

JN0-334.VCEplus.premium.exam.65q

Number: JN0-334
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

JN0-334

Security, Specialist (JNCIS-SEC)



Exam A

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

Correct Answer: CD

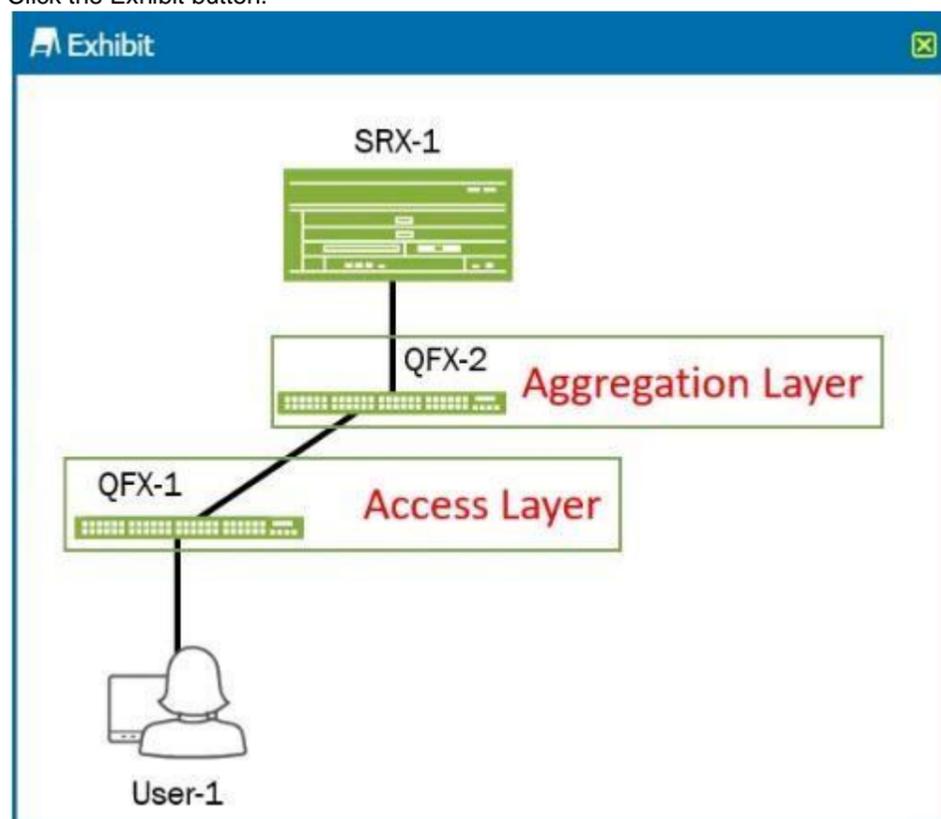
Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: B

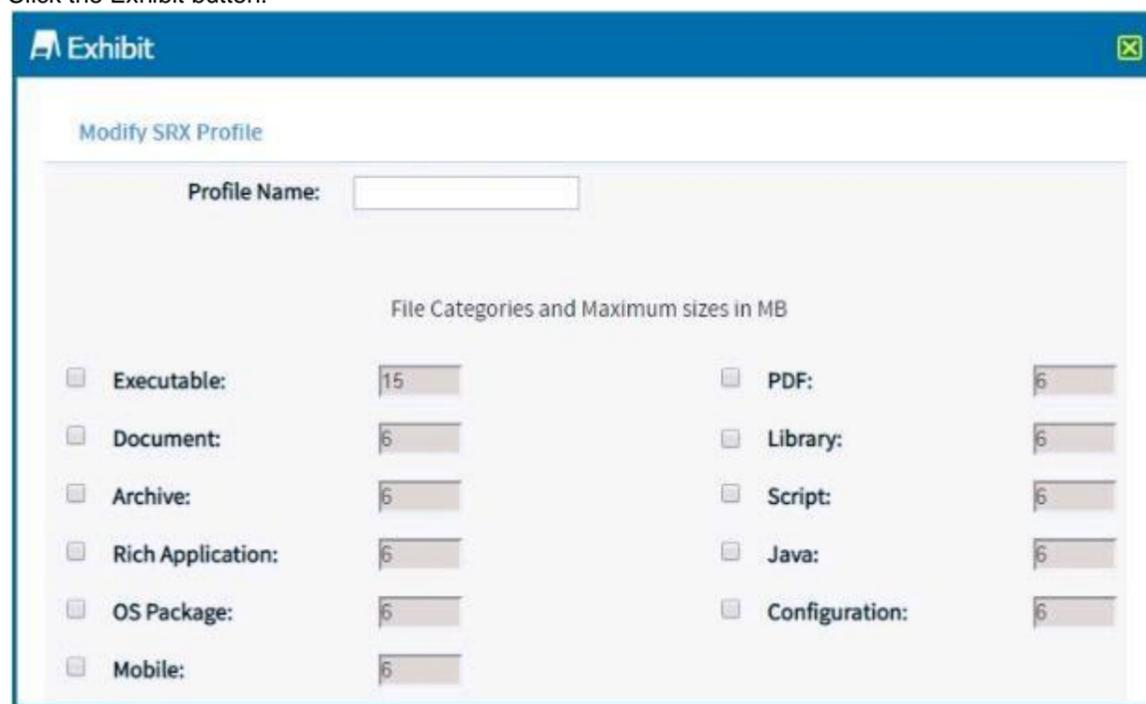
Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Click the Exhibit button.



File Categories and Maximum sizes in MB	
<input type="checkbox"/> Executable:	15
<input type="checkbox"/> Document:	6
<input type="checkbox"/> Archive:	6
<input type="checkbox"/> Rich Application:	6
<input type="checkbox"/> OS Package:	6
<input type="checkbox"/> Mobile:	6
<input type="checkbox"/> PDF:	6
<input type="checkbox"/> Library:	6
<input type="checkbox"/> Script:	6
<input type="checkbox"/> Java:	6
<input type="checkbox"/> Configuration:	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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Reference: 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.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

- A. session service timeout
- B. high watermark
- C. low watermark



D. policy rematch

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Click the Exhibit button.



```

Exhibit
[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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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 sessions 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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



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.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: C

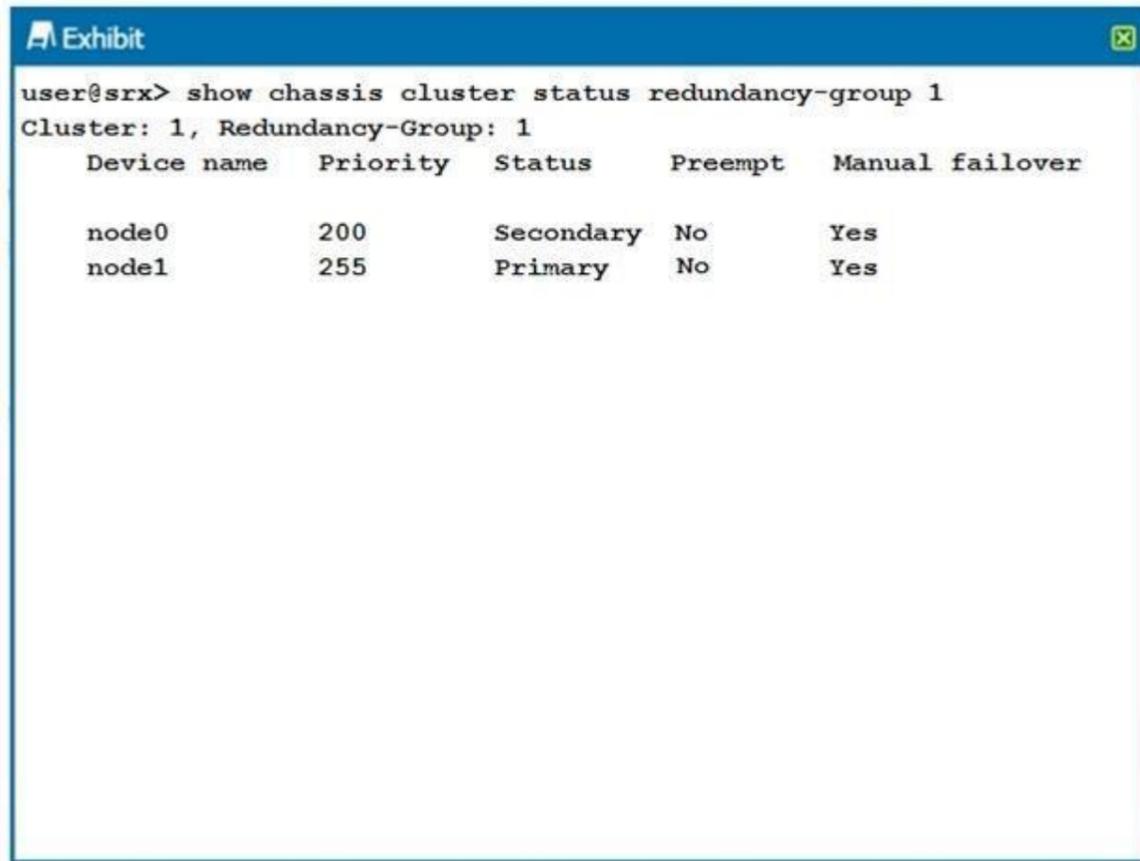
Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: C

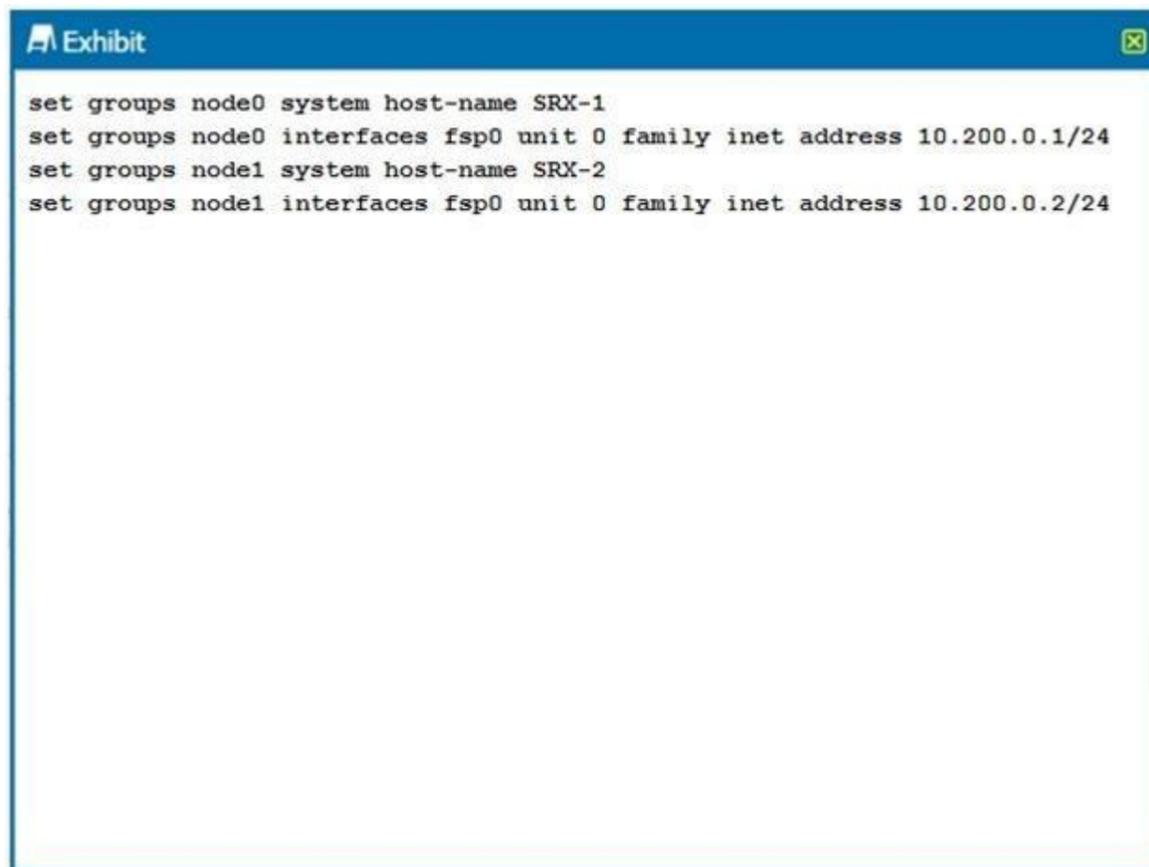
Section: (none)

Explanation

Explanation/Reference:

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 fxp0 unit 0 family inet address 10.200.0.254/24 master-only
```

```
set apply-groups node0
set apply-groups node1
set apply-groups ${node}
```

```
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
```

B.

C.

D.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Click the Exhibit button.

```
Exhibit
[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.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23 Which feature supports sandboxing of zero-day attacks?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 26

The AppQoS module of AppSecure provides which function?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: D
 Section: (none)
 Explanation

Explanation/Reference:

QUESTION 32 Which two solutions provide a sandboxing feature for finding zero-day malware threats?
 (Choose two.)

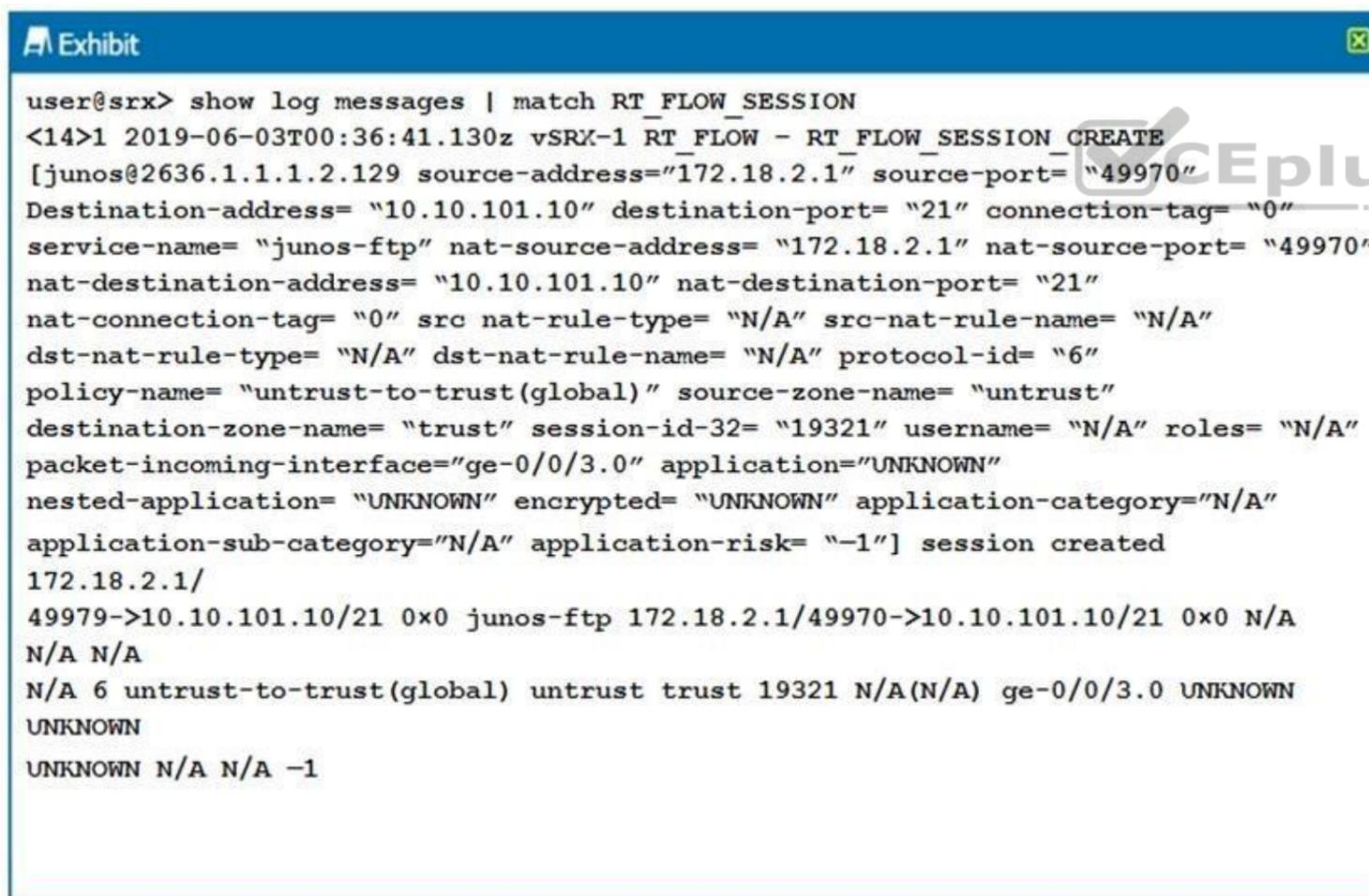
- A. Sky ATP
- B. UTM
- C. JATP
- D. IPS

Correct Answer: AC
 Section: (none)
 Explanation

Explanation/Reference:

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

In an Active/Active chassis cluster deployment, which chassis cluster component is responsible for RG0 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37 What are two types of collectors for the JATP core engine?
(Choose two.)

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

Correct Answer: BC

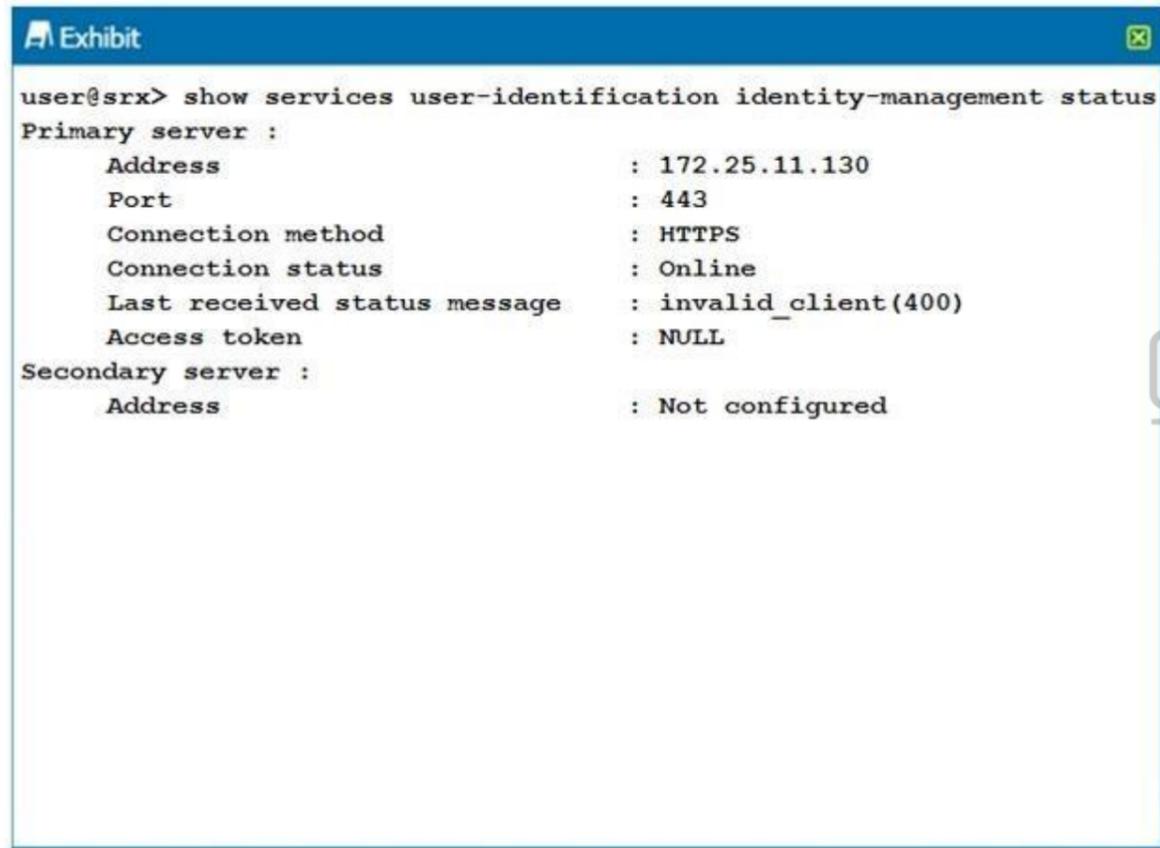
Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 41 Which security log message format reduces the consumption of CPU and storage?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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?

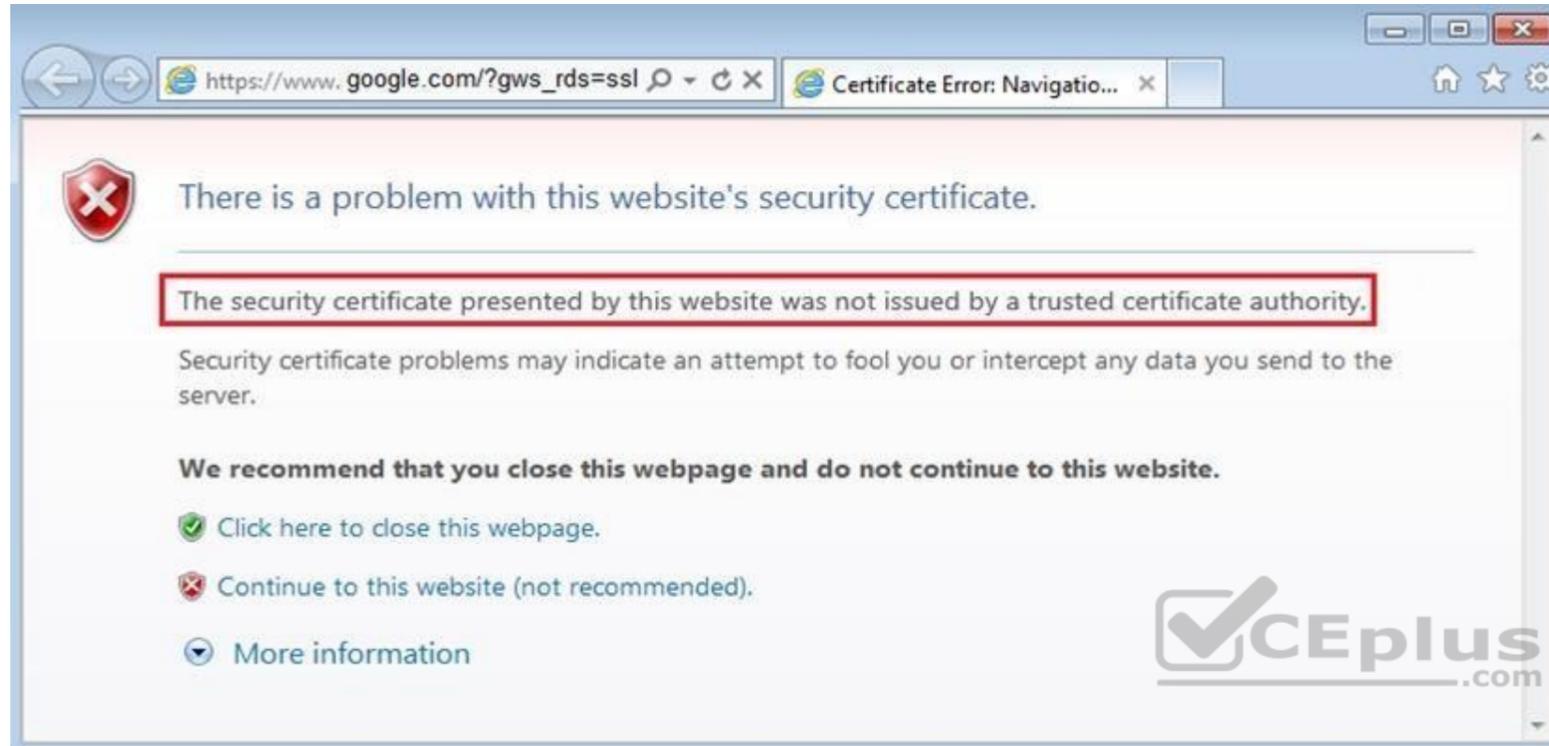
- A. Configure a new anti-virus configuration rule.
- B. Configure whitelist rules.
- C. Configure YARA rules.
- D. Configure the SAML settings.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: AD

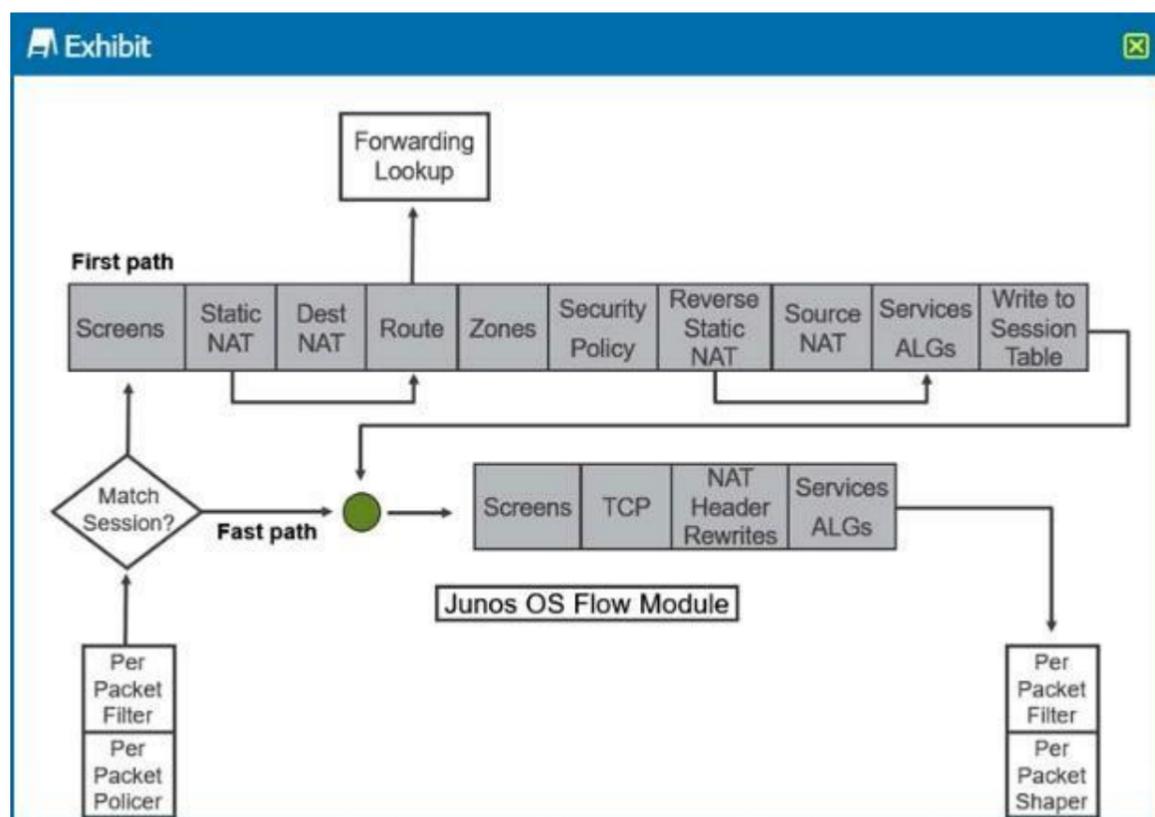
Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



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.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54 You have deployed JSA and you need to view events and network activity that match rule criteria. 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 56

Click the Exhibit button.



Create Threat Prevention Policy

Name *

Description

Profiles

Include C&C profile in policy

Include infected host profile in policy
Select an action to apply to infected hosts

Actions

Include malware profile in policy

HTTP File Download

Select a file scanning device profile and threat score range to apply to HTTP and HTTPS traffic.

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59 How many nodes are configurable in a chassis cluster using SRX Series devices?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63 Which two protocols are supported for Sky ATP advanced anti-malware scanning?

(Choose two.)

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

Correct Answer: CD

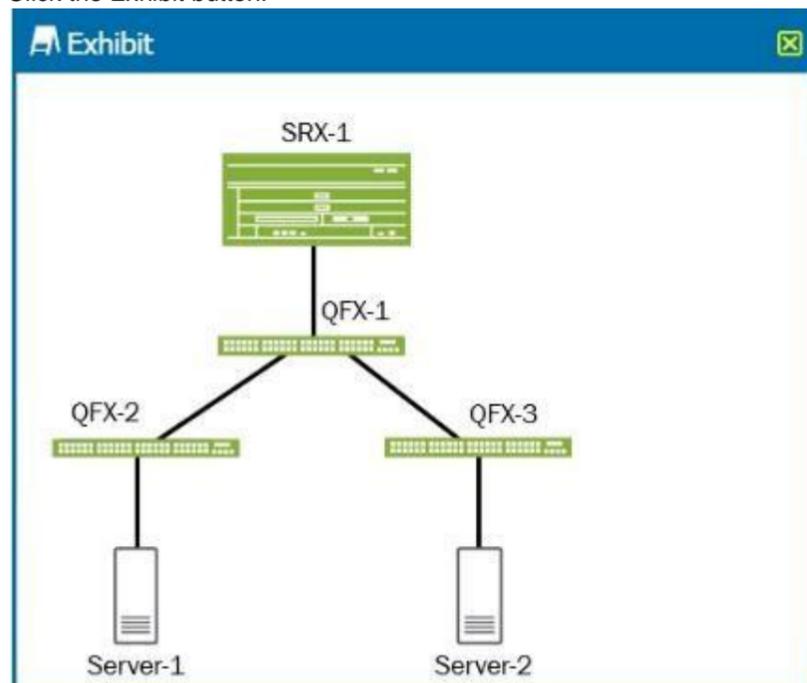
Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference: