



156-727.77^{Q&As}

Threat Prevention

Pass CheckPoint 156-727.77 Exam with 100% Guarantee

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

<https://www.passapply.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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

If a bot is detected on your network, which of the following statements is correct regarding anti-bot blade.

- A. outbound connections from the infected client are blocked to prevent further infection.
- B. outbound connections from the infected client are blocked; expect the connection to the Check Point ThreatCloud.
- C. outbound connections from the infected client to the command and control center, are blocked.
- D. outbound connections from every client are blocked, to prevent further data breaches.

Correct Answer: C

QUESTION 2

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 3

When is the default Threat Prevention profile enforced?

- A. At the first Security Policy installation.
- B. Only after SensorNET participation is enabled.
- C. When the profile is assigned to a gateway.
- D. When the administrator installs the profile on Security Gateway.

Correct Answer: D

QUESTION 4

Which of the following is information shared via ThreatCloud?

- A. Compromised Machine IP Addresses
- B. Anticipated Attack Methods
- C. Sensitive Corporate Data
- D. Address of command and control servers

Correct Answer: D

QUESTION 5

IPS is primarily a _____-based engine.

- A. Signature
- B. Difference
- C. Action



D. Anomaly

Correct Answer: A

[156-727.77 PDF Dumps](#)

[156-727.77 Study Guide](#)

[156-727.77 Braindumps](#)