

156-727.77<sup>Q&As</sup>

Threat Prevention

# Pass CheckPoint 156-727.77 Exam with 100% Guarantee

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

https://www.pass4itsure.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**

You just enabled the IPS blade, and have downloaded the latest signature updates. You created a custom profile but you are concerned that if you push a policy it might start dropping existing connections. What should you do?

- A. Use the recommend Protection profile instead
- B. Edit your custom profile and select Detect-only for Troubleshooting mode
- C. Edit your custom profile and enable Bypass under load
- D. Use the Default protection profile instead

Correct Answer: B

#### **QUESTION 2**

When pushing the Threat Prevention policy, which of the following blades will NOT get updated?

A. IPS

- B. Threat Emulation
- C. Anti-Bot
- D. Anti-Virus
- Correct Answer: A

#### **QUESTION 3**

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 4**

Looking at these logs, what happened at 10:55?



| Edit <u>View Query N</u> avigate <u>T</u> o | ools <u>W</u> | indow <u>H</u> el | þ                                     |    |                                      |               |    | 1            |               |         | neck Point   |
|---|---------------|-------------------|---------------------------------------|----|--------------------------------------|---------------|----|--------------|---------------|---------|--|
| <b>1</b> # # <b>1 E 5 5 5</b> 6             | ?             |                   |                                       |    |                                      |               |    |              |               | S       | neck Point<br>martView Tracke  |
| Network & Endpoint                          | ement         |                   |                                       |    |                                      |               |    |              |               |         |  |
| 🍚 Network & Endpoint Queries 🔄 🔺            | Fir.          | log : Al          |                                       |    |                                      |               |    |              |               |         |  |
| Predefined                                  | BIR           | abc 🕰             | • • • • • • • • • • • • • • • • • • • | 4  | \ <b>▼ L</b>   <b>  </b>   <b>  </b> |               |    |              |               |         |  |
| All Records                                 | No.           | T Date            | T Time                                | T  | T Source T Src. User Na              | T Destination |    | * *          | -             | * *     | T Attack   |
| Network Security Blades                     | 738           | 250ct2011         |                                       | 0  | 10.0.0.2                             | 11.0.0.2      | V  |              | 65            |         | IKE Enforcement Viol   |
| 🗄 🌆 Firewall Blade                          | 1096          | 270ct2011         |                                       | ě  | 10.0.0.2                             | 11.0.0.2      | œ  | and and      | Gento -       |         | Non Compliant CIFS   |
| 🖨 💔 IPS Blade                               | 1310          | 280ct2011         |                                       | E. | 10.0.0.2                             | 11.0.0.2      |    |              | (24))<br>(24) |         | Instant Messengers   |
|   | 1322          | 280ct2011         | 10:55:02                              | 19 | 10.0.0.2                             | 11.0.0.2      | -0 |              | (trail)       |         | IPS Bypass   |
| Critical Not Prevent                        | 1325          | 280ct2011         |                                       |    | 53.254.24                            | 11.0.0.2      | 17 | until 🔛      | B.            | - 6     | IP Fragments   |
|   | 1326          | 280ct2011         | 10:56:55                              | ŏ  | 74.176.12                            | 11.0.0.2      | v  |              | (Cal)         |         | IP Fragments   |
| Follow Up                                   | 1327          | 280ct2011         | 10:56:55                              | ŏ  | 45.24.254                            | 11.0.0.2      | 17 |              | 100           | 4       | IP Fragments   |
| Protocol Anomaly                            | 1328          | 280ct2011         | 10:56:55                              | ŏ  | 53,254,24                            | 11.0.0.2      | 17 |              | 1000          | ē       | IP Fragments   |
| Application Contro                          | 1335          | 280ct2011         |                                       | ŏ  | 74.176.12                            | 11.0.0.2      | V  | unt a        | -             | ē       | IP Fragments   |
| IPS Software Blade                          | 1336          | 280ct2011         | 10:57:08                              | ŏ  | 45.24.254                            | 11.0.02       | Ù  | .001         | (in)          | ě.      | IP Fragments   |
| IPS-1 Sensor                                | 1337          | 280ct2011         | 10:57:08                              | õ  | 53,254,24                            | 11.0.0.2      | V  |              | (a)           |         | IP Fragments   |
| Unidentified Clients                        | 1338          | 280ct2011         | 10:57:08                              | ō  | 53.254.24                            | 11.0.0.2      | V  |              | 600 V         |         | IP Fragments   |
| Geo Protection                              | 1-2403454     |                   |                                       |    |                                      |               |    | and a second | -             |         | and a second |
| Application Control Bla                     |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| Identity Awareness                          |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| 🗄 🚳 Anti-Spam & Email Sec                   |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| Mobile Access Blade                         |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| Data Loss Prevention B                      |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| Anti-Virus & Anti-Malv                      |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| URL Filtering Blade                         |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| IPSEC VPN Blade                             |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| Advanced Networking                         |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| E · · · · · · · · · · · · · · · · · · ·     |               |                   |                                       |    |                                      |               |    |              |               |         |  |
| H More                                      | C HARDEN      |                   |                                       | _  |                                      |               |    |              |               |         |  |
| Firewall-1 GX Blade                         |               | 10                |                                       | -  |                                      |               |    |              |               |         |  |
| UTM-1 Edge +                                | Ready         |                   |                                       |    |                                      |               |    |              | 2             | Total r | ecords in file: 1338   |

A. An IPS rule was installed, causing IPS to temporarily stop working

B. The Gateway was rebooted, causing IPS to temporarily stop working

C. A new IPS policy was installed, causing IPS to temporarily stop working

D. IPD Inspections were temporarily suspended, due to high load on the gateway

Correct Answer: D

## **QUESTION 5**

What is the main purpose of the ThreatCloud?

- A. It is used in conjunction with IPS.
- B. This is the place where ThreatWiki fetches the actual information.
- C. It feeds security gateway software blades (i.e. Anti-Virus and Anti-Bot) with real-time security intelligence.
- D. It is a database used by SANS institute (formerly known as StormCenter).

Correct Answer: C



156-727.77 PDF Dumps

156-727.77 Practice Test

156-727.77 Study Guide