

642-532 Practice Test

Cisco Securing Networks Using Intrusion Prevention Systems Exam (IPS)

642-532: Securing Networks Using Intrusion Prevention Systems Exam (IPS)

Practice Exam: 642-532 Exams

Exam Number/Code: 642-532

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

Questions and Answers: 67 Q&As
(CCSP)



Exam : [642-532](#)

For candidates making preparation for the Cisco 642-532 questions and answers, what they most desire is to easily pass the 642-532 (Securing Networks Using Intrusion Prevention Systems Exam (IPS)) exam. ItCertHome 642-532 includes 67 questions and answers, which are collected and collated by experts of Cisco. With our 642-532 study materials, you can successfully take Cisco certification of 642-532 exam and go further on Cisco career path.

Free 642-532 Demo

we provide Cisco 642-532 demo exam for free (in PDF format) before you decide to purchase it. Thus,you can know better about the quality of our practice exam and then make your right decision.

ItCertHome Test tool's advantages:

High Quality and Value of 642-532 exam

ItCertHome Cisco CCSP 642-532 Practice Questions is developed and finished by Cisco technical team , cover every field of the exam . Besides, we have verified 642-532 answers,almost 100% correct.

100% Guarantee to Pass 642-532 Exam

We promise to give you FULL REFUND if you fail the CCSP 642-532 certification(Cisco Certified Network Associate) with the use of our ItCertHome testing engine.

642-532 Self Test Mode

ItCertHome provides a simulated and interactive environment where you can test your knowledge and skills about 642-532 to ensure enough assurance in real testing center.

Periodic Updates of ItCertHome 642-532

Once there is some change on Cisco 642-532 exam, we will update it timely, and the product you buy will be updated within 90 days for free.

Professional and Efficient Service

We offer 7*24 customer support via diverse channels: LIVE CHAT,MAIL.Expecting the communication with you about IT certification.

The Questions & Answers cover the latest real test and with all the correct answer.we promise the Q&A for **Cisco CCSP 642-532** examination of original title complete coverage.ItCertHome **642-532 Braindumps** Questions & Answers help you pass the exam. Otherwise,we will give you a full refund.

We promised that use ItCertHome Q&A ensure you pass the exam at your first try.

1. The Q&A are from cooperation exam center of the real original title,summaried by our professional team and collated by senior IT lectured in co-training center to make sure the professional quality of the Q&A.The correctly of the Q&A is 100%, the coverage of 642-532 Q&A are more than 96%.All you need to study the whole 642-532 Q&A before you participate the certification exam,it should be possible to easily complete the exam and pass the

certification.

2. ItCertHome to all the Q&A, we promised "do not pass the exam give you a full refund". If you buy our 642-532 Q&A and did not pass the exam at the first try. You can take the examination report card that stamped with PROMETRIC or VUE test centers Seal. we will refund your full cost of 642-532 Q&A, absolutely guarantee you interests have no losses.(For a full refund details)

3. ItCertHome professional IT Q&A vendors, we provide well after-sale service. To all the customers buy the Q&A, we provide track service. when you buy the Q&A with in one year. you can enjoy the upgrade Q&A service for free. If in this period, the certified test center change the 642-532 Q&A, we will update the Q&A in the first time, and provide you the download update for free.

[Cisco 642-532](#) Test belongs to one of the CCSP certified test, if needs to obtain the CCSP certificate, you also need to participate in other related test, the details you may visit the CCSP certified topic, in there, you will see all related CCSP certified subject of examination.

642-532

ItCertHome professional provide CCSP 642-532 the newest Q&A, completely covers 642-532 test original topic. With our complete CCSP resources, you will minimize your CCSP cost and be ready to pass your 642-532 tests on Your First Try, 100% Money Back Guarantee included!

This 642-532 PDF demo do not include the questions and answers's picture:

Exam : Cisco 642-532

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

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. In which file format are IP logs stored?

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

Answer: D

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

More [642-532 practice test](#)

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

[646-588](#) [646-362](#) [646-230](#) [650-251](#) [642-871](#) [642-891](#) [642-067](#) [644-141](#)

[650-575](#) [640-811](#) [642-274](#) [642-242](#) [642-832](#) [642-513](#) [642-566](#) [646-276](#)

[642-741](#) [642-105](#) [350-030](#) [642-356](#)