156-727.77Q&As

Threat Prevention

Pass CheckPoint 156-727.77 Exam with 100% Guarantee

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

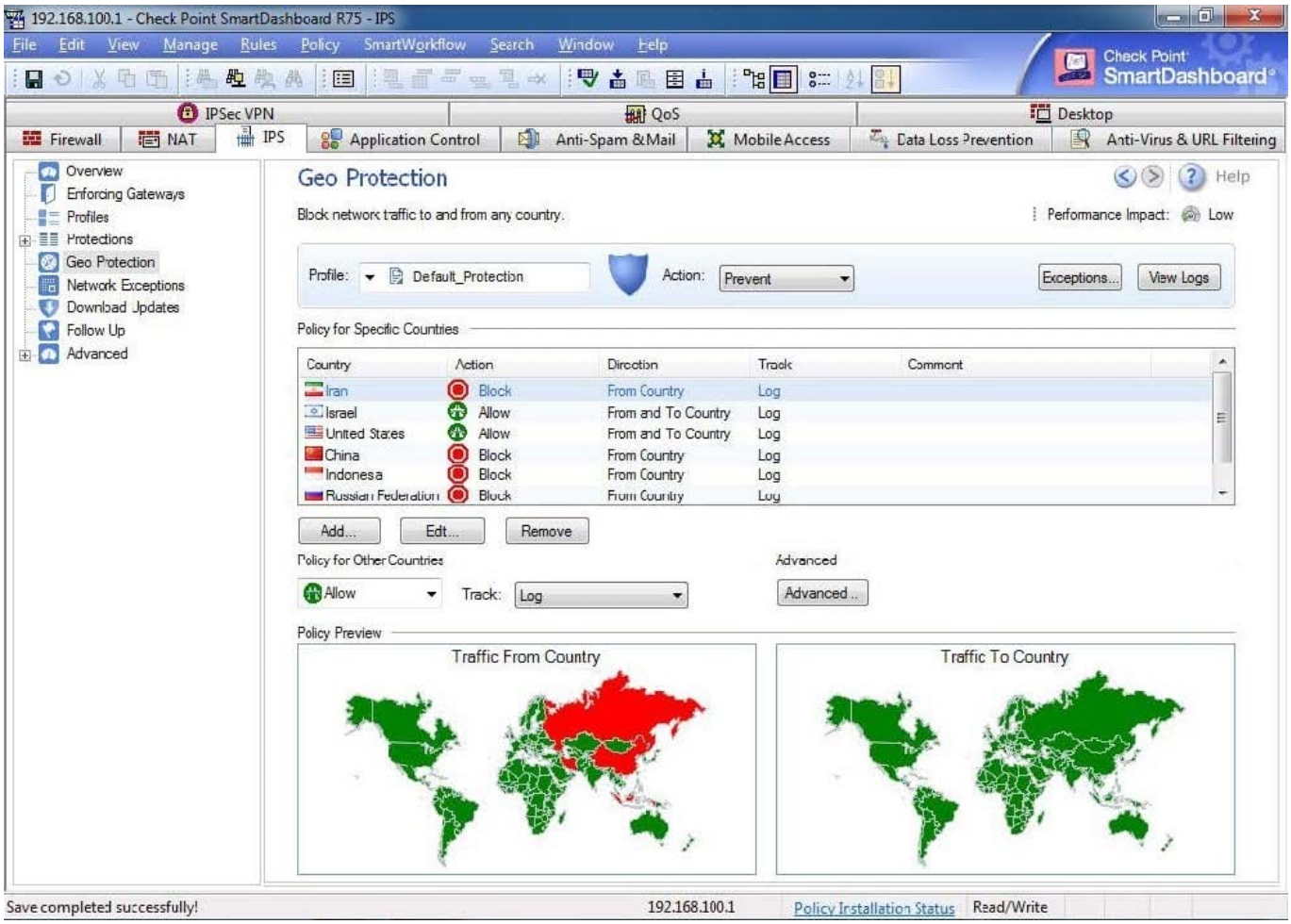
https://www.certbus.com/156-727-77.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

This graphic shows traffic being blocked from certain countries.



What is the deciding factor for this?

A. The traffic from selected countries is being blocked because of an IPS traffic-type rule in the rulebase

B. The traffic from selected countries is being blocked because it is overloading the Gateway

C. The traffic from selected countries is being blocked due to the GeoProtection ruleset

D. The traffic from selected countries is being blocked due to IPS-detected specific attacks originating there

Correct Answer: C

QUESTION 2

What is the minimum amount of RAM needed for a Threat Prevention Appliance?

A. 4 GB

B. It depends on the number of software blades enabled.

C. 2 GB with GAiA in 32-bit mode, 4 GB with GAiA in 64-bit mode

D. 6 GB

Correct Answer: A

QUESTION 3

What is the minimum software version required for a Threat Emulation deployment?

A. R76 or higher with Hotfix HF_001 for Threat Emulation

B. R75.4x with SecurePlatform, R77 or higher with GaiA

C. R77 or higher with GAiA (or SecurePlatform when using ThreatCloud)

D. R75.47 or higher with GAiA (or SecurePlatform when using ThreatCloud)

Correct Answer: C

QUESTION 4

SmartEvent has several components that work together to help track down security threats. What is the function of the Correlation Unit as one of those components in the architecture? The Correlation Unit:

A. connects with the SmartEvent Client when generating reports.

B. analyzes each log entry as it enters a log server, according to the Event Policy; when a threat pattern is identified, an event is forwarded to the SmartEvent Server.

C. collects syslog data from third party devices and saves them to the database.

D. correlates all the identified threats with the consolidation policy.

Correct Answer: B

QUESTION 5

IPS is primarily a _____-based engine.

A. Signature

B. Difference

C. Action

D. Anomaly

Correct Answer: A

QUESTION 6

When the feature _____ is ON, the Gateway does not block DNS requests that were identified as malicious. Instead it sends a false response with a bogus IP address to the client.

A. Malware DNS Blacklist

B. Malware DNS Trap

C. Malware DNS Sinkhole

D. Malware DNS Blackhole

Correct Answer: B

QUESTION 7

Check Point Signature teams are constantly monitoring the threat space.

A. True, twenty four hours a day, everyday

B. True, except for major holidays

C. True, from Sunday through Thursday

D. False

Correct Answer: A

QUESTION 8

Put these HTTPS traffic inspections steps in the correct order.

a.

Validates the web site\\'s server certificate

b.

Intercepts HTTPS requests

c.

Decrypts data from client and inspects clear text content

d.

Decrypts response from server and inspects clear text content

e.

Creates a certificate for use between gateway and client

f.

Encrypts data and sends data to web server

g.

Encrypts data and sends data to client

h.

Establishes a secure connection to the requested web site

A.

a, e, b, h, c, f, d, g

B.

a, b, f, d, c, g, h, e

C.

b, h, a, e, c, f, d, g

D.

a, b, e, f, d, c, g, h

Correct Answer: C

QUESTION 9

Bots and viruses appear as _____ in the reporting blade.

A. Threats

B. Incidents

C. Malware

D. Infections

Correct Answer: C

QUESTION 10

Which TCP ports allow LDAP users to communicate with the Account Unit?

A. 689 clear, or 336 encrypted

B. 636 clear, or 389 encrypted

C. 336 clear, or 689 encrypted

D. 389 clear, or 636 encrypted

Correct Answer: D