Boost up Your Certification Score

Palo Alto Networks
SSE-Engineer
Palo Alto Networks Security Service Edge Engineer



For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 9.3

Question: 1

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to-business (B2B) partners to their data centers. The solution must meet these requirements: The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the branch locations. The branch locations must have internet filtering and data center connectivity. The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports. The security team must have access to manage the mobile user and access to branch locations. The network team must have access to manage only the partner access. How should Prisma Access be implemented to meet the customer requirements?

A. Deploy two Prisma Access instances - the first with mobile users, remote networks, and private access for all internal connection types, and the second with remote networks and private application access for B2B connections - and use the Strata Multitenant Cloud Manager Prisma Access configuration scope to manage access.
B. Deploy a Prisma Access instance with mobile users, remote networks, and private access for all connection types, and use the Prisma Access Configuration scope to manage all access.
C. Deploy two Prisma Access instances - the first with mobile users, remote networks, and private access for all internal connection types, and the second with remote networks and private application access for B2B connections - and use the specific configuration scope for the connection type to manage access.
D. Deploy a Prisma Access instance with mobile users, remote networks, and private access for all connection types, and use the specific configuration scope for the connection type to manage access.

Answer: D

Explanation:
A single Prisma Access instance is sufficient here because the segmentation the customer needs — security team managing mobile users and branch locations, network team managing only partner access — is an administrative RBAC problem, not a data-plane isolation problem. Strata Cloud Manager's configuration scope model (Mobile Users, Remote Networks, Service Connections, and the parent Prisma Access scope) lets an administrator be granted access to only the folders relevant to their function, so the security team can be scoped to the Mobile Users and Remote Networks containers while the network team is scoped to the private application/service connection objects used for B2B access. Deploying two separate Prisma Access instances (options A and C) is operationally wasteful and unnecessary: it doubles licensing overhead, duplicates infrastructure subnets and service connections, and is a pattern reserved for genuine tenant isolation requirements (distinct compliance boundaries, MSSP customers, or M&A separation), not simple team-based access segmentation. Using the broad Prisma Access configuration scope for everyone (option B) collapses all administrative boundaries and violates least privilege, since it would let the network team touch mobile user

and branch policy. Scoping RBAC to the specific configuration scope (Mobile Users, Remote Networks, or the private access/service connection objects) within one instance cleanly satisfies both the connectivity requirements and the separation-of-duties requirement.

Question: 2

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to-business (B2B) partners to their data centers. The solution must meet these requirements: The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the branch locations. The branch locations must have internet filtering and data center connectivity. The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports. The security team must have access to manage the mobile user and access to branch locations. The network team must have access to manage only the partner access. How can the engineer configure mobile users and branch locations to meet the requirements?

A. Use GlobalProtect and Remote Networks to filter internet traffic and provide access to data center resources using service connections.
B. Use Explicit Proxy to filter internet traffic and provide access to data center resources using service connections.
C. Use GlobalProtect to filter internet traffic and provide access to data center resources using service connections.
D. Use Explicit Proxy and Remote Networks to filter internet traffic and provide access to data center resources using service connections.

Answer: A

Explanation:
GlobalProtect is the correct mobile-user connection method here because the requirement explicitly calls for remote site connectivity from mobile users to the branch locations, in addition to internet filtering and data center access — a full-tunnel capability that Explicit Proxy, which is scoped to web/proxy-aware traffic only, cannot provide. Remote Networks is the purpose-built onboarding method for the branch locations, tunneling their traffic into Prisma Access over IPSec for consistent internet filtering and, through the shared backbone, reachability to data center resources. Service connections are the piece that stitches both populations to the data center: they terminate at the customer's HQ/data center and, once established, become reachable from both the GlobalProtect mobile user pool and the Remote Networks locations across the Prisma Access backbone, satisfying the data center connectivity requirement for both user types without requiring a dedicated tunnel per site. Option B and D are eliminated because Explicit Proxy cannot deliver full network-layer access to internal branch or data center resources; it is designed for outbound web traffic redirection via PAC file or forwarding profile, not IPSec-based site-to-site or full-tunnel remote access. Option C omits Remote Networks entirely, which would leave the branch offices unconnected. GlobalProtect plus Remote Networks plus service connections is the standard, minimal-footprint design pattern for this exact hybrid mobile-user/branch/data-center topology.

Visit us at: https://www.examsboost.com/test/sse-engineer

Question: 3

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to-business (B2B) partners to their data centers. [Same scenario as above.] Which two options will allow the engineer to support the requirements? (Choose two.)

A. Configure the CPE with Static Routes pointing to Prisma Access Infrastructure and Mobile User routes.
B. Enable eBGP for dynamic routing and configure Remote Networks.
C. Configure Remote Networks and define the branch IP subnets using Static Routes.
D. Enable Remote Networks Advertise Default Route.

Answer: B, D

Explanation:
The branch requirement is internet filtering plus data center connectivity, which means every branch location needs Prisma Access to become its default gateway to the internet while still exchanging specific internal routes with the data center. Enabling eBGP on the Remote Networks connection is the scalable way to accomplish this: dynamic routing lets the CPE and Prisma Access exchange branch subnet reachability automatically, without the administrative burden of manually maintaining static routes across every site as the branch network changes — critical for a multi-branch B2B/enterprise deployment. Enabling the Advertise Default Route option on the Remote Networks connection is what actually delivers the internet-filtering requirement: it causes Prisma Access to advertise a 0.0.0.0/0 route to the branch CPE over the tunnel so that all branch-originated internet-bound traffic is pulled into Prisma Access for inspection, rather than breaking out locally. Static routes (options A and C) are technically workable at very small scale, but they do not scale for multi-site deployments, are error-prone to maintain, and do nothing on their own to steer default (internet) traffic into the tunnel the way the Advertise Default Route setting does. eBGP with Advertise Default Route is the documented best-practice combination for branch internet filtering and site connectivity through Remote Networks.

Question: 4

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to-business (B2B) partners to their data centers. [Same scenario.] Which two components can be provisioned to enable data center connectivity over the internet? (Choose two.)

A. ZTNA Connector

B. SD-WAN Connector
C. Service connections
D. Colo-Connect

Answer: A, C

Explanation:
The question specifically asks for components that provide data center connectivity over the internet, which is the distinguishing factor between the four options. Service connections are the classic IPSec-based method: they build an encrypted tunnel from the customer's data center edge device to Prisma Access across the public internet, requiring no private circuit. ZTNA Connector achieves the same outcome through a different architecture — a lightweight, outbound-only connector deployed in the data center that establishes a secure, brokered tunnel to the nearest Prisma Access cloud gateway, again entirely over the internet, without requiring inbound firewall rules or a traditional IPSec peer. Both are therefore valid answers. Colo-Connect is explicitly excluded because it is built for the opposite use case: it delivers private, high-bandwidth connectivity to data centers using GCP Dedicated or Partner Interconnects, bypassing the public internet entirely to achieve up to 100 Gbps with lower latency and jitter — the architecture exists specifically because customers want to avoid internet transport for their highest-throughput sites. SD-WAN Connector is not a genuine Prisma Access private-application access method; Prisma SD-WAN integrates with Prisma Access through ION devices acting as CPE for remote networks or service connections, not as a distinct "connector" component in this context, so it does not belong in this answer set.

Question: 5

Which two actions can a company with Prisma Access deployed take to use the Egress IP API to automate policy rule updates when the IP addresses used by Prisma Access change? (Choose two.)

A. Configure a webhook to receive notifications of IP address changes.
B. Copy the Egress IP API Key in the service infrastructure settings.
C. Enable the Egress IP API endpoint in Prisma Access.
D. Download a client certificate to authenticate to the Egress IP API.

Answer: A, B

Explanation:
Prisma Access egress and public IP addresses can change as a result of autoscaling or infrastructure upgrades, so any allow-list dependent on those addresses (SaaS tenant restrictions, partner firewalls, third-party services) needs a reliable way to stay current. Palo Alto Networks addresses this with two complementary mechanisms. First, an Egress IP Notification URL — the webhook referenced in option A — can be configured under Infrastructure Settings so that Prisma Access sends an HTTP POST a few seconds before a new IP address becomes

active, giving downstream automation advance warning to update firewall or SaaS allow-lists before the change takes effect. Second, retrieving the actual address list requires authenticating to the Egress/Public IP retrieval API using an API key that is generated and copied from the service infrastructure settings, as described in option B; this key is passed in the request header when calling the retrieval endpoint. There is no separate "enable the Egress IP API endpoint" toggle, since the retrieval API is available by default once a key is generated — making option C incorrect. Authentication to this API is strictly key-based, not certificate-based, so downloading a client certificate (option D) is not a supported or required step. Together, the webhook and API key form the complete automation loop: notify, then retrieve and apply.

Visit us at: https://www.examsboost.com/test/sse-engineer

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

