Security Design, Specialist (JNCDS-SEC)

1. You are deploying Security Director with the logging and reporting functionality for VMs that use SSDs. You expect to have approximately 20,000 events per second of logging in your network.
In this scenario, what is the minimum number of logging and reporting devices that should be used?

A. 2

B. 4

C. 1

D. 3

Answer(s): C

---

2. You are concerned about users attacking the publicly accessible servers in your data center through encrypted channels. You want to block these attacks using your SRX Series devices.
In this scenario, which two features should you use? (Choose two.)

- [ ] A. Sky ATP
- [ ] B. IPS
- [ ] C. SSL forward proxy
- [ ] D. SSL reverse proxy

Answer(s): B C

---

3. Your customer needs help designing a single solution to protect their combination of various Junos network devices from unauthorized management access.
Which Junos OS feature will provide this protection?

A. Use a firewall filter applied to the fxp0 interface

B. Use a security policy with the destination of the junos-host zone

C. Use the management zone host-inbound-traffic feature

D. Use a firewall filter applied to the lo0 interface

Answer(s): A

---

4. You must allow applications to connect to external servers. The session has embedded IP address information to enable the remote system to establish a return session.
In your design, which function should be implemented?

A. source NAT

B. application layer gateway

C. destination NAT

D. HTTP redirect

Answer(s): A

---

5. You are using SRX Series devices to secure your network and you require sandboxing for malicious file detonation. However, per company policy, you cannot send potentially malicious files outside your network for sandboxing. Which feature should you use in this situation?

A. Sky ATP

B. UTM antivirus

C. IPS

D. JATP

Answer(s): D

---

6. You are creating a security design proposal for an enterprise customer. As part of the design, you are implementing 802.1x authentication on your EX Series devices.
In this scenario, which two statements are correct? (Choose two.)

- ☐ A. The supplicant is the device that prevents the authenticator’s access until it is authenticated
- ☐ B. The supplicant is the device that is being authenticated
- ☐ C. The authenticator is the device that is being authenticated
- ☐ D. The authenticator is the device that prevents the supplicant’s access until it is authenticated

Answer(s): B D

---

7. You are asked to install a mechanism to protect an ISP network from denial-of-service attacks from a small number of sources. Which mechanism will satisfy this requirement?

A. RTBH

B. UTM

C. Sky ATP

D. GeoIP

Answer(s): A

---

8. You are responding to an RFP for securing a large enterprise. The RFP requires an onsite security solution which can use logs from third-party sources to prevent threats. The solution should also have the capability to detect and stop zero-day attacks.
Which Juniper Networks solution satisfies this requirement?

A. IDP

B. Sky ATP

C. JSA

D. JATP

Answer(s): D

---

9. You are designing an SDSN security solution for a new campus network. The network will consist of Juniper Networks Policy Enforcer, Juniper Networks switches, third-party switches, and SRX Series devices. The switches and the SRX Series devices will be used as security enforcement points.
Which component supports the SRX Series devices in this scenario?

A. Security Director

B. RADIUS server

C. certificate server

D. DHCP server

Answer(s): A

---

10. Your company has outgrown its existing secure enterprise WAN that is configured to use OSPF, AutoVPN, and IKE version 1. You are asked if it is possible to make a design change to improve the WAN performance without purchasing new hardware.
Which two design changes satisfy these requirements? (Choose two.)

- [ ] A. Modify the IPsec proposal from AES-128 to AES-256
- [ ] B. Change the IGP from OSPF to IS-IS
- [ ] C. Migrate to IKE version 2

- [ ] D. Implement Auto Discovery VPN

Answer(s): B D

---

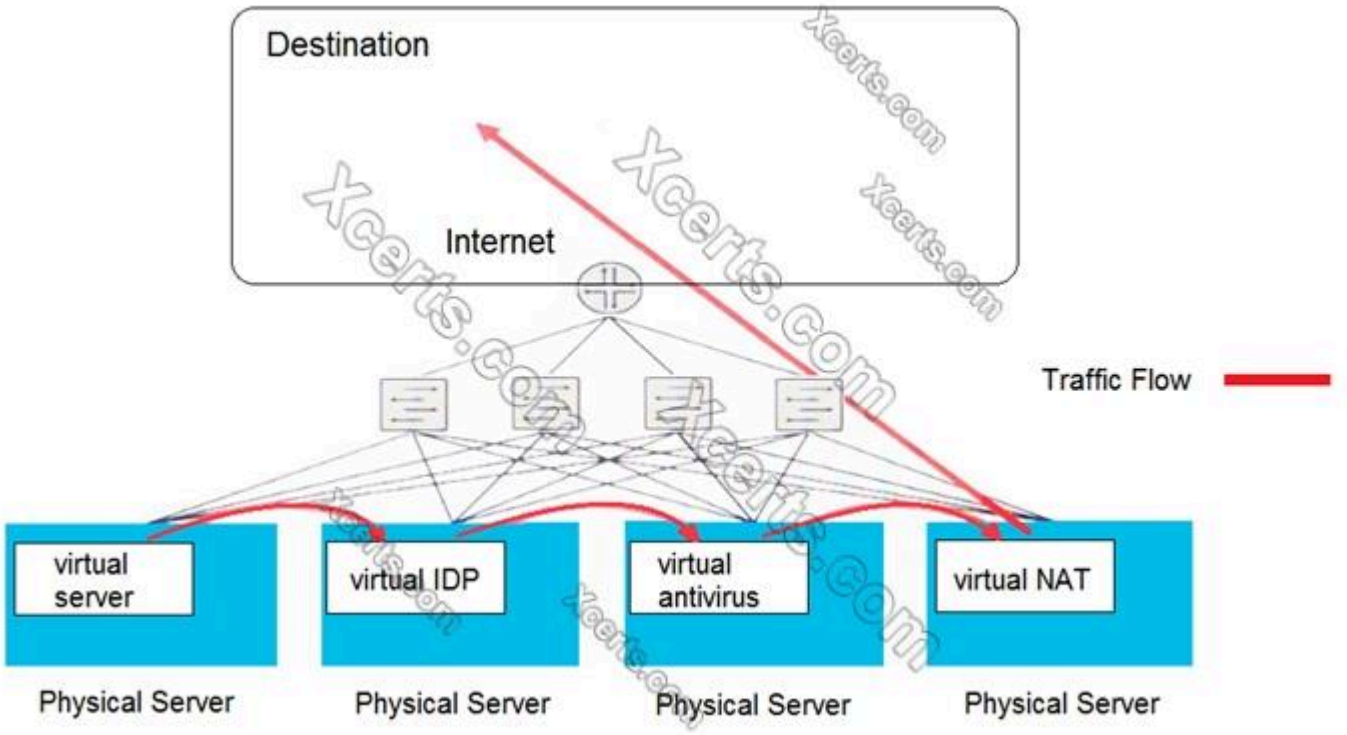
11. You are concerned about malicious attachments being transferred to your e-mail server at work through encrypted channels. You want to block these malicious files using your SRX Series device.
Which two features should you use in this scenario? (Choose two.)

- [ ] A. Sky ATP SMTP scanning
- [ ] B. Sky ATP HTTP scanning
- [ ] C. SSL forward proxy
- [ ] D. SSL reverse proxy

Answer(s): A C

---

12. Click the Exhibit button.



Which type of security solution is shown in this exhibit?

A. service chain model

B. centralized model

C. inline security model

D. de-centralized model

Answer(s): A

---

13. You are designing an Internet security gateway (ISG) for your company and are considering a centralized versus a distributed model for ISGs. Which two statements are correct in this scenario? (Choose two.)

- [ ] A. Distributed ISGs typically have less latency compared to centralized ISGs
- [ ] B. Distributed ISGs reduce bandwidth for end users
- [ ] C. Distributed ISGs typically require extra bandwidth for management
- [ ] D. Distributed ISGs are harder to manage compared to centralized ISGs

Answer(s): A D

---

14. You are creating a data center security design. Virtual security functions must be performed on east-west traffic. Security functions must be commissioned and decommissioned frequently, and the least resource- intensive architecture must be used.
In this scenario, what will accomplish this task?

A. all-in-one NFV security devices with device templates

B. service chaining with container-based security functions

C. a security appliance segmented into logical systems

D. filter-based forwarding to direct traffic to the required security devices

Answer(s): A

---

15. What are two reasons for using cSRX over vSRX? (Choose two.)

- [ ] A. cSRX loads faster
- [ ] B. cSRX uses less memory
- [ ] C. cSRX supports the BGP protocol
- [ ] D. cSRX supports IPsec

Answer(s): A B

---

16. You will be managing 1000 SRX Series devices. Each SRX Series device requires basic source NAT to access the Internet. Which product should you use to manage these NAT rules on the SRX Series devices?

A. Security Director

B. CSO

C. Contrail

D. JSA

Answer(s): A

---

17. Which two features are used to stop IP spoofing in and out of your network? (Choose two.)

- [ ] A. GeoIP
- [ ] B. firewall filters
- [ ] C. unicast reverse path forwarding

- [ ] D. IPS

Answer(s): C D

---

18. What are two benefits of the vSRX in a virtualized private or public cloud multitenant environment? (Choose two.)

- [ ] A. full logical systems capabilities
- [ ] B. stateful firewall protection at the tenant edge
- [ ] C. 100GbE interface support
- [ ] D. OSPFv3 capabilities

Answer(s): A B

---

19. You are designing a new network for your organization with the characteristics shown below.
-All traffic must pass inspection by a security device.
-A center-positioned segmentation gateway must provide deep inspection of each packet using 10 Gbps interfaces.
-Policy enforcement must be centrally managed.
Which security model should you choose for your network design?

A. Intrazone Permit

B. trust but verify

C. user-role firewall policies

D. Zero Trust

Answer(s): D

---

20. A hosting company is migrating to cloud-based solutions. Their customers share a physical firewall cluster, subdivided into individual logical firewalls for each customer. Projection data

shows that the cloud service will soon deplete all the resources within the physical firewall. As a consultant, you must propose a scalable solution that continues to protect all the cloud customers while still securing the existing physical network.
In this scenario, which solution would you propose?

A. Deploy a vSRX cluster in front of each customer’s servers while keeping the physical firewall cluster

B. Deploy a software-defined networking solution

C. Remove the physical firewall cluster and deploy vSRX clusters dedicated to each customer’s servers

D. Replace the physical firewall cluster with a higher-performance firewall

Answer(s): C
