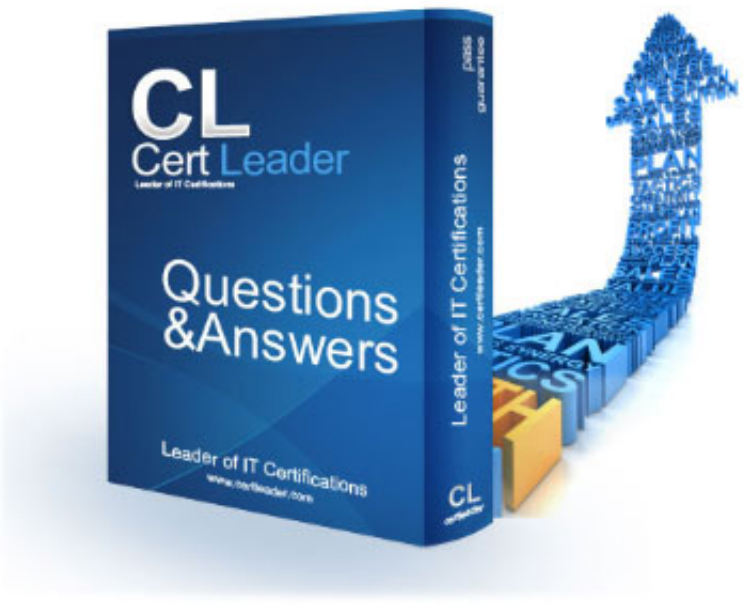
jn0-333 Dumps

Security, Specialist (JNCIS-SEC)

https://www.certleader.com/jn0-333-dumps.html



NEW QUESTION 1
Which three statements describes traditional firewalls? (Choose three.)

A. A traditional firewall performs stateless packet processing.
B. A traditional firewall offers encapsulation, authentication, and encryption.
C. A traditional firewall performs stateful packet processing.
D. A traditional firewall forwards all traffic by default.
E. A traditional firewall performs NAT and PAT.

Answer: BCE

NEW QUESTION 2
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

Answer: AB

NEW QUESTION 3
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 172.16.128.0/24;
}

[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.

Answer: D

NEW QUESTION 4
What are the maximum number of redundancy groups that would be used on a chassis cluster?

A. The maximum number of redundancy groups use is equal to the number of configured physical interfaces.
B. The maximum number of redundancy groups use is equal to one more than the number of configured physical interfaces.
C. The maximum number of redundancy groups use is equal to the number of configured logical interfaces.
D. The maximum number of redundancy groups use is equal to one more than the number of configured logical interfaces.

Answer: C

NEW QUESTION 5
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.

Answer: A

NEW QUESTION 6
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.

Answer: C

NEW QUESTION 7
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.

Answer: BD

NEW QUESTION 8
What are three defined zone types on an SRX Series device?

A. dynamic
B. junos-host
C. null
D. functional
E. routing

Answer: BCD

NEW QUESTION 9
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

Answer: B

NEW QUESTION 10
Which SRX5400 component is responsible for performing first pass security policy inspection?

A. Routing Engine
B. Switch Control Board
C. Services Processing Unit
D. Modular Port Concentrator

Answer: C

NEW QUESTION 10
What are the maximum number of supported interfaces on a vSRX hosted in a VMware environment?

A. 12
B. 3
C. 10
D. 4

Answer: A

NEW QUESTION 12
Which statement is true about functional zones?

A. Functional zones are a collection of regulated transit network segments.
B. Functional zones provide a means of distinguishing groups of hosts and their resources from one another.
C. Functional zones are used for management.
D. Functional zones are the building blocks for security policies.

Answer: C

NEW QUESTION 13
Which statement describes the function of NAT?

A. NAT encrypts transit traffic in a tunnel.
B. NAT detects various attacks on traffic entering a security device.
C. NAT translates a public address to a private address.
D. NAT restricts or permits users individually or in a group.

Answer: C

NEW QUESTION 18
Screens help prevent which three attack types? (Choose three.)

A. SYN flood
B. port scan
C. NTP amplification
D. ICMP fragmentation
E. SQL injection

Answer: ABD

NEW QUESTION 22
You must verify if destination NAT is actively being used by users connecting to an internal server from the Internet.
Which action will accomplish this task on an SRX Series device?

A. Examine the destination NAT translations table.
B. Examine the installed routes in the packet forwarding engine.
C. Examine the NAT translation table.
D. Examine the active security flow sessions.

Answer: A

NEW QUESTION 25
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

Answer: BC

NEW QUESTION 26
You recently configured an IPsec VPN between two SRX Series devices. You notice that the Phase 1 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 IPsec policy references the correct IKE proposals.
D. Verify that the IKE initiator is configured for main mode.

Answer: AC

NEW QUESTION 31

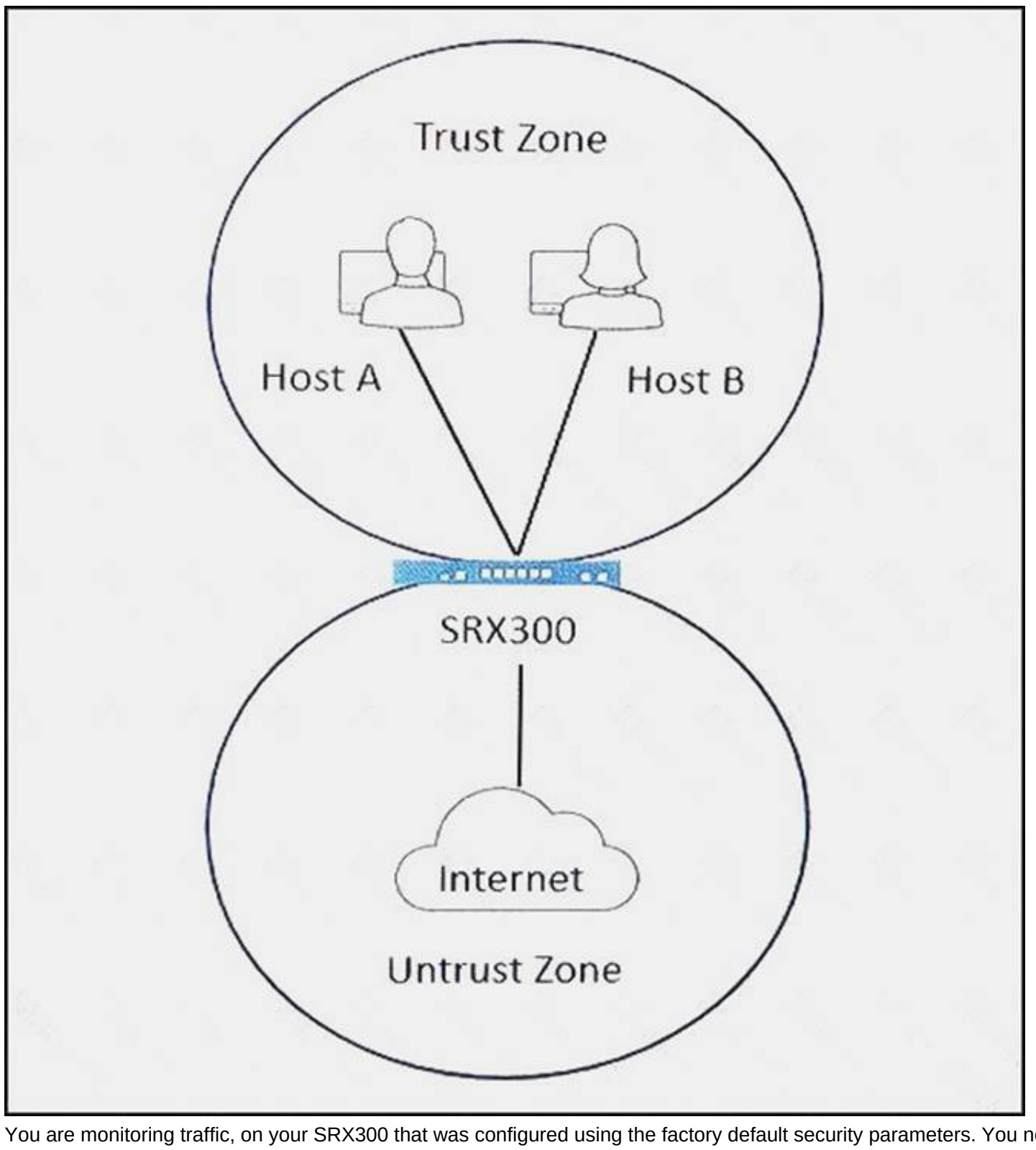
Click to the Exhibit button.
Referring to the exhibit, which two statements are true? (Choose two.)

```
[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.

Answer: BD

NEW QUESTION 34
Click the Exhibit button.



You are monitoring traffic, on your SRX300 that was configured using the factory default security parameters. You notice that the SRX300 is not blocking traffic between Host A and Host B as expected.
Referring to the exhibit, what is causing this issue?

A. Host B was not assigned to the Untrust zone.
B. You have not created address book entries for Host A and Host B.
C. The default policy has not been committed.
D. The default policy permits intrazone traffic within the Trust zone.

Answer: D

NEW QUESTION 38
What are two valid zones available on an SRX Series device? (Choose two.)

A. security zones
B. policy zones
C. transit zones
D. functional zones

Answer: AD

NEW QUESTION 41
Click the Exhibit button.

```
user@host> show security ike active-peer detail

Peer address: 31.0.0.6, Port: 500,
Peer IKE-ID: C=US, ST=California, L=Sunnyvale, O=Example, OU=sales, CN=SPOKE9061
XAUTH username: not available
Assigned network attributes:
IP Address: 0.0.0.0, netmask        : 0.0.0.0
DNS Address       : 0.0.0.0, DNS2 Address : 0.0.0.0
WINS Address      : 0.0.0.0, WINS2 Address : 0.0.0.0

Previous Peer address   : 0.0.0.0, Port   : 0
Active IKE SA indexes   : 75203629
IKE SA negotiated       : 1
IPsec tunnels active    : 1, IPSec Tunnel IDs   : 68157442

DPD Config Info  : Mode: always-send Interval: 60 Threshold: 5 plsa_index:75203629
DPD Statistics   : DPD-flags: REMOTE_ACCESS
DPD Statistics   : DPD TTL              :       0    DPD seq-no        :       0
DPD Statistics   : DPD Req Sent         :       0    DPD Resp Rcvd     :       0
```

A customer would like to monitor their VPN using dead peer detection.
Referring to the exhibit, for how many minutes was the peer down before the customer was notified?

A. 5
B. 3
C. 4
D. 2

Answer: A

NEW QUESTION 43
You need to configure an IPsec tunnel between a remote site and a hub site. The SRX Series device at the remote site receives a dynamic IP address on the external interface that you will use for IPsec.
Which feature would you need to configure in this scenario?

A. NAT-T
B. crypto suite B
C. aggressive mode
D. IKEv2

Answer: C

NEW QUESTION 45
Which statement is true about high availability (HA) chassis clusters for the SRX Series device?

A. Cluster nodes require an upgrade to HA compliant Routing Engines.
B. Cluster nodes must be connected through a Layer 2 switch.
C. There can be active/passive or active/active clusters.
D. HA clusters must use NAT to prevent overlapping subnets between the nodes.

Answer: C

NEW QUESTION 48
What is the correct ordering of Junos policy evaluation from first to last?

A. global policy > zone-based policy > default policy
B. default policy > zone-based policy > global policy
C. global policy > default policy > zone-based policy
D. zone-based policy > global policy > default policy

Answer: D

NEW QUESTION 52
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

Answer: AB

NEW QUESTION 55
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.

Answer: D

NEW QUESTION 59
You are asked to change when your SRX high availability failover occurs. One network interface is considered more important than others in the high availability configuration. You want to prioritize failover based on the state of that interface.
Which configuration would accomplish this task?

A. Create a VRRP group configuration that lists the reth's IP address as the VIP while using each physical interface that make up the reth definition of each SRX HA pair.
B. Configure IP monitoring of the important interface's IP address and adjust the heartbeat interval and heartbeat threshold to the shortest settings.
C. Create a separate redundancy group to isolate the important interface; set the priority of the new redundancy group to 255.
D. Configure interface monitor inside the redundancy group that contains the important physical interface; adjust the weight associated with the monitored interface to 255.

Answer: D

NEW QUESTION 63
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

Answer: AB

NEW QUESTION 66
Your internal webserver uses port 8088 for inbound connections. You want to allow external HTTP traffic to connect to the webserver.
Which two actions would accomplish this task? (Choose two.)

A. Create a custom application for port 8088 and create a security policy that permits the custom-http application.
B. Remap port 80 to port 8088 in the junos-http application and create a security policy that permits the junos-http application.
C. Use destination NAT to remap incoming traffic from port 80 to port 8088.
D. Create an Application Layer Gateway to permit HTTP traffic on port 8088.

Answer: AC

NEW QUESTION 68
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.

Answer: D

NEW QUESTION 69
What are three characteristics of session-based forwarding, compared to packet-based forwarding, on an SRX Series device? (Choose three.)

A. Session-based forwarding uses stateful packet processing.
B. Session-based forwarding requires less memory.
C. Session-based forwarding performs faster processing of existing session.
D. Session-based forwarding uses stateless packet processing,
E. Session-based forwarding uses six tuples of information.

Answer: ACE

NEW QUESTION 74
You are changing the default vCPU allocation on a vSRX. How are the additional vCPUs allocated in this scenario?

A. The vCPU are allocated equally across the Junos control plane and packet forwarding engine.
B. One dedicated vCPU is allocated for the Junos control plane and the remaining vCPUs for the packet forwarding engine.
C. One dedicated vCPU is allocated for the packet forwarding engine, one for the Junos control plane, and the remaining vCPUs are equally balanced.
D. One dedicated vCPU is allocated for the packet forwarding engine and the remaining vCPUs for the Junos plane.

Answer: B

NEW QUESTION 79
Click the Exhibit button.
You are trying to create a security policy on your SRX Series device that permits HTTP traffic from your private 172.25.11.0/24 subnet to the Internet. You create a policy named permit – http between the trust and untrust zones that permits HTTP traffic.
When you issue a commit command to apply the configuration changes, the commit fails with the error shown in the exhibit.
Which two actions would correct the error? (Choose two.)

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

[edit security policies from-zone trust to-zone untrust]
user@host# commit
[edit security policies from-zone trust to-zone untrust policy
permit-http match application]
'http'
      application or application-set must be defined
error: commit failed: (statements constraint check failed)
```

A. Create a custom application named http at the [edit applications] hierarchy.
B. Execute the Junos commit full command to override the error and apply the configuration.
C. Modify the security policy to use the built-in junos-http application.
D. Issue the rollback 1 command from the top of the configuration hierarchy and attempt the commit again.

Answer: BC

NEW QUESTION 80
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your jn0-333 Exam with Our Prep Materials Via below:

https://www.certleader.com/jn0-333-dumps.html