



JN0-331
SEC, Specialist (JNCIS-SEC)

Exam number/code: JN0-331
Exam name: SEC, Specialist (JNCIS-SEC)
Questions & Answers: 131 Q&A
Related Certifications: [JNCIS](#)



Hundreds of people each day pass their IT certification exams with Testking guaranteed certification resources and training kits.

Use the [Juniper JN0-331](#) questions and answers to practice for your next Juniper certification exam. If you don't pass – you don't pay! Testking has the first and only 100% product satisfaction and exam passing guarantee. Advanced practice questions and answers help drive the information into your routine thinking and surpass JN0-331 brain dumps in retention and skill building.

[Juniper](#) JN0-331 exam answers and practice questions can be used at home or office, installable on up to two PCs, or print the questions and answers to take with you and train on-the-go! Juniper JN0-331 preparation tools are the perfect fit for any Juniper certification candidate with [JN0-331](#) training materials for every level of entry.

Exam Engine Features

Control your IT training process by customizing your practice certification questions and answers. The fastest and best way to train.

- * Truly interactive practice tests
- * Create and take notes on any question
- * Retake tests until you're satisfied
- * YOU select the areas of the exam to cover
- * Filter questions for a new practice test experience each time
- * Re-visit difficult questions

Exam: JN0-331 Certification Questions & Answers

Question 1:

Which statement regarding the implementation of an IDP policy template is true?

- A. IDP policy templates are included in the factory-default configuration.
- B. IDP policy templates are automatically installed as the active IDP policy.
- C. IDP policy templates are enabled using a commit script.
- D. IDP policy templates can be downloaded without an IDP license.

Answer: C

Question 2:

Which three methods of source NAT does JUNOS Software support? (Choose three.)

- A. source NAT with address shifting
- B. source NAT with address shifting and PAT
- C. interface-based source NAT
- D. source NAT using static source pool
- E. interface-based source NAT without PAT

Answer: A,C,D

Question 3:

What are three configuration objects used to build JUNOS IDP rules? (Choose three.)

- A. zone objects
- B. network and address objects
- C. policy objects
- D. attack objects
- E. alert and notify objects

Answer: A,B,D

Question 4:

Your task is to provision the JUNOS security platform to permit transit packets from the Private zone to the External zone by using an IPsec VPN and log information at the time of session close.

Which configuration meets this requirement?

```
A. [edit security policies from-zone Private to-zone External]
user@host# show
policy allowTransit {
  match {
    source-address PrivateHosts;
    destination-address ExtServers;
    application ExtApps;
  }
  then {
    permit {
      tunnel {
```

```
ipsec-vpn VPN;
```

```
log;
```

```
count session-close;
```

```
}}}
```

B. [edit security policies from-zone Private to-zone External]

```
user@host# show
```

```
policy allowTransit {
```

```
match {
```

```
source-address PrivateHosts;
```

```
destination-address ExtServers;
```

```
application ExtApps;
```

```
}
```

```
then {
```

```
permit {
```

```
tunnel {
```

```
ipsec-vpn VPN;
```

```
}
```

```
}
```

```
log {
```

```
session-init;
```

```
}}}
```

C. [edit security policies from-zone Private to-zone External]

```
user@host# show
```

```
policy allowTransit {
```

```
match {
```

```
source-address PrivateHosts;
```

```
destination-address ExtServers;
```

```
application ExtApps;
```

```
}
```

```
then {
```

```
permit {
```

```
tunnel {
```

```
ipsec-vpn VPN;
```

```
}}
```

```
count {
```

```
session-close;
```

```
}}}
```

D. [edit security policies from-zone Private to-zone External]

```
user@host# show
```

```
policy allowTransit {
```

```
match {
```

```
source-address PrivateHosts;
```

```
destination-address ExtServers;
```

```
application ExtApps;
```

```
}
```

```
then {
```

```
permit {
```

```
tunnel {
```

```
ipsec-vpn VPN;
```

```
}}
```

```
log {
```

```
session-close;
```

```
}}}
```

Answer: D

Question 5:

What is a redundancy group in JUNOS Software?

A. a set of chassis clusters that fail over as a group

- B. a set of VRRP neighbors that fail over as a group
- C. a set of chassis cluster objects that fail over as a group
- D. a set of devices that participate in a chassis cluster

Answer: C

Question 6:

In a chassis cluster with two SRX 5800 devices, the interface ge-13/0/0 belongs to which device?

- A. This interface belongs to node 1 of the cluster.
- B. This interface belongs to node 0 of the cluster.
- C. This interface is a system-created interface.
- D. This interface will not exist because SRX 5800 devices have only 12 slots.

Answer: A

Question 7:

Which two statements about the use of SCREEN options are correct? (Choose two.)

- A. SCREEN options are deployed at the ingress and egress sides of a packet flow.
- B. SCREEN options offer protection against various attacks.
- C. When you deploy SCREEN options, you must take special care to protect OSPF.
- D. SCREEN options are deployed prior to route and policy processing in first path packet processing.

Answer: B,D

Question 8:

Which configuration shows a pool-based source NAT without PAT'?

- A.

```
[edit security nat source]
user@host# show
pool A {
address { 207.17.137.1/32 to 207.17.137.254/32;
}
overflow-pool interface;
}
rule-set 1A {
from zone trust;
to zone untrust;
rule 1 {
match {
source-address 10.1.10.0/24;
}
then {
source-nat pool A;
port no-translation;
}}}

```
- B.

```
[edit security nat source]
user@host# show
pool A {
address {207.17.137.1/32 to 207.17.137.254/32;
}
overflow-pool interface;
}

```

```
rule-set 1A {
from zone trust;
to zone untrust;
rule 1 {
match {
source-address 10.1.10.0/24;
}
then {
source-nat pool A;
}}}
C. [edit security nat source]
user@host# show
pool A {
address {207.17.137.1/32 to 207.17.137.254/32;
}
port no-translation;
}
rule-set 1A {
from zone trust;
to zone untrust;
rule 1 {
match {
source-address 10.1.10.0/24;
}
then {
source-nat pool A;
}}}
D. [edit security nat source]
user@host# show
pool A {
address { 207.17.137.1/32 to 207.17.137.254/32;
}}
rule-set 1A {
from zone trust;
to zone untrust;
rule 1 {
match {
source-address 10.1.10.0/24;
}
then {
source-nat pool A;
port no-translation;
}}
}
```

Answer: C

Question 9:

Which two external authentication server types are supported by JUNOS Software for firewall user authentication? (Choose two.)

- A. IIS
- B. LDAP
- C. RADIUS
- D. TACACS+

Answer: B,C

Question 10:

You are required to configure a SCREEN option that enables IP source route option detection.

Which two configurations meet this requirement? (Choose two.)

A. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
strict-source-route-option;
record-route-option;
}}
}}

B. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
loose-source-route-option;
strict-source-route-option;
}}
}}

C. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
record-route-option;
security-option;
}}
}}

D. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
source-route-option;
}}
}}

Answer: B,D

Question 11:

Regarding zone types, which statement is true?

- A. You can specify a functional zone in a security policy.
- B. You can use a security zone for traffic destined for the device itself.
- C. Security zones must have a scheduler applied.
- D. You cannot assign an interface to a functional zone.

Answer: B

Question 12:

Click the Exhibit button.

```
[edit schedulers]
user@host# show
scheduler now {
monday all-day;
tuesday exclude;
wednesday {
start-time 07:00:00 stop-time 18:00:00;
}
thursday {
start-time 07:00:00 stop-time 18:00:00;
```

```
}}  
[edit security policies from-zone Private to-zone External]  
user@host# show  
policy allowTransit {  
  match {  
    source-address PrivateHosts;  
    destination-address ExtServers;  
    application ExtApps;  
  }  
  then {  
    permit {  
      tunnel {  
        ipsec-vpn myTunnel;  
      }  
    }  
  }  
}  
scheduler-name now;
```

Based on the configuration shown in the exhibit, what are the actions of the security policy?

- A. The policy will always permit transit packets, but will only use the IPsec VPN myTunnel all day Monday and Wednesday 7am to 6pm, and Thursday 7am to 6pm.
- B. The policy will always permit transit packets and use the IPsec VPN myTunnel.
- C. The policy will permit transit packets only on Monday, and use the IPsec VPN Mytunnel.
- D. The policy will permit transit packets and use the IPsec VPN myTunnel all day Monday and Wednesday 7am to 6pm, and Thursday 7am to 6pm.

Answer: D

Question 13:

Which two functions of JUNOS Software are handled by the data plane? (Choose two.)

- A. OSPF
- B. SCREEN options
- C. SNMP
- D. NAT

Answer: B,D

Question 14:

Which two statements describe the difference between JUNOS Software for security platforms and a traditional router? (Choose two.)

- A. JUNOS Software for security platforms supports NAT and PAT; a traditional router does not support NAT or PAT.
- B. JUNOS Software for security platforms does not forward traffic by default; a traditional router forwards traffic by default.
- C. JUNOS Software for security platforms performs route lookup for every packet; a traditional router performs route lookup only for the first packet.
- D. JUNOS Software for security platforms uses session-based forwarding; a traditional router uses packet-based forwarding.

Answer: B,D

Question 15:

Click the Exhibit button.
[edit security policies]

```
user@host# show
from-zone trust to-zone untrust {
policy AllowHTTP{
match {
source-address HOSTA;
destination-address any;
application junos-ftp;
}
then {
permit;
}}
policy AllowHTTP2{
match {
source-address any;
destination-address HOSTA;
application junos-http;
}
then {
permit;
}}
policy AllowHTTP3{
match {
source-address any;
destination-address any;
application any;
}
then {
permit;
}}
}}}
```

A flow of HTTP traffic needs to go from HOSTA to HOSTB. Assume that traffic will initiate from

HOSTA and that HOSTA is in zone trust and HOSTB is in zone untrust.

What will happen to the traffic given the configuration in the exhibit?

- A. The traffic will be permitted by policy AllowHTTP3.
- B. The traffic will be permitted by policy AllowHTTP.
- C. The traffic will be permitted by policy AllowHTTP2.
- D. The traffic will be dropped as no policy match will be found.

Answer: A

Related JN0-331 Exams:

[JN0-304](#)
[JN0-570](#)

[JN0-303](#)
[JN0-350](#)

[JN0-332](#)
[JN0-532](#)

[JN0-360](#)
[JN0-531](#)

[JN0-330](#)
[JN0-343](#)

Popular Certification Exams:

[190-951](#)
[LOT-710](#)
[E20-501](#)

[HP2-Z03](#)
[HP0-J44](#)
[1z0-101](#)

[70-513](#)
[HP0-632](#)
[920-321](#)

[TK0-001](#)
[BH0-005](#)
[COG-112](#)

[920-235](#)
[190-802](#)
[920-105](#)

Hot Certifications:

[Linux](#)

[XenDesktop 5](#)

[Genesys](#)

[ICND](#)

[Filemaker 11
Certified
Developer](#)

Popular Certification Providers:

[BICSI](#)

[IBM](#)

[McAfee](#)

[Mincom](#)

[CIW](#)