Juniper.JN0-232.v2026-06-06.q60

Exam Code:	JN0-232
Exam Name:	Security, Associate (JNCIA-SEC)
Certification Provider:	Juniper
Free Question Number:	60
Version:	v2026-06-06
# of views:	134
# of Questions views:	600
https://www.freepdfdumps.com/Juniper.JN0-232.v2026-06-06.q60.html	

NEW QUESTION: 1
You are troubleshooting traffic traversing the SRX Series Firewall and require detailed information showing how the flow module is handing the traffic.
How would you accomplish this task?
A. Review the forwarding table.
B. Review the flow session table.
C. Enable flow trace options.
D. Enable firewall filters.
Answer: (SHOW ANSWER)
To obtain detailed, step-by-step information on how the SRX flow module is processing traffic, you enable flow trace options. This feature captures flow-level diagnostics, showing session creation, NAT, policy matches, and packet disposition, making it ideal for deep troubleshooting.

NEW QUESTION: 2
What are three requirements for creating a custom application? (Choose three.)
A. You must define the port number.
B. You must define the security policy.
C. You must define the application name.
D. You must define the source address.
E. You must define the protocol.
Answer: (SHOW ANSWER)
To create a custom application on an SRX Series Firewall, you must define:
- The port number, which specifies where the application listens or communicates.
- The application name, which uniquely identifies the custom application within the configuration.
- The protocol (such as TCP or UDP), which determines how traffic is handled and matched for that application.

NEW QUESTION: 3
What happens when traffic is matched by a unified security policy?
A. Further processing stops and traffic is assigned a dynamic application.
B. Processing continues until it matches three or more policies.
C. Further policy processing stops and applies the action.
D. Processing continues to any additional unified policies.
Answer: C (LEAVE A REPLY)
When traffic matches a unified security policy, the SRX immediately stops further policy evaluation and applies the action (such as permit, deny, or reject) defined in that matching policy.
Unified security policies, like traditional ones, are processed in a top-down order.

NEW QUESTION: 4
Which two statements about functional zones are correct? (Choose two.)
A. You create only one functional zone called management.
B. Functional zones consist of logical interfaces belonging to multiple zones.
C. You reference the management functional zone in a security policy.
D. The management functional zone controls management access to the firewall.
Answer: (SHOW ANSWER)
The management functional zone can be referenced in security policies when defining how management traffic interacts with other zones.
The management functional zone is designed specifically to control management access (e.g., SSH, HTTPS, SNMP) to the firewall, ensuring administrative traffic is properly isolated and secured.

NEW QUESTION: 5
Which statement about the flow module is correct in the context of destination NAT?
A. The flow module performs NAT during both first path and fast path processing.
B. The flow module performs NAT only for source IP addresses.
C. The flow module performs NAT only during fast path processing.
D. The flow module performs NAT only during first path processing.
Answer: A (LEAVE A REPLY)
The flow module on SRX Series Firewalls performs NAT translation - including both source and destination NAT - during both first path (session creation) and fast path (subsequent packets of an existing session) processing. This ensures consistency in address translation for all packets within a session.

NEW QUESTION: 6
Which two addresses are valid address book entries? (Choose two.)
A. 173.145.5.21/255.255.255.0
B. 153.146.0.145/255.255.0.255
C. 203.150.108.10/24
D. 191.168.203.0/24
Answer: (SHOW ANSWER)

The correct address book entries are:
173.145.5.21/255.255.255.0
203.150.108.10/24
Both of these entries represent a valid IP address and subnet mask combination, which can be used as an address book entry in a Juniper device.

NEW QUESTION: 7
What is the default timeout value for TCP sessions on an SRX Series device?
A. 30 seconds
B. 60 minutes
C. 60 seconds
D. 30 minutes
Answer: (SHOW ANSWER)
By default, TCP has a 30-minute idle timeout, and UDP has a 60-second idle timeout.
Additionally, known IP protocols have a 30-minute timeout, whereas unknown ones have a 60- second timeout. Setting the inactivity timeout is very useful, particularly if you are concerned about applications either timing out or remaining idle for too long and filling up the session table.
According to the Juniper SRX Series Services Guide, this can be configured using the 'timeout inactive' statement for the security policy.

NEW QUESTION: 8
Which type of policy is shown in the exhibit?

```
[edit security policies from-zone Trust to-zone Trust]
user@SRX# show
policy allow-all {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```


A. default policy
B. intra-zone policy
C. inter-zone policy

D. global policy

Answer: B (LEAVE A REPLY)

The policy is defined from-zone Trust to-zone Trust, which means traffic is controlled within the same security zone, making it an intra-zone policy.

NEW QUESTION: 9

What is the number of concurrent Secure Connect user licenses that an SRX Series device has by default?

A. 3

B. 4

C. 2

D. 5

Answer: C (LEAVE A REPLY)

The number of concurrent Secure Connect user licenses that an SRX Series device has by default is 2. Secure Connect is a feature of Juniper SRX Series devices that allows you to securely connect to remote networks via IPsec VPN tunnels. Each SRX Series device comes with two concurrent Secure Connect user licenses by default, meaning that it can support up to two simultaneous IPsec VPN connections.

NEW QUESTION: 10

You want to enable NextGen Web Filtering in SRX Series devices.

In this scenario, which two actions will accomplish this task? (Choose two.)

A. Generate a CA-signed certificate.

B. Generate a self-signed certificate.

C. Configure an SSL initiation profile.

D. Configure an SSL proxy profile.

Answer: B,D (LEAVE A REPLY)

Generate a self-signed certificate (or use a CA-signed one) to allow the SRX to decrypt and inspect SSL traffic for web filtering.

Configure an SSL proxy profile to enable SSL inspection, which is required for NextGen Web Filtering to identify and control encrypted web traffic.

NEW QUESTION: 11

The exhibit shows a table representing security policies from the trust zone to the untrust zone.

In this scenario, which two statements are correct? (Choose two.)

Security Policies from Trust Zone to Untrust Zone

Src Addr	Dst Addr	Application	Action
172.25.11.0/24	10.1.0.0/16	ftp	deny
172.25.11.0/24	10.1.0.0/16	ssh	permit
172.25.11.0/24	10.1.0.0/16	https	permit
172.25.11.0/24	any	ping	permit
any	any	any	deny

A. FTP requests from the source IP address of 172.25.11.11 are denied to the destination IP address of 10.1.0.10.
B. Ping command requests from the source IP address of 172.25.11.100 are denied to the destination IP address of 10.1.0.10.
C. SSH requests from the source IP address of 172.25.11.10 are permitted to the destination IP address of 10.1.0.10.
D. FTP requests from the source IP address of 10.1.0.10 are permitted to the destination IP address of 172.25.11.100.
Answer: (SHOW ANSWER)
FTP traffic from 172.25.11.0/24 to 10.1.0.0/16 matches the explicit FTP deny rule, so a session from 172.25.11.11 to 10.1.0.10 is denied.
SSH traffic from 172.25.11.0/24 to 10.1.0.0/16 matches the explicit SSH permit rule, so a session from 172.25.11.10 to 10.1.0.10 is permitted.

NEW QUESTION: 12
Your company is acquiring a smaller company that uses the same private address range that your company currently uses in its North America division. You have a limited number of public IP addresses to use for the acquisition. You want to allow the new acquisition's users to connect to the existing services in North America.
Which two features would you enable on your SRX Series Firewall to accomplish this task?
(Choose two.)
A. IDP
B. BGP
C. NAT
D. PAT
Answer: C,D (LEAVE A REPLY)
NAT (Network Address Translation) allows overlapping private IP address spaces (such as two companies using the same subnet) to communicate by translating one side's addresses into a unique range.
PAT (Port Address Translation) enables multiple internal hosts to share a single public IP address by differentiating sessions using port numbers, conserving limited public IP space while maintaining connectivity.

NEW QUESTION: 13

You plan to use unified security policies to identify and control nested HTTP applications.
In this scenario, which two actions must you perform on your SRX Series Firewall? (Choose two.)
A. Install the application identification (AppID) feature license on the SRX Series Firewall.
B. Include dynamic application objects in your security policies.
C. Create all the unified security policies in the global zone.
D. Disable the default security policy.
Answer: A,B (LEAVE A REPLY)
The AppID license must be installed and active to enable application identification, which is required for unified security policies to recognize and control nested HTTP applications.
Dynamic application objects must be included in the unified security policies to match and control specific applications identified through AppID, such as Facebook within HTTPS traffic.

NEW QUESTION: 14
An SRX Series Firewall operates in which two modes? (Choose two.)
A. flow mode
B. packet mode
C. route mode
D. wireless mode
Answer: (SHOW ANSWER)
SRX Series Firewalls can operate in flow mode and packet mode.
- Flow mode provides stateful inspection, applying security policies and UTM features.
- Packet mode performs stateless packet-based forwarding, bypassing session-based processing.

NEW QUESTION: 15
You must monitor security policies on SRX Series devices dispersed throughout locations in your organization using a 'single pane of glass' cloud-based solution.
Which solution satisfies the requirement?
A. Juniper Sky Enterprise
B. J-Web
C. Junos Secure Connect
D. Junos Space
Answer: D (LEAVE A REPLY)
Junos Space is a management platform that provides a single pane of glass view of SRX Series devices dispersed throughout locations in your organization. It provides visibility into the security policies of the devices, allowing you to quickly identify and respond to security threats.
Additionally, it provides the ability to manage multiple devices remotely and in real-time, enabling you to quickly deploy and update security policies on all devices.

NEW QUESTION: 16
Which two security features are applied in a security policy? (Choose two.)
A. SSL proxy

B. firewall authentication
C. captive portal authentication
D. MAC bypass
Answer: (SHOW ANSWER)
SSL proxy can be applied in a security policy to inspect and control encrypted traffic.
Firewall authentication can also be configured within a security policy to require user authentication before allowing traffic to pass through the SRX device.

NEW QUESTION: 17
What must also be enabled when using source NAT if the address pool is in the same subnet as the interface?
A. proxy ARP
B. dynamic DNS
C. static NAT
D. destination NAT
Answer: A (LEAVE A REPLY)
When the source NAT address pool belongs to the same subnet as the egress interface, the SRX must respond to ARP requests for those translated IPs. Enabling proxy ARP allows the firewall to reply on behalf of those NAT pool addresses, ensuring proper packet delivery.

NEW QUESTION: 18
What are two valid security address objects within Juniper Networks? (Choose two.)
A. global address object
B. prefix address object
C. routing address object
D. MAC address object
Answer: A,B (LEAVE A REPLY)
Global address objects are defined at the global level and can be referenced by any security zone or policy.
Prefix address objects define IP subnets (for example, 192.168.1.0/24) and are commonly used in security policies to match source or destination traffic.

NEW QUESTION: 19

What are two system-defined zones created on the SRX Series Firewalls? (Choose two.)
A. junos-host
B. null
C. DMZ
D. management
Answer: A,B (LEAVE A REPLY)
junos-host is a system-defined zone that represents traffic destined to or from the SRX device itself (host traffic).
null is another system-defined zone used for interfaces not assigned to any user-defined security zone; traffic entering interfaces in the null zone is automatically dropped.

NEW QUESTION: 20
What is the main purpose of using screens on an SRX Series device?
A. to provide multiple ports for accessing security zones
B. to provide an alternative interface into the CLI
C. to provide protection against common DoS attacks
D. to provide information about traffic patterns traversing the network
Answer: (SHOW ANSWER)
The main purpose of using screens on an SRX Series device is to provide protection against common Denial of Service (DoS) attacks. Screens help prevent network resources from being exhausted or unavailable by filtering or blocking network traffic based on predefined rules. The screens are implemented as part of the firewall function on the SRX Series device, and they help protect against various types of DoS attacks, such as TCP SYN floods, ICMP floods, and UDP floods.

NEW QUESTION: 21
Which two non-configurable zones exist by default on an SRX Series device? (Choose two.)
A. Junos-host
B. functional
C. null
D. management
Answer: (SHOW ANSWER)
Junos-host and null are two non-configurable zones that exist by default on an SRX Series device. Junos-host is the default zone for all internal interfaces and services, such as management and other loopback interfaces. The null zone is used to accept all traffic that is not explicitly accepted by other security policies, and is the default zone for all unclassified traffic.
Both zones cannot be modified or deleted.

NEW QUESTION: 22
What is a purpose for creating multiple routing instances on an SRX Series Firewall device?
A. to manage routing protocols and updates
B. to simplify the configuration of network interfaces

C. to maintain separation of routing information for security purposes
D. to enable network monitoring through SNMP
Answer: C (LEAVE A REPLY)
Multiple routing instances are used to isolate and separate routing tables, enabling logical segmentation of traffic for security and traffic separation purposes on the SRX Series Firewall.

NEW QUESTION: 23
Which three operating systems are supported for installing and running Juniper Secure Connect client software? (Choose three.)
A. Windows 7
B. Android
C. Windows 10
D. Linux
E. macOS
Answer: (SHOW ANSWER)
Juniper Secure Connect client software is supported on the following three operating systems: Windows 7, Windows 10, and macOS. For more information, please refer to the Juniper Secure Connect Administrator Guide, which can be found on Juniper's website. The guide states: "The Juniper Secure Connect client is supported on Windows 7, Windows 10, and macOS." It also provides detailed instructions on how to install and configure the software for each of these operating systems.

NEW QUESTION: 24
Which two statements are correct about unified security policies? (Choose two.)
A. Dynamic applications in unified security policies analyze traffic based on Layer 4 information.
B. Traffic that matches a unified policy will not be evaluated by traditional security policy.
C. Dynamic applications in unified security policies analyze traffic based on Layer 7 information.
D. Traffic that matches a traditional policy will not be evaluated by unified security policy.
Answer: B,C (LEAVE A REPLY)
Traffic that matches a unified security policy is handled exclusively by the unified policy framework and is not further evaluated by traditional security policies.
Dynamic applications in unified security policies perform deep inspection using Layer 7 (application-layer) information to classify and control traffic based on application behavior.

NEW QUESTION: 25
Which two statements about the host-inbound-trafficparameter in a zone configuration are correct? (Choose two.)
A. Deleting the host-inbound-trafficparameter blocks SSH access to the firewall.
B. The host-inbound-trafficparameter is implicitly configured in the management zone.
C. Deleting the host-inbound-trafficparameter blocks console access to the firewall.
D. The host-inbound-trafficparameter is explicitly configured in a security zone.
Answer: A,D (LEAVE A REPLY)

Removing or not configuring the host-inbound-traffic parameter in a security zone will block management traffic (such as SSH, HTTPS, or ping) destined for the SRX firewall itself from interfaces in that zone.
The host-inbound-traffic parameter must be explicitly configured in each security zone to specify which protocols and services are allowed to reach the device's control plane.

NEW QUESTION: 26
Which statement is correct about capturing transit packets on an SRX Series Firewall?
A. You can capture transit packets on the egress interface using a firewall filter.
B. You can capture transit packets by using a firewall filter on the loopback interlace.
C. You can capture transit packets by using the tcpdump utility in the shell.
D. You can capture transit packets using sampling and port mirroring.
Answer: C (LEAVE A REPLY)
The tcpdump utility in the SRX shell captures live transit traffic directly from interfaces, allowing inspection of packets as they pass through the firewall.

NEW QUESTION: 27
What is the purpose of assigning logical interfaces to separate security zones in Junos OS?
A. to simplify the configuration of network interfaces
B. to control traffic that traverses different VLANs using security policies
C. to manage routing protocols and updates
D. to enable network monitoring through SNMP
Answer: B (LEAVE A REPLY)
Assigning logical interfaces to different security zones allows Junos OS to enforce security policies on traffic flowing between those zones, enabling controlled and policy-based traffic inspection and filtering.

NEW QUESTION: 28
Content filtering supports which two of the following protocols? (Choose two.)
A. HTTP
B. TFTP
C. SMTP
D. SNMP
Answer: (SHOW ANSWER)
Content filtering inspects and controls web traffic carried over HTTP, enabling filtering based on content categories and URLs.
Content filtering also supports SMTP, allowing inspection and filtering of email content for security and policy enforcement.

NEW QUESTION: 29
Which statement is correct about exception traffic?
A. Exception traffic refers to malformed IP packets received on the Packet Forwarding Engine.
B. Exception traffic is only handled on the Packet Forwarding Engine.

C. Exception traffic is rate-limited on the connection between the Packet Forwarding Engine and the Routing Engine.
D. Exception traffic is anything that is rejected by security policies and requires additional processing.
Answer: C (LEAVE A REPLY)
Exception traffic refers to packets that require special handling by the Routing Engine (RE) rather than being processed normally by the Packet Forwarding Engine (PFE). To protect the RE from overload, this traffic is rate-limited on the internal connection between the PFE and RE.

NEW QUESTION: 30
Which two statements about management functional zones are correct? (Choose two.)
A. The management functional zone contains all available revenue ports until they are assigned to a user-defined security zone.
B. The management functional zone cannot be referenced in any security policies.
C. The management functional zone is automatically created on the SRX Series Firewalls.
D. The management functional zone is used to control the management-related traffic that is allowed to access your device.
Answer: (SHOW ANSWER)
The management functional zone is automatically created on SRX Series Firewalls to handle device management traffic.
It is used to control and separate management-related traffic (such as SSH, HTTPS, SNMP, and NTP) from regular data traffic, ensuring secure and isolated management access to the device.

NEW QUESTION: 31
When does screening occur in the flow module?
A. during route lookup
B. during policy lookup
C. after session lookup
D. before session lookup
Answer: D (LEAVE A REPLY)
Screening in the flow module occurs before session lookup, allowing the device to drop unwanted or malicious traffic early in the processing path before any session is created.

NEW QUESTION: 32

Which two statements are correct about the processing to NAT rules within a rule set? (Choose two.)
A. NAT rule processing stops at the first match.
B. NAT rule processing processes all rules.
C. NAT rules are processed from top to bottom
D. NAT rules are processed from bottom to top.
Answer: A,C (LEAVE A REPLY)
NAT rule evaluation stops as soon as the first matching rule is found, preventing further rule processing.
NAT rules within a rule set are evaluated sequentially from top to bottom, enforcing ordered rule logic.

NEW QUESTION: 33
Which two statements are correct about the Junos OS? (Choose two.)
A. It is a network operating system.
B. It is supported on physical and virtual devices.
C. It is a network management system for Juniper devices.
D. It is a network operating system for IoT devices.
Answer: (SHOW ANSWER)
Junos OS is a network operating system developed by Juniper Networks to run on its routing, switching, and security devices.
It is supported on both physical (hardware-based) and virtual (software-based) platforms, such as vSRX and vMX.

NEW QUESTION: 34
You are not able to ping an interface on an SRX Series Firewall.
Which two actions should you take to solve this issue? (Choose two.)
A. Configure the ICMP protocol for host-inbound-traffic.
B. Create a security policy to allow ping traffic.
C. Assign the interface to a security zone.
D. Assign the interface to the null zone.
Answer: A,C (LEAVE A REPLY)
You must allow ICMP under the host-inbound-traffic setting for the zone so that the SRX device itself can respond to ping requests.
The interface must be assigned to a security zone; if it's not part of any zone, traffic to or from that interface (including ping) will be dropped by default.

NEW QUESTION: 35
Which two statements are true about the NextGen Web Filtering (NGWF) feature on an SRX Series device? (Choose two.)
A. The NGWF feature consults your local lists before consulting the Juniper cloud.
B. The NGWF feature does not require a license.
C. The NGWF feature consults the Juniper cloud before consulting your local lists.
D. The NGWF features requires a license.

Answer: (SHOW ANSWER)
NextGen Web Filtering consults the Juniper cloud first to categorize and evaluate URLs in real time, ensuring up-to-date threat and content intelligence.
NextGen Web Filtering is a licensed feature and requires a valid subscription to operate on an SRX Series device.

NEW QUESTION: 36
Your company is adding IP cameras to your facility to increase physical security. You are asked to help protect these loT devices from becoming zombies in a DDoS attack. Which Juniper ATP feature should you configure to accomplish this task?
A. IPsec
B. static NAT
C. allowlists
D. C&C feeds
Answer: (SHOW ANSWER)
Juniper ATP should be configured with C&C feeds that contain lists of malicious domains and IP addresses in order to prevent IP cameras from becoming zombies in a DDoS attack. This is an important step to ensure that the IP cameras are protected from malicious requests - and thus, they will not be able to be used in any DDoS attacks against the facility.

NEW QUESTION: 37
Which statement is correct about Junos security policies?
A. Security policies enforce rules that should be applied to traffic transiting an SRX Series device.
B. Security policies determine which users are allowed to access an SRX Series device.
C. Security policies control the flow of internal traffic within an SRX Series device.
D. Security policies identity groups of users that have access to different features on an SRX Series device.
Answer: (SHOW ANSWER)
The correct statement about Junos security policies is that they enforce rules that should be applied to traffic transiting an SRX Series device. Security policies control the flow of traffic between different zones on the SRX Series device, and dictate which traffic is allowed or denied.
They can also specify which application and service requests are allowed or blocked.

NEW QUESTION: 38
Which Web filtering solution uses a direct Internet-based service for URL categorization?
A. Juniper ATP Cloud
B. Websense Redirect
C. Juniper Enhanced Web Filtering
D. local blocklist
Answer: C (LEAVE A REPLY)

Juniper Enhanced Web Filtering is a web filtering solution that uses a direct Internet-based service for URL categorization. This service allows Enhanced Web Filtering to quickly and accurately categorize URLs and other web content, providing real-time protection against malicious content. Additionally, Enhanced Web Filtering is able to provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies.

NEW QUESTION: 39
You just made a configuration change to a security policy on your SRX Series Firewall. Your users alert you that an application that uses FTP is no longer working.
Referring to the exhibit, what are two ways to solve this problem? (Choose two.)

A. Enter the rollback 1command followed by a commitcommand.
B. Activate the ftpsecurity policy and commit the configuration.
C. Insert the ftpsecurity policy before the web-smtpsecurity policy.
D. Change the destination address in the ftpsecurity policy to anyand commit the configuration.
Answer: A,B (LEAVE A REPLY)
Rolling back one commit (rollback 1) and committing restores the previous working configuration where the FTP policy was active and functioning correctly.
The ftp policy is marked as inactive, which prevents it from being enforced. Activating it and committing the configuration will re-enable FTP traffic to Server-1, restoring service functionality.

NEW QUESTION: 40
Referring to the exhibit, the top table shows the source and destination IP addresses and also the source and destination ports of the incoming packet. The lower table represents the security policies from the trust zone to the untrust zone.
In this scenario, which two statements are correct? (Choose two.)

Src-IP	Dst-IP	Src-Port	Dst-Port
172.25.11.10	10.1.0.111	28641	80

Security Policies from Trust Zone to Untrust Zone

Src Addr	Dst Addr	Application	Action
172.25.11.0/24	10.1.0.0/16	ftp	deny
172.25.11.0/24	10.1.0.0/16	ssh	permit
172.25.11.0/24	10.1.0.0/16	https	permit
172.25.11.0/24	any	ping	permit
any	any	any	deny

A. The incoming packet is permitted by the HTTPS application.
B. The incoming packet is permitted since it does not match any policy listed.
C. The incoming packet is denied by the final security policy.
D. The firewall processes security policies in a top-down manner.
Answer: C,D (LEAVE A REPLY)
The packet's destination port is 80 (HTTP), which does not match any specific application policy in the table. As a result, it proceeds to the final policy, which denies all unmatched traffic (any any any deny).
Junos SRX evaluates security policies sequentially from top to bottom until a match is found.
Since no earlier policy matches HTTP traffic, the firewall enforces the final deny rule.

NEW QUESTION: 41
Which solution will add antivirus features to your SRX Series device?
A. IDP
B. Content Security
C. NAT
D. firewall filters
Answer: B (LEAVE A REPLY)
Content Security on SRX devices provides antivirus functionality by integrating malware scanning and file inspection services to protect traffic passing through the firewall.

NEW QUESTION: 42
Which two statements are true about Juniper ATP Cloud? (Choose two.)
A. Juniper ATP Cloud is an on-premises ATP appliance.
B. Juniper ATP Cloud can be used to block and allow IPs.
C. Juniper ATP Cloud is a cloud-based ATP subscription.
D. Juniper ATP Cloud delivers intrusion protection services.
Answer: (SHOW ANSWER)
Juniper ATP Cloud is a cloud-based ATP subscription that delivers advanced threat protection services, such as URL categorization, file reputation analysis, and malware analysis. It is able to quickly and accurately categorize URLs and other web content, and can also provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies.
Additionally, Juniper ATP Cloud is able to block and allow specific IPs, providing additional protection against malicious content.

NEW QUESTION: 43
Which two statements are correct about the content filter shown in the exhibit? (Choose two.)

A. .exe files will not be allowed to be downloaded over HTTP.
B. There will be an e-mail sent to the user about why the SRX is blocking the file.
C. There will be a notice added to the SRX log file about the file being blocked.
D. .exe files will not be allowed to be uploaded over HTTP.
Answer: A,C (LEAVE A REPLY)
The policy specifies direction download and file-types exe, meaning .exe files are blocked when users attempt to download them over HTTP.
The notification { log; } statement ensures that each blocked file attempt is recorded in the SRX device logs.

NEW QUESTION: 44
You are troubleshooting first path traffic not passing through an SRX Series Firewall. You have determined that the traffic is ingressing and egressing the correct interfaces using a route lookup.
In this scenario, what is the next step in troubleshooting why the device may be dropping the traffic?
A. Verify that the correct ALG is being used.
B. Verify that the interfaces are in the correct security zones.
C. Verify that source NAT is occurring.
D. Verify the routing protocol being used.
Answer: (SHOW ANSWER)
If traffic is entering and leaving the correct interfaces but still being dropped, the next step is to verify that the interfaces are assigned to the correct security zones. If an interface is in the wrong zone (or unassigned), the SRX will not apply the expected security policies, and the traffic will be dropped even though routing is correct.

NEW QUESTION: 45
Your manager asks you to verify when your antivirus definitions were last updated on your SRX Series Firewall.
Which operational mode command allows you to see this information?
A. show security web filtering status

B. show security utm anti-virus status
C. show security utm content-filtering statistics
D. show security utm anti-spam status
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
You are modifying the NAT rule order and you notice that a new NAT rule has been added to the bottom of the list.
In this situation, which command would you use to reorder NAT rules?
A. insert
B. run
C. top
D. up
Answer: (SHOW ANSWER)
The insert command is used to reorder NAT rules in Junos OS. It allows you to move a rule to a specific position within the rule set, such as insert rule rule-name before rule other-rule-name.
This ensures the correct evaluation order for NAT processing.

NEW QUESTION: 47
When a new traffic flow enters an SRX Series device, in which order are these processes performed?
A. screens --> zones --> security policies --> routes
B. routes --> zones --> screens --> security policies
C. screens --> routes --> zones --> security policies
D. screens --> security policies --> zones --> routes
Answer: C (LEAVE A REPLY)
When a new traffic flow enters an SRX Series Firewall, the processing order is:
1. Screens - Detect and block malicious or abnormal packets.
2. Routes - Determine the forwarding path based on the routing table.
3. Zones - Identify the source and destination security zones.
4. Security Policies - Evaluate the defined policies to permit or deny the traffic.

NEW QUESTION: 48
You must ensure that sessions can only be established from the external device.

Referring to the exhibit, which type of NAT is being performed?

A. static NAT and source NAT
B. static PAT only
C. source NAT only
D. destination NAT only
Answer: (SHOW ANSWER)
Destination NAT allows inbound session initiation from the external network by translating the public (untrust) address to a private internal (trust) address, ensuring that sessions can only be established from the external device.

NEW QUESTION: 49
Which type of NAT performs port address translation?
A. interface-based source NAT
B. static NAT
C. source NAT with address shifting
D. destination NAT without port forwarding
Answer: (SHOW ANSWER)
Interface-based source NAT performs Port Address Translation (PAT) by translating multiple internal source IP addresses and ports to the interface's IP address with unique port numbers.
This allows many internal hosts to share a single public IP address simultaneously.

NEW QUESTION: 50
Which two statements are correct about the null zone on an SRX Series device? (Choose two.)
A. The null zone is created by default.
B. The null zone is a functional security zone.
C. Traffic sent or received by an interface in the null zone is discarded.
D. You must enable the null zone before you can place interfaces into it.
Answer: (SHOW ANSWER)
According to the Juniper SRX Series Services Guide, the null zone is a predefined security zone that is created on the SRX Series device when it is booted. Traffic that is sent to or received on an interface in the null zone is discarded. The null zone is not a functional security zone, so you cannot enable or disable it.

NEW QUESTION: 51
Which two characteristics of destination NAT and static NAT are correct? (Choose two.)

A. Destination NAT requires address range sizes that match the devices being translated.
B. Destination NAT supports port forwarding.
C. Static NAT automatically creates a matching rule for the opposite direction.
D. Static NAT uses Port Address Translation.
Answer: (SHOW ANSWER)
Destination NAT supports port forwarding, allowing specific destination ports on a public IP to be translated to different internal IP addresses and ports.
Static NAT automatically creates a matching reverse translation, making it bi-directional - traffic can flow in both directions using the same mapping without additional configuration.

NEW QUESTION: 52
Which two security policies are installed by default on SRX 300 Series Firewalls? (Choose two.)
A. a security policy to allow all traffic from the trust zone to the trust zone
B. a security policy to allow all traffic from the trust zone to the untrust zone
C. a security policy to allow all traffic from the untrust zone to the trust zone
D. a security policy to allow all traffic from the management zone to the trust zone
Answer: (SHOW ANSWER)
A policy allowing all traffic from the trust zone to the trust zone, permitting internal communication.
A policy allowing all traffic from the untrust zone to the trust zone, which is implicitly denied, does not exist by default - however, the second default policy allows all traffic within the same zone, such as intra-zone communication (trust-to-trust).

NEW QUESTION: 53
You want to verify the peer before IPsec tunnel establishment.
What would be used as a final check in this scenario?
A. traffic selector
B. perfect forward secrecy
C. st0 interfaces
D. proxy ID
Answer: D (LEAVE A REPLY)
The proxy ID is used as a final check to verify the peer before IPsec tunnel establishment. The proxy ID is a combination of local and remote subnet and protocol, and it is used to match the traffic that is to be encrypted. If the proxy IDs match between the two IPsec peers, the IPsec tunnel is established, and the traffic is encrypted.

NEW QUESTION: 54
Which two statements are correct about security policies in SRX Series Firewalls? (Choose two.)
A. A security policy can only control inter-zone traffic.
B. A security policy can control both transit traffic and self-traffic.
C. A security policy can control both intra-zone traffic and inter-zone traffic.
D. A security policy can only control transit traffic.

Answer: C,D (LEAVE A REPLY)
Security policies on SRX Firewalls can control both intra-zone traffic (traffic within the same zone) and inter-zone traffic (traffic between different zones).
Security policies are designed to control transit traffic, meaning traffic passing through the firewall, not traffic destined to the device itself.

NEW QUESTION: 55
Which statement is correct about static NAT?
A. Static NAT supports port translation.
B. Static NAT rules are evaluated after source NAT rules.
C. Static NAT implements unidirectional one-to-one mappings.
D. Static NAT implements unidirectional one-to-many mappings.
Answer: C (LEAVE A REPLY)
Static NAT (Network Address Translation) is a type of NAT that maps a public IP address to a private IP address. With static NAT, a one-to-one mapping is created between a public IP address and a private IP address. This means that a single public IP address is mapped to a single private IP address, and all incoming traffic to the public IP address is forwarded to the private IP address.

NEW QUESTION: 56
What are two ways that an SRX Series device identifies content? (Choose two.)
A. It identifies and inspects the file extension of each file.
B. It uses ALGs.
C. It uses AppID.
D. It identifies file types in HTTP, FTP, and e-mail protocols.
Answer: C,D (LEAVE A REPLY)
The SRX uses AppID (Application Identification) to classify and inspect application traffic, enabling content-based controls such as web filtering and UTM.
The SRX can identify file types carried within HTTP, FTP, and e-mail protocols, allowing enforcement of content filtering, antivirus scanning, and data protection policies.

NEW QUESTION: 57
In which order does Junos OS process the various forms of NAT?
A. destination NAT, source NAT, static NAT
B. static NAT, destination NAT, source NAT
C. source NAT, static NAT, destination NAT
D. source NAT, destination NAT, static NAT
Answer: (SHOW ANSWER)
Junos OS processes NAT in the following order:
1. Static NAT - performed first so that address translations are consistent and reversible.
2. Destination NAT - applied next to translate destination addresses (e.g., inbound connections).
3. Source NAT - applied last to translate source addresses (e.g., outbound traffic).

NEW QUESTION: 58
You want to verify that your NextGen Web Filtering (NGWF) feature is connected to the Juniper cloud. Which operational mode command would you use for this task?
A. show security utm anti-spam status
B. show security utm content-filtering statistics
C. show security utm anti-virus status
D. show security web filtering status
Answer: (SHOW ANSWER)
The show security web filtering status command displays the connection status between the SRX device's NextGen Web Filtering (NGWF) feature and the Juniper Cloud. It verifies that the SRX is properly communicating with the cloud service for URL categorization and policy enforcement.

NEW QUESTION: 59
When traffic enters an interface, which two results does a route lookup determine? (Choose two.)
A. egress interface
B. egress security zone
C. ingress interface
D. DNS name
Answer: A,B (LEAVE A REPLY)
A route lookup determines the egress interface through which the traffic will exit the device.
Once the egress interface is known, the SRX identifies its associated egress security zone, which is then used for applying security policies.

NEW QUESTION: 60
Which UI enables you to manage, monitor and maintain multiple firewalls using a single interface?
A. Juniper Secure Analytics
B. Juniper Identify Management Service
C. Secure Connect
D. Security Director
Answer: D (LEAVE A REPLY)
Security Director provides centralized management, monitoring, and maintenance of multiple Juniper firewalls through a single unified interface.