JN0-635.VCEplus.premium.exam.65q

Number: JN0-635
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

JN0-635

Security, Professional (JNCIP-SEC)

Version 1.0

Exam A

QUESTION 1
Click the Exhibit button.

```
user@srx> show security mka statistics

      Interface name: fxp1
      Received packets:                          3
      Transmitted packets:                       3
      Version mismatch packets:                  0
      CAK mismatch packets:                      6
      ICV mismatch packets:                      0
      Duplicate message identifier packets:      0
      Duplicate message number packets:          0
      Duplicate address packets:                 0
      Invalid destination address packets:       0
      Formatting error packets:                  0
      Old Replayed message number packets        0
```

While configuring the SRX345, you review the MACsec connection between devices and note that it is not working.

Referring to the exhibit, which action would you use to identify problem?

A. Verify that the formatting settings are correct between the devices and that the software supports the version of MACsec in use
B. Verify that the connectivity association key and the connectivity association key name match on both devices
C. Verify that the transmission path is not replicating packets or correcting frame check sequence error packets
D. Verify that the interface between the two devices is up and not experiencing errors

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-security-mka-statistics.html

QUESTION 2
Click the Exhibit button.

```
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 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  close-client-and-server;
            }
```

You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all the rules in your IPS policy.

In this scenario, which action would be taken?

A. `drop packet`
B. `no-action`
C. `close-client-and-server`
D. `ignore-connection`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policy-rules-and-rulebases.html

QUESTION 3
Your organization has multiple Active Directory domains to control user access. You must ensure that security policies are passing traffic based upon the users' access rights.

What would you use to assist your SRX Series devices to accomplish this task?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-intergrated-user-firewall-overview.html

QUESTION 4 You are asked to set up notifications if one of your collector traffic feeds drops below 100 kbps.

Which two configuration parameters must be set to accomplish this task? (Choose two.)

A. Set a traffic SNMP trap on the JATP appliance
B. Set a logging notification on the JATP appliance
C. Set a general triggered notification on the JATP appliance
D. Set a traffic system alert on the JATP appliance

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You have configured static NAT for a webserver in your DMZ. Both internal and external users can reach the webserver using the webserver's IP address. However, only internal users can reach the webserver using the webserver's DNS name. When external users attempt to reach the webserver using the webserver's DNS name, an error message is received.

Which action would solve this problem?

A. Disable Web filtering
B. Use DNS doctoring

C. Modify the security policy
D. Use destination NAT instead of static NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-dns-algs.html

QUESTION 6 Which interface family is required for Layer 2 transparent mode on SRX Series devices?

A. LLDP
B. Ethernet switching
C. inet
D. VPLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Click the Exhibit button.

```
user@srx> show chassis cluster interfaces
Control link status: Up

Control interfaces:
      Index    Interface         Monitored-Status     Internal-SA    Security
      0        em0               Up                   Disabled       Enabled

Fabric link status: Up

...
```

Referring to the exhibit, which statement is true?

A. ARP security is securing data across the control interface
B. IPsec is securing data across the control interface
C. SSH is securing data across the control interface
D. MACsec is securing data across the control interface

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-cluster-interfaces.html

QUESTION 8
You have configured three logical tunnel interfaces in a tenant system on an SRX1500 device. When committing the configuration, the commit fails.

In this scenario, what would cause this problem?

A. There is no GRE tunnel between the tenant system and master system allowing SSH traffic
B. There is no VPLS switch on the tenant system containing a peer It-0/0/0 interface
C. The SRX1500 device does not support more than two logical interfaces per tenant systemD. The SRX1500 device requires a tunnel PIC to allow for logical tunnel interfaces

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/logical-systems-overview.html

QUESTION 9
You are asked to merge to corporate network with the network from a recently acquired company. Both networks use the same private IPv4 address space (172.25.126.0/24). An SRX Series device servers as the gateway for each network.

Which solution allows you to merge the two networks without modifying the current address assignments?

A. persistent NAT
B. NAT46
C. source NATD. double NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.juniper.net/InfoCenter/index?page=content&id=KB21286

QUESTION 10
You have set up Security Director with Policy Enforcer and have configured 12 third-party feeds and a Sky ATP feed. You are also injecting 16 feeds using the available open API. You want to add another compatible feed using the available open API, but Policy Enforcer is not receiving the new feed.

What is the problem in this scenario?

A. You must wait 48 hours for the feed to update
B. You cannot add more than 16 feeds through the available open API
C. You have reached the maximum limit of 29 total feeds
D. You cannot add more than 16 feeds with the available open API

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/pathway-pages/sky-atp-admin-guide.pdf page 110

QUESTION 11 Which three types of peer devices are supported for CoS-based IPsec VPNs?
(Choose three.)

A. branch SRX Series device
B. third-party device
C. cSRX
D. high-end SRX Series device
E. vSRX

Correct Answer: ADE

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-based-ipsec-vpns.html

QUESTION 12 You are asked to configure a new SRX Series CPE device at a remote office. The device must participate in forwarding MPLS and IPsec traffic.

Which two statements are true regarding this implementation? (Choose two.)

A. Host inbound traffic must not be processed by the flow module
B. Host inbound traffic must be processed by the flow module
C. The SRX Series device can process both MPLS and IPsec with default traffic handling
D. A firewall filter must be configured to enable packet mode forwarding

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-packet-based-forwarding.html

QUESTION 13 Which three roles or protocols are required when configuring an ADVPN?
(Choose three.)

A. OSPF
B. shortcut partner
C. shortcut suggester
D. IKEv1
E. BGP

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discovery-vpns.html

QUESTION 14 You must troubleshoot ongoing problems with IPsec tunnels and security policy processing. Your network consists of SRX340s and SRX5600s.

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

A. IPsec logs are written to the kmd log file by default
B. IKE logs are written to the messages log file by default
C. You must enable data plane logging on the SRX340 devices to generate security policy logs
D. You must enable data plane logging on the SRX5600 devices to generate security policy logs

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 15
Click the Exhibit button.

```
user@host> telnet 172.20.202.10
Connected to 172.20.202.10.
Escape character is '^]'.
remote-device (ttyp1)
login:

user@srx> show security flow session application telnet
Session ID: 68748, Policy name: FBF-Internet/11, Timeout: 1722, Valid
 In: 172.20.201.10/55530 --> 172.20.202.10/23;tcp, Conn Tag: 0x0, If: ge-
0/0/5.0,
Pkts: 28, Bytes: 1624,
 Out: 172.20.202.10/23 --> 172.20.201.10/55530;tcp, Conn Tag: 0x0, If:
ge-0/0/1.0, Pkts: 22, Bytes: 1418,
Total sessions: 1
```

You are implementing a new branch site and want to ensure Internet traffic is sent directly to your ISP and other traffic is sent to your company headquarters. You have configured filter-based forwarding to accomplish this objective. You verify proper functionality using the outputs shown in the exhibit.

Which two statements are true in this scenario? (Choose two.)

A. The session utilizes one routing instance
B. The ge-0/0/5 and ge-0/0/1 interfaces must reside in a single security zone
C. The ge-0/0/5 and ge-0/0/1 interfaces can reside in different security zones
D. The session utilizes two routing instances

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Click the Exhibit button.

```
user@srx> show log flow-trace
Apr 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:
...
Apr 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
...
Apr 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow first create session
...
...
Apr 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
...
Apr 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)
...
Apr 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by
policy
...
Apr 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
...
Apr 3 02:10:28 02:10:28.0451 92:CID-0.THREAD_ID-01:RT: packet dropped, policy
deny
```

The exhibit shows a snippet of a security flow trace. A user cannot open an SSH session to a server.

Which action will solve the problem?

A. Create a security policy that matches the traffic parameters
B. Edit the source NAT to correct the translated address
C. Create a route entry to direct traffic into the configured tunnel
D. Create a route to the desired server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Click the Exhibit button.

```
user@srx> show security macsec connections
Interface name: ge-0/0/0
      CA name: ca1
      Cipher suite: GCM-AES-128          Encryption: on
      Key server offset: 0               Include SCI: no
      Replay protect: off                Replay window: 0
            Outbound secure channels
                  SC Id: 02:00:00:01:01:04/1
                  Outgoing packet number: 1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
            Inbound secure channels
                  SC Id: 02:00:00:02:01:04/1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
```

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

A. Data is transmitted across the link in plaintext
B. The link is not protected against man-in-the-middle attacks
C. The link is protected against man-in-the-middle attacks
D. Data is transmitted across the link in cyphertext

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 You are asked to secure your network against TOR network traffic.

Which two Juniper products would accomplish this task? (Choose two.)

A. Contrail Edge
B. Contrail Insights
C. Juniper Sky ATP
D. Juniper ATP Appliance

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 You are asked to implement the session cache feature on an SRX5400.

In this scenario, what information does a session cache entry record? (Choose two.)

A. The type of processing to do for ingress traffic
B. The type of processing to do for egress traffic

C. To which SPU the traffic of the session should be forwarded
D. To which NPU the traffic of the session should be forwarded

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-packet-based-forwarding.html

QUESTION 20 Which feature of Sky ATP is deployed with Policy Enforcer?

A. zero-day threat mitigation
B. software image snapshot support
C. device inventory management
D. service redundancy daemon configuration support

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Click the Exhibit button.

```
user@srx> show services advanced-anti-malware status
Server connection status:
  Server hostname: 172.25.11.120
  Server port: 443
  Proxy hostname: None
  Proxy port: None
     Control Plane:
          Connection time: 2019-11-04 02:19:57 UTC
          Connection status: Connected
     Service Plane:
          fpc0
            Connection active number: 0
            Connection retry statistics: 0

user@srx> show services security-intelligence category summary

Category name         :CC
  Status              :Enable
  Description         :Command and Control data schema
  Update interval     :1800s
  TTL                 :3456000s
  Feed name           :cc_ip_data
     Version          :N/A
     Objects number   :0
     Create time      :2019-08-22 06:49:32 PDT
     Update time      :2019-09-12 12:47:47 PDT
     Update status    :N/A
     Expired          :No
     Options          :N/A
  Feed name           :cc_ipv6_data
     Version          :20180413.1
     Objects number   :1
     Create time      :2019-08-22 06:32:29 PDT
     Update time      :2019-09-12 12:48:27 PDT
     Update status    :Store succeeded
     Expired          :No
     Options          :N/A
  Feed name           :cc_url_data
     Version          :N/A
     Objects number   :0
     Create time      :2019-08-22 06:45:32 PDT
     Update time      :N/A
     Update status    :N/A
     Expired          :No
     Options          :N/A
```

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

A. The SRX Series device is enrolled and communicating with a JATP Appliance
B. The JATP Appliance cannot download the security feeds from the GSS servers
C. The SRX Series device cannot download the security feeds from the JATP Appliance
D. The SRX Series device is not enrolled but can communicate with the JATP Appliance

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 You are asked to configure an SRX Series device to bypass all security features for IP traffic from the engineering department.

Which firewall filter will accomplish this task? A.

```
user@srx# show firewall filter eng-filter
term 1 {
     from {
          source-prefix-list {
               hr-subnet;
          }
          destination-prefix-list {
               eng-subnet;
          }
     }
     then packet-mode;
}
term 2 {
     then accept;
}
```


B.

```
user@srx# show firewall filter eng-filter
term 1 {
     from {
          source-prefix-list {
               eng-subnet;
          }
     }
     then packet-mode;
}
term 2 {
     then accept;
}
```

```
user@srx# show firewall filter eng-filter
term 1 {
     from {
          source-prefix-list {
               eng-subnet;
          }
          destination-prefix-list {
               hr-subnet;
          }
     }
     then accept;
}
term 2 {
     then packet-mode;
}
```

```
user@srx# show firewall filter eng-filter
term 1 {
     from {
          source-prefix-list {
               eng-subnet;
          }
     }
     then accept;
}
term 2 {
     then accept;
}
```

C.

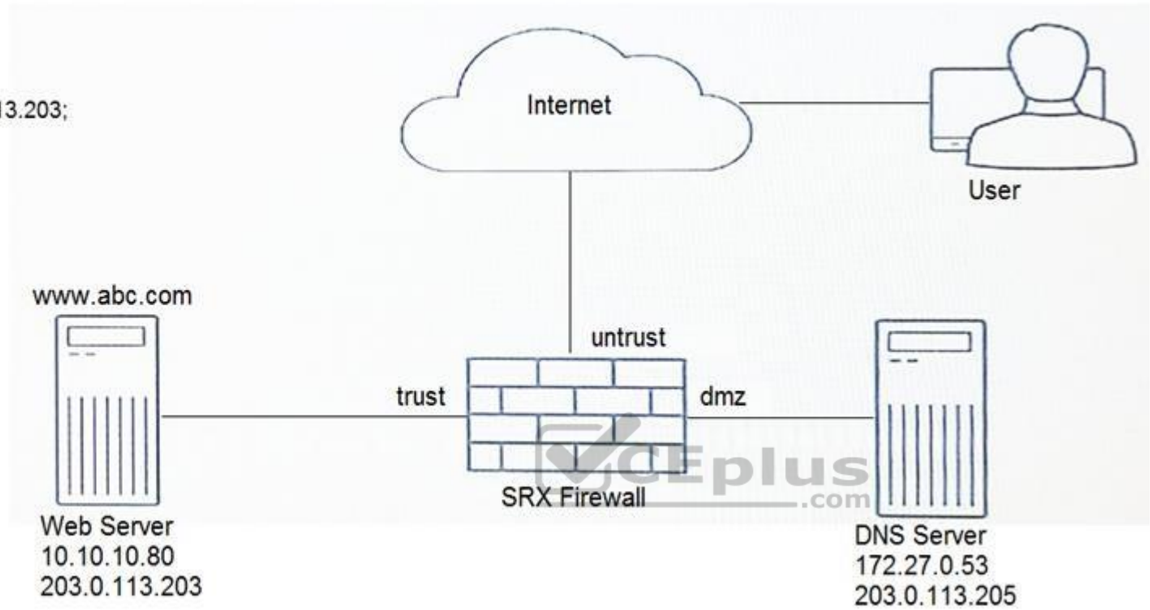
D.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Click the Exhibit button.

```
user@srx> show configuration security nat static
static {
  rule-set abc_rule1 {
        from zone untrust;
        rule 1 {
          match {
                destination-address 203.0.113.203;
          }
          then {
             static-nat {
                prefix {
                    10.10.10.80;
                }
             }
          }
        }
    }
}
```



A user is trying to reach a company's website, but the connection errors out. The security policies are configured correctly.

Referring to the exhibit, what is the problem?

A. Persistent NAT must be enabled
B. The action for rule 1 must change to `static-nat inet`
C. DNS ALG must be disabled
D. Static NAT is missing a rule for DNS server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Click the Exhibit button.


```
user@hq# show security ike
...
gateway ike_gtw-branch {
     ike-policy ike-policy-branch;
     dynamic hostname branch.abc.com;
     external-interface ge-0/0/0;
     local-address 203.0.113.1;
}
```

The IKE policy and proposal are configured properly on both devices as shown in the exhibit.

Which configuration snippet will complete the IKE configuration on the branch SRX Series device? A.

```
[edit security ike]
user@srx# show gateway ike_gtw_hq
ike-policy ike-policy-hq;
dynamic hostname branch.abc.com;
external-interface ge-0/0/0;
local-address 203.0.113.2;
```



```
[edit security ike]
user@srx# show gateway ike_gtw_hq
ike-policy ike-policy-hq;
dynamic hostname hq.abc.com;
external-interface ge-0/0/0;
local-address 203.0.113.2;
```

```
[edit security ike]
user@srx# show gateway ike_gtw_hq
ike-policy ike-policy-hq;
local-identity hostname hq.abc.com;
external-interface ge-0/0/0;
local-address 203.0.113.2;
```

```
[edit security ike]
user@srx# show gateway ike_gtw_hq
ike-policy ike-policy-hq;
local-identity hostname branch.abc.com;
external-interface ge-0/0/0;
local-address 203.0.113.2;
```

B. C.

D.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 25 You are trying to get a SSH honeypot set up on a Juniper ATP Appliance collector. The collector is running on hardware with two physical interfaces and two physical CPU cores. The honeypot feature is not working.

Which statement is true in this scenario?

A. The collector must have at least three physical interfaces
B. The collector must have at least four physical cores
C. The collector must have at least four physical interfaces
D. The collector must have at least six physical cores

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
You correctly configured a security policy to deny certain traffic, but logs reveal that traffic is still allowed.

Which specific `traceoption` flag will help you troubleshoot this problem?

A. `lookup`
B. `configuration`
C. `routing-socket`
D. `rules`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Click the Exhibit button.

```
[edit]
user@srx# show
...
interfaces {
  xe-0/0/1 {
      description "Connected to Finance";
      unit 0 {
        family inet {
            address 10.1.1.1/24;
        }
      }
  }
  xe-0/1/0 {
      description "Connected to Internet";
      unit 0 {
        family inet {
            address 192.168.2.2/30;
        }
      }
  }
  xe-0/2/1 {
      description "Connected to Sales";
      unit 0 {
        family inet {
            address 10.3.2.21/24;
        }
      }
}
firewall {
     filter filter1 {
       term t1 {
           from {
                source-address {
                     10.1.1.3/32;
                }
           }
           then {
             next-interface {
                xe-0/1/0.0;
                routing-instance eval1;
             }
           }
       }
       term t2 {
           then {
                routing-instance default;
           }
       }
     }
  }
  routing-instances {
     eval1 {
       instance-type virtual-router;
       interface xe-0/1/0.0;
     }
  }
```

You are asked to look at a configuration that is designed to take all traffic with a specific source IP address and forward the traffic to a traffic analysis server for further evaluation. The configuration is not working as intended.

Referring to the exhibit, which change must be made to correct the configuration?

A. Apply the filter as an input filter on interface xe-0/2/1.0
B. Create a routing instance named default
C. Apply the filter as an input filter on interface xe-0/0/1.0
D. Apply the filter as an output filter on interface xe-0/1/0.0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
When would you use the `port-overloading-factor 1` setting?

A. to enable the port-overloading
B. to disable the port-overloading
C. to map ports with 1:1 ratio for port-overloading
D. to set the maximum port-overloading capacity to 65,536

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-edit-port-overloading-interface-source-nat.html

QUESTION 29 Which Junos security feature is used for signature-based attack prevention?

A. RADIUS B.
AppQoS
C. IPS
D. PIM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
You are asked to configure an IPsec VPN between two SRX Series devices that allows for processing of CoS on the intermediate routers.

What will satisfy this requirement?

A. route-based VPN
B. OpenVPN
C. remote access VPN
D. policy-based VPN

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-based-ipsec-vpns.html

QUESTION 31
Click the Exhibit button.

```
[edit]
user@srx# show security policies
from-zone client to-zone Internet {
     policy Adv-Services {
          match {
               source-address any;
               destination-address any;
               dynamic-application any;
          }
          then {
               permit {
                    application-services {
                         ssl-proxy {
                              profile-name SSL-pro;
                         }
                         security-intelligence-policy Sky-intel;
                         advanced-anti-malware-policy Sky-pol;
                    }
               }
          }
     }
}

[edit]
user@srx# show security flow
syn-flood-protection-mode syn-cookie;
tcp-session {
     maximum-window 1M;
}
```

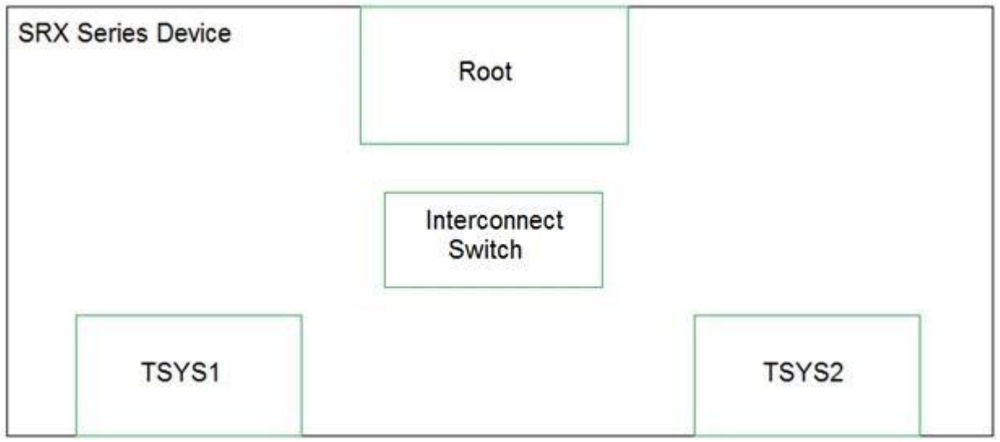
You deployed a site-to-site IPsec VPN connecting two data centers together using SRX5800s. After examining the performance of the IPsec VPN, you decide to enable IPsec performance acceleration to increase the rate of traffic that can be sent through the tunnel.

Referring to the exhibit, which two statements should you add to the configuration to accomplish this task? (Choose two.)

A. `[edit security flow] user@srx# set tcp-mss ipsec-vpn mss 65535` B. `[edit security flow] user@srx# set ipsec-performance-acceleration` C. `[edit security flow] user@srx# set power-mode-ipsec` D. `[edit security flow] user@srx# set load-distribution session-affinity ipsec`
Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-improving-ipsec-vpn-traffic-performance.html

QUESTION 32
Click the Exhibit button.



You have configured tenant systems on your SRX Series device.

Referring to the exhibit, which two actions should you take to facilitate inter-TSYS communication? (Choose two.)

A. Place the logical tunnel interfaces in a virtual router routing instance in the interconnect switch
B. Place the logical tunnel interfaces in a VPLS routing instance in the interconnect switch
C. Connect each TSYS with the interconnect switch by configuring INET configured logical tunnel interfaces in the interconnect switch
D. Connect each TSYS with the interconnect switch by configuring Ethernet VPLS configured logical tunnel interfaces in the interconnect switch

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 358216, Policy name: default-policy-logical-system-00/2, Timeout:
1788, Valid
  In: 10.10.10.1/63261 --> 203.0.113.10/443;tcp, Conn Tag: 0x0, If: ge-0/0/1.0,
Pkts: 632, Bytes: 49341,
  Out: 203.0.113.10/443 --> 172.25.11.4/21740;tcp, Conn Tag: 0x0, If: ge-
0/0/0.0, Pkts: 662, Bytes: 79325,
```

Referring to the exhibit, which statement is true?

A. Source NAT with PAT is occurring
B. Destination NAT is occurring
C. Static NAT without PAT is occurring
D. Source NAT without PAT is occurring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Click the Exhibit button.

```
  [edit interfaces]
user@new-site-gateway# show st0
unit 0 {
  family inet {
     address 10.0.0.2/30;
     }
}

  [edit interfaces]
user@new-site-gateway# show ge-0/0/2
unit 0 {
family inet {
dhcp ;

  [edit security zones]
user@new-site-gateway# show security-zone untrust
interfaces {
  ge-0/0/2.0 {
     host-inbound-traffic {
      system-services {
          ike;
          dhcp;
       }
     }
  }
}
  [edit security ike]
user@new-site-gateway# show
policy ike-pol-1 {
     mode main;
     proposal-set standard;
     pre- shared- key ascii - text "  $9$6st6CpOhSeX7V1RwYZG69A"; ## SECRET-
DATA
     }
gateway gate-1 {
  ike-policy ike-pol-1;
  address 203.0.113.5;
  local-identity hostname "srx1@srx.juniper.net";
  external-interface ge-0/0/2.0;
}
```

Your company has purchased a competitor and now must connect the new network to the existing one. The competitor's gateway device is receiving its ISP address using DHCP. Communication between the two sites must be secured; however, obtaining a static public IP address for the new site gateway is not an option at this time. The company has several requirements for this solution:

▪ A site-to-site IPsec VPN must be used to secure traffic between the two sites;
▪ The IKE identity on the new site gateway device must use the hostname option; and ▪ Internet traffic from each site should exit through its local Internet connection.

The configuration shown in the exhibit has been applied to the new site's SRX, but the secure tunnel is not working.

In this scenario, what configuration change is needed for the tunnel to come up?

A. Remove the quotes around the hostname
B. Bind interface st0 to the gateway
C. Change the IKE policy mode to aggressive
D. Apply a static address to ge-0/0/2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Click the Exhibit button.

```
user@host> show ethernet-switching global-information
Global Configuration:

MAC aging interval          : 300
MAC learning                : Enabled
MAC statistics              : Disabled
MAC limit Count             : 65535
MAC limit hit               : Disabled
MAC packet action drop      : Disabled
LE aging time               : 1200
LE VLAN aging time          : 1200
Global Mode                 : Switching
```

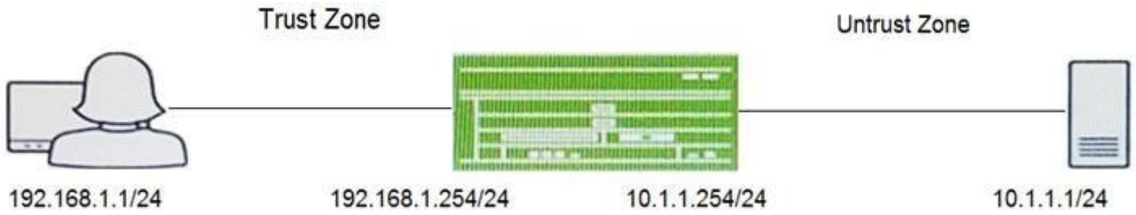
Referring to the exhibit, which two statements are true? (Choose two.)

A. You can secure intra-VLAN traffic with a security policy on this device
B. You can secure inter-VLAN traffic with a security policy on this device
C. The device can pass Layer 2 and Layer 3 traffic at the same time
D. The device cannot pass Layer 2 and Layer 3 traffic at the same time

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ethernet-port-switching-modes.html

QUESTION 36
Click the Exhibit button.



A user reports trouble when using SSH to a server outside your organization. The traffic traverses an SRX Series device that is performing NAT and applying security policies.

Referring to the exhibit, which configuration will allow you to see the bidirectional flow through the SRX Series device? A.

```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 192.168.1.254/32;
}
packet-filter MATCH-TRAFFIC-IN {
     source-prefix 10.1.1.1/32;
     destination-prefix 10.1.1.254./32;
}
```



```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 192.168.1.254/32;
}
```

```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC {
     source-prefix 192.168.1.1/32;
     destination-prefix 10.1.1.1/32;
}
```

B.

C.

```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 10.1.1.1/32;
}
packet-filter MATCH-TRAFFIC-IN {
     source-prefix 10.1.1.1/32;
     destination-prefix 192.168.1.1./32;
}
```

D.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Click the Exhibit button.

```
user@host# show system security-profile
production-profile {
  zone {
      maximum 10;
      reserved 5;
  }
  logical-system [ ACME WILEY ];
}
development-profile {
  zone {
      maximum 7;
      reserved 0;
  }
  logical-system [ IT-design security ];
}
master-profile {
  zone {
      maximum 40;
      reserved 17;
  }
  root-logical-system;
}
```

Referring to the exhibit, what is the maximum number of zones that are able to be created within all logical systems?

A. 74 B.
34
C. 40

D. 17

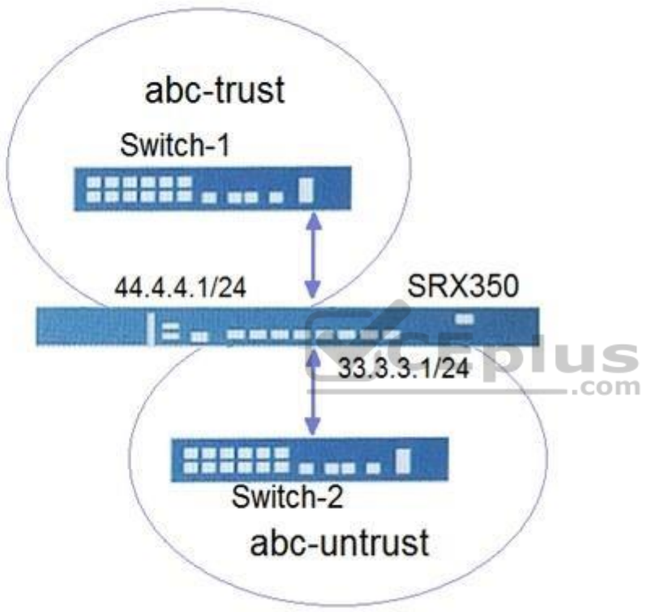
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Click the Exhibit button.

```
from-zone abc-trust to-zone abc-untrust {
     policy abc {
          match {
               source-address any;
               destination-address any;
               application any;
          }
          then {
               permit {
                    application-services {
                         idp;
from-zone abc-untrust to-zone abc-trust {
     policy abc {
          match {
               source-address any;
               destination-address any;
               application any;
          }
          then {
               permit {
                    application-services {
                         idp;
```



Referring to the exhibit, which three types of traffic would be examined by the IPS policy between Switch-1 and Switch-2? (Choose three.)

A. TCP
B. LLDP
C. ARP
D. ICMP
E. UDP

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policy-rules-and-rulebases.html

QUESTION 39
Click the Exhibit button.

```
user@srx> show log flow-trace
CID-0:RT: flow process pak fast ifl 71 in_ifp ge-0/0/5.0
CID-0:RT: ge-0/0/5.0:10.0.0.2/55892->192.168.1.2/80, tcp, flag 2 syn
CID-0:RT: find flow: table 0x5a386c90, hash 50728(0xffff), sa 10.0.0.2, da
192.168.1.2, sp 55892,
dp 80, proto 6, tok 7
CID-0:RT: no session found, start first path. in_tunnel - 0x0, from_cp_flag -
0
CID-0:RT: flow_first_create_session
CID-0:RT: flow_first_in_dst_nat: in <ge-0/0/5.0>, out <N/A> dst_adr
192.168.1.2, sp 55892, dp 80
CID-0:RT: chose interface ge-0/0/5.0 as incoming nat if.
CID-0:RT:flow_first_rule_dst_xlatE. DST no-xlatE. 0.0.0.0.(0) to
192.168.1.2(80)
CID-0:RT:flow_first_routinG. vr_id 0, call flow-route_lookup(): src_ip
10.0.0.2, x_dst_ip
192.168.1.2, in ifp ge-0/0/5.0, out ifp N/A sp 55892, dp 80, ip_proto 6, tos
10
CID-0:RT:Doing DESTINATION addr route-lookup
CID-0:RT: routed (x_dst_ip 192.168.1.2) from LAN (ge-0/0/5.0 in 0) to ge-
0/0/1.0, Next-hop:
172.16.32.1
CID-0:RT:flow_first_policy_search.policy search from zone LAN-> zone WAN
(0x0,0xda540050,0x50)
CID-0:RT:Policy lkup: vsys 0 zone(7:LAN) -> zone(6:WAN) scope:0
CID-0:RT:10.0.0.2/55892 -> 192.168.1.2/80 proto 6
CID-0:RT:Policy lkup: vsys 0 zone(5:Unknown) -> zone(5:Unknown) scope:0
CID-0:RT: 10.0.0.2/55892 -> 192.168.1.2/80 proto 6
CID-0:RT: app 6, timeout 1800s, curr ageout 20s
CID-0:RT: packet dropped, denied by policy
CID-0:RT: denied by policy default-policy-00(2), dropping pkt
CID-0:RT: packet dropped, policy deny
CID-0:RT: flow find session returns error
CID-0:RT: ----- flow_process_pkt rc 0x7 (fp rc -1)
CID-0:RT:jsf sess close notify
CID-0:RT:flow ipv4 del flow: sess, in hash 32
```

A host is unable to communicate with a webserver.

Referring to the exhibit, which statement is correct?

A. The webserver is not listening for traffic on port 80
B. A policy is denying the traffic between these two hosts
C. A session is created for this flow
D. The session table is running out of resources

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Click the Exhibit button.

```
user@srx-1> show security ipsec next-hop-tunnels
Next-hop gateway    interface     IPsec VPN name       Flag      XAUTH-USERNAME
10.10.10.2          st0.0         srx1-to-srx2         Auto      Not-Available
10.10.10.3          st0.0         srx1-to-srx3         Auto      Not-Available
10.10.10.4          st0.0         srx1-to-srx4         Auto      Not-Available
```

Which statement is correct regarding the information show in the exhibit?

A. The tunnel binding was discovered automatically
B. The output is for an ADVPN
C. The tunnel gateway address was automatically discovered
D. The tunnel is not encrypting the traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-security-ipsec-next-hop-tunnels.html

QUESTION 41 In which two ways are tenant systems different from logical systems?
(Choose two.)

A. Tenant systems have higher scalability than logical systems
B. Tenant systems have less scalability than logical systems
C. Tenant systems have fewer routing features than logical systems
D. Tenant systems have more routing features than logical systems

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/tenant-systems-overview.html#:~:text=Although%20similar%20to%20logical%20systems,administrative%20domain%20for%20security%20services

QUESTION 42
Which two statements are true about ADVPN members? (Choose two.)

A. ADVPN members are authenticated using pre-shared keys
B. ADVPN members are authenticated using certificates
C. ADVPN members can use IKEv2
D. ADVPN members can use IKEv1

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discovery-vpns.html

QUESTION 43 Which two VPN features are supported with CoS-based IPsec VPNs?
(Choose two.)

A. IKEv2
B. VPN monitoring

C. dead peer detection
D. IKEv1

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-based-ipsec-vpns.html

QUESTION 44
Click the Exhibit button.

```
user@srx> show security flow session destination-prefix 172.31.15.1
destination-port 22 extensive
Session ID: 19867, Status: Normal
Flags: 0x40/0x0/0x8003
Policy name: internet-trust/5
Source NAT pool: Null, Application: junos-ssh/22
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 1766
Session State: Valid
Start time: 598746, Duration: 45
  In: 10.10.101.10/61179 --> 172.31.15.1/22;tcp,
 Conn Tag: 0x0, Interface: ge-0/0/4.0,
   Session token: 0x7, Flag: 0x1021
   Route: 0x110010, Gateway: 10.10.101.10, Tunnel: 0
   Port sequence: 0, FIN sequence: 0,
   FIN state: 0,
    Pkts: 18, Bytes: 3261
  Out: 172.31.15.1/22 --> 10.10.101.10/61179;tcp,
 Conn Tag: 0x0, Interface; ge-0/0/3.0,
  Session token: 0x9, Flag: 0x1020
  Route: 0x120010, Gateway: 172.18.1.2, Tunnel: 0
  Port sequence: 0, FIN sequence: 0,
  FIN state: 0,
  Pkts: 16, Bytes: 3773
Total sessions: 1
```

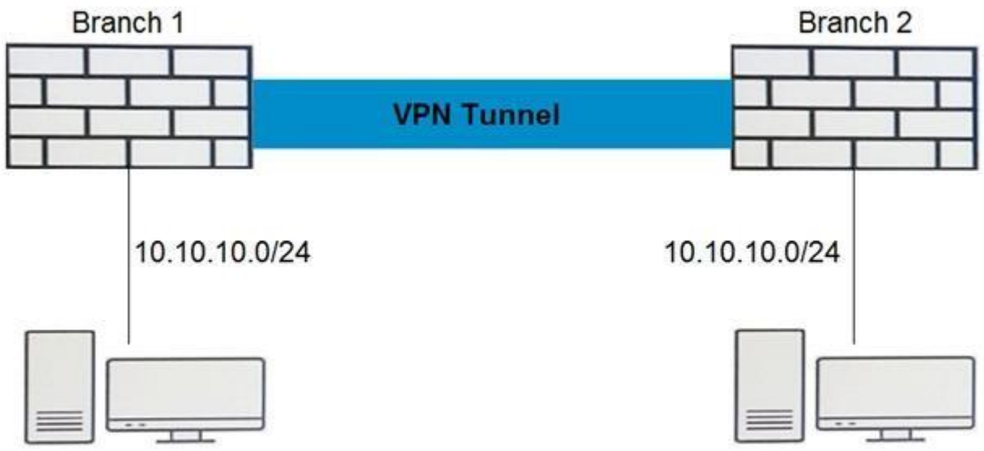
Given the command output shown in the exhibit, which two statements are true? (Choose two.)

A. The host 172.31.15.1 is directly connected to interface ge-0/0/3.0
B. Traffic matching this session has been received since the session was established
C. The host 10.10.101.10 is directly connected to interface ge-0/0/4.0
D. Network Address Translation is applied to this session

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Click the Exhibit button.



Branch 1 and Branch 2 have an active VPN tunnel configured, but internal hosts cannot communicate with each other.

Referring to the exhibit, which type of configuration should be applied to solve the problem?

A. Configure destination NAT on both Branch 1 and Branch 2
B. Configure source NAT on Branch 1
C. Configure destination NAT on Branch 2 only
D. Configure static NAT on both Branch 1 and Branch 2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Your SRX Series device does not see the SYN packet.

What is the default action in this scenario?

A. The device will forward the subsequent packets and the session will be established
B. The device will forward the subsequent packets and the session will not be established
C. The device will drop the subsequent packets and the session will not be established
D. The device will drop the subsequent packets and the session will be established

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-tcp-session-checks.html

QUESTION 47
Click the Exhibit button.

```
[edit]
user@srx# show security policies
from-zone Client to-zone Internet {
     policy Adv-Services {
          match {
               source-address any;
               destination-address any;
               dynamic-application any;
          }
          then {
               permit {
                    application-services {
                         ssl-proxy {
                              profile-name SSL-pro;
                         }
                         security-intelligence-policy Sky-intel;
                         advanced-anti-malware-policy Sky-pol;
                    }
               }
          }
     }
}

[edit]
user@srx# show security flow
ipsec-performance-acceleration;
load-distribution session-affinity ipsec;
tcp-mss {
     ipsec-vpn {
          mss 65535;
     }
}
```

Referring to the exhibit, you are attempting to enable IPsec power mode to improve IPsec VPN performance. However, you are unable to use IPsec power mode.

What is the problem?

A. IPsec power mode cannot be used with IPsec performance acceleration
B. IPsec power mode cannot be used with high IPsec maximum segment size values
C. IPsec power mode cannot be used with advanced services
D. IPsec power mode requires that you configure a policy-based VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation//en_US/junos/topics/reference/configuration-statement/security-flow-power-mode-ipsec.html

QUESTION 48
Click the Exhibit button.

```
user@SRX5800> show security idp status

------------------------------------------------------------------------
State of IDP: Default,  Up since: 2019-11-02 09:58:29 EDT (1w5d 03:44 ago)

Packets/second: 1           Peak: 441 @ 2019-11-14 11:02:54 EST
KBits/second : 35881        Peak: 285133 @ 2019-11-14 12:43:05 EST
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 713498] [UDP: 0] [Other: 0]

Flow Statistics:
 ICMP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]
 TCP:[Current: 10] [Max: 23153 @ 2019-11-14 12:28:38 EST]
 UDP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]
 Other:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]

Session Statistics:
 [ICMP: 0] [TCP: 5] [UDP: 0] [Other: 0]

Number of SSL Sessions : 0

 Policy Name : IPS-POLICY
 Running Detector Version : 12.6.130190828

Forwarding process mode : regular
```

Referring to the exhibit, which IPS deployment mode is running on the SRX5800 device?

A. sniffer mode
B. integrated mode
C. monitor mode
D. in-line tap mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 In a Juniper ATP Appliance, what would be a reason for the mitigation rule to be in the failed-remove state?

A. The Juniper ATP Appliance received a commit error message from the SRX Series device
B. The Juniper ATP Appliance received an unknown error message from the SRX Series device
C. The Juniper ATP Appliance was not able to communicate with the SRX Series device
D. The Juniper ATP Appliance was not able to obtain the config lock

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/topic-map/jatp-mitigation-and-reporting.html

QUESTION 50 An administrator wants to implement persistent NAT for an internal resource so that external hosts are able to initiate communications to the resource, with the internal resource having previously sent packets to the external hosts.

Which configuration setting is used to accomplish this goal?

A. `persistent-nat permit any-remote-host`
B. `persistent-nat permit target-host-port`
C. `address-persistent`
D. `persistent-nat permit target-host`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 How does secure wire mode differ from transparent mode?

A. In secure wire mode, no switching lookup takes place to forward traffic
B. In secure wire mode, traffic can be modified using source NAT
C. In secure wire mode, IRB interfaces can be configured to route inter-VLAN traffic
D. In secure wire mode, security policies cannot be used to secure intra-VLAN traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-secure-wire.html

QUESTION 52 What are two important functions of the Juniper Networks ATP Appliance solution? (Choose two.)

A. filtration
B. detection
C. statistics
D. analytics

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 53
Click the Exhibit button.

```
[edit]
user@host# show interfaces ge-0/0/4
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show interfaces ge-0/0/5
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show vlans
SV {
     vlan-id 101;
}

[edit]
user@host# show security zones security-zone L2
interfaces {
     ge-0/0/4.0;
     ge-0/0/5.0;
}

[edit]
user@host# show security policies

[edit]
user@host#

[edit]
user@host# run show ethernet-switching global-information
Global Configuration:

MAC aging interval          : 300
MAC learning                : Enabled
MAC statistics              : Disabled
MAC limit Count             : 65535
MAC limit hit               : Disabled
MAC packet action drop      : Disabled
LE aging time               : 1200
LE VLAN aging time          : 1200
Global Mode                 : Transparent bridge
```


You have two hosts on the same subnet connecting to an SRX340 on interfaces ge-0/0/4 and ge-0/0/5. However, the two hosts cannot communicate with each other.

Referring to the exhibit, what are two actions that would solve this problem? (Choose two.)

A. Set the SRX340 to Ethernet switching mode and reboot
B. Add an IRB interface to the VLAN
C. Put the ge-0/0/4 and ge-0/0/5 interfaces in different VLANs
D. Remove the ge-0/0/4 and ge-0/0/5 interfaces from the L2 security zone

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You have downloaded and initiated the installation of the application package for the JATP Appliance on an SRX1500. You must confirm that the installation of the application package has completed successfully.

In this scenario, which command would you use to accomplish this task?

A. `show services application-identification version`
B. `show services application-identification application detail`
C. `show services application-identification application version`
D. `show services application-identification status`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-application-identification-predefined-signatures.html

QUESTION 55
You have a remote access VPN where the remote users are using the NCP client. The remote users can access the internal corporate resources as intended; however, traffic that is destined to all other Internet sites is going through the remote access VPN. You want to ensure that only traffic that is destined to the internal corporate resources use the remote access VPN.

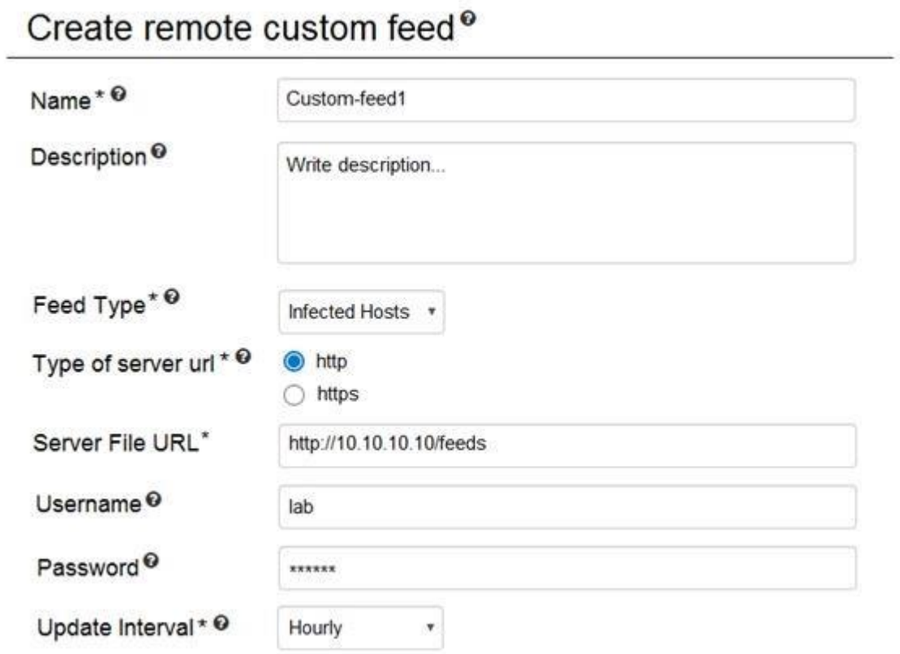
Which two actions should you take to accomplish this task? (Choose two.)

A. Enable the split tunneling feature within the VPN configuration on the SRX Series device
B. Enable IKEv2 within the VPN configuration on the SRX Series device
C. Configure the necessary traffic selectors within the VPN configuration on the SRX Series deviceD. Configure split tunneling on the NCP profile on the remote client

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-remote-access-vpns-with-ncp-exclusive-remote-access-client.html

QUESTION 56
Click the Exhibit button.



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

A. Events based on this third-party feed will not affect a host's threat score
B. SRX Series devices will block traffic based on this third-party feed
C. SRX Series devices will not block traffic based on this third-party feed
D. Events based on this third-party feed will affect a host's threat score

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-integrated-feeds.html

QUESTION 57
Click the Exhibit button.

```
[edit protocols ospf area 0.0.0.0]
user@srx# show
interface ge-0/0/4.0 {
     passive;
}
interface ge-0/0/5.0 {
     passive;
}
interface ge-0/0/6.0 {
     passive;
}
interface st0.0 {
     interface-type p2mp;
}
```

You have configured an ADVPN that is operational. However, OSPF will not establish correctly across the ADVPN tunnels. Referring

to the exhibit, which two commands will solve the problem? (Choose two.)

A. `[edit protocols ospf area 0.0.0.0] user@srx# set interface st0.0 dynamic-neighbors` B. `[edit protocols ospf area 0.0.0.0] user@srx# set interface st0.0 topology advpn` C. `[edit protocols ospf area 0.0.0.0] user@srx# set interface st0.0 interface-type nbma` D. `[edit protocols ospf area 0.0.0.0] user@srx# set interface st0.0 demand-circuit`

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discovery-vpns.html

QUESTION 58 Which two modes are supported on Juniper Sky ATP?
(Choose two.)

A. private mode
B. global mode
C. tap mode
D. secure wire mode

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-about.html

QUESTION 59
You configured a security policy permitting traffic from the trust zone to the DMZ zone, inserted the new policy at the top of the list, and successfully committed it to the SRX Series device. Upon monitoring, you notice that the hit count does not increase on the newly configured policy.

In this scenario, which two commands would help you to identify the problem? (Choose two.)

A. `user@srx> show security zones trust detail`
B. `user@srx> show security shadow-policies from zone trust to zone DMZ`
C. `user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port 443`
D. `user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port 443 result-count 10`

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/monitoring-troubleshooting-security-policy.html

QUESTION 60
A user is unable to reach a necessary resource. You discover the path through the SRX Series device includes several security features. The traffic is not being evaluated by any security policies.

In this scenario, which two components within the flow module would affect the traffic? (Choose two.)

A. services/ALG
B. destination NAT
C. source NAT
D. route lookup

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Malware that is detonated by the JATP sandbox must be able to communicate with the Internet without being able to harm your local network resources.

Which statement is correct in this scenario?

A. The management interface must be connected to the Internet zone
B. The exhaust interface must be connected to the Internet zone
C. The honeypot interface must be connected to the Internet zone
D. The monitoring interface must be connected to the Internet zone

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/topic-map/jatp-getting-started.html

QUESTION 62
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: (none)
Explanation

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

QUESTION 63
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.

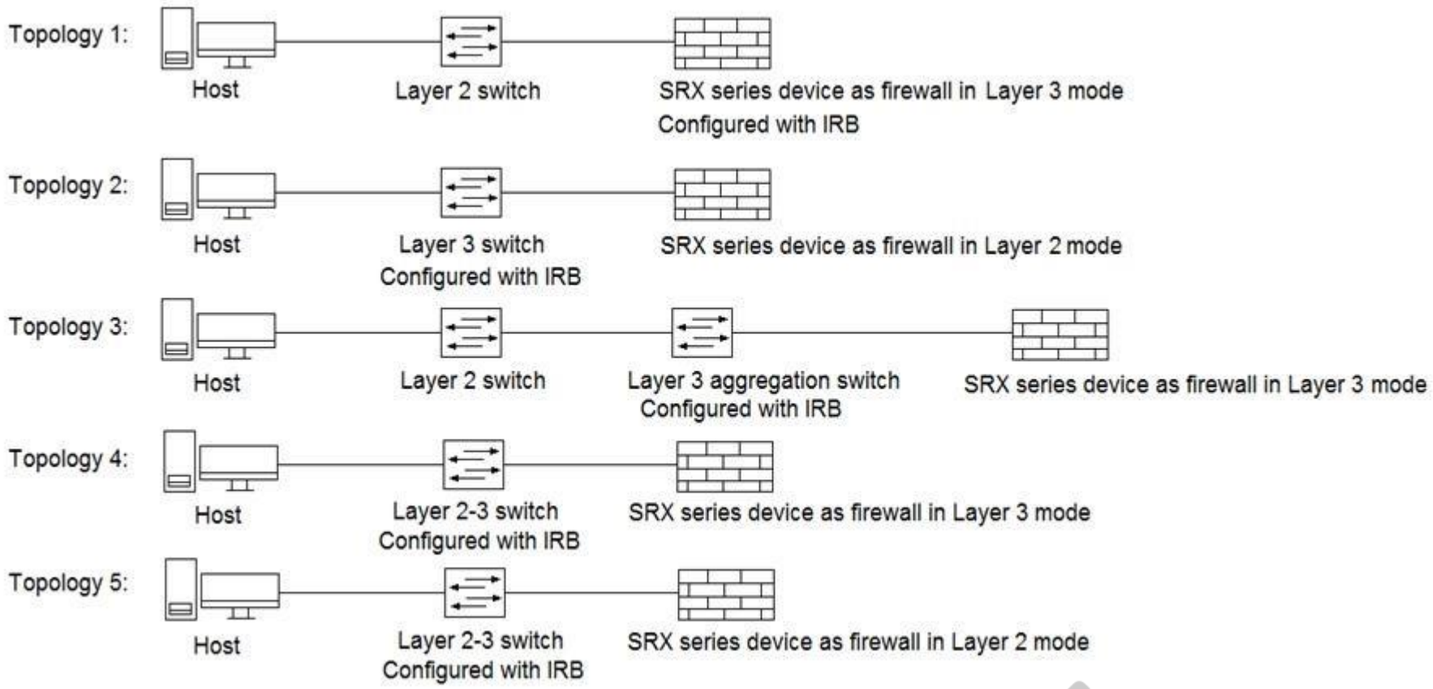
```
bridge {
block-non-ip-all;
bpdu-vlan-flooding;
}
```

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.oreilly.com/library/view/juniper-srx-series/9781449339029/ch06.html

QUESTION 64

Click the Exhibit button.



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
Section: (none)
Explanation

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

QUESTION 65
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: (none)
Explanation

Explanation/Reference: