Free Questions for JN0-636 by braindumpscollection

Shared by Lancaster on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are required to secure a network against malware. You must ensure that in the event that a compromised host is identified within the network. In this scenario after a threat has been identified, which two components are responsible for enforcing MAC-level infected host ?

Options:

A- SRX Series device

B- Juniper ATP Appliance

C- Policy Enforcer

D- EX Series device

Answer:

C, D

Explanation:

You are required to secure a network against malware. You must ensure that in the event that a compromised host is identified within the network, the host is isolated from the rest of the network. In this scenario, after a threat has been identified, the two components that are responsible for enforcing MAC-level infected host are:

C) Policy Enforcer. Policy Enforcer is a software solution that integrates with Juniper ATP Cloud and Juniper ATP Appliance to provide automated threat remediation across the network. Policy Enforcer can receive threat intelligence feeds from Juniper ATP Cloud or Juniper ATP Appliance and apply them to the security policies on the SRX Series devices and the EX Series devices. Policy Enforcer can also enforce MAC-level infected host, which is a feature that allows you to quarantine a compromised host by blocking its MAC address on the switch port.Policy Enforcer can communicate with the EX Series devices and instruct them to apply the MAC-level infected host policy to the infected host1.

D) EX Series device. EX Series devices are Ethernet switches that can provide Layer 2 and Layer 3 switching capabilities and security features. EX Series devices can integrate with Policy Enforcer and Juniper ATP Cloud or Juniper ATP Appliance to provide automated threat remediation across the network. EX Series devices can support MAC-level infected host, which is a feature that allows them to quarantine a compromised host by blocking its MAC address on the switch port.EX Series devices can receive instructions from Policy Enforcer and apply the MAC-level infected host policy to the infected host2.

The other options are incorrect because:

A) SRX Series device. SRX Series devices are high-performance firewalls that can provide Layer 3 and Layer 4 security features and integrate with Juniper ATP Cloud or Juniper ATP Appliance to provide advanced threat prevention. SRX Series devices can receive threat intelligence feeds from Juniper ATP Cloud or Juniper ATP Appliance and apply them to the security policies.However, SRX Series devices cannot enforce MAC-level infected host, which is a feature that requires Layer 2 switching capabilities and is supported by EX Series devices3.

B) Juniper ATP Appliance. Juniper ATP Appliance is a hardware solution that provides advanced threat prevention by detecting and blocking malware, ransomware, and other cyberattacks. Juniper ATP Appliance can analyze the network traffic and identify the compromised hosts based on their behavior and communication patterns. Juniper ATP Appliance can also send threat intelligence feeds to Policy Enforcer and SRX Series devices to enable automated threat remediation across the network. However, Juniper ATP Appliance cannot enforce MAC-level infected host, which is a feature that requires Layer 2 switching capabilities and is supported by EX Series devices.

Policy Enforcer Overview

EX Series Switches Overview

SRX Series Services Gateways Overview

[Juniper ATP Appliance Overview]

Question 2

Question Type: **MultipleChoice**

A company wants to paron their physical SRX series firewall into multiple logical units and assign

each unit (tenant) to a department within the organization. You are the primary administrator of firewall

and a colleague is the administrator for one of the departments.

Which two statements are correct about your colleague? (Choose two)

Options:

A- The colleague can configure the resources allocated and routing protocols

B- The colleague can access and view the resources of the tenant system.

C- The colleague can create and assign logical interfaces to the tenant system

D- The colleague can modify the number of allocated resources for the tenant system

Answer:

B, C

Explanation:

A)company wants to partition their physical SRX series firewall into multiple logical units and assign each unit (tenant) to a department within the organization. You are the primary administrator of the firewall and a colleague is the administrator for one of the departments. The two statements that are correct about your colleague are:

B) The colleague can access and view the resources of the tenant system. A tenant system is a type of logical system that is created and managed by the primary administrator of the firewall. A tenant system has its own discrete administrative domain, logical interfaces, routing instances, security policies, and other features. The primary administrator can assign a tenant system to a department within the organization and delegate the administration of the tenant system to a colleague.The colleague can access and view the resources of

the tenant system, such as the allocated CPU, memory, and bandwidth, and the configured interfaces, zones, and policies1.

C) The colleague can create and assign logical interfaces to the tenant system. A logical interface is a software interface that represents a subset of the physical interface. A logical interface can have its own address, encapsulation, and routing parameters. The primary administrator can allocate a number of logical interfaces to a tenant system and allow the colleague to create and assign logical interfaces to the tenant system.The colleague can configure the logical interfaces with the appropriate address, encapsulation, and routing parameters for the tenant system2.

The other statements are incorrect because:

A) The colleague cannot configure the resources allocated and routing protocols. The resources allocated and routing protocols are configured by the primary administrator of the firewall. The primary administrator can allocate a fixed amount of resources, such as CPU, memory, and bandwidth, to a tenant system and specify the routing protocols that are allowed for the tenant system.The colleague cannot modify the resources allocated or routing protocols for the tenant system1.

D) The colleague cannot modify the number of allocated resources for the tenant system. The number of allocated resources for the tenant system is configured by the primary administrator of the firewall. The primary administrator can allocate a fixed amount of resources, such as CPU, memory, and bandwidth, to a tenant system and monitor the resource usage of the tenant system.The colleague cannot modify the number of allocated resources for the tenant system1.

Understanding Tenant Systems

Understanding Logical Interfaces

Question 3

Question Type: MultipleChoice

your company wants to take your juniper ATP appliance into private mode. You must give them a list

of impacted features for this request.

Which two features are impacted in this scenario? (Choose two)

Options:

A- False Positive Reporting

B- Threat Progression Monitoring

C- GSS Telemetry

D- Cyber Kill Chain mapping

Answer:

A, C

Explanation:

Your company wants to take your Juniper ATP Appliance into private mode. You must give them a list of impacted features for this request. The two features that are impacted in this scenario are:

A) False Positive Reporting. False Positive Reporting is a feature that allows you to report false positive detections to Juniper Networks for analysis and improvement. False Positive Reporting requires an Internet connection to send the reports to Juniper Networks.If you take your Juniper ATP Appliance into private mode, False Positive Reporting will be disabled and you will not be able to report false positives1.

C) GSS Telemetry. GSS Telemetry is a feature that allows you to send anonymized threat data to Juniper Networks for analysis and improvement. GSS Telemetry requires an Internet connection to send the data to Juniper Networks.If you take your Juniper ATP Appliance into private mode, GSS Telemetry will be disabled and you will not be able to contribute to the threat intelligence community2.

The other options are incorrect because:

B) Threat Progression Monitoring. Threat Progression Monitoring is a feature that allows you to monitor the threat activity and progression across your network. Threat Progression Monitoring does not require an Internet connection and can be performed locally by the Juniper ATP Appliance.If you take your Juniper ATP Appliance into private mode, Threat Progression Monitoring will not be impacted and you will still be able to monitor the threat activity and progression3.

D) Cyber Kill Chain mapping. Cyber Kill Chain mapping is a feature that allows you to map the threat activity and progression to the stages of the Cyber Kill Chain framework. Cyber Kill Chain mapping does not require an Internet connection and can be performed locally by the Juniper ATP Appliance.If you take your Juniper ATP Appliance into private mode, Cyber Kill Chain mapping will not be impacted and you will still be able to map the threat activity and progression4.

False Positive Reporting

GSS Telemetry

Threat Progression Monitoring

Cyber Kill Chain Mapping

Question 4

Question Type: MultipleChoice

You must setup a Ddos solution for your ISP. The solution must be agile and not block legitimate traffic.

Which two products will accomplish this task? (Choose two.)

Options:

A- Contrail Insights

B- MX Series device

C- Corero Smartwall TDD

D- SRX Series device

Answer:

B, C

Explanation:

You must set up a DDoS solution for your ISP. The solution must be agile and not block legitimate traffic. The two products that will accomplish this task are:

B) MX Series device. MX Series devices are high-performance routers that can provide DDoS protection at the network edge by integrating with Corero SmartWall Threat Defense Director (TDD) software. MX Series devices can leverage the packet processing capabilities of the MX-SPC3 Services Card to perform real-time DDoS detection and mitigation at line rate, scaling from 50 Gbps to 40 Tbps. MX Series devices can also use Juniper Networks Security Intelligence (SecIntel) to receive threat intelligence feeds from Juniper ATP Cloud or Juniper Threat Labs and apply them to the security policies.MX Series devices can provide an agile and effective DDoS solution for your ISP without blocking legitimate traffic12.

C) Corero SmartWall TDD. Corero SmartWall TDD is a software solution that runs on MX Series devices and PTX Series devices to provide DDoS protection at the network edge. Corero SmartWall TDD uses behavioral analytics and detailed network visibility to detect and block DDoS attacks in seconds, without affecting the normal traffic. Corero SmartWall TDD can also provide advanced protection from "carpet bombing" attacks, 5G DDoS visibility, and multi-tenant portal for as-a-service offerings or views by department within an enterprise.Corero SmartWall TDD can provide an agile and effective DDoS solution for your ISP without blocking legitimate traffic34.

The other options are incorrect because:

A) Contrail Insights. Contrail Insights is a software solution that provides network analytics and visibility for cloud and data center environments. Contrail Insights can help you monitor, troubleshoot, and optimize the performance and security of your network, but it

does not provide DDoS protection by itself.Contrail Insights can integrate with other Juniper products, such as Contrail Enterprise Multicloud, Contrail Service Orchestration, and AppFormix, to provide a comprehensive network management solution, but it is not a DDoS solution for your ISP5.

D) SRX Series device. SRX Series devices are high-performance firewalls that can provide DDoS protection at the network perimeter by integrating with Juniper ATP Cloud and Juniper Threat Labs. SRX Series devices can use SecIntel to receive threat intelligence feeds from Juniper ATP Cloud or Juniper Threat Labs and apply them to the security policies. SRX Series devices can also use IDP to detect and prevent application-level attacks, such as SQL injection, cross-site scripting, and buffer overflow. SRX Series devices can provide a robust and effective DDoS solution for your network, but they are not designed to handle high-volume DDoS attacks at the network edge, as MX Series devices and Corero SmartWall TDD are .

Juniper and Corero Joint DDoS Protection Solution

MX-SPC3 Services Card Overview

Corero SmartWall Threat Defense Director (TDD)

Juniper Networks and Corero: A Modern Approach to DDoS Protection at Scale

Contrail Insights Overview

[SRX Series Services Gateways]

[Juniper Networks Security Intelligence (SecIntel)]

Question 5

Question Type: MultipleChoice

you are connecting two remote sites to your corporate headquarters site. You must ensure that traffic

passes corporate headquarter.

Options:

A- In this scenario, which VPN should be used?

B- full mesh IPsec VPNs with tunnels between all sites

C- a full mesh Layer 3 VPN with the BGP route reflector behind the corporate firewall device

D- a Layer 3 VPN with the corporate firewall acting as the hub device

E- hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device

Answer:

D

Explanation:

You are connecting two remote sites to your corporate headquarters site. You must ensure that traffic passes through the corporate headquarters. In this scenario, the VPN that should be used is:

D) Hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device. A hub-and-spoke IPsec VPN is a type of VPN that connects multiple remote sites to a central site, or hub, over a public network. The hub site acts as a gateway for the remote sites and provides security and routing services. The remote sites, or spokes, communicate with each other through the hub site. The hub site and the spoke sites use IPsec tunnels to encrypt and authenticate the traffic between them. A hub-and-spoke IPsec VPN is suitable for connecting two remote sites to your corporate headquarters site, because it allows you to control the traffic flow and enforce security policies at the hub site.The corporate firewall can act as the hub device and provide IPsec VPN services to the remote sites1.

The other options are incorrect because:

A) Full mesh IPsec VPNs with tunnels between all sites. A full mesh IPsec VPN is a type of VPN that connects every site to every other site over a public network. Each site has an IPsec tunnel with every other site, forming a mesh topology. A full mesh IPsec VPN provides direct and secure communication between any pair of sites, but it also requires a large number of IPsec tunnels and complex configuration.A full mesh IPsec VPN is not suitable for connecting two remote sites to your corporate headquarters site, because it does not ensure that traffic passes through the corporate headquarters site, and it may introduce unnecessary overhead and complexity2.

B) A full mesh Layer 3 VPN with the BGP route reflector behind the corporate firewall device. A full mesh Layer 3 VPN is a type of VPN that uses MPLS and BGP to provide Layer 3 connectivity and routing between multiple sites over a service provider's network. Each site has a BGP session with every other site, forming a full mesh topology. A BGP route reflector is a device that reduces the number of BGP sessions required in a full mesh topology by reflecting routes between its clients.A full mesh Layer 3 VPN with the BGP route reflector behind the corporate firewall device is not suitable for connecting two remote sites to your corporate headquarters site, because it does not ensure that traffic passes through the corporate firewall device, and it may require additional configuration and coordination with the service provider3.

C) A Layer 3 VPN with the corporate firewall acting as the hub device. A Layer 3 VPN is a type of VPN that uses MPLS and BGP to provide Layer 3 connectivity and routing between multiple sites over a service provider's network. A Layer 3 VPN can have different topologies, such as full mesh, hub-and-spoke, or partial mesh.A Layer 3 VPN with the corporate firewall acting as the hub device is not suitable for connecting two remote sites to your corporate headquarters site, because the corporate firewall may not support MPLS and BGP, and it may require additional configuration and coordination with the service provider3.

Hub-and-Spoke VPNs Overview

Full Mesh VPNs Overview

Layer 3 VPNs Overview

Question 6

Question Type: **MultipleChoice**

You want traffic to avoid the flow daemon for administrative task.

In this scenario which two stateless service are available with selective stateless packet based service. (Choose Two)

Options:

A- Layer 2 switching

B- IPv4 routing

C- IPsec

D- IPv6 routing

Answer:

A, B

Explanation:

You want traffic to avoid the flow daemon for administrative tasks. In this scenario, the two stateless services that are available with selective stateless packet-based services are:

A) Layer 2 switching. Layer 2 switching is a stateless service that forwards packets based on the MAC addresses of the source and destination hosts. Layer 2 switching does not require any routing or flow processing, and can be performed by the Packet Forwarding Engine (PFE) of the SRX Series device. You can use selective stateless packet-based services to enable Layer 2 switching for traffic that matches a stateless firewall filter.The firewall filter must have the packet-mode action modifier to bypass the flow daemon1.

B) IPv4 routing. IPv4 routing is a stateless service that forwards packets based on the IP addresses of the source and destination hosts. IPv4 routing does not require any flow processing, and can be performed by the PFE of the SRX Series device. You can use selective stateless packet-based services to enable IPv4 routing for traffic that matches a stateless firewall filter.The firewall filter must have the packet-mode action modifier to bypass the flow daemon1.

The other options are incorrect because:

C) IPsec. IPsec is a stateful service that provides security and encryption for IP packets. IPsec requires flow processing, and cannot be performed by the PFE of the SRX Series device. You cannot use selective stateless packet-based services to enable IPsec for traffic that matches a stateless firewall filter.The firewall filter cannot have the packet-mode action modifier to bypass the flow daemon2.

D) IPv6 routing. IPv6 routing is a stateful service that forwards packets based on the IP addresses of the source and destination hosts. IPv6 routing requires flow processing, and cannot be performed by the PFE of the SRX Series device. You cannot use selective stateless packet-based services to enable IPv6 routing for traffic that matches a stateless firewall filter.The firewall filter cannot have the packet-mode action modifier to bypass the flow daemon3.

Selective Stateless Packet-Based Services Overview

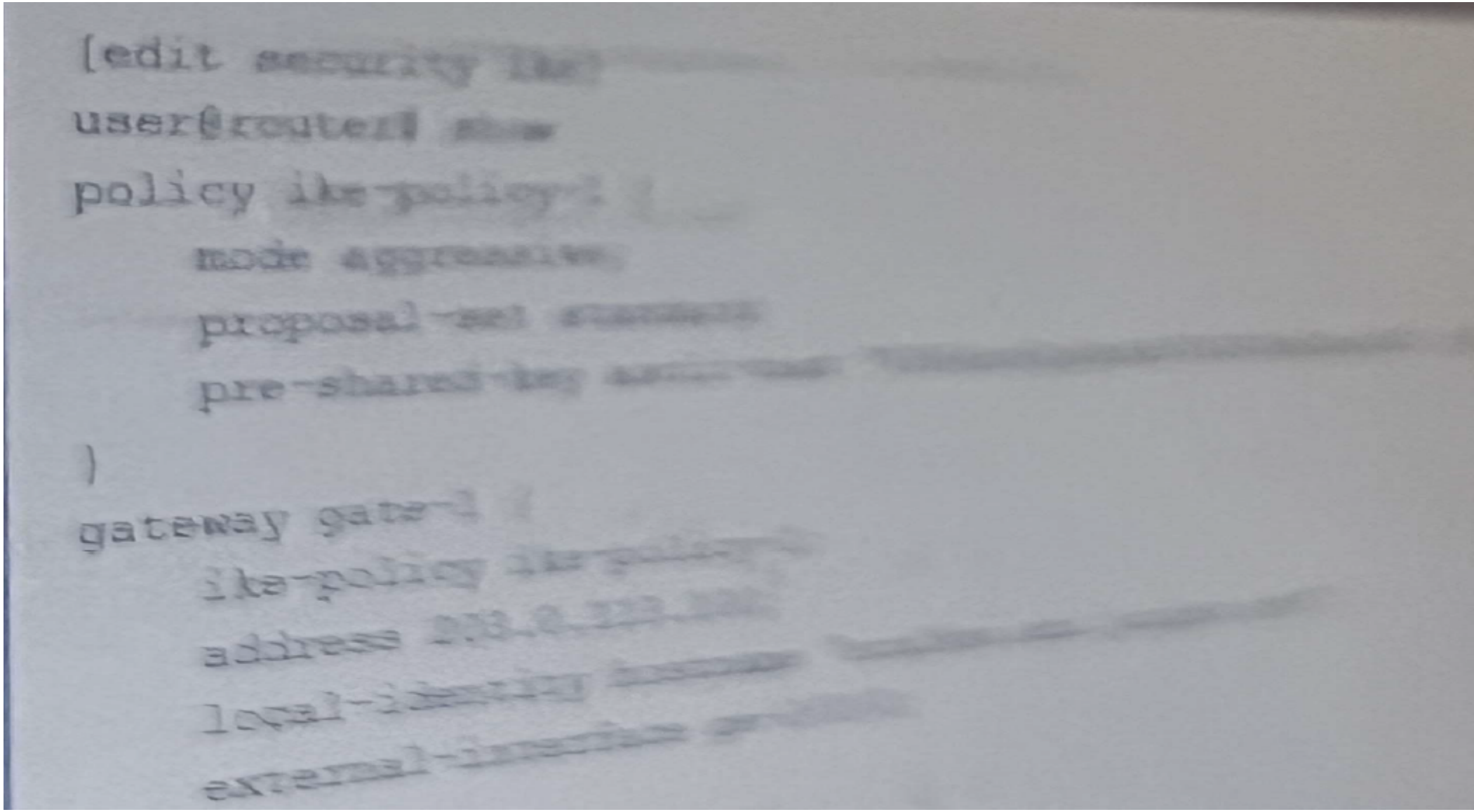
IPsec VPN Overview

IPv6 Overview

Question 7

Question Type: **MultipleChoice**

Refer to the Exhibit:



which two statements about the configuration shown in the exhibit are correct ?

Options:

A- The remote IKE gateway IP address is 203.0.113.100.

B- The local peer is assigned a dynamic IP address.

C- The local IKE gateway IP address is 203.0.113.100.

D- The remote peer is assigned a dynamic IP address.

Answer:

A, D

Explanation:

The two statements about the configuration shown in the exhibit are correct are:

A) The remote IKE gateway IP address is 203.0.113.100. The exhibit shows that the address option under the gateway statement is set to 203.0.113.100, which specifies the IP address of the primary IKE gateway.The address option is used to configure the IP address or the hostname of the remote peer that has a static IP address1.

D) The remote peer is assigned a dynamic IP address. The exhibit shows that the dynamic option under the gateway statement is configured with various attributes, such as general-ikeid, ike-user-type, and user-at-hostname. The dynamic option is used to configure the identifier for the remote gateway with a dynamic IP address.The dynamic option also enables the SRX Series device to accept multiple connections from remote peers that have the same identifier2.

The other statements are incorrect because:

B) The local peer is not assigned a dynamic IP address, but a static IP address. The exhibit shows that the local-address option under the gateway statement is set to 192.0.2.100, which specifies the IP address of the local IKE gateway.The local-address option is used to configure the IP address of the local peer that has a static IP address1.

C) The local IKE gateway IP address is not 203.0.113.100, but 192.0.2.100, as explained above.

gateway (Security IKE)

dynamic (Security IKE)

Question 8

Question Type: **MultipleChoice**

Exhibit:

Referring to the exhibit, your company's infrastructure team implemented new printers

To make sure that the policy enforcer pushes the updated Ip address list to the SRX.

Which three actions are required to complete the requirement? (Choose three)

Options:

A- Configure the server feed URL as http://172.25.10.254/myprinters

B- Create a security policy that uses the dynamic address feed to allow access

C- Configure Security Director to create a dynamic address feed

D- Configure Security Director to create a C&C feed.

E- Configure server feed URL as https://172.25.10.254/myprinters.

Answer:

A, B, C

Explanation:

Referring to the exhibit, your company's infrastructure team implemented new printers. To make sure that the policy enforcer pushes the updated IP address list to the SRX, you need to perform the following actions:

A) Configure the server feed URL as http://172.25.10.254/myprinters. The server feed URL is the address of the remote server that provides the custom feed data. You need to configure the server feed URL to match the location of the file that contains the IP addresses of the new printers.In this case, the file name is myprinters and the server IP address is 172.25.10.254, so the server feed URL should be http://172.25.10.254/myprinters1.

B) Create a security policy that uses the dynamic address feed to allow access. A security policy is a rule that defines the action to be taken for the traffic that matches the specified criteria, such as source and destination addresses, zones, protocols, ports, and

applications. You need to create a security policy that uses the dynamic address feed as the source or destination address to allow access to the new printers. A dynamic address feed is a custom feed that contains a group of IP addresses that can be entered manually or imported from external sources.The dynamic address feed can be used in security policies to either deny or allow traffic based on either source or destination IP criteria2.

C) Configure Security Director to create a dynamic address feed. Security Director is a Junos Space application that enables you to create and manage security policies and objects. You need to configure Security Director to create a dynamic address feed that contains the IP addresses of the new printers. You can create a dynamic address feed by using the local file or the remote file server option.In this case, you should use the remote file server option and specify the server feed URL as http://172.25.10.254/myprinters3.

The other options are incorrect because:

D) Configuring Security Director to create a C&C feed is not required to complete the requirement. A C&C feed is a security intelligence feed that contains the IP addresses of servers that are used by malware or attackers to communicate with infected hosts. The C&C feed is not related to the new printers or the dynamic address feed.

E) Configuring the server feed URL as https://172.25.10.254/myprinters is not required to complete the requirement. The server feed URL can use either the HTTP or the HTTPS protocol, depending on the configuration of the remote server.In this case, the exhibit shows that the remote server is using the HTTP protocol, so the server feed URL should use the same protocol1.

Configuring the Server Feed URL

Dynamic Address Overview

Creating Custom Feeds

[Command and Control Feed Overview]

Question 9

Question Type: MultipleChoice

which security feature bypasses routing or switching lookup?

Options:

A- transparent mode

B- secure wire

C- mixed mode

D- MACsec

Answer:

A

Explanation:

The security feature that bypasses routing or switching lookup is transparent mode. The other options are incorrect because:

B) Secure wire is a feature that allows you to connect two interfaces on the same device and forward traffic between them without any processing.Secure wire does not bypass routing or switching lookup, but rather eliminates them altogether1.

C) Mixed mode is a mode of operation for SRX Series devices that allows you to configure both transparent mode and switching mode on the same device.Mixed mode does not bypass routing or switching lookup, but rather uses them depending on the interface type2.

D) MACsec (Media Access Control Security) is a feature that provides encryption and authentication for Layer 2 traffic.MACsec does not bypass routing or switching lookup, but rather operates at a lower layer3.

Therefore, the correct answer is

A) Transparent mode is a mode of operation for SRX Series devices that provides Layer 2 bridging capabilities with full security services. In transparent mode, the SRX Series device acts as a bridge between two network segments and inspects the packets without modifying the source or destination information in the IP packet header. The SRX Series device does not have an IP address in transparent mode, except for the management interface.Transparent mode bypasses routing or switching lookup, because the SRX Series device does not perform any routing or switching functions, but rather forwards the packets based on the MAC addresses4.

Secure Wire Overview

Mixed Mode Overview

MACsec Overview

Transparent Mode Overview

Question 10

Question Type: MultipleChoice

Which two security intelligence feed types are supported?

Options:

A- infected host feed

B- Command and Control feed

C- custom feeds

D- malicious URL feed

Answer:

A, B

Explanation:

The two security intelligence feed types that are supported are:

A) Infected host feed. An infected host feed is a security intelligence feed that contains the IP addresses of hosts that are infected by malware or compromised by attackers. The SRX Series device can download the infected host feed from the Juniper ATP Cloud or generate its own infected host feed based on the detection events from IDP.The SRX Series device can use the infected host feed to block or quarantine the traffic to or from the infected hosts based on the security policies1.

B) Command and Control feed. A command and control feed is a security intelligence feed that contains the IP addresses of servers that are used by malware or attackers to communicate with infected hosts. The SRX Series device can download the command and control feed from the Juniper ATP Cloud or generate its own command and control feed based on the detection events from IDP.The SRX Series device can use the command and control feed to block or log the traffic to or from the command and control servers based on the security policies2.

The other options are incorrect because:

C) Custom feeds. Custom feeds are not a security intelligence feed type, but a feature that allows you to create your own security intelligence feeds based on your own criteria and sources. You can configure custom feeds by using the Junos Space Security Director or the CLI.Custom feeds are not supported by the Juniper ATP Cloud or the IDP3.

D) Malicious URL feed. Malicious URL feed is not a security intelligence feed type, but a feature that allows you to block or log the traffic to or from malicious URLs based on the security policies. The SRX Series device can download the malicious URL feed from the Juniper ATP Cloud or the Juniper Threat Labs.Malicious URL feed is not supported by the IDP4.

Infected Host Feed Overview

Command and Control Feed Overview

Custom Feed Overview

Question 11

Question Type: MultipleChoice

Exhibit:

Referring to the exhibit, which two statements are correct?

Options:

A- All of the entries are a threat level 8

B- All of the entries are command and control entries.

C- All of the entries are Dshield entries

D- All of the entries are a threat level 10.

Answer:

B, C

Explanation:

Referring to the exhibit, the following statements are correct:

B) All of the entries are command and control entries. Command and control entries are dynamic addresses that represent the IP addresses of servers that are used by malware to communicate with infected hosts. The SRX Series device can block or log the traffic to or from these IP addresses based on the security policies.The exhibit shows that all of the entries have the category DC/1, which stands for command and control1.

C) All of the entries are Dshield entries. Dshield is a feed source that provides a list of IP addresses that are associated with malicious activities, such as scanning, spamming, or attacking. The SRX Series device can download the Dshield feed and use it to populate the dynamic address entries.The exhibit shows that all of the entries have the feed dshield, which indicates that they are from the Dshield feed source2.

The other statements are incorrect because:

A) All of the entries are not a threat level 8, but a threat level 10. The threat level is a numeric value that indicates the severity of the threat associated with a dynamic address entry. The higher the threat level, the more dangerous the threat. The SRX Series device can use the threat level to prioritize the actions for the dynamic address entries. The exhibit shows that all of the entries have the cc CN, which stands for country code China. According to the Juniper documentation, the country code China has a threat level of 10, which is the highest.

D) All of the entries are not a threat level 10, but they are. See the explanation for option A.

Understanding Dynamic Address Categories

Understanding Dynamic Address Feed Sources

[Understanding Dynamic Address Threat Levels]

Question 12

Question Type: MultipleChoice

Exhibit:

The security trace options configuration shown in the exhibit is committed to your SRX series firewall. Which two statements are correct in this Scenario? (Choose Two)

Options:

A- The file debugger will be readable by all users.

B- Once the trace has generated 10 log files, older logs will be overwritten.

C- Once the trace has generated 10 log files, the trace process will halt.

D- The file debugger will be readable only by the user who committed this configuration

Answer:

B, D

Explanation:

The security trace options configuration shown in the exhibit is committed to your SRX series firewall. The following statements are correct in this scenario:

B) Once the trace has generated 10 log files, older logs will be overwritten. The files option in the traceoptions statement specifies the maximum number of trace files to keep. When a trace file reaches its maximum size, it is renamed with a numeric suffix, such as kmd.0, kmd.1, and so on, until the maximum number of files is reached. Then the oldest trace file is overwritten by the newest one.In this case, the files option is set to 10, which means that the trace will generate 10 log files and then overwrite the older ones1.

D) The file debugger will be readable only by the user who committed this configuration. The file option in the traceoptions statement specifies the name of the trace file and the permissions for the file. The permissions can be either world-readable or owner-readable.In this case, the file option is set to debugger owner-readable, which means that the trace file will be named debugger and will be readable only by the user who committed the configuration1.

The other statements are incorrect because:

A) The file debugger will not be readable by all users, but only by the user who committed this configuration, as explained above.

C) The trace will not halt after generating 10 log files, but will continue to overwrite the older ones, as explained above.

traceoptions (Security)