



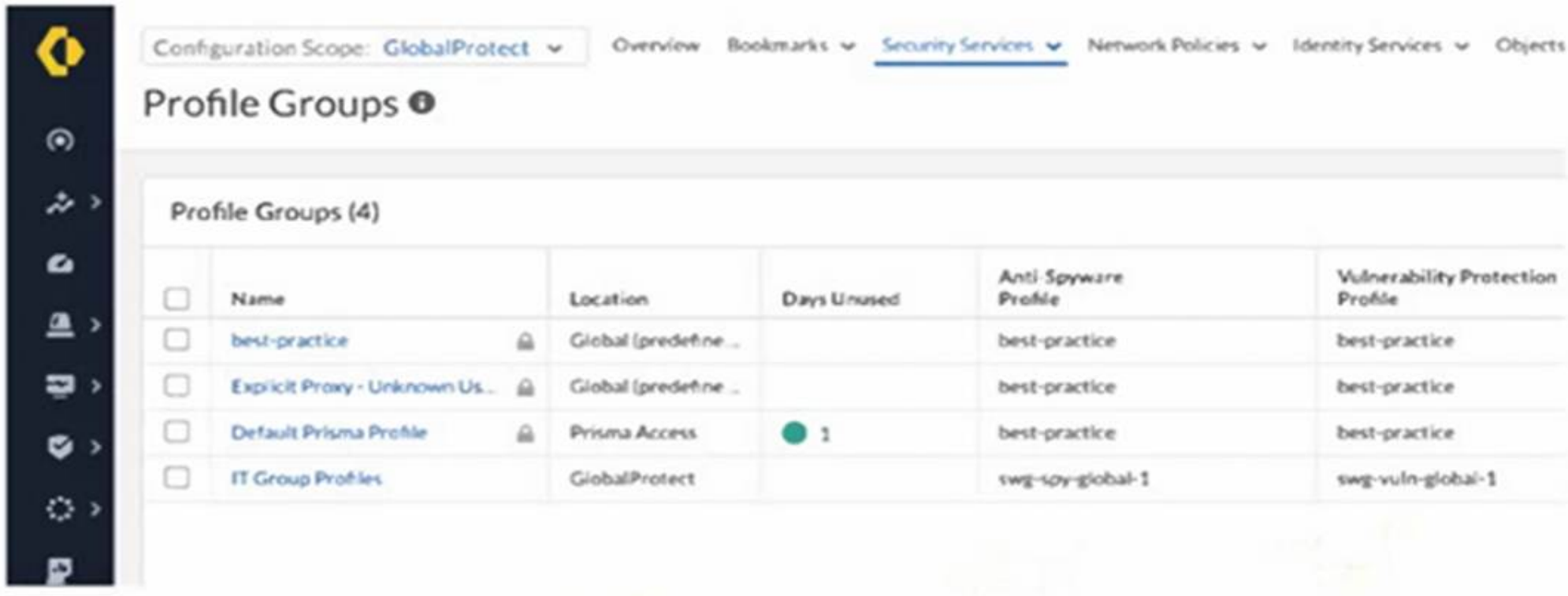
Paloalto-Networks

Exam Questions SSE-Engineer

Palo Alto Networks Security Service Edge Engineer

NEW QUESTION 1

An intern is tasked with changing the Anti-Spyware Profile used for security rules defined in the GlobalProtect folder. All security rules are using the Default Prisma Profile. The intern reports that the options are greyed out and cannot be modified when selecting the Default Prisma Profile. Based on the image below, which action will allow the intern to make the required modifications?



- A. Request edit access for the GlobalProtect scope.
- B. Change the configuration scope to Prisma Access and modify the profile group.
- C. Create a new profile, because default profile groups cannot be modified.
- D. Modify the existing anti-spyware profile, because best-practice profiles cannot be removed from a group.

Answer: C

NEW QUESTION 2

Strata Logging Service is configured to forward logs to an external syslog server; however, a month later, there is a disruption on the syslog server. Which action will send the missing logs to the external syslog server?

- A. Configure a replay profile with the affected time range and associate it with the affected syslog server profile.
- B. Delete the affected syslog server profile and create a new one.
- C. Export the logs from Strata Logging Service, and then manually import them to the syslog server.
- D. Configure a log filter under the syslog server profile with the affected time range.

Answer: A

NEW QUESTION 3

During a deployment of Prisma Access (Managed by Strata Cloud Manager) for mobile users, a SAML authentication type and authentication profile in the Cloud Identity Engine application is successfully created. Using this SAML authentication, what is a valid next step to configure authentication for mobile users?

- A. Perform a full commit to Strata Cloud Manager so the Cloud Identity Engine profiles get synchronized from the application.
- B. Permit the Cloud Identity Engine service account RBAC access to the mobile user folder in Strata Cloud Manager.
- C. In Strata Cloud Manager, create a new authentication type of ??Cloud Identity Engine.??
- D. Create a SAML authentication profile in Strata Cloud Manager and link it to the Cloud Identity Engine profile.

Answer: D

NEW QUESTION 4

All mobile users are unable to authenticate to Prisma Access (Managed by Strata Cloud Manager) using SAML authentication through the Cloud Identity Engine. Users report that after entering their credentials on the Identity Provider (IdP) login page, they are redirected to the Prisma Access portal without successful authentication, and they receive this error message:
 Error: Prisma Access Portal Authentication Failed using CIE-SAML with message ??400 Bad Request??
 Which action will identify the root cause of this error?

- A. Verify the SAML metadata configuration in both Strata Cloud Manager and the IdP portal to confirm that the endpoint URLs and certificates are correctly configured.
- B. Examine the Security policy rules in Prisma Access to ensure that traffic from the IdP is allowed and not blocked.
- C. Verify the SAML metadata configuration in both the Cloud Identity Engine and the IdP portal to confirm that the endpoint URLs and certificates are correctly configured.
- D. Review the Authentication logs in Strata Cloud Manager to check for any SAML error messages or authentication failures.

Answer: C

NEW QUESTION 5

What is the flow impact of updating the Cloud Services plugin on existing traffic flows in Prisma Access?

- A. They will experience latency during the plugin upgrade process.
- B. They will automatically terminate when the upgrade begins.
- C. They will be unaffected because the plugin upgrade is transparent to users.
- D. They will be unaffected only if Panorama is deployed in high availability (HA) mode.

Answer: C

NEW QUESTION 6

How can a network security team be granted full administrative access to a tenant's configuration while restricting access to other tenants by using role-based access control (RBAC) for Panorama Managed Prisma Access in a multitenant environment?

- A. Create an Access Domain and restrict access to only the Device Groups and Templates for the Target Tenant.
- B. Create a custom role enabling all privileges within the specific tenant's scope and assign it to the security team's user accounts.
- C. Create a custom role with Device Group and Template privileges and assign it to the security team's user accounts.
- D. Set the administrative accounts for the security team to the "Superuser" role.

Answer: A

NEW QUESTION 7

In an Explicit Proxy deployment where no agent can be used on the endpoint, which authentication method is supported with mobile users?

- A. LDAP
- B. Kerberos
- C. SAML
- D. SSO

Answer: C

NEW QUESTION 8

Where are tags applied to control access to Generative AI when implementing AI Access Security?

- A. To Generative AI applications for identifying sanctioned, tolerated, or unsanctioned applications
- B. To security rules for defining which types of Generative AI applications are allowed or blocked
- C. To user devices for identifying and controlling which Generative AI applications they can access
- D. To Generative AI URL categories for classifying trusted and untrusted Generative AI websites

Answer: A

NEW QUESTION 9

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: AD

NEW QUESTION 10

An engineer configures User-ID redistribution from an on-premises firewall connected to Prisma Access (Managed by Panorama) using a service connection. After committing the configuration, traffic from remote network connections is still not matching the correct user-based policies. Which two configurations need to be validated? (Choose two.)

- A. Ensure the Remote_Network_Template is selected when adding the User-ID Agent in Panorama.
- B. Confirm there is a Security policy configured in Prisma Access to allow the communication on port 5007.
- C. Confirm the Collector Pre-Shared Keys match between Prisma Access and the on-premises firewall.
- D. Ensure the Service_Conn_Template is selected when adding the User-ID Agent in Panorama.

Answer: AD

NEW QUESTION 10

How can an engineer verify that only the intended changes will be applied when modifying Prisma Access policy configuration in Strata Cloud Manager (SCM)?

- A. Review the SCM portal for blue circular indicators next to each configuration menu item and ensure only the intended areas of configuration have this indicator.
- B. Compare the candidate configuration and the most recent version under "Config Version Snapshots/
- C. Select the most recent job under Operations > Push Status to view the pending changes that would apply to Prisma Access.
- D. Open the push dialogue in SCM to preview all changes which would be pushed to Prisma Access.

Answer: D

NEW QUESTION 15

How can a senior engineer use Strata Cloud Manager (SCM) to ensure that junior engineers are able to create compliant policies while preventing the creation of policies that may result in security gaps?

- A. Use security checks under posture settings and set the action to ??deny?? for all checks that do not meet the compliance standards.
- B. Configure role-based access controls (RBACs) for all junior engineers to limit them to creating policies in a disabled state, manually review the policies, and enable them using a senior engineer role.
- C. Configure an auto tagging rule in SCM to trigger a Security policy review workflow based on a security rule tag, then instruct junior engineers to use this tag for all new Security policies.
- D. Run a Best Practice Assessment (BPA) at regular intervals and manually revert any policies not meeting company compliance standards.

Answer: A

NEW QUESTION 19

Which statement applies when enabling multitenancy in Prisma Access (Managed by Panorama)?

- A. Service connection licenses will be assigned only to the first tenant, and these service connections can be shared with the other tenants.
- B. A single tenant cannot consist solely of mobile users or solely of remote networks.
- C. Each tenant is allocated its own dedicated Prisma Access instances, with compute resources that are not shared across tenants.
- D. There is flexibility to manage different tenants using separate Panoramas, which allows for better organization and management of the multiple tenants.

Answer: C

NEW QUESTION 24

When a review of devices discovered by IoT Security reveals network routers appearing multiple times with different IP addresses, which configuration will address the issue by showing only unique devices?

- A. Add the duplicate entries to the ignore list in IoT Security.
- B. Merge individual devices into a single device with multiple interfaces.
- C. Create a custom role to merge devices with the same hostname and operating system.
- D. Delete all duplicate devices, keeping only those discovered using their management IP addresses.

Answer: B

NEW QUESTION 25

Which advanced AI-powered functionality does Strata Copilot provide to enhance the capabilities of Prisma Access security teams?

- A. Real-time traffic analysis for automated threat prevention
- B. Initial configuration of Prisma Access using a natural language interface
- C. Customized guidance for resolving issues through recommended next steps
- D. Automated remediation of misconfigured security policies

Answer: C

NEW QUESTION 29

A large retailer has deployed all of its stores with the same IP address subnet. An engineer is onboarding these stores as Remote Networks in Prisma Access. While onboarding each store, the engineer selects the ??Overlapping Subnets?? checkbox. Which Remote Network flow is supported after onboarding in this scenario?

- A. To private applications
- B. To the internet
- C. To remote network
- D. To mobile users

Answer: A

NEW QUESTION 32

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: C

NEW QUESTION 34

An engineer has configured a new Remote Networks connection using BGP for route advertisements. The IPSec tunnel has been established, but the BGP peer is

not up.

Which two elements must the engineer validate to solve the issue? (Choose two.)

- A. Secret
- B. MRAI Timers
- C. Peer AS Number
- D. Advertise Default Route Checkbox

Answer: AC

NEW QUESTION 39

Which two statements apply when a customer has a large branch office with employees who all arrive and log in within a five-minute time period? (Choose two.)

- A. DNS results are only cached for frequently used hostnames.
- B. Maximum pending TCP DNS requests is 64.
- C. Maximum number of TCP DNS retries is 3.
- D. DNS results are cached for 300 seconds.

Answer: BC

NEW QUESTION 43

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SSE-Engineer Practice Exam Features:

- * SSE-Engineer Questions and Answers Updated Frequently
- * SSE-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * SSE-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SSE-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SSE-Engineer Practice Test Here](#)