

# DUMPSBOSS.

## Securing Cisco Networks with Sourcefire IPS

Cisco 500-285

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

<https://dumpsboss.co>

[support@dumpsboss.co](mailto:support@dumpsboss.co)

support@dumpsboss.co  
dumpsboss.co

## Topic Break Down

Topic	No. of Questions
Topic 1, Object Management	4
Topic 2, Access Control Policy	6
Topic 3, Event Analysis	3
Topic 4, IPS Policy Basics	3
Topic 5, FireSIGHT Technologies	7
Topic 6, Network Based Malware Detection	6
Topic 7, Basic Administration	7
Topic 8, Account Management	3
Topic 9, Creating Snort Rules	3
Topic 10, Device Management	6
Topic 11, Correlation Policies	6
Topic 12, Advanced IPS Policy Configuration	6
<b>Total</b>	<b>60</b>

## QUESTION NO: 1

How do you configure URL filtering?

- A. Add blocked URLs to the global blacklist.
- B. Create a Security Intelligence object that contains the blocked URLs and add the object to the access control policy.
- C. Create an access control rule and, on the URLs tab, select the URLs or URL categories that are to be blocked or allowed.
- D. Create a variable.

**ANSWER: C**

## QUESTION NO: 2

Which policy controls malware blocking configuration?

- A. file policy
- B. malware policy
- C. access control policy
- D. IPS policy

**ANSWER: A**

## QUESTION NO: 3

Which statement regarding user exemptions is true?

- A. Non-administrators can be made exempt on an individual basis.
- B. Exempt users have a browser session timeout restriction of 24 hours.
- C. Administrators can be exempt from any browser session timeout value.
- D. By default, all users cannot be exempt from any browser session timeout value.

**ANSWER: A**

## QUESTION NO: 4

Remote access to the Defense Center database has which characteristic?

- A. read/write
- B. read-only
- C. Postgres
- D. Estreamer

**ANSWER: B**

## QUESTION NO: 5

The collection of health modules and their settings is known as which option?

- A. appliance policy
- B. system policy
- C. correlation policy
- D. health policy

**ANSWER: D**

## QUESTION NO: 6

Context Explorer can be accessed by a subset of user roles. Which predefined user role is not valid for FireSIGHT event access?

- A. Administrator
- B. Intrusion Administrator
- C. Security Analyst
- D. Security Analyst (Read-Only)

**ANSWER: B**

## QUESTION NO: 7

Which option can you enter in the Search text box to look for the trajectory of a particular file?

- A. the MD5 hash value of the file
- B. the SHA-256 hash value of the file
- C. the URL of the file
- D. the SHA-512 hash value of the file

**ANSWER: B**

## QUESTION NO: 8

Which statement is true when network traffic meets the criteria specified in a correlation rule?

- A. Nothing happens, because you cannot assign a group of rules to a correlation policy.
- B. The network traffic is blocked.
- C. The Defense Center generates a correlation event and initiates any configured responses.
- D. An event is logged to the Correlation Policy Management table.

**ANSWER: C**

## QUESTION NO: 9

Which option is not a characteristic of dashboard widgets or Context Explorer?

- A. Context Explorer is a tool used primarily by analysts looking for trends across varying periods of time.
- B. Context Explorer can be added as a widget to a dashboard.
- C. Widgets offer users an at-a-glance view of their environment.
- D. Widgets are offered to all users, whereas Context Explorer is limited to a few roles.

**ANSWER: B**

## QUESTION NO: 10

The gateway VPN feature supports which deployment types?

- A. SSL and HTTPS

- B. PPTP and MPLS
- C. client and route-based
- D. point-to-point, star, and mesh

**ANSWER: D**