JN0-636$^{Q\&As}$

Service Provider Routing and Switching Professional (JNCIP-SP)

QUESTION 1

Which two modes are supported on Juniper ATP Cloud? (Choose two.)

A. global mode

B. transparent mode

C. private mode

D. Layer 3 mode

Correct Answer: AC

Explanation: Juniper ATP Cloud supports two main modes of operation:

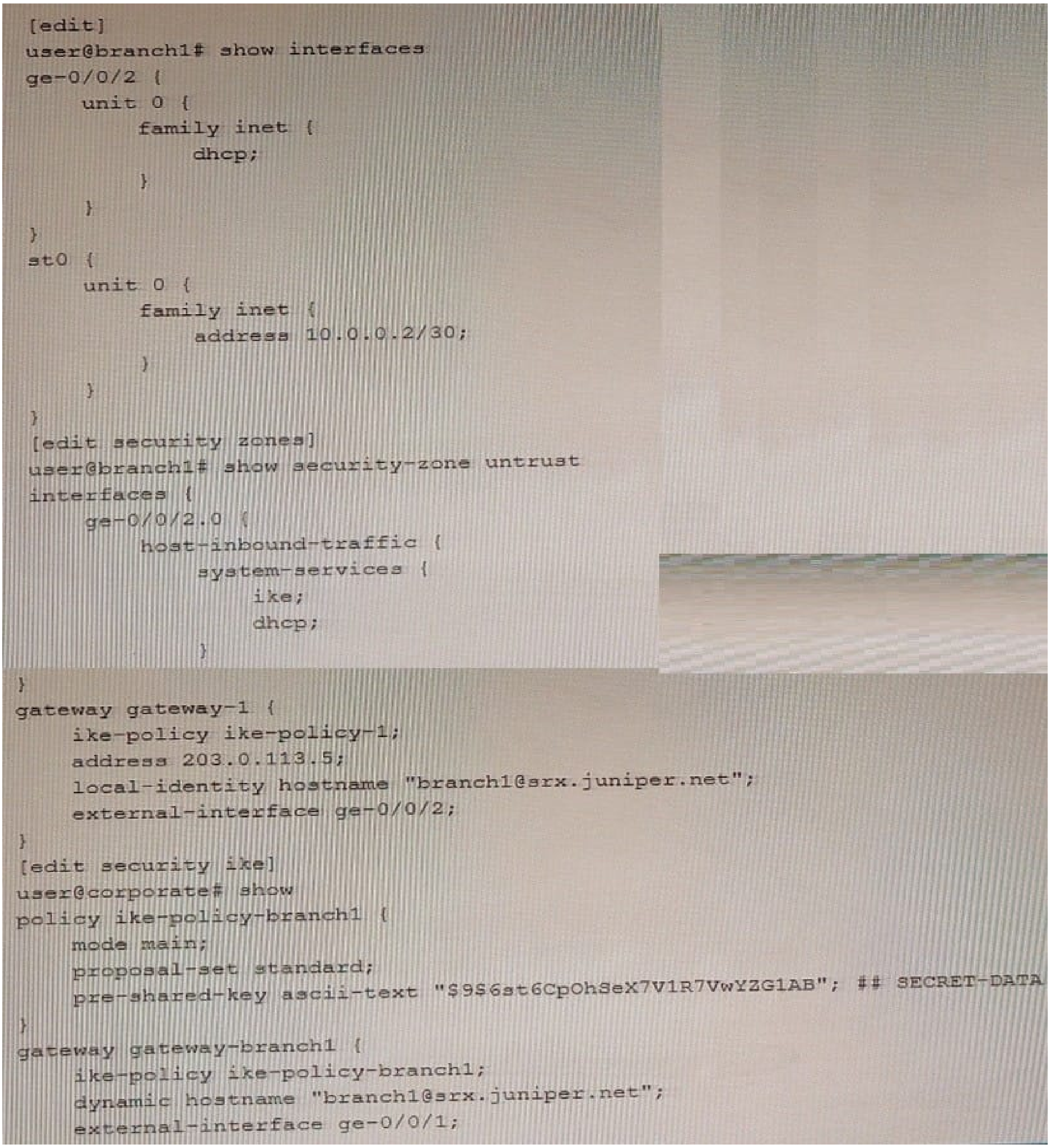
Global mode: In this mode, the Juniper ATP Cloud service analyzes all files and network traffic that pass through the cloud-based service. It uses a combination of static and dynamic analysis techniques, as well as machine learning, to detect

and block malicious files, even if they are not known to traditional anti-virus software. Private mode: In this mode, the Juniper ATP Cloud service analyzes only the files and network traffic that are specifically uploaded or submitted for analysis

by the user. It uses the same analysis techniques as in global mode, but the user has more control over which files and network traffic are analyzed and can be used to analyze files that are behind the firewall.

QUESTION 2

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.

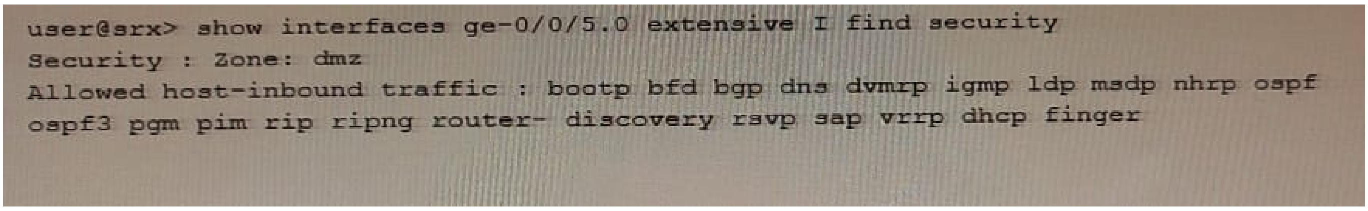
C. Change the local identity to inet advpn on the branch1 device.

D. Change the IKE mode to aggressive on the branch1 and corporate devices.

Correct Answer: C

QUESTION 3

Exhibit



```
user@srx> show interfaces ge-0/0/5.0 extensive I find security
Security : Zone: dmz
Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp ospf
ospf3 pgm 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: BDE

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

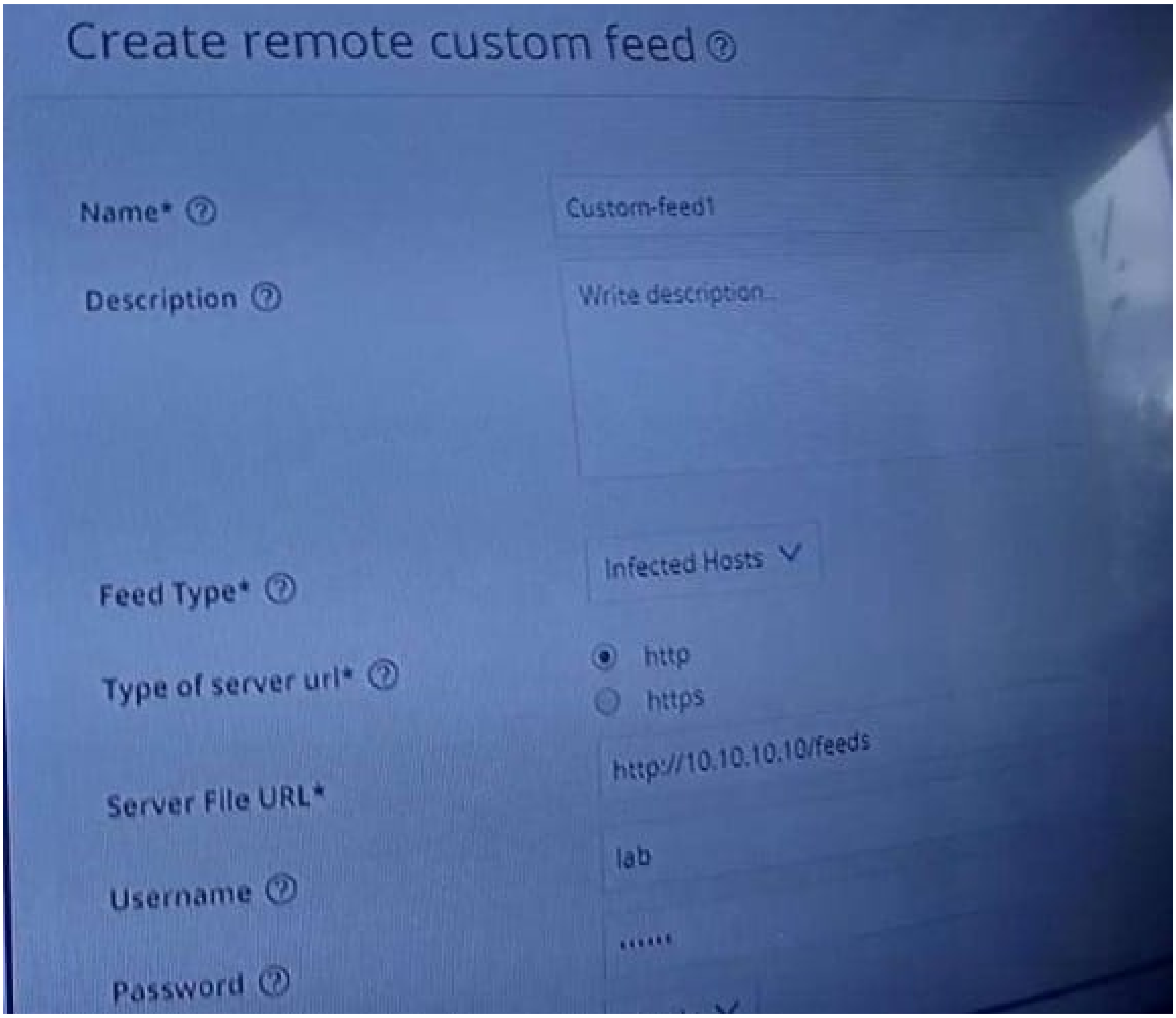
DHCP

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 4

Exhibit.



Create remote custom feed

Name*: Custom-feed1

Description: Write description...

Feed Type*: Infected Hosts

Type of server url*: ● http ○ https

Server File URL*: http://10.10.10.10/feeds

Username: lab

Password: ••••••

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: AC

Explanation: https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host- configure.html

QUESTION 5

You want to enforce I DP 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: AD

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

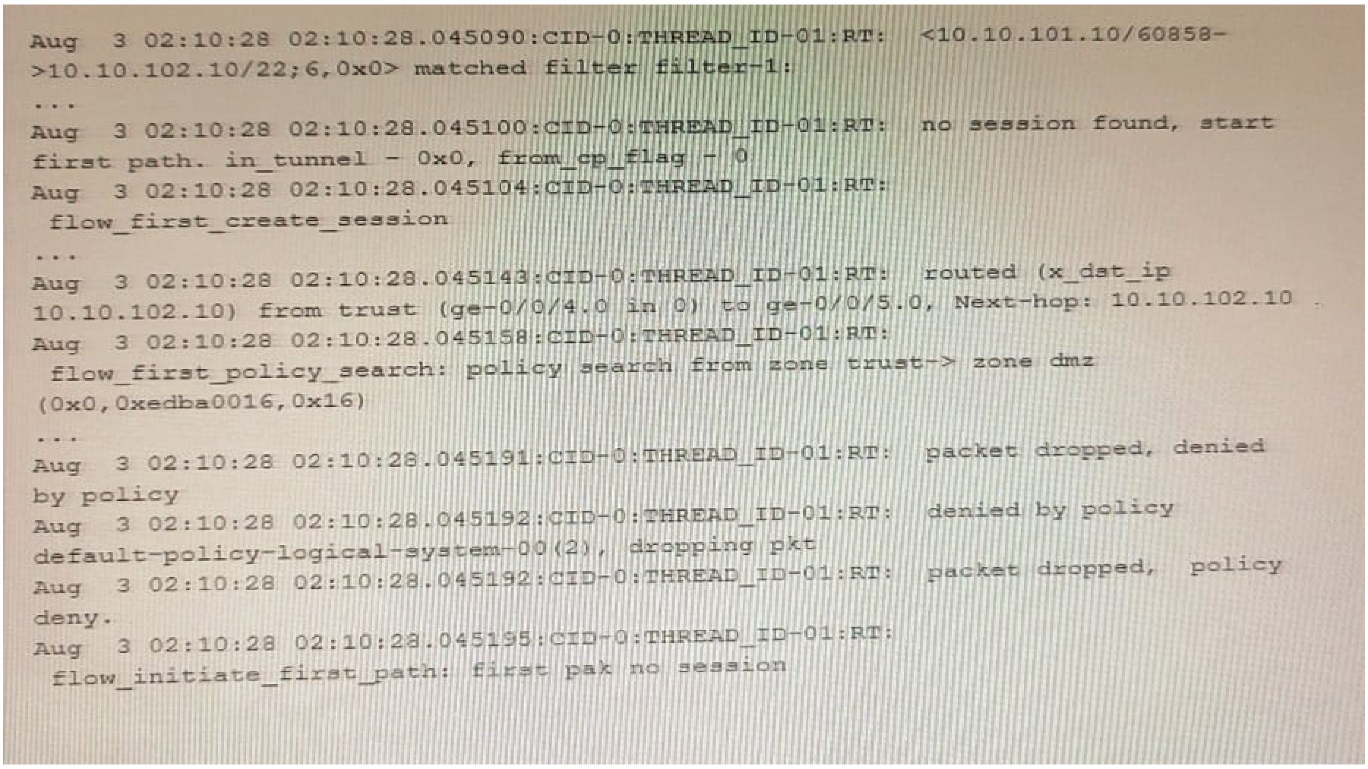
(XSS) attacks.

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 6

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: AB

QUESTION 7

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: CD

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

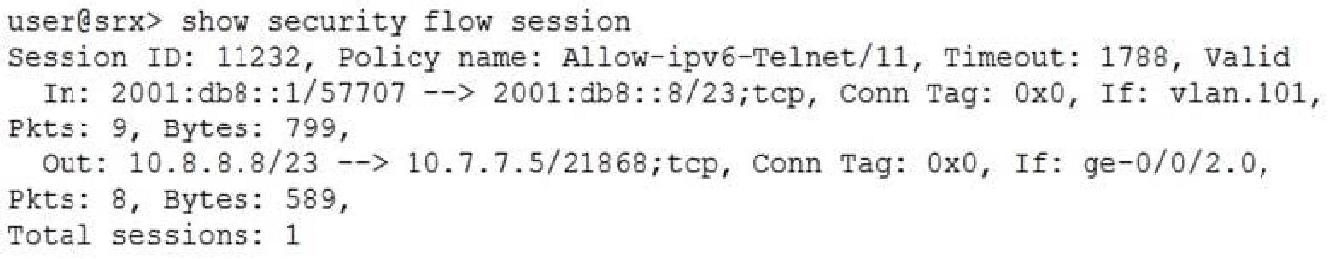
Each tenant system runs its own instance of the routing protocol process. Each tenant system is isolated, and it has its own routing table, interfaces, and security policies.

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 8

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

QUESTION 9

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

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 10

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: AB

Explanation: To block all known Tor network IP addresses on an SRX Series device, the following steps must be taken:

Enroll the devices with Juniper ATP Appliance or Juniper ATP Cloud: both of these services provide threat intelligence feeds that include known IP addresses associated with the Tor network. By enrolling the SRX Series device, the device

will have access to the latest Tor network IP addresses, and it can then use this information to block traffic from those IP addresses. Creating a custom feed containing all current known MAC addresses, is not a valid option since Tor network

uses IP addresses, MAC addresses are not used to identify the Tor network.

Enable a third-party Tor feed may be used but it\\'s not necessary as Juniper ATP Appliance and Juniper ATP Cloud already provide the same feature.

QUESTION 11

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

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 12

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: BC

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: BD

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.

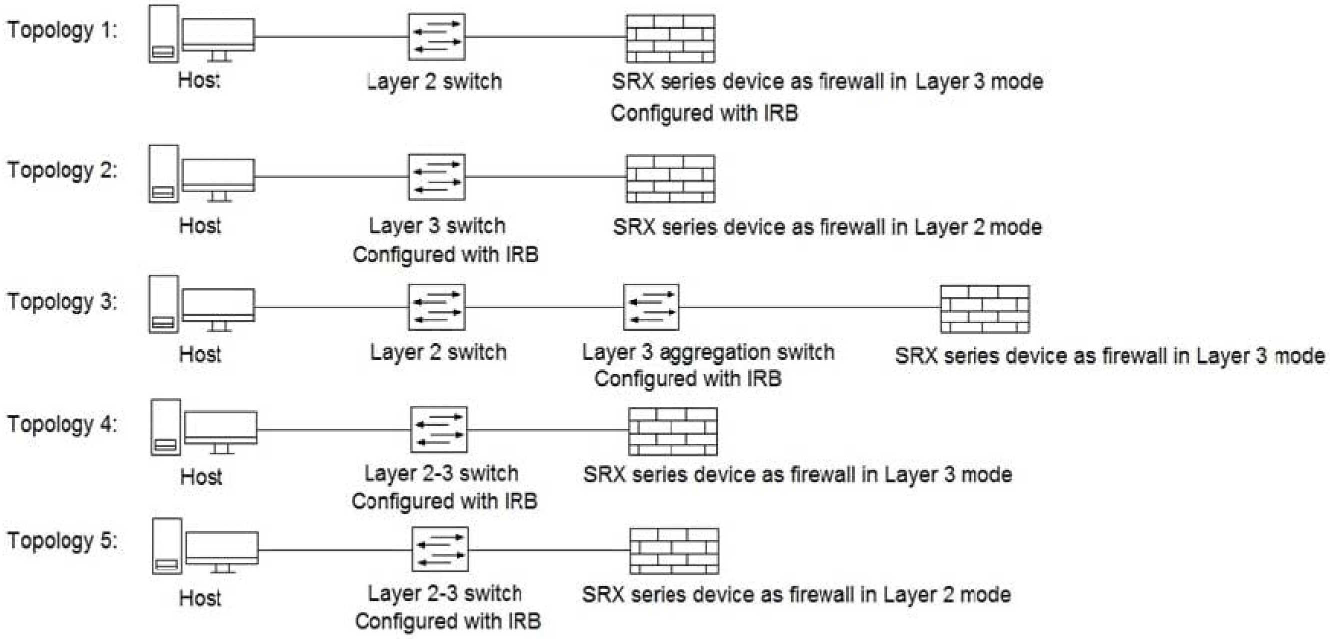
Quarantine the host: This action will isolate the infected host from the network by placing it in a quarantine VLAN. This will prevent the host from communicating with other devices on the network, which will prevent it from spreading malware

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.

QUESTION 14

Click the Exhibit button.


Topology 1:
Host
Layer 2 switch
SRX series device as firewall in Layer 3 mode
Configured with IRB
Topology 2:
Host
Layer 3 switch
Configured with IRB
SRX series device as firewall in Layer 2 mode
Topology 3:
Host
Layer 2 switch
Layer 3 aggregation switch
Configured with IRB
SRX series device as firewall in Layer 3 mode
Topology 4:
Host
Layer 2-3 switch
Configured with IRB
SRX series device as firewall in Layer 3 mode
Topology 5:
Host
Layer 2-3 switch
Configured with IRB
SRX series device as firewall in Layer 2 mode

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

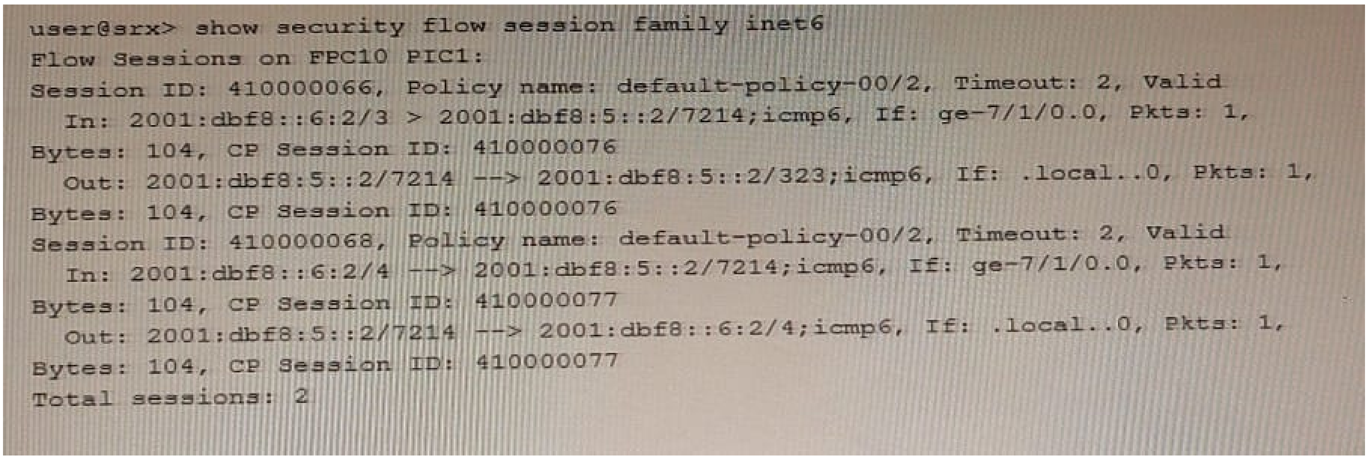
E. Topology 1

Correct Answer: ADE

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

QUESTION 15

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: A

[Latest JN0-636 Dumps](#) [JN0-636 PDF Dumps](#) [JN0-636 VCE Dumps](#)