JN0-230.VCEplus.premium.exam.65q

Number: JN0-230
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

JN0-230

Security, Associate (JNCIA-SEC)

Version 1.0

Exam A

QUESTION 1

Which statement is correct about Junos security zones?

A. User-defined security zones must contain at least one interface.
B. Logical interfaces are added to user-defined security zones.
C. Security policies are referenced within a user-defined security zone.
D. User-defined security zones must contain the key word “zone”.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 Which type of traffic is analyzed by an SRX Series device configured to use an antispam UTM policy?

A. IMAP
B. POP3
C. SMTP
D. HTTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

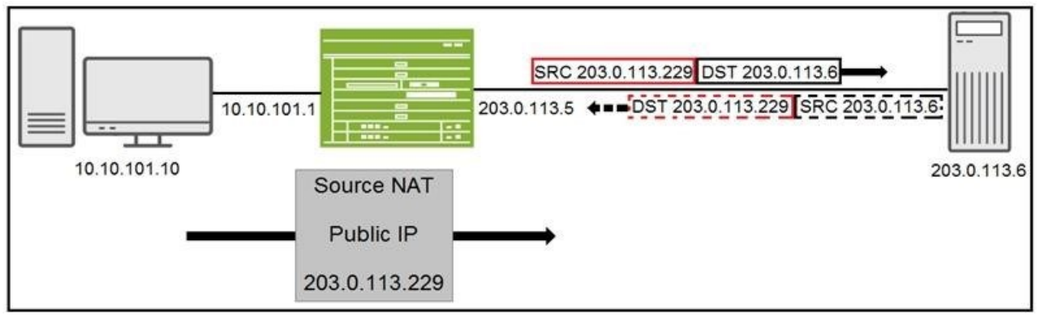
QUESTION 3 What is the definition of a zone on an SRX Series device?

A. a collection of one or more network segments sharing similar security requirements
B. an individual logical interface with a public IP address
C. a collection of one or more network segments with different security requirements
D. an individual logical interface with a private IP address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Click the Exhibit button.



You have configured source NAT using an address pool as shown in the exhibit. Traffic is reaching the 203.0.113.6 server but return traffic is not being received by the SRX Series device.

Which feature must be configured to allow return traffic to be accepted by the SRX Series device?

A. proxy ARP
B. destination NAT
C. port forwarding
D. reverse static NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Your company uses SRX Series devices to secure the edge of the network. You are asked to protect the company from ransomware attacks.

Which solution will satisfy this requirement?

A. screens
B. unified security policies
C. AppSecure
D. Sky ATP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6 Which method do VPNs use to prevent outside parties from viewing packets in clear text?

A. integrity
B. authentication
C. encryption
D. NAT-T

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 What is the correct order of processing when configuring NAT rules and security policies?

A. destination NAT > policy lookup > source NAT > static NAT B.
policy lookup > source NAT > static NAT > destination NAT
C. source NAT > static NAT > destination NAT > policy lookup
D. static NAT > destination NAT > policy lookup > source NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 Which two statements describe IPsec VPNs?
(Choose two.)

A. IPsec VPN traffic is always authenticated.
B. IPsec VPNs are dedicated physical connections between two private networks.
C. IPsec VPN traffic is always encrypted.
D. IPsec VPNs use security measures to secure traffic over a public network between two remote sites.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 Which zone is considered a functional zone?

A. junos host
B. null
C. trust
D. management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 What does IPsec use to negotiate encryption algorithms?

A. AH
B. TLS
C. IKE
D. ESP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 Which source NAT rule set would be used when a packet matches the conditions in multiple rule sets?

A. The most specific rule set will be used.
B. The least specific rule set will be used.C. The first rule set matched will be used.
D. The last rule set matched will be used.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 Which statement is correct about SKY ATP?

A. SKY ATP can provide live threat feeds to SRX Series devices.
B. SKY ATP relies on the SRX Series device to open and analyze suspect file attachments.
C. The local Sky ATP platform downloads the latest threat feeds from a managed file.
D. Sky ATP is a local hardware-based security threat analyzer that performs multiple tasks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 Which two statements are true about Junos Space Security Director? (Choose two.)

A. Security Director supports creation and maintenance of metadata-based policies.
B. Security Director can deploy enforcement policies automatically to firewalls and switches.
C. Security Director can perform deep-packet analysis.
D. Security Director is preinstalled on SRX Series devices.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 Which two statements are correct about using global-based policies over zone-based policies? (Choose two.)

A. With global-based policies, you do not need to specify a source address in the match criteria.
B. With global-based policies, you do not need to specify a destination zone in the match criteria.
C. With global-based policies, you do not need to specify a destination address in the match criteria.
D. With global-based policies, you do not need to specify a source zone in the match criteria.

Correct Answer: BD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 15
You want to configure your SRX Series device so that employees configured with IP addresses on the 172.16.0.0/16 subnet can access the Internet. The device has been allocated a single public IP address.

In this scenario, which NAT mode should you enable?

A. static NAT
B. destination NAT
C. source NAT
D. NAT-T

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
What is the behavior of an SRX Series device when UDP and TCP traffic is rejected by a security policy action? (Choose two.)

A. The reject action drops UDP packets and sends an ICMP message to the source.
B. The reject action drops TCP packets and sends an RST message to the source.
C. The reject action drops TCP packets and sends an ICMP message to the source.
D. The reject action drops UDP packets and does not send any message to the source.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 390, Policy name: internet-trust/5, Timeout: 1792, Valid
     In: 10.10.101.10/53450 --> 203.0.113.6/23;tcp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 28, Bytes: 1622,
     Out: 203.0.113.6/23 --> 203.0.113.229/53450;tcp, Conn Tag: 0x0, If: ge-
0/0/3.0, Pkts: 21, Bytes: 1395,
Total sessions: 1
```

Referring to the exhibit, which type of NAT is performed by the SRX Series device?

A. source NAT with PAT
B. source NAT without PAT
C. destination NAT with PAT
D. destination NAT without PAT

Correct Answer: A
Section: (none)
Explanation
QUESTION 18 Which two statements are correct about global security policies? (Choose two.)

A. Global-based policies can reference the destination zone.

Explanation/Reference:

B. Global-based policies can reference the source zone.
C. Global-based policies must reference a dynamic application.
D. Global-based policies must reference the source and destination zones.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 Which type of security policy protects restricted services from running on non-standard ports?

A. application firewall
B. IDP
C. Sky ATP
D. antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 By default, revenue interfaces are placed into which system-defined security zone on an SRX Series device?

A. junos-trust
B. untrust
C. trust
D. null

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Click the Exhibit button.

	Hit Count	Name	Source			Destination		Dynamic Application	Service	URL Category	Action
			Zone	Address	Identity	Zone	Address				
	trust to untrust(1 Rules)										
☐	1 2...	Internet-Access	trust	any		untrust	any	any	any	None	✓
	Global(1 Rules)										
☐	1 -	Block-Facebook-Access	-	any		-	any	FACEBOOK-ACCESS	junos-defaults	None	⊖

Users on the network are restricted from accessing Facebook, however, a recent examination of the logs show that users are accessing Facebook.

Referring to the exhibit, why is this problem happening?

A. The Internet-Access rule is listed first
B. Zone-based rules are honored before global rules.
C. Global rules are honored before zone-based rules.
D. The Internet-Access rule has a higher precedence value.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Your company has been assigned one public IP address. You want to enable Internet traffic to reach multiple servers in your DMZ that are configured with private IP addresses.

In this scenario, which type of NAT would be used to accomplish this task?

A. source NAT
B. destination NAT
C. NAT without PAT
D. static NAT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 You want to deploy, manage, and configure multiple SRX Series devices without an on-premises software solution.

Which solution would satisfy this requirement?

A. Junos Space Network Director
B. Juniper Sky Enterprise
C. Juniper SKY ATP
D. Juniper Advanced Threat Prevention

Correct Answer: B
Section: (none)
Explanation
QUESTION 24
You configured and applied several global policies and some of the policies have overlapping match criteria.

In this scenario, how are these global policies applied?

A. The most restrictive policy that matches is applied.
B. The last matched policy is the only policy applied.
C. The least restrictive policy that matches is applied.
D. The first matched policy is the only policy applied.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation/Reference:

QUESTION 25
You have created a zone-based security policy that permits traffic to a specific webserver for the marketing team. Other groups in the company are not permitted to access the webserver. When marketing users attempt to access the server they are unable to do so.

What are two reasons for this access failure? (Choose two.)

A. You failed to position the policy before the policy that denies access to the webserver.
B. You failed to position the policy after the policy that denies access to the webserver.
C. You failed to commit the policy change.
D. You failed to change the source zone to include any source zone.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26 Which two statements describe unified security policies? (Choose two.)

A. Unified security policies allow the SRX Series device to match on URL categories in the match field.
B. Unified security policies allow the SRX Series device to match on applications in the match field.
C. Unified security policies allow the SRX Series device to match on applications in the action field.
D. Unified security policies allow the SRX Series device to match on URL categories in the action field.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

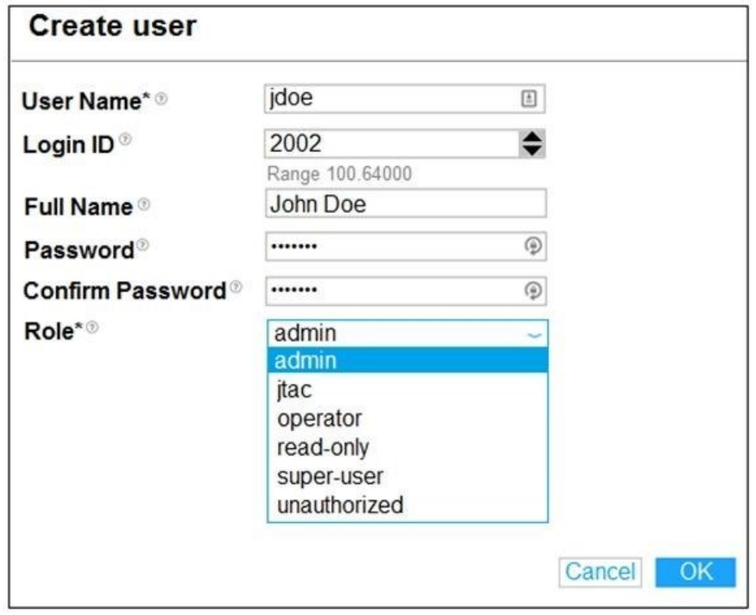
QUESTION 27 What must you do first to use the Monitor/Alarms/Policy Log workspace in J-Web?

A. You must enable event mode security logging on the SRX Series device.
B. You must enable stream mode security logging on the SRX Series device.
C. You must enable security logging that uses the TLS transport mode.
D. You must enable security logging that uses the SD-Syslog format.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Click the Exhibit button.



Which two user roles shown in the exhibit are available by default? (Choose two.)

A. super-user
B. operator
C. jtac
D. admin

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 Which Juniper product sends command and control feeds to the SRX Series device?

A. Sky Enterprise
B. Juniper Secure Analytics
C. Sky Advanced Threat Prevention
D. Juniper Identification Management Service

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Which statement is correct about address books for security policies on SRX Series devices?

A. Address sets can contain addresses from different security zones.
B. A zone can only use one address book at a time.
C. NAT rules can use address objects only from the global address book.
D. Addresses in the global address book are preferred over addresses in a zone-based address book.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 What are two available methods used to authenticate users connecting to an SRX Series device? (Choose two.)

A. Use Local authentication
B. Use two-factor authentication
C. Use Active-Directory authentication
D. Use RADIUS authentication

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Click the Exhibit button.

```
Apr 10 14:23:07 vSRX-1 RT_UTM: ANTISPAM_SPAM_DETECTED_MT: Antispam: SPAM
detected:
name= "jcart@example.com" source-ip= (172.23.10.100)
profile-name= "block-spam" action= "Deny" reason= "Match local blacklist"
username= "N/A" roles= "N/A"
```

You have configured antispam to allow e-mails from example.com; however, reviewing the logs you see that jcart@example.com is blocked.

Referring to the exhibit, what are two ways to solve this problem? (Choose two.)

A. Add jcart@example.com to the profile antispam address whitelist.
B. Verify connectivity with the SBL server.
C. Delete jcart@example.com from the profile antispam address whitelist.
D. Delete jcart@example.com from the profile antispam address blacklist.

Correct Answer: AD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 33 In which order are NAT types evaluated?

A. reverse static > source > static > destination
B. source > destination > static > reverse static
C. static > destination > reverse static > source
D. destination > static > reverse static > source

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Click the Exhibit button.

	Hit Count	Name	Source			Destination		Dynamic Application	Service	URL Category	Action
			Zone	Address	Identity	Zone	Address				
	trust to untrust (2 Rules)										
☐	1 2...	Internet-Access	trust	any		untrust	any	any	any	None	✓
☐	2 0	Block-Facebook-Access	trust	any		untrust	any	FACEBOOK-ACCESS	junos-defaults	None	⊖

Users should not have access to Facebook, however, a recent examination of the security logs show that users are accessing Facebook.
Referring to the exhibit, what should you do to solve this problem?

A. Change the source address for the Block-Facebook-Access rule to the prefix of the users.
B. Change the Block-Facebook-Access rule from a zone policy to a global policy.
C. Move the Block-Facebook-Access rule before the Internet-Access rule.
D. Change the Internet-Access rule from a zone policy to a global policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35 Which security feature is applied to traffic on an SRX Series device when the device is running in packet mode?

A. ALGs
B. Sky ATP
C. firewall filters
D. unified policies

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 36 Firewall filters define which type of security?

A. stateful
B. stateless
C. NGFW
D. dynamic enforcement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Users in your network are downloading files with file extensions that you consider to be unsafe for your network. You must prevent files with specific file extensions from entering your network.

Which UTM feature should be enabled on an SRX Series device to accomplish this task?

A. content filtering
B. antispam
C. Web filtering
D. URL filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 You want to automatically generate the encryption and authentication keys during IPsec VPN tunnel establishment.

What would be used to accomplish this task?

A. main mode
B. aggressive mode
C. IPsec
D. Diffie-Hellman

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 Which two statements about security policy processing on SRX Series devices are true? (Choose two.)

A. Zone-based security policies are processed before global policies.
B. Traffic matching a global policy cannot be processed against a firewall filter.
C. Traffic matching a zone-based policy is not processed against global policies.
D. Zone-based security policies are processed after global policies.

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 You are asked to run a report to find the top talkers on your network in the past 48 hours.

In this scenario, the report will be in which format when the J-Web UI delivers it to you?

A. JPG
B. HTML
C. xls
D. CSV

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 Which UTM feature should you use to protect users from visiting certain blacklisted websites?

A. content filtering
B. Web filtering
C. antivirus
D. antispam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 Which two statements are true about security policies in the factory-default configuration of an SRX340? (Choose two.)

A. All traffic from the trust zone to the untrust zone is allowed.
B. All interzone traffic is denied.
C. All interzone traffic is allowed.
D. All traffic from the untrust zone to the trust zone is denied.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which two actions are performed on an incoming packet matching an existing session? (Choose two.)
A. security policy evaluation
B. service ALG processing
C. screens processing

D. zones processing

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 On an SRX Series device, how should you configure your IKE gateway if the remote endpoint is a branch office using a dynamic IP address?

A. Configure the IPsec policy to use MD5 authentication.
B. Configure the IKE policy to use aggressive mode.
C. Configure the IPsec policy to use aggressive mode.
D. Configure the IKE policy to use a static IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 What must you do first to use the Monitor/Events workspace in the J-Web interface?

A. You must enable security logging that uses the TLS transport mode.
B. You must enable security logging that uses the SD-Syslog format.
C. You must enable stream mode security logging on the SRX Series device.
D. You must enable event mode security logging on the SRX Series device.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Which statement is correct about IKE?

A. IKE phase 1 is used to establish the data path.
B. IKE phase 1 only supports aggressive mode.
C. IKE phase 1 establishes the tunnel between devices.
D. IKE phase 1 negotiates a secure channel between gateways.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

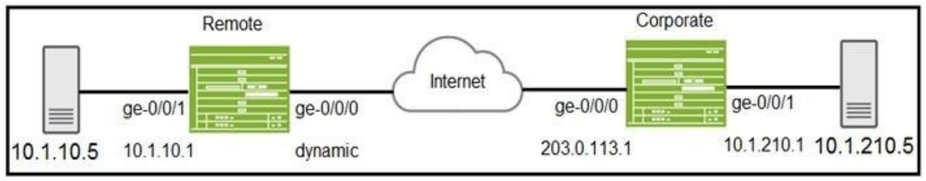
QUESTION 47
Which two statements are correct about security zones? (Choose two.)
A. Security zones use address books to link usernames to IP addresses.
B. Security zones use a stateful firewall to provide secure network connections.

C. Security zones use packet filters to prevent communication between management ports.
D. Security zones use security policies that enforce rules for the transit traffic.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Click the Exhibit button.



You are configuring an IPsec VPN for the network shown in the exhibit.

Which feature must be enabled for the VPN to establish successfully?

A. Main mode must be configured on the IKE gateway.
B. Main mode must be configured on the IPsec VPN.
C. Aggressive mode must be configured on the IPsec VPN.
D. Aggressive mode must be configured on the IKE gateway.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 When configuring IPsec VPNs, setting a hash algorithm solves which security concern?

A. availability
B. encryption
C. redundancy
D. integrity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 Which security object defines a source or destination IP address that is used for an employee workstation?

A. zone
B. screen
C. address book entry
D. scheduler

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 What is a type of security feed that Sky ATP provides to a vSRX Series device by default?

A. RSS feeds
B. C&C feeds
C. ACL feeds
D. malware feeds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
You are designing a new security policy on an SRX Series device. You must block an application silently and log all occurrences of the application access attempts. In this scenario, which two actions must be enabled in the security policy? (Choose two.)

A. Log the session initiations.
B. Enable a reject action.
C. Log the session closures.
D. Enable a deny action.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 Which two notifications are available when the antivirus engine detects an infected file? (Choose two.)

A. e-mail notifications
B. protocol-only notifications
C. SNMP notifications
D. SMS notifications

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
What is a characteristic of the Junos Enhanced Web filtering solution?

A. Junos Enhanced Web filtering allows the SRX Series device to categorize URLs using an on-premises Websense server.
B. The SRX Series device intercepts HTTP and HTTPS requests and sends the source IP address to the on-premises Websense server.

C. The Websense Cloud categorizes the URLs and also provides site reputation information.
D. The Websense Cloud resolves the categorized URLs to IP addresses by performing a DNS reverse lookup.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
You verify that the SSH service is configured correctly on your SRX Series device, yet administrators attempting to connect through a revenue port are not able to connect.

In this scenario, what must be configured to solve this problem?

A. a host-inbound-traffic setting on the incoming zone
B. an MTU value larger than the default value
C. a screen on the internal interface
D. a security policy allowing SSH traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56 Which two features on the SRX Series device are common across all Junos devices? (Choose two.)

A. the separation of control and forwarding planes
B. screens
C. stateless firewall filters
D. UTM services

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Click the Exhibit button.

```
user@vSRX-1> show security flow session
Session ID: 30, Policy name: internet-trust/5, Timeout: 1758, Valid
     In: 10.10.101.10/63797 --> 203.0.113.6/23;tcp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 28, Bytes: 1622,
     Out: 203.0.113.6/23 --> 203.0.113.5/30859; tcp, Conn Tag: 0x0, If: ge-0/0/3.0,
Pkts: 22, Bytes: 1447,
Total sessions: 1
```

Referring to the exhibit, which type of NAT is being performed?
A. source NAT without PAT
B. destination NAT without PAT
C. source NAT with PAT
D. destination NAT with PAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 What is the purpose of the Shadow Policies workspace in J-Web?

A. The Shadow Policies workspace shows unused security policies due to policy overlap.
B. The Shadow Policies workspace shows used security policies due to policy overlap.
C. The Shadow Policies workspace shows unused IPS policies due to policy overlap.
D. The Shadow Policies workspace shows used IPS policies due to policy overlap.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 Which UTM feature uses MIME pattern filters to identify traffic in HTTP and e-mail protocols?

A. antispam
B. antivirus
C. Web filtering
D. content filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 Which statement is correct about IKE?

A. IKE phase 1 supports both main and aggressive mode.
B. IKE phase 2 is where the encryption algorithm is negotiated between peers.
C. IKE phase 1 is where the tunnel is established for transit traffic.
D. IKE phase 2 negotiates the secure channel between gateways.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which statement describes stateless firewalls on SRX Series devices?
A. Each packet is analyzed based on source zone.
B. Each packet is analyzed based on Application Layer security.
C. Each packet is analyzed as part of a session.
D. Each packet is analyzed by firewall filters.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 You have configured a Web filtering UTM policy.

Which action must be performed before the Web filtering UTM policy takes effect?

A. The UTM policy must be configured as a routing next hop.
B. The UTM policy must be linked to an ingress interface.
C. The UTM policy must be linked to an egress interface.
D. The UTM policy must be linked to a security policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63 The free licensing model for Sky ATP includes which two features? (Choose two.)

A. C&C feeds
B. infected host blocking
C. executable file inspection
D. compromised endpoint dashboard

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 What should you configure if you want to translate private source IP addresses to a single public IP address?

A. source NAT
B. destination NAT
C. content filtering
D. Security Director

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 65 Which statement is correct about global security policies?

A. Global policies eliminate the need to assign logical interfaces to security zones.
B. Global security policies require you to identify a source and destination zone.
C. Traffic matching global policies is not added to the session table.

D. Global policies allow you to regulate traffic with addresses and applications, regardless of their security zones.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: