

# Juniper

## JN0-334 Exam

### Security, Specialist



Thank you for Downloading JN0-334 exam PDF Demo

You can Buy Latest JN0-334 Full Version Download

<https://www.certkillers.net/Exam/JN0-334>

<https://www.certkillers.net>

## Version: 9.0

---

**Question: 1**

---

What are two examples of RTOs? (Choose two.)

- A. IPsec SA entries
- B. session table entries
- C. fabric link probes
- D. control link heartbeats

---

**Answer: AB**

---

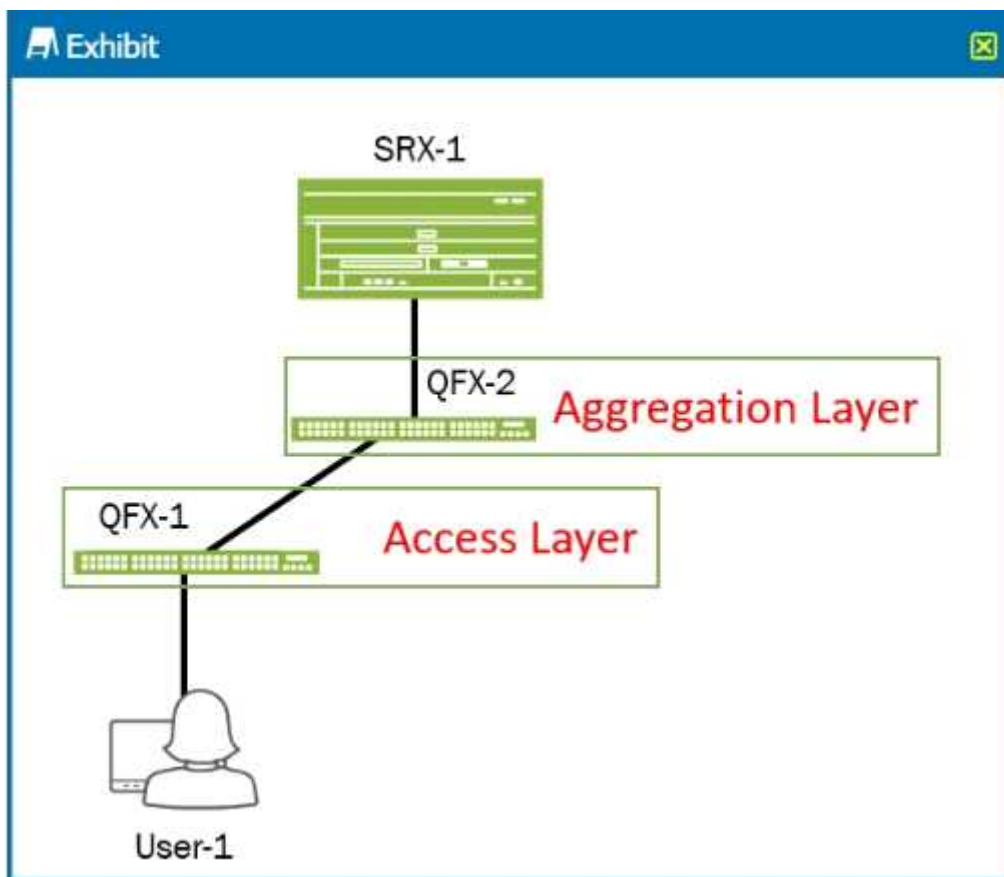
The data plane software creates RTOs for UDP and TCP sessions and tracks state changes. It also synchronizes traffic for IPv4 pass-through protocols such as Generic Routing Encapsulation (GRE) and IPsec. [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-chassis-cluster-data-plane-interfaces#id-45975](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-data-plane-interfaces#id-45975)

---

**Question: 2**

---

Click the Exhibit button.



Referring to the exhibit, you want to deploy Sky ATP with Policy Enforcer to block infected hosts at the access layer.

To complete this task, where should you configure the default gateway for the User-1 device?

- A. the irb interface on QFX-2
- B. the irb interface on QFX-1
- C. the interface of QFX-1 that connects to User-1
- D. the interface on SRX-1 that connects to QFX-2

---

**Answer: A**

---

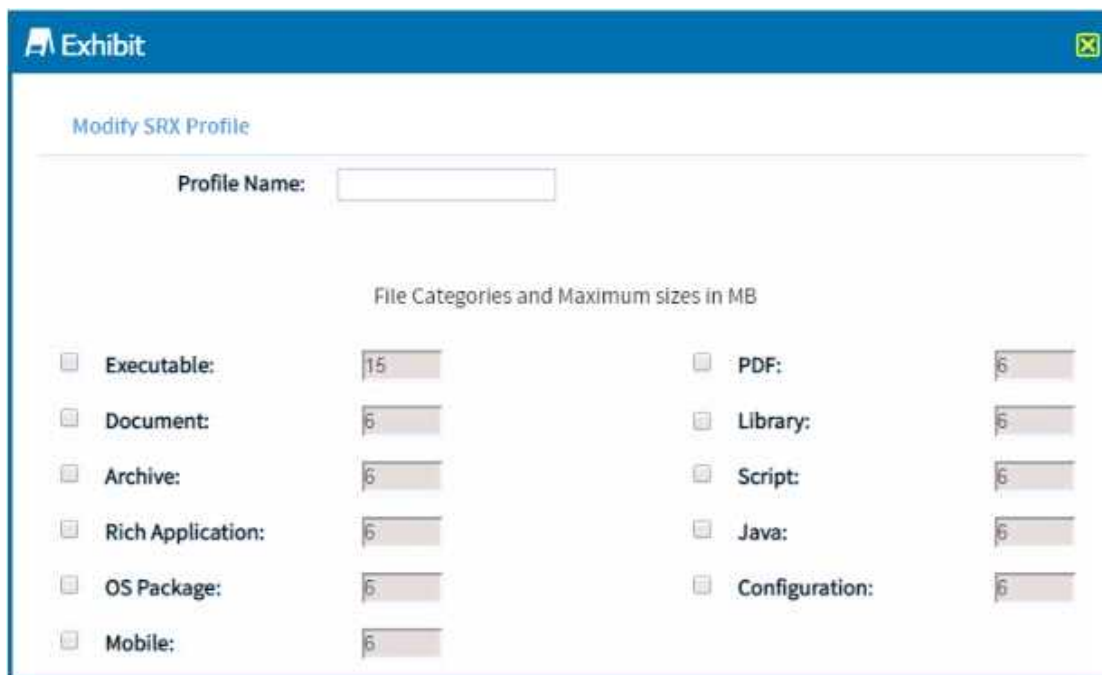
[https://www.juniper.net/documentation/en\\_US/release-independent/nce/topics/example/nce-162-sdsn-example](https://www.juniper.net/documentation/en_US/release-independent/nce/topics/example/nce-162-sdsn-example)

---

### Question: 3

---

Click the Exhibit button.



**Modify SRX Profile**

Profile Name:

File Categories and Maximum sizes in MB

<input type="checkbox"/> Executable:	<input type="text" value="15"/>	<input type="checkbox"/> PDF:	<input type="text" value="6"/>
<input type="checkbox"/> Document:	<input type="text" value="6"/>	<input type="checkbox"/> Library:	<input type="text" value="6"/>
<input type="checkbox"/> Archive:	<input type="text" value="6"/>	<input type="checkbox"/> Script:	<input type="text" value="6"/>
<input type="checkbox"/> Rich Application:	<input type="text" value="6"/>	<input type="checkbox"/> Java:	<input type="text" value="6"/>
<input type="checkbox"/> OS Package:	<input type="text" value="6"/>	<input type="checkbox"/> Configuration:	<input type="text" value="6"/>
<input type="checkbox"/> Mobile:	<input type="text" value="6"/>		

You need to have the JATP solution analyzer .jar, .xls, and .doc files.

Referring to the exhibit, which two file types must be selected to accomplish this task? (Choose two.)

- A. Java
- B. library
- C. document
- D. executable

---

**Answer: AC**

---

[https://www.juniper.net/documentation/en\\_US/release-independent/sky-atp/topics/reference/general/sky-atp-profile-overview](https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/reference/general/sky-atp-profile-overview)

---

#### Question: 4

---

Which three features are parts of Juniper Networks' AppSecure suite? (Choose three.)

- A. AppQoE
- B. APBR
- C. Secure Application Manager
- D. AppQoS
- E. AppFormix

---

**Answer: ABD**

---

Reference:

[https://www.juniper.net/documentation/en\\_US/junos/information-products/pathway-](https://www.juniper.net/documentation/en_US/junos/information-products/pathway-)

[pages/security/security-application-identification.pdf](#)

---

**Question: 5**

---

Which two statements are correct about server-protection SSP proxy? (Choose two.)

- A. The server-protection SSL proxy intercepts the server certificate.
- B. The server-protection SSL proxy is also known as SSL reverse proxy.
- C. The server-protection SSL proxy forwards the server certificate after modification.
- D. The server-protection SSL proxy acts as the server from the client's perspective.

---

**Answer: BD**

---

[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-ssl-proxy](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ssl-proxy)

---

**Question: 6**

---

Which statement is true about high availability (HA) chassis clusters for the SRX Series device?

- A. Cluster nodes require an upgrade to HA compliant Routing Engines.
- B. Cluster nodes must be connected through a Layer 2 switch.
- C. There can be active/passive or active/active clusters.
- D. HA clusters must use NAT to prevent overlapping subnets between the nodes.

---

**Answer: C**

---

---

**Question: 7**

---

What are two types of attack objects used by IPS on SRX Series devices? (Choose two.)

- A. protocol anomaly-based attacks
- B. spam-based attacks
- C. signature-based attacks
- D. DDoS-based attacks

---

**Answer: AC**

---

---

**Question: 8**

---

When considering managed sessions, which configuration parameter determines how full the session table must be to implement the early age-out function? (Choose two)

- A. session service timeout
- B. high watermark
- C. low watermark
- D. policy rematch

---

**Answer: AB**

---

---

**Question: 9**

---

You are asked to improve resiliency for individual redundancy groups in an SRX4600 chassis cluster. Which two features would accomplish this task? (Choose two.)

- A. IP address monitoring
- B. control link recovery
- C. interface monitoring
- D. dual fabric links

---

**Answer: BD**

---

---

**Question: 10**

---

What are two elements of a custom IDP/IPS attack object? (Choose two.)

- A. the attack signature
- B. the severity of the attack
- C. the destination zone
- D. the exempt rulebase

---

**Answer: AB**

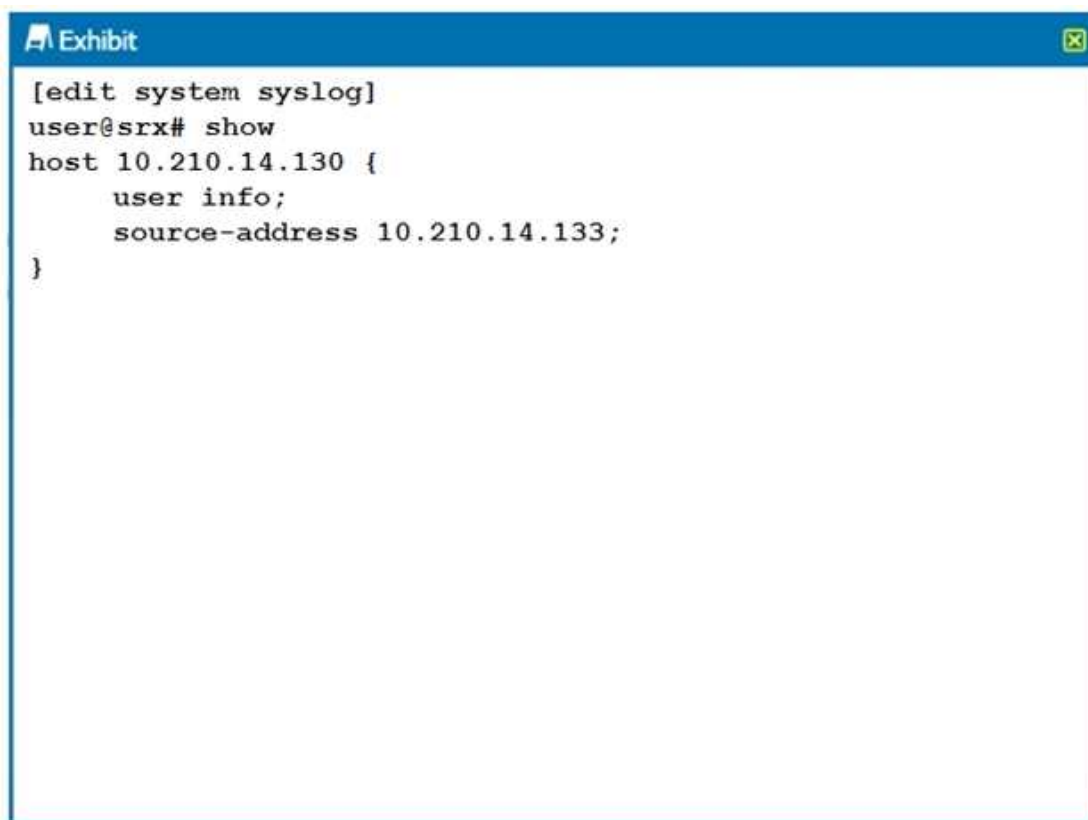
---

---

**Question: 11**

---

Click the Exhibit button.



```
[edit system syslog]
user@srx# show
host 10.210.14.130 {
    user info;
    source-address 10.210.14.133;
}
```

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

- A. The log is being stored on the local Routing Engine.
- B. The log is being sent to a remote server.
- C. The syslog is configured for a user facility.
- D. The syslog is configured for an info facility.

---

**Answer: BC**

---

[https://www.juniper.net/documentation/en\\_US/junos/topics/reference/configuration-statement/syslog-edit-system](https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/syslog-edit-system)

---

### Question: 12

---

Your network uses a remote e-mail server that is used to send and receive e-mails for your users. In this scenario, what should you do to protect users from receiving malicious files through e-mail?

- A. Deploy Sky ATP IMAP e-mail protection
- B. Deploy Sky ATP MAPI e-mail protection
- C. Deploy Sky ATP SMTP e-mail protection
- D. Deploy Sky ATP POP3 e-mail protection

---

**Answer: C**

---

---

**Question: 13**

---

Which two statements are true about virtualized SRX Series devices? (Choose two.)

- A. vSRX cannot be deployed in transparent mode.
- B. cSRX can be deployed in routed mode.
- C. cSRX cannot be deployed in routed mode.
- D. vSRX can be deployed in transparent mode.

---

**Answer: BD**

---

[https://www.juniper.net/documentation/en\\_US/csrX/information-products/pathway-pages/security-csrX-contrail-guide-pwp.pdf](https://www.juniper.net/documentation/en_US/csrX/information-products/pathway-pages/security-csrX-contrail-guide-pwp.pdf)

---

**Question: 14**

---

A routing change occurs on an SRX Series device that involves choosing a new egress interface. In this scenario, which statement is true for all affected current sessions?

- A. The current session are torn down only if the policy-rematch option has been enabled.
- B. The current sessions do not change.
- C. The current sessions are torn down and go through first path processing based on the new route.
- D. The current sessions might change based on the corresponding security policy.

---

**Answer: B**

---

<https://forums.juniper.net/t5/ScreenOS-Firewalls-NOT-SRX/Affect-of-Route-change-on-Session/m-p/27810#M11385>

---

**Question: 15**

---

What information does JIMS collect from domain event log sources? (Choose two.)

- A. For user login events, JIMS collects the username and group membership information.
- B. For device login events, JIMS collects the device IP address and operating system version.
- C. For device login events, JIMS collects the device IP address and machine name information.
- D. For user login events, JIMS collects the login source IP address and username information.

---

**Answer: CD**

---

---

**Question: 16**

---

Which statement describes the AppTrack module in AppSecure?

- A. The AppTrack module provides enforcement with the ability to block traffic, based on specific



applications.

- B. The AppTrack module provides control by the routing of traffic, based on the application.
- C. The AppTrack module identifies the applications that are present in network traffic.
- D. The AppTrack module provides visibility and volumetric reporting of application usage on the network.

---

**Answer: D**

---

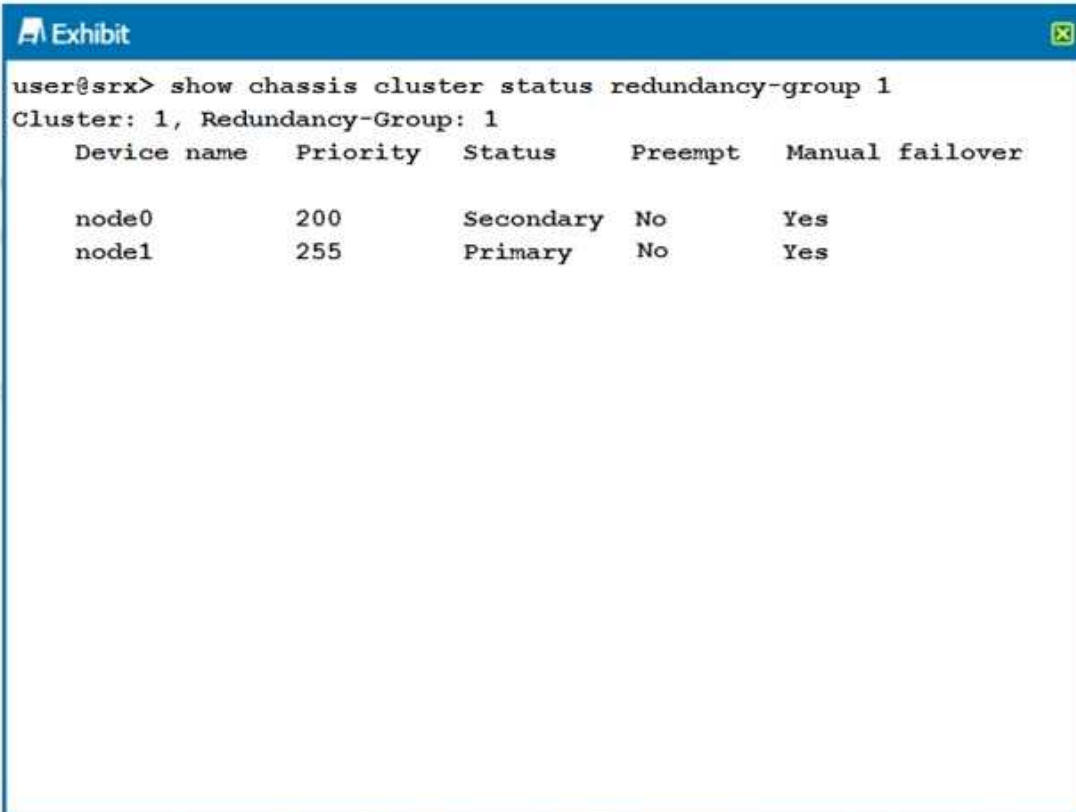
[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-application-tracking](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-application-tracking)

---

**Question: 17**

---

Click the Exhibit button.



```
user@srx> show chassis cluster status redundancy-group 1
Cluster: 1, Redundancy-Group: 1
  Device name  Priority  Status    Preempt  Manual failover
  -----
  node0        200     Secondary No        Yes
  node1        255     Primary   No        Yes
```

Which two statements describe the output shown in the exhibit? (Choose two.)

- A. Node 0 is passing traffic for redundancy group 1.
- B. Redundancy group 1 experienced an operational failure.
- C. Redundancy group 1 was administratively failed over.
- D. Node 1 is passing traffic for redundancy group1.

---

**Answer: CD**

---

---

**Question: 18**

---

Which statement is true about JATP incidents?

- A. Incidents have an associated threat number assigned to them.
- B. Incidents are sorted by category, followed by severity.
- C. Incidents consist of all the events associated with a single threat.
- D. Incidents are always automatically mitigated.

---

**Answer: A**

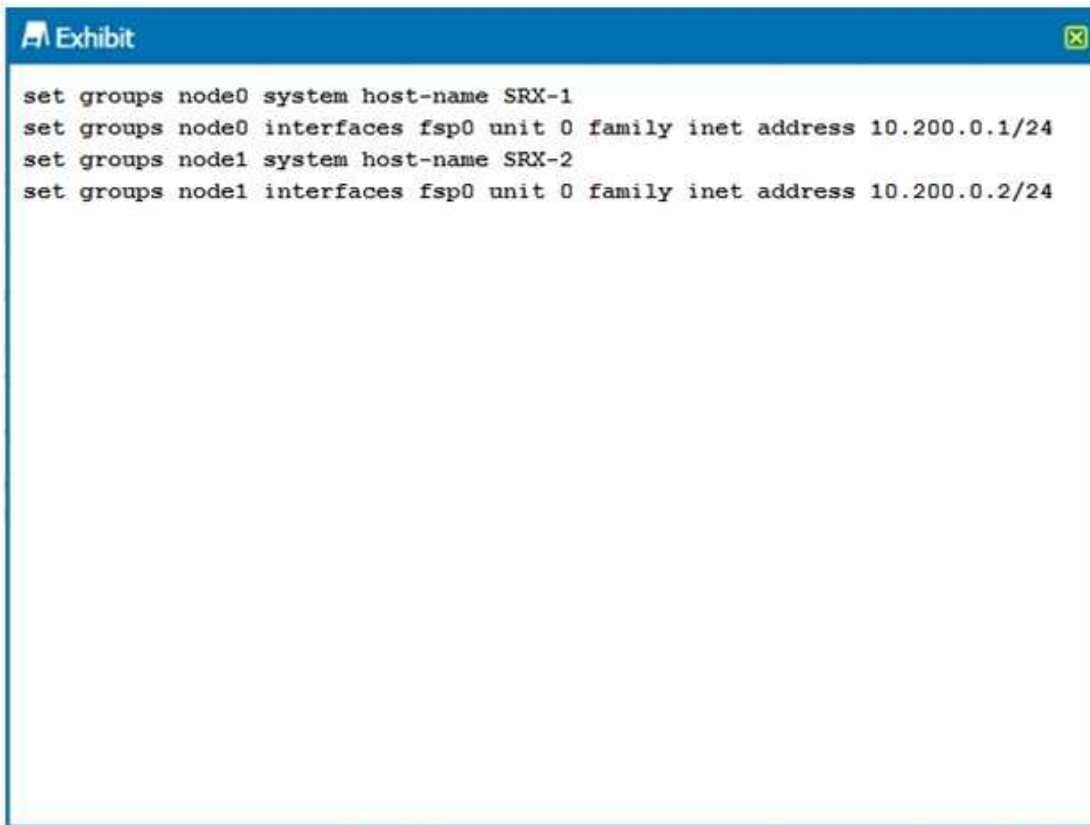
---

---

**Question: 19**

---

Click the Exhibit button.



```
set groups node0 system host-name SRX-1
set groups node0 interfaces fsp0 unit 0 family inet address 10.200.0.1/24
set groups node1 system host-name SRX-2
set groups node1 interfaces fsp0 unit 0 family inet address 10.200.0.2/24
```

You are configuring an SRX chassis cluster with the node-specific hostname and management address. Referring to the exhibit, which configuration completes this requirement?

- A)  

```
set groups node$ interfaces fsp0 unit 0 family inet address 10.200.0.254/24 master-only
```
- B)  

```
set apply-groups node0
set apply-groups node1
```
- C)  

```
set apply-groups ${node}
```

D)

```
set groups node0 interfaces fxp0 unit 0 family inet address 10.200.0.254/24 master-only
set groups node1 interfaces fxp0 unit 0 family inet address 10.200.0.254/24 master-only
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

---

**Answer: C**

---

<https://kb.juniper.net/InfoCenter/index?page=content&id=KB31080>

---

### Question: 20

---

You must ensure that all encrypted traffic passing through your SRX device uses strong protocols and ciphers.

Which feature should you implement to satisfy this requirement?

- A. SSL proxy
- B. AppSecure
- C. JIMS
- D. JATP

---

**Answer: A**

---

---

### Question: 21

---

You want to deploy vSRX in Amazon Web Services (AWS) virtual private clouds (VPCs).

Which two statements are true in this scenario? (Choose two.)

- A. The vSRX devices serving as local enforcement points for VPCs can be managed by a centralized Junos Space Network Director instance.
- B. MPLS LSPs can be used to connect vSRXs in different VPCs.
- C. IPsec tunnels can be used to connect vSRX in different VPCs.
- D. The vSRX devices serving as local enforcement points for VPCs can be managed by a centralized Junos Space Security Director instance.

---

**Answer: CD**

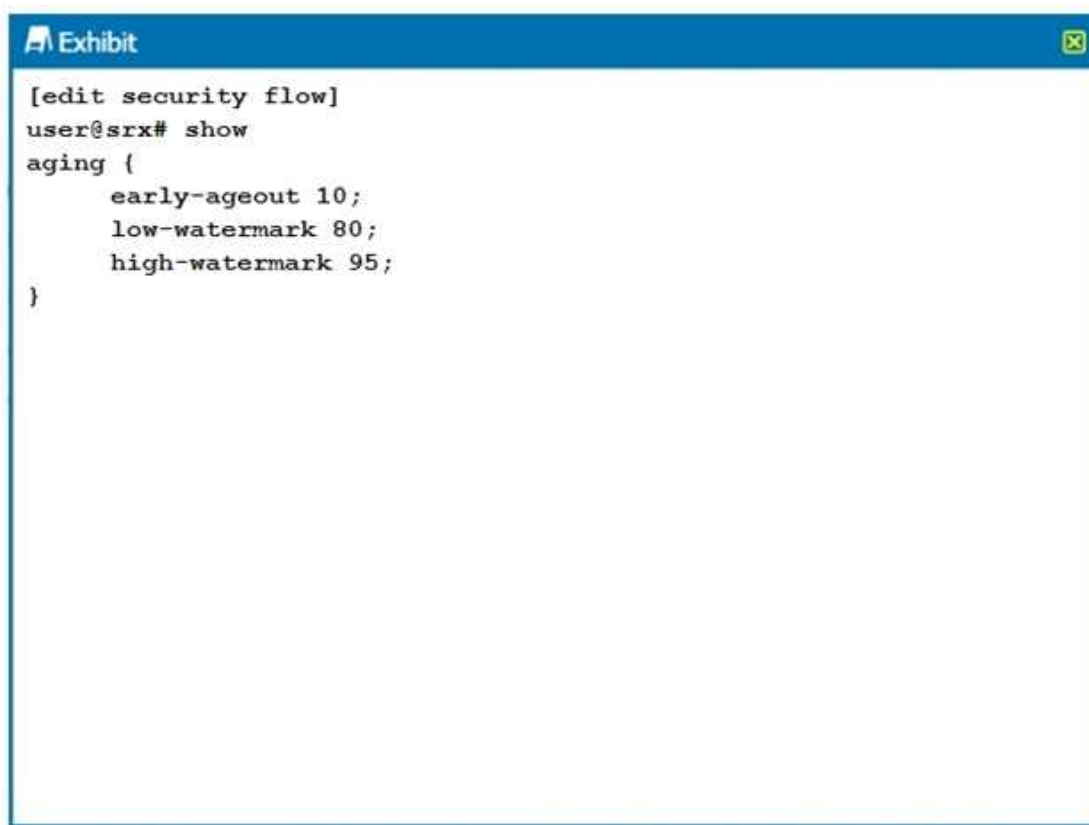
---

---

### Question: 22

---

Click the Exhibit button.



```
[edit security flow]
user@srx# show
aging {
    early-ageout 10;
    low-watermark 80;
    high-watermark 95;
}
```

Which two statements are true about the configuration shown in the exhibit? (Choose two.)

- A. The session is removed from the session table after 10 seconds of inactivity.
- B. The session is removed from the session table after 10 milliseconds of inactivity.
- C. Aggressive aging is triggered if the session table reaches 95% capacity.
- D. Aggressive aging is triggered if the session table reaches 80% capacity.

---

**Answer: AC**

---

---

**Question: 23**

---

Which feature supports sandboxing of zero-day attacks?

- A. Sky ATP
- B. SSL proxy
- C. ALGs
- D. high availability

---

**Answer: A**

---

---

**Question: 24**

---

Which two statements describe how rules are used with Juniper Secure Analytics? (Choose two.)

- A. When a rule is triggered, JSA can respond by sending an e-mail to JSA administrators.
- B. Rules are defined on Junos Space Security Director, and then pushed to JSA log collectors.
- C. A rule defines matching criteria and actions that should be taken when an events matches the rule.
- D. When a rule is triggered, JSA can respond by blocking all traffic from a specific source address.

---

**Answer: AC**

---

---

**Question: 25**

---

Which solution should you use if you want to detect known attacks using signature-based methods?

- A. SSL proxy
- B. JIMS
- C. IPS
- D. ALGs

---

**Answer: C**

---

---

**Question: 26**

---

The AppQoE module of AppSecure provides which function?

- A. The AppQoE module provides application-based routing.
- B. The AppQoE module prioritizes important applications.
- C. The AppQoE module provides routing, based on network conditions.
- D. The AppQoE module blocks access to risky applications.

---

**Answer: C**

---

[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-appqoe#id0e28](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-appqoe#id0e28)

---

**Question: 27**

---

You are configuring a client-protection SSL proxy profile.  
Which statement is correct in this scenario?

- A. A server certificate is not used but a root certificate authority is used.
- B. A server certificate and root certificate authority are not used.
- C. A server certificate is used but a root certificate authority is not used.
- D. A server certificate and a root certificate authority are both used.

---

**Answer: D**

---

---

**Question: 28**

---

Which two statements describe application-layer gateways (ALGs)? (Choose two.)

- A. ALGs are designed for specific protocols that require multiple sessions.
- B. ALGs are used with protocols that use multiple ports.
- C. ALGs can only be configured using Security Director.
- D. ALGs are designed for specific protocols that use a single TCP session.

---

**Answer: AB**

---

---

**Question: 29**

---

What is the default session timeout value for ICMP and UDP traffic?

- A. 30 seconds
- B. 30 minutes
- C. 60 seconds
- D. 5 minutes

---

**Answer: C**

---

---

**Question: 30**

---

What are two valid JIMS event log sources? (Choose two.)

- A. Microsoft Windows Server 2012 audit logs
- B. Microsoft Active Directory server event logs
- C. Microsoft Exchange Server event logs
- D. Microsoft Active Directory audit logs

---

**Answer: BC**

---

---

**Question: 31**

---

You must configure JSA to accept events from an unsupported third-party log source. In this scenario, what should you do?

- A. Separate event collection and flow collection on separate collectors.
- B. Configure an RPM for a third-party device service module.
- C. Configure JSA to silently discard unsupported log types.
- D. Configure a universal device service module.

---

**Answer: D**

---

**Question: 32**

Which two solutions provide a sandboxing feature for finding zero-day malware threats? (Choose two.)

- A. Sky ATP
- B. UTM
- C. JATP
- D. IPS

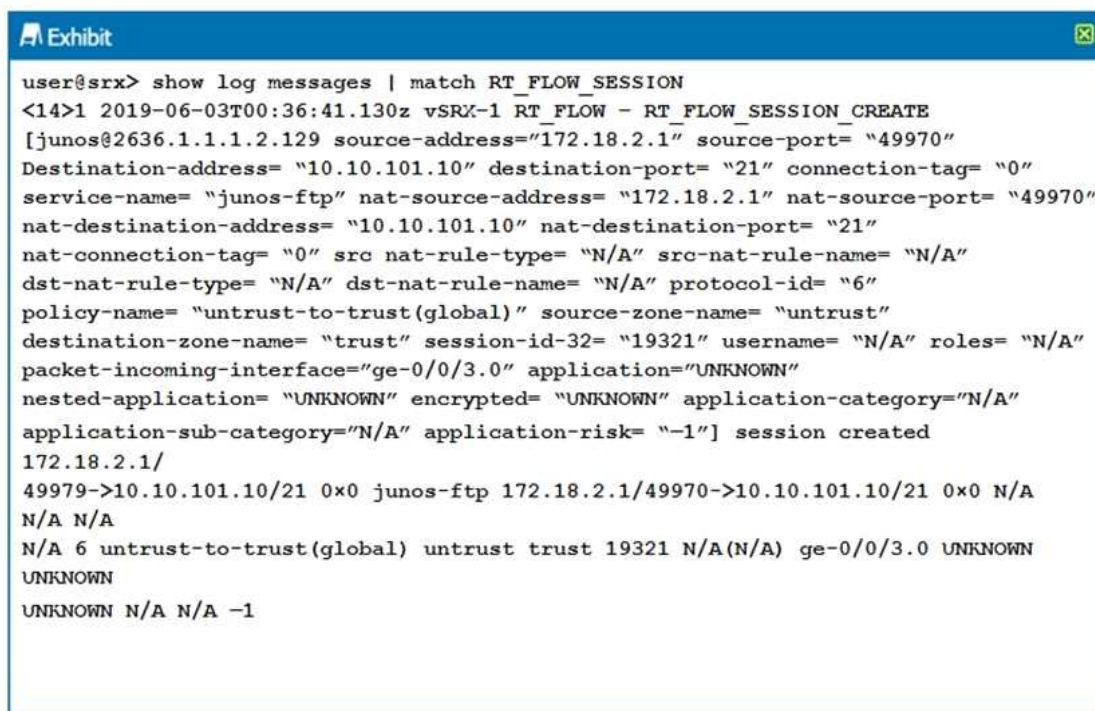
---

**Answer: AC**

---

**Question: 33**

Click the Exhibit button.



```

user@srx> show log messages | match RT_FLOW_SESSION
<14>1 2019-06-03T00:36:41.130z vSRX-1 RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.129 source-address="172.18.2.1" source-port= "49970"
Destination-address= "10.10.101.10" destination-port= "21" connection-tag= "0"
service-name= "junos-ftp" nat-source-address= "172.18.2.1" nat-source-port= "49970"
nat-destination-address= "10.10.101.10" nat-destination-port= "21"
nat-connection-tag= "0" src nat-rule-type= "N/A" src-nat-rule-name= "N/A"
dst-nat-rule-type= "N/A" dst-nat-rule-name= "N/A" protocol-id= "6"
policy-name= "untrust-to-trust(global)" source-zone-name= "untrust"
destination-zone-name= "trust" session-id-32= "19321" username= "N/A" roles= "N/A"
packet-incoming-interface="ge-0/0/3.0" application="UNKNOWN"
nested-application= "UNKNOWN" encrypted= "UNKNOWN" application-category="N/A"
application-sub-category="N/A" application-risk= "-1"] session created
172.18.2.1/
49979->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/49970->10.10.101.10/21 0x0 N/A
N/A N/A
N/A 6 untrust-to-trust(global) untrust trust 19321 N/A(N/A) ge-0/0/3.0 UNKNOWN
UNKNOWN
UNKNOWN N/A N/A -1
  
```

The output shown in the exhibit is displayed in which format?

- A. syslog
- B. WELF
- C. binary
- D. sd-syslog

---

**Answer: D**

---

**Question: 34**

You are using the JIMS Administrator user interface to add multiple SRX client devices. You must share common configuration attributes across the SRX clients without having to re-enter those attributes for each SRX client instance.

Which JIMS Administrator feature would be used to accomplish this task?

- A. JIMS automation
- B. JIMS templates
- C. JIMS client profiles
- D. JIMS client defaults

---

**Answer: B**

---

---

**Question: 35**

---

In an Active/Active chassis cluster deployment, which chassis cluster component is responsible for R/G0 traffic?

- A. the backup routing engine of the primary node
- B. the master routing engine of the secondary node
- C. the primary node
- D. the secondary node

---

**Answer: C**

---

---

**Question: 36**

---

Your manager asks you to find employees that are watching YouTube during office hours. Which AppSecure component would you configure to accomplish this task?

- A. AppQoS
- B. AppFW
- C. AppTrack
- D. AppQoS

---

**Answer: C**

---

---

**Question: 37**

---

What are two types of collectors for the JATP core engine? (Choose two.)

- A. SNMP
- B. e-mail
- C. Web
- D. telemetry

---

**Answer: BC**

---

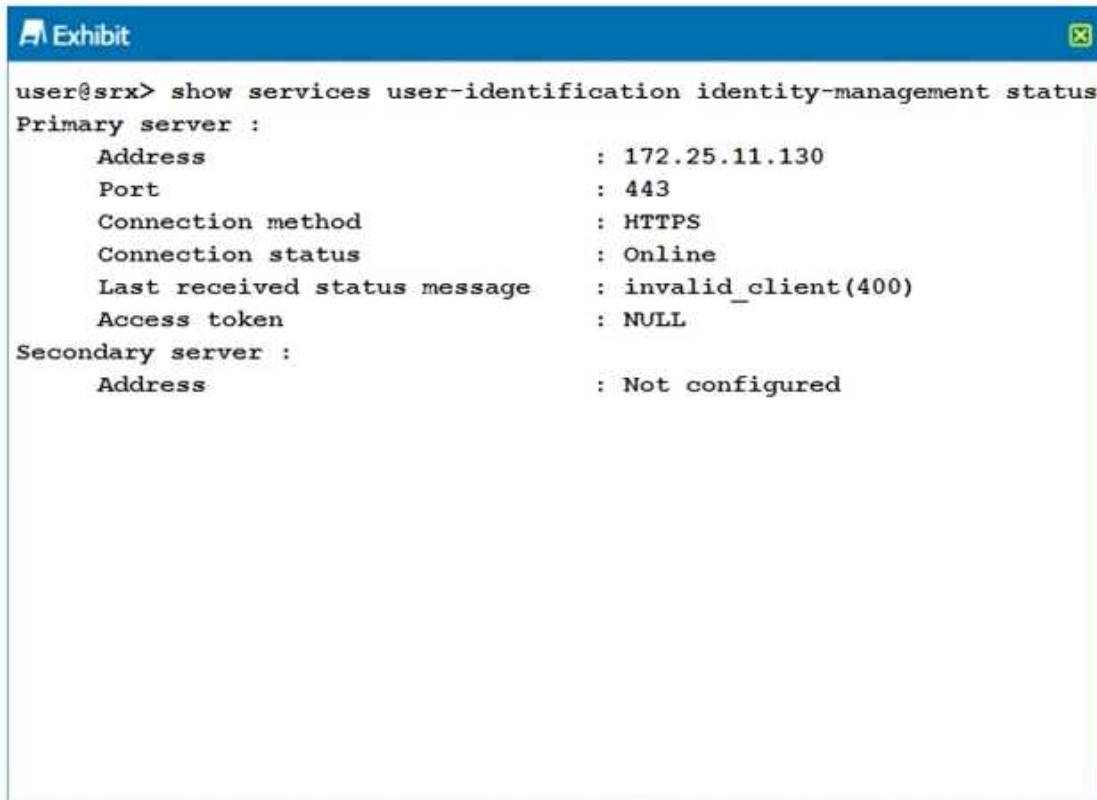


---

**Question: 38**

---

Click the Exhibit button.



```
user@srx> show services user-identification identity-management status
Primary server :
  Address          : 172.25.11.130
  Port             : 443
  Connection method : HTTPS
  Connection status : Online
  Last received status message : invalid_client(400)
  Access token     : NULL
Secondary server :
  Address          : Not configured
```

You have configured your SRX Series device to receive authentication information from a JIMS server. However, the SRX is not receiving any authentication information. Referring to the exhibit, how would you solve the problem?

- A. Use the JIMS Administrator user interface to add the SRX device as client.
- B. Generate an access token on the SRX device that matches the access token on the JIMS server.
- C. Update the IP address of the JIMS server
- D. Change the SRX configuration to connect to the JIMS server using HTTP.

---

**Answer: A**

---

The device obtains an access token after it authenticates to the JIMS server. The device must use this token to query JIMS for user information. Token is used for the user identity information after if authentication is successful and in this case it is stuck in the authentication. Following is the link. ([https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-user-auth-configure-jims](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-configure-jims))

---

**Question: 39**

---

After a software upgrade on an SRX5800 chassis cluster, you notice that both node0 and node1 are in the primary state, when node1 should be secondary. All control and fabric links are operating

normally.

In this scenario, which step must you perform to recover the cluster?

- A. Execute the request system reboot command on node1.
- B. Execute the request system software rollback command on node0.
- C. Execute the request system software add command on node1.
- D. Execute the request system reboot command on node0.

---

**Answer: A**

---

---

**Question: 40**

---

What is the default timeout period for a TCP session in the session table of a Junos security device?

- A. 1 minute
- B. 60 minutes
- C. 15 minutes
- D. 30 minutes

---

**Answer: D**

---

---

**Question: 41**

---

Which security log message format reduces the consumption of CPU and storage?

- A. WELF
- B. BSD syslog
- C. binary
- D. structured syslog

---

**Answer: C**

---

[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/security-binary-logging-understanding](https://www.juniper.net/documentation/en_US/junos/topics/concept/security-binary-logging-understanding)

Security log messages can also be maintained in text-based formats. Because security logging can produce large amounts of data, however, text-based log files can quickly consume storage and CPU resources. Depending on your implementation of security logging, a log file in a binary-based format can provide more efficient use of on-box or off-box storage and improved CPU utilization. Binary format for security log messages is available on all SRX Series devices.

---

**Question: 42**

---

You must block the lateral spread of Remote Administration Tools (RATs) that use SMB to propagate within the network, using the JATP solution.

Which action would accomplish this task?

- A. Configure a new anti-virus configuration rule.
- B. Configure whitelist rules
- C. Configure YARA rules.
- D. Configure the SAML settings.

---

**Answer: C**

---

[https://www.juniper.net/documentation/en\\_US/release-independent/jatp/information-products/pathway-pages/jatp-operators-guide.pdf](https://www.juniper.net/documentation/en_US/release-independent/jatp/information-products/pathway-pages/jatp-operators-guide.pdf) pg 43

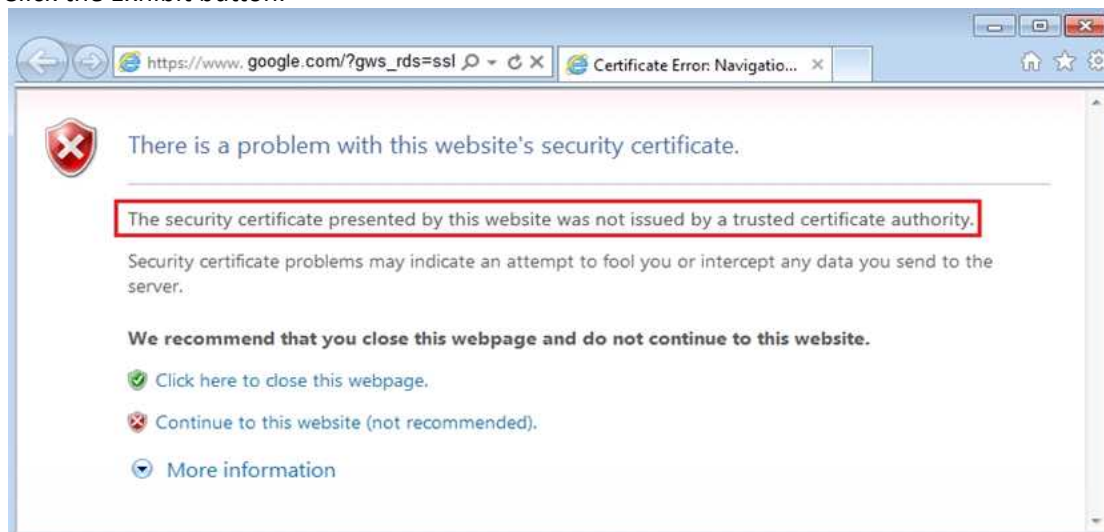
YARA Rules and Lateral Detection Remote Administration Tools (RATs) can be detected using YARA rules. By adding the ability to push YARA rules to Juniper ATP Appliance devices, Juniper ATP Appliance can detect the lateral spread of Remote Administration Tools (RATs) within a network.

---

### Question: 43

---

Click the Exhibit button.



You have implemented SSL proxy client protection. After implementing this feature, your users are complaining about the warning message shown in the exhibit. Which action must you perform to eliminate the warning message?

- A. Configure the SRX Series device as a trusted site in the client Web browsers.
- B. Regenerate the SRX self-signed CA certificate and include the correct organization name.
- C. Import the SRX self-signed CA certificate into the client Web browsers.
- D. Import the SRX self-signed CA certificate into the SRX certificate public store.

---

**Answer: C**

---

---

### Question: 44

---

You are asked to enable AppTrack to monitor application traffic from hosts in the User zone destined to hosts in the Internet zone.

In this scenario, which statement is true?

- A. You must enable the AppTrack feature within the Internet zone configuration.
- B. You must enable the AppTrack feature within the ingress interface configuration associated with the Internet zone.
- C. You must enable the AppTrack feature within the interface configuration associated with the User zone.
- D. You must enable the AppTrack feature within the User zone configuration.

---

**Answer: D**

---

---

**Question: 45**

---

The DNS ALG performs which three functions? (Choose three.)

- A. The DNS ALG performs the IPv4 and IPV6 address transformations.
- B. The DNS ALG performs DNS doctoring.
- C. The DNS ALG modifies the DNS payload in NAT mode.
- D. The DNS ALG performs DNSSEC.
- E. The DNS ALG performs DNS load balancing.

---

**Answer: ABC**

---

---

**Question: 46**

---

When referencing a SSL proxy profile in a security policy, which two statements are correct? (Choose two.)

- A. A security policy can reference both a client-protection SSL proxy profile and a server-protection proxy profile.
- B. If you apply an SSL proxy profile to a security policy and forget to apply any Layer7 services to the security policy, any encrypted traffic that matches the security policy is not decrypted.
- C. A security policy can only reference a client-protection SSL proxy profile or a server-protection SSL proxy profile.
- D. If you apply an SSL proxy profile to a security policy and forget to apply any Layer7 services to the security policy, any encrypted traffic that matches the security policy is decrypted.

---

**Answer: BC**

---

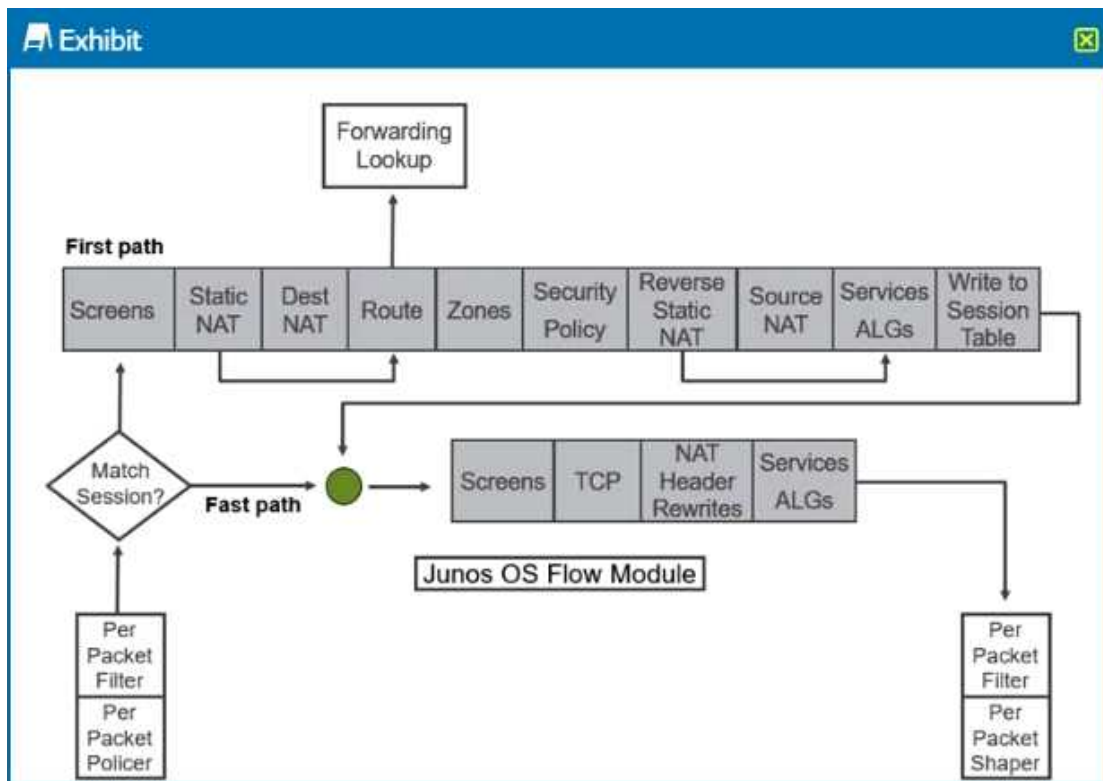
[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-ssl-proxy](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ssl-proxy)

---

**Question: 47**

---

Click the Exhibit button.



Referring to the SRX Series flow module diagram shown in the exhibit, where is IDP/IPS processed?

- A. Forwarding Lookup
- B. Services ALGs
- C. Screens
- D. Security Policy

**Answer: D**

**Question: 48**

Click the Exhibit button.

```
Exhibit
user@srx> show log messages | match RT_FLOW_SESSION
Jun 3 00:36:41 vSRX-1 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
172.18.2.1/
57929->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/57929->10.10.101.10/21 0x0 N/A
N/A N/A N/A 6 untrust-to-trust(global) untrust trust 19307 N/A(N/A) ge-0/0/3.0
UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
```

The output shown in the exhibit is displayed in which format?

- A. syslog
- B. sd-syslog
- C. binary
- D. WELF

---

**Answer: A**

---

---

### Question: 49

---

You want to collect events and flows from third-party vendors. Which solution should you deploy to accomplish this task?

- A. Log Director
- B. JSA
- C. Policy Enforcer
- D. Contrail

---

**Answer: B**

---

---

### Question: 50

---

Which feature is used when you want to permit traffic on an SRX Series device only at specific times?

- A. scheduler
- B. pass-through authentication

- C. ALGs
- D. counters

---

**Answer: A**

---

---

**Question: 51**

---

You must fine tune an IPS security policy to eliminate false positives. You want to create exemptions to the normal traffic examination for specific traffic.

Which two parameters are required to accomplish this task? (Choose two.)

- A. source IP address
- B. destination IP address
- C. destination port
- D. source port

---

**Answer: AB**

---

---

**Question: 52**

---

Which two statements describe JSA? (Choose two.)

- A. Security Director must be used to view third-party events from JSA flow collectors.
- B. JSA supports events and flows from Junos devices, including third-party devices.
- C. JSA events must be manually imported into Security Directory using an SSH connection.
- D. JSA can be used as a log node with Security Director or as a standalone solution.

---

**Answer: BD**

---

---

**Question: 53**

---

What is the maximum number of supported interfaces on a vSRX hosted in a VMware environment?

- A. 4
- B. 10
- C. 3
- D. 12

---

**Answer: B**

---

---

**Question: 54**

---

You have deployed JSA and you need to view events and network activity that match rule criteria

a. You must view this data using a single interface.

Which JSA feature should you use in this scenario?

- A. Log Collector

- B. Assets
- C. Network Activity
- D. Offense Manager

---

**Answer: C**

---

---

**Question: 55**

---

Which two settings must be enabled on the hypervisor in a vSRX deployment to ensure proper chassis cluster operation? (Choose two.)

- A. Control links must operate in promiscuous mode.
- B. Control links must have an MTU of 9000.
- C. Fabric links must operate in promiscuous mode.
- D. Fabric links must have an MTU of 9000.

---

**Answer: AD**

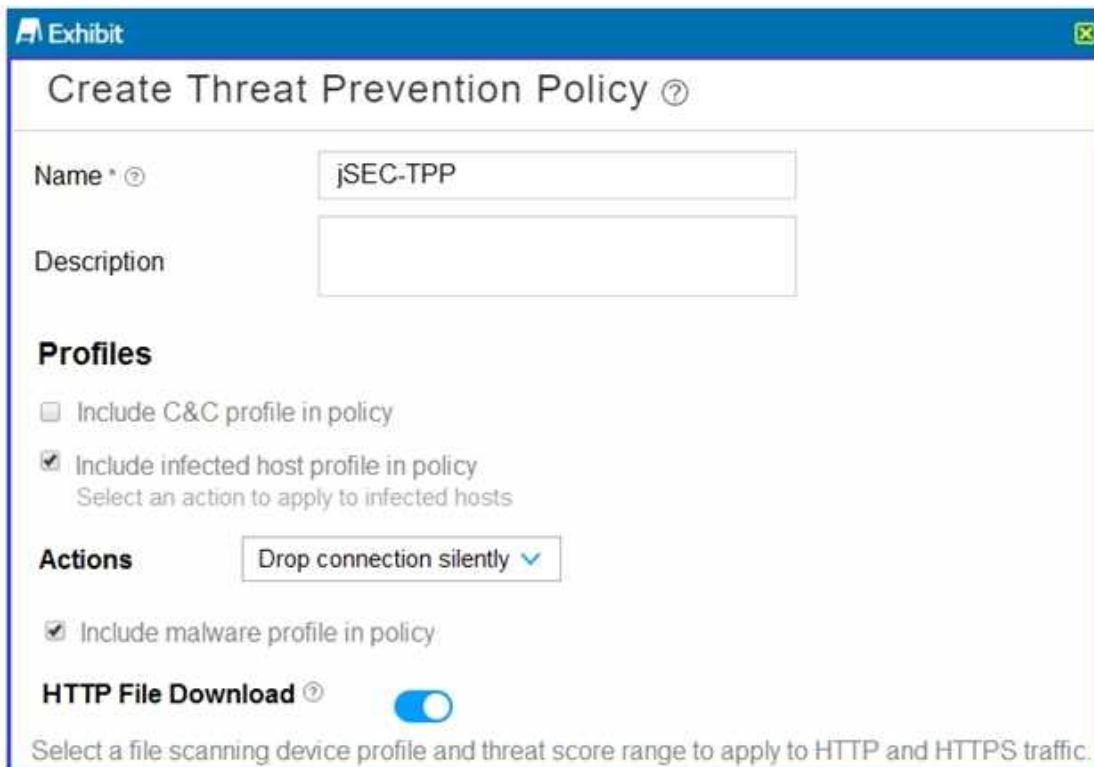
---

---

**Question: 56**

---

Click the Exhibit button.



Referring to the exhibit, which statement is true?

- A. Hosts are always able to communicate through the SRX Series device no matter the threat score assigned to them on the infected host feed.



- B. Hosts are unable to communicate through the SRX Series device after being placed on the infected host feed with a high enough threat score.
- C. Malicious HTTP file downloads are never blocked.
- D. Malicious HTTP file downloads are always blocked.

---

**Answer: B**

---

---

### Question: 57

---

You want to use Sky ATP to protect your network; however, company policy does not allow you to send any files to the cloud.

Which Sky ATP feature should you use in this situation?

- A. Only use on-premises local Sky ATP server anti-malware file scanning.
- B. Only use cloud-based Sky ATP file hash lookups.
- C. Only use on-box SRX anti-malware file scanning.
- D. Only use cloud-based Sky ATP file blacklists.

---

**Answer: B**

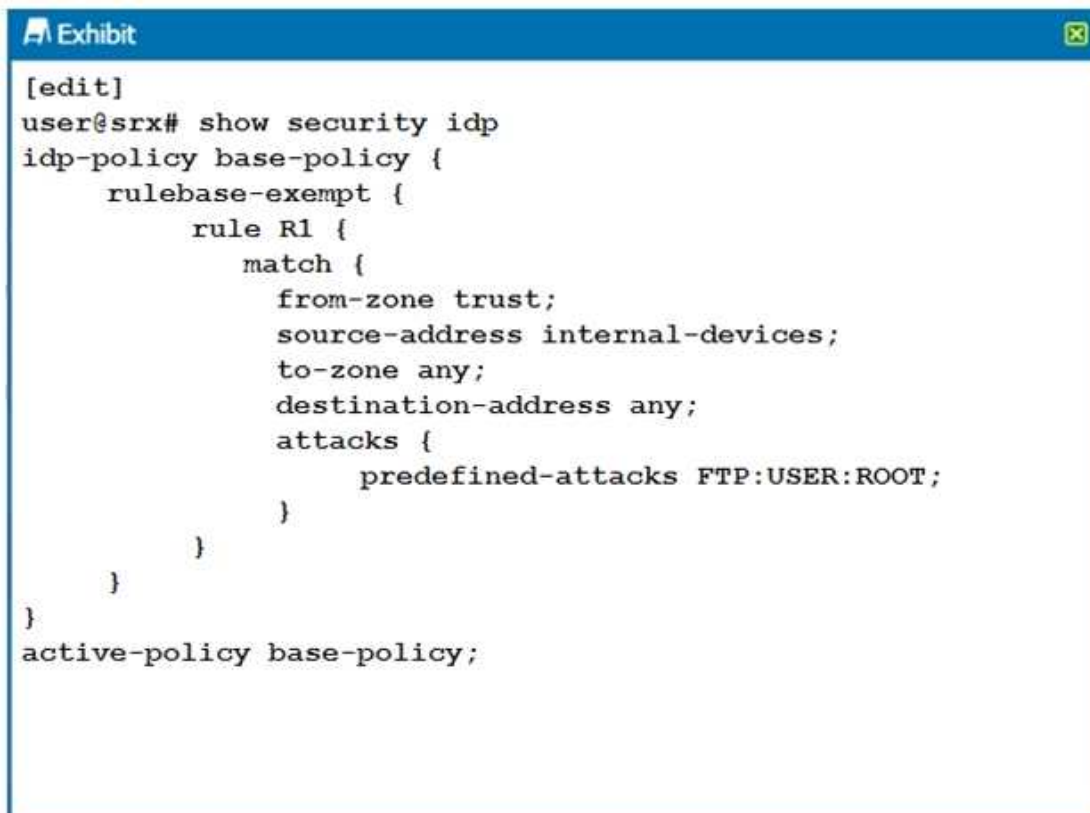
---

---

### Question: 58

---

Click the Exhibit button.



```
[edit]
user@srx# show security idp
idp-policy base-policy {
    rulebase-exempt {
        rule R1 {
            match {
                from-zone trust;
                source-address internal-devices;
                to-zone any;
                destination-address any;
                attacks {
                    predefined-attacks FTP:USER:ROOT;
                }
            }
        }
    }
}
active-policy base-policy;
```

Referring to the exhibit, which statement is true?

- A. IDP blocks root users.
- B. IDP closes the connection on matched sessions.
- C. IDP ignores the connection on matched sessions.
- D. IDP blocks all users.

---

**Answer: C**

---

---

**Question: 59**

---

How many nodes are configurable in a chassis cluster using SRX Series devices?

- A. 2
- B. 4
- C. 6
- D. 8

---

**Answer: A**

---

---

**Question: 60**

---

Which two functions are performed by Juniper Identity Management Service (JIMS)? (Choose two.)

- A. JIMS synchronizes Active Directory authentication information between a primary and secondary JIMS server.
- B. JIMS forwards Active Directory authentication information to SRX Series client devices.
- C. JIMS collects and maintains a database of authentication information from Active Directory domains.
- D. JIMS replicates Active Directory authentication information to non-trusted Active Directory domain controllers.

---

**Answer: AC**

---

[https://www.juniper.net/documentation/en\\_US/junos/topics/reference/configuration-statement/services-user-identification-identity-management-connection-primary](https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/services-user-identification-identity-management-connection-primary)

---

**Question: 61**

---

What are two management methods for cSRX? (Choose two.)

- A. Network Director
- B. J-Web
- C. CLI
- D. Contrail

---

**Answer: BC**

---

---

**Question: 62**

---

You are deploying the Junos application firewall feature in your network. In this scenario, which two elements are mapped to applications in the application system cache? (Choose two.)

- A. destination port
- B. source port
- C. destination IP address
- D. source IP address

---

**Answer: AC**

---

---

**Question: 63**

---

Which two protocols are supported for Sky ATP advanced anti-malware scanning? (Choose two.)

- A. POP3
- B. MAPI
- C. IMAP
- D. SMTP

---

**Answer: CD**

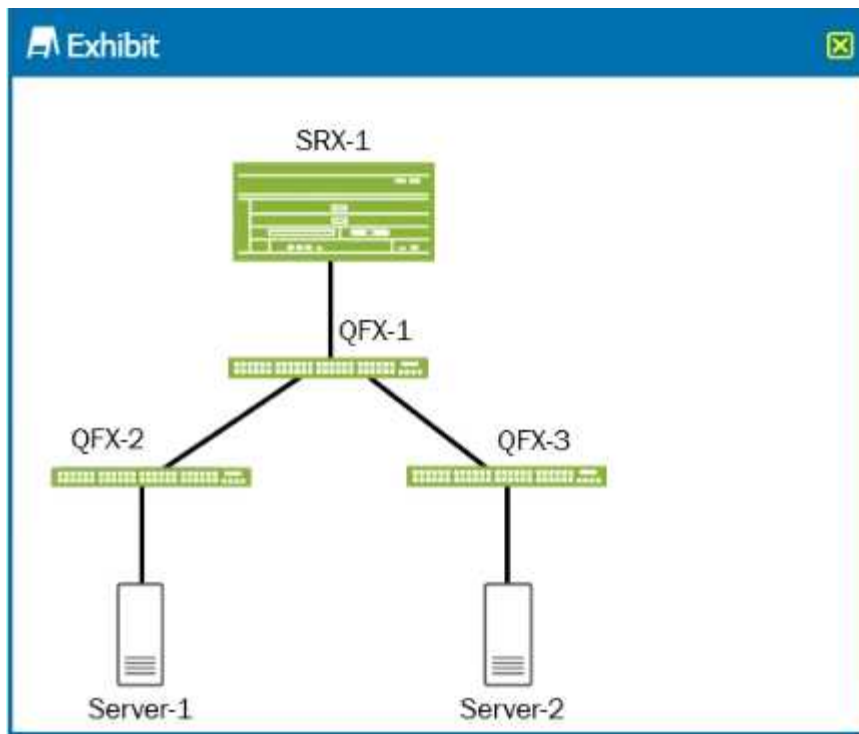
---

---

**Question: 64**

---

Click the Exhibit button.



Referring to the exhibit, which two devices are considered to be part of the secure fabric site with Policy Enforcer? (Choose two.)

- A. Server-2
- B. SRX-1
- C. Server-1
- D. QFX-1

---

**Answer: BD**

---

---

**Question: 65**

---

You are asked to convert two standalone SRX Series devices to a chassis cluster deployment. You must ensure that your IPsec tunnels will be compatible with the new deployment. In this scenario, which two interfaces should be used when binding your tunnel endpoints? (Choose two.)

- A. pp0
- B. reth
- C. lo0
- D. ge

---

**Answer: BD**

---

---

**Question: 66**

---

Which of the following lists the correct order that the Sky ATP pipeline evaluates traffic?

- A. Cache lookup. Static Analysis. Dynamic Analysis. Antivirus Scanning
- B. Static Analysis. Cache lookup. Antivirus Scanning, Dynamic Analysis
- C. Cache lookup. Antivirus Scanning, Static Analysis, Dynamic Analysis

---

**Answer: C**

---

---

**Question: 67**

---

Which two session parameters would be used to manage space on the session table? (Choose two.)

- A. low watermark
- B. high watermark
- C. TCP MSS
- D. TCP RST

---

**Answer: AB**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-flow-based-session-for-srx-series-devices](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-flow-based-session-for-srx-series-devices)

---

**Question: 68**

---

Click the Exhibit button.

```
user@srx> show log messages
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
no commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
no transient commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
finished loading commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
exporting juniper.conf
...
Aug 3 15:47:51 chiron idpd[2678]: IDP_POLICY_LOAD_SUCCEEDED: IDP
policy[/var/db/idpd/bins/idpengine.bin.gz.v] and
detector[/var/db/idpd/sec-repository/installed-detector/libidp-detector.so.tgz.v]
loaded successfully (Regular load).
Aug 3 15:47:51 chiron idpd[2678]: IDP_COMMIT_COMPLETED: IDP policy commit is
complete.
...
Aug 3 15:47:51 chiron chiron sc_set_flow_max_sessions: max sessions set 16384
```

You examine the log file shown in the exhibit after running the set security idp active-policy command.

Which two statements are true in this scenario? (Choose two.)

- A. The IDP policy compiled successfully.
- B. The IDP policy loaded successfully.

- C. The IDP hit cache is set to 16384.
- D. The entire configuration was committed.

---

**Answer: AB**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-idp-policies](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policies)- overview

---

### Question: 69

---

Click the Exhibit button.

```
[edit schedulers]
user@srx# show
scheduler 1 {
    daily {
        start-time 01:00 stop-time 03:00;
    }
}
```

You have configured the scheduler shown in the exhibit to prevent users from accessing certain websites from 1:00 PM to 3:00 PM Monday through Friday. This policy will remain in place until further notice. When testing the policy, you determine that the websites are still accessible during the restricted times.

In this scenario, which two actions should you perform to solve the problem? (Choose two.)

- A. Add the saturday exclude parameter and the sunday exclude parameter to ensure weekends are excluded from the schedule.
- B. Use the 13:00 parameter and the 15:00 parameter when specifying the time.
- C. Use the start-date parameter to specify the date for each Monday and use the stop-date parameter to specify the date for each Friday.
- D. Use the PM parameter when specifying the time in the schedule.

---

**Answer: AB**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/reference/configuration-statement/schedulers-edit-scheduler](https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/schedulers-edit-scheduler)

---

### Question: 70

---

After performing a software upgrade on an SRX5800 chassis cluster, you notice that node1 is in the primary state and node0 is in the backup state. Your network standards dictate that node0 should be in the primary state.

In this scenario, which command should be used to comply with the network standards?

- A. request chassis cluster failover redundancy-group 254 node 1
- B. request chassis cluster failover redundancy-group 0 node 0

- C. request chassis cluster failover redundancy-group 254 mode 0
- D. request chassis cluster failover redundancy-group 0 node 1

---

**Answer: B**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-chassis-cluster-redundancy-group-failover](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-redundancy-group-failover)

---

### Question: 71

---

Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 19068, Policy name: trust-to-untrust/15, Timeout: 1800, Valid
Resource information : FTP ALG, 1, 0
  In: 172.20.104.10/58479 --> 172.18.1.2/21;tcp, Conn Tag: 0x0, If: ge-0/0/3.0,
Pkts: 42, Bytes: 1796,
  Out: 172.18.1.2/21 --> 172.20.104.10/58479;tcp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 43, Bytes: 2739,
```

Which two statements are true about the session shown in the exhibit? (Choose two.)

- A. Two security policies are required for bidirectional traffic flow.
- B. The ALG was enabled by manual configuration.
- C. The ALG was enabled by default.
- D. One security policy is required for bidirectional traffic flow.

---

**Answer: AB**

---

---

### Question: 72

---

Which two statements describe superflows in Juniper Secure Analytics? (Choose two.)

- A. JSA only supports Type A and Type C superflows.
- B. Superflows can negatively impact licensing limitations.
- C. Disk space usage is reduced on the JSA device.
- D. Superflows combine many flows into a single flow.

---

**Answer: CD**

---

---

### Question: 73

---

Which three statements are true about the difference between cSRX-based virtual security deployments and vSRX-based virtual security deployments? (Choose three.)

- A. vSRX provides Layer 2 to Layer 7 secure services and cSRX provides Layer 4 to Layer 7 secure services.
- B. cSRX requires less storage and memory space for a given deployment than vSRX-based solutions.
- C. cSRX-based solutions are more scalable than vSRX-based solutions.

- D. vSRX and cSRX both provide Layer 2 to Layer 7 secure services.
- E. vSRX provides faster deployment time and faster reboots compared to cSRX.

---

**Answer: ABC**

---

Reference: [https://www.juniper.net/documentation/en\\_US/day-one-books/topics/concept/juniper-vsrx-versus-csrx](https://www.juniper.net/documentation/en_US/day-one-books/topics/concept/juniper-vsrx-versus-csrx)

---

### Question: 74

---

You are deploying a vSRX into a vSphere environment which applies the configuration from a bootable ISO file containing the juniper.conf file. After the vSRX boots and has the configuration applied, you make additional device specific configuration changes, commit, and reboot the device. Once the device finishes rebooting, you notice the specific changes you made are missing but the original configuration is applied.

In this scenario, what is the problem?

- A. Configuration changes do not persist after reboots on vSRX.
- B. The juniper.conf file was not applied to the vSRX.
- C. The configuration file is corrupt.
- D. The ISO file is still mounted on the vSRX.

---

**Answer: D**

---

Reference: <https://www.juniper.net/documentation/us/en/software/vsrx/vsrx-kvm/topics/task/security-vsrx-kvm-bootstrap-config>

---

### Question: 75

---

When working with network events on a Juniper Secure Analytics device, flow records come from which source?

- A. tap port
- B. SPAN
- C. switch
- D. mirror

---

**Answer: B**

---

Reference: [https://www.juniper.net/documentation/en\\_US/jsa7.3.1/jsa-arch-deployment-guide/topics/concept/jsa-ad-jsa-events-and-flows](https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-arch-deployment-guide/topics/concept/jsa-ad-jsa-events-and-flows)

---

### Question: 76

---

You are troubleshooting advanced policy-based routing (APBR). Which two actions should you perform in this scenario? (Choose two.)



- A. Verify that the APBR profiles are applied to the egress zone.
- B. Verify inet.0 for correct route leaking.
- C. Review the APBR statistics for matching rules and route modifications.
- D. Inspect the application system cache for the application entry.

---

**Answer: CD**

---

---

**Question: 77**

---

Which two statements describe SSL proxy on SRX Series devices? (Choose two.)

- A. SSL proxy supports TLS version 1.2.
- B. Client-protection is also known as reverse proxy.
- C. SSL proxy is supported when enabled within logical systems.
- D. SSL proxy relies on Active Directory to provide secure communication.

---

**Answer: AC**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-user-auth-ssl-tls](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-ssl-tls)

---

**Question: 78**

---

Click the Exhibit button.

The screenshot shows a dialog box titled "Add SRX Client Configuration". The fields are as follows:

- Template: \*\*\*\*\*
- SRX IP Address: 172.25.11.1
- Description: vsrx1
- WebAPI Configuration:  WebAPI (Legacy) [Configure]
- IPv6 Reporting:  Enable
- SRX Client to JIMS:
  - Client ID: vsrx1
  - Client Secret: \*\*\*\*\*
  - Token Lifetime: 1200 (60 - 36000 sec(s))

Buttons: OK, Cancel

Referring to the exhibit, which two values in the JIMS SRX client configuration must match the values

configured on the SRX client? (Choose two.)

- A. IPv6 Reporting
- B. Client ID
- C. Client Secret
- D. Token Lifetime

---

**Answer: BC**

---

Reference: [https://www.juniper.net/documentation/en\\_US/jims/topics/task/configuration/jims-srx-configuring](https://www.juniper.net/documentation/en_US/jims/topics/task/configuration/jims-srx-configuring)

---

**Question: 79**

---

Which two statements apply to policy scheduling? (Choose two.)

- A. A policy refers to many schedules.
- B. A policy refers to one schedule.
- C. Multiple policies can refer to the same schedule.
- D. A policy stays active regardless of when the schedule is active.

---

**Answer: BC**

---

Reference: [https://www.juniper.net/documentation/en\\_US/cso5.4.0/topics/concept/cp-about-schedule-overview](https://www.juniper.net/documentation/en_US/cso5.4.0/topics/concept/cp-about-schedule-overview)

---

**Question: 80**

---

Click the Exhibit button.

```
user@srx> show configuration services
advanced-anti-malware {
  policy TPP {
    http {
      inspection-profile default profile;
      action block;
      notification {
        log;
      }
    }
    verdict-threshold 7;
    fallback-options {
      action permit;
      notification {
        log;
      }
    }
    default-notification {
      log;
    }
    whitelist-notification {
      log;
    }
    blacklist-notification {
      log;
    }
  }
}
```

```
user@srx> show configuration security policies
from-zone Client to-zone Internet {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          advanced-anti-malware-policy TPP;
        }
      }
    }
  }
}
```

You have deployed Sky ATP to protect your network from attacks so that users are unable to download malicious files. However, after a user attempts to download a malicious file, they are still able to communicate through the SRX Series device.

Referring to the exhibit, which statement is correct?

- A. Change the security policy from a standard security policy to a unified security policy.
- B. Remove the fallback options in the advanced anti-malware policy.
- C. Configure a security intelligence policy and apply it to the security policy.
- D. Lower the verdict threshold in the advanced anti-malware policy.

---

**Answer: C**

---

---

### Question: 81

---

Which default protocol and port are used for JIMS to SRX client communication?

- A. WMI over TCP; port 389
- B. ADSI over TCP; port 389
- C. HTTPS over TCP; port 443
- D. RPC over TCP, port 135

---

**Answer: C**

---

Reference: [https://www.juniper.net/documentation/en\\_US/jims/topics/task/configuration/jims-certificate-configure#:~:text=By%20default%2C%20the%20HTTPS%20port%20is%20443.&text=The%20JIMS%20server%20communicates%20with,Firewall%20to%20allow%20this%20communication](https://www.juniper.net/documentation/en_US/jims/topics/task/configuration/jims-certificate-configure#:~:text=By%20default%2C%20the%20HTTPS%20port%20is%20443.&text=The%20JIMS%20server%20communicates%20with,Firewall%20to%20allow%20this%20communication)

---

### Question: 82

---

Which statement about the control link in a chassis cluster is correct?

- A. A cluster can have redundant control links.
- B. Recovering from a control link failure requires a reboot.
- C. The control link heartbeats contain the configuration file of the nodes.
- D. The control messages sent over the link are encrypted by default.

---

**Answer: A**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-chassis-cluster-dual-control-links](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-dual-control-links)

---

### Question: 83

---

Data plane logging operates in which two modes? (Choose two.)

- A. syslog
- B. binary
- C. event
- D. stream

---

**Answer: CD**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/system-logging-for-a-security-device](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/system-logging-for-a-security-device)

---

**Question: 84**

---

Where is AppSecure executed in the flow process on an SRX Series device?

- A. screens
- B. security policy
- C. zones
- D. services

---

**Answer: D**

---

---

**Question: 85**

---

Which two statements about JIMS high availability are true? (Choose two.)

- A. JIMS supports high availability through the installation of the primary and secondary JIMS servers.
- B. SRX clients are configured with the shared virtual IP (VIP) address of the JIMS server.
- C. SRX clients are configured with the unique IP addresses of the primary and secondary JIMS servers.
- D. SRX clients synchronize authentication tables with both the primary and secondary JIMS servers.

---

**Answer: AC**

---

---

**Question: 86**

---

What is the correct step sequence used when Sky ATP analyzes a file?

- A. static analysis -> cache lookup -> antivirus scanning -> dynamic analysis
- B. cache lookup -> static analysis -> antivirus scanning -> dynamic analysis
- C. cache lookup -> antivirus scanning -> static analysis -> dynamic analysis
- D. dynamic analysis -> static analysis -> antivirus scanning -> cache lookup

---

**Answer: C**

---

Reference: [https://www.juniper.net/documentation/en\\_US/release-independent/sky-atp/information-products/pathway-pages/sky-atp-admin-guide.pdf](https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/pathway-pages/sky-atp-admin-guide.pdf) page 9

---

**Question: 87**

---

Which two statements describe IPS? (Choose two.)

- A. IPS can be used to prevent future attacks from occurring.
- B. IPS dynamically sends policy changes to SRX Series devices.
- C. IPS inspects up to Layer 4 in the OSI model.
- D. IPS inspects up to Layer 7 in the OSI model.

---

**Answer: AD**

---

---

**Question: 88**

---

You must deploy AppSecure in your network to block risky applications. In this scenario, which two AppSecure features are required? (Choose two.)

- A. AppFW
- B. AppID
- C. APBR
- D. AppTrack

---

**Answer: BD**

---

---

**Question: 89**

---

What are three primary functions of JATP? (Choose three.)

- A. detection
- B. encryption
- C. optimization
- D. analytics
- E. mitigation

---

**Answer: ADE**

---

---

**Question: 90**

---

You want to support reth LAG interfaces on a chassis cluster. What must be enabled on the interconnecting switch to accomplish this task?

- A. RSTP
- B. 802.3ad
- C. LLDP
- D. swfab

---

**Answer: B**

---

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-chassis-cluster](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster)- redundant-ethernet-lag-interfaces

---

**Question: 91**

---

Which three statements are correct about fabric interfaces on the SRX5800? (Choose three.)

- A. Fabric interfaces must be user-assigned interfaces.
- B. Fabric interfaces must have a user-assigned IP address.
- C. Fabric interfaces must be same interface type.
- D. Fabric interfaces must be on the same Layer 2 segment.
- E. Fabric interfaces must be system-assigned interfaces.

---

**Answer: CDE**

---

Reference: <[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-chassis-cluster-data-plane-interfaces](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-data-plane-interfaces)>

## Thank You for trying JN0-334 PDF Demo

To try our JN0-334 Full Version Download visit link below

<https://www.certkillers.net/Exam/JN0-334>

## Start Your JN0-334 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your JN0-334 preparation with actual exam questions.

<https://www.certkillers.net>