

Juniper.JN0-636.by.VuanQ.88q

Number: JN0-636
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: JN0-636
Exam Name: Security, Professional



Exam A

QUESTION 1

You are asked to determine if the 203.0.113.5 IP address has been added to the third-party security feed, DS hield, from Juniper SecInte1. You have an SRX Series device that is using SecInte1 feeds from Juniper ATP Cloud. Which command will return this information?

- A. `show security dynamic—address category—name CC | match 203.0.113.5`
- B. `show security dynamic—address category—name Infected—Hosts | match 203.0.113.5`
- C. `show security dynamic-address category-name IP Filter I match 203.0.113.5`
- D. `show Security dynamic-address category-name JWAS | match 203.0.113.5`

Correct Answer: A

Section:

Explanation:

The command "show security dynamic-address category-name DS hield" will show the IP addresses that are part of the DS hield category. By filtering the output of this command with the "match 203.0.113.5" command, you can determine if the IP address 203.0.113.5 is part of the DS hield feed.

This command will check the feeds that are configured on SRX Series device and are associated to juniper ATP Cloud.

QUESTION 2

You want to use selective stateless packet-based forwarding based on the source address. In this scenario, which command will allow traffic to bypass the SRX Series device flow daemon?

- A. `set firewall family inet filter bypaa3_flowd term t1 then skip—services accept`
- B. `set firewall family inet filter bypass_flowd term t1 then routing-instance stateless`
- C. `set firewall family inet filter bypas3_flowd term t1 then virtual-channel stateless`
- D. `set firewall family inet filter bypass__f lowd term t1 then packet—mode`

Correct Answer: D

Section:

Explanation:

The command that will allow traffic to bypass the SRX Series device flow daemon based on the source address is `set firewall family inet filter bypass_flowd term t1 then packet-mode`. This command configures a stateless firewall filter named `bypass_flowd` that has one term `t1`. The term `t1` can match the traffic based on the source address or any other criteria. The term `t1` then applies the action `packet-mode`, which means that the traffic will be forwarded using packet-based processing and will not be sent to the flow daemon for stateful inspection. This feature is known as selective stateless packet-based forwarding and it allows you to use both flow-based and packet-based forwarding on the same device for different types of traffic. You can apply the firewall filter to the input or output direction of an interface to enable selective stateless packet-based forwarding for the traffic passing through that interface. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-option-filterbased-forwarding-overview.html

https://www.juniper.net/documentation/en_US/junos/topics/example/filter-based-forwardingexample.html

QUESTION 3

Exhibit.

```

(edit security nat)
user@host# show
source {
  pool servers {
    address {
      198.51.100.240/32 to 198.51.100.254/32;
    }
    address-persistent subscriber ipv6-prefix-length 64;
  }
}
rule-set RS1 {
  from zone trust;
  to zone untrust;
  rule R1 {
    match {
      source-address 2001:db8::/32;
      destination-address 198.51.100.198/32;
    }
    then {
      source-nat {
        pool {
          servers;
        }
      }
    }
  }
}

```

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

- A. The configured solution allows IPv6 to IPv4 translation.
- B. The configured solution allows IPv4 to IPv6 translation.
- C. The IPv6 address is invalid.
- D. External hosts cannot initiate contact.

Correct Answer: A, C

Section:

QUESTION 4

You opened a support ticket with JTAC for your Juniper ATP appliance. JTAC asks you to set up access to the device using the reverse SSH connection. Which three settings must be configured to satisfy this request? (Choose three.)

- A. Enable JTAC remote access
- B. Create a temporary root account.
- C. Enable a JATP support account.
- D. Create a temporary admin account.
- E. Enable remote support.

Correct Answer: C, D, E

Section:

Explanation:

<https://kb.juniper.net/InfoCenter/index?page=content&id=TN326&cat=&actp=LIST&showDraft=false>

QUESTION 5

The monitor traffic interface command is being used to capture the packets destined to and the from the SRX Series device. In this scenario, which two statements related to the feature are true? (Choose two.)

- A. This feature does not capture transit traffic.
- B. This feature captures ICMP traffic to and from the SRX Series device.
- C. This feature is supported on high-end SRX Series devices only.
- D. This feature is supported on both branch and high-end SRX Series devices.

Correct Answer: A, D

Section:

Explanation:

<https://forums.juniper.net/t5/Ethernet-Switching/monitor-traffic-interface/td-p/462528>

QUESTION 6

You have a webserver and a DNS server residing in the same internal DMZ subnet. The public Static NAT addresses for the servers are in the same subnet as the SRX Series devices internet-facing interface. You implement DNS doctoring to ensure remote users can access the webserver. Which two statements are true in this scenario? (Choose two.)

- A. The DNS doctoring ALG is not enabled by default.
- B. The Proxy ARP feature must be configured.
- C. The DNS doctoring ALG is enabled by default.
- D. The DNS CNAME record is translated.

Correct Answer: B, C

Section:



QUESTION 7

You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance. What would be a cause of this problem?

- A. The collector must have a minimum of two interfaces.
- B. The collector must have a minimum of three interfaces.
- C. The collector must have a minimum of five interfaces.
- D. The collector must have a minimum of four interfaces.

Correct Answer: D

Section:

Explanation:

https://www.juniper.net/documentation/en_US/releaseindependent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypotdetection.html

QUESTION 8

You are requested to enroll an SRX Series device with Juniper ATP Cloud. Which statement is correct in this scenario?

- A. If a device is already enrolled in a realm and you enroll it in a new realm, the device data or configuration information is propagated to the new realm.
- B. The only way to enroll an SRX Series device is to interact with the Juniper ATP Cloud Web portal.

- C. When the license expires, the SRX Series device is disenrolled from Juniper ATP Cloud without a grace period
- D. Juniper ATP Cloud uses a Junos OS op script to help you configure your SRX Series device to connect to the Juniper ATP Cloud service.

Correct Answer: D

Section:

Explanation:

Juniper ATP Cloud is a cloud-based service that provides advanced threat prevention and detection for SRX Series devices. To enroll an SRX Series device with Juniper ATP Cloud, you need to have a valid license and authorization code, and you need to run a Junos OS op script on the device. The op script performs the following tasks:

Downloads and installs certificate authority (CA) licenses onto your SRX Series device.

Creates local certificates and enrolls them with the cloud server.

Performs basic Juniper ATP Cloud configuration on the SRX Series device.

Establishes a secure connection to the cloud server.

You can run the op script either by copying the CLI command from the Juniper ATP Cloud Web Portal and running it on the device, or by using the enroll command on the device. The op script is the only way to enroll an SRX Series device with Juniper ATP Cloud. You cannot enroll the device manually or by using other methods.

The other statements in the question are incorrect for the following reasons:

If a device is already enrolled in a realm and you enroll it in a new realm, none of the device data or configuration information is propagated to the new realm. This includes history, infected hosts feeds, logging, API tokens, and administrator accounts. You can view and change the realm association of a device from the Realm Management page in the Juniper ATP Cloud Web Portal.

The only way to enroll an SRX Series device is not to interact with the Juniper ATP Cloud Web Portal.

You can also use the enroll command on the device, which performs all the necessary enrollment steps without requiring you to access the Web Portal.

When the license expires, the SRX Series device is not disenrolled from Juniper ATP Cloud without a grace period. The device enters a grace period of 30 days, during which it can still send files to the cloud for inspection and receive threat intelligence feeds. After the grace period, the device is disenrolled and stops communicating with the cloud.

Reference:

How to Enroll Your SRX Series Firewalls in Juniper Advanced Threat Prevention (ATP) Cloud Using Policy Enforcer

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal

ATP Cloud | Step 2: Up and Running

Enroll an SRX Series Firewall Using the CLI



QUESTION 9

Exhibit

```
user@srx> show security macsec statistics interface ge-0/0/0 detail
Interface name: ge-0/0/0
Secure Channel transmitted
  Encrypted packets: 0
  Encrypted bytes: 0
  Protected packets: 2397
  Protected bytes: 129922
Secure Association transmitted
  Encrypted packets: 0
  Protected packets: 2397
Secure Channel received
  Accepted packets: 2395
  Validated bytes: 0
  Decrypted bytes: 0
Secure Association received
  Accepted packets: 2395
  Validated bytes: 0
  Decrypted bytes: 0
```

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

- A. The data that traverses the ge-0/0/70 interface is secured by a secure association key.
- B. The data that traverses the ge-070/0 interface can be intercepted and read by anyone.
- C. The data that traverses the ge-070/0 interface cannot be intercepted and read by anyone.
- D. The data that traverses the ge-0/0/0 interface is secured by a connectivity association key.

Correct Answer: A, C

Section:

Explanation:

The exhibit shows the output of the show security macsec statistics interface ge-0/0/70 detail command on an SRX Series device. This command displays the statistics for the Media Access Control Security (MACsec) feature on the ge-0/0/70 interface. MACsec is a feature that provides point-to-point security on Ethernet links by using encryption and data integrity checks. MACsec uses two types of keys to secure the traffic: the Connectivity Association Key (CAK) and the Secure Association Key (SAK). The CAK is used for authentication and key exchange between the MACsec peers. The SAK is used for encryption and decryption of the MACsec traffic.

The two statements that are true based on the exhibit are:

The data that traverses the ge-0/0/70 interface is secured by a secure association key. This is because the exhibit shows that the interface has a Secure Channel (SC) and a Secure Association (SA) established. The SC is a logical connection between the MACsec peers that carries the encrypted traffic. The SA is a subset of the SC that contains the SAK and other parameters for encrypting and decrypting the traffic. The exhibit shows that the interface has encrypted and protected packets, which means that the traffic is secured by the SAK.

The data that traverses the ge-0/0/70 interface cannot be intercepted and read by anyone. This is because the exhibit shows that the interface has encryption enabled. The encryption option indicates whether the MACsec traffic is encrypted or not. If encryption is enabled, the traffic is encrypted by the SAK and cannot be viewed by anyone monitoring the link. If encryption is disabled, the traffic is only protected by the SAK and can be viewed by anyone monitoring the link.

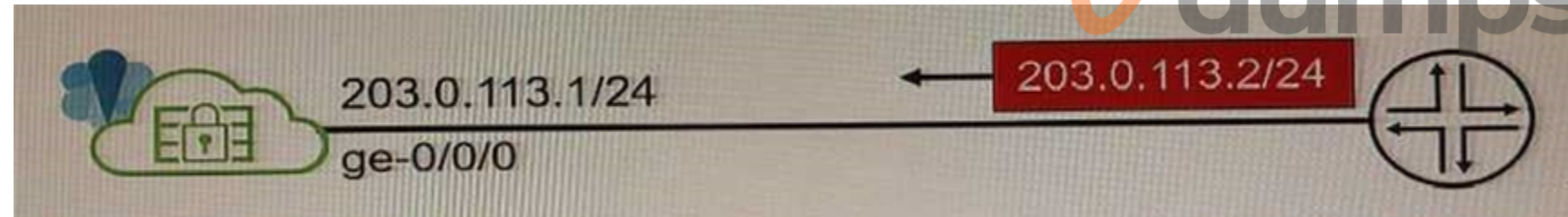
Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-security-macsec-statistics-interface-detail.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-macsecoverview.html

QUESTION 10

Exhibit



You configure Source NAT using a pool of addresses that are in the same subnet range as the external ge-0/0/0 interface on your vSRX device. Traffic that is exiting the internal network can reach external destinations, but the return traffic is being dropped by the service provider router.

Referring to the exhibit, what must be enabled on the vSRX device to solve this problem?

- A. STUN
- B. Proxy ARP
- C. Persistent NAT
- D. DNS Doctoring

Correct Answer: B

Section:

Explanation:

Proxy ARP is a technique used by routers to answer ARP requests on one network segment on behalf of hosts on another network segment. This is useful in situations where a host on one network segment needs to communicate with a host on another network segment, but the two hosts are not directly connected. In this case, the router acts as a proxy, answering ARP requests on behalf of the other host. In the exhibit, the vSRX device is configured to use a pool of addresses that are in the same subnet as the external interface ge-0/0/0 for source NAT. This means that the vSRX device will translate the source IP address of the internal hosts to one of the addresses in the pool before sending the packets to the external network. However, the external hosts will not know how to reach the NATed addresses, since they are not directly connected to the vSRX device. They will send ARP requests for the NATed addresses, expecting to receive a MAC address from the vSRX device. If proxy ARP is not enabled on the vSRX device, it will not respond to these ARP requests, since it does not have the NATed

addresses configured on its interface. The ARP requests will time out and the packets will be dropped by the external hosts or the service provider router. To solve this problem, proxy ARP must be enabled on the vSRX device for the NATed addresses. This will allow the vSRX device to respond to the ARP requests from the external hosts, providing its own MAC address as the destination. The external hosts will then send the packets to the vSRX device, which will reverse the NAT and forward the packets to the internal hosts. Reference:

Configuring Proxy ARP (CLI Procedure)

[SRX] When and how to configure Proxy ARP (https://supportportal.juniper.net/s/article/SRXDynamic-VPN-scenario-for-configuring-Proxy-ARP-on-SRX?language=en_US)

QUESTION 11

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

Correct Answer: A

Section:

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.

Reference: 1: Auto Discovery VPN Overview 2: Understanding Auto Discovery VPN 3: Configuring NHRP on the Hub and Spoke Devices 4: Configuring IPsec VPN on the Hub and Spoke Devices :

[Configuring Routing Protocols on the Hub and Spoke Devices] : [Hub-and-Spoke VPNs Overview] :

[Layer 2 VPNs Feature Guide for Security Devices] : [Layer 3 VPNs Feature Guide for Security Devices]

QUESTION 12

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.

Correct Answer: B, C

Section:

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 <policyname>
```

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.

Reference: 1: Configuring Security Metadata Streaming 2: Configuring Advanced Anti-Malware Policies 3: Configuring Security Policies

QUESTION 13

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.



Correct Answer: B, D

Section:

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.

Reference: 1: Configuring Threat Prevention Policies

QUESTION 14

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.
```

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

- A. This is the last packet in the session.
- B. The SRX Series device is performing both source and destination NAT on this session.
- C. This is the first packet in the session.
- D. The SRX Series device is performing only source NAT on this session.

Correct Answer: B, C

Section:

Explanation:

The SRX Series device is performing both source and destination NAT on this session because the traceoptions output shows that both source and destination IP addresses and ports are translated.

The source IP address 192.168.5.2 is translated to 192.168.100.1 and the destination IP address 1.1.1.1 is translated to 192.168.5.1. The source port 0 is translated to 14777 and the destination port 80 is translated to 80. The traceoptions output also shows the rule and pool IDs for both source and destination NAT: 2/32770 and 1/1 respectively.

This is the first packet in the session because the traceoptions output shows the flag `flow_first_packet`, which indicates that this is the first packet of a new session. The traceoptions output also shows the flag `flow_first_src_xlate` and `flow_first_rule_dst_xlate`, which indicate that this is the first time that source and destination NAT are applied to this session.

Reference:

traceoptions (Security NAT) | Junos OS | Juniper Networks

[SRX] How to interpret Flow TraceOptions output for NAT troubleshooting

QUESTION 15

Exhibit




```

Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.201.10/59009->
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug  3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT: packet [64] ipid =
36644, @0xef3edece
Aug  3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT: ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug  3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug  3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug  3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT: no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Aug  3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_addr 10.0.1.129, sp 59009, dp 22
Aug  3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT: chose interface ge-
0/0/4.0 as incoming nat if.
Aug  3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug  3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT: flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug  3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug  3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: denied by policy Deny-
Telnet(5), dropping pkt
Aug  3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT: packet dropped,
policy deny.

```

Which two statements are correct about the output shown in the exhibit. (Choose two.)

- A. The source address is translated.
- B. The packet is an SSH packet
- C. The packet matches a user-configured policy
- D. The destination address is translated.

Correct Answer: A, B

Section:

Explanation:

The source address is translated because the traceoptions output shows that the source IP address 192.168.5.2 is translated to 192.168.100.1 and the source port 0 is translated to 14777. The traceoptions output also shows the flag `flow_first_src_xlate`, which indicates that this is the first time that source NAT is applied to this session.

The packet is an SSH packet because the traceoptions output shows that the application protocol is tcp/22, which is the default port for SSH. The traceoptions output also shows the flag flow_tcp_syn, which indicates that this is the first packet of a TCP connection.

Reference:

traceoptions (Security NAT) | Junos OS | Juniper Networks

[SRX] How to interpret Flow TraceOptions output for NAT troubleshooting

QUESTION 16

Which statement is true about persistent NAT types?

- A. The target-host-port parameter cannot be used with IPv4 addresses in NAT46.
- B. The target-host parameter cannot be used with IPv6 addressee in NAT64.
- C. The target-host parameter cannot be used with IPv4 addresses in NAT46
- D. The target-host-port parameter cannot be used with IPv6 addresses in NAT64

Correct Answer: D

Section:

Explanation:

NAT (Network Address Translation) is a method to map one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. There are different types of NAT, one of them is the persistent NAT which is a type of NAT that allows you to map the same internal IP address to the same external IP address each time a host initiates a connection.

QUESTION 17

You are deploying a virtualization solution with the security devices in your network Each SRX Series device must support at least 100 virtualized instances and each virtualized instance must have its own discrete administrative domain.

In this scenario, which solution would you choose?

- A. VRF instances
- B. virtual router instances
- C. logical systems
- D. tenant systems



Correct Answer: C

Section:

Explanation:

A logical system is a virtualization feature in SRX Series devices that allows you to create multiple, isolated virtual routers within a single physical device. Each logical system has its own routing table, firewall policies, and interfaces, and it can be managed and configured independently of the other logical systems. Logical systems are an effective way to isolate different administrative domains and to support a large number of virtualized instances.

According to the Juniper documentation, the solution that would best meet the requirements of deploying a virtualization solution with the security devices in the network is logical systems. Logical systems are a feature that allows the SRX Series device to be partitioned into multiple logical devices, each with its own discrete administrative domain, routing table, firewall policies, VPNs, and interfaces¹. Each logical system can support up to 100 virtualized instances, depending on the SRX Series model and the available resources².

The following solutions are not suitable or incorrect for this scenario:

VRF instances: VRF instances are a type of routing instance that allows the SRX Series device to maintain multiple routing tables for different VPNs or customers. However, VRF instances do not provide separate administrative domains, firewall policies, or interfaces for each instance³.

Virtual router instances: Virtual router instances are a type of routing instance that allows the SRX Series device to create multiple logical routers, each with its own routing table and interfaces.

However, virtual router instances do not provide separate administrative domains or firewall policies for each instance.

Tenant systems: Tenant systems are a feature that allows the SRX Series device to create multiple logical devices, each with its own discrete administrative domain, routing table, firewall policies, VPNs, and interfaces.

However, tenant systems are only supported on the SRX1500, SRX4100, and SRX4200 devices, and each tenant system can only support up to 10 virtualized instances.

Reference: 1: Understanding Logical Systems 2: SRX Series Logical Systems Feature Guide 3: vrf (Routing Instances) : [virtual-router (Routing Instances)] : [Understanding Tenant Systems]

QUESTION 18

Exhibit

```
Aug 3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT: <10.10.101.10/60858-
>10.10.102.10/22;6,0x0> matched filter filter-1:
...
Aug 3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT:
flow_first_create_session
...
Aug 3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.10
Aug 3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0, 0xedba0016, 0x16)
...
Aug 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy
default-policy-logical-system-00(2), dropping pkt
Aug 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
Aug 3 02:10:28 02:10:28.045195:CID-0:THREAD_ID-01:RT:
flow_initiate_first_path: first pak no session
```

Which two statements are correct about the output shown in the exhibit? (Choose two.)

- A. The packet is processed as host inbound traffic.
- B. The packet matches the default security policy.
- C. The packet matches a configured security policy.
- D. The packet is processed in the first path packet flow.

Correct Answer: A, D

Section:

Explanation:

The packet is processed as host inbound traffic because the traceoptions output shows that the destination IP address 10.10.10.1 belongs to the SRX device itself, which is configured with the ge-0/0/1.0 interface. The traceoptions output also shows the flag flow_host_inbound, which indicates that the packet is destined to the device.

The packet matches the default security policy because the traceoptions output shows that the policy name is default-deny, which is the implicit system-default security policy that denies all packets. The traceoptions output also shows the flag flow_policy_deny, which indicates that the packet is denied by the policy.

Reference:

traceoptions (Security NAT) | Junos OS | Juniper Networks

[SRX] How to interpret Flow TraceOptions output for NAT troubleshooting Default Security Policies | Junos OS | Juniper Networks

QUESTION 19

Your company wants to use the Juniper SecIntel feeds to block access to known command and control servers, but they do not want to use Security Director to manage the feeds.

Which two Juniper devices work in this situation? (Choose two)

- A. EX Series devices
- B. MX Series devices
- C. SRX Series devices
- D. QFX Series devices

Correct Answer: B, C

Section:

Explanation:

Juniper MX and SRX series devices support the integration of SecIntel feeds, which provide information about known command and control servers, for the purpose of blocking access to them.

These devices can be configured to use the SecIntel feeds without the need for Security Director to manage the feeds.

EX series and QFX series devices are not capable of working in this situation, as they do not support the integration of SecIntel feeds.

According to the Juniper documentation, the two Juniper devices that work in this situation are MX Series devices and SRX Series devices. These devices can use the Juniper SecIntel feeds to block access to known command and control servers without using Security Director to manage the feeds.

The Juniper SecIntel feeds are curated and verified threat intelligence data that are continuously collected from Juniper ATP Cloud, Juniper Threat Labs, and other sources. The SecIntel feeds include command and control IPs, URLs, certificate hashes, and domains that are used by attackers to control malware or maintain their connection to the network¹.

The MX Series devices and the SRX Series devices can subscribe to the SecIntel feeds by using the following steps:

Configure the SecIntel service on the device by specifying the SecIntel URL, the SecIntel policy, and the SecIntel license².

Configure the SecIntel policy on the device by specifying the SecIntel feeds, the SecIntel actions, and the SecIntel logging³.

Apply the SecIntel policy to the security zones or the firewall policies on the device by using the secintel-policy option⁴.

Once the SecIntel service is configured and applied, the MX Series devices and the SRX Series devices will receive the SecIntel feeds from Juniper ATP Cloud and use them to block the traffic from or to the command and control servers. The SecIntel service will also send the SecIntel logs to Juniper ATP Cloud or a third-party SIEM solution for further analysis and reporting.

The following devices are not suitable or incorrect for this situation:

EX Series devices: EX Series devices are Ethernet switches that can integrate with SecIntel to block infected hosts at the switch port. However, they cannot use the SecIntel feeds to block command and control servers, as they do not support the SecIntel service or policy.

QFX Series devices: QFX Series devices are Ethernet switches that can integrate with SecIntel to block infected hosts at the switch port. However, they cannot use the SecIntel feeds to block command and control servers, as they do not support the SecIntel service or policy.

Reference: 1: SecIntel Threat Intelligence 2: Configuring SecIntel Service 3: Configuring SecIntel

Policy 4: Applying SecIntel Policy : [SecIntel Logging] : [SecIntel Integration with EX Series Switches] :

[SecIntel Integration with QFX Series Switches]

QUESTION 20

To analyze and detect malware, Juniper ATP Cloud performs which two functions? (Choose two.)

- A. cache lookup: to see if the file is seen already and known to be malicious
- B. antivirus scan: with a single vendor solution to see if the file contains any potential threats
- C. dynamic analysis: to see what happens if you execute the file in a real environment
- D. static analysis: to see what happens if you execute the file in a real environment

Correct Answer: A, C

Section:

Explanation:

Juniper ATP Cloud performs cache lookup to see if the file is seen already and known to be malicious and dynamic analysis to see what happens if you execute the file in a real environment.

Cache lookup is one of the functions that Juniper ATP Cloud performs to analyze and detect malware.

Cache lookup is the first step in the pipeline approach that Juniper ATP Cloud uses to examine files.

Cache lookup checks whether the file has been seen before and whether it has a stored verdict in the database. If the file is known to be malicious, the verdict is returned to the SRX Series Firewall and the file is dropped. If the file is not found in the cache, the analysis continues with the other techniques¹.

Dynamic analysis is another function that Juniper ATP Cloud performs to analyze and detect malware. Dynamic analysis runs the file in a sandbox environment and observes its behavior and actions. Dynamic analysis can reveal the hidden or obfuscated functionality of malware, such as network connections, file modifications, registry changes, and process injections. Dynamic analysis can also detect zero-day threats and evasive malware that try to avoid static analysis¹.

Reference:

How is Malware Analyzed and Detected? | ATP Cloud | Juniper Networks

QUESTION 21

Exhibit

```
user@SRX> show security flow session
...
Session ID: 4546, Policy name: policy1/8, Timeout: 4, Valid
  In: 10.10.10.2/6 --> 10.10.20.2/1382;icmp, Conn Tag 0x0, If: st0.0, Pkts: 1,
Bytes: 84
  Out: 10.20.20.2/1382 --> 10.10.10.2/6;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
Session ID: 4547, Policy name: policy2/5, Timeout: 4, Valid
  In: 10.20.20.2/226 --> 10.10.10.2/38703;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
  Out: 10.10.10.2/38703 --> 10.10.20.2/226;icmp, Conn Tag 0x0, If: st0.0, Pkts:
1, Bytes: 84
Total sessions: 13
```

You are validating bidirectional traffic flows through your IPsec tunnel. The 4546 session represents traffic being sourced from the remote end of the IPsec tunnel. The 4547 session represents traffic that is sourced from the local network destined to the remote network.

Which statement is correct regarding the output shown in the exhibit?

- A. The remote gateway address for the IPsec tunnel is 10.20.20.2
- B. The session information indicates that the IPsec tunnel has not been established
- C. The local gateway address for the IPsec tunnel is 10.20.20.2
- D. NAT is being used to change the source address of outgoing packets



Correct Answer: C

Section:

Explanation:

According to the output shown in the exhibit, which is a security flow session on an SRX Series device, the correct statement is that the local gateway address for the IPsec tunnel is 10.20.20.2. This is indicated by the line In: 10.20.20.2/2060 -> 10.20.20.1/3382, which shows that the source IP address of the incoming packet is 10.20.20.2, which is the local gateway address of the IPsec tunnel.

The destination IP address of the incoming packet is 10.20.20.1, which is the remote gateway address of the IPsec tunnel.

The following statements are incorrect or not supported by the output:

The remote gateway address for the IPsec tunnel is 10.20.20.2. This is false, as explained above. The remote gateway address for the IPsec tunnel is 10.20.20.1, not 10.20.20.2.

The session information indicates that the IPsec tunnel has not been established. This is false, as the output shows that there are two active sessions with the communication tag IPsec VPN: vpn1, which indicates that the IPsec tunnel has been established and is named vpn1.

NAT is being used to change the source address of outgoing packets. This is not supported by the output, as there is no indication of NAT being applied to the outgoing packets. The source IP address of the outgoing packet is 192.168.1.1, which is the same as the source IP address of the original packet. If NAT was being used, the source IP address of the outgoing packet would be different from the source IP address of the original packet.

Reference: 1: show security flow session - Technical Documentation - Support - Juniper Networks

QUESTION 22

Exhibit

```

Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.101.10/59009-
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug  3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT: packet [64] ipid =
36644, @0xef3edece
Aug  3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT: ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug  3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug  3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug  3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT: no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Aug  3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_addr 10.0.1.129, sp 59009, dp 22
Aug  3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT: chose interface ge-
0/0/4.0 as incoming nat if.
Aug  3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug  3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT: flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug  3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug  3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: denied by policy Deny-
Telnet(5), dropping pkt
Aug  3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT: packet dropped,
policy deny.

```

Which two statements are correct about the output shown in the exhibit? (Choose two.)

- A. The packet is silently discarded.
- B. The packet is part of an existing session.
- C. The packet is part of a new session.
- D. The packet is explicitly rejected.

Correct Answer: A, C

Section:

Explanation:

The packet is silently discarded because the traceoptions output shows that the packet is dropped with the flag `flow_spu_drop`, which indicates that the packet is dropped by the SPU without sending any response to the sender. The traceoptions output also shows the reason for the drop as "no session found, start first path. in_tunnel - 0, from_cp_flag - 0" which means that the packet does not match any existing session and is not part of a

tunnel or a control plane traffic1.

The packet is part of a new session because the traceoptions output shows that the packet is the first packet of a TCP connection with the flag flow_tcp_syn, which indicates that the packet has the SYN flag set. The traceoptions output also shows that the packet is processed in the first path packet flow with the message "no session found, start first path" which means that the packet is initiating a new session1.

Reference:

traceoptions (Security Flow) | Junos OS | Juniper Networks

[SRX] How to interpret Flow TraceOptions output for NAT troubleshooting

QUESTION 23

You are asked to provide single sign-on (SSO) to Juniper ATP Cloud. Which two steps accomplish this goal? (Choose two.)

- A. Configure Microsoft Azure as the service provider (SP).
- B. Configure Microsoft Azure as the identity provider (IdP).
- C. Configure Juniper ATP Cloud as the service provider (SP).
- D. Configure Juniper ATP Cloud as the identity provider (IdP).

Correct Answer: B, C

Section:

Explanation:

To provide single sign-on (SSO) to Juniper ATP Cloud, you need to configure the following:

Microsoft Azure as the identity provider (IdP): This allows users to authenticate to Juniper ATP Cloud using their Azure credentials.

Juniper ATP Cloud as the service provider (SP): This allows Juniper ATP Cloud to accept the authentication from Microsoft Azure and provide SSO access to the users.

Configuring Microsoft Azure as the service provider (SP) and Juniper ATP Cloud as the identity provider (IdP) are not the correct steps to provide SSO, as the roles are reversed.

QUESTION 24

Which two statements are correct regarding tenant systems on SRX Series devices? (Choose two.)

- A. A maximum of 32 tenant systems can be configured on a physical SRX device.
- B. All tenant systems share a single routing protocol process.
- C. Each tenant system runs its own instance of the routing protocol process
- D. A maximum of 500 tenant systems can be configured on a physical SRX device.

Correct Answer: C, D

Section:

Explanation:

The following statements are true regarding tenant systems on SRX Series devices:

Each tenant system runs its own instance of the routing protocol process. Each tenant system is isolated, and it has its own routing table, interfaces, and security policies.

A maximum of 500 tenant systems can be configured on a physical SRX device. This allows for a high degree of flexibility and scalability, as each tenant system can be configured with its own set of features and security policies.

A maximum of 32 tenant systems can be configured on a physical SRX device and All tenant systems share a single routing protocol process are not correct statements

QUESTION 25

You are asked to allocate security profile resources to the interconnect logical system for it to work properly.

In this scenario, which statement is correct?

- A. The NAT resources must be defined in the security profile for the interconnect logical system.
- B. No resources are needed to be allocated to the interconnect logical system.
- C. The resources must be calculated based on the amount of traffic that will flow between the logical systems.
- D. The flow-session resource must be defined in the security profile for the interconnect logical system.

Correct Answer: D

Section:

Explanation:

The flow-session resource is needed in order to ensure adequate and secure communication between the two logical systems.

The flow-session resource must be defined in the security profile for the interconnect logical system because the interconnect logical system is responsible for forwarding traffic between other logical systems. The flow-session resource determines the maximum number of sessions that the interconnect logical system can create and maintain. If the flow-session resource is not allocated or is insufficient, the interconnect logical system might drop packets or fail to establish sessions.

The NAT resources are not needed to be allocated to the interconnect logical system because the interconnect logical system does not perform any NAT operations on the traffic. The NAT resources are only relevant for the logical systems that need to translate the source or destination IP addresses or ports of the traffic.

No resources are not needed to be allocated to the interconnect logical system is incorrect because the interconnect logical system still requires some resources to function properly, such as the flowsession resource. The interconnect logical system cannot operate without any resources allocated to it.

The resources must be calculated based on the amount of traffic that will flow between the logical systems is partially correct, but not the best answer. The resources must be calculated based on the amount of traffic and the type of traffic that will flow between the logical systems. For example, the flow-session resource depends on the number and duration of sessions, the security-log-streamnumber resource depends on the number and size of logs, and the NAT resource depends on the number and type of NAT rules.

Reference:

Security Profiles for Logical Systems | Junos OS | Juniper Networks

QUESTION 26

Exhibit

```
Aug 1 11:28:23 11:28:23.434801:CID-0:THREAD_ID-01:RT:<172.20.101.10/59009->
>10.0.1.129/22;6,0x0> matched filter TestFilter:
Aug 1 11:28:23 11:28:23.434805:CID-0:THREAD_ID-01:RT:packet [64] ipid = 36644,
@0xef3edece
Aug 1 11:28:23 11:28:23.434810:CID-0:THREAD_ID-01:RT:---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug 1 11:28:23 11:28:23.434817:CID-0:THREAD_ID-01:RT:ge-0/0/4.0:
172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug 1 11:28:23 11:28:23.434819:CID-0:THREAD_ID-01:RT:find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug 1 11:28:23 11:28:23.434822:CID-0:THREAD_ID-01:RT:no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 1 11:28:23 11:28:23.434826:CID-0:THREAD_ID-01:RT:flow_first_create_session
Aug 1 11:28:23 11:28:23.434834:CID-0:THREAD_ID-01:RT:flow_first_in_dst_nat: in
<ge-0/0/4.0>, out <N/A> dst_addr 10.0.1.129, sp 59009, dp 22
Aug 1 11:28:23 11:28:23.434835:CID-0:THREAD_ID-01:RT:chose interface ge-0/0/4.0
as incoming nat if.
Aug 1 11:28:23 11:28:23.434838:CID-0:THREAD_ID-01:RT:flow_first_rule_dst_xlate:
DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
```

The exhibit shows a snippet of a security flow trace.

In this scenario, which two statements are correct? (Choose two.)

- A. This packet arrived on interface ge-0/0/4.0.
- B. Destination NAT occurs.
- C. The capture is a packet from the source address 172.20.101.10 destined to 10.0.1.129.
- D. An existing session is found in the table.

Correct Answer: A, D

Section:

Explanation:

According to the security flow trace shown in the exhibit, which is a snippet of a packet capture on an SRX Series device, the two statements that are correct are:

This packet arrived on interface ge-0/0/4.0. This is indicated by the line In: 10.0.1.129/22 -> 10.0.1.129/3382;1,0x0, which shows that the ingress interface of the packet is ge-0/0/4.0, as the interface name is prefixed to the source and destination IP addresses and ports of the packet1.

An existing session is found in the table. This is indicated by the line Found: session id 0x12. sess tok 28685, which shows that the packet matches an existing session in the session table with the session ID 0x12 and the session token 286852.

The following statements are incorrect or not supported by the output:

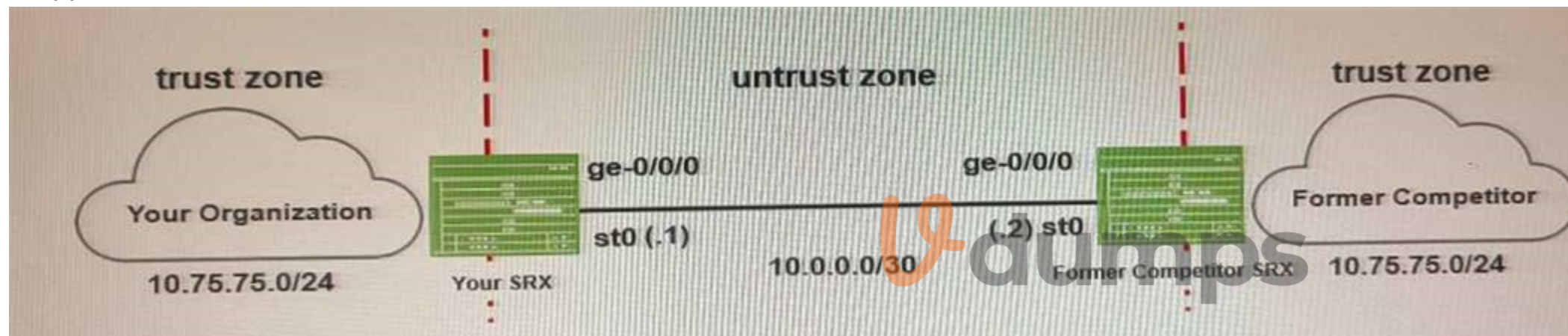
Destination NAT occurs. This is not supported by the output, as there is no indication of destination NAT being applied to the packet. The destination IP address of the packet is 10.0.1.129, which is the same as the destination IP address of the original packet. If destination NAT was applied, the destination IP address of the packet would be different from the destination IP address of the original packet.

The capture is a packet from the source address 172.20.101.10 destined to 10.0.1.129. This is false, as the output shows that the source address of the packet is 10.0.1.129, not 172.20.101.10. The source IP address of the packet is prefixed to the ingress interface name ge-0/0/4.0.

Reference: 1: Understanding Security Flow Trace 2: show security flow session - Technical Documentation - Support - Juniper Networks

QUESTION 27

Exhibit



Your company recently acquired a competitor. You want to use using the same IPv4 address space as your company.

Referring to the exhibit, which two actions solve this problem? (Choose two)

- A. Configure static NAT on the SRX Series devices.
- B. Connect the competitor network using IPsec policy-based VPNs.
- C. Identify two neutral IPv4 address spaces for address translation.
- D. Configure IPsec Transport mode.

Correct Answer: A, C

Section:

Explanation:

To solve the problem of using the same IPv4 address space as your company, you can identify two neutral IPv4 address spaces for address translation. This will allow you to use the same IPv4 address space as your company without any conflicts. Additionally, you can configure static NAT on the SRX Series devices to ensure that the traffic is properly routed between the two networks.

Static NAT is a type of network address translation that maps a private IP address to a public IP address on a one-to-one basis. Static NAT is useful when you need to expose a server or device with a private IP address to the Internet or another network with a different IP address range. Static NAT also preserves the original source or destination IP address in the packet header, which can be useful for logging or auditing purposes1.

Neutral IPv4 address spaces are IP address ranges that are not assigned to any specific organization or entity. They are usually reserved for special purposes, such as private networks, multicast, loopback, or documentation.

Neutral IPv4 address spaces can be used for address translation when there is an overlap or conflict between two networks that need to communicate with each other. For example, you can use the 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 address ranges, which are designated for private use, as neutral IPv4 address spaces for address translation2.

Reference:

SRX Getting Started - Configure VPN tunnel for site-to-site connectivity

SRX & J Series Site-to-Site VPN Configurator

QUESTION 28

Exhibit

```
user@SRX> show service security-intelligence category summary
Category name      :SecProfiling
Status             :Enable
Description        :Security Profiling Data
Update interval   :300s
TTL                :172800s
Feed name         :Proxy_Nodes
Version           :20220812.1
Objects number    :80
Create time       :2022-08-14 11:53:46 UTC
Update time      :2022-08-15 06:11:11 UTC
Update status    :Store succeeded
Expired          :No
Status           :Active
Options         :N/A
user@SRX> show security dynamic-address category-name SecProfiling feed-name
Proxy_Nodes
user@SRX>
```

You have recently configured Adaptive Threat Profiling and notice 20 IP address entries in the monitoring section of the Juniper ATP Cloud portal that do not match the number of entries locally on the SRX Series device, as shown in the exhibit.

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

- A. You must configure the DAE in a security policy on the SRX device.
- B. Refresh the feed in ATP Cloud.
- C. Force a manual download of the Proxy__Nodes feed.
- D. Flush the DNS cache on the SRX device.

Correct Answer: B

Section:

Explanation:

The correct action to solve this problem on the SRX device is to refresh the feed in ATP Cloud. This is because the number of IP address entries in the monitoring section of the Juniper ATP Cloud portal does not match the number of entries locally on the SRX Series device. This discrepancy can be caused by a number of factors, such as the SRX device not being properly configured for Adaptive Threat Profiling, or the feed not being properly downloaded from the Juniper ATP Cloud portal. By refreshing the feed in ATP Cloud, the SRX device can synchronize its local feed with the latest feed from the cloud service and ensure that the entries are consistent and accurate. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-adaptivethreat-profiling-configuring.html

QUESTION 29

You want to enroll an SRX Series device with Juniper ATP Appliance. There is a firewall device in the path between the devices. In this scenario, which port should be opened in the firewall device?

- A. 8080
- B. 443
- C. 80

D. 22

Correct Answer: B

Section:

Explanation:

This is the port used for encrypted communication between the SRX series device and the Juniper ATP Appliance

In order to enroll an SRX Series device with Juniper ATP Appliance, the firewall device must have port 443 open. Port 443 is the default port used for HTTPS traffic, the communication between the SRX Series device and the ATP Appliance needs to be encrypted, that's why this port should be opened.

QUESTION 30

Which two types of source NAT translations are supported in this scenario? (Choose two.)

- A. translation of IPv4 hosts to IPv6 hosts with or without port address translation
- B. translation of one IPv4 subnet to one IPv6 subnet with port address translation
- C. translation of one IPv6 subnet to another IPv6 subnet without port address translation
- D. translation of one IPv6 subnet to another IPv6 subnet with port address translation

Correct Answer: A, C

Section:

Explanation:

The two types of source NAT translations that are supported in this scenario are translation of IPv4 hosts to IPv6 hosts with or without port address translation, and translation of one IPv6 subnet to another IPv6 subnet without port address translation. These are the types of source NAT translations that are supported by the Junos OS for IPv6 NAT. Translation of IPv4 hosts to IPv6 hosts allows IPv4-only hosts to communicate with IPv6-only hosts by changing the source IPv4 address to a corresponding IPv6 address. Port address translation can be optionally enabled to conserve IPv6 addresses by using different port numbers for different sessions. Translation of one IPv6 subnet to another IPv6 subnet allows IPv6 hosts to use a different IPv6 address range for outbound traffic, such as for security or policy reasons. Port address translation is not supported for this type of translation, as IPv6 addresses are abundant and do not need to be conserved. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents: https://www.juniper.net/documentation/en_US/junos/topics/concept/security-nat-ipv6-overview.html

QUESTION 31

Exhibit


```

Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.101.10/59009->
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug  3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT: packet [64] ipid =
36644, @0xef3edece
Aug  3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT: ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug  3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug  3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug  3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT: no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Aug  3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_addr 10.0.1.129, sp 59009, dp 22
Aug  3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT: chose interface ge-
0/0/4.0 as incoming nat if.
Aug  3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug  3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT: flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug  3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug  3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: denied by policy Deny-
Telnet(5), dropping pkt
Aug  3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT: packet dropped,
policy deny.

```

Referring to the exhibit, which statement is true?

- A. This custom block list feed will be used before the Juniper SecIntel
- B. This custom block list feed cannot be saved if the Juniper SecIntel block list feed is configured.
- C. This custom block list feed will be used instead of the Juniper SecIntel block list feed
- D. This custom block list feed will be used after the Juniper SecIntel block list feed.

Correct Answer: C

Section:

Explanation:

According to the Juniper documentation, a custom block list feed is a user-defined list of IP addresses or URLs that are considered malicious or unwanted. A custom block list feed can be configured to override the default Juniper SecIntel block list feed, which is a cloud-based service that provides a list of known malicious IP addresses and URLs. To override the Juniper SecIntel block list feed, the custom block list feed must have a higher

priority value than the Juniper SecIntel block list feed. In the exhibit, the custom block list feed has a priority value of 10, which is higher than the default priority value of 5 for the Juniper SecIntel block list feed. Therefore, this custom block list feed will be used instead of the Juniper SecIntel block list feed. Reference: : [Configuring Custom Block List Feeds]

QUESTION 32

Exhibit

```
Profile: xyz-profile3
  Server address: 192.168.30.188
  Authentication port: 1645
  Preauthentication port: 1810
  Accounting port: 1646
  Status: UNREACHABLE
Profile: xyz-profile2
  Server address: 192.168.30.190
  Authentication port: 1812
  Preauthentication port: 1810
  Accounting port: 1813
  Status: DOWN ( 60 seconds )
Profile: xyz-profile11
  Server address: 2001:DB8:0:f101::2
  Authentication port: 1645
  Preauthentication port: 1810
  Accounting port: 1646
  Status: UP
Profile: xyz-profile7
  Server address: 192.168.30.191
  Authentication port: 1812
  Preauthentication port: 1810
  Accounting port: 1813
  Status: DOWN ( 30 seconds )
```



The show network-access aaa radius-servers command has been issued to solve authentication issues.

Referring to the exhibit, to which two authentication servers will the SRX Series device continue to send requests? (Choose TWO)

- A. 2001:DB8:0:f101::2
- B. 192.168.30.191
- C. 192.168.30.190
- D. 192.168.30.188

Correct Answer: B, C

Section:

Explanation:

The SRX Series device will continue to send requests to authentication servers 192.168.30.190 and 192.168.30.191. This is because the exhibit shows the output of the show network-access aaa radiusservers command. This command displays the status of the RADIUS servers configured on the device.

In the output, we can see that there are three RADIUS servers configured - 192.168.30.190, 192.168.30.191, and 2001:DB8:0:f101::2. However, the status of the third server is shown as "DOWN". This means that the device is not able to communicate with this server. Therefore, the device will continue to send requests to the other two servers - 192.168.30.190 and 192.168.30.191. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents: https://www.juniper.net/documentation/en_US/junos/topics/reference/commandsummary/show-network-access-aaa-radius-servers.html

QUESTION 33

All interfaces involved in transparent mode are configured with which protocol family?

- A. mpls
- B. bridge
- C. inet
- D. ethernet — switching

Correct Answer: B

Section:

Explanation:

In transparent mode, all interfaces involved are configured with the bridge protocol family. This allows the SRX device to act as a bridge between the interfaces and forward traffic transparently without any modification. The bridge interfaces can be configured to forward traffic based on layer 2 headers, such as MAC addresses, without the need for routing or IP addressing.

QUESTION 34

What are two valid modes for the Juniper ATP Appliance? (Choose two.)

- A. flow collector
- B. event collector
- C. all-in-one
- D. core

Correct Answer: C, D

Section:

Explanation:

The two valid modes for the Juniper ATP Appliance are all-in-one and core. The all-in-one mode is a single appliance that performs both the collector and the core functions. The collector function collects traffic from the network and sends it to the core function for analysis and detection. The core function performs the threat detection, mitigation, and analytics. The all-in-one mode is suitable for small to medium-sized networks that do not require high scalability or performance. The core mode is a dedicated appliance that performs only the core function. The core mode is used in conjunction with one or more collector appliances that collect traffic from the network and send it to the core appliance for analysis and detection. The core mode is suitable for large-scale networks that require high scalability and performance. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-atp-applianceoverview.html

QUESTION 35

Exhibit

```

[edit security nat source]
user@SRX# show
pool internal-voip-pool {
  address {
    203.0.113.1/32;
  }
}
rule-set support-internal-voip {
  from zone trust;
  to zone untrust;
  rule allow-voip-nat {
    match {
      source-address 10.1.1.0/24;
      destination-address 0.0.0.0/0;
    }
    then {
      source-nat {
        pool {
          internal-voip-pool;
          persistent-nat {
            permit any-remote-host;
            inactivity-timeout 180;
          }
        }
      }
    }
  }
}

```

Referring to the exhibit, an internal host is sending traffic to an Internet host using the 203.0.113.1 reflexive address with source port 54311.

Which statement is correct in this situation?

- A. Only the Internet host that the internal host originally communicated with can initiate traffic to reach the internal host using the 203.0.113.1 address, source port 54311, and a random destination port.
- B. Only the Internet host that the internal host originally communicated with can initiate traffic to reach the internal host using the 203.0.113.1 address, a random source port, and destination port 54311.
- C. Any host on the Internet can initiate traffic to reach the internal host using the 203.0.113.1 address, source port 54311, and a random destination port.
- D. Any host on the Internet can initiate traffic to reach the internal host using the 203.0.113.1 address, a random source port, and destination port 54311.

Correct Answer: B

Section:

Explanation:

According to the Juniper documentation, reflexive NAT is a type of source NAT that allows an internal host to communicate with an external host using a single public IP address and port. The reflexive NAT session is created when the internal host initiates the traffic to the external host, and the session is deleted when the traffic stops. The reflexive NAT session is bidirectional, meaning that the external host can send traffic back to the internal host using the same public IP address and port that the internal host used to reach the external host. However, the external host cannot initiate a new session to the internal host using the same public IP address and port, unless the internal host has already established a session with the external host. Therefore, only the Internet host that the internal host originally communicated with can initiate traffic to reach the internal host using the 203.0.113.1 address, a random source port, and destination port 54311. Reference: [Configuring Reflexive NAT]

QUESTION 36

Your IPsec VPN configuration uses two CoS forwarding classes to separate voice and data traffic. How many IKE security associations are required between the IPsec peers in this scenario?

- A. 1
- B. 3
- C. 4
- D. 2

Correct Answer: A

Section:**Explanation:**

An IKE security association (SA) is a set of parameters that define how the Internet Key Exchange (IKE) protocol will authenticate and establish the secure channel between the IPsec VPN peers. When you configure an IPsec VPN, one IKE SA is created between the peers, regardless of how many CoS forwarding classes are used to separate the traffic. The SA will be used to negotiate the IPsec SA parameters, such as encryption algorithms and keys. In this scenario, only 1 IKE security association is required between the IPsec peers, no matter how many CoS forwarding classes are used to separate the voice and data traffic.

QUESTION 37

You are required to deploy a security policy on an SRX Series device that blocks all known Tor network IP addresses. Which two steps will fulfill this requirement? (Choose two.)

- A. Enroll the devices with Juniper ATP Appliance.
- B. Enroll the devices with Juniper ATP Cloud.
- C. Enable a third-party Tor feed.
- D. Create a custom feed containing all current known MAC addresses.

Correct Answer: B, C

Section:**Explanation:**

The two steps that will fulfill the requirement of deploying a security policy on an SRX Series device that blocks all known Tor network IP addresses are enrolling the devices with Juniper ATP Cloud and enabling a third-party Tor feed. Juniper ATP Cloud is a cloud-based service that provides advanced threat detection and mitigation capabilities for SRX Series devices. By enrolling the devices with Juniper ATP Cloud, the devices can leverage the cloud intelligence and analytics to identify and block malicious traffic, including Tor traffic. A third-party Tor feed is a source of information that provides a list of IP addresses that are associated with the Tor network. By enabling a third-party Tor feed on the SRX Series device, the device can use the feed to create a dynamic address object that contains all the known Tor IP addresses. The device can then apply a security policy that denies traffic from or to the dynamic address object, effectively blocking the Tor network IP addresses. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-atp-cloudoverview.html

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/securityintelligence-third-party-feed-configuring.html

QUESTION 38

Your company uses non-Juniper firewalls and you are asked to provide a Juniper solution for zero-day malware protection. Which solution would work in this scenario?

- A. Juniper ATP Cloud
- B. Juniper Secure Analytics
- C. Juniper ATP Appliance
- D. Juniper Security Director

Correct Answer: A

Section:**Explanation:**

Juniper ATP Cloud provides zero-day malware protection for non-Juniper firewalls. It's a cloud-based service that analyzes files and network traffic to detect and prevent known and unknown (zero-day) threats. It uses a combination of static and dynamic analysis techniques, as well as machine learning, to detect and block malicious files, even if they are not known to traditional anti-virus software. It also provides real-time visibility and detailed forensics for incident response and remediation.

QUESTION 39

Exhibit

```

[edit]
user@branch1# show interfaces
ge-0/0/2 {
  unit 0 {
    family inet {
      dhcp;
    }
  }
}
st0 {
  unit 0 {
    family inet {
      address 10.0.0.2/30;
    }
  }
}
[edit security zones]
user@branch1# show security-zone untrust
interfaces {
  ge-0/0/2.0 {
    host-inbound-traffic {
      system-services {
        ike;
        dhcp;
      }
    }
  }
}
gateway gateway-1 {
  ike-policy ike-policy-1;
  address 203.0.113.5;
  local-identity hostname "branch1@srx.juniper.net";
  external-interface ge-0/0/2;
}
[edit security ike]
user@corporate# show
policy ike-policy-branch1 {
  mode main;
  proposal-set standard;
  pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VwYZG1AB"; ## SECRET-DATA
}
gateway gateway-branch1 {
  ike-policy ike-policy-branch1;
  dynamic hostname "branch1@srx.juniper.net";
  external-interface ge-0/0/1;
}

```

You are trying to configure an IPsec tunnel between SRX Series devices in the corporate office and branch1. You have committed the configuration shown in the exhibit, but the IPsec tunnel is not establishing. In this scenario, what would solve this problem.

- A. Add multipoint to the st0.0 interface configuration on the branch1 device.

- B. Change the IKE proposal-set to compatible on the branch1 and corporate devices.
- C. Change the local identity to inet advpn on the branch1 device.
- D. Change the IKE mode to aggressive on the branch1 and corporate devices.

Correct Answer: C

Section:

Explanation:

According to the Juniper documentation, the local identity for an IPsec VPN tunnel must match the remote identity of the peer device. The local identity can be configured as an IP address, a hostname, a distinguished name, or an advpn identifier. The advpn identifier is used for dynamic VPNs that support multiple remote endpoints. In the exhibit, the corporate device has the local identity configured as inet advpn, which means it expects the branch1 device to have the same remote identity. However, the branch1 device has the local identity configured as inet, which does not match the corporate device's remote identity. Therefore, the IKE negotiation fails and the IPsec tunnel is not established. To solve this problem, the local identity on the branch1 device should be changed to inet advpn, so that it matches the corporate device's remote identity. Reference: [Configuring an IKE Gateway] 1, [Configuring Local and Remote Identities] 2

1: <https://www.juniper.net/documentation/us/en/software/junos/vpnipsec/topics/task/configuration/security-ike-gateway-configuring.html> 2:

<https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topicmap/security-ipsec-vpn-identities.html>

QUESTION 40

Exhibit

```
[edit security policies from-zone trust to-zone untrust policy Adaptive-Threat-
Profiling]
user@SRX-1# show
match {
  source-address any;
  destination-address any;
  application any;
  dynamic-application [ junos:web:proxy junos:web:anonymizer junos:TOR ];
}
then {
  reject {
    application-services {
      security-intelligence {
        add-destination-ip-to-feed {
          Proxy_Nodes;
        }
      }
    }
  }
}
...
```

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

- A. The SRX-1 device can use the Proxy__Nodes feed in another security policy.
- B. You can use the Proxy_Nodes feed as the source-address and destination-address match criteria of another security policy on a different SRX Series device.
- C. The SRX-1 device creates the Proxy_wodes feed, so it cannot use it in another security policy.
- D. You can only use the Proxy_Node3 feed as the destination-address match criteria of another security policy on a different SRX Series device.

Correct Answer: C, D

Section:

Explanation:

The exhibit shows the output of the show security intelligence category summary command on the SRX-1 device. This command displays the status of the security intelligence categories configured on the device. In the output, we can see that there are two categories configured - Proxy_Nodes and Proxy_Node3. The Proxy_Nodes category is a custom category that is created by the SRX-1 device using the adaptive threat profiling feature. The Proxy_Node3 category is a third-party category that is downloaded from the Juniper ATP Cloud service. The Proxy_Nodes category contains the IP addresses that match the security policy named Proxy-ATP on the SRX-1 device. The Proxy_Node3 category contains the IP addresses that are associated with the Tor network.

The two statements that are true based on the exhibit are:

The SRX-1 device creates the Proxy_Nodes feed, so it cannot use it in another security policy. This is because the adaptive threat profiling feature does not allow the device that creates the feed to use it in another security policy. The feed is intended to be shared with other devices in the same realm through the Juniper ATP Cloud service. The SRX-1 device can only use the feeds that are created by other devices or downloaded from third-party sources.

You can only use the Proxy_Node3 feed as the destination-address match criteria of another security policy on a different SRX Series device. This is because the Proxy_Node3 feed is a third-party feed that is downloaded from the Juniper ATP Cloud service. The SRX-1 device can use this feed as a dynamic address object in its security policies. However, the feed is configured with the destinationonly option, which means that it can only be used as the destination-address match criteria of a security policy. The source-address match criteria of a security policy cannot use this feed.

Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/showsecurity-intelligence-category-summary.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-intelligence-thirdparty-feed-configuring.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-adaptive-threatprofiling-overview.html

QUESTION 41

You want to enforce IDP policies on HTTP traffic.

In this scenario, which two actions must be performed on your SRX Series device? (Choose two)

- A. Choose an attacks type in the predefined-attacks-group HTTP-All.
- B. Disable screen options on the Untrust zone.
- C. Specify an action of None.
- D. Match on application junos-http.

Correct Answer: A, D

Section:

Explanation:

To enforce IDP policies on HTTP traffic on an SRX Series device, the following actions must be performed:

Choose an attacks type in the predefined-attacks-group HTTP-All: This allows the SRX Series device to match on specific types of attacks that can occur within HTTP traffic. For example, it can match on SQL injection or cross-site scripting (XSS) attacks.

Match on application junos-http: This allows the SRX Series device to match on HTTP traffic specifically, as opposed to other types of traffic. It is necessary to properly identify the traffic that needs to be protected.

Disabling screen options on the Untrust zone and specifying an action of None are not necessary to enforce IDP policies on HTTP traffic. The first one is a feature used to prevent certain types of attacks, the second one is used to take no action in case of a match.

QUESTION 42

Exhibit

```
user@host> show security mka sessions summary
Interface  Member-ID          Type Status Tx Rx CAK Name
-----
ge-0/0/1   E752CAEAE8DDEFB82D4EA4BF7 preceding live 8887
           8951              8888
ge-0/0/1   0F2D5171F38EAB16C2E0CB62 fallback active 8959
           8952              FFFF
ge-0/0/1   6B49BD5CF7188F3CD9A29D30 primary in-progress 2439 0
           AAAA
```

Referring to the exhibit, which two statements are true about the CAK status for the CAK named "FFFF"? (Choose two.)

- A. CAK is not used for encryption and decryption of the MACsec session.
- B. SAK is successfully generated using this key.
- C. CAK is used for encryption and decryption of the MACsec session.
- D. SAK is not generated using this key.

Correct Answer: A, D

Section:

Explanation:

The exhibit shows the output of the show security mka sessions summary command on an SRX Series device. This command displays the status of the MACsec Key Agreement (MKA) sessions on the device. In the output, we can see that there are two CAKs configured for the interface ge-0/0/1 - FFFF and EEEE. The CAK named FFFF has the type preceding and the status live. The CAK named EEEE has the type fallback and the status active.

The two statements that are true about the CAK status for the CAK named FFFF are:

CAK is not used for encryption and decryption of the MACsec session. This is because the CAK is only used for authentication and key exchange between the MACsec peers. The CAK is not used for encrypting or decrypting the MACsec traffic. The encryption and decryption of the MACsec session is done by the Secure Association Key (SAK), which is derived from the CAK using the MKA protocol. SAK is not generated using this key. This is because the CAK named FFFF has the type preceding, which means that it is a legacy key that is used for backward compatibility with older MACsec devices. The preceding key is not used for generating the SAK, but only for authenticating the MACsec peers. The SAK is generated using the active key, which is the CAK named EEEE in this case.

Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/showsecurity-mka-sessions-summary.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-macsecoverview.html

QUESTION 43

Exhibit

```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
version v2-only;
[edit interfaces]
user@srx# show st0
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}
```

Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly.

Which two commands will solve this problem? (Choose two.)

A)

```
[edit interfaces]
user@srx# set st0.0 multipoint
```

B)

```
[edit security ike gateway advpn-gateway]
user@srx# set advpn suggerster disable
```

C)

```
[edit security ike gateway advpn-gateway]
user@srx# set local-identity inet advpn
```

D)

```
[edit security ike gateway advpn-gateway]
user@srx# set advpn partner disable
```

A. Option A

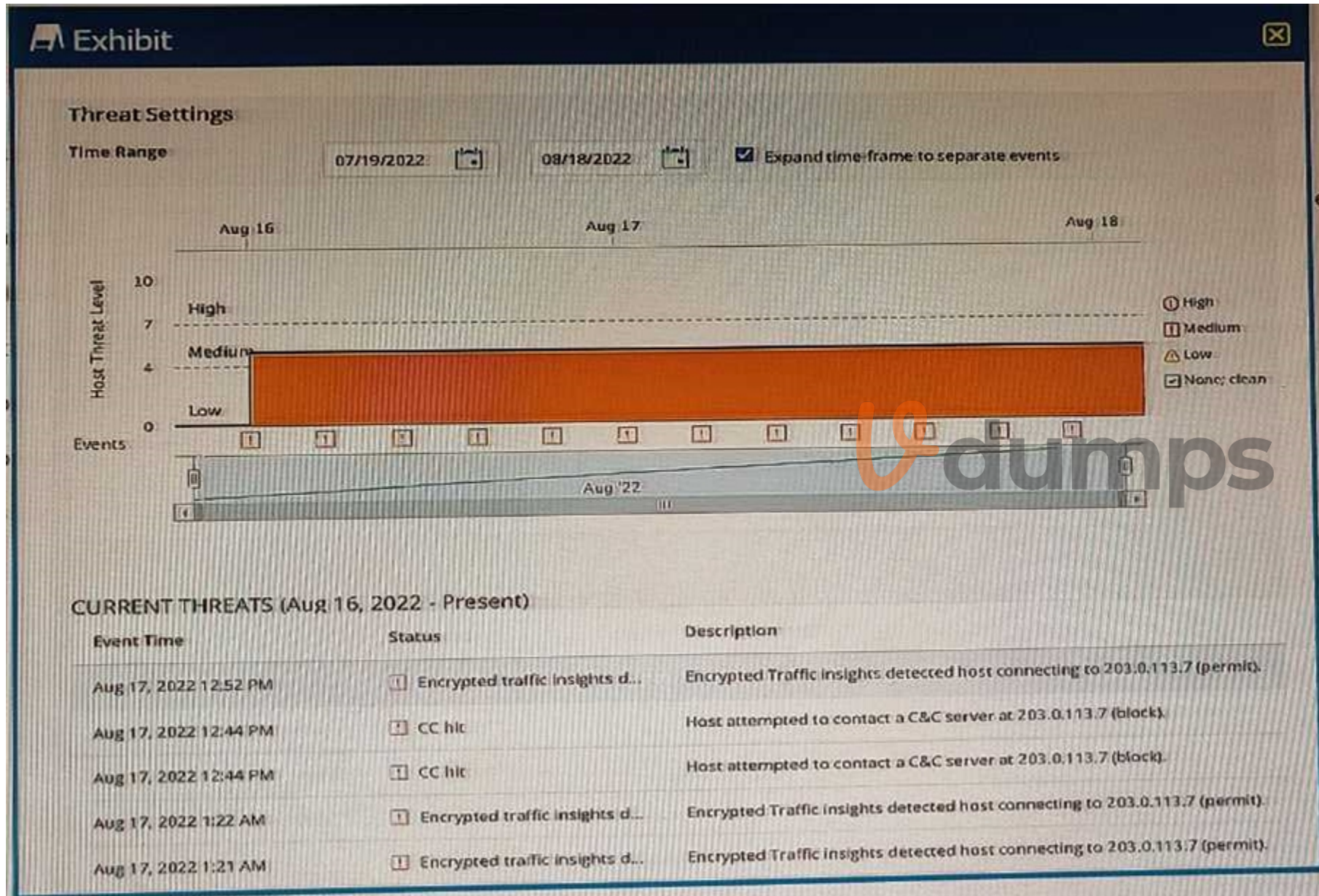
- B. Option B
- C. Option C
- D. Option D

Correct Answer: A, B

Section:

QUESTION 44

Exhibit



You are using ATP Cloud and notice that there is a host with a high number of ETI and C&C hits sourced from the same investigation and notice that some of the events have not been automatically mitigated. Referring to the exhibit, what is a reason for this behavior?

- A. The C&C events are false positives.
- B. The infected host score is globally set below a threat level of 5.
- C. The infected host score is globally set above a threat level of 5.
- D. The ETI events are false positives.

Correct Answer: C

Section:

Explanation:

According to the Juniper documentation, the infected host score is a global setting that determines the minimum threat level required for a host to be considered infected and blocked by Juniper ATP Cloud. The infected host score can be configured from 1 to 10, where 1 is the lowest and 10 is the highest. The default infected host score is 5, which means that any host with a threat level of 5 or higher will be automatically blocked by Juniper ATP Cloud. However, the infected host score can be changed to a higher value, such as 6 or 7, to reduce the number of false positives and allow more traffic to pass through. In the exhibit, the host has a threat level of 5, which indicates that it is infected with malware and has attempted to contact command-and-control servers. However, some of the events have not been automatically mitigated, which means that the host has not been blocked by Juniper ATP Cloud. A possible reason for this behavior is that the infected host score is globally set above a threat level of 5, such as 6 or 7, which means that the host does not meet the minimum threshold for blocking. Therefore, the correct answer is C. The infected host score is globally set above a threat level of 5. Reference: [Configuring the Infected Host Score] 1, [Compromised Hosts: More Information] 2

1: <https://www.juniper.net/documentation/us/en/software/sky-atp/atp-cloud-userguide/topics/task/sky-atp-infected-host-score.html>

2: <https://www.juniper.net/documentation/us/en/software/sky-atp/atp-cloud-userguide/topics/concept/sky-atp-infected-host-overview.html>

QUESTION 45

Which two features would be used for DNS doctoring on an SRX Series firewall? (Choose two.)

- A. The DNS ALG must be enabled.
- B. static NAT
- C. The DNS ALG must be disabled.
- D. source NAT

Correct Answer: A, B

Section:

Explanation:

DNS doctoring is a feature that allows the SRX Series firewall to modify the IP address in a DNS response based on a static NAT rule. This can be useful when the DNS server returns an IP address that is not reachable by the client, such as a private IP address or an IP address from a different network. To use DNS doctoring, the following requirements must be met:

The DNS ALG must be enabled. The DNS ALG is responsible for parsing the DNS messages and performing the IP address translation. The DNS ALG can be enabled globally or per security policy. To enable the DNS ALG globally, use the command `set security alg dns enable`. To enable the DNS ALG per security policy, use the command `set security policies from-zone zone1 to-zone zone2 policy policy1 then permit application-services application-firewall rule-set rule-set-name application junos-dns`.

Static NAT must be configured for the IP address that needs to be translated. Static NAT is a type of NAT that maps a fixed IP address to another fixed IP address. Static NAT can be configured using the command `set security nat static rule-set rule-set-name rule rule-name match destination-address address and set security nat static rule-set rule-set-name rule rule-name then static-nat prefix prefix`. Reference:

DNS ALG and Doctoring Support

Understanding DNS ALG and NAT Doctoring

Disabling DNS ALG and NAT Doctoring

SRX Getting Started - Configure DNS

QUESTION 46

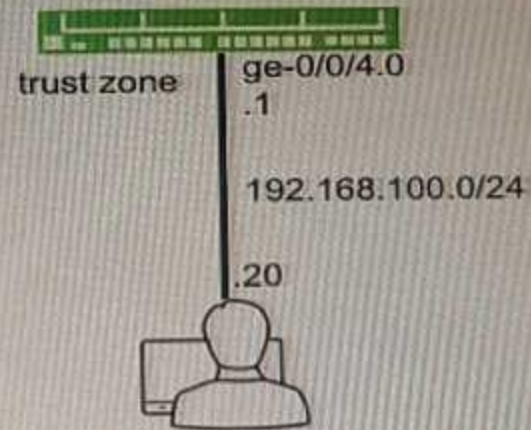
Exhibit


```

[edit]
user@SRX# show interfaces ge-0/0/4
unit 0 {
  family inet {
    address 192.168.100.1/32;
  }
}

[edit security zones]
user@SRX# show security-zone trust
host-inbound-traffic {
  system-services {
    netconf;
  }
}
interfaces {
  ge-0/0/4.0 {
    host-inbound-traffic {
      system-services {
        ssh;
      }
    }
  }
}

```



You are not able to ping the default gateway of 192.168.100.1 (or your network that is located on your SRX Series firewall). Referring to the exhibit, which two commands would correct the configuration of your SRX Series device? (Choose two.)

A)

```
[edit security zones security-zone trust]
user@SRX# set interfaces ge-0/0/4.0 host-inbound-traffic system-services ping
```

B)

```
[edit interfaces ge-0/0/4]
user@SRX# replace pattern 32 with 24
```

C)

```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping
```

D)

```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping except
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: A, B

Section:

QUESTION 47

You configured a chassis cluster for high availability on an SRX Series device and enrolled this HA cluster with the Juniper ATP Cloud. Which two statements are correct in this scenario? (Choose two.)

- A. You must use different license keys on both cluster nodes.
- B. When enrolling your devices, you only need to enroll one node.
- C. You must set up your HA cluster after enrolling your devices with Juniper ATP Cloud
- D. You must use the same license key on both cluster nodes.

Correct Answer: B, D

Section:

Explanation:

When enrolling your devices, you only need to enroll one node: The Juniper ATP Cloud automatically recognizes the HA configuration and applies the same license and configuration to both nodes of the cluster.

You must use the same license key on both cluster nodes: The HA cluster needs to share the same license key in order to be recognized as a single device by the Juniper ATP Cloud.

You must set up your HA cluster before enrolling your devices with Juniper ATP Cloud. And it is not necessary to use different license keys on both cluster nodes because the HA cluster shares the same license key.

The two statements that are correct in this scenario are:

When enrolling your devices, you only need to enroll one node. This is because the Juniper ATP Cloud service supports chassis cluster mode for SRX Series devices. When you enroll a chassis cluster, you only need to enroll the primary node of the cluster. The secondary node will be automatically enrolled and synchronized with the primary node. You do not need to enroll the secondary node separately or perform any additional configuration on it.

You must use the same license key on both cluster nodes. This is because the Juniper ATP Cloud service requires a license key to activate the service on the SRX Series devices. The license key is tied to the serial number of the device. When you enroll a chassis cluster, you must use the same license key on both nodes of the cluster. The license key must match the serial number of the primary node of the cluster. You cannot use different license keys on the cluster nodes.

Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-atp-cloudenrolling-srx-series.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-atp-cloud-licensingoverview.html

QUESTION 48

Exhibit

```

[edit]
user@srx# show interfaces ge-0/0/1
unit 0 {
  family inet {
    filter {
      input my-filter;
    }
    address 172.25.0.1/24;
    address 172.25.1.1/24;
  }
}
[edit]
user@srx# show routing-instances
ISP-1 {
  instance-type forwarding;
  routing-options {
    static {
      route 0.0.0.0/0 next-hop 172.20.0.2;
    }
  }
}
[edit]
user@srx# show routing-options
static {
  route 0.0.0.0/0 next-hop 172.21.0.2;
}
interface-routes {
  rib-group inet my-rib-group;
}
rib-groups {
  my-rib-group {
    import-rib [ inet.0 ISP-1.inet.0 ];
  }
}

```

Vdumps

You are implementing filter-based forwarding to send traffic from the 172.25.0.0/24 network through ISP-1 while sending all other traffic through your connection to ISP-2. Your ge-0/0/1 interface connects to two networks, including the 172.25.0.0/24 network. You have implemented the configuration shown in the exhibit. The traffic from the 172.25.0.0/24 network is being forwarded as expected to 172.20.0.2, however traffic from the other network (172.25.1.0/24) is not being forwarded to the upstream 172.21.0.2 neighbor. In this scenario, which action will solve this problem?

- A. You must specify that the 172.25.1.1/24 IP address is the primary address on the ge-0/0/1 interface.
- B. You must apply the firewall filter to the lo0 interface when using filter-based forwarding.
- C. You must add another term to the firewall filter to accept the traffic from the 172.25.1.0/24 network.
- D. You must create the static default route to neighbor 172.21 0.2 under the ISP-1 routing instance hierarchy.

Correct Answer: C

Section:

Explanation:

The exhibit shows the configuration of filter-based forwarding on an SRX Series device. Filter-based forwarding is a feature that allows the device to use firewall filters to direct traffic to different routing instances based on the match criteria. In this scenario, the device has two routing instances - ISP-1 and ISP-2 - and two firewall filters - FBF and FBF-ISP-1. The FBF filter is applied to the ge-0/0/1 interface as an input filter. The FBF filter has one term that matches the traffic from the 172.25.0.0/24 network and directs it to the ISP-1 routing instance. The ISP-1 routing instance has a static route to the next hop 172.20.0.2. The FBF-ISP-1 filter is applied to the ge-0/0/0 interface as an output filter. The FBF-ISP-1 filter has one term that matches the traffic to the 172.20.0.2 next hop and sets the forwarding class to expedited-forwarding.

The problem in this scenario is that the traffic from the other network (172.25.1.0/24) is not being forwarded to the upstream 172.21.0.2 neighbor. This is because the FBF filter does not have a term that accepts the traffic from the 172.25.1.0/24 network. The FBF filter only has one term that matches the traffic from the 172.25.0.0/24 network and directs it to the ISP-1 routing instance. The traffic from the 172.25.1.0/24 network does not match this term and is therefore discarded by the implicit deny action at the end of the filter. The traffic from the 172.25.1.0/24 network should be forwarded to the ISP-2 routing instance, which has a static default route to the next hop 172.21.0.2.

To solve this problem, you must add another term to the FBF filter to accept the traffic from the 172.25.1.0/24 network. This term should have the action accept, which means that the traffic will be forwarded according to the routing table of the master routing instance. The master routing instance has a static default route to the ISP-2 routing instance, which in turn has a static default route to the next hop 172.21.0.2. By adding this term, the traffic from the 172.25.1.0/24 network will be forwarded to the upstream 172.21.0.2 neighbor as expected.

The configuration of the new term in the FBF filter could look something like this:

```
[edit firewall family inet filter FBF] term 2 { from { source-address { 172.25.1.0/24; } } then { accept; } }
```

Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-option-filterbased-forwarding-overview.html

https://www.juniper.net/documentation/en_US/junos/topics/example/filter-based-forwardingexample.html

QUESTION 49

Exhibit

```
user@srx> show security flow session family inet6
Flow Sessions on FPC10 PIC1:
Session ID: 410000066, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/3 > 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8:5::2/323;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
Session ID: 410000068, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/4 --> 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8::6:2/4;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
Total sessions: 2
```

Which statement is true about the output shown in the exhibit?

- A. The SRX Series device is configured with default security forwarding options.
- B. The SRX Series device is configured with packet-based IPv6 forwarding options.
- C. The SRX Series device is configured with flow-based IPv6 forwarding options.
- D. The SRX Series device is configured to disable IPv6 packet forwarding.

Correct Answer: C

Section:

Explanation:

The output shown in the exhibit is from the command "show security flow session family inet6". This command displays the IPv6 flow sessions on the SRX Series device. The output shows that there are two total sessions, both of which are valid. This means that the SRX Series device is configured with flow-based IPv6 forwarding options. Flow-based IPv6 forwarding options enable the device to process IPv6 packets using the security policies, NAT, and other security features. To configure flowbased IPv6 forwarding options, use the command set security forwarding-options family inet6 mode flow-based and reboot the device. Reference:

show security flow session family inet6

Configuring Flow-Based IPv6 Forwarding Options

QUESTION 50

You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents. Which security feature achieves this objective?

- A. infected host feeds
- B. encrypted traffic insights
- C. DNS security
- D. Secure Web Proxy

Correct Answer: B

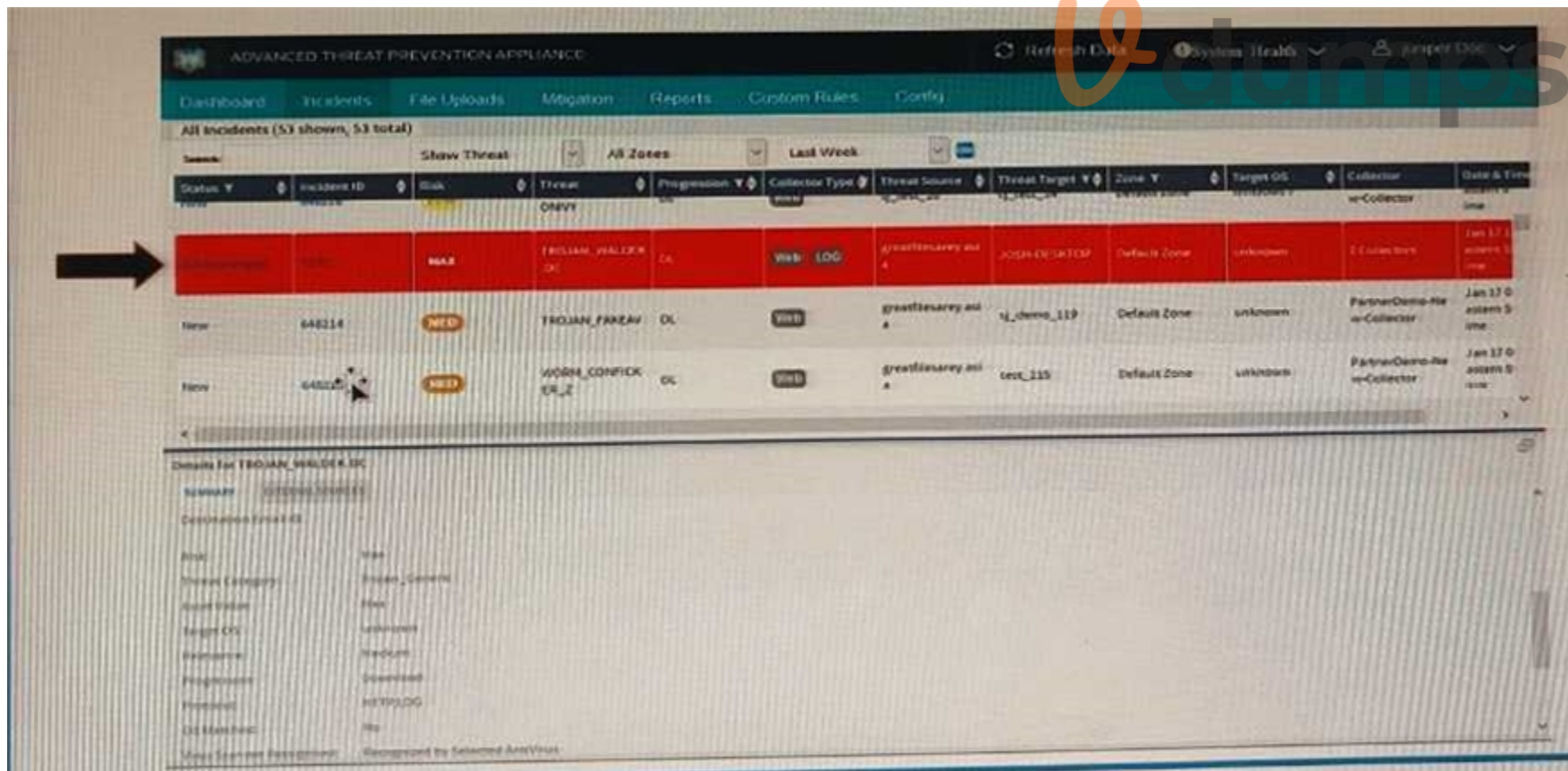
Section:

Explanation:

The security feature that achieves the objective of identifying potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents is encrypted traffic insights. Encrypted traffic insights (ETI) is a feature of Juniper ATP Cloud that helps you to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic. ETI uses machine learning and behavioral analysis to identify anomalies and suspicious patterns in the encrypted traffic metadata, such as the SSL/TLS handshake, the certificate, the cipher suite, and the session duration. ETI can also leverage third-party feeds and threat intelligence from Juniper ATP Cloud to correlate the encrypted traffic with known indicators of compromise (IoCs). ETI can provide insights into the risk level, the threat category, the threat location, and the threat time of the encrypted traffic. ETI can also trigger mitigation actions, such as blocking, quarantining, or alerting, based on the threat severity and the policy configuration. ETI can help you to improve your security posture and visibility without compromising the privacy and performance of the encrypted traffic. Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents: https://www.juniper.net/documentation/en_US/junos/topics/concept/security-atpcloud-encrypted-traffic-insights-overview.html

QUESTION 51

Exhibit



- A. The highlighted incident (arrow) shown in the exhibit shows a progression level of "Download" in the kill chain. What are two appropriate mitigation actions for the selected incident? (Choose two.)
- B. Immediate response required: Block malware IP addresses (download server or CnC server)

- C. Immediate response required: Wipe infected endpoint hosts.
- D. Immediate response required: Deploy IVP integration (if configured) to confirm if the endpoint has executed the malware and is infected.
- E. Not an urgent action: Use IVP to confirm if machine is infected.

Correct Answer: A, C

Section:

Explanation:

The appropriate mitigation actions for the selected incident are to block malware IP addresses (download server or CnC server) and to deploy IVP integration (if configured) to confirm if the endpoint has executed the malware and is infected. This is because the incident shows a progression level of "Download" in the kill chain, which means that the malware has been downloaded and is likely to be executed. Blocking the malware IP addresses can prevent further communication with the malicious server and stop the malware from receiving commands or exfiltrating data. Deploying IVP integration can help verify the infection status of the endpoint and provide additional information about the malware behavior and impact. IVP integration is an optional feature that allows the ATP Appliance to interact with third-party endpoint security solutions such as Carbon Black, Cylance, and CrowdStrike. Reference:

Advanced Threat Prevention Appliance Solution Brief

Advanced Threat Prevention Appliance Datasheet

[Advanced Threat Prevention Appliance Mitigation Actions]

[Advanced Threat Prevention Appliance IVP Integration]

QUESTION 52

Exhibit

```
user@srx> show interfaces ge-0/0/5.0 extensive | find security
Security : Zone: dmz
Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp mdp nh
ospf3 pgn pim rip ripng router- discovery rsvp sap vrrp dhcp finger
```

Referring to the exhibit, which three protocols will be allowed on the ge-0/0/5.0 interface? (Choose three.)

- A. IBGP
- B. OSPF
- C. IPsec
- D. DHCP
- E. NTP

Correct Answer: B, D, E

Section:

Explanation:

The exhibit shows the output of the "show interfaces ge-0/0/5.0 extensive" command on an SRX

Series device. The output includes a section called "Security" that lists the protocols that are allowed on the ge-0/0/5.0 interface. The protocols that are allowed on the ge-0/0/5.0 interface are:

OSPF

DHCP

NTP

It's important to notice that the output don't have IBGP, IPsec, so these protocols are not allowed on the ge-0/0/5.0 interface.

QUESTION 53

Exhibit


```
user@router> show security flow session
Session ID: 36, Policy name: pre-id-default-policy/n, Timeout: 2, Valid
  In: 10.10.10.2/61606 --> 203.0.113.100/179;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 1, Bytes: 64,
  Out: 203.0.113.100/179 --> 203.0.113.1/61606;tcp, Conn Tag: 0x0, If:
.local..0, Pkts: 1, Bytes: 40,
```

Referring to the exhibit, which type of NAT is being performed?

- A. Static NAT
- B. Destination NAT
- C. Persistent NAT
- D. Source NAT

Correct Answer: D

Section:

Explanation:

Source NAT is a type of NAT that is used to translate the source IP address and port number of a packet. This is typically used to allow multiple devices on a private network to access the internet using a single public IP address. In the exhibit, we can see that the source IP address and port number of the packet are being translated from 10.10.10.2/61606 to 203.0.113.100/179. This is a clear indication that Source NAT is being performed.

Reference:

Network Address Translation Feature Guide SRX NAT with Illustrated Examples



QUESTION 54

Regarding IPsec CoS-based VPNs, what is the number of IPsec SAs associated with a peer based upon?

- A. The number of traffic selectors configured for the VPN.
- B. The number of CoS queues configured for the VPN.
- C. The number of classifiers configured for the VPN.
- D. The number of forwarding classes configured for the VPN.

Correct Answer: D

Section:

Explanation:

In IPsec CoS-based VPNs, the number of IPsec Security Associations (SAs) associated with a peer is based on the number of forwarding classes configured for the VPN. The forwarding classes are used to classify and prioritize different types of traffic, such as voice and data traffic. Each forwarding class requires a separate IPsec SA to be established between the peers, in order to provide the appropriate level of security and quality of service for each type of traffic.

QUESTION 55

Which method does an SRX Series device in transparent mode use to learn about unknown devices in a network?

- A. LLDP-MED
- B. IGMP snooping
- C. RSTP
- D. packet flooding

Correct Answer: D

Section:

Explanation:

The SRX Series device in transparent mode uses packet flooding to learn about unknown devices in a network. Packet flooding is a process wherein the device sends out packets to every device it knows about or suspects in the network. When the packets are returned, the device can identify and classify the unknown devices in the network.

QUESTION 56

Your Source NAT implementation uses an address pool that contains multiple IPv4 addresses Your users report that when they establish more than one session with an external application, they are prompted to authenticate multiple times External hosts must not be able to establish sessions with internal network hosts What will solve this problem?

- A. Disable PAT.
- B. Enable destination NAT.
- C. Enable persistent NAT
- D. Enable address persistence.

Correct Answer: D

Section:

Explanation:

The solution to this problem is to enable address persistence. This will ensure that the same external IP address is used for multiple sessions between an internal host and an external host. This will result in only one authentication being required, as the same external IP address will be used for all sessions.

QUESTION 57

While troubleshooting security policies, you added the count action. Where do you see the result of this action?

- A. In the show security policies hit-count command output.
- B. In the show security flow statistics command output.
- C. In the show security policies detail command output.
- D. In the show firewall log command output.

Correct Answer: C

Section:

Explanation:

The result of adding the count action to a security policy can be seen in the show security policies detail command output. The count action is a feature that allows you to enable statistics collection for sessions that enter the device for a given policy, and for the number of packets and bytes that pass through the device in both directions for a given policy. The count action can help you to monitor the traffic that matches a security policy and to troubleshoot security policy issues. The show security policies detail command displays the detailed information about the security policies configured on the device, including the count statistics. The output shows the number of packets and bytes that have been processed by the policy in both directions, as well as the number of sessions that have been created by the policy. You can use this command to verify that the count action is working as expected and to see the traffic volume and session count for each policy. Reference:

Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/showsecurity-policies-detail.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-policy-countoverview.html

QUESTION 58

Exhibit



```
[edit security policies from-zone trust to-zone untrust policy Adaptive-Threat-
Profiling]
user@SRX-1# show
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application [ junos:web:proxy junos:web:anonymizer ];
}
then {
    reject {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    Suspicious_Endpoints;
                }
            }
        }
    }
}
...

```

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

- A. The suspicious_Endpoints feed is only usable by the SRX-1 device.
- B. You must manually create the suspicious_Endpoints feed in the Juniper ATP Cloud interface.
- C. The suspicious_Endpoints feed is usable by any SRX Series device that is a part of the same realm as SRX-1.
- D. Juniper ATP Cloud automatically creates the suspicious_Endpoints feed after you commit the security policy.

Correct Answer: C, D

Section:

Explanation:

The suspicious_Endpoints feed is a dynamic address group that is created by Juniper ATP Cloud based on the IoT device discovery and policy enforcement feature. This feature allows the SRX Series device to send IoT traffic to Juniper ATP Cloud for analysis and classification. Juniper ATP Cloud then creates a threat feed that contains the IP addresses of the suspicious IoT devices and sends it back to the SRX Series device. The SRX Series device can then use this feed to create and enforce security policies for the IoT traffic. The suspicious_Endpoints feed is usable by any SRX Series device that is a part of the same realm as SRX-1, because the feed is shared among the devices that belong to the same Juniper ATP Cloud realm. Juniper ATP Cloud automatically creates the suspicious_Endpoints feed after you commit the security policy that references the feed, because the feed is dynamically generated based on the IoT traffic analysis. You do not need to manually create the feed in the Juniper ATP Cloud interface. Reference:

Example- Configure IoT Device Discovery and Policy Enforcement

Juniper Advanced Threat Prevention Cloud Policy Overview

QUESTION 59

You want to configure a threat prevention policy.

Which three profiles are configurable in this scenario? (Choose three.)

- A. device profile
- B. SSL proxy profile
- C. infected host profile
- D. C&C profile
- E. malware profile

Correct Answer: C, D, E

Section:

Explanation:

The three profiles that are configurable in a threat prevention policy are infected host profile, C&C profile, and malware profile. A threat prevention policy is a feature of Juniper ATP Cloud that provides protection and monitoring for selected threat profiles, including command and control servers, infected hosts, and malware. Using feeds from Juniper ATP Cloud and optional custom feeds that you configure, ingress and egress traffic is monitored for suspicious content and behavior. Based on a threat score, detected threats are evaluated and action may be taken once a verdict is reached.

You can create a threat prevention policy by selecting one or more of the following profiles:

Infected host profile: This profile detects and blocks traffic from hosts that are infected with malware or compromised by attackers. You can configure the threat score thresholds and the actions for different levels of severity. You can also enable Geo IP filtering to block traffic from or to specific countries or regions.

C&C profile: This profile detects and blocks traffic to or from command and control servers that are used by attackers to control malware or botnets. You can configure the threat score thresholds and the actions for different levels of severity. You can also enable Geo IP filtering to block traffic from or to specific countries or regions.

Malware profile: This profile detects and blocks traffic that contains malware or malicious content.

You can configure the threat score thresholds and the actions for different levels of severity. You can also enable protocol-specific settings for HTTP and SMTP traffic, such as file type filtering, file size filtering, and file name filtering.

The other two profiles, device profile and SSL proxy profile, are not configurable in a threat prevention policy. A device profile is a feature of Policy Enforcer that defines the device type, the device group, and the device settings for the SRX Series devices that are enrolled with Juniper ATP Cloud. An SSL proxy profile is a feature of SRX Series devices that enables SSL proxy to decrypt and inspect SSL/TLS traffic for threats and policy violations.

Reference: Juniper Security, Professional (JNCIP-SEC) Reference Materials source and documents:

https://www.juniper.net/documentation/en_US/junos-space23.1/policyenforcer/topics/concept/threat-management-policy-overview.html

https://www.juniper.net/documentation/en_US/junos-space23.1/policyenforcer/topics/task/configuration/junos-space-policy-enforcer-threat-management-policyconfigure.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/securitypolicy-enforcer-device-profile-overview.html

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-ssl-proxyoverview.html

QUESTION 60

You are asked to download and install the IPS signature database to a device operating in chassis cluster mode. Which statement is correct in this scenario?

- A. You must download and install the IPS signature package on the primary node.
- B. The first synchronization of the backup node and the primary node must be performed manually.
- C. The first time you synchronize the IPS signature package from the primary node to the backup node, the primary node must be rebooted.
- D. The IPS signature package must be downloaded and installed on the primary and backup nodes.

Correct Answer: A

Section:

Explanation:

The IPS signature database is one of the major components of the intrusion prevention system (IPS).

It contains definitions of different objects, such as attack objects, application signature objects, and service objects, that are used in defining IDP policy rules. As a response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper Networks website. You can download this file to protect your network from new threats. Note: IPS does not need a separate license to run as a service on the SRX Series Firewall; however, a license is required for IPS updates¹.

When you configure a chassis cluster, the two nodes back up each other, with one node acting as the primary device and the other as the secondary device, ensuring stateful failover of processes and services in the event of system or hardware failure. If the primary device fails, the secondary device takes over processing of traffic².

To download and install the IPS signature database to a device operating in chassis cluster mode, you must perform the following steps:

Download the IPS signature package from the Juniper Networks website to the primary node of the chassis cluster. You can use the request security idp security-package download CLI command or the Security Director user interface to download the package. Note: You must have a valid license key installed on the device to download the package³.

Install the IPS signature package on the primary node of the chassis cluster. You can use the request security idp security-package install CLI command or the Security Director user interface to install the package. Note: You must reboot the primary node after installing the package³.

Synchronize the IPS signature package from the primary node to the backup node of the chassis cluster. You can use the request security idp security-package install-backup CLI command or the Security Director user interface to synchronize the package. Note: You do not need to reboot the backup node after synchronizing the package³.

Therefore, the correct answer is A. You must download and install the IPS signature package on the primary node. The other options are incorrect because:

B) The first synchronization of the backup node and the primary node is performed automatically after you install the package on the primary node. You do not need to perform it manually³.

C) The first time you synchronize the IPS signature package from the primary node to the backup node, the primary node does not need to be rebooted. You only need to reboot the primary node after installing the package³.

D) The IPS signature package does not need to be downloaded and installed on the primary and backup nodes separately. You only need to download and install it on the primary node and then synchronize it to the backup node³.

Reference:

IDP Signature Database Overview

Understanding IDP Signature Database for Migration

Configuring Chassis Clustering on SRX Series Devices

QUESTION 61

Click the Exhibit button.

```
Communicate with JATP server...
error: [Error] Failed to communicate with JATP server when retrieving
registration status.
Please make sure you are able to connect to JATP server. If this issue still
remains, please contact JTAC for help.
```

When attempting to enroll an SRX Series device to JATP, you receive the error shown in the exhibit.

What is the cause of the error?

- A. The fxp0 IP address is not routable
- B. The SRX Series device certificate does not match the JATP certificate
- C. The SRX Series device does not have an IP address assigned to the interface that accesses JATP
- D. A firewall is blocking HTTPS on fxp0

Correct Answer: C

Section:

Explanation:

Reference: https://kb.juniper.net/InfoCenter/index?page=content&id=KB33979&cat=JATP_SERIES&actp=LIST



QUESTION 62

You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restricted to the VLANs from which they originate.

Which configuration accomplishes these objectives?

A)

```
bridge {
block-non-ip-all;
bypass-non-ip-unicast;
no-packet-flooding;
}
```

B)

```
bridge {
block-non-ip-all;
bypass-non-ip-unicast;
bpdu-vlan-flooding;
}
```

C)
bridge {
bypass-non-ip-unicast;
bpdu-vlan-flooding;
}

D)
bridge {
block-non-ip-all;
bpdu-vlan-flooding;
}

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: D

Section:

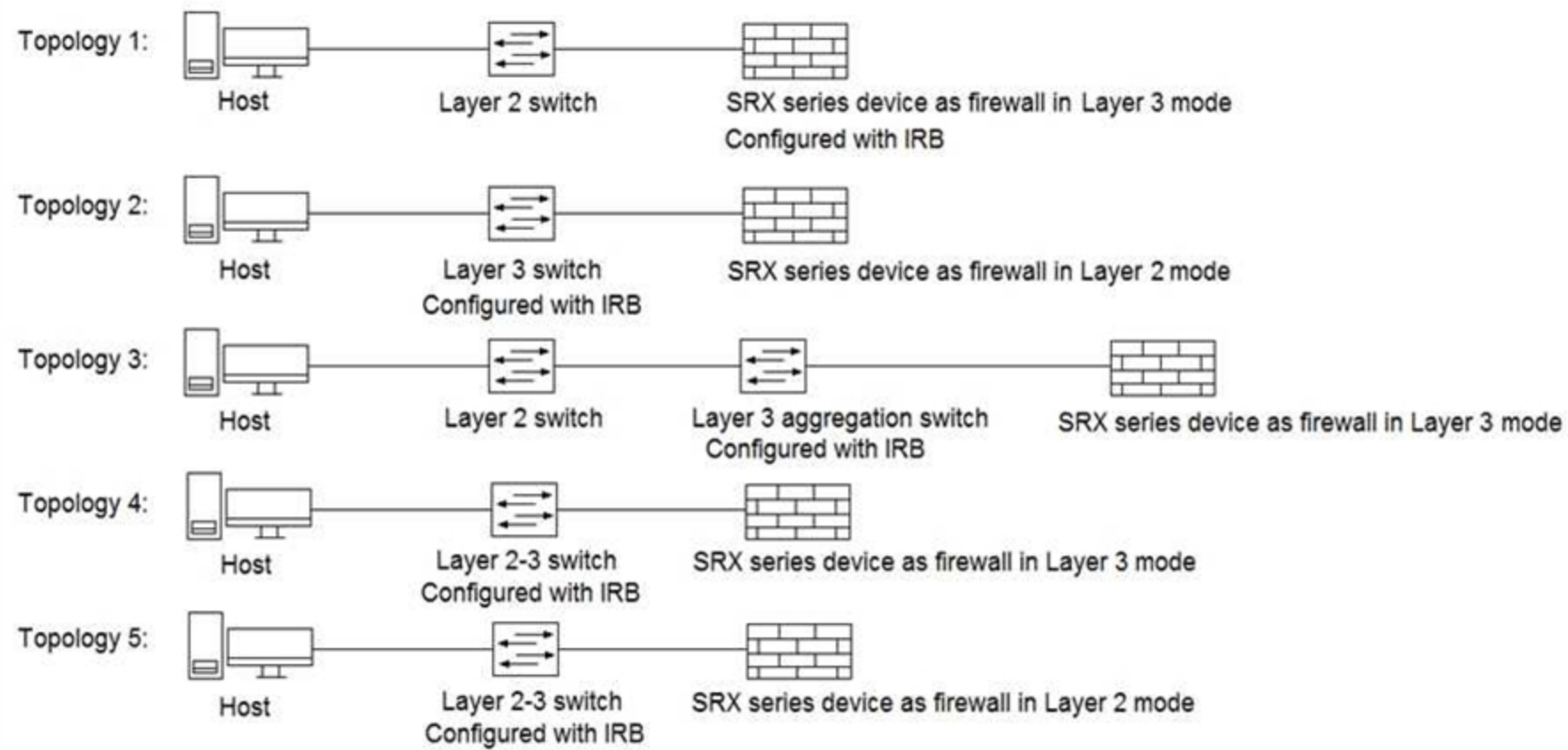
Explanation:

https://www.juniper.net/documentation/us/en/software/junos/multicastl2/topics/ref/statement/family-ethernet-switching-edit-interfaces-qfx-series.html#statement-namestatement_d26608e73

QUESTION 63

Refer to the Exhibit.

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase, sans-serif font.



Referring to the exhibit, which three topologies are supported by Policy Enforcer? (Choose three.)

- A. Topology 3
- B. Topology 5
- C. Topology 2
- D. Topology 4
- E. Topology 1

Correct Answer: A, D, E

Section:

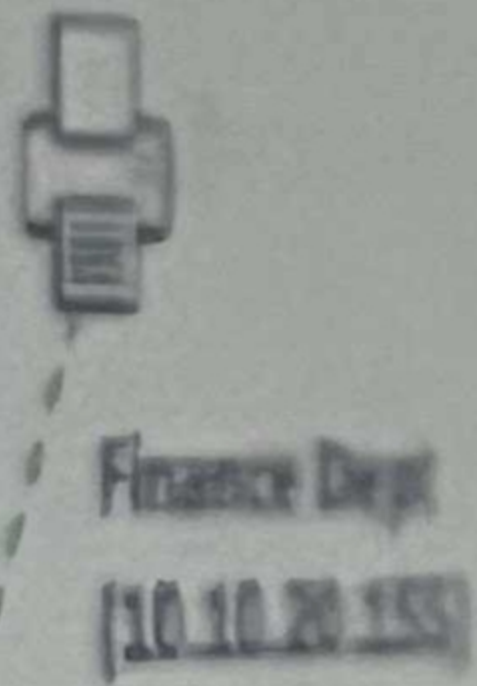
Explanation:

Reference: https://www.juniper.net/documentation/en_US/junos-space17.2/policyenforcer/topics/concept/policy-enforcer-deployment-supported-topologies.html

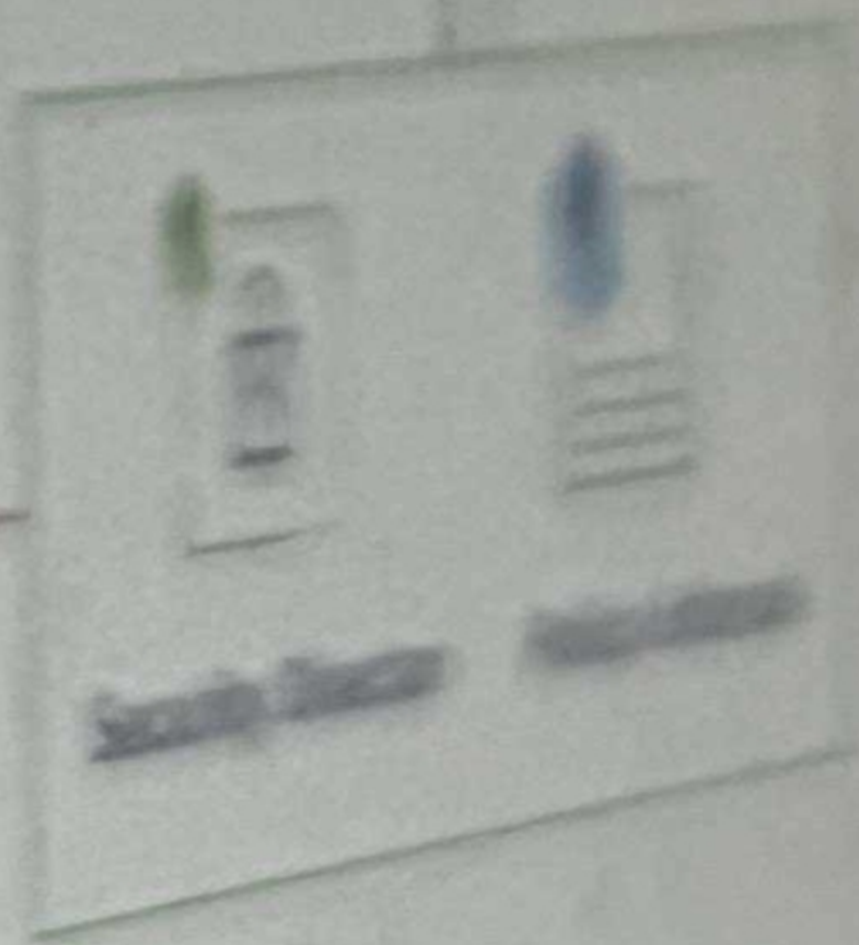
QUESTION 64

Exhibit:





Vdumps



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)

- 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`.

Correct Answer: A, B, C

Section:

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.

Reference:

Configuring the Server Feed URL Dynamic Address Overview Creating Custom Feeds [Command and Control Feed Overview]

QUESTION 65

Refer to the Exhibit:


```
[edit security ike]
user@router1# show
policy ike-policy1 {
  mode aggressive;
  proposal-set standard;
  pre-shared-key ascii-text *****;
}
gateway gate-1 {
  ike-policy ike-policy1;
  address 203.0.113.100;
  local-identity hostname;
  external-identity hostname;
```



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

- 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.

Correct Answer: A, D

Section:

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-usertype, 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.

Reference:
gateway (Security IKE) dynamic (Security IKE)

QUESTION 66

You are asked to control access to network resources based on the identity of an authenticated device. Which three steps will accomplish this goal on the SRX Series firewalls? (Choose three.)

- A. Configure an end-user-profile that characterizes a device or set of devices
- B. Reference the end-user-profile in the security zone
- C. Reference the end-user-profile in the security policy.
- D. Apply the end-user-profile at the interface connecting the devices
- E. Configure the authentication source to be used to authenticate the device

Correct Answer: A, C, E

Section:

Explanation:

To control access to network resources based on the identity of an authenticated device on the SRX Series firewalls, you need to perform the following steps:

A) Configure an end-user-profile that characterizes a device or set of devices. An end-user-profile is a device identity profile that contains a collection of attributes that are characteristics of a specific group of devices, or of a specific device, depending on the attributes configured in the profile. The end-user-profile must contain a domain name and at least one value in each attribute. The attributes include device-identity, device-category, device-vendor, device-type, device-os, and device-osversion¹.

You can configure an end-user-profile by using the Junos Space Security Director or the CLI².

C) Reference the end-user-profile in the security policy. 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 can reference the end-user-profile in the source-end-user-profile field of the security policy to identify the traffic source based on the device from which the traffic issued. The SRX Series device matches the IP address of the device to the enduser-profile and applies the security policy accordingly³. You can reference the end-user-profile in the security policy by using the Junos Space Security Director or the CLI⁴.

E) Configure the authentication source to be used to authenticate the device. An authentication source is a system that provides the device identity information to the SRX Series device. The authentication source can be Microsoft Windows Active Directory or a third-party network access control (NAC) system. You need to configure the authentication source to be used to authenticate the device and to send the device identity information to the SRX Series device. The SRX Series device stores the device identity information in the device identity authentication table⁵. You can configure the authentication source by using the Junos Space Security Director or the CLI⁶.

The other options are incorrect because:

B) Referencing the end-user-profile in the security zone is not a valid step to control access to network resources based on the identity of an authenticated device. A security zone is a logical grouping of interfaces that have similar security requirements. You can reference the user role in the security zone to identify the user who is accessing the network resources, but not the end-userprofile⁷.

D) Applying the end-user-profile at the interface connecting the devices is also not a valid step to control access to network resources based on the identity of an authenticated device. You cannot apply the end-user-profile at the interface level, but only at the security policy level. The end-userprofile is not a firewall filter or a security policy, but a device identity profile that is referenced in the security policy¹.

Reference:

End User Profile Overview

Creating an End User Profile

source-end-user-profile

Creating Firewall Policy Rules

Understanding the Device Identity Authentication Table and Its Entries

Configuring the Authentication Source for Device Identity

user-role

QUESTION 67

Which three type of peer devices are supported for Cos-Based IPsec VPN?

- A. High-end SRX Series device
- B. cSRX
- C. vSRX

D. Branch-end SRX Series devices

Correct Answer: A, C, D

Section:

QUESTION 68

Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 11232, Policy name: Allow-ipv6-Telnet/11, Timeout: 1788, Valid
  In: 2001:db8::1/57707 --> 2001:db8::8/23;tcp, Conn Tag: 0x0, If: vlan.101,
Pkts: 9, Bytes: 799,
  Out: 10.8.8.8/23 --> 10.7.7.5/21868;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 8, Bytes: 589,
Total sessions: 1
```

Which type of NAT is shown in the exhibit?

- A. NAT46
- B. NAT64
- C. persistent NAT
- D. DS-Lite

Correct Answer: B

Section:



QUESTION 69

Which two additional configuration actions are necessary for the third-party feed shown in the exhibit to work properly? (Choose two.)

- A. You must create a dynamic address entry with the IP filter category and the ipfilter_office365 value.
- B. You must create a dynamic address entry with the C&C category and the cc_offic365 value.
- C. You must apply the dynamic address entry in a security policy.
- D. You must apply the dynamic address entry in a security intelligence policy.

Correct Answer: A, C

Section:

QUESTION 70

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

- A. Policy p4
- B. Policy p7
- C. Policy p1
- D. Policy p12

Correct Answer: B

Section:

QUESTION 71

You have designed the firewall filter shown in the exhibit to limit SSH control traffic to yours SRX Series device without affecting other traffic. Which two statements are true in this scenario? (Choose two.)

- A. The filter should be applied as an output filter on the loopback interface.
- B. Applying the filter will achieve the desired result.
- C. Applying the filter will not achieve the desired result.
- D. The filter should be applied as an input filter on the loopback interface.

Correct Answer: C, D

Section:

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-ex-serieevaluation-understanding.html

QUESTION 72

You have noticed a high number of TCP-based attacks directed toward your primary edge device. You are asked to configure the IDP feature on your SRX Series device to block this attack. Which two IDP attack objects would you configure to solve this problem? (Choose two.)

- A. Network
- B. Signature
- C. Protocol anomaly
- D. host

Correct Answer: B, C

Section:

**QUESTION 73**

Which two log format types are supported by the JATP appliance? (Choose two.)

- A. YAML
- B. XML
- C. CSV
- D. YANG

Correct Answer: B, C

Section:

Explanation:

https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/topic-map/jatpcustom-log-ingestion.html

QUESTION 74

Exhibit.

```
user@host# show security idp-policy my-policy rulebase-ips
rule 1 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      no-action;
    }
  }
}
rule 2 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      ignore-connection;
    }
  }
}
rule 3 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      drop-packet;
    }
  }
}
rule 4 {
```



A hub member of an ADVPN is not functioning correctly.
Referring the exhibit, which action should you take to solve the problem?

- A. [edit interfaces]
root@vSRX-1# delete st0.0 multipoint
- B. [edit interfaces]
user@hub-1# delete ipsec vpn advpn-vpn traffic-selector
- C. [edit security]
user@hub-1# set ike gateway advpn-gateway advpn suggester disable
- D. [edit security]
user@hub-1# delete ike gateway advpn-gateway advpn partner

Correct Answer: B

Section:

QUESTION 75

Your organization has multiple Active Directory domain to control user access. You must ensure that security polices are passing traffic based upon the user's access rights.
What would you use to assist your SRX series devices to accomplish this task?

- A. JIMS
- B. Junos Space
- C. JSA
- D. JATP Appliance

Correct Answer: A

Section:

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-authconfigure-jims.html

QUESTION 76

According to the log shown in the exhibit, you notice the IPsec session is not establishing.
What is the reason for this behavior?

- A. Mismatched proxy ID
- B. Mismatched peer ID
- C. Mismatched preshared key
- D. Incorrect peer address.

Correct Answer: B

Section:

Explanation:

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/example/policybased-vpn-using-j-series-srxseries-device-configuring.html

QUESTION 77

You must implement an IPsec VPN on an SRX Series device using PKI certificates for authentication.
As part of the implementation, you are required to ensure that the certificate submission, renewal, and retrieval processes are handled automatically from the certificate authority.
In this scenario, which statement is correct.



- A. You can use CRL to accomplish this behavior.
- B. You can use SCEP to accomplish this behavior.
- C. You can use OCSP to accomplish this behavior.
- D. You can use SPKI to accomplish this behavior.

Correct Answer: B

Section:

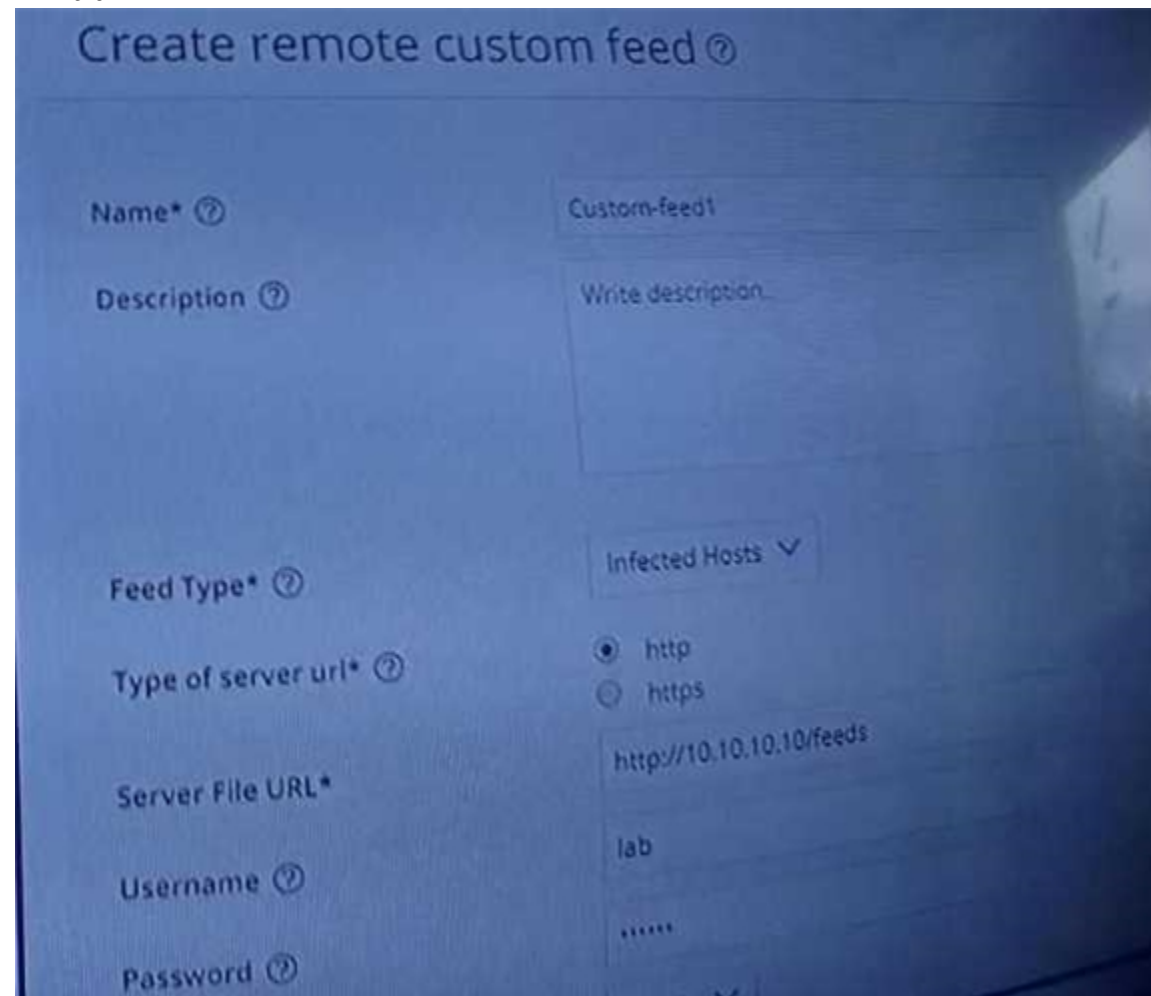
Explanation:

Certificate Renewal

The renewal of certificates is much the same as initial certificate enrollment except you are just replacing an old certificate (about to expire) on the VPN device with a new certificate. As with the initial certificate request, only manual renewal is supported. SCEP can be used to re-enroll local certificates automatically before they expire. Refer to Appendix D for more details.

QUESTION 78

Exhibit.



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

- A. Juniper Networks will not investigate false positives generated by this custom feed.
- B. The custom infected hosts feed will not overwrite the Sky ATP infected host's feed.
- C. The custom infected hosts feed will overwrite the Sky ATP infected host's feed.
- D. Juniper Networks will investigate false positives generated by this custom feed.

Correct Answer: A, C

Section:

Vdumps

Explanation:

https://www.juniper.net/documentation/en_US/junos-space18.1/policyenforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-hostconfigure.html

QUESTION 79

You are asked to configure a security policy on the SRX Series device. After committing the policy, you receive the "Policy is out of sync between RE and PFE <SPU-name(s)>." error. Which command would be used to solve the problem?

- A. request security polices resync
- B. request service-deployment
- C. request security polices check
- D. restart security-intelligence

Correct Answer: A

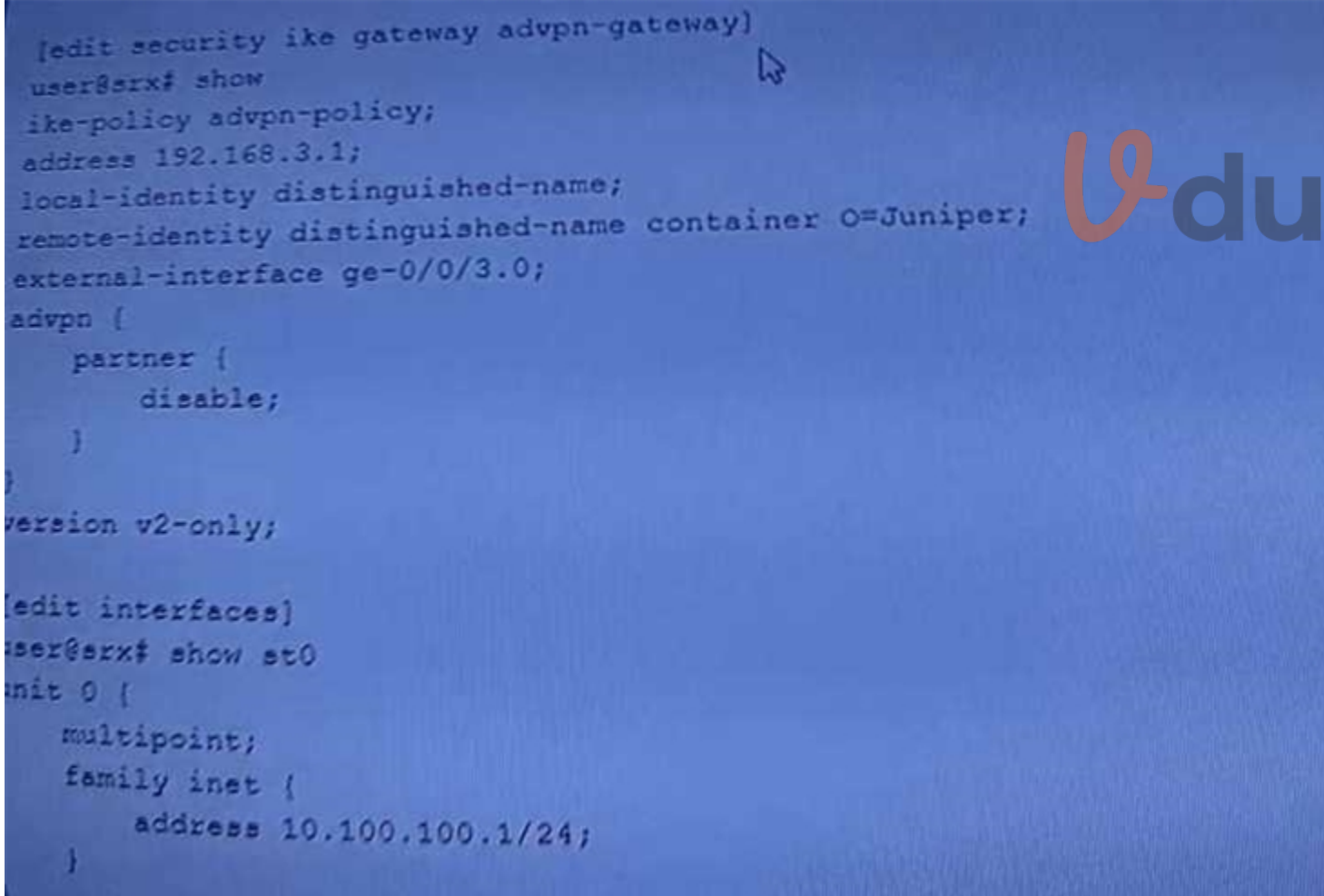
Section:

Explanation:

https://kb.juniper.net/InfoCenter/index?page=content&id=KB30443&cat=SRX_SERIES&actp=LIST

QUESTION 80

Exhibit.



```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
advpn {
  partner {
    disable;
  }
}
version v2-only;

[edit interfaces]
user@srx# show st0
unit 0 {
  multipoint;
  family inet {
    address 10.100.100.1/24;
  }
}
```

Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly.

Which two commands will solve this problem? (Choose two.)

- A. [edit interfaces]
user@srx# delete st0.0 multipoint

- B. [edit security ike gateway advpn-gateway]
user@srx# delete advpn partner
- C. [edit security ike gateway advpn-gateway]
user@srx# set version v1-only
- D. [edit security ike gateway advpn-gateway]
user@srx# set advpn suggerter disable

Correct Answer: B, D

Section:

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discoveryvpns.html

QUESTION 81

You are connecting two remote sites to your corporate headquarters site; you must ensure that all traffic is secured and only uses a single Phase 2 SA for both sites. In this scenario, which VPN should be used?

- A. An IPsec group VPN with the corporate firewall acting as the hub device.
- B. Full mesh IPsec VPNs with tunnels between all sites.
- C. A hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device.
- D. A full mesh Layer 3 VPN with the corporate firewall acting as the hub device.

Correct Answer: A

Section:

Explanation:

<https://www.juniper.net/us/en/local/pdf/app-notes/3500202-en.pdf>



QUESTION 82

You have the NAT rule, shown in the exhibit, applied to allow communication across an IPsec tunnel between your two sites with identical networks. Which statement is correct in this scenario?

- A. The NAT rule will translate the source and destination addresses.
- B. The NAT rule will only translate two addresses at a time.
- C. The NAT rule is applied to the N/A routing instance.
- D. 10 packets have been processed by the NAT rule.

Correct Answer: A

Section:

QUESTION 83

You are asked to share threat intelligence from your environment with third party tools so that those tools can identify and block lateral threat propagation from compromised hosts. Which two steps accomplish this goal? (Choose Two)

- A. Configure application tokens in the SRX Series firewalls to limit who has access
- B. Enable Juniper ATP Cloud to share threat intelligence
- C. Configure application tokens in the Juniper ATP Cloud to limit who has access
- D. Enable SRX Series firewalls to share Threat intelligence with third party tool.

Correct Answer: B, C

Section:**Explanation:**

To share threat intelligence from your environment with third party tools, you need to enable Juniper

ATP Cloud to share threat intelligence and configure application tokens in the Juniper ATP Cloud to limit who has access. The other options are incorrect because:

A) Configuring application tokens in the SRX Series firewalls is not necessary or sufficient to share threat intelligence with third party tools. Application tokens are used to authenticate and authorize requests to the Juniper ATP Cloud API, which can be used to perform various operations such as submitting files, querying C&C feeds, and managing allowlists and blocklists¹. However, to share threat intelligence with third party tools, you need to enable the TAXII service in the Juniper ATP Cloud, which is a different protocol for exchanging threat information².

D) Enabling SRX Series firewalls to share threat intelligence with third party tools is not possible or supported. SRX Series firewalls can send potentially malicious objects and files to the Juniper ATP Cloud for analysis and receive threat intelligence from the Juniper ATP Cloud to block malicious traffic³. However, SRX Series firewalls cannot directly share threat intelligence with third party tools.

You need to use the Juniper ATP Cloud as the intermediary for threat intelligence sharing.

Therefore, the correct answer is B and C. You need to enable Juniper ATP Cloud to share threat intelligence and configure application tokens in the Juniper ATP Cloud to limit who has access. To do so, you need to perform the following steps:

Enable and configure the TAXII service in the Juniper ATP Cloud. TAXII (Trusted Automated eXchange of Indicator Information) is a protocol for communication over HTTPS of threat information between parties. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII. Juniper ATP Cloud can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper ATP Cloud also uses threat information from STIX reports as well as other sources for threat prevention². To enable and configure the TAXII service, you need to select Configure > Threat Intelligence Sharing in the Juniper ATP Cloud WebUI, move the knob to the right to Enable TAXII, and move the sidebar to designate a file sharing threshold².

Configure application tokens in the Juniper ATP Cloud. Application tokens are used to authenticate and authorize requests to the Juniper ATP Cloud API and the TAXII service. You can create and manage application tokens in the Juniper ATP Cloud WebUI by selecting Configure > Application Tokens. You can specify the name, description, expiration date, and permissions of each token. You can also revoke or delete tokens as needed. You can use the application tokens to limit who has access to your shared threat intelligence by granting or denying permissions to the TAXII service¹.

Reference:

Threat Intelligence Open API Setup Guide

Configure Threat Intelligence Sharing

About Juniper Advanced Threat Prevention Cloud

QUESTION 84

You want to enable inter-tenant communication with tenant system.

In this Scenario, Which two solutions will accomplish this task?

- A. interconnect EVPN switch
- B. interconnect VPLS switch
- C. external router
- D. logical tunnel interface

Correct Answer: C, D

Section:**Explanation:**

To enable inter-tenant communication with tenant system, you need to use an external router or a logical tunnel interface. The other options are incorrect because:

A) Interconnecting EVPN switch is not a valid solution for inter-tenant communication with tenant system. EVPN (Ethernet VPN) is a technology that provides layer 2 connectivity over an IP network. It can be used to connect different logical systems on the same device, but not tenant systems. Tenant systems are isolated from each other and do not share the same layer 2 domain¹.

B) Interconnecting VPLS switch is also not a valid solution for inter-tenant communication with tenant system. VPLS (Virtual Private LAN Service) is another technology that provides layer 2 connectivity over an IP network. It can also be used to connect different logical systems on the same device, but not tenant systems. Tenant systems are isolated from each other and do not share the same layer 2 domain¹.

Therefore, the correct answer is C and D. You need to use an external router or a logical tunnel interface to enable inter-tenant communication with tenant system. To do so, you need to perform the following steps:

For external router, you need to connect the external router to the interfaces of the tenant systems that you want to communicate with. You also need to configure the routing protocols and policies on the external router and the tenant systems to exchange routes and traffic. The external router acts as a gateway between the tenant systems and provides layer 3 connectivity².

For logical tunnel interface, you need to create a logical tunnel interface on the device and assign it to a tenant system. You also need to configure the IP address and routing protocols on the logical tunnel interface and the tenant systems that you want to communicate with. The logical tunnel interface acts as a virtual link between the tenant systems and provides layer 3 connectivity³.

Reference:

Tenant Systems Overview

Example: Configuring Inter-Tenant Communication Using External Router



Example: Configuring Inter-Tenant Communication Using Logical Tunnel Interface

QUESTION 85

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)

- A. Layer 2 switching
- B. IPv4 routing
- C. IPsec
- D. IPv6 routing

Correct Answer: A, B

Section:

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.

Reference:

Selective Stateless Packet-Based Services Overview

IPsec VPN Overview

IPv6 Overview

QUESTION 86

which security feature bypasses routing or switching lookup?

- A. transparent mode
- B. secure wire
- C. mixed mode
- D. MACsec

Correct Answer: A

Section:

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.

Reference:

Secure Wire Overview

Mixed Mode Overview

MACsec Overview

Transparent Mode Overview

QUESTION 87

What are two important function of the Juniper Networks ATP appliance solution? (Choose two.).

- A. Statistics
- B. Analysis
- C. Detection
- D. Filtration

Correct Answer: B, C

Section:

Explanation:

<https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention/>

QUESTION 88

Exhibit.




```
[edit]
user@srx# show system security-profile
SP-1 {
    policy {
        maximum 100;
        reserved 50;
    }
    zone {
        maximum 100;
        reserved 50;
    }
    nat-nopat-address {
        maximum 115;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
}

[edit]
user@srx# show tenants
C-1 {
    security-profile {
        SP-1;
    }
}
```

Vdumps

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

- A. The c-1 TSYS has a reservation for the security flow resource.
- B. The c-1 TSYS can use security flow resources up to the system maximum.
- C. The c-1 TSYS cannot use any security flow resources.
- D. The c-1 TSYS has no reservation for the security flow resource.

Correct Answer: C, D

Section:

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-profile-logicalsyste.html