300-206Q&As

Implementing Cisco Edge Network Security Solutions

Pass Cisco 300-206 Exam with 100% Guarantee

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

https://www.lead4pass.com/300-206.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which three configurations tasks do you perform to allow Not Flow on a Cisco ASA G500 Series firewall? (Choose three)

A. Apply the newly created class map to the global policy.

B. Enable NetFlow Version 9.

C. Create a class map match interesting traffic.

D. Create an ACL to allow UDP traffic on port 9996.

E. Define a NetFlow collector by using the flow-export command.

F. Apply NetFlow Exporter to the outside interface in the inbound direction

Correct Answer: ACE

QUESTION 2

Refer to the exhibit. Which two statements about this firewall output are true? (Choose two.)

A. The output is from a packet tracer debug.

B. All packets are allowed to 192.168.1.0 255.255.0.0.

C. All packets are allowed to 192.168.1.0 255.255.255.0.

D. All packets are denied.

E. The output is from a debug all command.

Correct Answer: AC

QUESTION 3

Which feature is a limitation of a Cisco ASA 5555-X running 8.4.5 version with multiple contexts?

A. Deep packet inspection

B. Packet tracer

C. IPsec

D. Manual/auto NAT

E. Multipolicy packet capture

Correct Answer: C

QUESTION 4

CSM (or Prime Infra) Dashboards

Report Name	Drill-down Reports Shown
Firewall	
Top Sources	Top Destinations, Top Services
Top Destinations	Top Sources, Top Services
Top Services	Top Sources, Top Destinations
IPS	
Top Signatures	Top Attackers, Top Victims
Top Attackers	Top Signatures, Top Victims
Top Victims	Top Signatures, Top Attackers

Correct Answer:

Top Destinations --This report ranks the session destinations of all built/deny firewall events received by Security Manager. The report shows the destination IP address, the count of the number of events for each address, and the percentage

of the count compared to the sum of all counts in the report. You can click on a data point in the Pie, XY, or Bar graph that represents a specific destination to see report information about the top sources and top services associated with that

destination (see Drilling Down into Report Data).

Top Sources --This report ranks the session sources of all built/deny firewall events received by Security Manager. The report shows the source IP address, the count of the number of events for each address, and the percentage of the count

compared to the sum of all counts in the report. You can click on a data point in the Pie, XY, or Bar graph that represents a specific source to see report information about the top destinations and top services associated with that source (see

Drilling Down into Report Data).

Top Services --This report ranks the destination services of all built/deny firewall events received by Security Manager. TCP and UDP services include the port number. The report shows the service, the count of the number of events for each

service, and the percentage of the count compared to the sum of all counts in the report. You can click on a data point in the Pie, XY, or Bar graph that represents a specific service to see report information about the top destinations and top

sources associated with that service (see Drilling Down into Report Data).

Top Infected Hosts --This report ranks the top infected hosts for traffic originating from infected hosts to black- or gray-listed sites based on all botnet events received by Security Manager. The report shows the IP address of the infected host

with the firewall interface name on which the event was detected in parentheses, the count of the number of connections logged to blacklisted or gray-listed sites for each address, the count of the number of connections that were blocked

(dropped) by botnet traffic filtering, and the percentage of the count compared to the sum of all counts in the report.

Top Malware Ports --This report ranks the top destination ports for traffic originating from infected hosts to black or gray-listed sites based on all botnet events received by Security Manager. The report shows the destination malware port, the

count of the number of connections logged to blacklisted or gray-listed sites for each port, the count of the number of connections that were blocked (dropped) by botnet traffic filtering, and the percentage of the count compared to the sum of

all counts in the report.

Top Malware Sites --This report ranks the top botnet sites (black or gray-listed sites) for all inbound and outbound sessions based on all botnet events received by Security Manager. The report shows the following information:

IP Address--The IP address that is indicated as the malicious host in botnet events, either on the black list or the grey list.

Malware Site--The domain name or IP address in the dynamic filter database to which the traffic was initiated.

List Type--Whether the site is on the black list or the grey list. Connections Logged--The count of the number of connections logged or monitored for each site. Connections Blocked--The count of the number of connections that were blocked

(dropped) by botnet traffic filtering for each site. Threat Level--The botnet threat level for the site, from very low to very high, or none. Category--The category of threat the site poses as defined in the botnet database, such as botnet, Trojan,

spyware, and so on.

VPN dashboards

Top Bandwidth Users --This report ranks the VPN users who consumed the most bandwidth. The report shows the usernames, the bandwidth in total number of bytes sent and received, and the percentage of reported bandwidth used by

each user.

Top Duration Users --This report ranks the VPN users who remained connected to the network for the longest time. The report shows the usernames, the connection duration time in days hours:minutes:seconds format, and the percentage of

the reported duration by each user.

The chart shows duration in seconds.

Top Throughput Users --This report ranks the VPN users who sent and received data at the highest throughput rate. The report shows the usernames, the throughput for each user in kbps, and the percentage of reported throughput by each

user. The throughput is calculated as 8.0 *(bandwidth of the user in bytes)/(duration for which the user is connected in seconds*1000.0).

Connection Profile Report --This report provides a count of user, session, and summary of the bandwidth utilization and throughput usage for each remote access connection profile. The default report contains this information for all devices

for the previous hour. You can customize the report in several different ways.

User Report --This report provides a summary of the bandwidth utilization, connection duration and throughput usage for each remote access VPN user. The report shows the usernames, the bandwidth in total number of bytes sent and

received, the connection duration time in days hours:minutes:seconds format, and the throughput for each user in kbps. The throughput is throughput is calculated as 8.0*(bandwidth of the user in bytes)/(duration for which the user is

connected in seconds*1000.0). Beginning with Security Manager 4.7, the User Report provides both user-level details and session-level details:

User-Level Details --For a particular user, the user-level details represent the combined value of all that user\\'s sessions: Username, Total no. of Sessions, Bandwidth, Duration, and Throughput. Session-Level Details --Expanding the tree

displays the session-level details for each session that a particular user has a VPN connection with; the session-level details encompass the Session ID, Login Time, Logout Time, Bandwidth, Throughput, and Duration of the Session. (Here

the logout time is calculated by using the formula Logout Time = Login Time + Duration.)

QUESTION 5

What are Options of capture command

A. host

B. real-time

C. type

Correct Answer: BC

real-time, type, interface,buffer, match, packet-lenght,trace,circular-buffer, ethernet-type,acces-list, headers-only