Vendor: Juniper

Exam Code: JN0-314

Exam Name: Junos Pulse Access Control, Specialist (JNCIS-AC)

Version: DEMO

QUESTION NO: 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

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: A

QUESTION NO: 3

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

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

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 IFMAP Federation server,

D. The Junos Pulse Secure Access Service provisions enforcement points to enable resource access for that user.

Answer: C

QUESTION NO: 6

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

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

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

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

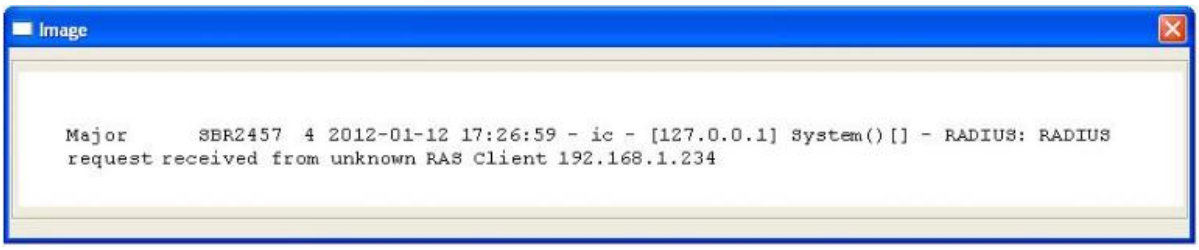
C. To scan an endpointfor compliance with security policies

D. To push a firewall policy to the endpoint's local firewall application

Answer: B

QUESTION NO: 10

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