Number: JN0-231
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: JN0-231
Exam Name: Security, Associate

IT Certification Exams - Questions & Answers | Vdumps.com

Exam A

QUESTION 1
Which feature would you use to protect clients connected to an SRX Series device from a SYN flood attack?

A. security policy
B. host inbound traffic
C. application layer gateway
D. screen option

Correct Answer: D
Section:
Explanation:
A screen option in the SRX Series device can be used to protect clients connected to the device from a SYN flood attack. Screens are security measures that you can use to protect your network from various types of attacks, including SYN floods. A screen option specifies a set of rules to match against incoming packets, and it can take specific actions such as discarding, logging, or allowing the packets based on the rules.
Reference:
Juniper Networks SRX Series Services Gateway Screen Configuration Guide:
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-screenconfiguring.html

QUESTION 2
Which two statements about user-defined security zones are correct? (Choose two.)

A. Users cannot share security zones between routing instances.
B. Users can configure multiple security zones.
C. Users can share security zones between routing instances.
D. User-defined security zones do not apply to transit traffic.

Correct Answer: B, C
Section:
Explanation:
User-defined security zones allow users to configure multiple security zones and share them between routing instances. This allows users to easily manage multiple security zones and their associated policies. For example, a user can create a security zone for corporate traffic, a security zone for guest traffic, and a security zone for public traffic, and then configure policies to control the flow of traffic between each of these security zones. Transit traffic can also be managed using userdefined security zones, as the policies applied to these zones will be applied to the transit traffic as well.
Reference:
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-zonesoverview-configuring.html
https://www.juniper.net/documentation/en_US/junos/topics/task/security/security-zonesconfiguring-shared.html

QUESTION 3
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

Correct Answer: C
Section:
Explanation:
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.
Reference: https://www.juniper.net/documentation/en_US/junos-space-securitydirector/topics/task/configuration/security-services-web-filtering-enhanced.html
https://www.juniper.net/documentation/en_US/junos-space-securitydirector/topics/task/configuration/security-services-web-filtering-enhanced-overview.html

QUESTION 4
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

Correct Answer: A, C
Section:
Explanation:
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.

QUESTION 5
What is the default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel?

A. 20 seconds
B. 5 seconds
C. 10 seconds
D. 40 seconds

Correct Answer: B
Section:
Explanation:
The default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel is 5 seconds. DPD is a mechanism that enables the IPsec device to detect if the peer is still reachable or if the IPsec VPN tunnel is still active. The DPD interval determines how often the IPsec device sends DPD packets to the peer to check the status of the VPN tunnel. A value of 5 seconds is a common default, but the specific value can vary depending on the IPsec device and its configuration.
Reference:
Juniper Networks Technical Documentation: Configuring IPsec VPNs:
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ipsec-vpnoverview-srx-series.html

QUESTION 6
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

Correct Answer: C
Section:
Explanation:
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.
Reference: https://www.juniper.net/documentation/en_US/junos/topics/concept/security-srxseries-firewall-screen-dos.html

QUESTION 7
What are two functions of Juniper ATP Cloud? (Choose two.)

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

Correct Answer: A, D
Section:
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.

QUESTION 8
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>

Correct Answer: A
Section:

QUESTION 9
You want to enable the minimum Juniper ATP services on a branch SRX Series device.
In this scenario, what are two requirements to accomplish this task? (Choose two.)

A. Install a basic Juniper ATP license on the branch device.
B. Configure the juniper-atp user account on the branch device.
C. Register for a Juniper ATP account on https://sky.junipersecurity.net.
D. Execute the Juniper ATP script on the branch device.

Correct Answer: C, D
Section:
Explanation:
https://manuals.plus/m/95fded847e67e8f456453182a54526ba3224a61a337c47177244d345d1f3b19e.pdf

QUESTION 10
SRX Series devices have a maximum of how many rollback configurations?

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

Correct Answer: C
Section:

QUESTION 11
Unified threat management (UTM) inspects traffic from which three protocols? (Choose three.)

A. FTP
B. SMTP
C. SNMP
D. HTTP
E. SSH

Correct Answer: A, B, D
Section:
Explanation:
https://www.inetzero.com/blog/unified-threat-management-deeper-dive-traffic-inspection/

QUESTION 12
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

Correct Answer: D
Section:
Explanation:

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

QUESTION 13
When configuring antispam, where do you apply any local lists that are configured?

A. custom objects
B. advanced security policy
C. antispam feature-profile
D. antispam UTM policy

Correct Answer: A
Section:
Explanation:
https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/securitylocal-list-antispam-filtering.html

QUESTION 14
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

Correct Answer: A, B
Section:
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/topicmap/security-introduction-to-adp.html

QUESTION 15
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.

Correct Answer: A
Section:
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.

QUESTION 16
You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.
Which Juniper ATP solution will accomplish this task?

A. Geo IP
B. unified security policies
C. IDP
D. C&C feed

Correct Answer: A
Section:
Explanation:
Juniper ATP Geo IP can help to accomplish this task by using geolocation services to determine the geographical location of IP addresses. As IP prefixes get allocated to the countries that you have specified, the Geo IP solution will automatically update the configured firewall policies to block any traffic that is coming from those specific countries.
This is a great solution for blocking specific countries - as it will allow for a more personalized and targeted approach to firewall policies - and thus, to increase the effectiveness of the solution at blocking potential malicious traffic.

QUESTION 17
Which two statements are correct about IKE security associations? (Choose two.)

A. IKE security associations are established during IKE Phase 1 negotiations.
B. IKE security associations are unidirectional.
C. IKE security associations are established during IKE Phase 2 negotiations.
D. IKE security associations are bidirectional.

Correct Answer: A, D
Section:

QUESTION 18
You want to deploy a NAT solution.
In this scenario, which solution would provide a static translation without PAT?

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

Correct Answer: B
Section:
Explanation:
Translation of the original source IP address to an IP address from a user-defined address pool by shifting the IP addresses. This type of translation is one-to-one, static, and without port address translation. If the original source IP address range is larger than the IP address range in the userdefined pool, untranslated packets are dropped.
https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-securitysource-and-source-pool.html

QUESTION 19
Which Juniper Networks solution uses static and dynamic analysis to search for day-zero malware threats?

A. firewall filters

B. UTM
C. Juniper ATP Cloud
D. IPS

Correct Answer: C
Section:
Explanation:
Malware Sandboxing
Detect and stop zero-day and commodity malware within web, email, data center, and application traffic targeted for Windows, Mac, and IoT devices.
https://www.juniper.net/us/en/products/security/advanced-threat-prevention.html

QUESTION 20
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

Correct Answer: D
Section:
Explanation:
https://www.juniper.net/documentation/en_US/day-one-books/nat-and-pat-en.htmlAnd the specific text that would support the above answer is as follows: "Static NAT, which requiresmanual configuration, is often the most appropriate configuration for mapping one internal addressto one external address."

QUESTION 21
You want to provide remote access to an internal development environment for 10 remote developers.
Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

A. an additional license for an SRX Series device
B. Juniper Secure Connect client software
C. an SRX Series device with an SPC3 services card
D. Marvis virtual network assistant

Correct Answer: A, B
Section:

QUESTION 22
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

Correct Answer: A
Section:
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.

QUESTION 23
Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server.
In this scenario, which two configuration features need to be added? (Choose two.)

A. firewall filter
B. security policy
C. proxy-ARP
D. UTM policy

Correct Answer: B, C
Section:

QUESTION 24
Click the Exhibit button.

```
user@vSRX-VR> ping 10.10.102.10 count 5 routing-instance DMZ
PING 10.10.102.10 (10.10.102.10): 56 data bytes
64 bytes from 10.10.102.10: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 10.10.102.10: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.10.102.10: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.10.102.10: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.102.10: icmp_seq=4 ttl=64 time=0.070 ms
--- 10.10.102.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.051/0.070/0.011 ms
user@vSRX-VR>
```

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

A. The DMZ routing-instance is the source.
B. The 10.10.102.10 IP address is the source.
C. The 10.10.102.10 IP address is the destination.
D. The DMZ routing-instance is the destination.

Correct Answer: A, C
Section:

QUESTION 25
Which IPsec protocol is used to encrypt the data payload?

A. ESP
B. IKE

C. AH
D. TCP

Correct Answer: A
Section:

QUESTION 26
What are three primary match criteria used in a Junos security policy? (Choose three.)

A. application
B. source address
C. source port
D. class
E. destination address

Correct Answer: A, B, E
Section:

QUESTION 27
You have an FTP server and a webserver on the inside of your network that you want to make available to users outside of the network. You are allocated a single public IP address.
In this scenario, which two NAT elements should you configure? (Choose two.)

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

Correct Answer: A, B
Section:
Explanation:
With single Ip address it is port forwarding. So, destination NAT and a pool address point to the single public IP of the internet facing interface.

QUESTION 28
Which three Web filtering deployment actions are supported by Junos? (Choose three.)

A. Use IPS.
B. Use local lists.
C. Use remote lists.
D. Use Websense Redirect.
E. Use Juniper Enhanced Web Filtering.

Correct Answer: B, D, E
Section:
Explanation:
https://www.juniper.net/documentation/us/en/software/junos/utm/topics/concept/utm-webfiltering-overview.html

QUESTION 29

Which two IPsec hashing algorithms are supported on an SRX Series device? (Choose two.)

A. SHA-1
B. SHAKE128
C. MD5
D. RIPEMD-256

Correct Answer: A, C
Section:

QUESTION 30
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

Correct Answer: C
Section:

QUESTION 31
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

Correct Answer: A, C
Section:

QUESTION 32
Which two statements are correct about the default behavior on SRX Series devices? (Choose two.)

A. The SRX Series device is in flow mode.
B. The SRX Series device supports stateless firewalls filters.
C. The SRX Series device is in packet mode.
D. The SRX Series device does not support stateless firewall filters.

Correct Answer: A, B
Section:

QUESTION 33
Which two statements are correct about functional zones? (Choose two.)

A. Functional zones must have a user-defined name.
B. Functional zone cannot be referenced in security policies or pass transit traffic.
C. Multiple types of functional zones can be defined by the user.
D. Functional zones are used for out-of-band device management.

Correct Answer: B, D
Section:

QUESTION 34
You are assigned a project to configure SRX Series devices to allow connections to your webservers.
The webservers have a private IP address, and the packets must use NAT to be accessible from the Internet. The webservers must use the same address for both connections from the Internet and communication with update servers.
Which NAT type must be used to complete this project?

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

Correct Answer: C
Section:
Explanation:
Only static NAT with pool ensures both traffic initiated from inside and outside networks use the same IP address.

QUESTION 35
Which two user authentication methods are supported when using a Juniper Secure Connect VPN?
(Choose two.)

A. certificate-based
B. multi-factor authentication
C. local authentication
D. active directory

Correct Answer: C, D
Section:
Explanation:
"Local Authentication—In local authentication, the SRX Series device validates the user credentials by checking them in the local database. In this method, the administrator handles change of password or resetting of forgotten password.
Here, it requires that an user must remember a new password. This option is not much preferred from a security standpoint.
• External Authentication—In external authentication, you can allow the users to use the same user credentials they use when accessing other resources on the network. In many cases, user credentials are domain logon used for Active Directory or any other LDAP authorization system. This method simplifies user experience and improves the organization's security posture; because you can maintain the authorization system with the regular security policy used by your organization."
https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connectadministrator-guide/topics/topic-map/secure-connect-getting-started.html

QUESTION 36
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.

Correct Answer: A, B
Section:

QUESTION 37
Which two IKE Phase 1 configuration options must match on both peers to successfully establish a tunnel? (Choose two.)

A. VPN name
B. gateway interfaces
C. IKE mode
D. Diffie-Hellman group

Correct Answer: C, D
Section:

QUESTION 38
What are three Junos UTM features? (Choose three.)

A. screens
B. antivirus
C. Web filtering
D. IDP/IPS
E. content filtering

Correct Answer: B, C, E
Section:

QUESTION 39
You are investigating a communication problem between two hosts and have opened a session on the SRX Series device closest to one of the hosts and entered the show security flow session command.
What information will this command provide? (Choose two.)

A. The total active time of the session.
B. The end-to-end data path that the packets are taking.
C. The IP address of the host that initiates the session.
D. The security policy name that is controlling the session.

Correct Answer: C, D
Section:

QUESTION 40
A security zone is configured with the source IP address 192.168.0.12/255.255.0.255 wildcard match.
In this scenario, which two IP packets will match the criteria? (Choose two.)

A. 192.168.1.21
B. 192.168.0.1
C. 192.168.1.12
D. 192.168.22.12

Correct Answer: C, D
Section:

QUESTION 41
When creating a site-to-site VPN using the J-Web shown in the exhibit, which statement is correct?

A. The remote gateway is configured automatically based on the local gateway settings.
B. RIP, OSPF, and BGP are supported under Routing mode.
C. The authentication method is pre-shared key or certificate based.
D. Privately routable IP addresses are required.

Correct Answer: D
Section:

QUESTION 42
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

Correct Answer: D
Section:

QUESTION 43
Which two statements are correct about the integrated user firewall feature?(Choose two.)

A. It maps IP addresses to individual users.
B. It supports IPv4 addresses.
C. It allows tracking of non-Windows Active Directory users.
D. It uses the LDAP protocol.

Correct Answer: A, C
Section:

QUESTION 44
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

Correct Answer: D
Section:

QUESTION 45
What does the number ''2'' indicate in interface ge—0/1/2?

A. The interface logical number
B. The physical interface card (PIC)

C. The port number
D. The flexible PIC concentrator (FPC)

Correct Answer: C
Section:

QUESTION 46
Which statement about service objects is correct?

A. All applications are predefined by Junos.
B. All applications are custom defined by the administrator.
C. All applications are either custom or Junos defined.
D. All applications in service objects are not available on the vSRX Series device.

Correct Answer: C
Section:
Explanation:
"Service objects represent applications and services that can be assigned to a security policy rule.
Applications and services can either be predefined by Junos software or custom defined by the administrator."
Reference:
Juniper Networks JNCIA-SEC Exam Guide:
https://www.juniper.net/training/certification/certification-exam-guides/jncia-sec-exam-guide/

QUESTION 47
You want to block executable files ("exe) from being downloaded onto your network.
Which UTM feature would you use in this scenario?

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

Correct Answer: B
Section:
Explanation:
According to the Juniper Networks official JNCIA-SEC Exam Guide, web filtering is a feature used to control access to web content, including the ability to block specific types of files.
In the scenario mentioned, you want to block executable files from being downloaded, which can be accomplished by using web filtering. The feature allows administrators to configure policies that block specific file types, including "exe" files, from being downloaded.
Reference:
Juniper Networks JNCIA-SEC Exam Guide:
https://www.juniper.net/training/certification/certification-exam-guides/jncia-sec-exam-guide/

QUESTION 48
What are two Juniper ATP Cloud feed analysis components? (Choose two.)

A. IDP signature feed
B. C&C cloud feed
C. infected host cloud feed

D. US CERT threat feed

Correct Answer: A, B
Section:
Explanation:
The Juniper ATP Cloud feed analysis components are the IDP signature feed and the C&C cloud feed.
The IDP signature feed provides a database of signatures from known malicious traffic, while the C&C cloud feed provides the IP addresses of known command and control servers. The infected host cloud feed and US CERT threat feed are not components of the Juniper ATP Cloud feed analysis.
To learn more about the Juniper ATP Cloud feed analysis components, refer to the Juniper Networks Security Automation and Orchestration (SAO) official documentation, which can be found at https://www.juniper.net/documentation/en_US/sao/topics/concept/security-automation-andorchestration-overview.html. The documentation provides an overview of the SAO platform and an in-depth look at the various components of the
Juniper ATP Cloud feed analysis.

QUESTION 49
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.

Correct Answer: B, C
Section:
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-policyoverview.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.

QUESTION 50
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.

Correct Answer: C
Section:
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.
Reference:
Juniper Networks SRX Series Services Gateway Web Filtering Configuration Guide:
https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topicmap/security-services-web-filtering.html

QUESTION 51
You have configured a UTM feature profile.
Which two additional configuration steps are required for your UTM feature profile to take effect?

IT Certification Exams - Questions & Answers | Vdumps.com

(Choose two.)

A. Associate the UTM policy with an address book.
B. Associate the UTM policy with a firewall filter.
C. Associate the UTM policy with a security policy.
D. Associate the UTM feature profile with a UTM policy.

Correct Answer: C, D
Section:
Explanation:
For the UTM feature profile to take effect, it must be associated with a security policy and a UTM policy. The security policy defines the traffic flow and the actions that should be taken on the traffic, while the UTM policy defines the security features to be applied to the traffic, such as antivirus, intrusion prevention, and web filtering. The UTM feature profile provides the necessary configuration for the security features defined in the UTM policy.
Reference:
Juniper Networks SRX Series Services Gateway UTM Configuration Guide:
https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topicmap/security-services-utm.html

QUESTION 52
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

vdumps

Correct Answer: D
Section:
Explanation:
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.
Reference:
Juniper Networks SRX Series Services Gateway IPsec Configuration Guide:
https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topicmap/security-ipsec-vpn-configuring.html

QUESTION 53
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

Correct Answer: A, C, E
Section:
Explanation:
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.

QUESTION 54
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

Correct Answer: C
Section:

QUESTION 55
Which two statements are correct about IPsec security associations? (Choose two.)

A. IPsec security associations are bidirectional.
B. IPsec security associations are unidirectional.
C. IPsec security associations are established during IKE Phase 1 negotiations.
D. IPsec security associations are established during IKE Phase 2 negotiations.

Correct Answer: A, D
Section:
Explanation:
The two statements that are correct about IPsec security associations are that they are bidirectional and that they are established during IKE Phase 2 negotiations. IPsec security associations are bidirectional, meaning that they provide security for both incoming and outgoing traffic. IPsec security associations are established during IKE Phase 2 negotiations, which negotiates the security parameters and establishes the security association between the two peers. For more information, please refer to the Juniper Networks IPsec VPN Configuration Guide, which can be found on Juniper's website.

QUESTION 56
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

Correct Answer: D
Section:
Explanation:
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. For more information, please refer to the Juniper Networks Junos Space Network Director User Guide, which can be found on Juniper's website.

QUESTION 57
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

Correct Answer: C
Section:
Explanation:
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. For more information, please refer to the Juniper Networks SRX Series Services Gateways Security Configuration Guide, which can be found on Juniper's website.

QUESTION 58
You need to collect the serial number of an SRX Series device to replace it. Which command will accomplish this task?

A. show chassis hardware
B. show system information
C. show chassis firmware
D. show chassis environment

Correct Answer: A
Section:
Explanation:
The correct command to collect the serial number of an SRX Series device is the show chassis hardware command [1]. This command will return the serial number of the device, along with other information about the device such as the model number, part number, and version.
This command is available in Junos OS. More information about the show chassis hardware command can be found in the Juniper Networks technical documentation here [1]:
https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/showchassis-hardware.html.

QUESTION 59
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.

Correct Answer: A
Section:
Explanation:
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. More information about Junos security policies can be found in the Juniper Networks technical documentation here:
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-policiesoverview.html.

QUESTION 60
Which two statements about the Junos OS CLI are correct? (Choose two.)

A. The default configuration requires you to log in as the admin user.
B. A factory-default login assigns the hostname Amnesiac to the device.
C. Most Juniper devices identify the root login prompt using the % character.
D. Most Juniper devices identify the root login prompt using the > character.

Correct Answer: A, D
Section:
Explanation:
The two correct statements about the Junos OS CLI are that the default configuration requires you to log in as the admin user, and that most Juniper devices identify the root login prompt using the > character. The factory-default login assigns the hostname "juniper" to the device and the root login prompt is usually identified with the % character. More information about the Junos OS CLI can be found in the Juniper Networks technical documentation here:https:// www.juniper.net/documentation/en_US/junos/topics/reference/commandsummary/ cli-overview.html.

QUESTION 61
An application firewall processes the first packet in a session for which the application has not yet been identified.
In this scenario, which action does the application firewall take on the packet?

A. It allows the first packet.
B. It denies the first packet and sends an error message to the user.
C. It denies the first packet.
D. It holds the first packet until the application is identified.

Correct Answer: D
Section:
Explanation:
This is necessary to ensure that the application firewall can properly identify the application and the correct security policies can be applied before allowing any traffic to pass through.
If the first packet was allowed to pass without first being identified, then the application firewall would not know which security policies to apply - and this could potentially lead to security vulnerabilities or breaches. So it's important that the first packet is held until the application is identified.

QUESTION 62
Your company is adding IP cameras to your facility to increase physical security. You are asked to help protect these IoT 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

Correct Answer: D
Section:
Explanation:
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.