VCEplus.com

Selftestengine.300-206.108 questions.

Number: 300-206
Passing Score: 800
Time Limit: 120 min
File Version: 6.2

VCEplus.com VCEplus.com

Cisco 300-206

Implementing Cisco Edge Network Security Solutions

- 100% Valid in US, UK, Australia, India and Emirates. All my friends in group have these same questions.
- Many new questions are added, Good for review go ahead and pass the exam now.
- I liked it very much. The content in both products provides exactly what you need to pass.
- Make yourself wise and talented with studies and look out for the video lectures for your exam because they are perfect to train you for the exam and its modules.
- Start your career with this assistance and you will never regret investing in its amazing study tools that are for you and your training in any kind of certification exam preparation.

Exam A

QUESTION 1
All 30 users on a single floor of a building are complaining about network slowness. After investigating the access switch, the network administrator notices that the MAC address table is full (10,000 entries) and all traffic is being flooded out of every port. Which action can the administrator take to prevent this from occurring?

A. Configure port-security to limit the number of mac-addresses allowed on each port
B. Upgrade the switch to one that can handle 20,000 entries
C. Configure private-vlans to prevent hosts from communicating with one another
D. Enable storm-control to limit the traffic rate
E. Configure a VACL to block all IP traffic except traffic to and from that subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
A network printer has a DHCP server service that cannot be disabled. How can a layer 2 switch be configured to prevent the printer from causing network issues?

A. Remove the ip helper-address
B. Configure a Port-ACL to block outbound TCP port 68
C. Configure DHCP snooping
D. Configure port-security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
Which three options are hardening techniques for Cisco IOS routers? (Choose three.)

A. limiting access to infrastructure with access control lists
B. enabling service password recovery

VCEplus.com

C. using SSH whenever possible
D. encrypting the service password
E. using Telnet whenever possible
F. enabling DHCP snooping

VCEplus.com

Real 4
Cisco 300-206 Exam

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Which three commands can be used to harden a switch? (Choose three.)

A. switch(config-if)# spanning-tree bpdufilter enable
B. switch(config)# ip dhcp snooping
C. switch(config)# errdisable recovery interval 900
D. switch(config-if)# spanning-tree guard root
E. switch(config-if)# spanning-tree bpduguard disable
F. switch(config-if)# no cdp enable

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
properly sorted answer.

QUESTION 5
What are three features of the Cisco ASA 1000V? (Choose three.)

A. cloning the Cisco ASA 1000V
B. dynamic routing
C. the Cisco VNMC policy agent
D. IPv6

E. active/standby failover
F. QoS

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
If the Cisco ASA 1000V has too few licenses, what is its behavior?

A. It drops all traffic.
B. It drops all outside-to-inside packets.
C. It drops all inside-to-outside packets.
Real 5
Cisco 300-206 Exam
D. It passes the first outside-to-inside packet and drops all remaining packets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
A network administrator is creating an ASA-CX administrative user account with the following parameters:

- The user will be responsible for configuring security policies on network devices.
- The user needs read-write access to policies.
- The account has no more rights than necessary for the job.

What role will the administrator assign to the user?

A. Administrator
B. Security administrator
C. System administrator

VCEplus.com

D. Root Administrator
E. Exec administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access?

A. sslconfig
B. sslciphers
C. tlsconifg
D. certconfig

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 6
Cisco 300-206 Exam

QUESTION 9
What is the CLI command to enable SNMPv3 on the Cisco Web Security Appliance?

A. snmpconfig
B. snmpenable
C. configsnmp
D. enablesnmp

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
Explanation:

QUESTION 10
The Cisco Email Security Appliance can be managed with both local and external users of different privilege levels. What three external modes of authentication are supported? (Choose three.)

A. LDAP authentication
B. RADIUS Authentication
C. TACAS
D. SSH host keys
E. Common Access Card Authentication
F. RSA Single use tokens

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A network administrator is creating an ASA-CX administrative user account with the following parameters:

- The user will be responsible for configuring security policies on network devices.
- The user needs read-write access to policies.
- The account has no more rights than necessary for the job.

What role will be assigned to the user?

A. Administrator
   Real 7
   Cisco 300-206 Exam
B. Security administrator
C. System administrator
D. Root Administrator
E. Exec administrator

VCEplus.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
good answer.

QUESTION 12
Which tool provides the necessary information to determine hardware lifecycle and compliance details for deployed network devices?

A. Prime Infrastructure
B. Prime Assurance
C. Prime Network Registrar
D. Prime Network Analysis Module

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
Which three compliance and audit report types are available in Cisco Prime Infrastructure? (Choose three.)

A. Service
B. Change Audit
C. Vendor Advisory
D. TAC Service Request
E. Validated Design
F. Smart Business Architecture

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VCEplus.com

QUESTION 14
Cisco Security Manager can manage which three products? (Choose three.)

Real 8
Cisco 300-206 Exam

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
Section: (none)
Explanation

Explanation/Reference:
right answer.

QUESTION 15
Which two web browsers are supported for the Cisco ISE GUI? (Choose two.)

A. HTTPS-enabled Mozilla Firefox version 3.x
B. Netscape Navigator version 9
C. Microsoft Internet Explorer version 8 in Internet Explorer 8-only mode
D. Microsoft Internet Explorer version 8 in all Internet Explorer modes
E. Google Chrome (all versions)

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VCEplus.com

QUESTION 16
When a Cisco ASA is configured in multicontext mode, which command is used to change between contexts?

A. changeto config context
B. changeto context
C. changeto/config context change
D. changeto/config context 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 9
Cisco 300-206 Exam

QUESTION 17
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
When you install a Cisco ASA AIP-SSM, which statement about the main Cisco ASDM home page is true?

A. It is replaced by the Cisco AIP-SSM home page.
B. It must reconnect to the NAT policies database.
C. The administrator can manually update the page.

VCEplus.com

D. It displays a new Intrusion Prevention panel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which Cisco product provides a GUI-based device management tool to configure Cisco access routers?

A. Cisco ASDM
B. Cisco CP Express
C. Cisco ASA 5500
D. Cisco CP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 10
Cisco 300-206 Exam

QUESTION 20
Which statement about Cisco IPS Manager Express is true?

A. It provides basic device management for large-scale deployments.
B. It provides a GUI for configuring IPS sensors and security modules.
C. It enables communication with Cisco ASA devices that have no administrative access.
D. It provides greater security than simple ACLs.

Correct Answer: B
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
definite answer.

QUESTION 21
Which three options describe how SNMPv3 traps can be securely configured to be sent by IOS? (Choose three.)

A. An SNMPv3 group is defined to configure the read and write views of the group.
B. An SNMPv3 user is assigned to SNMPv3 group and defines the encryption and authentication credentials.
C. An SNMPv3 host is configured to define where the SNMPv3 traps will be sent.
D. An SNMPv3 host is used to configure the encryption and authentication credentials for SNMPv3 traps.
E. An SNMPv3 view is defined to configure the address of where the traps will be sent.
F. An SNMPv3 group is used to configure the OIDs that will be reported.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
A network engineer is asked to configure NetFlow to sample one of every 100 packets on a router's fa0/0 interface. Which configuration enables sampling, assuming that NetFlow is already configured and running on the router's fa0/0 interface?

A. flow-sampler-map flow1
mode random one-out-of 100
interface fas0/0
flow-sampler flow1
B. flow monitor flow1
mode random one-out-of 100
Real 11
Cisco 300-206 Exam
interface fas0/0
ip flow monitor flow1
C. flow-sampler-map flow1
one-out-of 100
interface fas0/0
flow-sampler flow1
D. ip flow-export source fas0/0 one-out-of 100

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
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
Section: (none)
Explanation

Explanation/Reference:
well answered.

QUESTION 24
Which two options are two purposes of the packet-tracer command? (Choose two.)

Real 14
Cisco 300-206 Exam

A. to filter and monitor ingress traffic to a switch
B. to configure an interface-specific packet trace
C. to inject virtual packets into the data path
D. to debug packet drops in a production network
E. to correct dropped packets in a production network

Correct Answer: CD
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
Explanation:

QUESTION 25
Which set of commands enables logging and displays the log buffer on a Cisco ASA?

A. enable logging
show logging
B. logging enable
show logging
C. enable logging int e0/1
view logging
D. logging enable
logging view config

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which command displays syslog messages on the Cisco ASA console as they occur?

A. Console logging <level>
B. Logging console <level>
C. Logging trap <level>
D. Terminal monitor
E. Logging monitor <level>

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 15

QUESTION 27
Which set of commands creates a message list that includes all severity 2 (critical) messages on a Cisco security device?

A. logging list critical_messages level 2
   console logging critical_messages
B. logging list critical_messages level 2
   logging console critical_messages
C. logging list critical_messages level 2
   logging console enable critical_messages
D. logging list enable critical_messages level 2
   console logging critical_messages

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
An administrator is deploying port-security to restrict traffic from certain ports to specific MAC addresses. Which two considerations must an administrator take into account when using the switchport port-security mac-address sticky command? (Choose two.)

A. The configuration will be updated with MAC addresses from traffic seen ingressing the port.
   The configuration will automatically be saved to NVRAM if no other changes to the configuration have been made.
B. The configuration will be updated with MAC addresses from traffic seen ingressing the port.
   The configuration will not automatically be saved to NVRAM.
C. Only MAC addresses with the 5th most significant bit of the address (the 'sticky' bit) set to 1 will be learned.
D. If configured on a trunk port without the 'vlan' keyword, it will apply to all vlans.
E. If configured on a trunk port without the 'vlan' keyword, it will apply only to the native vlan.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
actual answer.

QUESTION 29
A Cisco ASA is configured for TLS proxy. When should the security appliance force remote IP phones connecting to the phone proxy through the internet to be in secured mode?

Real 16
Cisco 300-206 Exam

A. When the Cisco Unified Communications Manager cluster is in non-secure mode
B. When the Cisco Unified Communications Manager cluster is in secure mode only
C. When the Cisco Unified Communications Manager is not part of a cluster
D. When the Cisco ASA is configured for IPSec VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which two features are supported when configuring clustering of multiple Cisco ASA appliances? (Choose two.)

A. NAT
B. dynamic routing
C. SSL remote access VPN
D. IPSec remote access VPN

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
Which four are IPv6 First Hop Security technologies? (Choose four.)

A. Send

VCEplus.com

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
IPv6 addresses in an organization's network are assigned using Stateless Address Autoconfiguration. What is a security concern of using SLAAC for IPv6 address assignment?

A. Man-In-The-Middle attacks or traffic interception using spoofed IPv6 Router Advertisements
B. Smurf or amplification attacks using spoofed IPv6 ICMP Neighbor Solicitations
C. Denial of service attacks using TCP SYN floods
D. Denial of Service attacks using spoofed IPv6 Router Solicitations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
Which two device types can Cisco Prime Security Manager manage in Multiple Device mode? (Choose two.)

A. Cisco ESA
B. Cisco ASA
C. Cisco WSA
D. Cisco ASA CX

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 20
Cisco 300-206 Exam

QUESTION 34
Which technology provides forwarding-plane abstraction to support Layer 2 to Layer 7 network services in Cisco Nexus 1000V?

A. Virtual Service Node
B. Virtual Service Gateway
C. Virtual Service Data Path
D. Virtual Service Agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
To which interface on a Cisco ASA 1000V firewall should a security profile be applied when a VM sits behind it?

A. outside
B. inside
C. management
D. DMZ

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
absolute answer.

QUESTION 36
You are configuring a Cisco IOS Firewall on a WAN router that is operating as a Trusted Relay Point (TRP) in a voice network. Which feature must you configure to open data-channel pinholes for voice packets that are sourced from a TRP within the WAN?

A. CAC
B. ACL
C. CBAC
D. STUN
Real 21
Cisco 300-206 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
Which two voice protocols can the Cisco ASA inspect? (Choose two.)

A. MGCP
B. IAX
C. Skype
D. CTIQBE

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
You have explicitly added the line deny ipv6 any log to the end of an IPv6 ACL on a router interface. Which two ICMPv6 packet types must you explicitly allow to enable traffic to traverse the interface? (Choose two.)

A. router solicitation

VCEplus.com

B. router advertisement
C. neighbor solicitation
D. neighbor advertisement
E. redirect

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP?

A. MACsec
B. Flex VPN
C. Control Plane Protection
Real 22
Cisco 300-206 Exam
D. Dynamic Arp Inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 40
Which log level provides the most detail on the Cisco Web Security Appliance?

A. Debug
B. Critical
C. Trace
D. Informational

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 41
What is the lowest combination of ASA model and license providing 1 Gigabit Ethernet interfaces?

A. ASA 5505 with failover license option
B. ASA 5510 Security+ license option
C. ASA 5520 with any license option
D. ASA 5540 with AnyConnect Essentials License option

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
Which URL matches the regex statement "http"*/"www.cisco.com/"*[^E]"xe"?

A. https://www.cisco.com/ftp/ios/tftpserver.exe
B. https://cisco.com/ftp/ios/tftpserver.exe
C. http:/www.cisco.com/ftp/ios/tftpserver.Exe
D. https:/www.cisco.com/ftp/ios/tftpserver.EXE
Real 23
Cisco 300-206 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
Which two statements about Cisco IOS Firewall are true? (Choose two.)

A. It provides stateful packet inspection.
B. It provides faster processing of packets than Cisco ASA devices provide.
C. It provides protocol-conformance checks against traffic.
D. It eliminates the need to secure routers and switches throughout the network.
E. It eliminates the need to secure host machines throughout the network.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
sophisticated answer.

QUESTION 44
Which two VPN types can you monitor and control with Cisco Prime Security Manager? (Choose two.)

A. AnyConnect SSL
B. site-to-site
C. clientless SSL
D. IPsec remote-access

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://www.cisco.com/c/en/us/td/docs/security/asacx/9- 1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

QUESTION 45
What are three attributes that can be applied to a user account with RBAC? (Choose three.)

A. domain
B. password
C. ACE tag
D. user roles

www.vceplus.com - Website designed to help IT pros advance their careers.

E. VDC group tag
F. expiry date

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
If you encounter problems logging in to the Cisco Security Manager 4.4 web server or client or backing up its databases, which account has most likely been improperly modified?

A. admin (the default administrator account)
B. casuser (the default service account)
C. guest (the default guest account)
D. user (the default user account)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
Which component does Cisco ASDM require on the host Cisco ASA 5500 Series or Cisco PIX security appliance?

A. a DES or 3DES license
B. a NAT policy server
C. a SQL database
D. a Kerberos key
E. a digital certificate

Correct Answer: A
Section: (none)
Explanation

VCEplus.com

Explanation/Reference:
reliable answer.

QUESTION 48
Which command configures the SNMP server group1 to enable authentication for members of the access list east?

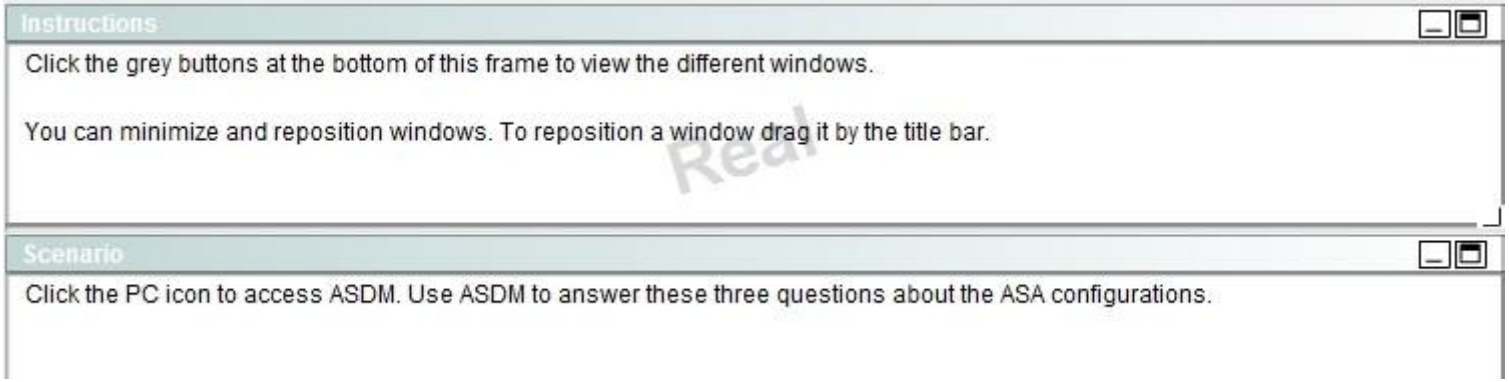
Real 25
Cisco 300-206 Exam

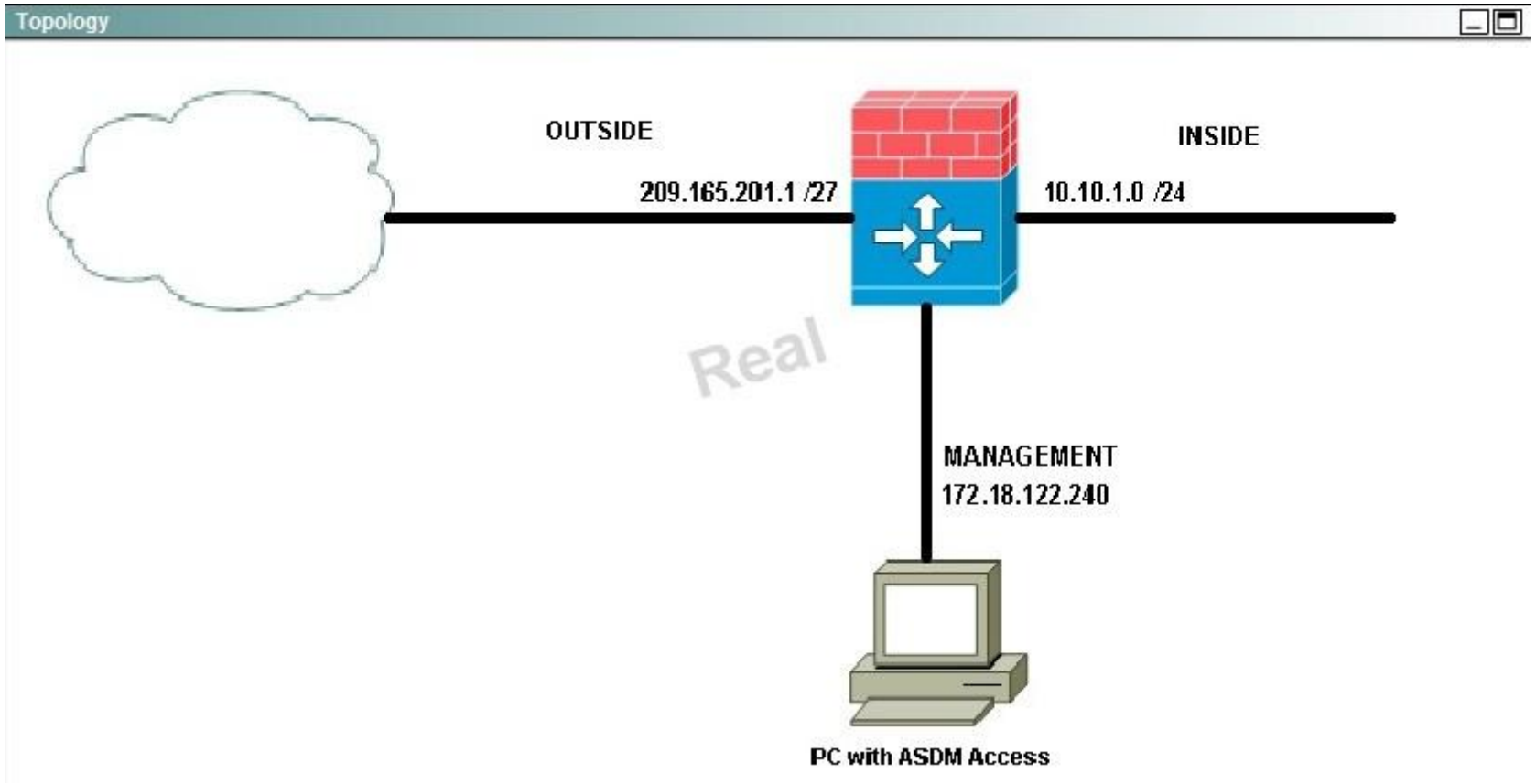
A. snmp-server group group1 v3 auth access east
B. snmp-server group1 v3 auth access east
C. snmp-server group group1 v3 east
D. snmp-server group1 v3 east access

Correct Answer: A
Section: (none)
Explanation

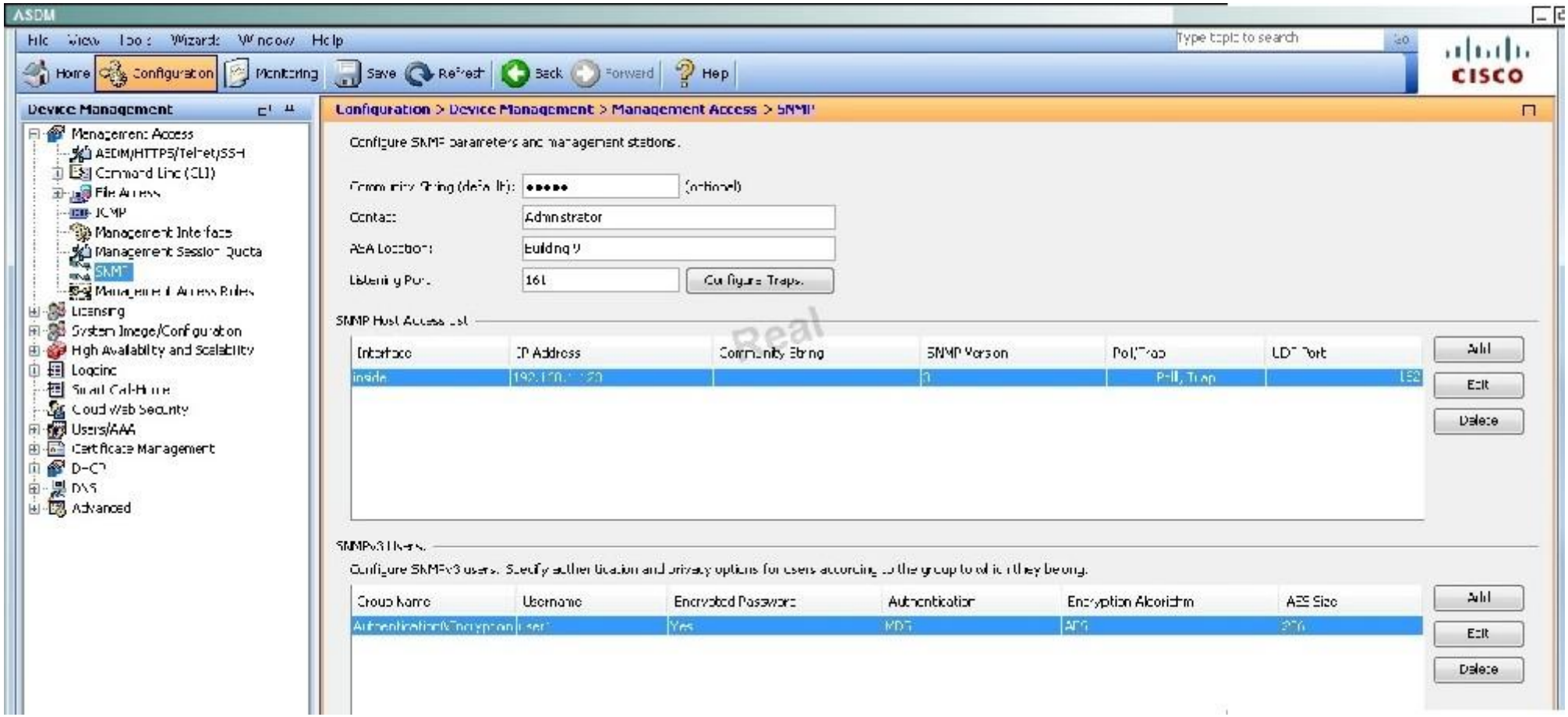
Explanation/Reference:
Explanation:

QUESTION 49





Real 29
Cisco 300-206 Exam



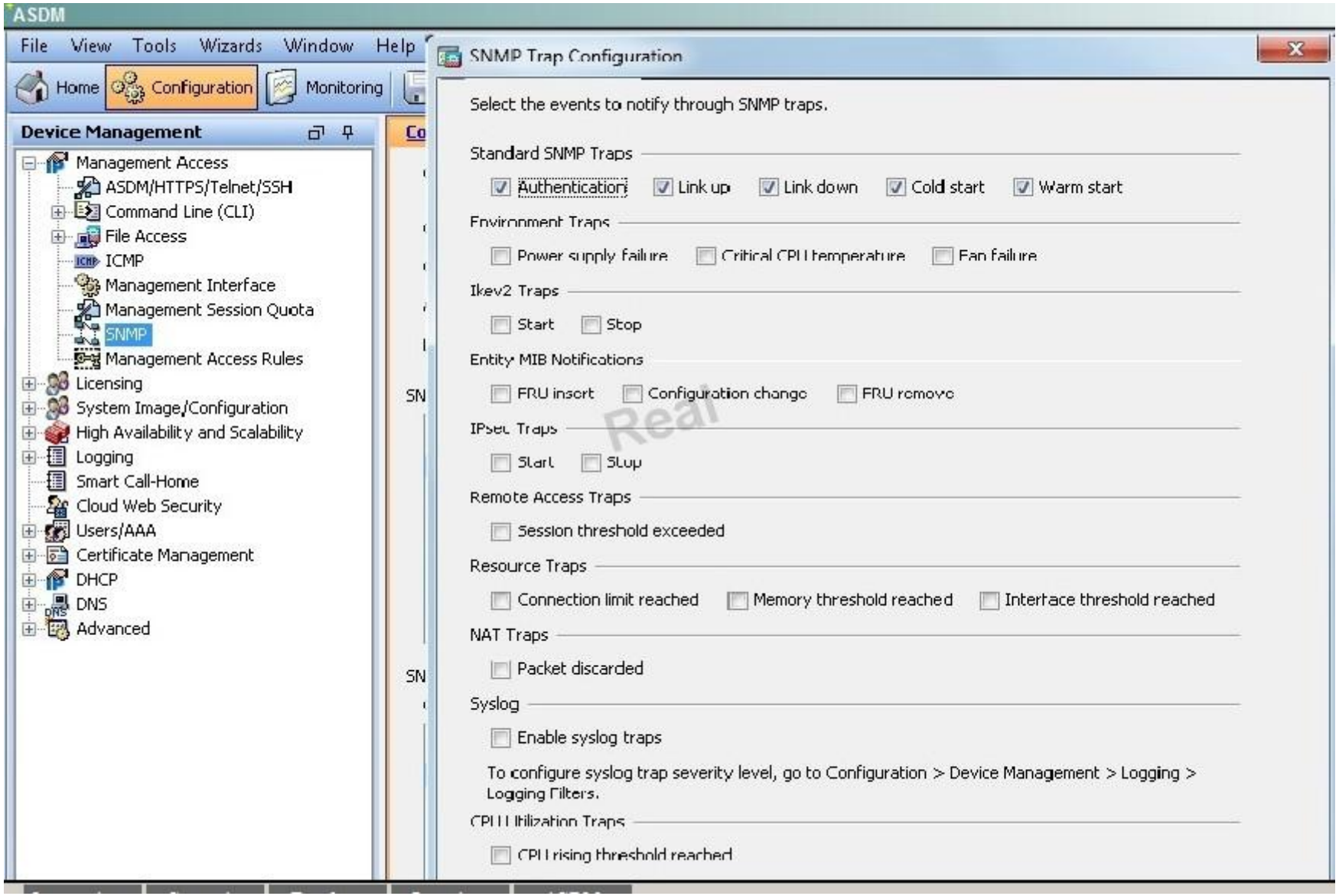
Which statement about how the Cisco ASA supports SNMP is true?

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
Section: (none)
Explanation

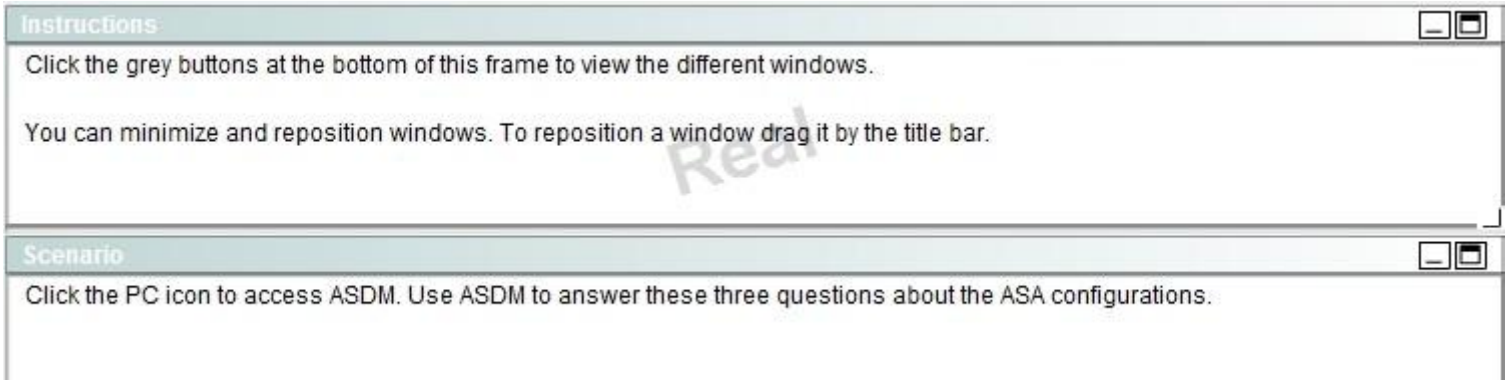
Explanation/Reference:
Explanation:
This can be verified by this ASDM screen shot:

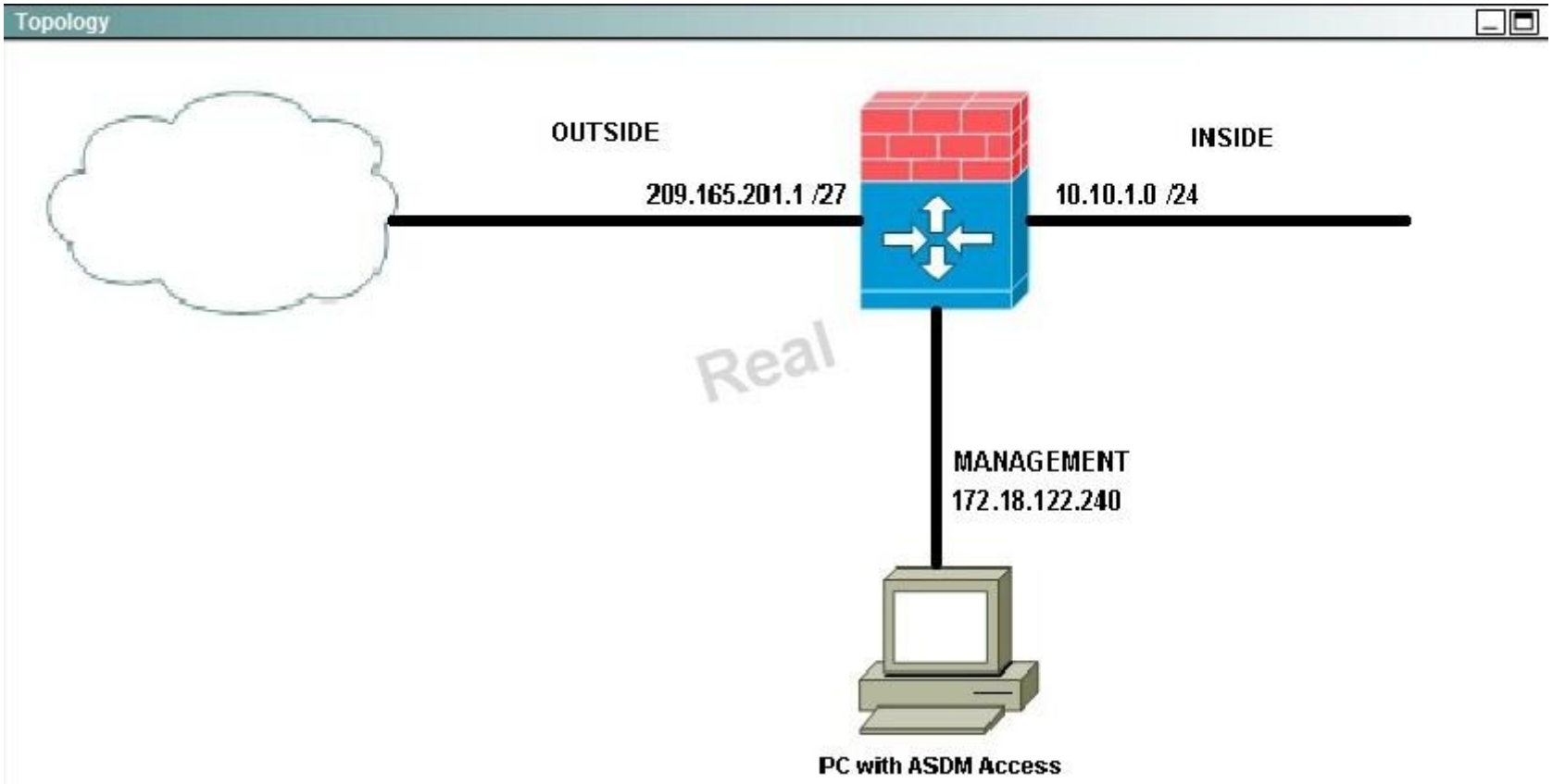
VCEplus.com



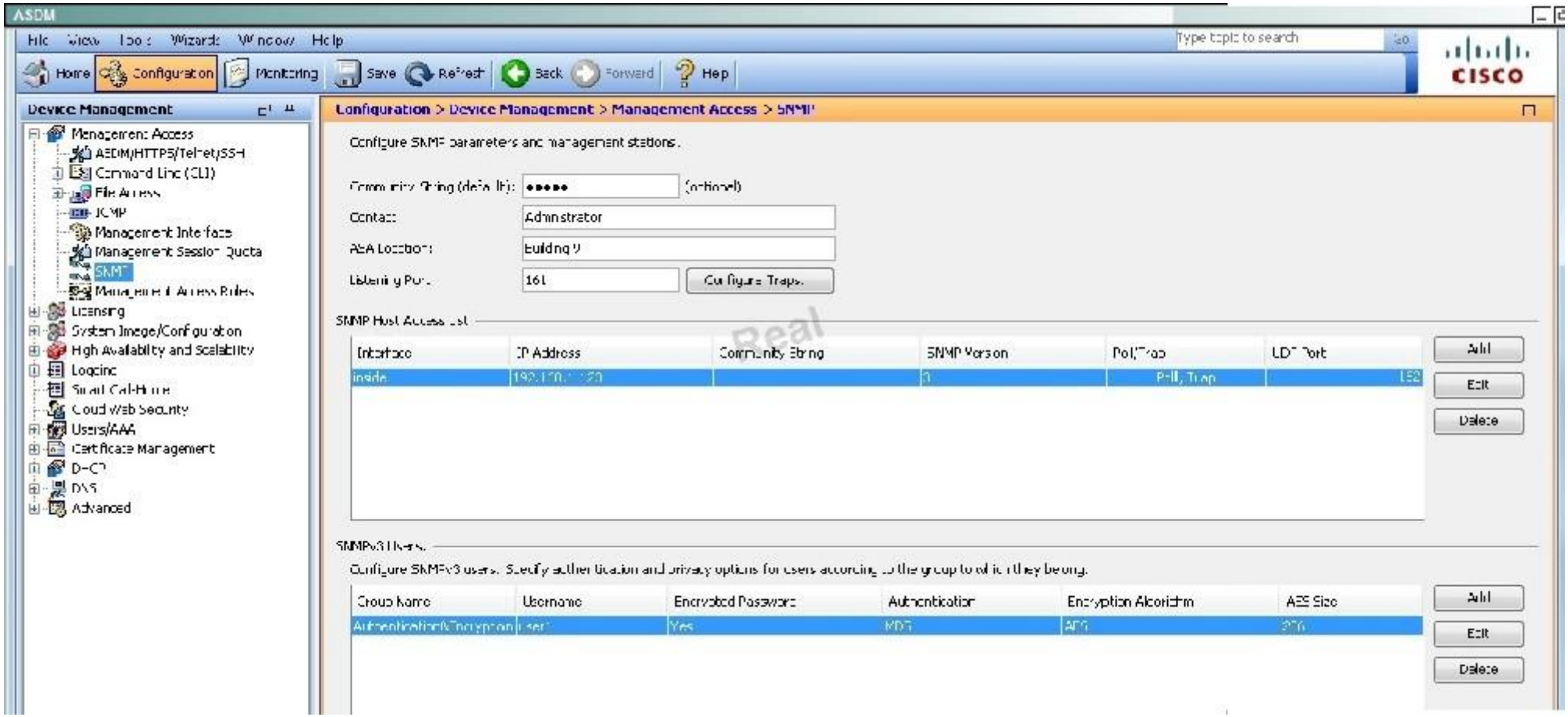
Real 30
Cisco 300-206 Exam

QUESTION 50


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



www.vceplus.com - Website designed to help IT pros advance their careers.



Real 31
Cisco 300-206 Exam
SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, andAES (which is available in 128,192, and 256 versions). When you create a user, with which option must you associate it?

A. an SNMP group
B. at least one interface
C. the SNMP inspection in the global_policy

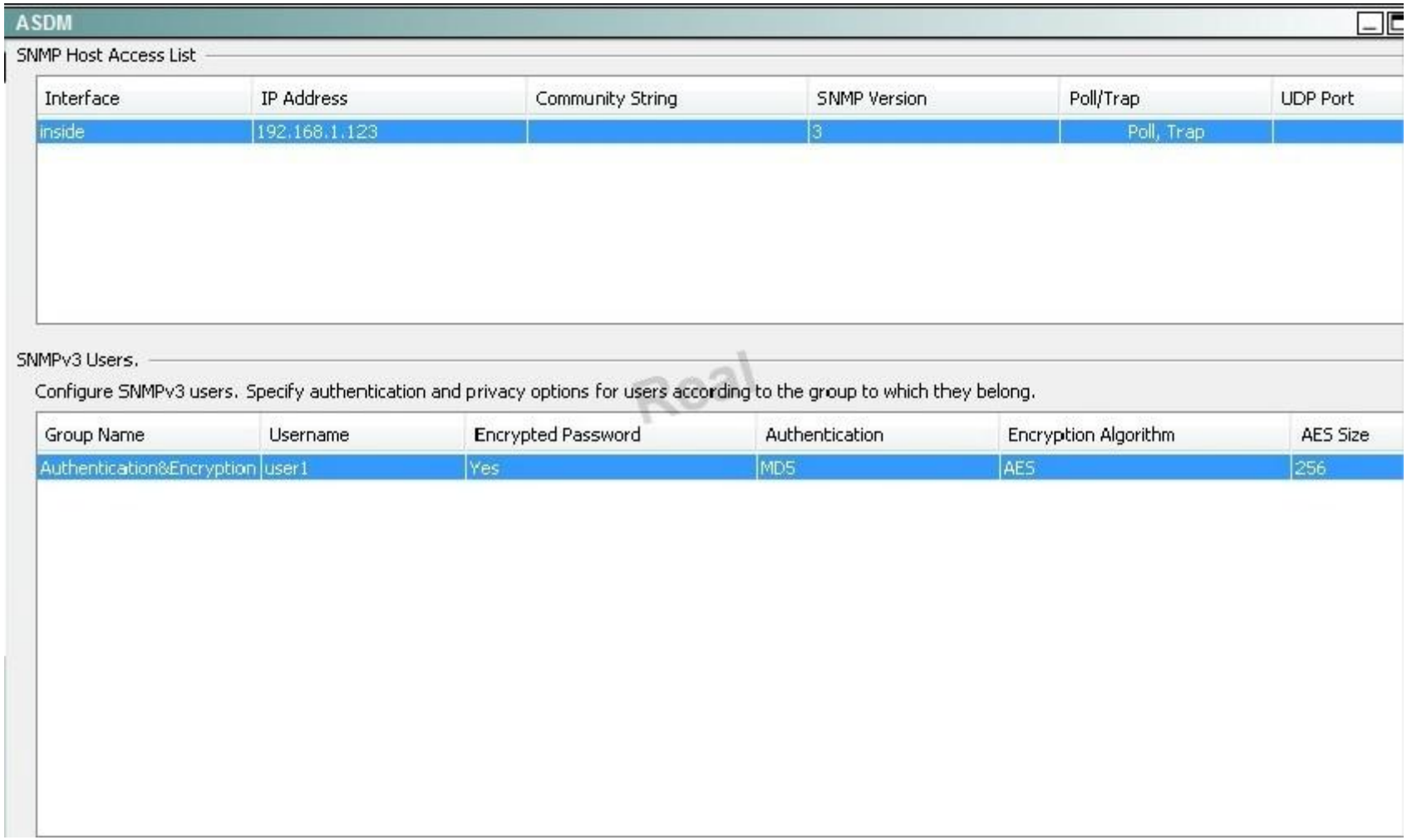
www.vceplus.com - Website designed to help IT pros advance their careers.

D. at least two interfaces

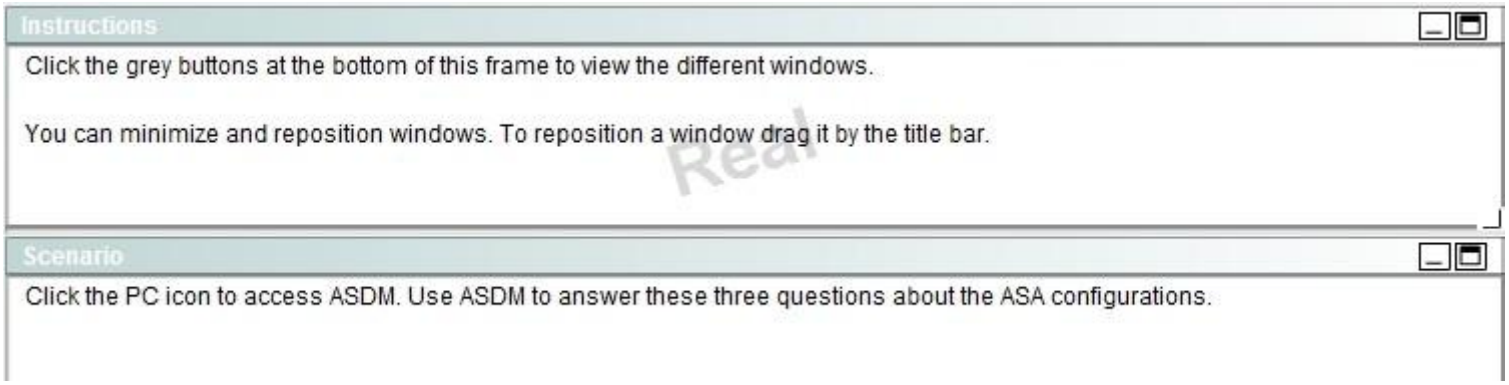
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: This can be verified via the ASDM screen shot shown here:

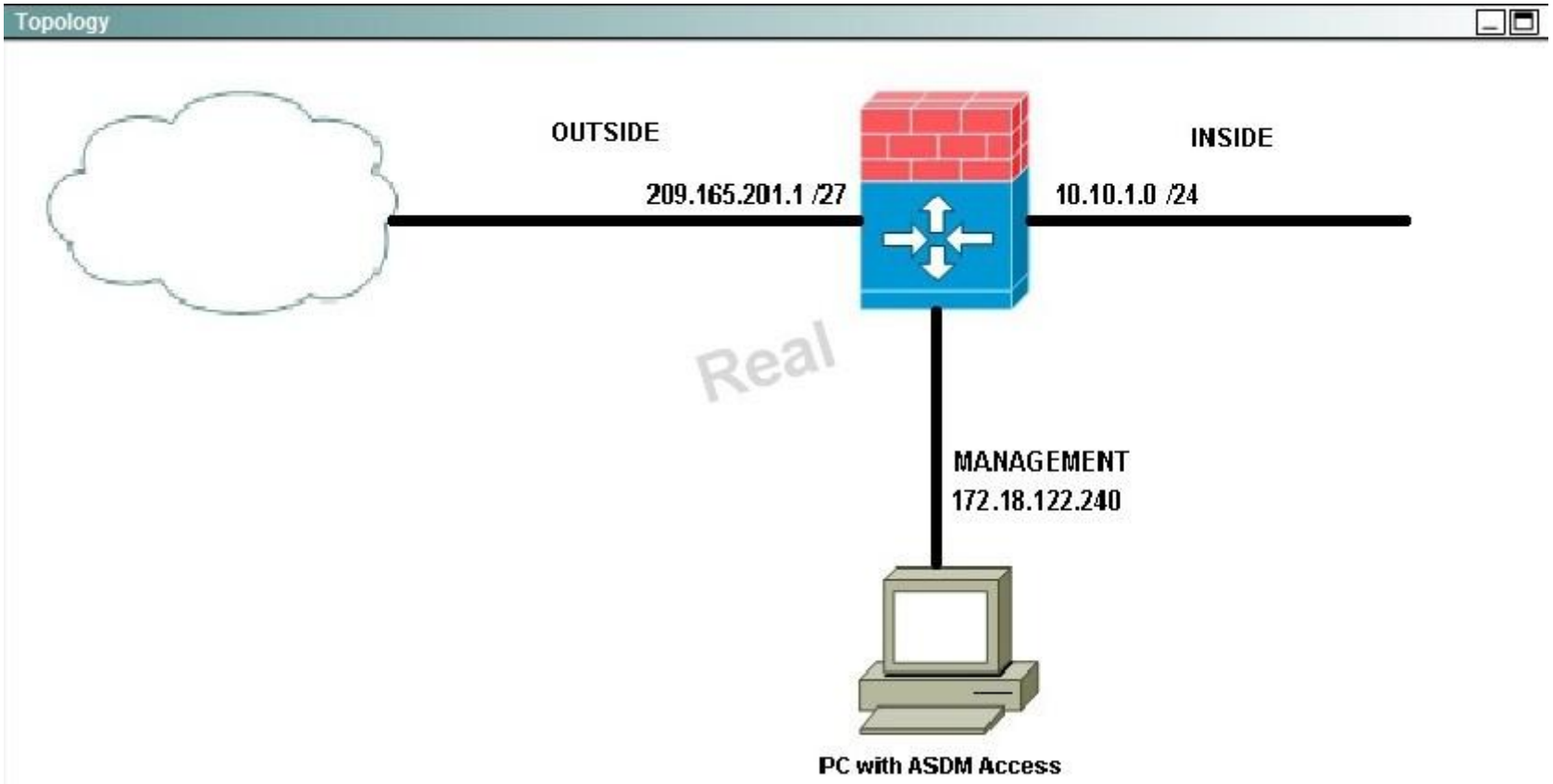
VCEplus.com



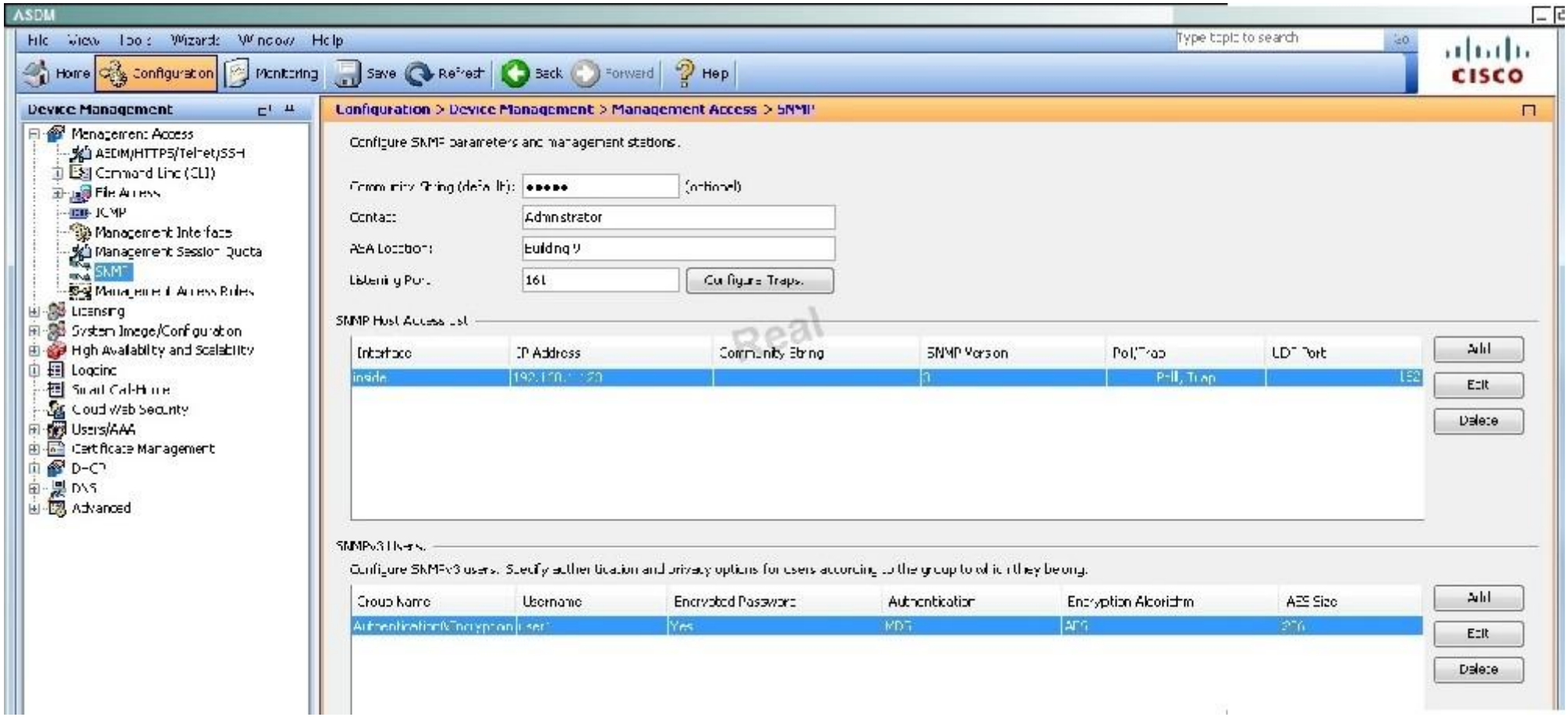
QUESTION 51



Real 32
Cisco 300-206 Exam



www.vceplus.com - Website designed to help IT pros advance their careers.



An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMFV3 hosts, which option must you configure in addition to the target IP address?

A. the Cisco ASA as a DHCP server, so the SNMFV3 host can obtain an IP address
B. a username, because traps are only sent to a configured user
C. SSH, so the user can connect to the Cisco ASA
D. the Cisco ASA with a dedicated interface only for SNMP, to process the SNMP host traffic.

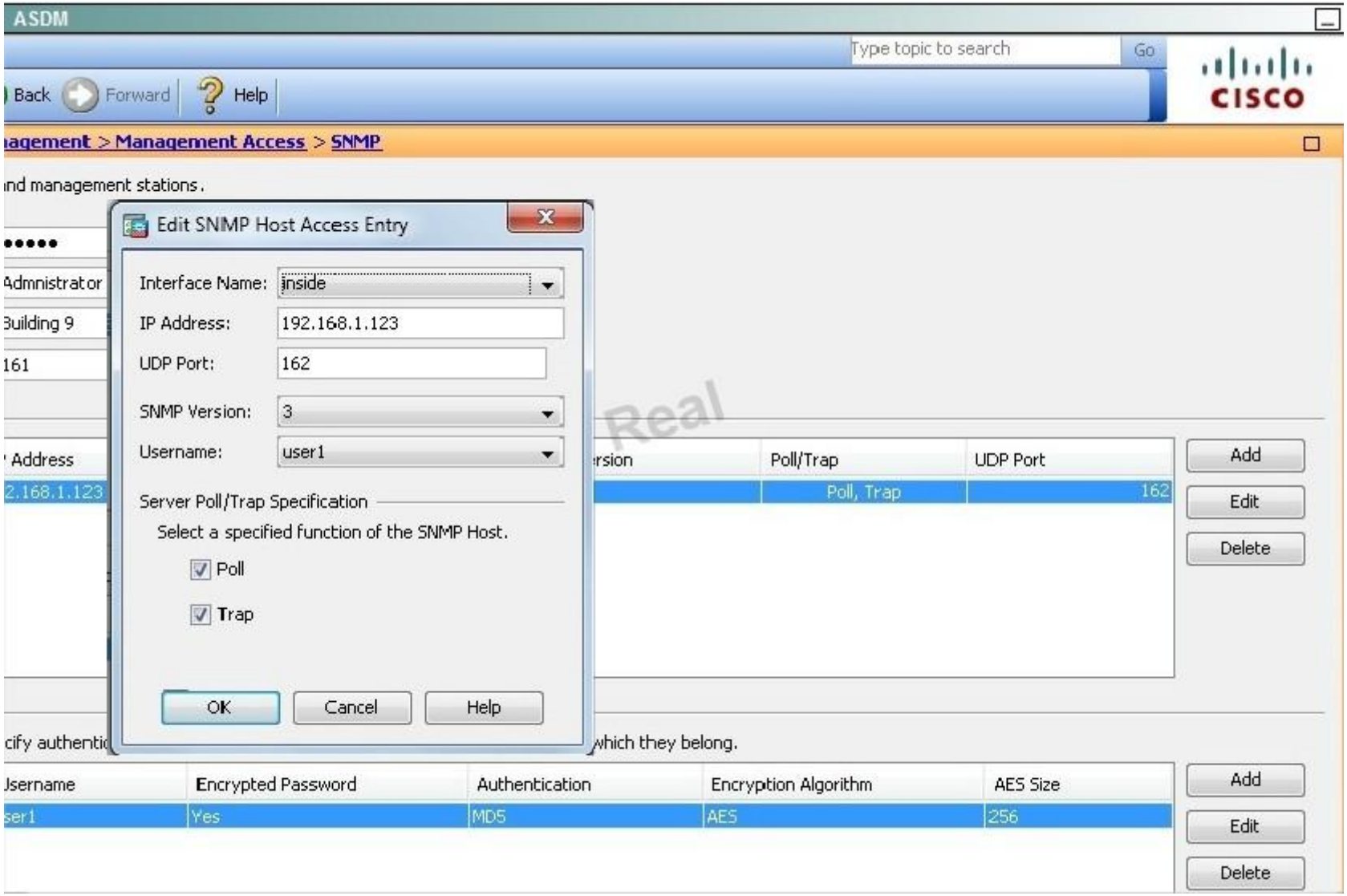
Correct Answer: B

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:
Explanation: The username can be seen here on the ASDM simulator screen shot:

Real 33
Cisco 300-206 Exam



QUESTION 52
Enabling what security mechanism can prevent an attacker from gaining network topology information from CDP via a man-in-the-middle attack?

A. MACsec
B. Flex VPN
C. Control Plane Protection
D. Dynamic Arp Inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
perfectly answered.

QUESTION 53
On an ASA running version 9.0, which command is used to nest objects in a pre-existing group?

A. object-group
B. network group-object
C. object-group network
Real 34
Cisco 300-206 Exam
D. group-object

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
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
Section: (none)

VCEplus.com

Explanation

Explanation/Reference:
Explanation:

QUESTION 55
What is the default behavior of an access list on a Cisco ASA?

A. It will permit or deny traffic based on the access list criteria.
B. It will permit or deny all traffic on a specified interface.
C. It will have no affect until applied to an interface, tunnel-group or other traffic flow.
D. It will allow all traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
When configuring a new context on a Cisco ASA device, which command creates a domain for the context?

A. domain config name
B. domain-name
C. changeto/domain name change
Real 35
Cisco 300-206 Exam
D. domain context 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which statement describes the correct steps to enable Botnet Traffic Filtering on a Cisco ASA version 9.0 transparent-mode firewall with an active Botnet Traffic Filtering license?

A. Enable DNS snooping, traffic classification, and actions.
B. Botnet Traffic Filtering is not supported in transparent mode.
C. Enable the use of the dynamic database, enable DNS snooping, traffic classification, and actions.
D. Enable the use of dynamic database, enable traffic classification and actions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Which Cisco switch technology prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast flood on a port?

A. port security
B. storm control
C. dynamic ARP inspection
D. BPDU guard
E. root guard
F. dot1x

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
You are a security engineer at a large multinational retailer. Your Chief Information Officer recently attended a security conference and has asked you to secure the network infrastructure from VLAN hopping.

Real 36
Cisco 300-206 Exam

Which statement describes how VLAN hopping can be avoided?

A. There is no such thing as VLAN hopping because VLANs are completely isolated.
B. VLAN hopping can be avoided by using IEEE 802.1X to dynamically assign the access VLAN to all endpoints and setting the default access VLAN to an unused VLAN ID.
C. VLAN hopping is avoided by configuring the native (untagged) VLAN on both sides of an ISL trunk to an unused VLAN ID.
D. VLAN hopping is avoided by configuring the native (untagged) VLAN on both sides of an IEEE 802.1Q trunk to an unused VLAN ID.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
real answer.

QUESTION 60
You are the administrator of a Cisco ASA 9.0 firewall and have been tasked with ensuring that the Firewall Admins Active Directory group has full access to the ASA configuration. The Firewall Operators Active Directory group should have a more limited level of access.

Which statement describes how to set these access levels?

A. Use Cisco Directory Agent to configure the Firewall Admins group to have privilege level 15 access. Also configure the Firewall Operators group to have privilege level 6 access.
B. Use TACACS+ for Authentication and Authorization into the Cisco ASA CLI, with ACS as the AAA server. Configure ACS CLI command authorization sets for the Firewall Operators group.
Configure level 15 access to be assigned to members of the Firewall Admins group.
C. Use RADIUS for Authentication and Authorization into the Cisco ASA CLI, with ACS as the AAA server. Configure ACS CLI command authorization sets for the Firewall Operators group.
Configure level 15 access to be assigned to members of the Firewall Admins group.
D. Active Directory Group membership cannot be used as a determining factor for accessing the Cisco ASA CLI.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
A router is being enabled for SSH command line access.

www.vceplus.com - Website designed to help IT pros advance their careers.

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Which two configurations are necessary to enable password-less SSH login to an IOS router? (Choose two.)

A. Enter a copy of the administrator's public key within the SSH key-chain
B. Enter a copy of the administrator's private key within the SSH key-chain
C. Generate a 512-bit RSA key to enable SSH on the router
D. Generate an RSA key of at least 768 bits to enable SSH on the router
E. Generate a 512-bit ECDSA key to enable SSH on the router
F. Generate a ECDSA key of at least 768 bits to enable SSH on the router

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Which two features does Cisco Security Manager provide? (Choose two.)

A. Configuration and policy deployment before device discovery
B. Health and performance monitoring
Real 38
Cisco 300-206 Exam
C. Event management and alerting
D. Command line menu for troubleshooting
E. Ticketing management and tracking

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
An administrator installed a Cisco ASA that runs version 9.1. You are asked to configure the firewall through Cisco ASDM.

When you attempt to connect to a Cisco ASA with a default configuration, which username and password grants you full access?

A. admin / admin
B. asaAdmin / (no password)
C. It is not possible to use Cisco ASDM until a username and password are created via the username usernamepassword password CLI command.
D. enable_15 / (no password)
E. cisco / cisco

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
best suitable answer.

QUESTION 65
Which three options are default settings for NTP parameters on a Cisco ASA? (Choose three.)

VCEplus.com

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 39
Cisco 300-206 Exam

QUESTION 66
Which two options are purposes of the packet-tracer command? (Choose two.)

A. to filter and monitor ingress traffic to a switch
B. to configure an interface-specific packet trace
C. to simulate network traffic through a data path
D. to debug packet drops in a production network
E. to automatically correct an ACL entry in an ASA

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
Which security operations management best practice should be followed to enable appropriate network access for administrators?

Real 44
Cisco 300-206 Exam

A. Provide full network access from dedicated network administration systems
B. Configure the same management account on every network device
C. Dedicate a separate physical or logical plane for management traffic
D. Configure switches as terminal servers for secure device access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
Which two features block traffic that is sourced from non-topological IPv6 addresses? (Choose two.)

A. DHCPv6 Guard
B. IPv6 Prefix Guard
C. IPv6 RA Guard
D. IPv6 Source Guard

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
Which three options correctly identify the Cisco ASA1000V Cloud Firewall? (Choose three.)

A. operates at Layer 2
B. operates at Layer 3
C. secures tenant edge traffic
D. secures intraswitch traffic
E. secures data center edge traffic
F. replaces Cisco VSG
G. complements Cisco VSG

H. requires Cisco VSG

Correct Answer: BCG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Real 45
Cisco 300-206 Exam
Which two SNMPv3 features ensure that SNMP packets have been sent securely? (Choose two.)

A. host authorization
B. authentication
C. encryption
D. compression

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Which two statements about zone-based firewalls are true? (Choose two.)

A. More than one interface can be assigned to the same zone.
B. Only one interface can be in a given zone.
C. An interface can only be in one zone.
D. An interface can be a member of multiple zones.
E. Every device interface must be a member of a zone.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
An attacker has gained physical access to a password protected router. Which command will prevent access to the startup-config in NVRAM?

A. no service password-recovery
B. no service startup-config
C. service password-encryption
D. no confreg 0x2142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
Real 46
Cisco 300-206 Exam
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
Section: (none)
Explanation

Explanation/Reference:
definite answer.

QUESTION 74
Which configuration keyword will configure SNMPv3 with authentication but no encryption?

A. Auth

B. Priv
C. No auth
D. Auth priv

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
In IOS routers, what configuration can ensure both prevention of ntp spoofing and accurate time ensured?

A. ACL permitting udp 123 from ntp server
B. ntp authentication
C. multiple ntp servers
D. local system clock

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
Which product can manage licenses, updates, and a single signature policy for 15 separate IPS

Real 47
Cisco 300-206 Exam
appliances?

A. Cisco Security Manager
B. Cisco IPS Manager Express
C. Cisco IPS Device Manager
D. Cisco Adaptive Security Device Manager

Correct Answer: A

VCEplus.com

Section: (none)
Explanation

Explanation/Reference:
appropriate answer.

QUESTION 77
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
When you set a Cisco IOS Router as an SSH server, which command specifies the RSA public key of the remote peer when you set the SSH server to perform RSA-based authentication?

A. router(config-ssh-pubkey-user)#key
B. router(conf-ssh-pubkey-user)#key-string
C. router(config-ssh-pubkey)#key-string
D. router(conf-ssh-pubkey-user)#key-string enable ssh

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Real 48

QUESTION 79

Instructions

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

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

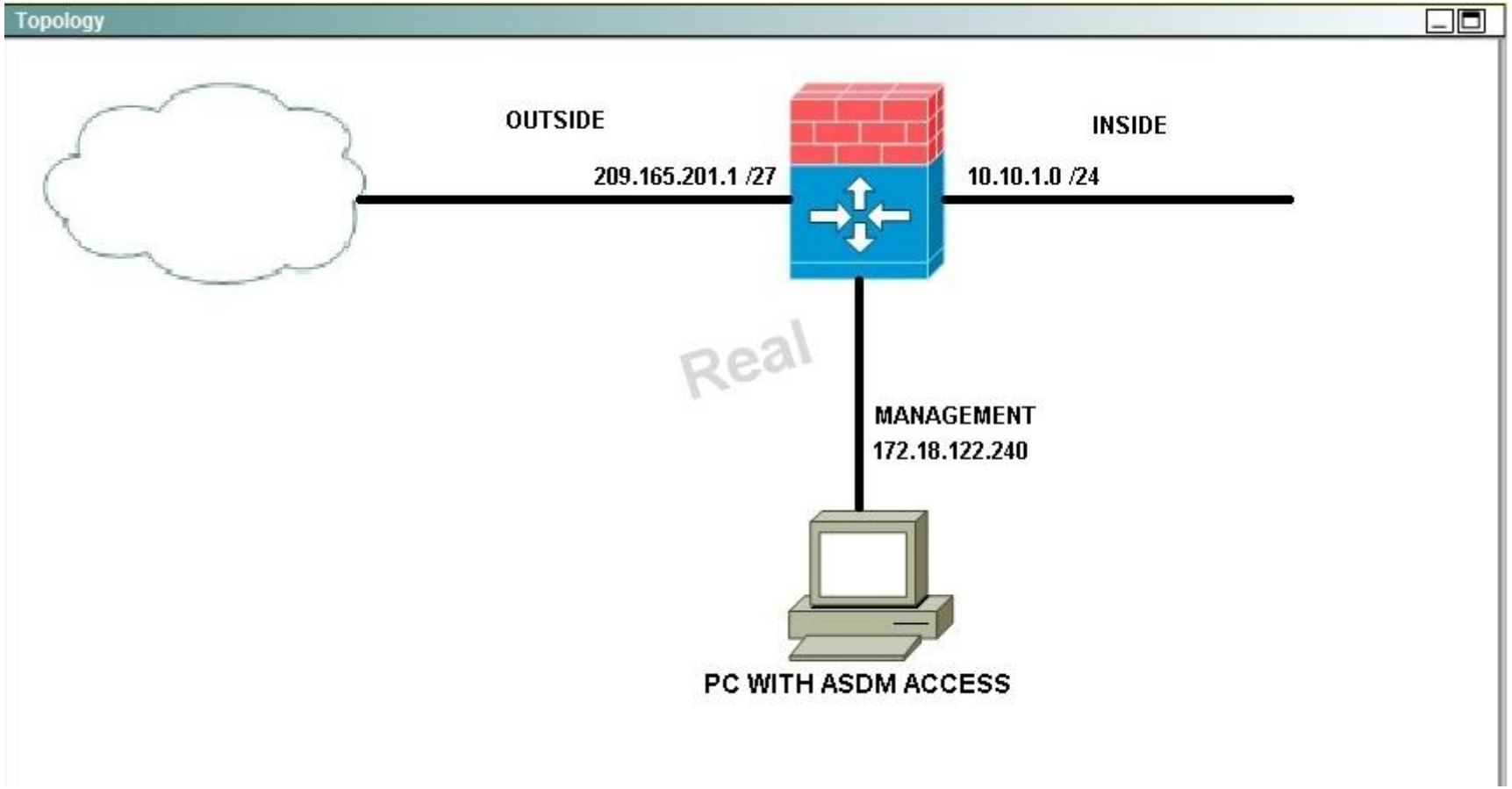
You have been given access to a Cisco ASA 5512 Adaptive Security Appliance via Cisco ASDM. Use Cisco ASDM to edit the Cisco ASA 5505 Adaptive Security Appliance configurations to enable Advanced HTTP application inspection by completing the following tasks:

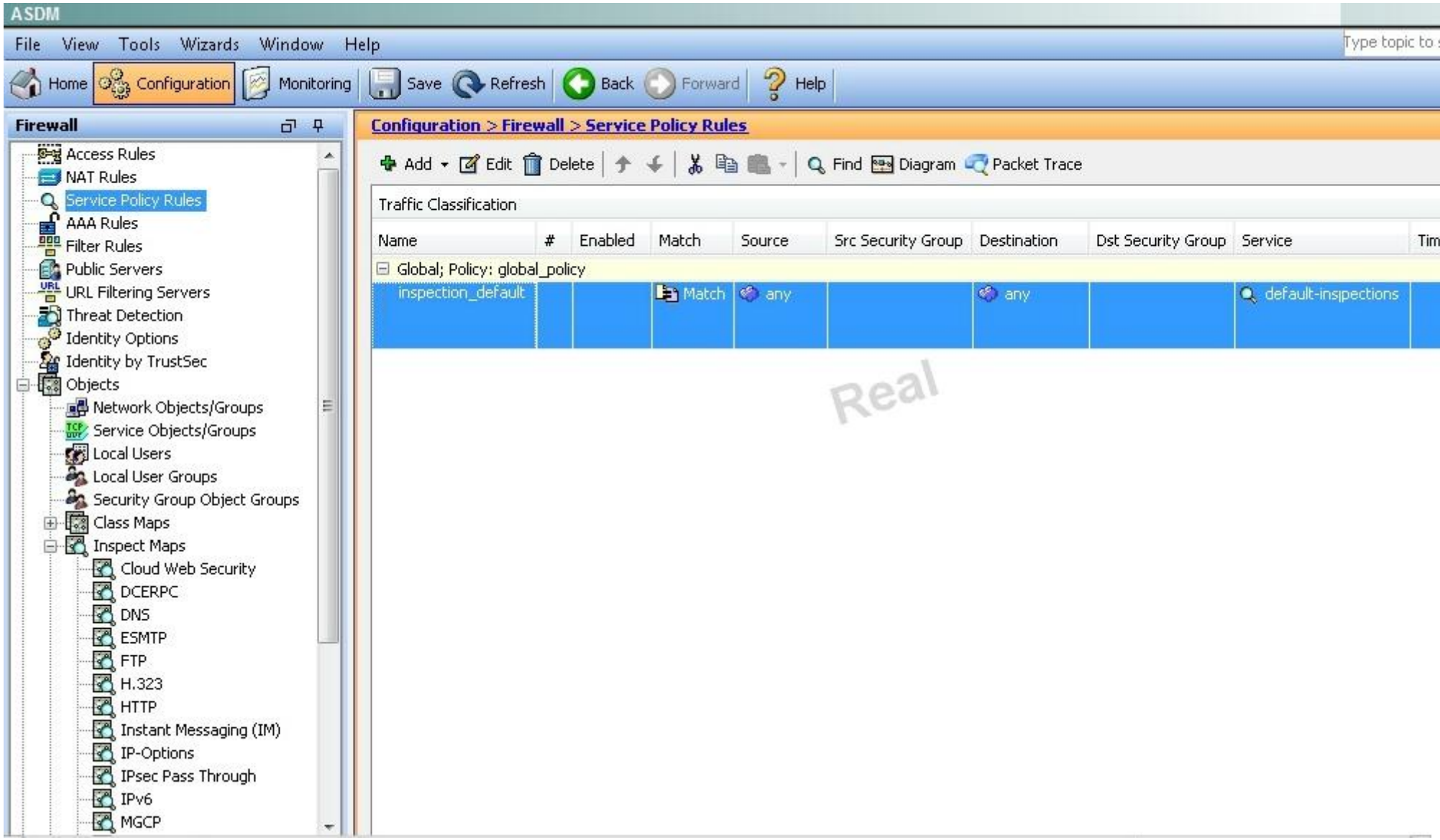
Real

Starting from the Service Policy Rules ASDM pane,

- Enable HTTP inspection globally on the Cisco ASA appliance
- Create a new HTTP Inspect Map named: **http-inspect-map** to:
  - Enable the *dropping* of any HTTP connections that encounter HTTP protocol violations
  - Enable the *dropping and logging* of any HTTP connections when the content type in the HTTP response does not match one of the MIME types in the accept field of the HTTP request

Note: After you complete the configuration, you do not need to save the running configuration to the startup-config. In this simulation, you cannot test the HTTP inspection policy that was created after you completed your configuration. Not all ASDM screens are fully functional. However, you should be able to view, edit, and delete the HTTP inspect map that you created from the **Configuration > Firewall > Objects > Inspect Maps > HTTP** ASDM screen.


Topology
OUTSIDE
INSIDE
209.165.201.1 /27
10.10.1.0 /24
Real
MANAGEMENT
172.18.122.240
PC WITH ASDM ACCESS



Correct Answer: Please check the steps in explanation part below:
Section: (none)

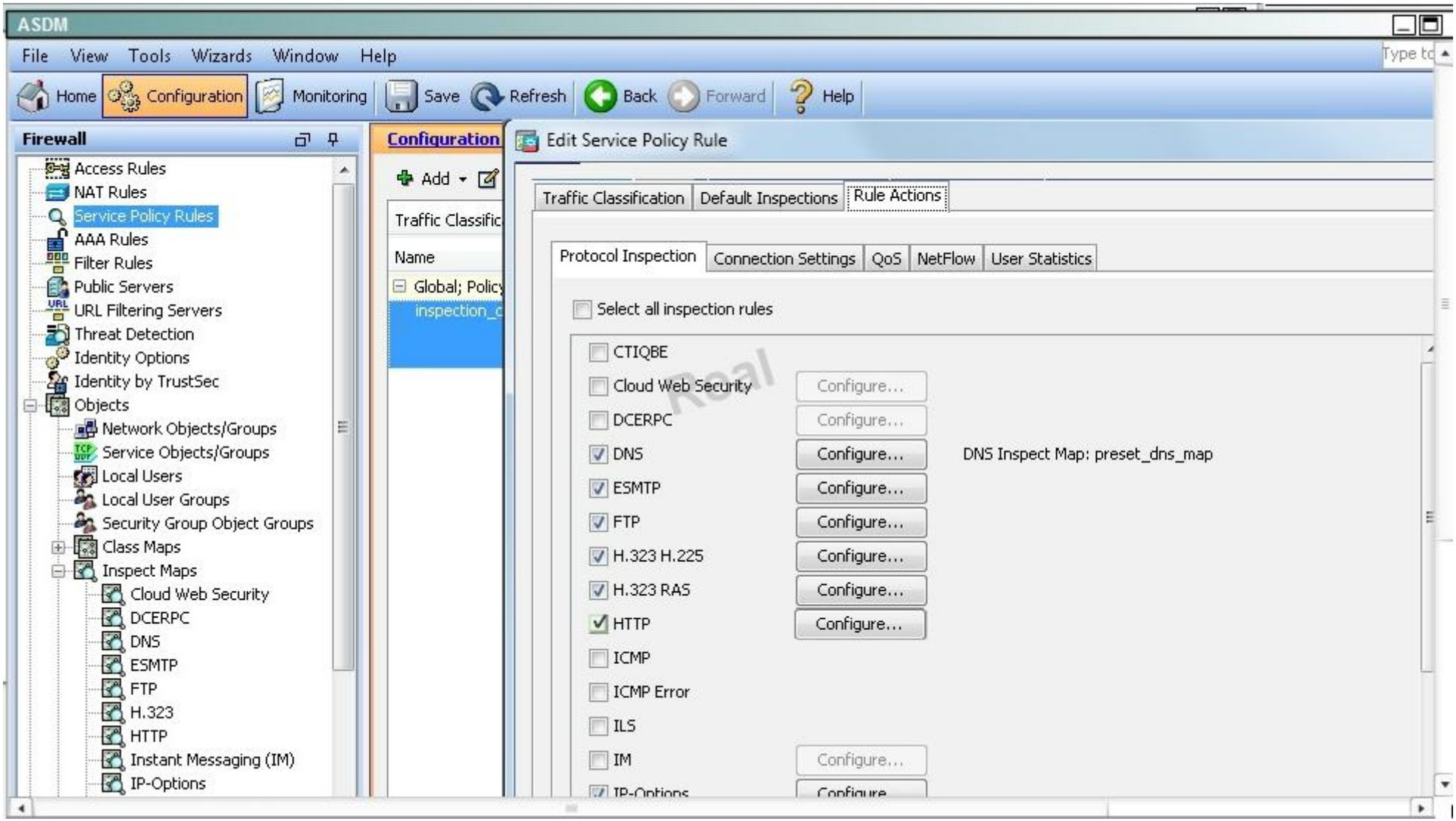
VCEplus.com

Explanation

Explanation/Reference:

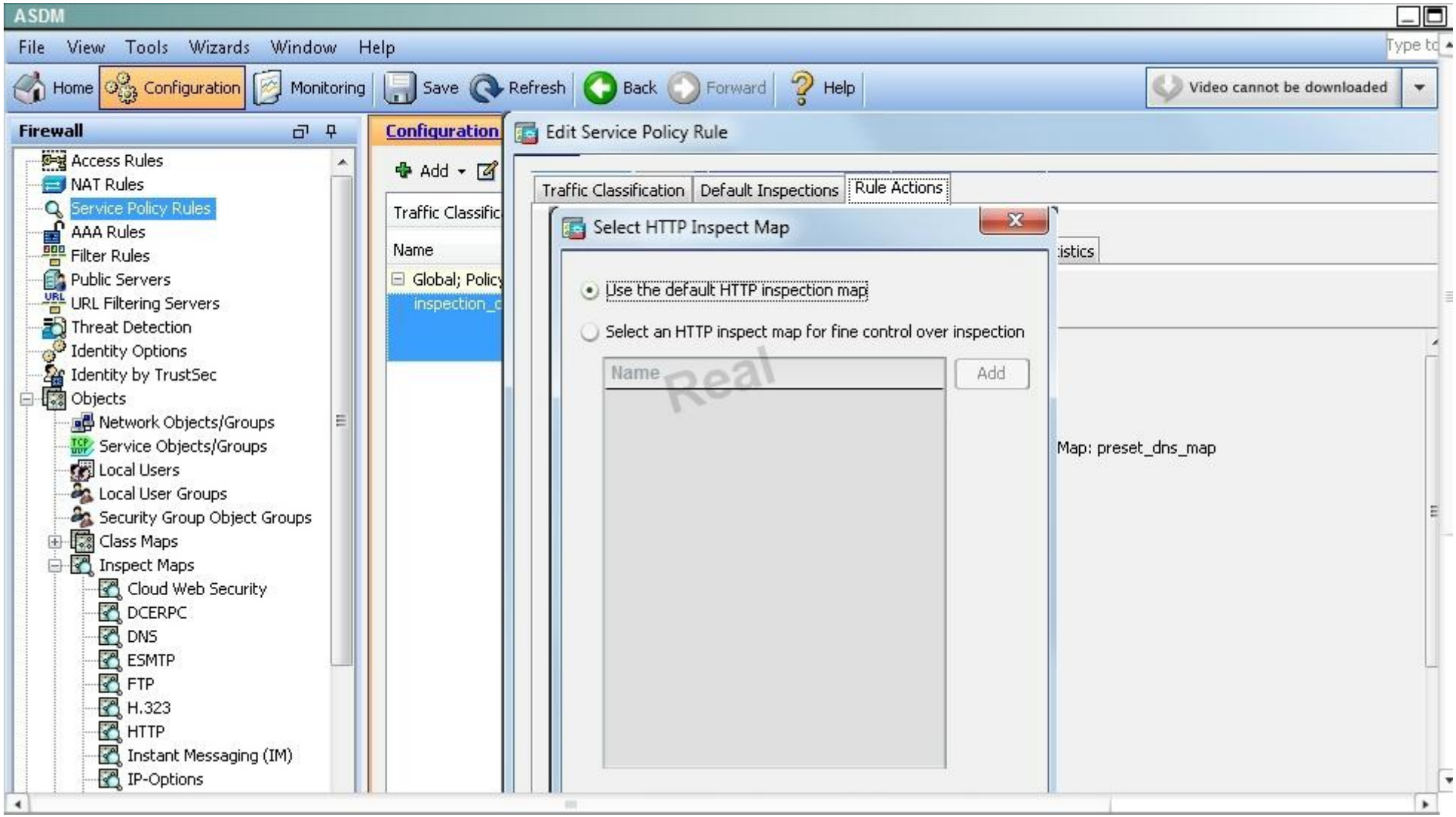
Explanation:

1) Click on Service Policy Rules, then Edit the default inspection rule.
2) Click on Rule Actions, then enable HTTP as shown here:

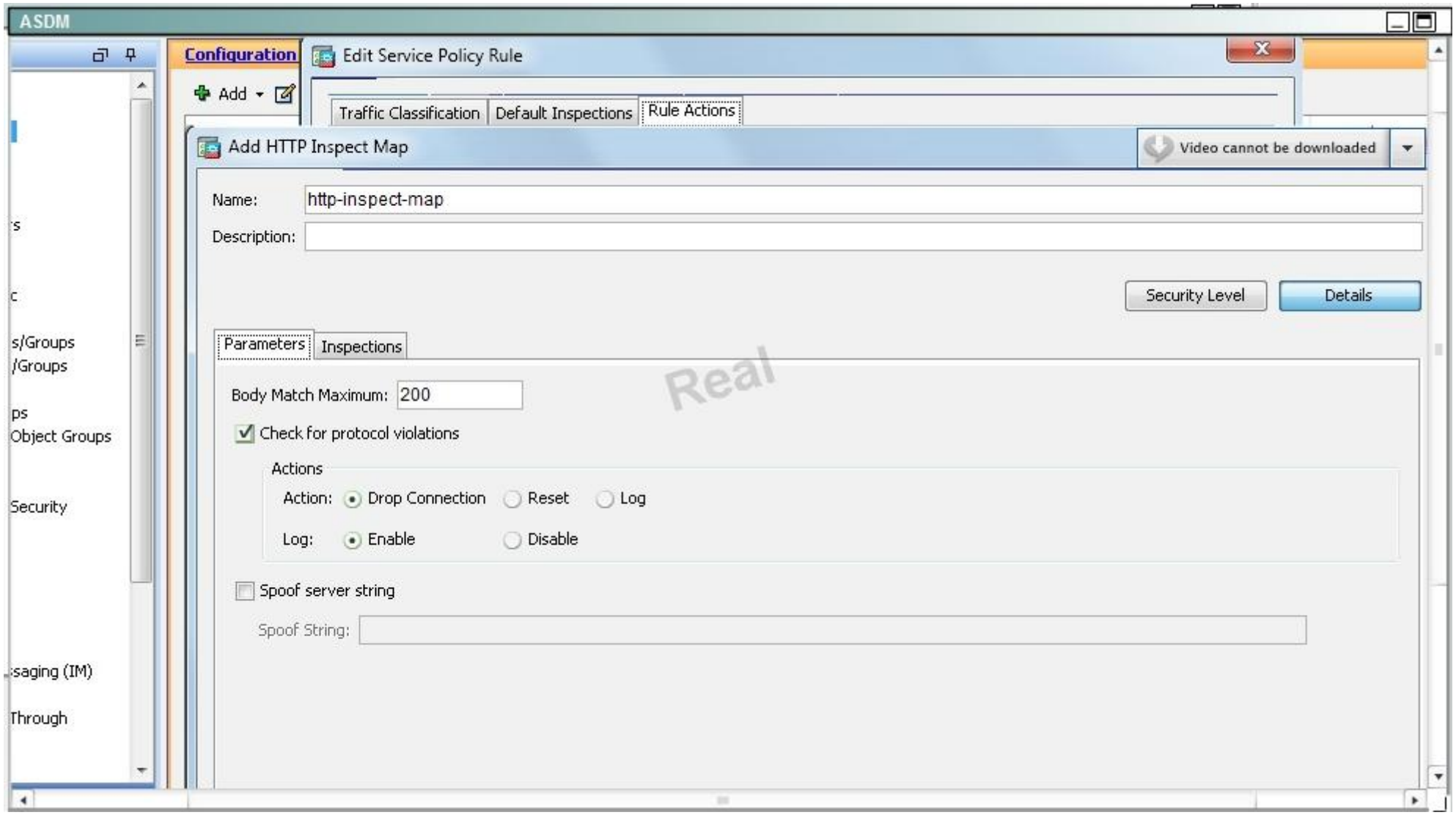


3) Click on Configure, then add as shown here:

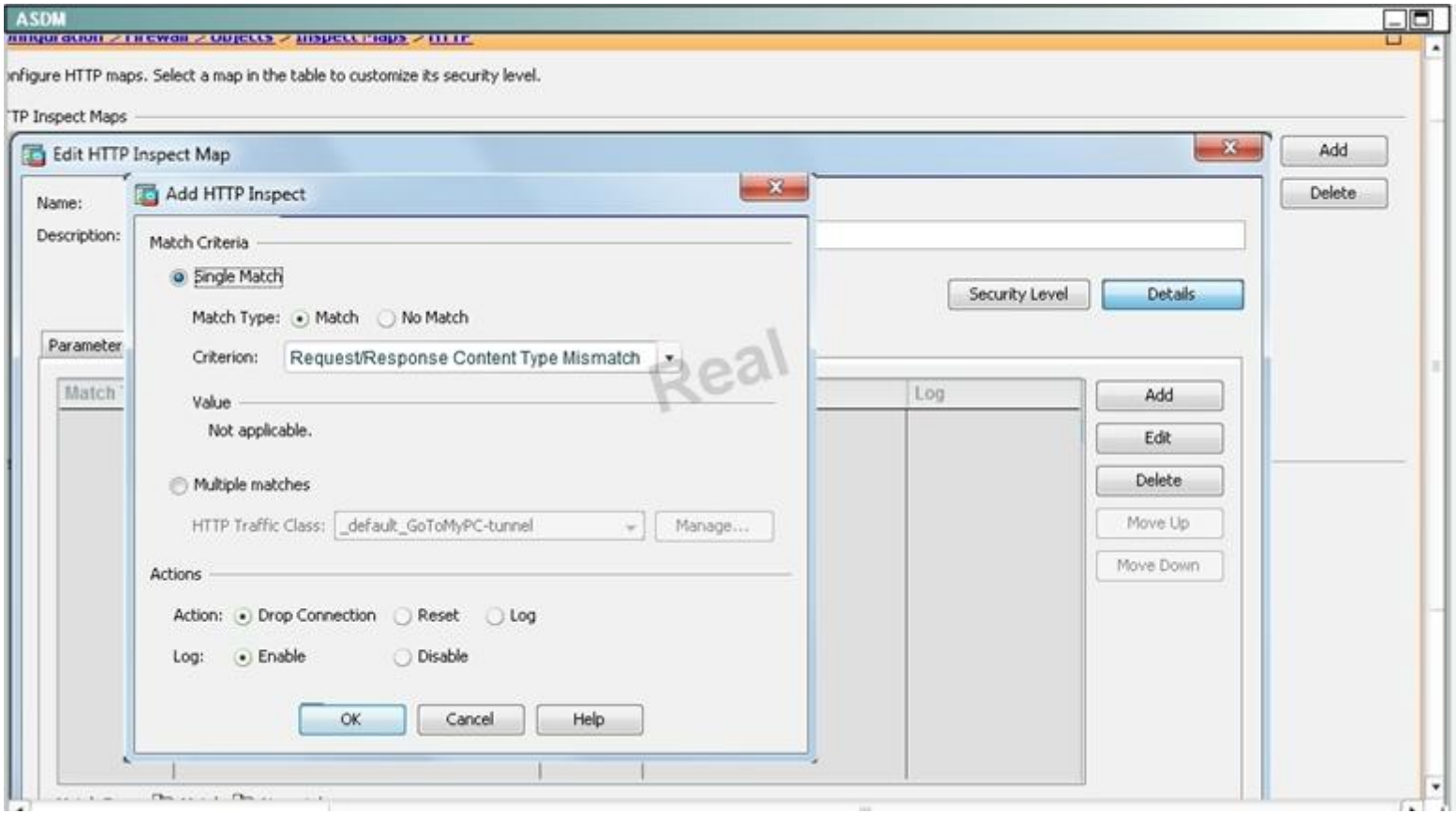
VCEplus.com



4) Create the new map in ASDM like shown:



5) Edit the policy as shown:



6) Hit OK

QUESTION 80
A switch is being configured at a new location that uses statically assigned IP addresses. Which will ensure that ARP inspection works as expected?

A. Configure the 'no-dhcp' keyword at the end of the ip arp inspection command
B. Enable static arp inspection using the command 'ip arp inspection static vlan vlan-number
C. Configure an arp access-list and apply it to the ip arp inspection command
D. Enable port security

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Real 2
Cisco 300-206 Exam

Explanation:

QUESTION 81
Which of the following would need to be created to configure an application-layer inspection of SMTP traffic operating on port 2525?

A. A class-map that matches port 2525 and applying an inspect ESMTP policy-map for that class in the global inspection policy
B. A policy-map that matches port 2525 and applying an inspect ESMTP class-map for that policy
C. An access-list that matches on TCP port 2525 traffic and applying it on an interface with the inspect option
D. A class-map that matches port 2525 and applying it on an access-list using the inspect option

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
right answer.

QUESTION 82
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VCEplus.com

QUESTION 83
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
Real 3
Cisco 300-206 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
What is the default behavior of an access list on the Cisco ASA security appliance?

A. It will permit or deny traffic based on the access-list criteria.
B. It will permit or deny all traffic on a specified interface.
C. An access group must be configured before the access list will take effect for traffic control.
D. It will allow all traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

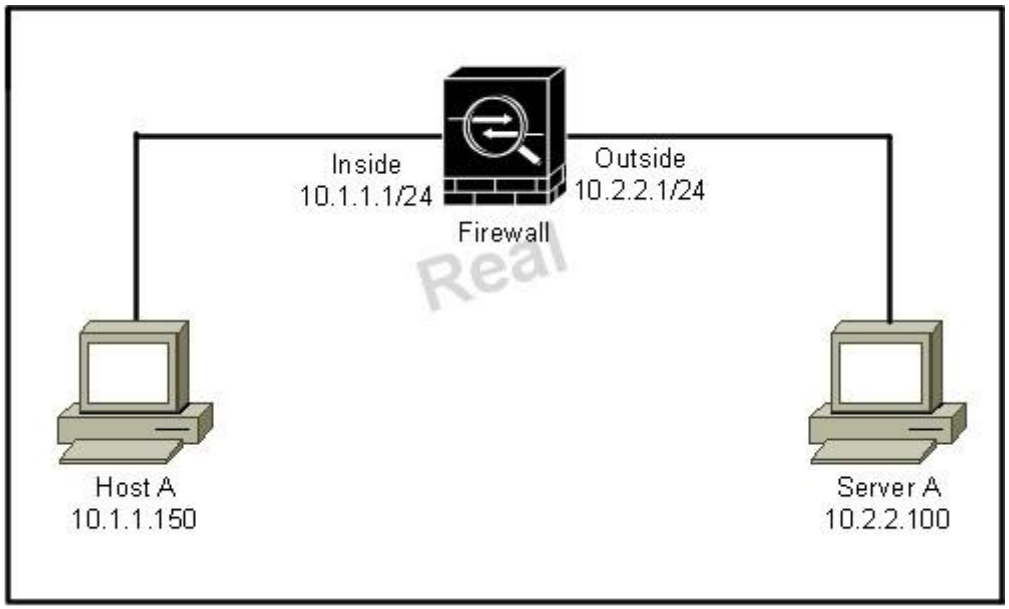
QUESTION 85
What is the default behavior of NAT control on Cisco ASA Software Version 8.3?

A. NAT control has been deprecated on Cisco ASA Software Version 8.3.
B. It will prevent traffic from traversing from one enclave to the next without proper access configuration.
C. It will allow traffic to traverse from one enclave to the next without proper access configuration.
D. It will deny all traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
Refer to the exhibit.



Server A is a busy server that offers these services:

· World Wide Web

· DNS

Real 40
Cisco 300-206 Exam
Which command captures http traffic from Host A to Server A?

A. capture traffic match udp host 10.1.1.150 host 10.2.2.100
B. capture traffic match 80 host 10.1.1.150 host 10.2.2.100
C. capture traffic match ip 10.2.2.0 255.255.255.192 host 10.1.1.150
D. capture traffic match tcp host 10.1.1.150 host 10.2.2.100
E. capture traffic match tcp host 10.2.2.100 host 10.1.1.150 eq 80

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
Your company is replacing a high-availability pair of Cisco ASA 5550 firewalls with the newer Cisco ASA 5555-X models. Due to budget constraints, one Cisco ASA 5550 will be replaced at a time.

Which statement about the minimum requirements to set up stateful failover between these two firewalls is true?

A. You must install the USB failover cable between the two Cisco ASAs and provide a 1 Gigabit Ethernet interface for state exchange.
B. It is not possible to use failover between different Cisco ASA models.
C. You must have at least 1 Gigabit Ethernet interface between the two Cisco ASAs for state exchange.
D. You must use two dedicated interfaces. One link is dedicated to state exchange and the other link is for heartbeats.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
In which two modes is zone-based firewall high availability available? (Choose two.)

A. IPv4 only
B. IPv6 only
C. IPv4 and IPv6
D. routed mode only

VCEplus.com

E. transparent mode only
F. both transparent and routed modes

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
You are the administrator of a multicontext transparent-mode Cisco ASA that uses a shared interface that belongs to more than one context. Because the same interface will be used within all three contexts, which statement describes how you will ensure that return traffic will reach the correct context?

A. Interfaces may not be shared between contexts in routed mode.
B. Configure a unique MAC address per context with the no mac-address auto command.
C. Configure a unique MAC address per context with the mac-address auto command.
D. Use static routes on the Cisco ASA to ensure that traffic reaches the correct context.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
A rogue device has connected to the network and has become the STP root bridge, which has caused a network availability issue.

Which two commands can protect against this problem? (Choose two.)

A. switch(config)#spanning-tree portfast bpduguard default
B. switch(config)#spanning-tree portfast bpdufilter default
C. switch(config-if)#spanning-tree portfast
D. switch(config-if)#spanning-tree portfast disable
E. switch(config-if)#switchport port-security violation protect

F. switch(config-if)#spanning-tree port-priority 0

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 42
Cisco 300-206 Exam

QUESTION 91
According to Cisco best practices, which two interface configuration commands help prevent VLAN hopping attacks? (Choose two.)

A. switchport mode access
B. switchport access vlan 2
C. switchport mode trunk
D. switchport access vlan 1
E. switchport trunk native vlan 1
F. switchport protected

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
When it is configured in accordance to Cisco best practices, the switchport port-security maximum command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation
D. MAC spoofing
E. CAM attacks

F. IP spoofing

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

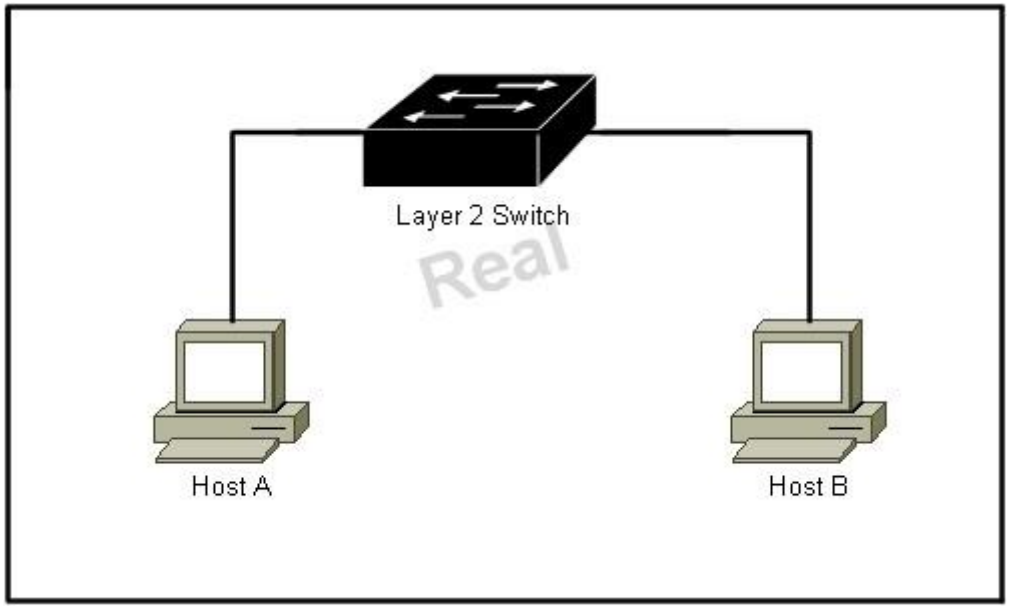
QUESTION 93
When configured in accordance to Cisco best practices, the ip verify source command can mitigate which two types of Layer 2 attacks? (Choose two.)

A. rogue DHCP servers
B. ARP attacks
C. DHCP starvation
D. MAC spoofing
E. CAM attacks
F. IP spoofing
Real 43
Cisco 300-206 Exam

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
fine answer.

QUESTION 94
Refer to the exhibit.



To protect Host A and Host B from communicating with each other, which type of PVLAN port should be used for each host?

A. Host A on a promiscuous port and Host B on a community port
B. Host A on a community port and Host B on a promiscuous port
C. Host A on an isolated port and Host B on a promiscuous port
D. Host A on a promiscuous port and Host B on a promiscuous port
E. Host A on an isolated port and host B on an isolated port
F. Host A on a community port and Host B on a community port

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
What is the default log level on the Cisco Web Security Appliance?

A. Trace
B. Debug
C. Informational
D. Critical

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
Which command sets the source IP address of the NetFlow exports of a device?

A. ip source flow-export
B. ip source netflow-export
C. ip flow-export source
D. ip netflow-export source

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
best suitable answer.

QUESTION 97
Which two SNMPv3 features ensure that SNMP packets have been sent securely?" Choose two.

Real 12
Cisco 300-206 Exam

A. host authorization
B. authentication
C. encryption
D. compression

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
Which three logging methods are supported by Cisco routers? (Choose three.)

A. console logging
B. TACACS+ logging
C. terminal logging
D. syslog logging
E. ACL logging
F. RADIUS logging

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
appropriate answer.

QUESTION 99
Which three options are default settings for NTP parameters on a Cisco device? (Choose three.)

A. NTP authentication is enabled.
B. NTP authentication is disabled.
C. NTP logging is enabled.
D. NTP logging is disabled.
E. NTP access is enabled.
F. NTP access is disabled.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 100
Which two parameters must be configured before you enable SCP on a router? (Choose two.)

Real 13
Cisco 300-206 Exam

A. SSH
B. authorization
C. ACLs
D. NTP
E. TACACS+

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 101
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
When a Cisco ASA is configured in transparent mode, how can ARP traffic be controlled?

A. By enabling ARP inspection; however, it cannot be controlled by an ACL
B. By enabling ARP inspection or by configuring ACLs
C. By configuring ACLs; however, ARP inspection is not supported
D. By configuring NAT and ARP inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is true.

QUESTION 103
What are two primary purposes of Layer 2 detection in Cisco IPS networks? (Choose two.)

A. identifying Layer 2 ARP attacks
Real 17
Cisco 300-206 Exam
B. detecting spoofed MAC addresses and tracking 802.1X actions and data communication after a successful client association
C. detecting and preventing MAC address spoofing in switched environments
D. mitigating man-in-the-middle attacks

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
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

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
What are two reasons to implement Cisco IOS MPLS Bandwidth-Assured Layer 2 Services? (Choose two.)

A. guaranteed bandwidth and peak rates as well as low cycle periods, regardless of which systems access the device
B. increased resiliency through MPLS FRR for AToM circuits and better bandwidth utilization through MPLS TE
C. enabled services over an IP/MPLS infrastructure, for enhanced MPLS Layer 2 functionality
D. provided complete proactive protection against frame and device spoofing

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
What is the maximum jumbo frame size for IPS standalone appliances with 1G and 10G fixed or

Real 18
Cisco 300-206 Exam
add-on interfaces?

A. 1024 bytes
B. 1518 bytes
C. 2156 bytes
D. 9216 bytes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
Which two statements about Cisco IDS are true? (Choose two.)

A. It is preferred for detection-only deployment.
B. It is used for installations that require strong network-based protection and that include sensor tuning.
C. It is used to boost sensor sensitivity at the expense of false positives.
D. It is used to monitor critical systems and to avoid false positives that block traffic.
E. It is used primarily to inspect egress traffic, to filter outgoing threats.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
definite choice of answer.

QUESTION 108
What are two reasons for implementing NIPS at enterprise Internet edges? (Choose two.)

A. Internet edges typically have a lower volume of traffic and threats are easier to detect.
B. Internet edges typically have a higher volume of traffic and threats are more difficult to detect.
C. Internet edges provide connectivity to the Internet and other external networks.
D. Internet edges are exposed to a larger array of threats.
E. NIPS is more optimally designed for enterprise Internet edges than for internal network configurations.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 19
Cisco 300-206 Exam