

Juniper JN0-637

Security - Professional (JNCIP-SEC)

- Up to Date products, reliable and verified.
- Questions and Answers in PDF Format.

Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

For More Information:

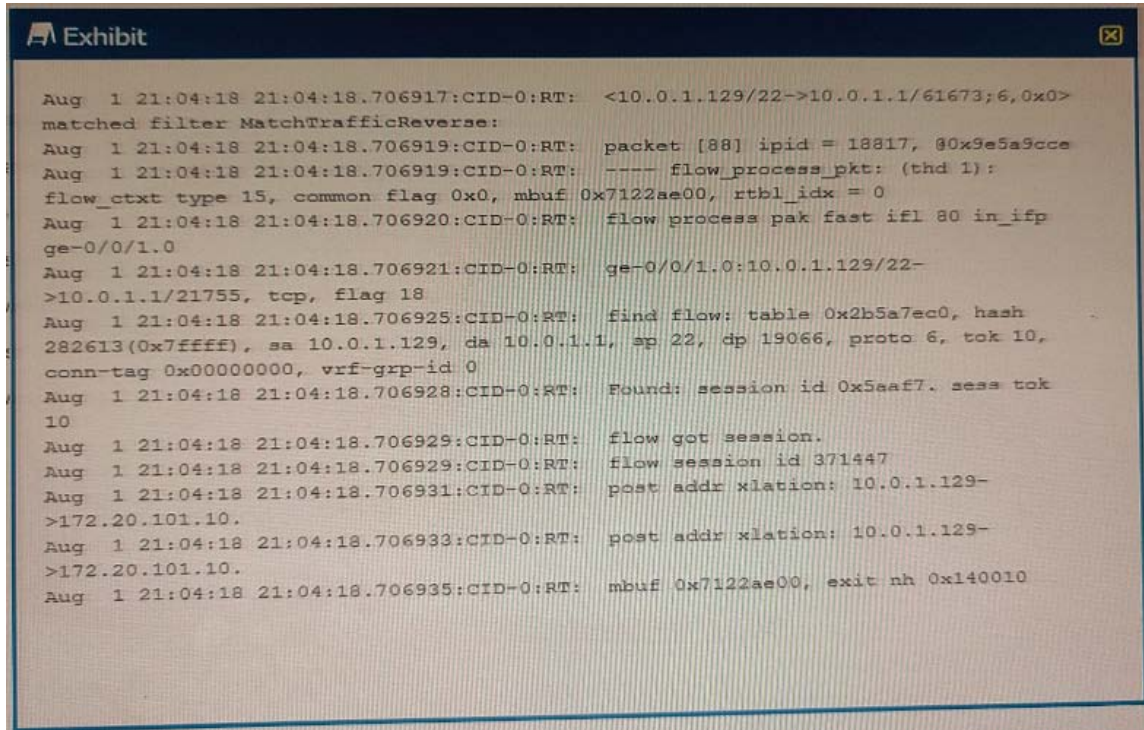
<https://www.testsexpert.com/>

• Product Version

Latest Version: 6.1

Question: 1

Exhibit



```
Aug 1 21:04:18 21:04:18.706917:CID-0:RT: <10.0.1.129/22->10.0.1.1/61673;6,0x0>
matched filter MatchTrafficReverse:
Aug 1 21:04:18 21:04:18.706919:CID-0:RT: packet [88] ipid = 18817, 80x9e5a9cce
Aug 1 21:04:18 21:04:18.706919:CID-0:RT: ---- flow_process_pkt: (thd 1):
flow_ctxt type 15, common flag 0x0, mbuf 0x7122ae00, rtbl_idx = 0
Aug 1 21:04:18 21:04:18.706920:CID-0:RT: flow process pak fast ifl 80 in_ifp
ge-0/0/1.0
Aug 1 21:04:18 21:04:18.706921:CID-0:RT: ge-0/0/1.0:10.0.1.129/22-
>10.0.1.1/21755, tcp, flag 18
Aug 1 21:04:18 21:04:18.706925:CID-0:RT: find flow: table 0x2b5a7ec0, hash
282613(0x7ffff), sa 10.0.1.129, da 10.0.1.1, sp 22, dp 19066, proto 6, tok 10,
conn-tag 0x00000000, vrf-grp-id 0
Aug 1 21:04:18 21:04:18.706928:CID-0:RT: Found: session id 0x5aaf7, sess tok
10
Aug 1 21:04:18 21:04:18.706929:CID-0:RT: flow got session.
Aug 1 21:04:18 21:04:18.706929:CID-0:RT: flow session id 371447
Aug 1 21:04:18 21:04:18.706931:CID-0:RT: post addr xlation: 10.0.1.129-
>172.20.101.10.
Aug 1 21:04:18 21:04:18.706933:CID-0:RT: post addr xlation: 10.0.1.129-
>172.20.101.10.
Aug 1 21:04:18 21:04:18.706935:CID-0:RT: mbuf 0x7122ae00, exit nh 0x140010
```

You are using trace options to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

- A. This packet is part of an existing session.
- B. The SRX device is changing the source address on this packet from
- C. This is the first packet in the session
- D. The SRX device is changing the destination address on this packet 10.0.1.1 to 172.20.101.10.

Answer: A, D

Explanation:

According to the trace options output in the exhibit, the following statements are correct:

This packet is part of an existing session. This is indicated by the line flow session id 0x00000000, hash 0x00000000, table 0x00000000, flow process exit, which shows that the packet matches an existing session entry in the flow table1.

The SRX device is changing the destination address on this packet from 10.0.1.1 to 172.20.101.10. This is indicated by the line nat: translated 10.0.1.1->172.20.101.10, which shows that the packet undergoes destination NAT2.

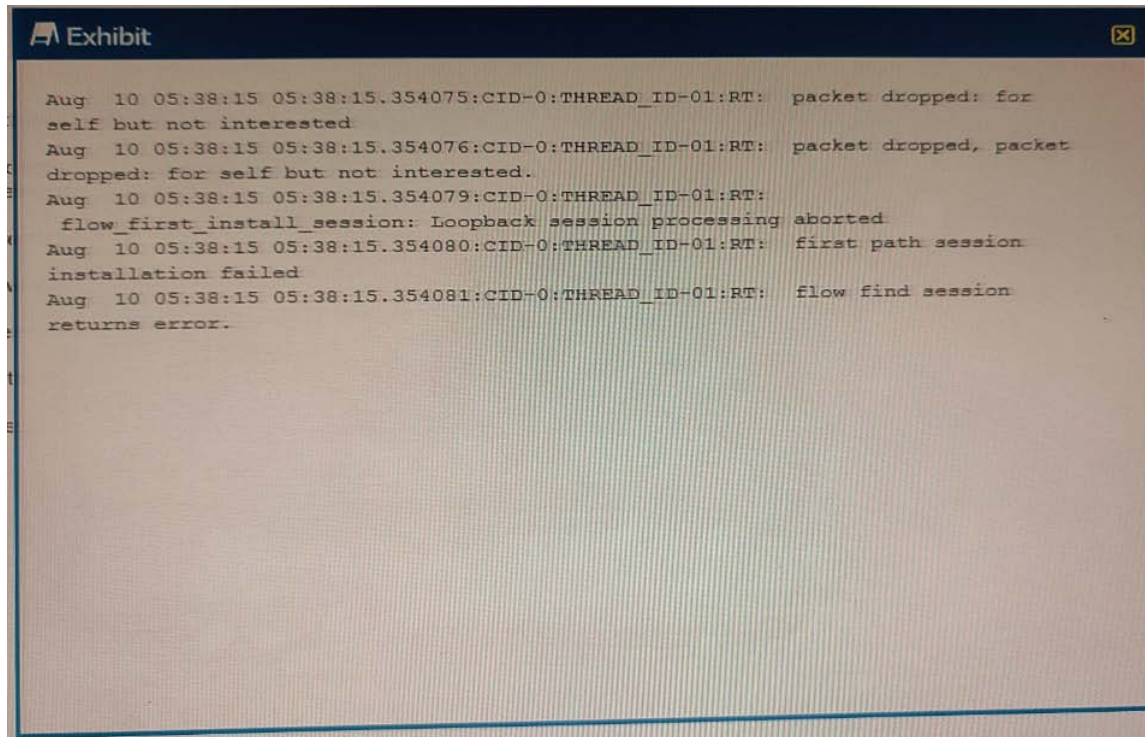
The following statements are incorrect:

The SRX device is changing the source address on this packet. There is no indication of source NAT in the trace options output2.

This is the first packet in the session. The first packet in a session would have a different trace options output, which would include the line `flow_first_inline_processing` and show the creation of a new session entry in the flow table1.

Question: 2

Exhibit



You are asked to establish an IBGP peering between the SRX Series device and the router, but the session is not being established. In the security flow trace on the SRX device, packet drops are observed as shown in the exhibit.

What is the correct action to solve the problem on the SRX device?

- A. Create a firewall filter to accept the BGP traffic
- B. Configure destination NAT for BGP traffic.
- C. Add BGP to the Allowed host-inbound-traffic for the interface
- D. Modify the security policy to allow the BGP traffic.

Answer: C

Explanation:

According to the security flow trace in the exhibit, the packets are dropped for self but not interested. This means that the SRX device is receiving packets destined to itself, but it does not have

the corresponding service configured in the host-inbound-traffic stanza for the interface1. In this case, the service is BGP, which uses TCP port 179. Therefore, the correct action to solve the problem on the SRX device is to add BGP to the allowed host-inbound-traffic for the interface. This can be done by using the following command:

```
set security zones security-zone <zone-name> interfaces <interface-name> host-inbound-traffic system-services bgp
```

This command will allow the SRX device to accept BGP packets on the specified interface and zone. Alternatively, the command can be applied to all interfaces in a zone by using the all-interfaces option2.

Question: 3

SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following command show configuration services security—intelligence url

```
https://cloudfeeds.argon.junipersecurity.net/api/manifest.xml
```

and receives the following output:

What is the problem in this scenario?

- A. The device is directly enrolled with Juniper ATP Cloud.
- B. The device is already enrolled with Policy Enforcer.
- C. The SRX Series device does not have a valid license.
- D. Junos Space does not have matching schema based on the

Answer: C

Explanation:

According to the output of the command show configuration services security-intelligence url, the SRX Series device is directly enrolled with Juniper ATP Cloud. This is indicated by the URL `https://cloudfeeds.argon.junipersecurity.net/api/manifest.xml`, which is the default URL for Juniper ATP Cloud1. This means that the device is not enrolled with Policy Enforcer, which would use a different URL that includes the IP address of the Policy Enforcer server2. Therefore, the problem in this scenario is that the device is directly enrolled with Juniper ATP Cloud, which prevents it from being enrolled with Policy Enforcer.

To enroll the device with Policy Enforcer, the user needs to disenroll the device from Juniper ATP Cloud first. This can be done by using the following command:

```
delete services security-intelligence url
```

This command will remove the Juniper ATP Cloud URL from the device configuration and stop the device from receiving threat feeds from Juniper ATP Cloud1. After that, the user can enroll the device with Policy Enforcer by using the Security Director GUI or the SLAX script2.

Question: 4

Exhibit

```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

Referring to the exhibit, which three statements are true? (Choose three.)

- A. The packet's destination is to an interface on the SRX Series device.
- B. The packet's destination is to a server in the DMZ zone.
- C. The packet originated within the Trust zone.
- D. The packet is dropped before making an SSH connection.
- E. The packet is allowed to make an SSH connection.

Answer: A, C, D

Explanation:

According to the exhibit, which is a security flow trace on an SRX Series device, the following statements are true:

The packet's destination is to an interface on the SRX Series device. This is indicated by the line packet dropped for self but not interested, which means that the packet is destined to the SRX device itself, but the device does not have the corresponding service configured in the host-inbound-traffic stanza for the interface1.

The packet originated within the Trust zone. This is indicated by the line zone name: Trust, which shows that the packet belongs to the Trust zone. The Trust zone is typically the zone where the internal network is connected to the SRX device2.

The packet is dropped before making an SSH connection. This is indicated by the line flow_first_inline_processing: pak(0x4a9c0d0), which shows that the packet is the first packet in the session and is processed by the firewall. The packet is dropped because it does not match any security policy or host-inbound-traffic rule1. The packet is trying to make an SSH connection, which uses TCP port 22, as shown by the line source port: 22.

The following statements are false:

The packet's destination is to a server in the DMZ zone. There is no indication of the DMZ zone in the trace output. The DMZ zone is typically the zone where the external servers are connected to the SRX device2.

The packet is allowed to make an SSH connection. The packet is not allowed to make an SSH connection, as explained above.

Question: 5

Exhibit

```
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:36
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:15
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Framework - module(radius) return: FAILURE
```

You configure a traceoptions file called radius on your returns the output shown in the exhibit
What is the source of the problem?

- A. An incorrect password is being used.
- B. The authentication order is misconfigured.
- C. The RADIUS server IP address is unreachable.
- D. The RADIUS server suffered a hardware failure.

Answer: A

Explanation:

According to the output of the traceoptions file called radius, the source of the problem is that the RADIUS server IP address is unreachable. This is indicated by the line FAILURE: sendto: No route to host, which shows that the SRX device cannot send the authentication request to the RADIUS server. This could be due to a network issue, such as a misconfigured route, a firewall blocking the traffic, or a physical link failure.

To troubleshoot this issue, the user should check the following:

The RADIUS server IP address and port are correctly configured on the SRX device. The user can verify this by using the command `show configuration access radius-server1`.

The SRX device can ping the RADIUS server IP address. The user can use the command `ping <RADIUS-server-IP>` to test the connectivity2.

The SRX device has a valid route to the RADIUS server IP address. The user can use the command `show route <RADIUS-server-IP>` to check the routing table3.

The SRX device and the RADIUS server are using the same shared secret key. The user can verify this by using the command `show configuration access radius-server secret1`.

The SRX device and the RADIUS server are using the same authentication protocol. The user can verify this by using the command `show configuration access profile <profile-name>4`.

The firewall policies on the SRX device and any intermediate devices are allowing the RADIUS traffic. The user can use the command `show security policies from-zone <source-zone> to-zone <destination-zone>` to check the firewall policies5.

Question: 6

Exhibit

```
user@SRX> show ethernet-switching global-information
Global Configuration:
MAC aging interval      : 300
MAC learning           : Enabled
MAC statistics          : Disabled
MAC limit Count         : 65536
MAC limit hit           : Disabled
MAC packet action drop  : Disabled
MAC+IP aging interval  : IPv4 - 1200 seconds
                       : IPv6 - 1200 seconds
MAC+IP limit Count      : 65536
MAC+IP limit reached    : No
LE aging time           : 1200
LE BD aging time        : 1200
MP discard notification interval: 60
Global Mode             : Not set
RE state                 : Master
VXLAN Overlay load bal  : Disabled
VXLAN ECMP               : Disabled
```

You have configured the SRX Series device to switch packets for multiple directly connected hosts that are within the same broadcast domain. However, the traffic between two hosts in the same broadcast domain are not matching any security policies.

Referring to the exhibit, what should you do to solve this problem?

A. You must change the global mode to security switching mode.

- B. You must change the global mode to security bridging mode
- C. You must change the global mode to transparent bridge mode.
- D. You must change the global mode to switching mode.

Answer: C

Explanation:

According to the exhibit, which is a configuration snippet of the SRX Series device, the global mode for the device is set to switching mode. This means that the device is operating as a Layer 2 switch and does not apply any security policies to the traffic between hosts in the same broadcast domain¹. Therefore, the traffic between two hosts in the same broadcast domain are not matching any security policies.

To solve this problem, the user should change the global mode to transparent bridge mode. This means that the device will operate as a Layer 2 transparent bridge and apply security policies to the traffic between hosts in the same broadcast domain². This will allow the user to enforce security policies based on the source and destination IP addresses, ports, and protocols of the traffic.

To change the global mode to transparent bridge mode, the user should use the following command:

`set protocols l2-learning global-mode transparent-bridge`

This command will set the global mode for the SRX Series device as Layer 2 transparent bridge mode. After changing the mode, the user must reboot the device for the configuration to take effect².

Question: 7

You are asked to deploy filter-based forwarding on your SRX Series device for incoming traffic sourced from the 10.10.100.0/24 network in this scenario, which three statements are correct? (Choose three.)

- A. You must create a forwarding-type routing instance.
- B. You must create and apply a firewall filter that matches on the source address 10.10.100.0/24 and then sends this traffic to your routing
- C. You must create and apply a firewall filter that matches on the destination address 10.10.100.0/24 and then sends this traffic to your routing instance.
- D. You must create a RIB group that adds interface routes to your routing instance.
- E. You must create a VRF-type routing instance.

Answer: A, B, D

Explanation:

According to the Juniper documentation, filter-based forwarding (FBF) is a technique that allows the SRX Series device to forward packets based on firewall filter rules, rather than the default routing table¹. FBF can be used to implement policy-based routing, load balancing, or traffic engineering². To deploy FBF on the SRX Series device for incoming traffic sourced from the 10.10.100.0/24 network, the following steps are required:

You must create a forwarding-type routing instance. A forwarding-type routing instance is a special type of routing instance that is used for FBF. It does not have any interfaces or routing protocols associated

with it, but it has its own routing table that can be populated by static routes, RIB groups, or routing policies³. You can create a forwarding-type routing instance by using the following command:

```
set routing-instances <instance-name> instance-type forwarding
```

You must create and apply a firewall filter that matches on the source address 10.10.100.0/24 and then sends this traffic to your routing instance. A firewall filter is a set of rules that can match on various packet attributes, such as source and destination addresses, ports, protocols, and so on. You can use the then routing-instance action to specify the routing instance that the packet should be forwarded to⁴. You can create and apply a firewall filter by using the following commands:

```
set firewall family inet filter <filter-name> term <term-name> from source-address 10.10.100.0/24 set
firewall family inet filter <filter-name> term <term-name> then routing-instance <instance-name> set
interfaces <interface-name> unit <unit-number> family inet filter input <filter-name>
```

You must create a RIB group that adds interface routes to your routing instance. A RIB group is a mechanism that allows you to import routes from one routing table to another. You can use a RIB group to add the interface routes of the ingress interface to the routing table of the forwarding-type routing instance. This will ensure that the SRX device can forward the packets to the correct next hop based on the destination address⁵. You can create a RIB group by using the following commands:

```
set routing-options rib-groups <rib-group-name> import-rib inet.0 set routing-options rib-groups <rib-
group-name> import-rib <instance-name>.inet.0 set routing-instances <instance-name> routing-options
instance-import <rib-group-name>
```

The following steps are not required or incorrect:

You do not need to create a VRF-type routing instance. A VRF-type routing instance is a type of routing instance that is used for virtual routing and forwarding. It allows you to create multiple logical routers on the same physical device, each with its own interfaces, routing protocols, and routing tables. VRF-type routing instances are typically used for VPNs, MPLS, or network segmentation. However, they are not necessary for FBF, which can be achieved with a forwarding-type routing instance.

You do not need to create and apply a firewall filter that matches on the destination address 10.10.100.0/24 and then sends this traffic to your routing instance. This would be redundant and unnecessary, as the destination address of the incoming traffic is already determined by the routing table of the forwarding-type routing instance. Moreover, this would create a loop, as the traffic would be sent back to the same routing instance that it came from.

Question: 8

You are connecting two remote sites to your corporate headquarters site. You must ensure that all traffic is secured and sent directly between sites In this scenario, which VPN should be used?

- A. IPsec ADVPN
- B. hub-and-spoke IPsec VPN
- C. Layer 2 VPN
- D. full mesh Layer 3 VPN with EBGP

Answer: A

Explanation:

According to the Juniper documentation, the best VPN type for connecting two remote sites to the corporate headquarters site while ensuring that all traffic is secured and sent directly between sites is IPsec ADVPN. ADVPN stands for Auto Discovery VPN, which is a feature that allows the SRX Series devices to dynamically establish IPsec tunnels between remote sites without requiring a full mesh configuration¹. IPsec ADVPN uses NHRP (Next Hop Resolution Protocol) to discover the optimal path between two remote sites and create a shortcut tunnel that bypasses the hub device². This reduces the latency and bandwidth consumption of the traffic and improves the performance and scalability of the VPN.

To configure IPsec ADVPN on the SRX Series devices, the following steps are required:

Configure the hub device as an NHRP server and assign it a unique NHRP network ID and a public IP address³.

Configure the spoke devices as NHRP clients and register them with the hub device using the same NHRP network ID and the hub's public IP address³.

Configure the IPsec VPN parameters on the hub and spoke devices, such as the IKE and IPsec proposals, policies, and gateways⁴.

Configure the routing protocols on the hub and spoke devices, such as OSPF or BGP, to advertise the routes between the sites.

Once the IPsec ADVPN is configured, the hub and spoke devices will establish IPsec tunnels with each other and exchange NHRP information. When a spoke device needs to send traffic to another spoke device, it will send an NHRP resolution request to the hub device, which will reply with the public IP address of the destination spoke device. The source spoke device will then initiate a shortcut IPsec tunnel with the destination spoke device and send the traffic directly to it².

The following VPN types are not suitable for this scenario:

Hub-and-spoke IPsec VPN: This type of VPN requires that all traffic between the remote sites go through the hub device, which adds latency and consumes bandwidth. It also does not scale well as the number of remote sites increases.

Layer 2 VPN: This type of VPN allows the remote sites to extend their Layer 2 networks over a Layer 3 network, such as the internet. It is typically used for data center interconnection or service provider networks. However, it does not provide any security or encryption for the traffic, and it may not be compatible with the existing network infrastructure.

Full mesh Layer 3 VPN with EBGP: This type of VPN allows the remote sites to exchange Layer 3 routing information over a Layer 3 network, such as the internet, using EBGP (External Border Gateway Protocol). It is typically used for enterprise networks or service provider networks. However, it requires that each remote site has a unique AS (Autonomous System) number and a public IP address, and that each remote site establishes a BGP session with every other remote site. This can be complex and cumbersome to configure and maintain, and it may not provide any security or encryption for the traffic.

Question: 9

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)

- A. Define an advanced-anti-malware policy under [edit services].
- B. Attach the security-metadata-streaming policy to a security
- C. Define a security-metadata-streaming policy under [edit

D. Attach the advanced-anti-malware policy to a security policy.

Answer: B, C

Explanation:

According to the Juniper documentation, the steps to detect domain generation algorithms (DGA) on an SRX Series firewall are as follows:

Define a security-metadata-streaming policy under [edit services]. A security-metadata-streaming policy is a configuration that enables the SRX Series firewall to collect and stream security metadata, such as DNS queries and responses, to Juniper ATP Cloud for analysis. Juniper ATP Cloud uses machine learning models and known pre-computed DGA domain names to provide domain verdicts, which helps in-line blocking and sinkholing of DNS queries on SRX Series firewalls¹. You can define a security-metadata-streaming policy by using the following command:

```
set services security-metadata-streaming policy <policy-name>
```

Attach the security-metadata-streaming policy to a security zone. A security zone is a logical grouping of interfaces that have similar security requirements. You can attach the security-metadata-streaming policy to a security zone by using the following command:

```
set security zones security-zone <zone-name> services security-metadata-streaming policy <policy-name>
```

The following steps are not required or incorrect:

Define an advanced-anti-malware policy under [edit services]. An advanced-anti-malware policy is a configuration that enables the SRX Series firewall to scan files for malware using Juniper ATP Cloud. It is not related to DGA detection².

Attach the advanced-anti-malware policy to a security policy. A security policy is a configuration that defines the rules for permitting or denying traffic between security zones. It is not related to DGA detection³.

Question: 10

In Juniper ATP Cloud, what are two different actions available in a threat prevention policy to deal with an infected host? (Choose two.)

- A. Send a custom message
- B. Close the connection.
- C. Drop the connection silently.
- D. Quarantine the host.

Answer: B, D

Explanation:

In Juniper ATP Cloud, a threat prevention policy allows you to define how the system should handle an infected host. Two of the available actions are:

Close the connection: This action will close the connection between the infected host and the destination to which it is trying to connect. This will prevent the host from communicating with the destination and will stop any malicious activity.

Quarantine the host: This action will isolate the infected host from the network by placing it in a quarantine VLAN. This will prevent the host from communicating with other devices on the network, which will prevent it from spreading malware or exfiltrating data.

Sending a custom message is used to notify the user and administrator of the action taken. Drop the connection silently is not an action available in Juniper ATP Cloud.

According to the Juniper documentation, the threat prevention policy in Juniper ATP Cloud is a configuration that defines the actions and notifications for different threat levels of the traffic. The threat levels are based on the verdicts returned by Juniper ATP Cloud after analyzing the files, URLs, and domains. The threat levels range from 1 to 10, where 1 is the lowest and 10 is the highest¹.

The threat prevention policy allows the user to specify different actions for different threat levels. The actions can be applied to the traffic or to the infected host. The actions available for the traffic are:

Permit: Allows the traffic to pass through the SRX Series device without any interruption.

Block: Blocks the traffic and sends a reset packet to the client and the server.

Drop: Drops the traffic silently without sending any reset packet.

Redirect: Redirects the traffic to a specified URL, such as a warning page or a sinkhole server.

The actions available for the infected host are:

None: Does not take any action on the infected host.

Quarantine: Quarantines the infected host by applying a firewall filter that blocks all outbound traffic from the host, except for the traffic to Juniper ATP Cloud or the specified redirect URL.

Custom: Executes a custom script on the SRX Series device to perform a user-defined action on the infected host, such as sending an email notification or triggering an external system.

Therefore, the two different actions available in a threat prevention policy to deal with an infected host are:

Block: This action will block the traffic from or to the infected host and send a reset packet to the client and the server. This will prevent the infected host from communicating with the malicious server or spreading the malware to other hosts.

Quarantine: This action will quarantine the infected host by blocking all outbound traffic from the host, except for the traffic to Juniper ATP Cloud or the redirect URL. This will isolate the infected host from the network and allow the user to remediate the infection.

The following actions are not available or incorrect:

Send a custom message: This is not an action available in the threat prevention policy. However, the user can use the custom action to execute a script that can send a custom message to the infected host or the administrator.

Drop the connection silently: This is an action available for the traffic, not for the infected host. It will drop the traffic without sending any reset packet, which may not be effective in stopping the infection or notifying the user.

For More Information – Visit link below:
<https://www.testsexpert.com/>

16\$ Discount Coupon: **9M2GK4NW**

Features:

■ Money Back Guarantee.....



■ 100% Course Coverage.....



■ 90 Days Free Updates.....



■ Instant Email Delivery after Order.....

