

Implementing Cisco Network Security

Number: 210-260
Passing Score: 860
Time Limit: 45 min
File Version: 1.0

CCNA SECURITY 210-260

Implementing Cisco Network Security

Exam A

QUESTION 1

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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: (none)

Explanation

Explanation/Reference:

QUESTION 3

In which two situations should you use out-of-band management? (Choose two)

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

E. when the control plane fails to respond

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Which statement about communication over failover interfaces is true?

- A. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default
- B. All information that is sent over the failover and stateful failover interfaces is encrypted by default
- C. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default
- D. Usernames, password and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is in clear text

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

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: (none)

Explanation

Explanation/Reference:

QUESTION 6

How many crypto map sets can you apply to a router interface?

- A. 3
- B. 2
- C. 4
- D. 1

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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 the authentication methods configured on the switch, how will the switch respond?

- A. The switch will cycle through the configured authentication methods indefinitely
- B. The supplicant will fail to advance beyond the webauth method
- 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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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. 0.0.0.225

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Which statements about reflexive access lists are true?

- 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: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

- A. BOOTP
- B. TFTP

- C. DNS
- D. MAB
- E. HTTP
- F. 802.1X

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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: (none)

Explanation

Explanation/Reference:

QUESTION 12

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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: (none)

Explanation

Explanation/Reference:

QUESTION 14

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 authenticates and authorizes simultaneously, causing fewer packets to be transmitted
- D. TACACS uses UDP to communicate with the NAS
- E. TACACS encrypts only the password field in an authentication packet
- F. TACACS supports per-command authorization

Correct Answer: ABF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

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: (none)

Explanation

Explanation/Reference:

QUESTION 16

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: (none)

Explanation

Explanation/Reference:

QUESTION 17

What are the two 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: (none)

Explanation

Explanation/Reference:

QUESTION 18

Which protocol provides security to Secure Copy?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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: (none)

Explanation

Explanation/Reference:

QUESTION 20

Which security zone is automatically defined by the system?

- A. The source zone
- B. The self zone

- C. The destination zone
- D. The inside zone

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

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: (none)

Explanation

Explanation/Reference:

QUESTION 22

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

- A. 2002::/16
- B. FE00::/8
- C. 2001::/32
- D. FB00::/8

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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: (none)

Explanation

Explanation/Reference:

QUESTION 24

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: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

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: (none)

Explanation

Explanation/Reference:

QUESTION 26

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: (none)

Explanation

Explanation/Reference:

QUESTION 27

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: (none)

Explanation

Explanation/Reference:

QUESTION 28

Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?

- A. no switchport nonnegotiate
- B. switchport
- C. no switchport mode dynamic auto
- D. no switchport

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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: (none)

Explanation

Explanation/Reference:

QUESTION 30

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: (none)

Explanation

Explanation/Reference:

QUESTION 31

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

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 issue 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: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Which statement about Cisco ACS authentication and authorization is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

What are two default Cisco IOS privilege levels? (Choose two)

- A. 0
- B. 5
- C. 1
- D. 7
- E. 10
- F. 15

Correct Answer: CF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

What is the effect of the given command sequence?

```
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
```

- 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: (none)

Explanation

Explanation/Reference:

QUESTION 38

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

Which statement about application blocking is true?

- A. It blocks access to files with specific extensions
- B. It blocks access to specific network addresses
- C. It blocks access to specific programs
- D. It blocks access to specific network services

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

- A. hairpinning
- B. tunnel mode
- C. split tunneling
- D. transparent mode

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

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: (none)

Explanation

Explanation/Reference:

QUESTION 44

What Statement about personal firewalls is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

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

```
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 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*

- A. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1
- B. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5
- 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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

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

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Refer to the exhibit. Which statement about the device time is true?

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

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: (none)

Explanation

Explanation/Reference:

QUESTION 53

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: (none)

Explanation

Explanation/Reference:

QUESTION 54

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

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

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which two features do CoPP and CPPR use to protect the control plane? (Choose two)

- A. access lists
- B. traffic classification
- C. policy maps
- D. QoS
- E. class maps
- F. Cisco Express Forwarding

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

Refer to the exhibit. What is the effect of the given command sequence?

```
crypto ikev1 policy 1
encryption aes
hash md5
```


authentication pre-share
group 2
lifetime 14400



<http://www.gratisexam.com/>

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

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: (none)

Explanation

Explanation/Reference:

QUESTION 61

Which tasks is the session management path responsible for? (Choose three)

- A. Verifying IP checksums
- B. Performing route lookup
- C. Performing session lookup
- D. Allowing NAT translations
- E. Checking TCP sequence numbers
- F. Checking packets against the access list

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

Which components does HMAC use to determine the authenticity and integrity of a message?

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

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

- A. BPDU guard
- B. loop guard
- C. root guard
- D. Etherchannel guard

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

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

- A. EAP
- B. ASCII
- C. PAP

- D. PEAP
- E. MS-CHAPv2
- F. MS-CHAPv1

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

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: (none)

Explanation

Explanation/Reference:

QUESTION 71

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Which statement about extended access lists is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

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. HTTP
- F. HTTPS

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

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

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?

- A. Issue the command anyconnect keep-installer installed under the group policy or username webvpn mode
- B. Issue the command anyconnect keep-installer installed in the global configuration
- C. Issue the command anyconnect keep-installer under the group policy or username webvpn mode
- D. Issue the command anyconnect keep-installer under the group policy or username webvpn mode

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

What is the FirePOWER impact flag used for?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

Which two services define cloud networks? (Choose two)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

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

```
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
```

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

What can the SMTP preprocessor in a FirePOWER normalize?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

You want to allow all of your companies 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. Install a Web content filter to hid users local IP addresses
- B. Configure a firewall to use Port Address Translation
- C. Assign the same IP addresses to all users
- D. Configure a proxy server to hide users local IP addresses
- E. Assign unique IP addresses to all users

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

Which two authentication types does OSPF support? (Choose two)

- A. plaintext
- B. MD5
- C. HMAC
- D. AES 256
- E. SHA-1
- F. DES

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

Refer to the exhibit. 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?

```
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
```

- 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: (none)

Explanation

Explanation/Reference:

QUESTION 86

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 87

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:

- Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use ASDM to configure the ASA to allow the Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP address when HTTPing to the DMZ server.
- Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower security level interfaces. Your task is to dynamically allow the echo-reply responses back through the ASA.

Once the correct ASA configurations have been configured:

- You can test the connectivity to <http://209.165.201.30> from the Outside PC browser.
- You can test the pings to the Outside (www.cisco.com) by opening the inside PC command prompt window. In this simulation, only test the connectivity to the Outside.

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:

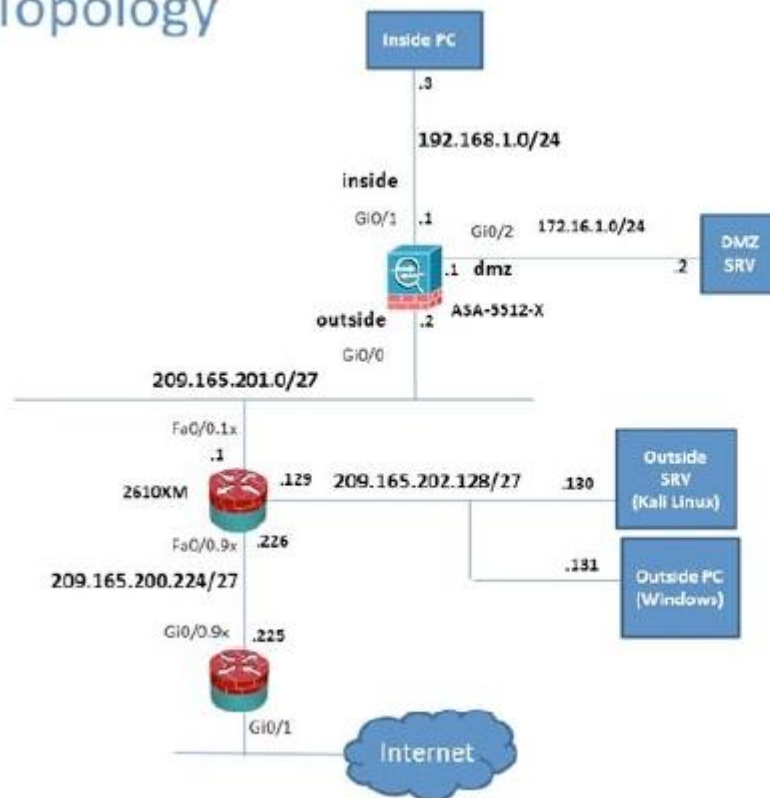
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.

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.



<http://www.gratisexam.com/>

Lab Topology



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

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Step1: Firewall > Configuration > NAT Rules > Add Network Object. Name=http, IP version=IPv4, IP address = 209.165.201.30, Static NAT = 172.16.1.2
 Step2: Firewall > Configuration > NAT Rules > Add Access Rule. Interface=Outside, Action=Permit, Source=any, Destination=209.165.201.30,

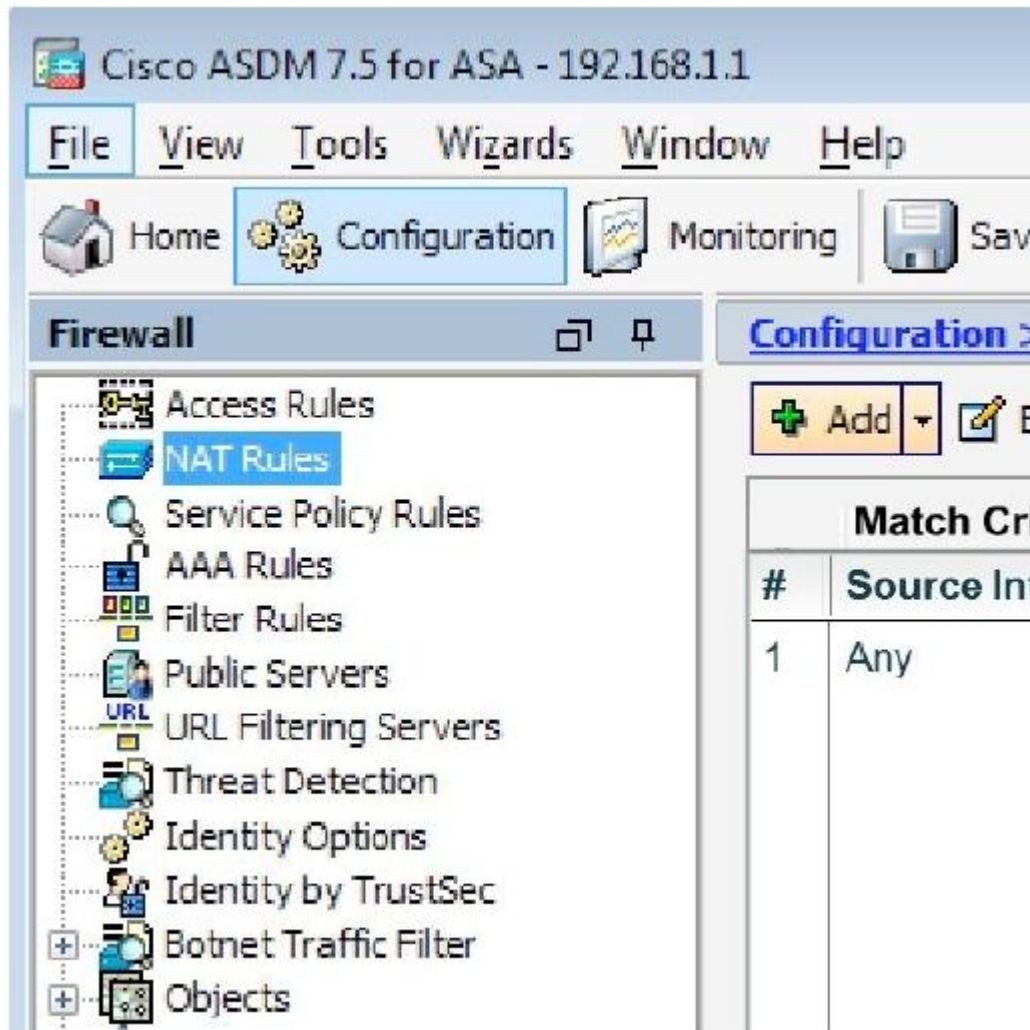
Service=tcp/http

Step3: Firewall > Configuration> Service policy Rules > Click Global Policy and edit, Rule Action tab, Click ICMP and apply

Step4: Ping www.cisco.com from Inside PC




<http://www.gratisexam.com/>





<http://www.gratisexam.com/>

 Add Network Object

Name:

Type:

IP Version: ☒ IPv4 ☐ IPv6

IP Address:

NAT

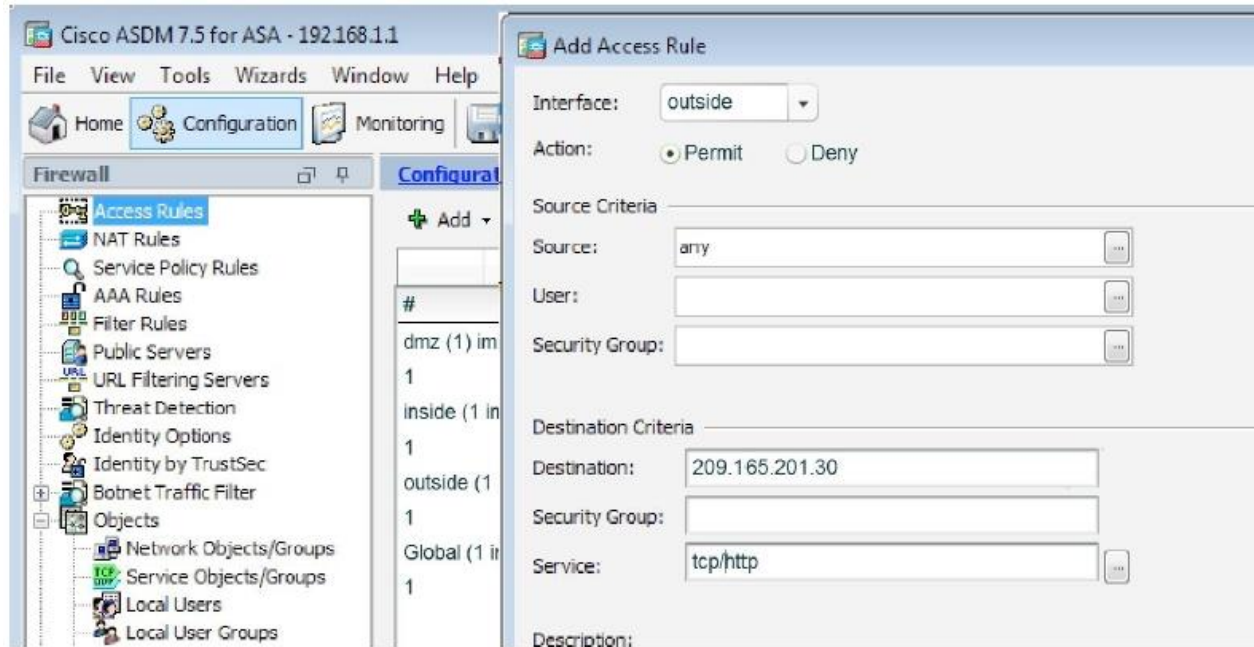
☒ Add Automatic Address Translation Rules

Type:

Translated Addr:



<http://www.gratisexam.com/>



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

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

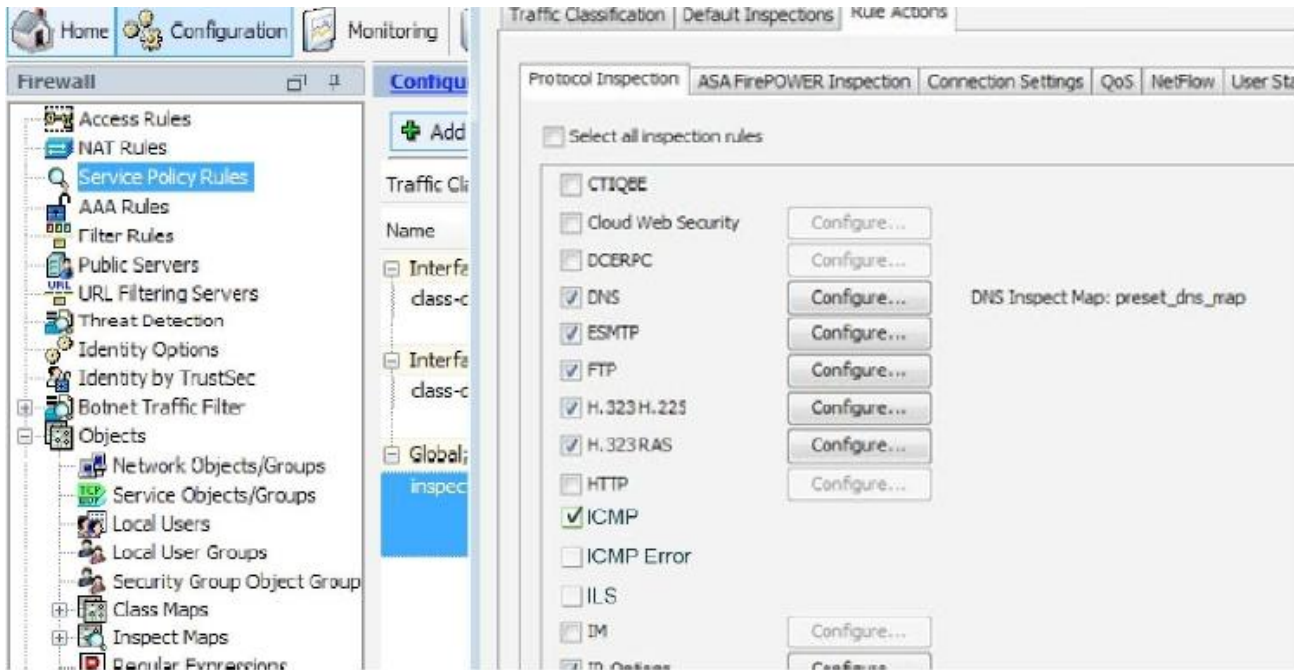
Local Users

Local User Groups

Security Group Object Group

Source Criteria:

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



```
Press RETURN to get started!
C:\ping www.cisco.com
Pinging with 32 bytes of data:Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for www.cisco.com:    Packets: Sent = 4,  Recieved = 0
(100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\ping www.cisco.com
Pinging el44.dscb.akamaiedge.net [23.72.192.170] with 32 bytes of data
bytes of data:
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Ping statistics for 23.72.192.170:    Packets: Sent = 4,  Recieved = 4
(0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5s, Average = 4ms
```



<http://www.gratisexam.com/>

QUESTION 88

Scenario

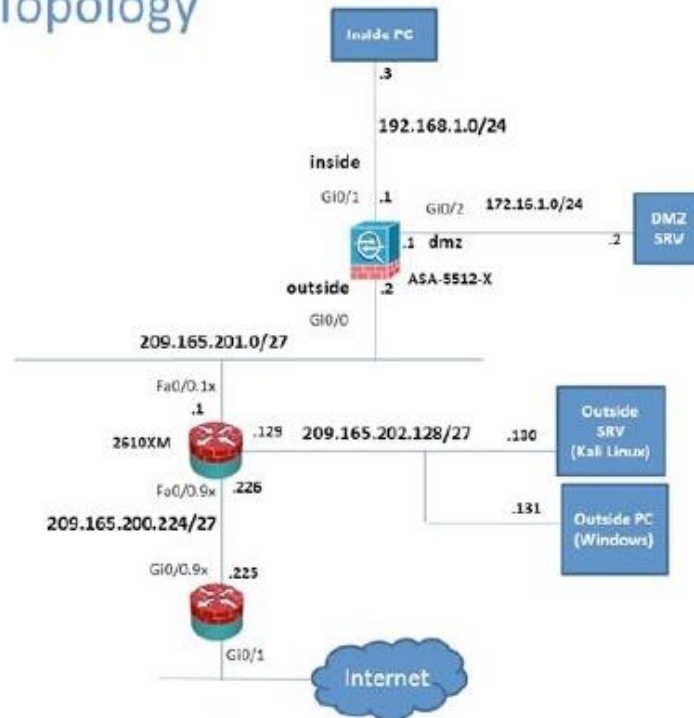
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions.

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 un-expand the expanded menu first.

Lab Topology



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 SSL VPN configurations.

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

- A. IPsec IKEv1
- B. IPsec IKEv2
- C. L2TP/IPsec

- D. Clientless SSL VPN
- E. SSL VPN Client
- F. PPTP

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Via - Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies



<http://www.gratisexam.com/>

Virtual Terminal

Home Configuration Monitoring Save Refresh Back Forward Help

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/va 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-client
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2

DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-client
--------------------------------	----------	------------------------

QUESTION 89

Scenario

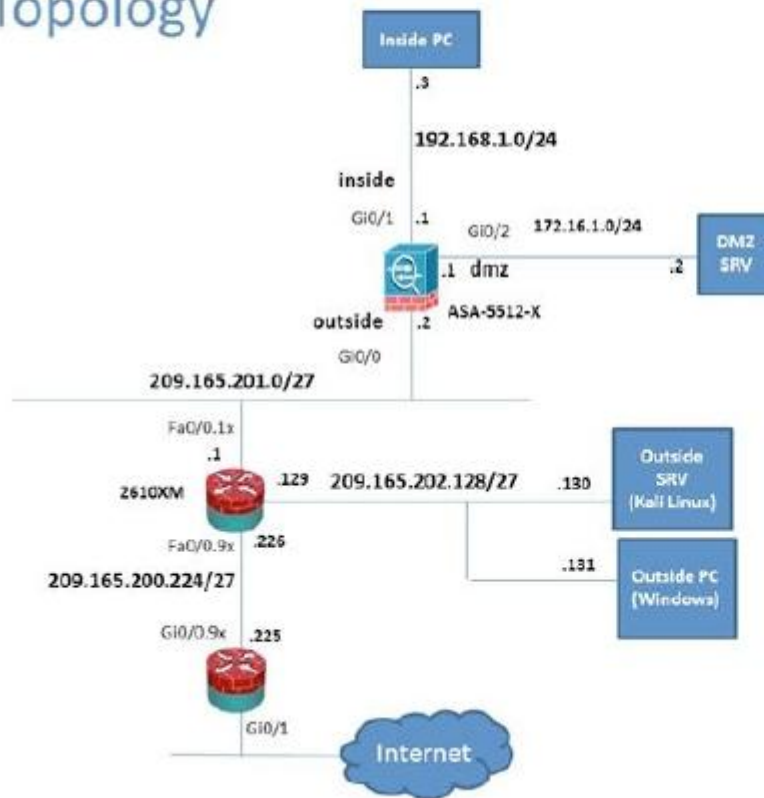
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions.

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 un-expand the expanded menu first.

Lab Topology



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 SSL VPN configurations.



<http://www.gratisexam.com/>

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

- A. The Inside-SRV bookmark has not been applied to the Sales group policy
- B. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_Trustpoit1
- C. The Inside-SRV bookmark references the https://192.168.1.2 URL
- D. Any Connect, IPsec IKEv1 and IPsec IKEv2 VPN access is enabled on the outside interface
- E. Only Clientless SSL VPN VPN access is allowed with the Sales group Policy
- F. The DefaultWEBVPNGroup Connection Profile is using the AAA with Radius server method

Correct Answer: CF

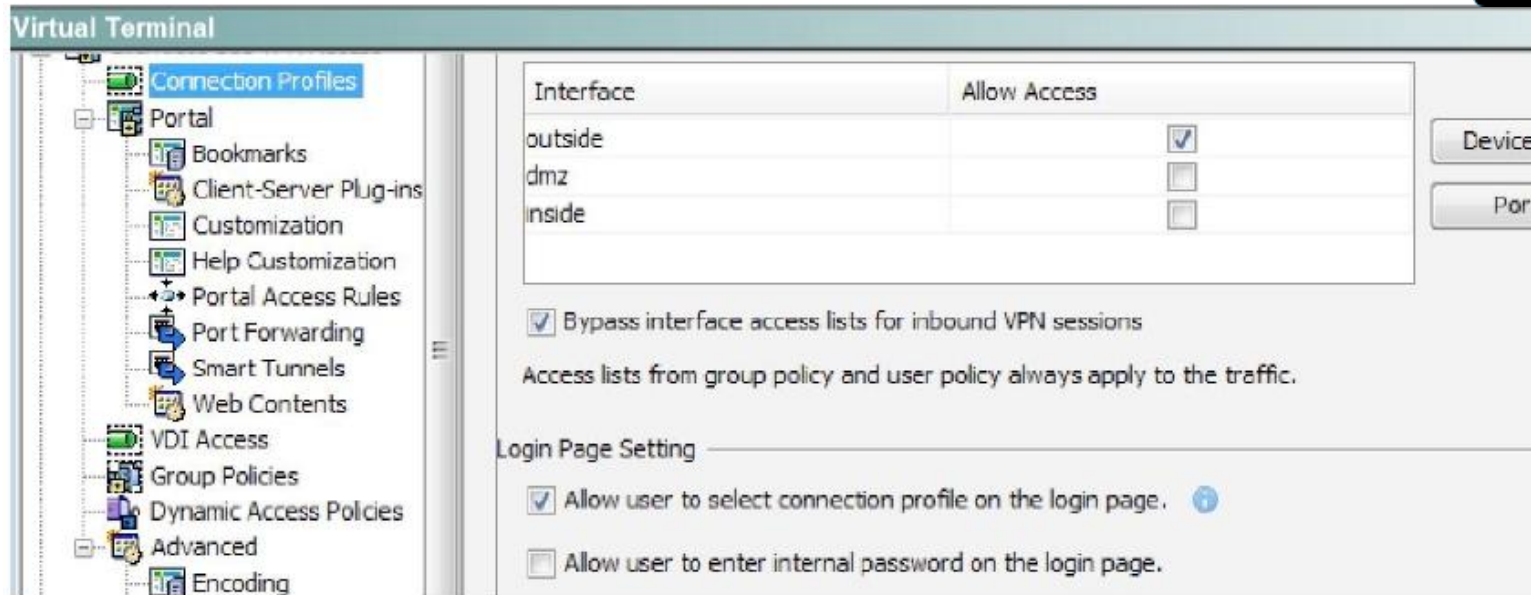
Section: (none)

Explanation

Explanation/Reference:

Via - Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
AND

Via - Configuration > Remote Access VPN > Certificate Management > Identity Certificates



[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Portal](#) > [Bookmarks](#)

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](#) configuration.

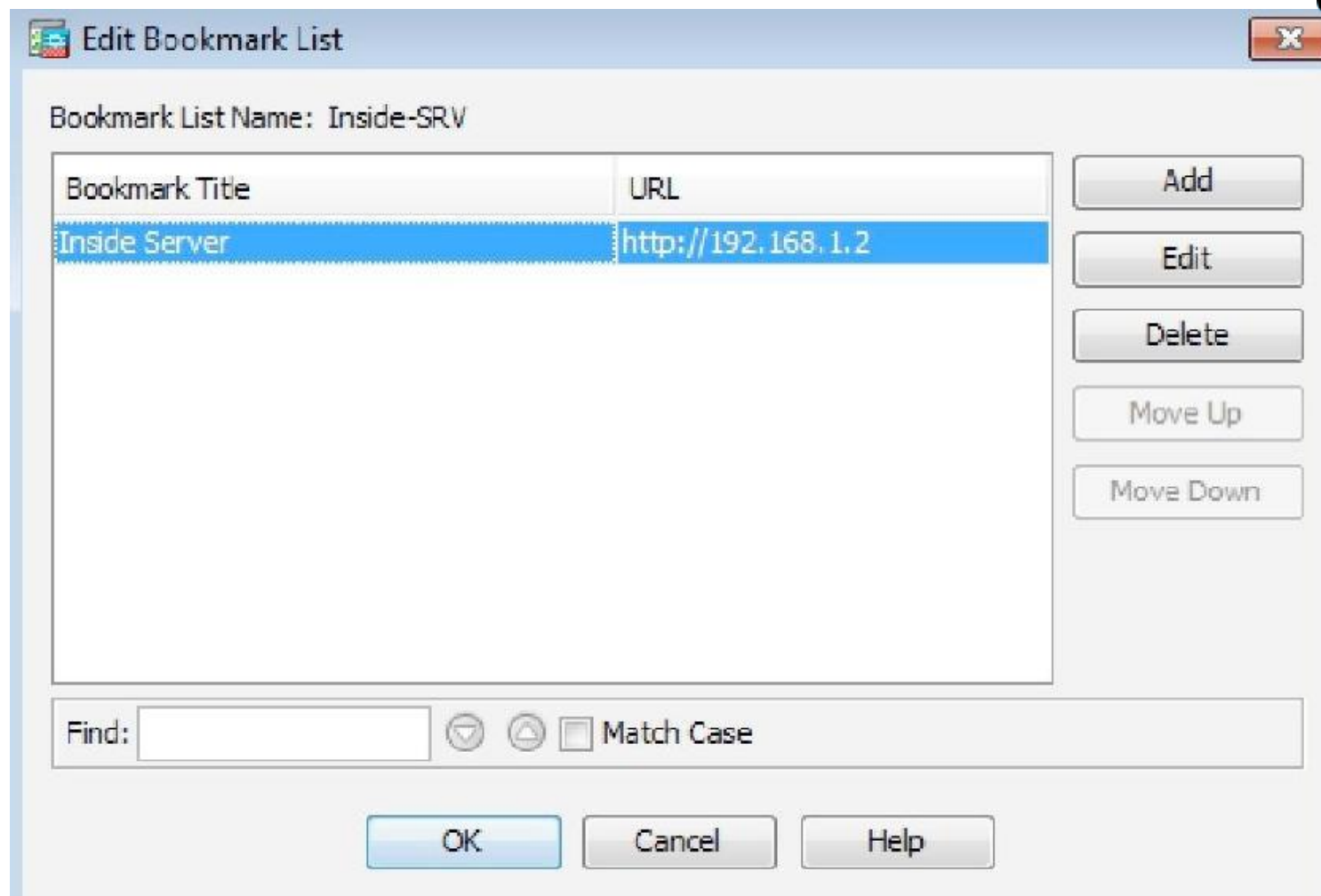
 Add
  Edit
  Delete
  Import
  Export
  Assign

Bookmarks	Group Policies/DAPs
Template	
Inside-SRV	Sales

 Edit



<http://www.gratisexam.com/>



Virtual Terminal

Remote Access VPN

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

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

Issued To	Issued By	Expiry Date	Associated Tr
hostname=P 17-ASA.sec...	hostname=P 17-ASA.sec...	11: 10:33 pst Dec 20 2024	ASDM_TrustPo

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 Profile

Introduction

Network (Client) Access

AnyConnect Connection Profile

AnyConnect Customization/L

AnyConnect Client Profile

AnyConnect Client Software

Dynamic Access Policies

Group Policies

IPsec(IKEv1) Connection Profile

IPsec(IKEv2) Connection Profile

Secure Mobility Solution

Address Assignment

Advanced

Clientless SSL VPN Access

AAA/Local Users

Host Scan Image

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon successful authentication. 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 Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable DTLS
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.

QUESTION 90

Scenario

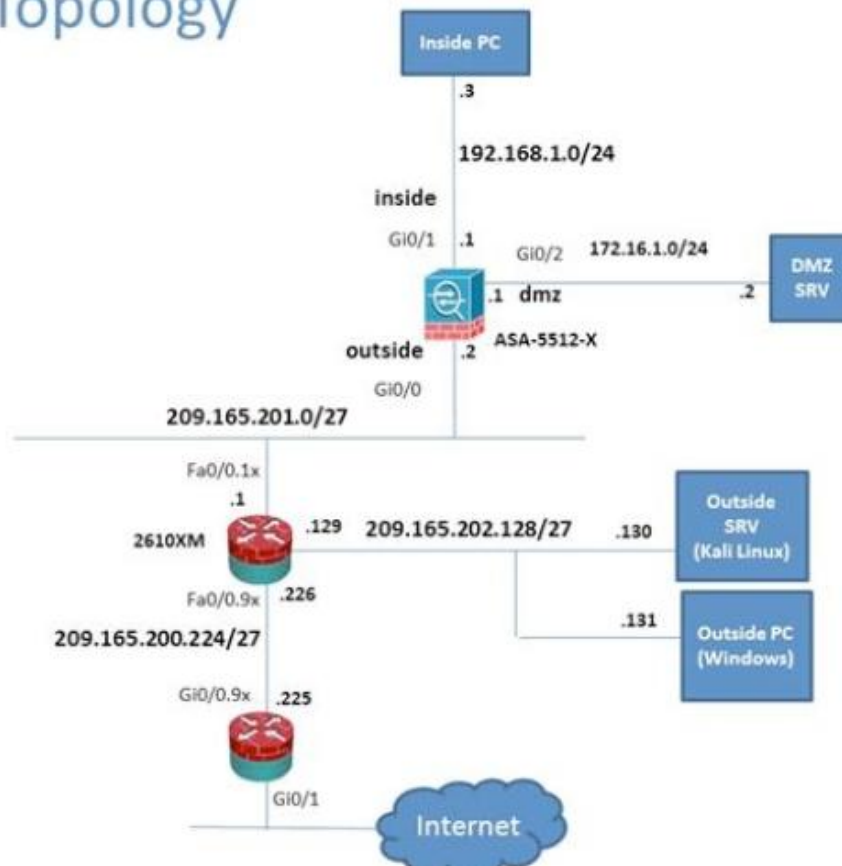
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions.

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 un-expand the expanded menu first.

Lab Topology



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 SSL VPN configurations.



<http://www.gratisexam.com/>

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Via - Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Edit



<http://www.gratisexam.com/>

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

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"/>

☒ Bypass interface access lists for inbound VPN sessions

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

Device Cert
 Port Sett

Press Edit button

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping fr



Add



Edit



Delete

Find:



☐ Match Case

Name	Enabled	Aliases	Authentication
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(RAD)
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>		AAA(RAD)
clientless	<input checked="" type="checkbox"/>	test	AAA(LOCAL)

Aliases:	test
Authentication	
Method:	<input checked="" type="radio"/> AAA <input type="radio"/> Certificate <input type="radio"/> Both
AAA Server Group:	LOCAL
<input type="checkbox"/> 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.)	
<input checked="" type="checkbox"/> Enable clientless SSL VPN protocol	



<http://www.gratisexam.com/>

QUESTION 91

Scenario

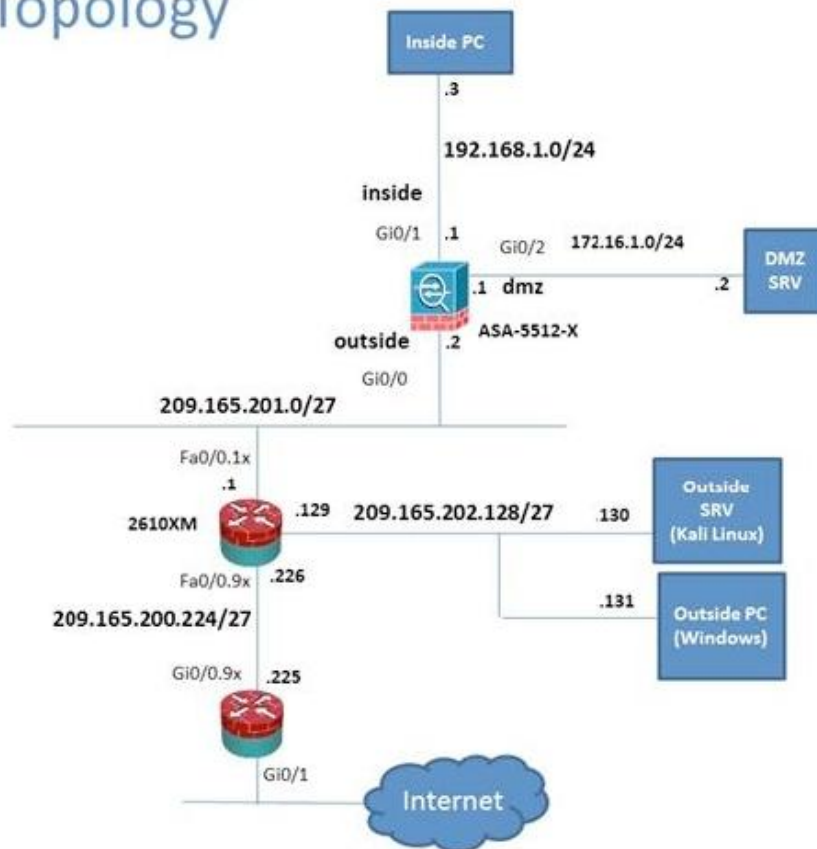
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions.

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 un-expand the expanded menu first.

Lab Topology



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 SSL VPN configurations.



<http://www.gratisexam.com/>

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

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

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 Certificate
 Port Setting

☒ 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. ⓘ

Connection Profiles

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

 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

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 > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
RAD	RADIUS	Single	Depletion	10	3
myAD	LDAP		Depletion	10	3
myCDA	RADIUS	Single	Depletion	10	3

Find: Match Case

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
---------------------------	-----------	---------

Find: Match Case

LDAP Attribute Map

Apply Reset

student 15 5/29/15 8:59:57 AM pst