Juniper

Exam JN0-314

Junos Pulse Access Control, Specialist (JNCIS-AC)

Version: 7.0

[Total Questions: 222]

Topic 1, Volume A

Question No : 1 - (Topic 1)

A customer wants to create a custom Junos Pulse configuration. Which two are required? (Choose two)

A. Connection set
B. Configuration set
C. Custom installer
D. Component set

Answer: A,D

Question No : 2 - (Topic 1)

What is a type of firewall enforcer supported by the Junos Pulse Access Control Service?

A. Checkpoint firewall
B. SRX Series device
C. DP sensor
D. MX Series device

Answer: B

Question No : 3 - (Topic 1)

A customer is trying to decide which 802.1X inner protocol to use on their network. The customer requires that no passwords be sent across the network in plain text, that the protocol be supported by the Windows native supplicant, and that the protocol supports password changes at Layer 2.

Which protocol would meet the customer's needs?

A. EAP-TLS
B. EAP-MD5
C. PAP
D. EAP-MSCHAPv2

Answer: D

Question No : 4 - (Topic 1)

You navigate to "UAC" > "Infranet Enforcer" > "Auth Table Mapping" in the admin GUI. You see one policy, which is the unmodified, original default policy.

Which statement is true?

A. Dynamic auth table mapping is not enabled.
B. A successful authentication attempt will result in a new authentication table entry, which will be delivered only to the Junos enforcer protecting the network from which the user has authenticated.
C. To create a static auth table mapping, you must delete the default policy.
D. The default policy applies only to the factory-default role User.

Answer: A

Question No : 5 - (Topic 1)

You have a Junos Pulse Secure Access Service acting as an IF-MAP client, configured to federate all user roles to a Junos Pulse Access Control Service acting as an IF-MAP Federation server. A remote user using Junos Pulse logs in to the Junos Pulse Secure Access Service; the Junos Pulse Secure Access Service provisions a remote access session for that user.

What happens next?

A. The Junos Pulse Secure Access Service redirects the user to the Junos Pulse Secure Access Service for authentication
B. The Junos Pulse Access Control Service provisions enforcement points to enable resource access for that user.
C. The Junos Pulse Secure Access Service publishes user session and role information to the IF-MAP Federation server,
D. The Junos Pulse Secure Access Service provisions enforcement points to enable resource access for that user.

Answer: C

Question No : 6 - (Topic 1)

You are configuring an active/passive cluster of SRX Series devices as the firewall enforcer on a MAG Series device. Which statement is true?

A. Multiple Infranet Enforcer instances are created with a single serial number of an SRX Series device defined in each configuration.
B. A single Infranet Enforcer instance is created with both serial numbers of the clustered SRX Series devices defined in the configuration.
C. Multiple Infranet Enforcer instances are created with a single IP address of an SRX Series device defined in each configuration.
D. A single Infranet Enforcer instance is created with the VIP of the clustered SRX Series device defined in the configuration.

Answer: B

Question No : 7 - (Topic 1)

A customer has purchased a third-party switch to use for Layer 2 access with their Junos Pulse Access Control Service. When configuring the switch on the Junos Pulse Access Control Service, the customer does not find a make/model entry for it.

Which two actions should the customer take to make the switch work with the Junos Pulse Access Control Service? (Choose two.)

A. Add the switch to the Junos Pulse Access Control Service as a standard RADIUS.
B. Add the switch to the Junos Pulse Access Control Service using the "Any" make/model.
C. Add the switch as a firewall enforcer.
D. Obtain and configure the RADIUS dictionary for the switch and use that vendor listing for the make/model.

Answer: A,D

Question No : 8 - (Topic 1)

Which three settings are accessible from the serial console menu on a MAG Series device? (Choose three.)

A. The ping command

B. Factory default reset
C. Personality image
D. License imports
E. Admin login credentials

Answer: A,B,E

Question No : 9 - (Topic 1)

What is the function of Host Checker?

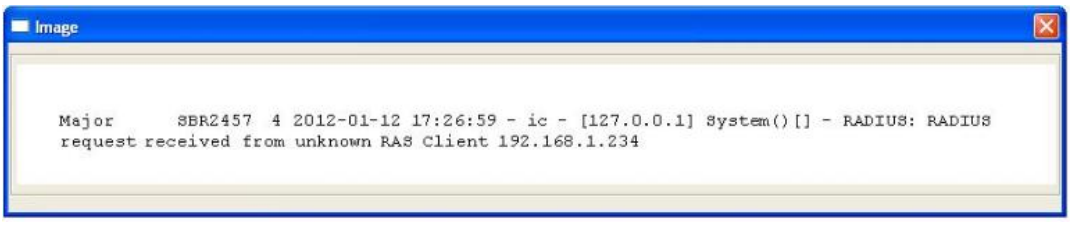
A. To allow clientless access to the network
B. To restrict access to protected resources on the network
C. To scan an endpointfor compliance with security policies
D. To push a firewall policy to the endpoint's local firewall application

Answer: C

Explanation: http://www.juniper.net/techpubs/en_US/uac4.2/internal/topic-collections/Junos-Pulse-Access-Control.pdf

Question No : 10 - (Topic 1)

Click the Exhibit button.



What is the cause of the error shown in the exhibit?

A. A RADIUS request is being received from a device that is not configured on the RADIUS Client page.
B. A user entered an incorrect password during RADIUS authentication.
C. A RADIUS proxy attempt failed to reach the configured proxy server.
D. The RADIUS shared secret is incorrect.

Answer: A

Question No : 11 - (Topic 1)

You have a firewall enforcer protecting resources in a data center. A user is experiencing difficulty connecting to a protected resource.

Which two elements must exist so the user can access the resource? (Choose two.)

A. Resource access policy on the MAG Series device
B. IPsec routing policy on the MAG Series device
C. General traffic policy blocking access through the firewall enforcer
D. Auth table entry on the firewall enforcer

Answer: A,D

Question No : 12 - (Topic 1)

A user's Junos Pulse client uses 802.1X to access a wired network and is failing to authenticate. You run a packet capture from the user's PC and notice that immediately after the client machine sends an EAPoL-start packet, an EAP-failure packet is returned. You review the RADIUS troubleshooting logs on the MAG Series device and do not see any authentication attempts from the user. Other users on the same Ethernet switch are successfully authenticating.

Which device is sending the EAP-failure packet to the workstation?

A. The RADIUS server
B. The EAPoL server
C. The workstation's network adapter
D. The Ethernet switch

Answer: D

Question No : 13 - (Topic 1)

You want to ensure that users who access the company's protected resources present a client certificate before they are allowed to sign in.

What should you configure?

A. A certificate authentication policy that allows all users and remembers certificate information while the user is signed in.
B. A certificate authentication policy that only allows users with a client-side certificate signed by a trusted client CA to sign in.
C. A certificate role restriction that allows all users and remembers certificate information while the user is signed in.
D. A certificate role restriction that only allows users with a client-side certificate signed by a trusted client CA to sign in.

Answer: B

Question No : 14 - (Topic 1)

What are two ways to access the Junos Pulse Access Control Service? (Choose two.)

A. admin GUI
B. Telnet
C. SSH
D. console

Answer: A,C

Question No : 15 - (Topic 1)

You are configuring an IPsec routing policy that will be used with a ScreenOS firewall enforcer. What must you also configure?

A. Source IP policies on the ScreenOS device
B. ScreenOS IPsec policies on the Junos Pulse Access Control Service
C. VPN NAT traversal on the ScreenOS device
D. Source interface policies on the Junos Pulse Access Control Service

Answer: B

Question No : 16 - (Topic 1)

On a MAG Series device, where is the preauthentication sign-in message configured?

A. On the configuration page for the sign-in notification message
B. On the wireless user realm authentication policy
C. On the sign-in policy of the URL being used by the wireless users
D. On the sign-in page of the URL being used by the wireless users

Answer: C

Question No : 17 - (Topic 1)

You are the administrator in your company and you have restricted administrator access to require a user certificate to access the admin GUI on your company's MAG Series device. You must now access the admin GUI from a PC that does not have your user certificate installed.

How would you access the MAG Series device admin GUI with this PC?

A. Perform a factory reset of the MAG Series device.
B. Connect to the MAG Series device with HTTP instead of HTTPS, e.g.. http://<MAG address>/admin.
C. Create a Super Admin Session through the console menu and use the resulting one-time token to access the admin GUI.
D. Log in through the console port and reset the admin password to get into the admin GUI.

Answer: C

Question No : 18 - (Topic 1)

Which two actions are available in the GUI for creating location awareness rules? (Choose two.)

A. WINS server
B. DNS server
C. IP reachability
D. Resolve address

Answer: B,D

Question No : 19 - (Topic 1)

You are the network administrator for your company. A user is complaining that they are not able to access the network with the Junos Pulse client. You run a packet capture on the network interface to monitor the 802.1X authentication process. You notice that after the EAP-request/identity packet is received, and the supplicant responds with an EAP-response/identity packet, no further communication occurs for several seconds.

What are three causes for this behavior? (Choose three.)

A. The authenticator is not licensed to support Junos Pulse.
B. The authenticator did not receive the EAP-response/identity packet.
C. The authentication server is not receiving the RADIUS packet containing the EAP-response/identity data.
D. The authenticator is sending the request over its loopback interface.
E. The authentication server is sending back a RADIUS response packet, but the authenticator is not forwarding the response back to the supplicant.

Answer: B,C,E

Question No : 20 - (Topic 1)

An administrator has created three different Odyssey Access Client preconfiguration files and assigned them to three different roles in the same realm.

Which action should the administrator take to ensure that users get the correct Odyssey Access Client preconfiguration file?

A. Configure each user account in the auth server with the appropriate Odyssey Access Client preconfiguration files.
B. Configure the role-mapping rules with the appropriate Odyssey Access Client preconfiguration files.
C. Ensure that merge roles is selected in the role-mapping rules.
D. Ensure that the first role a user is mapped to is the role with the appropriate Odyssey Access Client preconfiguration file.

Answer: D

Question No : 21 - (Topic 1)

You want to create a Host Checker policy that looks for a specific antivirus product that is running on your client machines, but the predefined antivirus options do not include the antivirus product version that you use.

Which feature should you verify the antivirus product is up to date?

A. Enhanced Endpoint Security
B. DP signatures
C. Antivirus licensing
D. Endpoint Security Assessment Plug-in

Answer: D

Question No : 22 - (Topic 1)

What are three benefits of IF-MAP Federation? (Choose three.)

A. Enables seamless access for remote access users to firewall enforcer protected resources.
B. Scales a Junos Pulse Access Control Service deployment beyond the capacity of a single cluster.
C. Enables dynamic configuration synchronization across multiple MAG Series devices.
D. Provides a substitute for WAN clustering among geographically separated MAG Series devices.
E. Shares non-localized DP integration and IPsec configuration information between multiple Junos Pulse Access Control Service instances.

Answer: A,B,E

Question No : 23 - (Topic 1)

Which three authentication server types are supported for retrieving user attributes used in role-mapping rules? (Choose three.)