

Latest Version: 26.0

Question: 1

What happens to traffic traversing SD-WAN fabric that doesn't match any SD-WAN policies?

- A. Traffic is dropped because there is no matching SD-WAN policy to direct traffic.
- B. Traffic matches a catch-all policy that is created through the SD-WAN plugin.
- C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.
- D. Traffic is forwarded to the first physical interface participating in SD-WAN based on lowest interface number (i.e., Eth1/1 over Eth1/3).

Answer: C

Explanation:

If there is no match to any SD-WAN policy rule in the list, the session matches an implied SD-WAN policy rule at the end of the list that uses the round-robin method to distribute unmatched sessions among all links in one SD-WAN interface, which is based on the route lookup.

Question: 2

What are three reasons for excluding a site from SSL decryption? (Choose three.)

- A. the website is not present in English
- B. unsupported ciphers
- C. certificate pinning
- D. unsupported browser version
- E. mutual authentication

Answer: BCE

Explanation:

Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption.html>

Question: 3

DRAG DROP

Place the steps to onboard a ZTP firewall into Panorama/CSP/ZTP-Service in the correct order.

Installer or IT administrator registers ZTP firewalls by adding them to Panorama using firewall serial number and claim key.

After connecting to the internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service.

The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.

The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls.

Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service.



[Empty dashed box]

FIRST

[Empty dashed box]

SECOND

[Empty dashed box]

THIRD

[Empty dashed box]

FOURTH

[Empty dashed box]

FIFTH

Answer:

Installer or IT administrator registers ZTP firewalls by adding them to Panorama using firewall serial number and claim key.

FIRST

Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service.

SECOND

After connecting to the internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service.

THIRD

The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls.

FOURTH

The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.

FIFTH

Explanation:
<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/set-up-zero-touch->

Question: 4

An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infrastructure?

- A. To comply with data privacy regulations, WildFire signatures and verdicts are not shared globally.
- B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
- C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
- D. The WildFire Global Cloud only provides bare metal analysis.

Answer: C

Question: 5

A company wants to use their Active Directory groups to simplify their Security policy creation from Panorama.

Which configuration is necessary to retrieve groups from Panorama?

- A. Configure an LDAP Server profile and enable the User-ID service on the management interface.
- B. Configure a group mapping profile to retrieve the groups in the target template.
- C. Configure a Data Redistribution Agent to receive IP User Mappings from User-ID agents.
- D. Configure a master device within the device groups.

Answer: D

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFQCA0>