642-627Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/642-627.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which two are the functions of the learning feature of anomaly detection within a Cisco IPS appliance? (Choose two.)

A. observes actual traffic patterns to the zones

B. retrieves zero-day attack information from the Cisco SIO

C. dynamically populates the host operating system database

D. allows false-positive training by an IPS administrator

E. builds the host reputation histogram

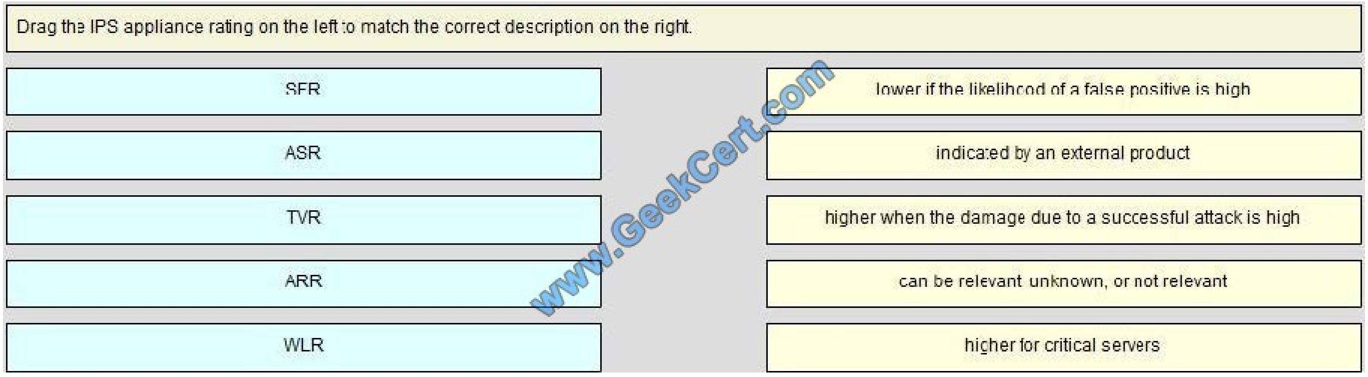
F. learns which legitimate services have a scanning behavior

Correct Answer: AF

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_anomaly_detection.ht ml#wp1046814

QUESTION 2

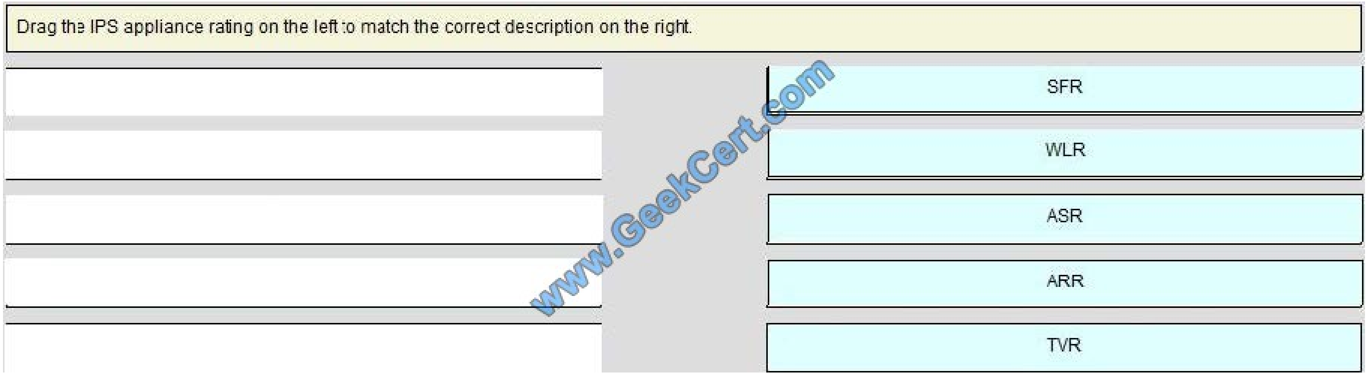
Select and Place:



Drag the IPS appliance rating on the left to match the correct description on the right.

SFR	lower if the likelihood of a false positive is high
ASR	indicated by an external product
TVR	higher when the damage due to a successful attack is high
ARR	can be relevant, unknown, or not relevant
WLR	higher for critical servers

Correct Answer:



Drag the IPS appliance rating on the left to match the correct description on the right.

	SFR
	WLR
	ASR
	ARR
	TVR

QUESTION 3

Which two operations would put an inline Cisco IPS sensor in detection mode? (Choose two.)

A. subtract all aggressive actions using event action filters

B. decrease the event count using event action filters

C. increase the maximum inter-event interval using event action overrides

D. remove the default event action override, which drops traffic with a risk rating of 90 to 100

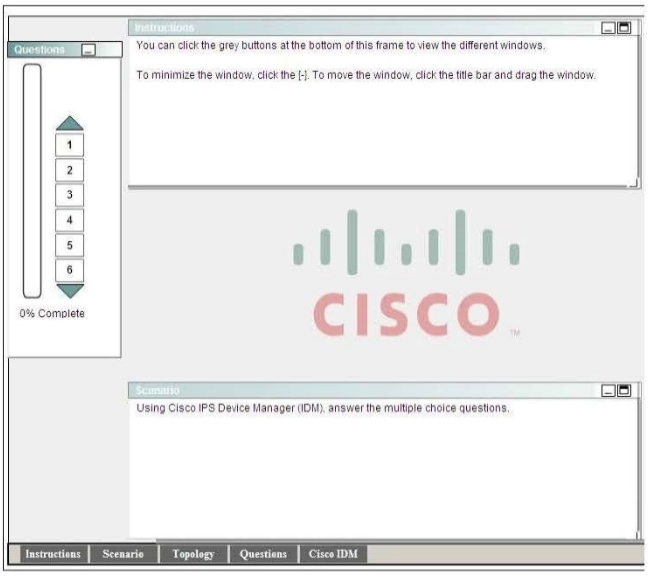
E. enable anomaly detection in detection mode only

Correct Answer: AD

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/cli/cli_anomaly_detection.ht ml#wp1041433

Not sure of this answer yet - 9/25/12 - DD but seems to be another Cisco classif question, meaning that once a signature is tuned it is ready for prime time i.e. detection mode After the signatures are tuned, remove the event action filters that removed the aggressive actions, and remove the event action overrides that produced the verbose alerts.

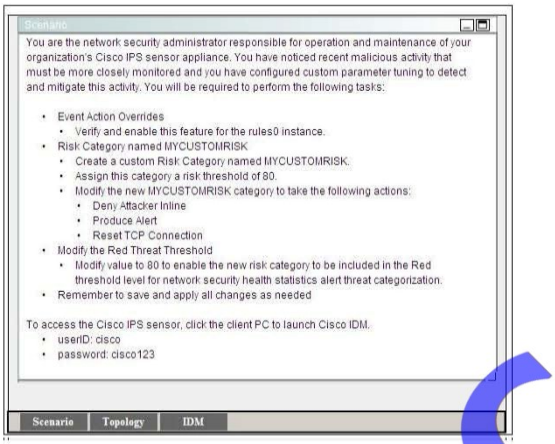
QUESTION 4



You can click the grey buttons at the bottom of this frame to view the different windows.

To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.

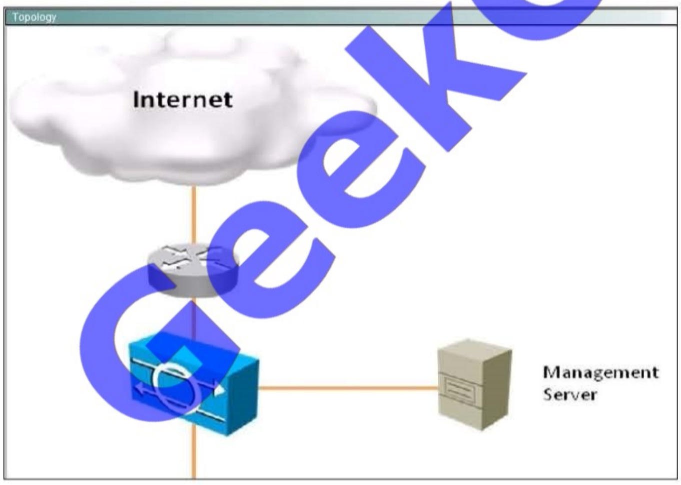


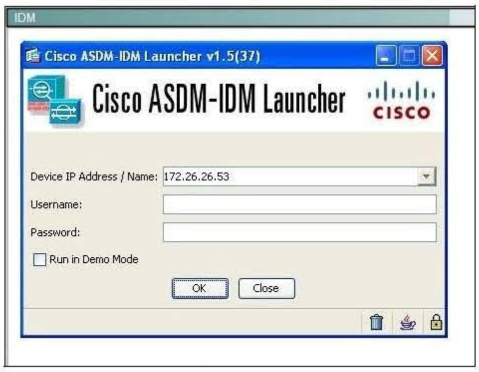
You are the network security administrator responsible for operation and maintenance of your organization's Cisco IPS sensor appliance. You have noticed recent malicious activity that must be more closely monitored and you have configured custom parameter tuning to detect and mitigate this activity. You will be required to perform the following tasks:

- Event Action Overrides
  - Verify and enable this feature for the rules0 instance.
- Risk Category named MYCUSTOMRISK
  - Create a custom Risk Category named MYCUSTOMRISK.
  - Assign this category a risk threshold of 80.
  - Modify the new MYCUSTOMRISK category to take the following actions:
    - Deny Attacker Inline
    - Produce Alert
    - Reset TCP Connection
- Modify the Red Threat Threshold
  - Modify value to 80 to enable the new risk category to be included in the Red threshold level for network security health statistics alert threat categorization.
- Remember to save and apply all changes as needed

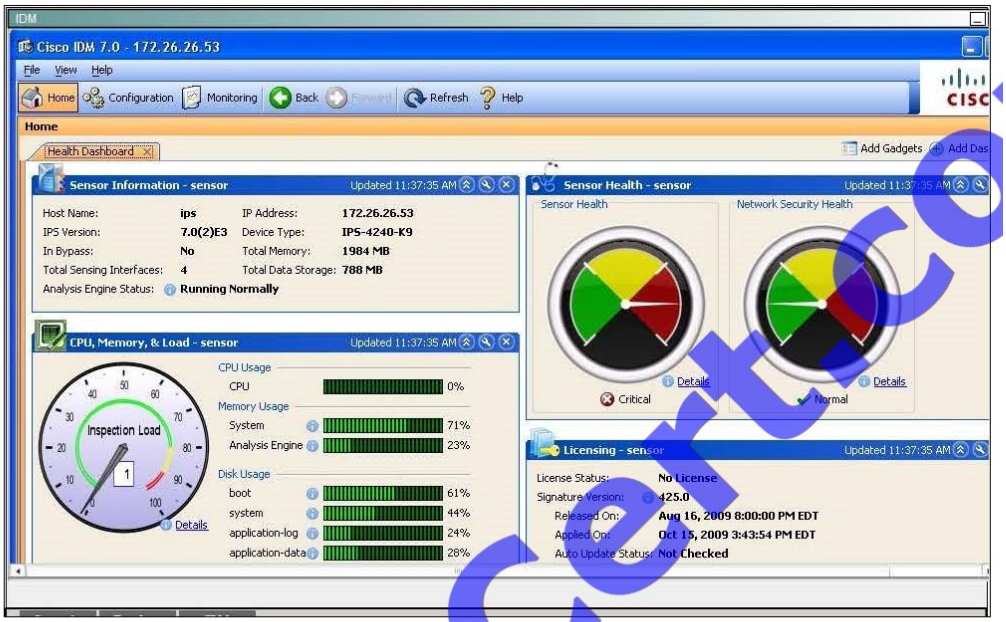
To access the Cisco IPS sensor, click the client PC to launch Cisco IDM.

- userID: cisco
- password: cisco123





Device IP Address / Name: 172.26.26.53
Username:
Password:
□ Run in Demo Mode



Sensor Information - sensor Updated 11:37:35 AM

Host Name:	ips	IP Address:	172.26.26.53
IPS Version:	7.0(2)E3	Device Type:	IPS-4240-K9
In Bypass:	No	Total Memory:	1984 MB
Total Sensing Interfaces:	4	Total Data Storage:	788 MB
Analysis Engine Status:	Running Normally		

CPU, Memory, & Load - sensor Updated 11:37:35 AM

CPU Usage

CPU	0%

Memory Usage

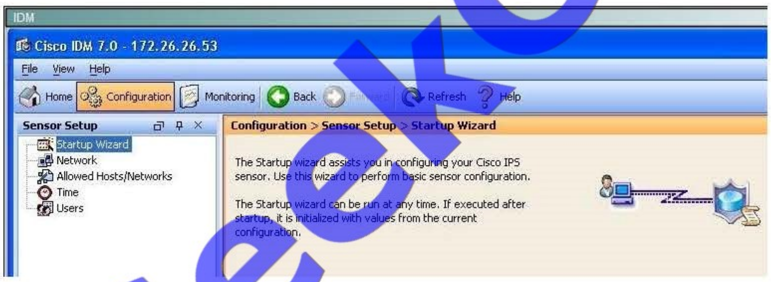
System	71%
Analysis Engine	23%

Disk Usage

boot	61%
system	44%
application-log	24%
application-data	28%

Licensing - sensor Updated 11:37:35 AM

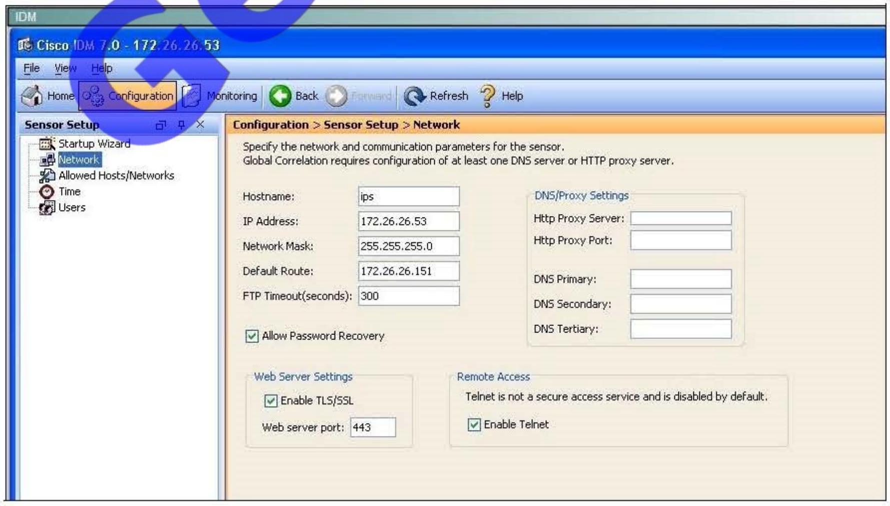
License Status:	No License
Signature Version:	425.0
Released On:	Aug 16, 2009 8:00:00 PM EDT
Applied On:	Oct 15, 2009 3:43:54 PM EDT
Auto Update Status:	Not Checked


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Sensor Setup
Startup Wizard
Network
Allowed Hosts/Networks
Time
Users

Configuration > Sensor Setup > Startup Wizard

The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.


IDM
Cisco IDM 7.0 - 172.26.26.53
File View Help
Home Configuration Monitoring Back Forward Refresh Help
Sensor Setup
Startup Wizard
Network
Allowed Hosts/Networks
Time
Users

Configuration > Sensor Setup > Network

Specify the network and communication parameters for the sensor.
Global Correlation requires configuration of at least one DNS server or HTTP proxy server.

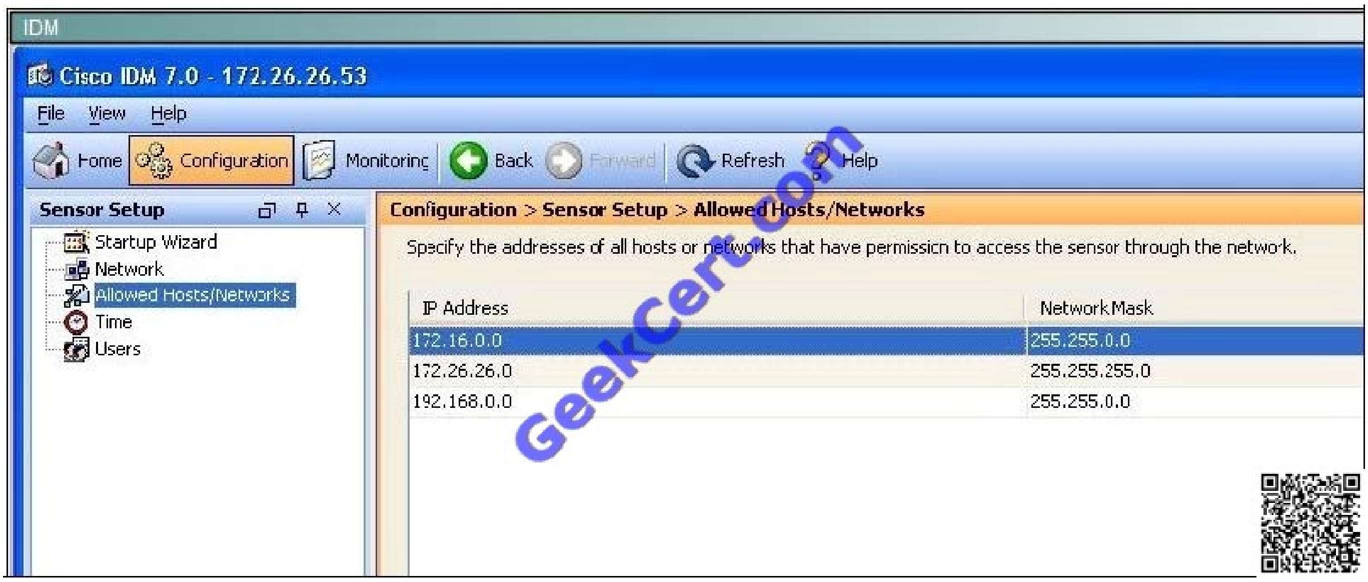
Hostname: ips
IP Address: 172.26.26.53
Network Mask: 255.255.255.0
Default Route: 172.26.26.151
FTP Timeout(seconds): 300

☑ Allow Password Recovery

DNS/Proxy Settings
Http Proxy Server:
Http Proxy Port:
DNS Primary:
DNS Secondary:
DNS Tertiary:

Web Server Settings
☑ Enable TLS/SSL
Web server port: 443

Remote Access
Telnet is not a secure access service and is disabled by default.
☑ Enable Telnet



Cisco IDM 7.0 - 172.26.26.53

Configuration > Sensor Setup > Allowed Hosts/Networks

Specify the addresses of all hosts or networks that have permission to access the sensor through the network.

IP Address	Network Mask
172.16.0.0	255.255.0.0
172.26.26.0	255.255.255.0
192.168.0.0	255.255.0.0

What is the status of OS Identification?

A. It is only enabled to identify Cisco IOS" OS using statically mapped OS fingerprinting

B. OS mapping information will not be used for Risk Rating calculations.

C. It is configured to enable OS mapping and ARR only for the 10.0.0.0/24 network.

D. It is enabled for passive OS fingerprinting for all networks.

Correct Answer: C

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/ime/ime_event_action_rules.

html#wp2119120

Understanding Passive OS Fingerprinting

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK

packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk

rating of the alert for the attack and/or the sensor may filter the alert for the attack.

You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the

victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

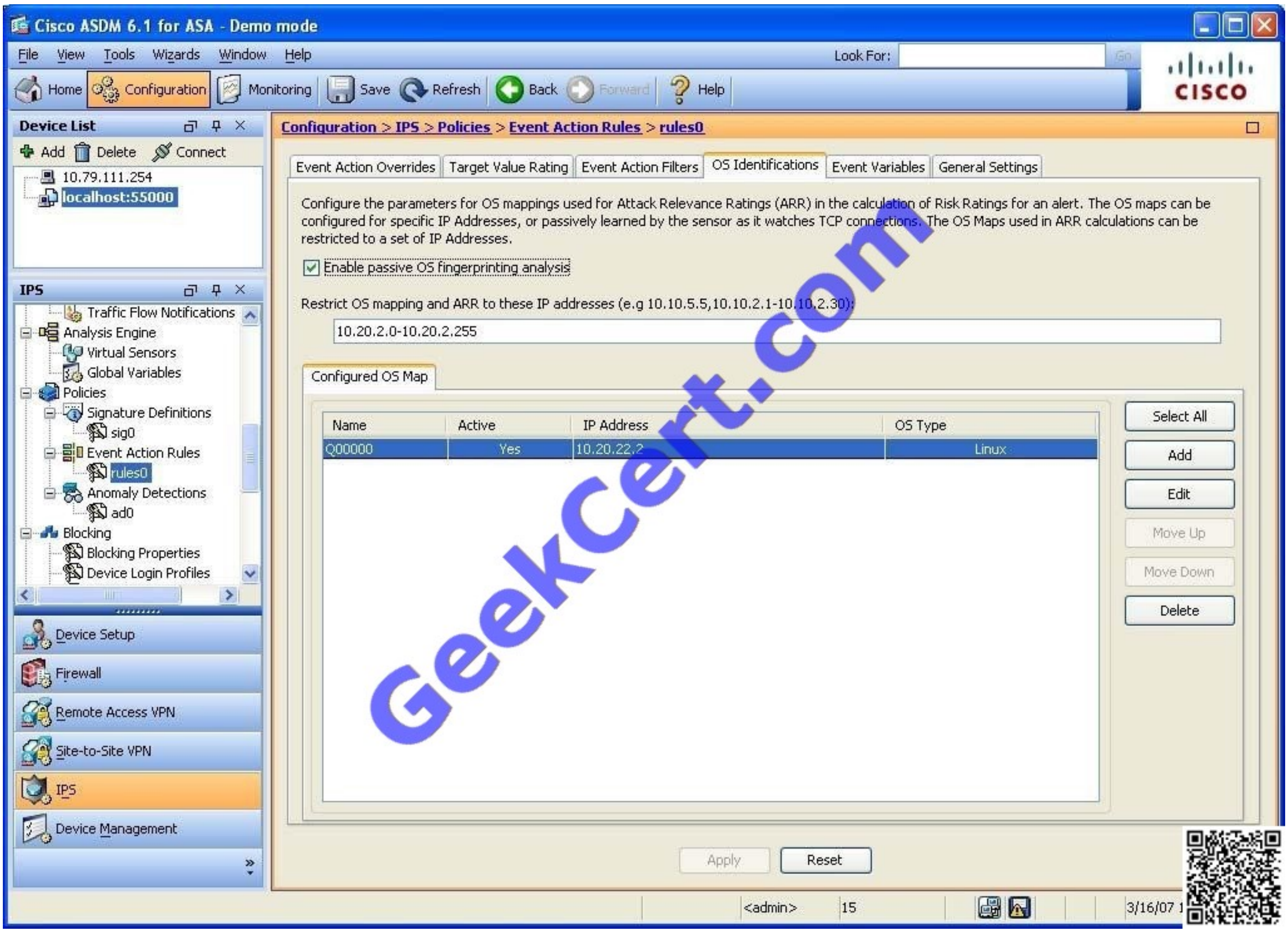
?assive OS learning

Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP

SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.

?ser-configurable OS identification

You can configure OS host mappings, which take precedence over learned OS mappings. ?omputation of attack relevance rating and risk rating



Configuration > IPS > Policies > Event Action Rules > rules0

Configure the parameters for OS mappings used for Attack Relevance Ratings (ARR) in the calculation of Risk Ratings for an alert. The OS maps can be configured for specific IP Addresses, or passively learned by the sensor as it watches TCP connections. The OS Maps used in ARR calculations can be restricted to a set of IP Addresses.

☑ Enable passive OS fingerprinting analysis

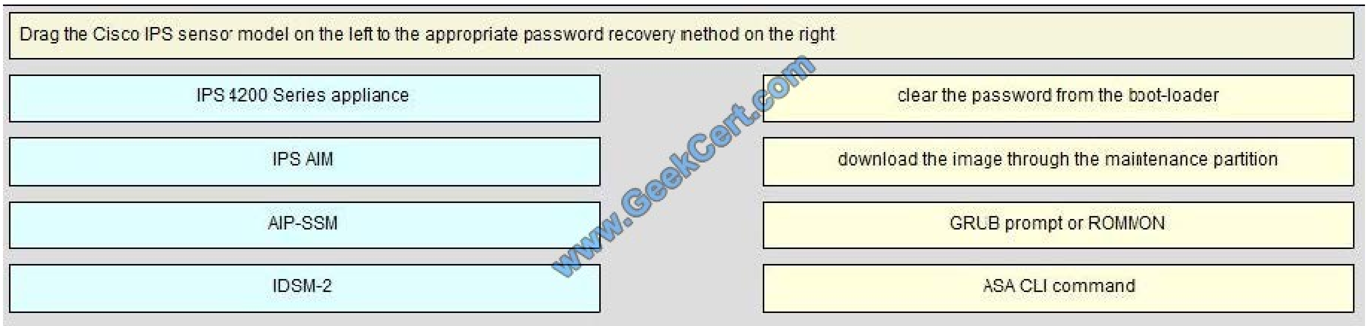
Restrict OS mapping and ARR to these IP addresses (e.g 10.10.5.5,10.10.2.1-10.10.2.30):

10.20.2.0-10.20.2.255

Name	Active	IP Address	OS Type
Q00000	Yes	10.20.22.2	Linux

QUESTION 5

Select and Place:



Drag the Cisco IPS sensor model on the left to the appropriate password recovery method on the right

IPS 4200 Series appliance

IPS AIM

AIP-SSM

IDSM-2

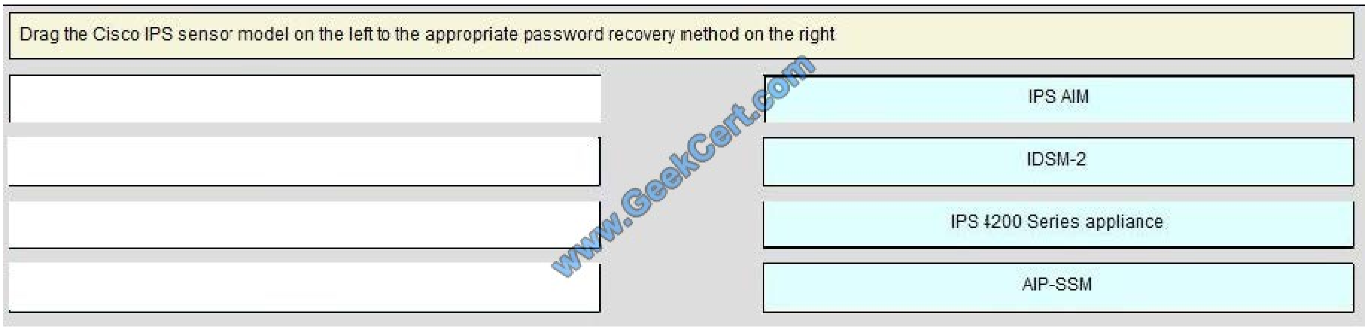
clear the password from the boot-loader

download the image through the maintenance partition

GRUB prompt or ROMMON

ASA CLI command

Correct Answer:



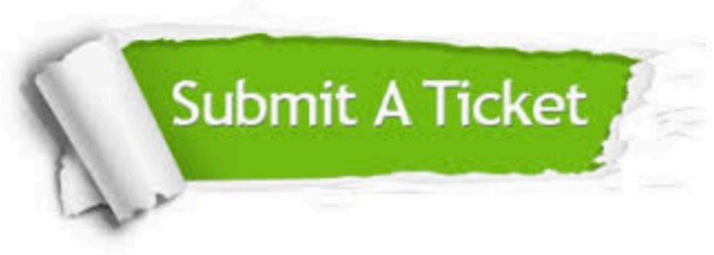
Drag the Cisco IPS sensor model on the left to the appropriate password recovery method on the right

IPS AIM

IDSM-2

IPS 4200 Series appliance

AIP-SSM


Submit A Ticket