

Cisco-210-260

Number: Cisco-210-260
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Sections

1. Sims
2. Multi Select
3. Normal

A

QUESTION 1

What type of packet creates and performs network operations on a network device?

- A. control plane packets
- B. data plane packets
- C. management plane packets
- D. services plane packets

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 2

What is an advantage of implementing a Trusted Platform Module for disk encryption?

- A. It provides hardware authentication.
- B. It allows the hard disk to be transferred to another device without requiring re- encryption.dis
- C. It supports a more complex encryption algorithm than other disk-encryption technologies.
- D. It can protect against single points of failure.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 3

In what type of attack does an attacker virtually change a device's burned-in address in an attempt to circumvent access lists and mask the device's true identity?

- A. gratuitous ARP
- B. ARP poisoning
- C. IP spoofing
- D. MAC spoofing

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 4

What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

- A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
- B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
- C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.
- D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59:00 local time on December 31, 2013.
- E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.
- F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 5

What type of algorithm uses the same key to encrypt and decrypt data?

- A. a symmetric algorithm
- B. an asymmetric algorithm
- C. a Public Key Infrastructure algorithm
- D. an IP security algorithm

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 6

What type of security support is provided by the Open Web Application Security Project?

- A. Education about common Web site vulnerabilities.
- B. A Web site security framework.
- C. A security discussion forum for Web site developers.
- D. Scoring of common vulnerabilities and exposures.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 7

What is one requirement for locking a wired or wireless device from ISE?

- A. The ISE agent must be installed on the device.
- B. The device must be connected to the network when the lock command is executed.
- C. The user must approve the locking action.
- D. The organization must implement an acceptable use policy allowing device locking.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 8

What is the FirePOWER impact flag used for?

- A. A value that indicates the potential severity of an attack.
- B. A value that the administrator assigns to each signature.
- C. A value that sets the priority of a signature.

D. A value that measures the application awareness.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 9

What mechanism does asymmetric cryptography use to secure data?

- A. a public/private key pair
- B. shared secret keys
- C. an RSA nonce
- D. an MD5 hash

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 10

Which statement about IOS privilege levels is true?

- A. Each privilege level supports the commands at its own level and all levels below it.
- B. Each privilege level supports the commands at its own level and all levels above it.
- C. Privilege-level commands are set explicitly for each user.
- D. Each privilege level is independent of all other privilege levels.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 11

Which Cisco product can help mitigate web-based attacks within a network?

- A. Adaptive Security Appliance
- B. Web Security Appliance
- C. Email Security Appliance
- D. Identity Services Engine

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 12

A proxy firewall protects against which type of attack?

- A. cross-site scripting attack
- B. worm traffic
- C. port scanning
- D. DDoS attacks

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 13

Refer to the exhibit.

```
crypto ikev1 policy 1
encryption aes
hash md5
authentication pre-share
group 2
lifetime 14400
```

What is the effect of the given command sequence?

- A. It configures IKE Phase 1.
- B. It configures a site-to-site VPN tunnel.
- C. It configures a crypto policy with a key size of 14400.
- D. It configures IPSec Phase 2.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 14

When an administrator initiates a device wipe command from the ISE, what is the immediate effect?

- A. It requests the administrator to choose between erasing all device data or only managed corporate data.
- B. It requests the administrator to enter the device PIN or password before proceeding with the operation.
- C. It notifies the device user and proceeds with the erase operation.
- D. It immediately erases all data on the device.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 15

What is an advantage of placing an IPS on the inside of a network?

- A. It can provide higher throughput.
- B. It receives traffic that has already been filtered.
- C. It receives every inbound packet.
- D. It can provide greater security.

Correct Answer: B

Section: Normal

Explanation**Explanation/Reference:****QUESTION 16**

What improvement does EAP-FASTv2 provide over EAP-FAST?

- A. It allows multiple credentials to be passed in a single EAP exchange.
- B. It supports more secure encryption protocols.
- C. It allows faster authentication by using fewer packets.
- D. It addresses security vulnerabilities found in the original protocol.

Correct Answer: A

Section: Normal

Explanation**Explanation/Reference:****QUESTION 17**

What type of attack was the Stuxnet virus?

- A. cyber warfare
- B. hacktivism
- C. botnet
- D. social engineering

Correct Answer: A

Section: Normal

Explanation**Explanation/Reference:****QUESTION 18**

Which statement about communication over failover interfaces is true?

- A. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default.
- B. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.

- C. All information that is sent over the failover and stateful failover interfaces is encrypted by default.
- D. User names, passwords, and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 19

Which sensor mode can deny attackers inline?

- A. IPS
- B. fail-close
- C. IDS
- D. fail-open

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 20

What is the only permitted operation for processing multicast traffic on zone-based firewalls?

- A. Only control plane policing can protect the control plane against multicast traffic.
- B. Stateful inspection of multicast traffic is supported only for the self-zone.
- C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
- D. Stateful inspection of multicast traffic is supported only for the internal zone.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 21

Which option is the most effective placement of an IPS device within the infrastructure?

- A. Inline, behind the internet router and firewall
- B. Inline, before the internet router and firewall
- C. Promiscuously, after the Internet router and before the firewall
- D. Promiscuously, before the Internet router and the firewall

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 22

Which statement about Cisco ACS authentication and authorization is true?

- A. ACS servers can be clustered to provide scalability.
- B. ACS can query multiple Active Directory domains.
- C. ACS uses TACACS to proxy other authentication servers.
- D. ACS can use only one authorization profile to allow or deny requests.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 23

An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

- A. The switch could offer fake DHCP addresses.
- B. The switch could become the root bridge.
- C. The switch could be allowed to join the VTP domain.
- D. The switch could become a transparent bridge.

Correct Answer: B

Section: Normal
Explanation

Explanation/Reference:

QUESTION 24

Which type of address translation should be used when a Cisco ASA is in transparent mode?

- A. Static NAT
- B. Dynamic NAT
- C. Overload
- D. Dynamic PAT

Correct Answer: A

Section: Normal
Explanation

Explanation/Reference:

QUESTION 25

Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

- A. aaa authentication enable console LOCAL SERVER_GROUP
- B. aaa authentication enable console SERVER_GROUP LOCAL
- C. aaa authentication enable console local
- D. aaa authentication enable console LOCAL

Correct Answer: D

Section: Normal
Explanation

Explanation/Reference:

QUESTION 26

What hash type does Cisco use to validate the integrity of downloaded images?

- A. Sha1

- B. Sha2
- C. Md5
- D. Md1

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 27

Which NAT option is executed first during in case of multiple NAT translations?

- A. Dynamic NAT with shortest prefix
- B. Dynamic NAT with longest prefix
- C. Static NAT with shortest prefix
- D. Static NAT with longest prefix

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 28

How can firepower block malicious email attachments?

- A. It forwards email requests to an external signature engine
- B. It sends the traffic through a file policy
- C. It scans inbound email messages for known bad URLs
- D. It sends an alert to the administrator to verify suspicious email messages

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 29

what PAT configuration command allows it to use the next IP in the dynamic pool instead of the next port?

- A. next IP
- B. round robin
- C. Dynamic rotation
- D. Dynamic PAT rotation

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

Exam B**QUESTION 1**

Scenario

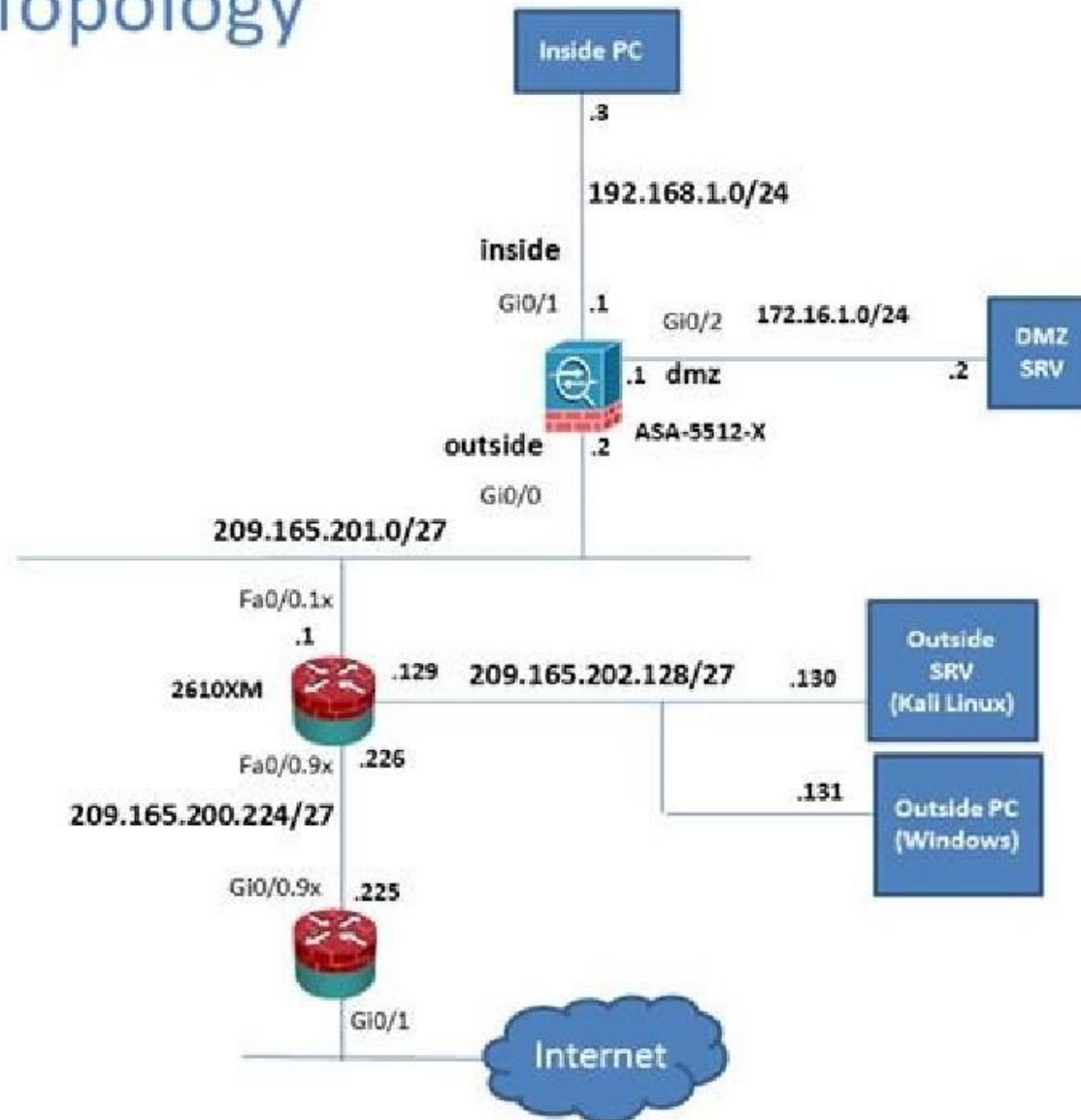
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to unexpand the expanded menu first.

Lab Topology



Which two statements regarding the ASA VPN configurations are correct? (Choose two)

- A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
- B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server Method.
- C. The Inside-SRV bookmark references the https://192.168.1.2 URL
- D. Only Clientless SSL VPN access is allowed with the Sales group policy
- E. AnyConnect, IPSec IKEv1, and IPSec IKEv2 VPN access is enabled on the outside interface
- F. The Inside-SRV bookmark has not been applied to the Sales group policy

Correct Answer: BD

Section: Sims

Explanation

Explanation/Reference:

Explanation:

For B:

Virtual Terminal

Connection Profiles

- Portal
 - Bookmarks
 - Client-Server Plug-ins
 - Customization
 - Help Customization
 - Portal Access Rules
 - Port Forwarding
 - Smart Tunnels
 - Web Contents
- VDI Access
- Group Policies
- Dynamic Access Policies
- Advanced
 - Encoding
 - Proxy Bypass
 - Proxies
 - Java Code Signer
 - Content Cache
 - Content Rewrite
 - Application Helper
 - Single Signon Servers
 - Microsoft KCD Server
 - Web ACLs

AAA/Local Users

Device Setup


Firewall

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>
inside	<input type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

- ☒ Allow user to select connection profile on the login page. 
- ☐ Allow user to enter internal password on the login page.
- ☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

 Add
  Edit
  Delete
 Find:

☐ Match Case

Name	Enabled	Aliases
DefaultRAGroup	<input checked="" type="checkbox"/>	
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	
clientless	<input checked="" type="checkbox"/>	test

For C, Navigate to the Bookmarks tab:

The screenshot shows the VCEplus Virtual Terminal interface. On the left, a tree view under 'Remote Access VPN' shows the navigation path: Introduction, Network (Client) Access, Clientless SSL VPN Access, Connection Profiles, Portal, and Bookmarks (highlighted). The main panel displays the 'Bookmarks' configuration page. It includes a breadcrumb trail: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The page text states: 'Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#).' Below this is a toolbar with icons for Add, Edit, Delete, Import, Export, and Assign. A table lists the configured bookmarks:

Bookmarks	Group Policies/D
Template	
Inside-SRV	Sales

Then hit "edit" and you will see this:



Edit Bookmark List

Bookmark List Name: Inside-SRV

Bookmark Title	URL
Inside Server	http://192.168.1.2

Find:



Match Case

Not A, as this is listed under the Identity Certificates, not the CA certificates:

Virtual Terminal

Remote Access VPN

Configuration > Remote Access VPN > Certificate Management > Identity Certificate

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
 - CA Certificates
 - Identity Certificates
 - Trusted Certificate Pool
 - Code Signer
 - Local Certificate Authority
 - CA Server
 - Manage User Database
 - Manage User Certificates
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

Issued To	Issued By	Expiry Date	Associated
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM

Find: ☐ Match Case

Certificate Expiration Alerts

Send the first alert before : (days)

Repeat Alert Interval : (days)

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital c

Note E:

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

- Introduction
- Network (Client) Access
 - AnyConnect Connection Profiles
 - AnyConnect Customization/L
 - AnyConnect Client Profile
 - AnyConnect Client Software
 - Dynamic Access Policies
 - Group Policies
 - IPsec(IKEv1) Connection Profiles
 - IPsec(IKEv2) Connection Profiles
 - Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users up to 1000. The VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS).

Access Interfaces

☐ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web L

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☒ Allow user to select connection profile on the login page. [?](#)

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You

QUESTION 2

Scenario

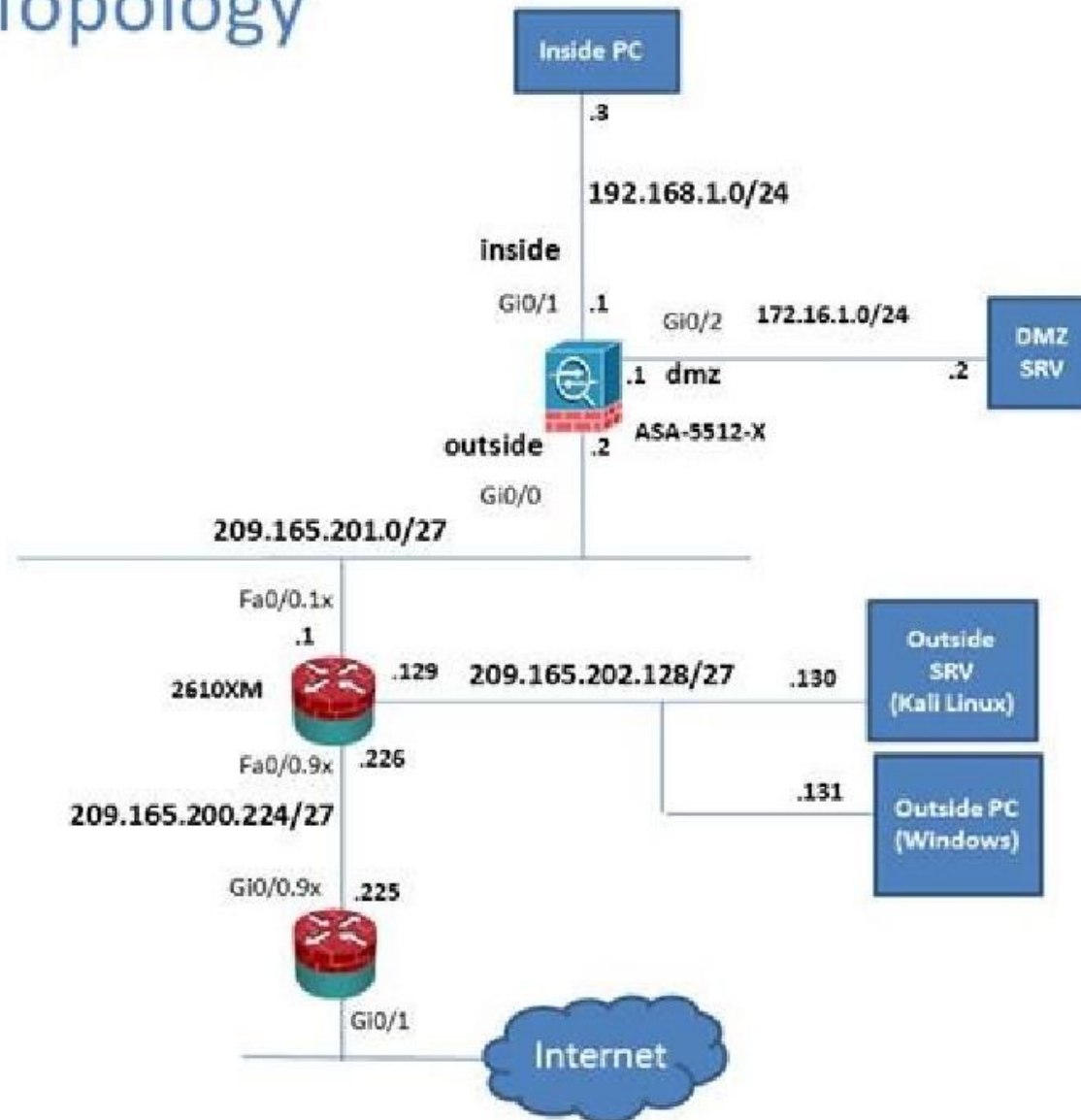
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to unexpand the expanded menu first.

Lab Topology



Which user authentication method is used when users login to the Clientless SSLVPN portal using <https://209.165.201.2/test?>

- A. AAA with LOCAL database
- B. AAA with RADIUS server
- C. Certificate
- D. Both Certificate and AAA with LOCAL database
- E. Both Certificate and AAA with RADIUS server

Correct Answer: A

Section: Sims

Explanation

Explanation/Reference:

Explanation:

This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used,

Virtual Terminal

Home
 Configuration
 Monitoring
 Save
 Refresh
 Back
 Forward
 Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
 - Connection Profiles
 - Portal
 - Bookmarks
 - Client-Server Plug-ins
 - Customization
 - Help Customization
 - Portal Access Rules
 - Port Forwarding
 - Smart Tunnels
 - Web Contents
- VDI Access
- Group Policies
- Dynamic Access Policies
- Advanced
 - Encoding
 - Proxy Bypass
 - Proxies
 - Java Code Signer
 - Content Cache
 - Content Rewrite
 - Application Helper
 - Single Signon Servers
 - Microsoft KCD Server
 - Web ACLs
- AAA/Local Users

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>
inside	<input type="checkbox"/>

Device Ca

Port Se

☒ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☒ Allow user to select connection profile on the login page.

☐ Allow user to enter internal password on the login page.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You

Add
 Edit
 Delete
 Find:
☐ Match Case

Name	Enabled	Aliases
DefaultRAGroup	<input checked="" type="checkbox"/>	
DefaultRAGroup	<input type="checkbox"/>	

QUESTION 3
CORRECT TEXT

Scenario

Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.

New additional connectivity requirements:

Once the correct ASA configurations have been configured:

To access ASDM, click the ASA icon in the topology diagram.

To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.

To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.

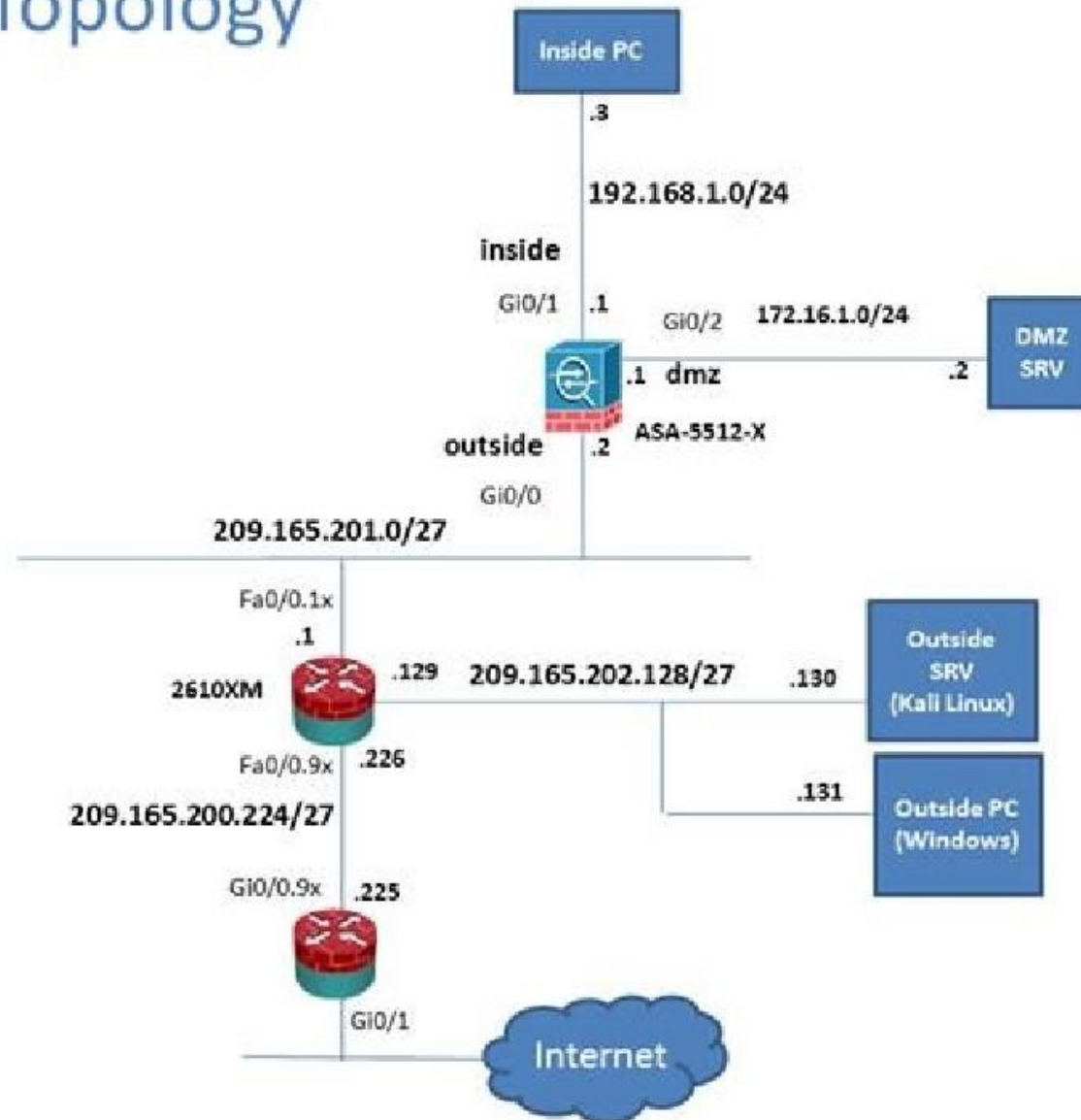
Note:

After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.

Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.

In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

Lab Topology



- A.
- B.
- C.
- D.

Correct Answer: A

Section: Sims

Explanation

Explanation/Reference:

Answer: Follow the explanation part to get answer on this sim question.

Explanation:

First, for the HTTP access we need to create a NAT object. Here I called it HTTP but it can be given any name.

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Configuration >

Add Edit

Match Criteria

#	Source Interface
1	Any

Add Network Object

Name: HTTP

Type: Host

IP Version: ☒ IPv4 ☐ IPv6

IP Address: 209.165.201.30

NAT

☒ Add Automatic Address Translation Rules

Type: Static

Translated Address: 172.16.1.2

☐ Use one-to-one address translation

☐ PAT Pool Translated Address:

☐ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535 ☐ Include

☐ Fail through to interface PAT (dest intf): DMZ

Then, create the firewall rules to allow the HTTP access:

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring

Firewall

Configuration

Access Rules

NAT Rules

Service Policy Rules

AAA Rules

Filter Rules

Public Servers

URL Filtering Servers

Threat Detection

Identity Options

Identity by TrustSec

Botnet Traffic Filter

Objects

Network Objects/Groups

Service Objects/Groups

Local Users

Local User Groups

Security Group Object Group

Class Maps

Inspect Maps

Regular Expressions

TCP Maps

Time Ranges

Unified Communications

Advanced

+ Add

#

dmz (1) in

1

inside (1 in

1

outside (1

1

Global (1 in

1

Add Access Rule

Interface: outside

Action: ☒ Permit ☐ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: 209.166.201.30

Security Group:

Service: tcp/http

Description:

☒ Enable Logging

Logging Level: Default

More Options

OK

Cancel

Help

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Access Rules

Add Edit Delete Where Used Not Used

Diagram Export

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
 - Network Objects/Groups
 - Service Objects/Groups
 - Local Users
 - Local User Groups
 - Security Group Object Group
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
- Unified Communications
- Advanced

Source Criteria:

#	Enabled	Source	User	Security Gr	Destination
dmz (1) implicitly incoming					
1		any			Any less secure
inside (1) implicit incoming					
1		any			Any less secure
outside (1) incoming rule					
1	<input checked="" type="checkbox"/>	any			209.165.201.30
Global (1) implicit rule					
1		any			any

You can verify using the outside PC to HTTP into 209.165.201.30.

For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Service Policy Rules

Add Edit Delete Up Down Copy Paste Find Diagram Packet Tracer

Traffic Classification

Name	#	Enabled	Match	Source	Src Security Group	Dest Security Group
Interface: dmz; Policy: asaex_policy						
class-default			Match	any		
Interface: inside; Policy: asaex_policy						
class-default			Match	any		
Global; Policy: global_policy						
inspection_def...			Match	any		

Apply

Reset

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
 - Network Objects/Groups
 - Service Objects/Groups
 - Local Users
 - Local User Groups
 - Security Group Object Group
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
- Unified Communications
- Advanced

And then check the ICMP box only as shown below, then hit Apply.

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring

Firewall **Configure**

- Access Rules
- NAT Rules
- Service Policy Rules**
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Eoynet Traffic Filter
- Objects
 - Network Objects/Groups
 - Service Objects/Groups
 - Local Users
 - Local User Groups
 - Security Group Object Group
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
- Unified Communications
- Advanced

Traffic Classification

Name

- Interface class-0
- Interface class-1
- Global; inspect

Edit Service Policy Rule

Traffic Classification Default Inspections Rule Actions

Protocol Inspection ASA FirePOWER Inspection Connection Settings QoS NetFlow User

☐ Select all inspection rules

<input type="checkbox"/> CTIQBE	
<input type="checkbox"/> Cloud Web Security	Configure...
<input type="checkbox"/> DCERPC	Configure...
<input checked="" type="checkbox"/> DNS	Configure... DNS Inspect Map: preset_dns_map
<input checked="" type="checkbox"/> ESMTP	Configure...
<input checked="" type="checkbox"/> FTP	Configure...
<input checked="" type="checkbox"/> H.323 H.225	Configure...
<input checked="" type="checkbox"/> H.323 RAS	Configure...
<input type="checkbox"/> HTTP	Configure...
<input checked="" type="checkbox"/> ICMP	
<input type="checkbox"/> ICMP Error	
<input type="checkbox"/> ILS	
<input type="checkbox"/> IM	Configure...
<input checked="" type="checkbox"/> IP-Options	Configure...
<input type="checkbox"/> IPSec-Pass-Thru	Configure...
<input type="checkbox"/> IPv6	Configure...
<input type="checkbox"/> MNP	Configure...
<input type="checkbox"/> MSS	Configure...

After that is done, we can ping www.cisco.com again to verify:

Inside PC



Inside PC



Bginfo -
Shortcut



Recycle Bin



Nmap -
Zenmap GUI



cmd.exe

Press RETURN to get started!

C:\>ping www.cisco.com

Pinging with 32 bytes of data:Request

Request timed out.

Request timed out.

Request timed out.

Ping statistics for www.cisco.com:

(100% loss),

Approximate round trip times in milli

Minimum - 0ms, Maximum - 0ms, Avc

C:\>ping www.cisco.com

Pinging e144.dsdb.akamaiedge.net [23.
bytes of data:

Reply from 23.72.192.170 bytes=32 tim

Reply from 23.72.192.170 bytes=32 tim

Reply from 23.72.192.170 bytes=32 tim

Reply from 23.72.192.170 bytes=32 tim

QUESTION 4

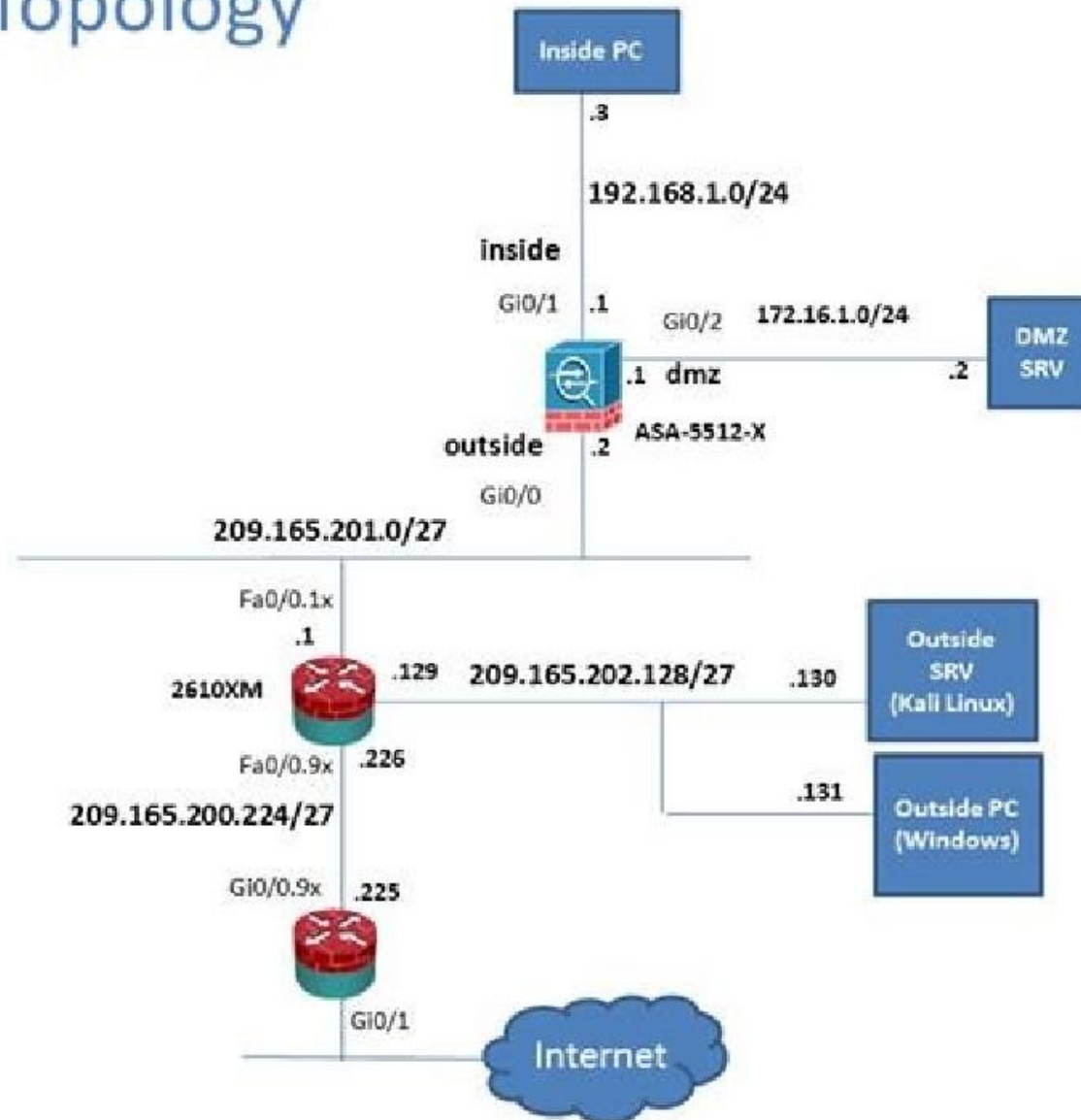
Scenario

In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation. To see all the menu options available on the left navigation pane, you may also need to unexpand the expanded menu first.

Lab Topology



Which four tunnelling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

- A. Clientless SSL VPN
- B. SSL VPN Client
- C. PPTP
- D. L2TP/IPsec
- E. IPsec IKEv1
- F. IPsec IKEv2

Correct Answer: ADEF

Section: Sims

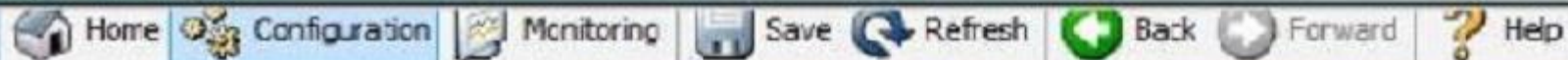
Explanation

Explanation/Reference:

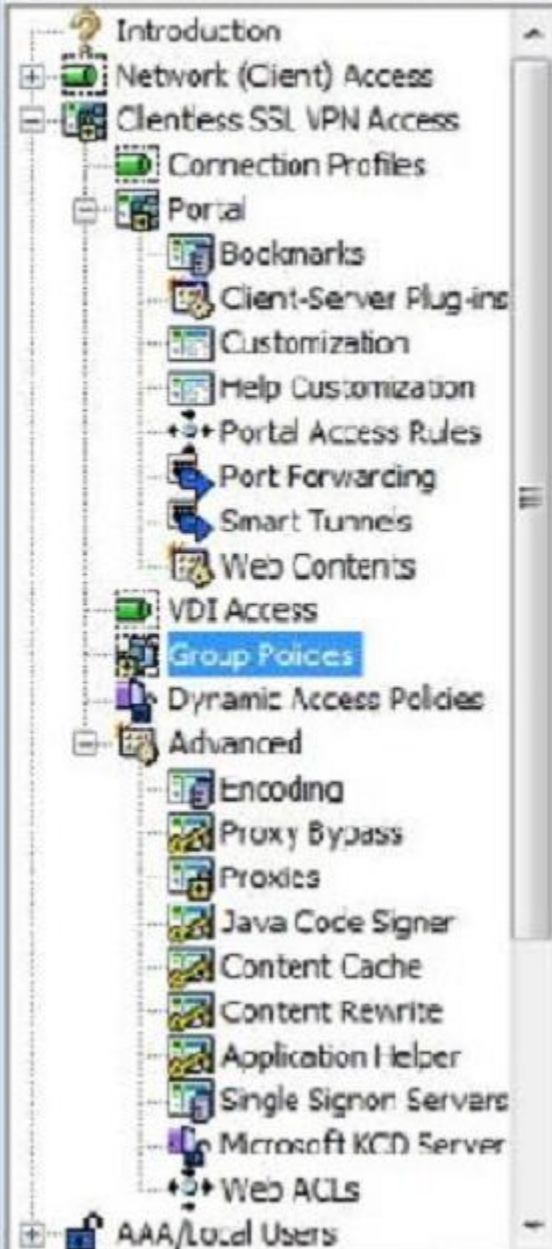
Explanation:

By clicking one the Configuration-> Remote Access -> Clientless CCL VPN Access-> Group Policies tab you can view the DfltGrpPolicy protocols as shown below:

Virtual Terminal







Remote Access VPN

[Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies](#)


Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

 Add
  Edit
  Delete
  Assign

Name	Type	Tunneling
Sales	Internal	ssl-clientle
DfltGrpPolicy (System Default)	Internal	ikev1;ikev

QUESTION 5

Scenario

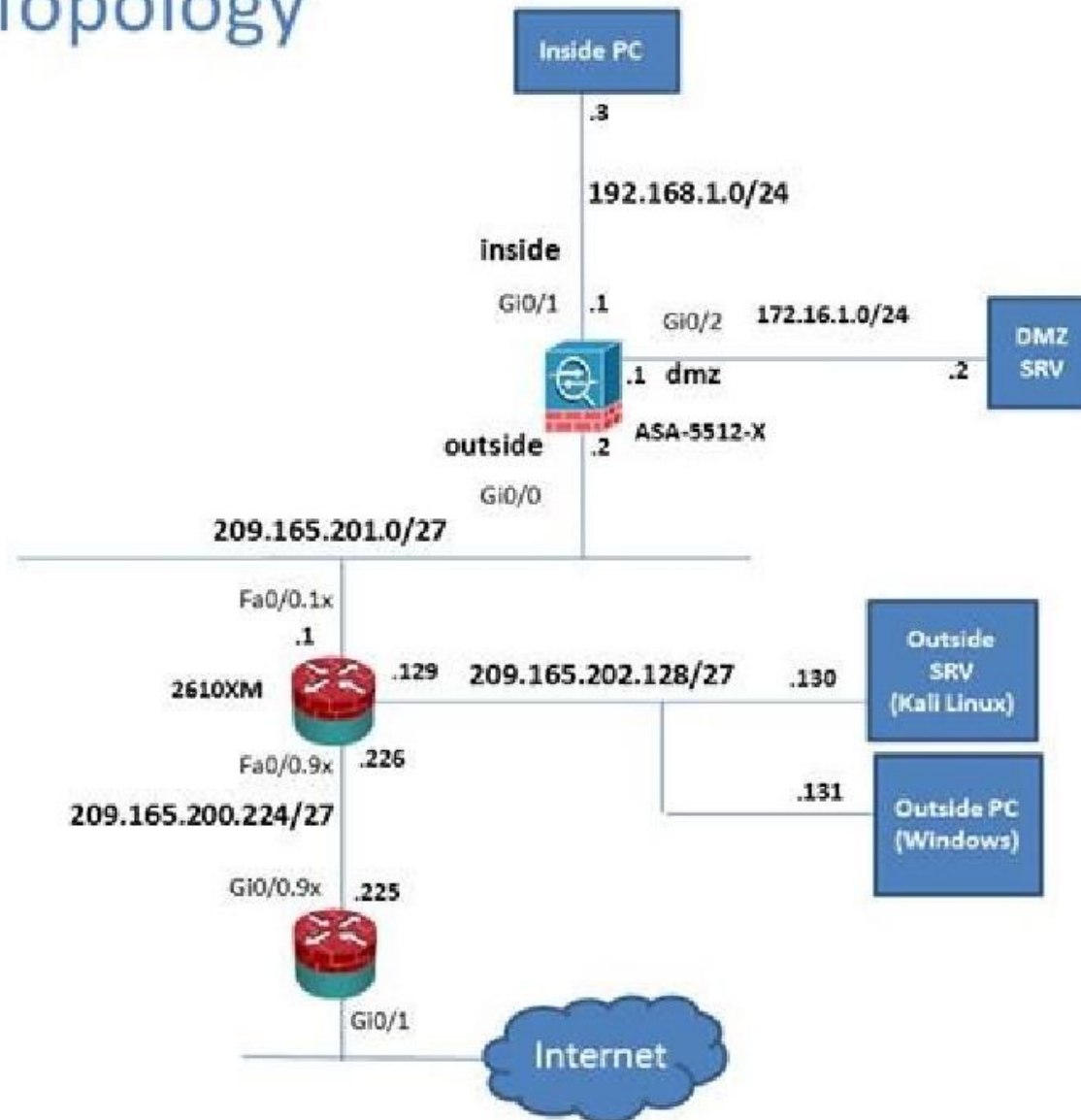
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to unexpand the expanded menu first.

Lab Topology



When users login to the Clientless SSLVPN using <https://209.165.201.2/test>, which group policy will be applied?

- A. test
- B. clientless
- C. Sales
- D. DfltGrpPolicy
- E. DefaultRAGroup
- F. DefaultWEBVPNGroup

Correct Answer: C

Section: Sims

Explanation

Explanation/Reference:

Explanation:

First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:

Virtual Terminal

Home
 Configuration
 Monitoring
 Save
 Refresh
 Back
 Forward
 Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
 - Connection Profiles
 - Portal
 - Bookmarks
 - Client-Server Plug-ins
 - Customization
 - Help Customization
 - Portal Access Rules
 - Port Forwarding
 - Smart Tunnels
 - Web Contents
 - VDI Access
 - Group Policies
 - Dynamic Access Policies
 - Advanced
 - Encoding
 - Proxy Bypass
 - Proxies
 - Java Code Signer
 - Content Cache
 - Content Rewrite
 - Application Helper
 - Single Signon Servers
 - Microsoft KCD Server
 - Web ACLs
- AAA/Local Users

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>
inside	<input type="checkbox"/>

Device Cert

Port Se

☒ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☒ Allow user to select connection profile on the login page.

☐ Allow user to enter internal password on the login page.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You



Add



Edit



Delete

Find:



Match Case

Name	Enabled	Aliases
DefaultRAGroup	<input checked="" type="checkbox"/>	
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	

Then hit the "edit" button and you can clearly see the Sales Group Policy being applied.

Virtual Terminal

Remote Access

- Introduction
- Network ()
- Clientless
- Connect
- Portal
- Edge
- Client
- Configuration
- Home
- Forward
- Forward
- Secure
- Web
- VDI Access
- Group
- Dynamic
- Advanced
- Encryption
- Firewall
- Firewall
- Java
- Configuration
- Configuration
- Application
- Simulation
- Monitoring
- Web
- AAA/Local

Aliases: test

Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

AAA Server Group: LOCAL

☐ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2

Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales

(Following field is an attribute of the group policy selected above.)

☒ Enable clientless SSL VPN protocol

Exam C**QUESTION 1**

Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What type of attack did your team discover?

- A. advanced persistent threat
- B. targeted malware
- C. drive-by spyware
- D. social activism
- E. Email Harvesting

Correct Answer: AD

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 2

Refer to the exhibit.

```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

What is the effect of the given command? (Chose Two)

- A. It merges authentication and encryption methods to protect traffic that matches an ACL.
- B. It configures the network to use a different transform set between peers.
- C. It configures encryption for MD5 HMAC.
- D. It configures authentication as AES 256.

Correct Answer: CD

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 3

Which two statements about stateless firewalls are true? (Choose two.)

- A. They compare the 5-tuple of each incoming packet against configurable rules.
- B. They cannot track connections.
- C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
- D. Cisco IOS cannot implement them because the platform is stateful by nature.
- E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Correct Answer: AB

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 4

What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

- A. The Internet Key Exchange protocol establishes security associations
- B. The Internet Key Exchange protocol provides data confidentiality
- C. The Internet Key Exchange protocol provides replay detection
- D. The Internet Key Exchange protocol is responsible for mutual authentication

Correct Answer: AD

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 5

Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

- A. Modifying packets
- B. Requesting connection blocking
- C. Denying packets
- D. Resetting the TCP connection
- E. Requesting host blocking

F. Denying frames

Correct Answer: BDE

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 6

What are the primary attack methods of VLAN hopping? (Choose two.)

- A. VoIP hopping
- B. Switch spoofing
- C. CAM-table overflow
- D. Double tagging

Correct Answer: BD

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 7

Which two services define cloud networks? (Choose two.)

- A. Infrastructure as a Service
- B. Platform as a Service
- C. Security as a Service
- D. Compute as a Service
- E. Tenancy as a Service

Correct Answer: AB

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 8

Which of the following are features of IPsec transport mode? (Choose three.)

- A. IPsec transport mode is used between end stations
- B. IPsec transport mode is used between gateways
- C. IPsec transport mode supports multicast
- D. IPsec transport mode supports unicast
- E. IPsec transport mode encrypts only the payload
- F. IPsec transport mode encrypts the entire packet

Correct Answer: ADE

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 9

What features can protect the data plane? (Choose three.)

- A. policing
- B. ACLs
- C. IPS
- D. antispoofing
- E. QoS
- F. DHCP-snooping

Correct Answer: BDF

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 10

What are the three layers of a hierarchical network design? (Choose three.)

- A. access
- B. core

- C. distribution
- D. user
- E. server
- F. Internet

Correct Answer: ABC

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 11

Which two statements about Telnet access to the ASA are true? (Choose two).

- A. You may VPN to the lowest security interface to telnet to an inside interface.
- B. You must configure an AAA server to enable Telnet.
- C. You can access all interfaces on an ASA using Telnet.
- D. You must use the command virtual telnet to enable Telnet.
- E. Best practice is to disable Telnet and use SSH.

Correct Answer: AE

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 12

Which three statements about host-based IPS are true? (Choose three.)

- A. It can view encrypted files.
- B. It can have more restrictive policies than network-based IPS.
- C. It can generate alerts based on behaviour at the desktop level.
- D. It can be deployed at the perimeter.
- E. It uses signature-based policies.
- F. It works with deployed firewalls.

Correct Answer: ABC

Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 13

If a router configuration includes the line `aaa authentication login default group tacacs+ enable`, which events will occur when the TACACS+ server returns an error? (Choose two.)

- A. The user will be prompted to authenticate using the enable password
- B. Authentication attempts to the router will be denied
- C. Authentication will use the router's local database
- D. Authentication attempts will be sent to the TACACS+ server

Correct Answer: AB
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 14

Which statements about smart tunnels on a Cisco firewall are true? (Choose two.)

- A. Smart tunnels can be used by clients that do not have administrator privileges
- B. Smart tunnels support all operating systems
- C. Smart tunnels offer better performance than port forwarding
- D. Smart tunnels require the client to have the application installed locally

Correct Answer: AC
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 15

What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

- A. deny attacker

- B. deny packet
- C. modify packet
- D. request block connection
- E. request block host
- F. reset TCP connection

Correct Answer: ABC

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 16

What are two ways to prevent eavesdropping when you perform device-management tasks? (Choose two.)

- A. Use an SSH connection.
- B. Use SNMPv3.
- C. Use out-of-band management.
- D. Use SNMPv2.
- E. Use in-band management.

Correct Answer: AB

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 17

In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)

- A. RADIUS uses UDP to communicate with the NAS.
- B. RADIUS encrypts only the password field in an authentication packet.
- C. RADIUS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
- D. RADIUS uses TCP to communicate with the NAS.
- E. RADIUS can encrypt the entire packet that is sent to the NAS.
- F. RADIUS supports per-command authorization.

Correct Answer: ABC
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 18

Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

- A. Port security
- B. DHCP snooping
- C. IP source guard
- D. Dynamic ARP inspection

Correct Answer: BD
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 19

In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

- A. when matching NAT entries are configured
- B. when matching ACL entries are configured
- C. when the firewall receives a SYN-ACK packet
- D. when the firewall receives a SYN packet
- E. when the firewall requires HTTP inspection
- F. when the firewall requires strict HTTP inspection

Correct Answer: ABE
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 20

In which two situations should you use in-band management? (Choose two.)

- A. when management applications need concurrent access to the device
- B. when you require administrator access from multiple locations
- C. when a network device fails to forward packets
- D. when you require ROMMON access
- E. when the control plane fails to respond

Correct Answer: AB

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 21

Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.)

- A. The password
- B. The hash
- C. The key
- D. The transform set

Correct Answer: BC

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 22

Which security measures can protect the control plane of a Cisco router? (Choose two.)

- A. CCPr
- B. Parser views
- C. Access control lists
- D. Port security
- E. CoPP

Correct Answer: AE

Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 23

Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

- A. EAP
- B. ASCII
- C. PAP
- D. PEAP
- E. MS-CHAPv1
- F. MS-CHAPv2

Correct Answer: CEF
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 24

Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

- A. EAP
- B. ASCII
- C. PAP
- D. PEAP
- E. MS-CHAPv1
- F. MS-CHAPv2

Correct Answer: BCE
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 25

Which statements about reflexive access lists are true? (Choose three.)

- A. Reflexive access lists create a permanent ACE
- B. Reflexive access lists approximate session filtering using the established keyword
- C. Reflexive access lists can be attached to standard named IP ACLs
- D. Reflexive access lists support UDP sessions
- E. Reflexive access lists can be attached to extended named IP ACLs
- F. Reflexive access lists support TCP sessions

Correct Answer: DEF

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 26

According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

- A. BOOTP
- B. TFTP
- C. DNS
- D. MAB
- E. HTTP
- F. 802.1x

Correct Answer: ABC

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 27

Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)

- A. AES
- B. 3DES

- C. DES
- D. MD5
- E. DH-1024
- F. SHA-384

Correct Answer: AF
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 28

Which three statements describe DHCP spoofing attacks? (Choose three.)

- A. They can modify traffic in transit.
- B. They are used to perform man-in-the-middle attacks.
- C. They use ARP poisoning.
- D. They can access most network devices.
- E. They protect the identity of the attacker by masking the DHCP address.
- F. They can physically modify the network gateway.

Correct Answer: ABC
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 29

Which three ESP fields can be encrypted during transmission? (Choose three.)

- A. Security Parameter Index
- B. Sequence Number
- C. MAC Address
- D. Padding
- E. Pad Length
- F. Next Header

Correct Answer: DEF
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 30

In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

- A. TACACS uses TCP to communicate with the NAS.
- B. TACACS can encrypt the entire packet that is sent to the NAS.
- C. TACACS supports per-command authorization.
- D. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
- E. TACACS uses UDP to communicate with the NAS.
- F. TACACS encrypts only the password field in an authentication packet.

Correct Answer: ABC
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 31

Which accounting notices are used to send a failed authentication attempt record to a AAA server? (Choose two.)

- A. start-stop
- B. stop-record
- C. stop-only
- D. stop

Correct Answer: BD
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 32

Which options are filtering options used to display SDEE message types? (Choose two.)

- A. stop
- B. none
- C. error
- D. all

Correct Answer: CD

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 33

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

- A. FTP
- B. SSH
- C. Telnet
- D. AAA
- E. HTTPS
- F. HTTP

Correct Answer: BE

Section: Multi Select

Explanation

Explanation/Reference:

QUESTION 34

What are two uses of SIEM software? (Choose two.)

- A. collecting and archiving syslog data
- B. alerting administrators to security events in real time
- C. performing automatic network audits
- D. configuring firewall and IDS devices
- E. scanning email for suspicious attachments

Correct Answer: AB
Section: Multi Select
Explanation

Explanation/Reference:

QUESTION 35

You want to allow all of your company's users to access the Internet without allowing other Web servers to collect the IP addresses of individual users. What two solutions can you use? (Choose two).

- A. Configure a proxy server to hide users' local IP addresses.
- B. Assign unique IP addresses to all users.
- C. Assign the same IP address to all users.
- D. Install a Web content filter to hide users' local IP addresses.
- E. Configure a firewall to use Port Address Translation.

Correct Answer: AE
Section: Multi Select
Explanation

Explanation/Reference:

Exam D**QUESTION 1**

A data breach has occurred and your company database has been copied. Which security principle has been violated?

- A. confidentiality
- B. availability
- C. access
- D. control

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 2

Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

- A. SDEE
- B. Syslog
- C. SNMP
- D. CSM

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 3

How can you detect a false negative on an IPS?

- A. View the alert on the IPS.
- B. Review the IPS log.
- C. Review the IPS console.
- D. Use a third-party system to perform penetration testing.
- E. Use a third-party to audit the next-generation firewall rules.

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 4

Which statement provides the best definition of malware?

- A. Malware is unwanted software that is harmful or destructive.
- B. Malware is software used by nation states to commit cybercrimes.
- C. Malware is a collection of worms, viruses, and Trojan horses that is distributed as a single package.
- D. Malware is tools and applications that remove unwanted programs.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 5

How can FirePOWER block malicious email attachments?

- A. It forwards email requests to an external signature engine.
- B. It scans inbound email messages for known bad URLs.
- C. It sends the traffic through a file policy.
- D. It sends an alert to the administrator to verify suspicious email messages.

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 6

A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page. Which action should you take to begin troubleshooting?

- A. Ensure that the RDP2 plug-in is installed on the VPN gateway
- B. Reboot the VPN gateway
- C. Instruct the user to reconnect to the VPN gateway
- D. Ensure that the RDP plug-in is installed on the VPN gateway

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 7

Refer to the exhibit.

```
crypto map mymap 20 match address 201
access-list 201 permit ip 10.10.10.0 255.255.255.0 10.100.100.0 255.255.255.0
```

What is the effect of the given command sequence?

- A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
- B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.
- C. It defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
- D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 8

Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

- A. FlexConfig

- B. Device Manager
- C. Report Manager
- D. Health and Performance Monitor

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 9

You have been tasked with blocking user access to websites that violate company policy, but the sites use dynamic IP addresses. What is the best practice for URL filtering to solve the problem?

- A. Enable URL filtering and use URL categorization to block the websites that violate company policy.
- B. Enable URL filtering and create a blacklist to block the websites that violate company policy.
- C. Enable URL filtering and create a whitelist to block the websites that violate company policy.
- D. Enable URL filtering and use URL categorization to allow only the websites that company policy allows users to access.
- E. Enable URL filtering and create a whitelist to allow only the websites that company policy allows users to access.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 10

Which Sourcefire event action should you choose if you want to block only malicious traffic from a particular end user?

- A. Allow with inspection
- B. Allow without inspection
- C. Block
- D. Trust
- E. Monitor

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:**QUESTION 11**

You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP Address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

- A. Create a whitelist and add the appropriate IP address to allow the traffic.
- B. Create a custom blacklist to allow the traffic.
- C. Create a user based access control rule to allow the traffic.
- D. Create a network based access control rule to allow the traffic.
- E. Create a rule to bypass inspection to allow the traffic.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:**QUESTION 12**

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

- A. The supplicant will fail to advance beyond the webauth method.
- B. The switch will cycle through the configured authentication methods indefinitely.
- C. The authentication attempt will time out and the switch will place the port into the unauthorized state.

D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 13

In which stage of an attack does the attacker discover devices on a target network?

- A. Reconnaissance
- B. Covering tracks
- C. Gaining access
- D. Maintaining access

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 14

Which statement about personal firewalls is true?

- A. They can protect a system by denying probing requests.
- B. They are resilient against kernel attacks.
- C. They can protect email messages and private documents in a similar way to a VPN.
- D. They can protect the network against attacks.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 15

What is a possible reason for the error message: Router(config)#aaa server?% Unrecognized command

- A. The command syntax requires a space after the word "server"
- B. The command is invalid on the target device
- C. The router is already running the latest operating system
- D. The router is a new device on which the aaa new-model command must be applied before continuing

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 16

Which command is needed to enable SSH support on a Cisco Router?

- A. crypto key lock rsa
- B. crypto key generate rsa
- C. crypto key zeroize rsa
- D. crypto key unlock rsa

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

Exam E**QUESTION 1**

What is the transition order of STP states on a Layer 2 switch interface?

- A. listening, learning, blocking, forwarding, disabled
- B. listening, blocking, learning, forwarding, disabled
- C. blocking, listening, learning, forwarding, disabled
- D. forwarding, listening, learning, blocking, disabled

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 2

Which type of PVLAN port allows hosts in the same VLAN to communicate directly with each other?

- A. community for hosts in the PVLAN
- B. promiscuous for hosts in the PVLAN
- C. isolated for hosts in the PVLAN
- D. span for hosts in the PVLAN

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 3

What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

- A. 5 seconds
- B. 10 seconds
- C. 15 seconds
- D. 20 seconds

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 4

Refer to the exhibit.

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

Which statement about the device time is true?

- A. The time is authoritative, but the NTP process has lost contact with its servers.
- B. The time is authoritative because the clock is in sync.
- C. The clock is out of sync.
- D. NTP is configured incorrectly.
- E. The time is not authoritative.

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 5

Refer to the exhibit.

```
209.114.111.1 configured, ipv4, sane, valid, stratum 2
ref ID 132.163.4.103 , time D7AD124D.9D6FC576 (03:17:33.614 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 46.34 msec, root disp 23.52, reach 1, sync dist 268.59
delay 63.27 msec, offset 7.9817 msec, dispersion 187.56, jitter 2.07 msec
precision 2**23, version 4
```

```
204.2.134.164 configured, ipv4, sane, valid, stratum 2
ref ID 241.199.164.101, time D7AD1419.9EB5272B (03:25:13.619 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 256
root delay 30.83 msec, root disp 4.88, reach 1, sync dist 223.80
delay 28.69 msec, offset 6.4331 msec, dispersion 187.55, jitter 1.39 msec
precision 2**20, version 4
```

```
192.168.10.7 configured, ipv4, our_master, sane, valid, stratum 3
ref ID 108.61.73.243 , time D7AD0D8F.AE79A23A (02:57:19.681 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 86.45 msec, root disp 87.82, reach 377, sync dist 134.25
delay 0.89 msec, offset 19.5087 msec, dispersion 1.69, jitter 0.84 msec
precision 2**32, version 4
```

With which NTP server has the router synchronized?

- A. 192.168.10.7
- B. 108.61.73.243
- C. 209.114.111.1
- D. 132.163.4.103
- E. 204.2.134.164
- F. 241.199.164.101

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 6

For what reason would you configure multiple security contexts on the ASA firewall?

- A. To separate different departments and business units.
- B. To enable the use of VRFs on routers that are adjacently connected.
- C. To provide redundancy and high availability within the organization.
- D. To enable the use of multicast routing and QoS through the firewall.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 7

Which type of encryption technology has the broadest platform support to protect operating systems?

- A. software
- B. hardware
- C. middleware
- D. file-level

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 8

Which type of security control is defence in depth?

- A. Threat mitigation
- B. Risk analysis
- C. Botnet mitigation
- D. Overt and covert channels

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 9

When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

- A. Deny the connection inline.
- B. Perform a Layer 6 reset.
- C. Deploy an antimalware system.
- D. Enable bypass mode.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 10

Which FirePOWER preprocessor engine is used to prevent SYN attacks?

- A. Rate-Based Prevention
- B. Portscan Detection
- C. IP Defragmentation
- D. Inline Normalization

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 11

What is a potential drawback to leaving VLAN 1 as the native VLAN?

- A. It may be susceptible to a VLAN hopping attack.
- B. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.
- C. The CAM might be overloaded, effectively turning the switch into a hub.
- D. VLAN 1 might be vulnerable to IP address spoofing.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 12

Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

- A. Unidirectional Link Detection
- B. Unicast Reverse Path Forwarding
- C. TrustSec
- D. IP Source Guard

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 13

If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

- A. portfast
- B. EtherChannel guard
- C. loop guard
- D. BPDU guard

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 14

How does the Cisco ASA use Active Directory to authorize VPN users?

- A. It queries the Active Directory server for a specific attribute for the specified user.
- B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.
- C. It downloads and stores the Active Directory database to query for future authorization requests.
- D. It redirects requests to the Active Directory server defined for the VPN group.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 15

What command can you use to verify the binding table status?

- A. show ip dhcp snooping database
- B. show ip dhcp snooping binding
- C. show ip dhcp snooping statistics
- D. show ip dhcp pool
- E. show ip dhcp source binding
- F. show ip dhcp snooping

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 16

Which command verifies phase 1 of an IPsec VPN on a Cisco router?

- A. show crypto map
- B. show crypto ipsec sa
- C. show crypto isakmp sa

D. show crypto engine connection active

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 17

What is a benefit of a web application firewall?

- A. It blocks known vulnerabilities without patching applications.
- B. It simplifies troubleshooting.
- C. It accelerates web traffic.
- D. It supports all networking protocols.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 18

Refer to the exhibit.

dst	src	state	conn-id	slot
10.10.10.2	10.1.1.5	QM_IDLE	1	0

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

- A. IPsec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
- B. IPsec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
- C. IPsec Phase 1 is down due to a QM_IDLE state.
- D. IPsec Phase 2 is down due to a QM_IDLE state.

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 19

Which statement about a PVLAN isolated port configured on a switch is true?

- A. The isolated port can communicate only with the promiscuous port.
- B. The isolated port can communicate with other isolated ports and the promiscuous port.
- C. The isolated port can communicate only with community ports.
- D. The isolated port can communicate only with other isolated ports.

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 20

What can the SMTP preprocessor in FirePOWER normalize?

- A. It can extract and decode email attachments in client to server traffic.
- B. It can look up the email sender.
- C. It compares known threats to the email sender.
- D. It can forward the SMTP traffic to an email filter server.
- E. It uses the Traffic Anomaly Detector.

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

Exam F**QUESTION 1**

When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?

- A. STP elects the root bridge
- B. STP selects the root port
- C. STP selects the designated port
- D. STP blocks one of the ports

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 2

Which statement correctly describes the function of a private VLAN?

- A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains
- B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains
- C. A private VLAN enables the creation of multiple VLANs using one broadcast domain
- D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 3

What is the purpose of a honeypot IPS?

- A. To create customized policies
- B. To detect unknown attacks
- C. To normalize streams
- D. To collect information about attacks

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 4

Which protocol provides security to Secure Copy?

- A. IPsec
- B. SSH
- C. HTTPS
- D. ESP

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 5

Which address block is reserved for locally assigned unique local addresses?

- A. 2002::/16
- B. FD00::/8
- C. 2001::/32
- D. FB00::/8

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 6

Which tool can an attacker use to attempt a DDoS attack?

- A. botnet

- B. Trojan horse
- C. virus
- D. adware

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 7

How does a device on a network using ISE receive its digital certificate during the new device registration process?

- A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server.
- B. ISE issues a certificate from its internal CA server.
- C. ISE issues a pre-defined certificate from a local database.
- D. The device requests a new certificate directly from a central CA.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 8

Refer to the exhibit.


```
R1
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 1
authentication pre-share
lifetime 84600
crypto isakmp key test67890 address 10.20.20.4

R2
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 10
authentication pre-share
lifetime 84600
crypto isakmp key test12345 address 10.30.30.5
```

You have configured R1 and R2 as shown, but the routers are unable to establish a site-to site VPN tunnel. What action can you take to correct the problem?

- A. Edit the crypto keys on R1 and R2 to match.
- B. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.
- C. Set a valid value for the crypto key lifetime on each router.
- D. Edit the crypto isakmp key command on each router with the address value of its own interface.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 9

Refer to the exhibit.

```
current_peer: 10.1.1.5
  PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1205, #pkts encrypt: 1205, #pkts digest 1205
    #pkts decaps: 1168, #pkts decrypt: 1168, #pkts verify 1168
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
```

While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

- A. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5.
- B. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1.
- C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5.
- D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 10

In a security context, which action can you take to address compliance?

- A. Implement rules to prevent a vulnerability.
- B. Correct or counteract a vulnerability.
- C. Reduce the severity of a vulnerability.
- D. Follow directions from the security appliance manufacturer to remediate a vulnerability.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 11

Which IPS mode provides the maximum number of actions?

- A. inline
- B. promiscuous
- C. span
- D. failover
- E. bypass

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 12

By which kind of threat is the victim tricked into entering username and password information at a disguised website?

- A. Spoofing
- B. Malware
- C. Spam
- D. Phishing

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 13

Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

- A. file reputation
- B. file analysis

- C. signature updates
- D. network blocking

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 14

In which type of attack does an attacker send email messages that ask the recipient to click a link such as <https://www.cisco.net.cc/securelogin?>

- A. phishing
- B. pharming
- C. solicitation
- D. secure transaction

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 15

What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the computer?

- A. always-on
- B. proxy
- C. transparent mode
- D. Trusted Network Detection

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 16

Which source port does IKE use when NAT has been detected between two VPN gateways?

- A. TCP 4500
- B. TCP 500
- C. UDP 4500
- D. UDP 500

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 17

Refer to the exhibit.

```
Username Engineer privilege 9 password 0 configure
Username Monitor privilege 8 password 0 watcher
Username HelpDesk privilege 6 password help
Privilege exec level 6 show running
Privilege exec level 7 show start-up
Privilege exec level 9 configure terminal
Privilege exec level 10 interface
```

Which line in this configuration prevents the HelpDesk user from modifying the interface configuration?

- A. Privilege exec level 9 configure terminal
- B. Privilege exec level 10 interface
- C. Username HelpDesk privilege 6 password help
- D. Privilege exec level 7 show start-up

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 18

Which statement about extended access lists is true?

- A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
- B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
- C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
- D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 19

What is the Cisco preferred countermeasure to mitigate CAM overflows?

- A. Port security
- B. Dynamic port security
- C. IP source guard
- D. Root guard

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 20

A specific URL has been identified as containing malware. What action can you take to block users from accidentally visiting the URL and becoming infected with malware?

- A. Enable URL filtering on the perimeter router and add the URLs you want to block to the router's local URL list.
- B. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the router's local URL list.

- C. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewall's local URL list.
- D. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
- E. Create a whitelist that contains the URLs you want to allow and activate the whitelist on the perimeter router.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 21

Which feature filters CoPP packets?

- A. access control lists
- B. class maps
- C. policy maps
- D. route maps

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibit.

dst	src	state	conn-id	slot
10.10.10.2	10.1.1.5	MM_NO_STATE	1	0

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

- A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
- B. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

- C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
- D. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 23

Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
  6 Bad SNMP version errors
  3 Unknown community name
  9 Illegal operation for community name supplied
  4 Encoding errors
  2 Number of requested variables
  0 Number of altered variables
  98 Get-request PDUs
  12 Get-next PDUs
  2 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  31 Response PDUs
  1 Trap PDUs
```


How many times was a read-only string used to attempt a write operation?

- A. 9
- B. 6
- C. 4
- D. 3
- E. 2

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 24

After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

- A. The secure boot-image command is configured.
- B. The secure boot-comfit command is configured.
- C. The confreg 0x24 command is configured.
- D. The reload command was issued from ROMMON.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 25

When a company puts a security policy in place, what is the effect on the company's business?

- A. Minimizing risk
- B. Minimizing total cost of ownership
- C. Minimizing liability
- D. Maximizing compliance

Correct Answer: A

Section: Normal
Explanation

Explanation/Reference:

Exam G**QUESTION 1**

What security feature allows a private IP address to access the Internet by translating it to a public address?

- A. NAT
- B. hairpinning
- C. Trusted Network Detection
- D. Certification Authority

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 2

Which type of mirroring does SPAN technology perform?

- A. Remote mirroring over Layer 2
- B. Remote mirroring over Layer 3
- C. Local mirroring over Layer 2
- D. Local mirroring over Layer 3

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 3

If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?

- A. The trunk port would go into an error-disabled state.
- B. A VLAN hopping attack would be successful.
- C. A VLAN hopping attack would be prevented.
- D. The attacked VLAN will be pruned.

Correct Answer: C
Section: Normal
Explanation

Explanation/Reference:

QUESTION 4

What is the most common Cisco Discovery Protocol version 1 attack?

- A. Denial of Service
- B. MAC-address spoofing
- C. CAM-table overflow
- D. VLAN hopping

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 5

Refer to the exhibit.

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autocommand show running
Privilege exec level 6 configure terminal
```

The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

- A. Remove the autocommand keyword and arguments from the username admin privilege line.
- B. Change the Privilege exec level value to 15.
- C. Remove the two Username Admin lines.

D. Remove the Privilege exec line.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 6

On which Cisco Configuration Professional screen do you enable AAA

- A. AAA Summary
- B. AAA Servers and Groups
- C. Authentication Policies
- D. Authorization Policies

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 7

In the router OSPF 200 command, what does the value 200 stand for?

- A. process ID
- B. area ID
- C. administrative distance value
- D. ABR ID

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 8

Which type of IPS can identify worms that are propagating in a network?

- A. Policy-based IPS
- B. Anomaly-based IPS
- C. Reputation-based IPS
- D. Signature-based IPS

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 9

Which statement about the communication between interfaces on the same security level is true?

- A. Interfaces on the same security level require additional configuration to permit interface communication.
- B. Configuring interfaces on the same security level can cause asymmetric routing.
- C. All traffic is allowed by default between interfaces on the same security level.
- D. You can configure only one interface on an individual security level.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 10

Which wildcard mask is associated with a subnet mask of /27?

- A. 0.0.0.31
- B. 0.0.0.27
- C. 0.0.0.224
- D. 0.0.0.255

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 11

Which option describes information that must be considered when you apply an access list to a physical interface?

- A. Protocol used for filtering
- B. Direction of the access class
- C. Direction of the access group
- D. Direction of the access list

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 12

What is the purpose of the Integrity component of the CIA triad?

- A. to ensure that only authorized parties can modify data
- B. to determine whether data is relevant
- C. to create a process for accessing data
- D. to ensure that only authorized parties can view data

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 13

If the native VLAN on a trunk is different on each end of the link, what is a potential consequence?

- A. The interface on both switches may shut down
- B. STP loops may occur
- C. The switch with the higher native VLAN may shut down
- D. The interface with the lower native VLAN may shut down

Correct Answer: B

Section: Normal

Explanation

Explanation/Reference:

QUESTION 14

How does PEAP protect the EAP exchange?

- A. It encrypts the exchange using the server certificate.
- B. It encrypts the exchange using the client certificate.
- C. It validates the server-supplied certificate, and then encrypts the exchange using the client certificate.
- D. It validates the client-supplied certificate, and then encrypts the exchange using the server certificate.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 15

How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

- A. Traffic between two interfaces in the same zone is allowed by default.
- B. Traffic between interfaces in the same zone is blocked unless you configure the same security permit command.
- C. Traffic between interfaces in the same zone is always blocked.
- D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 16

Refer to the exhibit.


```
tacacs server tacacs1
  address ipv4 1.1.1.1
  timeout 20
  single-connection

tacacs server tacacs2
  address ipv4 2.2.2.2
  timeout 20
  single-connection

tacacs server tacacs3
  address ipv4 3.3.3.3
  timeout 20
  single-connection
```

Which statement about the given configuration is true?

- A. The single-connection command causes the device to establish one connection for all TACACS transactions.
- B. The single-connection command causes the device to process one TACACS request and then move to the next server.
- C. The timeout command causes the device to move to the next server after 20 seconds of TACACS inactivity.
- D. The router communicates with the NAS on the default port, TCP 1645.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 17

In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch acts as a hub?

- A. MAC spoofing
- B. gratuitous ARP
- C. MAC flooding

D. DoS

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 18

Which syslog severity level is level number 7?

- A. Warning
- B. Informational
- C. Notification
- D. Debugging

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 19

Refer to the exhibit.

```
UDP outside 209.165.201.225:53 inside 10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

- A. a stateful firewall
- B. a personal firewall
- C. a proxy firewall
- D. an application firewall
- E. a stateless firewall

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 20

Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

- A. contextual analysis
- B. holistic understanding of threats
- C. graymail management and filtering
- D. signature-based IPS

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 21

Which Sourcefire logging action should you choose to record the most detail about a connection?

- A. Enable logging at the end of the session.
- B. Enable logging at the beginning of the session.
- C. Enable alerts via SNMP to log events off-box.
- D. Enable eStreamer to log events off-box.

Correct Answer: A
Section: Normal
Explanation

Explanation/Reference:

QUESTION 22

When is the best time to perform an anti-virus signature update?

- A. Every time a new update is available.

- B. When the local scanner has detected a new virus.
- C. When a new virus is discovered in the wild.
- D. When the system detects a browser hook.

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference:

QUESTION 23

Which command initializes a lawful intercept view?

- A. username cisco1 view lawful-intercept password cisco
- B. parser view cisco li-view
- C. li-view cisco user cisco1 password cisco
- D. parser view li-view inclusive

Correct Answer: C

Section: Normal

Explanation

Explanation/Reference:

QUESTION 24

Which type of firewall can act on the behalf of the end device?

- A. Stateful packet
- B. Application
- C. Packet
- D. Proxy

Correct Answer: D

Section: Normal

Explanation

Explanation/Reference:

QUESTION 25

Which EAP method uses Protected Access Credentials?

- A. EAP-FAST
- B. EAP-TLS
- C. EAP-PEAP
- D. EAP-GTC

Correct Answer: A

Section: Normal

Explanation

Explanation/Reference: