Leads4Pass

JN0-633^{Q&As}

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-633 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/jn0-633.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Click the Exhibit button.

Based on the output shown in the exhibit, what are two results? (Choose two.)

Exhibit:

```
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, Bytes: 176
   Out: 192.168.10.100/80 --> 192.168.1.10/60246;tcp, If: ge-0/0/9.0, Pkts: 2, Bytes: 120
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.

Correct Answer: BD

QUESTION 2

-- Exhibit -user@srx> show security flow session Session ID. 7724, Policy namE. default-permit/4, Timeout: 2

 In: 1.1.70.6/17 --> 100.0.0.1/2326;icmp, IF. ge-0/0/3

 Out: 10.1.10.5/2326 --> 1.1.70.6/17;icmp, IF. ge-0/0/2

Session ID. 18408, Policy namE. default-permit/4, Timeout: 2 In: 10.1.10.5/64513 --> 1.1.70.6/512;icmp, IF. ge-0/0/2.0 Out: 1.1.70.6/512 --> 100.0.0.1/64513;icmp, IF. ge-0/0/3.10

-- Exhibit -

A user has reported a traffic drop issue between a host with the 10.1.10.5 internal IP address and a host with the 1.1.70.6 IP address. The traffic transits an SRX240 acting as a NAT translator. You are investigating the issue on the SRX240 using the output shown in the exhibit. Regarding this scenario, which two statements are true? (Choose two.)

A. The sessions shown indicate interface-based NAT processing.

B. The sessions shown indicate static NAT processing.

C. ICMP traffic is passing in both directions.

D. ICMP traffic is passing in one direction.

Correct Answer: BC

QUESTION 3

What is a benefit of using a group VPN?

A. It provides a layer of redundancy on top of a point-to-point VPN mesh architecture.

B. It eliminates the need for point-to-point VPN tunnels.

C. It provides a way to grant VPN access on a per-user-group basis.

D. It simplifies IPsec access for remote clients.

Correct Answer: B

QUESTION 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

Correct Answer: ABC

QUESTION 5

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

Correct Answer: A

QUESTION 6

Your company is providing multi-tenant security services on an SRX5800 cluster. You have been asked to

create a new logical system (LSYS) for a customer. The customer must be able to access and manage

new resources within their LSYS.

How do you accomplish this goal?

A. Create the new LSYS, allocate resources, and then create the user administrator role so that the customer can manage their allocated resources.

B. Create the new LSYS, and then create the user administrator role so that the customer can allocate and manage resources.

C. Create the new LSYS, and then create the master adminstrator role for the LSYS so that the customer can allocate and manage resources.

D. Create the new LSYS, then request the required resources from the customer, and create the required resources.

Correct Answer: A

QUESTION 7

Click the Exhibit button.

You have been asked to block YouTube video streaming for internal users. You have implemented the

configuration shown in the exhibit, however users are still able to stream videos.

What must be modified to correct the problem?

Exhibit:

```
user@srx# show
application-firewall {
    rule-sets employee-productivity {
        rule block-youtube-videos {
            match {
                dynamic-application junos:YOUTUBE-STREAM;
            }
            then {
                deny;
            }
        }
        default-rule {
            permit;
        }
    }
}
policies {
    from-zone office to-zone Internet {
        policy application-services-office {
            match {
                source-address any;
                destination-address any;
                application [ junos-ftp junos-http junos-smtp junos-pop3 junos-imap ];
            }
            then {
                permit;
            }
        }
    }
}
...
```

A. The application firewall rule needs to be applied to an IDP policy.

B. You must create a custom application to block YouTube streaming.

C. The application firewall rule needs to be applied to the security policy.

D. You must apply the dynamic application to the security policy

Correct Answer: C

QUESTION 8

Click the Exhibit button.

In the exhibit, the SRX device has hosts connected to interface ge-0/0/1 and ge-0/0/6. The devices are not able to ping each other. What is causing this behavior?

Exhibit:

```
[edit]
user@srx# show interfaces
qe-0/0/1 {
    unit 0 {
        family bridge {
            interface-mode access;
            vlan-id 20;
        }
    }
}
ge-0/0/6 {
    unit 0 {
        family bridge {
            interface-mode access;
            vlan-id 20;
        }
    }
}

[edit]
user@srx# show security
policies {
    default-policy {
        permit-all;
    }
}
zones {
    security-zone L2 {
        interfaces {
            ge-0/0/6.0;
            ge-0/0/1.0;
        }
    }
}
```

A. The interfaces must be in trunk mode.

B. The interfaces need to be configured for Ethernet switching.

C. The default security policy does not apply to transparent mode.

D. A bridge domain has not been defined.

Correct Answer: D

QUESTION 9

You want to route traffic between two newly created virtual routers without the use of logical systems using the

configuration options on the SRX5800.

Which two methods of forwarding, between virtual routers, would you recommend? (Choose two.)

A. Use a static route to forward traffic across virtual routers using the next-table option. Enable the return route by using a RIB group. next-table command.

B. Create static routes in each virtual router using the

C. Use a RIB group to share the internal routing protocol routes from the master routing instance.

D. Connect a direct cable between boo physical interfaces, one in each virtual router and use next-hop command. static routes with the

Correct Answer: BD

QUESTION 10

You want to query User Group membership directly using the integrated user firewall services from an Active Directory controller to an SRX Series device.

Which two actions are required? (Choose two.)

A. Configure the LDAP base distinguished name.

B. Connect the SRX Series device and the MAG Series device in an enforcer configuration.

C. Configure a domain name, the username and password of the domain, and the name and IP address of the domain controller in the domain.

D. Configure the Access Control Service on the MAG Series device for local user authentication and verify that authentication information is transferred between the devices.
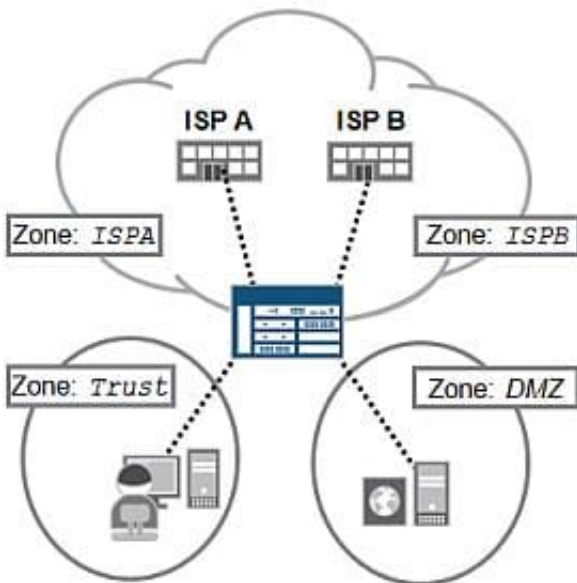
Correct Answer: AC

QUESTION 11

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?

Exhibit:

A. source NAT

B. static NAT

C. filter-based forwarding

D. source-based routing

Correct Answer: C

QUESTION 12

Which statement is true about Layer 2 zones when implementing transparent mode security?

A. All interfaces in the zone must be configured with the protocol family mpls.

B. All interfaces in the zone must be configured with the protocol family inet.

C. All interfaces in the zone must be configured with the protocol family bridge.

D. All interfaces in the zone must be configured with the protocol family inet6.

Correct Answer: C

QUESTION 13

user@host> show interfaces routing-instance all ge* terse Interface Admin Link Proto Local Instance ge-0/0/0.0 up up inet 172.16.12.205/24 default ge-0/0/1.0 up up inet 5.0.0.5/24

 iso A ge-0/0/2.0 up up inet 25.0.0.5/24 iso B

user@host> show security flow session

Session ID: 82274, Policy name: default-policy-00/2, Timeout: 1770, Valid In: 5.0.0.25/61935 --> 25.0.0.25/23;tcp, If: ge-0/0/1.0, Pkts: 31, Bytes: 1781 Out: 25.0.0.25/23 --> 5.0.0.25/61935;tcp, If: ge-0/0/2.0, Pkts: 23, Bytes: 1452

Total sessions: 3

user@host> show route

inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

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

0.0.0.0/0 *[Static/5] 04:08:52 > to 172.16.12.1 via ge-0/0/0.0 172.16.12.0/24 *[Direct/0] 04:08:52 via ge-0/0/0.0 172.16.12.205/32 *[Local/0] 4w4d 23:04:29 Loca1 via ge-0/0/0.0 224.0.0.5/32 *[OSPF/10] 14:37:35, metric 1 MultiRecv

A.inet.0: 4 destinations, 4 routes {4 active, 0 holddown, 0 hidden)

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

5.0.0.0/24 5 *[Direct/0] 00:05:04 > via ge-0/0/1.0 5.0.0.5/32 *[Local/0] 00:05:04 Local via ge-0/0/1.0 25.0.0.0/24 *[Direct/0] 00:02:37 > via ge-0/0/2.0

B.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

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

5.0.0.25/32 *[Static/5] 00:02:38 to table A.inet.0 25.0.0.0/24 *[Direct/0] 00:02:37 > via ge-0/0/2.0 25.0.0.5/32 *[Local/0] 00:02:37 Local via ge-0/0/2.0

A. The routing instances A and B are connected using an lt interface.

B. Routing instance A\\'s routes are shared with routing instance B.

C. Routing instance B\\'s routes are shared with routing instance A.

D. The routing instances A and B are connected using a vt interface.

Correct Answer: C

QUESTION 14

-- Exhibit -[edit forwarding-options] user@srx240# show packet-capture {

 file filename my-packet-capture;

 maximum-capture-size 1500; } -- Exhibit -

Referring to the exhibit, you are attempting to perform a packet capture on an SRX240 to troubleshoot an SSH issue in your network. However, no information appears in the packet capture file.

Which firewall filter must you apply to the necessary interface to collect data for the packet capture?

A. user@srx240# show filter pkt-capture { term pkt-capture-term {

 from {

```
protocol tcp;

port ssh;

}

then packet-mode;

}

term allow-all {

then accept;

}

}
```

[edit firewall family inet]

B. user@srx240# show filter pkt-capture { term pkt-capture-term {

```
from {

protocol tcp;

port ssh;

}

then {

count packet-capture;

}

}

term allow-all {

then accept;

}

}
```

[edit firewall family inet]

C. user@srx240# show filter pkt-capture { term pkt-capture-term {

```
from {

protocol tcp;

port ssh;

}
```

then {

routing-instance packet-capture;

}

}

term allow-all {

then accept;

}

}

[edit firewall family inet]

D. user@srx240# show

filter pkt-capture {

term pkt-capture-term {

from {

protocol tcp;

port ssh;

}

then {

sample;

accept;

}

}

term allow-all {

then accept;

}

}

[edit firewall family inet]

Correct Answer: D

QUESTION 15

What are three advantages of group VPNs? (Choose three.)

A. Supports any-to-any member connectivity.

B. Provides redundancy with cooperative key servers.

C. Eliminates the need for full mesh VPNs.

D. Supports translating private to public IP addresses.

E. Preserves original IP source and destination addresses.

Correct Answer: ACE

JN0-633 Practice Test   JN0-633 Study Guide   JN0-633 Exam Questions