Juniper

Exam JN0-633

Security, Professional (JNCIP-SEC)

Verson: Demo

[Total Questions: 10]

Question No : 1

Your company's network has seen an increase in Facebook-related traffic. You have been asked to restrict the amount of Facebook-related traffic to less than 100 Mbps regardless of congestion.

What are three components used to accomplish this task? (Choose three.)

A. IDP policy
B. application traffic control
C. application firewall
D. security policy
E. application signature

Answer: B,D,E

Explanation:

An IDP policy defines how your device handles the network traffic. It will not limit the rate.
Reference: http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/idp-policy-overview-section.html)

Application Firewall enforces protocol and policy control at Layer 7. It inspects the actual content of the payload and ensures that it conforms to the policy, rather than limiting the rate.

Reference:
http://www.juniper.net/techpubs/en_US/junos12.1x44/topics/concept/application-firewall-overview.html

Question No : 2

-- Exhibit --

[edit]

user@srx# run show route

inet.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)

+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 01:09:08

> to 172.18.1.1 via ge-0/0/3.0

10.210.14.128/27 *[Direct/0] 8w6d 15:43:09

> via ge-0/0/0.0

10.210.14.135/32 *[Local/0] 11w0d 06:43:04

Local via ge-0/0/0.0

172.18.1.0/30 *[Direct/0] 8w6d 15:43:01

> via ge-0/0/3.0

172.18.1.2/32 *[Local/0] 11w0d 06:43:03

Local via ge-0/0/3.0

172.19.1.0/24 *[Direct/0] 03:46:56

> via ge-0/0/1.0

172.19.1.1/32 *[Local/0] 03:46:56

Local via ge-0/0/1.0

172.20.105.0/24 *[Direct/0] 03:46:56

> via ge-0/0/4.105

172.20.105.1/32 *[Local/0] 03:46:56

Local via ge-0/0/4.105

192.168.30.1/32 *[Direct/0] 4d 03:44:41

> via lo0.0

fbf.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 00:00:11

> to 172.19.1.2 via ge-0/0/1.0

172.19.1.0/24 *[Direct/0] 00:00:11

> via ge-0/0/1.0

```
[edit]
user@srx# show routing-instances
fbf {
routing-options {
static {
route 0.0.0.0/0 next-hop 172.19.1.2;
}
}
}

[edit]
user@srx# show routing-options
interface-routes {
rib-group inet fbf-int;
}
static {
route 0.0.0.0/0 next-hop 172.18.1.1;
}
rib-groups {
fbf-int {
import-rib [ inet.0 fbf.inet.0 ];
import-policy fbf-pol;
}
}

[edit]
user@srx# show policy-options policy-statement fbf-pol
```

term 1 {

from interface ge-0/0/1.0;

to rib fbf.inet.0;

then accept;

}

term 2 {

then reject;

}

-- Exhibit --

Referring to the exhibit, you notice that filter-based forwarding is not working.

What is the reason for this behavior?

A. The RIB group is configured incorrectly.
B. The routing policy is configured incorrectly.
C. The routing instance is configured incorrectly.
D. The default static routes are configured incorrectly.

Answer: C

Explanation:

By default, we have a static route in a routing instance sending the default route to 172.19.1.2. We want to hijack traffic matching a particular filter and send the traffic to a different next-hop, 172.18.1.1. Weshould create your rib group by importing FIRST the table belonging to your virtual router and SECOND the table for the forwarding instance that has the next-hop specified.

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

Question No : 3

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:

Reference :
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 No : 4

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

Question No : 5

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: B,D

Reference: 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 employed to 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 permitted on network (http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/enable-idp-security-policy-section.html)

Question No : 6

You are deploying a standalone SRX650 in transparent mode for evaluation purposes in a potential client's network. The client will need to access the device to modify security policies and perform other various configurations. Where would you configure a Layer 3 interface to meet this requirement?

A. fxp0.0
B. vlan.1

C. irb.1
D. ge-0/0/0.0

Answer: C
Reference: http://safetynet.trapezenetworks.com/techpubs/en_US/junos12.1/information-products/topic-collections/security/software-all/layer-2/index.html?topic-52755.html

Question No : 7

Two companies, A and B, are connected as separate customers on an SRX5800 residing on two virtual routers (VR-A and VR-B). These companies have recently been merged and now operate under a common IT security policy. You have been asked to facilitate communication between these VRs. Which two methods will accomplish this task? (Choose two.)

A. Use instance-import to share the routes between the two VRs.
B. Create logical tunnel interfaces to interconnect the two VRs.
C. Use a physical connection between VR-A and VR-B to interconnect them.
D. Create a static route using the next-table action in both VRs.

Answer: A,D
Explanation:
Logical or physical connections between instances on the same Junos device and route between the connected instances
Reference : http://kb.juniper.net/InfoCenter/index?page=content&id=KB21260

Question No : 8

Click the Exhibit button.

{primarynode0}[edit security idp idp-policy test-ips-policy]

user@host# show

rulebase-ips {

rule r1 {

```
match {
source-address any;
attacks {
predefined-attack-groups “HTTP - All”;
}
}
then {
action {
drop-packet;
}
}
terminal;
}
rule r2 {
match {
source-address 172.16.0.0/12;
attacks {
predefined-attack-groups “FTP - All”;
}
then {
action {
no-action;
}
}
}
rule r3 {
```

```
match {
source-address 172.16.0.0/12;
attacks {
predefined-attack-groups “TELNET - All”;
}
}
then {
action {
no-action;
 }
}
}
rule r4 {
match {
source-address any;
attacks {
predefined-attack-groups “FTP - All”;
}
}
then {
action {
drop-packet;
}
}
}
}
```

A user with IP address 172.301.100 initiates an FTP session to a host with IP address 10.100.1.50 through an SRX Series device and is subject to the IPS policy shown in the exhibit.

If the user tries to execute the cd ~root command, which statement is correct?

A. The FTP command will be denied with the offending packet dropped and the session will be closed by the SRX device.
B. The FTP command will be denied with the offending packet dropped and the rest of the FTP session will be inspected by the IPS policy.
C. The FTP command will be allowed to execute and the rest of the FTP session will be ignored by the IPS policy.
D. The FTP command will be allowed to execute but any other attacks executed during the session will be inspected.

Answer: D

Question No : 9

Your management has a specific set of Web-based applications that certain employees are allowed to use.

Which two SRX Series device features would be used to accomplish this task? (Choose two.)

A. UserFW
B. IDP
C. AppFW
D. firewall filter

Answer: C

Question No : 10

Click the Exhibit button.

-- Exhibit –

```
[edit security application-firewall]
user@srx# show
rule-sets office-rules {
    rule FB {
        match {
            dynamic-application junos:FACEBOOK-ACCESS;
        }
        then {
            deny;
        }
    }
    rule web {
        match {
            dynamic-application-group junos:web;
        }
        then {
            permit;
        }
    }
    default-rule {
        permit;
    }
}
```

-- Exhibit --

Referring to the exhibit, the application firewall configuration fails to commit.

What must you do to allow the configuration to commit?

A. Each firewall rule set must only have one rule.
B. A firewall rule set cannot mix dynamic applications and dynamic application groups.
C. The action in the rules must be different than the action in the default rule.
D. The action in the default rule must be set to deny.

Answer: C

Reference: http://www.juniper.net/techpubs/en_US/junos12.1/topics/concept/application-firewall-overview.html