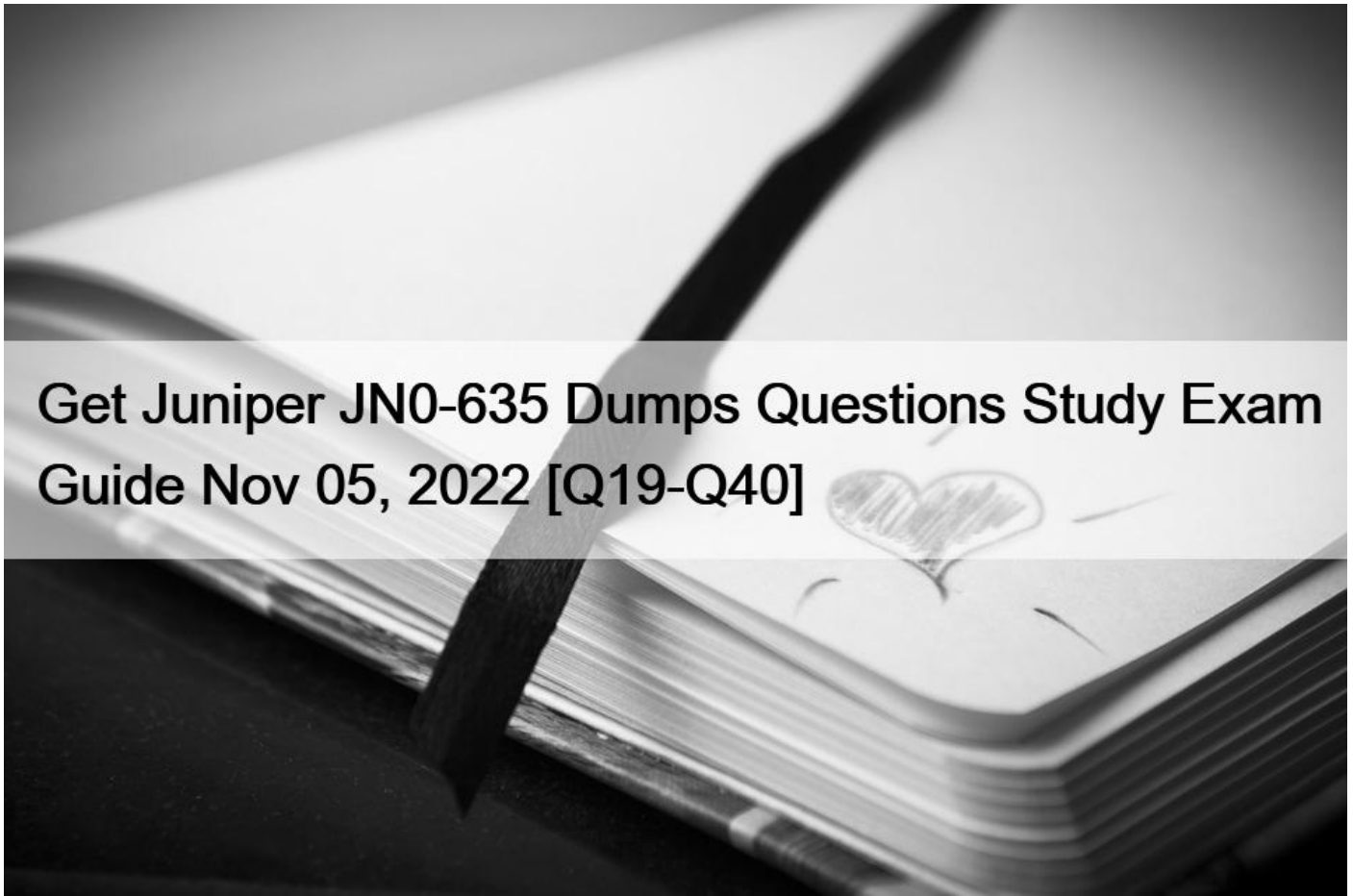


Get Juniper JN0-635 Dumps Questions Study Exam Guide Nov 05, 2022 [Q19-Q40]



Get Juniper JN0-635 Dumps Questions Study Exam Guide Nov 05, 2022 JN0-635 Premium Exam Engine - Download Free PDF Questions

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.

Exam JN0-635 must be taken to achieve the JNCIP-SEC certification, which is a professional Security designation offered by the renowned Juniper Networks. This vendor provides various security certificates at different levels such as associate (JNCIA-SEC), specialist (JNCIS-SEC), professional (JNCIP-SEC), and expert (JNCIE-SEC). For the professional level, the JNCIP-SEC certification is available, which targets networking specialists with substantial working experience and expertise in the Juniper Networks Junos OS for SRX Series gadgets. With this certificate, you can validate your security skills by utilizing advanced security technologies, the configuration of platforms, and troubleshooting techniques.

NEW QUESTION 19

A customer has recently deployed a next-generation firewall, sandboxing software, cloud access security brokers (CASB), and endpoint protection.

In this scenario, which tool would provide the customer with additional attack prevention?

- * Junos Space Cross Provisioning Platform
- * Contrail
- * Security Director Policy Enforcer
- * Network Director Inventory Manager

NEW QUESTION 20

You are asked to configure an SRX Series device to bypass all security features for IP traffic from the engineering department.

Which firewall filter will accomplish this task?

A)

```
user@srx# show firewall filter eng-filter
term 1 {
    from {
        source-prefix-list {
            hr-subnet;
        }
        destination-prefix-list {
            eng-subnet;
        }
    }
    then packet-mode;
}
term 2 {
    then accept;
}
```

B)

```
user@srx# show firewall filter eng-filter
term 1 {
    from {
        source-prefix-list {
            eng-subnet;
        }
    }
    then packet-mode;
}
term 2 {
    then accept;
}
```

C)

```
user@srx# show firewall filter eng-filter
term 1 {
  from {
    source-prefix-list {
      eng-subnet;
    }
    destination-prefix-list {
      hr-subnet;
    }
  }
  then accept;
}
term 2 {
  then packet-mode;
}
```

D)

```
user@srx# show firewall filter eng-filter
term 1 {
  from {
    source-prefix-list {
      eng-subnet;
    }
  }
  then accept;
}
term 2 {
  then accept;
}
```

- * Option B
- * Option A
- * Option C
- * Option D

NEW QUESTION 21

You must ensure that your Layer 2 traffic is secured on your SRX Series device in transparent mode.

What must be considered when accomplishing this task?

- * Layer 2 interfaces must use the ethernet-switching protocol family.
- * Security policies are not supported when operating in transparent mode.
- * Screens are not supported in your security zones with transparent mode.
- * You must reboot your device after configuring transparent mode.

NEW QUESTION 22

You are asked to configure an SRX Series device to bypass all security features for IP traffic from the engineering department.

Which firewall filter will accomplish this task?

A)

```
user@srx# show firewall filter eng-filter
term 1 {
    from {
        source-prefix-list {
            hr-subnet;
        }
        destination-prefix-list {
            eng-subnet;
        }
    }
    then packet-mode;
}
term 2 {
    then accept;
}
```

B)

```
user@srx# show firewall filter eng-filter
term 1 {
    from {
        source-prefix-list {
            eng-subnet;
        }
    }
    then packet-mode;
}
term 2 {
    then accept;
}
```

C)

```
user@srx# show firewall filter eng-filter
term 1 {
  from {
    source-prefix-list {
      eng-subnet;
    }
    destination-prefix-list {
      hr-subnet;
    }
  }
  then accept;
}
term 2 {
  then packet-mode;
}
```

D)

```
user@srx# show firewall filter eng-filter
term 1 {
  from {
    source-prefix-list {
      eng-subnet;
    }
  }
  then accept;
}
term 2 {
  then accept;
}
```

- * Option A
- * Option B
- * Option C
- * Option D

NEW QUESTION 23

Click the Exhibit button.

```
user@srx> show security mka statistics
```

```
Interface name: fxpl
Received packets: 3
Transmitted packets: 3
Version mismatch packets: 0
CAK mismatch packets: 6
IV mismatch packets: 0
Duplicate message identifier packets: 0
Duplicate message number packets: 0
Duplicate address packets: 0
Invalid destination address packets: 0
Formatting error packets: 0
Old Replayed message number packets: 0
```

While configuring the SRX345, you review the MACsec connection between devices and note that it is not working.

Referring to the exhibit, which action would you use to identify problem?

- * Verify that the connectivity association key and the connectivity association key name match on both devices
- * Verify that the interface between the two devices is up and not experiencing errors
- * Verify that the transmission path is not replicating packets or correcting frame check sequence error packets
- * Verify that the formatting settings are correct between the devices and that the software supports the version of MACsec in use

NEW QUESTION 24

Which Junos security feature is used for signature-based attack prevention?

- * AppQoS
- * PIM
- * RADIUS
- * IPS

NEW QUESTION 25

Click the Exhibit button.

```
user@SRX5800> show security idp status
```

```
-----  
State of IDP: Default, Up since: 2019-11-02 09:58:29 EDT (1w5d 03:44 ago)
```

```
Packets/second: 1 Peak: 441 @ 2019-11-14 11:02:54 EST  
KBits/second : 35881 Peak: 285133 @ 2019-11-14 12:42:01 EST  
Latency (microseconds): [min: 0] [max: 0] [avg: 0]
```

```
Packet Statistics:  
[ICMP: 0] [TCP: 713498] [UDP: 0] [Other: 0]
```

```
Flow Statistics:  
ICMP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]  
TCP:[Current: 10] [Max: 23153 @ 2019-11-14 12:28:38 EST]  
UDP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]  
Other:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]
```

```
Session Statistics:  
[ICMP: 0] [TCP: 5] [UDP: 0] [Other: 0]
```

```
Number of SSL Sessions : 0
```

```
Policy Name : IPS-POLICY  
Running Detector Version : 12.6.130190828
```

```
Forwarding process mode : regular
```

Referring to the exhibit, which IPS deployment mode is running on the SRX5800 device?

- * sniffer mode
- * integrated mode
- * monitor mode
- * in-line tap mode

NEW QUESTION 26

Click the Exhibit button.

```
user@srx> show security flow session  
Session ID: 358216, Policy name: default-policy-logical-system-00/2, Timeout:  
1788, Valid  
In: 10.10.10.1/63261 --> 203.0.113.10/443;tcp, Conn Tag: 0x0, If: ge-0/0/1.0,  
Pkts: 632, Bytes: 49341,  
Out: 203.0.113.10/443 --> 172.25.11.4/21740;tcp, Conn Tag: 0x0, If: ge-  
0/0/0.0, Pkts: 662, Bytes: 79325,
```

Referring to the exhibit, which statement is true?

- * Source NAT with PAT is occurring
- * Destination NAT is occurring
- * Static NAT without PAT is occurring
- * Source NAT without PAT is occurring

NEW QUESTION 27

A user is unable to reach a necessary resource. You discover the path through the SRX Series device includes several security

features. The traffic is not being evaluated by any security policies.

In this scenario, which two components within the flow module would affect the traffic? (Choose two.)

- * services/ALG
- * destination NAT
- * source NAT
- * route lookup

NEW QUESTION 28

Click the Exhibit button.

```
[edit security utm]
user@host# show
custom-objects {
  url-pattern {
    allow {
      value "user@example.com";
    }
    reject {
      value "user@example.com";
    }
  }
}
feature-profile {
  anti-spam {
    address-whitelist allow;
    address-blacklist reject;
    sbl {
      profile AS {
        sbl-default-server;
        spam-action block;
        custom-tag-string SPAM;
      }
    }
  }
}
```

Referring to the exhibit, which statement is true?

- * E-mails from the user@example.com address are marked with SPAM in the subject line by the spam block list server.
- * E-mails from the user@example.com address are blocked by the spam list server.
- * E-mails from the user@example.com address are blocked by the reject blacklist.
- * E-mails from the user@example.com address are allowed by the allow whitelist.

NEW QUESTION 29

Click the Exhibit button.


```
user@srx> show log flow-trace
Apr 3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT: <10.10.101.10/60858->
10.10.102.10/22; 6, 0x0> matched filter filter-1:
...
Apr 3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found, start
first path. in tunnel-0x0, from_cp_flag-0
...
Apr 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow first create session
...
Apr 3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4 0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.10
...
Apr 3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT: flow_first_policy search:
policy search from zone trust-> zone dmz (0x0 0xedba0016,0x16)
...
Apr 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by
policy
...
Apr 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy default-
policy-logical-system-00(2), dropping Pkt
...
Apr 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny
```

The exhibit shows a snippet of a security flow trace. A user cannot open an SSH session to a server.

Which action will solve the problem?

- * Create a security policy that matches the traffic parameters
- * Edit the source NAT to correct the translated address
- * Create a route entry to direct traffic into the configured tunnel
- * Create a route to the desired server

NEW QUESTION 30

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 31

Click the Exhibit button.

```
[edit]
user@srx# show security policies
from-zone client to-zone Internet {
  policy Adv-Services {
    match {
      source-address any;
      destination-address any;
      dynamic-application any;
    }
    then {
      permit {
        application-services {
          ssl-proxy {
            profile-name SSL-pro;
          }
          security-intelligence-policy Sky-intel;
          advanced-anti-malware-policy Sky-pol;
        }
      }
    }
  }
}

[edit]
user@srx# show security flow
syn-flood-protection-mode syn-cookie;
tcp-session {
  maximum-window 1M;
}
```

You deployed a site-to-site IPsec VPN connecting two data centers together using SRX5800s. After examining the performance of the IPsec VPN, you decide to enable IPsec performance acceleration to increase the rate of traffic that can be sent through the tunnel.

Referring to the exhibit, which two statements should you add to the configuration to accomplish this task?

(Choose two.)

```
[edit security flow]
* user@srx# set tcp-mss ipsec-vpn mss 65535
```

```
[edit security flow]
* user@srx# set ipsec-performance-acceleration
```

```
[edit security flow]
* user@srx# set power-mode-ipsec
```

```
[edit security flow]
* user@srx# set load-distribution session-affinity ipsec
```

Explanation/Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-improving-ipsec-

vpn-traffic-performance.html

NEW QUESTION 32

Your SRX Series device does not see the SYN packet.

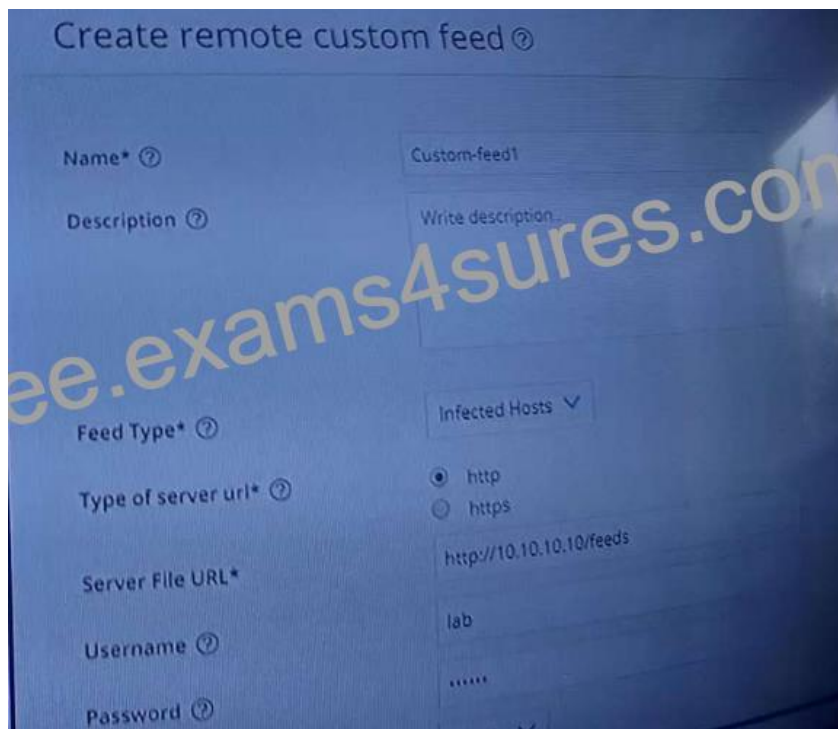
What is the default action in this scenario?

- * The device will forward the subsequent packets and the session will be established
- * The device will forward the subsequent packets and the session will not be established
- * The device will drop the subsequent packets and the session will not be established
- * The device will drop the subsequent packets and the session will be established

Explanation/Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-tcp-session-checks.html

NEW QUESTION 33

Exhibit.



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

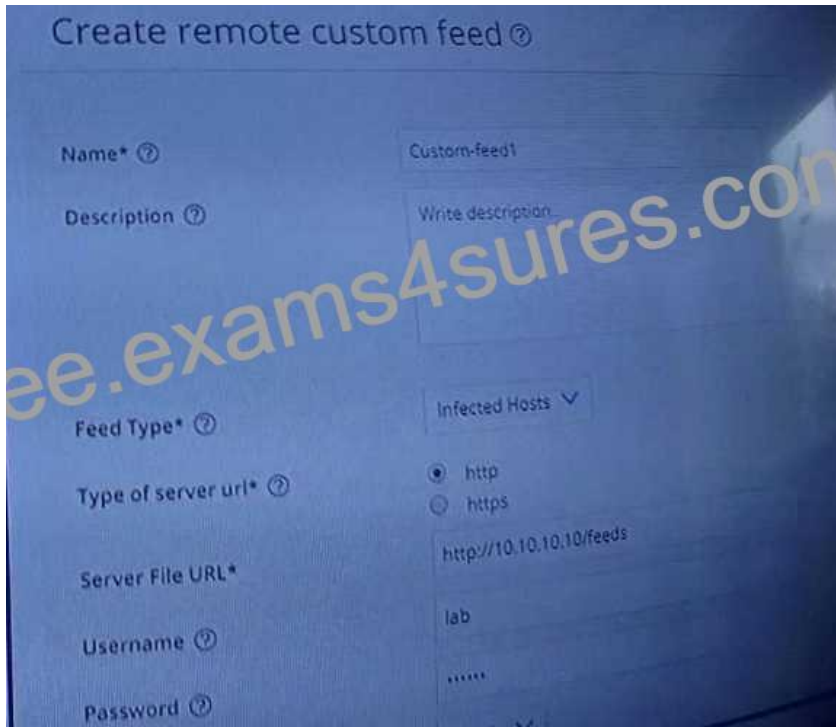
- * Juniper Networks will not investigate false positives generated by this custom feed.
- * The custom infected hosts feed will not overwrite the Sky ATP infected host's feed.
- * The custom infected hosts feed will overwrite the Sky ATP infected host's feed.
- * Juniper Networks will investigate false positives generated by this custom feed.

Reference:

https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host-configure.html

NEW QUESTION 34

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



- * Juniper Networks will not investigate false positives generated by this custom feed.
- * The custom infected hosts feed will not overwrite the Sky ATP infected host's feed.
- * The custom infected hosts feed will overwrite the Sky ATP infected host's feed.
- * Juniper Networks will investigate false positives generated by this custom feed.

[https://www.juniper.net/documentation/en_US/junos-space18.1/policy-](https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host-configure.html)

[enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host-configure.html](https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host-configure.html)

NEW QUESTION 35

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

```
[edit]
user@srxf# show system security-profile
SP-1 {
  policy {
    maximum 100;
    reserved 50;
  }
  zone {
    maximum 100;
    reserved 50;
  }
  nat-nopat-address {
    maximum 115;
    reserved 100;
  }
  nat-static-rule {
    maximum 125;
    reserved 100;
  }
}

[edit]
user@srxf# show tenants
C-1 {
  security-profile {
    SP-1;
```

- * The c-1 TSYS has a reservation for the security flow resource.
- * The c-1 TSYS can use security flow resources up to the system maximum.
- * The c-1 TSYS cannot use any security flow resources.
- * The c-1 TSYS has no reservation for the security flow resource.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-profile-logical-system.html

NEW QUESTION 36

You are asked to configure an IPsec VPN between two SRX Series devices that allows for processing of CoS on the intermediate routers.

What will satisfy this requirement?

- * route-based VPN
- * OpenVPN
- * remote access VPN
- * policy-based VPN

Explanation/Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-cos-based-ipsec-vpns.html

NEW QUESTION 37

What are two important functions of the Juniper Networks ATP Appliance solution? (Choose two.)

- * filtration
- * detection
- * statistics
- * analytics

<https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention/>

NEW QUESTION 38

Click the Exhibit button.

```
[edit]
user@srx# show security policies
from-zone client to-zone Internet {
  policy Adv-Services {
    match {
      source-address any;
      destination-address any;
      dynamic-application any;
    }
    then {
      permit {
        application-services {
          ssl-proxy {
            profile-name SSL-pro;
          }
          security-intelligence-policy Sky-intel;
          advanced-anti-malware-policy Sky-pol;
        }
      }
    }
  }
}

[edit]
user@srx# show security flow
syn-flood-protection-mode syn-cookie;
tcp-session {
  maximum-window 1M;
}
```

You deployed a site-to-site IPsec VPN connecting two data centers together using SRX5800s. After examining the performance of the IPsec VPN, you decide to enable IPsec performance acceleration to increase the rate of traffic that can be sent through the tunnel.

Referring to the exhibit, which two statements should you add to the configuration to accomplish this task?

(Choose two.)

- * [edit security flow]

```
user@srx# set tcp-mss ipsec-vpn mss 65535
```

- * [edit security flow]

```
user@srx# set ipsec-performance-acceleration
```

- * [edit security flow]


```
user@srx# set power-mode-ipsec  
* [edit security flow]
```

```
user@srx# set load-distribution session-affinity ipsec
```

NEW QUESTION 39

Click the Exhibit button.

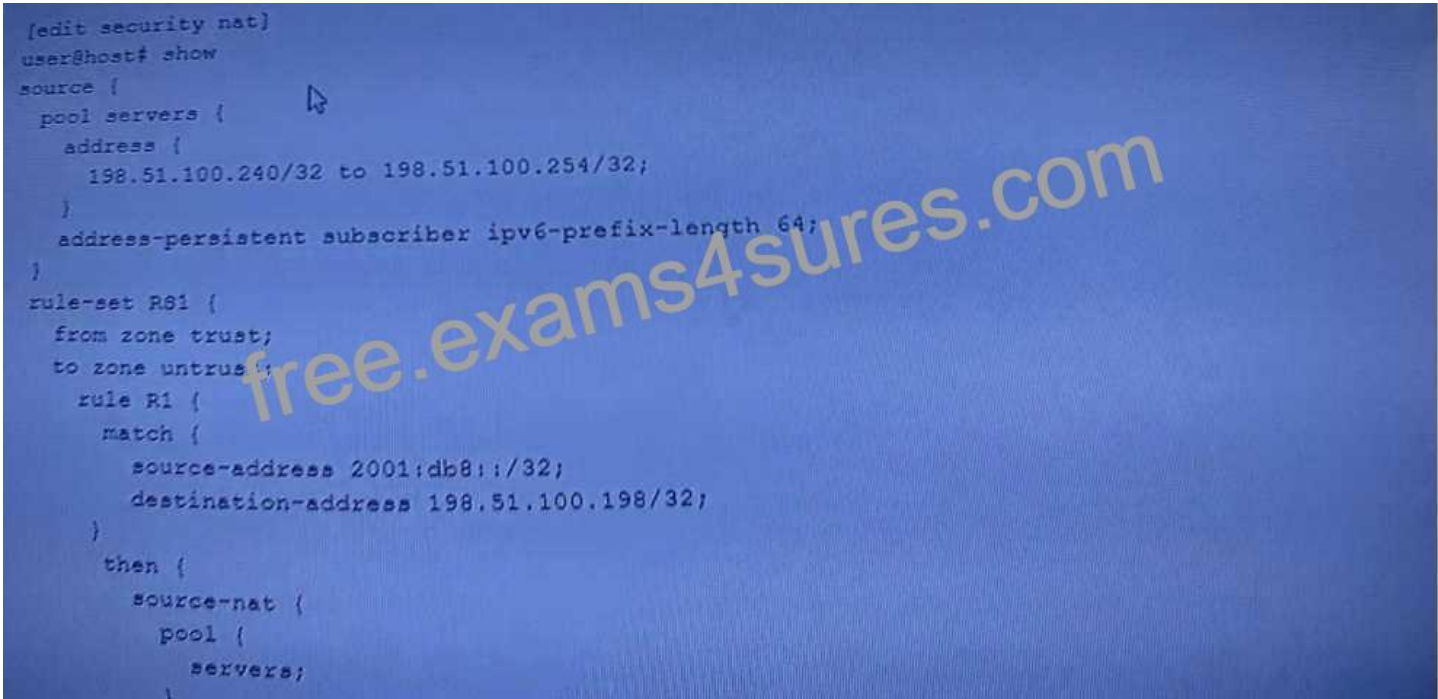
```
user@srx> show security flow session  
Session ID: 11232, Policy name: Allow-ipv6-TeOnet/11, Timeout: 1788, Valid  
In: 2001:db8::1/57707 --> 2001:db8:a6/23;tcp, Conn Tag: 0x0, If: vlan.101,  
Pkts: 9, Bytes: 799,  
Out: 10.8.8.8/23 --> 10.7.7.5/21868;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,  
Pkts: 8, Bytes: 589,  
Total sessions: 1
```

Which type of NAT is shown in the exhibit?

- * NAT46
- * NAT64
- * persistent NAT
- * DS-Lite

NEW QUESTION 40

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



```
(edit security nat)  
user@host# show  
source {  
  pool servers {  
    address {  
      198.51.100.240/32 to 198.51.100.254/32;  
    }  
    address-persistent subscriber ipv6-prefix-length 64;  
  }  
}  
rule-set RS1 {  
  from zone trust;  
  to zone untrust;  
  rule R1 {  
    match {  
      source-address 2001:db8::/32;  
      destination-address 198.51.100.198/32;  
    }  
    then {  
      source-nat {  
        pool {  
          servers;  
        }  
      }  
    }  
  }  
}
```


- * The configured solution allows IPv6 to IPv4 translation.
- * The configured solution allows IPv4 to IPv6 translation.
- * The IPv6 address is invalid.
- * External hosts cannot initiate contact.

Conclusion

The Juniper JN0-635 exam and the associated JNCIP-SEC certification will provide you with a professional skillset and validation to take up tough security tasks as well as lead teams confidently. With such a certificate, you can stand out as an experienced networker who is proficient in the Juniper Networks Junos OS, which is utilized by several renowned companies. Hence, this designation can significantly increase your job opportunities and boost your networking career. Since there are plenty of preparatory resources, as outlined in this article, you can confidently face your official exam and pass it.

Free JN0-635 Exam Braindumps Juniper Practice Exam:

<https://www.exams4sures.com/Juniper/JN0-635-practice-exam-dumps.html>