300-206 Q&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.passapply.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

What are mandatory policies needed to support IPSec VPN in CSM environment? (Choose two)

A. IKE Proposal

B. Group encryption

C. IPSec Proposal

D. GRE modes

E. Server load balance

Correct Answer: AC

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs). The IKE negotiation

comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec.

Both phases use proposals when they negotiate a connection.

An IKE proposal is a set of algorithms that two peers use to secure the IKE negotiation between them.

IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. For IKE version 1 (IKEv1), IKE proposals contain a single set

of algorithms and a modulus group. You can create multiple, prioritized policies at each peer to ensure that at least one policy matches a remote peer\\'s policy. Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and

modulus groups from which peers can choose during the Phase 1 negotiation, potentially making it possible to create a single IKE proposal (although you might want different proposals to give higher priority to your most desired options). You

can define several IKE proposals per VPN.

An IPsec proposal is used in Phase 2 of an IKE negotiation. The specific content of the proposal varies according to topology type (site-to-site or remote access) and device type, although the proposals are broadly similar and contain many of

the same elements, such as IPsec transform sets.

QUESTION 2

What is the result of the default ip ssh server authenticate user command?

A. It enables the public key, keyboard, and password authentication methods.

B. It enables the public key authentication method only.

C. It enables the keyboard authentication method only.

D. It enables the password authentication method only.

Correct Answer: A

QUESTION 3

If you disable PortFast on switch ports that are connected to a Cisco ASA and globally turn on BPDU filtering, what is the effect on the switch ports?

A. The switch ports are prevented from going into an err-disable state if a BPDU is received.

B. The switch ports are prevented from going into an err-disable state if a BPDU is sent.

C. The switch ports are prevented from going into an err-disable state if a BPDU is received and sent.

D. The switch ports are prevented from forming a trunk.

Correct Answer: C

QUESTION 4

A router is being enabled for SSH command line access. The following steps have been taken:

- The vty ports have been configured with transport input SSH and login local.

-Local user accounts have been created.

-The enable password has been configured.

What additional step must be taken if users receive a \\'connection refused\\' error when attempting to access the router via SSH?

A. A RSA keypair must be generated on the router

B. An access list permitting SSH inbound must be configured and applied to the vty ports

C. An access list permitting SSH outbound must be configured and applied to the vty ports

D. SSH v2.0 must be enabled on the router

Correct Answer: A

QUESTION 5

Where in the Cisco ASA appliance CLI are Active/Active Failover configuration parameters configured?

A. admin context

B. customer context

C. system execution space

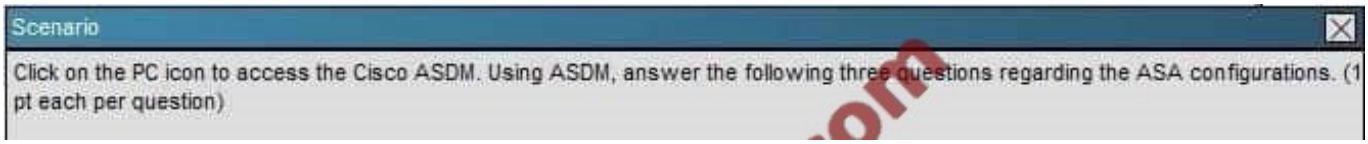
D. within the system execution space and admin context

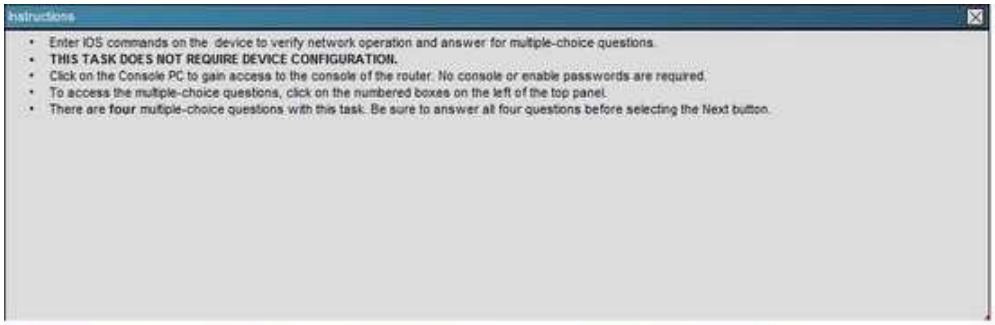
E. within each customer context and admin context

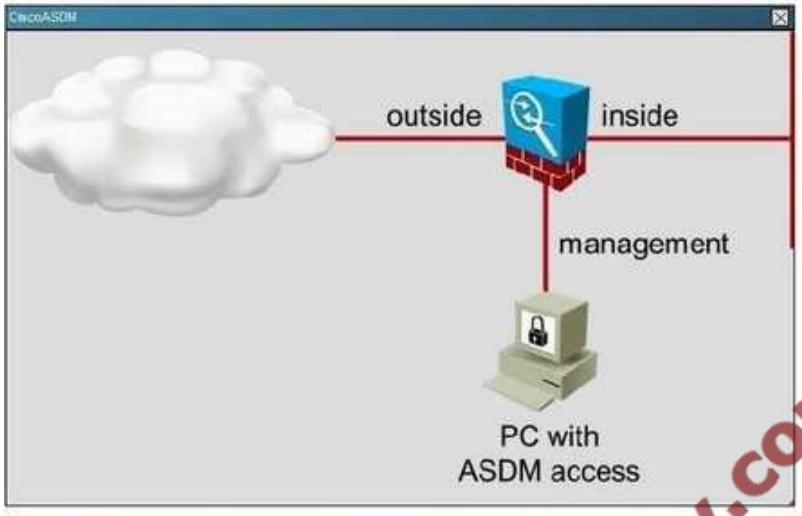
Correct Answer: C

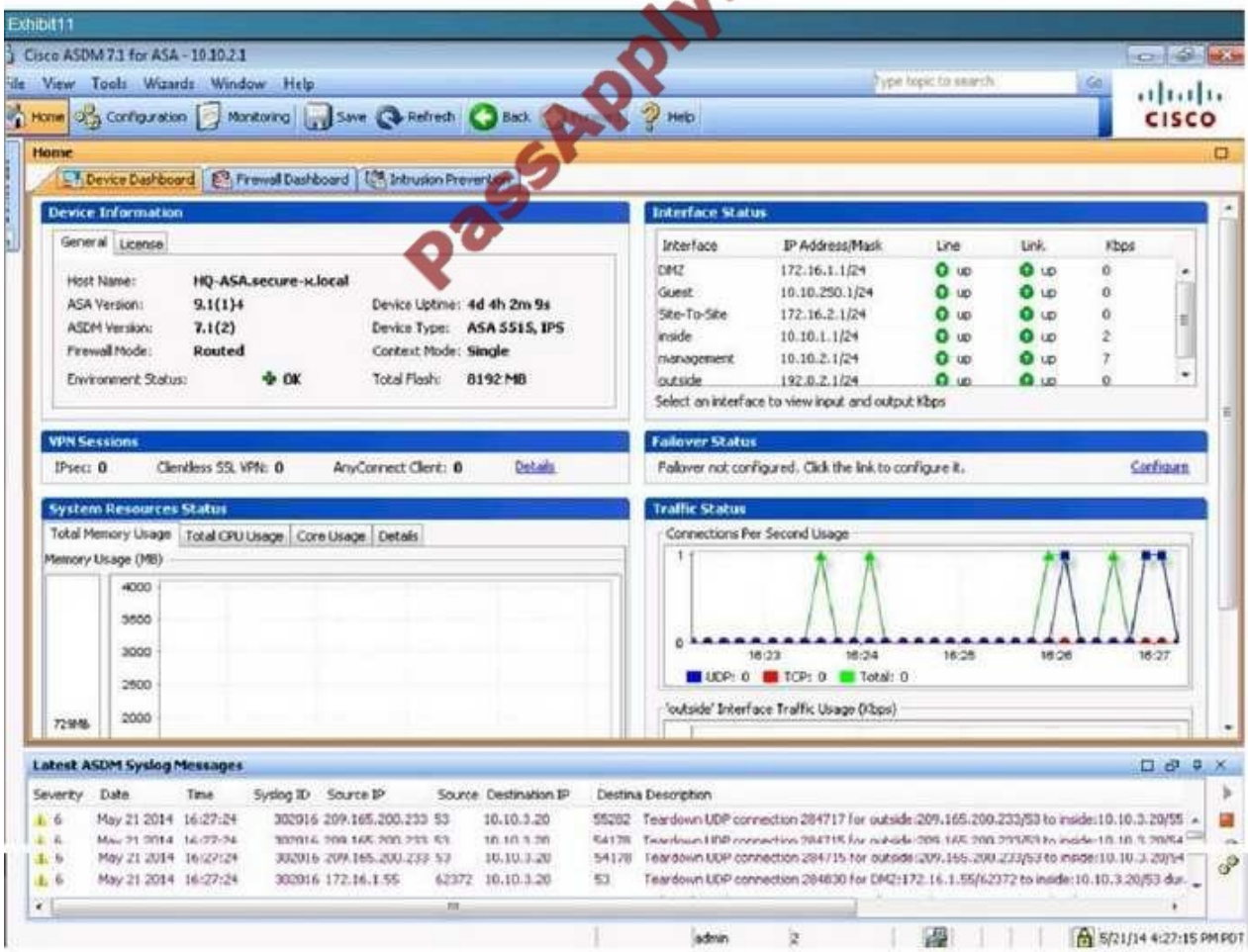
QUESTION 6

Hotspot Question









According to the logging configuration on the Cisco ASA, what will happen if syslog server 10.10.2.40 fails?

A. New connections through the ASA will be blocked and debug system logs will be sent to the internal buffer.

B. New connections through the ASA will be blocked and informational system logs will be sent to the internal buffer.

C. New connections through the ASA will be blocked and system logs will be sent to server 10.10.2.41.

D. New connections through the ASA will be allowed and system logs will be sent to server 10.10.2.41.

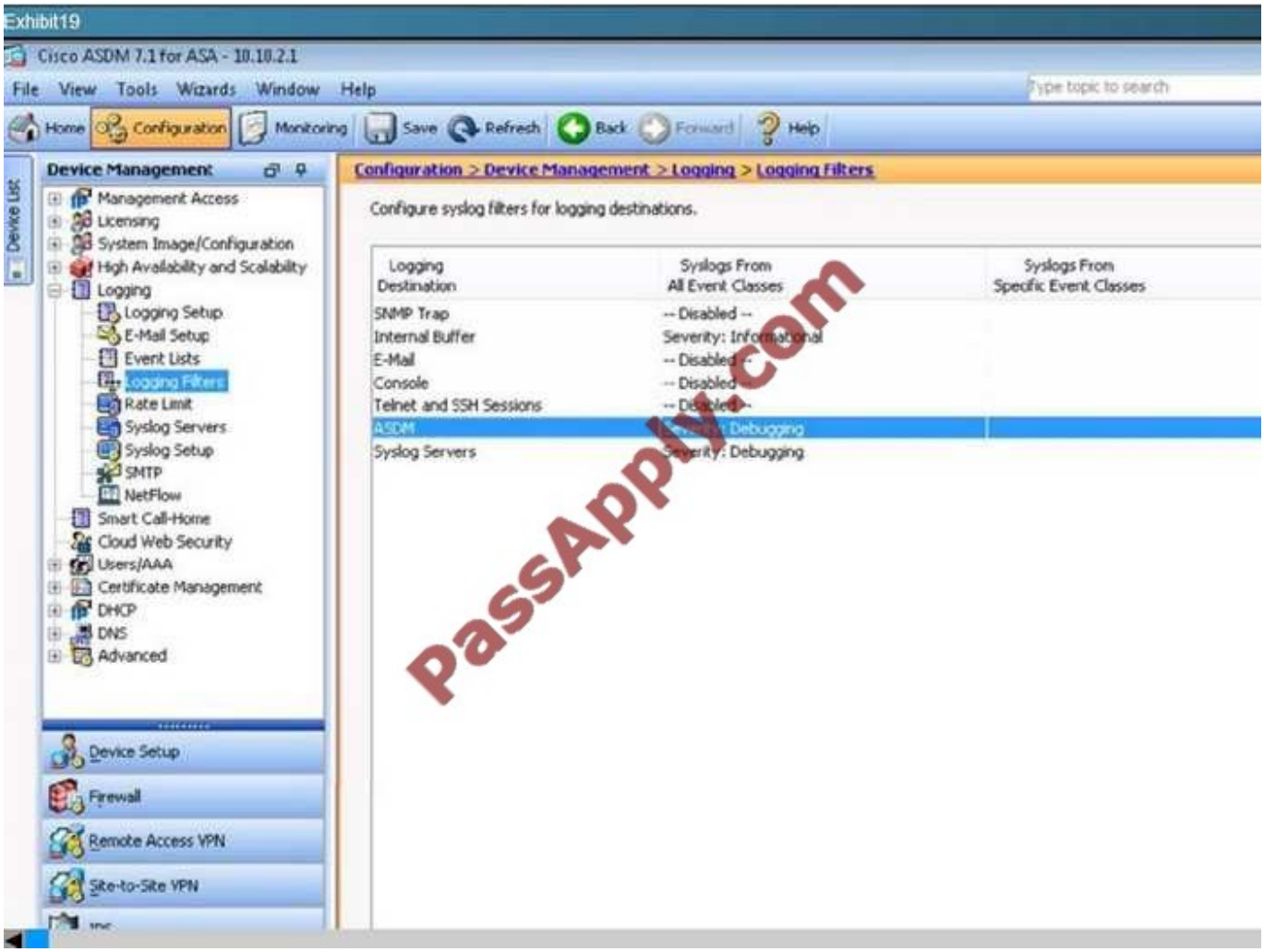
E. New connections through the ASA will be allowed and informational system logs will be sent to the internal buffer.

F. New connections through the ASA will be allowed and debug system logs will be sent to the internal buffer.

Correct Answer: E

Connections are blocked only if the syslog server uses TCP. Here, it uses UDP. Also, the logging filters screen shows `informational\\' for the Internal Buffer destination.

This is shown by the following screen shot:



QUESTION 7

A network engineer is troubleshooting and configures the ASA logging level to debugging. The logging-buffer is dominated by %ASA-6-305009 log messages. Which command suppresses those syslog messages while maintaining ability to troubleshoot?

A. no logging buffered 305009

B. message 305009 disable

C. no message 305009 logging

D. no logging message 305009

Correct Answer: D

QUESTION 8

Host cannot communicate with server. Traffic goes through ASA. Which cli command can confirm if ASA is blocking traffic or not?

A. Capture

Correct Answer: A

QUESTION 9

Which threat-detection feature is used to keep track of suspected attackers who create connections to too many hosts or ports?

A. complex threat detection

B. scanning threat detection

C. basic threat detection

D. advanced threat detection

Correct Answer: B

QUESTION 10

When creating a cluster of Cisco ASA firewalls, which feature is configured on the cluster, instead of being applied to each Cisco ASA unit?

A. OSPF routing

B. URL filtering

C. HTTPS inspection

D. resource management

Correct Answer: B

See "Centralized Features" section on
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_cluster.html#62546

QUESTION 11

There was installed some product (don\\'t remember which one) on Windows server 2008 SP1. Why is product from time to time crashing?

A. Memory needs to be upgraded to 16GB of RAM

Correct Answer: A

QUESTION 12

It has been reported that an application is not working where an ASA is inline with the data path. Which command can be used to confirm or deny if the ASA is responsible for this issue?

A. test

B. packet-tracer

C. capture

D. perfmon

E. verify

Correct Answer: B

In addition to capturing packets, it is possible to trace the lifespan of a packet through the ASA to see if it is behaving as expected.

The packet-tracer command enables you to do the following:

Debug all packet drops in production network.

Verify the configuration is working as intended.

Show all rules applicable to a packet along with the CLI lines that caused the rule addition.

Show a time line of packet changes in a data-path.

Inject tracer packets into the data-path.

Search for an IPv4 or IPv6 address based on the user identity and the FQDN. The packet-tracer command provides detailed information about the packets and how they are processed by the ASA. Packet-tracer allows a firewall administrator to inject a virtual packet into the security appliance and track the flow from ingress to egress. Along the way, the packet is evaluated against flow and route lookups, ACLs, protocol inspection, NAT, and IDS. The power of the utility comes from the ability to simulate real-world traffic by specifying source and destination addresses with protocol and port information. http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2/p1.html

QUESTION 13

What is the best practice about storm control - where to implement?

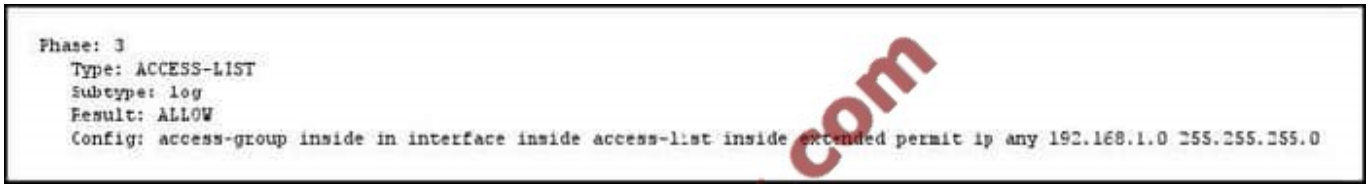
A. PortChannel

B. interfaces of that Po

Correct Answer: A

QUESTION 14

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 15

Which addresses are considered "ambiguous addresses" and are put on the greylist by the Cisco ASA botnet traffic filter feature?

A. addresses that are unknown

B. addresses that are on the greylist identified by the dynamic database

C. addresses that are blacklisted by the dynamic database but also are identified by the static whitelist

D. addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist

Correct Answer: D

QUESTION 16

Which three statements about private VLANs are true? (Choose three.)

A. Isolated ports can talk to promiscuous and community ports.

B. Promiscuous ports can talk to isolated and community ports.

C. Private VLANs run over VLAN Trunking Protocol in client mode.

D. Private VLANS run over VLAN Trunking Protocol in transparent mode.

E. Community ports can talk to each other as well as the promiscuous port.

F. Primary, secondary, and tertiary VLANs are required for private VLAN implementation.

Correct Answer: BDE

QUESTION 17

If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

A. STP bpdu guard

B. STP root guard

C. SPT bpdu filter

Correct Answer: B

QUESTION 18

What is the primary purpose of stateful pattern recognition in Cisco IPS networks?

A. mitigating man-in-the-middle attacks

B. using multipacket inspection across all protocols to identify vulnerability-based attacks and to thwart attacks that hide within a data stream

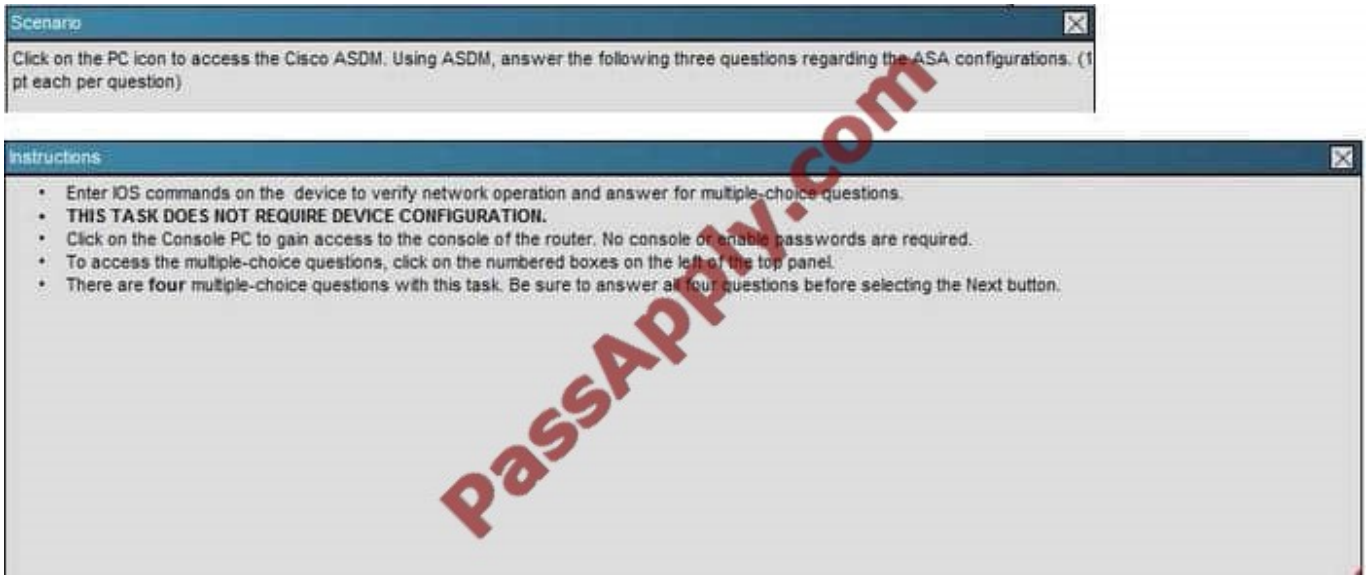
C. detecting and preventing MAC address spoofing in switched environments

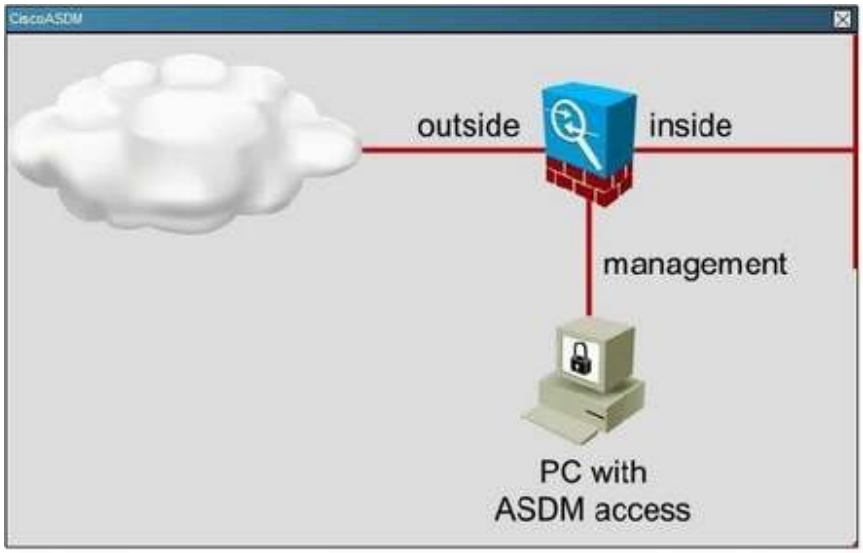
D. identifying Layer 2 ARP attacks

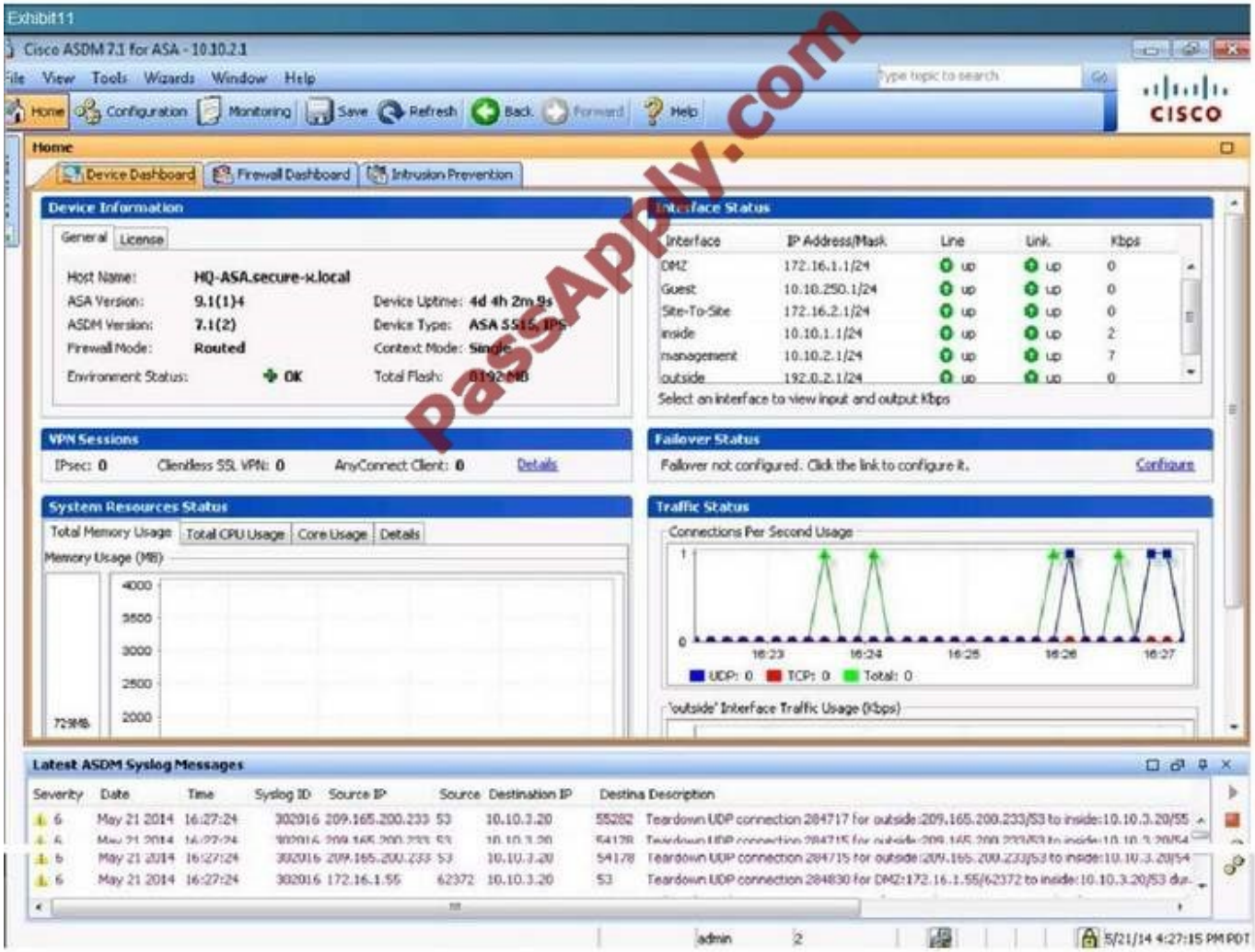
Correct Answer: B

QUESTION 19

Hotspot Question In your role as network security administrator, you have installed syslog server software on a server whose IP address is 10.10.2.40. According to the exhibits, why isn\\'t the syslog server receiving any syslog messages?







A. Logging is not enabled globally on the Cisco ASA.

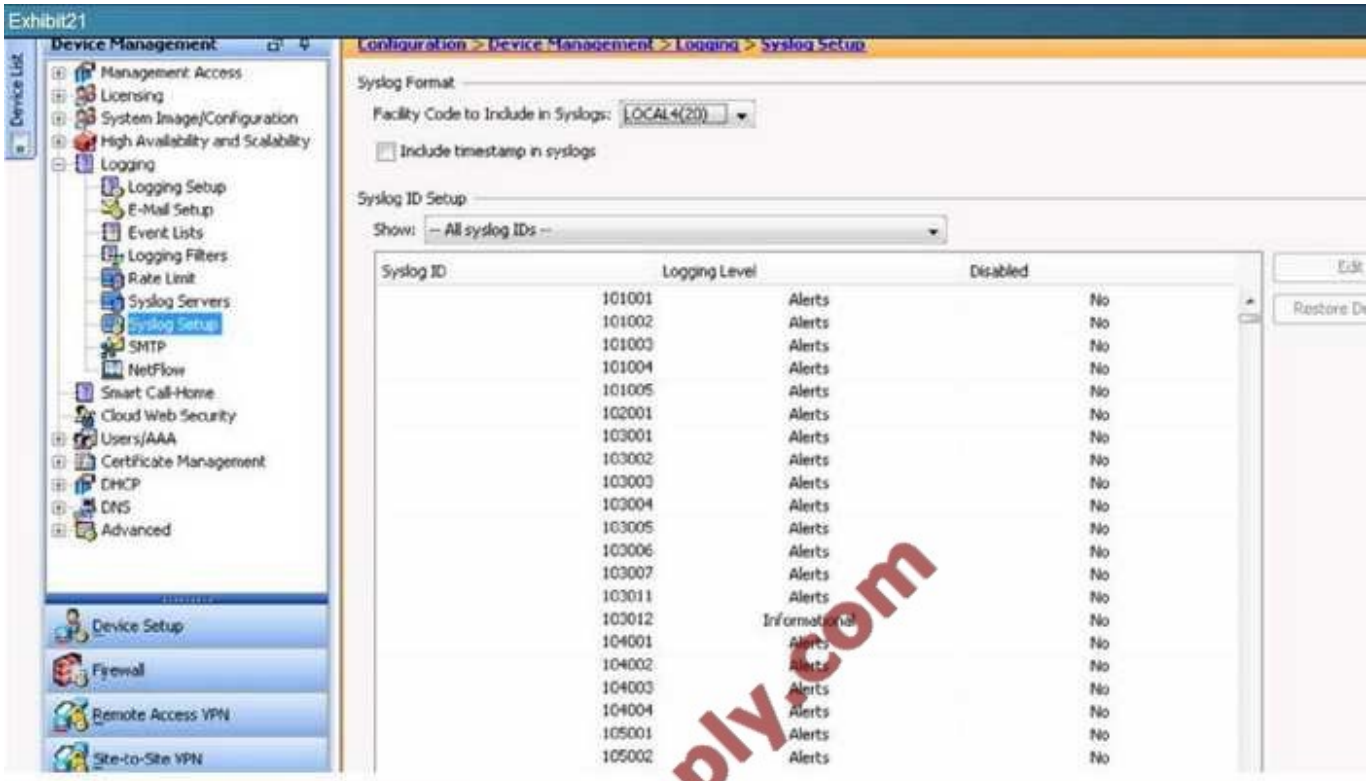
B. The syslog server has failed.

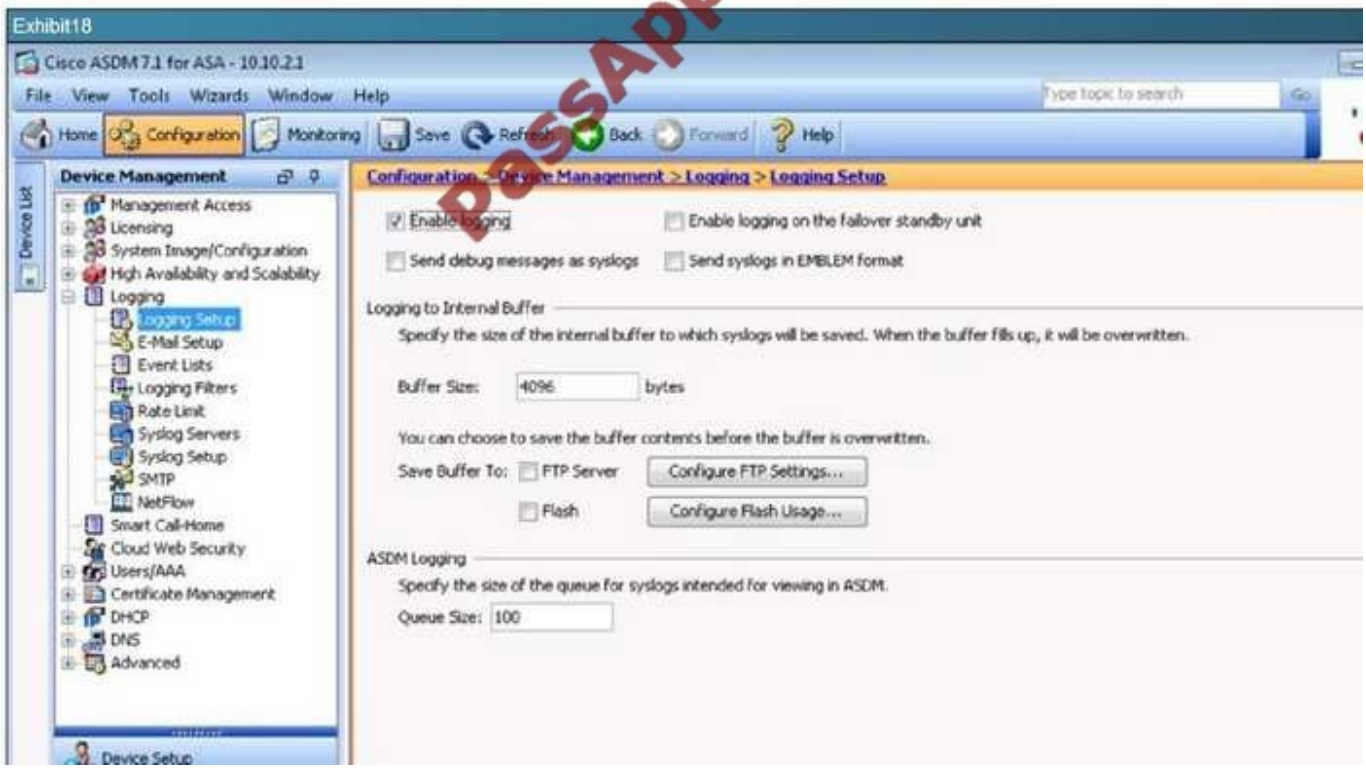
C. There have not been any events with a severity level of seven.

D. The Cisco ASA is not configured to log messages to the syslog server at that IP address.

Correct Answer: D

By process of elimination, we know that the other answers choices are not correct so that only leaves us with the server must have failed. We can see from the following screen shots, that events are being generated with severity level of debugging and below, The 10.10.2.40 IP address has been configured as a syslog server, and that logging has been enabled globally:





QUESTION 20

What is the default log level on the Cisco Web Security Appliance?

A. Trace

B. Debug

C. Informational

D. Critical

Correct Answer: C

QUESTION 21

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

A. To view bandwidth usage for the NetFlow record, you must enable QoS features

B. Use sysopt command to enable NSEL on a specific interface

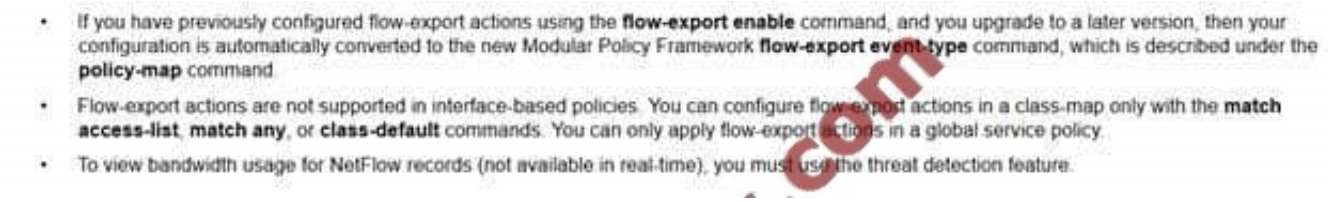
C. NSEL can be used without a collector configured

D. NSEL tracks the flow continuously and provides updates every 10 seconds

E. You must define a flow-export event type under a policy

Correct Answer: E

http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html


- If you have previously configured flow-export actions using the **flow-export enable** command, and you upgrade to a later version, then your configuration is automatically converted to the new Modular Policy Framework **flow-export event-type** command, which is described under the **policy-map** command.
- Flow-export actions are not supported in interface-based policies. You can configure flow-export actions in a class-map only with the **match access-list**, **match any**, or **class-default** commands. You can only apply flow-export actions in a global service policy.
- To view bandwidth usage for NetFlow records (not available in real-time), you must use the threat detection feature.

QUESTION 22

How does the DAI works? (Choose two)

A. DAI relies on DHCP snooping.

B. It is applied on configured untrusted interfaces

C. IP address binding stored in trusted database

D. User-configured ARP ACLs

Correct Answer: AB

QUESTION 23

Which two option are protocol and tools are used by management plane when using cisco ASA general management

plane hardening ?

A. Unicast Reverse Path Forwarding

B. NetFlow

C. Routing Protocol Authentication

D. Threat detection

E. Syslog

F. ICMP unreachables

G. Cisco URL Filtering

Correct Answer: BE

http://www.cisco.com/web/about/security/intelligence/firewall-best-practices.html

QUESTION 24

Control plane thresholding limit for which protocols

A. ICMP

B. BGP

C. ARP

Correct Answer: B

The queue-thresholding feature policy supports the following TCP/UDP-based protocols:
Bgp,dns,ftp,http,igmp,snmp,ssh,syslog,telnet,Tftp,host-protocols

QUESTION 25

Which command tests authentication with SSH and shows a generated key?

A. show key mypubkey rsa

B. show crypto key mypubkey rsa

C. show crypto key

D. show key mypubkey

Correct Answer: B

QUESTION 26

Which three options are default settings for NTP parameters on a Cisco ASA? (Choose three.)

A. NTP authentication is enabled.

B. NTP authentication is disabled.

C. NTP logging is enabled.

D. NTP logging is disabled.

E. NTP traffic is not restricted.

F. NTP traffic is restricted.

Correct Answer: BDE

QUESTION 27

Cisco Security Manager can manage which three products? (Choose three.)

A. Cisco IOS

B. Cisco ASA

C. Cisco IPS

D. Cisco WLC

E. Cisco Web Security Appliance

F. Cisco Email Security Appliance

G. Cisco ASA CX

H. Cisco CRS

Correct Answer: ABC

QUESTION 28

Which statement about the Cisco Security Manager 4.4 NAT Rediscovery feature is true?

A. It provides NAT policies to existing clients that connect from a new switch port.

B. It can update shared policies even when the NAT server is offline.

C. It enables NAT policy discovery as it updates shared polices.

D. It enables NAT policy rediscovery while leaving existing shared polices unchanged.

Correct Answer: D

QUESTION 29

Configuration of SSH on ASA

Ip ssh version 2	Ssh version 2
Enable password <password>	Enable password for SSH
Username <username> password <password>	Username and password for SSH
crypto key generate rsa modulus 1024	Generate SSH key
aaa authentication ssh console LOCAL	Enable AAA for SSH
ssh 192.168.1.0 255.255.255.0 trust	Access host for SSH
Ip domain-name	Create host domain for SSH

Correct Answer: explanation

Cisco ASA correction:

domain-name

crypto key generate rsa modulus

ssh version 2

enable password

username password

aaa authentication ssh console LOCAL

ssh

Cisco IOS correction:

domain-name

crypto key generate rsa modulus

ip ssh version 2

enable secret 0

username secret 0

aaa new-model

aaa authentication login default local-case enable

line vty 0 4

transport input ssh

login authentication default

QUESTION 30

Where to apply security policies on Nexus1000V for group of VMs instead of applying it directly on interface?

A. port group

B. port profile

C. security group

D. security profile

Correct Answer: B

Security policies can be applied to port profile in ASDM or VNMC. Port profiles represent port groups that are configured in Nexus 1000V environment.

QUESTION 31

Which ASA feature is used to keep track of suspected attackers who create connections to too many hosts or ports?

A. complex threat detection

B. scanning threat detection

C. basic threat detection

D. advanced threat detection

Correct Answer: B

QUESTION 32

What statements are true about IPv4 and IPv6 addresses on the ASA, which options are true? (Choose 2)

A. IPv4 and IPv6 IPs can be included in the same ACL

B. IPv4 and IPv6 IPs can not be included in the same ACL

C. IPv4 and IPv6 IPs can be added in the same Object group

D. IPv4 and IPv6 IPs can not be added in the same Object group

Correct Answer: AC

QUESTION 33

Which three Cisco ASA configuration commands are used to enable the Cisco ASA to log only the debug output to syslog? (Choose three.)

A. logging list test message 711001

B. logging debug-trace

C. logging trap debugging

D. logging message 711001 level 7

E. logging trap test

Correct Answer: ABE

QUESTION 34

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 35

Which two commands can be used to create a Cisco Unified ACL within the ASA CLI? (Choose two.)

A. ipv6 access-list

B. object-group network

C. ipv6 access-list webtype

D. access-list extended

E. object-group network nat-pat-grp

Correct Answer: BD

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/acl_extended.pdf

QUESTION 36

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 37

You need to group similar VMs together to classify traffic on the cisco ASA 1000V. Which command would you use?

A. network-port

B. network-profile

C. security-port

D. security-profile

Correct Answer: D

https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/asa1000V/1000V_get_start/before.html#wp1066087

QUESTION 38

What can you do to enable inter-interface firewall communication for traffic that flows between two interfaces of the same security level?

A. Run the command same-security-traffic permit inter-interface globally.

B. Run the command same-security-traffic permit intra-interface globally.

C. Configure both interfaces to have the same security level.

D. Run the command same-security-traffic permit inter-interface on the interface with the highest security level.

Correct Answer: A

QUESTION 39

Prior to a software upgrade, which Cisco Prime Infrastructure feature determines if the devices being upgraded have sufficient RAM to support te new software ?

A. Software Upgrade Report

B. Image Management Report

C. Upgrade Analysis Report

D. Image Analysis Report

Correct Answer: C

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/maint_images.html

Analyzing Software Image Upgrades

Prime Infrastructure can generate an Upgrade Analysis report to help you determine prerequisites for a new software image deployment. These reports analyze the software images to determine the hardware upgrades (boot ROM, flash memory, RAM, and boot flash, if applicable) required before you can perform the software upgrade.

The Upgrade Analysis report answers the following questions:

- Does the device have sufficient RAM to hold the new software?
- Is the device's flash memory large enough to hold the new software?

To analyze software image upgrades:

QUESTION 40

Private VLANs have been configured in the data center. Which type of Private VLAN port would allow a new server to communicate with all other interfaces?

A. shared

B. private

C. isolated

D. promiscuous

E. community

Correct Answer: D