Free Questions for PCNSE by certsinside

Shared by Sutton on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.

What should an administrator configure to route interesting traffic through the VPN tunnel?

Options:

A- Proxy IDs

B- GRE Encapsulation

C- Tunnel Monitor

D- ToS Header

Answer:

A

Explanation:

An administrator should configure proxy IDs to route interesting traffic through the VPN tunnel when the peer device is a policy-based VPN device. Proxy IDs are used to identify the traffic that belongs to a particular IPSec VPN and to direct it to the appropriate tunnel. Proxy IDs consist of a local IP address, a remote IP address, and an application (protocol and port numbers). Each proxy ID is considered to be a VPN tunnel and is counted towards the IPSec VPN tunnel capacity of the firewall. Proxy IDs are required for IKEv1 VPNs and optional for IKEv2 VPNs. If the proxy ID is not configured, the firewall uses the default values of source IP: 0.0.0.0/0, destination IP: 0.0.0.0/0, and application: any, which may not match the peer's policy and result in a failure to establish the VPN connection.Reference:

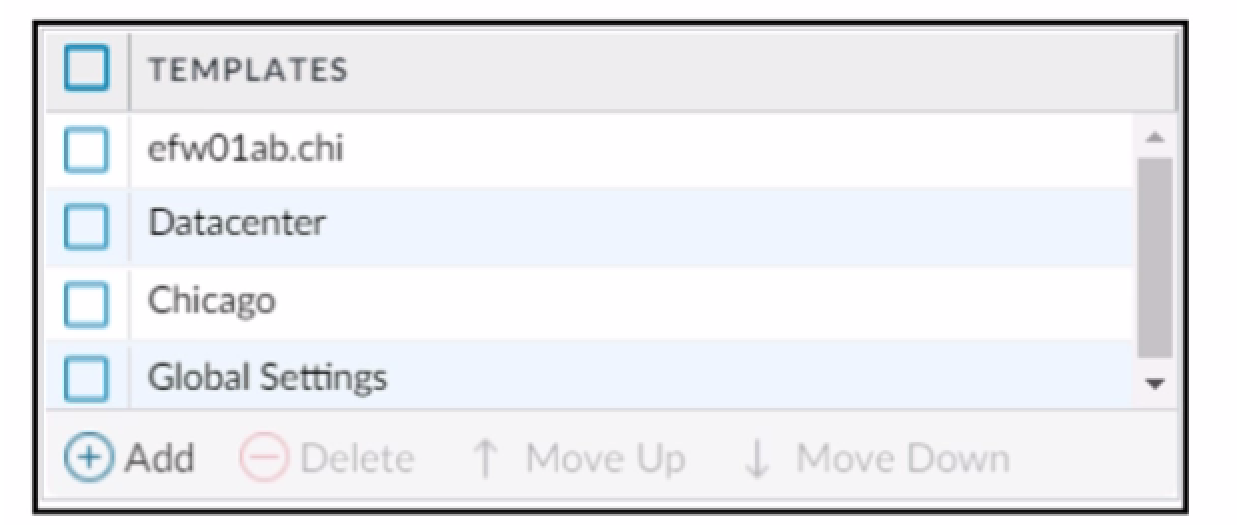
Proxy ID for IPSec VPN

Set Up an IPSec Tunnel

Question 2

Question Type: MultipleChoice

Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.



□	TEMPLATES
□	efw01ab.chi
□	Datacenter
□	Chicago
□	Global Settings

Which template values will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management?

Options:

A- Values in Datacenter

B- Values in efwOlab.chi

C- Values in Global Settings

D- Values in Chicago

Answer:

D

Explanation:

The template stack should consist of four templates arranged according to the diagram. The template values that will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management will be the values in Chicago. This is because the SSL/TLS Service profile is configured in the Chicago template, which is the highest priority template in the stack. The firewall will inherit the settings from the highest priority template that has the setting configured, and ignore the settings from the lower priority templates that have the same setting configured. Therefore, the values in Datacenter, efwOlab.chi, and Global Settings will not be applied to the firewall.Reference:

[Manage Templates and Template Stacks]

[Template Stack Configuration]

[Template Stack Priority]

Question 3

Question Type: MultipleChoice

Which statement about High Availability timer settings is true?

Options:

A- Use the Critical timer for faster failover timer settings.

B- Use the Aggressive timer for faster failover timer settings

C- Use the Moderate timer for typical failover timer settings

D- Use the Recommended timer for faster failover timer settings.

Answer:

D

Explanation:

Recommended: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the Recommended settings.

Aggressive: Use for faster failover timer settings.

Advanced: Allows you to customize the values to suit your network requirement for each of the following timers:

Question 4

Question Type: **MultipleChoice**

If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

Options:

A- Post-NAT destination address

B- Pre-NAT destination address

C- Post-NAT source address

D- Pre-NAT source address

Answer:

C

Explanation:

If an administrator wants to apply QoS to traffic based on source, they must specify the post-NAT source address in a QoS policy rule. This is because QoS is enforced on traffic as it egresses the firewall, and the firewall applies NAT rules before QoS rules. Therefore, the firewall will match the QoS policy rule based on the translated source address, not the original source address. If the administrator uses the pre-NAT source address in the QoS policy rule, the firewall will not be able to identify the traffic correctly and apply the desired QoS treatment.Reference:

QoS Policy

Configure QoS

Question 5

Question Type: **MultipleChoice**

An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.

Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

Options:

A- Configure the DNS server locally on the firewall.

B- Change the DNS server on the global template.

C- Override the DNS server on the template stack.

D- Configure a service route for DNS on a different interface.

Answer:

A, C

Explanation:

To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will copy the setting to the local configuration of the device and will no longer be controlled by the template. Overriding the setting on the template stack will apply the setting to all the firewalls that are assigned to the template stack, unless the setting is also overridden locally on a firewall. Changing the setting on the global template will affect all the firewalls that inherit the setting from the template, which is not desirable in this scenario. Configuring a service route for DNS on a different interface will not change the DNS server address, but only the interface that the firewall uses to reach the DNS server.Reference:

Override a Template Setting

How to override panorama pushed template configuration on the local firewall

Overriding Panorama Template settings

Question 6

Question Type: **MultipleChoice**

An engineer troubleshoots a high availability (HA) link that is unreliable.

Where can the engineer view what time the interface went down?

Options:

A- Monitor > Logs > System

B- Device > High Availability > Active/Passive Settings

C- Monitor > Logs > Traffic

D- Dashboard > Widgets > High Availability

Answer:

C

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNlUCAU&lang=en_US