Free Questions for JN0-636 by dumpssheet

Shared by Cline on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

Options:

A- Policy p4

B- Policy p7

C- Policy p1

D- Policy p12

Answer:

B

Question 2

Question Type: MultipleChoice

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

Options:

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.

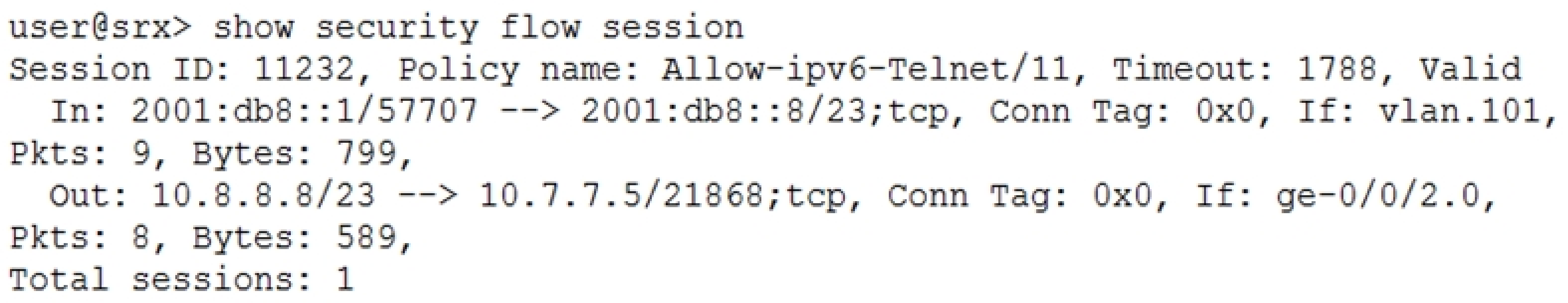
Answer:

A, C

Question 3

Question Type: MultipleChoice

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?

Options:

A- NAT46

B- NAT64

C- persistent NAT

D- DS-Lite

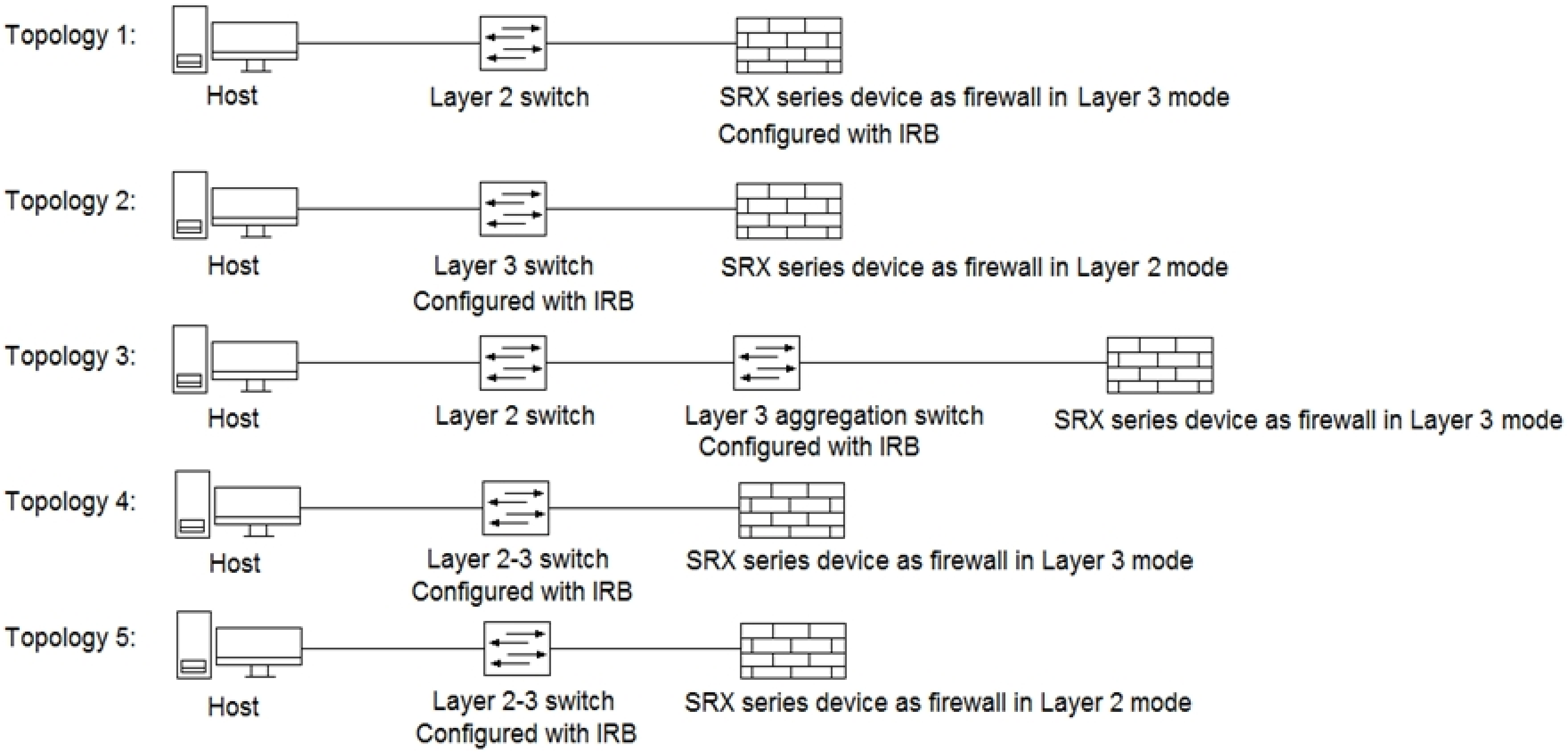
Answer:

B

Question 4

Question Type: MultipleChoice

Refer to the Exhibit.


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.)

Options:

A- Topology 3

B- Topology 5

C- Topology 2

D- Topology 4

E- Topology 1

Answer:

A, D, E

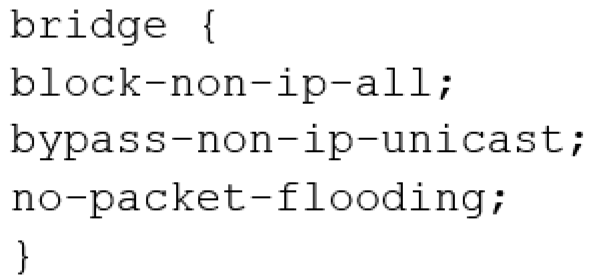
Question 5

Question Type: **MultipleChoice**

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.

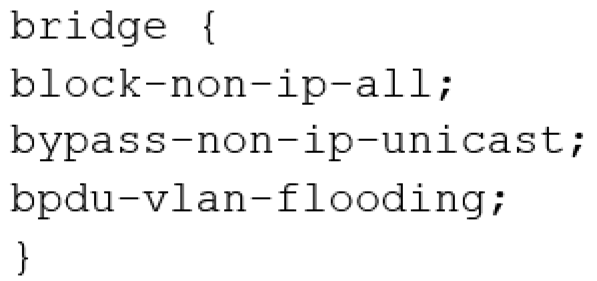
Which configuration accomplishes these objectives?

A)



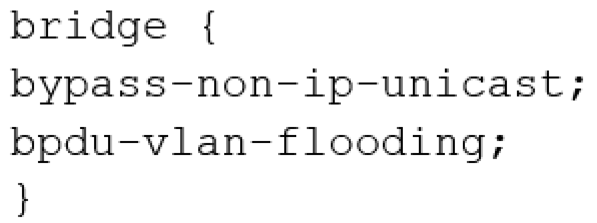
```
bridge {
block-non-ip-all;
bypass-non-ip-unicast;
no-packet-flooding;
}
```

B)



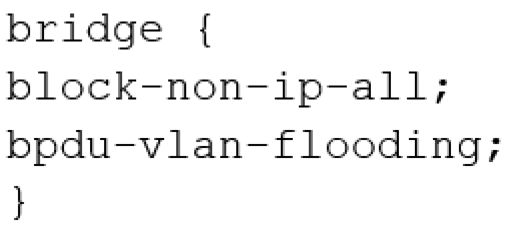
```
bridge {
block-non-ip-all;
bypass-non-ip-unicast;
bpdu-vlan-flooding;
}
```

C)



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

D)



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

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

D

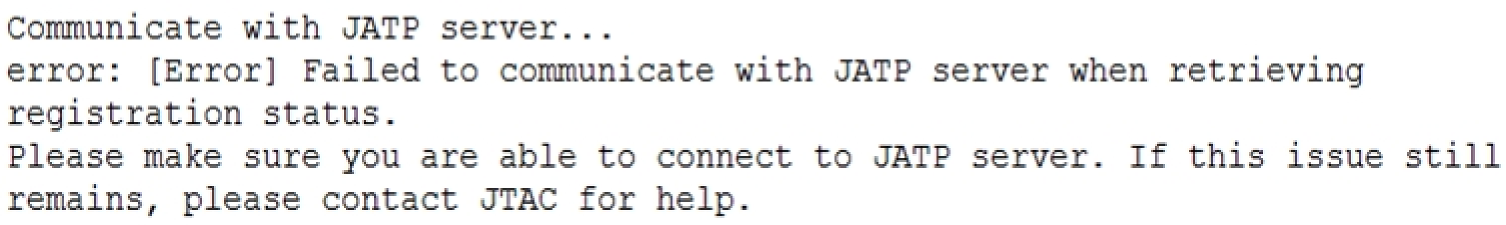
Explanation:

https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/ref/statement/family-ethernet-switching-edit-interfaces-qfx-series.html#statement-name-statement__d26608e73

Question 6

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Question 7

Question Type: **MultipleChoice**

You are requested to enroll an SRX Series device with Juniper ATP Cloud.

Which statement is correct in this scenario?

Options:

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.

Answer:

D

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 theenrollcommand 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 theenrollcommand 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.

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 8

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

D

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

Question 9

Question Type: MultipleChoice

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 Seclnte1. You have an SRX Series device that is using Seclnte1 feeds from Juniper ATP Cloud

Which command will return this information?

Options:

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

Answer:

A

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 10

Question Type: MultipleChoice

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?

Options:

A- Disable PAT.

B- Enable destination NAT.

C- Enable persistent NAT

D- Enable address persistence.

Answer:

D

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 11

Question Type: MultipleChoice

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

Options:

A- LLDP-MED

B- IGMP snooping

C- RSTP

D- packet flooding

Answer:

D

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.