Juniper

Exam JN0-633

Security, Professional (JNCIP-SEC)

Version: 8.0

[Total Questions: 175]

Question No : 1

Click the Exhibit button.

```
user@host# show interfaces
ge-0/0/0 {
unit 1 {
family bridge {
interface-mode trunk;
vlan-id-list 20;
vlan-rewrite {
translate 2 20;
}
}
}
}
```

Referring to the exhibit, which two statements are correct regarding VLAN rewrite? (Choose two.)

A. An incoming packet with VLAN tag 20 will be translated to VLAN tag 2.
B. An outgoing packet with VLAN tag 2 will be translated to VLAN tag 20.
C. An incoming packet with VLAN tag 2 will be translated to VLAN tag 20.
D. An outgoing packet with VLAN tag 20 will be translated to VLAN tag 2.

Answer: C

Question No : 2

Which AppSecure module provides Quality of Service?

A. AppTrack
B. AppFW

C. AppID
D. AppQoS

Answer: D

Question No : 3

You are asked to configure your SRX Series device to support IDP SSL inspections for up to 6,000 concurrent HTTP sessions to a server within your network.

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

A. You must add at least one PKI certificate.
B. Junos does not support more than 5000 sessions in this scenario.
C. You must enable SSL decoding.
D. You must enable SSL inspection.

Answer: C,D

Question No : 4

You are troubleshooting an SRX240 acting as a NAT translator for transit traffic. Traffic is dropping at the SRX240 in your network.Which three tools would you use to troubleshoot the issue? (Choose three.)

A. security flow traceoptions
B. monitor interface traffic
C. show security flow session
D. monitor traffic interface
E. debug flow basic

Answer: A,B,C
Reference: http://kb.juniper.net/InfoCenter/index?page=content&id=KB16110

Question No : 5

You are asked to establish a baseline for your company's network traffic to determine the bandwidth usage per application. You want to undertake this task on the central SRX device that connects all segments together.What are two ways to accomplish this goal? (Choose two.)

A. Configure a mirror port on the SRX device to capture all traffic on a data collection server for further investigation.
B. Use interface packet counters for all permitted and denied traffic and calculate the values using Junos scripts.
C. Send SNMP traps with bandwidth usage to a central SNMP server.
D. Enable AppTrack on the SRX device and configure a remote syslog server to receive AppTrack messages.

Answer: A,D

Explanation:

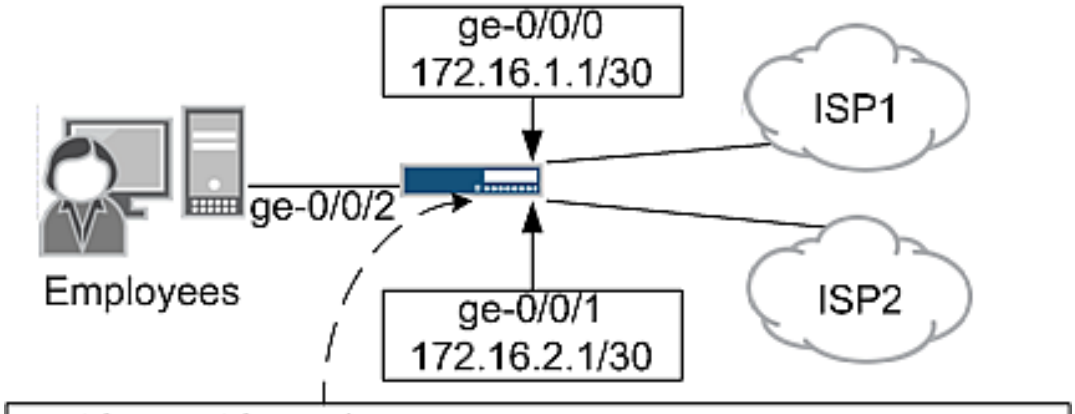
AppTrack is used for visibility for application usage and bandwidth

Reference:http://www.juniper.net/us/en/local/pdf/datasheets/1000327-en.pdf

Question No : 6

Click the Exhibit button.

-- Exhibit–




```
routing-options {
    autonomous-system 65500;
}
routing-instances {
    isp1 {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 172.16.1.2;
            }
    }
}
```

-- Exhibit --

In the network shown in the exhibit, you want to forward traffic from the employees to ISP1 and ISP2. You want to forward all Web traffic to ISP1 and all other traffic to ISP2. However, your configuration is not producing the expected results. Part of the configuration is shown in the exhibit. When you run the show route table isp1 command, you do not see the default route listed.

What is causing this behavior?

A. The autonomous system number is incorrect, which is preventing the device from receiving a default route from ISP1.
B. The device is not able to resolve the next-hop.
C. The isp1 routing instance is configured with an incorrect instance-type.
D. The show route table isp1 command does not display the default route unless you add the exact 0.0.0.0/0 option.

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

Question No : 7

Click the Exhibit button.

-- Exhibit --

[edit security idp]

user@srx# show | no-more

idp-policy basic {

rulebase-ips {

rule 1 {

match {

from-zone untrust;

source-address any;

to-zone trust;

destination-address any;

application default;

attacks {

custom-attacks data-inject;

}

}

then {

action {

recommended;

}

notification {

log-attacks;

```
}
}
}
}
}
active-policy basic;
custom-attack data-inject {
recommended-action close;
severity critical;
attack-type {
signature {
context mssql-query;
pattern "SELECT * FROM accounts";
direction client-to-server;
}
}
}
```

-- Exhibit --

You have configured the custom attack signature shown in the exhibit. This configuration is valid, but you want to improve the efficiency and performance of your IDP.

Which two commands should you use? (Choose two.)

A. set custom attack data-inject recommended-action drop
B. set custom-attack data-inject attack-type signature protocol-binding tcp
C. set idp-policy basic rulebase-ips rule 1 match destination-address webserver
D. set idp-policy basic rulebase-ips rule 1 match application any

Answer: B,C

Question No : 8

You are asked to implement a Dynamic IPsec VPN on your new SRX240. You are required to facilitate up to 5 simultaneous users.

Which two statements must be considered when accomplishing the task?

A. You must acquire at least three additional licenses.
B. Your devices must be in a chassis cluster.
C. You must be a policy-based VPN.
D. You must use main mode for your IKE phase 1 policy.

Answer: A,C

Question No : 9

Click the Exhibit button.

user@key-server> show security group-vpn server ike security-associations Index State Initiator cookie Responder cookie Mode Remote Address

97 UP bb224408940cc5d 435b9404284083c2 Main 192.168.11.1

98 UP 242c840089404d15 ab19284089408ba8 Main 192.168.11.2

user@key-server> show security group-vpn server ipsec security-associations Group: group-1, Group Id: 1

Total IPsec SAs: 1

IPsec SA Algorithm SPI Lifetime

group-l-sa ESP:3des/shal 1343991c 2736

Group: group-2, Group id: 2

Total IPsec SAs: 1

IPsec SA Algorithm SPI Lifetime

group-2-sa ESP:3des/shal 13be9e9 2741

Group: group-3, Group Id: 3

Total IPsec SAs: 1

IPsec SA Algorithm SPI Lifetime

group-3-sa ESP:3des/shal 20709057 2741

Group: group-4, Group Id: 4

Total IPsec SAs: 1

IPsec SA Algorithm SPI Lifetime

group-4-sa ESP:3des/shal 5111c2e1 2741

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

A. Two established peers are in the group VPNs.
B. One established peer is in the group VPNs.
C. No established peer is in the group VPNs.
D. Four established peers are in the group VPNs.

Answer: A

Question No : 10

Which two statements are true regarding DNS doctoring? (Choose two.)

A. DNS doctoring translates the DNS CNAME payload.
B. DNS doctoring for IPv4 is supported on SRX devices.
C. DNS doctoring for IPv4 and IPv6 is supported on SRX devices.
D. DNS doctoring translates the DNS A-record.

Answer: B,D

Explanation:

Reference :http://www.juniper.net/techpubs/en_US/junos11.4/information-products/topic-collections/security/software-all/security/index.html?topic-61847.html

Question No : 11

You have configured static NAT for a Web server in your DMZ. Both internal and external users can reach the Web server using its IP address. However, only internal users are able to reach the Web server using its DNS name. External users receive an error message from their browser.

Which action would solve this problem?

A. Modify the security policy.
B. Disable Web filtering.
C. Use destination NAT instead of static NAT.
D. Use DNS doctoring.

Answer: D

Explanation:

Reference :http://www.networker.co.in/2013/03/dns-doctoring.html

Question No : 12

You are troubleshooting an IPsec session and see the following IPsec security associations:

ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys

< 192.168.224.1 500 ESP:aes-256/sha1 d6393645 26/ unlim - 0

> 192.168.224.1 500 ESP:aes-256/sha1 153ec235 26/ unlim - 0

< 192.168.224.1 500 ESP:aes-256/sha1 f9a2db9a 3011/ unlim - 0

> 192.168.224.1 500 ESP:aes-256/sha1 153ec236 3011/ unlim - 0

What are two reasons for this behavior? (Choose two.)

A. Both peers are trying to establish IKE Phase 1 but are not successful.
B. Both peers have established SAs with one another, resulting in two IPsec tunnels.
C. The lifetime of the Phase 2 negotiation is close to expiration.
D. Both peers have establish-tunnels immediately configured.

Answer: C,D

Reference: http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swcmdref/show-security-ipsec-security-associations.html