300-206$^{\text{Q\&As}}$

Implementing Cisco Edge Network Security Solutions

QUESTION 1

Which four are IPv6 First Hop Security technologies? (Choose four.)

A. Send

B. Dynamic ARP Inspection

C. Router Advertisement Guard

D. Neighbor Discovery Inspection

E. Traffic Storm Control

F. Port Security

G. DHCPv6 Guard

Correct Answer: ACDG

QUESTION 2

With what commands you can configure unified access-list on ASA CLI? (Choose two)

A. access-list

B. ipv6 access-list

C. ipv6 access-list website

D. object-group network

E. object network

Correct Answer: AD

ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The any keyword was changed to represent IPv4 and IPv6 traffic. The any4 and any6 keywords were added

to represent IPv4-only and IPv6-only traffic, respectively. The IPv6-specific ACLs are deprecated. Existing IPv6 ; are migrated to extended ACLs. See the release notes for more information about migration.

We modified the following commands: access-list extended , access-list webtype.

We removed the following commands: ipv6 access-list, ipv6 access-list webtype, ipv6-vpn-filter.

Network object groups can contain multiple network objects as well as inline networks. Network object groups can support a mix of both IPv4 and IPv6 addresses.

You cannot use a mixed IPv4 and IPv6 object group for NAT, or object groups that include FQDN objects.

QUESTION 3

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 4

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

QUESTION 5

Which function in the Cisco ADSM ACL Manager pane allows an administrator to search for a specfic element?

A. Find

B. Device Management

C. Search

D. Device Setup

Correct Answer: A

QUESTION 6

Which statement about traffic storm control behavior is true?

A. Traffic storm control cannot determine if the packet is unicast or broadcast.

B. If you enable broadcast and multicast traffic storm control and the combined broadcast and multicast traffic exceeds the level within a 1 second traffic storm interval, storm control drops all broadcast and multicast traffic until the end of the storm interval

C. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

D. Traffic storm control monitors incoming traffic levels over a 10 second traffic storm control interval

Correct Answer: B

QUESTION 7

Which information does the ASA fail to replicate to the secondary Cisco ASA adaptive security appliance in an active/standby configuration with stateful and failover links?

A. TCP sessions

B. routing tables

C. DHCP lease

D. NAT translations

Correct Answer: C

QUESTION 8

Which two types of addresses can be blocked with BRF on the ASA? (Choose two)

A. instant messaging

B. ads

C. P2P

D. spyware

E. Games

Correct Answer: BD

Botnets are a collection of malicious software or "bots" covertly installed on endpoints and controlled by another entity through a communications channel such as IRC, peer-to-peer (P2P), or HTTP. The dynamic database includes the

following types of addresses:

Ads - These are advertising networks that deliver banner ads, interstitials, rich media ads, pop- ups, and pop-unders for websites, spyware and adware. Some of these networks send ad- oriented HTML emails and email verification services.

Data Tracking - These are sources associated with companies and websites that offer data tracking and metrics services to websites and other online entities. Some of these also run small advertising networks. Spyware - These are sources that distribute spyware, adware, greyware, and other potentially unwanted advertising software. Some of these also run exploits to install such software. Malware - These are sources that use various exploits to deliver adware, spyware and

other malware to victim computers. Some of these are associated with rogue online vendors and distributors of dialers which deceptively call premium-rate phone numbers.

Adult - These are sources associated with adult networks/services offering web hosting for adult content, advertising, content aggregation, registration and billing, and age verification. These may be tied to distribution of adware, spyware, and

dialers.

Bot and Threat Networks - These are rogue systems that control infected computers. They are either systems hosted on threat networks or systems that are part of the botnet itself.

QUESTION 9

Which Cisco prime Infrastructure features allows you to assign templates to a group of wireless LAN controllers with similar configuration requirements?

A. Lightweight access point configuration template

B. Composite template

C. Controller configuration group

D. Shared policy object

Correct Answer: C

QUESTION 10

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

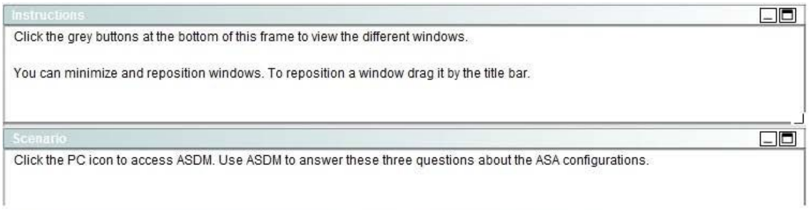
modulus groups from which peers can choose during the Phase 1 negotiation, potentially making it possible to create a single IKE proposal (although you might want different proposals to give higher priority to your most desired options). You

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.

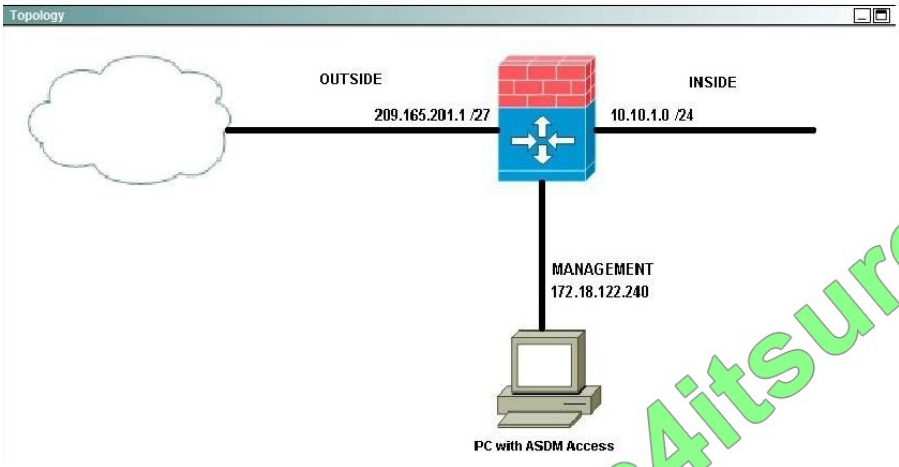
QUESTION 11

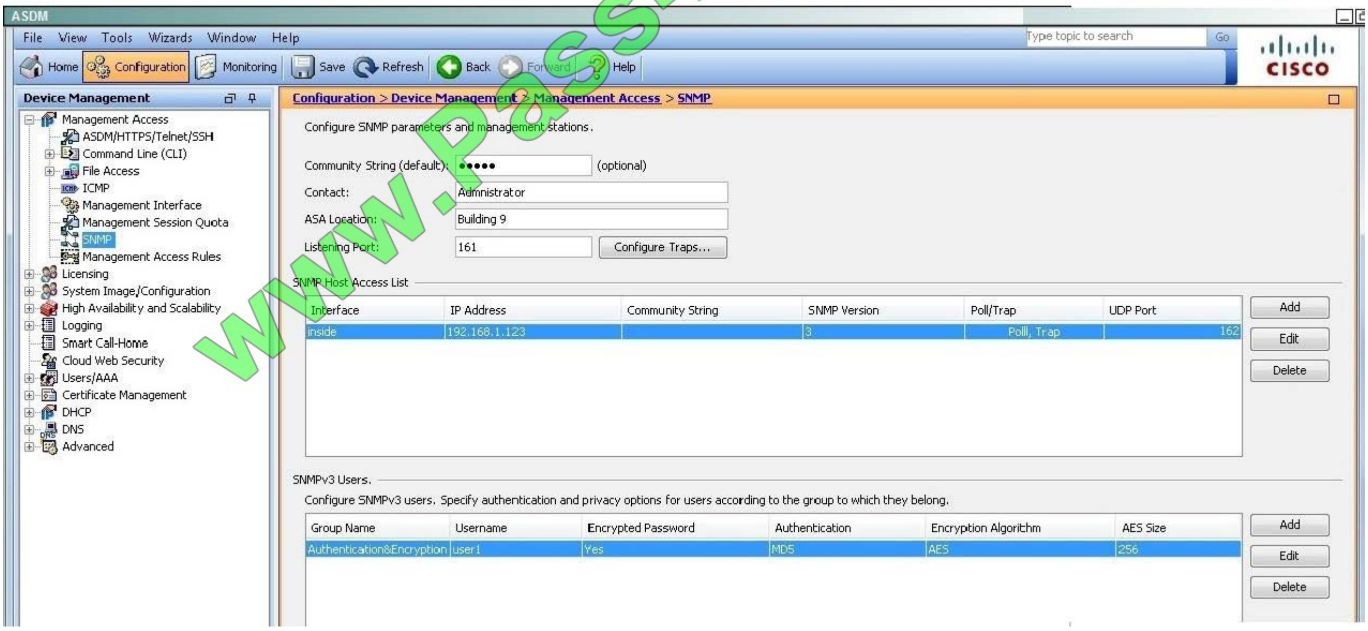


Click the grey buttons at the bottom of this frame to view the different windows.

You can minimize and reposition windows. To reposition a window drag it by the title bar.

Click the PC icon to access ASDM. Use ASDM to answer these three questions about the ASA configurations.





Configure SNMP parameters and management stations.

Community String (default): ●●●●● (optional)

Contact: Administrator

ASA Location: Building 9

Listening Port: 161

Configure Traps...

SNMP Host Access List

Interface	IP Address	Community String	SNMP Version	Poll/Trap	UDP Port
inside	192.168.1.123		3	Poll, Trap	162

SNMPv3 Users.

Configure SNMPv3 users. Specify authentication and privacy options for users according to the group to which they belong.

Group Name	Username	Encrypted Password	Authentication	Encryption Algorithm	AES Size
Authentication&Encryption	user1	Yes	MD5	AES	256

Which statement about how the Cisco ASA supports SNMP is true?

A. All SNMFV3 traffic on the inside interface will be denied by the global ACL

B. The Cisco ASA and ASASM provide support for network monitoring using SNMP Versions 1,2c, and 3, but do not support the use of all three versions simultaneously.

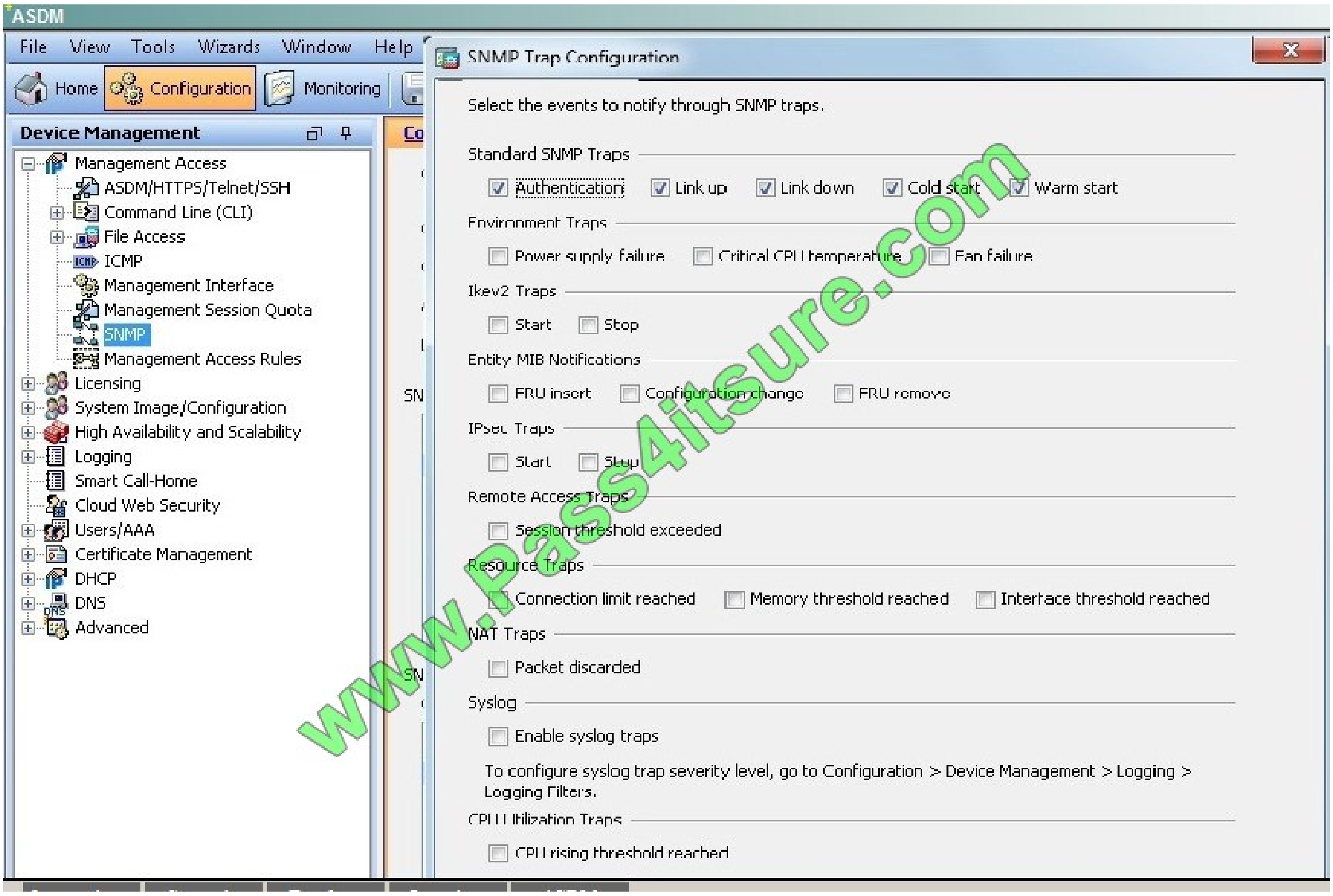
C. The Cisco ASA and ASASM have an SNMP agent that notifies designated management ,. stations if events occur that are predefined to require a notification, for example, when a link in the network goes up or down.

D. SNMPv3 is enabled by default and SNMP v1 and 2c are disabled by default.

E. SNMPv3 is more secure because it uses SSH as the transport mechanism.

Correct Answer: C

This can be verified by this ASDM screen shot:



SNMP Trap Configuration

Select the events to notify through SNMP traps.

Standard SNMP Traps

☑ Authentication ☑ Link up ☑ Link down ☑ Cold start ☑ Warm start

Environment Traps

□ Power supply failure □ Critical CPU temperature □ Fan failure

Ikev2 Traps

□ Start □ Stop

Entity MIB Notifications

□ FRU insert □ Configuration change □ FRU remove

IPsec Traps

□ Start □ Stop

Remote Access Traps

□ Session threshold exceeded

Resource Traps

□ Connection limit reached □ Memory threshold reached □ Interface threshold reached

NAT Traps

□ Packet discarded

Syslog

□ Enable syslog traps

To configure syslog trap severity level, go to Configuration > Device Management > Logging > Logging Filters.

CPU Utilization Traps

□ CPU rising threshold reached

QUESTION 12

Choose two correct statements about private-vlan.

A. Interface that is assigned to primary-vlan ID (access mode) can communicate with interface with secondary vlan ID that belongs to same primary-vlan (same switch)

B. Interface that is assigned to community vlan can communicate with interface in the same secondary vlan but it is also configured as protected (same switch)

C. You have to configure dhcp snooping for both primary and secondary VLANs

D. You have to configure DAI only for primary vlan

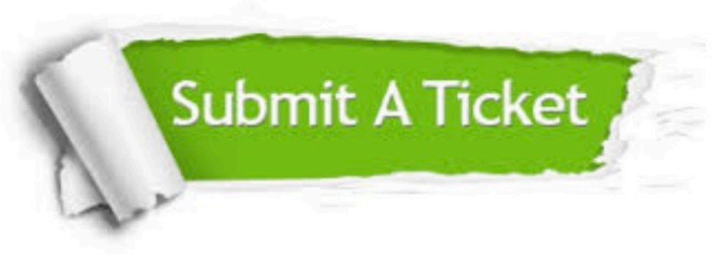
E. You cannot combine private-vlan feature with protected ports ?

Correct Answer: DE

You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP snooping on a secondary VLAN, the configuration does not take

effect if the primary VLAN is already configured. The same statement is true about DAI.

A private-VLAN port cannot be a secure port and should not be configured as a protected port.


Submit A Ticket

100%