Juniper

Exam JN0-696

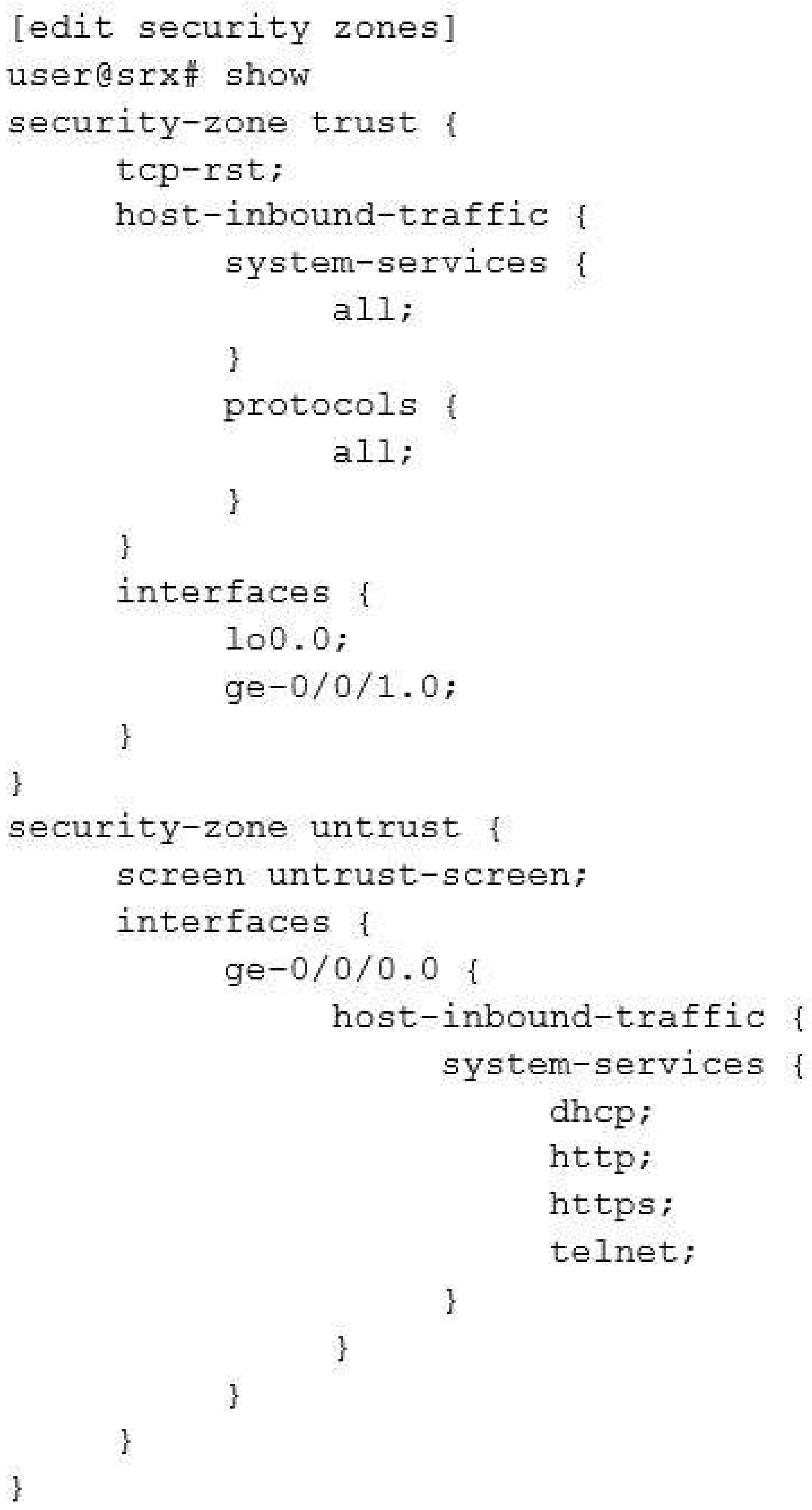
Security Support, Professional (JNCSP-SEC)

Version: 9.0

[Total Questions: 71]

Question No : 1

Click the Exhibit button.



```
[edit security zones]
user@srx# show
security-zone trust {
     tcp-rst;
     host-inbound-traffic {
          system-services {
               all;
          }
          protocols {
               all;
          }
     }
     interfaces {
          lo0.0;
          ge-0/0/1.0;
     }
}
security-zone untrust {
     screen untrust-screen;
     interfaces {
          ge-0/0/0.0 {
               host-inbound-traffic {
                    system-services {
                         dhcp;
                         http;
                         https;
                         telnet;
                    }
               }
          }
     }
}
```

A customer has a problem connecting to an SRX Series device from the untrust zone using SSH only.

Referring to the exhibit, which action will solve the problem?

A. Configure the ssh parameter under the [edit security zones security-zone trust interfaces ge-0/0/1.0 host inbound-traffic protocols] hierarchy.
B. Configure the ssh parameter under the [edit security zones security-zone untrust hostinbound-traffic system-services] hierarchy.
C. Configure the ssh parameter under the [edit security zones security-zone untrust hostinbound-traffic protocols] hierarchy.
D. Configure the ssh parameter under the [edit security zones security-zone trust hostinbound-traffic system-services] hierarchy.

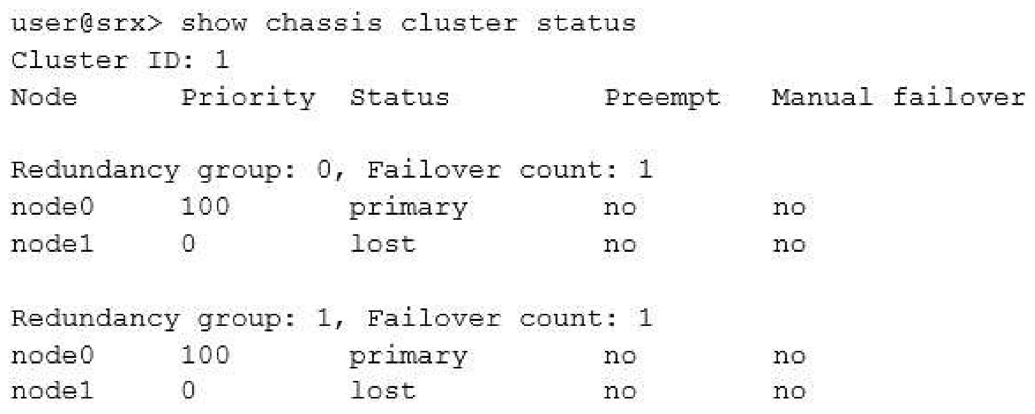
Answer: B

Explanation:

Assume that inbound ssh, ftp, and ping traffic should be permitted from the untrusted zone. Then you should do the following:
[edit security zones]
root# set security zone untrust host-inbound-traffic ssh root# set security zone untrust host-inbound-traffic ftp root# set security zone untrust host-inbound-traffic ping
Note: For SRX Series branch devices, a factory default security policy is provided that:
Allows all traffic from the trust zone to the untrust zone.
Allows all traffic between trusted zones, that is from the trust zone to intrazone trusted zones. Denies all traffic from the untrust zone to the trust zone.
References: http://www.dummies.com/how-to/content/how-to-configure-srx-security-zones-with-junos.html
http://www.juniper.net/documentation/en_US/junos12.3x48/topics/concept/security-srx-device-zone-and-policyunderstanding.html

Question No : 2

Click the Exhibit button.



```
user@srx> show chassis cluster status
Cluster ID: 1
Node       Priority  Status         Preempt   Manual failover

Redundancy group: 0, Failover count: 1
node0      100       primary        no        no
node1      0         lost           no        no

Redundancy group: 1, Failover count: 1
node0      100       primary        no        no
node1      0         lost           no        no
```

You recently configured a chassis cluster between two branch SRX Series devices and realize that the cluster is not functional, with node device status lost.

Referring to the exhibit, which two actions will correct this problem? (Choose two.)

A. Confirm both devices are synchronized with the local NTP.
B. Confirm that the software on both devices is the same Junos OS version.
C. Confirm both devices are running with the same security policies.
D. Confirm that the hardware on both devices is the same.

Answer: B,D

Explanation:

Chassis Cluster prerequisites include:

B: The SOFTWARE on both standalone devices must be the same Junos OS version.

Verify using this command on both devices:

root> show version

Model: srx220h

JUNOS Software Release [11.4R7.5]

D: Confirm that the HARDWARE on both devices is the same.

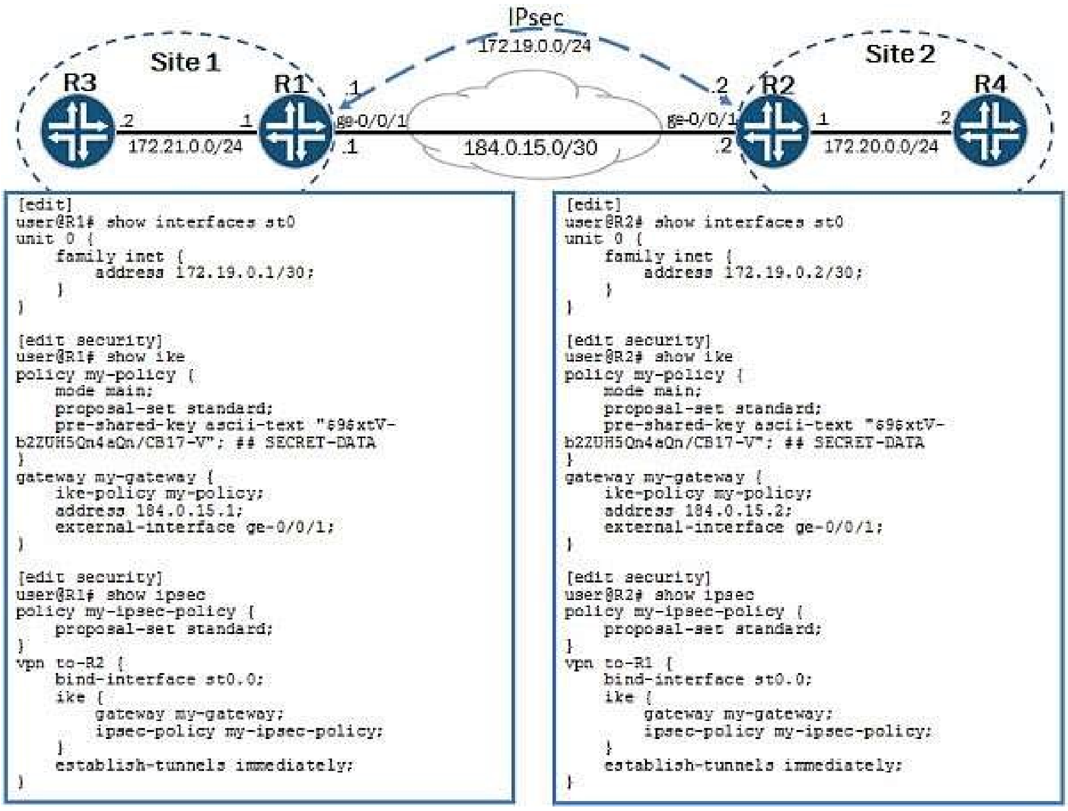
Verify using this command on both devices: root@srx220> show chassis hardware detail

References:

http://kb.juniper.net/InfoCenter/index?page=content&id=KB21312&actp=search

Question No : 3

-- Exhibit –



```
[edit]
user@R1# show interfaces st0
unit 0 {
    family inet {
        address 172.19.0.1/30;
    }
}

[edit security]
user@R1# show ike
policy my-policy {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$xtV-
b2ZUH5Qn4aQn/CB17-V"; ## SECRET-DATA
}
gateway my-gateway {
    ike-policy my-policy;
    address 184.0.15.1;
    external-interface ge-0/0/1;
}

[edit security]
user@R1# show ipsec
policy my-ipsec-policy {
    proposal-set standard;
}
vpn to-R2 {
    bind-interface st0.0;
    ike {
        gateway my-gateway;
        ipsec-policy my-ipsec-policy;
    }
    establish-tunnels immediately;
}
```

```
[edit]
user@R2# show interfaces st0
unit 0 {
    family inet {
        address 172.19.0.2/30;
    }
}

[edit security]
user@R2# show ike
policy my-policy {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$xtV-
b2ZUH5Qn4aQn/CB17-V"; ## SECRET-DATA
}
gateway my-gateway {
    ike-policy my-policy;
    address 184.0.15.2;
    external-interface ge-0/0/1;
}

[edit security]
user@R2# show ipsec
policy my-ipsec-policy {
    proposal-set standard;
}
vpn to-R1 {
    bind-interface st0.0;
    ike {
        gateway my-gateway;
        ipsec-policy my-ipsec-policy;
    }
    establish-tunnels immediately;
}
```

-- Exhibit --

Click the Exhibit button.

You are asked to troubleshoot a new IPsec VPN that is not establishing. You do not receive any output from the show security ike security-associations command.

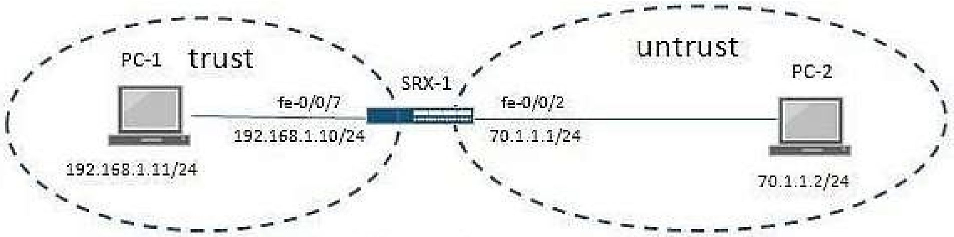
Referring to the exhibit, which section of the configuration is causing the problem?

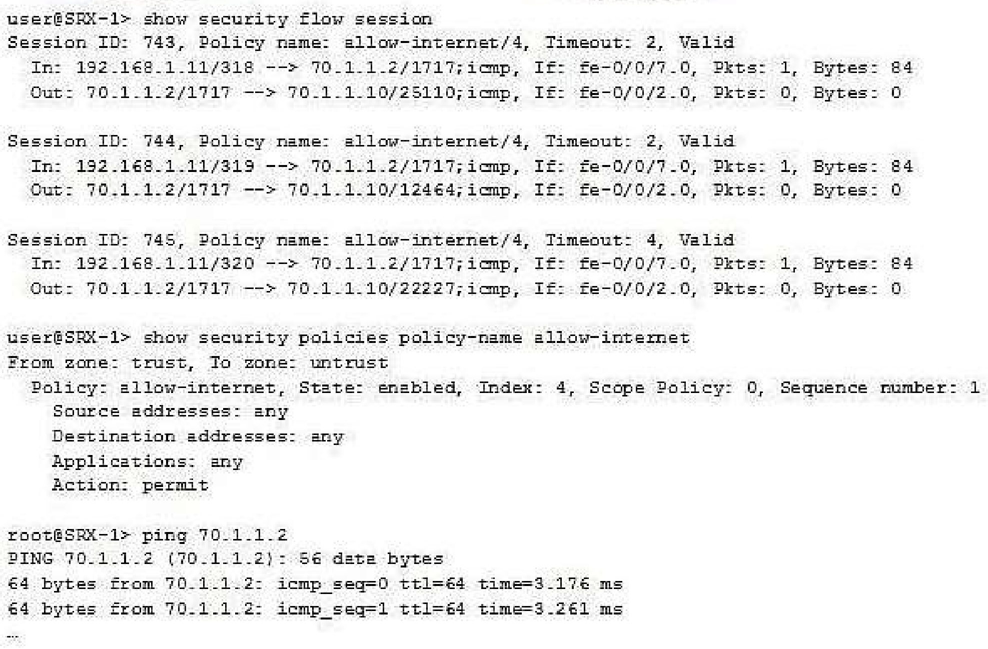
A. the IKE proposal
B. the IKE gateway
C. the IPsec policy
D. the st0 interface

Answer: B

Question No : 4

-- Exhibit –





```
user@SRX-1> show security flow session
Session ID: 743, Policy name: allow-internet/4, Timeout: 2, Valid
  In: 192.168.1.11/318 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Bytes: 84
  Out: 70.1.1.2/1717 --> 70.1.1.10/25110;icmp, If: fe-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 744, Policy name: allow-internet/4, Timeout: 2, Valid
  In: 192.168.1.11/319 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Bytes: 84
  Out: 70.1.1.2/1717 --> 70.1.1.10/12464;icmp, If: fe-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 745, Policy name: allow-internet/4, Timeout: 4, Valid
  In: 192.168.1.11/320 --> 70.1.1.2/1717;icmp, If: fe-0/0/7.0, Pkts: 1, Bytes: 84
  Out: 70.1.1.2/1717 --> 70.1.1.10/22227;icmp, If: fe-0/0/2.0, Pkts: 0, Bytes: 0

user@SRX-1> show security policies policy-name allow-internet
From zone: trust, To zone: untrust
  Policy: allow-internet, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit

root@SRX-1> ping 70.1.1.2
PING 70.1.1.2 (70.1.1.2): 56 data bytes
64 bytes from 70.1.1.2: icmp_seq=0 ttl=64 time=3.176 ms
64 bytes from 70.1.1.2: icmp_seq=1 ttl=64 time=3.261 ms
...
```

-- Exhibit --

Click the Exhibit button.

You are troubleshooting a communication problem between a trust zone and an untrust zone in the network, where PC-1 cannot ping PC-2.

Referring to the exhibit, which configuration change on SRX-1 would resolve this problem?

A. Configure proxy-arp under the [edit security nat] hierarchy.
B. Add a security policy to allow ICMP traffic from the trust zone to the untrust zone.
C. Add an address book entry for address 70.1.1.2.
D. Add a security policy to allow ICMP traffic from the untrust zone to the trust zone.

Answer: A

Explanation:

Incorrect:

B: This has already been done by permitting any source, any dest and any app.

C: No address book is used in the policy, so no need for an address book entry.

D: Add a security policy to allow ICMP from untrust to trust; this one is not valid, as session is initiated from trust zone.

Question No : 5

You are asked to troubleshoot a number of dynamic VPN connections on an SRX Series device.

Which three statements are correct? (Choose three.)

A. The configuration supports DH groups 1, 3, and 5.
B. Only RSAs are supported for IKE phase 1 authentication.
C. Dynamic VPN tunnels must be configured with extended authentication (XAUTH).
D. The SRX Series device requires a license for each remote client.
E. Only policy-based VPNs are supported.

Answer: C,D,E
Explanation:

C: Dynamic VPN tunnels must be configured with extended authentication (XAuth).
D: When configuring a shared or group IKE ID gateway, you can configure the maximum number of connections to be greater than the number of installed dynamic VPN licenses. However, if a new connection exceeds the number of licensed connections, the connection will be denied.
E: Only policy-based VPNs are supported. Route-based VPNs are not supported with dynamic VPN tunnels.
Incorrect:
A: The dynamic VPN client supports DH groups 1,2, and 5.
B: Only preshared keys are supported for Phase 1 authentication with dynamic VPN tunnels.
References:
http://www.juniper.net/documentation/en_US/junos12.1x44/topics/concept/vpn-security-dynamic-tunnelunderstanding.html

Question No : 6

You have an SRX branch device with two ISP connections. During analysis of the traffic, you notice that traffic from internal users to ISP 1 are replied to by ISP 2.

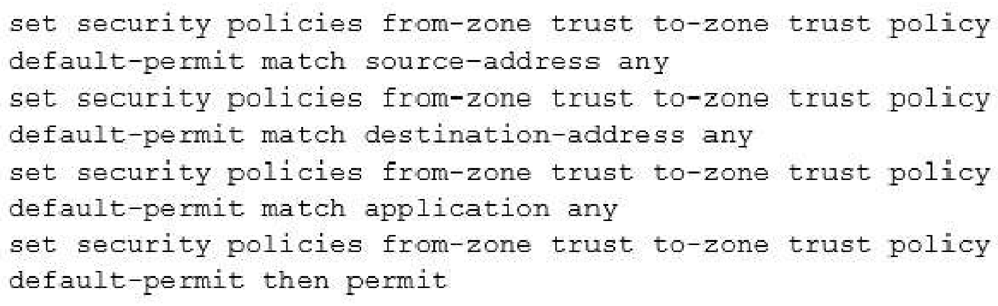
Which two configurations will correct the asymmetric problem? (Choose two.)

A. Create a security policy to allow traffic through ISP 1 only.
B. Create routing instances that include routes to ISP 1 and ISP 2.
C. Configure filter-based forwarding to provide load balancing.
D. Create an interface-specific firewall filter to forward the traffic to ISP 1.

Answer: A,B

Question No : 7

Click the Exhibit button.



```
set security policies from-zone trust to-zone trust policy
default-permit match source-address any
set security policies from-zone trust to-zone trust policy
default-permit match destination-address any
set security policies from-zone trust to-zone trust policy
default-permit match application any
set security policies from-zone trust to-zone trust policy
default-permit then permit
```

A customer created a security policy and is not receiving any logs from permitted sessions, you are asked to obtain the logs for the customer.

Which parameter must you add to the configuration shown in the exhibit to accomplish this task?

A. set system syslog file traffic-log any any
B. set default-permit then log session-close
C. set default-permit then count
D. set system syslog file traffic-log match “traffic_session”.

Answer: A

Explanation:

To send security policy logs to a file named traffic-log on the SRX Series device:
user@host# set system syslog file traffic-log any any user@host# set system syslog file traffic-log match "RT_FLOW_SESSION"
In the example above, traffic log messages are sent to a separate log file named traffic-log. The severity level is set to any so that the traffic log messages are captured. Only log messages that match RT_FLOW_SESSION, which identifies traffic log messages, are sent to the traffic-log file.
References:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB16509&actp=search

Question No : 8

While attempting to set up IDP on an SRX Series device, the IDP attack database fails to download.

What is one reason for this behavior?

A. The device's Untrust zone to Trust zone security policy does not allow this traffic.
B. The device's configuration does not include the URL from which to retrieve the attack database.
C. A firewall filter applied to the loopback interface is preventing the download of the attack database.
D. The host inbound traffic has not been configured correctly.

Answer: B

Explanation:

Note: The scenarios, which might cause the above error, can be broadly classified as follows:

The SRX device does not have Internet connectivity.

The DNS server is not configured on the SRX device.

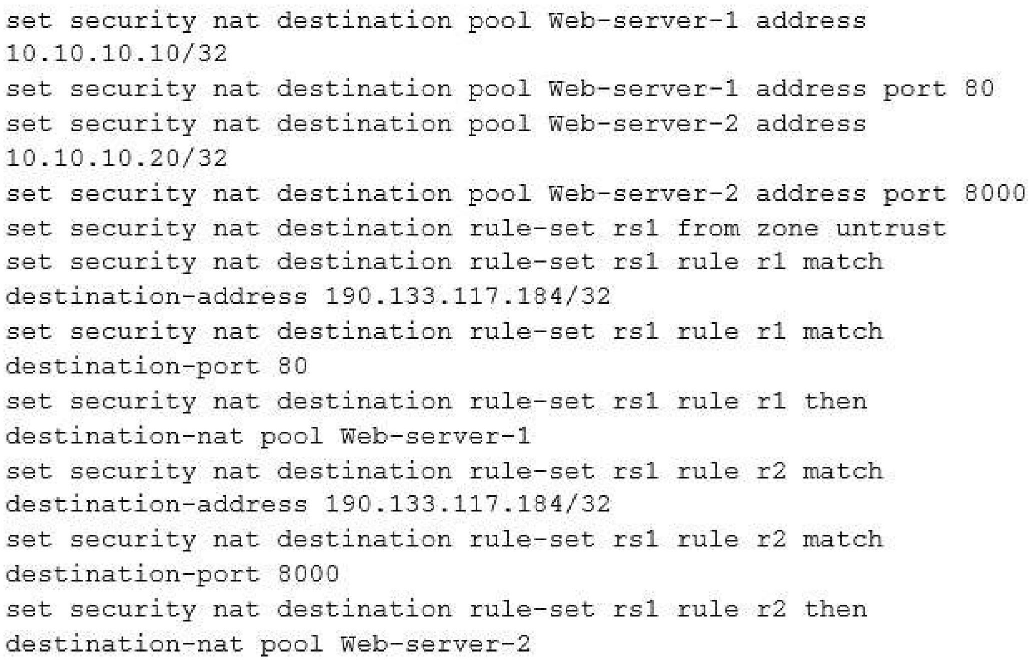
The SRX device does not have access to the SIG DB server.

Storage space in the Compact Flash is full.

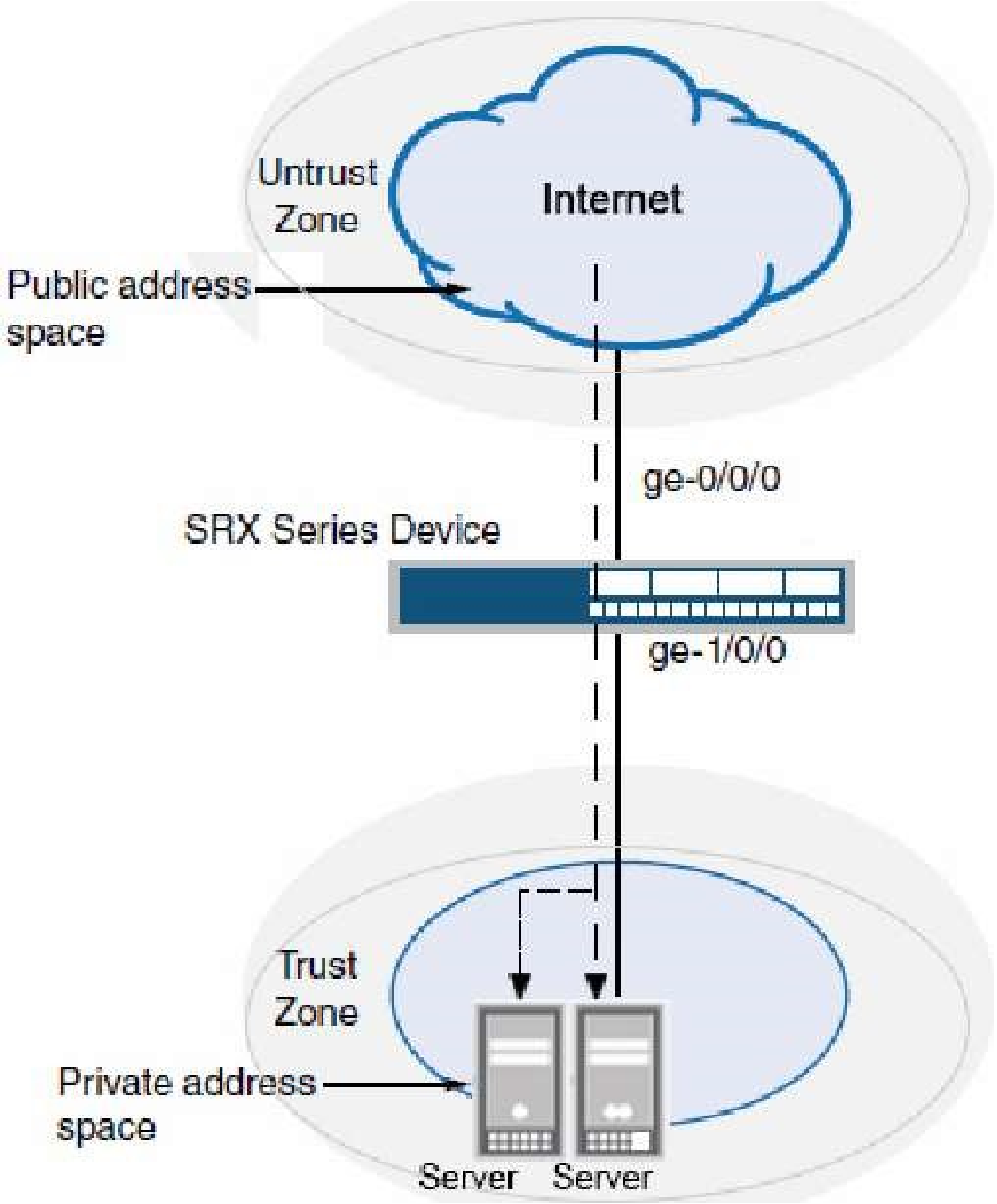
References: http://kb.juniper.net/InfoCenter/index?page=content&id=KB23359

Question No : 9

Click the exhibit button.



```
set security nat destination pool Web-server-1 address
10.10.10.10/32
set security nat destination pool Web-server-1 address port 80
set security nat destination pool Web-server-2 address
10.10.10.20/32
set security nat destination pool Web-server-2 address port 8000
set security nat destination rule-set rs1 from zone untrust
set security nat destination rule-set rs1 rule r1 match
destination-address 190.133.117.184/32
set security nat destination rule-set rs1 rule r1 match
destination-port 80
set security nat destination rule-set rs1 rule r1 then
destination-nat pool Web-server-1
set security nat destination rule-set rs1 rule r2 match
destination-address 190.133.117.184/32
set security nat destination rule-set rs1 rule r2 match
destination-port 8000
set security nat destination rule-set rs1 rule r2 then
destination-nat pool Web-server-2
```



You recently installed two new internal webservers. You configure destination NAT on your SRX Series device so that external users will have access to internal Web resources. However, the external users reported that they still do not have access to the server.

Referring to the exhibit, what should you do to solve the problem?

A. Configure proxy ARP for the address 190.133.117.184/32.
B. Contact your ISP since the packets are not reaching the SRX Series device.
C. Configure 190.133.117.184/32 under a security zone.
D. Configure a different IP address for the internal servers.

Answer: C

Explanation: