Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1
What are two characteristics of a null zone? (Choose two.)

A. The null zone is configured by the super user.
B. By default, all unassigned interfaces are placed in the null zone.
C. All ingress and egress traffic on an interface in a null zone is permitted.
D. When an interface is deleted from a zone, it is assigned back to the null zone.

Answer: BD

NEW QUESTION 2
What is the correct order in which interface names should be identified?

A. system slot number –> interface media type –> port number –> line card slot number
B. system slot number –> port number –> interface media type –> line card slot number
C. interface media type –> system slot number –> line card slot number –> port number
D. interface media type –> port number –> system slot number –> line card slot number

Answer: C

NEW QUESTION 3
Click the Exhibit button.

```
[edit]
user@SRX# show security zones
security-zone Internal {
    host-inbound-traffic {
        system-services {
            http {
                except;
            }
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
```

What is the purpose of the host-inbound-traffic configuration shown in the exhibit?

A. to permit host inbound HTTP traffic and deny all other traffic on the internal security zone
B. to deny and log all host inbound traffic on the internal security zone, except for HTTP traffic
C. to permit all host inbound traffic on the internal security zone, but deny HTTP traffic
D. to permit host inbound HTTP traffic on the internal security zone

Answer: C

NEW QUESTION 4
Click the Exhibit button.

```
[edit security policies]
user@SRX# show
from-zone trust to-zone untrust {
    policy Rule-1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
    policy Rule-2 {
        match {
            source-address any;
            destination-address any;
            application [ junos-ping junos-ssh ];
        }
        then {
            permit;
        }
    }
}
```

You are asked to allow only ping and SSH access to the security policies shown in the exhibit. Which statement will accomplish this task?

A. Rename policy Rule-2 to policy Rule-0.
B. Insert policy Rule-2 before policy Rule-1.
C. Replace application any with application [junos-ping junos-ssh] in policy Rule-1.
D. Rename policy Rule-1 to policy Rule-3.

Answer: B

NEW QUESTION 5
You want to implement user-based enforcement of security policies without the requirement of certificates and supplicant software.
Which security feature should you implement in this scenario?

A. integrated user firewall
B. screens
C. 802.1X
D. Juniper ATP

Answer: D

Explanation:
In this scenario, you should implement Juniper ATP (Advanced Threat Prevention). Juniper ATP provides user-based enforcement of security policies without the requirement of certificates and supplicant software. It uses a combination of behavioral analytics, sandboxing, and threat intelligence to detect and respond to advanced threats in real time. Juniper ATP provides robust protection against targeted attacks, malicious insiders, and zero-day malware. For more information, please refer to the Juniper ATP product page on Juniper's website.

NEW QUESTION 6
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

Explanation:
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 7
You are deploying an SRX Series firewall with multiple NAT scenarios. In this situation, which NAT scenario takes priority?

A. interface NAT
B. source NAT
C. static NAT
D. destination NAT

Answer: A

Explanation:
This is because the interface NAT would allow the connections to pass through the firewall - and thus, would ensure that the appropriate ports are open in order to allow for the connections to be established.
This is a really important step in order to ensure that all of the appropriate traffic is allowed through the SRX Series firewall - and thus, it must be a priority when deploying the firewall.

NEW QUESTION 8
You are installing a new SRX Series device and you are only provided one IP address from your ISP. In this scenario, which NAT solution would you implement?

A. pool-based NAT with PAT
B. pool-based NAT with address shifting
C. interface-based source NAT
D. pool-based NAT without PAT

Answer: C

NEW QUESTION 9
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: CD

Explanation:
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.
References:
https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s
https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s

NEW QUESTION 10
What information does the show chassis routing-engine command provide?

A. chassis serial number
B. resource utilization
C. system version
D. routing tables

Answer: B

NEW QUESTION 10
Click the Exhibit button.

```
[edit security policies]
user@vSRX-1# edit from-zone trust to-zone dmz policy Trust-DMZ-Access
[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access]
user@vSRX-1# exit
```

Referring to the exhibit, a user is placed in which hierarchy when the exit command is run?

A. [edit security policies from-zone trust to-zone dmz] user@vSRX-1#
B. [edit] user@vSRX-1#
C. [edit security policies] user@vSRX-1#
D. user@vSRX-1>

Answer: A

NEW QUESTION 11
Which two security features inspect traffic at Layer 7? (Choose two.)

A. IPS/IDP
B. security zones
C. application firewall
D. integrated user firewall

Answer: AC

NEW QUESTION 15
Which statement is correct about Web filtering?

A. The Juniper Enhanced Web Filtering solution requires a locally managed server.

B. The decision to permit or deny is based on the body content of an HTTP packet.
C. The decision to permit or deny is based on the category to which a URL belongs.
D. The client can receive an e-mail notification when traffic is blocked.

Answer: C

Explanation:
Web filtering is a feature that allows administrators to control access to websites by categorizing URLs into different categories such as gambling, social networking, or adult content. The decision to permit or deny access to a website is based on the category to which a URL belongs. This is done by comparing the URL against a database of categorized websites and making a decision based on the policy defined by the administrator.

NEW QUESTION 17
Which statement about global NAT address persistence is correct?

A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.
B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.
C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.
D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

Answer: A

Explanation:
Use the persistent-nat feature to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address (the public IP address and port created by the NAT device closest to the STUN server). The source NAT rule action can use a source NAT pool (with or without port translation) or an egress interface.

NEW QUESTION 18
Which two statements are correct about screens? (Choose two.)

A. Screens process inbound packets.
B. Screens are processed on the routing engine.
C. Screens process outbound packets.
D. Screens are processed on the flow module.

Answer: AD

NEW QUESTION 19
What must be enabled on an SRX Series device for the reporting engine to create reports?

A. System logging
B. SNMP
C. Packet capture
D. Security logging

Answer: D

NEW QUESTION 23
Which security policy type will be evaluated first?

A. A zone policy with no dynamic application set
B. A global with no dynamic application set
C. A zone policy with a dynamic application set
D. A global policy with a dynamic application set

Answer: D

NEW QUESTION 28
Which statement about NAT is correct?

A. Destination NAT takes precedence over static NAT.
B. Source NAT is processed before security policy lookup.
C. Static NAT is processed after forwarding lookup.
D. Static NAT takes precedence over destination NAT.

Answer: D

NEW QUESTION 30
Which two UTM features should be used for tracking productivity and corporate user behavior? (Choose two.)

A. the content filtering UTM feature
B. the antivirus UTM feature
C. the Web filtering UTM feature
D. the antispam UTM feature

Answer: AC

NEW QUESTION 31
Which Juniper ATP feed provides a dynamic list of known botnet servers and known sources of malware downloads?

A. infected host cloud feed
B. Geo IP feed
C. C&C cloud feed
D. blocklist feed

Answer: A

NEW QUESTION 33
Which two statements are correct about global policies? (Choose two.)

A. Global policies are evaluated after default policies.
B. Global policies do not have to reference zone context.
C. Global policies are evaluated before default policies.
D. Global policies must reference zone contexts.

Answer: BC

Explanation:
Global policies are used to define rules for traffic that is not associated with any particular zone. This type of policy is evaluated first, before any rules related to specific zones are evaluated.
For more detailed information about global policies, refer to the Juniper Networks Security Policy Overview guide, which can be found at
https://www.juniper.net/documentation/en_US/junos/topics/reference/security-policy-overview.html. The guide provides an overview of the Juniper Networks security policy architecture, as well as detailed descriptions of the different types of policies and how they are evaluated.

NEW QUESTION 37
What are two functions of Juniper ATP Cloud? (Choose two.)

A. malware inspection
B. Web content filtering
C. DDoS protection
D. Geo IP feeds

Answer: AD

Explanation:
Juniper Advanced Threat Prevention (ATP) Cloud is a security service that helps organizations protect against advanced threats by providing real-time threat intelligence and automated response capabilities. It combines a cloud-based threat intelligence platform with the security capabilities of Juniper Networks security devices to provide comprehensive protection against advanced threats. The two functions of Juniper ATP Cloud include malware inspection and Geo IP feeds. The malware inspection component provides real-time protection against known and unknown threats by analyzing suspicious files and determining if they are malicious. The Geo IP feeds provide a global view of IP addresses and their associated countries, allowing organizations to identify and block traffic from known malicious countries.

NEW QUESTION 42
Click the Exhibit button.

```
policies {
    from-zone untrust to-zone trust {
        policy permit-all {
        [...]
            then {
                permit;
            }
        }
        policy deny-all {
        [...]
            then {
                deny;
            }
        }
        policy reject-all {
        [...]
            then {
                reject;
            }
        }
    }
}
```

Which two statements are correct about the partial policies shown in the exhibit? (Choose two.)

A. UDP traffic matched by the deny-all policy will be silently dropped.

B. TCP traffic matched by the reject-all policy will have a TCP RST sent.
C. TCP traffic matched from the zone trust is allowed by the permit-all policy.
D. UDP traffic matched by the reject-all policy will be silently dropped.

Answer: AB

NEW QUESTION 46
You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses. Which NAT configuration is appropriate in this scenario?

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

Answer: D

Explanation:
https://www.juniper.net/documentation/en_US/day-one-books/nat-and-pat-en.html
And the specific text that would support the above answer is as follows: "Static NAT, which requires manual configuration, is often the most appropriate configuration for mapping one internal address to one external address."

NEW QUESTION 51
Which two traffic types are considered exception traffic and require some form of special handling by the PFE? (Choose two.)

A. SSH sessions
B. ICMP reply messages
C. HTTP sessions
D. traceroute packets

Answer: BD

NEW QUESTION 54
Screens on an SRX Series device protect against which two types of threats? (Choose two.)

A. IP spoofing
B. ICMP flooding
C. zero-day outbreaks
D. malicious e-mail attachments

Answer: AB

Explanation:
 ICMP flood
Use the ICMP flood IDS option to protect against ICMP flood attacks. An ICMP flood attack typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
The threshold value defines the number of ICMP packets per second (pps) allowed to be send to the same destination address before the device rejects further ICMP packets.
IP spoofing
Use the IP address spoofing IDS option to prevent spoofing attacks. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-introdu

NEW QUESTION 58
What are two valid address books? (Choose two.)

A. 66.129.239.128/25
B. 66.129.239.154/24
C. 66.129.239.0/24
D. 66.129.239.50/25

Answer: AC

Explanation:
Network Prefixes in Address Books
You can specify addresses as network prefixes in the prefix/length format. For example, 203.0.113.0/24 is an acceptable address book address because it translates to a network prefix. However, 203.0.113.4/24 is not acceptable for an address book because it exceeds the subnet length of 24 bits. Everything beyond the subnet length must be entered as 0 (zero). In special scenarios, you can enter a hostname because it can use the full 32-bit address length.
https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-address

NEW QUESTION 60
SRX Series devices have a maximum of how many rollback configurations?

A. 40
B. 60
C. 50
D. 10

Answer: C

NEW QUESTION 62
When are Unified Threat Management services performed in a packet flow?

A. before security policies are evaluated
B. as the packet enters an SRX Series device
C. only during the first path process
D. after network address translation

Answer: D

Explanation:
https://iosonounrouter.wordpress.com/2018/07/07/how-does-a-flow-based-srx-work/

NEW QUESTION 63
When operating in packet mode, which two services are available on the SRX Series device? (Choose two.)

A. MPLS
B. UTM
C. CoS
D. IDP

Answer: AC

NEW QUESTION 67
......