

Verified Answers Researched by Industry Experts and almost 100% correct

642-532 exam questions updated on regular basis

Same type as the certification exams, 642-532 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 642-532 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Cisco 642-532

Title : Securing Networks Using Intrusion Prevention Systems Exam (IPS)

1. Your sensor is detecting a large volume of web traffic because it is monitoring traffic outside the firewall. What is the most appropriate sensor tuning for this scenario?

- A. lowering the severity level of certain web signatures
- B. raising the severity level of certain web signatures
- C. disabling all web signatures
- D. disabling the Meta Event Generator
- E. retiring certain web signatures

Answer: A

2. Refer to the exhibit.

You are the security administrator for the network in the exhibit. You want your inline Cisco IPS 4255 sensor to drop packets that pose the most severe risk to your network, especially to the servers on your DMZ.

Which two should you use to accomplish your goal in the most time-efficient manner? (Choose two.)

- A. Event Action Filter
- B. Signature Fidelity Rating
- C. Alert Severity
- D. Event Action Override
- E. Application Policy
- F. Target Value Rating

Answer: DF

3. In which scenario are an AIC engine and the Application Policy Enforcement feature needed?

- A. You think some users with operator privileges have been misusing their privileges. You want the sensor to detect this activity and revoke authentication privileges.
- B. You think users on your network are disguising the use of file-sharing applications by tunneling the traffic through port 80. You want your sensor to identify and stop this activity.
- C. You have been experiencing attacks on your voice gateways. You want to implement advanced VoIP protection.
- D. You believe that hackers are evading the Cisco IPS. You want the sensor to eradicate anomalies in the IP and TCP layers that allow an IPS to be evaded.

Answer: B

4. In which file format are IP logs stored?

- A. Microsoft Word
- B. Microsoft Excel
- C. text
- D. libpcap

Answer: D

5. How does a Cisco network sensor detect malicious network activity?

- A. by using a blend of intrusion detection technologies

- B. by performing in-depth analysis of the protocols that are specified in the packets that are traversing the network
- C. by comparing network activity to an established profile of normal network activity
- D. by using behavior-based technology that focuses on the behavior of applications

Answer: A

6. What are three differences between inline and promiscuous sensor functionality? (Choose three.)

- A. A sensor that is operating in inline mode can drop the packet that triggers a signature before it reaches its target, but a sensor that is operating in promiscuous mode cannot.
- B. A sensor that is operating in inline mode supports more signatures than a sensor that is operating in promiscuous mode.
- C. Deny actions are available only to inline sensors, but blocking actions are available only to promiscuous mode sensors.
- D. A sensor that is operating in promiscuous mode can perform TCP resets, but a sensor that is operating in inline mode cannot.
- E. Inline operation provides more protection from Internet worms than promiscuous mode does.
- F. Inline operation provides more protection from atomic attacks than promiscuous mode does.

Answer: AEF

7. What is a configurable weight that is associated with the perceived importance of a network asset?

- A. Risk Rating
- B. parameter value
- C. Target Value Rating
- D. severity level
- E. storage key
- F. rate parameter

Answer: C

8. Which two statements are true about Cisco IPS signatures? (Choose two.)

- A. A signature is a set of rules that pertain to typical intrusion activity.
- B. When network traffic matches a signature, the signature must generate an alert, but it can also initiate a response action.
- C. Some signatures can be triggered by the contents of a single packet.
- D. Signatures trigger alerts only when they match a specific pattern of traffic.
- E. You can disable signatures and later re-enable them; however, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic.
- F. You can enable and modify built-in signatures, but you cannot disable them.

Answer: AC

9. Which two are necessary to take into consideration when preparing to tune your sensor? (Choose two.)

- A. the security policy
- B. the network topology
- C. which outside addresses are statically assigned to the servers and which are DHCP addresses
- D. the IP addresses of your inside gateway and outside gateway
- E. which traffic the sensor denies by default
- F. the current configuration for each virtual sensor

Answer: AB

10. What would best mitigate the executable-code exploits that can perform a variety of malicious acts, such as erasing your hard drive?

- A. assigning deny actions to signatures that are controlled by the Trojan engines
- B. assigning the TCP reset action to signatures that are controlled by the Normalizer engine
- C. enabling blocking
- D. enabling Application Policy Enforcement

E. assigning blocking actions to signatures that are controlled by the State engine

Answer: A

11. Which user account role on a Cisco IPS sensor must you specifically create in order to allow special root access for troubleshooting purposes only?

- A. Operator
- B. Viewer
- C. Service
- D. Administrator

Answer: C

12. Your network has only one entry point. However, you are concerned about internal attacks. Select the three best choices for your network. (Choose three.)

- A. CSA Agents on corporate mail servers
- B. CSA Agents on critical network servers and user desktops
- C. the network sensor behind (inside) the corporate firewall
- D. the network sensor in front of (outside) the corporate firewall
- E. sensor and CSA Agents that report to management and monitoring servers that are located inside the corporate firewall
- F. sensor and CSA Agents that report to management and monitoring servers that are located outside the corporate firewall

Answer: BCE

13. In which three ways does a Cisco network sensor protect network devices from attacks? (Choose three.)

- A. It uses a blend of intrusion detection technologies to detect malicious network activity.
- B. It can generate an alert when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
- C. It permits or denies traffic into the protected network that is based on access lists that you create on the sensor.
- D. It can take a variety of actions when it detects traffic that matches a set of rules that pertain to typical intrusion activity.
- E. It uses behavior-based technology that focuses on the behavior of applications to protect network devices from known attacks and from new attacks for which there is no known signature.

Answer: ABD

14. Which three values are used to calculate the Risk Rating for an event? (Choose three.)

- A. Attack Severity Rating
- B. Signature Fidelity Rating
- C. Target Value Rating
- D. Target Fidelity Rating
- E. Reply Ratio
- F. Rate

Answer: ABC

15. Which two are appropriate installation points for a Cisco IPS sensor? (Choose two.)

- A. on publicly accessible servers
- B. on critical network servers
- C. at network entry points
- D. on user desktops
- E. on corporate mail servers
- F. on critical network segments

Answer: CF

[More 642-532 Information](#)

Related 642-532 Exams

[642-515](#) *Securing Networks with ASA Advanced*

[642-545](#) *Implementing Cisco Security Monitoring, Analysis and Response System*

[642-542](#) *Cisco SAFE Implementation Exam*

[642-552](#) *Securing Cisco Network Devices Exam*

[642-513](#) *Securing Hosts Using Cisco Security Agent Exam (HIPS)*

[642-502](#) *Securing Networks with Cisco Routers and Switches Exam (SNRS)*

[642-503](#) *Securing Networks with Cisco Routers and Switches*

[642-523](#) *Securing Networks with PIX and ASA*

[642-532](#) *Securing Networks Using Intrusion Prevention Systems Exam (IPS)*

[642-521](#) *Cisco Secure PIX Firewall Advanced*

[642-551](#) *Securing Cisco Network Devices Exam (SND)*

[642-522](#) *Securing Networks with PIX and ASA Exam (SNPA)*

Other Cisco Exams

[642-731](#) [646-056](#) [352-001](#) [642-971](#) [650-178](#) [642-359](#) [646-229](#) [642-582](#)

[642-241](#) [642-052](#) [642-567](#) [642-371](#) [642-071](#) [642-832](#) [642-972](#) [642-481](#)

[646-362](#) [642-381](#) [642-591](#) [642-892](#)