642-533

Cisco

Implementing Cisco Intrusion Prevention System (IPS)

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=642-533

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 642-533 exam in first attempt, but also you can get a high score to acquire Cisco certification.

If you use pass4sureofficial 642-533 Certification questions and answers, you will experience actual 642-533 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 642-533 exam. Every point from pass4sure 642-533 PDF, 642-533 review will help you take Cisco 642-533 exam much easier and become Cisco certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Cisco 642-533 course:

** Up-to-Date Cisco 642-533 questions taken from the real exam.*
** 100% correct Cisco 642-533 answers you simply can't find in other 642-533 courses.*
** All of our tests are easy to download. Your file will be saved as a 642-533 PDF.*
** Cisco 642-533 brain dump free content featuring the real 642-533 test questions.*

Cisco 642-533 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 642-533 exam training are an absolute favorite in the industry. You will pass Cisco 642-533 certification test and career opportunities will be open for you.

642-533

QUESTION 1
In which three ways does a Cisco IPS network sensor protect the network from attacks? (Choose three.)

A. It can take variety of actions when it detects traffic that matches a set of rules that pertain to typical intrusion activity
B. It permits or denies traffic into the protected network based on access lists that you create on the sensor
C. It uses a blend of intrusion detection technologies to detect malicious network activity
D. It can generate an alert when it detects traffic that matches a set of rules that pertain to typical intrusion activity

Answer: A,C,D

QUESTION 2
You would like to have your inline sensor deny attackers inline when events occur that have risk ratings over 85. Which two actions, when taken in conjunction will accomplish this? (Choose two.)

A. Assign the risk rating range of 85 to 100 to the Deny Attacker inline event action
B. Create target value ratings of 85 to 100
C. Create an event variable for the protected network
D. Create an Event Action Filter and assign the risk rating range of 85 to 100 to the filter
E. Enable Event Action overrides
F. Enable Event Action Filters

Answer: A,E

QUESTION 3
Which statement accurately describes Cisco IPS Sensor Automatic signature and service pack updates?

A. If multiple signature or service pack updates are available when the sensor checks for an update, the Cisco IPS Sensor installs the first update it detects
B. You must download service pack and signature updates form cisco.com to locally accessible server before they can be automatically applied to your Cisco IPS Sensor
C. When you configure automatic updates, the Cisco IPS Sensor checks Cisco.com for updates hourly.
D. The Cisco IPS Sensor can automatically download service pack and signature updates form cisco.com
E. The Cisco IPS Sensor can download signature and service pack updates only from an TFTP or HTTP server

Answer: B

QUESTION 4
You think users on your corporate network are disguising the user of file-sharing applications by tunneling the traffic through port 80. How can you configure your Cisco IPS Sensor to identify and stop this activity?

A. Enable all signatures in the Service HTTP engine
B. Assign the Deny Packet inline action to all signatures in the service HTTP Engine
C. Enable the alarm for the non-HTTP traffic signature. Then create an Event Action Override that adds the Deny Packet inline action to event triggered by the signature if the traffic originates from your corporate network
D. Enable both the HTTP application policy and the alarm on non-HTTP traffic signature
E. Enable all signature in the Service HTTP engine. Then create an event action override that adds the Deny packet inline action to events triggered by these signatures if the traffic originates form your corporate network

Answer: D

QUESTION 5
With Cisco IPS 6.0, what is the maximum number of Virtual sensors that can be configured on a single platform?

A. The number depends on the amount of device memory
B. Six
C. Four
D. Two
E. Two in promiscuous mode using VLAN groups, four in inline mode supporting all interface type configurations

Answer: C

QUESTION 6
Which two management access methods are enabled by default on a Cisco IPS sensor? (Choose two.)

A. HTTP
B. SSH
C. Telnet
D. IPSec
E. HTTPS

Answer: B,E

QUESTION 7
What is used to perform password recovery for the "cisco" admin account on a Cisco IPS 4200 Series Sensor?

A. ROMMON CLI
B. Cisco IDM
C. Setup mode
D. Recovery Partition
E. GRUB menu

Answer: E

QUESTION 8
How should you create a custom signature that will fire when a series of pre-defined signature occur and you want the Cisco IPS Sensor to generate alerts only for the new custom signature, not for the individual signatures?

A. Use the Normalizer Engine and se the summary mode to Global Summarize
B. Use the Service Engine and Set the summary mode to global summarize
C. Use the Trojan Engine and remove the Produce Alert action from the component signatures
D. Use the Normalizer engine and remove the Produce Alert action from the component signatures
E. Use the ATOMIC Engine and set the summary mode to Global Summarize
F. Use the Meta engine and remove the produce alert action from the component signatures

Answer: F

QUESTION 9
When configuring Passive OS Fingerprinting, what is the purpose of restricting operating system mapping to specific addresses?

A. Limits the ARR to the defined IP Addresses
B. Specifies which IP Address range to import from EPI for OS fingerprinting
C. Excludes the defined IP Addresses from automatic risk rating calculations so that you can specify the desired risk rating
D. Allows you to configure separate OS maps within that IP address range

Answer: A

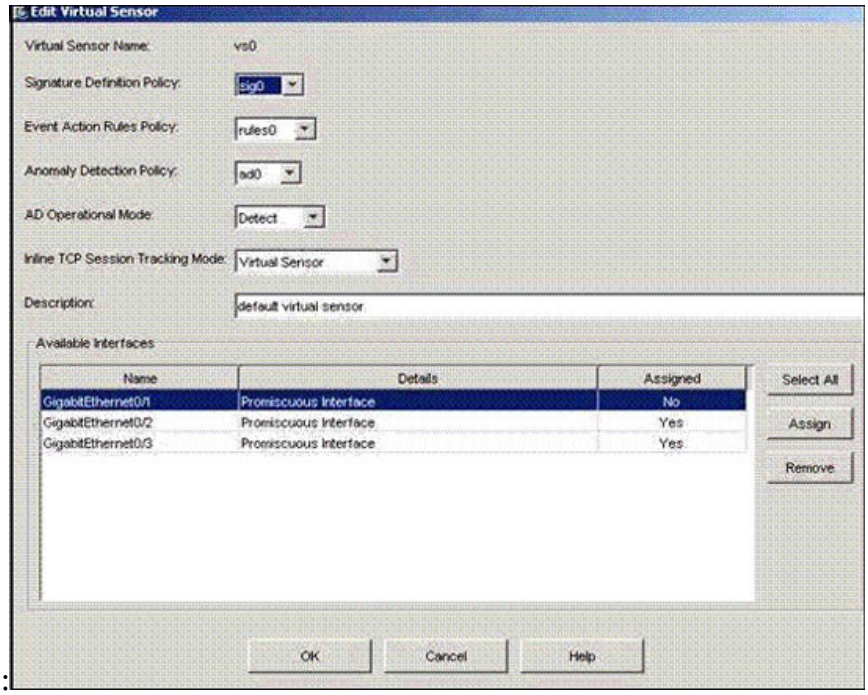
QUESTION 10
You have been made aware of new and unwanted traffic on your network. You want to create a signature to monitor and perform an action against that traffic when certain thresholds are reached. What would be the best way to configure this new signature?

A. Use the Anomaly Detection functions to learn abut the unwanted traffic, then create a new meta signature using Cisco IDM
B. Clone and edit an existing signature that closely matches the traffic you are trying to prevent

C. Create a new signature definition, edit it, and then enable it
D. Edit a built-in signature that closely matches the traffic you are trying to prevent

Answer: C

QUESTION 11
Exhibit:



:
Your work as a network technician at Certkiller .com. Study the exhibit carefully. Which interfaces are assigned to an inline VLAN pair?

A. GigabitEthernet0/1 with GigbitEthernet0/3
B. GigabitEthernet0/2 with GigabitEthernet0/3
C. GigabitEthernet0/1 with GigabitEthernet0/2
D. None in this Virtual Sensor

Answer: D

QUESTION 12
A user with which user account role on a Cisco IPS Sensor can log into the native operating system shell for advanced troubleshooting purposes when directed to do so by Cisco TAC?

A. Viewer
B. Administrator
C. Super
D. Operator
E. Root
F. Service

Answer: F

QUESTION 13
Which action does the copy /erase ftp://172.26.26.1/sensor_config01 current_config command perform?

A. Copies and saves the running configuration to the FTP server and replaces it with the source configuration file
B. Merges the source configuration file with the current configuration
C. Erase the sensor_config01 file the FTP server and replaces it with the current configuration file from the Cisco IPS Sensor
D. Overwrites the backup configuration and applies the source configuration file to the system default configuration

Answer: D

QUESTION 14
You are using Cisco IDM. What precaution must you keep in mind when adding, editing or deleting allowed hosts on a Cisco IPS Sensor?

A. You must not delete the IP Address used for remote management
B. When using access lists to permit remote access, you must specify the direction of allowed communications
C. You must use an inverse mask, such as 10.0.2.0 0.0.0.255 for the specified network mask for the IP Address
D. You can only configure the allowed hosts using the CLI
E. You must not allow entire subnets to access the Cisco IPS Sensor

Answer: A

QUESTION 15
Which signature action or actions should be selected to cause the attacker's traffic flow to terminate when the Cisco IPS Sensor is operating in promiscuous mode?

A. Deny connection, reset tcp connection
B. Deny Packet, reset tcp connection
C. Deny Packet
D. Reset tcp connection
E. Deny Connection
F. Deny Attacker

Answer: D

QUESTION 16
Which character must precede a variable to indicate that you are using a variable rather

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA