



300-210^{Q&As}

Cisco Threat Control Solutions

Pass Cisco 300-210 Exam with 100% Guarantee

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

<https://www.lead4pass.com/300-210.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

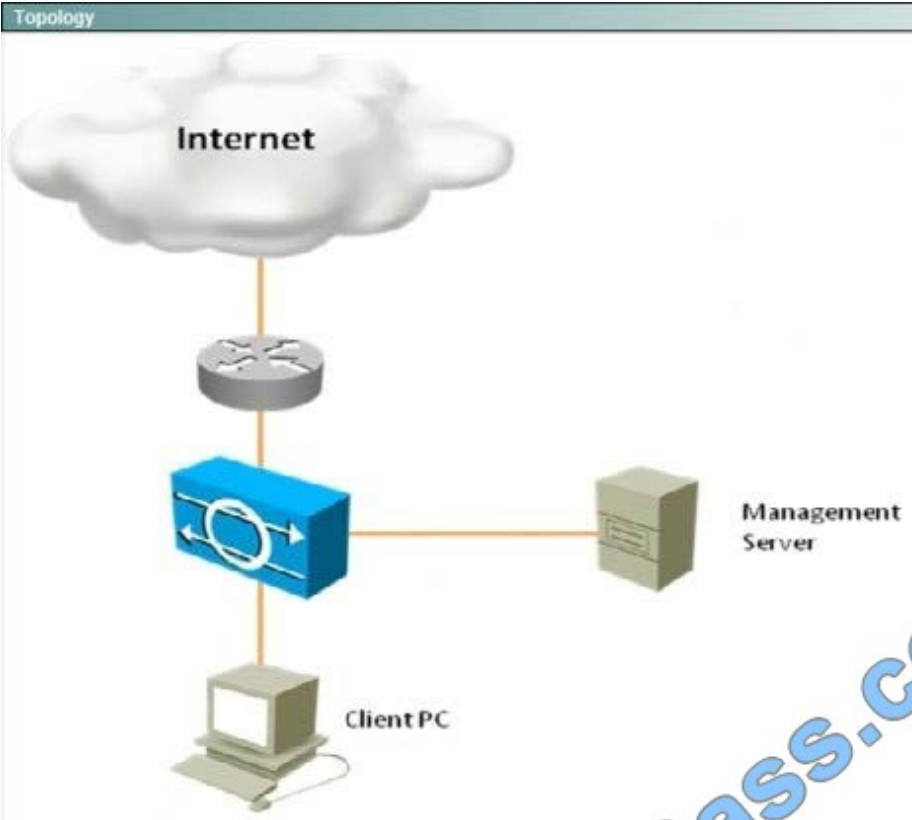
Instructions

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.

Scenario

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



Cisco IDM

Cisco IDM 7.0 - 172.26.26.53

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Home

Health Dashboard

Sensor Information - sensor Updated 1:46:22 PM

Host Name: ips IP Address: 172.26.26.53
IPS Version: 7.0(2) 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 1:46:22 PM

Inspection Load: 1

CPU Usage: CPU 1%

Memory Usage: System 73%, Analysis Engine 23%

Disk Usage: boot 51%, system 44%, application-log 24%

Sensor Health - sensor Updated 1:46:22 PM

Sensor Health: Critical

Network Security Health: Normal

Licensing - sensor Updated 1:46:22 PM

License Status: Not expired until Aug 27, 2011 4:59:59 PM MST
Signature version: 425.0
Released On: Aug 16, 2009 5:00:00 PM MST
Applied On: Oct 15, 2009 12:43:54 PM MST
Released On: Oct 15, 2009 1:09:06 AM MST
Applied On: Jul 13, 2010 3:05:43 AM MST
Auto Update Status: Not Checked

Interface Status - sensor Updated 1:46:22 PM

Interface	Link	Enabled	Speed (...)	Mode	Received Packets	Transmitted Packets
GigabitEthernet0/0	up	yes	100	inline-v...	7,157,393	6,467,360
GigabitEthernet0/1	d...	yes		unpaired	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: D

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.

QUESTION 2

When https traffic is scanned, which component of the full URL does CWS log?

- A. not log
- B. only host host and query path and query

Correct Answer: B



QUESTION 3

Which website can be used to validate group information about connections that flow through Cisco CWS?

- A. whoami.scansafe.net
- B. policytrace.scansafe.net
- C. whoami.scansafe.com
- D. policytrace.scansafe.com

Correct Answer: B

QUESTION 4

Which Cisco ESA predefined sender group uses parameter-matching to reject senders?

- A. BLACKLIST
- B. WHITELIST
- C. SUSPECTLIST
- D. UNKNOWNLIST

Correct Answer: A

QUESTION 5

Which type of policy do you configure if you want to look for a combination of events using Boolean logic?

- A. correlation
- B. application detector
- C. traffic profile
- D. access control
- E. intrusion

Correct Answer: A

[Latest 300-210 Dumps](#)

[300-210 PDF Dumps](#)

[300-210 Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.