Juniper JNCIS-SEC Certification JN0-333 Exam

- **Vendor: Juniper**
- **Exam Code: JN0-333**
- **Exam Name: Juniper Networks Certified Specialist Security (JNCIS-SEC)**

Get Complete Version Exam JN0-333 Dumps with VCE and PDF Here

https://www.passleader.com/jn0-333.html

QUESTION 1
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

QUESTION 2
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

QUESTION 3
Referring to the exhibit, what will happen if client 172.16.128.50 tries to connect to destination 192.168.150.111 using HTTP?

```
[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;
     }
}
```

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

QUESTION 4
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.

Answer: C

QUESTION 5
Which interface is used exclusively to forward Ethernet-switching traffic between two chassis cluster nodes?

A. swfab0
B. fxp0
C. fab0
D. me0

Answer: A

QUESTION 6
Which feature is enabled with destination NAT as shown in the exhibit?

```
user@host# show security nat
destination {
     pool dst-nat-pool-1 {
          address 192.168.1.200/32 port 80;
          }
          pool dst-nat-pool-2 {
               address 192.168.1.220/32 port 8000;
          }
          rule-set rs1 {
               from zone untrust;
               rule r1 {
                    match {
                         destination-address 203.0.113.200/32;
                         destination-port 80;
                    }
                    then {
                         destination-nat pool dst-nat-pool-1;
                    }
          }
          rule r2 {
               match {
                    destination-address 203.0.113.200/32;
                    destination-port 8000;
               }
               then {
                    destination-nat pool dst-nat-pool-2;
               }
          }
     }
}
```

A. NAT overload
B. block allocation
C. port translation
D. NAT hairprinting

Answer: C

QUESTION 7
A customer would like to monitor their VPN using dead peer detection.

```
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  p1sa_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
```

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

QUESTION 8
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.

Answer: C

QUESTION 9
Referring to the exhibit, what will happen if client 172.16.128.50 tries to connect to destination 192.168.150.3 using HTTP?

```
[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;
               }
          }
     }
}
```

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

QUESTION 10
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

QUESTION 11
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

QUESTION 12
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

QUESTION 13
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?

```
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;
               }
          }
     }
}
```

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: D

QUESTION 14
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

QUESTION 15
You notice that your SRX Series device is not blocking HTTP traffic as expected. Referring to the exhibit, what should you do to solve the problem?

```
[edit]
user@host# show security policies
from-zone red to-zone blue {
     policy deny-http {
          match {
               source-address any;
               destination-address any;
               application junos-https;
          }
          then {
               deny;
          }
     }
}
from-zone red to-zone blue{
     policy default-permit {
          match {
               source-address any;
               destination-address any;
               application any;
          }
          then {
               permit;
          }
     }
}

[edit]
user@host# run show security flow status
Flow forwarding mode:
Inet forwarding mode: packet based (reboot needed to change to flow based)
Inet6 forwarding mode: drop
MPLS forwarding mode: drop
ISO forwarding mode: drop
Flow trace status
Flow tracing status: off
Flow session distribution
Distribution mode: RR-based
Flow ipsec performance acceleration: off
Flow packet ordering
Ordering mode: Hardware
```

A. Commit the configuration.
B. Reboot the SRX Series device.
C. Configure the SRX Series device to operate in packet-based mode.
D. Move the deny-http policy to the bottom of the policy list.

Answer: B

QUESTION 16
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

QUESTION 17
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

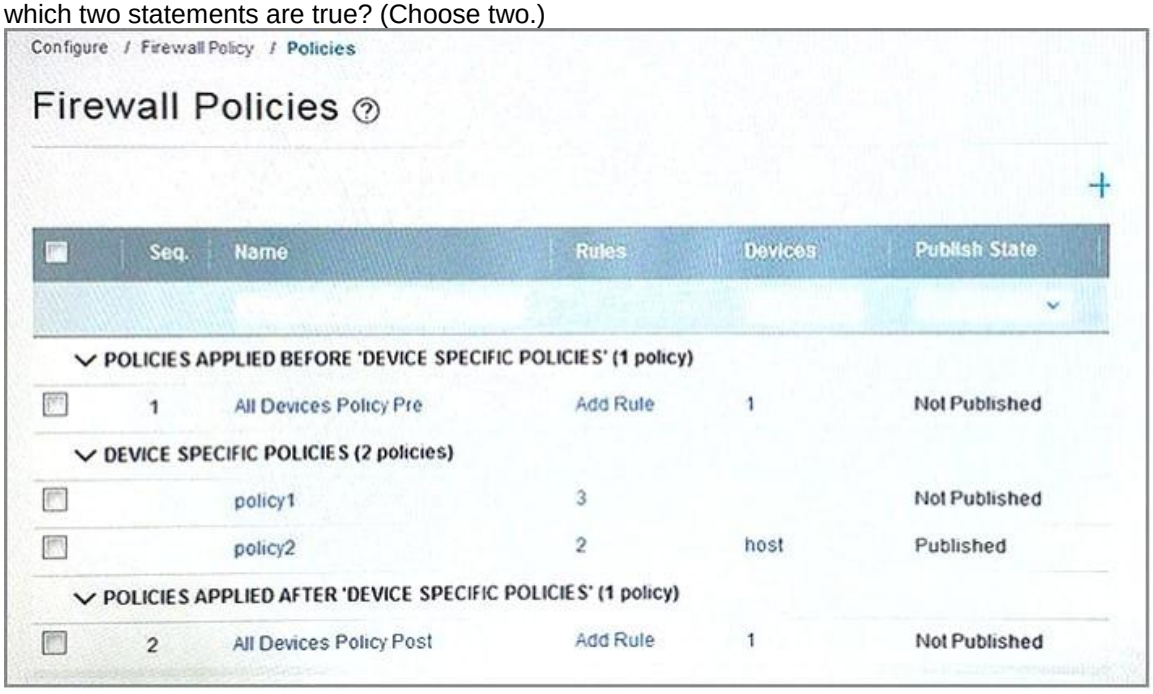
Answer: C

QUESTION 18
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 usesstateless packet processing,
E. Session-based forwarding uses six tuples of information.

Answer: ACE

QUESTION 19
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

QUESTION 20
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.

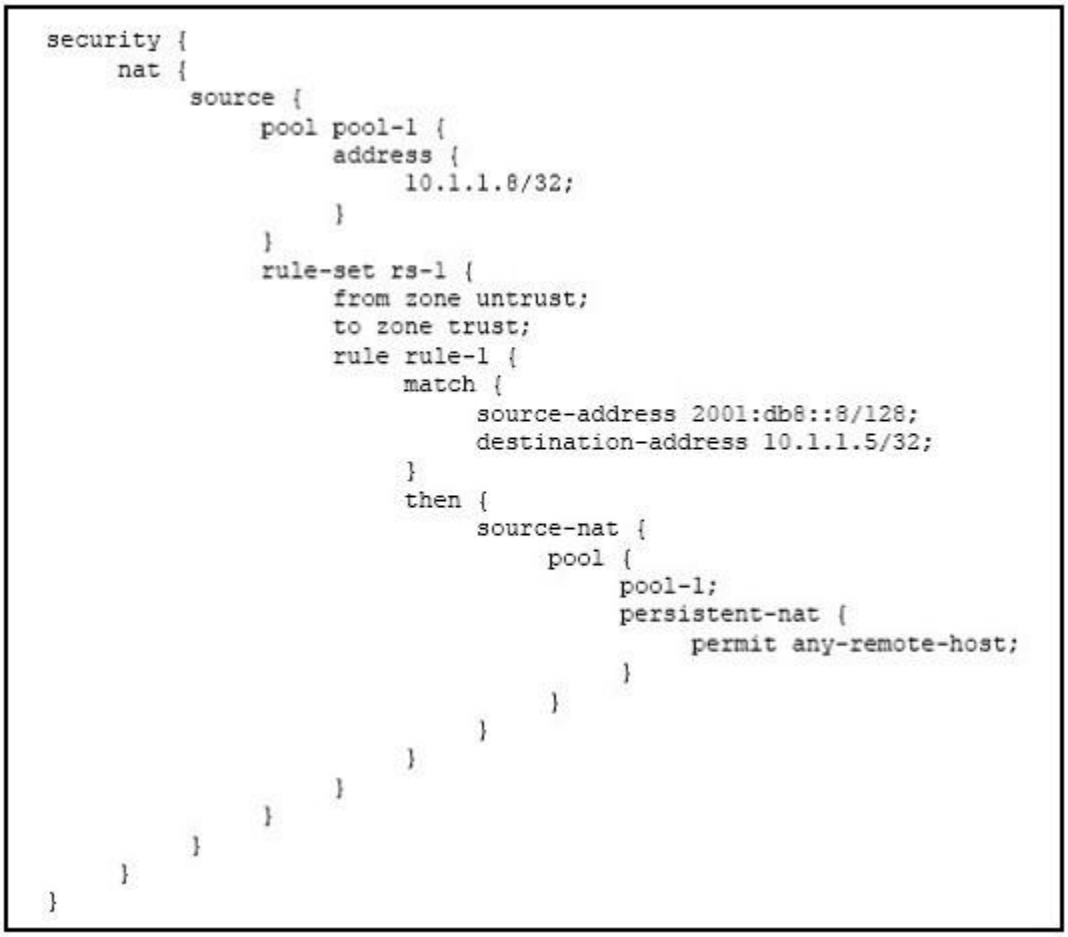
Answer: BC

QUESTION 21
Which two statements are true when implementing source NAT on an SRX Series device? (Choose two.)

A. Source NAT is applied before the security policy search.
B. Source NAT is applied after the route table lookup.
C. Source NAT is applied before the route table lookup.
D. Source NAT is applied after the security policy search.

Answer: BD

QUESTION 22
Referring to the exhibit, which action will be taken for traffic coming from the untrust zone going to the trust zone?

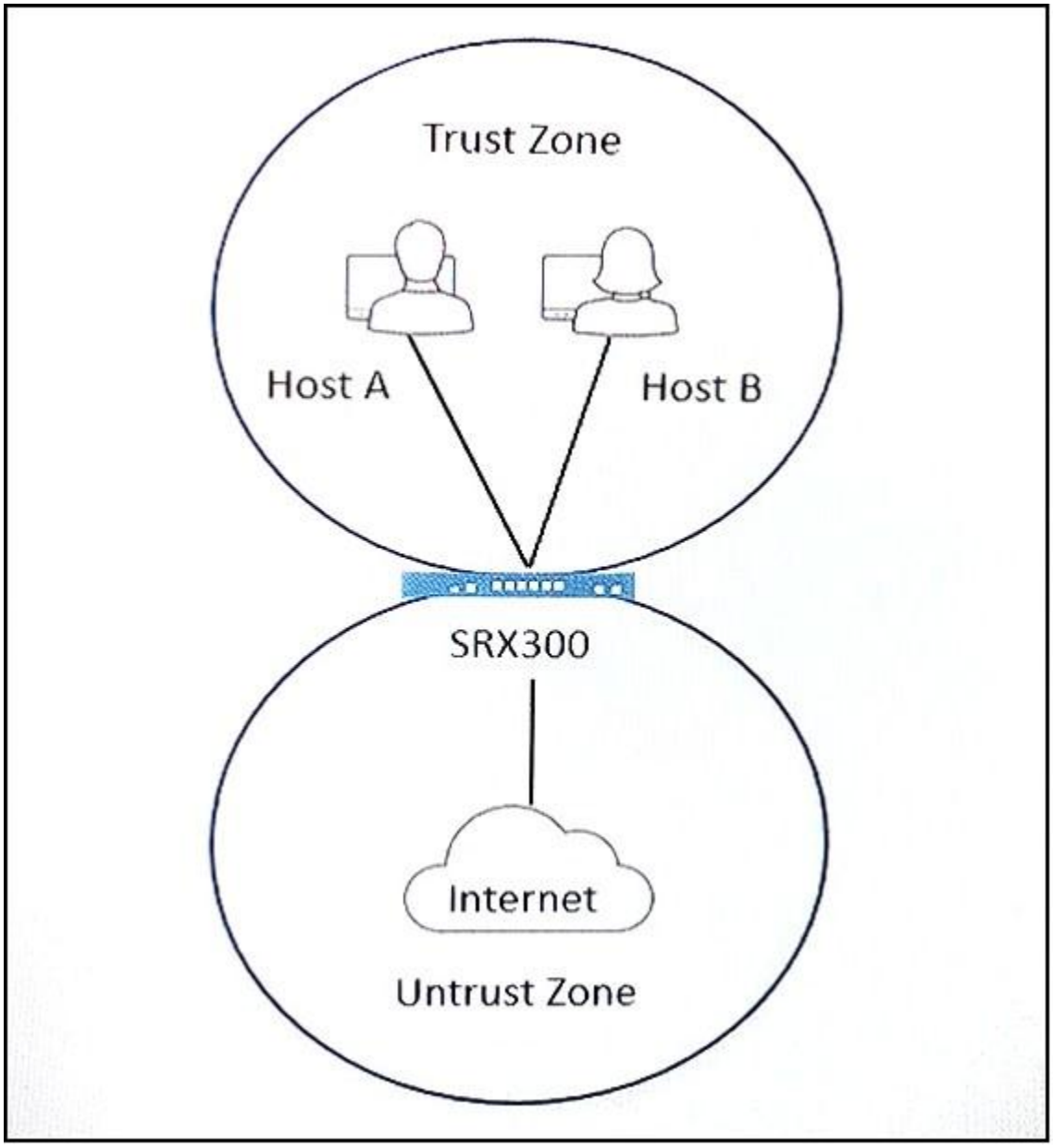


```
security {
    nat {
        source {
            pool pool-1 {
                address {
                    10.1.1.8/32;
                }
            }
            rule-set rs-1 {
                from zone untrust;
                to zone trust;
                rule rule-1 {
                    match {
                        source-address 2001:db8::8/128;
                        destination-address 10.1.1.5/32;
                    }
                    then {
                        source-nat {
                            pool {
                                pool-1;
                                persistent-nat {
                                    permit any-remote-host;
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

A. Source address 2001:db8::8 will be translated to 10.1.1.5.
B. Source address 2001:db8::8 will be translated to 10.1.1.8.
C. Source address 10.1.1.8 will be translated to 2001:db8::8.
D. Source address 10.1.1.5 will be translated to 2001:db8::8.

Answer: B

QUESTION 23
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

QUESTION 24
After an SRX Series device processes the first packet of a session, how are subsequent packets for the same session processed?

A. They are processed using fast-path processing.

B. They are forwarded to the control plane for deep packet inspection.
C. All packets are processed in the same manner.
D. They are queued on the outbound interface until a matching security policy is found.

Answer: A

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

QUESTION 26
Which three elements does AH provide in an IPsec implementation? (Choose three.)

A. confidentiality
B. authentication
C. integrity
D. availability
E. replay attack protection

Answer: BCE

QUESTION 27
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.

Answer: AB

QUESTION 28
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

QUESTION 29
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 theJunos plane.

Answer: B

QUESTION 30
What are two supported hypervisors for hosting a vSRX? (Choose two.)

A. VMware ESXi
B. Solaris Zones
C. KVM
D. Docker

Answer: AC

QUESTION 31
Referring to the exhibit, which statement is true?

```
user#host> show interface ge-0/0/1 extensive | find Zone
     Security: Zone: Null
     Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp 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:                      0
          No SA for incoming SPI:                0
          No tunnel found:                       0
          No session for a gate:                 0
          No zone or NULL zone binding           68
          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
```

A. Packets entering the interface are being dropped because of a stateless filter.
B. Packets entering the interface matching an ALG are getting dropped.
C. TCP packets entering the interface are failing the TCP sequence check.
D. Packets entering the interface are getting dropped because the interface is not bound to a zone.

Answer: D

QUESTION 32
Which three Encapsulating Security Payload protocols do the SRX Series devices support with IPsec? (Choose three.)

A. DES

B. RC6
C. TLS
D. AES
E. 3DES

Answer: ADE

QUESTION 33
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.

Answer: AC

QUESTION 34
Which statement describes the function of screen options?

A. Screen options encrypt transit traffic in a tunnel.
B. Screen options protect against various attacks on traffic entering a security device.
C. Screen options translate a private address to a public address.
D. Screen options restrict or permit users individually or in a group.

Answer: B

QUESTION 35
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. Examinethe active security flow sessions.

Answer: A

QUESTION 36
You want to implement IPsec on your SRX Series devices, but you do not want to use a preshared key. Which IPsec implementation should you use?

A. public key infrastructure
B. next-hop tunnel binding
C. tunnel mode
D. aggressive mode

Answer: A

QUESTION 37
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

QUESTION 38
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

QUESTION 39
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.

```
[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;
```

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

QUESTION 40
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

QUESTION 41
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.

Answer: D

QUESTION 42
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.

Answer: B

QUESTION 43
You are asked to support source NAT for an application that requires that its original source port not be changed. Which configuration would satisfy the requirement?

A. Configure a source NAT rule that references an IP address pool with interface proxy ARP enabled.
B. Configure the egress interface to source NAT fixed-port status.
C. Configure a source NAT rule that references an IP address pool with the port no-translation parameter enabled.
D. Configure a source NAT rule that sets the egress interface to the overload status.

Answer: C

QUESTION 44
What are three valid virtual interface types for a vSRX? (Choose three.)

A. SR-IOV
B. fxp0
C. eth0
D. VMXNET 3

E. virtio

Answer: ABD

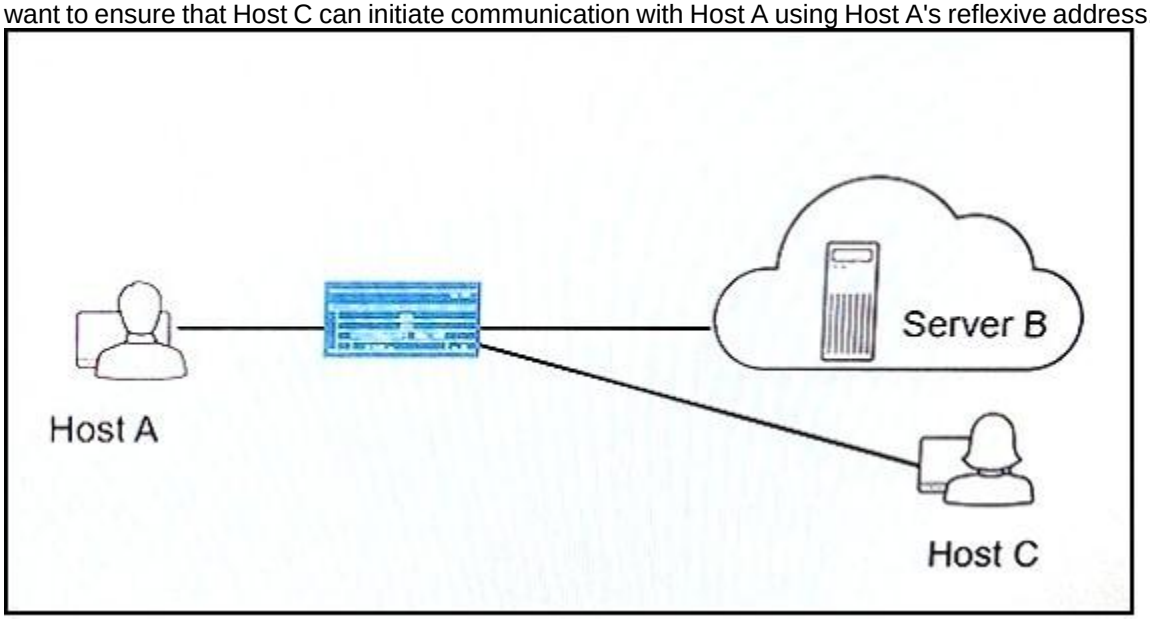
QUESTION 45
Referring to the exhibit, which statement is true?

```
user#host> show interface ge-0/0/1 extensive | find Zone
     Security: Zone: host
     Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp 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
```

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.

Answer: C

QUESTION 46
You have configured NAT on your network so that Host A can communicate with Server B. You want to ensure that Host C can initiate communication with Host A using Host A's reflexive address.



Referring to the exhibit, which parameter should you configure on the SRX Series device to satisfy this requirement?

A. Configure persistent NAT with the target-host parameter.
B. Configure persistent NAT with the target-host-port parameter.
C. Configure persistent NAT with the any-remote-host parameter.
D. Configure persistent NAT with the port-overloading parameter.

Answer: A

QUESTION 47
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

Answer: C

QUESTION 48
Which statement would explain why the IP-monitoring feature is functioning incorrectly?

```
{primary:node0}[edit]
user@host# show chassis cluster
reth-count 2;
control-ports {
     fpc 0 port 0;
     fpc 3 port 0;
}
redundancy-group 0 {
     node 0 priority 200;
     node 1 priority 100;
}
redundancy-group 1 {
     node 0 priority 200;
     node 1 priority 100;
     ip-monitoring {
          global-weight 150;
          global-threshold 240;
          retry-interval 3;
          retry-count 10;
          family {
               inet {
                    172.16.1.100 {
                         weight 150;
                         interface reth0.0 secondary-ip-address 10.1.1.1;
                    }
               }
          redundant-parent reth0;
     }
}
xe-4/0/0 {
     gigether-options {
          redundant-parent reth0;
     }
}
fab0 {
     fabric-options {
          member-interfaces {
               xe-1/1/10;
          }
     }
}
fab1 {
     fabric-options {
          mamber-interfaces {
               xe-4/1/10;
          }
     }
}
reth0 {
     unit 0 {
          family inet {
               address 10.1.1.1/24;
          }
     }
}
```

A. The global weight value is too large for the configured global threshold.
B. The secondary IP address should be on a different subnet than the reth IP address.
C. The secondary IP address is the same as the reth IP address.
D. The monitored IP address is not on the same subnet as the reth IP address.

Answer: C

QUESTION 49
You want to protect your SRX Series device from the ping-of-death attack coming from the untrust security zone. How would you accomplish this task?

A. Configure the host-inbound-traffic system-services ping except parameter in the untrust security zone.
B. Configure the application tracking parameter in the untrust security zone.
C. Configure a from-zone untrust to-zone trust security policy that blocks ICMP traffic.
D. Configure the appropriate screen and apply it to the [edit security zone security-zone untrust] hierarchy.

Answer: D

QUESTION 50
You have configured source NAT with port address translation. You also need to guarantee that the same IP address is assigned from the source NAT pool to a specific host for multiple concurrent sessions. Which NAT parameter would meet this requirement?

A. port block-allocation
B. port range twin-port
C. address-persistent
D. address-pooling paired

Answer: D

QUESTION 51
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

QUESTION 52
Your network includes IPsec tunnels. One IPsec tunnel transits an SRX Series device with NAT configured. You must ensure that the IPsec tunnels function properly. Which statement is correct in this scenario?

A. Persistent NAT should be enabled.
B. NAT-T should be enabled.
C. Destination NAT should be configured.
D. A source address pool should be configured.

Answer: B

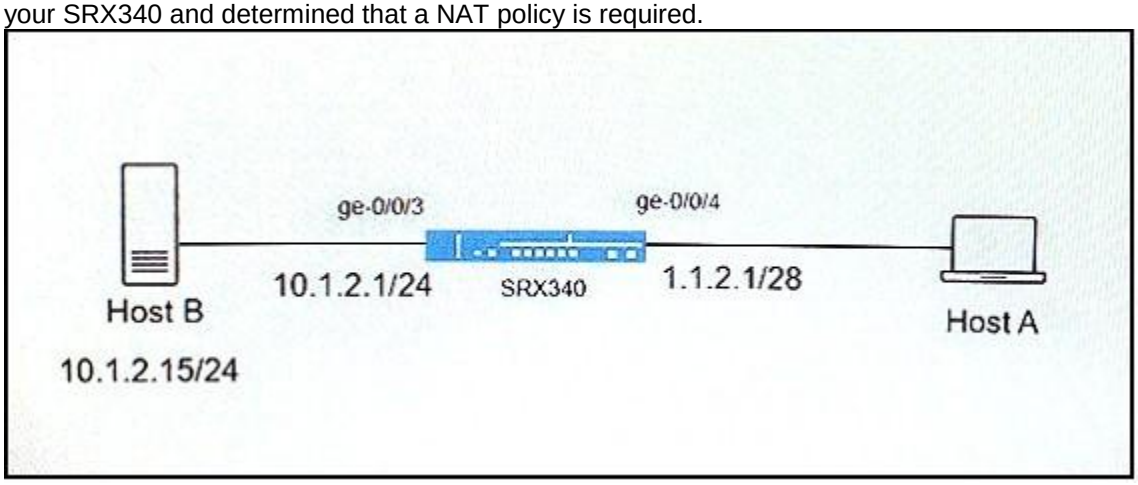
QUESTION 53
Referring to the exhibit, what does proxy ARP allow?

```
user@host# show security nat
static {
     rule-set rs1 {
          from zone untrust;
          rule r1 {
               match {
                    destination-address 1.1.1.200/32;
               }
               then {
                    static-nat prefix 192.168.1.200/32;
               }
          }
     }
}
     proxy-arp {
          interface ge-0/0/0.0 {
               address {
                    1.1.1.200/32;
               }
          }
     }
}
```

A. the internal network to ARP for the internal address of the server
B. the external network to ARP for the internal address of the server
C. the internal network to ARP for the public address of the server
D. the external network to ARP for the public address of the server

Answer: A

QUESTION 54
Host A is attempting to connect to Host B using the domain name, which is tied to a public IP address. All attempts to connect to Host B have failed. You have examined the configuration on your SRX340 and determined that a NAT policy is required.



Referring to the exhibit, which two NAT types will allow Host A to connect to Host B? (Choose two.)

A. source NAT
B. NAT-T
C. destination NAT
D. static NAT

Answer: CD

QUESTION 55
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

Answer: D

QUESTION 56
Which two statements about security policy actions are true? (Choose two.)

A. The log action implies an accept action.
B. The log action requires an additional terminating action.
C. The count action implies an accept action.
D. The count action requires an additional terminating action.

Answer: BD

QUESTION 57
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

QUESTION 58
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

Answer: B

QUESTION 59

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

QUESTION 60
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

Answer: A

QUESTION 61
What are three defined zone types on an SRX Series device?

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

Answer: BCD

QUESTION 62
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

QUESTION 63
Which statement describes the function of NAT is true?

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 ina group.

Answer: C

QUESTION 64
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

Answer: A

QUESTION 65
.....