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.certbus.com/300-206.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Which command is used to nest objects in a pre-existing group?

A. object-group

B. network group-object

C. object-group network

D. group-object

Correct Answer: D

QUESTION 2

How much storage is allotted to maintain system,configuration , and image files on the Cisco ASA 1000V during OVF template file deployment?

A. 1GB

B. 5GB

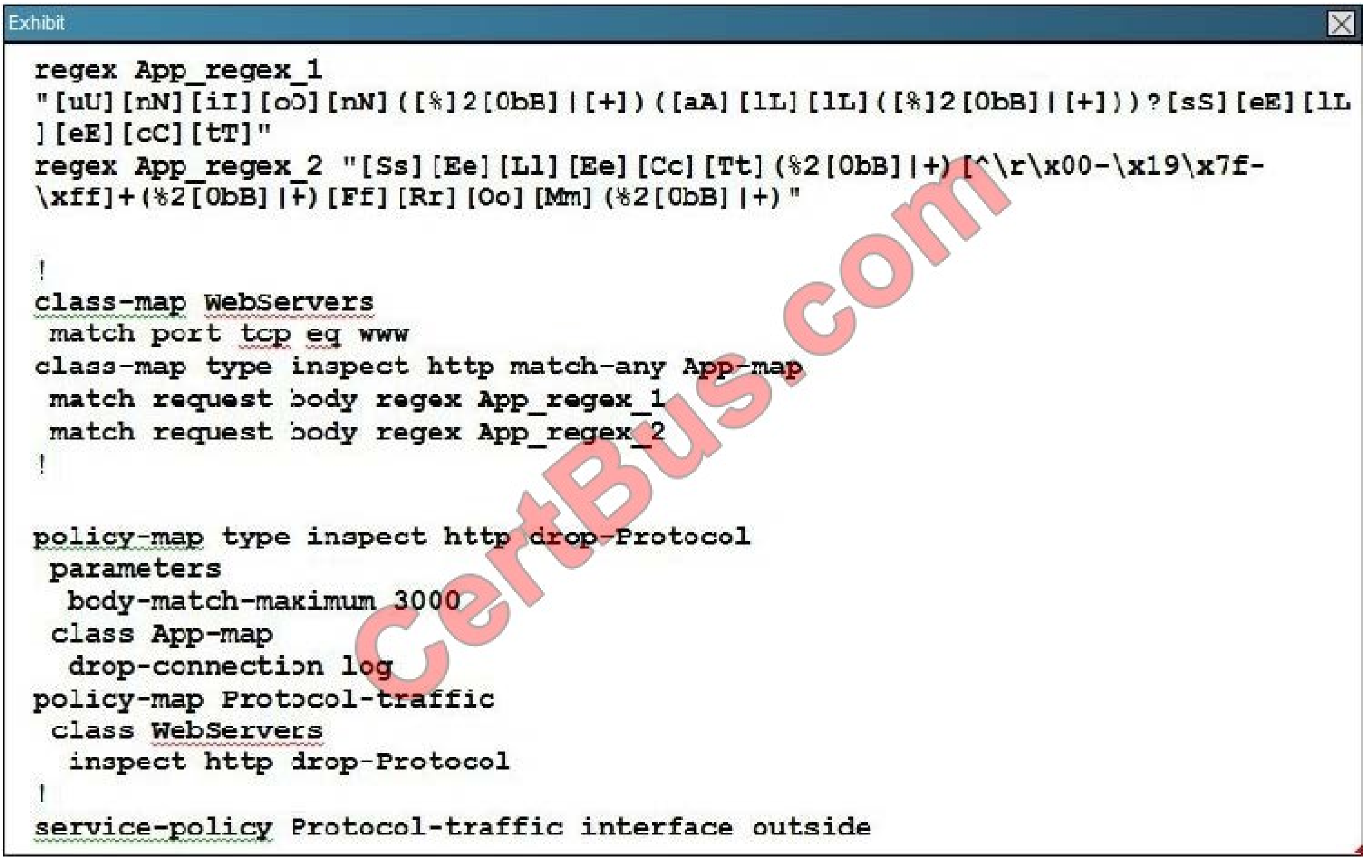
C. 2GB

D. 10GB

Correct Answer: C

QUESTION 3

Refer to the exhibit. What type of attack is being mitigated on the Cisco ASA appliance?



```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%]2[0bB]|[+])([aA][lL][lL]([%]2[0bB]|[+]))?[sS][eE][lL
][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB]|+)[^\r\x00-\x19\x7f-
\xff]+(%2[0bB]|+)[Ff][Rr][Oo][Mm](%2[0bB]|+)"

!
class-map WebServers
 match port tcp eq www
class-map type inspect http match-any App-map
 match request body regex App_regex_1
 match request body regex App_regex_2
!

policy-map type inspect http drop-Protocol
 parameters
  body-match-maximum 3000
 class App-map
  drop-connection log
policy-map Protocol-traffic
 class WebServers
  inspect http drop-Protocol
!
service-policy Protocol-traffic interface outside
```

CertBus.com

A. HTTP and POST flood attack

B. HTTP Compromised-Key Attack

C. HTTP Shockwave Flash exploit

D. HTTP SQL injection attack

Correct Answer: D

QUESTION 4

Which option describes the purpose of the input parameter when you use the packet-tracer command on a Cisco device?

A. to provide detailed packet-trace information

B. to specify the source interface for the packet trace

C. to display the trace capture in XML format

D. to specify the protocol type for the packet trace

Correct Answer: B

QUESTION 5

An engineer must secure a current monitoring environment by using the strongest encryption allowed within SNMPv3 configuration. Which two encryption methods meet this requirement? (Choose two.)

A. 3DES

B. AES

C. RSA-SIG

D. DES

E. MD5

Correct Answer: AB

QUESTION 6

Which statement about Cisco ASA NetFlow v9 (NSEL) is true?

A. NSEL events match all traffic classes in parallel

B. NSEL is has a time interval locked at 20 seconds and is not user configurable

C. NSEL tracks flow-create, flow-teardown, and flow-denied events and generates appropriate NSEL data records

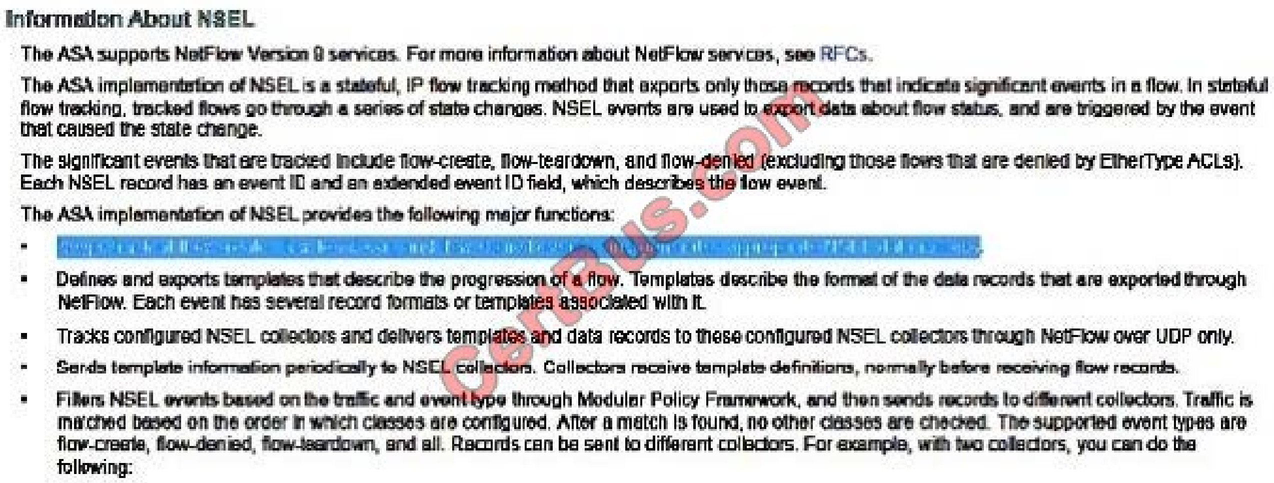
D. You cannot disable syslog messages that have become redundant because of NSEL

E. NSEL tracks the flow continuously and provides updates every 10 second

F. NSEL provides stateless IP flow tracking that exports all record od a specific flow

Correct Answer: C

http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_nsel.html



Information About NSEL

The ASA supports NetFlow Version 9 services. For more information about NetFlow services, see RFCs.

The ASA implementation of NSEL is a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status, and are triggered by the event that caused the state change.

The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). Each NSEL record has an event ID and an extended event ID field, which describes the flow event.

The ASA implementation of NSEL provides the following major functions:

- [illegible]
- Defines and exports templates that describe the progression of a flow. Templates describe the format of the data records that are exported through NetFlow. Each event has several record formats or templates associated with it.
- Tracks configured NSEL collectors and delivers templates and data records to these configured NSEL collectors through NetFlow over UDP only.
- Sends template information periodically to NSEL collectors. Collectors receive template definitions, normally before receiving flow records.
- Filters NSEL events based on the traffic and event type through Modular Policy Framework, and then sends records to different collectors. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked. The supported event types are flow-create, flow-denied, flow-teardown, and all. Records can be sent to different collectors. For example, with two collectors, you can do the following:

CertBus.com

QUESTION 7

A Cisco ASA is configured in multiple context mode and has two user-defined contexts-- Context_A and Context_B. From which context are device logging messages sent?

A. Admin

B. Context_A

C. Context_B

D. System

Correct Answer: A

QUESTION 8

What configuration can affect snmp-server ID modification?

A. Earlier snmp configuration

B. Earlier snmp group

C. Earlier snmp user

D. SNMP is disabled

E. SNMP is set to version 3

Correct Answer: C

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the

command snmp-server engineID with the remote option.

The remote agent\\'s SNMP engine ID is needed when computing the authentication/privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

QUESTION 9

ACL config exibit:

-Shows an ACL called OUTSIDE-IN controlling whether IPSEC connections are allowed

-ACL has permits on it to allow IPSEC connections to and from an inside network address of 10.10.10.x to an outside IP of 198.x.x.x along with some explicit denies -Shows the ACL being applied to the outside interface using something like:

access-group OUTSIDE-IN in interface outside control-plane

Which direction is traffic inspected on the interface

A. Controling IP traffic from the outside interface

B. Controling IPsec traffic from the outside interface

C. Controling IP traffic to the outside interface

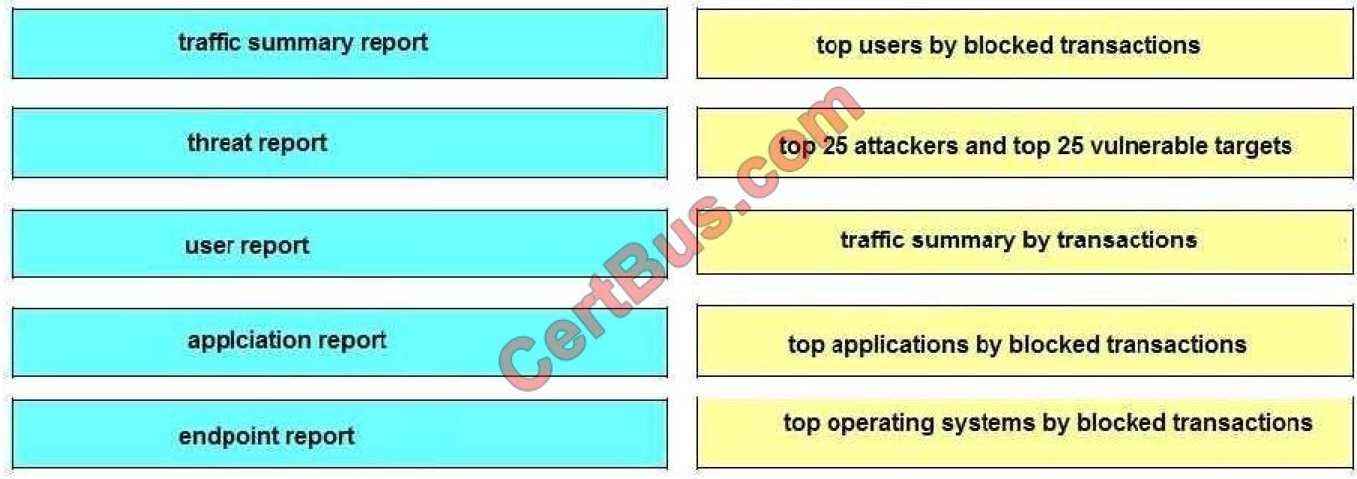
D. Controling IPsec traffic to the outside interface

Correct Answer: D

QUESTION 10

Drag and drop the Cisco Prime Security Manager available reports on the left onto the correct report examples on the right.

Select and Place:



traffic summary report

threat report

user report

applciation report

endpoint report

top users by blocked transactions

top 25 attackers and top 25 vulnerable targets

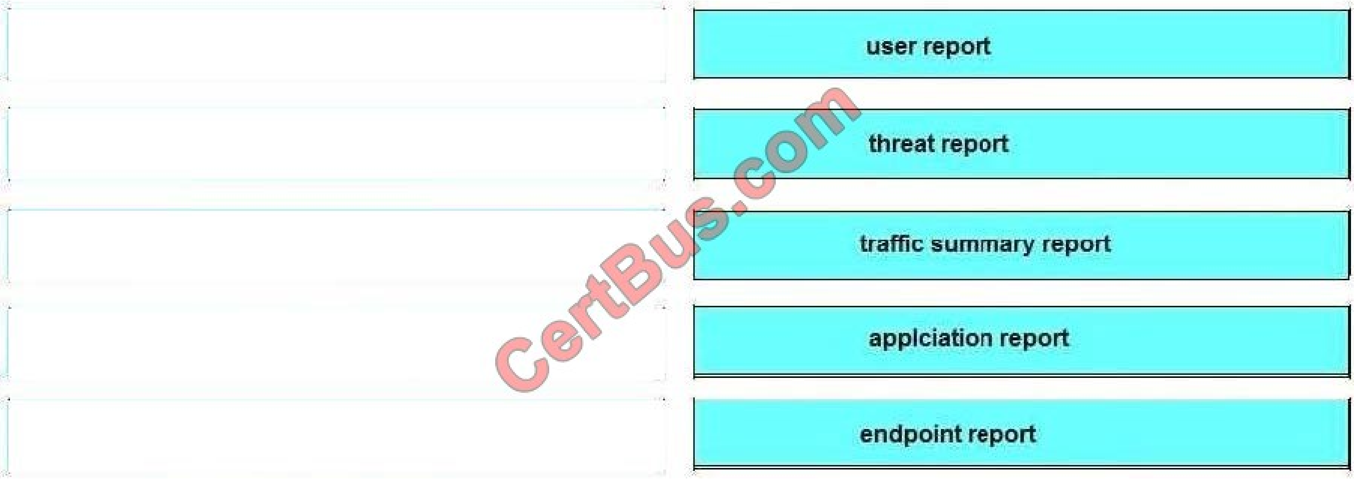
traffic summary by transactions

top applications by blocked transactions

top operating systems by blocked transactions

CertBus.com

Correct Answer:



user report

threat report

traffic summary report

applciation report

endpoint report

CertBus.com

QUESTION 11

Which two statements about the utilization of IPv4 and IPv6 addresses in the Cisco ASA 9.x firewall access list configuration are true? (Choose two.)

A. Mixed IPv4 and IPv6 addresses cannot be used in the same access list entry

B. Mixed IPv4 and IPv6 addresses can be used in the same access list entry

C. Mixed IPv4 and IPv6 addresses can be used in the same access list for network object group

D. Mixed IPv4 and IPv6 addresses cannot be used in the same access list

E. Mixed IPv4 and IPv6 addresses cannot be used in the same access list for network object group

Correct Answer: BC

QUESTION 12

Which command in ASA allows ASDM connection from client PC over https with the Local AAA user database?

A. aaa authentication enable console LOCAL

B. aaa authentication http console LOCAL

C. aaa authentication ssh console LOCAL

D. aaa authentication Telnet console LOCAL

Correct Answer: B

300-206 PDF Dumps 300-206 Study Guide 300-206 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

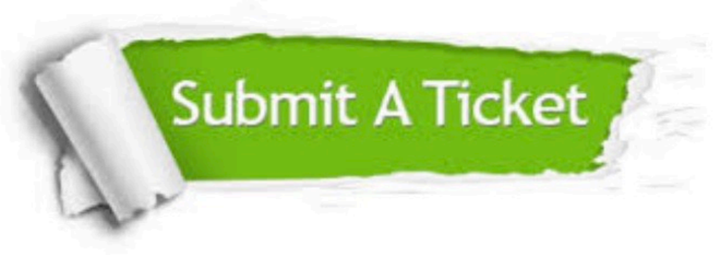
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.certbus.com/allproducts

Need Help

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



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.

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.

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.

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