Paloalto-Networks

Exam Questions SSE-Engineer

Palo Alto Networks Security Service Edge Engineer

NEW QUESTION 1
A user connected to Prisma Access reports that traffic intermittently is denied after matching a Catch-All Deny rule at the bottom and bypassing HIP-based policies. Refreshing VPN connection restores the access.
What are two reasons for this behavior? (Choose two.)

A. "Collect HIP data' needs to be enabled in the configuration.
B. User mapping is learned from sources other than gateway authentication.
C. Firewall loses user mapping due to missed HIP report checks.
D. HIP-enforced policy is scheduled for certain hours of the day.

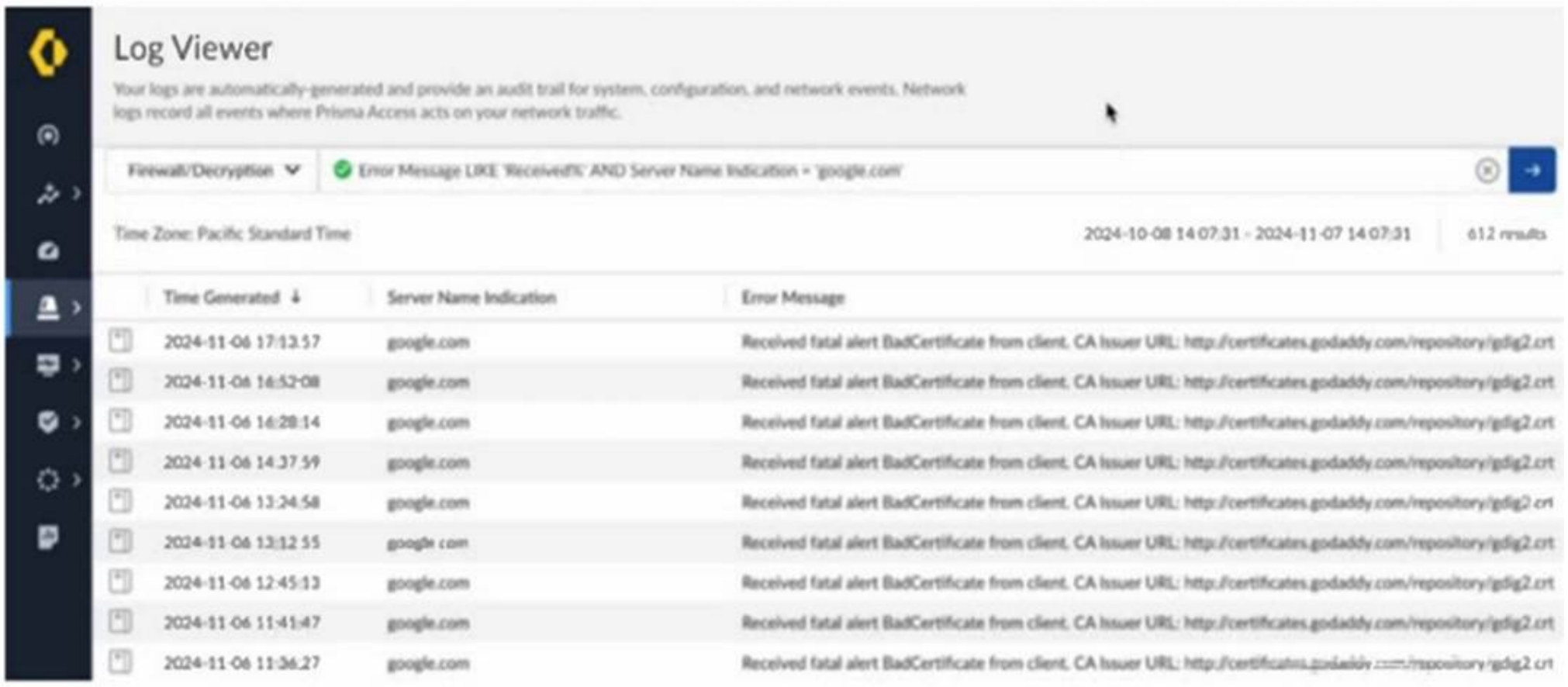
Answer: BC

NEW 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.
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: CD

NEW QUESTION 3
Based on the image below, which two statements describe the reason and action required to resolve the errors? (Choose two.)



A. The client is misconfigured.
B. Create a do not decrypt rule for the hostname ??google.com.??
C. The server has pinned certificates.
D. Create a do not decrypt rule for the hostname ??certificates.godaddy.com.??

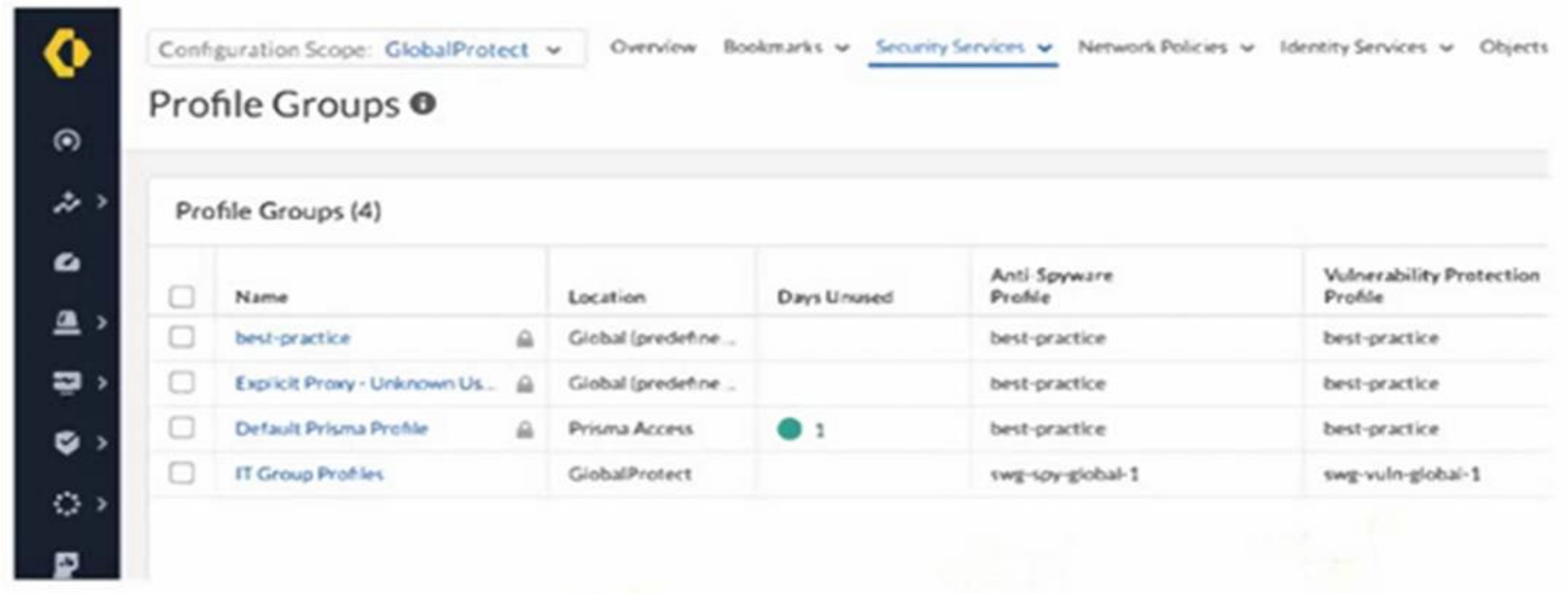
Answer: BC

NEW QUESTION 4
A company has a Prisma Access deployment for mobile users in North America and Europe. Service connections are deployed to the data centers on these continents, and the data centers are connected by private links.
With default routing mode, which action will verify that traffic being delivered to mobile users traverses the service connection in the appropriate regions?

A. Configure BGP on the customer premises equipment (CPE) to prefer the assigned community string attribute on the mobile user prefixes in its respective Prisma Access region.
B. Configure each service connection to filter out the mobile user pool prefixes from the other region in the advertisements to the data center.
C. Configure BGP on the customer premises equipment (CPE) to prefer the MED attribute on the mobile user prefixes in its respective Prisma Access region.
D. Configure each service connection to prepend the BGP ASN five times for mobile user pool prefixes originating from the other region.

Answer: B

NEW QUESTION 5
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 6
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 7
What is the flow impact of updating the Cloud Services plugin on existing traffic flows in Prisma Access?

A. They willexperience 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 8
An engineer has configured a Web Security rule that restricts access to certain web applications for a specific user group. During testing, the rule does not take effect as expected, and the users can still access blocked web applications.
What is a reason for this issue?

A. The rule was created with improper threat management settings.
B. The rule was created in the wrong scope, affecting only GlobalProtect users instead of all users.
C. The rule was created at a higher level in the rule hierarchy, giving priority to a lower- level rule.
D. The rule was created at a lower level in the rule hierarchy, giving priority to a higher- level rule.

Answer: D

NEW QUESTION 9
An engineer deploys a new branch connected to Prisma Access. From the customer premises equipment (CPE) device at the branch, Phase 1 on the tunnel is established, but Phase 2-encrypted packets are not coming back from Prisma Access.
Which Strata Logging Service log facility should the engineer review to determine why Phase 2-encrypted traffic is not being received?

A. Decrypt logs
B. System logs
C. Traffic logs

D. Tunnel logs

Answer: D

NEW QUESTION 10
In addition to creating a Security policy, how can an AI Access Security be used to prevent users from uploading financial information to ChatGPT?

A. Apply File Blocking to stop file uploads containing financial information.
B. Configure an Enterprise DLP rule to block uploads containing financial information.
C. Add the ChatGPT domains using URL Filtering to block uploads containing financial information.
D. Apply a vulnerability profile to stop attempts to exploit system flaws or gain unauthorized access to financial systems.

Answer: B

NEW QUESTION 10
A malicious user is attempting to connect to a blocked website by crafting a packet using a fake SNI and the correct website in the HTTP host header.
Which option will prevent this form of attack?

A. Advanced Threat Prevention option to block ??Domain Fronting??
B. Advanced URL Filtering and block the ??Malicious Behavior?? category
C. Advanced URL Filtering and block ??SNI mismatch with Server Certificate (SAN/CN)??
D. SSL Decryption to ??Block sessions on SNI mismatch with Server Certificate (SAN/CN)??

Answer: D

NEW QUESTION 14
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 orblocked
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 18
What is the purpose of embargo rules in Prisma Access?

A. Rate-limiting connections originating from specific countries
B. Allowing traffic only from specific countries
C. Blocking connections from specific countries
D. Blocking traffic from Russi
E. China, and North Korea only

Answer: C

NEW QUESTION 20
Which Cloud Identity Engine capability will create a Security policy that uses Entra ID attributes as the source identification?

A. Entra ID Group Attribute
B. Attribute Group Mapping
C. Entra ID Cloud Group
D. Cloud Dynamic User Group

Answer: D

NEW QUESTION 21
How can role-based access control (RBAC) for Prisma Access (Managed by Strata Cloud Manager) be used to grant each member of a security team full administrative access to manage the Security policy in a single tenant while restricting access to other tenants in a multitenant deployment?

A. Add the team to the Parent Tenant, select the Prisma Access Configuration Scope, and set the role to Security Administrator.
B. Add the team to the Child Tenant, select All Apps & Services, and set the role to Security Administrator.
C. Add the team to the Parent Tenant, select Prisma Access & NGFW Configuration, and set the role to Security Administrator.
D. Add the team to the Child Tenant, select Prisma Access & NGFW Configuration, and set the role to Security Administrator.

Answer: D

NEW QUESTION 26
An engineer has configured IPSec tunnels for two remote network locations; however, users are experiencing intermittent connectivity issues across the tunnels.
What action will allow the engineer to receive notifications when the IPSec tunnels are down or experiencing instability?

A. Create a new notification profile specifying conditions for remote network IPSec tunnels.
B. Create a tunnel log notification rule to alert on specified remote network IPSec tunnel conditions.
C. Set up the operational health dashboard to email alerts for remote Network IPSec tunnel issues.
D. Select the IPSec tunnel monitoring and notifications checkbox when configuring the remote network IPSec tunnels.

Answer: A

NEW QUESTION 27
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

NEW QUESTION 30
Which feature will fetch user and group information to verify whether a group from the Cloud Identity Engine is present on a security processing node (SPN)?

A. SASE Health Dashboard
B. User Activity Insights
C. Prisma Access Locations
D. Region Activity Insights

Answer: A

NEW QUESTION 35
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 36
After configuring domain-based split tunnel for zoom.us, how is expected behavior on the client machine confirmed?

A. Verify from the routing table.
B. Enable dump level logs on GlobalProtect Application.
C. Verify zoom.us is resolved by the tunnel assigned DNS server.
D. Ping zoom.us from the CLI.

Answer: A

NEW QUESTION 38
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 39
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 40
Which feature within Strata Cloud Manager (SCM) allows an operations team to view applications, threats, and user insights for branch locations for both NGFW and Prisma Access simultaneously?

A. Command Center
B. Log Viewer
C. Branch Site Monitor
D. SASE Health Dashboard

Answer: A

NEW QUESTION 45
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 46
.....

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