QUESTION 529
In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom. Which of the following statements is correct?

A. If the Action of the matching rule is Accept, the gateway will drop the packet.
B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down.
C. If the Action of the matching rule is Drop, the gateway stops matching against later rules in the Policy Rule Base and drops the packet.
D. If the rule does not matched in the Network policy it will continue to other enabled policies

Answer: C

QUESTION 530
Connections to the Check Point R80 Web API use what protocol?

A. HTTPS
B. SOAP
C. HTTP
D. SIC

Answer: A

QUESTION 531
What Factors preclude Secure XL Templating?

A. Source Port Ranges/Encrypted Connections
B. Simple Groups
C. ClusterXL in load sharing Mode
D. CoreXL

Answer: A

QUESTION 532
The fwd process on the Security Gateway send logs to the fwd process on the Management Server, where it is forwarded to _____ via _____.

A. cpwd, fwsd
B. cpd, fwm
C. cpm, cpd
D. fwm, cpd

Answer: C

QUESTION 533
CoreXL is NOT supported when one of the following features is enabled:

A. Route-based VPN
B. Overlapping NAT
C. IPv6
D. IPS

Answer: B

QUESTION 534
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called, and what are you defining?

A. Network; and defining your Class A space
B. Topology; and you are defining the Internal network
C. Internal addresses; you are defining the gateways
D. Internal network(s); you are defining your networks

Answer: B

QUESTION 535
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n)_____ or _____ action for the file types.

A. Inspect/Bypass
B. Inspect/Prevent
C. Prevent/Bypass
D. Detect/Bypass

Answer: A

QUESTION 536
To fully enable Dynamic Dispatcher on a Security Gateway:

A. run "fw ctl multik dynamic_dispatching on" and then reboot
B. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXl menu
C. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot
D. run fw ctl multik set_mode 1 in Expert mode and then reboot

Answer: A

QUESTION 537
Which view is NOT a valid CPVIEW view?

A. IDA
B. DLP
C. PDP
D. VPN

Answer: C

QUESTION 538
The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

A. ccp
B. cphaconf
C. cphad
D. cphastart

Answer: A

QUESTION 539
Which component is NOT required to communicate with the Web Services API?

A. API key
B. session ID token
C. content-type
D. Request payload

Answer: A

QUESTION 540
Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network

Answer: D

QUESTION 541
Which of the following describes how Threat Extraction functions?

A. Detect threats and provides a detailed report of discovered threats
B. Proactively detects threats
C. Delivers file with original content
D. Delivers PDF versions of original files with active content removed

Answer: D

156-915.80 Exam Dumps 156-915.80 Exam Questions

156-915.80PDF Dumps 156-915.80 VCE Dumps

https://www.braindump2go.com/156-915.80.html