DUMPSBOSS.

Securing Cisco Networks with Sourcefire IPS

Cisco 500-285

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, FireSIGHT System Overview	8
Topic 2, FireSIGHT System Configuration	6
Topic 3, Access Control	14
Topic 4, Security Intelligence	5
Topic 5, Network Discovery	6
Topic 6, Intrusion Policy	22
Topic 7, Advanced Malware Protection	6
Topic 8, Correlation	4
Topic 9, System Administration	8
Topic 10, Mix Questions	1
Total	80

QUESTION NO: 1

Which option describes Spero file analysis?

A. a method of analyzing the SHA-256 hash of a file to determine whether a file is malicious or not

B. a method of analyzing the entire contents of a file to determine whether it is malicious or not

C. a method of analyzing certain file characteristics, such as metadata and header information, to determine whether a file is malicious or not

D. a method of analyzing a file by executing it in a sandbox environment and observing its behaviors to determine if it is malicious or not

ANSWER: C

Explanation:

Spero file analysis is correctly described as a method of analyzing certain file characteristics, such as metadata and header information, to determine whether a file is malicious or not. In Cisco's file-analysis workflow, Spero is a static-analysis capability that rapidly evaluates attributes extracted from a file rather than relying on execution of the file. These attributes can include structural and contextual properties that help build a malware-likelihood assessment. This approach is useful because it can provide a verdict quickly, including for files that may not be suitable for dynamic execution or that require a preliminary assessment before deeper analysis is needed.

Static file analysis is part of a layered malware-detection strategy in Cisco security products. Cisco distinguishes file reputation and analysis services from behavioral observation: Spero contributes an analysis result based on file properties, while dynamic analysis involves observing a submitted file's actions in an isolated environment. The metadata- and header-focused description therefore accurately captures the purpose and operation of Spero analysis. See Cisco's File Analysis documentation and the Cisco Secure Endpoint data sheet for Cisco's broader file-inspection and malware-analysis capabilities.

QUESTION NO: 2

Stacking allows a primary device to utilize which resources of secondary devices?

A. interfaces, CPUs, and memory

B. CPUs and memory

C. interfaces, CPUs, memory, and storage

D. interfaces and storage

ANSWER: C

Explanation:

In a Cisco Sourcefire stacked deployment, multiple compatible physical appliances operate as one logical device under the control of the primary device. The primary device can use the secondary devices' network interfaces, processing capacity, memory, and storage resources. This aggregation is the purpose of stacking: it expands the logical appliance's ability to inspect traffic, apply intrusion-prevention policies, retain event and packet-related data, and provide connectivity without requiring each member to be managed as an independent appliance. Interfaces on secondary members participate in traffic handling, while their CPUs and memory contribute to inspection and system processing. Their storage also becomes available to the logical stack for the data functions supported by the platform. Cisco's Firepower 8000 Series documentation describes stacking as combining appliance resources into a single logical system, with a primary member managing and using the capabilities supplied by secondary members. See the Cisco Firepower 8000 Series support documentation and Cisco's Firepower 8000 Series Quick Start Guide for platform documentation and stacking information.

QUESTION NO: 3

When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery?

A. host

B. IPS event

C. anti-malware

D. networks

ANSWER: A

Explanation:

host is correct because FireSIGHT network discovery is designed to identify and profile hosts observed on monitored network segments. When a discovery rule is configured with the Discover action, the system analyzes network traffic and gathers host attributes such as IP and MAC addresses, operating system information, host names, detected services, and client or server roles. This information is retained in the network map and can be used to build host profiles, understand assets present in the environment, and support policy decisions based on discovered network characteristics.

Discovery rules define the traffic and networks to monitor, while the selected discovery settings control which host information is collected. This makes host discovery a foundational FireSIGHT capability: it provides visibility into endpoints communicating through the sensors without requiring an agent on each endpoint. Administrators can then review the discovered-host data in the management interface and use it to investigate assets and observed behavior. Cisco describes network discovery as a process for collecting information about hosts, applications, and users from network traffic; host identification is therefore a valid discovery type for a rule using the Discover action. See Cisco's Network Discovery documentation and the Network Discovery overview.

QUESTION NO: 4

Which policy is evaluated before access control rules to determine how tunneled traffic is handled?

A. prefilter policy

B. identity policy

C. file policy

D. health policy

ANSWER: A

Explanation:

prefilter policy is correct. A prefilter policy is evaluated before the access control policy and can identify encapsulated traffic, such as GRE or site-to-site VPN traffic, for specialized handling. Depending on the configured rule action, the device can analyze the outer tunnel headers, block the traffic, or apply further inspection to decapsulated traffic.

This early evaluation allows administrators to control tunnel processing before normal access-control rule matching occurs. Cisco documents prefilter policies and their role in tunnel and encapsulation handling in the Secure Firewall Management Center prefilter policy documentation.

QUESTION NO: 5

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

Explanation:

Intrusion Administrator is the predefined role that is not valid for FireSIGHT event access through Context Explorer. In the legacy FireSIGHT Management Center role model, event investigation and contextual analysis are assigned to roles intended for security-event visibility and analysis. Context Explorer correlates information from FireSIGHT events and related network context so that authorized analysts can investigate activity, hosts, applications, and users. The Intrusion Administrator role is instead focused on administering intrusion-prevention capabilities, including intrusion policy and rule configuration. Its predefined permissions do not grant the FireSIGHT event-access capability required to open and use Context Explorer. Cisco's documentation on Firepower Management Center user accounts and role-based access control explains that permissions are assigned according to administrative or analysis responsibilities, and access to event data is separately controlled. This separation supports least-privilege administration by preventing an intrusion-policy administrator from automatically receiving broad security-event investigation access. See Cisco's Firepower Management Center User Accounts documentation and the Secure Firewall Management Center Administration Guide.

QUESTION NO: 6

Which option is true regarding a Firepower Management Center deployment?

A. It deploys configuration changes to managed devices.

B. It inspects traffic directly on every managed network segment.

C. It replaces the data interfaces on managed devices.

D. It applies policy changes without a deployment operation.

ANSWER: A

Explanation:

A Firepower Management Center **deploys configuration changes to managed devices**. Administrators create and edit policies, device settings, and objects on the management center, but those changes do not affect traffic handling until they are deployed to the applicable managed devices.

Deployment provides a controlled mechanism for applying policy updates and allows the administrator to select the devices that receive pending changes. Monitoring data and events are then sent from managed devices to the Firepower Management Center for centralized analysis. Cisco documents the deployment process in the Secure Firewall Management Center Deploy Configuration Changes documentation.

QUESTION NO: 7

What does the whitelist attribute value "not evaluated" indicate?

A. The host is not a target of the whitelist.

B. The host could not be evaluated because no profile exists for it.

C. The whitelist status could not be updated because the correlation policy it belongs to is not enabled.

D. The host is not on a monitored network segment.

ANSWER: A

Explanation:

The host is not a target of the whitelist. In Sourcefire host discovery and correlation workflows, whitelist evaluation applies only to hosts that fall within the targets or criteria defined by the applicable whitelist configuration. The *not evaluated* value is therefore a scope indicator: the system did not apply that whitelist to the host because the host is outside the whitelist's intended target set. It does not itself represent a failed evaluation or a determination that the host is allowed or disallowed; rather, it records that no whitelist assessment was applicable for that host under the configured policy. This distinction is useful when reviewing discovered-host attributes and correlation results, because it helps administrators identify whether a host's status reflects an actual whitelist decision or simply that the whitelist was not meant to cover it. Cisco's Firepower documentation describes how discovered host information, network-based correlation, and policy scope are used to evaluate hosts and events. See the Cisco Defense Center installation and configuration guides and the Cisco Firepower Management Center documentation resources.

QUESTION NO: 8

Which object contains the network and port variable definitions used by an intrusion policy?

A. variable set

B. network discovery rule

C. correlation rule

D. URL category

ANSWER: A

Explanation:

variable set is correct. A variable set contains named network and port values that intrusion rules can reference, including values for variables such as `$HOME_NET`, `$EXTERNAL_NET`, and service-port variables. Associating a variable set with an intrusion policy lets the same rule content adapt to the protected environment without modifying individual rule headers.

Variable sets are especially useful when policies are deployed to environments with different protected networks, internal services, or address plans. Administrators can select the appropriate variable set for the intrusion policy and centrally maintain the values used by rules. Cisco documents variable sets as part of intrusion-policy configuration in the Secure Firewall Management Center network analysis and intrusion policies documentation.