

Cisco 642-974

Data Center Network Infrastructure Support – 2
Version: 4.2

QUESTION NO: 1

How would you configure a NAM to monitor and report the most heavily viewed sections of a website?

- A.** Create a separate domain name or virtual server IP address for each section of the site. Add each domain name or IP address to the NAM application protocol directory.
- B.** Enable regular-expression pattern matching. Define application protocol filters based on regular expressions that match the desired URLs.
- C.** Enable URL monitoring. Define each desired URL as an application in the protocol directory.
- D.** Use SPAN or VACLs to capture upper-layer protocol data from the web servers. Use a third-party application to parse the stored capture files.

Answer: C

Explanation:

QUESTION NO: 2

Which command must be issued to activate the FWSM firewall context?

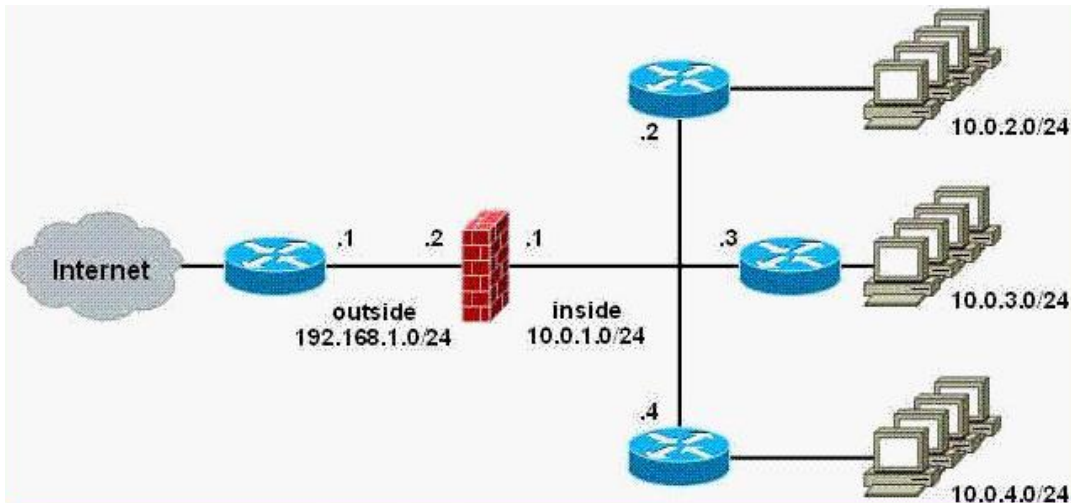
- A.** allocate-vlan
- B.** config-url
- C.** limit-resource
- D.** map-interface

Answer: B

Explanation:

QUESTION NO: 3

Refer to the exhibit. Which FWSM command allows routing of TCP traffic from the Internet to network 10.0.3.0/24?



- A. access-list inside permit tcp 192.168.1.0 255.255.255.0 10.0.3.0 255.255.255.0
- B. route inside 10.0.3.0 255.255.255.0 10.0.1.3
- C. route outside 10.0.3.0 255.255.255.0 10.0.1.3
- D. route inside 0 0 10.0.1.3

Answer: B

Explanation:

QUESTION NO: 4

In a Cisco Catalyst 6500 Series Switch, in which slot or slots should you install the NAM?

- A. slots 1 to 4
- B. slot 5 or 6
- C. any slot except a supervisor module slot
- D. the slots that are closest to the supervisor modules

Answer: C

Explanation:

QUESTION NO: 5

A customer has installed an FWSM in the data center. Which feature must be configured to enable FTP to work?

- A. dynamic NAT
- B. dynamic PAT

- C. access lists
- D. transparent mode
- E. deep packet inspection

Answer: E

Explanation:

QUESTION NO: 6

Which IDS capture method has the ability to impact the performance of VoIP applications?

- A. in-line
- B. promiscuous
- C. SPAN
- D. VACLs

Answer: A

Explanation:

QUESTION NO: 7

The install all command performs which two functions? (Choose two.)

- A. restores the old image as the new kickstart image
- B. backs up the currently active software image before upgrading it
- C. causes a switchover back to the originally active supervisor module
- D. copies the kickstart and system images to the standby supervisor module
- E. reloads the standby supervisor module with the new Cisco NX-OS software

Answer: D,E

Explanation:

QUESTION NO: 8

How many paths can be considered in NX-OS for equal-cost multipathing?

- A. 4
- B. 8

- C. 12
- D. 16

Answer: D

Explanation:

QUESTION NO: 9

Which command enables uRPF in strict mode?

- A. ip verify unicast source strict
- B. ip verify unicast source reachable-via rx
- C. ip verify unicast source reachable-via any
- D. ip verify unicast source reachable-via strict

Answer: B

Explanation:

QUESTION NO: 10

What will be upgraded as a result of this command?

```
Upgrade ftp://ftpuser@ 10.1.2.3//upgrade/IPS-K9-r-1.1-a-5.1-1 .pkg
```

- A. recovery partition
- B. application partition
- C. both application and recovery partitions immediately
- D. both application and recovery partitions at the next scheduled automatic IDSM update

Answer: A

Explanation:

QUESTION NO: 11

What is the effect of executing the command intrusion-detection module 5 management-port access-vlan 10 on an IDSM?

- A. allows the IDSM to be managed by devices in VLAN 10

- B. configures the IDSM to monitor traffic from VLAN 10 in in-line mode
- C. allows the IDSM to perform blocking actions on devices in VLAN 10
- D. configures the IDSM to monitor traffic from VLAN 10 in promiscuous mode

Answer: A

Explanation:

QUESTION NO: 12

Your customer uses these file-oriented network applications:

FTP

Web-based file repositories

Windows and Linux file sharing

How can you use the NAM to create a report showing total network traffic for these applications?

- A. Define a VACL that forwards traffic for all of the applications.
- B. Define an application group that contains all of the interfaces for the application servers.
- C. This cannot be accomplished because the NAM cannot monitor upper-layer protocol data.
- D. Add each application to the Cisco Traffic Analyzer protocol directory and create an application group with all of the applications

Answer: D

Explanation:

QUESTION NO: 13

In policy-based routing, what action is taken to packets that do not match any of the route-map statements?

- A. dropped
- B. forwarded using the specified "set" policy
- C. continue being evaluated against the implicit "permit" statement
- D. forwarded using a policy identical to packets matching a "deny" statement

Answer: D

Explanation:

QUESTION NO: 14

How does the Ethernet Host Virtualizer accomplish multiple active uplinks and loop prevention in a Cisco Nexus 5000 Switch?

- A. by implementing PVST
- B. by PortChanneling uplink ports
- C. by pinning MAC addresses to specific ports
- D. by tying a server interface to a border interface in the switching fabric

Answer: C

Explanation:

QUESTION NO: 15

Using the default VDC high-availability options in the Cisco Nexus 7010 Switch, which of the following occurs after a failure?

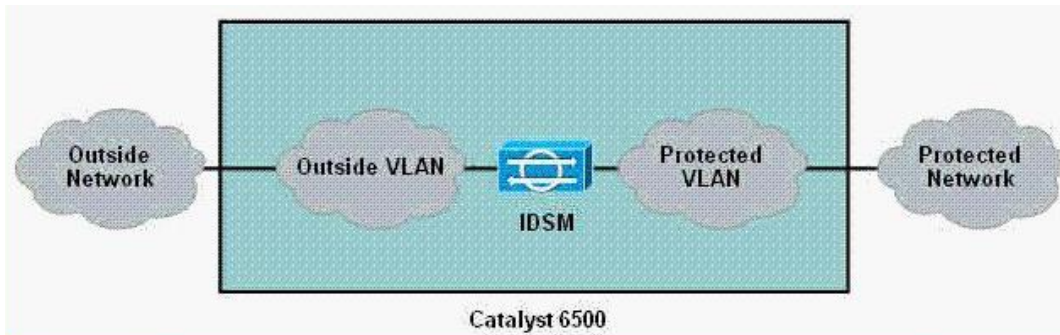
- A. If single supervisor, a graceful restart is forced
- B. If dual supervisors, asupervisor switchover is forced
- C. The VDC is deleted and no further action will be performed
- D. The VDC is deleted and then re-created with startup configuration

Answer: B

Explanation:

QUESTION NO: 16

Refer to the exhibit. Given this network design, what can you use to configure the IDSM to capture traffic?



- A. SPAN
- B. VACLs
- C. SPAN or VACLs
- D. neither SPAN nor VACLs

Answer: D

Explanation:

QUESTION NO: 17

Which signature action can be configured only on an IDS sensor in IPS mode?

- A. log packets containing the attacker and victim address pair
- B. modify data in the packet
- C. send a request to block a connection
- D. terminate the TCP flow

Answer: B

Explanation:

QUESTION NO: 18

What can a Cisco Nexus 7010 Switch administrator do per VDC to provide OOB management?

- A. allocate separate VLANs and VRFs per VDC
- B. use 802.1Q trunking and provide a separate VLAN per VDC
- C. use different OOB management ports for the different VDCs
- D. use the same VLAN and subnet for all VDCs, with different IP addresses

Answer: D

Explanation:

QUESTION NO: 19

How can a customer with multiple FWSM contexts limit the number of connections that are permitted in each context?

- A. Map the context to a class, and apply resource limits to the class.
- B. Map the context to a VLAN, and apply resource limits to the VLAN.
- C. Map the context to a class, and apply resource limits to the context.
- D. You cannot limit the number of connections that are permitted in a context.

Answer: A

Explanation:

QUESTION NO: 20

During failover, what happens with the MAC address of the standby HSRP router?

- A. It is reclaimed by the active router.
- B. The standby router sends gratuitous ARP messages.
- C. The standby router assumes the virtual MAC address.
- D. It defaults to the factory-burned MAC address of the standby router.

Answer: C

Explanation:

QUESTION NO: 21

What is required when configuring NTP on the IDSM?

- A. Configure an MD5 key.
- B. Add a service account for the NTP service.
- C. Configure the IDSM host access list to allow access to the NTP server.
- D. Associate the VLAN containing the NTP server with the IDSM management port.

Answer: A

Explanation:

QUESTION NO: 22

Information gathered during the DCNM initial discovery includes information about which of the following?

- A. MIBs
- B. SNMP clients
- C. running configuration
- D. directly connected devices only

Answer: C

Explanation:

QUESTION NO: 23

How are DHCP messages validated in the DHCP snooping process?

- A. Traffic is blocked if it matches MAC addresses of invalid DHCP servers.
- B. Trusted sources are matched by identifying RFC-consistent DHCP calls.
- C. Untrusted sources are identified by configuring their connecting interfaces.
- D. Untrusted sources are matched against a database of valid DHCP bindings.

Answer: C

Explanation:

QUESTION NO: 24

You work as a Cisco engineer. You know Dynamic Host Configuration Protocol (DHCP) well, so how are DHCP messages authenticated in the DHCP snooping process?

- A. Untrusted sources are identified by configuring their connecting interfaces.
- B. Traffic is blocked if it matches MAC addresses of invalid DHCP servers.
- C. Untrusted sources are matched against a database of valid Dynamic Host Configuration Protocol bindings.
- D. Trusted sources are matched by identifying RFC-consistent Dynamic Host Configuration Protocol calls.

Answer: B