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.passapply.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

You have recently configured an IPsec tunnel between two SRX Series devices. One of the devices is assigned an IP address using DHCP with an IP address that changes frequently. Initial testing indicates that the IPsec tunnel is not working. Troubleshooting has revealed that Phase 1 negotiations are failing.

Which two actions would solve the problem? (Choose two.)

A. Verify that the device with the IP address assigned by DHCP is the traffic initiator.

B. Verify that VPN monitoring is enabled.

C. Verify that the IKE policy is configured for aggressive mode.

D. Verify that PKI is properly configured.

Correct Answer: AC

QUESTION 2

Clients at a remote office are accessing a website that is against your company Internet policy. You change the action of the security policy that controls HTTP access from permit to deny on the remote office SRX Series device. After committing the policy change, you notice that new users cannot access the website but users that have existing sessions on the device still have access. You want to block all user sessions immediately.

Which change would you make on the SRX Series device to accomplish this task?

A. Add the set security flow tcp-session rst-invalidate-session option to the configuration and commit the change.

B. Add the set security policies policy-rematch parameter to the configuration and commit the change.

C. Add the security flow tcp-session strict-syn-check option to the configuration and commit the change.

D. Issue the commit full command from the top of the configuration hierarchy.

Correct Answer: B

QUESTION 3

Which host-inbound-traffic security zone parameter would allow access to the REST API configured to listen on custom TCP port 5080?

A. http

B. all

C. xnm-clear-text

D. any-service

Correct Answer: D

QUESTION 4

You recently configured an IPsec VPN between two SRX Series devices. You notice that the Phase1 negotiation succeeds and the Phase 2 negotiation fails.

Which two configuration parameters should you verify are correct? (Choose two.)

A. Verify that the IKE gateway proposals on the initiator and responder are the same.

B. Verify that the VPN tunnel configuration references the correct IKE gateway.

C. Verify that the IKE initiator is configured for main mode.

D. Verify that the IPsec policy references the correct IKE proposals.

Correct Answer: AB

QUESTION 5

A session token on an SRX Series device is derived from what information? (Choose two.)

A. routing instance

B. zone

C. screen

D. MAC address

Correct Answer: AB

QUESTION 6

You want to trigger failover of redundancy group 1 currently running on node 0 and make node 1 the primary node the redundancy group 1.

Which command would be used accomplish this task?

A. user@host# set chassis cluster redundancy-group 1 node 1

B. user@host> request chassis cluster failover redundancy-group 1 node 1

C. user@host# set chassis cluster redundancy-group 1 preempt

D. user@host> request chassis cluster failover reset redundancy-group 1

Correct Answer: B

QUESTION 7

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 pclicies 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 zcne 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 8

Click the Exhibit button.

```
user@host# show security
address-book {
     global {
          address inside-server 10.0.2.1/32;
          address inside-dns-server 10.100.75.75/32;
     }
}
nat {
     source {
          rule-set outbound-nat {
               from zone trust;
               to zone untrust;
               rule translate {
                    match {
                         source-address 0.0.0.0/0;
                    }
                    then  {
                         source-nat {
                              interface;
                         }
                    }
               }
          }
     }
     static {
          rule-set static-nat {
               from zone trust;
               rule static-translation {
                    match {
                         destination-address 10.100.75.75/32;
                    }
                    then {
                         static-nat {
                              prefix {
                                   75.75.76.76/32;
                              }
                         }
                    }
               }
          }
     }
}
policies {
     from-zone trust to-zone untrust {
          policy allow-server {
               match {
                    source-address inside-server;
                    destination-address inside-dns-server;
                    application any;
               }
               then {
                    permit;
               }
          }
     }
}
```

The inside server must communicate with the external DNS server. The internal DNS server address is

10.100.75.75. The external DNS server address is 75.75.76.76. Traffic from the inside server to the DNS server fails.

Referring to the exhibit, what is causing the problem?

A. The security policy must match the translated destination address.

B. Source and static NAT cannot be configured at the same time.

C. The static NAT rule must use the global address book entry name for the DNS server.

D. The security policy must match the translated source and translated destination address.

Correct Answer: A

QUESTION 9

Which statement is true about Perfect Forward Secrecy (PFS)?

A. PFS is used to resolve compatibility issues with third-party IPsec peers.

B. PFS is implemented during Phase 1 of IKE negotiations and decreases the amount of time required for IKE negotiations to complete.

C. PFS increases security by forcing the peers to perform a second DH exchange during Phase 2.

D. PFS increases the IPsec VPN encryption key length and uses RSA or DSA certificates.

Correct Answer: C

QUESTION 10

Click to the Exhibit button.

Referring to the exhibit, which two statements are true? (Choose two.)

```
[edit]
user@host# show security zones security zones security-zone
trust
host-inbound-traffic {
    system-services {
        all;
    }
}
interfaces {
    ge-0/0/0.0;
    ge-0/0/1.0 {
        host-inbound-traffic {
            system-services {
            ssh;
            }
        }
    }
}
```

A. Interface ge-0/0/0 will not accept SSH connections.

B. Interfaces ge-0/0/0.0 and ge-0/0/1.0 will allow SSH connections.

C. Interface ge-0/0/0.0 will respond to pings.

D. Interface ge-0/0/1.0 will respond to pings.

Correct Answer: BD

QUESTION 11

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 12

You want to ensure that any certificates used in your IPsec implementation do not expire while in use by your SRX Series devices.

In this scenario, what must be enabled on your devices?

A. RSA

B. TLS

C. SCEP

D. CRL

Correct Answer: C

QUESTION 13

Which feature is used when you want to permit traffic on an SRX Series device only at specific times?

A. scheduler

B. pass-through authentication

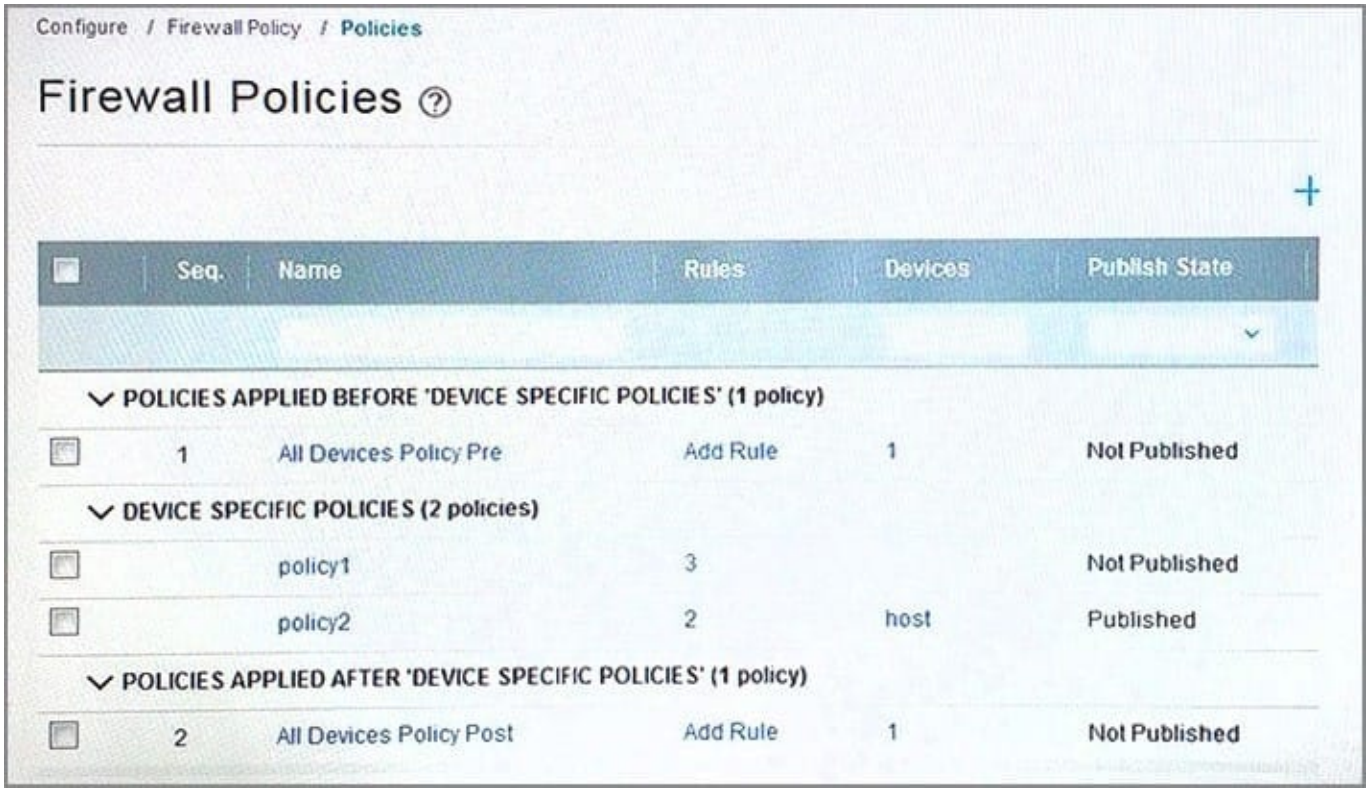
C. ALGs

D. counters

Correct Answer: A

QUESTION 14

Click the exhibit button.



You are configuring security policies with Junos Space Security Director. Referring to the exhibit, which two statements are true? (Choose two.)

A. The host device has three rules assigned to it.

B. The policy assigned to the host device is published.

C. The policy assigned to the host device requires publishing.

D. The host device has two rules assigned to it.

Correct Answer: BD

QUESTION 15

Which UDP port is used in Ipsec tunneling when NAT-T is in use?

A. 50

B. 4500

C. 500

D. 51

Correct Answer: B