Question #1 *Topic 1*

A customer currently uses a third-party proxy solution for client endpoints and would like to migrate to Prisma Access to secure mobile user internet-bound traffic.
Which recommendation should the Systems Engineer make to this customer?

A. With the explicit proxy license add-on, set up GlobalProtect.

B. With the mobile user license, set up explicit proxy.

C. With the explicit proxy license, set up a service connection.

D. With the mobile user license, set up a corporate access node.

Suggested Answer: *B*

Community vote distribution

B (100%)

examtopics2234 6 months ago

Selected Answer: B

It's B

upvoted 1 times

johannes0815 10 months ago

Selected Answer: B

https://docs.paloaltonetworks.com/prisma-access/administration/your-prisma-access-license

upvoted 1 times

confusion 1 year, 2 months ago

Selected Answer: B

For sure B

upvoted 1 times

Lapas 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 2 times

yet_another_user 1 year, 6 months ago

Reading through docu below, agree with B as a better choise.

upvoted 1 times

NodummyIQ 1 year, 8 months ago

Option D is a better choice because it involves setting up a corporate access node with the mobile user license, which allows Prisma Access to secure mobile user traffic effectively without relying on an explicit proxy configuration.

upvoted 1 times

Pretorian 1 year, 9 months ago

Selected Answer: B

Agreed, B

upvoted 2 times

Toubster 2 years, 1 month ago

Selected Answer: B

> Prisma Access Explicit Proxy requires that you have a Prisma Access license for Mobile Users.

upvoted 3 times

Question #2 *Topic 1*

What is a benefit of deploying secure access service edge (SASE) with a secure web gateway (SWG) over a SASE solution without a SWG?

A. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down.

B. It prepares the keys and certificates required for decryption, creating decryption profiles and policies, and configuring decryption port mirroring.

C. Protection is offered in the cloud through a unified platform for complete visibility and precise control over web access while enforcing security policies that protect users from hostile websites.

D. It creates tunnels that allow users and systems to connect securely over a public network as if they were connecting over a local area network (LAN).

Suggested Answer: *C*

Community vote distribution

C (100%)

confusion 2 months ago

Selected Answer: C

none of the rest makes sense, so C

upvoted 2 times

Lapas 3 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

sguerouate 4 months, 2 weeks ago

Selected Answer: C

Agreed on C

upvoted 2 times

NodummyIQ 8 months ago

C. Protection is offered in the cloud through a unified platform for complete visibility and precise control over web access while enforcing security policies that protect users from hostile websites.

upvoted 3 times

Question #3 *Topic 1*

Which action protects against port scans from the internet?

A. Apply App-ID Security policy rules to block traffic sourcing from the untrust zone.

B. Assign Security profiles to Security policy rules for traffic sourcing from the untrust zone.

C. Apply a Zone Protection profile on the zone of the ingress interface.

D. Assign an Interface Management profile to the zone of the ingress surface.

Suggested Answer: *C*

Community vote distribution

C (86%) 14%

examtopics2234 6 months ago

Selected Answer: B

Should be B, Zone Protection isn't available for Prisma Access.

upvoted 1 times

Mr_Cipher 7 months, 2 weeks ago

It should be B since in SASE there are only two Zones and no interface mapping

upvoted 1 times

TheIronSheik 8 months, 2 weeks ago

strange question for SASE

upvoted 1 times

confusion 1 year, 2 months ago

Selected Answer: C

Definitely C.

upvoted 1 times

Lapas 1 year, 3 months ago

Selected Answer: C

C is correct.

Configure protection against floods, reconnaissance, packet-based attacks, and non-IP-protocol-based attacks with Zone Protection profiles.

upvoted 2 times

Pretorian 1 year, 9 months ago

Selected Answer: C

100% Zone Protection Profile

upvoted 3 times

Question #4 *Topic 1*

Which product continuously monitors each segment from the endpoint to the application and identifies baseline metrics for each application?

A. App-ID Cloud Engine (ACE)

B. Autonomous Digital Experience Management (ADEM)

C. CloudBlades

D. WildFire

Suggested Answer: *B*

Community vote distribution

B (100%)

confusion 2 months ago

Selected Answer: B

ADEM, so B

upvoted 1 times

Lapas 3 months, 3 weeks ago

Selected Answer: B

B is correct.

https://docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-admin/adem-monitoring-and-tests

One of the advantages of Autonomous DEM (ADEM) is that it is continuously monitoring each segment in your Secure Access Service Edge (SASE) environment from the user all the way to the application

upvoted 2 times

Pretorian 9 months, 3 weeks ago

Selected Answer: B

No question, ADEM

upvoted 4 times

Question #5 *Topic 1*

Which application gathers health telemetry about a device and its WiFi connectivity in order to help determine whether the device or the WiFi is the cause of any performance issues?

A. data loss prevention (DLP)

B. remote browser isolation (RBI)

C. Cortex Data Lake

D. GlobalProtect

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **Helloory** Highly Voted 👍 1 year, 10 months ago

Correct answer is Global Protect

upvoted 6 times

⊟ **raquinopsky** Highly Voted 👍 1 year, 10 months ago

I think the answer should be "GlobalProtect"

upvoted 6 times

⊟ **efrah** Most Recent 🕒 1 month ago

Selected Answer: D

D globalprotect

upvoted 1 times

⊟ **StevenWilliams0728** 3 months, 1 week ago

Its global protect.

upvoted 1 times

⊟ **examtopics2234** 6 months ago

Selected Answer: D

It's not the CDL for sure. By elimination, D should be Global Protect but with ADEM addon.

upvoted 2 times

⊟ **zebrahead** 9 months, 4 weeks ago

Quizlet:C

upvoted 1 times

⊟ **confusion** 1 year, 2 months ago

Selected Answer: D

Global Protect helps helps ADEM, so D.

upvoted 3 times

⊟ **Lapas** 1 year, 3 months ago

Selected Answer: D

Global Protect 100%

upvoted 4 times

⊟ **sguerouate** 1 year, 4 months ago

Selected Answer: D

Global protect

upvoted 3 times

⊟ **Pretorian** 1 year, 9 months ago

Selected Answer: D

GlobalProtect with the ADEM addon for Prisma Access is the correct answer. Absolutely NOT CDL lol

upvoted 5 times

⊟ **AB_SA** 1 year, 11 months ago

I think it should be D. GlobalProtect

upvoted 4 times

Question #6 *Topic 1*

What is a differentiator between the Palo Alto Networks secure access service edge (SASE) solution and competitor solutions?

A. path analysis

B. playbooks

C. ticketing systems

D. inspections

Suggested Answer: *A*

Community vote distribution

A (100%)

confusion 2 months ago

Selected Answer: A

Path analysis in ADEM.

upvoted 2 times

Lapas 3 months, 3 weeks ago

Selected Answer: A

Competitor does not have ADEM.

upvoted 2 times

yet_another_user 6 months ago

Selected Answer: A

I guess, the question relates to ADEM.

upvoted 2 times

Question #7 *Topic 1*

Which secure access service edge (SASE) networking component inspects web-based protocols and traffic to securely connect users to applications?

A. proxy

B. SD-WAN

C. secure web gateway (SWG)

D. cloud access security broker (CASB)

Suggested Answer: *C*

Community vote distribution

C (100%)

Mr_Cipher 1 month, 1 week ago

Should be D. Secure traffic from user to App is CASB

upvoted 1 times

Doobiedoo 3 weeks, 3 days ago

CASB can be more than just Web Based, I think that's why SWG is the answer.

upvoted 1 times

veryboringitstudent 1 month, 3 weeks ago

Selected Answer: C

Should be C

upvoted 1 times

johannes0815 3 months, 3 weeks ago

Selected Answer: C

The secure web gateway (C) is a proxy (A). But I think PANW would like to hear their name --> hence it should be C.

upvoted 1 times

Lapas 9 months, 3 weeks ago

Selected Answer: C

I think the answer is C.

upvoted 3 times

confusion 11 months, 2 weeks ago

Should be C

upvoted 2 times

Question #8 *Topic 1*

What is a benefit of the Palo Alto Networks secure access service edge (SASE) solution's ability to provide insight into SD-WAN and network security metrics while highlighting critical issues across all managed tenants?

A. It rearchitects the way signatures are delivered, performing updates and streaming them to the firewall within seconds after the analysis is done.

B. It helps protect inbound, outbound, and east-west traffic between container workload types in Kubernetes environments without slowing development speed.

C. It simplifies workflows and instantly automates common use cases with hundreds of prebuilt playbooks.

D. It helps managed service providers (MSPs) accelerate troubleshooting and meet service level agreements (SLAs) for all their customers.

Suggested Answer: *D*

Community vote distribution

D (100%)

ArangoTopics 4 months, 3 weeks ago

Selected Answer: D

D make sense, the question says "across all managed tenants"

upvoted 1 times

veryboringitstudent 7 months, 3 weeks ago

Selected Answer: D

Only D makes sense for me

upvoted 1 times

Ajit_Seeker 1 year, 1 month ago

D WOULD BE CORRECT

upvoted 1 times

confusion 1 year, 5 months ago

Selected Answer: D

Probably D

upvoted 1 times

Question #9 *Topic 1*

Which component of the secure access service edge (SASE) solution provides complete session protection, regardless of whether a user is on or off the corporate network?

A. Zero Trust

B. threat prevention

C. single-pass architecture (SPA)

D. DNS Security

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

zebrahead 3 months, 3 weeks ago

Quizlet:A

upvoted 1 times

Ajit_Seeker 7 months, 2 weeks ago

definitely A

upvoted 1 times

MakaraMEAS 9 months, 3 weeks ago

A. Zero Trust.

Zero Trust: A Zero Trust approach to the cloud removes trust assumptions when users, devices and applications connect. A SASE solution will provide complete session protection, regardless of whether a user is on or off the corporate network.

https://www.paloaltonetworks.com/cyberpedia/what-is-sase#:~:text=Zero%20Trust%3A%20A%20Zero%20Trust,or%20off%20the%20corporate%20network.

upvoted 2 times

dbh1 10 months ago

Selected Answer: A

A

https://www.paloaltonetworks.com/cyberpedia/what-is-sase#:~:text=Zero%20Trust%3A%20A%20Zero%20Trust,or%20off%20the%20corporate%20network.

upvoted 3 times

hcir 11 months, 1 week ago

Selected Answer: B

Zero Trust is not a component of SASE, while Threat Prevention is and protects user sessions

upvoted 1 times

hcir 11 months, 1 week ago

Zeto Trust is not a component of PANW SASE, it is a concept and a tool to that helps architect and build security policies. I would go instead with Threat Prevention which is an actual component of PANW SASE

upvoted 1 times

confusion 11 months, 2 weeks ago

Selected Answer: A

Would go for A on this

upvoted 1 times

yet_another_user 12 months ago

Selected Answer: A

Somewhat misleading this question but A is the only what is possible.

upvoted 2 times

Question #10 *Topic 1*

In which step of the Five-Step Methodology of Zero Trust are application access and user access defined?

A. Step 4: Create the Zero Trust Policy

B. Step 3: Architect a Zero Trust Network

C. Step 1: Define the Protect Surface

D. Step 5: Monitor and Maintain the Network

Suggested Answer: *A*

Community vote distribution

A (100%)

ahmaddaghes 5 months, 3 weeks ago

Application access and user access are defined in:

4. Create the Zero Trust Policy

This step involves developing and enforcing policies that specify who can access what resources under what conditions, ensuring that access is granted based on the principle of least privilege.

upvoted 1 times

veryboringitstudent 7 months, 3 weeks ago

I believe this question needs to be reviewed: should be Step 2: Map and Verify Transactions

https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/the-five-step-methodology/step-2-map-the-protect-surface-transaction-flows#id322db094-7ed0-4bcf-a663-58b450d1260c

Step 2: Map and Verify Transactions

Map the transactions between users, applications, and data, so that you can verify and inspect those transactions. Map:
Which applications have access to which critical data.
Which users have access to those applications.
Which users and applications have access to which infrastructure.

Step 4 is Implementation: https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/the-five-step-methodology/step-4-implementation#id8af03732-03e2-404a-9030-dfb63dfabffd

upvoted 1 times

zebrahead 9 months, 3 weeks ago

https://lightstream.io/the-5-step-model-to-implementing-zero-trust/

upvoted 1 times

Lapas 1 year, 3 months ago

I think the correct answer would be Step 2.

upvoted 2 times

hcir 1 year, 5 months ago

Selected Answer: A

In Step 4 you define the security policy based on the Kipling method, which is equivalent to defining user and application access. Step 2 is about defining the flow between users and application/data. Step 3 is about designing the solution and placing the firewalls for micro segmentation

upvoted 3 times

yet_another_user 1 year, 6 months ago

It is step 2, agree with Pretorian comment below. I guess this is a transfer error.

upvoted 2 times

NodummyIQ 1 year, 8 months ago

B. Step 3: Architect a Zero Trust Network

In Step 3 of the Five-Step Methodology of Zero Trust, application access and user access are defined.

upvoted 1 times

Normio 1 year, 10 months ago

Shouldn't it be Step 3? Step 3 is design according to Palo Alto:

Also, there is another question 50 which has step 4 as the solution. Why should they include two questions with the same answer?

upvoted 1 times

Pretorian 1 year, 9 months ago

It's actually "Step 2: Map and Verify Transactions" (not an option) from the document you shared:

"Map the transactions between users, applications, and data, so that you can verify and inspect those transactions. Map:
Which applications have access to which critical data.
Which users have access to those applications.
Which users and applications have access to which infrastructure."

upvoted 4 times

Question #11 *Topic 1*

In the aggregate model, how are bandwidth allocations and interface tags applied beginning in Prisma Access 1.8?

A. License bandwidth is allocated to a CloudGenix controller; interface tags are set with a compute region.

B. License bandwidth is allocated to a compute region; interface tags are set with a CloudGenix controller.

C. License bandwidth is allocated to a compute region; interface tags are set with a Prisma Access location.

D. License bandwidth is allocated to a Prisma Access location; interface tags are set with a compute region.

Suggested Answer: *C*

Community vote distribution

C (100%)

johannes0815 3 months, 3 weeks ago

Selected Answer: C

I think it's C. The only part where I can find something about "tags" is CloudBlades within Prisma Access (and not with CloudGenix): https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/3-1-6/prisma-access-cloudblade-integration-guide-panorama-managed/prisma-access-for-networks-aggregate-bandwidth-licensing/ipsec-termination-node-conventions-and-tag-nomenclature

upvoted 1 times

confusion 8 months, 1 week ago

Selected Answer: C

I go for C here.

upvoted 1 times

Lapas 9 months, 3 weeks ago

Selected Answer: C

Probably C. Refer to https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/2-1-1/prisma-access-cloudblade-integration-guide/prisma-access-for-networks-aggregate-bandwidth-licensing

upvoted 2 times

Question #12 *Topic 1*

Which three decryption methods are available in a security processing node (SPN)? (Choose three.)

A. SSL Outbound Proxy

B. SSHv2 Proxy

C. SSL Forward Proxy

D. SSL Inbound Inspection

E. SSH Inbound Inspection

Suggested Answer: *BCD*

Community vote distribution

BCD (80%) ACD (20%)

⊟ **veryboringitstudent** 1 month, 3 weeks ago

Selected Answer: BCD

Most of times the community helps me a lot, so I'm trying to help too:

In this link already here:

https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/security-services/decryption

First it says:

Strata Cloud Manager provides two types of Decryption policy rules: SSL Forward Proxy to control outbound SSL traffic and SSL Inbound Inspection to control inbound SSL traffic.

But in the end - Decryption at a Glance: it mention the SSH Proxy!

D) Decryption Policies—List of onboarded decryption policies. Review the policy configuration, policy type (SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy), policy action (decrypt or no-decrypt), and BPA Verdict.

So, I believe the correct are B, C, D.

upvoted 2 times

⊟ **confusion** 10 months, 2 weeks ago

Selected Answer: BCD

I believe hcir is correct.

upvoted 1 times

⊟ **raquinopsky** 10 months, 2 weeks ago

Answers correct is B, C, D.

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-concepts

upvoted 3 times

⊟ **hcir** 11 months, 1 week ago

Selected Answer: BCD

ssl forward proxy, ssl inbound inspection and sshv2

upvoted 2 times

⊟ **yet_another_user** 12 months ago

Selected Answer: ACD

Agree with NodummyIQ but another misleading question (SSL outbound and forward proys are actually the same).
https://docs.paloaltonetworks.com/cloud-management/administration/manage-configuration-ngfw-and-prisma-access/security-services/decryption

upvoted 1 times

NodummyIQ 1 year, 2 months ago

A. SSL Outbound Proxy

C. SSL Forward Proxy

D. SSL Inbound Inspection

Option B, SSHv2 Proxy, is not correct because it is not one of the decryption methods available in a security processing node (SPN). While SSHv2 is a secure protocol used for encrypted communication between devices, it is not specifically designed for decryption and inspection of encrypted traffic in the context of an SPN.

upvoted 2 times

Question #13 *Topic 1*

Which App Response Time metric measures the amount of time it takes to transfer incoming data from an external server to a local client?

A. UDP Response Time (UDP-TRT)

B. Server Response Time (SRT)

C. Network Transfer Time (NTTn)

D. Round Trip Time (RTT)

Suggested Answer: *C*

Community vote distribution

C (100%)

raquinopsky Highly Voted 1 year, 4 months ago

Answer is C ---> Network Transfer Time (NTTn) The measure of network congestion. The amount of time it takes to transfer incoming data from an external server to a local client

upvoted 5 times

veryboringitstudent Most Recent 1 month, 3 weeks ago

Selected Answer: C

Network Transfer Time (NTTn)—The measure of network congestion. The amount of time it takes to transfer incoming data from an external server to a local client.

https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/get-started-with-prisma-sd-wan/site-summary-dashboard

upvoted 1 times

sov4 2 months ago

Selected Answer: C

It is C. https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-application-visibility-and-reporting/network-tab/network-activity-charts/app-response-time

upvoted 1 times

zebrahead 3 months, 3 weeks ago

Round Trip Time (RTT)—The measure of network latency. RTT is measured only for TCP flows and defined as the time taken between a forward and return related protocol exchange; TCP SYN to SYN-ACK for outbound flows, TCP SYN-ACK to ACK for inbound flows and the time between a data sequence and ACK of that data sequence.
Thus, RTT is measured throughout the life of a flow and not just at the TCP establishment. Measuring RTT throughout the flows life allows the system to account for TCP proxy devices like WAN optimization in the path, providing a more accurate measurement of RTT.

upvoted 1 times

zebrahead 3 months, 3 weeks ago

Network Transfer Time (NTTn)—The measure of network congestion. The amount of time it takes to transfer incoming data from an external server to a local client.

upvoted 1 times

johannes0815 3 months, 3 weeks ago

Selected Answer: C

C, ref: https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-application-visibility-and-reporting/network-tab/network-activity-charts/app-response-time

upvoted 1 times

Guy100 4 months, 4 weeks ago

C is the correct answer :
Network Transfer Time (NTTn)—The measure of network congestion. The amount of time it takes to transfer incoming data from an external server to a local client.

upvoted 1 times

confusion 8 months, 1 week ago

Selected Answer: C

Network Transfer Time, so C

upvoted 1 times

MakaraMEAS 9 months, 3 weeks ago

Correct answer is C. Network Transfer Time (NTTn).

Network Transfer Time (NTTn) —The measure of network congestion. The amount of time it takes to transfer incoming data from an external server to a local client.

Round Trip Time (RTT) —The measure of network latency. RTT is measured only for TCP flows and defined as the time taken between a forward and return related protocol exchange; TCP SYN to SYN-ACK for outbound flows, TCP SYN-ACK to ACK for inbound flows and the time between a data sequence and ACK of that data sequence.

Thus, RTT is measured throughout the life of a flow and not just at the TCP establishment. Measuring RTT throughout the flows life allows the system to account for TCP proxy devices like WAN optimization in the path, providing a more accurate measurement of RTT.

upvoted 2 times

Lapas 9 months, 3 weeks ago

Selected Answer: C

C 100%

upvoted 2 times

hcir 11 months, 1 week ago

Selected Answer: C

C is correct as per the PSE SASE guide.

upvoted 3 times

customer12341451 11 months, 2 weeks ago

Selected Answer: C

Correct answer is c

upvoted 2 times

AB_SA 1 year, 5 months ago

The correct answer is C. Network Transfer Time (NTTn)

upvoted 2 times

CRG33 1 year, 5 months ago

I believe D is correct RTT, based on the link shared by PedramGZ21. The NTTn is based on The measure of network congestion.

upvoted 2 times

edineme 1 year, 5 months ago

Selected Answer: C

C is the correct answer.

upvoted 2 times

PedramGZ21 1 year, 6 months ago

I believe the answer is C.

https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-application-visibility-and-reporting/network-tab/network-activity-charts/app-response-time

upvoted 3 times

Question #14 *Topic 1*

Which two prerequisites must an environment meet to onboard Prisma Access mobile users? (Choose two.)

A. Zoning must be configured to require a user ID for the mobile users trust zone.

B. Mapping of trust and untrust zones must be configured.

C. BGP must be configured so that service connection networks can be advertised to the mobile gateways.

D. Mobile user subnet and DNS portal name must be configured.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

Toubster Highly Voted 2 years, 1 month ago

Selected Answer: BD

https://youtu.be/gGwFvi8rvqU?t=1456

upvoted 8 times

edineme Highly Voted 1 year, 11 months ago

Selected Answer: BD

B & D:

https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-users/globalprotect-prisma-access/configure-prisma-access-for-users

upvoted 6 times

StevenWilliams0728 Most Recent 3 months, 1 week ago

answer is B and D according to the content in palo alto beacon digital training.

upvoted 1 times

examtopics2234 6 months ago

Selected Answer: BD

It's BD. You can't configure User ID in Zone for Prisma Access. Zone are used only to differenciate Trust from Untrust

upvoted 1 times

zebrahead 9 months, 4 weeks ago

Quizlet:A,D

upvoted 1 times

confusion 1 year, 2 months ago

Selected Answer: BD

BD for sure

upvoted 1 times

MakaraMEAS 1 year, 3 months ago

Answer: BD.

You must map the zones you use within your organization as trust or untrust so that Prisma Access for users can translate the policy rules you push to the cloud service to the internal zones within the networking infrastructure.

upvoted 2 times

Question #15 *Topic 1*

How does SaaS Security Inline help prevent the data security risks of unsanctioned security-as-a-service (SaaS) application usage on a network?

A. It provides mobility solutions and/or large-scale virtual private network (VPN) capabilities.

B. It offers risk scoring, analytics, reporting, and Security policy rule authoring.

C. It provides built-in external dynamic lists (EDLs) that secure the network against malicious hosts.

D. It prevents credential theft by controlling sites to which users can submit their corporate credentials.

Suggested Answer: *B*

Community vote distribution

B (100%)

PedramGZ21 Highly Voted 2 years ago

The answer should be B according to Study Guide and the link below:
SaaS Inline Security is a security service that offers advanced risk scoring, analytics, reporting and
security policy rule authoring so that your organization has the SaaS visibility and security controls to
prevent data security risks of unsanctioned SaaS app usage on your network.
https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline/get-started-with-saas-security-inline/whats-saas-security-inline#idf9f840a9-055f-4320-9c1f-b0e46e5f4eed

upvoted 6 times

examtopics2234 Most Recent 6 months ago

Selected Answer: B

Should be B, SAAS doesn't provide EDL

upvoted 1 times

zebrahead 9 months, 4 weeks ago

Quizlet:C

upvoted 1 times

confusion 1 year, 4 months ago

Selected Answer: B

https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline
SaaS Security Inline is a security service that offers advanced risk scoring, analytics, reporting, and Security policy rule authoring so that your organization has the SaaS visibility and security controls to prevent data security risks of unsanctioned SaaS app usage on your network.

upvoted 1 times

hcir 1 year, 5 months ago

Selected Answer: B

B as per the study guide

upvoted 2 times

NodummyIQ 1 year, 8 months ago

D. It prevents credential theft by controlling sites to which users can submit their corporate credentials.SaaS Security Inline helps prevent the data security risks of unsanctioned security-as-a-service (SaaS) application usage on a network by preventing credential theft.

upvoted 1 times

Ac1d_ 1 year, 11 months ago

Selected Answer: B

Agree with PedramGZ21 it should be B.
EDL's is just a "static" list with IOC (IPs, URLs), it doesn't necessarily say anything about SaaS apps.

upvoted 4 times

Question #16 *Topic 1*

Which two point products are consolidated into the Prisma secure access service edge (SASE) platform? (Choose two.)

A. Autonomous Digital Experience Management (ADEM)

B. firewall as a service (FWaaS)

C. Threat Intelligence Platform (TIP)

D. security information and event management (SIEM)

Suggested Answer: *AB*

Community vote distribution

AB (100%)

Doobiedoo 6 months, 1 week ago

Selected Answer: AB

A and B are correct.

upvoted 1 times

Question #17 *Topic 1*

Which element of Prisma Access enables both mobile users and users at branch networks to access resources in headquarters or a data center?

A. User-ID

B. private clouds

C. App-ID

D. service connections

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **veryboringitstudent** 1 month, 3 weeks ago

Selected Answer: D

D 1000%

upvoted 1 times

⊟ **confusion** 8 months, 1 week ago

Selected Answer: D

DC = service connection

upvoted 2 times

⊟ **Lapas** 9 months, 3 weeks ago

Selected Answer: D

D 100%

upvoted 2 times

Question #18 *Topic 1*

Organizations that require remote browser isolation (RBI) to protect their users can automate connectivity to third-party RBI products with which platform?

A. Zero Trust

B. SaaS Security API

C. GlobalProtect

D. CloudBlades API

Suggested Answer: *D*

Community vote distribution

D (79%) B (21%)

Toubster Highly Voted 2 years, 1 month ago

Selected Answer: D

https://www.paloaltonetworks.com/blog/sase/remote-browser-isolation/

upvoted 8 times

zebrahead Most Recent 9 months, 4 weeks ago

Quizlet:A

upvoted 1 times

gemghdpm 8 months, 1 week ago

@ Zebrahead can we trust quizlet answers because i have some doubt in it

upvoted 1 times

Ironman_2022 6 months, 2 weeks ago

Nope I dont trust their answers.

upvoted 1 times

Guy100 11 months ago

B - the question is about the platform - ZTNA is a concept Cloud Blades is a platform - B

upvoted 1 times

confusion 1 year, 2 months ago

Selected Answer: D

automation = CloudBlades, so D

upvoted 1 times

hcir 1 year, 5 months ago

Selected Answer: D

the role of Cloudblades is to integrate third-party solutions with Prisma Access!

upvoted 2 times

oraziox 1 year, 8 months ago

Selected Answer: B

Cloudblades API

upvoted 3 times

Question #19 *Topic 1*

What is an advantage of the unified approach of the Palo Alto Networks secure access service edge (SASE) platform over the use of multiple point products?

A. It allows for automation of ticketing tasks and management of tickets without pivoting between various consoles.

B. It scans all traffic, ports, and protocols and automatically discovers new apps.

C. It turns threat intelligence and external attack surface data into an intelligent data foundation to dramatically accelerate threat response.

D. It reduces network and security complexity while increasing organizational agility.

Suggested Answer: *D*

Community vote distribution

D (100%)

sov4 2 months ago

Selected Answer: D

https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna

upvoted 1 times

nobody165456131354 2 months, 3 weeks ago

Selected Answer: D

correct

upvoted 1 times

Question #20 Topic 1

How does Autonomous Digital Experience Management (ADEM) improve user experience?

A. The root cause of any alert can be viewed with a single click, allowing users to swiftly stop attacks across the environment.

B. The virtual appliance receives and stores firewall logs without using a local Log Collector, simplifying required steps users must take.

C. Working from home or branch offices, all users get the benefit of a digital experience management solution without the complexity of installing additional software and hardware.

D. It applies in-depth hunting and forensics knowledge to identify and contain threats before they become a breach.

Suggested Answer: *C*

Community vote distribution

C (100%)

veryboringitstudent 1 month, 3 weeks ago

Selected Answer: C

Indeed, C

https://www.paloaltonetworks.com/cyberpedia/what-is-sase

upvoted 1 times

sov4 2 months ago

Selected Answer: C

https://www.paloaltonetworks.com/cyberpedia/what-is-sase

upvoted 1 times

Question #21 *Topic 1*

What are two ways service connections and remote network connections differ? (Choose two.)

A. Remote network connections provide secondary WAN options, but service connections use backup service connection for redundancy.

B. Remote network connections enforce security policies, but service connections do not.

C. An on-premises resource cannot originate a connection to the internet over a service connection.

D. Service connections support both OSPF and BGP for routing protocols, but remote networks support only BGP.

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

CRG33 Highly Voted 👍 1 year, 11 months ago

I think it's BC that's correct. (B because SC-CAN's do NOT provide security enforcement and C, because a session cannot be initiated through an SC-CAN to the I-net)

upvoted 8 times

Helloory Highly Voted 👍 1 year, 10 months ago

Correct answers are B and C

upvoted 5 times

MILOP88 Most Recent 2 months, 3 weeks ago

B and C

upvoted 1 times

examtopics2234 6 months ago

Selected Answer: B

It's only B : SC-CAN can NOT provide Security Enforcement, only MU or RN can.

it is possible to initiate session from SC to RN/MU so C is wrong

upvoted 1 times

Ironman_2022 6 months, 2 weeks ago

Agree B and C

upvoted 1 times

Ironman_2022 6 months, 3 weeks ago

I would agree BC

upvoted 1 times

NGCS 9 months, 3 weeks ago

B and C

upvoted 1 times

Ajit_Seeker 1 year, 1 month ago

b c ARE CORRECT

upvoted 1 times

Ajit_Seeker 1 year, 1 month ago

b & c are correct

upvoted 1 times

dbh1 1 year, 4 months ago

Selected Answer: B

B , C !!!

upvoted 2 times

mushi4ka 1 year, 7 months ago

Selected Answer: A

A&B

https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-connections/service-connection-routing

upvoted 1 times

froggy2638 1 year, 7 months ago

Selected Answer: B

BC is correct

upvoted 4 times

raquinopsky 1 year, 10 months ago

I think the answer is --> B, C

upvoted 3 times

Toubster 2 years, 1 month ago

I think AB is right.

upvoted 4 times

Question #22 *Topic 1*

What can prevent users from unknowingly downloading potentially malicious file types from the internet?

A. Apply a File Blocking profile to Security policy rules that allow general web access.

B. Apply a Zone Protection profile to the untrust zone.

C. Assign an Antivirus profile to Security policy rules that deny general web access.

D. Assign a Vulnerability profile to Security policy rules that deny general web access.

Suggested Answer: *A*

Community vote distribution

A (100%)

zebrahead 3 months, 3 weeks ago

Selected Answer: A

https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-file-blocking
For policy rules that allow general web browsing, be stricter with your file blocking because the risk of users unknowingly downloading malicious files is much higher.

upvoted 1 times

confusion 11 months, 2 weeks ago

Selected Answer: A

A, Security profiles are ONLY processed if rule action is allow!

upvoted 2 times

Question #23 *Topic 1*

Text of question will be provided later...A. It applies configuration changes and provides credential management, role-based controls, and a playbook repository.

B. It provides customized forms to collect and validate necessary parameters from the requester.

C. It natively ingests, normalizes, and integrates granular data across the security infrastructure at nearly half the cost of legacy security products attempting to solve the problem.

D. It provides IT teams with single-pane visibility that leverages endpoint, simulated, and real-time user traffic data to provide the most complete picture of user traffic flows possible.

Suggested Answer: *D*

Community vote distribution

D (100%)

ArangoTopics 4 months, 2 weeks ago

Agree with Passam, the question is:

How does Autonomous Digital Experience Management (ADEM) simplify troubleshooting?

upvoted 1 times

Passam 1 year, 3 months ago

Question is something like

How does Autonomous Digital Experience Management (ADEM) simplify troubleshooting?

upvoted 2 times

confusion 1 year, 5 months ago

Selected Answer: D

Question should be this:

What is feature of Autonomous Digital Experience Management (ADEM)?

Answer should be D.

upvoted 1 times

ExamBunnie 1 year, 11 months ago

https://www.paloaltonetworks.com/blog/sase/prisma-sase-adem-simplify-network-troubleshooting-for-the-hybrid-workforce/

Its about ADEM:

ADEM uplevels your IT teams with easy-to-use single-pane visibility that leverages endpoint, simulated, and real-time user traffic data to provide the most complete picture of user traffic flows possible.

upvoted 3 times

nchunter 2 years ago

does anybody know what the question is on this?

upvoted 2 times

Question #24 *Topic 1*

How can a network engineer export all flow logs and security actions to a security information and event management (SIEM) system?

A. Enable syslog on the Instant-On Network (ION) device.

B. Use a zone-based firewall to export directly through application program interface (API) to the SIEM.

C. Enable Simple Network Management Protocol (SNMP) on the Instant-On Network (ION) device.

D. Use the centralized flow data-export tool built into the controller.

Suggested Answer: *A*

Community vote distribution

A (100%)

confusion 5 months, 1 week ago

Selected Answer: A

Should be A, SNMP is also supported.

upvoted 1 times

yet_another_user 6 months ago

Selected Answer: A

Regarding link from docu below, it should be Syslog. However, SNMP is supported too.
https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-sites-and-devices/use-external-services-for-monitoring/syslog-server-support-in-prisma-sd-wan

upvoted 2 times

Question #25 *Topic 1*

Users connect to a server in the data center for file sharing. The organization wants to decrypt the traffic to this server in order to scan the files being uploaded and downloaded to determine if malware or sensitive data is being moved by users.
Which proxy should be used to decrypt this traffic?

A. SCP Proxy

B. SSL Inbound Proxy

C. SSH Forward Proxy

D. SSL Forward Proxy

Suggested Answer: *D*

Community vote distribution

D (63%) B (38%)

⊟ **Normio** Highly Voted 1 year, 10 months ago

SSL Inbound Proxy ecryption mode can only work if you have control on the targeted Web Server certificate to be allow to import Key Pair on Palo Alto Networks Device. That's why this decryption mode is often use to decrypt SSL inbound traffic to Internal Web Server.

Since in the question they talk about IN THE DATA CENTER, it needs to be this one.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV8CAK

upvoted 5 times

⊟ **ArangoTopics** Most Recent 4 months, 3 weeks ago

Selected Answer: D

SSL Inbound inspection not even exist. The decryption on this scenario it's applied to users when they access to the server.

upvoted 1 times

⊟ **Doobiedoo** 6 months, 1 week ago

Selected Answer: D

The real answer is "SSL Forward Proxy" on the Mobile User policy, for two reasons.

1) SSL Inbound Proxy is not a real thing. It is SSL Inbound Inspection, and it does not PROXY any connections; the client connects directly to the server and there is no man-in-the-middle proxy from the firewall.
2) The question mentions "DC/datacenter" and with Prisma Access you will have these deployed as Service Connections 99% of the time. Service Connections do not support policies like decryption, nat, and security.

upvoted 1 times

⊟ **sov4** 8 months ago

Selected Answer: D

D. SSL Forward Proxy. SSL inbound proxy isnt a thing... it's SSL inbound inspection.

upvoted 1 times

⊟ **JohnPalo** 10 months ago

Selected Answer: D

Since it's referring to internal users and SC-CAN do not enforce security, it would be SSL outbound proxy, that hits the users connecting from remote networks or as Mobile Users.

upvoted 2 times

⊟ **Pretorian** 1 year, 9 months ago

Selected Answer: B

Choosing "B" although SSL Inbound INSPECTION is not a proxy.

upvoted 3 times

Question #26 *Topic 1*

Which two actions take place after Prisma SD-WAN Instant-On Network (ION) devices have been deployed at a site? (Choose two.)

A. The devices continually sync the information from directories, whether they are on-premise, cloud-based, or hybrid.

B. The devices establish VPNs over private WAN circuits that share a common service provider.

C. The devices automatically establish a VPN to the data centers over every internet circuit.

D. The devices provide an abstraction layer between the Prisma SD-WAN controller and a particular cloud service.

Suggested Answer: *BC*

Community vote distribution

BC (83%) CD (17%)

yet_another_user Highly Voted 👍 12 months ago

Selected Answer: BC

Apologize for typo, it is B and C

upvoted 5 times

NixonSS Most Recent ⏲ 2 months ago

Selected Answer: BC

After you deploy the Prisma SD-WAN ION devices at your sites, the devices automatically establish a VPN to the data centers over every internet circuit. Additionally, the ION devices establish VPNs over private WAN circuits that share a common service provider.
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/sase-securing-internet-design-guide

upvoted 3 times

confusion 11 months, 2 weeks ago

Selected Answer: BC

Link from yet_another_user is correct, answer is B&C

upvoted 2 times

yet_another_user 12 months ago

Selected Answer: CD

Please refer to this guide, page 14
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/sase-securing-internet-design-guide

upvoted 2 times

Question #27

Topic 1

Cloud-delivered App-ID provides specific identification of which two applications? (Choose two.)

A. unknown-tcp

B. private

C. web-browsing

D. custom

Suggested Answer: *AC*

Community vote distribution

AC (100%)

NixonSS 2 months ago

Selected Answer: AC

Cloud-delivered App-IDs do not identify other types of public applications and do not identify private and custom applications.

upvoted 1 times

zebrahead 3 months, 3 weeks ago

Selected Answer: AC

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/app-id-features/cloud-based-app-id

Traditional, content-delivered App-ID only delivers new applications once per month and you need to analyze the new App-IDs before you install them to understand changes that they may make to Security policy rules. The monthly cadence and need for analysis slows down the adoption of new App-IDs in policy. ACE changes that scenario by providing on-demand App-IDs for SaaS applications identified as:

ssl

web-browsing

unknown-tcp

unknown-udp

upvoted 2 times

confusion 11 months, 2 weeks ago

Selected Answer: AC

unknown-tcp + web-browsing, as others can actually be a variable

upvoted 1 times

Question #28 *Topic 1*

Which connection method allows secure web gateway (SWG) access to internet-based SaaS applications using HTTP and HTTPS protocols?

A. GlobalProtect

B. Broker VM

C. explicit proxy

D. system-wide proxy

Suggested Answer: *C*

Community vote distribution

C (100%)

Homayounm Highly Voted 2 years ago

I think it is Explicit Proxy.

upvoted 7 times

PedramGZ21 Highly Voted 2 years ago

I think the Correct answer is C. Explicit Proxy

https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/explicit-proxy/explicit-proxy-guidelines

upvoted 5 times

ArangoTopics Most Recent 4 months, 3 weeks ago

Maybe I'm wrong but the question says Connection Method

Prisma Access offers two connection methods to secure mobile users: users can connect to Prisma Access using the GlobalProtect App or using a Proxy Auto-Configuration (PAC) file

https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users

At this point the connection method is GP, answer should be A

upvoted 1 times

zebrahead 9 months, 4 weeks ago

Selected Answer: C

https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users

upvoted 1 times

dbh1 1 year, 4 months ago

Selected Answer: C

its Explicit PROXY

upvoted 2 times

confusion 1 year, 5 months ago

Selected Answer: C

C. Explicit proxy

upvoted 1 times

froggy2638 1 year, 7 months ago

Selected Answer: C

the answer is explicit proxy

upvoted 3 times

CRG33 1 year, 11 months ago

I also think the Correct answer is C. Explicit Proxy https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/explicit-proxy/explicit-proxy-how-it-works

upvoted 4 times

Question #29 *Topic 1*

Which element of a secure access service edge (SASE)-enabled network uses many points of presence to reduce latency with support of in-country or in-region resources and regulatory requirements?

A. cloud-native, cloud-based delivery

B. converged WAN edge and network security

C. broad network-edge support

D. identity and network location

Suggested Answer: *A*

Community vote distribution

A (100%)

Doobiedoo 6 months, 1 week ago

Selected Answer: A

"cloud-native, cloud-based delivery"

It's the only one that makes sense. They are refering to the 200+ Mobile User nodes world-wide, and the different Compute Regions. The Mobile User nodes allow for in-country internet access (which give local web pages like users in France get French pages, German users get German pages).

For Compute Regions, they are placed strategically to allow you to meet latency and also regulatory compliance within different countries around the world.

upvoted 1 times