# 300-210Q&As

Cisco Threat Control Solutions

## Pass Cisco 300-210 Exam with 100% Guarantee

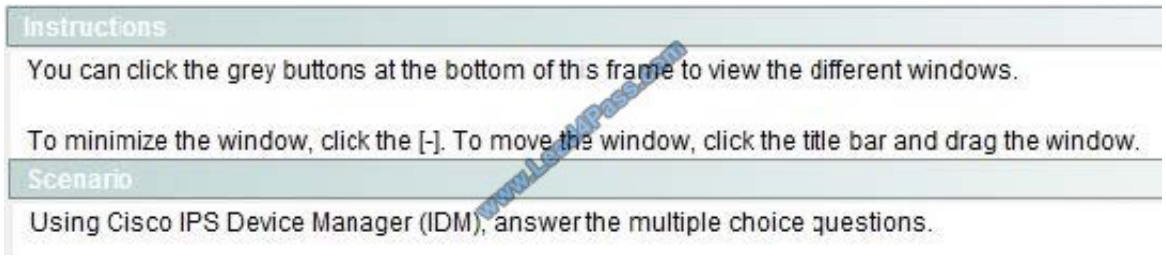
Free Download Real Questions & Answers **PDF** and **VCE** file from:

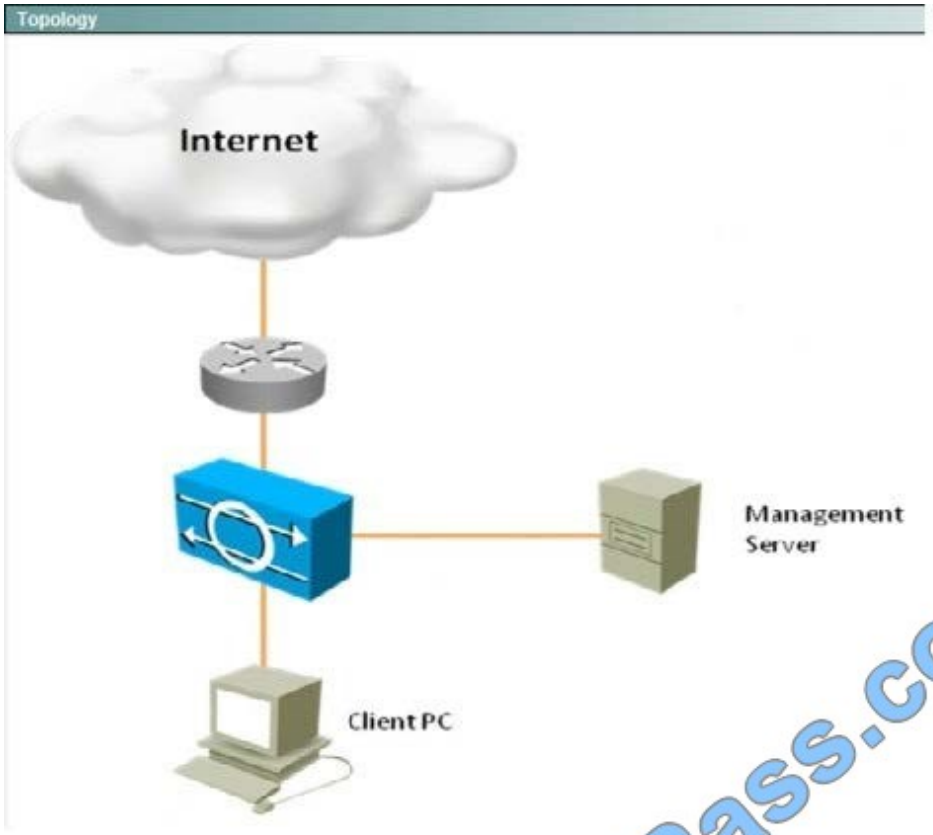
**https://www.lead4pass.com/300-210.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**


Instructions
You can click the grey buttons at the bottom of th s 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.




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