

# Security, Associate (JNCIA-SEC)

1. Which two criteria should a zone-based security policy include? (Choose two.)

A. a source port

B. a destination port

C. zone context

D. an action

**Answer(s):** A B

---

2. You are assigned a project to configure SRX Series devices to allow connections to your webservers. The webservers have a private IP address, and the packets must use NAT to be accessible from the Internet. You do not want the webservers to initiate connections with external update servers on the Internet using the same IP address as customers use to access them.

Which two NAT types must be used to complete this project? (Choose two.)

A. static NAT

B. hairpin NAT

C. destination NAT

D. source NAT

**Answer(s):** C D

---

3. You are asked to verify that a license for AppSecure is installed on an SRX Series device. In this scenario, which command will provide you with the required information?

A. user@srx> show system license

B. user@srx> show services accounting

C. user@srx> show configuration system

D. user@srx> show chassis firmware

**Answer(s):** A

---

4. Click the Exhibit button.

```
[edit security policies]
user@vSRX-1# edit from-zone trust to-zone dmz policy Trust-DMZ-Access
[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access
user@vSRX-1# exit
```

Referring to the exhibit, a user is placed in which hierarchy when the exit command is run?

A. [edit security policies from-zone trust to-zone dmz]user@vSRX-1#

B. [edit]user@vSRX-1#

C. [edit security policies]user@vSRX-1#

D. user@vSRX-1>

**Answer(s):** A

---

5. You want to enable the minimum Juniper ATP services on a branch SRX Series device. In this scenario, what are two requirements to accomplish this task? (Choose two.)

A. Install a basic Juniper ATP license on the branch device.

B. Configure the juniper-atp user account on the branch device.

C. Register for a Juniper ATP account on <https://sky.junipersecurity.net>.

D. Execute the Juniper ATP script on the branch device.

**Answer(s):** C D

---

6. SRX Series devices have a maximum of how many rollback configurations?

A. 40

B. 60

C. 50

D. 10

**Answer(s): C**

---

7. Unified threat management (UTM) inspects traffic from which three protocols? (Choose three.)

A. FTP

B. SMTP

C. SNMP

D. HTTP

E. SSH

**Answer(s): A B D**

---

8. When are Unified Threat Management services performed in a packet flow?

A. before security policies are evaluated

B. as the packet enters an SRX Series device

C. only during the first path process

D. after network address translation

**Answer(s): D**

---

9. When configuring antispam, where do you apply any local lists that are configured?

A. custom objects

B. advanced security policy

C. antispam feature-profile

D. antispam UTM policy

**Answer(s):** A

---

**10.** Screens on an SRX Series device protect against which two types of threats? (Choose two.)

A. IP spoofing

B. ICMP flooding

C. zero-day outbreaks

D. malicious e-mail attachments

**Answer(s):** A B

---

**11.** Which statement about global NAT address persistence is correct?

A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.

B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.

C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.

D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

**Answer(s):** A

---

**12.** You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.

Which Juniper ATP solution will accomplish this task?

A. Geo IP

B. unified security policies

C. IDP

D. C&C feed

**Answer(s):** A

---

**13.** Which two statements are correct about IKE security associations? (Choose two.)

A. IKE security associations are established during IKE Phase 1 negotiations.

B. IKE security associations are unidirectional.

C. IKE security associations are established during IKE Phase 2 negotiations.

D. IKE security associations are bidirectional.

**Answer(s):** A D

---

**14.** You want to deploy a NAT solution.

In this scenario, which solution would provide a static translation without PAT?

A. interface-based source NAT

B. pool-based NAT with address shifting

C. pool-based NAT with PAT

D. pool-based NAT without PAT

**Answer(s):** B

---

**15.** Which Juniper Networks solution uses static and dynamic analysis to search for day-zero malware threats?

A. firewall filters

B. UTM

C. Juniper ATP Cloud

D. IPS

**Answer(s): C**

---

**16.** You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses. Which NAT configuration is appropriate in this scenario?

A. source NAT with PAT

B. destination NAT

C. NAT-T

D. static NAT

**Answer(s): D**

---

**17.** You want to provide remote access to an internal development environment for 10 remote developers. Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

A. an additional license for an SRX Series device

B. Juniper Secure Connect client software

C. an SRX Series device with an SPC3 services card

D. Marvis virtual network assistant

**Answer(s): A B**

---

**18.** You are deploying an SRX Series firewall with multiple NAT scenarios. In this situation, which NAT scenario takes priority?

A. interface NAT

B. source NAT

C. static NAT

D. destination NAT

**Answer(s):** A

---

**19.** Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server. In this scenario, which two configuration features need to be added? (Choose two.)

A. firewall filter

B. security policy

C. proxy-ARP

D. UTM policy

**Answer(s):** B C

---

**20.** Click the Exhibit button.

```
user@vSRX-VR> ping 10.10.102.10 count 5 routing-instance DMZ
PING 10.10.102.10 (10.10.102.10): 56 data bytes
64 bytes from 10.10.102.10: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 10.10.102.10: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.10.102.10: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.10.102.10: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.102.10: icmp_seq=4 ttl=64 time=0.070 ms
--- 10.10.102.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.051/0.070/0.011 ms
user@vSRX-VR>
```

Referring to the exhibit, which two statements are correct about the ping command? (Choose two.)

A. The DMZ routing-instance is the source.

B. The 10.10.102.10 IP address is the source.

C. The 10.10.102.10 IP address is the destination.

D. The DMZ routing-instance is the destination.

**Answer(s):** A C

---

