Question #1 *Topic 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.

Suggested Answer: *D*

Community vote distribution

D (100%)

engineerpe25 3 months, 2 weeks ago

Selected Answer: D

That's correct. Additionally, the configuration scope must be specific.

upvoted 1 times

Pretorian 4 months, 1 week ago

Selected Answer: D

I believe the right answer is "D", why would two separate tenants be needed just for the Partner to access an internally developed application? This can be easily achieved with ZTNA Connector. Two tenants is a giant overkill and inefficiency in my opinion.

That level of isolation is rarely needed outside of an MSP infrastructure.

Perhaps you could argue a different DataLake / Strata Logging Service is needed, in which case, separate tenant could be the way.

upvoted 3 times

Question #2 *Topic 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 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.

Suggested Answer: *A*

Community vote distribution

A (100%)

engineerpe25 3 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

Question #3 *Topic 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.

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 RemoteNetworks.

C. Configure Remote Networks and define the branch IP subnets using Static Routes.

D. Enable Remote Networks Advertise Default Route.

Suggested Answer: *BC*

Community vote distribution

AC (67%) BD (33%)

Ac1d_ 1 month, 3 weeks ago

Selected Answer: AC

I also think this is AC, because you can specify the subnets, it is not necessary to enable BGP

upvoted 1 times

makgol62 3 months, 1 week ago

Selected Answer: BD

branch location requires internet connection but static routes' answers don't describe about default route.

upvoted 1 times

engineerpe25 3 months, 2 weeks ago

Selected Answer: AC

I think the answer is A y C, because it is not necessary to enable BGP.

upvoted 1 times

Question #4 *Topic 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.
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

Suggested Answer: *AC*

Community vote distribution

AC (100%)

engineerpe25 3 months, 2 weeks ago

Selected Answer: AC

That's correct (A and C)

upvoted 1 times

shaf3y 4 months, 1 week ago

Selected Answer: AC

A and C. ColoConnect uses private connectivity to the DC (ex: private WAN connection), and not internet-based connectivity. SD-WAN isn't relevant in this case.

upvoted 2 times

Fannn 3 months, 3 weeks ago

agree with you

upvoted 1 times

Pretorian 4 months, 1 week ago

Selected Answer: AC

I believe the correct answers are: A (ZTNA Connector) and C (Service Connections).

Colo Connect does not use the internet, " interconnects to one or more cloud providers and connections to the on-premises data centers over a private or leased WAN."

https://docs.paloaltonetworks.com/prisma-access/administration/colo-connect-in-prisma-access

upvoted 2 times

Pretorian 4 months, 1 week ago

Selected Answer: AC

Colo Connect connections to Prisma Access are not over the public internet. Therefore, I believe the right answers are A (ZTNA Connector) and C (Service Connection).

upvoted 2 times

shaf3y 4 months, 1 week ago

connection to the DC is private and not to Prisma Access ;)

upvoted 1 times

Question #5 *Topic 1*

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.

Suggested Answer: *AB*

Community vote distribution

AB (75%) AD (25%)

leonisc 2 weeks, 2 days ago

Selected Answer: AB

A and B are correct.

C : The Egress IP API endpoint is enabled by default.

D : Authentication is done via API key, not certificates.

upvoted 1 times

uber2019 1 month ago

Selected Answer: AD

A,D are correct.

upvoted 1 times

shaf3y 4 months, 1 week ago

Selected Answer: AB

A and B

upvoted 2 times

Question #6 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (75%) D (25%)

df8dffa 1 week, 5 days ago

Selected Answer: D

Push Dialogue Functionality: In Strata Cloud Manager, when an engineer initiates a push (e.g., by clicking Push Config), the push dialogue displays a detailed summary of all changes, including specific policy rule modifications, object changes, and network settings. This preview is tailored for pre-push validation, showing exactly what will be applied to Prisma Access.

upvoted 1 times

shaf3y 4 months, 1 week ago

Selected Answer: B

It's B

upvoted 1 times

Pretorian 4 months, 1 week ago

Selected Answer: B

Answer is B "Config Version Snapshots". Confirmed in the SCM GUI.

https://stratacloudmanager.paloaltonetworks.com/manage/operation/snapshots

upvoted 2 times

Question #7 *Topic 1*

When using the traffic replication feature in Prisma Access, where is the mirrored traffic directed for analysis?

A. Specified internal security appliance

B. Dedicated cloud storage location

C. Panorama

D. Strata Cloud Manager (SCM)

Suggested Answer: *B*

Community vote distribution

B (100%)

Pretorian 4 months, 1 week ago

Selected Answer: B

I believe "B" (Dedicated cloud storage location) is the answer:

"When enabling Traffic Replication, Prisma Access creates dedicated cloud storage buckets in each Prisma Access Compute Location where this feature is enabled and continuously saves pcap files containing a replica of the traffic that’s traversing Prisma Access."

https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/mobile-user-globalprotect-advanced-deployments/traffic-mirroring

upvoted 3 times

Question #8 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

fb75bfc 3 months, 2 weeks ago

Selected Answer: B

https://docs.paloaltonetworks.com/iot/administration/discover-iot-devices-and-take-inventory/create-multi-interface-devices

upvoted 1 times

Question #9 *Topic 1*

What is the impact of selecting the “Disable Server Response Inspection” checkbox after confirming that a Security policy rule has a threat protection profile configured?

A. Only HTTP traffic from the server to the client will bypass threat inspection.

B. The threat protection profile will override the “Disable Server Response Inspection” only for HTTP traffic from the server to the client.

C. All traffic from the server to the client will bypass threat inspection.

D. The threat protection profile will override the “Disable Server Response Inspection” for all traffic from the server to the client.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

2fcc0e5 3 months, 3 weeks ago

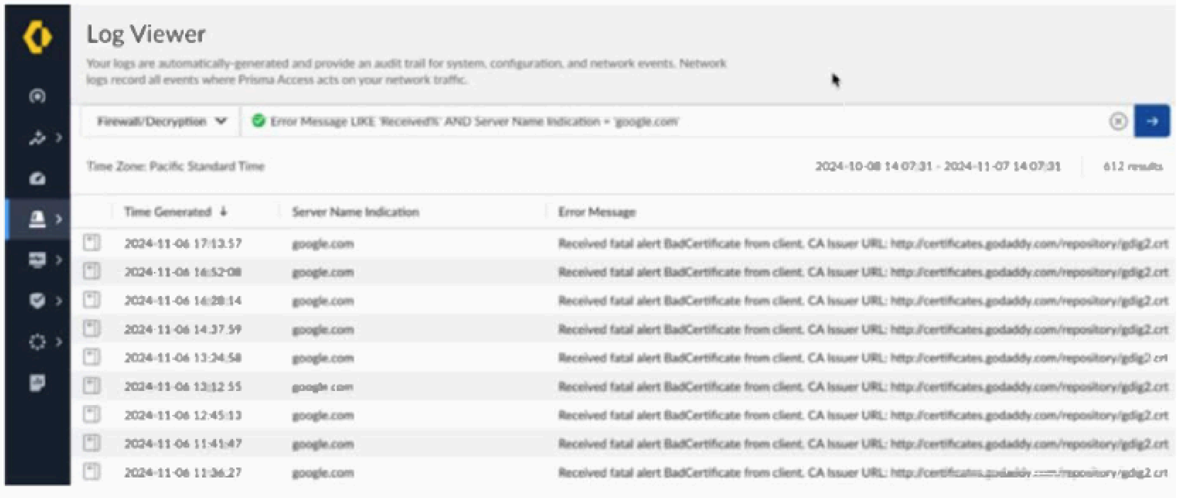
Selected Answer: B

B is valid assuming no inter-region backup is needed

upvoted 1 times

Question #11 *Topic 1*

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



Log Viewer

Your logs are automatically-generated and provide an audit trail for system, configuration, and network events. Network logs record all events where Prisma Access acts on your network traffic.

Firewall/Decryption

Error Message LIKE 'Received%' AND Server Name Indication = 'google.com'

Time Zone: Pacific Standard Time

2024-10-08 14:07:31 - 2024-11-07 14:07:31

612 results

Time Generated	Server Name Indication	Error Message
2024-11-06 17:13:57	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 16:52:08	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 16:28:14	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 14:37:59	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 13:24:58	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 13:12:55	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 12:45:13	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 11:41:47	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt
2024-11-06 11:36:27	google.com	Received fatal alert BadCertificate from client. CA Issuer URL: http://certificates.godaddy.com/repository/gdig2.crt

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.”

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

387d8c0 3 months, 2 weeks ago

Selected Answer: D

the most reasonable answer

upvoted 1 times

Question #14 *Topic 1*

What will cause a connector to fail to establish a connection with the cloud gateway during the deployment of a new ZTNA Connector in a data center?

A. There is a misconfiguration in the DNS settings on the connector.

B. The connector is deployed behind a double NAT.

C. The connector is using a dynamic IP address.

D. There is a high latency in the network connection.

Suggested Answer: *B*

Community vote distribution

A (100%)

Testeraccount 1 month, 2 weeks ago

Selected Answer: A

DNS sounds like it would make the most sense here.

upvoted 1 times

2fcc0e5 3 months, 3 weeks ago

Selected Answer: A

DNS issue makes more sense, NAT (double or simple) should not be a problem

upvoted 1 times

Question #15 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

B (100%)

bobmead 2 months, 1 week ago

Selected Answer: B

User Activity Insights provides visibility into user and group activity, including whether specific Cloud Identity Engine (CIE) user or group information has been successfully fetched and recognized by a Security Processing Node (SPN) within Prisma Access.

This is especially useful when troubleshooting group-based policy enforcement issues, as it helps validate identity propagation from CIE to the SPNs.

upvoted 1 times

Question #16 *Topic 1*

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.

Suggested Answer: *AD*

Community vote distribution

AC (100%)

fb75bfc 3 months, 2 weeks ago

Selected Answer: AC

https://docs.paloaltonetworks.com/prisma/prisma-access/3-0/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/redistribute-userid-information-for-users-and-networks/redistribute-user-id-information-to-prisma-access

upvoted 2 times

Question #17 *Topic 1*

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 Russia, China, and North Korea only

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

Pretorian 4 months, 1 week ago

Selected Answer: A

Replay profile is correct:

https://docs.paloaltonetworks.com/strata-logging-service/administration/forward-logs/forward-logs-with-log-replay

upvoted 2 times

Question #19 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

shaf3y 4 months, 1 week ago

Selected Answer: B

100% B

upvoted 2 times

Pretorian 4 months, 1 week ago

Selected Answer: B

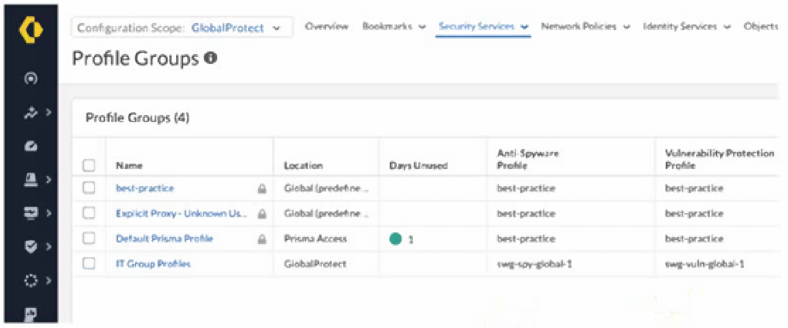
Correct answer is B "to the internet" 100%
The “Overlapping Subnets” checkbox limits connectivity of remote networks to ONLY the internet. Which makes sense as there are overlaps in the network.

Too lazy to add a KB but I guarantee this is the right answer :)

upvoted 4 times

Question #20 *Topic 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?



Profile Groups

Profile Groups (4)

□	Name	Location	Days Unused	Anti-Spyware Profile	Vulnerability Protection Profile
□	best-practice	Global (predefine ...		best-practice	best-practice
□	Explicit Proxy - Unknown Us...	Global (predefine ...		best-practice	best-practice
□	Default Prisma Profile	Prisma Access	● 1	best-practice	best-practice
□	IT Group Profiles	GlobalProtect		swg-spy-global-1	swg-vuln-global-1

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

An engineer configures a Security policy for traffic originating at branch locations in the Remote Networks configuration scope. After committing the configuration and reviewing the logs, the branch traffic is not matching the Security policy.
Which statement explains the branch traffic behavior?

A. The source address was configured with an address object including the branch location prefixes.

B. The source zone was configured as “Trust.”

C. The Security policy did not meet best practice standards and was automatically removed.

D. The traffic is matching a Security policy in the Prisma Access configuration scope.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which overlay protocol must a customer premises equipment (CPE) device support when terminating a Partner Interconnect-based Colo-Connect in Prisma Access?

A. Geneve

B. IPSec

C. GRE

D. DTLS

Suggested Answer: *C*

Community vote distribution

C (100%)

Pretorian 4 months, 1 week ago

Selected Answer: C

Correct option is C (GRE):

"Colo-Connect uses service connections, but they differ from Prisma Access in that they use GRE tunnels instead of IPSec tunnels and always use BGP for routing"

https://docs.paloaltonetworks.com/prisma-access/administration/colo-connect-in-prisma-access/configure-prisma-access-colo-connect/configure-prisma-access-colo-connect-panorama

upvoted 2 times

shaf3y 4 months, 1 week ago

Selected Answer: C

It's GRE

upvoted 1 times

Question #25 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!