

210-260.examcollection.premium.exam.68q

Number: 210-260
Passing Score: 800
Time Limit: 120 min
File Version: 4.0



210-260

Implementing Cisco Network Security

Version 4.0



Exam A**QUESTION 1**

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: (none)

Explanation

Explanation/Reference:

QUESTION 2

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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: (none)

Explanation

Explanation/Reference:

QUESTION 4

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: (none)

Explanation

Explanation/Reference:

QUESTION 5

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 6

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 7

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

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

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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 9

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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: (none)

Explanation

Explanation/Reference:

QUESTION 11

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 behavior 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: (none)

Explanation

Explanation/Reference:

QUESTION 12

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: (none)

Explanation

Explanation/Reference:

QUESTION 13

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: (none)

Explanation

Explanation/Reference:



QUESTION 14

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.
- 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: (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

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: (none)

Explanation



Explanation/Reference:

QUESTION 17

Which type of secure connectivity does an extranet provide?

- A. other company networks to your company network
- B. remote branch offices to your company network
- C. your company network to the Internet
- D. new networks to your company network

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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: (none)

Explanation

Explanation/Reference:

QUESTION 20

What type of attack was the Stuxnet virus?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

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 22

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: (none)

Explanation

Explanation/Reference:

QUESTION 23

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: (none)

Explanation

Explanation/Reference:



QUESTION 24

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: (none)

Explanation

Explanation/Reference:

QUESTION 25

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: (none)

Explanation

Explanation/Reference:

QUESTION 26

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: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which EAP method uses Protected Access Credentials?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

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: (none)

Explanation

Explanation/Reference:

QUESTION 29

What VPN feature allows traffic to exit the security appliance through the same interface it entered?

- A. hairpinning
- B. NAT
- C. NAT traversal
- D. split tunneling

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

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: (none)

Explanation

Explanation/Reference:

QUESTION 32

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: (none)

Explanation

Explanation/Reference:

**QUESTION 33**

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: (none)

Explanation

Explanation/Reference:

QUESTION 34

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: (none)

Explanation

Explanation/Reference:

QUESTION 35

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: (none)

Explanation

Explanation/Reference:



QUESTION 36

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: (none)

Explanation

Explanation/Reference:

QUESTION 37

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 38

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: (none)

Explanation

Explanation/Reference:

QUESTION 39

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 40

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: (none)

Explanation

Explanation/Reference:



QUESTION 41

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: (none)

Explanation

Explanation/Reference:**QUESTION 42**

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 43**

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: (none)

Explanation

Explanation/Reference:**QUESTION 44**

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: (none)

Explanation

Explanation/Reference:

QUESTION 45

What is a reason for an organization to deploy a personal firewall?

- A. To protect endpoints such as desktops from malicious activity.
- B. To protect one virtual network segment from another.
- C. To determine whether a host meets minimum security posture requirements.
- D. To create a separate, non-persistent virtual environment that can be destroyed after a session.
- E. To protect the network from DoS and syn-flood attacks.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 46

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: (none)

Explanation

Explanation/Reference:

QUESTION 47

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: (none)

Explanation

Explanation/Reference:

**QUESTION 48**

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: (none)

Explanation

Explanation/Reference:

QUESTION 49

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: (none)

Explanation

Explanation/Reference:

QUESTION 50

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 51

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: (none)

Explanation

Explanation/Reference:**QUESTION 52**

If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

- A. The ASA will apply the actions from only the first matching class map it finds for the feature type.
- B. The ASA will apply the actions from only the most specific matching class map it finds for the feature type.
- C. The ASA will apply the actions from all matching class maps it finds for the feature type.
- D. The ASA will apply the actions from only the last matching class map it finds for the feature type.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 53**

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: (none)

Explanation

Explanation/Reference:**QUESTION 54**

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 55

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: (none)

Explanation

Explanation/Reference:



QUESTION 56

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: (none)

Explanation

Explanation/Reference:

QUESTION 57

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: (none)

Explanation

Explanation/Reference:

QUESTION 58

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: (none)

Explanation

Explanation/Reference:

QUESTION 59

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: (none)

Explanation

Explanation/Reference:

QUESTION 60

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: (none)

Explanation

Explanation/Reference:



QUESTION 61

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: (none)

Explanation

Explanation/Reference:

QUESTION 62

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: (none)

Explanation

Explanation/Reference:

QUESTION 63

Which statement about application blocking is true?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

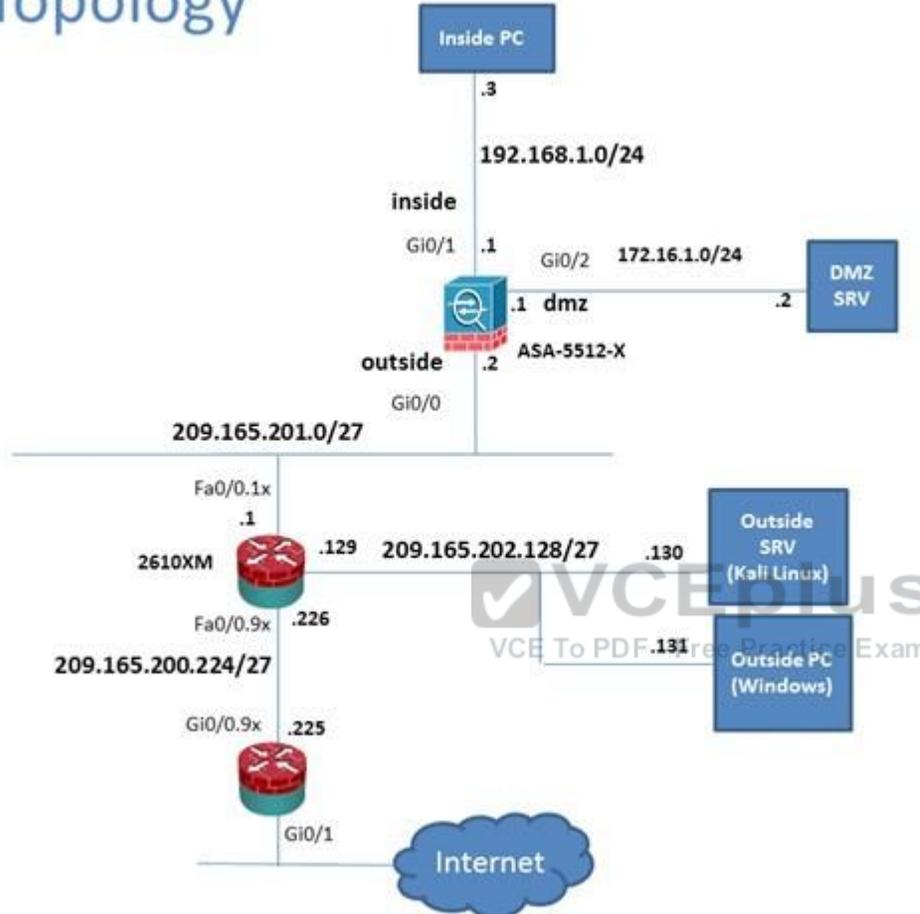
Scenario

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 un-expand the expanded menu first.

Lab Topology



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is divided into several sections:

- Device Information:**
 - Host Name: P17-ASA-secure-x-local
 - ASA Version: 100.14(6)13
 - ASDM Version: 7.5(8)1
 - Firewall Model: Routed
 - Environment Status: OK
 - Device Uptime: 11d 28h 42m 47s
 - Device Type: ASA 5512
 - Context Mode: Single
 - Total Flash: 4096 MB
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	up	up	0
inside	192.168.1.1/24	up	up	4
mgmt	10.10.10.1/24	up	up	0
outside	209.165.201.2/24	up	up	0
- System Resources Status:**
 - Total Memory Usage: 1024 MB
 - Total CPU Usage: 0%
 - Core Usage: 0%
- Traffic Status:**
 - Connections Per Second Usage: 0
 - Outside Interface Traffic Usage (Kbps): 0
 - Input Kbps: 0, Output Kbps: 0
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina Description
6	May 13 2015	12:35:09	302016	10.81.254.202	123	209.165.201.2	65535 Tear-down UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:00:01 bytes 96
6	May 13 2015	12:35:08	109015	192.168.1.3	14676	192.168.1.1	443 Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6	May 13 2015	12:35:08	302014	192.168.1.3	14676	192.168.1.1	443 Tear-down TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 289 TCP Reset=0

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.30.14.3820	No
inside	192.168.1.4	0050.56.33.3333	No
inside	192.168.1.3	0050.56.11.1111	No
inside	192.168.1.2	0050.56.22.2222	No
inside	192.168.1.26	0050.5692.3c7c	No
inside	192.168.1.55	0006.86e4.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.30.14.3820	No

Refresh

Clear Dynamic ARP Entries

Data Refreshed Successfully.

Last Updated: 5/19/15 9:32:02 AM

student 15 5/19/15 9:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/Phase Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- NM Proxy Statistics
- NM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN		1	1	1
Browser		1	1	1

Filter By: Clientless SSL VPN All Sessions Filter

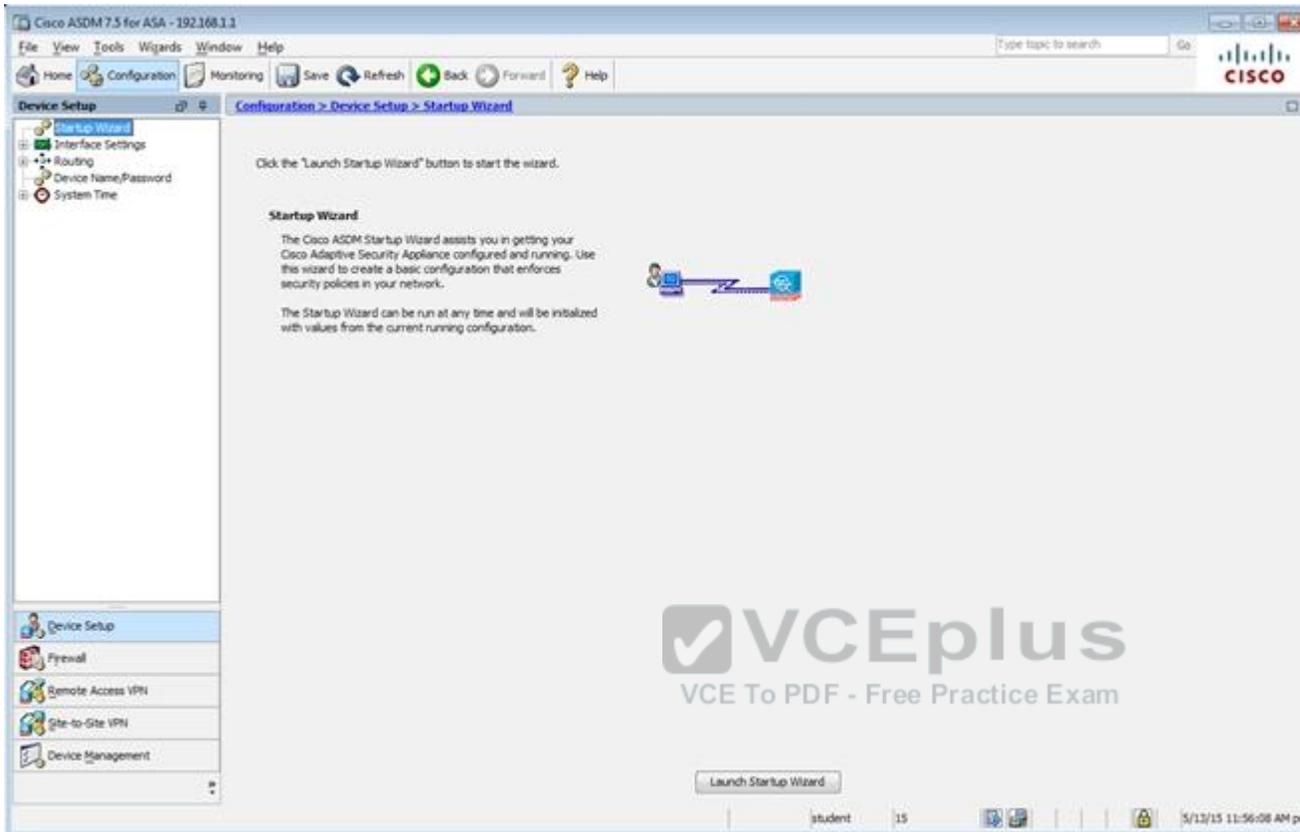
Username	IP Address	Group Policy	Connection Profile	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
student	209.165.202.131	Sales	Clientless	Clientless	Clientless (IPsec)	08:05:46 pm Thu May 21 2015	0h:09m:19s	316774	41633

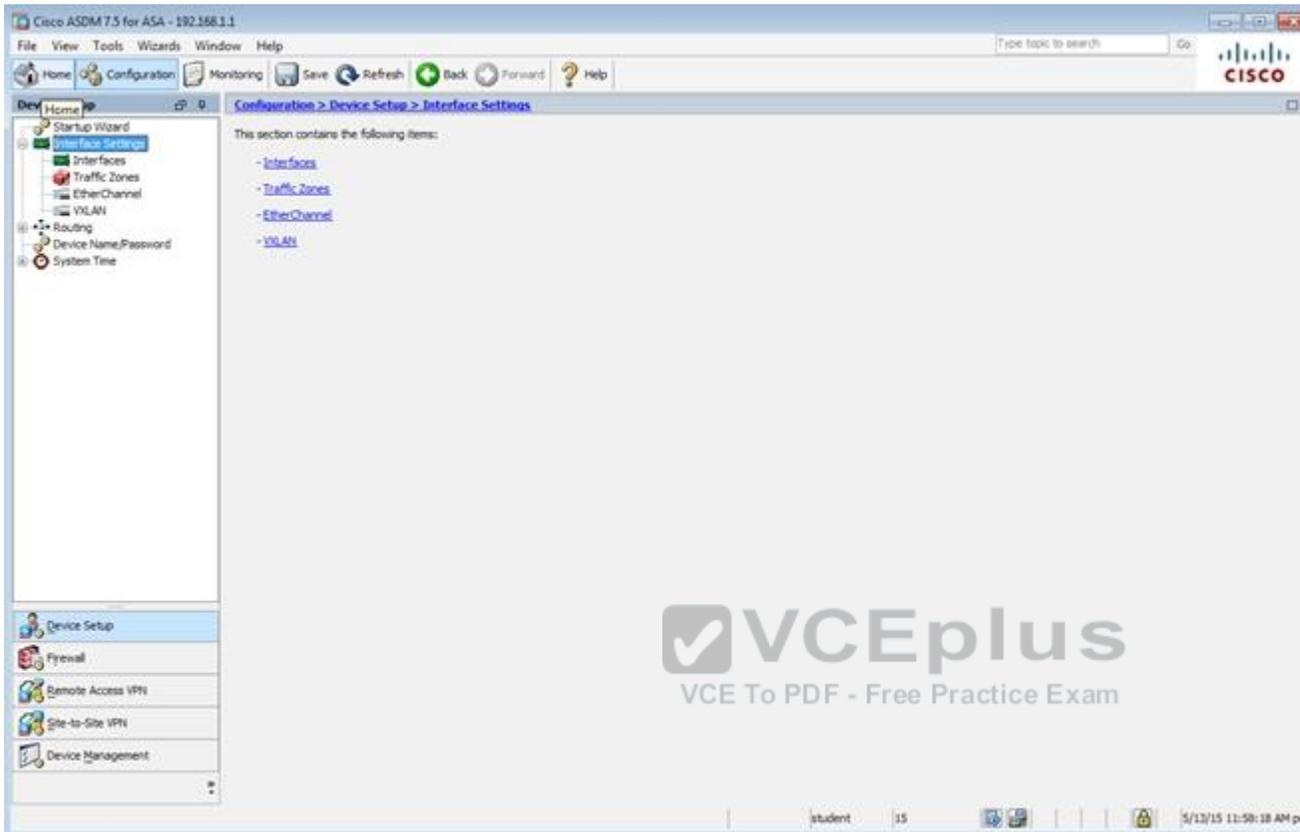
Details Logout Ping Refresh

Last Updated: 5/19/15 9:33:12 AM

Data Refreshed Successfully. student 15 5/19/15 8:33:37 AM pst



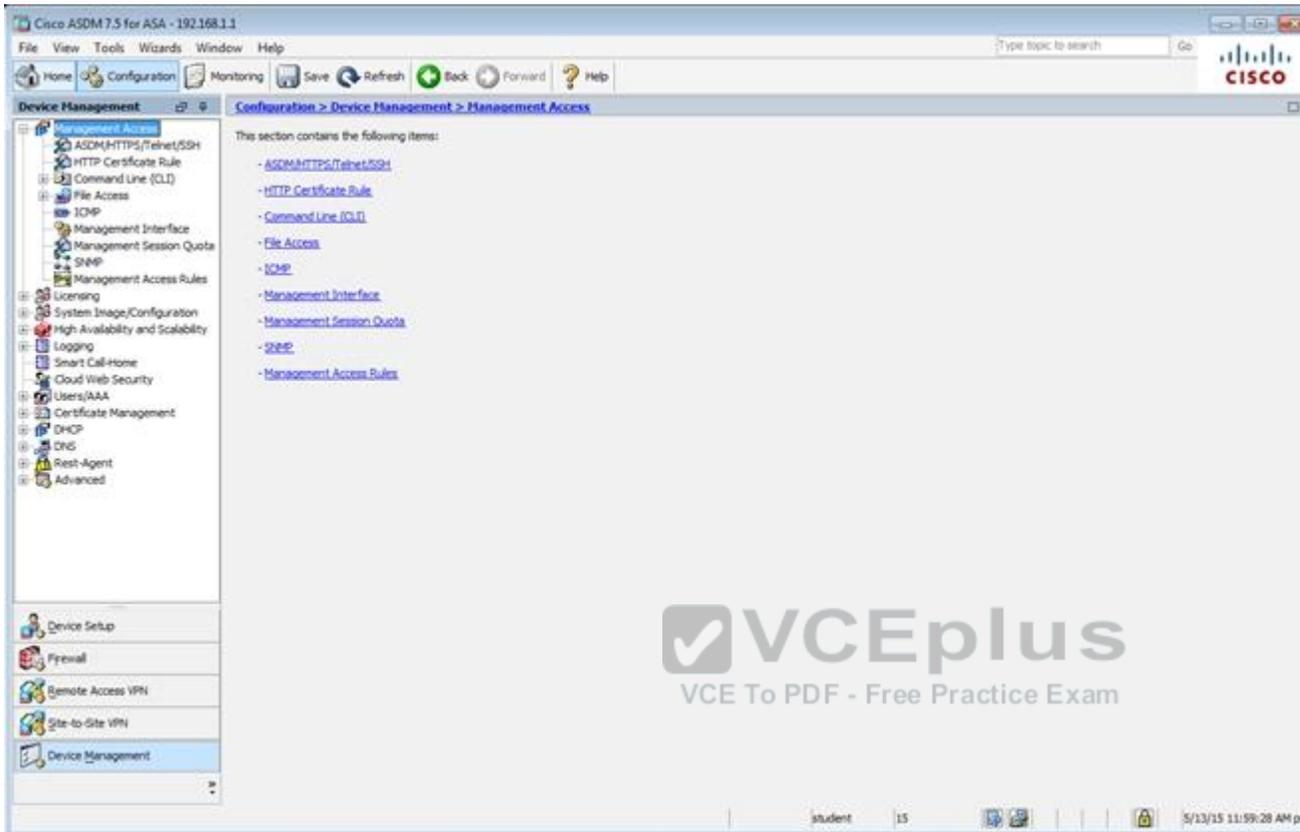




The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration page for Interfaces, with a table listing various interfaces and their settings. The table has columns for Interface, Name, Zone, Route Map, State, Security Level, IP Address, Subnet Mask Prefix Length, Group, and Type. The interfaces listed are GigabitEthernet0/0 through Management0/0. The 'outside' zone is highlighted in blue. Below the table, there are three checkboxes for enabling traffic between interfaces with the same security levels, between hosts connected to the same interface, and for enabling jumbo frame reservation. The 'Apply' and 'Reset' buttons are visible at the bottom of the configuration area.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled	0	209.165.201.2	255.255.255.0		Hardware
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1	255.255.255.0		Hardware
GigabitEthernet0/2	dmz			Enabled		172.16.1.1	255.255.255.0		Hardware
GigabitEthernet0/3				Enabled					Hardware
GigabitEthernet0/4				Enabled					Hardware
GigabitEthernet0/5	mgmt			Enabled	500	10.10.10.2	255.255.255.0		Hardware
Management0/0				Enabled					Hardware

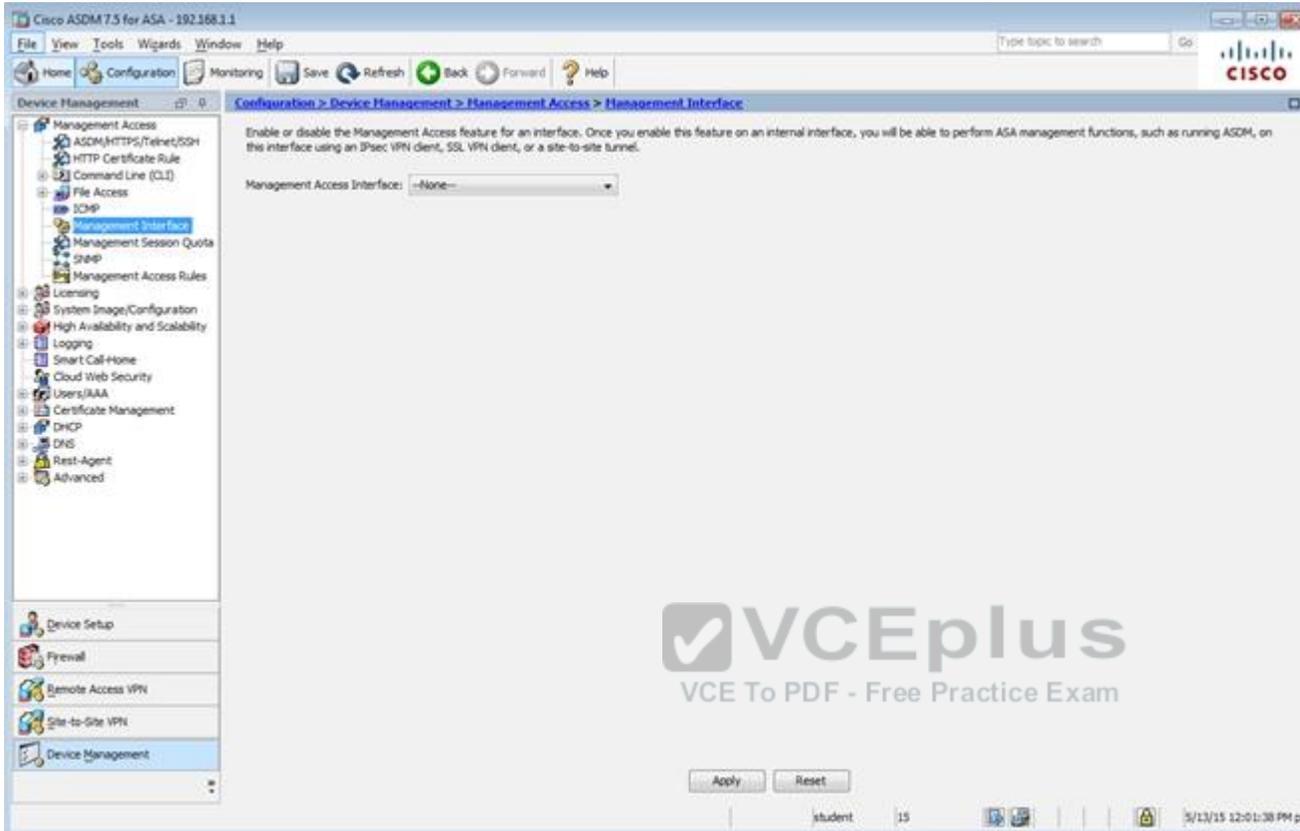
Enable traffic between two or more interfaces which are configured with same security levels
 Enable traffic between two or more hosts connected to the same interface
 Enable jumbo frame reservation

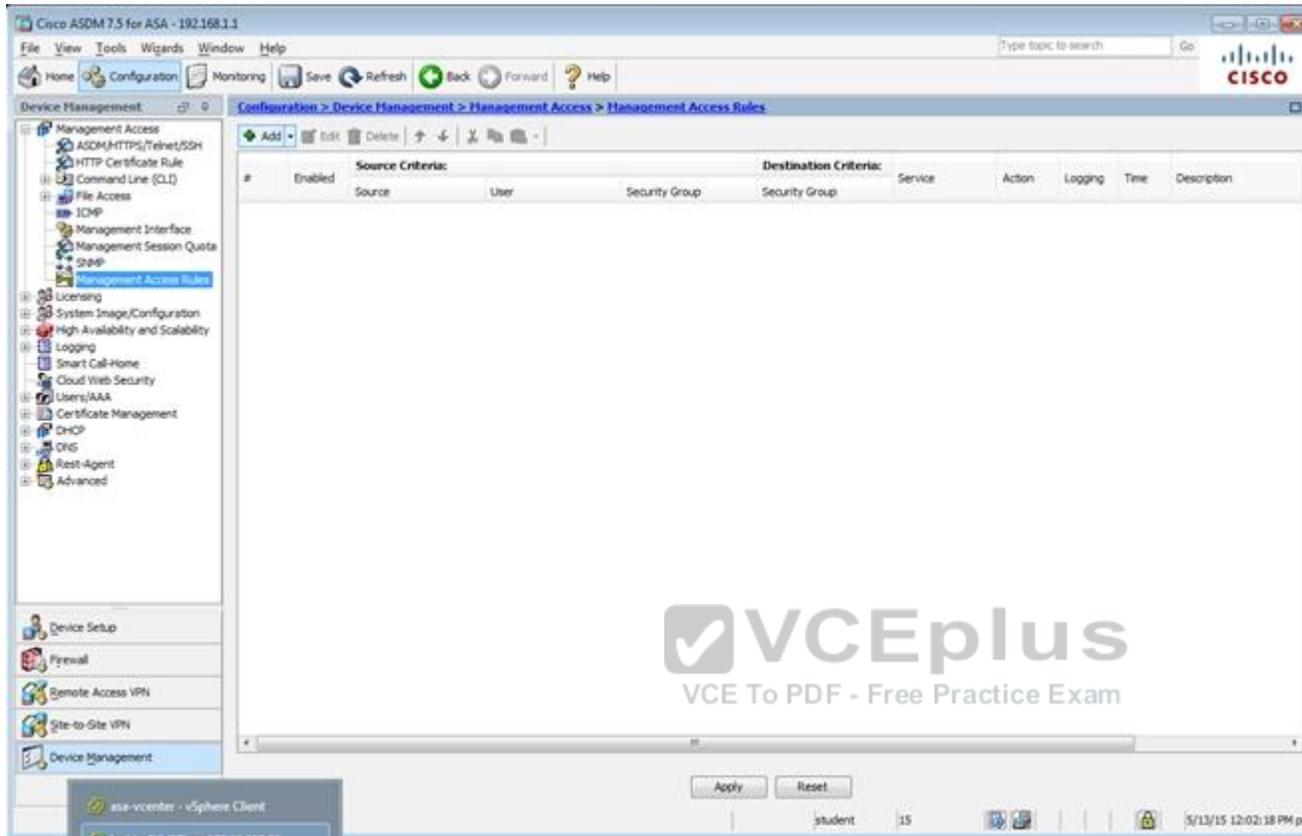


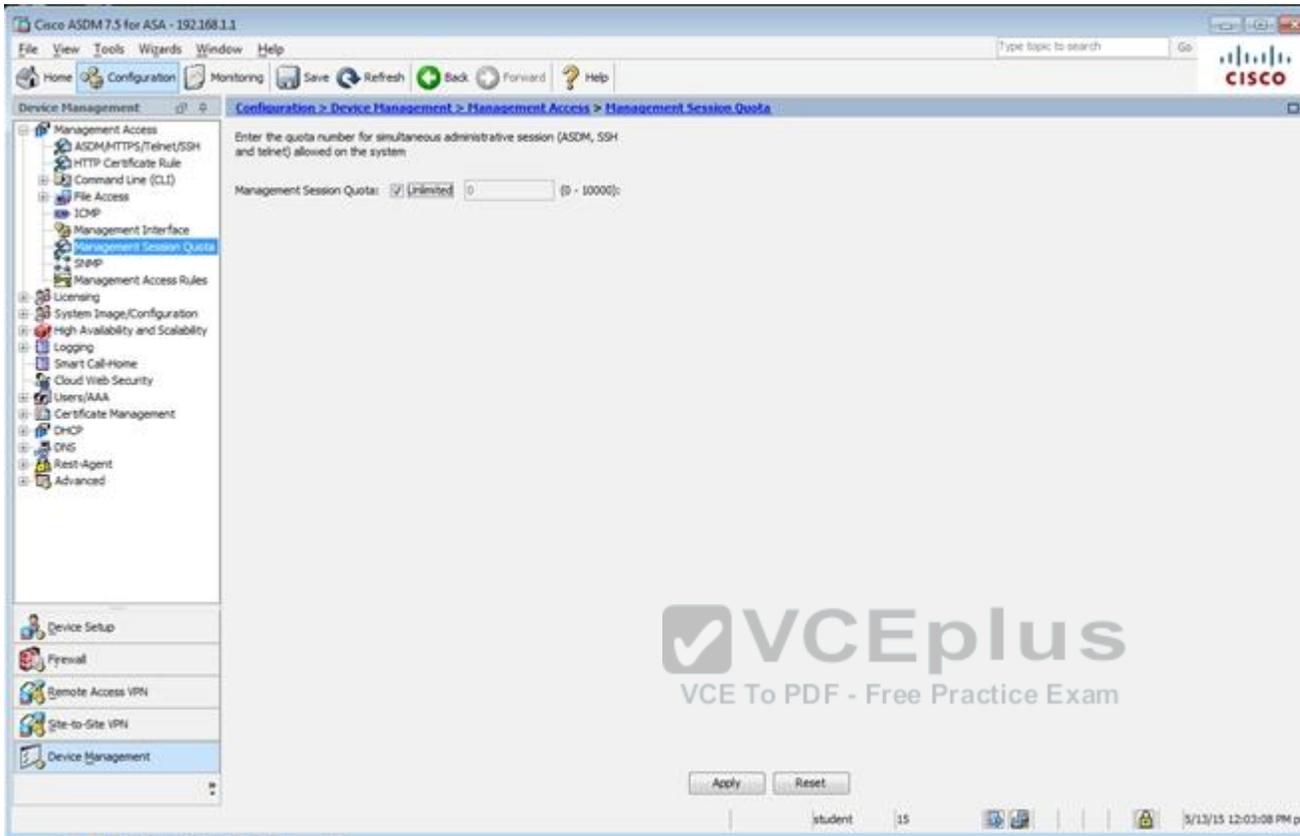
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows a tree view of configuration categories, with "Management Access" selected. The main content area displays a table for "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH".

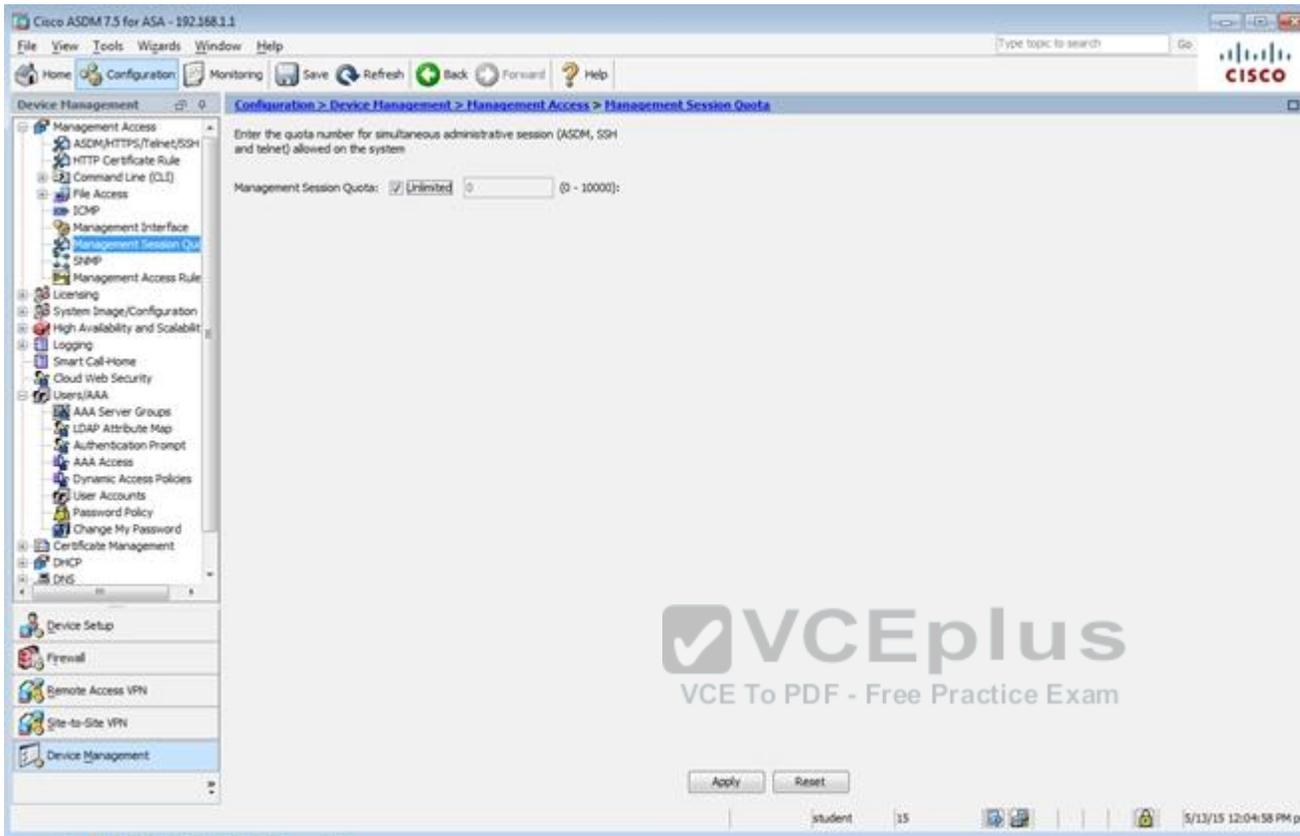
Type	Interface	IP Address	Mask/Prefix Length
Telnet	mgmt	10.10.10.1	255.255.255.255
SSH	inside	192.168.1.2	255.255.255.255
ASDM/HTTPS	inside	192.168.1.0	255.255.255.0

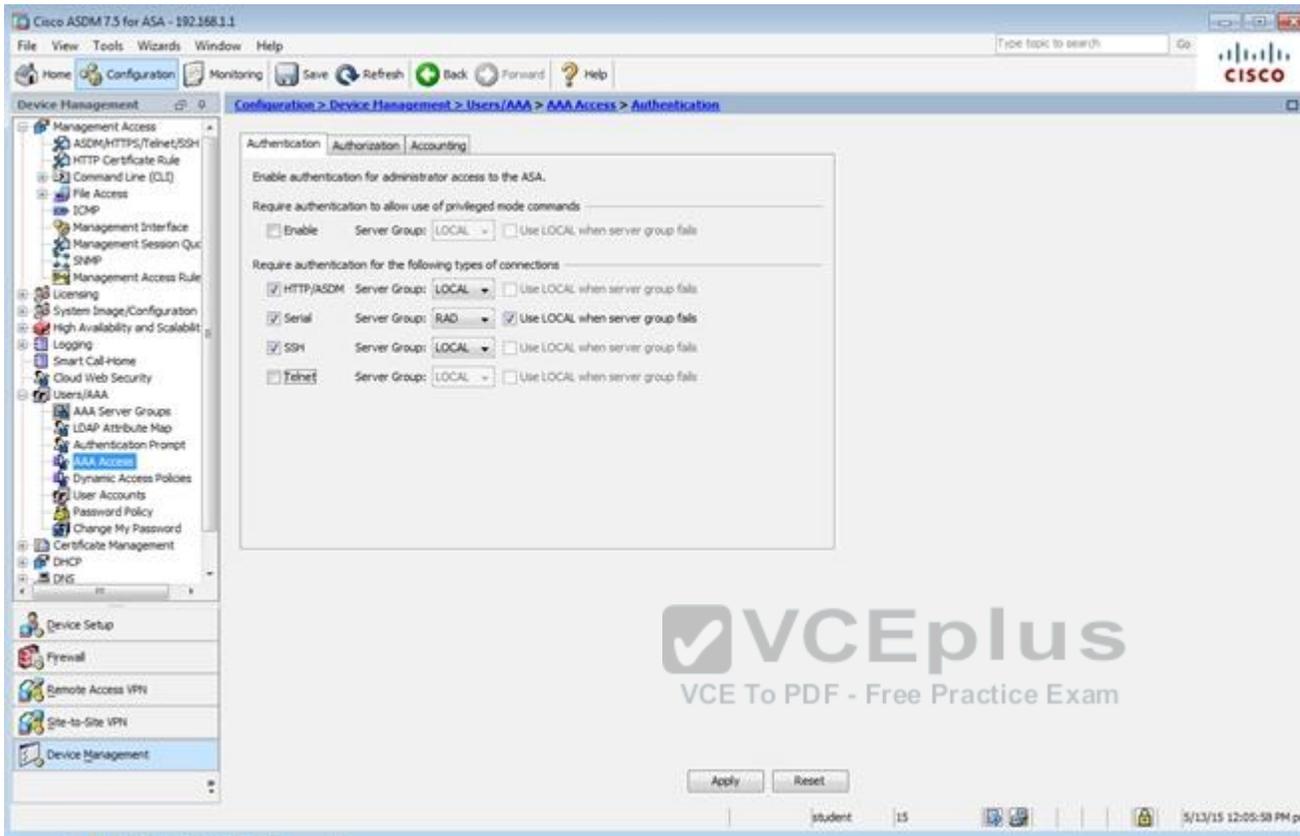
Below the table are sections for "Http Settings" (with "Enable HTTP Server" checked and port 443), "Telnet Settings" (with "Telnet Timeout" set to 5 minutes), and "SSH Settings" (with "Allowed SSH Version(s)" set to 1 & 2 and "SSH Timeout" set to 5 minutes). There are "Apply" and "Reset" buttons at the bottom.







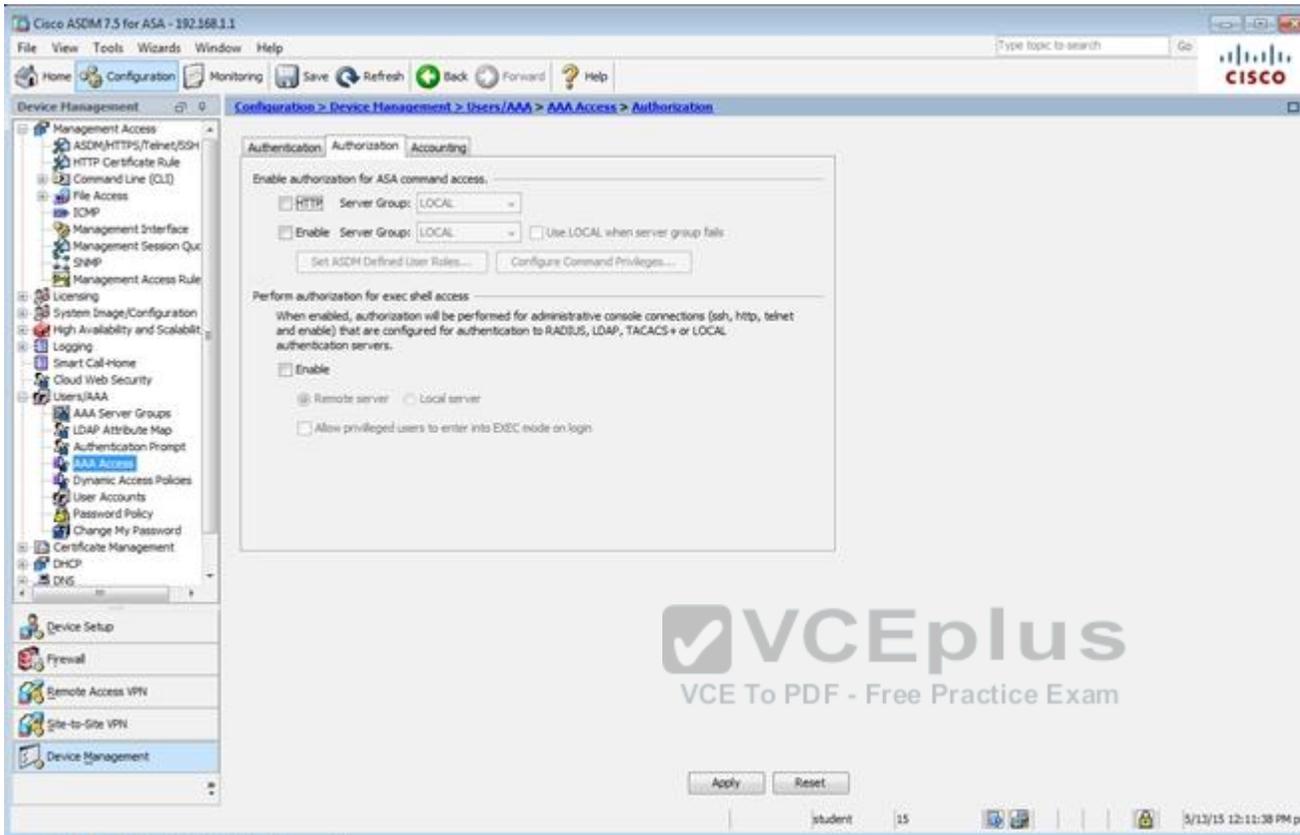




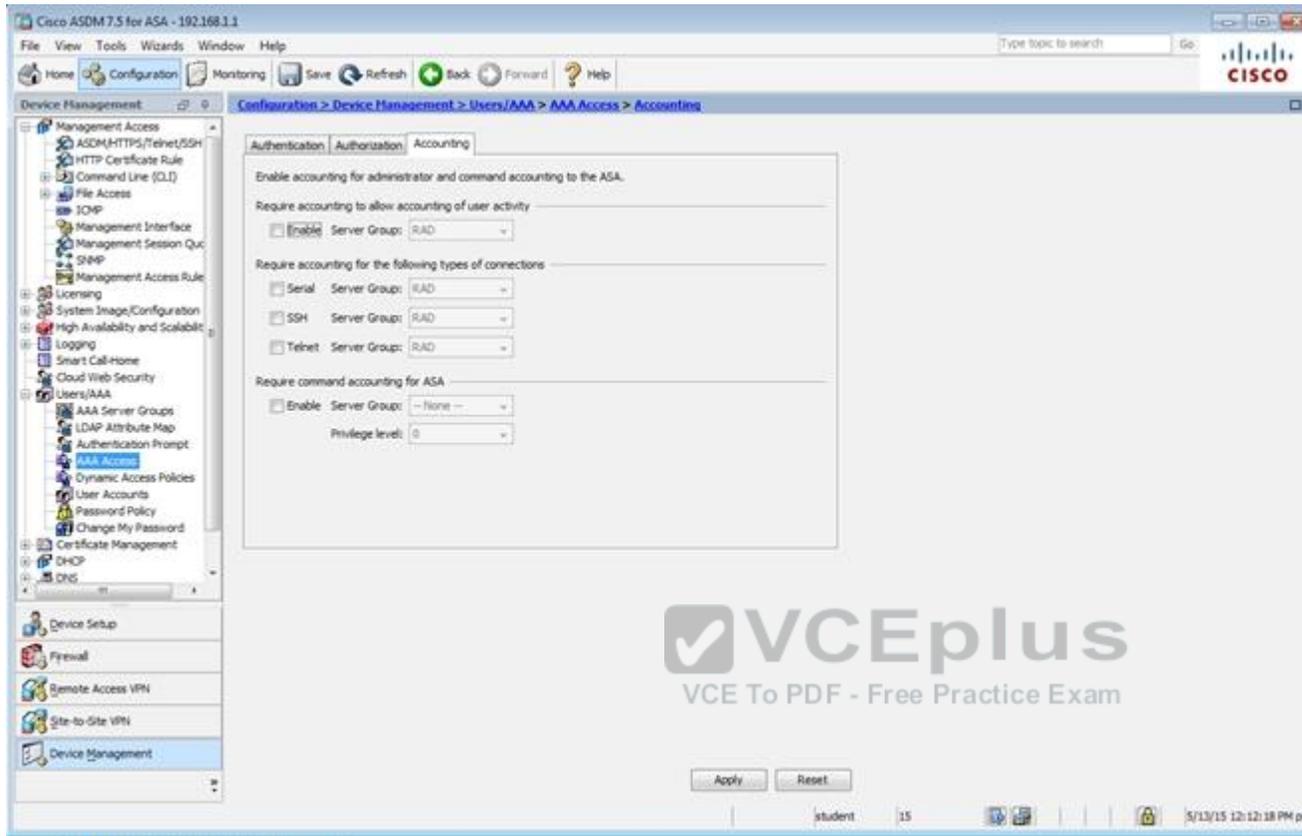
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The breadcrumb trail is Configuration > Device Management > Users/AAA > AAA Access > Authentication. The left sidebar shows a tree view with 'Users/AAA' expanded to 'AAA Access'. The main content area has three tabs: Authentication, Authorization, and Accounting. The 'Authentication' tab is active and contains the following configuration options:

- Enable authentication for administrator access to the ASA. (checked)
- Require authentication to allow use of privileged mode commands:
 - Enable
 - Server Group: LOCAL
 - Use LOCAL when server group fails
- Require authentication for the following types of connections:
 - HTTP/ASDM: Server Group: LOCAL, Use LOCAL when server group fails
 - Serial: Server Group: RAD, Use LOCAL when server group fails
 - SSH: Server Group: LOCAL, Use LOCAL when server group fails
 - Telnet: Server Group: LOCAL, Use LOCAL when server group fails

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The status bar at the very bottom shows 'student | 15 | 5/13/15 12:00:58 PM pet'.



The screenshot shows the Cisco ASDM 7.5 for ASA interface. The title bar reads "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation path is "Configuration > Device Management > Users/AAA > AAA Access > Authorization". The left sidebar contains a tree view with categories like "Management Access", "Licensing", "System Image/Configuration", "High Availability and Scalability", "Logging", "Users/AAA", "Certificate Management", "Device Setup", "Firewall", "Remote Access VPN", "Site-to-Site VPN", and "Device Management". The main content area is titled "Authorization" and has three tabs: "Authentication", "Authorization", and "Accounting". The "Authorization" tab is active, showing two sections: "Enable authorization for ASA command access" and "Perform authorization for exec shell access". The first section has checkboxes for "RTM" and "Enable", both currently unchecked. The "RTM" checkbox is accompanied by a "Server Group" dropdown menu set to "LOCAL". The "Enable" checkbox is also accompanied by a "Server Group" dropdown menu set to "LOCAL" and an unchecked checkbox labeled "Use LOCAL when server group fails". Below these are two buttons: "Set ASDM Defined User Roles..." and "Configure Command Privileges...". The second section, "Perform authorization for exec shell access", has a description: "When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers." It has an unchecked "Enable" checkbox and two radio buttons: "Remote server" (selected) and "Local server". Below these is an unchecked checkbox labeled "Allow privileged users to enter into EXEC mode on login". At the bottom of the configuration area are "Apply" and "Reset" buttons. The system tray at the bottom shows the user "student", the number "15", and the date/time "5/13/15 12:11:38 PM pst".

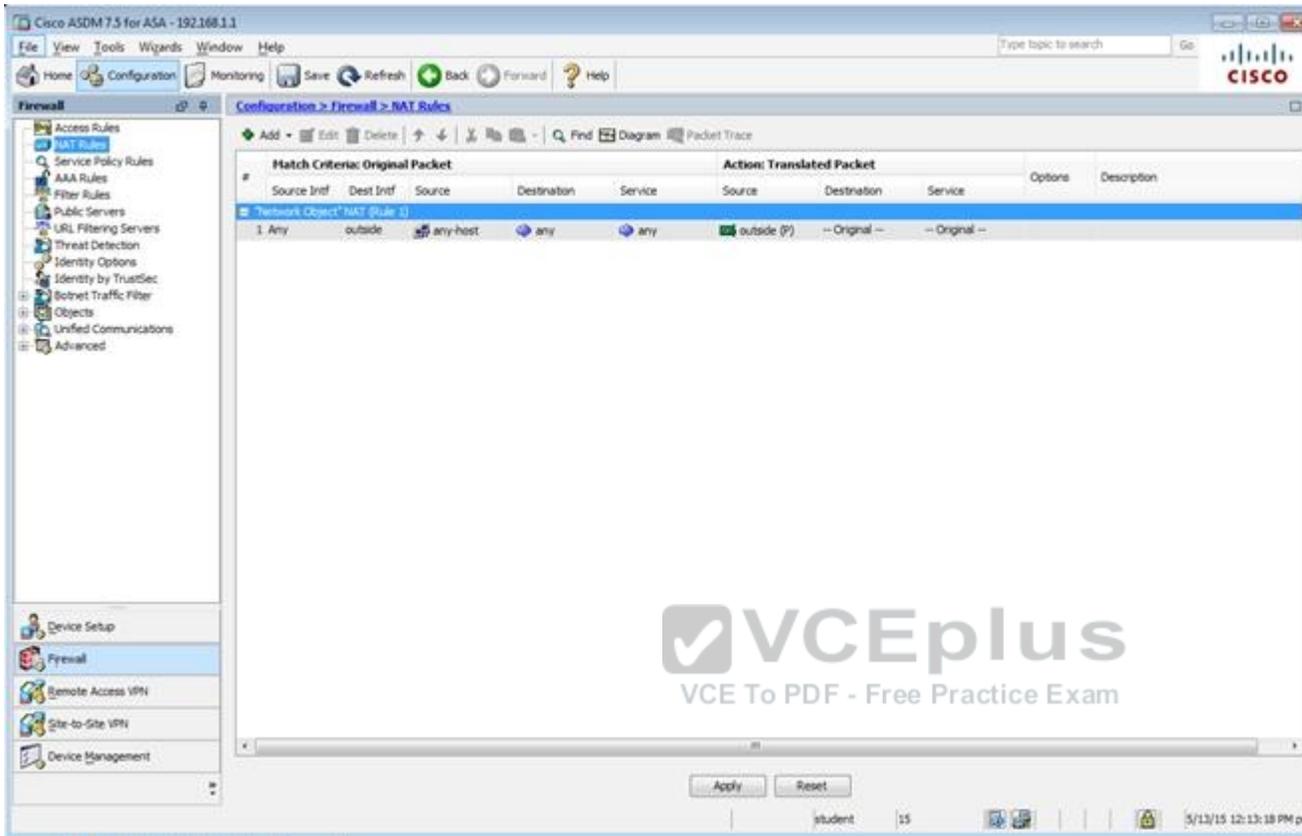


The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > Users/AAA > AAA Access > Accounting. The left sidebar shows a tree view with 'Users/AAA' expanded to 'AAA Access'.

The main configuration area has three tabs: Authentication, Authorization, and Accounting. The Accounting tab is active and contains the following settings:

- Enable accounting for administrator and command accounting to the ASA. **Enable**
- Require accounting to allow accounting of user activity. **Enable** Server Group: RAD
- Require accounting for the following types of connections:
 - Serial Server Group: RAD
 - SSH Server Group: RAD
 - Telnet Server Group: RAD
- Require command accounting for ASA. **Enable** Server Group: -- None -- Privilege level: 0

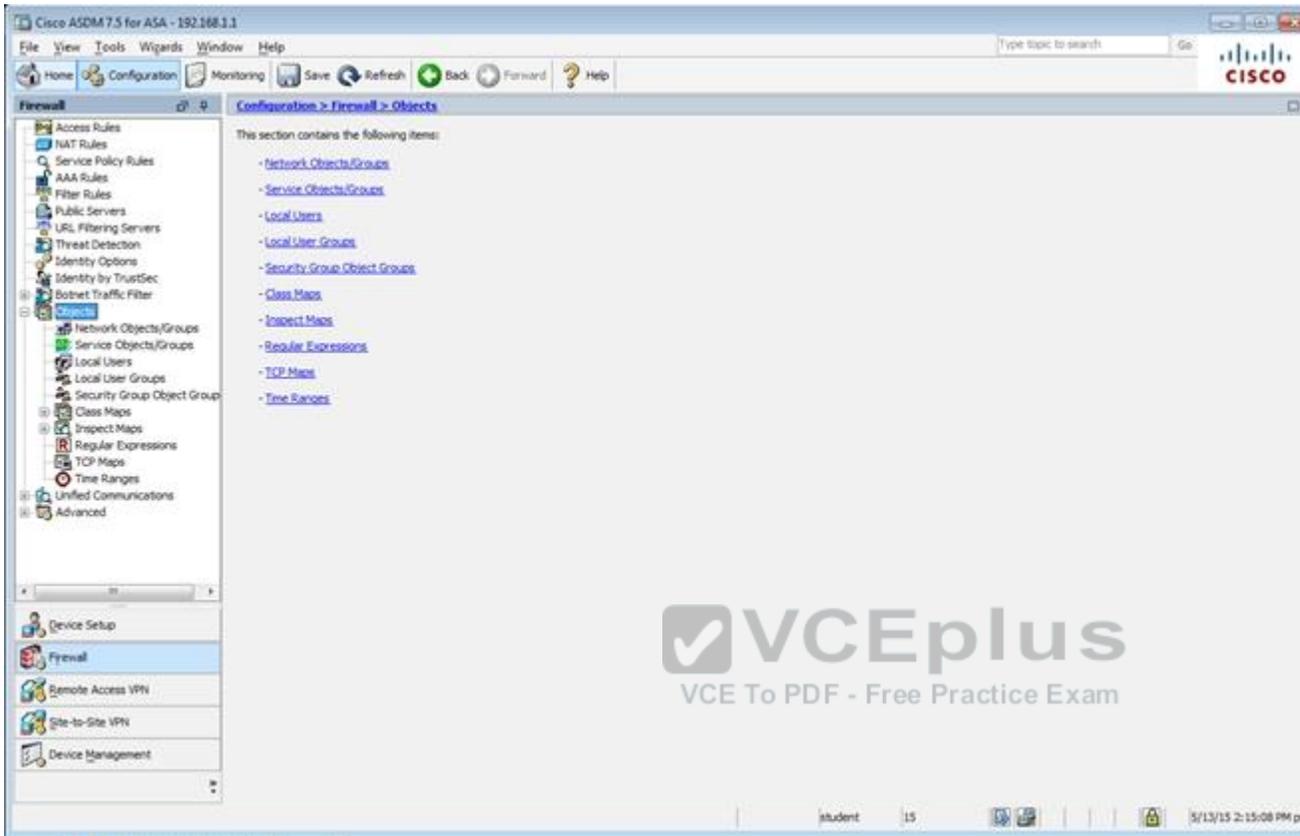
At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The status bar at the very bottom shows 'student | 15 | 5/13/15 12:18 PM pst'.



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for NAT Rules. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table with columns for Match Criteria and Action. The table contains one rule with the following details:

Match Criteria: Original Packet				Action: Translated Packet			Options	Description
Source Intf	Dest Intf	Source	Destination	Source	Destination	Service		
1. Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --	

At the bottom of the window, there are 'Apply' and 'Reset' buttons. The status bar at the bottom right shows the user 'student', the page number '15', and the date/time '5/13/15 12:13:18 PM pet'. A large watermark for VCEplus is visible in the center of the screen.



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End: Match Case

Apply Reset

student 15 5/13/15 12:14:18 PM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Network Objects/Groups

Filter: [Clear]

Name	IP Address	Netmask	Description	Object NAT Address
any				
any-host	0.0.0.0	0.0.0.0		outside (P)
any4				
any6				
facebook	www.facebook.com			
My_ASA_Demo_Obj	1.10.8.20			

Apply Reset

student 15 5/13/15 12:30:08 PM pet

VCEplus
VCE To PDF - Free Practice Exam

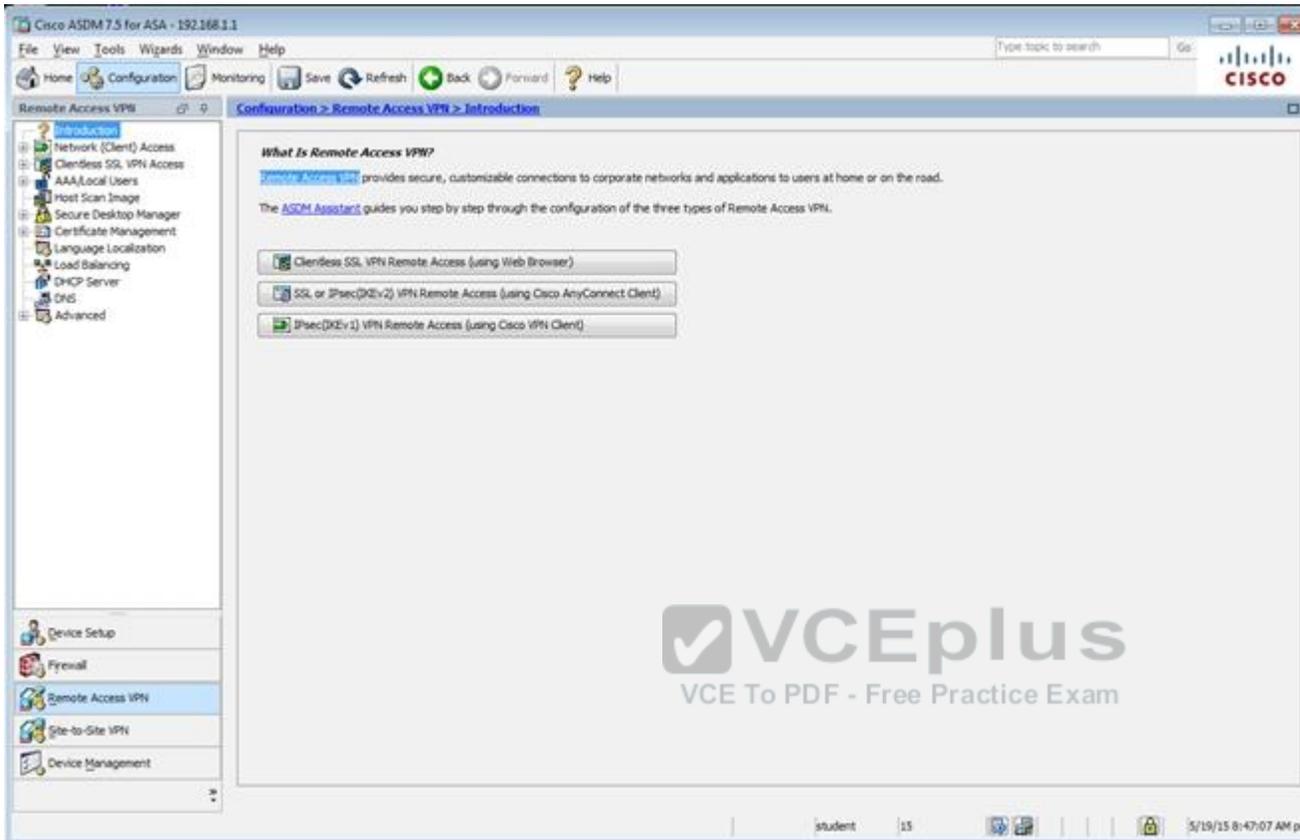
The screenshot displays the Cisco ASDM 7.5 for ASA - 292.168.1.1 interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left sidebar shows a tree view of configuration categories, with "Firewall" selected. The main area shows a table of "Traffic Classification" rules. The table has columns for Name, #, Enabled, Match, Source, Src Security Group, Destination, Dst Security Group, Service, Time, Rule Actions, and Description. Three rules are visible: "Interface: dmz; Policy: asash_policy", "Interface: inside; Policy: asash_policy", and "Global; Policy: global_policy". The "Global; Policy: global_policy" rule is expanded to show its actions: "default-inspec...", "Inspect DNS Map preset...", "Inspect ESMTP", and "(14 more inspect actions)".

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Interface: dmz; Policy: asash_policy			Match	any		any		any traffic class-default			
Interface: inside; Policy: asash_policy			Match	any		any		any traffic class-default			
Global; Policy: global_policy			Match	any		any		default-inspec...		Inspect DNS Map preset... Inspect ESMTP (14 more inspect actions)	

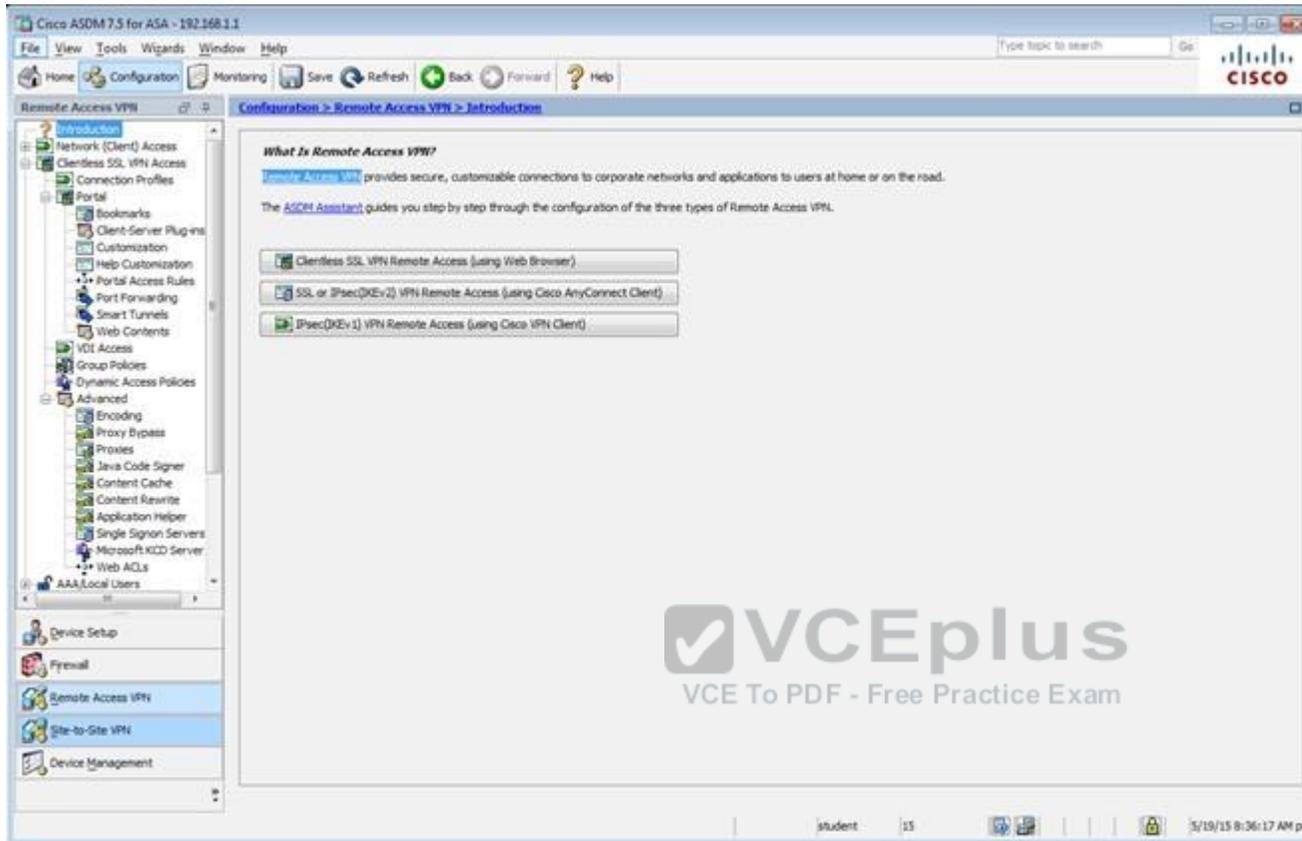
The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Access Rules". The left sidebar shows a tree view of configuration options, with "Firewall" selected. The main area contains a table of access rules. The table has columns for #, Enabled, Source Criteria, Destination Criteria, Service, Action, Hits, and Logging. The rules listed are:

#	Enabled	Source Criteria	Destination Criteria	Service	Action	Hits	Logging
1	<input checked="" type="checkbox"/>	any	Any less secure ne...	IP-IP	Permit		
1	<input checked="" type="checkbox"/>	inside (1 incoming rule)	any	IP-IP	Permit	54...	
1	<input checked="" type="checkbox"/>	ingmt (0 implicit incoming rules)	any	IP-IP	Permit		
1	<input checked="" type="checkbox"/>	outside (0 implicit incoming rules)	any	IP-IP	Permit		
1	<input checked="" type="checkbox"/>	Global (1 implicit rule)	any	IP-IP	Deny		

At the bottom of the window, there are buttons for "Apply", "Reset", and "Advanced...". The status bar at the bottom shows "student 15" and the date/time "5/13/15 12:28:58 PM pdt".



The screenshot displays the Cisco ASDM 7.5 for ASA interface. The title bar reads "Cisco ASDM 7.5 for ASA - 192.168.1.1". The main window is titled "Remote Access VPN" and shows the "Configuration > Remote Access VPN > Introduction" page. The left sidebar contains a navigation tree with categories like "Network (Client) Access", "Clientless SSL VPN Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". Below the sidebar are buttons for "Device Setup", "Firewall", "Remote Access VPN", "Site-to-Site VPN", and "Device Management". The main content area is titled "What Is Remote Access VPN?" and contains the following text: "Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road. The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN." Below this text are three buttons: "Clientless SSL VPN Remote Access (using Web Browser)", "SSL or IPsec(DKEv2) VPN Remote Access (using Cisco AnyConnect Client)", and "IPsec(DKEv1) VPN Remote Access (using Cisco VPN Client)". A large "VCEplus VCE To PDF - Free Practice Exam" watermark is overlaid on the bottom right of the screenshot. The status bar at the bottom shows "student | 15 | 5/19/15 8:47:07 AM pst".



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

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.

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 can configure the mapping from certificate to connection profile [here](#).

Find:

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultSAGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
DefaultEVPNGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
Services	<input checked="" type="checkbox"/>	test	LOCAL	Default

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Apply Reset

student 15 5/19/15 8:38:47 AM pst

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL Manage...
 Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS Manage...
(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2
Domain Name: secure-x.local

Default Group Policy

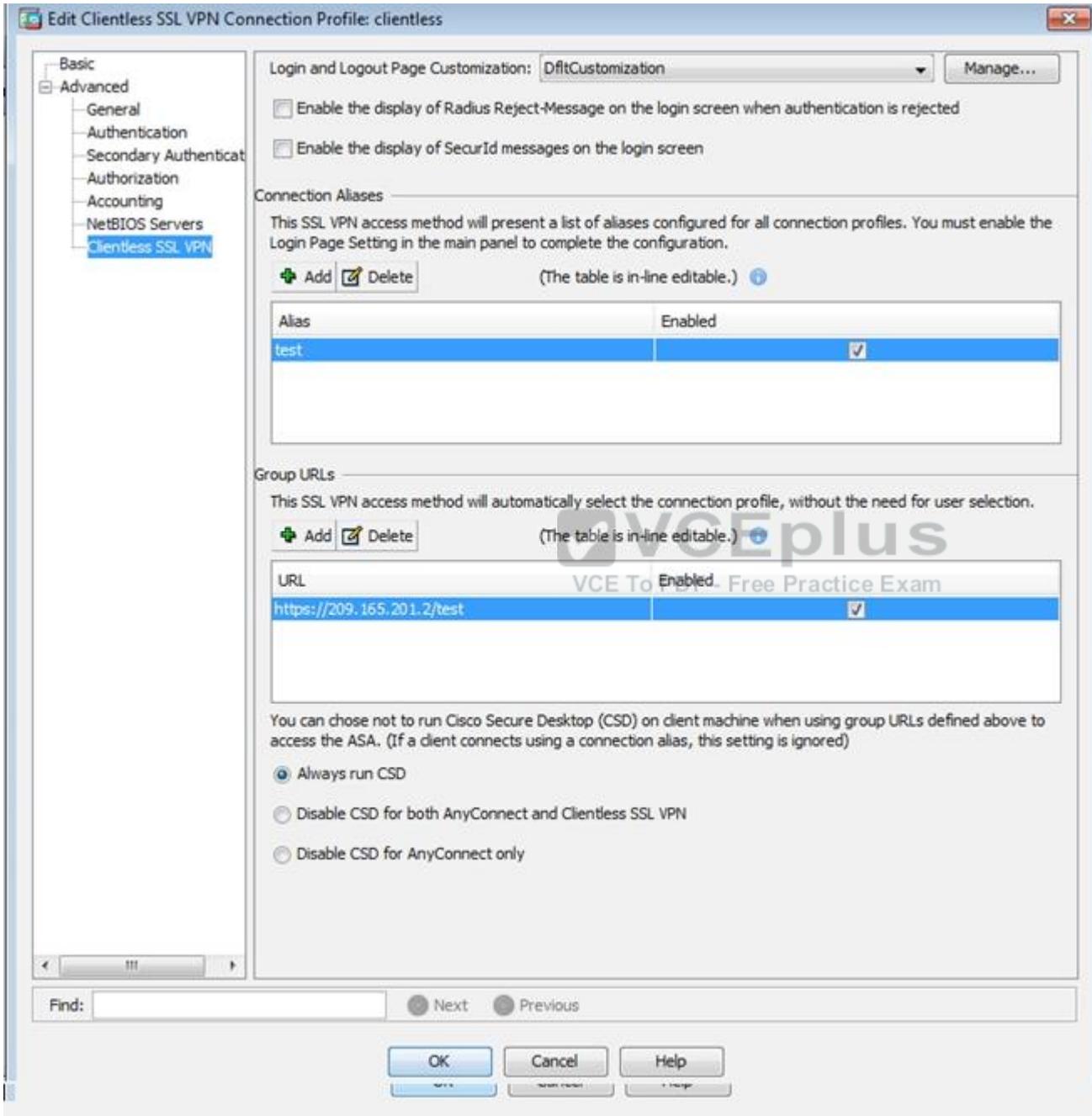
Group Policy: Sales Manage...
(Following field is an attribute of the group policy selected above.)

Enable clientless SSL VPN protocol

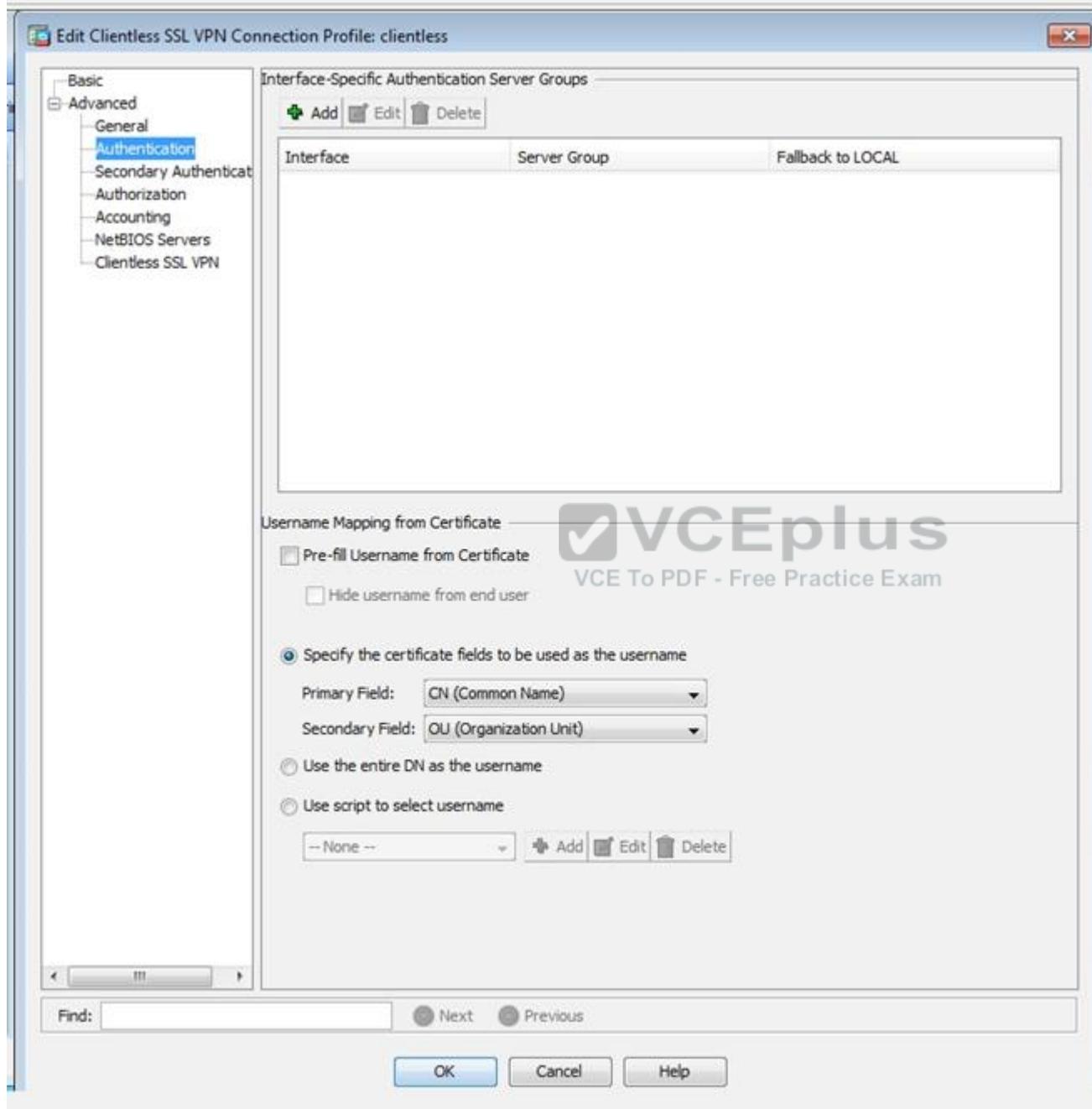
Find: Next Previous

OK Cancel Help

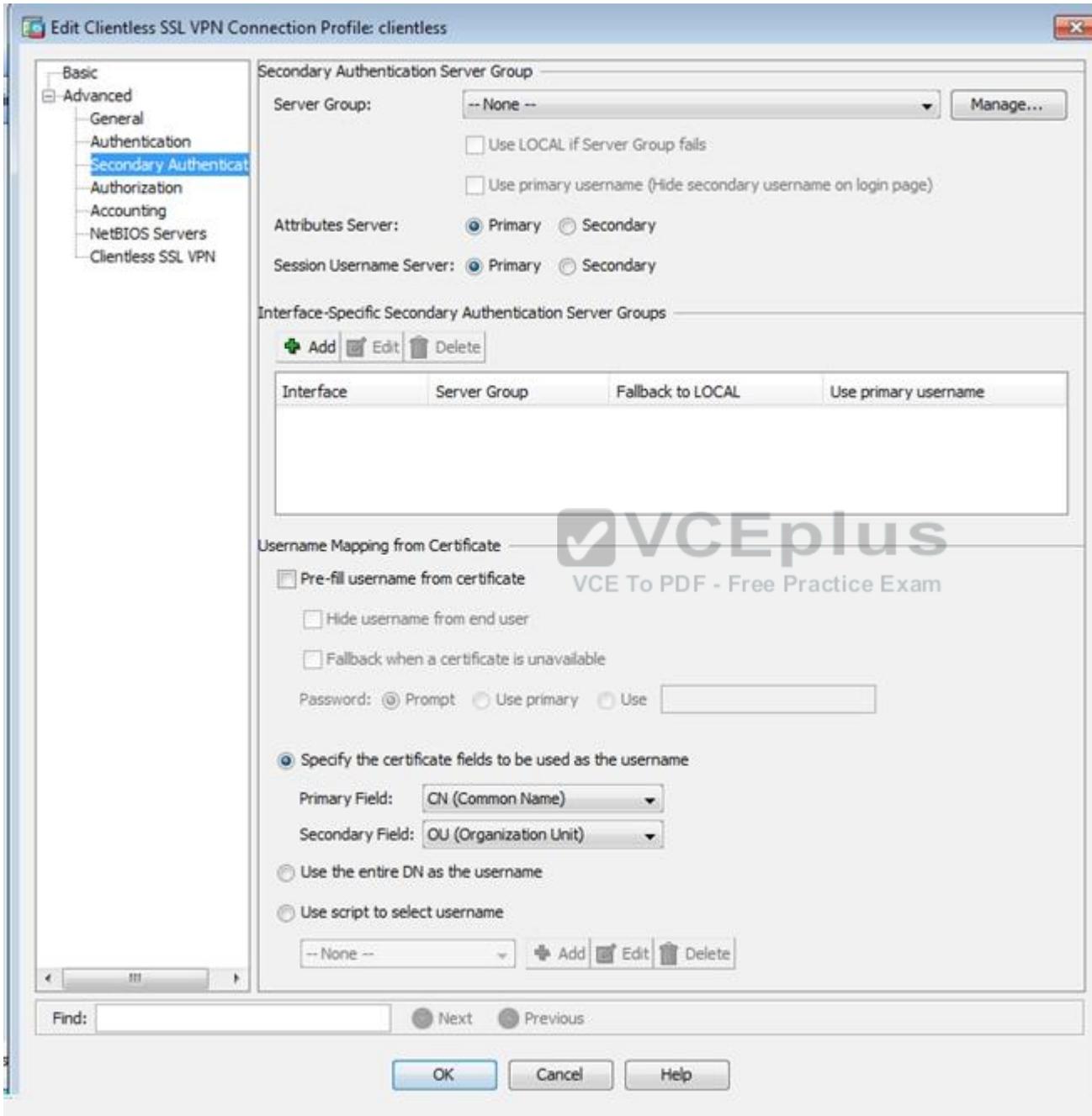


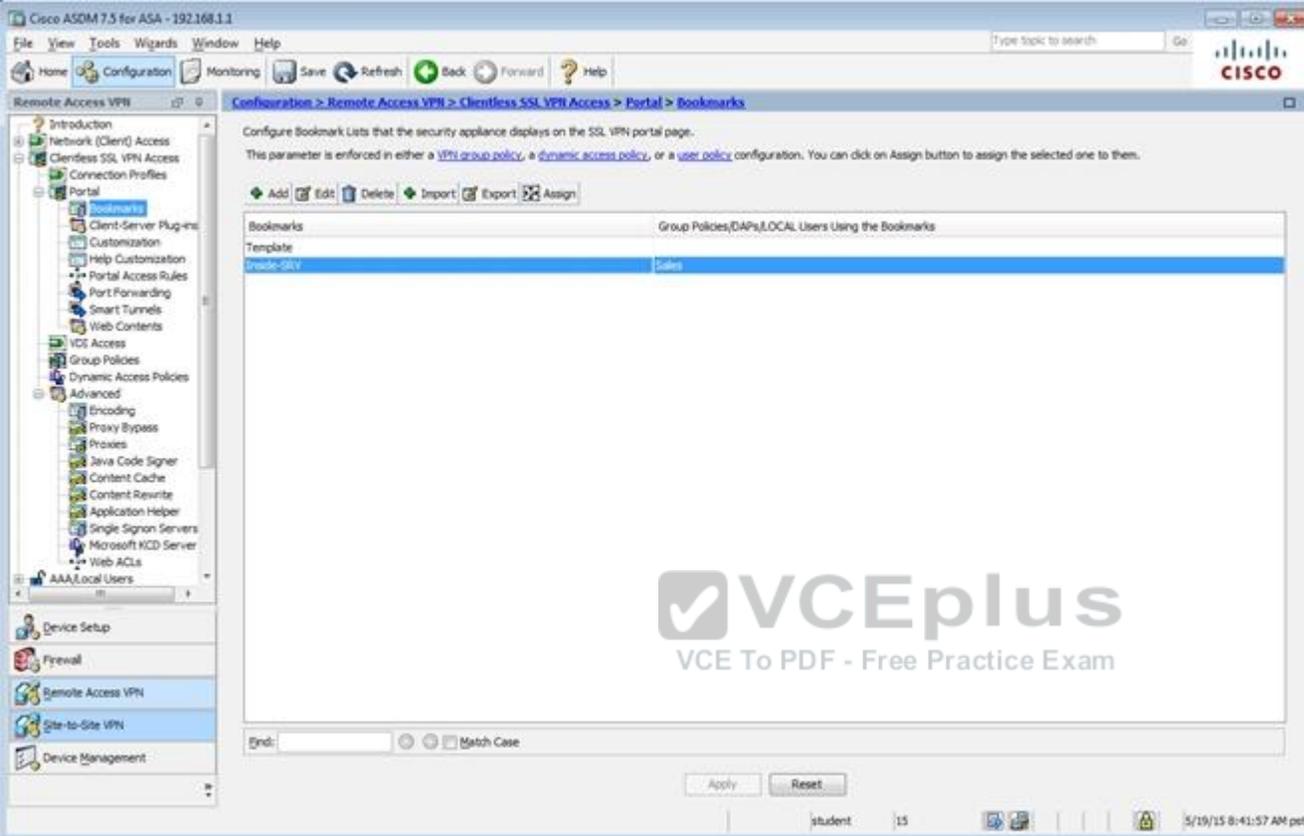












The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration page for Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area contains the following text:

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. You can click on Assign button to assign the selected one to them.

Buttons: Add, Edit, Delete, Import, Export, Assign

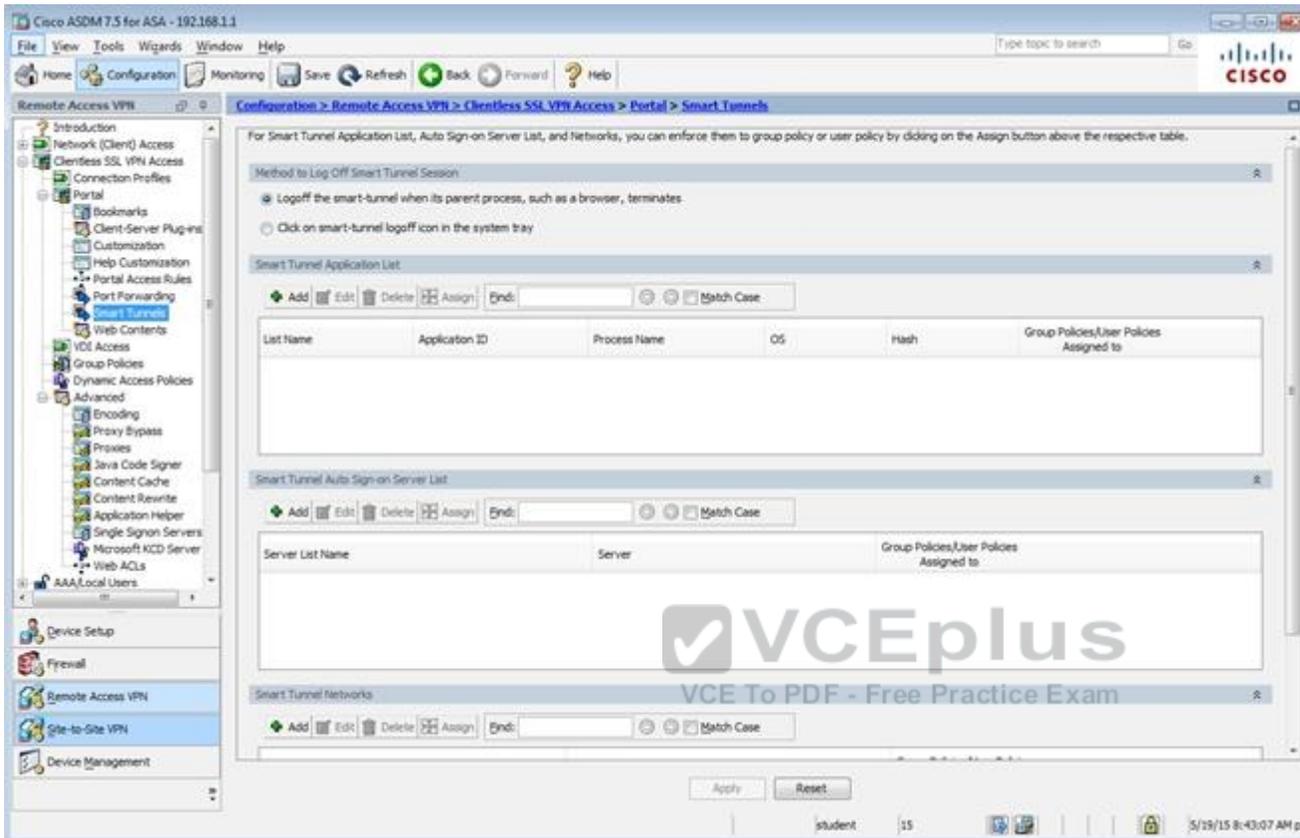
Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Inside-SSLV	Sales

Buttons: Apply, Reset

Footer: student 15 5/19/15 8:41:57 AM pst



VCEplus
VCE To PDF - Free Practice Exam



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 configuration page. The breadcrumb trail is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels. The main content area is titled "Smart Tunnel Configuration" and includes the following sections:

- Method to Log Off Smart Tunnel Session:** Two radio buttons are present: "Logoff the smart-tunnel when its parent process, such as a browser, terminates" (selected) and "Click on smart-tunnel logoff icon in the system tray".
- Smart Tunnel Application List:** A table with columns: List Name, Application ID, Process Name, OS, Hash, and Group Policies/User Policies Assigned to. The table is currently empty.
- Smart Tunnel Auto Sign-on Server List:** A table with columns: Server List Name, Server, and Group Policies/User Policies Assigned to. The table is currently empty.
- Smart Tunnel Networks:** A table with columns: Network Name, Network, and Group Policies/User Policies Assigned to. The table is currently empty.

At the bottom of the configuration area, there are "Apply" and "Reset" buttons. The status bar at the bottom of the window shows "student | 15 | 5/19/15 8:43:07 AM pst".

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding Lists. The main content area contains the following text:

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

Buttons: Add, Edit, Delete, Assign

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description	Group Policies/User Policies Assigned to
-----------	----------------	---------------	-----------------	-------------	--

Buttons: Apply, Reset

Find: Match Case

Footer: student | 15 | 5/19/15 8:43:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

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

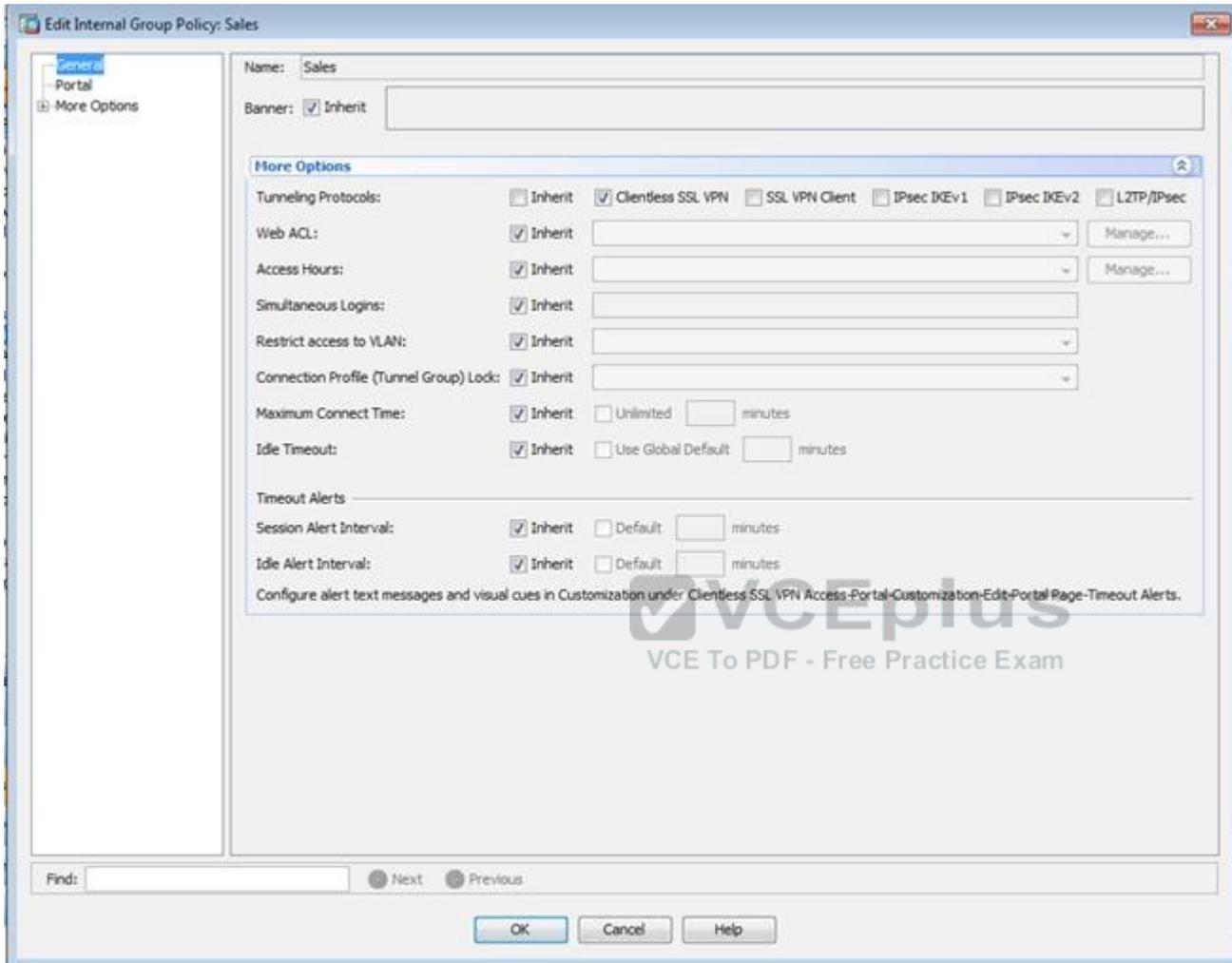
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

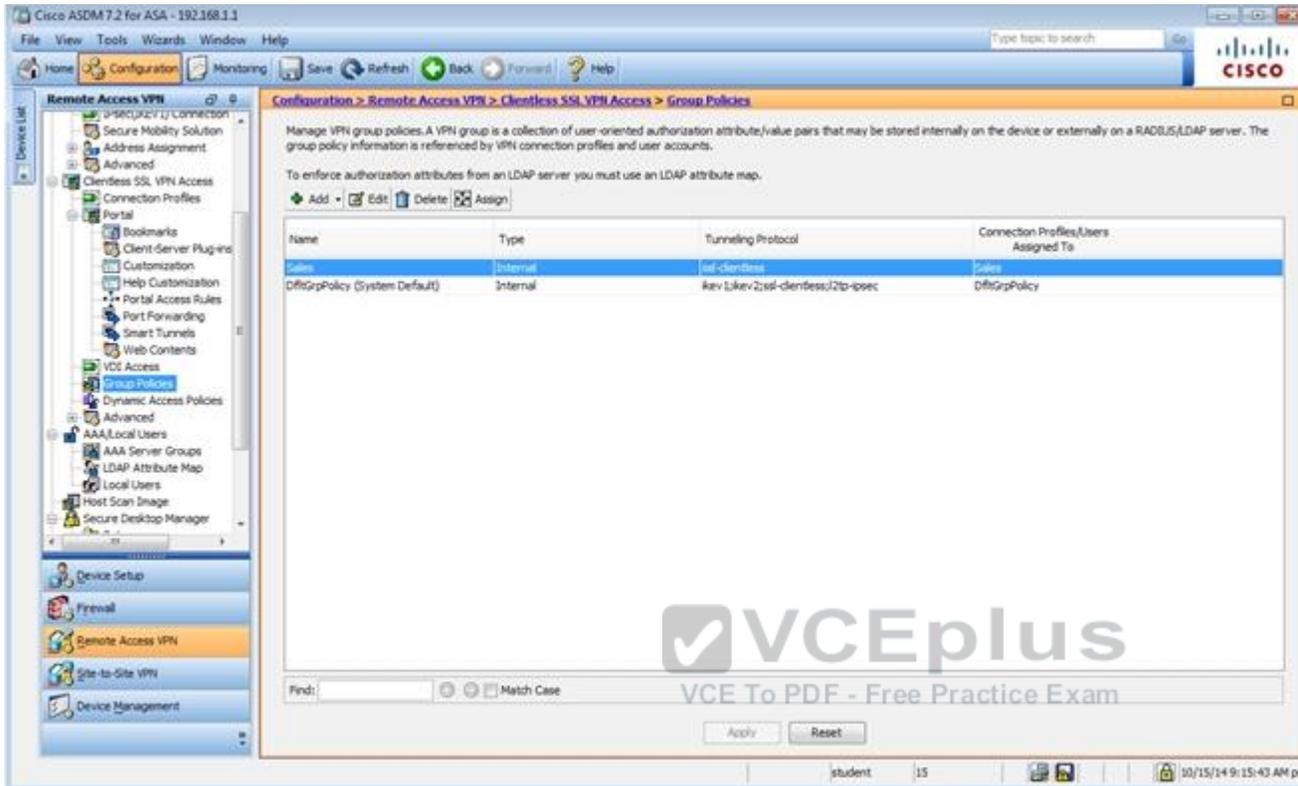
To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Clientless	Internal	ssl-clientless	Clientless
DefaultGroupPolicy (System Default)	Internal	kev1:kev2:ssl-clientless/2to-espsec	DefaultRAGroup;DefaultIL2;Group;DefaultADMDNGroup;Def...

End:

student 15 5/18/15 8:49:27 AM pst





The screenshot shows the Cisco ASDM 7.2 interface for configuration. The breadcrumb trail is Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies. The main content area contains a table of VPN group policies.

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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.

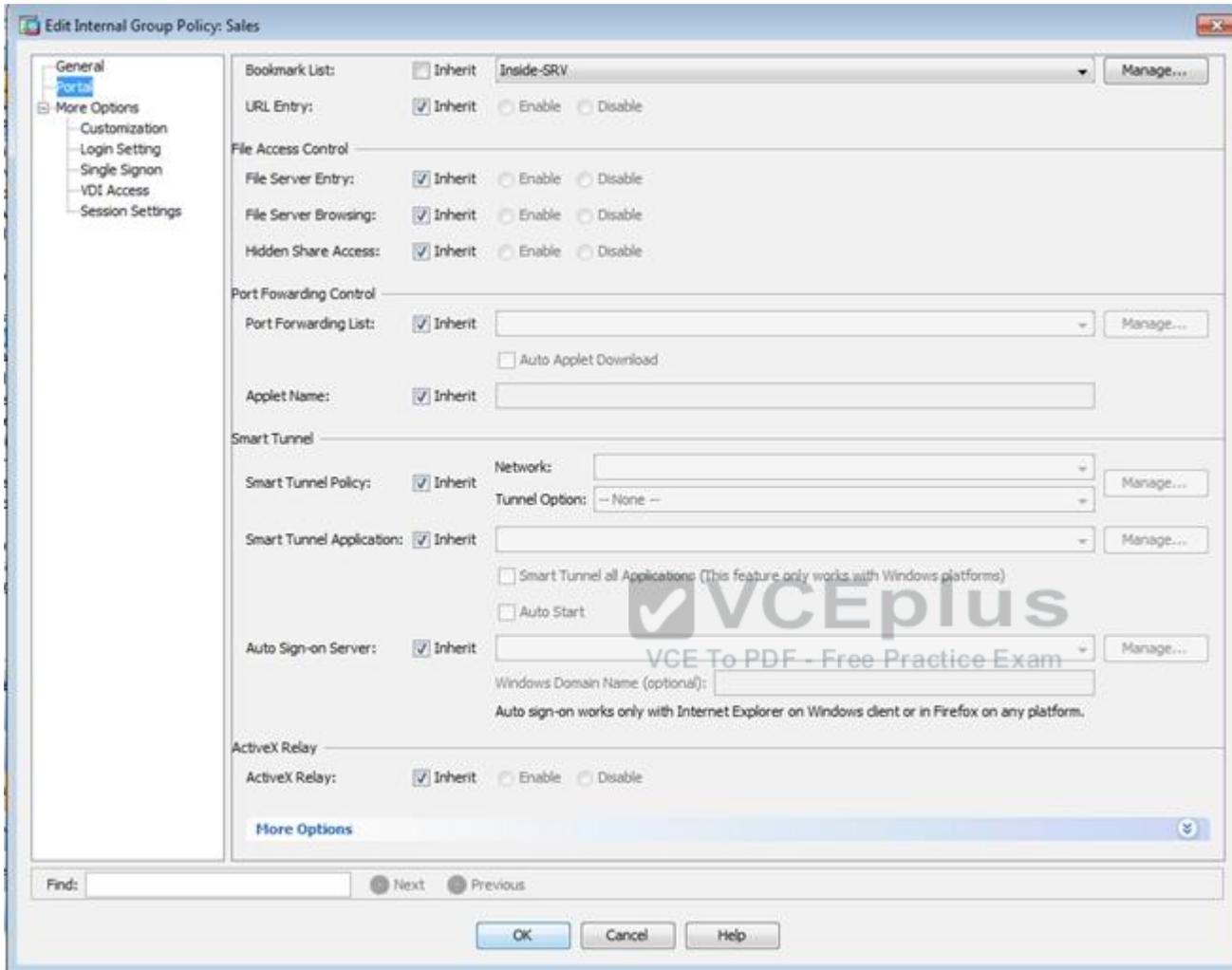
Buttons: Add, Edit, Delete, Assign

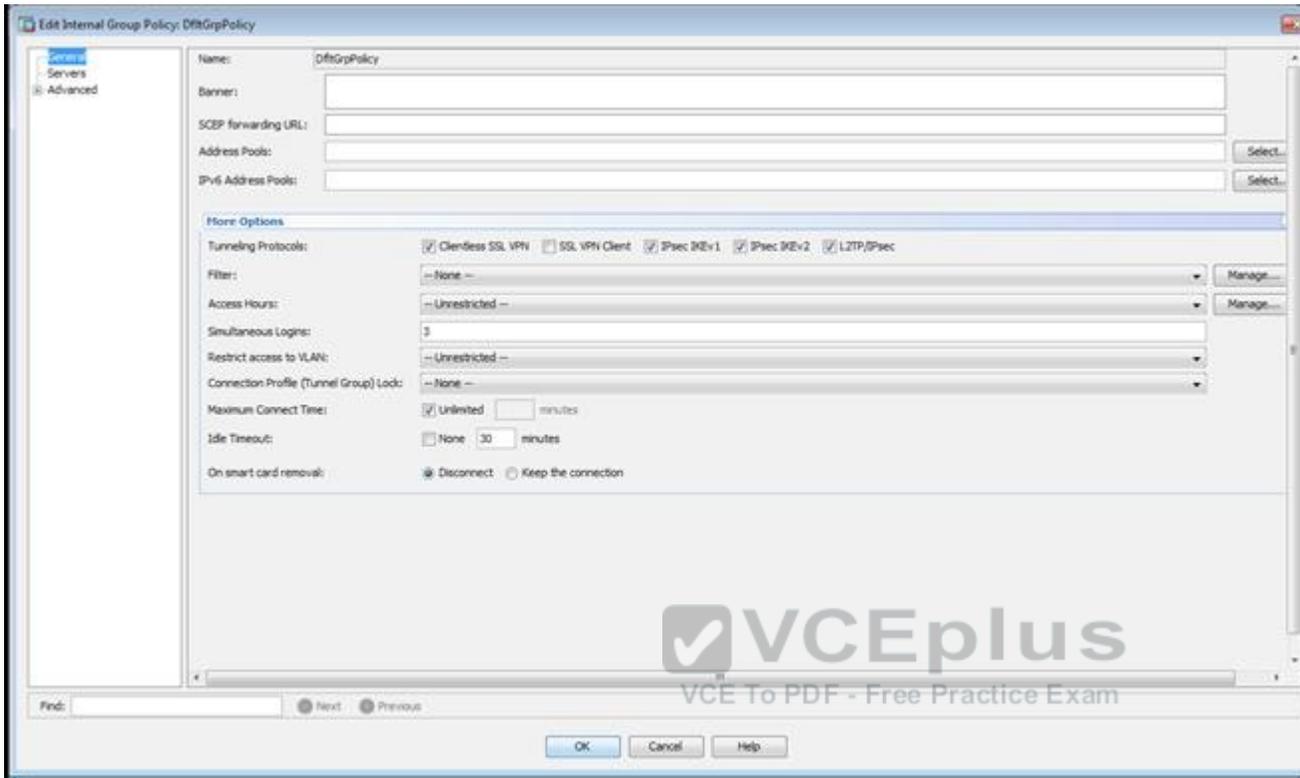
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	Sales
DfltGrpPolicy (System Default)	Internal	kev1/kev2/ssl-clientless/2tp-tpsec	DfltGrpPolicy

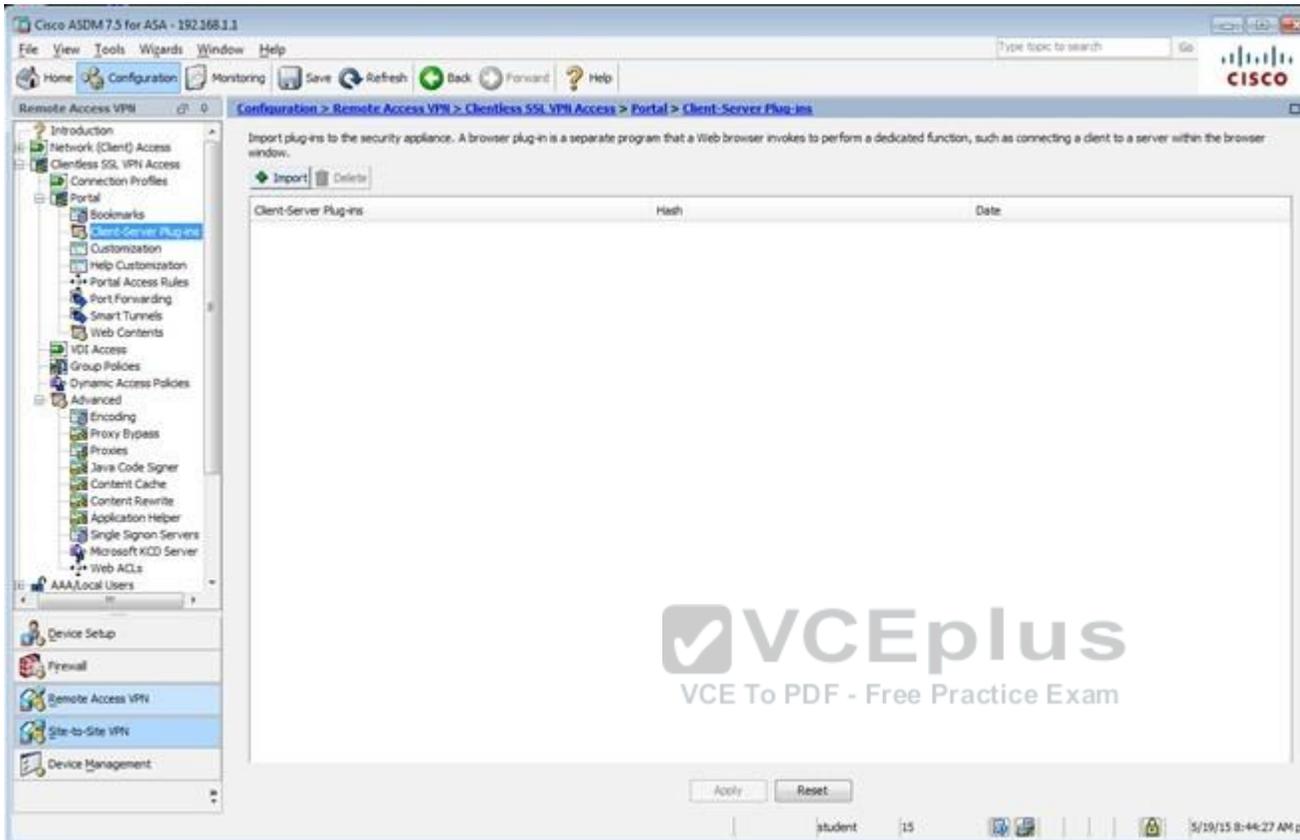
Find: Match Case

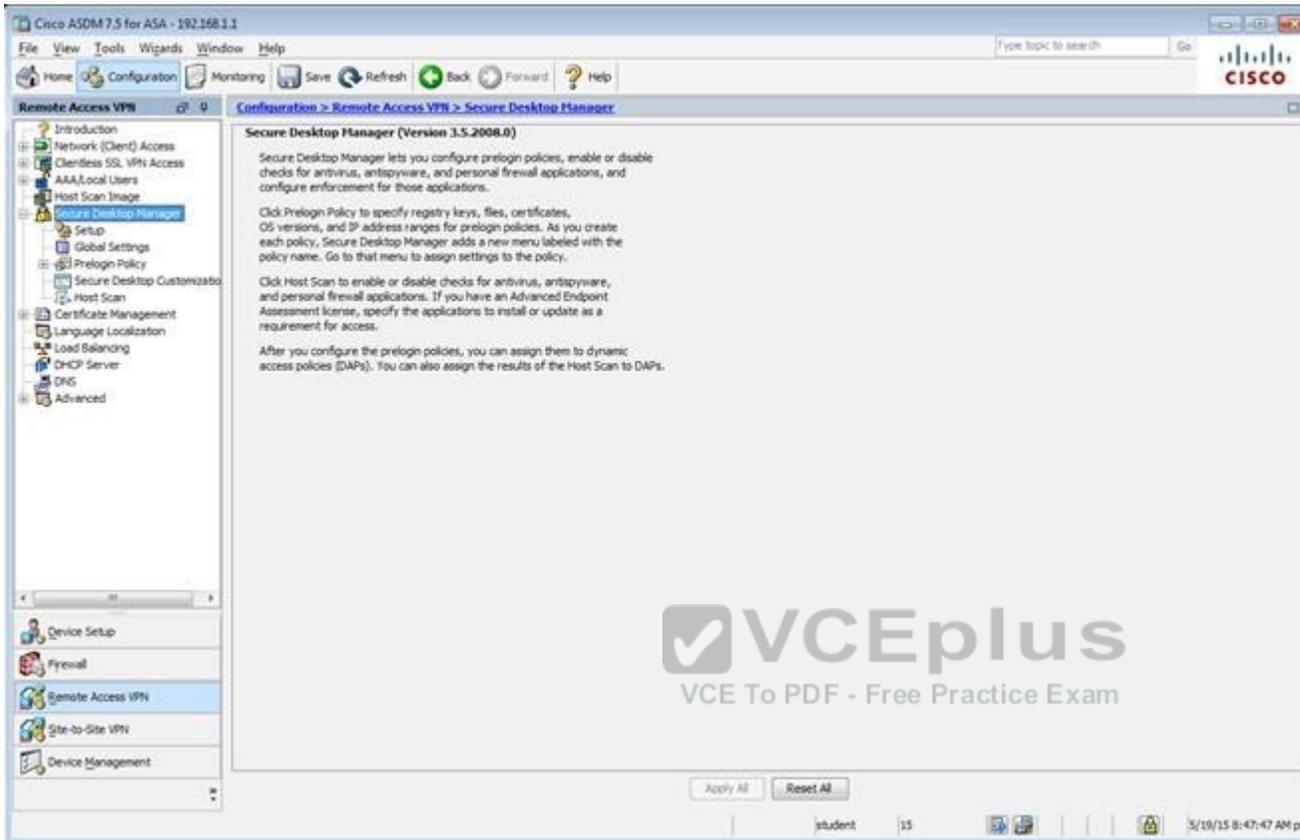
Buttons: Apply, Reset

Taskbar: student | 15 | 10/15/14 9:15:43 AM pst









The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is titled "Secure Desktop Manager (Version 3.5.2008.0)". The left sidebar shows a tree view with "Remote Access VPN" selected, and "Secure Desktop Manager" highlighted under the "Remote Access VPN" section. The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

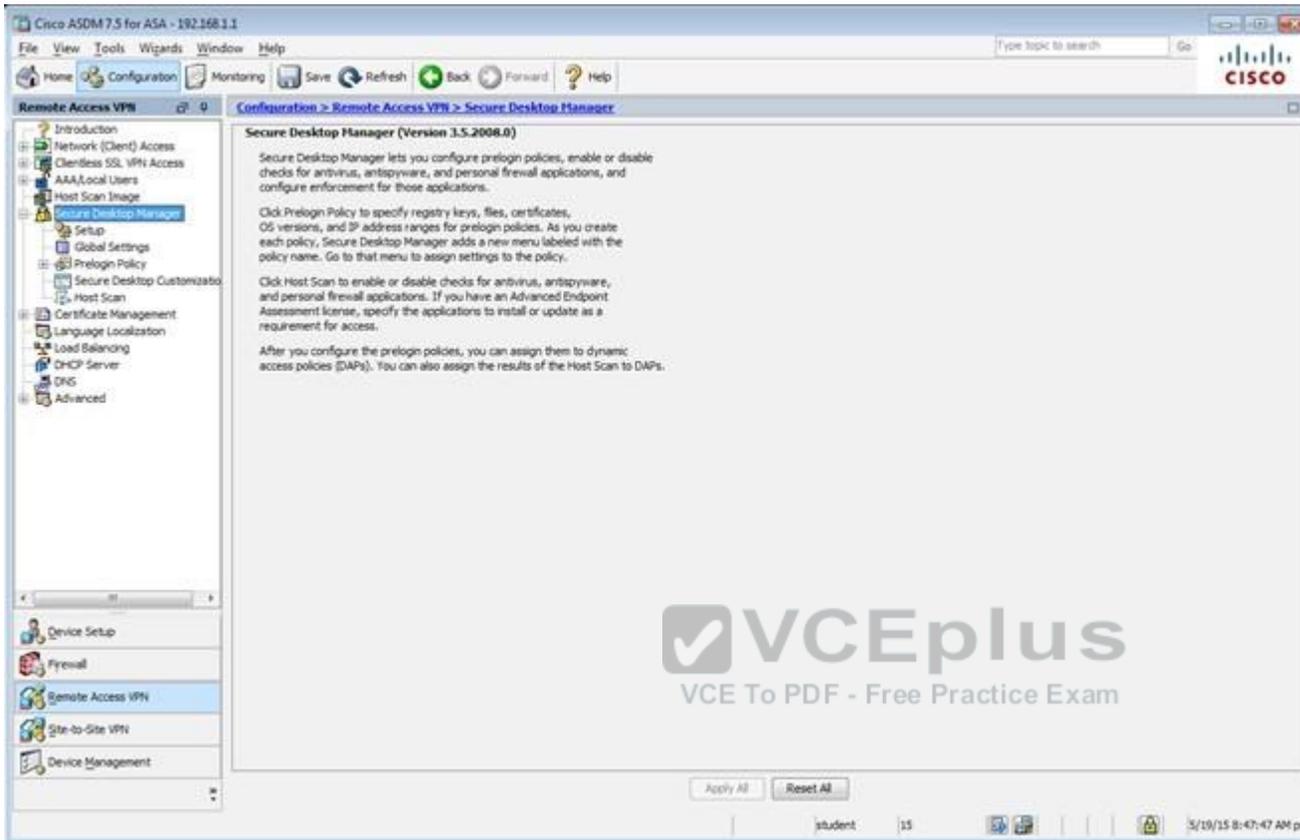
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispware, and personal firewall applications, and configure enforcement for those applications.

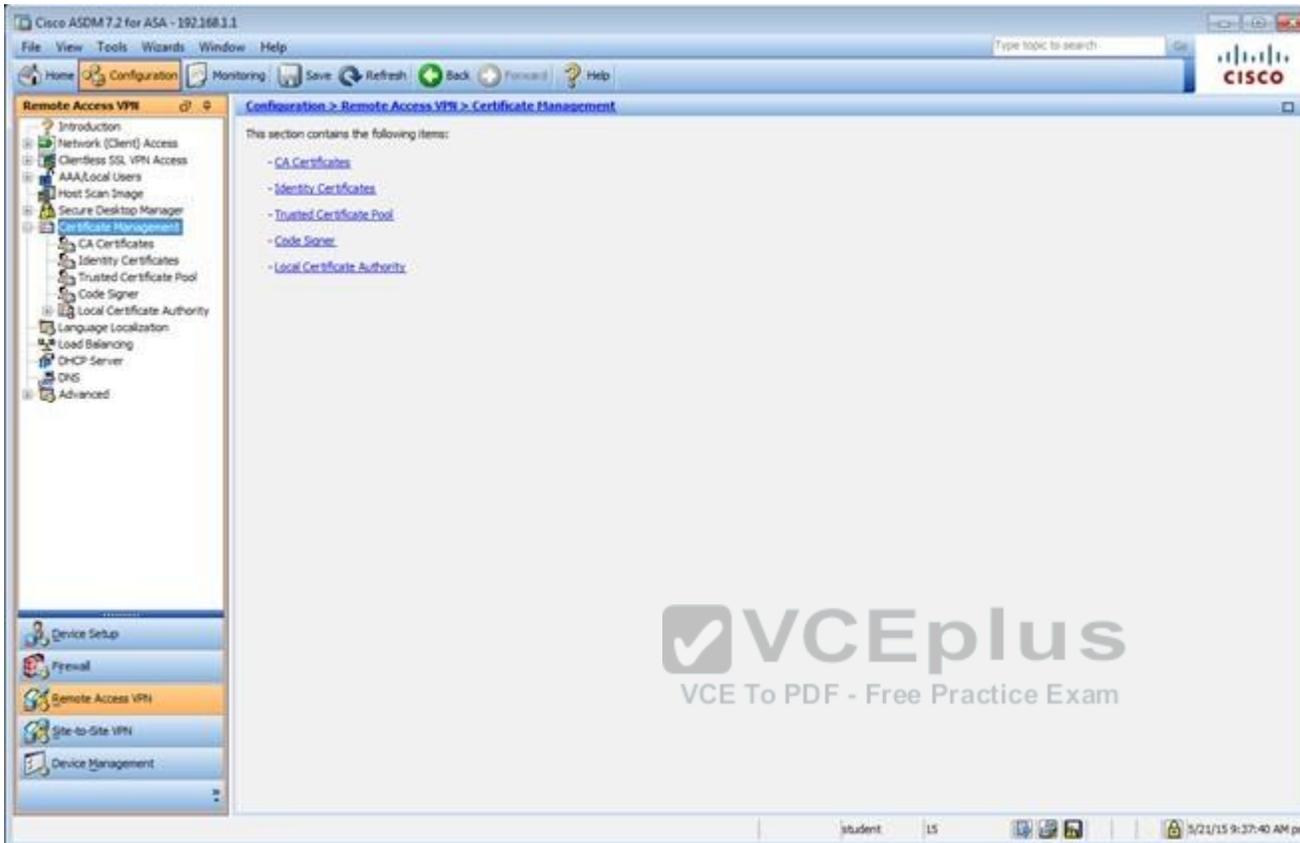
Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispware, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".

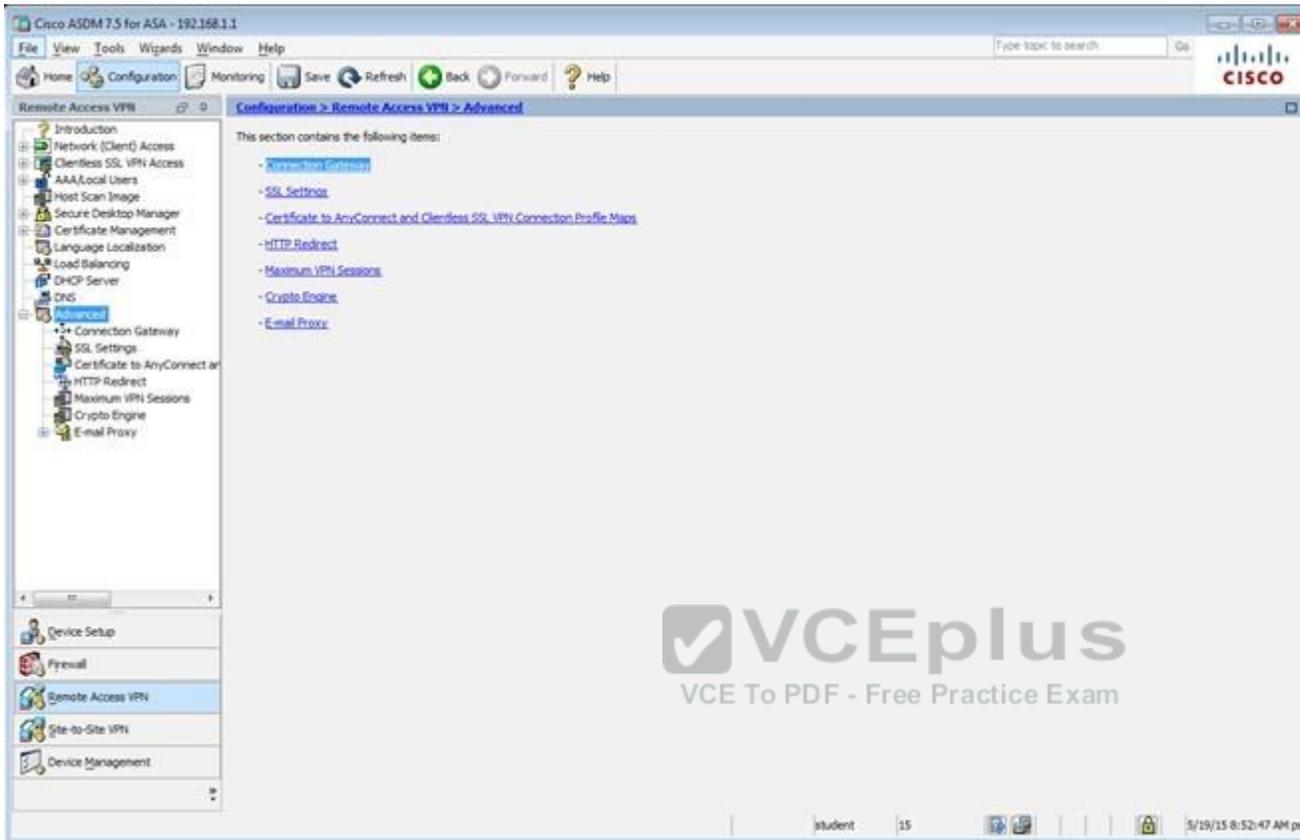




The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Remote Access VPN > Certificate Management > Identity Certificates. The main content area features a table with the following data:

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname-#1 [7-ASA.sec...]	hostname-#1 [7-ASA.sec...]	11:10:33 pet (Dec 20 2024)	ASDM_Trustpoint1	General Purpose	RSA (2048 bits)

Below the table, there are sections for Certificate Expiration Alerts and Public CA Enrollment. The Certificate Expiration Alerts section includes input fields for 'Send the first alert before' (set to 60 days) and 'Repeat Alert Interval' (set to 7 days). The Public CA Enrollment section contains promotional text and a 'Launch ASDM Identity Certificate Wizard' button. A large watermark for 'VCEplus VCE To PDF - Free Practice Exam' is overlaid on the bottom half of the interface.



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Advanced > SSL Settings". The left sidebar shows a tree view with "Remote Access VPN" selected. The main content area contains the following configuration options:

- Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.
- The minimum SSL version for the security appliance to negotiate as a "server": TLS V1
- The minimum SSL version for the security appliance to negotiate as a "client": TLS V1
- Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modAus
- ECDH group to be used with SSL: Group19 - 256-bit EC

The "Encryption" section contains a table with the following data:

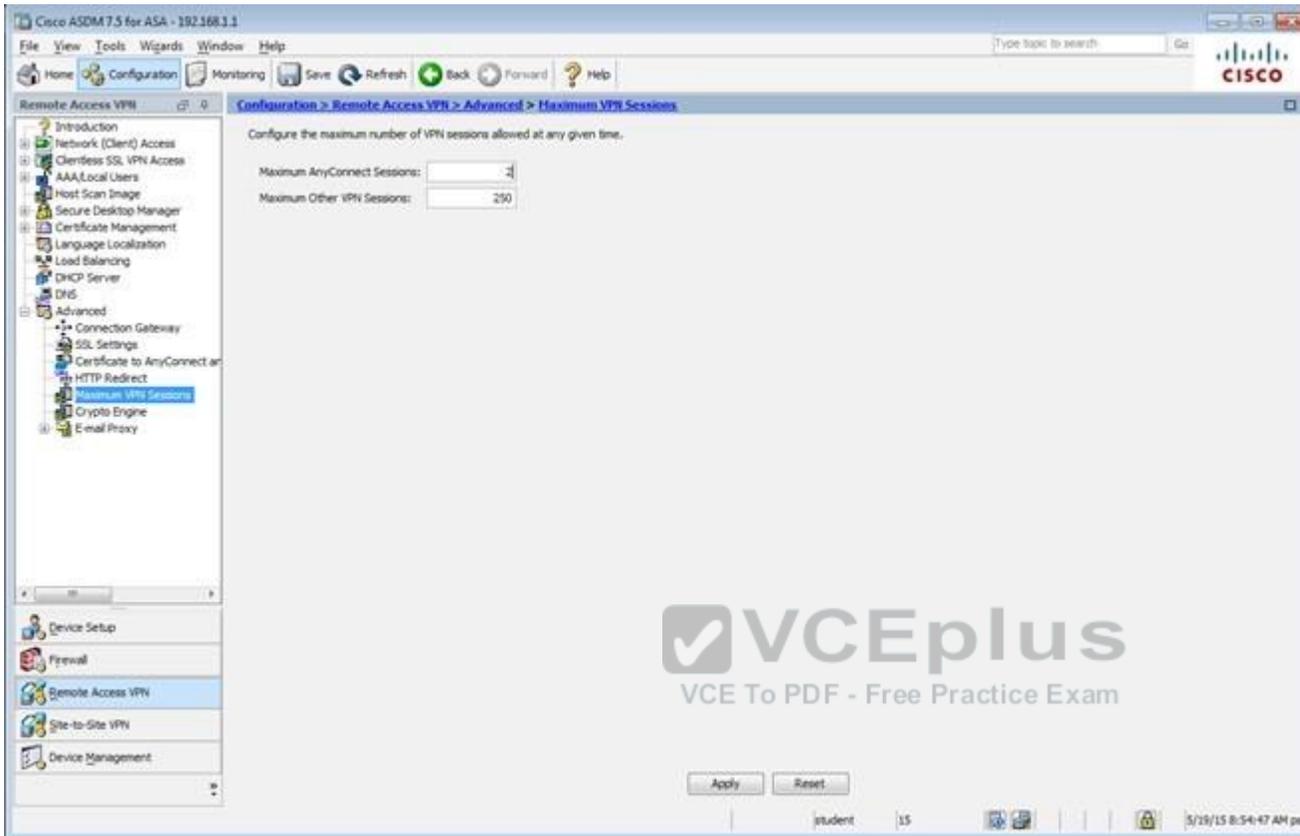
Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
DTLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...

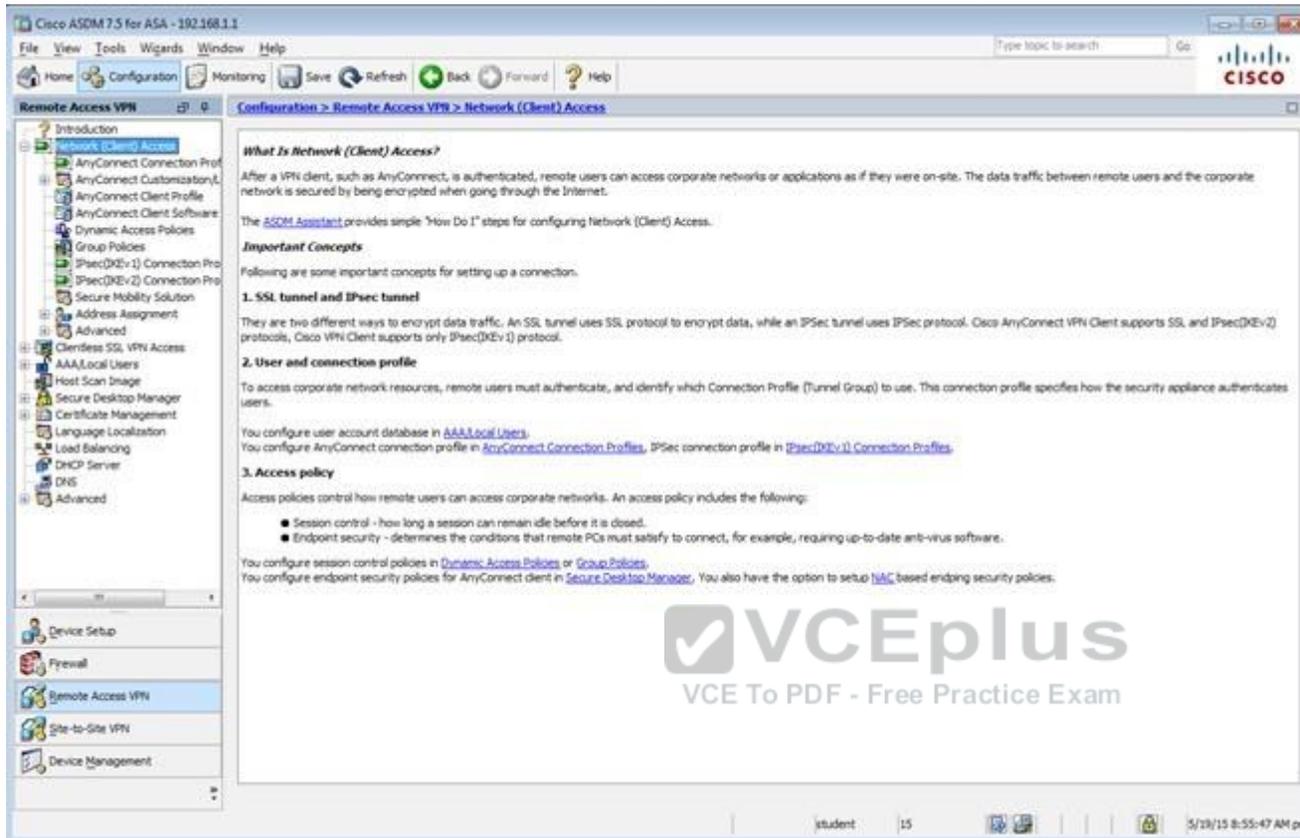
The "Server Name Indication (SNI)" section shows a table with the following data:

Domain	Certificate
dmz	ASDM_TrustPoint1.h...

Buttons for "Add", "Edit", and "Delete" are visible next to the certificate selection. The "Certificates" section at the bottom contains the text: "Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own."

At the bottom of the window, there are "Apply" and "Reset" buttons, and a status bar showing "student 15" and the time "3/19/15 8:54:07 AM pst".





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the configuration page for "Remote Access VPN > Network (Client) Access". The page title is "Configuration > Remote Access VPN > Network (Client) Access".

What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts
Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKv2) protocols. Cisco VPN Client supports only IPsec(DKv1) protocol.

2. User and connection profile
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

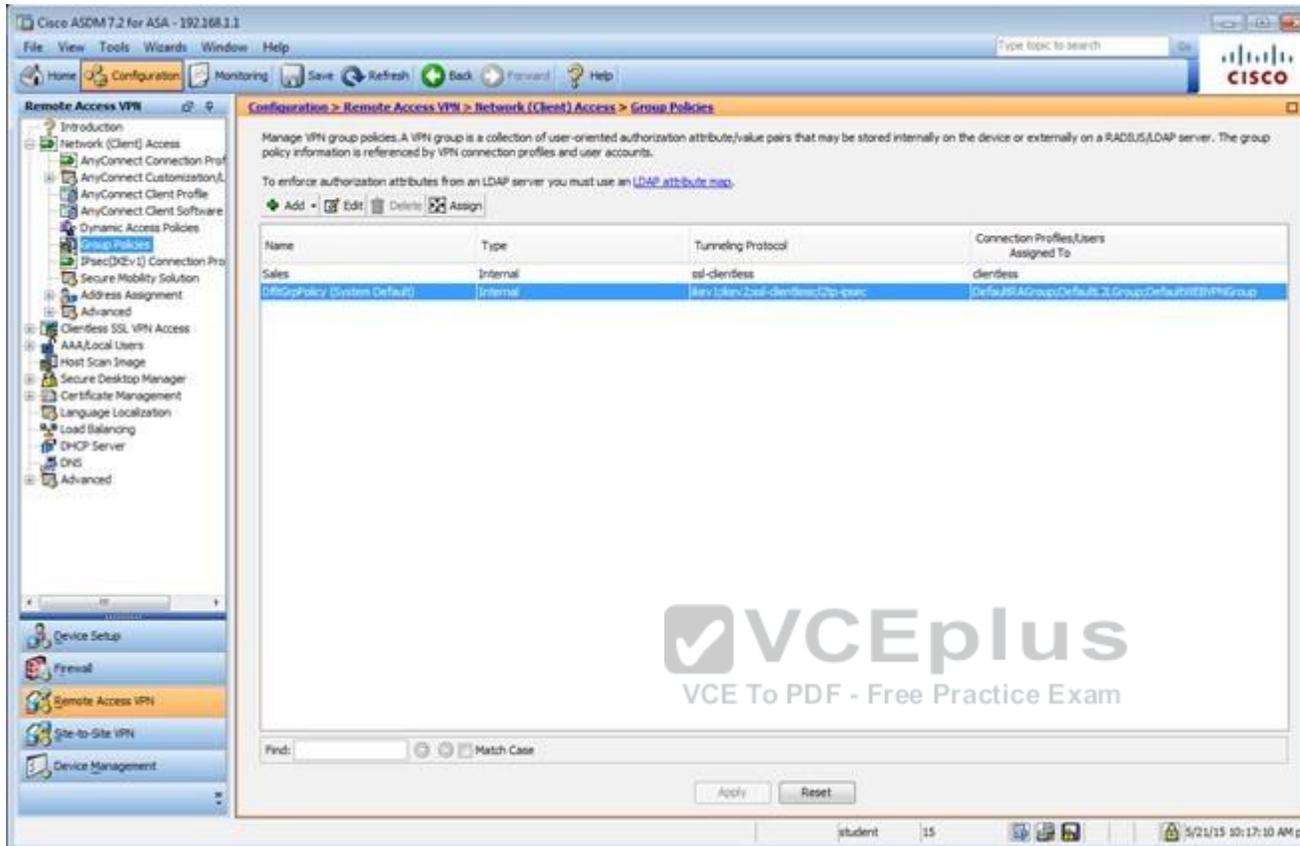
You configure user account database in [AAA Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKv1\) Connection Profiles](#).

3. Access policy
Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HAC](#) based endpoint security policies.

The interface also features a left-hand navigation pane with categories like "Remote Access VPN", "Site-to-Site VPN", and "Device Management". A bottom status bar shows "student | 15 | 5/28/15 8:55:47 AM pet".



Cisco ASDM 7.2 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

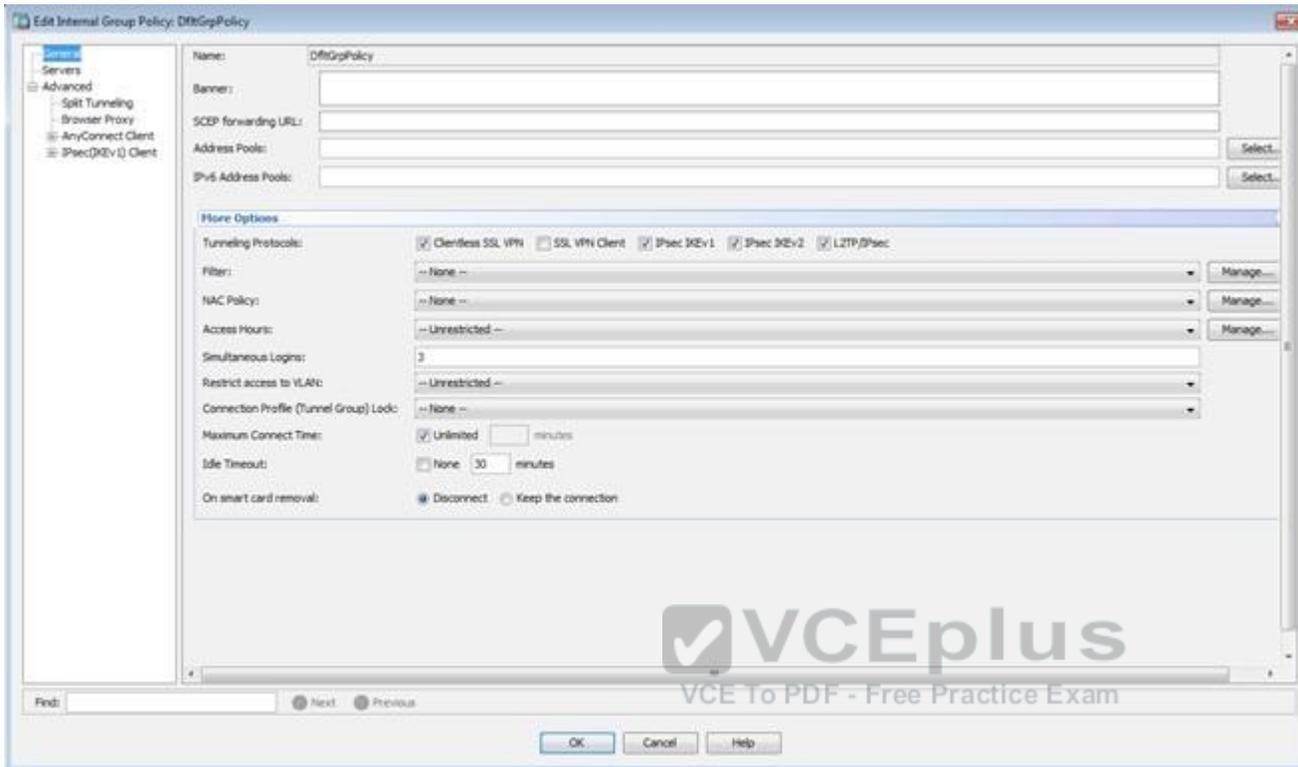
Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DRGpPolicy (System Default)	Internal	[rev:1.0]ssl-clientless/2ip-espac	DefaultAGroup/Default3LGroup/DefaultWEBPhGroup

Find: Match Case

Apply Reset

ytudent 15 3/21/15 10:17:10 AM pet



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window displays the configuration for Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles. The left sidebar shows a tree view with 'Remote Access VPN' selected. The main content area includes an 'Access Interfaces' section with a table to enable interfaces for IPsec access, a 'Connection Profiles' section with a table listing profiles, and an 'End!' field at the bottom.

Access Interfaces

Interface	Allow Access
outside	<input 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.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
DefaultE2EVPNGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
Default	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL	Local

End: Match Case

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:56:47 AM pst

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

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
dmz	<input checked="" 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

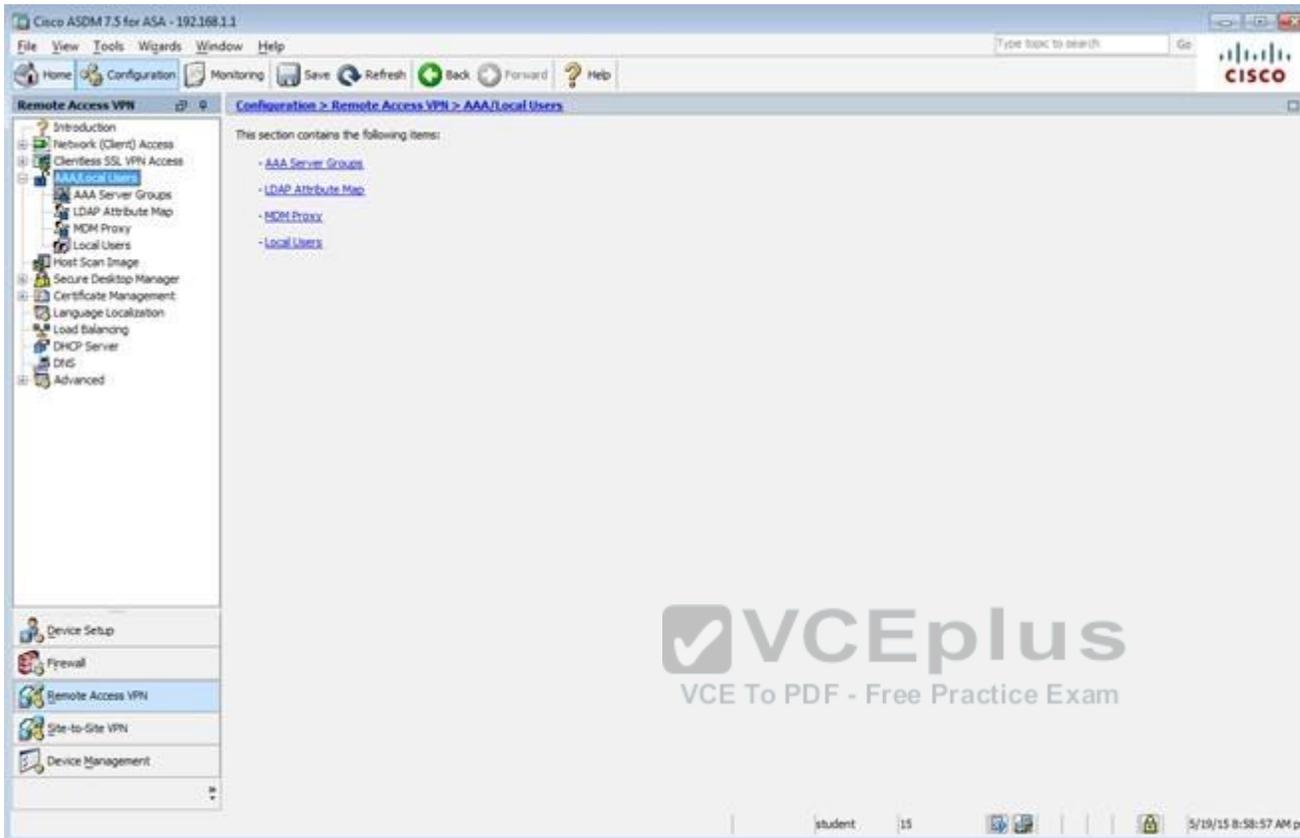
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

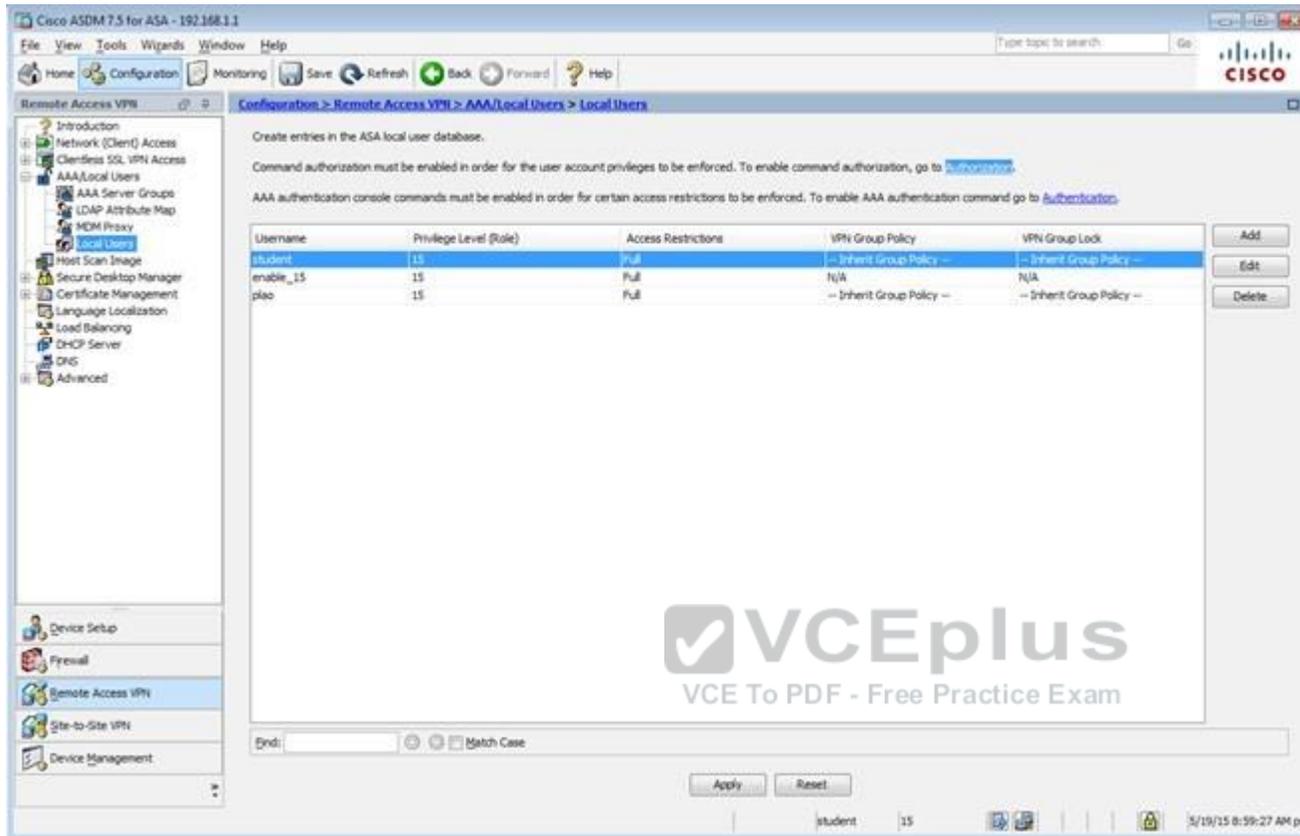
End:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
certless	<input checked="" type="checkbox"/>	<input type="checkbox"/>	yes	SSL(OCSP)	certless

Let group URLs take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

student 15 5/19/15 8:58:17 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

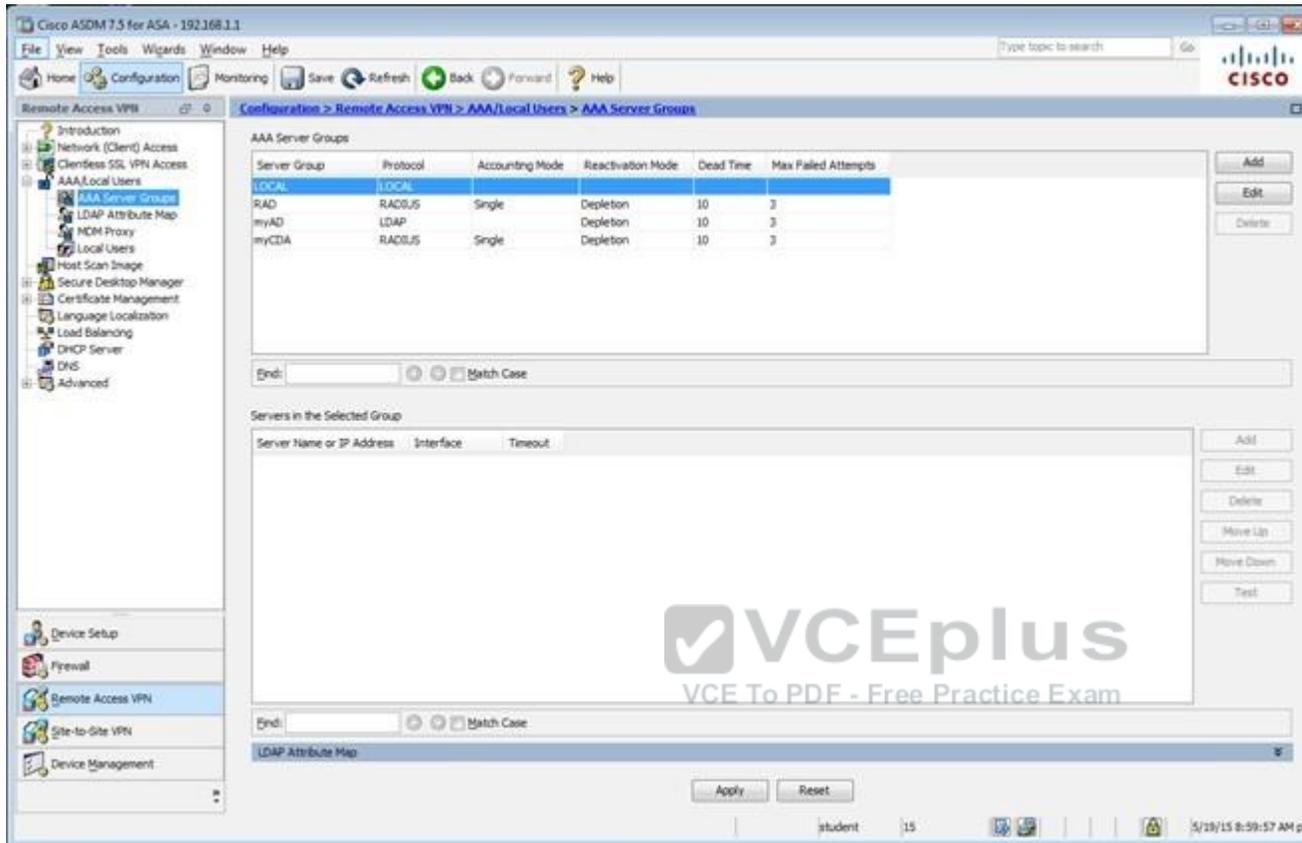
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plac	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End: Match Case

Apply Reset

student 15 5/19/15 8:59:27 AM pet



Which four tunneling 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: (none)

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

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Device Setup

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or 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 Protocol	Connect
Sales	Internal	ssl-clientless	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	Default

VCEplus
VCE To PDF - Free Practice Exam

Scenario Questions TOPOLOGY

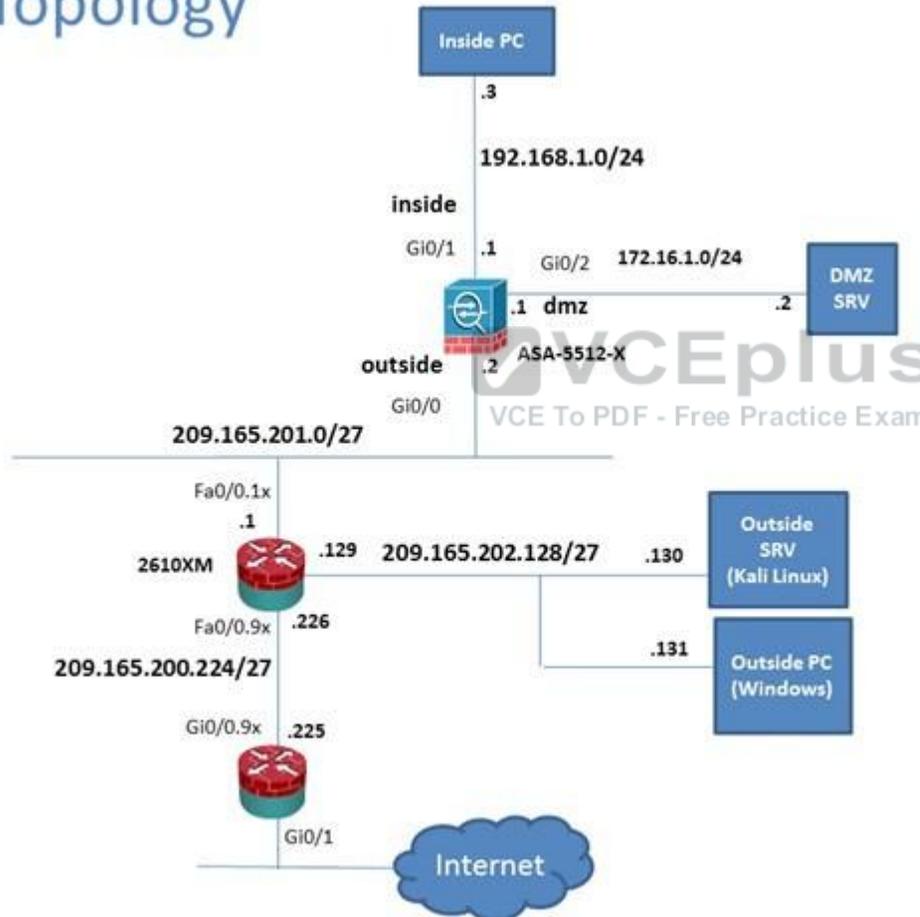
QUESTION 65
Scenario

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 un-expand the expanded menu first.

Lab Topology

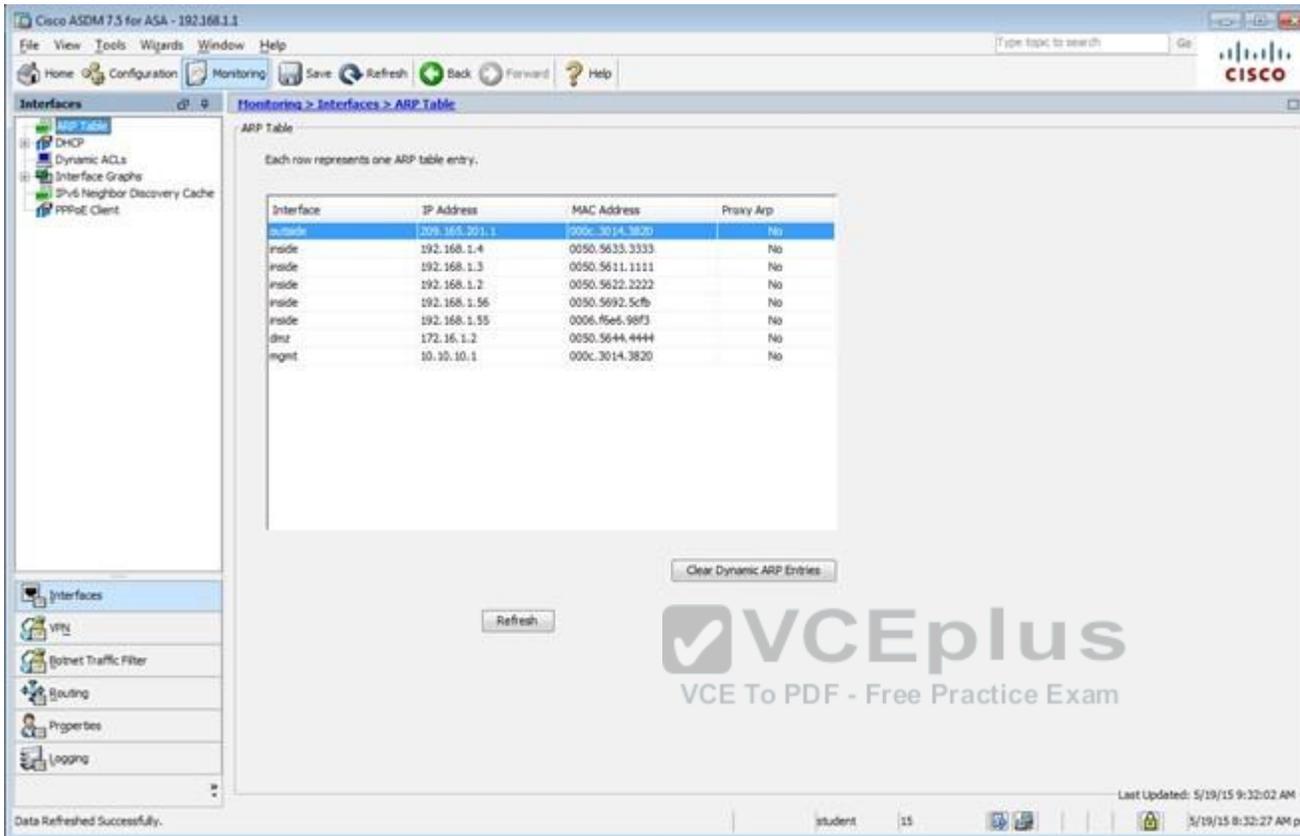


The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is divided into several sections:

- Device Information:**
 - General tab selected.
 - Host Name: P17-ASA,secure-x.local
 - ASA Version: 100.14(6)13
 - ASDM Version: 7.5(1)1
 - Firewall Mode: Routed
 - Environment Status: OK
 - Device Uptime: 11d 21h 42m 47s
 - Device Type: ASA 5512
 - Context Mode: Single
 - Total Flash: 4096 MB
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	up	up	0
inside	192.168.1.1/24	up	up	4
mgmt	10.10.10.2/24	up	up	0
outside	209.165.201.2/24	up	up	0
- VPN Sessions:**
 - IPsec: 0
 - Clientless SSL VPN: 0
 - AnyConnect Client: 0
- System Resources Status:**
 - Total Memory Usage: 500 MB (approx. 50% of 1GB total)
 - Total CPU Usage: 0%
 - Core Usage: 0%
- Traffic Status:**
 - Connections Per Second Usage: 0
 - 'outside' Interface Traffic Usage (Kbps): 0
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina Description
6	May 13 2015	12:35:09	302016	10.81.254.202	123	209.165.201.2	65535: Teardown UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6	May 13 2015	12:35:08	106015	192.168.1.3	14676	192.168.1.1	443: Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6	May 13 2015	12:35:08	302014	192.168.1.3	14676	192.168.1.1	443: Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.3014.3800	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.f5e5.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

Last Updated: 5/19/15 9:32:02 AM

student 15 5/19/15 8:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/ISAK Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- NM Proxy Statistics
- NM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN		1	1	1
Browser		1	1	1

Filter By: Clientless SSL VPN -- All Sessions -- Filter

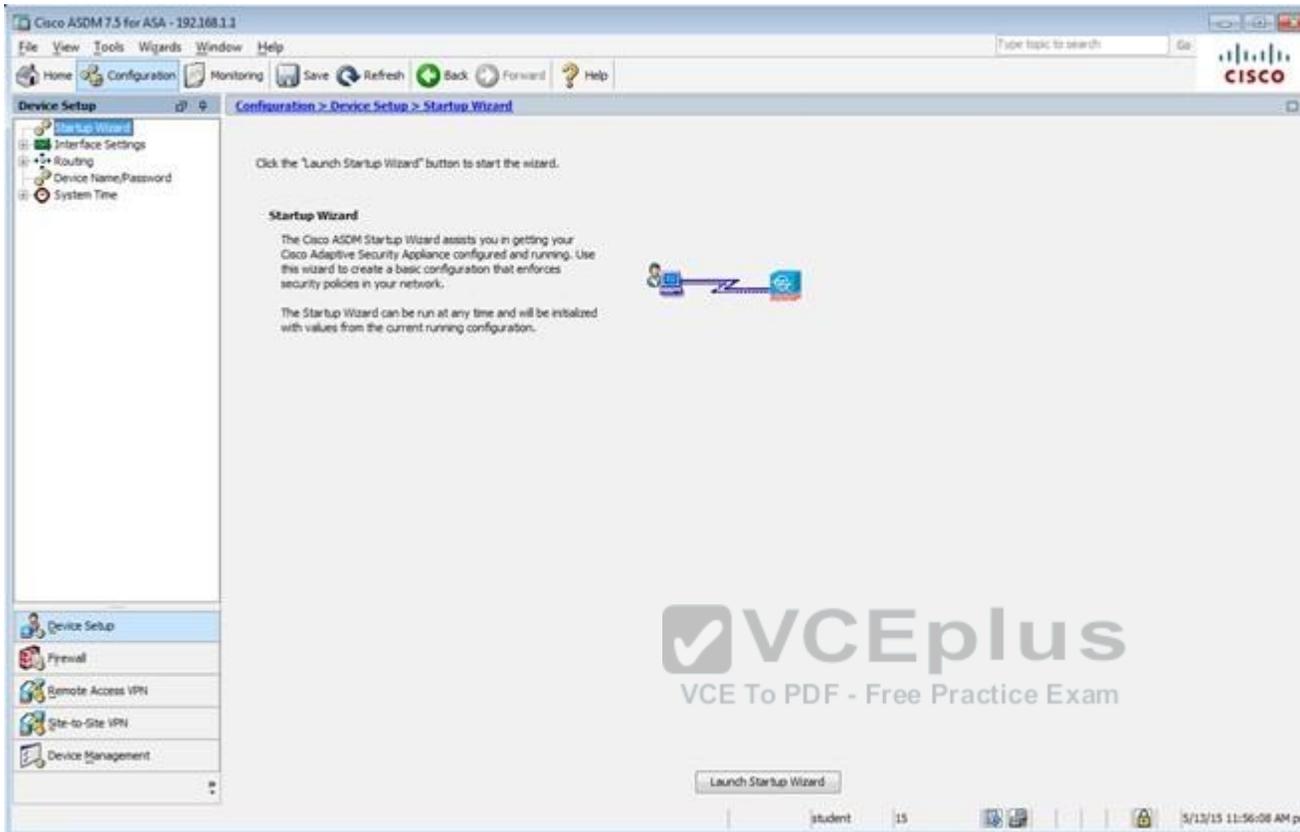
Username	IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
student	209.165.202.131	Sales	Clientless	08:03:46 pm Thu May 21 2015	316774 41833

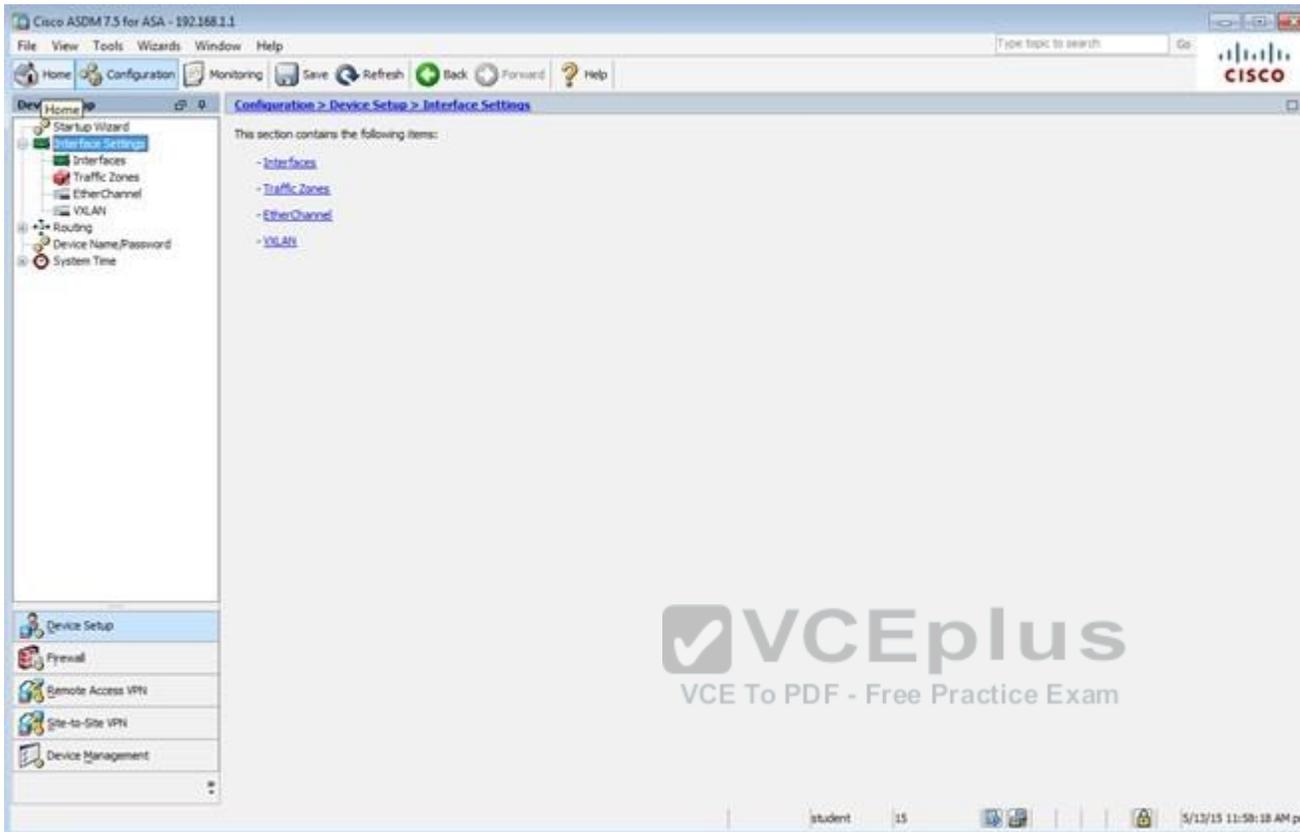
Refresh

Last Updated: 5/19/15 9:33:12 AM

Data Refreshed Successfully. | student | 15 | 5/19/15 8:33:37 AM pst







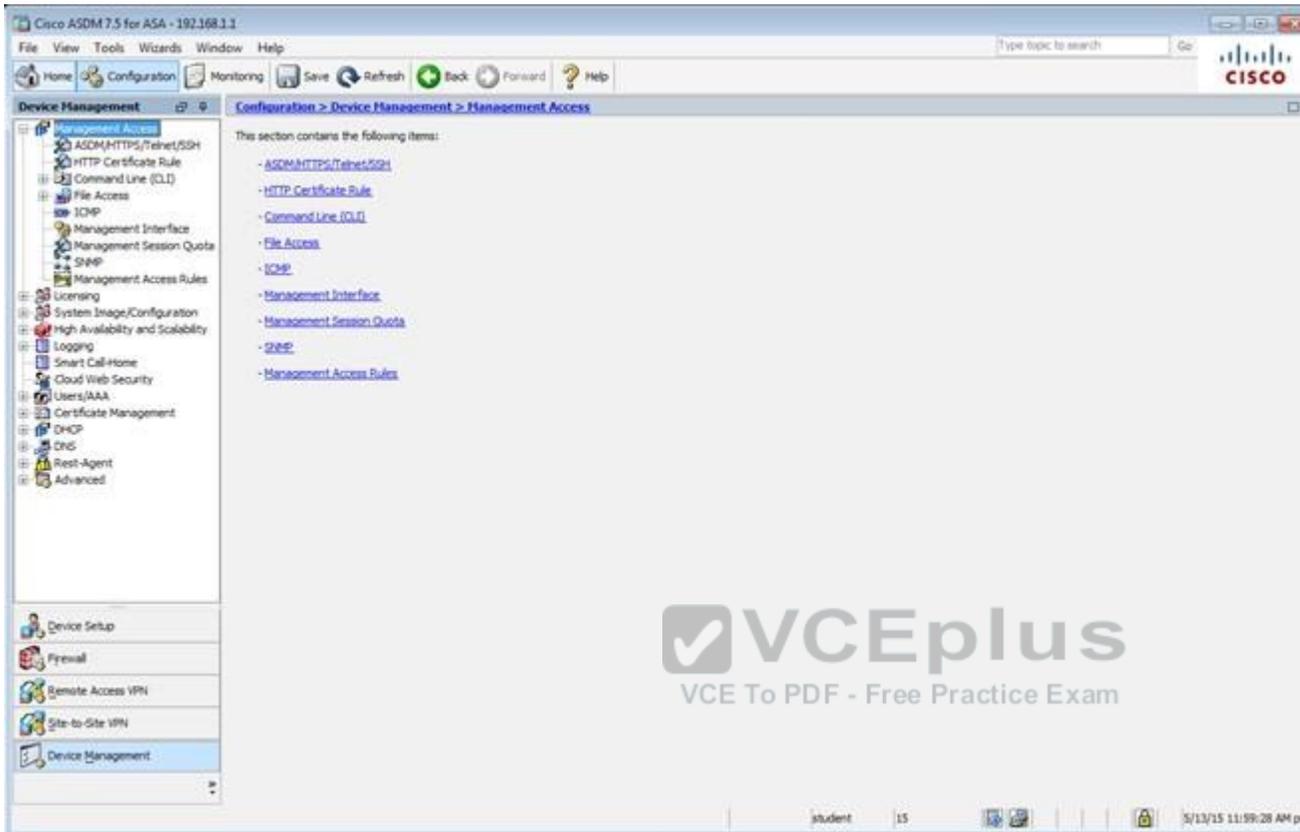
The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for the 'Interfaces' section. A table lists the configured interfaces with their respective settings.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled	0	209.165.201.2	255.255.255.0		Hardware
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1	255.255.255.0		Hardware
GigabitEthernet0/2	dmz			Enabled	172	16.1.1	255.255.255.0		Hardware
GigabitEthernet0/3				Enabled					Hardware
GigabitEthernet0/4				Enabled					Hardware
GigabitEthernet0/5	mgmt			Enabled	100	10.10.10.2	255.255.255.0		Hardware
Management0/0				Enabled					Hardware

Below the table, there are three checkboxes for advanced settings:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface
- Enable jumbo frame reservation

The interface also includes 'Apply' and 'Reset' buttons at the bottom.



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows a tree view with 'Management Access' selected. The main pane is titled 'Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH'. It contains a table for specifying host/network addresses and various settings for HTTP, Telnet, and SSH.

Type	Interface	IP Address	Mask/Prefix Length
Telnet	mgmt	10.10.10.1	255.255.255.255
SSH	inside	192.168.1.2	255.255.255.255
ASDM/HTTPS	inside	192.168.1.0	255.255.255.0

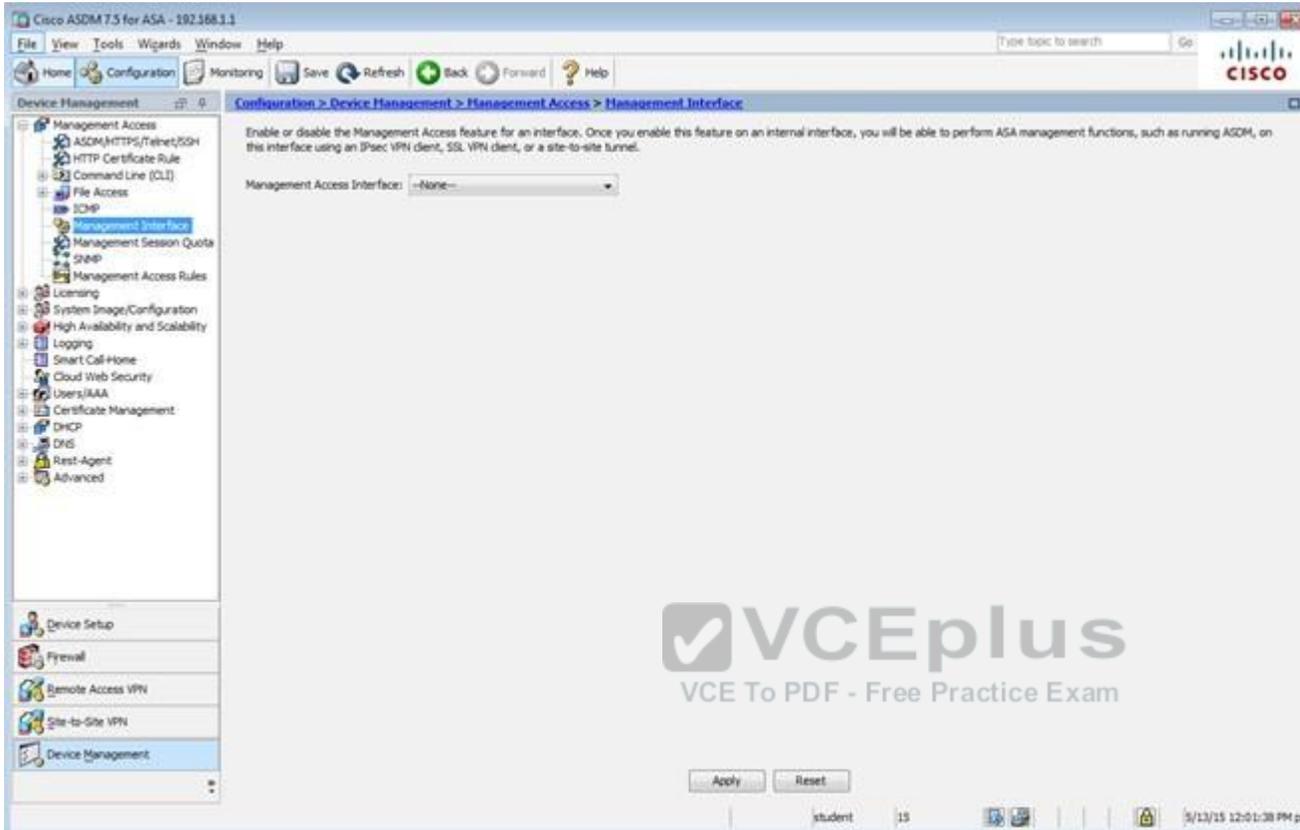
HTTP Settings
 Enable HTTP Server
Port Number: 443
Idle Timeout: 20 minutes
 Session Timeout: minutes
Require client certificate to access ASDM on the following interfaces
Interfaces: [Dropdown]

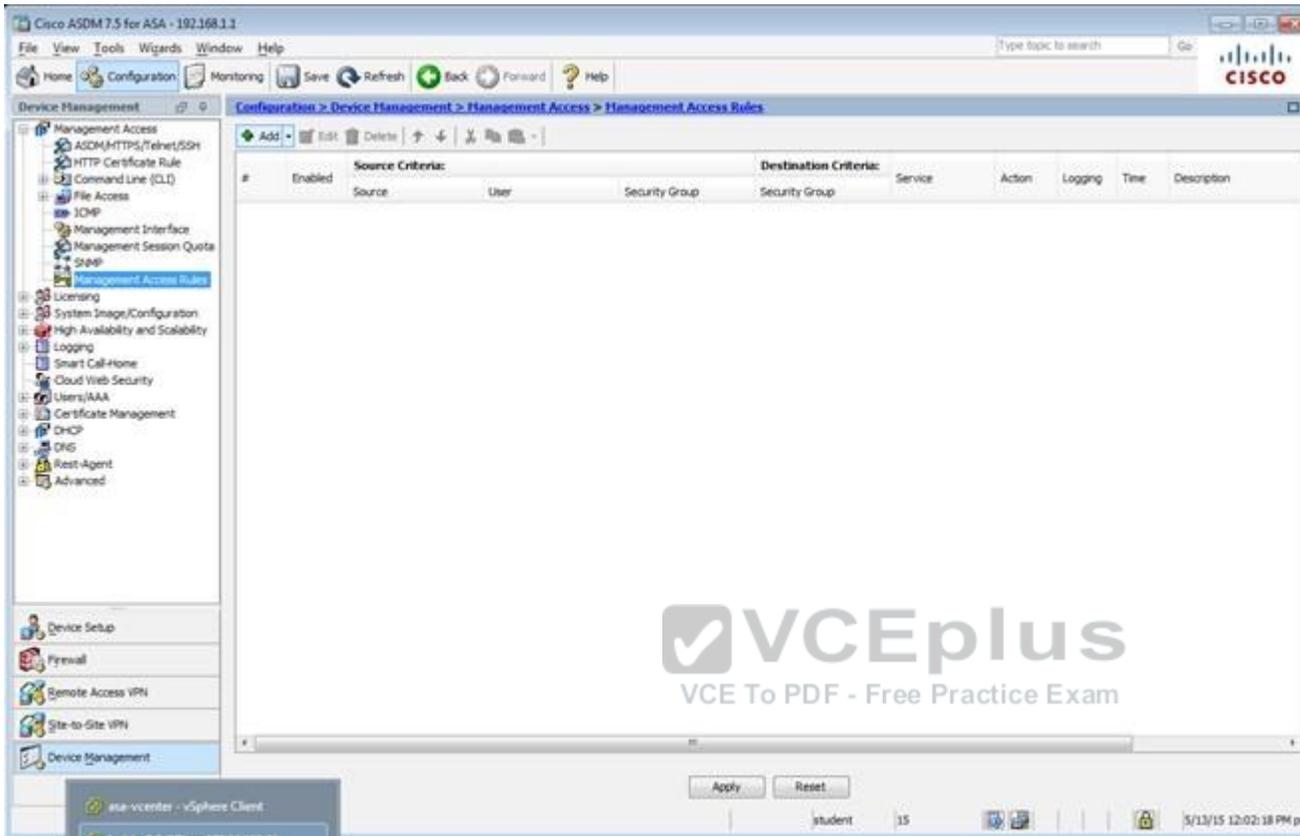
Telnet Settings
Telnet Timeout: 5 minutes

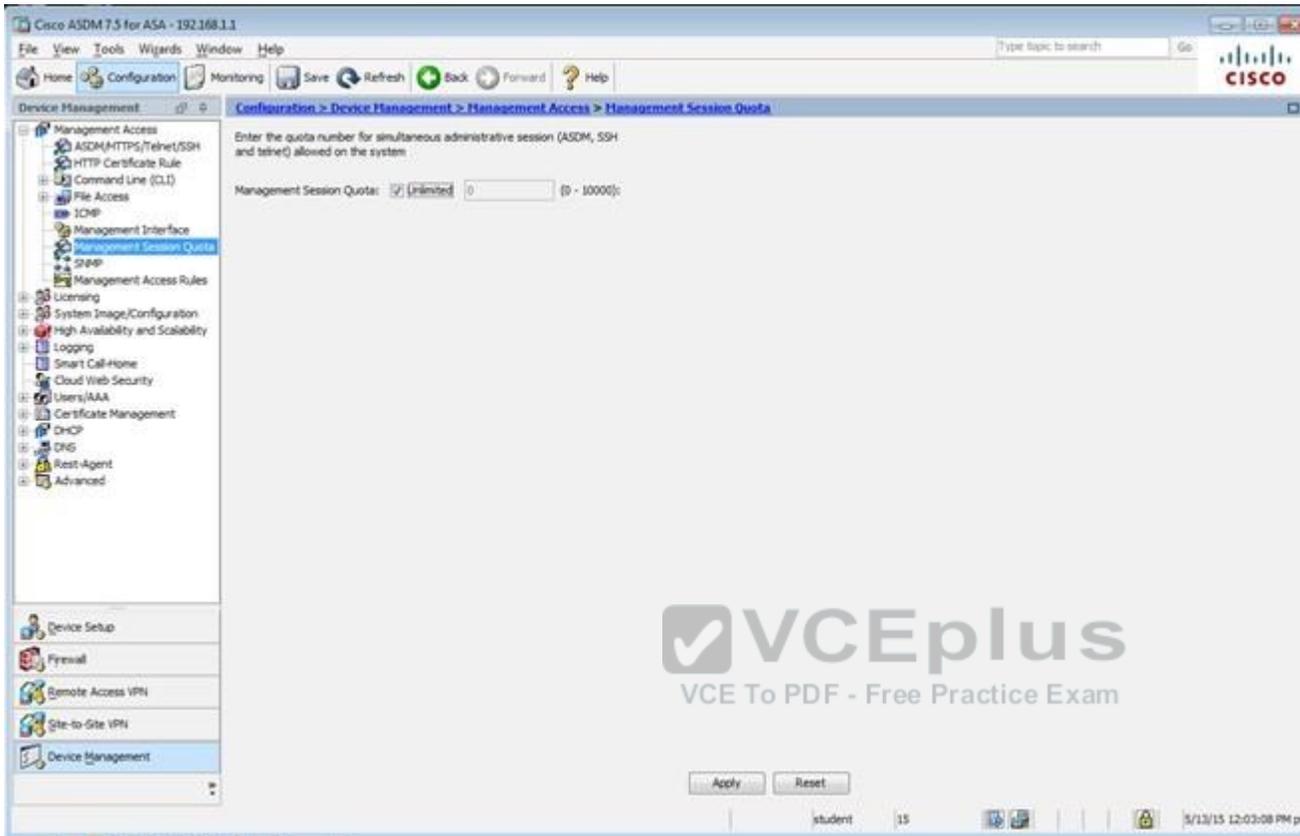
SSH Settings
Allowed SSH Version(s): 1 & 2
SSH Timeout: 5 minutes
DH Key Exchange: Group 1 Group 14

Buttons: Add, Edit, Delete, Apply, Reset

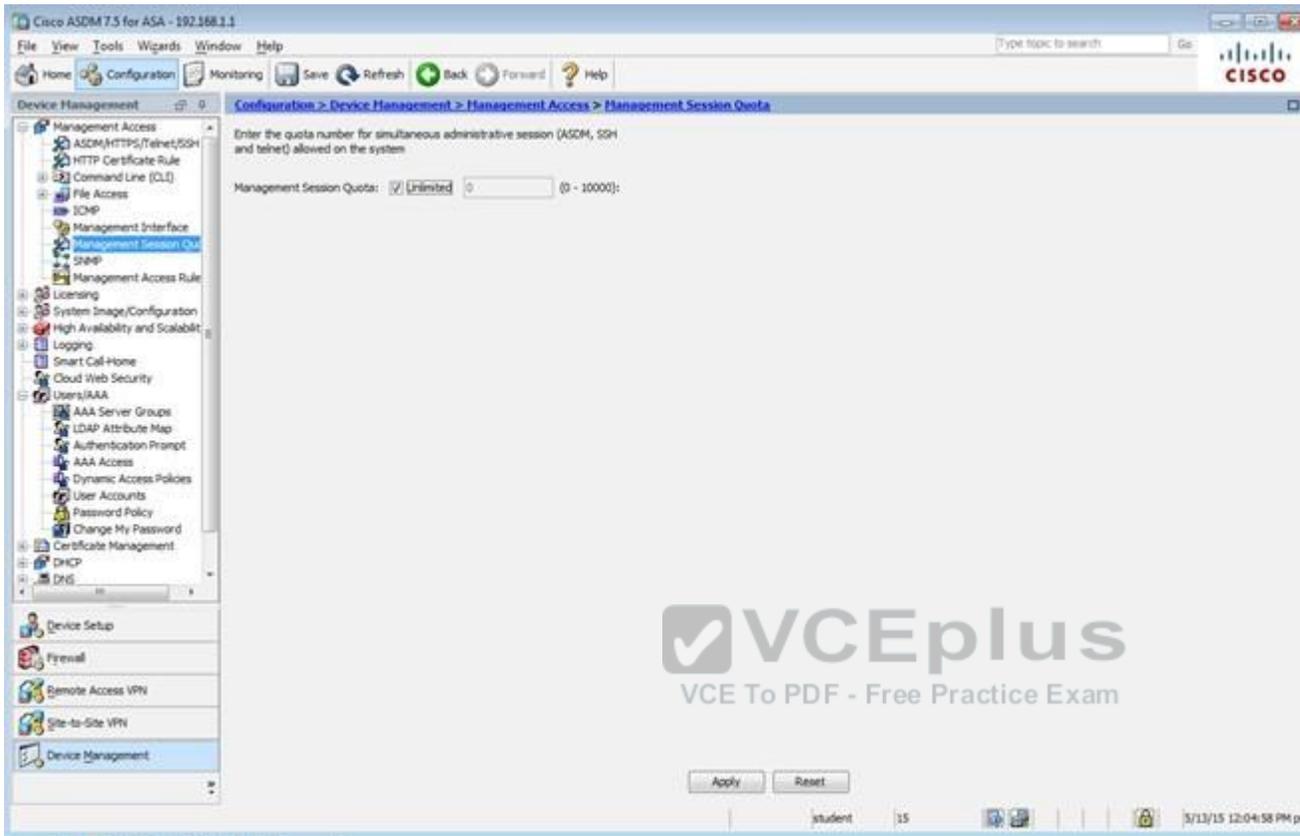


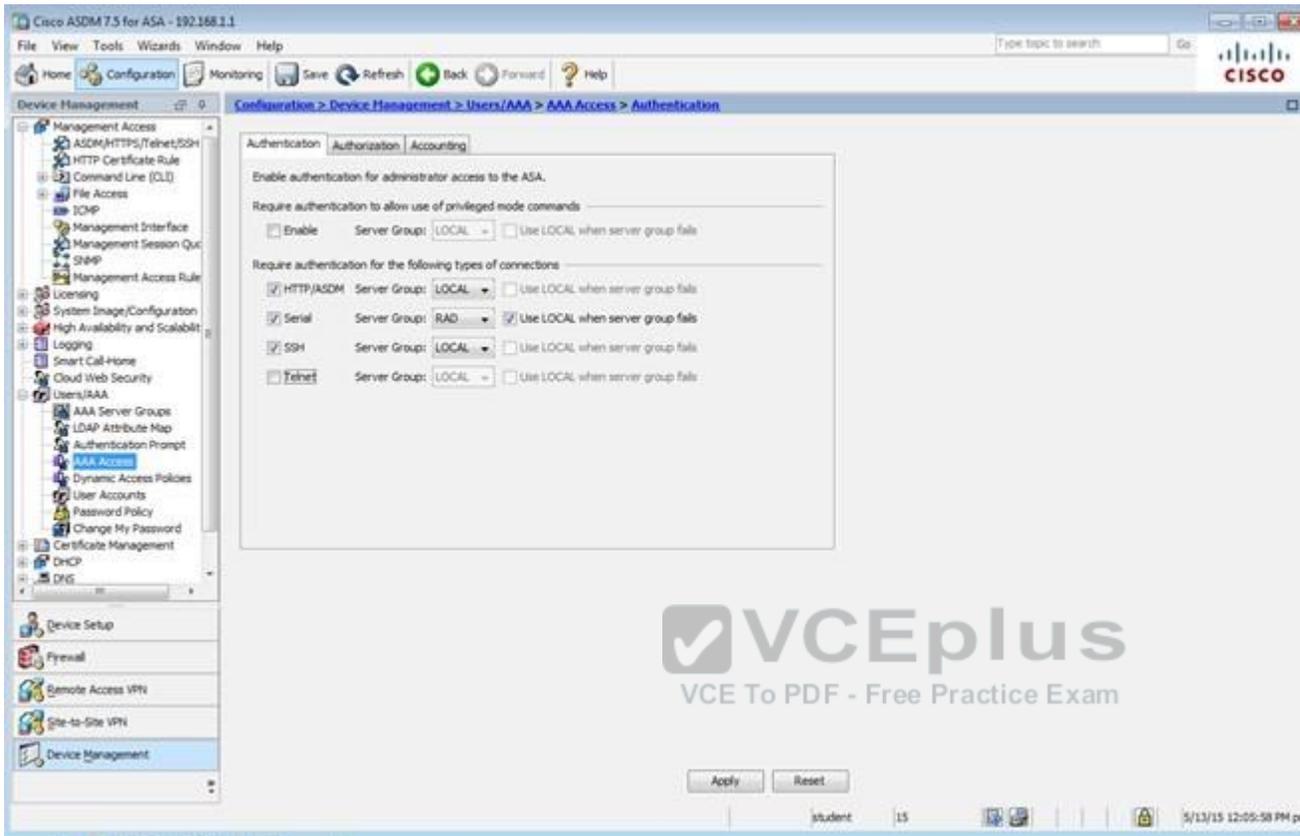


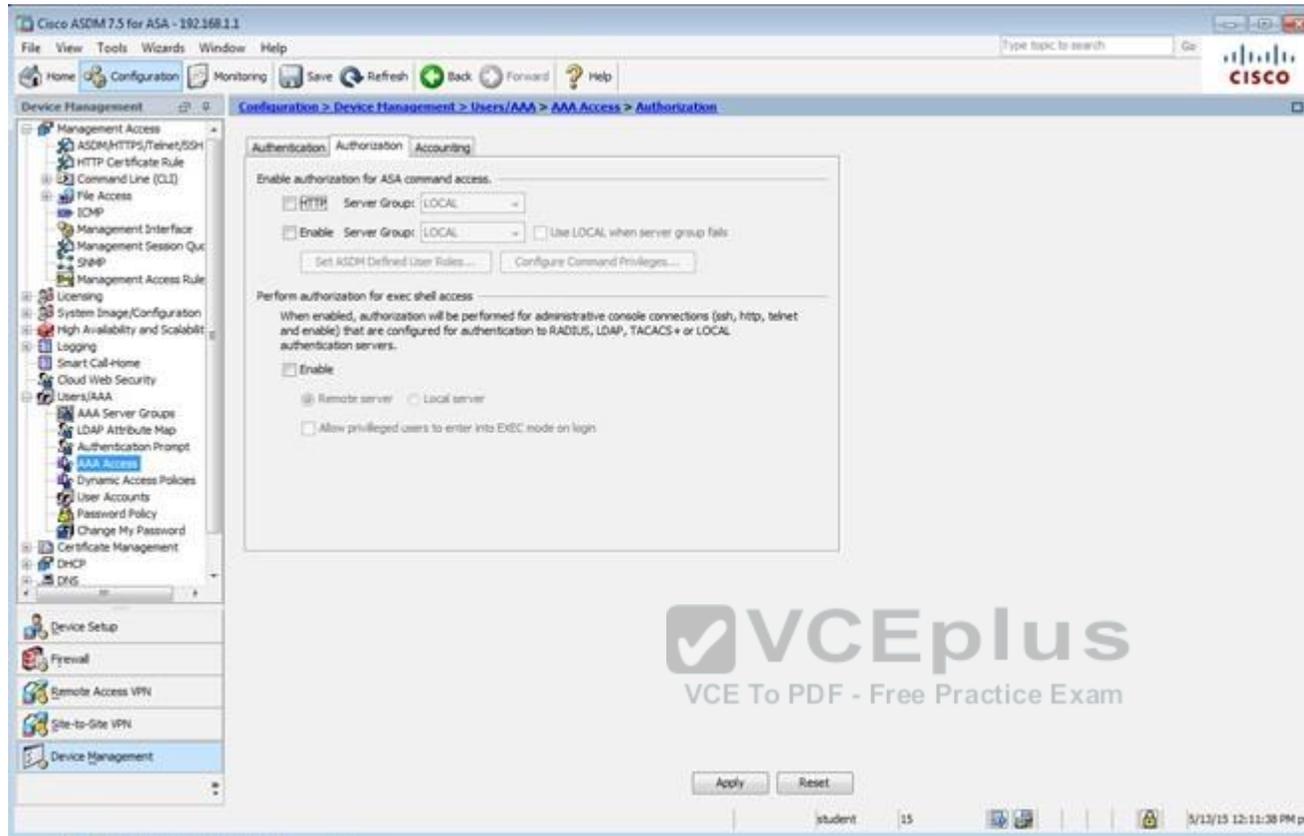




The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb trail is Configuration > Device Management > Management Access > Management Session Quota. The main content area contains the following text: "Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system." Below this, there is a "Management Session Quota" section with a radio button for "Limited" selected and a text input field containing the value "0". The range "(0 - 10000)" is shown to the right of the input field. At the bottom of the page, there are "Apply" and "Reset" buttons. The system tray at the bottom shows the user "student", the number "15", and the date/time "5/13/15 12:03:08 PM pet".



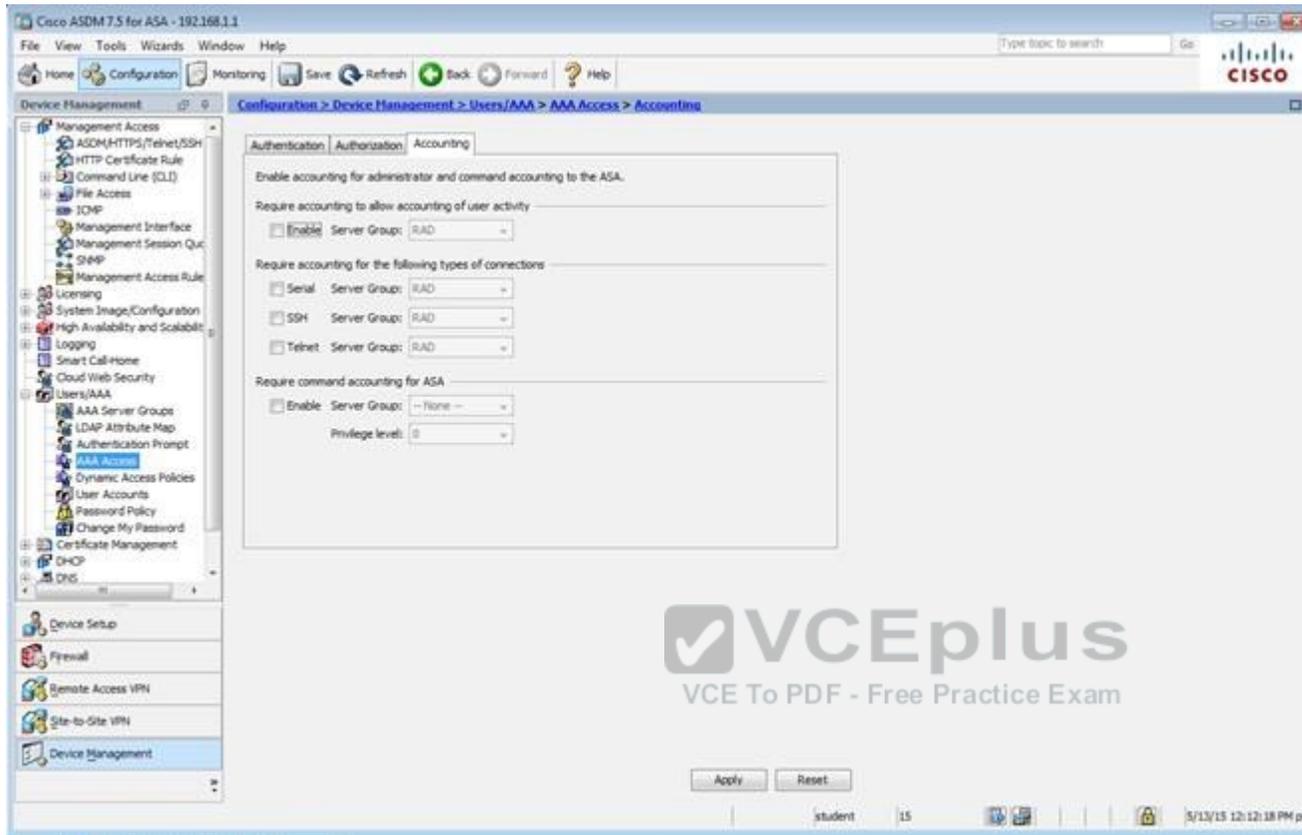




The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The title bar reads "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation path is "Configuration > Device Management > Users/AAA > AAA Access > Authorization". The left sidebar contains a tree view of configuration categories, with "Users/AAA" expanded to show "AAA Access". The main content area is titled "Authorization" and contains two sections:

- Enable authorization for ASA command access:** Includes checkboxes for "HTTP" and "Enable", each with a "Server Group" dropdown menu set to "LOCAL". There is also a checkbox for "Use LOCAL when server group fails".
- Perform authorization for exec: shell access:** Includes a checkbox for "Enable" and radio buttons for "Remote server" (selected) and "Local server". There is also a checkbox for "Allow privileged users to enter into EXEC mode on login".

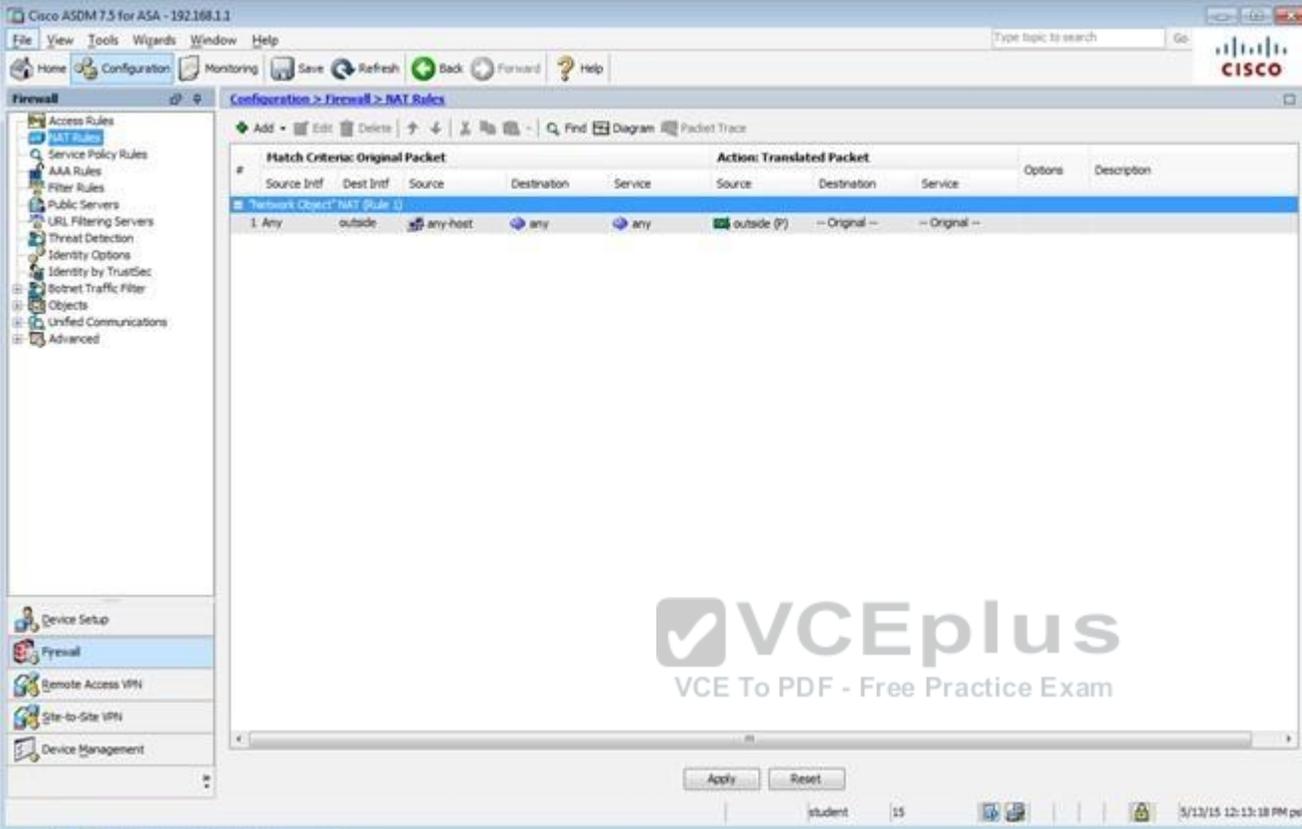
At the bottom of the configuration area, there are "Apply" and "Reset" buttons. The system tray at the bottom right shows the date and time: "5/13/15 12:11:38 PM pet".



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The browser title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The navigation path is "Configuration > Device Management > Users/AAA > AAA Access > Accounting". The left sidebar shows a tree view with "Users/AAA" expanded to "AAA Access". The main content area has three tabs: "Authentication", "Authorization", and "Accounting", with "Accounting" selected. The "Accounting" tab contains the following configuration options:

- Enable accounting for administrator and command accounting to the ASA. (checked)
- Require accounting to allow accounting of user activity:
 - Enable Server Group: RAD
- Require accounting for the following types of connections:
 - Serial Server Group: RAD
 - SSH Server Group: RAD
 - Telnet Server Group: RAD
- Require command accounting for ASA:
 - Enable Server Group: -- None --
 - Privilege level: 0

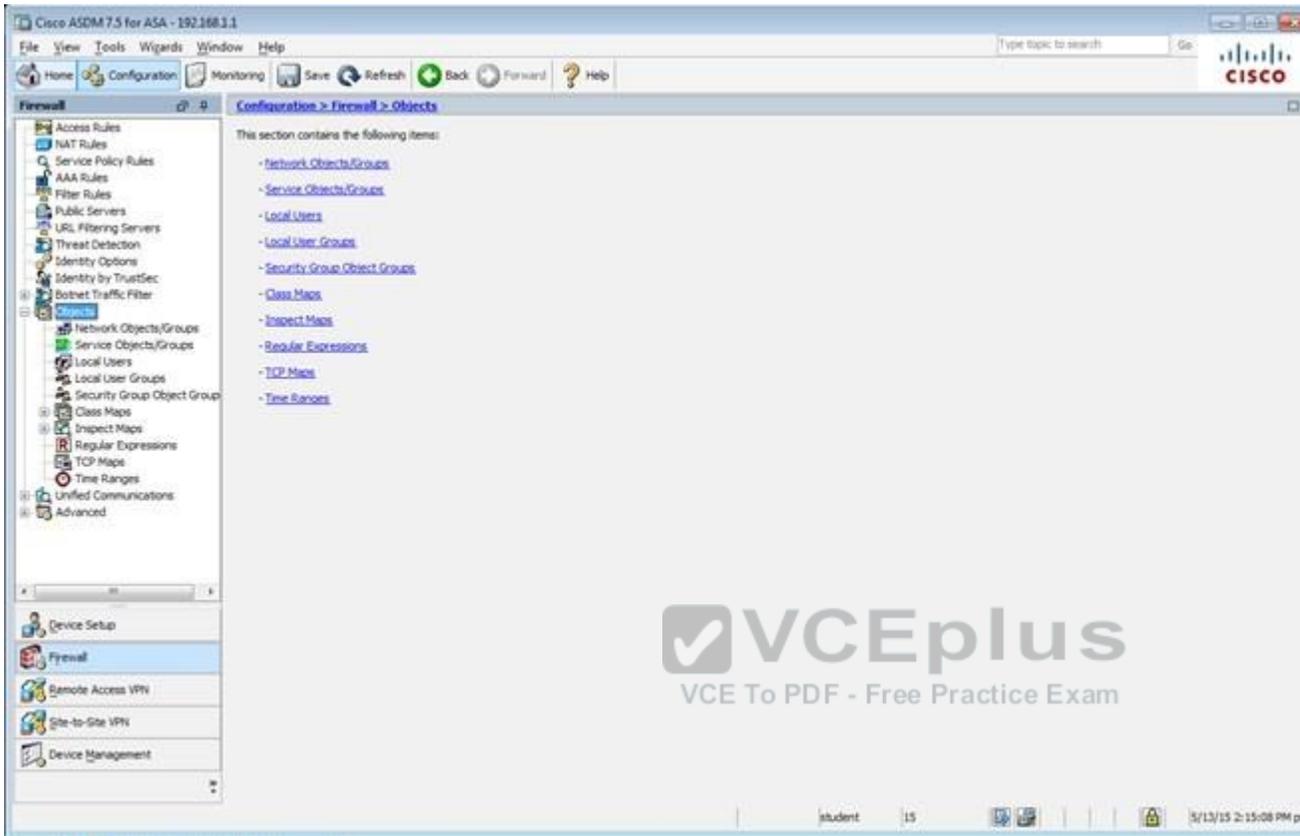
At the bottom of the configuration area are "Apply" and "Reset" buttons. The status bar at the very bottom shows "student | 15 | 5/13/15 12:12:18 PM pdt".

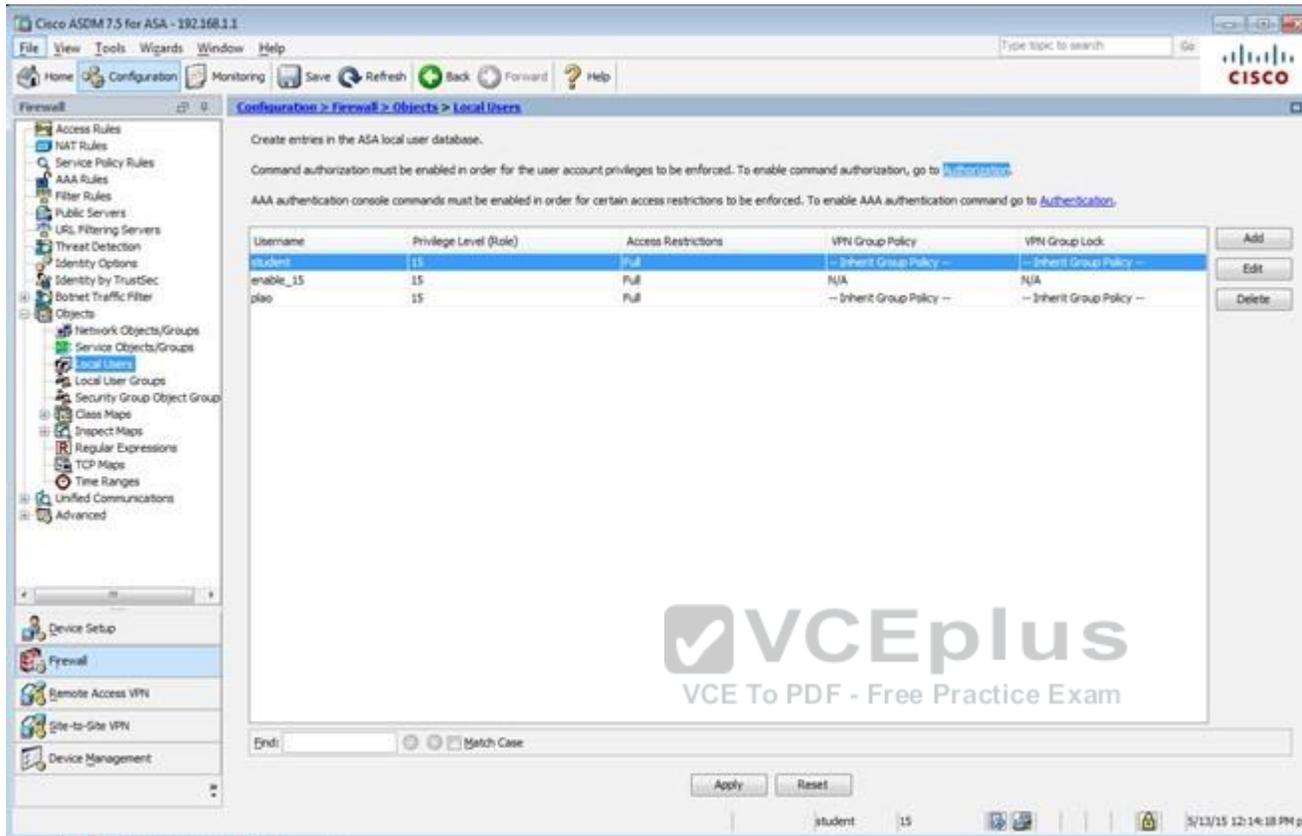


The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for NAT Rules. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table with columns for Match Criteria and Action. The table contains one rule with the following details:

Match Criteria: Original Packet				Action: Translated Packet				Options	Description
Source Intf	Dest Intf	Source	Destination	Source	Destination	Service			
1. Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		

At the bottom of the window, there are 'Apply' and 'Reset' buttons. The status bar at the very bottom shows 'student 15' and the date '5/13/15 12:13:18 PM pet'.





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End:

student 15 5/13/15 12:14:18 PM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Network Objects/Groups

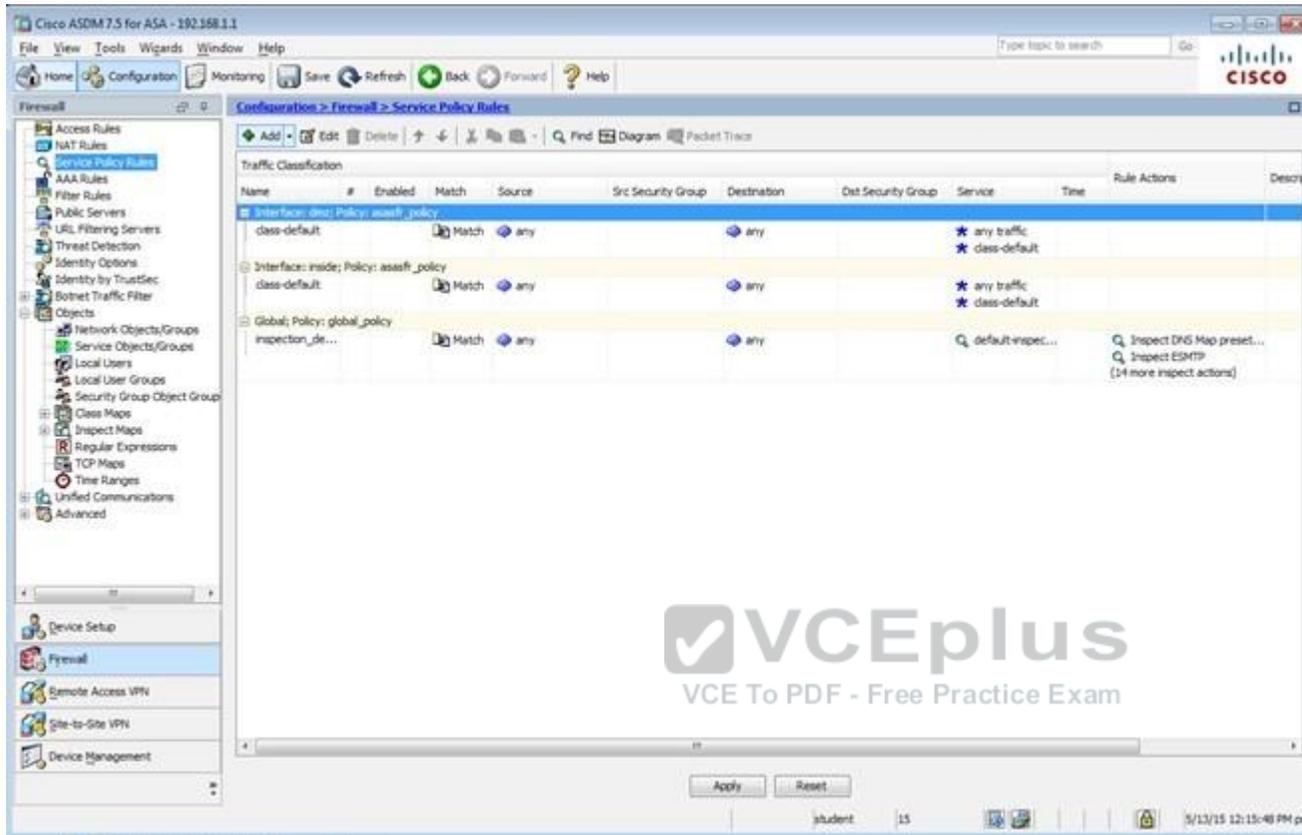
Filter: [Clear]

Name	IP Address	Netmask	Description	Object NAT Address
any				
any-host	0.0.0.0	0.0.0.0		outside (F)
any4				
any6				
facebook	www.facebook.com			
My_ASA_Demo_Obj	1.10.8.20			

Apply Reset

student 15 5/13/15 12:30:08 PM pet

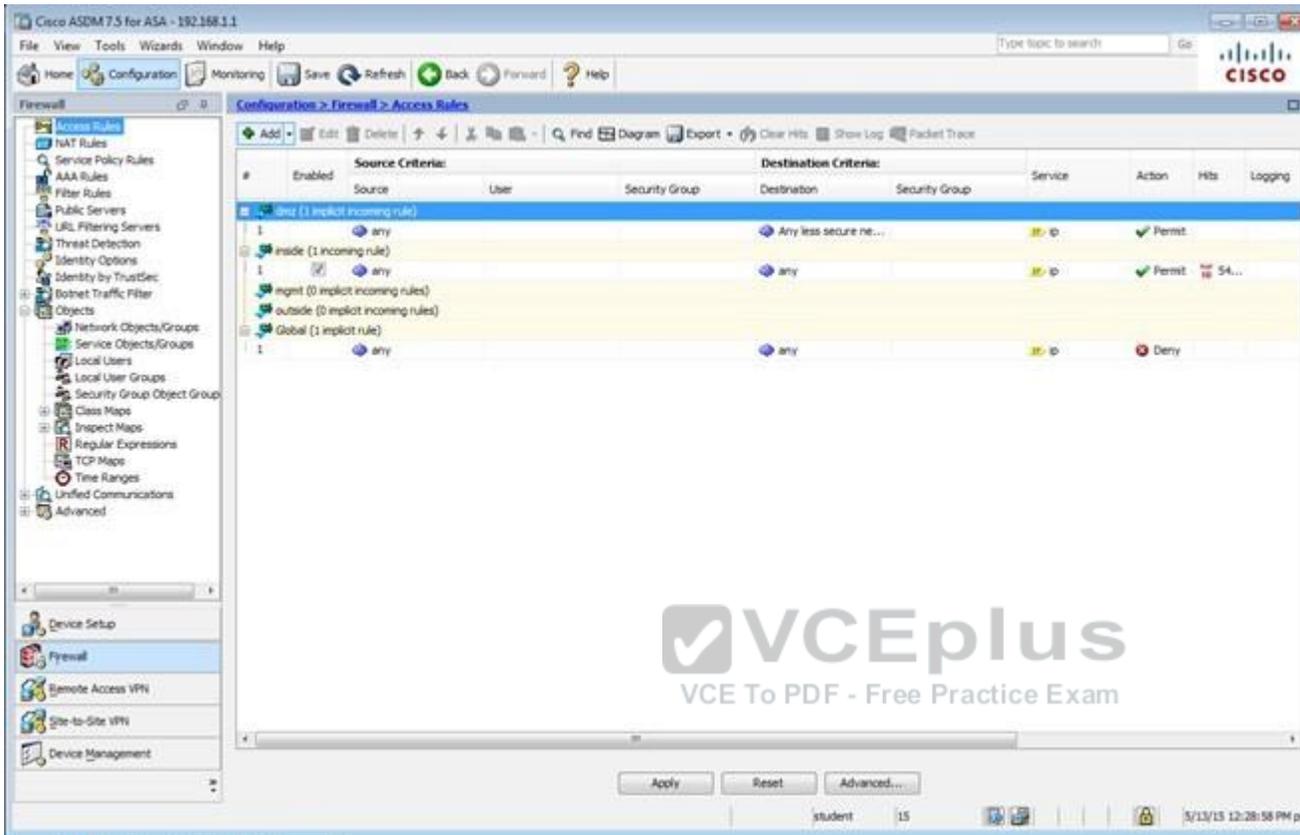
VCEplus
VCE To PDF - Free Practice Exam



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left-hand navigation pane shows a tree structure with "Service Policy Rules" selected. The main area contains a table of traffic classification rules. The table has columns for Name, #, Enabled, Match, Source, Src Security Group, Destination, Dst Security Group, Service, Time, Rule Actions, and Description. The rules listed are:

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Interface: (int); Policy: asastf_policy											
class-default			Match	any		any		any traffic			
								class-default			
Interface: inside; Policy: asaastf_policy											
class-default			Match	any		any		any traffic			
								class-default			
Global; Policy: global_policy											
inspection_de...			Match	any		any		default-inspec...		Inspect DNS Map preset... Inspect ESMTP (14 more inspect actions)	

The bottom status bar shows "student | 15 | 5/13/15 12:15:48 PM pst".



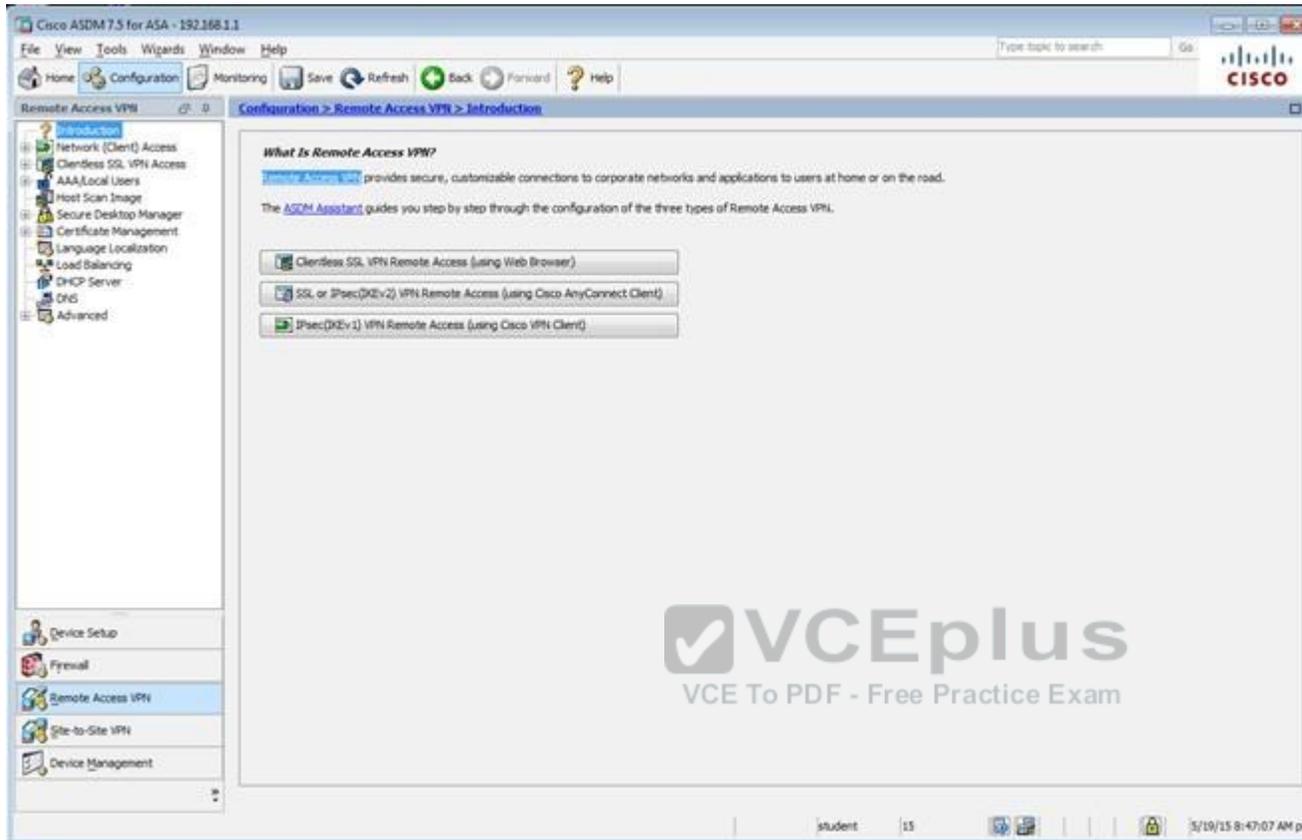
Cisco ASDM 7.5 for ASA - 192.168.1.1

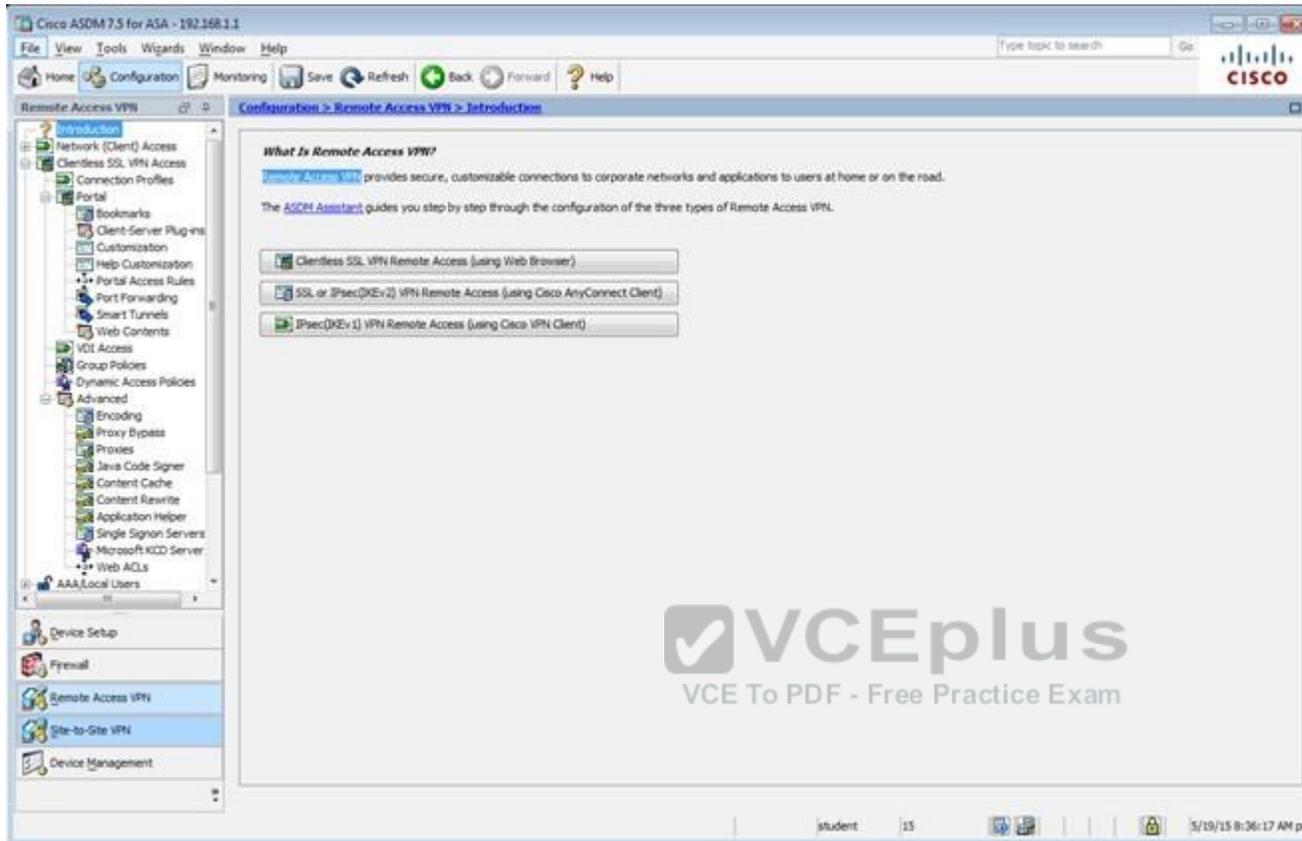
Configuration > Firewall > Access Rules

#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group				
ibzz (1 implicit incoming rule)										
1		any			Any less secure ne...		IP	Permit		
inside (1 incoming rule)										
1		any			any		IP	Permit	54...	
ingnt (0 implicit incoming rules)										
outside (0 implicit incoming rules)										
Global (1 implicit rule)										
1		any			any		IP	Deny		

Apply Reset Advanced...

student 15 3/13/15 12:28:58 PM pdt





The screenshot shows the Cisco ASDM 7.5 for ASA interface. The breadcrumb trail is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows a tree view with 'Remote Access VPN' selected. The main content area is divided into three sections:

- Access Interfaces:** A table to enable interfaces for clientless SSL VPN access.

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

 Below the table are buttons for 'Device Certificate ...' and 'Port Setting ...'. A checkbox 'Bypass interface access lists for inbound VPN sessions' is checked. A note states: '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 can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete, Find: [text box], Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
DefaultVEBVPNGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
test	<input checked="" type="checkbox"/>	test	AAA(LOCAL)	DfltGrpPolicy

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

At the bottom are 'Apply' and 'Reset' buttons. The status bar shows 'student | 15 | 5/19/15 8:38:47 AM pet'.

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL Manage...
 Use LOCAL if Server Group fails

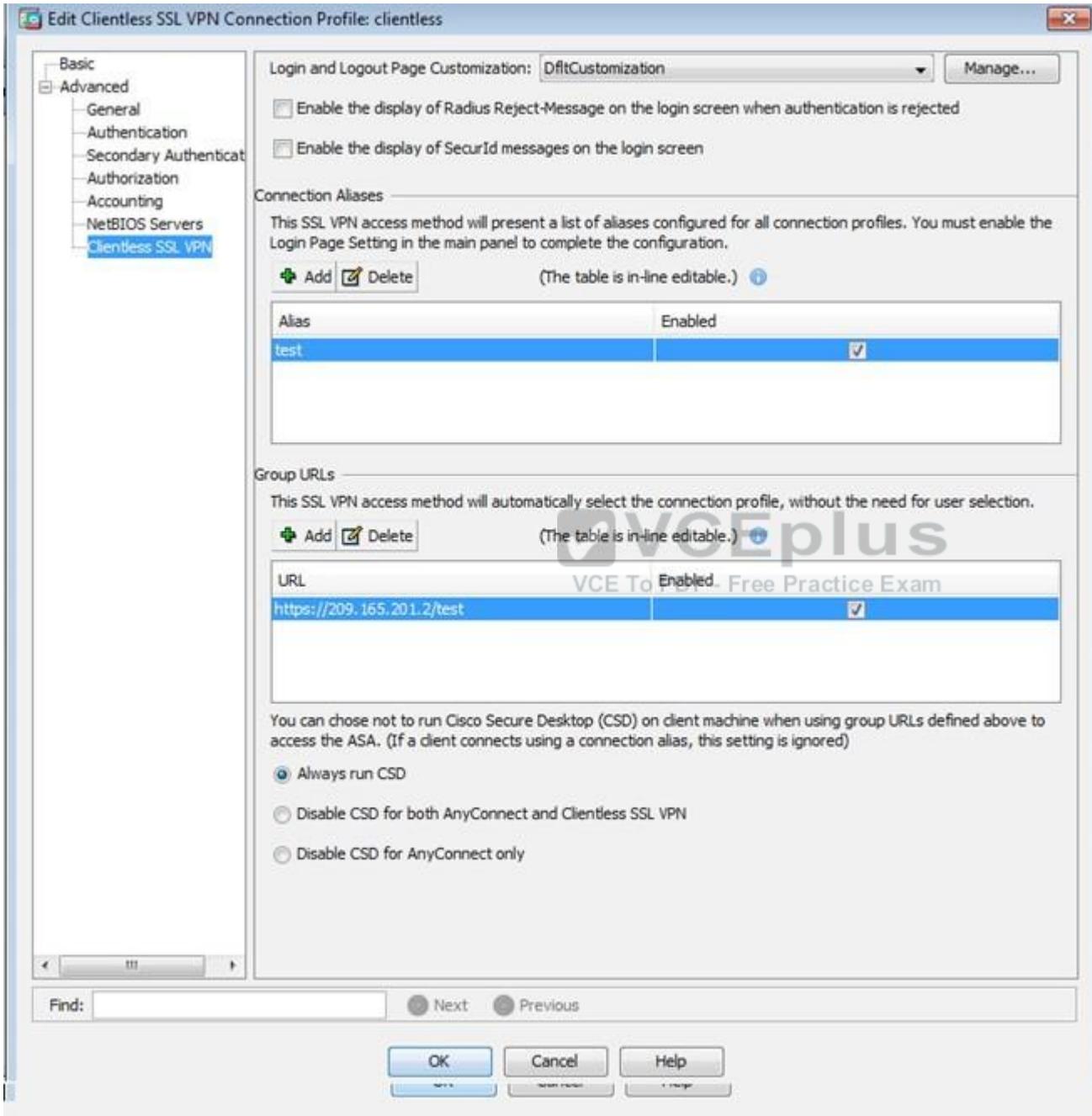
DNS
Server Group: DefaultDNS Manage...
(Following fields are attributes of the DNS server group selected above.)
Servers: 192.168.1.2
Domain Name: secure-x.local

Default Group Policy
Group Policy: Sales Manage...
(Following field is an attribute of the group policy selected above.)
 Enable clientless SSL VPN protocol

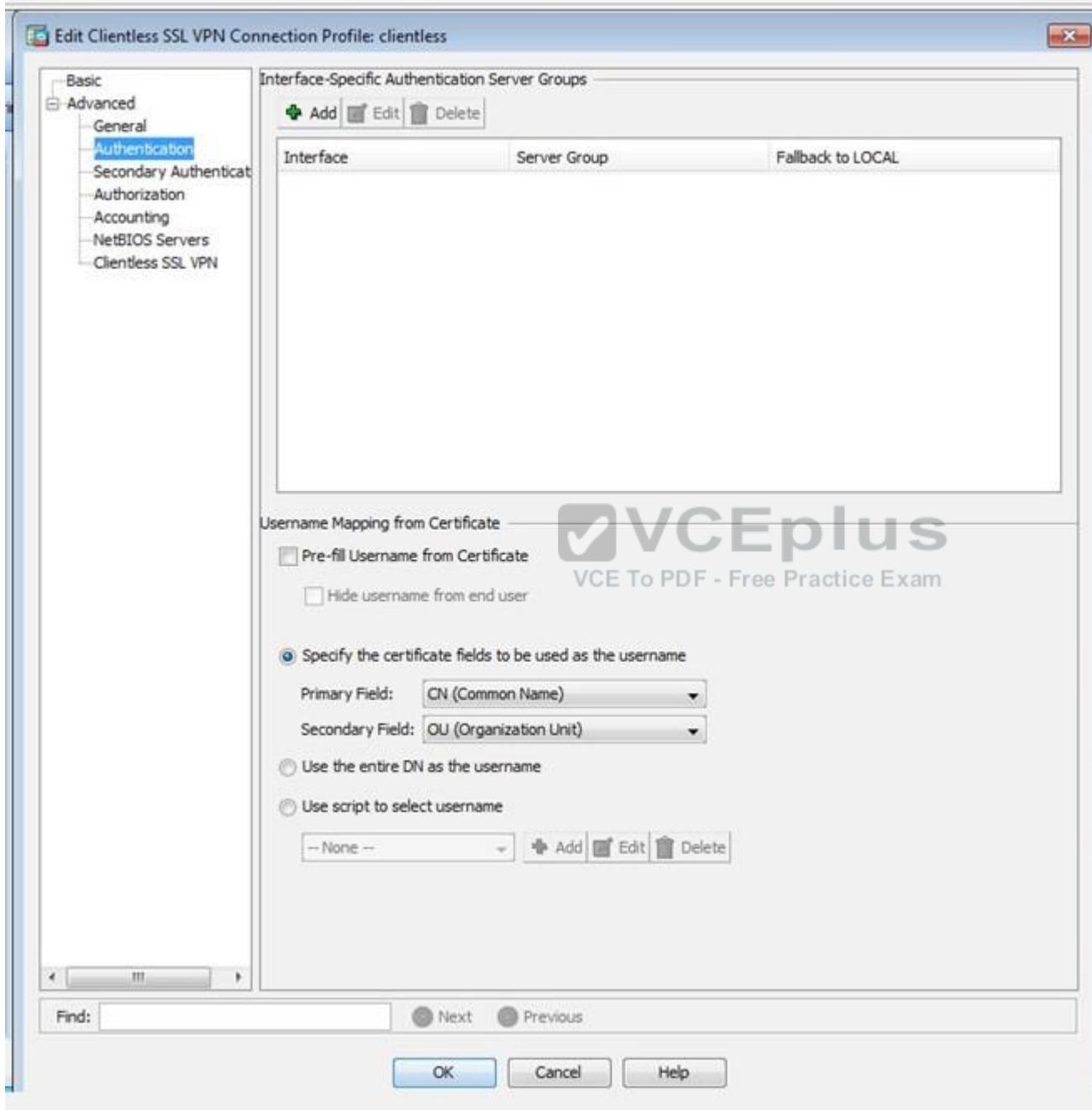
Find: Next Previous

OK Cancel Help

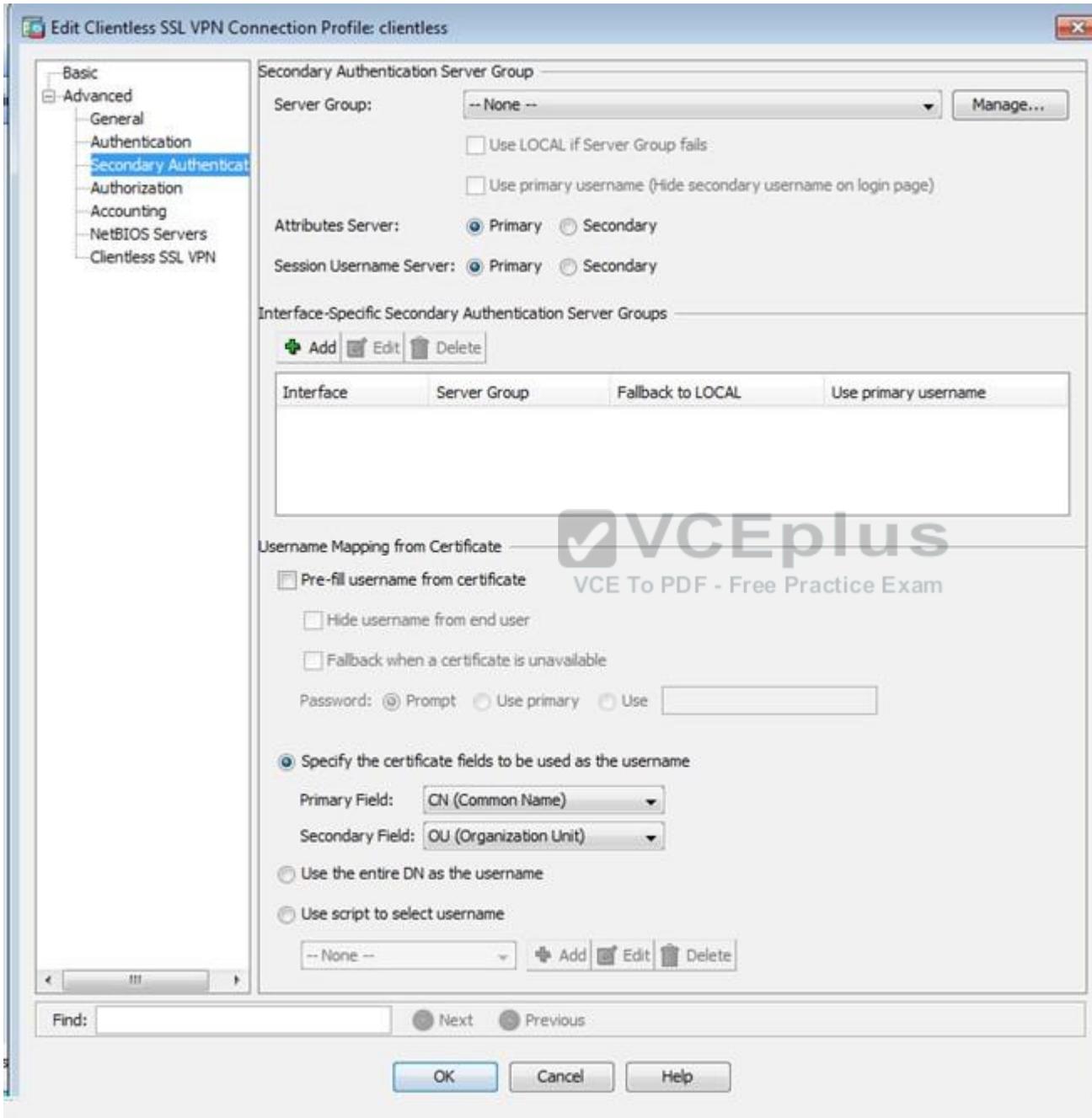


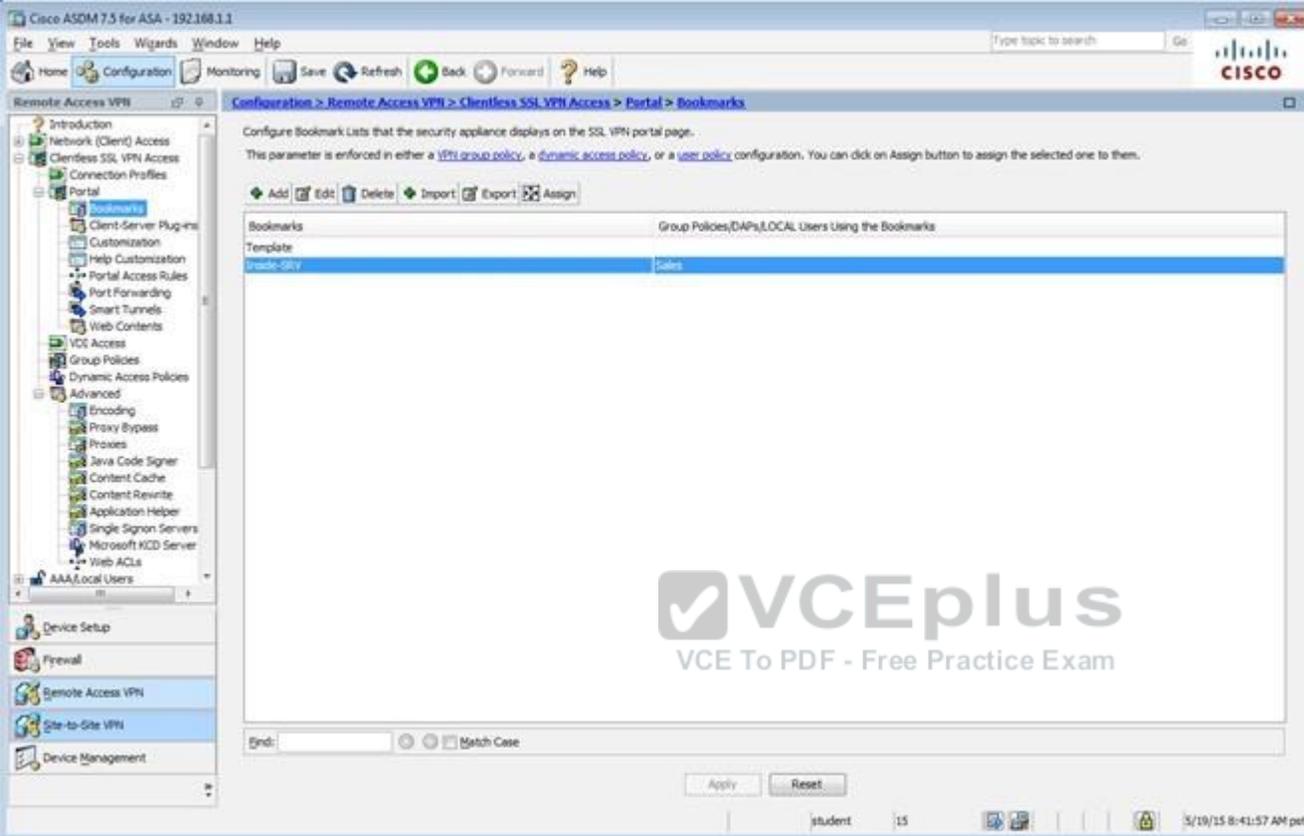










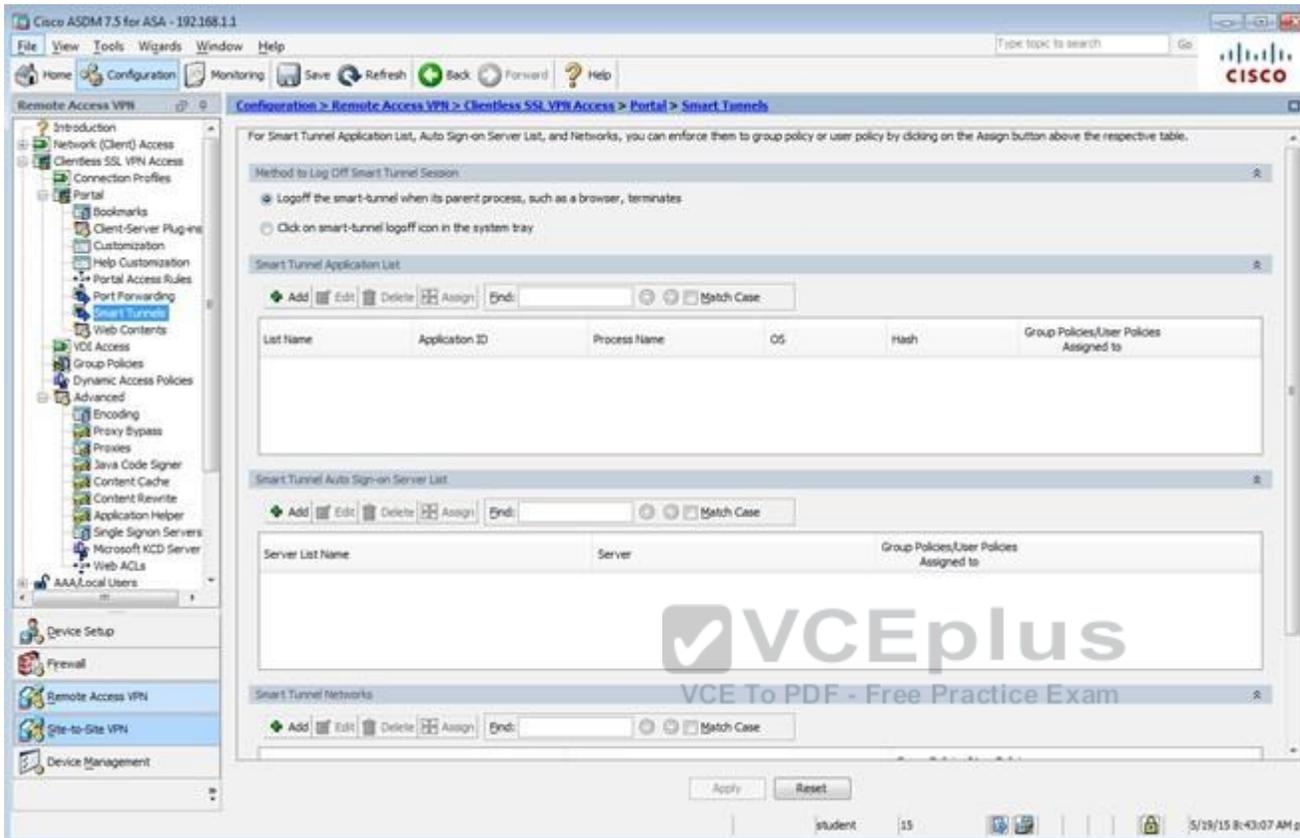


The screenshot shows the Cisco ASDM 7.5 interface for configuring the Bookmarks section of the Clientless SSL VPN portal. The breadcrumb path is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The main content area contains a table with the following data:

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Inside-01V	Sales

Below the table, there is an 'End:' field and a 'Match Case' checkbox. At the bottom of the configuration area are 'Apply' and 'Reset' buttons. The interface also features a left-hand navigation tree and a top menu bar with 'File', 'View', 'Tools', ' Wizards', 'Window', and 'Help'.

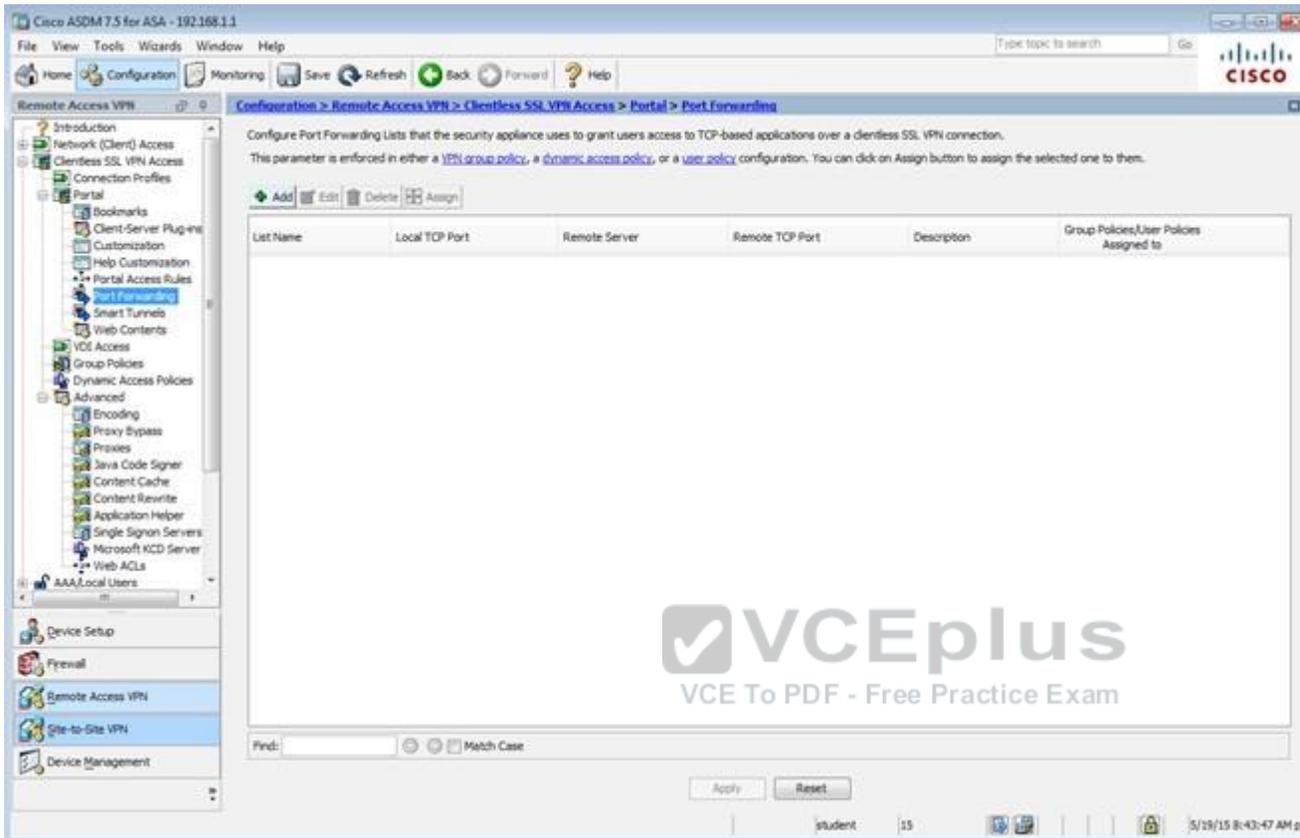




The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The navigation pane on the left shows the configuration path: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**. The main content area is titled "Smart Tunnels" and contains the following sections:

- Method to Log Off Smart Tunnel Session:** Includes radio buttons for "Logoff the smart-tunnel when its parent process, such as a browser, terminates" (selected) and "Click on smart-tunnel logoff icon in the system tray".
- Smart Tunnel Application List:** Features a table with columns: List Name, Application ID, Process Name, OS, Hash, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Auto Sign-on Server List:** Features a table with columns: Server List Name, Server, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Networks:** Features a table with controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".

At the bottom of the main content area, there are "Apply" and "Reset" buttons. The status bar at the very bottom shows "student | 15 | 5/19/15 8:43:07 AM pst". A large "VCEplus" watermark is overlaid on the center of the screenshot.



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb trail is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding Lists. The main content area contains the following text:

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

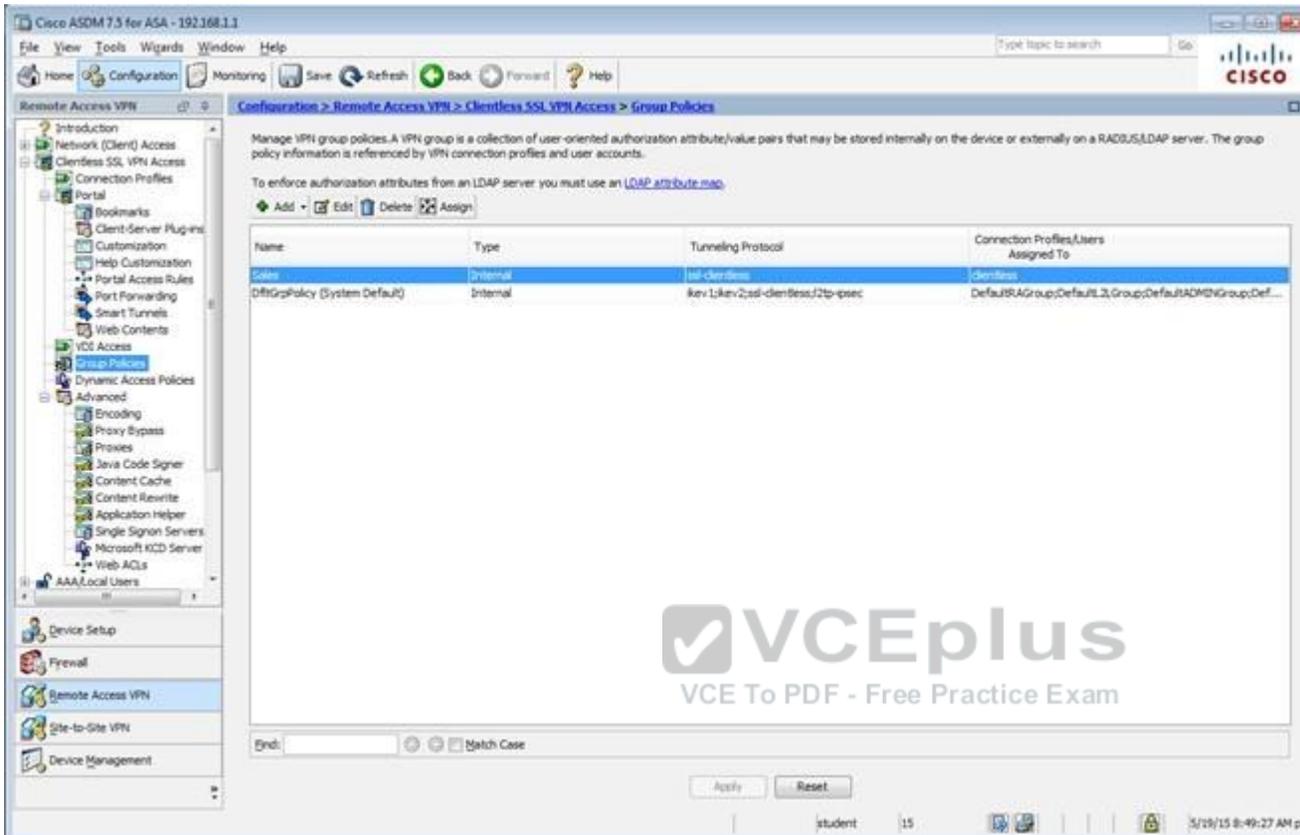
Buttons: Add, Edit, Delete, Assign

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description	Group Policies/User Policies Assigned to
-----------	----------------	---------------	-----------------	-------------	--

Find: Match Case

Buttons: Apply, Reset

Footer: student 15 5/19/15 8:43:47 AM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

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 pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

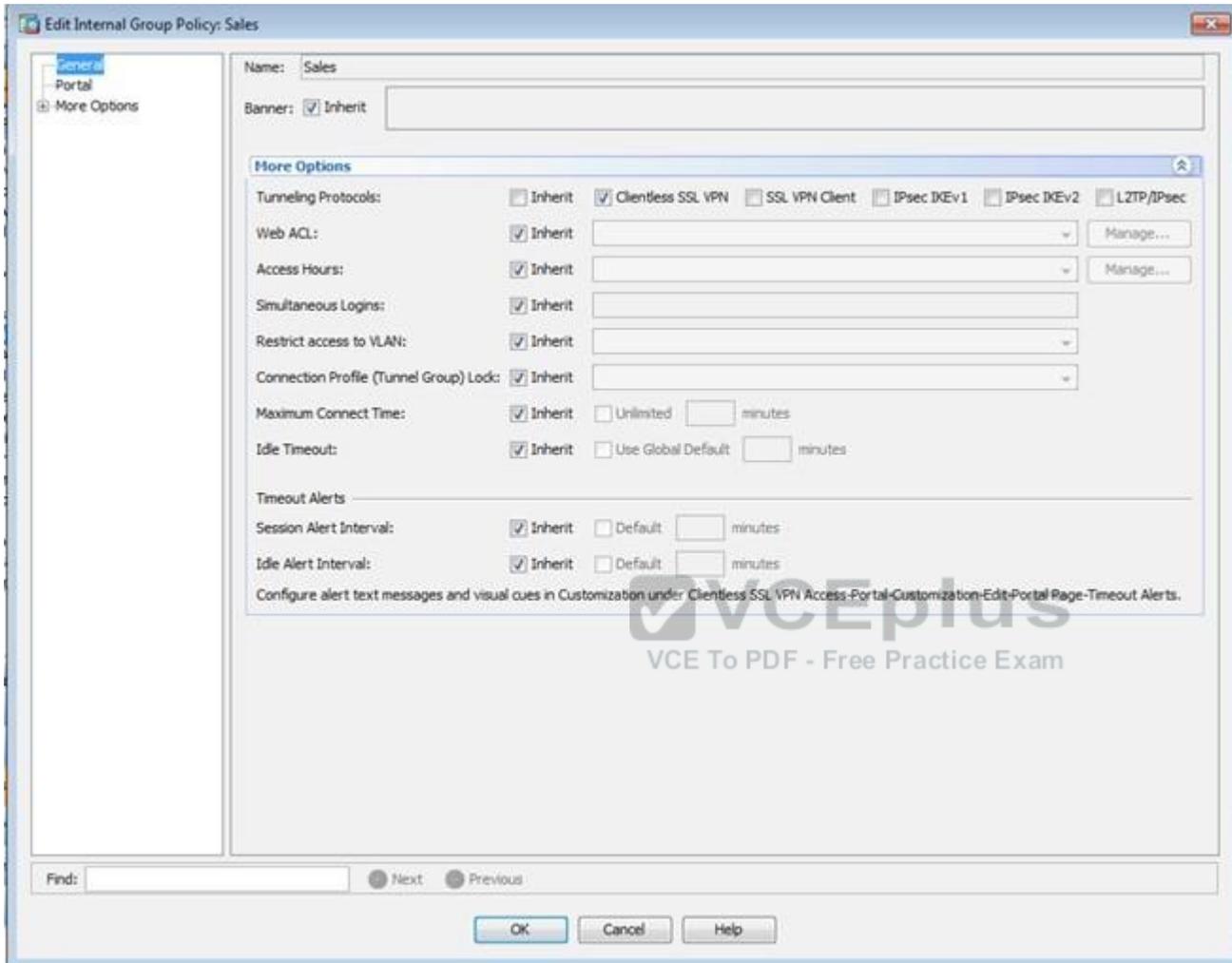
◆ Add ◆ Edit ◆ Delete ◆ Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Clientless	Internal	ssl-clientless	Clientless
DefaultGroupPolicy (System Default)	Internal	kev1okriv2ssl-clientless/2tp-espsec	DefaultRAGroup/DefaultIL2,Group/DefaultADMDNGroup/Def...

End: Match Case

Apply Reset

student 15 5/18/15 8:49:27 AM pst



The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the navigation tree with 'Remote Access VPN' selected. The main content area is titled 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies'. It contains instructions on managing VPN group policies and a table of existing policies.

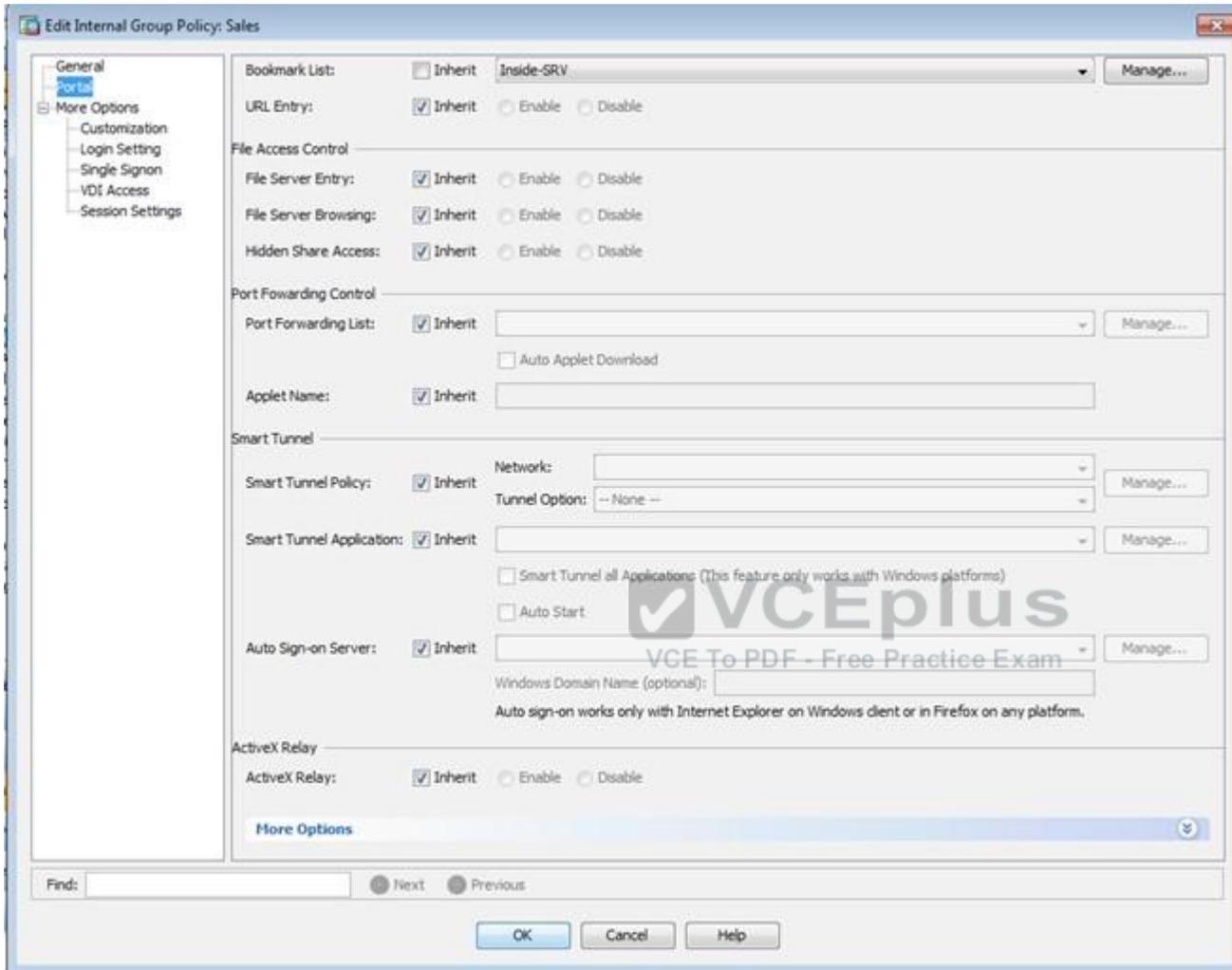
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

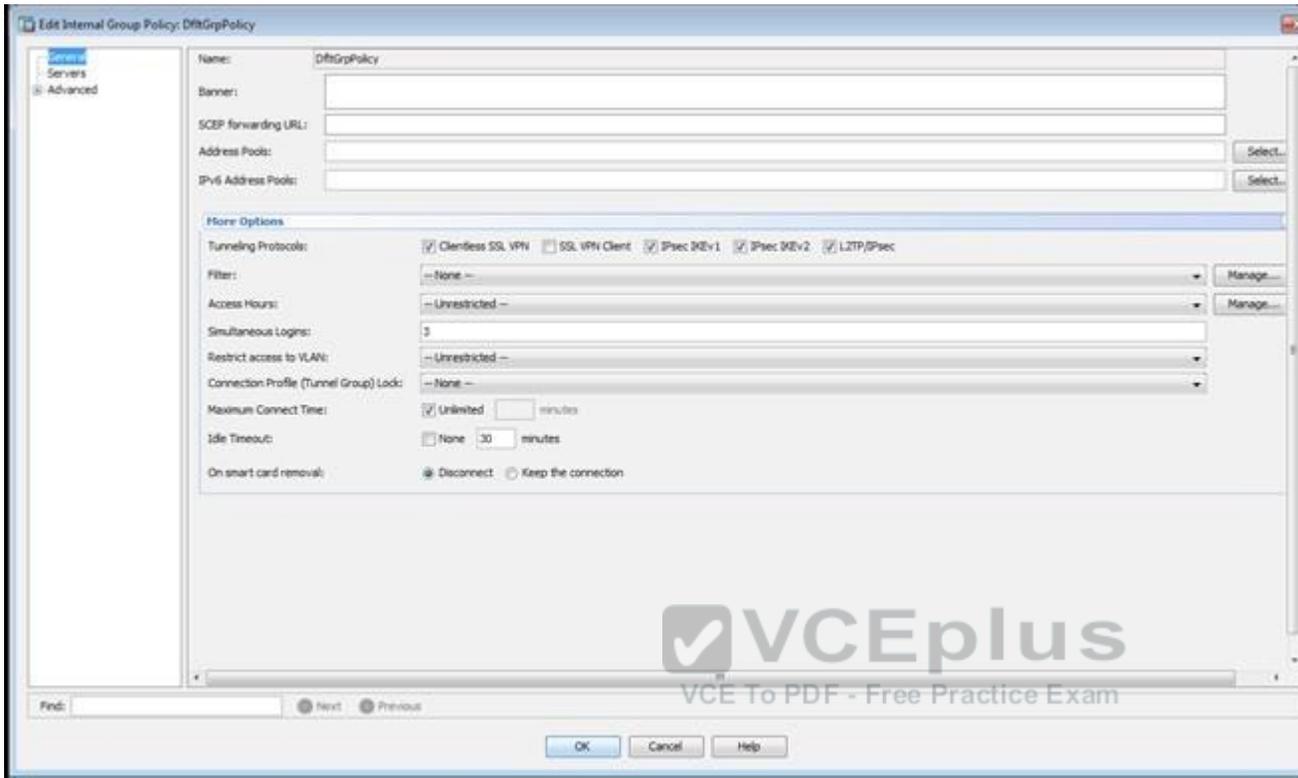
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

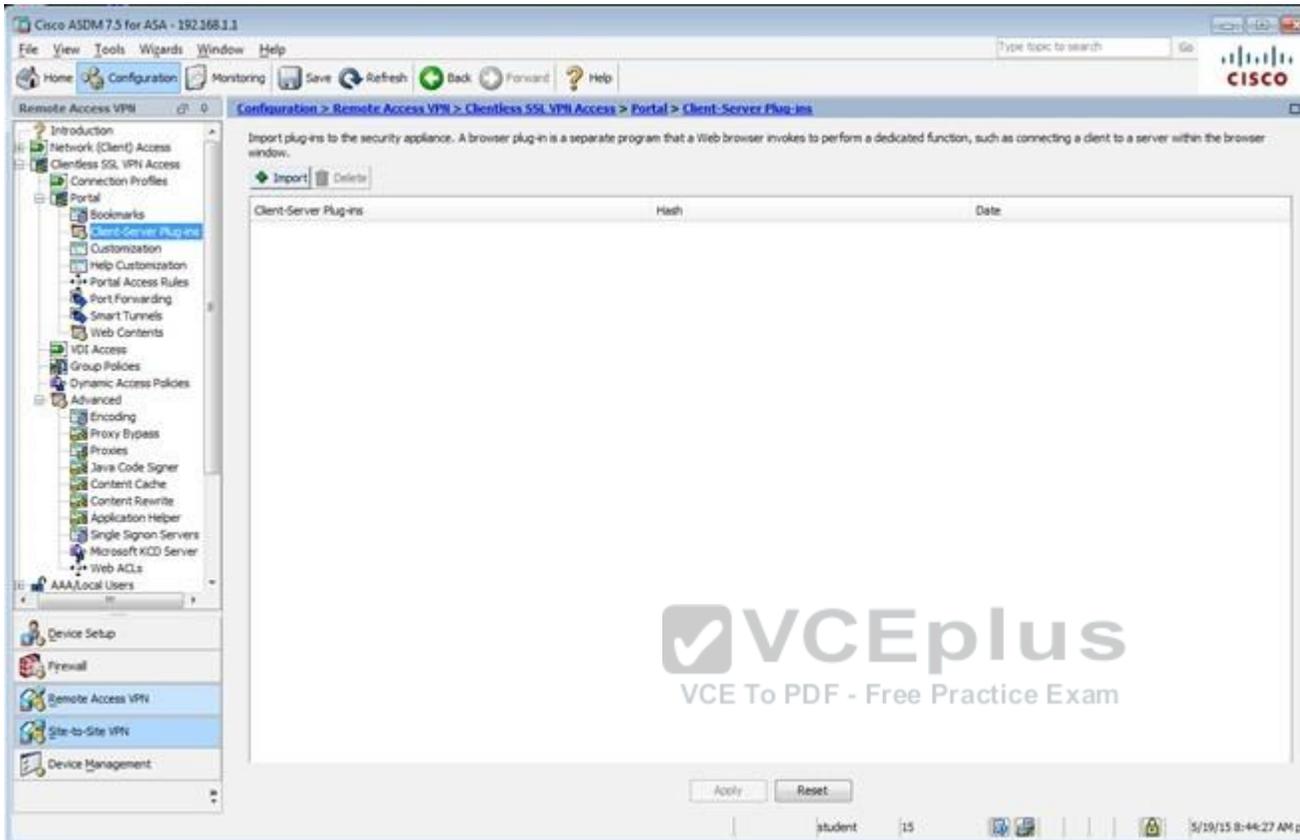
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	l2l-Clientless	Sales
DfltGrpPolicy (System Default)	Internal	ikev1/ikev2ssl-clientless/2ip-sslsec	DfltGrpPolicy

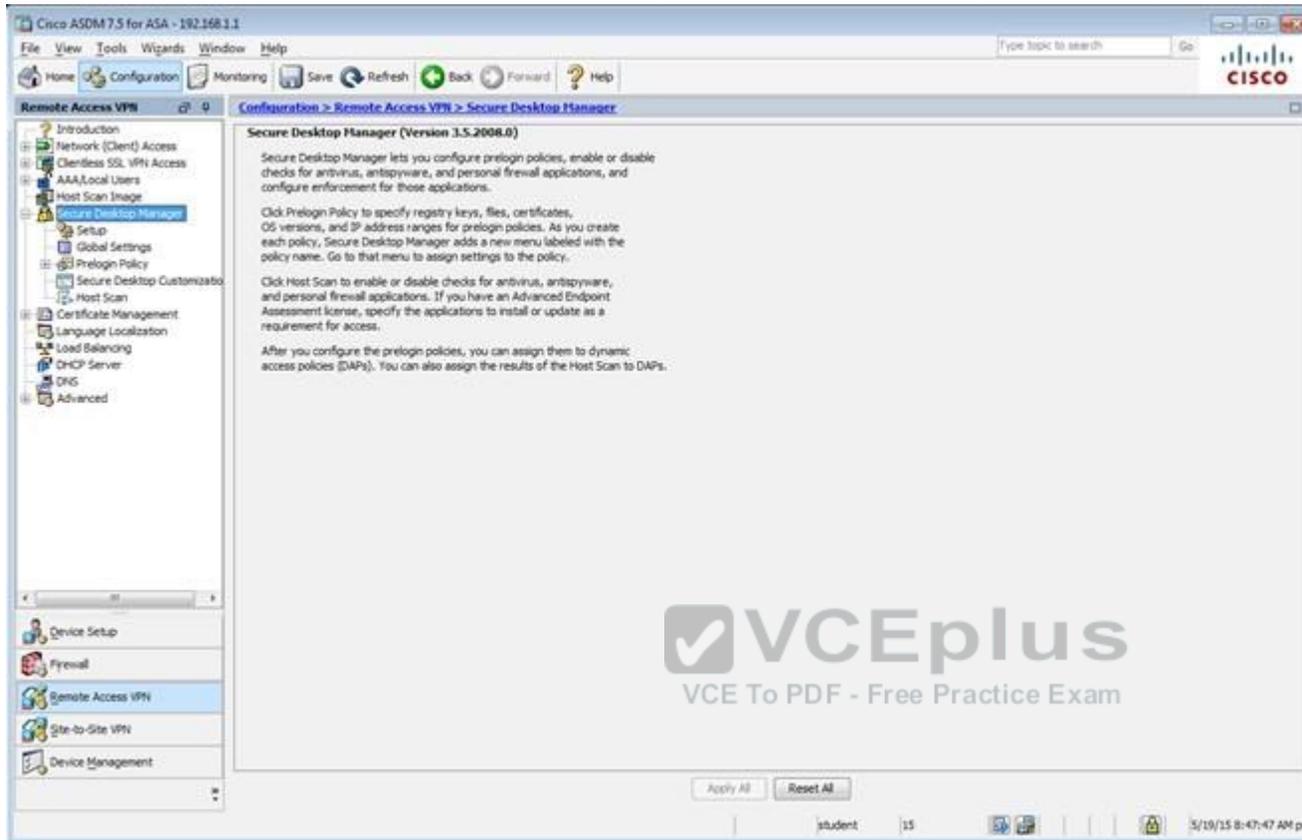
Find:

student | 15 | 10/15/14 9:15:43 AM pst









The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the "Secure Desktop Manager (Version 3.5.2008.0)" configuration page. The page includes a navigation tree on the left with categories like "Remote Access VPN", "Network (Client) Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The "Secure Desktop Manager" section is expanded, showing sub-items: "Introduction", "Setup", "Global Settings", "Prelogin Policy", "Secure Desktop Customization", "Host Scan", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

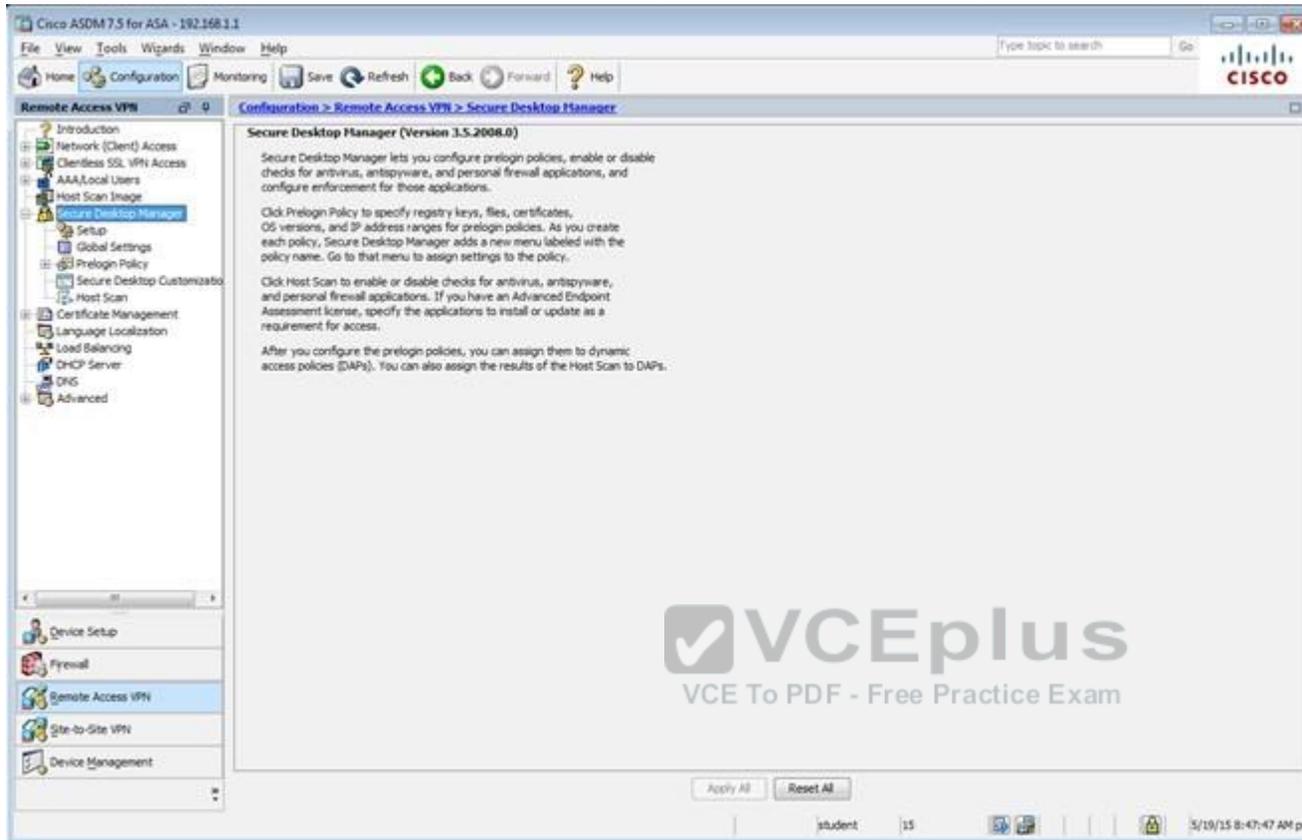
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispware, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispware, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the "Secure Desktop Manager (Version 3.5.2008.0)" configuration page. The left sidebar shows a tree view with "Remote Access VPN" selected, and "Secure Desktop Manager" highlighted under the "Remote Access VPN" section. The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

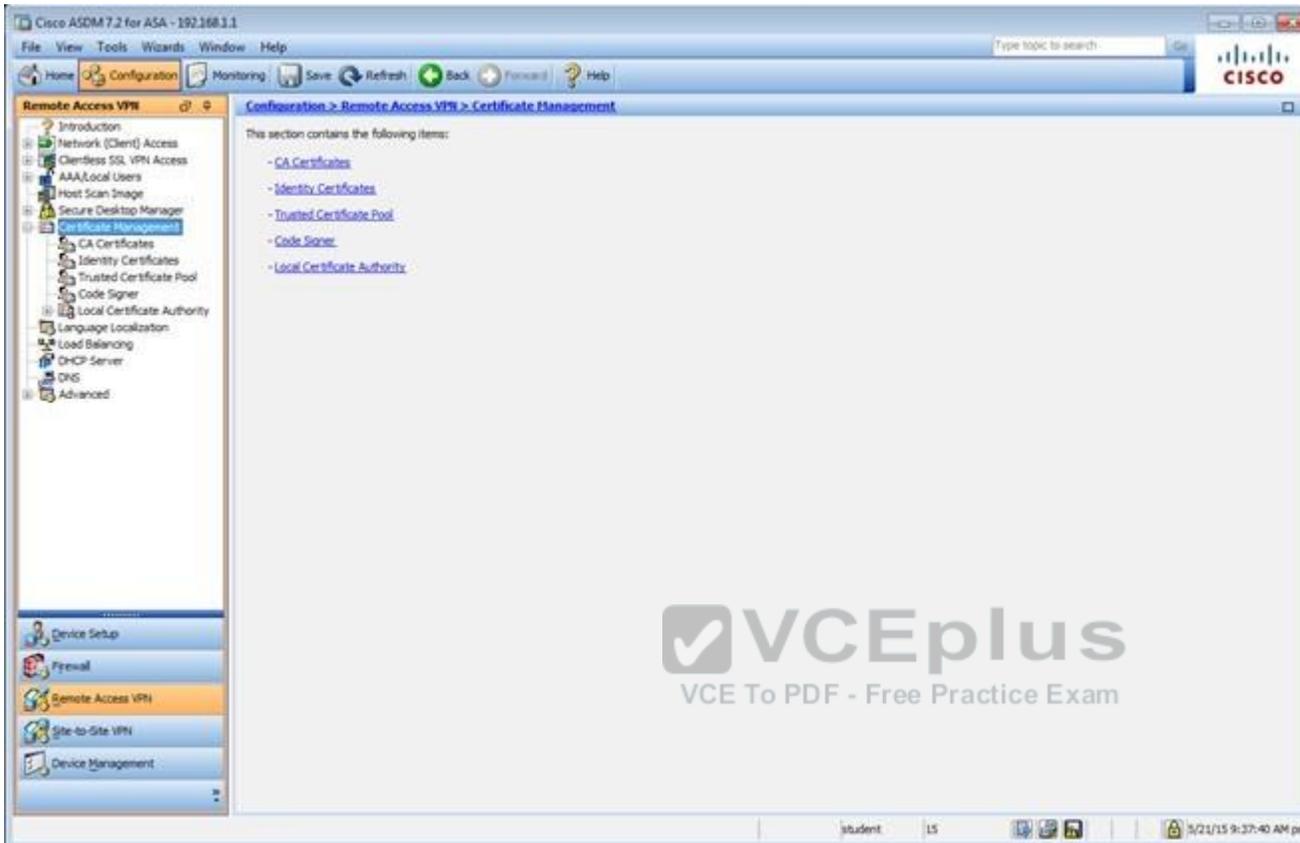
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispam, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispam, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

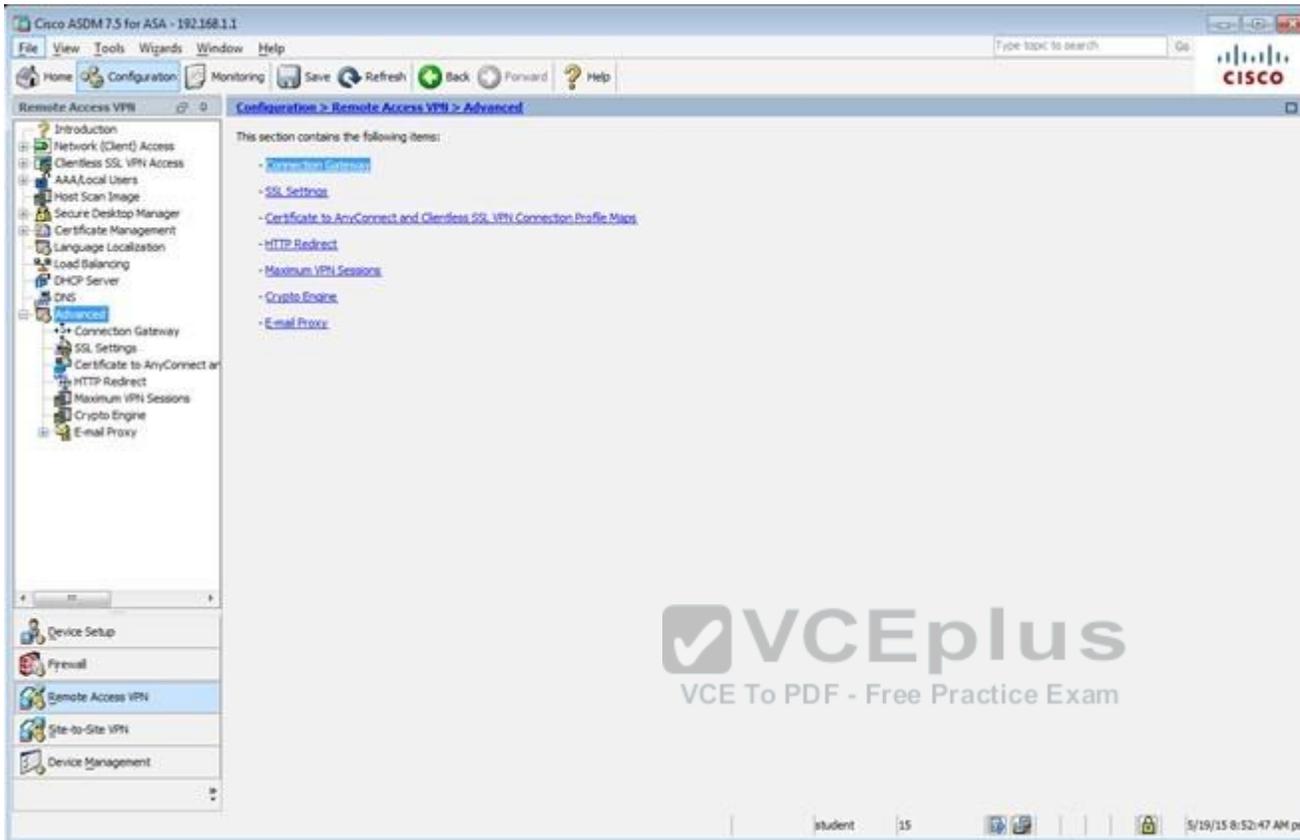
At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Certificate Management > Identity Certificates". The left sidebar shows a tree view with "Identity Certificates" selected. The main content area contains a table with the following data:

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname-#1 [7-ASA.sec...]	hostname-#1 [7-ASA.sec...]	11:10:33 pet (Dec 20 2024)	ASDM_Trustpoint1	General Purpose	RSA (2048 bits)

Below the table, there are sections for "Certificate Expiration Alerts" (Send the first alert before: 60 (days), Repeat Alert Interval: 7 (days)) and "Public CA Enrollment" (Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust). A "Launch ASDM Identity Certificate Wizard" button is visible at the bottom of the main content area. The status bar at the bottom shows "student | 15 | 5/19/15 8:51:47 AM pet".



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Advanced > SSL Settings". The left sidebar shows a tree view with "Remote Access VPN" selected. The main content area is titled "Configure SSL parameters. These parameters affect both ASDM and SSL VPN access." and contains the following settings:

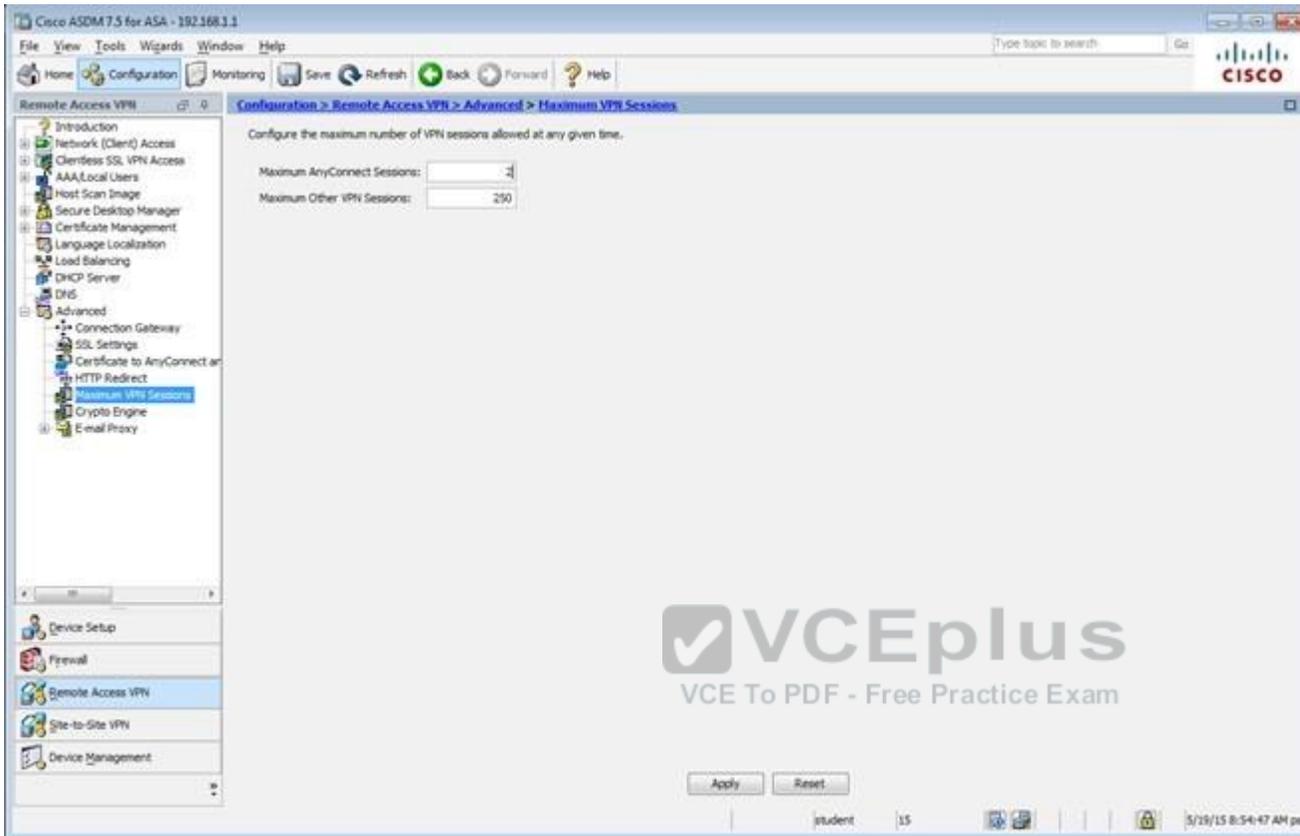
- The minimum SSL version for the security appliance to negotiate as a "server": TLS V1
- The minimum SSL version for the security appliance to negotiate as a "client": TLS V1
- Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modAus
- ECDH group to be used with SSL: Group19 - 256-bit EC

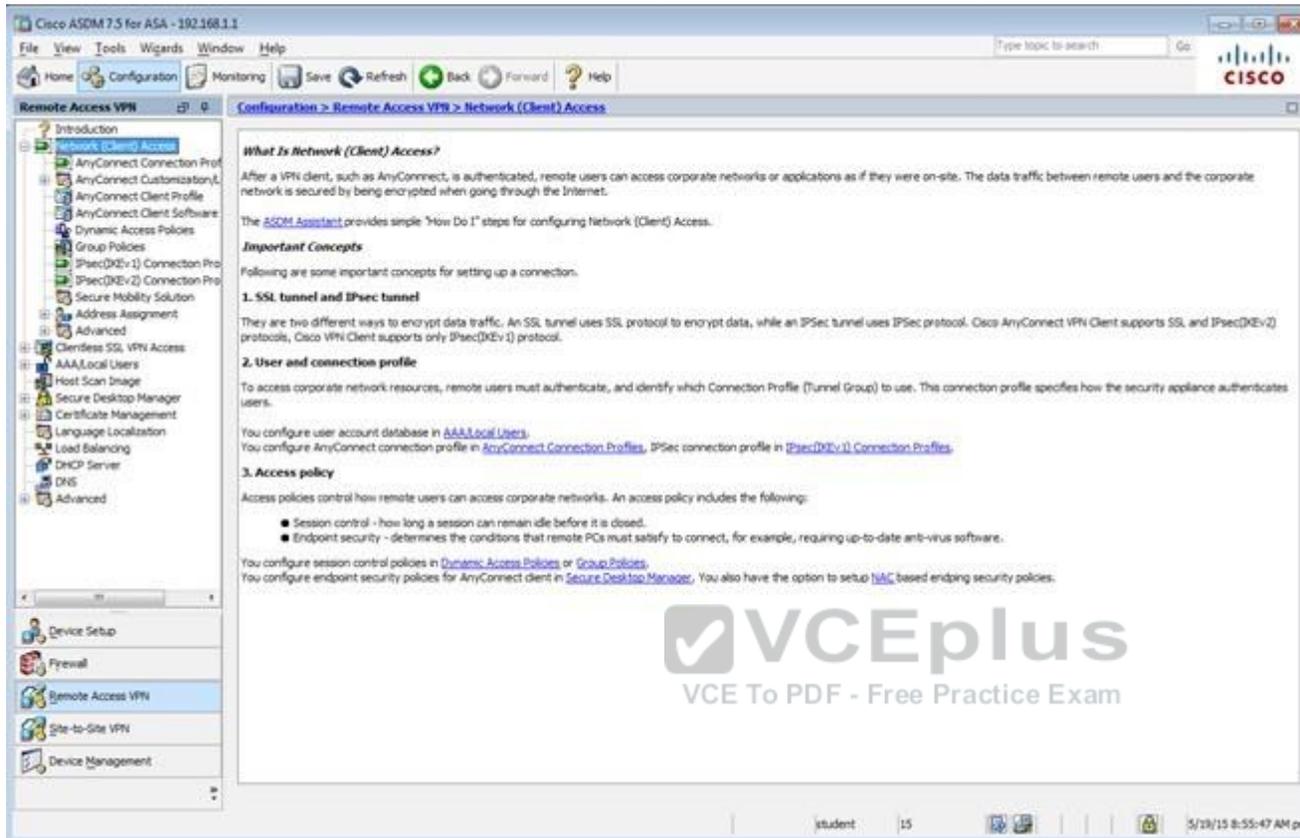
The "Encryption" section contains a table with the following data:

Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
DTLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...

The "Server Name Indication (SNI)" section shows a "Domain" field with the value "dmz" and a "Certificate" dropdown menu with "ASDM_TrustPoint1.h..." selected. There are "Add", "Edit", and "Delete" buttons for the SNI entries.

The "Certificates" section at the bottom states: "Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own." There are "Apply" and "Reset" buttons at the bottom of the configuration area.





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the configuration page for "Remote Access VPN > Network (Client) Access". The page includes a navigation pane on the left with a tree view of configuration options, a main content area with text and links, and a bottom status bar.

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKv2) protocols. Cisco VPN Client supports only IPsec(DKv1) protocol.

2. User and connection profile

To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user account database in [AAA Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKv1\) Connection Profiles](#).

3. Access policy

Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HMAC](#) based endpoint security policies.

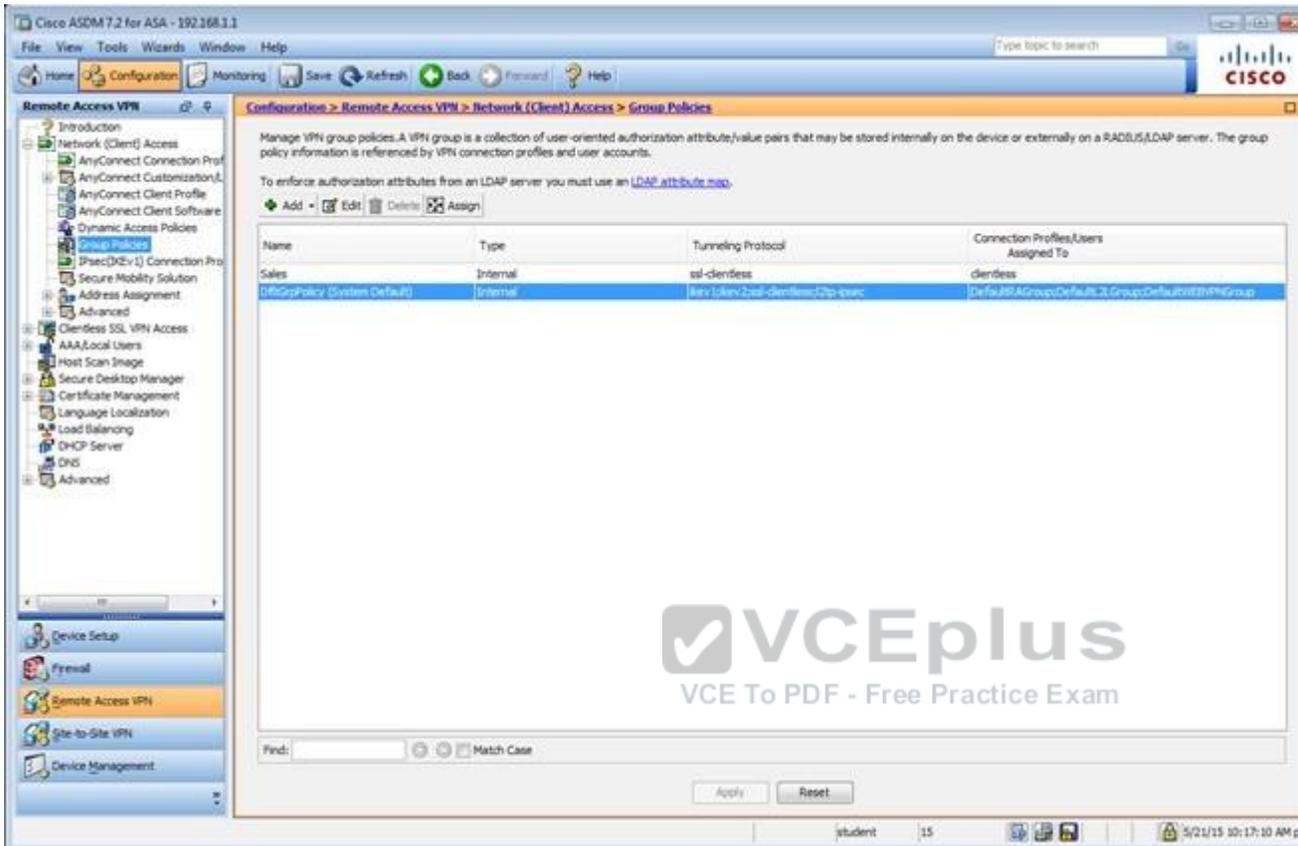
Navigation Pane:

- Introduction
- Network (Client) Access
- AnyConnect Connection Profile
- AnyConnect Customization List
- AnyConnect Client Profile
- AnyConnect Client Software
- Dynamic Access Policies
- Group Policies
- IPsec(DKv1) Connection Profile
- IPsec(DKv2) Connection Profile
- 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

Bottom Bar:

- Device Setup
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- Device Management

student | 15 | 5/28/15 8:55:47 AM pet



Cisco ASDM 7.2 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

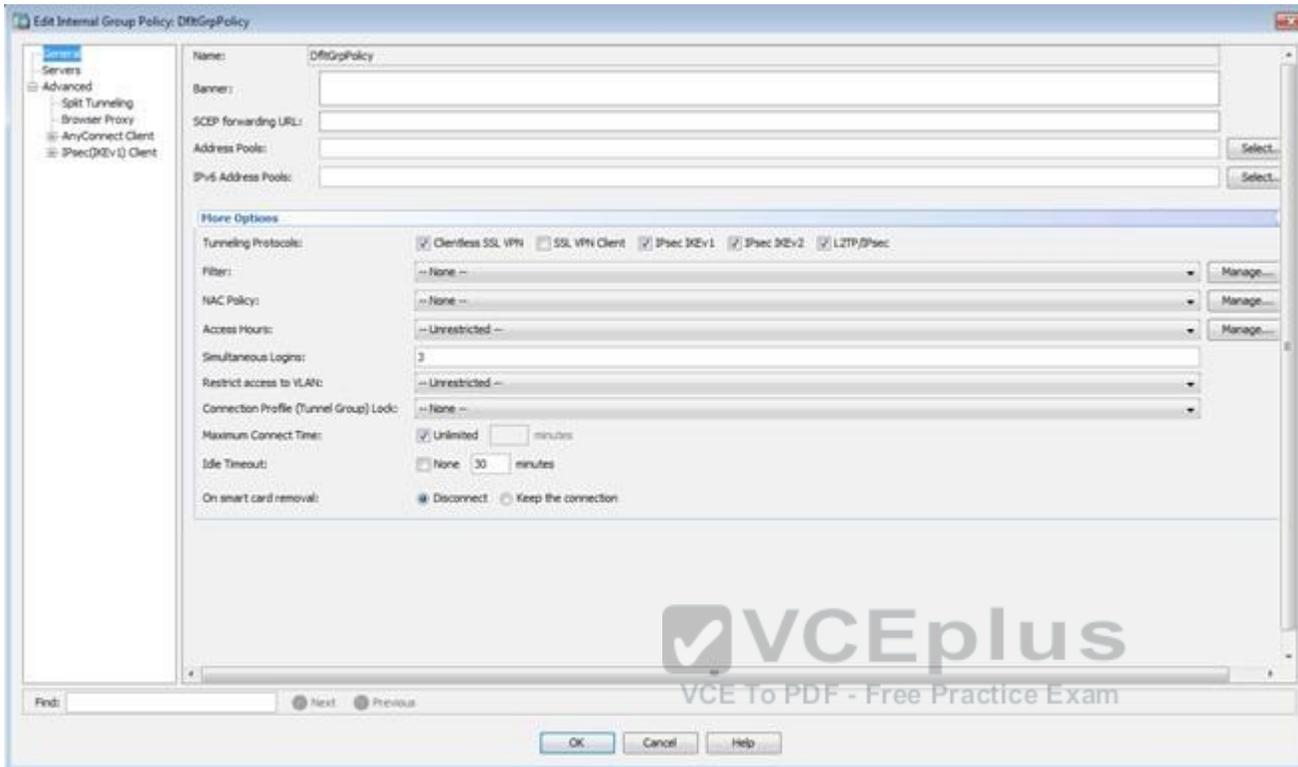
Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DRGpPolicy (System Default)	Internal	[rev:1.0]ssl-clientless/2ip-espac	DefaultAGroup/Default3LGroup/DefaultWEBPhGroup

Find: Match Case

Apply Reset

ytudent 15 5/21/15 10:17:10 AM pet



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window is titled "Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles". The left sidebar shows a tree view with "Remote Access VPN" selected. The main content area is divided into two sections: "Access Interfaces" and "Connection Profiles".

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input 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.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
DefaultE2EVPNGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
Default	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL	Local

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:56:47 AM pst

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

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input checked="" 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 can configure the mapping from certificate to connection profile [here](#).

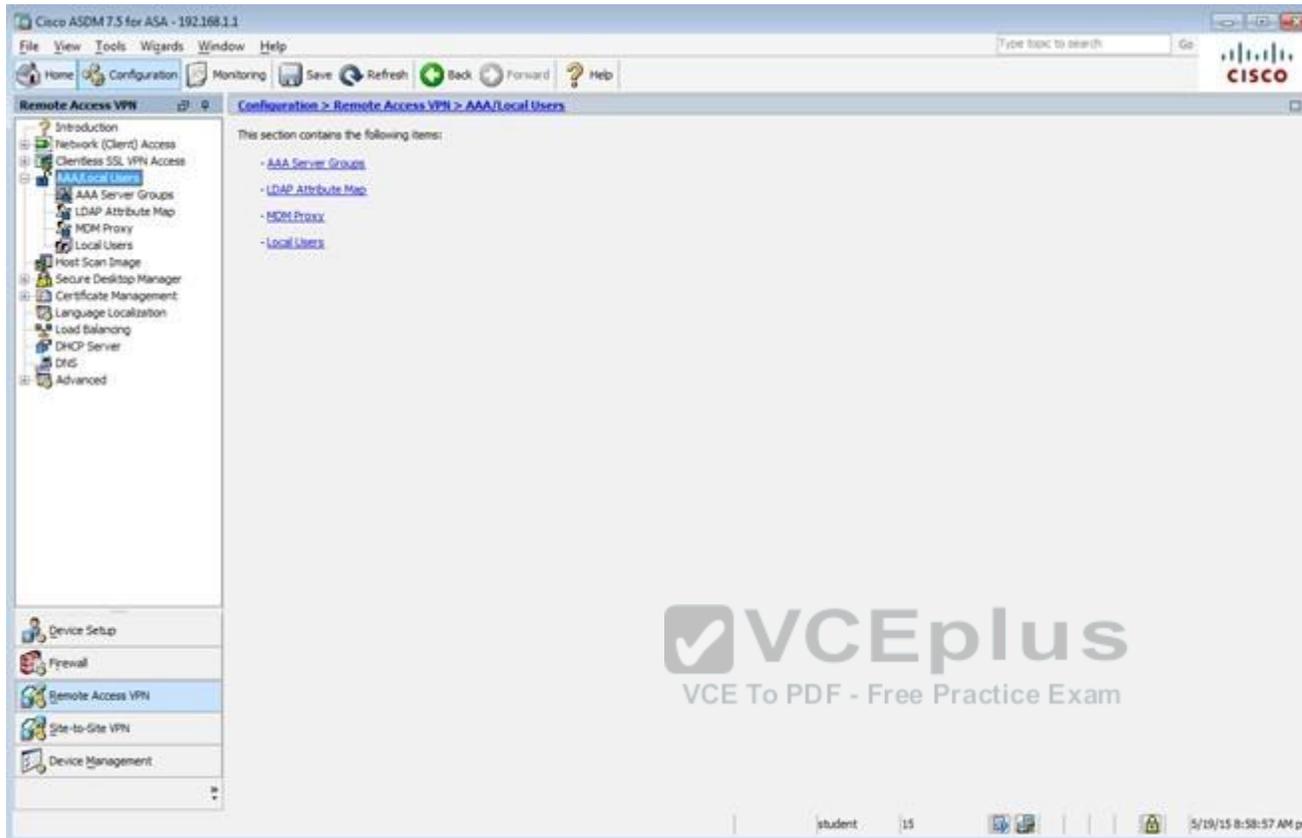
End:

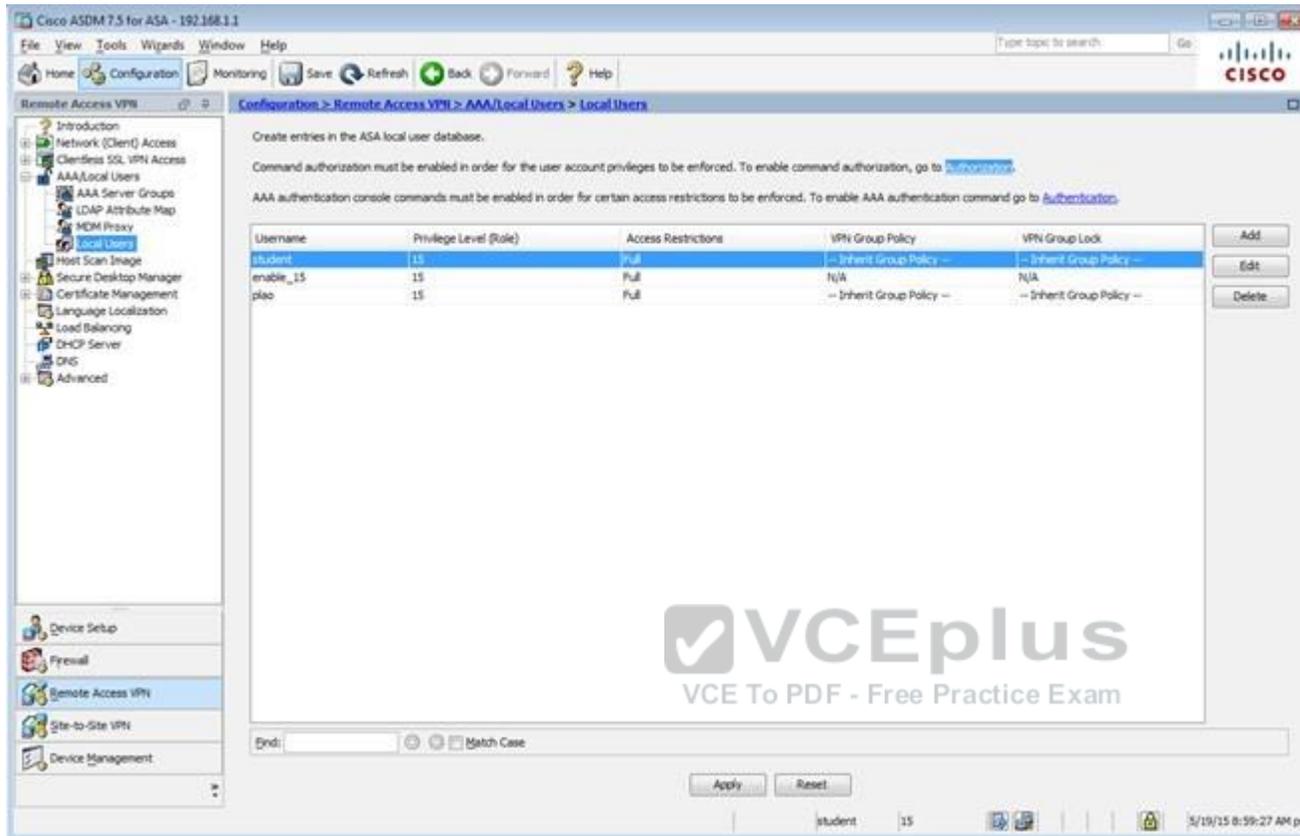
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
certless	<input checked="" type="checkbox"/>	<input type="checkbox"/>	yes	SSL(OCSP)	certless

Let group URLs take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Apply Reset

student 15 5/19/15 8:58:17 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

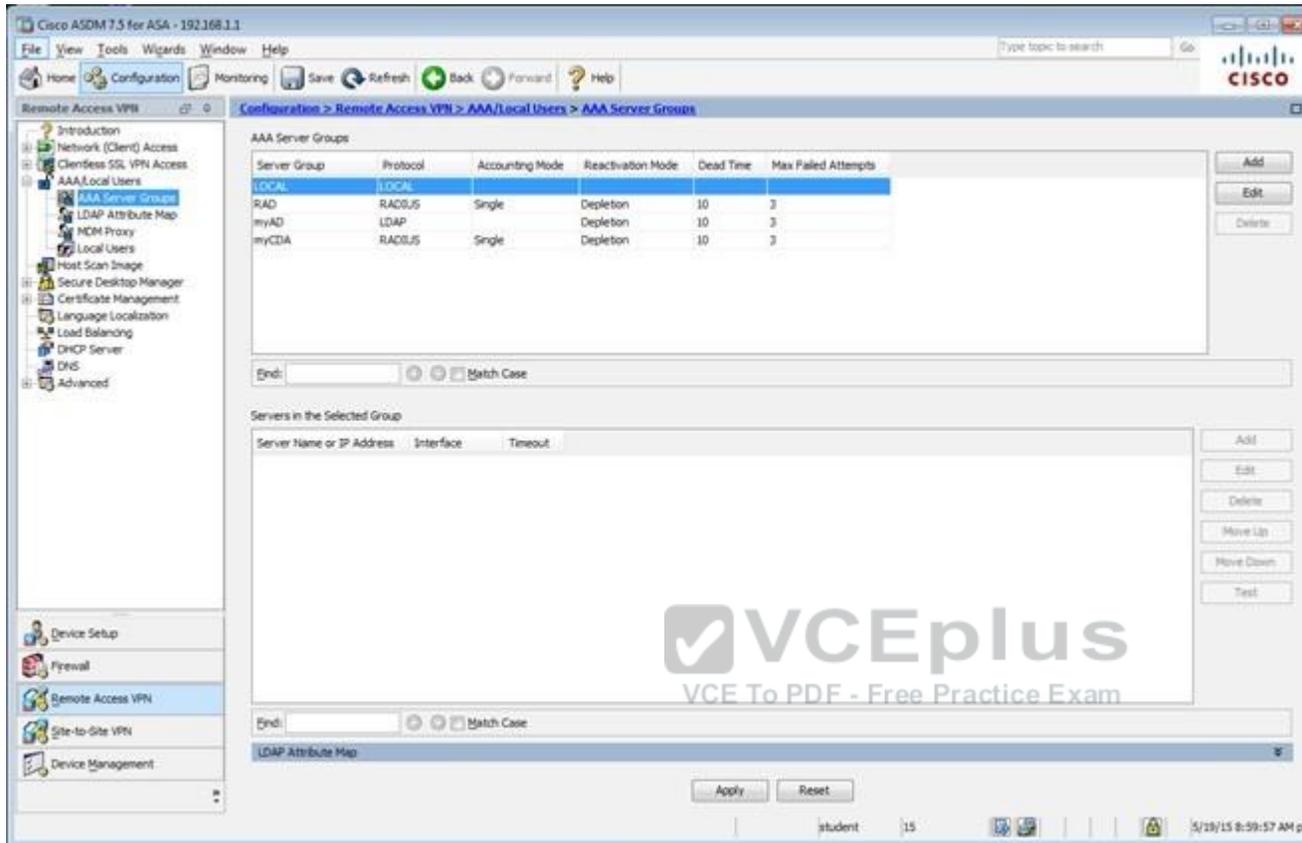
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

Apply Reset

student 15 5/19/15 8:59:27 AM pet



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: (none)

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,

The screenshot shows the VCEplus Virtual Terminal interface. The main window is titled "Remote Access VPN" and is currently on the "Connection Profiles" tab. The left sidebar shows a tree view of the configuration hierarchy, with "Connection Profiles" selected. The main content area is divided into several sections:

- Access Interfaces:** A table with columns "Interface" and "Allow Access". The "outside" interface has "Allow Access" checked. Below the table is a checkbox for "Bypass interface access lists for inbound VPN sessions" which is checked. A note states: "Access lists from group policy and user policy always apply to the traffic." There are buttons for "Device Certificate ..." and "Port Setting ...".
- Login Page Setting:** Contains three checkboxes:
 - 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:** A section with a description: "Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connect". It includes "Add", "Edit", and "Delete" buttons, a "Find:" search box, and a "Match Case" checkbox. Below is a table of connection profiles:

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

QUESTION 66

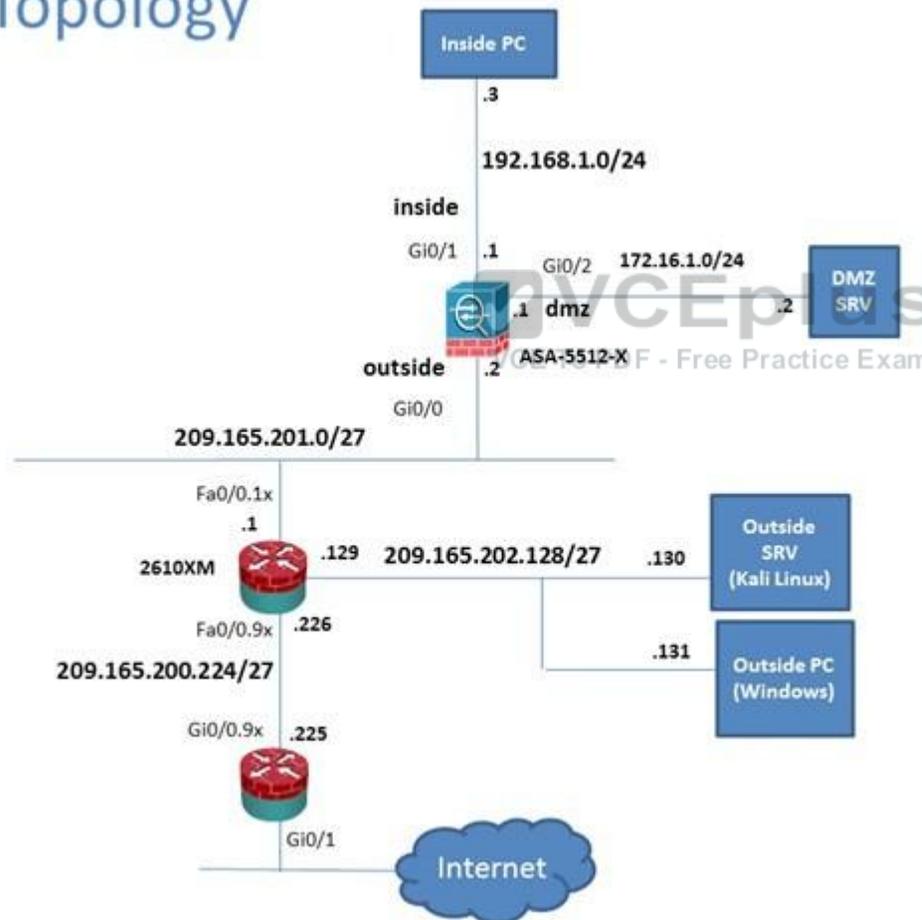
Scenario

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 un-expand the expanded menu first.

Lab Topology



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA FirePOWER Status

Device Information

General License

Host Name: **P17-ASA.secure-x.local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(1)1**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 23h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	UP	UP	0
inside	192.168.1.1/24	UP	UP	4
mgmt	10.10.10.2/24	UP	UP	0
outside	209.165.201.2/24	UP	UP	0

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

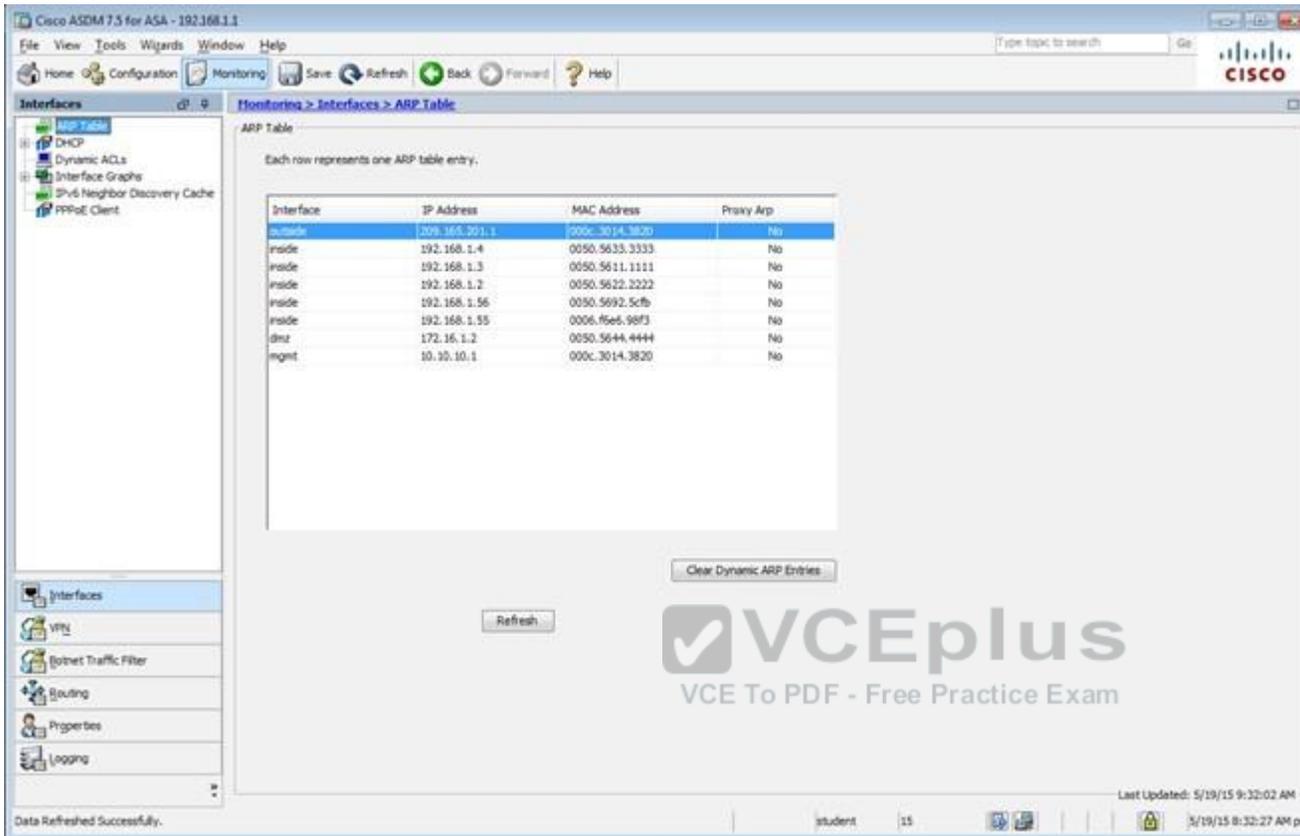
Traffic Status

Connections Per Second Usage

'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 13 2015	12:35:09	302016	10.81.254.202	123	209.165.201.2	65535	Teardown LDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6	May 13 2015	12:35:08	106015	192.168.1.3	14676	192.168.1.1	443	Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6	May 13 2015	12:35:08	302014	192.168.1.3	14676	192.168.1.1	443	Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.3014.3800	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.f5e5.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

Last Updated: 5/19/15 9:32:02 AM

student 15 5/19/15 8:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/ISAK Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- NM Proxy Statistics
- NM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Interfaces

VPN

Internet Traffic Filter

Routing

Properties

Logging

Type Active Cumulative Peak Concurrent Inactive

Clientless VPN		1	1	1
Browser		1	1	1

Filter By: Clientless SSL VPN -- All Sessions -- Filter

Username	IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx	Bytes Rx
student	209.165.202.131	Sales	Clientless	08:03:46 pm Thu May 21 2015	316774	41833

Details

Logout

Ping

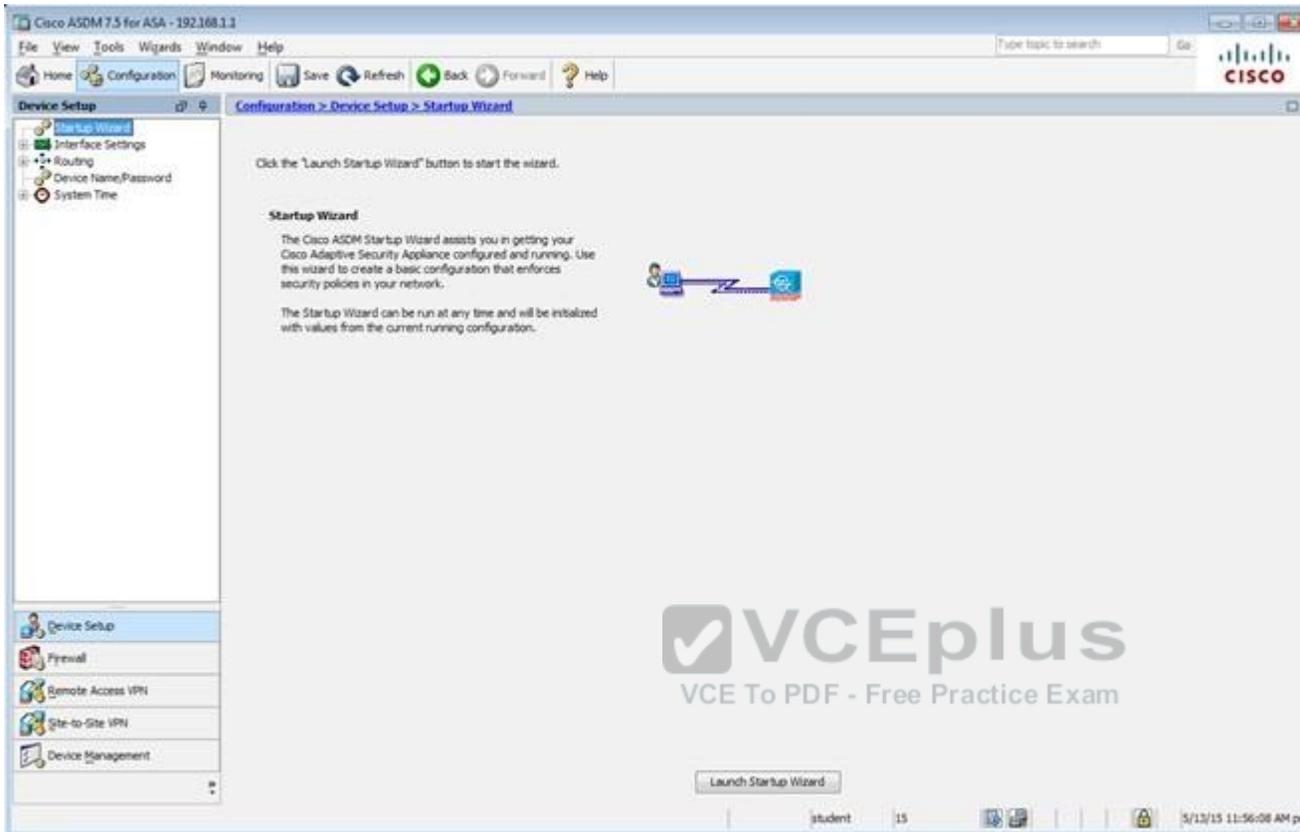
Refresh

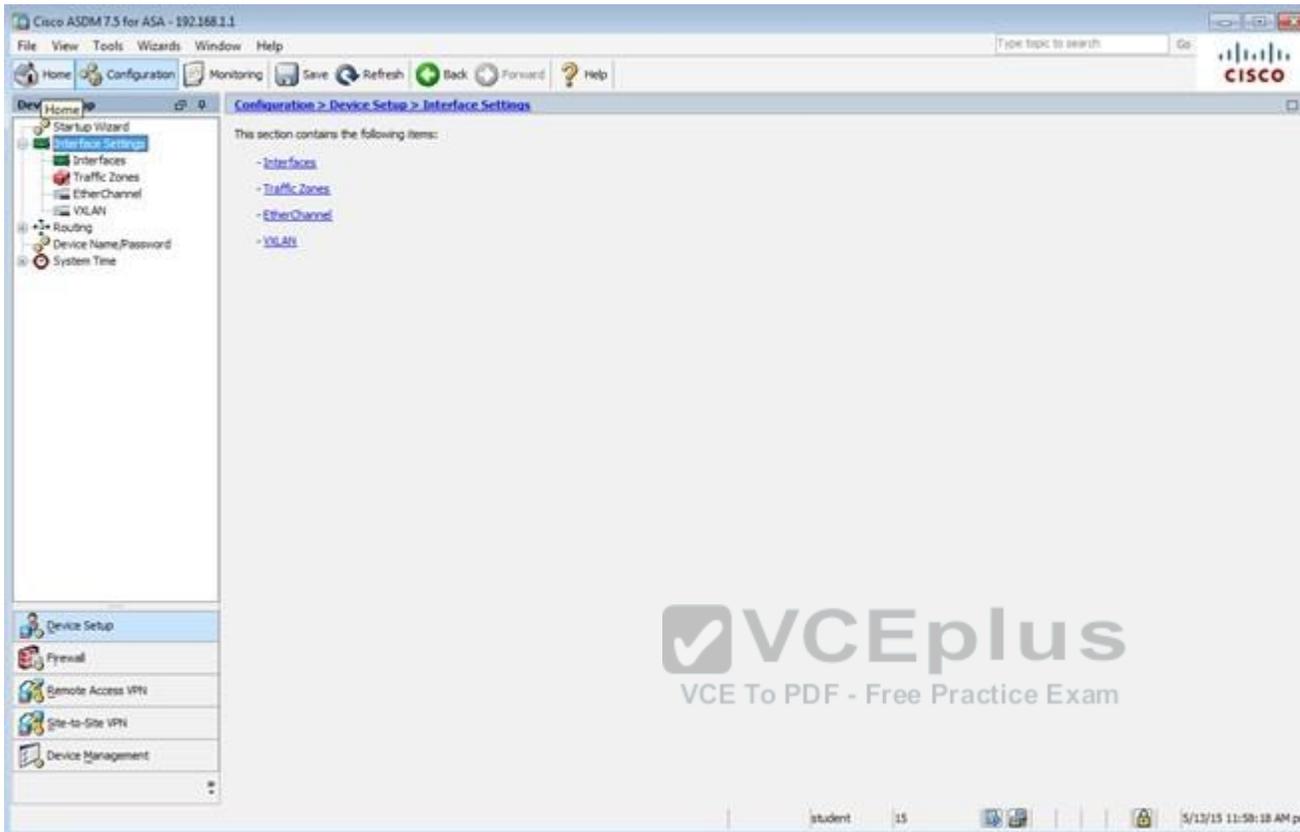
Last Updated: 5/19/15 9:33:12 AM

Data Refreshed Successfully.

student 15

5/19/15 8:33:37 AM pst





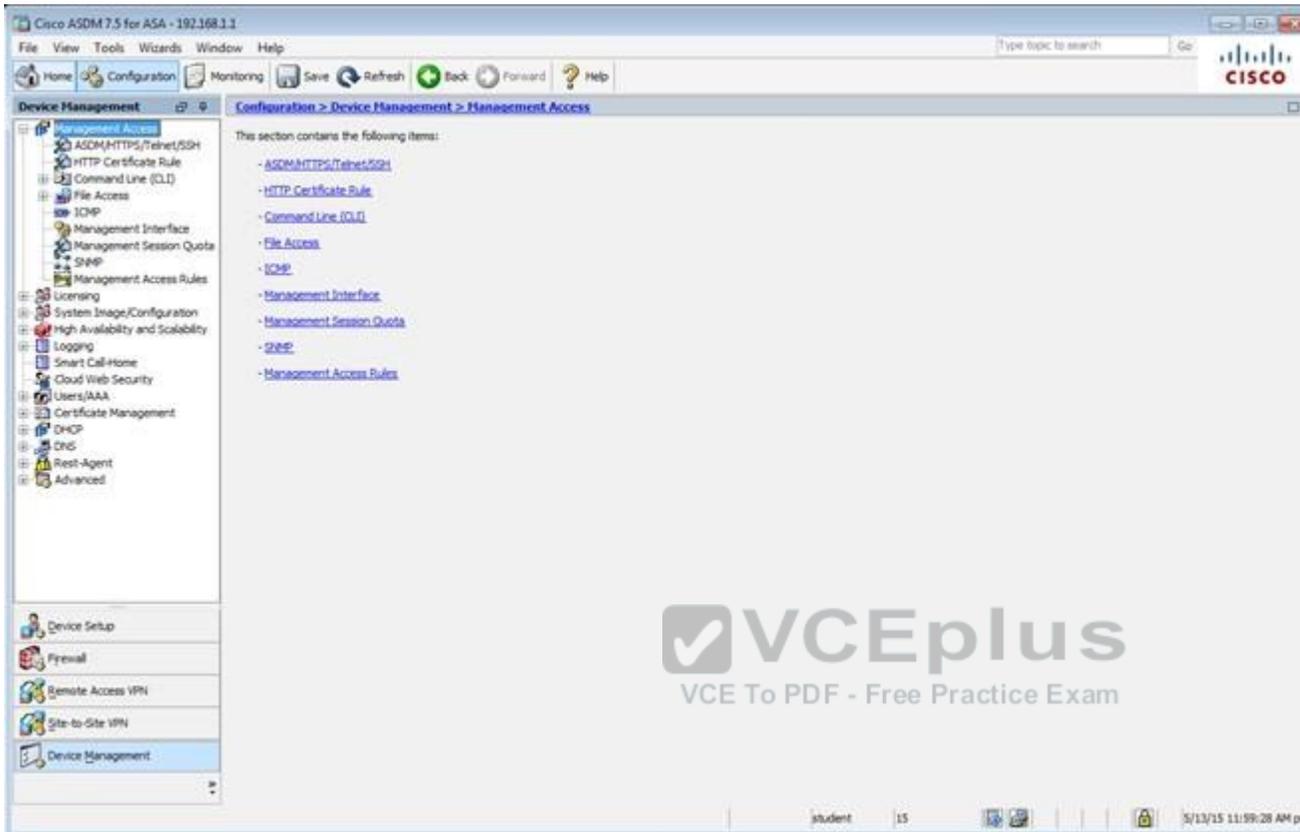
The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for the 'Interfaces' section. A table lists the configured interfaces with their respective settings.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled	0	209.165.201.2	255.255.255.0		Hardware
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1	255.255.255.0		Hardware
GigabitEthernet0/2	dmz			Enabled	172	16.1.1	255.255.255.0		Hardware
GigabitEthernet0/3				Enabled					Hardware
GigabitEthernet0/4				Enabled					Hardware
GigabitEthernet0/5	mgmt			Enabled	100	10.10.10.2	255.255.255.0		Hardware
Management0/0				Enabled					Hardware

Below the table, there are three checkboxes for advanced settings:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface
- Enable jumbo frame reservation

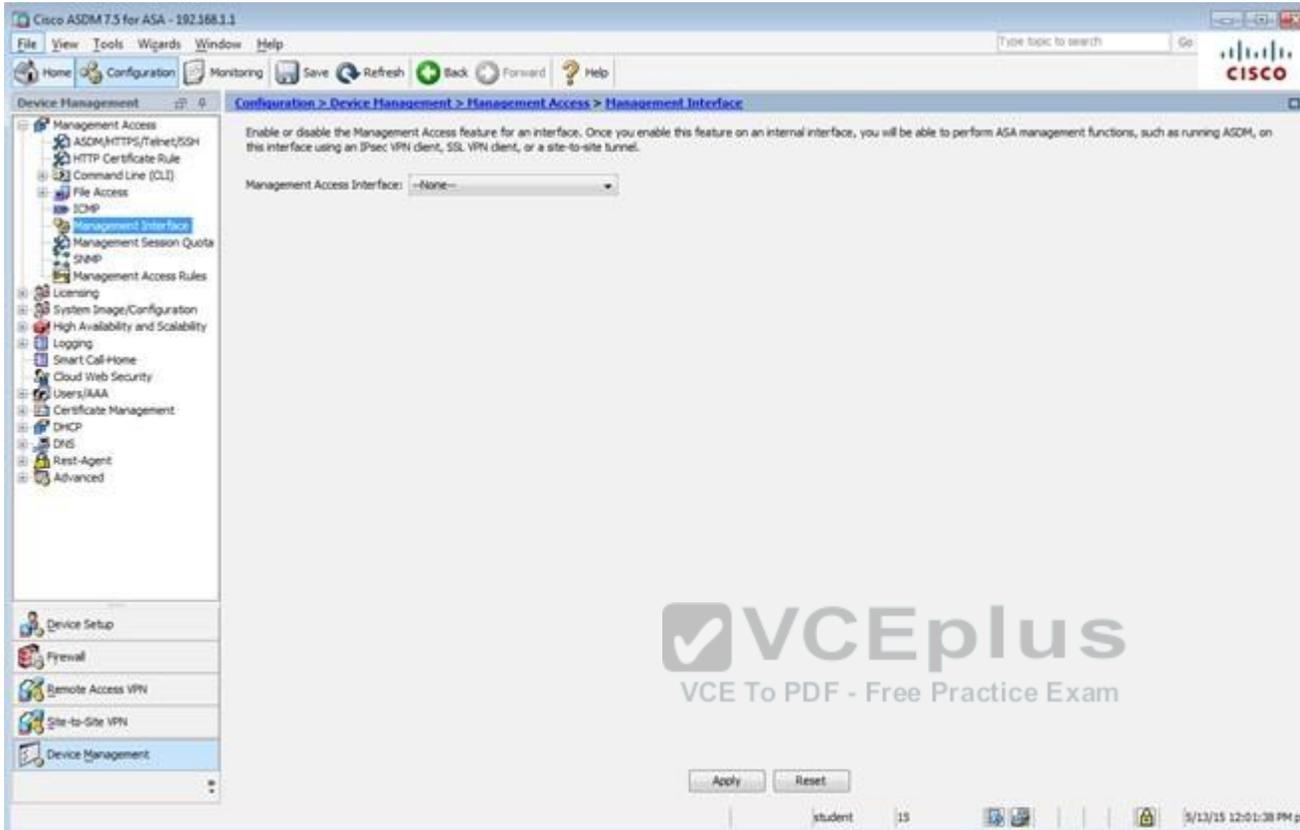
The interface also includes 'Apply' and 'Reset' buttons at the bottom.

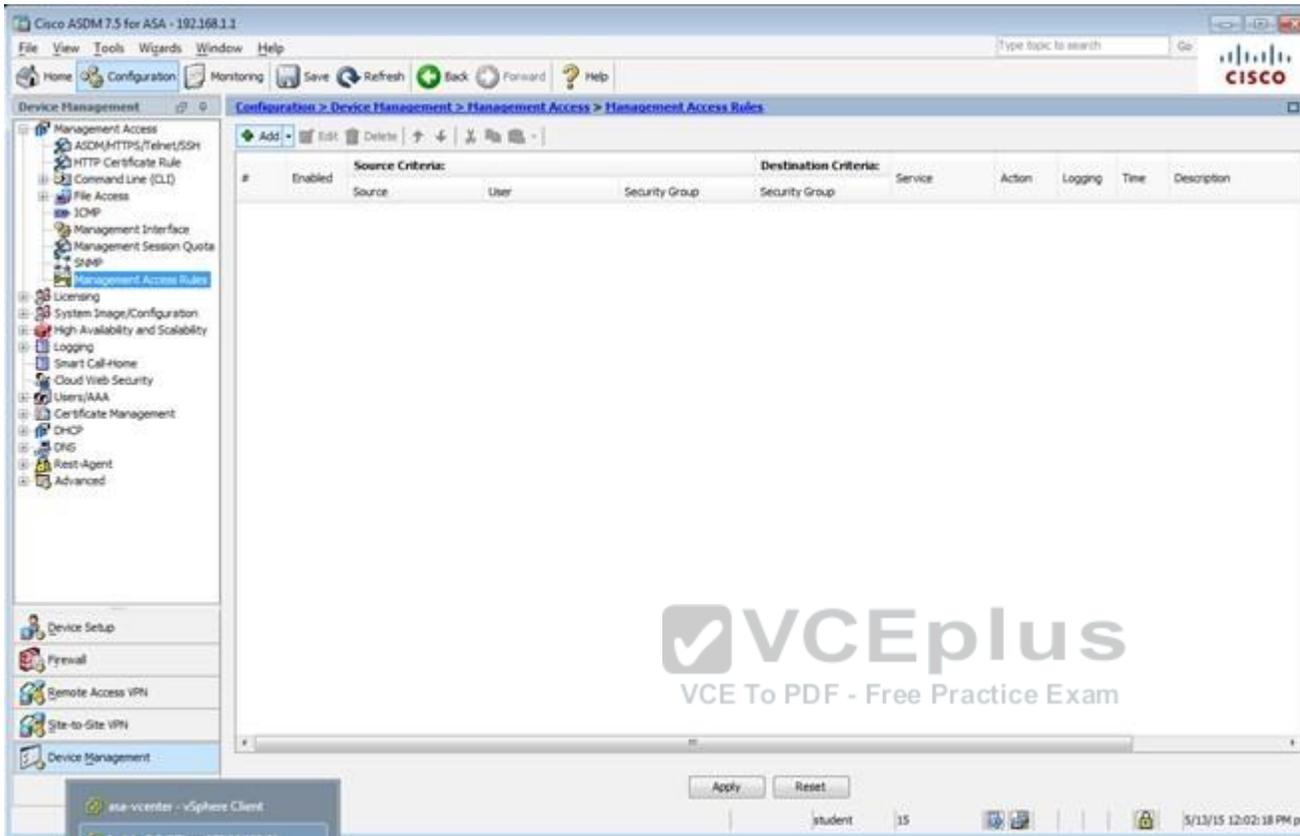


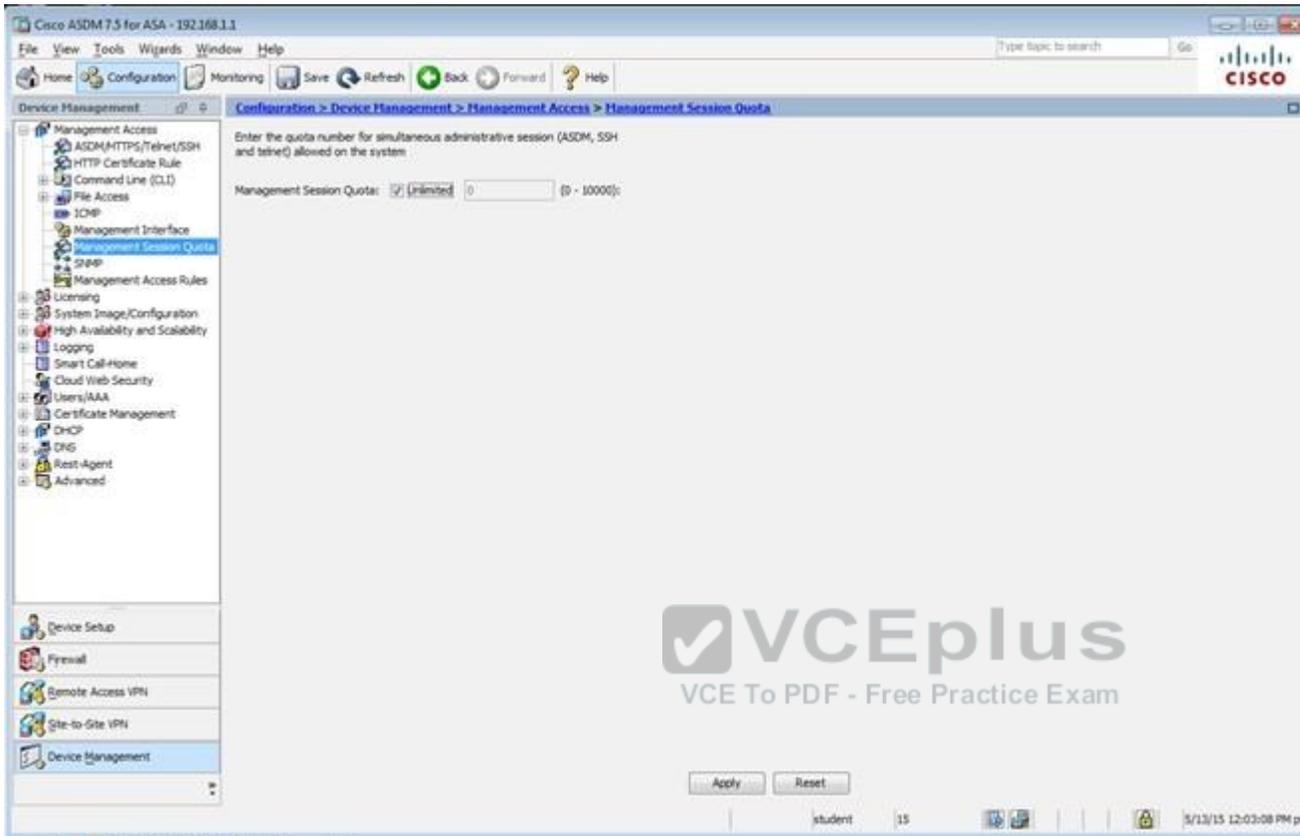
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation is "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows a tree view of configuration categories, with "Management Access" selected. The main content area is titled "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." and contains a table with the following data:

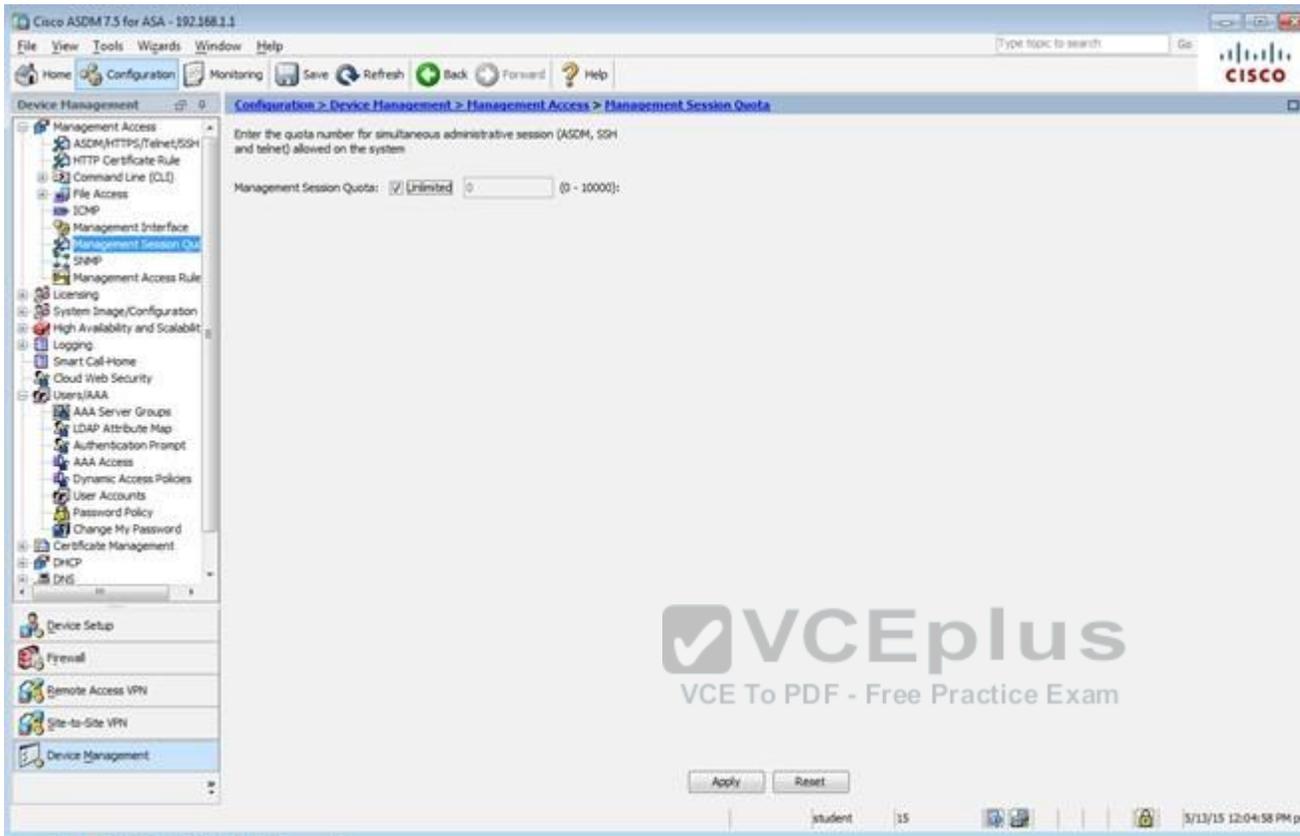
Type	Interface	IP Address	Mask/Prefix Length
Telnet	mgmt	10.10.10.1	255.255.255.255
SSH	inside	192.168.1.2	255.255.255.255
ASDM/HTTPS	inside	192.168.1.0	255.255.255.0

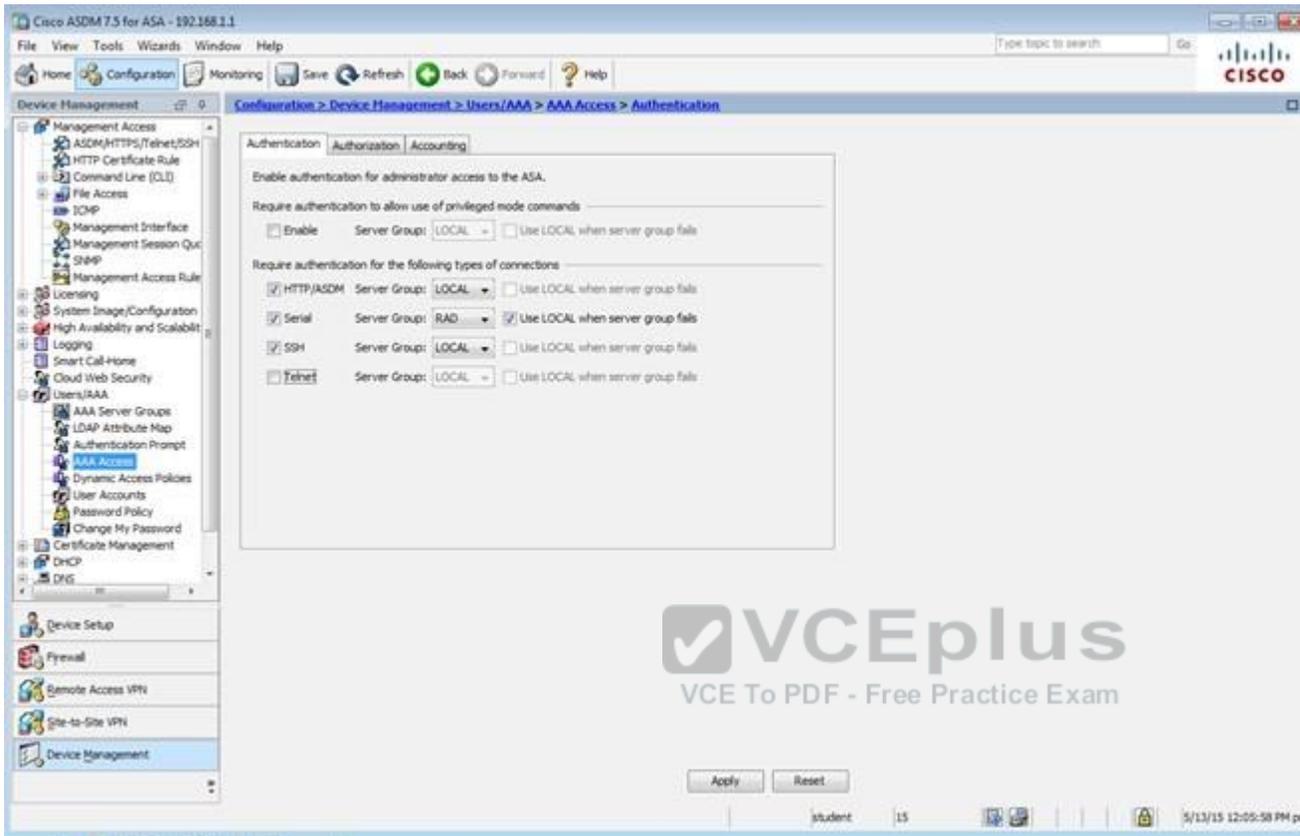
Below the table are "Add", "Edit", and "Delete" buttons. Further down, there are sections for "Http Settings" (with "Enable HTTP Server" checked, Port Number: 443, Idle Timeout: 20 minutes, and a "Require client certificate" section), "Telnet Settings" (Telnet Timeout: 5 minutes), and "SSH Settings" (Allowed SSH Version(s): 1&2, SSH Timeout: 5 minutes, and DH Key Exchange: Group 1 selected). "Apply" and "Reset" buttons are at the bottom. A watermark "VCEplus VCE To PDF - Free Practice Exam" is overlaid on the right side of the interface.











The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > Users/AAA > AAA Access > Authentication. The left sidebar shows a tree view with 'Users/AAA' expanded to 'AAA Access'. The main content area has three tabs: Authentication, Authorization, and Accounting. The 'Authentication' tab is active, showing options to enable authentication for administrator access and for various connection types. The 'Require authentication for the following types of connections' section is expanded, showing checkboxes for HTTP/ASDM, Serial, SSH, and Telnet, each with a 'Server Group' dropdown menu and a 'Use LOCAL when server group fails' checkbox. The 'Apply' and 'Reset' buttons are at the bottom. A watermark for VCEplus is visible in the center of the screenshot.

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

Enable Server Group: LOCAL Use LOCAL when server group fails

Require authentication for the following types of connections

HTTP/ASDM Server Group: LOCAL Use LOCAL when server group fails

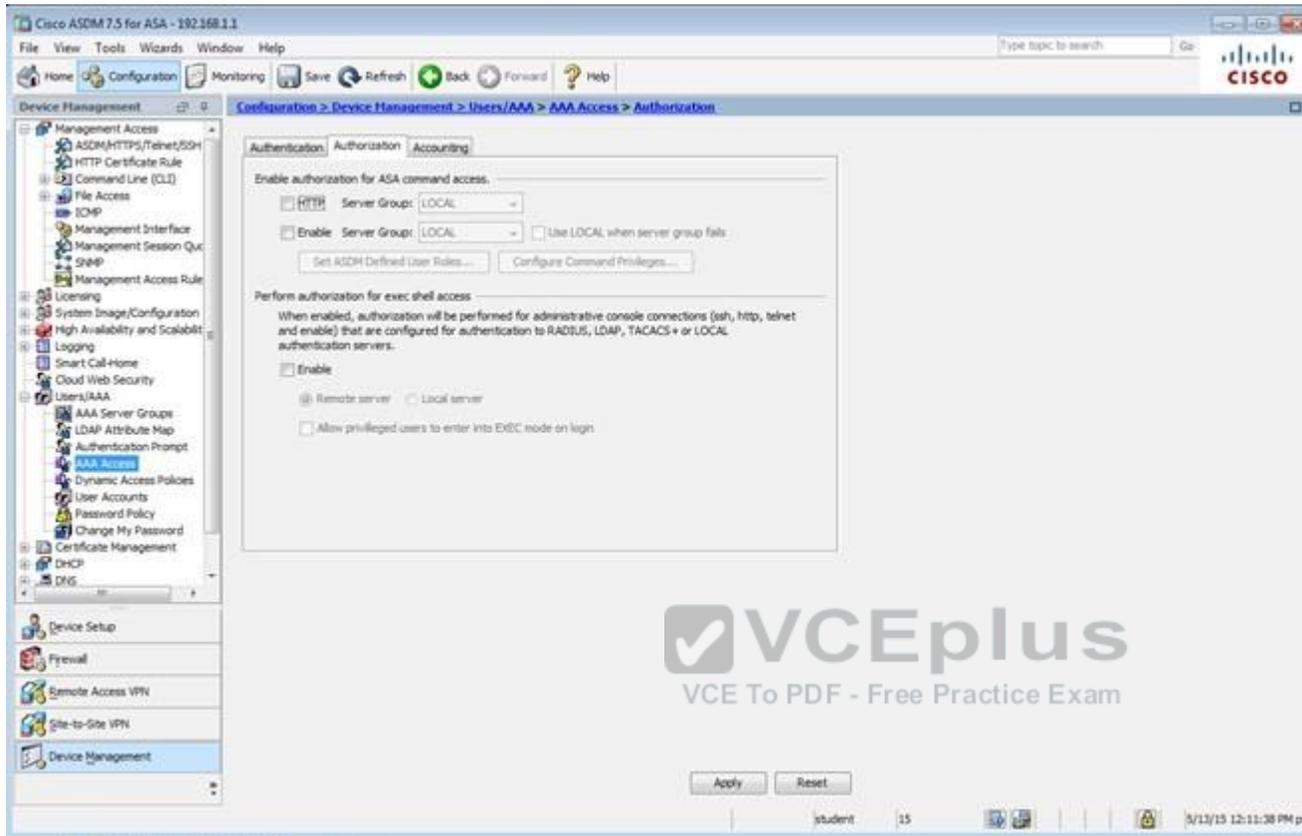
Serial Server Group: RAD Use LOCAL when server group fails

SSH Server Group: LOCAL Use LOCAL when server group fails

Telnet Server Group: LOCAL Use LOCAL when server group fails

Apply Reset

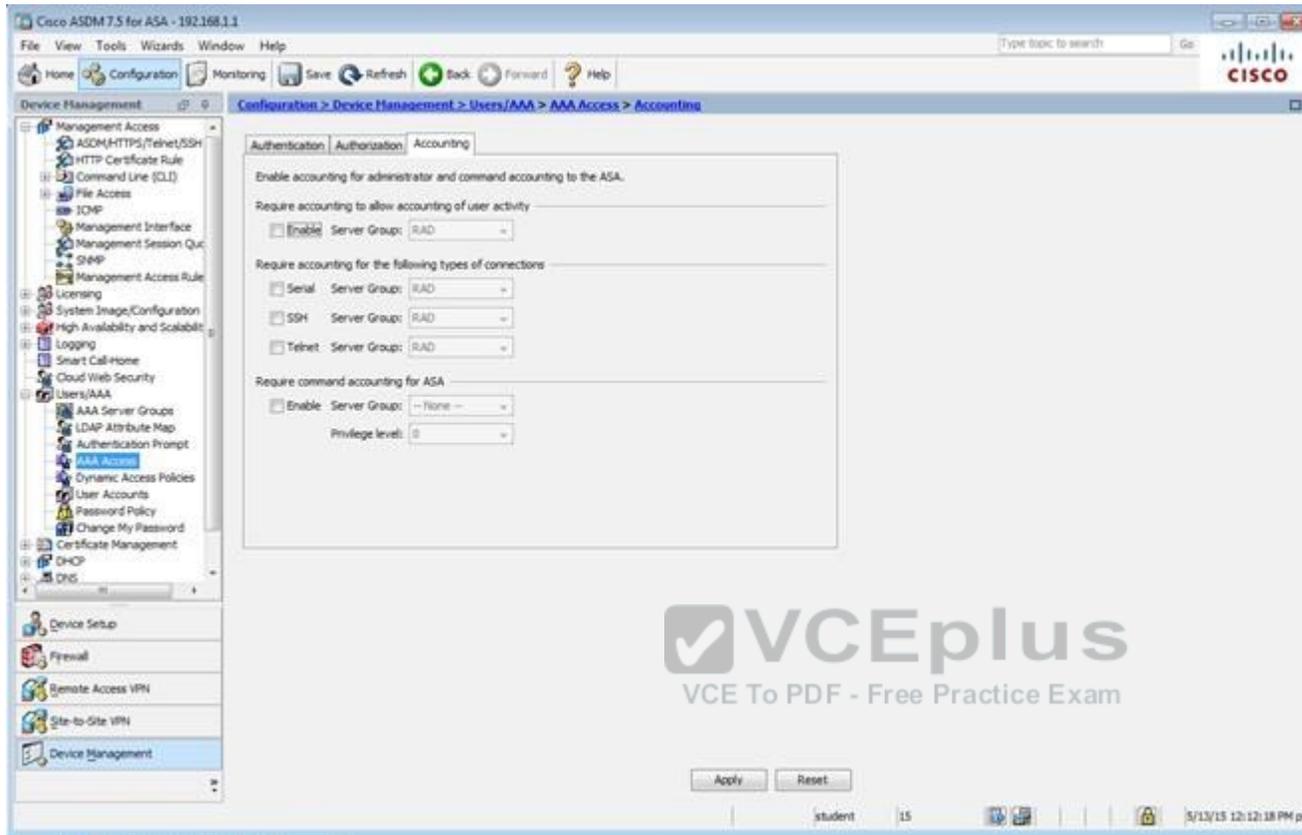
student 15 5/13/15 12:05:58 PM pst



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The title bar reads "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation is "Configuration > Device Management > Users/AAA > AAA Access > Authorization". The left sidebar shows a tree view with "Users/AAA" expanded to "AAA Access". The main content area has three tabs: "Authentication", "Authorization", and "Accounting", with "Authorization" selected. The "Authorization" tab contains the following configuration options:

- Enable authorization for ASA command access:**
 - HTTP Server Group: LOCAL
 - Enable Server Group: LOCAL Use LOCAL when server group fails
 - Buttons: Set ASDM Defined User Roles... Configure Command Privileges...
- Perform authorization for exec shell access:**
 - When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.
 - Enable
 - Remote server Local server
 - Allow privileged users to enter into EXEC mode on login

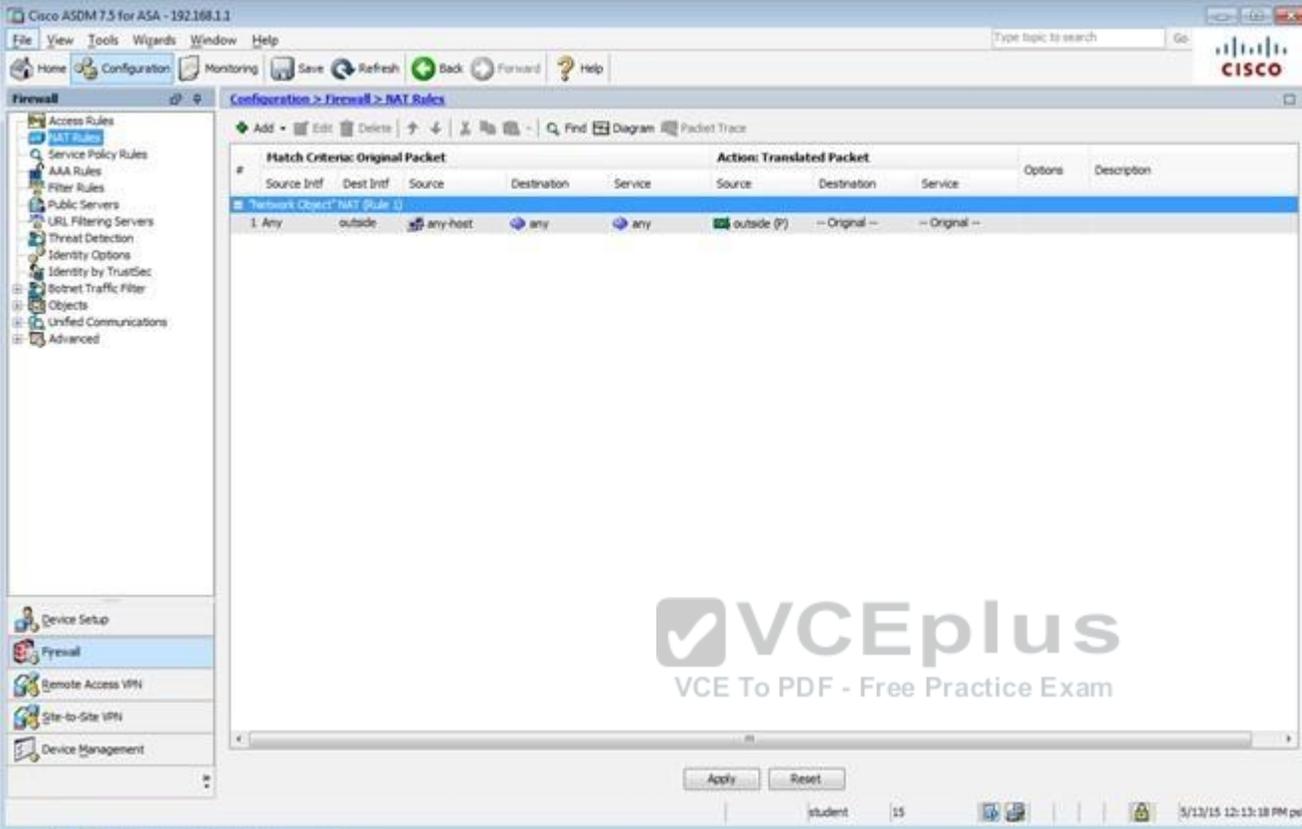
At the bottom of the configuration area are "Apply" and "Reset" buttons. The system tray at the bottom shows the user "student", the page number "15", and the date/time "5/13/15 12:11:38 PM pet".



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The browser title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb path is "Configuration > Device Management > Users/AAA > AAA Access > Accounting". The left sidebar shows a tree view with "Users/AAA" expanded to "AAA Access". The main content area has three tabs: "Authentication", "Authorization", and "Accounting", with "Accounting" selected. The "Accounting" tab contains the following configuration options:

- Enable accounting for administrator and command accounting to the ASA. (checked)
- Require accounting to allow accounting of user activity:
 - Enable Server Group: RAD
- Require accounting for the following types of connections:
 - Serial Server Group: RAD
 - SSH Server Group: RAD
 - Telnet Server Group: RAD
- Require command accounting for ASA:
 - Enable Server Group: -- None --
 - Privilege level: 0

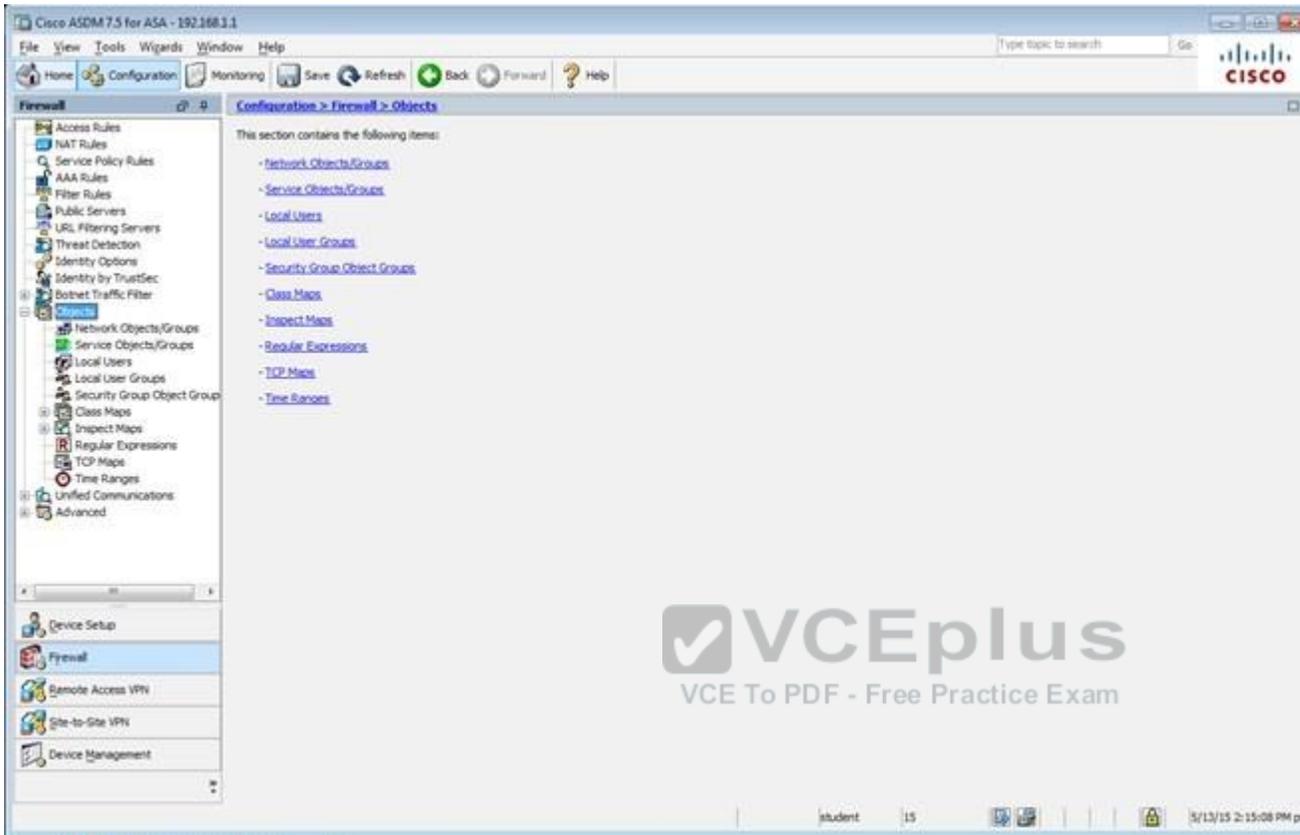
At the bottom of the configuration area are "Apply" and "Reset" buttons. The status bar at the very bottom shows "student | 15 | 5/13/15 12:12:18 PM pdt".

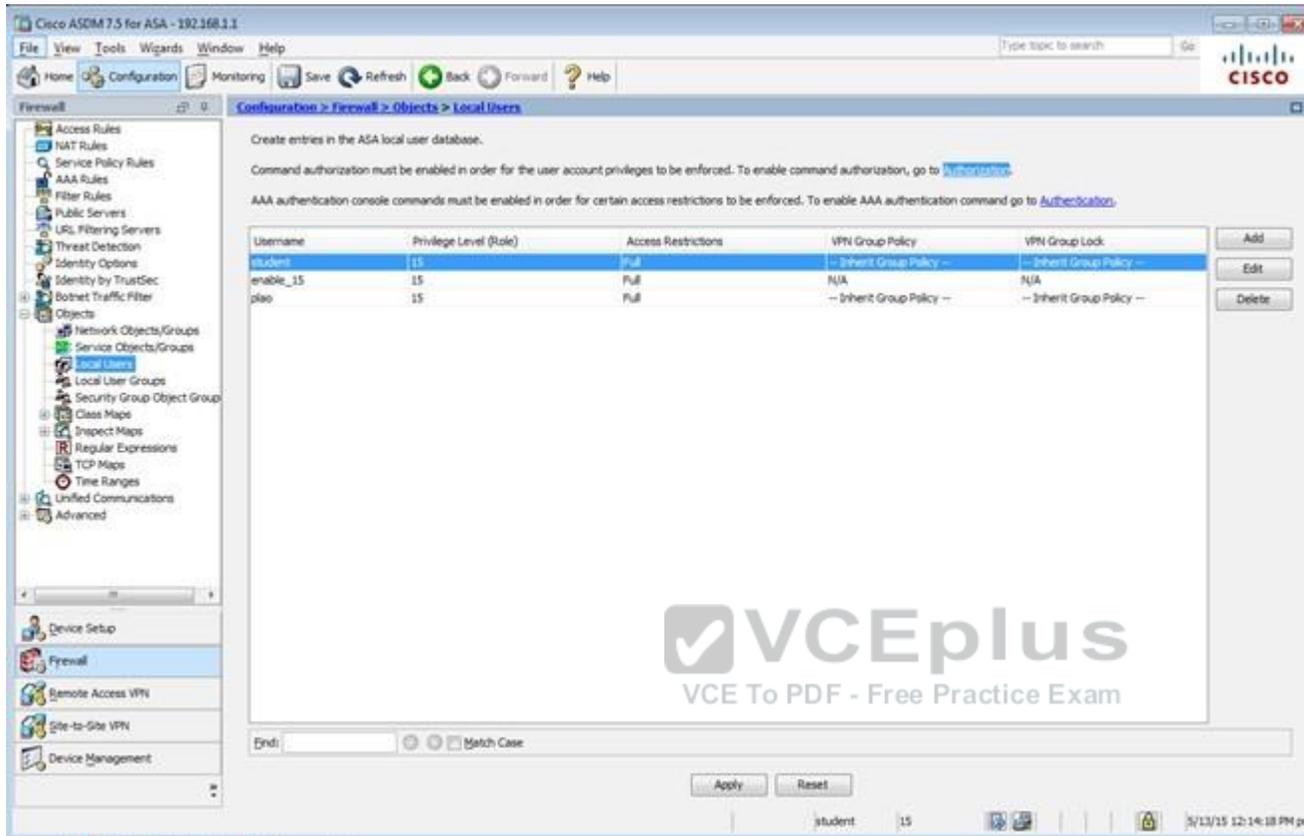


The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for NAT Rules. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table with columns for Match Criteria and Action. The table contains one rule with the following details:

Match Criteria: Original Packet				Action: Translated Packet				Options	Description
Source Intf	Dest Intf	Source	Destination	Source	Destination	Service			
1. Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		

At the bottom of the window, there are 'Apply' and 'Reset' buttons. The status bar at the bottom indicates the user is 'student' and the time is '5/13/15 12:13:18 PM pet'.





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End:

student 15 5/13/15 12:14:18 PM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Network Objects/Groups

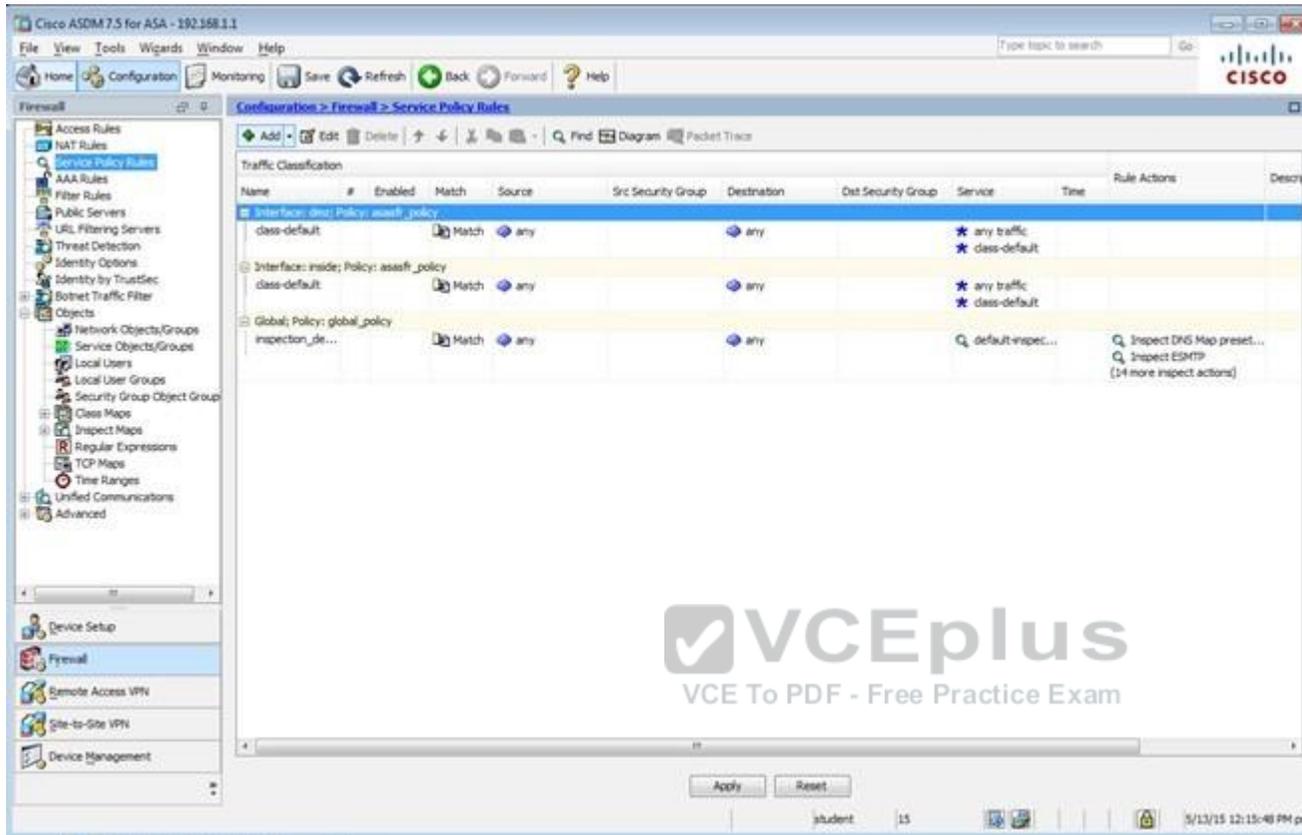
Filter: [Clear]

Name	IP Address	Netmask	Description	Object NAT Address
any				
any-host	0.0.0.0	0.0.0.0		outside (F)
any4				
any6				
facebook	www.facebook.com			
My_ASA_Demo_Obj	1.10.8.20			

Apply Reset

student 15 5/13/15 12:30:08 PM pet

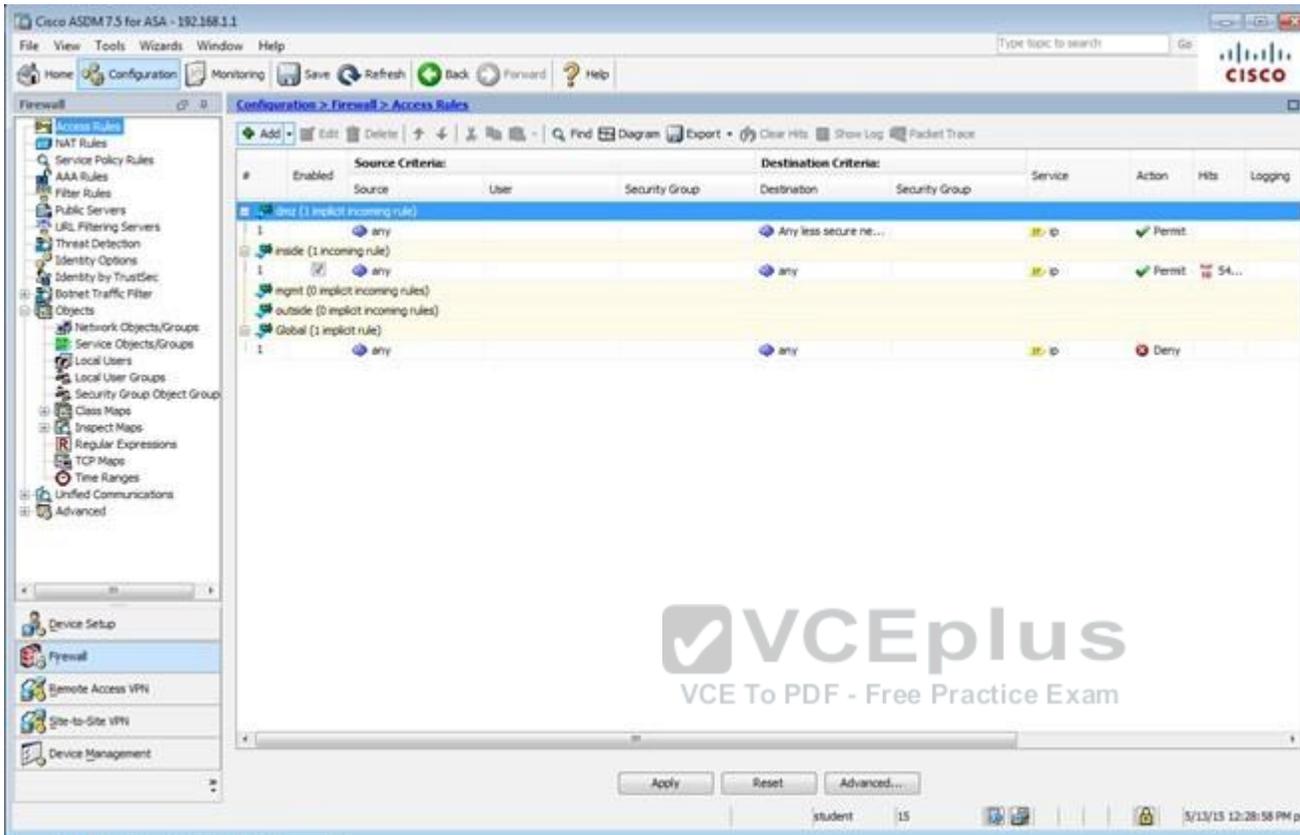
VCEplus
VCE To PDF - Free Practice Exam



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left-hand navigation pane shows a tree structure with "Service Policy Rules" selected. The main area contains a table of traffic classification rules. The table has columns for Name, #, Enabled, Match, Source, Src Security Group, Destination, Dst Security Group, Service, Time, Rule Actions, and Description. The rules listed are:

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Interface: (int); Policy: asastf_policy											
class-default			Match	any		any		any traffic			
								class-default			
Interface: inside; Policy: asaastf_policy											
class-default			Match	any		any		any traffic			
								class-default			
Global; Policy: global_policy											
inspection_de...			Match	any		any		default-inspec...		Inspect DNS Map preset...	Inspect ESMTP (14 more inspect actions)

The bottom status bar shows "student | 15 | 5/13/15 12:15:48 PM pst".



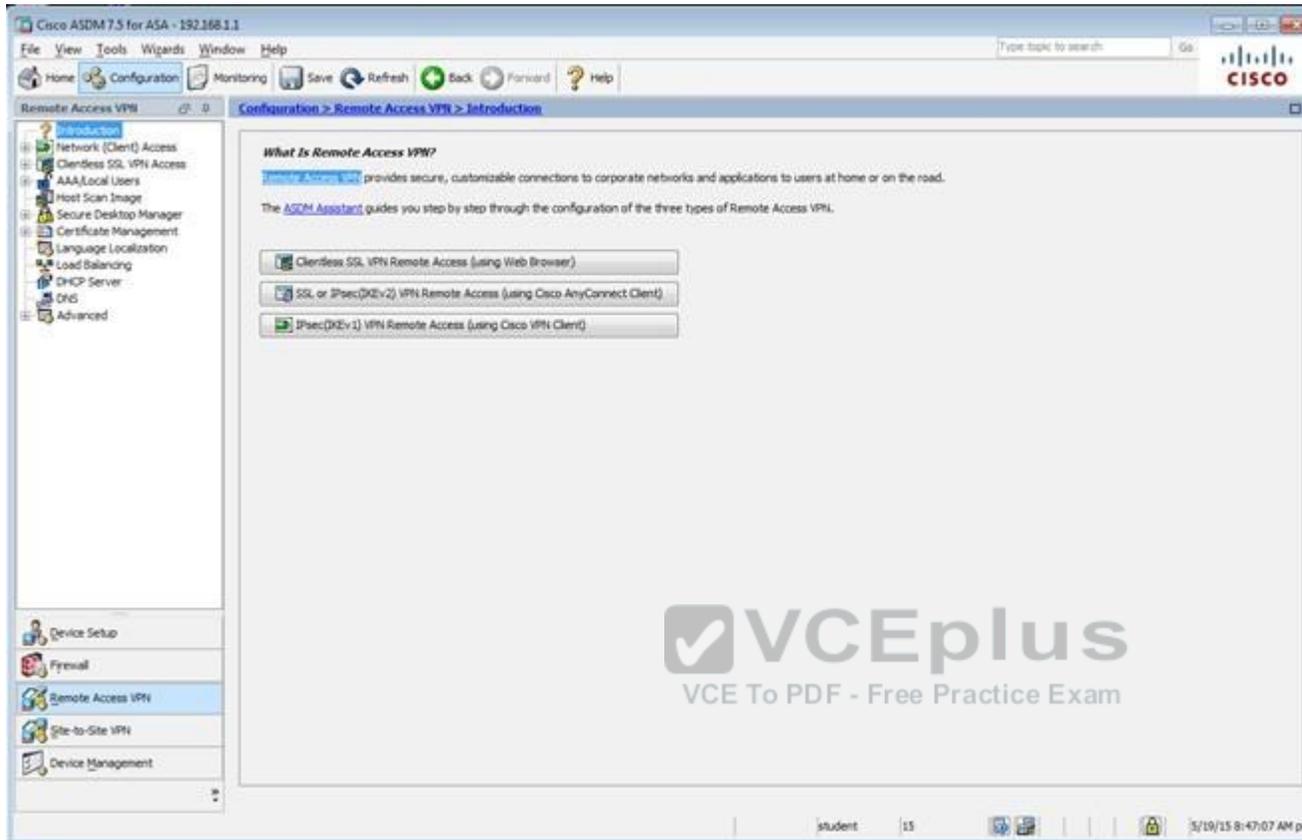
Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

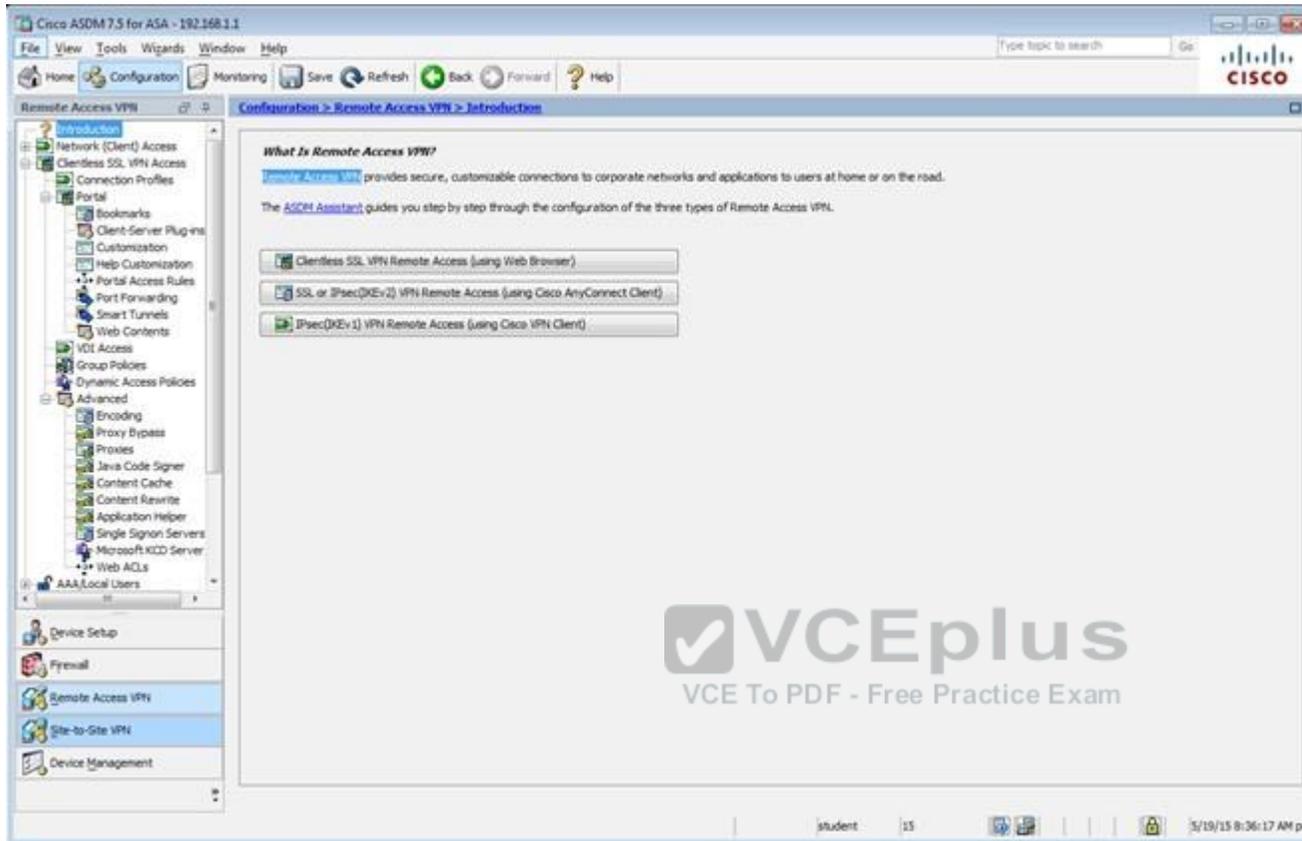
#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group				
ibzz (1 implicit incoming rule)										
1		any			Any less secure ne...		IP	Permit		
inside (1 incoming rule)										
1		any			any		IP	Permit	54...	
ingnt (0 implicit incoming rules)										
outside (0 implicit incoming rules)										
Global (1 implicit rule)										
1		any			any		IP	Deny		

Apply Reset Advanced...

student 15 3/13/15 12:28:58 PM pdt



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 web interface. The browser address bar shows the URL. The navigation menu on the left includes sections like Network (Client) Access, Clientless SSL VPN Access, AAA/Local Users, Host Scan Image, Secure Desktop Manager, Certificate Management, Language Localization, Load Balancing, DHCP Server, DNS, and Advanced. The main content area is titled "Configuration > Remote Access VPN > Introduction". It contains the heading "What Is Remote Access VPN?" followed by a paragraph: "Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road. The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN." Below this text are three buttons: "Clientless SSL VPN Remote Access (Using Web Browser)", "SSL or IPsec (IKEv2) VPN Remote Access (Using Cisco AnyConnect Client)", and "IPsec (IKEv1) VPN Remote Access (Using Cisco VPN Client)". A large watermark for VCEplus is overlaid on the bottom right of the interface. The status bar at the bottom shows the user is logged in as "student" and the time is 5/19/15 8:47:07 AM pet.



The screenshot shows the Cisco ASDM 7.5 for ASA interface. The breadcrumb trail is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows a tree view with 'Remote Access VPN' selected. The main content area is divided into three sections:

- Access Interfaces:** A table to enable interfaces for clientless SSL VPN access.

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

 Below the table are buttons for 'Device Certificate ...' and 'Port Setting ...'. A checkbox 'Bypass interface access lists for inbound VPN sessions' is checked. A note states: '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 can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete, Find: [text box], Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
DefaultVEBVPNGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
test	<input checked="" type="checkbox"/>	test	AAA(LOCAL)	DfltGrpPolicy

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

At the bottom are 'Apply' and 'Reset' buttons. The status bar shows 'student | 15 | 5/19/15 8:38:47 AM pet'.

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL Manage...
 Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS Manage...
(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2
Domain Name: secure-x.local

Default Group Policy

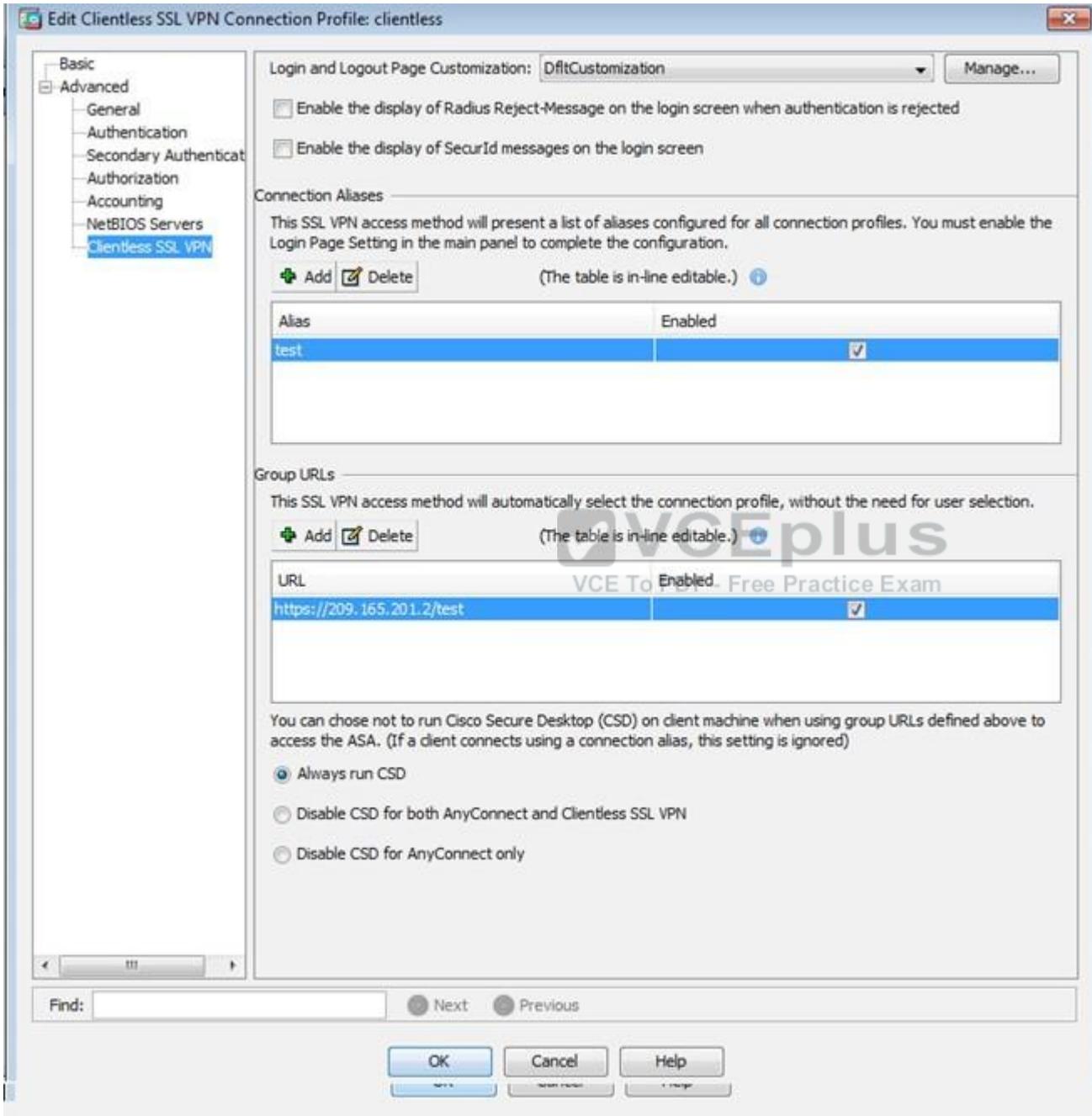
Group Policy: Sales Manage...
(Following field is an attribute of the group policy selected above.)

Enable clientless SSL VPN protocol

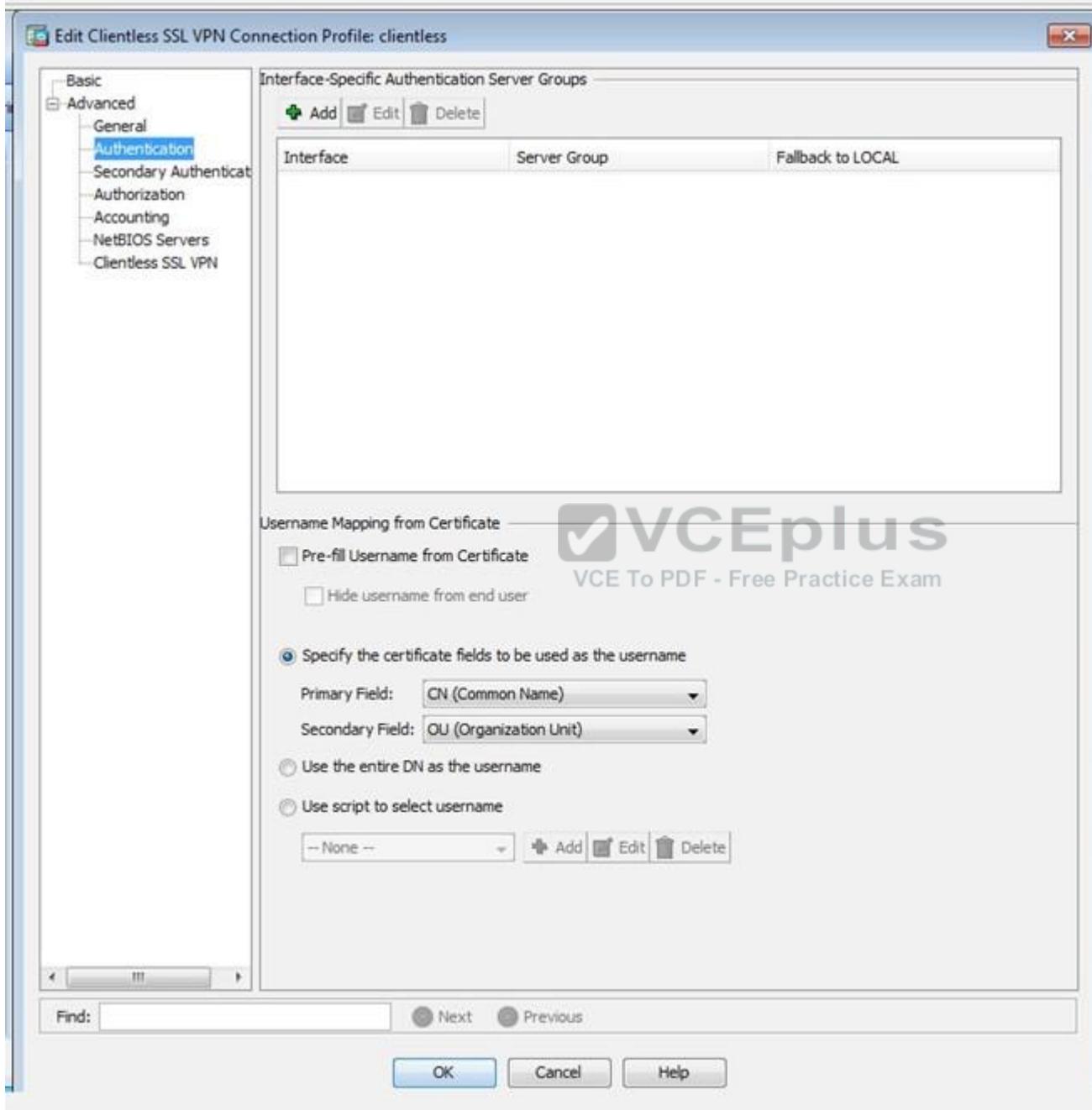
Find: Next Previous

OK Cancel Help

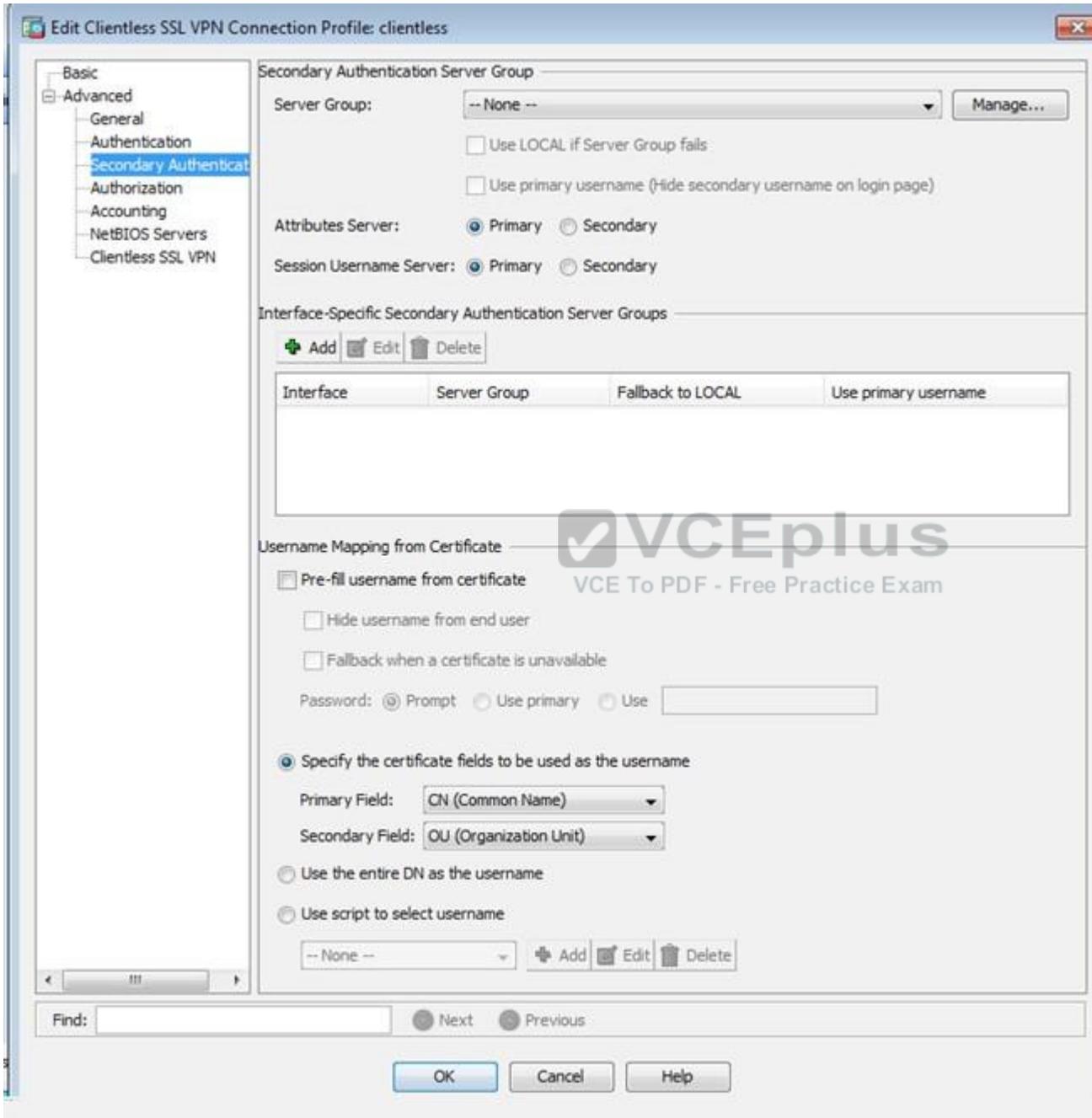


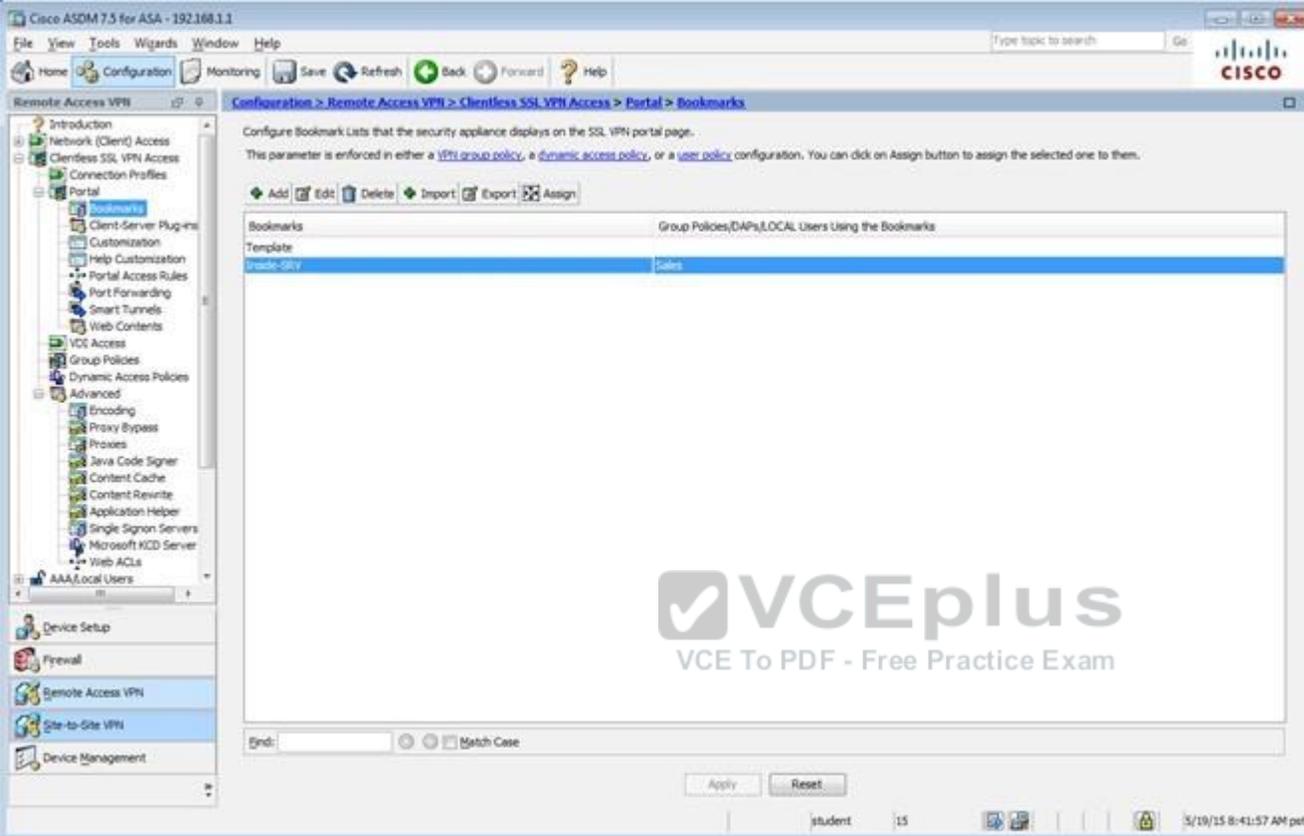












The screenshot shows the Cisco ASDM 7.5 interface for configuring the Bookmarks section of the Clientless SSL VPN Access Portal. The breadcrumb trail is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The main content area contains the following text:

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. You can click on Assign button to assign the selected one to them.

Buttons: Add, Edit, Delete, Import, Export, Assign

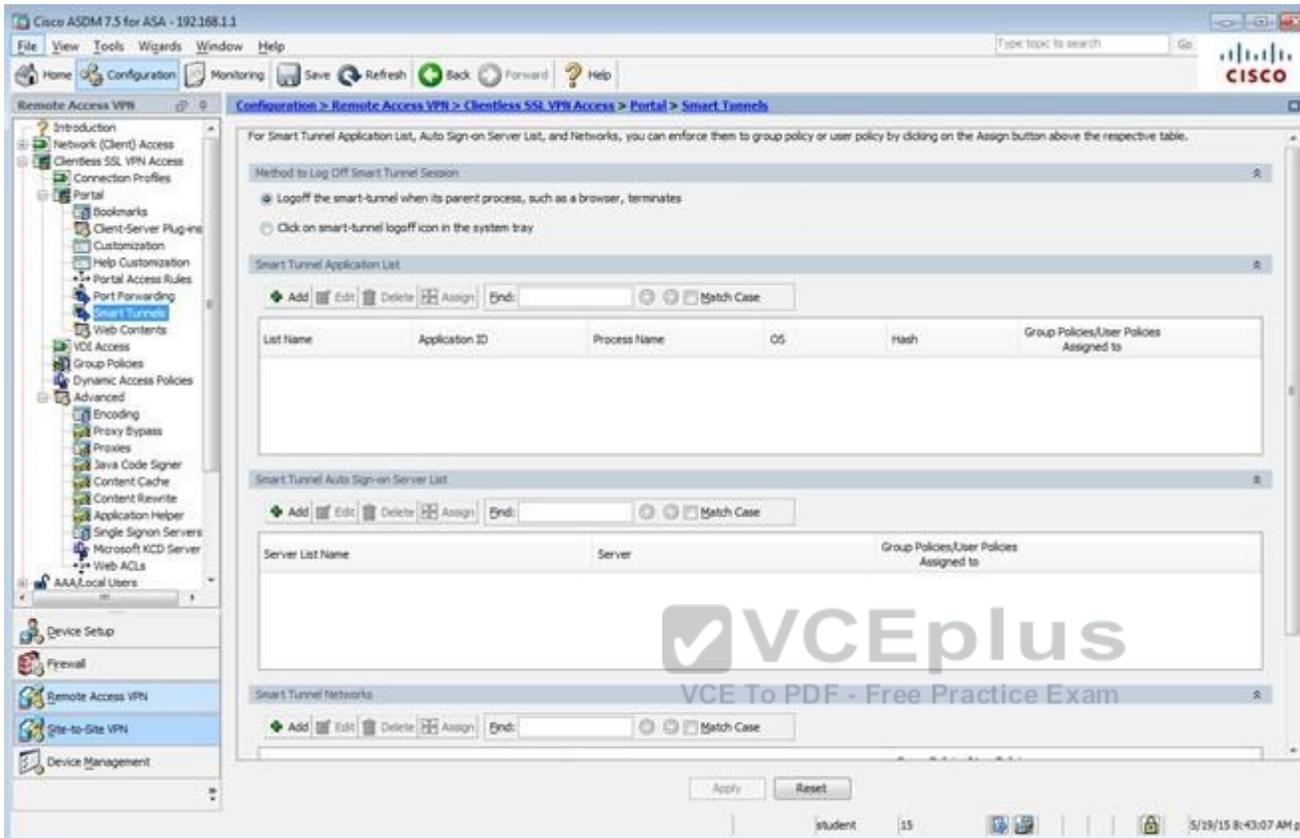
Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Inside-01V	Sales

Search field: End: [] [] Match Case

Buttons: Apply, Reset

System tray: student 15 5/19/15 8:41:57 AM pet

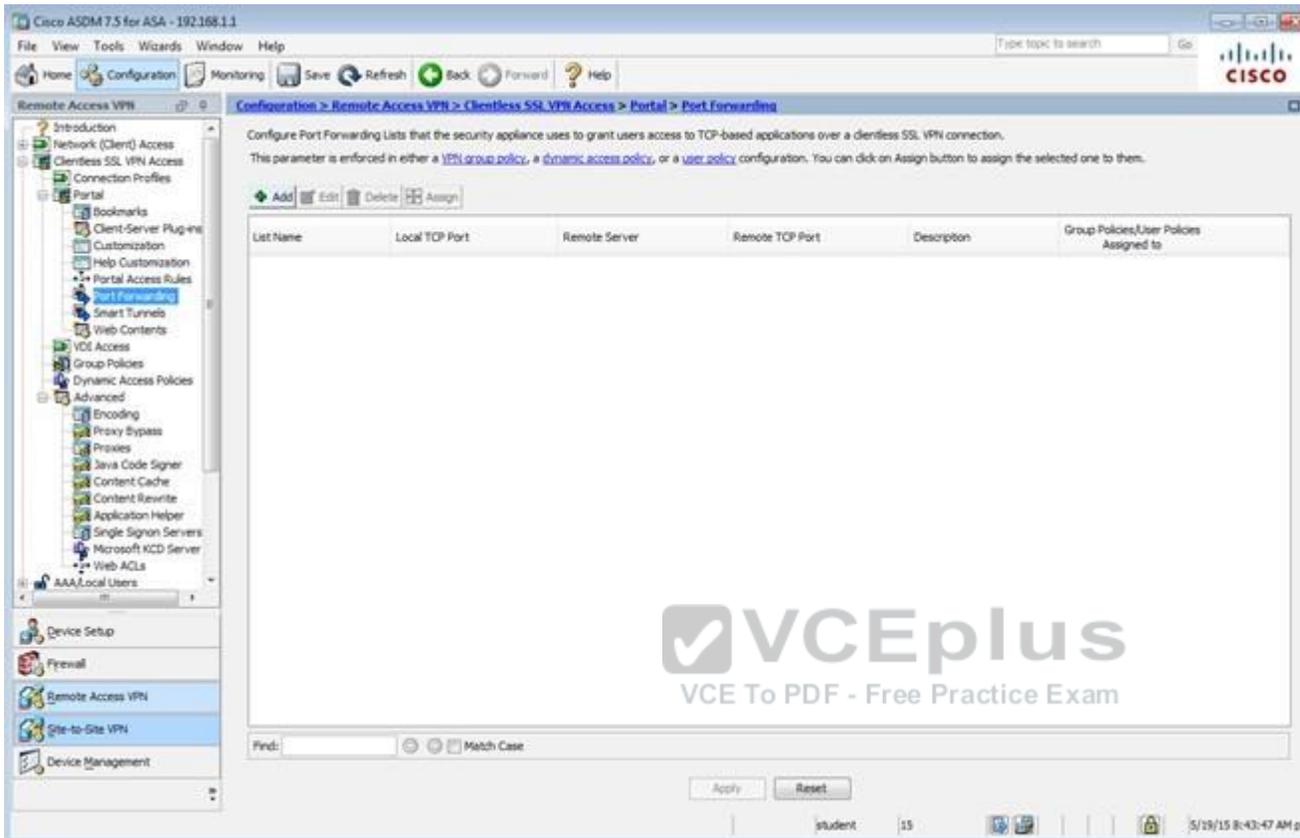




The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The navigation pane on the left shows the configuration path: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**. The main content area is titled "Smart Tunnels" and contains the following sections:

- Method to Log Off Smart Tunnel Session:** Includes radio buttons for "Logoff the smart-tunnel when its parent process, such as a browser, terminates" (selected) and "Click on smart-tunnel logoff icon in the system tray".
- Smart Tunnel Application List:** Features a table with columns: List Name, Application ID, Process Name, OS, Hash, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Auto Sign-on Server List:** Features a table with columns: Server List Name, Server, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Networks:** Features a table with controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".

At the bottom of the main content area, there are "Apply" and "Reset" buttons. The status bar at the very bottom shows "student | 15 | 5/19/15 8:43:07 AM pst". A large "VCEplus" watermark is overlaid on the center of the screenshot.



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

Add Edit Delete Assign

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description	Group Policies/User Policies Assigned to
-----------	----------------	---------------	-----------------	-------------	--

Find: Match Case

Apply Reset

student 15 5/19/15 8:43:47 AM pst

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

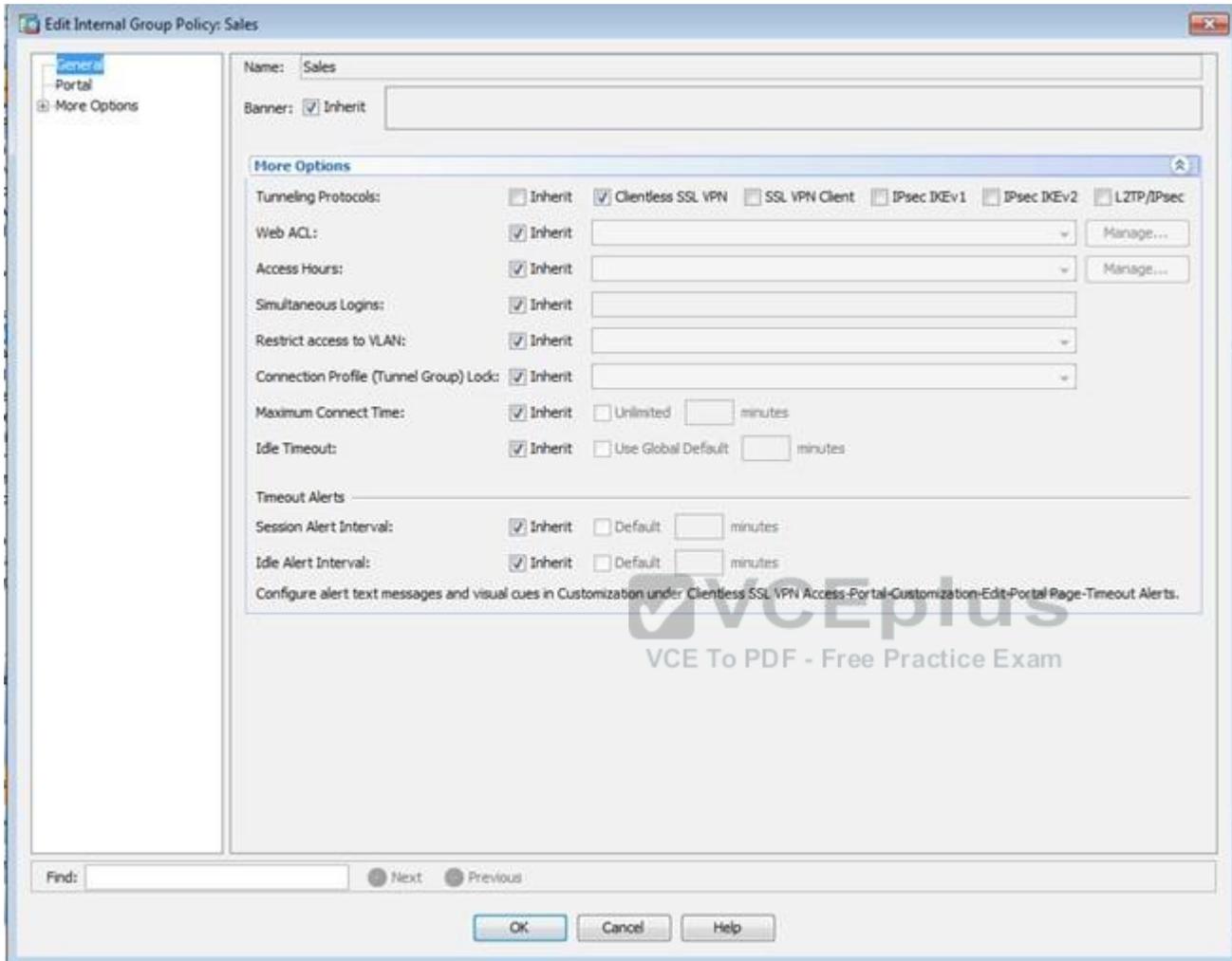
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

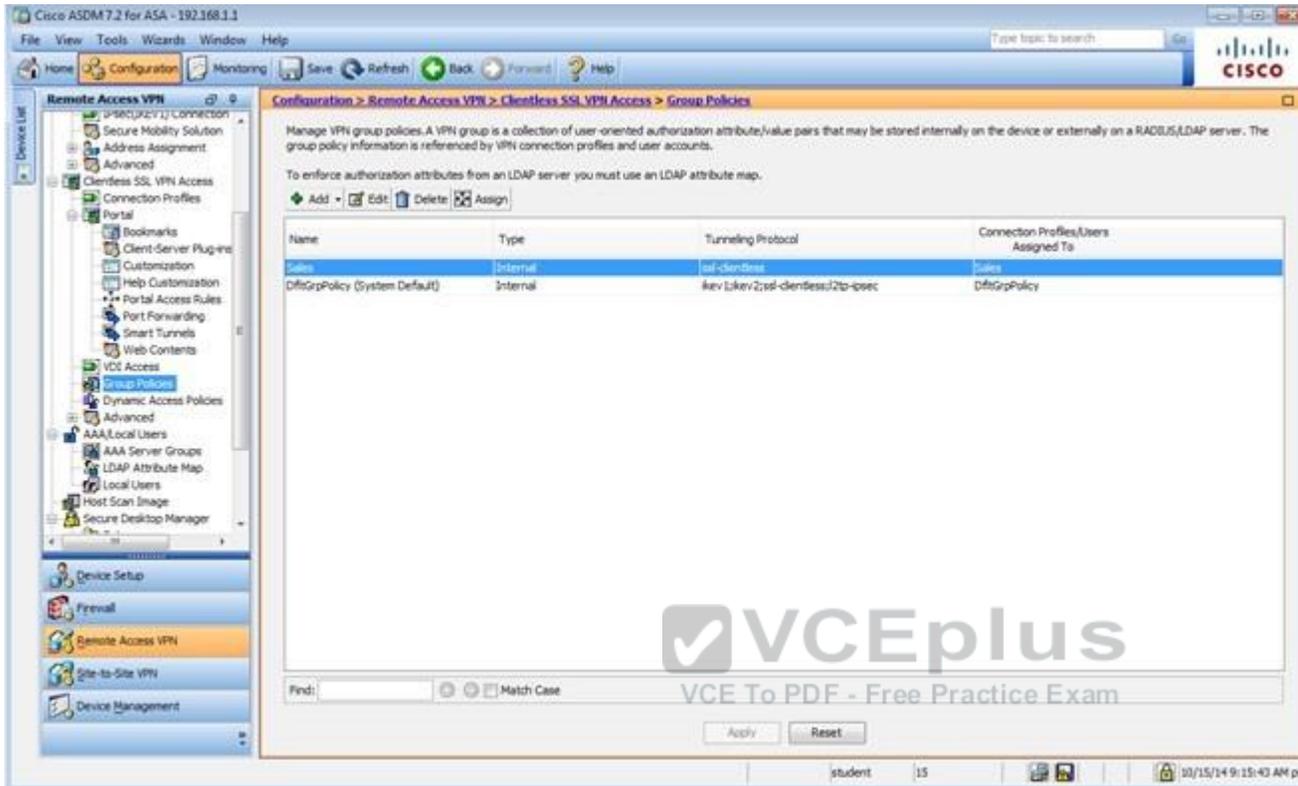
To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Clientless	Internal	ssl-clientless	Clientless
DefaultGroupPolicy (System Default)	Internal	kev1okriv2ssl-clientless/2to-espsec	DefaultRAGroup/DefaultIL2,Group/DefaultADMDNGroup/Def...

End:

student 15 5/18/15 8:49:27 AM pst





The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane displays the 'Group Policies' configuration page under 'Remote Access VPN > Clientless SSL VPN Access > Group Policies'. The page contains a table of group policies and a search bar.

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 pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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.

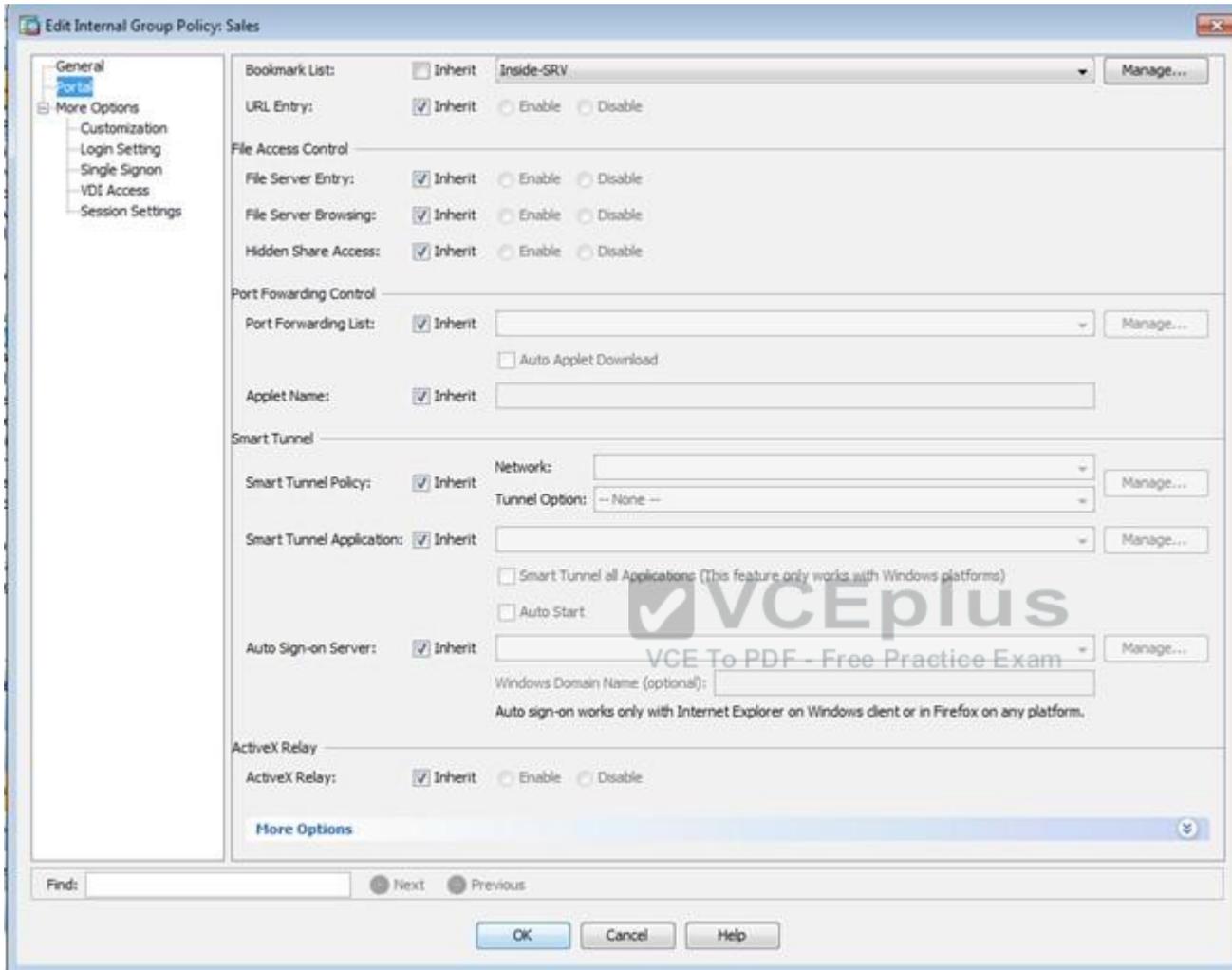
◆ Add ◆ Edit ◆ Delete ◆ Assign

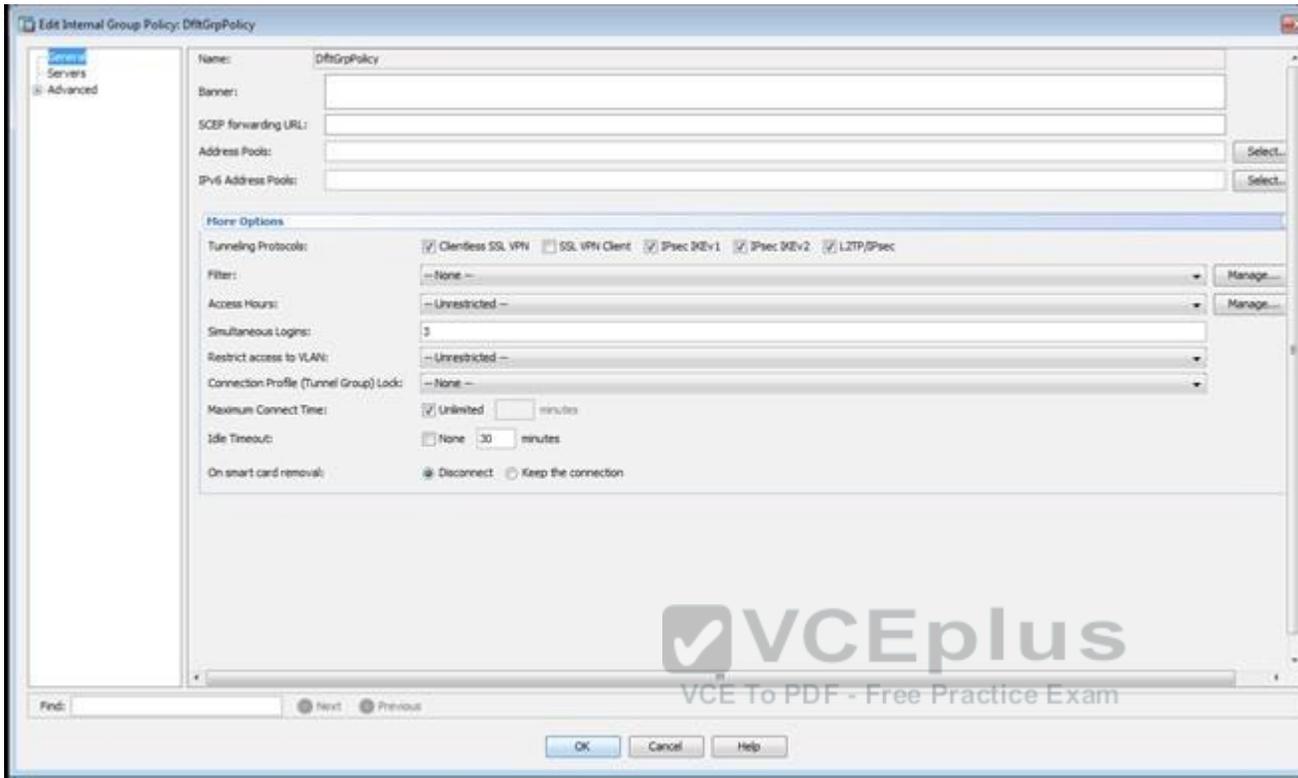
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	l2l-Clientless	Sales
DfltGrpPolicy (System Default)	Internal	ikev2ssl-clientless/2ip-ipsek	DfltGrpPolicy

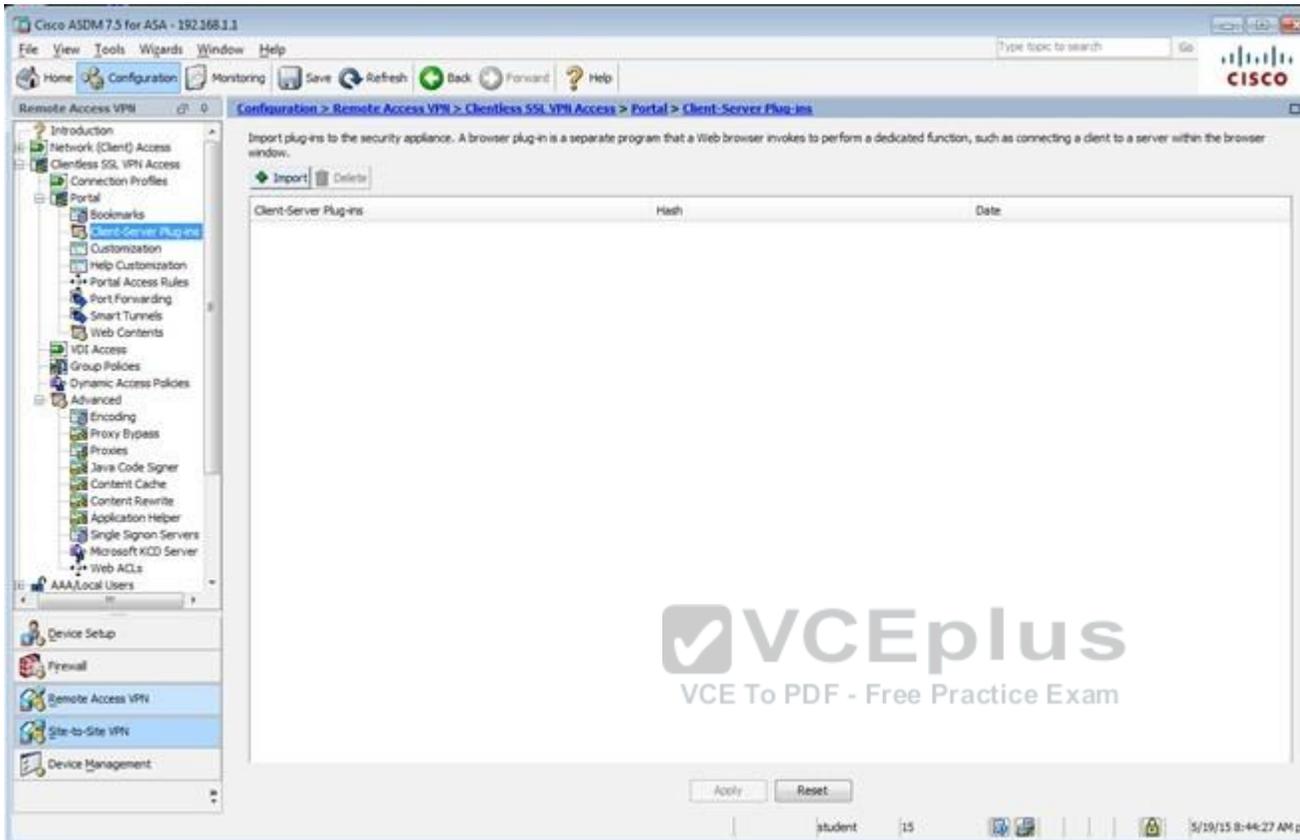
Find: Match Case

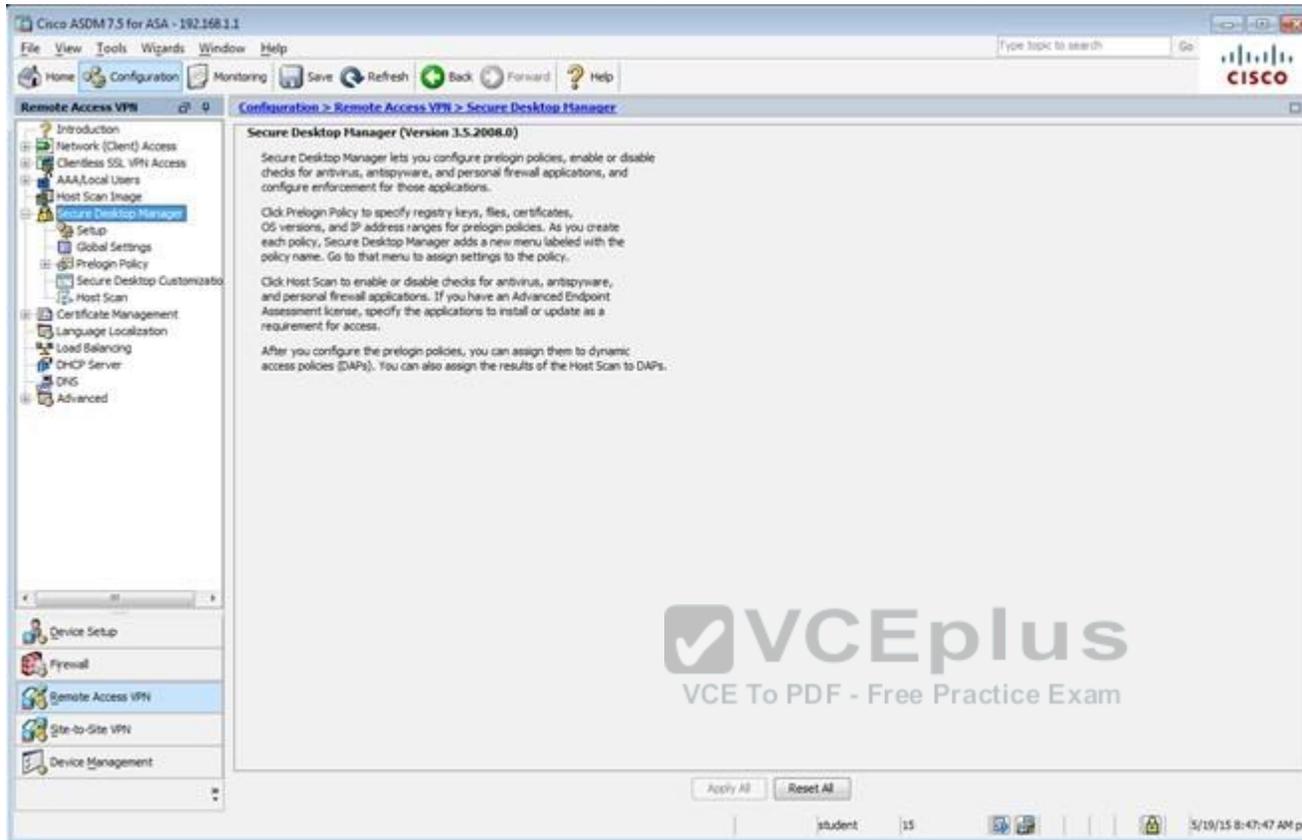
Apply Reset

student | 15 | 30/15/14 9:15:43 AM pst









The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 configuration interface. The breadcrumb path is Configuration > Remote Access VPN > Secure Desktop Manager. The left sidebar shows a tree view with 'Secure Desktop Manager' selected. The main content area displays the following text:

Secure Desktop Manager (Version 3.5.2008.0)

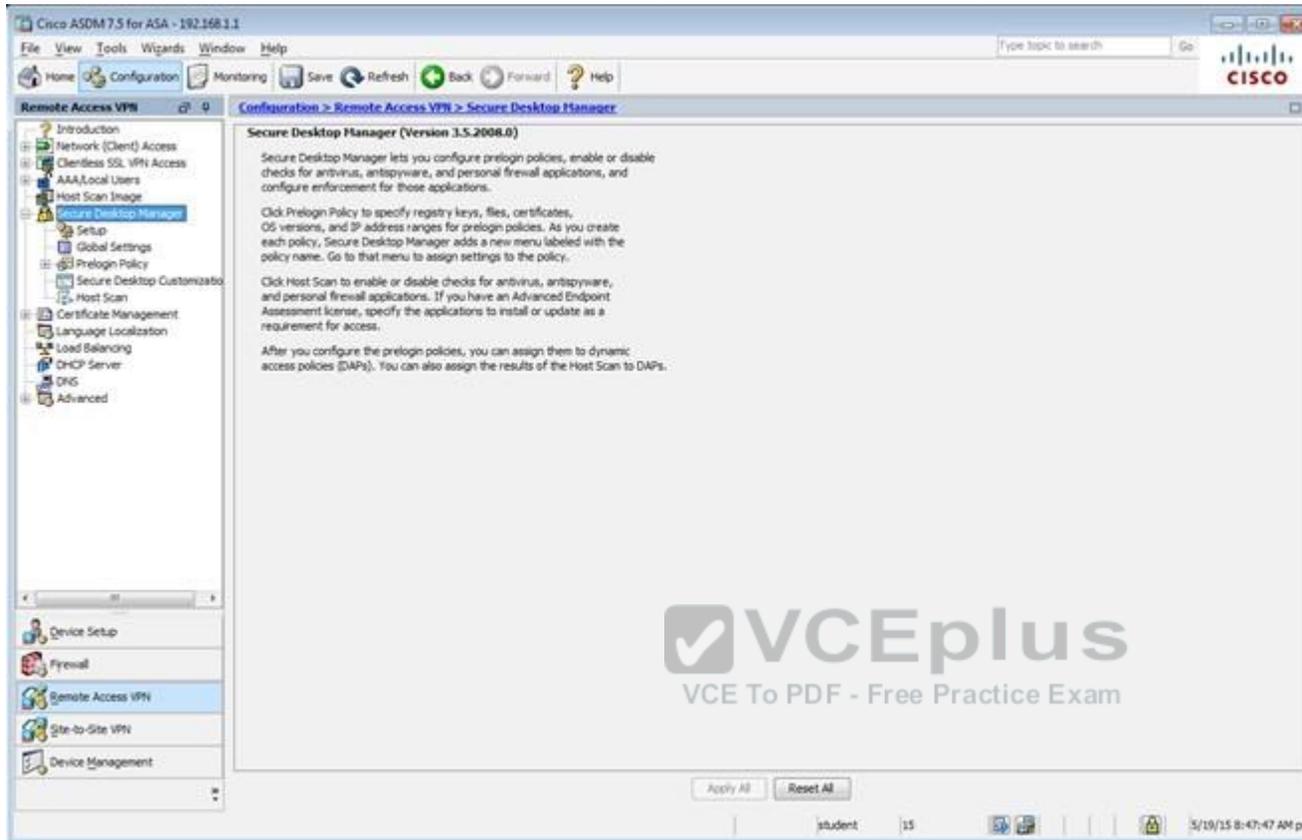
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispware, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispware, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

At the bottom of the page, there are 'Apply All' and 'Reset All' buttons. The status bar at the bottom shows 'student | 15 | 3/19/15 8:47:47 AM pst'.



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the "Secure Desktop Manager (Version 3.5.2008.0)" configuration page. The page includes a navigation tree on the left with categories like "Remote Access VPN", "Network (Client) Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The "Secure Desktop Manager" section is expanded, showing sub-items: "Introduction", "Setup", "Global Settings", "Prelogin Policy", "Secure Desktop Customization", "Host Scan", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

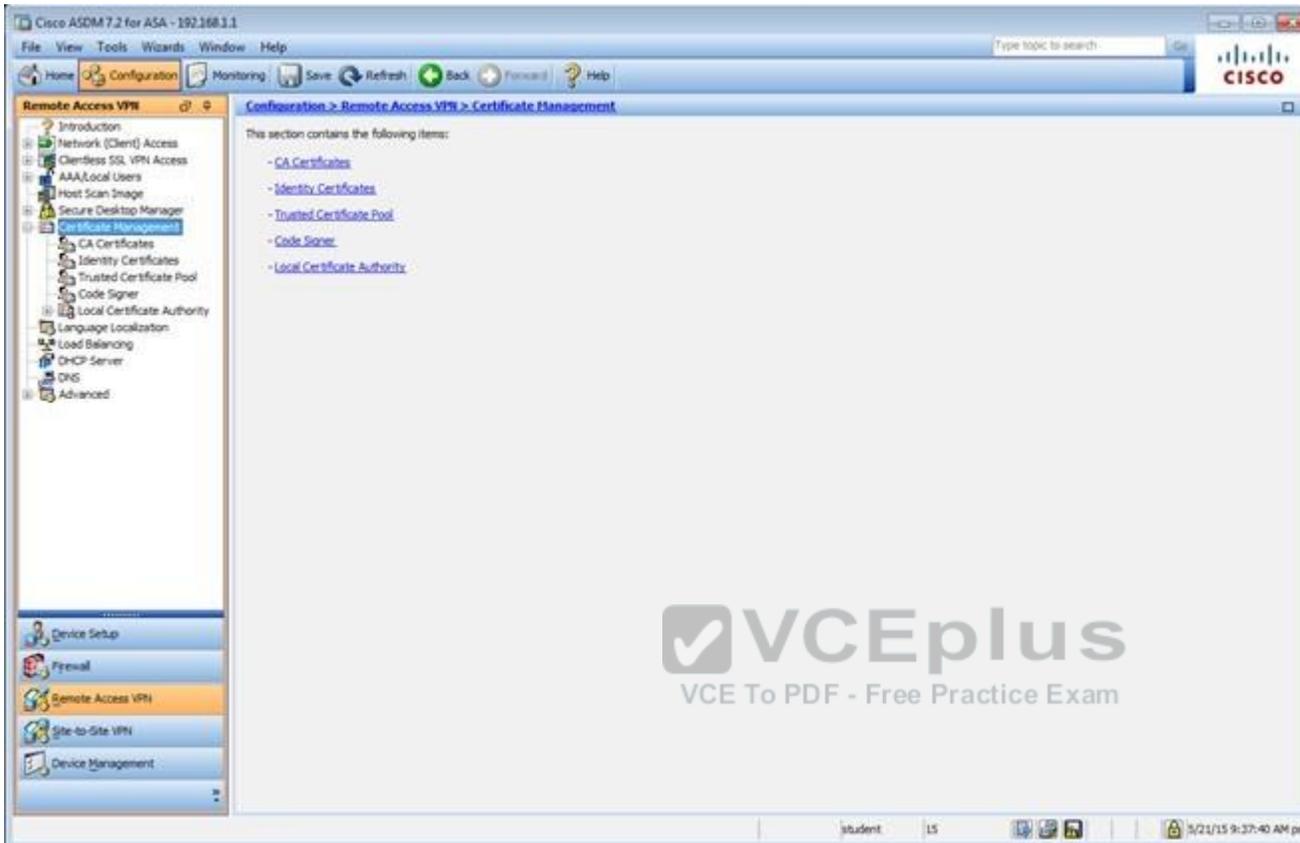
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispware, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispware, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

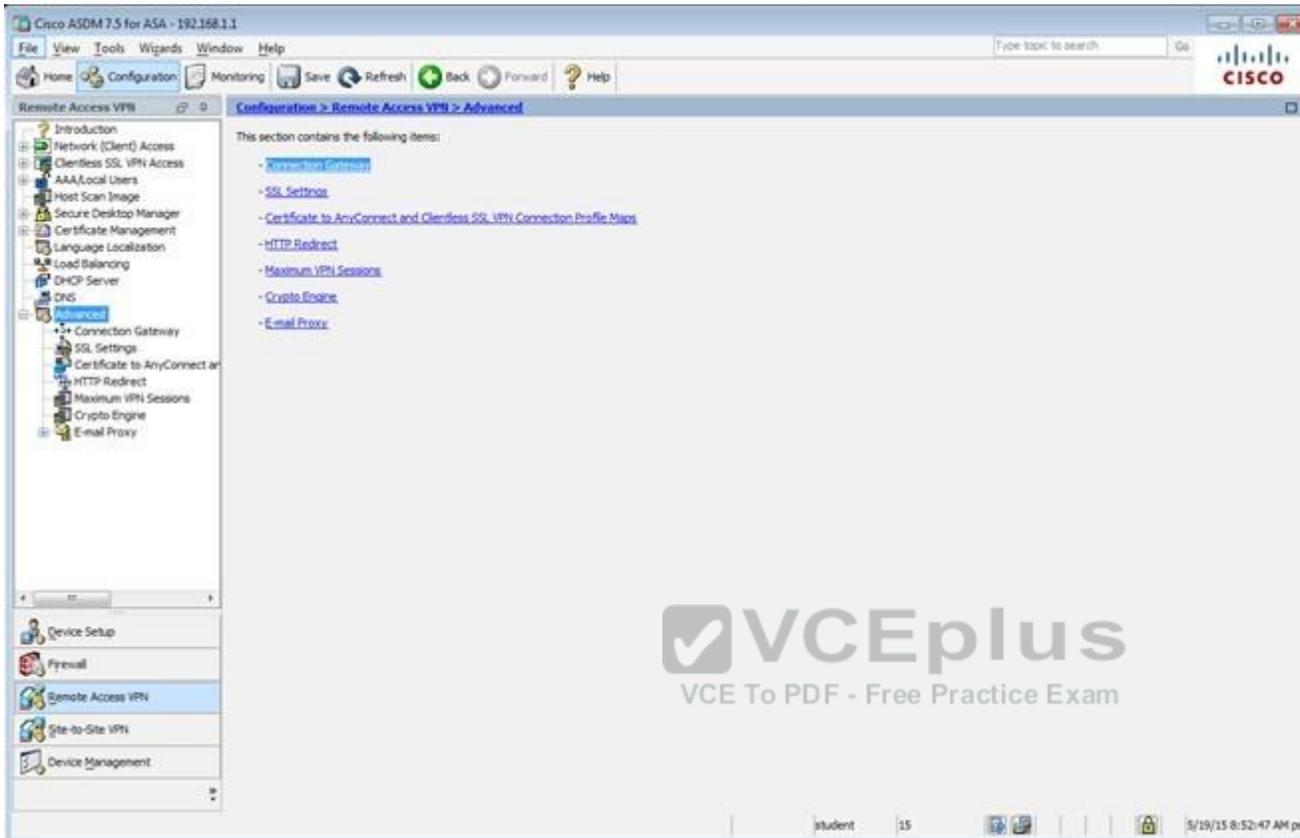
At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Certificate Management > Identity Certificates". The left sidebar shows a tree view with "Identity Certificates" selected under "Certificate Management". The main content area features a table with the following data:

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname-#1 [7-ASA.sec...]	hostname-#1 [7-ASA.sec...]	11:10:33 pet (Dec 20 2024)	ASDM_Trustpoint1	General Purpose	RSA (2048 bits)

Below the table, there are sections for "Certificate Expiration Alerts" (Send the first alert before: 60 (days), Repeat Alert Interval: 7 (days)) and "Public CA Enrollment" (Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust). A "Launch ASDM Identity Certificate Wizard" button is visible at the bottom of the main content area. The interface includes a search bar, navigation buttons (Home, Configuration, Monitoring, Save, Refresh, Back, Forward, Help), and a Cisco logo. The bottom status bar shows "student | 15 | 5/19/15 8:51:47 AM pet".



Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The minimum SSL version for the security appliance to negotiate as a "server": TLS V1

The minimum SSL version for the security appliance to negotiate as a "client": TLS V1

Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modAus

ECDH group to be used with SSL: Group19 - 256-bit EC

Encryption

Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
DTLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...

Server Name Indication (SNI)

Domain: dmz

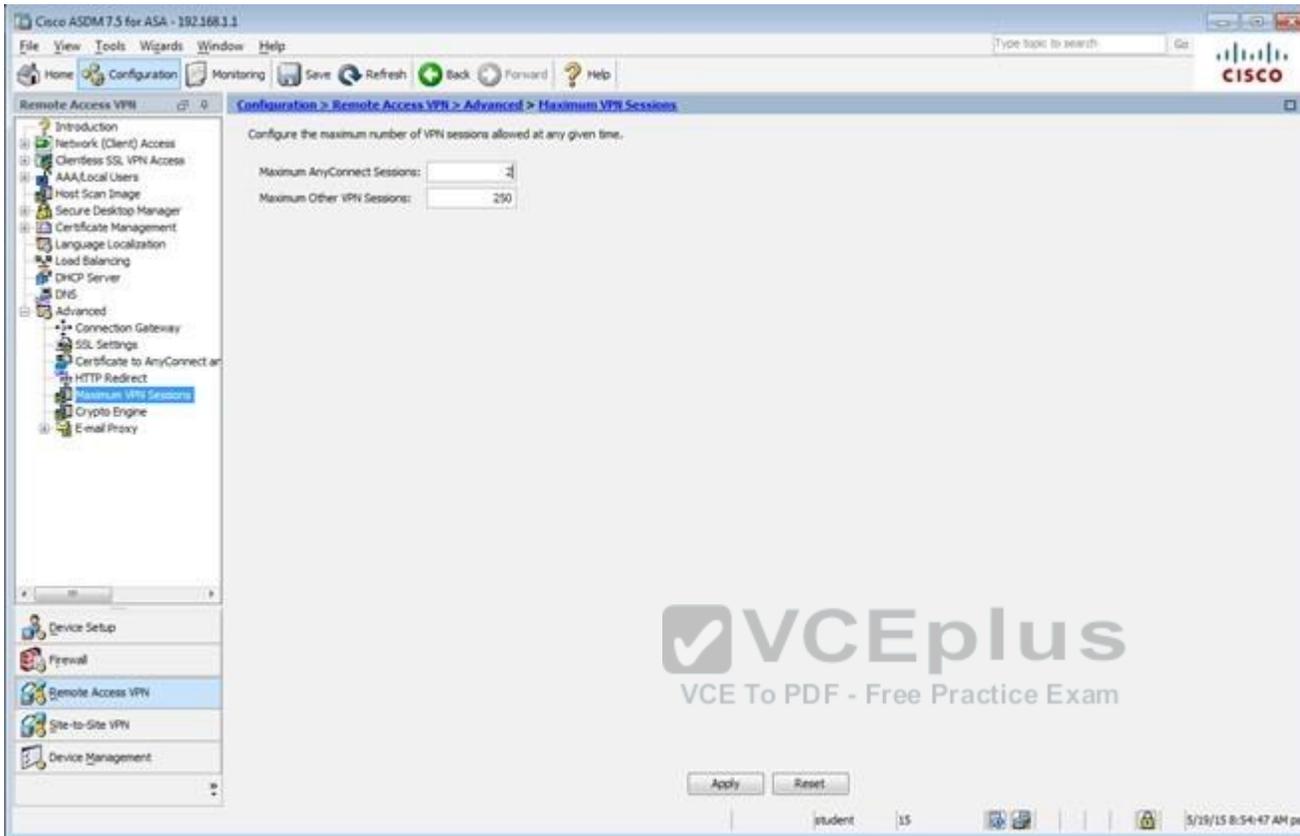
Certificate: ASDM_TrustPoint1.h...

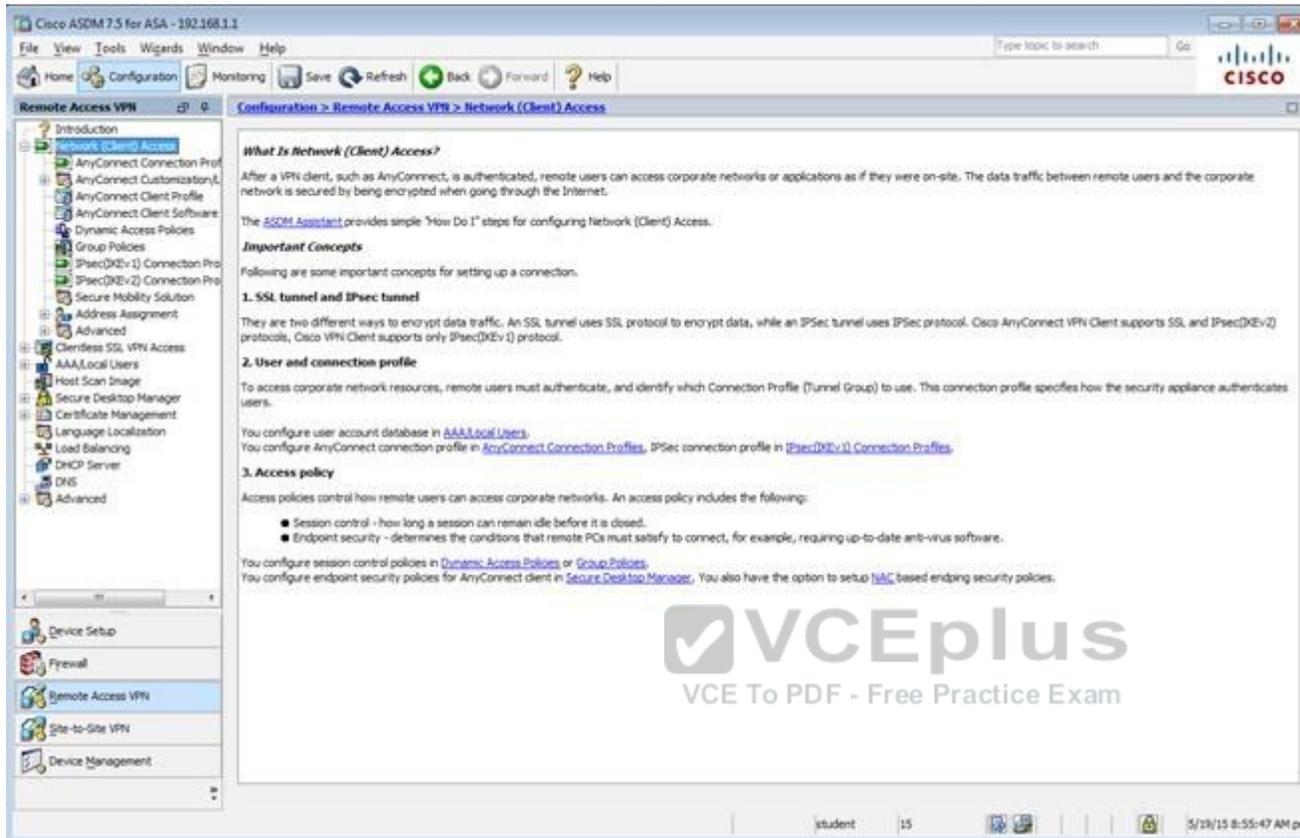
Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Apply Reset

student 15 3/19/15 8:54:07 AM pst





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the configuration page for "Remote Access VPN > Network (Client) Access". The page includes a navigation tree on the left, a search bar at the top, and a main content area with the following text:

What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts
Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKv2) protocols. Cisco VPN Client supports only IPsec(DKv1) protocol.

2. User and connection profile
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

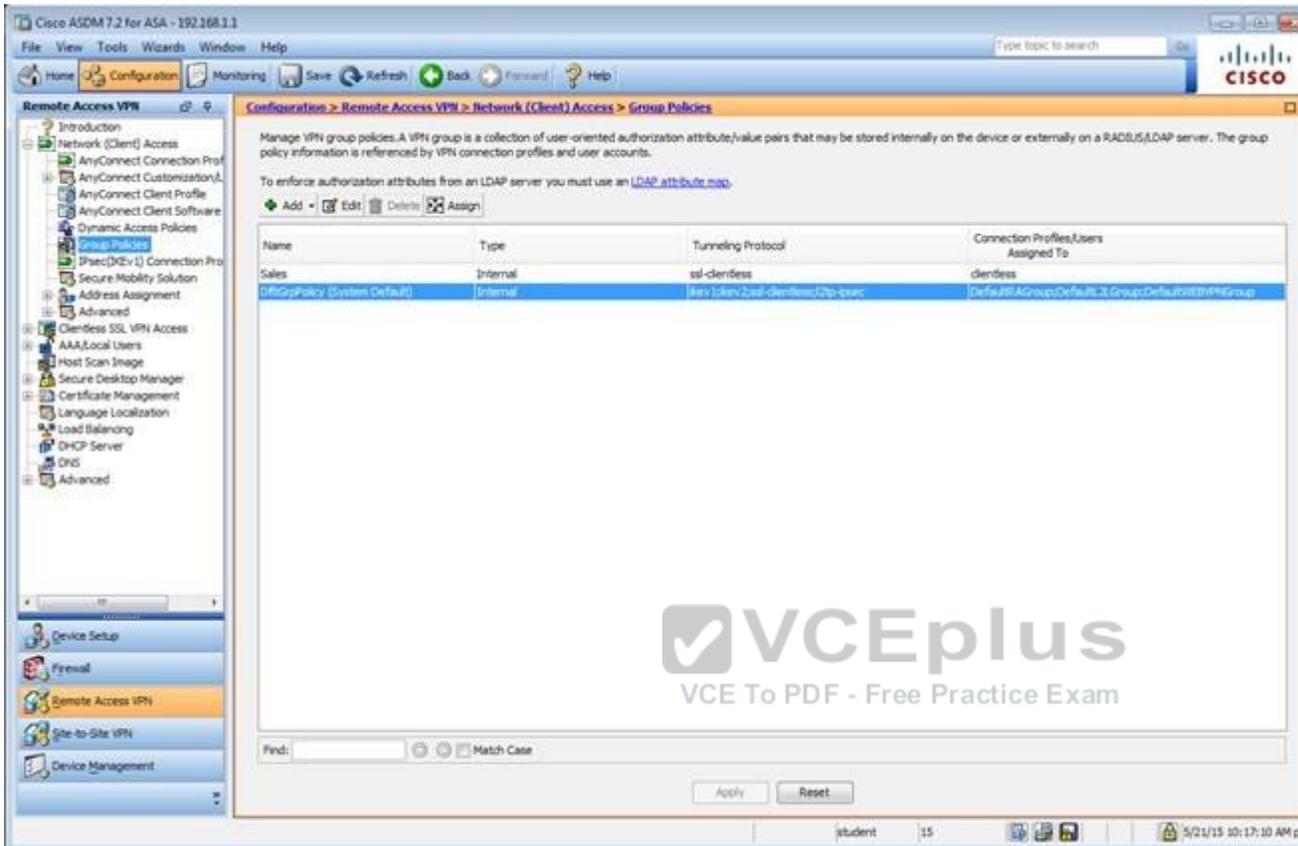
You configure user account database in [AAA Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKv1\) Connection Profiles](#).

3. Access policy
Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HMAC](#) based endpoint security policies.

The bottom of the screenshot shows a taskbar with "student" and "15" and a system tray with the date "5/28/15 8:55:47 AM pet".



Cisco ASDM 7.2 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

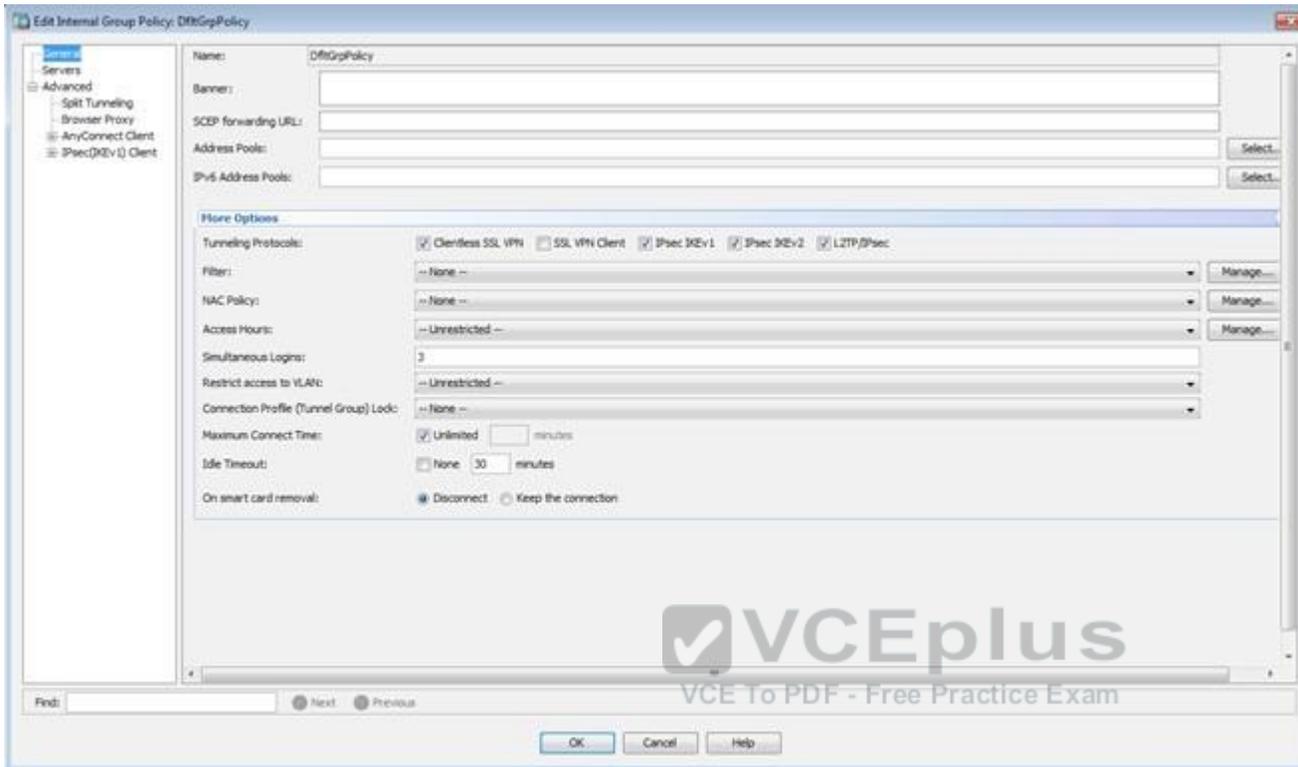
Add - Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DRGpPolicy (System Default)	Internal	[rev:1.0]ssl-clientless/2ip-espac	DefaultRAGroup/Default3LGroup/DefaultRIPGroup

Find: Match Case

Apply Reset

ytudent 15 5/21/15 10:17:10 AM pet



The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area is titled 'Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles'.

Access Interfaces
Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input type="checkbox"/>
dmt	<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.

Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DfltGrpPolicy
DefaultIkev1Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DfltGrpPolicy
Default	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL	Sales

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:56:47 AM pst

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

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input checked="" 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 can configure the mapping from certificate to connection profile [here](#).

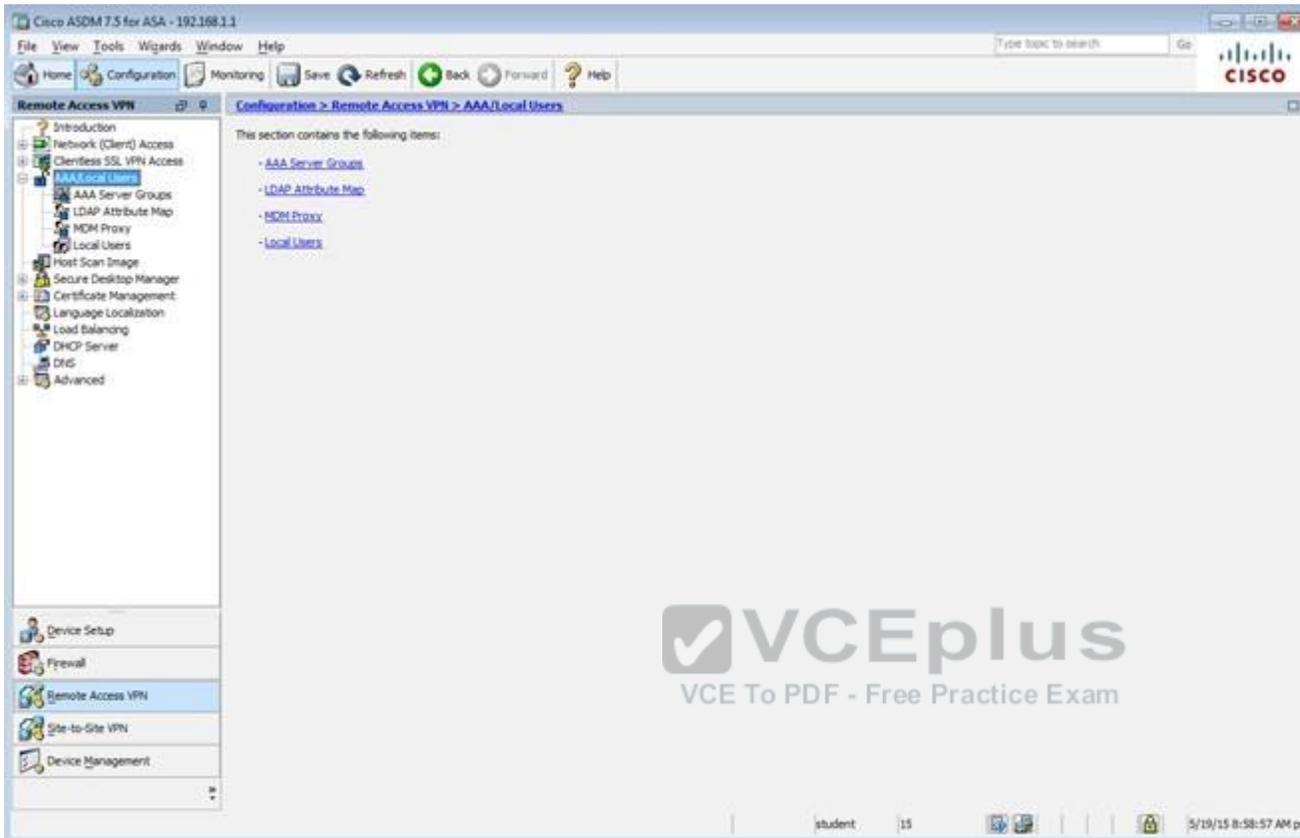
End:

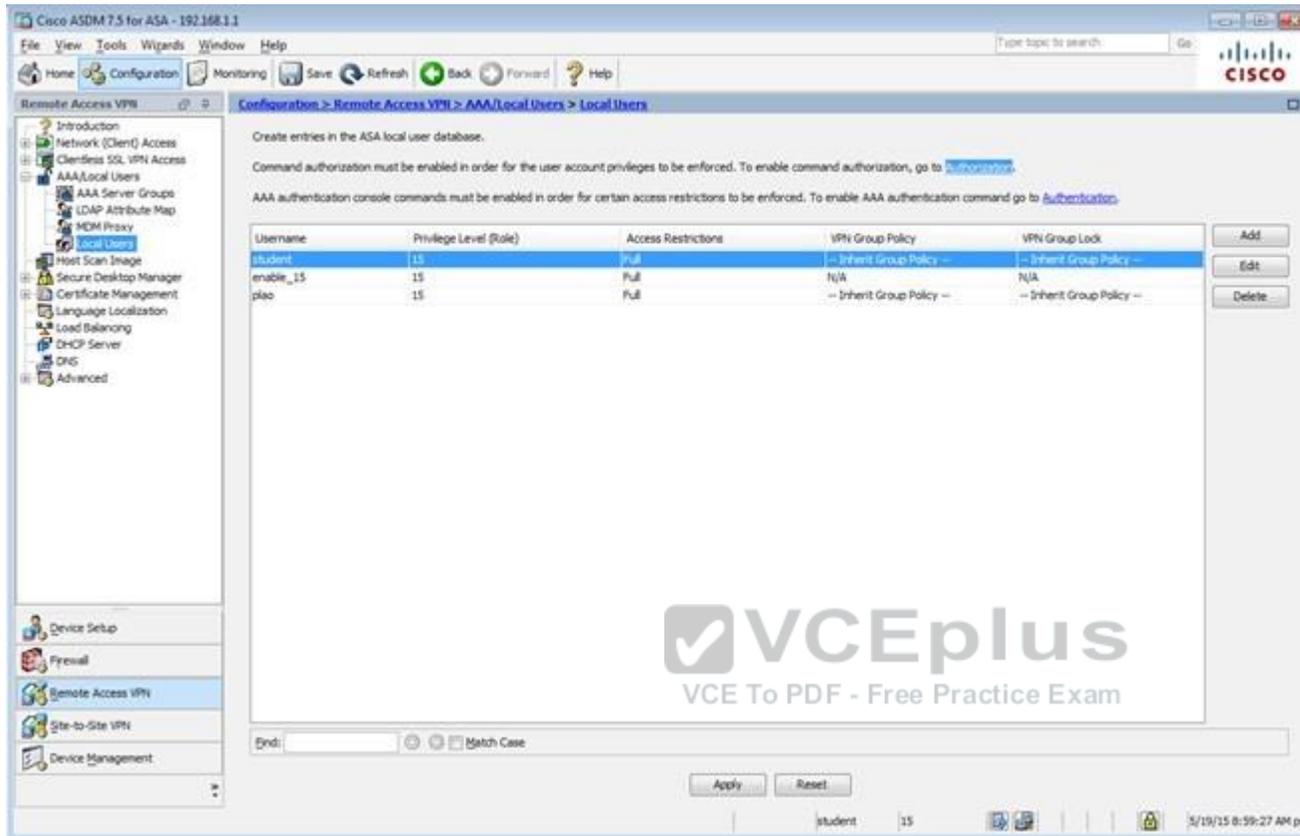
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
certless	<input checked="" type="checkbox"/>	<input type="checkbox"/>	yes	SSL(OCSP)	certless

Let group URLs take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Apply Reset

student 15 5/19/15 8:58:17 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

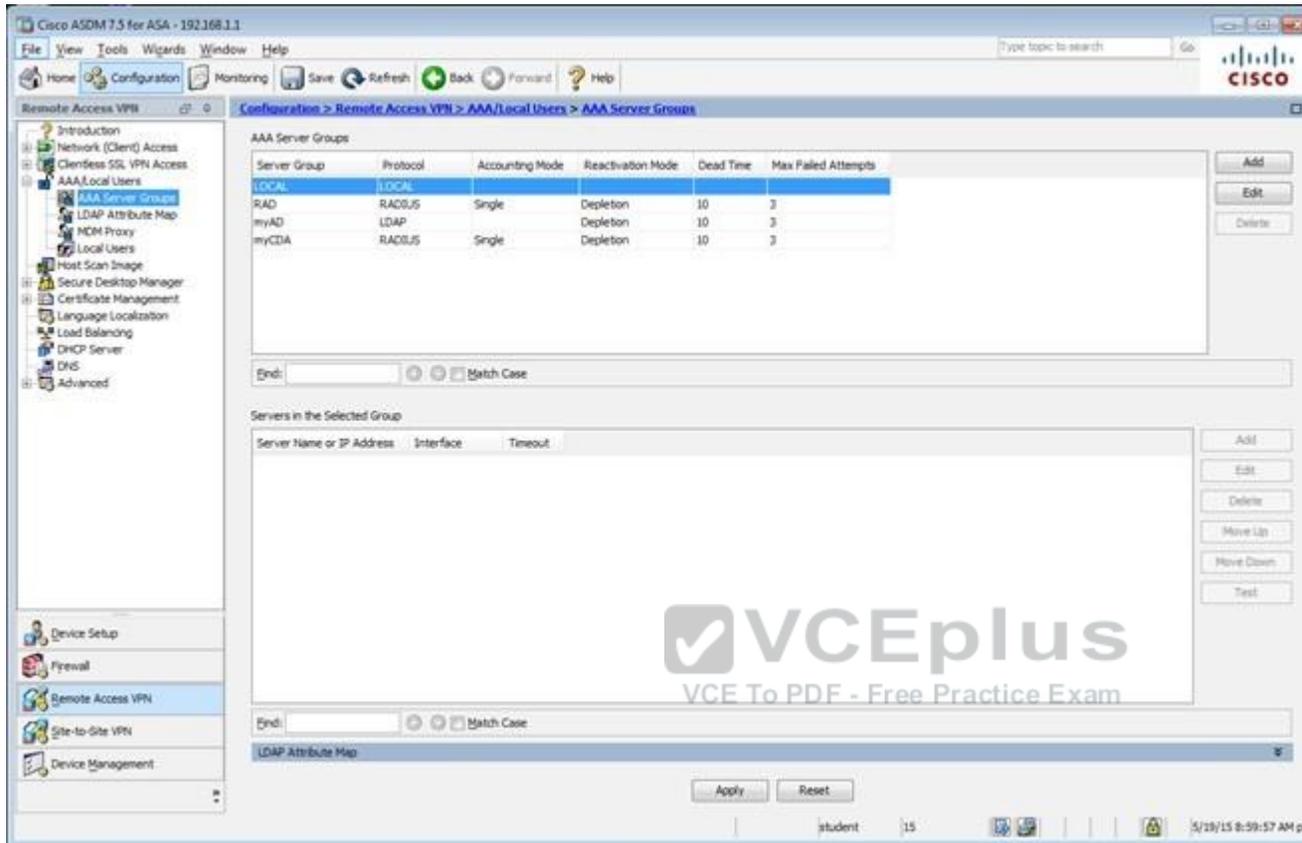
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plac	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End: Match Case

Apply Reset

student 15 5/19/15 8:59:27 AM pet



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: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:
For B:

Interface Allow 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.

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 can configure the mapping from certificate to connection profile.

+ Add Edit Delete Find: Match Case

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

For C, Navigate to the Bookmarks tab:

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. You can click on Assign button to assign

+ Add Edit Delete + Import Export Assign

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
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

 **VCEplus**
VCE To PDF - Free Practice Exam

Add

Edit

Delete

Move Up

Move Down

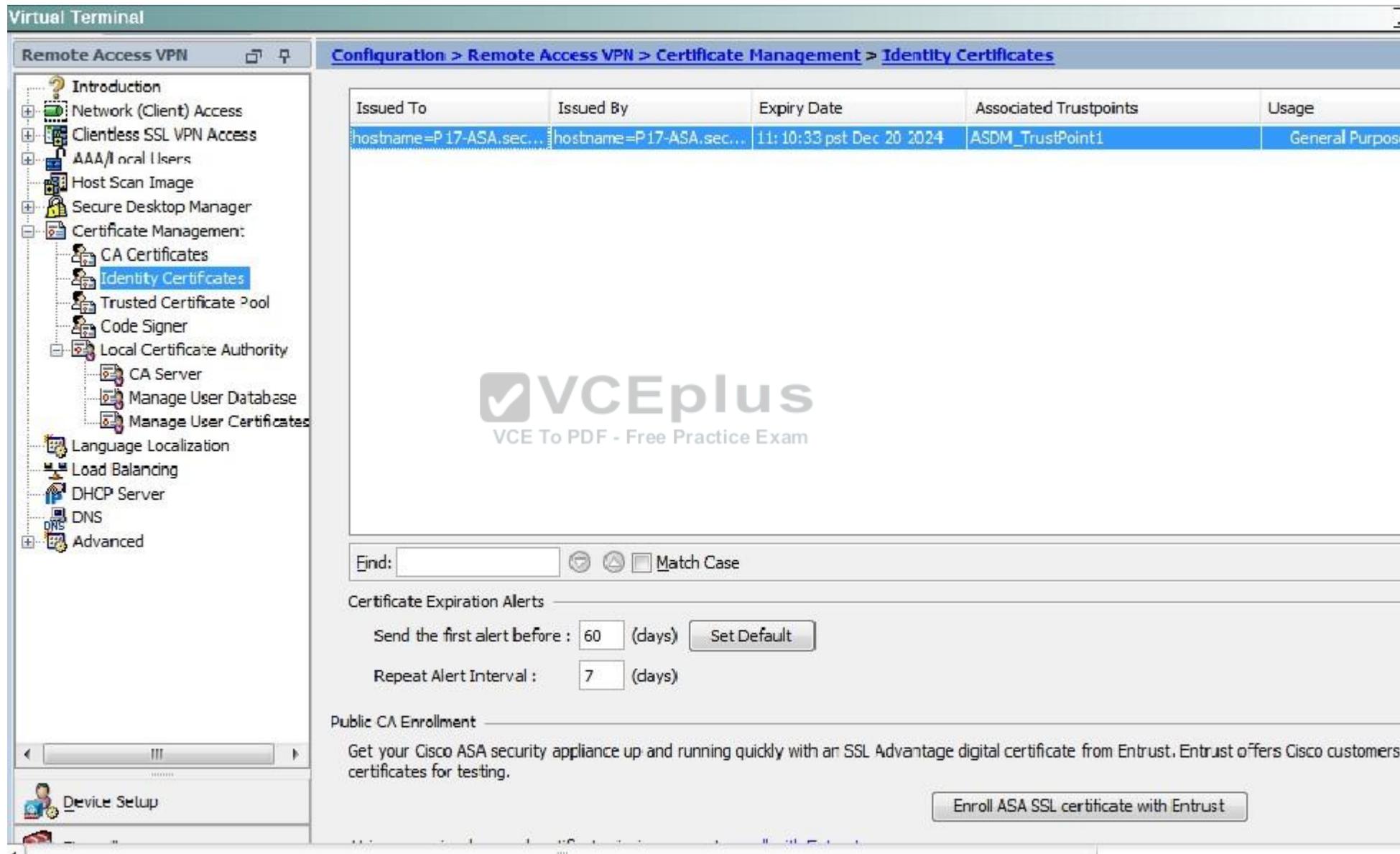
Find:   Match Case

OK

Cancel

Help

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



The screenshot shows the Cisco ASA configuration interface for Remote Access VPN > Certificate Management > Identity Certificates. The left sidebar shows a tree view with 'Identity Certificates' selected. The main content area displays a table of certificates and configuration options.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM_TrustPoint1	General Purpose

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 certificate from Entrust. Entrust offers Cisco customers certificates for testing.

Note E:

The screenshot shows the Cisco ASDM 7.5 for ASA interface. The breadcrumb path is: Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. The left sidebar shows a tree view with 'AnyConnect Connection Prof' selected. The main content area contains the following sections:

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires er VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 Client Services
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 can configure the mapping from certificate to connecti

Buttons: Device Certificate ... Port Settings ...

Bottom toolbar: + Add, Edit, Delete, Find: [text box], Match Case

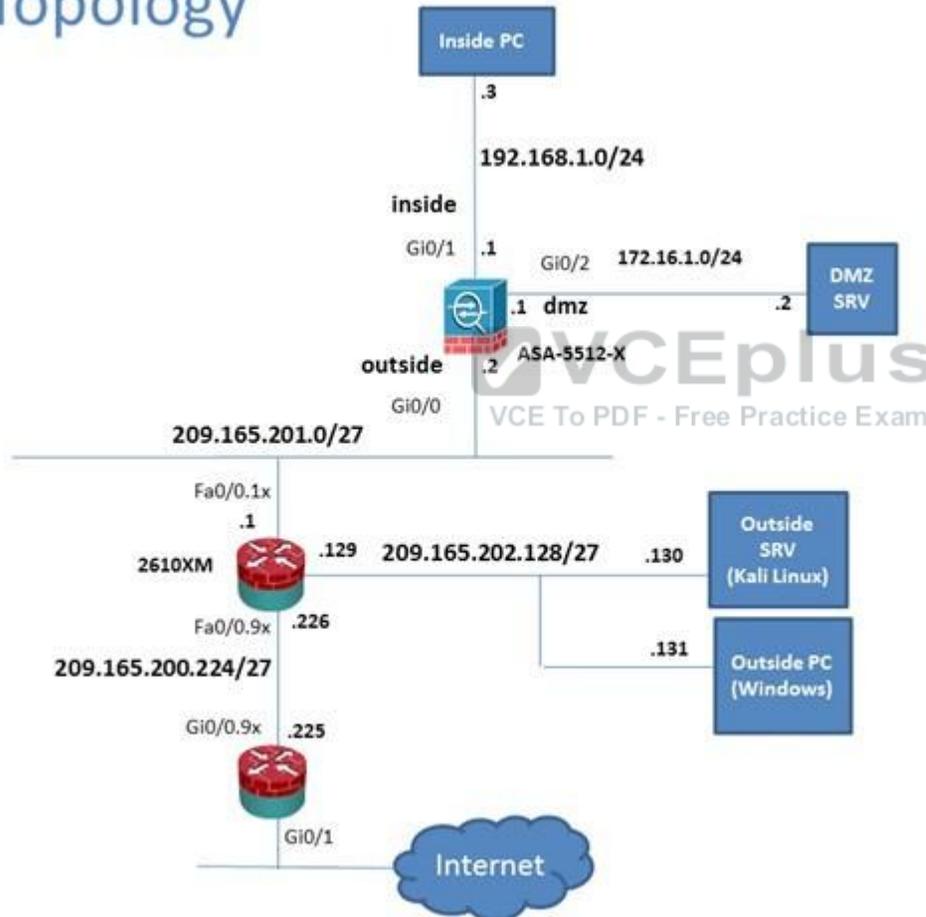
QUESTION 67
Scenario

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 un-expand the expanded menu first.

Lab Topology

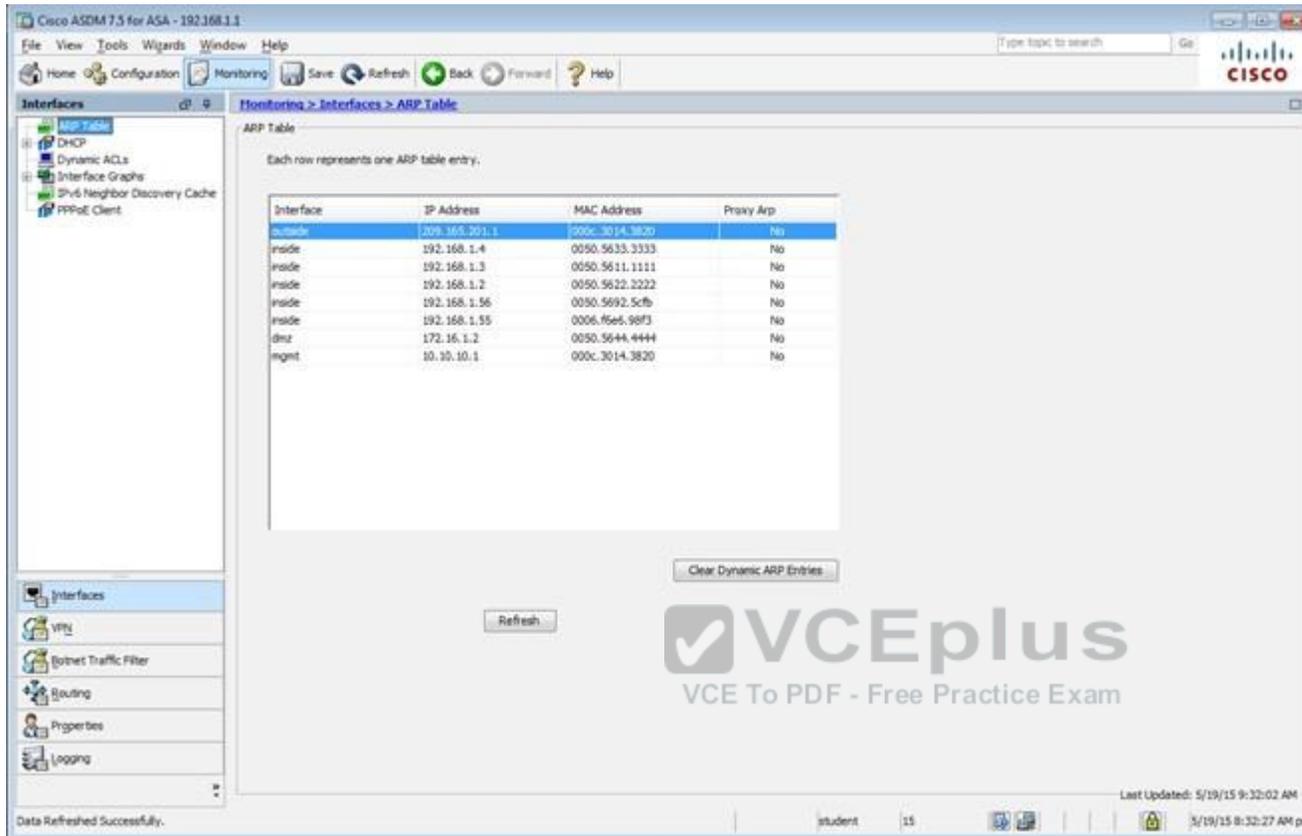


The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is divided into several sections:

- Device Information:**
 - General tab selected.
 - Host Name: P17-ASA,secure-x.local
 - ASA Version: 100.14(6)13
 - ASDM Version: 7.5(1)1
 - Firewall Mode: Routed
 - Environment Status: OK
 - Device Uptime: 11d 21h 42m 47s
 - Device Type: ASA 5512
 - Context Mode: Single
 - Total Flash: 4096 MB
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	up	up	0
inside	192.168.1.1/24	up	up	4
mgmt	10.10.10.2/24	up	up	0
outside	209.165.201.2/24	up	up	0
- VPN Sessions:**
 - IPsec: 0
 - Clientless SSL VPN: 0
 - AnyConnect Client: 0
- System Resources Status:**
 - Total Memory Usage: 500 MB (approx. 50% of 1GB total)
 - Total CPU Usage: 0%
 - Core Usage: 0%
- Traffic Status:**
 - Connections Per Second Usage: 0
 - 'outside' Interface Traffic Usage (Kbps): 0
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina Description
6	May 13 2015	12:35:09	302016	10.81.254.202	123	209.165.201.2	65535 Teardown UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6	May 13 2015	12:35:08	106015	192.168.1.3	14676	192.168.1.1	443 Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6	May 13 2015	12:35:08	302014	192.168.1.3	14676	192.168.1.1	443 Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.3014.3800	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.f5e5.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

Last Updated: 5/19/15 9:32:02 AM

student 15 5/19/15 8:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/ISAK Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- NM Proxy Statistics
- NM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN		1	1	1
Browser		1	1	1

Filter By: Clientless SSL VPN -- All Sessions -- Filter

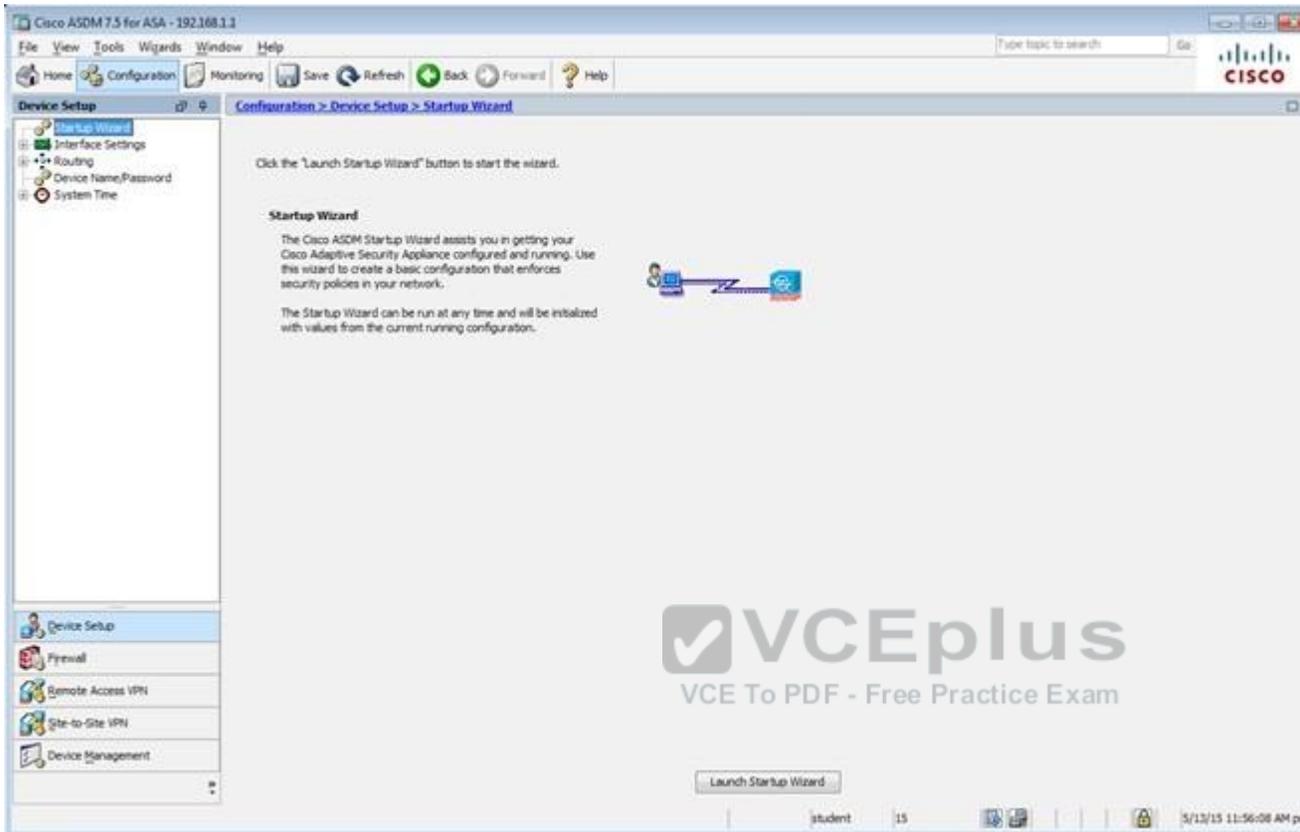
Username	IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
student	209.165.202.131	Sales	Clientless	08:03:46 [Sat May 21 2015]	316774 41833

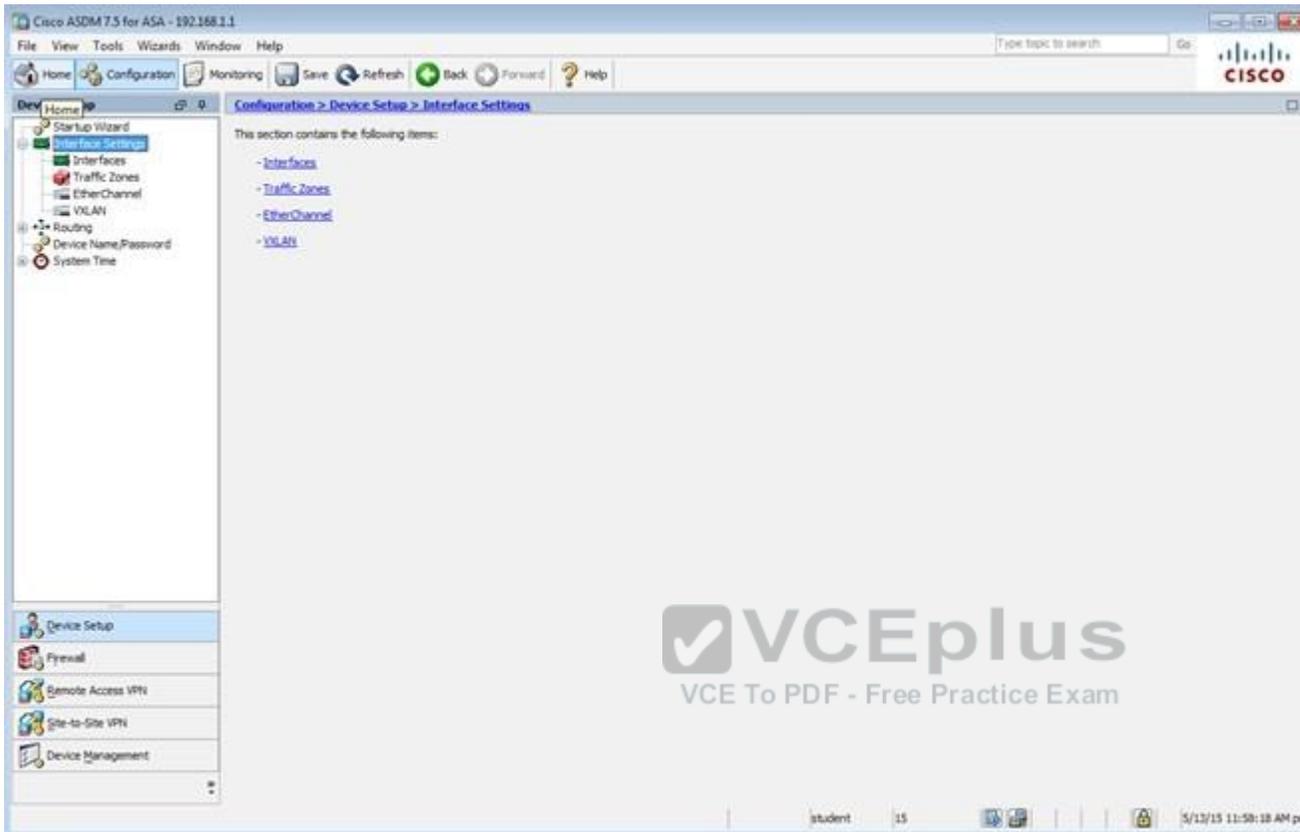
Refresh

Last Updated: 5/19/15 9:33:12 AM

Data Refreshed Successfully. | student | 15 | 5/19/15 8:33:37 AM pst







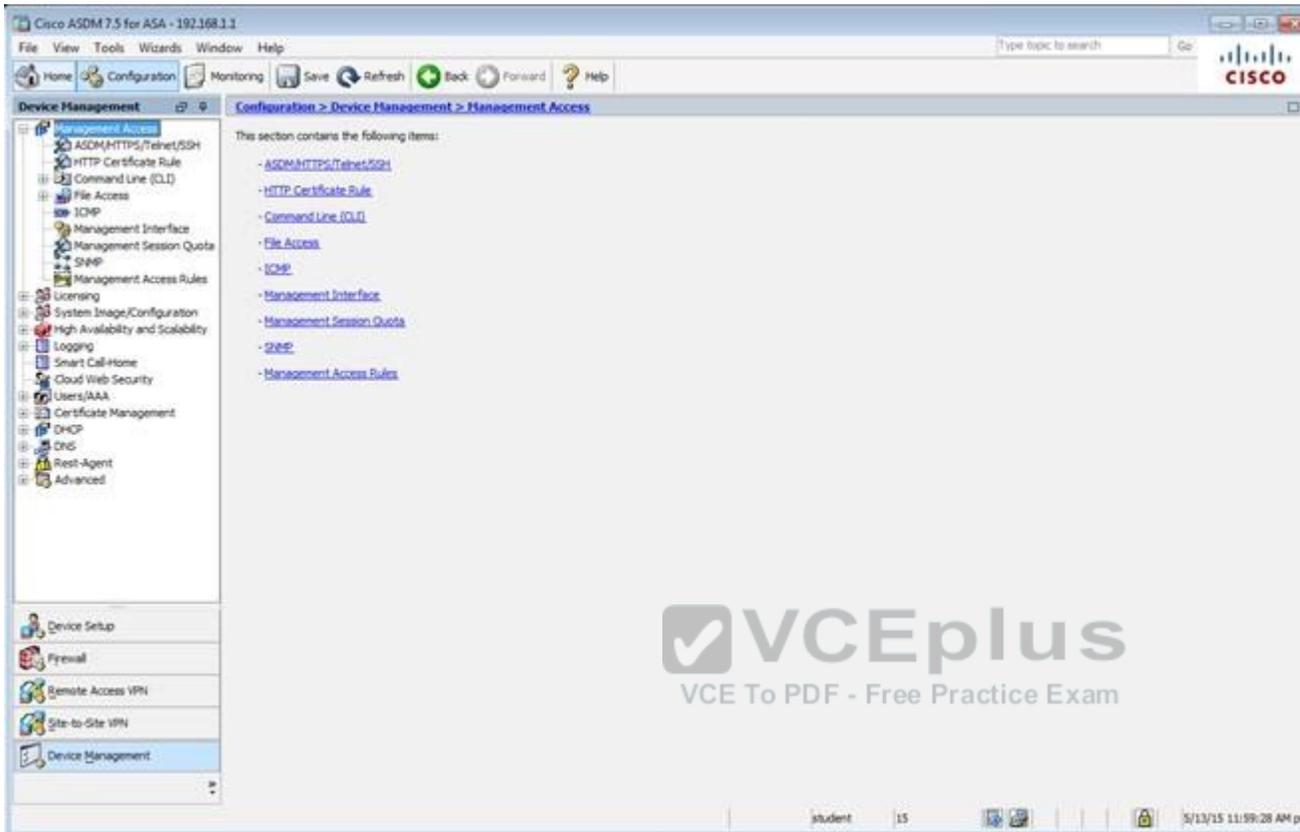
The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration page for Interfaces, with a table listing the following data:

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled	0	209.165.201.2	255.255.255.0		Hardware
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1	255.255.255.0		Hardware
GigabitEthernet0/2	dmz			Enabled	172	16.1.1	255.255.255.0		Hardware
GigabitEthernet0/3				Enabled					Hardware
GigabitEthernet0/4				Enabled					Hardware
GigabitEthernet0/5	mgmt			Enabled	100	10.10.10.2	255.255.255.0		Hardware
Management0/0				Enabled					Hardware

Below the table, there are three checkboxes for advanced settings:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface
- Enable jumbo frame reservation

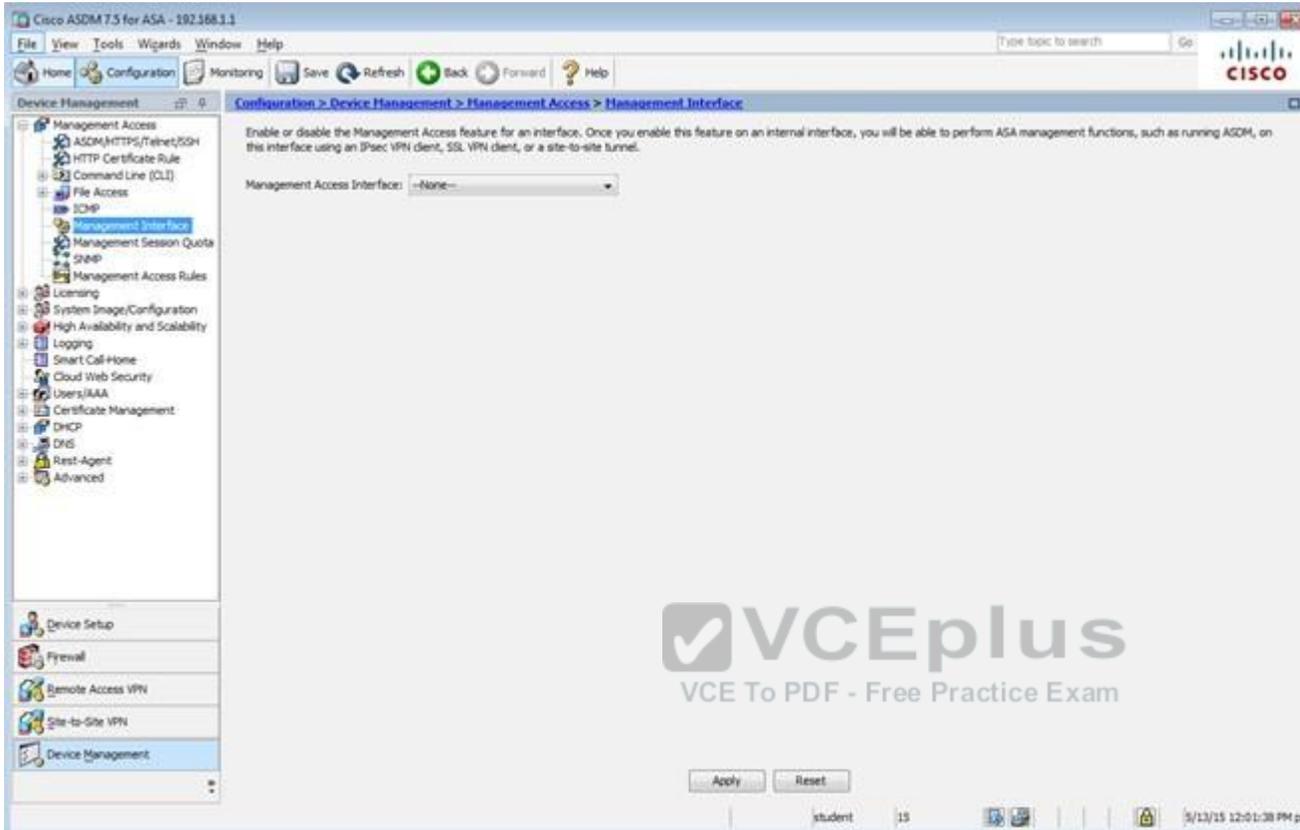
The interface also includes 'Add', 'Edit', and 'Delete' buttons on the right side, and 'Apply' and 'Reset' buttons at the bottom.

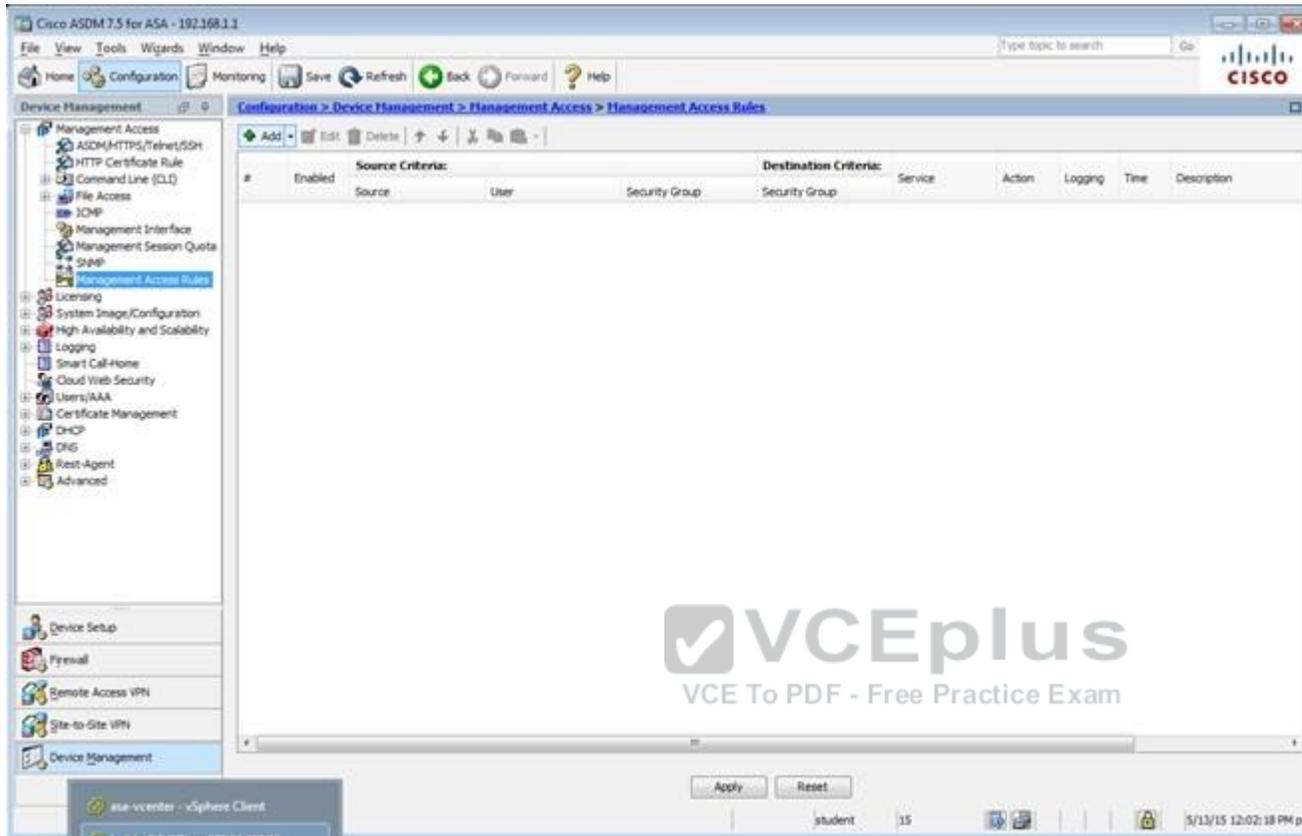


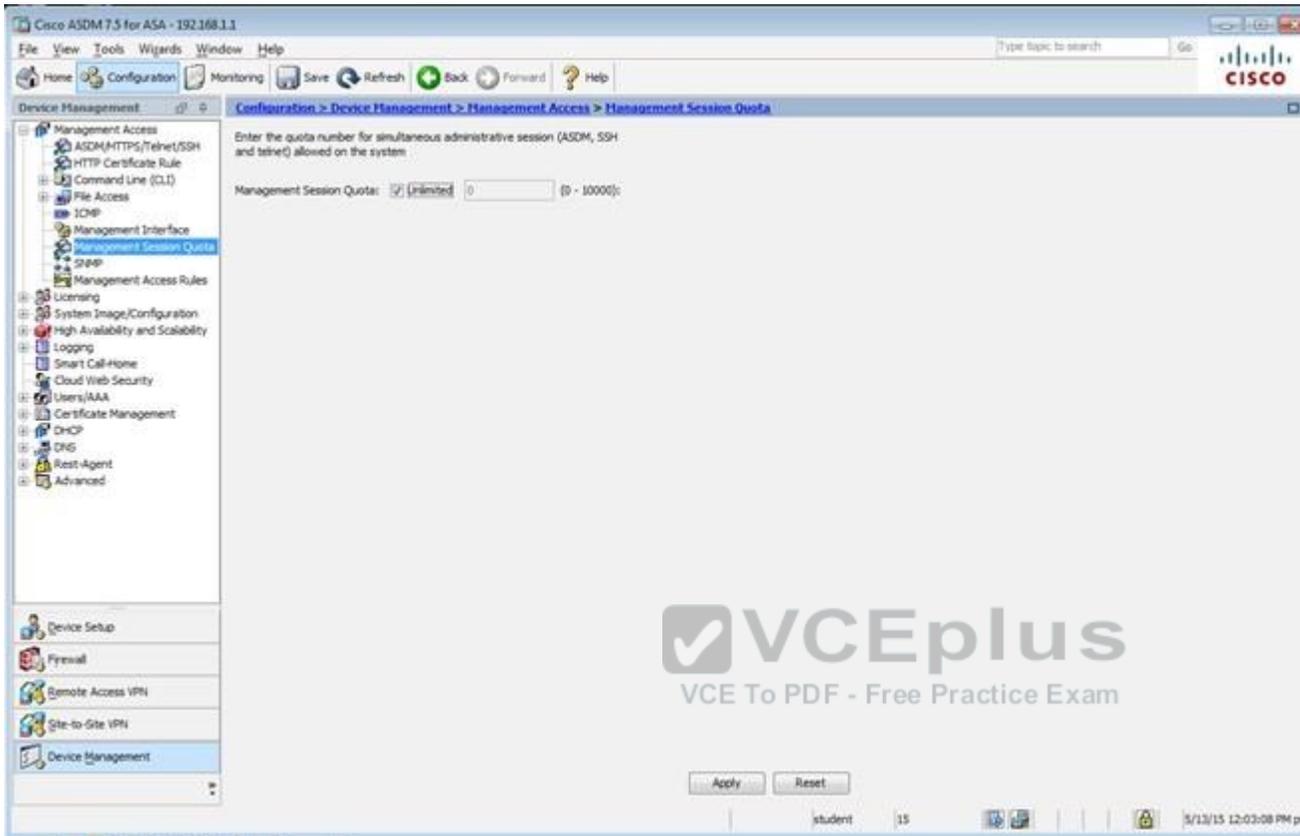
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation is "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows a tree view of configuration categories, with "Management Access" selected. The main content area is titled "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." and contains a table with the following data:

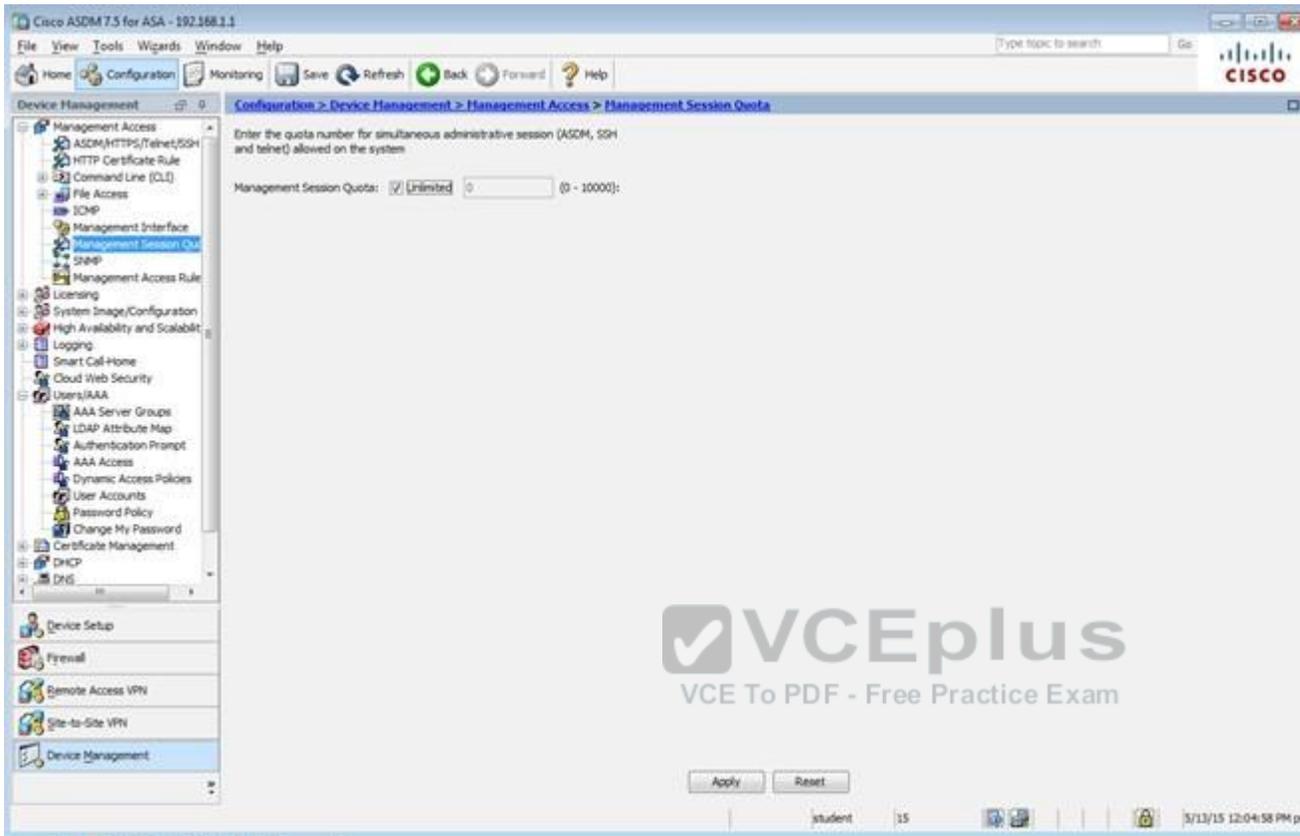
Type	Interface	IP Address	Mask/Prefix Length
Telnet	mgmt	10.10.10.1	255.255.255.255
SSH	inside	192.168.1.2	255.255.255.255
ASDM/HTTPS	inside	192.168.1.0	255.255.255.0

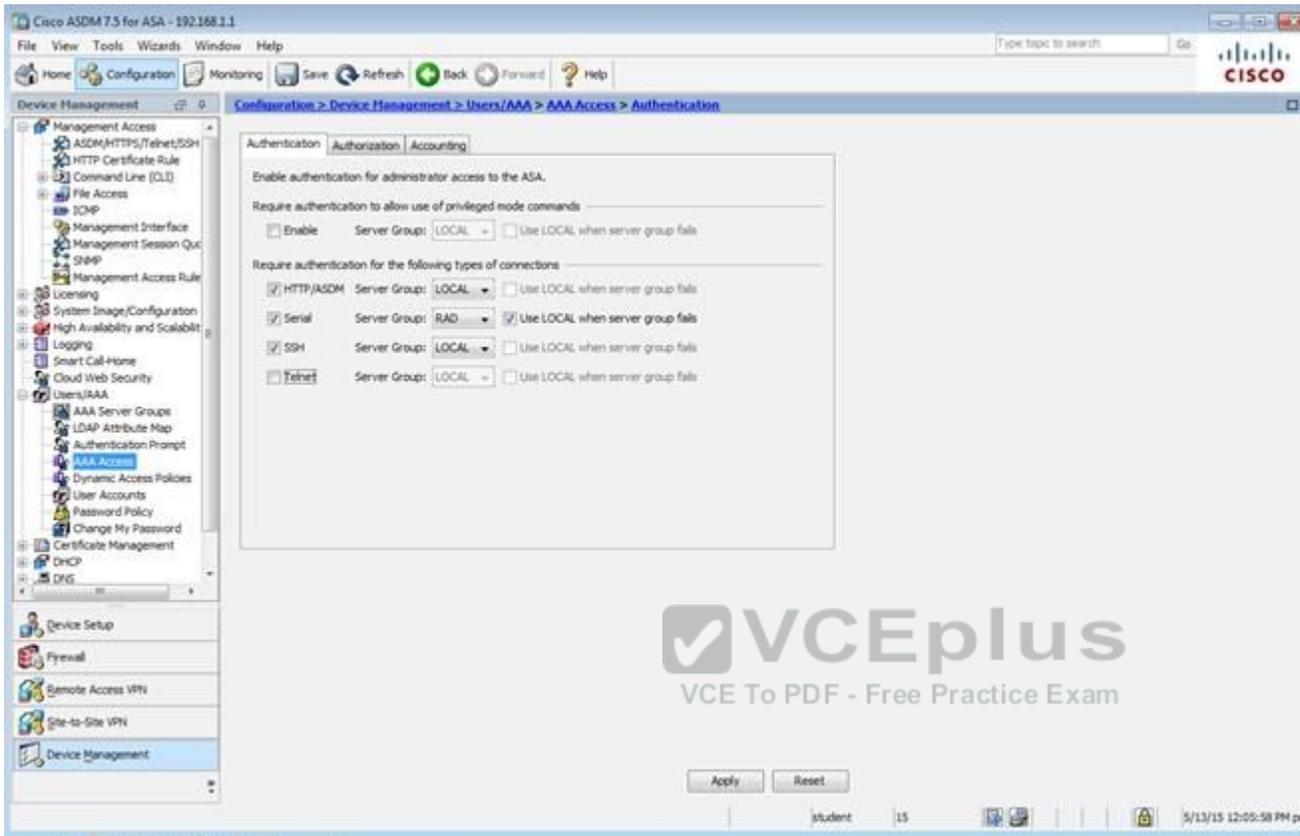
Below the table are "Add", "Edit", and "Delete" buttons. Further down, there are sections for "Http Settings" (with "Enable HTTP Server" checked, Port Number: 443, Idle Timeout: 20 minutes, and "Require client certificate to access ASDM on the following interfaces" section), "Telnet Settings" (Telnet Timeout: 5 minutes), and "SSH Settings" (Allowed SSH Version(s): 1&2, SSH Timeout: 5 minutes, and DH Key Exchange: Group 1 selected). "Apply" and "Reset" buttons are at the bottom. A large "VCEplus" watermark is overlaid on the right side of the interface.

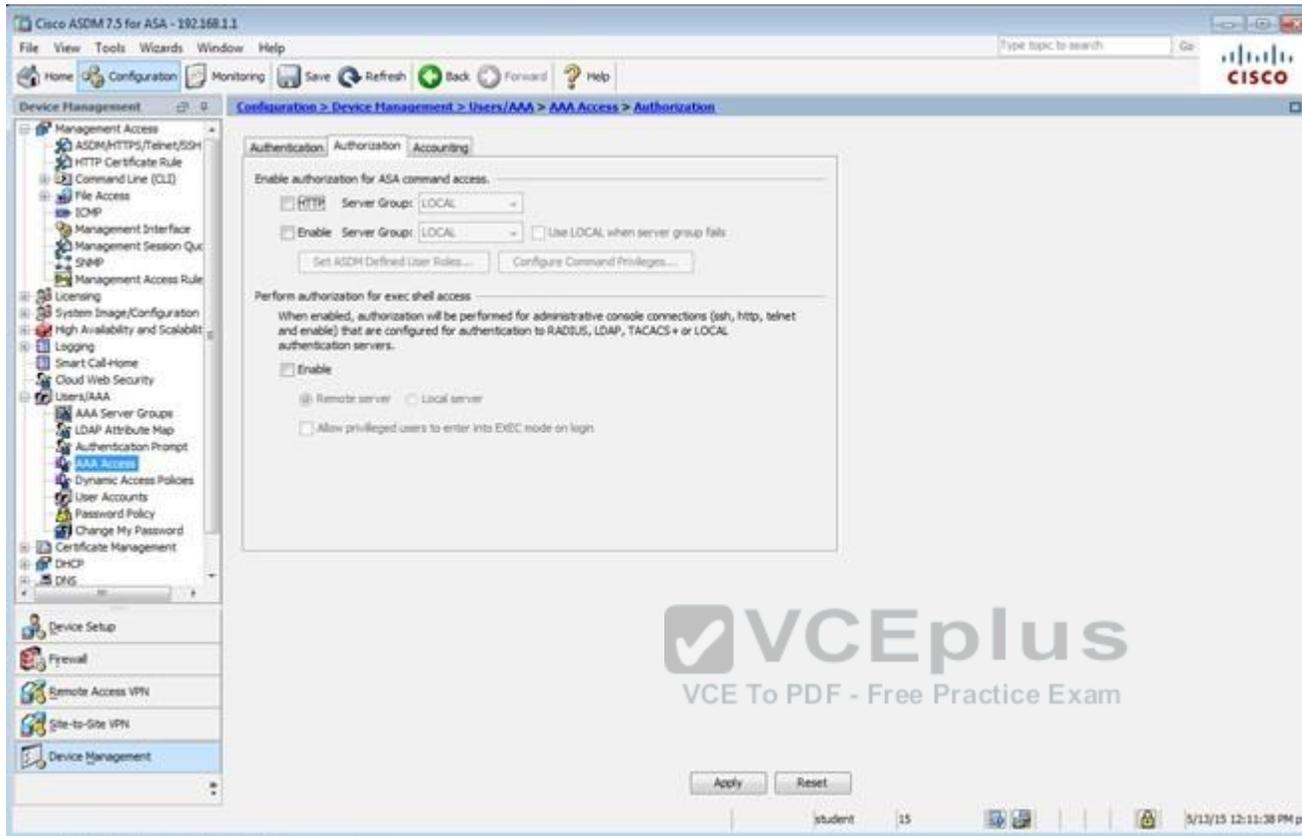








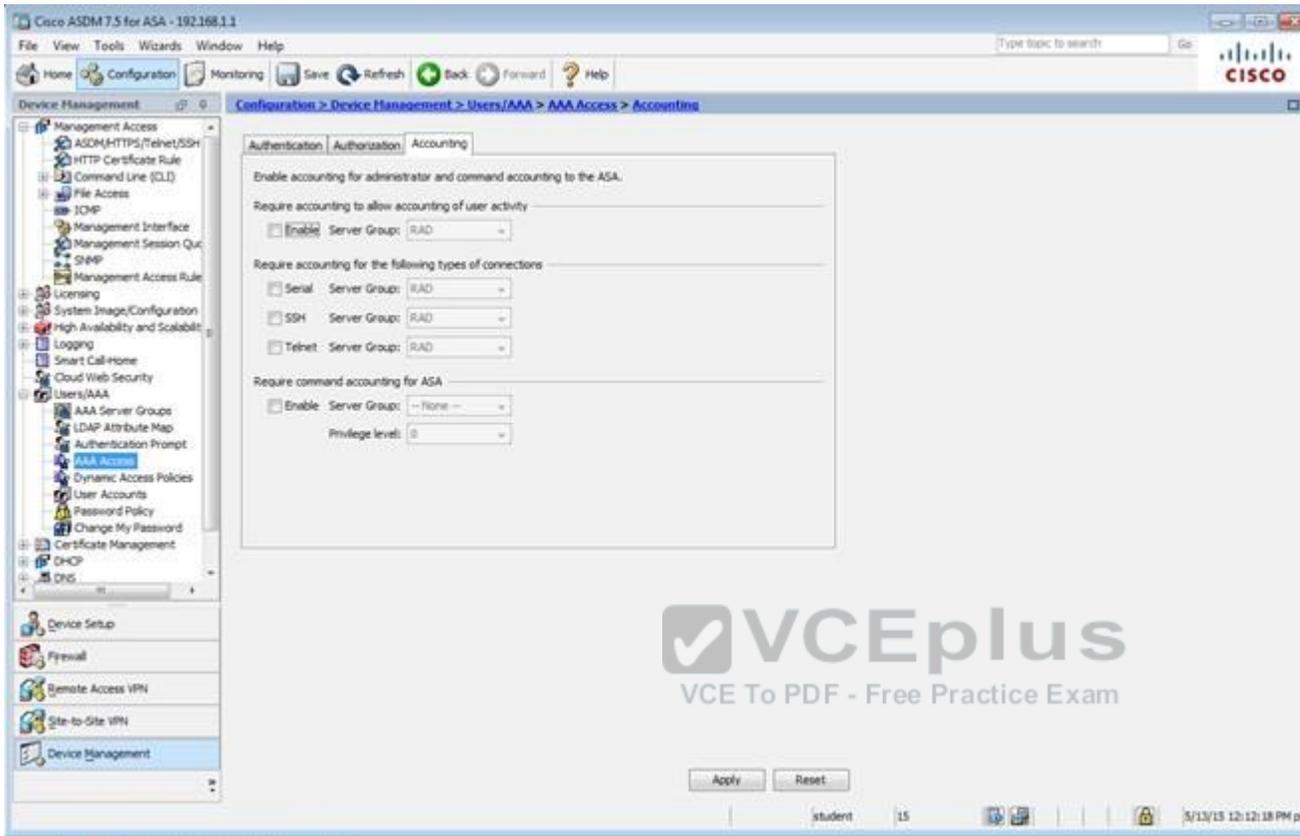




The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The title bar reads "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation path is "Configuration > Device Management > Users/AAA > AAA Access > Authorization". The left sidebar contains a tree view of configuration categories, with "Users/AAA" expanded to show "AAA Access". The main content area is titled "Authorization" and contains the following configuration options:

- Enable authorization for ASA command access:**
 - HTTP Server Group: LOCAL
 - Enable Server Group: LOCAL Use LOCAL when server group fails
 - Buttons: Set ASDM Defined User Roles... Configure Command Privileges...
- Perform authorization for exec shell access:**
 - When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.
 - Enable
 - Remote server Local server
 - Allow privileged users to enter into EXEC mode on login

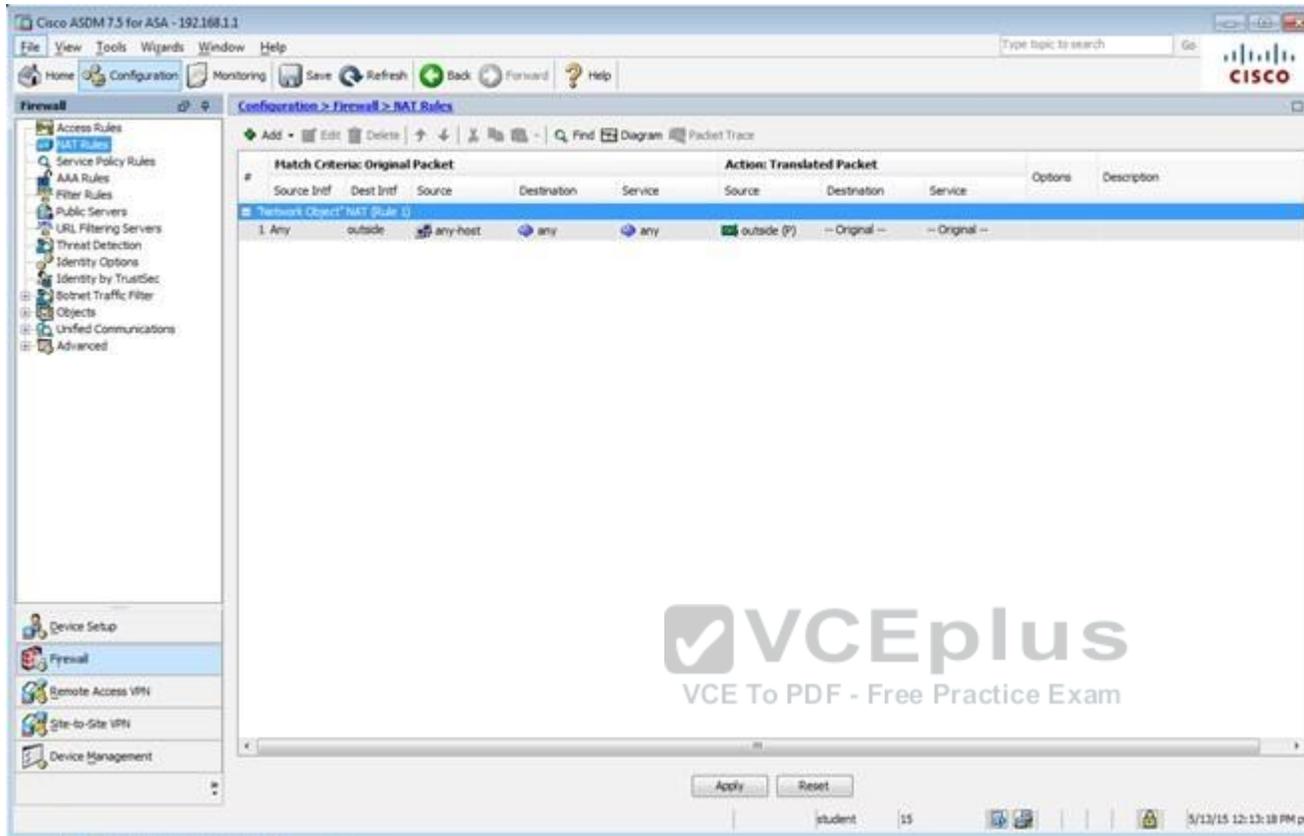
At the bottom of the configuration area are "Apply" and "Reset" buttons. The system tray at the bottom shows the user "student", the page number "15", and the date/time "5/13/15 12:11:38 PM pet".



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The browser title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb path is "Configuration > Device Management > Users/AAA > AAA Access > Accounting". The left sidebar shows a tree view with "Users/AAA" expanded to "AAA Access". The main content area has three tabs: "Authentication", "Authorization", and "Accounting", with "Accounting" selected. The "Accounting" tab contains the following settings:

- Enable accounting for administrator and command accounting to the ASA. **Enable**
- Require accounting to allow accounting of user activity. **Enable** Server Group: RAD
- Require accounting for the following types of connections:
 - Serial Server Group: RAD
 - SSH Server Group: RAD
 - Telnet Server Group: RAD
- Require command accounting for ASA. **Enable** Server Group: -- None -- Privilege level: 0

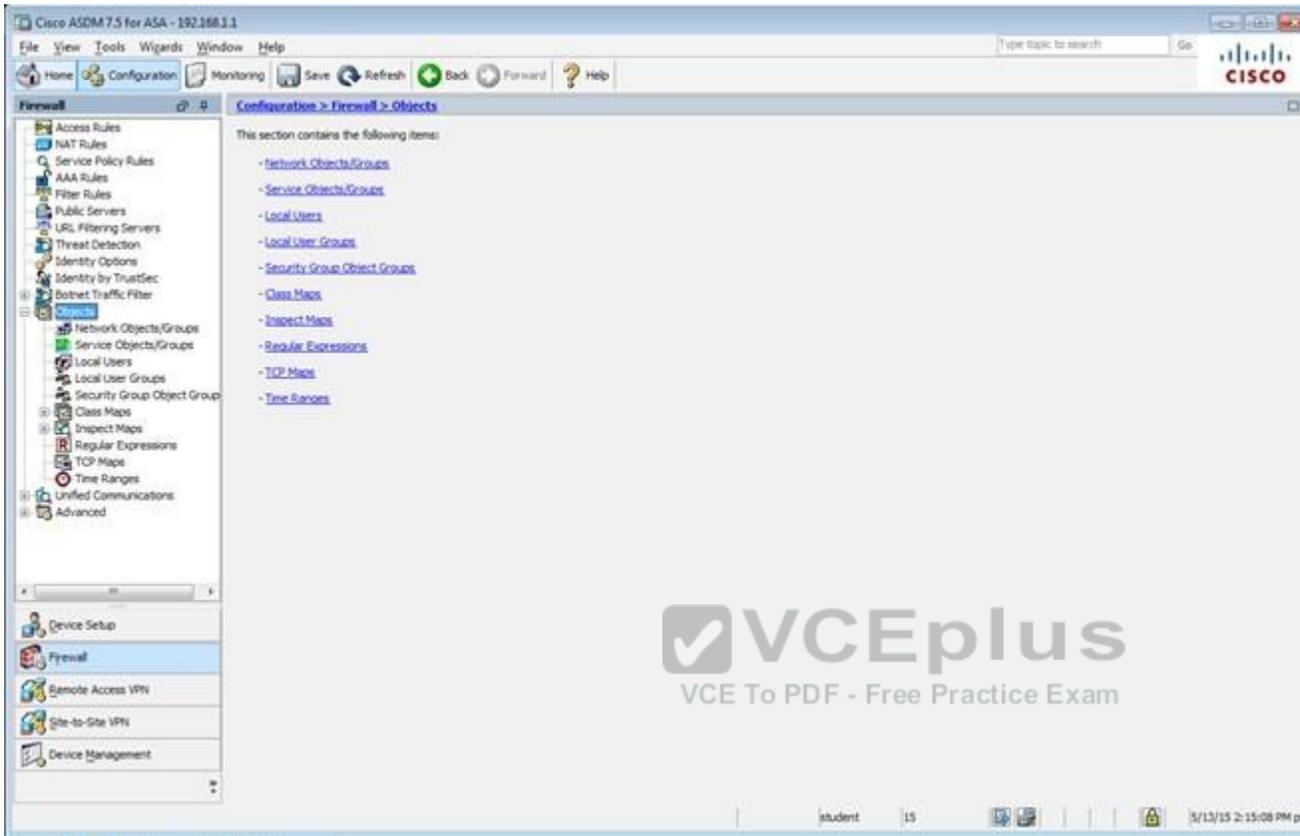
At the bottom of the configuration area are "Apply" and "Reset" buttons. The status bar at the bottom shows "student | 15 | 5/13/15 12:12:18 PM pdt".

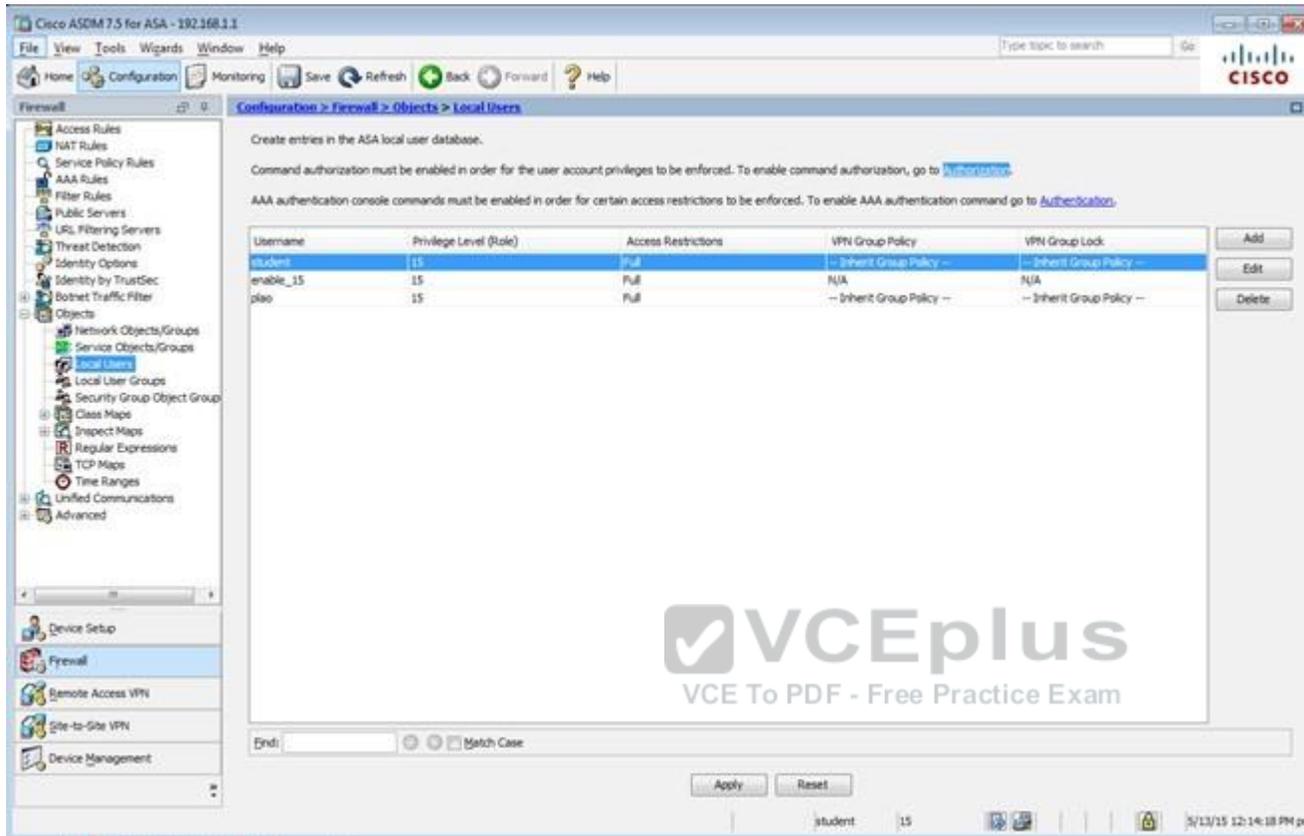


The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for NAT Rules. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table with columns for Match Criteria and Action. The table contains one rule with the following details:

Match Criteria: Original Packet				Action: Translated Packet				Options	Description
Source Intf	Dest Intf	Source	Destination	Source	Destination	Service			
1. Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		

At the bottom of the window, there are 'Apply' and 'Reset' buttons. The status bar at the very bottom shows 'student 15' and the date '5/13/15 12:13:18 PM pet'.





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

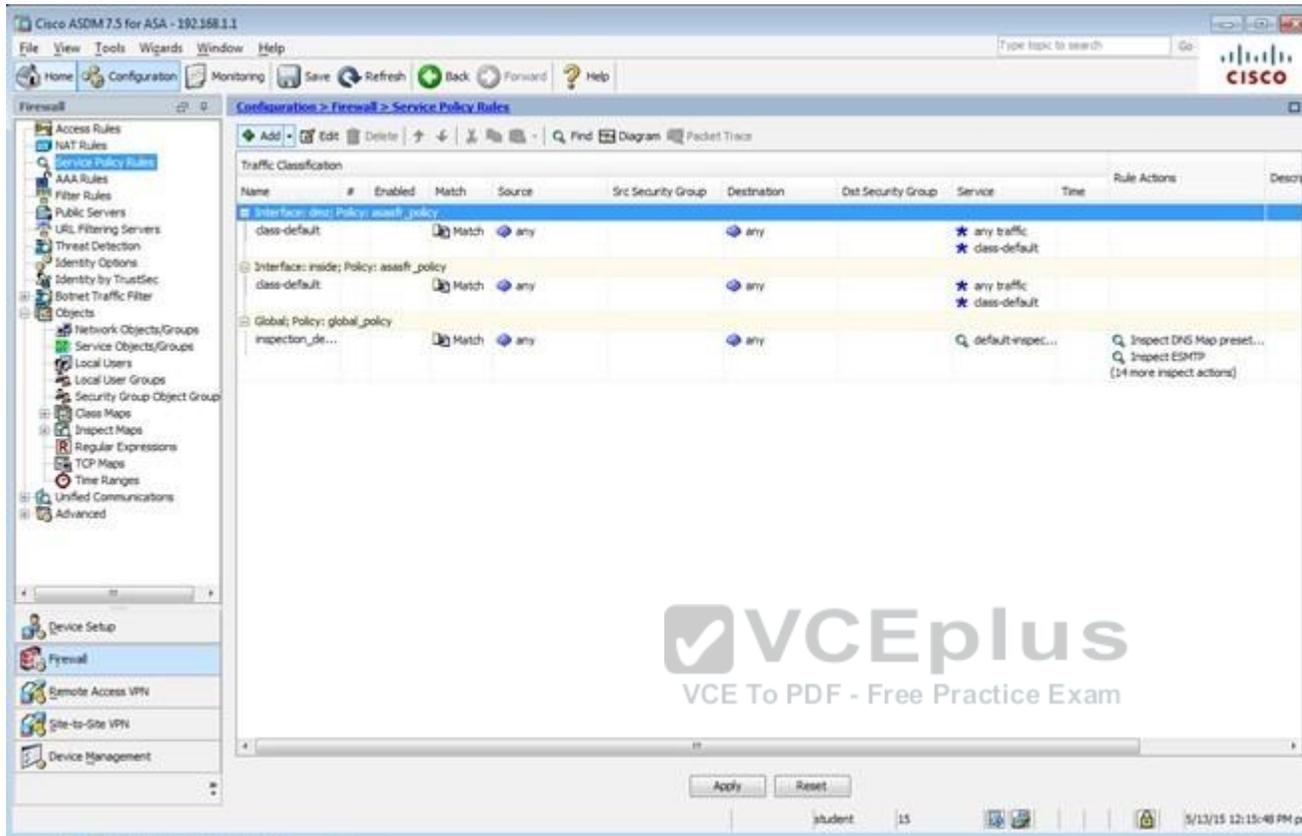
End:

student 15 5/13/15 12:14:18 PM pst

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Objects > Network Objects/Groups". The left sidebar shows a tree view with "Objects" expanded to "Network Objects/Groups". The main content area displays a table of network objects with the following columns: Name, IP Address, Netmask, Description, and Object NAT Address.

Name	IP Address	Netmask	Description	Object NAT Address
any				
any-host	0.0.0.0	0.0.0.0		outside (F)
any4				
any6				
facebook	www.facebook.com			
My_ASA_Demo_Obj	1.10.8.20			

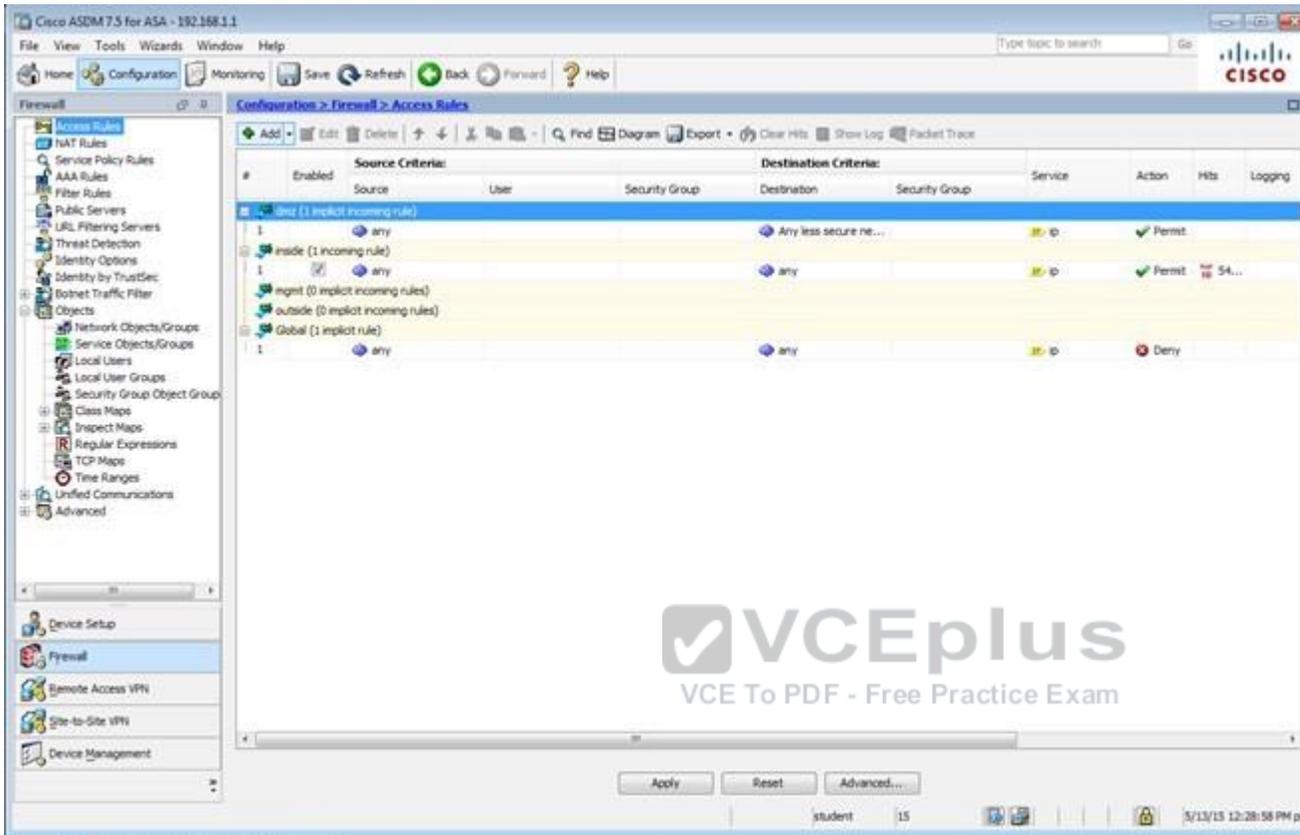
At the bottom of the window, there are "Apply" and "Reset" buttons. The status bar at the bottom right shows the user "student", the page number "15", and the date/time "5/13/15 12:30:08 PM pet".



The screenshot displays the Cisco ASDM 7.5 interface for configuring Service Policy Rules on an ASA device. The left sidebar shows a tree view with 'Service Policy Rules' selected. The main pane shows a table of traffic classification rules.

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Interface: (int); Policy: asastf_policy											
class-default			Match	any		any		any traffic			
Interface: inside; Policy: asaastf_policy											
class-default			Match	any		any		any traffic			
Global; Policy: global_policy											
inspection_de...			Match	any		any		default-inspec...			Inspect DNS Map preset... Inspect ESMTP (14 more inspect actions)

At the bottom of the window, there are 'Apply' and 'Reset' buttons, and a status bar showing 'student | 15 | 5/13/15 12:15:48 PM pst'.



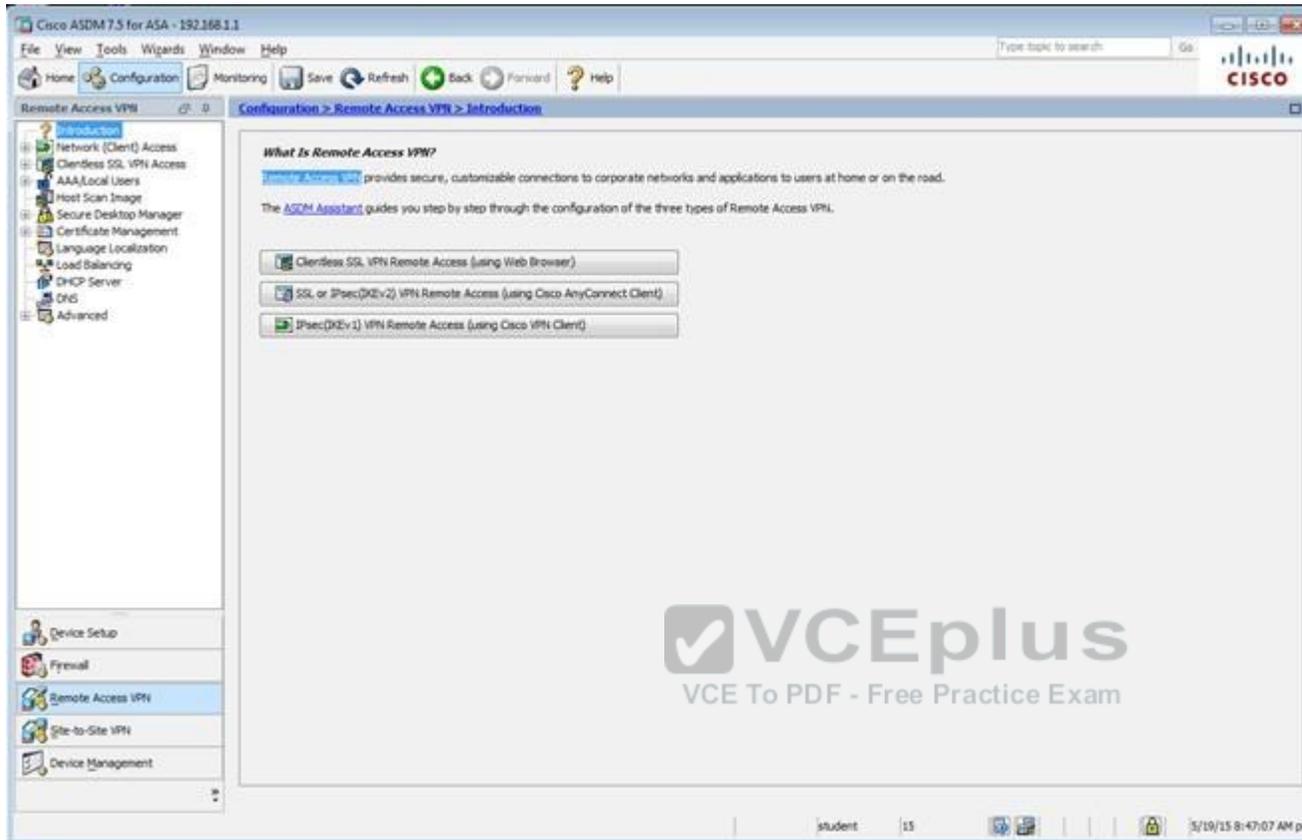
Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

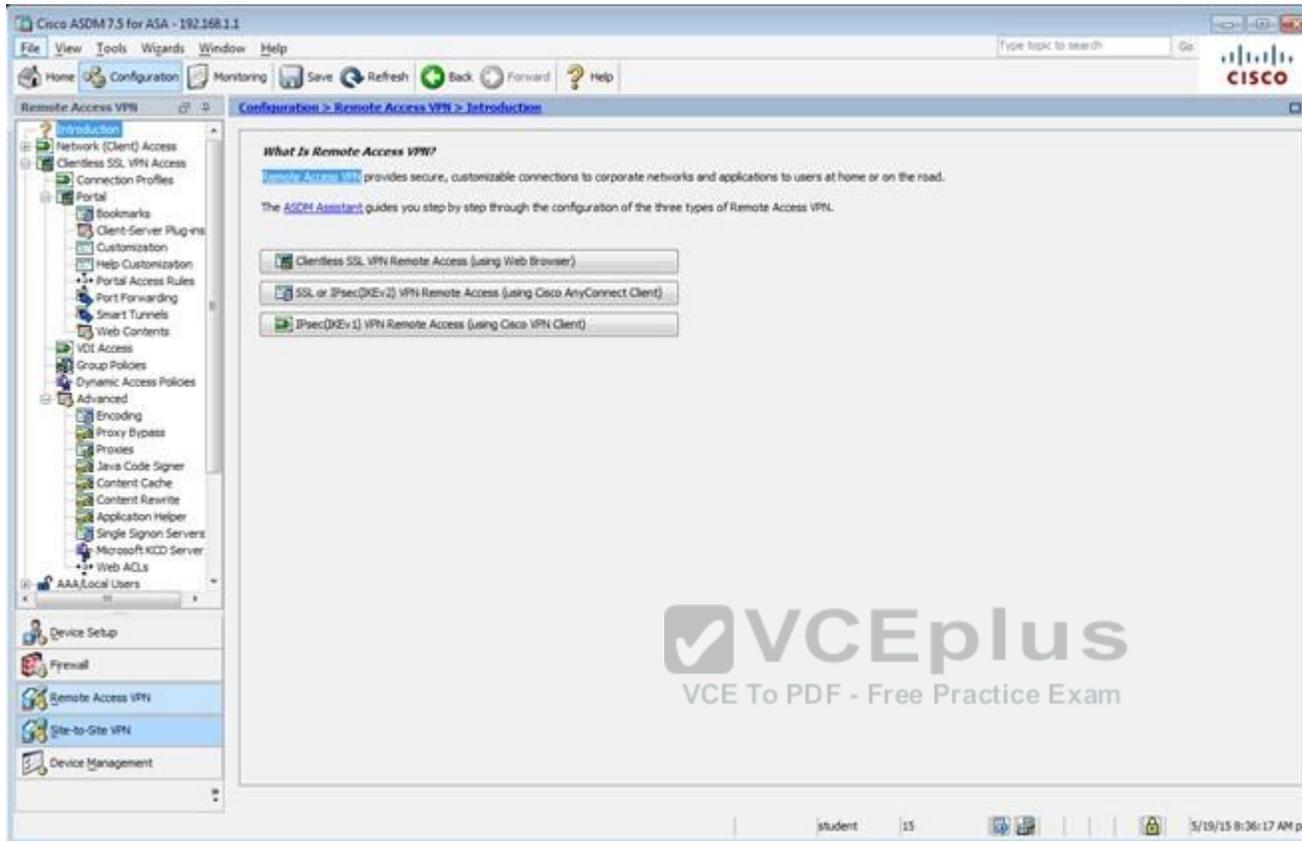
#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group				
ibzz (1 implicit incoming rule)										
1	<input checked="" type="checkbox"/>	any			Any less secure ne...		IP	Permit		
inside (1 incoming rule)										
1	<input checked="" type="checkbox"/>	any			any		IP	Permit	54...	
ingnt (0 implicit incoming rules)										
outside (0 implicit incoming rules)										
Global (1 implicit rule)										
1	<input checked="" type="checkbox"/>	any			any		IP	Deny		

Apply Reset Advanced...

student 15 3/13/15 12:28:58 PM pdt



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 web interface. The main content area is titled "Remote Access VPN" and "Configuration > Remote Access VPN > Introduction". It includes a navigation pane on the left with categories like "Network (Client) Access", "Clientless SSL VPN Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". Below these are "Device Setup", "Firewall", "Remote Access VPN", "Site-to-Site VPN", and "Device Management". The main content area contains the heading "What Is Remote Access VPN?" and a paragraph: "Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road. The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN." Below this text are three buttons: "Clientless SSL VPN Remote Access (Using Web Browser)", "SSL or IPsec (IKEv2) VPN Remote Access (Using Cisco AnyConnect Client)", and "IPsec (IKEv1) VPN Remote Access (Using Cisco VPN Client)". A large "VCEplus VCE To PDF - Free Practice Exam" watermark is overlaid on the bottom right of the interface. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:07 AM pet".



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The breadcrumb trail is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area is divided into three sections:

- Access Interfaces:** A table to enable interfaces for clientless SSL VPN access.

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

 Below the table are buttons for 'Device Certificate ...' and 'Port Setting ...'. A checkbox 'Bypass interface access lists for inbound VPN sessions' is checked. A note states: '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 can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete, Find: [text box], Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
DefaultVEBVPNGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
test	<input checked="" type="checkbox"/>	test	AAA(LOCAL)	DfltGrpPolicy

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

At the bottom are 'Apply' and 'Reset' buttons. The status bar shows 'student | 15 | 5/19/15 8:38:47 AM pet'.

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL Manage...
 Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS Manage...
(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2
Domain Name: secure-x.local

Default Group Policy

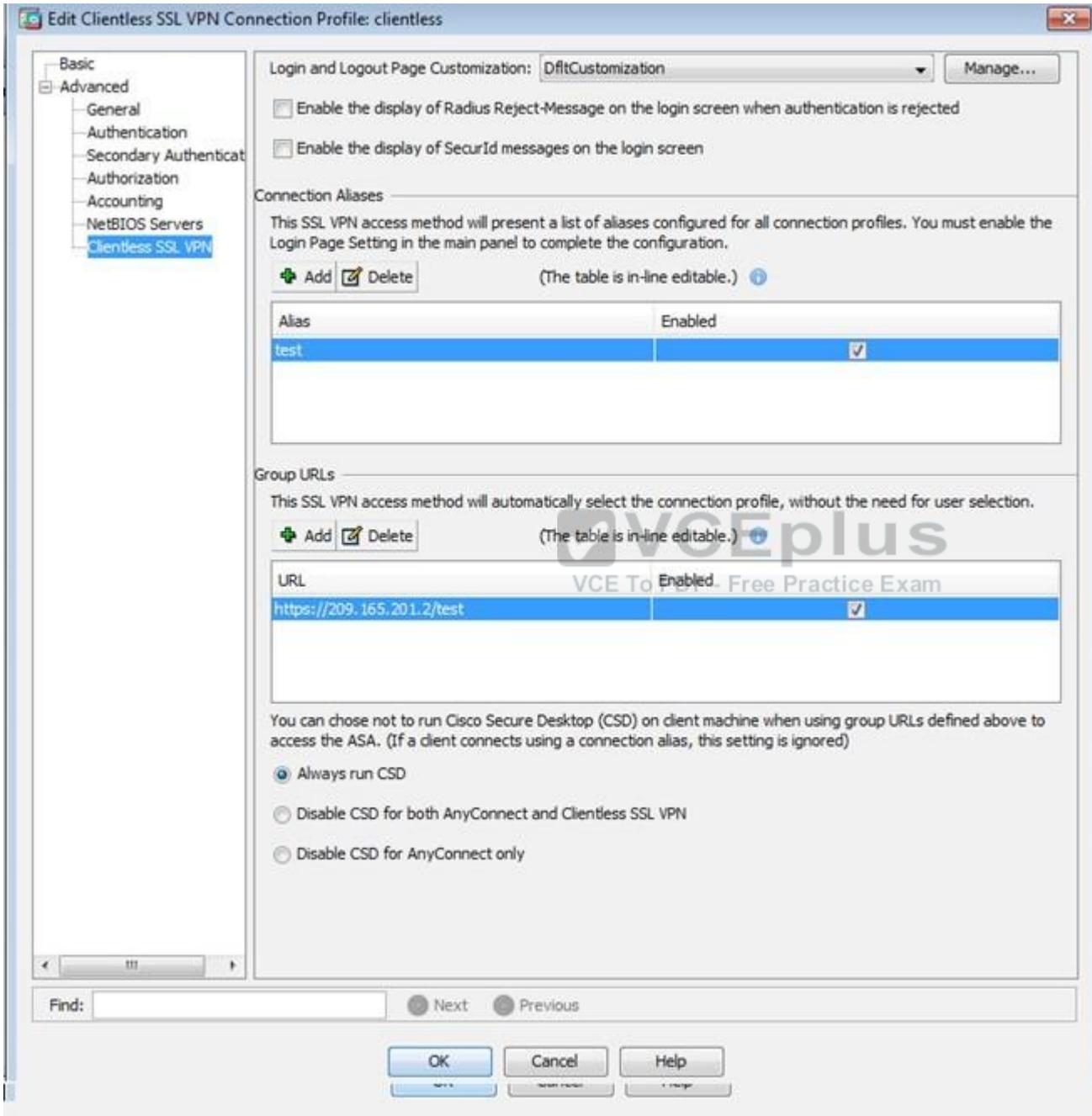
Group Policy: Sales Manage...
(Following field is an attribute of the group policy selected above.)

Enable clientless SSL VPN protocol

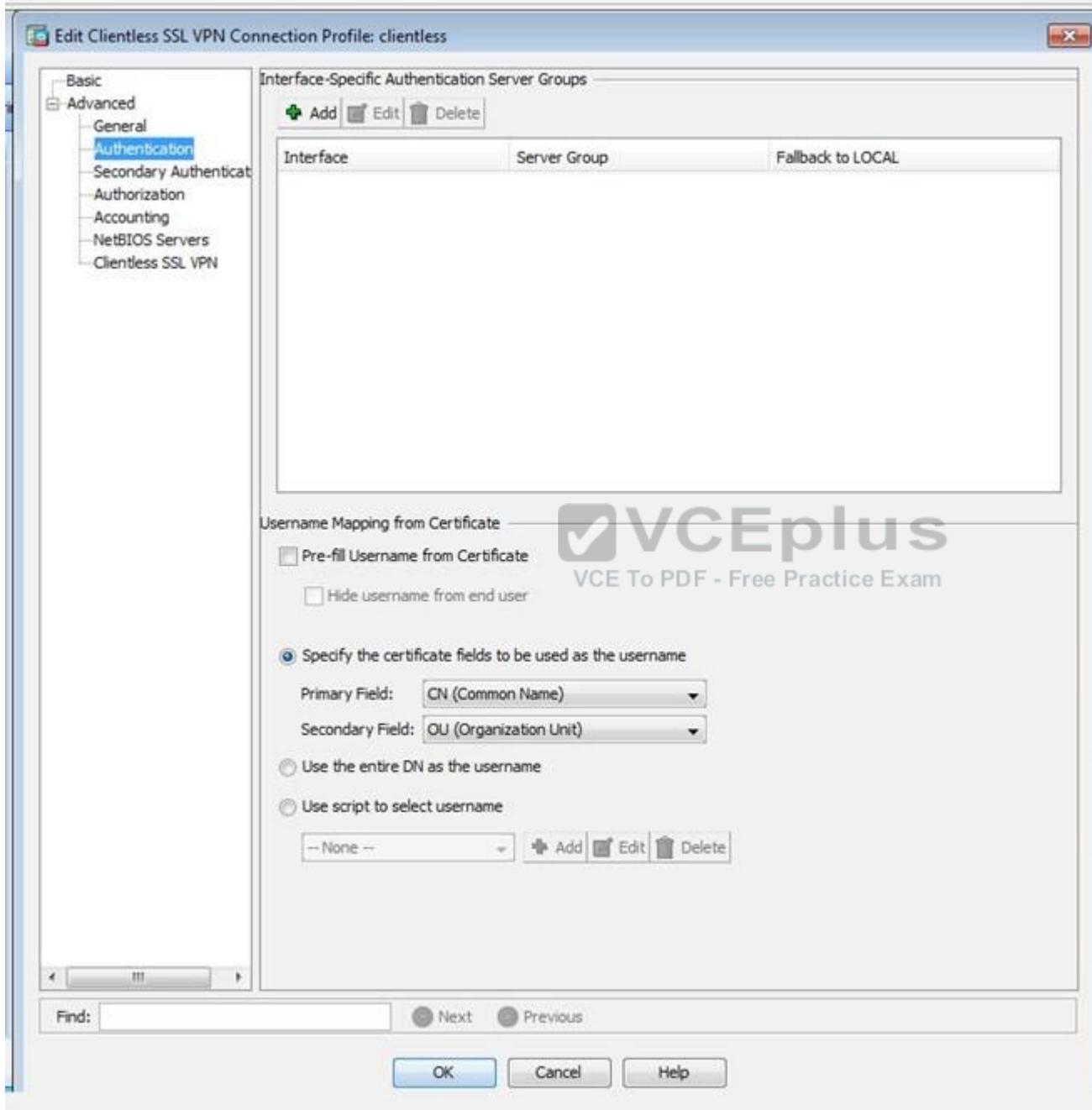
Find: Next Previous

OK Cancel Help

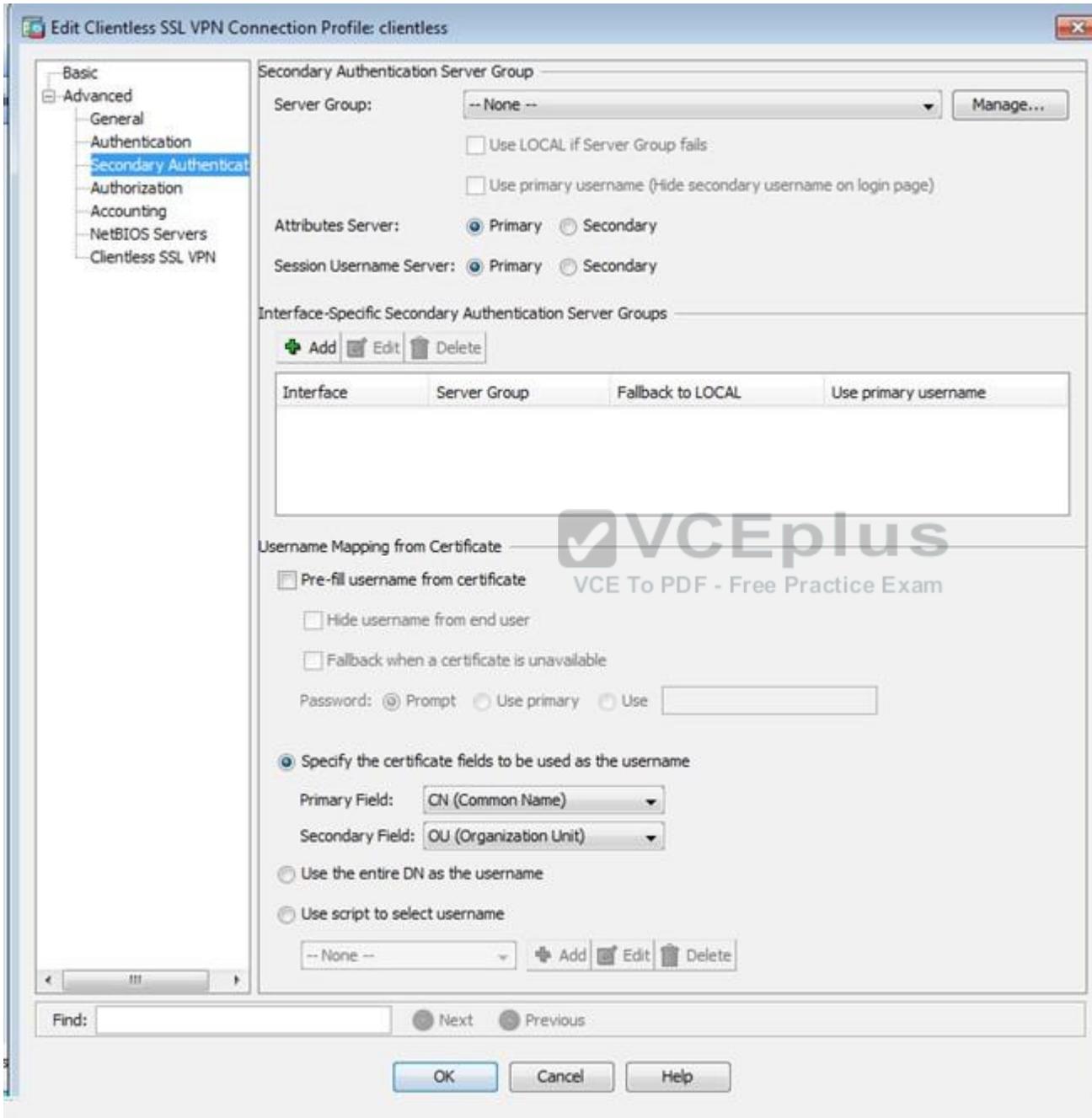


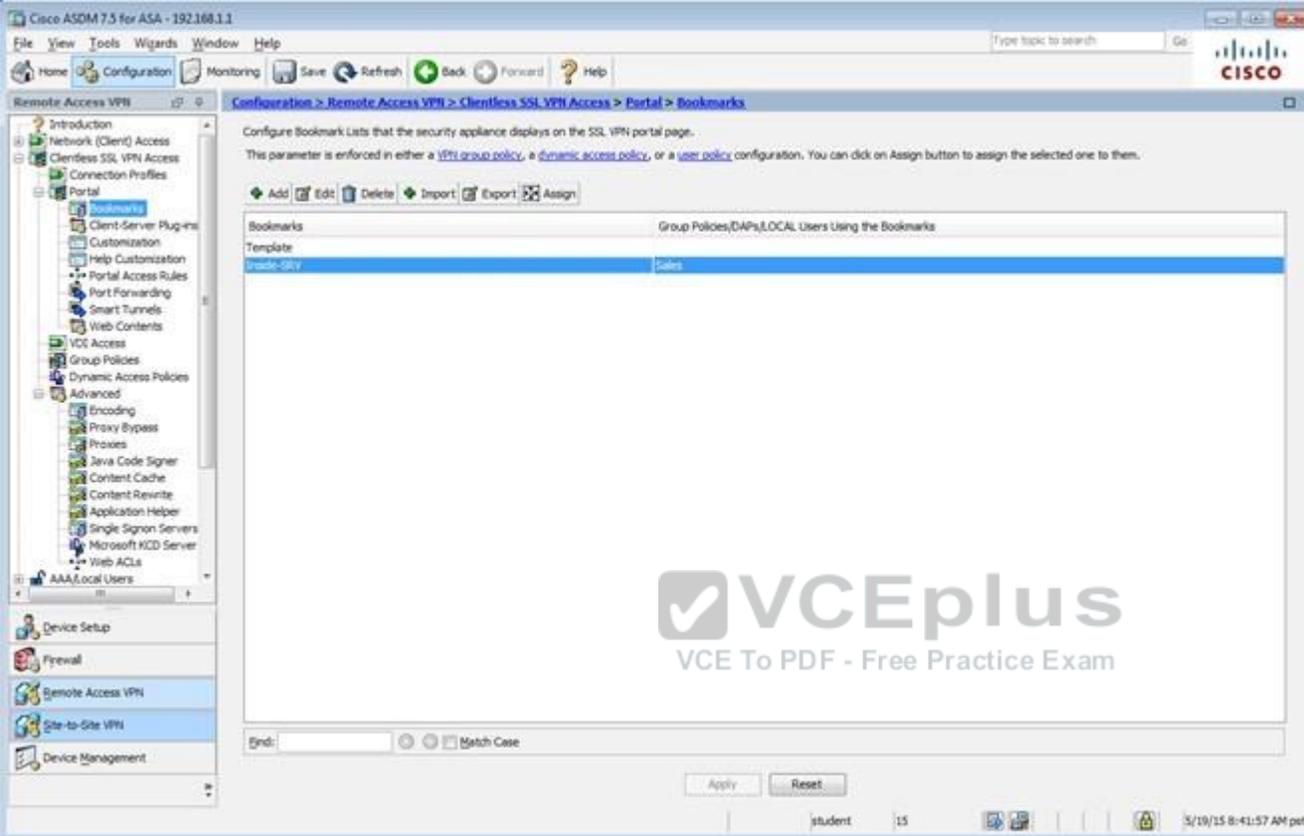










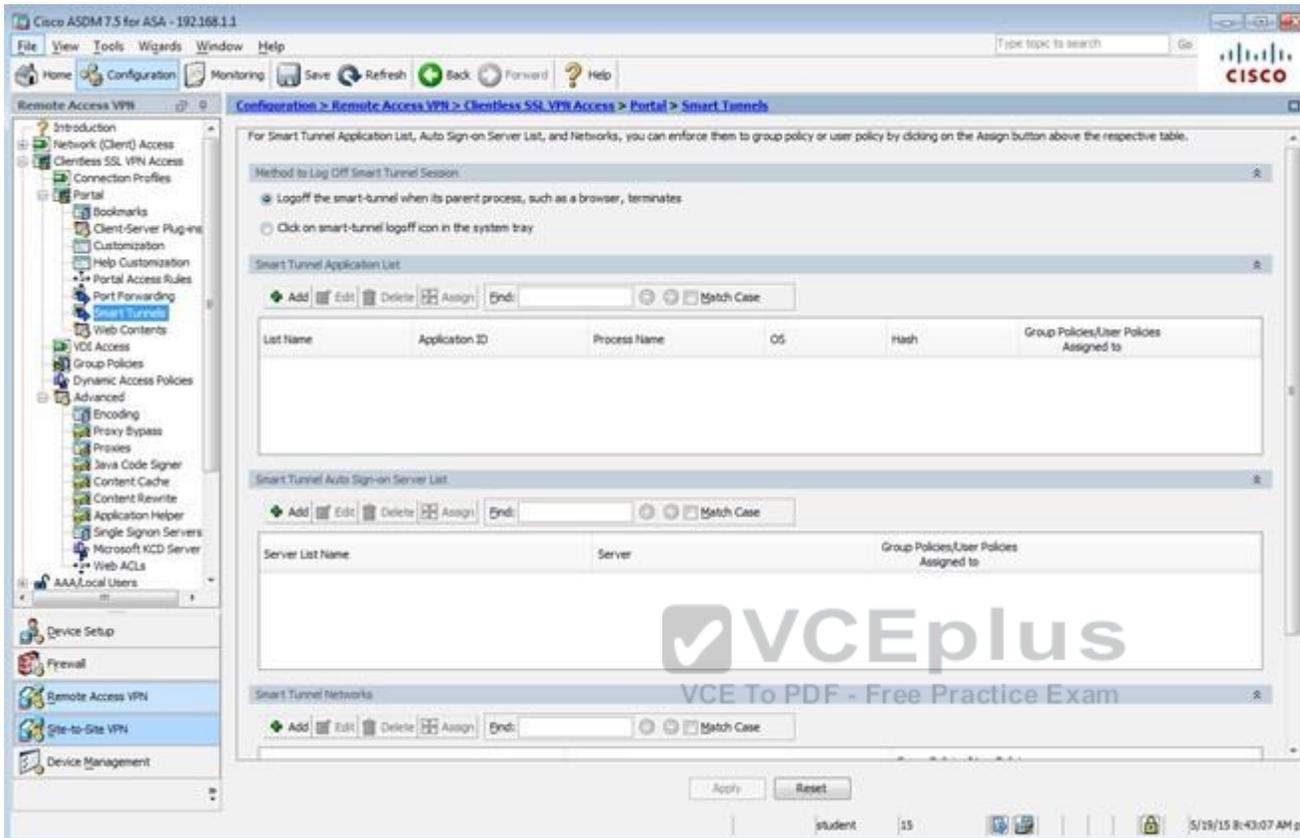


The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The main content area displays the 'Configure Bookmark Lists' configuration page. It includes a table with the following data:

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Inside-01V	Sales

Below the table, there is an 'End:' field and a 'Match Case' checkbox. At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The status bar at the bottom of the window shows 'student 15' and the date/time '5/19/15 8:41:57 AM pet'. A large 'VCEplus VCE To PDF - Free Practice Exam' watermark is overlaid on the center of the screenshot.

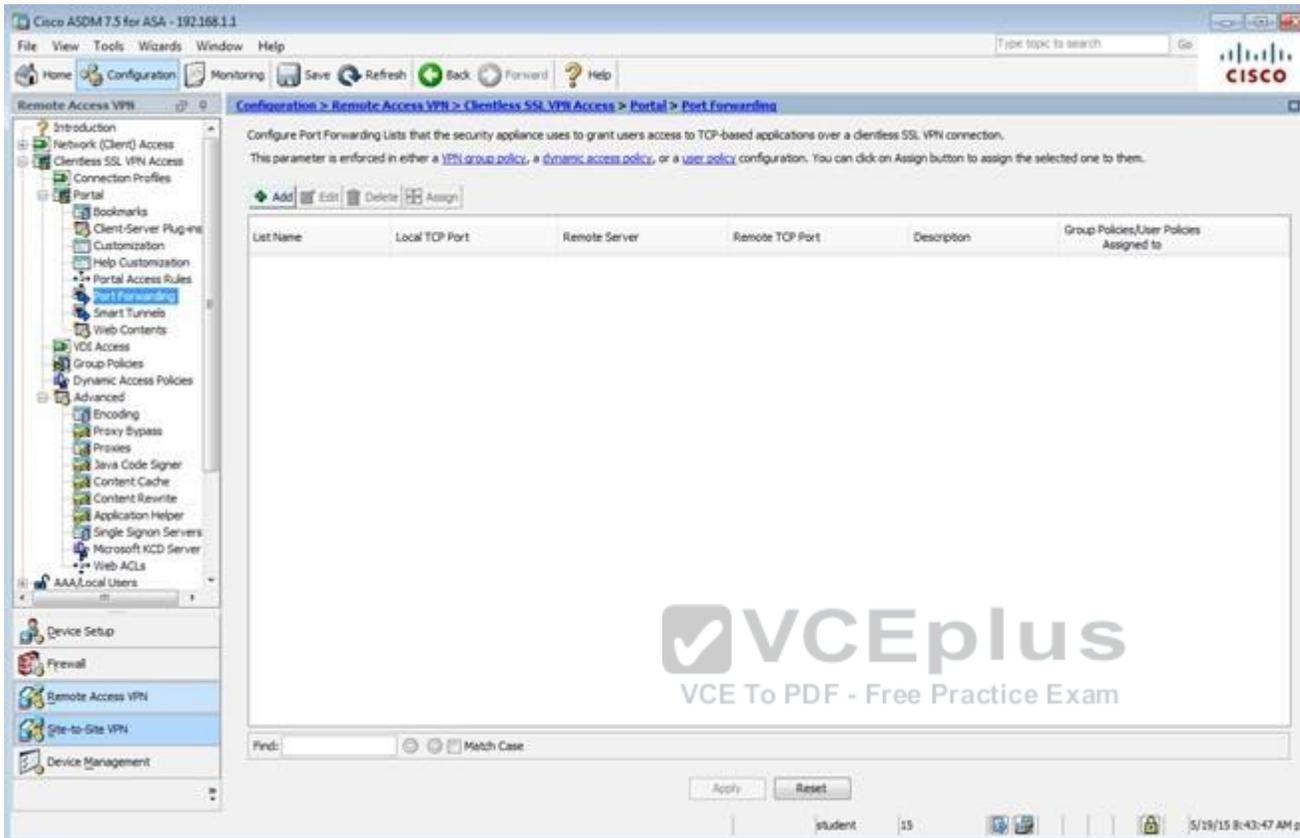




The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The navigation pane on the left shows the configuration path: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels. The main content area is titled "Smart Tunnels" and contains the following sections:

- Method to Log Off Smart Tunnel Session:** Includes radio buttons for "Logoff the smart-tunnel when its parent process, such as a browser, terminates" (selected) and "Click on smart-tunnel logoff icon in the system tray".
- Smart Tunnel Application List:** Features a table with columns: List Name, Application ID, Process Name, OS, Hash, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Auto Sign-on Server List:** Features a table with columns: Server List Name, Server, and Group Policies/User Policies Assigned to. Above the table are controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".
- Smart Tunnel Networks:** Features a table with controls for "Add", "Edit", "Delete", "Assign", "End:", and "Match Case".

At the bottom of the main content area, there are "Apply" and "Reset" buttons. The status bar at the very bottom shows "student | 15 | 5/19/15 8:43:07 AM pst". A large "VCEplus" watermark is overlaid on the center of the screenshot.



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

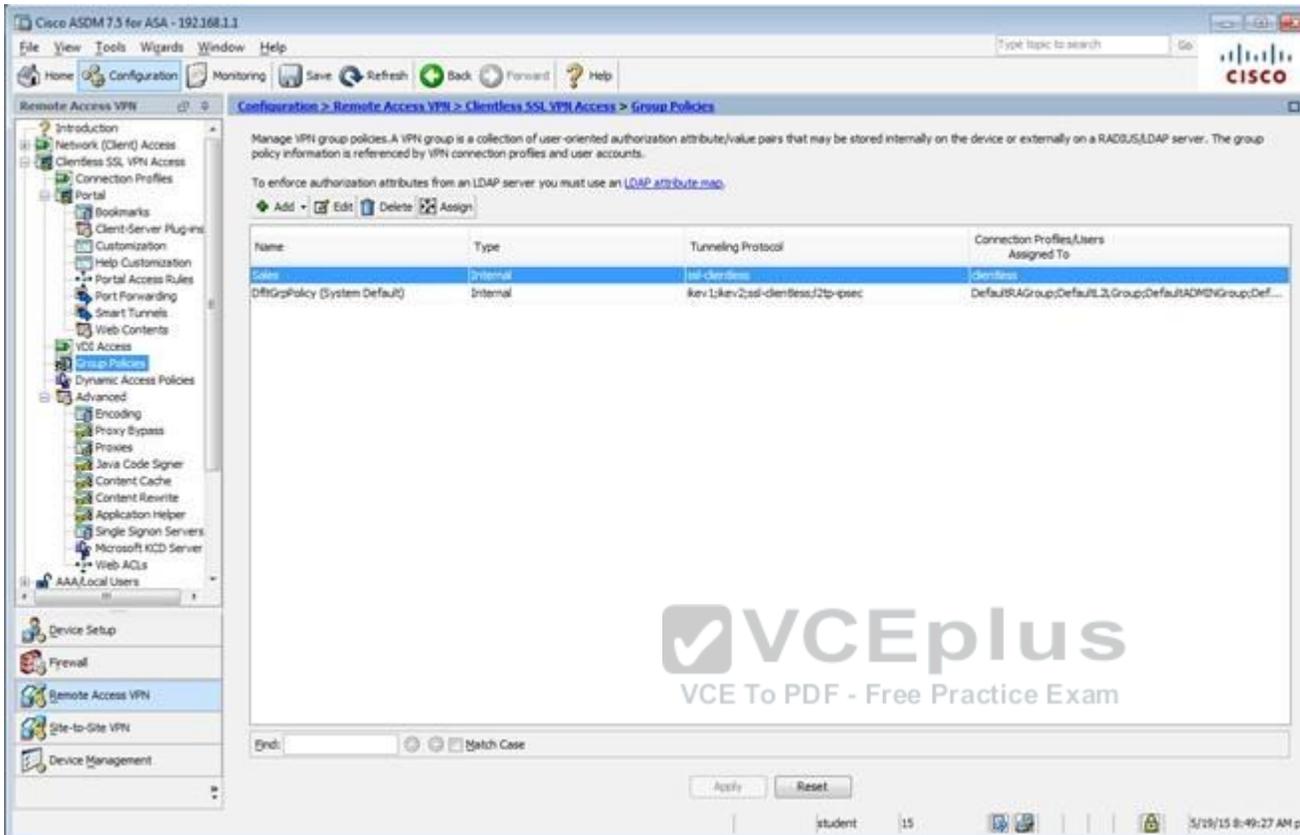
Add Edit Delete Assign

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description	Group Policies/User Policies Assigned to
-----------	----------------	---------------	-----------------	-------------	--

Find: Match Case

Apply Reset

student 15 5/19/15 8:43:47 AM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

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 pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

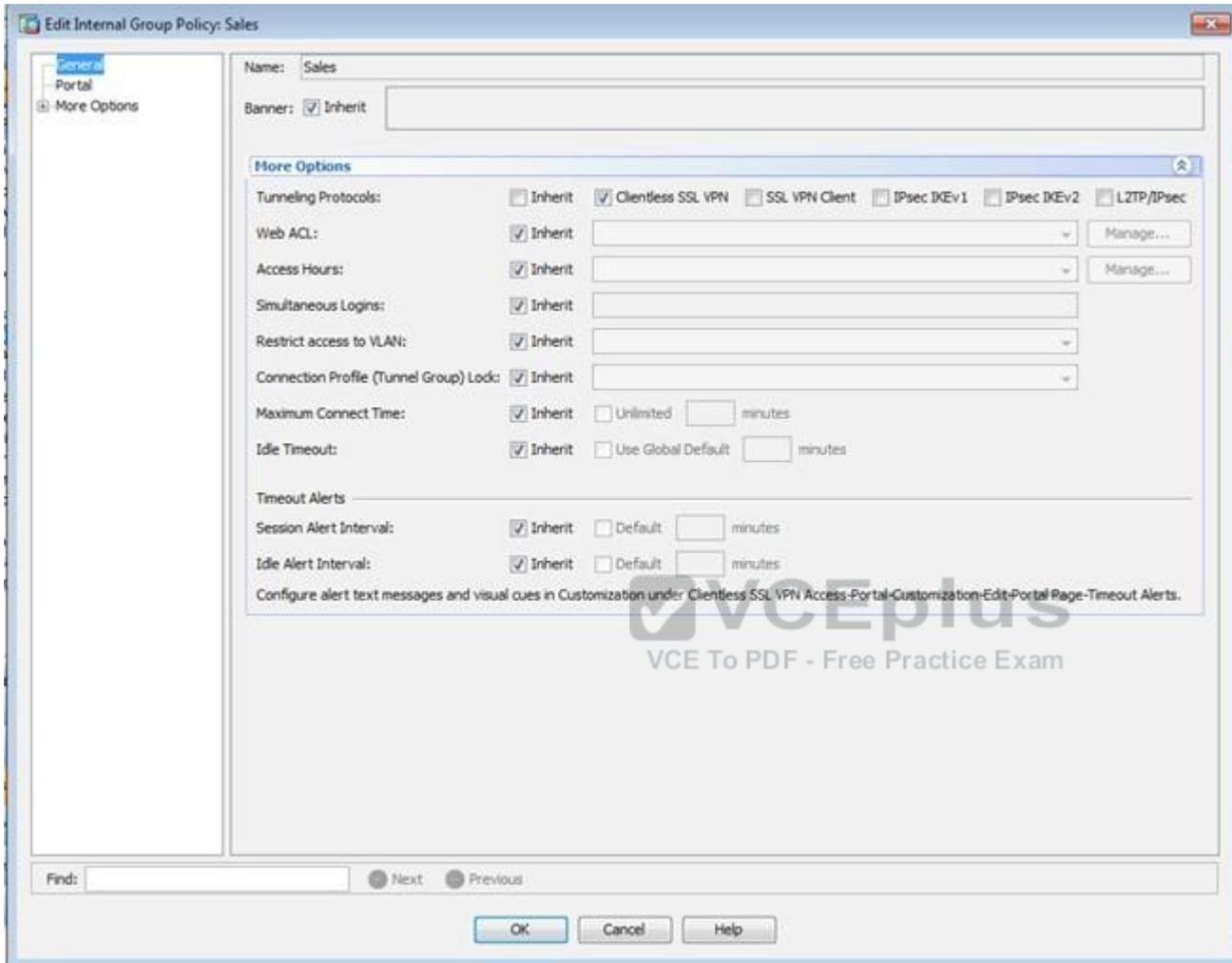
◆ Add ◆ Edit ◆ Delete ◆ Assign

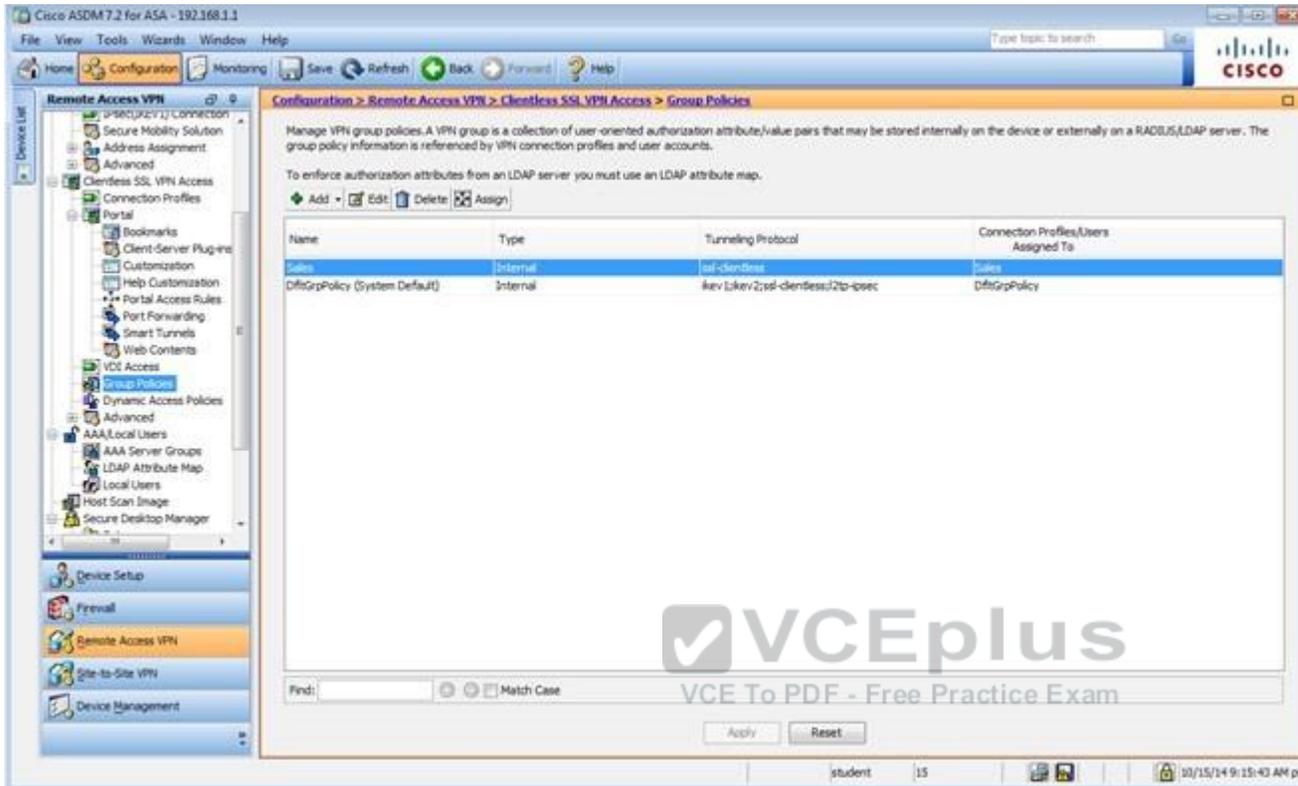
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Clientless	Internal	ssl-clientless	Clientless
DefaultGroupPolicy (System Default)	Internal	kev1okriv2ssl-clientless/2tp-espsec	DefaultRAGroup/DefaultIL2,Group/DefaultADMDNGroup/Def...

End: Match Case

Apply Reset

student 15 5/18/15 8:49:27 AM pst





The screenshot shows the Cisco ASDM 7.2 interface for an ASA device at 192.168.1.1. The navigation pane on the left is expanded to 'Remote Access VPN > Clientless SSL VPN Access > Group Policies'. The main content area displays instructions on managing VPN group policies and a table of existing policies.

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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.

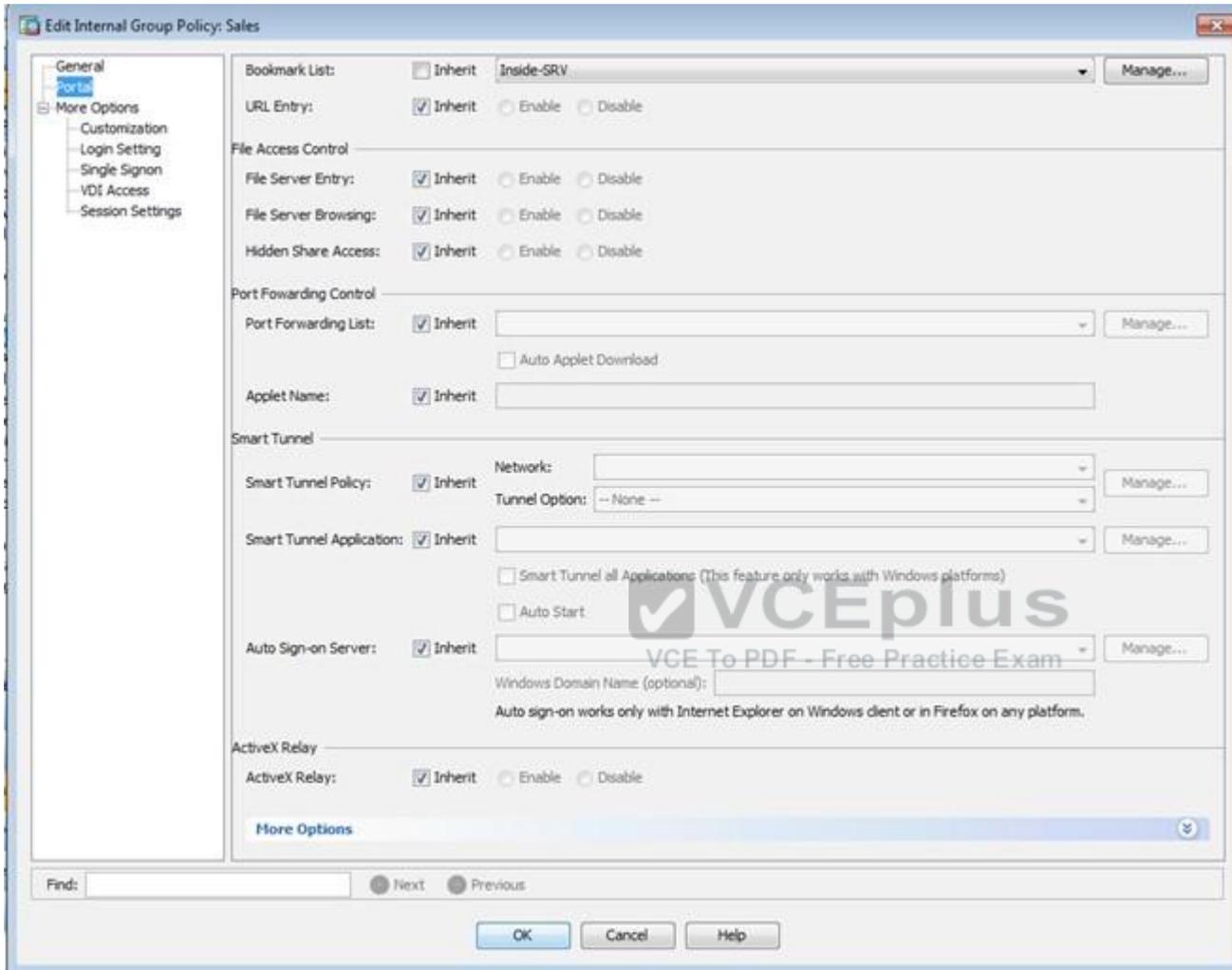
◆ Add ◆ Edit ◆ Delete ◆ Assign

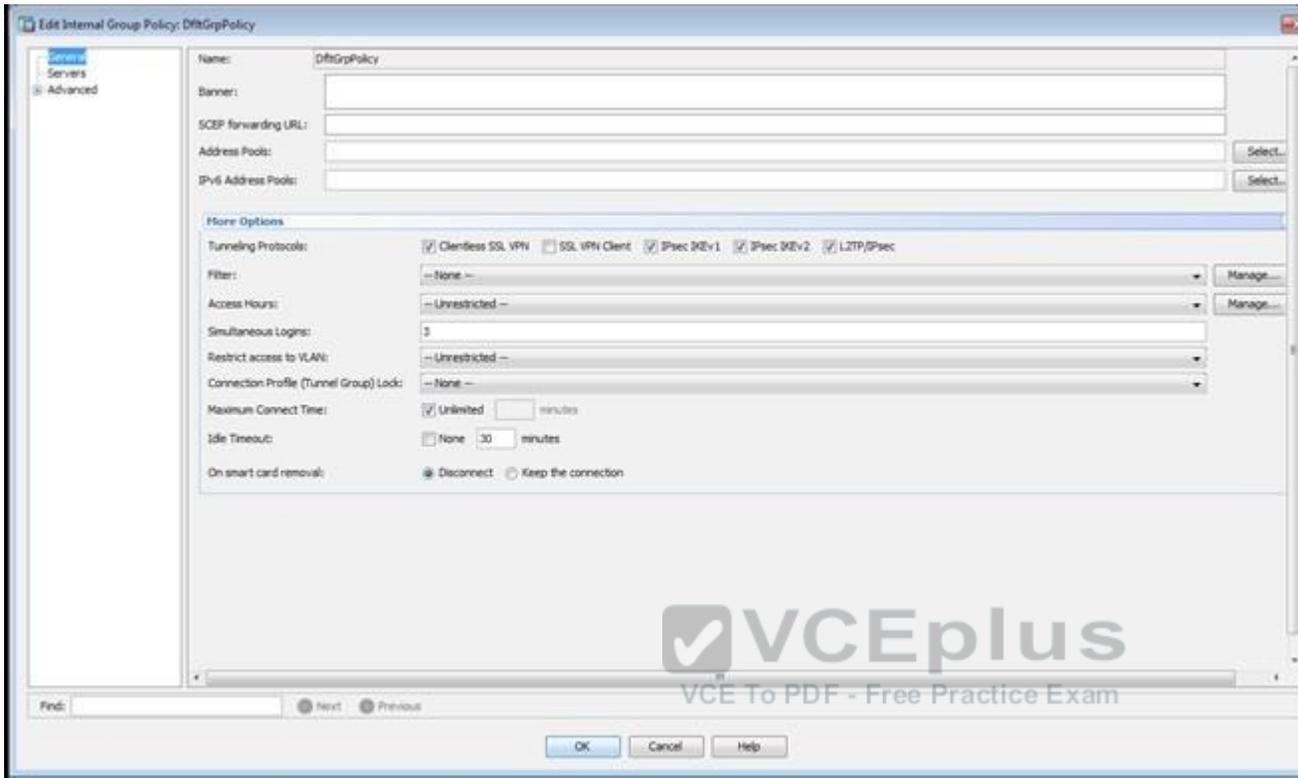
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	l2l-ssl-https	Sales
DfltGrpPolicy (System Default)	Internal	ikev1-ssl-clientless/2ip-sslsec	DfltGrpPolicy

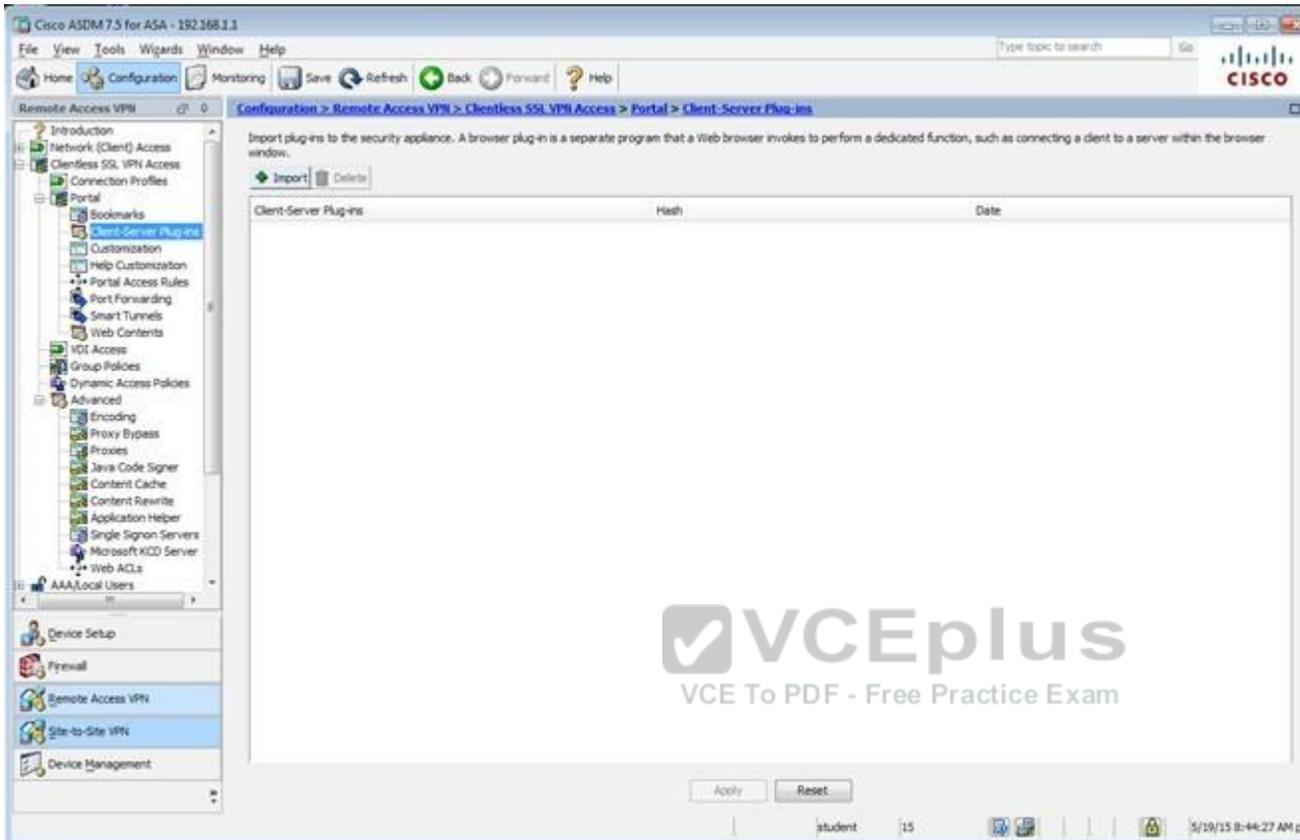
Find: Match Case

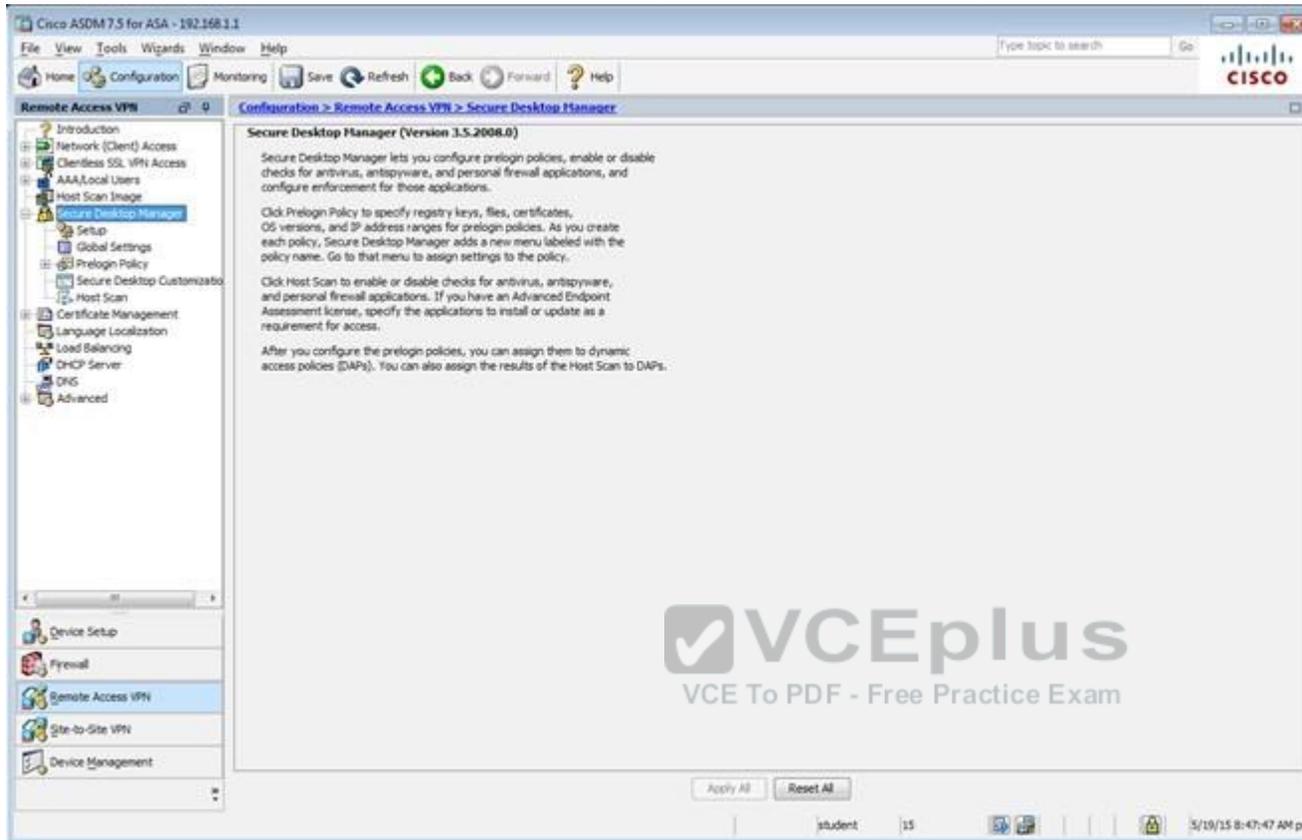
Apply Reset

student | 15 | 30/15/14 9:15:43 AM pst









The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the "Secure Desktop Manager (Version 3.5.2008.0)" configuration page. The left sidebar shows a tree view with "Remote Access VPN" selected, and "Secure Desktop Manager" highlighted under the "Remote Access VPN" section. The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

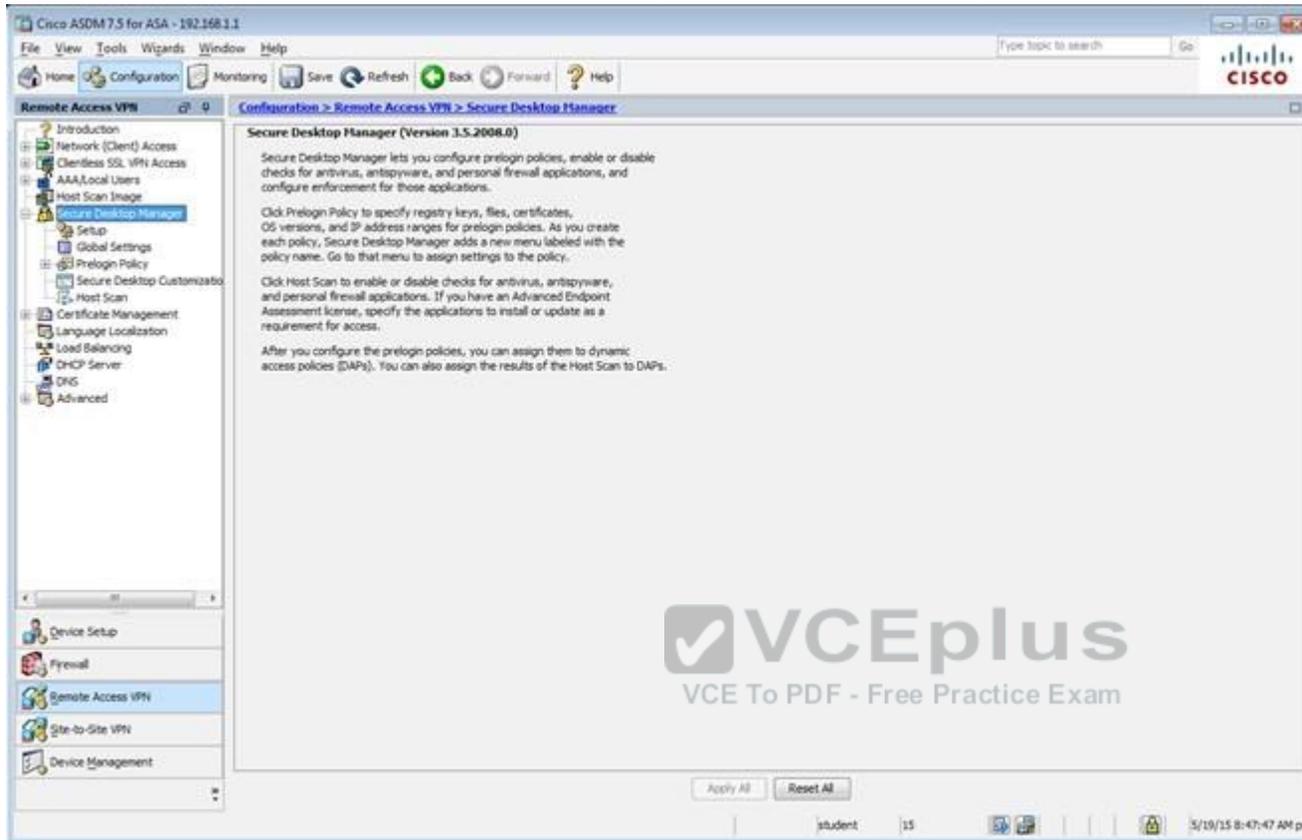
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispam, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispam, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the "Secure Desktop Manager (Version 3.5.2008.0)" configuration page. The page includes a navigation tree on the left with categories like "Remote Access VPN", "Network (Client) Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The "Secure Desktop Manager" section is expanded, showing sub-items: "Introduction", "Setup", "Global Settings", "Prelogin Policy", "Secure Desktop Customization", "Host Scan", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". The main content area contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

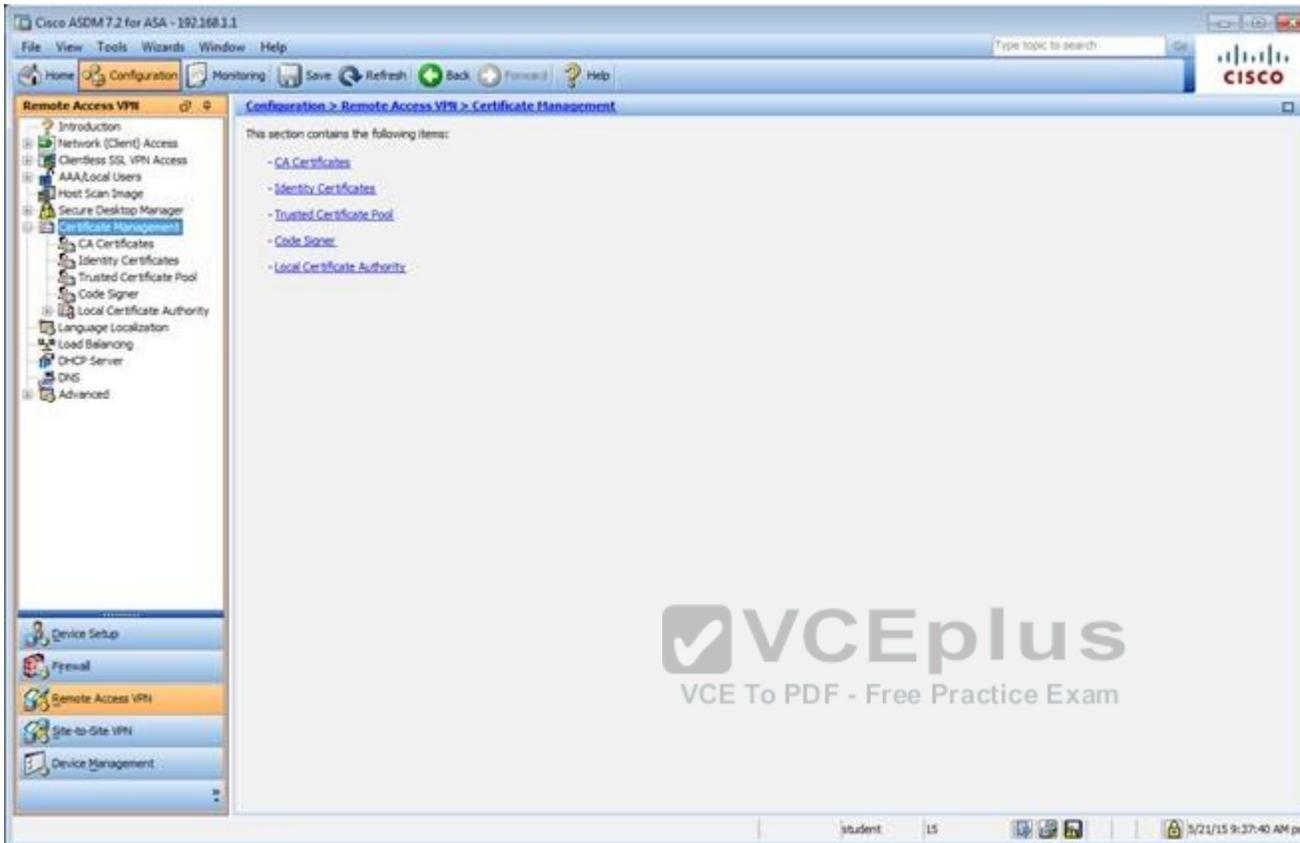
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispam, and personal firewall applications, and configure enforcement for those applications.

Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispam, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

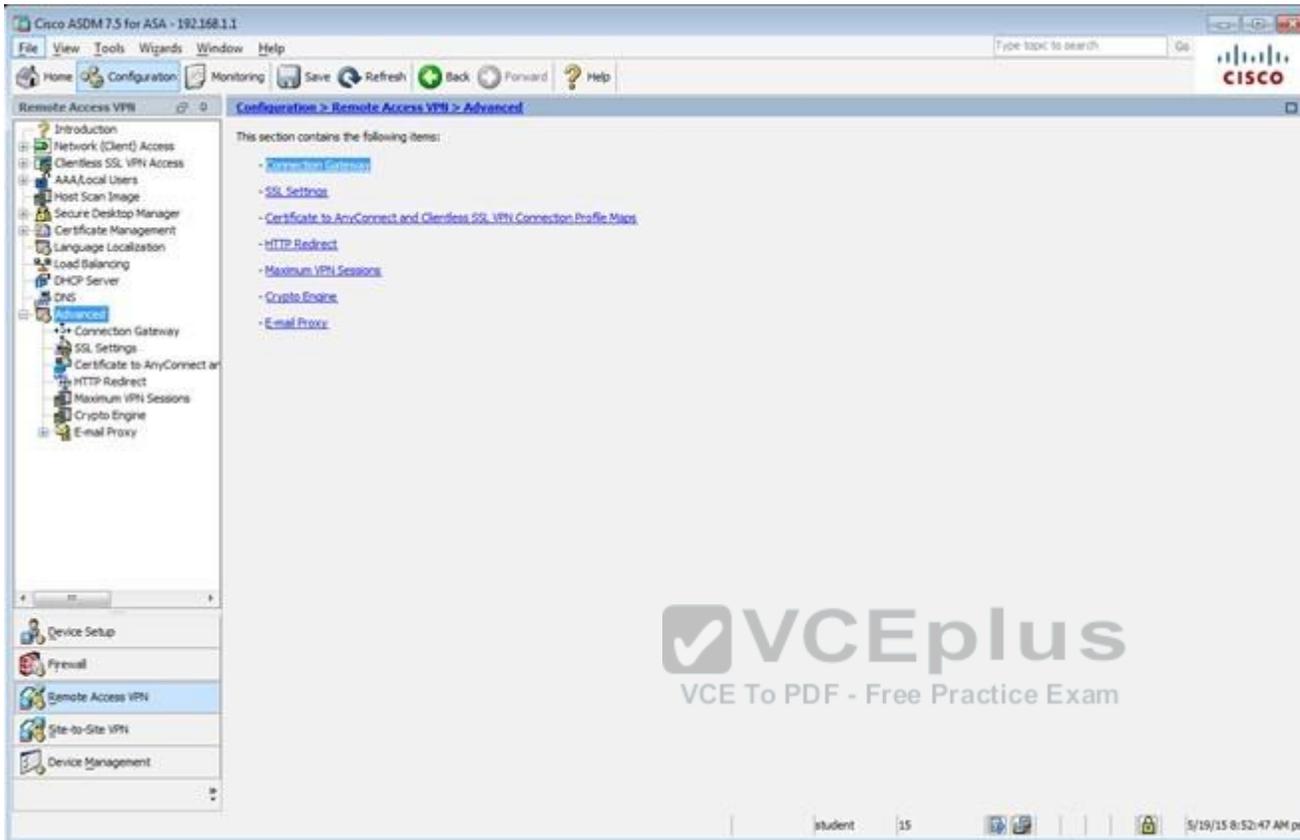
At the bottom of the page, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "student | 15 | 3/19/15 8:47:47 AM pst".



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Certificate Management > Identity Certificates". The left sidebar shows a tree view with "Identity Certificates" selected under "Certificate Management". The main content area features a table with the following data:

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname-#1 [7-ASA.sec...]	hostname-#1 [7-ASA.sec...]	11:10:33 pet (Dec 20 2024)	ASDM_Trustpoint1	General Purpose	RSA (2048 bits)

Below the table, there are sections for "Certificate Expiration Alerts" (Send the first alert before: 60 (days), Repeat Alert Interval: 7 (days)) and "Public CA Enrollment" (Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust). A "Launch ASDM Identity Certificate Wizard" button is visible. The bottom status bar shows "student 15" and the time "5/19/15 8:51:47 AM pet".



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Advanced > SSL Settings". The left sidebar shows a tree view with "Remote Access VPN" selected. The main content area contains the following configuration options:

- Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.
- The minimum SSL version for the security appliance to negotiate as a "server": TLS V1
- The minimum SSL version for the security appliance to negotiate as a "client": TLS V1
- Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modAus
- ECDH group to be used with SSL: Group19 - 256-bit EC

The "Encryption" section contains a table with the following data:

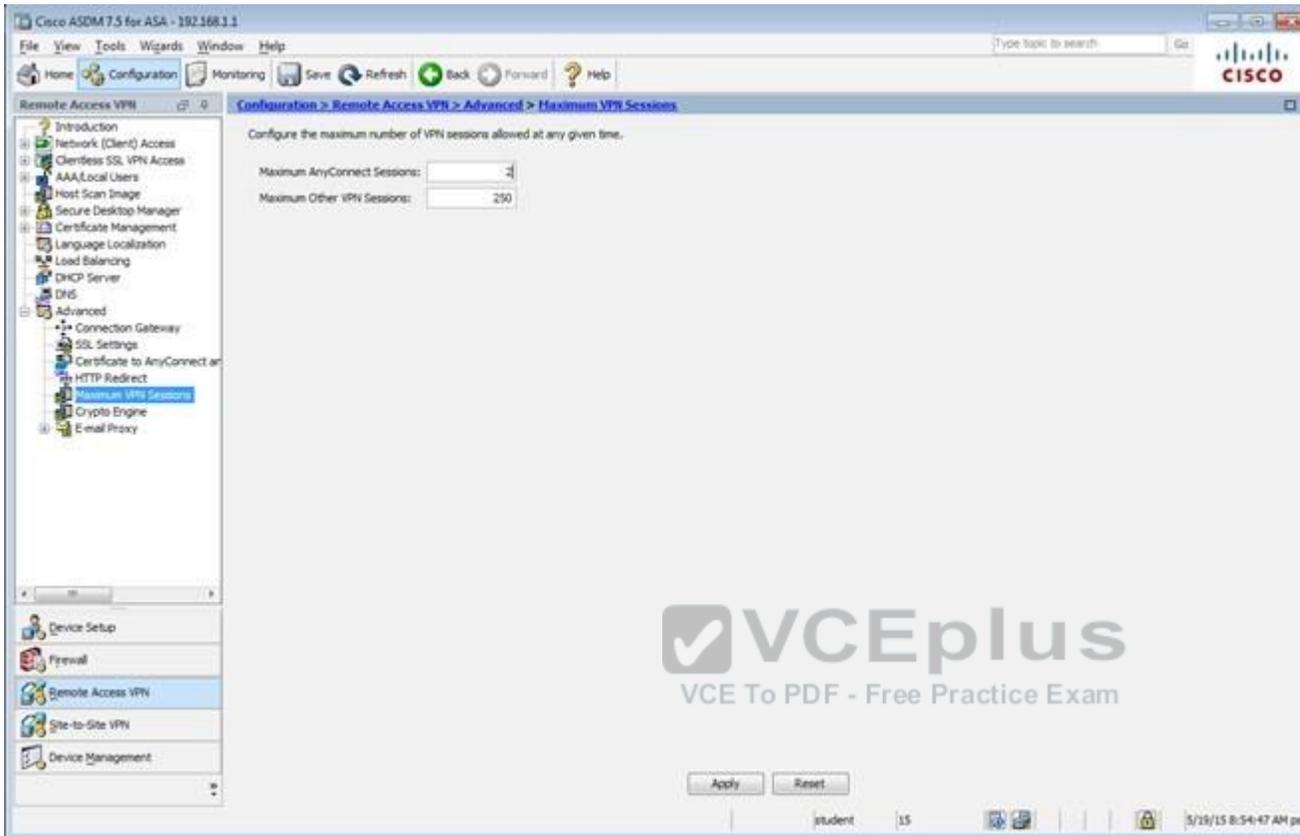
Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
DTLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...

The "Server Name Indication (SNI)" section shows a table with the following data:

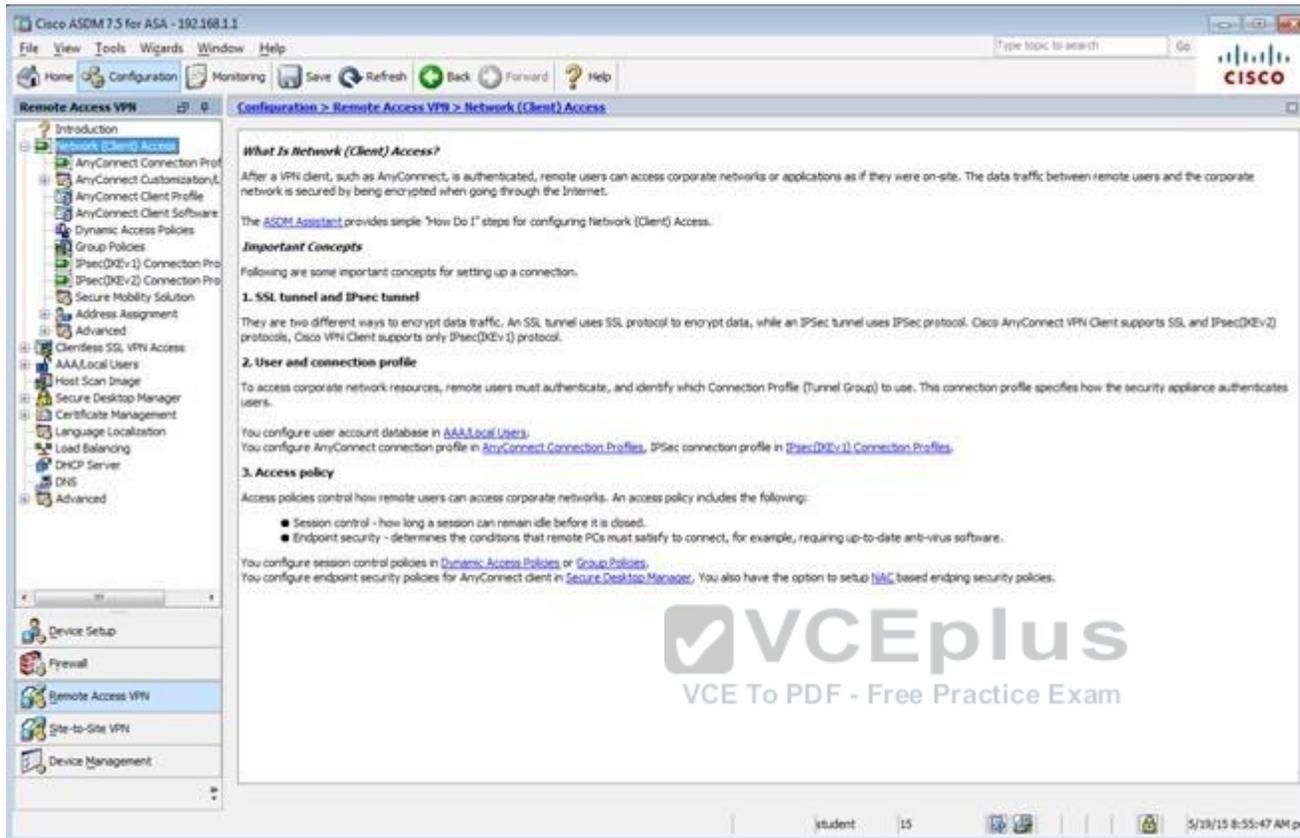
Domain	Certificate
dmz	ASDM_TrustPoint1.h...

The "Certificates" section contains the text: "Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own."

Buttons for "Apply" and "Reset" are located at the bottom of the configuration area. The status bar at the bottom shows "student 15" and the time "3/19/15 8:54:07 AM pst".



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions. The main content area contains the text "Configure the maximum number of VPN sessions allowed at any given time." and two input fields: "Maximum AnyConnect Sessions:" (empty) and "Maximum Other VPN Sessions:" (set to 250). The left sidebar shows a tree view with "Maximum VPN Sessions" selected. The bottom of the window features "Apply" and "Reset" buttons, a system tray with the user "student", the number "15", and the date/time "5/19/15 8:54:47 AM pat". A large, semi-transparent "VCEplus VCE To PDF - Free Practice Exam" watermark is overlaid on the center of the screenshot.



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area displays the configuration page for "Remote Access VPN > Network (Client) Access". The page includes a navigation pane on the left with a tree view of configuration options, a main content area with text and links, and a bottom status bar.

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKv2) protocols. Cisco VPN Client supports only IPsec(DKv1) protocol.

2. User and connection profile

To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user account database in [AAA Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKv1\) Connection Profiles](#).

3. Access policy

Access policies control how remote users can access corporate networks. An access policy includes the following:

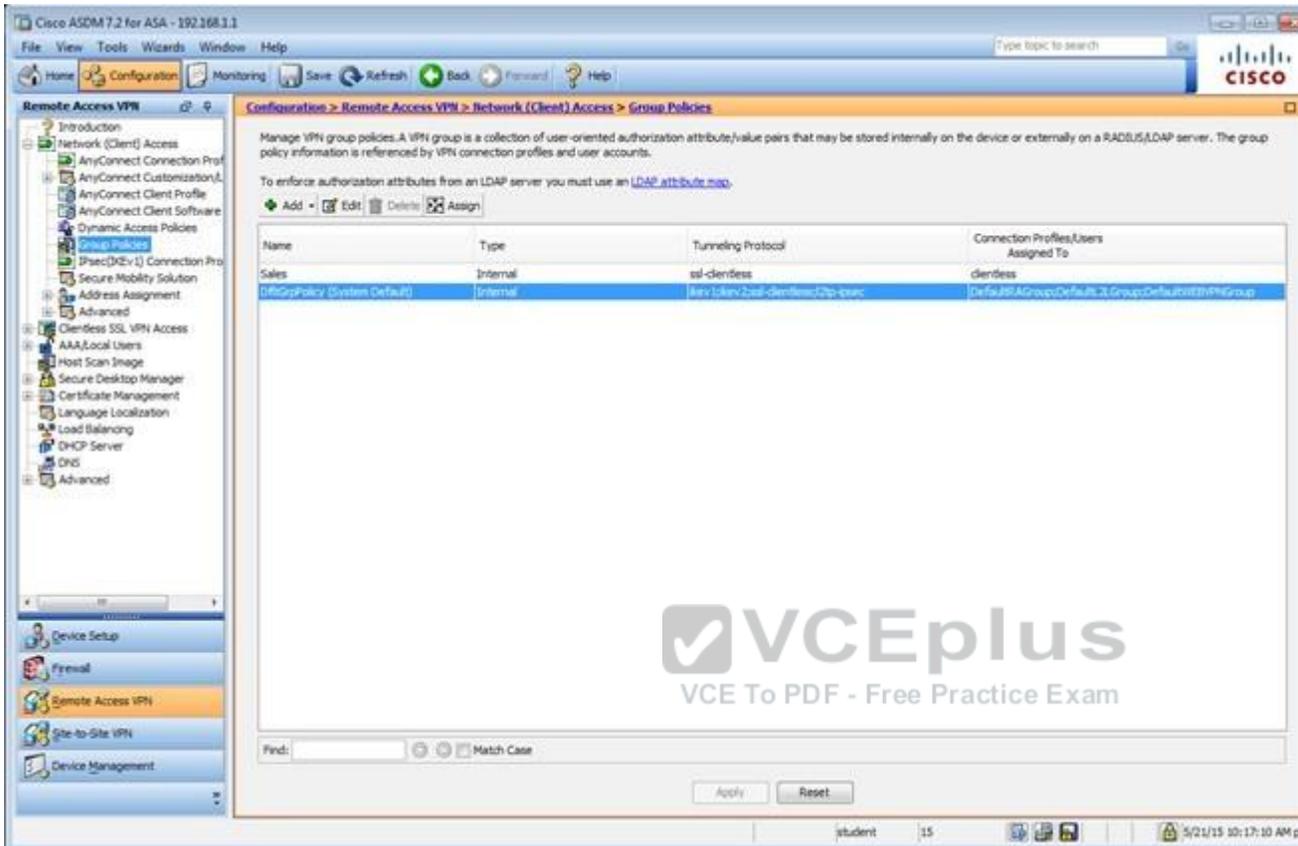
- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HAC](#) based endpoint security policies.

Navigation Pane:

- Introduction
- Network (Client) Access
- AnyConnect Connection Profile
- AnyConnect Customization List
- AnyConnect Client Profile
- AnyConnect Client Software
- Dynamic Access Policies
- Group Policies
- IPsec(DKv1) Connection Profile
- IPsec(DKv2) Connection Profile
- 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

Bottom Bar: student | 15 | 5/28/15 8:55:47 AM pet



Cisco ASDM 7.2 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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](#).

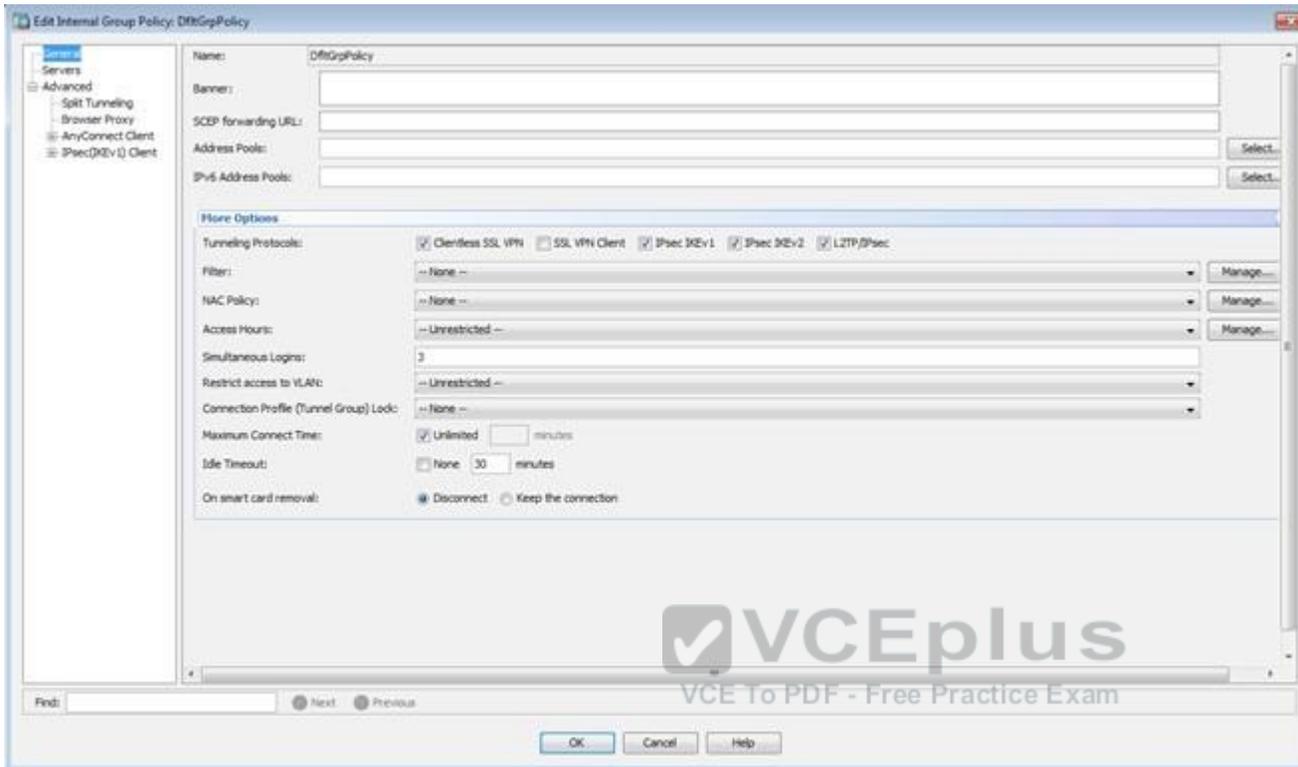
Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DRGpPolicy (System Default)	Internal	[rev:1.0]ssl-clientless/2ip-espac	DefaultAGroup/Default3LGroup/DefaultWEBPhGroup

Find: Match Case

Apply Reset

ytudent 15 3/21/15 10:17:10 AM pet



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window is titled "Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles". The left sidebar shows a tree view with "Remote Access VPN" selected. The main content area is divided into two sections: "Access Interfaces" and "Connection Profiles".

Access Interfaces
 Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input 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.

Connection Profiles
 Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
DefaultE2EVPNGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DiffGrpPolicy
Default	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL	Local

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:56:47 AM pst

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

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
dmz	<input checked="" 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

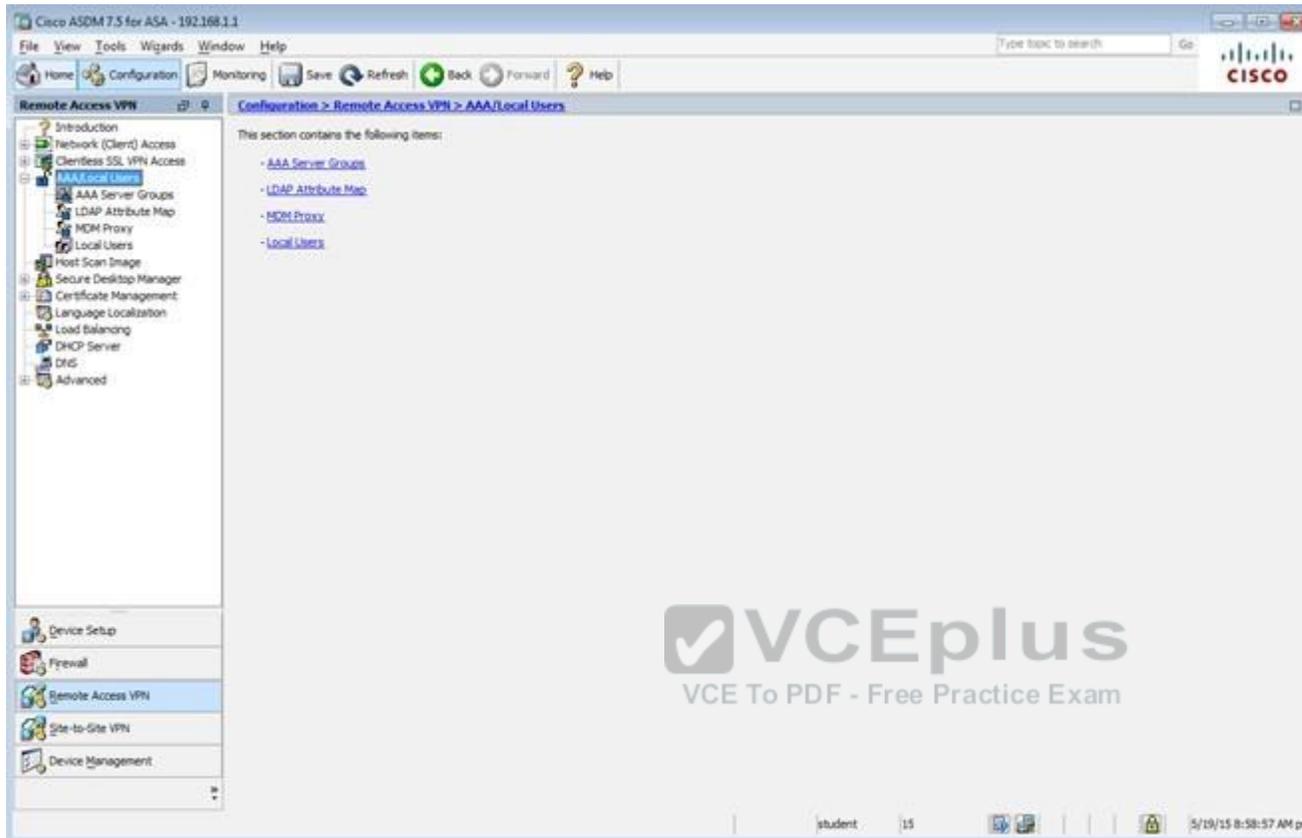
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

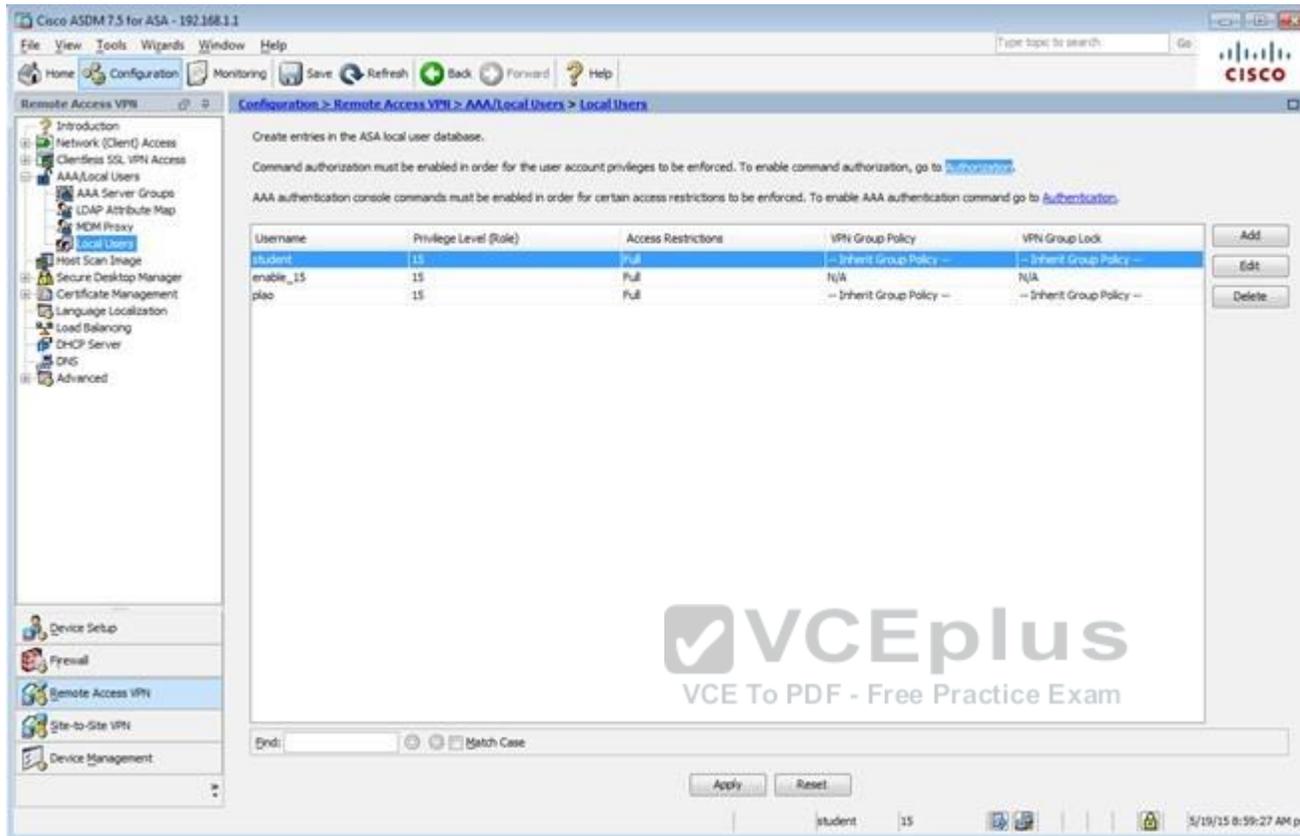
End:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
certless	<input checked="" type="checkbox"/>	<input type="checkbox"/>	yes	SSL(OCSP)	certless

Let group URLs take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

student 15 5/19/15 8:58:17 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

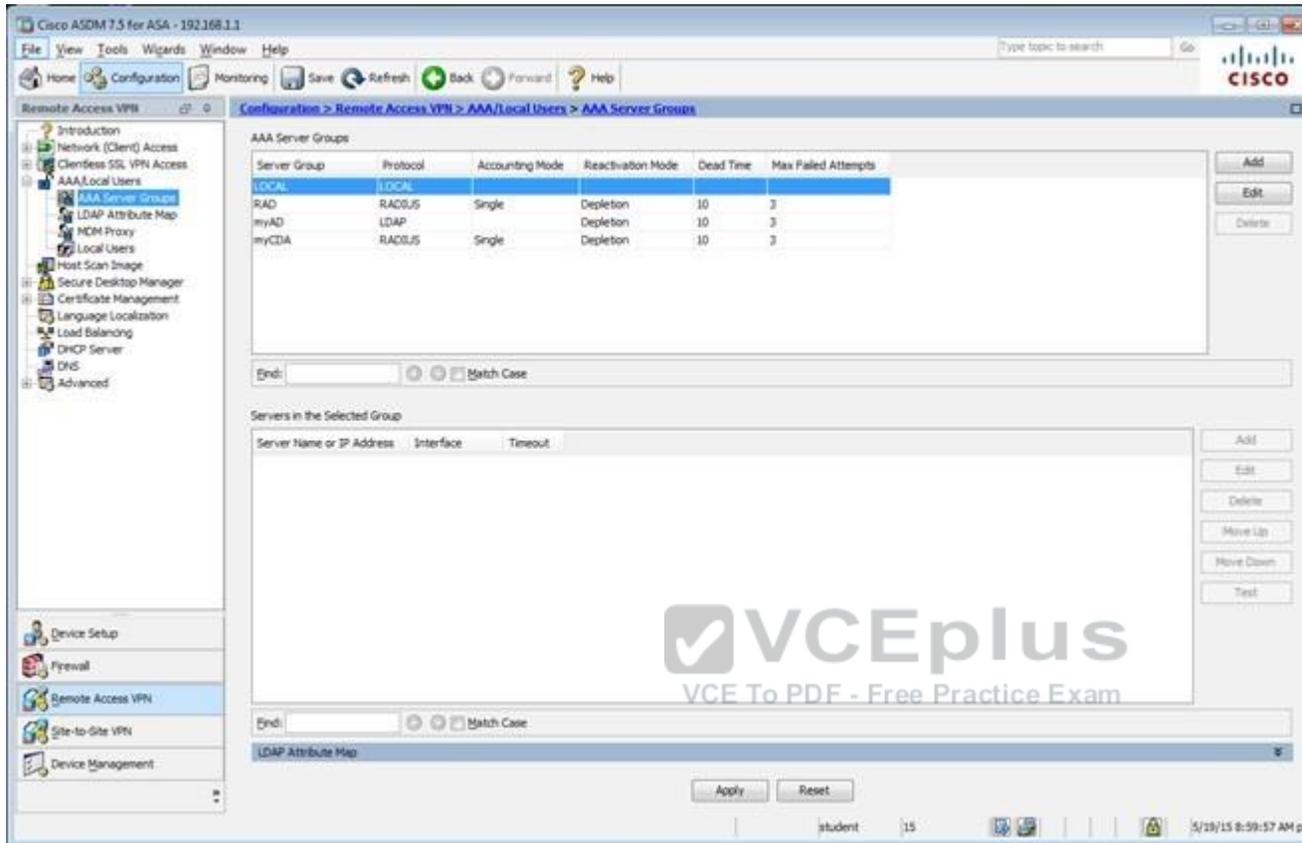
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plac	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End: Match Case

Apply Reset

student 15 5/19/15 8:59:27 AM pet



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: (none)

Explanation

Explanation/Reference:

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

The screenshot shows the Cisco VTI configuration interface. The breadcrumb path is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows a tree view with 'Connection Profiles' selected. The main content area is divided into sections: Access Interfaces, Login Page Setting, and Connection Profiles.

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.

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.

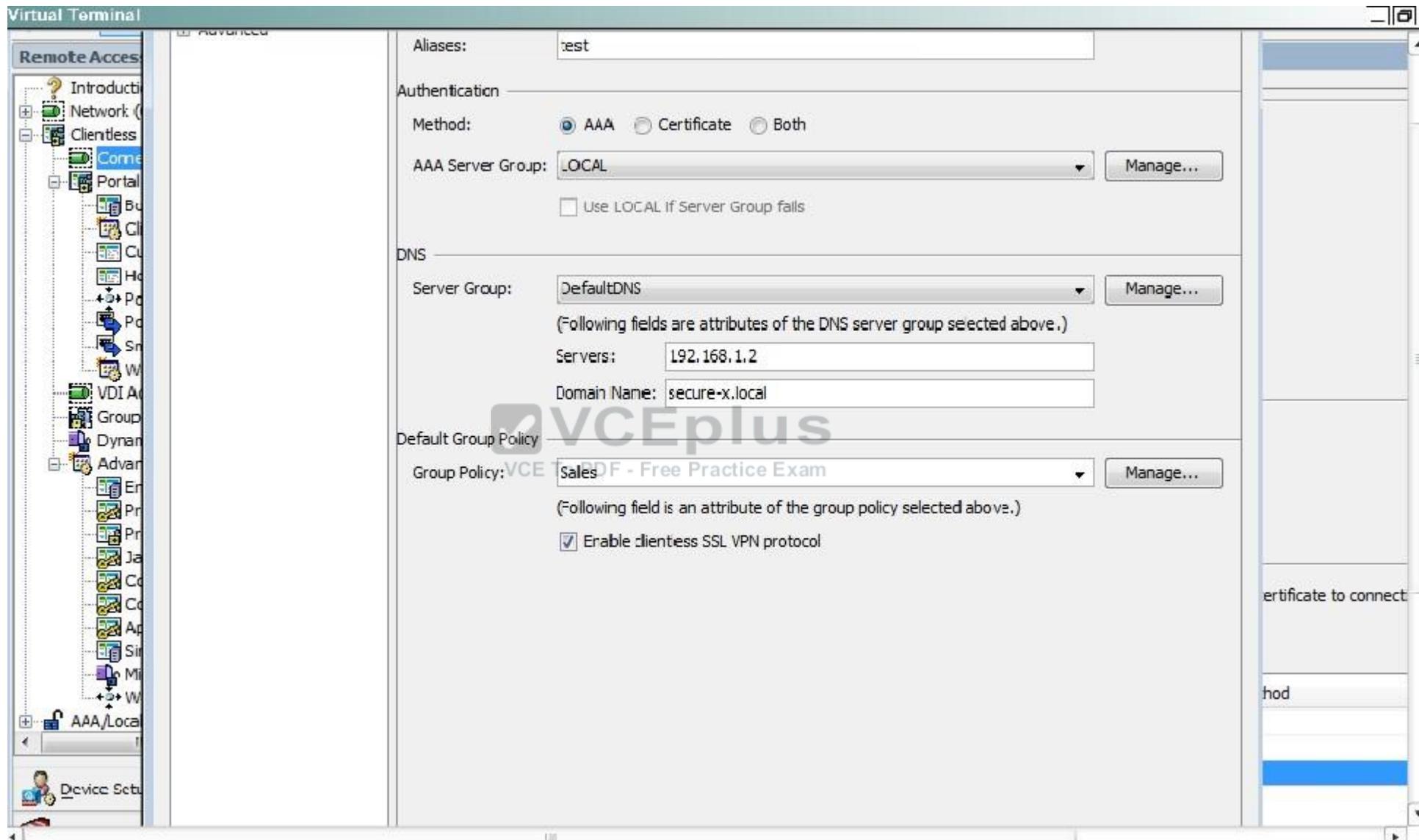
Connection Profiles

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

+ Add Edit Delete Find: Match Case

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

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



QUESTION 68
SIMULATION

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 also allow any host only on 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 in this simulation is to use ASDM to enable the ASA 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 testing pings to `www.cisco.com` will work.

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.

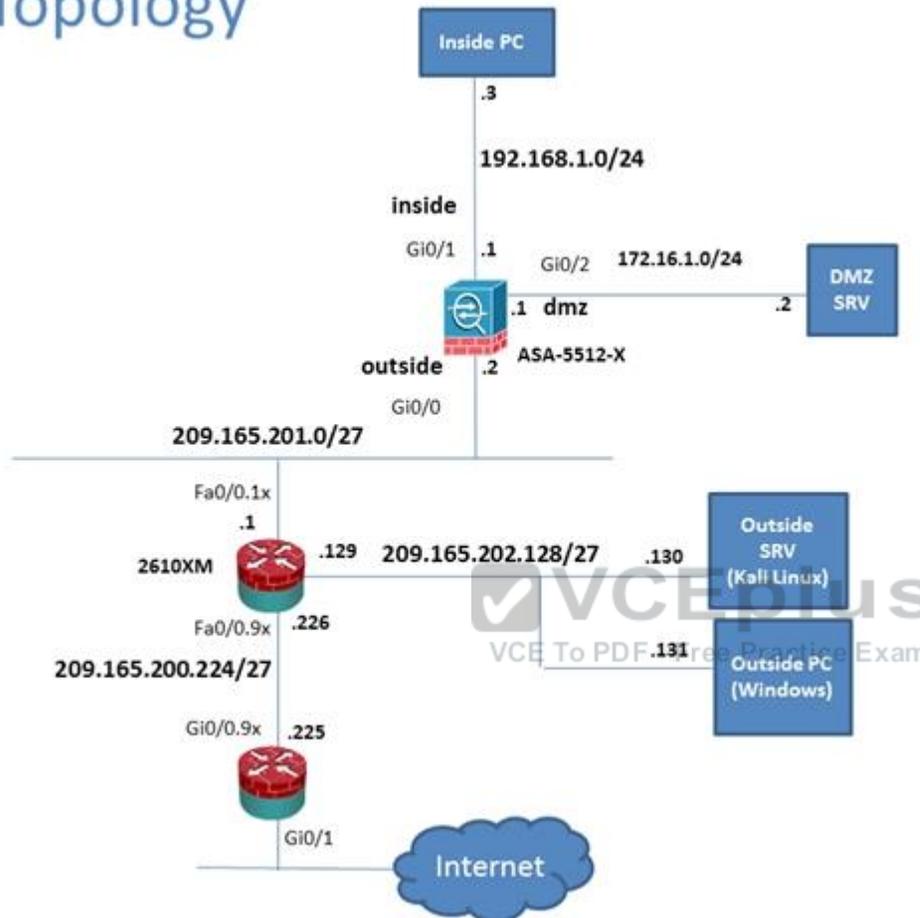
Note:

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA FirePOWER Status

Device Information

General License

Host Name: **P17-ASA.secure-x.local**

ASA Version: **100.14(6)13**

ASDM Version: **7.5(1)1**

Firewall Mode: **Routed**

Environment Status: **OK**

Device Uptime: **11d 21h 42m 47s**

Device Type: **ASA 5512**

Context Mode: **Single**

Total Flash: **4096 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	up	up	0
inside	192.168.1.1/24	up	up	4
mgmt	10.10.10.2/24	up	up	0
outside	209.165.201.2/24	up	up	0

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

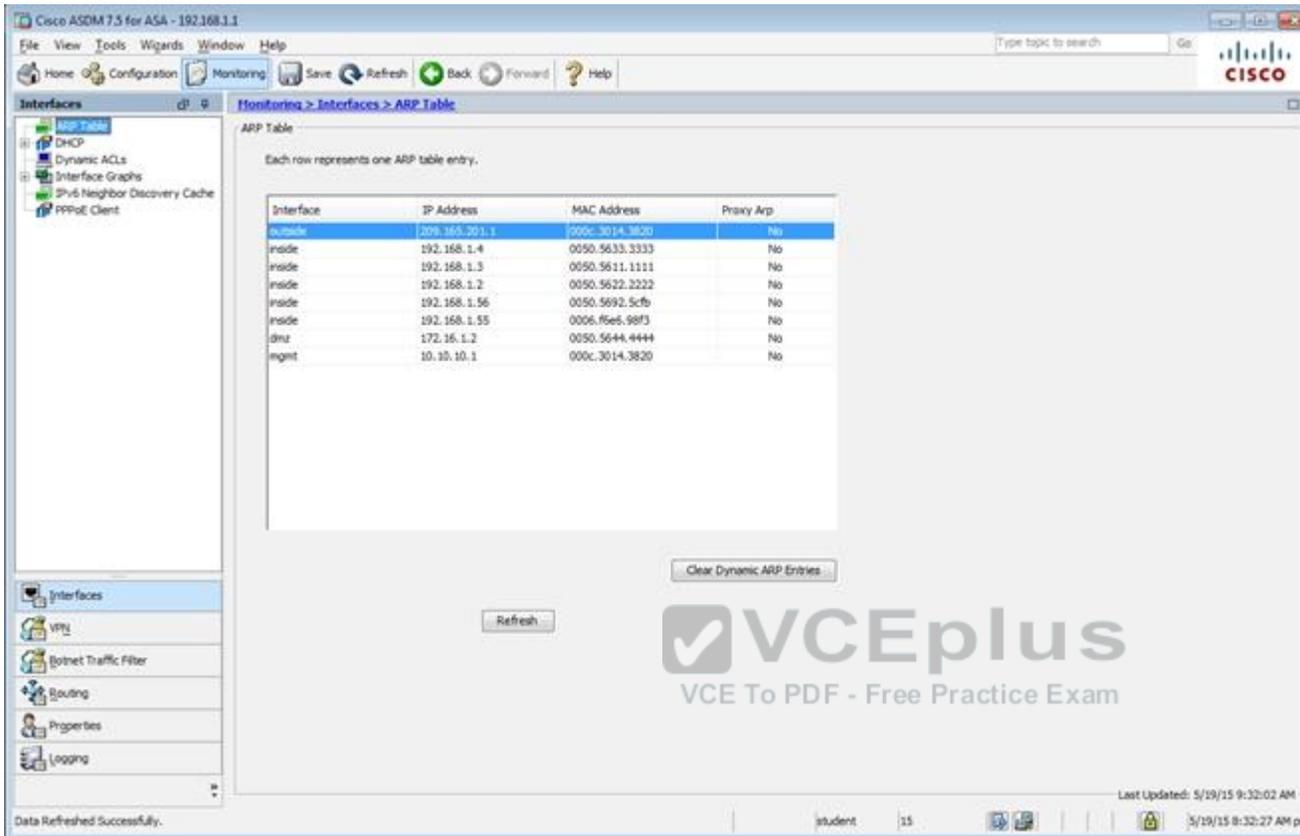
Traffic Status

Connections Per Second Usage

'outside' Interface Traffic Usage (Kbps)

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	May 13 2015	12:35:09	302016	10.81.254.202	123	209.165.201.2	65535	Teardown UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6	May 13 2015	12:35:08	106015	192.168.1.3	14676	192.168.1.1	443	Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6	May 13 2015	12:35:08	302014	192.168.1.3	14676	192.168.1.1	443	Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

- ARP Table
- DHCP
- Dynamic ACLs
- Interface Graphs
- IPv6 Neighbor Discovery Cache
- PPPoE Client

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.3014.3000	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.f5e5.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

Refresh

 **VCEplus**
VCE To PDF - Free Practice Exam

Last Updated: 5/19/15 9:32:02 AM

Data Refreshed Successfully.

student 15 5/19/15 8:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

Monitoring > VPN > VPN Statistics > Sessions

Filter By: Site-to-Site -- All Sessions -- Filter

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN				
Browser				

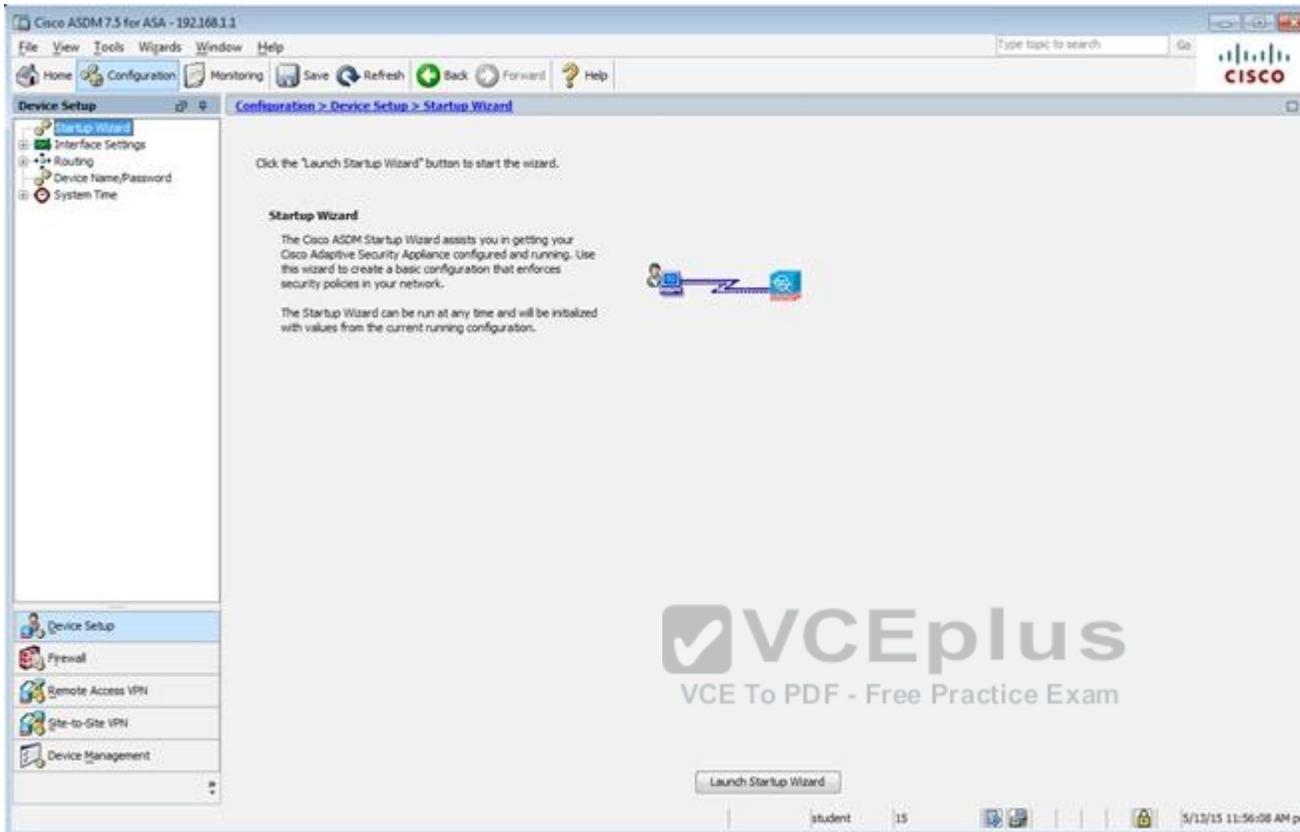
Connection Profile: IP Address Protocol Encryption Login Time Duration Bytes Tx Bytes Rx Cer Auth Int Cer Auth Left

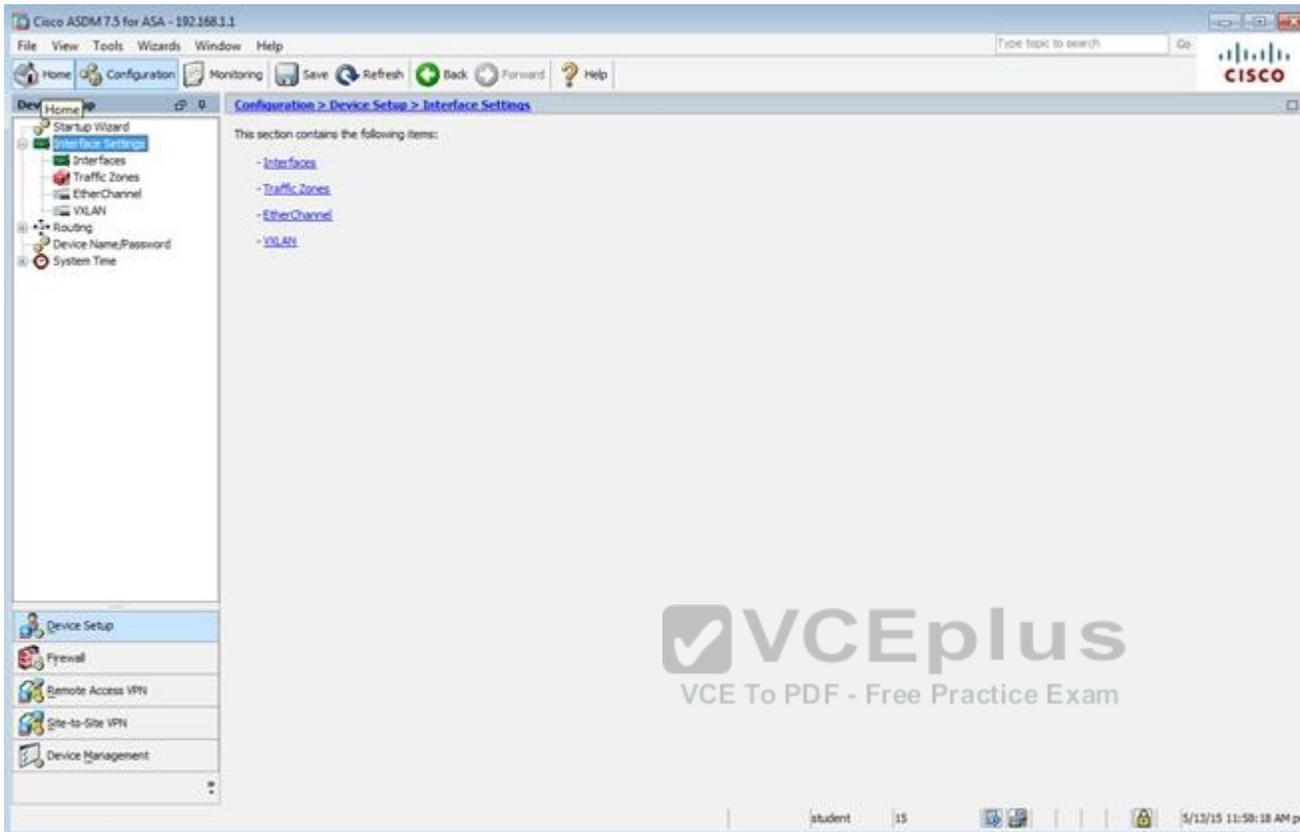
Logout By: -- All Sessions -- Logout Sessions Refresh

Last Updated: 5/19/15 9:33:12 AM

Data Refreshed Successfully.

Filter By: Clientless SSL VPN -- All Sessions -- Filter

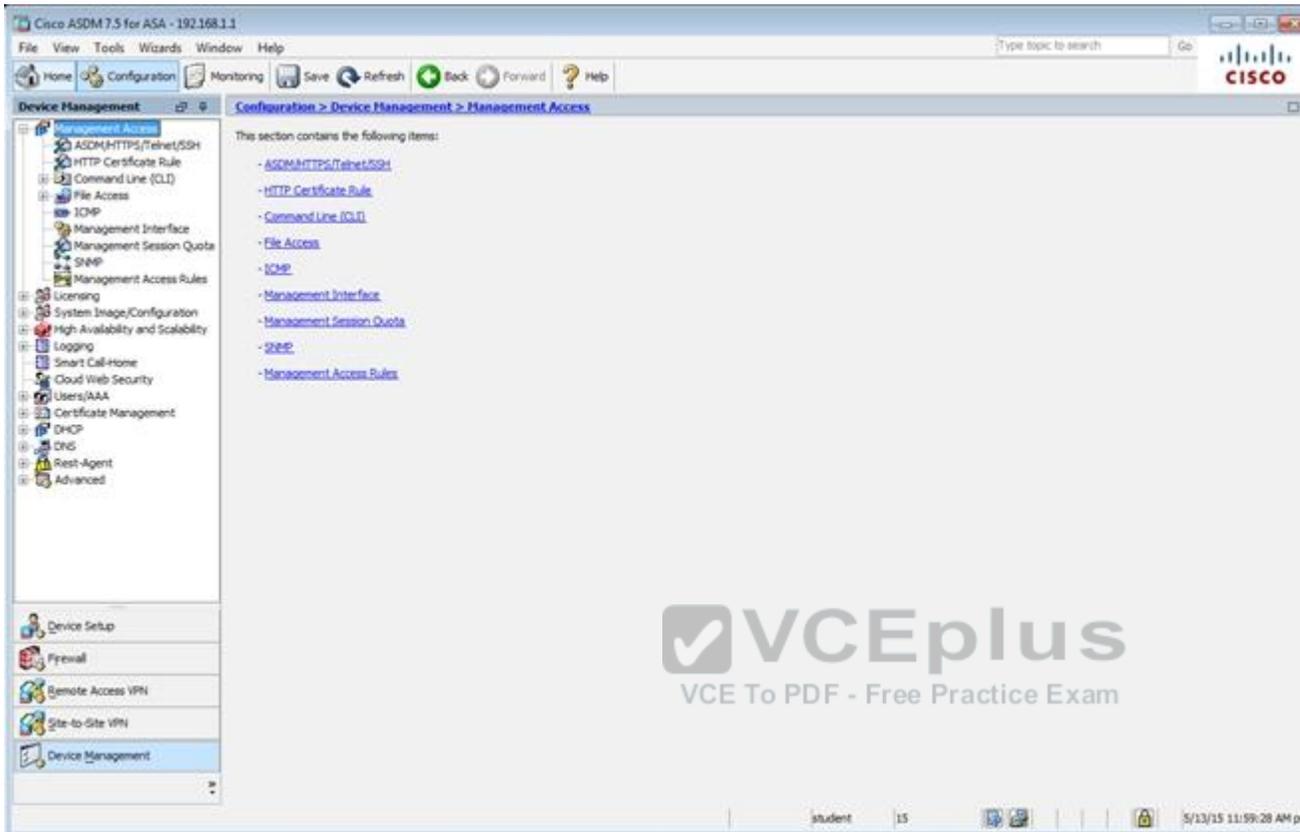




The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration page for Interfaces, with a table listing various interfaces and their settings. The table has columns for Interface, Name, Zone, Route Map, State, Security Level, IP Address, Subnet Mask Prefix Length, Group, and Type. The 'GigabitEthernet0/0' interface is highlighted in blue. Below the table, there are three checkboxes for enabling traffic between interfaces with the same security levels, between hosts connected to the same interface, and for enabling jumbo frame reservation. The 'Apply' and 'Reset' buttons are visible at the bottom of the configuration area.

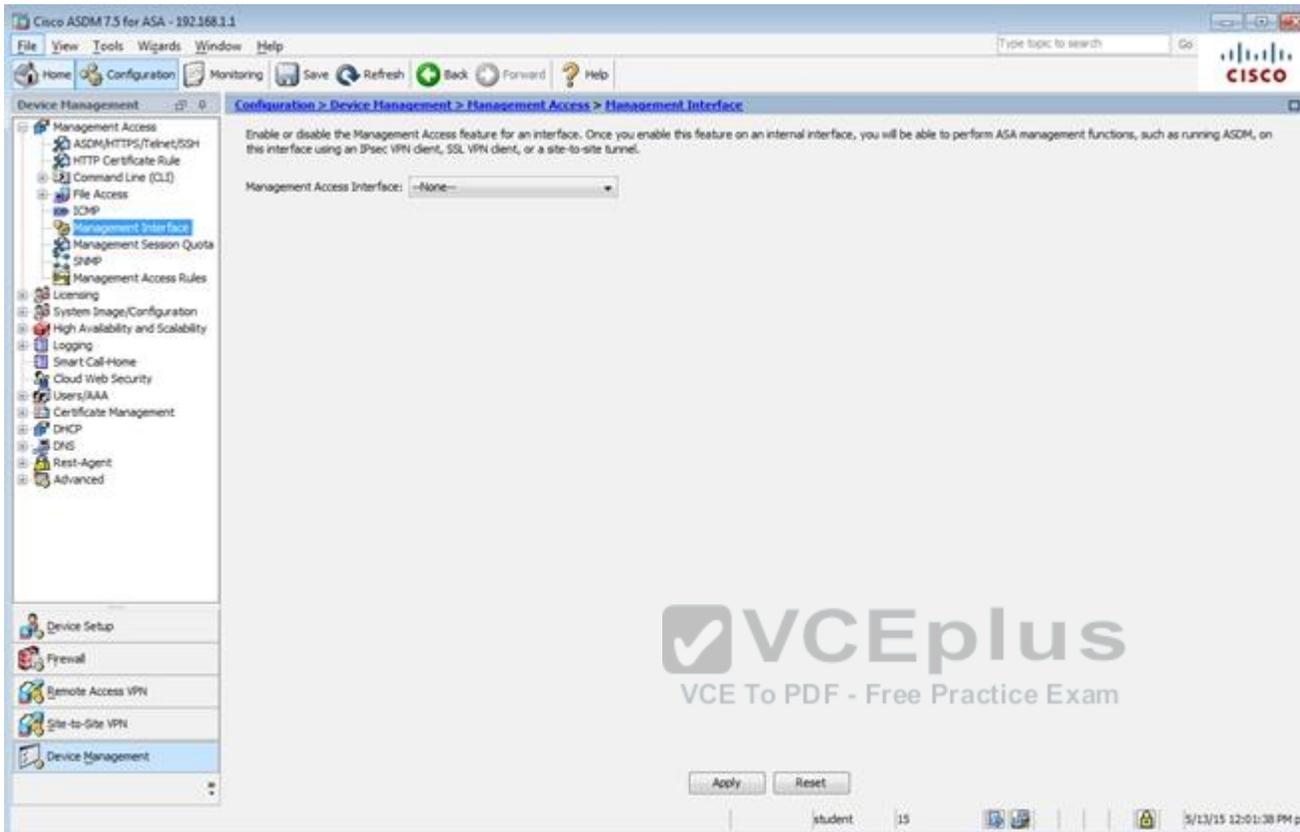
Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled	0	209.165.201.2	255.255.255.0		Hardware
GigabitEthernet0/1	inside			Enabled	100	192.168.1.1	255.255.255.0		Hardware
GigabitEthernet0/2	dmz			Enabled		172.16.1.1	255.255.255.0		Hardware
GigabitEthernet0/3				Enabled					Hardware
GigabitEthernet0/4				Enabled					Hardware
GigabitEthernet0/5	mgmt			Enabled	500	10.10.10.2	255.255.255.0		Hardware
Management0/0				Enabled					Hardware

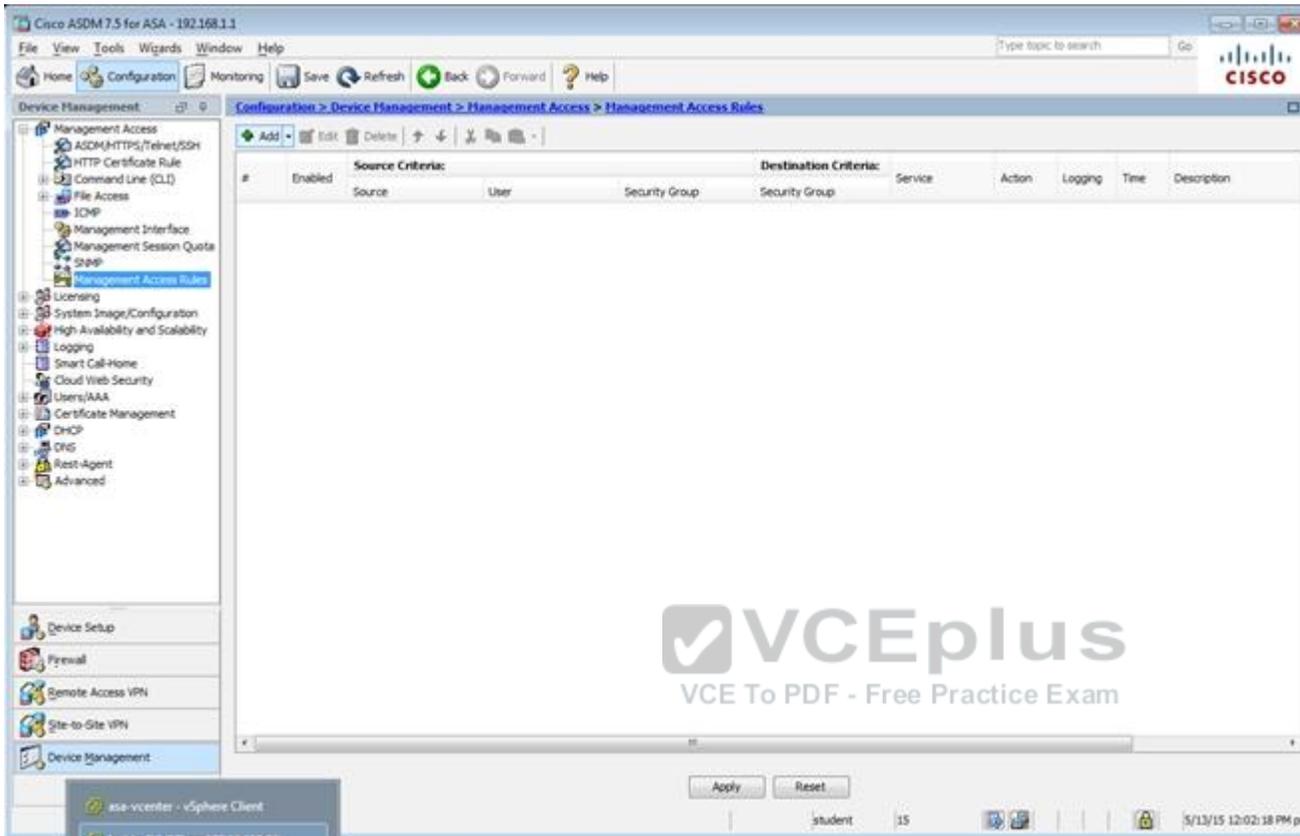
Enable traffic between two or more interfaces which are configured with same security levels
 Enable traffic between two or more hosts connected to the same interface
 Enable jumbo frame reservation

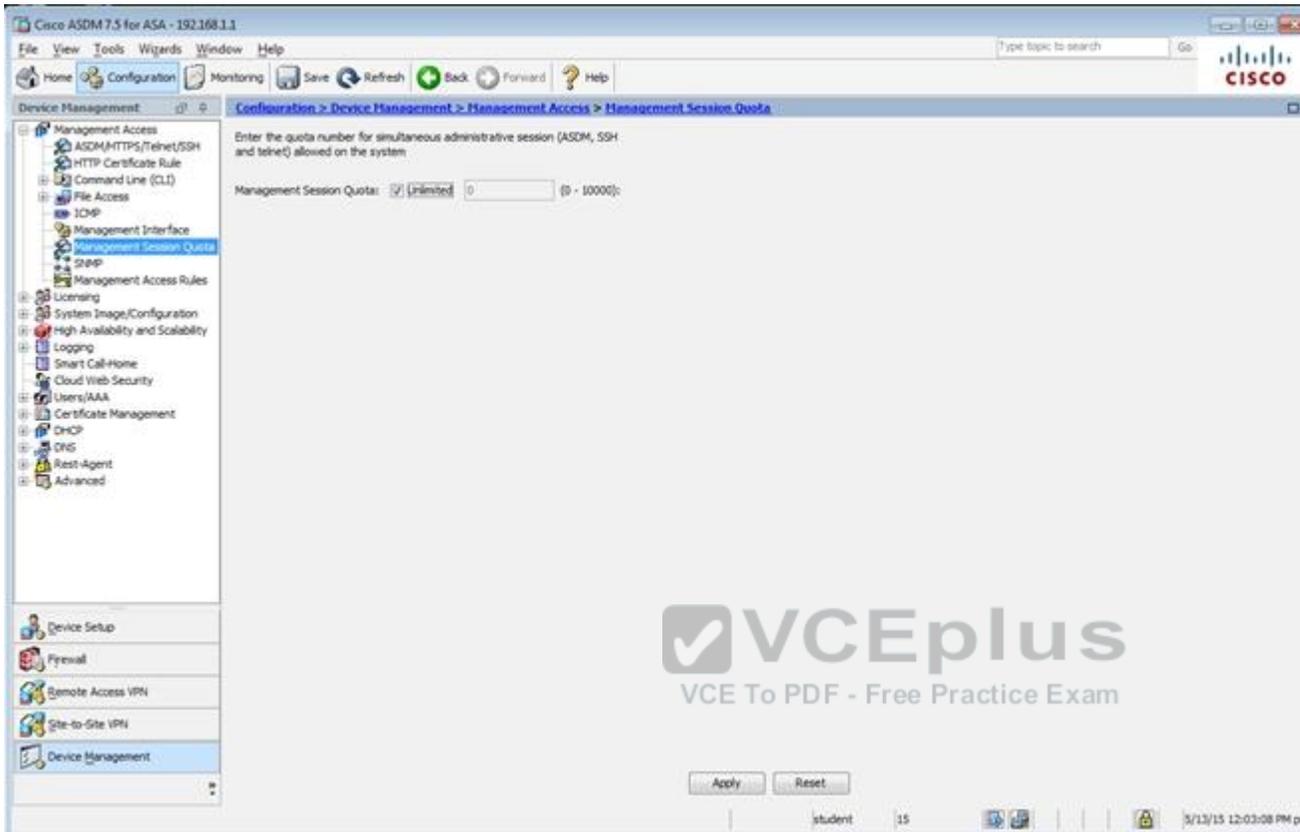


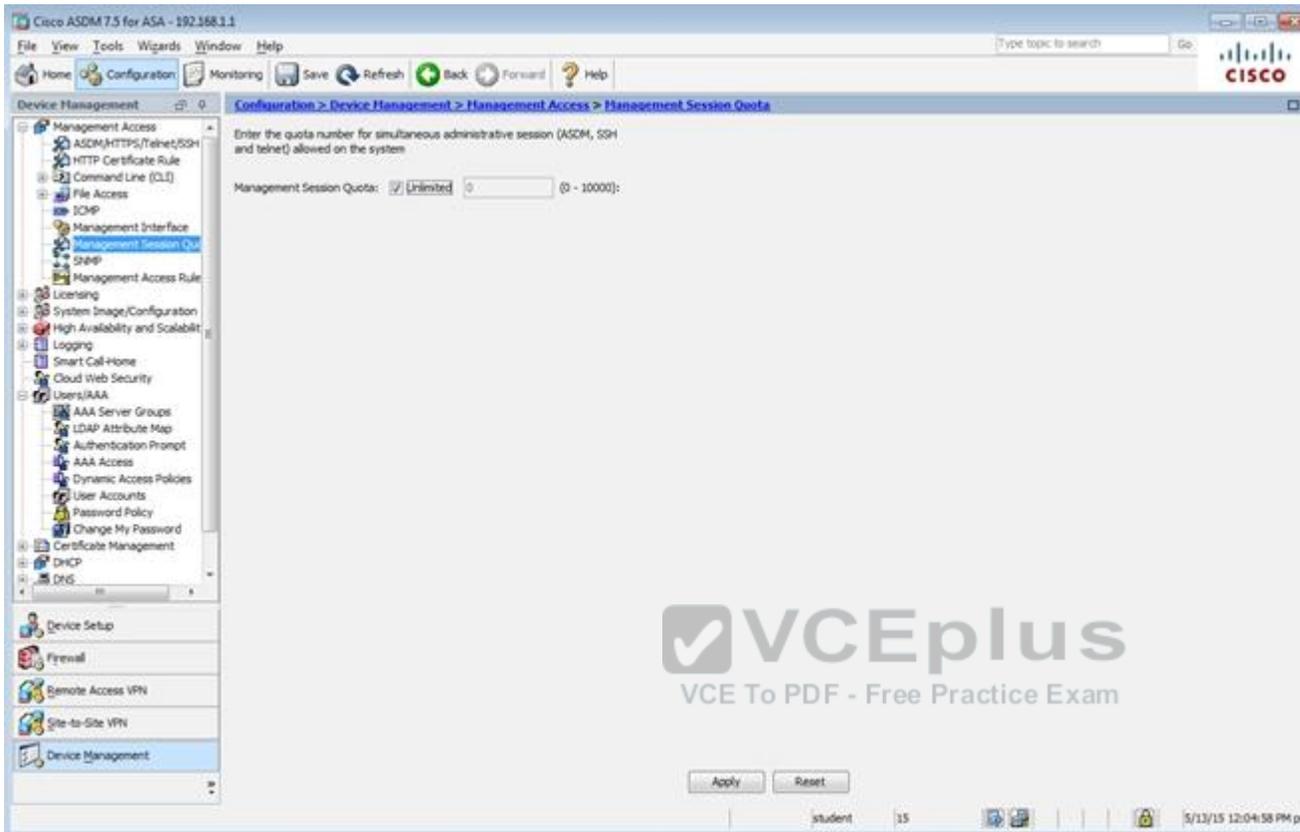
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows a tree view of configuration categories, with "Management Access Rules" selected. The main content area displays a table for specifying host addresses allowed to access the ASA. The table has four columns: Type, Interface, IP Address, and Mask/Prefix Length. Three entries are listed: Telnet (mgmt, 10.10.10.1, 255.255.255.255), SSH (inside, 192.168.1.2, 255.255.255.255), and ASDM/HTTPS (inside, 192.168.1.0, 255.255.255.0). Below the table are sections for HTTP Settings (Enable HTTP Server checked, Port Number 443, Idle Timeout 20 minutes), Telnet Settings (Telnet Timeout 5 minutes), and SSH Settings (Allowed SSH Version(s) 1 & 2, SSH Timeout 5 minutes). The interface includes "Apply" and "Reset" buttons at the bottom.

Type	Interface	IP Address	Mask/Prefix Length
Telnet	mgmt	10.10.10.1	255.255.255.255
SSH	inside	192.168.1.2	255.255.255.255
ASDM/HTTPS	inside	192.168.1.0	255.255.255.0

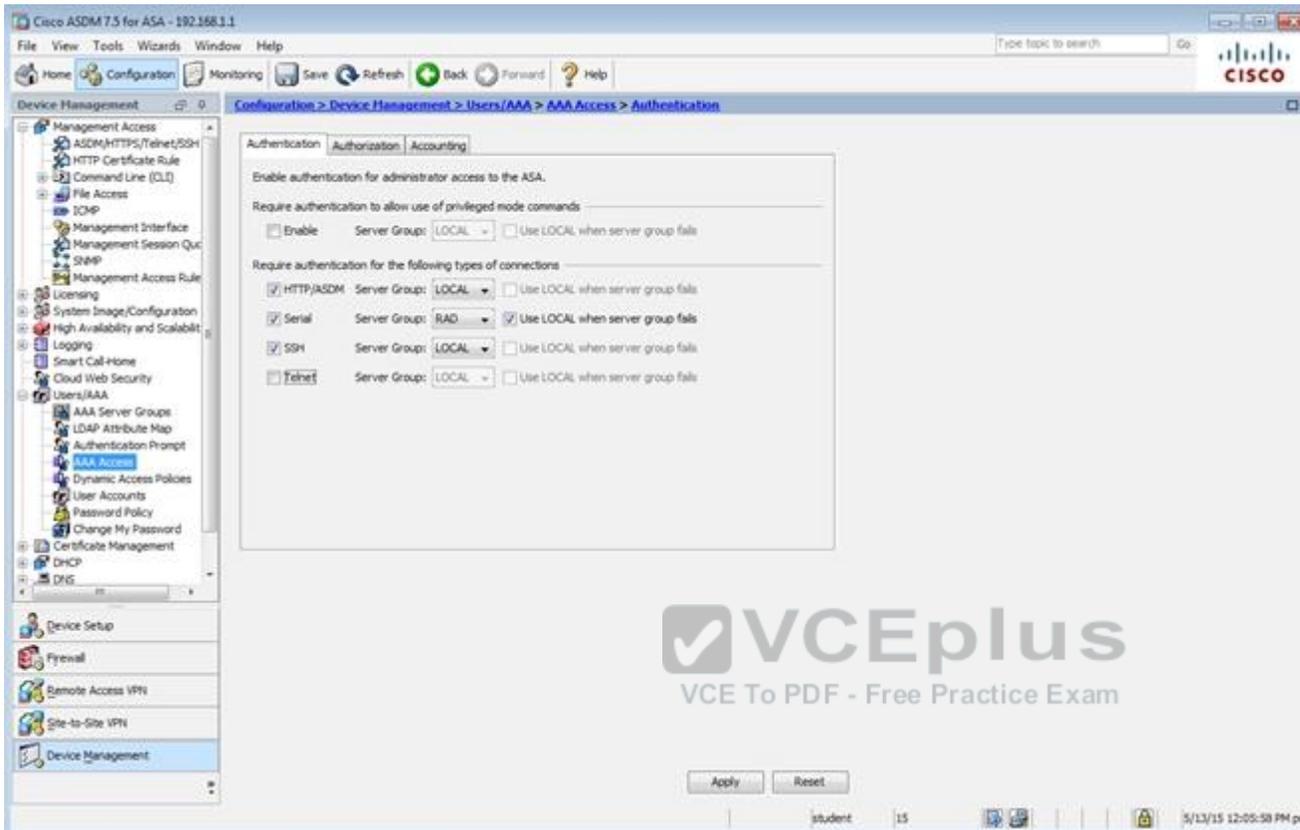


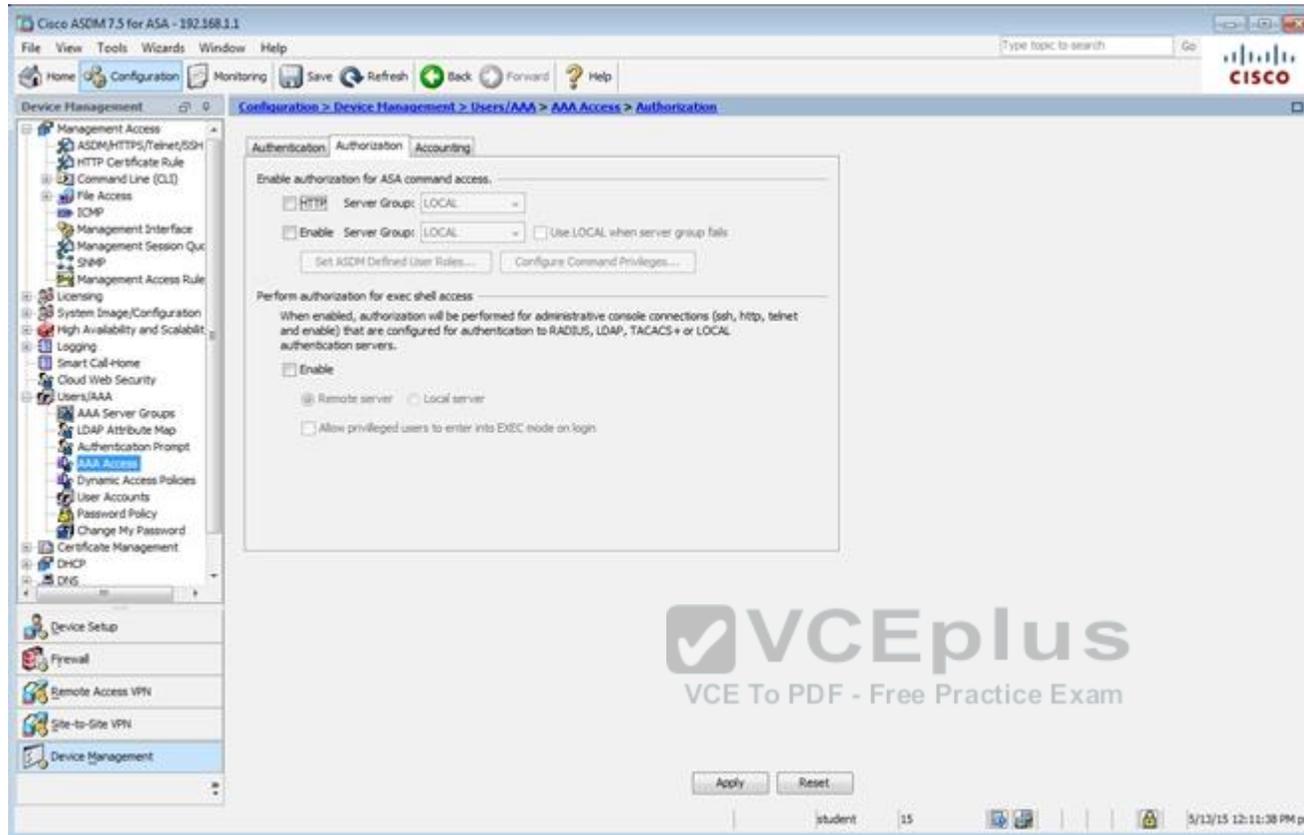


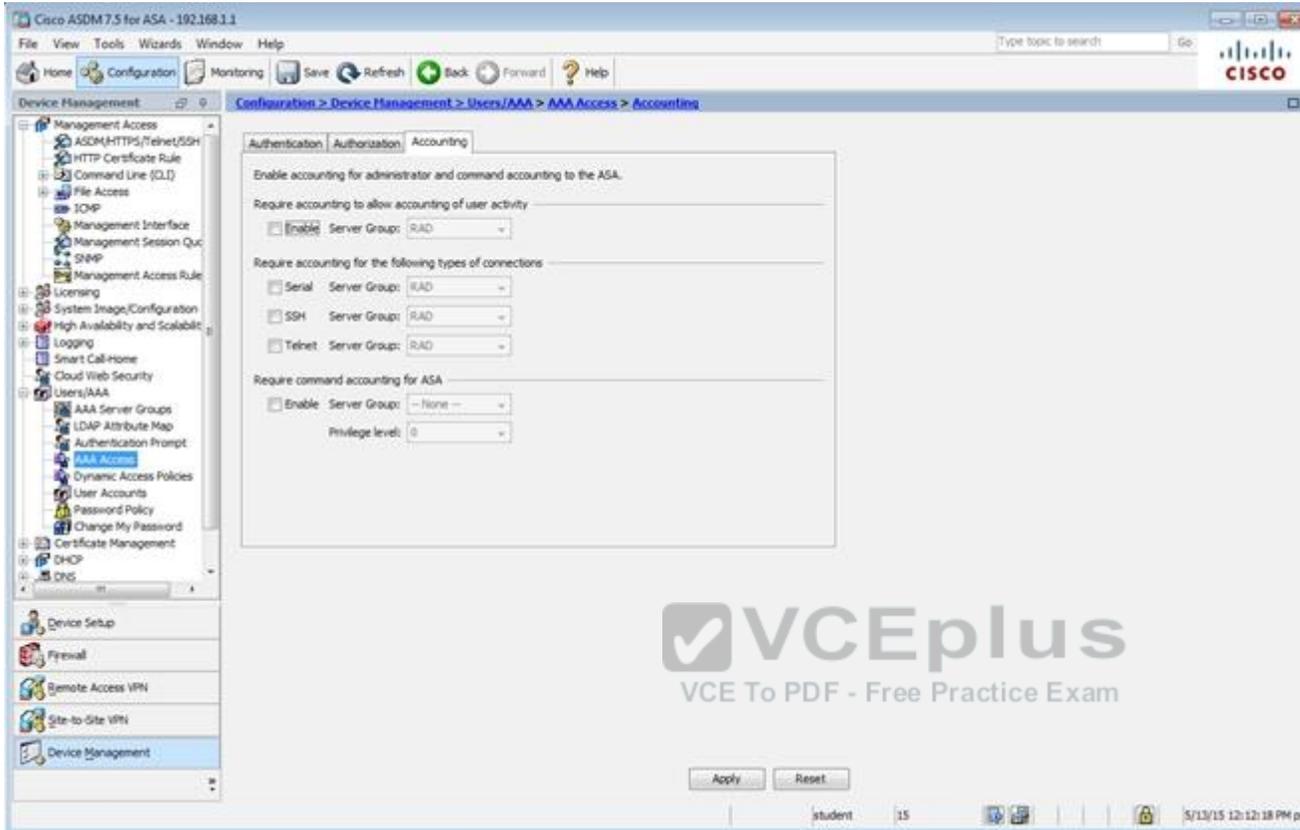




The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Device Management > Management Access > Management Session Quota. The main content area contains the text: "Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system." Below this, there is a "Management Session Quota" section with a checked "Unlimited" radio button and a text input field containing "0" (range 0 - 10000). At the bottom of the configuration area are "Apply" and "Reset" buttons. The left sidebar shows a tree view with "Management Session Quota" selected. The bottom status bar shows the user "student" and the time "5/13/15 12:04:58 PM pst".





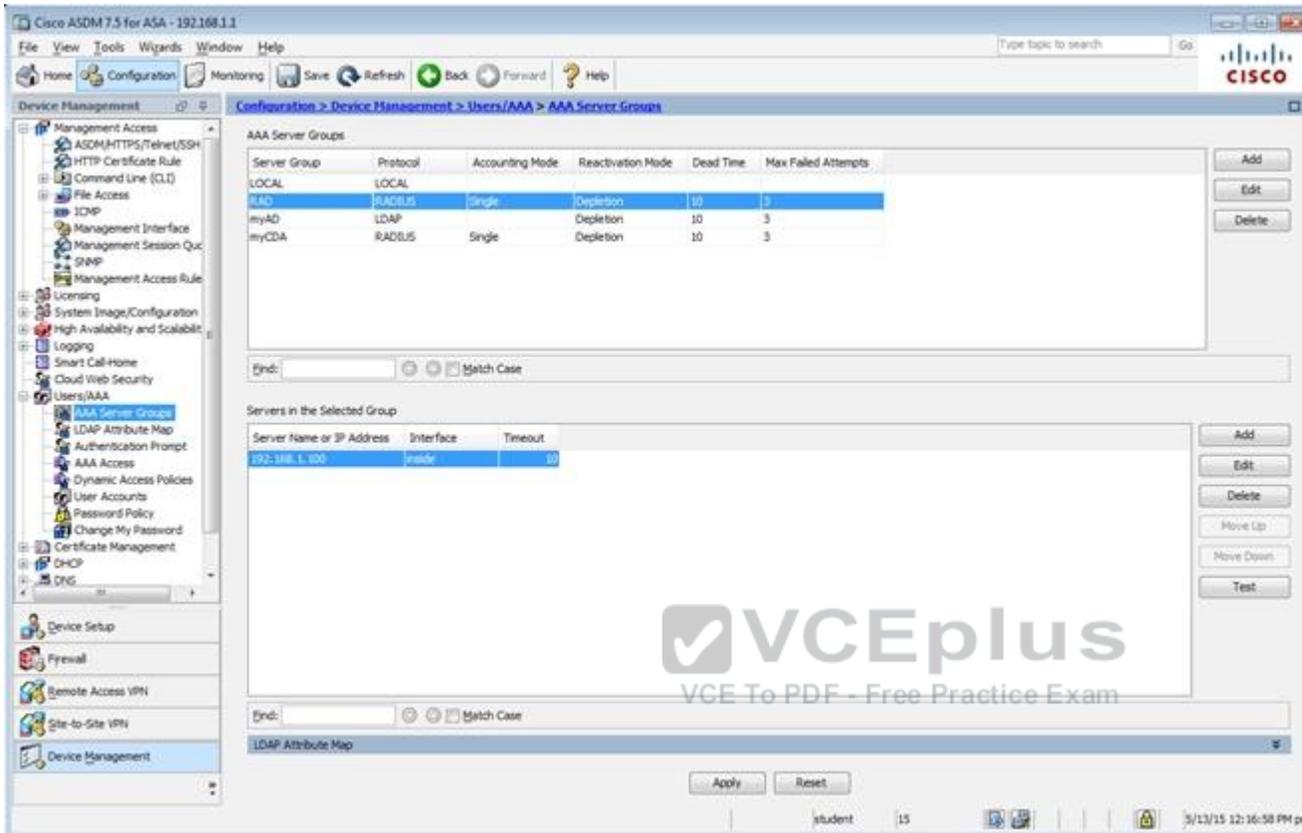


The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > Users/AAA > AAA Access > Accounting. The left sidebar shows a tree view with 'Users/AAA' expanded to 'AAA Access'.

The main configuration area has three tabs: Authentication, Authorization, and Accounting. The Accounting tab is active and contains the following settings:

- Enable accounting for administrator and command accounting to the ASA. (unchecked)
- Require accounting to allow accounting of user activity. (unchecked) Server Group: RAD
- Require accounting for the following types of connections:
 - Serial: (unchecked) Server Group: RAD
 - SSH: (unchecked) Server Group: RAD
 - Telnet: (unchecked) Server Group: RAD
- Require command accounting for ASA. (unchecked) Server Group: -- None --
- Privilege level: 0

At the bottom of the configuration area are 'Apply' and 'Reset' buttons. The status bar at the very bottom shows 'student', '15', and the date/time '5/13/15 12:12:18 PM pst'.



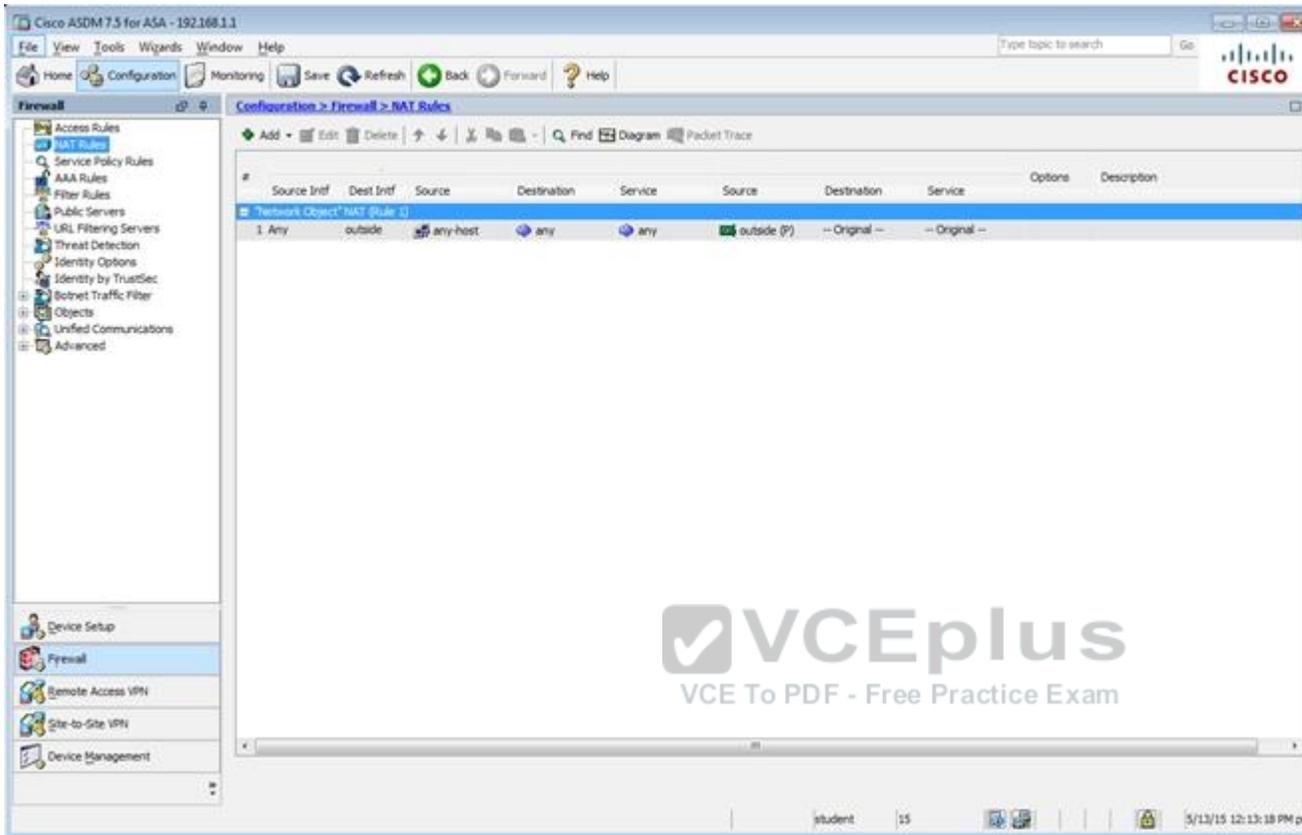
The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The main window is titled "Configuration > Device Management > Users/AAA > AAA Server Groups". The left sidebar shows a tree view with "Users/AAA" expanded to "AAA Server Groups". The main content area displays a table of AAA Server 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

Below the table is a search field labeled "Find:" with a "Match Case" checkbox. Underneath is a section titled "Servers in the Selected Group" with a table:

Server Name or IP Address	Interface	Timeout
192.168.1.100	inside	10

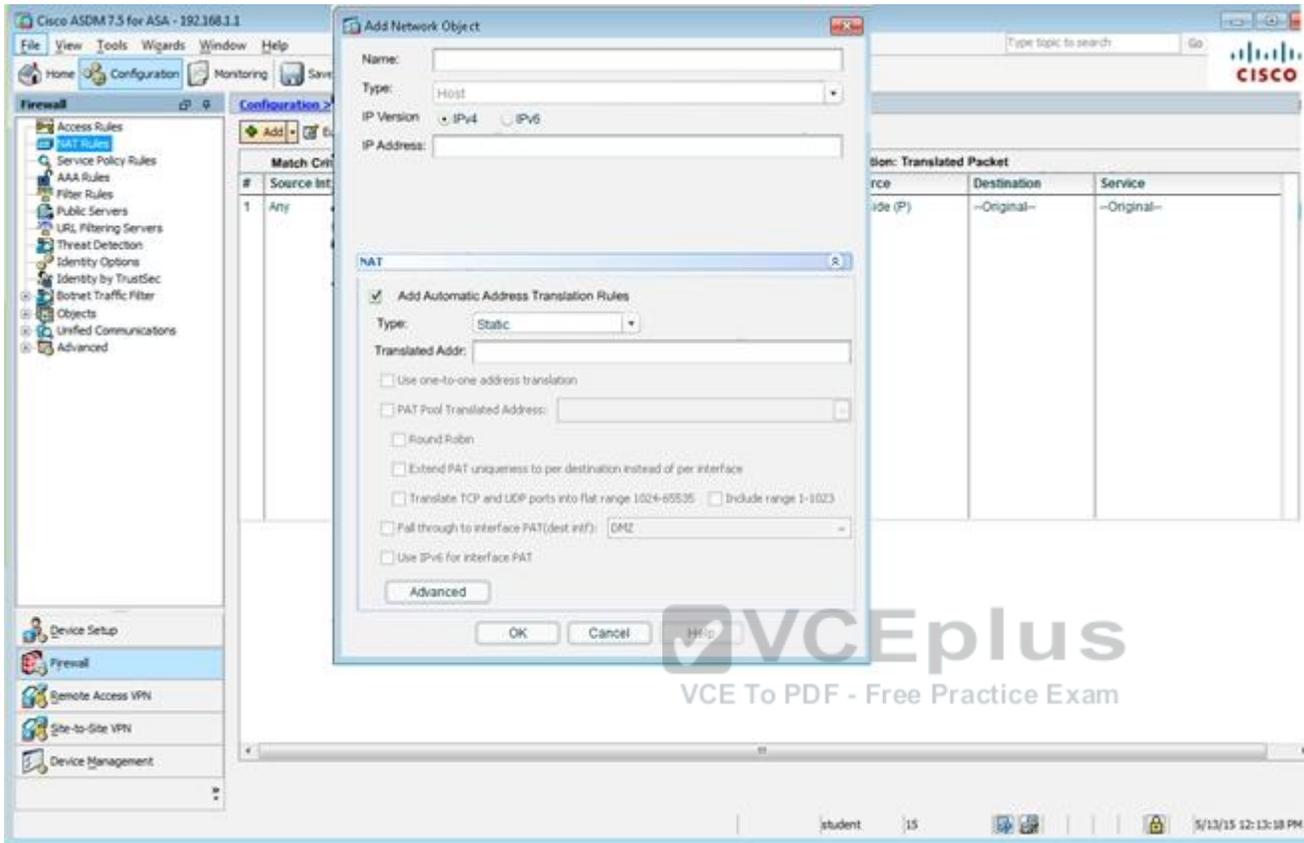
At the bottom of the main content area is another search field labeled "Find:" with a "Match Case" checkbox. The bottom status bar shows "LDAP Attribute Map" and "Apply" and "Reset" buttons. The system tray at the bottom right shows the user "student", the number "15", and the date/time "5/13/15 12:16:58 PM pst".

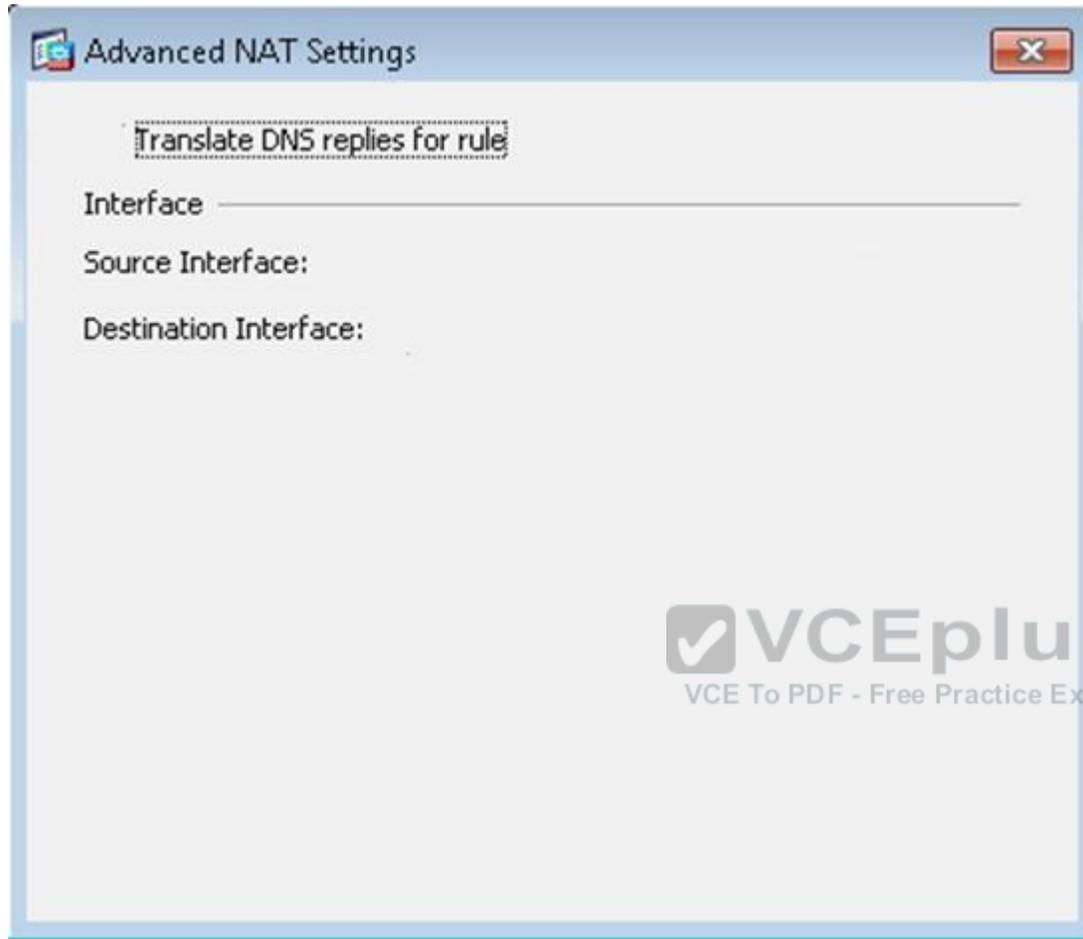


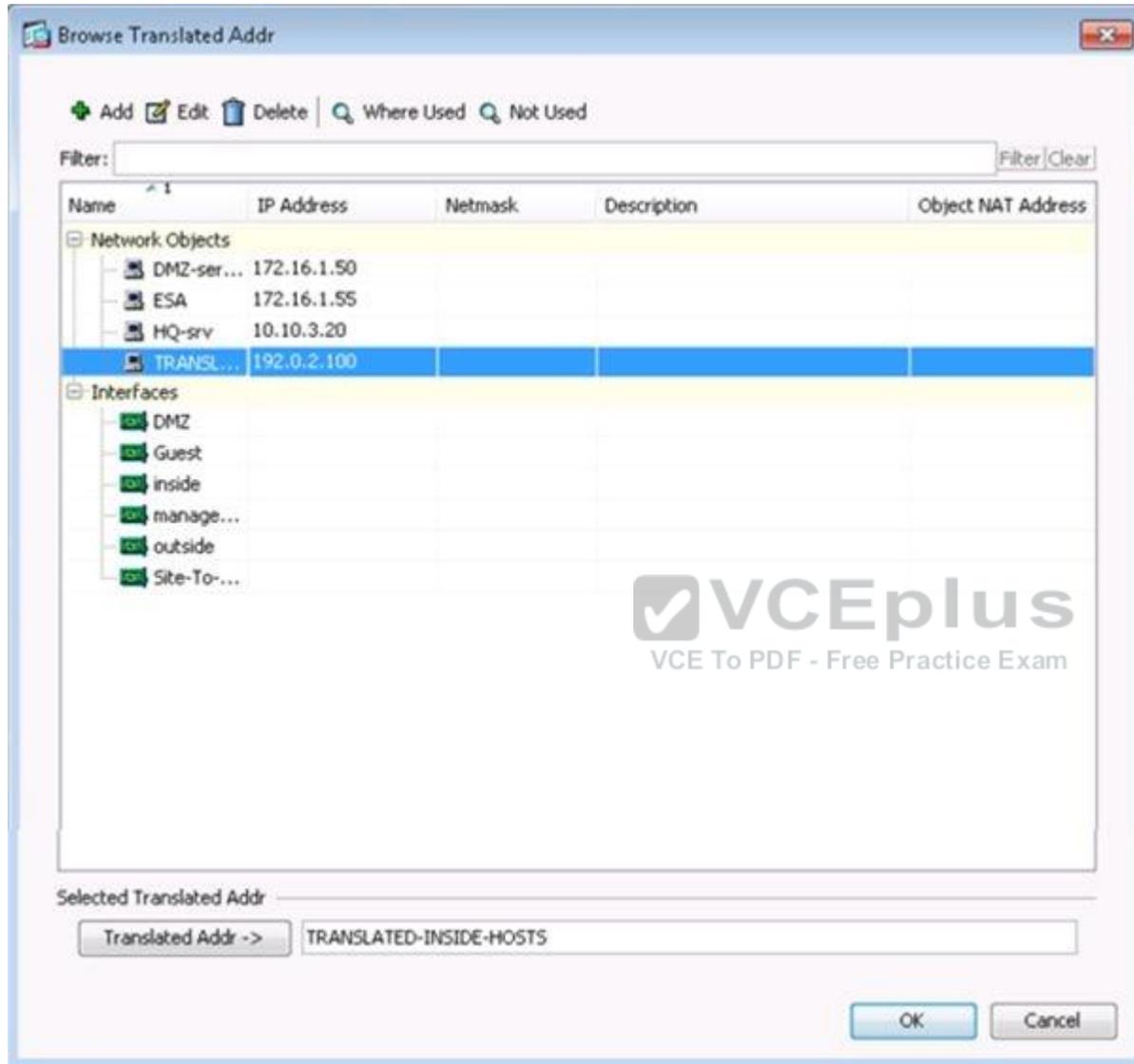
The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration for NAT Rules. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table of NAT rules. The table has columns for #, Source Intf, Dest Intf, Source, Destination, Service, Source, Destination, Service, Options, and Description. A single rule is listed with the following values:

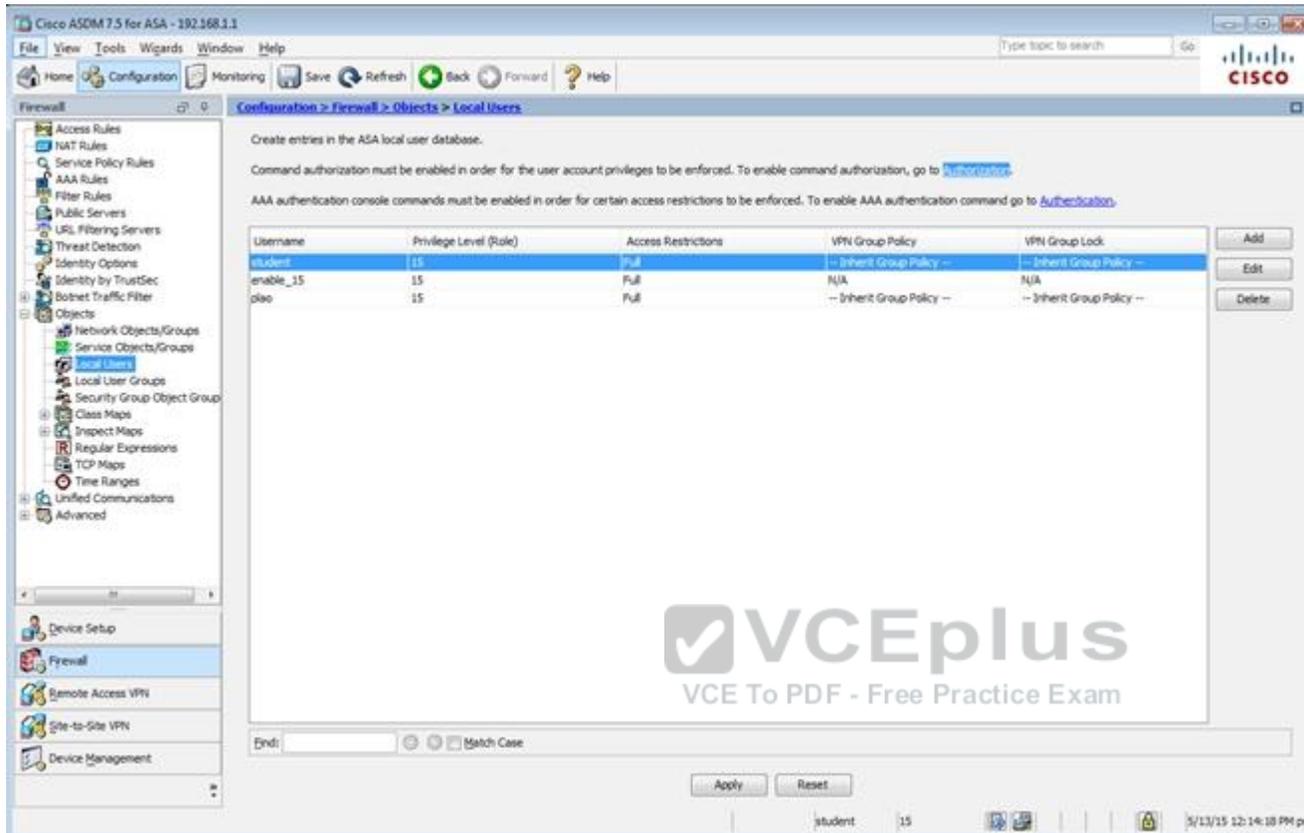
#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Options	Description
1	Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		

The interface also features a top menu bar with File, View, Tools, Wizards, Window, and Help. A search bar is present in the top right. The bottom status bar shows the user 'student', page number '15', and the date '5/13/15 12:13:18 PM pet'. A large watermark for VCEplus is overlaid on the bottom half of the screenshot.









Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

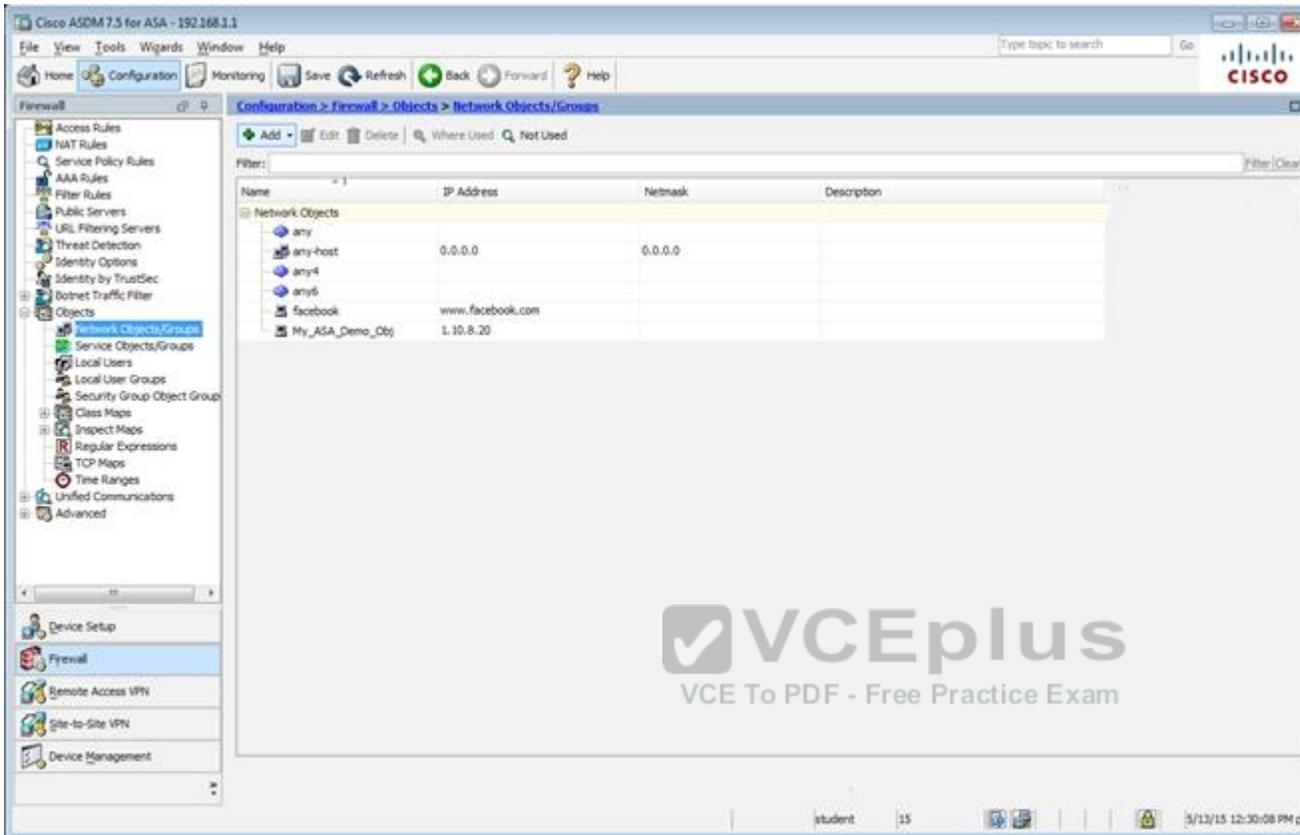
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End:

student 15 5/13/15 12:14:18 PM pst



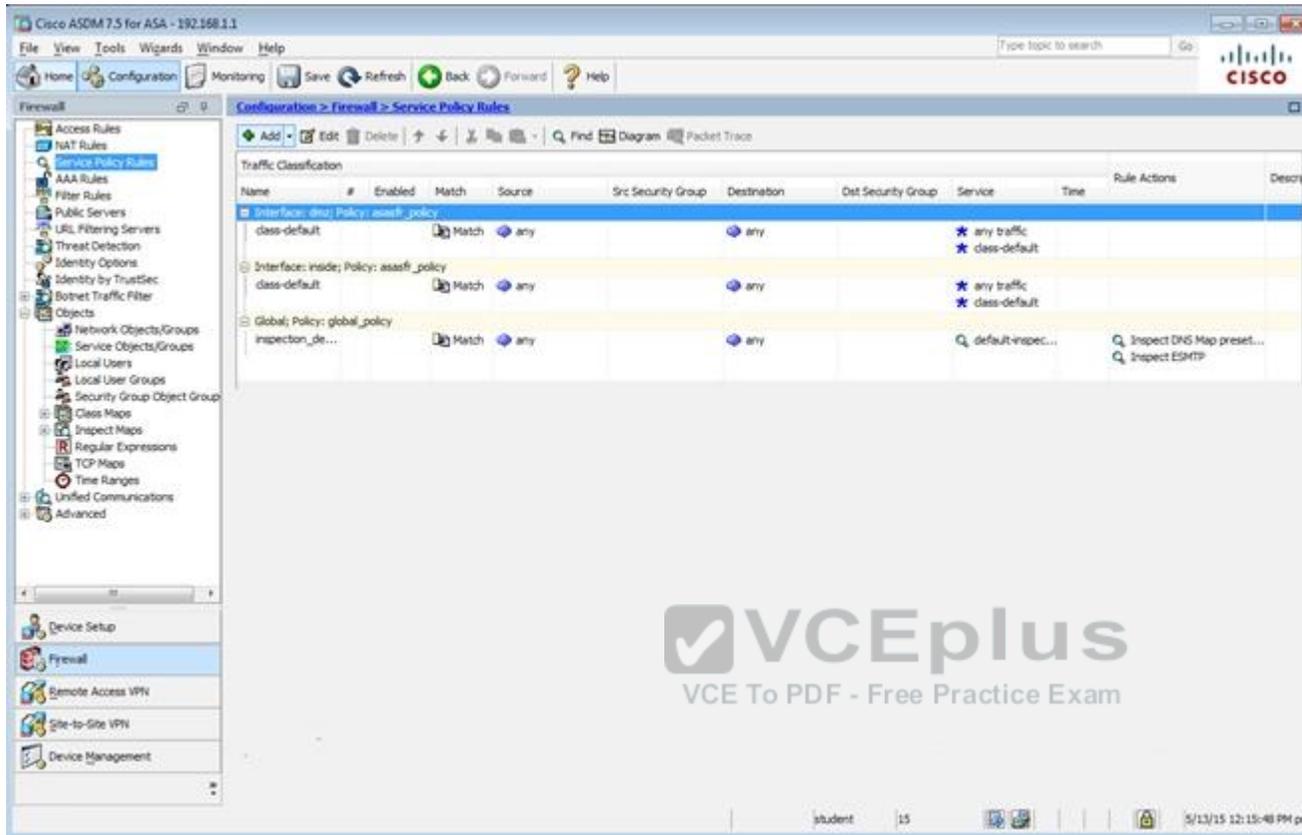
Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Network Objects/Groups

Filter: [Clear]

Name	IP Address	Netmask	Description
any			
any-host	0.0.0.0	0.0.0.0	
any4			
any6			
facebook	www.facebook.com		
My_ASA_Demo_Obj	1.10.8.20		

student 15 5/13/15 12:30:08 PM pet



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left sidebar shows a tree view of configuration categories, with "Firewall" selected. The main area shows a table of Traffic Classification rules. The table has columns for Name, #, Enabled, Match, Source, Src Security Group, Destination, Dst Security Group, Service, Time, Rule Actions, and Description. Three rules are visible: "Interface: dno; Policy: asash_policy", "Interface: inside; Policy: asash_policy", and "Global; Policy: global_policy".

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Interface: dno; Policy: asash_policy			Match	any		any		any traffic class-default			
Interface: inside; Policy: asash_policy			Match	any		any		any traffic class-default			
Global; Policy: global_policy			Match	any		any		default-inspec...		Inspect DNS Map preset... Inspect ESMTF	

At the bottom of the window, there is a watermark for "VCEplus VCE To PDF - Free Practice Exam" and a system tray showing the date and time as 5/13/15 12:15:48 PM pst.

Edit Service Policy Rule

Traffic Classification | Default Inspections | Rule Actions

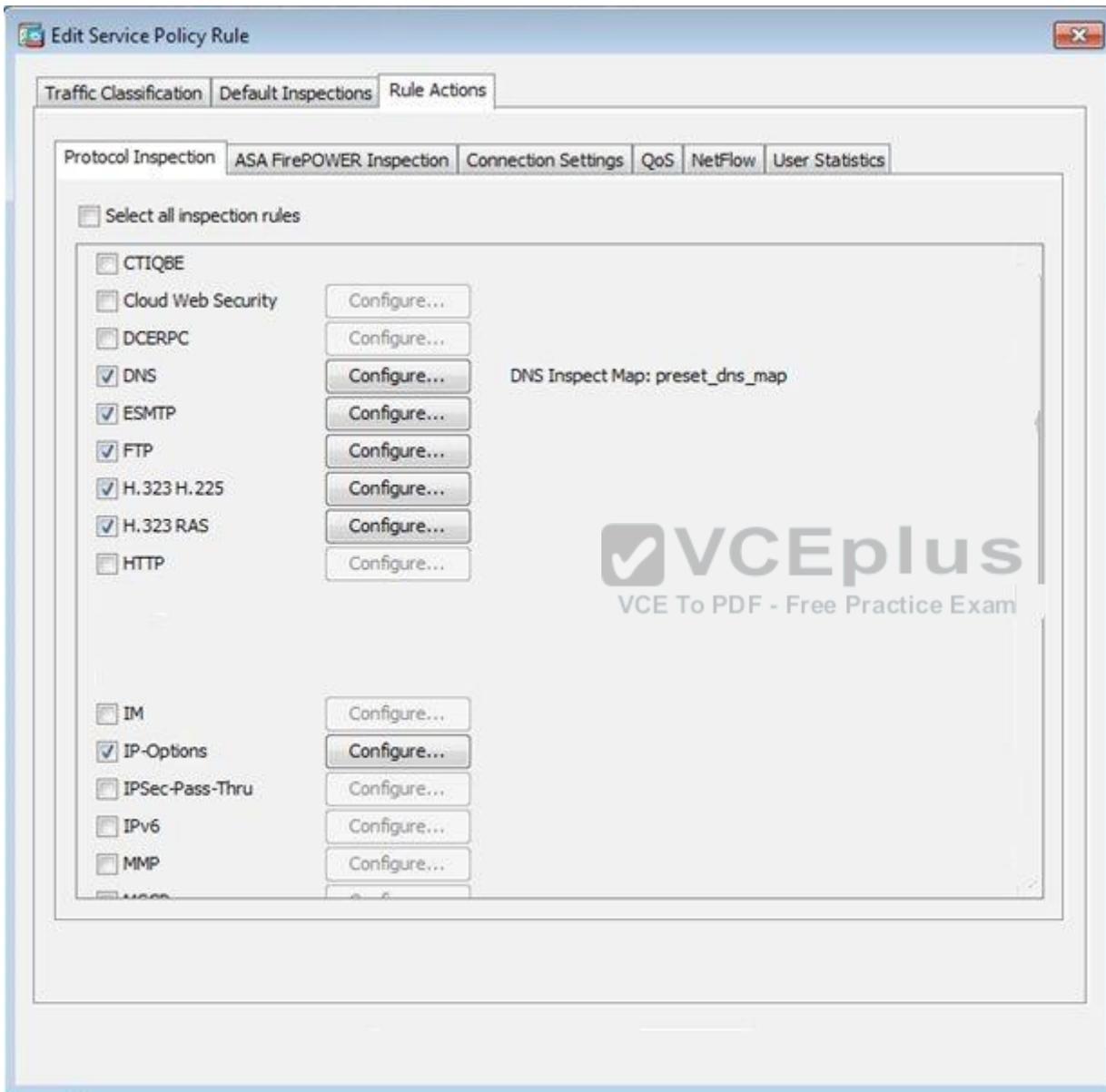
Name: inspection_default

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

 **VCEplus**
VCE To PDF - Free Practice Exam



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Access Rules". The left-hand navigation pane shows a tree structure with "Access Rules" selected. The main area contains a table of rules with the following columns: #, Enabled, Source Criteria, Destination Criteria, Service, Action, Hits, and Logging.

#	Enabled	Source Criteria:		Destination Criteria:		Service	Action	Hits	Logging
		Source	User	Destination	Security Group				
inetz (1 implicit incoming rule)									
1		any		Any less secure ne...	IP-IP	Permit			
inside (1 incoming rule)									
1		any		any	IP-IP	Permit	54...		
ingnt (0 implicit incoming rules)									
outside (0 implicit incoming rules)									
Global (1 implicit rule)									
1		any		any	IP-IP	Deny			

The bottom status bar shows the user "student", the number "15", and the date/time "5/13/15 12:28:58 PM pst".

Add Access Rule

Interface:

Action:

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

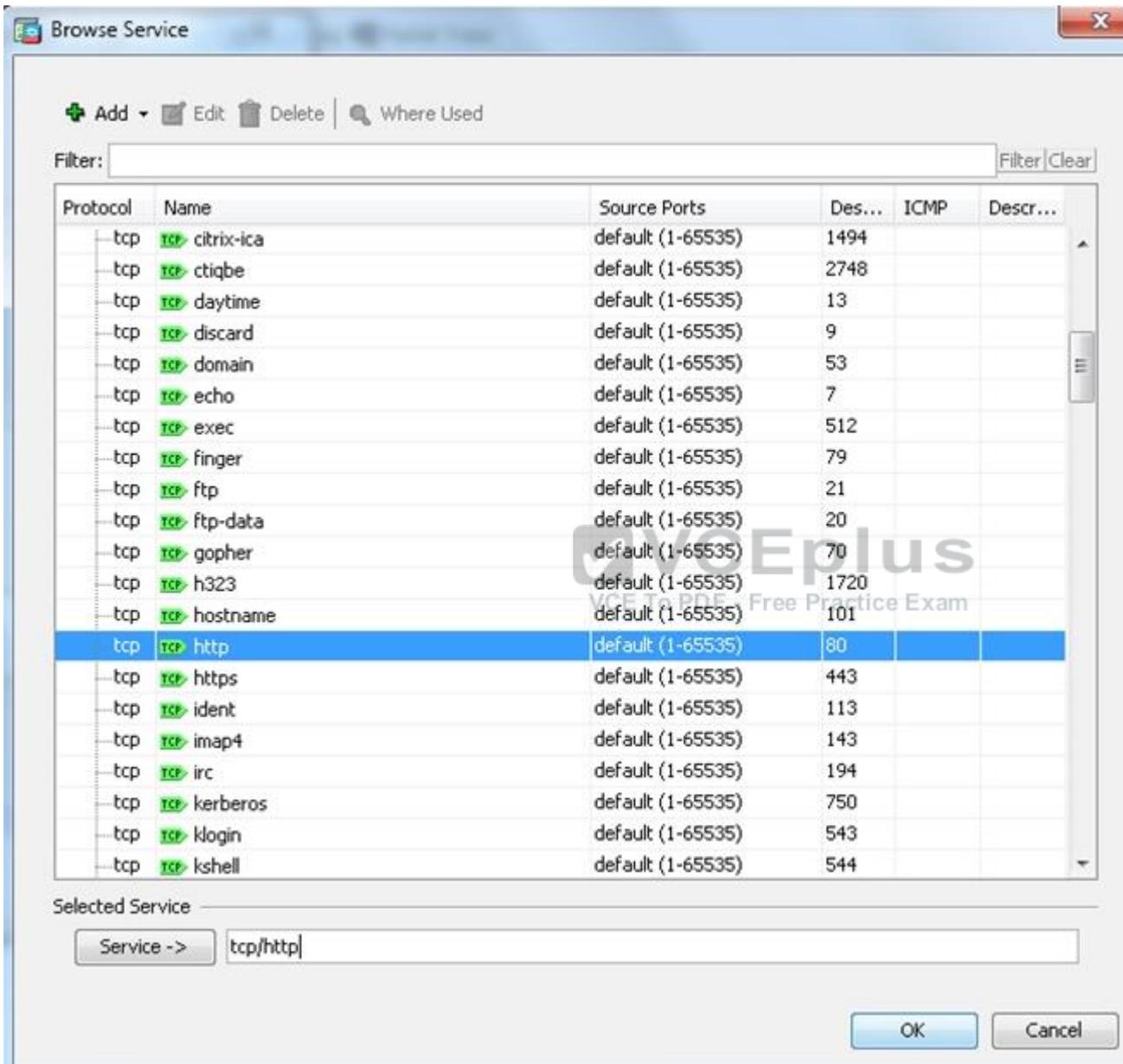
Description:

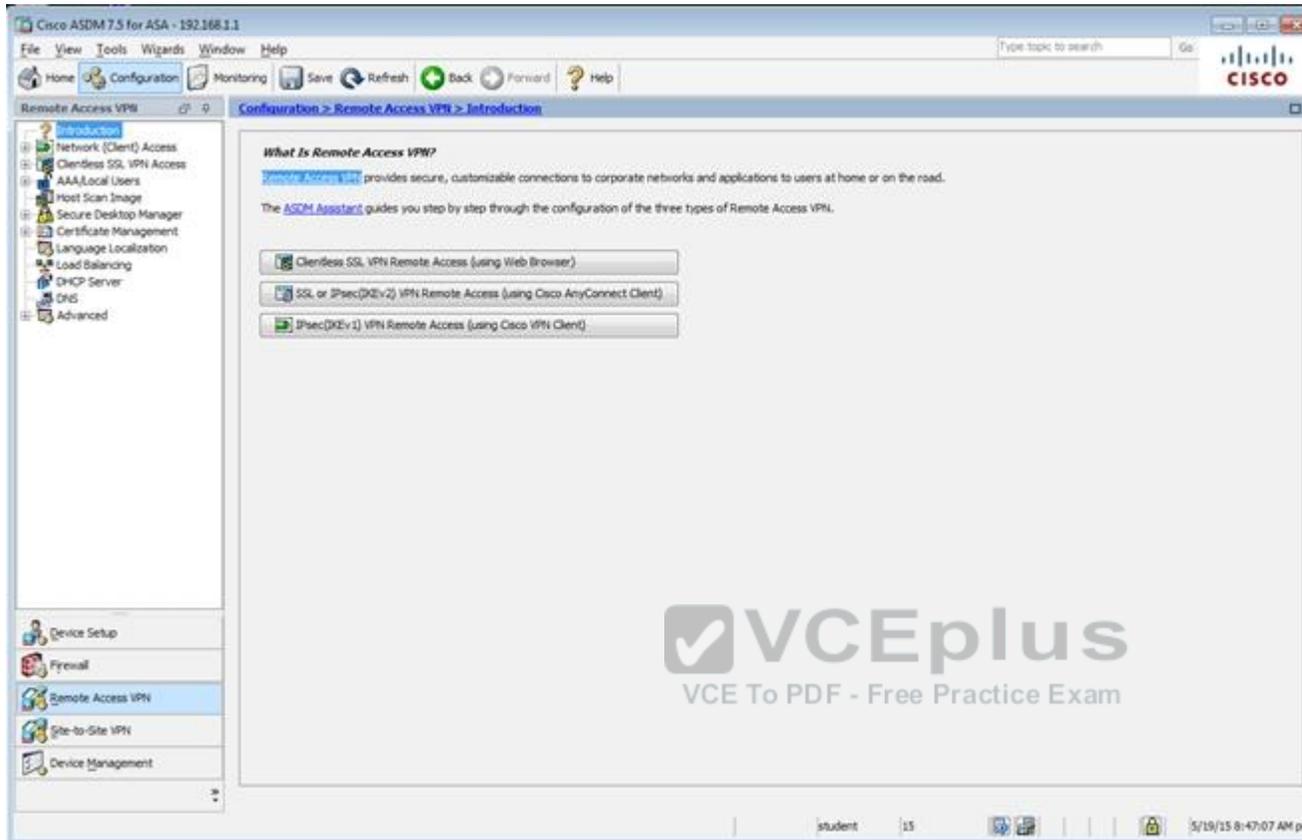
Enable Logging

Logging Level: Default

More Options

OK Cancel Help





The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 web interface. The main content area is titled "Remote Access VPN" and "Configuration > Remote Access VPN > Introduction". It includes a navigation menu on the left with categories like "Network (Client) Access", "Clientless SSL VPN Access", "AAA/Local Users", "Host Scan Image", "Secure Desktop Manager", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", and "Advanced". Below the menu are icons for "Device Setup", "Firewall", "Remote Access VPN", "Site-to-Site VPN", and "Device Management". The main content area contains the following text:

What Is Remote Access VPN?

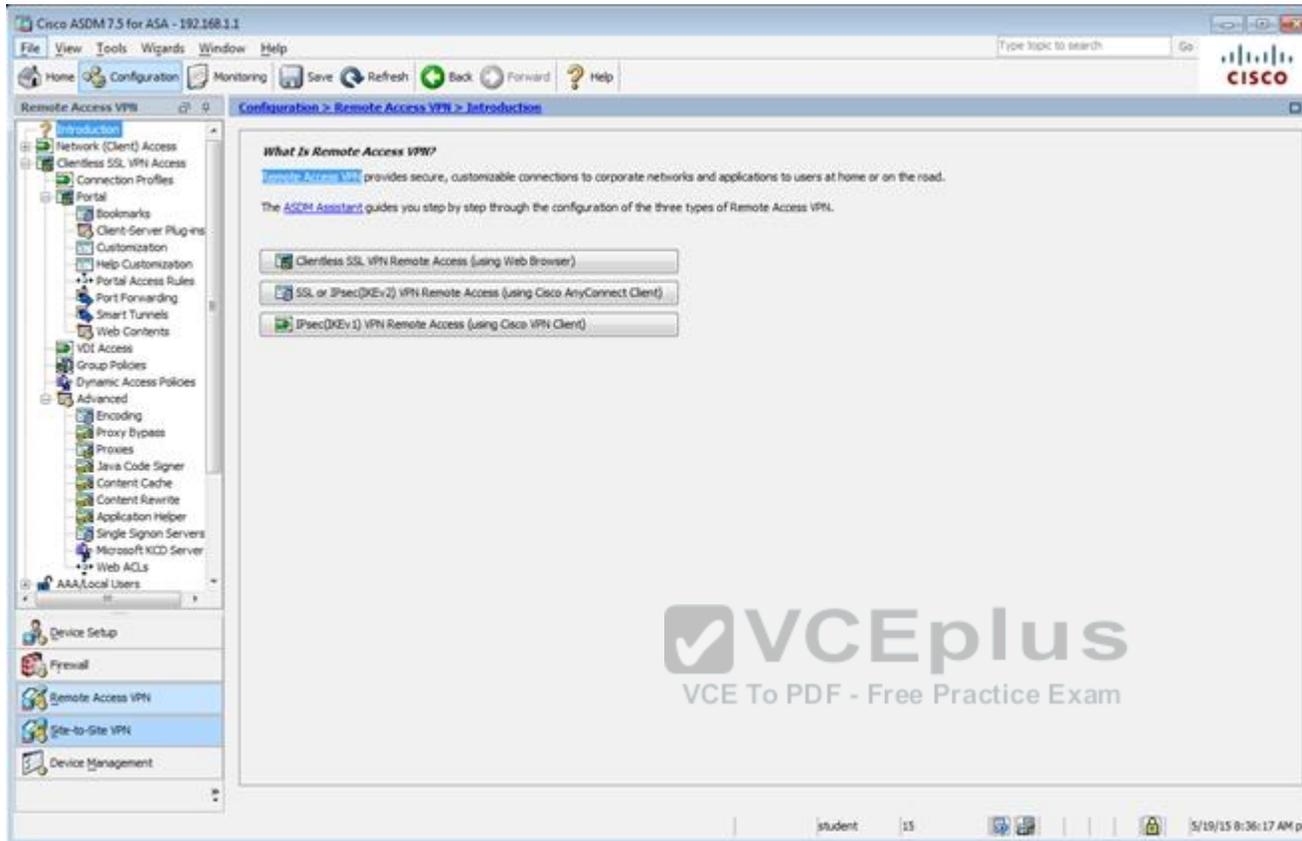
[Remote Access VPN](#) provides secure, customizable connections to corporate networks and applications to users at home or on the road.

The [ASDM Assistant](#) guides you step by step through the configuration of the three types of Remote Access VPN.

Three configuration options are listed in buttons:

- Clientless SSL VPN Remote Access (using Web Browser)
- SSL or IPsec(DKEv2) VPN Remote Access (using Cisco AnyConnect Client)
- IPsec(DKEv1) VPN Remote Access (using Cisco VPN Client)

A large "VCEplus VCE To PDF - Free Practice Exam" watermark is overlaid on the bottom right of the interface. The status bar at the bottom shows "student | 15 | 5/19/15 8:47:07 AM pst".



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Remote Access VPN > Introduction". The left sidebar shows a tree view of configuration options, with "Remote Access VPN" selected. The main content area contains the following text:

What Is Remote Access VPN?

Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road. The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.

Three configuration options are listed in buttons:

- Clientless SSL VPN Remote Access (Using Web Browser)
- SSL or IPsec(DKEv2) VPN Remote Access (Using Cisco AnyConnect Client)
- IPsec(DKEv1) VPN Remote Access (Using Cisco VPN Client)

A large watermark for VCEplus is overlaid on the bottom right of the screenshot.

The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The breadcrumb path is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.

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.

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 can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete, Find: _____ Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>		AAA(RADIUS)	DfltGrpPolicy
Services	<input checked="" type="checkbox"/>	test	LOCAL	Default

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:38:47 AM pst

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
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

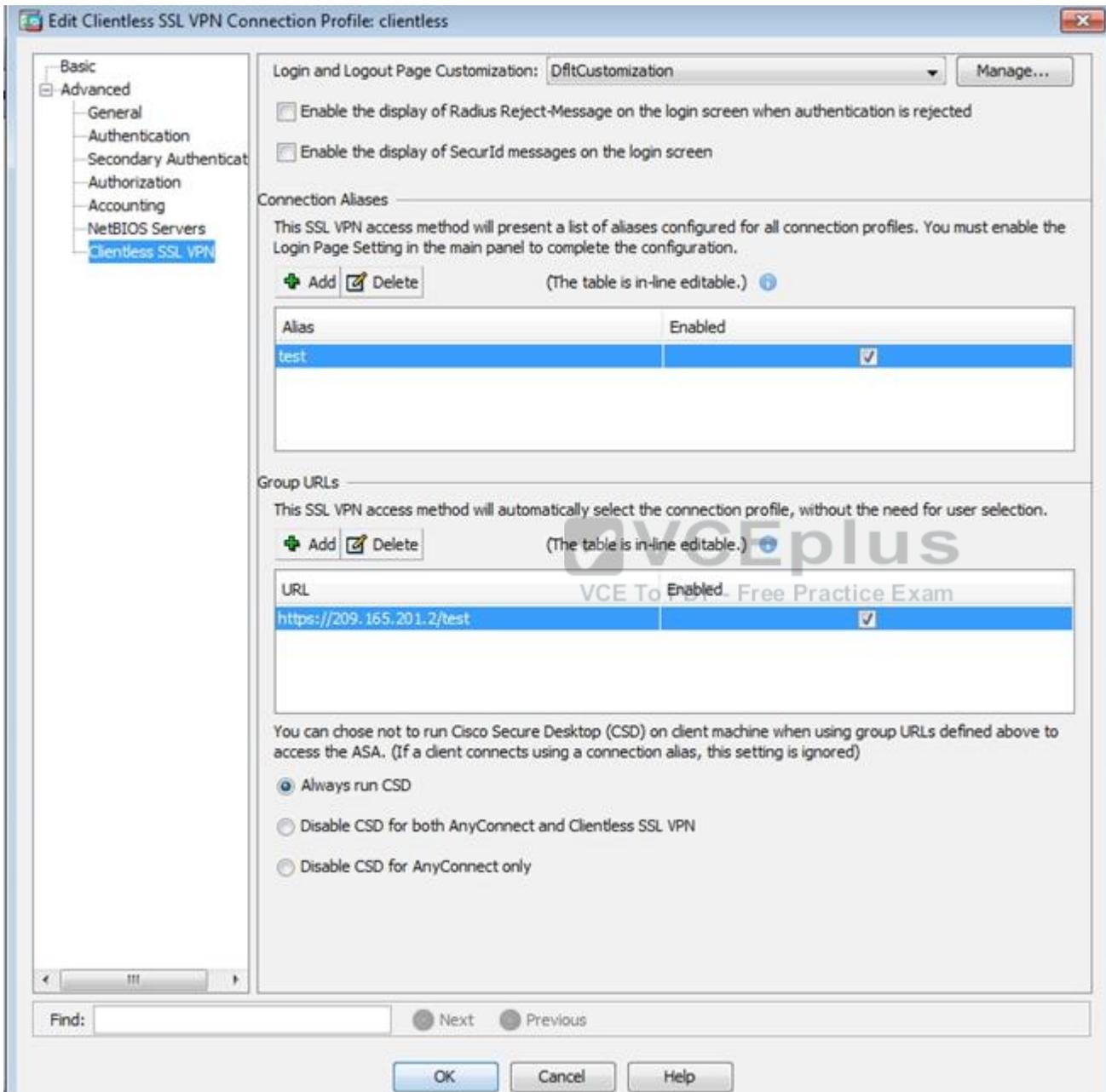
(Following field is an attribute of the group policy selected above.)

Enable clientless SSL VPN protocol

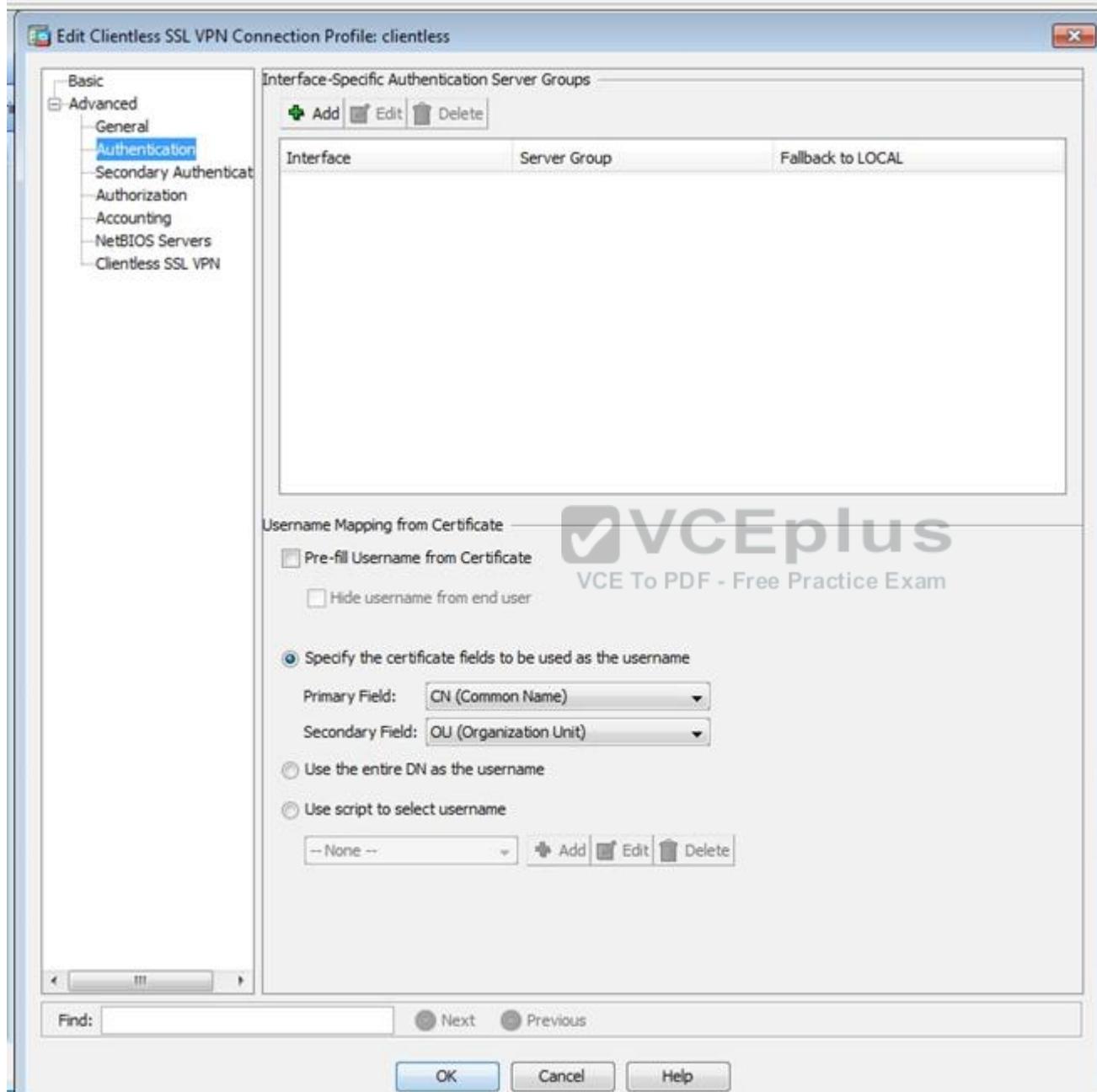
Find:

Next Previous

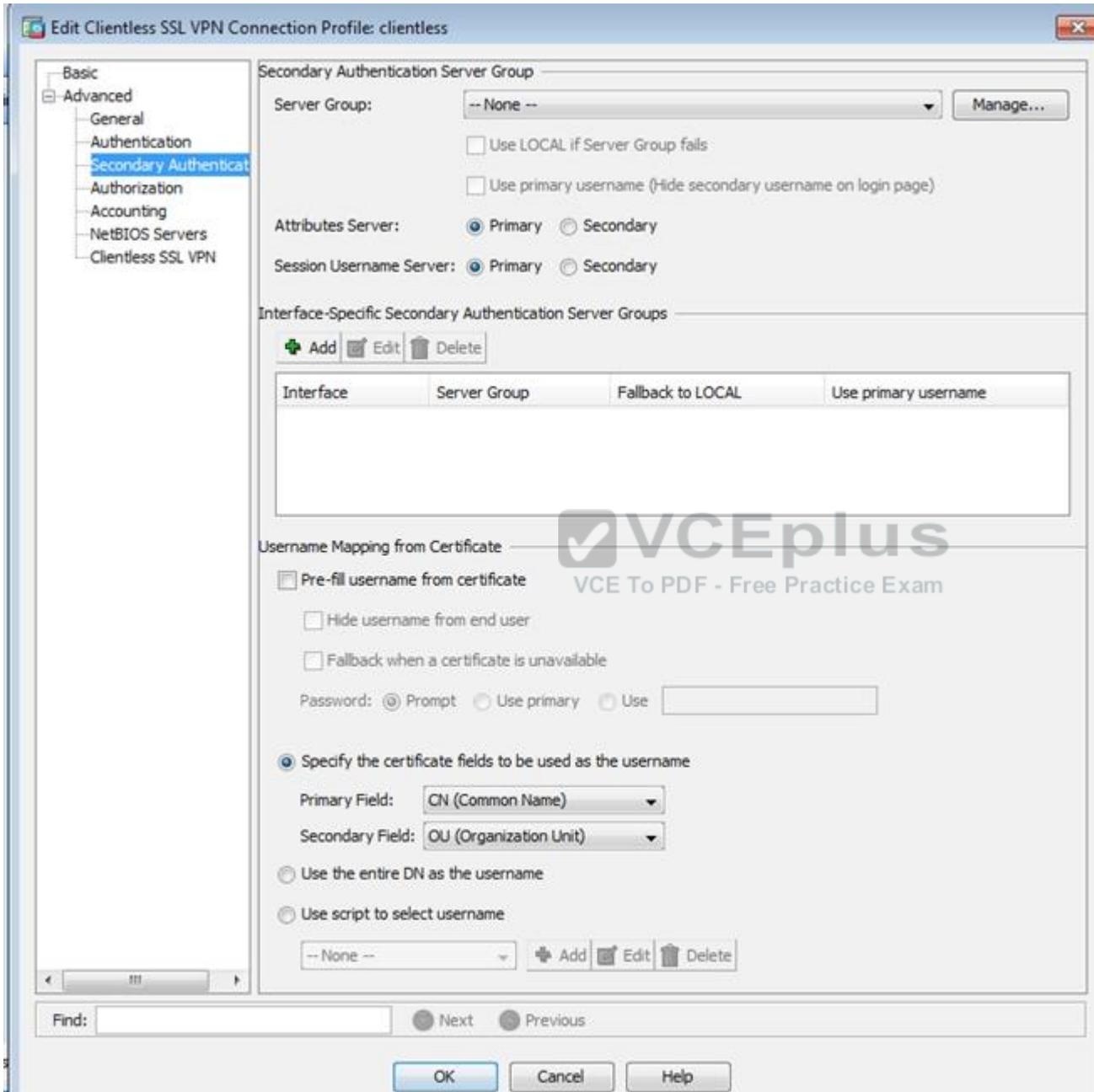


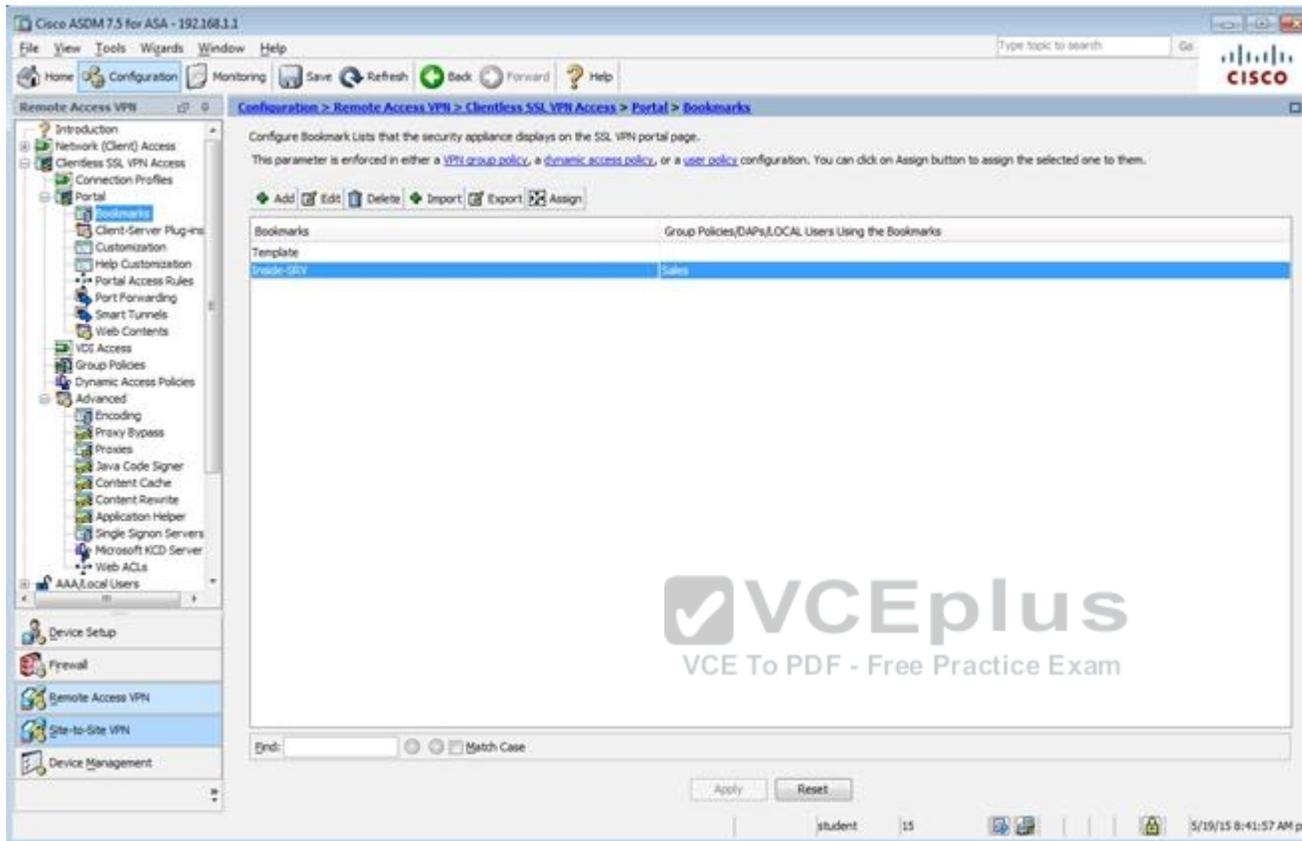












The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main window displays the configuration page for Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area contains the following text:

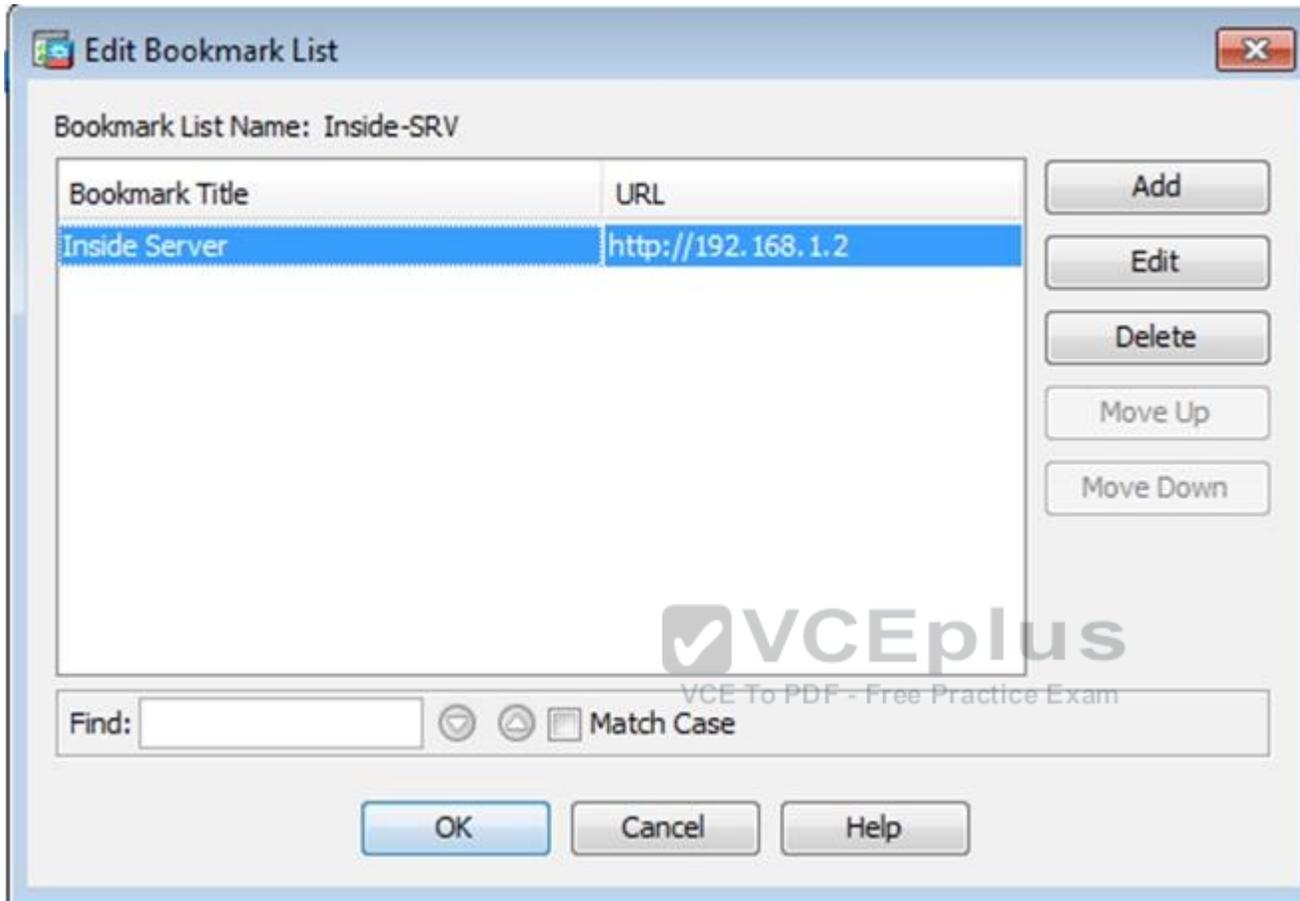
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

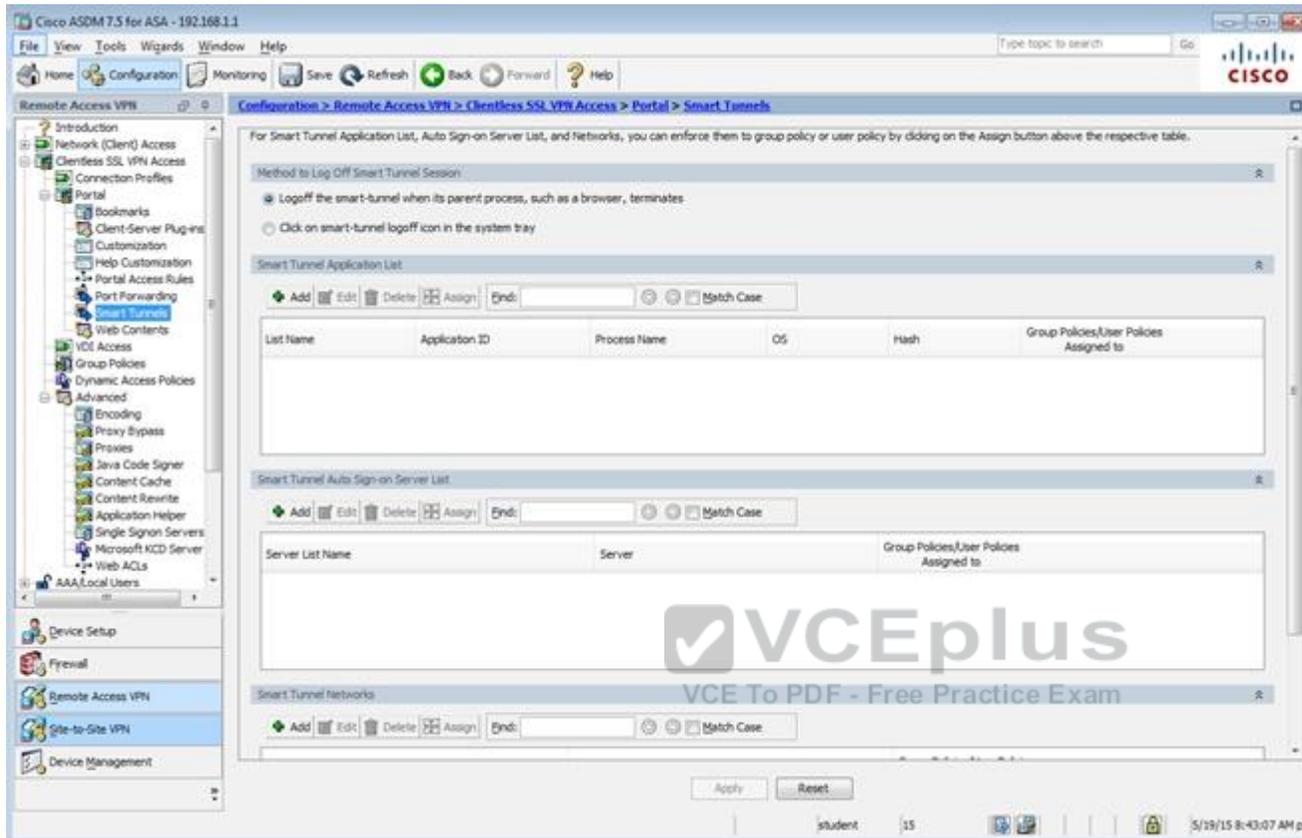
Buttons: Add, Edit, Delete, Import, Export, Assign

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Inside-SLV	Sales

Buttons: Apply, Reset

Footer: student 15 5/19/15 8:41:57 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels

For Smart Tunnel Application List, Auto Sign-on Server List, and Networks, you can enforce them to group policy or user policy by clicking on the Assign button above the respective table.

Method to Log Off Smart Tunnel Session

- Logoff the smart-tunnel when its parent process, such as a browser, terminates
- Click on smart-tunnel logoff icon in the system tray

Smart Tunnel Application List

List Name	Application ID	Process Name	OS	Hash	Group Policies/User Policies Assigned to
-----------	----------------	--------------	----	------	--

Smart Tunnel Auto Sign-on Server List

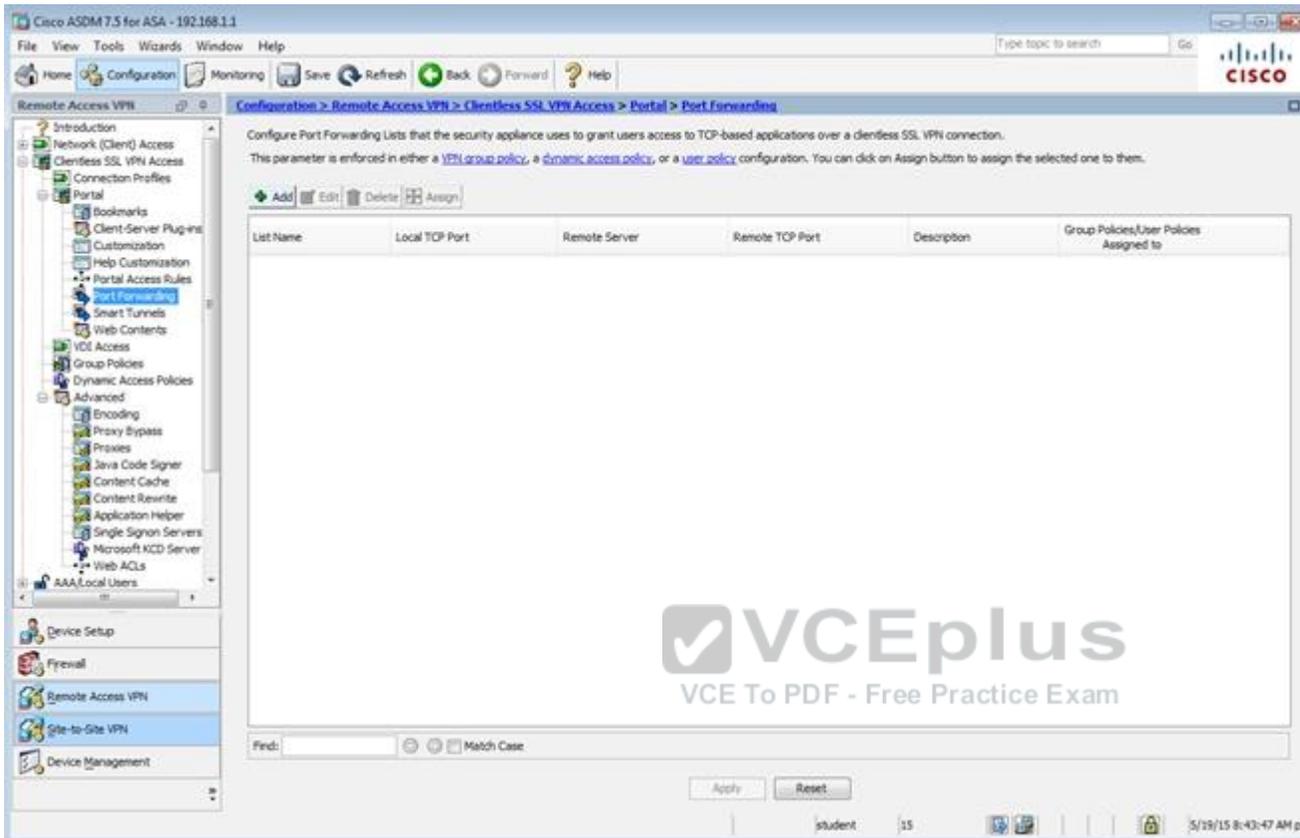
Server List Name	Server	Group Policies/User Policies Assigned to
------------------	--------	--

Smart Tunnel Networks

Network Name	Network	Group Policies/User Policies Assigned to
--------------	---------	--

Apply Reset

student 15 5/19/15 8:43:07 AM pst



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding. The main content area contains the following text:

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them.

Buttons: Add, Edit, Delete, Assign

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description	Group Policies/User Policies Assigned to
-----------	----------------	---------------	-----------------	-------------	--

Buttons: Apply, Reset

Search: Find: [] Match Case

Footer: student 15 5/19/15 8:43:47 AM pst

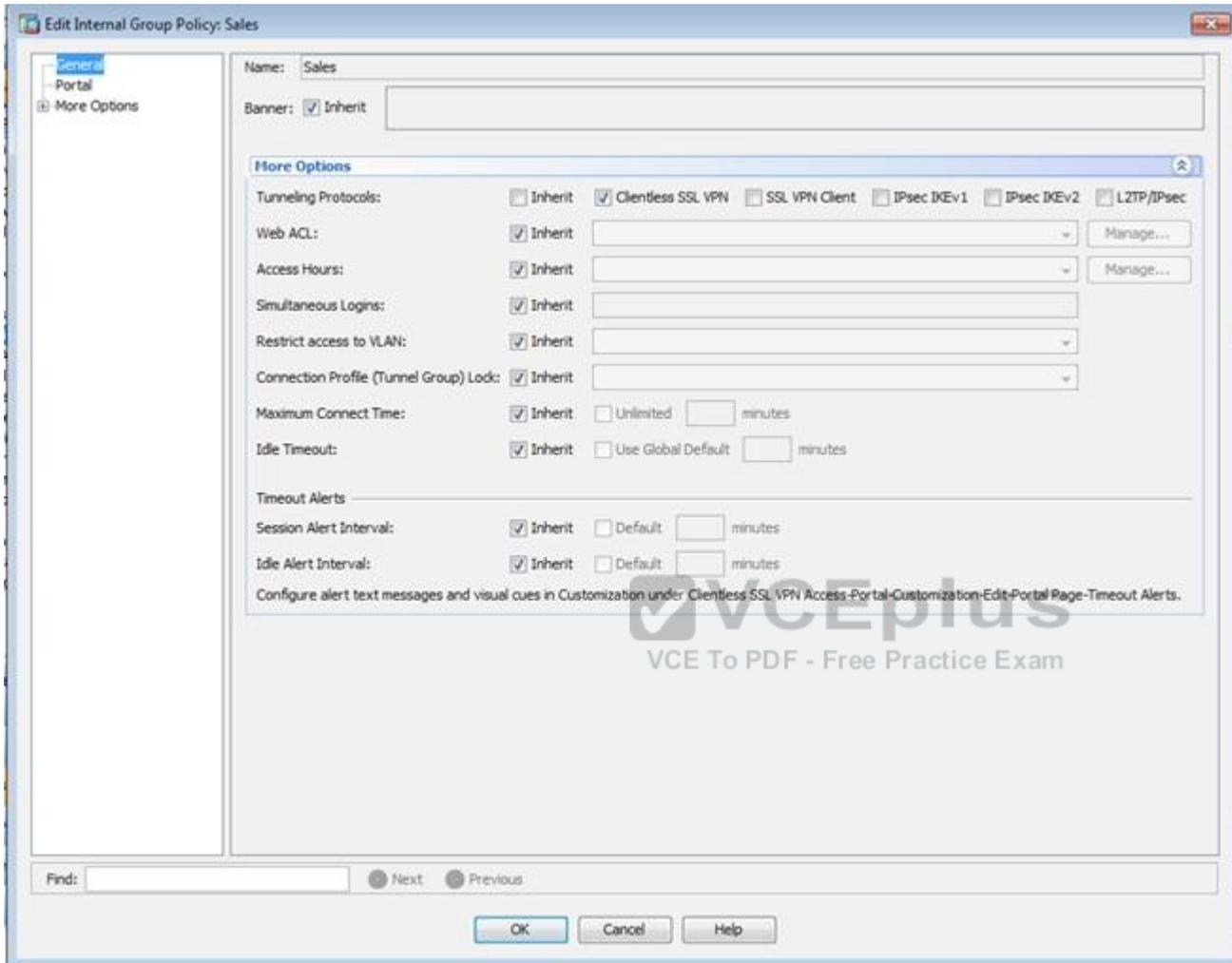
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

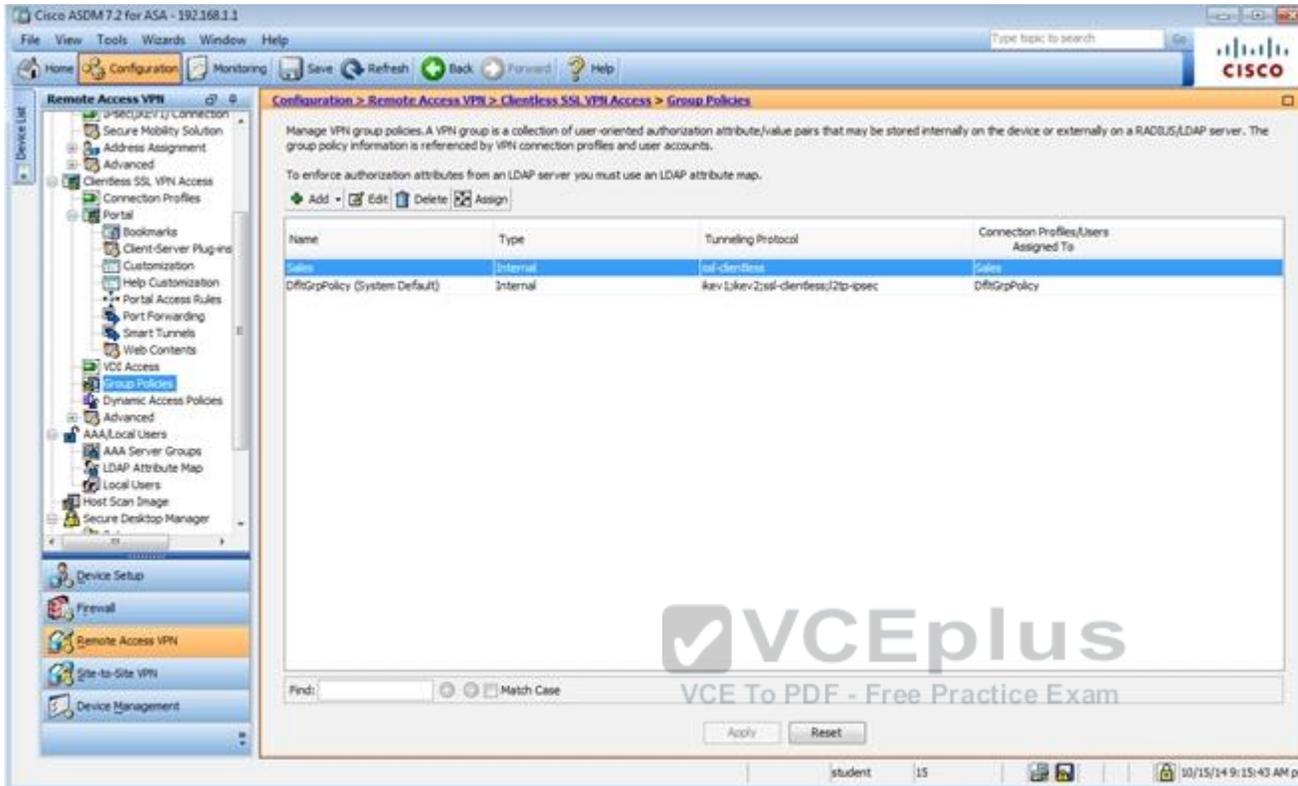
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

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

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	ssl-clientless	Clientless
DiffGrpPolicy (System Default)	Internal	Rev 1;rev 2;ssl-clientless;2tp-espsec	DefaultRAGroup;Default;2;Group;DefaultADMPDGroup;Def...

End:





Cisco ASDM 7.2 for ASA - 192.168.1.1

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 pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group 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.

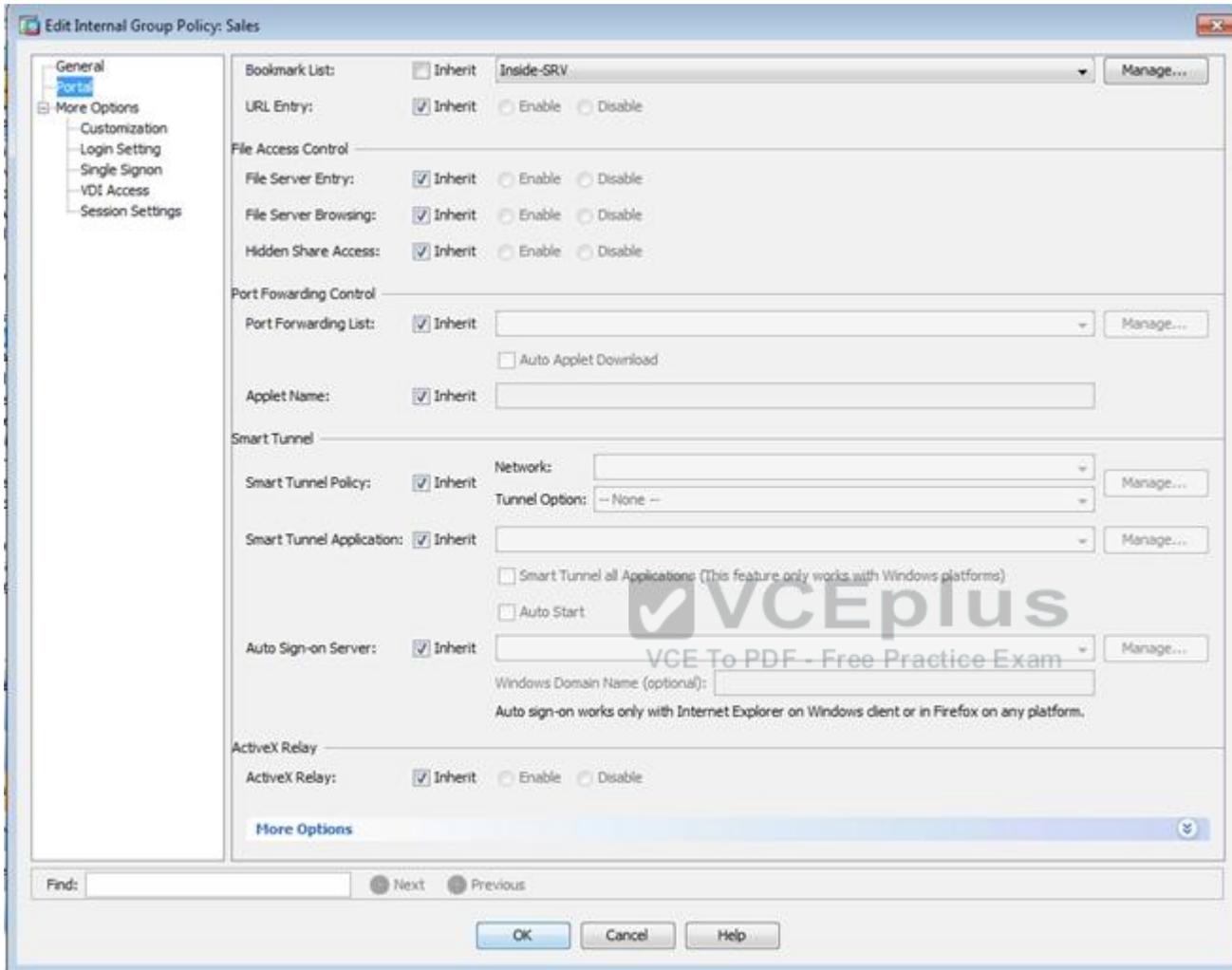
◆ Add ◆ Edit ◆ Delete ◆ Assign

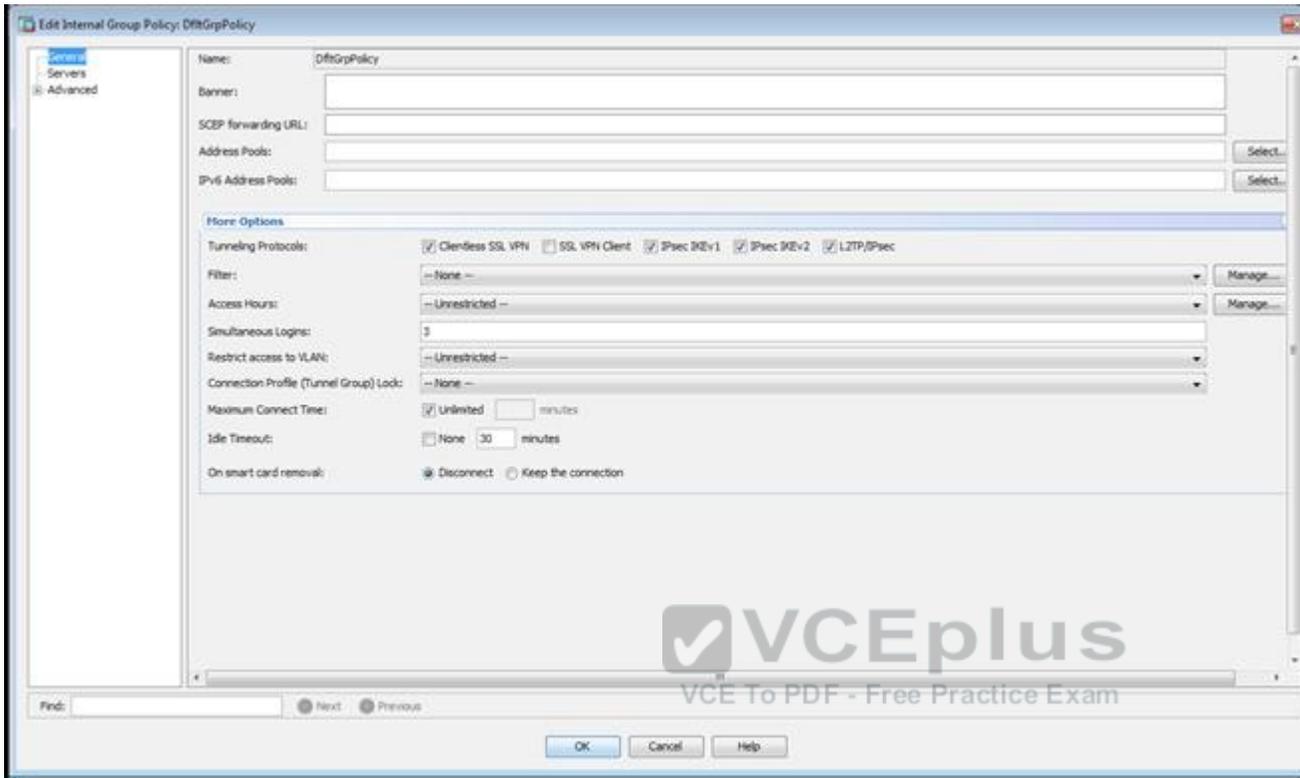
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	l2l-Service	Sales
DfltGrpPolicy (System Default)	Internal	kev-l2l-ssl-clientless/l2l-sspec	DfltGrpPolicy

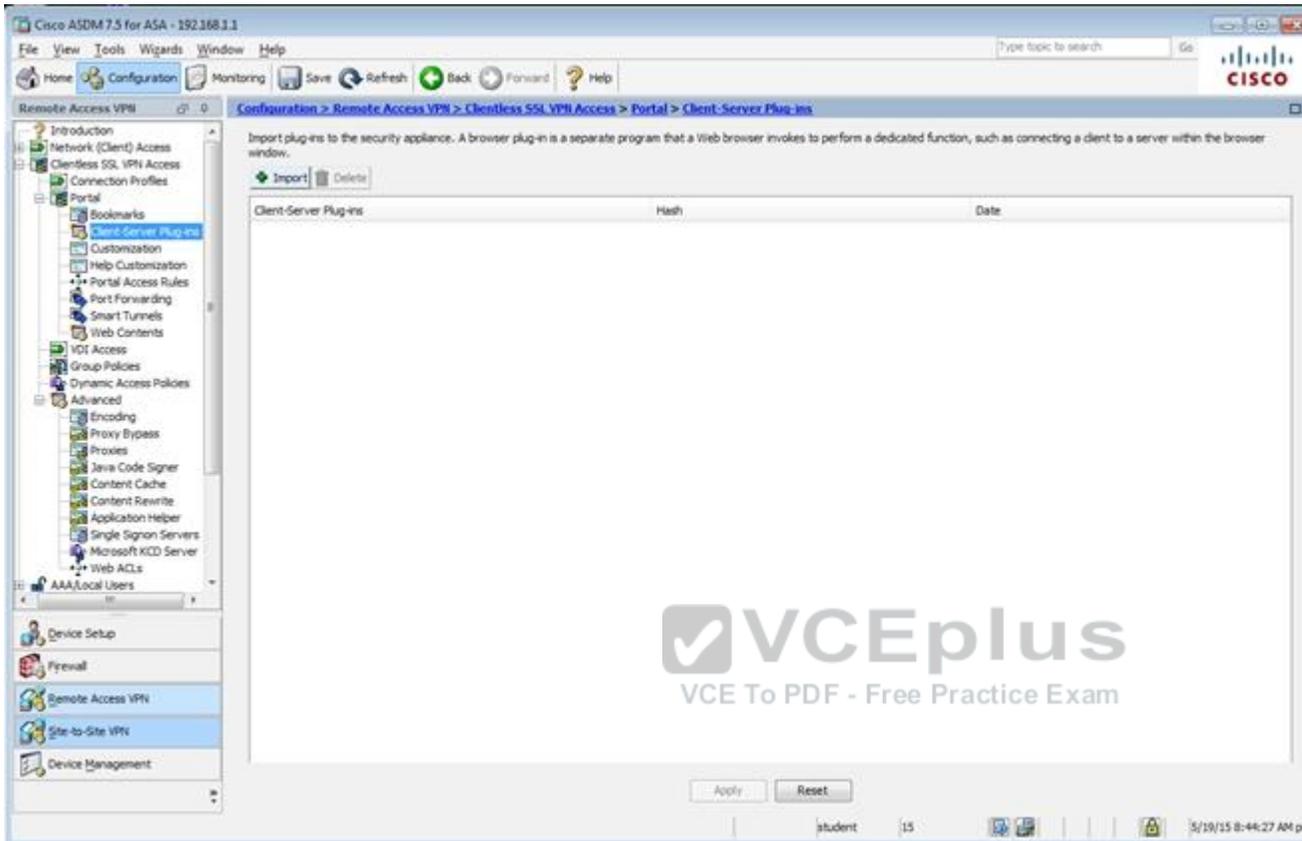
Find: Match Case

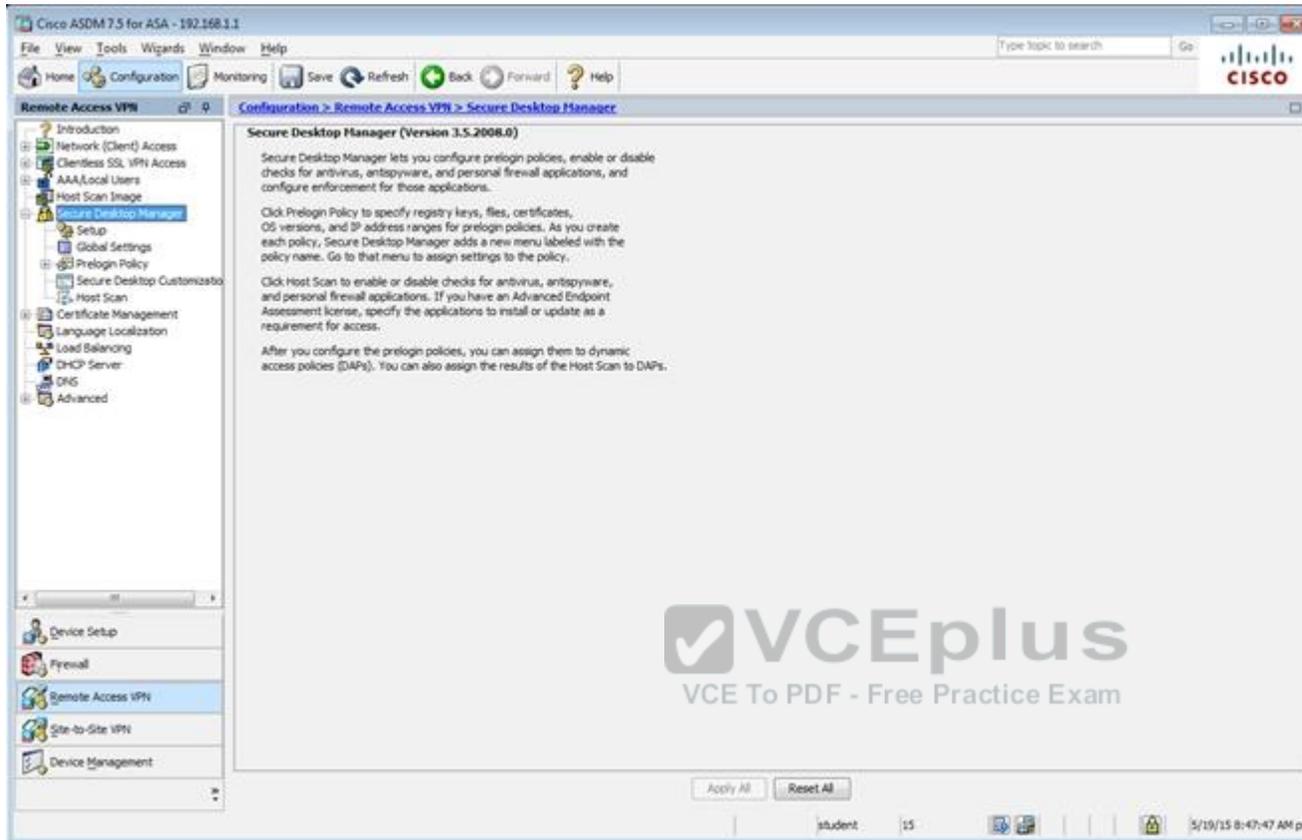
Apply Reset

student | 15 | 10/15/14 9:15:43 AM pst









The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is titled "Secure Desktop Manager (Version 3.5.2008.0)". The left-hand navigation pane shows a tree structure with "Remote Access VPN" expanded, and "Secure Desktop Manager" selected. The main pane contains the following text:

Secure Desktop Manager (Version 3.5.2008.0)

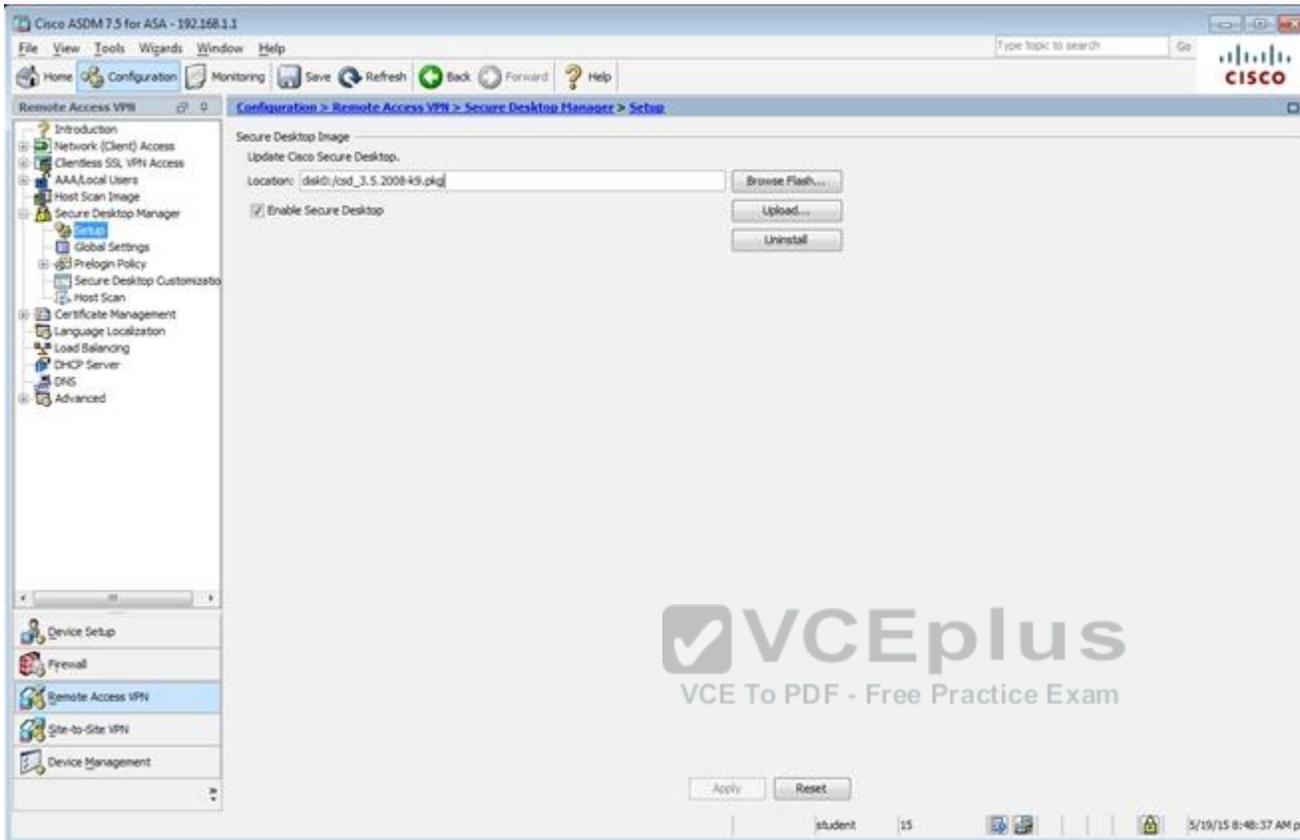
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispyware, and personal firewall applications, and configure enforcement for those applications.

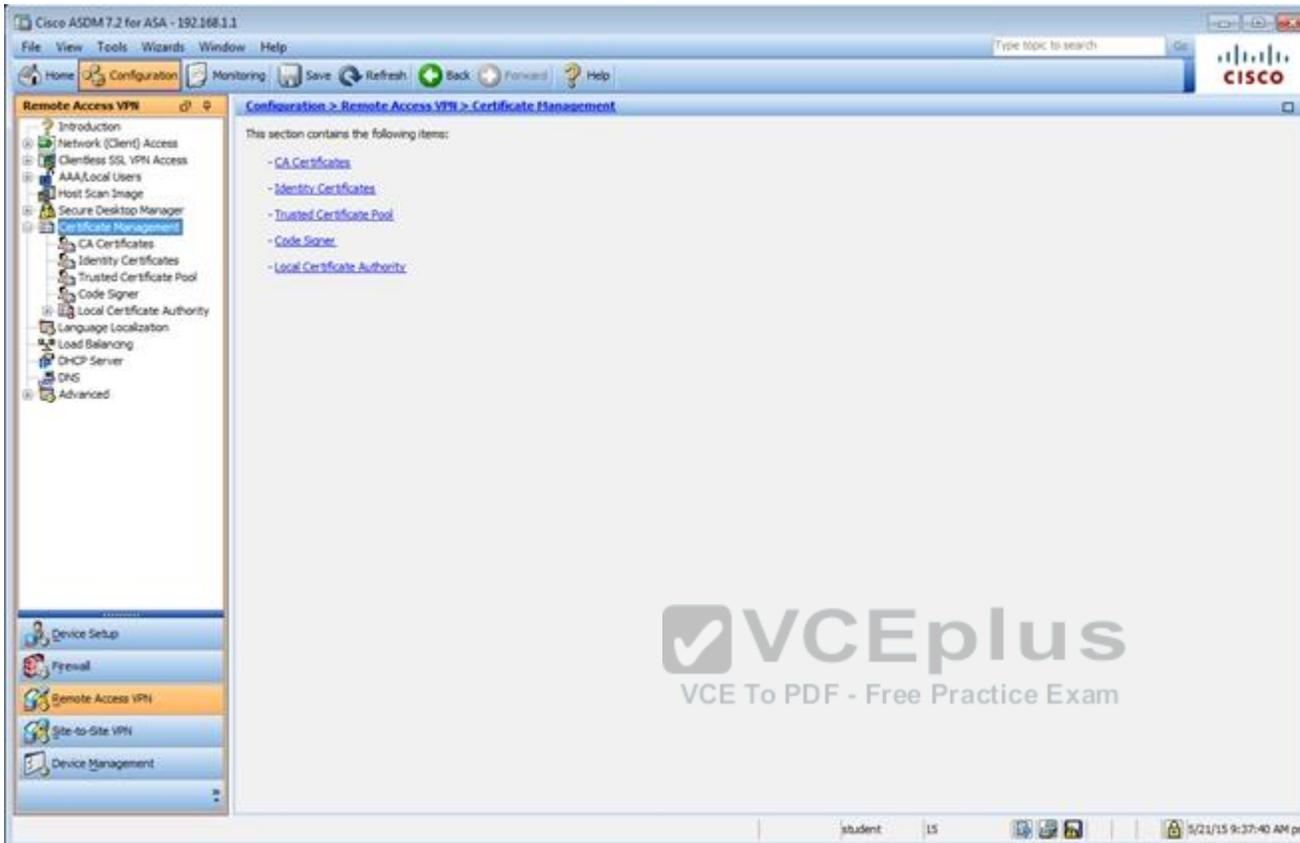
Click Prelogin Policy to specify registry keys, files, certificates, OS versions, and IP address ranges for prelogin policies. As you create each policy, Secure Desktop Manager adds a new menu labeled with the policy name. Go to that menu to assign settings to the policy.

Click Host Scan to enable or disable checks for antivirus, antispyware, and personal firewall applications. If you have an Advanced Endpoint Assessment license, specify the applications to install or update as a requirement for access.

After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.

At the bottom of the main pane, there are "Apply All" and "Reset All" buttons. The status bar at the bottom of the window shows "student | 15 | 5/19/15 8:47:47 AM pst".





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname-wf [7-ASA,sec...	hostname-wf [7-ASA,sec...	11:10:33 pmt Oct 20 2024	ASDM_TrustPoint1	General Purpose	RSA (2048 bits)

End: Match Case

Certificate Expiration Alerts

Send the first alert before: 60 (days)

Repeat Alert Interval: 7 (days)

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

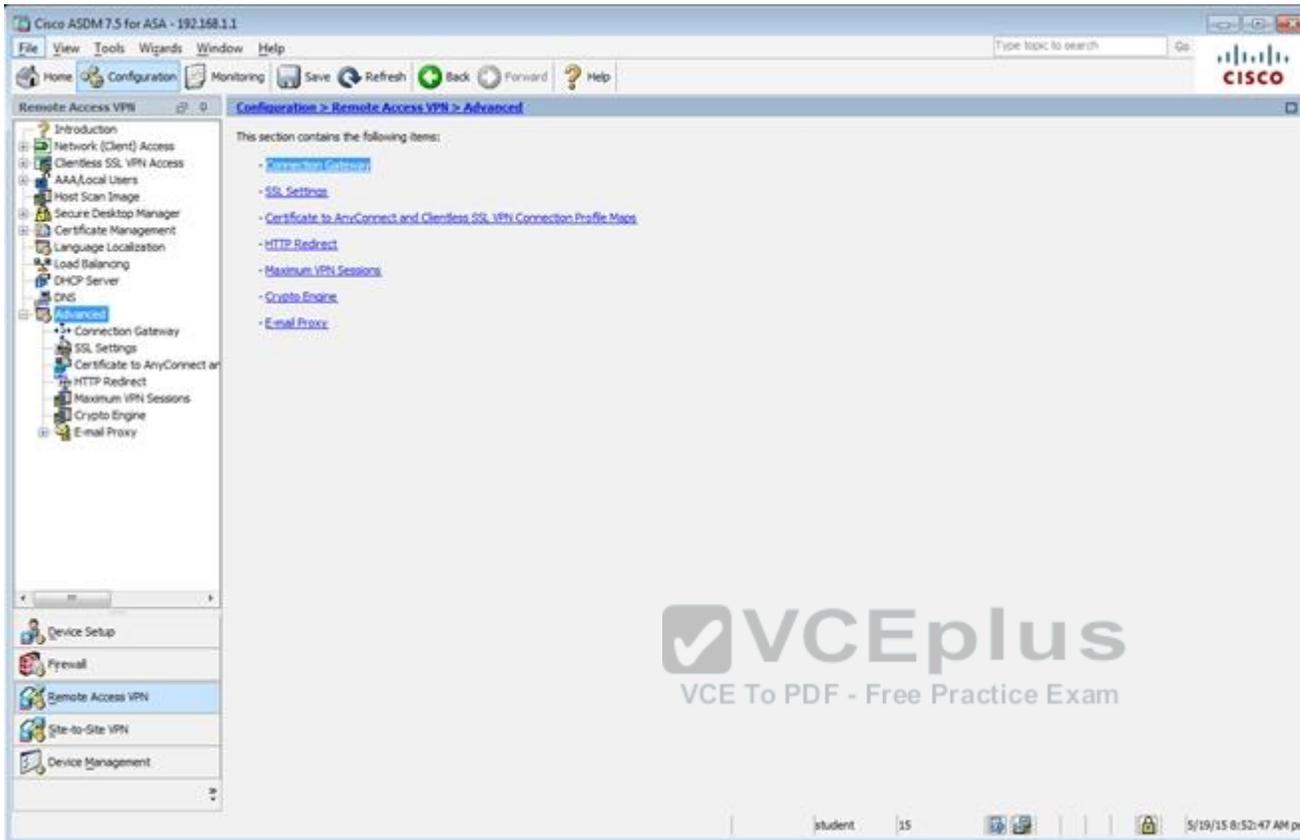
Enroll ASA SSL certificate with Entrust.

Using a previously saved certificate signing request, [enroll with Entrust](#).

ASDM Identity Certificate Wizard

The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

student 15 5/19/15 8:51:47 AM pet



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 > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The minimum SSL version for the security appliance to negotiate as a "server": TLS V1

The minimum SSL version for the security appliance to negotiate as a "client": TLS V1

Diffie-Hellman group to be used with SSL: Group2 - 1024-bit modulus

ECDH group to be used with SSL: Group19 - 256-bit EC

Encryption

Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String	Edit
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...	
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...	
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...	
TLSV1.2	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...	
DTLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...	

Server Name Indication (SNI)

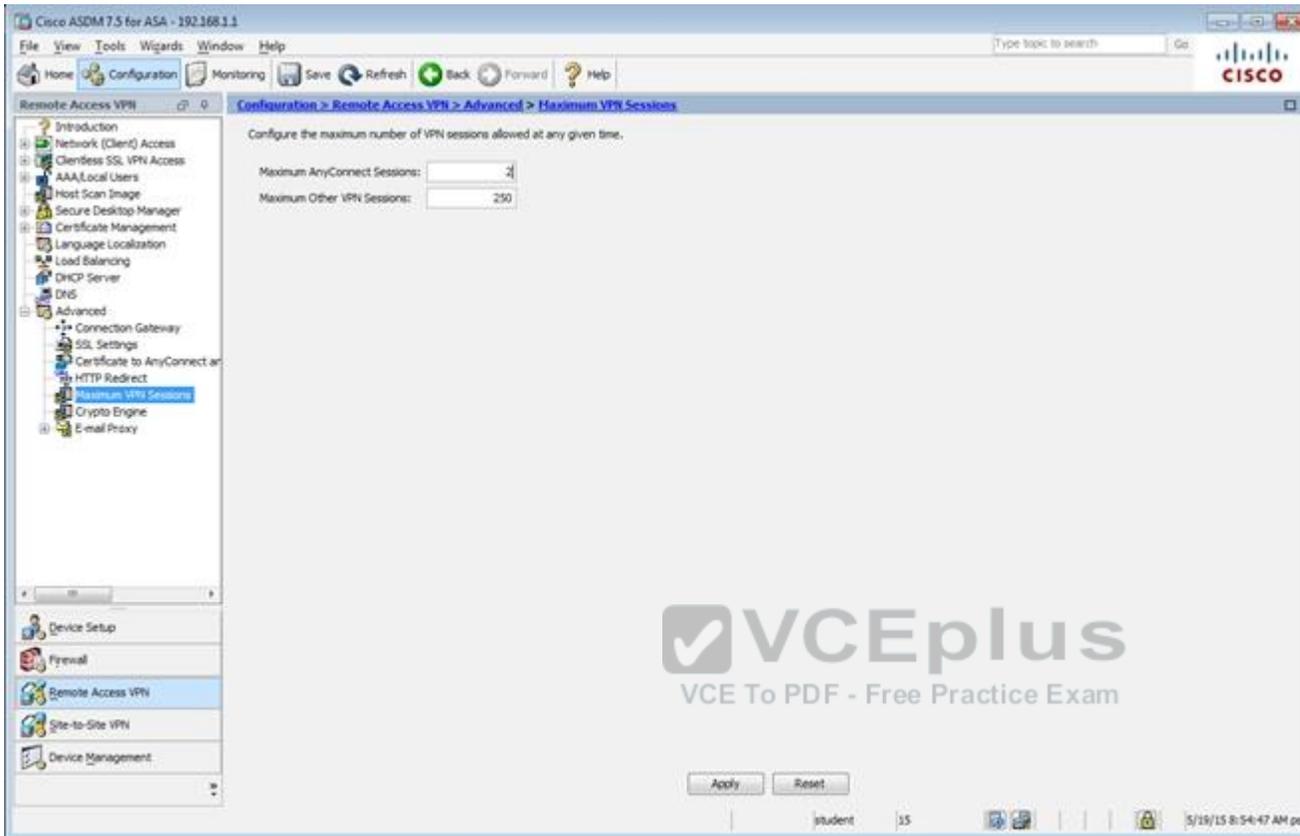
Domain	Certificate	Add	Edit	Delete
dmz	ASDM_ThaIPont1.h...			

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

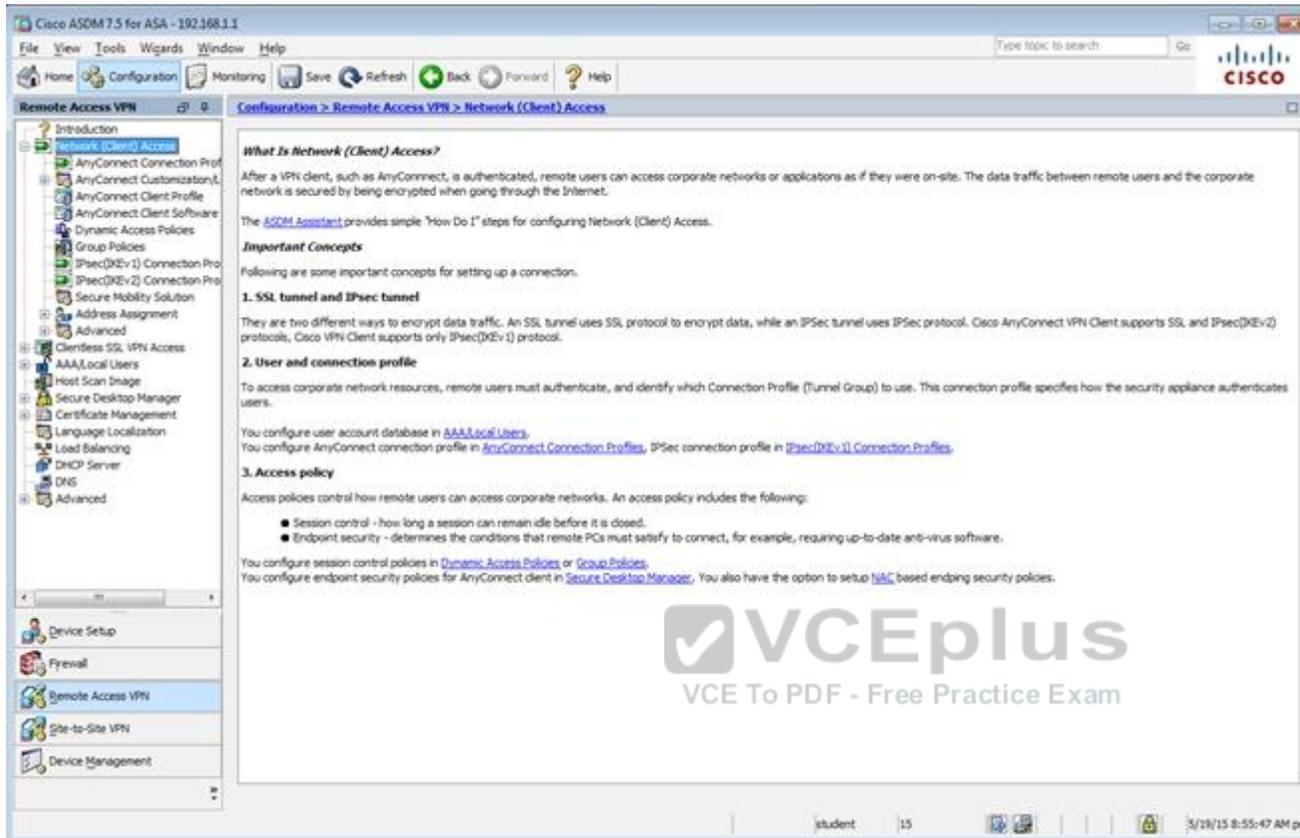
Apply Reset

student 15 3/19/15 8:54:07 AM pst



The screenshot shows the Cisco ASDM 7.5 for ASA configuration interface. The browser title is "Cisco ASDM 7.5 for ASA - 192.168.1.1". The breadcrumb navigation is "Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions". The main content area is titled "Configure the maximum number of VPN sessions allowed at any given time." and contains two input fields: "Maximum AnyConnect Sessions:" with a value of 2, and "Maximum Other VPN Sessions:" with a value of 250. The left sidebar shows a tree view with "Maximum VPN Sessions" selected. The bottom of the window has "Apply" and "Reset" buttons, and a system tray showing the user "student" and the date "5/19/15 8:54:47 AM pst".

 **VCEplus**
VCE To PDF - Free Practice Exam



The screenshot shows the Cisco ASDM 7.5 interface for configuration. The left sidebar lists various configuration categories, with 'Remote Access VPN' selected. The main content area displays the 'Network (Client) Access' configuration page. The page title is 'Configuration > Remote Access VPN > Network (Client) Access'. The content includes a section titled 'What is Network (Client) Access?' which explains that after a VPN client is authenticated, remote users can access corporate networks or applications as if they were on-site. It also mentions that data traffic is encrypted when going through the Internet. Below this, it states that the ASDM Assistant provides simple 'How Do I' steps for configuring Network (Client) Access. An 'Important Concepts' section follows, listing three key concepts: 1. SSL tunnel and IPsec tunnel, 2. User and connection profile, and 3. Access policy. Each concept is accompanied by a brief description and links to related configuration pages. A large watermark for 'VCEplus VCE To PDF - Free Practice Exam' is overlaid on the bottom right of the screenshot.

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

What is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKv2) protocols, Cisco VPN Client supports only IPsec(DKv1) protocol.

2. User and connection profile

To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user account database in [AAA,Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKv1\) Connection Profiles](#).

3. Access policy

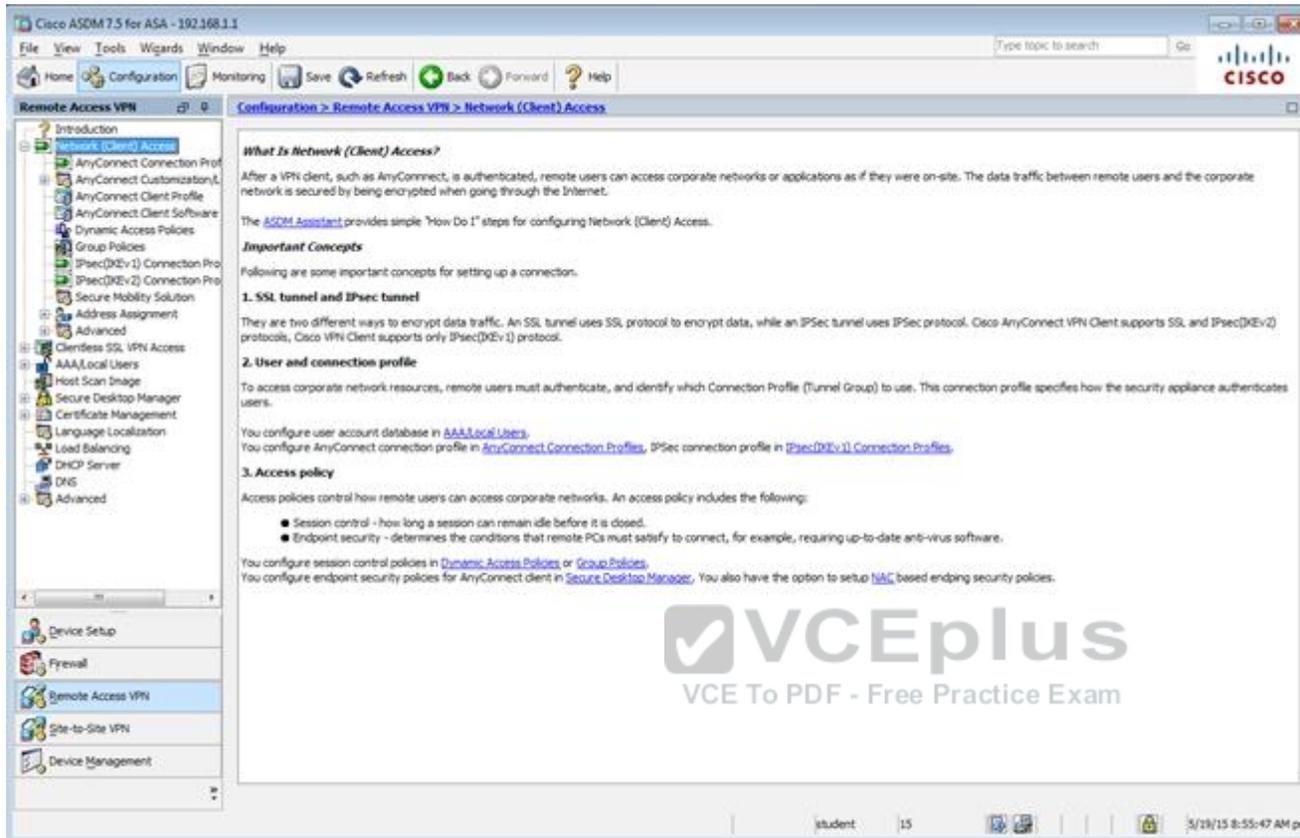
Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HAC](#) based endpoint security policies.

Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

student | 15 | 5/19/15 8:55:47 AM pst



The screenshot shows the Cisco ASDM 7.5 interface for configuration. The main content area is titled "Configuration > Remote Access VPN > Network (Client) Access".

What is Network (Client) Access?

After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Network (Client) Access.

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKEv2) protocols, Cisco VPN Client supports only IPsec(DKEv1) protocol.

2. User and connection profile

To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user account database in [AAA Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKEv1\) Connection Profiles](#).

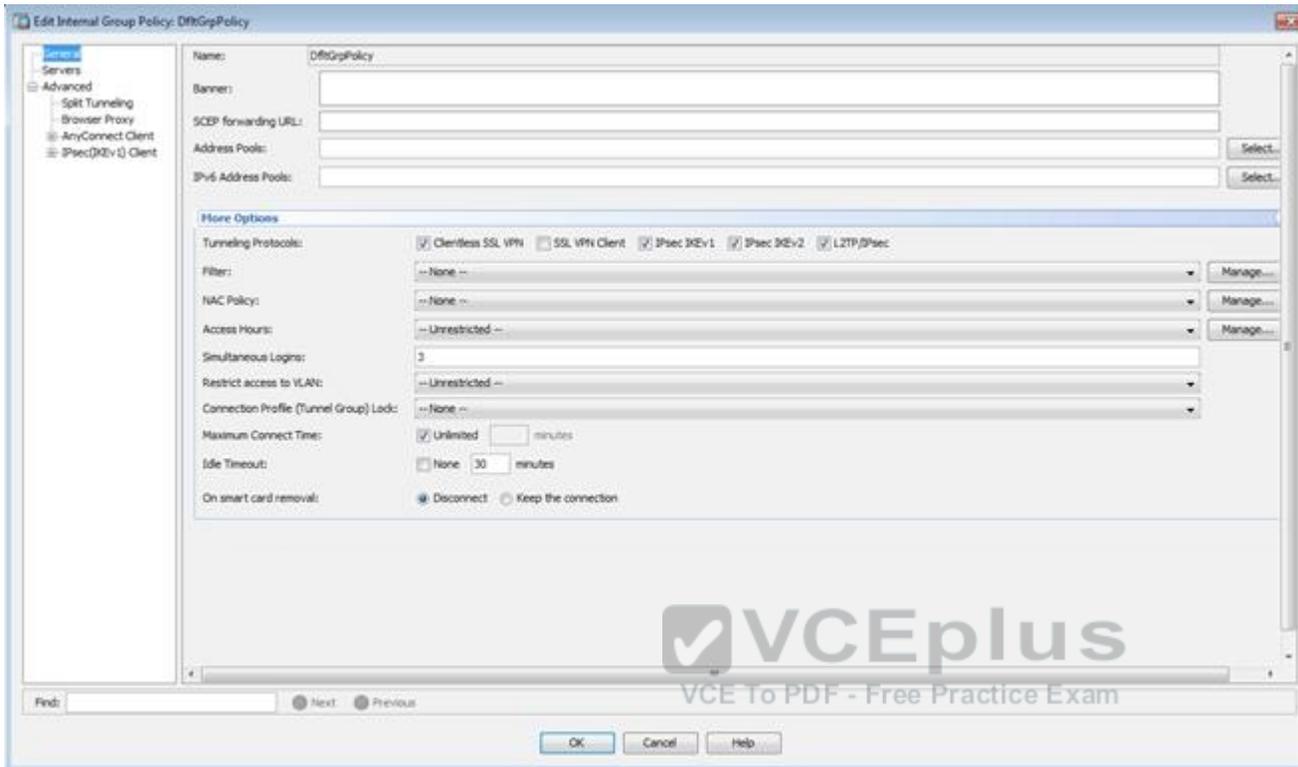
3. Access policy

Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [HAC](#) based endpoint security policies.

The interface also features a left-hand navigation pane with categories like "Remote Access VPN", "Device Setup", "Firewall", "Site-to-Site VPN", and "Device Management". A bottom status bar shows "student | 15 | 5/19/15 8:55:47 AM pst".



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The main content area is titled "Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles".

Access Interfaces
Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input type="checkbox"/>
dmsr	<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.

Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultSRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DfltGrpPolicy
DefaultIISVPhGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RAD	DfltGrpPolicy
Certless	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL	Sales

Search: Find: [] Match Case

Buttons: Apply, Reset

Footer: student 15 5/19/15 8:56:47 AM pst

The screenshot shows the Cisco ASDM 7.5 interface for configuring AnyConnect Connection Profiles. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area is titled 'Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles'.

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 Client Services
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 can configure the mapping from certificate to connection profile [here](#).

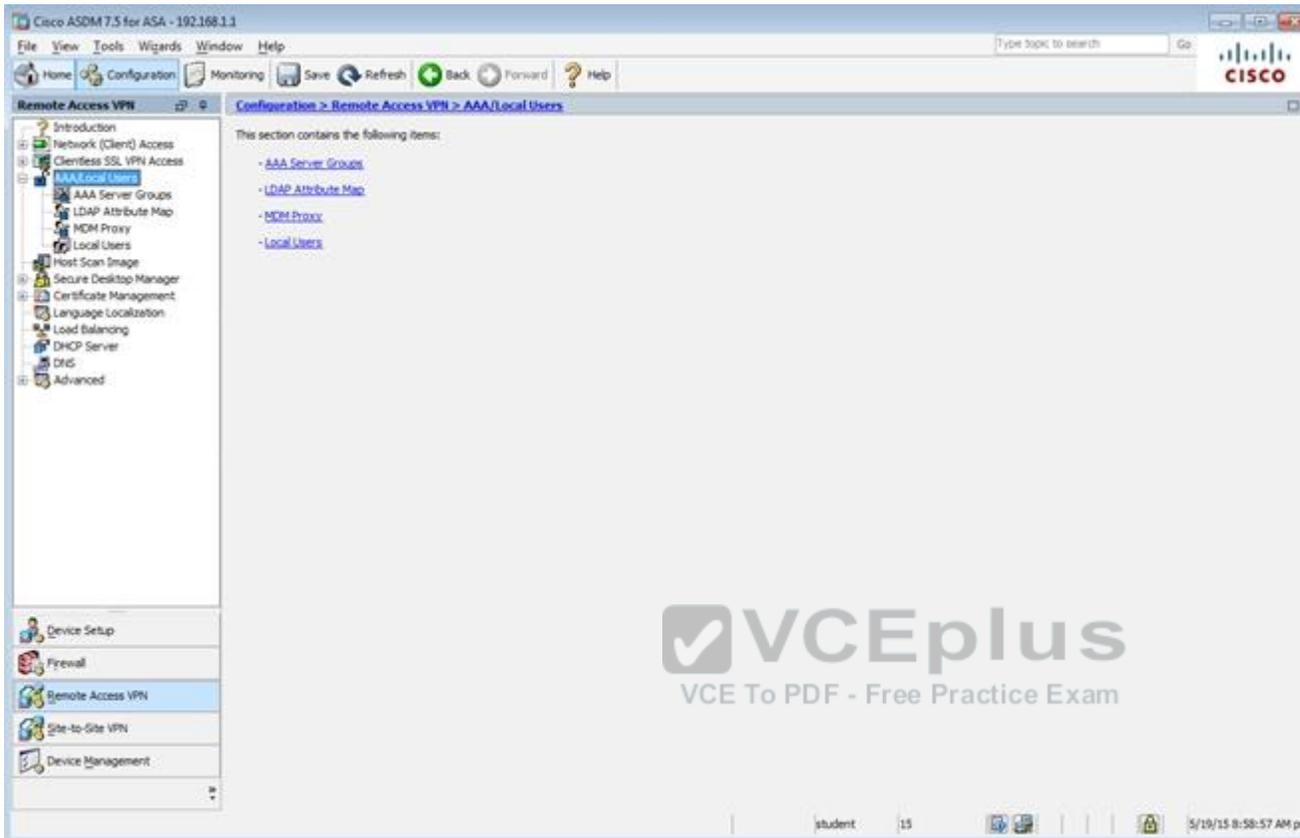
Buttons: Add, Edit, Delete, End: [input type="text"], Match Case

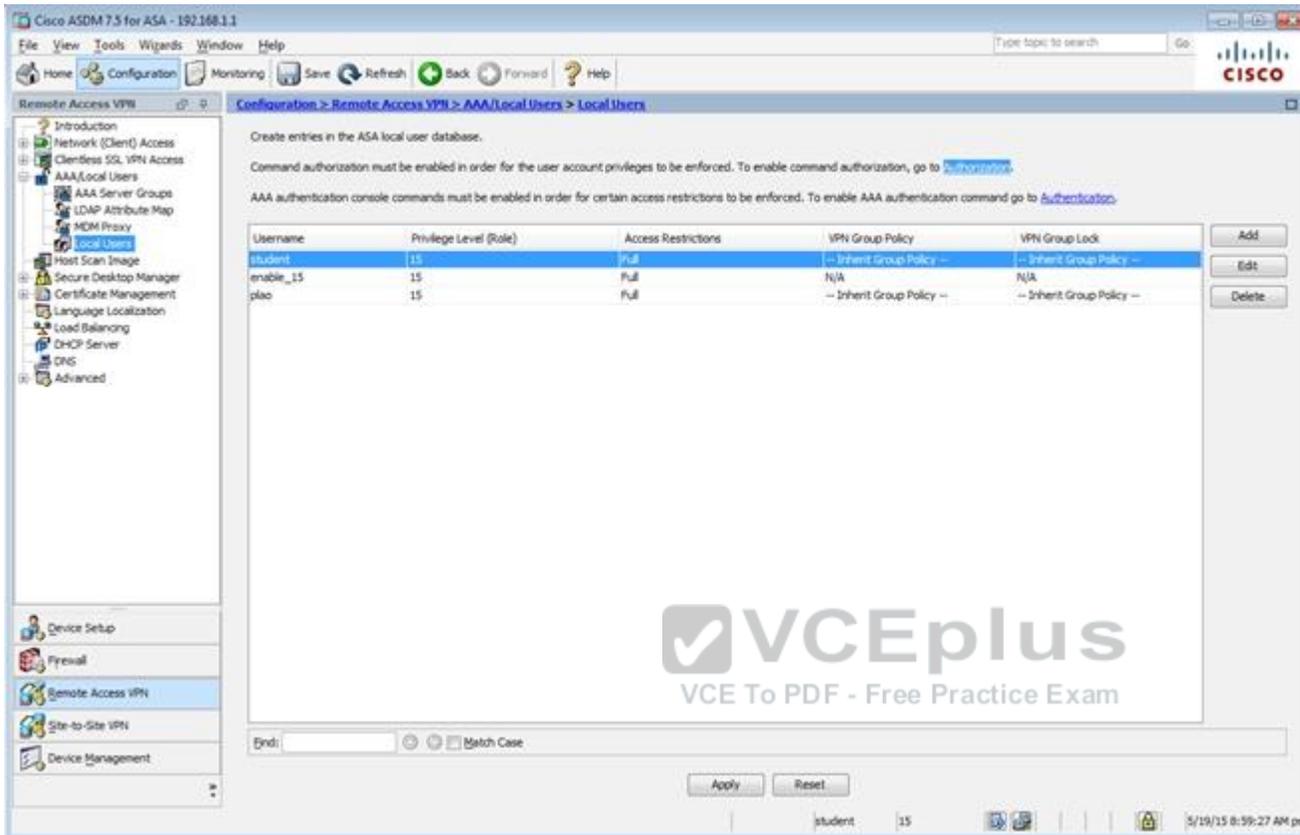
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultVPIVpnGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
Certificates	<input type="checkbox"/>	<input type="checkbox"/>	yes	AAA(OCSP)	Global

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Buttons: Apply, Reset

Footer: student | 15 | 5/19/15 8:58:17 AM pet





Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

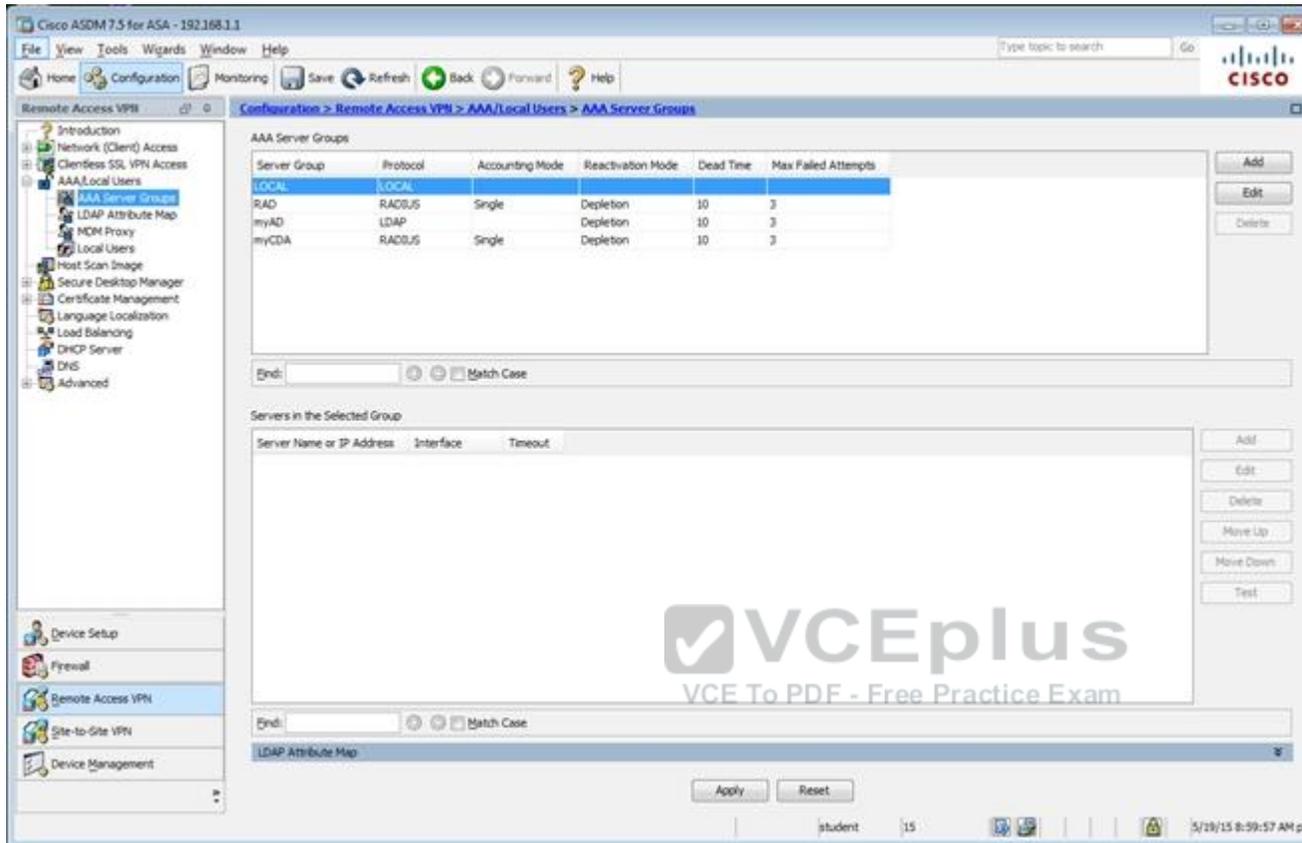
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Add
enable_15	15	Full	N/A	N/A	Edit
plac	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --	Delete

End: Match Case

Apply Reset

student 15 5/19/15 8:59:27 AM pet



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 configuration page. The breadcrumb trail is Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups. The main content area displays a table of 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

Below the table, there is a search field labeled "Find:" with a "Match Case" checkbox. Underneath, there is a section for "Servers in the Selected Group" with a table header: "Server Name or IP Address", "Interface", and "Timeout". To the right of this section are buttons for "Add", "Edit", "Delete", "Move Up", "Move Down", and "Test". At the bottom of the configuration page, there are "Apply" and "Reset" buttons. The status bar at the bottom shows "student | 15" and the date/time "5/28/15 8:59:57 AM pst".

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

Section: (none)

Explanation

Explanation/Reference:

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 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
- Unified Communications
- Advanced

Match Criteria

#	Source Int
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 Addr: 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 range 1-1023

Fall through to interface PAT(dst intf): DMZ

Use IPv6 for interface PAT

Scenario TOPOLOGY

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

- 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

Configural

+ Add

#	
dmz (1 in	
1	
inside (1 in	
1	
outside (1	
1	
Global (1 in	
1	

Add Access Rule

Interface:

Action: Permit Deny

Source Criteria

Source:

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

Description:

Enable Logging

Logging Level:

More Options

OK Cancel Help

Scenario TOPOLOGY

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

- 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 Edit Delete Where Used Not Used

Diagram Export Clear Hits Show Log Packet Tr

Source Criteria:							Destination Criteria:		
#	Enabled	Source	User	Security Gi	Destination	Security Gi	Service	Action	
dmz (1) implicitly incomm									
1		any			Any less secure ne..		ip	Permit	
inside (1) implicit incomm									
1		any			Any less secure ne..		ip	Permit	
outside (1) incoming rule	<input checked="" type="checkbox"/>								
1		any			209.165.201.30		tcp/http	Permit	
Global (1) implicit rule									
1		any			any		ip	Deny	

Apply Reset Advanced

Scenario TOPOLOGY

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

Traffic Classification

Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group
[-] Interface: dmz; Policy: asacx_policy							
class-default			<input checked="" type="checkbox"/> Match	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	
[-] Interface: inside; Policy: asacx_policy							
class-default			<input checked="" type="checkbox"/> Match	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	
[-] Global; Policy: global_policy							
inspection_de...			<input checked="" type="checkbox"/> Match	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	

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

- 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

Edit Service Policy Rule

Traffic Classification Default Inspections Rule Actions

Protocol Inspection ASA FirePOWER Inspection Connection Settings QoS NetFlow User Statistics

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"/> ESMTTP	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"/> MMP	Configure...

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



Inside PC



cmd.exe

```
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,  Lost =  
(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: with 3  
bytes of data: VCE To PDF - Free Practice Exam  
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52  
Ping statistics for 23.72.192.170:    Packets: Sent = 4,  Recieved = 4,  Lost =  
(0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 4ms, Maximum = 5s, Average = 4ms  
  
C:\
```

