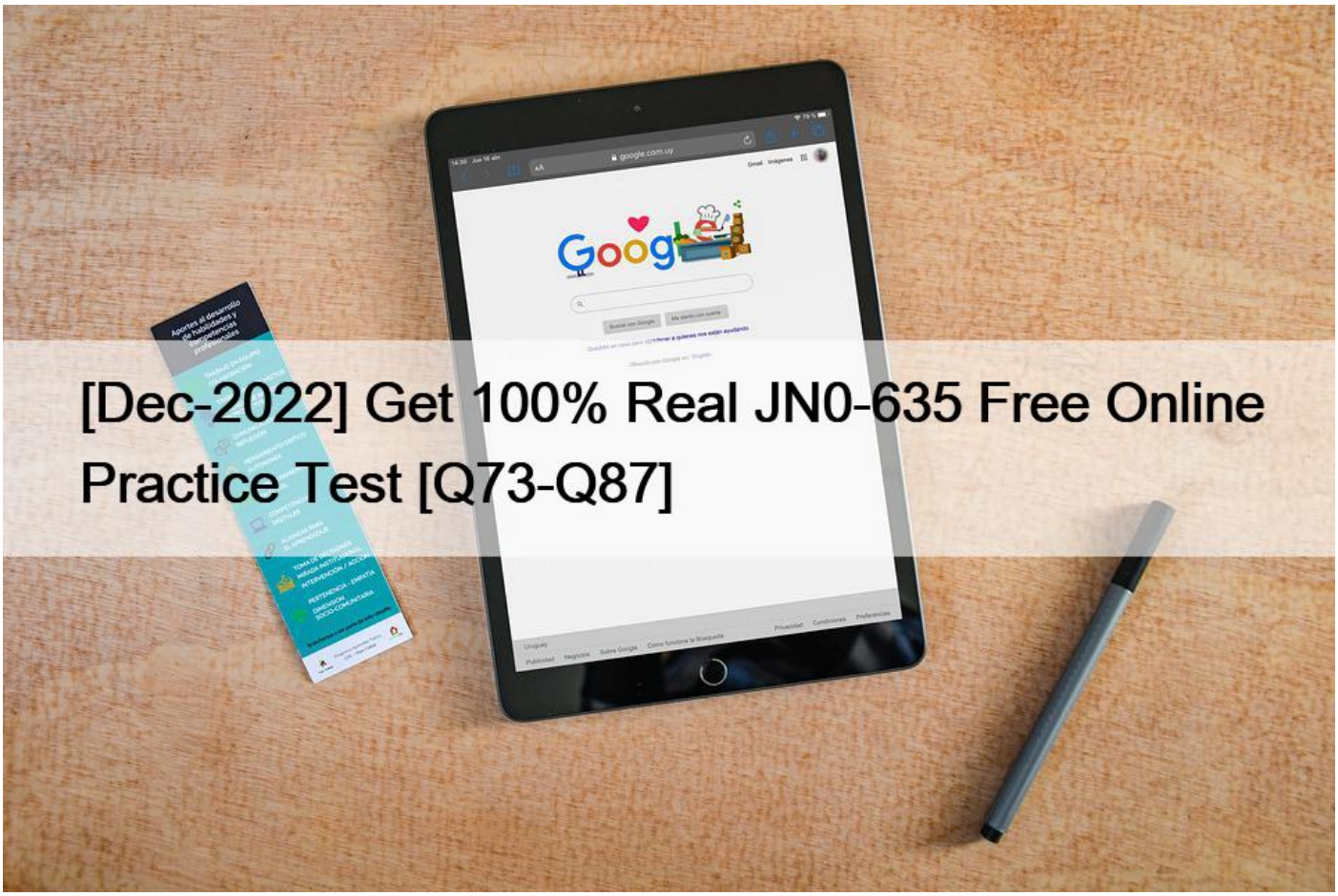
[Dec-2022 Get 100% Real JN0-635 Free Online Practice Test [Q73-Q87



[Dec-2022 Get 100% Real JN0-635 Free Online Practice Test BEST Verified Juniper JN0-635 Exam Questions (2022)

JN0-635 Exam Process

The Juniper JN0-635 test will continue for 120 minutes. Besides, there are 65 multiple-choice items. You can get to know your pass/fail status immediately after the official test. Once you successfully clear such an exam and obtain your JNCIP-SEC certification, it is valid for three years.

NEW QUESTION 73

How does secure wire mode differ from transparent mode?
* In secure wire mode, security policies cannot be used to secure intra-VLAN traffic
* In secure wire mode, no switching lookup takes place to forward traffic
* In secure wire mode, traffic can be modified using source NAT
* In secure wire mode, IRB interfaces can be configured to route inter-VLAN traffic

NEW QUESTION 74

You are using IDP on your SRX Series device and are asked to ensure that the SRX Series device has the latest IDP database, as well as the latest application signature database.

In this scenario, which statement is true?
* The application signature database cannot be updated on a device with the IDP database installed.
* You must download each database separately.
* The IDP database includes the latest application signature database.
* You must download the application signature database before installing the IDP database.

NEW QUESTION 75

Click the Exhibit button.

```
[edit]
user@srx# show
...
interfaces {
  xe-0/0/1 {
      description "Connected to Finance";
      unit 0 {
        family inet {
            address 10.1.1.1/24;
        }
      }
  }
  xe-0/1/0 {
      description "Connected to Internet";
      unit 0 {
        family inet {
            address 192.168.2.2/30;
        }
      }
  }
  xe-0/2/1 {
      description "Connected to Sales";
      unit 0 {
        family inet {
            address 10.3.2.2/24;
        }
      }
  }
  firewall {
        filter filter1 {
          term t1 {
              from {
                    source-address {
                          10.1.1.3/32;
                    }
              }
              then {
                next-interface {
                    xe-0/1/0.0;
                    routing-instance eval1;
                }
              }
          }
          term t2 {
              then {
                    routing-instance default;
              }
          }
        }
    }
    routing-instances {
        eval1 {
          instance-type virtual-router;
          interface xe-0/1/0.0;
        }
    }
```

You are asked to look at a configuration that is designed to take all traffic with a specific source IP address and forward the traffic to a traffic analysis server for further evaluation. The configuration is not working as intended.

Referring to the exhibit, which change must be made to correct the configuration?
* Apply the filter as an input filter on interface xe-0/2/1.0
* Create a routing instance named default
* Apply the filter as an input filter on interface xe-0/0/1.0
* Apply the filter as an output filter on interface xe-0/1/0.0

NEW QUESTION 76

You have a remote access VPN where the remote users are using the NCP client. The remote users can access the internal corporate resources as intended; however, traffic that is destined to all other Internet sites is going through the remote access VPN. You want to ensure that only traffic that is destined to the internal corporate resources use the remote access VPN.

Which two actions should you take to accomplish this task? (Choose two.)
* Enable IKEv2 within the VPN configuration on the SRX Series device
* Configure split tunneling on the NCP profile on the remote client
* Configure the necessary traffic selectors within the VPN configuration on the SRX Series device
* Enable the split tunneling feature within the VPN configuration on the SRX Series device

NEW QUESTION 77

You configured a security policy permitting traffic from the trust zone to the DMZ zone, inserted the new policy at the top of the list, and successfully committed it to the SRX Series device. Upon monitoring, you notice that the hit count does not increase on the newly configured policy.

In this scenario, which two commands would help you to identify the problem? (Choose two.)
* user@srx> show security zones trust detail
* user@srx> show security shadow-policies from zone trust to zone DMZ
* user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port 443
* user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port
443 result-count 10

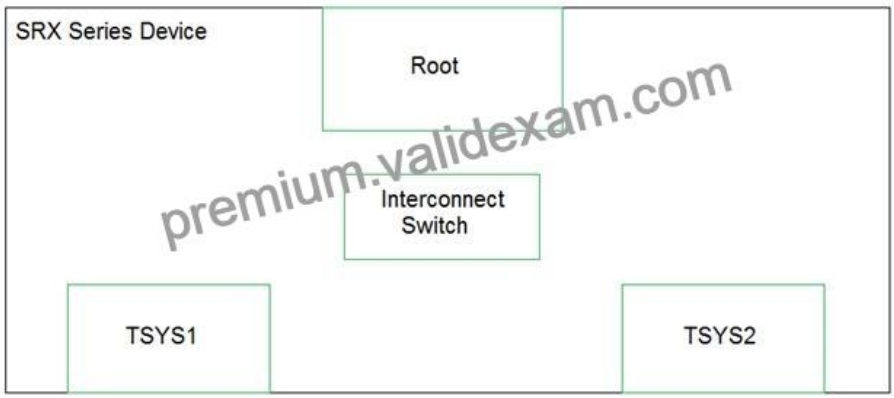
NEW QUESTION 78

You opened a support ticket with JTAC for your Juniper ATP appliance. JTAC asks you to set up access to the device using the reverse SSH connection.

Which three setting must be configured to satisfy this request? (Choose three.)
* Enable JTAC remote access
* Create a temporary root account.
* Enable a JATP support account.
* Create a temporary admin account.
* Enable remote support.
https://kb.juniper.net/InfoCenter/index?page=content&id=TN326&cat=&actp=LIST&showDraft=fal se

NEW QUESTION 79

Click the Exhibit button.



You have configured tenant systems on your SRX Series device.

Referring to the exhibit, which two actions should you take to facilitate inter-TSYS communication? (Choose two.)
* Place the logical tunnel interfaces in a virtual router routing instance in the interconnect switch
* Place the logical tunnel interfaces in a VPLS routing instance in the interconnect switch
* Connect each TSYS with the interconnect switch by configuring INET configured logical tunnel interfaces in the interconnect switch
* Connect each TSYS with the interconnect switch by configuring Ethernet VPLS configured logical tunnel interfaces in the interconnect switch
Explanation

VPLS routing Instance into Switch and LT-0/0/0 ethernet-vpls type

https://www.juniper.net/documentation/us/en/software/junos/logical-system-security/topics/topic-map/tenant-sys

NEW QUESTION 80

Referring to the configuration shown in the exhibit, which statement explains why traffic matching the IDP signature DNS:OVERFLOW:TOO-LONG-TCP-MSG is not being stopped by the SRX Series device?

```
[edit]
user@host# show security policies from-zone internet to-zone dmz
policy dmz-pol1 {
     match {
          source-address any;
          destination-address any;
          application any;
     }
     then {
          permit {
               application-services {
                    idp;
               }
          }
          log {
               session-close;
          }
     }
}

[edit]
user@host# show security idp
idp-policy idp-poll {
     rulebase-ips {
          rule r1 {
               match {
                    attacks {
                         predefined-attack-groups "HTTP All";
                    }
               }
               then {
                    action {
                         ignore-connection;
                    }
               }
          }
          rule r2 {
               match {
                    attacks {
                         predefined-attack-groups "DNS All";
                    }
               }
               then {
                    action {
                         close-server;
                    }
                    ip-action {
                         ip-notify;
                    }
               }
          }
     }
}
```

* The security policy dmz-pol1 has an action of permit.
* The IDP policy idp-pol1 is not configured as active.
* The IDP rule r2 has an ip-action value of notify.
* The IDP rule r1 has an action of ignore-connection.

NEW QUESTION 81

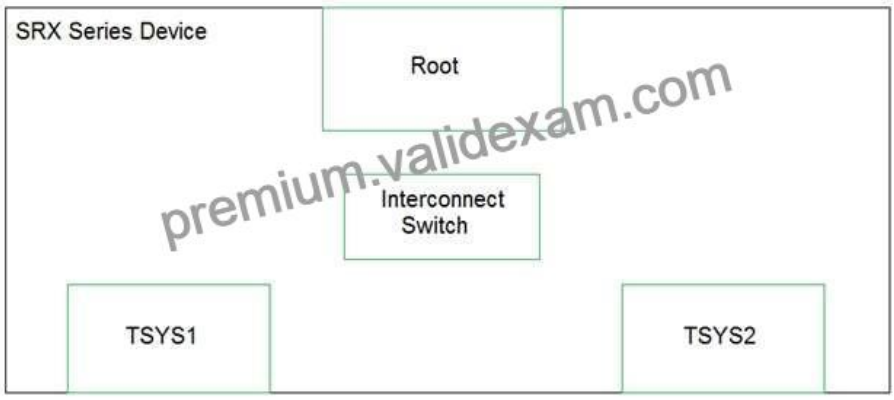
Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 11232, Policy name: Allow-ipv6-Telnet/11, Timeout: 1788, Valid
  In: 2001:db8::1/57707 --> 2001:db8::8/23;tcp, Conn Tag: 0x0, If: vlan.101,
Pkts: 9, Bytes: 799,
  Out: 10.8.8.8/23 --> 10.7.7.5/21868;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 8, Bytes: 589,
Total sessions: 1
```

Which type of NAT is shown in the exhibit?
* NAT46
* NAT64
* persistent NAT
* DS-Lite

NEW QUESTION 82

Click the Exhibit button.



You have configured tenant systems on your SRX Series device.

Referring to the exhibit, which two actions should you take to facilitate inter-TSYS communication?

(Choose two.)
* Place the logical tunnel interfaces in a virtual router routing instance in the interconnect switch
* Place the logical tunnel interfaces in a VPLS routing instance in the interconnect switch
* Connect each TSYS with the interconnect switch by configuring INET configured logical tunnel interfaces in the interconnect switch
* Connect each TSYS with the interconnect switch by configuring Ethernet VPLS configured logical tunnel interfaces in the interconnect switch

NEW QUESTION 83

Click the Exhibit button.

```
user@srx> show log flow-trace
CID-0:RT: flow process pak fast ifl 71 in_ifp ge-0/0/5.0
CID-0:RT: ge-0/0/5.0:10.0.0.2/55892->192.168.1.2/80, tcp, flag 2 syn
CID-0:RT: find flow: table 0x5a386c90, hash 50728(0xffff), sa 10.0.0.2, da
192.168.1.2, sp 55892,
dp 80, proto 6, tok 7
CID-0:RT: no session found, start first path. in_tunnel - 0x0, from_cp_flag -
0
CID-0:RT: flow_first_create_session
CID-0:RT: flow_first_in_dst_nat: in <ge-0/0/5.0>, out <N/A> dst ad
192.168.1.2, sp 55892, dp 80
CID-0:RT: chose interface ge-0/0/5.0 as incoming nat if
CID-0:RT:flow_first_rule_dst_xlatE. DST no-xlatE 0.0.0.0(0) to
192.168.1.2(80)
CID-0:RT:flow_first_routinG. vr_id 0 call flow-route_lookup(): src_ip
10.0.0.2, x_dst_ip
192.168.1.2, in ifp ge-0/0/5.0, out ifp N/A sp 55892, dp 80, ip_proto 6, tos
10
CID-0:RT:Doing DESTINATION addr route-lookup
CID-0:RT: routed (x_dst_ip 192.168.1.2) from LAN (ge-0/0/5.0 in 0) to ge-
0/0/2.0, Next-hop:
172.16.32.1
CID-0:RT:flow_first_policy_search.policy search from zone LAN-> zone WAN
(0x0,0xda540050,0x50)
CID-0:RT:Policy lkup: vsys 0 zone(7:LAN) -> zone(6:WAN) scope:0
CID-0:RT:10.0.0.2/55892 -> 192.168.1.2/80 proto 6
CID-0:RT:Policy lkup: vsys 0 zone(5:Unknown) -> zone(5:Unknown) scope:0
CID-0:RT: 10.0.0.2/55892 -> 192.168.1.2/80 proto 6
CID-0:RT: app 6, timeout 1800s, curr ageout 20s
CID-0:RT: packet dropped, denied by policy
CID-0:RT: denied by policy default-policy-00(2), dropping pkt
CID-0:RT: packet dropped, policy deny
CID-0:RT: flow find session returns error
CID-0:RT: ----- flow_process_pkt rc 0x7 (fp rc -1)
CID-0:RT:jsf sess close notify
CID-0:RT:flow ipv4 del flow: sess, in hash 32
```


A host is unable to communicate with a webserver.

Referring to the exhibit, which statement is correct?

* The webserver is not listening for traffic on port 80
* A policy is denying the traffic between these two hosts
* A session is created for this flow
* The session table is running out of resources

NEW QUESTION 84

Click the Exhibit button.

```
user@host# show security idp-policy my-policy rulebase-ips
rule 1 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  no-action;
            }
      }
}
rule 2 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  ignore-connection
            }
      }
}
rule 3 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  drop-packet;
            }
      }
}
rule 4 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  close-client-and-server;
            }
      }
}
```


You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all the rules in your IPS policy.

In this scenario, which action would be taken?

* drop packet

* no-action
* close-client-and-server
* ignore-connection

NEW QUESTION 85

The monitor traffic interface command is being used to capture the packets destined to and the from the SRX Series device.

In this scenario, which two statements related to the feature are true? (Choose two.)
* This feature does not capture transit traffic.
* This feature captures ICMP traffic to and from the SRX Series device.
* This feature is supported on high-end SRX Series devices only.
* This feature is supported on both branch and high-end SRX Series devices.

Reference:

https://forums.juniper.net/t5/Ethernet-Switching/monitor-traffic-interface/td-p/462528

NEW QUESTION 86

Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are configured for IPS. There has been a node failover.

In this scenario, which statement is true?
* Existing sessions continue to be processed by IPS because of table synchronization.
* Existing sessions are no longer processed by IPS and become firewall sessions.
* Existing session continue to be processed by IPS as long as GRES is configured.
* Existing sessions are dropped and must be reestablished so IPS processing can occur.

https://www.juniper.net/documentation/en_US/junos/topics/concept/security-ips-overview.html IPS with Chassis Clustering Limitations:

IPS is supported in both active/passive and active/active chassis cluster modes on SRX Series devices with the following limitations:

No inspection is performed on sessions that fail over or fail back. Only new sessions after a failover are inspected by IPS, and older sessions become firewall session

NEW QUESTION 87

You are asked to ensure that your IPS engine blocks attacks. You must ensure that your system continues to drop additional malicious traffic without additional IPS processing for up to 30 minutes. You must ensure that the SRX Series device does send a notification packet when the traffic is dropped.

Which statement is correct?
* Use the IP-Block action.
* Use the Drop Packet action.
* Use the Drop Connection action.
* Use the IP-Close action.

JN0-635 Exam Dumps, Practice Test Questions BUNDLE PACK: https://www.validexam.com/JN0-635-latest-dumps.html]