JN0-333$^{Q\&As}$

Security, Specialist (JNCIS-SEC)

Pass Juniper JN0-333 Exam with 100% Guarantee

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

https://www.certbus.com/jn0-333.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

Which process describes the implementation of screen options on an SRX Series device?

A. Configured screen options are only applied when traffic does not match a valid route.

B. Configured screen options are applied only to the first packet that is processed in a stateful session.

C. Configured screen options are applied to all packets that are processed by the stateful session firewall processor.

D. Configured screen options are only applied when traffic does not match a valid policy.

Correct Answer: C

QUESTION 2

Click the Exhibit button.

```
[edit security policies from-zone trust to-zone untrust]
user@host# show
policy custom-ftp {
    match {
        source-address 172.25.11.0/24;
        destination-address any;
        application custom-ftp;
    }
    then {
        permit;
    }
}

[edit]
user@host# show applications
application custom-ftp destination-port 2121;
```

Users at a remote office are unable to access an FTP server located at the remote corporate data center as expected. The remote FTP server is listening on the non-standard TCP port 2121.

Referring to the exhibit, what is causing the problem?

A. The FTP clients must be configured to listen on non-standard client ports for the FTP data channel negotiations to succeed.

B. Two custom FTP applications must be defined to allow bidirectional FTP communication through the SRX Series device.

C. The custom FTP application definition does not have the FTP ALG enabled.

D. A new security policy must be defined between the untrust and trust zones.

Correct Answer: D

QUESTION 3

Which two statements are true about global security policies? (Choose two.)

A. Global security policies are evaluated before regular security policies.

B. Global security policies can be configured to match addresses across multiple zones.

C. Global security policies can match traffic regardless of security zones.

D. Global security policies do not support IPv6 traffic.

Correct Answer: BC

QUESTION 4

What is the function of redundancy group 0 in a chassis cluster?

A. Redundancy group 0 identifies the node controlling the cluster management interface IP addresses.

B. The primary node for redundancy group 0 identifies the first member node in a chassis cluster.

C. The primary node for redundancy group 0 determines the interface naming for all chassis cluster nodes.

D. The node on which redundancy group 0 is primary determines which Routing Engine is active in the cluster.

Correct Answer: D

QUESTION 5

Which type of VPN provides a secure method of transporting encrypted IP traffic?

A. IPsec

B. Layer 3 VPN

C. VPLS

D. Layer 2 VPN

Correct Answer: A

QUESTION 6

What are two fields that an SRX Series device examines to determine if a packet is associated with an existing flow? (Choose two.)

A. protocol

B. source IP address

C. source MAC address

D. type of service

Correct Answer: AB

QUESTION 7

A link from the branch SRX Series device chassis cluster to the Internet requires more bandwidth. In this scenario, which command would you issue to begin provisioning a second link?

A. set chassis cluster reth-count 2

B. set interfaces fab0 fabric-options member-interfaces ge-0/0/1

C. set interfaces ge-0/0/1 gigether-options redundant-parent reth1

D. set chassis cluster redundancy-group 1 node 1 priority 1

Correct Answer: B

QUESTION 8

Click the Exhibit button.

```
user@host> show security ike security-associations

user@host> show route 172.16.1.2

inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.0/24          *[Static/5] 00:04:21
                       > via st0.0

user@host> ping 172.16.1.2 source 172.16.1.1
PING 172.16.1.2 (172.16.1.2): 56 data bytes
64 bytes from 172.16.1.2: icmp_seq=0 ttl=64 time=3.428 ms
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=1.367 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=1.911 ms
```

You have an IPsec tunnel between two devices. You clear the IKE security associations, but traffic continues to flow across the tunnel.

Referring to the exhibit, which statement is correct in this scenario?

A. The IPsec security association is independent from the IKE security association

B. The traffic is no longer encrypted

C. The IKE security association immediately reestablishes

D. The traffic is using an alternate path

Correct Answer: AB

QUESTION 9

Click the Exhibit button.

You are configuring an OSPF session between two SRX Series devices. The session will not come up.

Referring to the exhibit, which configuration change will solve this problem?

```
[edit]
user@host# show security policies from-zone trust to-zone trust
policy allow-trusted-traffic {
    match {
      source-address any;
      destination-address any;
      application [ junos-http junos-https ];
    }
      then {
        permit;
      }
    }
}
[edit]
user@host# show security zone security-zone trust
host-inbound-traffic {
      system-services {
        all;
      }
    }
}
Interfaces {
    ge-0/0/0.0
    ge-0/0/1.0;
}
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.0.1.11/24
      }
    }
}
[edit]
user@host# run show ospf neighbor
Address           Interface       State      ID             Pri      Dead
10.0.2.1          ge-0/0/1.0      ExStart    10.0.1.112     128      38
```

A. Configure a loopback interface and add it to the trust zone.

B. Configure the host-inbound-traffic protocols ospf parameter in the trust security zone.

C. Configure the application junos-ospf parameter in the allow-trusted-traffic security policy.

D. Configure the host-inbound-traffic system-services any-service parameter in the trust security zone.

Correct Answer: A

QUESTION 10

Click the Exhibit button.

```
user#host> show interface ge-0/0/1 extensive | find Zone
      Security: Zone: host
      Allowed host-inbound traffic: any-service bfd bgp dvmrp icmp ldp msdp nhrp
      ospf pgm pim rip router-discovery rsvp sap vrrp
      Flow Statistics:
      Flow Input statistics:
            Self packets:                       0
            ICMP packets:                       0
            VPN packets:                        0
            Multicast packets:                  0
            Bytes permitted by policy:          0
            Connections established:            0
      Flow Output statistics:
            Multicast packets:                  0
            Bytes permitted by policy:          0
      Flow error statistics (Packets dropped due to):
            Address spoofing:                   0
            Authentication failed:              0
            Incoming NAT errors:                0
            Invalid zone received packet:       0
            Multiple user authentications:      0
            Multiple incoming NAT:              0
            No parent for a gate:               0
            No one interested in self packets: 0
            No minor session:                   0
            No more sessions:                   0
            No NAT gate:                        0
            No route present:                   135
            No SA for incoming SPI:             0
            No tunnel found:                    0
            No session for a gate:              0
            No zone or NULL zone binding        0
            Policy denied:                      0
            Security associated not active:     0
            TCP sequence number out of window: 0
            Syn-attack protection:              0
            User authentication errors:         0
      Protocol inet, MTU: 1500, Generation: 162, Route table: 0
            Flags: Sendbcast-pkt-to-re
            Addresses, Flags: Is-Preferred Is-Primary
                  Destination: 5.0.0/24, Local: 5.0.0.5, Broadcast: 5.0.0.255,
                  Generation: 158
      Protocol iso, MTU: 1497, Generation: 163, Route table: 0
            Flags: Is-Primary
```

Referring to the exhibit, which statement is true?

A. TCP packets entering the interface are failing the TCP sequence check.

B. Packets entering the interface are being dropped due to a stateless filter.

C. Packets entering the interface are getting dropped because there is no route to the destination.

D. Packets entering the interface matching an ALG are getting dropped.

Correct Answer: C

QUESTION 11

What are the maximum number of supported interfaces on a vSRX hosted in a VMware environment?

A. 12

B. 3

C. 10

D. 4

Correct Answer: A

QUESTION 12

In a chassis cluster, which two characteristics are true regarding reth interfaces? (Choose two.)

A. A reth interface inherits its failover properties from a redundancy group.

B. Reth interfaces must be the same type of interface.

C. Reth interfaces must be in the same slots on each node.

D. A reth interface goes down if one of its child interfaces become unavailable.

Correct Answer: AB

QUESTION 13

Which action will restrict SSH access to an SRX Series device from a specific IP address which is connected to a security zone named trust?

A. Implement a firewall filter on the security zone trust.

B. Implement a security policy from security zone junos-host to security zone trust.

C. Implement host-inbound-traffic system-services to allow SSH.

D. Implement a security policy from security zone trust to security zone junos-host.

Correct Answer: D

QUESTION 14

Which two modes are supported during the Phase 1 IKE negotiations used to establish an IPsec tunnel? (Choose two.)

A. transport mode

B. aggressive mode

C. main mode

D. tunnel mode

Correct Answer: BC

QUESTION 15

Click the Exhibit button.

```
[edit]
user@host# show security address-book
global {
    address dmz-net 192.168.150.0/24;
    address dns-svrs {
        range-address 192.168.150.100 {
            to {
                192.168.150.115;
            }
        }
    }
    address client-net 172.16.123.0/24;
}

[edit security policies from-zone trust to-zone dmz]
user@host# show
policy p1 {
    match {
        source-address client-net;
        destination-address dns-svrs;
        destination-address-excluded;
        application [ junos-http junos-https ];
    }
    then {
        permit;
    }
}
policy p2 {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

Referring to the exhibit, what will happen if client 172.16.128.50 tries to connect to destination

192.168.150.111 using HTTP?

A. The client will be denied by policy p2.

B. The client will be denied by policy p1.

C. The client will be permitted by policy p2.

D. The client will be permitted by policy p1.

Correct Answer: D

[Latest JN0-333 Dumps](#)   [JN0-333 PDF Dumps](#)   [JN0-333 Braindumps](#)