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.dis
C. It supports a more complex encryption algorithm than other disk-encryption technologies.
D. It can protect against single points of failure.

Correct Answer: A
Section: (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 dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx 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

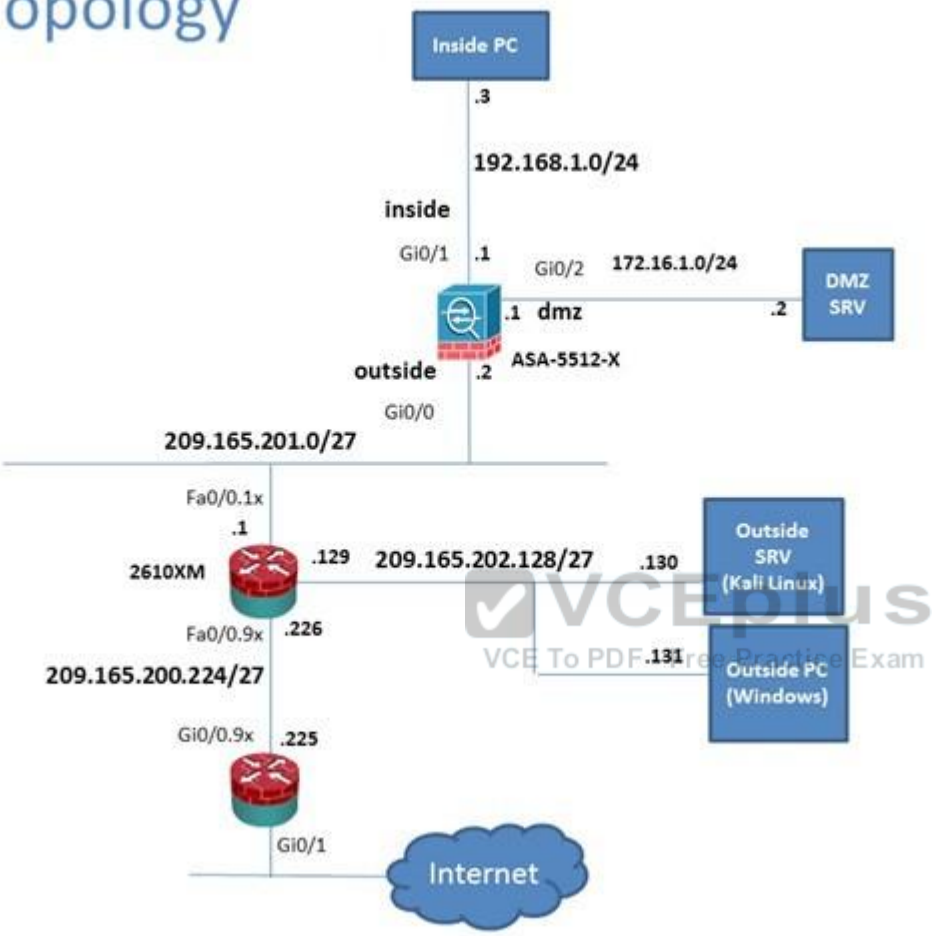
Explanation/Reference:

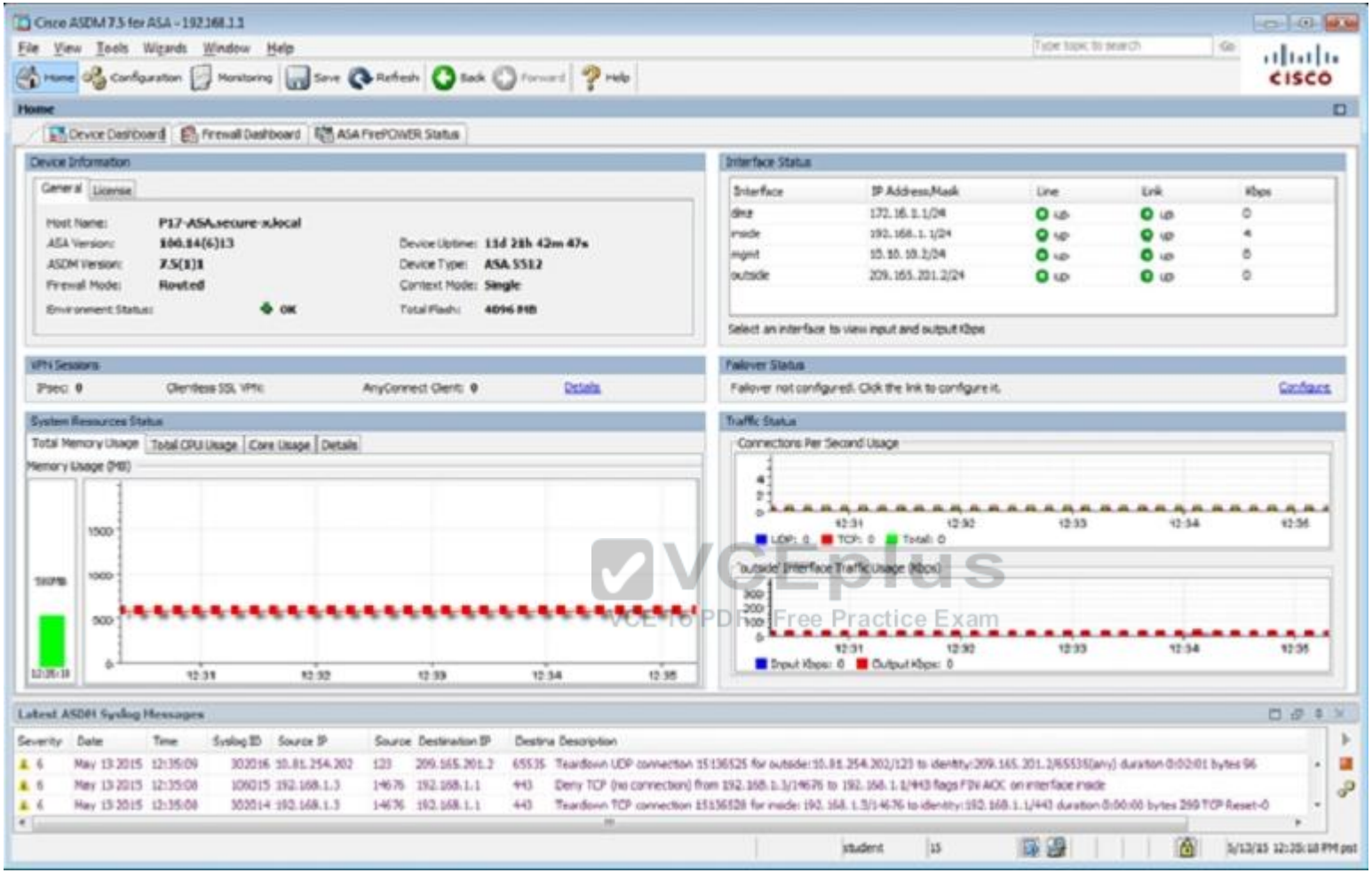
QUESTION 64
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

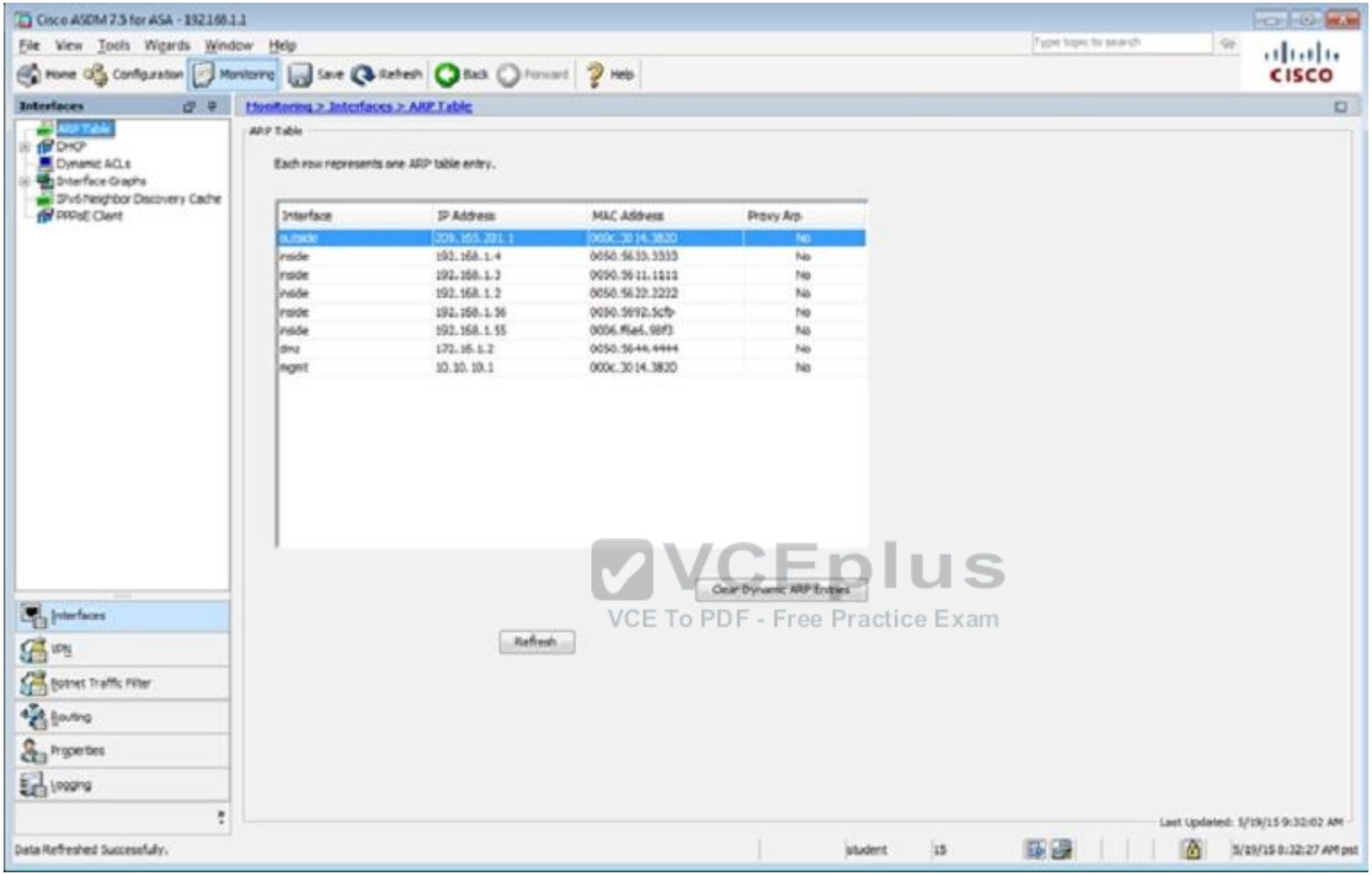
To access ASDM, click the ASA icon in the topology diagram.

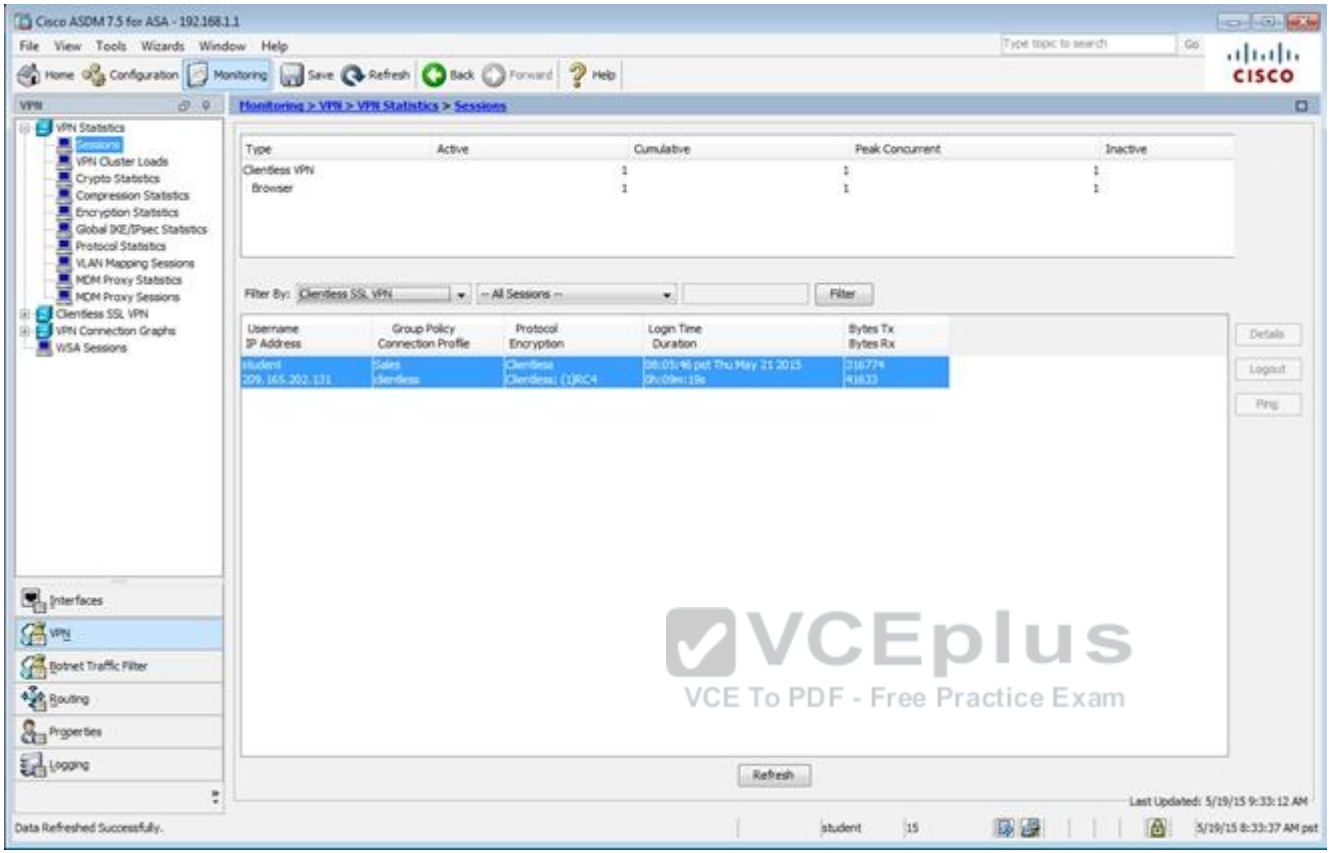
Note: Not all ASDM functionalities are enabled in this simulation. To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

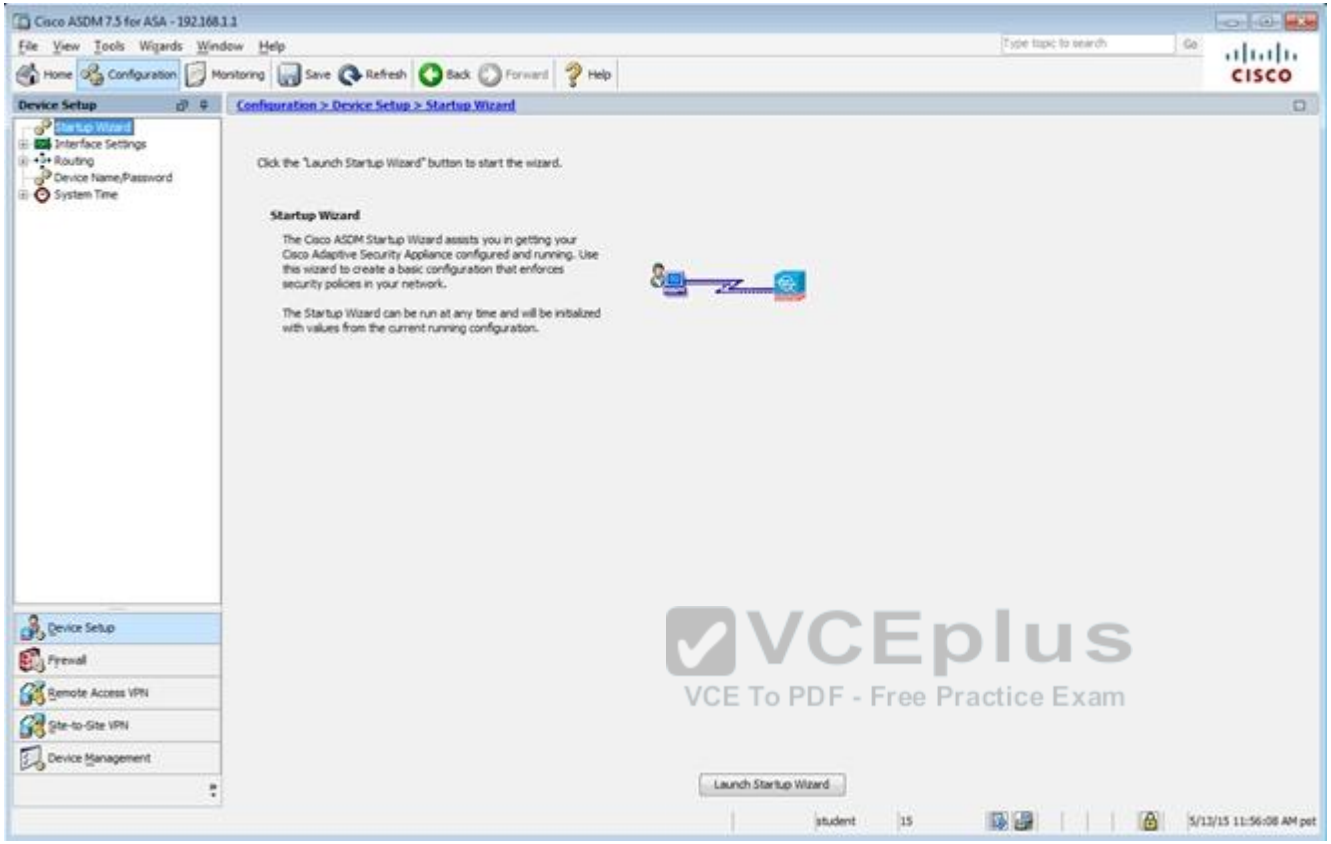
Lab Topology

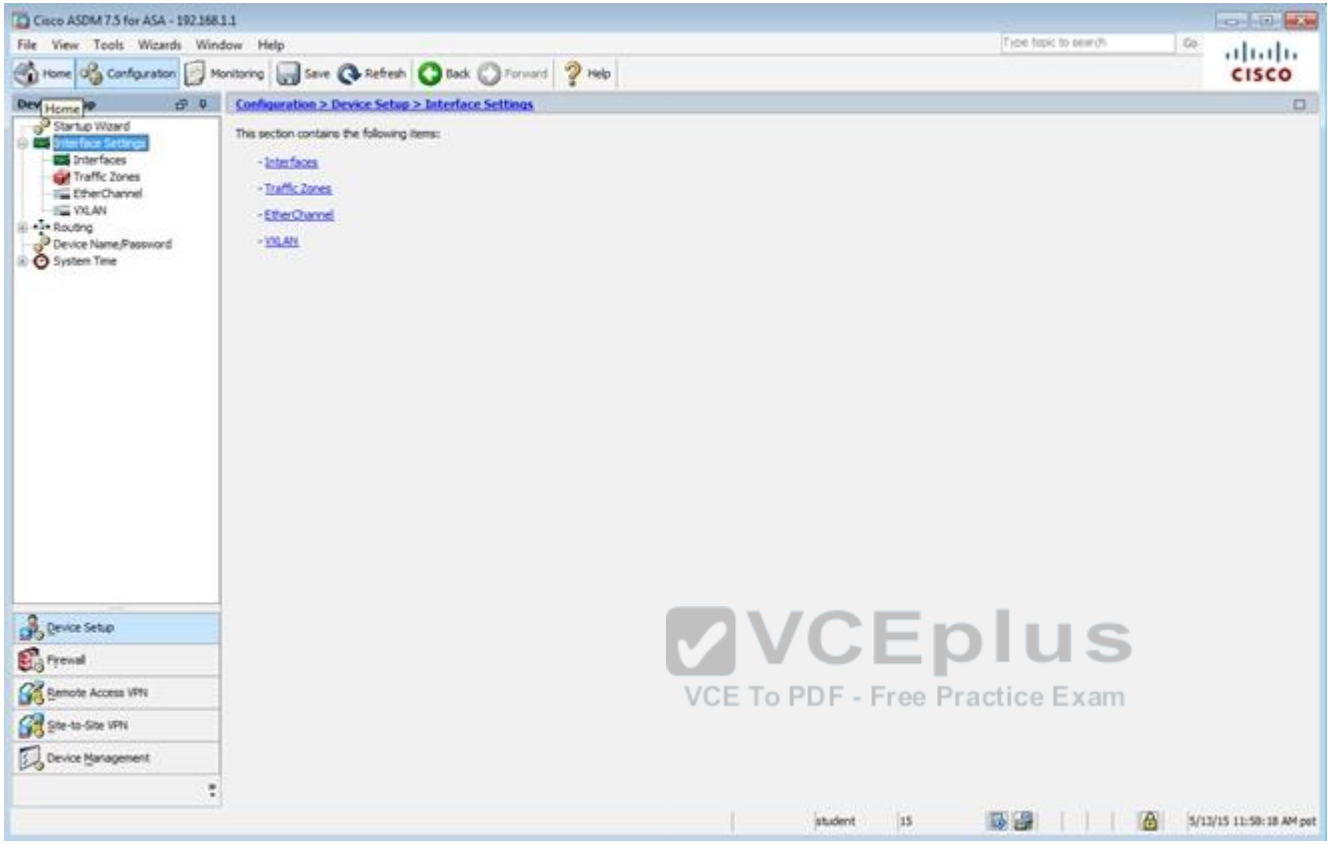


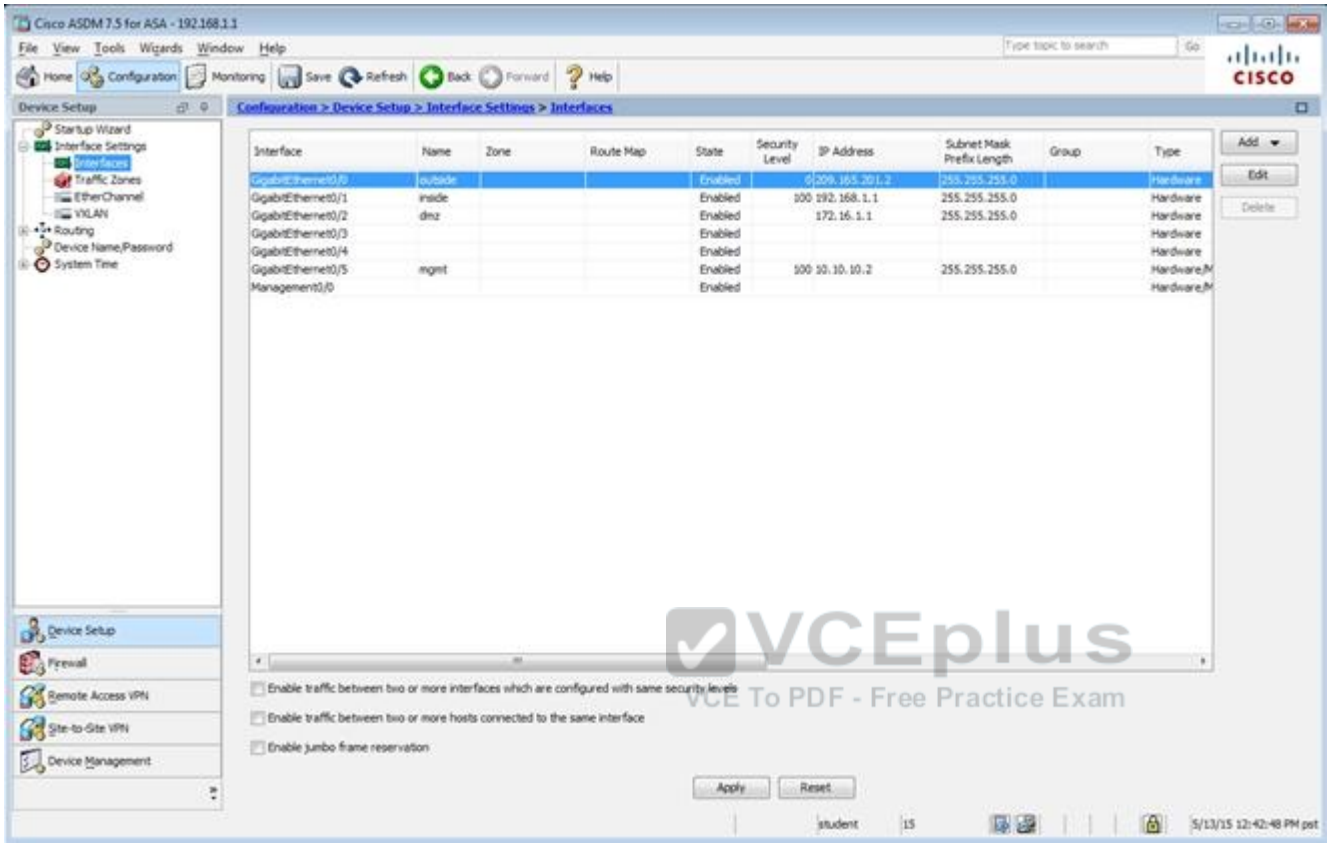


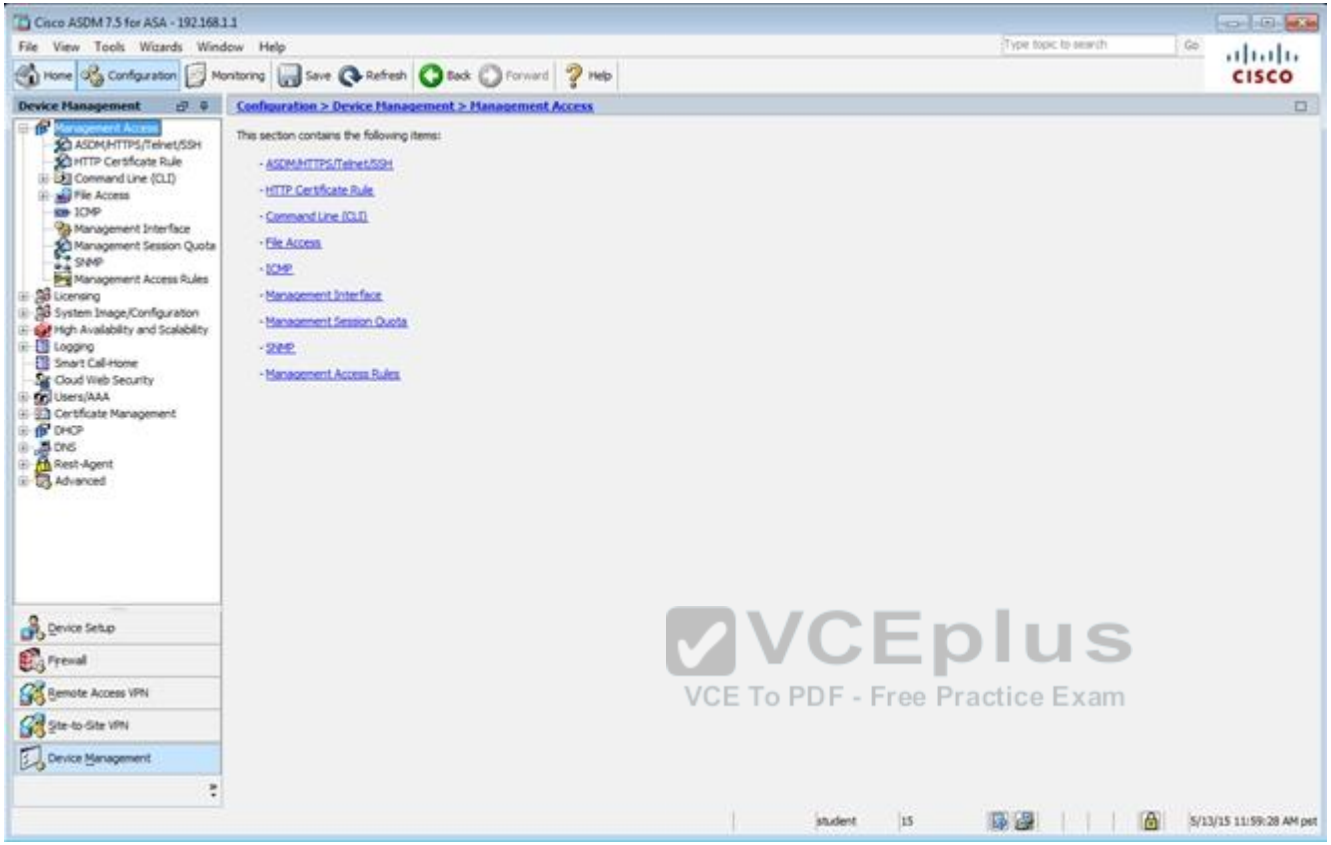


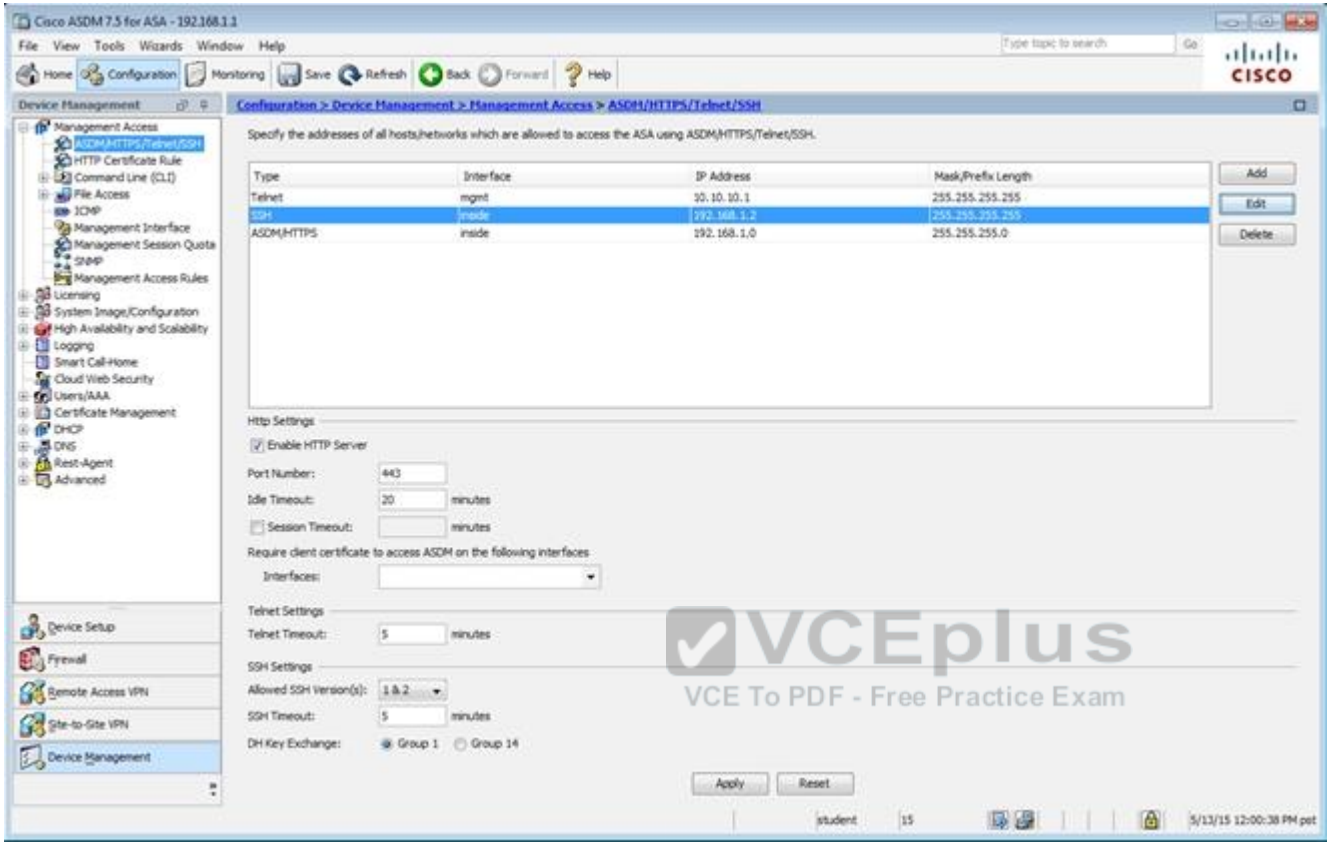


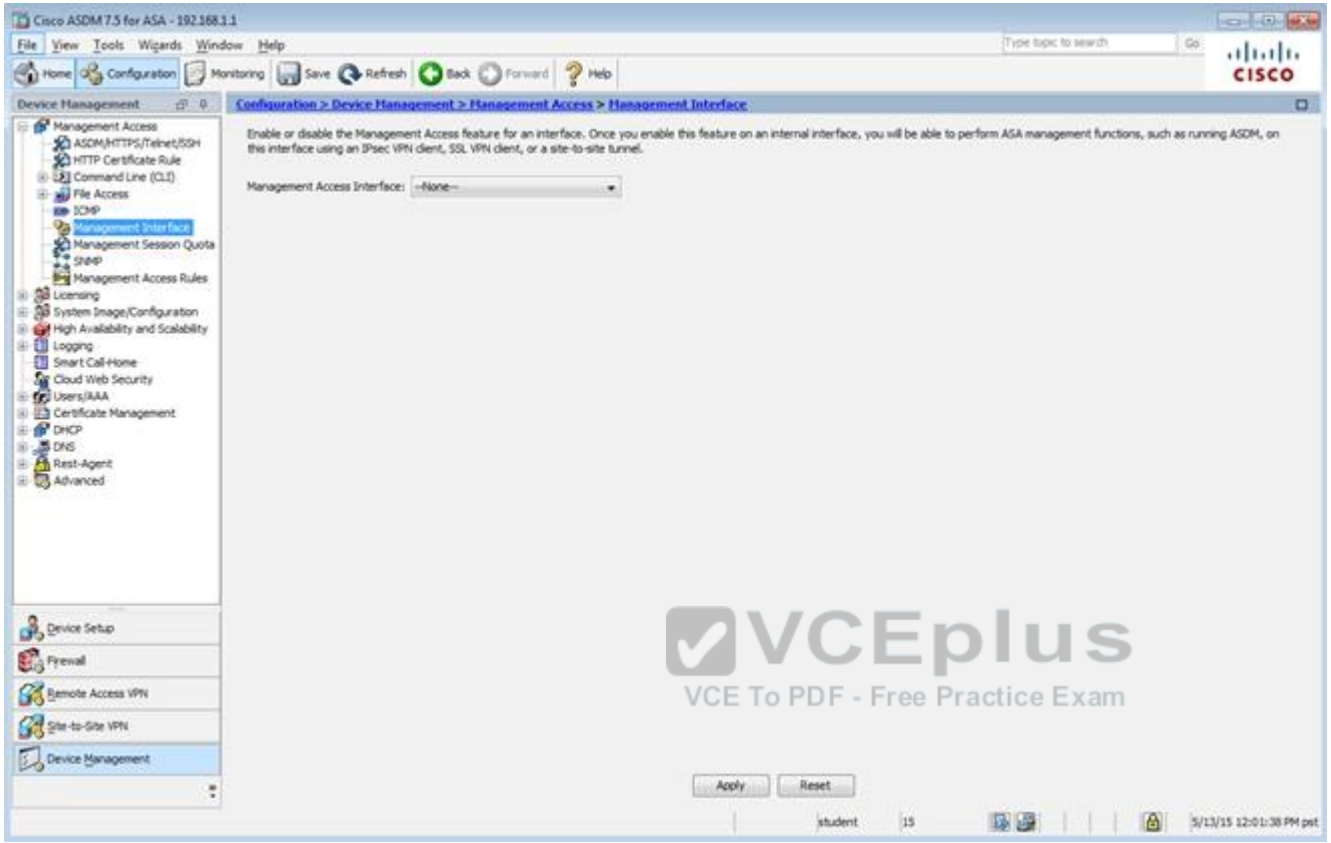


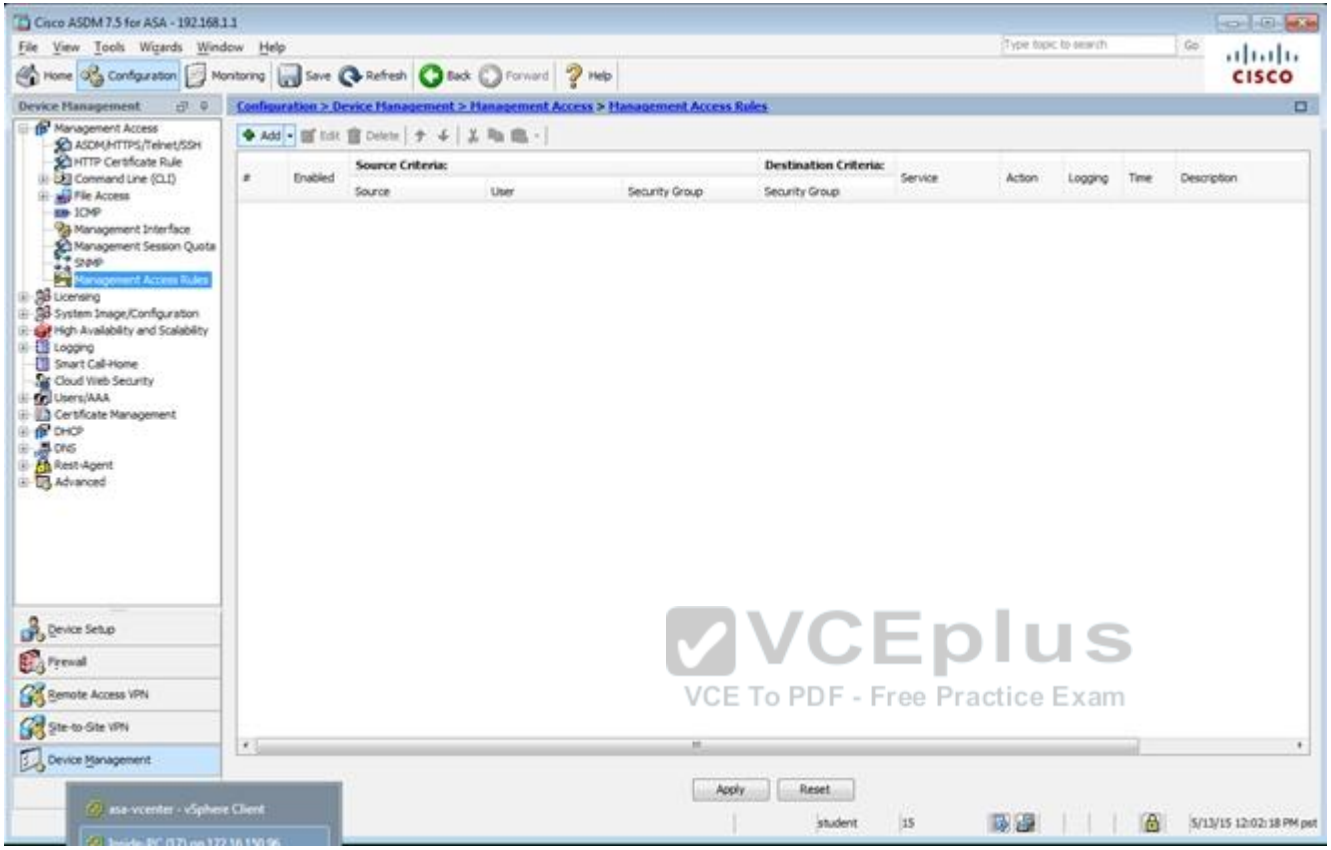


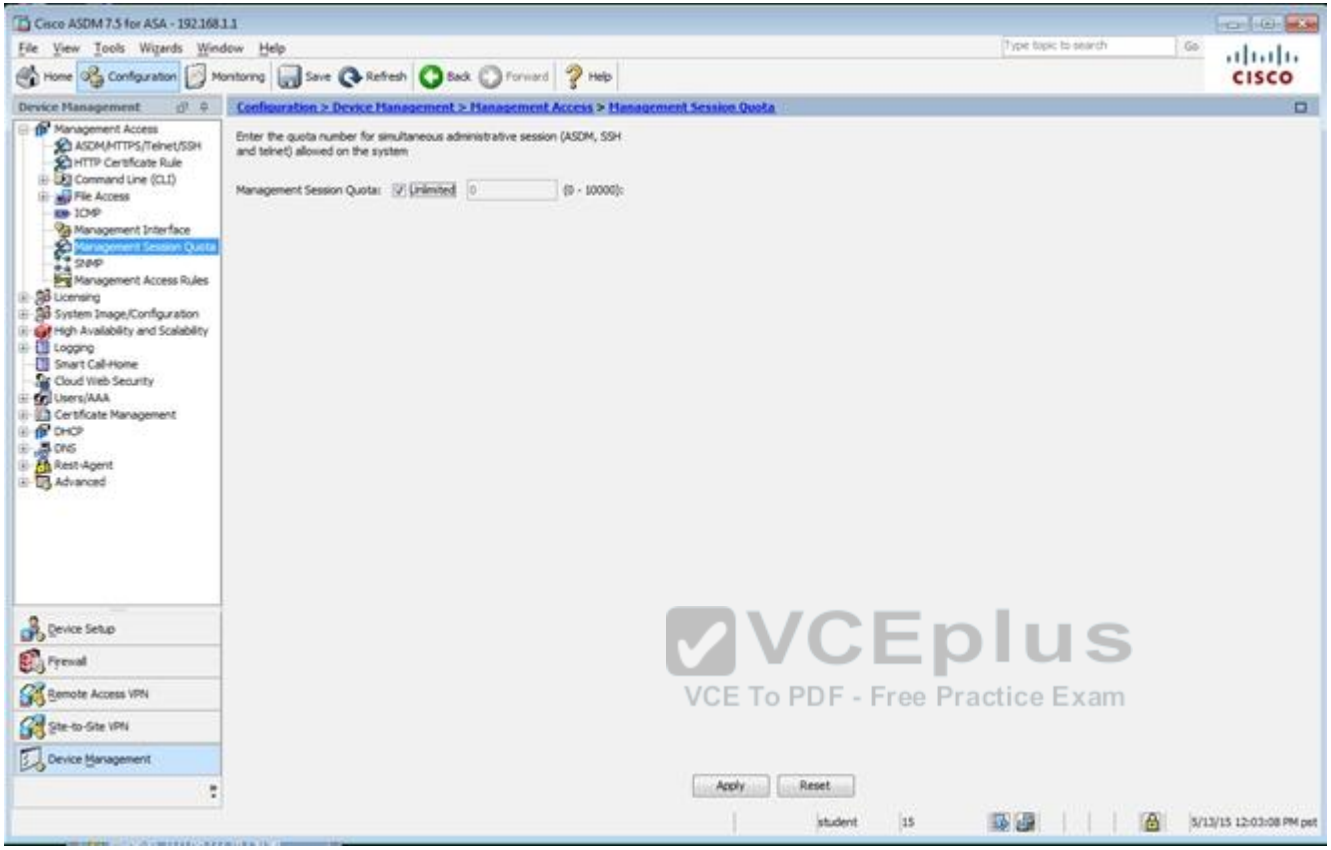


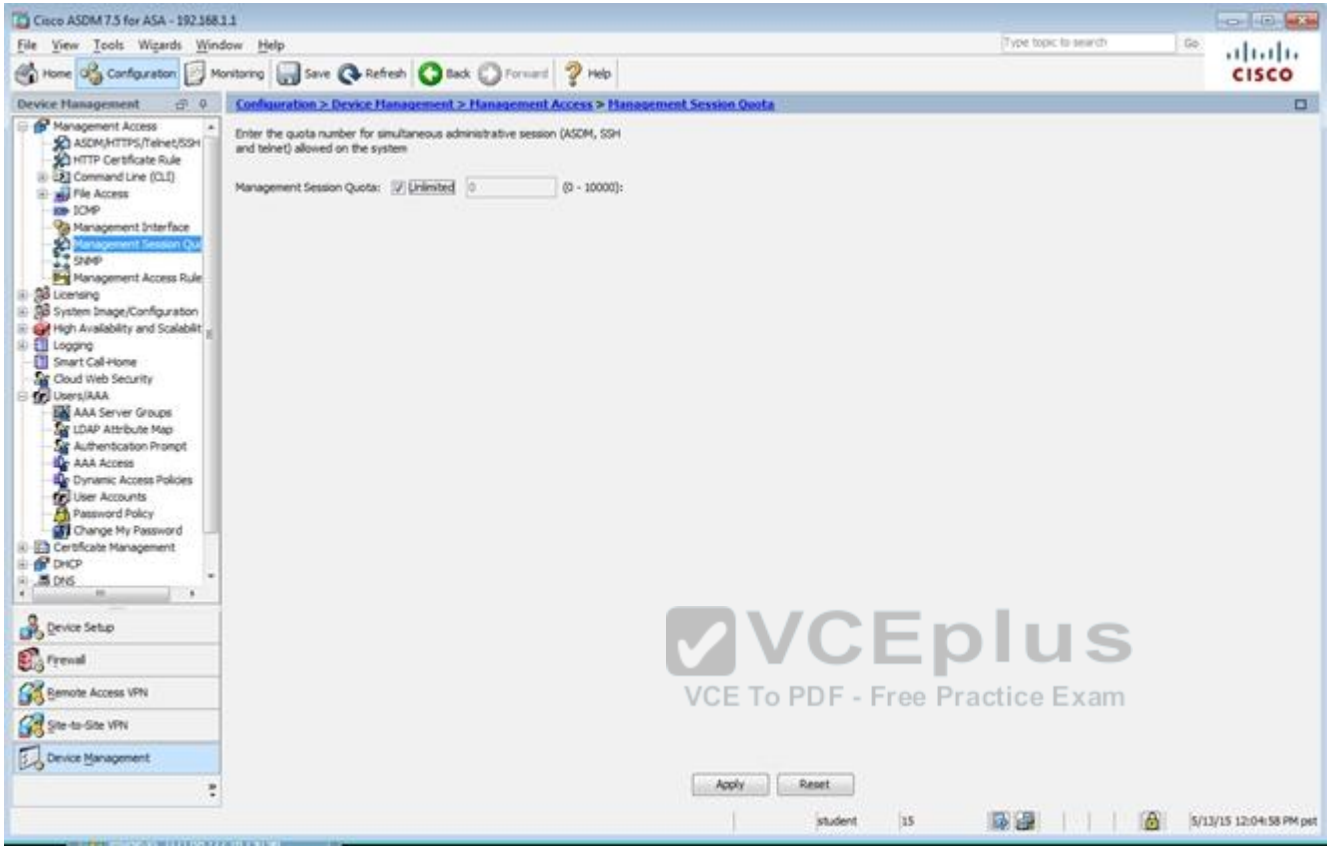


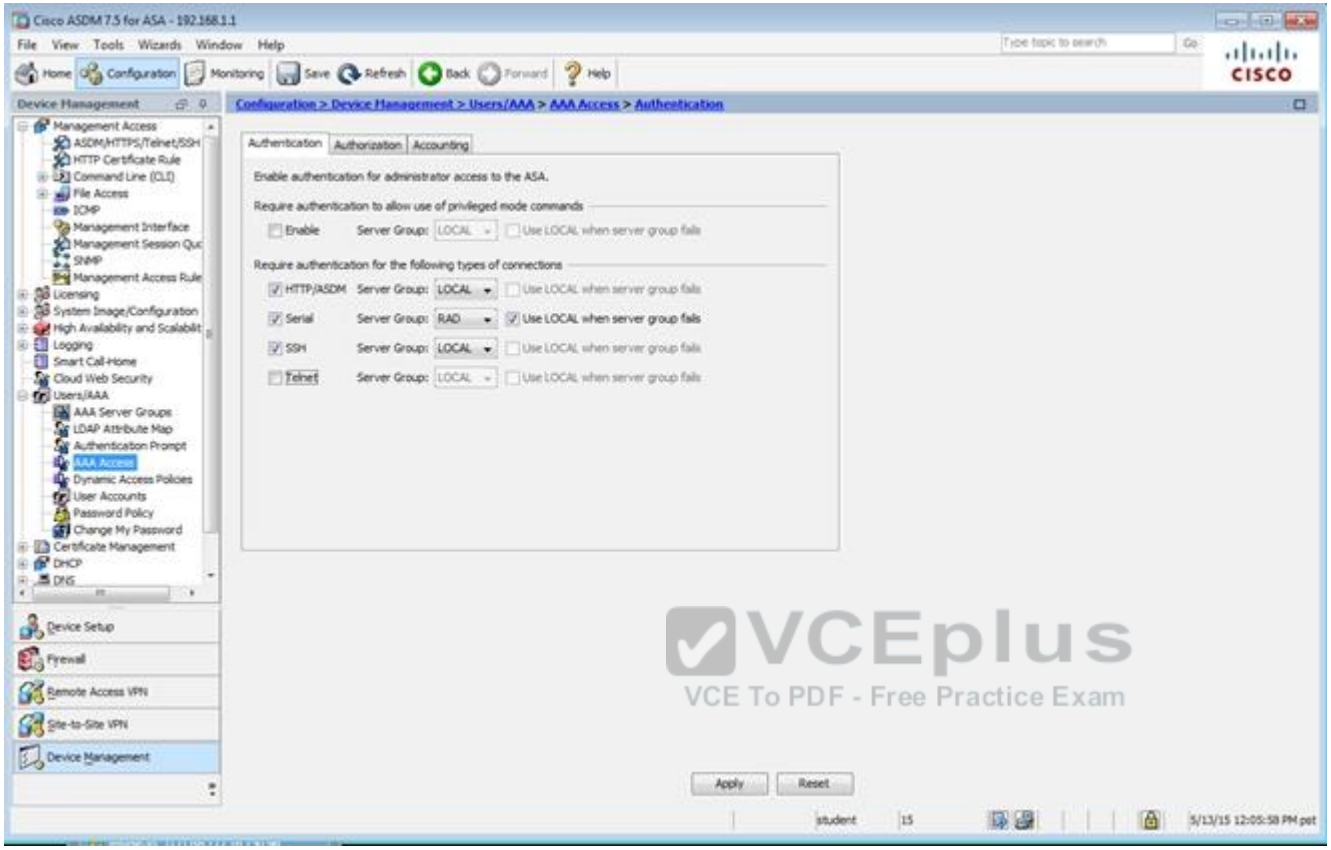


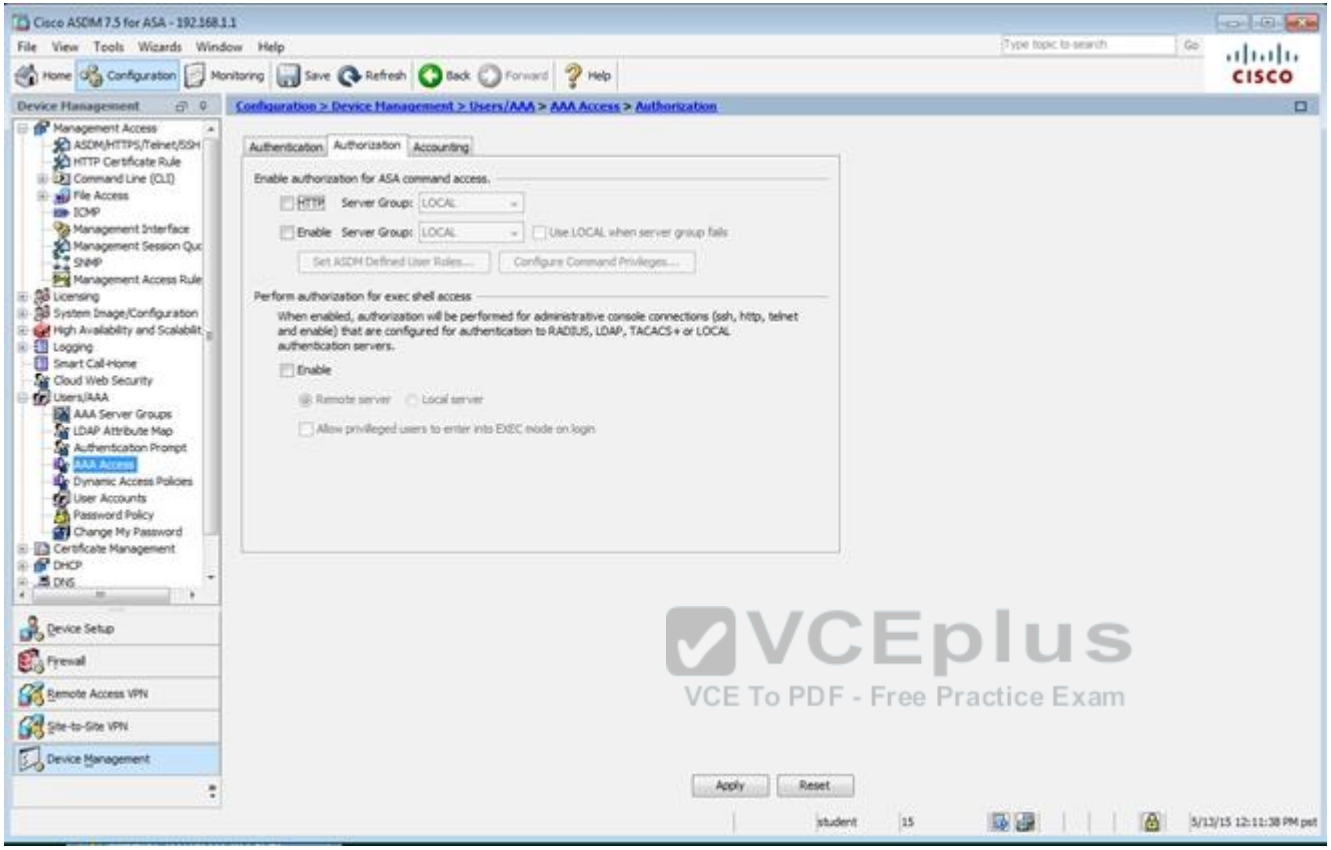


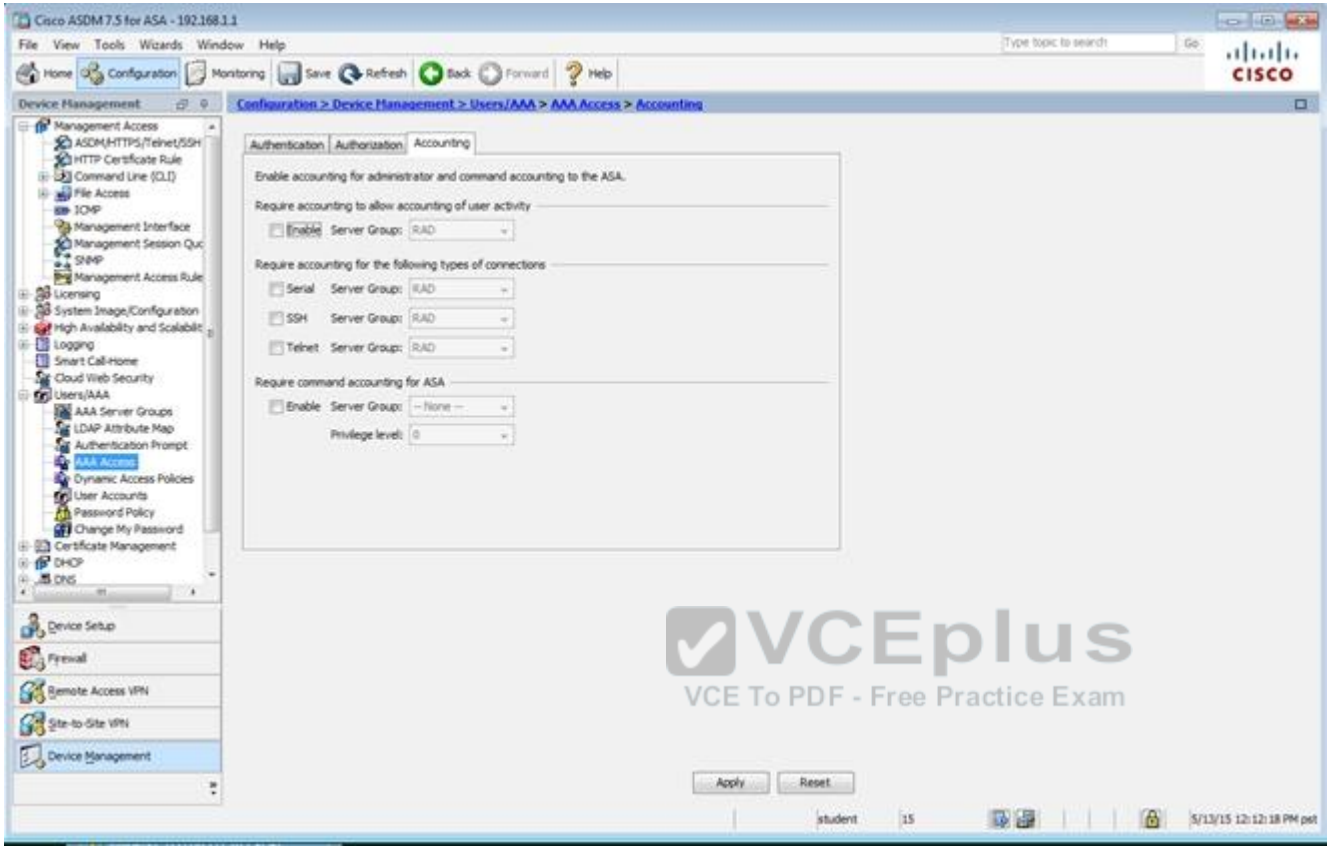


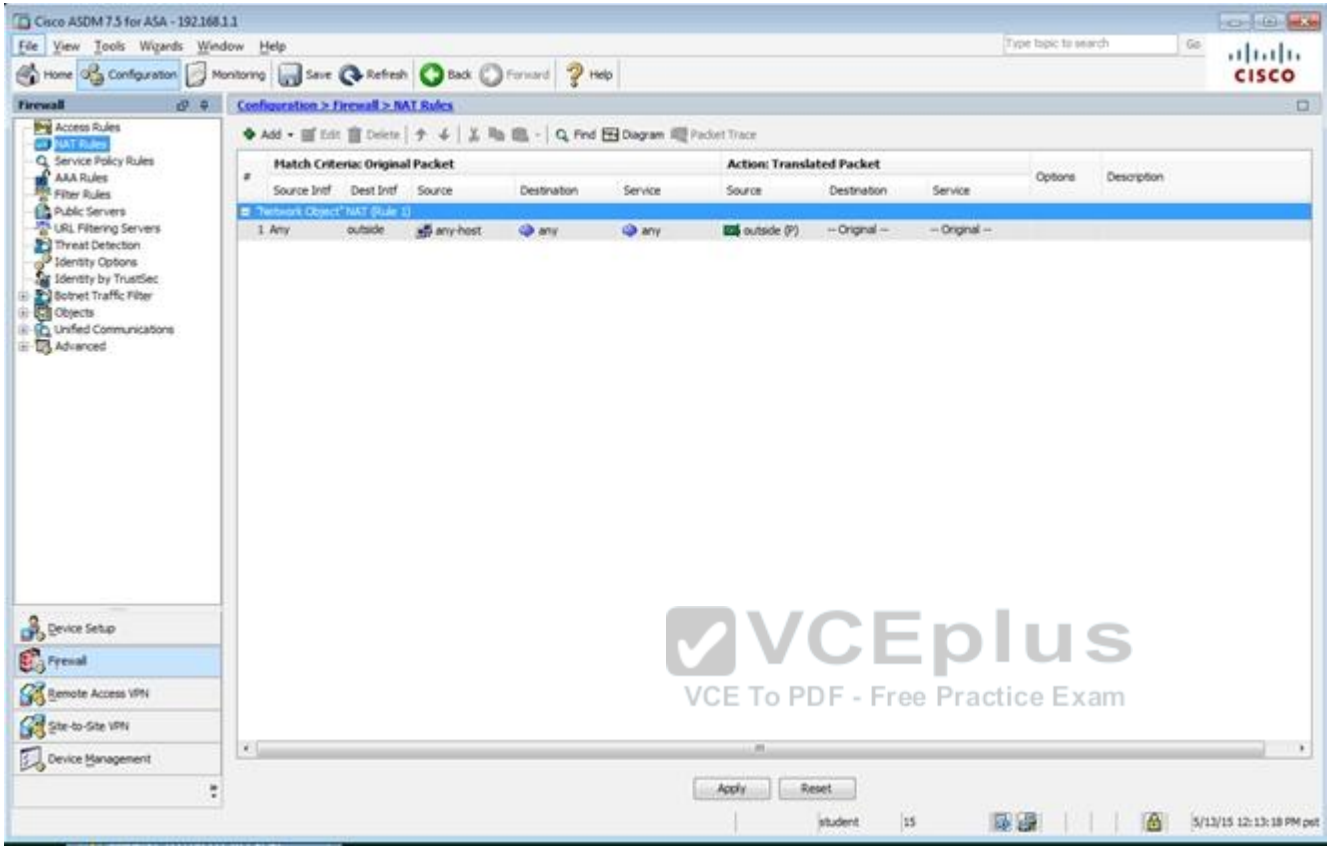


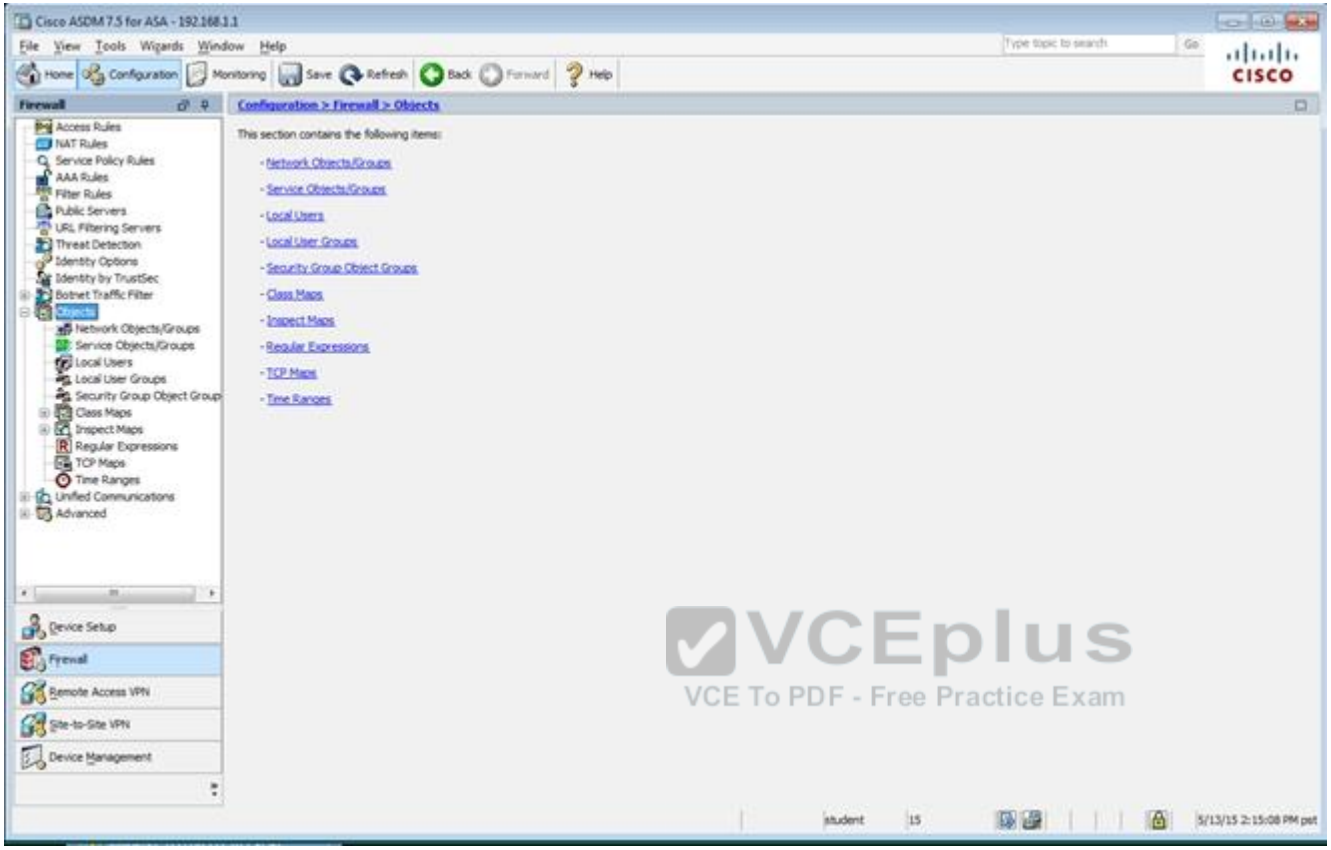


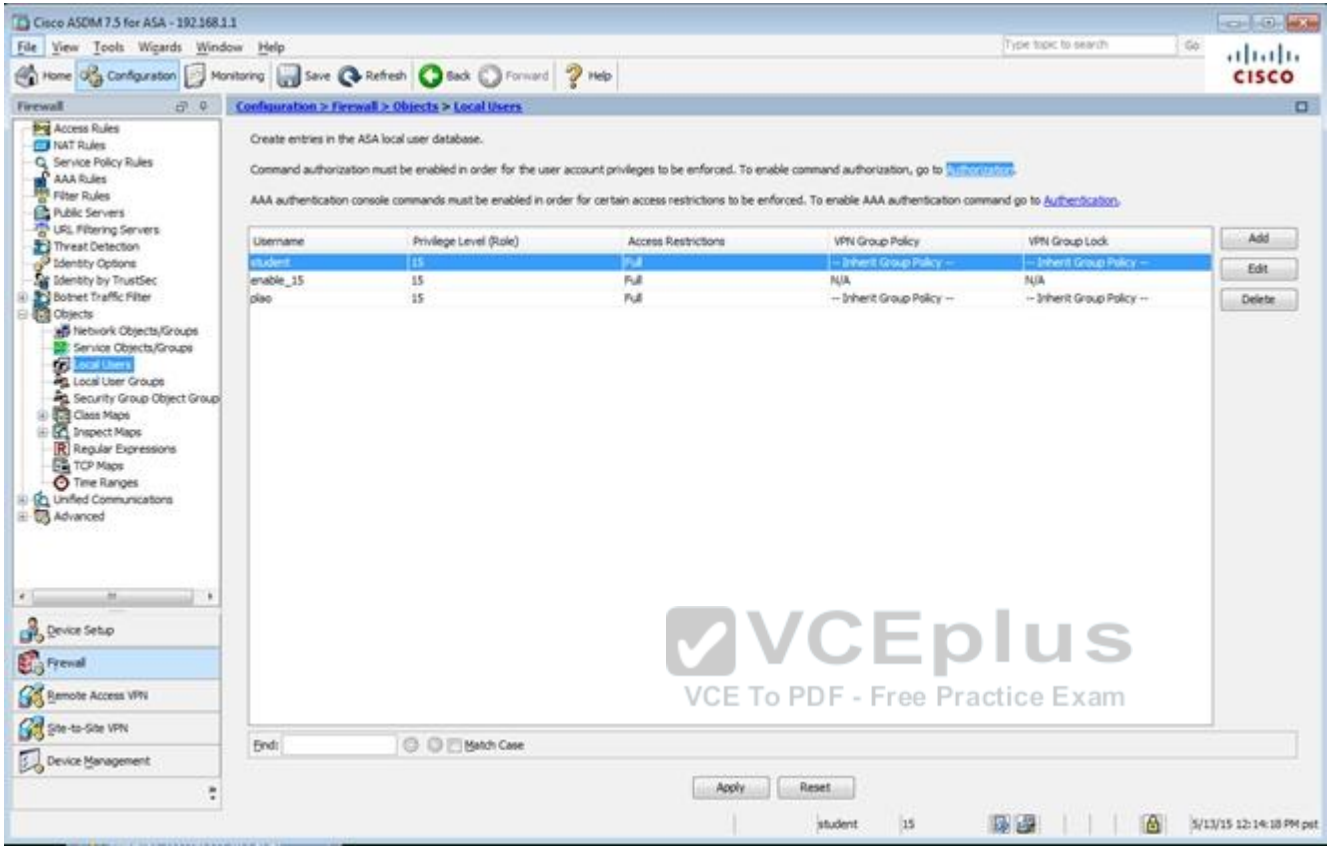


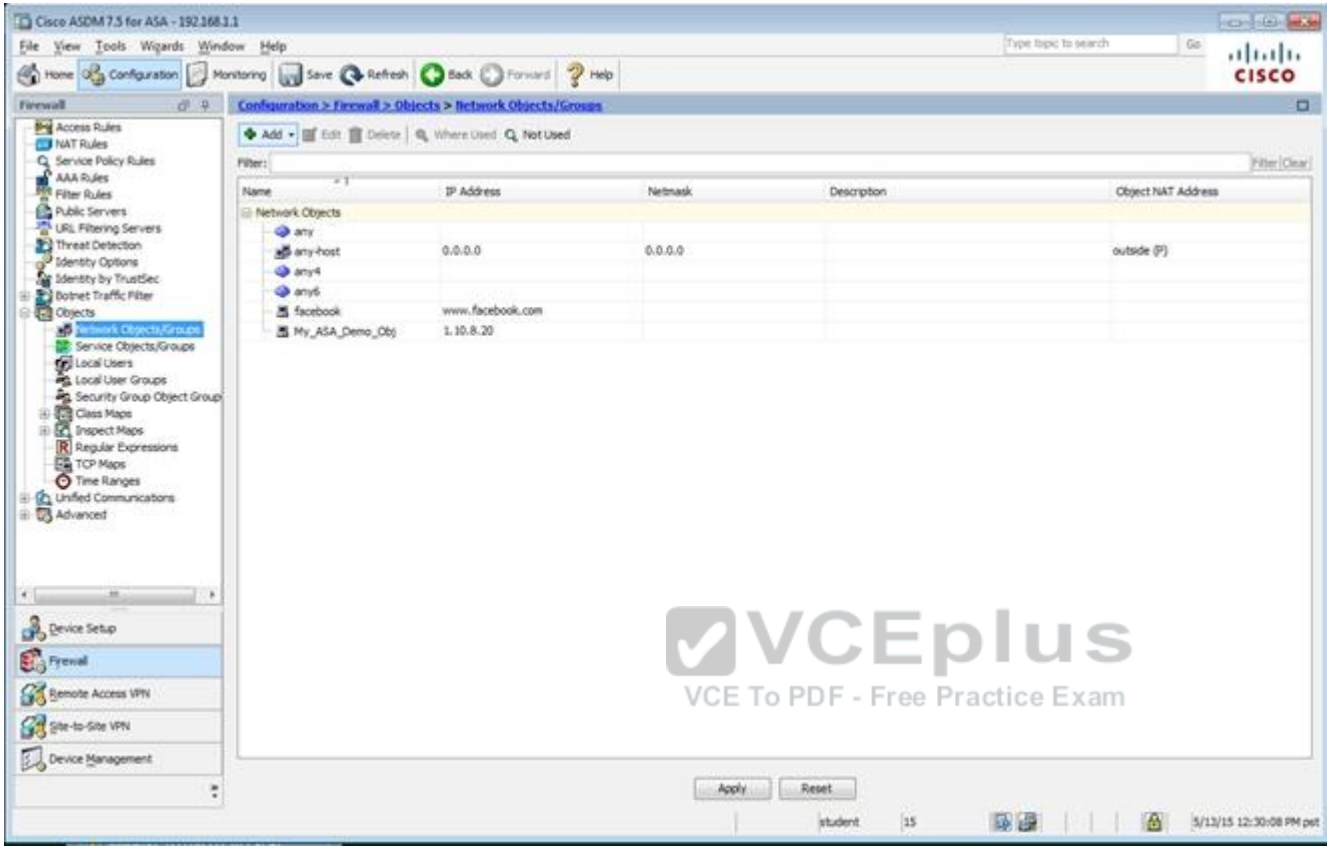


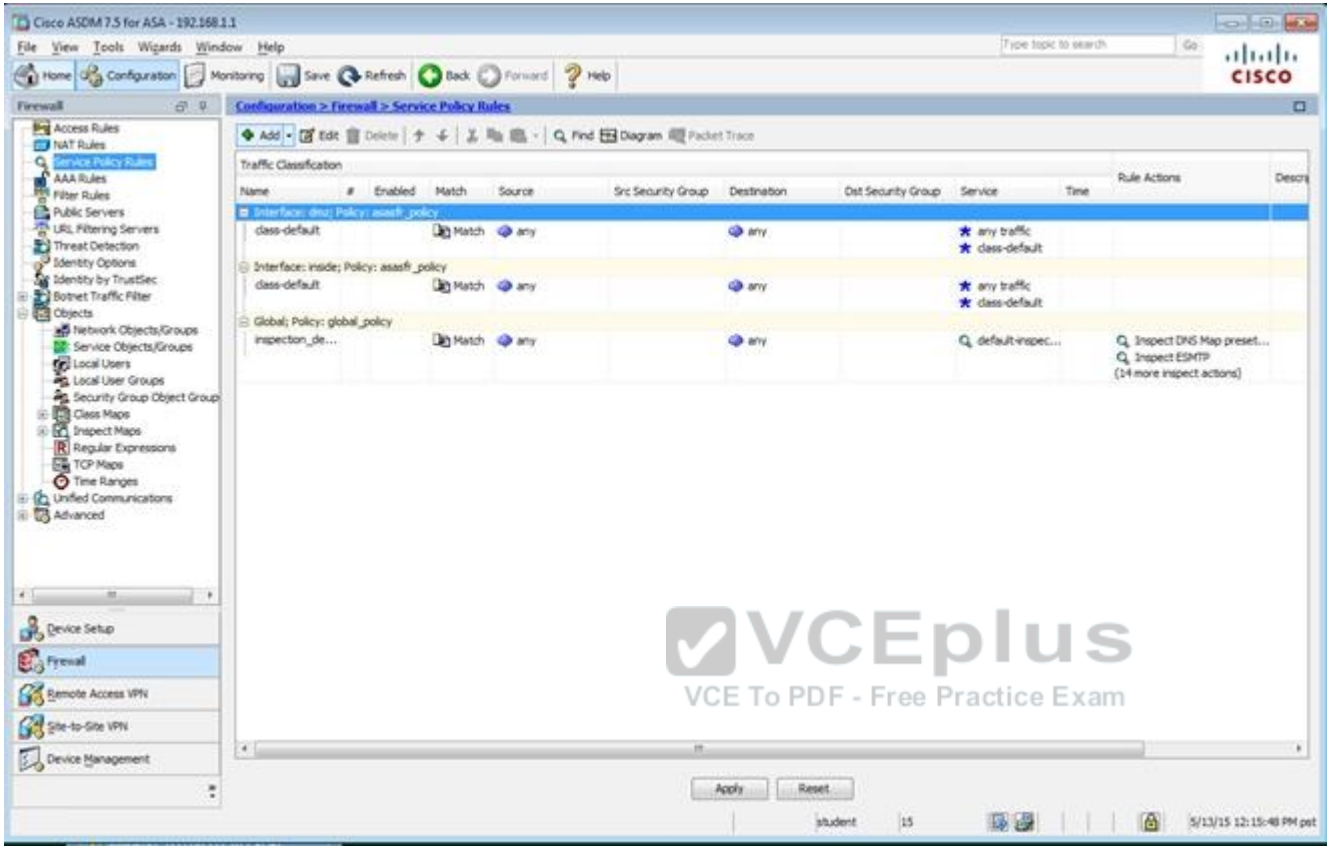


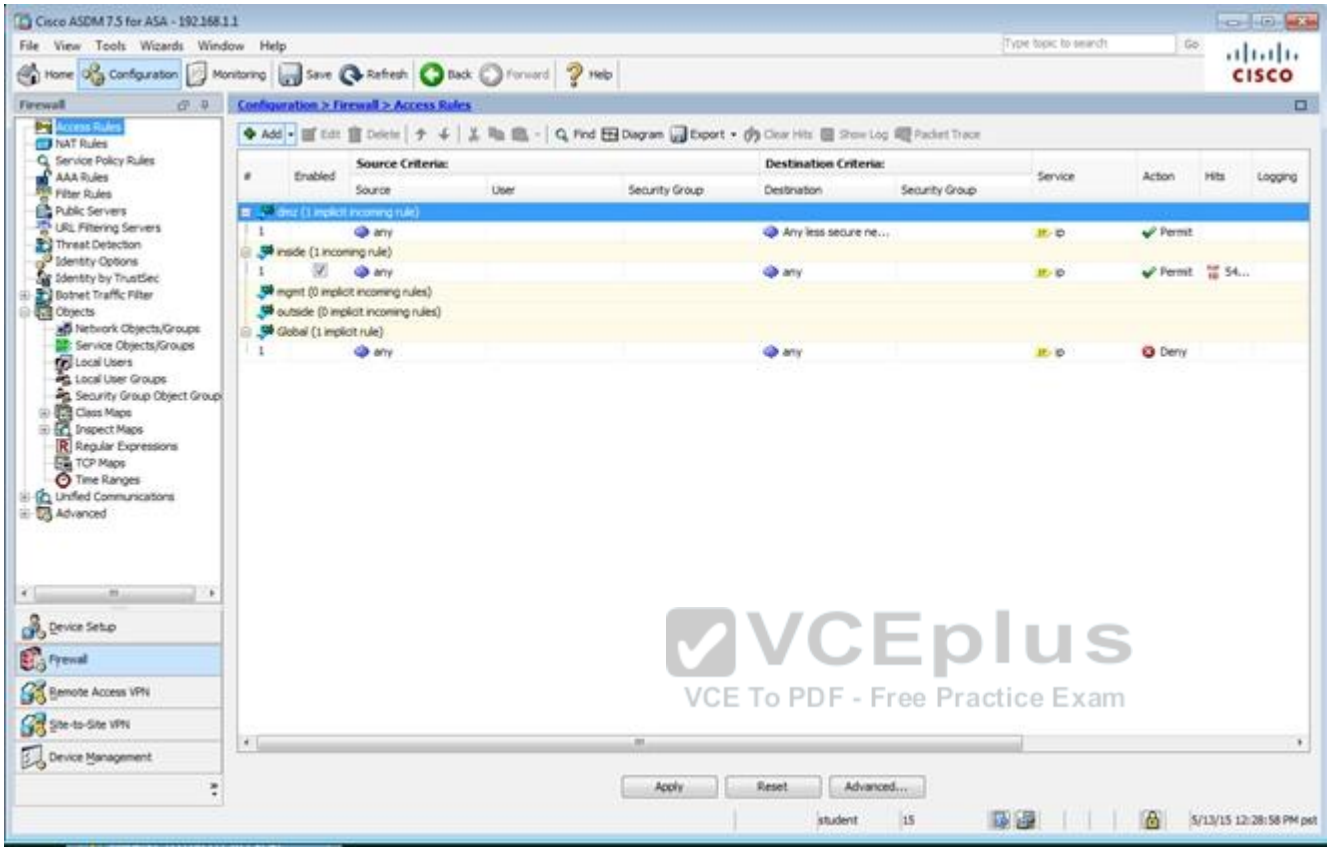


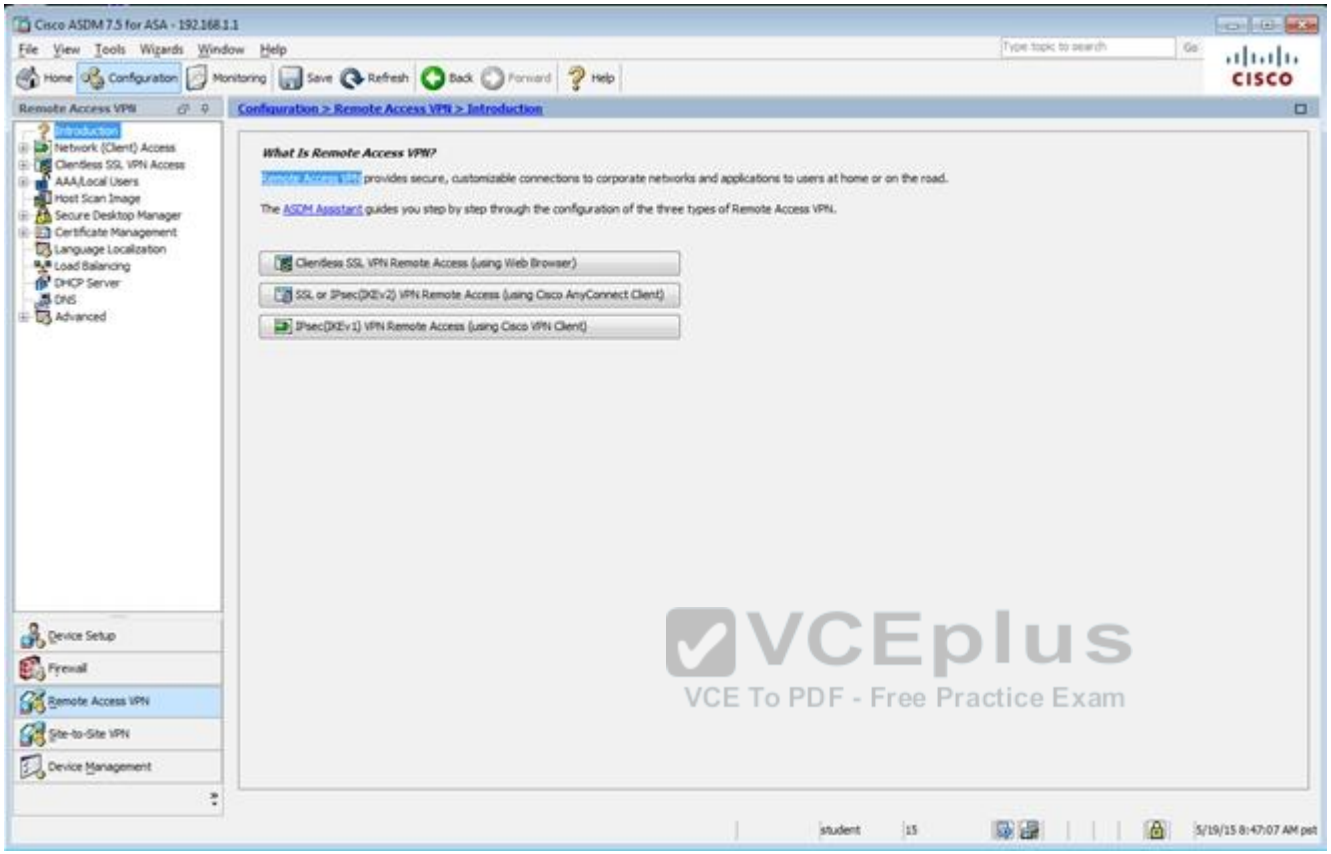


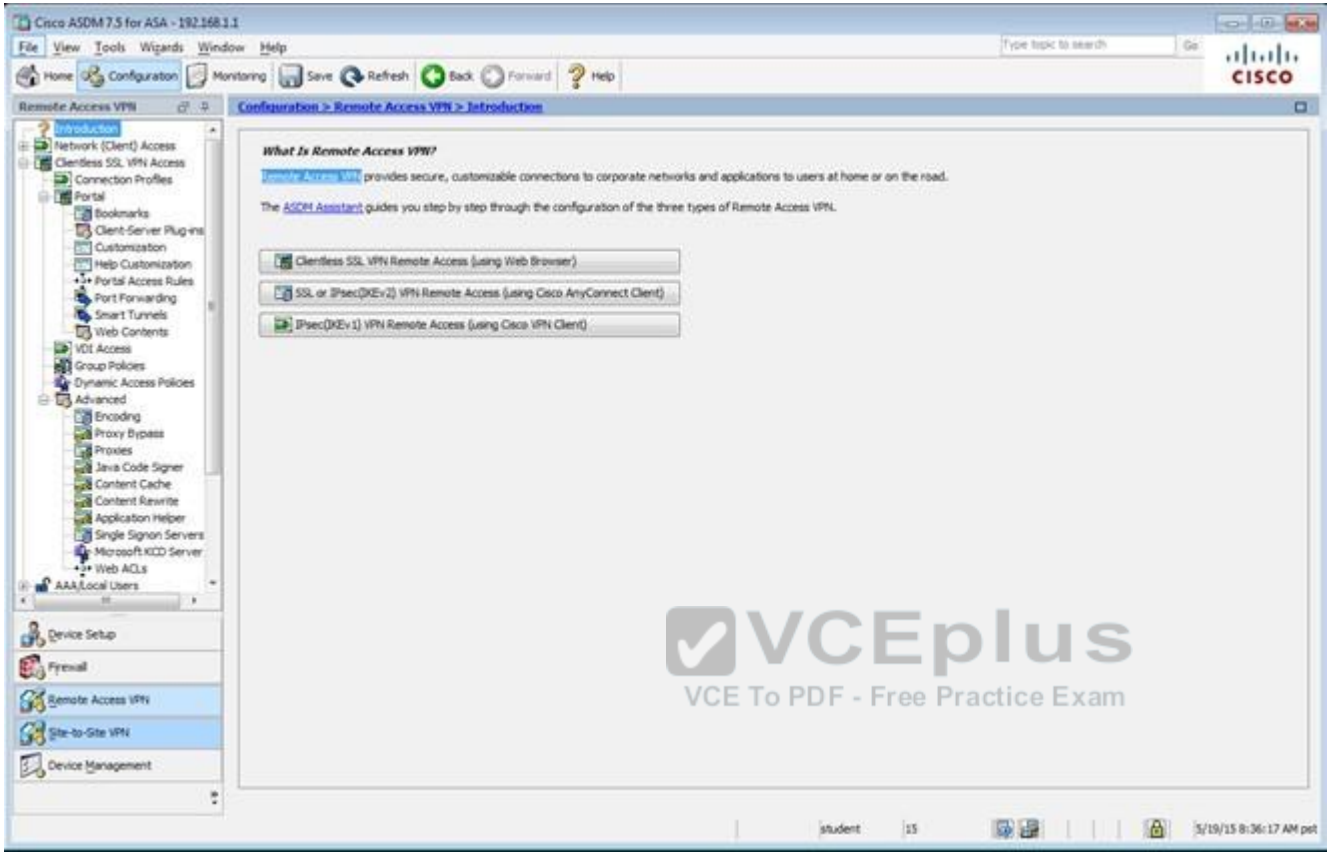


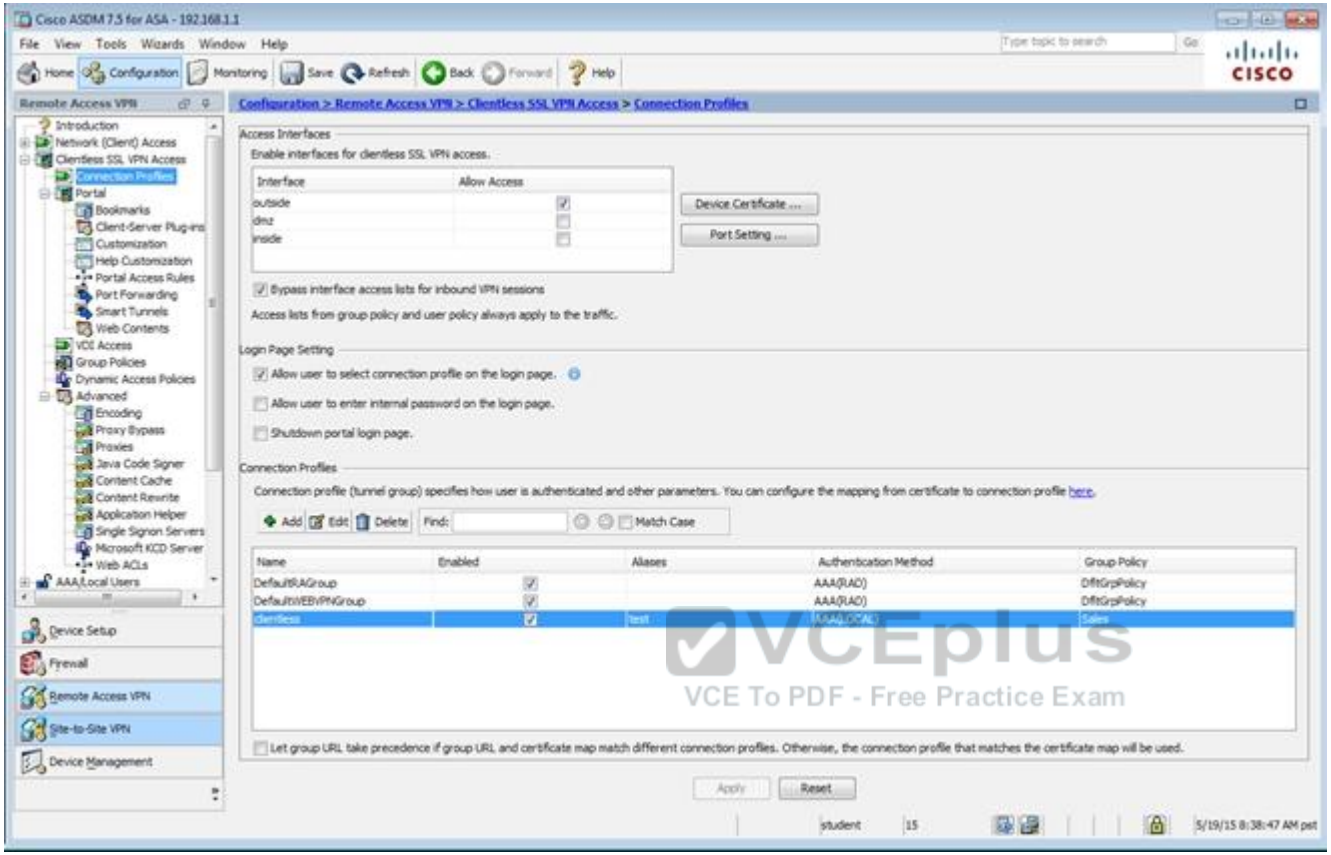


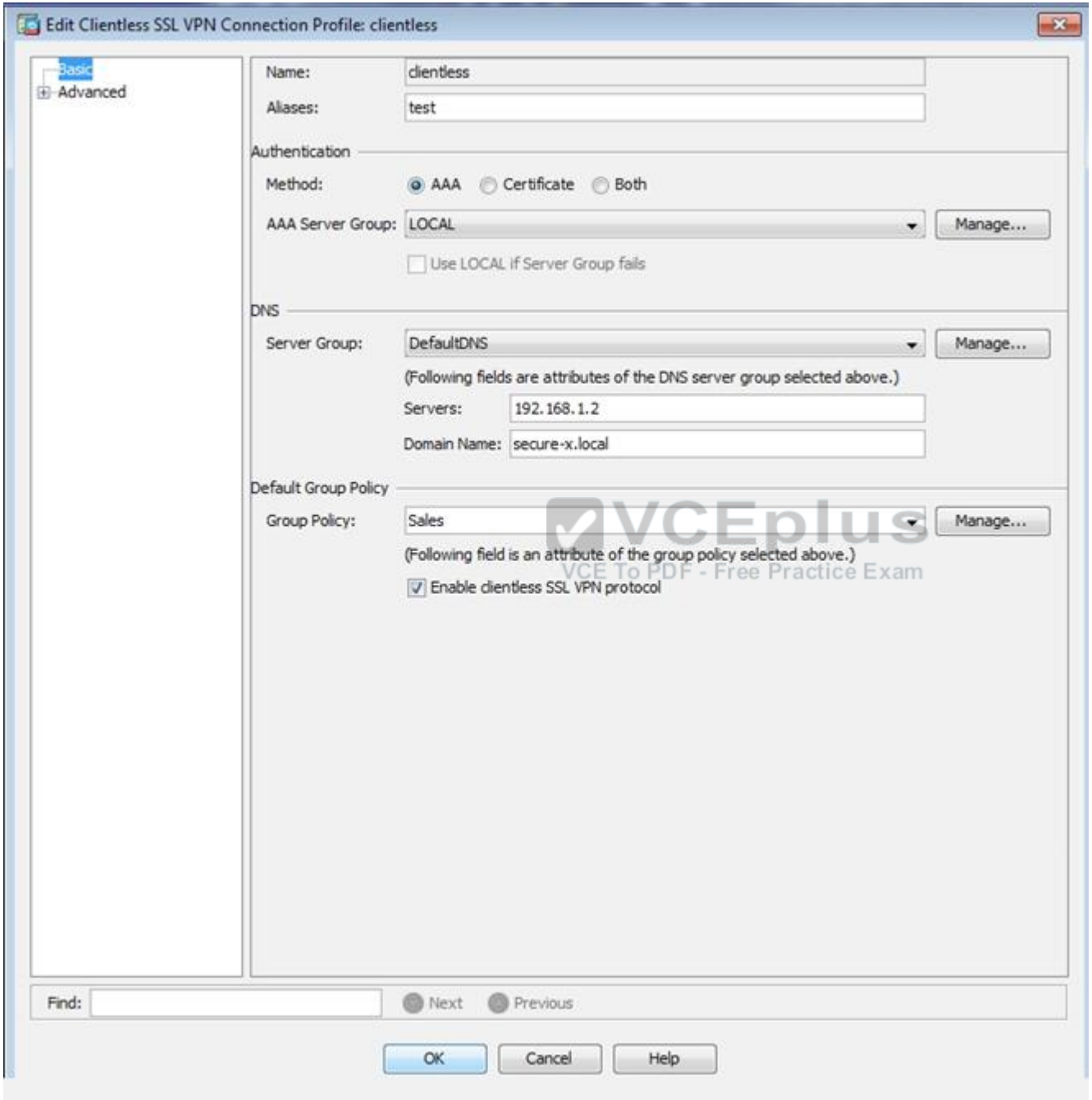


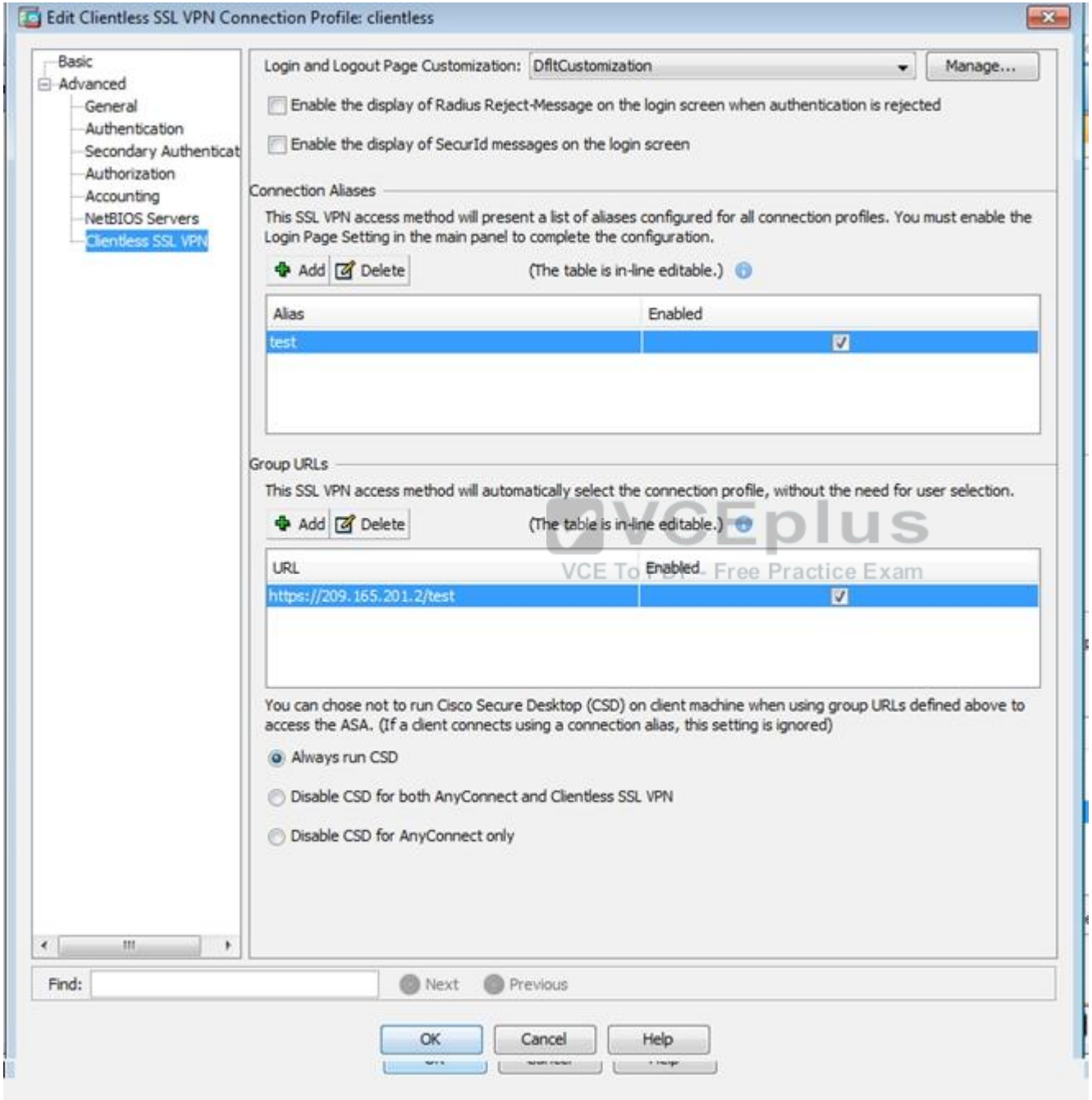


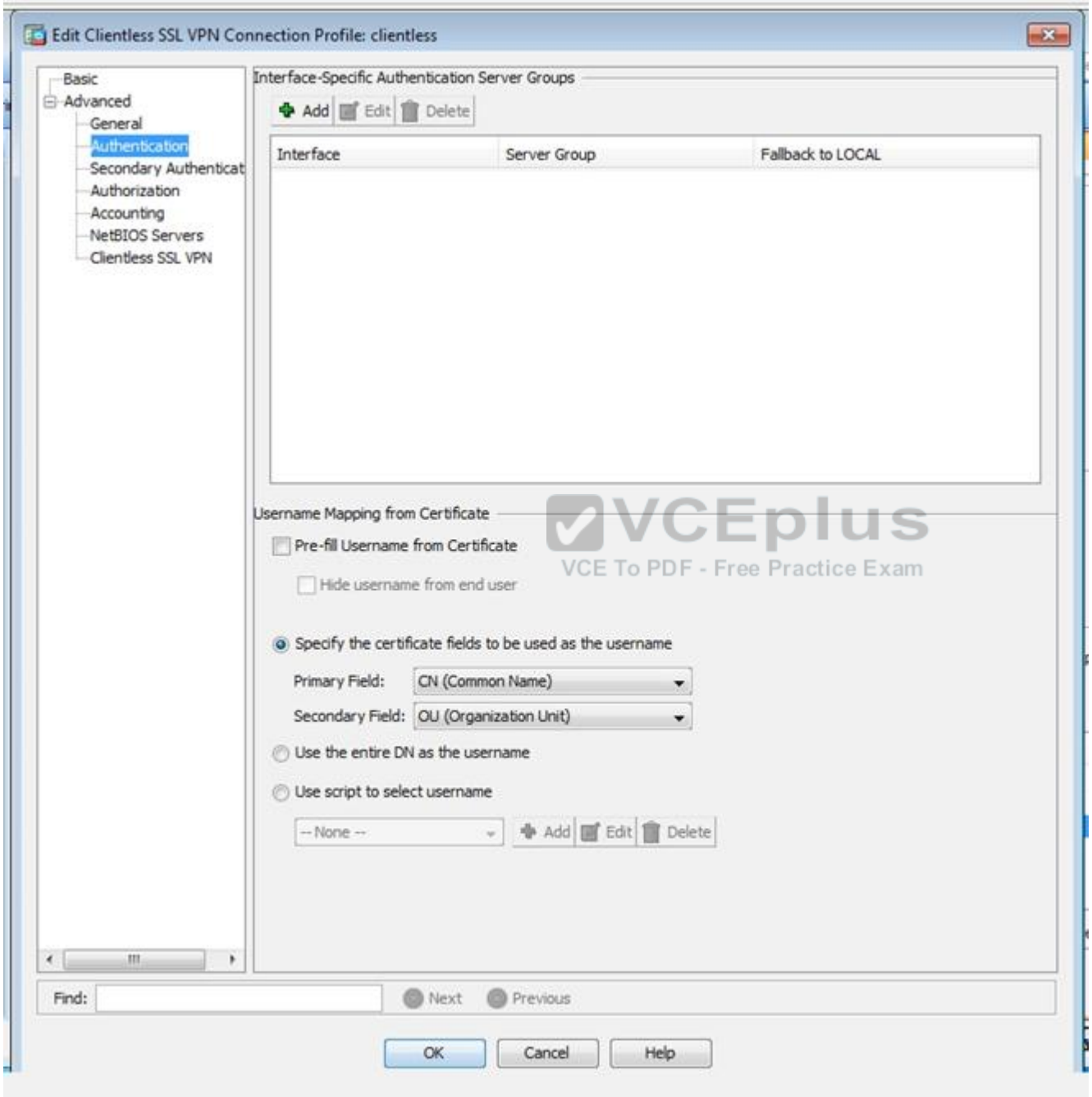


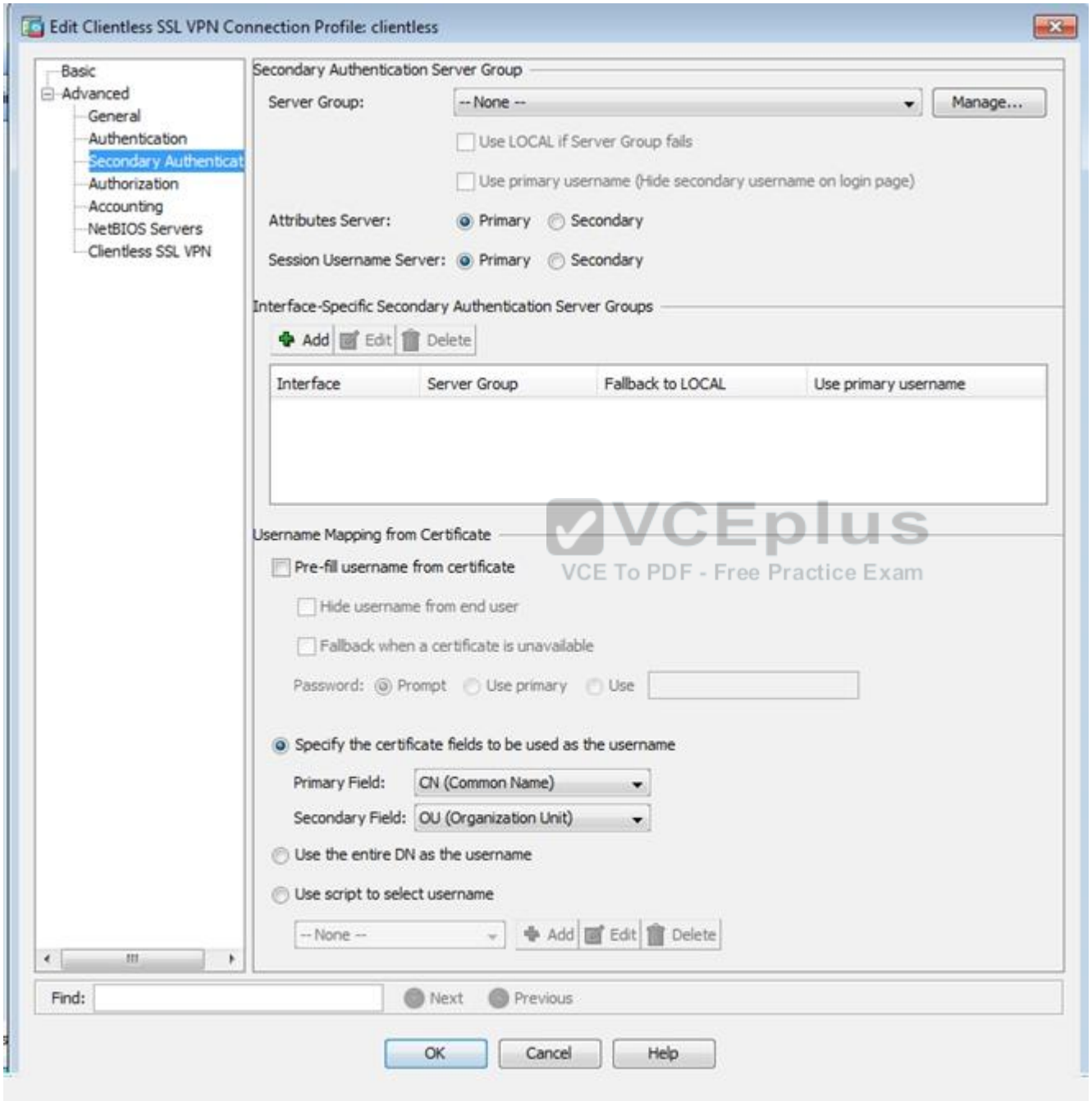


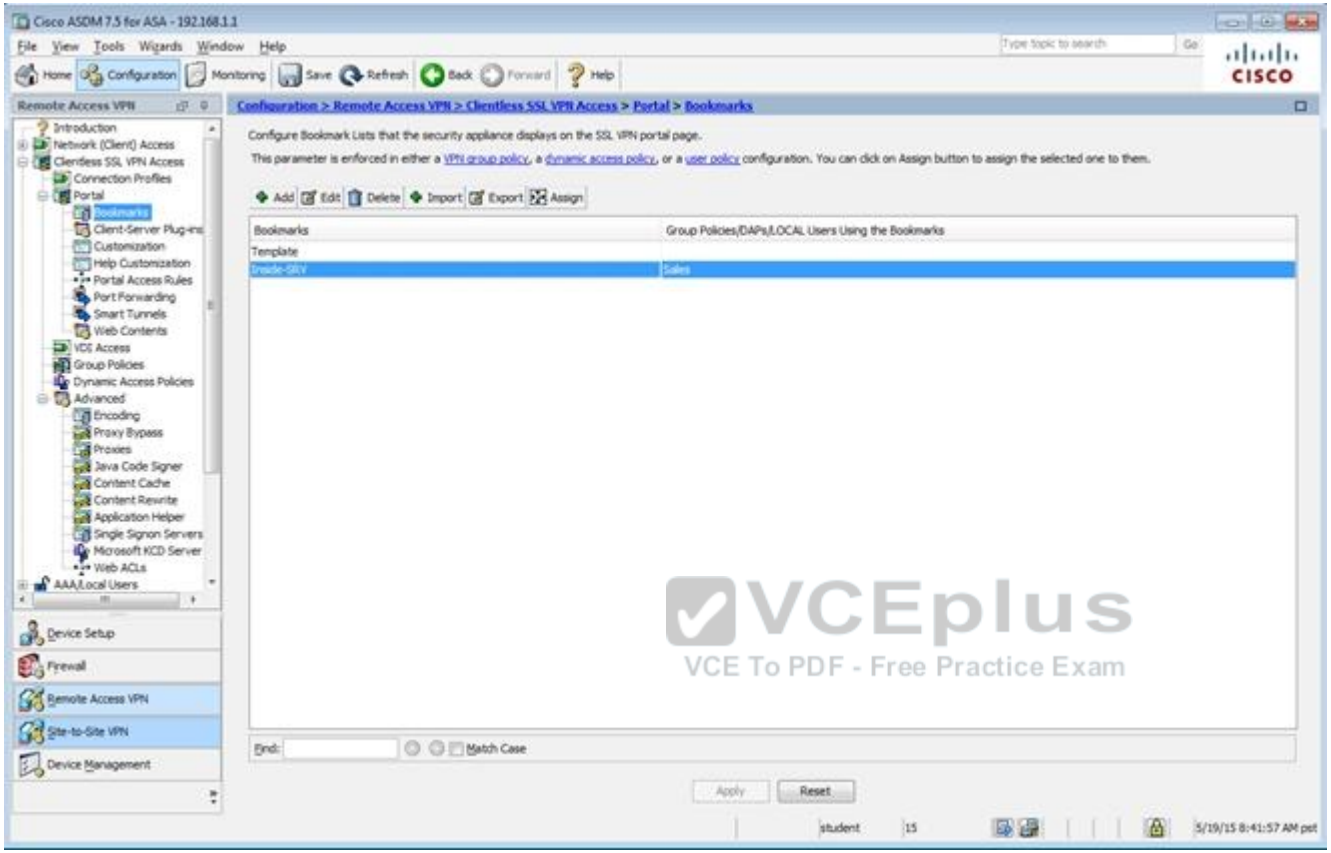


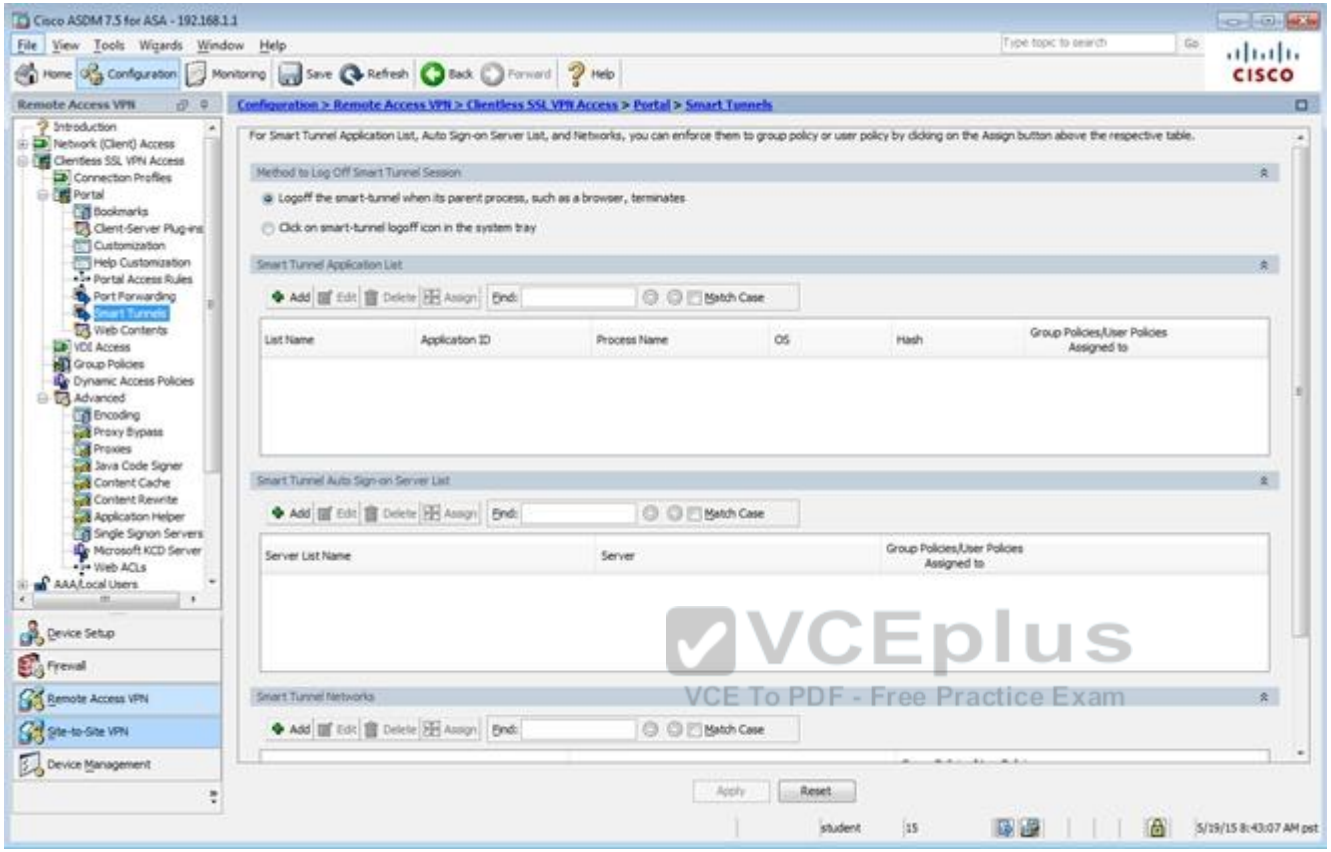


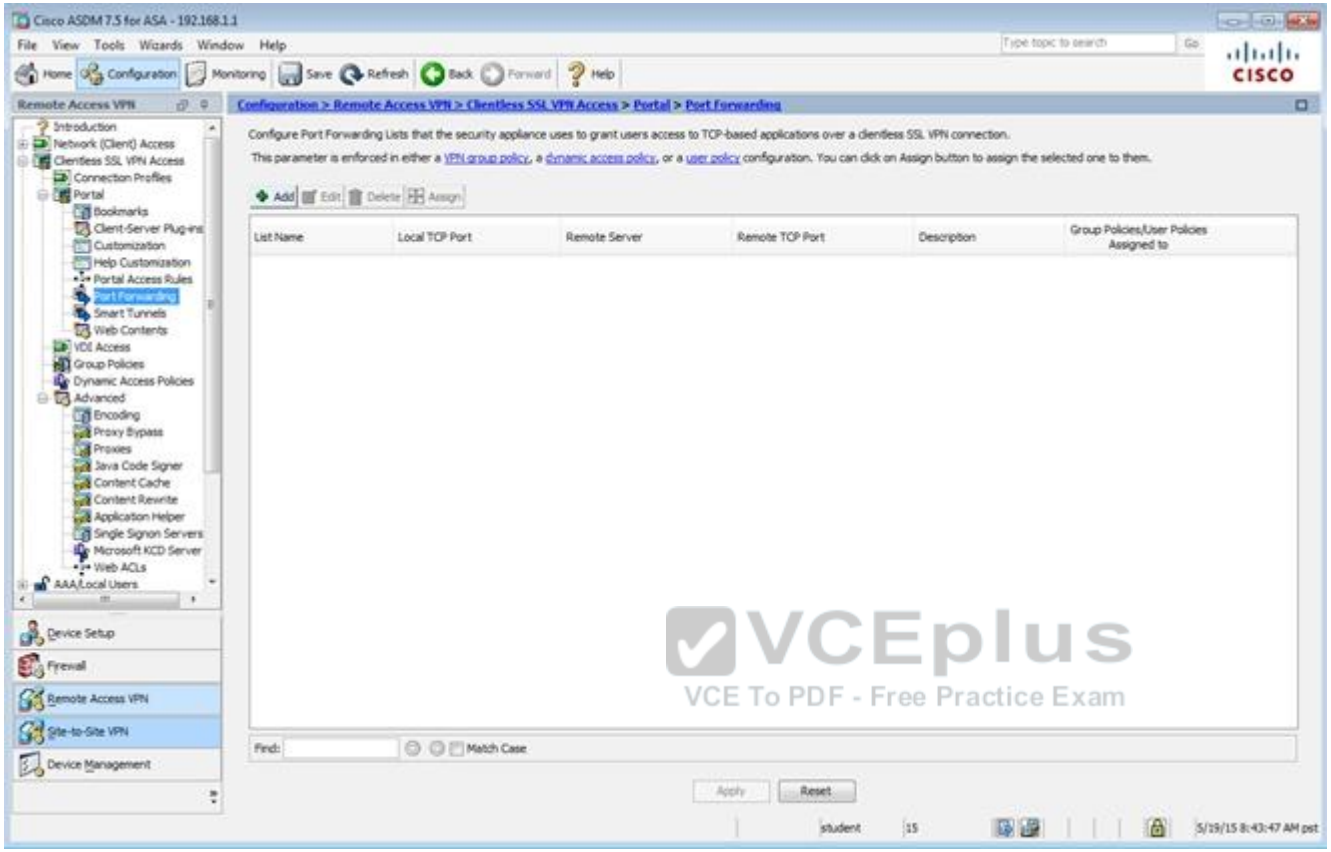


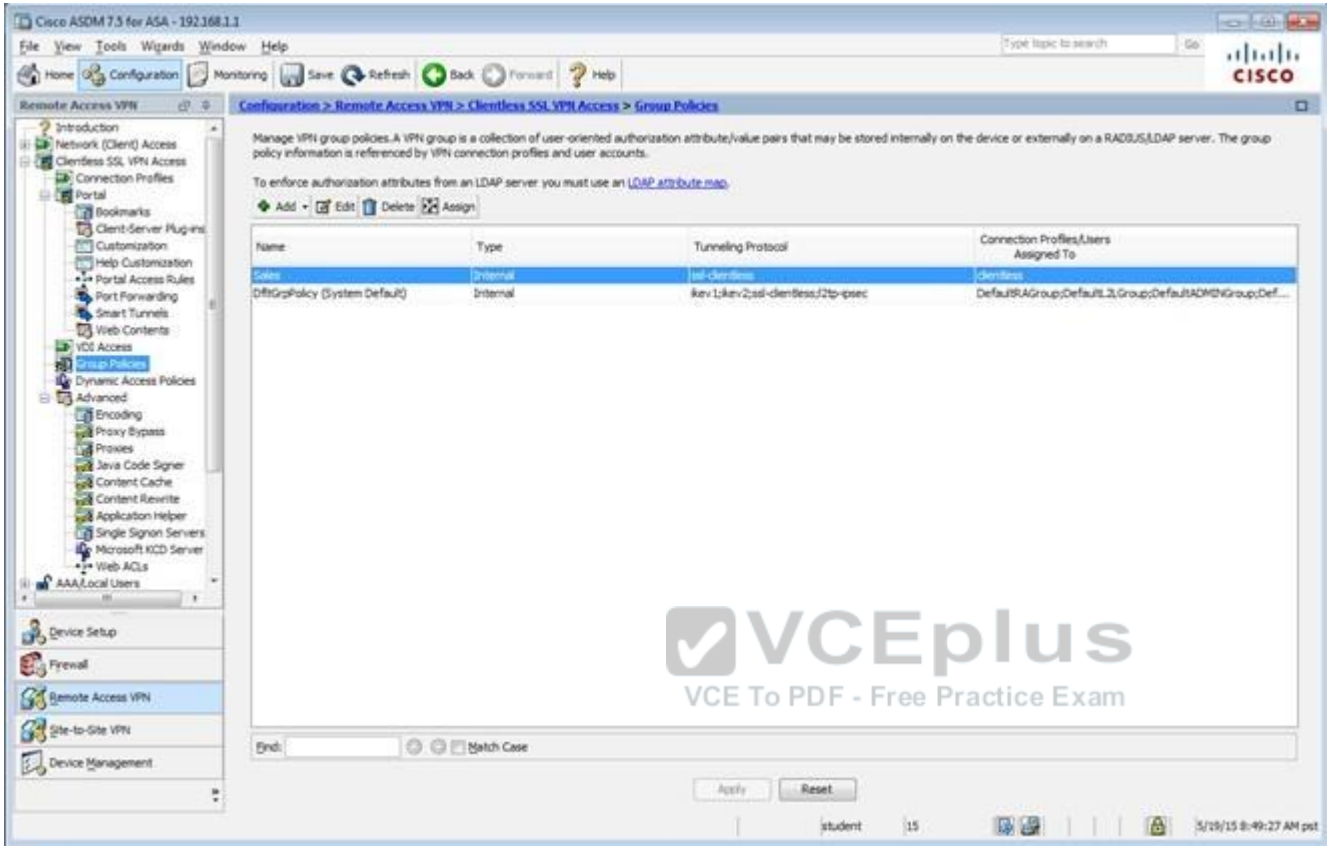


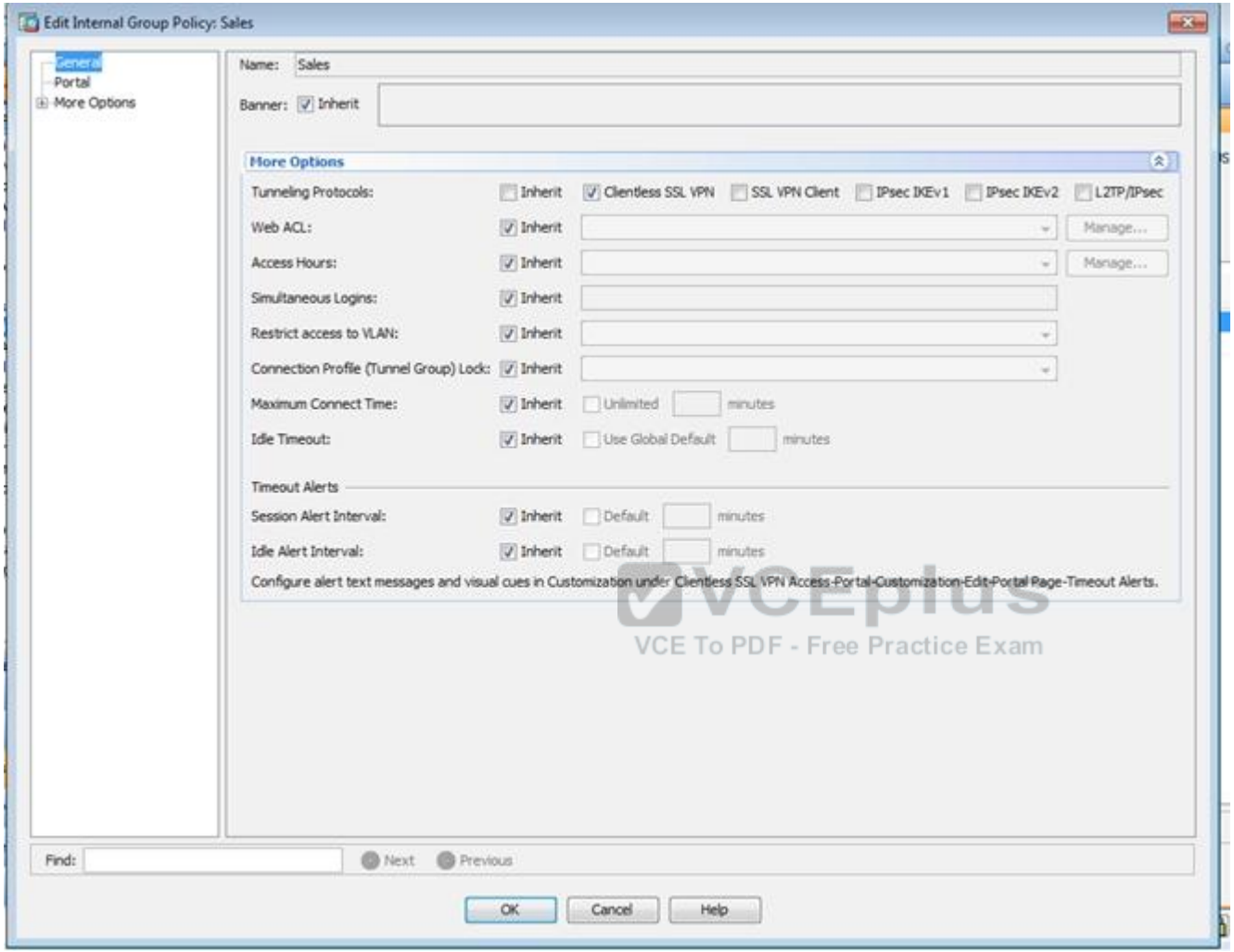


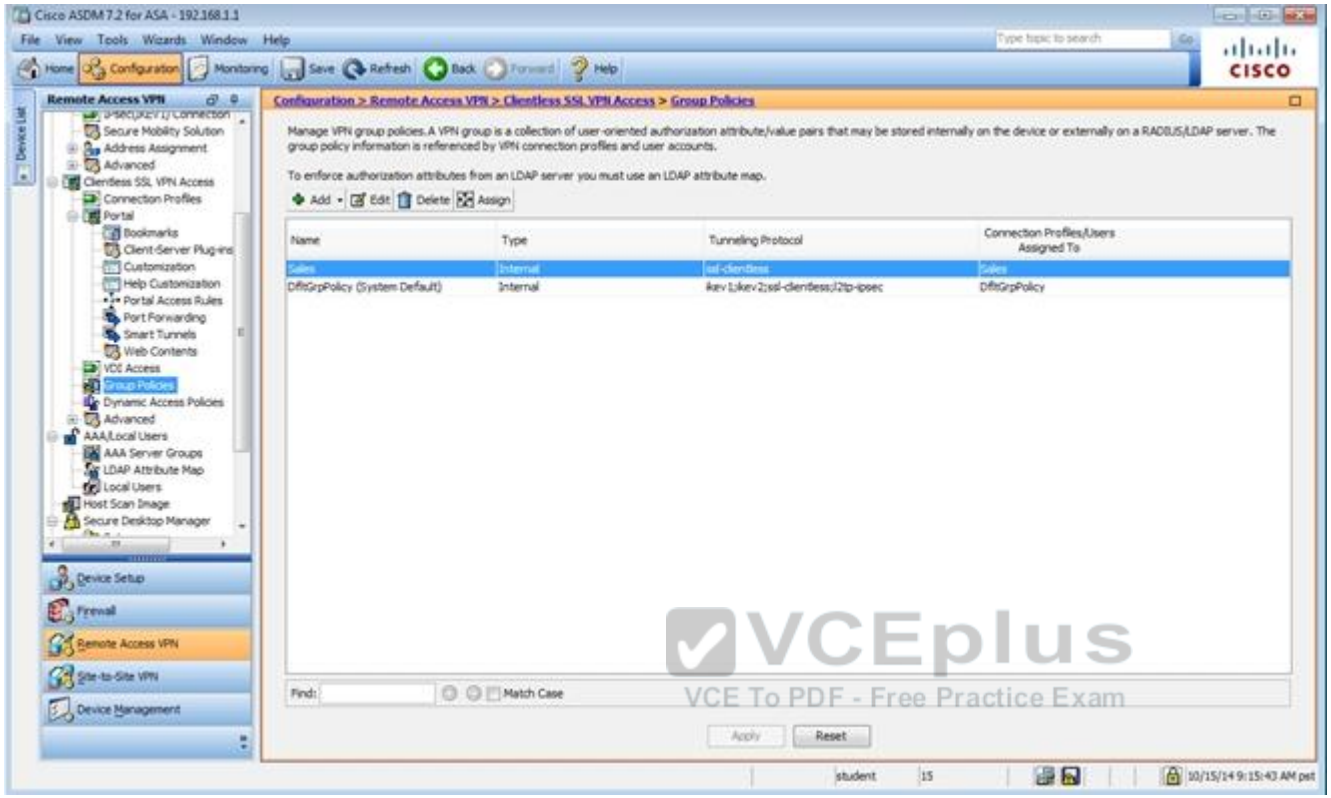


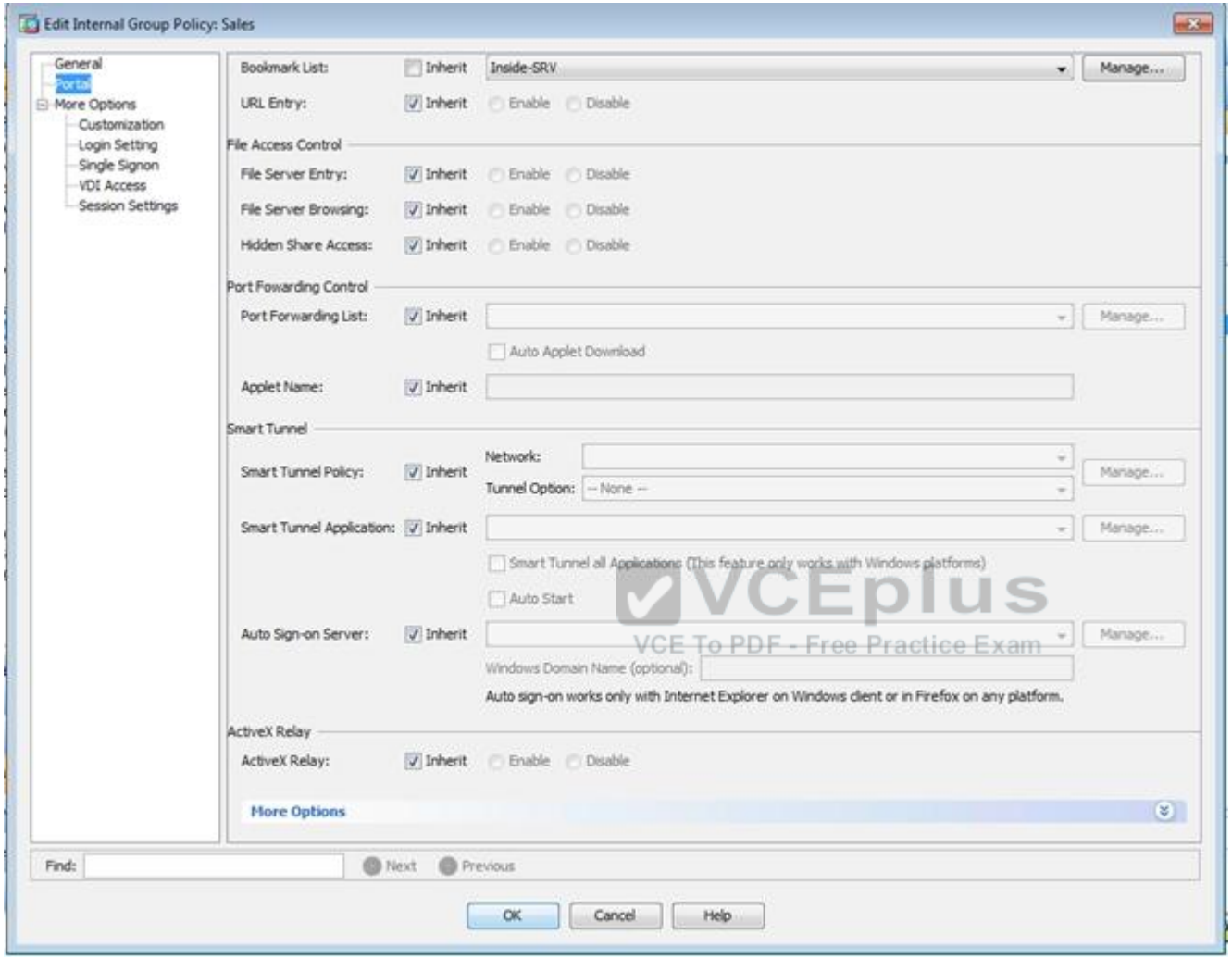


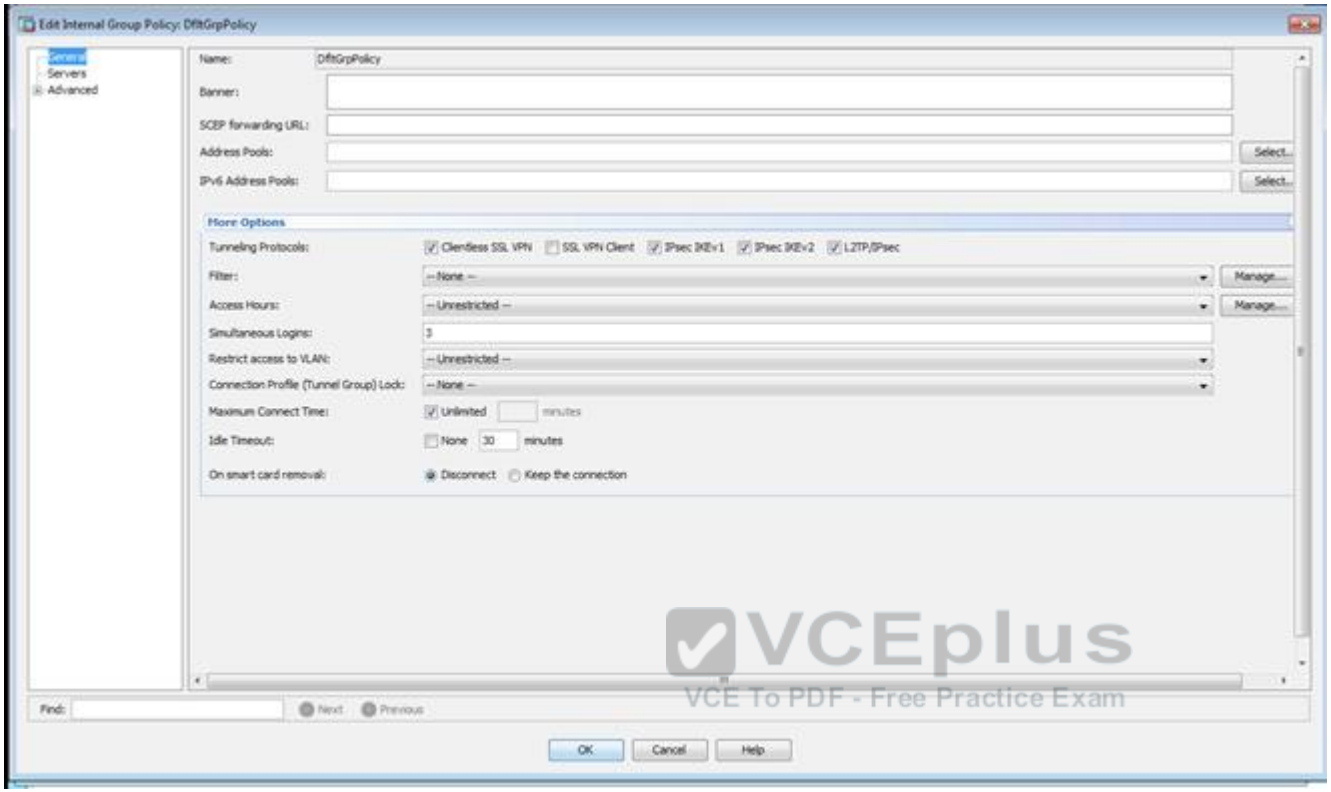


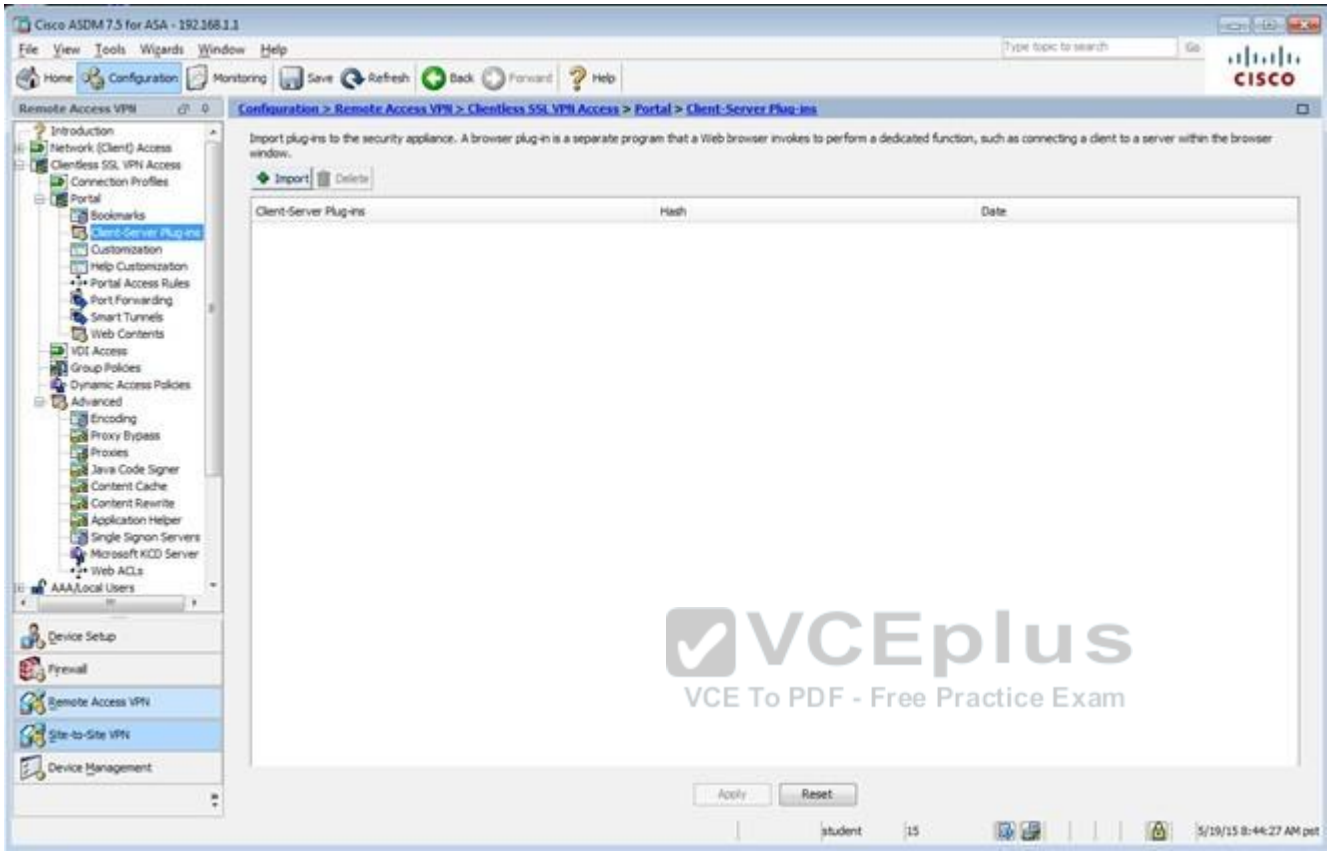


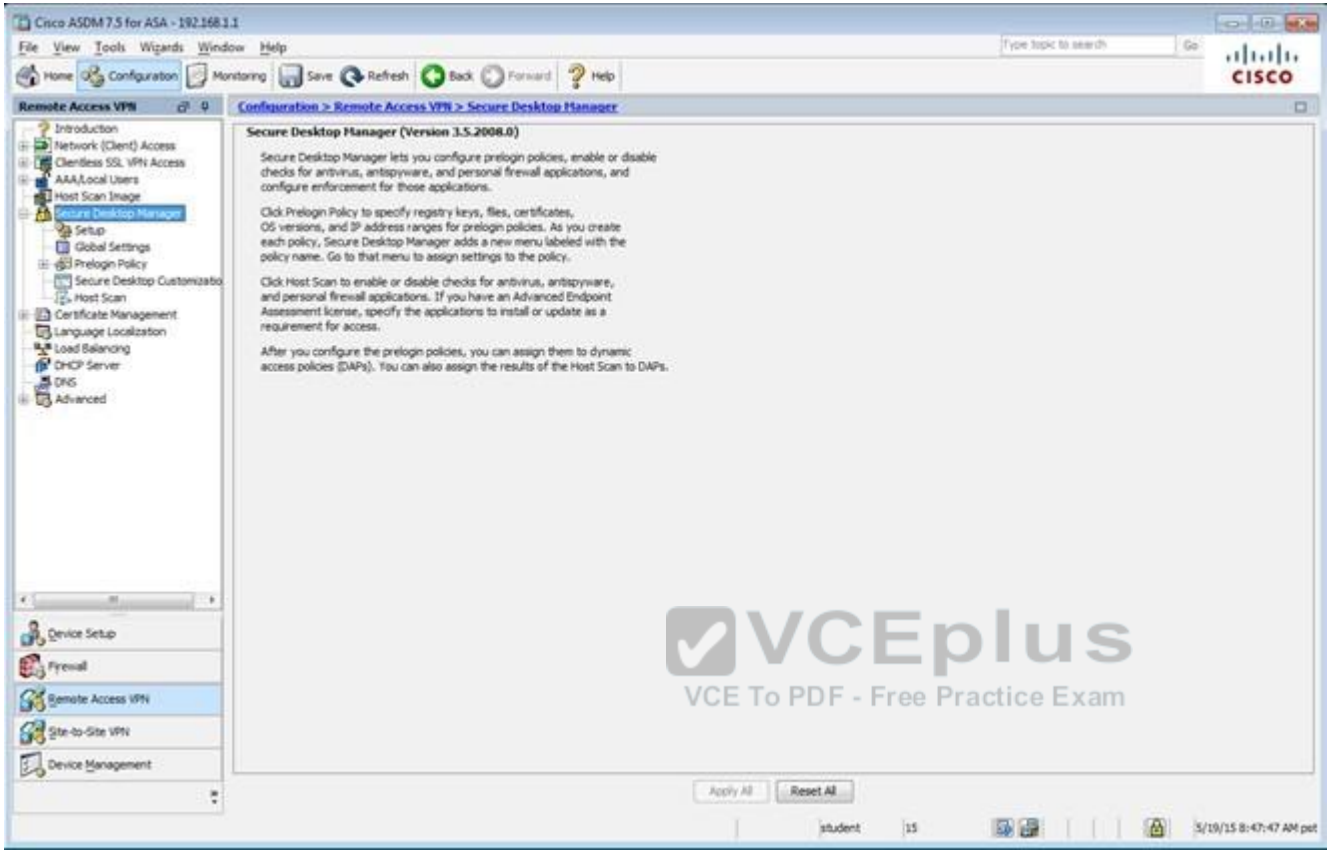


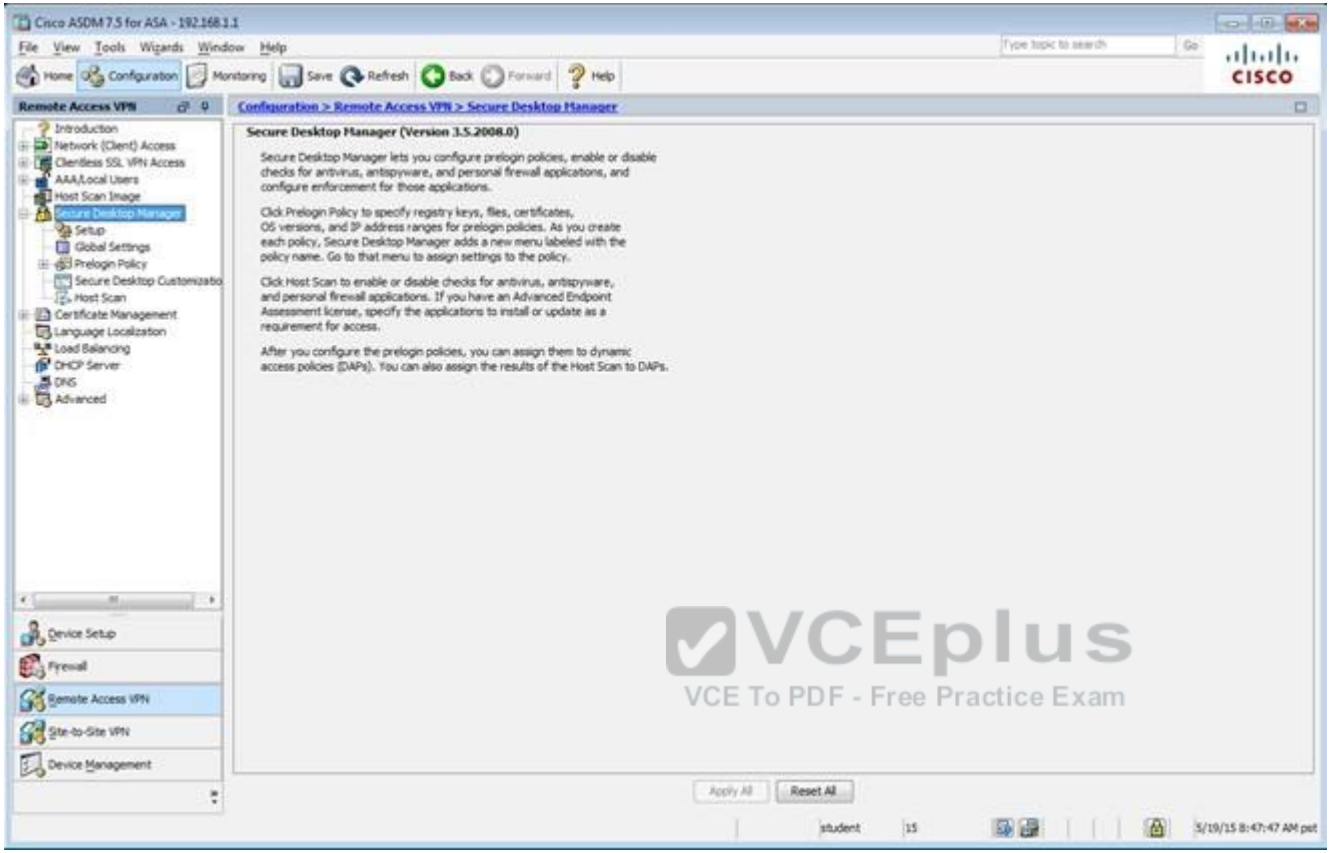


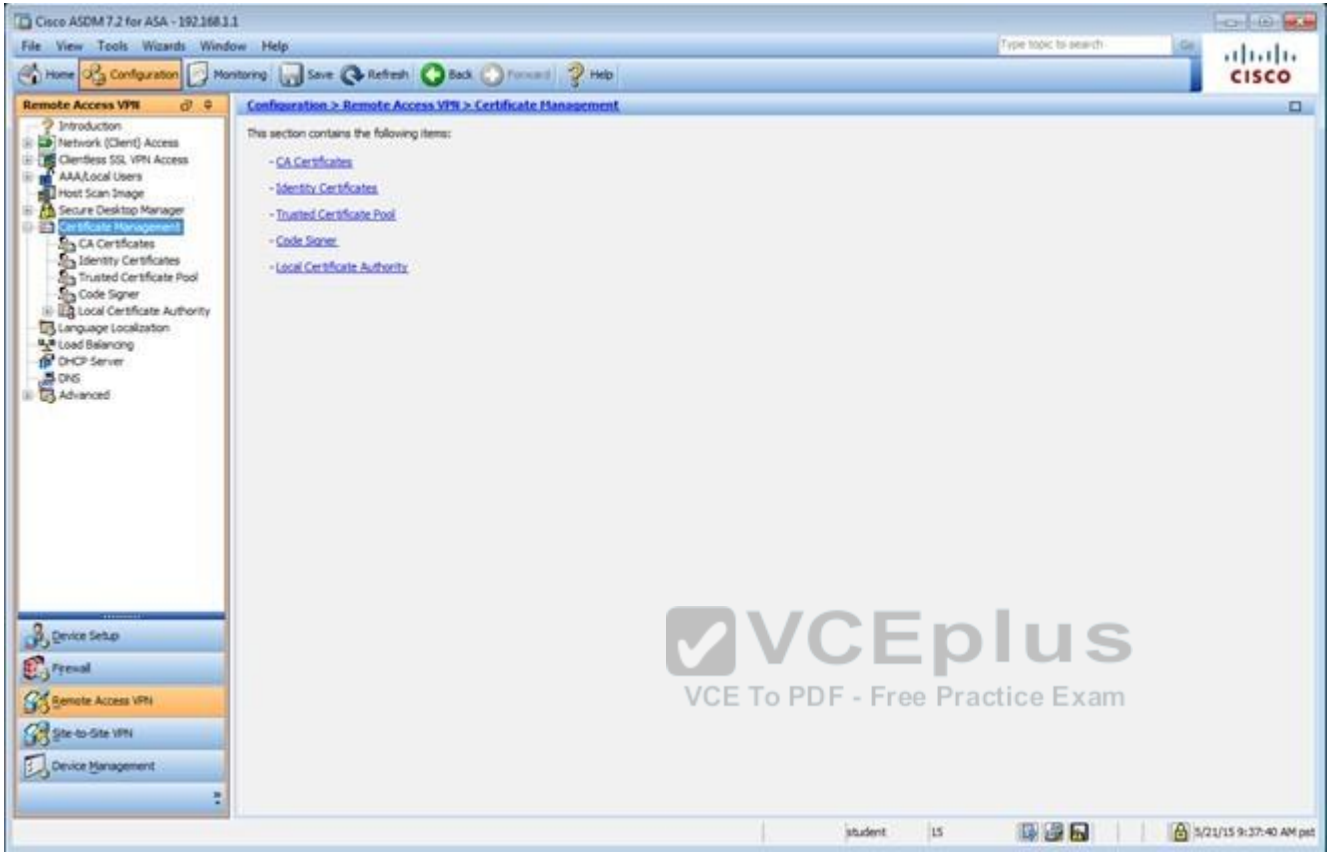


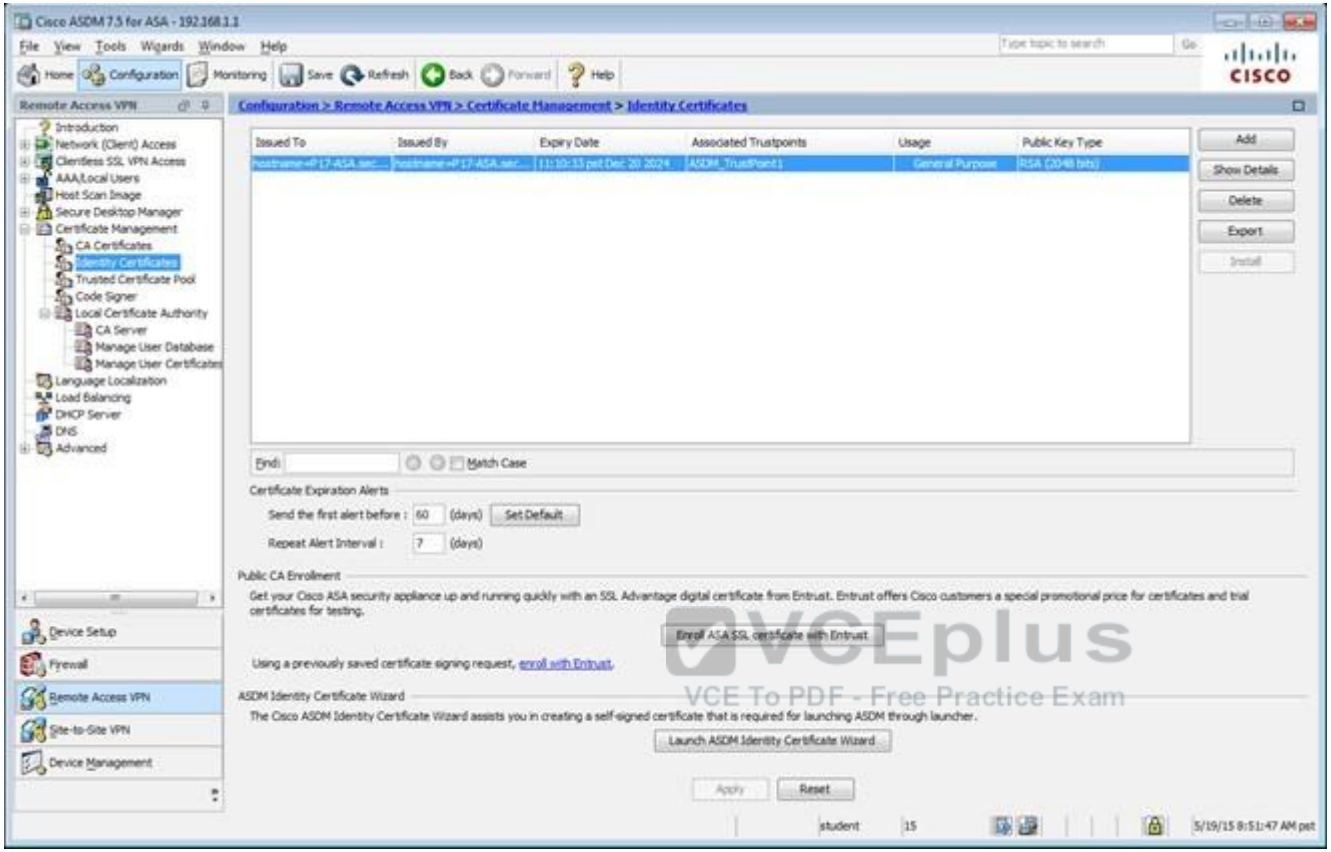


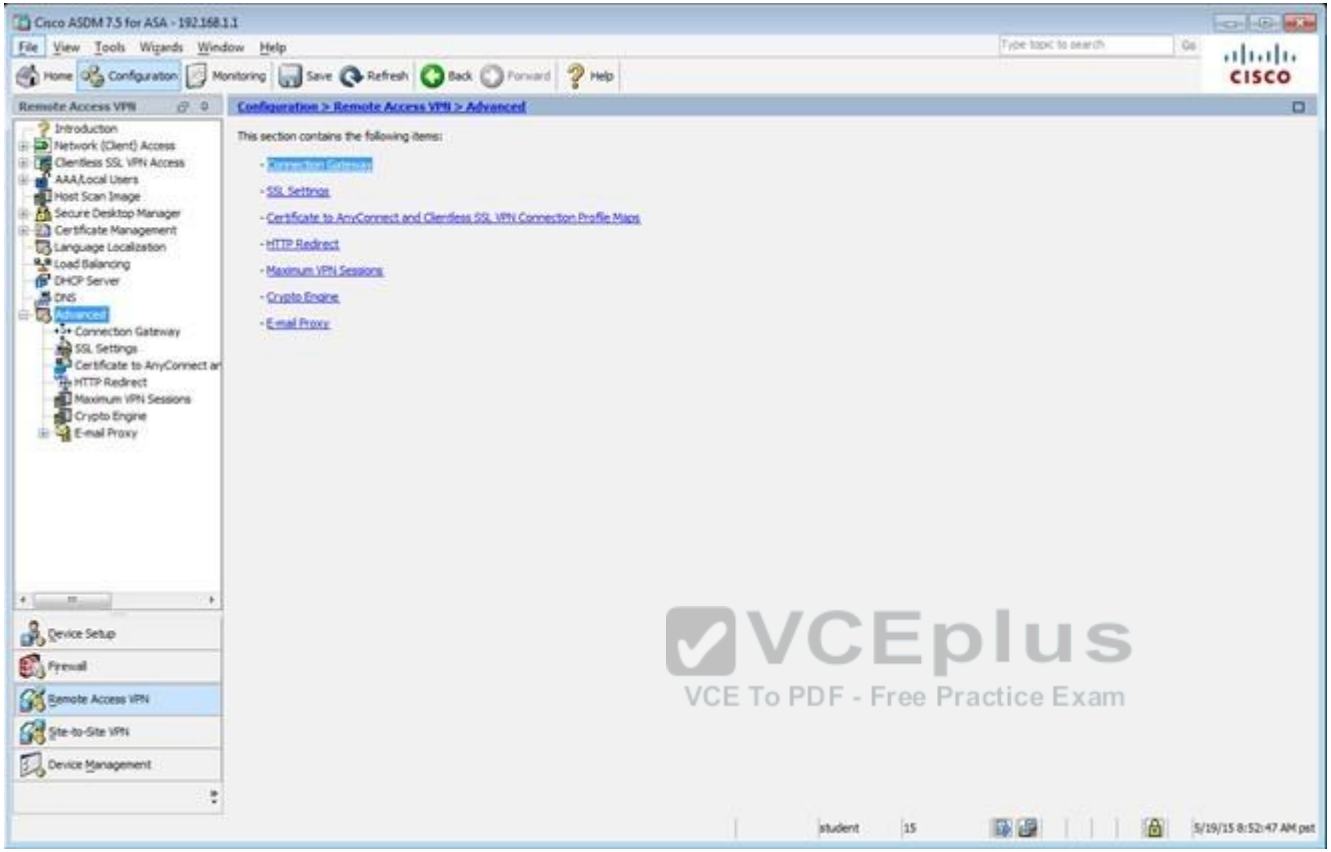


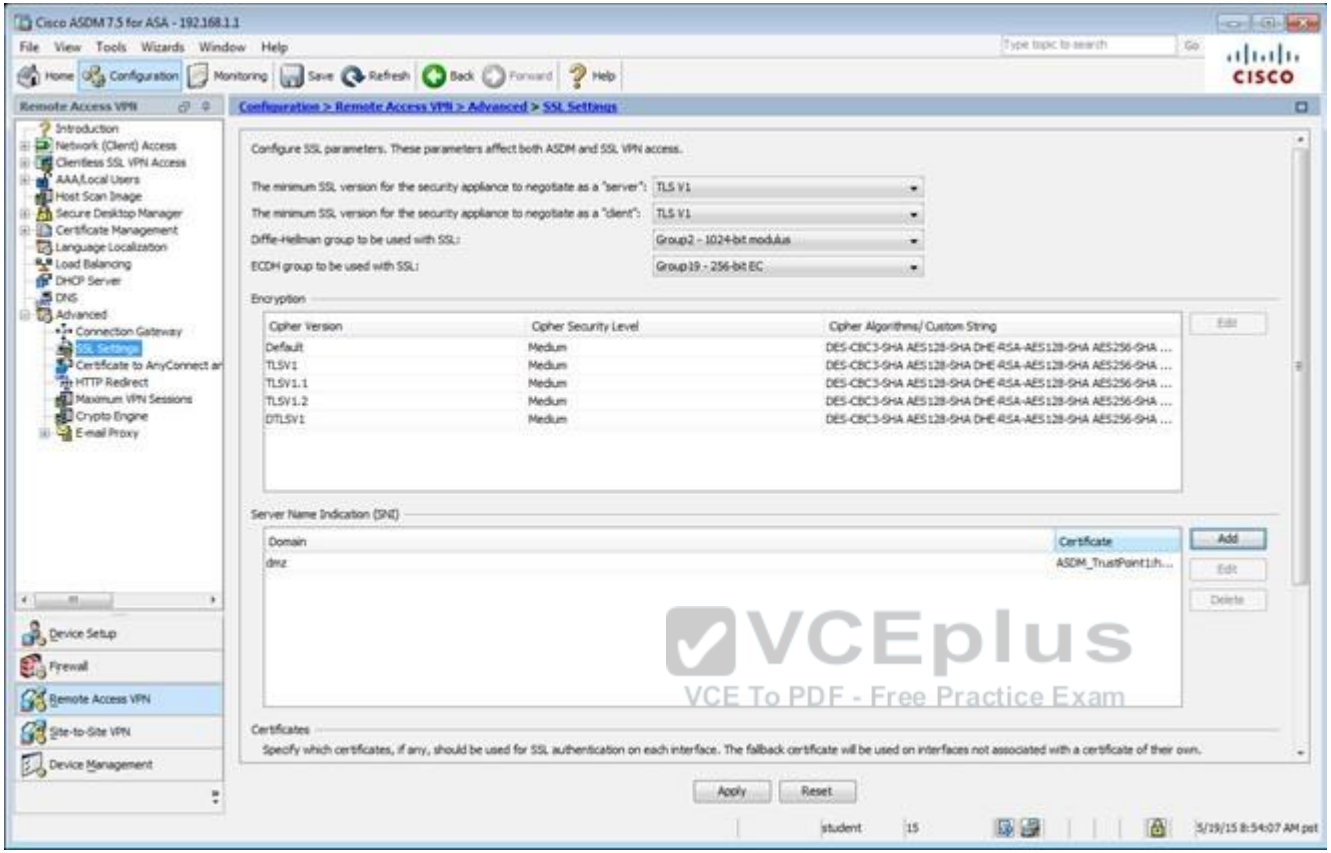


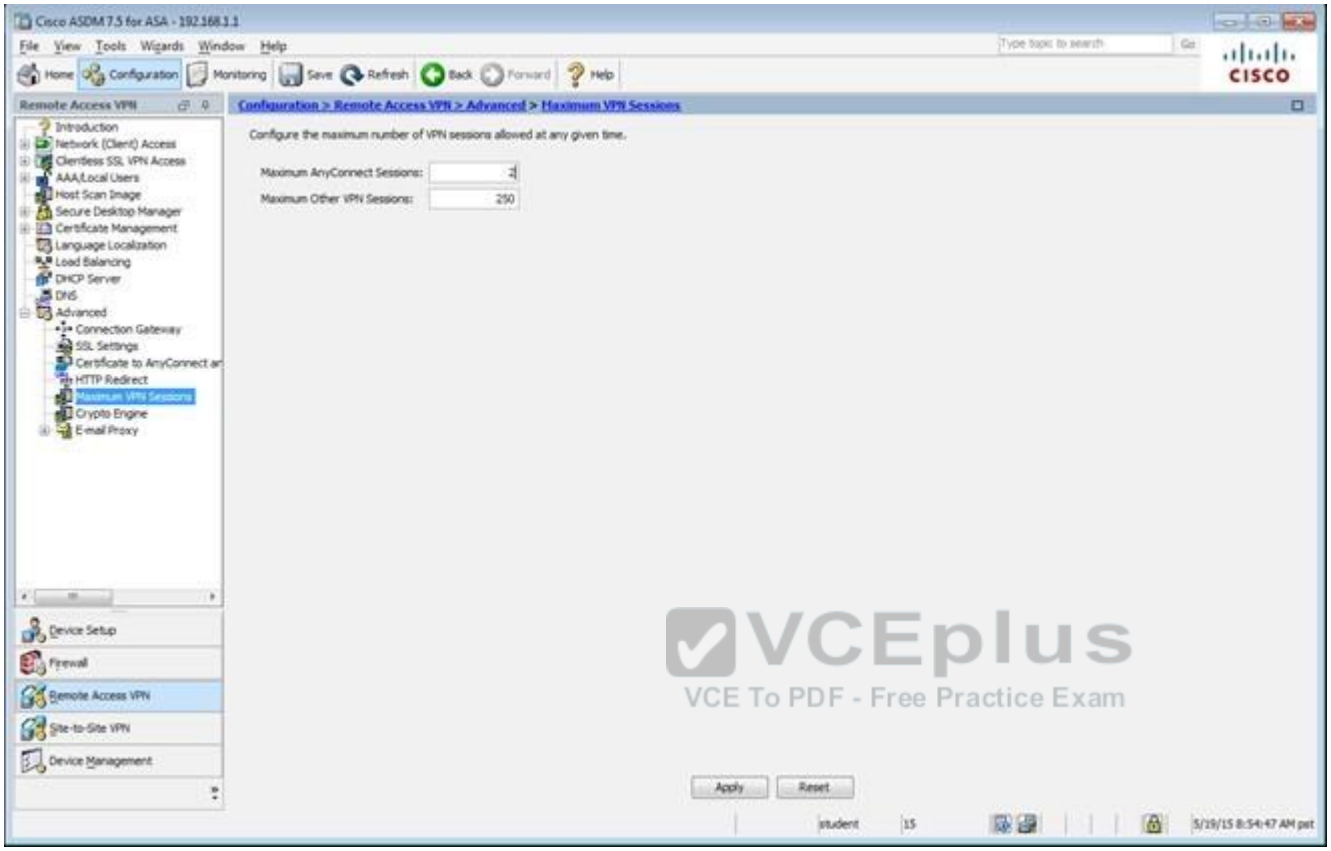


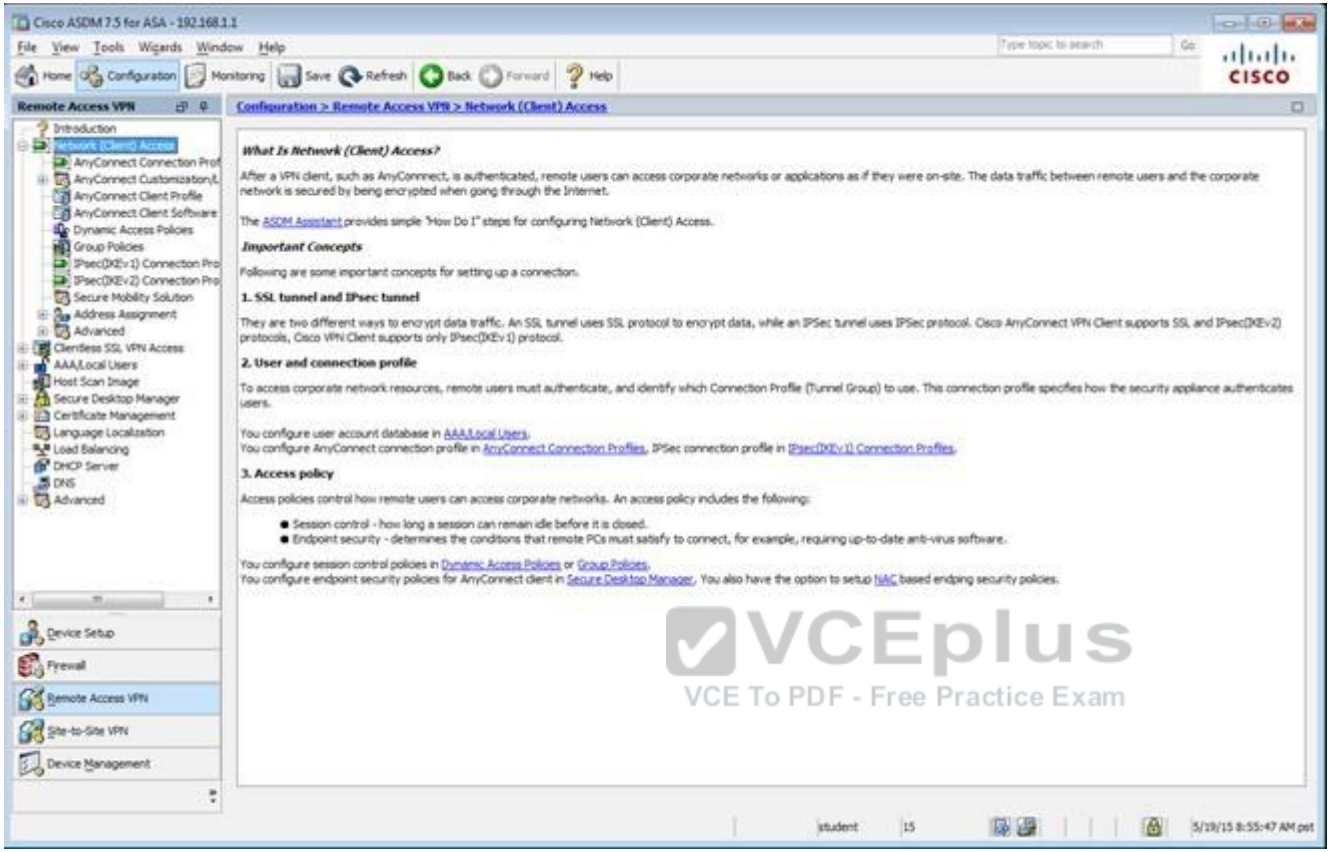


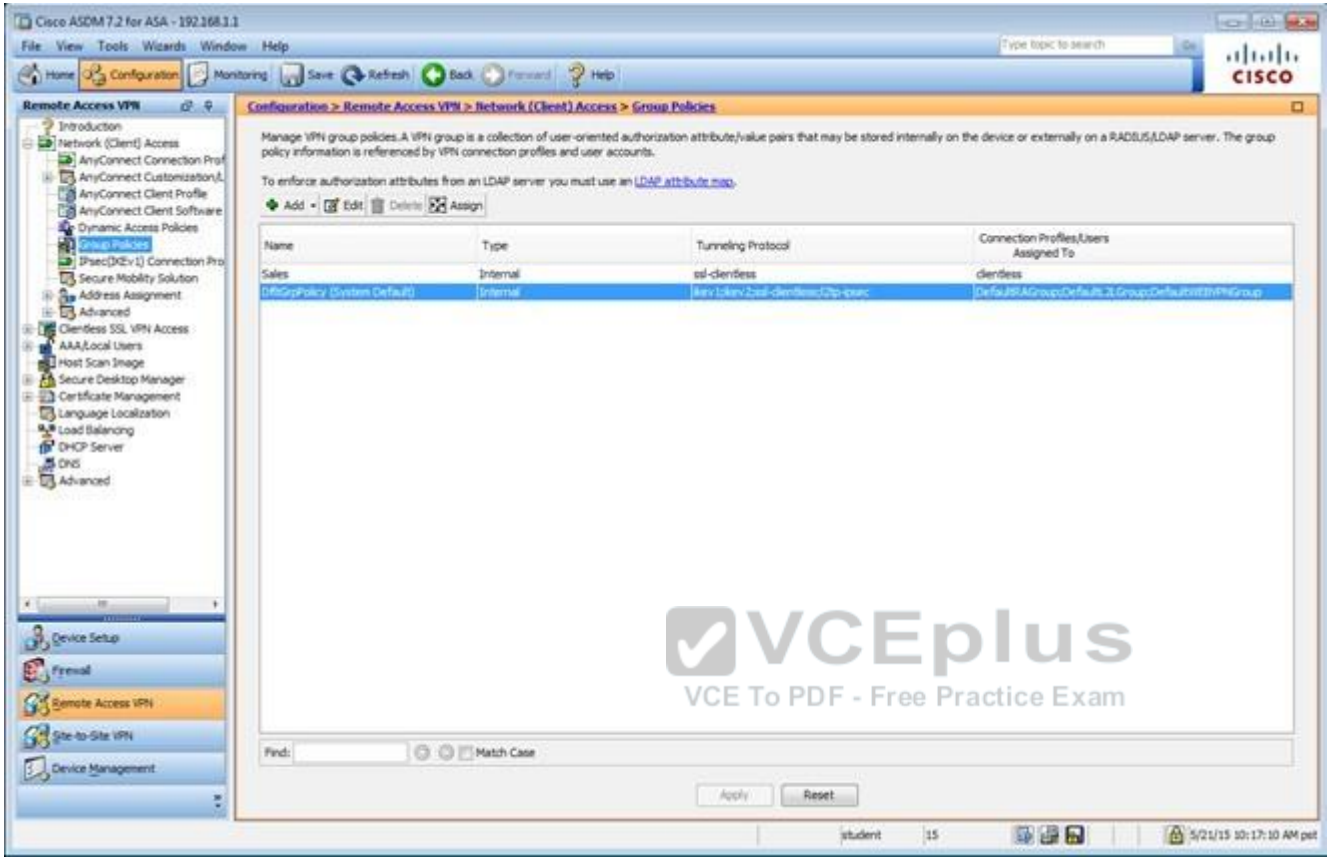


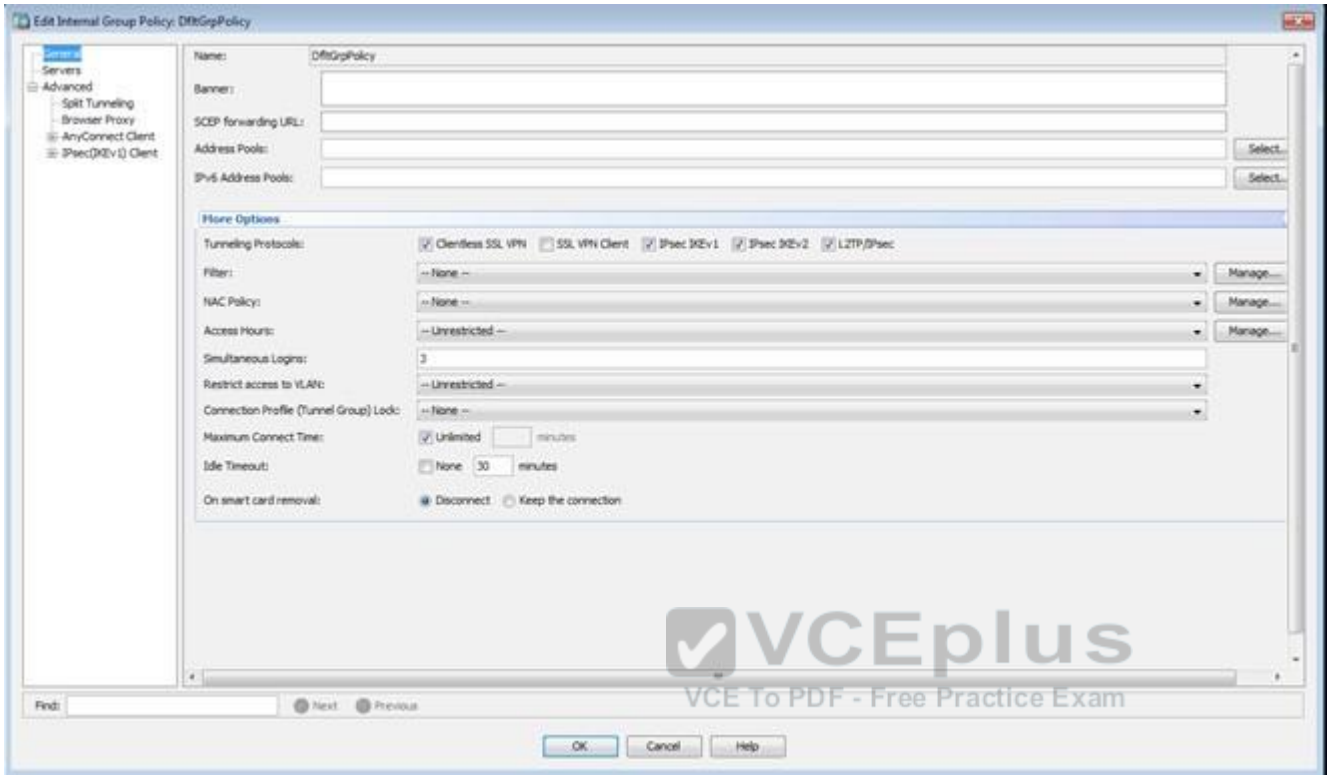


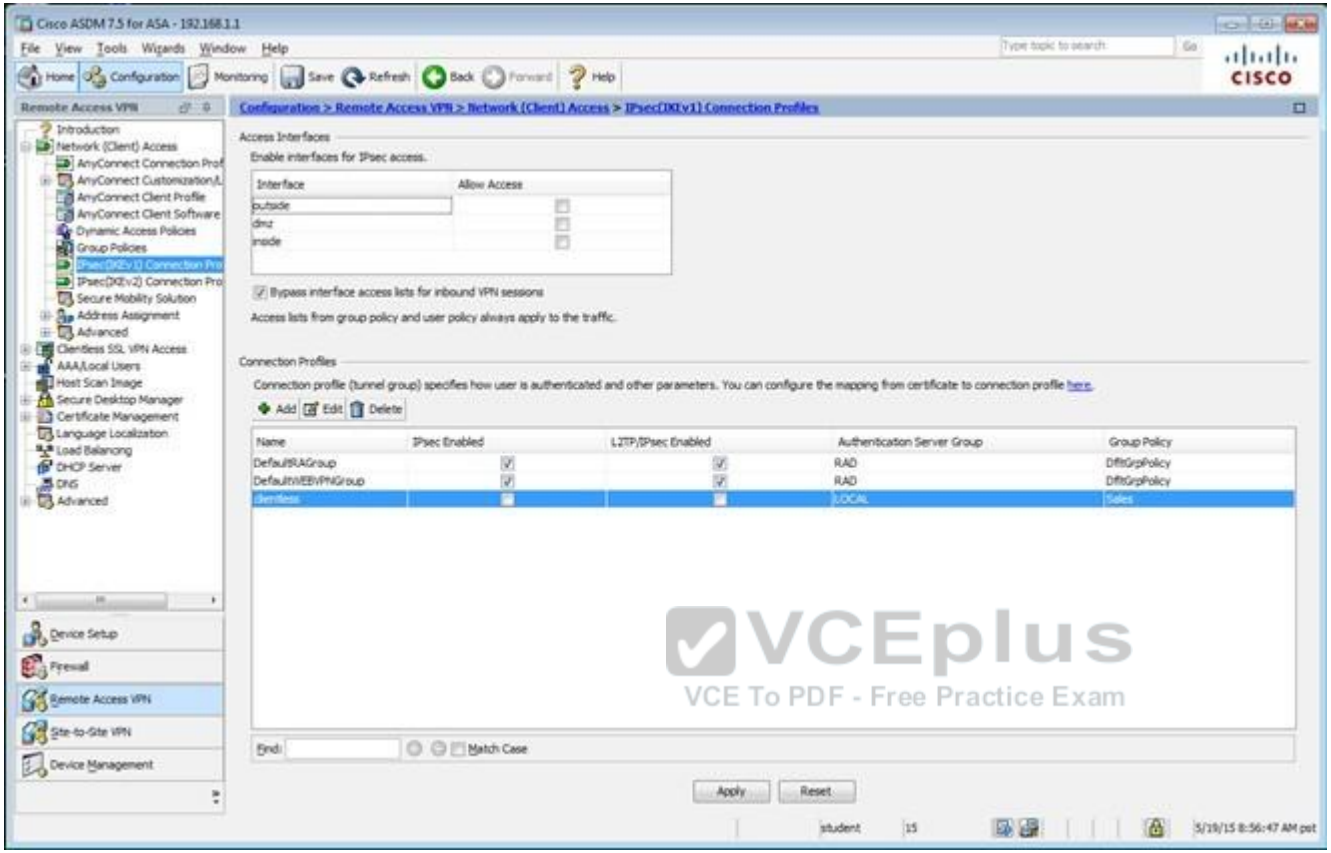


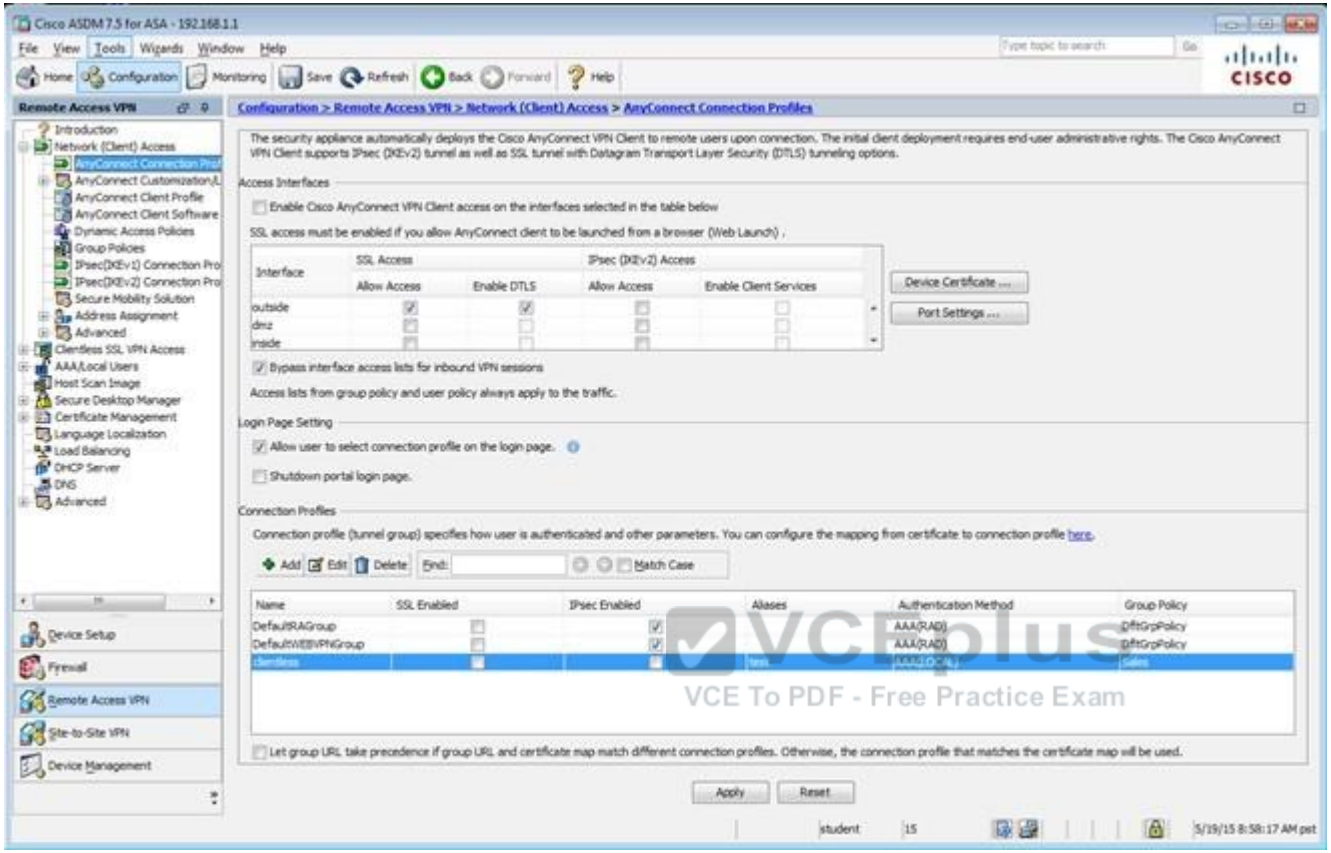


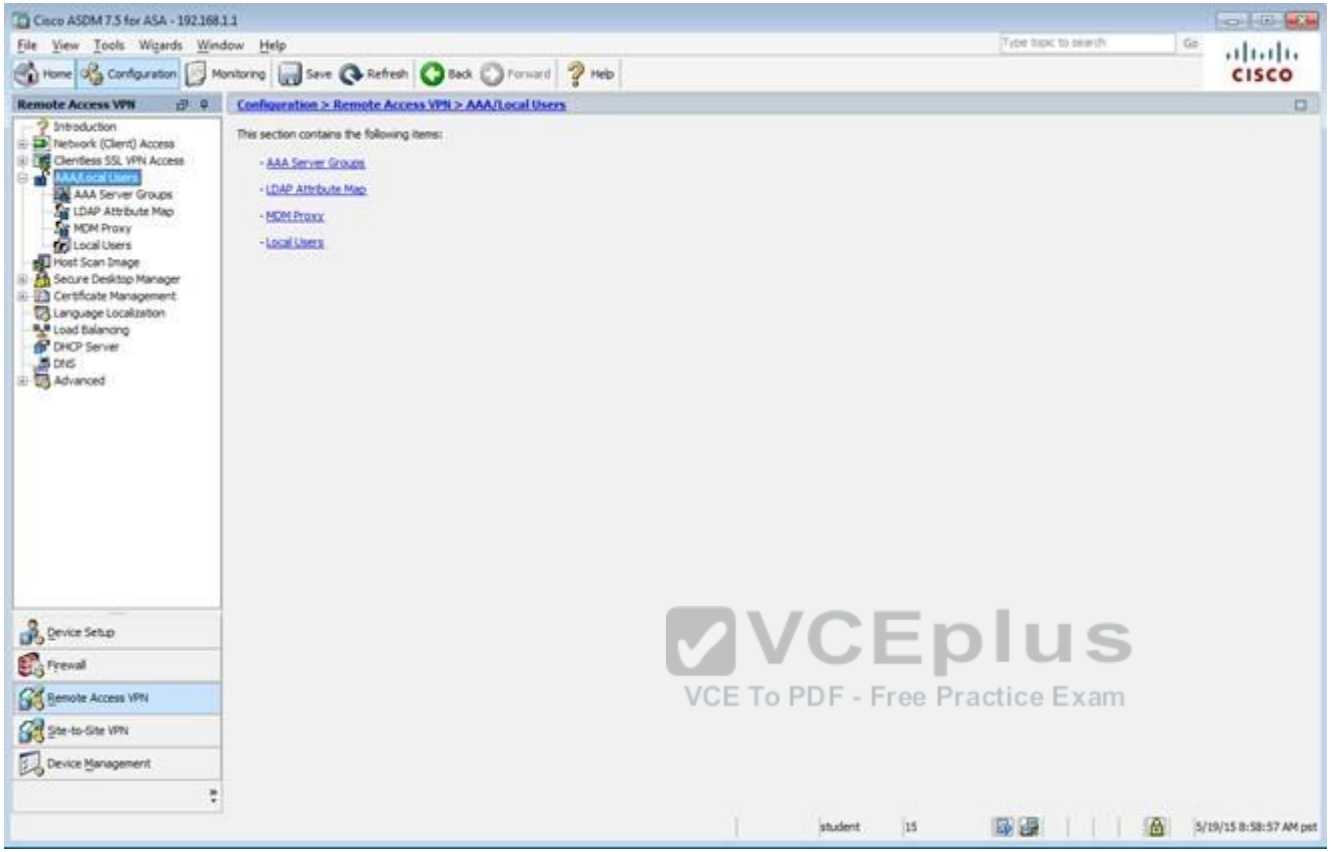


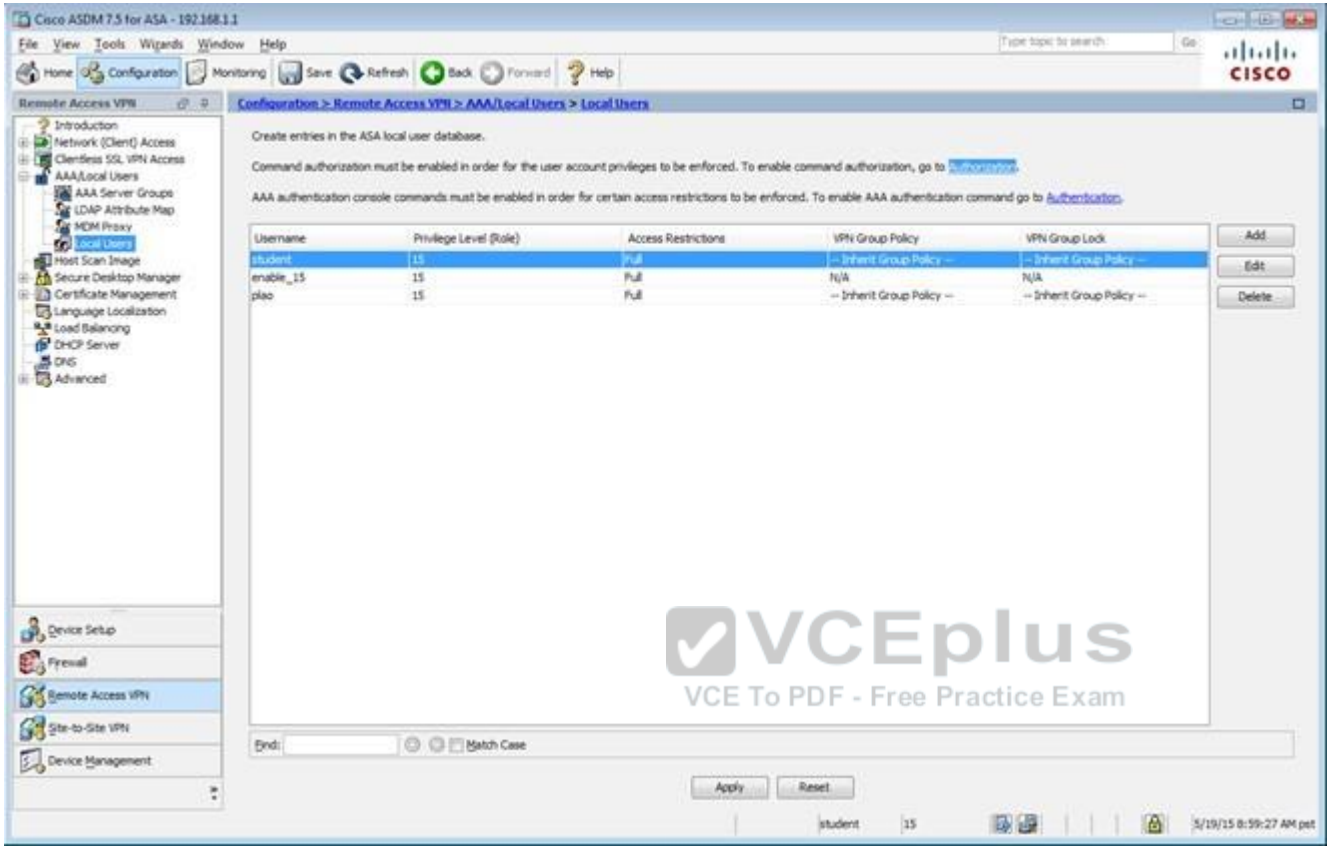


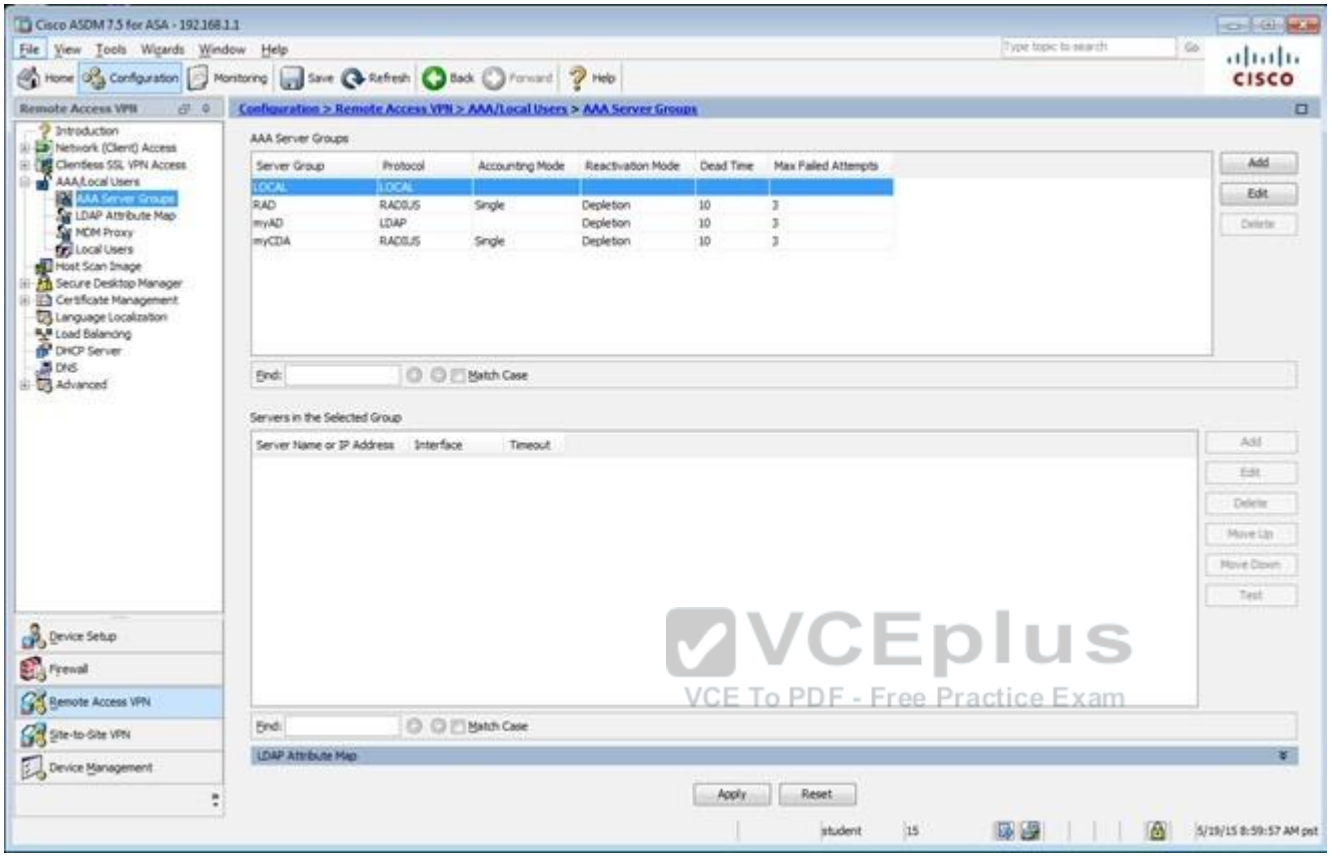










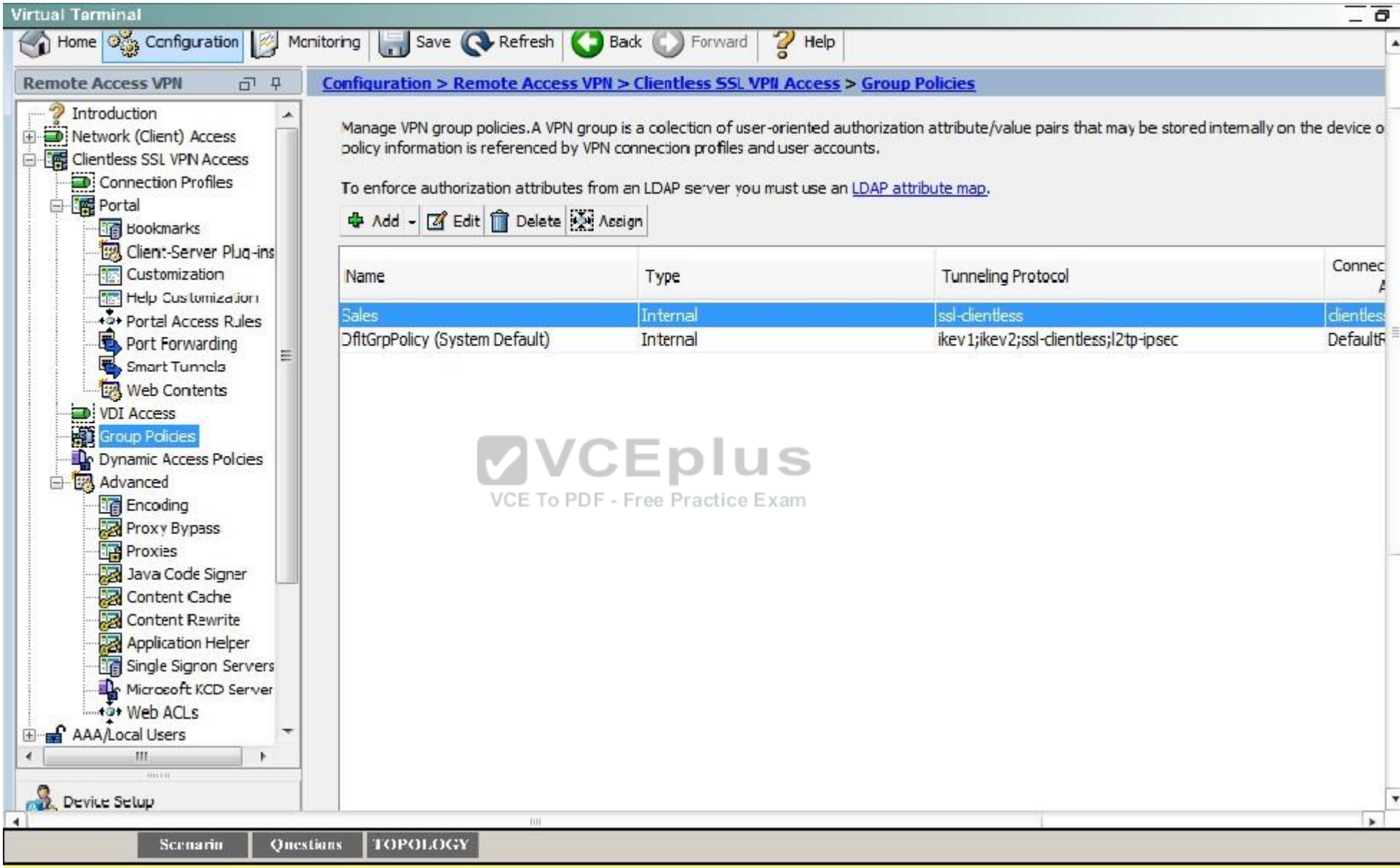


Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

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:

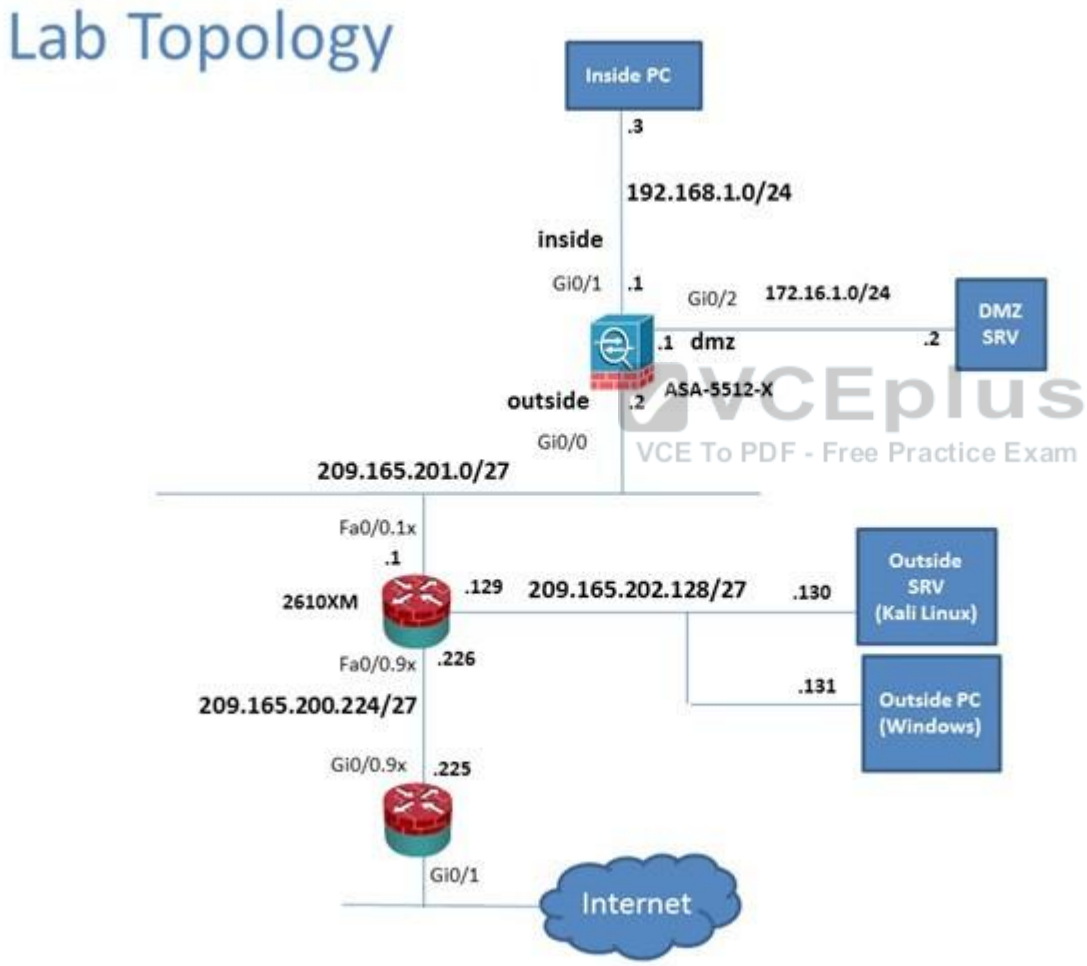


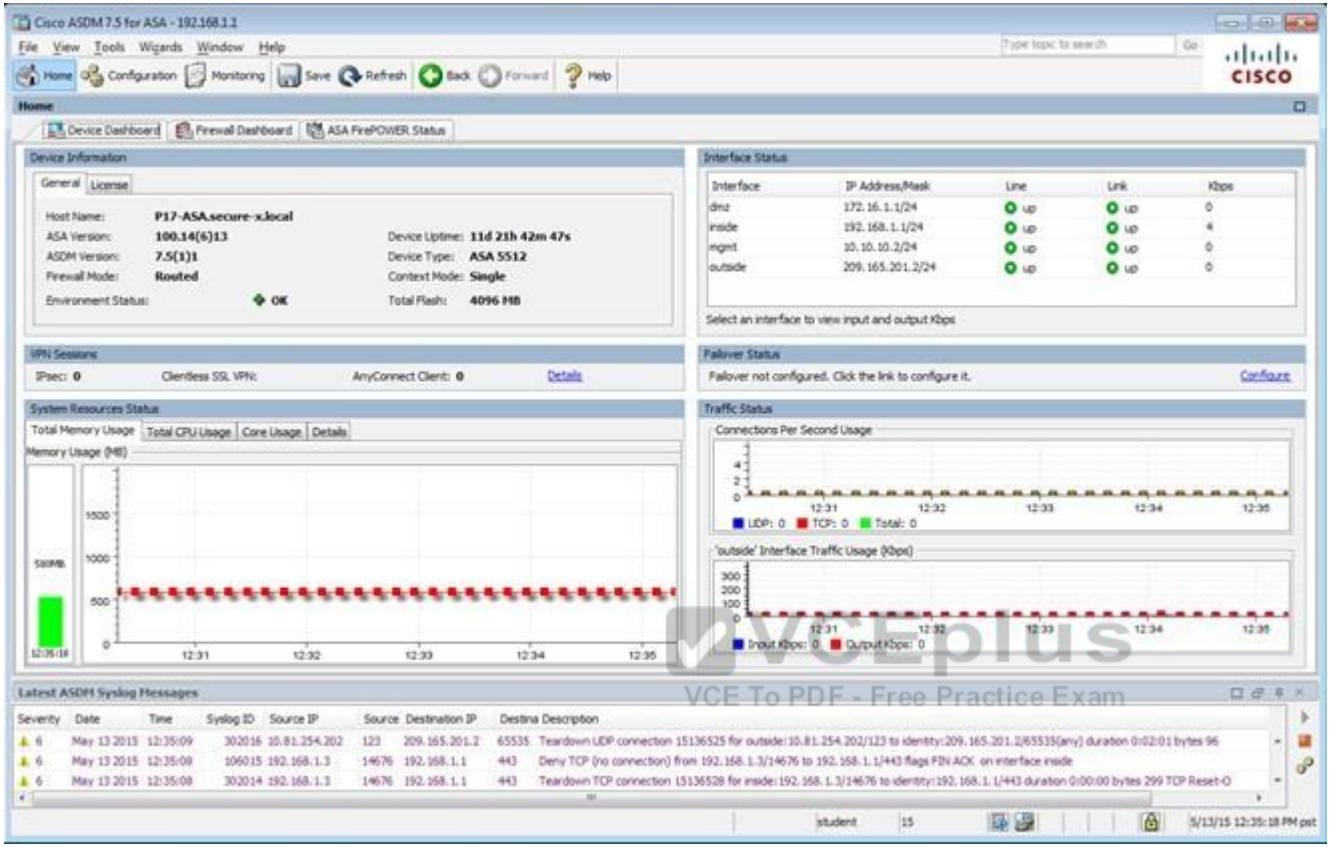
QUESTION 65
Scenario

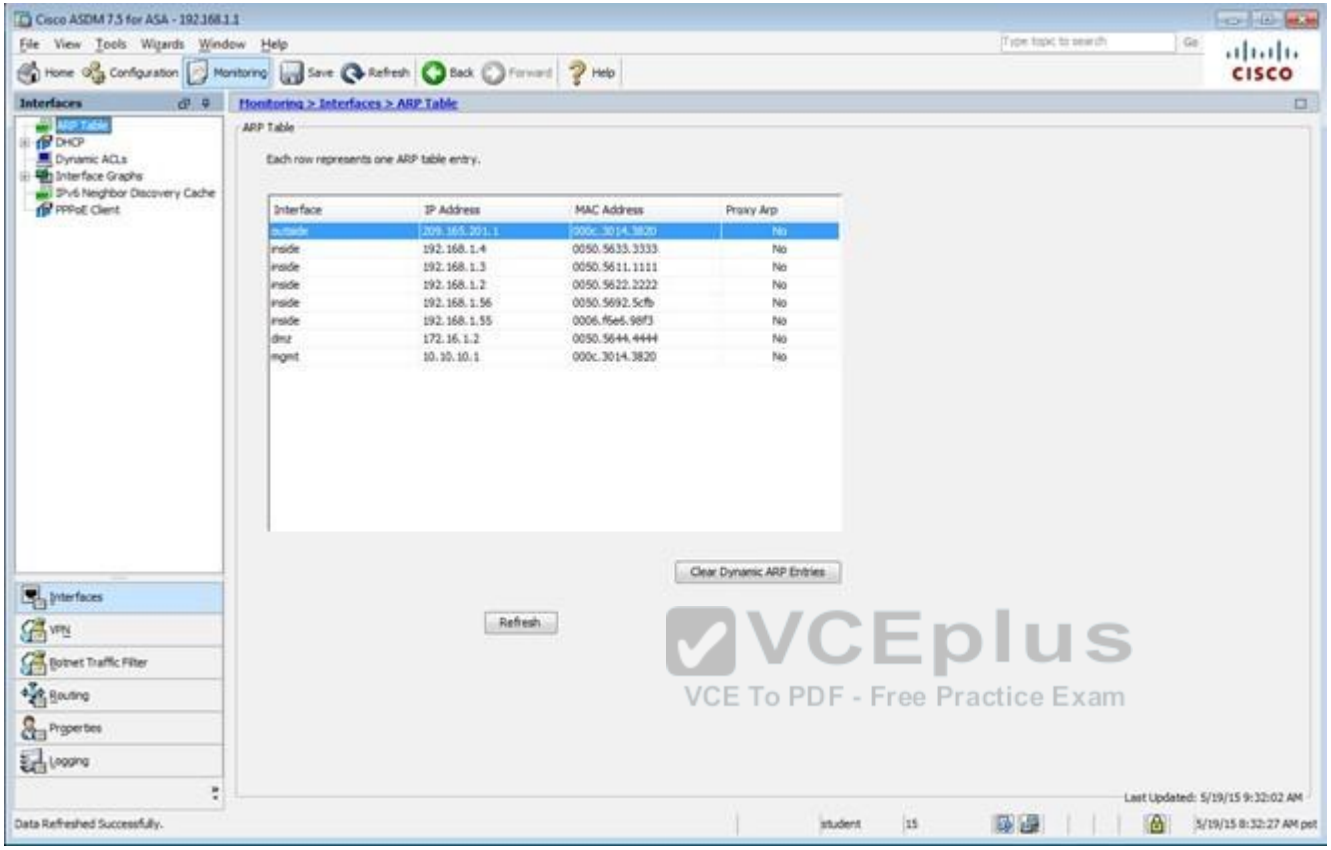
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

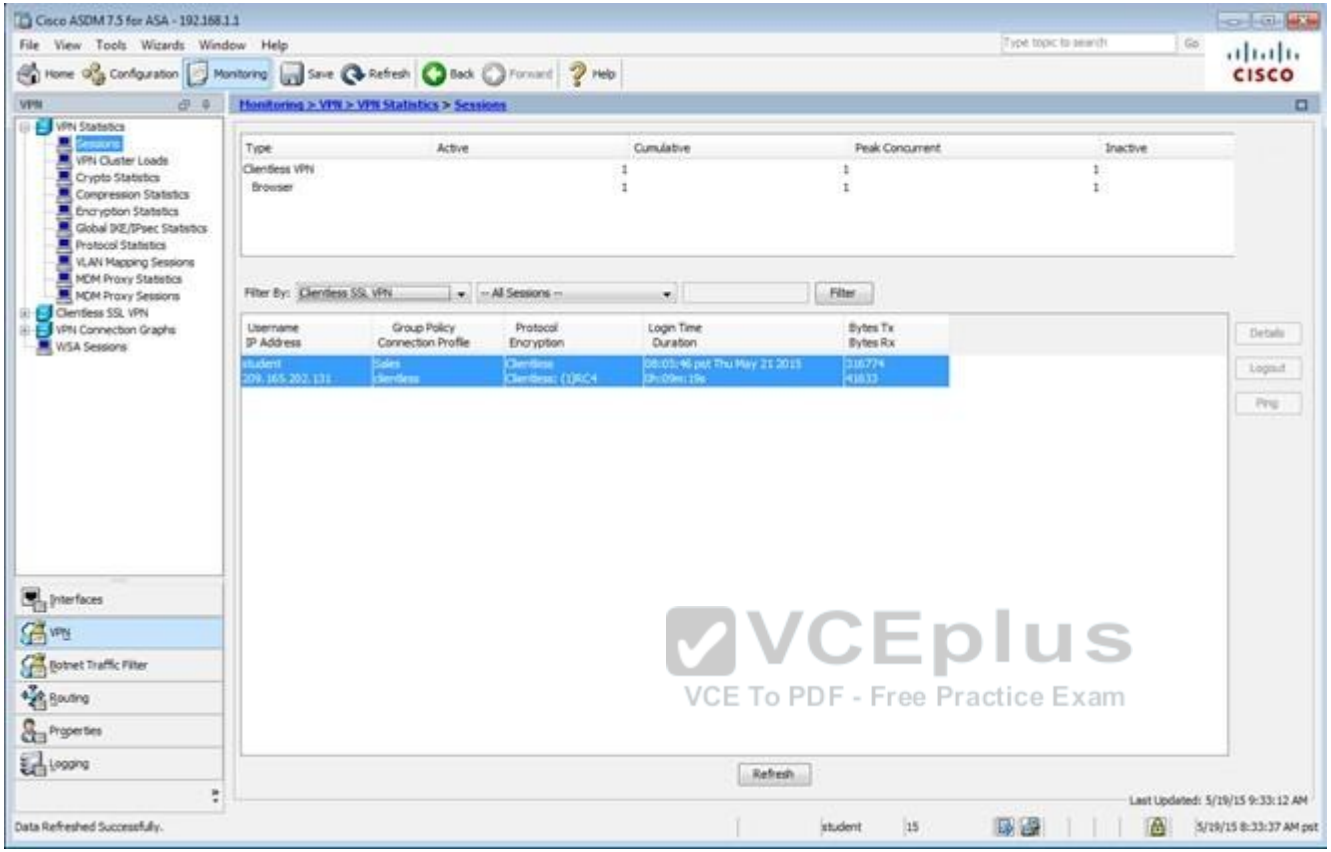
To access ASDM, click the ASA icon in the topology diagram.

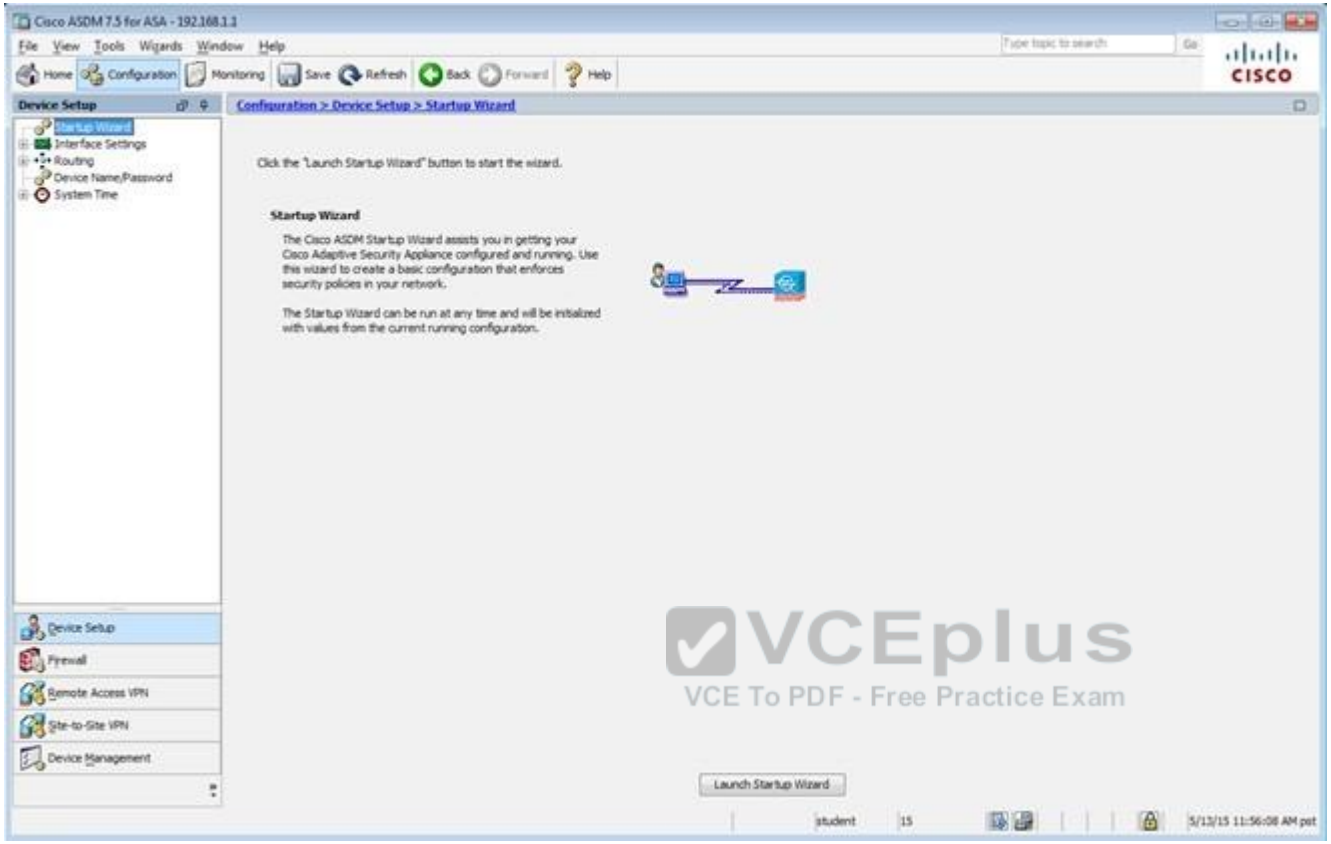
Note: Not all ASDM functionalities are enabled in this simulation. To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

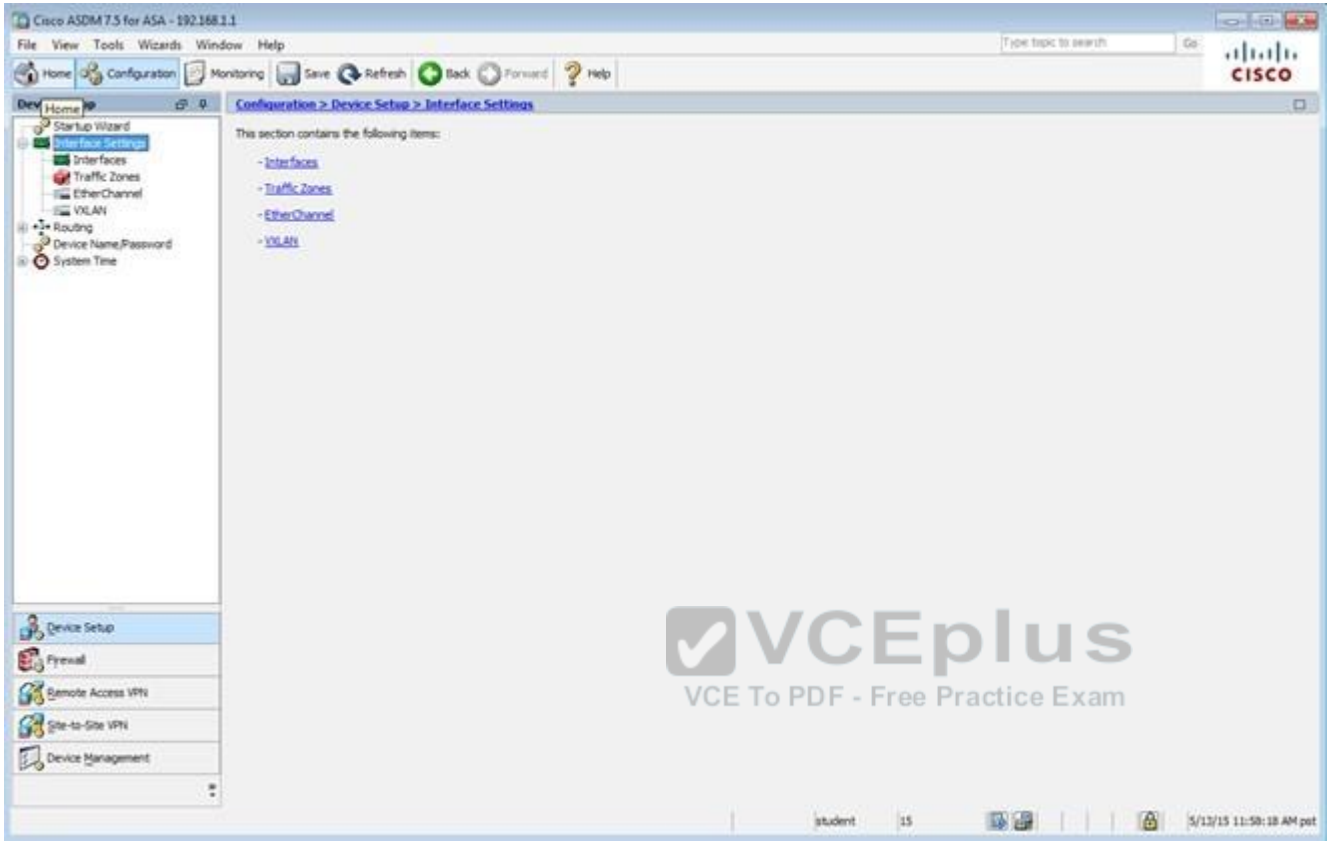


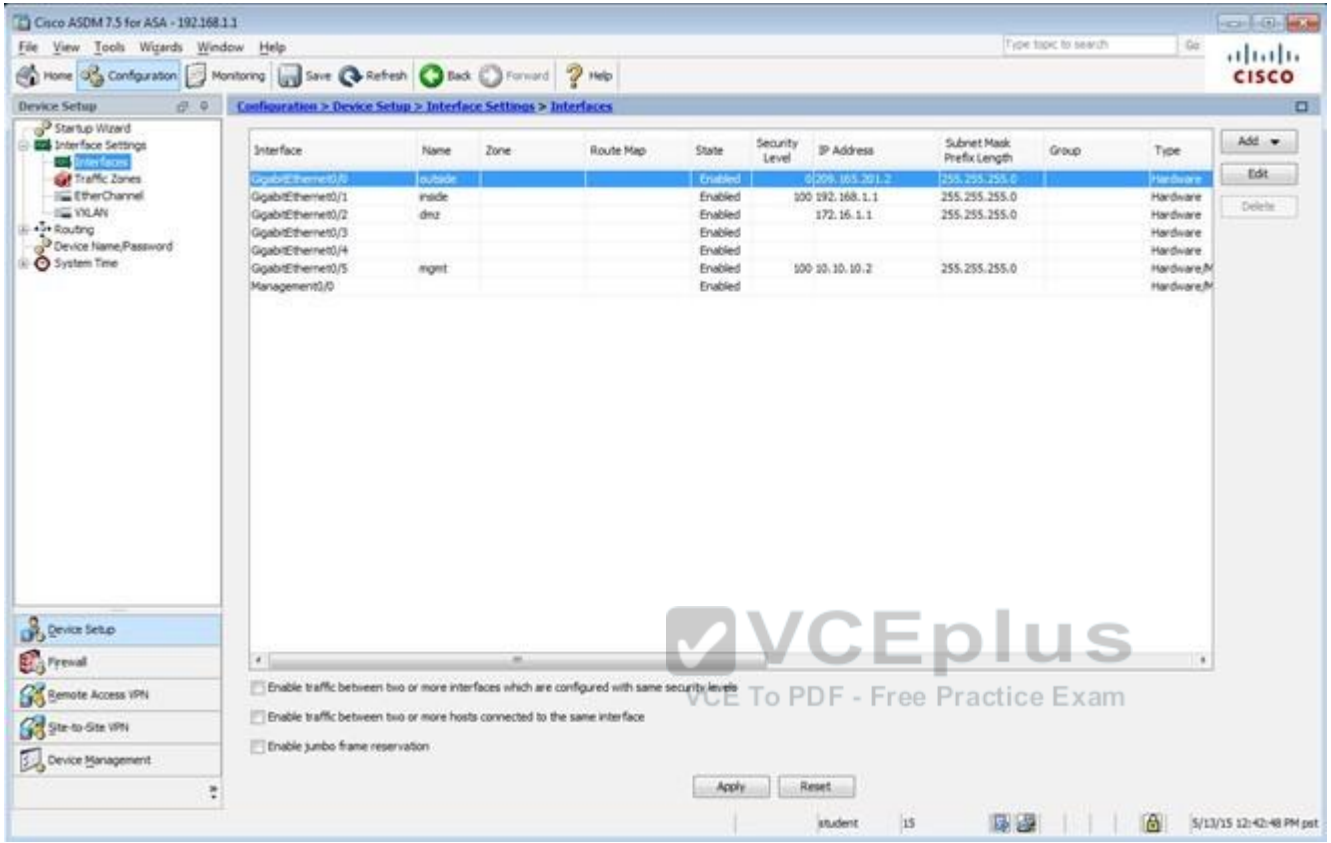


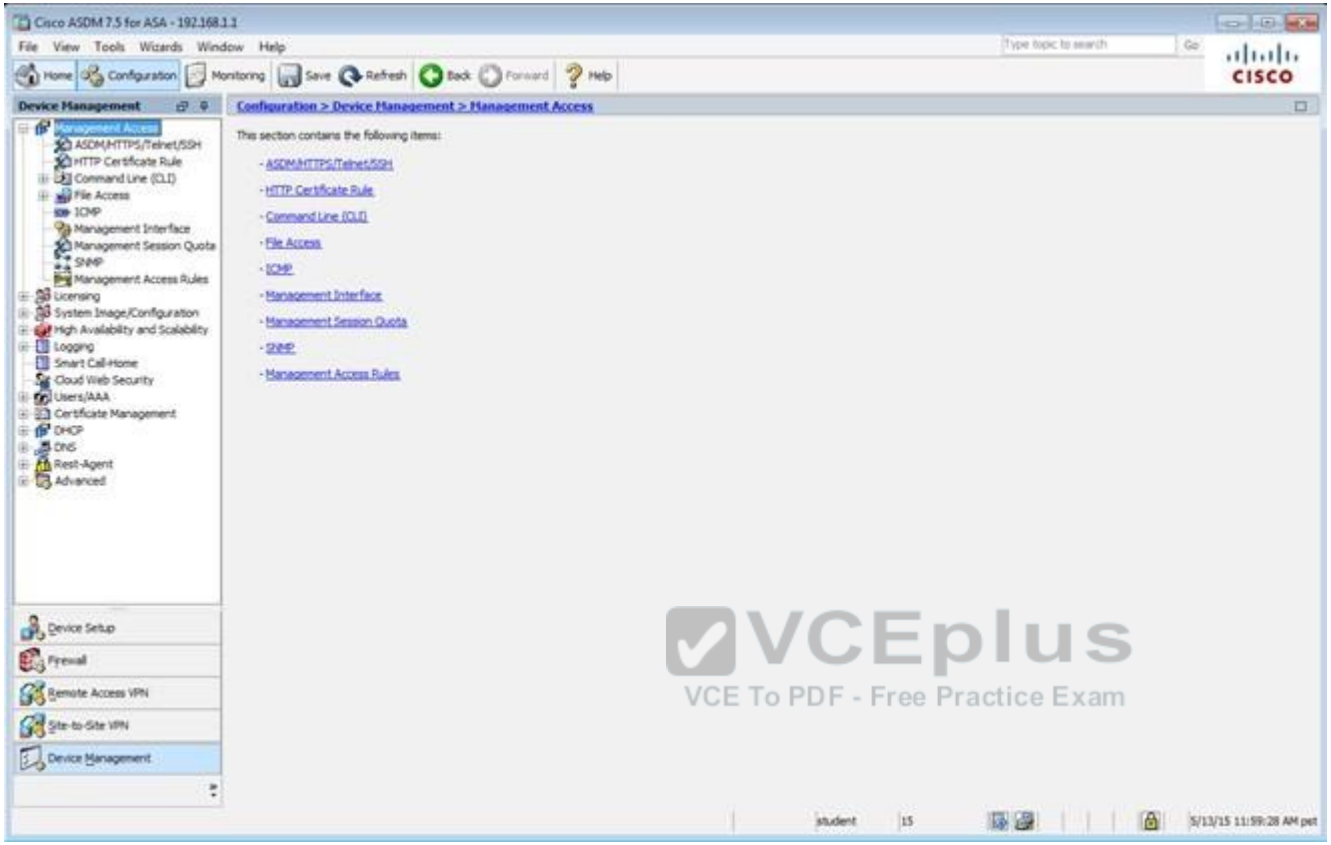


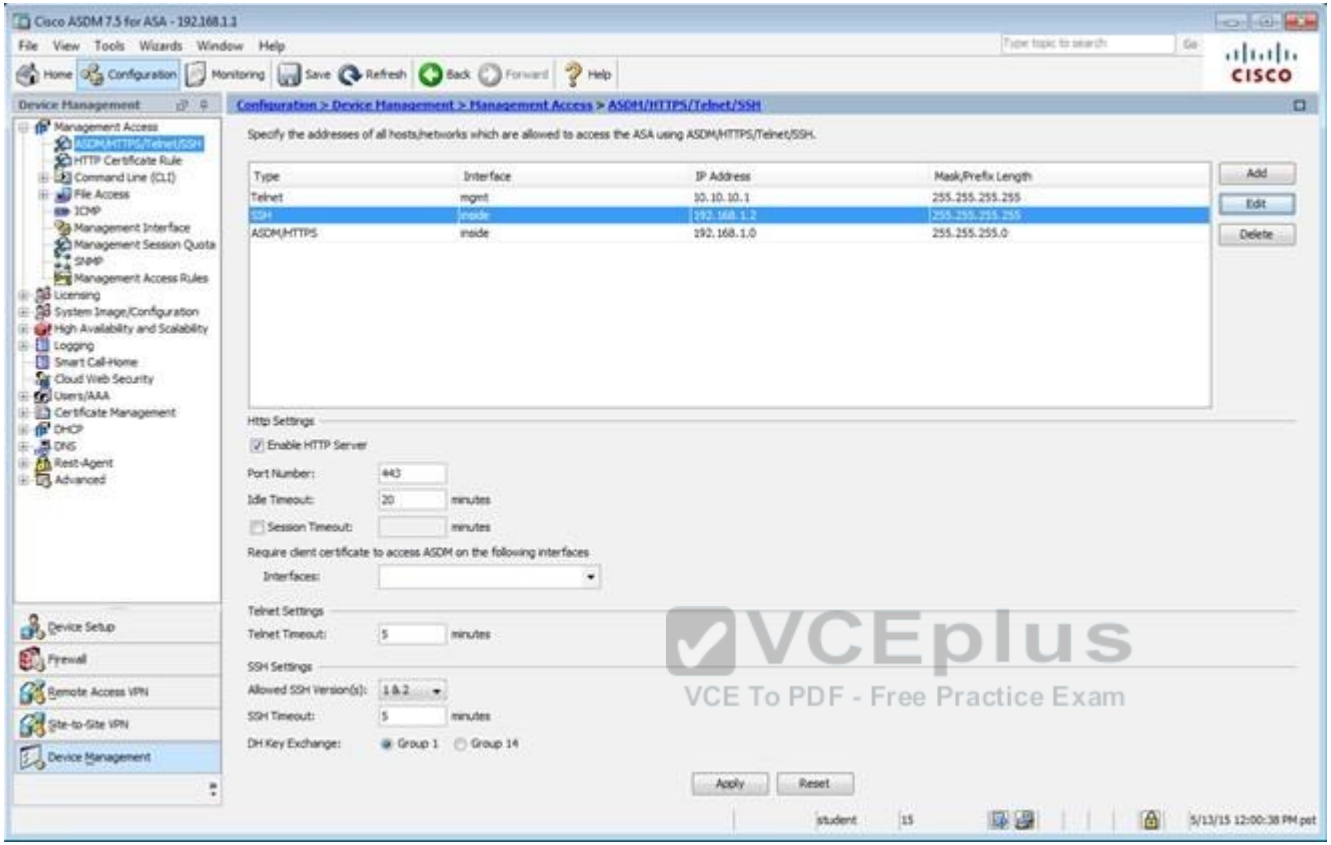


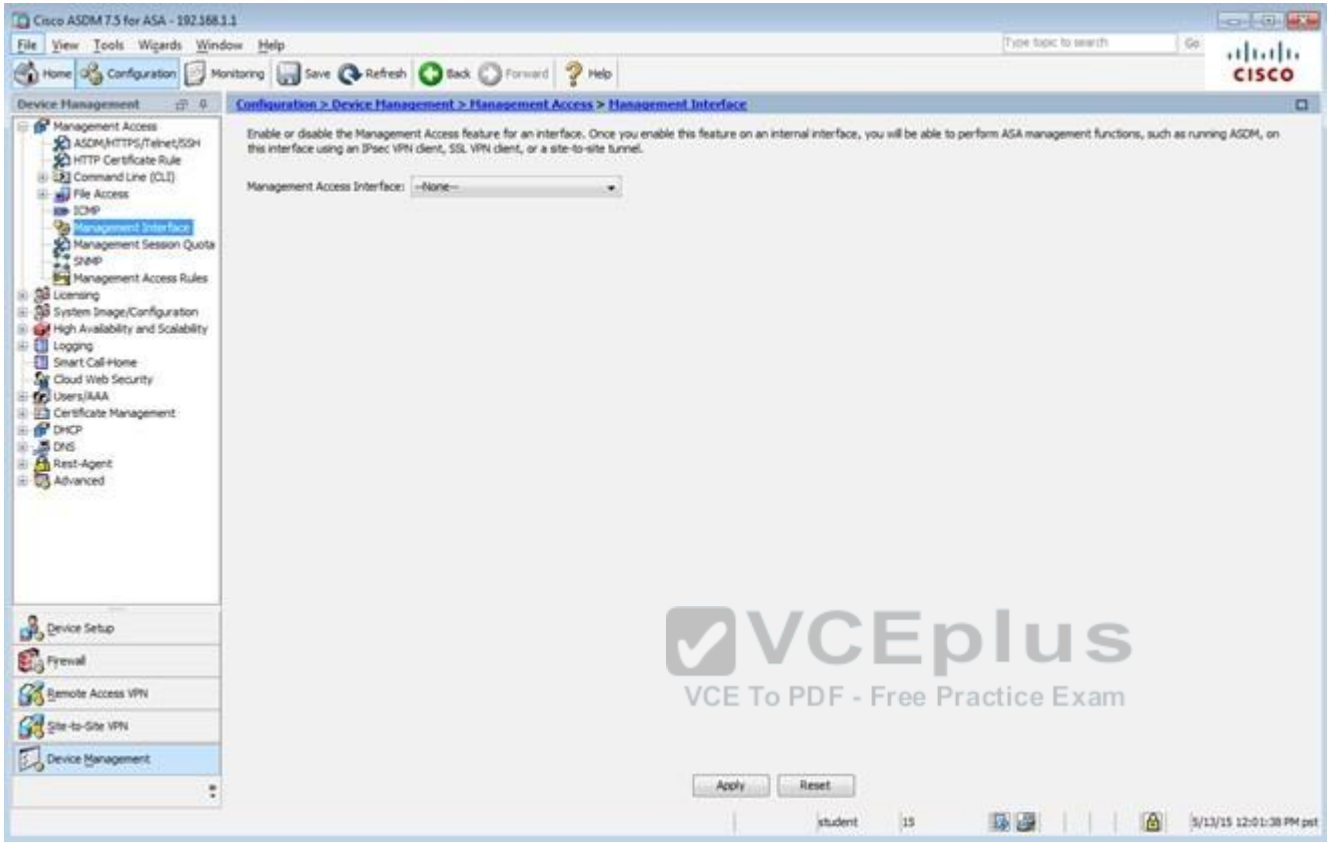


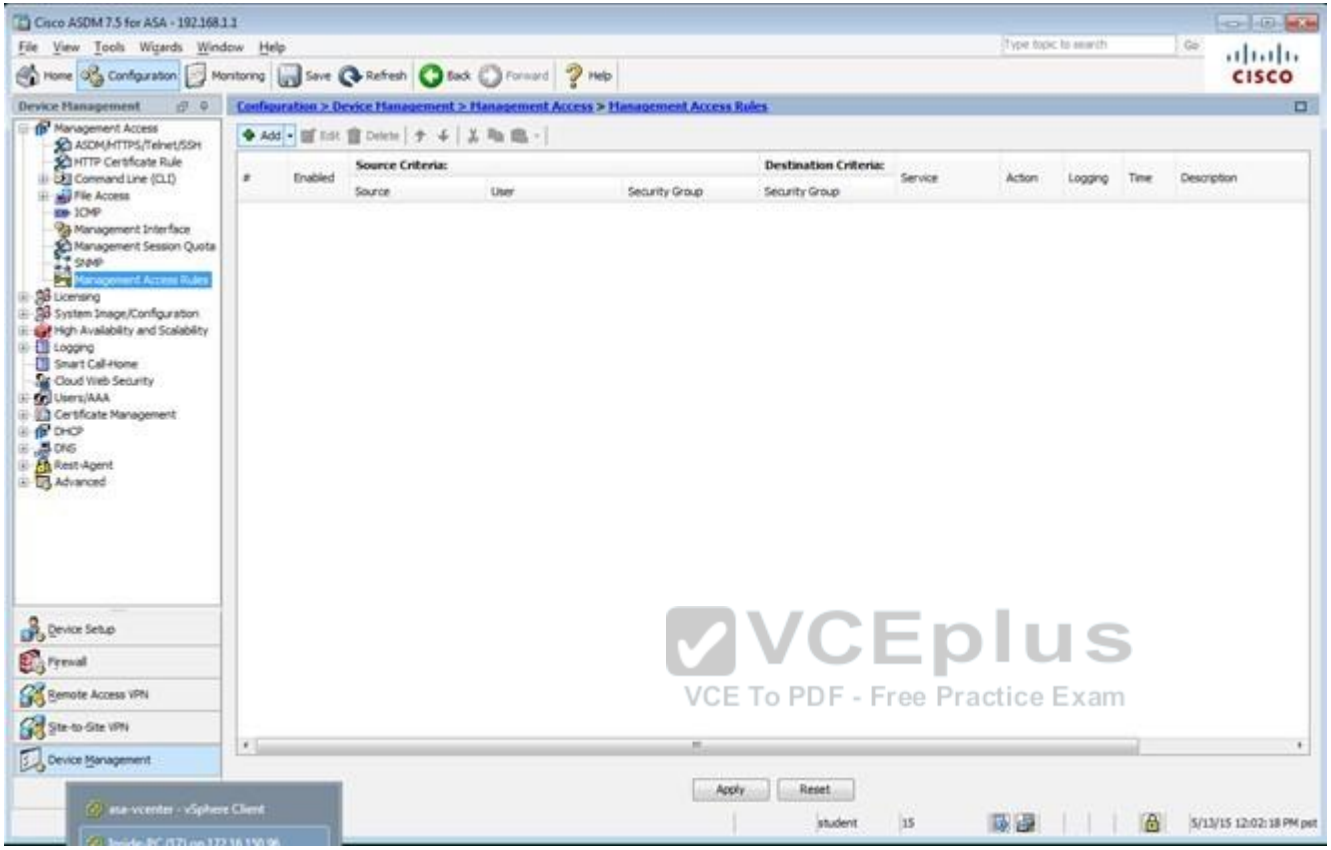


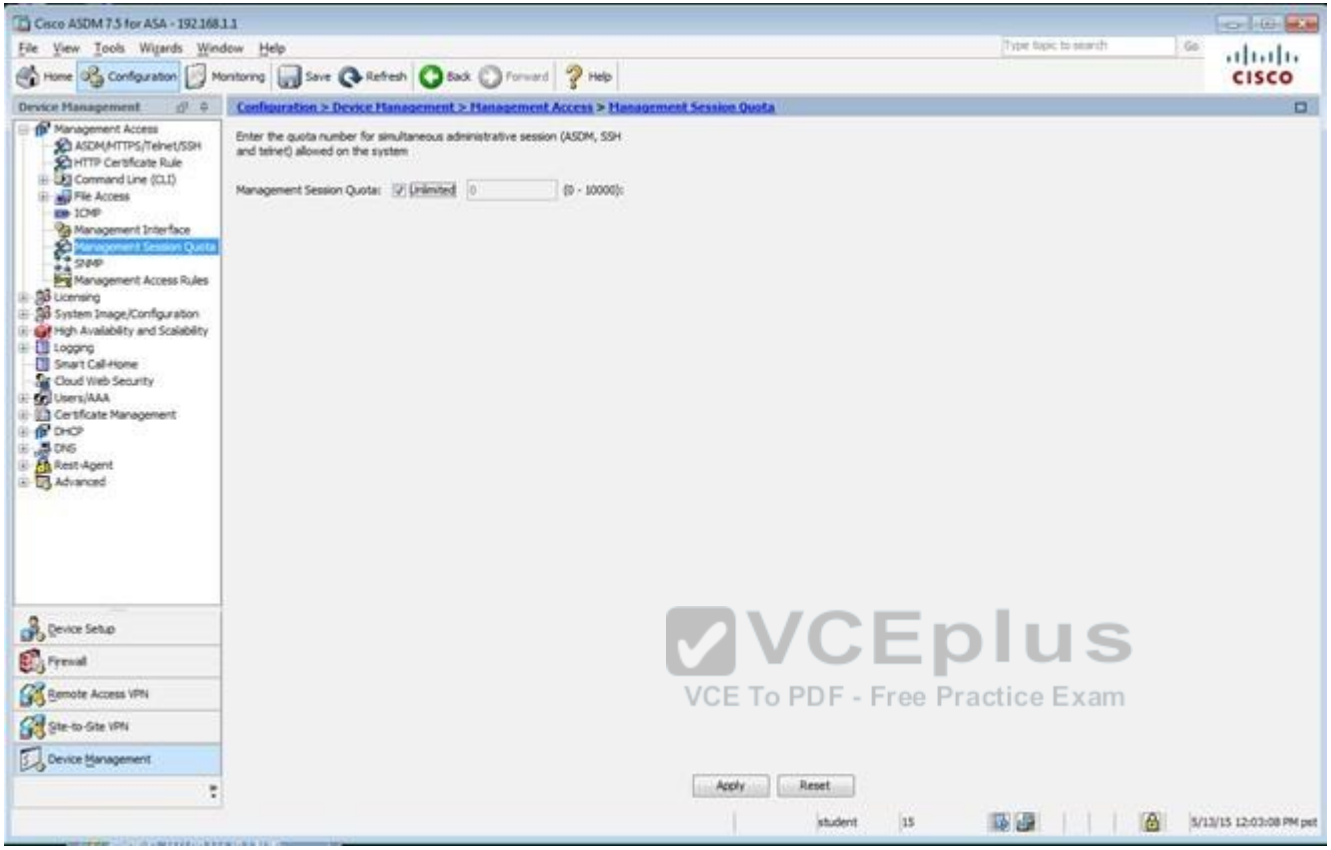


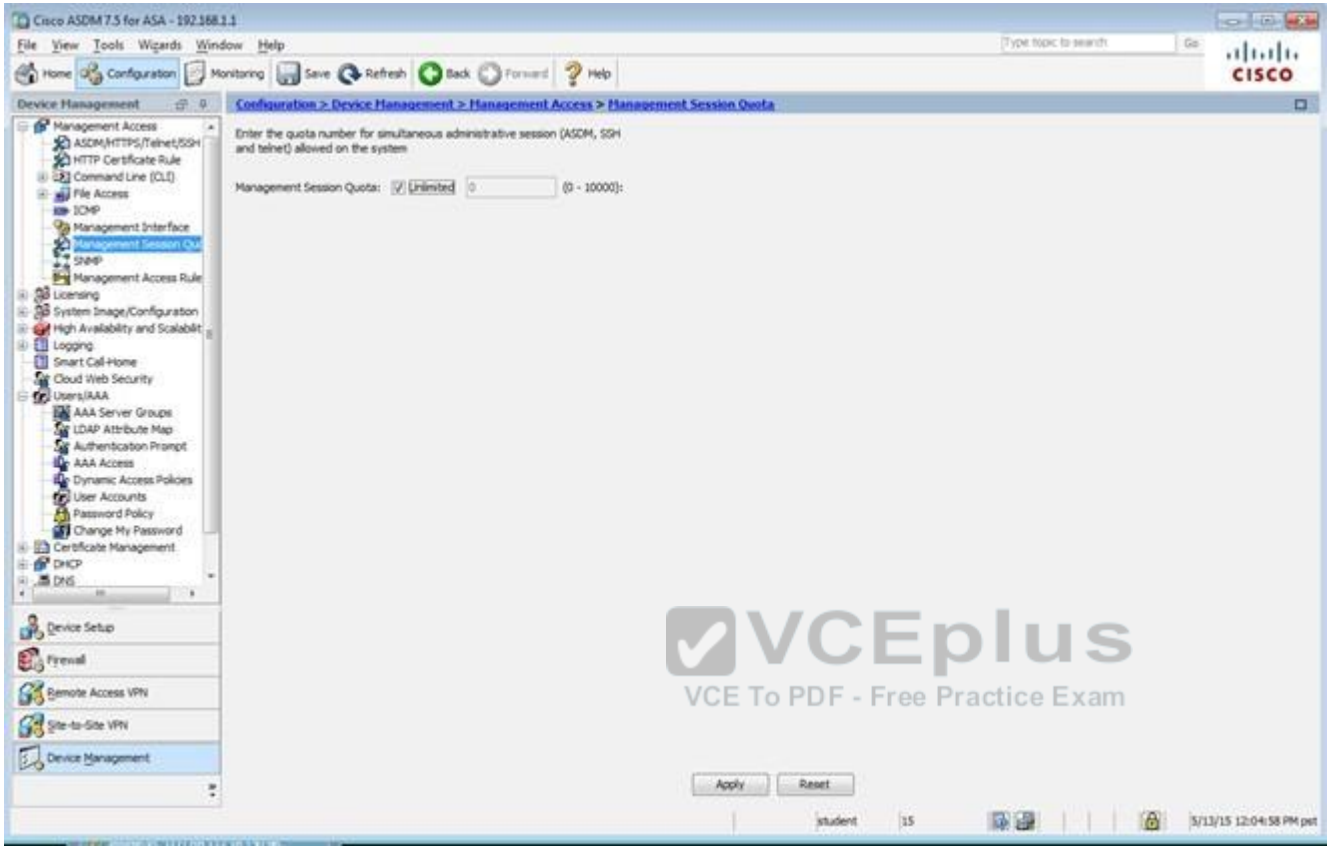


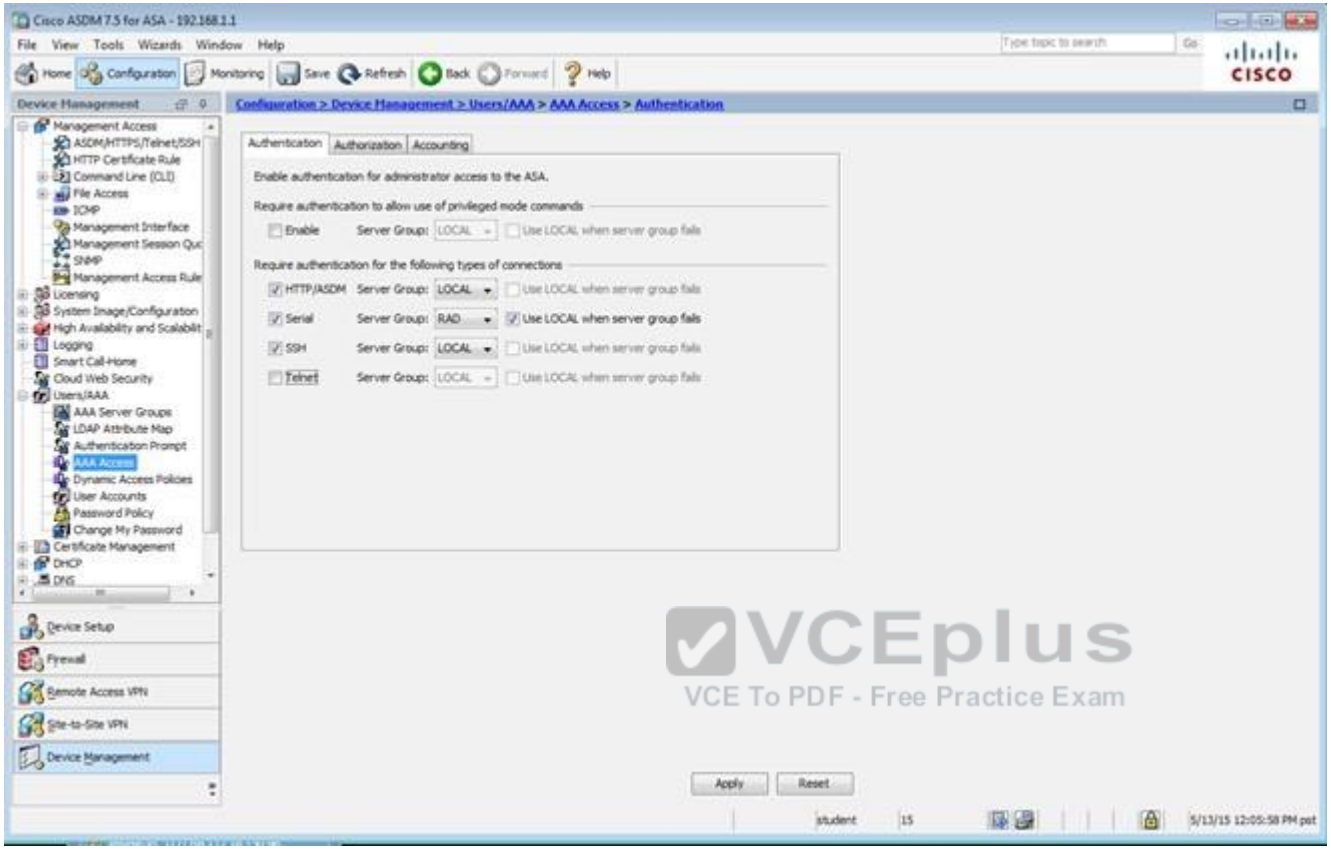


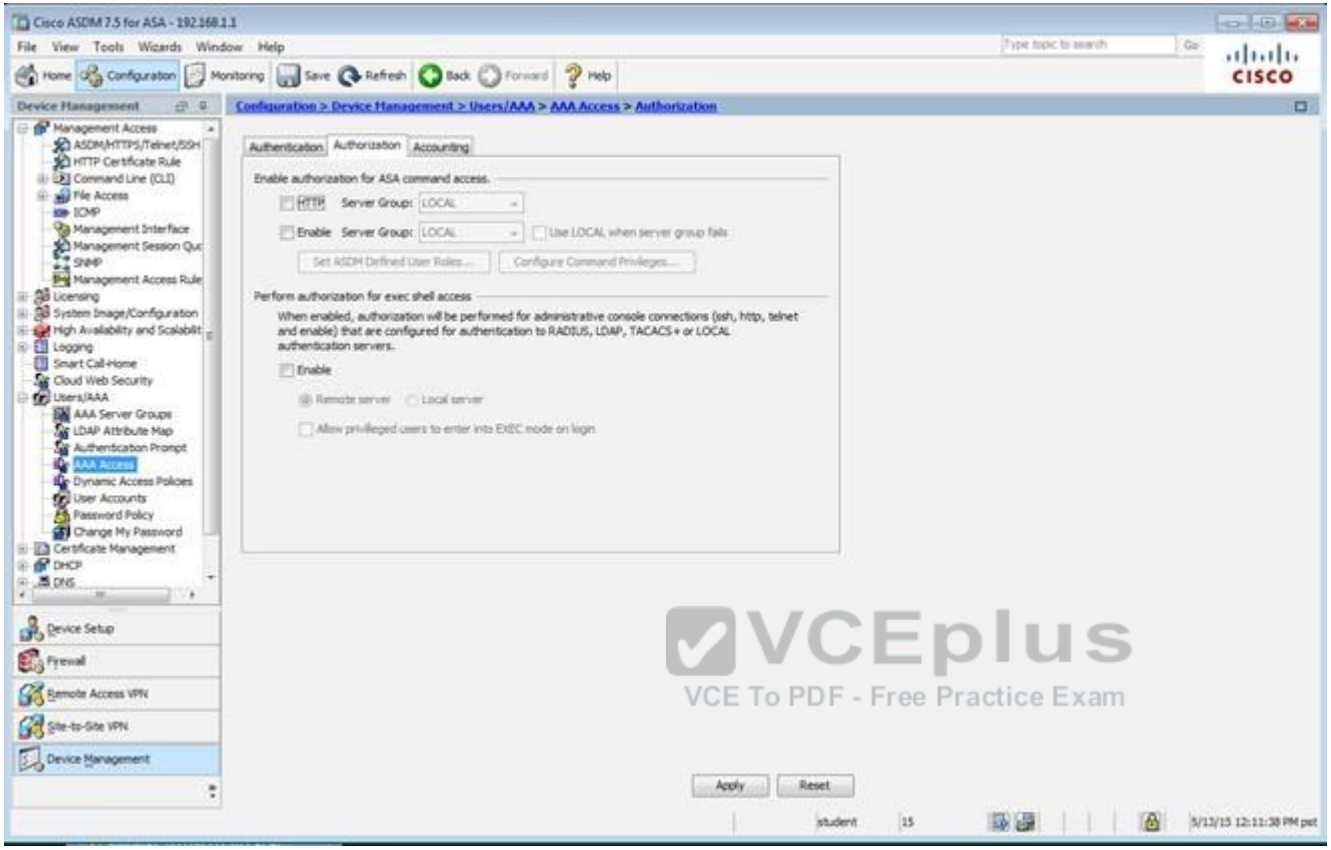


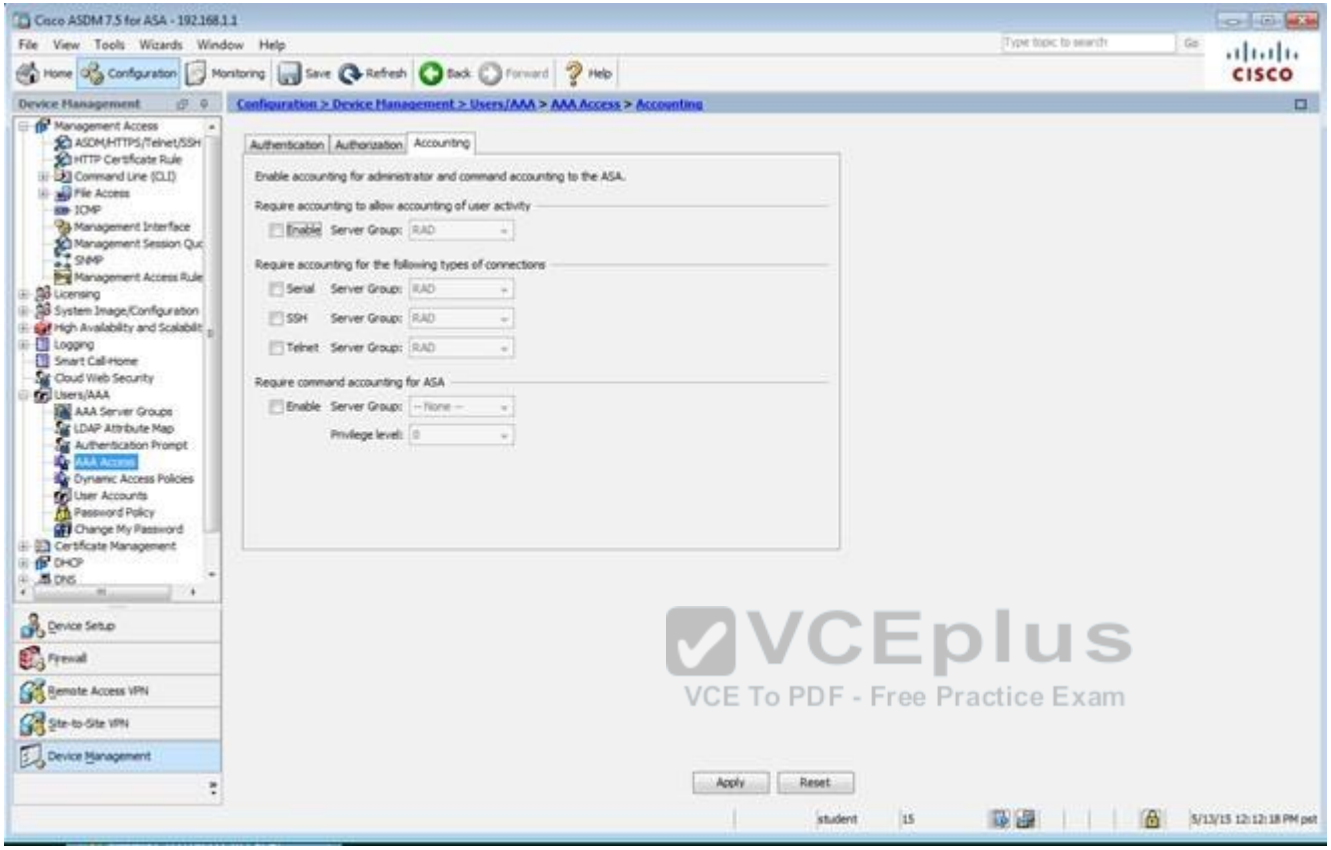


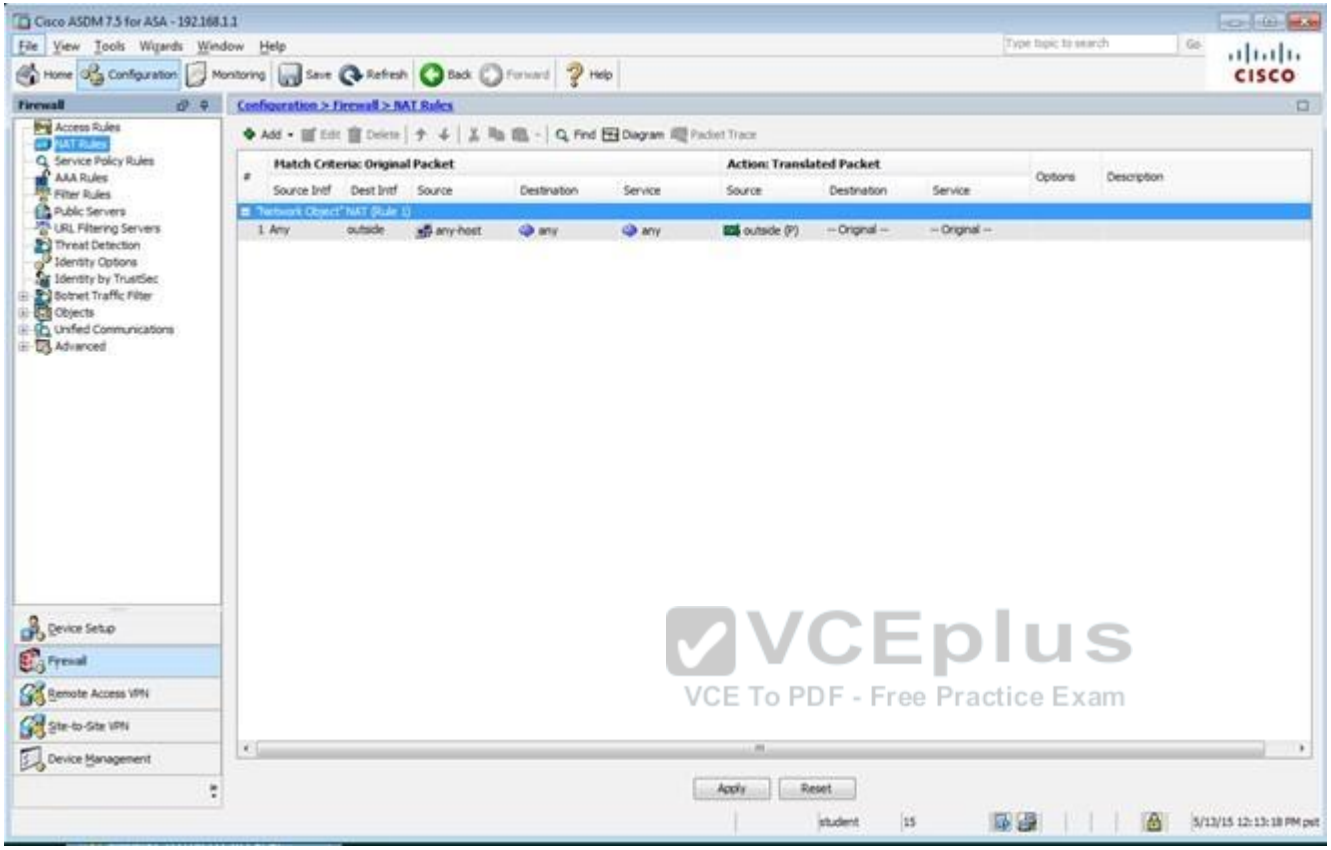


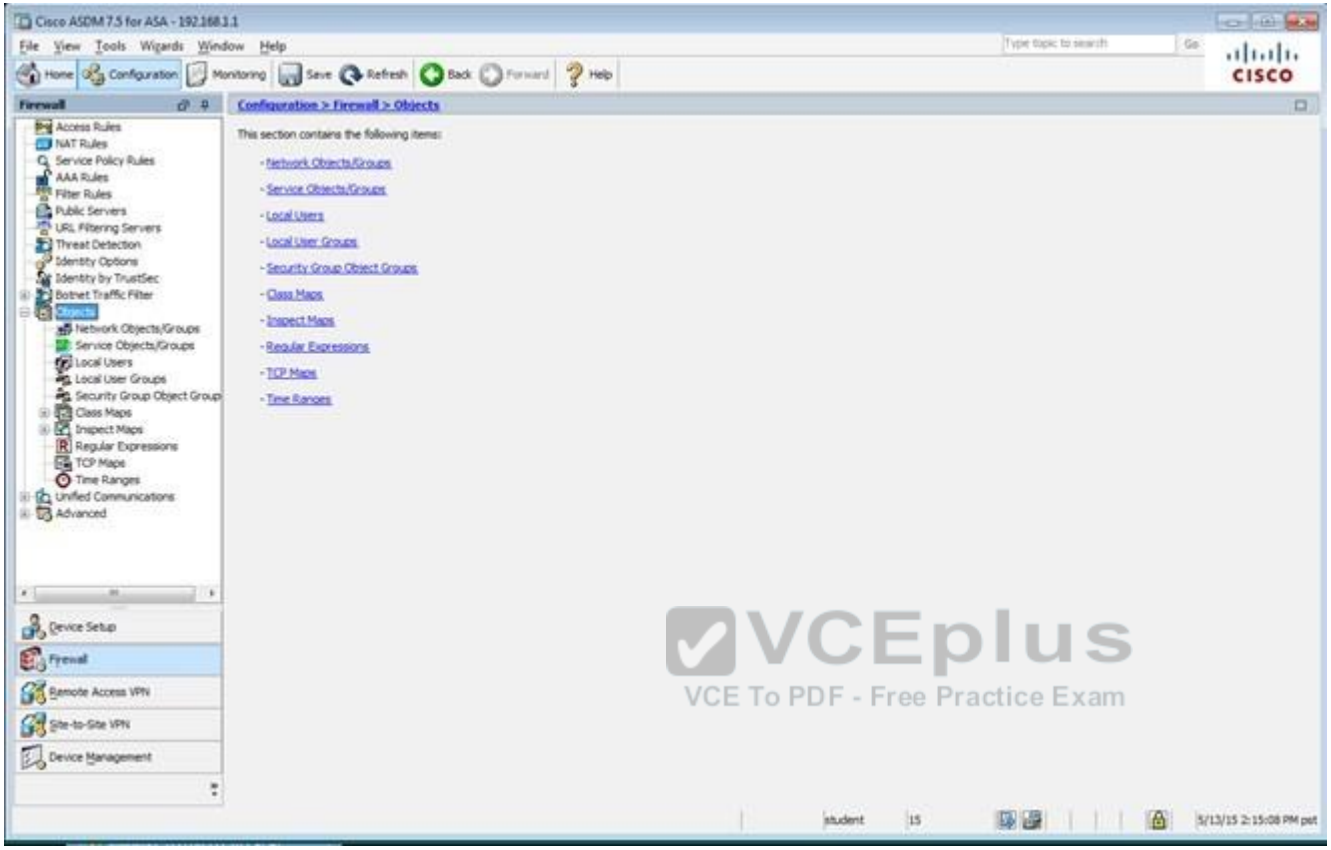


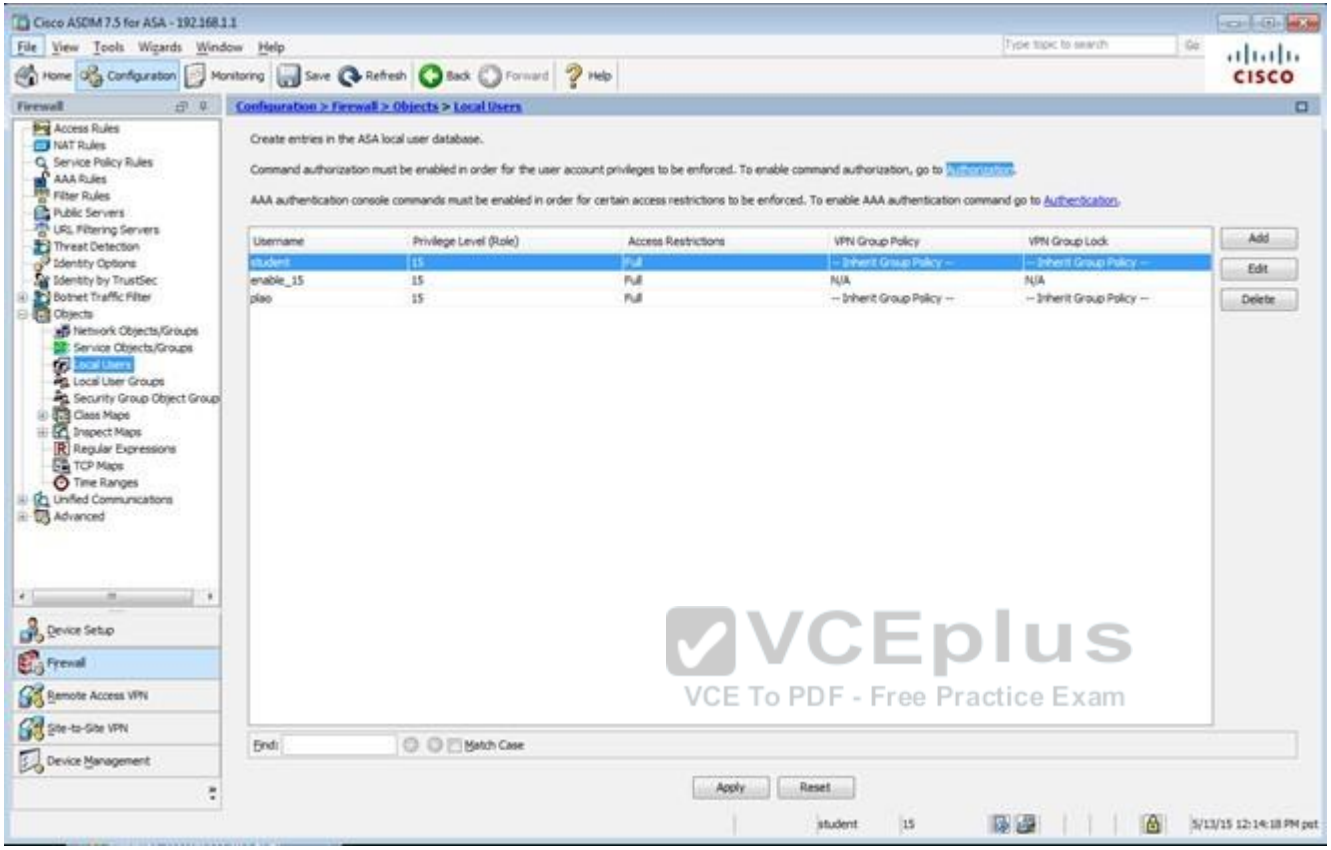


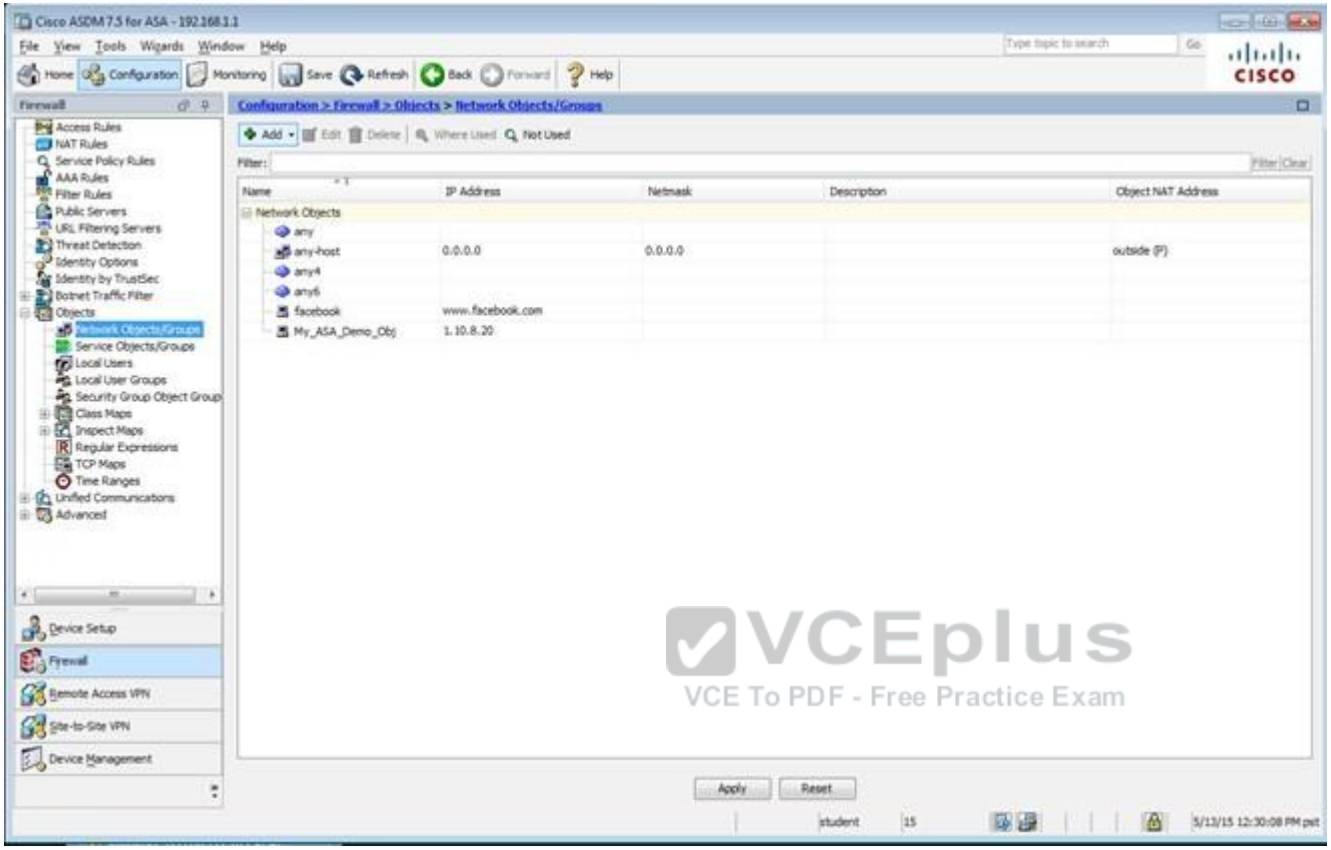


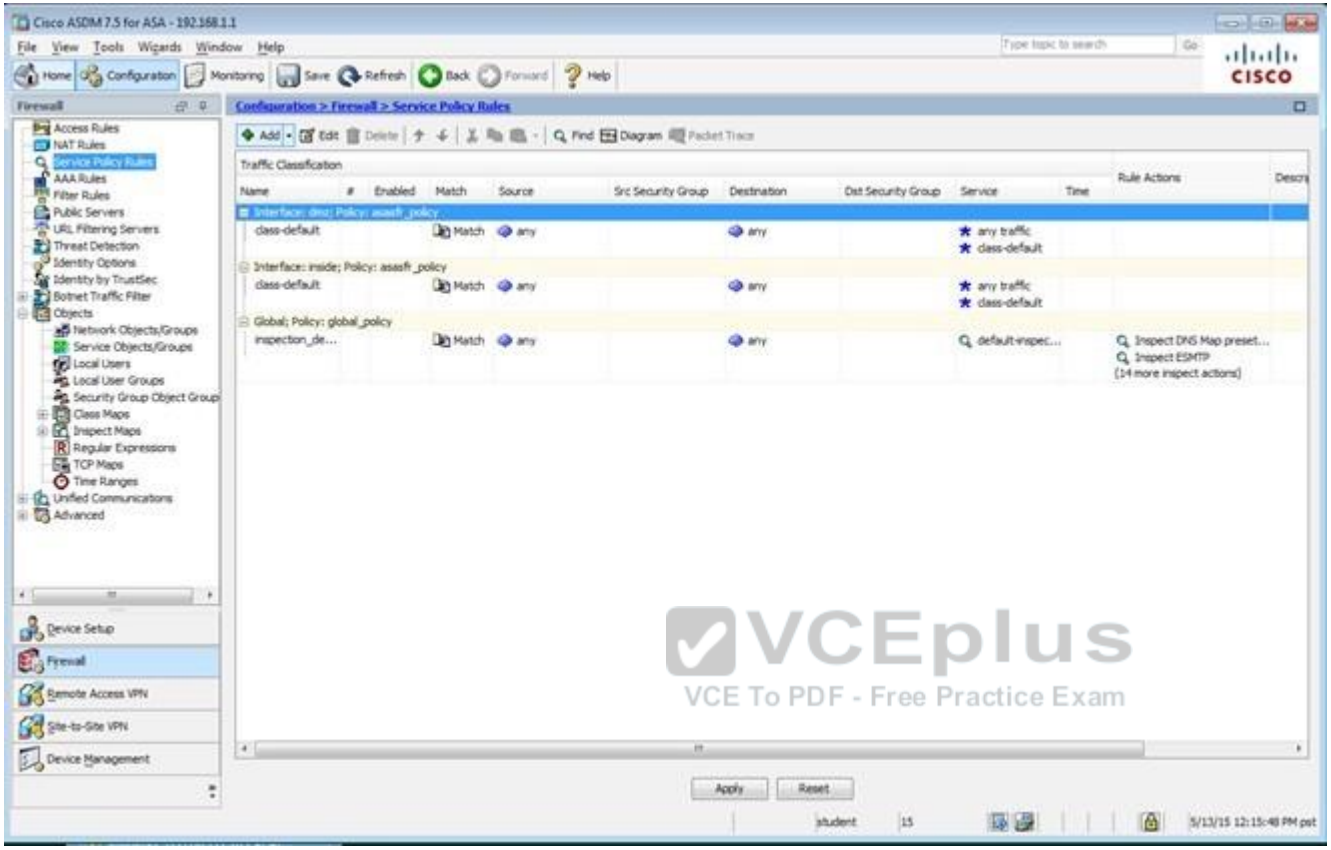


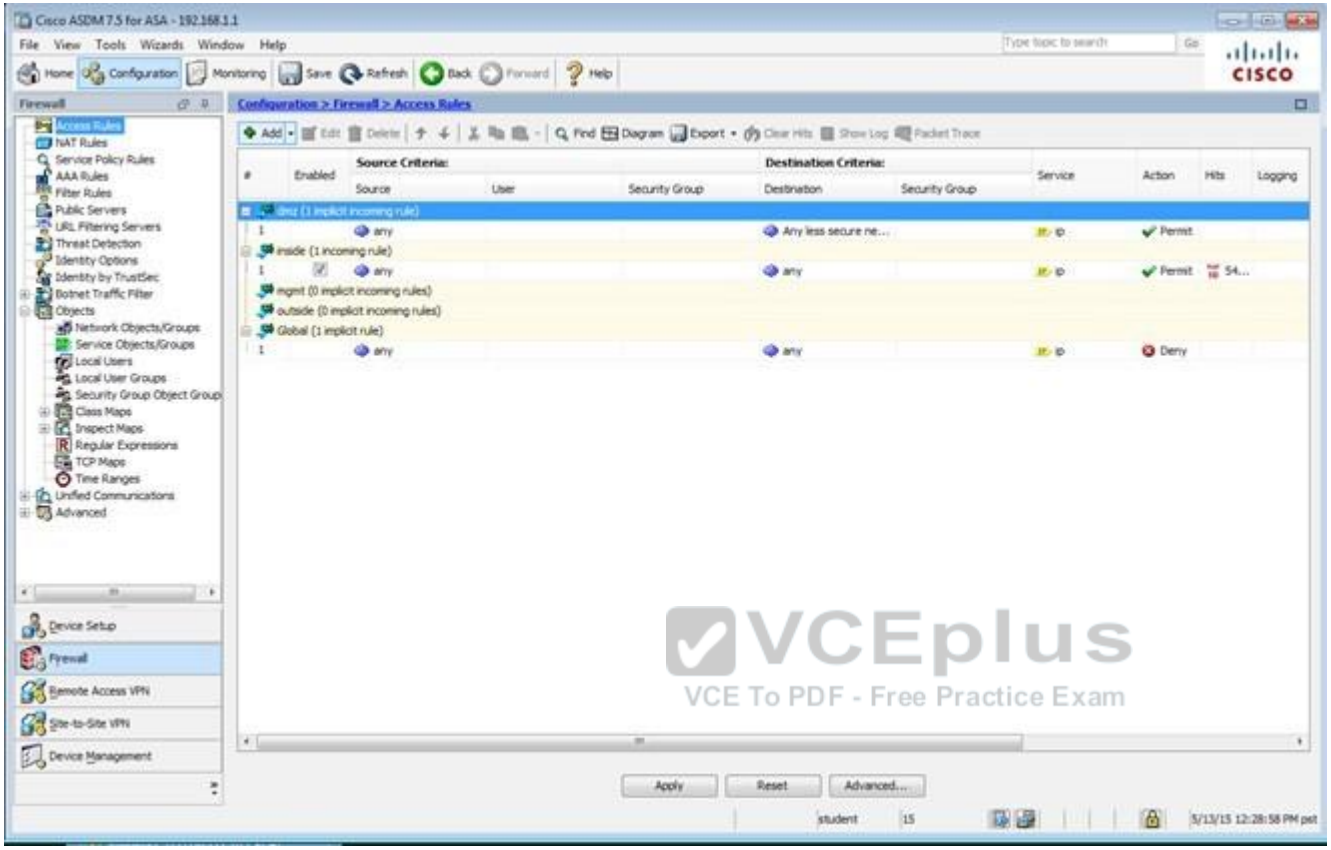


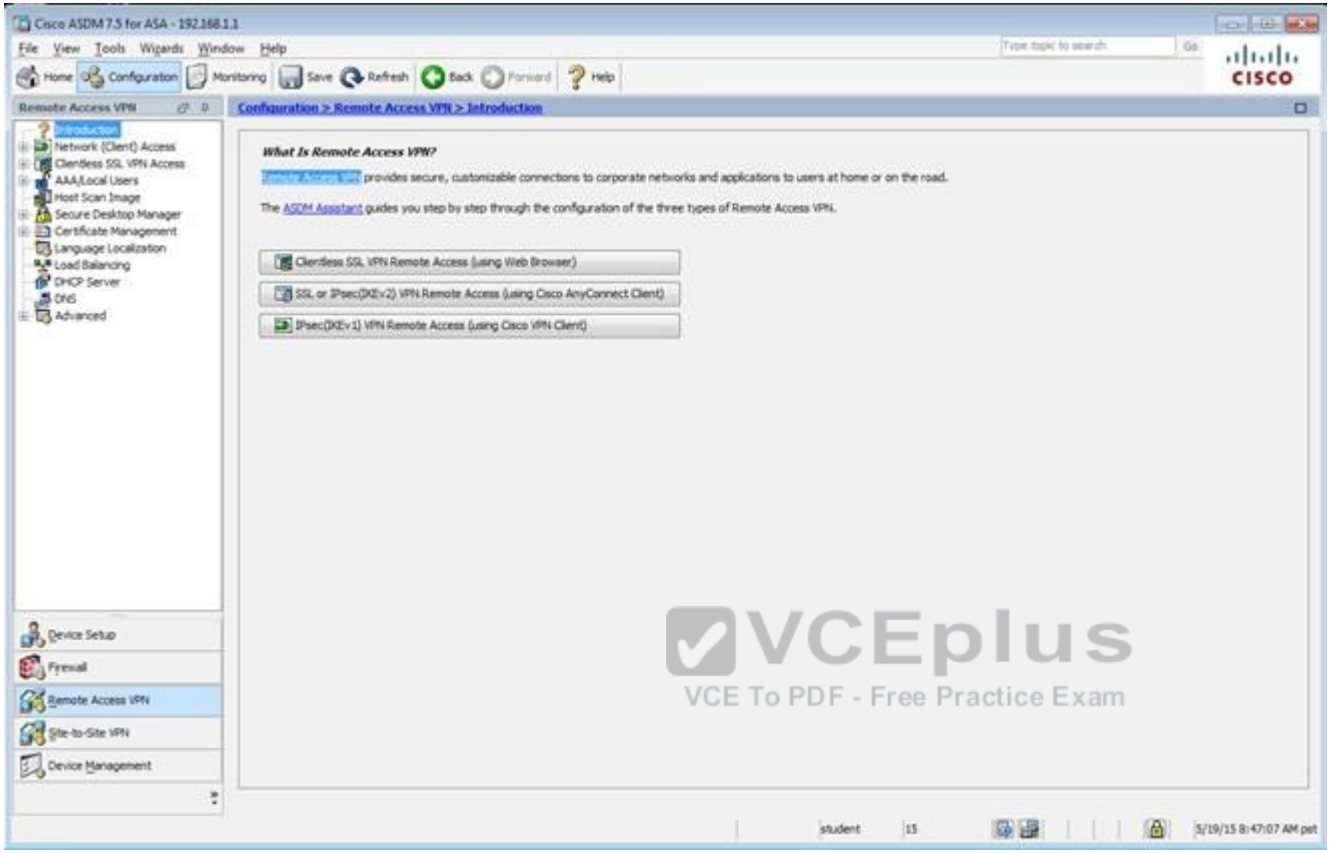


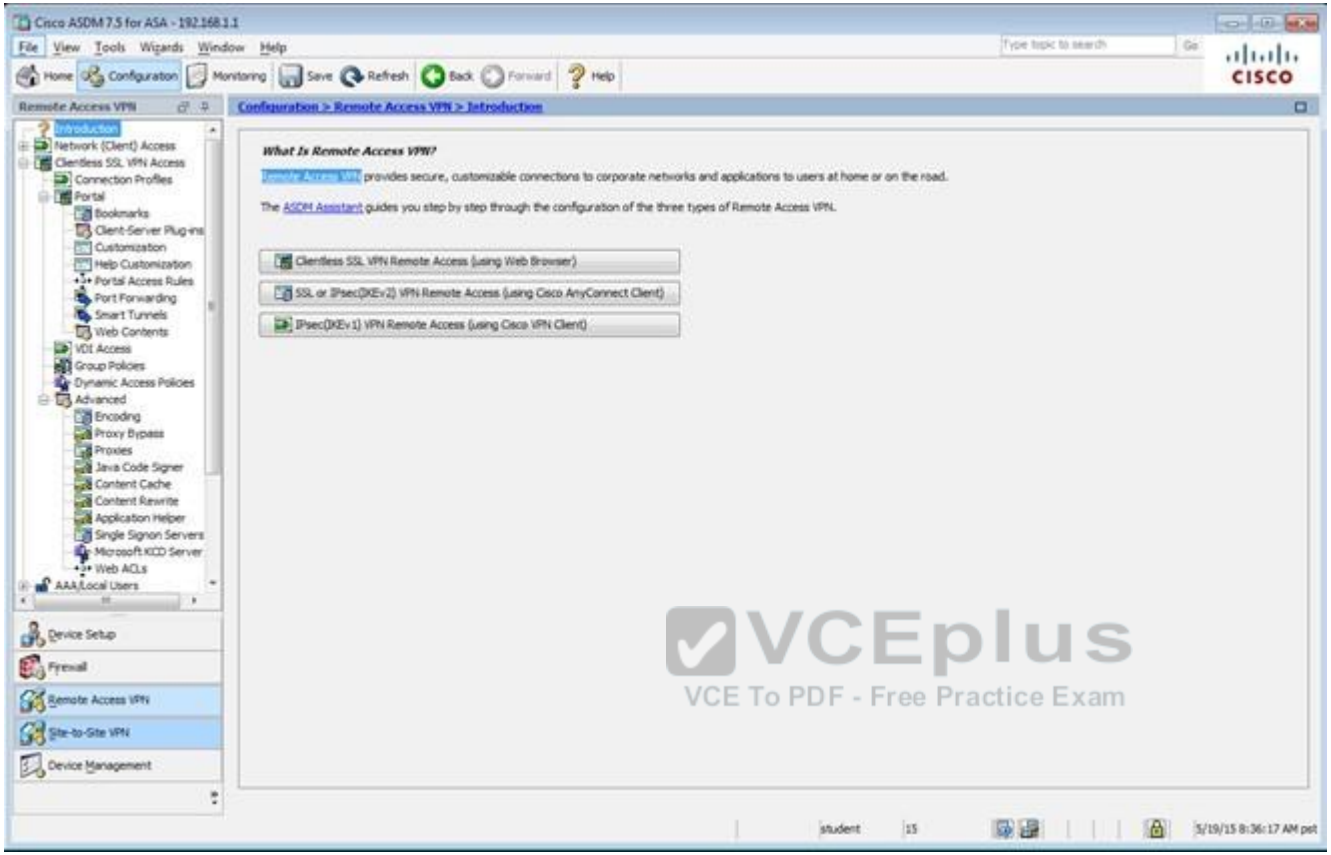


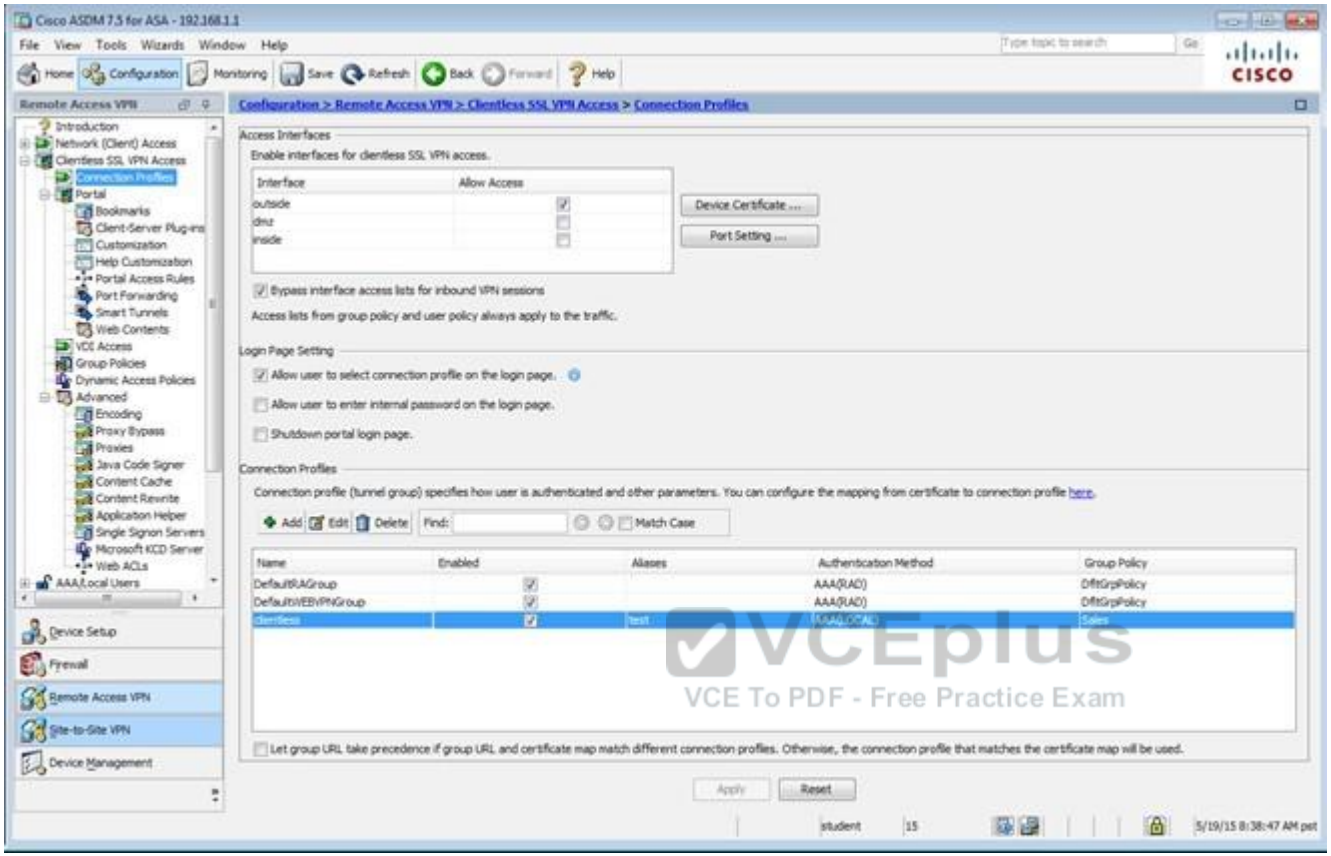


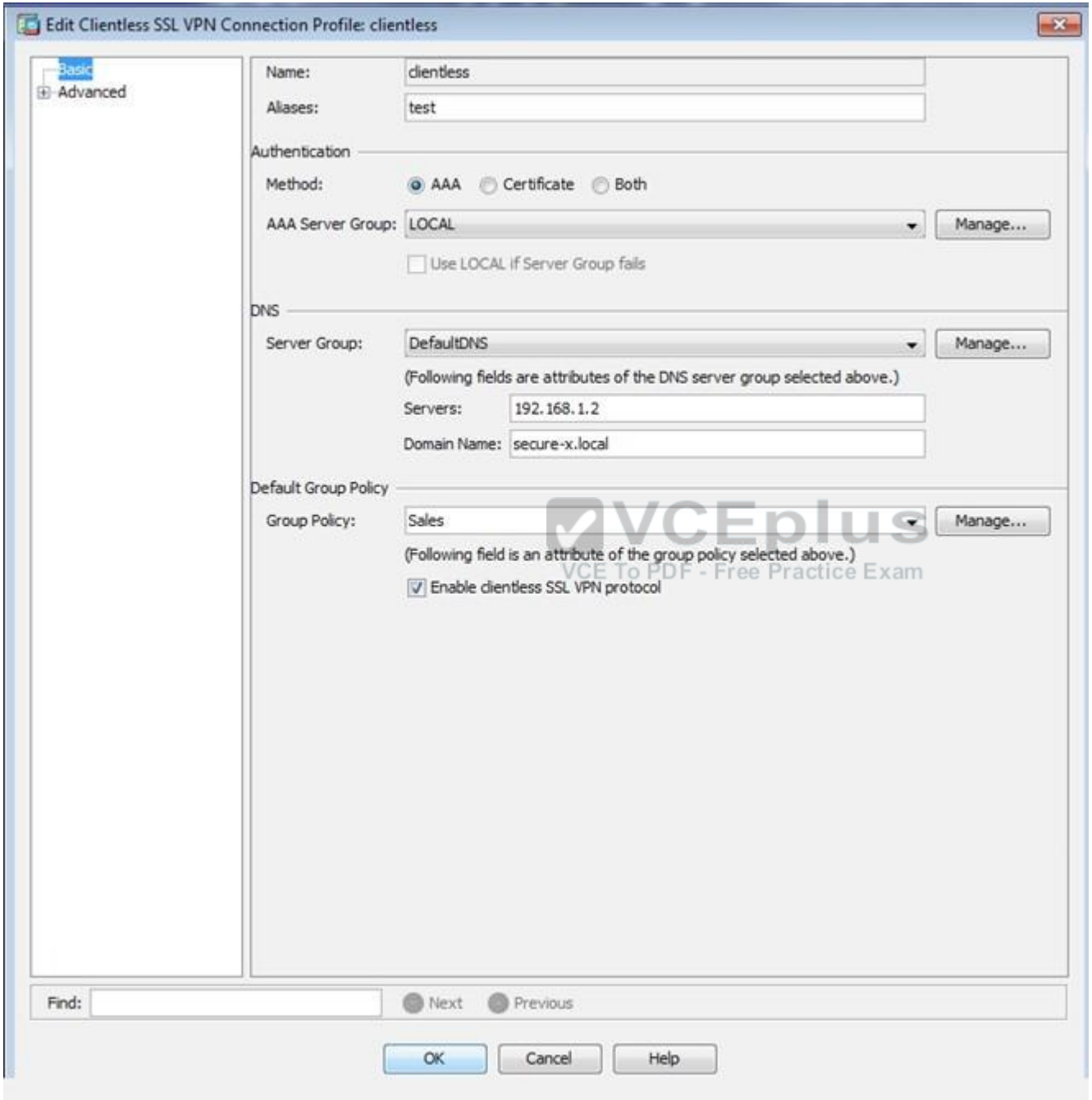


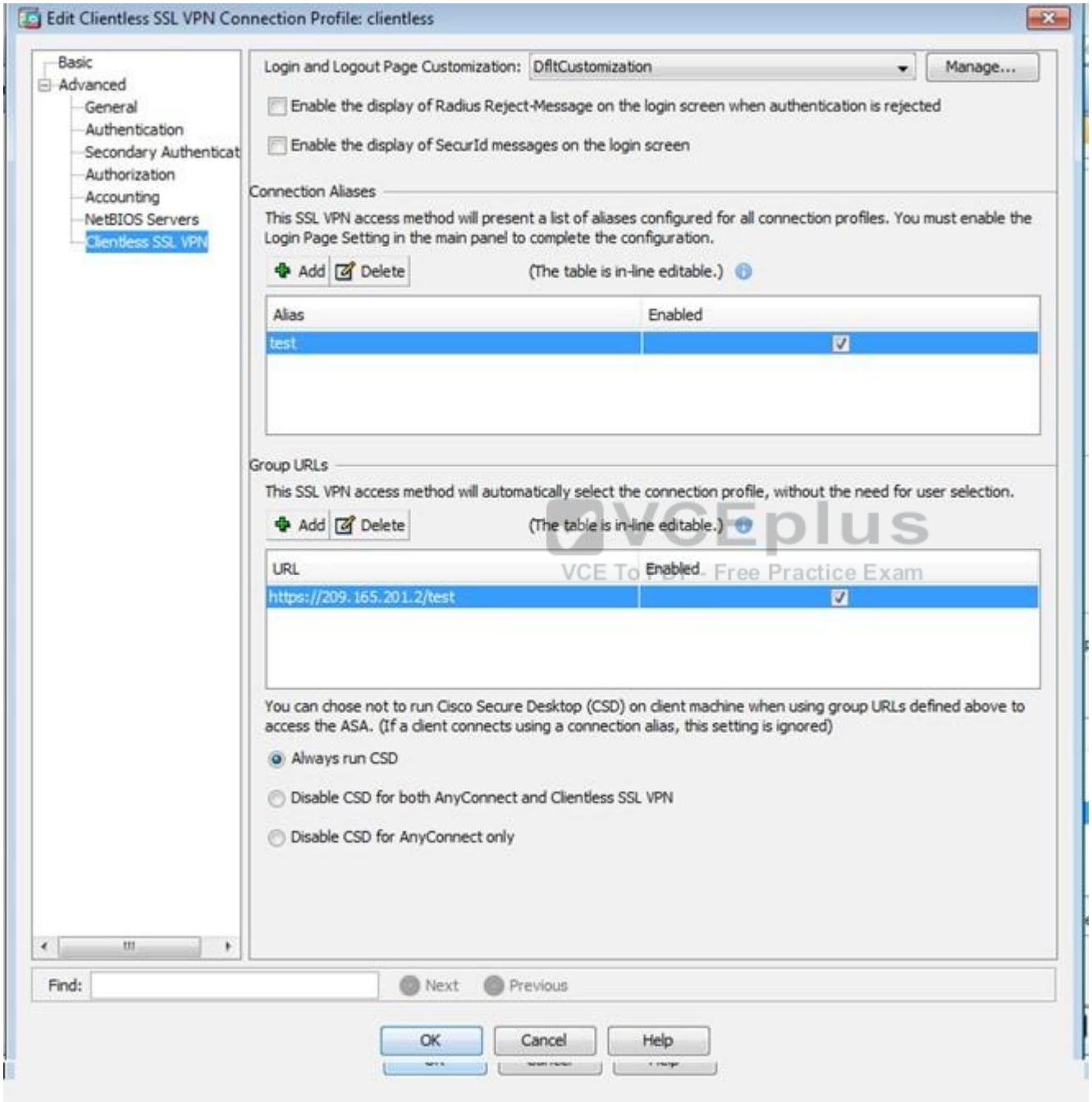


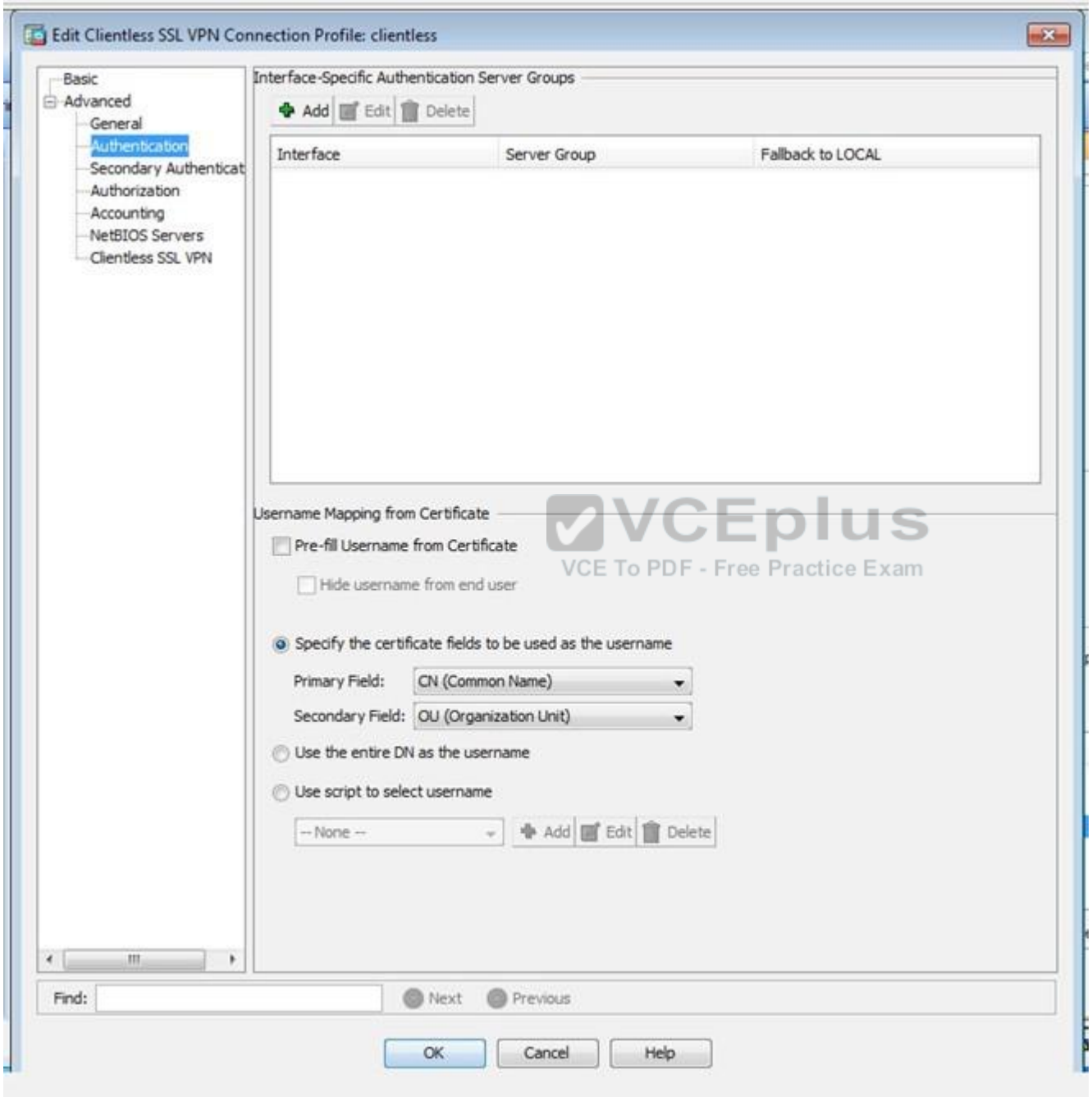


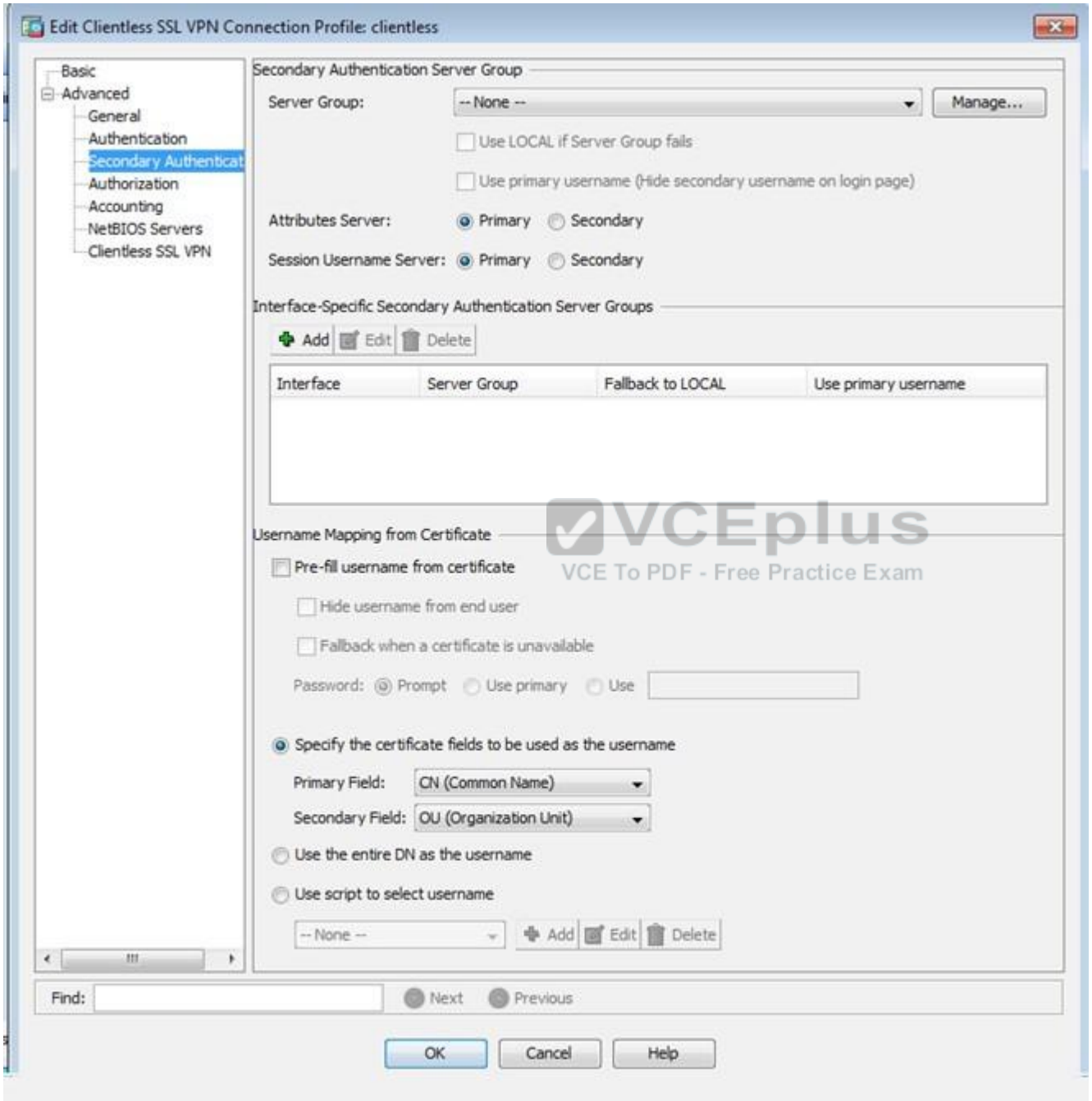


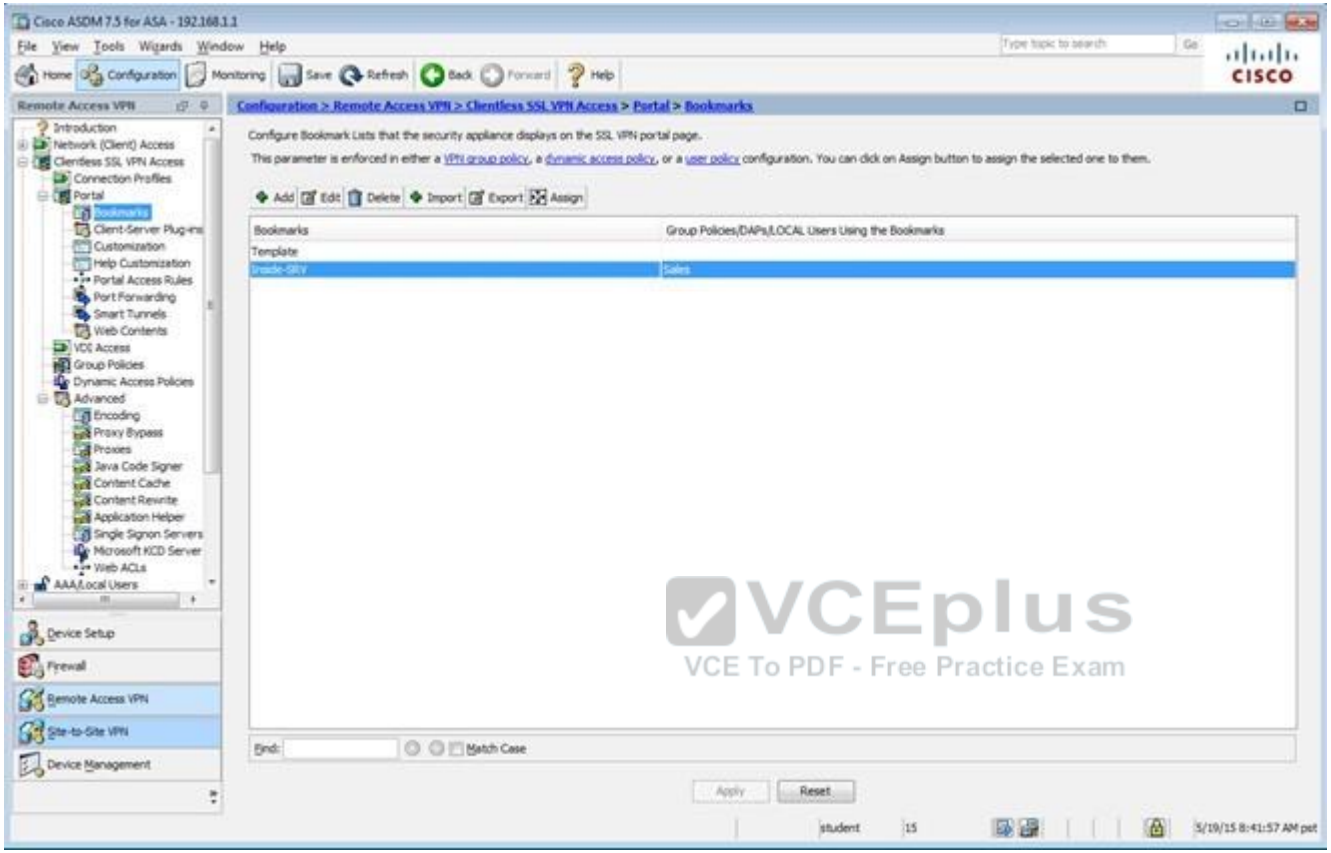


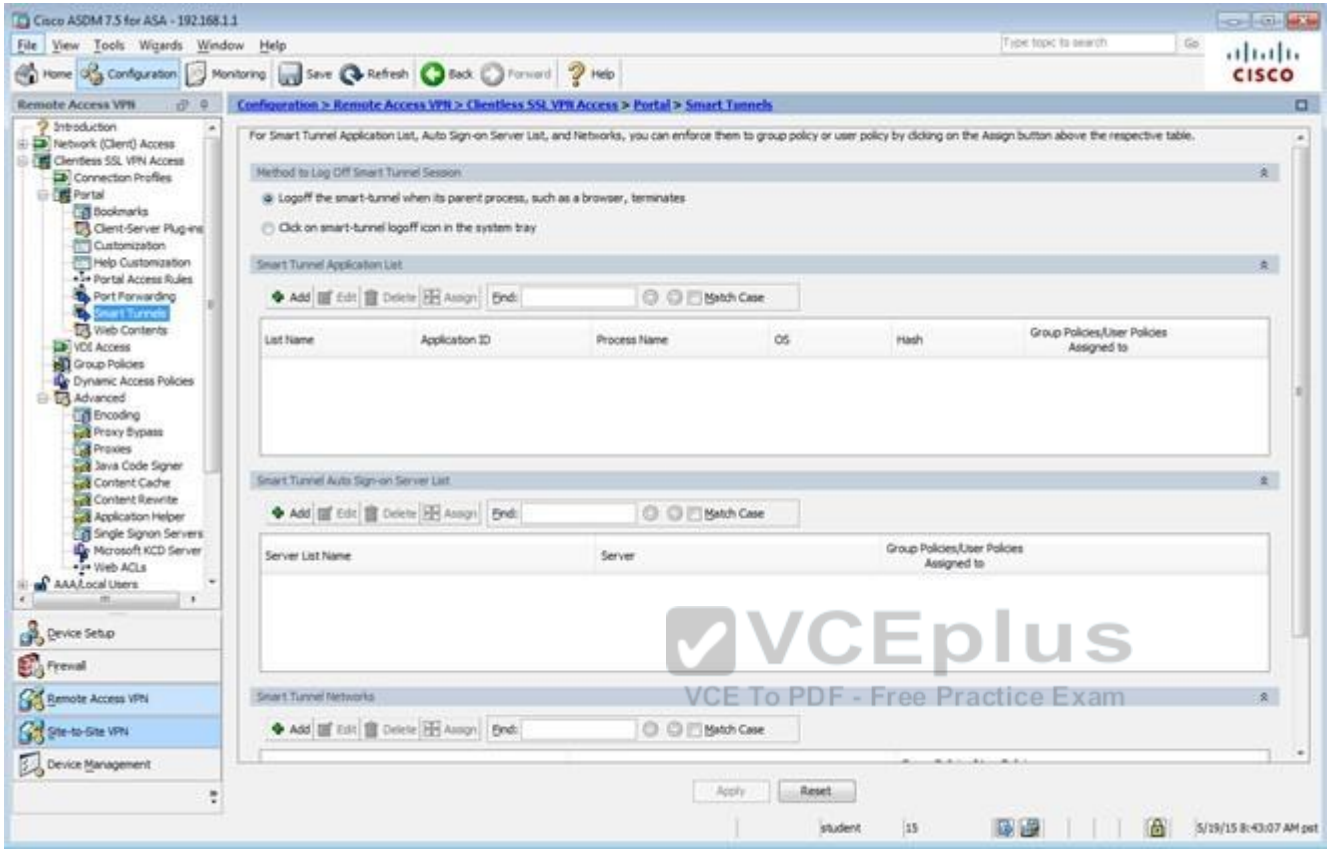


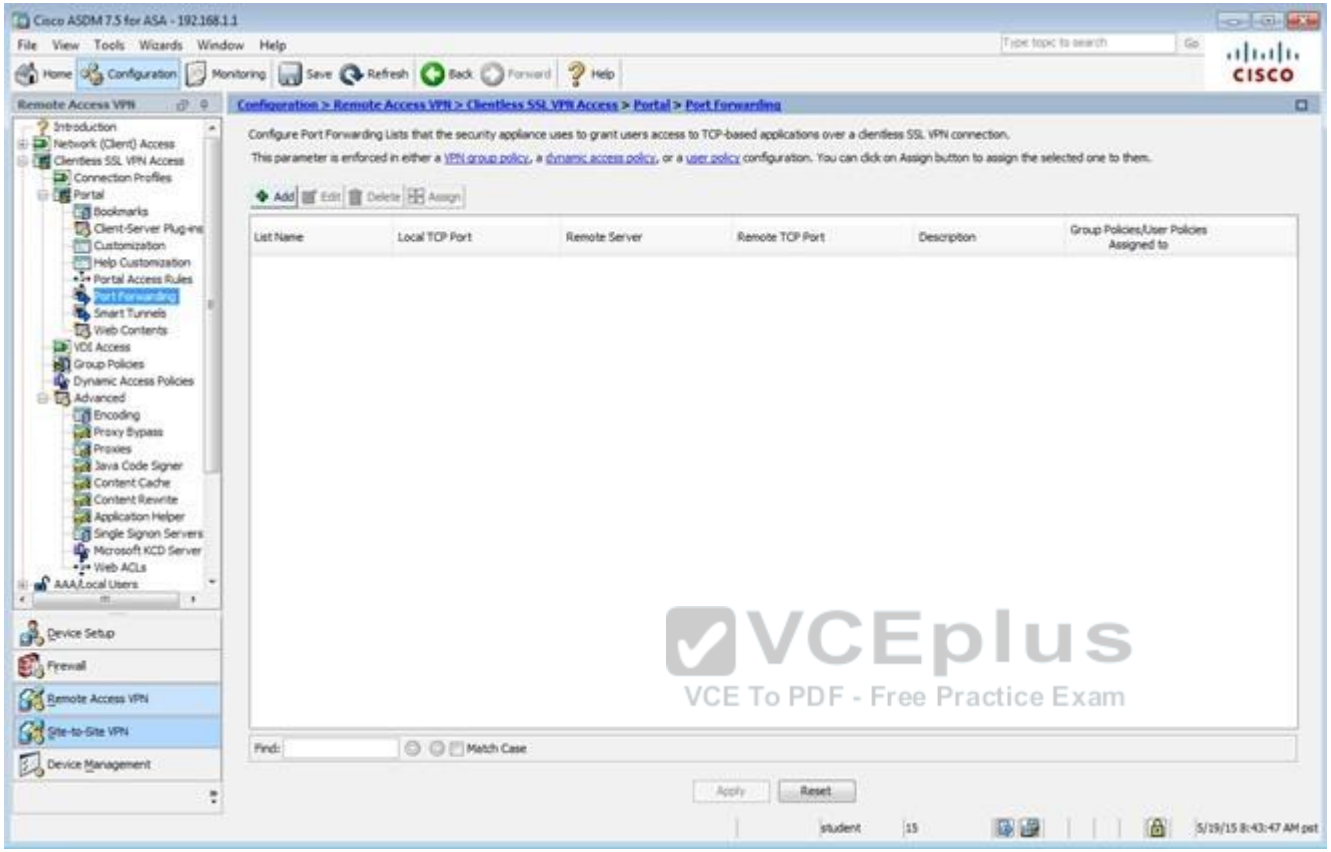


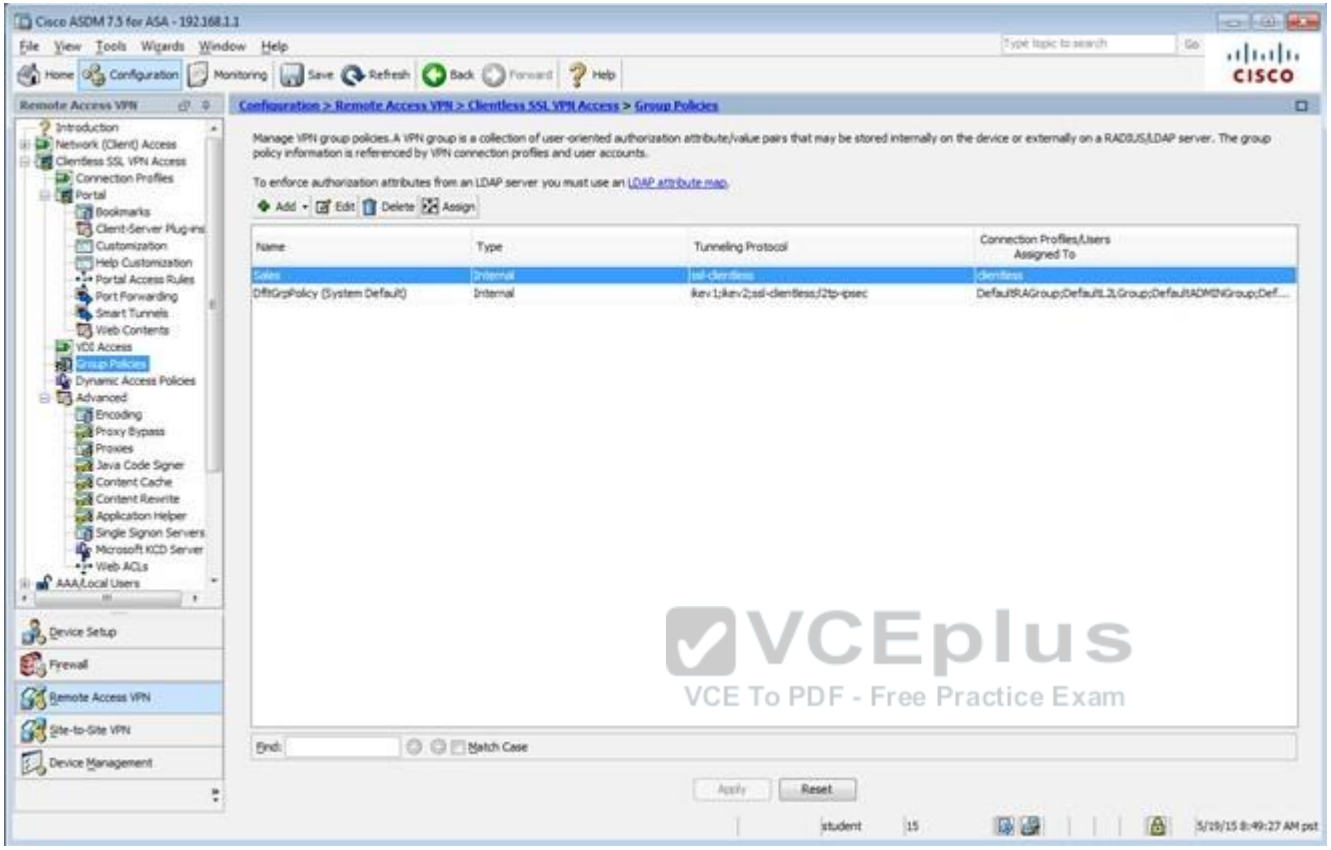


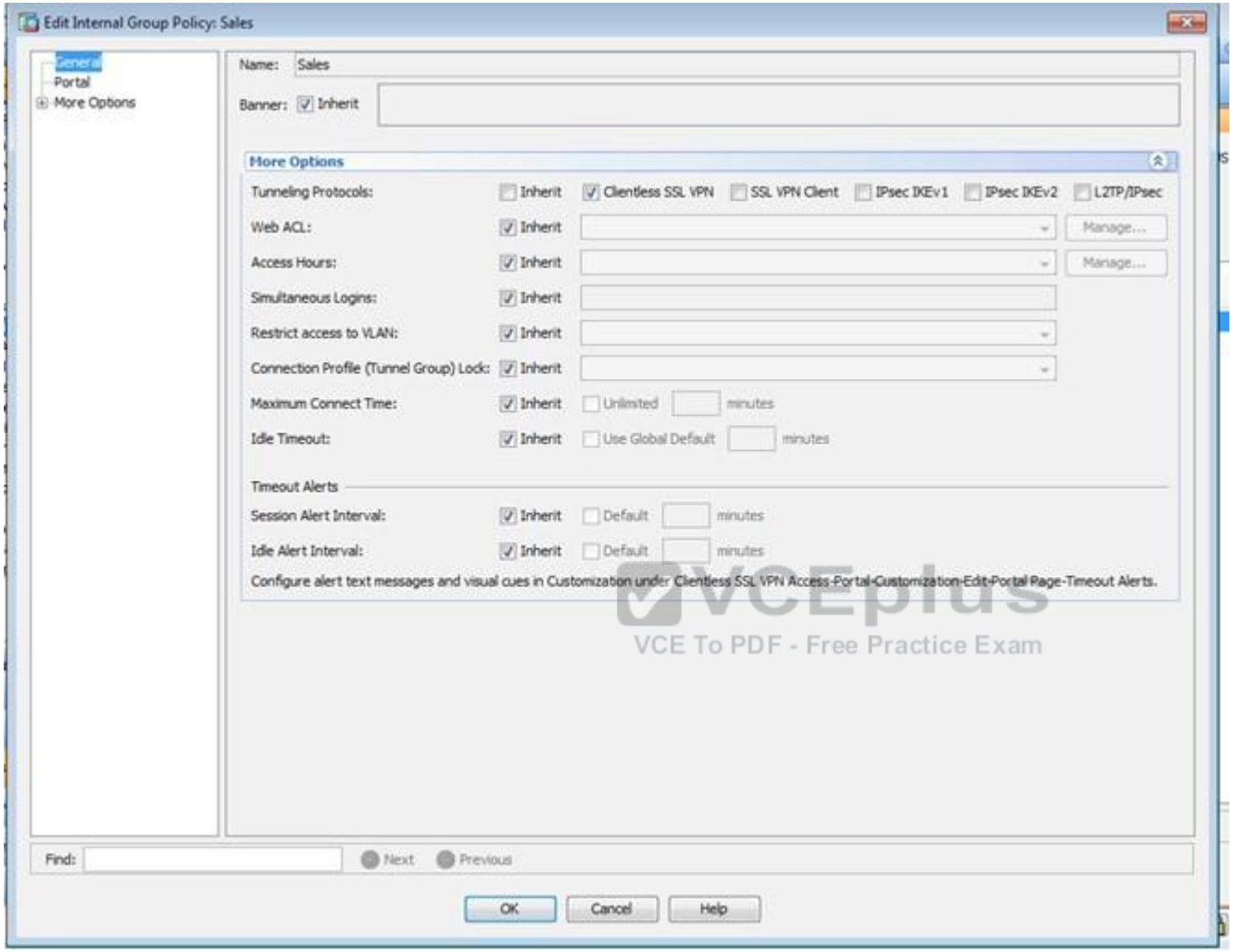


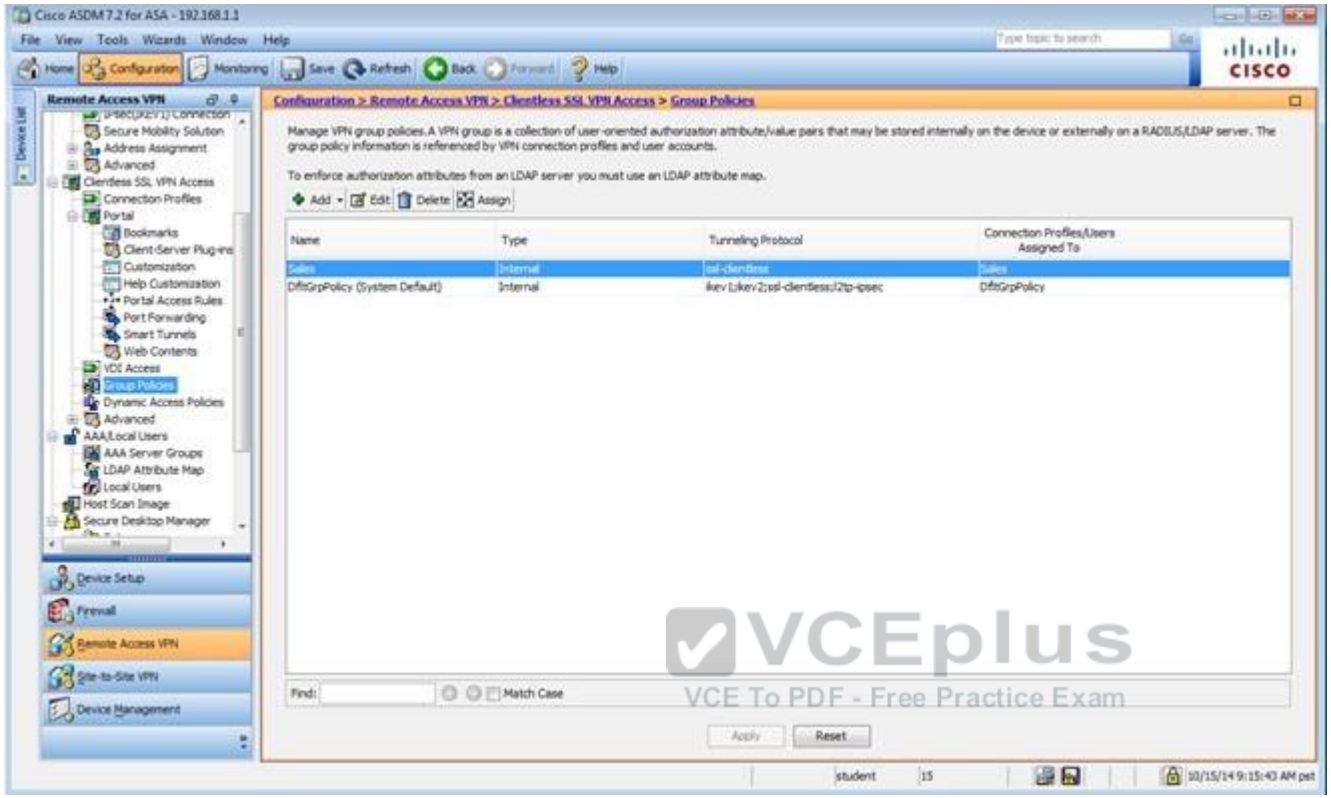


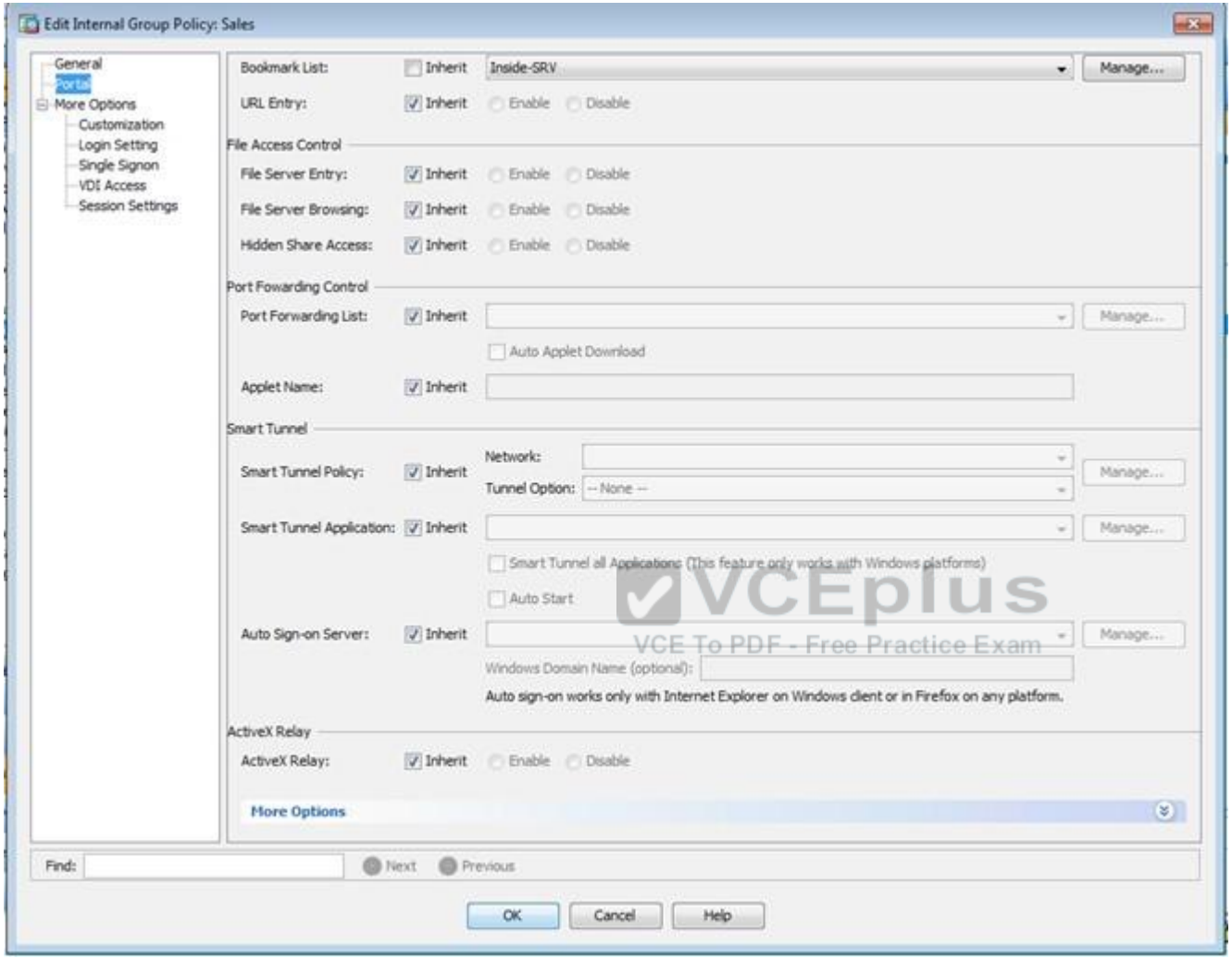


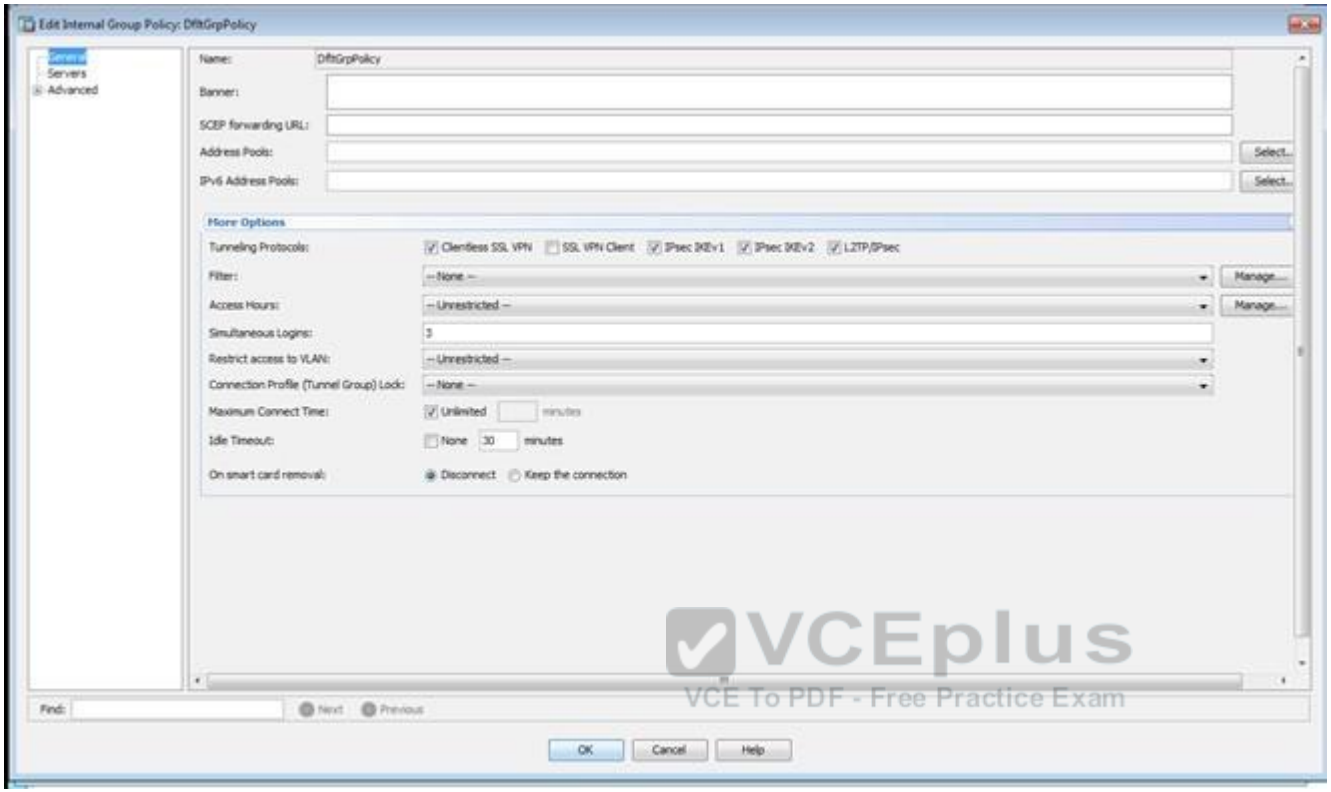


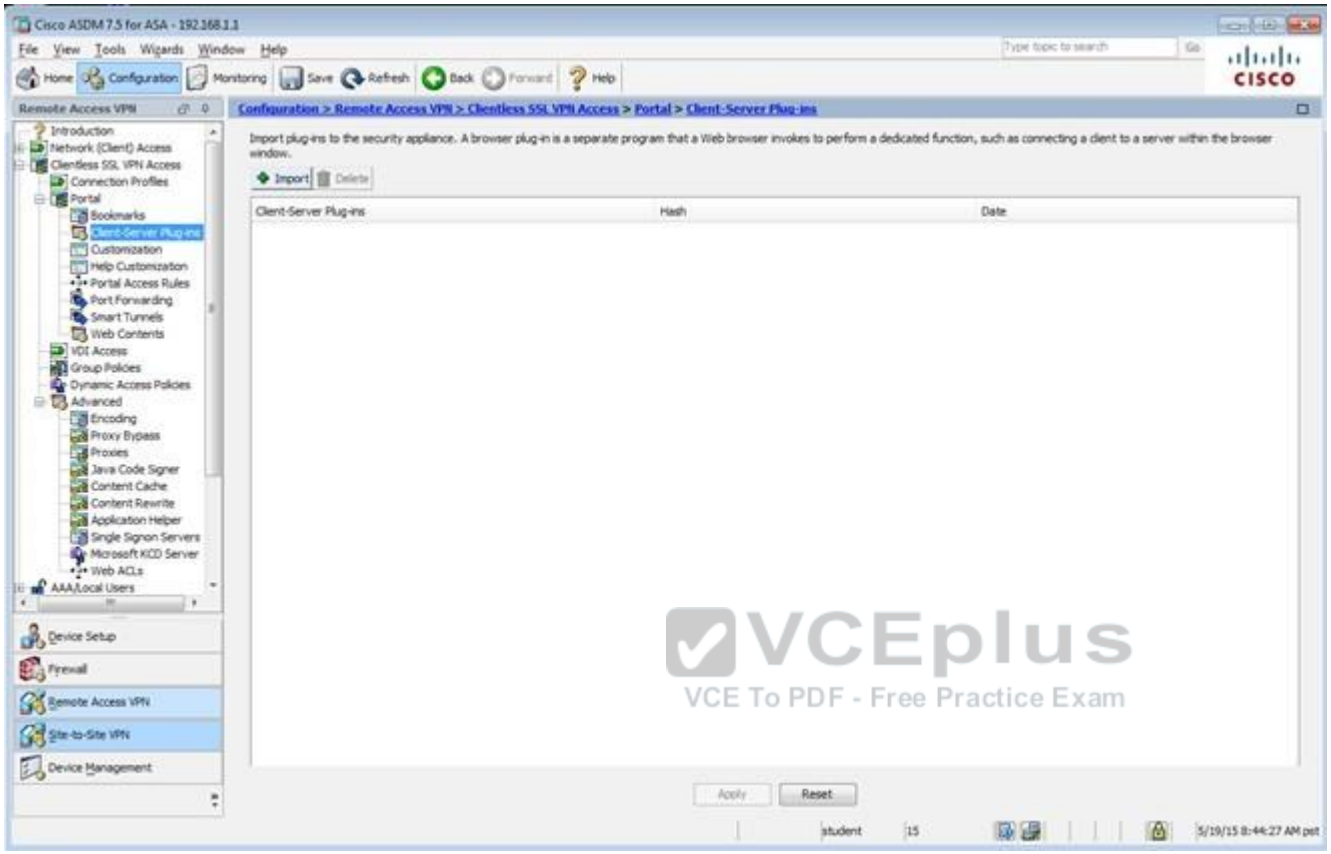


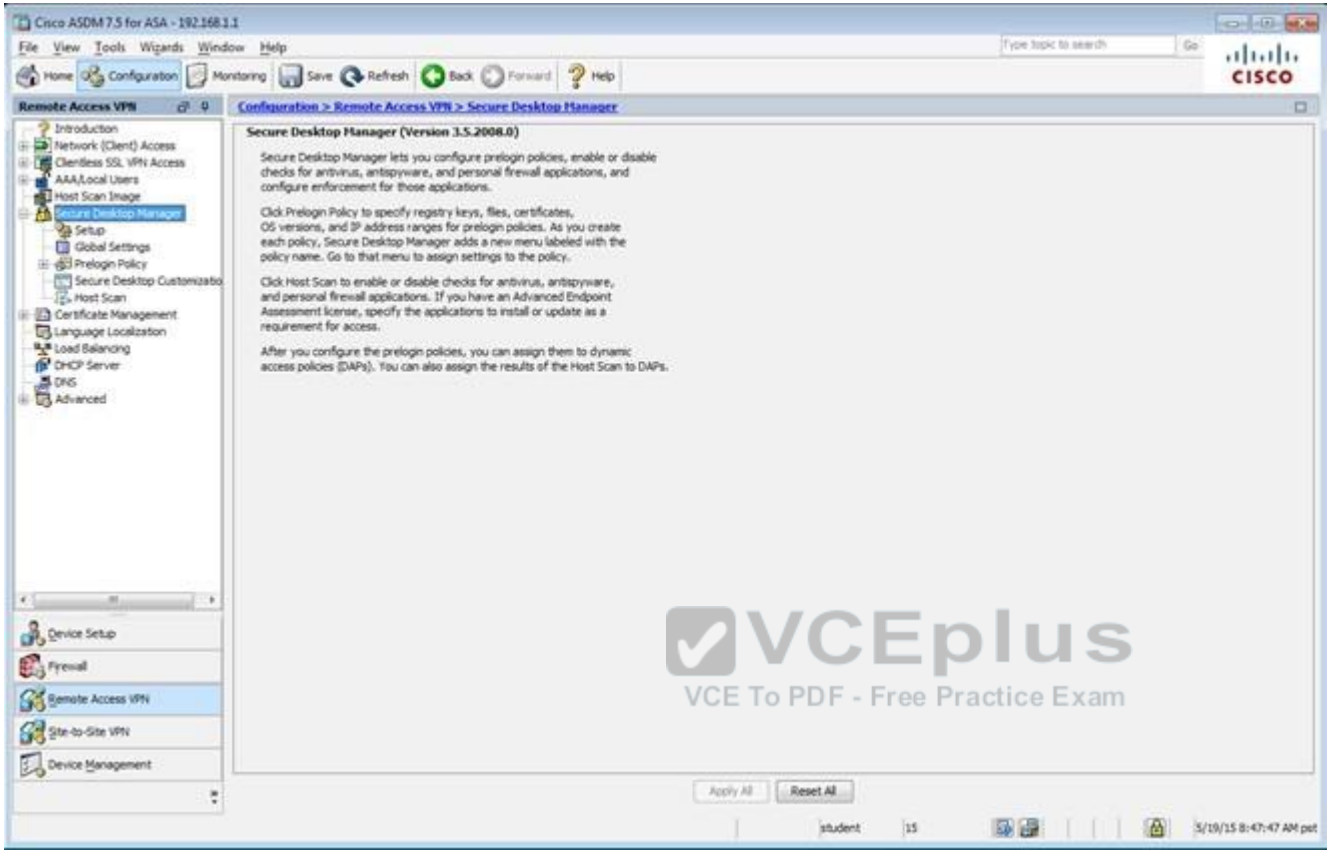


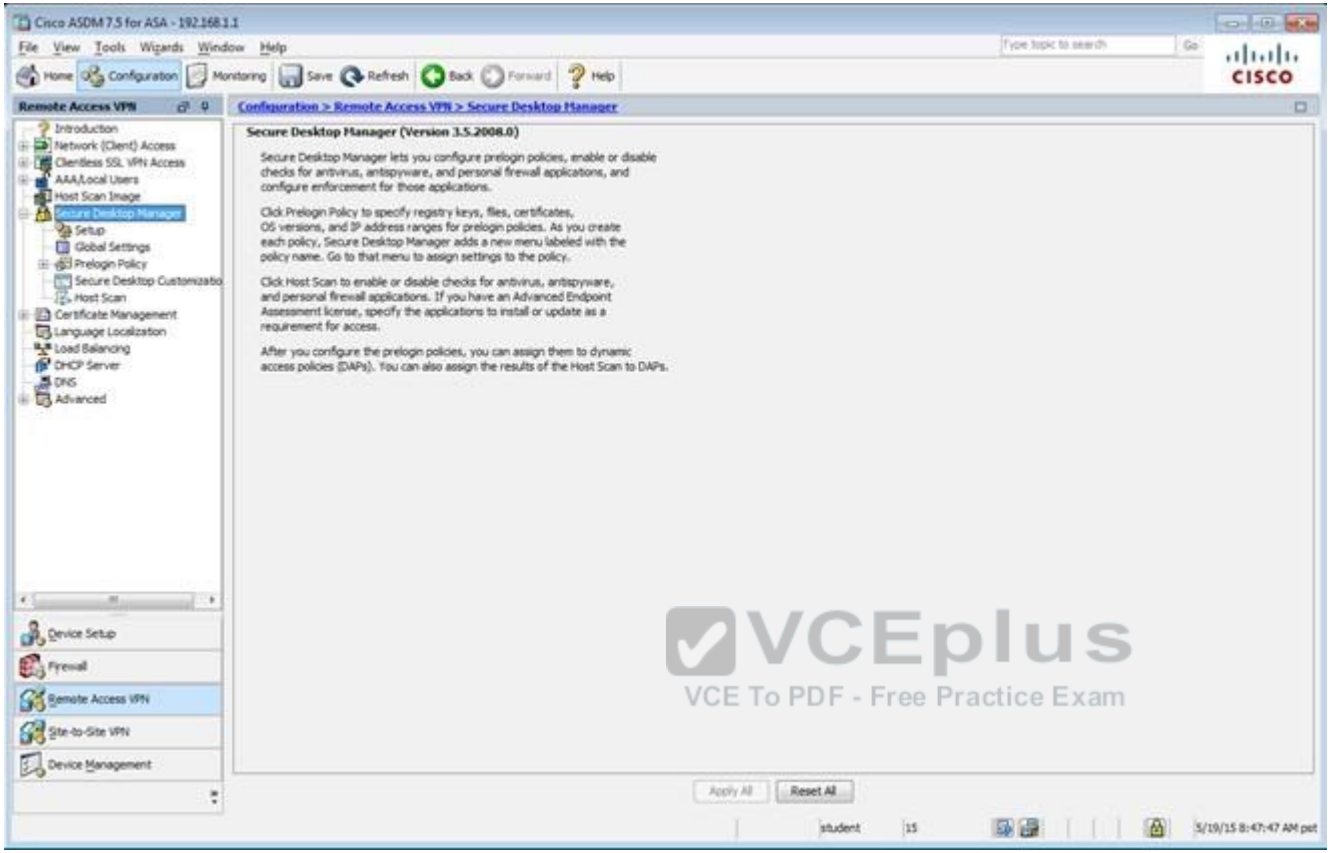


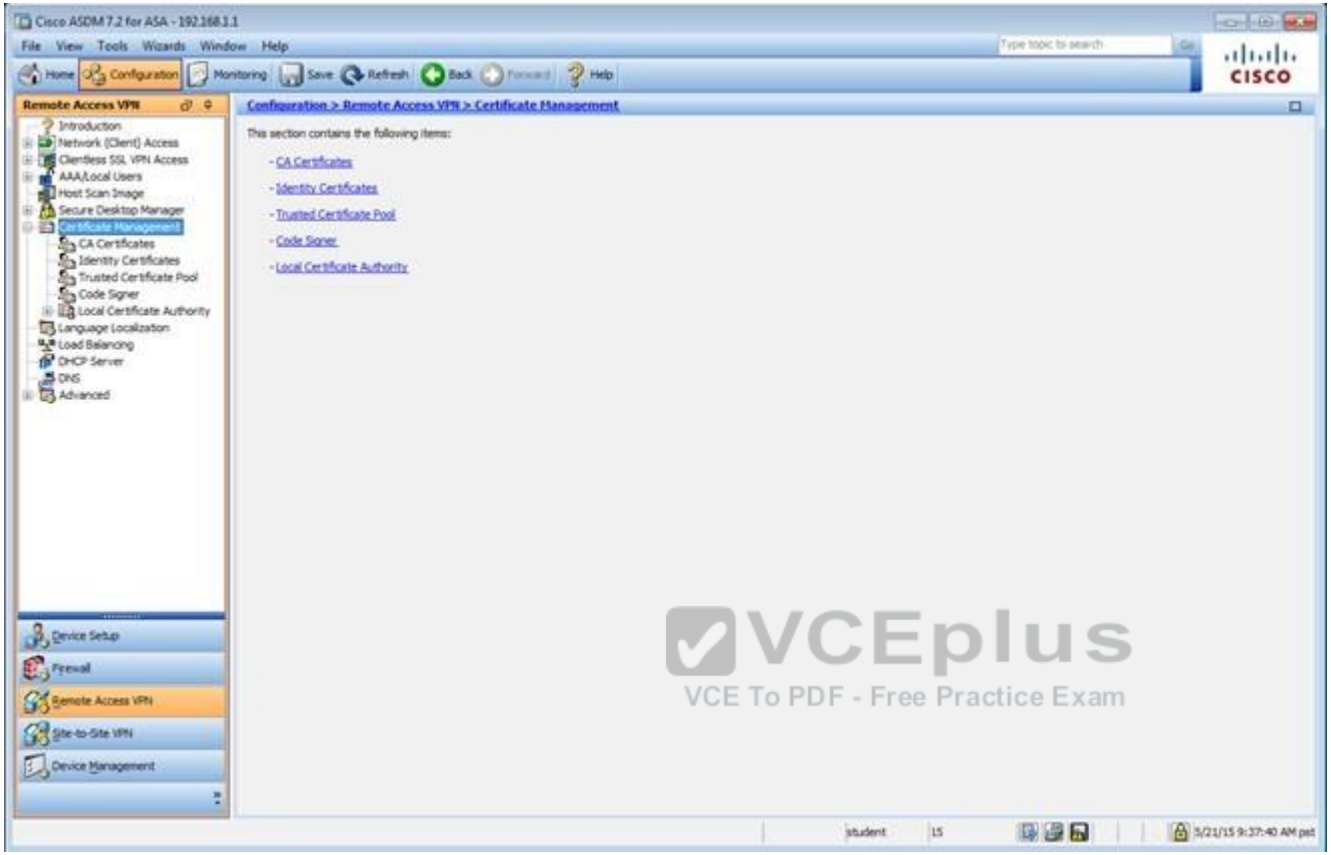


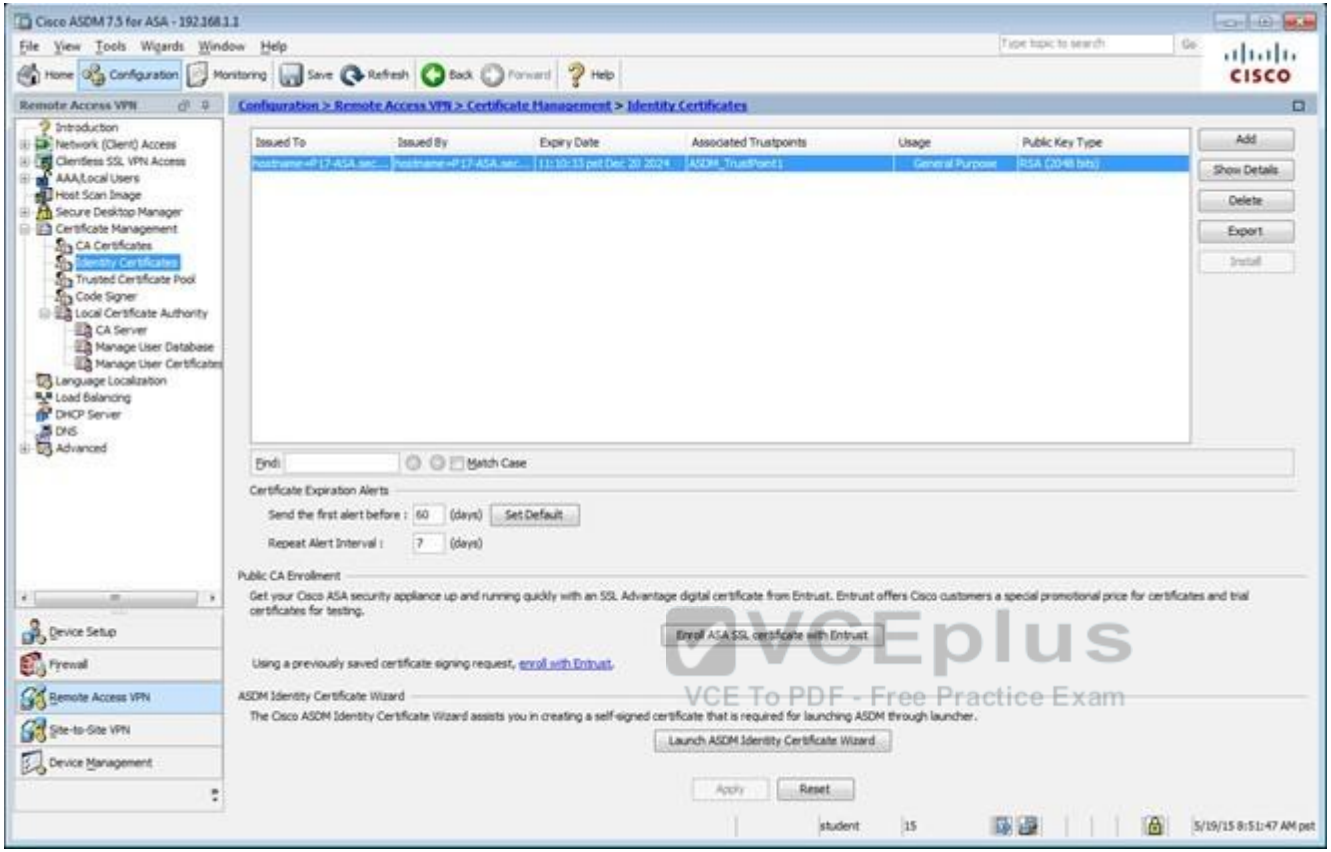


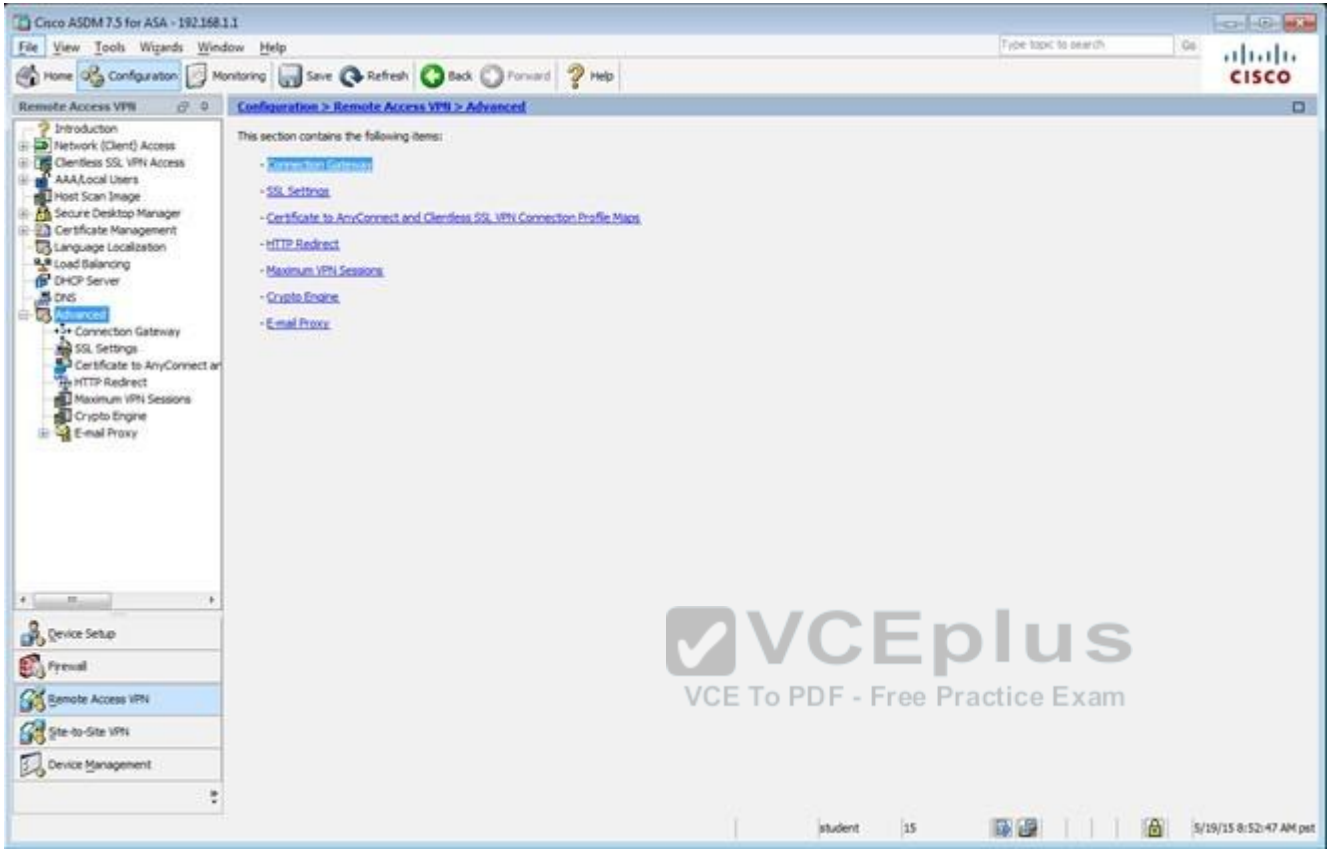


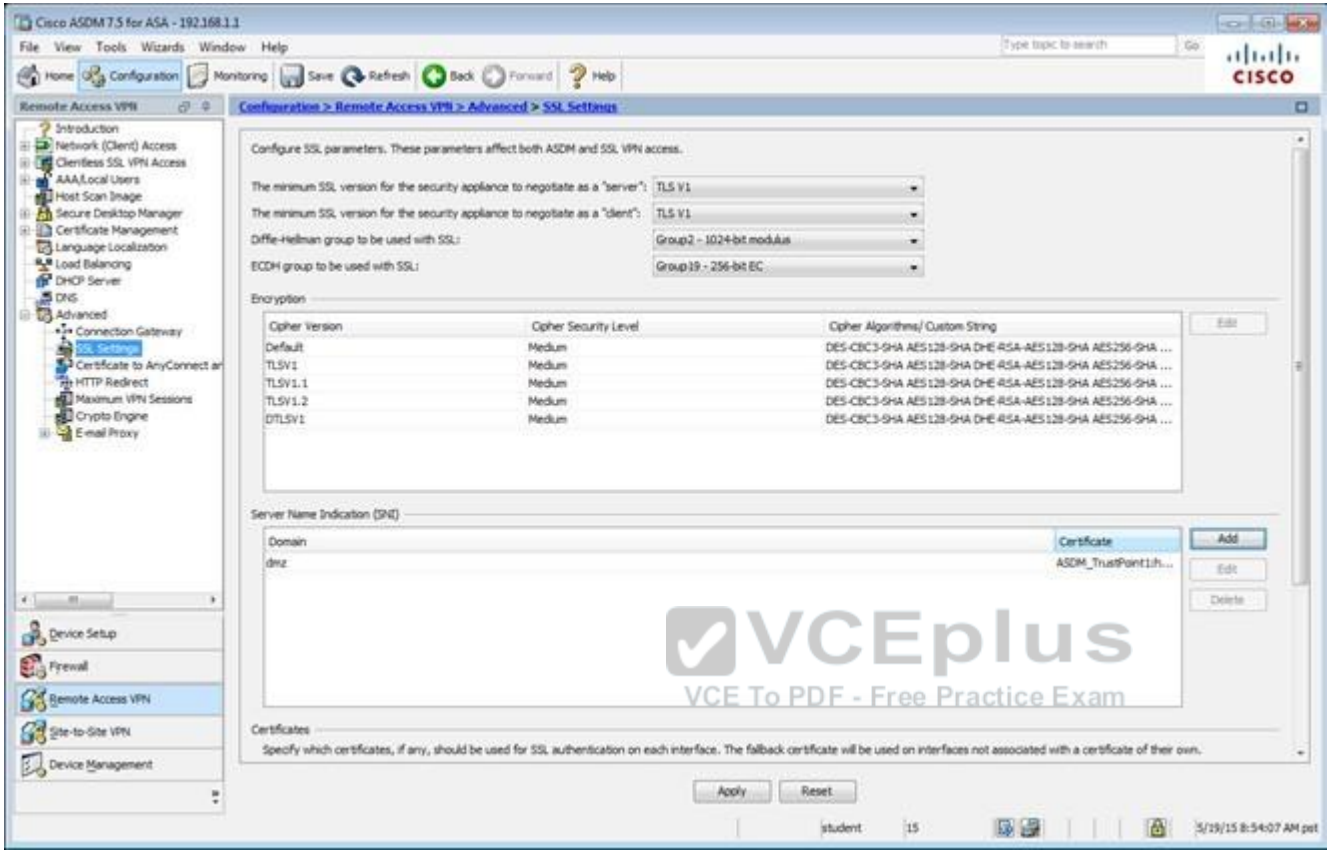


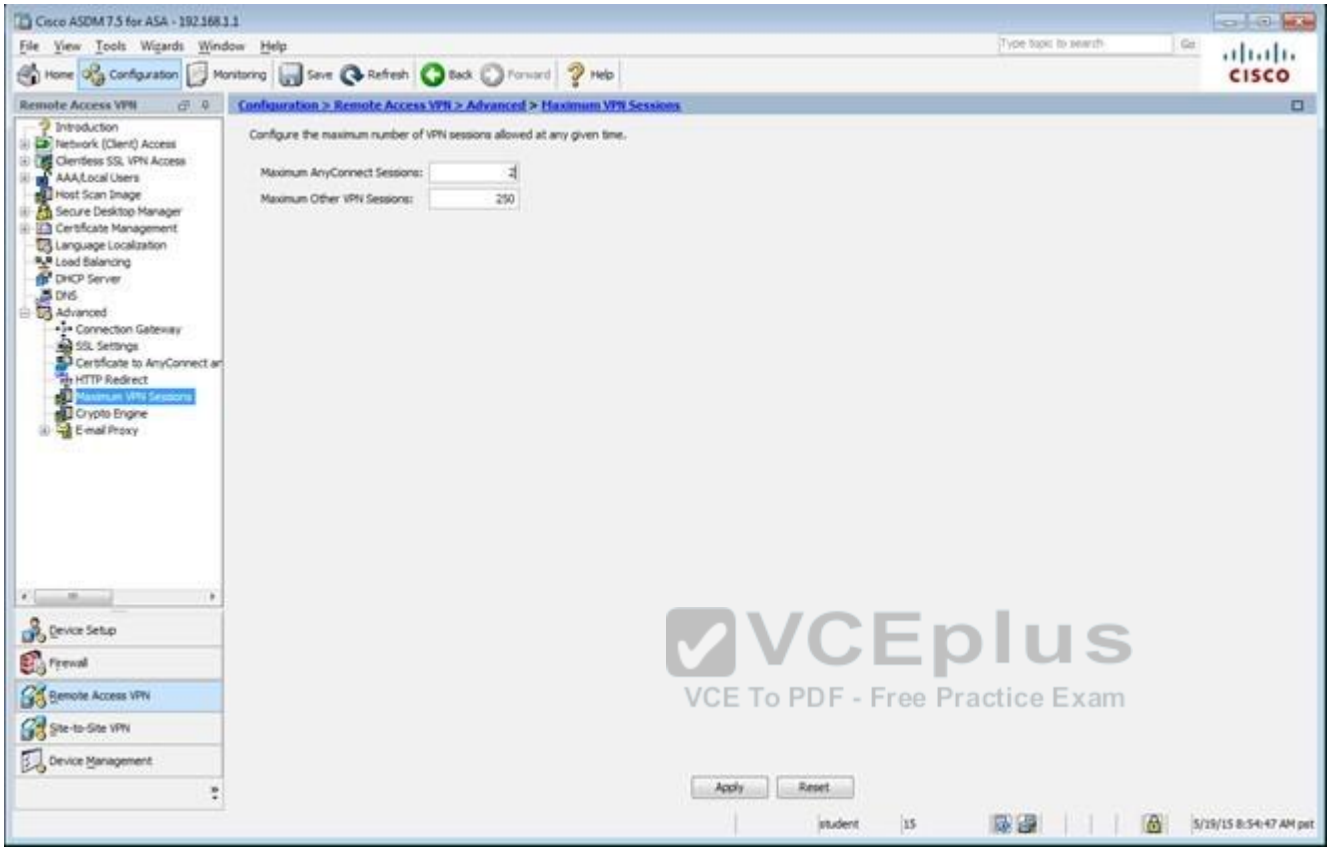


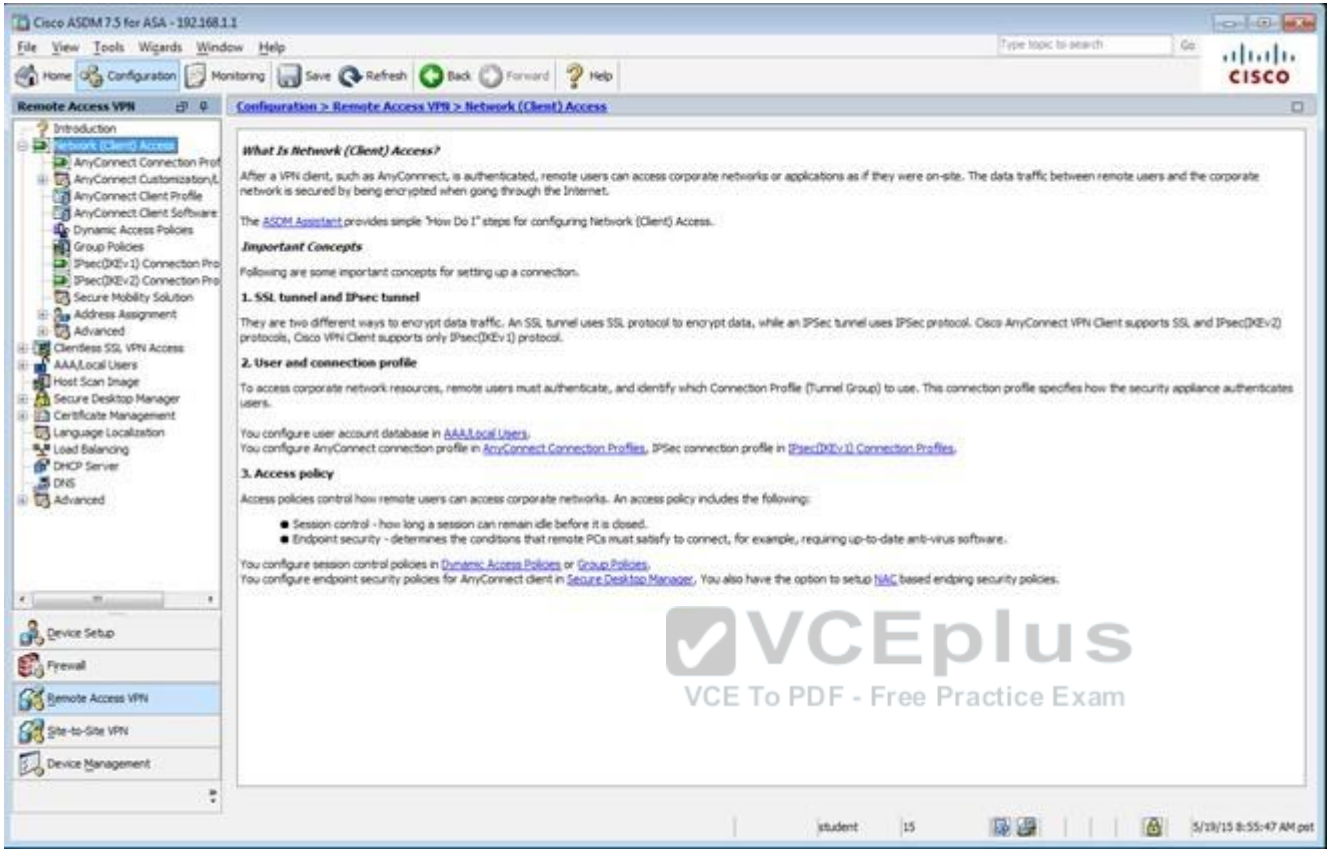


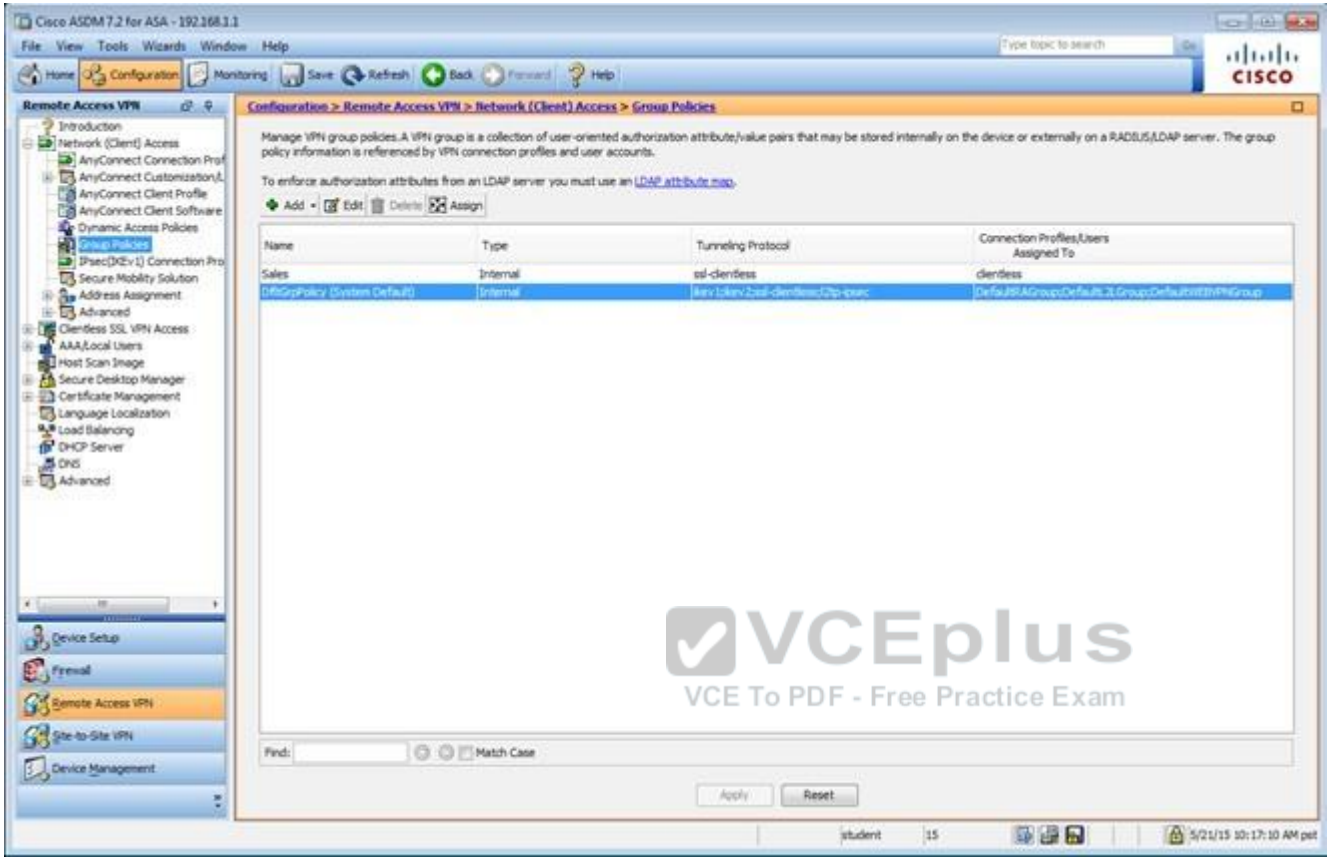


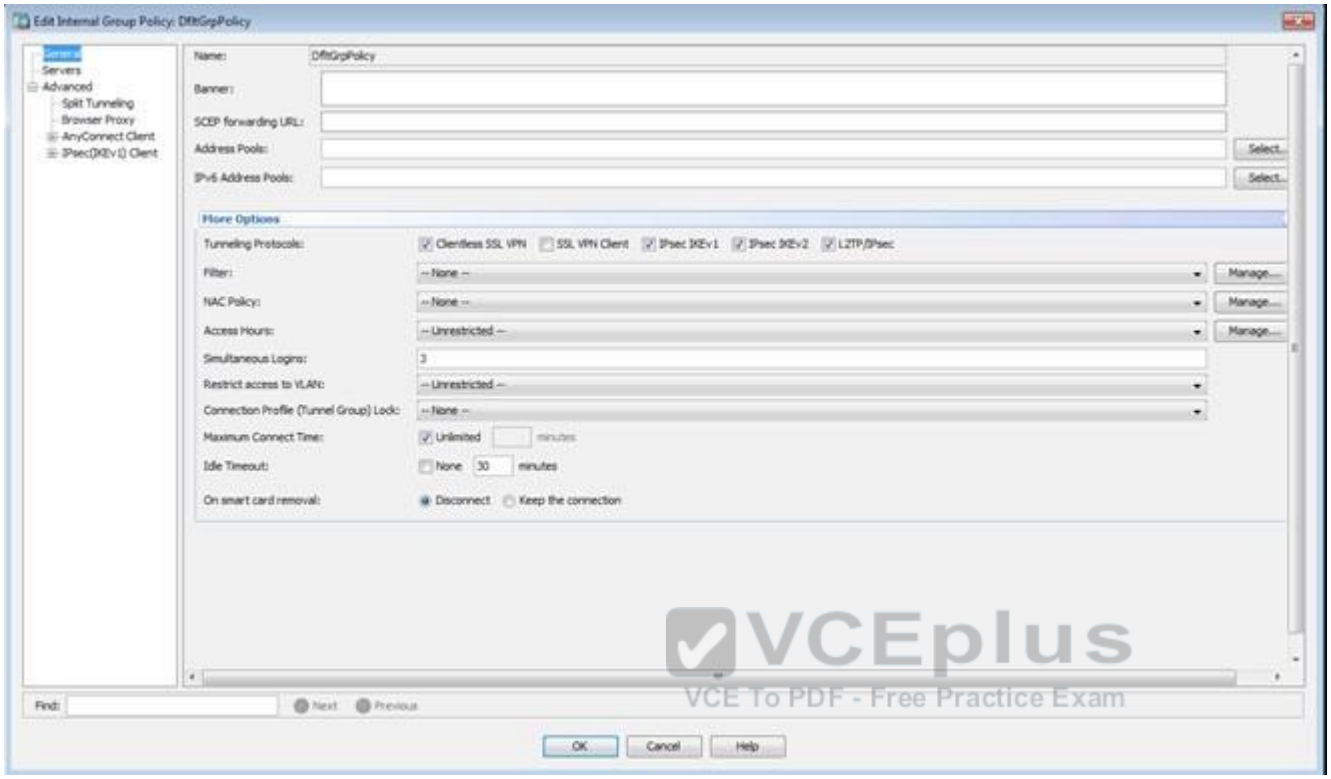


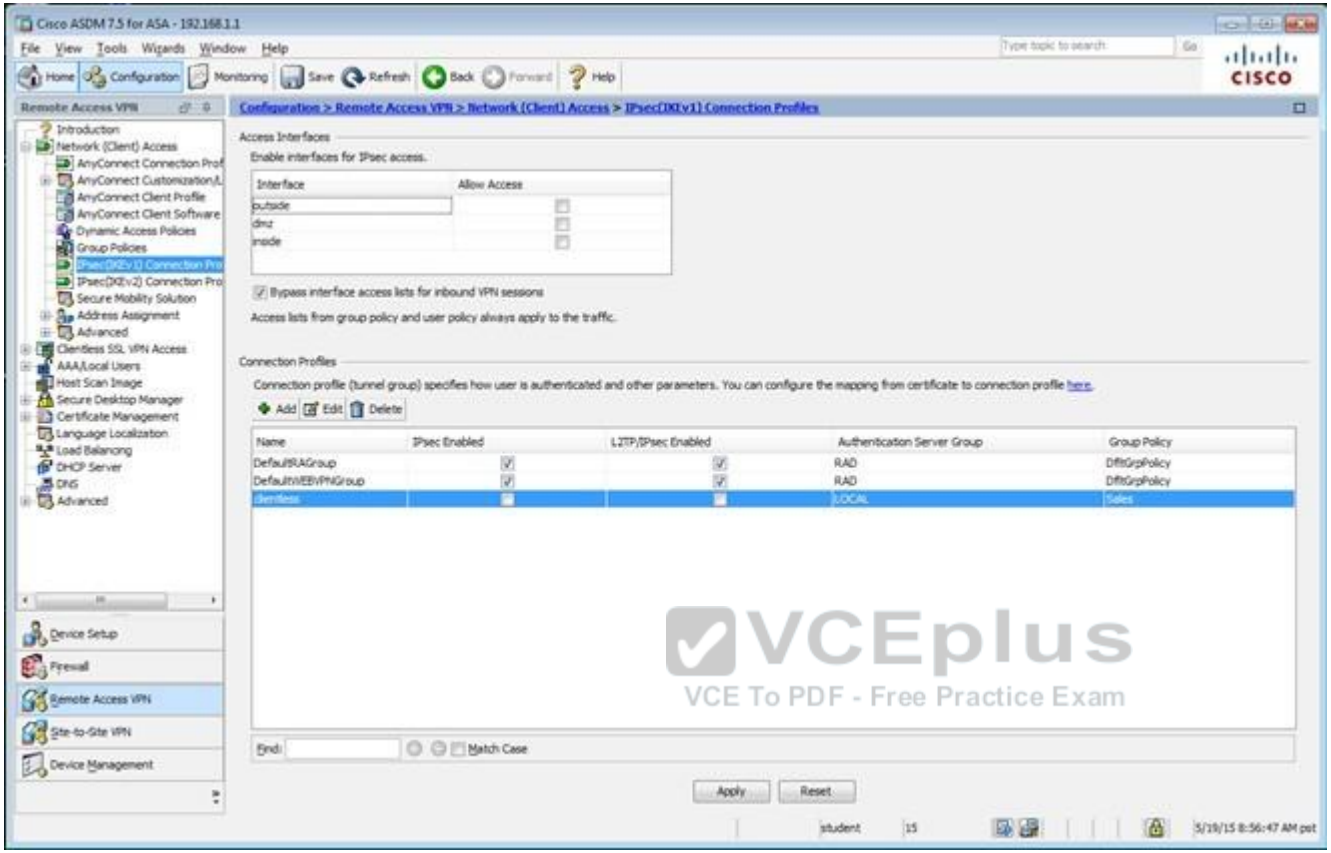


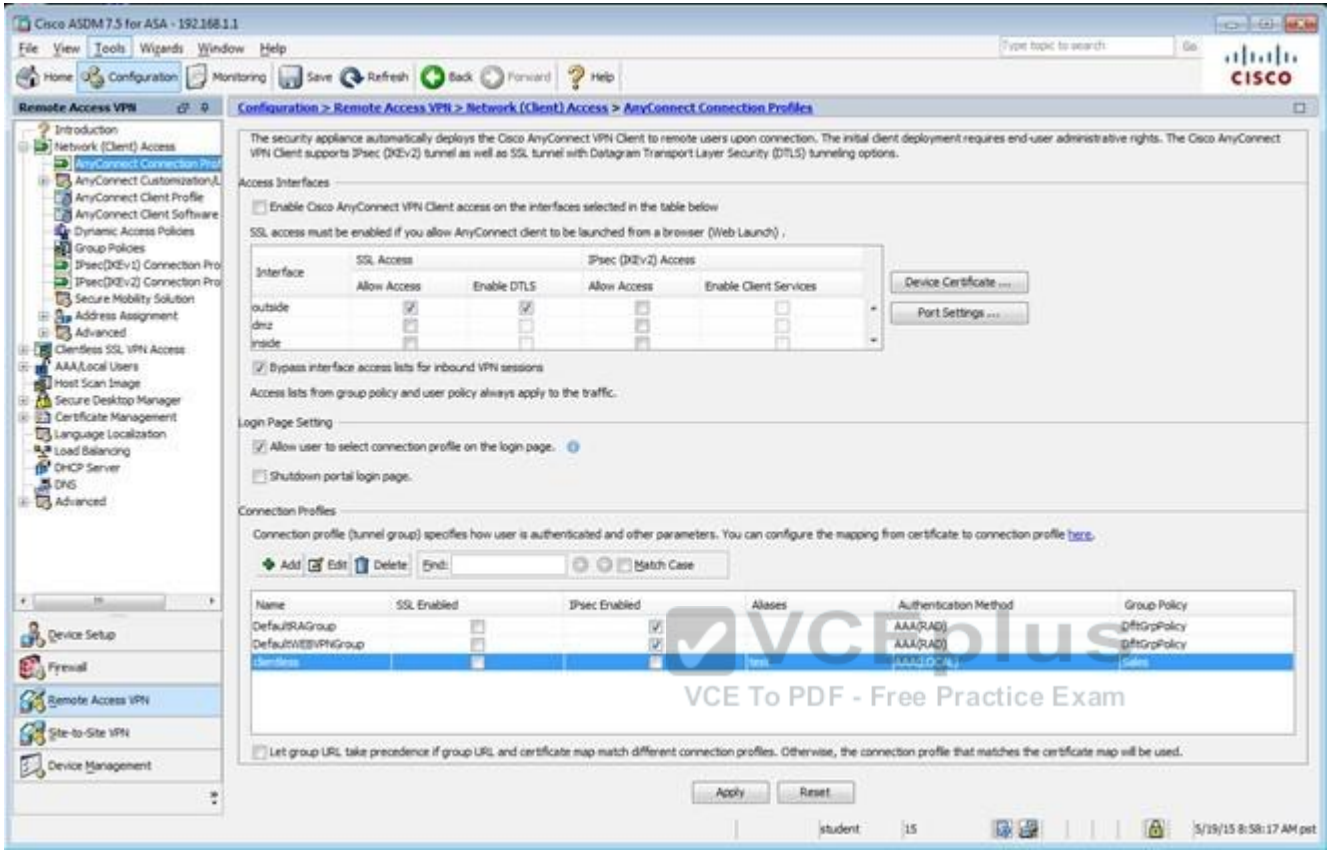


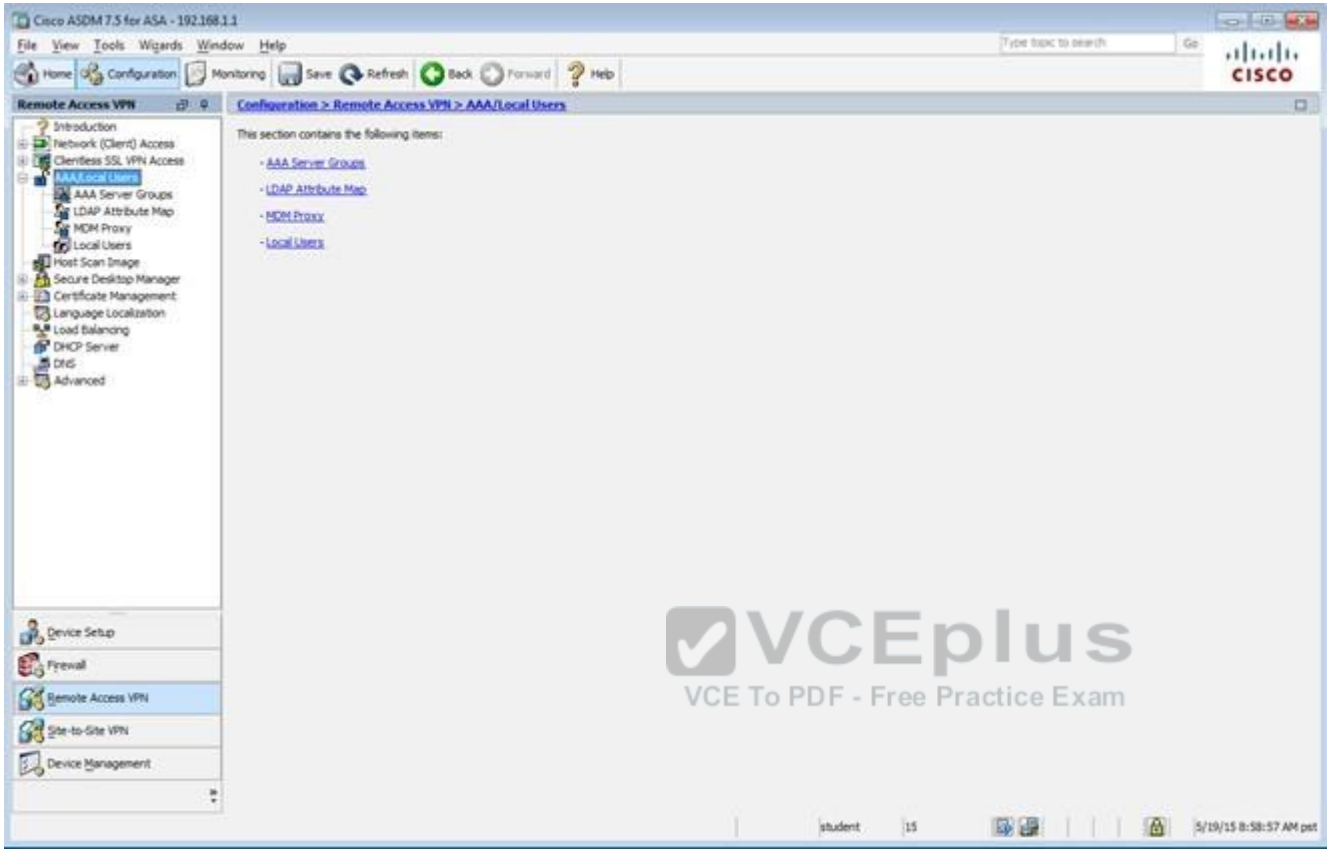


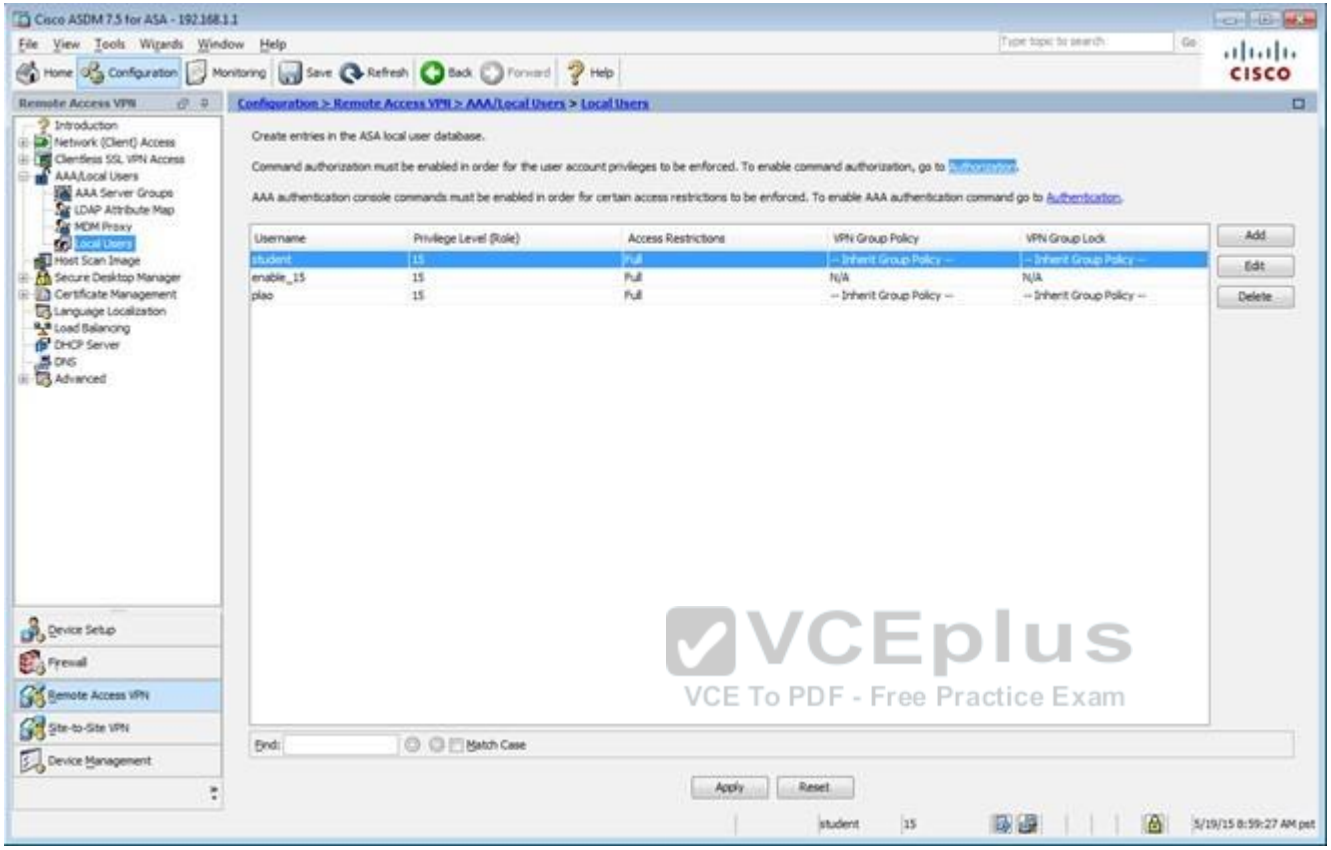


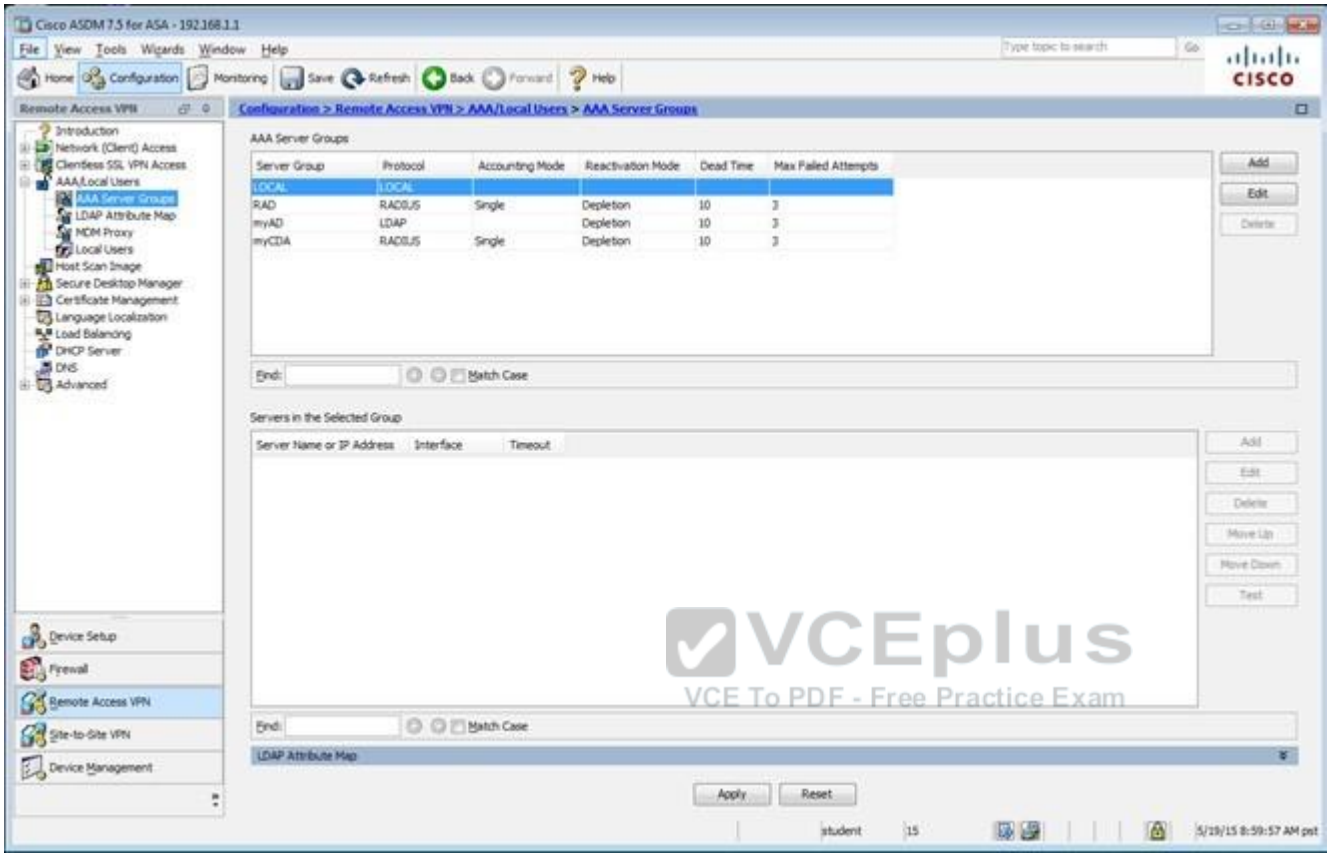










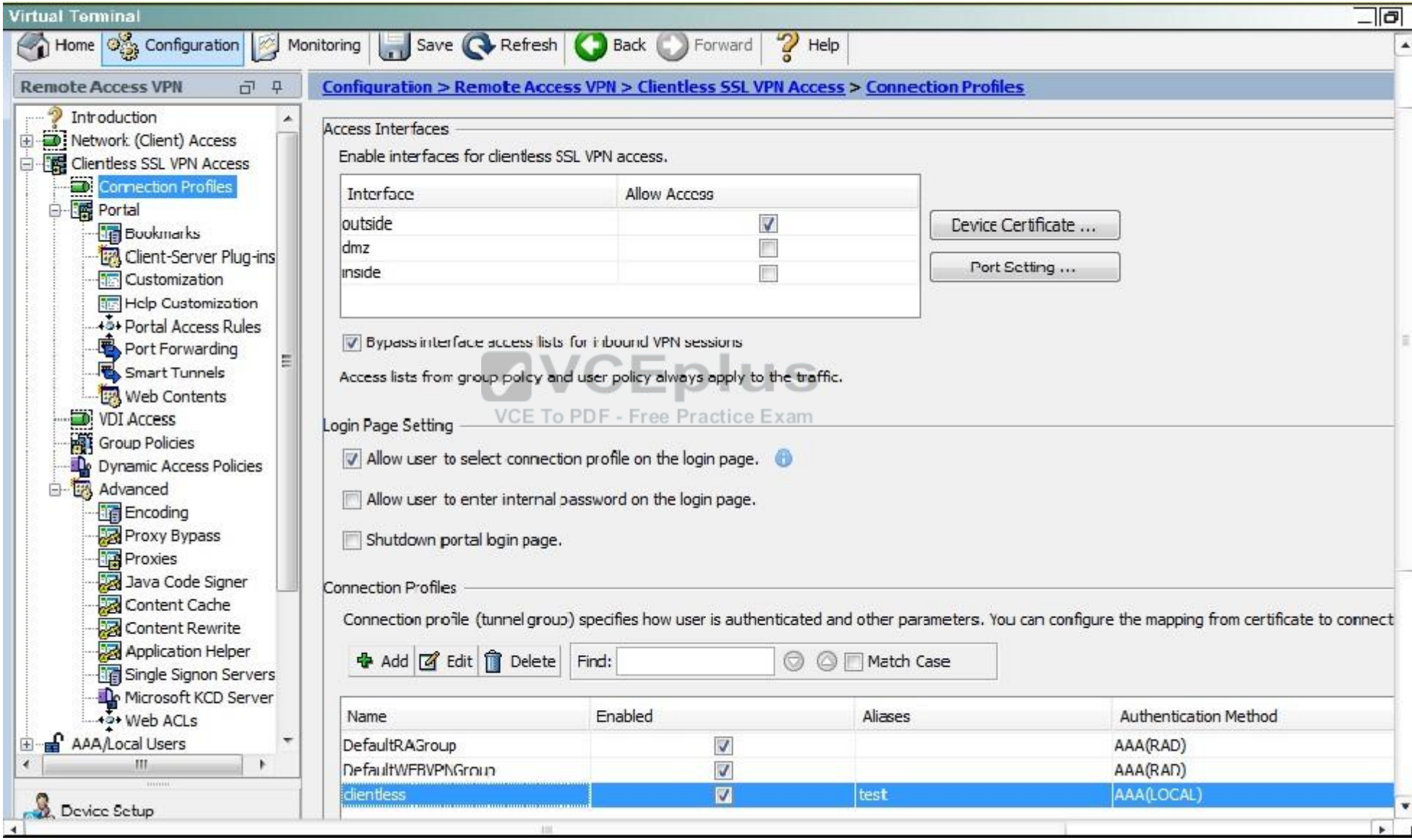


Which user authentication method is used when users login to the Clientless SSLVPN portal using https://209.165.201.2/test?

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

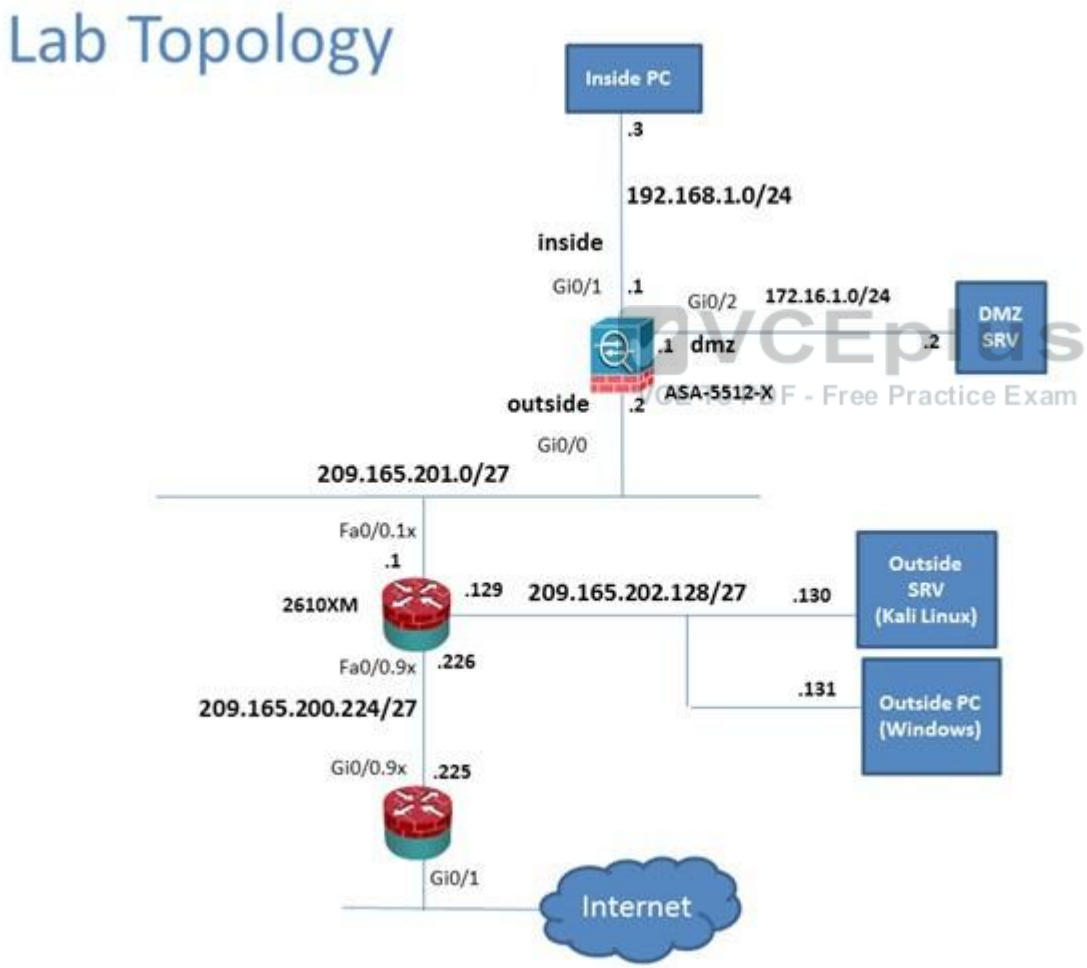
Explanation/Reference:
Explanation:
This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used,

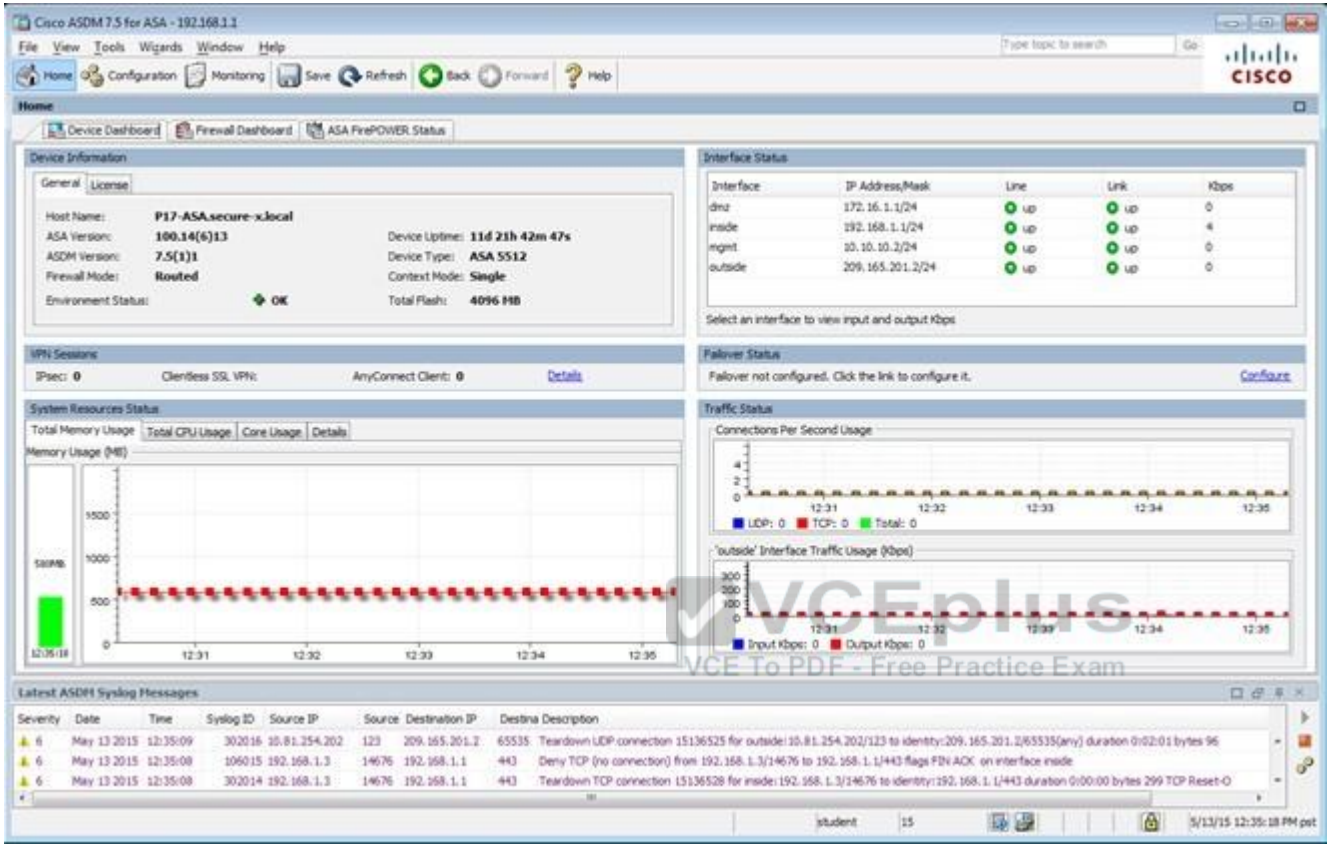


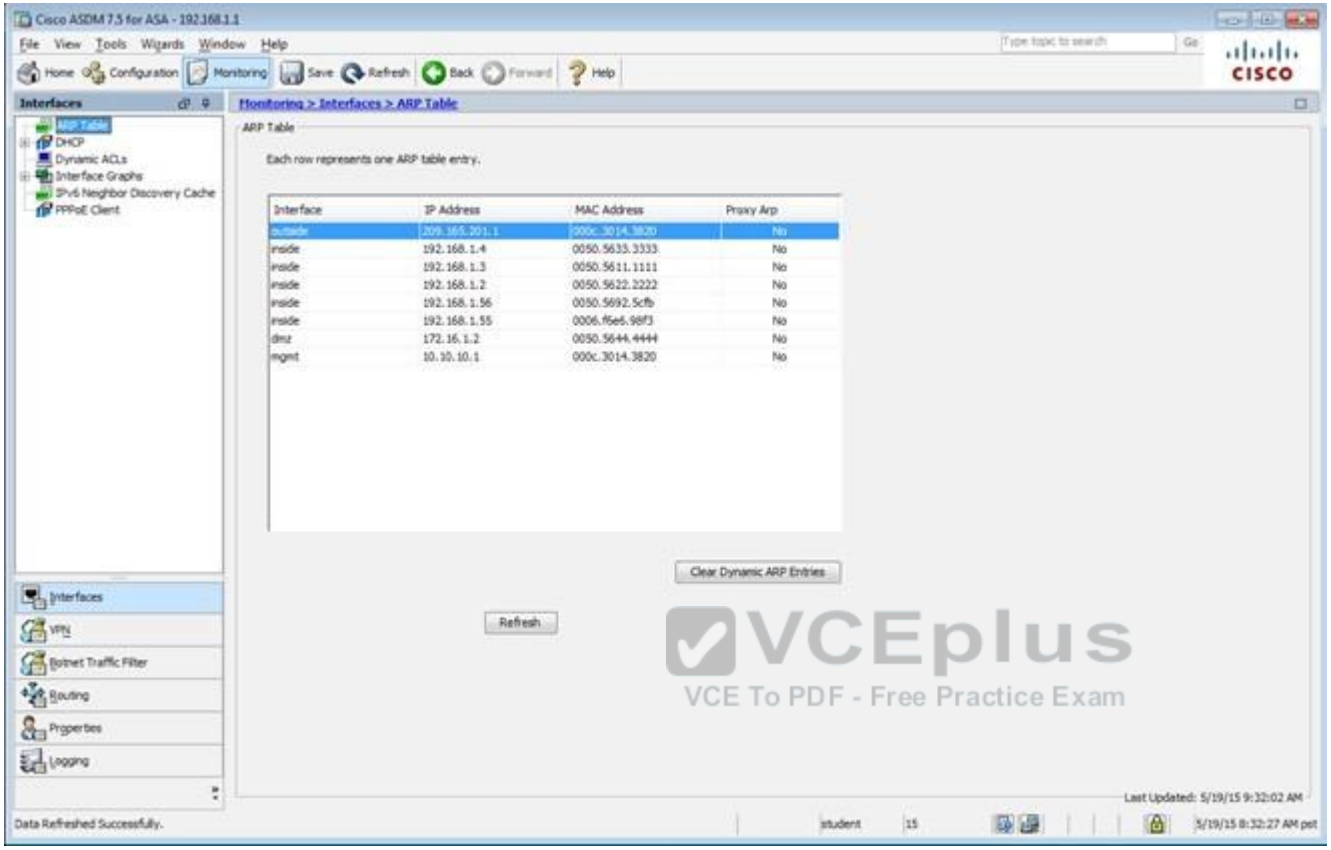
QUESTION 66
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

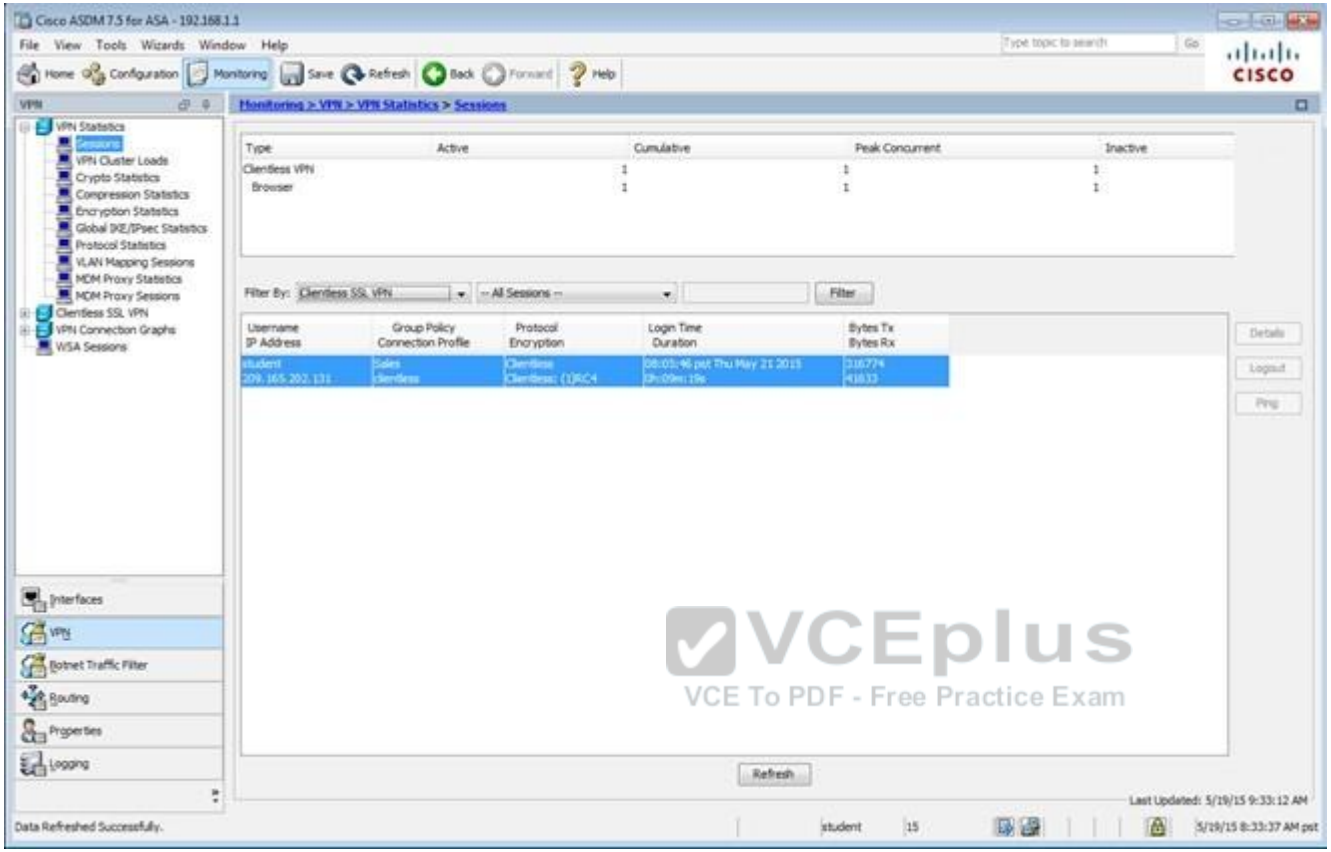
To access ASDM, click the ASA icon in the topology diagram.

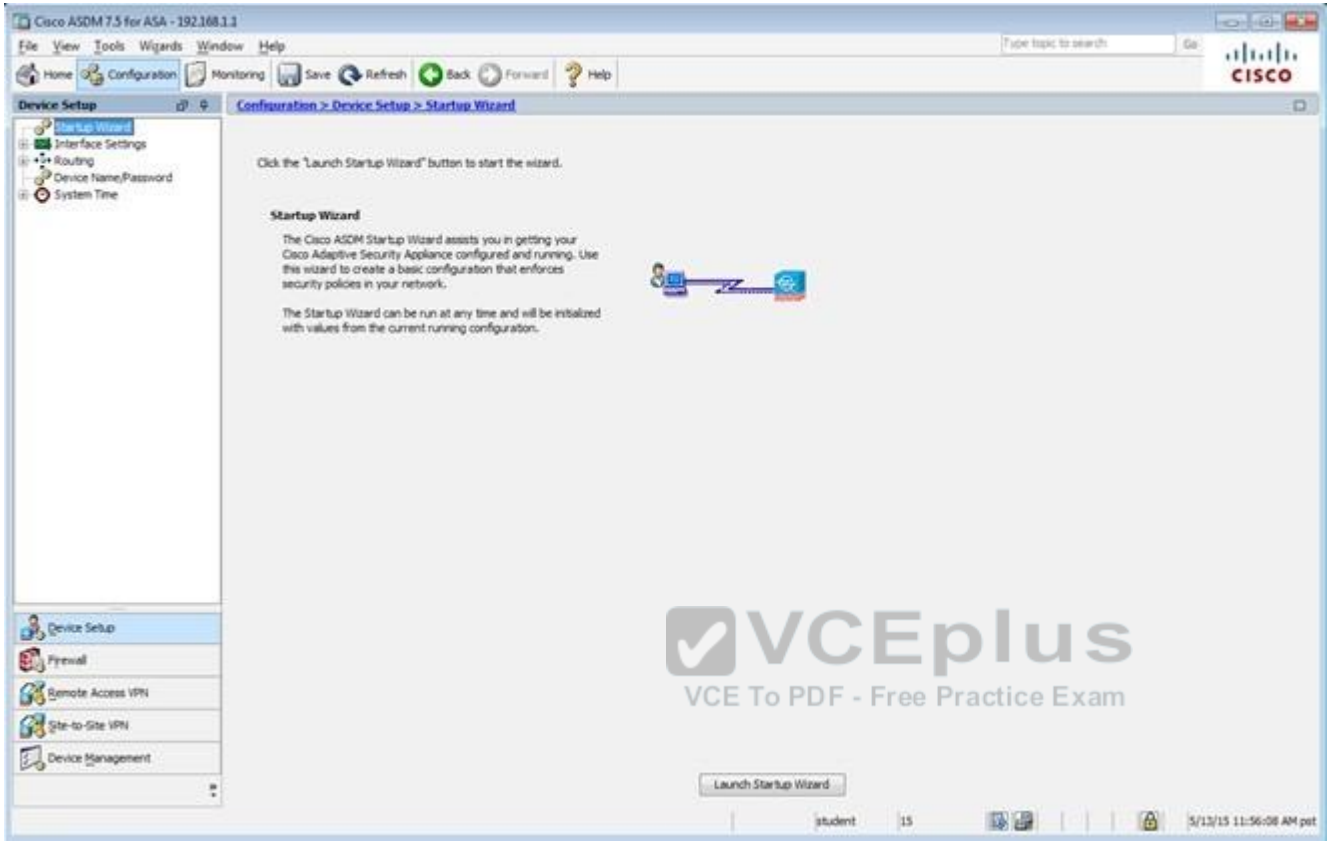
Note: Not all ASDM functionalities are enabled in this simulation. To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

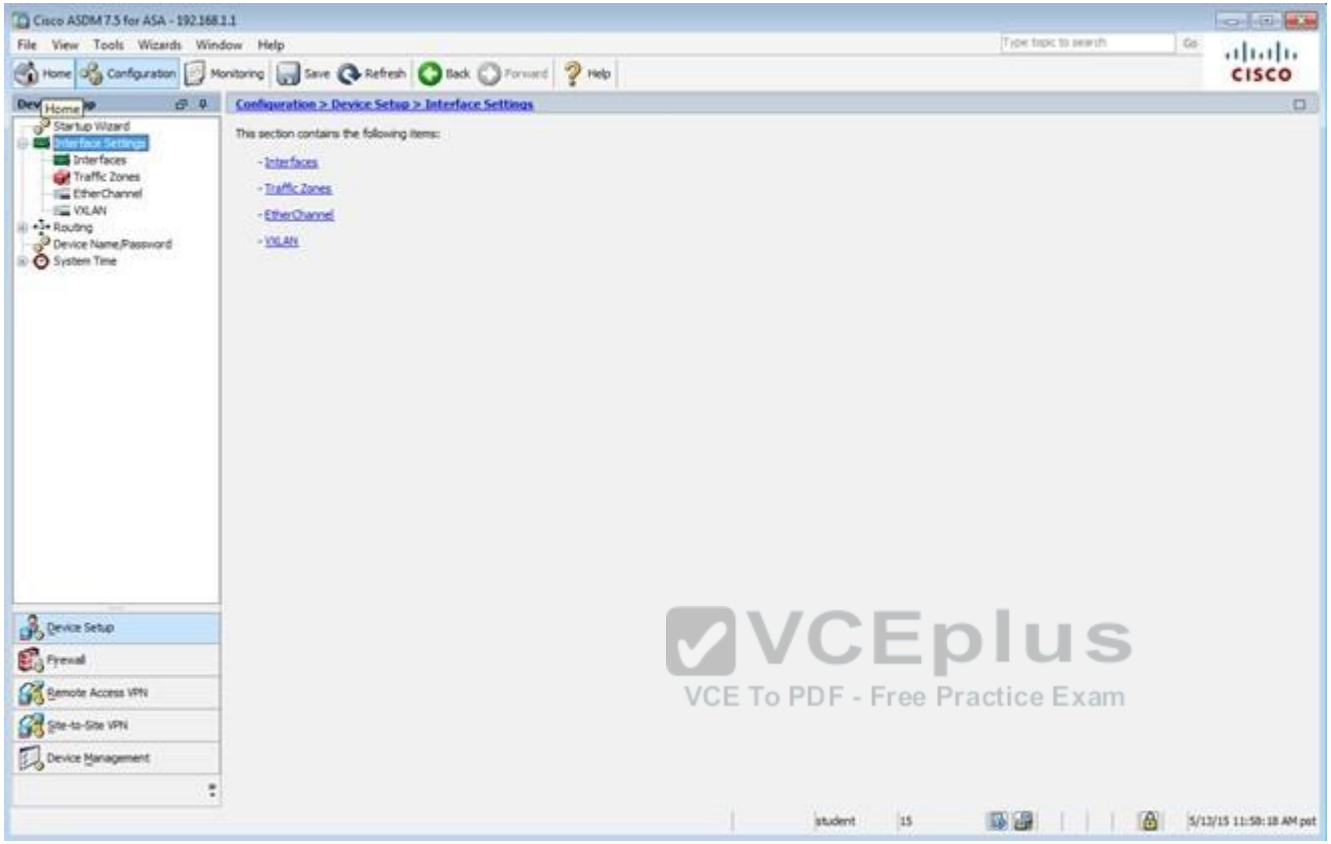


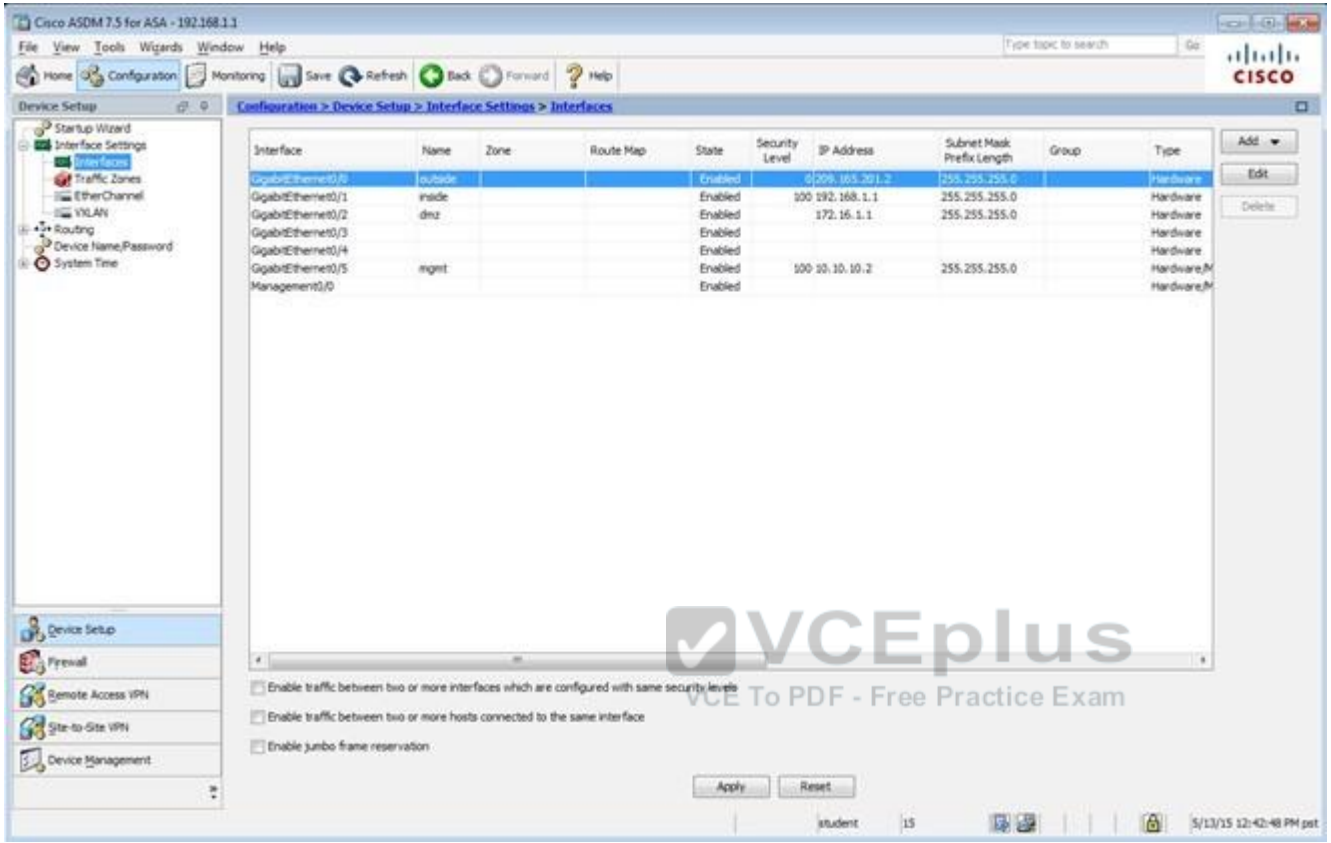


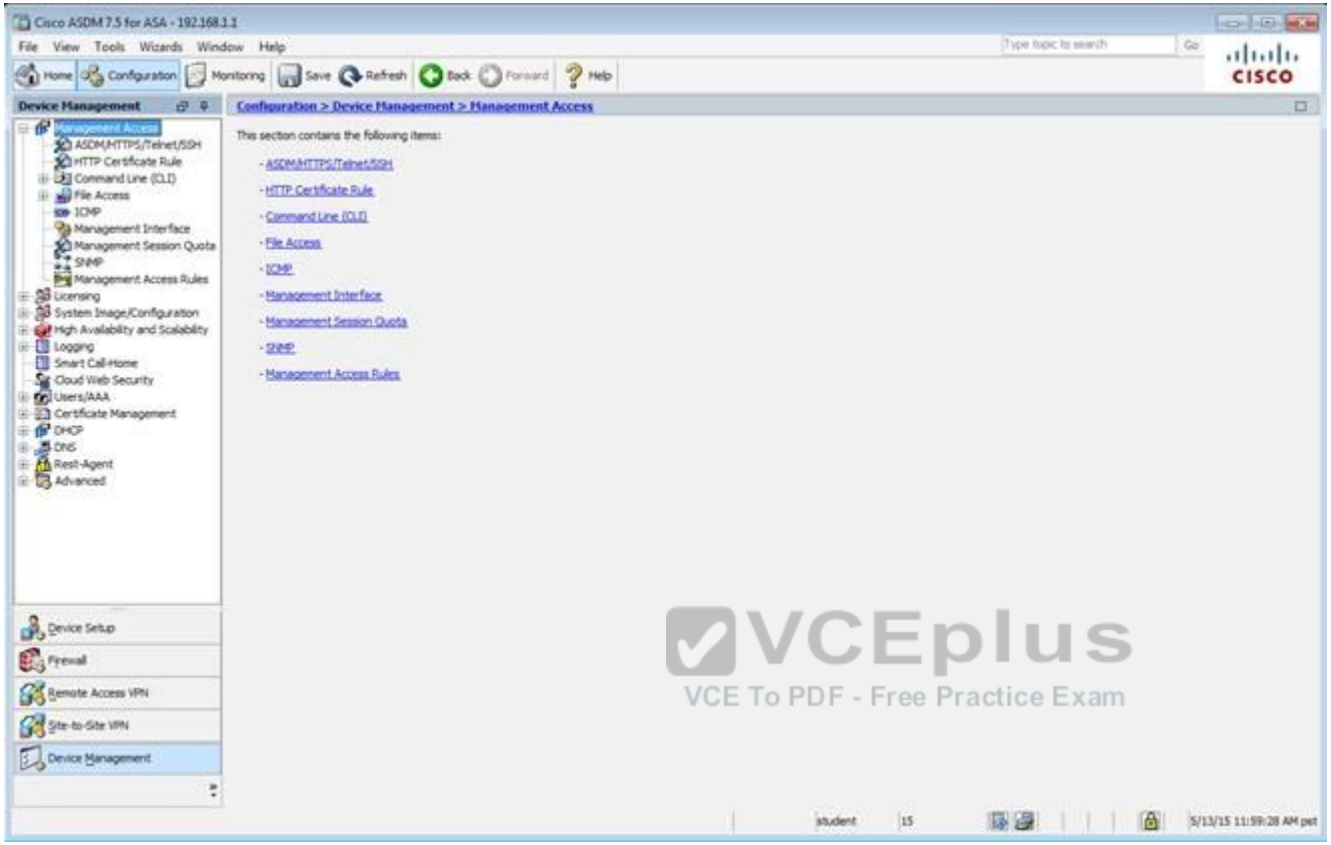


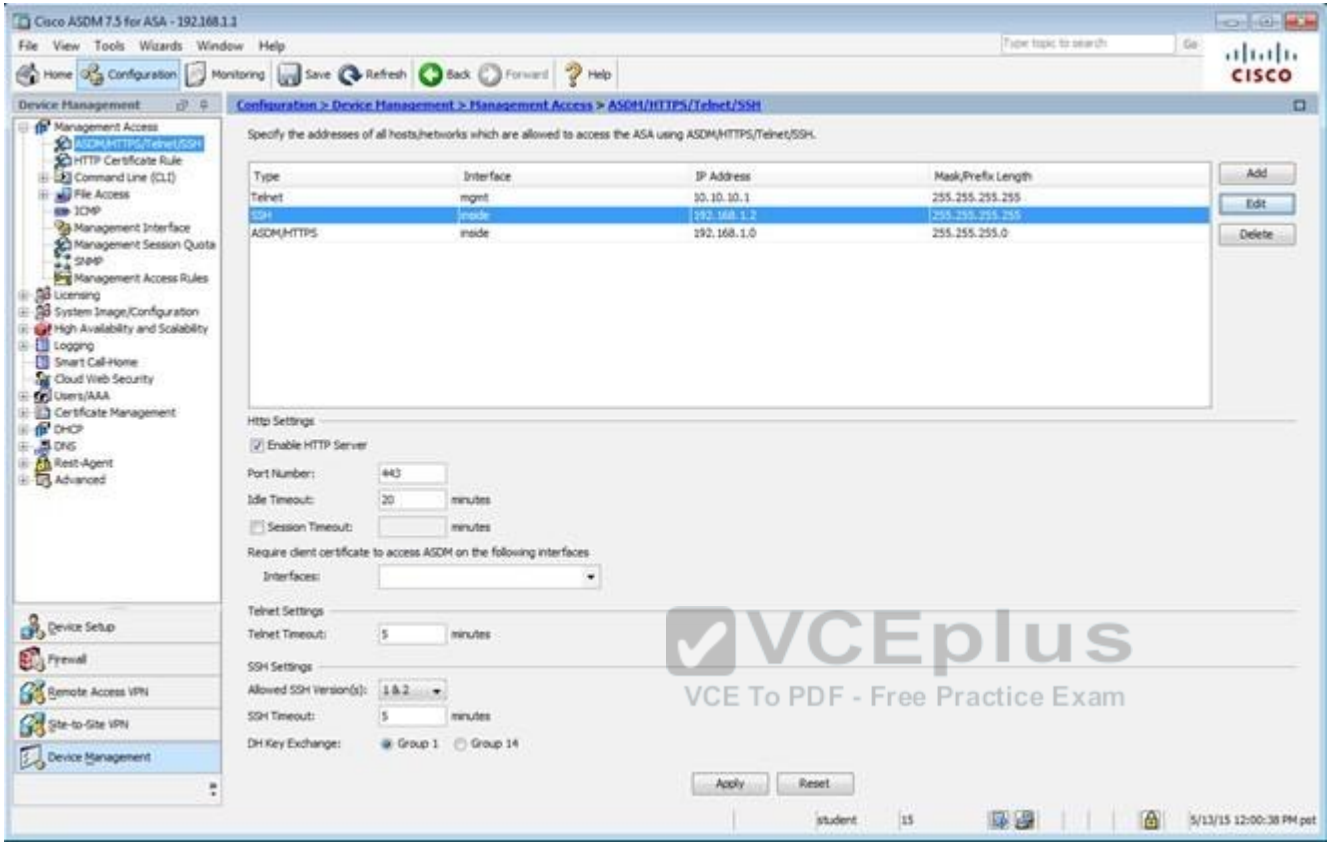


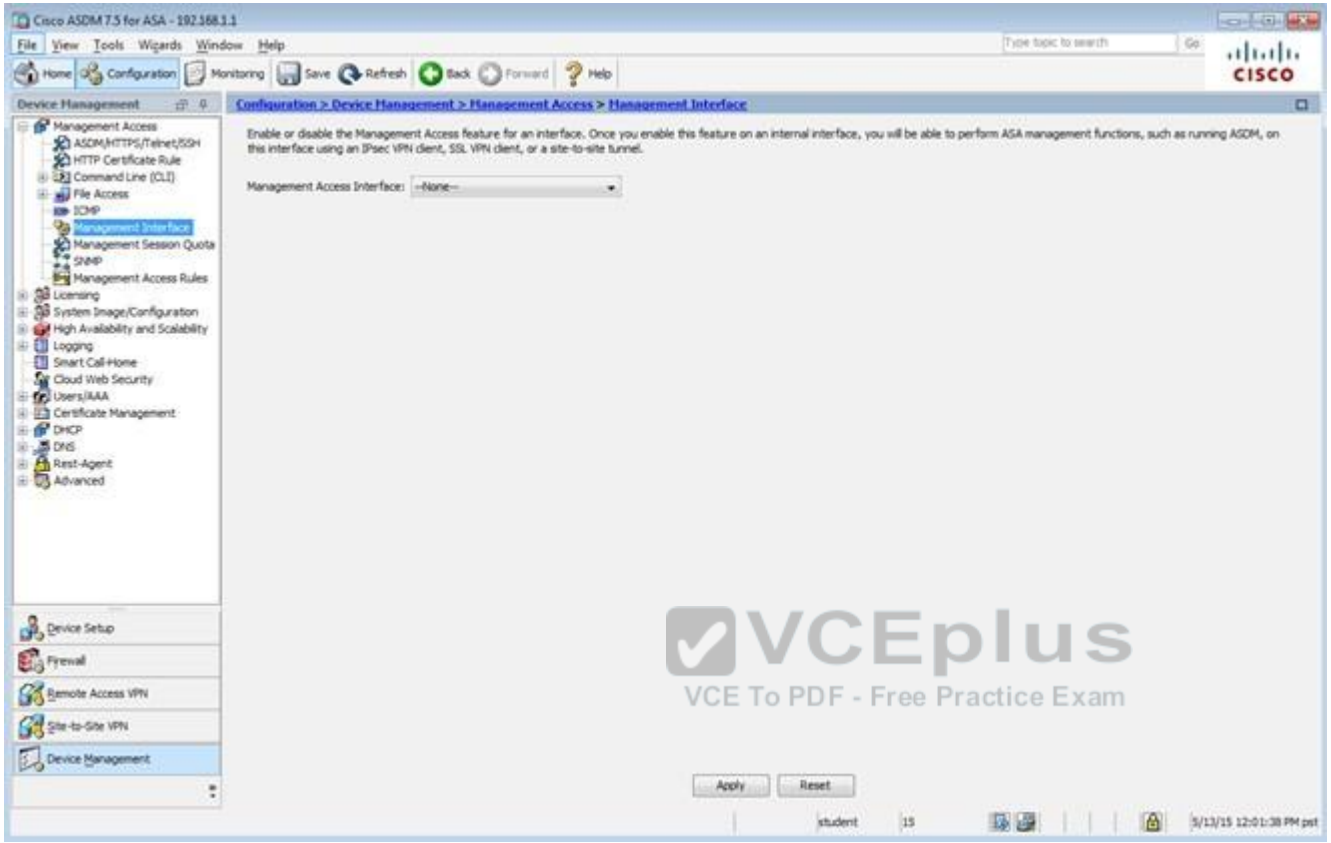


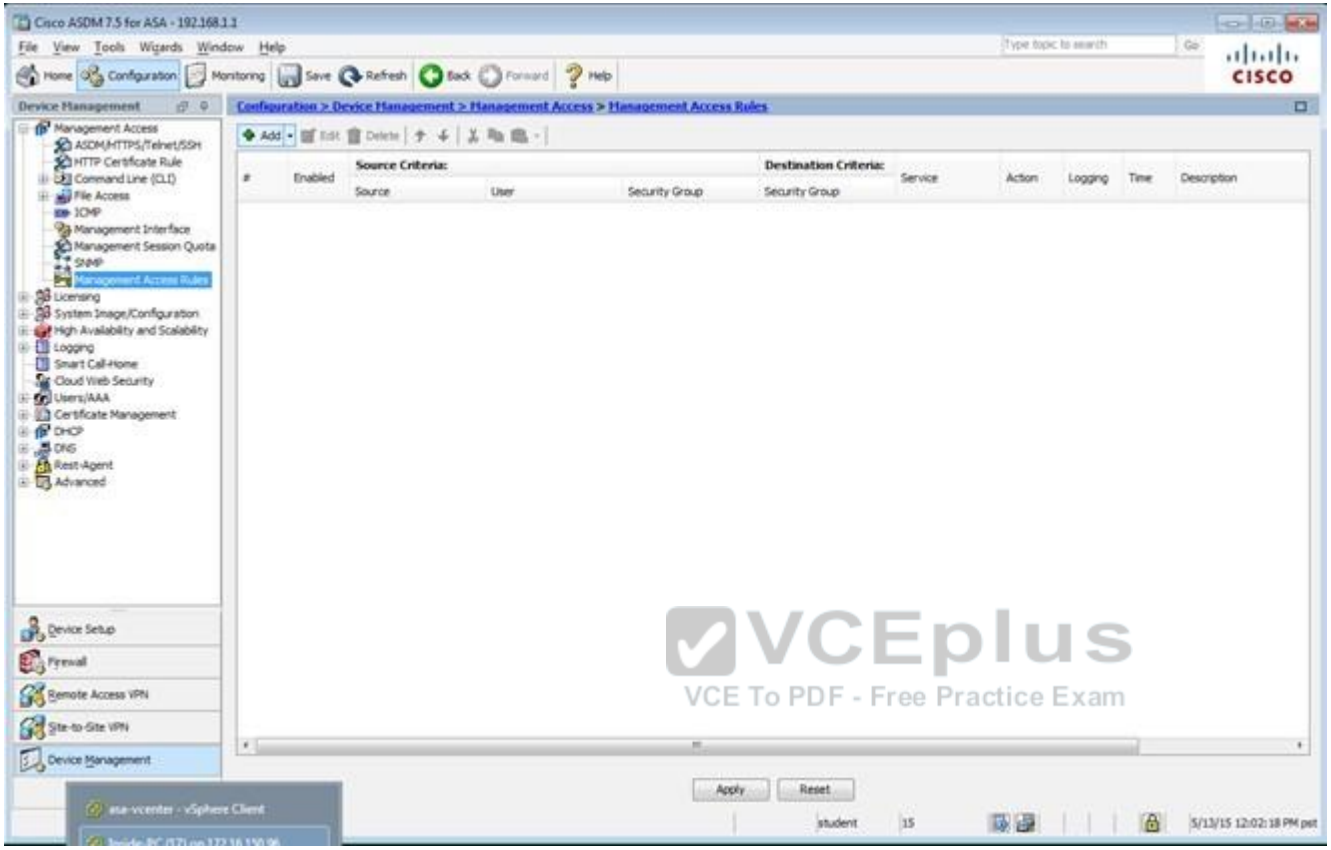


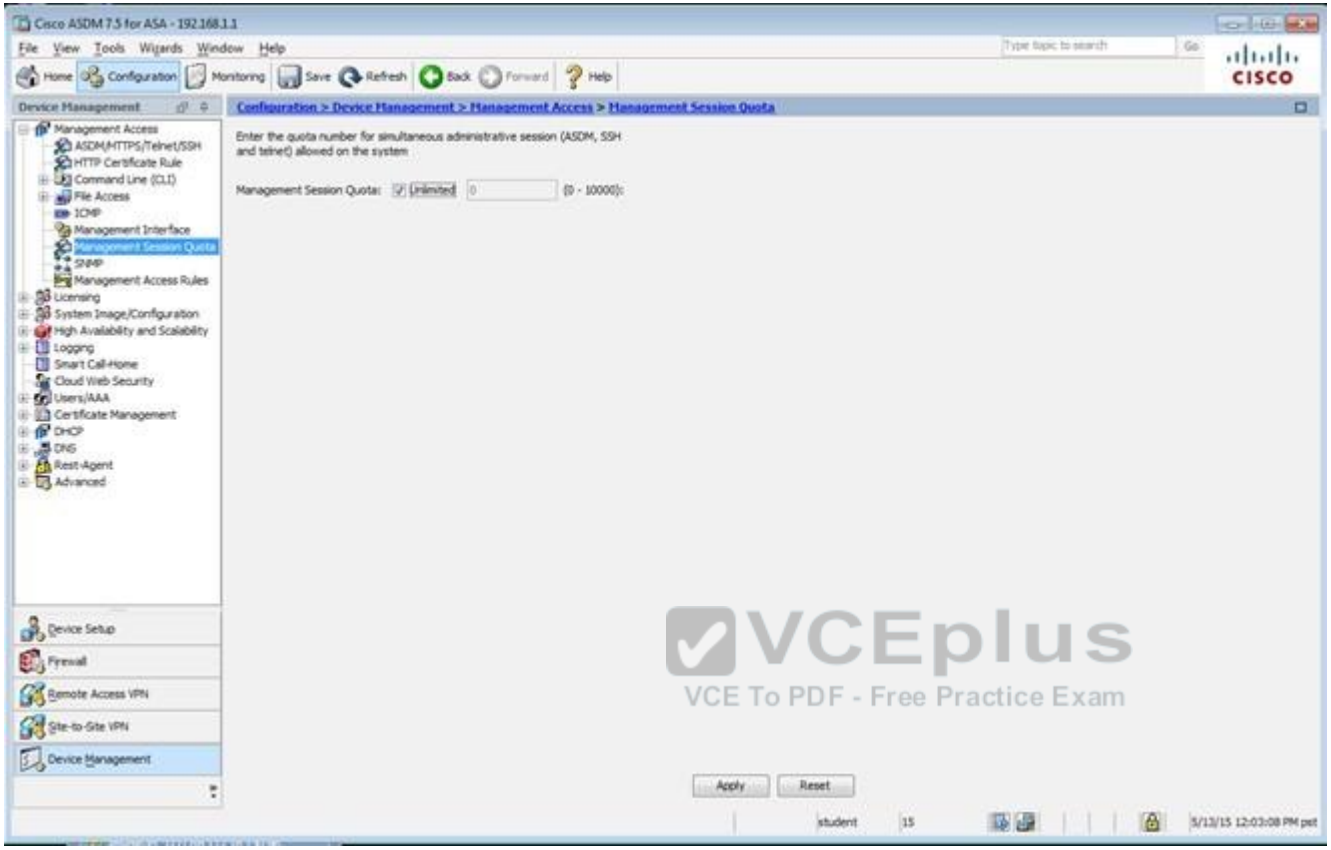


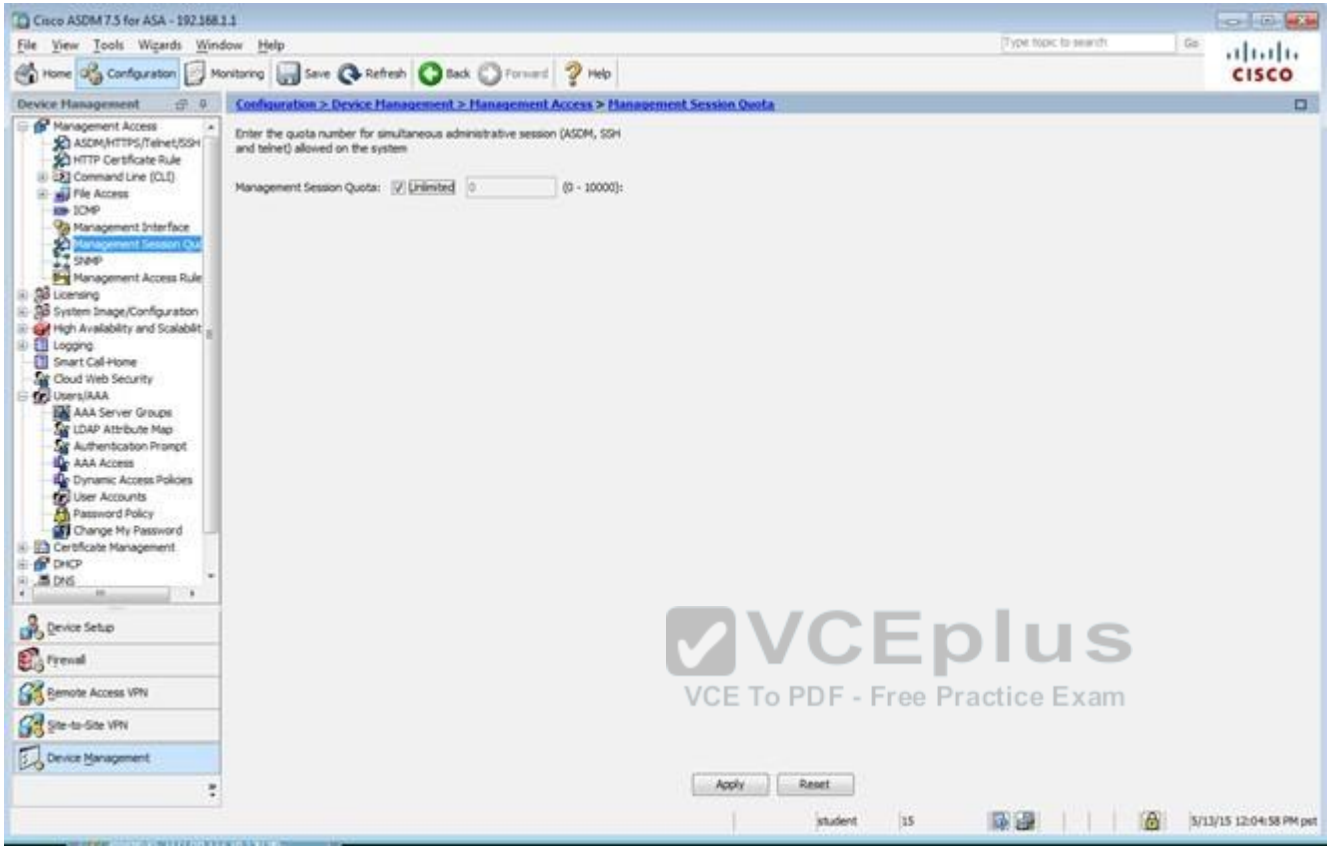


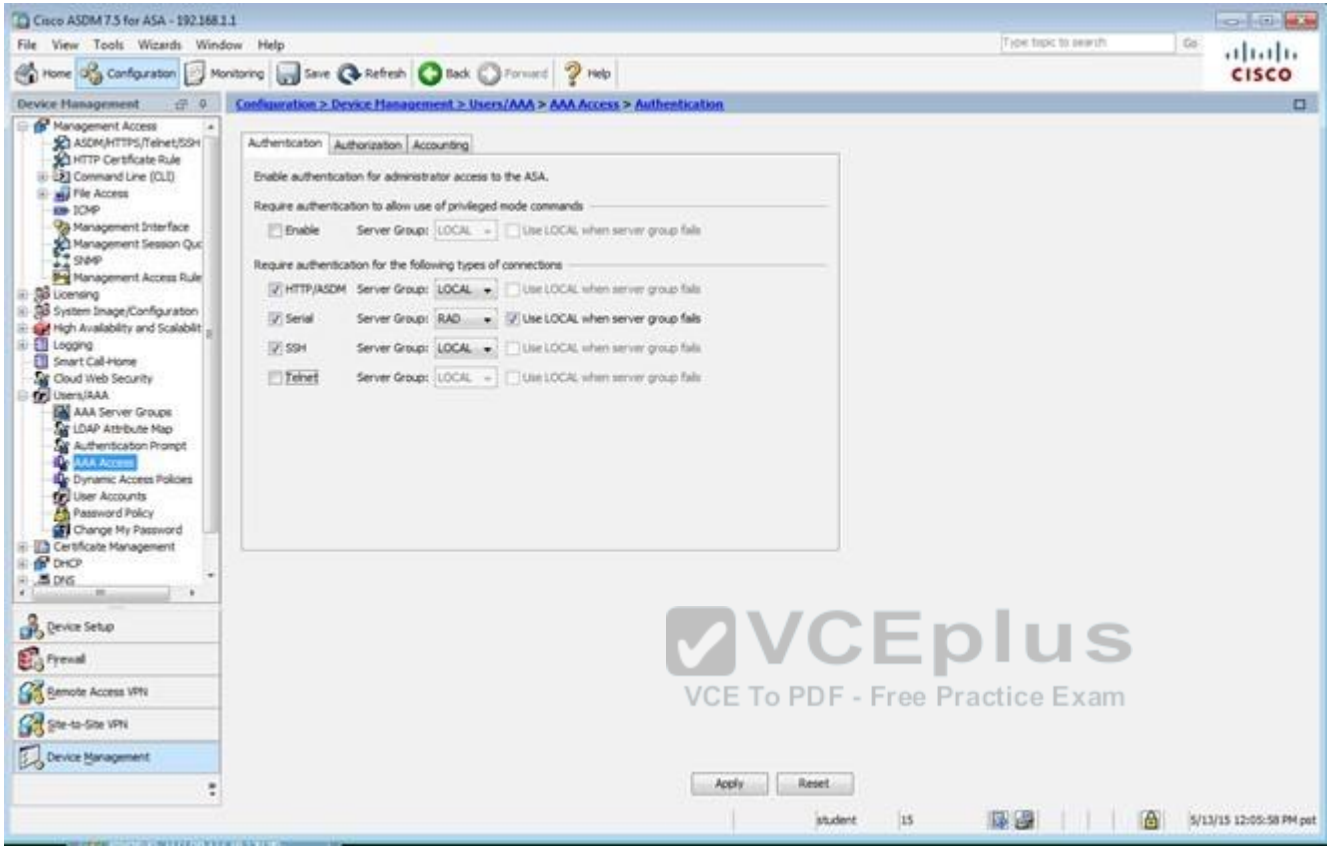


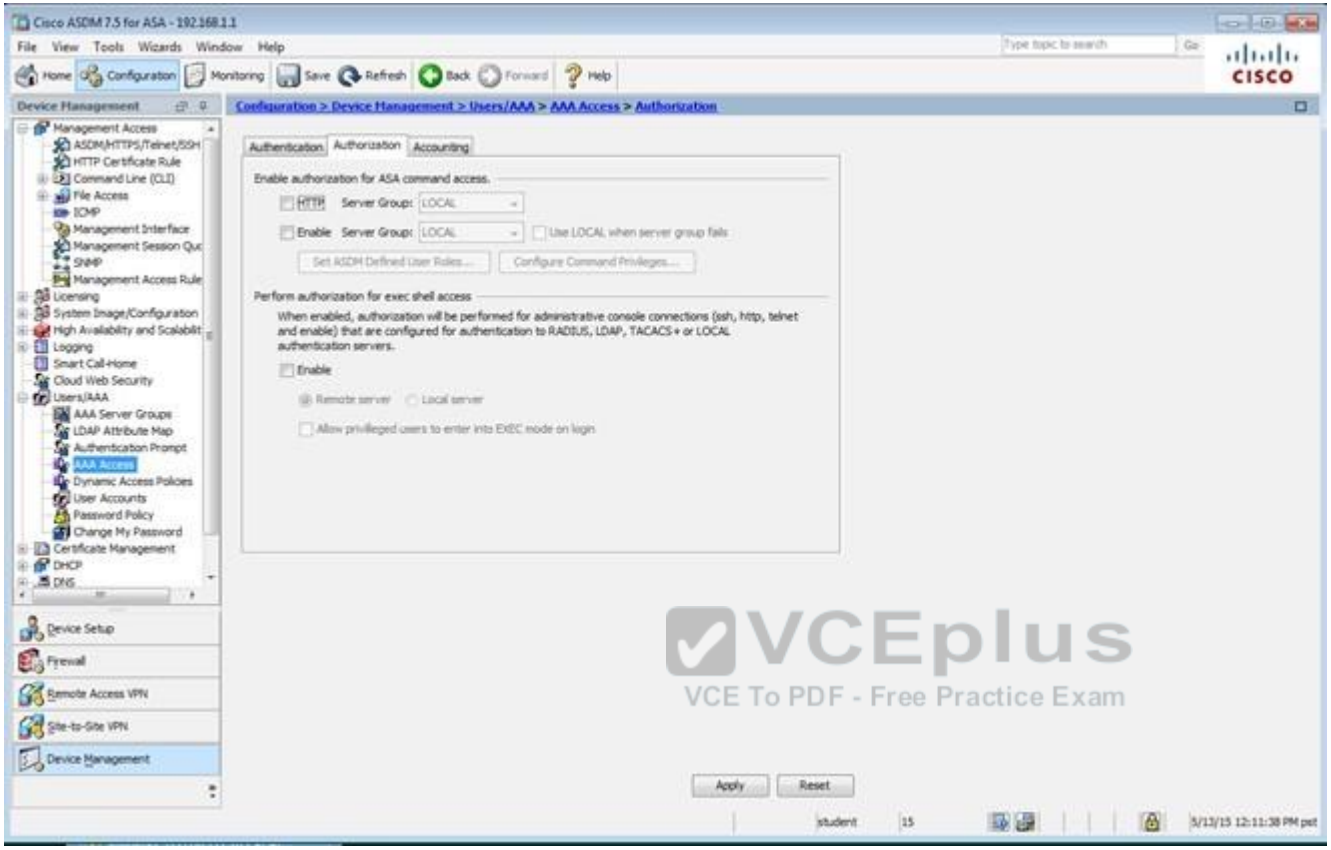


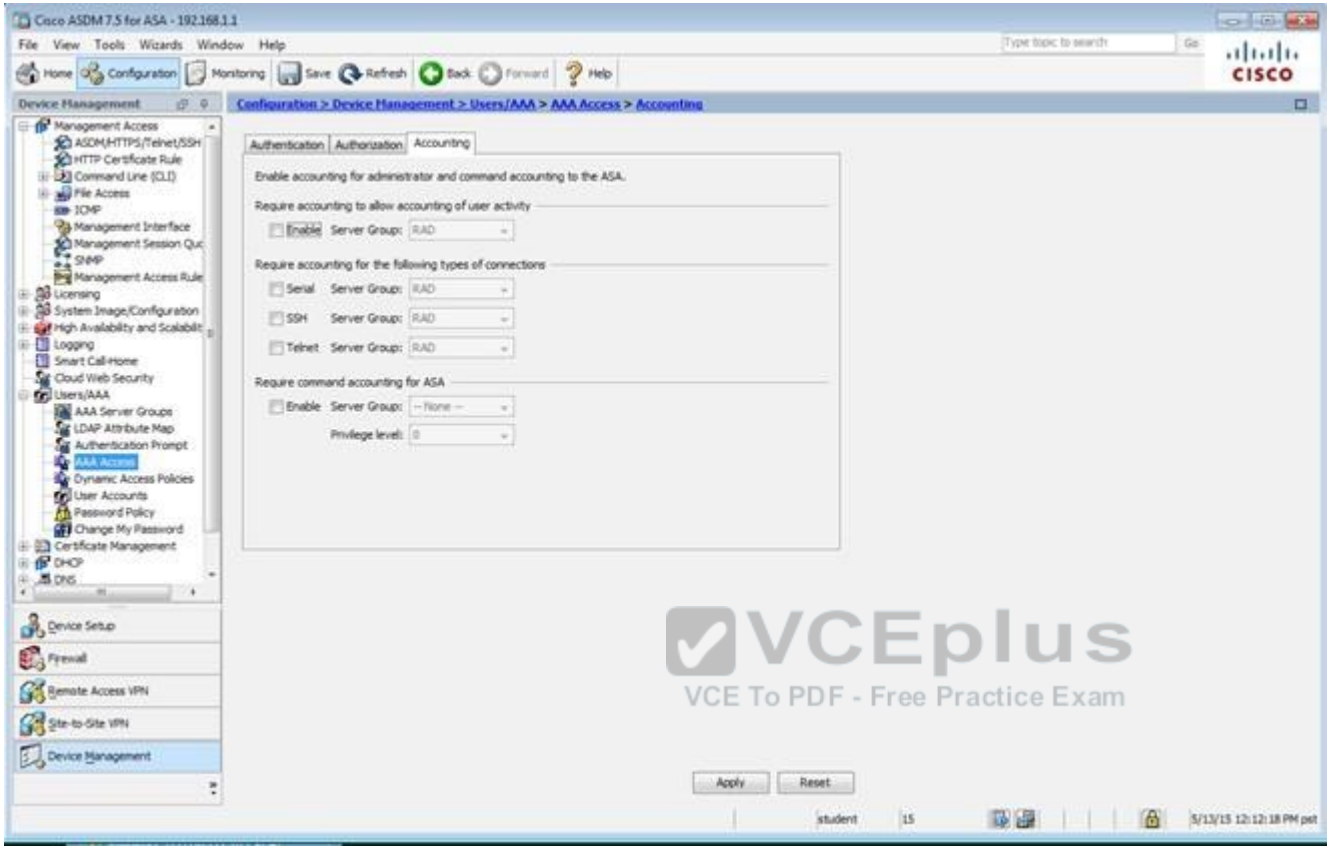


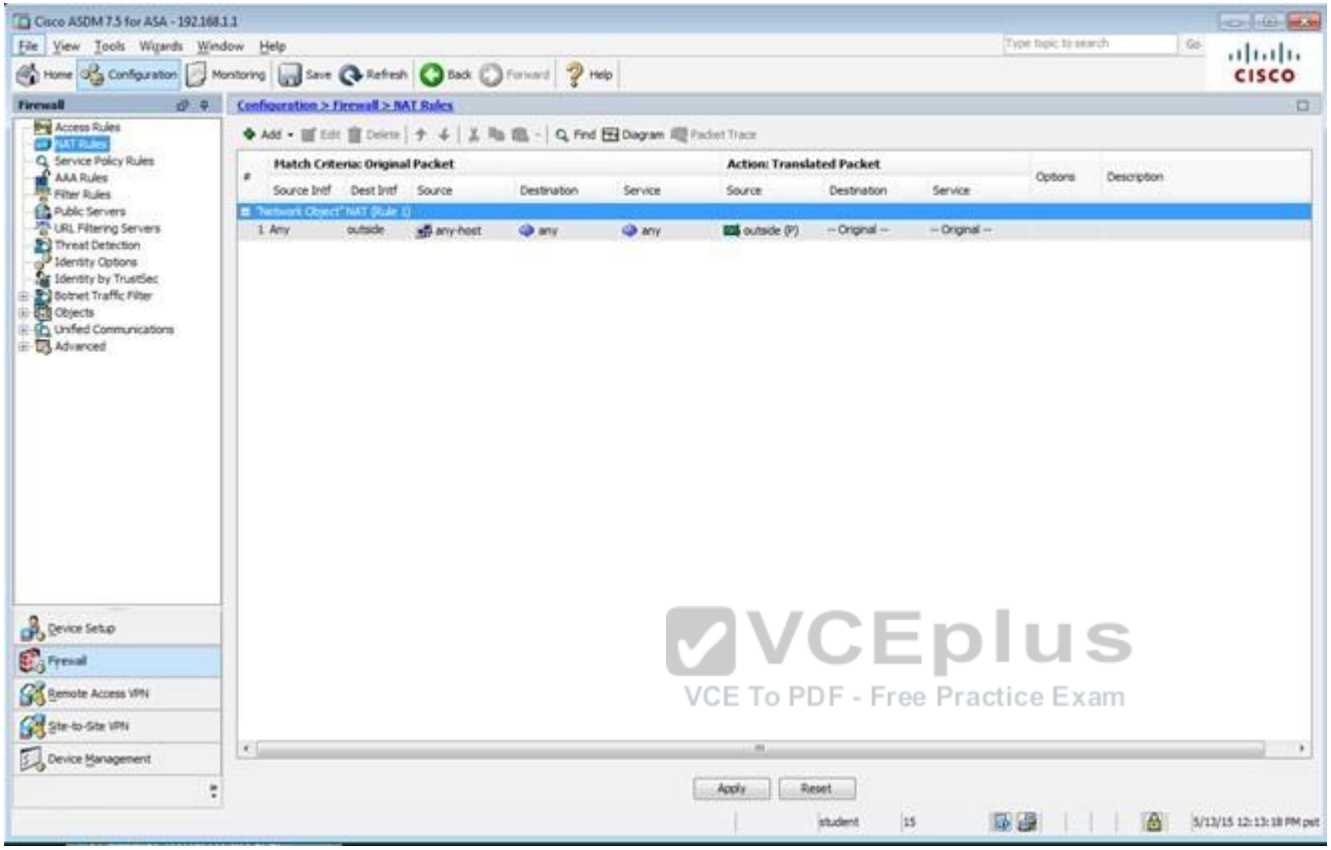


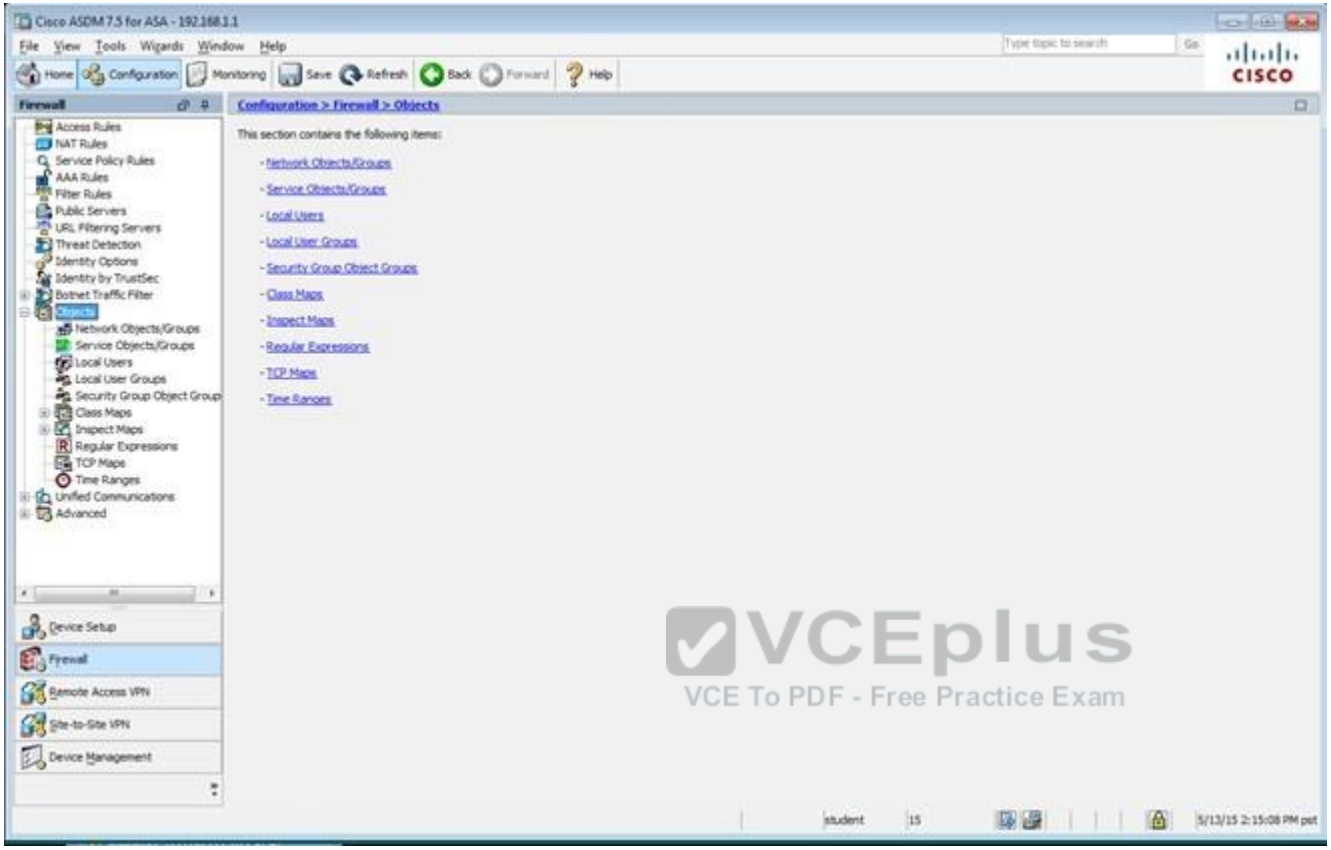


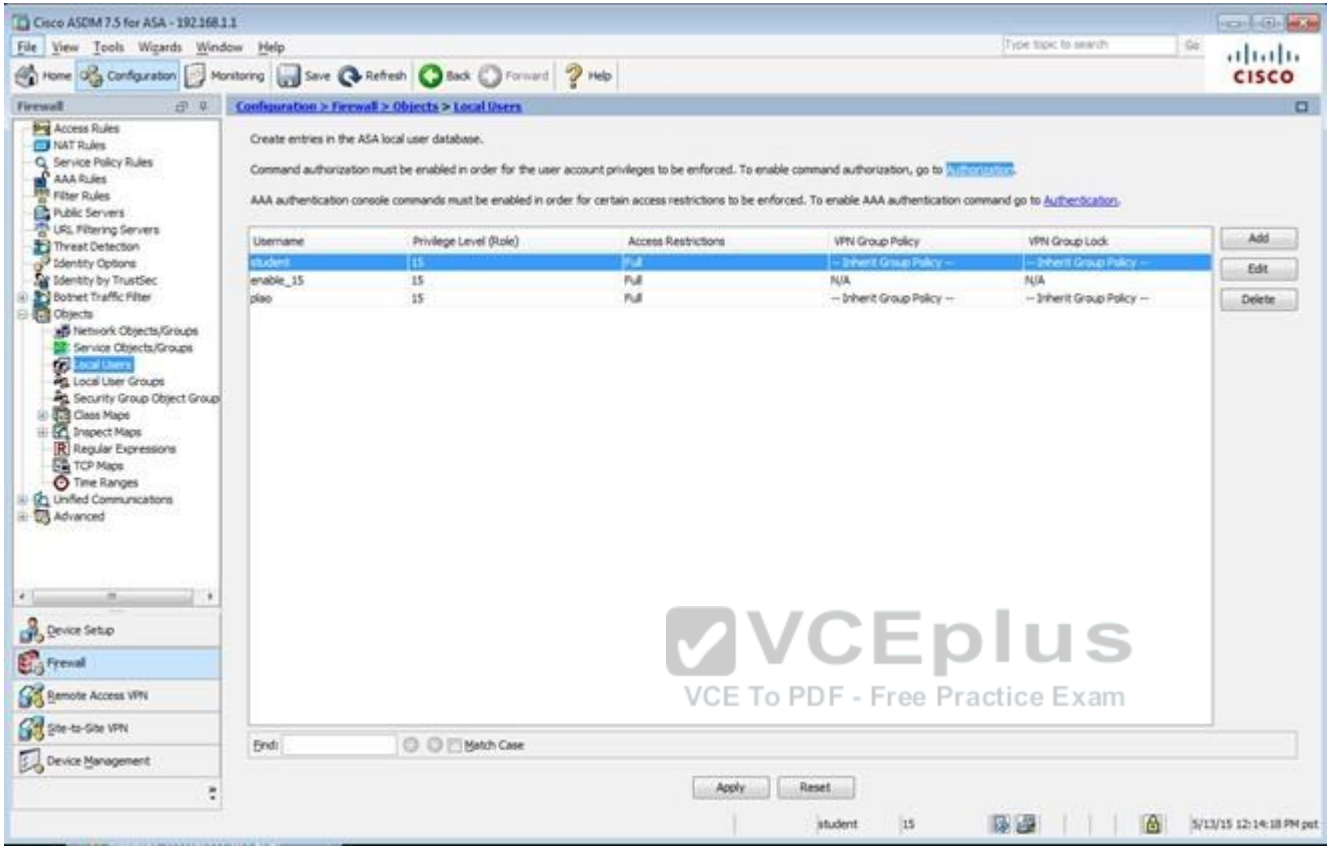


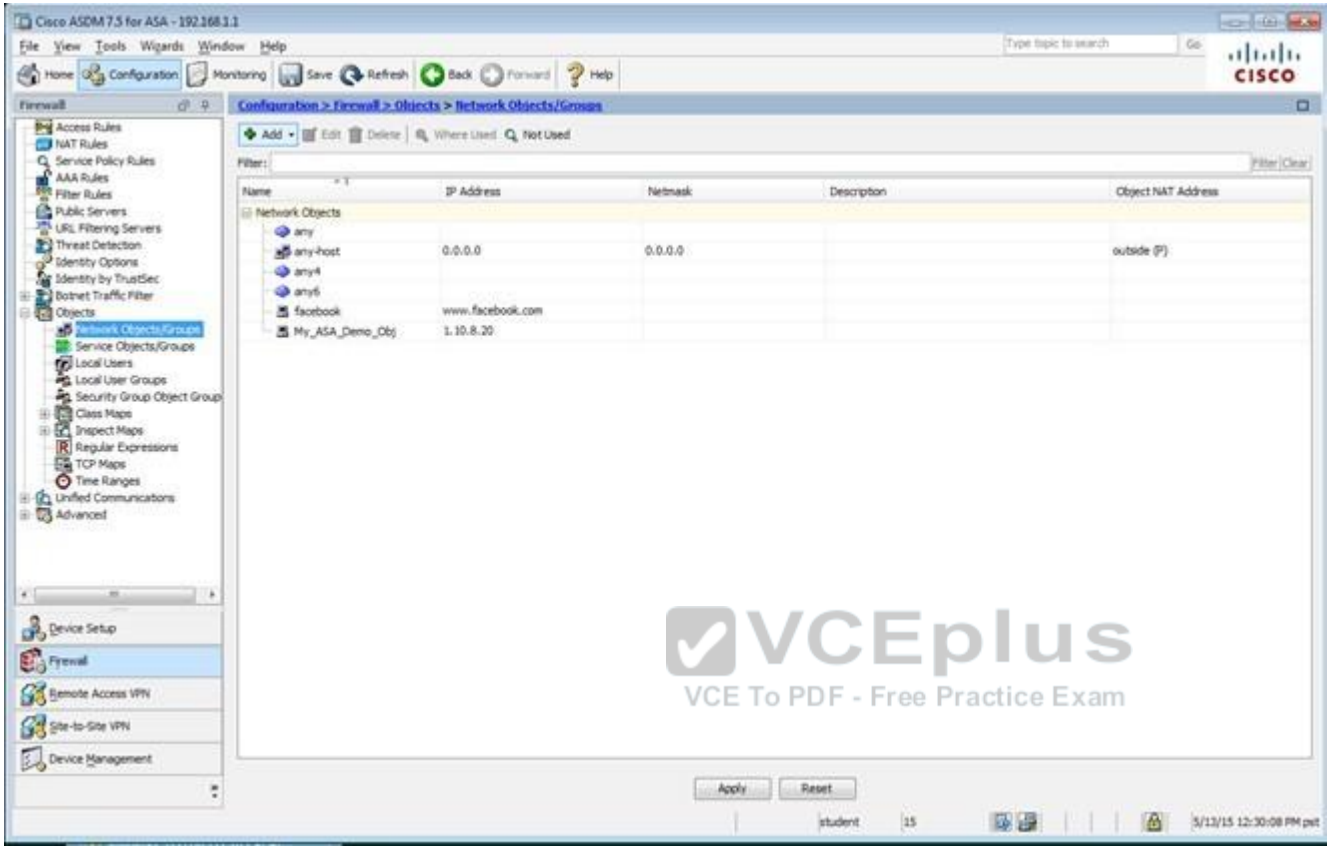


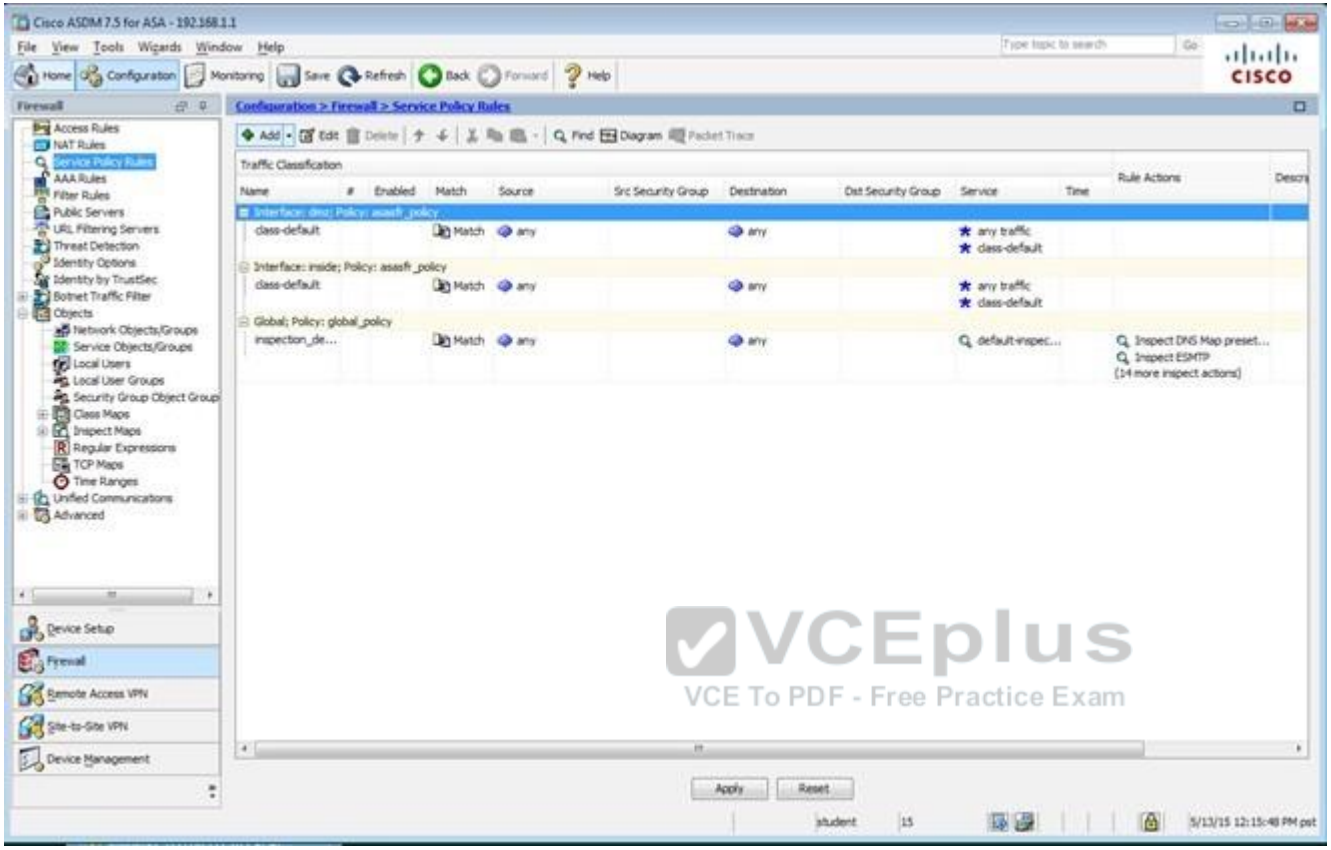


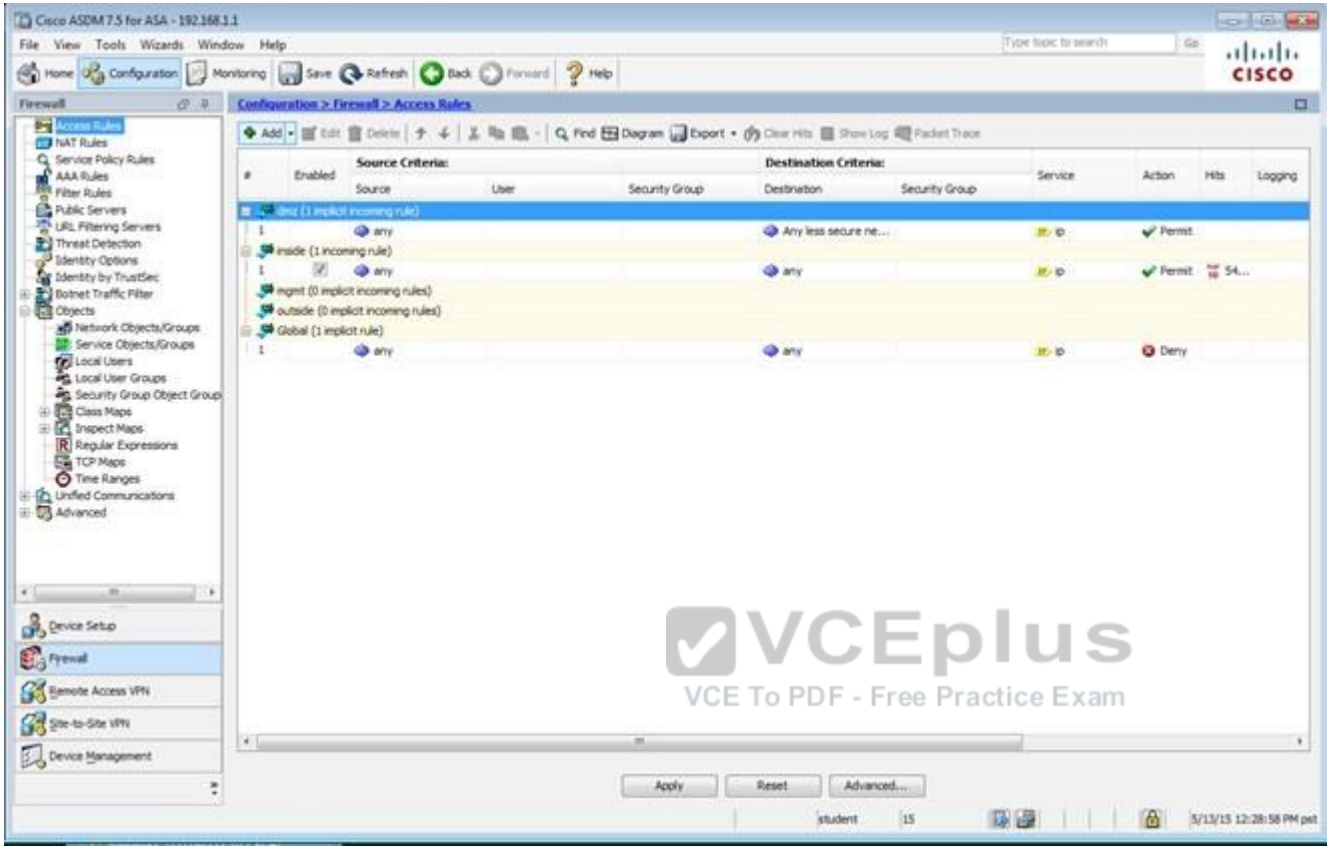


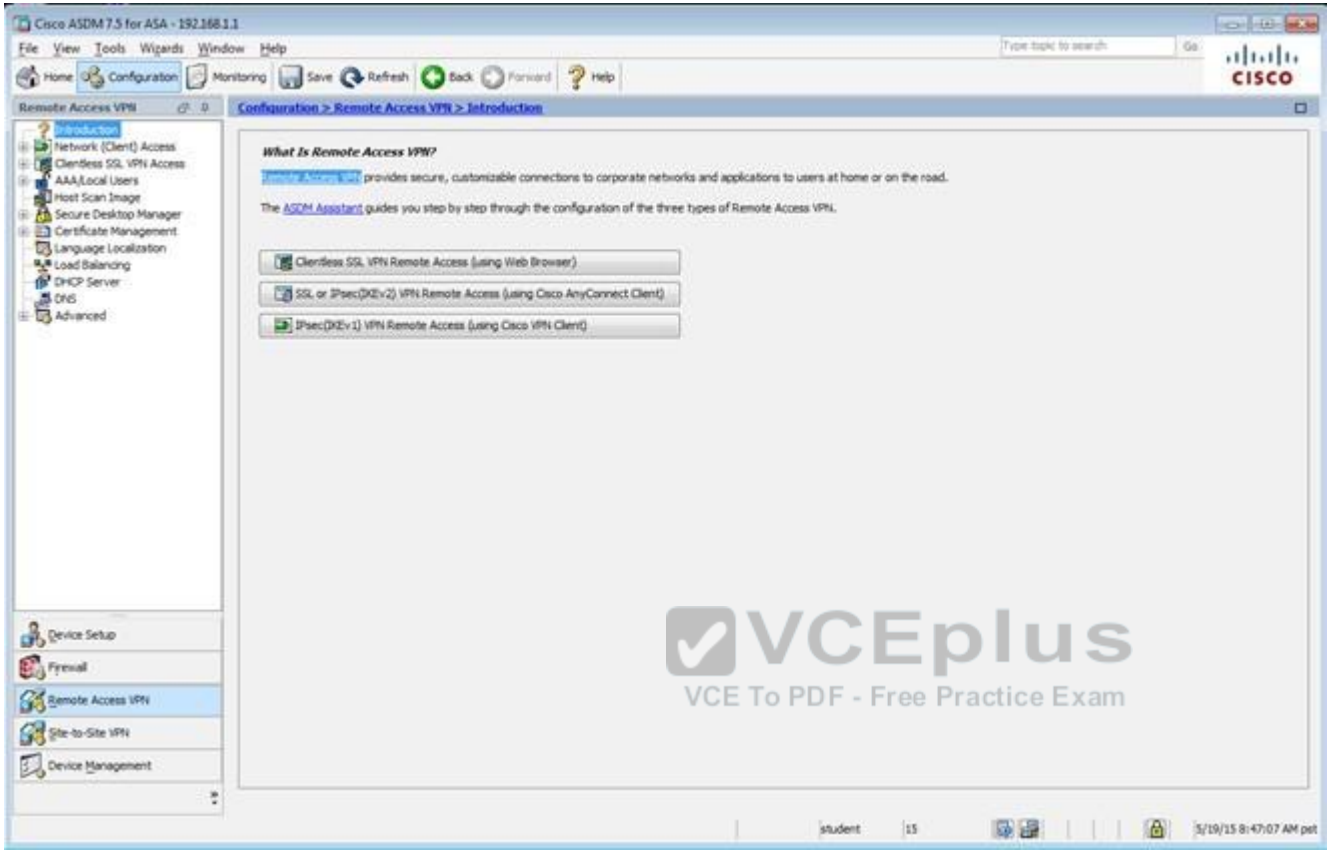


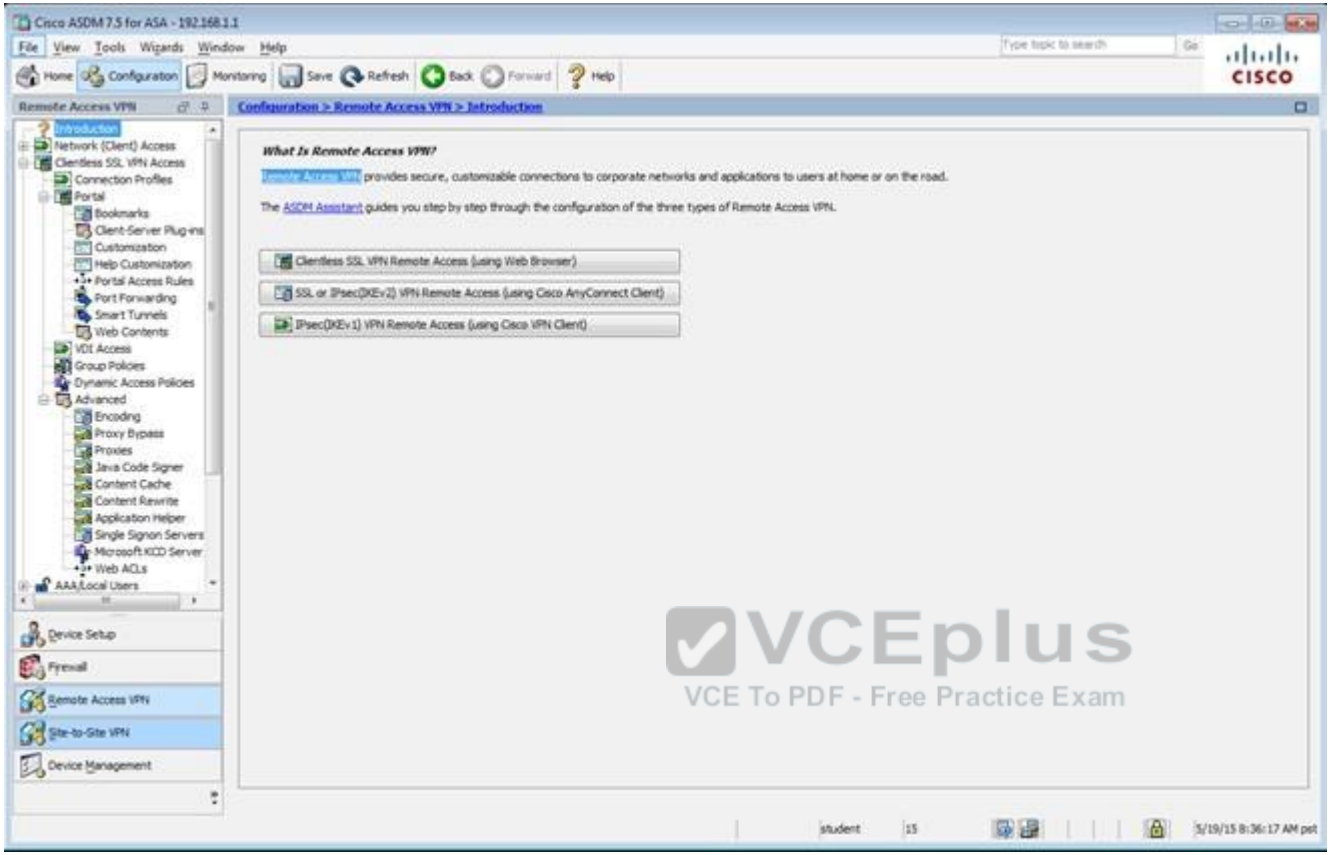


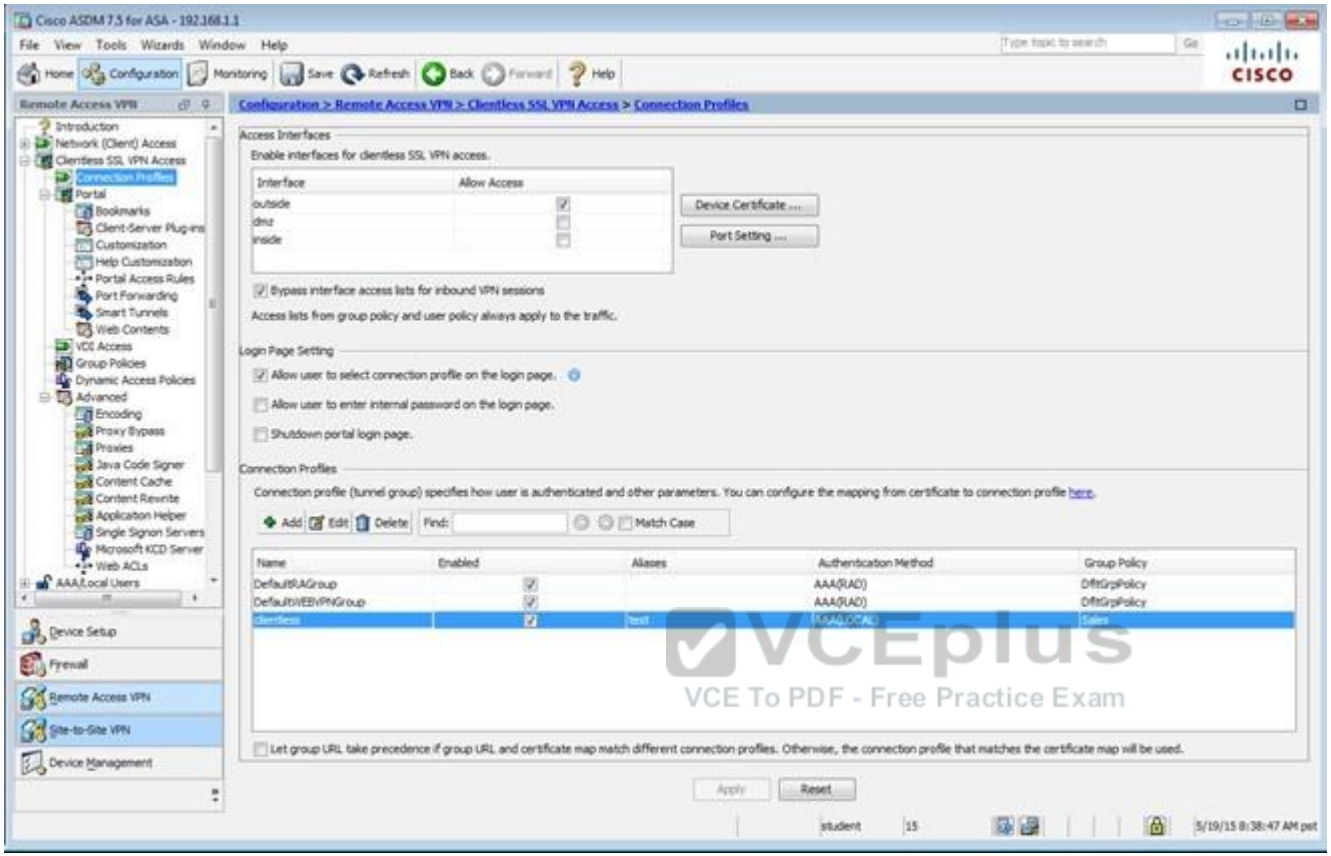


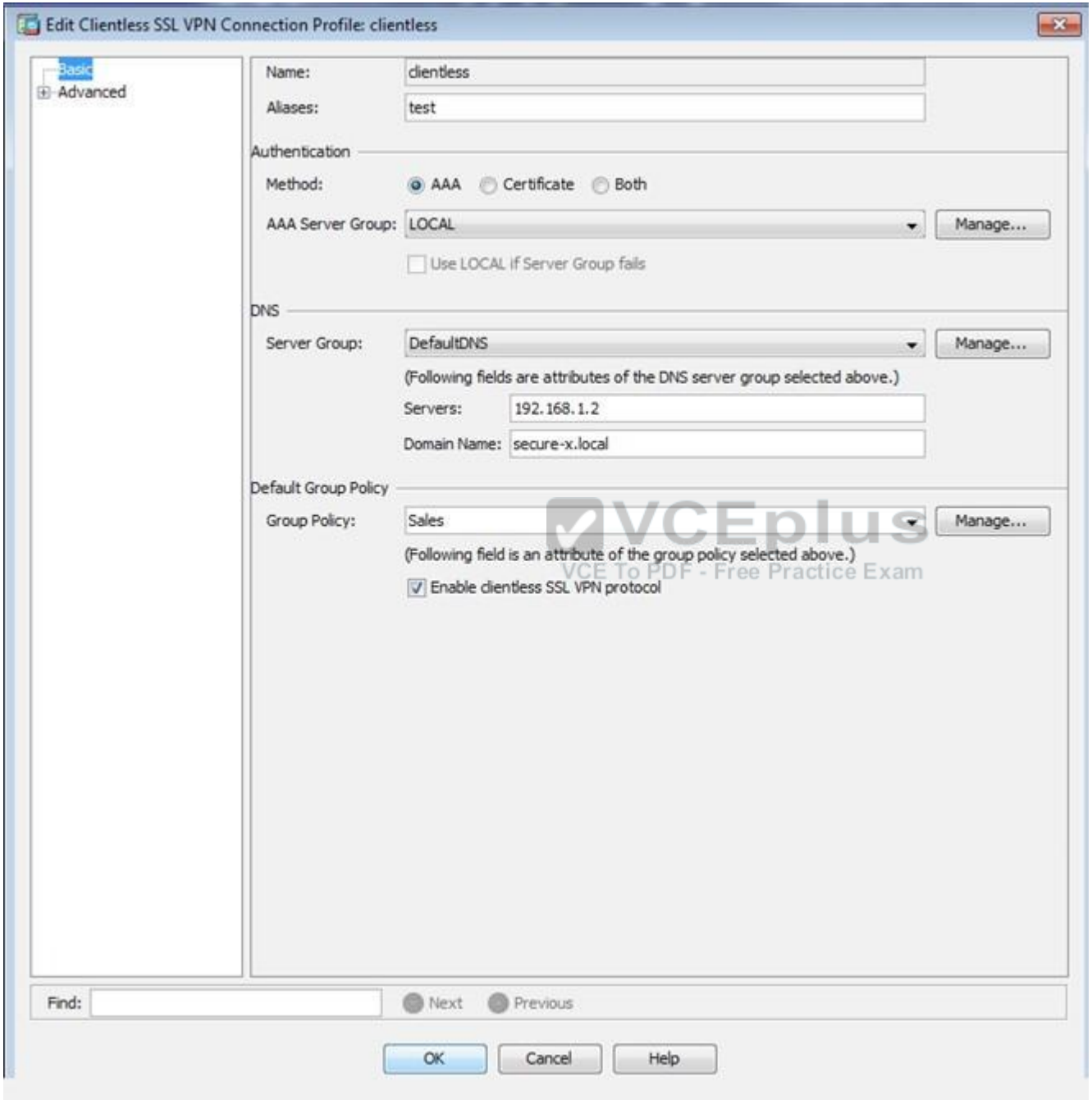


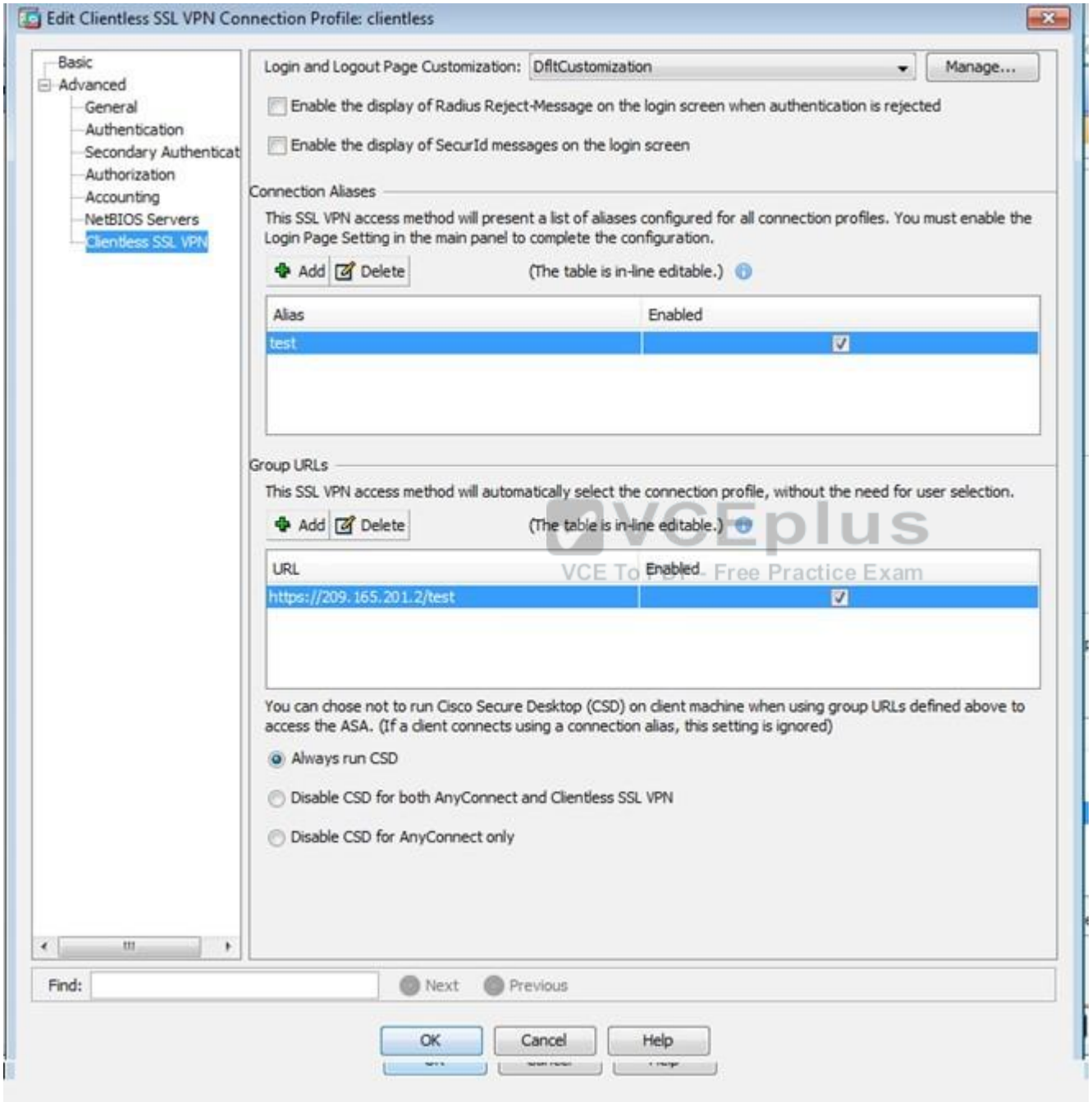


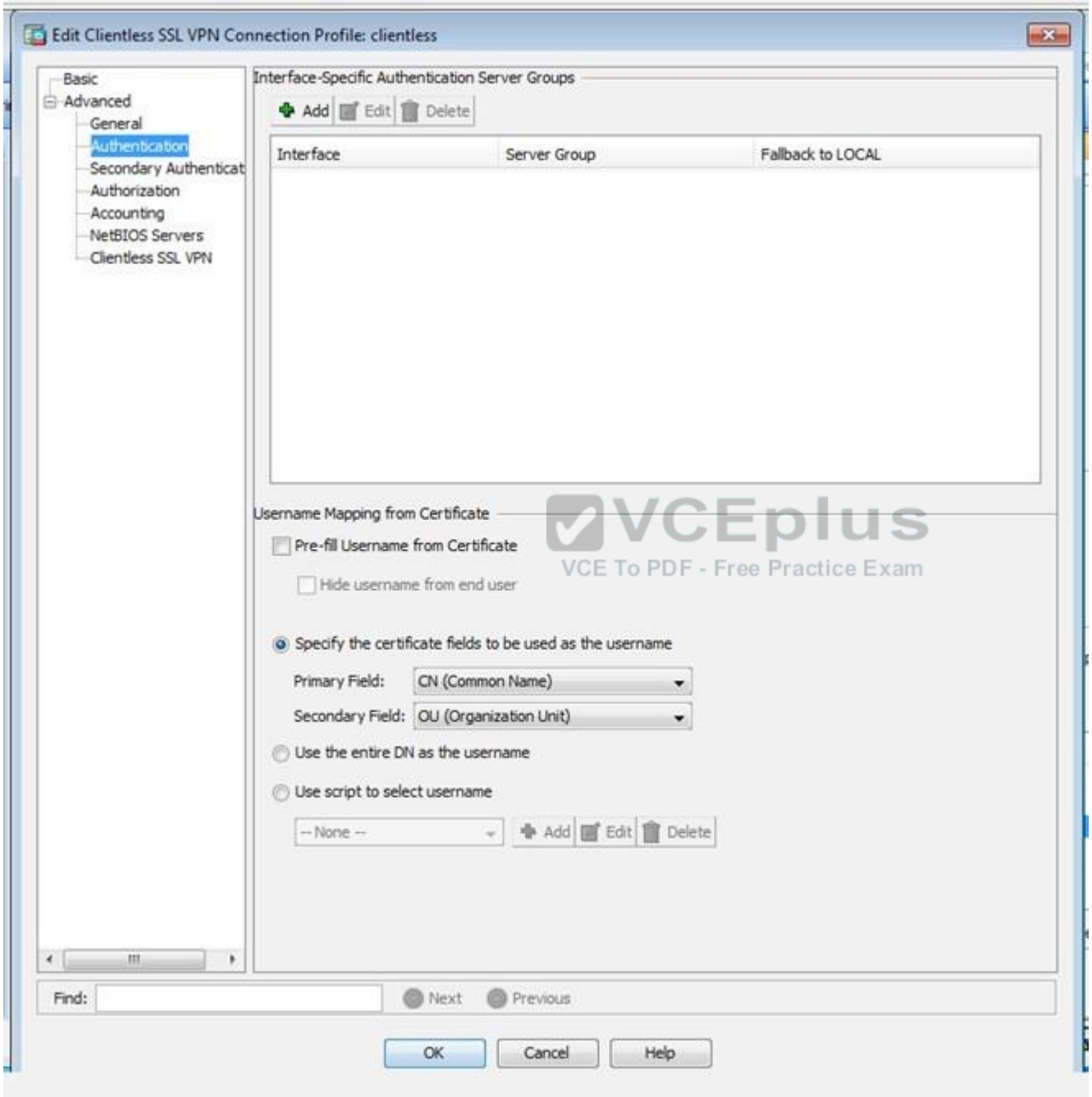


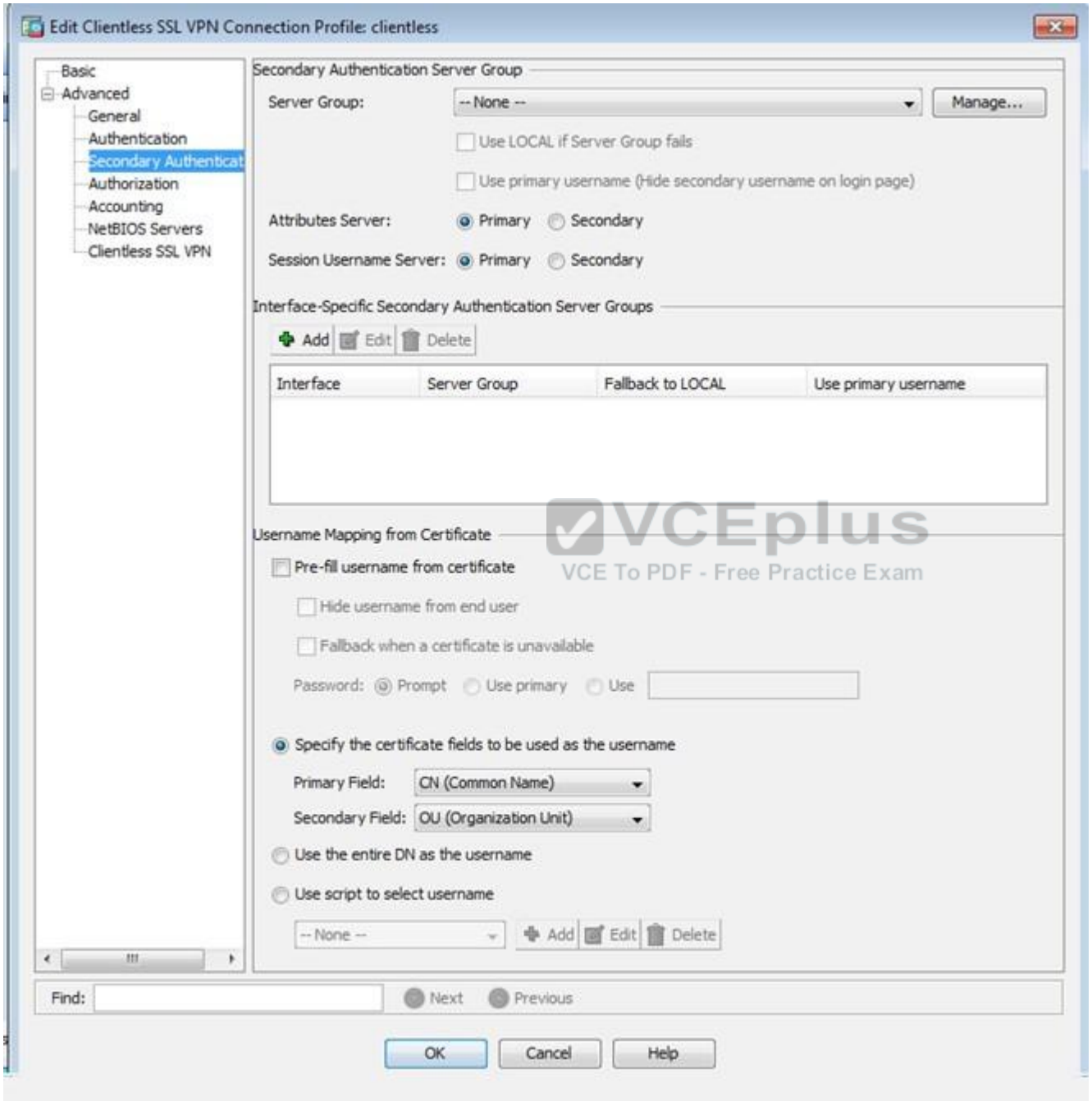


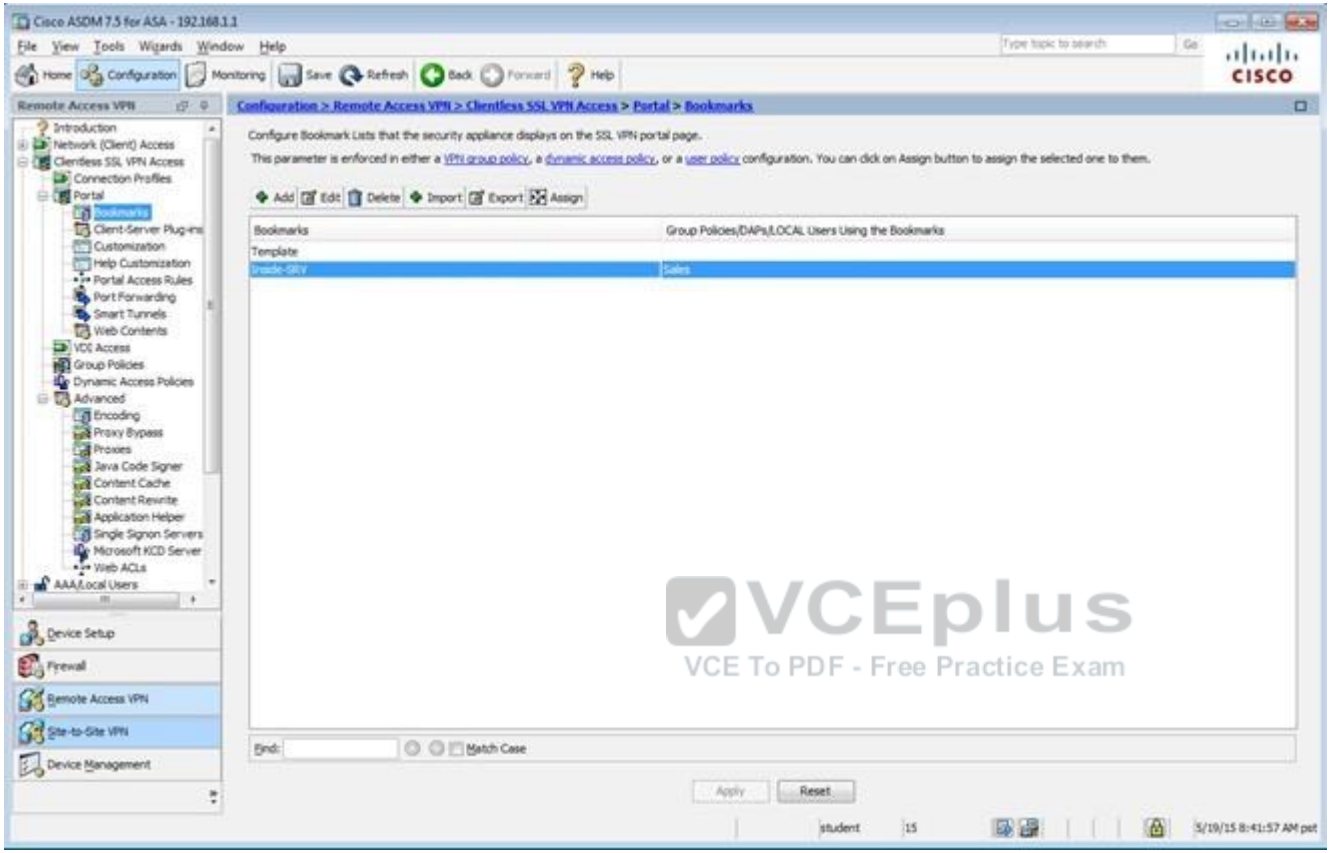


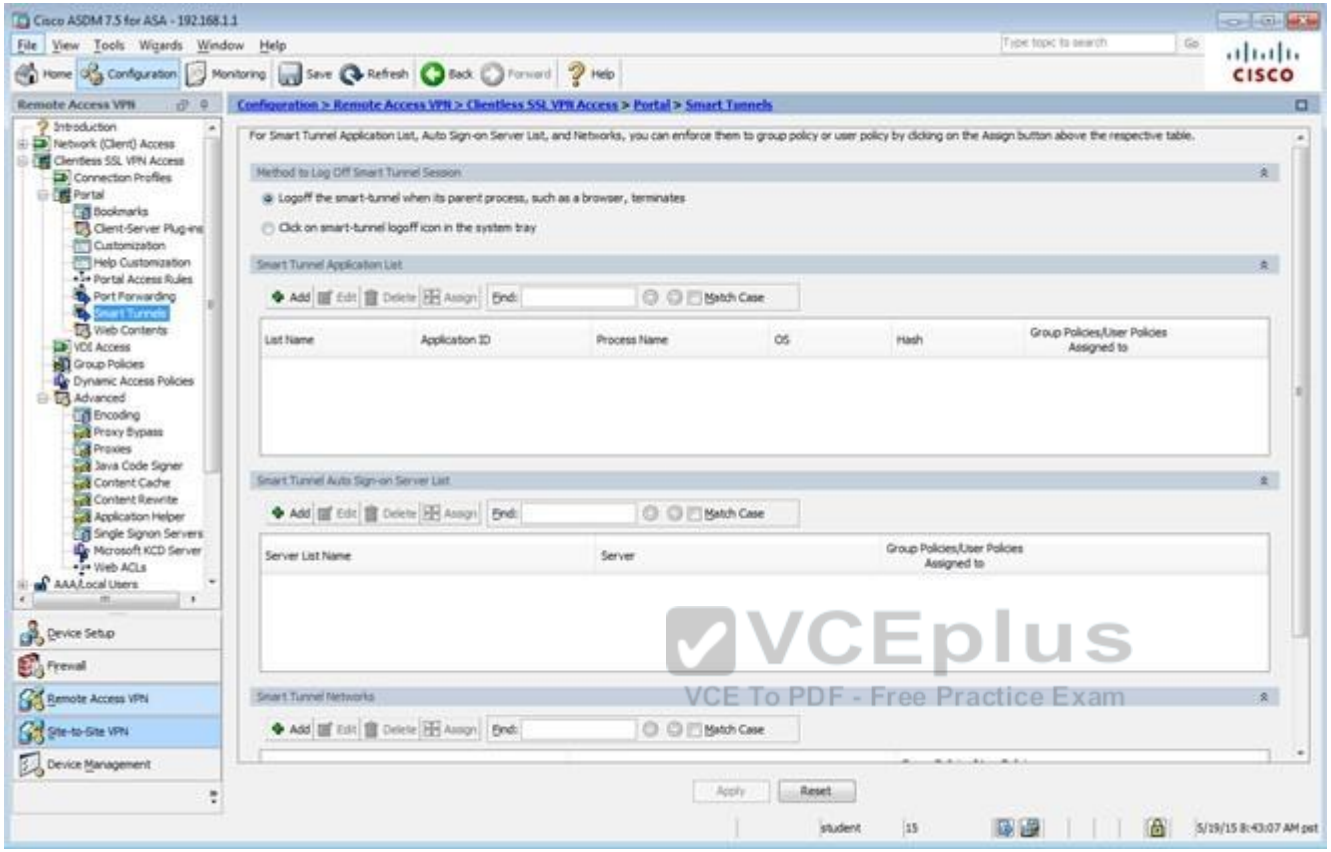


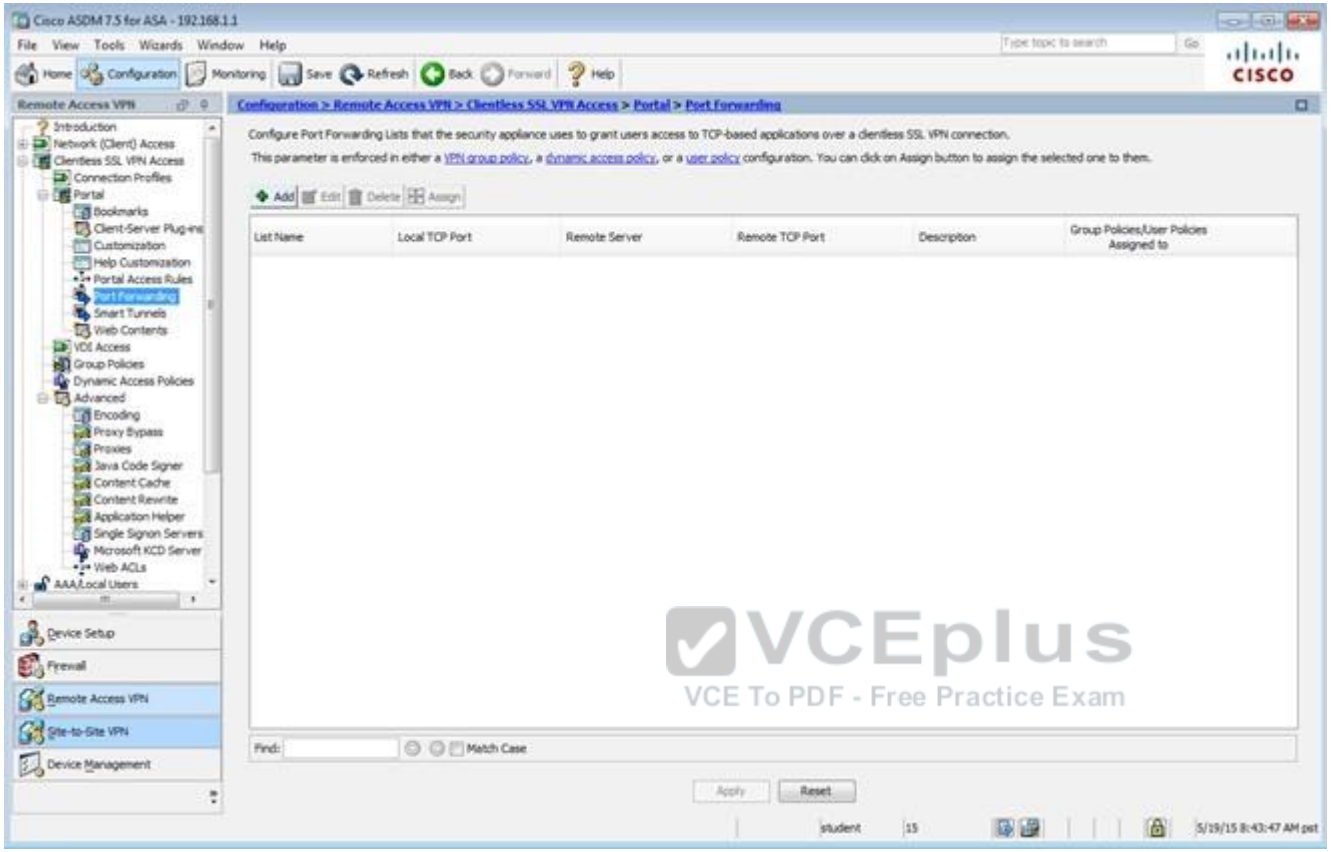


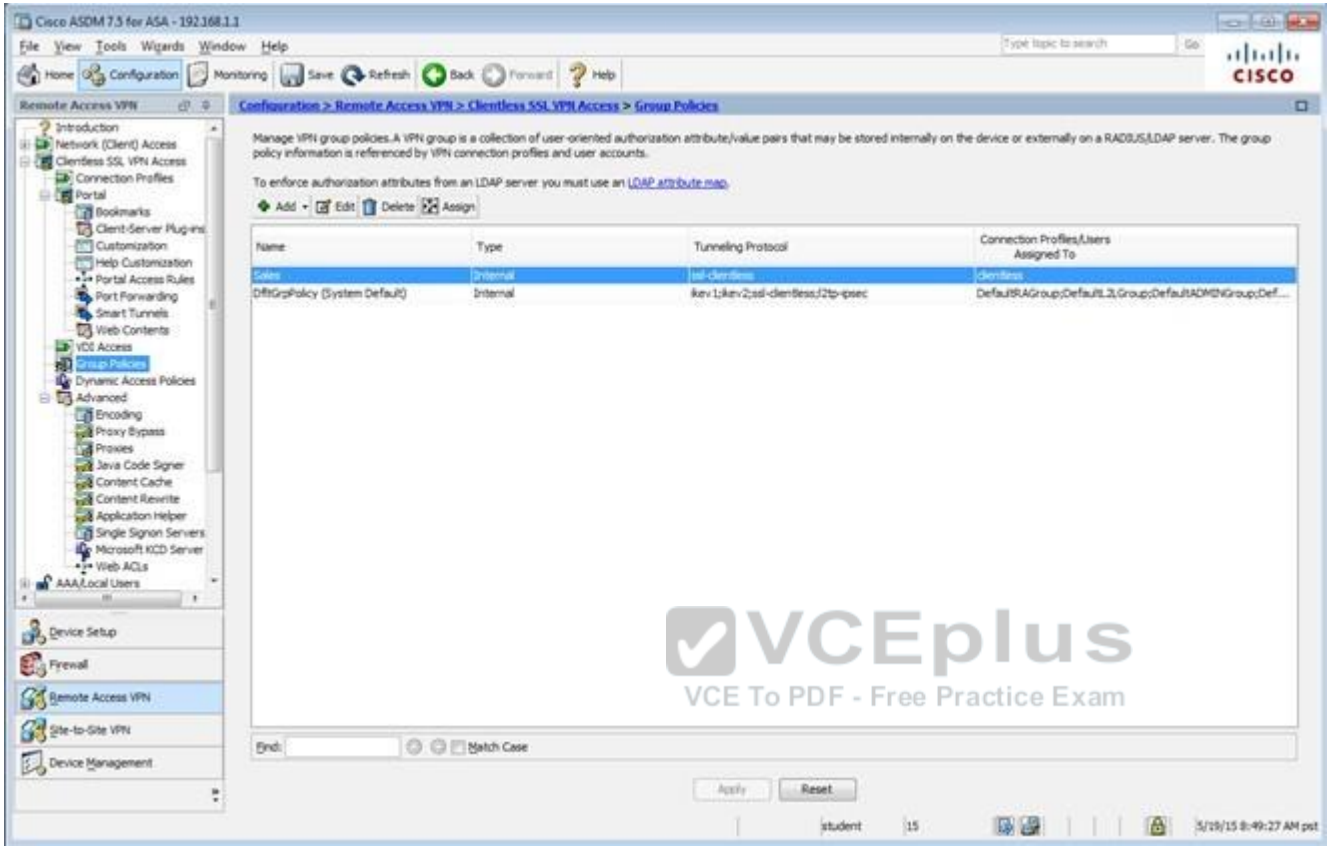


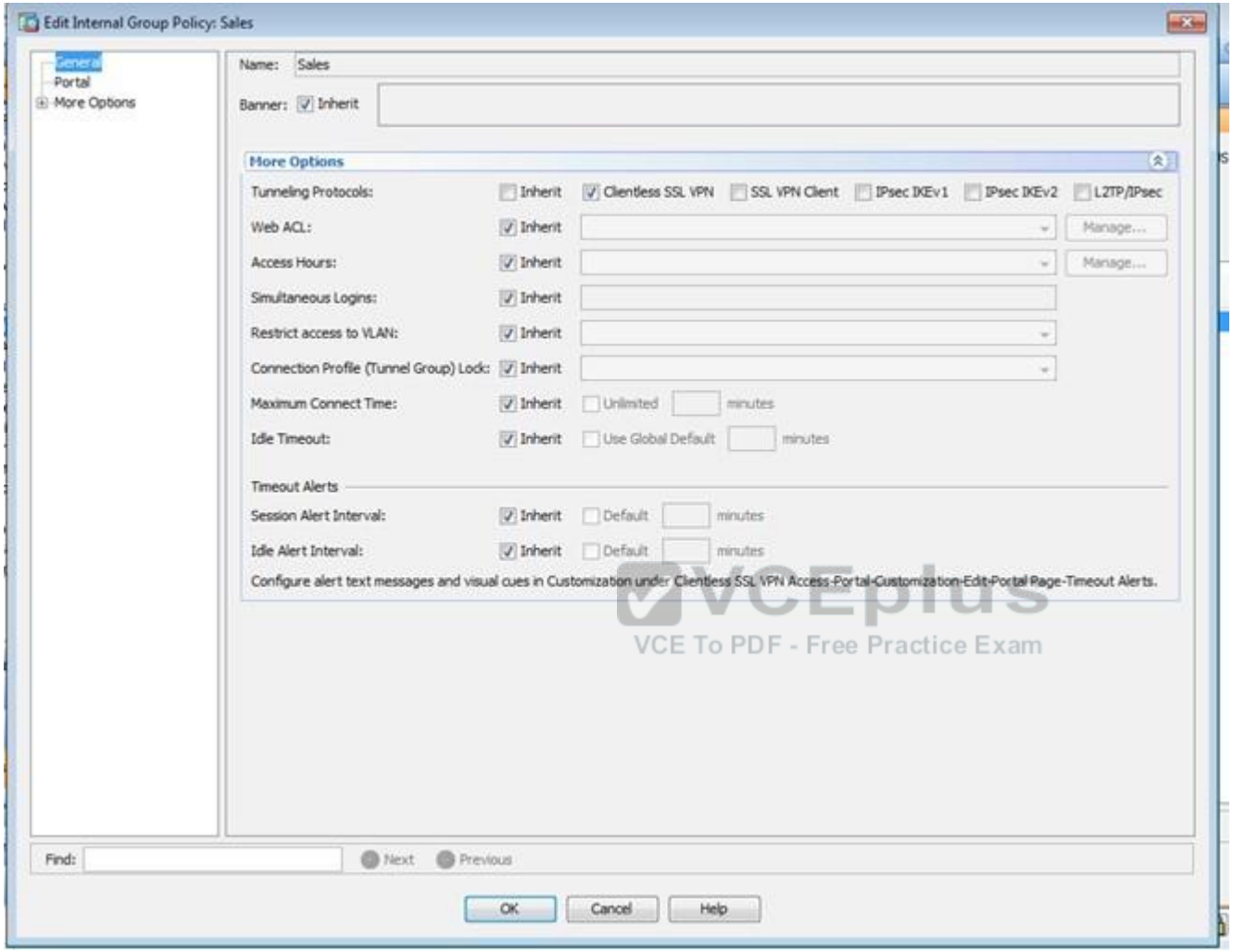


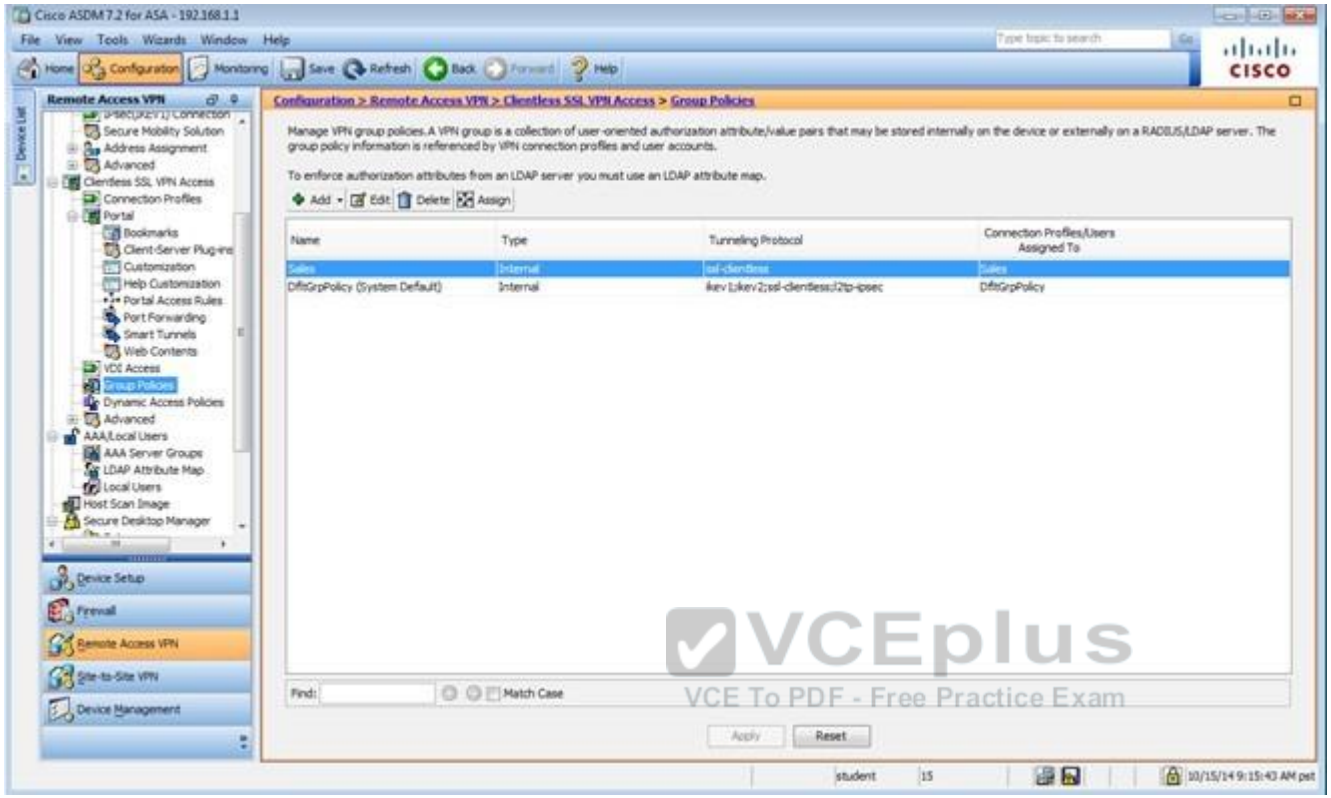


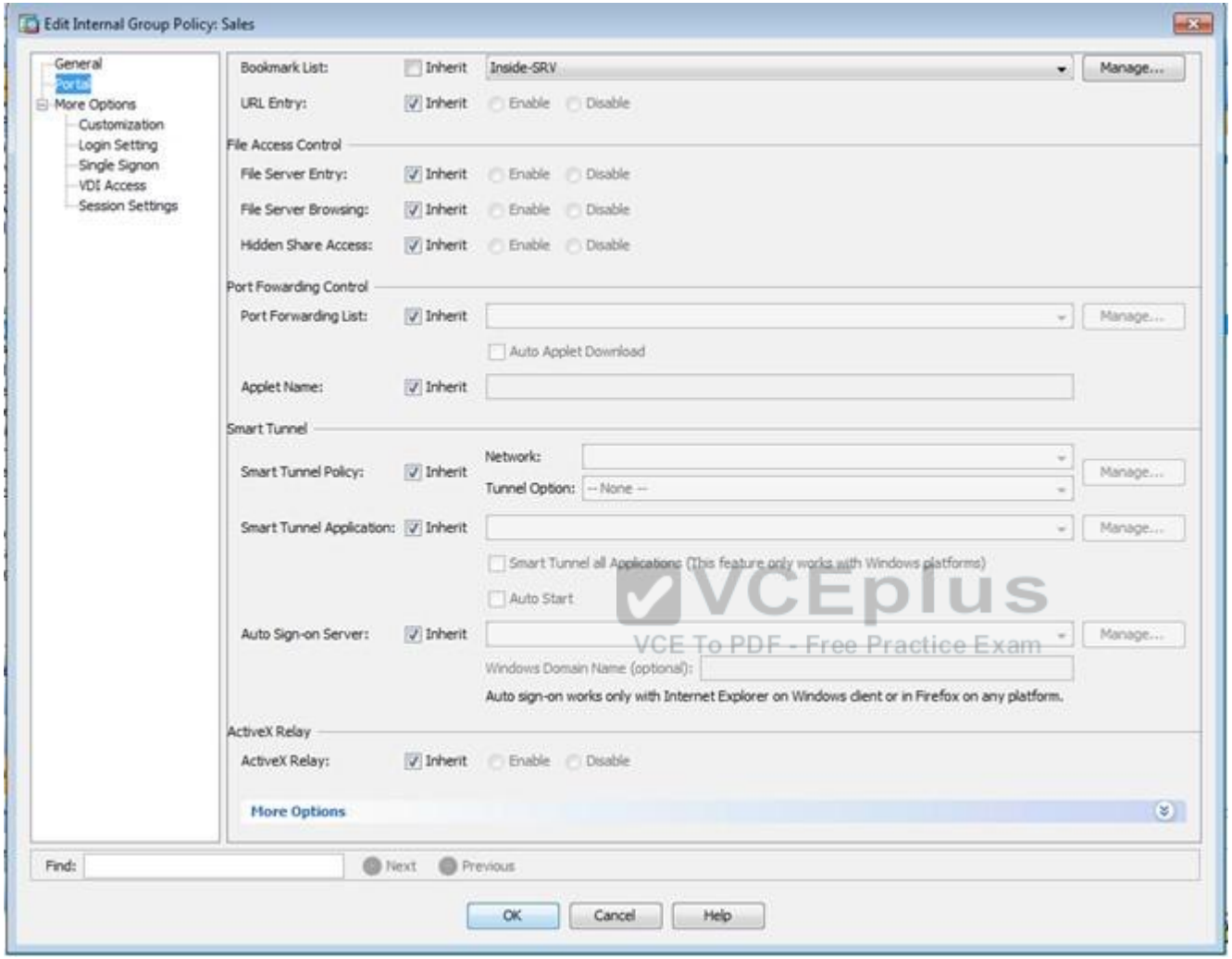


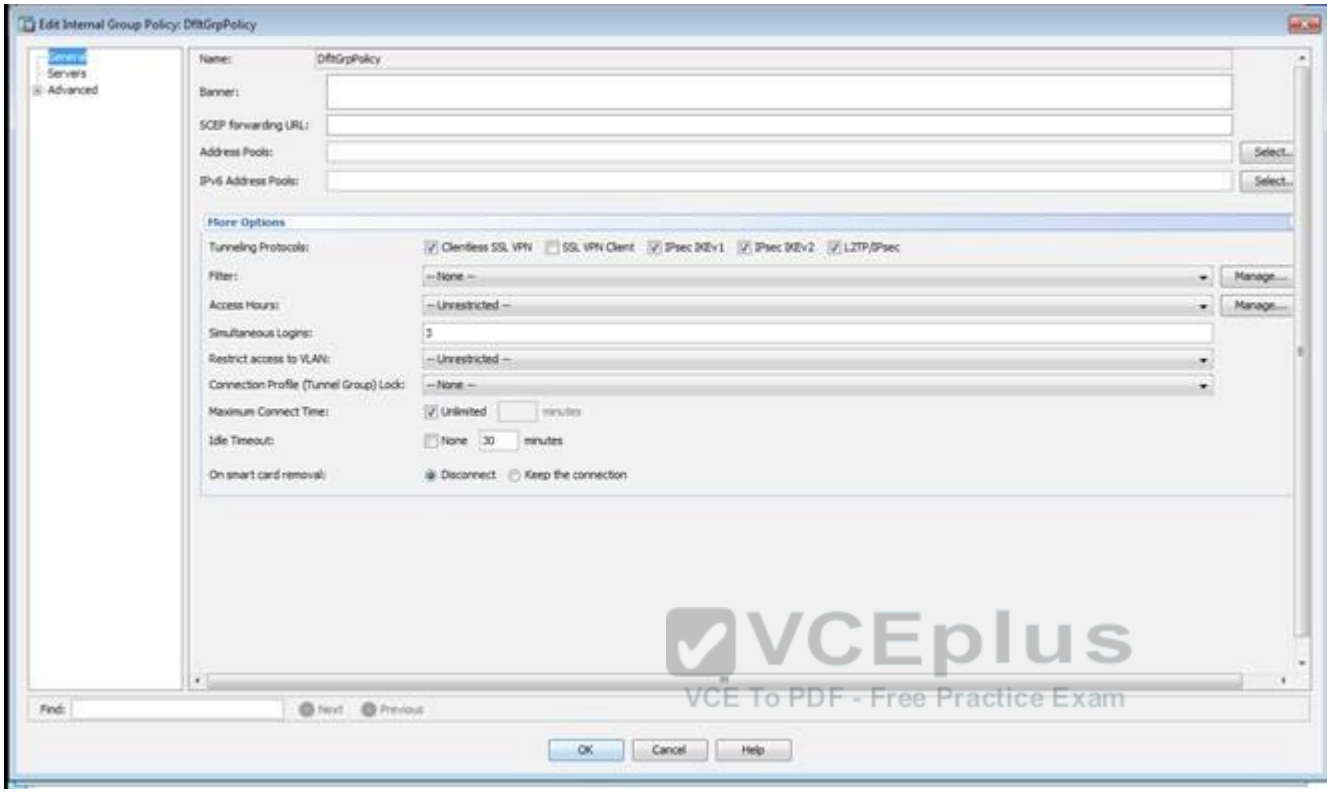


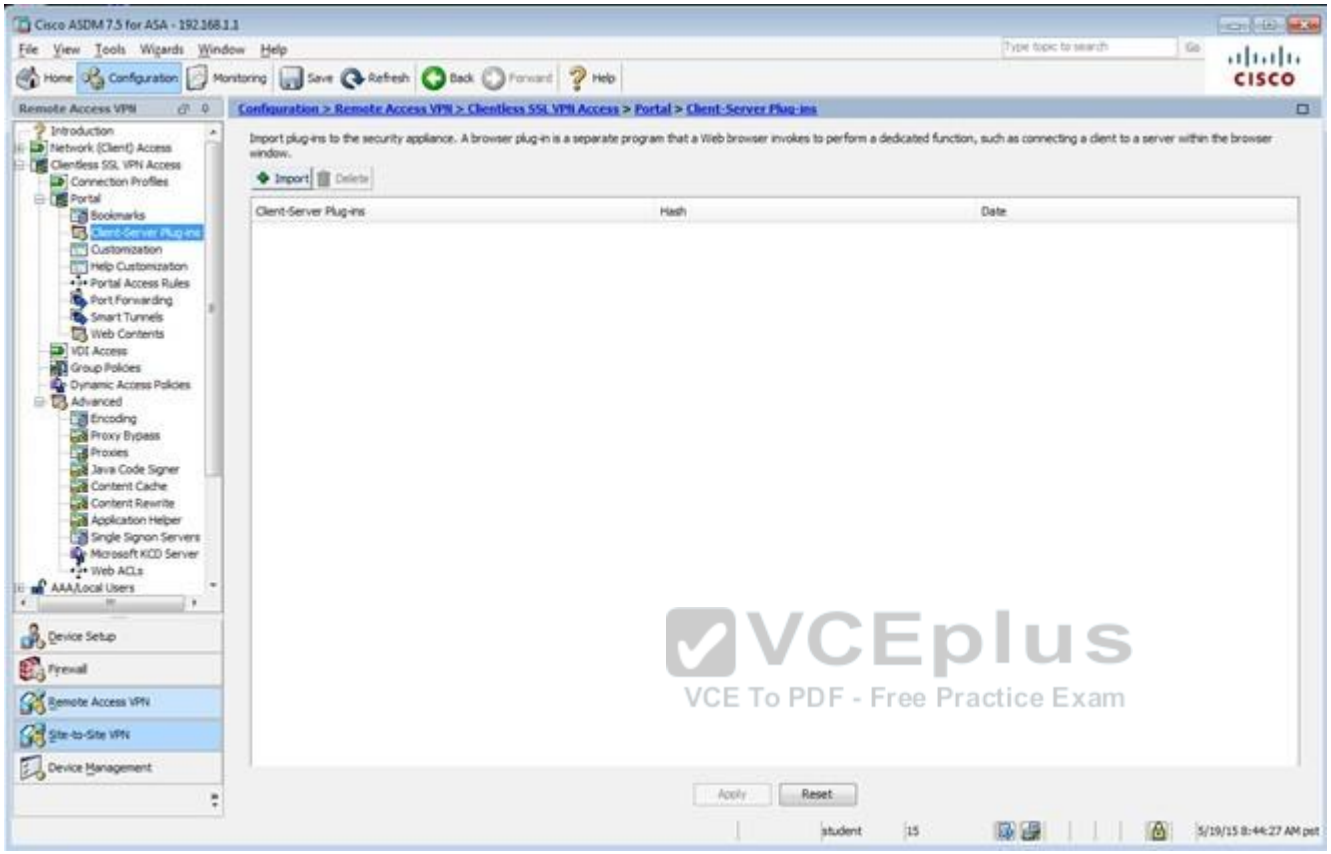


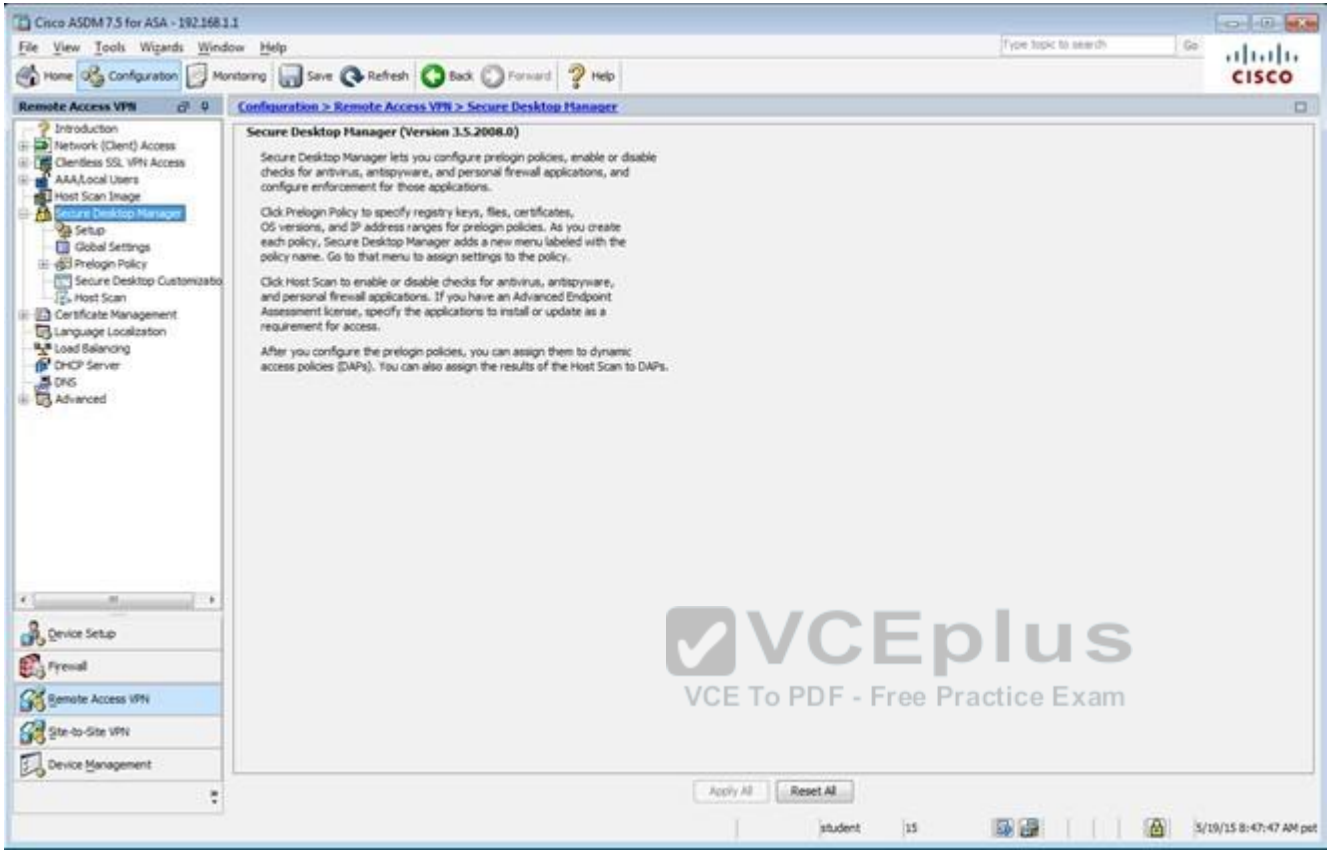


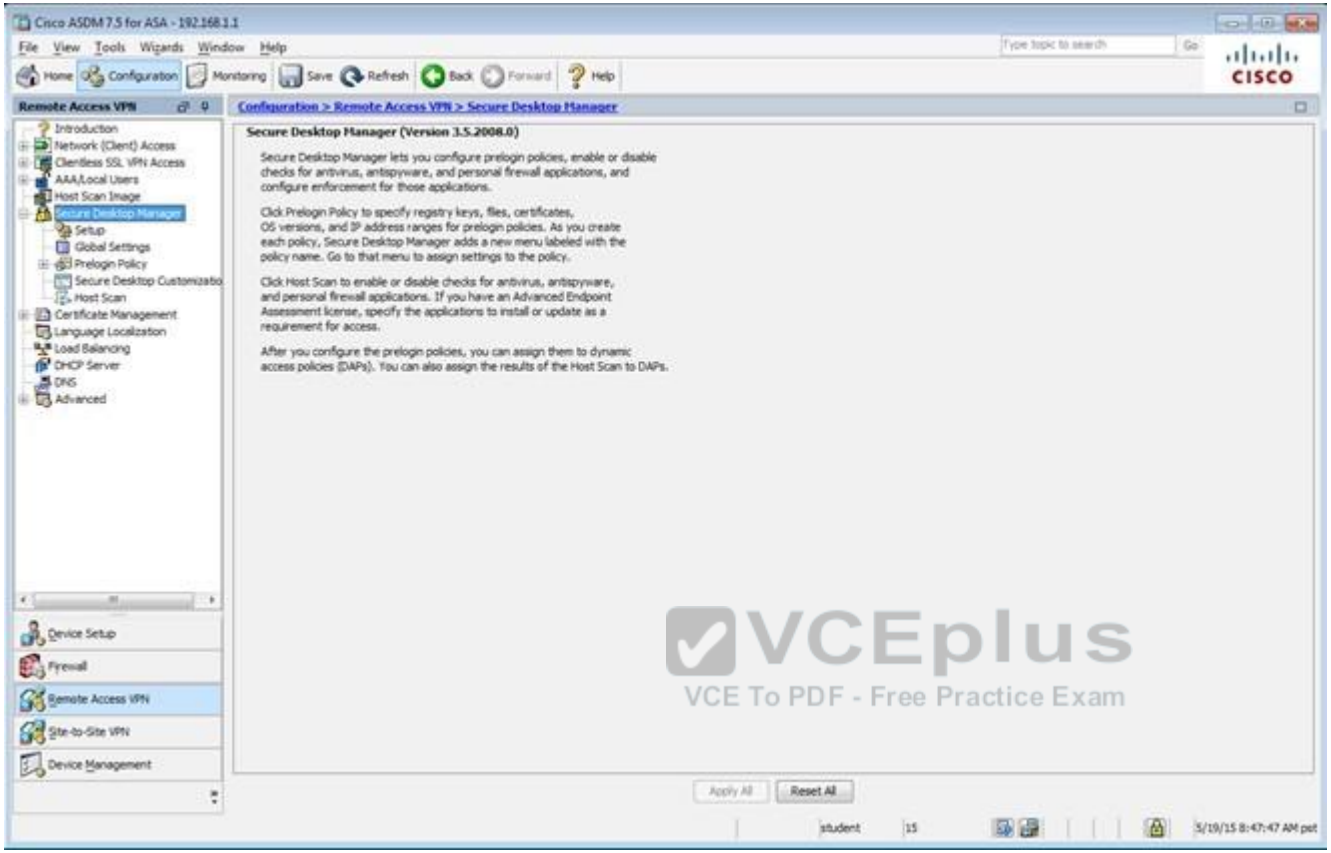


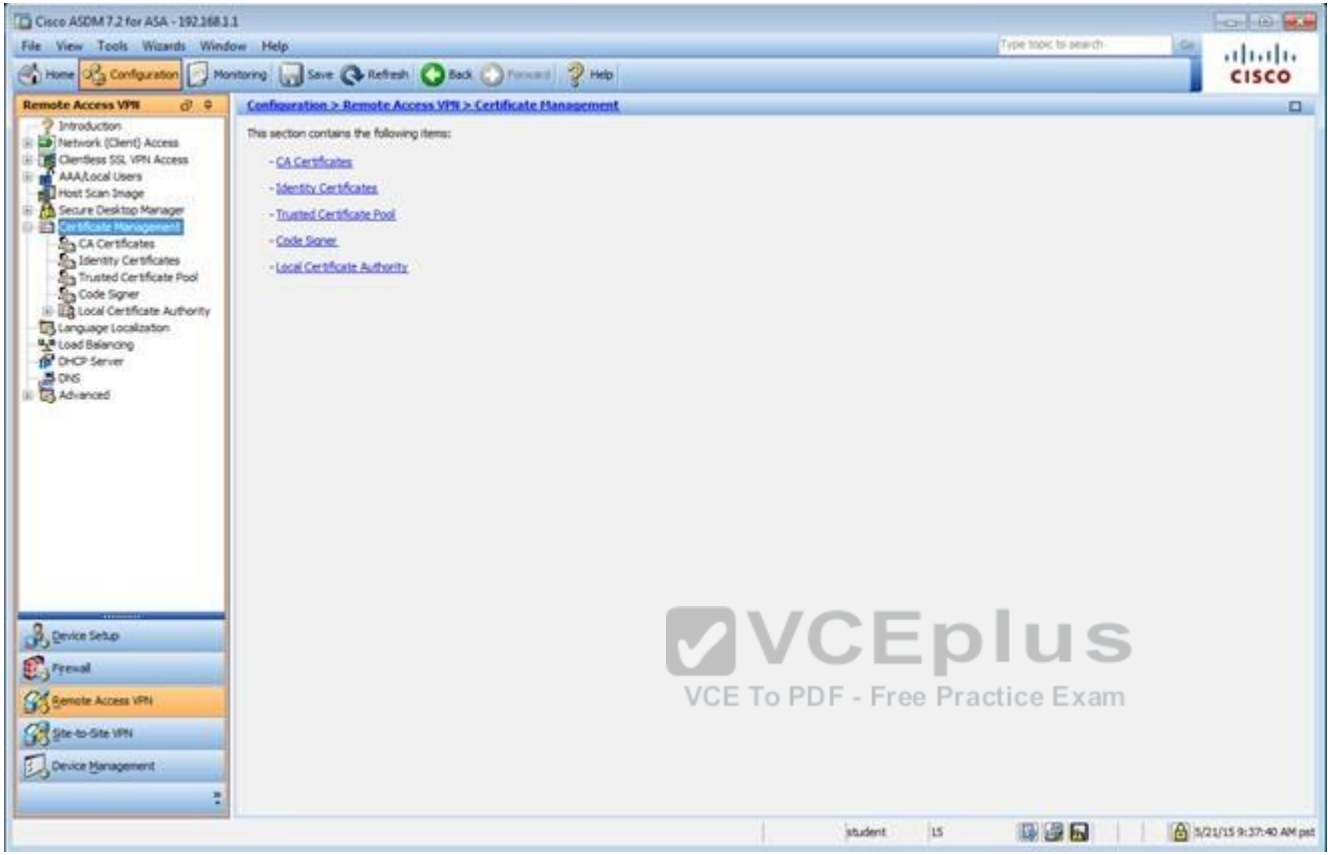


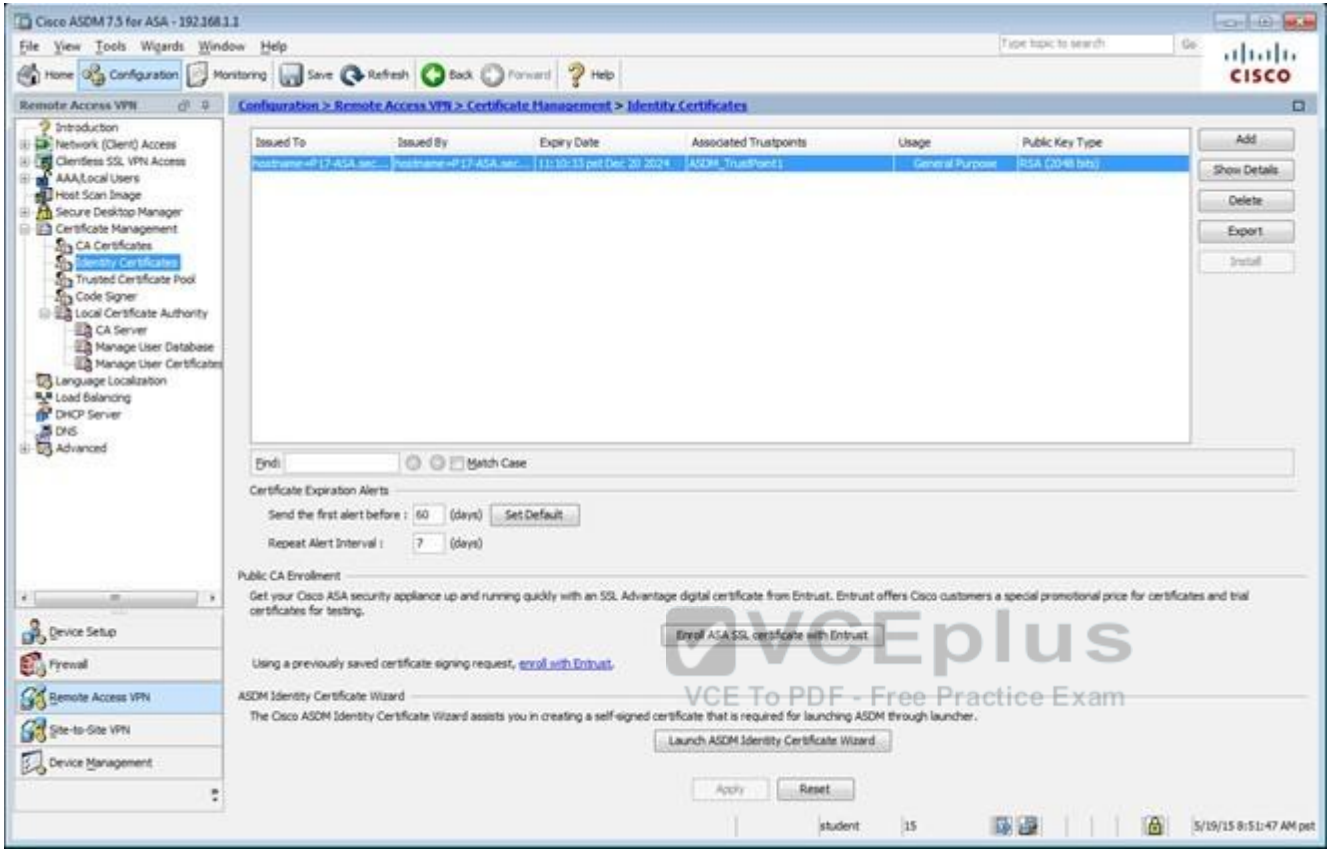


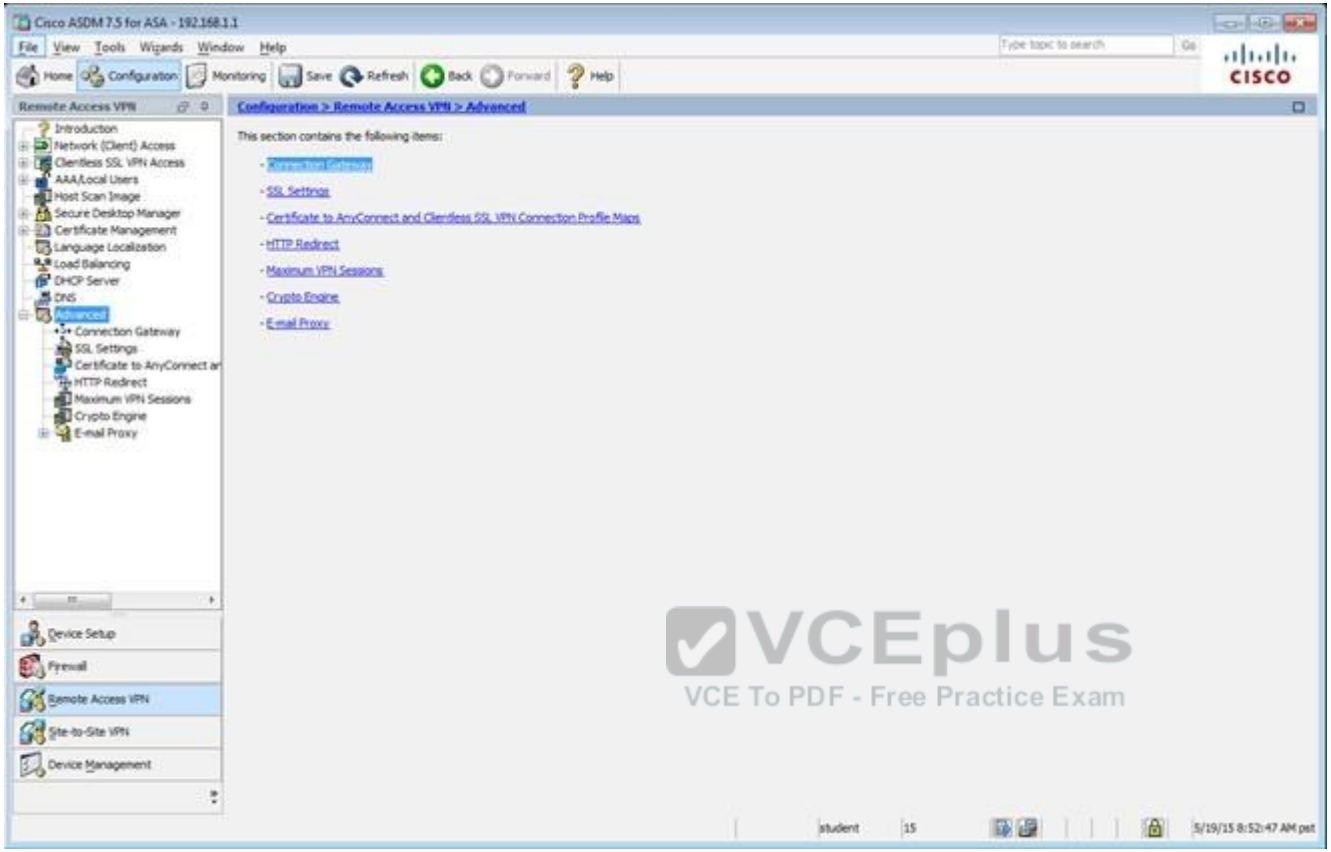


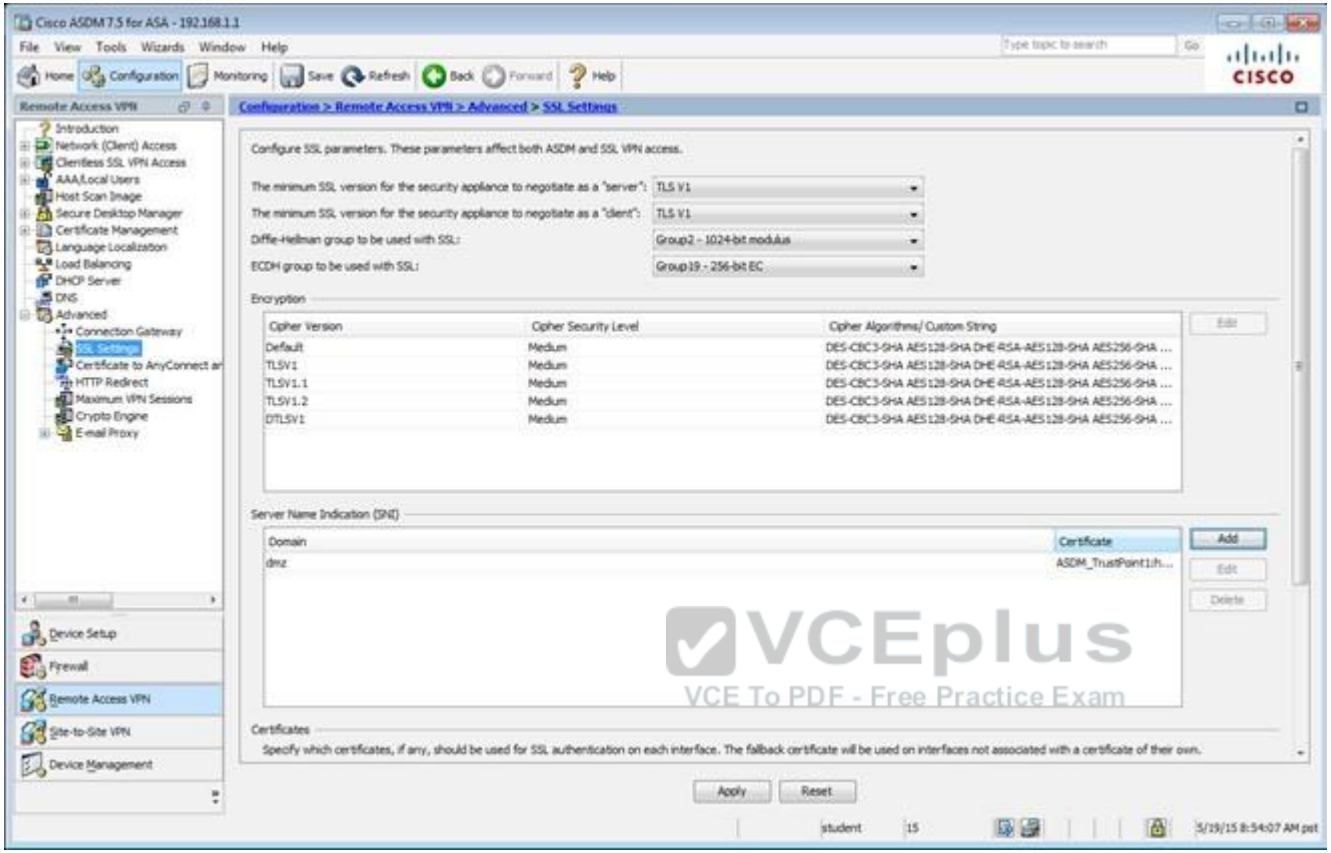


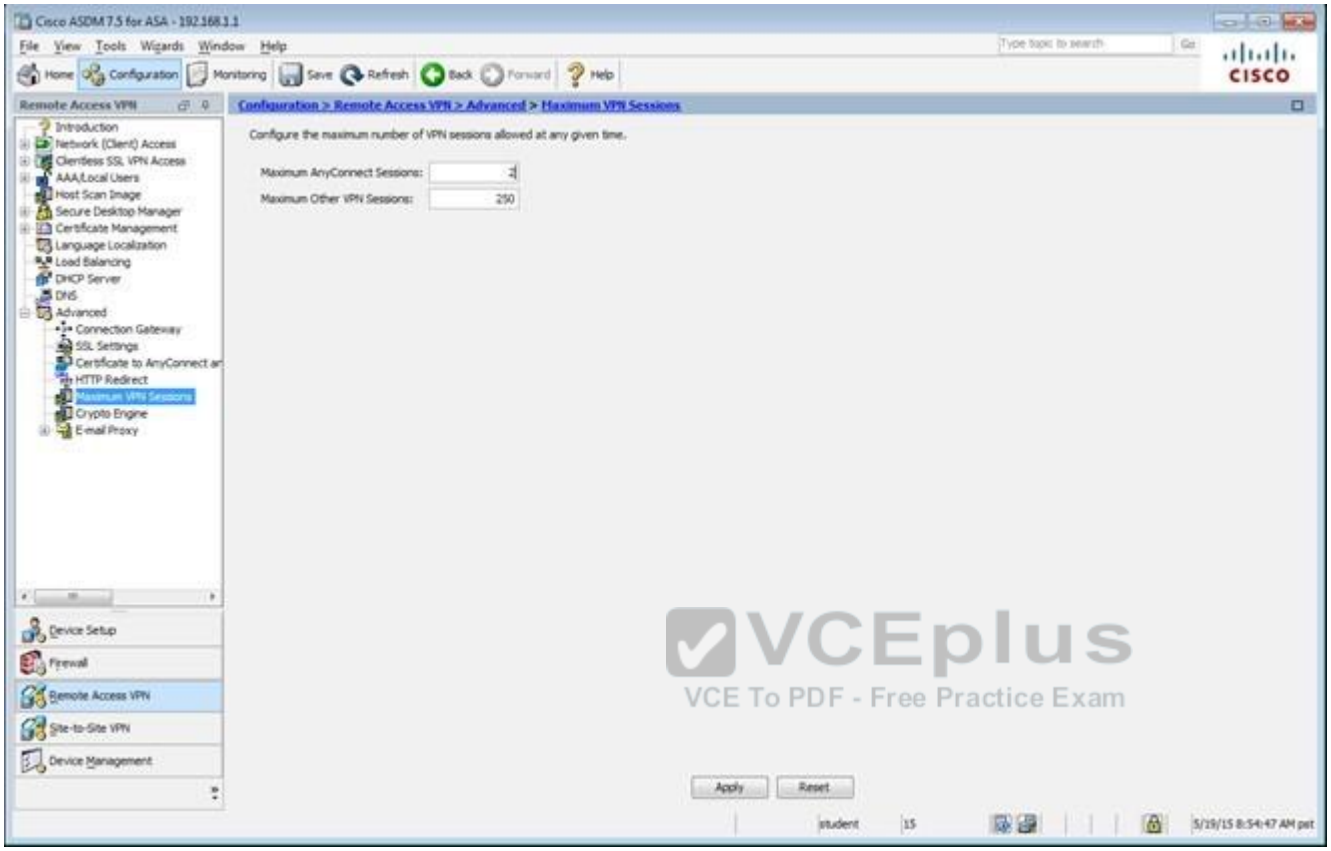


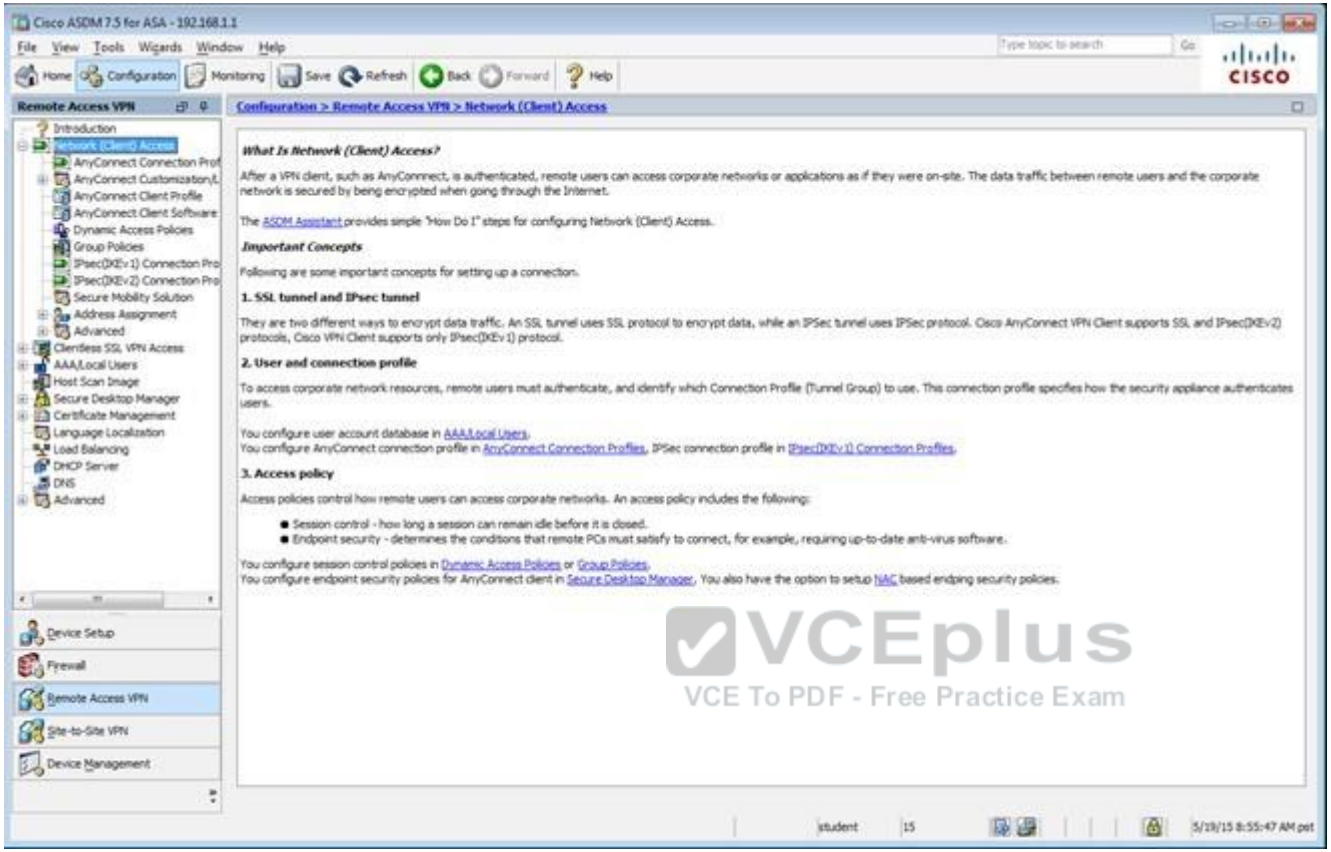


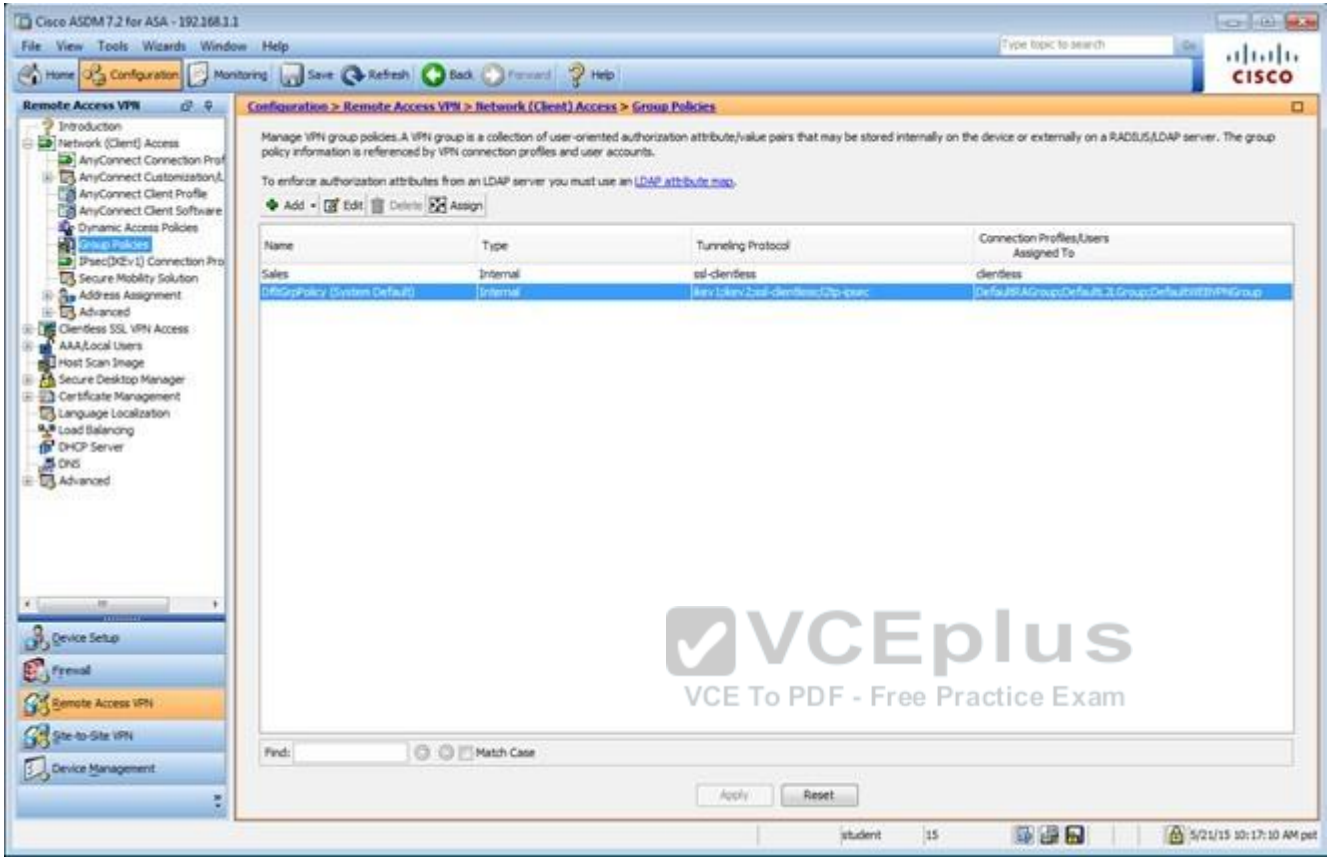


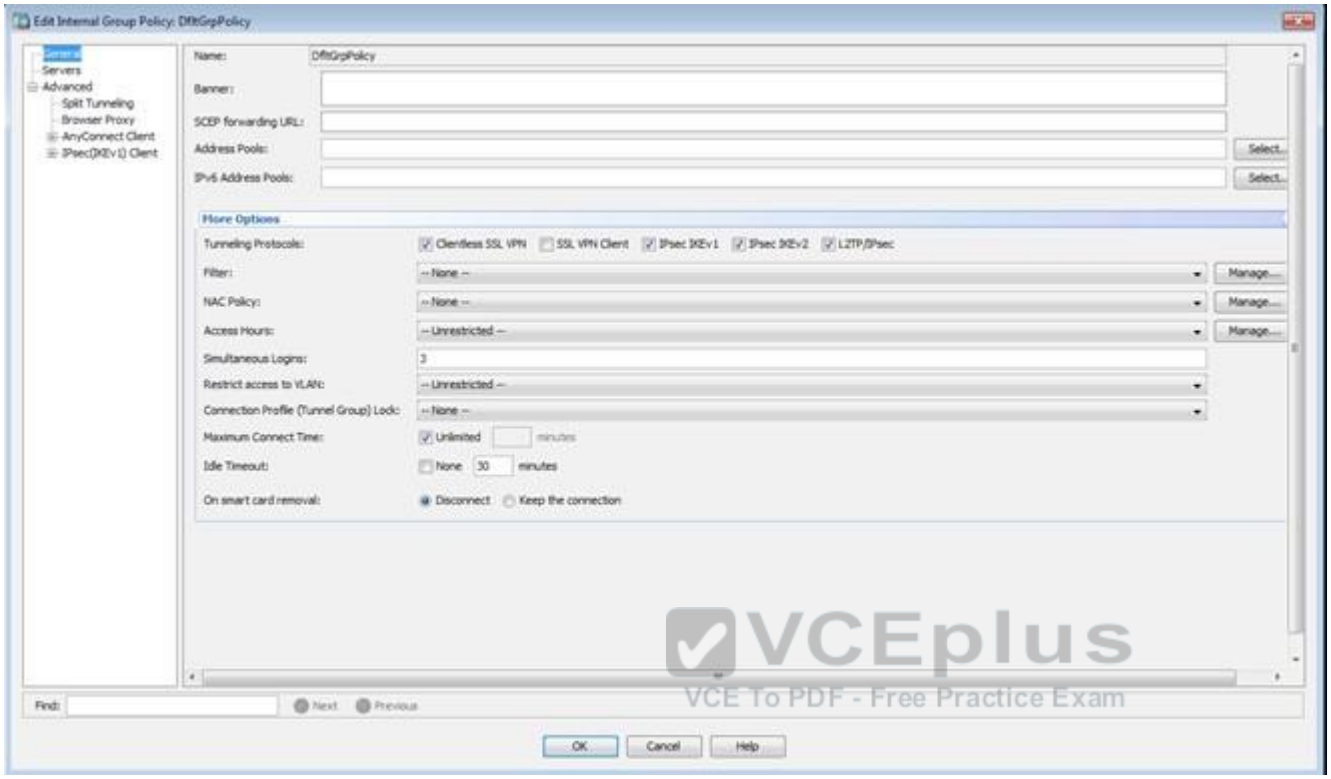


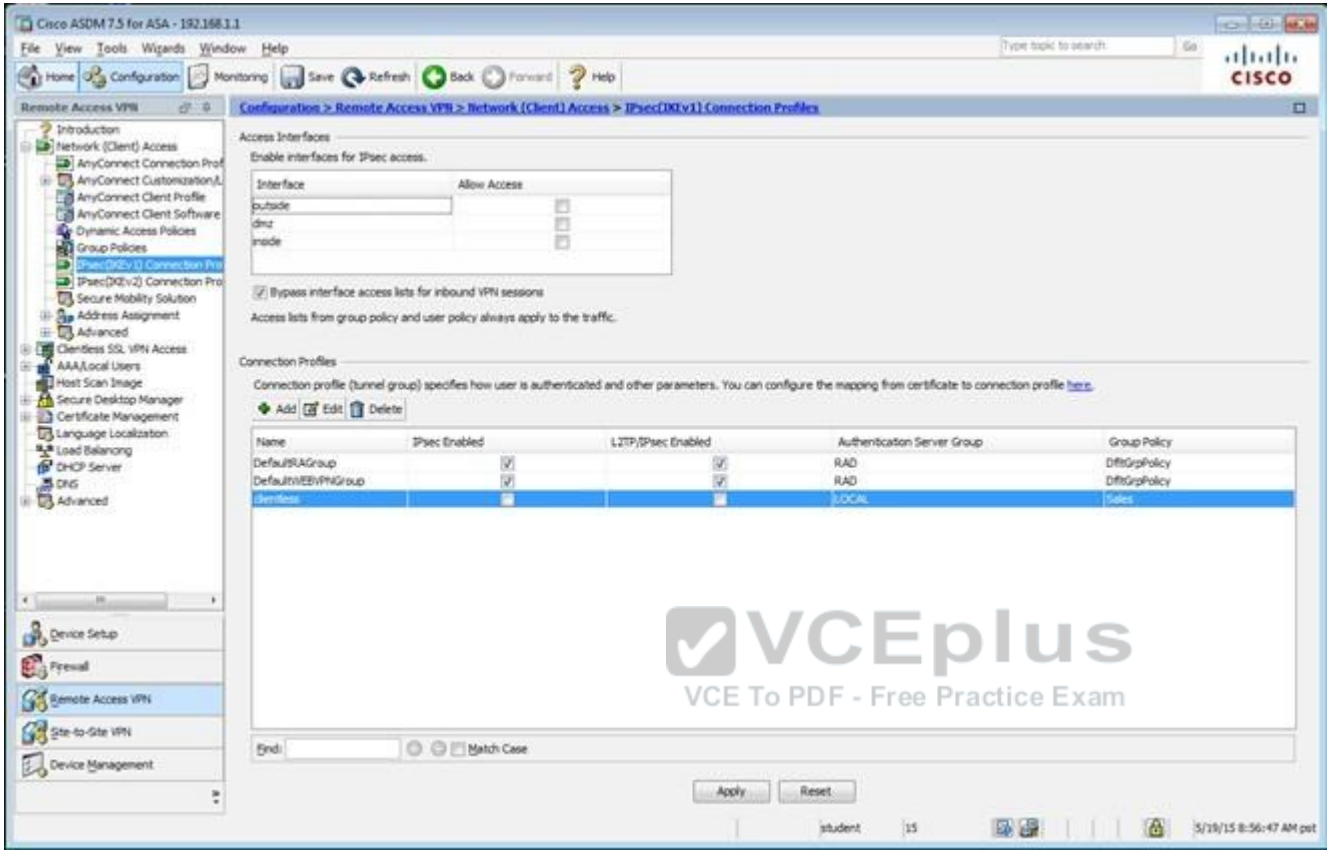


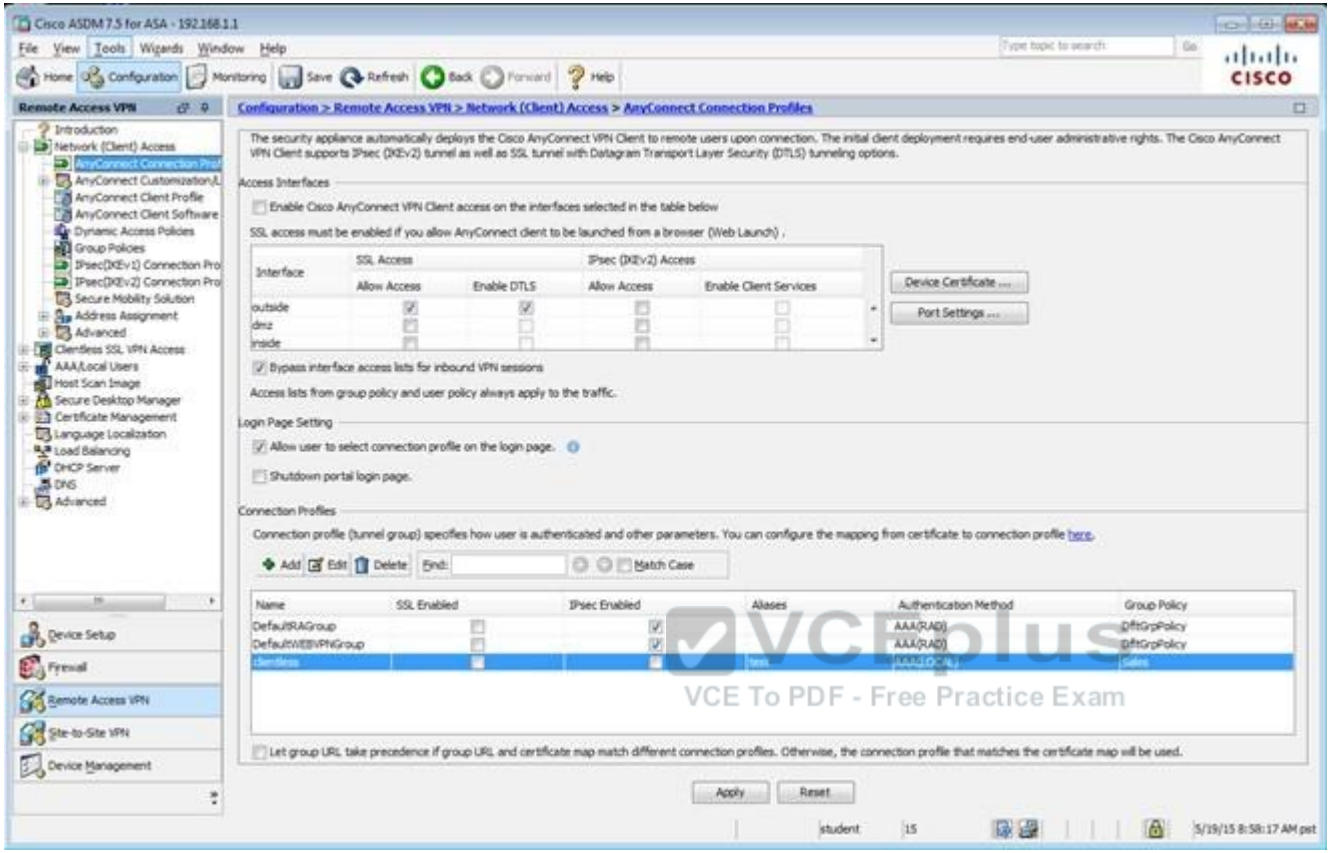


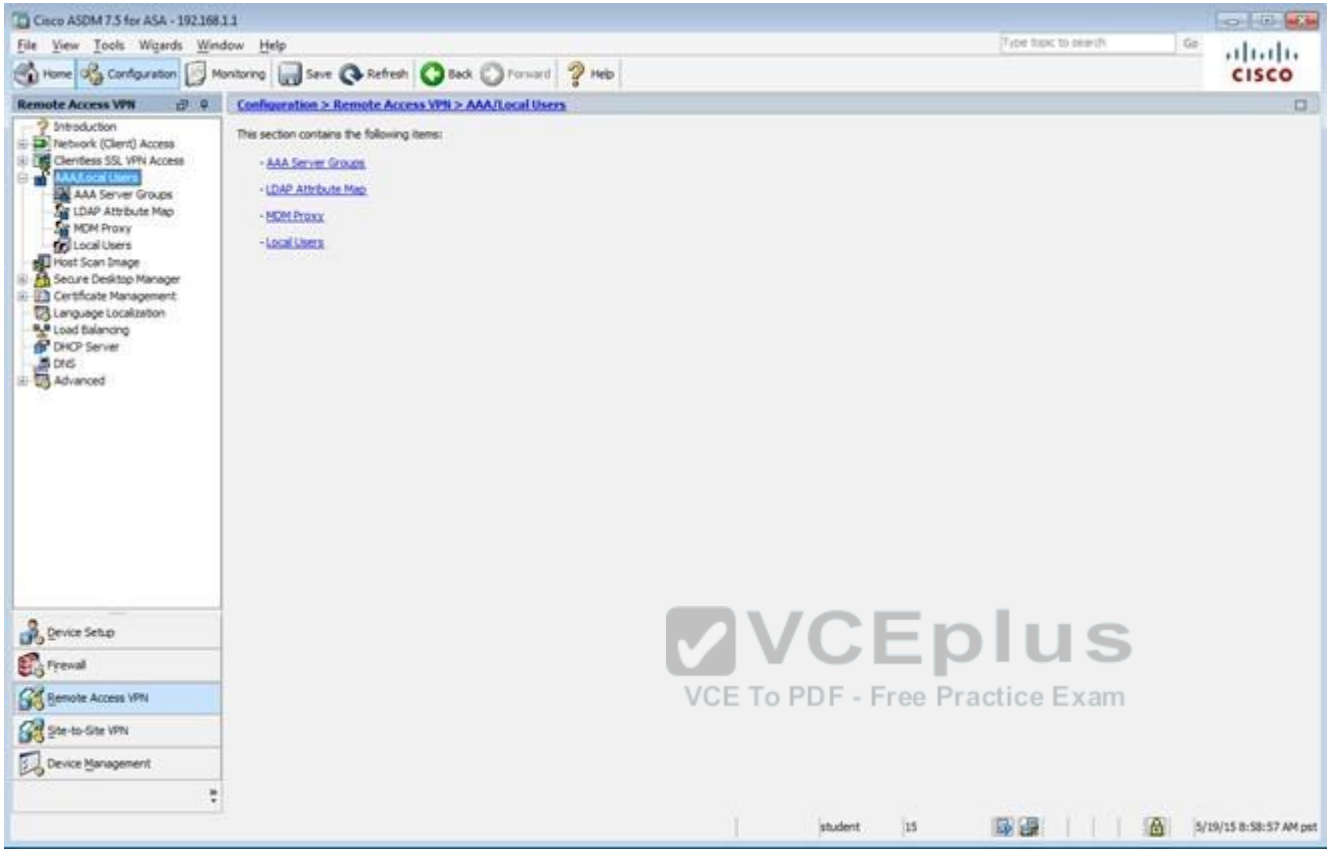


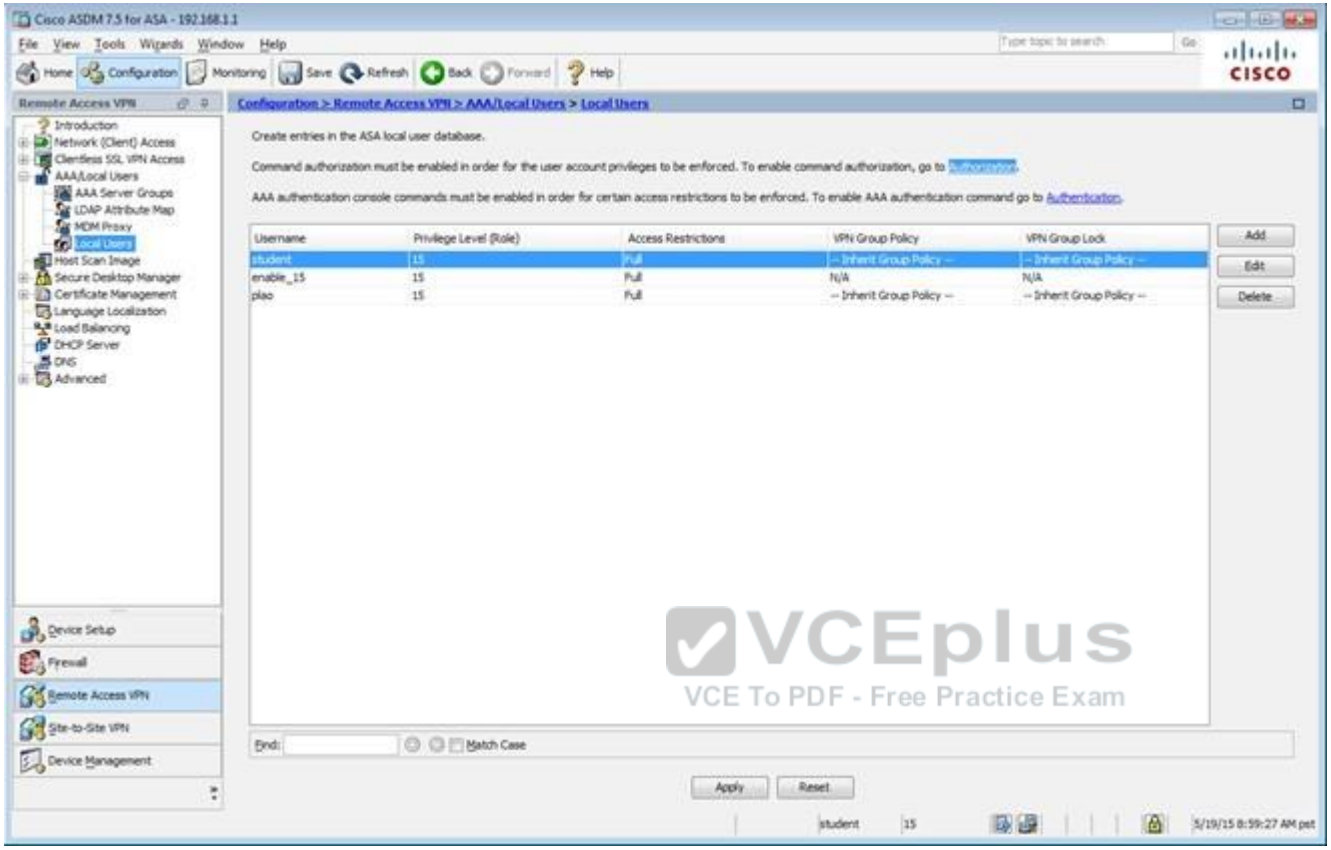


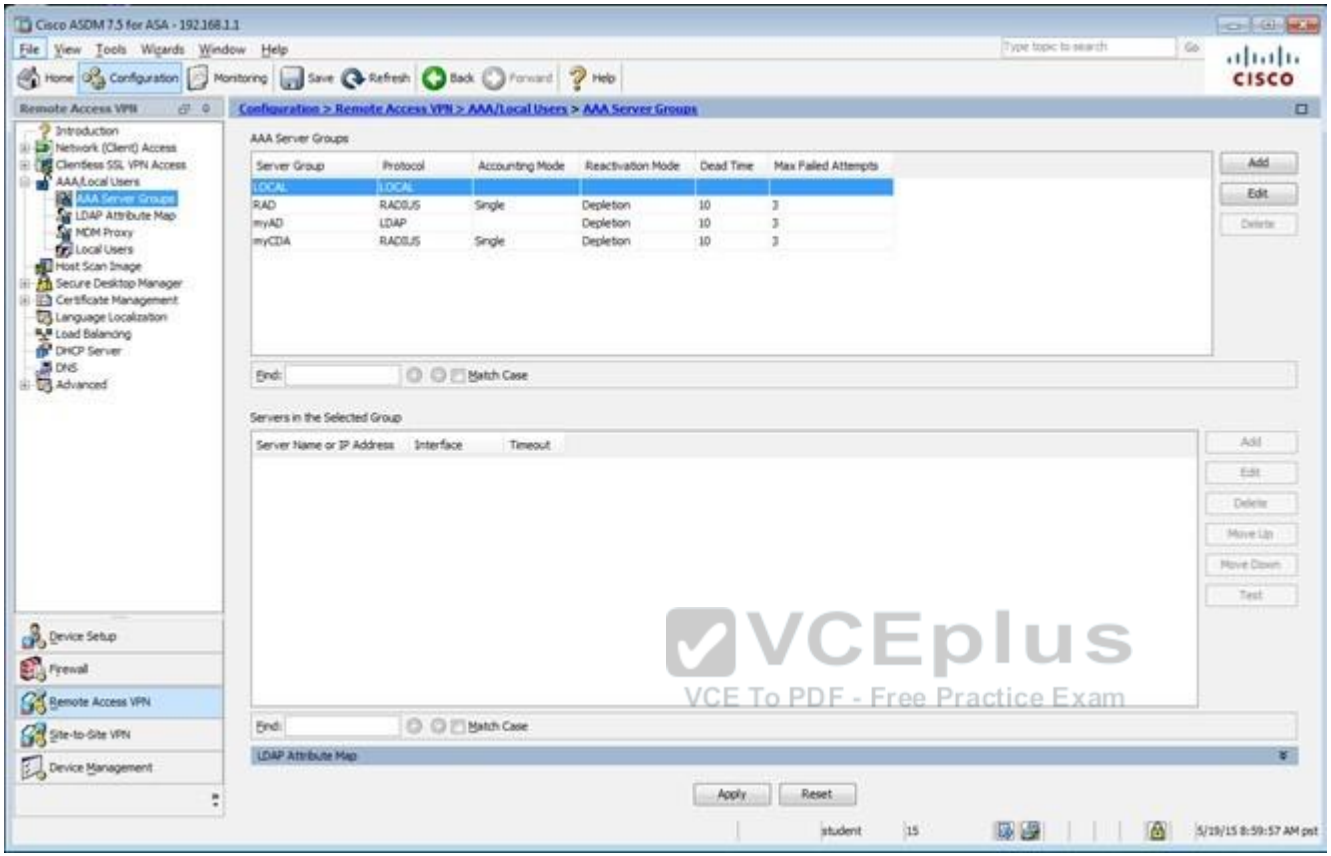










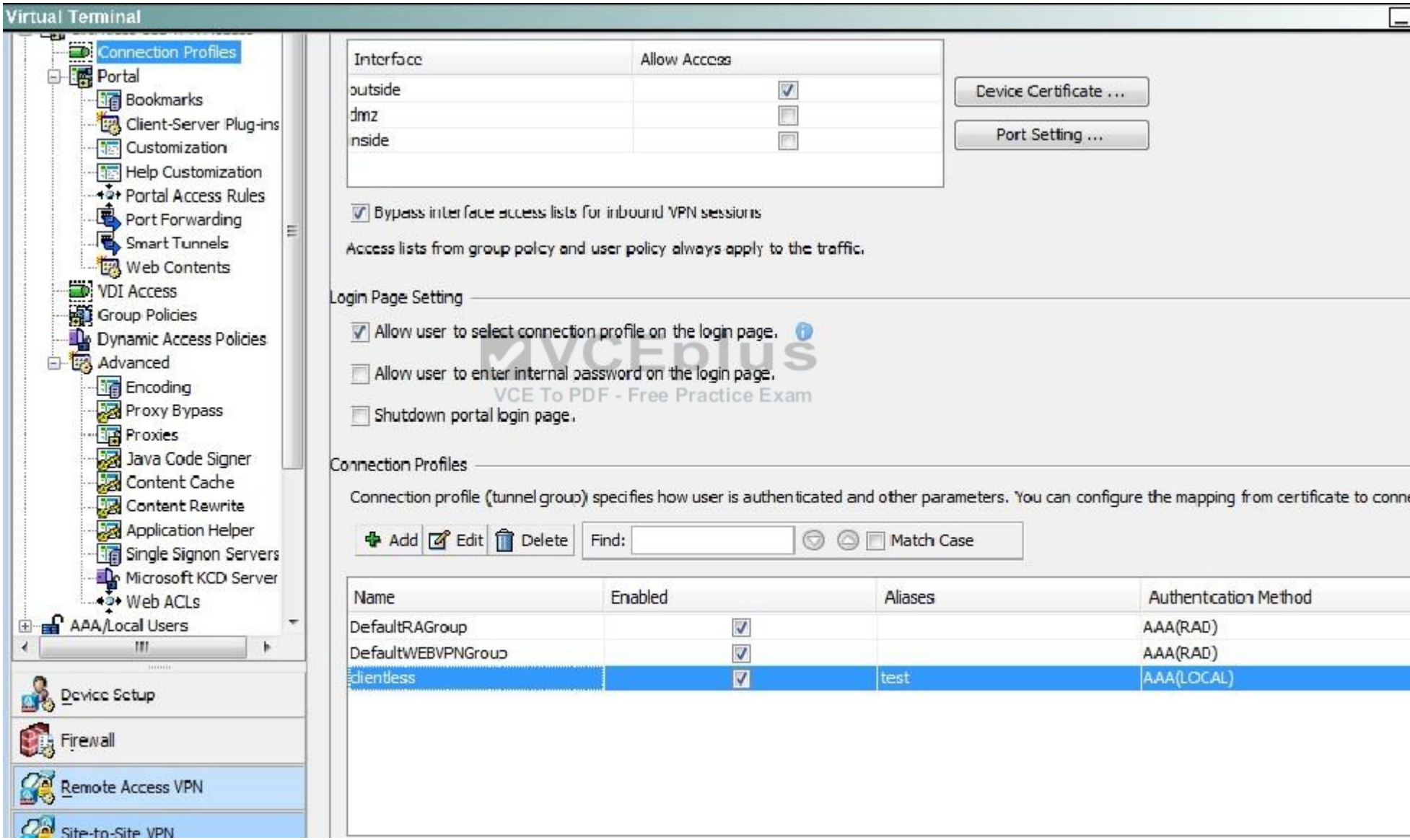


Which two statements regarding the ASA VPN configurations are correct? (Choose two)

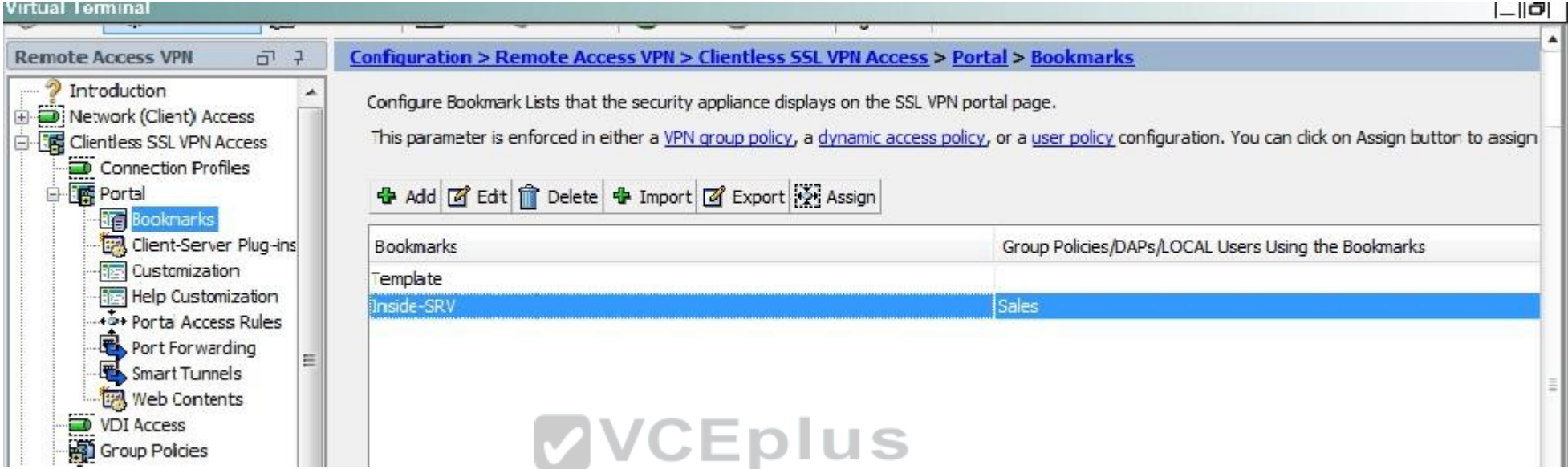
A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
C. The Inside-SRV bookmark references the https://192.168.1.2 URL
D. Only Clientless SSL VPN access is 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

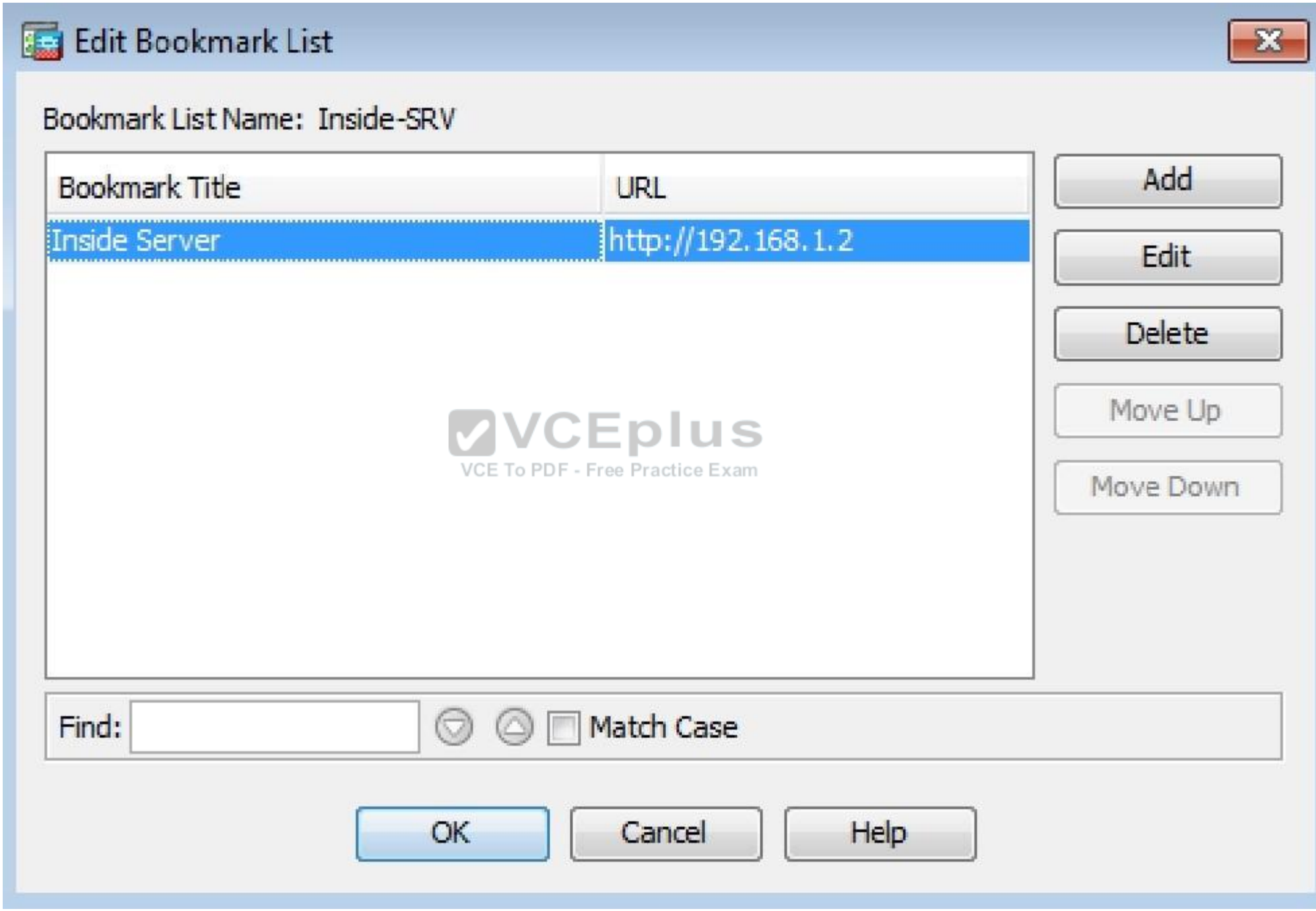
Explanation/Reference:
Explanation:
For B:



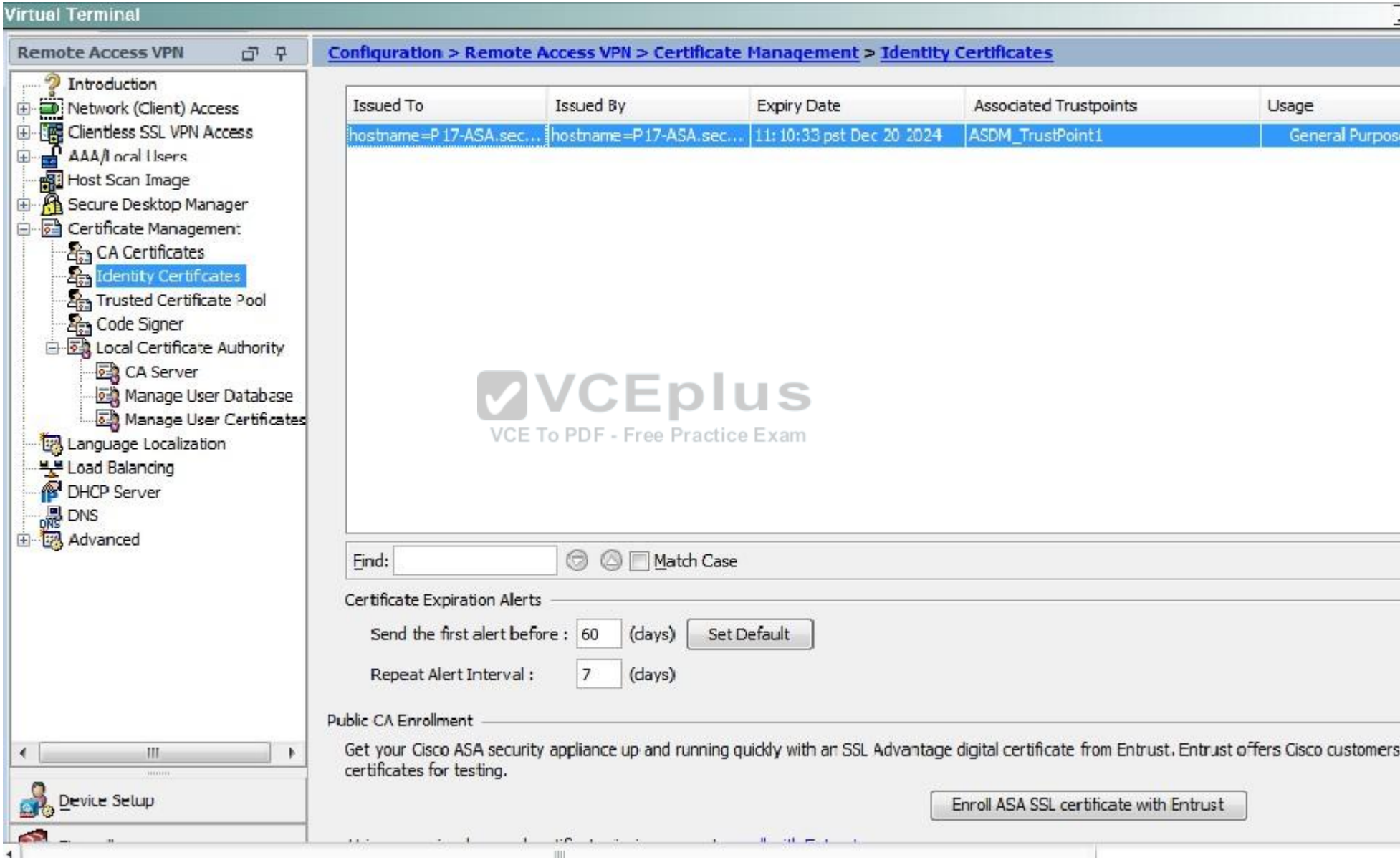
For C, Navigate to the Bookmarks tab:



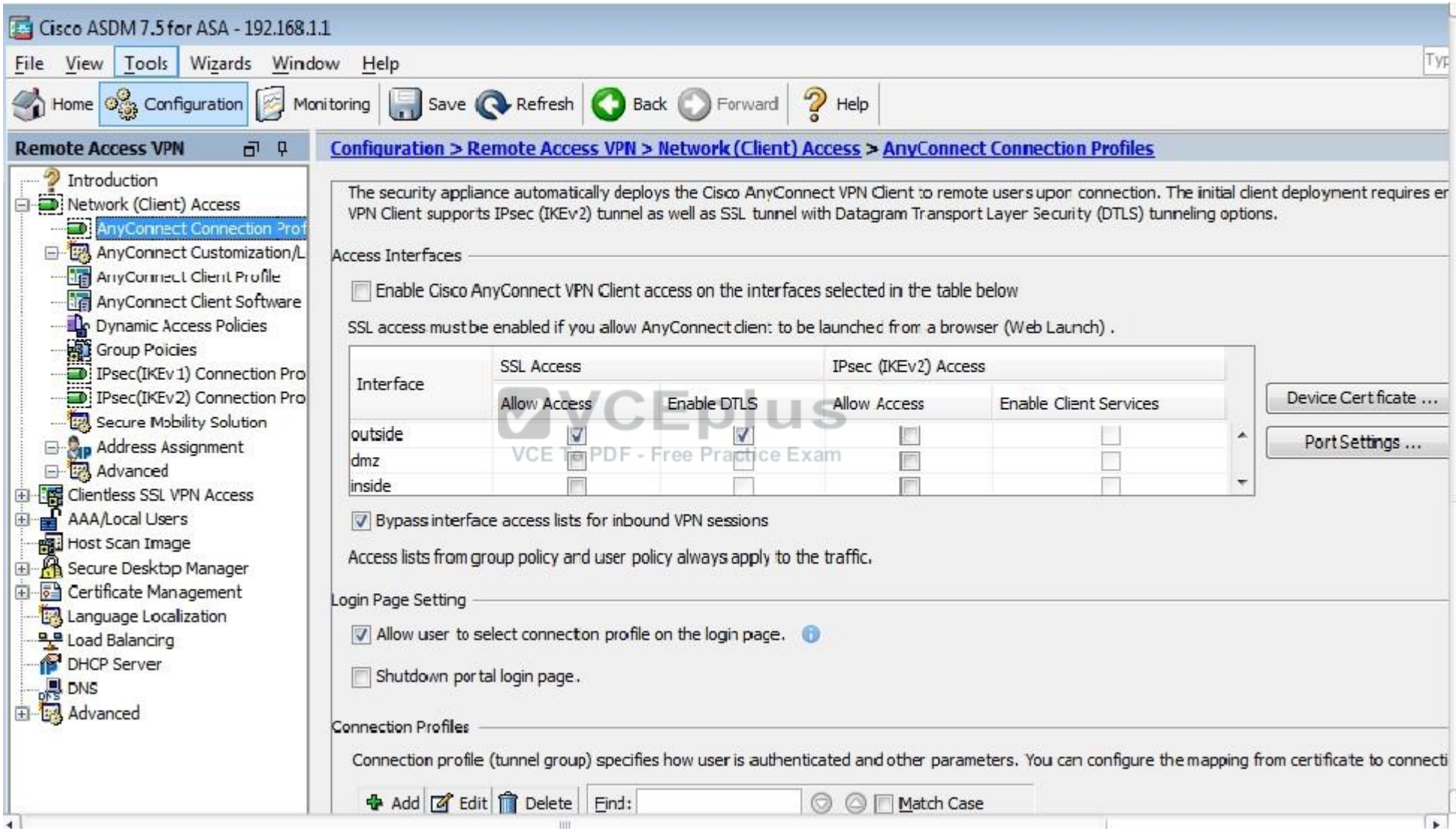
Then hit "edit" and you will see this:



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



Note E:

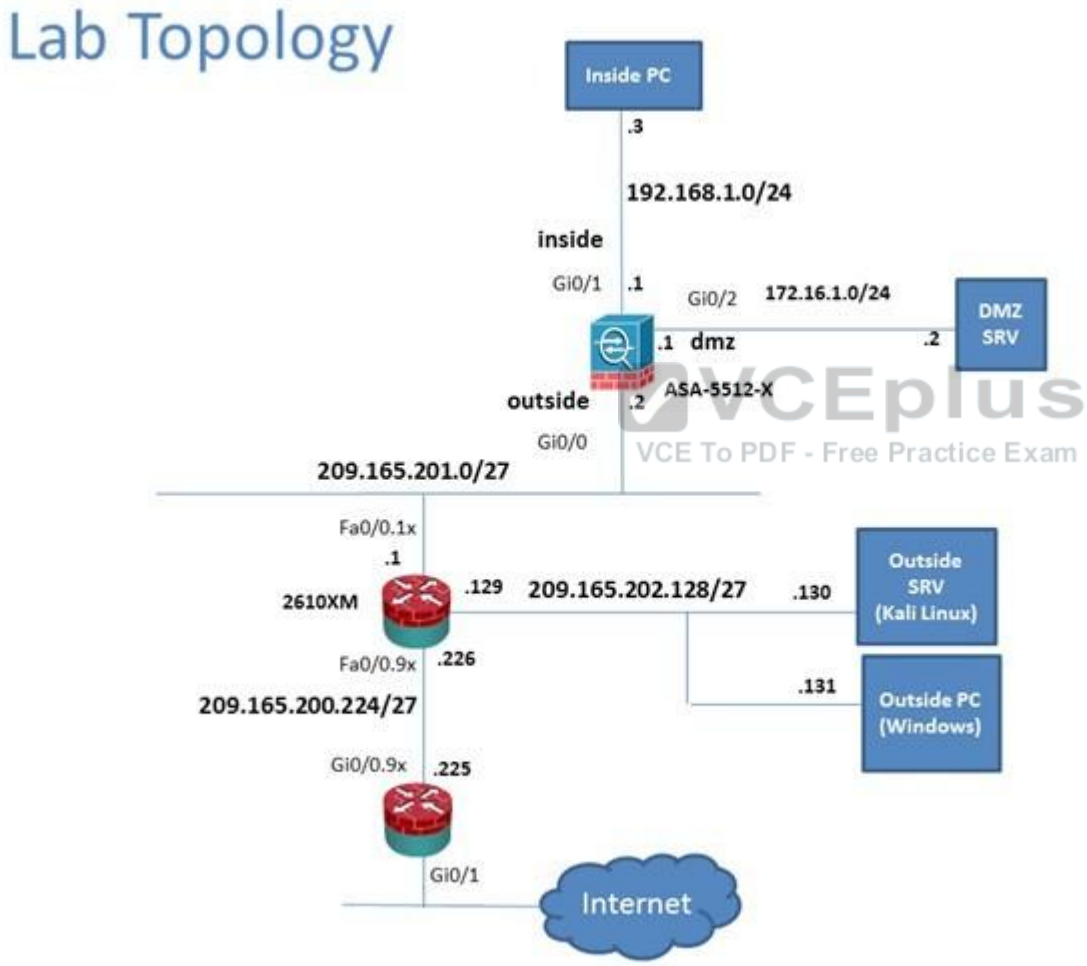


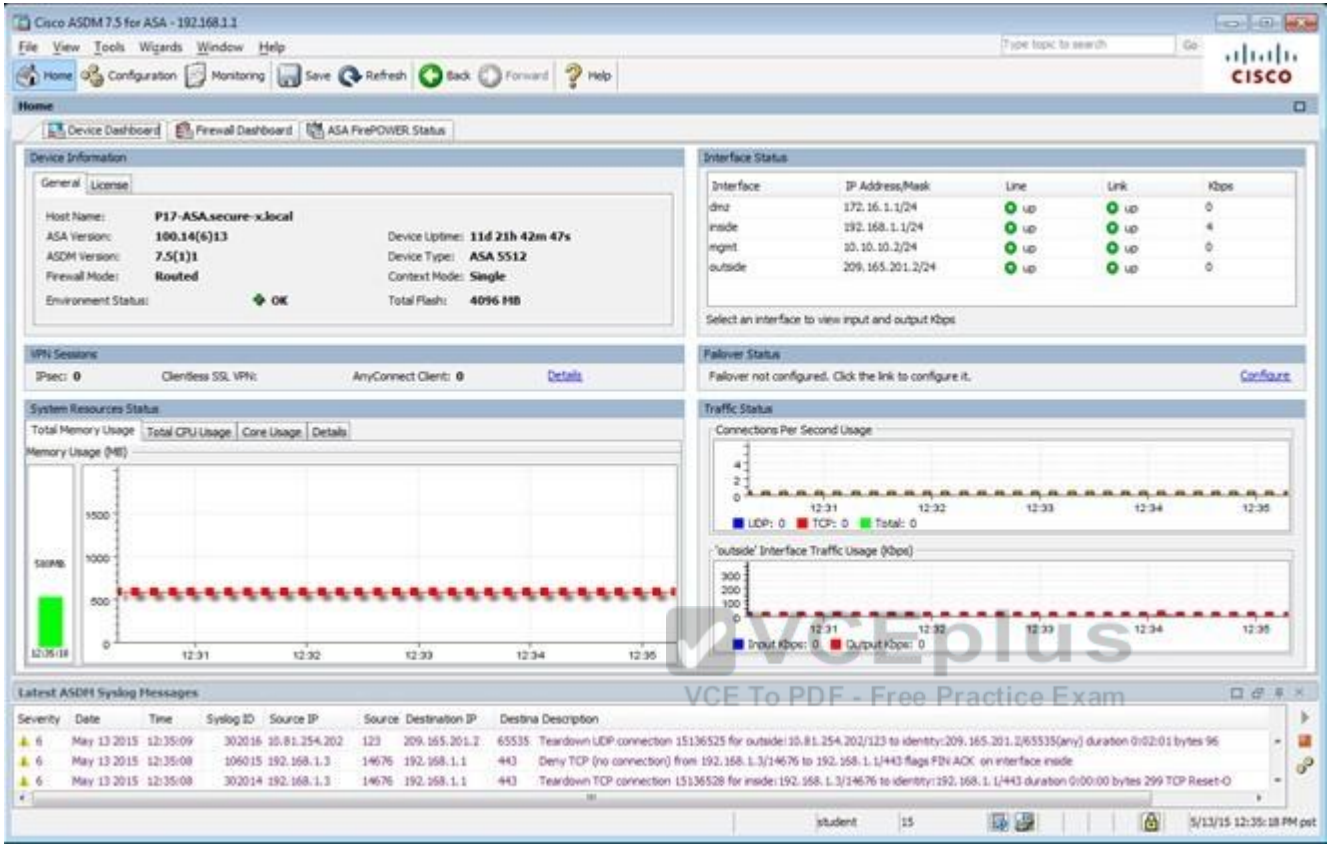
QUESTION 67
Scenario

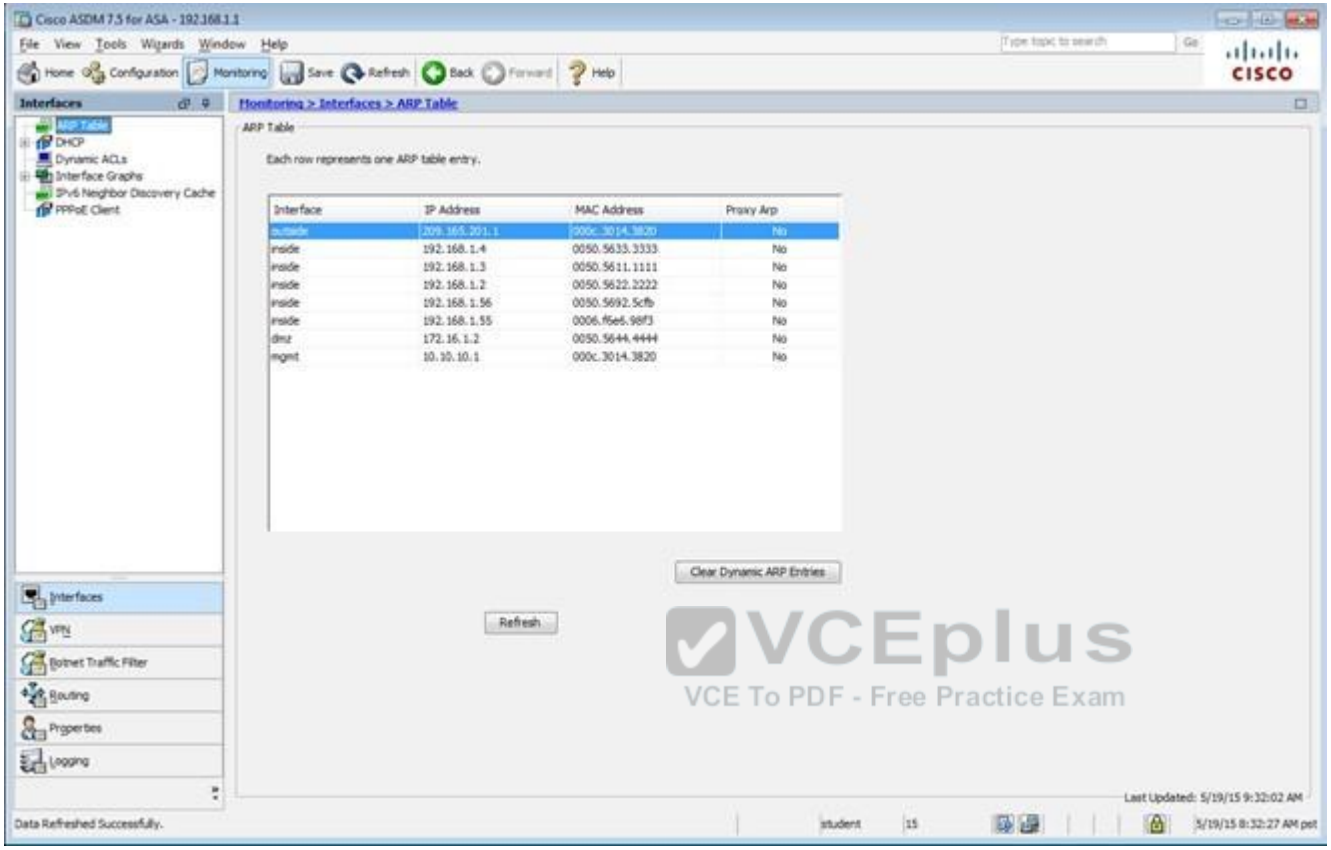
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

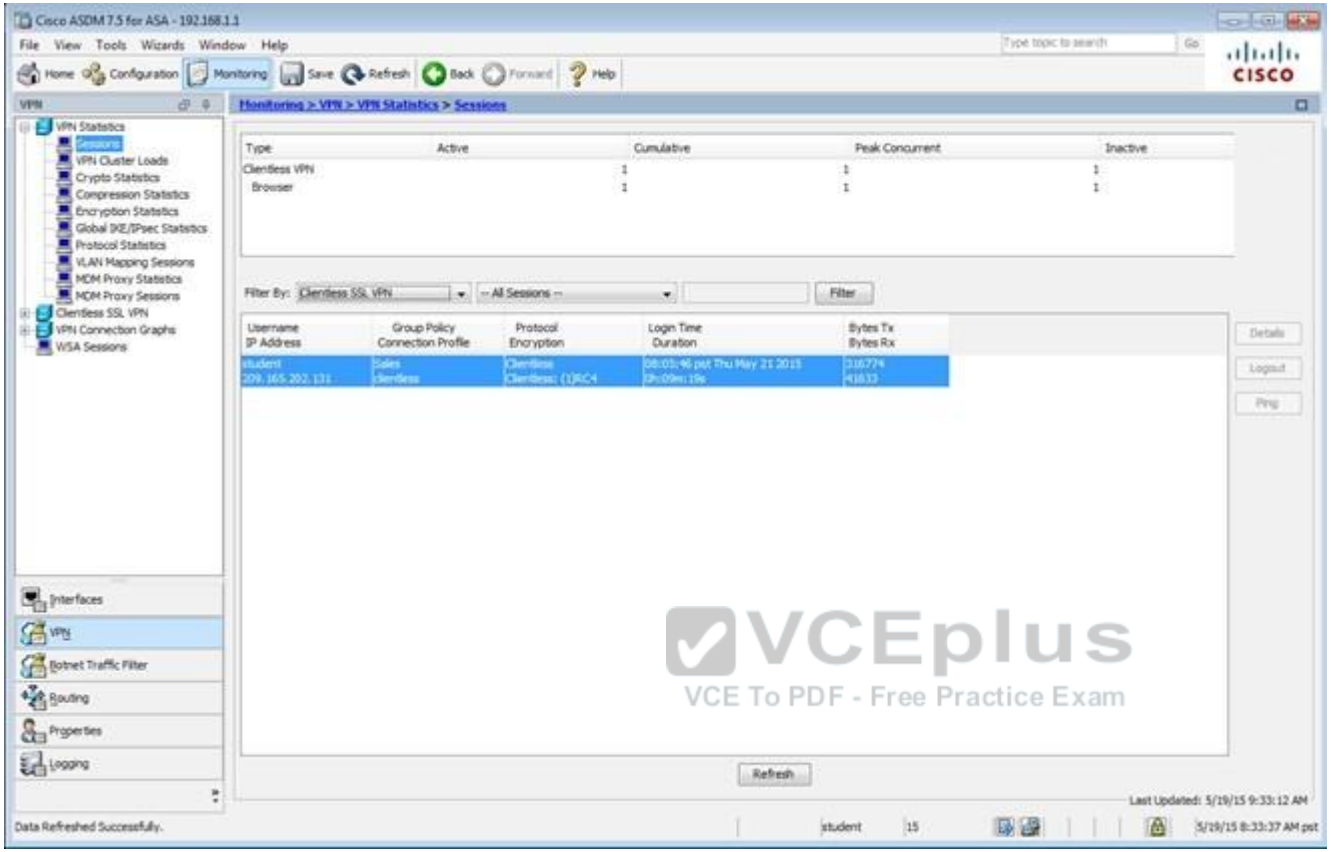
To access ASDM, click the ASA icon in the topology diagram.

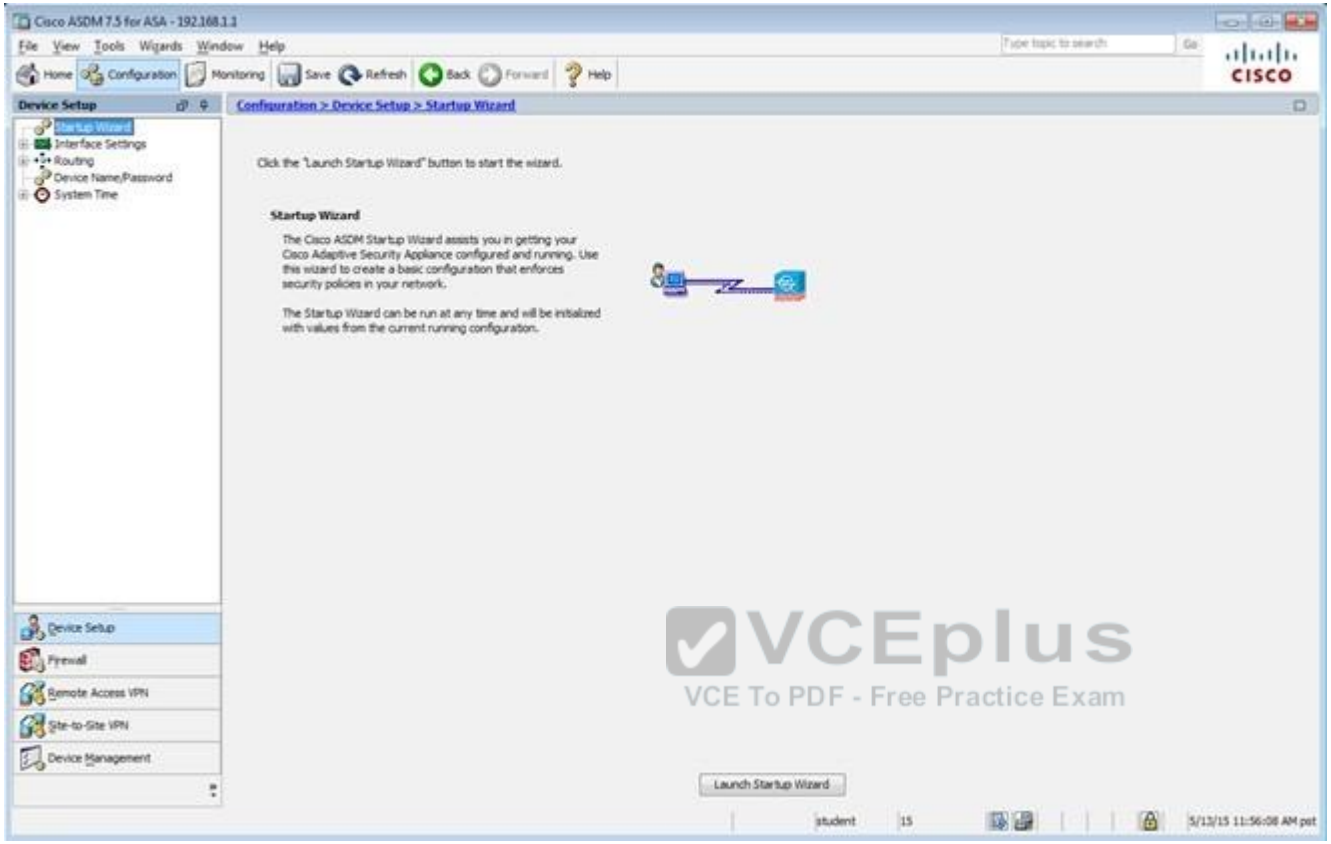
Note: Not all ASDM functionalities are enabled in this simulation. To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

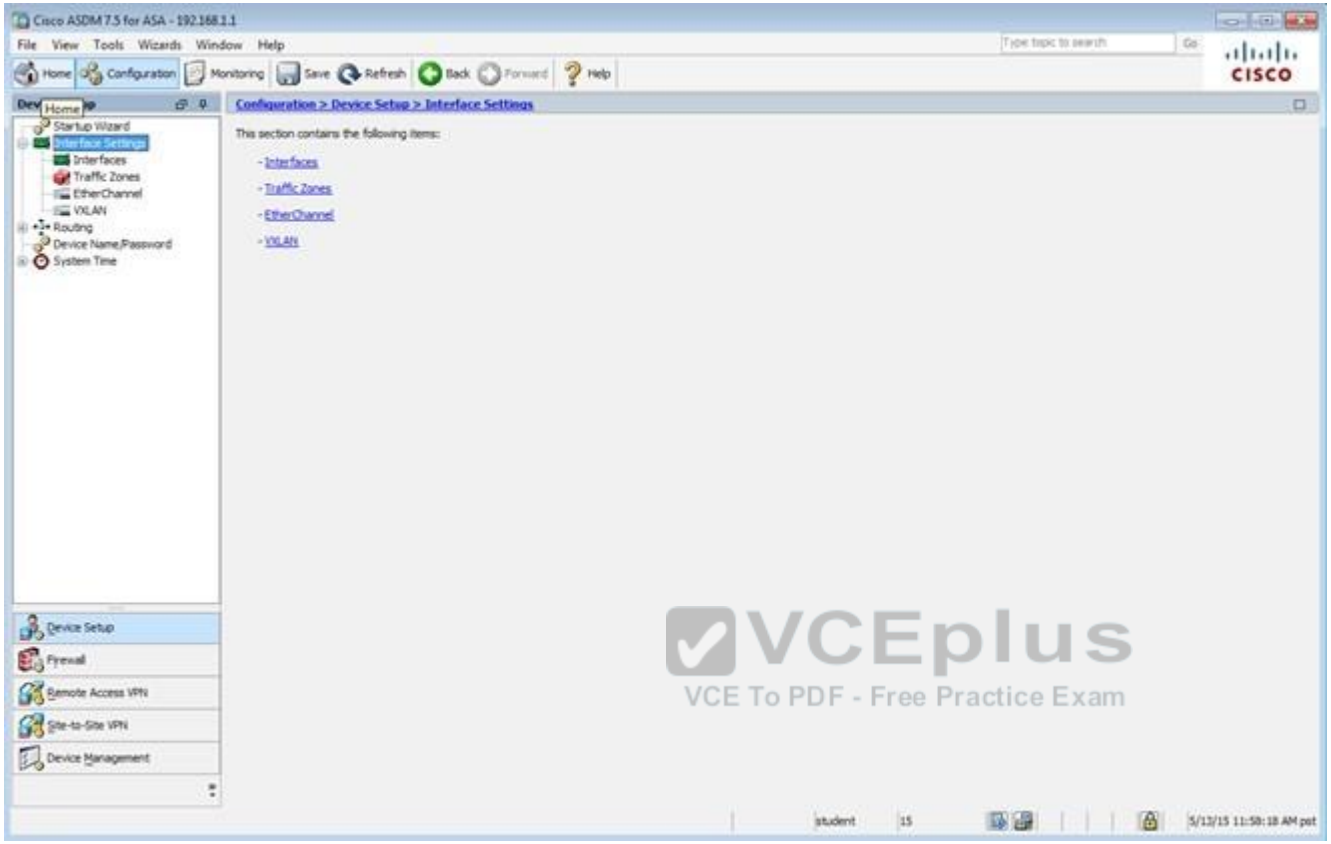


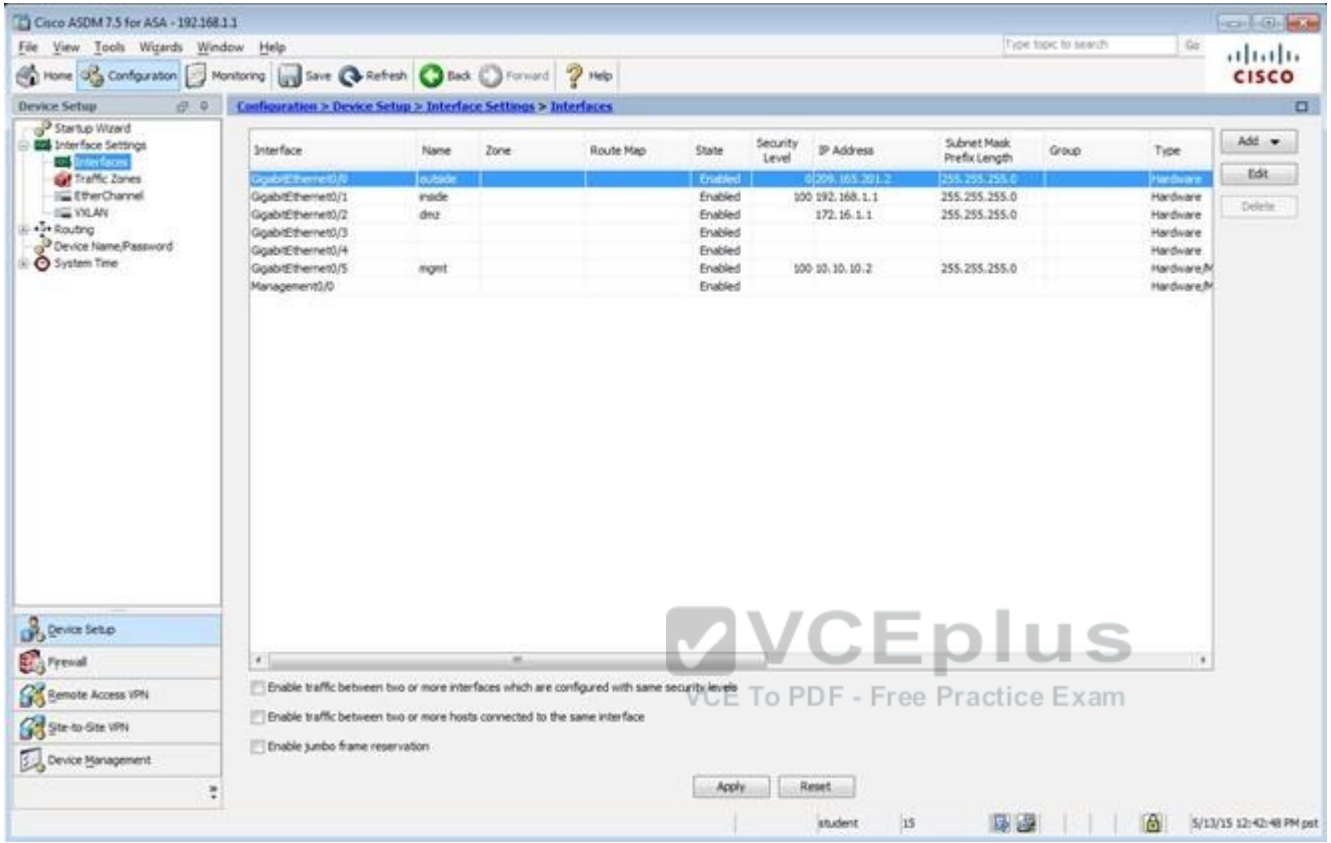


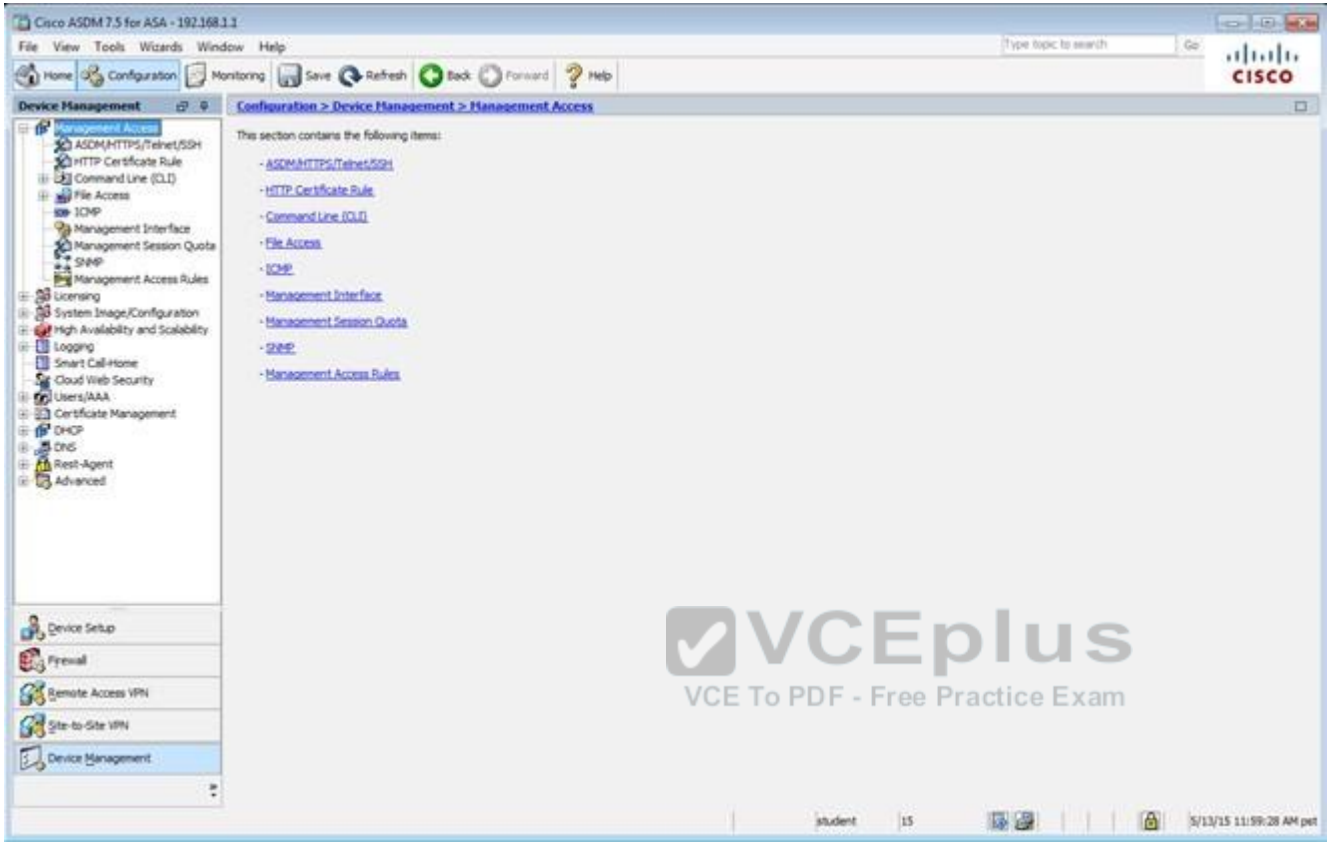


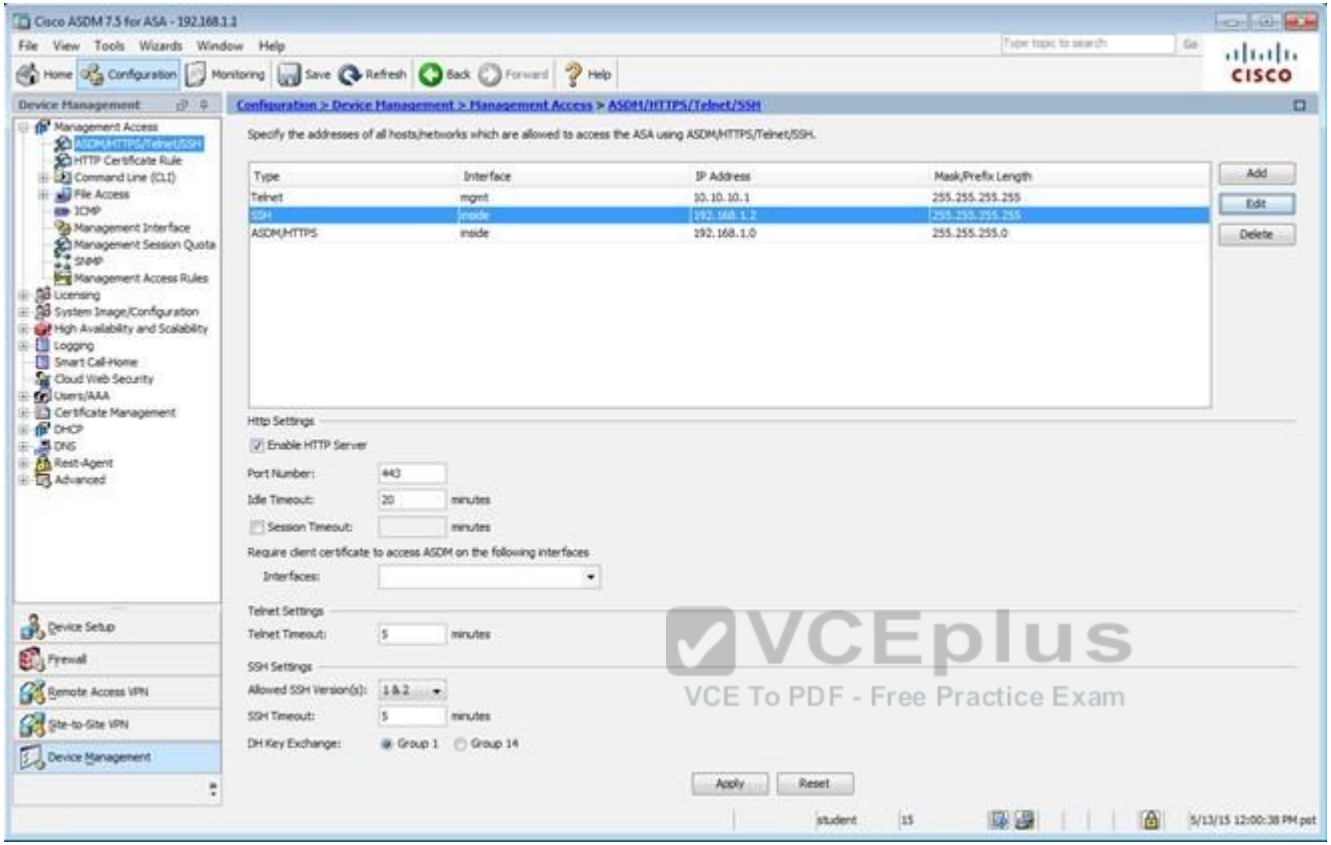


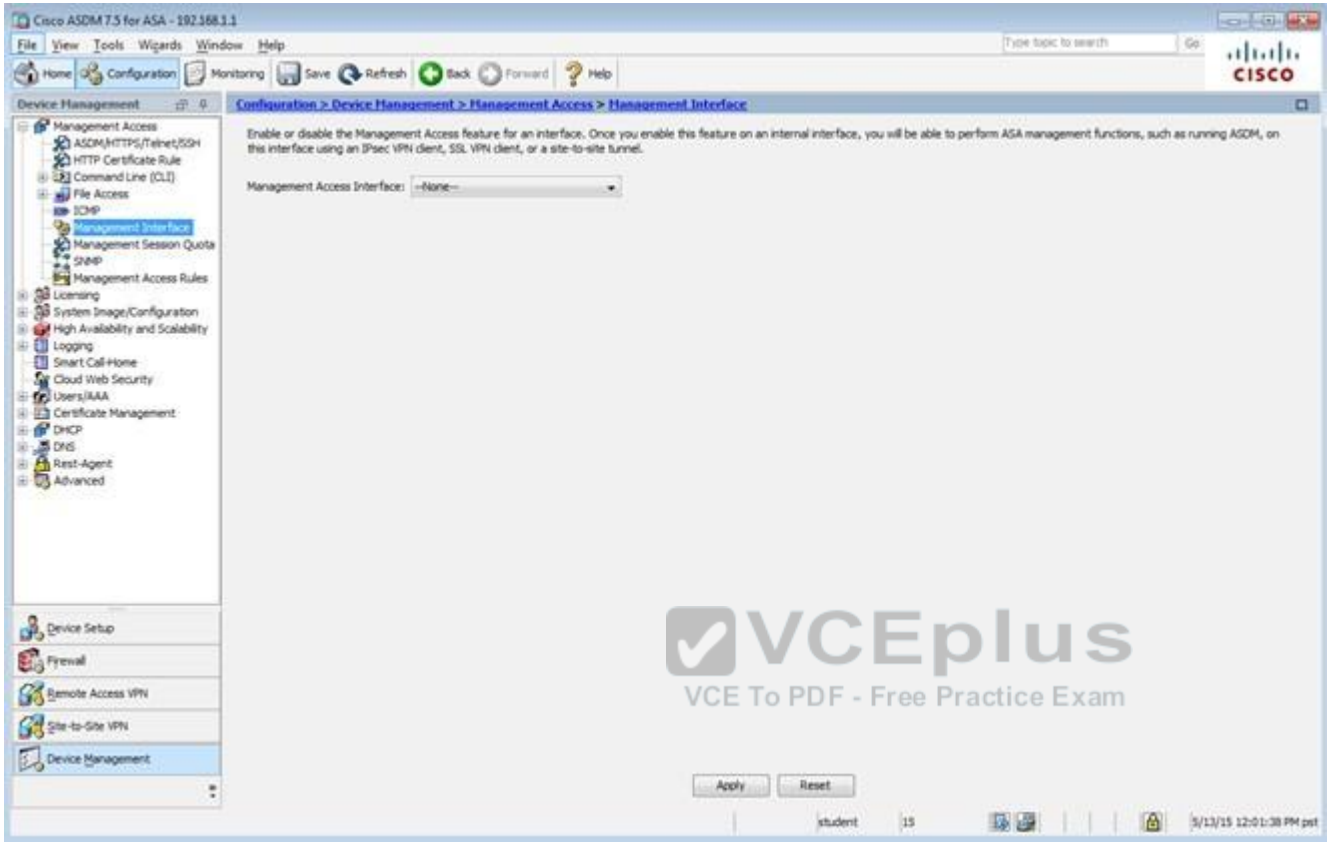


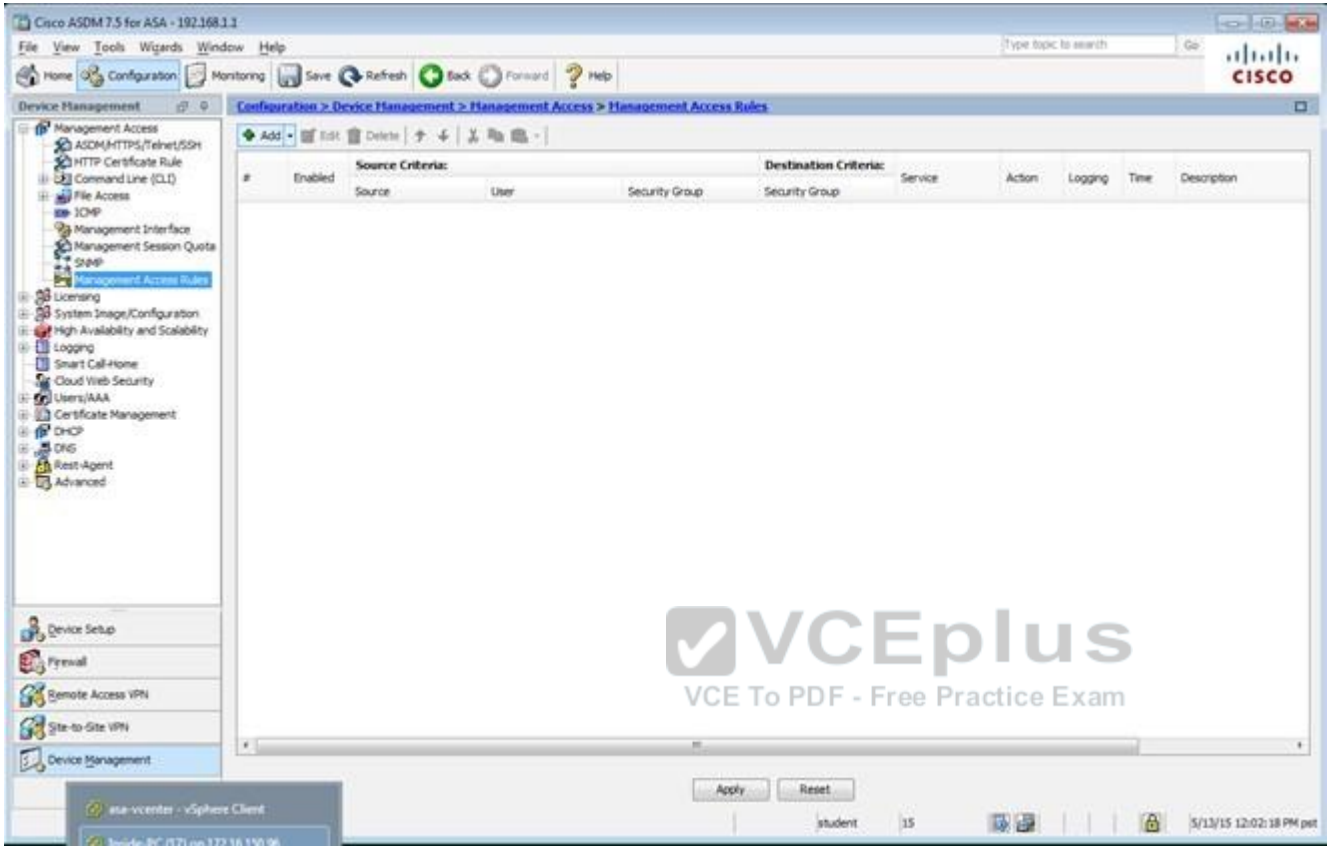


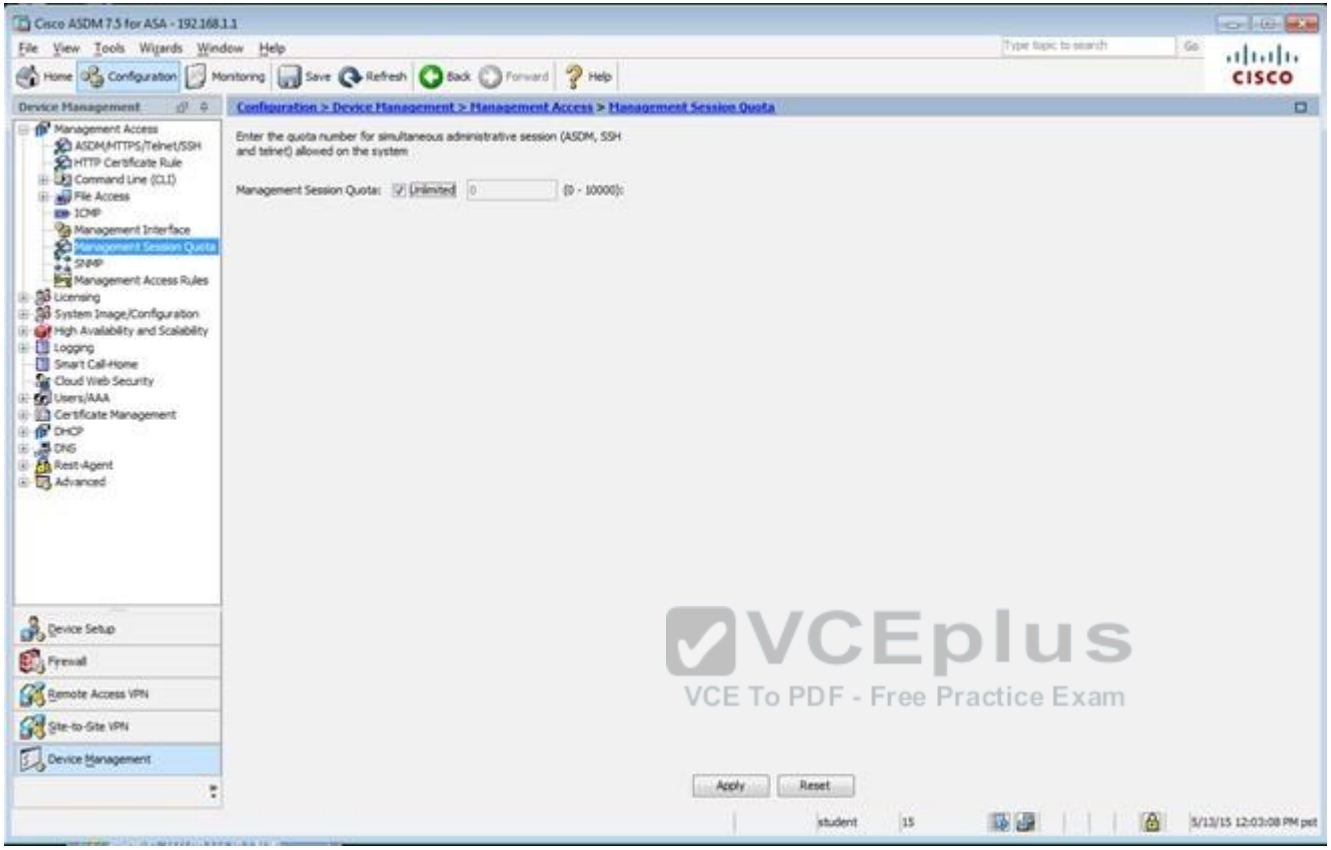


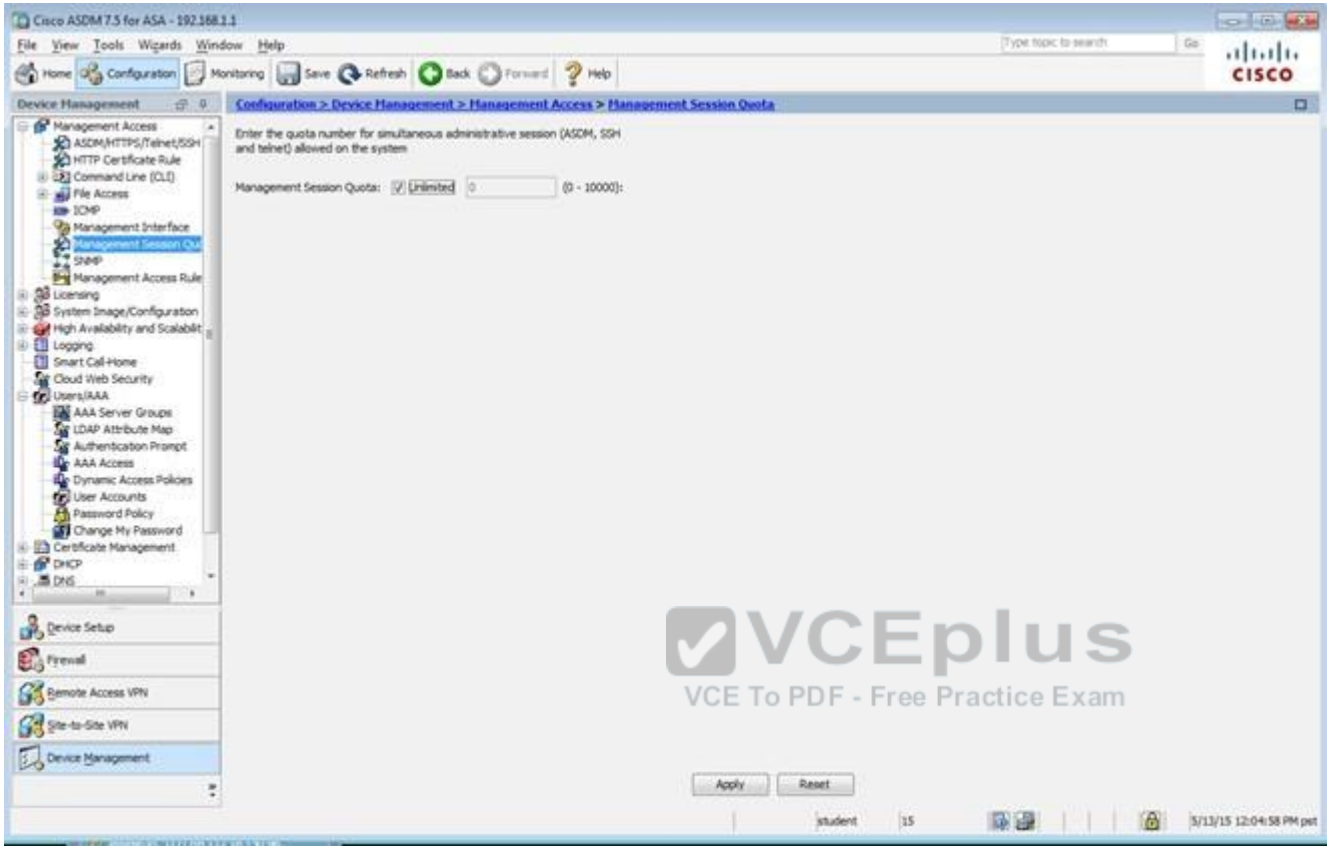


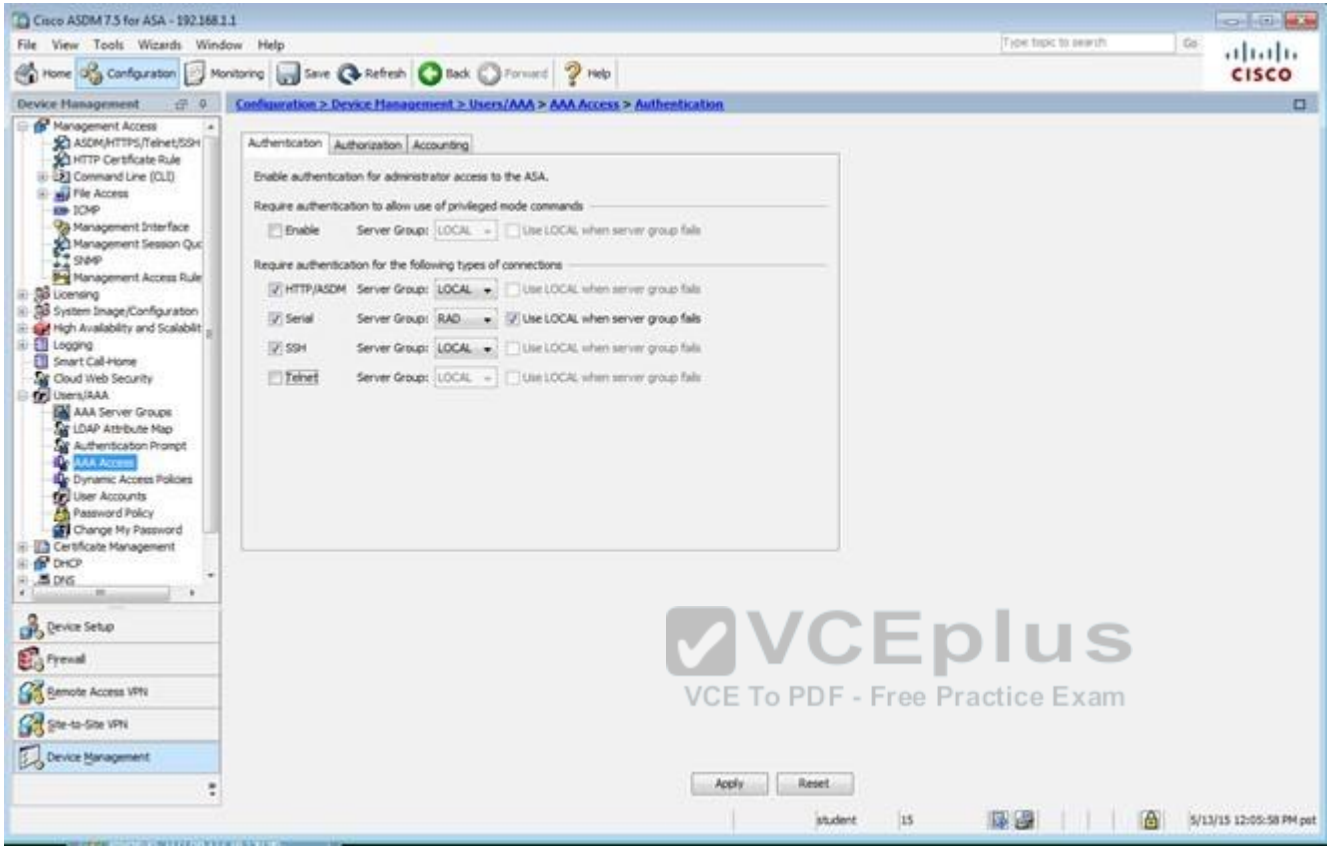


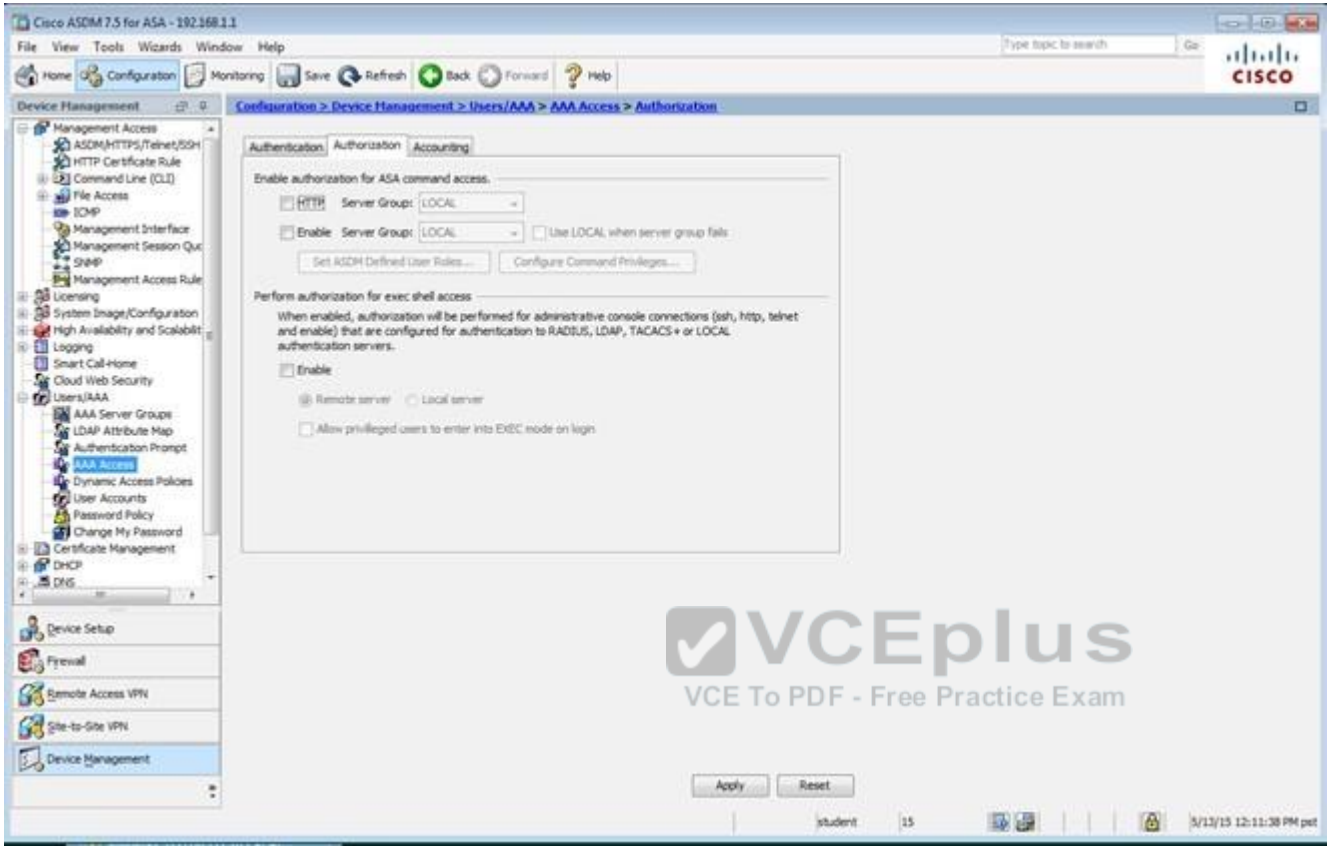


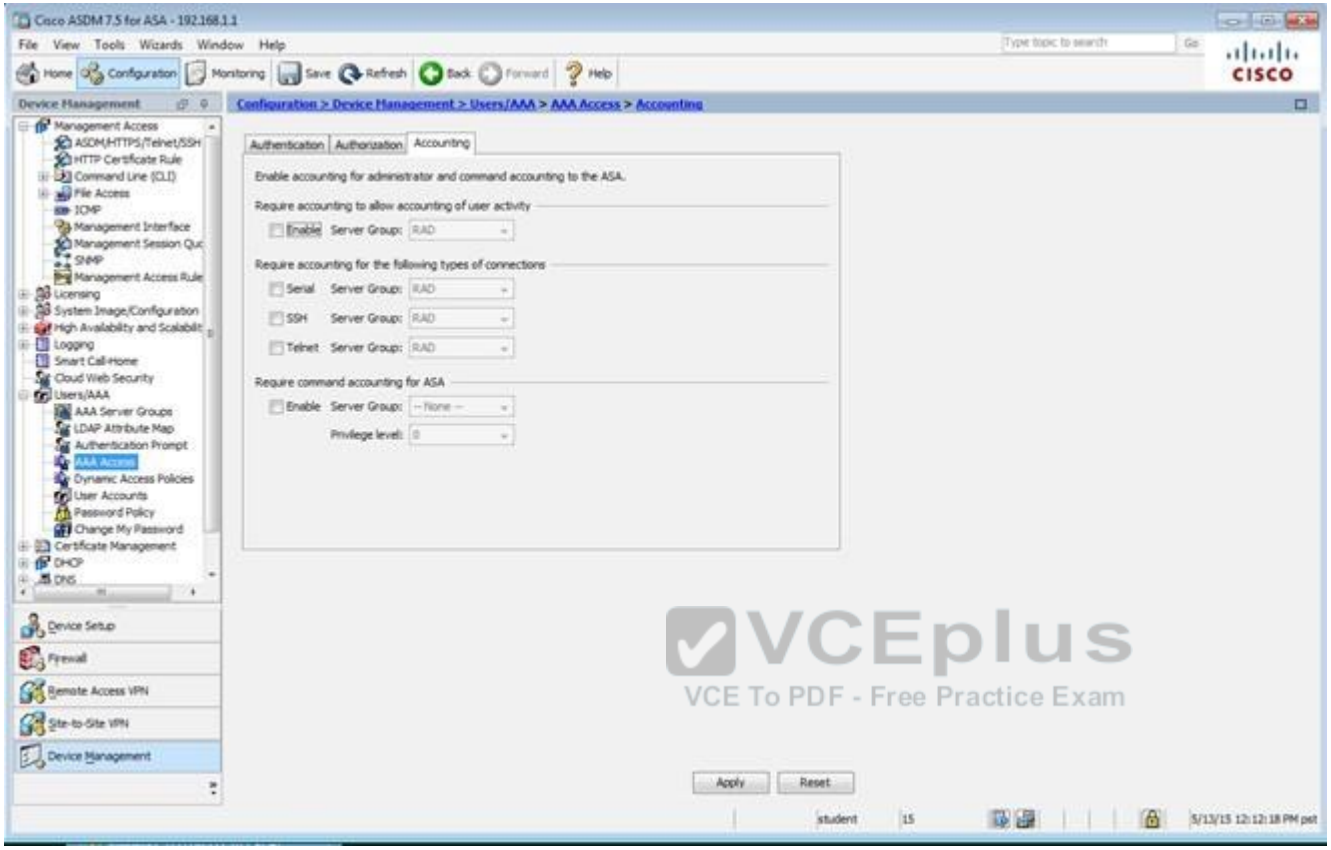


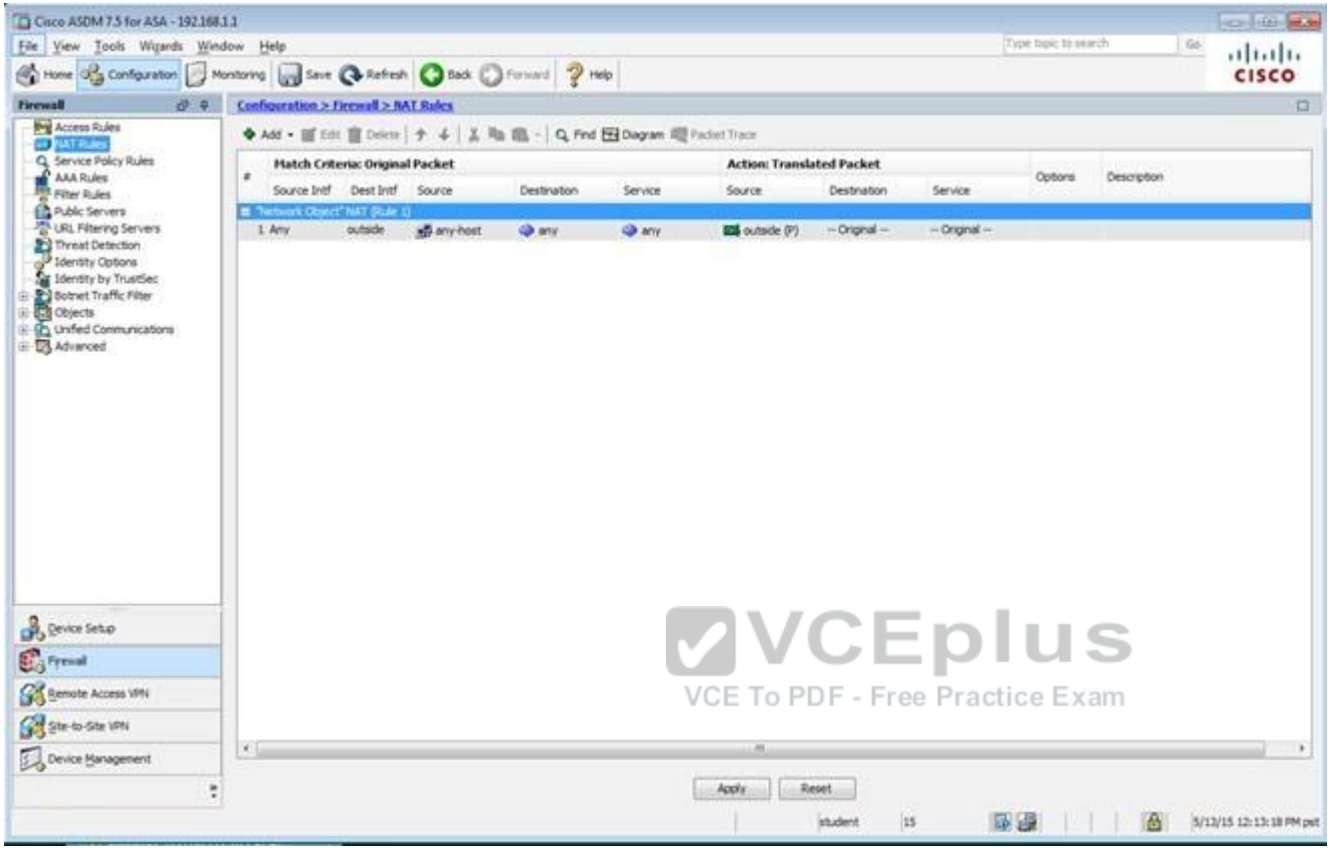


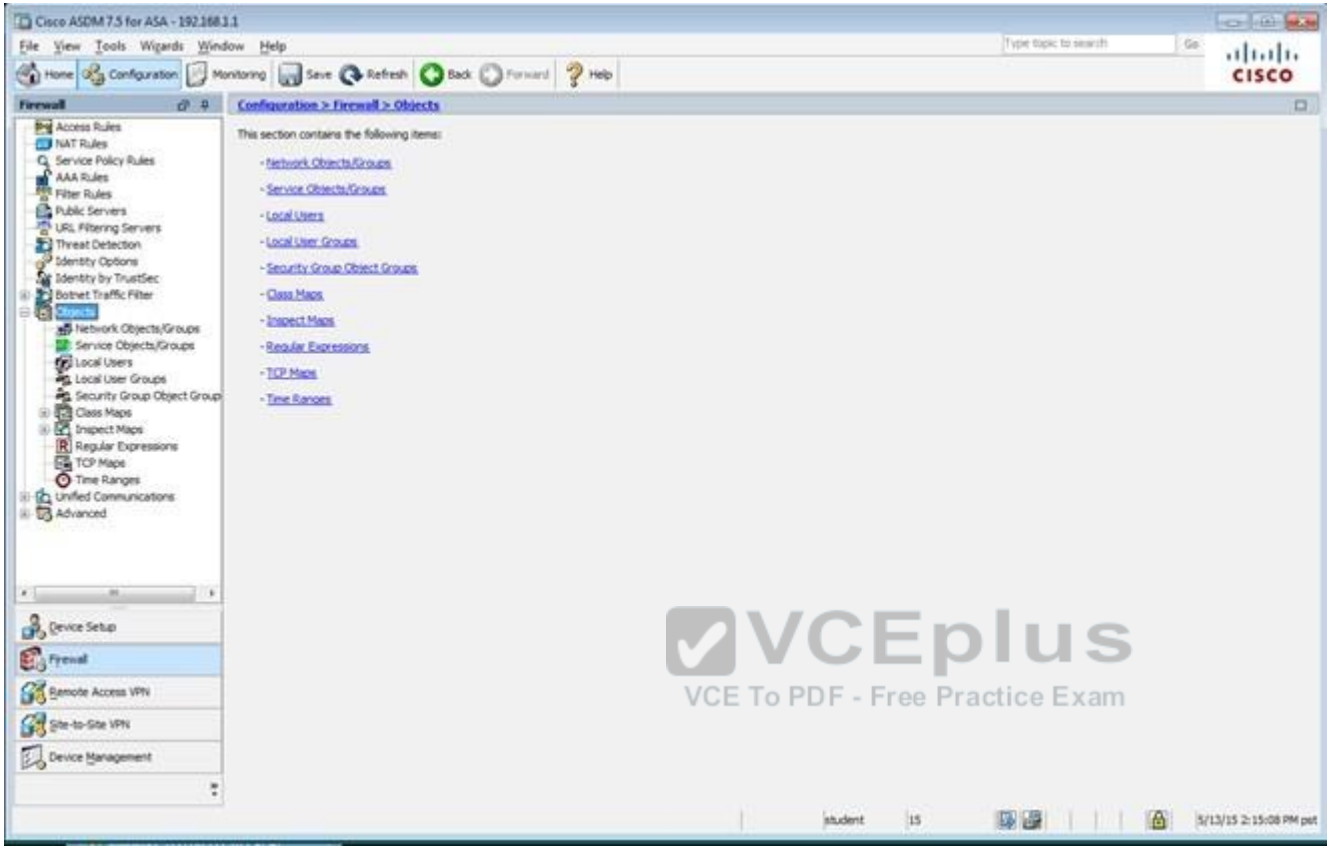


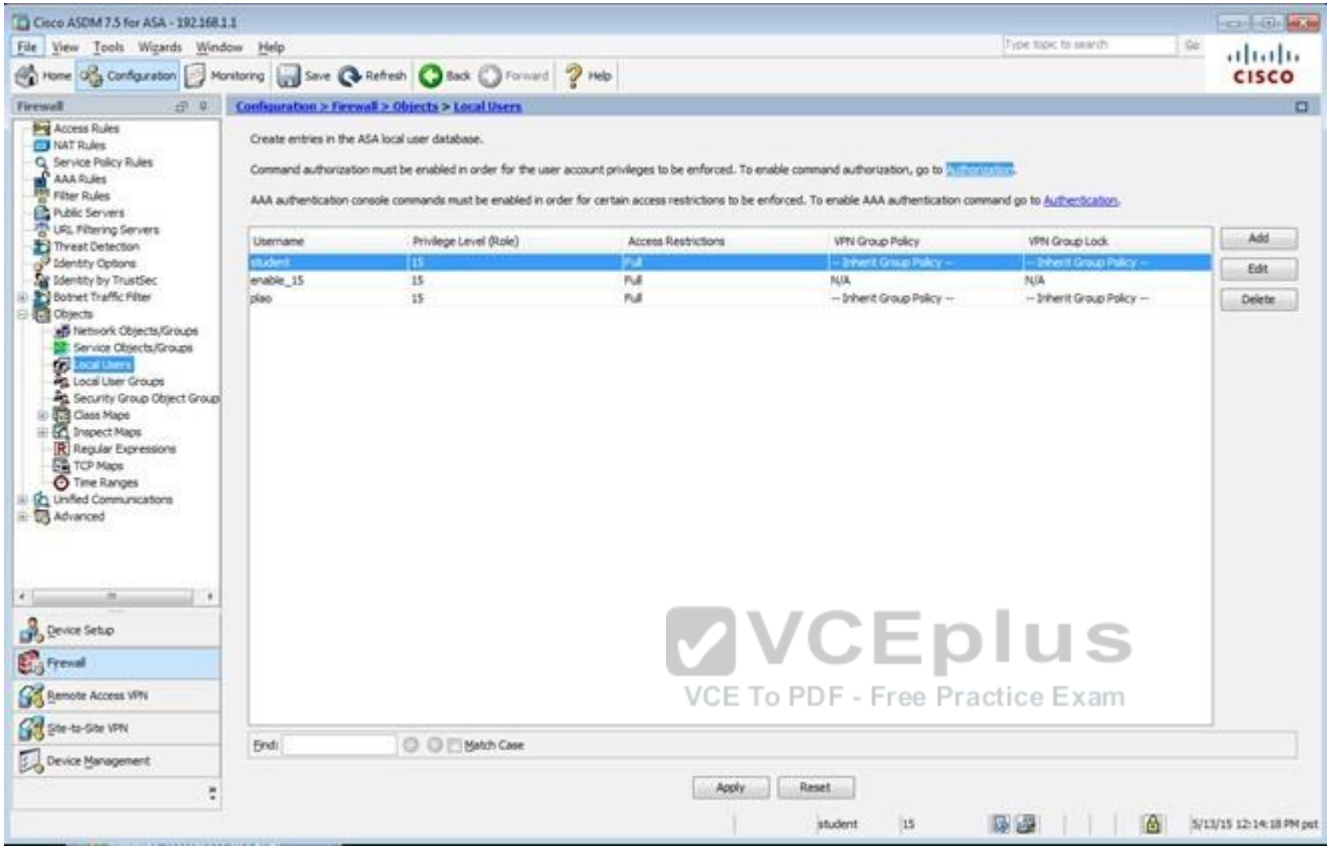


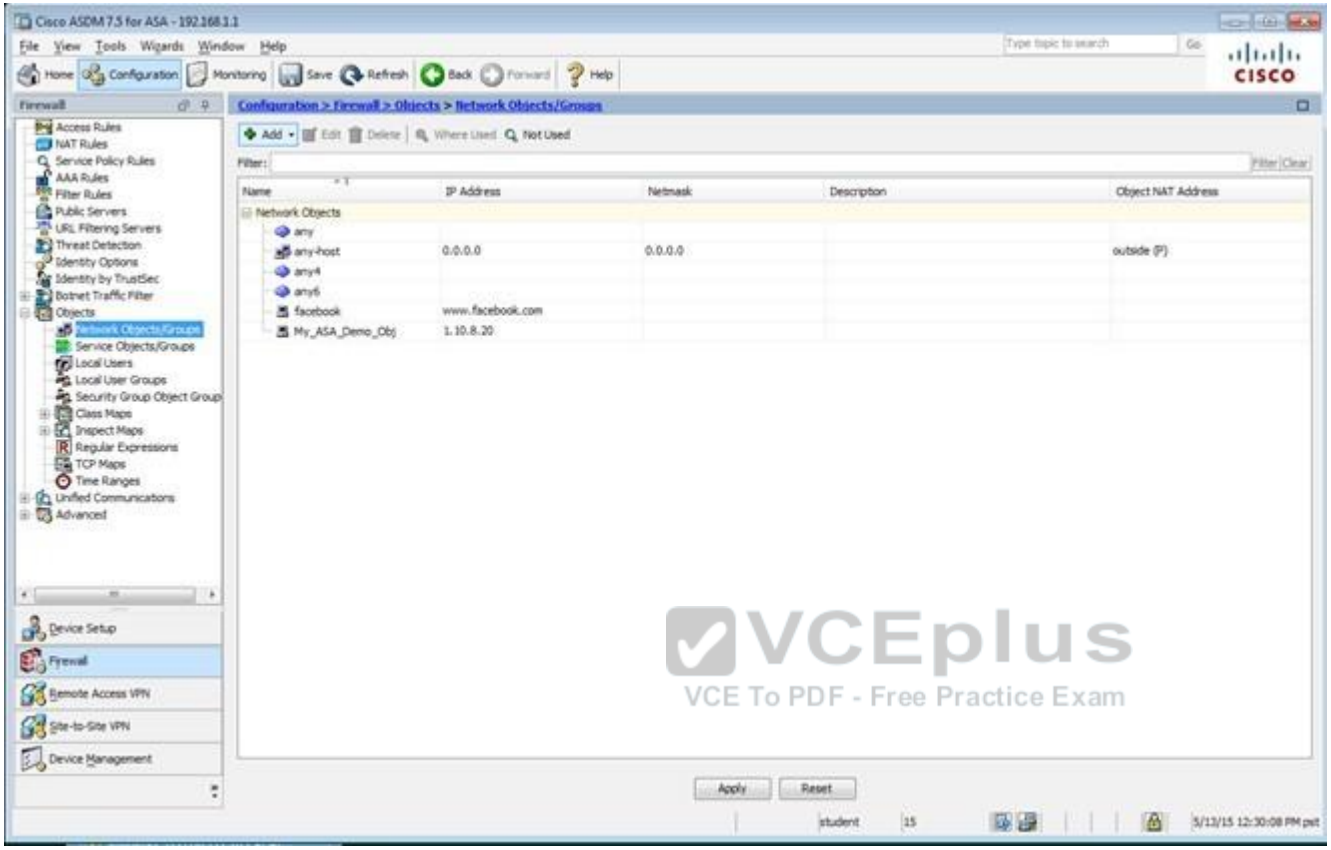


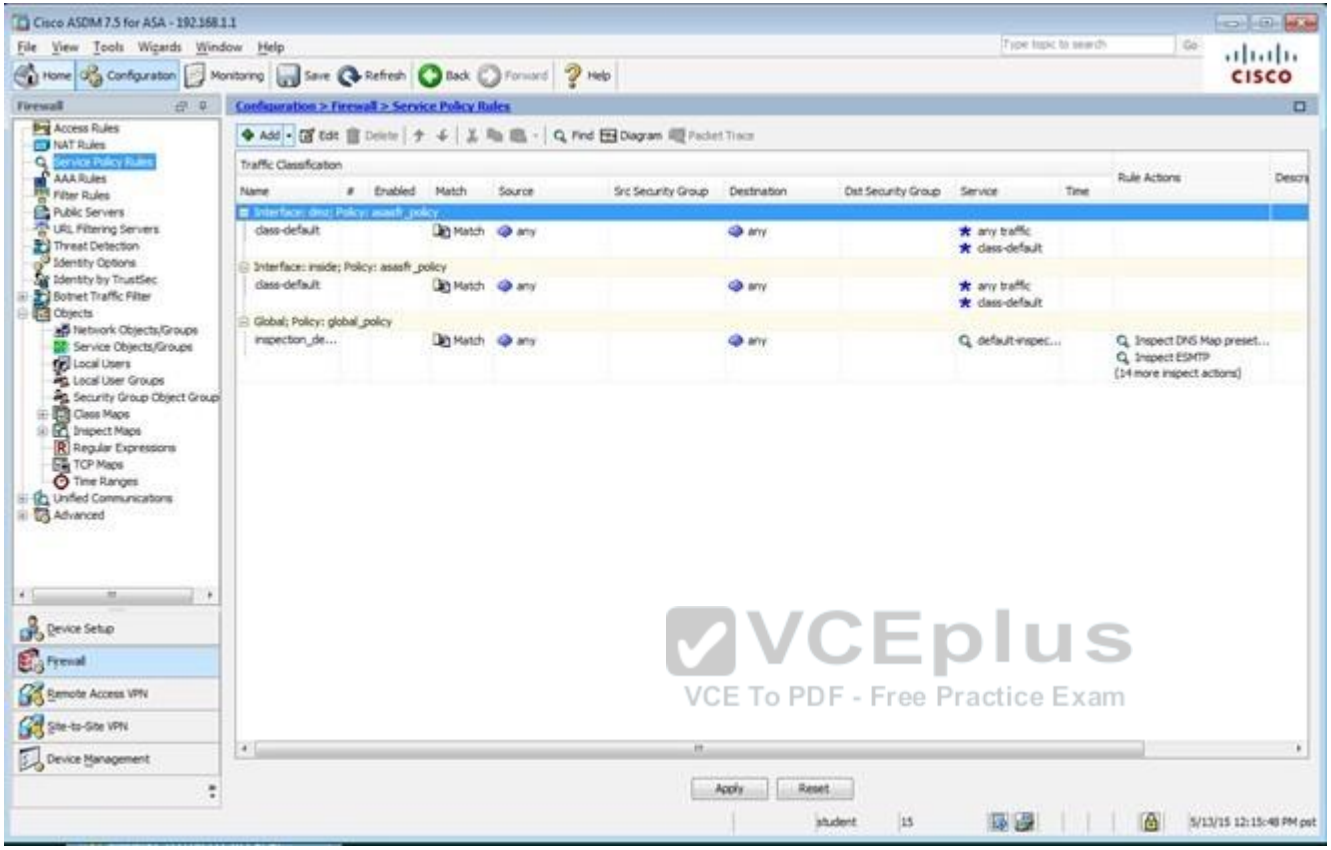


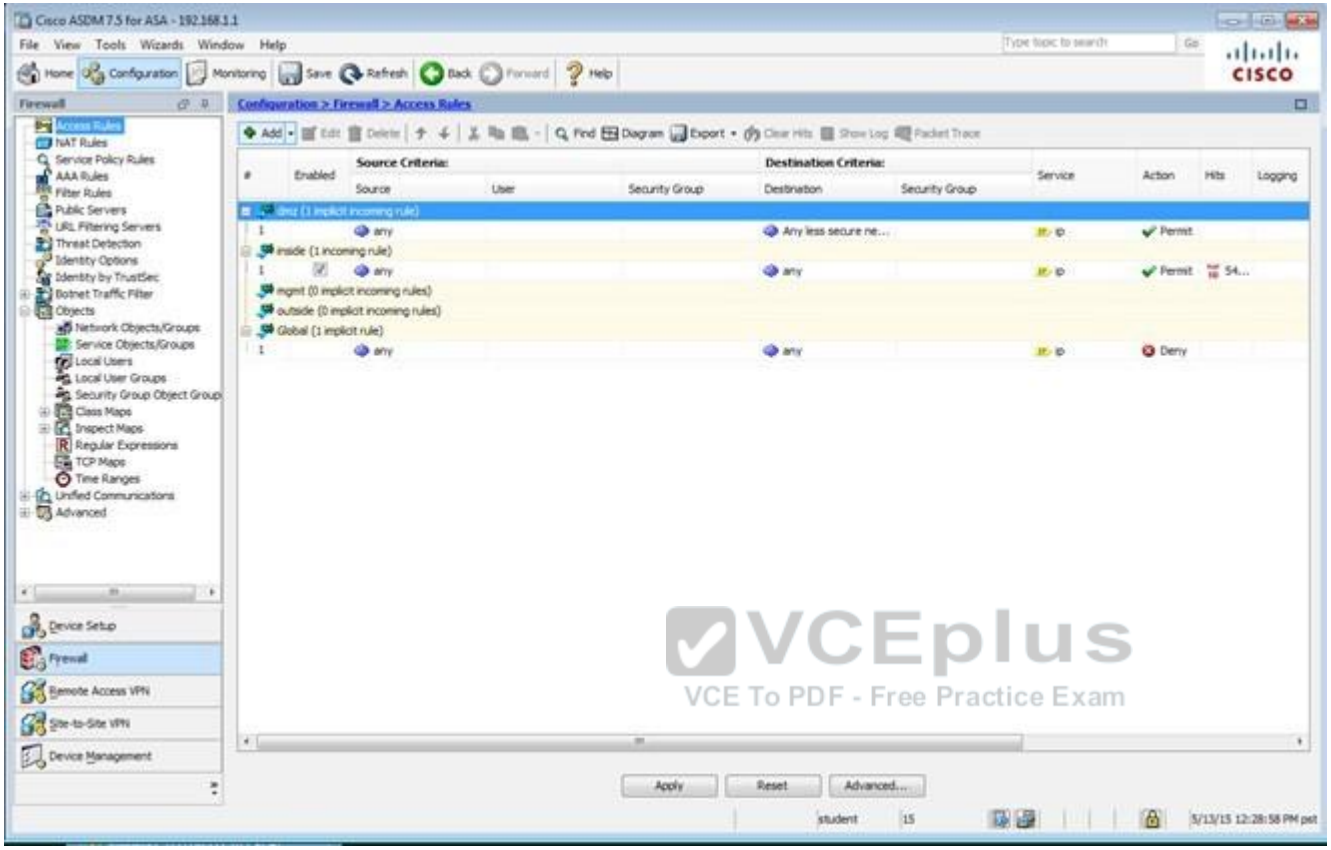


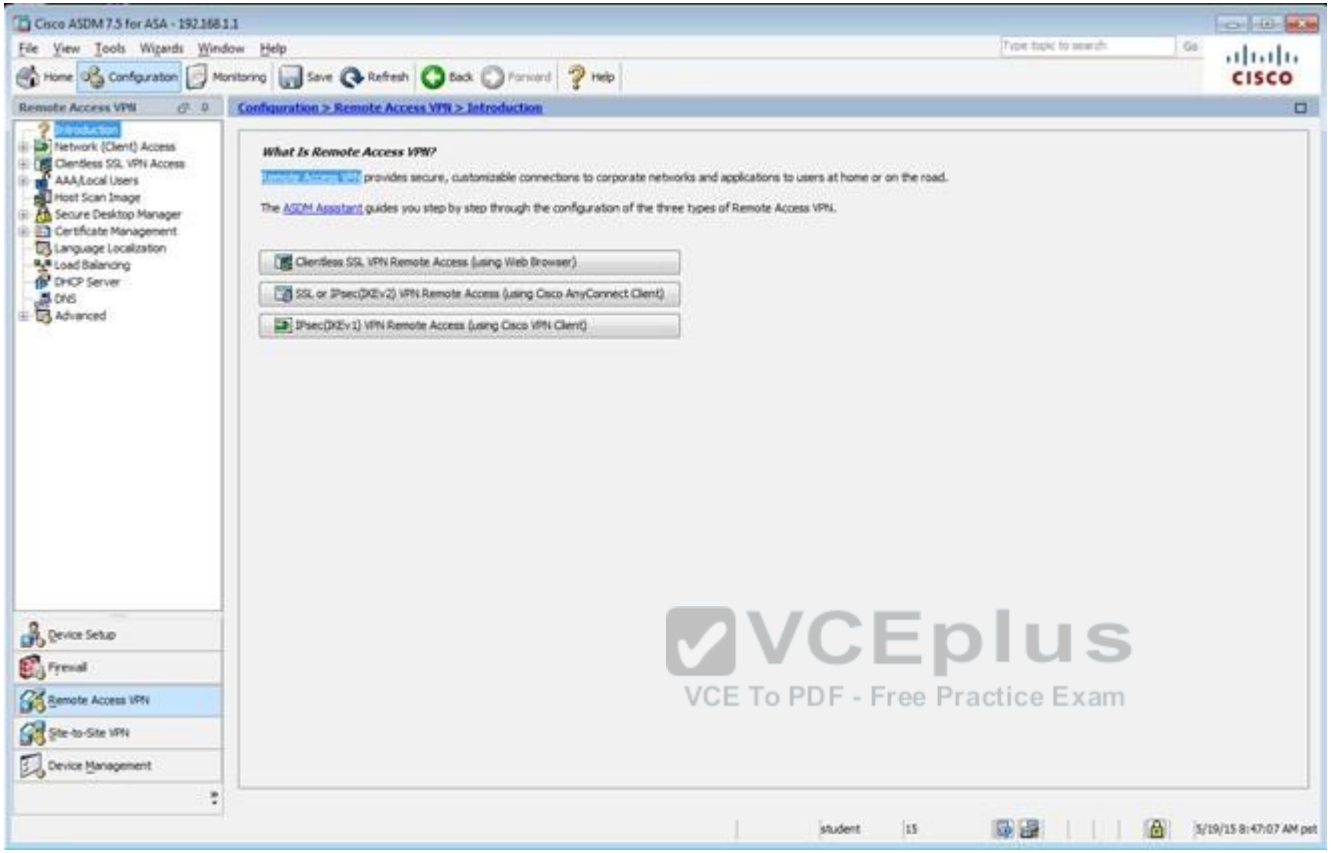


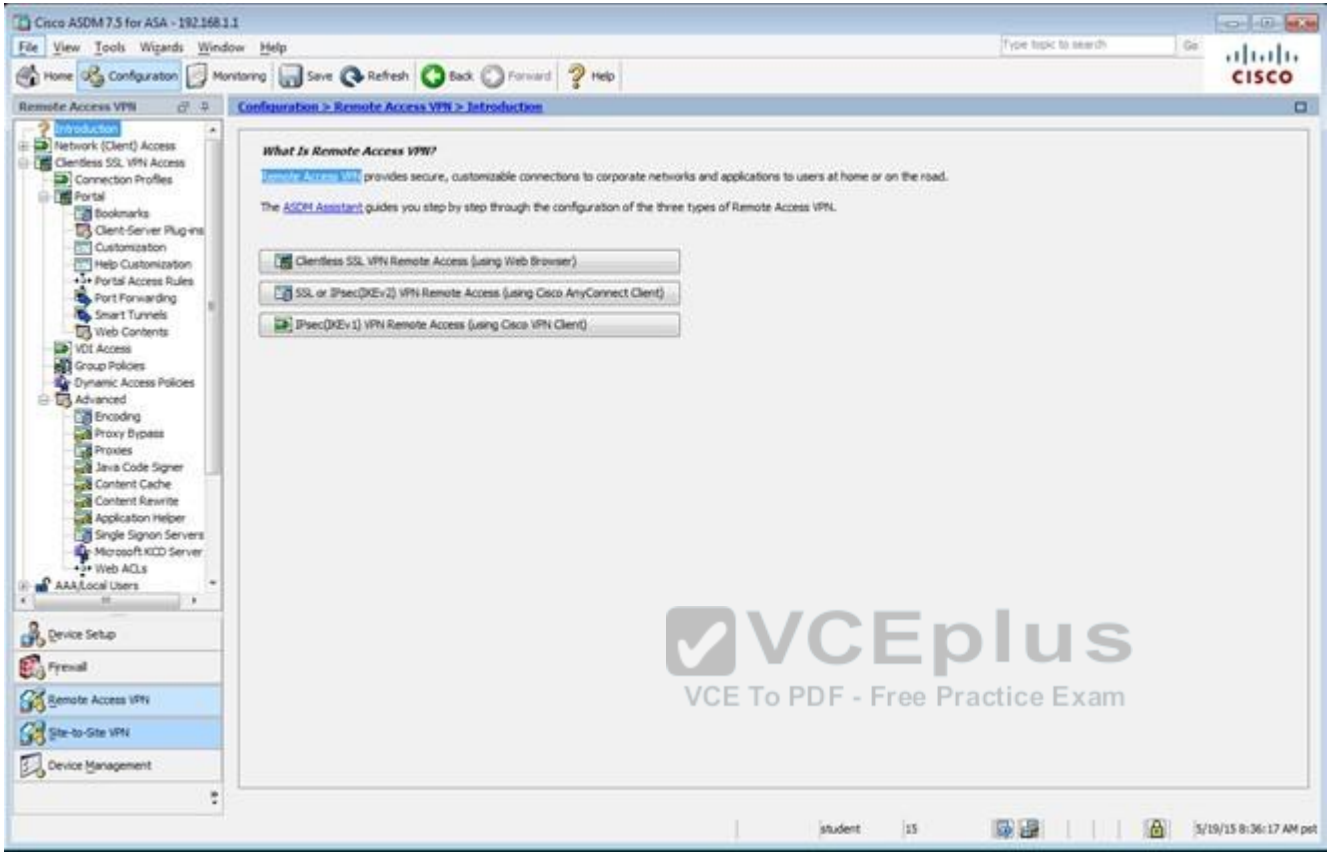


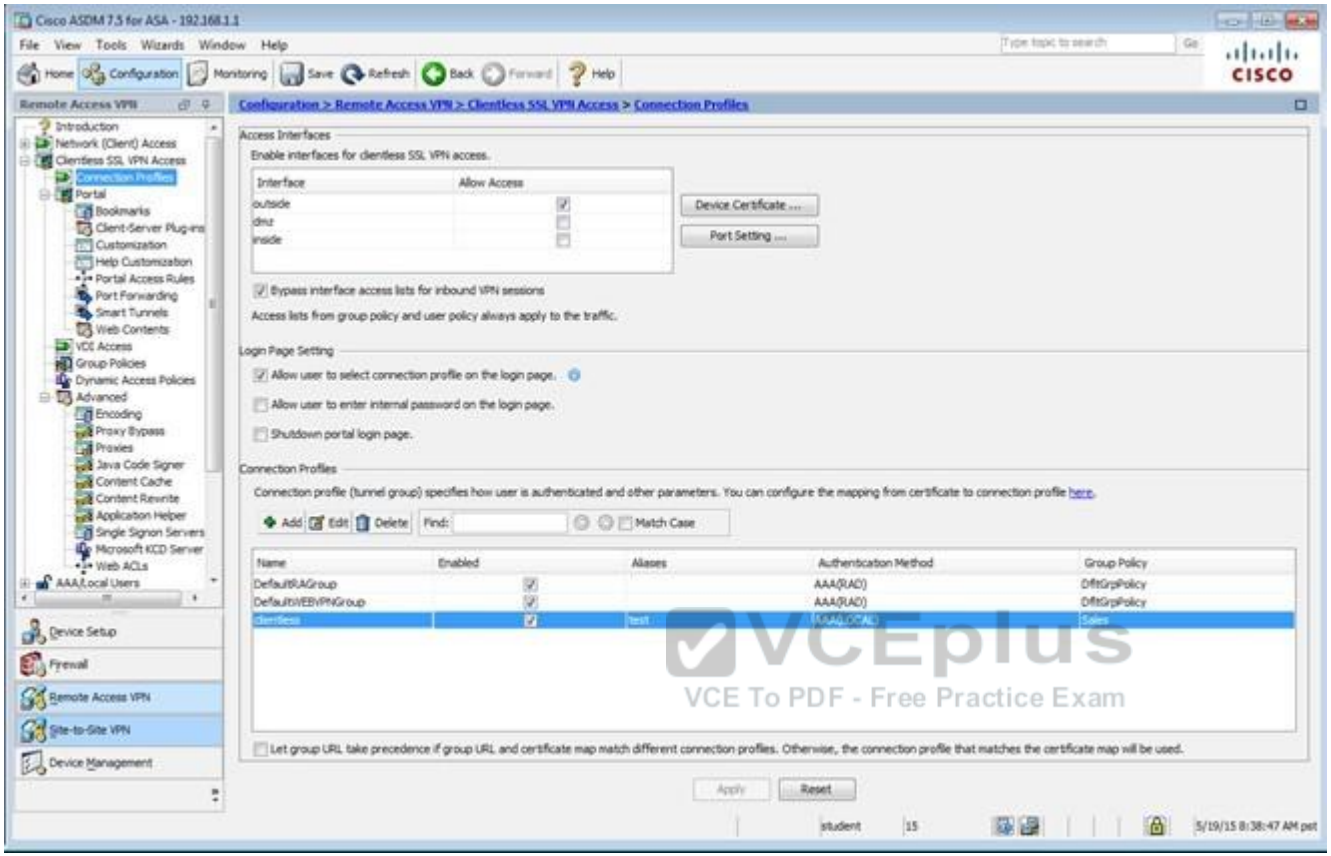


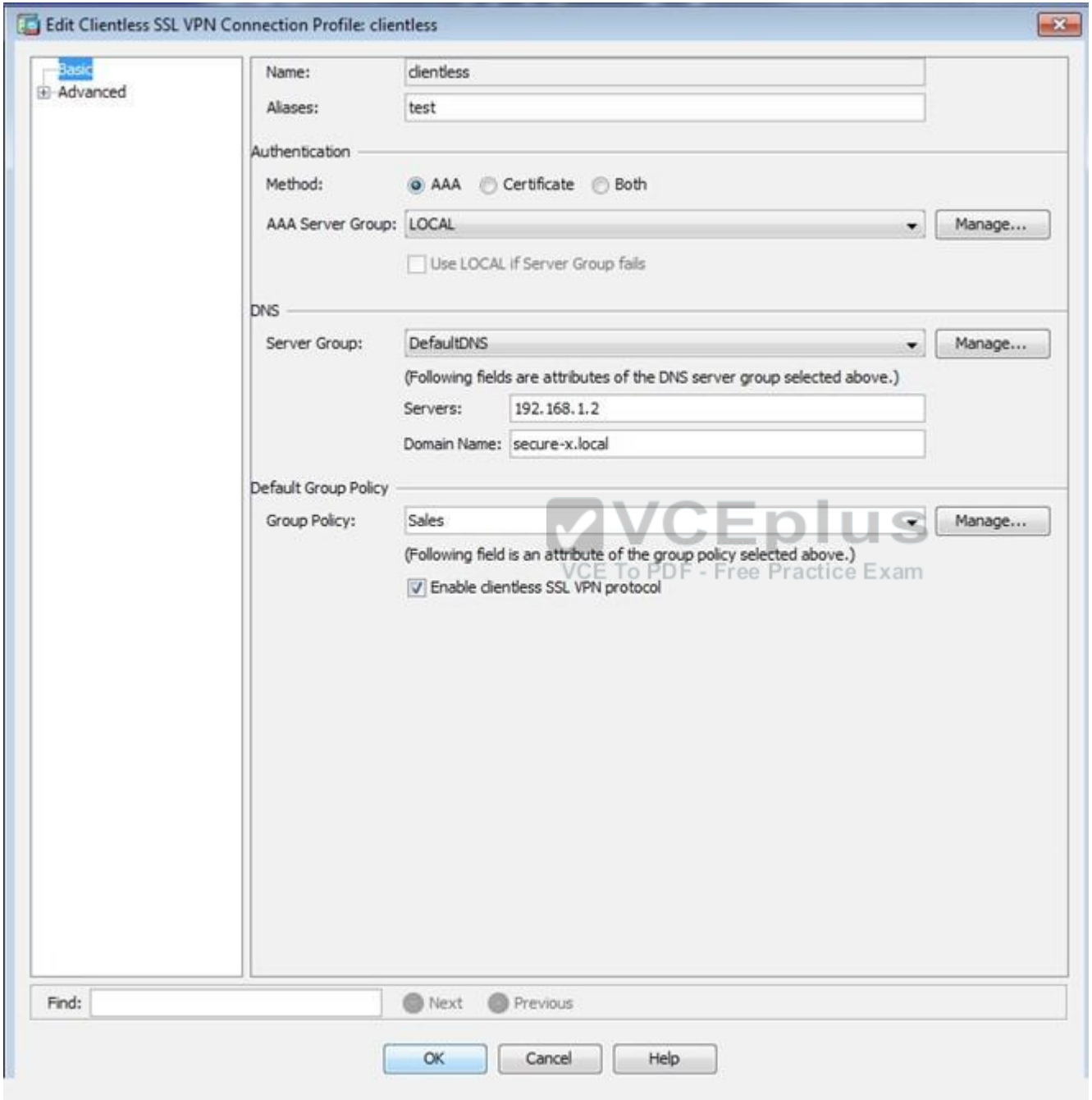


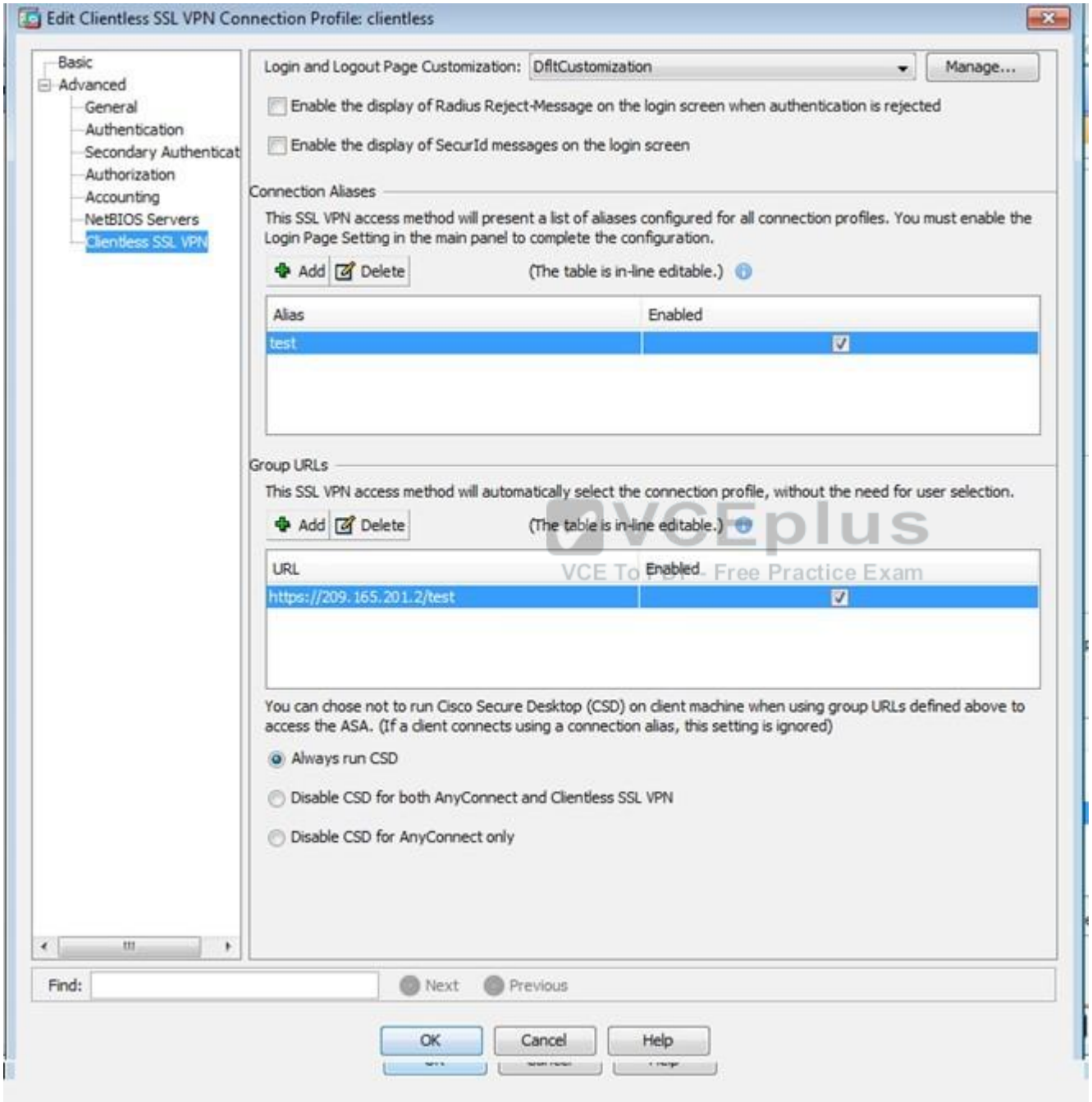


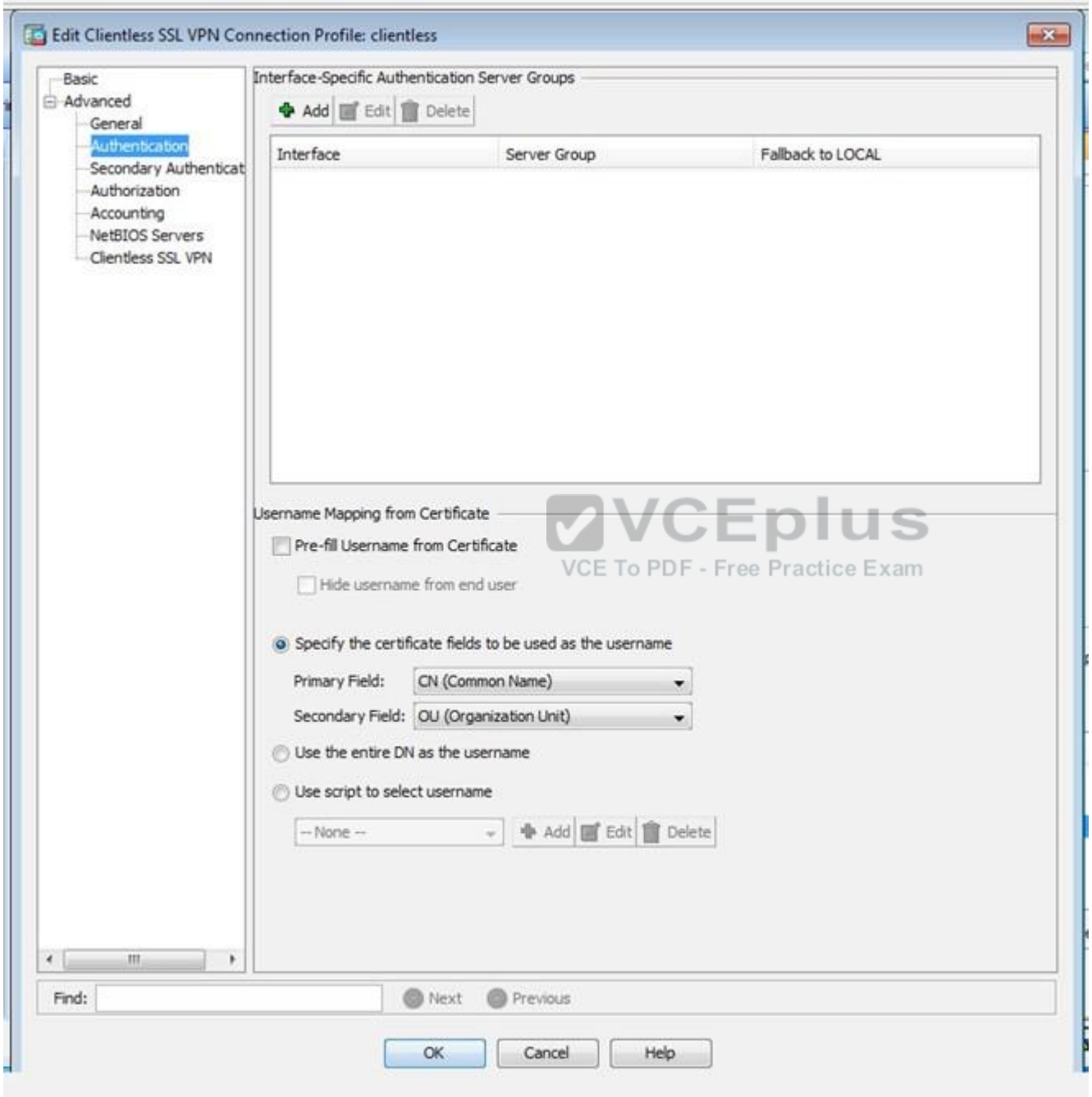


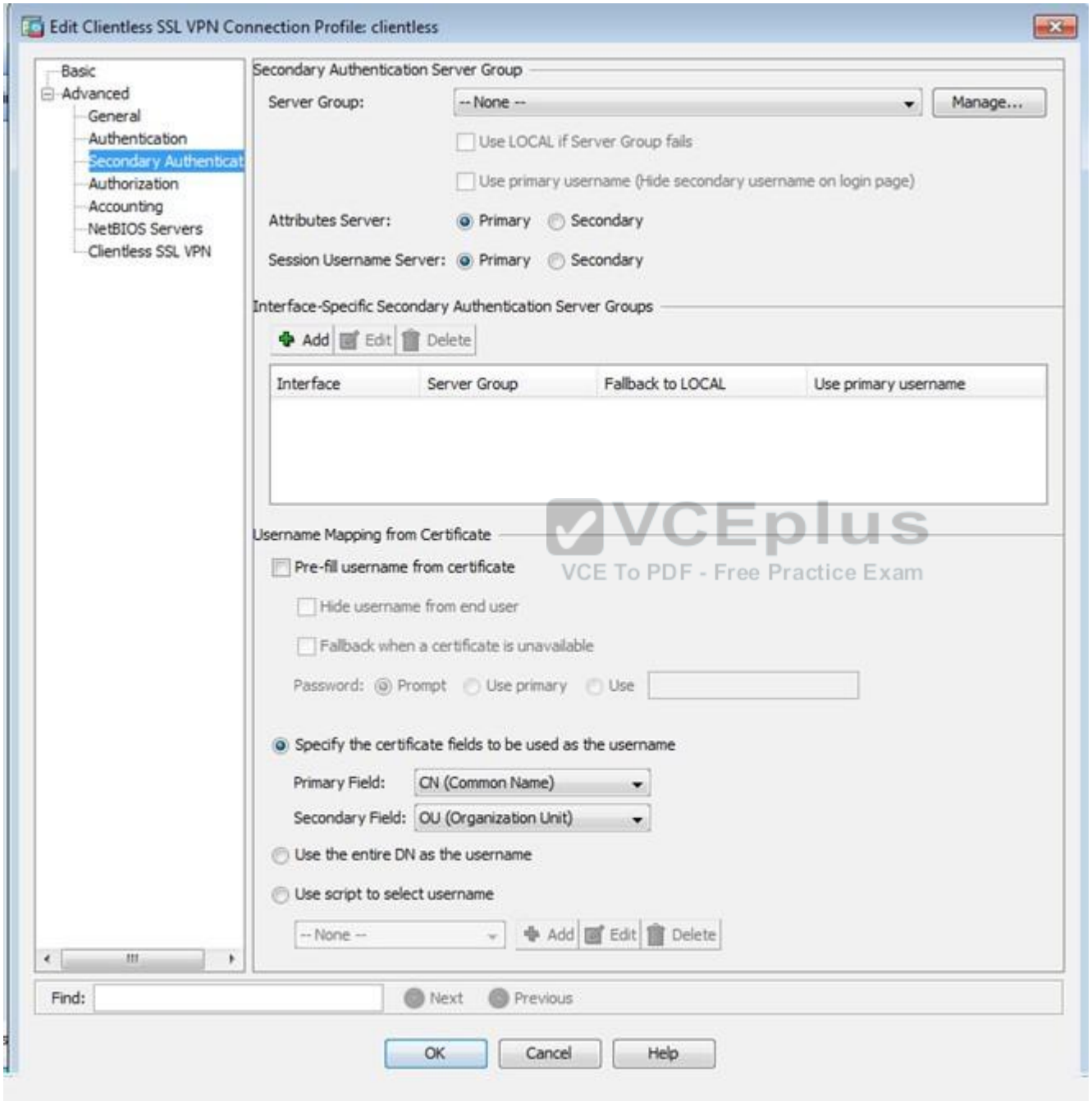


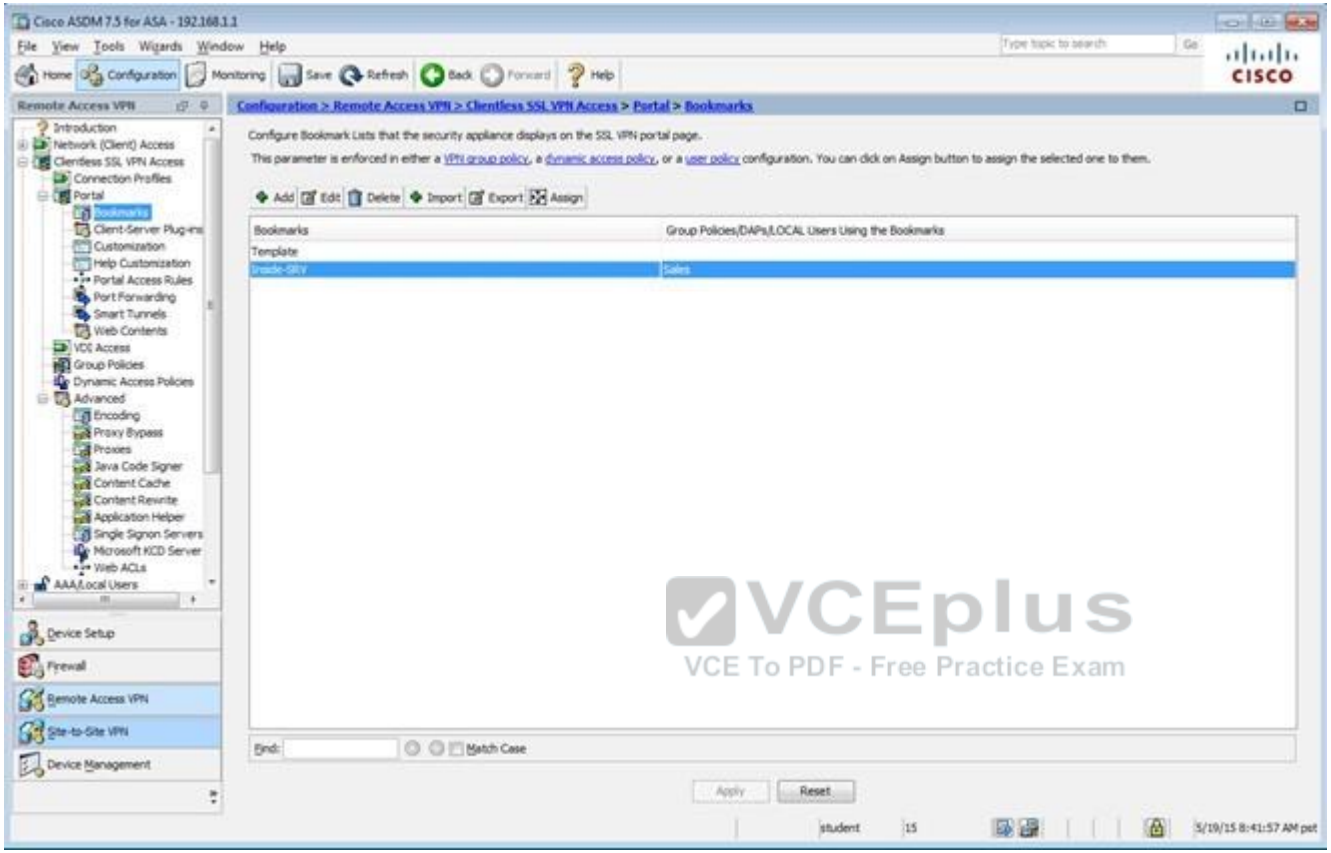


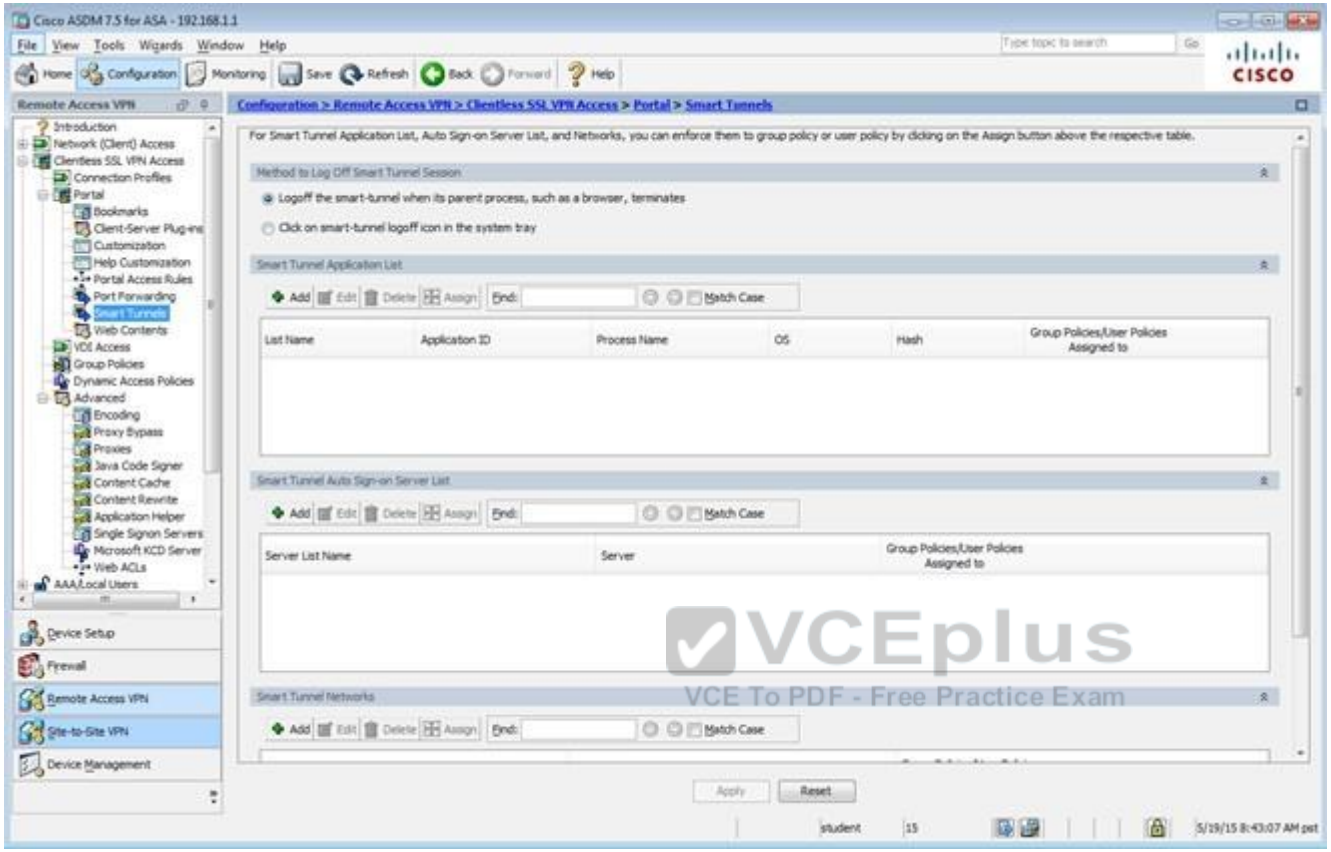


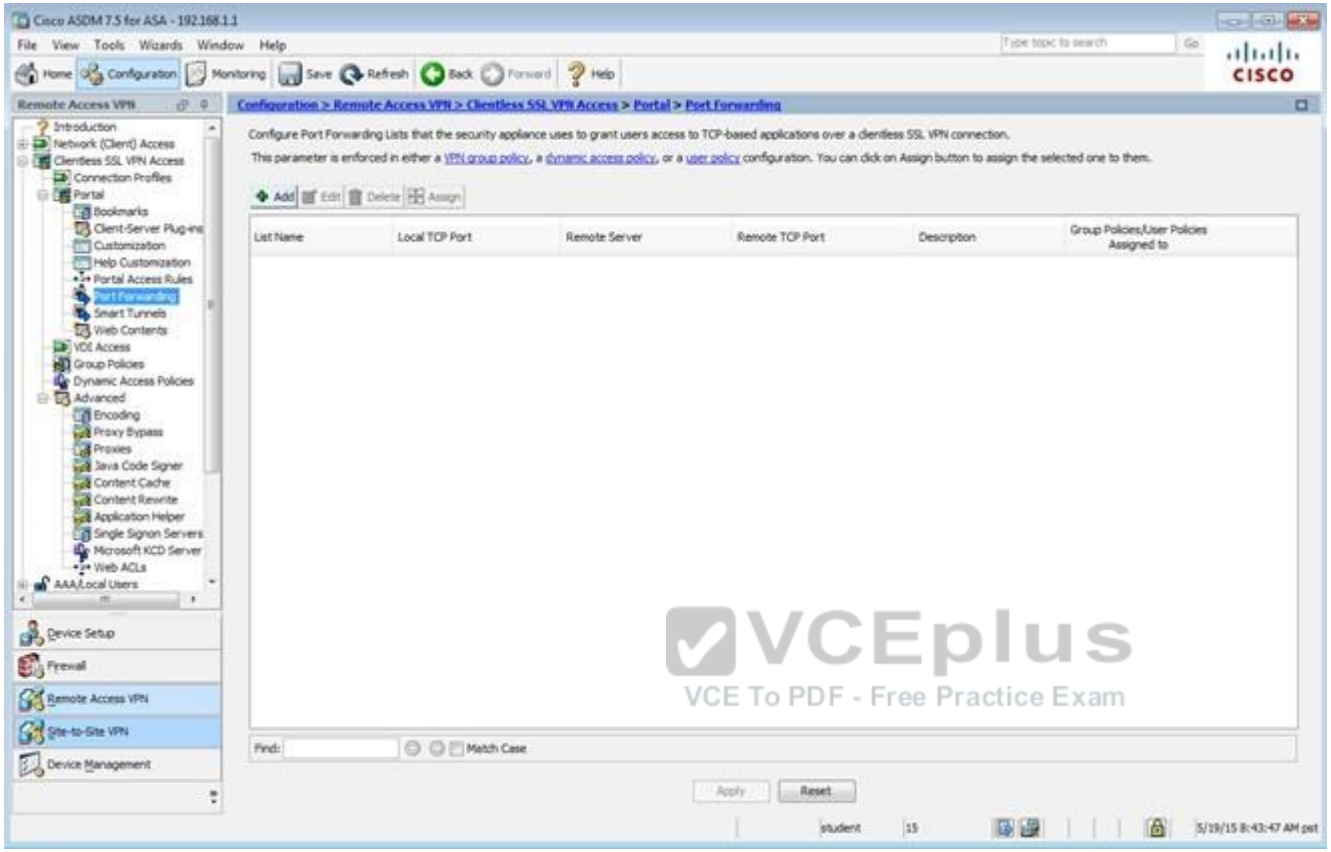


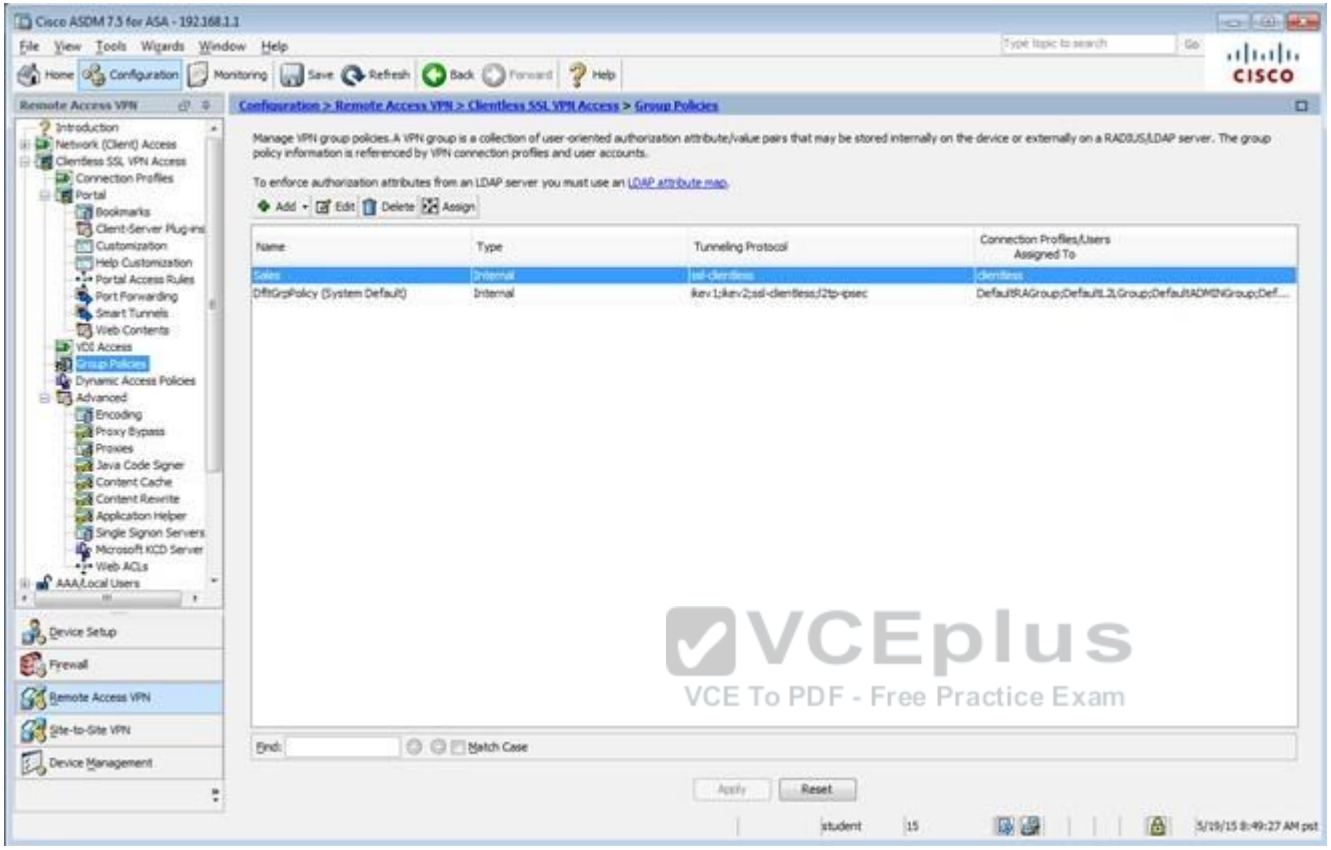


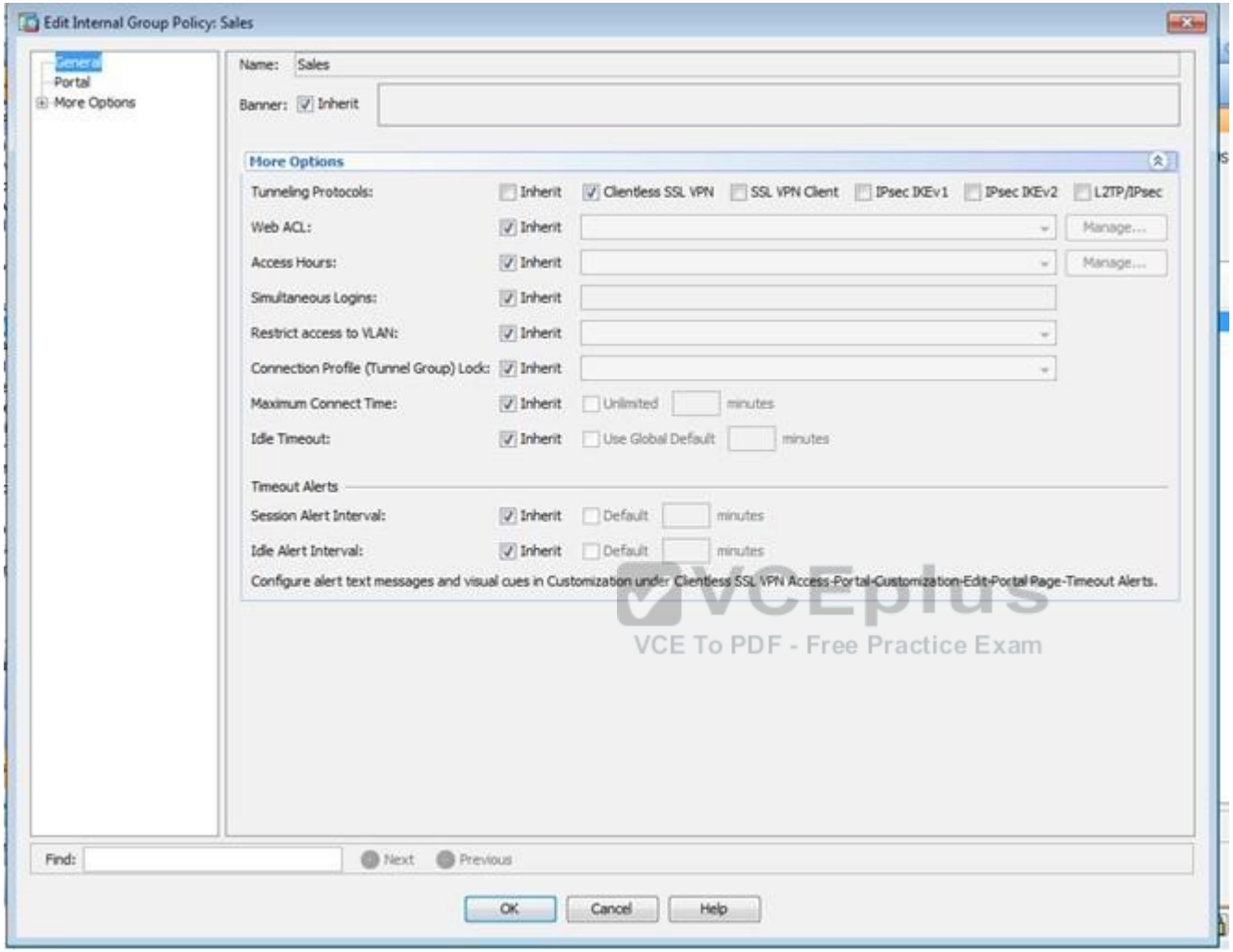


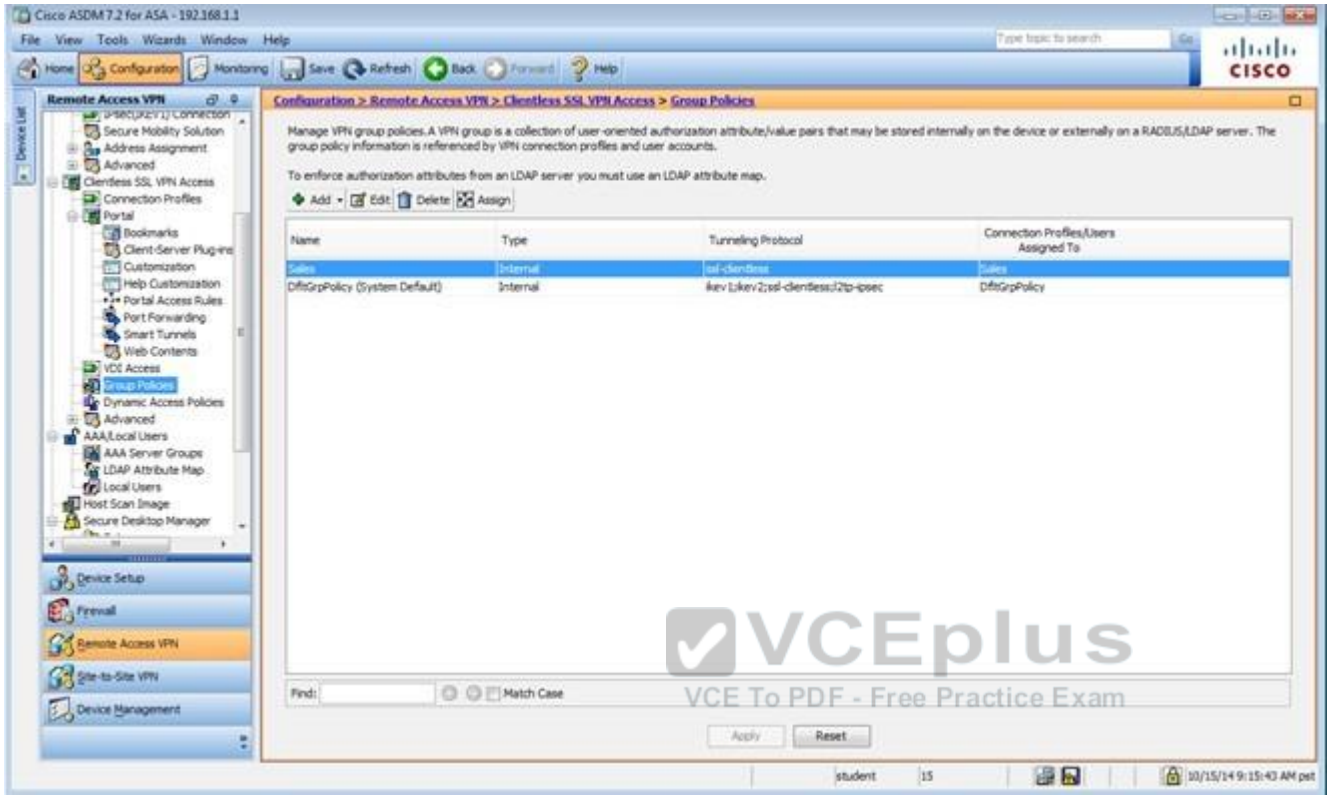


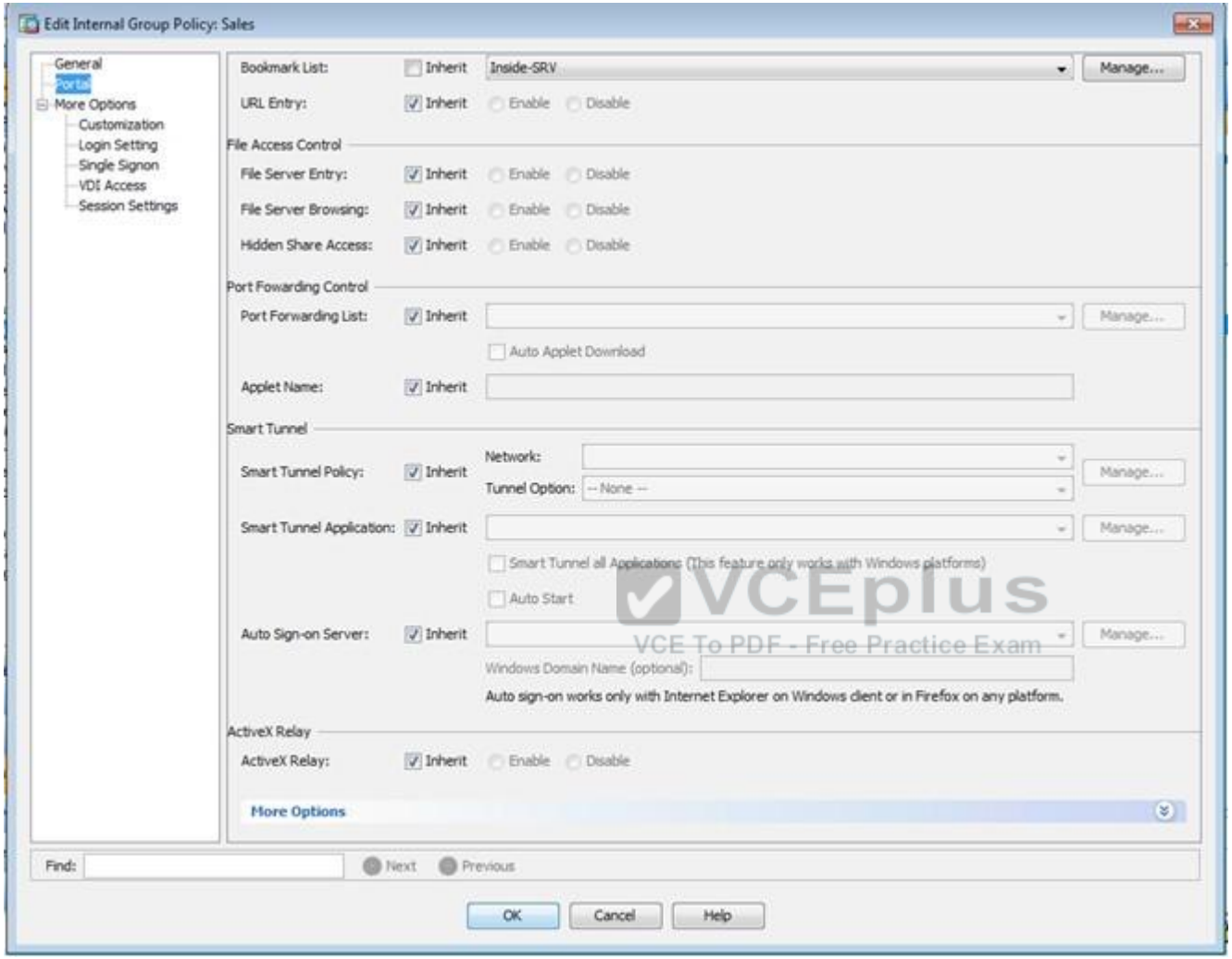


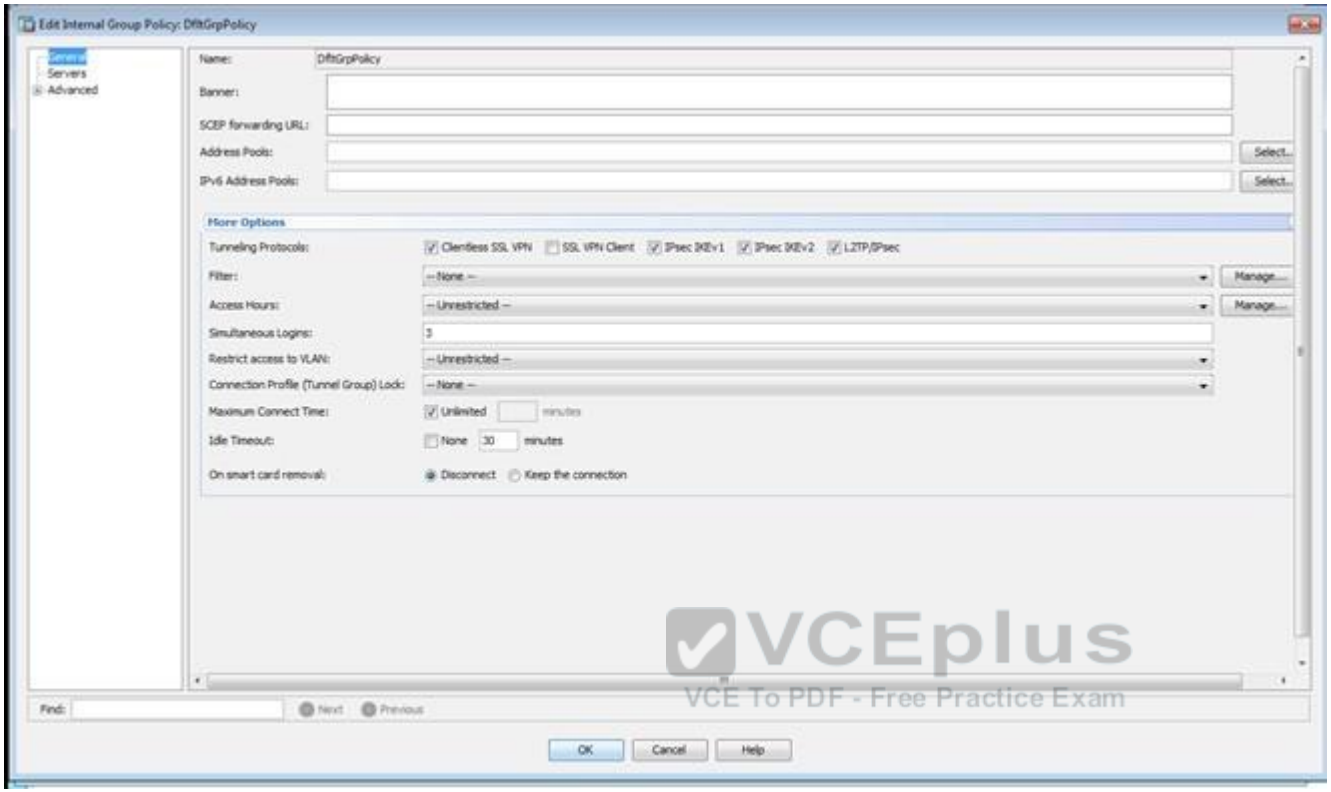


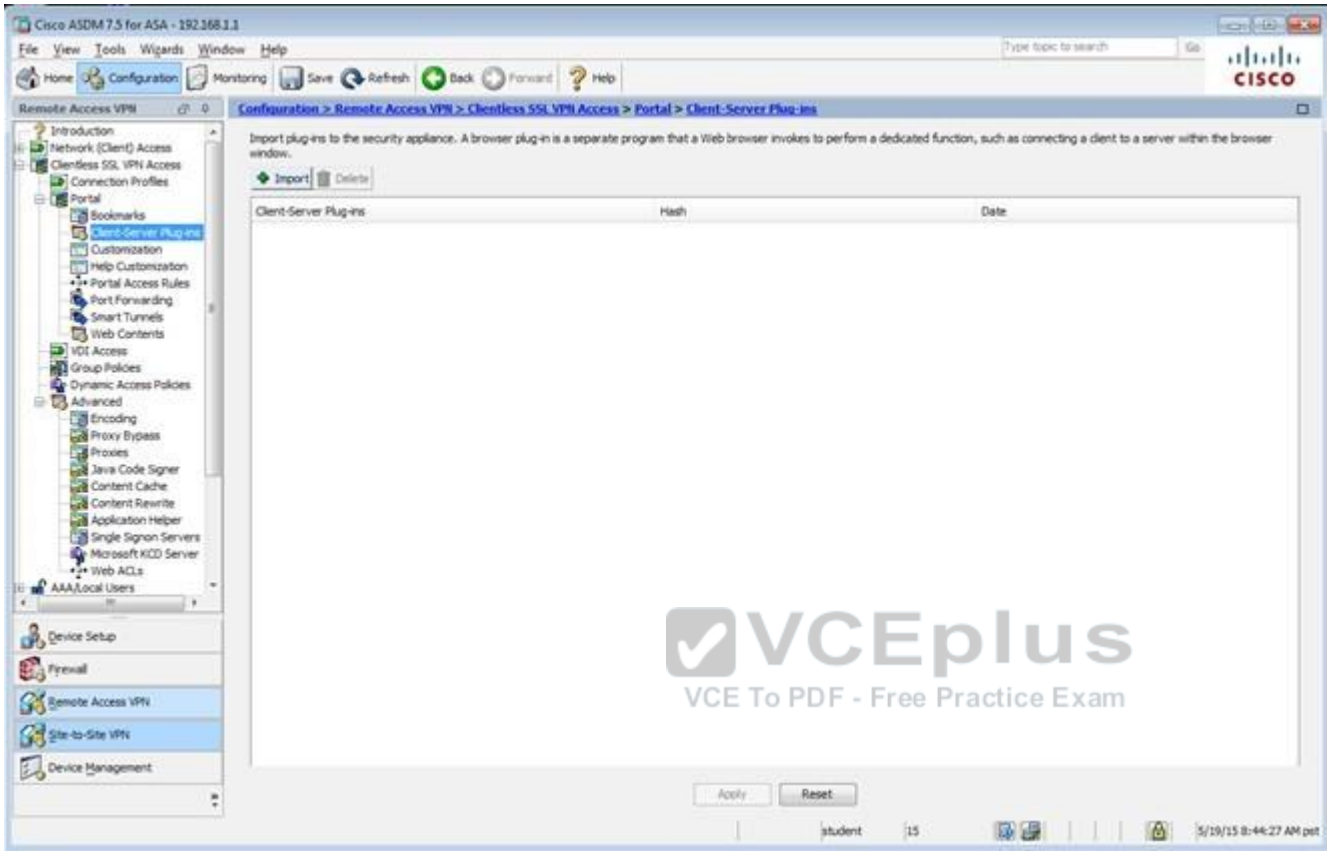


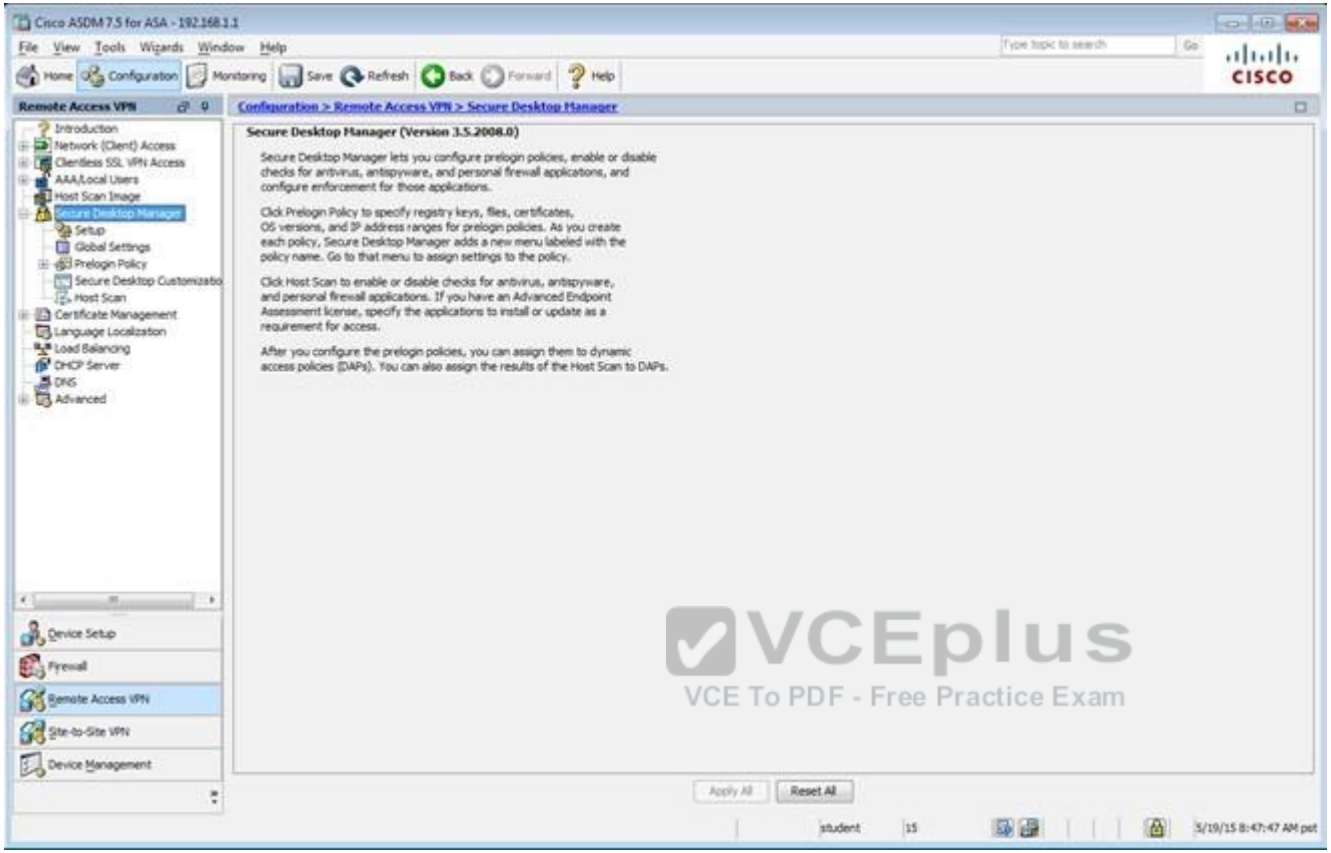


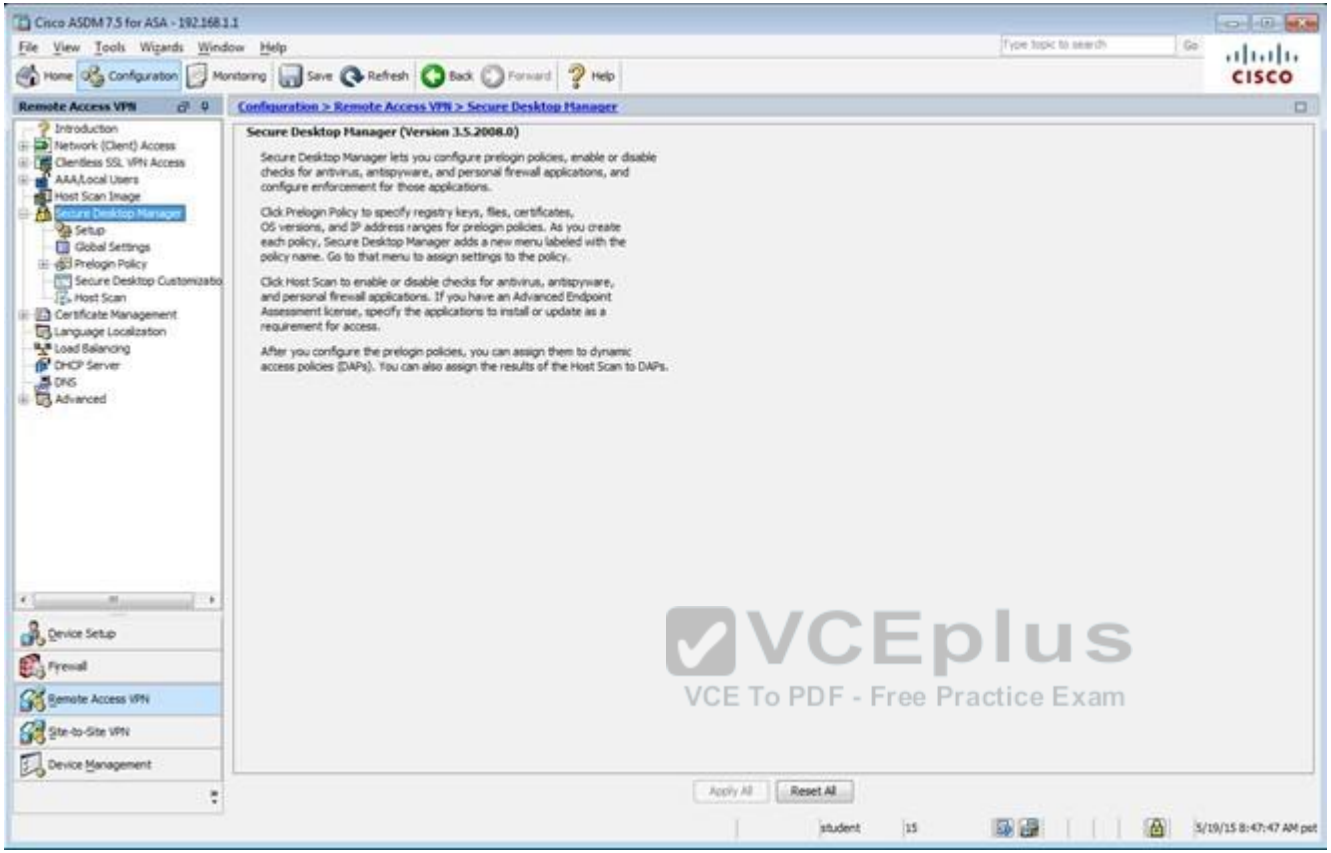


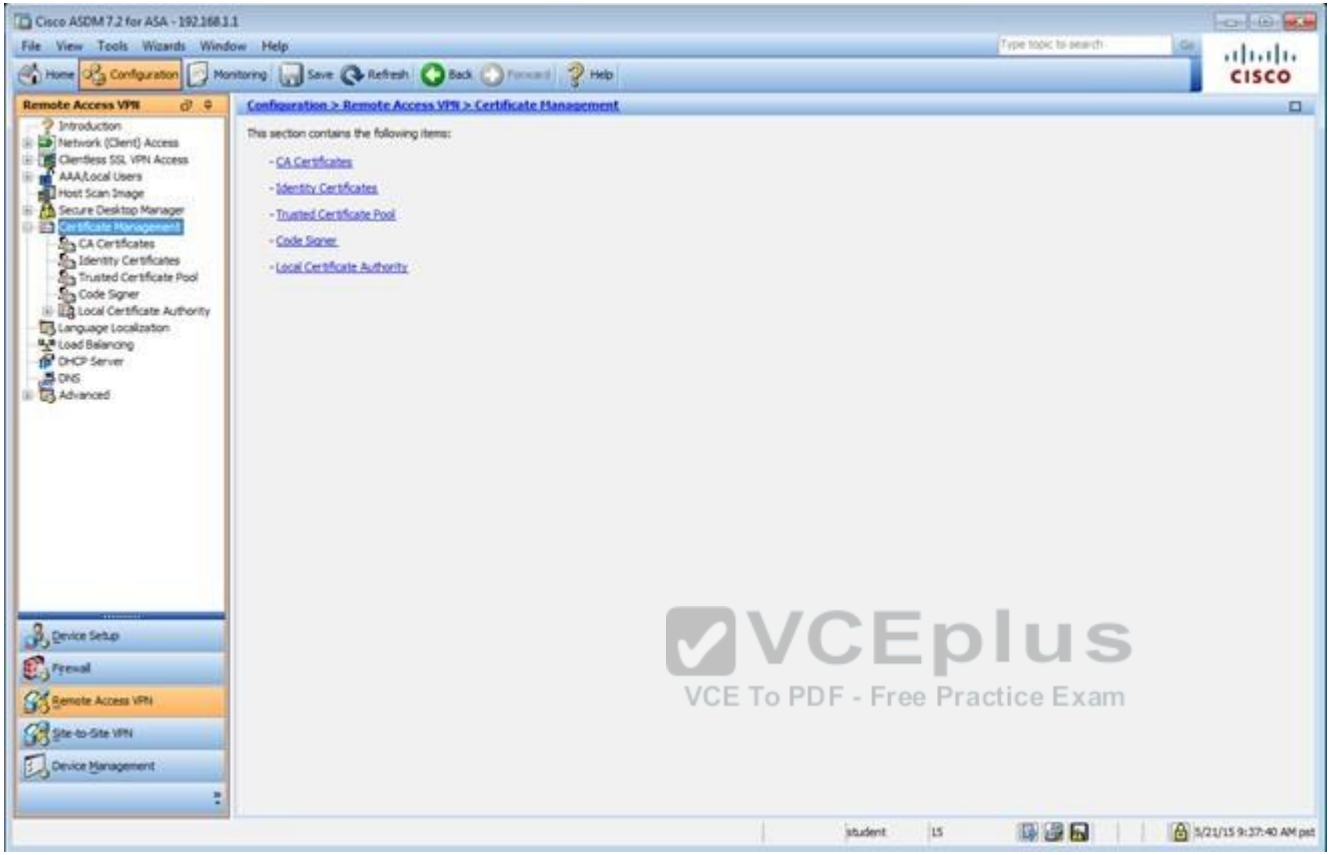


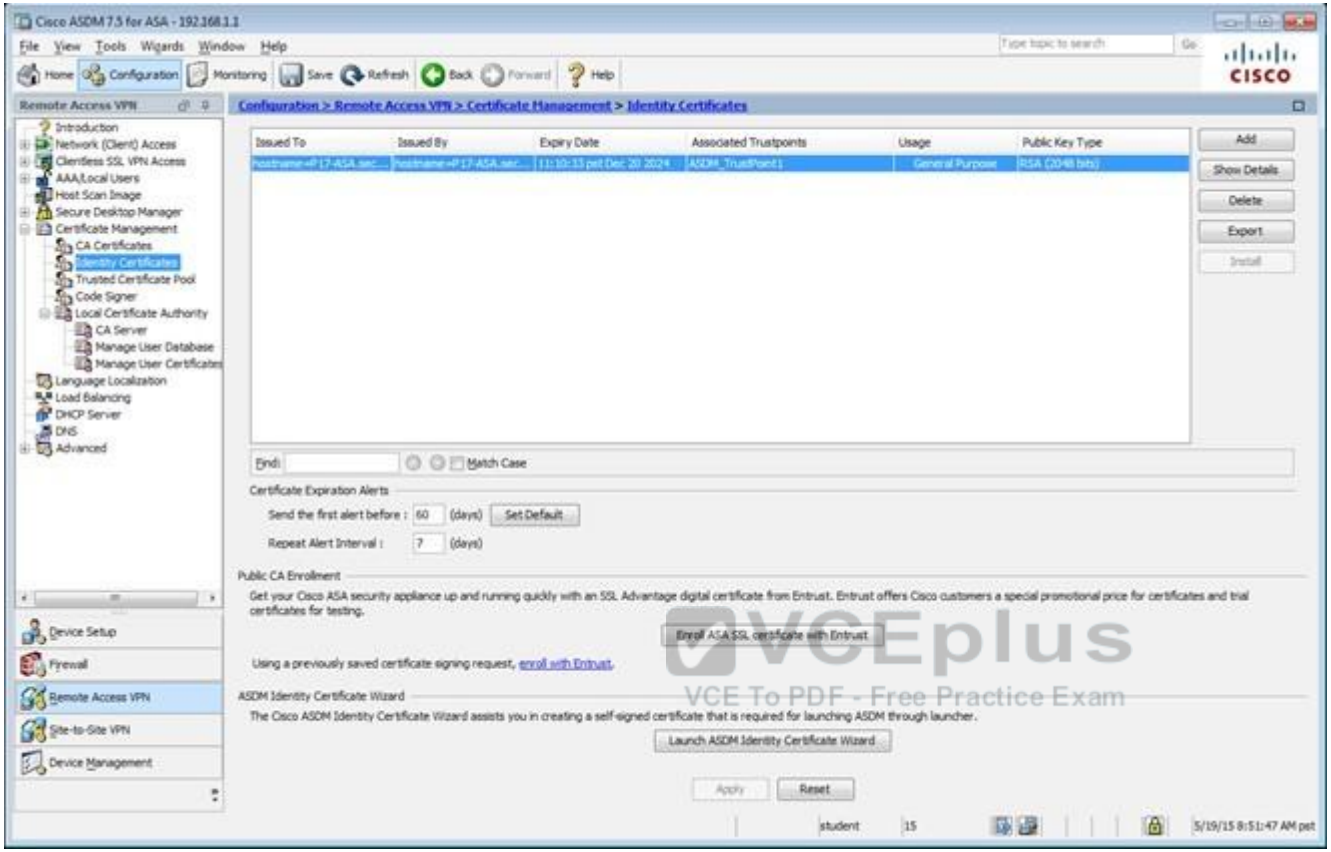


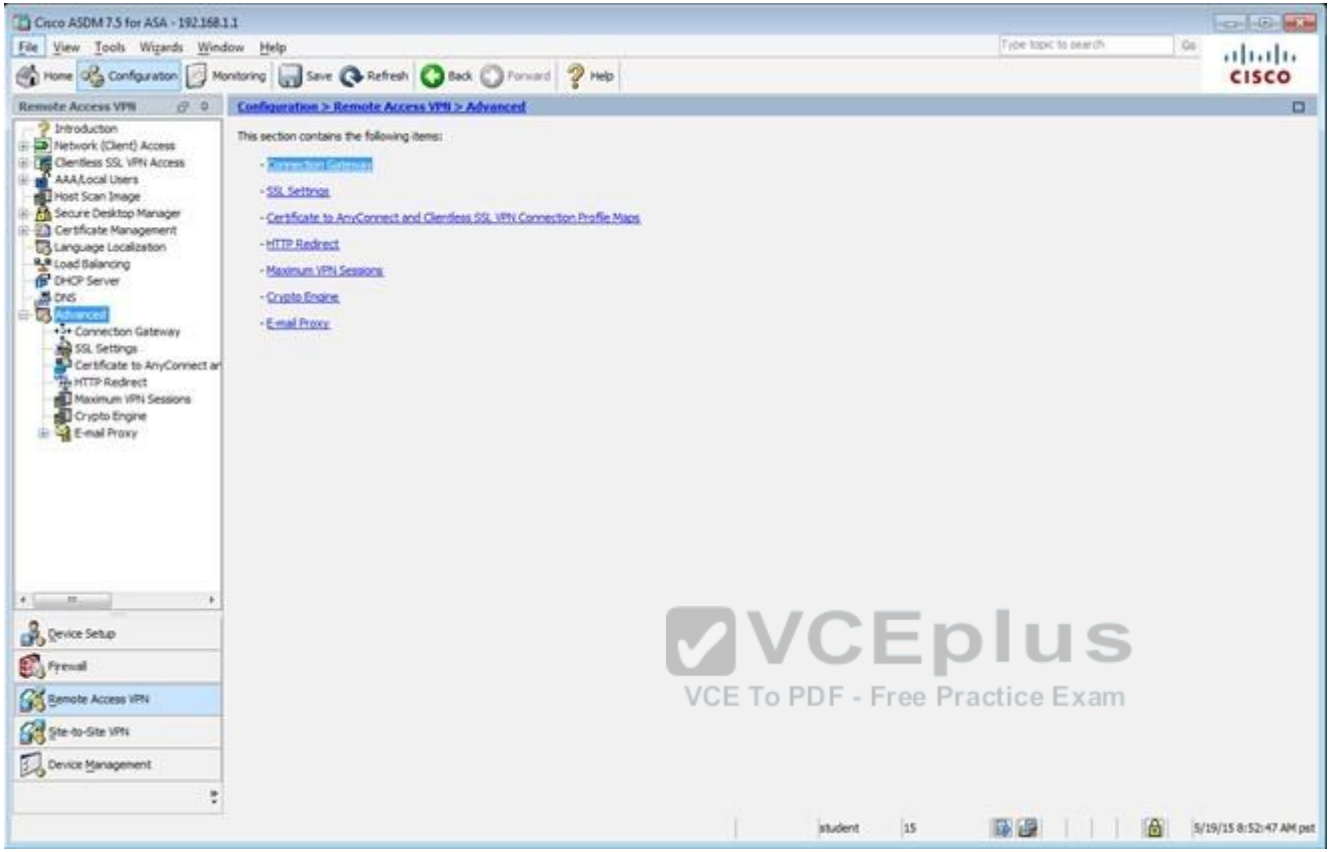


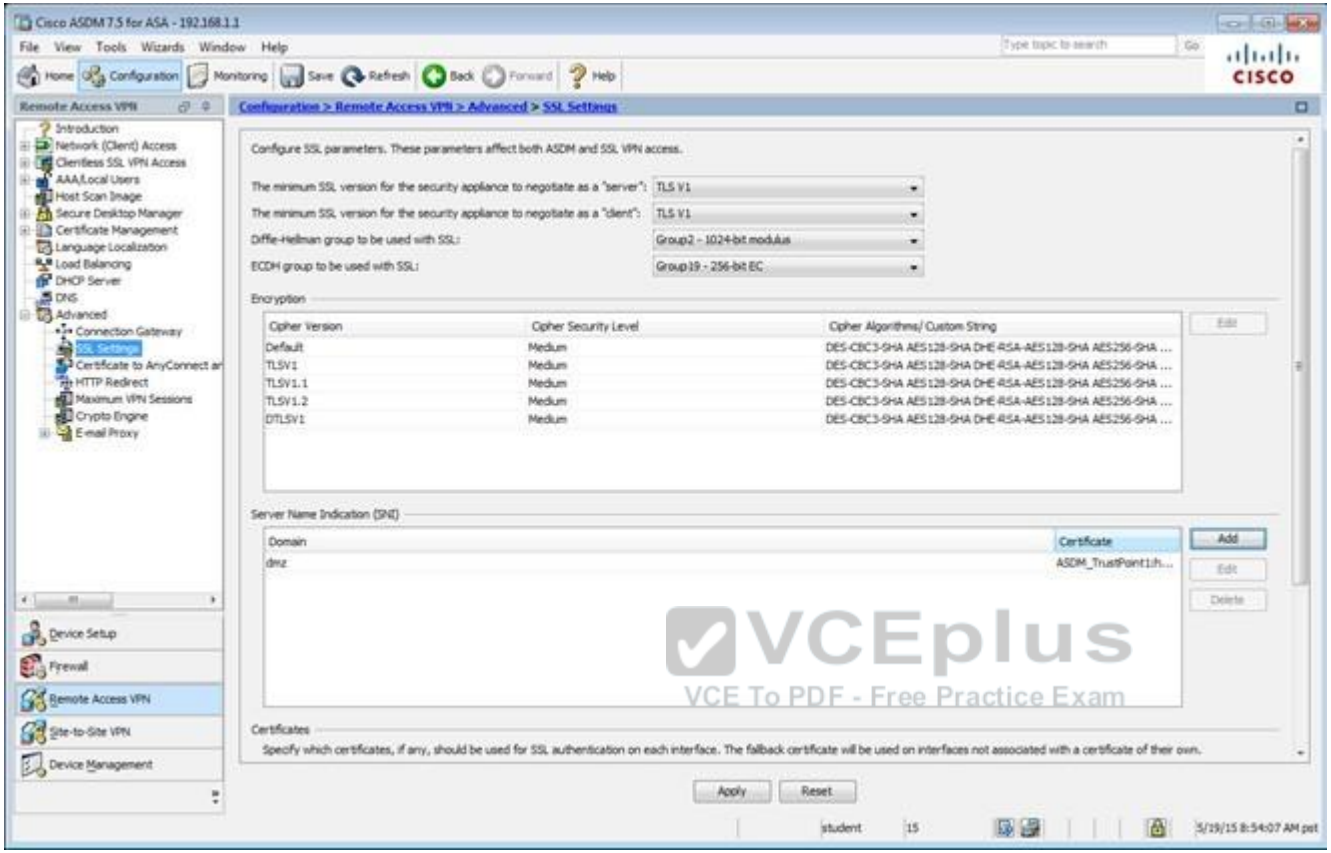


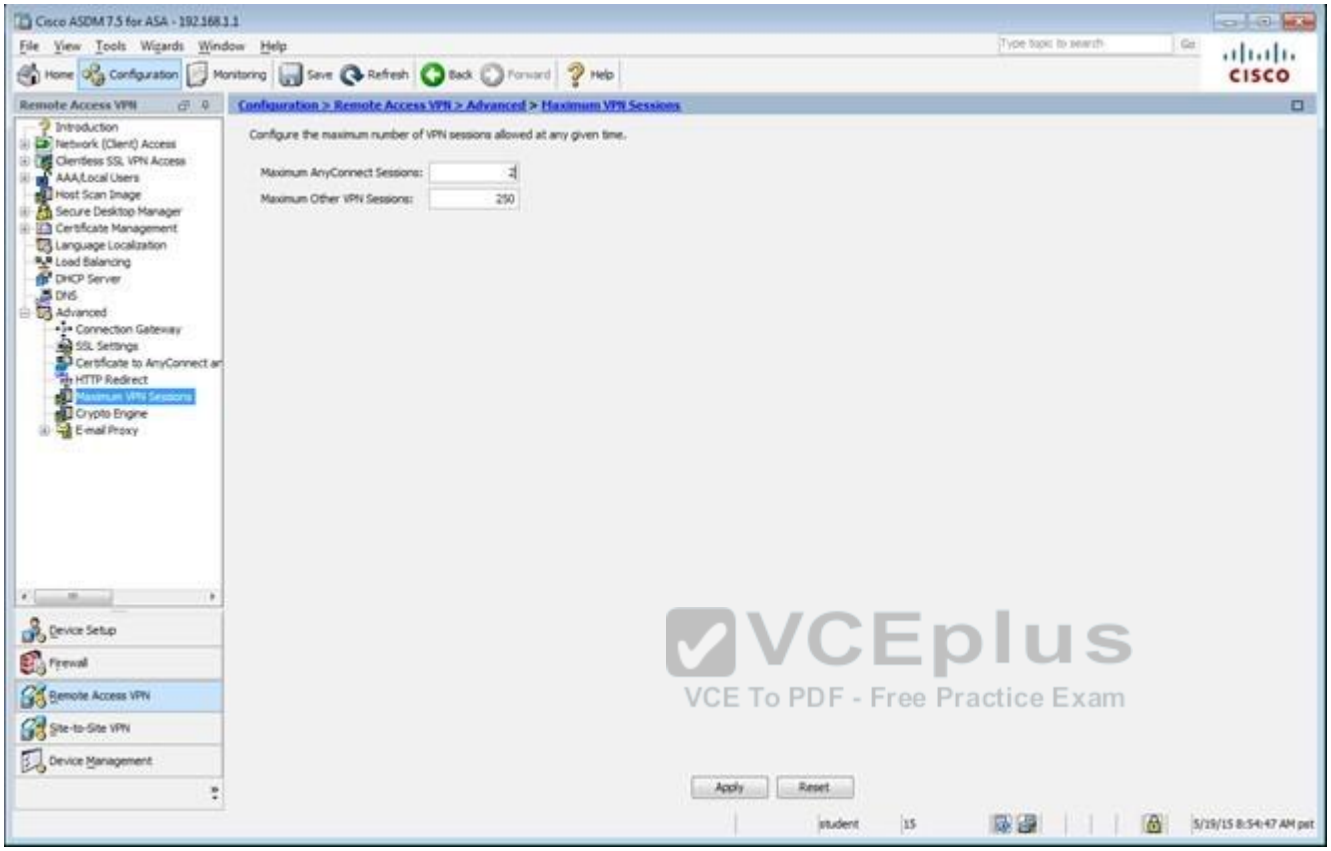


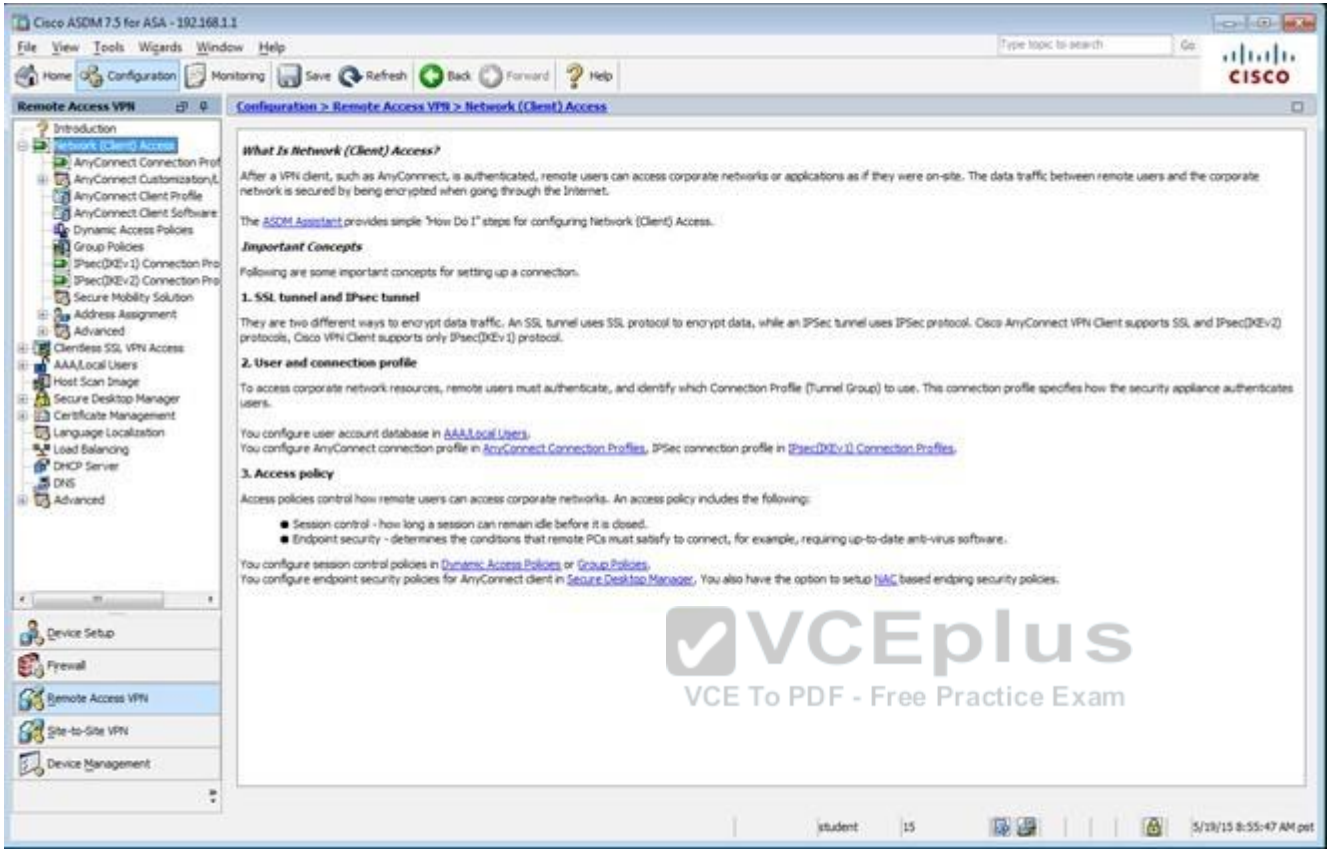


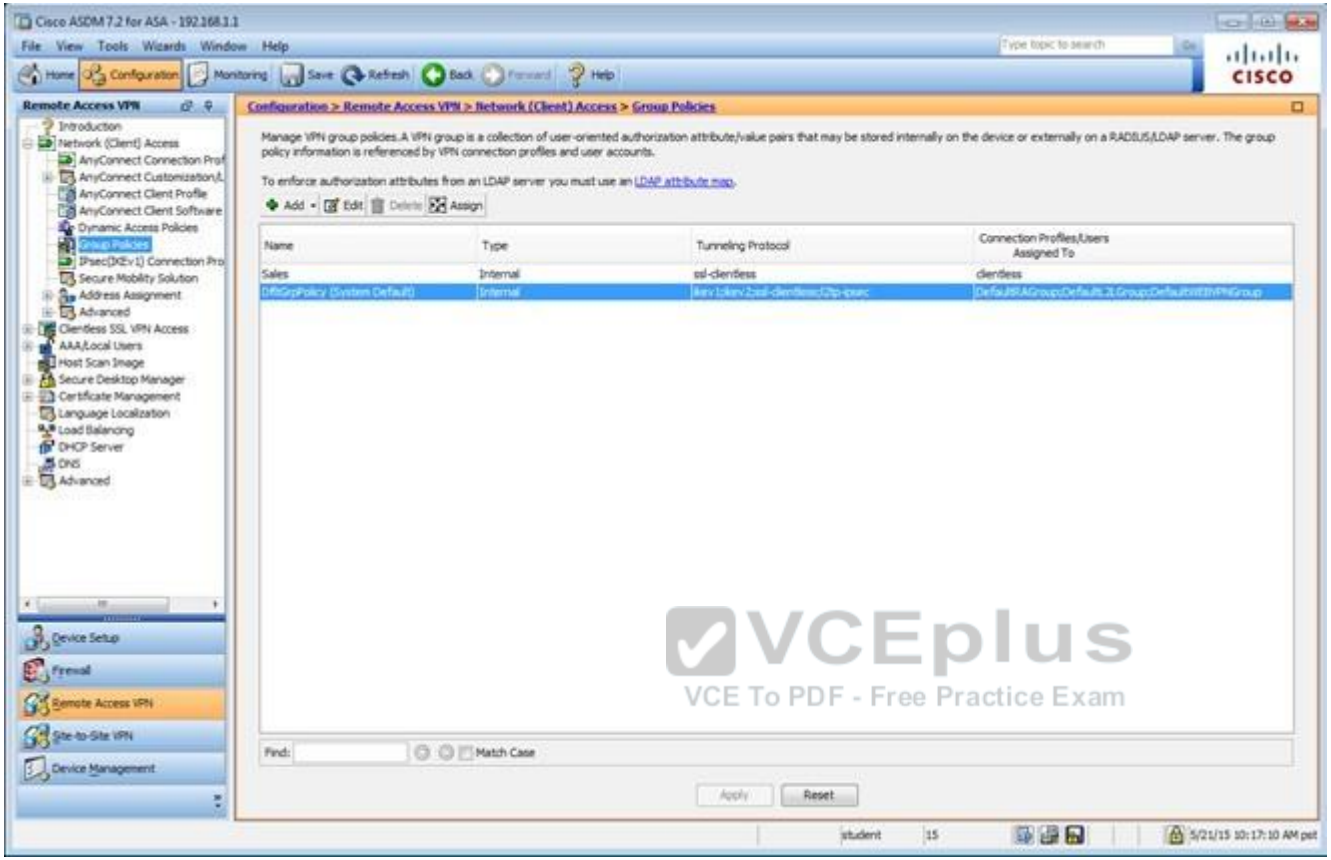


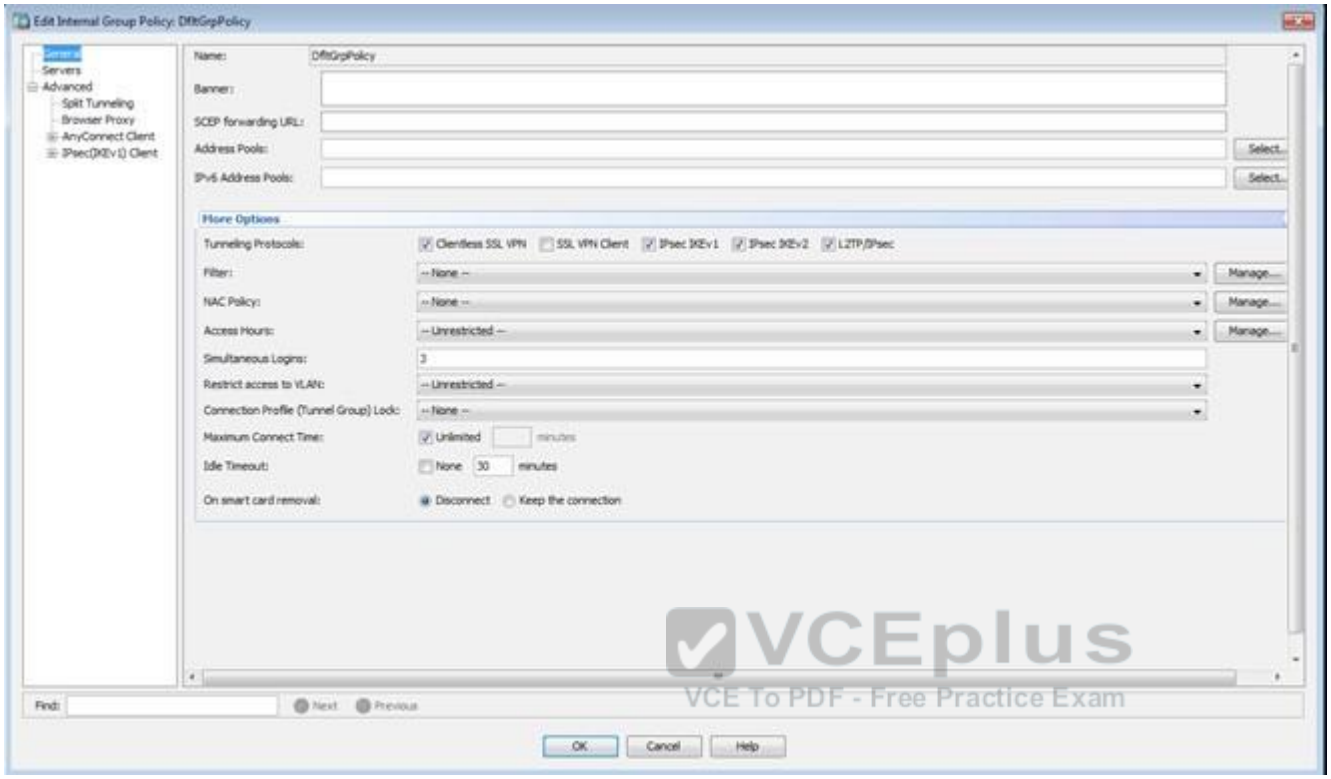


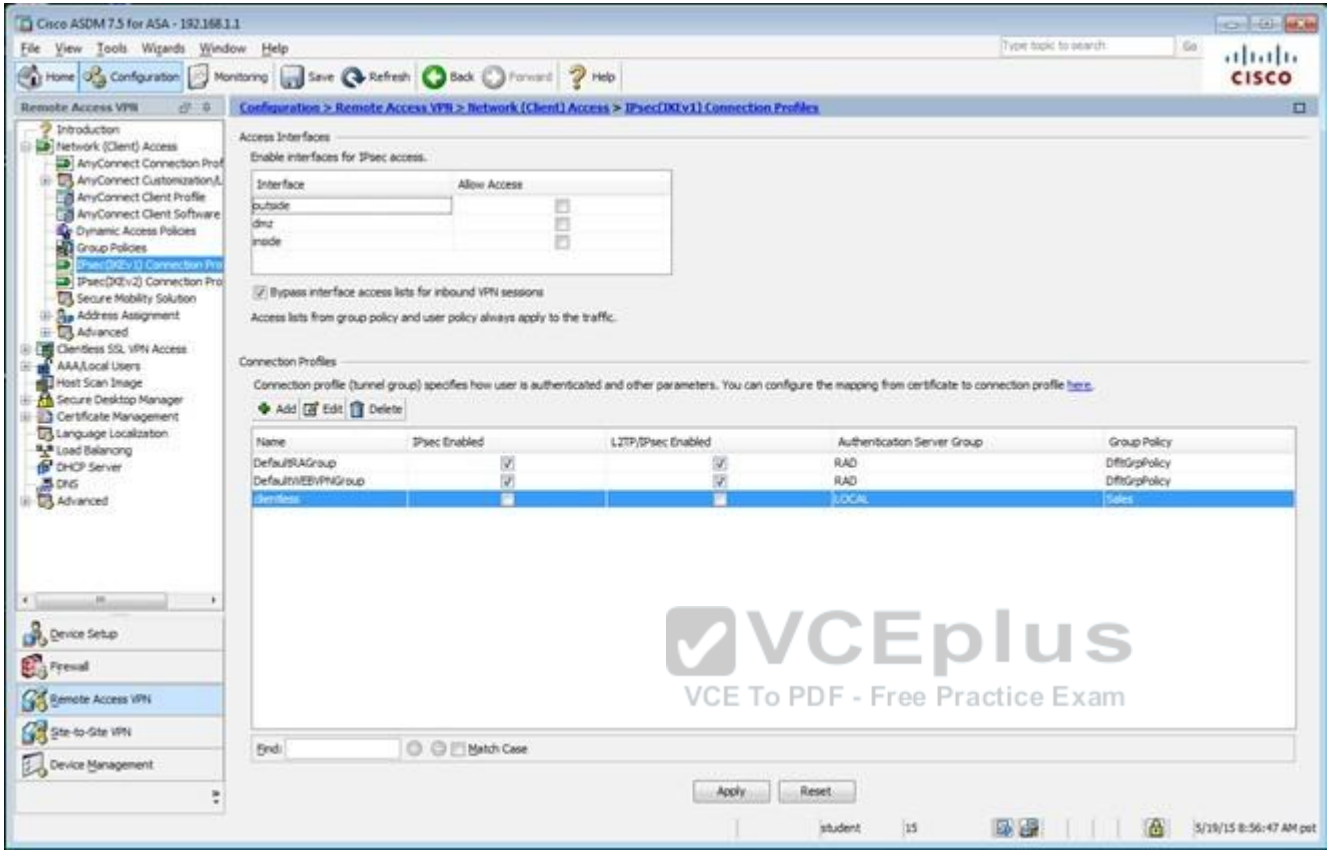


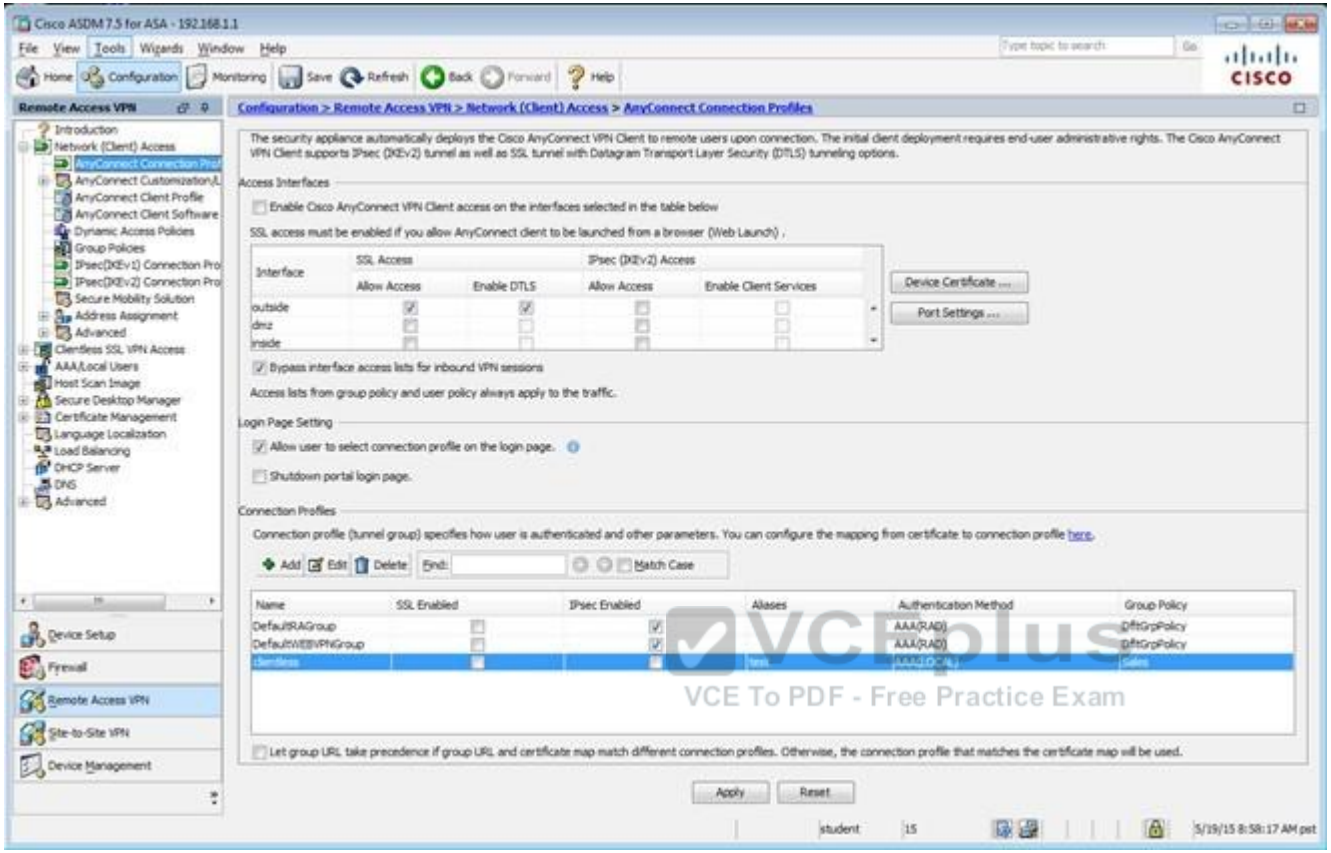


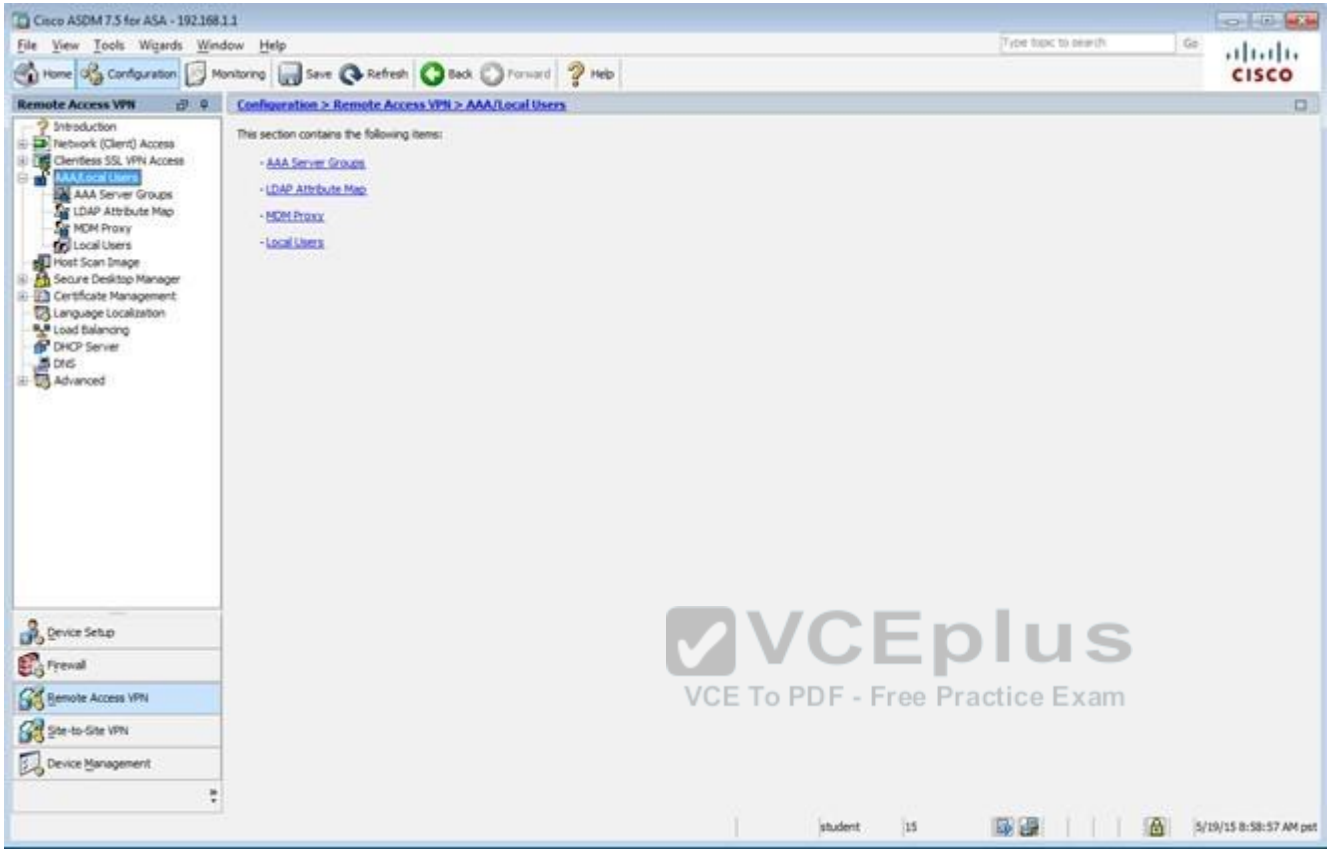


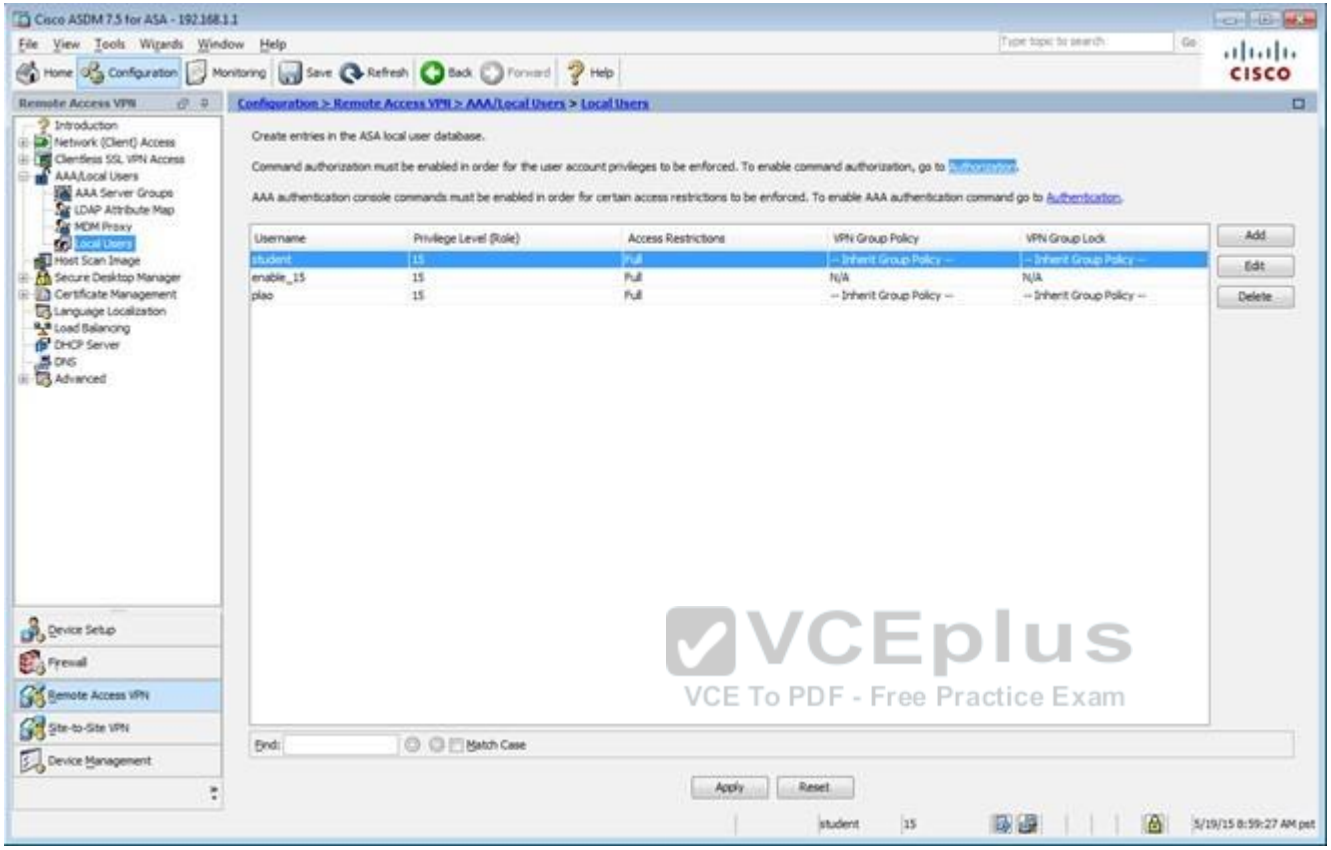


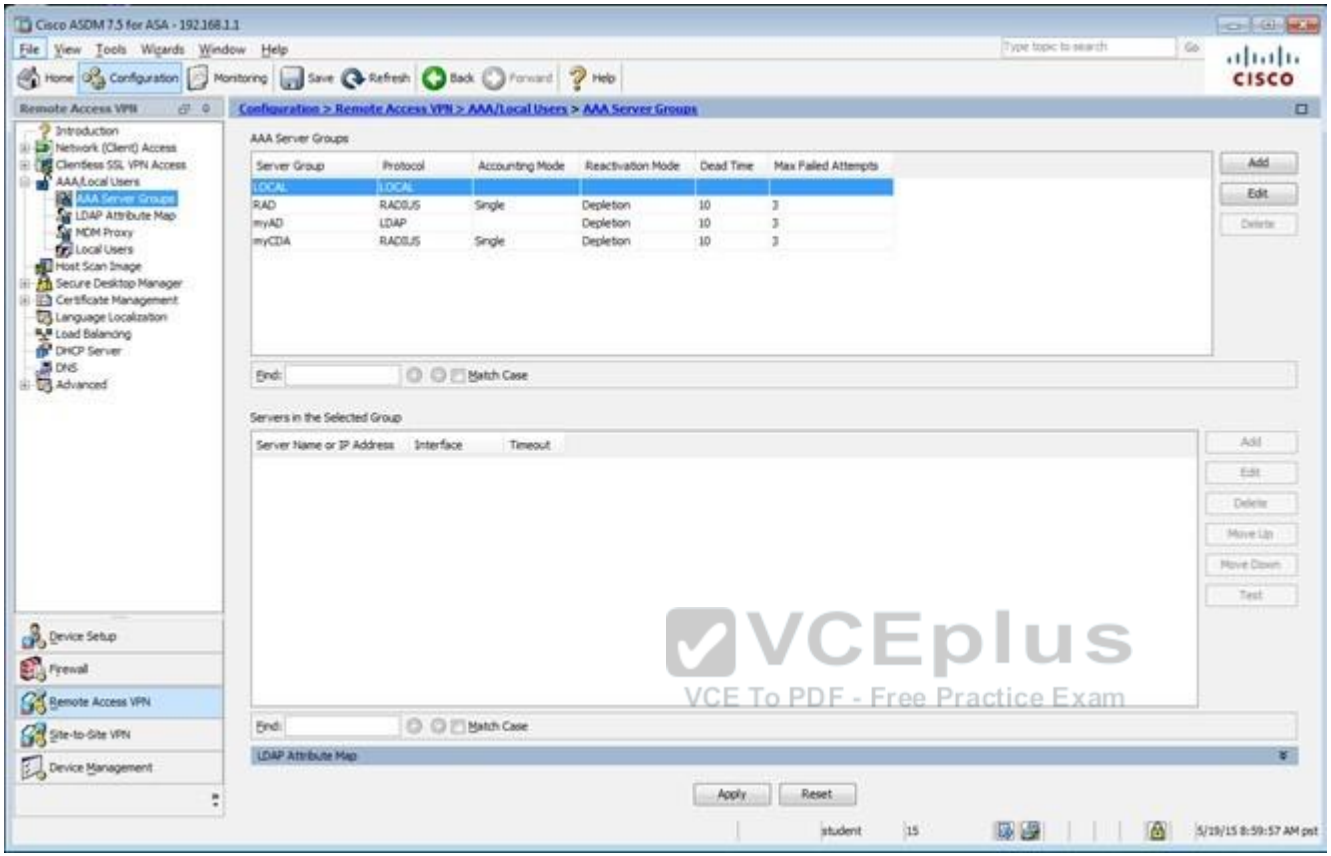










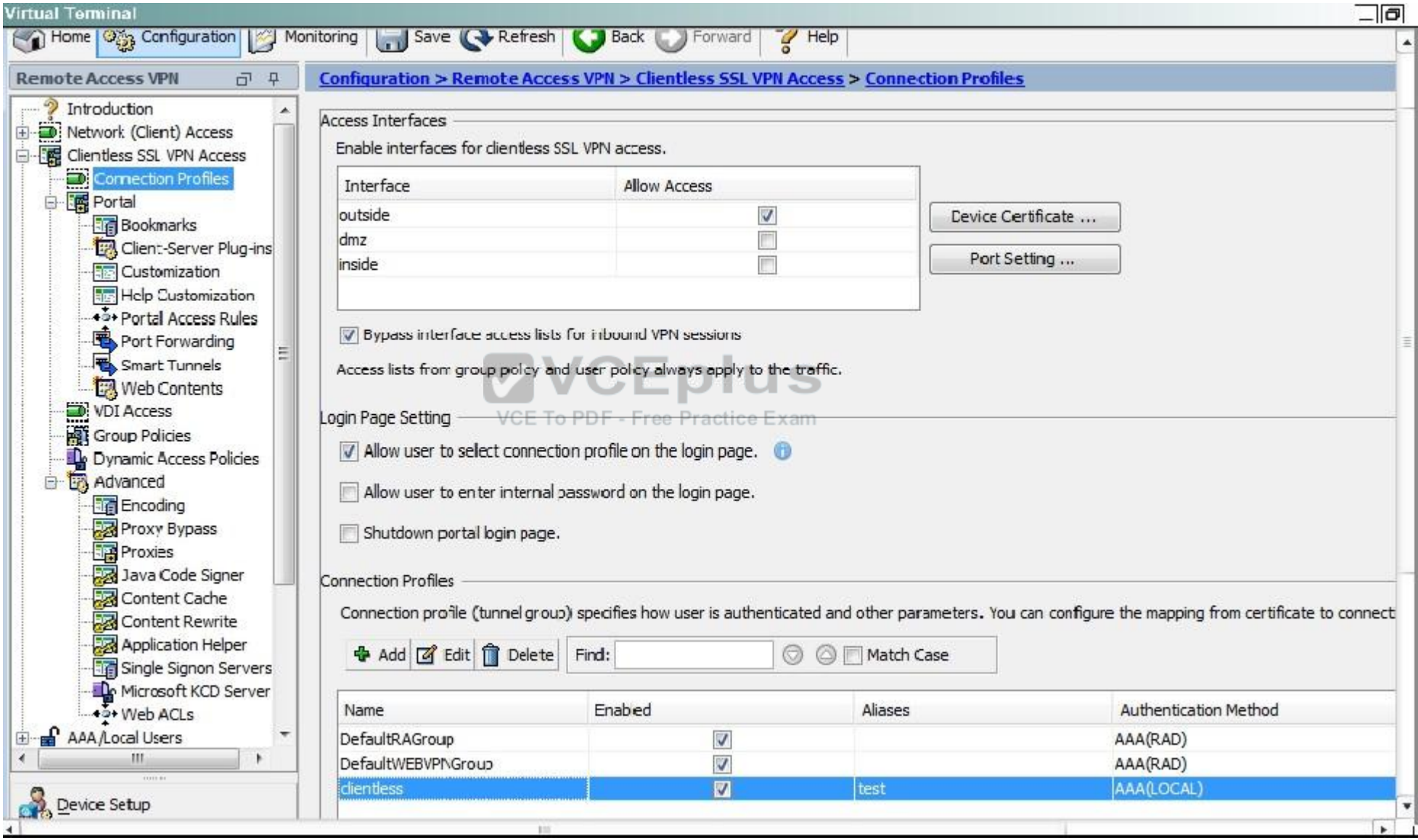


When users login to the Clientless SSLVPN using https://209.165.201.2/test, which group policy will be applied?

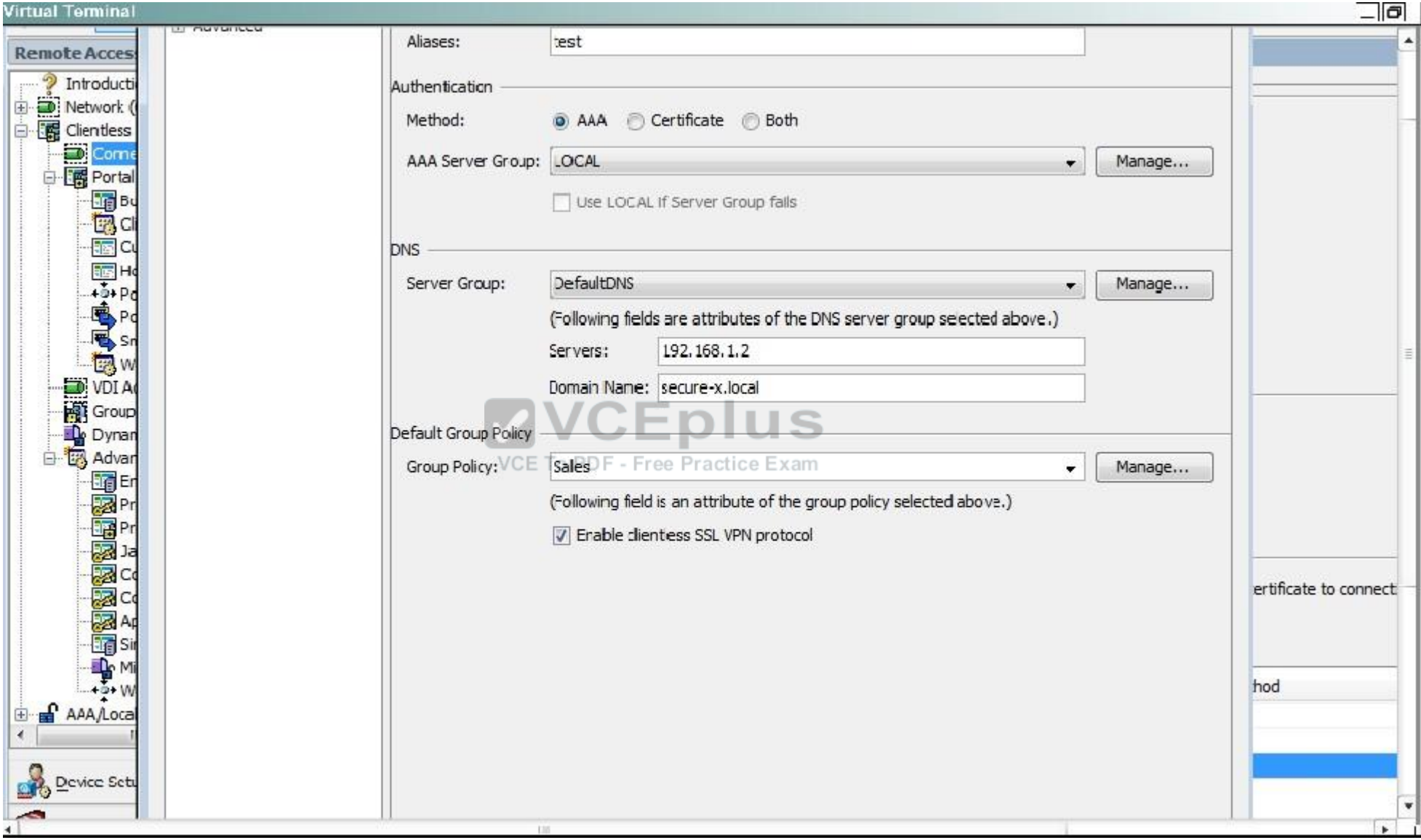
A. test
B. clientless
C. Sales
D. DfltGrpPolicy
E. DefaultRAGroup
F. DefaultWEBVPNGroup

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:



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:

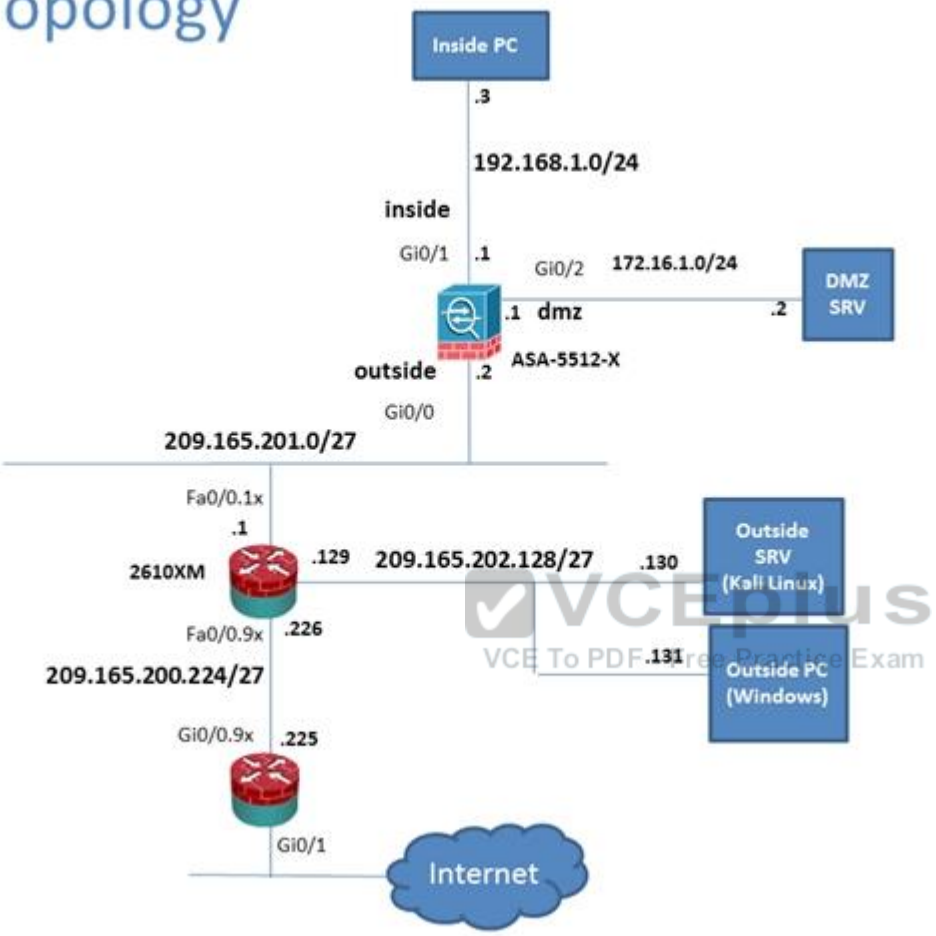
- Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use ASDM to configure the ASA to also allow any host only on the Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP 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.

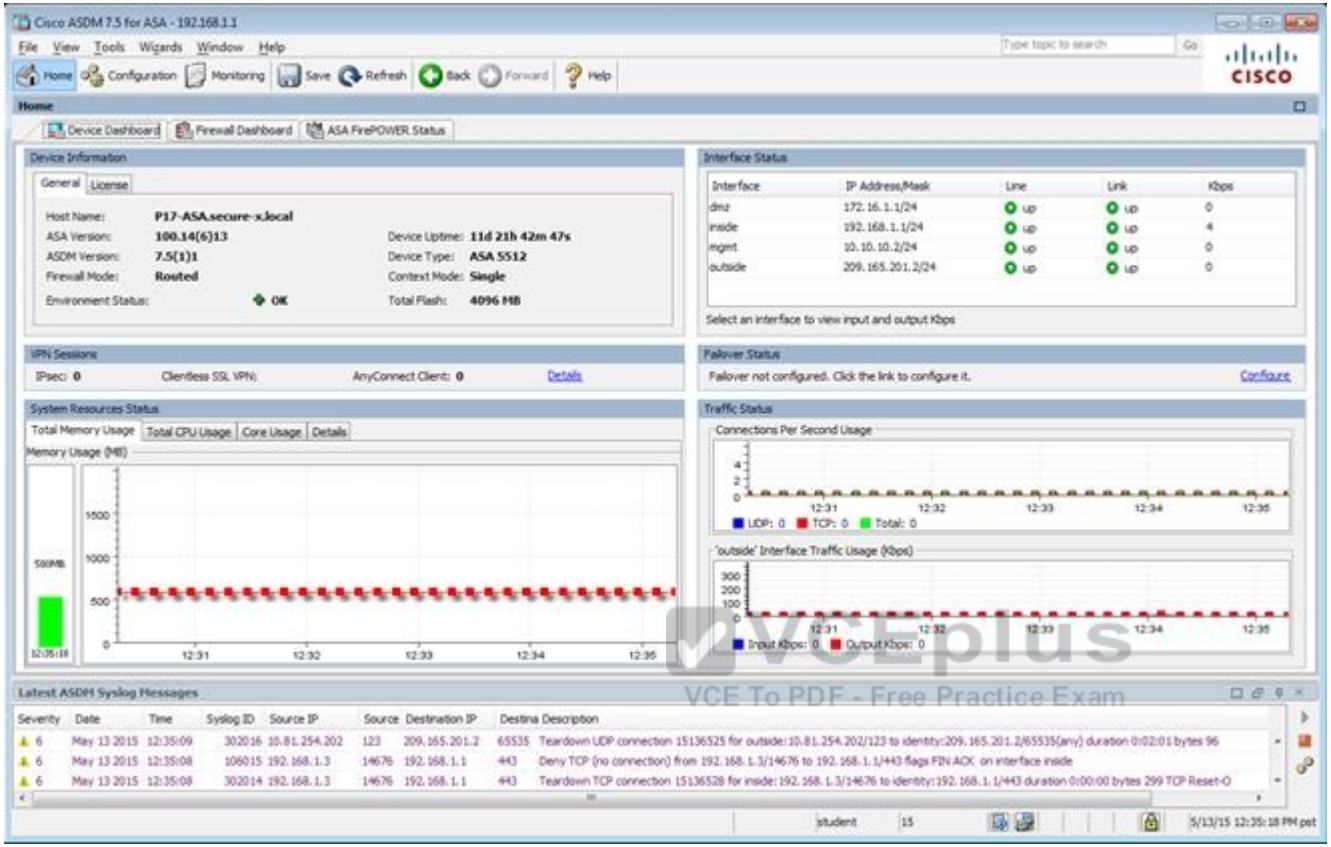
Once the correct ASA configurations have been configured:
- You can test the connectivity to http://209.165.201.30 from the Outside PC browser.
- You can test the pings to the Outside (www.cisco.com) by opening the inside PC command prompt window. In this simulation, only testing pings to www.cisco.com will work.

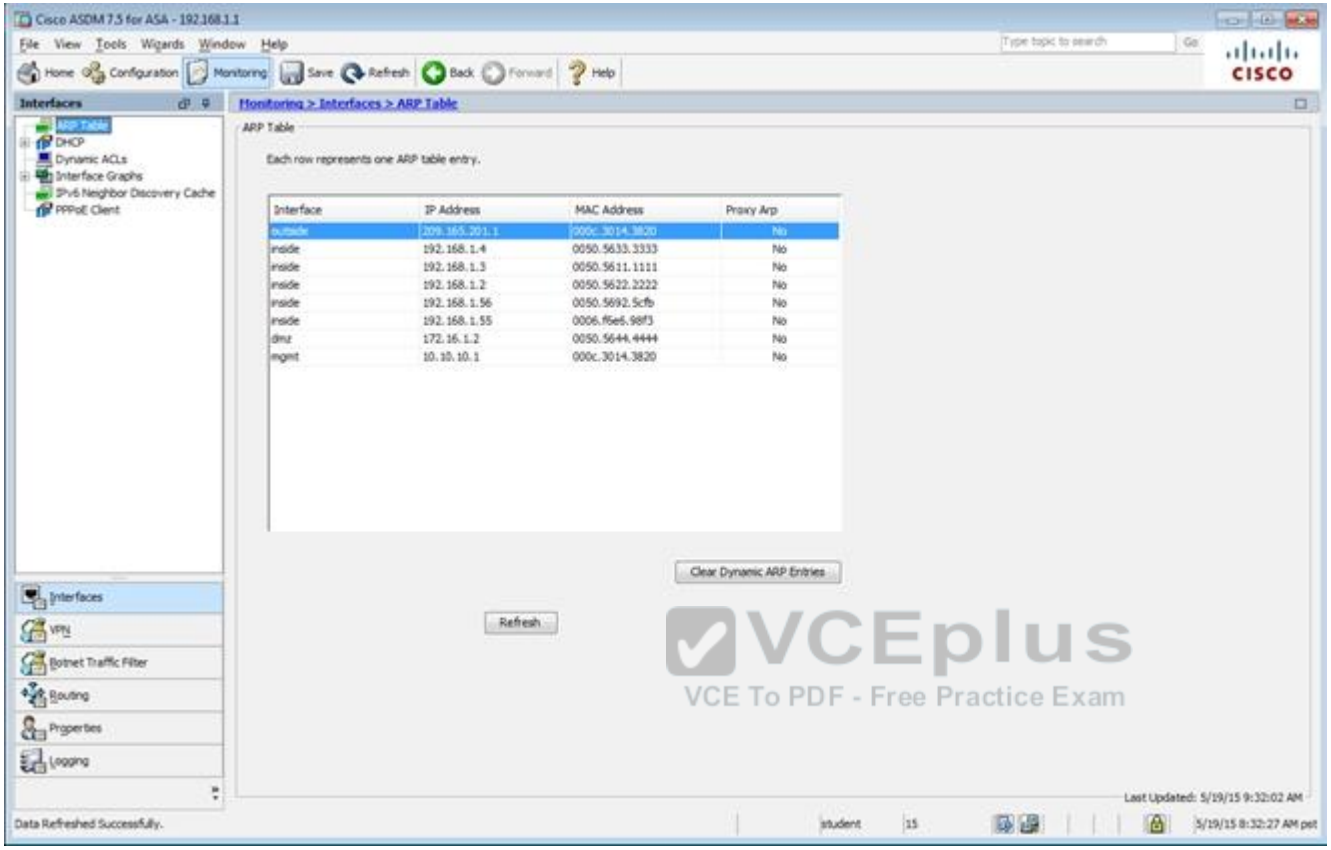
To access ASDM, click the ASA icon in the topology diagram.
To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.
To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.

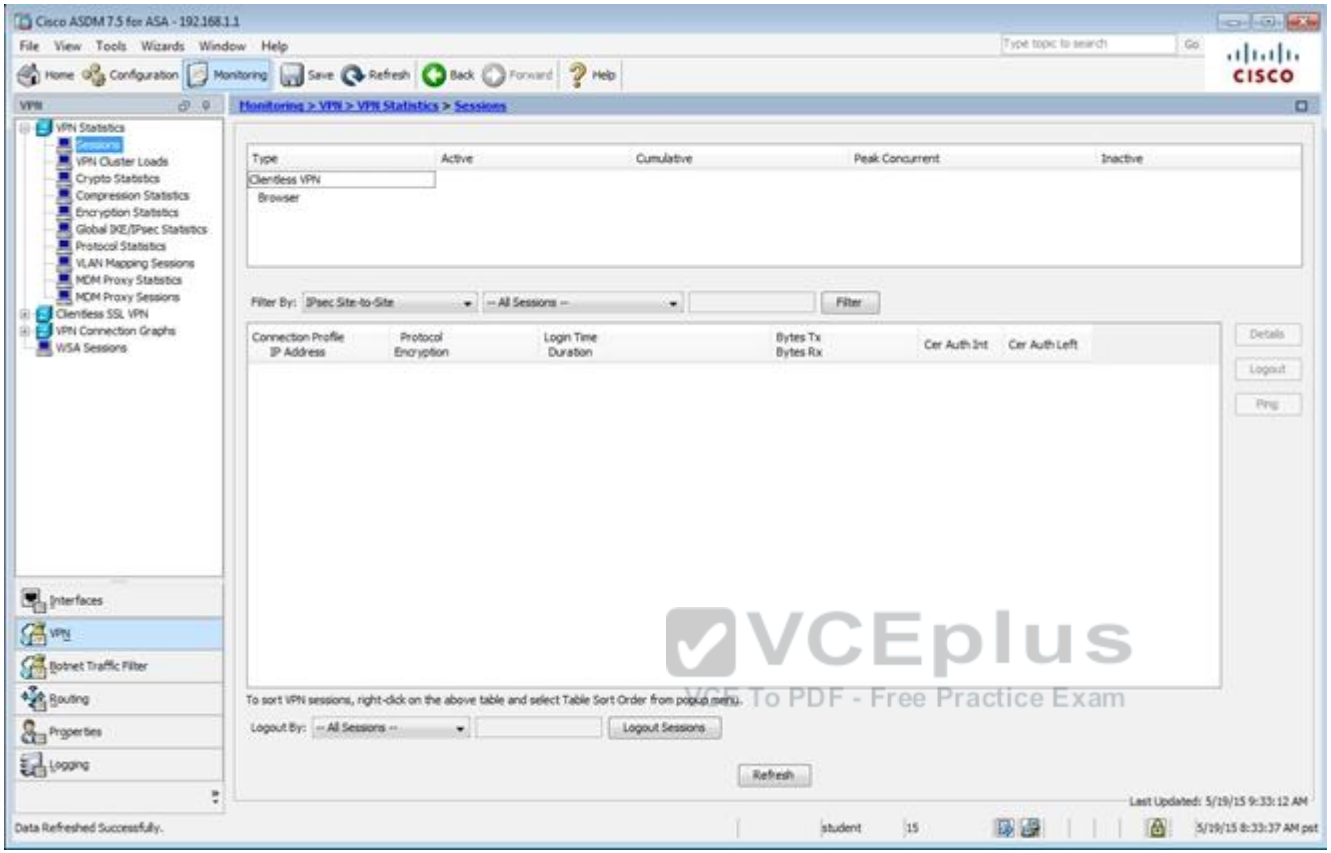
Note:
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.
In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

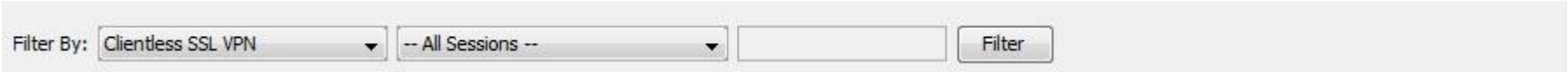
Lab Topology

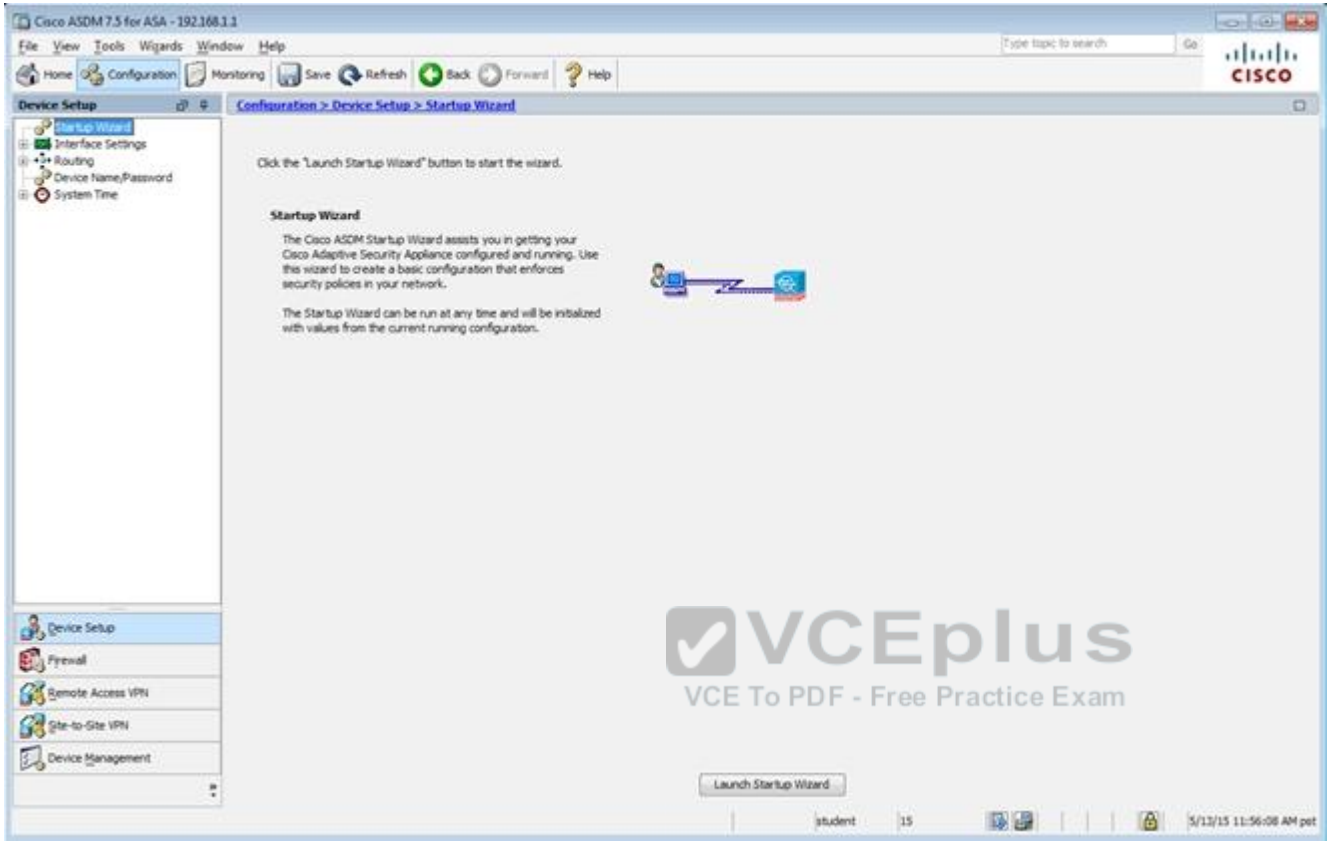


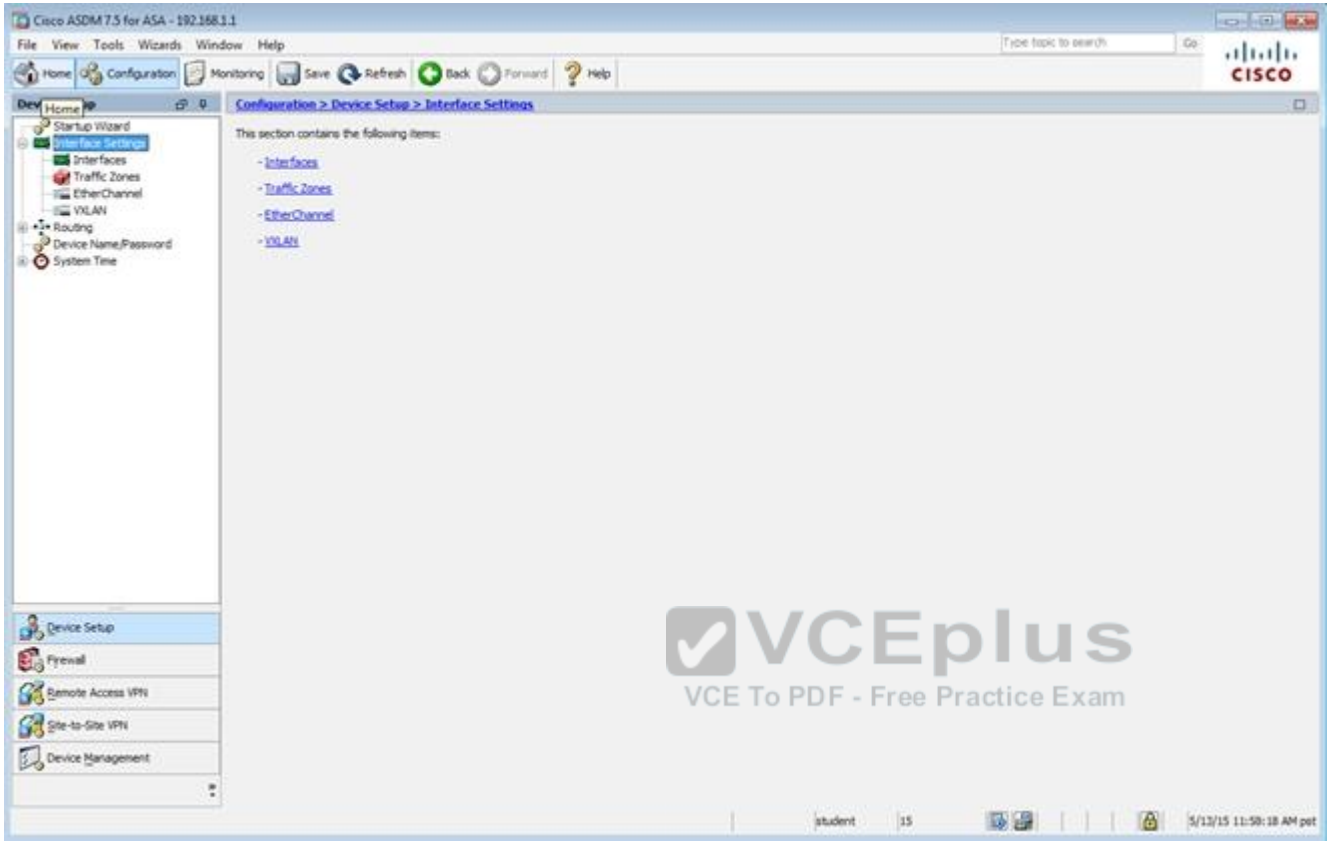


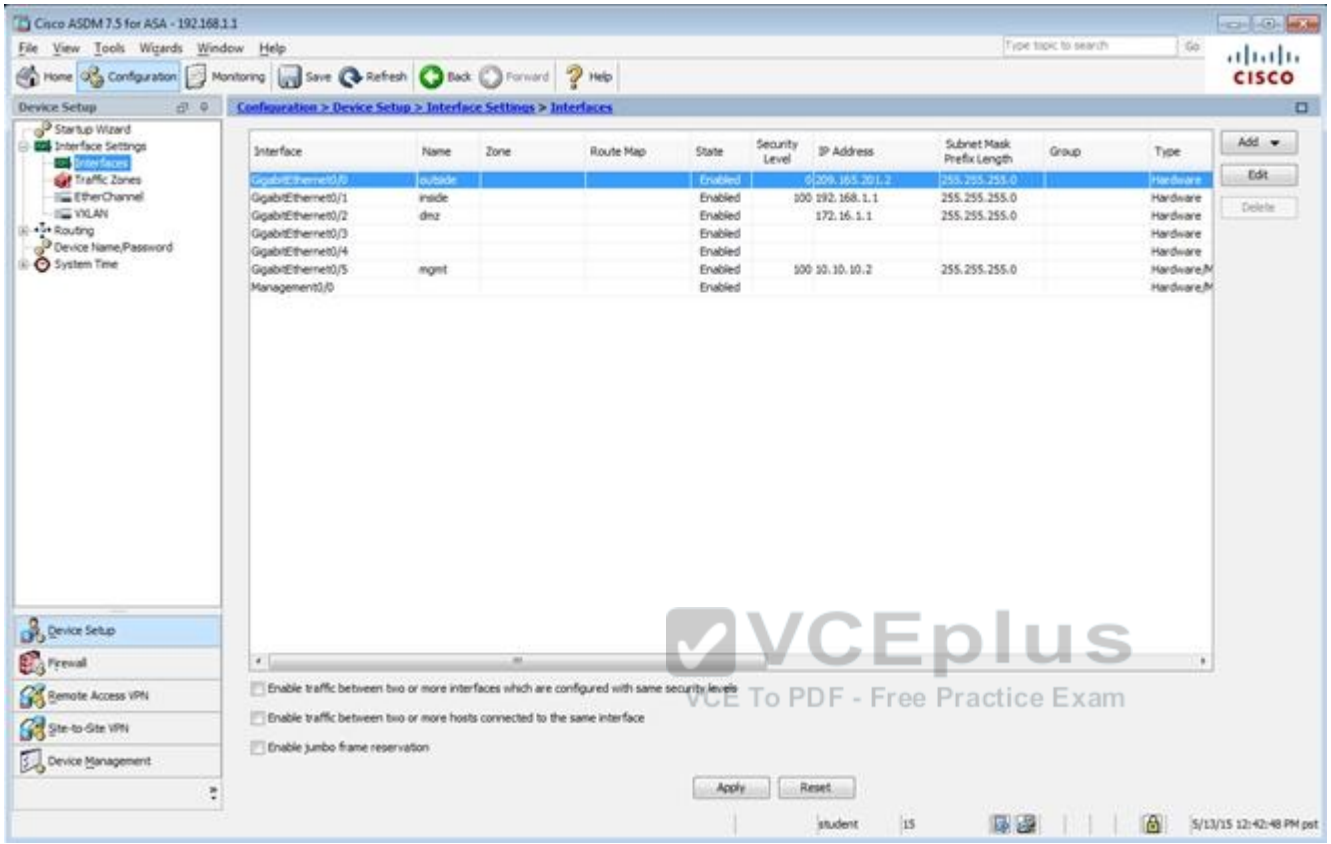


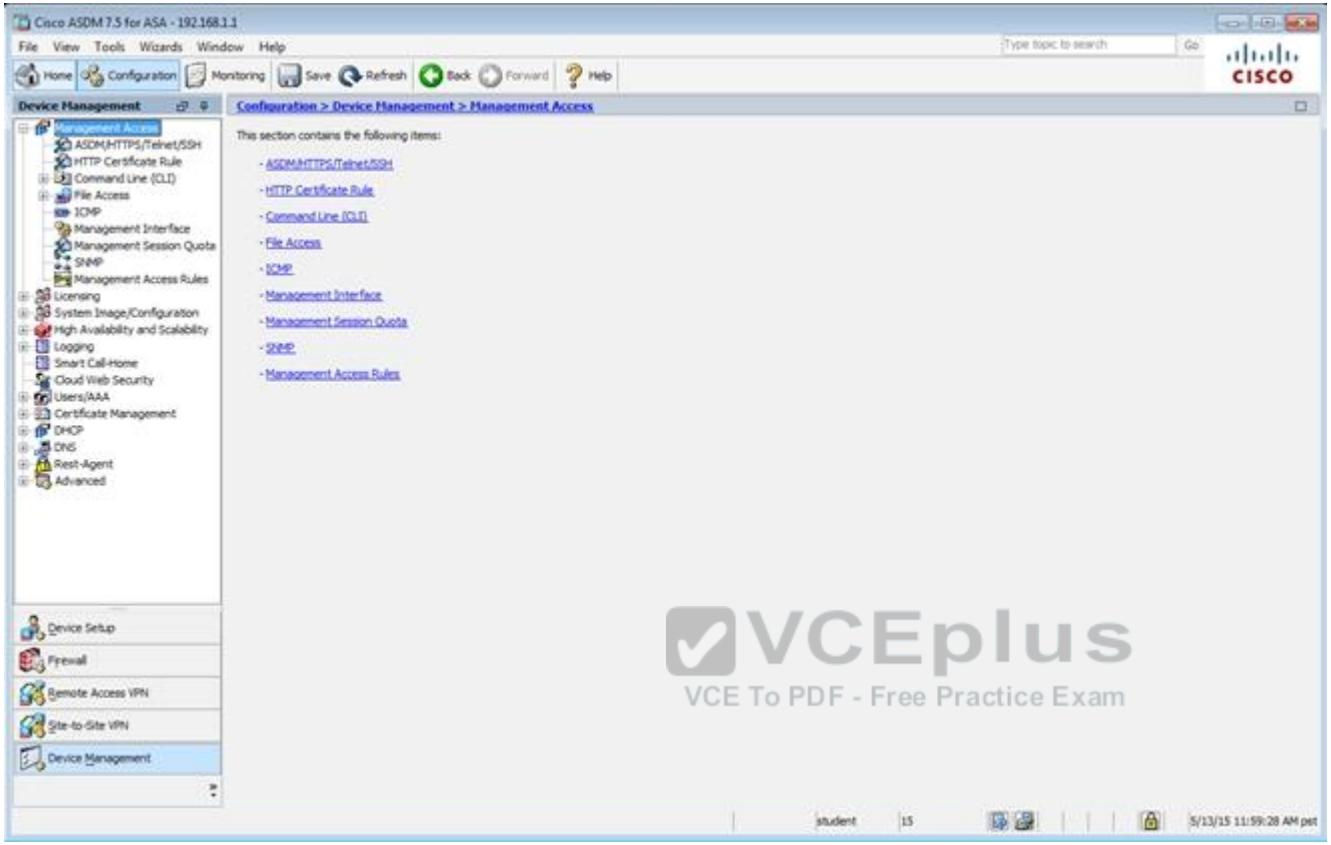


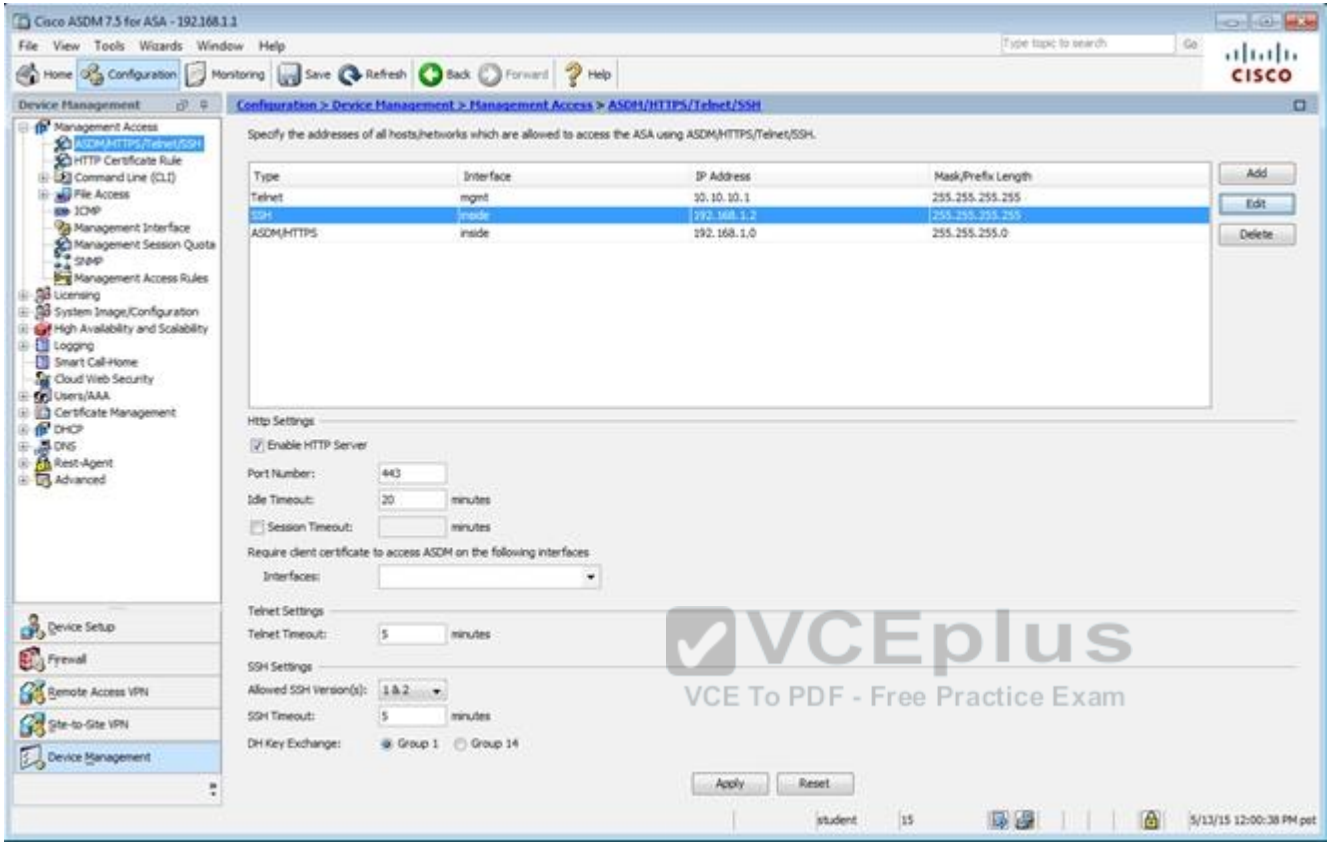


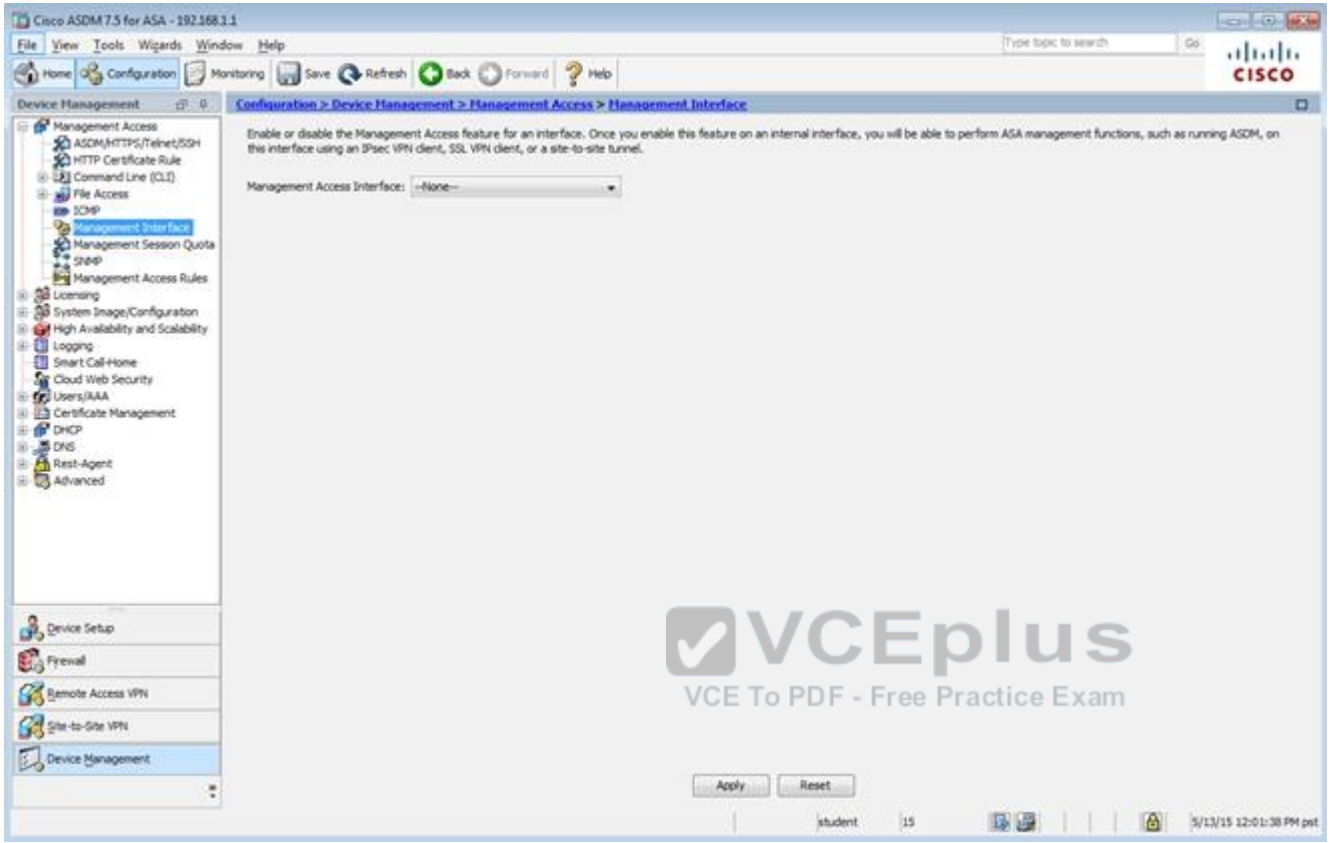


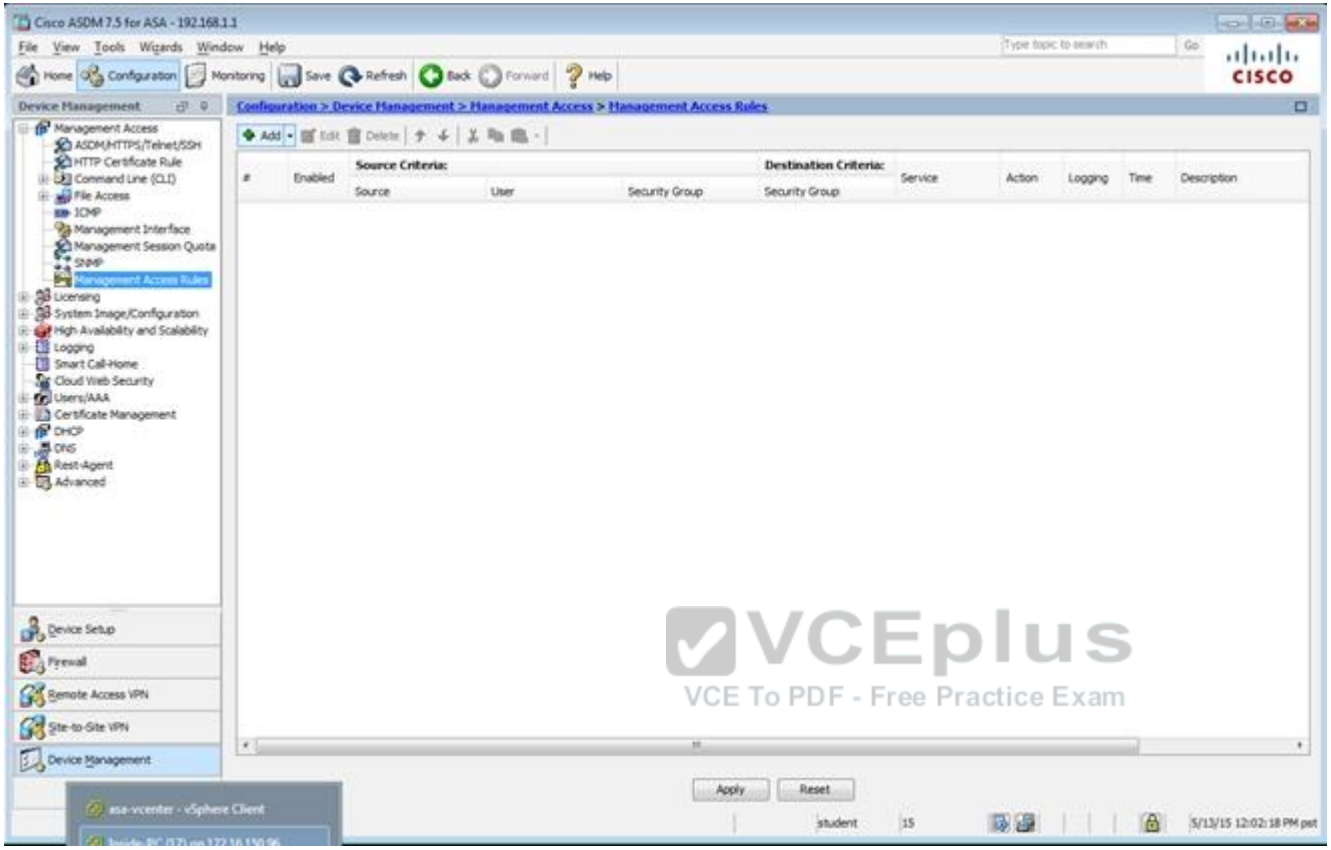


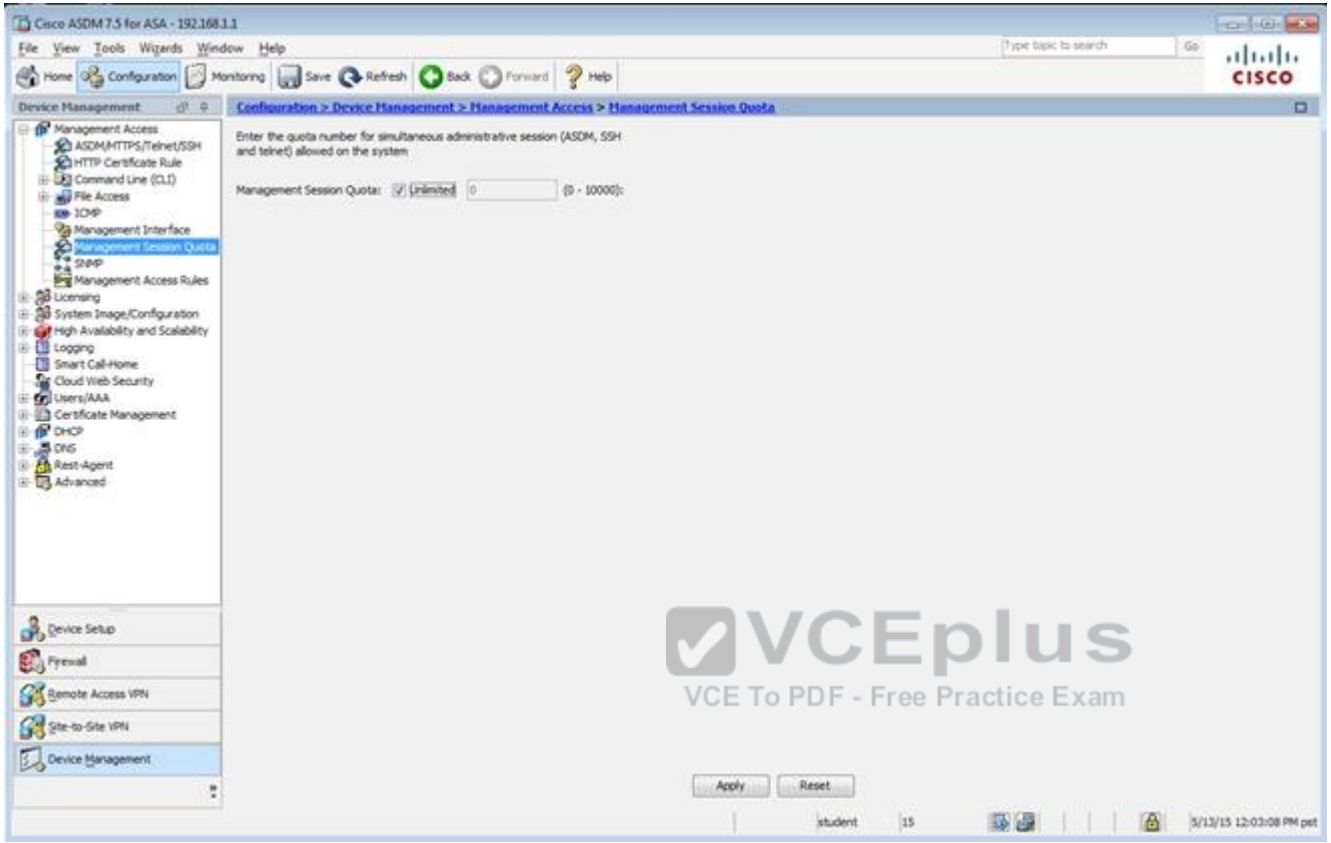


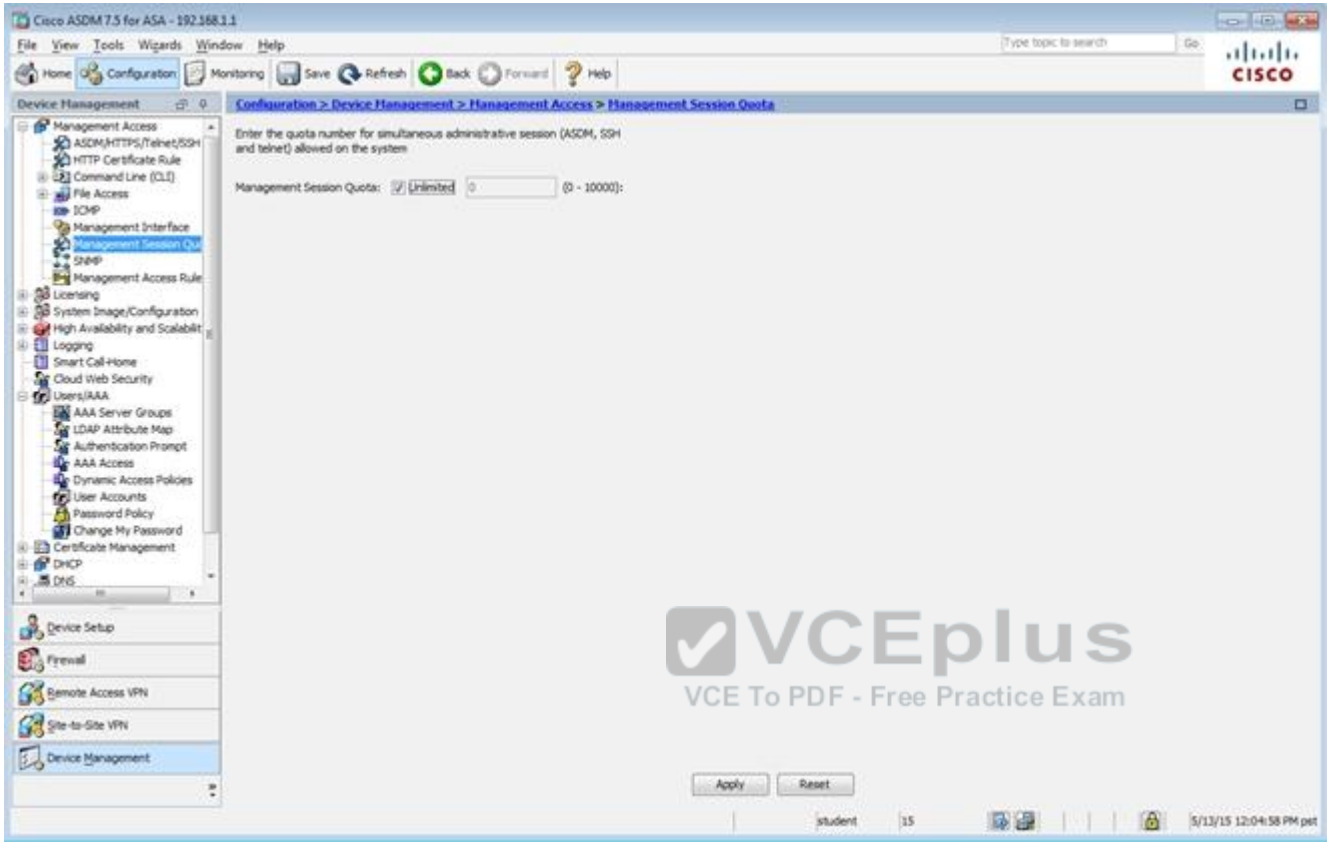


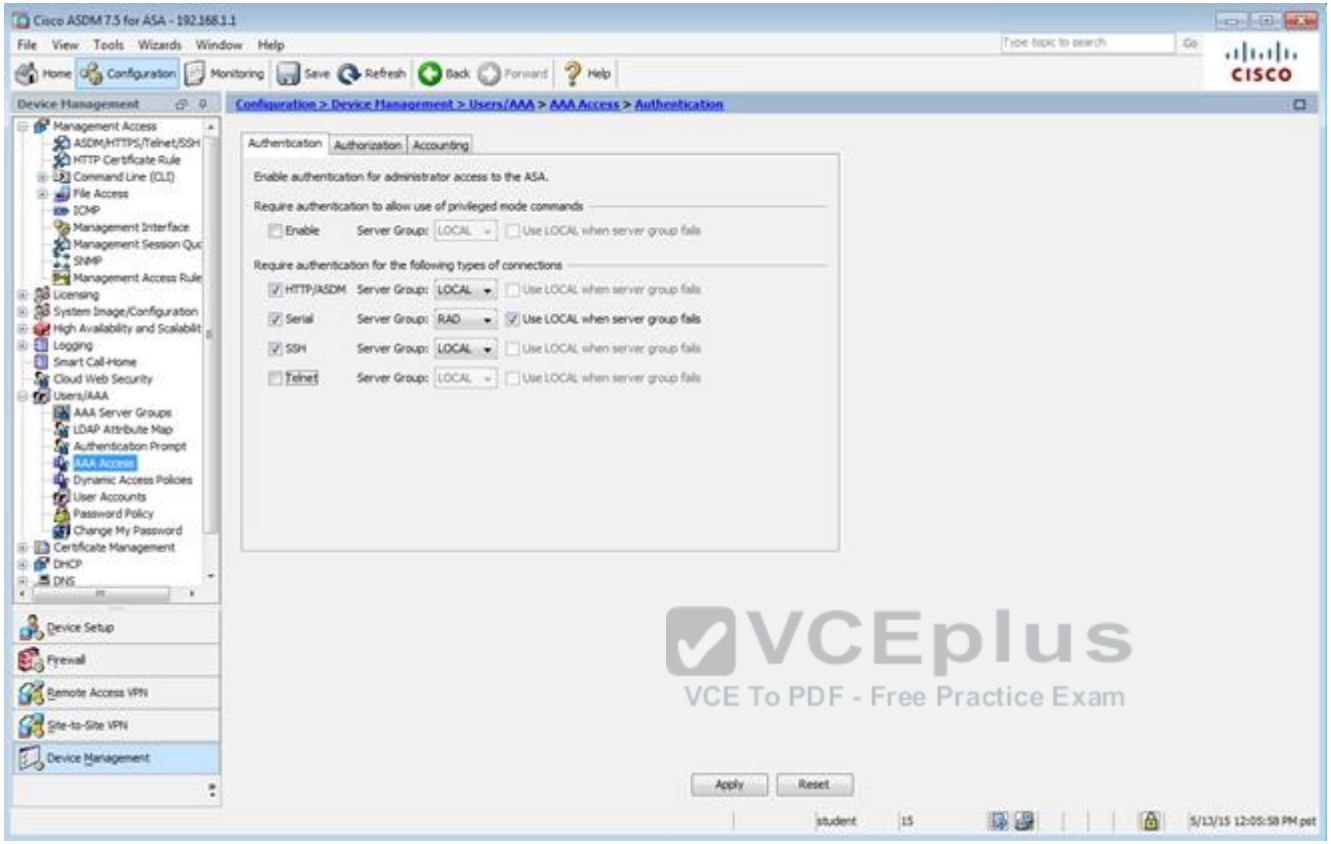


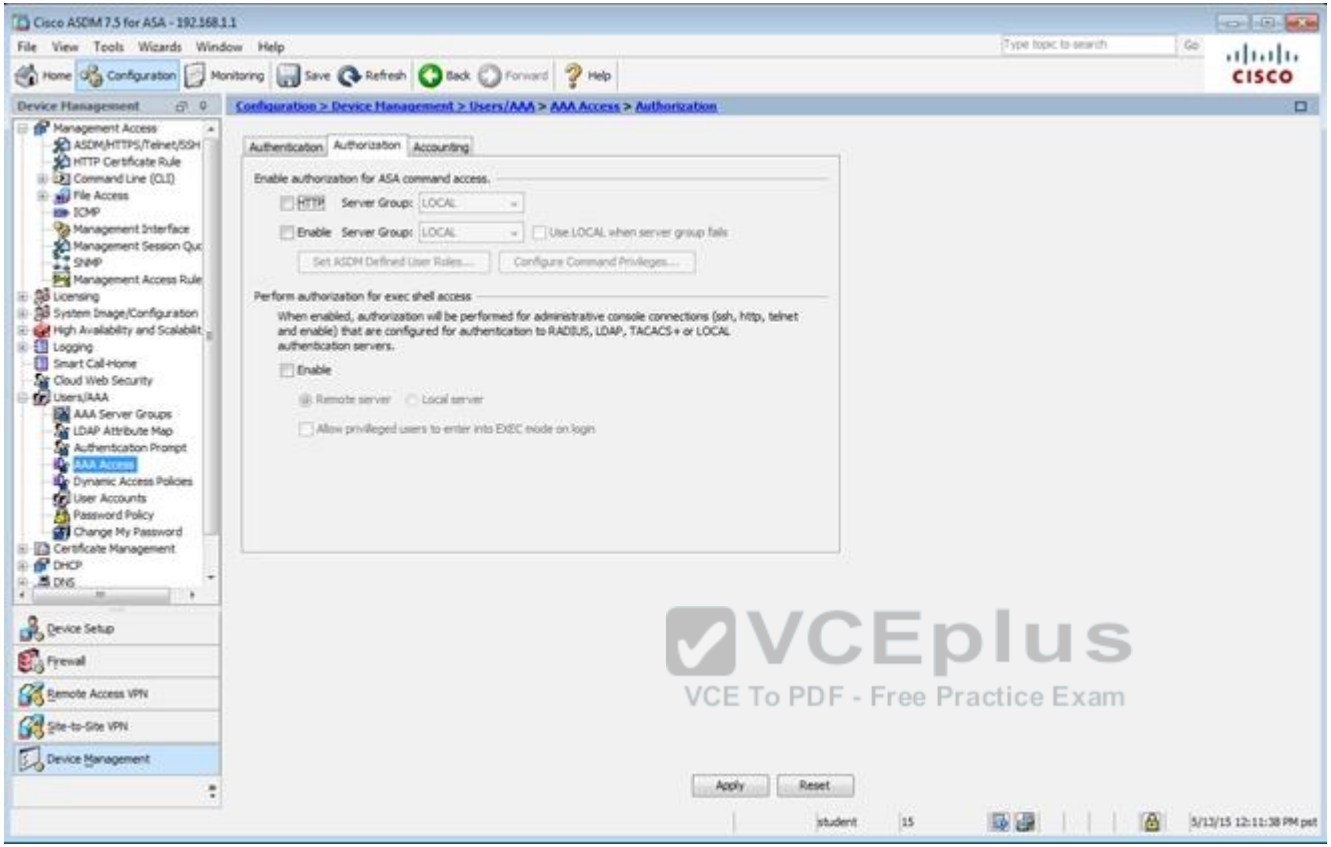


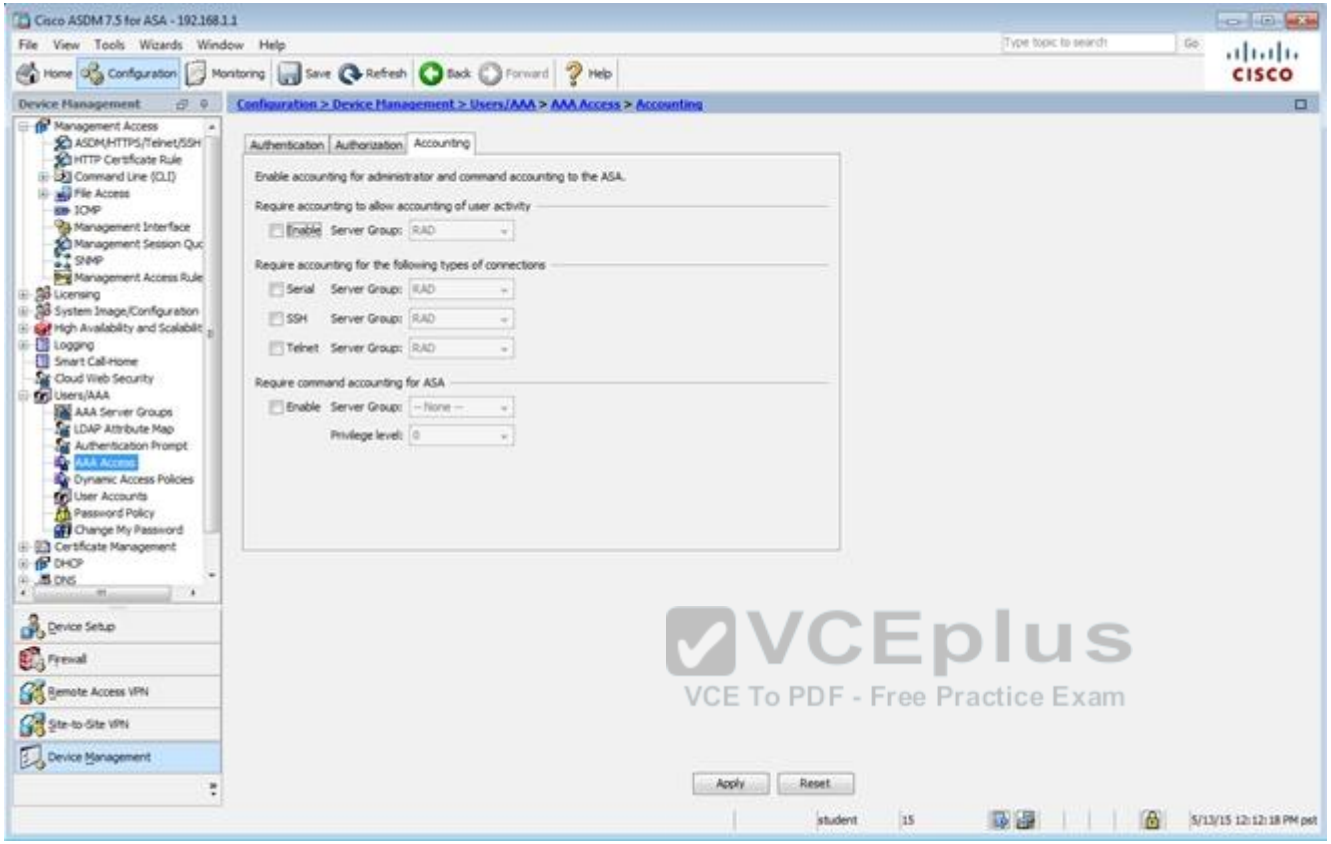


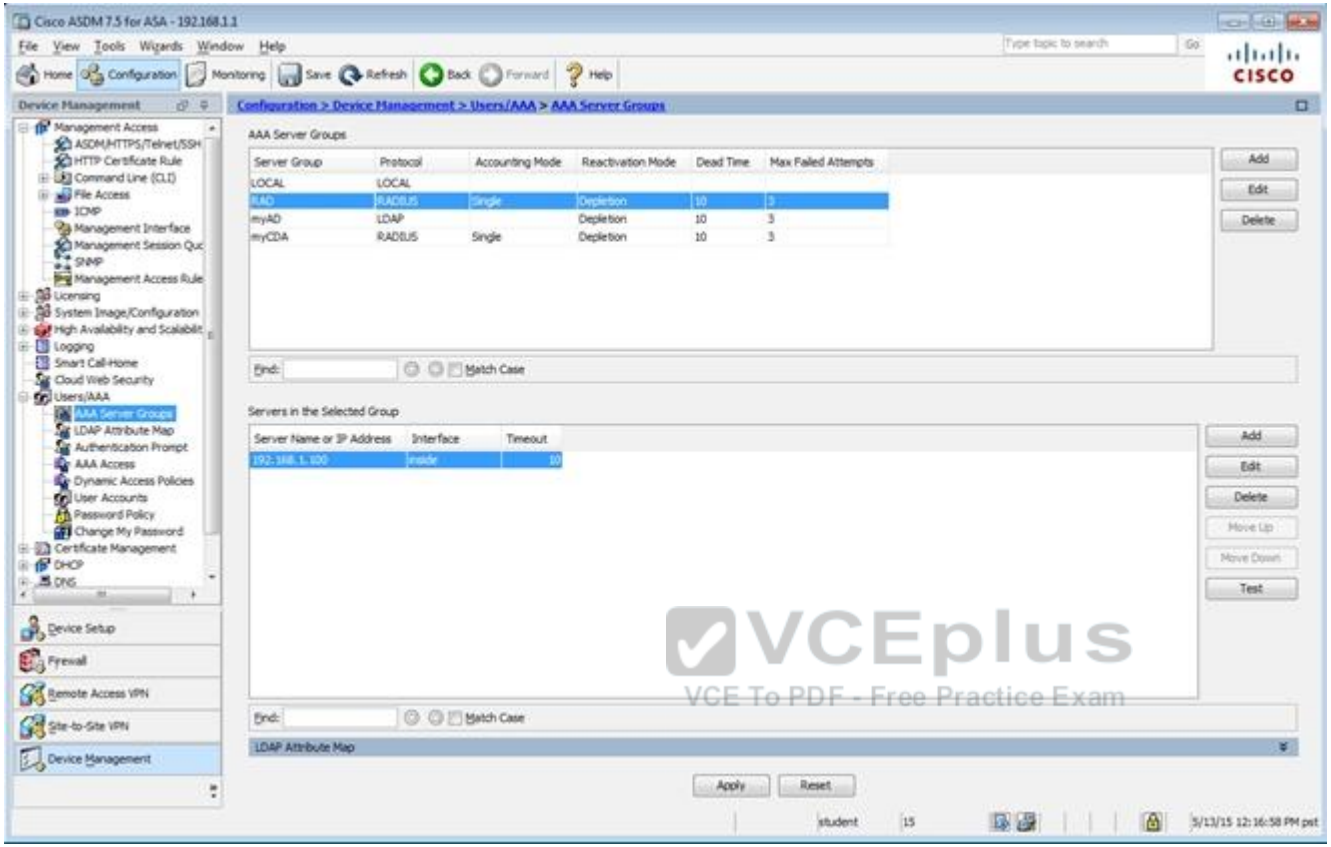


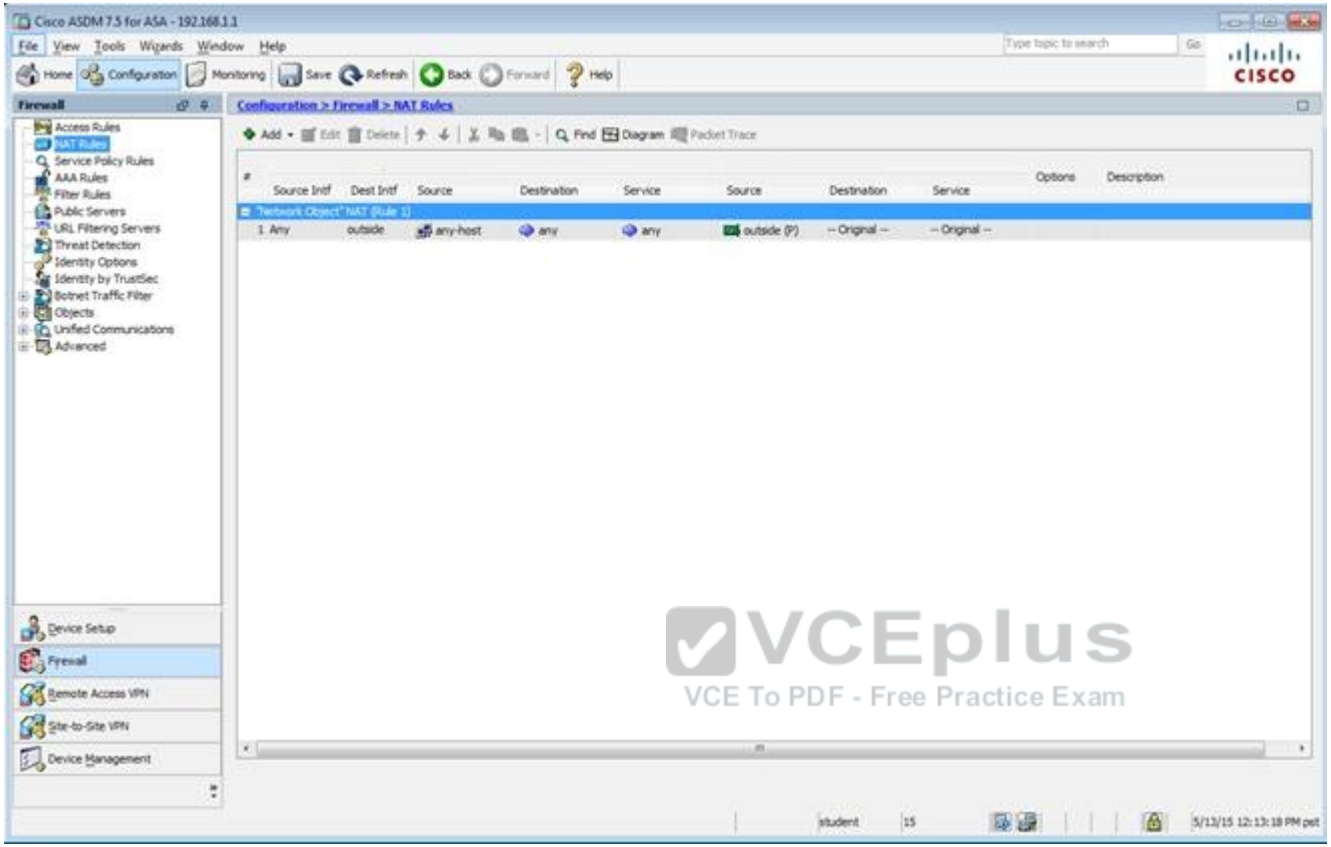


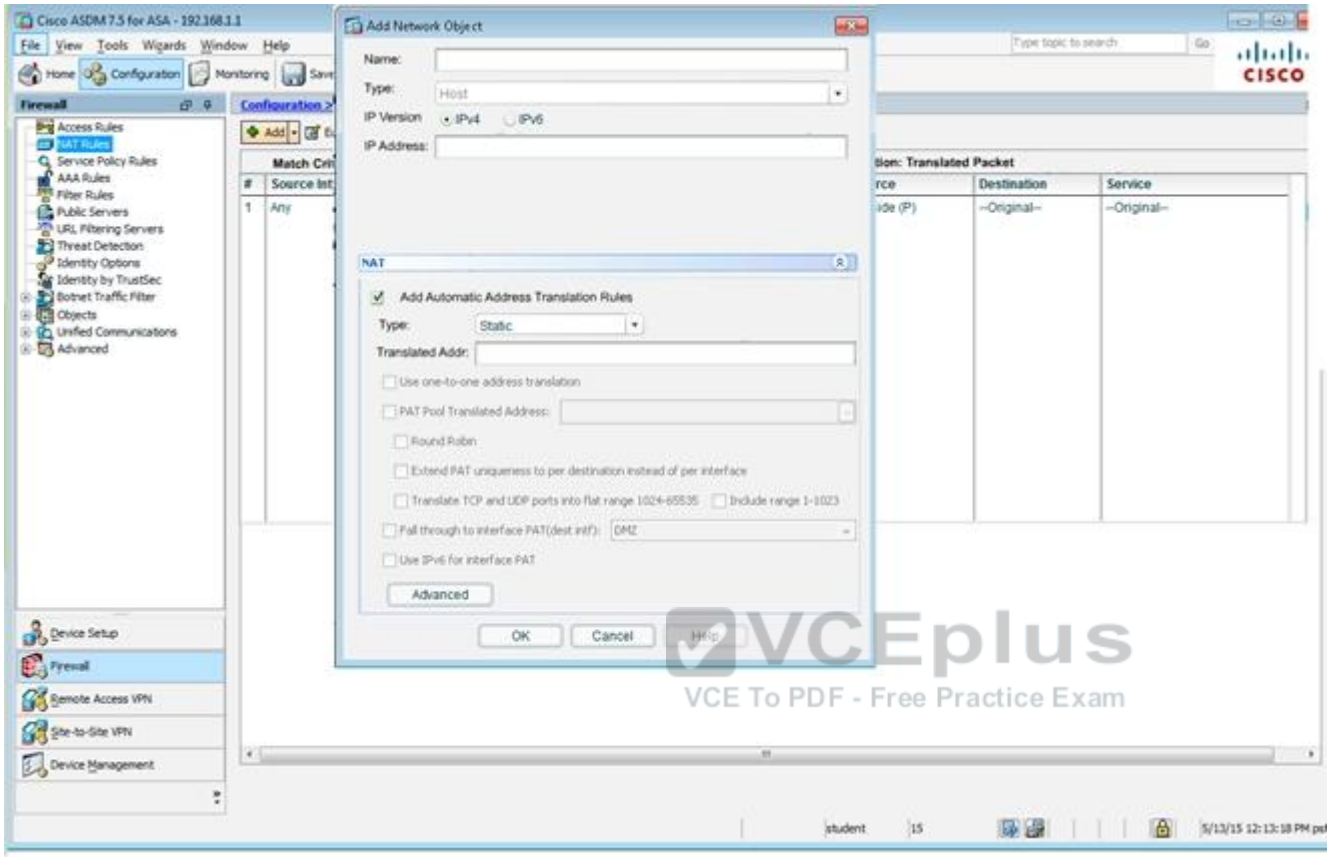


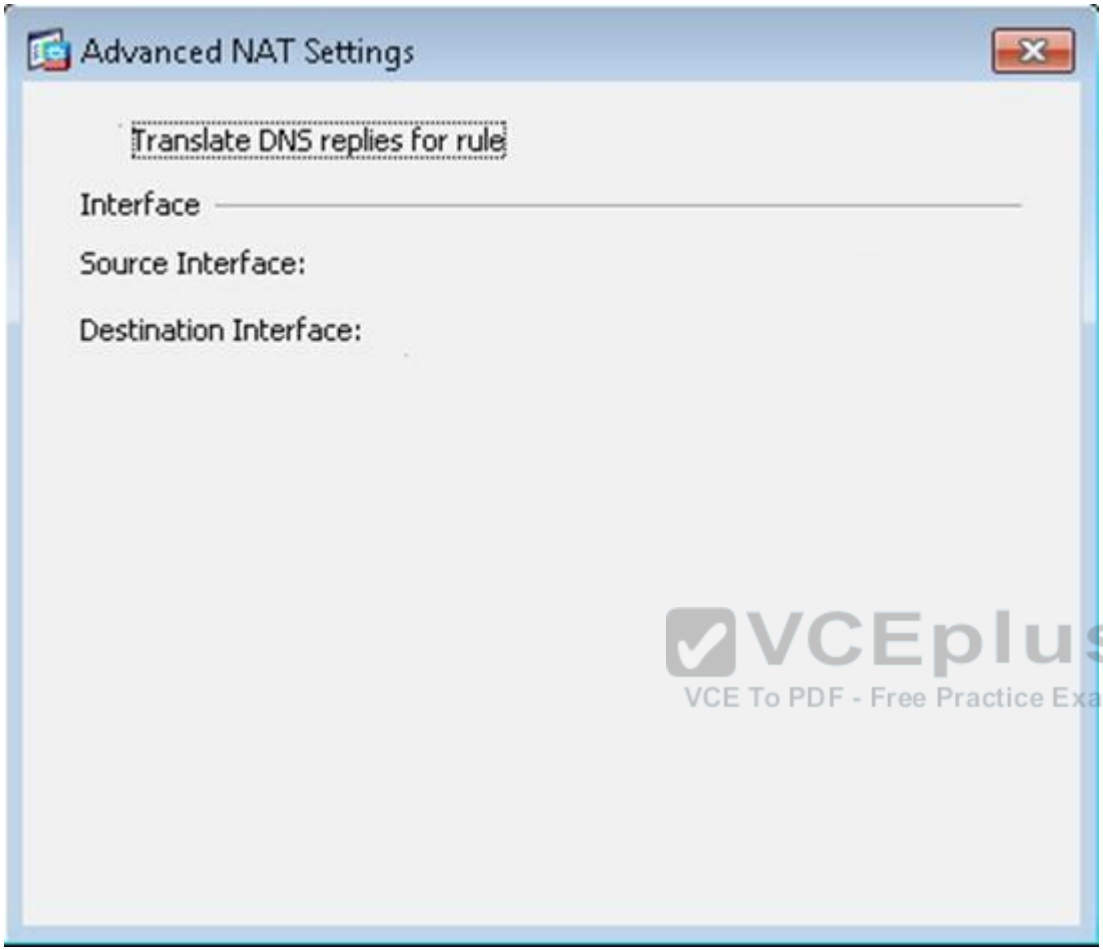


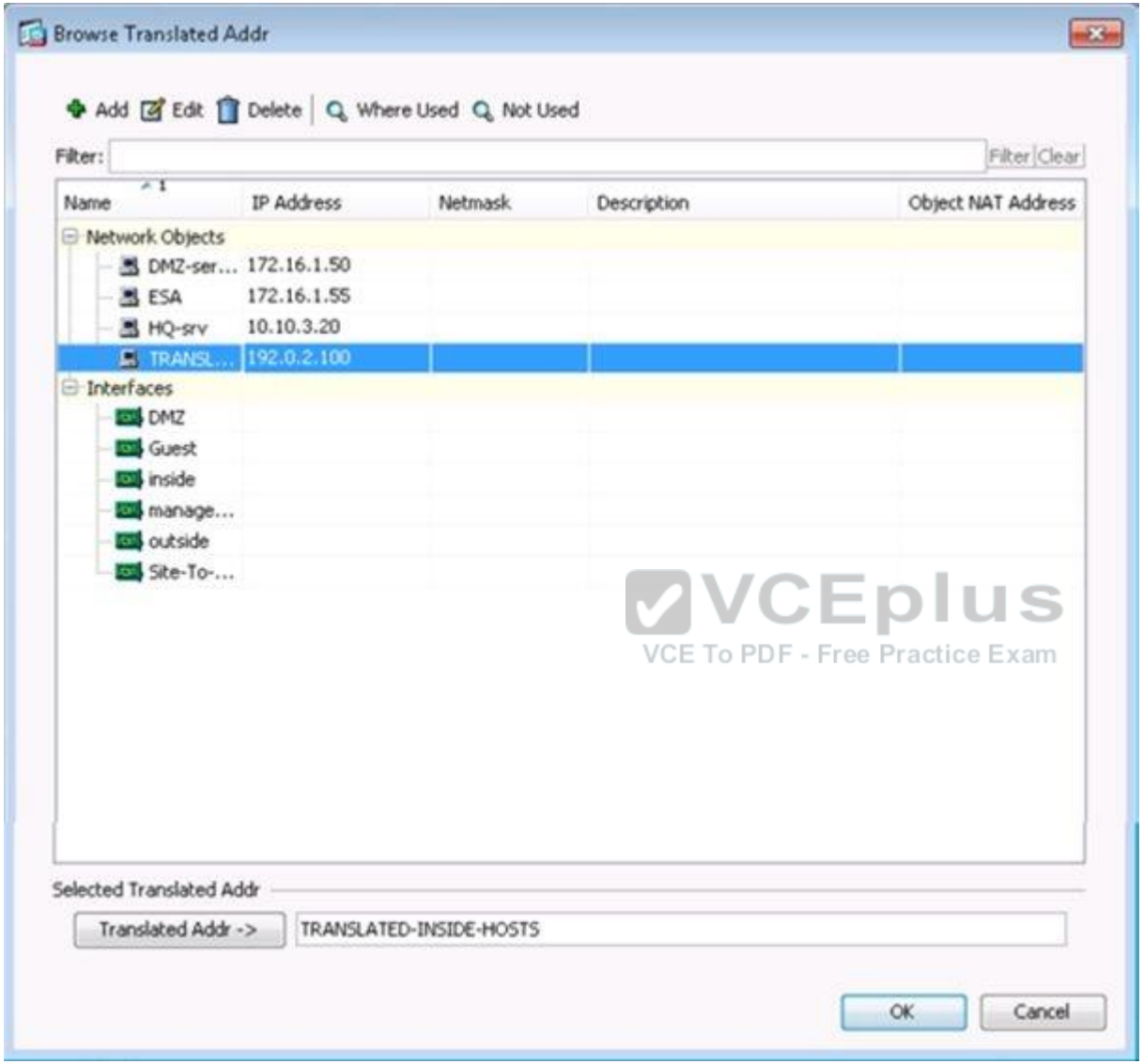


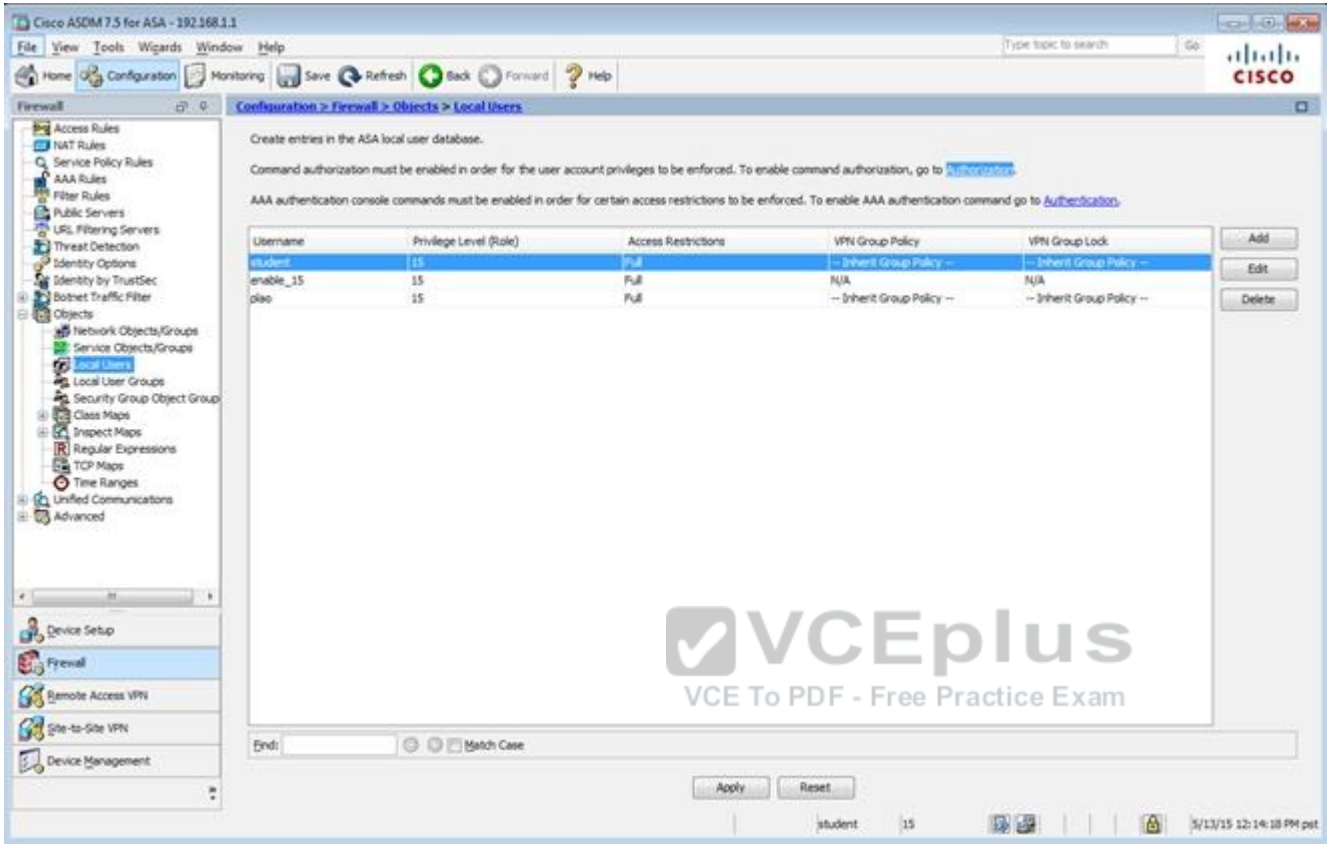


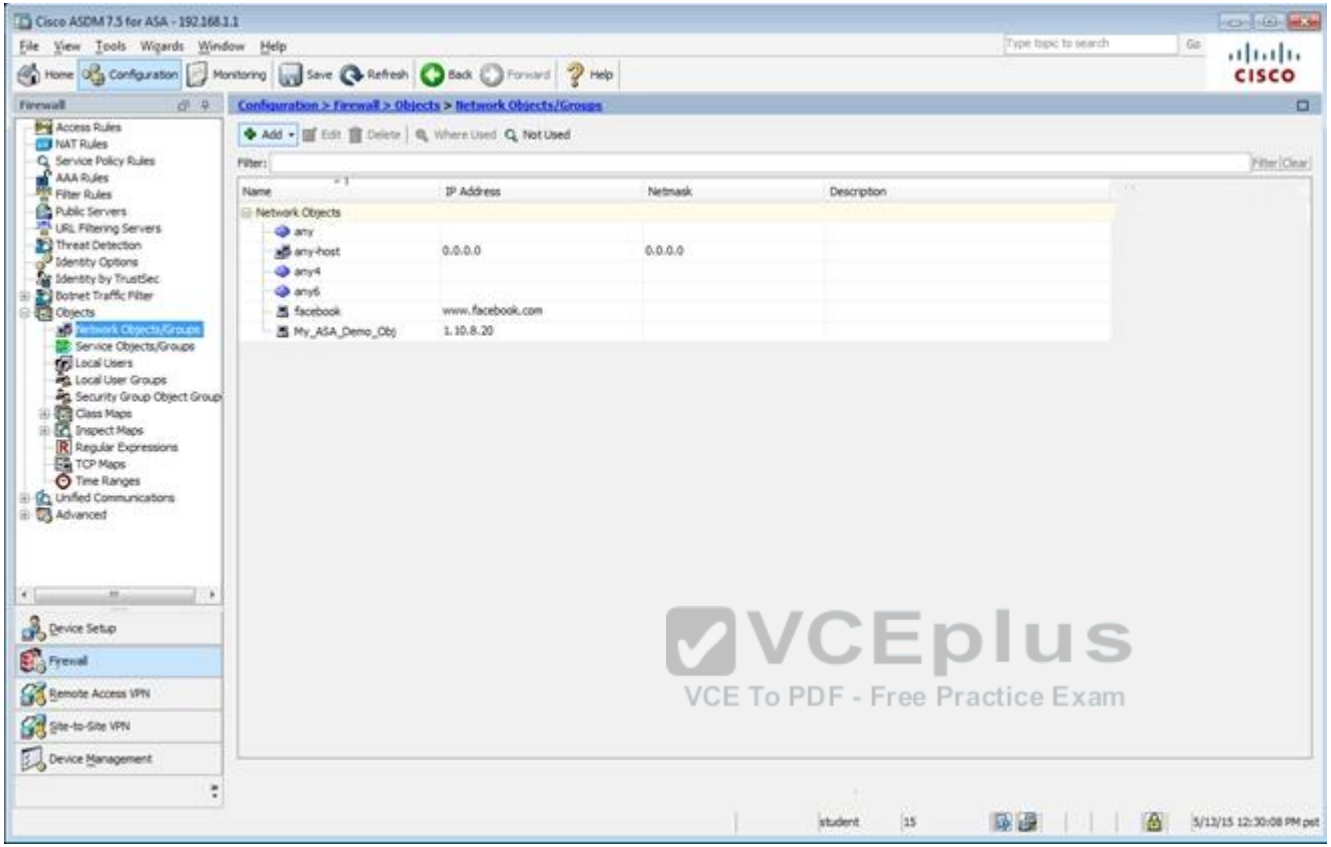


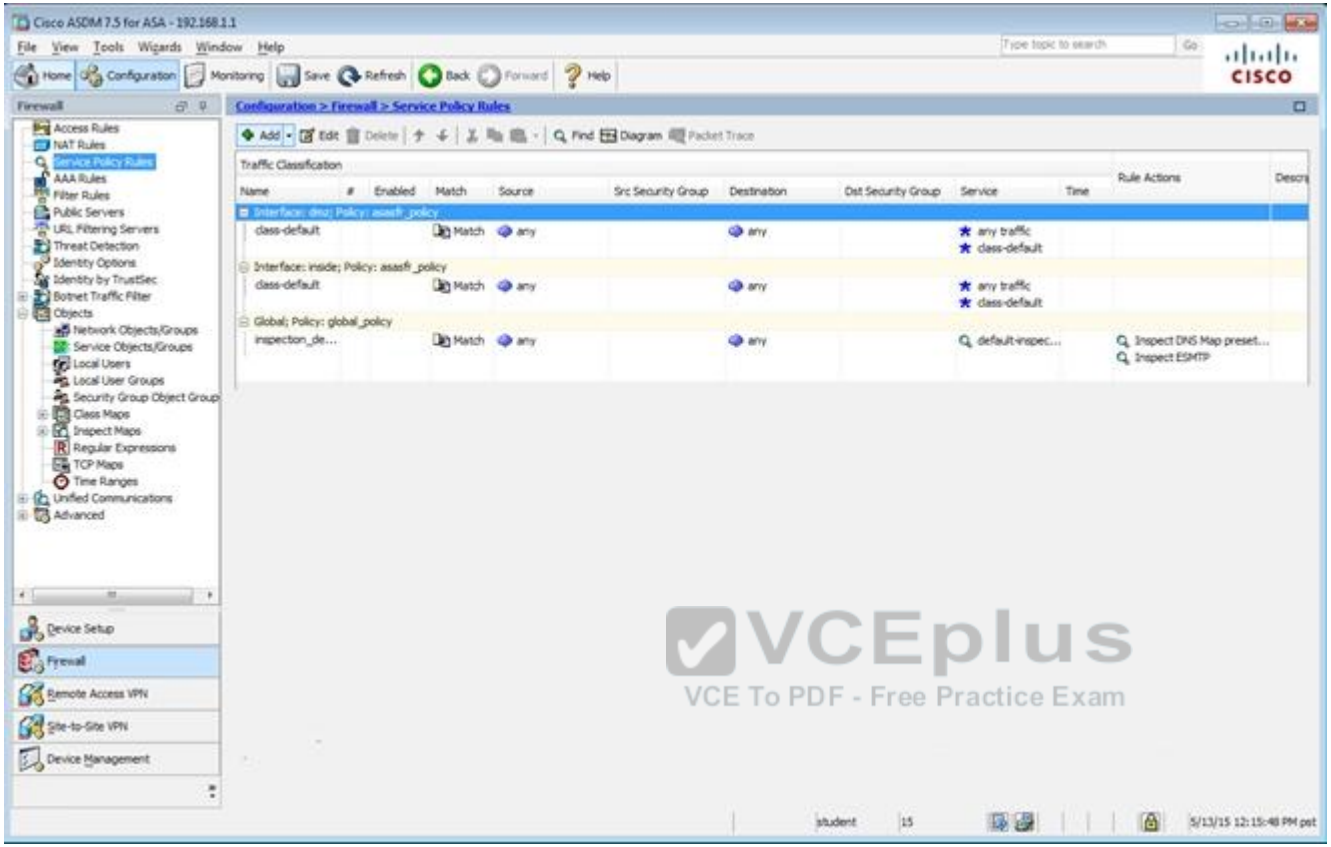


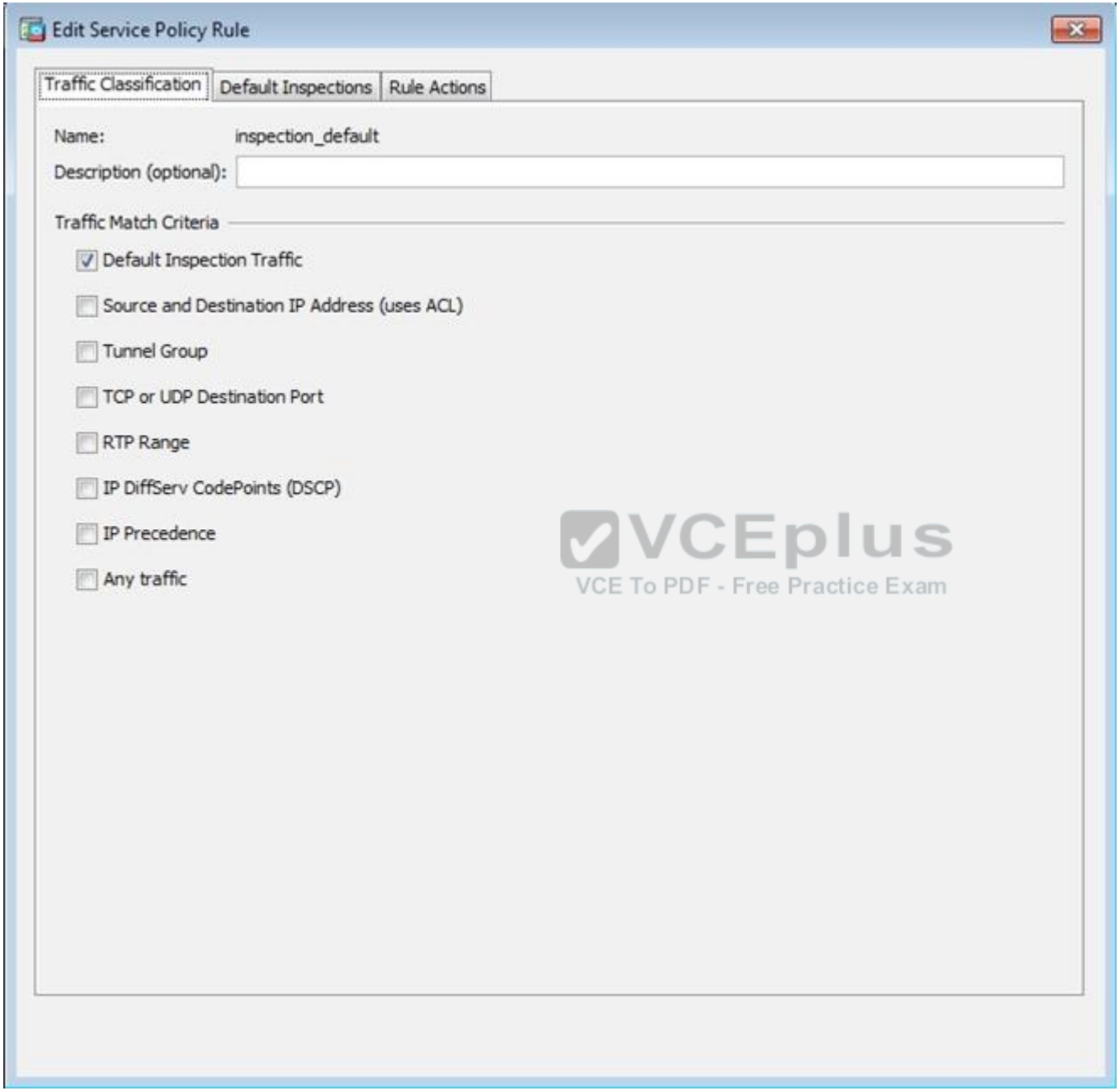


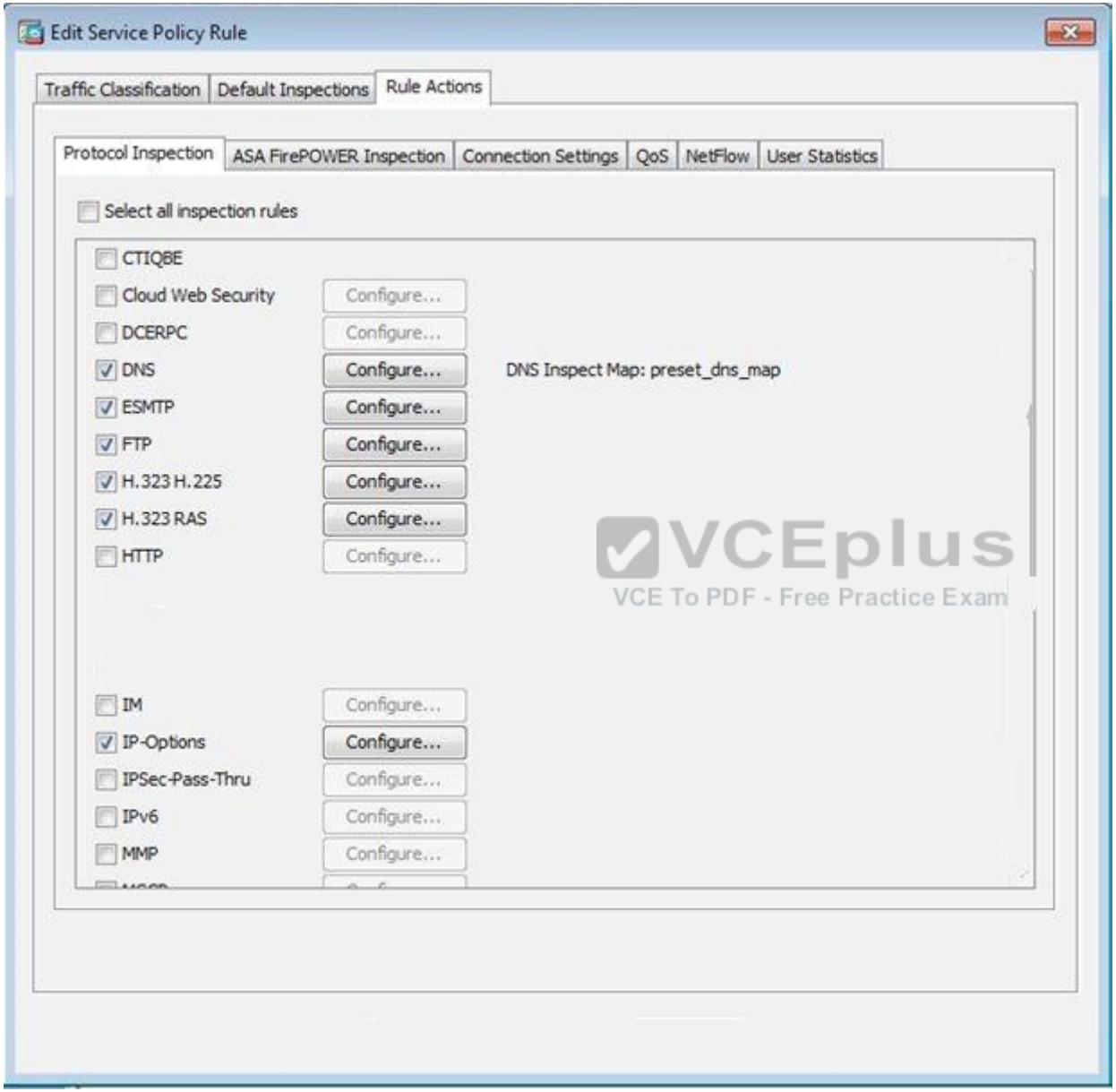


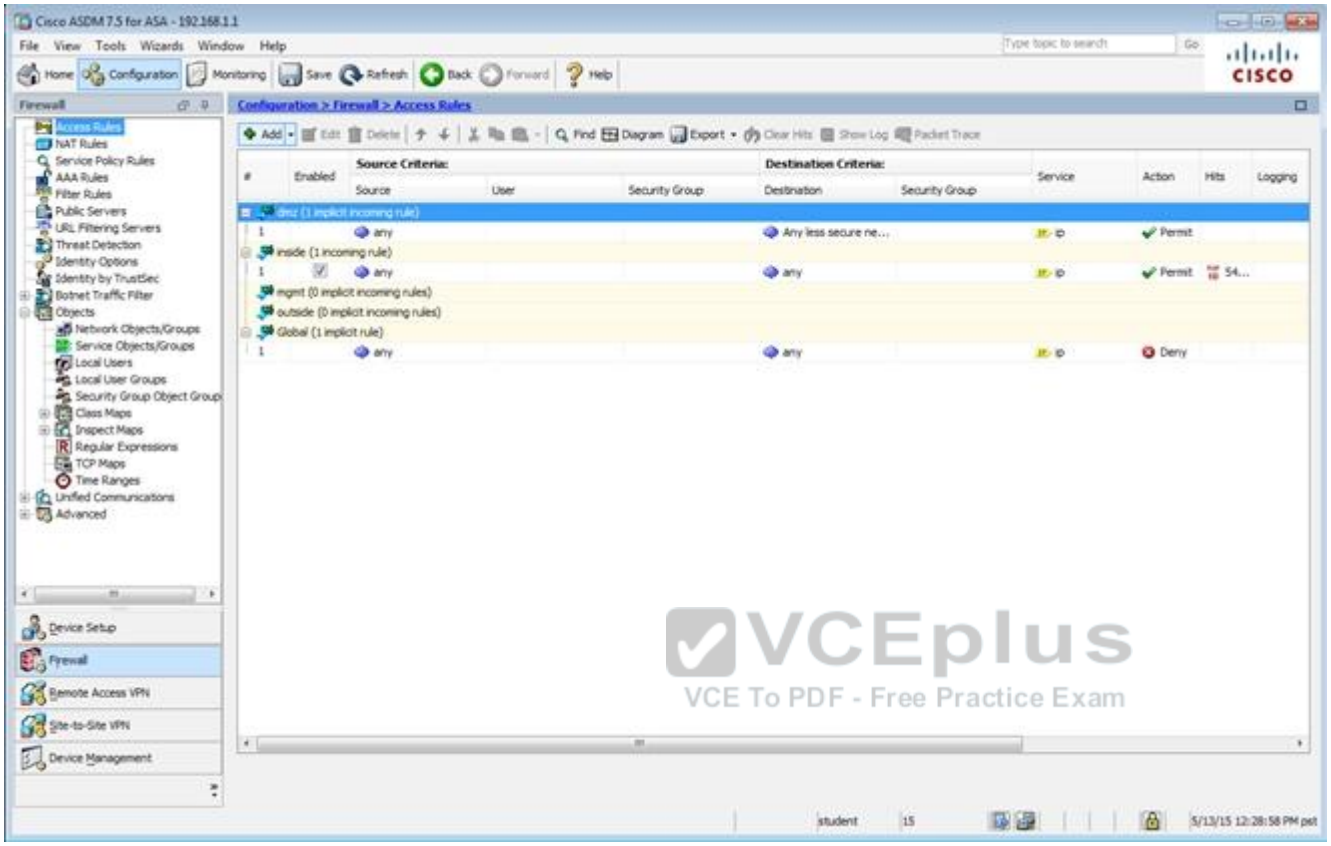


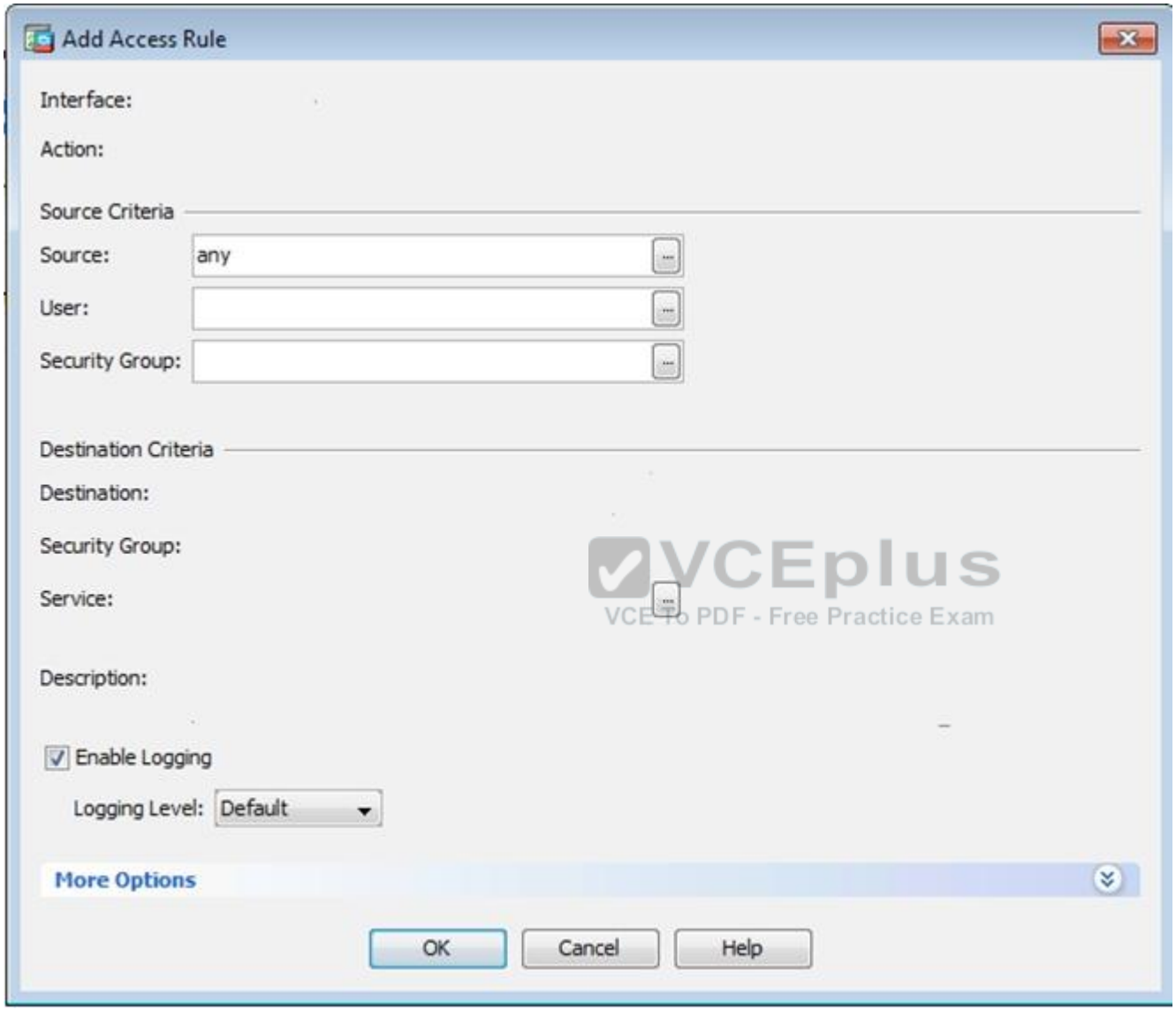


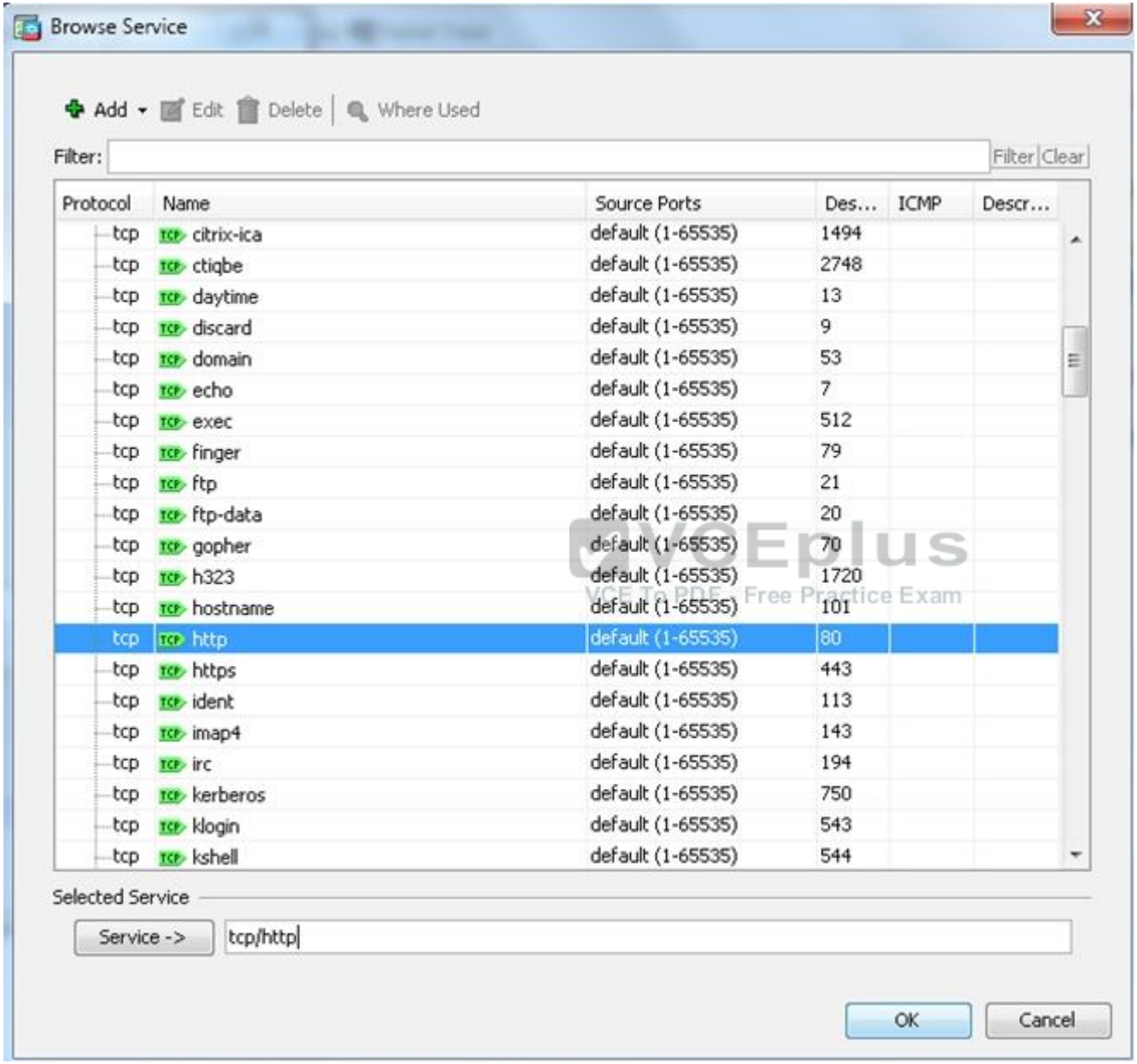


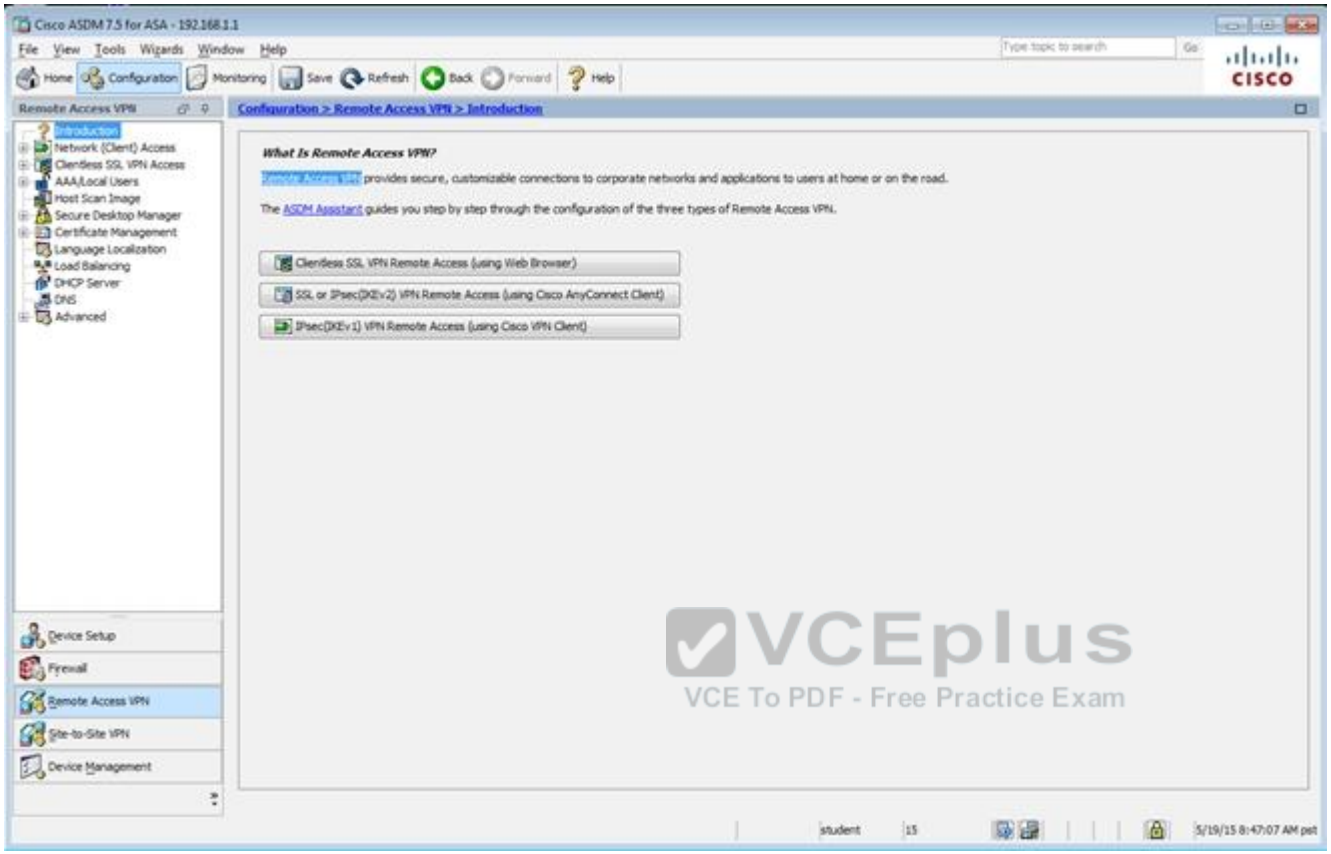


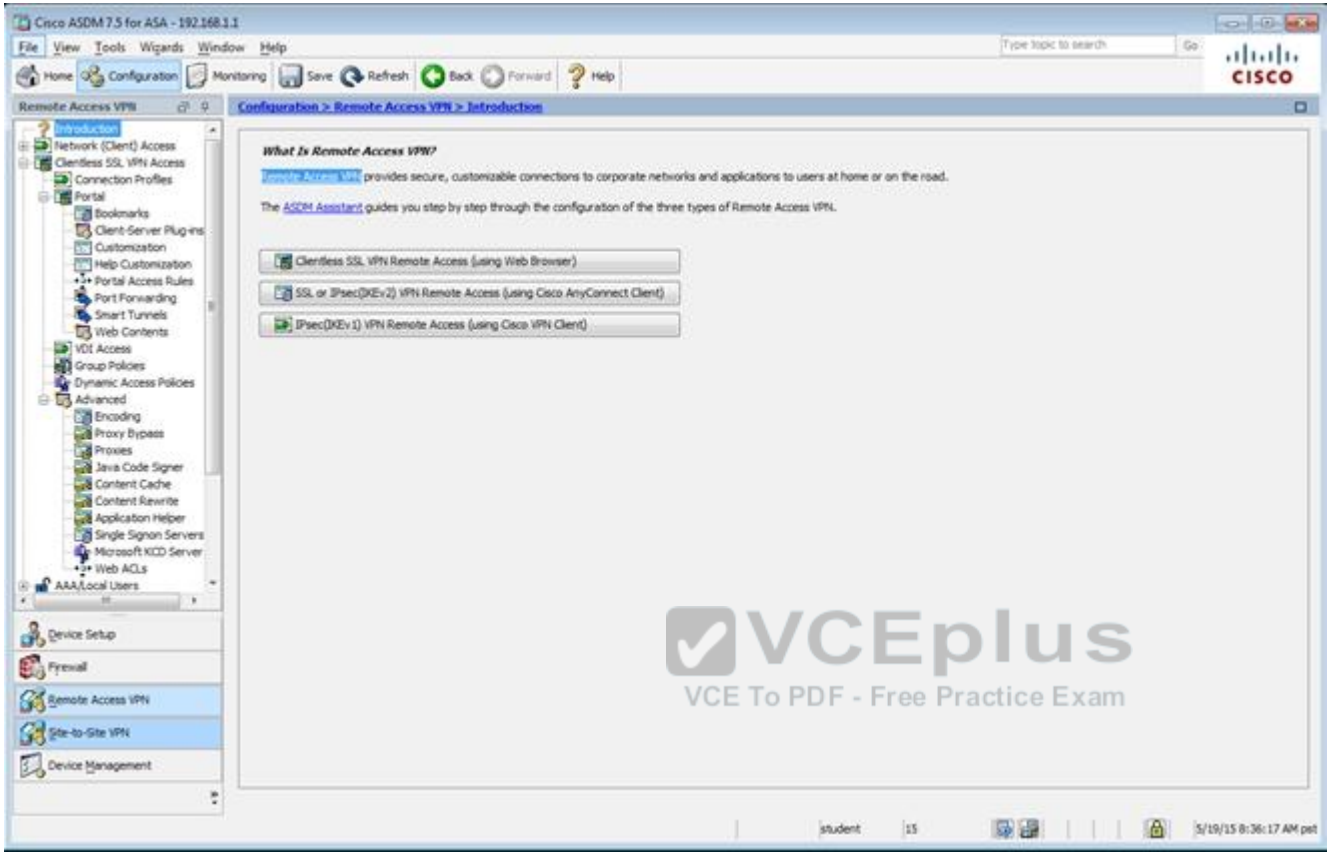


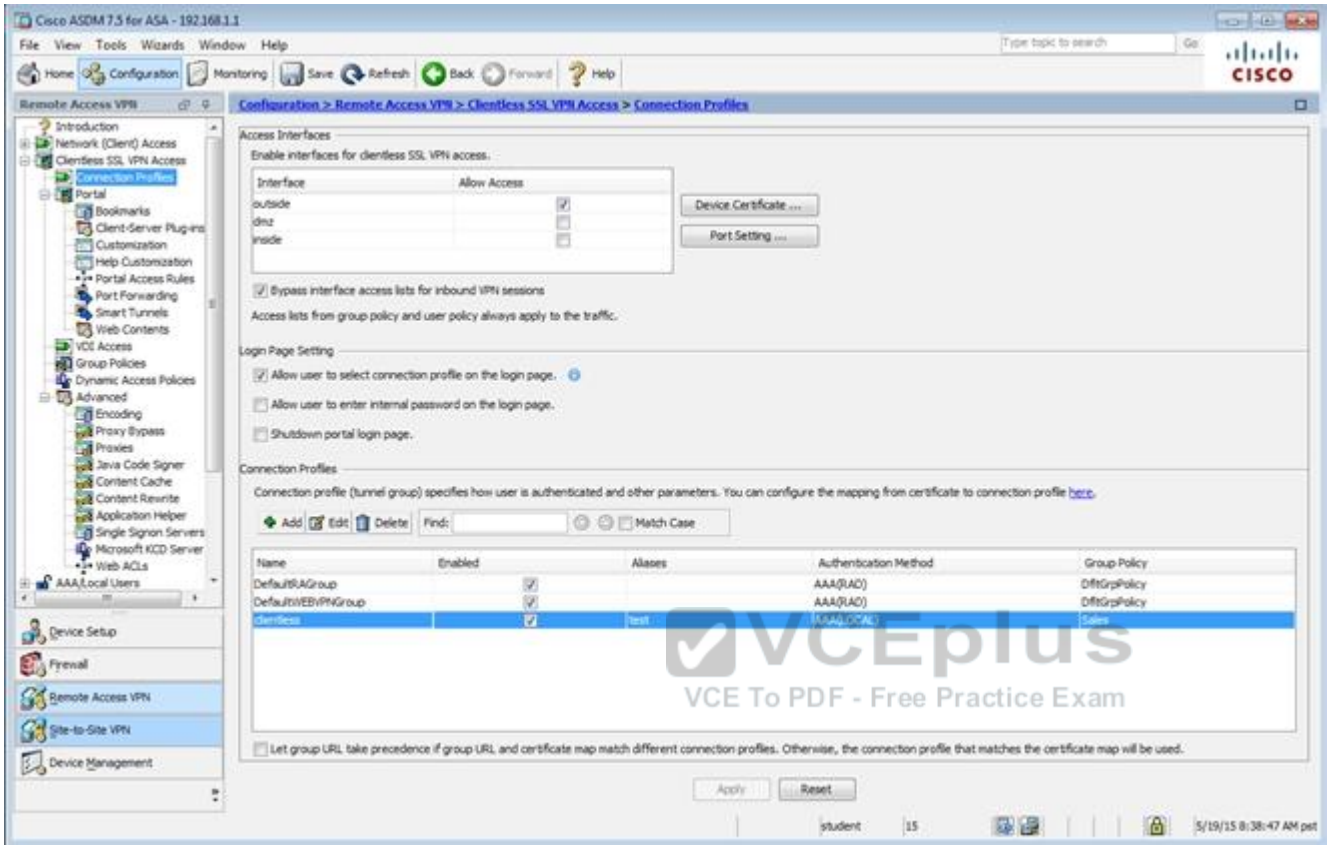


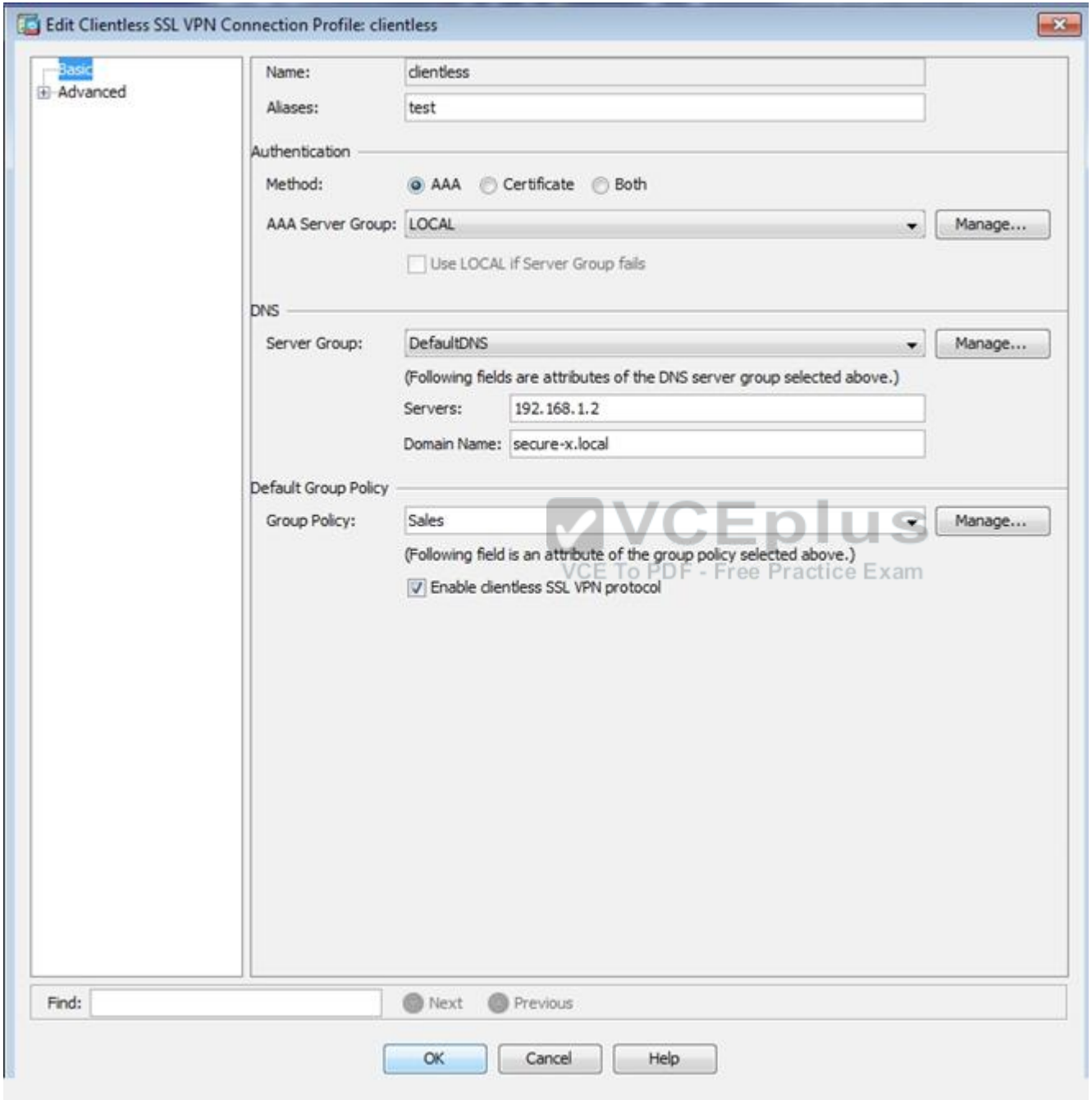


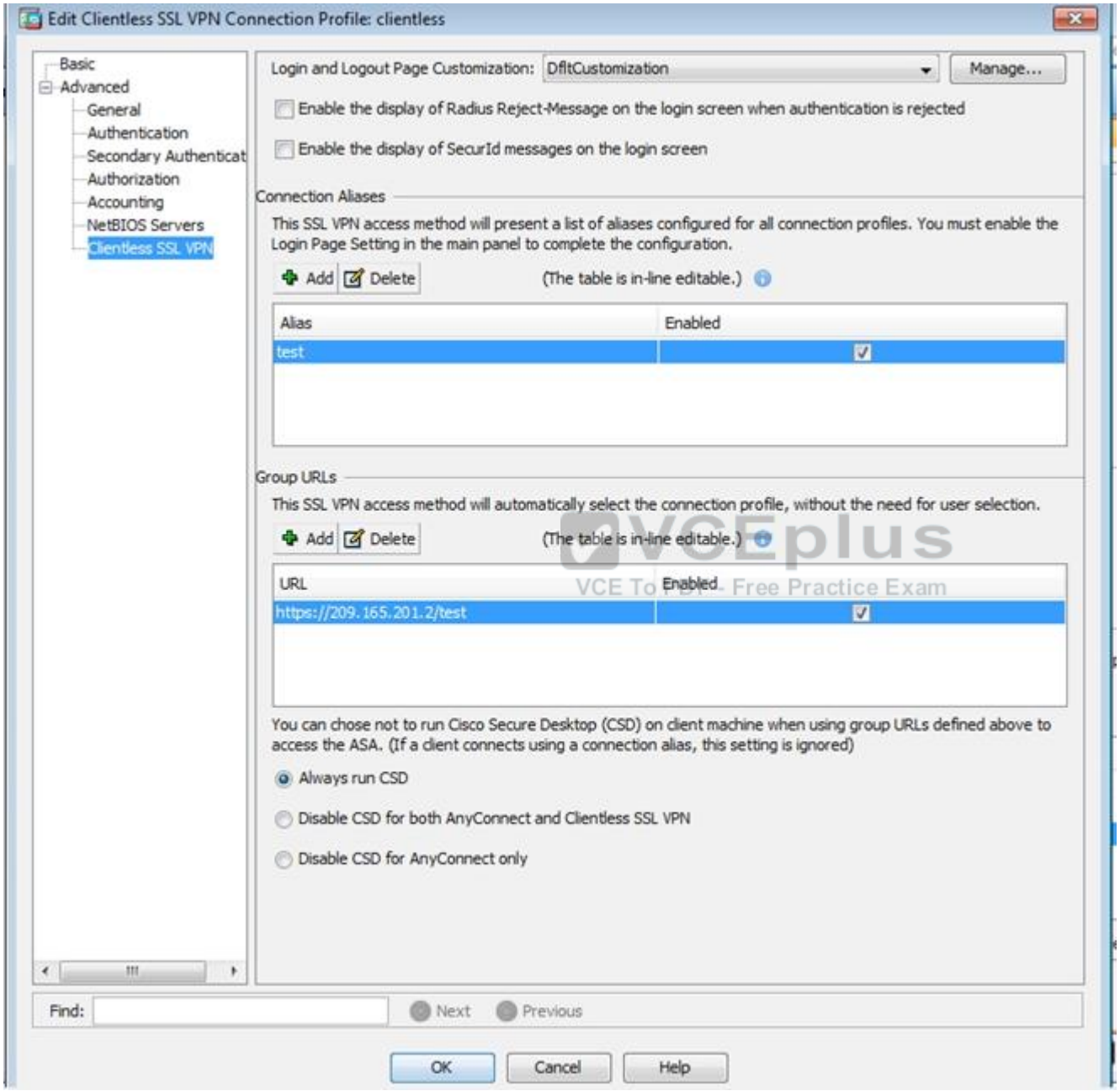


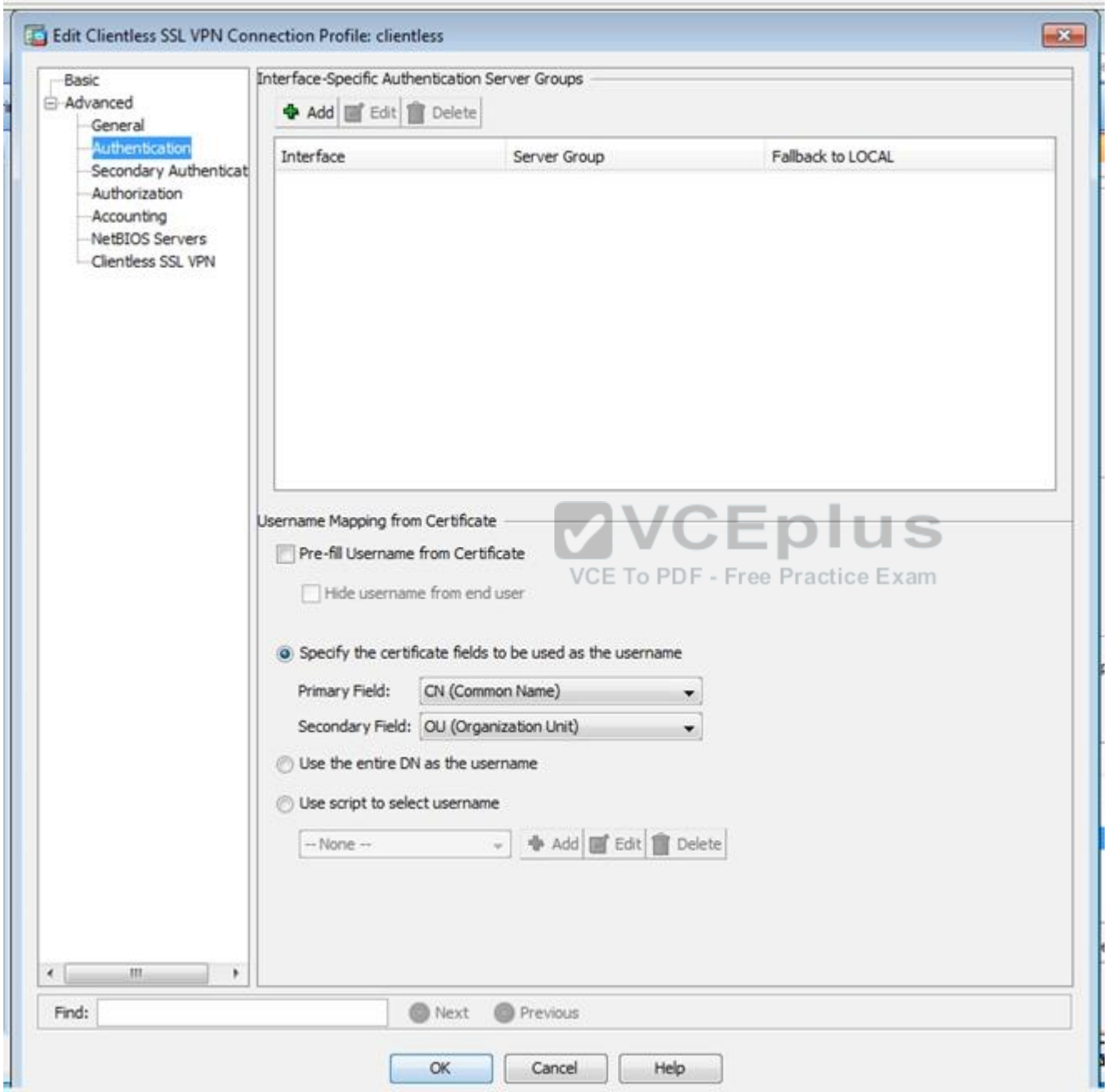


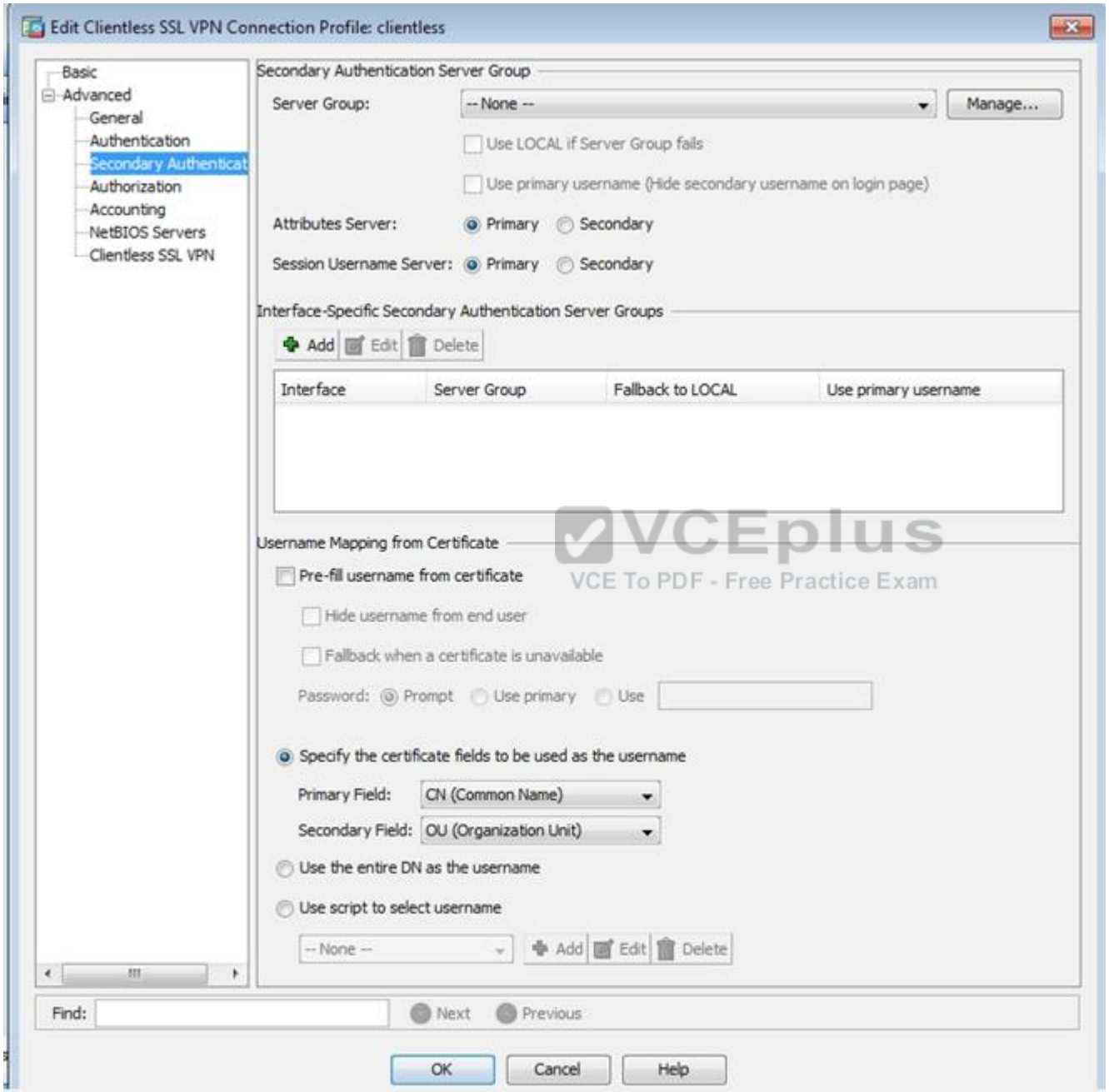


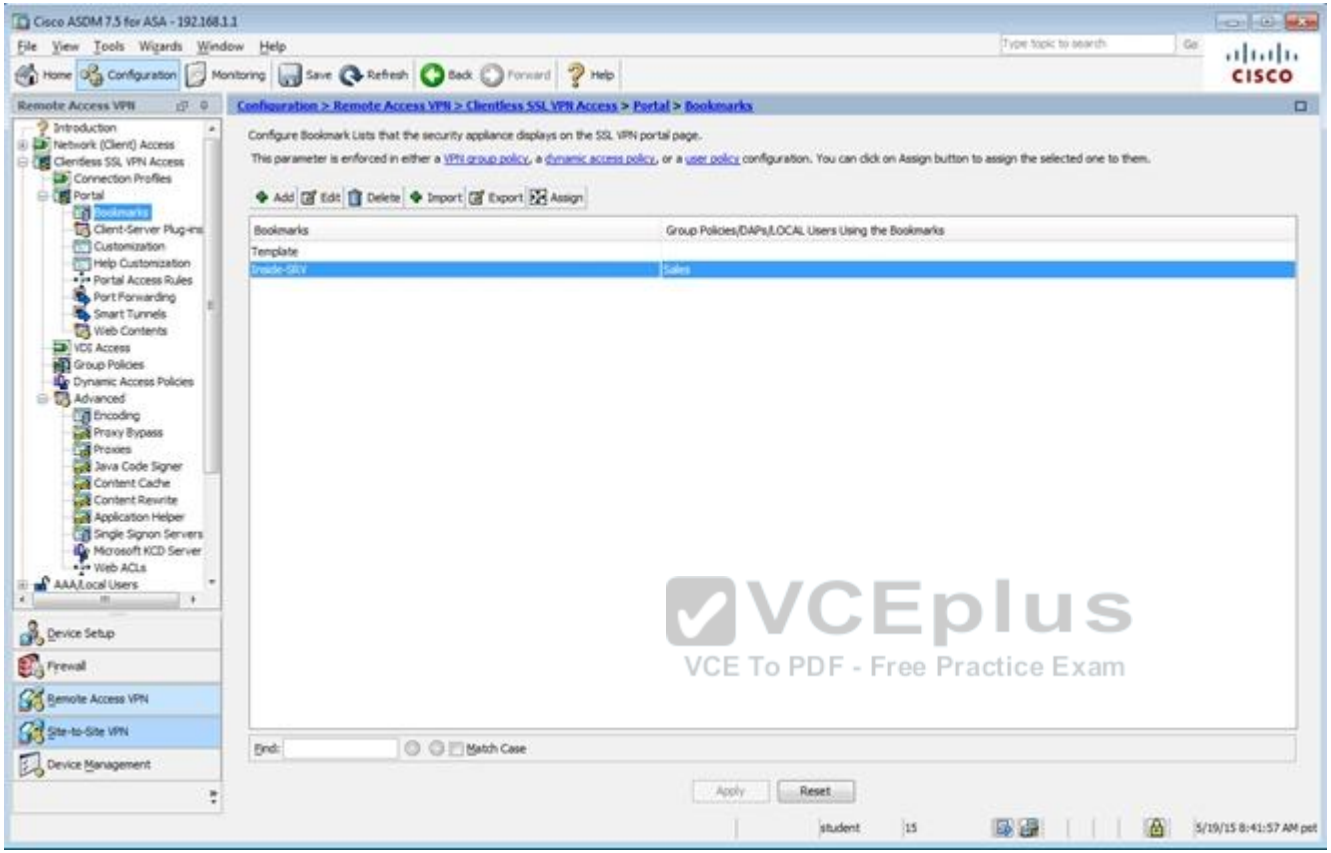


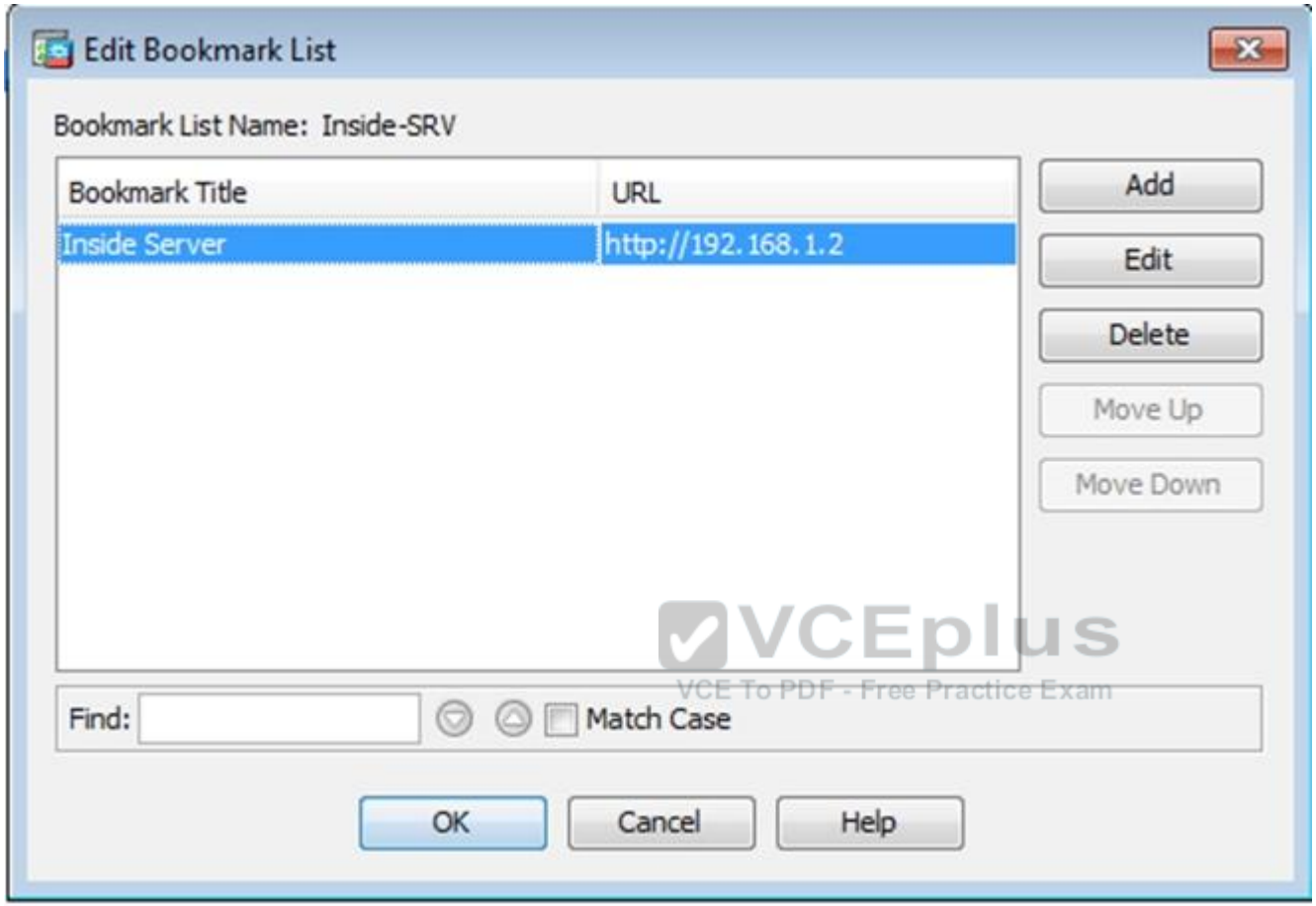


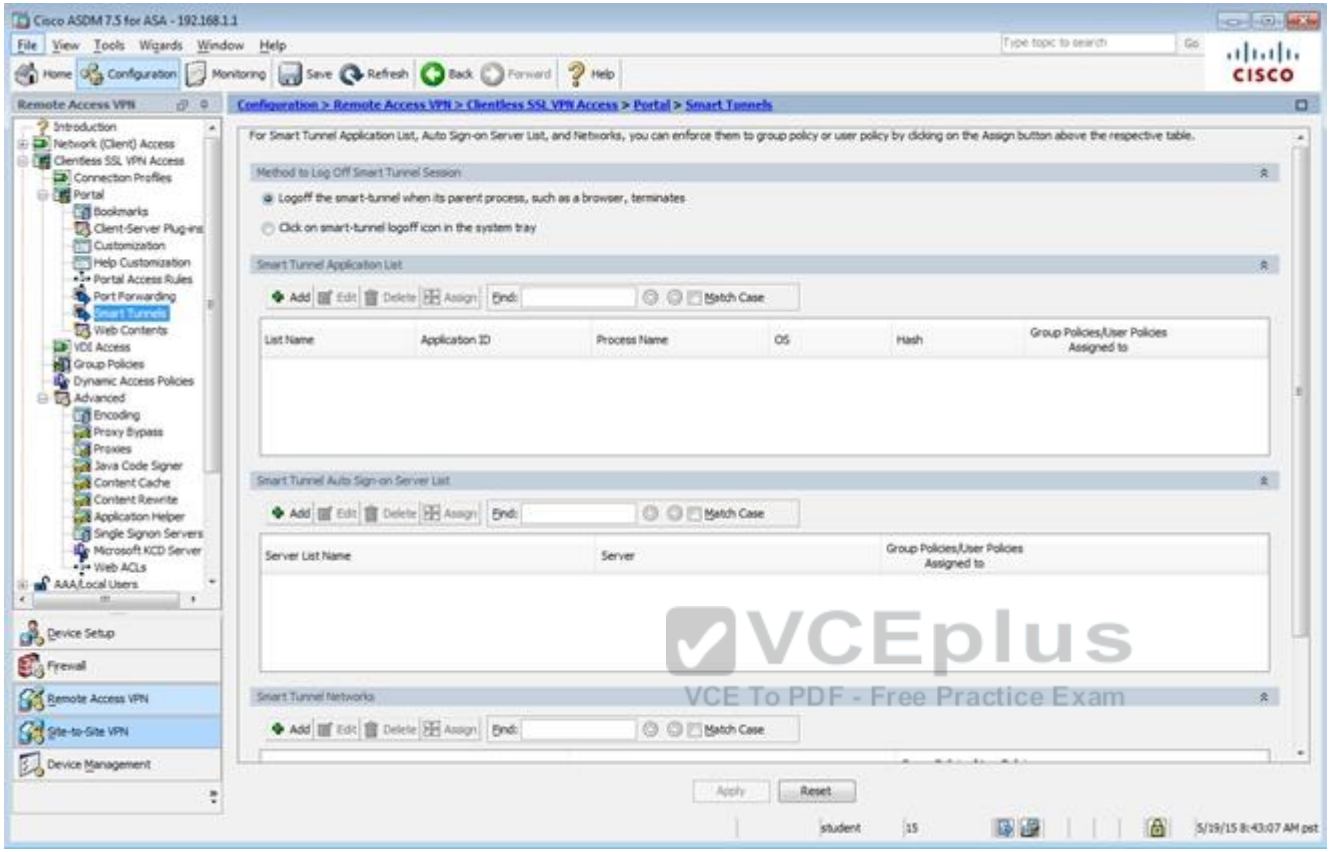


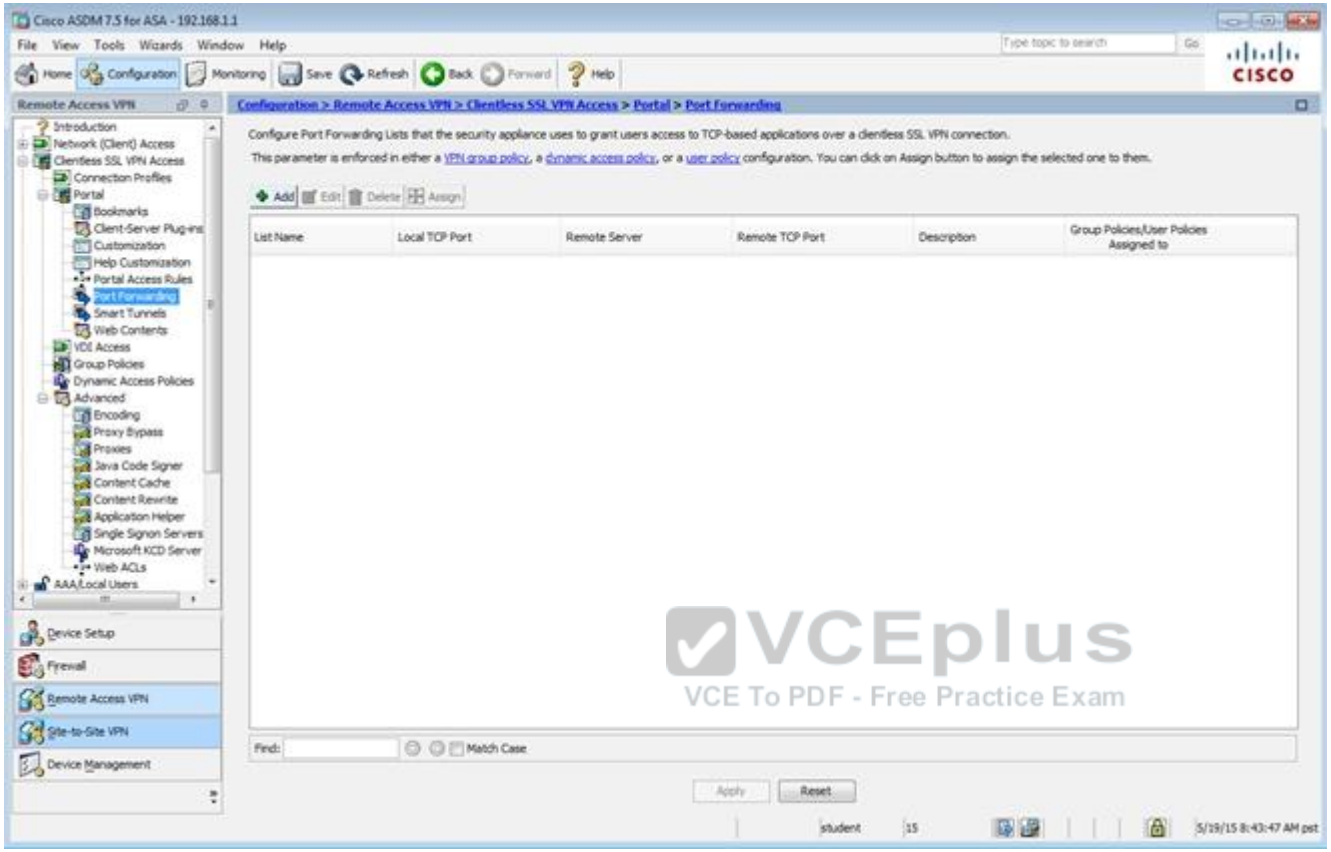


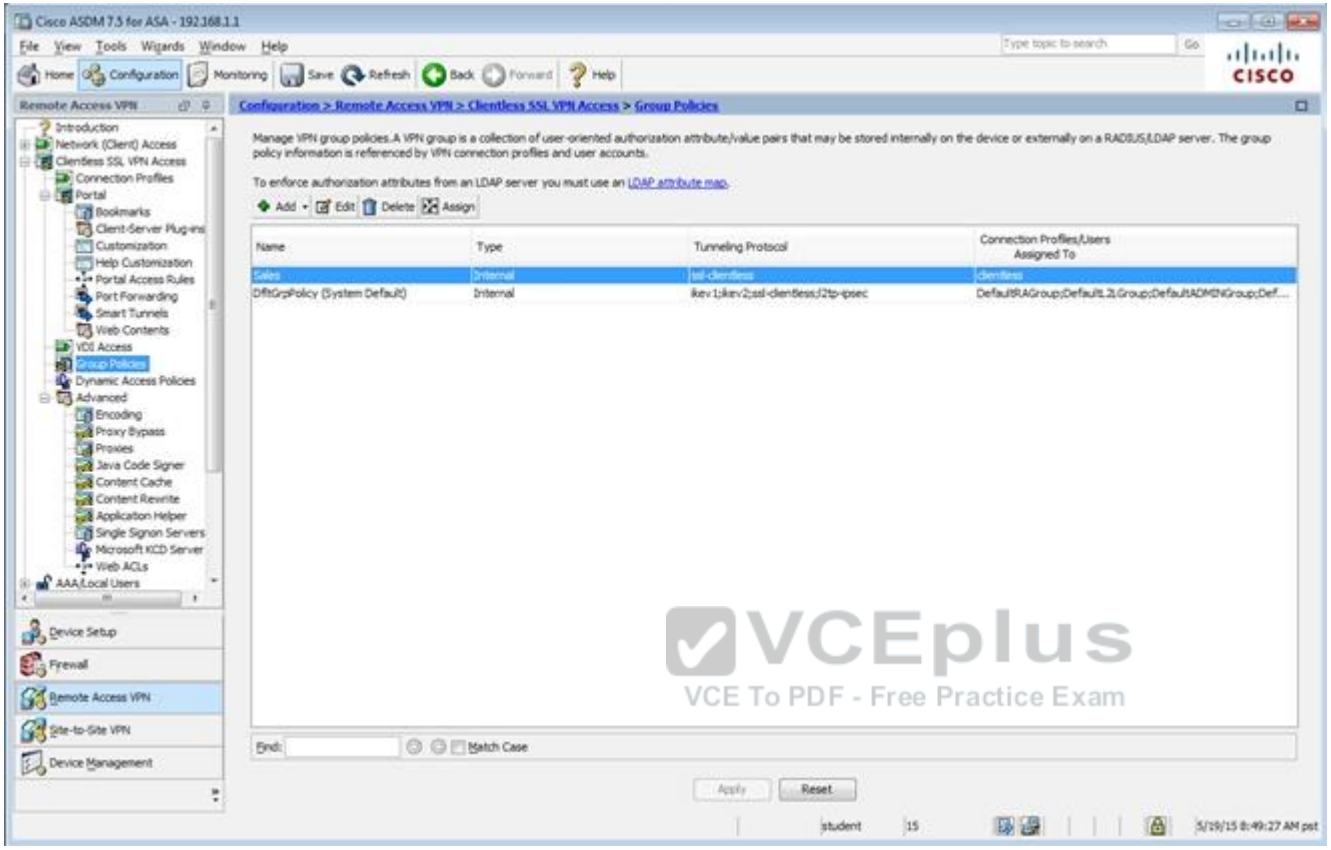


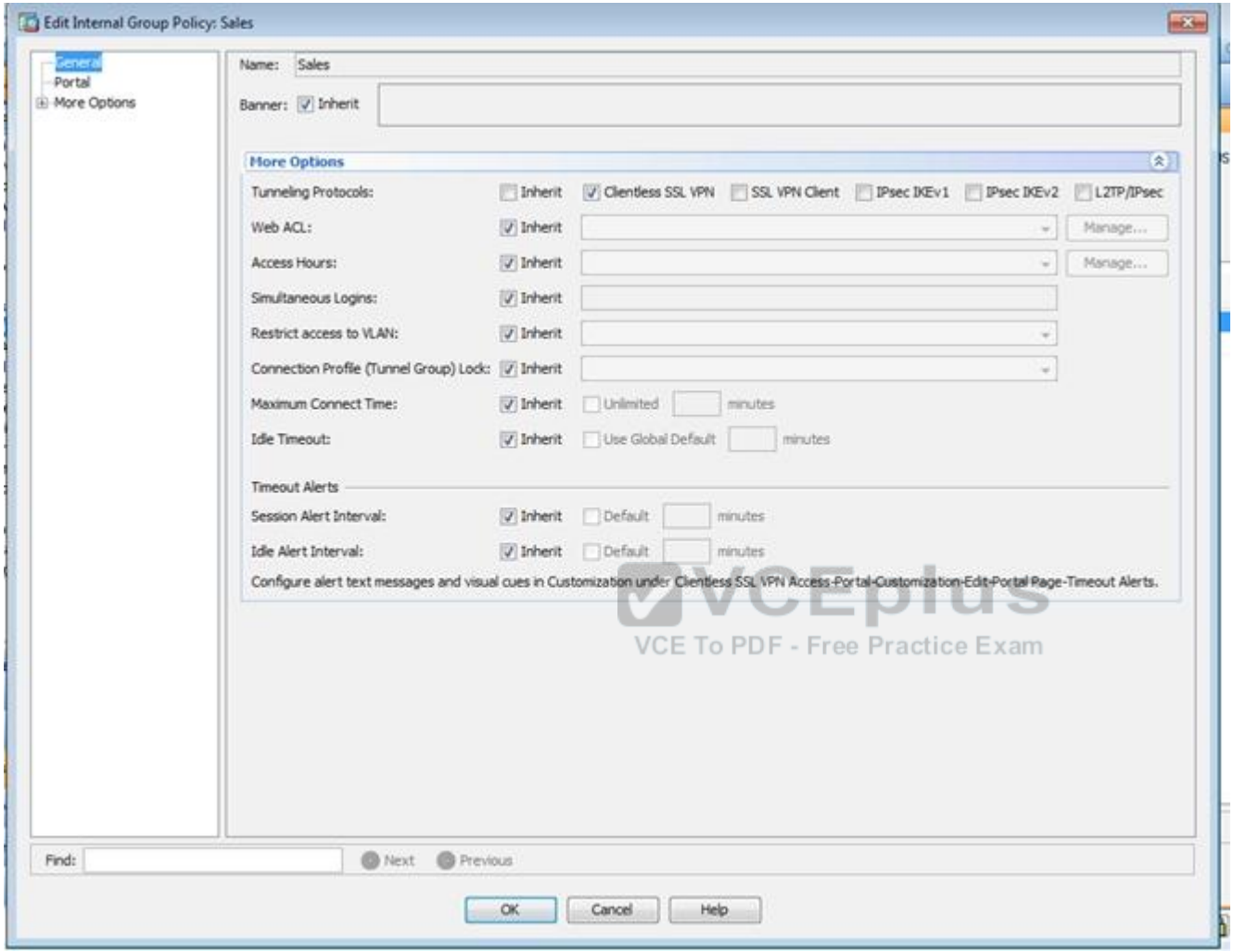


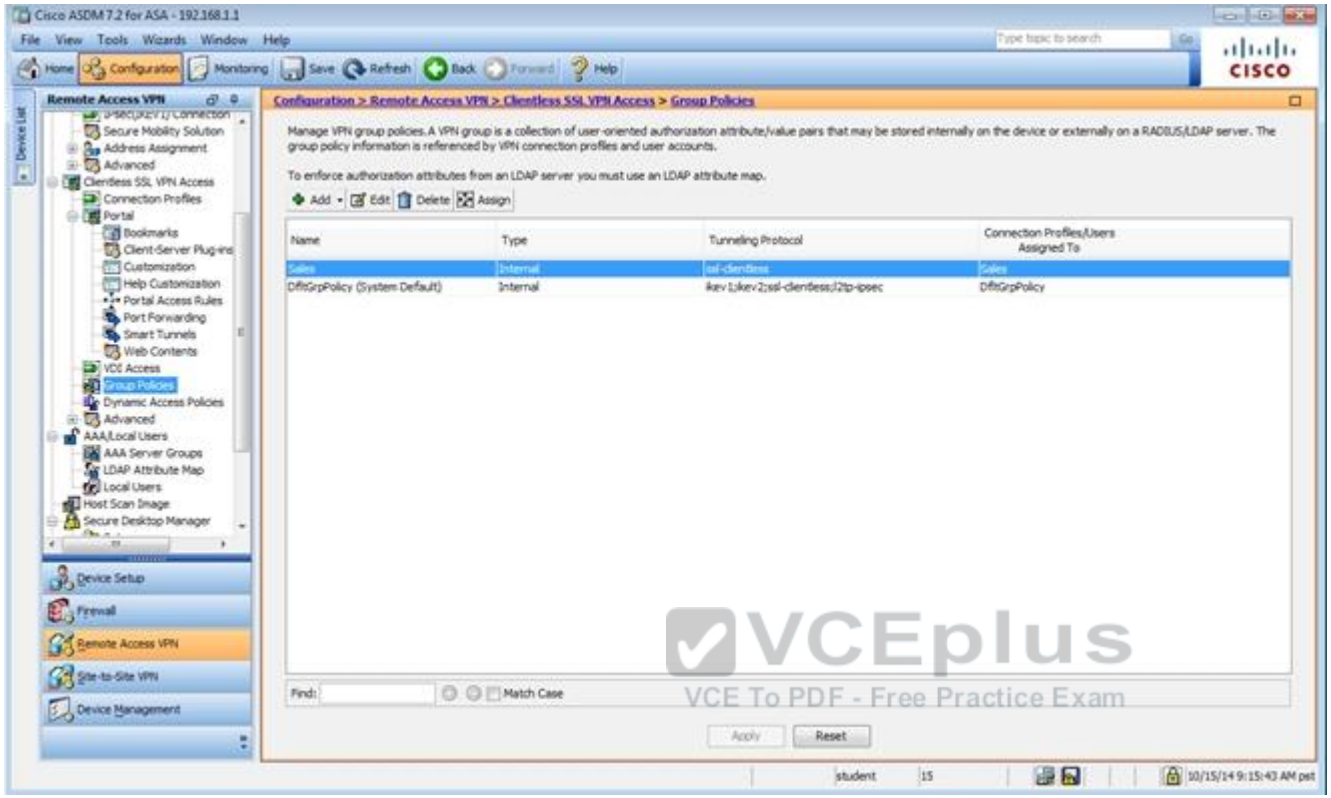


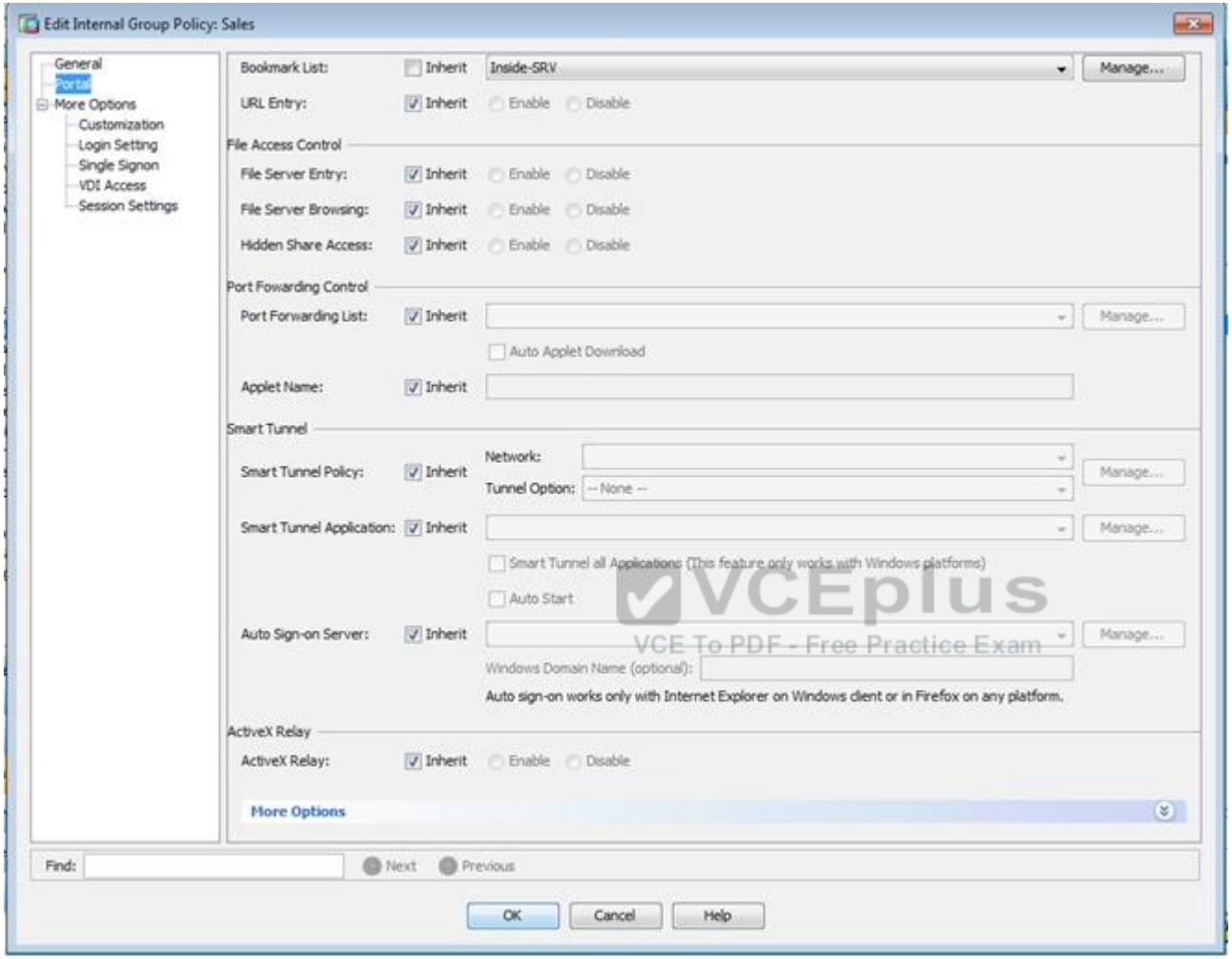


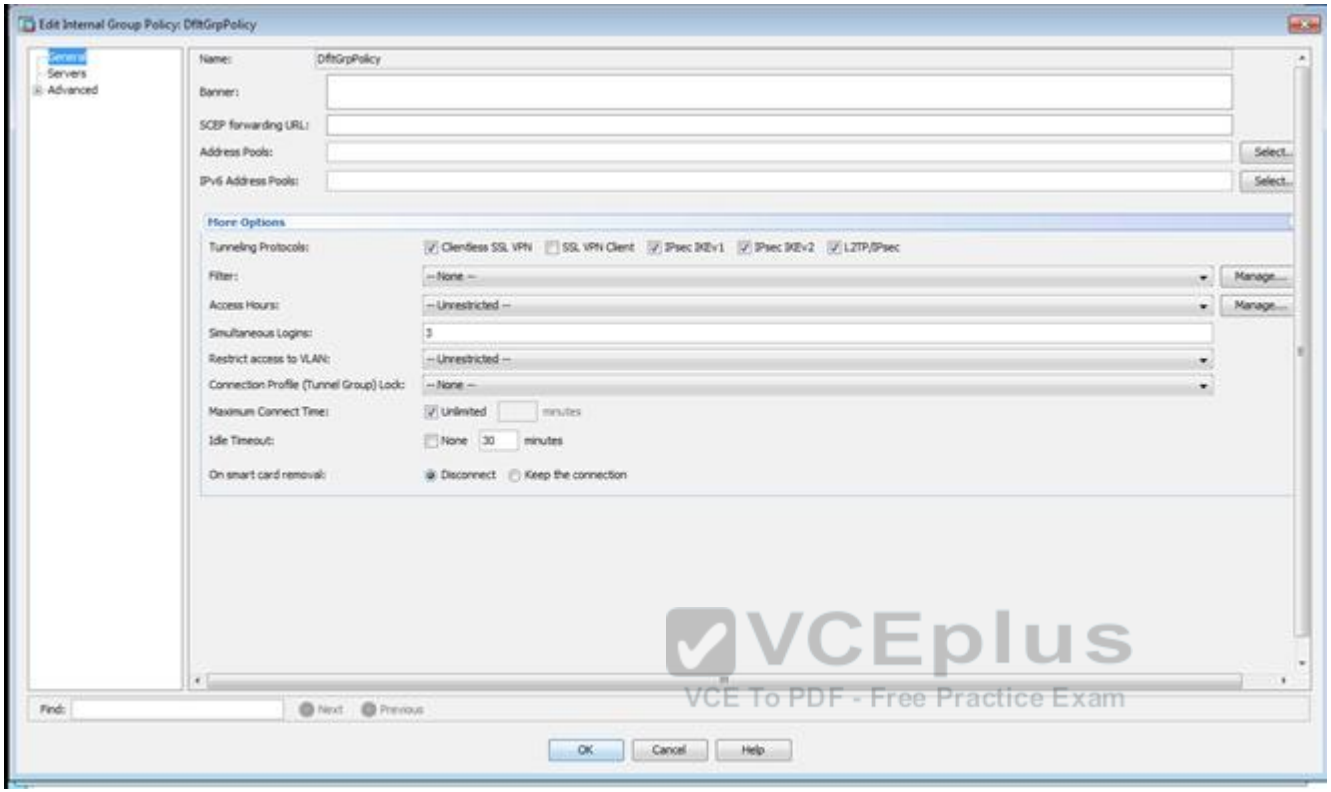


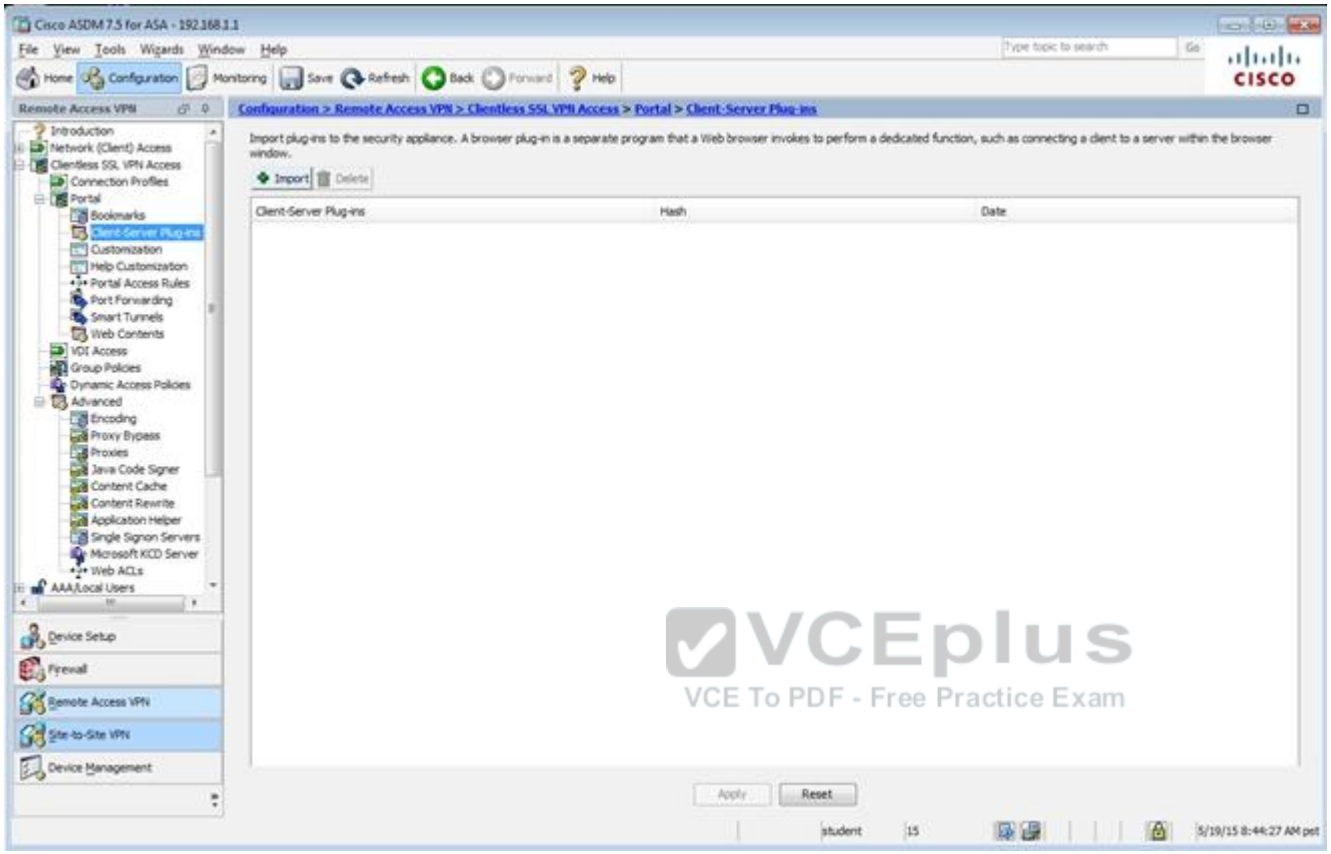


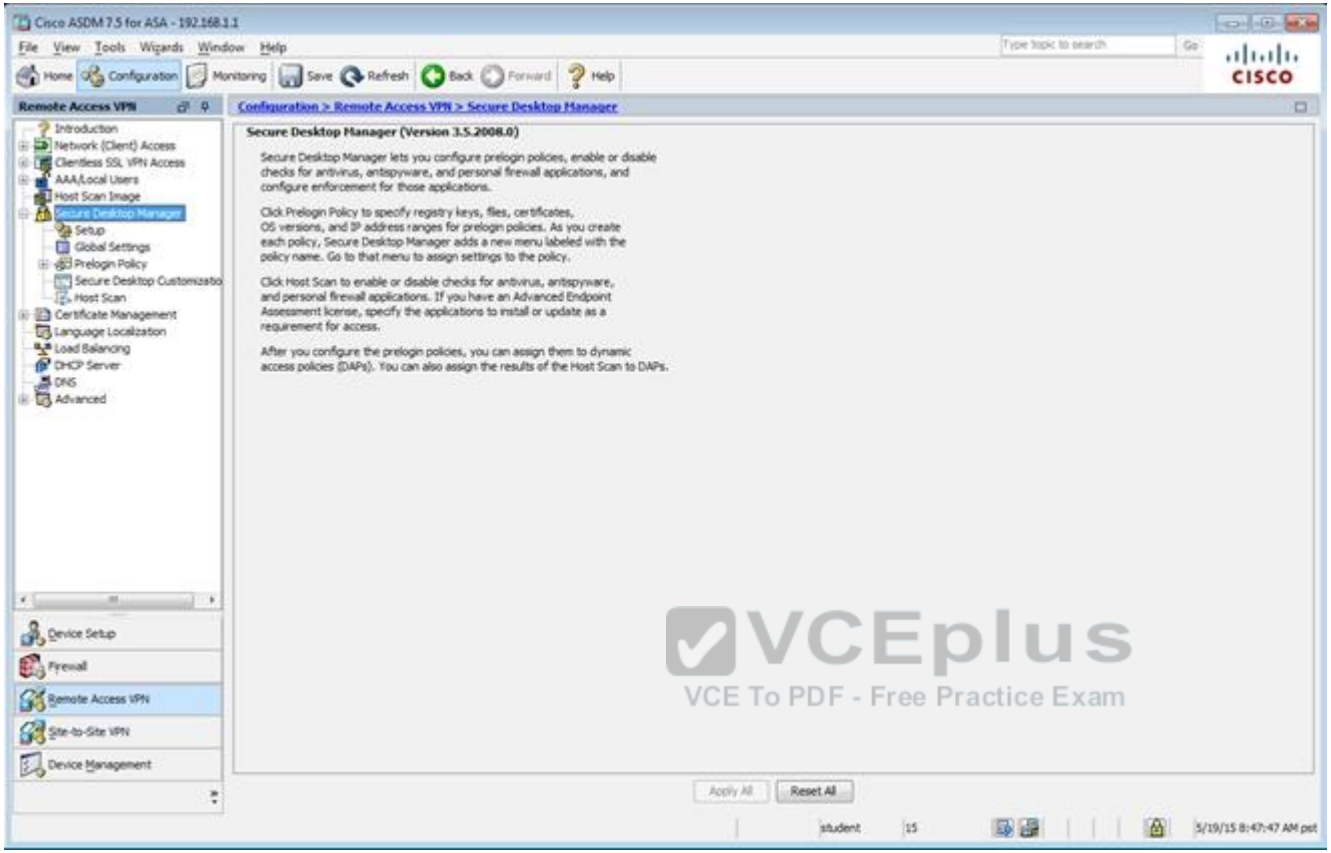


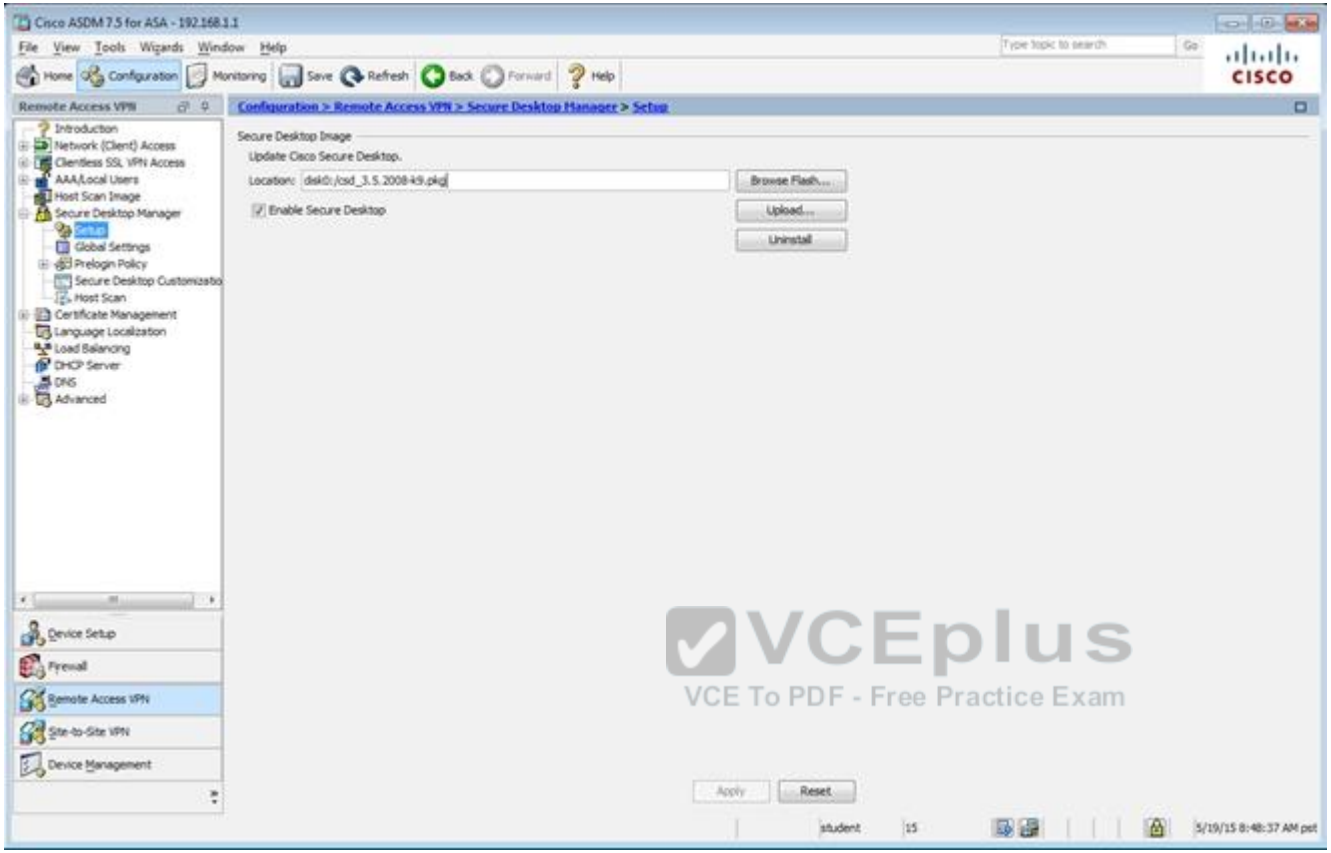


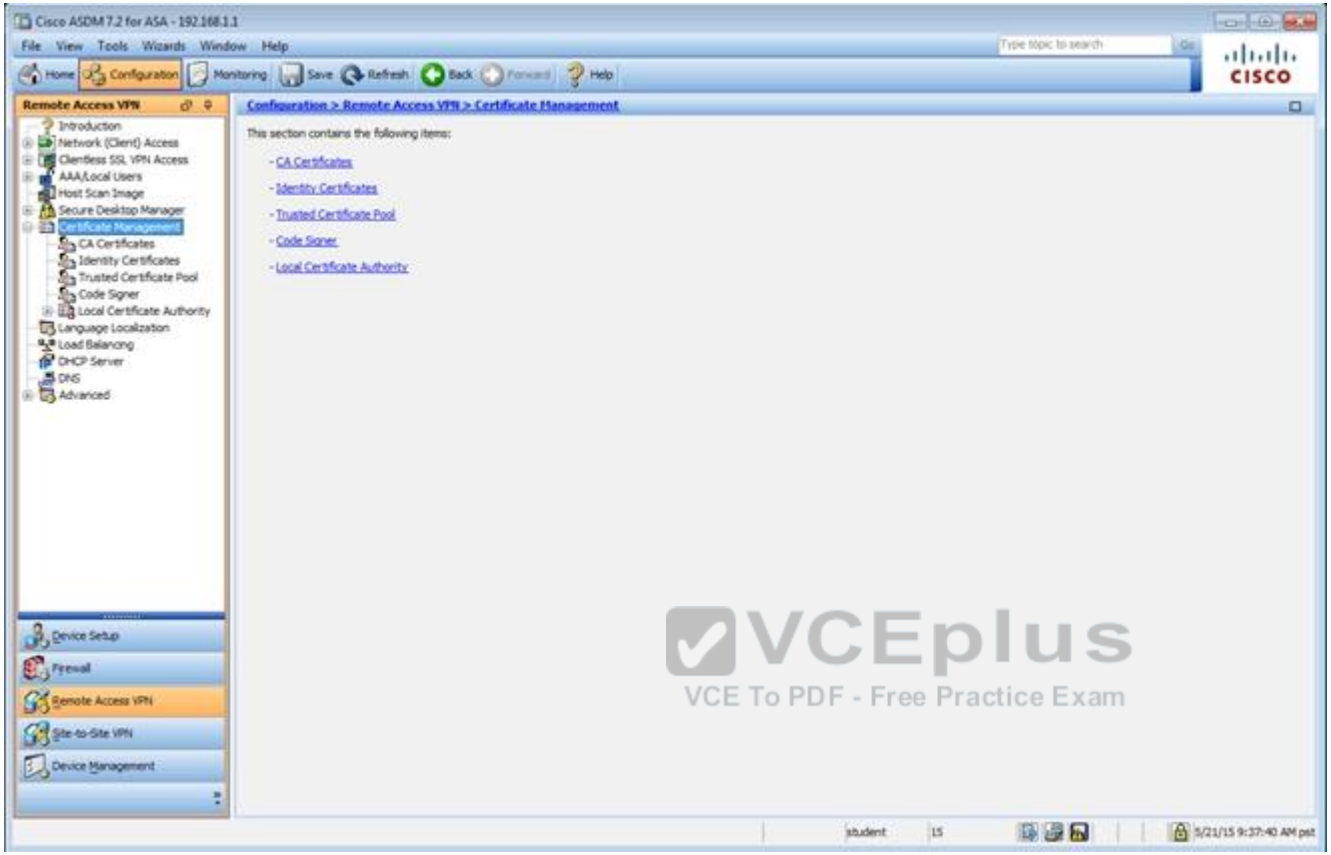


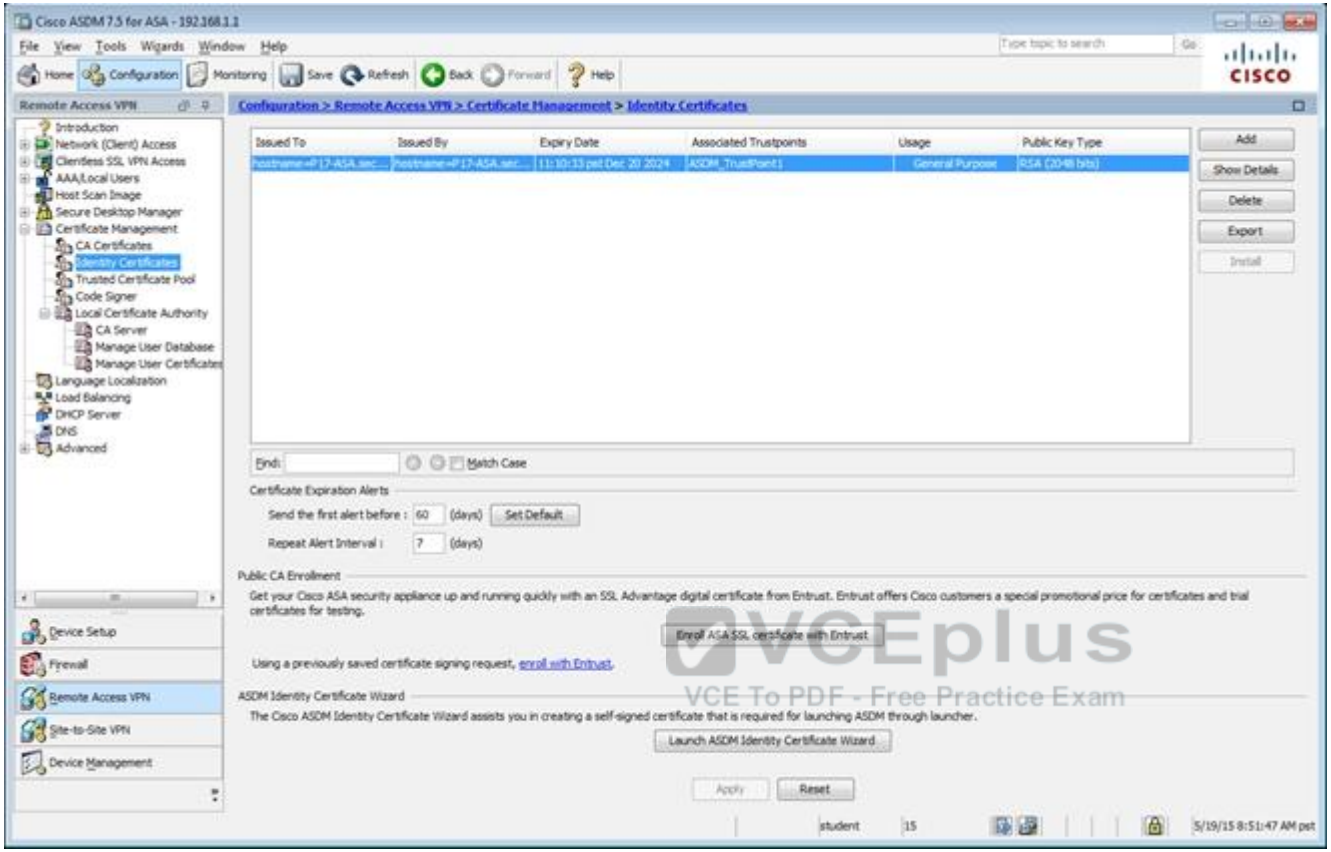


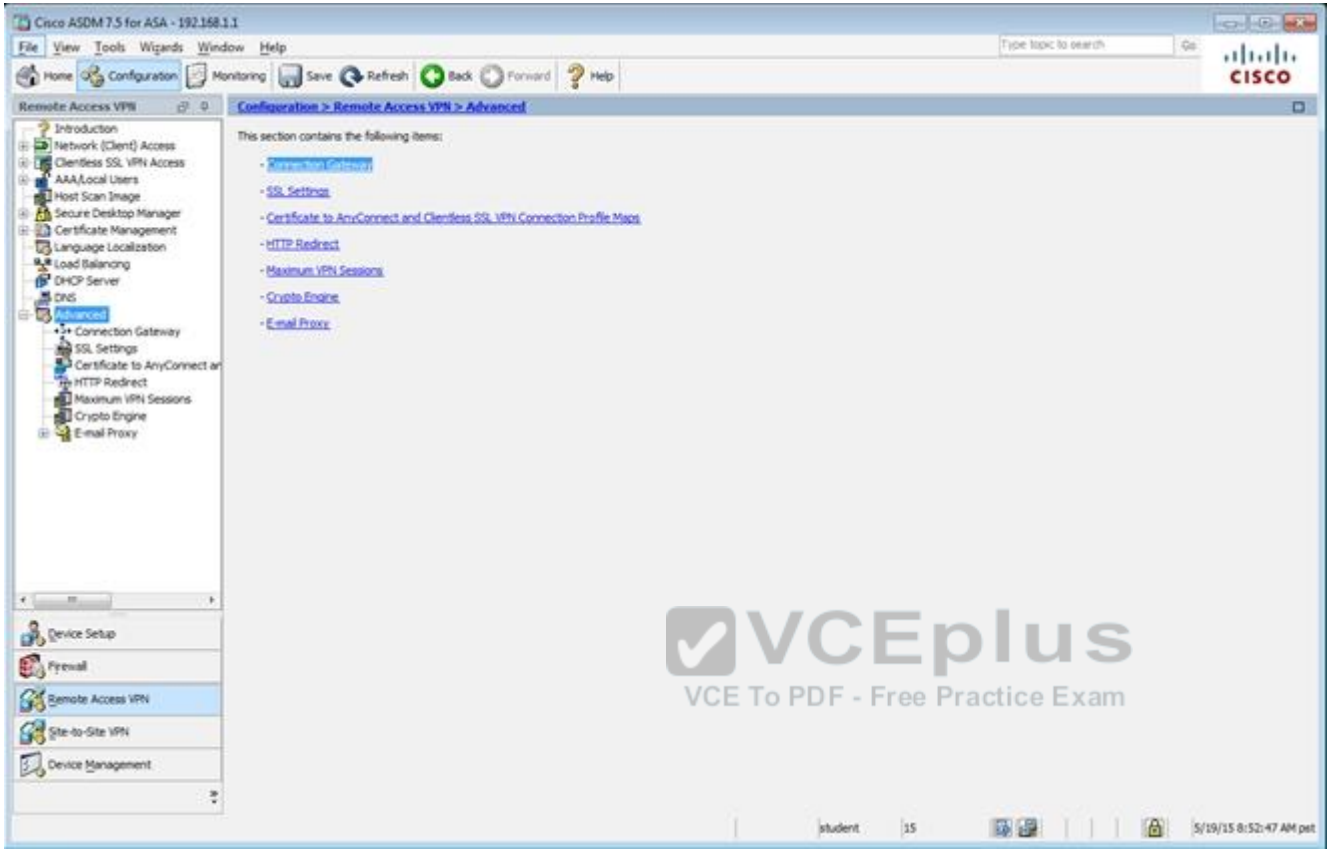


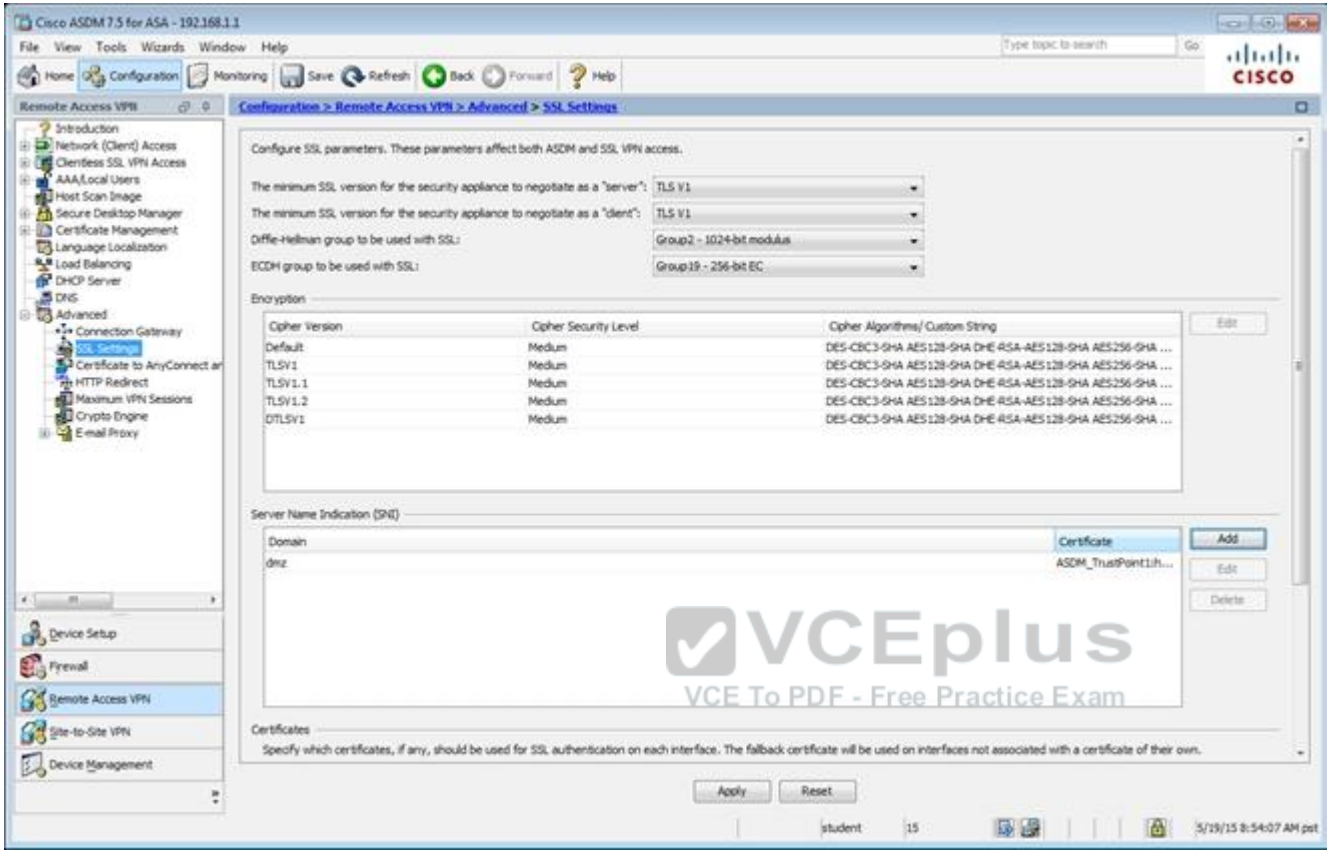


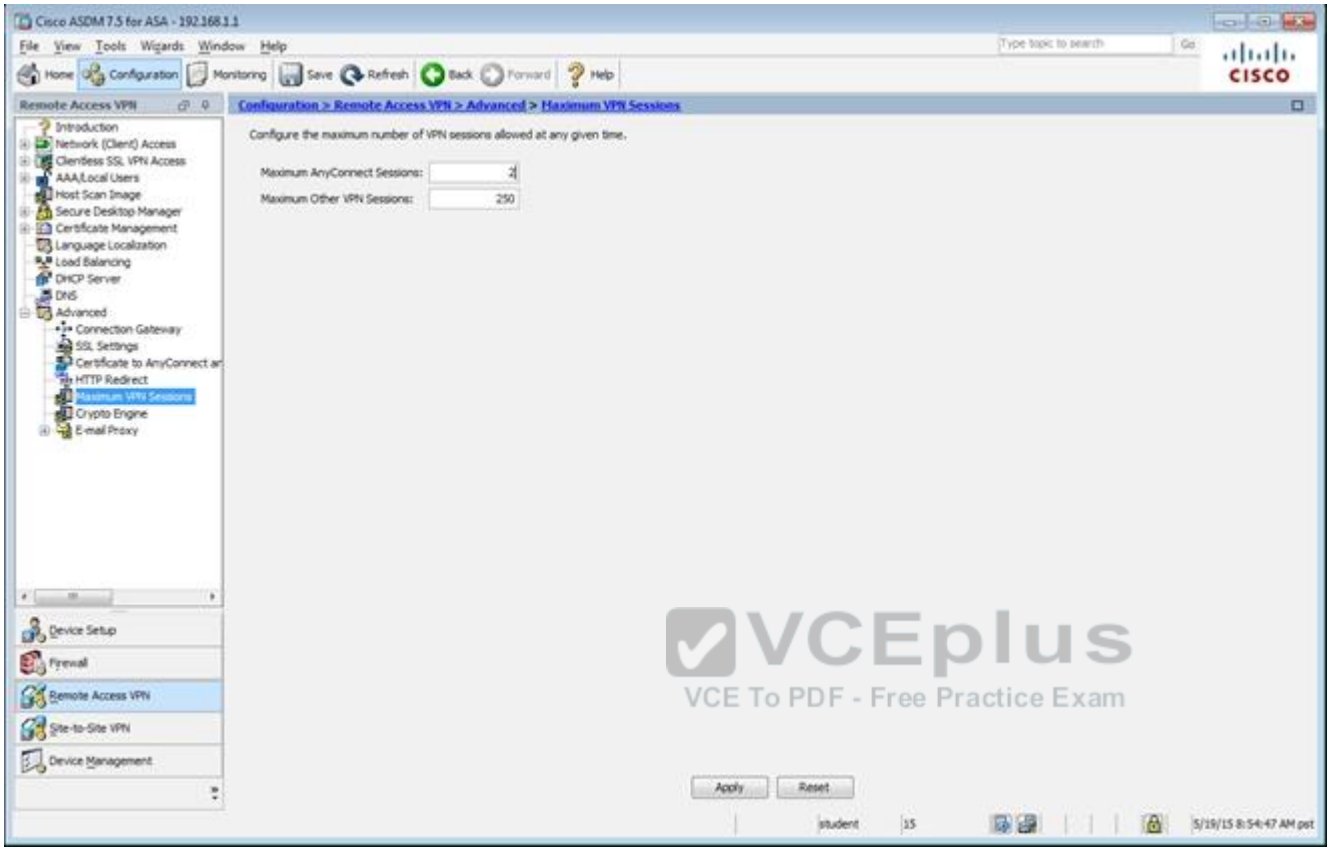


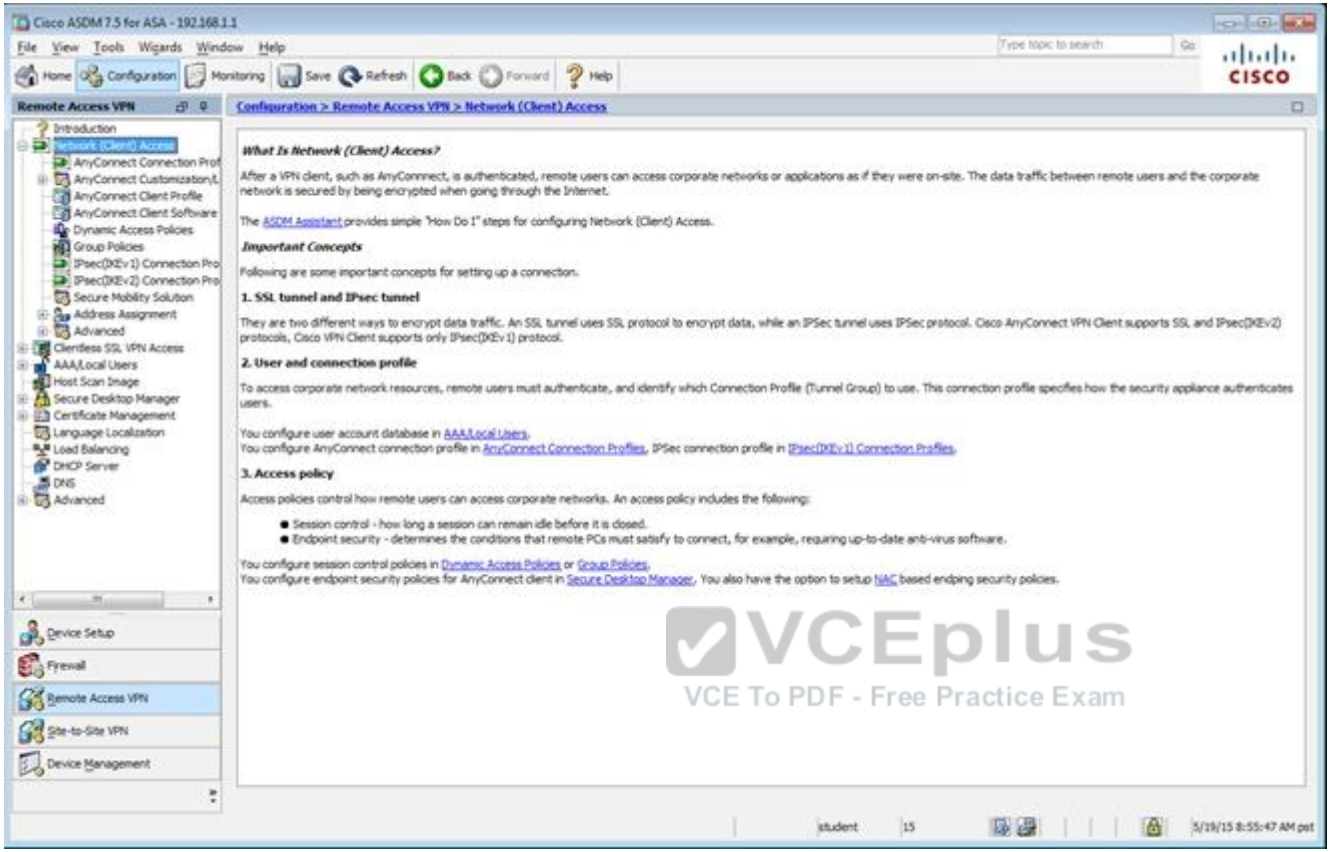


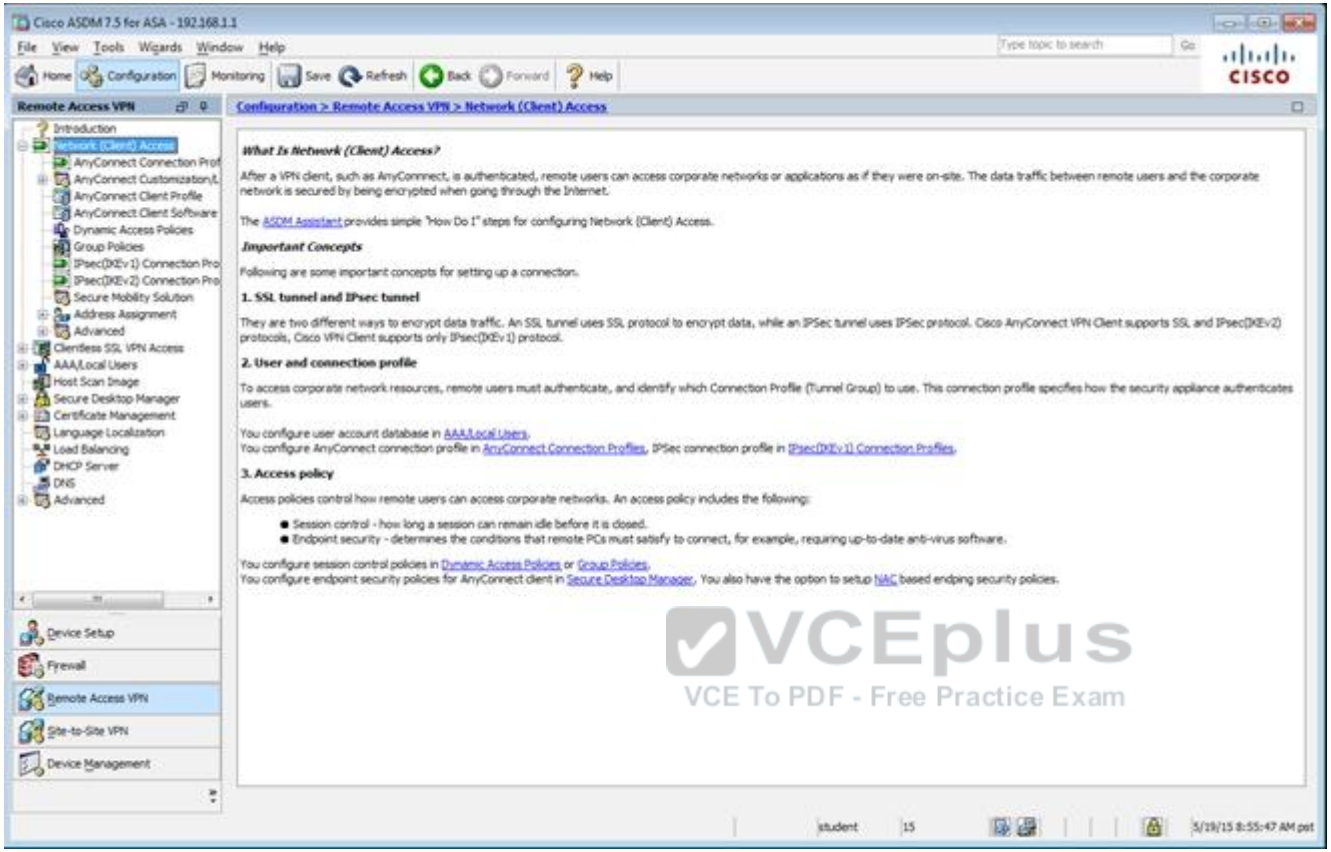


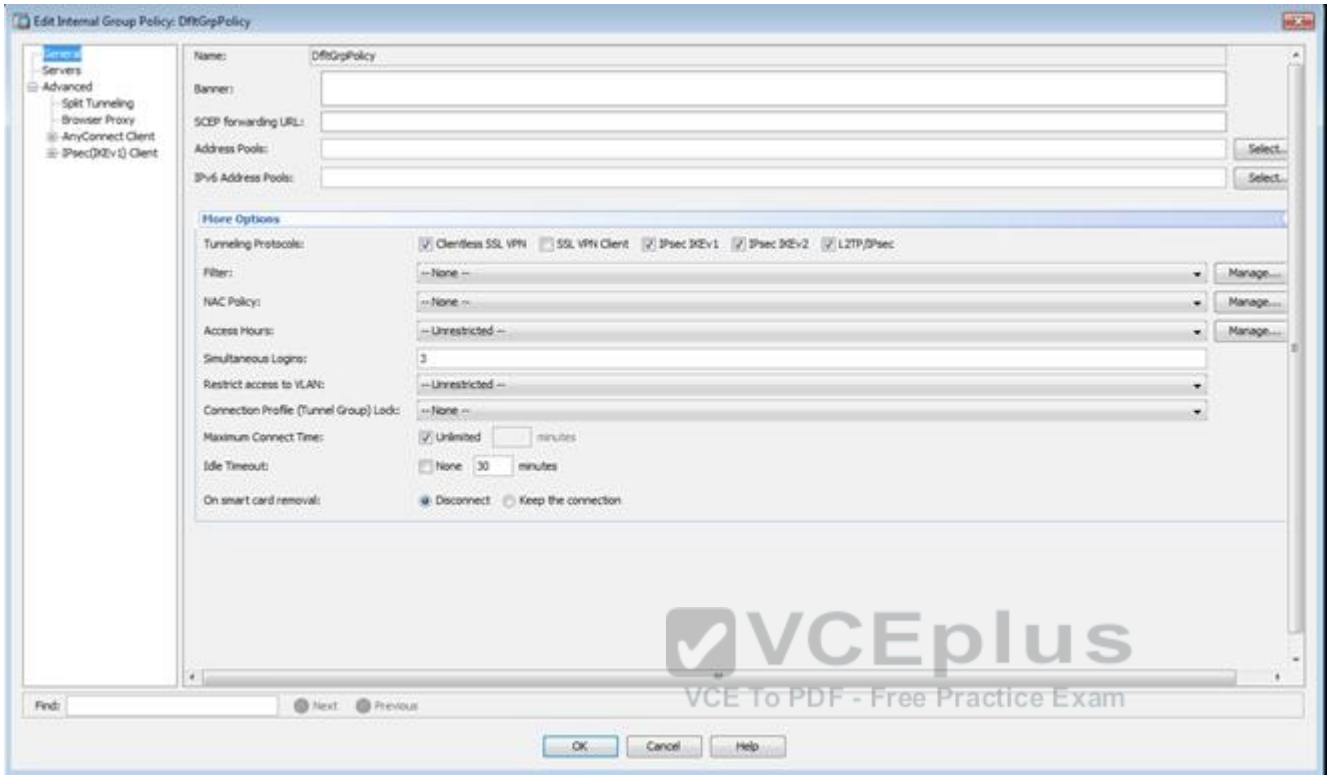


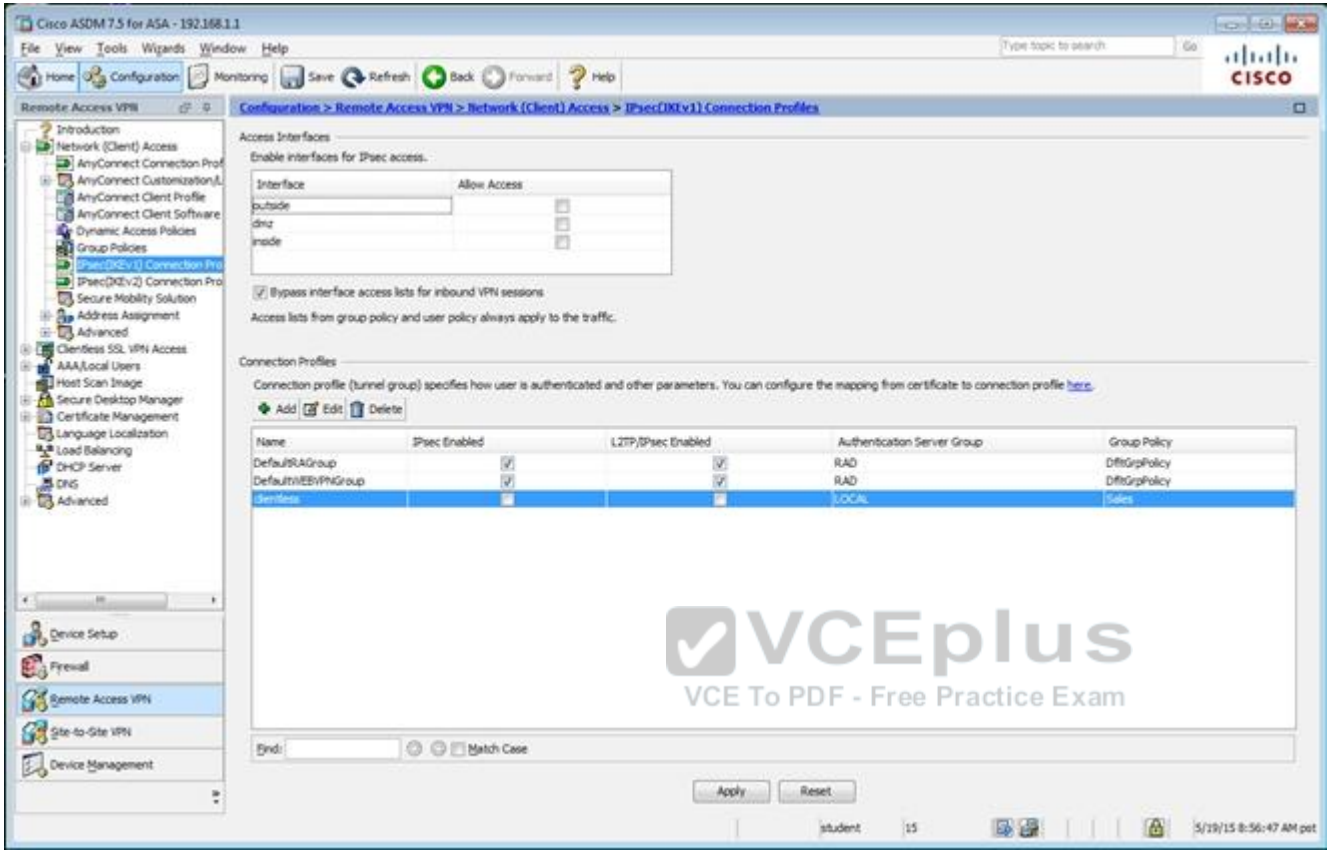


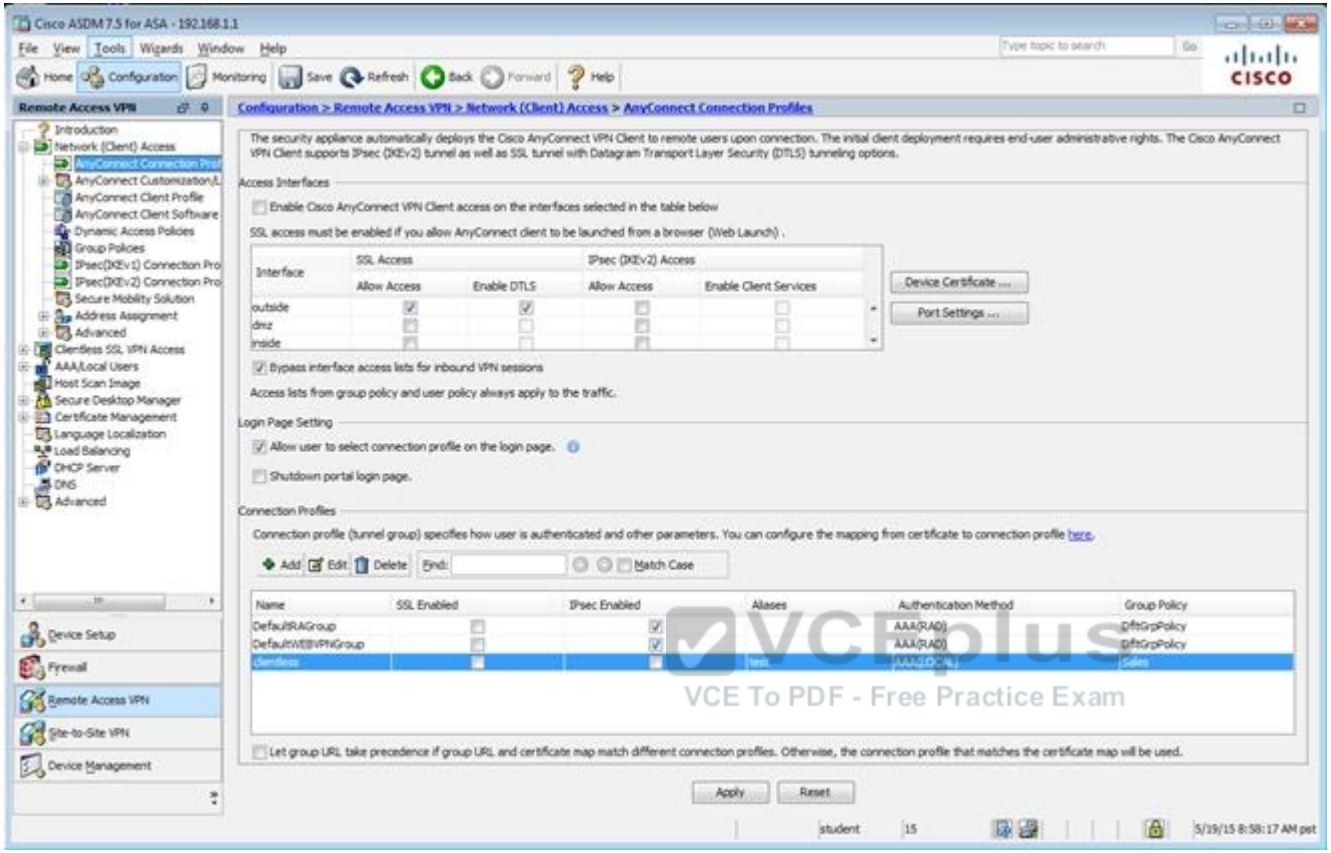


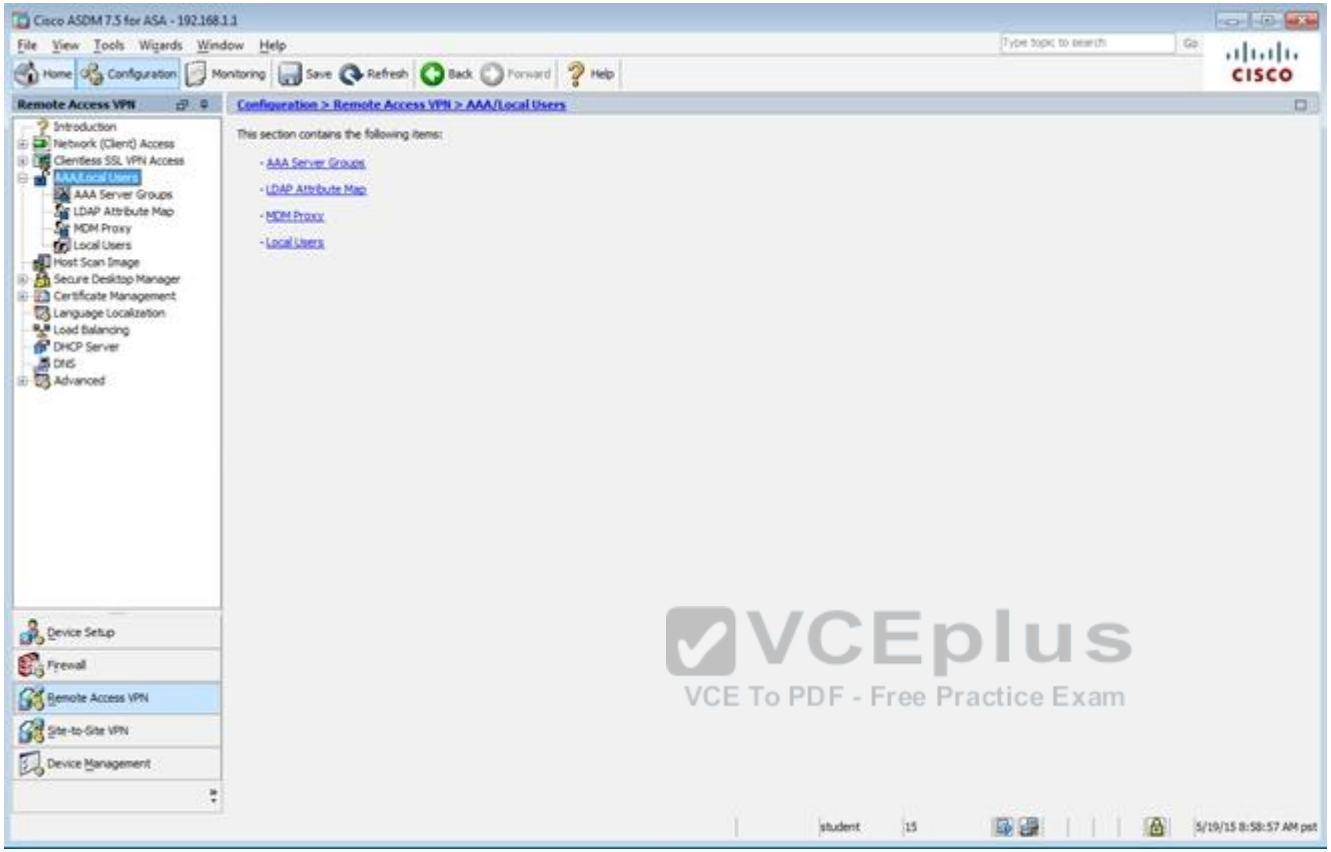


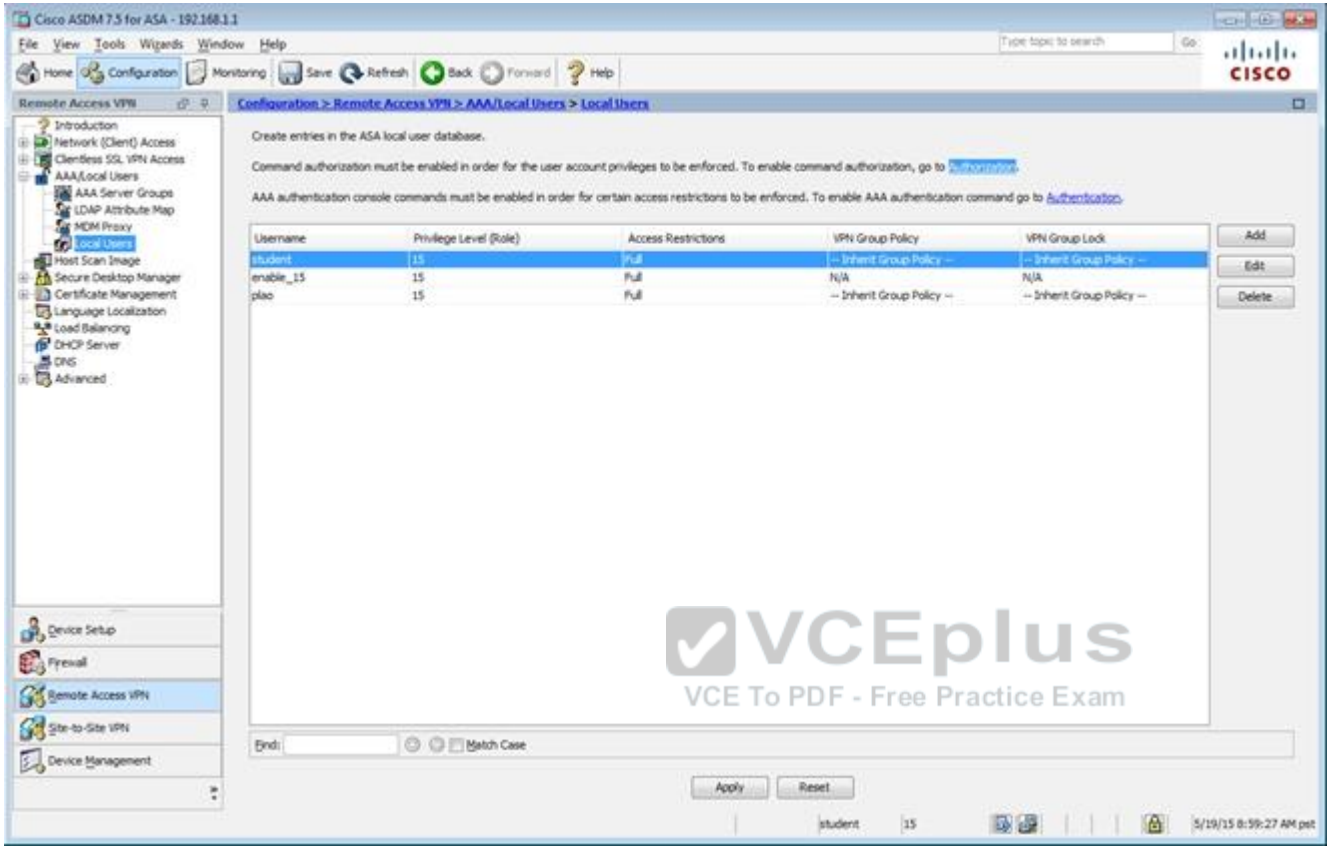


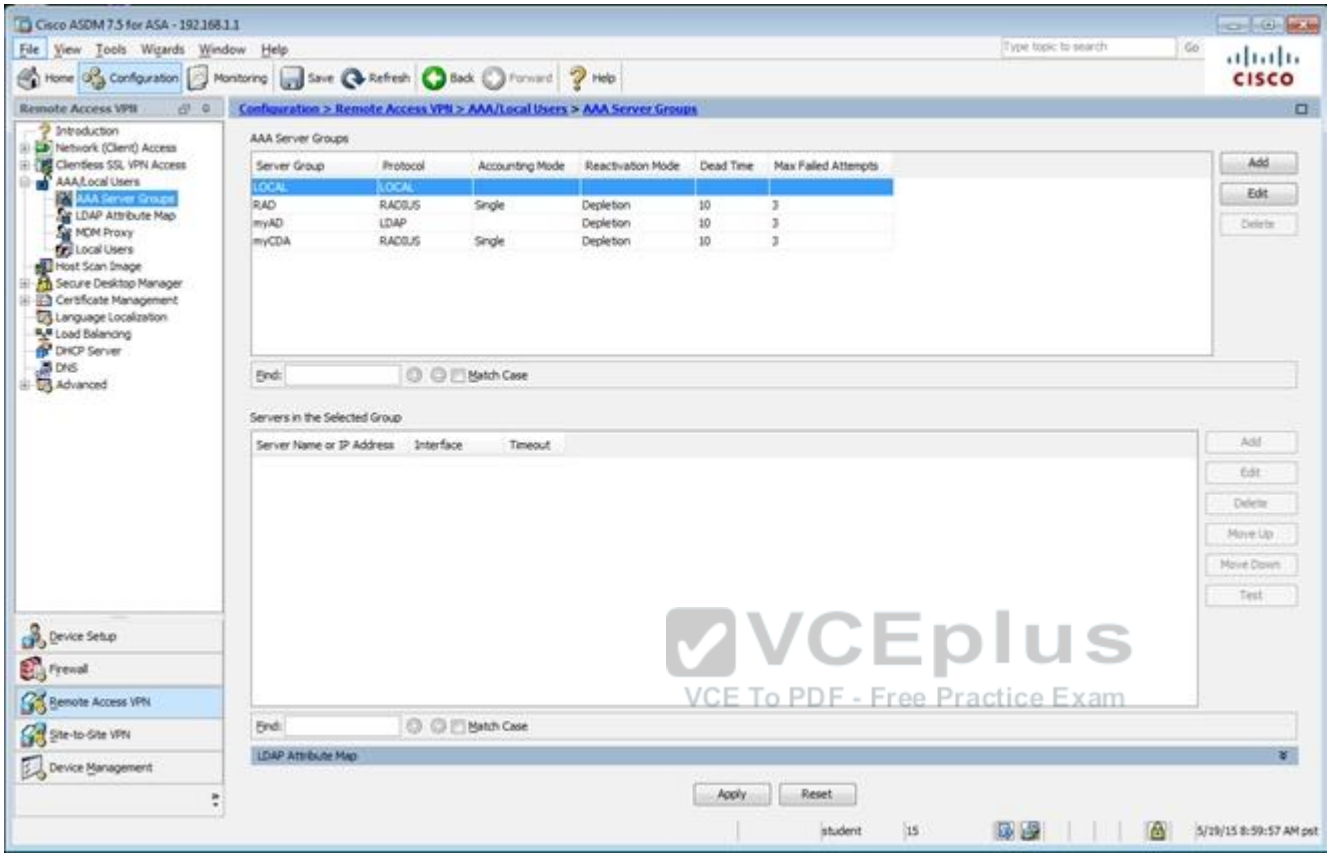












Correct Answer: Follow the explanation part to get answer on this sim question.
Section: (none)
Explanation

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

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

Configuration >

Add

#	Source Int	Match Crit	tion: Translated P
			rce
1	Any		ide (P)

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

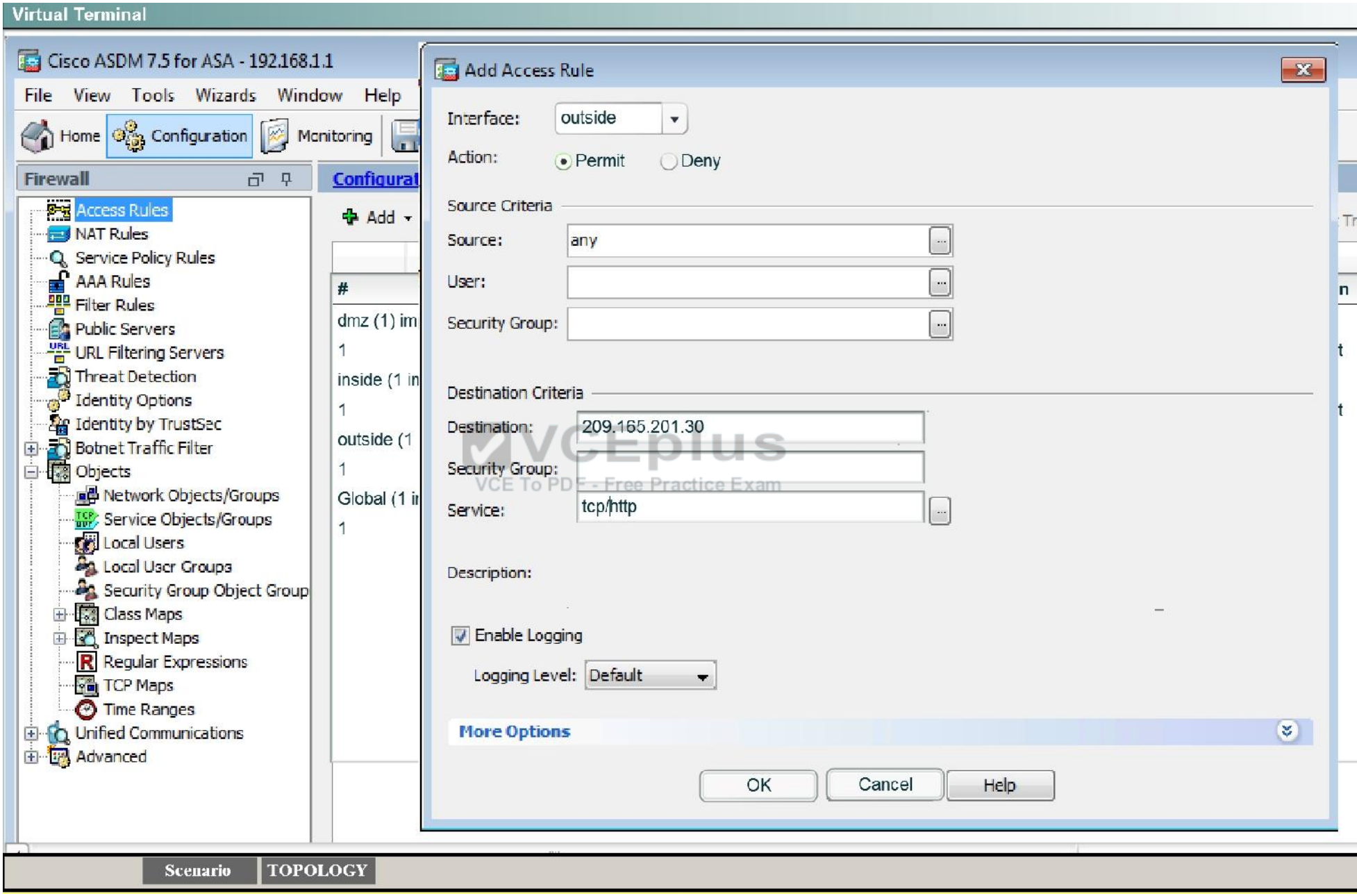
Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest 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 | Save | Refresh | Back | Forward | Help

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

Configuration > Firewall > Access Rules

Add | Edit | Delete | Where Used | Not Used | Diagram | Export | Clear Hits | Show Log | Packet Tra

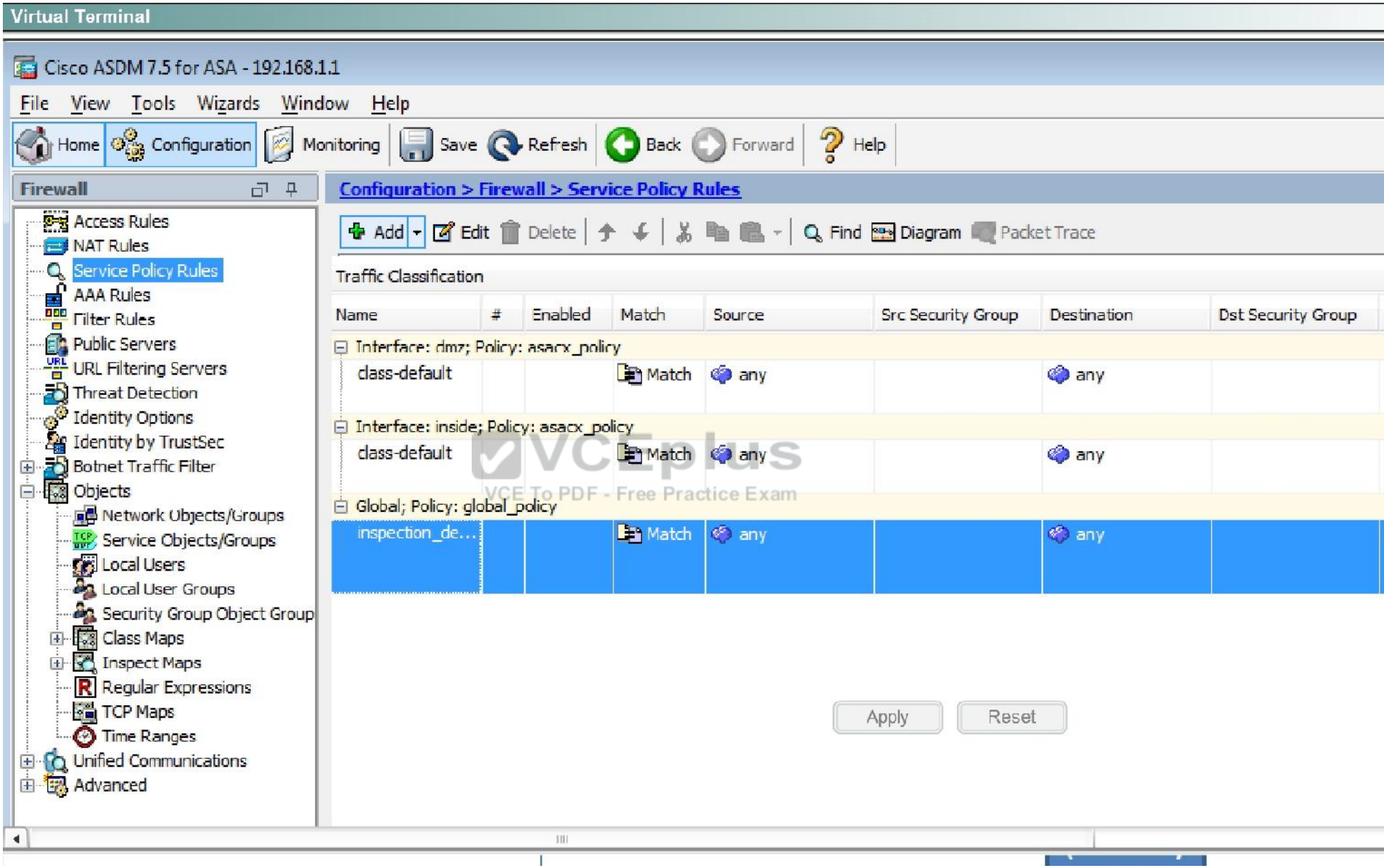
		Source Criteria:			Destination Criteria:			
#	Enabled	Source	User	Security Gr	Destination	Security Gr	Service	Action
dmz (1) implicity incomi								
1		any			Any less secure ne..		ip	Permit
inside (1 implicit incomi								
1		any			Any less secure ne..		ip	Permit
outside (1 incoming rule								
1	☑	any			209.165.201.30		tcp/http	Permit
Global (1 implict 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:



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

Configu

Add

Traffic Cla

Name

Interfa

class-c

Interfa

class-c

Global;

inspec

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

CTIQBE		
Cloud Web Security	Configure...	
DCERPC	Configure...	
DNS	Configure...	DNS Inspect Map: preset_dns_map
ESMTP	Configure...	
FTP	Configure...	
H.323 H.225	Configure...	
H.323 RAS	Configure...	
HTTP	Configure...	
ICMP		
ICMP Error		
ILS		
IM	Configure...	
IP-Options	Configure...	
IPSec-Pass-Thru	Configure...	
IPv6	Configure...	
MMP	Configure...	

Scenario TOPOLOGY

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 e144.dscb.akamaiedge.net [23.72.192.170] with 32 bytes of data: with 3
bytes of data:
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Ping statistics for 23.72.192.170:    Packets: Sent = 4,  Recieved = 4, Lost =
 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5s, Average = 4ms



C:\
```