PassQueen
a.k.a dumpsqueen.com

Security, Expert (JNCIE-SEC)

Juniper JPR-934

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

You are reviewing a zone-based security policy on an SRX Series device.

Which three criteria can be used during security-policy matching for a new session? (Choose three.)

A. Source and destination zones

B. Source and destination addresses

C. Application

D. Ethernet switching VLAN membership

E. OSPF area identifier

F. Chassis cluster node priority

ANSWER: A B C

Explanation:

A security policy is evaluated in the context of the source zone and destination zone identified for the session. Within that zone context, the policy can match configured source and destination addresses and can match the application associated with the traffic.

The application match can use a predefined Junos application, a custom application, or an application set. The selected policy then determines whether the matching session is permitted, denied, rejected, or processed by configured services such as logging or IDP.

QUESTION NO: 2

You have several users who dial in to a remote access server using multilink connections, combining two modems into a single link. Although this provides a higher bandwidth to the users, you find the server runs out of modem lines frequently, and most users are not using their connections to their full potential. Which of the following is a solution to this issue?

A. Disable multilink connections.

B. Set the maximum number of multilink ports to one.

C. Use VPN instead of dial-in access.

D. Enable Bandwidth Allocation Protocol (BAP).

ANSWER: D

Explanation:

Enable Bandwidth Allocation Protocol (BAP). BAP is designed specifically for managing bundled links in Multilink PPP sessions when bandwidth demand varies. Rather than permanently reserving two modem lines for every connected user, BAP allows the network access server and client to dynamically add a link when the current link does not provide enough capacity and remove an extra link when demand falls. This preserves the higher throughput available from multilink operation during periods of genuine need while returning an idle or underused modem line to the shared access pool.

In this situation, users retain their multilink capability, but the remote access server can serve more concurrent dial-in users because modem resources are not unnecessarily tied up by lightly used second links. BAP therefore directly addresses both stated conditions: constrained modem-line availability and generally low utilization of the bundled connections. The protocol defines messages for requesting, adding, and dropping links based on bandwidth requirements and policy. Its operation with Multilink PPP is specified in RFC 2125, Bandwidth Allocation Protocol; the underlying bundle model is defined in RFC 1990, The PPP Multilink Protocol.

QUESTION NO: 3

You have an IAS server running Windows Server. It supports a group of RRAS servers used to manage VPN connections for clients. You are configuring the authentication methods for the IAS server and want to allow the clients to use smart cards for secure and convenient authentication. Which of the following authentication protocols should you select?

A. MS-CHAP

B. EAP-TLS

C. MD5 CHAP

D. MS-CHAP v2

ANSWER: B

Explanation:

EAP-TLS is the appropriate authentication protocol because it supports certificate-based mutual authentication between the VPN client and the IAS server. A smart card stores the user's private key and presents the associated user certificate during the EAP-TLS exchange. The private key remains protected on the card, and the user typically unlocks it with a PIN, providing strong authentication without relying solely on a reusable password.

For an IAS/RRAS VPN deployment, EAP-TLS allows IAS to validate the client certificate through the organization's public key infrastructure, including certificate-chain validation and certificate status checking where configured. The client can also validate the server certificate, helping ensure that credentials are provided only to the legitimate authentication server. This makes EAP-TLS well suited to managed enterprise VPN access where smart-card logon and certificate enrollment are available.

Microsoft documents EAP-TLS as an EAP method that uses certificates for authentication and describes its use for secure network access. See Microsoft's EAP network access documentation and Microsoft's guidance for certificates in NPS.

QUESTION NO: 4

You are the backup administrator for your company. You are responsible for ensuring that all data on ten files servers are protected against data loss. Normal business hours from 8 A.M. to 5 P.M., Monday through Friday, are observed. Network access is prohibited outside normal business hours.

A member server named File1 contains shared folder accessed by users in the sales department. The disk structure of File1 is shown in the following exhibit:

Volume	Hosts	Disk Size	Available Space
C	System and Boot Files	9 GB	2.54 GB
D	Shared Folders and User Profiles	25 GB	9.8 GB
F	Shared Folders	75 GB	53.35 GB

You have scheduled a daily backup of File1 as shown in the exhibit. (Click the Exhibit(s) button.) Users in the Sales department frequently leave documents open on their desktops when they leave work. These users occasionally request that you restore a previous version of a file from backup. However, some of these files are not included in recent backup sets. You must modify the backup procedures for File1 so that all files, including open documents, will be included in the daily backup. You also want to provide users with the ability to restore their files.

What should you do? (Choose all that apply. Each correct answer presents part of the solution.)

A. Move all shared user data folders from drive D to drive F.

B. Move all shared folders user data from drive F to drive D.

C. Enable Shadow Copies of Shared Folders on drive F.

D. Enable Volume shadow copy for the scheduled backup job.

E. Select the Disable volume shadow copy option for the scheduled backup job.

F. Install the Previous Versions Client software on all Sales department computers.

G. Create a new daily backup job by using the same settings, but clear the Disable volume shadow copy option.

ANSWER: A C F G

Explanation:

Move all shared user data folders from drive D to drive F because Shadow Copies of Shared Folders requires the volume containing the shared data to use NTFS. Placing the shared folders on the eligible volume makes both the snapshot and end-user recovery design possible. Enable Shadow Copies of Shared Folders on drive F so the server retains point-in-time copies of the shared data. Those copies let users browse a shared folder's Previous Versions and recover an earlier file version without requiring an administrator to perform a full backup restore.

Install the Previous Versions Client software on all Sales department computers because this legacy client component provides the Previous Versions user interface for supported client systems, allowing Sales users to access the snapshots exposed by the file server. Finally, create a new daily backup job by using the same settings, but clear the Disable volume shadow copy option. This causes the backup process to use Volume Shadow Copy Service (VSS), which creates a consistent snapshot from which the backup can include files that remain open at backup time. Together, VSS-based backup protects current open-file data, while shared-folder shadow copies provide convenient user self-service recovery of earlier versions. See Microsoft's Volume Shadow Copy Service documentation and its Shadow Copies of Shared Folders overview.

QUESTION NO: 5

You work as a Network Administrator for ABC.com. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server. The company's headquarters is located at Los Angeles. The company has three branch offices located at San Jose, Oakland, and San Francisco. The company's network is shown in the image below:

All the offices are connected to each other by using 56Kbps demand-dial connections. The branch offices and the headquarters are required to communicate with each other on a regular basis. As you are using demand-dial connections, you do not want the routing updates to be broadcast throughout the network. However, for reliable communications, any changes to the network should be sent to the routers configured on the network. Every router in the network is a server running Windows Server. Which of the following protocols will you use on the routers?

A. RIP 1

B. CHAP

C. RIP 2

D. OSPF

ANSWER: C

Explanation:

RIP 2 is the appropriate routing protocol for this Windows Server Routing and Remote Access demand-dial environment. RIP version 2 supports classless routing information, including subnet-mask information, which is necessary for reliable route exchange in modern IP networks. Unlike RIP version 1, RIP version 2 sends routing updates using the multicast address 224.0.0.9 rather than broadcasting them to every host on a subnet. This limits update delivery to routers that participate in RIP version 2, satisfying the requirement to avoid broadcasts across the connected networks.

RIP version 2 is also supported by Windows Server RRAS and can be used with demand-dial interfaces. RRAS can use RIP route announcements and triggered route updates so that routing changes are communicated to participating routers without requiring broadcast-based routing behavior. This makes RIP version 2 a suitable fit for the low-bandwidth, 56-Kbps interoffice links while retaining automatic propagation of routing changes. Microsoft documents RIP for IP as a routing protocol supported by RRAS, including its RIP version 2 capabilities and configuration behavior. See Microsoft documentation for RIP for IP and RFC 2453: RIP Version 2.

QUESTION NO: 6

You are working on an existing server. The NIC manufacturer has notified you of an updated driver for your card that will greatly improve performance. You download and install the new driver. Before you reboot the system, you perform an ASR backup. When you reboot the system, it reaches the graphical portion of the boot process and presents a STOP message. What is the proper process for recovering from this problem?

A. Perform an ASR restore from the ASR backup set you created before the reboot.

B. Reboot the system, press F8 when prompted during the boot process, select Last Known Good Configuration, and press Enter.

C. Reinstall the operating system and do a restore of the system from tape backup.

D. Reboot the system, press F8 when prompted during the boot process, select Safe Mode, and press Enter.

ANSWER: B

Explanation:

Reboot the system, press F8 when prompted during the boot process, select Last Known Good Configuration, and press Enter. This is the appropriate initial recovery action when a newly installed NIC driver causes a STOP error during startup. In the Windows versions that provide this startup choice, Last Known Good Configuration starts the computer using the most recently successful control set: the configuration that was in use the last time a user successfully logged on. That control set includes the service and driver startup configuration, so it can roll the system back from the newly applied driver configuration without requiring a full operating-system recovery.

The timing in this scenario is important. The failure occurs immediately after a driver update and before a successful post-change logon, which means the prior working configuration remains available as the last known good state. This recovery method is designed to be attempted before more disruptive recovery procedures. After the server starts successfully, the administrator can obtain a compatible driver version, review the driver installation, and validate normal network operation. Microsoft's driver-installation overview explains how drivers are integrated into Windows device configuration: Windows driver installation overview. Microsoft's startup recovery guidance also describes startup-mode recovery concepts: Start your PC in Safe Mode.

QUESTION NO: 7

You are configuring OSPF on an SRX Series device interface assigned to the trust zone. The device must establish OSPF adjacencies with a router connected to that interface.

Which two configuration tasks are required? (Choose two.)

A. Configure the interface under an OSPF area.

B. Permit OSPF as host-inbound traffic on the zone or interface.

C. Configure a security policy from the trust zone to the trust zone permitting OSPF.

D. Configure source NAT for OSPF packets.

E. Configure an IPsec VPN to the adjacent router.

ANSWER: A B

Explanation:

You must configure the interface under the appropriate OSPF area so that the routing protocol operates on the interface. This enables the SRX device to send and receive OSPF protocol packets as part of the routing process.

You must also permit OSPF as host-inbound traffic on the applicable zone or interface. OSPF packets are addressed to the SRX device and are processed by its routing engine, so they are controlled by host-inbound traffic configuration rather than by an interzone security policy.

QUESTION NO: 8

You are deploying Intrusion Detection and Prevention (IDP) inspection on an SRX Series device. Traffic from the trust zone to the untrust zone must be inspected and blocked when it matches a configured critical IDP signature.

Which three configuration tasks are required? (Choose three.)

A. Install an IDP signature database.

B. Configure an IDP policy containing the required IDP rule.

C. Attach the IDP policy to the applicable security policy.

D. Configure a security screen in the destination zone.

E. Configure the security policy action as deny.

ANSWER: A B C

Explanation:

An IDP policy must be configured with rules that match the required traffic and specify the desired action, such as drop, reject, or no-action. The IDP policy must then be referenced by an application-services action in the applicable security policy. The security policy still controls whether the session is permitted between zones, while the attached IDP policy performs signature-based inspection of permitted traffic.

The SRX Series device must also have an installed and current IDP signature database. Without the signature database, the device has no signature set against which it can inspect traffic. A security policy action of permit by itself does not activate IDP processing, and a security screen is a separate zone-based mechanism intended for basic network and transport-layer attack detection. Juniper describes IDP policies, signature databases, and security-policy attachment in the Junos IDP documentation.