Question #1 *Topic 1*

Which Cloud-Delivered Security Services (CDSS) solution is required to configure and enable Advanced DNS Security?

A. Advanced WildFire

B. Enterprise SaaS Security

C. Advanced Threat Prevention

D. Advanced URL Filtering

Correct Answer: *C*

Community vote distribution

D (100%)

maffo02 1 month ago

Selected Answer: D

D. Advanced URL Filtering includes DNS Security as part of its capabilities, making it the correct choice.

upvoted 1 times

Question #2 *Topic 1*

Which statement best demonstrates a fundamental difference between Content-ID and traditional network security methods?

A. Content-ID inspects traffic at the application layer to provide real-time threat protection.

B. Content-ID focuses on blocking malicious IP addresses and ports.

C. Traditional methods provide comprehensive application layer inspection.

D. Traditional methods block specific applications using signatures.

Correct Answer: *A*

Community vote distribution

A (100%)

maffo02 1 month ago

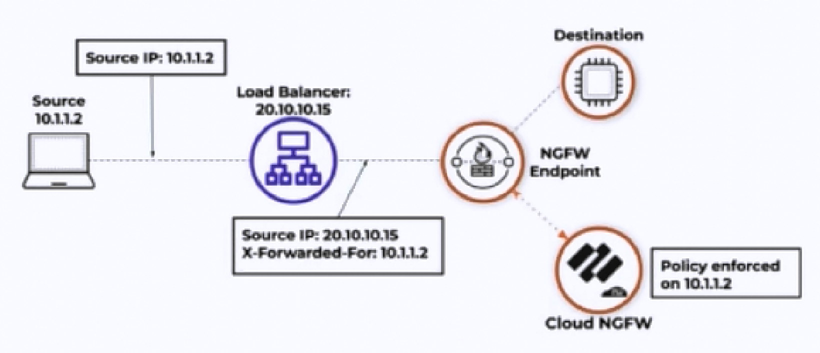
Selected Answer: A

A is the best answer because it highlights Content-ID’s application-layer inspection capability, which traditional methods lack.

upvoted 1 times

Question #3 *Topic 1*

Based on the image below, which source IP address will be seen in the data filtering logs of the Cloud NGFW for AWS with the default rulestack settings?



A. 10.1.1.3

B. 20.10.10.16

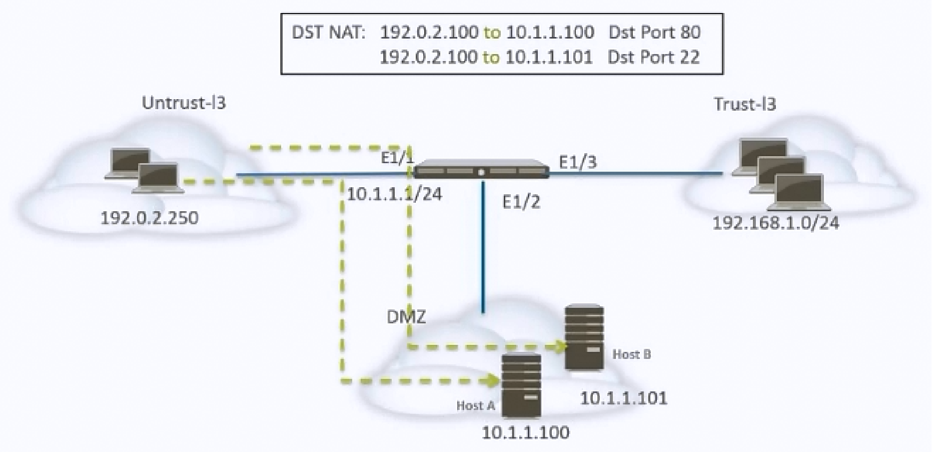
C. 20.10.10.15

D. 10.1.1.2

Correct Answer: *C*

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

Question #4 *Topic 1*



A network administrator is using DNAT to map two servers to one public IP address. Traffic will be directed to a specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.
Which two sets of Security policy rules will accomplish this configuration? (Choose two.)

A. Source: Untrust (Any)

Destination: Untrust -

Application(s): web-browsing -
Action: allow

B. Source: Untrust (Any)

Destination: Trust -
Application(s): web-browsing, ssh
Action: allow

C. Source: Untrust (Any)

Destination: DMZ -

Application(s): web-browsing -
Action: allow

D. Source: Untrust (Any)

Destination: DMZ -

Application(s): ssh -
Action: allow

Correct Answer: *CD*

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

Question #5 *Topic 1*

Which two configurations are required when creating deployment profiles to migrate a perpetual VM-Series firewall to a flexible VM? (Choose two.)

A. Choose "Fixed vCPU Models" for configuration type.

B. Allocate the same number of vCPUs as the perpetual VM.

C. Deploy virtual Panorama for management.

D. Allow only the same security services as the perpetual VM.

Correct Answer: *AB*

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

Question #6 *Topic 1*

What is the primary role of Advanced DNS Security in protecting against DNS-based threats?

A. It replaces traditional DNS servers with more reliable and secure ones.

B. It centralizes all DNS management and simplifies policy creation.

C. It automatically redirects all DNS traffic through encrypted tunnels.

D. It uses machine learning (ML) to detect and block malicious domains in real-time.

Correct Answer: *D*

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

Question #7 *Topic 1*

When a firewall acts as an application-level gateway (ALG), what does it require in order to establish a connection?

A. Pinholes

B. Dynamic IP and Port (DIPP)

C. Session Initiation Protocol (SIP)

D. Payload

Correct Answer: *A*

Community vote distribution

D (100%)

Dre330 3 weeks, 2 days ago

Selected Answer: D

I agree

upvoted 1 times

maffo02 1 month ago

Selected Answer: D

When a firewall functions as an Application-Level Gateway (ALG), it must inspect the payload (actual content) of network traffic to:

Understand application-layer protocols (e.g., FTP, SIP, SQL) embedded within the packet.

Dynamically open and close ports as needed (e.g., for FTP data connections or VoIP calls).

Modify packet headers/payloads when necessary (e.g., NAT traversal for SIP).

upvoted 2 times

Question #8 *Topic 1*

In which mode should an ION device be configured at a newly acquired site to allow site traffic to be audited without steering traffic?

A. Access

B. Control

C. Disabled

D. Analytics

Correct Answer: *D*

Community vote distribution

D (100%)

maffo02 1 month ago

Selected Answer: D

Analytics mode is the correct choice because:

It allows the device to monitor and audit traffic passively without impacting or steering the traffic flow.

Provides visibility into network performance, application usage, and potential issues before implementing traffic policies.

Does not enforce any routing or security policies, making it ideal for initial assessment.

upvoted 1 times

Question #9 *Topic 1*

A company has an ongoing initiative to monitor and control IT-sanctioned SaaS applications. To be successful, it will require configuration of decryption policies, along with data filtering and URL Filtering Profiles used in Security policies.
Based on the need to decrypt SaaS applications, which two steps are appropriate to ensure success? (Choose two.)

A. Validate which certificates will be used to establish trust.

B. Configure SSL Forward Proxy.

C. Create new self-signed certificates to use for decryption.

D. Configure SSL Inbound Inspection.

Correct Answer: *AB*

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

Question #10 *Topic 1*

A firewall administrator wants to segment the network traffic and prevent noncritical assets from being able to access critical assets on the network.
Which action should the administrator take to ensure the critical assets are in a separate zone from the noncritical assets?

A. Create a deny Security policy with "any" set for both the source and destination zones.

B. Create an allow Security policy with "any" set for both the source and destination zones.

C. Logically separate physical and virtual interfaces to control the traffic that passes across the interface.

D. Assign a single interface to multiple security zones.

Correct Answer: *C*

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

Question #11 *Topic 1*

With Strata Cloud Manager (SCM), which action will efficiently manage Security policies across multiple cloud providers and on-premises data centers?

A. Use snippets and folders to define and enforce uniform Security policies across environments.

B. Use the "Feature Adoption" visibility tab on a weekly basis to make adjustments across the network.

C. Allow each cloud provider's native security tools to handle policy enforcement independently.

D. Create and manage separate Security policies for each environment to address specific needs.

Correct Answer: *A*

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

Question #12 *Topic 1*

How are content updates downloaded and installed for Cloud NGFWs?

A. Through the management console

B. Through Panorama

C. Automatically

D. From the Customer Support Portal

Correct Answer: *C*

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

Question #13 *Topic 1*

Which two components of a Security policy, when configured, allow third-party contractors access to internal applications outside business hours? (Choose two.)

A. User-ID

B. Schedule

C. Service

D. App-ID

Correct Answer: *AB*

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

Question #14 *Topic 1*

Which action is only taken during slow path in the NGFW policy?

A. Session lookup

B. SSL/TLS decryption

C. Layer 2-Layer 4 firewall processing

D. Security policy lookup

Correct Answer: *B*

Community vote distribution

D (100%)

cncpower 2 weeks, 3 days ago

Selected Answer: D

Security Policy lookup

upvoted 1 times

Question #15 *Topic 1*

Which Security profile should be queried when investigating logs for upload attempts that were recently blocked due to sensitive information leaks?

A. Anti-spyware

B. Data Filtering

C. Antivirus

D. URL Filtering

Correct Answer: *B*

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

Question #16

Topic 1

Which two content updates can be pushed to next-generation firewalls from Panorama? (Choose two.)

A. GlobalProtect data file

B. WildFire

C. Advanced URL Filtering

D. Applications and threats

Correct Answer: *BD*

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

Question #17 *Topic 1*

A security administrator is adding a new sanctioned cloud application to SaaS Data Security.
After authentication, how does the tool gain API access for monitoring?

A. It transmits the configured SAML user profile to the cloud application for security event attribution.

B. It establishes an encrypted key pair with the cloud application to safely transmit user data.

C. It generates a certificate and sends it to the cloud application for TLS decryption and inspection.

D. It receives a token from the cloud application for establishing and maintaining a secure connection.

Correct Answer: *D*

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

Question #18 *Topic 1*

When using the perfect forward secrecy (PFS) key exchange, how does a firewall behave when SSL Inbound Inspection is enabled?

A. It acts as meddler-in-the-middle between the client and the internal server.

B. It acts transparently between the client and the internal server.

C. It decrypts inbound and outbound SSH connections.

D. It decrypts traffic between the client and the external server.

Correct Answer: *A*

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

Question #19 *Topic 1*

Which feature is available in both Panorama and Strata Cloud Manager (SCM)?

A. Template stacks

B. Configuration snippets

C. Policy Optimizer

D. Plug-ins

Correct Answer: *C*

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

Question #20 *Topic 1*

Infrastructure performance issues and resource constraints have prompted a firewall administrator to monitor hardware NGFW resource statistics. Which AIOps feature allows the administrator to review these statistics for each firewall in the environment?

A. Capacity Analyzer

B. Host information profile (HIP)

C. Policy Analyzer

D. Security Posture Insights

Correct Answer: *A*

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

Question #21 *Topic 1*

What should be reviewed when log forwarding from an NGFW to Strata Logging Service becomes disconnected?

A. Device certificates

B. Decryption profile

C. Auth codes

D. Software warranty

Correct Answer: *C*

Community vote distribution

A (100%)

maffo02 1 month ago

Selected Answer: A

When log forwarding from an NGFW to Strata Logging Service (SLS) fails or disconnects, the most likely issue is related to authentication and secure communication, which relies on:

Device Certificates – SLS uses certificates to verify the identity of the NGFW. If the certificate is expired, invalid, or misconfigured, log forwarding will break.

Connectivity & Permissions – Ensure the firewall has proper outbound internet access (TCP/443) to SLS.

upvoted 2 times

Question #22 *Topic 1*

In Prisma SD-WAN, what is the recommended initial action when VoIP traffic experiences high latency and packet loss during business hours?

A. Configure a new VPN gateway connection.

B. Monitor real-time path performance metrics.

C. Add new link tags to existing interfaces.

D. Disable the most recently created path quality.

Correct Answer: *B*

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

Question #23 *Topic 1*

Which action in the Customer Support Portal is required to generate authorization codes for Software NGFWs?

A. Create a deployment profile.

B. Use the Enterprise Support Agreement (ESA) authorization code.

C. Register the device with the cloud service provider.

D. Download authorization codes from the public cloud marketplace.

Correct Answer: *A*

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

Question #24 *Topic 1*

Which type of traffic can a firewall use for proper classification and visibility of internet of things (IoT) devices?

A. DHCP

B. RTP

C. RADIUS

D. SSH

Correct Answer: *A*

Community vote distribution

A (100%)

maffo02 1 month ago

Selected Answer: A

IoT devices often use DHCP to obtain IP addresses.

upvoted 1 times

Question #25 *Topic 1*

A hospital system allows mobile medical imaging trailers to connect directly to the internal network of its various campuses. The network security team is concerned about this direct connection and wants to begin implementing a Zero Trust approach in the flat network.
Which solution provides cost-effective network segmentation and security enforcement in this scenario?

A. Deploy edge firewalls at each campus entry point to monitor and control various traffic types through direct connection with the trailers.

B. Manually inspect large images like holograms and MRIs, but permit smaller images to pass freely through the campus core firewalls.

C. Configure separate zones to isolate the imaging trailer's traffic and apply enforcement using the existing campus core firewalls.

D. Configure access control lists on the campus core switches to control and inspect traffic based on image size, type, and frequency.

Correct Answer: *C*

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

Question #26 *Topic 1*

An IT security administrator is maintaining connectivity and security between on-premises infrastructure, private cloud, and public cloud environments in Strata Cloud Manager (SCM).
Which set of practices must be implemented to effectively manage certificates and ensure secure communication across these segmented environments?

A. Use a centralized certificate management solution.
Regularly renew and update certificates.
Employ strong encryption protocols.

B. Use self-signed certificates for all environments.
Renew certificates manually once a year.
Avoid automating certificate management to maintain control.

C. Rely on the cloud provider's default certificates.
Avoid renewing certificates to reduce overhead and complexity.
Manage certificate deployment manually.

D. Implement different certificate authorities (CAs) for each environment.
Use default certificate settings.
Renew certificates only when they expire to reduce overhead and complexity.

Correct Answer: *A*

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

Question #27 *Topic 1*

Which step is necessary to ensure an organization is using the inline cloud analysis features in its Advanced Threat Prevention subscription?

A. Configure Advanced Threat Prevention profiles with default settings and only focus on high-risk traffic to avoid affecting network performance.

B. Enable SSL decryption in Security policies to inspect and analyze encrypted traffic for threats.

C. Update or create a new anti-spyware security profile and enable the appropriate local deep learning models.

D. Disable anti-spyware to avoid performance impacts and rely solely on external threat intelligence.

Correct Answer: *B*

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

Question #28

Topic 1

Which network design for internet of things (IoT) Security allows traffic mirroring from the switch to a TAP interface on the firewall to monitor traffic not otherwise seen?

A. DHCP server on firewall

B. Firewall as DHCP relay

C. Firewall in DHCP path

D. Firewall outside DHCP path

Correct Answer: *D*

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

Question #29 *Topic 1*

What is the most efficient way in Strata Cloud Manager (SCM) to apply a Security policy to all ten firewalls in one data center?

A. Create the Security policy on each firewall individually.

B. Set the configuration scope to "Global" and create the Security policy.

C. Create the Security policy at any configuration scope, then clone it to the ten firewalls.

D. Create a folder that groups the ten firewalls together, then create the Security policy at that configuration scope.

Correct Answer: *D*

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