Get Free Juniper JN0-232 Dumps PDF Questions

Why risk failure? Download updated Juniper Security, Associate exam PDF questions today. Practice with real JN0-232 dumps and verified answers designed to help you ace your certification quickly using PrepBolt JN0-232 exam pdf questions and answers.

Thank you for Downloading JN0-232 exam PDF Demo

https://prepbolt.com/JN0-232.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

Which two statements about functional zones are correct? (Choose two.)

Options:

A- You can 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:

A, D

Explanation:

A functional zone is used for special purposes, such as management interfaces. Juniper documentation states that currently only the management (MGT) functional zone is supported, which makes option A correct. The management functional zone is used for dedicated management interfaces and can be configured with host-inbound-traffic and screen options to protect management access, which makes option D correct. Option B is incorrect because functional zones are not groups of logical interfaces belonging to multiple security zones; they are special-purpose zones. Option C is incorrect because Juniper specifically states that the management functional zone cannot be specified in security policies, and traffic entering the management zone does not match policies.

Question 2

Question Type: MultipleChoice

You want to enable NextGen Web Filtering (NGWF) on your SRX Series Firewall. Which two actions must you perform in this scenario? (Choose two.)

Options:

A- Install a NextGen Web Filtering feature license.

B- Enable NextGen Web Filtering as the default Web Filtering type.
C- Assign a public IP address to the loopback interface.
D- Enable SSL host inbound traffic on the untrust security zone.

Answer:

A, B

Explanation:

To enable Juniper NextGen Web Filtering, the SRX must have the required NGWF license and the web-filtering type must be configured for NGWF. Juniper documentation states that Enhanced Web Filtering and NGWF require separate licenses and that NGWF can use the wf_key_ng_juniper license key. Juniper also documents NGWF as a configurable web-filtering type, including ng-juniper, and notes that administrators can confirm missing license conditions using the web-filtering status command. A public IP address on the loopback interface is not a general NGWF requirement. SSL host inbound traffic on the untrust zone is also not required for enabling NGWF; SSL proxy or SNI behavior may affect HTTPS inspection, but it is not the base enablement step.

Question 3

Question Type: MultipleChoice

Referring to the exhibit, which two statements are correct? (Choose two.)

```
user@SRX> show security policies policy-name https-access detail
Policy: https-access, action-type: permit, services-offload:not-configured , State: enabled,
Index: 9, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: Trust, To zone: Untrust
  Source vrf group:
    any
  Destination vrf group:
    any
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-https
    IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination ports: 443
  Source identity feeds:
    any
  Destination identity feeds:
    any
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Session log: at-close
```

Options:

A- This security policy is a zone-based security policy.
B- This security policy uses a non-default inactivity timeout.
C- This security policy permits HTTPS traffic.
D- This security policy is the second security policy in the list.

Answer:

A, C

Explanation:

The exhibit shows From zone: Trust, To zone: Untrust, which identifies the policy as a zone-based security policy. It also shows the policy action as permit and the application as junos-https, with TCP destination port 443. Therefore, the policy permits HTTPS traffic. The displayed inactivity timeout is 1800 seconds, which is the normal value shown for predefined TCP applications such as HTTPS, so it does not prove a non-default timeout. The exhibit also shows sequence number 1, not sequence number 2, so it is not the second policy in the list. Junos security policies are configured in a from-zone to to-zone context and match traffic by criteria such as source address, destination address, and application before applying the configured action.

Question 4

Question Type: MultipleChoice

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

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

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

Options:

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:

A, C

Explanation:

The policy table applies to traffic from the Trust zone to the Untrust zone. The source prefix 172.25.11.0/24 and destination prefix 10.1.0.0/16 are matched for FTP, SSH, HTTPS, and ping actions. FTP traffic from 172.25.11.11 to 10.1.0.10 matches the FTP deny policy, so option A is correct. SSH traffic from 172.25.11.10 to 10.1.0.10 matches the SSH permit policy, so option C is correct. Ping from 172.25.11.100 to 10.1.0.10 is permitted, not denied, because the ping policy permits it. Option D reverses the source and destination direction and does not match the displayed Trust-to-Untrust policy table. Security policies are matched using zone context, source address, destination address, and application.

Question 5

Question Type: MultipleChoice

Which two statements correctly describe static NAT? (Choose two.)

Options:

A- It requires address ranges of the same size.
B- Address pools are necessary.
C- No address pools are necessary.
D- It performs PAT.

Answer:

A, C

Explanation:

Static NAT creates a fixed one-to-one mapping between real and mapped addresses. Juniper documentation describes static NAT as mapping one IP subnet to another IP subnet and states that translation is limited to one-to-one mappings or address blocks of the same size. This makes option A correct. Juniper also states that no address pools are necessary for static NAT, which makes option C correct. Address pools are commonly associated with source NAT or destination NAT pool configurations, not the basic static NAT mapping model. Static NAT can support static port mapping in specific configurations, but the general static NAT behavior tested here is one-to-one address translation, not dynamic PAT. Therefore, the correct answers are A and C.

Question 6

Question Type: MultipleChoice

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;
    }
}
```

Options:

A- default policy
B- intra-zone policy
C- inter-zone policy
D- global policy

Answer:

B

Explanation:

The exhibit shows a policy configured under from-zone Trust to-zone Trust. Because the source zone and destination zone are the same, this is an intra-zone security policy. An inter-zone policy would have different source and destination zones, such as Trust to Untrust. A global policy does not require the same specific from-zone and to-zone context in the same way as a zone-based policy. A default policy is the implicit final behavior used when no configured security policy matches. Junos security policies enforce rules for transit traffic using zone context, source address, destination address, application, and action. Since both zone references are Trust, the displayed policy is clearly an intra-zone policy.

Question 7

Question Type: MultipleChoice

Which solution will add antivirus features to your SRX Series device?

Options:

A- IDP
B- Content Security
C- NAT
D- firewall filters

Answer:

B

Explanation:

Content Security is the Juniper solution that adds antivirus capabilities to SRX Series Firewalls. Juniper Content Security includes several UTM-style services, such as antivirus, antispam, content filtering, and web filtering. The antivirus feature scans supported traffic to detect and block malicious files or virus-related content according to configured profiles and policies. IDP provides intrusion detection and prevention signatures, but it is not the specific solution that adds antivirus scanning. NAT translates IP addresses and ports and has no antivirus function. Firewall filters provide stateless packet filtering and traffic classification, not file-based malware inspection. Therefore, Content Security is the correct answer for adding antivirus features to an SRX Series device.

Thank You for trying JN0-232 PDF Demo

To try our JN0-232 practice exam software visit link below

https://prepbolt.com/JN0-232.html

Start Your JN0-232 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your JN0-232 preparation with actual exam questions.