Cisco

Exam 500-290

IPS Express Security Engineer Representative (IPSESER)

Verson: Demo

[Total Questions: 10]

Question No : 1

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

Question No : 2

What are the two categories of variables that you can configure in Object Management?

A. System Default Variables and FireSIGHT-Specific Variables
B. System Default Variables and Procedural Variables
C. Default Variables and Custom Variables
D. Policy-Specific Variables and Procedural Variables

Answer: C

Question No : 3

One of the goals of geolocation is to identify which option?

A. the location of any IP address
B. the location of a MAC address
C. the location of a TCP connection
D. the location of a routable IP address

Answer: D

Question No : 4

Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?

A. subscribe to a URL intelligence feed
B. subscribe to a VRT
C. upload a list that you create
D. automatically upload lists from a network share

Answer: C

Question No : 5

Suppose an administrator is configuring an IPS policy and attempts to enable intrusion rules that require the operation of the TCP stream preprocessor, but the TCP stream preprocessor is turned off. Which statement is true in this situation?

A. The administrator can save the IPS policy with the TCP stream preprocessor turned off, but the rules requiring its operation will not function properly.
B. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the TCP stream preprocessor will be turned on for the IPS policy.
C. The administrator will be prevented from changing the rule state of the rules that require the TCP stream preprocessor until the TCP stream preprocessor is enabled.
D. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the rules that require the TCP stream preprocessor will be turned off for the IPS policy.

Answer: B

Question No : 6

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule?

A. testing password strength when accessing an application
B. limiting general user access to administrative file shares
C. enforcing two-factor authentication for access to critical servers
D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Answer: D

Question No : 7

Which statement is true regarding malware blocking over HTTP?

A. It can be done only in the download direction.
B. It can be done only in the upload direction.
C. It can be done in both the download and upload direction.
D. HTTP is not a supported protocol for malware blocking.

Answer: C

Question No : 8

Which option is true of the Packet Information portion of the Packet View screen?

A. provides a table view of events
B. allows you to download a PCAP formatted file of the session that triggered the event
C. displays packet data in a format based on TCP/IP layers
D. shows you the user that triggered the event

Answer: C

Question No : 9

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

Question No : 10

Which option is a remediation module that comes with the Sourcefire System?

A. Cisco IOS Null Route
B. Syslog Route
C. Nmap Route Scan
D. Response Group

Answer: A