

# Checkpoint

**Exam 156-727.77**

**Threat Prevention**

Version: 6.0

[ Total Questions: 53 ]

**Question No : 1**

Which of these is a Check Point Firewall attribute?

- A. Malicious P2P application protection
- B. Buffer overflow prevention
- C. Worm injection blocking
- D. Granular access control

**Answer: D**

**Question No : 2**

Order the steps to bypass the IPS for specific protection:

- a. Open the SmartDashboard
- b. Find the protection you want to bypass
- c. Add the exception for this specific protection
- d. Go to Network Exception tab
- e. Click New.
- f. Go to Protections view
- g. Install Security policy
- h. Go to IPS tab

- A. a, g, h, f, e, c, b, d
- B. a, d, f, h, e, c, b, g
- C. a, h, f, b, d, e, c, g
- D. a, f, h, c, e, d, b, g

**Answer: C**

**Question No : 3**

What is the name of Check Point collaborative network that delivers real-time dynamic

security intelligence to Check Point threat prevention blades?

- A. ThreatSpect
- B. ThreatWiki
- C. ThreatCloud
- D. ThreatEmulator

**Answer: C**

**Question No : 4**

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.

**Answer: C**

**Question No : 5**

Which of the following are valid Boolean search terms that can be used in custom SmartLog queries?

- A. And, or, with
- B. And, or, not
- C. None, Boolean search terms cannot be used in SmartLog.
- D. And, or, not, with

**Answer: B**

**Question No : 6**

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)

**Answer: C**

**Question No : 7**

A customer does not own Check Point Gateways, but he wants to use Threat Emulation Service to detect SMTP Zero-Day vulnerabilities. What is his option?

- A. Use MTA plug-in on his exchange server.
- B. Needs to buy a Check Point security gateway.
- C. Needs to install Mail Transfer Agent on his firewall.
- D. Purchase SMTE cloud service.

**Answer: A**

**Question No : 8**

When adding IPS to a gateway, which profile will be set?

- A. Default\_Protection, but with all actions set to "Detect only"
- B. Default\_Protection, but with all actions set to "Prevent"
- C. Default\_Protection
- D. Recommended\_Protection

**Answer: C**

**Question No : 9**

An end-user calls the helpdesk, complaining that he cannot access a web site. You check the log and see that an IPS signature is dropping his connections. What can you do?  
Change the signature action to: