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.geekcert.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

Click the Exhibit button.

```
[edit]
user@host# show security address-book
global {
    address dmz-net 192.168.150.0/24;
    address client-net 172.16.128.0/24;
    address web-servers 192.168.150.0/29;
}

[edit security policies]
user@host# show
from-zone trust to-zone dmz {
    policy p1 {
        match {
            source-address client-net;
            destination-address dmz-net;
            application [ junos-http junos-https ];
        }
        then {
            permit;
        }
    }
    policy p2 {
        match {
            source-address client-net;
            destination-address web-servers;
            application [ junos-http junos-https ];
        }
        then {
            deny;
        }
    }
    policy p3 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}
global
    policy global-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
}
```

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

192.168.150.3 using HTTP?

A. The client will be denied by policy p2.

B. The client will be permitted by the global policy.

C. The client will be permitted by policy p1.

D. The client will be denied by policy p3.

Correct Answer: C

QUESTION 2

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 3

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 4

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 5

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

Latest JN0-333 Dumps   JN0-333 Exam Questions   JN0-333 Braindumps