156-727.77^{Q&As}

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

Which of the following is information uploaded to ThreatCloud?

A. Compromised Machine IP Addresses

B. Malware Site IP Addresses

C. Anticipated Attack Methods

D. Sensitive Corporate Data

Correct Answer: B

QUESTION 2

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

QUESTION 3

SmartLog can be used to identify which of the following:

A. Security Policy version control information

B. A list of currently connected users

C. The country of origin of specific traffic displayed on a map

D. The top destination IP addresses of a specific source

Correct Answer: D

QUESTION 4

Sensitive corporate data is uploaded to ThreatCloud:

A. When the administrator manually sends suspected traffic to ThreatCloud for inspection.

B. Never

C. When the administrator configures the sensor to be a SensorNET participant.

D. After the bot attack has been confirmed.

Correct Answer: B

QUESTION 5

Damage from a bot attack can take place after the bot compromises a machine. Which of the following represents the order by which this process takes place? The bot:

A. infects a machine, communicates with its command and control handlers, and penetrates the organization.

B. penetrates the organization, infects a machine, and communicates with its command and control handlers.

C. communicates with its command and control handlers, infects a machine, and penetrates the organization.

D. penetrates the organization, communicates with its command and control handlers, and infects a machine.

Correct Answer: B

QUESTION 6

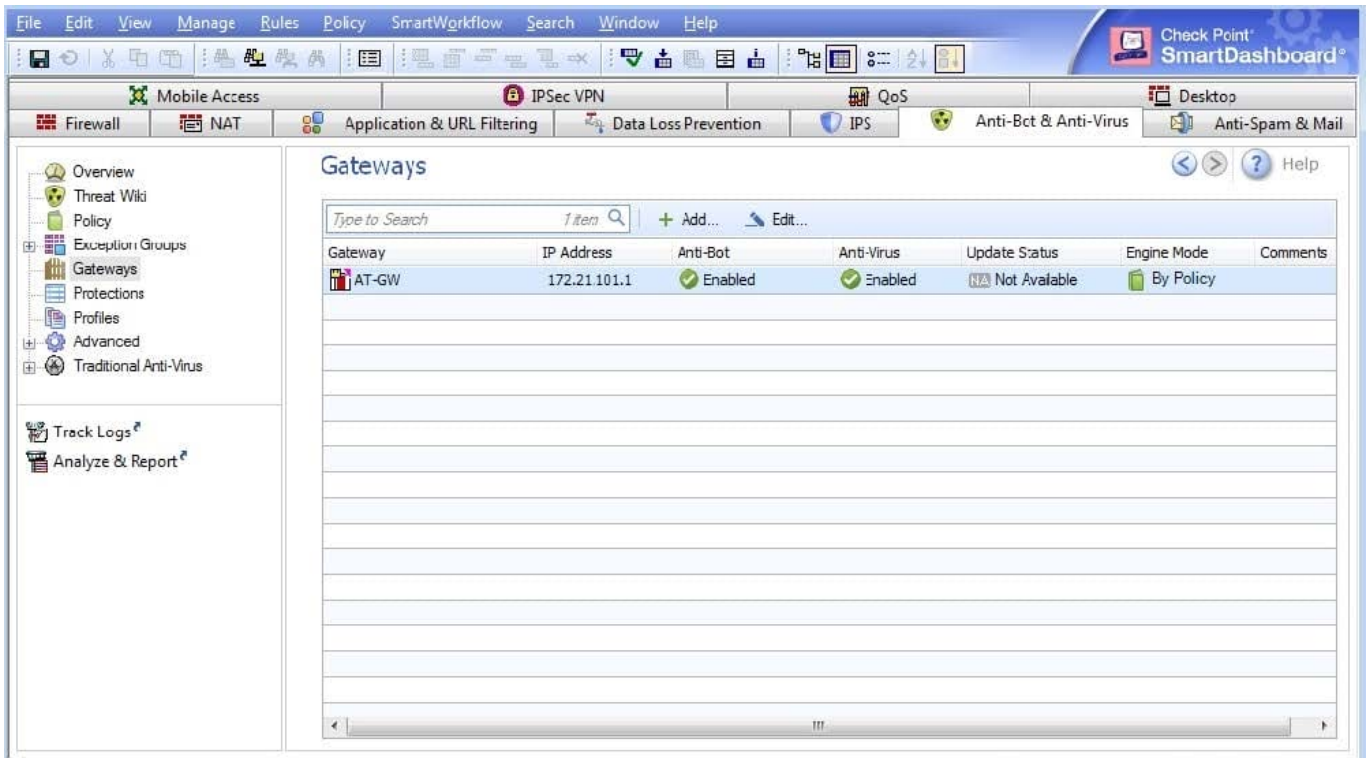Which of the following is information shared via ThreatCloud?

A. Sensitive Corporate Data

B. Bot and virus signatures

C. Anticipated Attack Methods

D. Compromised Machine IP Addresses

Correct Answer: B

QUESTION 7

When configuring Anti-Bot and Anti-Virus, you notice the following error in the Update Status of the Gateways page:

What is the most likely cause of this error?

A. The Security Gateway is not licensed for Anti-Bot and Anti-Virus inspection.

B. There are no updates available for the participating gateway.

C. The Anti-Bot and Anti-Virus policy is not installed on the gateway.

D. You do not have DNS or proxy settings configured for the gateway.

Correct Answer: D

QUESTION 8

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

Correct Answer: C

QUESTION 9

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 10

Which of the following statements regarding the threat prevention database is NOT correct?

A. The Security management server connects to the internet to get Malware Database updates.

B. By default, updates run on the security gateway every two hours.

C. The malware database only updates if you have a valid Anti-Bot/ or Anti-Virus contract.

D. The security gateway contains a local cache of the malware requests.

Correct Answer: A