interfaces (SVIs). This action informs the network that the MAC address associated with the Gateway I1P is now reachable via the port connected to the new Active ION.234

NEW QUESTION: 41
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)
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: 42
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: (SHOW ANSWER)
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: 43
A network engineer is troubleshooting an ION device that is showing as "Offline" in the Prisma SD-WAN portal, despite the site reporting that local internet access is working. The engineer has console access to the device.
Which CLI command should be used to specifically validate the device's ability to resolve the controller's hostname and establish a secure connection to it over a specific interface?
A. ping <controller-ip>
B. debug controller reachability <interface>
C. show system connectivity
D. dump vpn summary
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
The CLI command debug controller reachability <interface> (e.g., debug controller reachability 1) is the specific diagnostic tool designed to verify the entire connectivity chain required for management plane availability.
Unlike a simple ICMP ping (Option A), which only tests Layer 3 connectivity to an IP address, the debug controller reachability command performs a sequential set of tests:
DNS Resolution: It attempts to resolve the specific Locator service URL (locator.cgnx.net or region-specific FQDN) to verify DNS functionality.
TCP Connectivity: It tests the ability to establish a TCP connection to the controller on port 443 (HTTPS).
SSL/TLS Handshake: It validates that the device can successfully negotiate the secure tunnel required for authentication.
If this command fails at the DNS step, the issue is likely a missing DNS server in the interface config. If it fails at the TCP step, it implies an upstream firewall is blocking outbound port 443. This targeted output allows the engineer to pinpoint exactly why the device is offline in the portal.

NEW QUESTION: 44
An administrator needs to generate a monthly report showing the "Top Applications" by bandwidth usage across all branch sites to justify a bandwidth upgrade.
Which specific component of the Prisma SD-WAN interface is designed to create, schedule, and email these PDF summaries?
A. Activity Charts
B. Media Analytics
C. Reports
D. Flow Browser
Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation
Prisma SD-WAN separates real-time visibility from historical summarization.
Reports (C): The Reports section is the dedicated engine for generating historical summaries. Administrators can create custom report templates (e.g., "Monthly Executive Summary") that include specific widgets like "Top Applications by Volume," "Site Availability," or "Circuit Utilization." Crucially, this feature allows for Scheduling, where the system automatically generates the PDF report at a set interval (e.g., first day of the month) and emails it to a distribution list.
Activity Charts (A) / Media Analytics (B): These provide interactive, visual graphs for ad-hoc analysis but are not designed for generating downloadable, scheduled PDF summaries for management.
Flow Browser (D): This is for deep-dive troubleshooting of individual sessions, not for high-level aggregate reporting.

NEW QUESTION: 45
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: (SHOW ANSWER)
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.

NEW QUESTION: 46
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: (SHOW ANSWER)
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.

Valid SD-WAN-Engineer Dumps shared by TrainingQuiz.com for Helping Passing SD-WAN-Engineer Exam! TrainingQuiz.com now offer the **newest SD-WAN-Engineer exam dumps**, the TrainingQuiz.com SD-WAN-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com SD-WAN-Engineer dumps with Test Engine here: https://www.trainingquiz.com/SD-WAN-Engineer-practice-quiz.html (**88** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

Valid SD-WAN-Engineer Dumps shared by TrainingQuiz.com for Helping Passing SD-WAN-Engineer Exam! TrainingQuiz.com now offer the **newest SD-WAN-Engineer exam dumps**, the TrainingQuiz.com SD-WAN-Engineer exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingQuiz.com SD-WAN-Engineer dumps with Test Engine here: https://www.trainingquiz.com/SD-WAN-Engineer-practice-quiz.html (**88** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)