

# JNCIA-Security

## NEW QUESTION: 1

Which statements about NAT are correct? (Choose two.)

- A. When multiple NAT rules have overlapping match conditions, the most specific rule is chosen.
- B. Source NAT translates the source IP address of packet.
- C. When multiple NAT rules have overlapping match conditions, the rule listed first is chosen.
- D. Source NAT translates the source port and destination IP address.

**Answer: B,C**

## NEW QUESTION: 2

What are the valid actions for a source NAT rule in J-Web? (choose three.)

- A. On
- B. Off
- C. Pool
- D. Source
- E. interface

**Answer: B,C,E**

Explanation [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/nat-security-source-andsource-pool.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/nat-security-source-andsource-pool.html)

## NEW QUESTION: 3

Which type of security policy protect restricted services from running on non-standard ports?

- A. Sky ATP
- B. antivirus
- C. Application firewall
- D. IDP

**Answer: C**

## NEW QUESTION: 4

Which two private cloud solution support vSRX devices? (Choose two.)

- A. Amazon Web Services (AWS)
- B. Microsoft Azure
- C. VMware NSX

- D. Contrail Cloud
- E. VMware Web Services (AWS)

**Answer: B,E**

### NEW QUESTION: 5

Users should not have access to Facebook, however, a recent examination of the logs security show that users are accessing Facebook. Referring to the exhibit,

|                            | Hit Count | Name | Source                |         |          | Destination |         | Dynamic Application | Service       | URL Category | Action |
|----------------------------|-----------|------|-----------------------|---------|----------|-------------|---------|---------------------|---------------|--------------|--------|
|                            |           |      | Zone                  | Address | Identity | Zone        | Address |                     |               |              |        |
| trust to untrust (2 Rules) |           |      |                       |         |          |             |         |                     |               |              |        |
| <input type="checkbox"/>   | 1         | 2    | Internet-Access       | trust   | any      | untrust     | any     | any                 | any           | None         |        |
| <input type="checkbox"/>   | 2         | 0    | Block-Facebook-Access | trust   | any      | untrust     | any     | FACEBOOK-ACCESS     | junos-default | None         |        |

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 Internet-Access rule from a zone policy to a global policy
- C. Move the Block-Facebook-Access rule from a zone policy to a global policy
- D. Move the Block-Facebook-Access rule before the Internet-Access rule**

**Answer: D**

### NEW QUESTION: 6

A new SRX Series device has been delivered to your location. The device has the factory-default configuration loaded. You have powered on the device and connected to the console port.

What would you use to log into the device to begin the initial configuration?

- A. Root with no password**
- B. Admin with password
- C. Root with a password of juniper"
- D. Admin with a password "juniper"

**Answer: A**

### NEW QUESTION: 7

Which statement is correct about IKE?

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

Answer: D

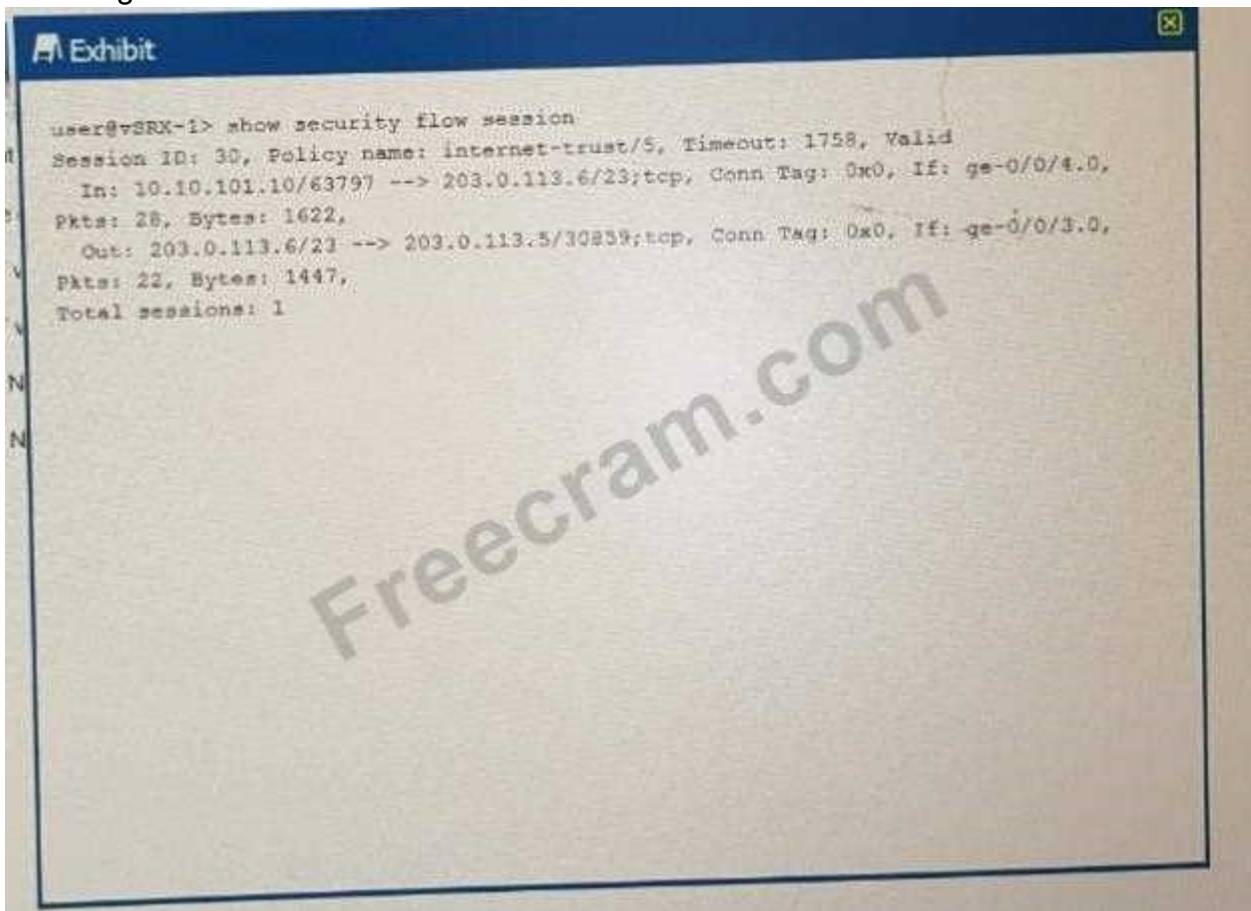
### NEW QUESTION: 8

Which two actions are performed on an incoming packet matching an existing session? (Choose two.)

- A. Service ALG processing
  - B. Security policy evolution
  - C. Screens processing
  - D. Zone processing
- Answer: A,C

### NEW QUESTION: 9

Referring to the exhibit.



Which type of NAT is being performed?

- A. Source NAT without PAT

**B. Source NAT with PAT**

C. Destination NAT without PAT

D. Destination NAT with PAT **Answer: B**

#### **NEW QUESTION: 10**

Which two statements are true about UTM on an SRX340? (Choose two.)

A. A default UTM policy is created.

B. A default UTM profile is created

**C. No default UTM policy is created**

**D. No default profile is created.**

**Answer: C,D**

#### **NEW QUESTION: 11**

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

A. Compromised endpoint dashboard

B. C&C feeds

**C. Executable file inspection**

**D. Infected host blocking** **Answer: C,D**

#### **NEW QUESTION: 12**

Which management software supports metadata-based security policies that are ideal for cloud deployments? **A. J-Web**

**B. Security Director**

C. Sky Enterprise

D. Network Director **Answer: B**

#### **NEW QUESTION: 13**

On an SRX device, you want to regulate traffic base on network segments.

In this scenario, what do you configure to accomplish this task?

A. ALGs

B. Zones

**C. Screens** D. NAT

**Answer: C**

#### **NEW QUESTION: 14**

You have created a zones-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 the webserver
- B. You failed to position the policy after the policy that denies access to the webserver.
- C. You failed to change the source zone to include any source zone.
- D. You failed to commit the policy change. **Answer: A,D**

#### NEW QUESTION: 15

Which statement about IPsec is correct?

- A. IPsec can provide encryption but not data integrity.
- B. IPsec support packet fragmentation by intermediary devices.
- C. IPsec must use certificates to provide data encryption
- D. IPsec support both tunnel and transport modes. **Answer: D**

#### NEW QUESTION: 16

Which statements is correct about Junos security zones?

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

**Answer: D**

**Valid JN0-230 Dumps** shared by PrepAwayExam.com for Helping Passing JN0-230 Exam!

PrepAwayExam.com now offer the **newest JN0-230 exam dumps**, the PrepAwayExam.com JN0-230 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepAwayExam.com JN0-230 dumps with Test Engine here:

<https://www.prepawayexam.com/Juniper/braindumps.JN0-230.ete.file.html> (65 Q&As Dumps, **40%OFF Special Discount: freecram**)

#### NEW QUESTION: 17

What are two characteristic of static NAT SRX Series devices? (Choose two.)

- A. Static NAT rule take precedence over source and destination NAT rules.
- B. A reverse mapping rule is automatically created for the source translation.
- C. Source and destination NAT rules take precedence over static NAT rules.
- D. Static rules cannot coexist with destination NAT rules on the same SRX Series device configuration.

**Answer: D**

### NEW QUESTION: 18

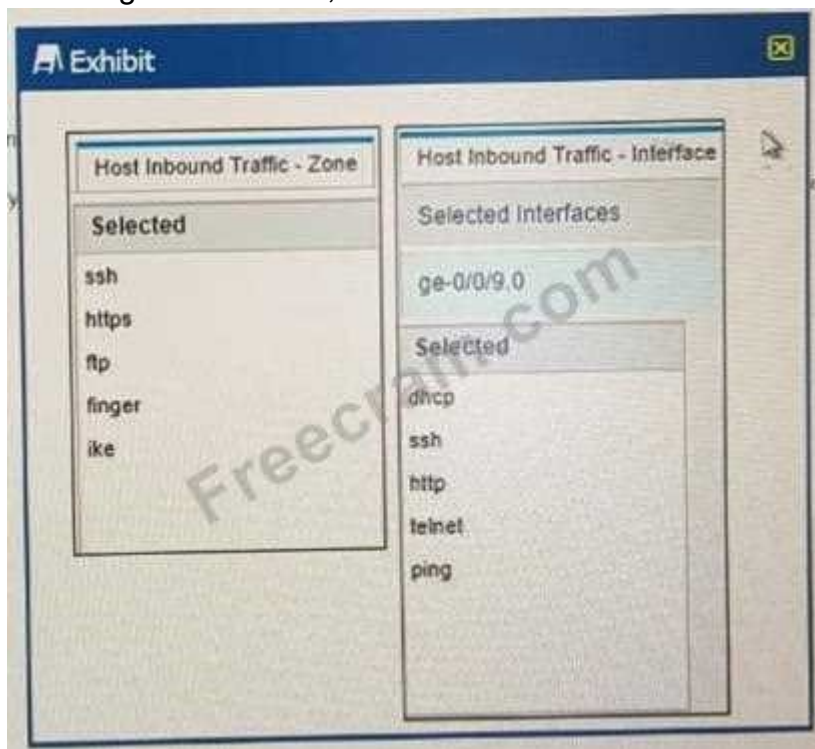
Which statement about IPsec is correct?

- A. IPsec can be used to transport native Layer 2 packets.
  - B. IPsec is a standards-based protocol.
  - C. IPsec can provide encapsulation but not encryption
  - D. IPsec is used to provide data replication
- Answer: D**

### NEW QUESTION: 19

Host-inbound-traffic is configured on the DMZ zone and the ge-0/0/9.0 interface attached to that zone.

Referring to the exhibit,



which to types of management traffic would be performed on the SRX Series device? (Choose two.)

- A. Finger
- B. HTTP
- C. SSH
- D. HTTPS

**Answer: B,C**

### NEW QUESTION: 20

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

- A. SMS notifications
- B. Protocol-only notification

C. SNMP notifications

D. e-mail notifications **Answer: A,C**

#### **NEW QUESTION: 21**

Your company uses SRX Series devices to secure the edge of the network. You are asked protect the company from ransom ware attacks.

Which solution will satisfy this requirement?

A. screens

B. Unified security policies

C. AppSecure

D. Sky ATP

**Answer: D**

#### **NEW QUESTION: 22**

Which actions would be applied for the pre-IDdefault policy unified policies?

A. Redirect the session

B. Reject the session

C. Silently drop the session

D. Log the session **Answer: A**

#### **NEW QUESTION: 23**

You are concerned that unauthorized traffic is using non-standardized ports on your network.

In this scenario, which type of security feature should you implement?

A. Sky ATP

B. Firewall filters

C. Application firewall

D. Zone-based policies **Answer: B**

#### **NEW QUESTION: 24**

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

What would be used to accomplish this task?

A. Main mode

B. Diffie\_Hellman

C. IPsec

D. Aggregate mode

**Answer: B**

**NEW QUESTION: 25**

Which two statements are true about security policy actions? (Choose two.)

- A. The reject action drops the traffic and sends a message to the source device.
- B. The deny action silently drop the traffic.
- C. The deny action drops the traffic and sends a message to the source device.
- D. The reject action silently drops the traffic. **Answer: B,A**

**NEW QUESTION: 26**

Which two elements are needed on an SRX Series device to set up a remotesyslogserver? (Choose two.)

- A. Data type
- B. Data size
- C. Data throughput
- D. IP address

**Answer: A,B**

**NEW QUESTION: 27**

Referring to the exhibit.

\*\*\*\*Exhibit is Missing\*\*\*\*

Which type of NAT is performed by the SRX Series device?

- A. Source NAT with PAT
- B. Destination NAT without PAT
- C. Source Nat without PAT
- D. Destination NAT with PAT **Answer: D**

**NEW QUESTION: 28**

Which two statements are true about UTM on an SRX340? (Choose two.)

- A. No default UTM policy is created
- B. A default UTM policy is created.
- C. No default profile is created.
- D. A default UTM profile is created

**Answer: C,D**

**NEW QUESTION: 29**

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 address.

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

- A. Static NAT
- B. Source NAT
- C. Destination NAT
- D. NAT without PAT

**Answer: C**

**NEW QUESTION: 30**

By default, revenue interface are placed into which system-defined security zone on an SRX series device?

- A. Trust
- B. Null
- C. Junos-trust
- D. untrust

**Answer: A**

**NEW QUESTION: 31**

You configure and applied several global policies and some of the policies have overlapping match criteria.

- A. In this scenario, how are these global policies applies?
- B. The most restrictive that matches is applied.
- C. The least restrictive policy that matches is applied.
- D. The first matched policy is the only policy applied.

**Answer: A**

**NEW QUESTION: 32**

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

- A. Static NAT > destination NAT > policy lookup > source NAT
- B. Source NAT > static NAT > destination NAT > policy lookup
- C. Policy lookup > source NAT > static NAT > destination NAT
- D. Destination NAT > policy lookup > source NAT > static NAT

**Answer: A**

**NEW QUESTION: 33**

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

**Answer: A**

**NEW QUESTION: 34**

Which statements is correct about SKY ATP?

- A. Sky ATP is used to automatically push out changes to the AppSecure suite.
- B. Sky ATP only support sending threat feeds to vSRX Series devices
- C. Sky ATP is an open-source security solution.
- D. Sky ATP is a cloud-based security threat analyzer that performs multiple tasks

**Answer: D**

**NEW QUESTION: 35**

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,



| Hit Count                  | Name                  | Source |         |          | Destination |                 | Dynamic Application | Service | URL Category | Action |
|----------------------------|-----------------------|--------|---------|----------|-------------|-----------------|---------------------|---------|--------------|--------|
|                            |                       | Zone   | Address | Identity | Zone        | Address         |                     |         |              |        |
| trust to untrust (1 Rules) |                       |        |         |          |             |                 |                     |         |              |        |
| 1                          | internet-Access       | trust  | any     |          | untrust     | any             | any                 | any     | None         | Allow  |
| Global (1 Rules)           |                       |        |         |          |             |                 |                     |         |              |        |
| 1                          | Block-Facebook-Access |        | any     |          | any         | FACEBOOK-ACCESS | junos-defaults      | None    |              | Deny   |

Why is this problem happening?

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

**Answer: D**

**NEW QUESTION: 36**

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

- A. scheduler
- B. Screen
- C. Zone
- D. Address book entry **Answer: D**

**NEW QUESTION: 37**

Which statement about IPsec is correct?

- A. IPsec can be used to transport native Layer 2 packets.
- B. IPsec is a standards-based protocol.
- C. IPsec can provide encapsulation but not encryption
- D. IPsec is used to provide data replication **Answer: B**

### NEW QUESTION: 38

You have configured antispam to allow e-mail from example.com, however the logs you see thatjcart@example.comis blocked Referring to the exhibit.



What are two ways to solve this problem?

- A. Verify connectivity with the SBL server.
- B. Deletejcart@example.comfrom the profile antispam address blacklist
- C. Deletejcart@example.comfrom the profile antispam address whitelist
- D. Addjcart@exmpl.comto the profile antispam address whitelist.

**Answer: B,D**

### NEW QUESTION: 39

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

- A. Security Director
- B. Source NAT
- C. Destination NAT
- D. Content filtering

**Answer: B**

**NEW QUESTION: 40**

You are configuring an IPSec VPN tunnel between two location on your network. Each packet must be encryoted and authenticated.

Which protocol would satisfy these requirements?

- A. MD5
- B. SHA
- C. AH
- D. ESP

**Answer: D**

**NEW QUESTION: 41**

Which two statements are correct about functional zones?

- A. A functional zone uses security policies to enforce rules for transit traffic
- B. A function is used for special purpose, such as management interface
- C. Traffic received on the management interface in the functional zone cannot transit out other interface
- D. Functional zones separate groups of user based on their function

**Answer: B,C**

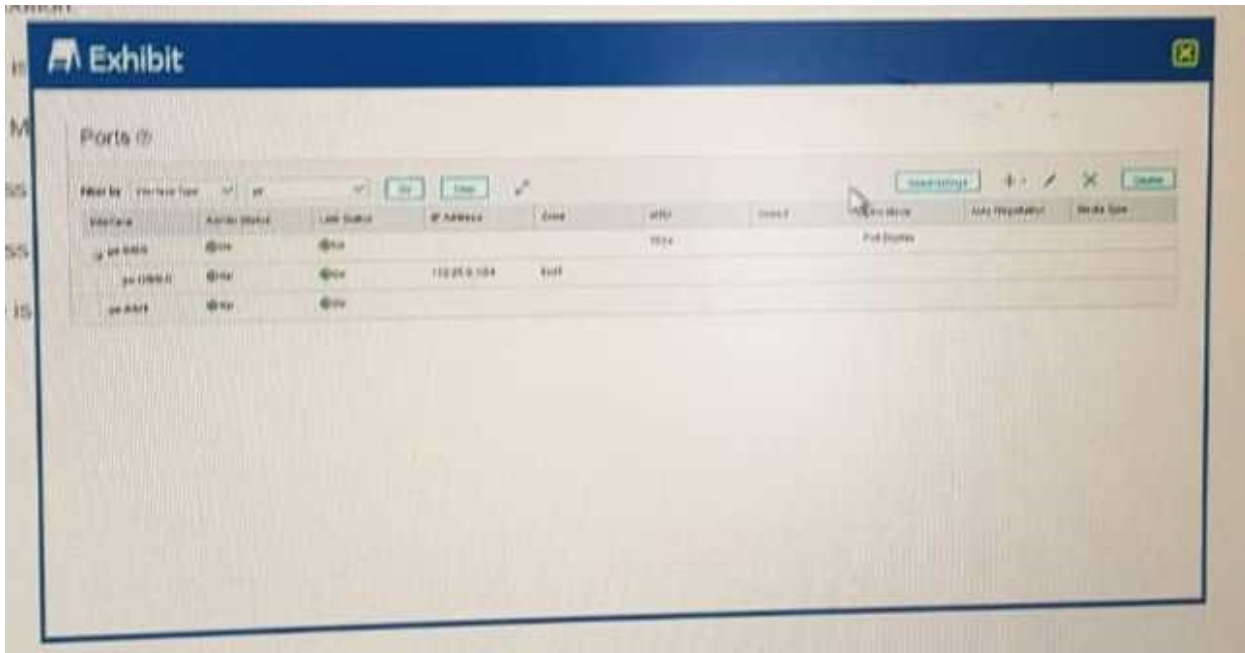
**NEW QUESTION: 42**

Which two segments describes IPsec VPNs? (Choose two)

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

**Answer: C**

### NEW QUESTION: 43



Which statement is correct regarding the interface configuration shown in the exhibit?

- A. The interface MTU has been increased
- B. The IP address has an invalid subnet mask
- C. The IP address is assigned to unit 0
- D. The interface is assigned to the trust zone by default

**Answer: A**

### NEW QUESTION: 44

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

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

**Answer: B**

### NEW QUESTION: 45

Which statements is correct about global security policies?

- A. Global policies allow you to regulate traffic with address and applications, regardless of their security zones.
- B. Traffic matching global is not added to the session table.
- C. Global policies eliminate the need to assign interface to security zones.
- D. Global security require you to identify a source and destination zone

**Answer: A**

**NEW QUESTION: 46**

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

**Answer: B**

**NEW QUESTION: 47**

What are configuring the antispam UTM feature on an SRX Series device.

Which two actions would be performed by the SRX Series device for e-mail that is identified as spam? (Choose two.)

- A Tag the e-mail
- B Queue the e-mail
- C Block the e-mail
- D Quarantine e-mail

**Answer: A,C**

**NEW QUESTION: 48**

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

**Answer: A**

**NEW QUESTION: 49**

On a 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 MDS 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

**Answer: B**

**NEW QUESTION: 50**

Which three actions would be performed on traffic traversing an IPsec VPAN? (Choose three)

- A Port forwarding
- B Authentication
- C Envryption
- D Deep inspection
- E Payload verification

**Answer: B,C,E**

**NEW QUESTION: 51**

You are designing a new security policy on an SRX Series device. You must block an application and log all occurrence 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

**Answer: A,D**

**NEW QUESTION: 52**

The Sky ATP premium or basic-Threat Feed license is needed for which two features? (Choose two)

- A Outbond protection
- B C&C feeds
- C Executable inspection
- D Custom feeds

**Answer: B,D**