156-315.81^Q&As^

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

The Correlation Unit performs all but the following actions:

A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.

B. Generates an event based on the Event policy.

C. Assigns a severity level to the event.

D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.

Correct Answer: C

QUESTION 2

What command verifies that the API server is responding?

A. api stat

B. api status

C. show api_status

D. app_get_status

Correct Answer: B

QUESTION 3

What is the purpose of Priority Delta in VRRP?

A. When a box up, Effective Priority = Priority + Priority Delta

B. When an Interface is up, Effective Priority = Priority + Priority Delta

C. When an Interface fail, Effective Priority = Priority ?Priority Delta

D. When a box fail, Effective Priority = Priority ?Priority Delta

Correct Answer: C

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP.

QUESTION 4

Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up.

B. There is Load Sharing solution set up.

C. Only when there is Unicast solution set up.

D. There is High Availability solution set up.

Correct Answer: D

QUESTION 5

What is false regarding a Management HA environment?

A. Only one Management Server should be active, while any others be in standby mode

B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.

C. SmartConsole can connect to any management server in Readonly mode.

D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Correct Answer: B

QUESTION 6

Which process handles connection from SmartConsole R81?

A. fwm

B. cpmd

C. cpm

D. cpd

Correct Answer: C

QUESTION 7

To add a file to the Threat Prevention Whitelist, what two items are needed?

A. File name and Gateway

B. Object Name and MD5 signature

C. MD5 signature and Gateway

D. IP address of Management Server and Gateway

Correct Answer: B

QUESTION 8

Which is the correct order of a log flow processed by SmartEvent components?

A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client

B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client

C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client

D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Correct Answer: D

QUESTION 9

IF the first packet of an UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), what message is sent back through the kernel?

A. Nothing

B. TCP FIN

C. TCP RST

D. ICMP unreachable

Correct Answer: A

QUESTION 10

Alice and Bob are going to deploy Management Data Plane Separation (MDPS) for all their Check Point Security Gateway(s)/Cluster(s). Which of the following statement is true?

A. Each network environment is dependent and includes interfaces, routes, sockets, and processes

B. Management Plane -To access, provision and monitor the Security Gateway

C. Data Plane -To access, provision and monitor the Security Gateway

D. Management Plane -for all other network traffic and processing

Correct Answer: B

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolution details=andsolutionid=sk138672

QUESTION 11

What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

A. CPUSE offline upgrade only

B. Advanced upgrade or CPUSE offline upgrade

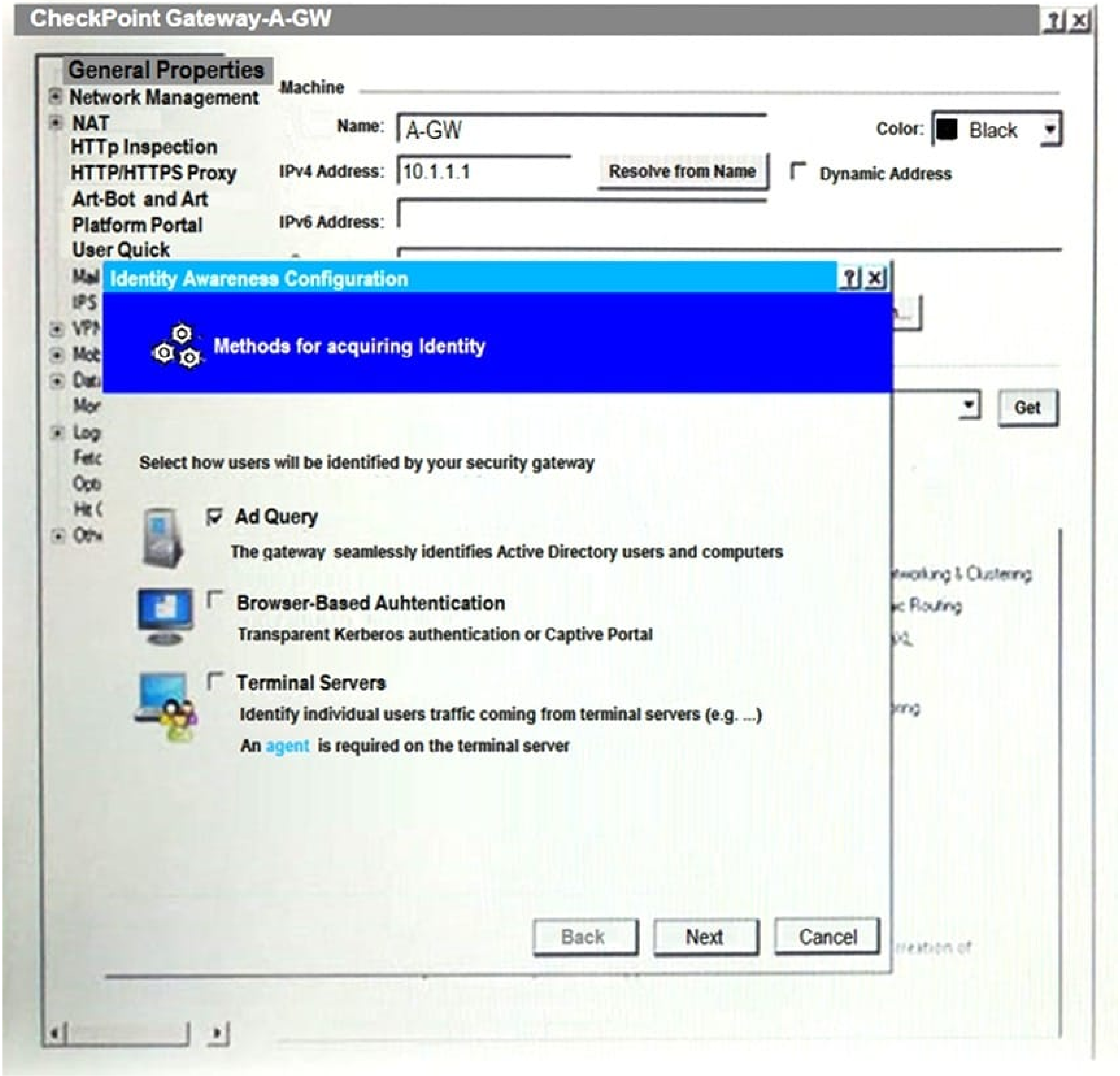
C. Advanced Upgrade only

D. SmartUpdate offline upgrade

Correct Answer: B

QUESTION 12

On the following picture an administrator configures Identity Awareness:



Name: A-GW

IPv4 Address: 10.1.1.1

Resolve from Name

Color: Black

□ Dynamic Address

IPv6 Address:

Identity Awareness Configuration

Methods for acquiring Identity

Select how users will be identified by your security gateway

☑ Ad Query

The gateway seamlessly identifies Active Directory users and computers

□ Browser-Based Auhtentication

Transparent Kerberos authentication or Captive Portal

□ Terminal Servers

Identify individual users traffic coming from terminal servers (e.g. ...)

An agent is required on the terminal server

After clicking "Next" the above configuration is supported by:

A. Kerberos SSO which will be working for Active Directory integration

B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.

C. Obligatory usage of Captive Portal.

D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Correct Answer: B

QUESTION 13

Which command lists all tables in Gaia?

A. fw tab –t

B. fw tab –list

C. fw-tab –s

D. fw tab -1

Correct Answer: C

QUESTION 14

In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Standalone

B. Remote

C. Distributed

D. Bridge Mode

Correct Answer: A

SRC: Installation and Upgrade Guide R81 In a Standalone deployment, a Check Point computer runs both the Security Gateway and Security Management Server products.

QUESTION 15

Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

A. infoCP

B. infoview

C. cpinfo

D. fw cpinfo

Correct Answer: C