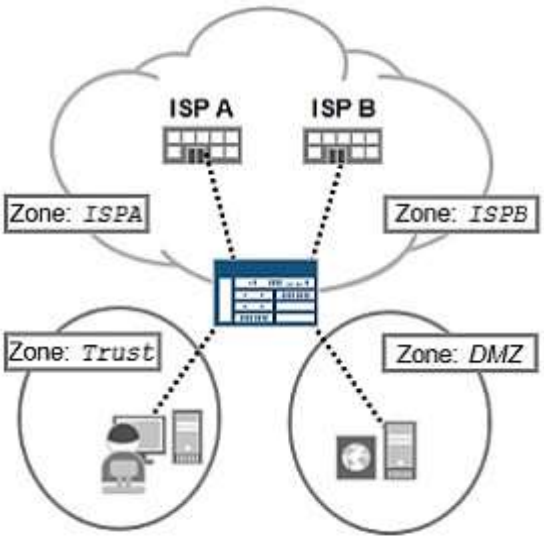
Vendor: Juniper

Exam Code: JN0-633

Exam Name: Security, Professional (JNCIP-SEC) Exam

Version: Demo

QUESTION 1
Click the Exhibit button. Referring to the exhibit, which feature allows the hosts in the Trust and DMZ zones to route to either ISP, based on source address?



A. source NAT
B. static NAT
C. filter-based forwarding
D. source-based routing

Answer: C
Explanation:
http://www.juniper.net/techpubs/en_US/junos12.2/topics/example/logical-systems-filter-based-forwarding.html

QUESTION 2
You have an existing group VPN established in your internal network using the group-id 1. You have been asked to configure a second group using the group-id 2. You must ensure that the key server for group 1 participates in group 2 but is not the key server for that group.Which statement is correct regarding the group configuration on the current key server for group 1?

A. You must configure both groups at the [edit security ipsec vpn] hierarchy.
B. You must configure both groups at the [edit security group-vpn member] hierarchy.
C. You must configure both groups at the [edit security ike] hierarchy.
D. You must configure both groups at the [edit security group-vpn] hierarchy.

Answer: D
Explanation:
http://www.jnpr.net/techpubs/en_US/junos11.4/information-products/topic-collections/security/software-all/security/index.html?topic-45791.html

QUESTION 3
You have installed a new IPS license on your SRX device and successfully downloaded the attack signature database. However, when you run the command to install the database, the

database fails to install.What are two reasons for the failure? (Choose two.)

A. The file system on the SRX device has insufficient free space to install the database.
B. The downloaded signature database is corrupt.
C. The previous version of the database must be uninstalled first.
D. The SRX device does not have the high memory option installed.

Answer: AB
Explanation:
We don't need to uninstall the previous version to install a new license, as we can update the same.
Reference: http://kb.juniper.net/InfoCenter/index?page=content&id=KB16491.
Also high memory option is licensed feature.
The only reason for failure is either there is no space left or downloaded file is corrupted due to incomplete download because of internet termination in between.
Reference: http://kb.juniper.net/InfoCenter/index?page=content&id=KB23359

QUESTION 4
Which QoS function is supported in transparent mode?

A. 802.1p
B. DSCP
C. IP precedence
D. MPLS EXP

Answer: A
Explanation:
http://chimera.labs.oreilly.com/books/1234000001633/ch06.html

QUESTION 5
You are asked to implement IPsec tunnels between your SRX devices located at various locations. You will use the public key infrastructure (PKI) to verify the identification of the endpoints.What are two certificate enrollment options available for this deployment? (Choose two.)

A. Manually generating a PKCS10 request and submitting it to an authorized CA.
B. Dynamically generating and sending a certificate request to an authorized CA using OCSP.
C. Manually generating a CRL request and submitting that request to an authorized CA.
D. Dynamically generating and sending a certificate request to an authorized CA using SCEP.

Answer: AD
Explanation:
http://www.juniper.net/techpubs/en_US/junos/information-products/topic-collections/nce/pki-conf-trouble/configuring-and-troubleshooting-public-key-infrastructure.pdf

QUESTION 6
Click the Exhibit button. According to the log shown in the exhibit, you notice that the IPsec session is not establishing. What are two reasons for this behavior? (Choose two.)

```
Feb 8 10:39:40 Unable to find phase-1 policy as remote peer:2.2.2.2 is not re
Feb 8 10:39:40 KMD_PM_P1_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-1 [re
p1_local=ipv4(any:0,[0..3]=1.1.1.2) p1_remote=ipv4(any:0,[0..3]=2.2.2.2)
Feb 8 10:39:40 1.1.1.2:500 (Responder) <-> 2.2.2.2:500 { 18983055 dbe1d0af -
0x00000000 } IP; Error = No proposal chosen (14)
```

- Exhibit --

Feb 8 10:39:40 Unable to find phase-1 policy as remote peer:2.2.2.2 is not recognized.

Feb 8 10:39:40 KMD_PM_P1_POLICY_LOOKUP_FAILURE.Policy lookup for Phase-1 [responder] failed for p1_local=ipv4(any:0,[0..3]=1.1.1.2) p1_remote=ipv4(any:0,[0..3]=2.2.2.2)

Feb 8 10:39:40 1.1.1.2:500 (Responder) <-> 2.2.2.2:500 { dbe1d0af - a4d6d829 f9ed3bba [-1] / 0x00000000 } IP; Error = No proposal chosen (14)

- Exhibit --

A. mismatched preshared key
B. mismatched proxy ID
C. incorrect peer address
D. mismatched peer ID

Answer: CD
Explanation:
If the peer was not matched with the peer ID, the line "Unable to find phase-1 policy as remote peer:192.168.1.60 is not recognized." should be shown.
Reference: http://kb.juniper.net/InfoCenter/index?page=content&id=KB10097&pmv=print

QUESTION 7
Your company has added a connection to a new ISP and you have been asked to send specific traffic to the new ISP. You have decided to implement filter-based forwarding. You have configured new routing instances with type forwarding. You must direct traffic into each instance.Which step would accomplish this goal?

A. Add a firewall filter to the ingress interface that specifies the intended routing instance as the action.
B. Create a routing policy to direct the traffic to the required forwarding instances.
C. Configure the ingress and egress interfaces in each forwarding instance.
D. Create a static default route for each ISP in inet.0, each pointing to a different forwarding instance.

Answer: A
Explanation:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB17223

QUESTION 8
Which problem is introduced by setting the terminal parameter on an IPS rule?

A. The SRX device will stop IDP processing for future sessions.
B. The SRX device might detect more false positives.
C. The SRX device will terminate the session in which the terminal rule detected the attack.

D. The SRX device might miss attacks.

Answer: D
Explanation:
http://www.juniper.net/techpubs/software/junos-security/junos- security10.2/junos-security-swconfig-security/topic-42464.html

QUESTION 9
You want to implement a hub-and-spoke VPN topology using a single logical interface on the hub.Which st0 interface configuration is correct for the hub device?

A.
```
[edit interfaces]
user@srx# show
st0 {
multipoint
unit 0 {
family inet {
address 10.10.10.1/24;
}
}
}
```
B.
```
[edit interfaces]
user@srx# show
st0 {
unit 0 {
family inet {
address 10.10.10.1/24;
}
}
}
```
C.
```
[edit interfaces]
user@srx# show
st0 {
unit 0 {
point-to-point;
family inet {
address 10.10.10.1/24;
}
}
}
```
D.
```
[edit interfaces]
user@srx# show
st0 {
unit 0 {
multipoint;
family inet {
address 10.10.10.1/24;
}
}
}
```

Answer: D
Explanation:
http://junos.com/techpubs/en_US/junos12.1/topics/example/ipsec-hub-and-spoke-

configuring.html

QUESTION 10
At which two times does the IPS rulebase inspect traffic on an SRX device? (Choose two.)

A. When traffic matches the active IDP policy.
B. When traffic first matches an IDP rule with the terminal parameter.
C. When traffic uses the application layer gateway.
D. When traffic is established in the firewall session table.

Answer: AB
Explanation:
http://books.google.co.in/books?id=2HSLsTJIgEQC&pg=PA814&lpg=PA814&dq=what+time+IPS+rulebase+inspects+traffic+on+SRX&source=bl&ots=_eDe_vLNBA&sig=1I4yX_S0OvkQVP-rqL273laMCyE&hl=en&sa=X&ei=nqvzUfn1Is-rrAf71oHYBA&ved=0CC4Q6AEwAQ#v=onepage&q=what%20time%20IPS%20rulebase%20inspects%20traffic%20on%20SRX&f=false

QUESTION 11
You want to configure in-band management of an SRX device in transparent mode. Which command is required to enable this functionality?

A. set interfaces irb unit 1 family inet address
B. set interfaces vlan unit 1 family inet address
C. set interfaces ge-0/0/0 unit 0 family inet address
D. set interfaces ge-0/0/0 unit 0 family bridge address

Answer: A
Explanation:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB23823

QUESTION 12
Click the Exhibit button. Based on the output shown in the exhibit, what are two results? (Choose two.)

```
user@srx> show security flow session
Session ID: 136, Policy name: Trust-Web-Server-Int/4, Timeout: 1794, Valid
  In: 192.168.1.10/60246 --> 172.16.1.7/80;tcp, If: ge-0/0/8.0, Pkts: 3, Byte
  Out: 192.168.10.100/80 --> 192.168.1.10/60246;tcp, If: ge-0/0/9.0, Pkts: 2,
Total sessions: 1
```

A. The output shows source NAT.
B. The output shows destination NAT.
C. The port information is changed.
D. The port information is unchanged.

Answer: BD
Explanation:
http://junos.com/techpubs/software/junos-security/junos-security10.2/junos-security-cli-reference/index.html?show-security-flow-session.html

QUESTION 13
You are asked to change the configuration of your company's SRX device so that you can block nested traffic from certain Web sites, but the main pages of these Web sites must remain available to users.Which two methods will accomplish this goal? (Choose two.)

A. Enable the HTTP ALG.
B. Implement a firewall filter for Web traffic.
C. Use an IDP policy to inspect the Web traffic.
D. Configure an application firewall rule set.

Answer: BD
Explanation:
An application layer gateway (ALG) is a feature on ScreenOS gateways that enables the gateway to parse application layer payloads and take decisions on them.ALGs are typically employedto support applications that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections
(http://kb.juniper.net/InfoCenter/index?page=content&id=KB13530)

IDP policy defines the rule for defining the type of traffic permittedon network(http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/enable-idp-security-policy-section.html)

QUESTION 14
Given the following session output:

Session ID., Policy namE.default-policy-00/2, StatE.Active, Timeout: 1794, Valid

In: 2001:660:1000:8c00::b/1053 --> 2001:660:1000:9002::aafe/80;tcp, IF.reth0.0, Pkts: 4, Bytes: 574

Out: 192.168.203.10/80 --> 192.168.203.1/24770;tcp, IF.reth1.0, Pkts: 3, Bytes:

Which statement is correct about the security flow session output?

A. This session is about to expire.
B. NAT64 is used.
C. Proxy NDP is used for this session.
D. The IPv4 Web server runs services on TCP port 24770.

Answer: B
Explanation:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB22391

QUESTION 15
Click the Exhibit button. You are performing the initial IDP installation on your new SRX device. You have configured the IDP exempt rulebase as shown in the exhibit, but the commit is not successful. Referring to the exhibit, what solves the issue?
- Exhibit --

[edit security]

```
user@srx# show

idp {

idp-policy NewPolicy {

rulebase-exempt {

rule 1 {

description AllowExternalRule;

match {

source-address any;

destination-address

}

}

}

}

}
```

- Exhibit --

A. You must configure the destination zone match.
B. You must configure the IPS exempt accept action.
C. You must configure the IPS rulebase.
D. You must configure the IPS engine flow action to ignore.

Answer: C
Explanation:
http://jncie-sec.exactnetworks.net/2013/01/srx-idp-overview-initial-setup.html

QUESTION 16
You want to implement an IPsec VPN on an SRX 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.Regarding this scenario, which statement is correct?

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

Answer: A
Explanation:
http://www.juniper.net/techpubs/en_US/junos/information-products/topic-collections/nce/pki-conf-trouble/configuring-and-troubleshooting-public-key-infrastructure.pdf

QUESTION 17
Which statement is true regarding the dynamic VPN feature for Junos devices?

A. Only route-based VPNs are supported.
B. Aggressive mode is not supported.
C. Preshared keys for Phase 1 must be used.
D. It is supported on all SRX devices.

Answer: C
Explanation:
http://www.juniper.net/techpubs/en_US/junos12.1x45/information-products/pathway-pages/security/security-vpn-dynamic.pdf

QUESTION 18
Referring to the following output, which command would you enter in the CLI to produce this result?

Pic2/1

Ruleset Application Client-to-server Rate(bps) Server-to-client Rate(bps)

http-App-QoS HTTP ftp-C2S 200 ftp-C2S 200

http-App-QoS HTTP ftp-C2S 200 ftp-C2S 200

ftp-App-QoS FTP ftp-C2S 100 ftp-C2S 100

A. show class-of-service interface ge-2/1/0
B. show interface flow-statistics ge-2/1/0
C. show security flow statistics
D. show class-of-service applications-traffic-control statistics rate-limiter

Answer: D
Explanation:
http://www.juniper.net/techpubs/en_US/junos12.1x44/topics/reference/command-summary/show-class-of-service-application-traffic-control-statistics-rate-limiter.html

QUESTION 19
What are two network scanning methods? (Choose two.)

A. SYN flood
B. ping of death
C. ping sweep
D. UDP scan

Answer: CD
Explanation:
The question is about the network scanning. So correct answers are ping sweep and UDP scan as both are port scanning types.
Reference: http://althing.cs.dartmouth.edu/local/Network_Scanning_Techniques.pdf

QUESTION 20
You configured a custom signature attack object to match specific components of an attack:

HTTP-request

Pattern .*\x90 90 90 ... 90

Direction: client-to-server

Which client traffic would be identified as an attack?

A. HTTP GET .*\x90 90 90 ... 90
B. HTTP POST .*\x90 90 90 ... 90
C. HTTP GET .*x909090 ... 90
D. HTTP POST .*x909090 ... 90

Answer: A
Explanation:
http://www.juniper.net/techpubs/en_US//idp/topics/task/configuration/intrusion-detection-prevention-signature-attack-object-creating-nsm.html