

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

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



**210-260**

**Implementing Cisco Network Security**

**Version 4.0**



**Exam A****QUESTION 1**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

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

- A. TACACS uses TCP to communicate with the NAS.
- B. TACACS can encrypt the entire packet that is sent to the NAS.
- C. TACACS supports per-command authorization.

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

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 4**

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

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



**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 5**

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

- A. AES
- B. 3DES
- C. DES
- D. MD5
- E. DH-1024
- F. SHA-384

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 6**

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

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

**Correct Answer:** DEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 7**

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

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

**Correct Answer:** BF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

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

- A. They compare the 5-tuple of each incoming packet against configurable rules.
- B. They cannot track connections.

- C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
- D. Cisco IOS cannot implement them because the platform is stateful by nature.
- E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 11

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

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



**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 12

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

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

**Correct Answer:** ABC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

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

- A. to ensure that only authorized parties can modify data

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### **QUESTION 17**

Which type of secure connectivity does an extranet provide?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

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

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



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

What type of attack was the Stuxnet virus?

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 21**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

Refer to the exhibit.

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 23

Refer to the exhibit.

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

Which statement about the device time is true?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 24

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 25

Which statement about Cisco ACS authentication and authorization is true?

- A. ACS servers can be clustered to provide scalability.

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 26

Refer to the exhibit.

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



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

- A. The supplicant will fail to advance beyond the webauth method.
- B. The switch will cycle through the configured authentication methods indefinitely.
- C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
- D. The authentication attempt will time out and the switch will place the port into VLAN 101.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 27

Which EAP method uses Protected Access Credentials?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 28**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 29**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

Refer to the exhibit.

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



What is the effect of the given command sequence?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

Refer to the exhibit.

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

What is the effect of the given command sequence?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

Refer to the exhibit.

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

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

- A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
- B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
- C. IPSec Phase 1 is down due to a QM\_IDLE state.
- D. IPSec Phase 2 is down due to a QM\_IDLE state.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

Refer to the exhibit.

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

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

Refer to the exhibit.

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autoccommand 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 autoccommand 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**

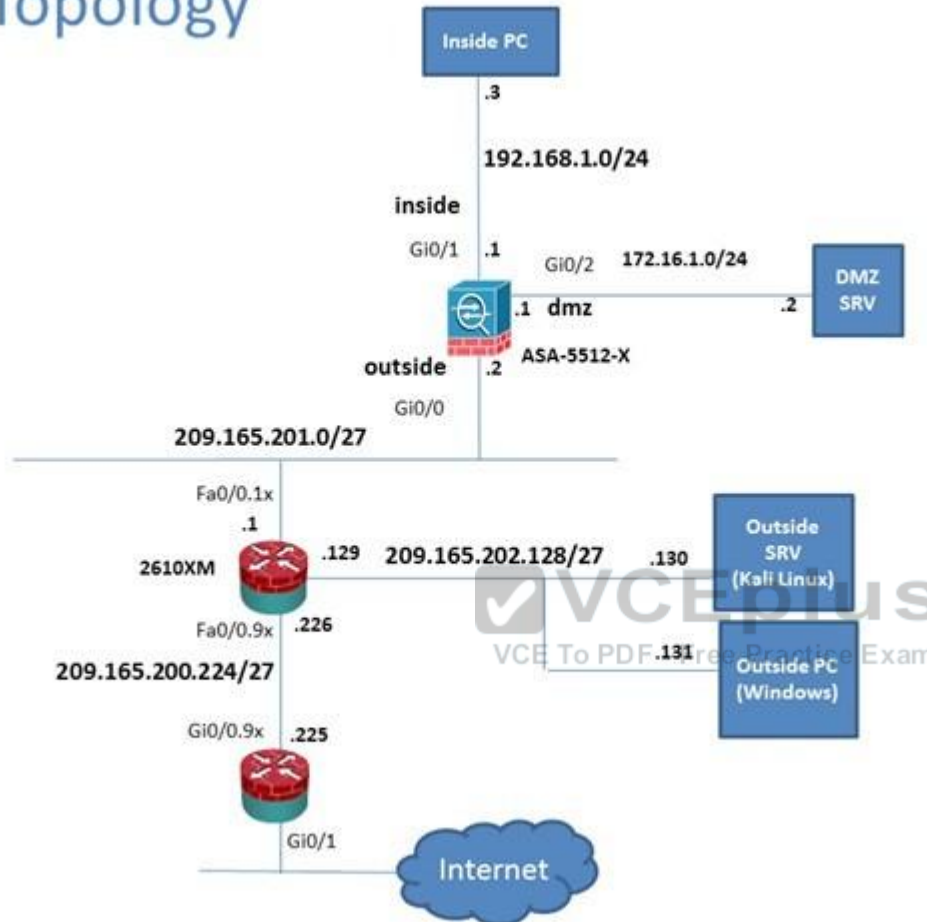
Scenario

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



Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA PrePOWER Status

### Device Information

General License

Host Name: **P17-ASA-secure-x-local**  
 ASA Version: **86.84(6)13**  
 ASDM Version: **7.5(1)1**  
 Firewall Mode: **Routed**  
 Environment Status: **OK**

Device Uptime: **11d 28h 42m 47s**  
 Device Type: **ASA 5512**  
 Context Mode: **Single**  
 Total Flash: **4096 MB**

### Interface Status

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

Select an interface to view input and output Kbps

### VPN Sessions

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

### System Resources Status

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

Memory Usage (MB)

### Failover Status

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

### Traffic Status

Connections Per Second Usage

outside Interface Traffic Usage (Kbps)

### Latest ASDM Syslog Messages

| Severity | Date        | Time     | Syslog ID | Source IP     | Source | Destination IP | Destination | Description  |
|----------|-------------|----------|-----------|---------------|--------|----------------|-------------|--|
| 6        | May 13 2015 | 12:35:09 | 302016    | 10.81.254.202 | 123    | 209.165.201.2  | 65535       | Teardown UDP connection 15136325 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96    |
| 6        | May 13 2015 | 12:35:08 | 106015    | 192.168.1.3   | 14676  | 192.168.1.1    | 443         | Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside                             |
| 6        | May 13 2015 | 12:35:08 | 302014    | 192.168.1.3   | 14676  | 192.168.1.1    | 443         | Teardown TCP connection 15136328 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset=0 |

student 15 5/13/15 12:35:18 PM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

None Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address    | MAC Address     | Proxy Arp |
|-----------|---------------|-----------------|-----------|
| outside   | 209.165.201.1 | 000c.30.14.3820 | No        |
| inside    | 192.168.1.4   | 0050.56.33.3333 | No        |
| inside    | 192.168.1.3   | 0050.56.11.1111 | No        |
| inside    | 192.168.1.2   | 0050.56.22.2222 | No        |
| inside    | 192.168.1.26  | 0050.5692.3c7b  | No        |
| inside    | 192.168.1.55  | 0006.86e4.98f3  | No        |
| dmz       | 172.16.1.2    | 0050.5644.4444  | No        |
| mgmt      | 10.30.10.1    | 000c.30.14.3820 | No        |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

student 15 3/18/15 9:32:27 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

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

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Monitoring > VPN > VPN Statistics > Sessions

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

Filter By: Clientless SSL VPN All Sessions Filter

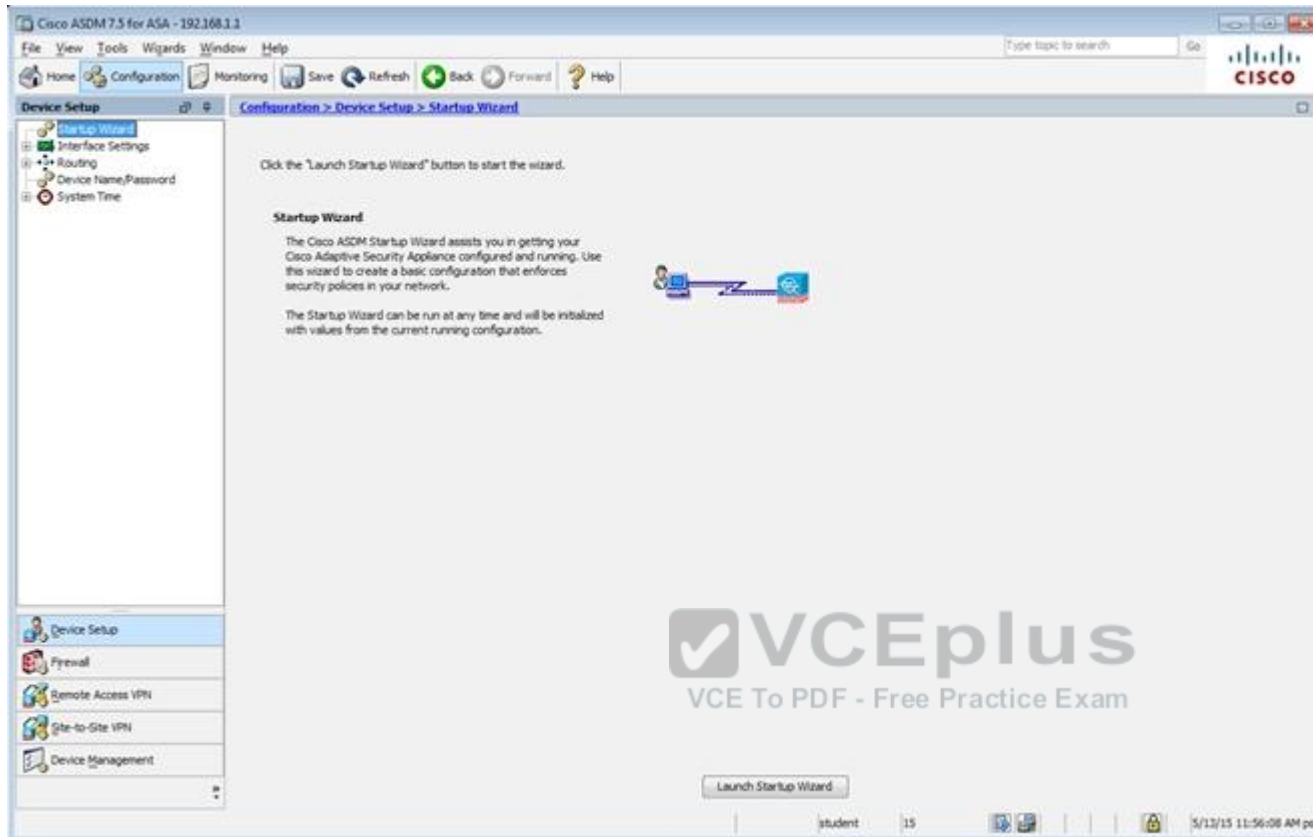
| Username | IP Address      | Group Policy | Connection Profile | Protocol   | Encryption | Login Time                    | Duration   | Bytes Tx | Bytes Rx |
|----------|-----------------|--------------|--------------------|------------|------------|-------------------------------|------------|----------|----------|
| student  | 209.165.202.131 | Sales        | Clientless         | Clientless | (1)RC4     | 08:05:46 (pt Thu May 21 2015) | 0h:09m:19s | 316774   | 41633    |

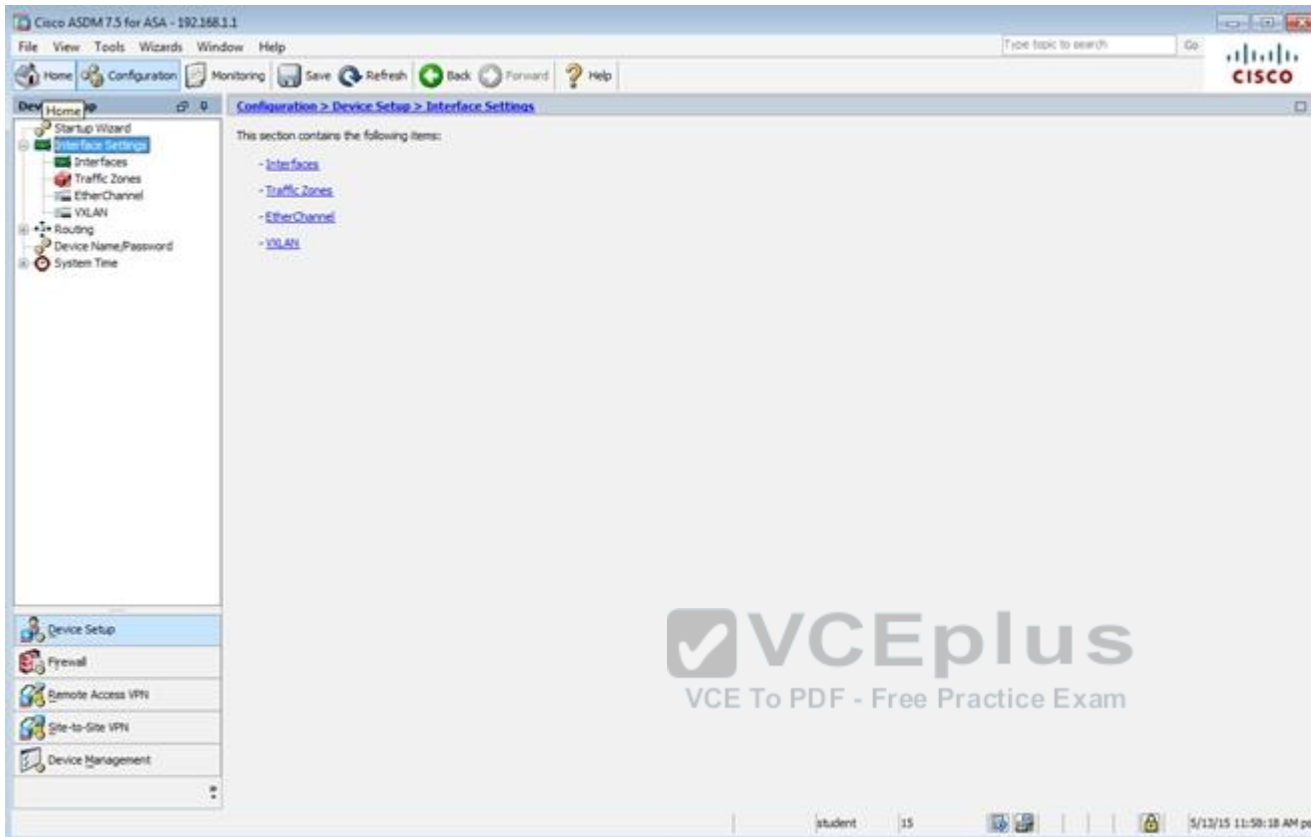
Details Logout Ping

Refresh

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

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

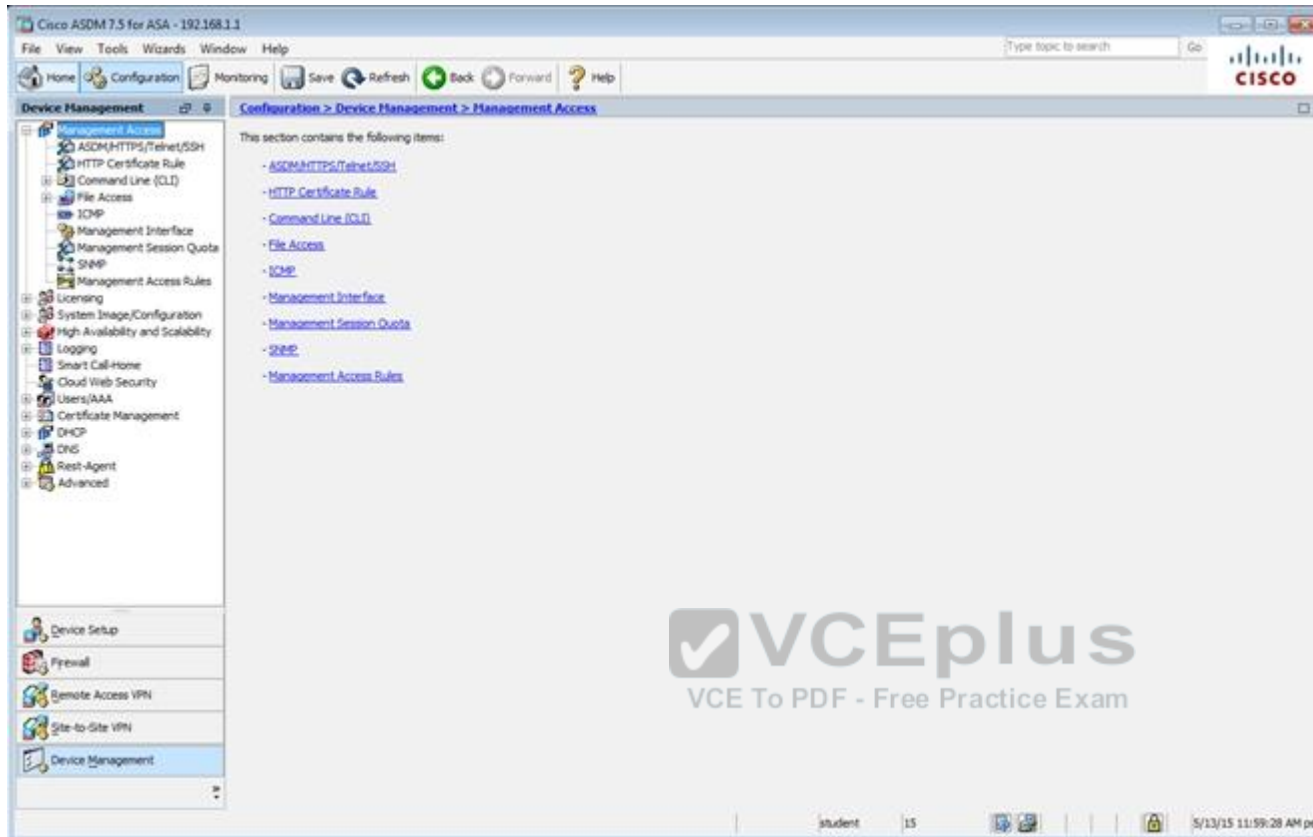
Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interface Settings > Interfaces

| Interface          | Name    | Zone | Route Map | State   | Security Level | IP Address      | Subnet Mask Prefix Length | Group | Type     |
|--------------------|---------|------|-----------|---------|----------------|-----------------|---------------------------|-------|----------|
| GigabitEthernet0/0 | outside |      |           | Enabled |                | 0/209.165.202.2 | 255.255.255.0             |       | Hardware |
| GigabitEthernet0/1 | inside  |      |           | Enabled | 100            | 192.168.1.1     | 255.255.255.0             |       | Hardware |
| GigabitEthernet0/2 | dmz     |      |           | Enabled |                | 172.16.1.1      | 255.255.255.0             |       | Hardware |
| GigabitEthernet0/3 |         |      |           | Enabled |                |                 |                           |       | Hardware |
| GigabitEthernet0/4 |         |      |           | Enabled |                |                 |                           |       | Hardware |
| GigabitEthernet0/5 | mgmt    |      |           | Enabled | 100            | 10.10.10.2      | 255.255.255.0             |       | Hardware |
| Management0/0      |         |      |           | Enabled |                |                 |                           |       | Hardware |

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

student 15 5/13/15 12:42:48 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

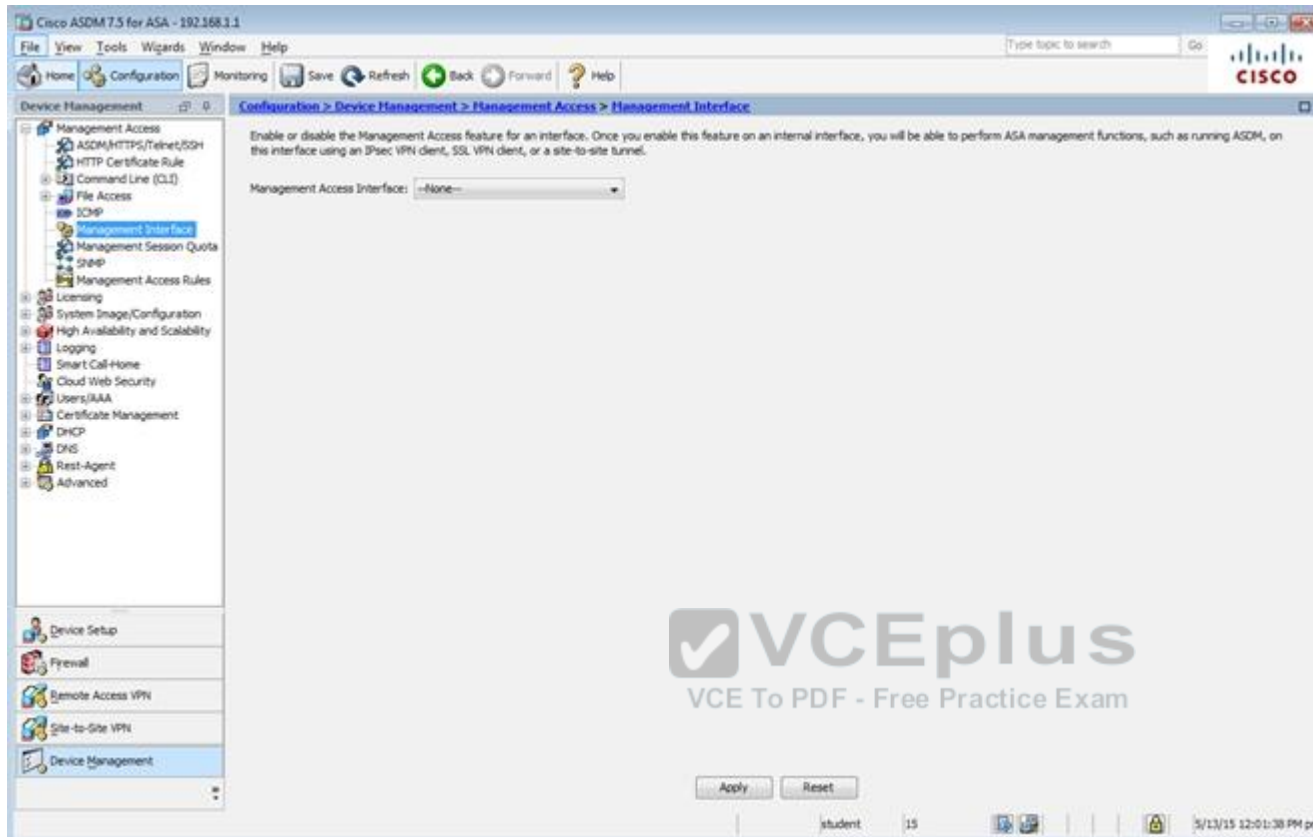
Allowed SSH Version(s): 1 & 2

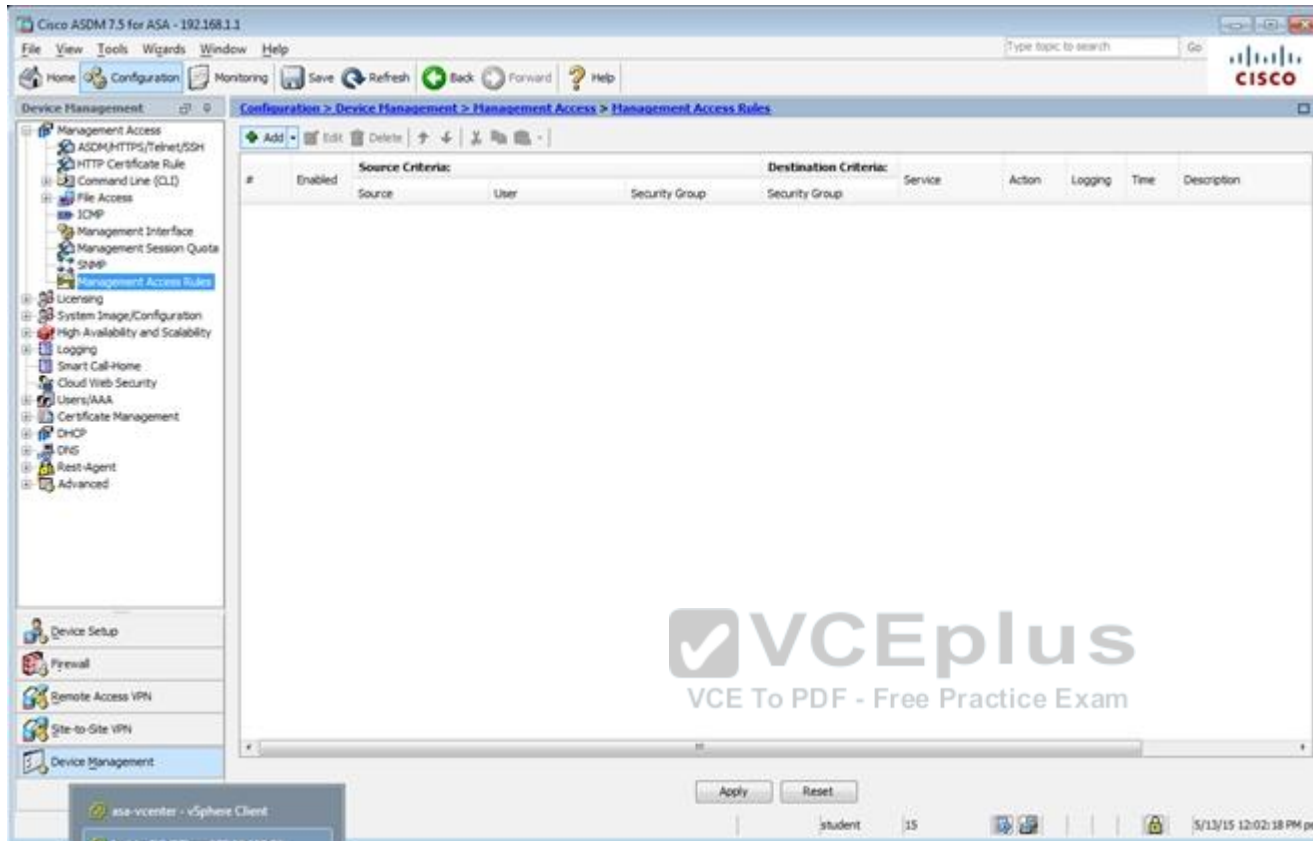
SSH Timeout: 5 minutes

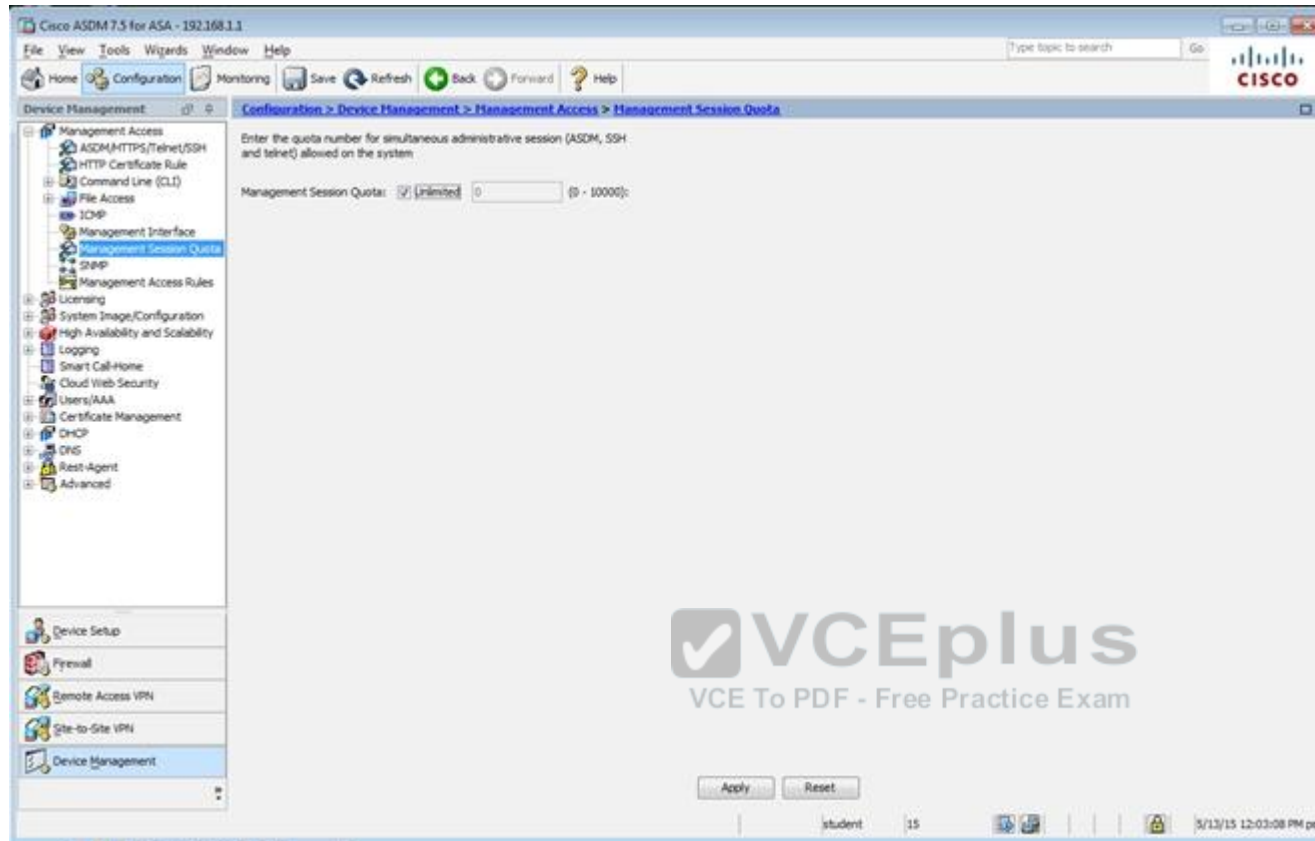
DH Key Exchange: ☒ Group 1 ☐ Group 14

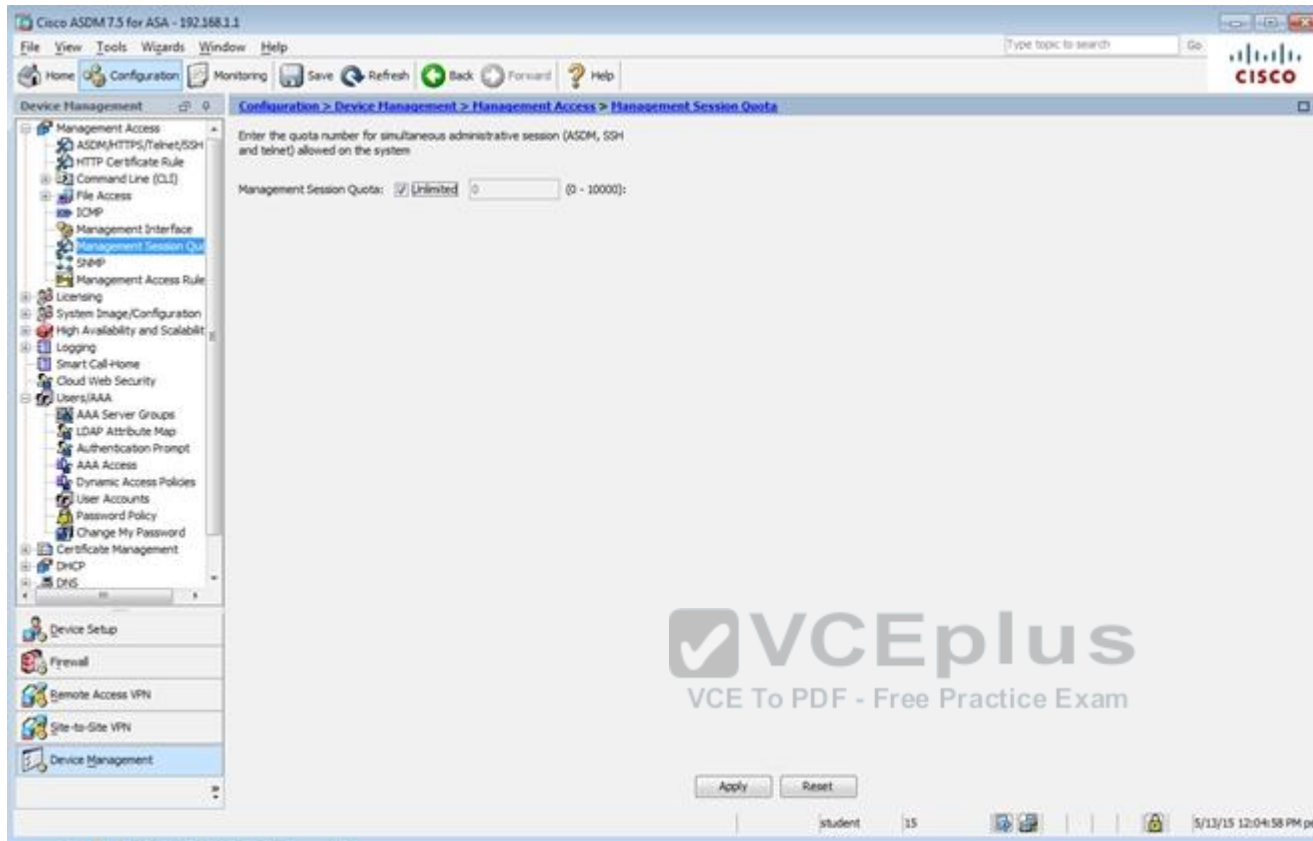
Apply Reset

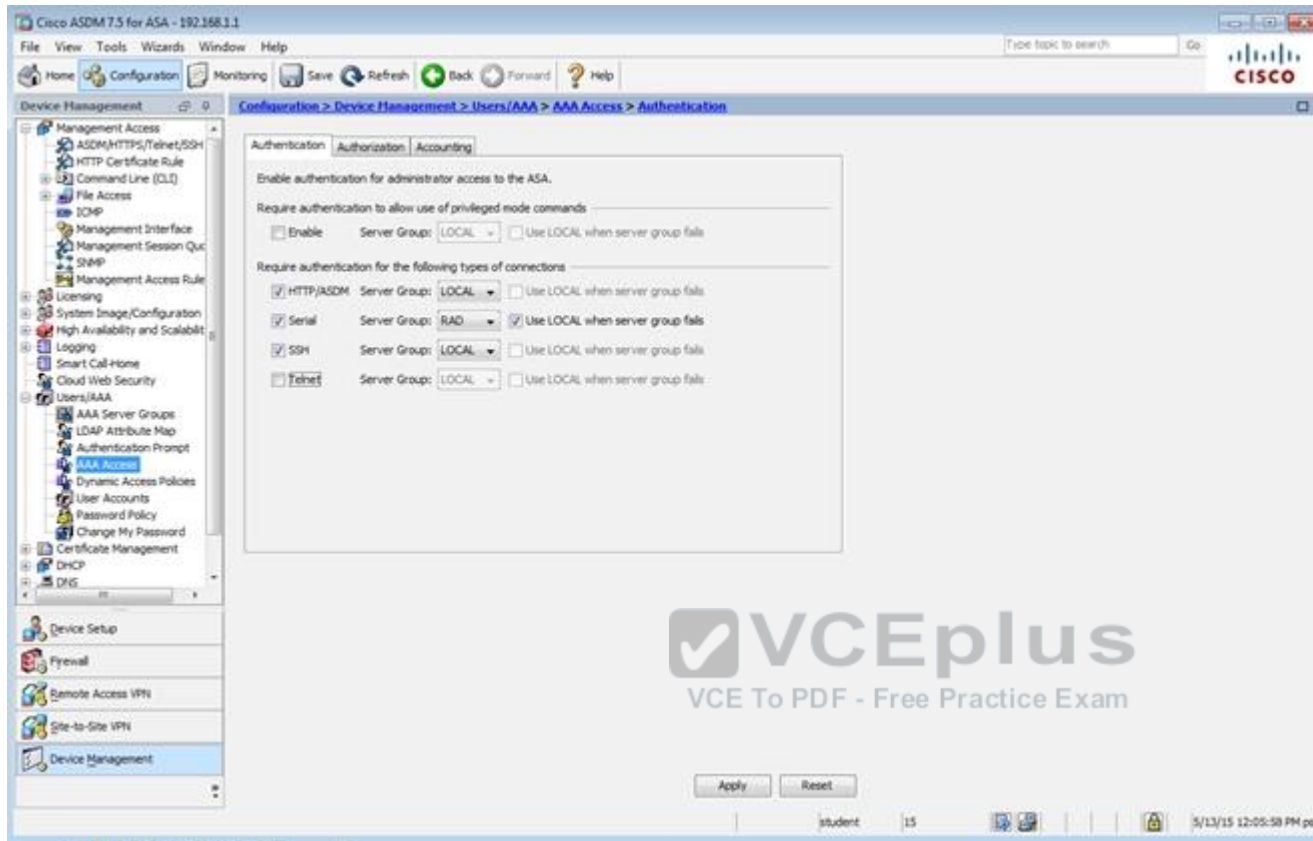
student 15 5/13/15 12:00:38 PM pst

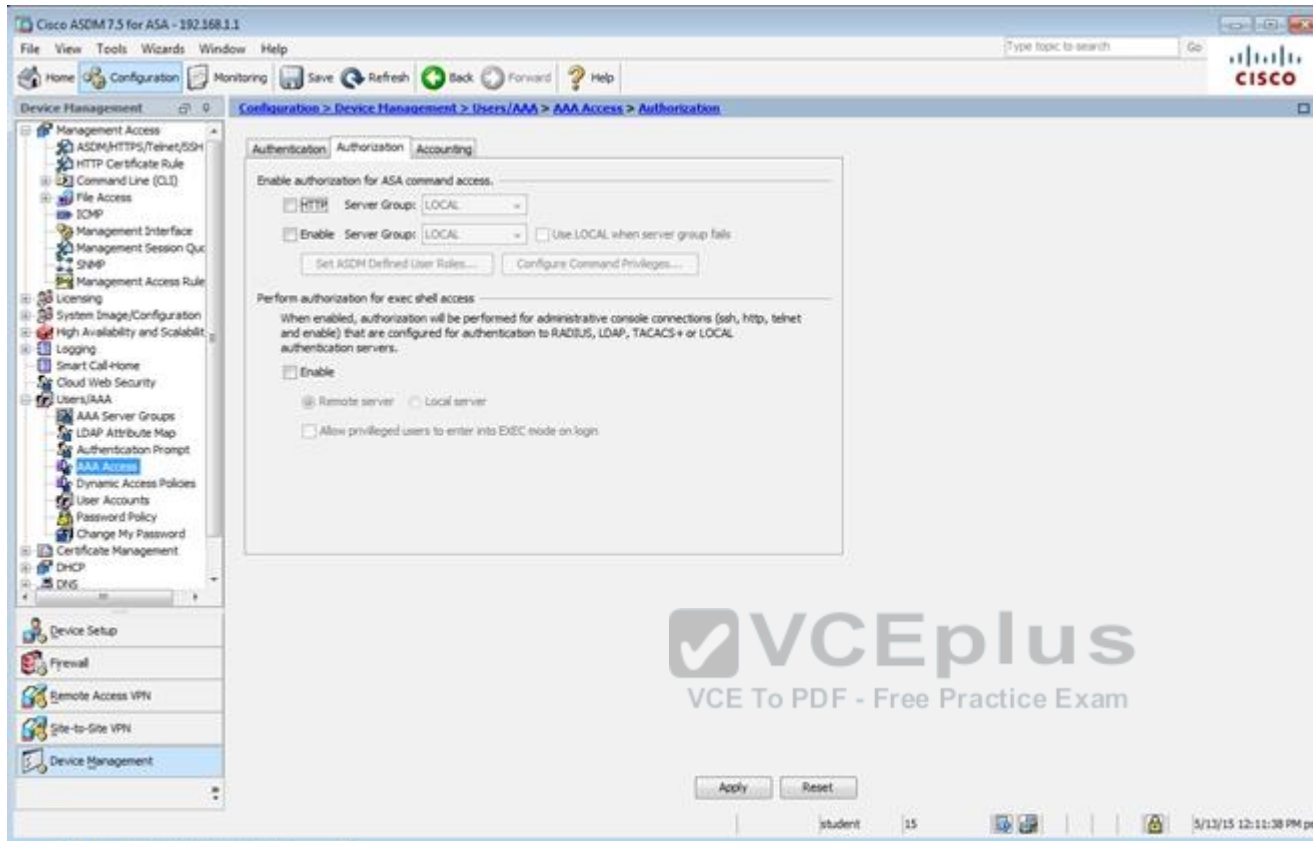


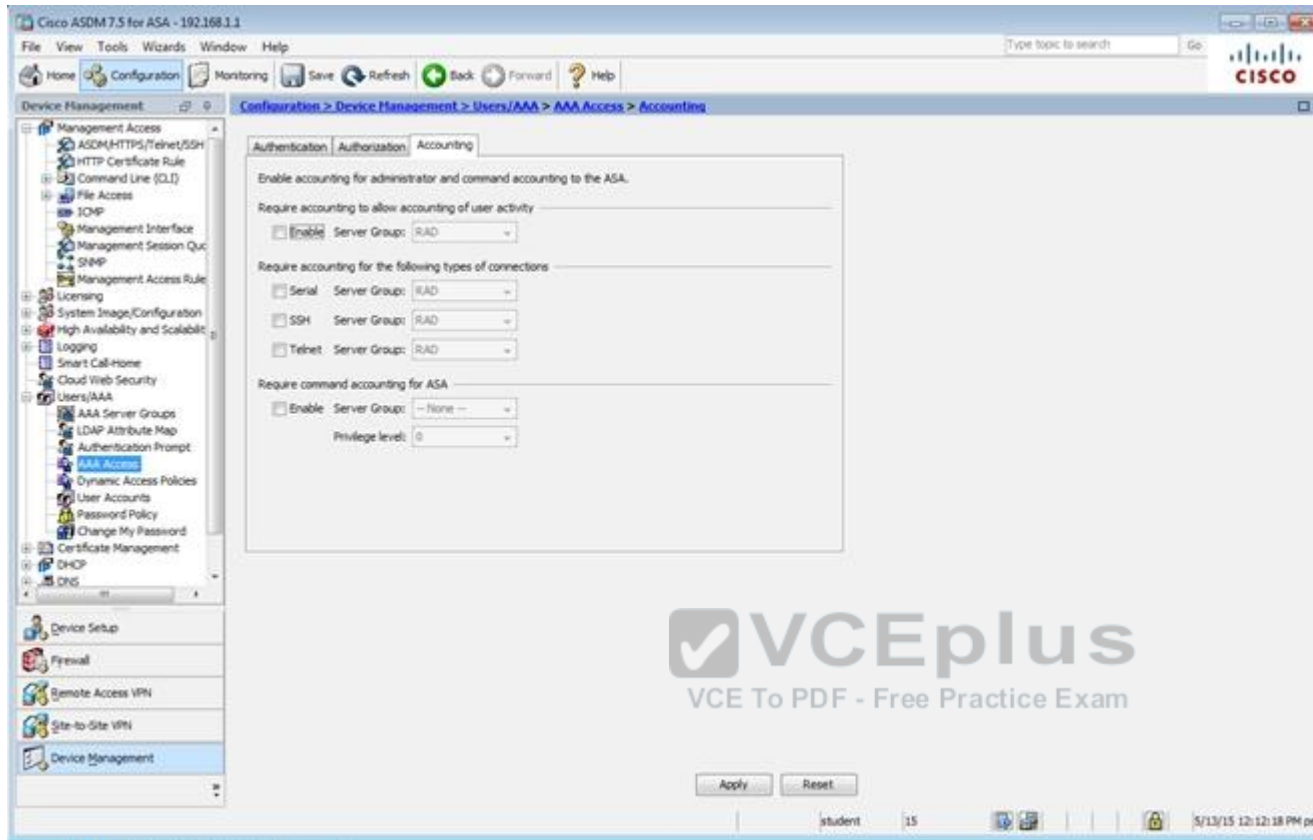


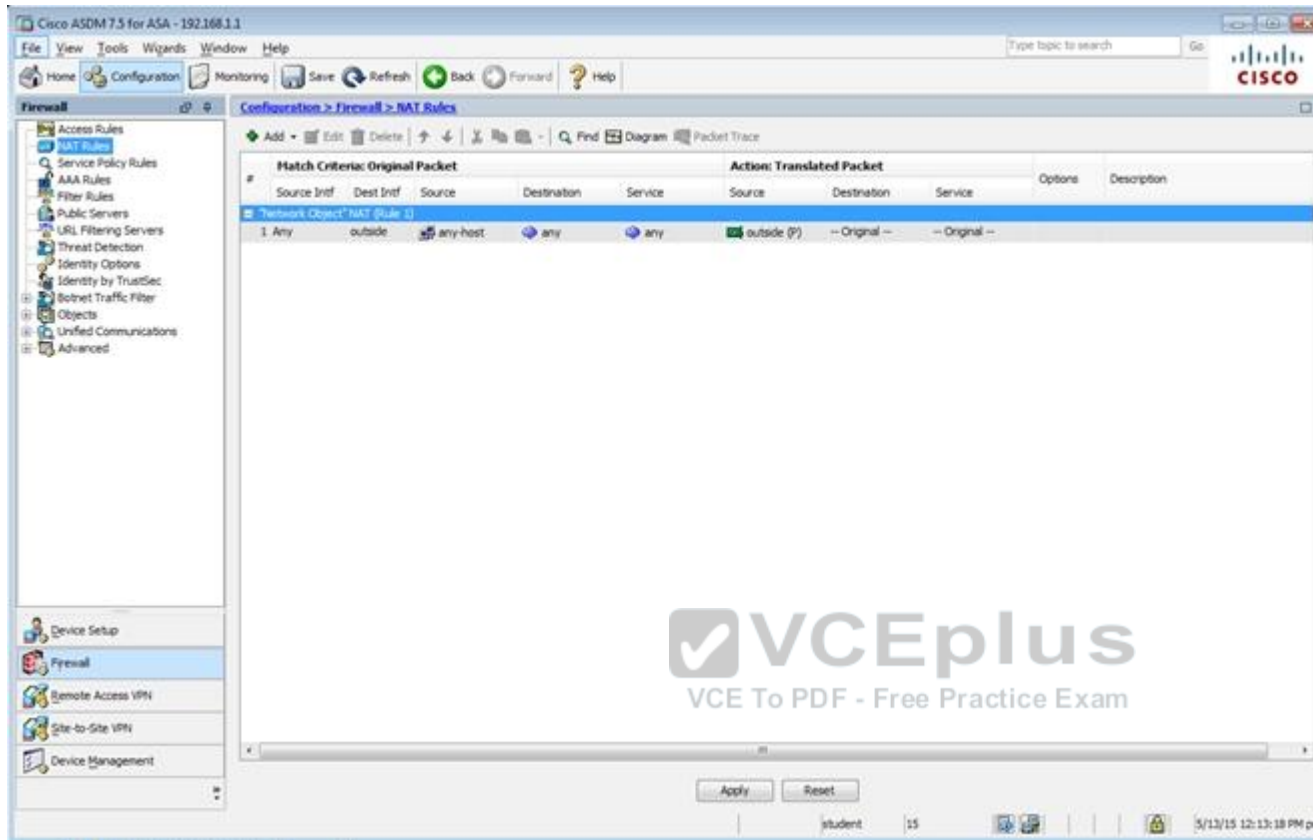


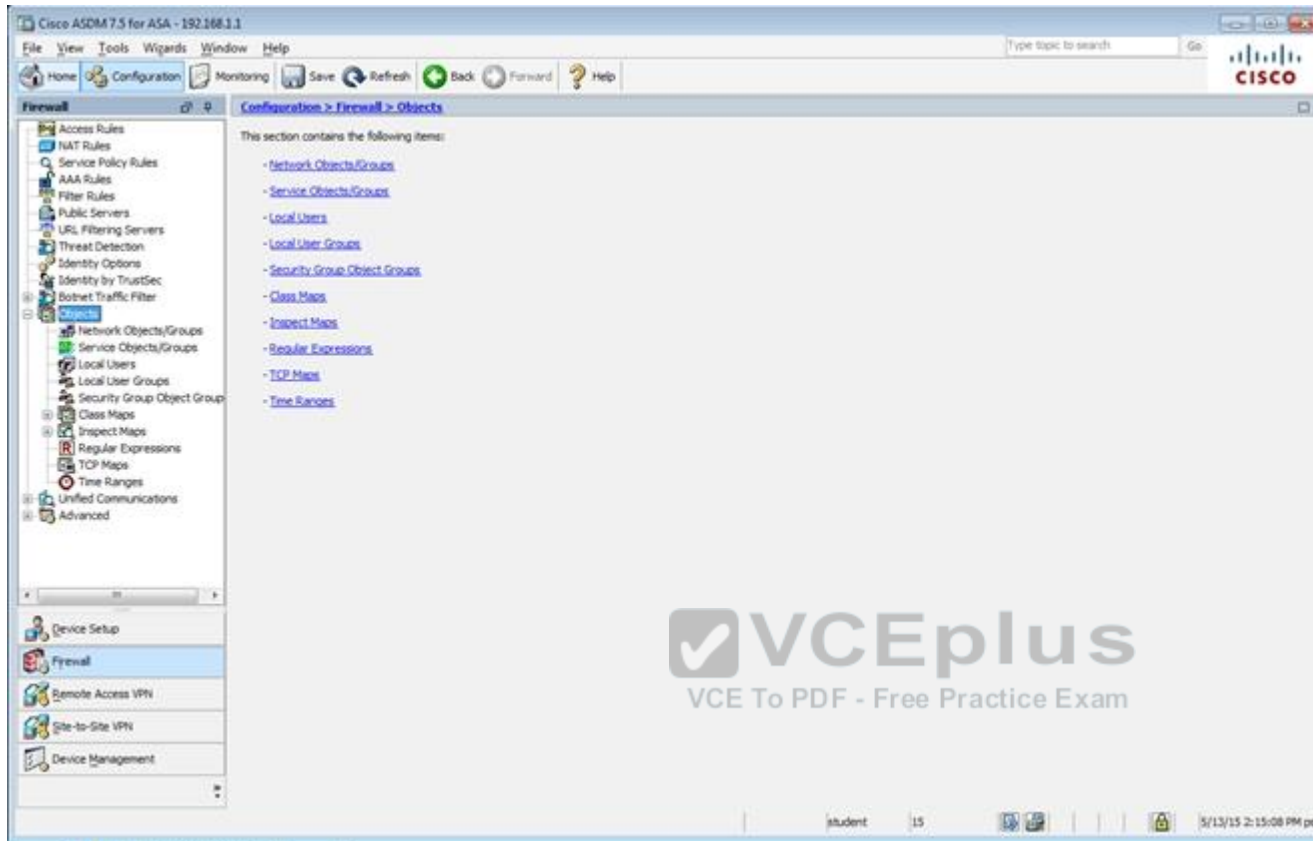












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

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

Add Edit Delete

End: [ ] [ ] [ ] Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

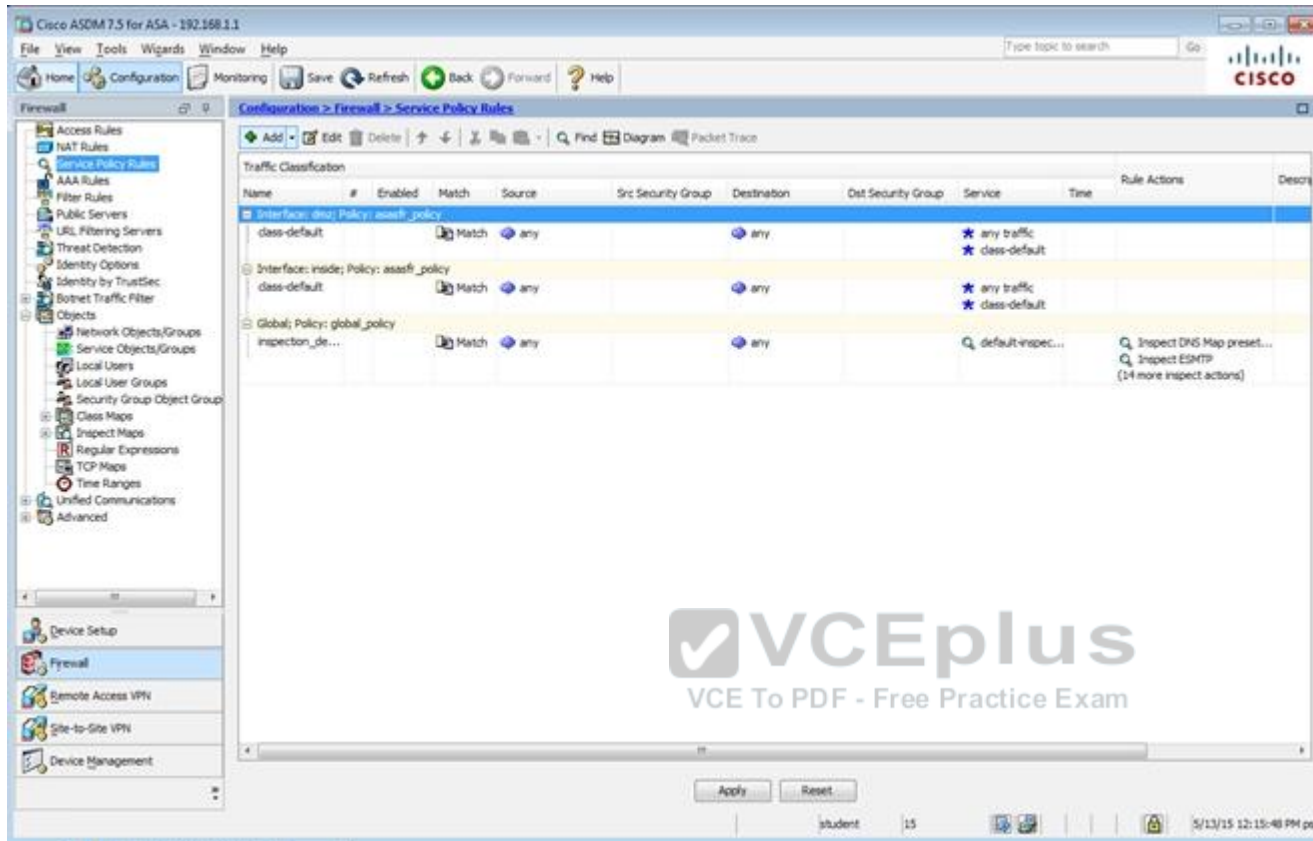
Firewall Configuration > Firewall > Objects > Network Objects/Groups

Filter: [Clear]

| Name                   | IP Address       | Netmask | Description | Object NAT Address |
|------------------------|------------------|---------|-------------|--------------------|
| <b>Network Objects</b> |                  |         |             |                    |
| any                    |                  |         |             |                    |
| any-host               | 0.0.0.0          | 0.0.0.0 |             | outside (P)        |
| any4                   |                  |         |             |                    |
| any6                   |                  |         |             |                    |
| facebook               | www.facebook.com |         |             |                    |
| My_ASA_Demo_Obj        | 1.10.8.20        |         |             |                    |

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Access Rules

Access Rules

- 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

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

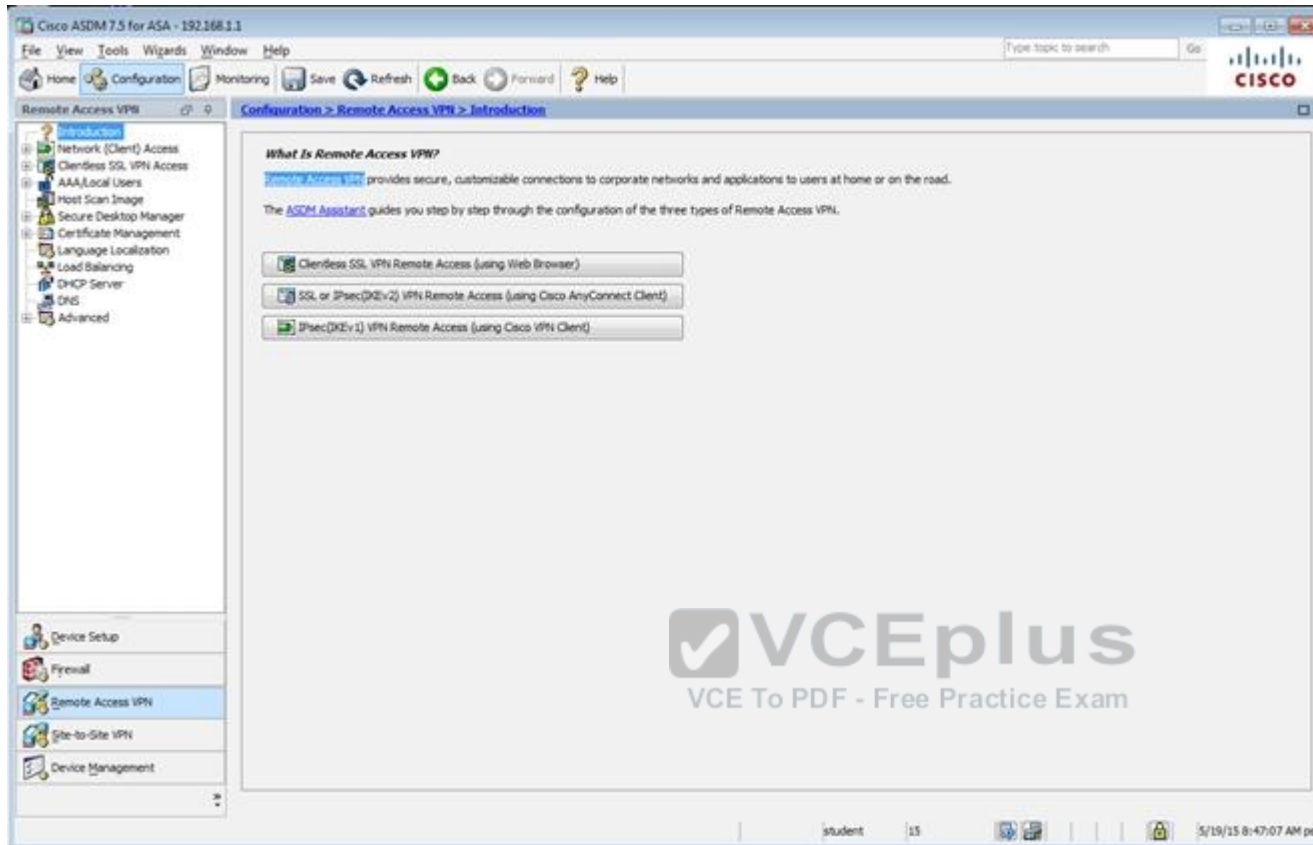
Configuration > Firewall > Access Rules

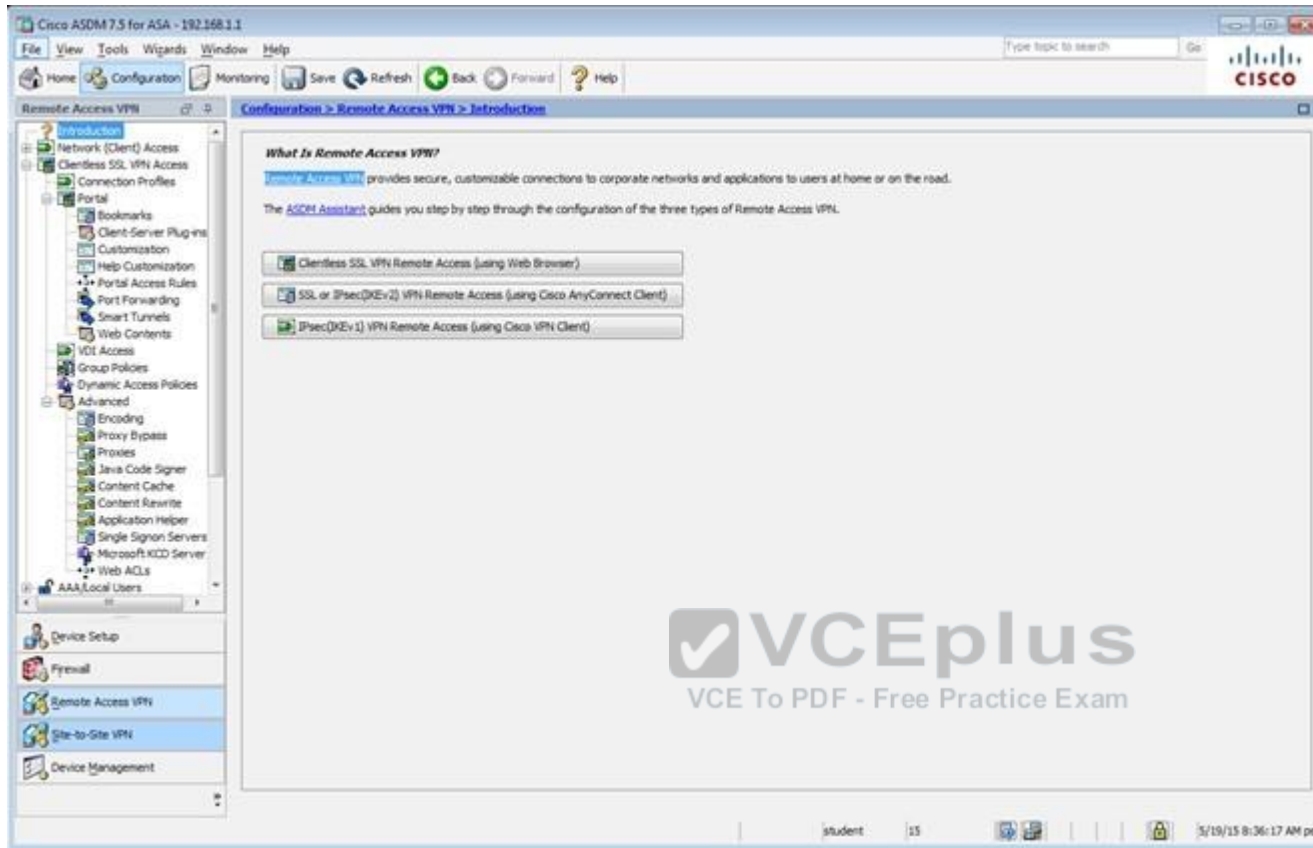
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

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

Apply Reset Advanced...

student 15 5/13/15 12:28:58 PM pst





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

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

Connection Profiles

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

Add Edit Delete Find: Match Case

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

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

Name: clientless  
Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

☐ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add - Delete (The table is in-line editable.)

| Alias | Enabled                             |
|-------|-------------------------------------|
| test  | <input checked="" type="checkbox"/> |

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add - Delete (The table is in-line editable.)

| URL                        | Enabled                             |
|----------------------------|-------------------------------------|
| https://209.165.201.2/test | <input checked="" type="checkbox"/> |

You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Interface-Specific Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL |
|-----------|--------------|-------------------|
|-----------|--------------|-------------------|

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Secondary Authentication Server Group

Server Group: -- None -- Manage...

☐ Use LOCAL if Server Group fails

☐ Use primary username (Hide secondary username on login page)

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

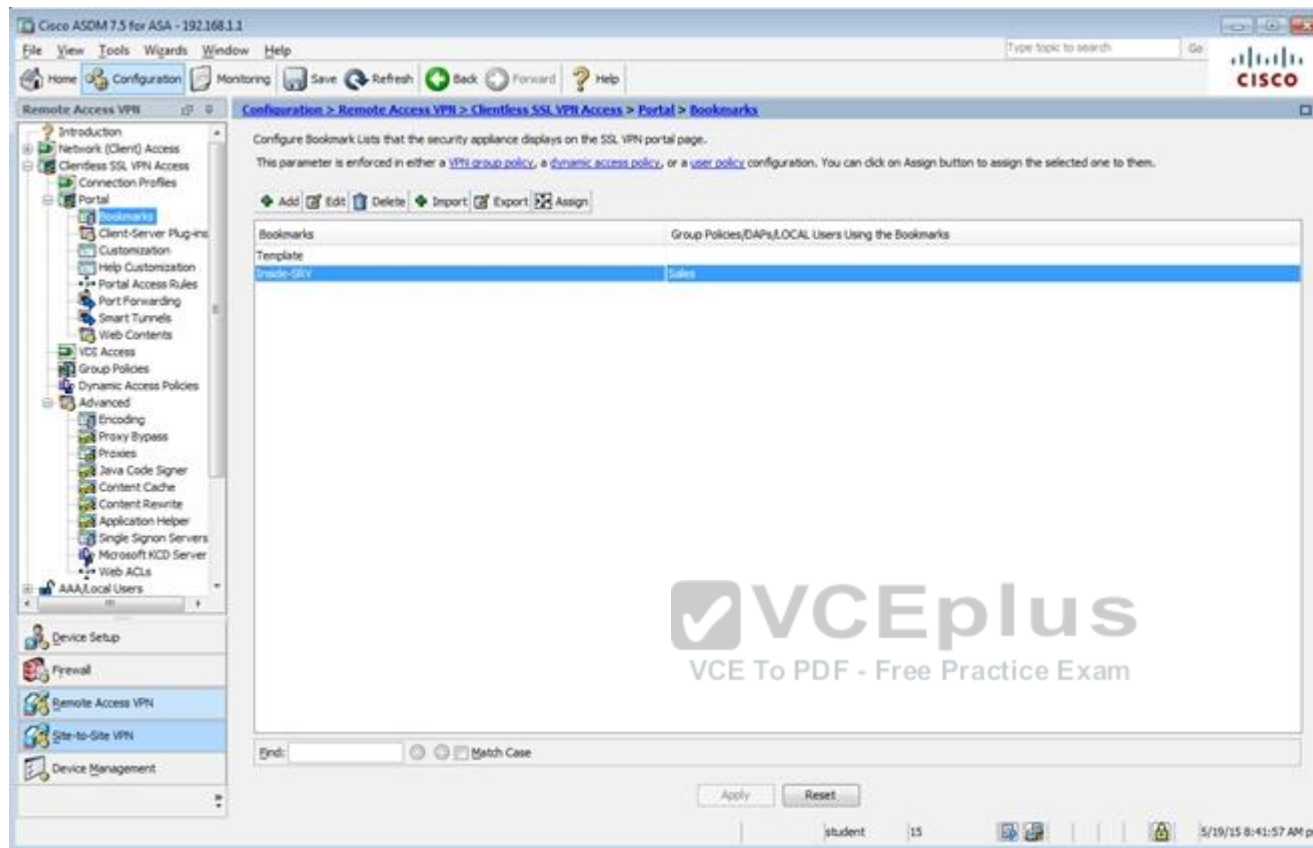
☐ Use the entire DN as the username

☐ Use script to select username

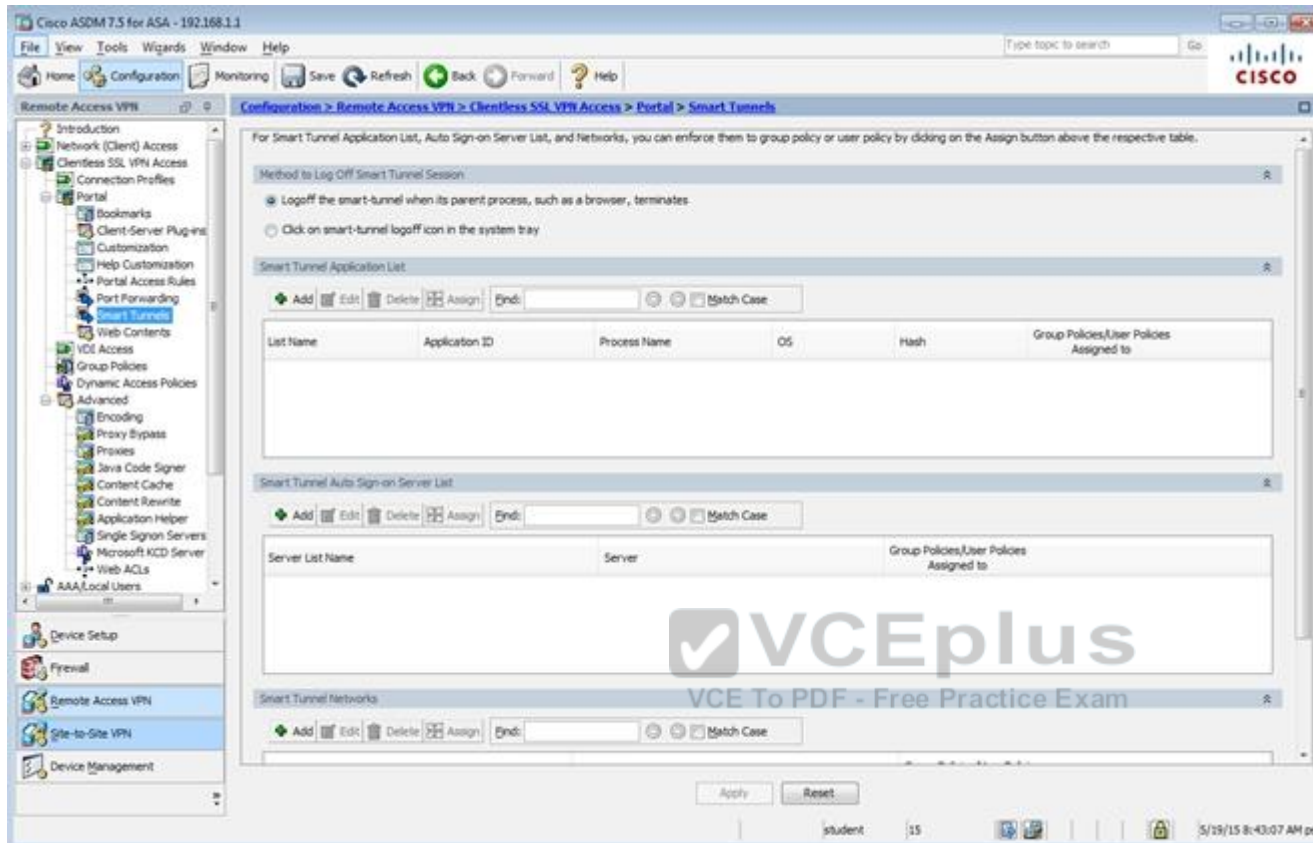
-- None -- + Add Edit Delete

Find:  Next Previous

OK Cancel Help







The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with the following items: Introduction, Network (Client) Access, Clientless SSL VPN Access, Connection Profiles, Portal, Bookmarks, Client-Server Plug-ins, Customization, Help Customization, Portal Access Rules, Smart Tunnels, Web Contents, VDI Access, Group Policies, Dynamic Access Policies, Advanced, Encoding, Proxy Bypass, Proxies, Java Code Signer, Content Cache, Content Rewrite, Application Helper, Single Signon Servers, Microsoft KCD Server, Web ACLs, AAA/Local Users, Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management. The main pane displays the configuration page for Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding. The page title is "Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection." Below the title, there is a text box stating: "This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them." Below the text box, there is a table with the following columns: List Name, Local TCP Port, Remote Server, Remote TCP Port, Description, and Group Policies/User Policies Assigned to. The table is currently empty. At the bottom of the main pane, there is a "Find:" search bar and a "Match Case" checkbox. The bottom status bar shows the user "student", the page number "15", and the date/time "5/19/15 8:43:47 AM pst".

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

◆ Add ◆ Edit ◆ Delete ◆ Assign

| Name                                | Type     | Tunneling Protocol                  | Connection Profiles/Users Assigned To                  |
|-------------------------------------|----------|-------------------------------------|--|
| Client                              | Internal | ssl-clientless                      | clientless   |
| DefaultGroupPolicy (System Default) | Internal | kev1:kev2:ssl-clientless/2to-espsec | DefaultRAGroup/DefaultIL2Group/DefaultADMPGroup/Def... |

Find: [ ] [ ] [ ] Match Case

Apply Reset

student 15 5/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

Tunneling Protocols: ☐ Inherit ☒ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 ☐ IPsec IKEv2 ☐ L2TP/IPsec

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default:  minutes

Idle Alert Interval: ☒ Inherit ☐ Default:  minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

Find:  ☐ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

Remote Access VPN

- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- VCE Access
- Group Policies
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

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

Find:

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

Edit Internal Group Policy: Sales

General  
More Options  
Customization  
Login Setting  
Single Signon  
VDI Access  
Session Settings

Bookmark List: ☐ Inherit Inside-SRV Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Network: Tunnel Option: -- None -- Manage...

Smart Tunnel Application: ☒ Inherit Manage...

☐ Smart Tunnel all Applications (This feature only works with Windows platforms)

☐ Auto Start

Auto Sign-on Server: ☒ Inherit Manage...

Windows Domain Name (optional):

Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

**General**  
Servers  
Advanced

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None--

Access Hours: --Unrestricted--

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

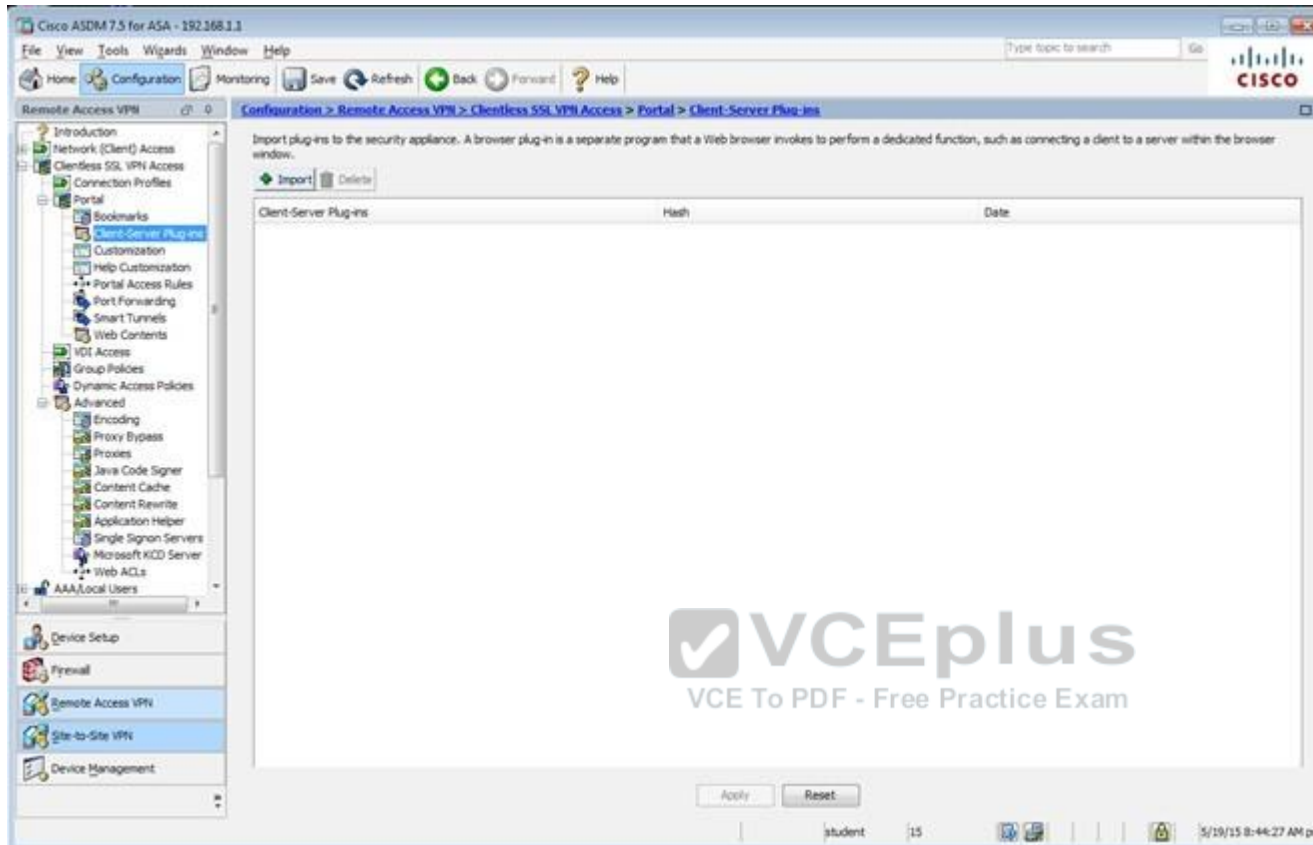
Maximum Connect Time: ☒ Unlimited  minutes

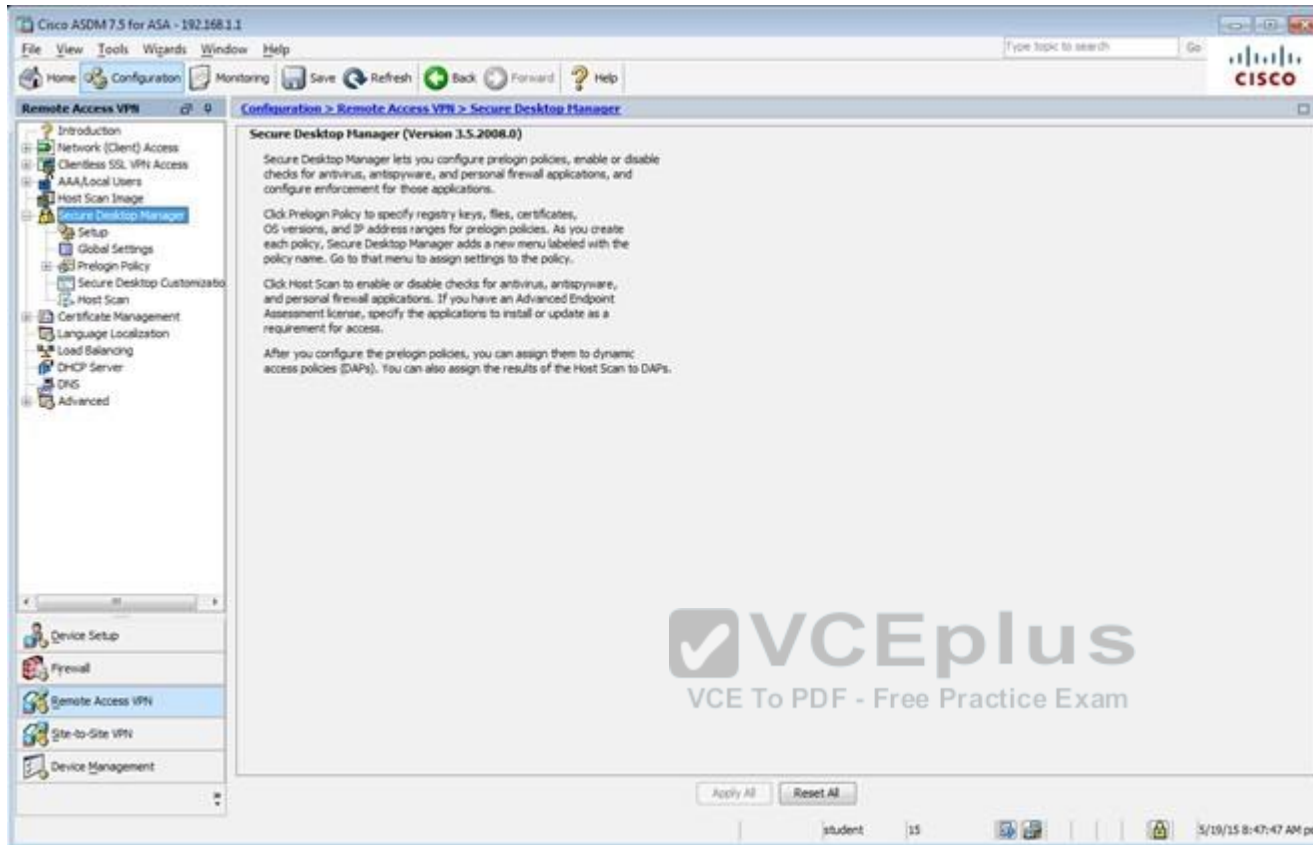
Idle Timeout: ☐ None  30 minutes

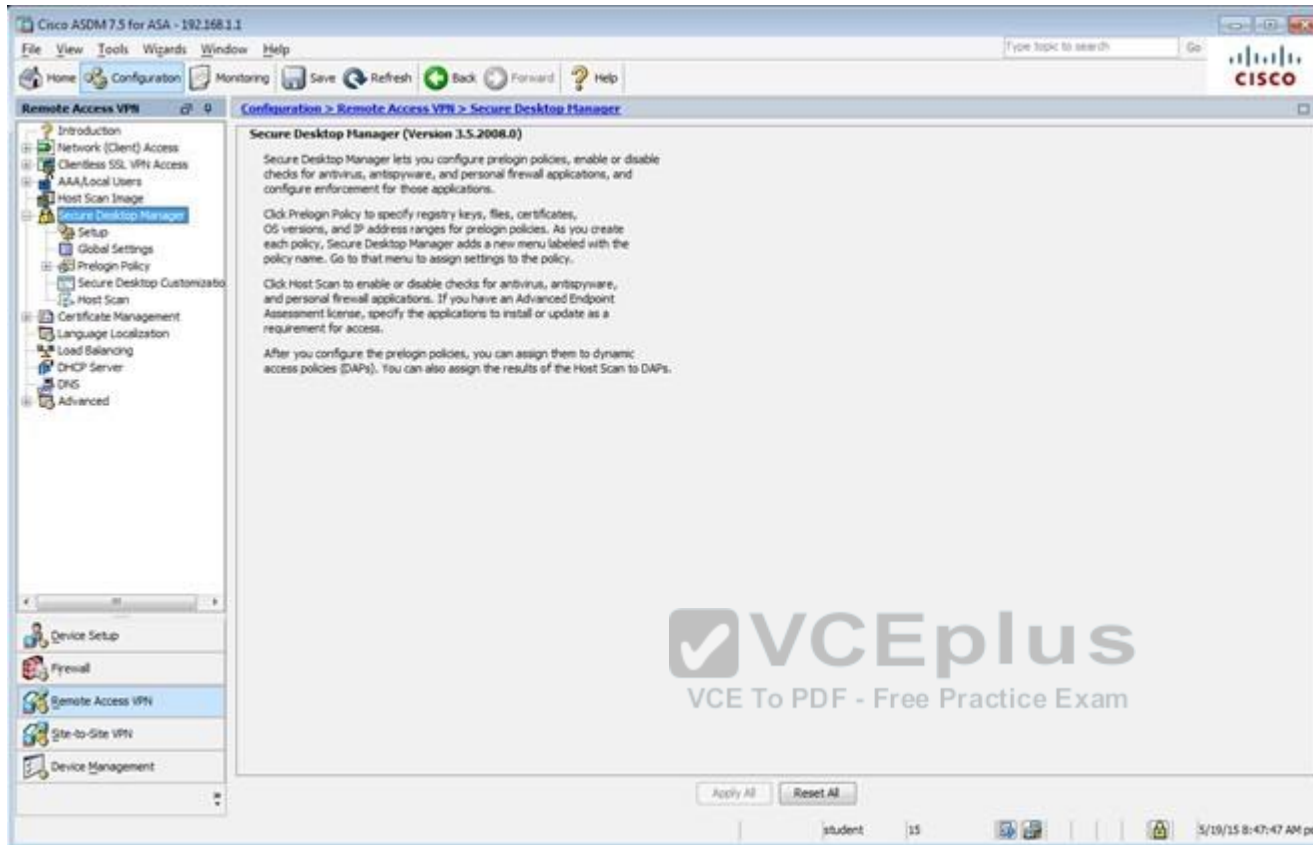
On smart card removal: ☒ Disconnect ☐ Keep the connection

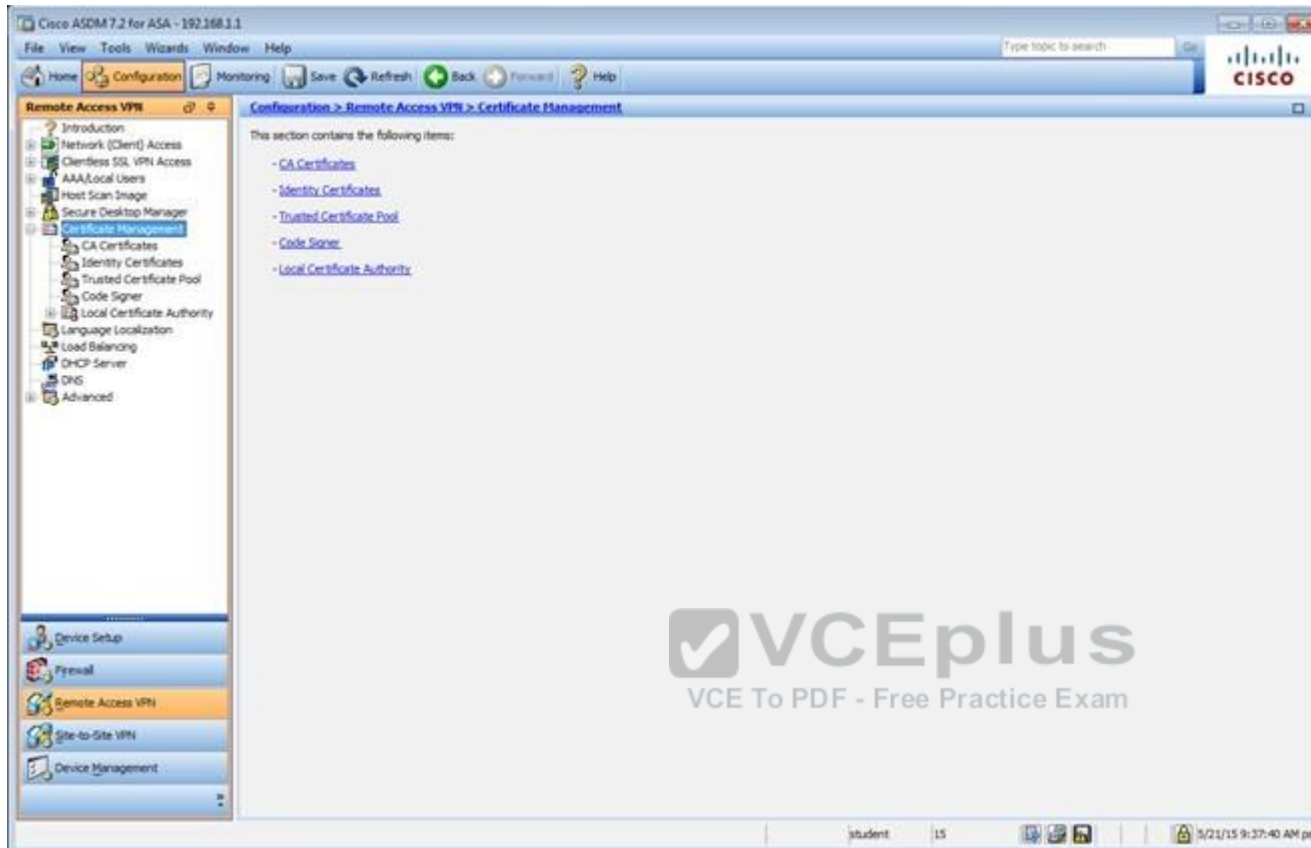
**VCEplus**  
VCE To PDF - Free Practice Exam

Find:





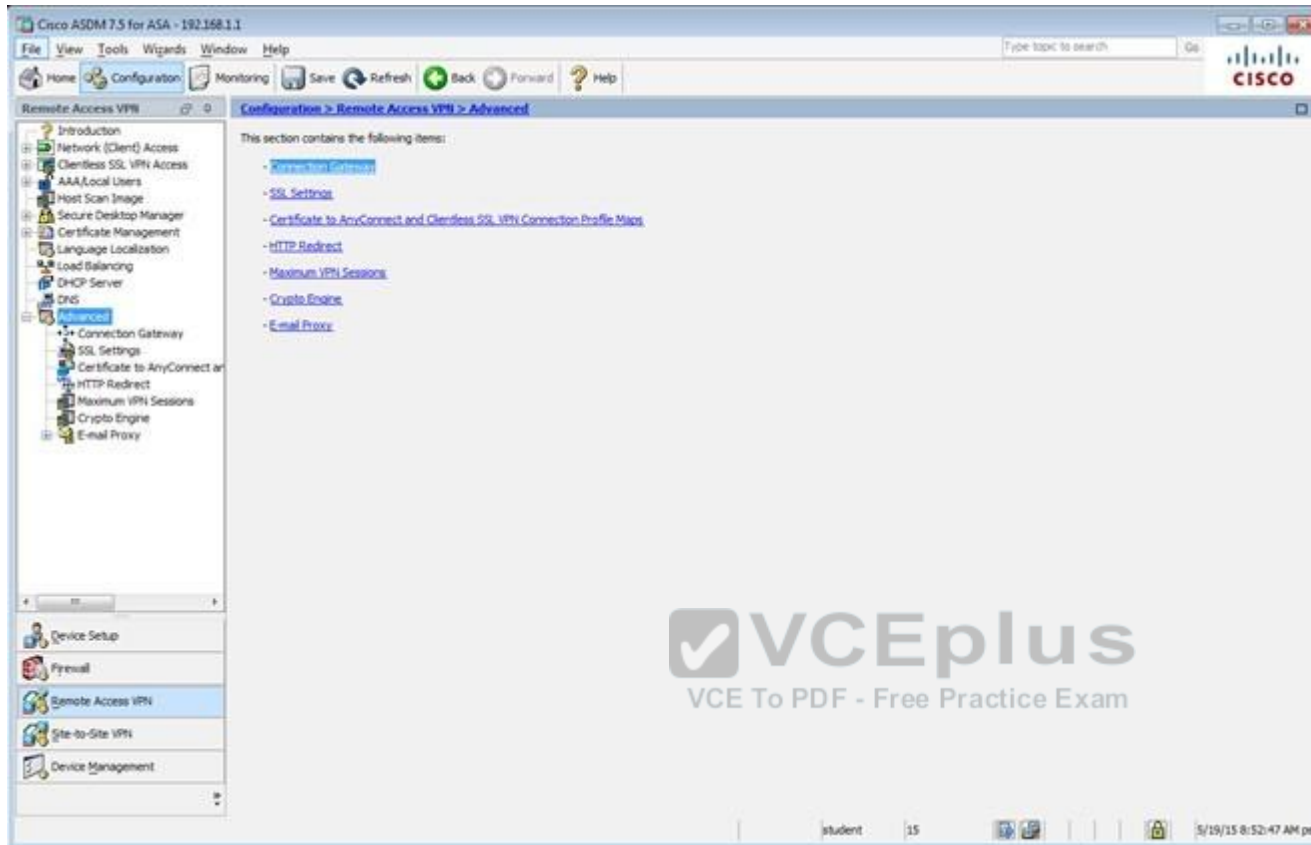




The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with the following data:

| Issued To                 | Issued By                 | Expiry Date              | Associated Trustpoints | Usage           | Public Key Type |
|---------------------------|---------------------------|--------------------------|------------------------|-----------------|-----------------|
| hostname-wp 17-ASA.sec... | hostname-wp 17-ASA.sec... | 11:10:33 pet Dec 20 2024 | ASDM_TrustPoint1       | Generic Purpose | RSA (2048 bits) |

Below the table, there are sections for 'Certificate Expiration Alerts' and 'Public CA Enrollment'. The 'Public CA Enrollment' section includes a link to 'Enroll ASA SSL certificate with Entrust' and a 'Launch ASDM Identity Certificate Wizard' button. The bottom status bar shows 'student', '15', and the date '5/19/15 8:51:47 AM pet'.



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

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

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

Encryption

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

Server Name Indication (SNI)

Domain: dmz

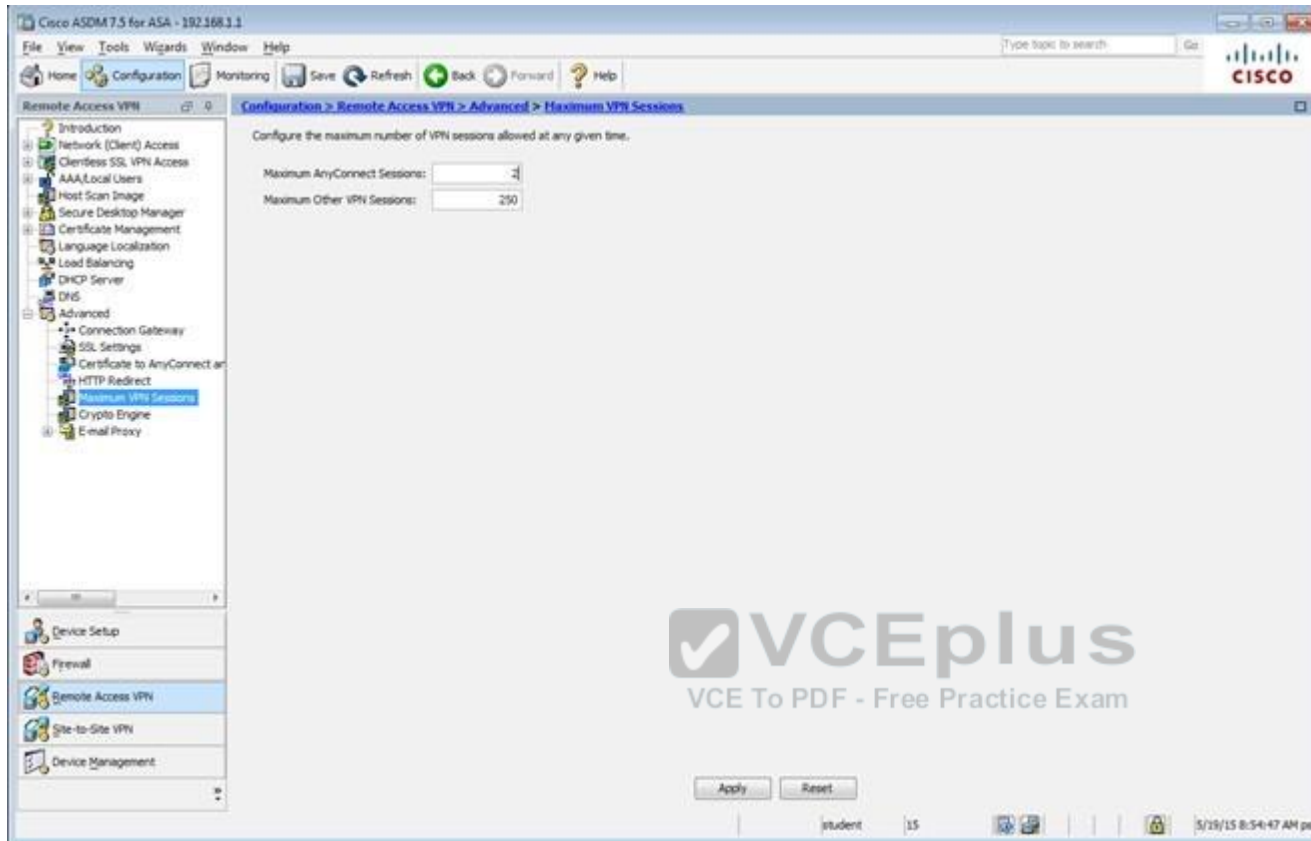
Certificate: ASDM\_TrustPoint1h...

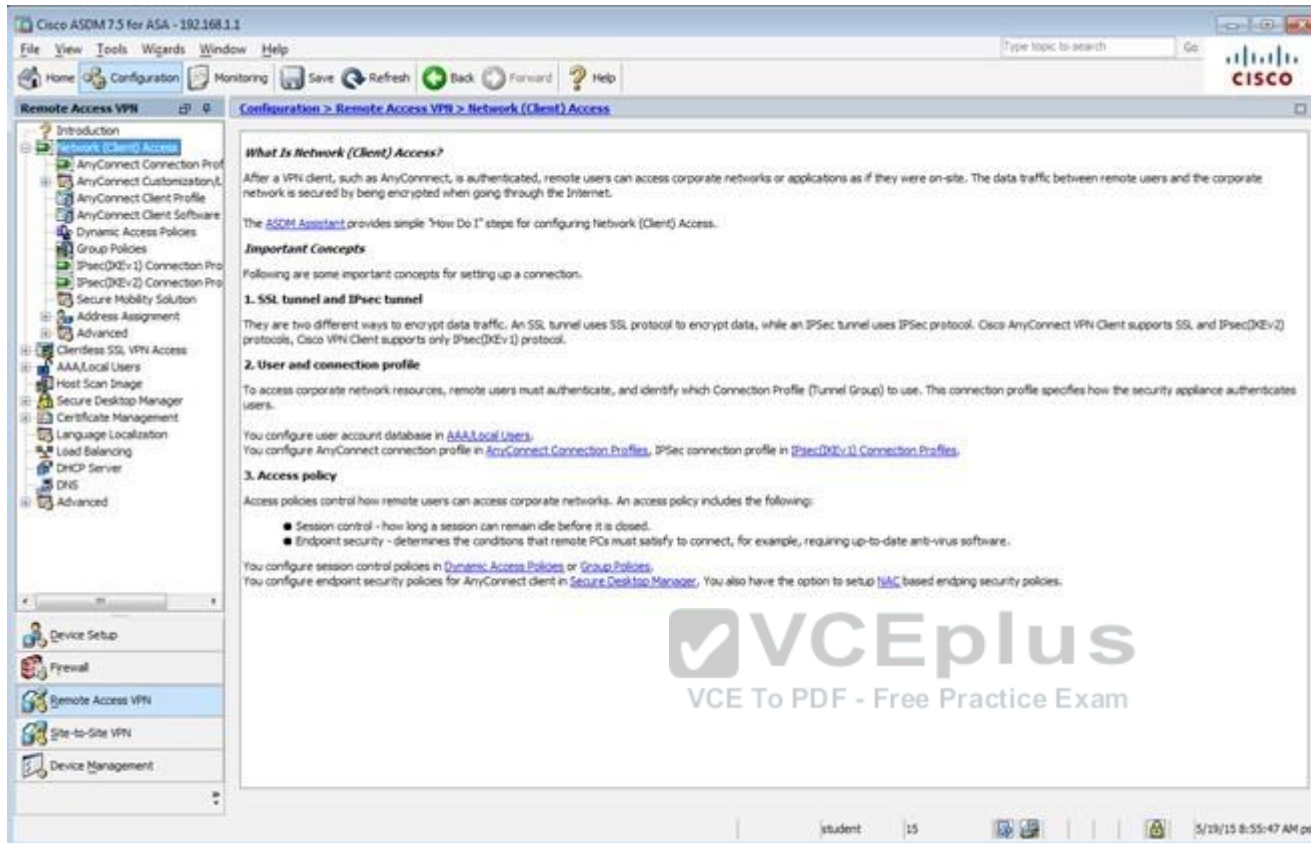
Certificates

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

Apply Reset

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





The screenshot displays the Cisco ASDM 7.5 for ASA - 102.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Network (Client) Access'. It contains the following text:

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

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

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

**1. SSL tunnel and IPsec tunnel**  
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.

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

You configure user account database in [AAA Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).

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

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

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

The bottom of the window shows a status bar with 'student', '15', and a timestamp '5/28/15 8:55:47 AM pet'.

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol               | Connection Profiles/Users Assigned To                  |
|--------------------------------|----------|----------------------------------|--|
| Sales                          | Internal | ssl-clientless                   | clientless   |
| DefaultPolicy (System Default) | Internal | (rev 1) ssl-clientless/ssl-ipsec | DefaultPolicyGroupDefaultPolicyGroupDefaultPolicyGroup |

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: DftrGpPolicy

**General**

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

Name: DftrGpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: -- None -- Manage...

NAC Policy: -- None -- Manage...

Access Hours: -- Unrestricted -- Manage...

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

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

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles

Introduction  
Network (Client) Access  
AnyConnect Connection Profile  
AnyConnect Customization...  
AnyConnect Client Profile  
AnyConnect Client Software  
Dynamic Access Policies  
Group Policies  
IPsec(IKv1) Connection Profile  
IPsec(IKv2) Connection Profile  
Secure Mobility Solution  
Advanced  
Clientless SSL VPN Access  
AAA/Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DHG  
Advanced

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

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

| Name              | IPsec Enabled                       | L2TP/IPsec Enabled                  | Authentication Server Group | Group Policy  |
|-------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| DefaultEIVpnGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| Clientless        | <input type="checkbox"/>            | <input type="checkbox"/>            | LOCAL                       | Sales         |

Find:  Match Case

Apply Reset

student 15 5/19/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

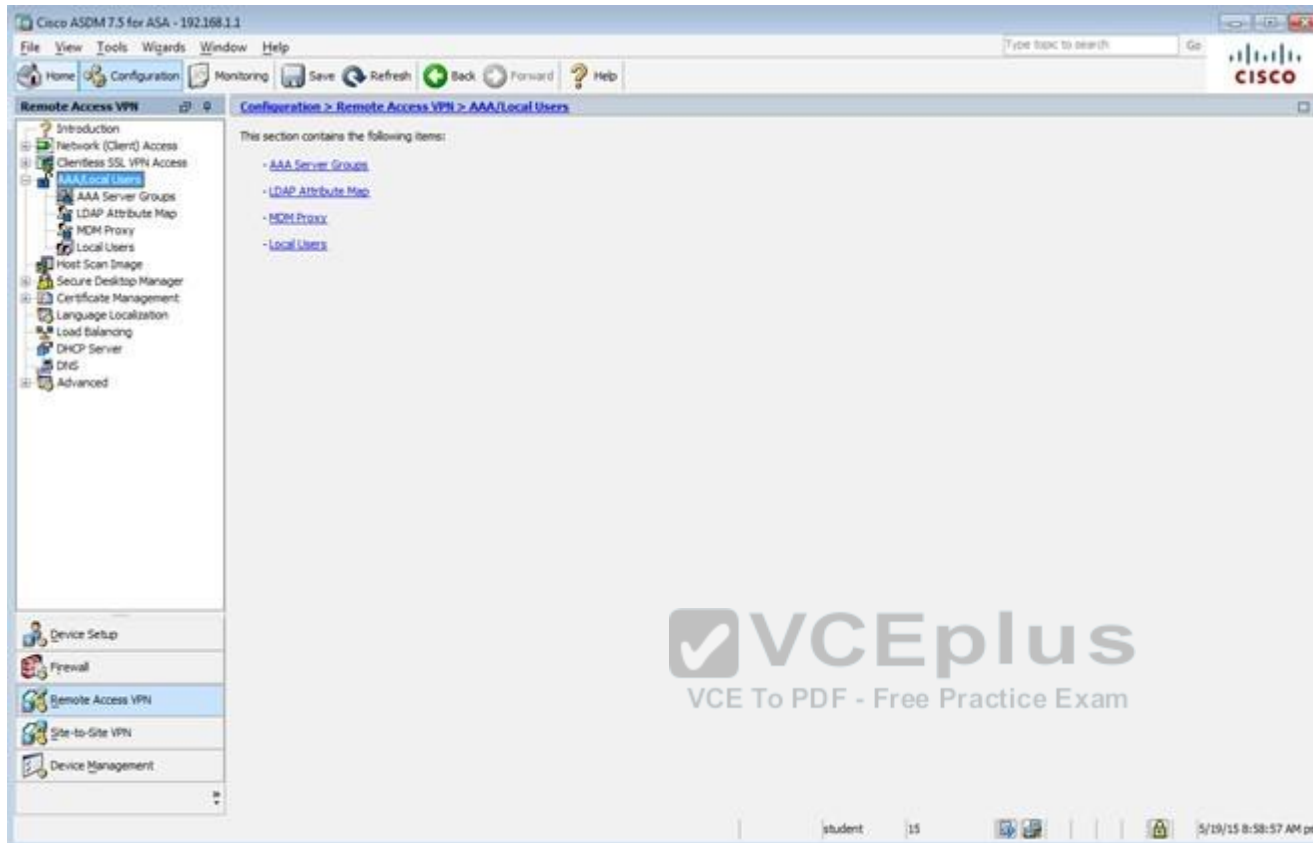
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name               | SSL Enabled                         | IPsec Enabled                       | Aliases | Authentication Method | Group Policy  |
|--------------------|-------------------------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultVRAGroup    | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| DefaultWEBVPNGroup | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| Clientless         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | yes     | SSL (OCSP)            | Clientless    |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction  
Network (Client) Access  
Clientless SSL VPN Access  
AAA/Local Users  
AAA Server Groups  
LDAP Attribute Map  
MDM Proxy  
Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DNS  
Advanced

Create entries in the ASA local user database.

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

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

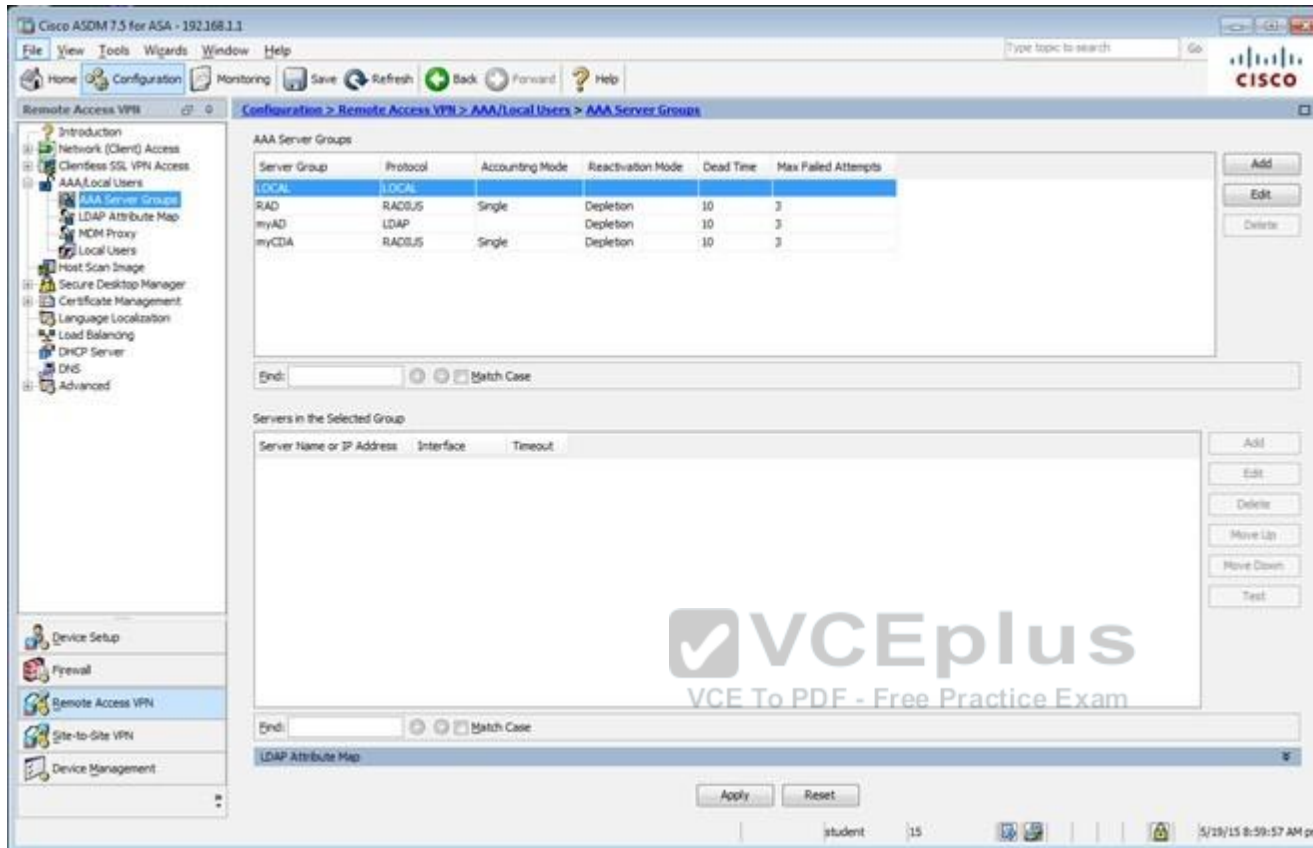
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

Add Edit Delete

Find: Match Case

Apply Reset

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



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

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

**Correct Answer:** ADEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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



Virtual Terminal

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

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

+ Add - Edit Delete Assign

| Name                              | Type     | Tunneling Protocol                    | Connect    |
|-----------------------------------|----------|---------------------------------------|------------|
| Sales                             | Internal | ssl-clientless                        | clientless |
| DefaultGrpPolicy (System Default) | Internal | ikev1;ikev2;ssl-clientless;l2tp-ipsec | Default    |

VCEplus  
VCE To PDF - Free Practice Exam

Scenario Questions TOPOLOGY

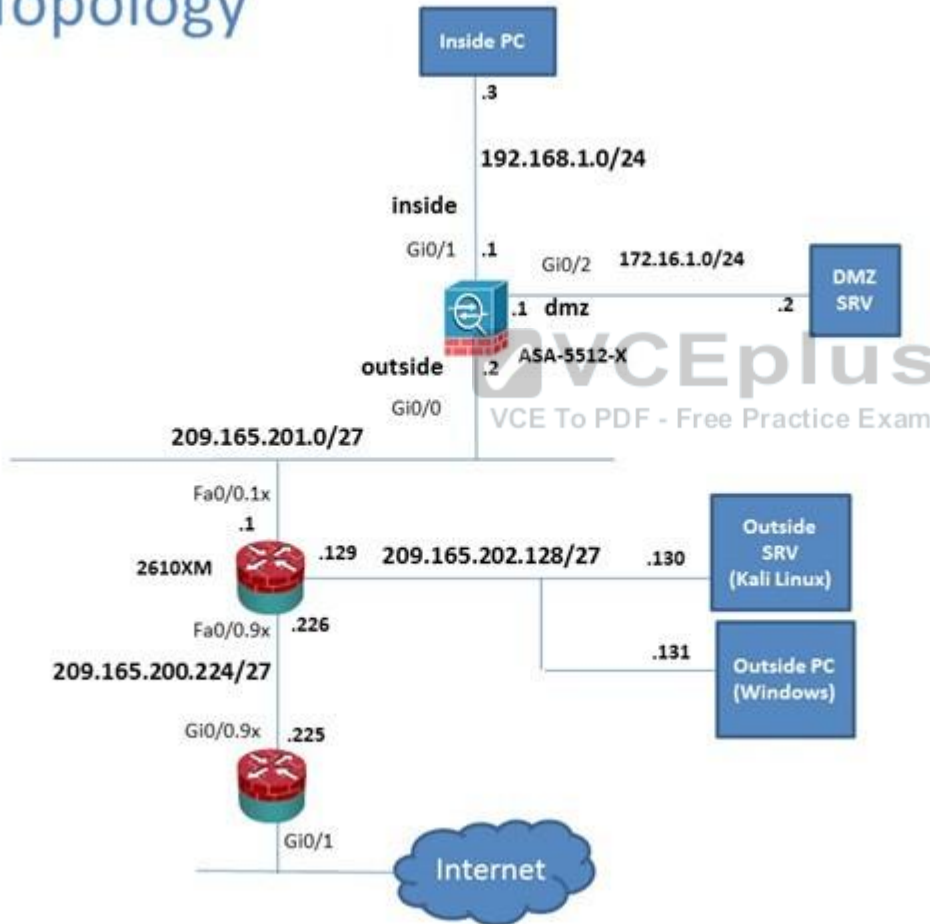
**QUESTION 65**  
Scenario

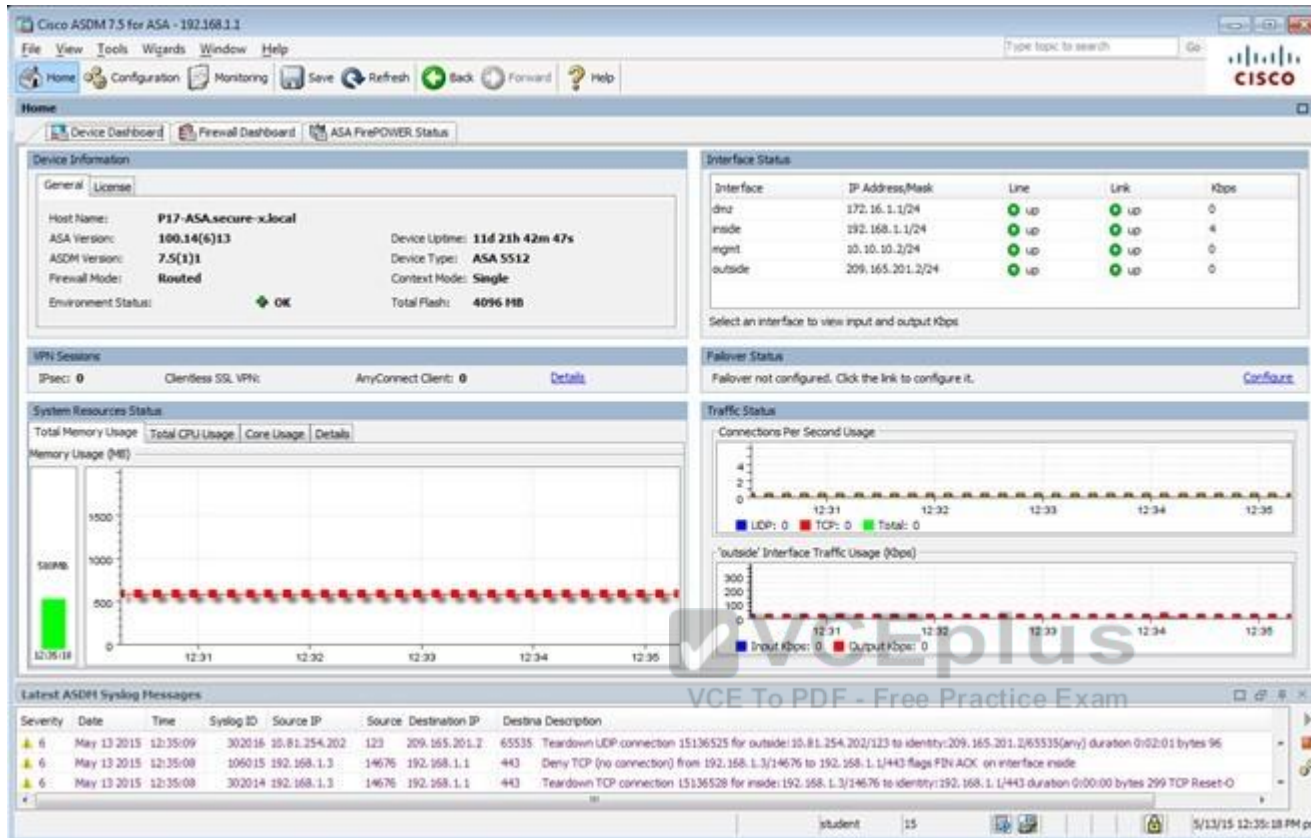
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

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

## Lab Topology





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address    | MAC Address    | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside   | 209.165.201.1 | 000c.3014.3820 | No        |
| inside    | 192.168.1.4   | 0050.5633.3333 | No        |
| inside    | 192.168.1.3   | 0050.5611.1111 | No        |
| inside    | 192.168.1.2   | 0050.5622.2222 | No        |
| inside    | 192.168.1.56  | 0050.5692.5c7b | No        |
| inside    | 192.168.1.55  | 0006.86e4.98f3 | No        |
| dmz       | 172.16.1.2    | 0050.5644.4444 | No        |
| mgmt      | 10.10.10.1    | 000c.3014.3820 | No        |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/PSec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions

Clientless SSL VPN

VPN Connection Graphs

WSA Sessions

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Monitoring > VPN > VPN Statistics > Sessions

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

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

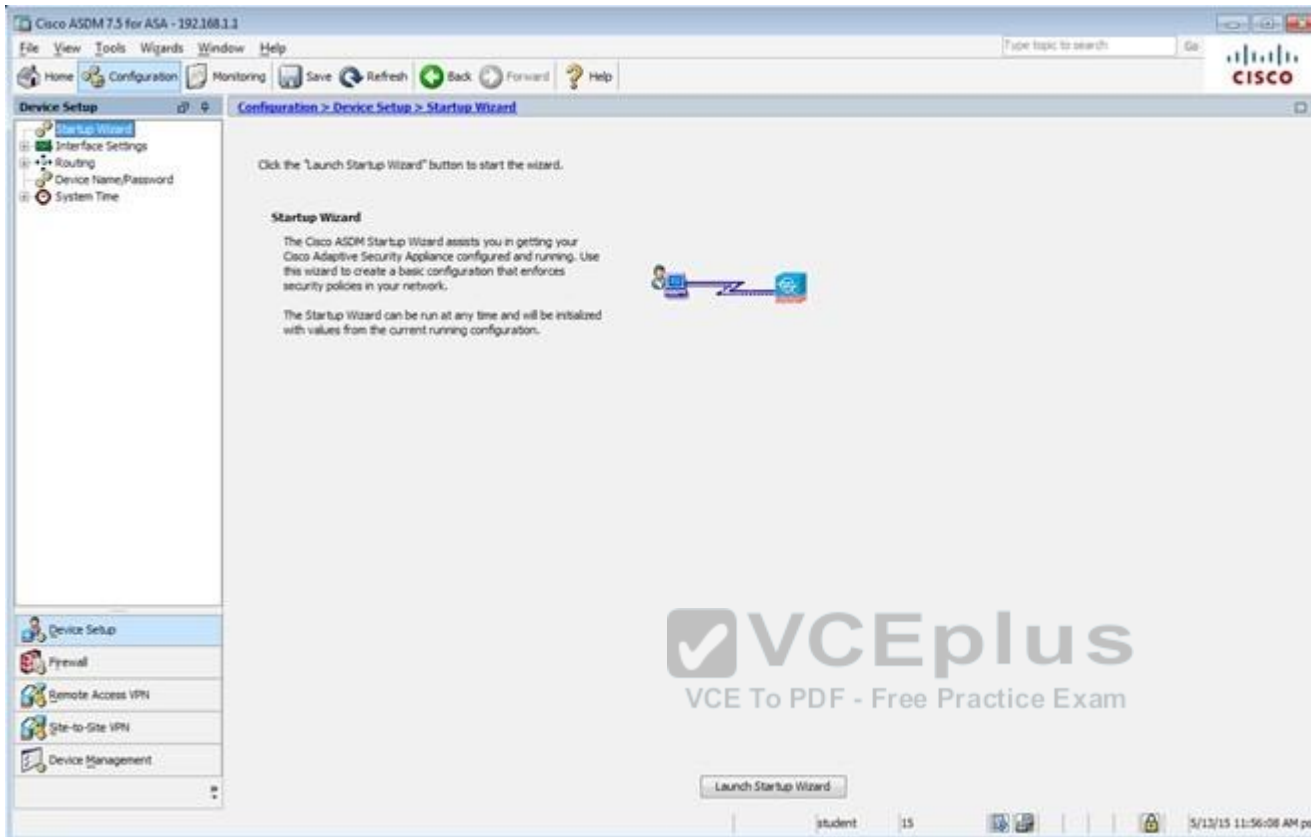
| Username | IP Address      | Group Policy | Connection Profile | Protocol   | Encryption         | Login Time                   | Duration   | Bytes Tx | Bytes Rx |
|----------|-----------------|--------------|--------------------|------------|--------------------|------------------------------|------------|----------|----------|
| student  | 209.165.202.131 | Sales        | Clientless         | Clientless | Clientless (13AC4) | 08:03:46 sat Thu May 21 2013 | 2h:09m:19s | 316774   | 41833    |

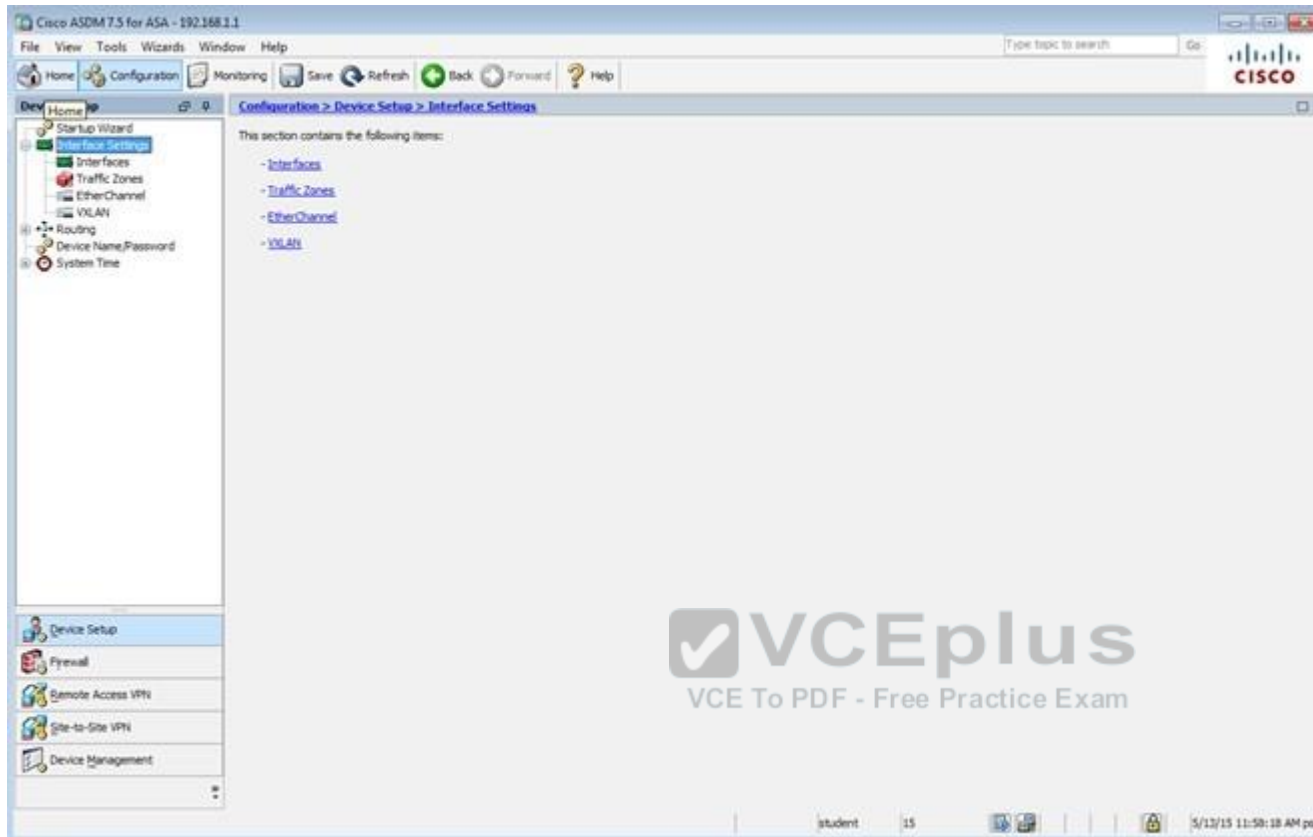
Details Logout Ping

Refresh

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

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

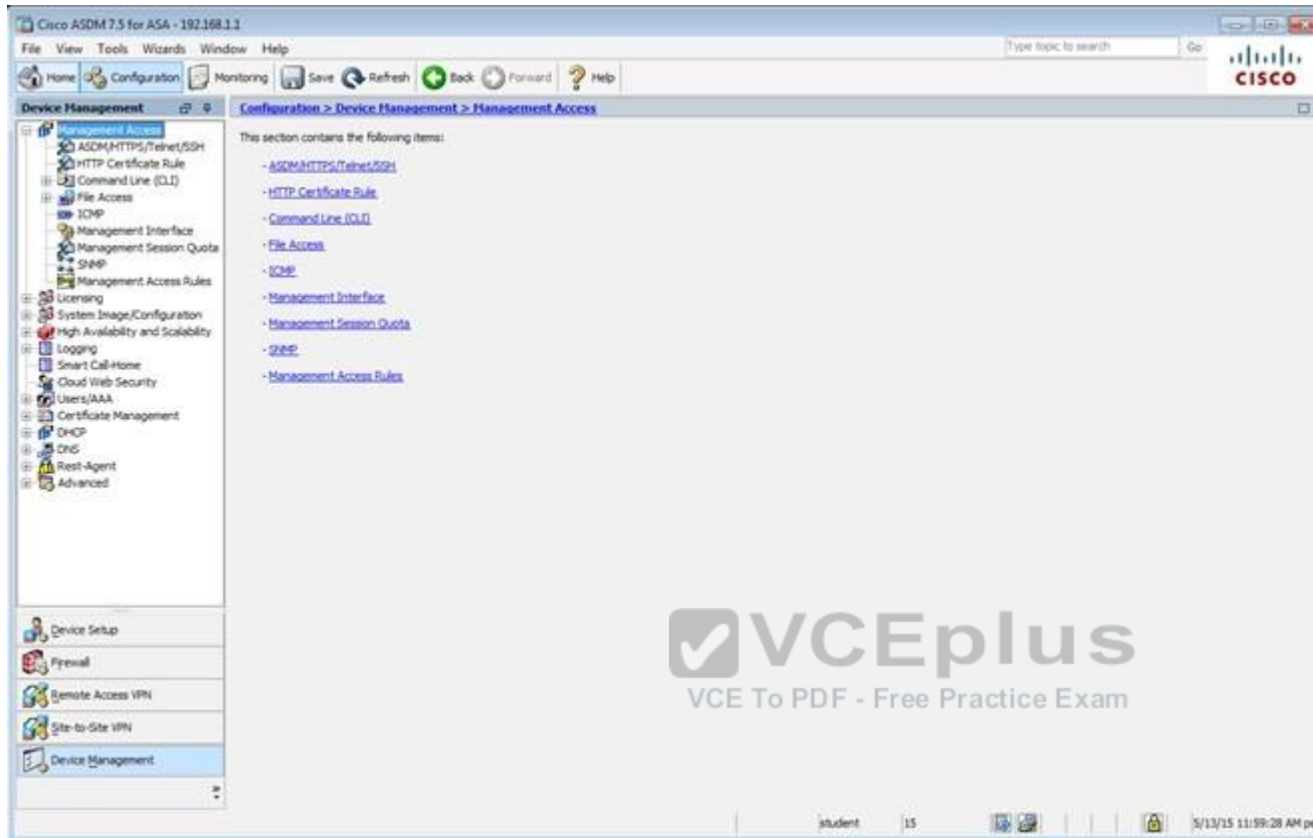
Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interface Settings > Interfaces

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

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

Student 15 5/13/15 12:42:48 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

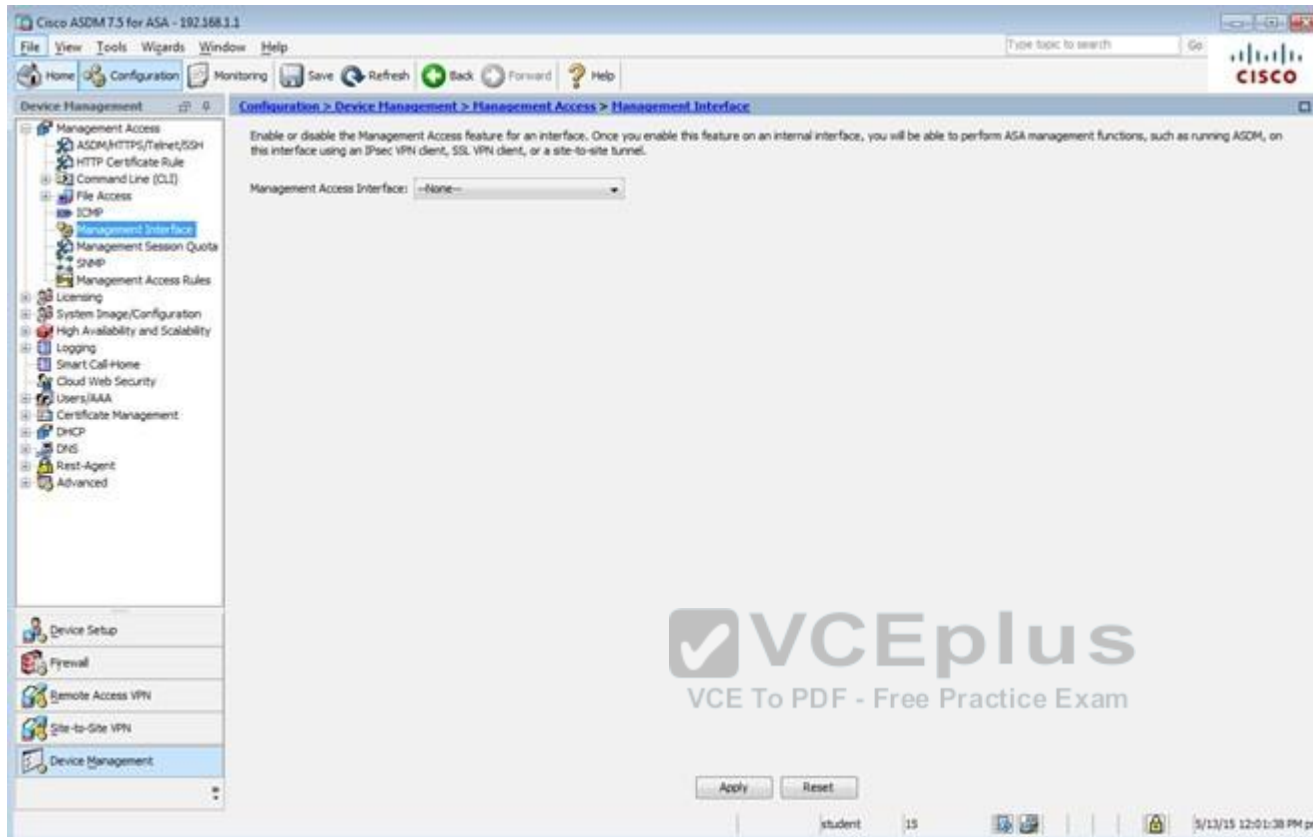
Allowed SSH Version(s): 1 & 2

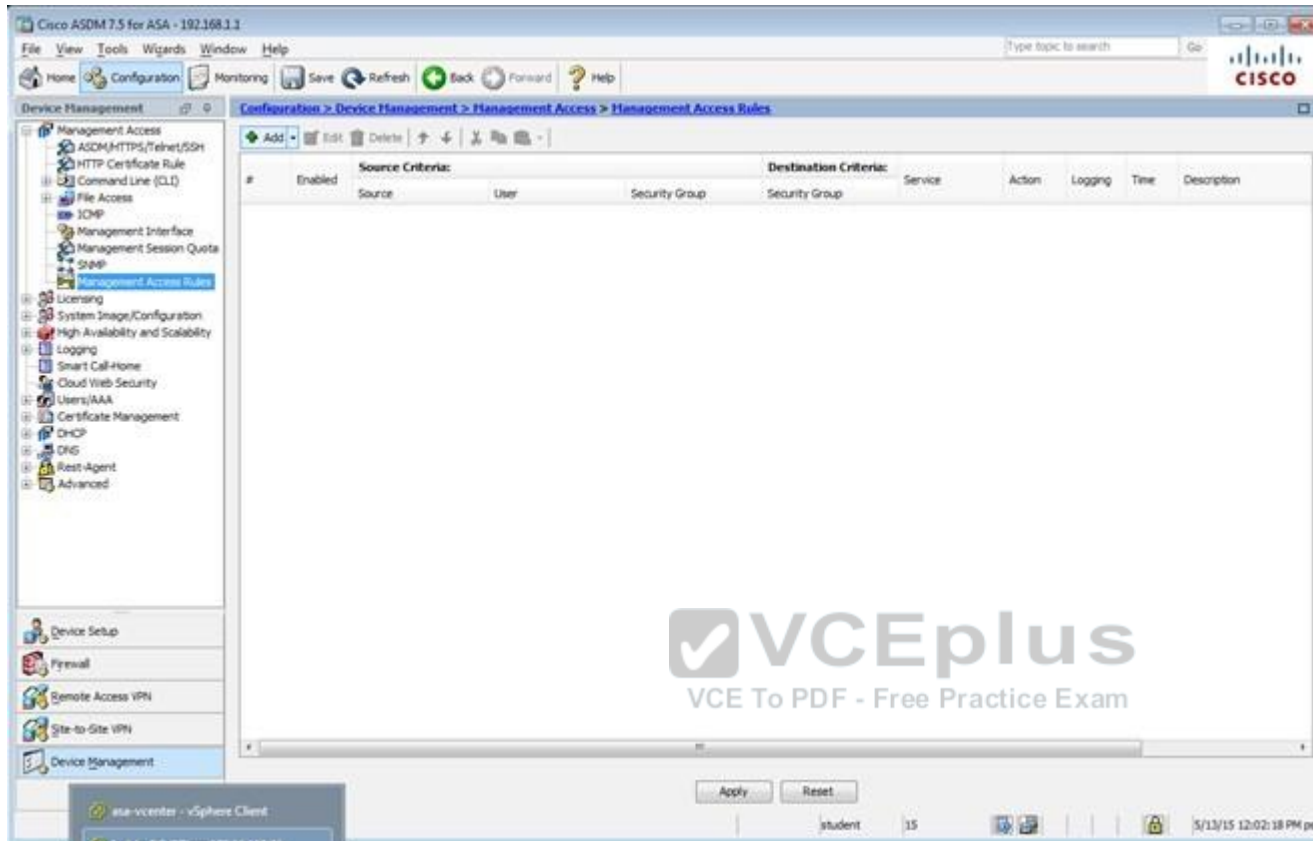
SSH Timeout: 5 minutes

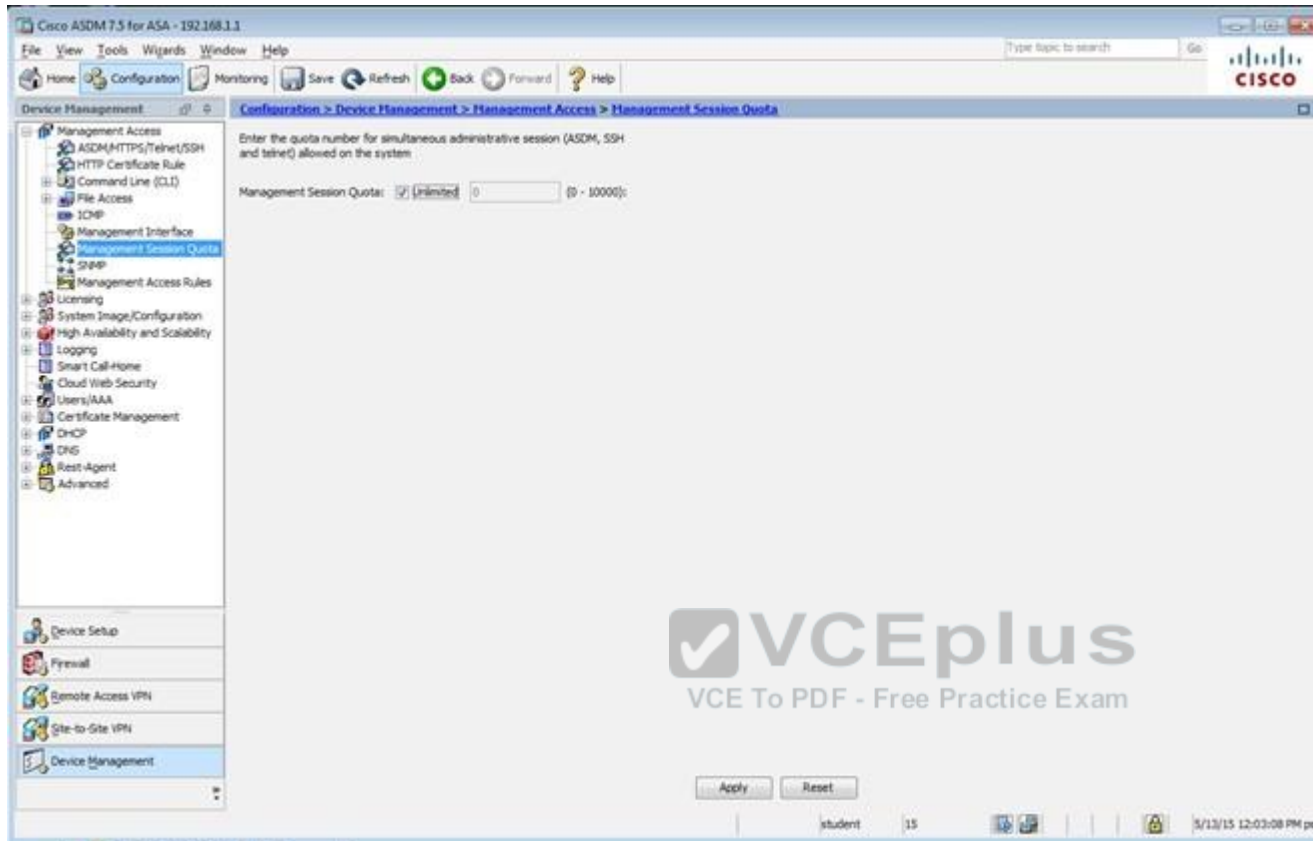
DH Key Exchange: ☒ Group 1 ☐ Group 14

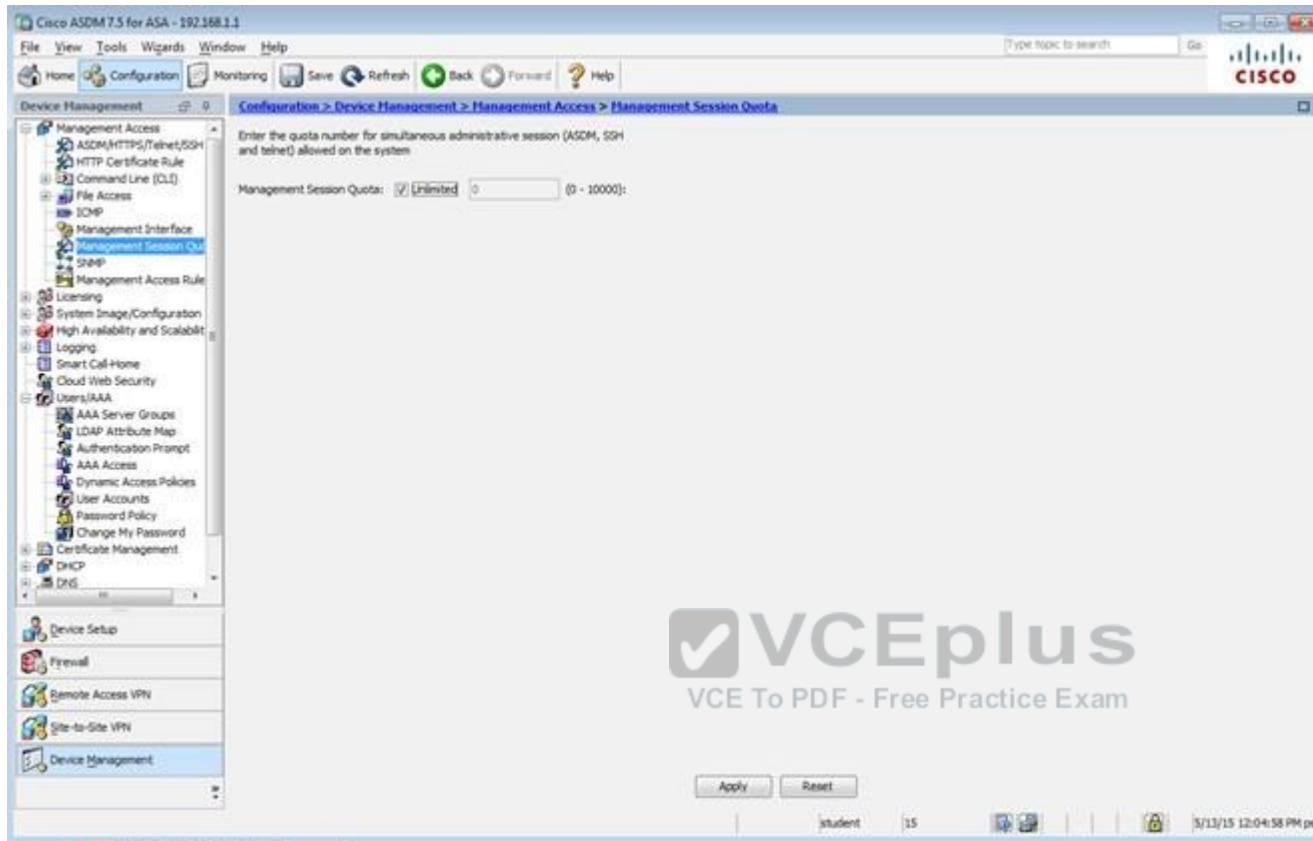
Apply Reset

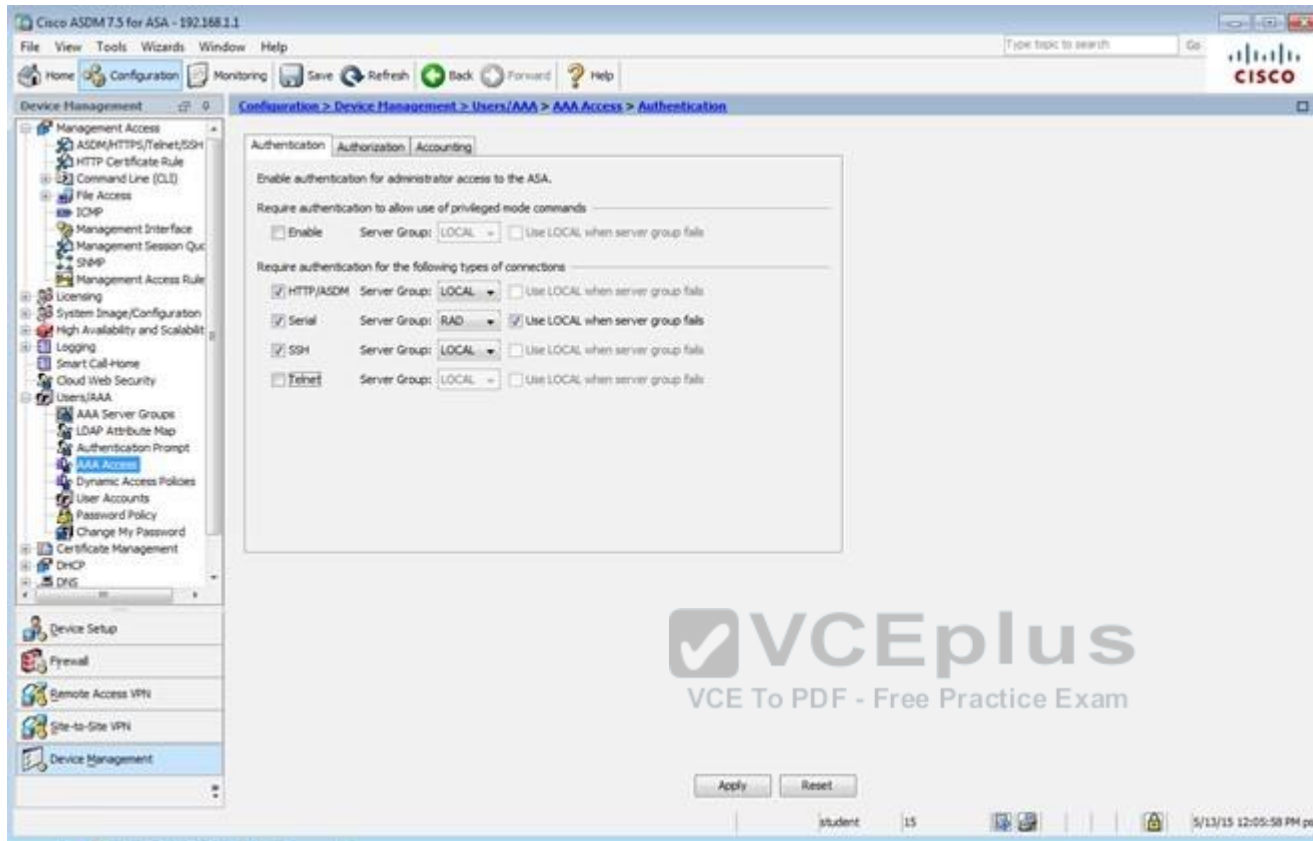
student 15 5/13/15 12:00:38 PM pet

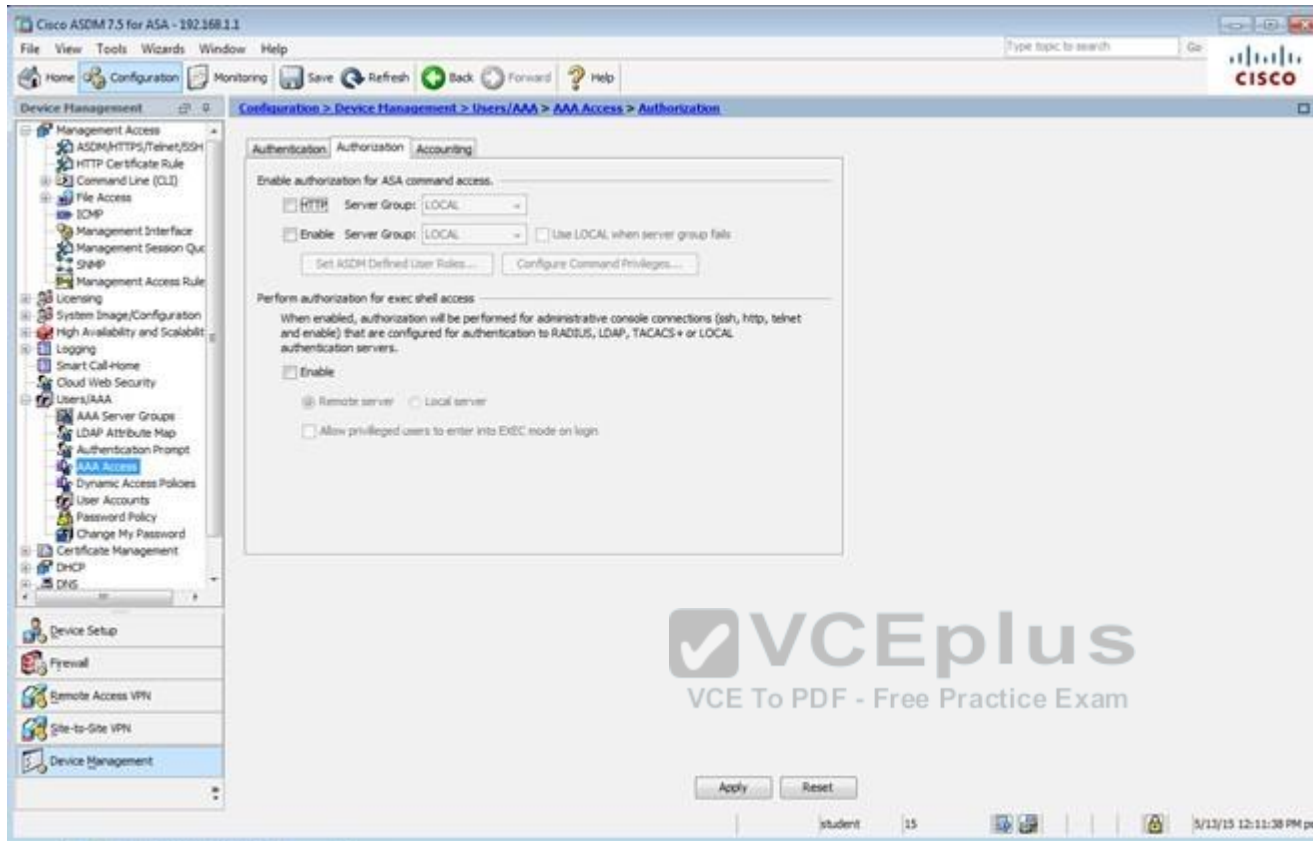


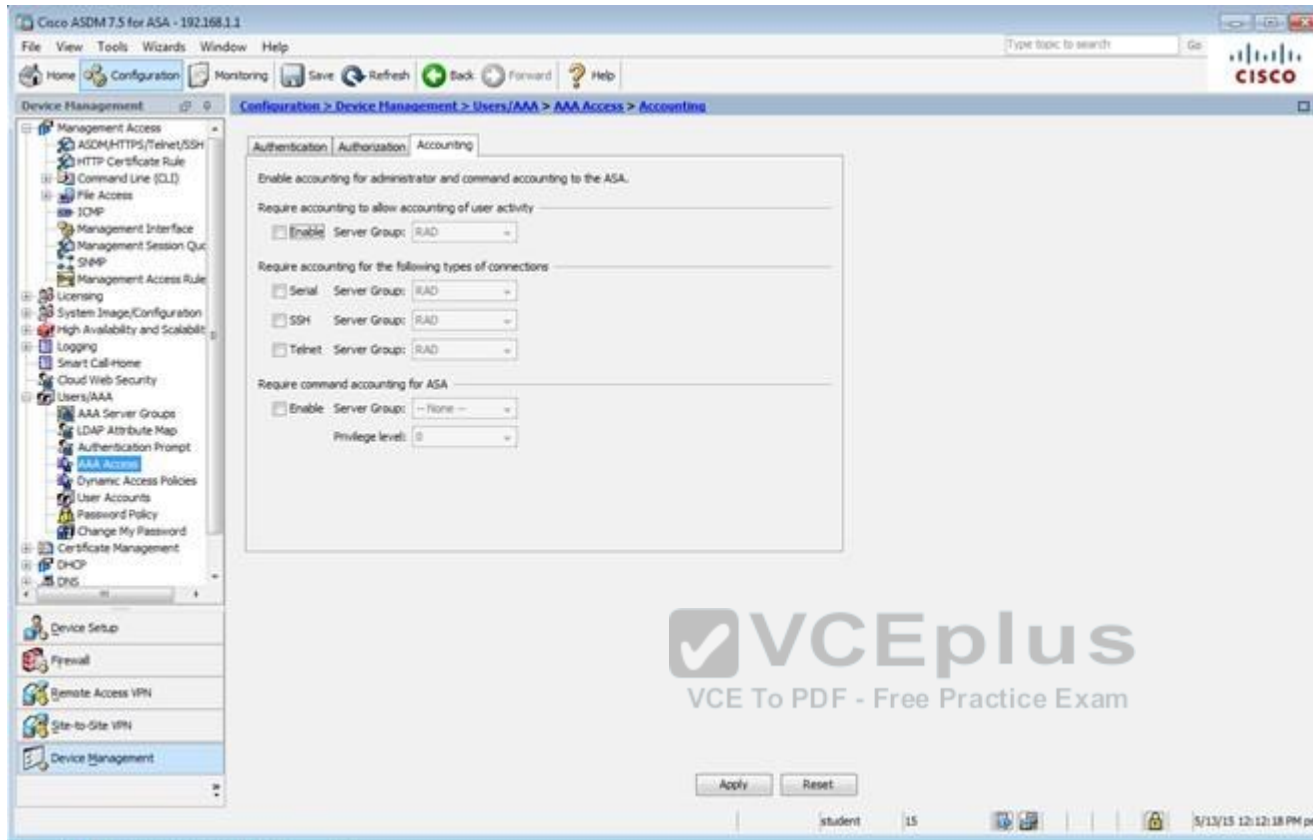


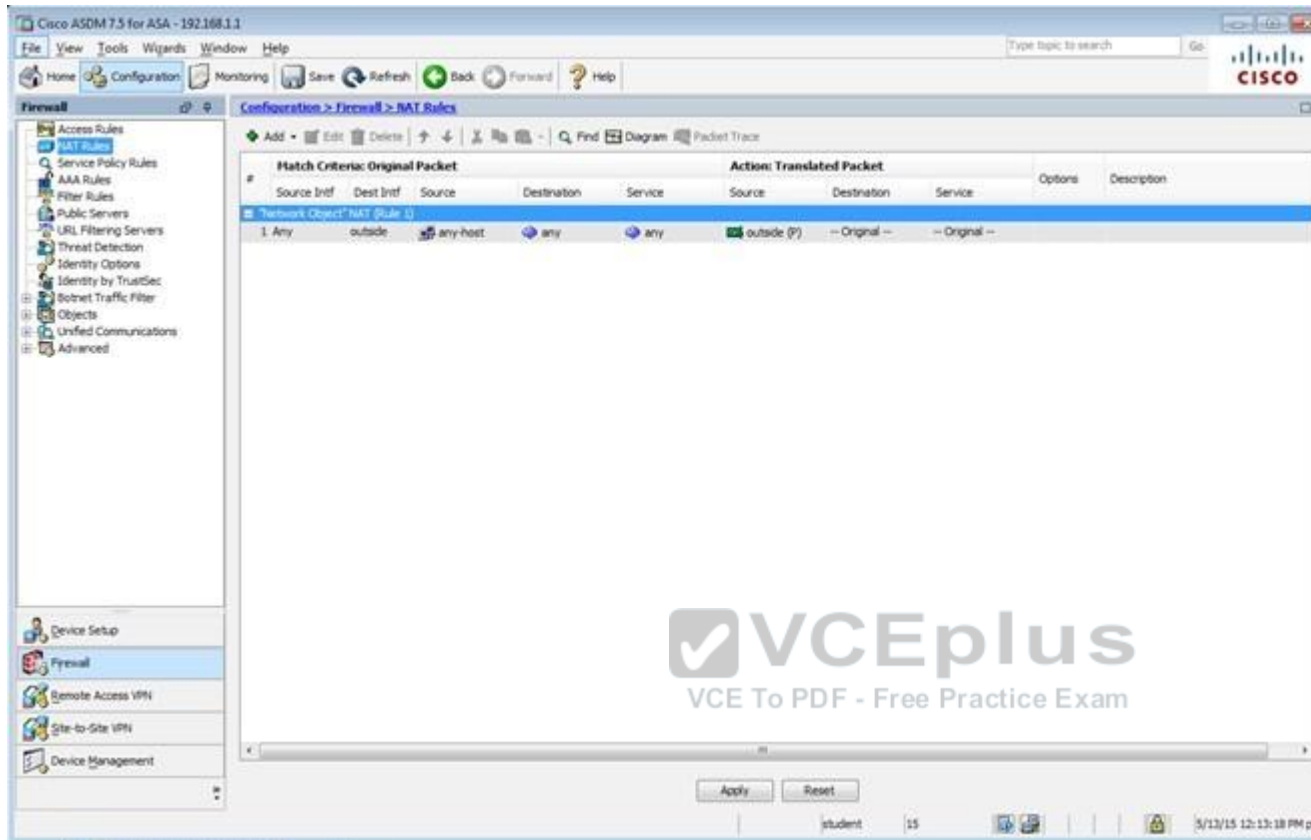


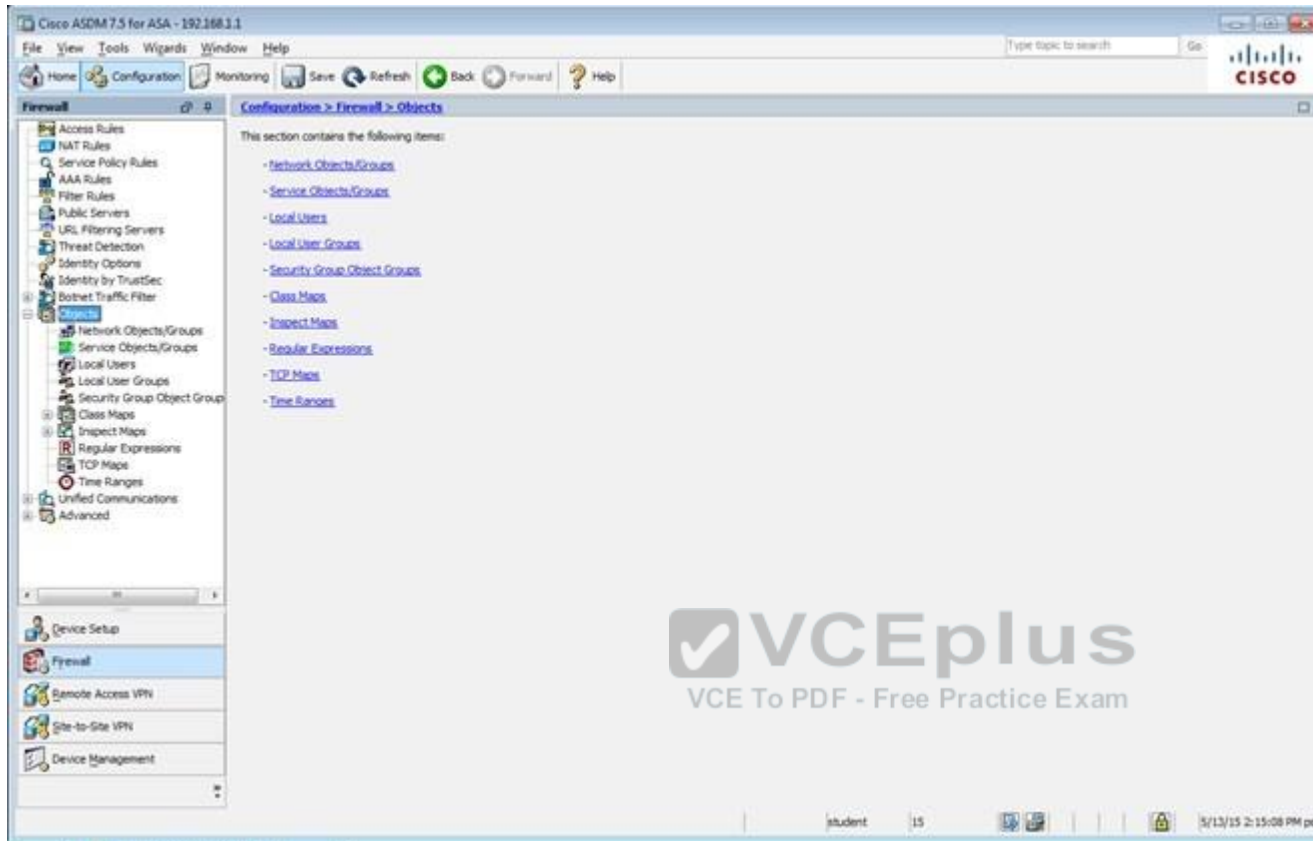












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

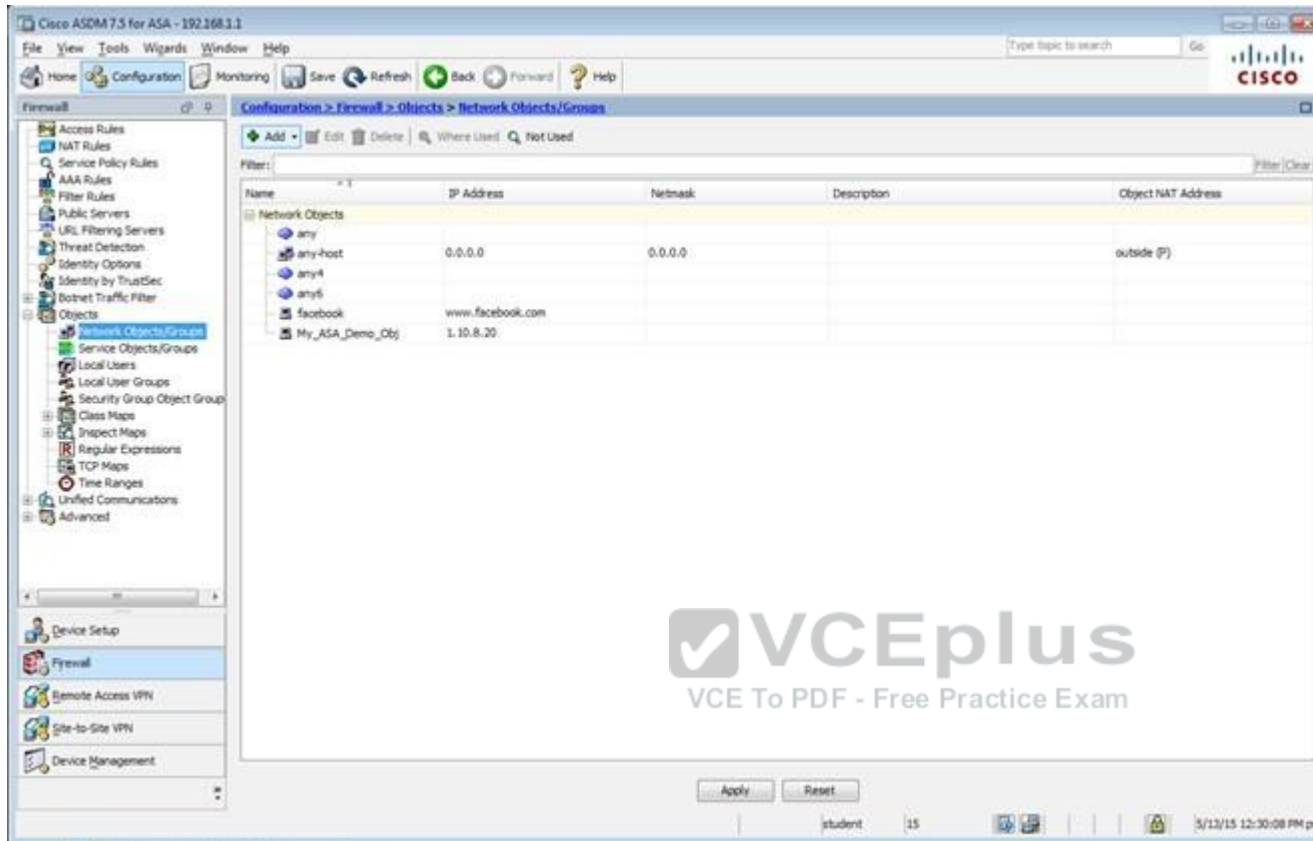
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

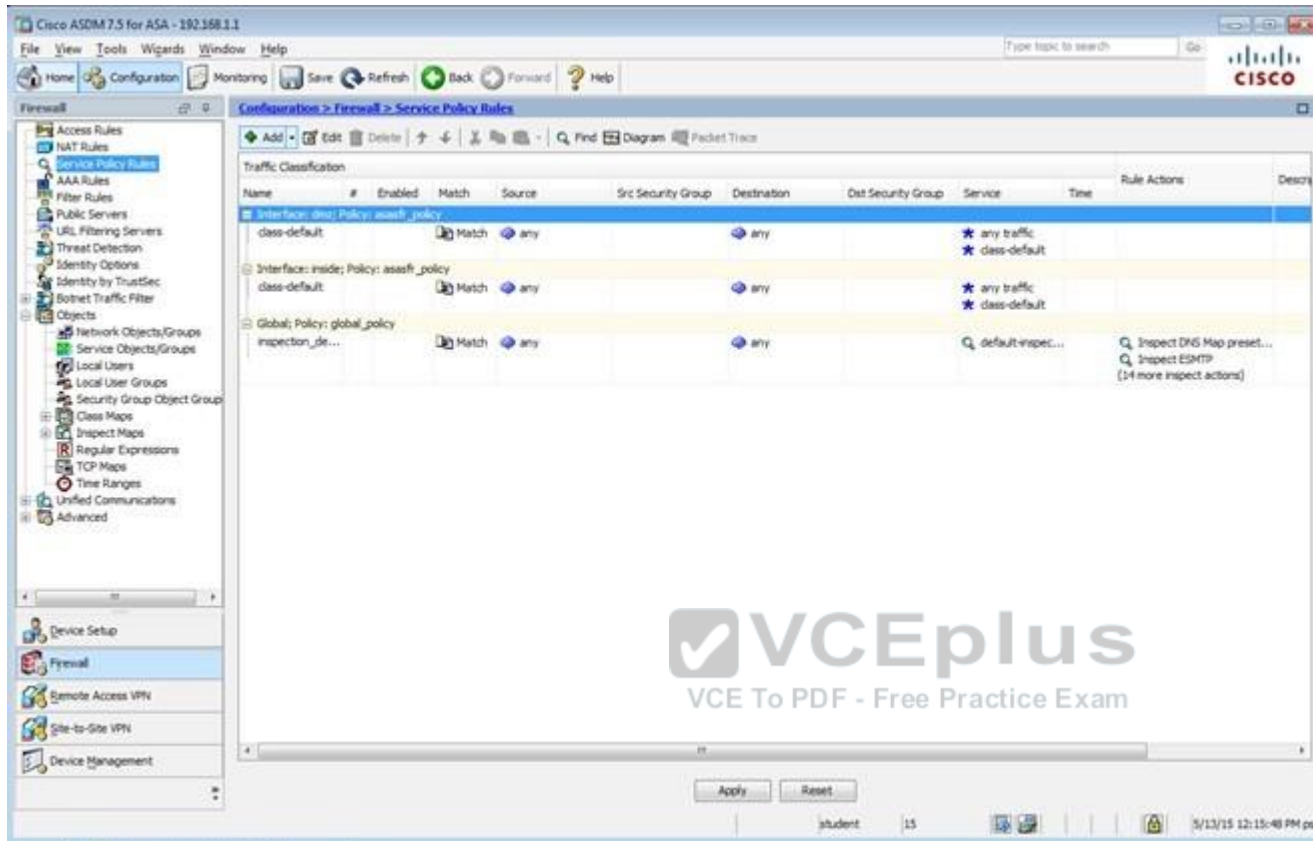
Add Edit Delete

End: [ ] [ ] [ ] Match Case

Apply Reset

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Access Rules

Access Rules

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

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

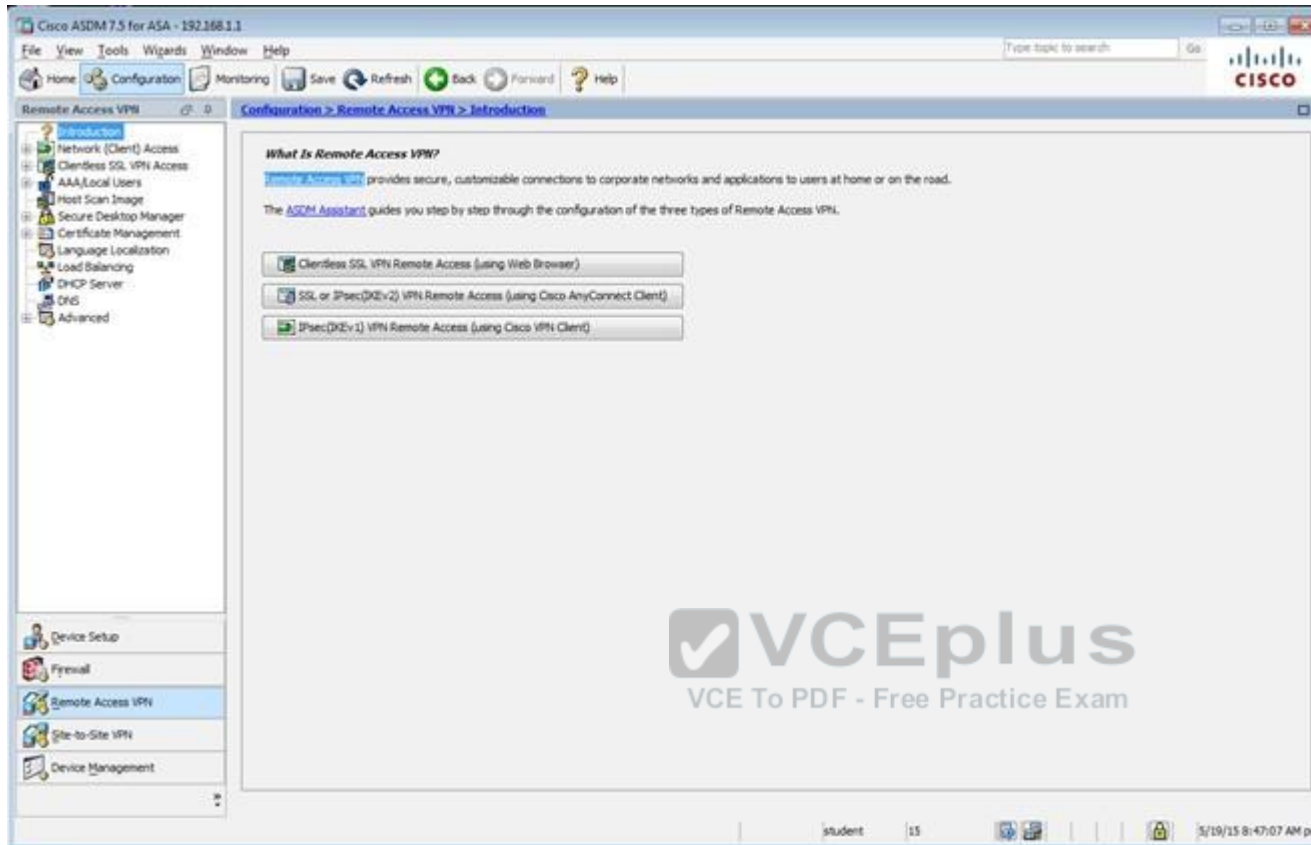
Configuration > Firewall > Access Rules

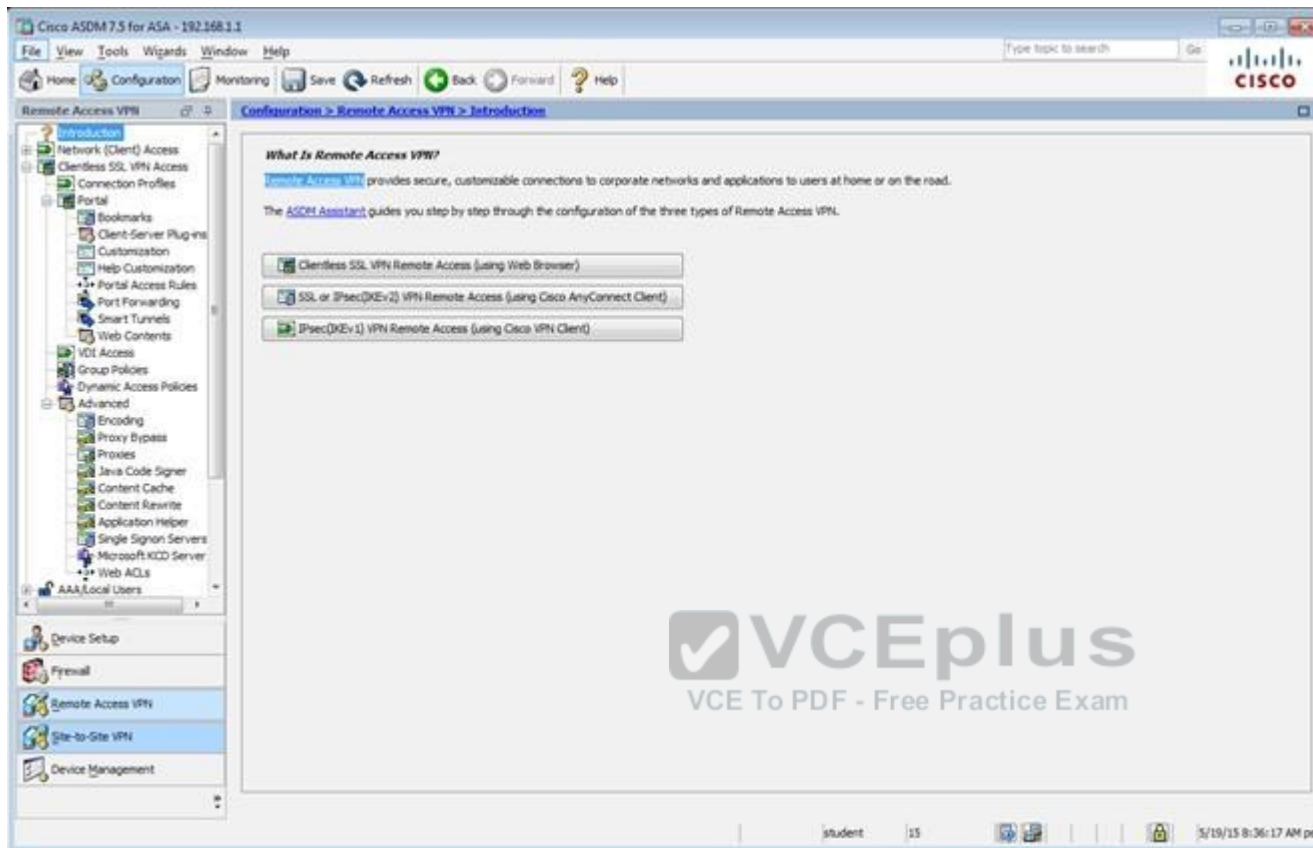
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

| # | Enabled                             | Source Criteria:                    | Destination Criteria: | Service | Action | Hits  | Logging |
|---|-------------------------------------|-------------------------------------|-----------------------|---------|--------|-------|---------|
|   |                                     | Source                              | Destination           |         |        |       |         |
| 1 | <input checked="" type="checkbox"/> | any                                 | Any less secure ne... | HTTP    | Permit |       |         |
| 2 | <input checked="" type="checkbox"/> | inside (1 implicit rule)            | any                   | HTTP    | Permit | 54... |         |
| 3 | <input checked="" type="checkbox"/> | any                                 | any                   | HTTP    | Permit |       |         |
| 4 | <input checked="" type="checkbox"/> | outside (0 implicit incoming rules) | any                   | HTTP    | Permit |       |         |
| 5 | <input checked="" type="checkbox"/> | inside (0 implicit incoming rules)  | any                   | HTTP    | Permit |       |         |
| 6 | <input checked="" type="checkbox"/> | outside (0 implicit incoming rules) | any                   | HTTP    | Permit |       |         |
| 7 | <input checked="" type="checkbox"/> | Global (1 implicit rule)            | any                   | HTTP    | Deny   |       |         |

Apply Reset Advanced...

student 15 5/13/15 12:28:58 PM pst





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

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

Connection Profiles

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

Add Edit Delete Find: Match Case

| Name               | Enabled                             | Aliases | Authentication Method | Group Policy       |
|--------------------|-------------------------------------|---------|-----------------------|--------------------|
| DefaultRAGroup     | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultGroupPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultGroupPolicy |
| clientless         | <input checked="" type="checkbox"/> | test    | AAA(LOCAL)            | Sales              |

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

Name: clientless  
Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

☐ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add - Delete (The table is in-line editable.)

| Alias | Enabled                             |
|-------|-------------------------------------|
| test  | <input checked="" type="checkbox"/> |

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add - Delete (The table is in-line editable.)

| URL                        | Enabled                             |
|----------------------------|-------------------------------------|
| https://209.165.201.2/test | <input checked="" type="checkbox"/> |

You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Interface-Specific Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL |
|-----------|--------------|-------------------|
|-----------|--------------|-------------------|

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Secondary Authentication Server Group

Server Group: -- None -- Manage...

☐ Use LOCAL if Server Group fails

☐ Use primary username (Hide secondary username on login page)

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

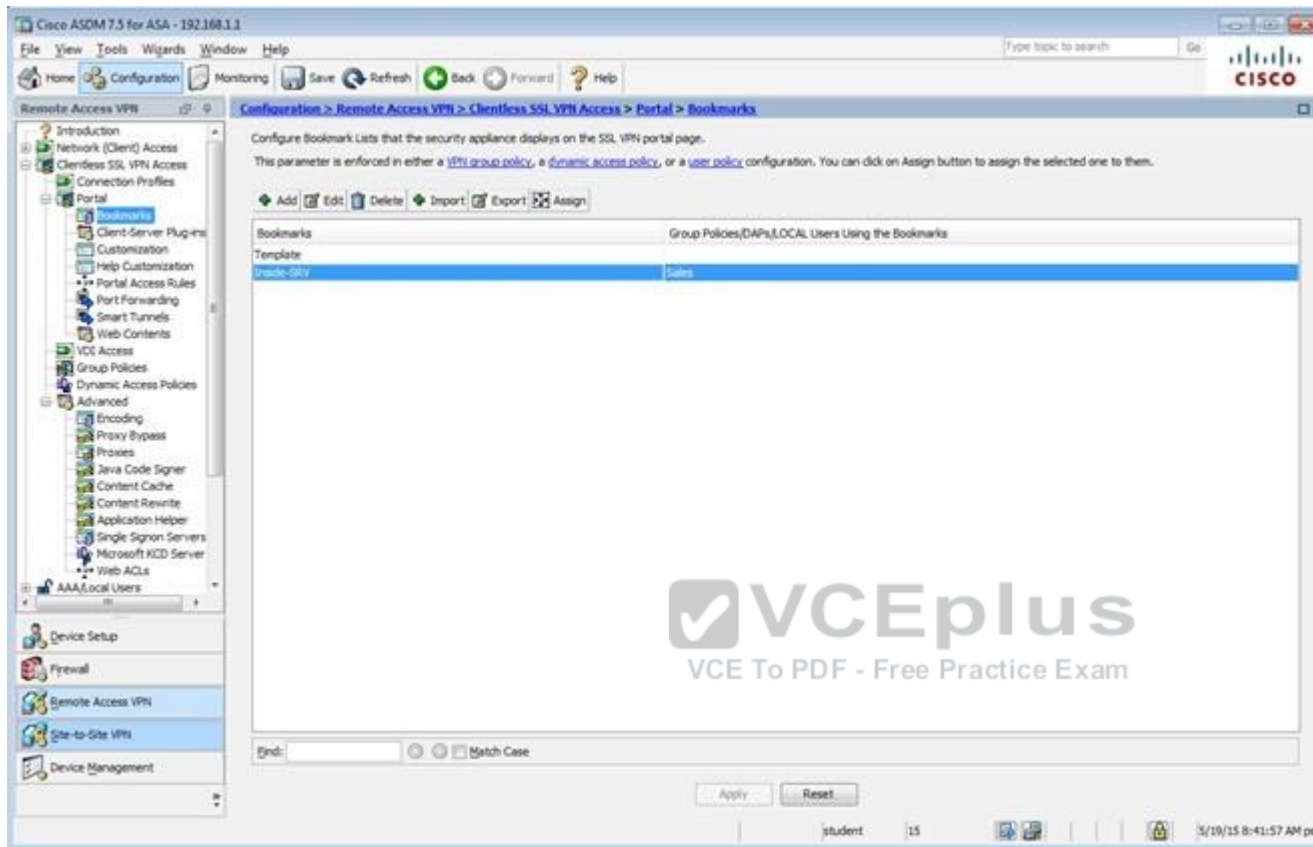
☐ Use the entire DN as the username

☐ Use script to select username

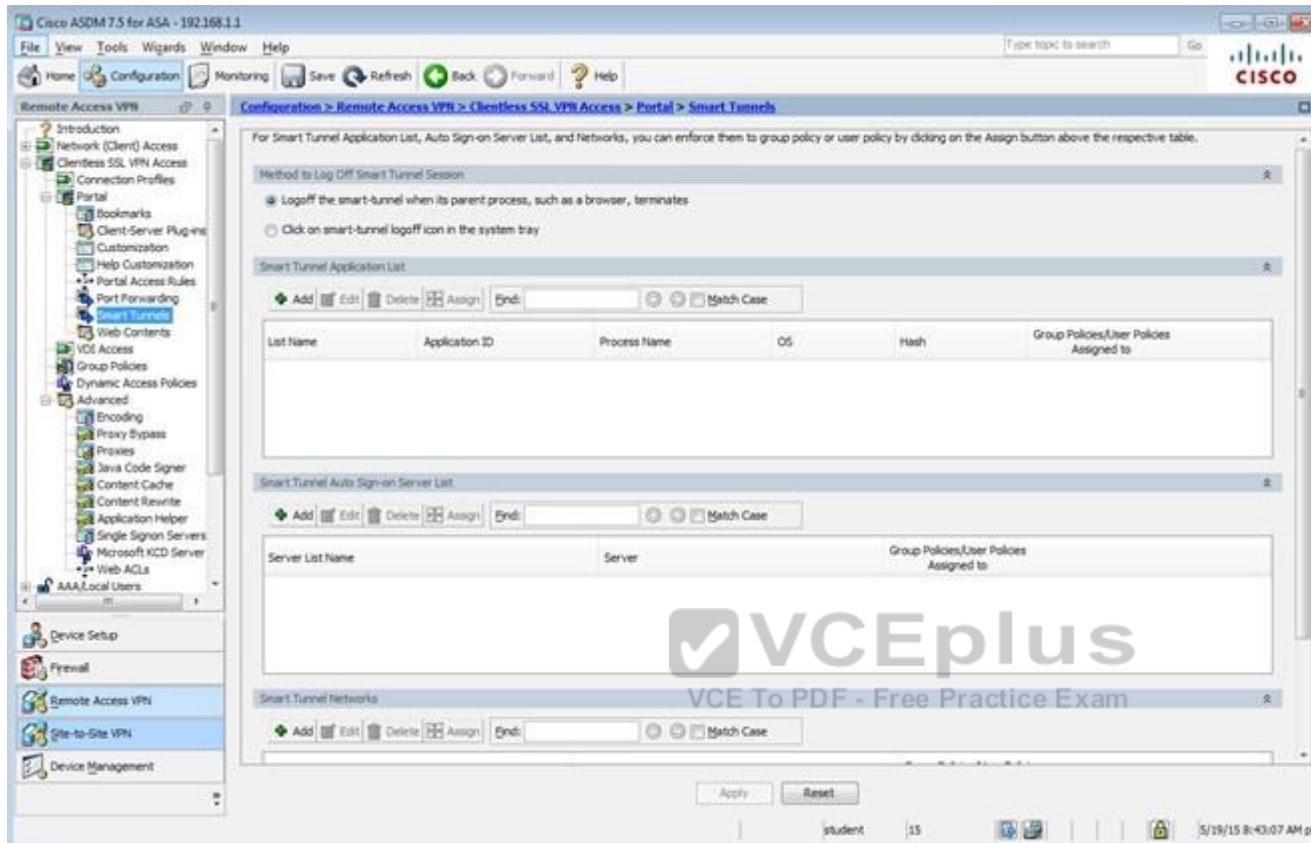
-- None -- + Add Edit Delete

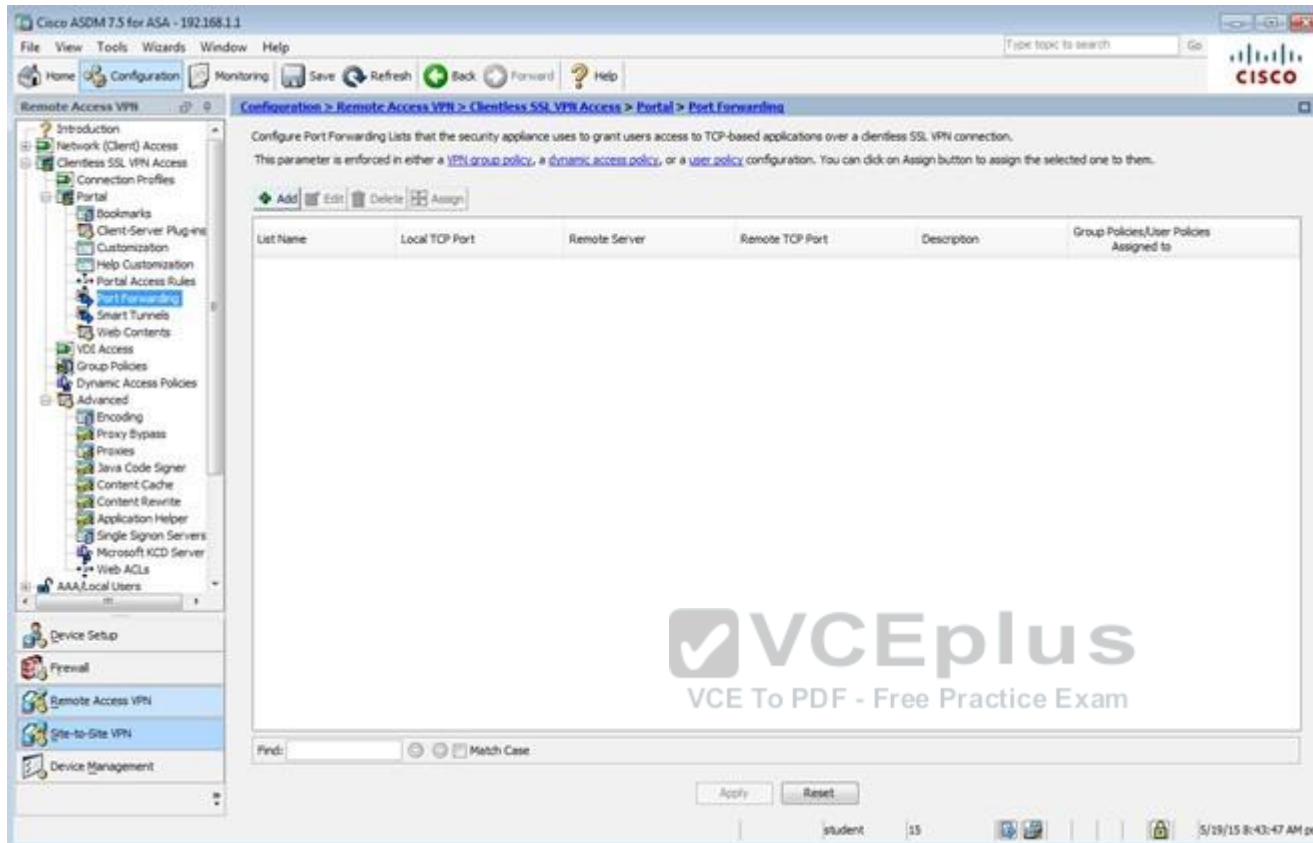
Find:  Next Previous

OK Cancel Help









The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' expanded, showing 'Clientless SSL VPN Access' and 'Group Policies'. The main pane is titled 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies'. It contains a description of VPN group policies and a table of existing policies.

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

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

Buttons: Add, Edit, Delete, Assign

| Name                                | Type     | Tunneling Protocol               | Connection Profiles/Users Assigned To                 |
|-------------------------------------|----------|----------------------------------|---|
| client                              | Internal | ssl-clientless                   | clientless  |
| DefaultGroupPolicy (System Default) | Internal | kev1:kev2:ssl-clientless/2:ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMPGroup/Def... |

Search bar: Find: [ ] Match Case

Buttons: Apply, Reset

Status bar: student 15 5/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

Tunneling Protocols: ☐ Inherit ☒ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 ☐ IPsec IKEv2 ☐ L2TP/IPsec

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

Find:  ☐ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

Remote Access VPN

- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- Voice Access
- Group Policies
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol                | Connection Profiles/Users Assigned To |
|--------------------------------|----------|-----------------------------------|---------------------------------------|
| Sales                          | Internal | l2l-clientless                    | Sales                                 |
| DfltGrpPolicy (System Default) | Internal | ikev1ikev2ssl-clientless/2ip-ipse | DfltGrpPolicy                         |

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

General  
More Options  
Customization  
Login Setting  
Single Signon  
VDI Access  
Session Settings

Bookmark List: ☐ Inherit  Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit  Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit  Manage...

Tunnel Option:  Manage...

Smart Tunnel Application: ☒ Inherit  Manage...

☐ Smart Tunnel all Applications (This feature only works with Windows platforms)

☐ Auto Start

Auto Sign-on Server: ☒ Inherit  Manage...

Windows Domain Name (optional):

Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find:  ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

**General**  
Servers  
Advanced

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None-- Manage...

Access Hours: --Unrestricted-- Manage...

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

Maximum Connect Time: ☒ Unlimited ☐ minutes

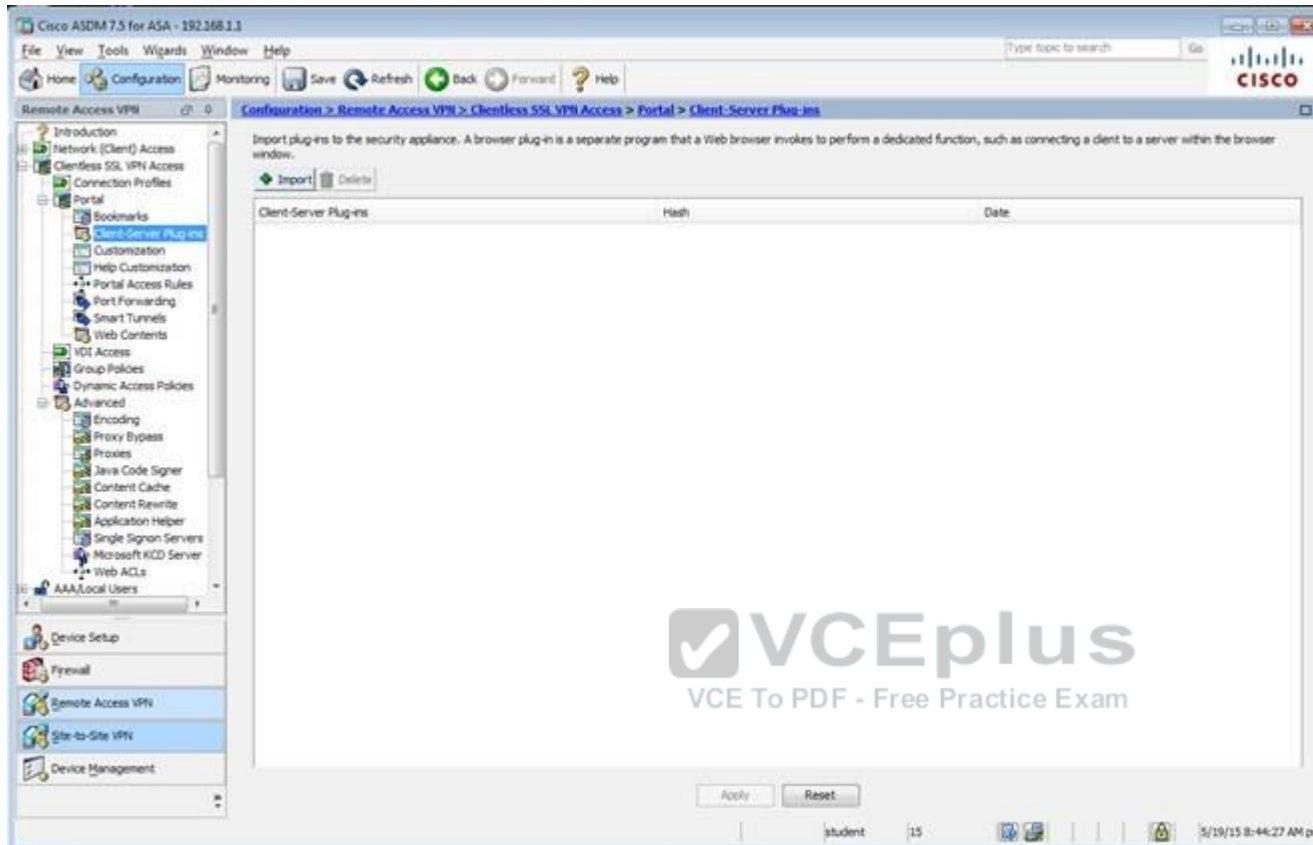
Idle Timeout: ☐ None ☐ 30 minutes

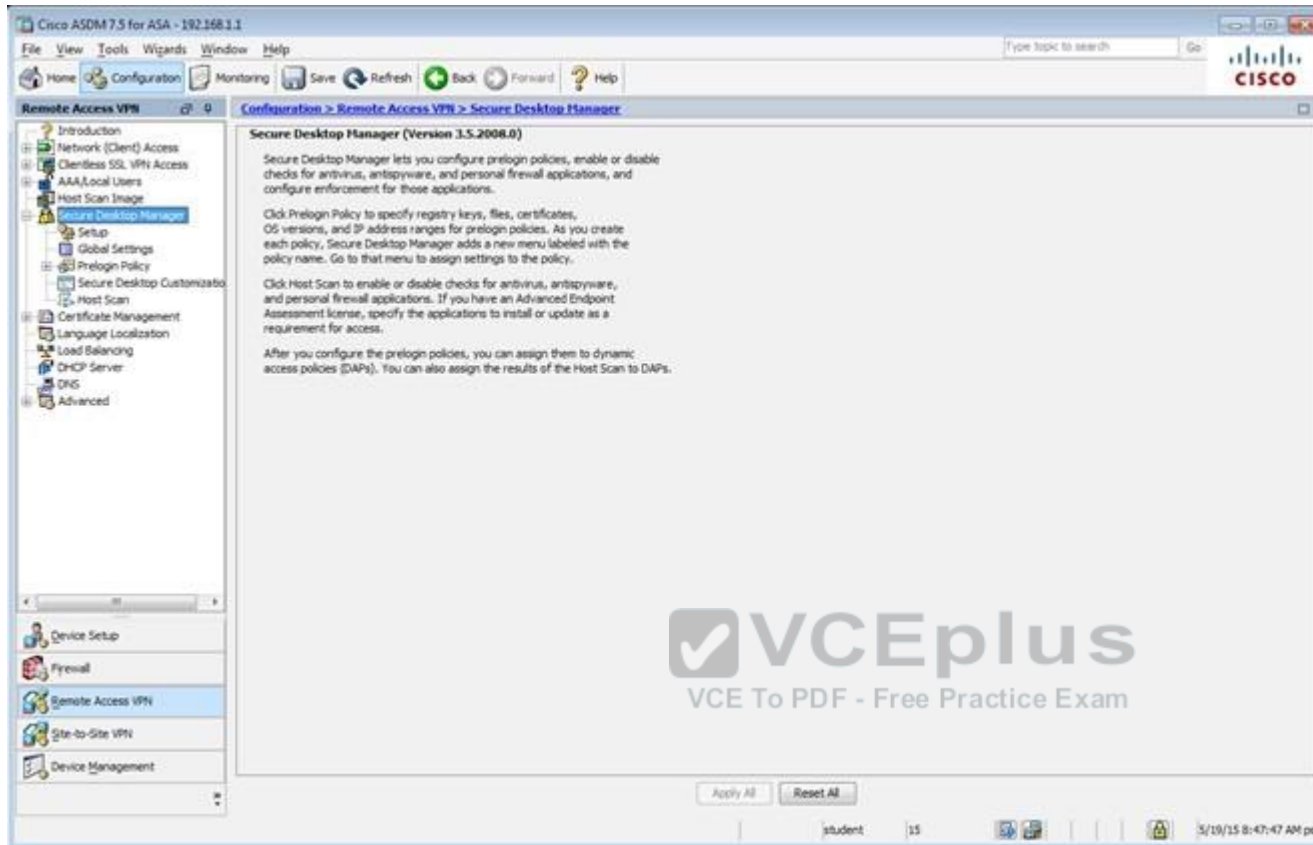
On smart card removal: ☒ Disconnect ☐ Keep the connection

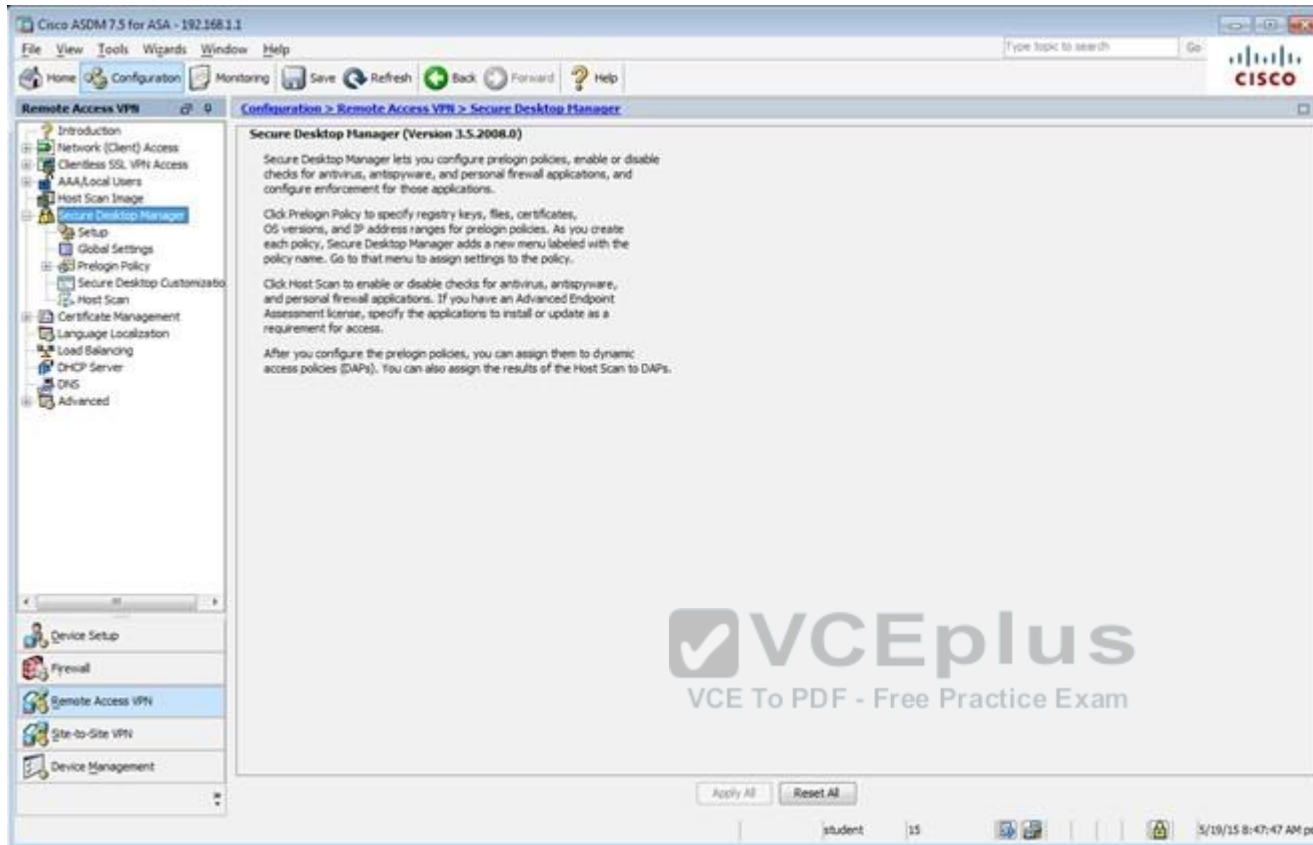
**VCEplus**  
VCE To PDF - Free Practice Exam

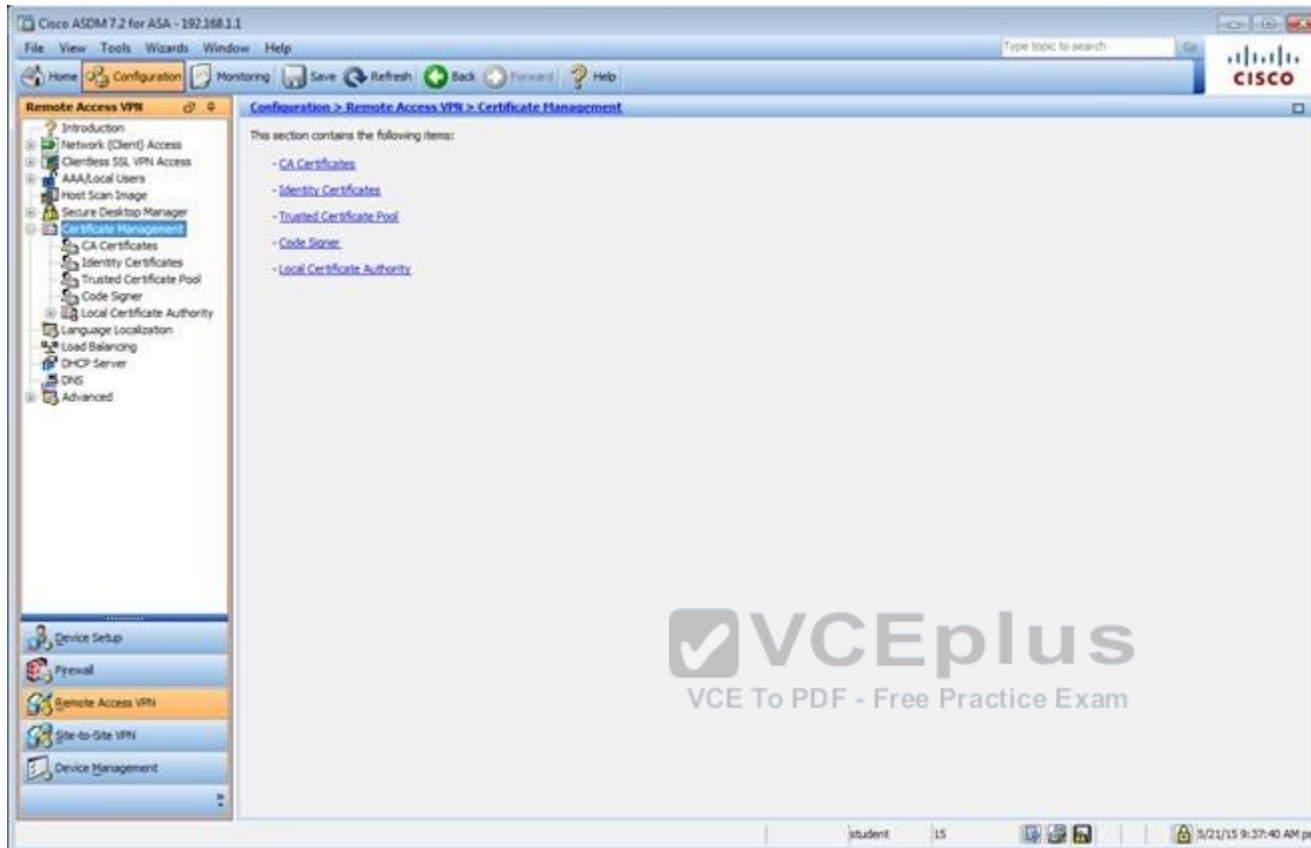
Find: Next Previous

OK Cancel Help

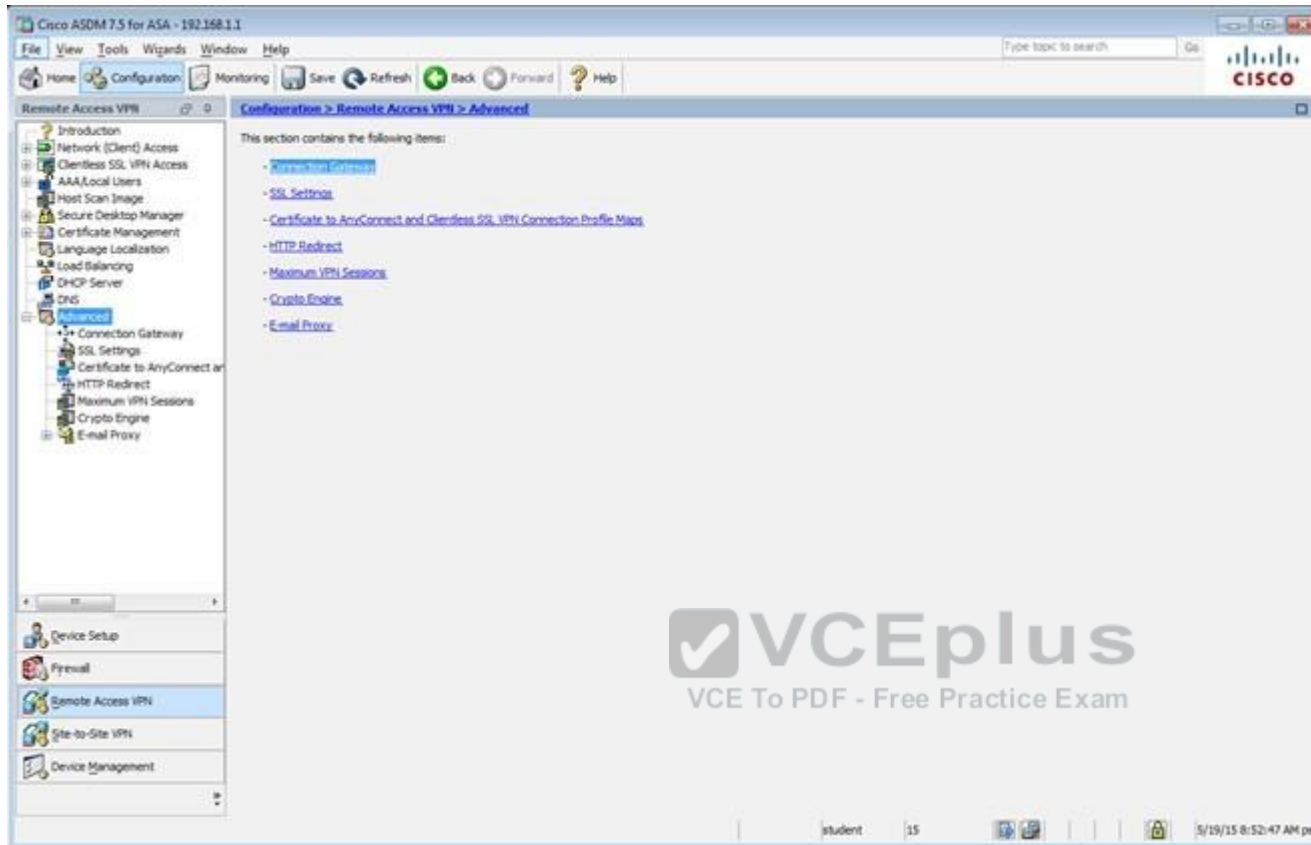


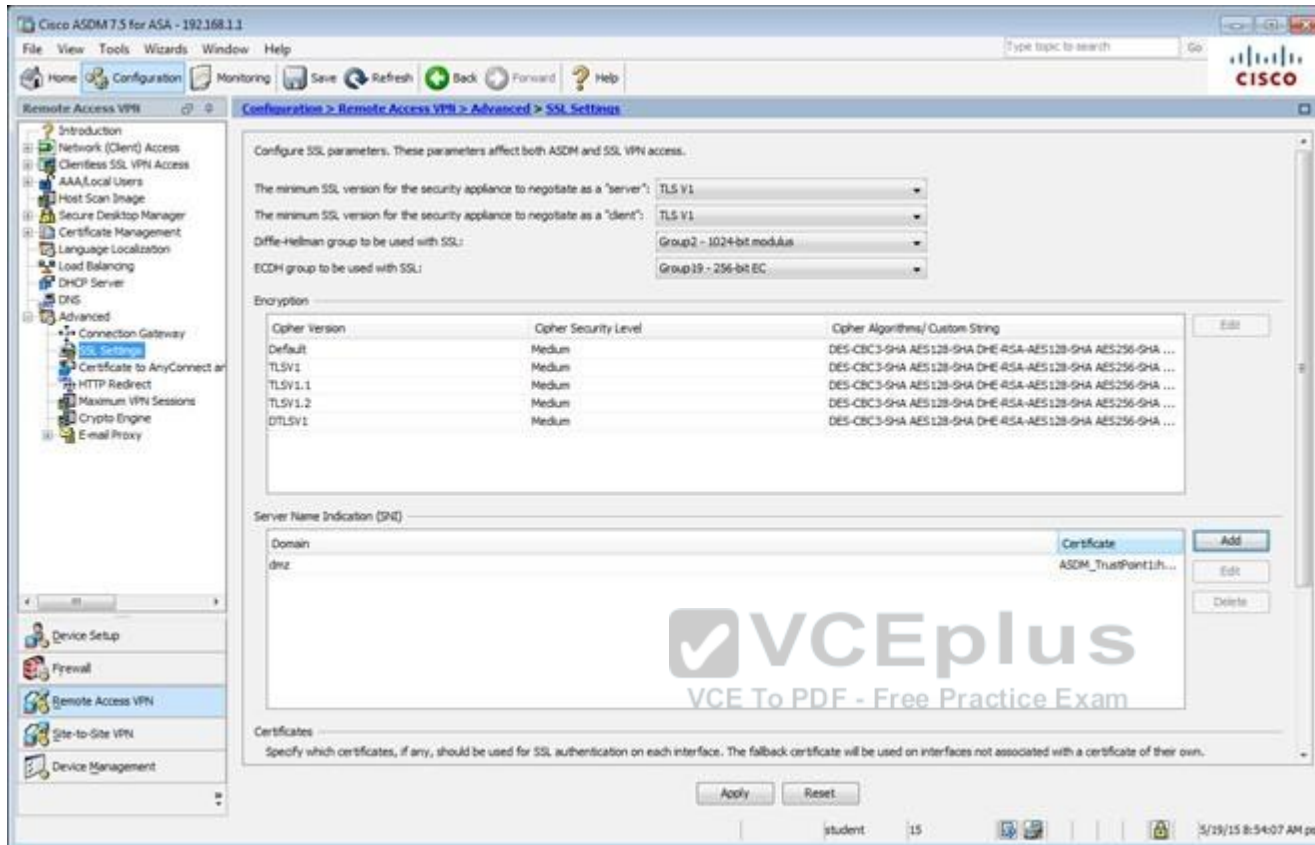


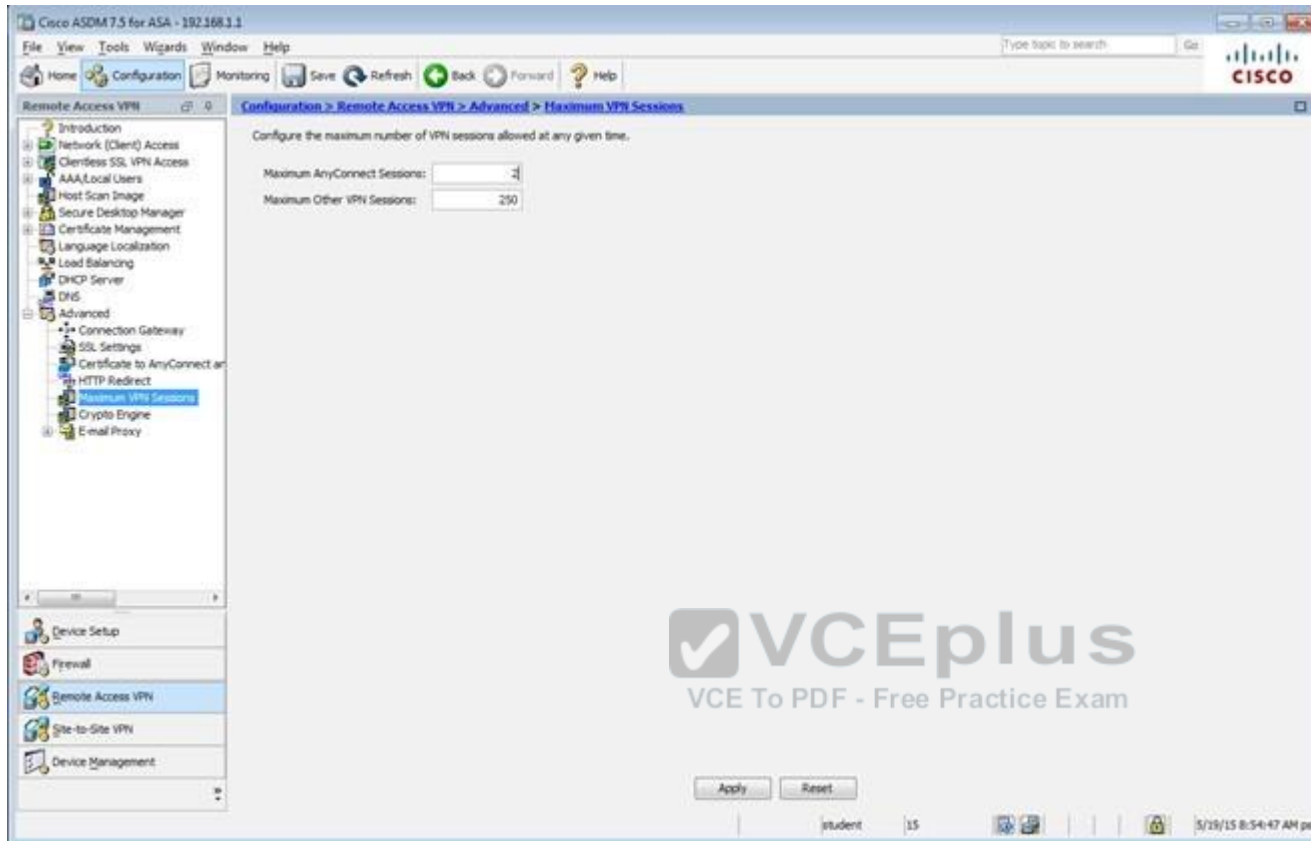


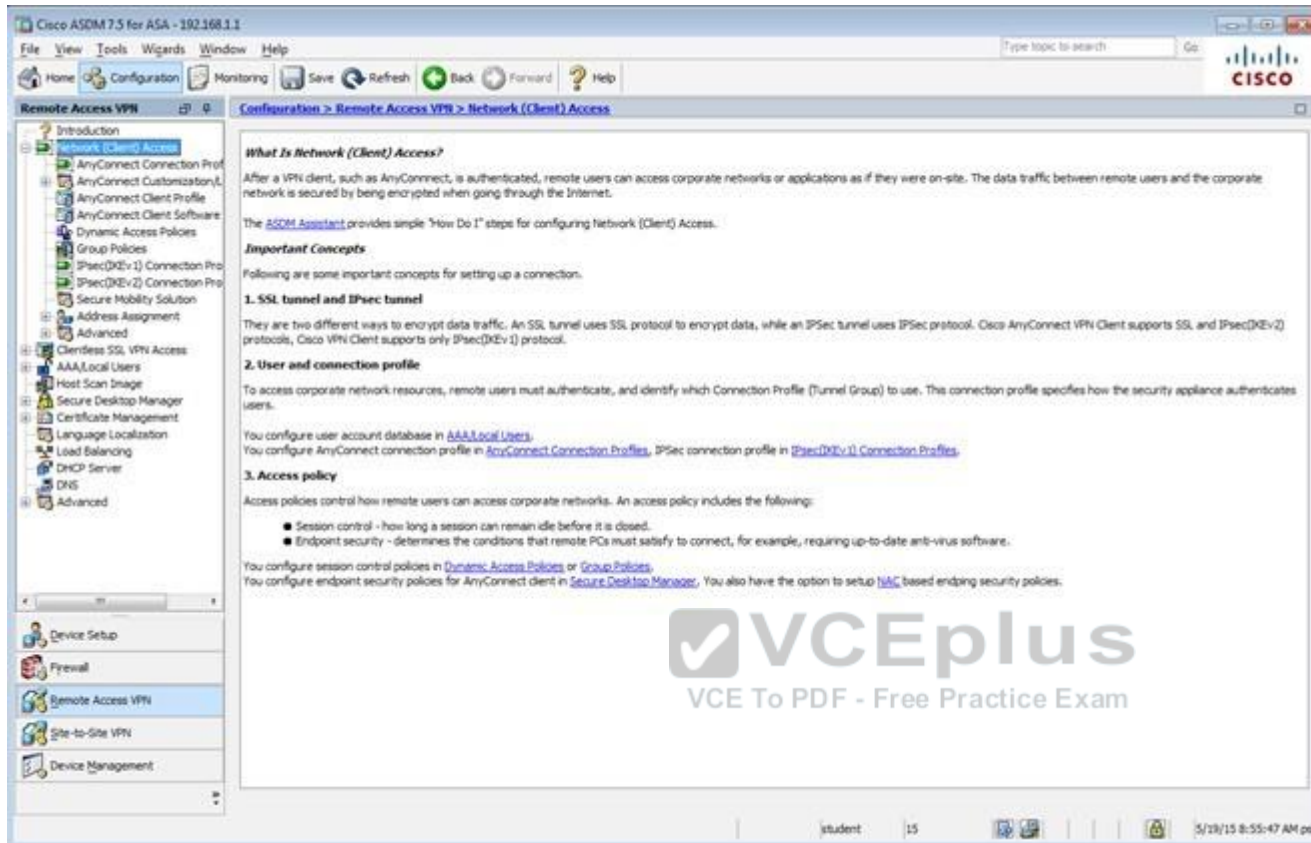


The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with categories like Remote Access VPN, Configuration, Monitoring, and Advanced. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It displays a table with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. A single entry is visible: Issued To: hostname-17-ASA.sec..., Issued By: hostname-17-ASA.sec..., Expiry Date: 11:10:33 pet Dec 20 2024, Associated Trustpoints: ASDM\_TrustPoint1, Usage: General Purpose, Public Key Type: RSA (2048 bits). To the right of the table are buttons: Add, Show Details, Delete, Export, and Install. Below the table is a search bar with 'Find:' and a 'Match Case' checkbox. Further down are 'Certificate Expiration Alerts' settings: 'Send the first alert before: 60 (days)' and 'Repeat Alert Interval: 7 (days)'. Below that is a 'Public CA Enrollment' section with a paragraph of text and a link 'enroll with Entrust...'. At the bottom, there is an 'ASDM Identity Certificate Wizard' section with a paragraph and a 'Launch ASDM Identity Certificate Wizard...' button. The status bar at the bottom shows 'student', '15', and the date/time '5/19/15 8:51:47 AM pet'.









The screenshot displays the Cisco ASDM 7.5 for ASA - 102.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Network (Client) Access'. It contains the following text:

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

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

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

**1. SSL tunnel and IPsec tunnel**  
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.

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

You configure user account database in [AAA Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).

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

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

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

The bottom of the window shows a status bar with 'student', '15', and a timestamp '5/28/15 8:55:47 AM pet'.

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol                  | Connection Profiles/Users Assigned To                  |
|--------------------------------|----------|-------------------------------------|--|
| Sales                          | Internal | ssl-clientless                      | clientless   |
| DefaultPolicy (System Default) | Internal | (rev 1)rev 2:ssl-clientless/2ip-sec | DefaultPolicyGroupDefaultPolicyGroupDefaultPolicyGroup |

Find: Match Case

Apply Reset

student 15 5/21/15 10:17:10 AM pst

Edit Internal Group Policy: DftrGpPolicy

**General**

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

Name: DftrGpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: -- None -- Manage...

NAC Policy: -- None -- Manage...

Access Hours: -- Unrestricted -- Manage...

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

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

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles

Introduction  
Network (Client) Access  
AnyConnect Connection Profile  
AnyConnect Customization...  
AnyConnect Client Profile  
AnyConnect Client Software  
Dynamic Access Policies  
Group Policies  
IPsec(IKv1) Connection Profile  
IPsec(IKv2) Connection Profile  
Secure Mobility Solution  
Advanced  
Clientless SSL VPN Access  
AAA/Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DHG  
Advanced

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

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

| Name              | IPsec Enabled                       | L2TP/IPsec Enabled                  | Authentication Server Group | Group Policy  |
|-------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultVRAGroup   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| DefaultIKEV1Group | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| Clientless        | <input type="checkbox"/>            | <input type="checkbox"/>            | LOCAL                       | Sales         |

Find:  Match Case

Apply Reset

student 15 5/19/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Widgets Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

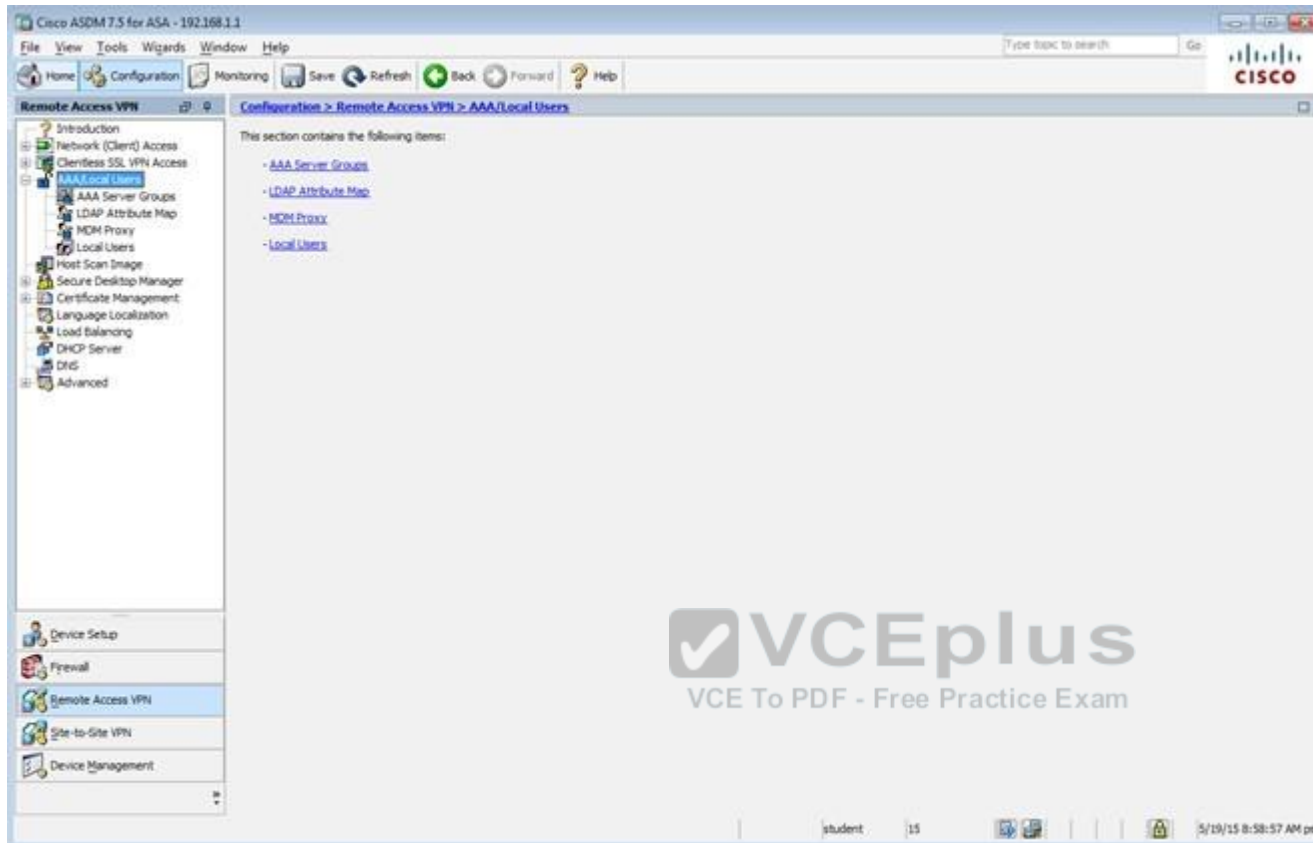
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name            | SSL Enabled                         | IPsec Enabled                       | Aliases | Authentication Method | Group Policy  |
|-----------------|-------------------------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| DefaultEAPGroup | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| Clientless      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | yes     | SSL (OCSP)            | Clientless    |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction  
Network (Client) Access  
Clientless SSL VPN Access  
AAA/Local Users  
AAA Server Groups  
LDAP Attribute Map  
MDM Proxy  
Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DNS  
Advanced

Create entries in the ASA local user database.

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

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

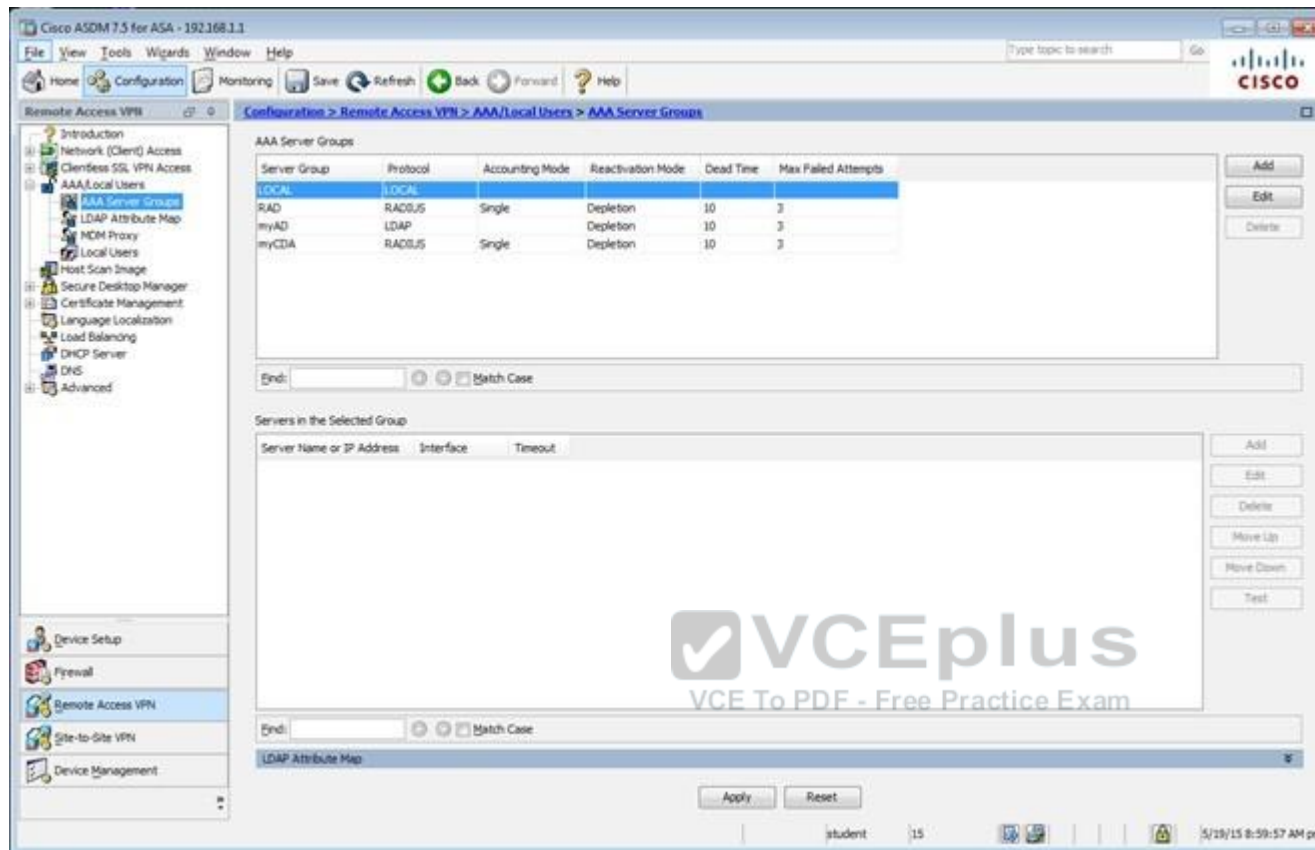
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

Add Edit Delete

Find: Match Case

Apply Reset

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



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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

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

**Virtual Terminal**

Home Configuration Monitoring Save Refresh Back Forward Help

**Remote Access VPN**

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

**Access Interfaces**

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

**Login Page Setting**

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

**Connection Profiles**

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

+ Add Edit Delete Find: Match Case

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

## QUESTION 66

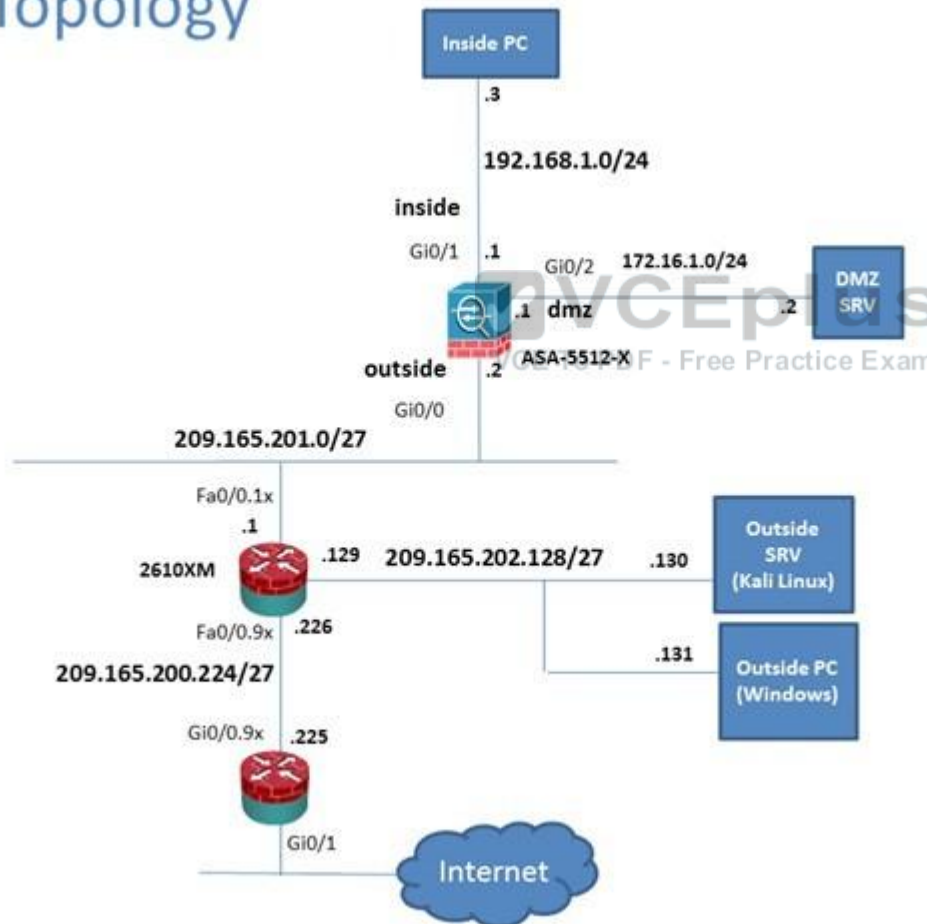
### Scenario

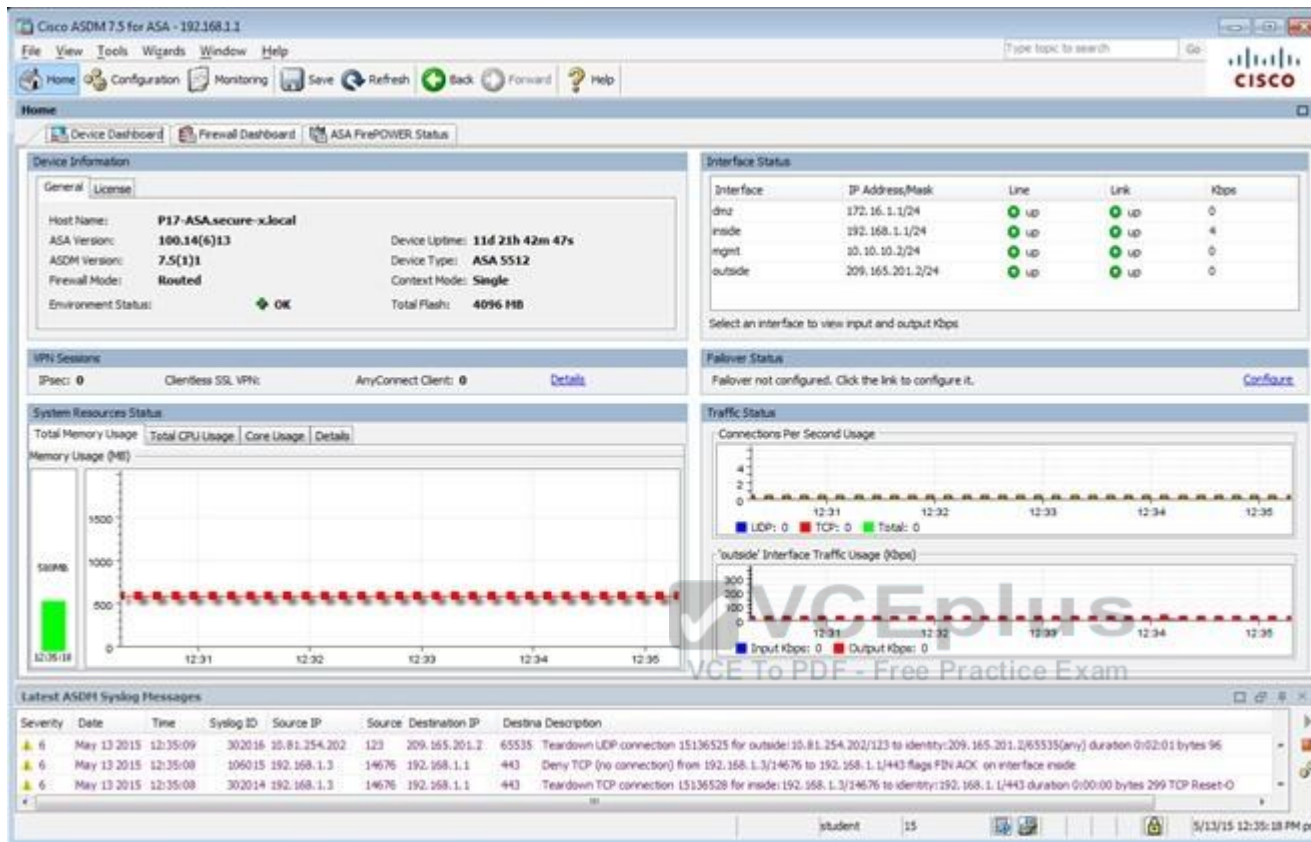
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

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

## Lab Topology





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address    | MAC Address    | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside   | 209.165.201.1 | 000c.3014.3820 | No        |
| inside    | 192.168.1.4   | 0050.5633.3333 | No        |
| inside    | 192.168.1.3   | 0050.5611.1111 | No        |
| inside    | 192.168.1.2   | 0050.5622.2222 | No        |
| inside    | 192.168.1.56  | 0050.5692.5c7b | No        |
| inside    | 192.168.1.55  | 0006.85e5.98f3 | No        |
| dmz       | 172.16.1.2    | 0050.5644.4444 | No        |
| mgmt      | 10.10.10.1    | 000c.3014.3820 | No        |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/ISAK Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions

Clientless SSL VPN

VPN Connection Graphs

WSA Sessions

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Monitoring > VPN > VPN Statistics > Sessions

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

Filter By: Clientless SSL VPN All Sessions Filter

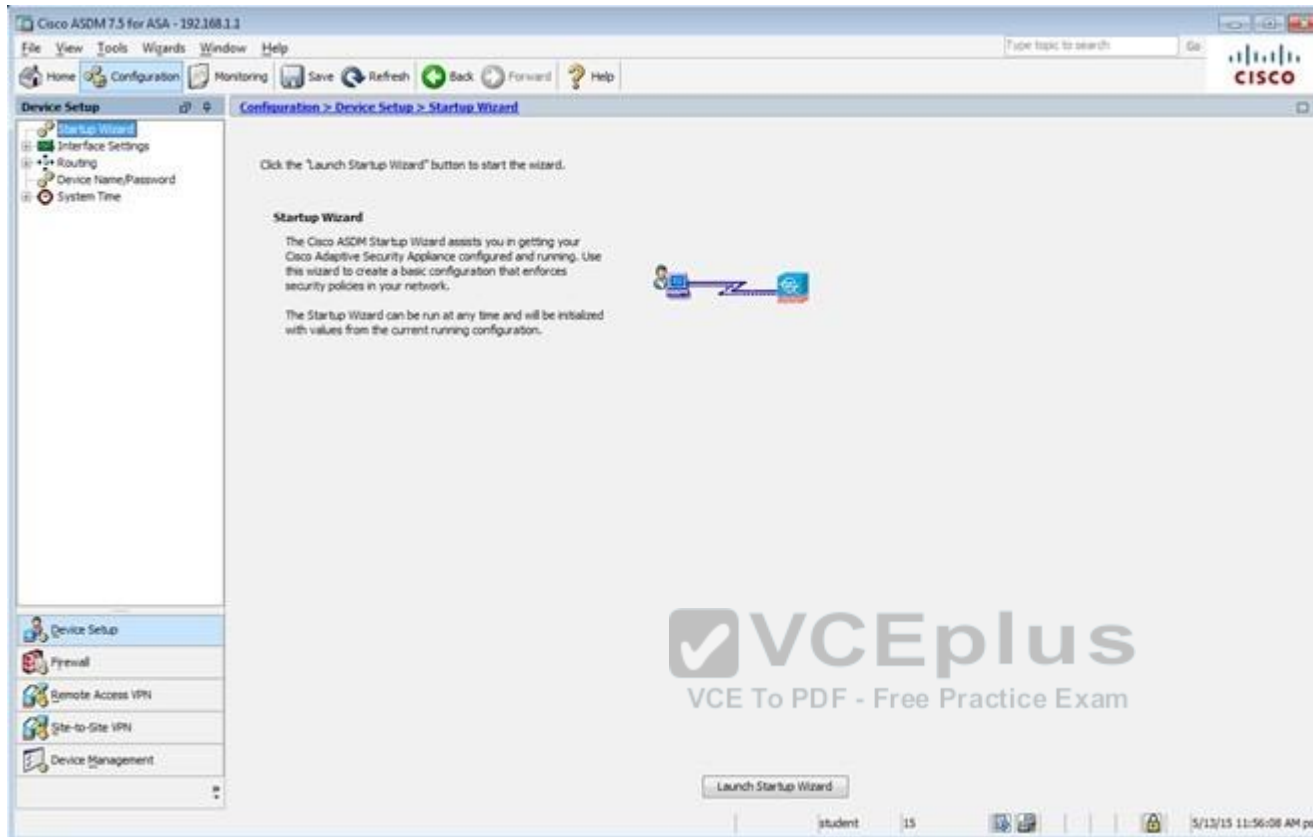
| Username | IP Address      | Group Policy | Connection Profile | Protocol   | Encryption         | Login Time                   | Duration   | Bytes Tx | Bytes Rx |
|----------|-----------------|--------------|--------------------|------------|--------------------|------------------------------|------------|----------|----------|
| student  | 209.165.202.131 | Sales        | Clientless         | Clientless | Clientless (13AC4) | 08:03:46 sat Thu May 21 2013 | 2h:09m:19s | 316774   | 41833    |

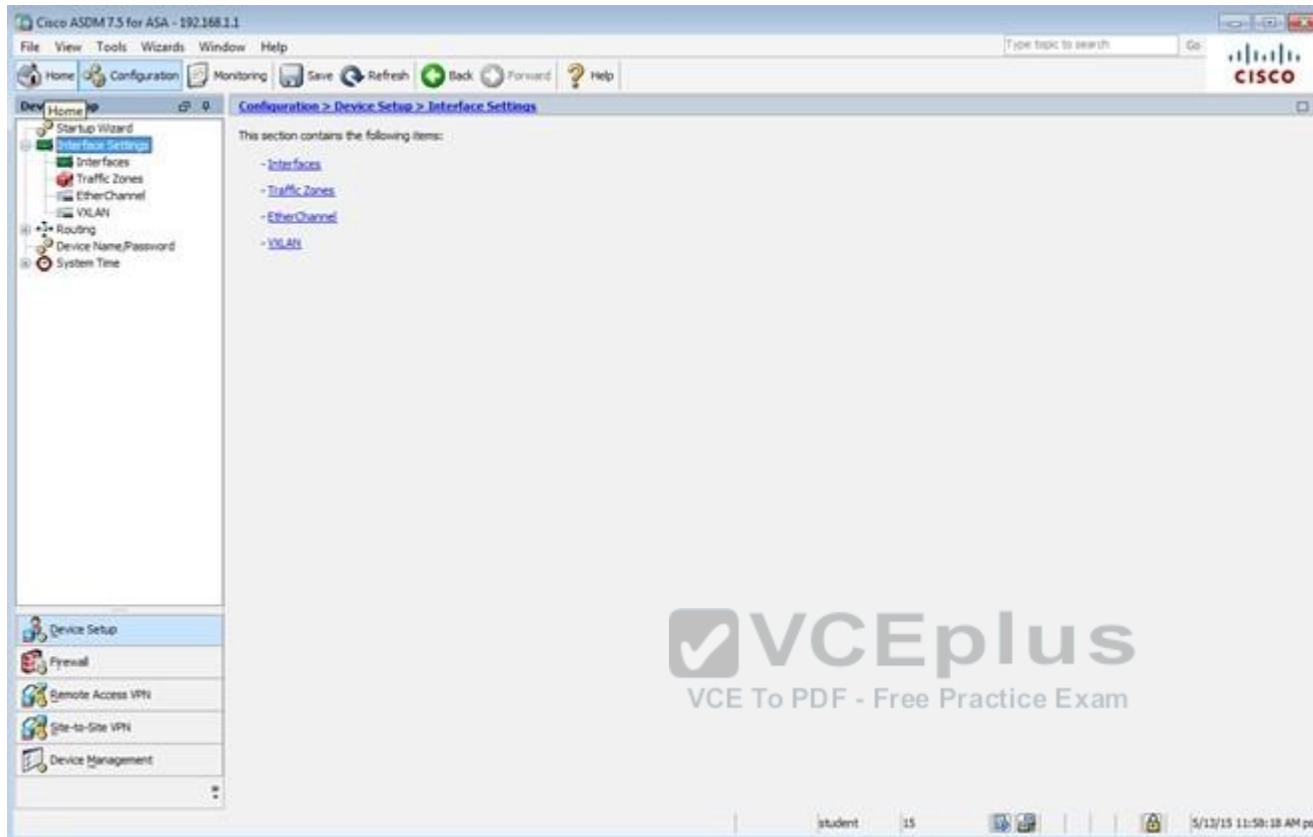
Details Logout Ping

Refresh

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

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Type topic to search Go

CISCO

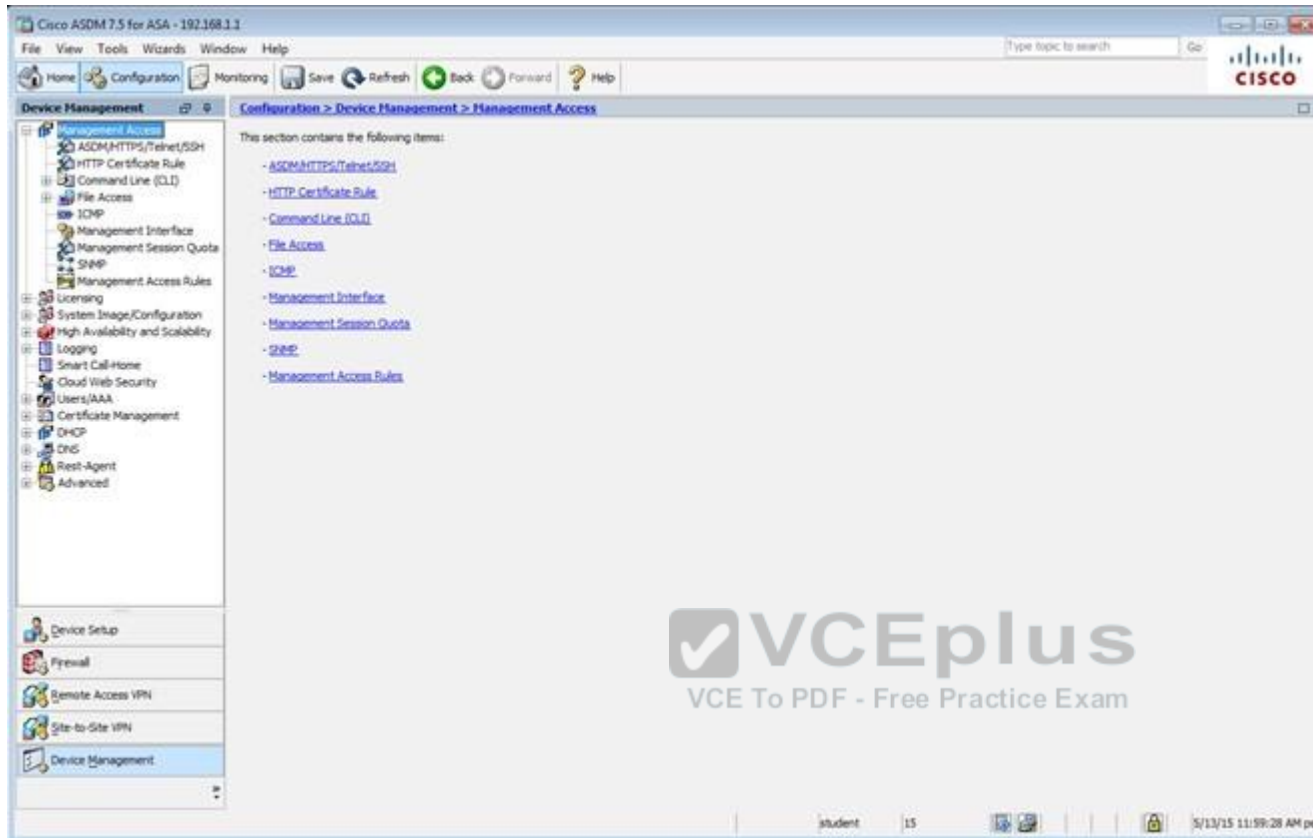
Device Setup

Configuration > Device Setup > Interface Settings > Interfaces

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

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

Student 15 5/13/15 12:42:48 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

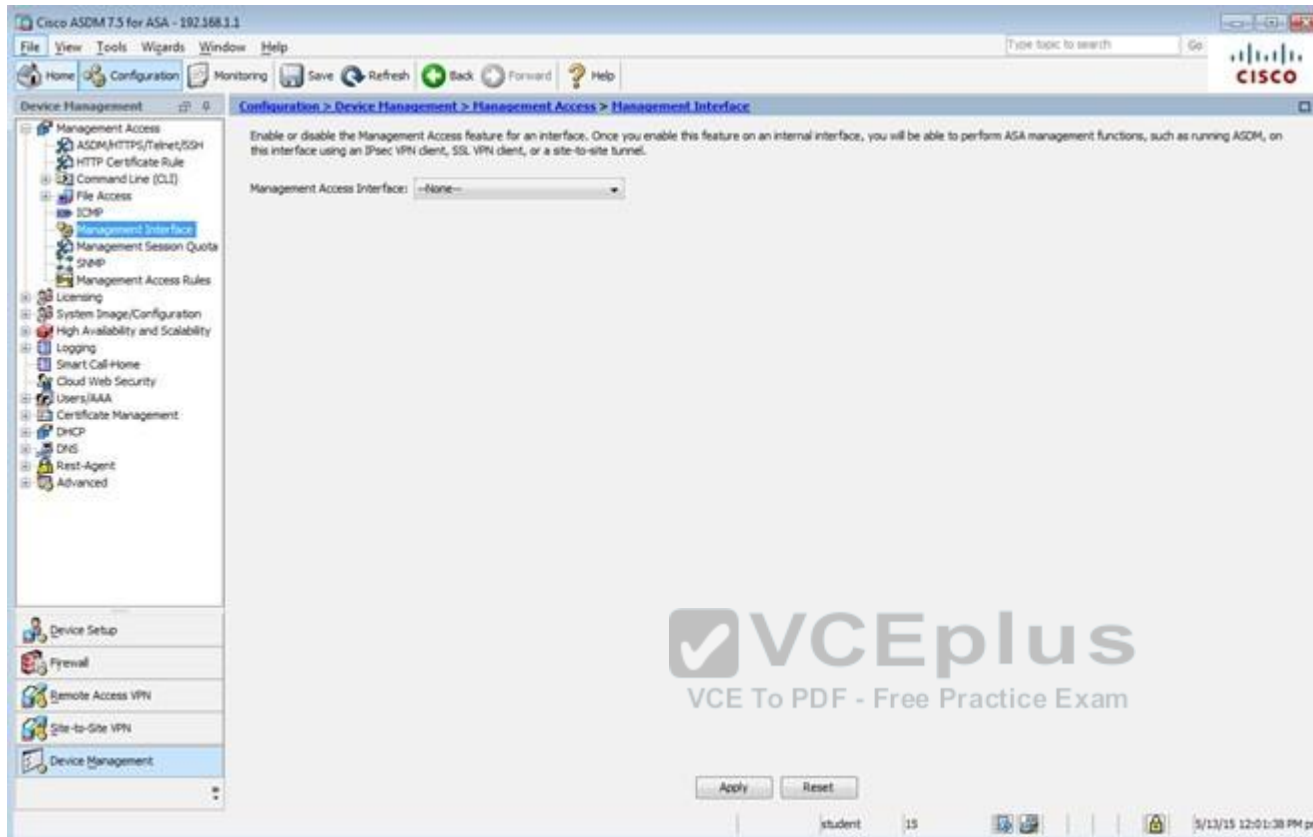
Allowed SSH Version(s): 1 & 2

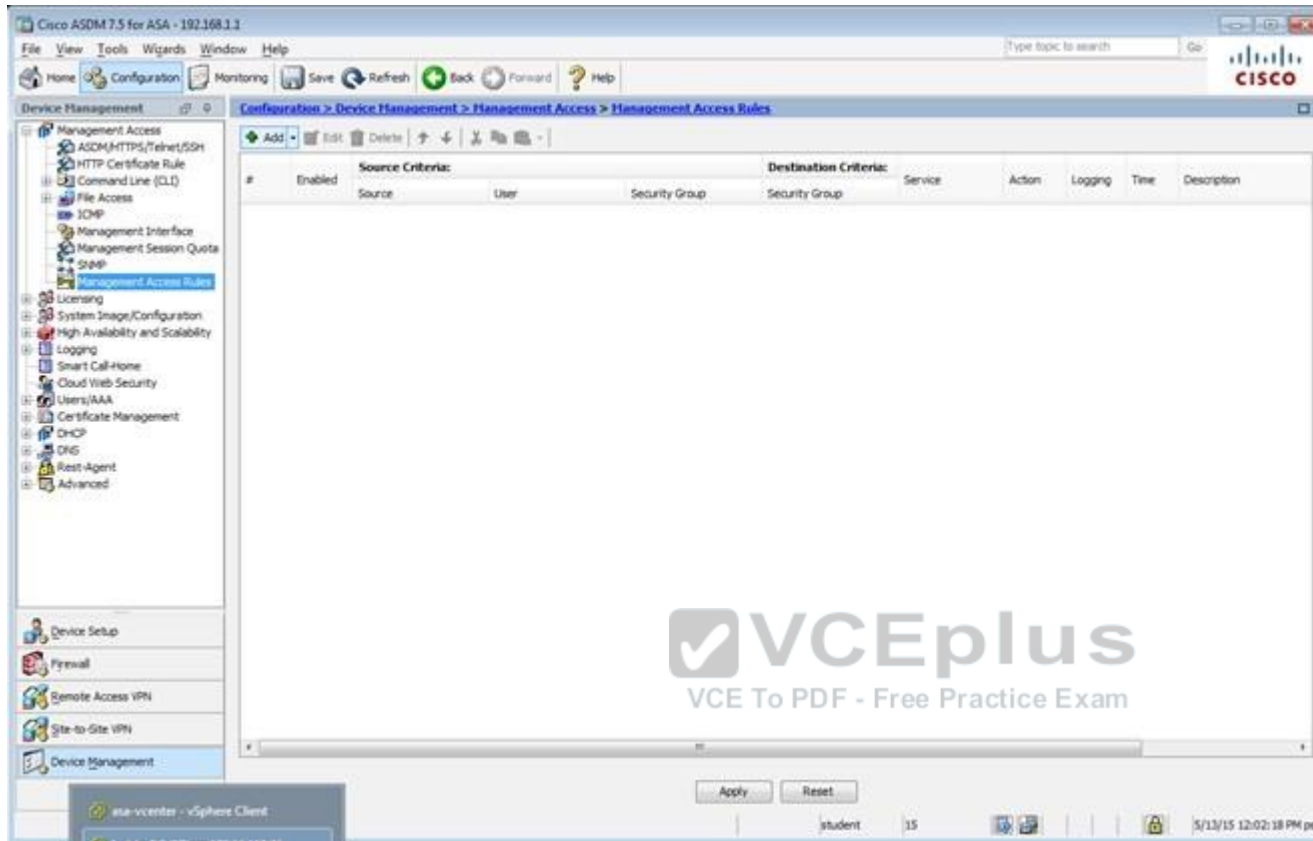
SSH Timeout: 5 minutes

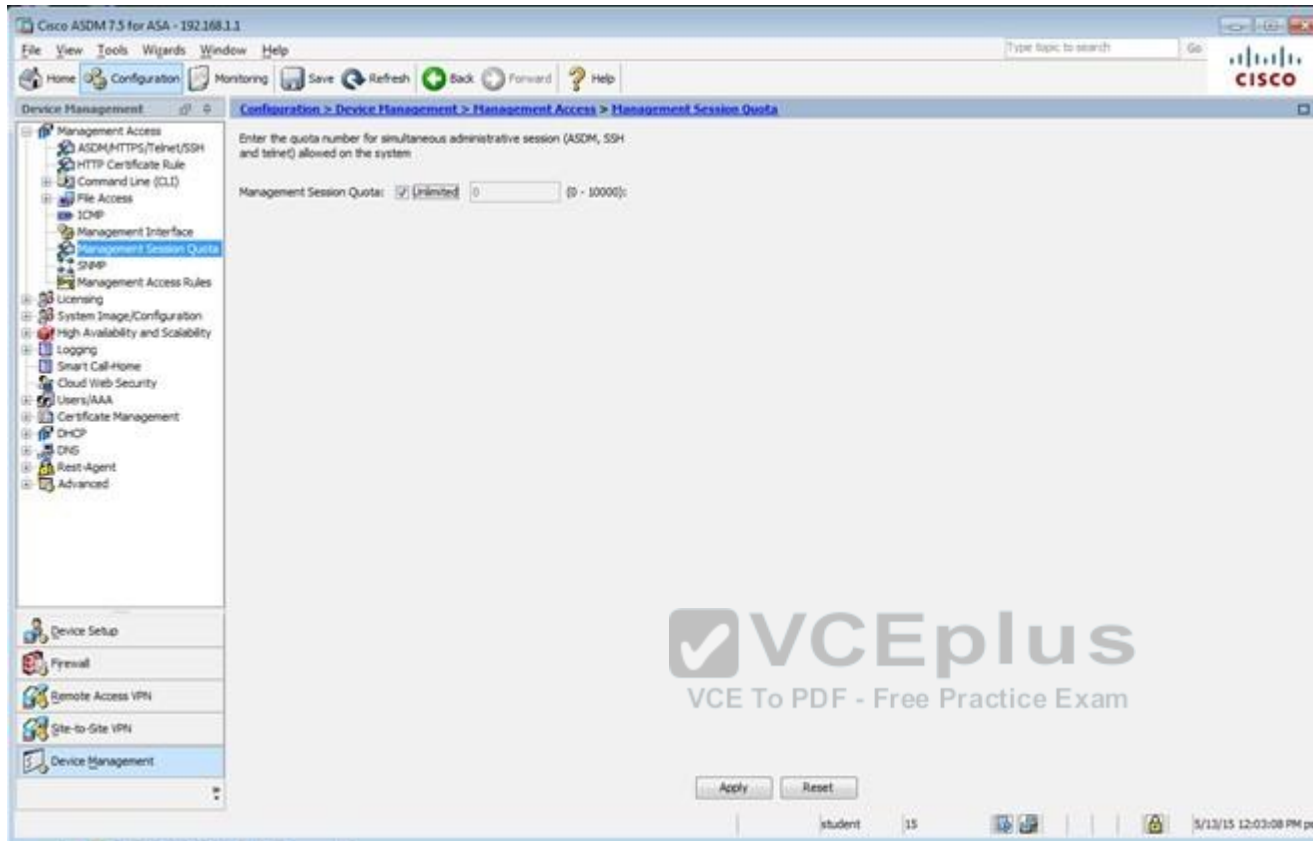
DH Key Exchange: ☒ Group 1 ☐ Group 14

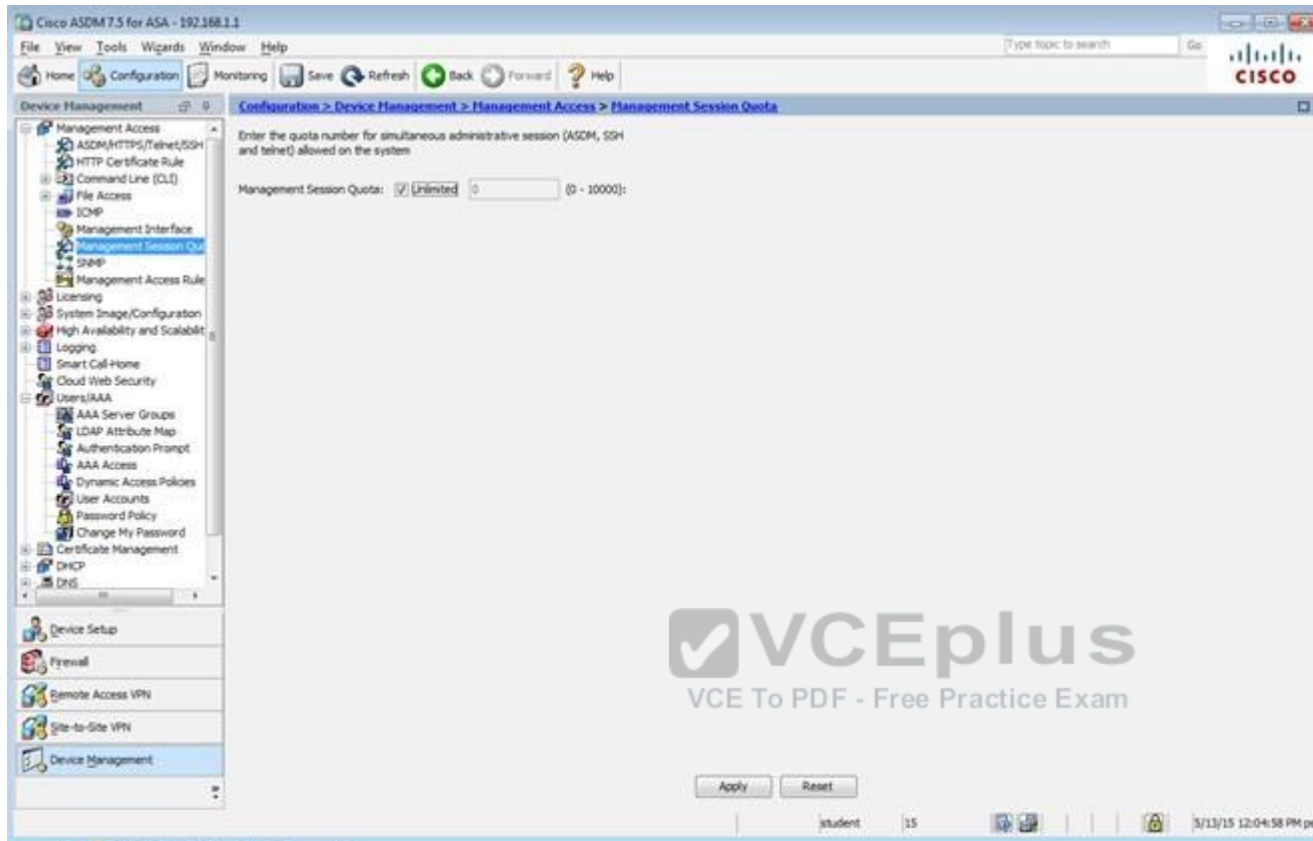
Apply Reset

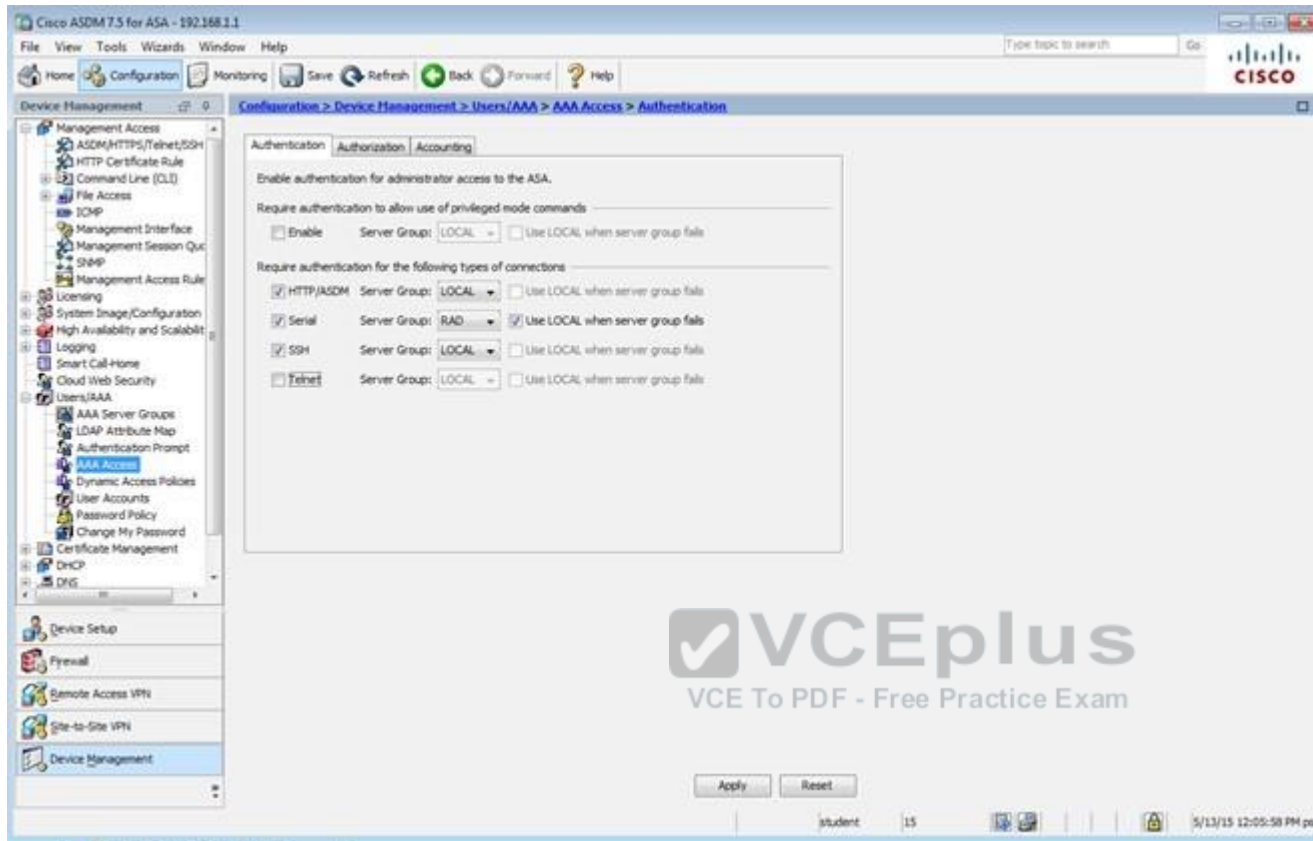
student 15 5/13/15 12:00:38 PM pst

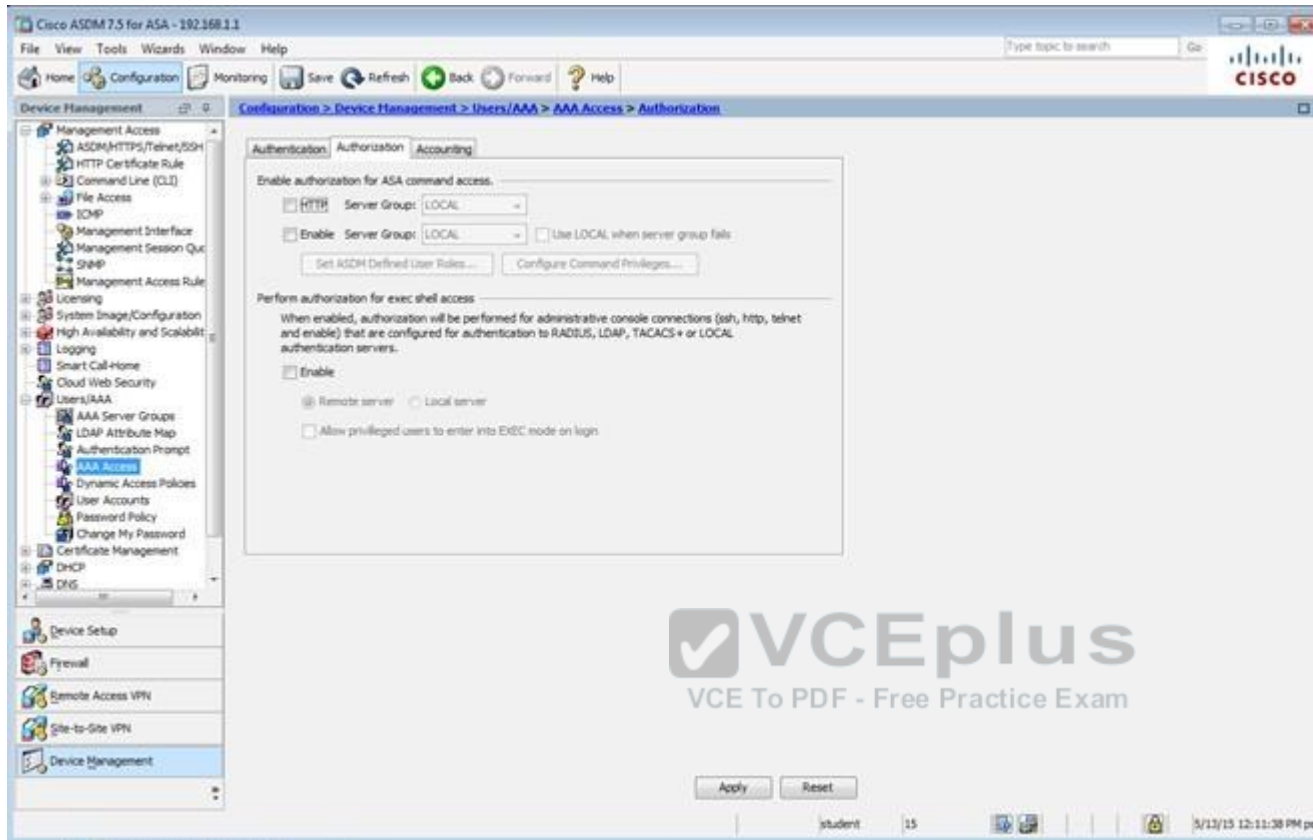


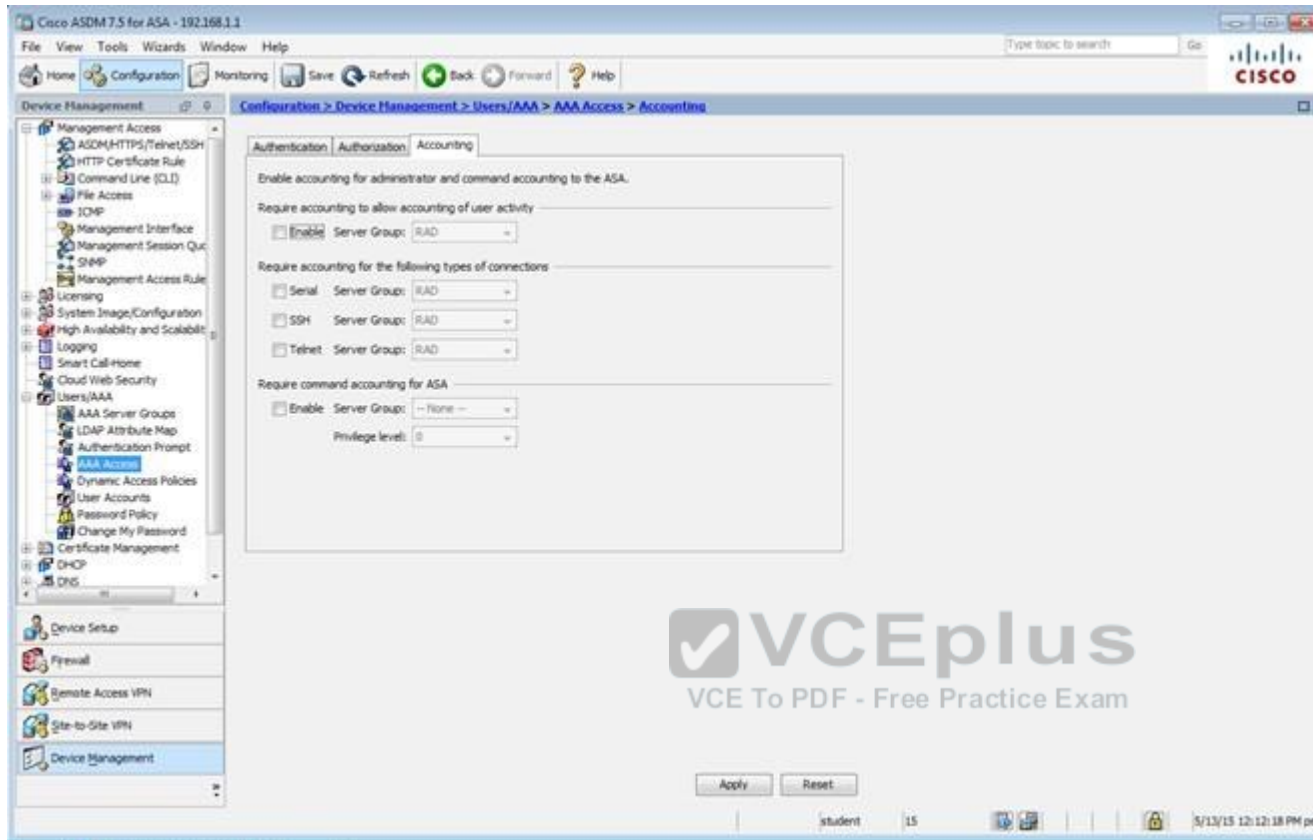


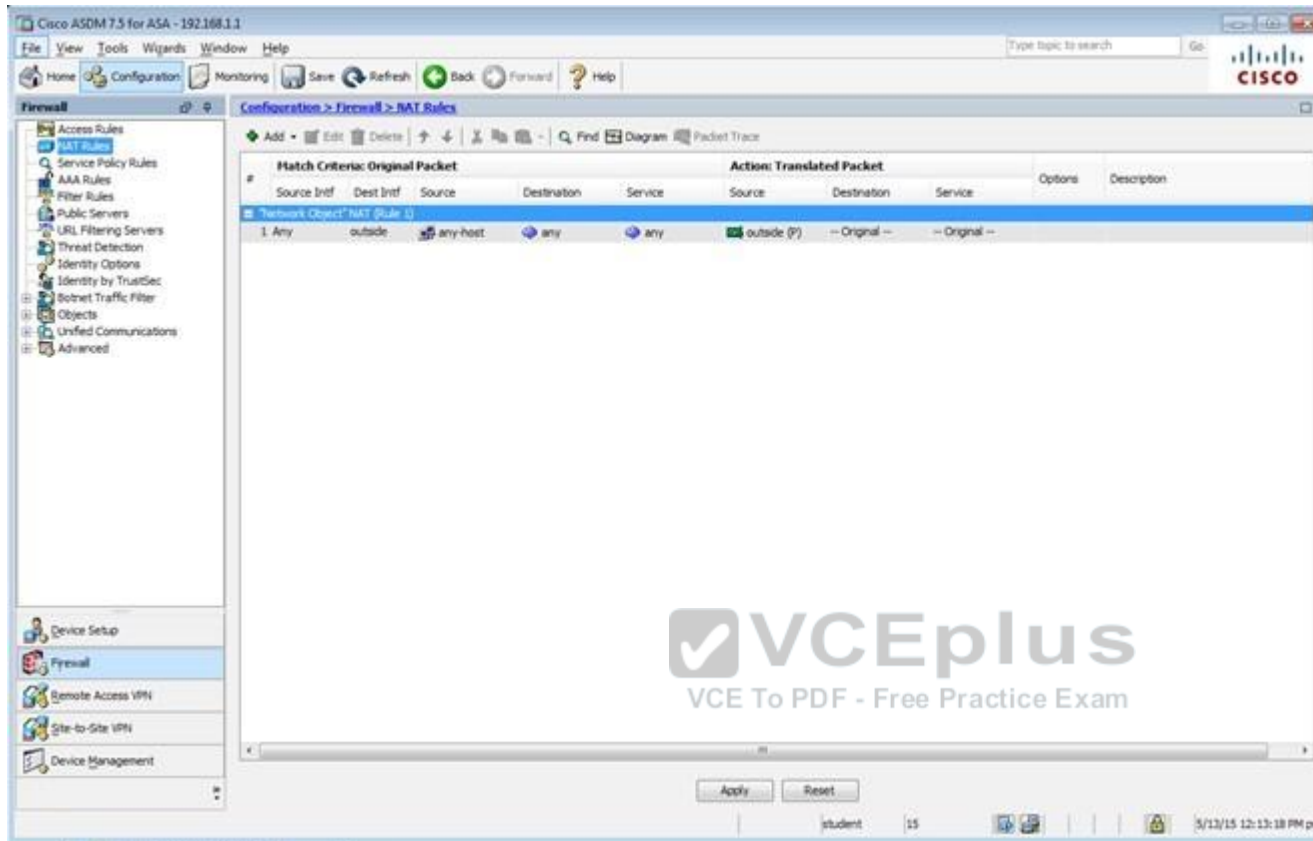


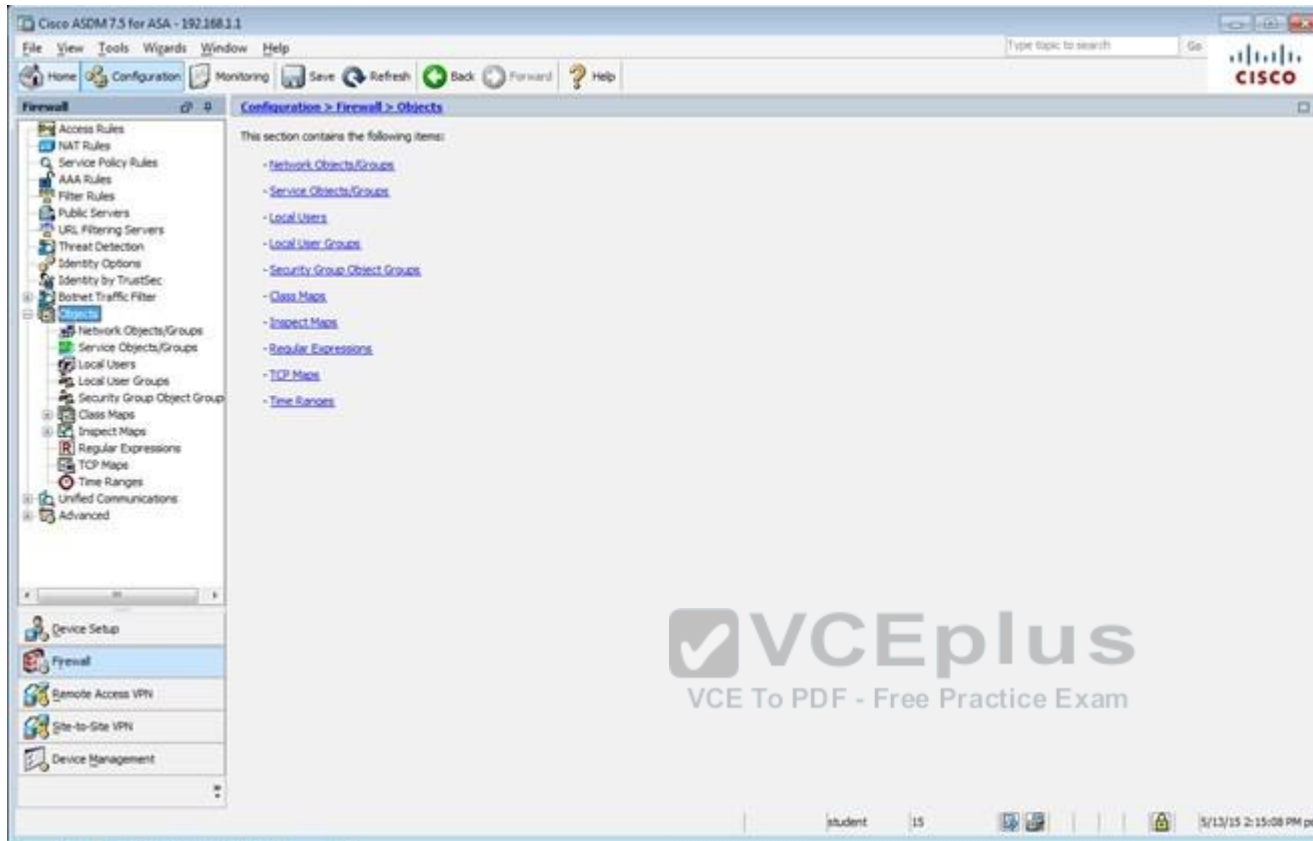












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

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

Add Edit Delete

End: [ ] [ ] [ ] Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

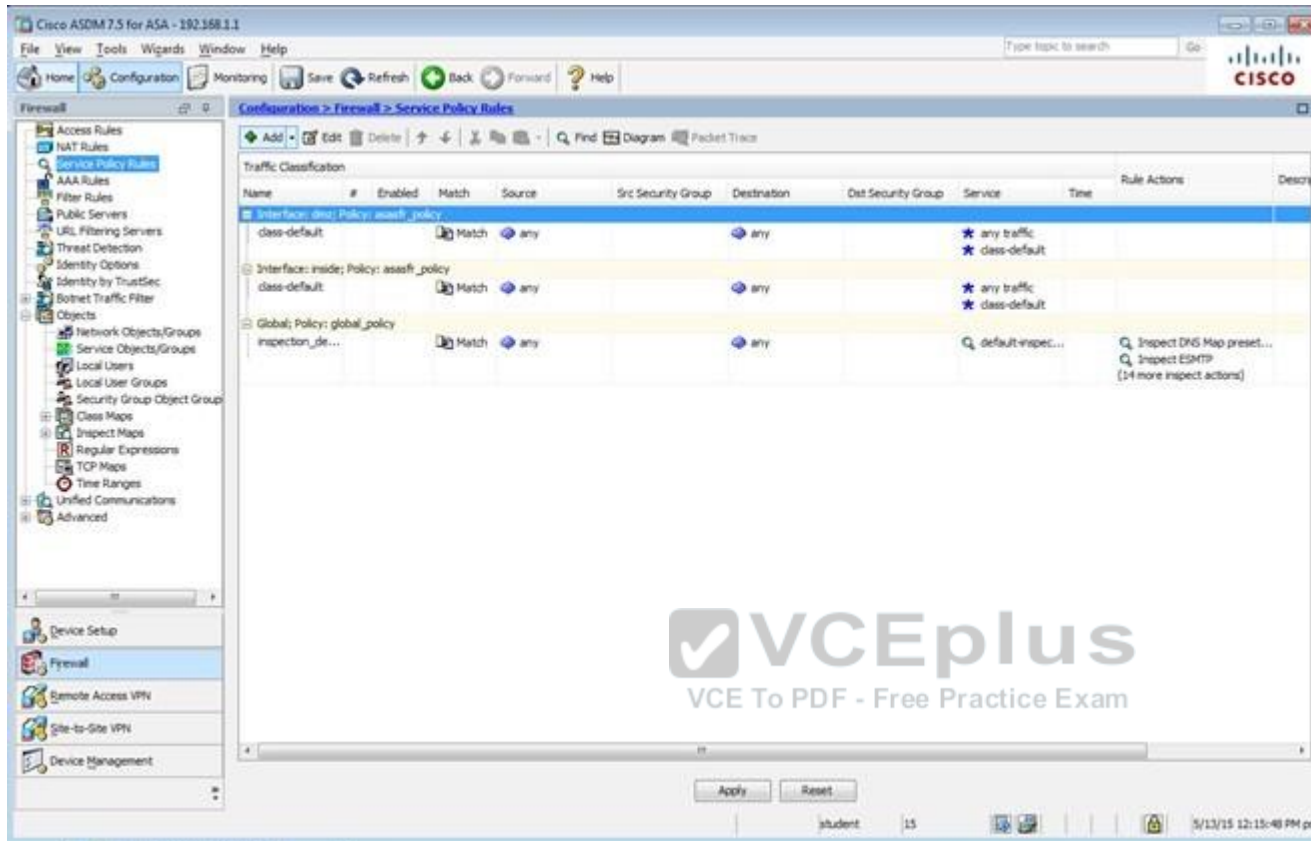
Firewall Configuration > Firewall > Objects > Network Objects/Groups

Filter: Filter (Clear)

| Name                   | IP Address       | Netmask | Description | Object NAT Address |
|------------------------|------------------|---------|-------------|--------------------|
| <b>Network Objects</b> |                  |         |             |                    |
| any                    |                  |         |             |                    |
| any-host               | 0.0.0.0          | 0.0.0.0 |             | outside (F)        |
| any4                   |                  |         |             |                    |
| any6                   |                  |         |             |                    |
| facebook               | www.facebook.com |         |             |                    |
| My_ASA_Demo_Obj        | 1.10.8.20        |         |             |                    |

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Access Rules

Access Rules

- 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

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

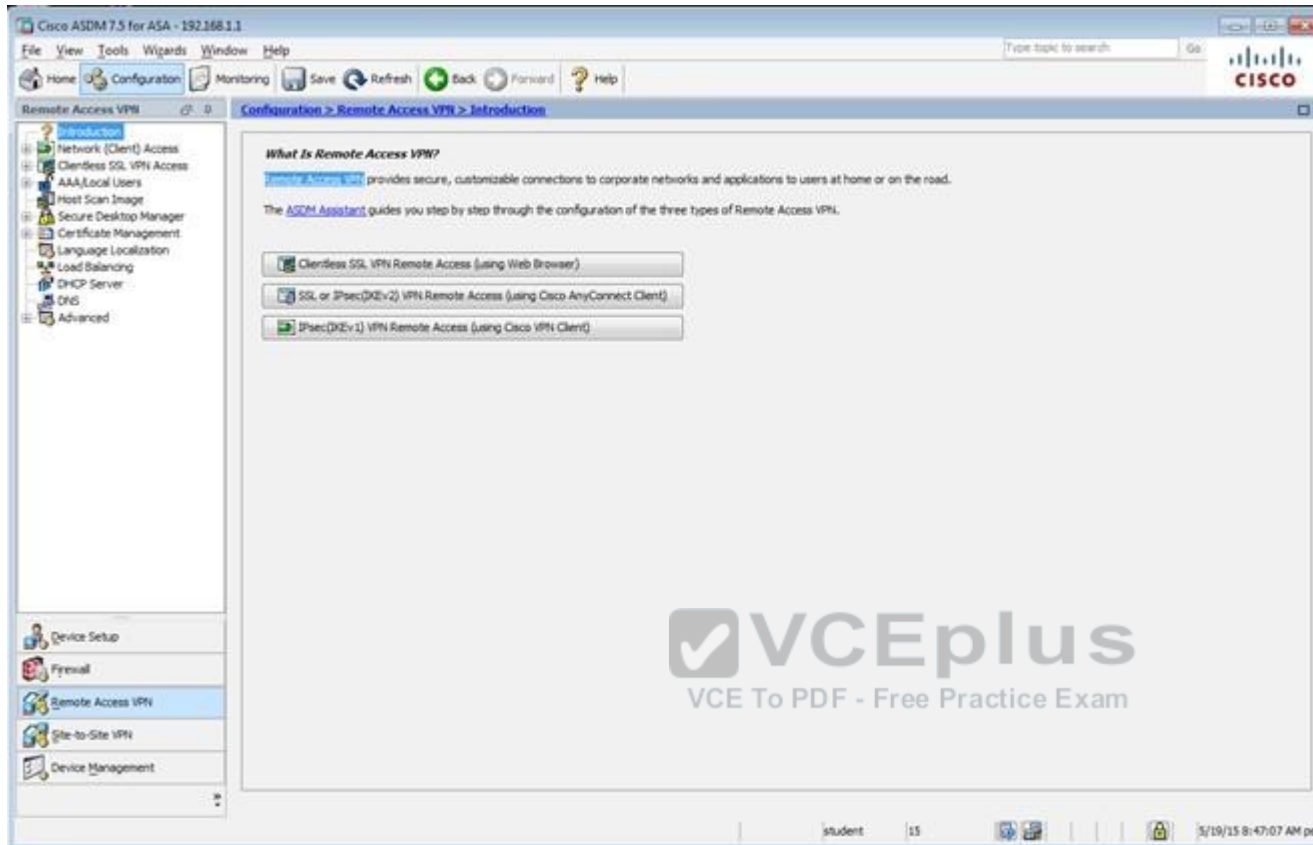
Configuration > Firewall > Access Rules

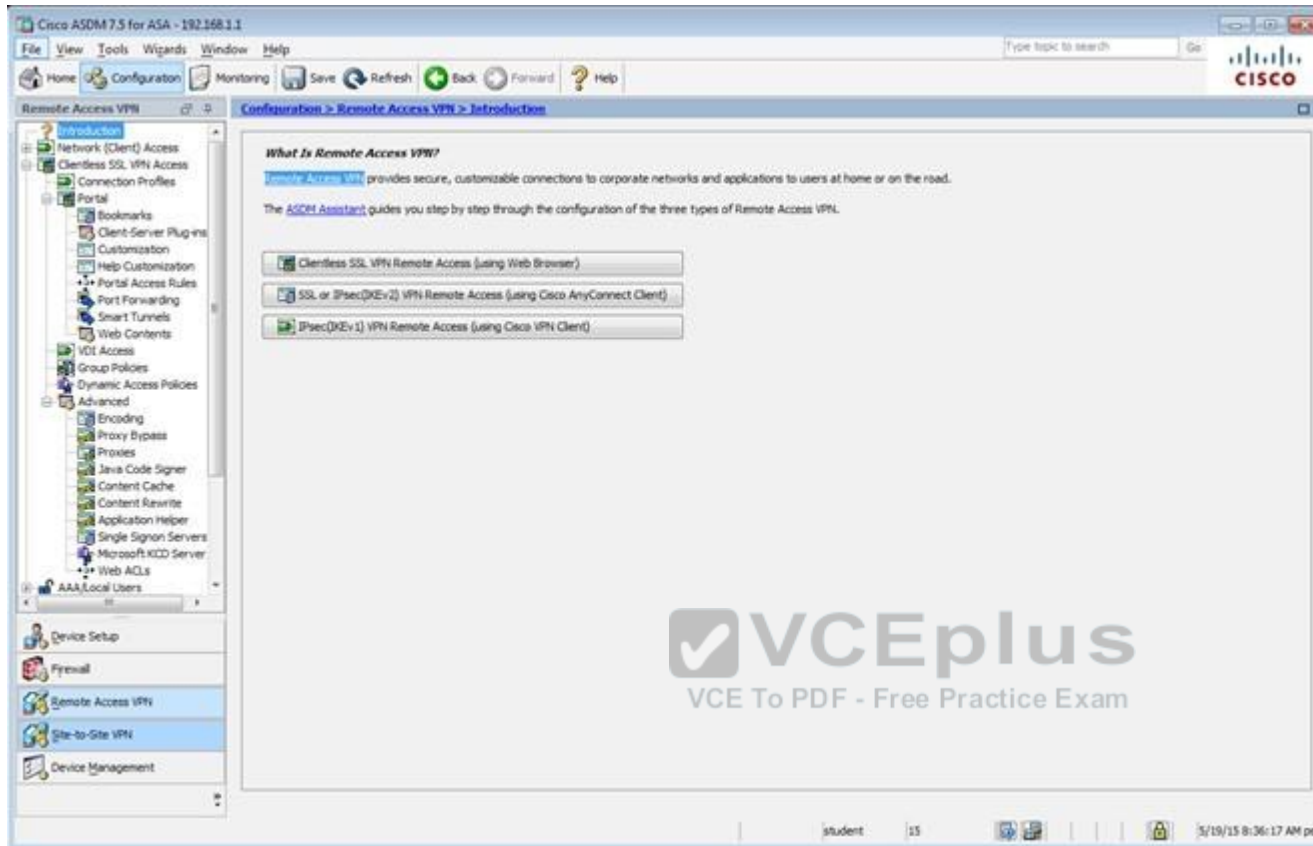
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

| # | Enabled                             | Source Criteria:                    | Destination Criteria: | Service | Action | Hits  | Logging |
|---|-------------------------------------|-------------------------------------|-----------------------|---------|--------|-------|---------|
|   |                                     | Source                              | Destination           |         |        |       |         |
| 1 | <input checked="" type="checkbox"/> | any                                 | Any less secure ne... | HTTP    | Permit |       |         |
| 2 | <input checked="" type="checkbox"/> | inside (1 implicit incoming rule)   | any                   | HTTP    | Permit | 54... |         |
| 3 | <input checked="" type="checkbox"/> | any                                 | any                   | HTTP    | Permit |       |         |
| 4 | <input checked="" type="checkbox"/> | outside (0 implicit incoming rules) | any                   | HTTP    | Permit |       |         |
| 5 | <input checked="" type="checkbox"/> | Global (1 implicit rule)            | any                   | HTTP    | Deny   |       |         |

Apply Reset Advanced...

student 15 5/13/15 12:28:58 PM pst





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

Access Interfaces  
Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

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

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

Add Edit Delete Find: Match Case

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

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

Name: clientless  
Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

☐ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add - Delete (The table is in-line editable.)

| Alias | Enabled                             |
|-------|-------------------------------------|
| test  | <input checked="" type="checkbox"/> |

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add - Delete (The table is in-line editable.)

| URL                        | Enabled                             |
|----------------------------|-------------------------------------|
| https://209.165.201.2/test | <input checked="" type="checkbox"/> |

You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Interface-Specific Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL |
|-----------|--------------|-------------------|
|-----------|--------------|-------------------|

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Secondary Authentication Server Group

Server Group: -- None -- Manage...

☐ Use LOCAL if Server Group fails

☐ Use primary username (Hide secondary username on login page)

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

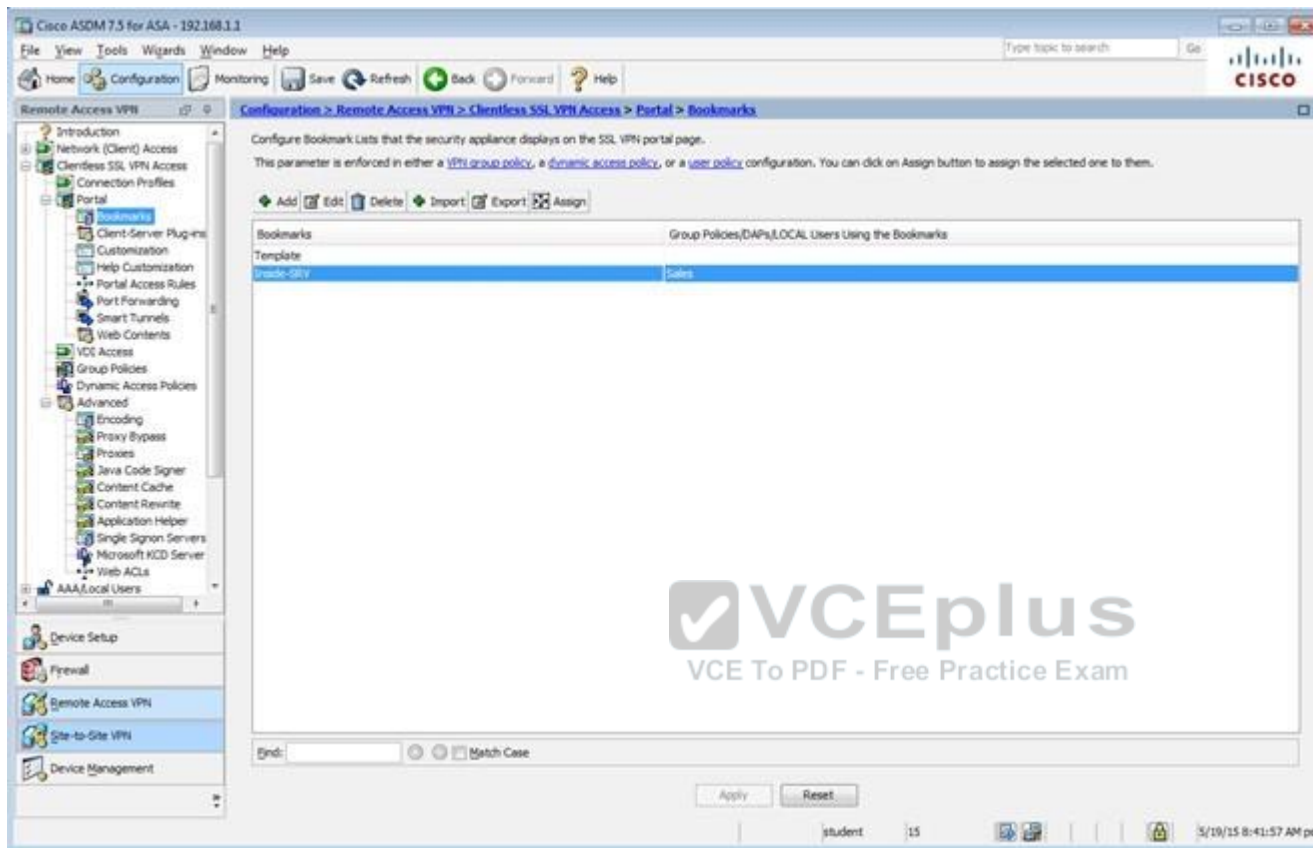
☐ Use the entire DN as the username

☐ Use script to select username

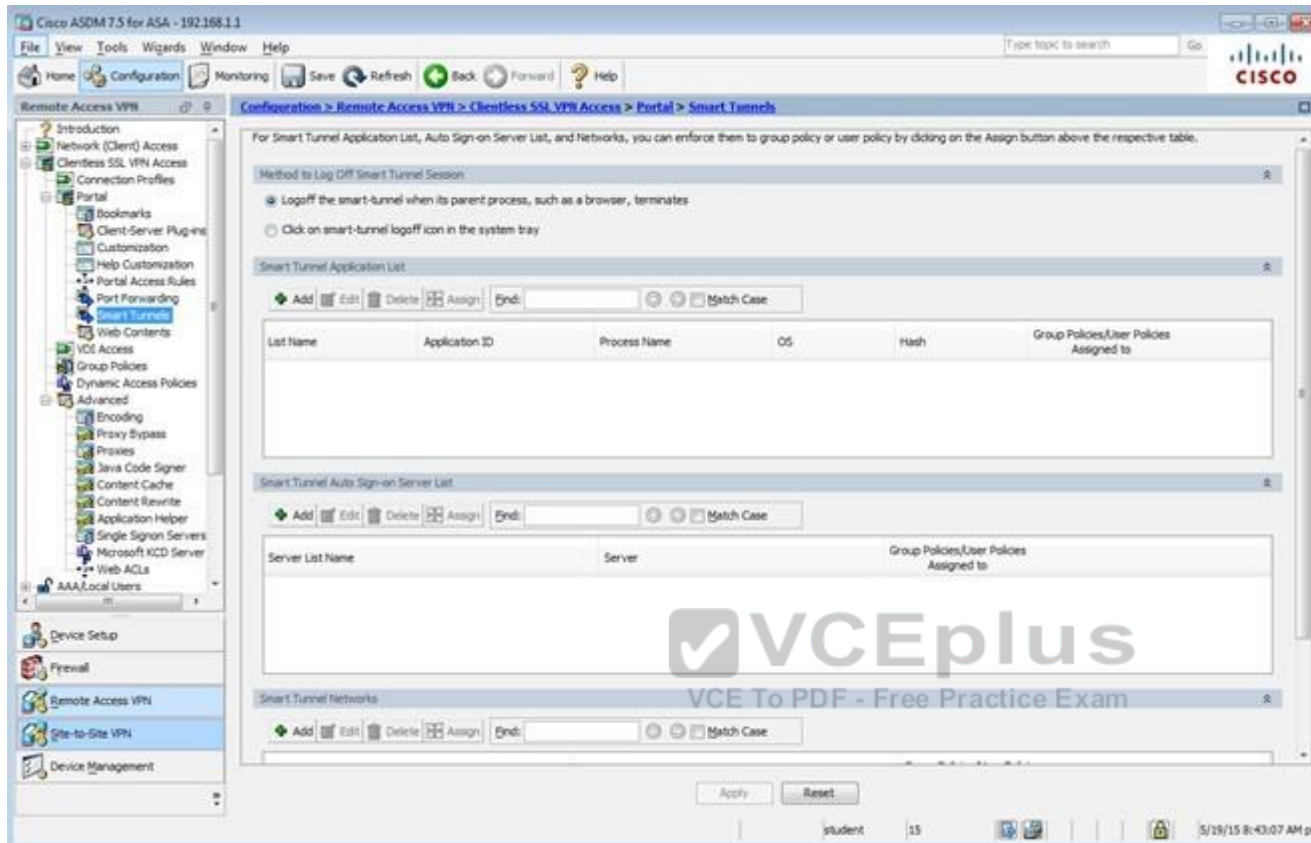
-- None -- + Add Edit Delete

Find:  Next Previous

OK Cancel Help







The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with the following items: Introduction, Network (Client) Access, Clientless SSL VPN Access, Connection Profiles, Portal, Bookmarks, Client-Server Plug-ins, Customization, Help Customization, Portal Access Rules, Port Forwarding (selected), Smart Tunnels, Web Contents, VDI Access, Group Policies, Dynamic Access Policies, Advanced, Encoding, Proxy Bypass, Proxies, Java Code Signer, Content Cache, Content Rewrite, Application Helper, Single Signon Servers, Microsoft KCD Server, Web ACLs, AAA/Local Users, Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management.

The main content area is titled "Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding". It contains the following text:

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

Below the text is a table with the following columns: List Name, Local TCP Port, Remote Server, Remote TCP Port, Description, and Group Policies/User Policies Assigned to. The table is currently empty.

At the bottom of the main content area, there is a "Find:" search bar and a "Match Case" checkbox. Below the search bar are "Apply" and "Reset" buttons.

The status bar at the bottom of the window shows "student", "15", and the date/time "5/19/15 8:43:47 AM pst".

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

◆ Add ◆ Edit ◆ Delete ◆ Assign

| Name                                | Type     | Tunneling Protocol                  | Connection Profiles/Users Assigned To                  |
|-------------------------------------|----------|-------------------------------------|--|
| Clientless                          | Internal | ssl-clientless                      | Clientless   |
| DefaultGroupPolicy (System Default) | Internal | key1:key2:ssl-clientless/2to-espsec | DefaultRAGroup/DefaultIL2Group/DefaultADMDGroup/Def... |

Find: [ ] [ ] [ ] Match Case

Apply Reset

student 15 5/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

Tunneling Protocols: ☐ Inherit ☒ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 ☐ IPsec IKEv2 ☐ L2TP/IPsec

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

Find:  ☐ Next ☐ Previous

OK Cancel Help

The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' expanded. The main pane shows the 'Group Policies' configuration page for 'Clientless SSL VPN Access'. The page includes a description of VPN group policies and a table listing the configured policies.

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

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

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

Buttons: Add, Edit, Delete, Assign

| Name                           | Type     | Tunneling Protocol                | Connection Profiles/Users Assigned To |
|--------------------------------|----------|-----------------------------------|---------------------------------------|
| Sales                          | Internal | l2l-clientless                    | Sales                                 |
| DfltGrpPolicy (System Default) | Internal | ikev1ikev2ssl-clientless/2ip-4sec | DfltGrpPolicy                         |

Find: [ ] Match Case [ ]

Buttons: Apply, Reset

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

Edit Internal Group Policy: Sales

General  
More Options  
Customization  
Login Setting  
Single Signon  
VDI Access  
Session Settings

Bookmark List: ☐ Inherit  Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit  Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit  Manage...

Tunnel Option:  Manage...

Smart Tunnel Application: ☒ Inherit  Manage...

☐ Smart Tunnel all Applications (This feature only works with Windows platforms)

☐ Auto Start

Auto Sign-on Server: ☒ Inherit  Manage...

Windows Domain Name (optional):

Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find:  ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DfBGrpPolicy

**General**  
Servers  
Advanced

Name: DfBGrpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None-- Manage...

Access Hours: --Unrestricted-- Manage...

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

Maximum Connect Time: ☒ Unlimited ☐ minutes

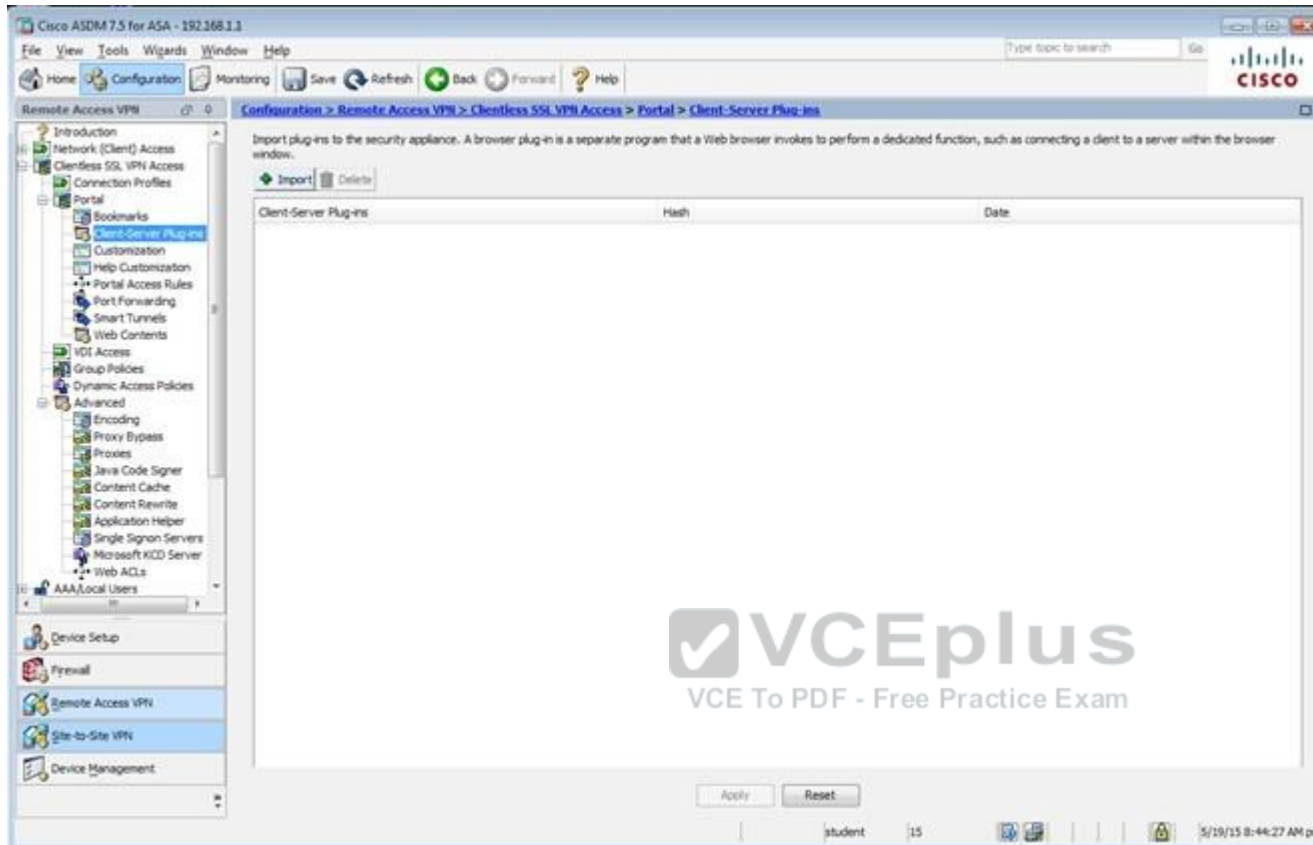
Idle Timeout: ☐ None ☐ 30 minutes

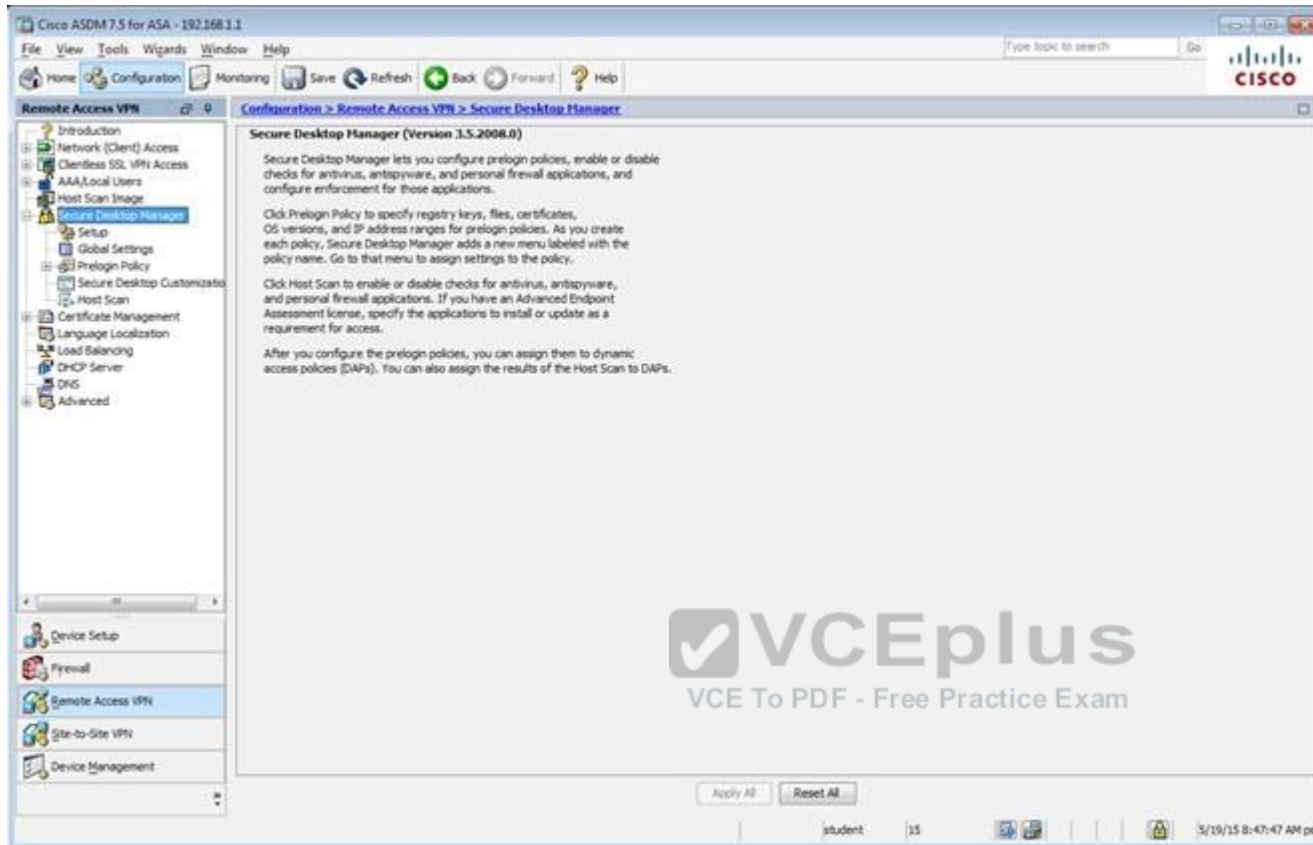
On smart card removal: ☒ Disconnect ☐ Keep the connection

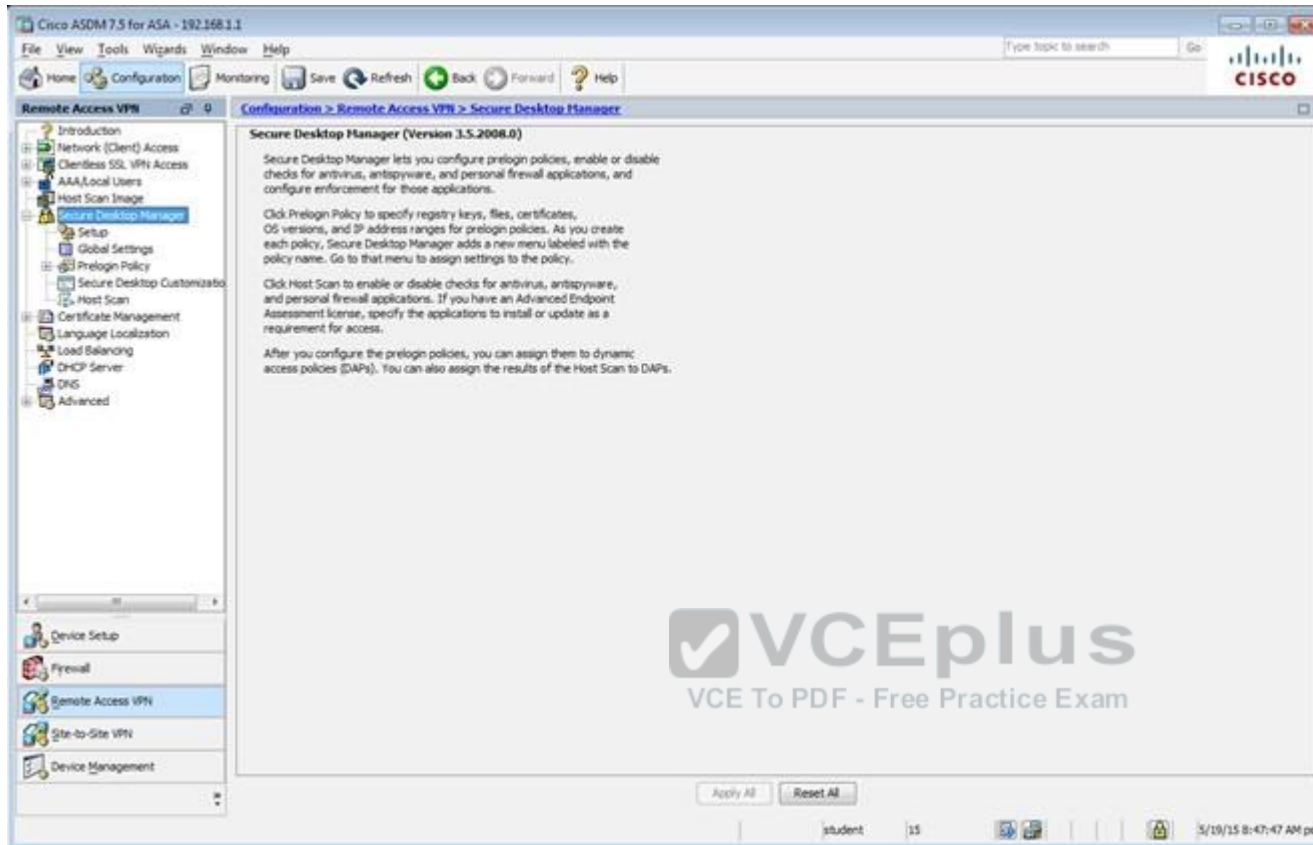
**VCEplus**  
VCE To PDF - Free Practice Exam

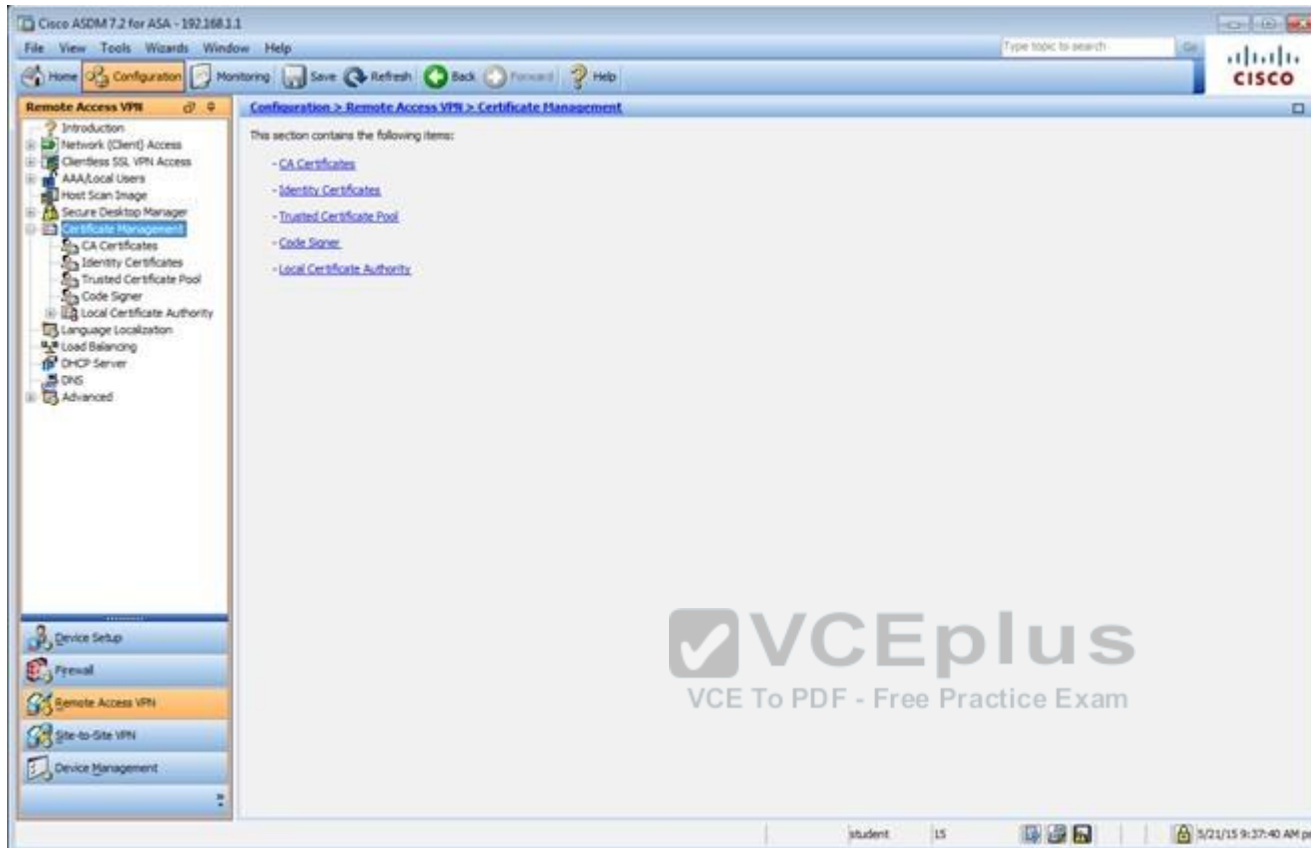
Find: Next Previous

OK Cancel Help



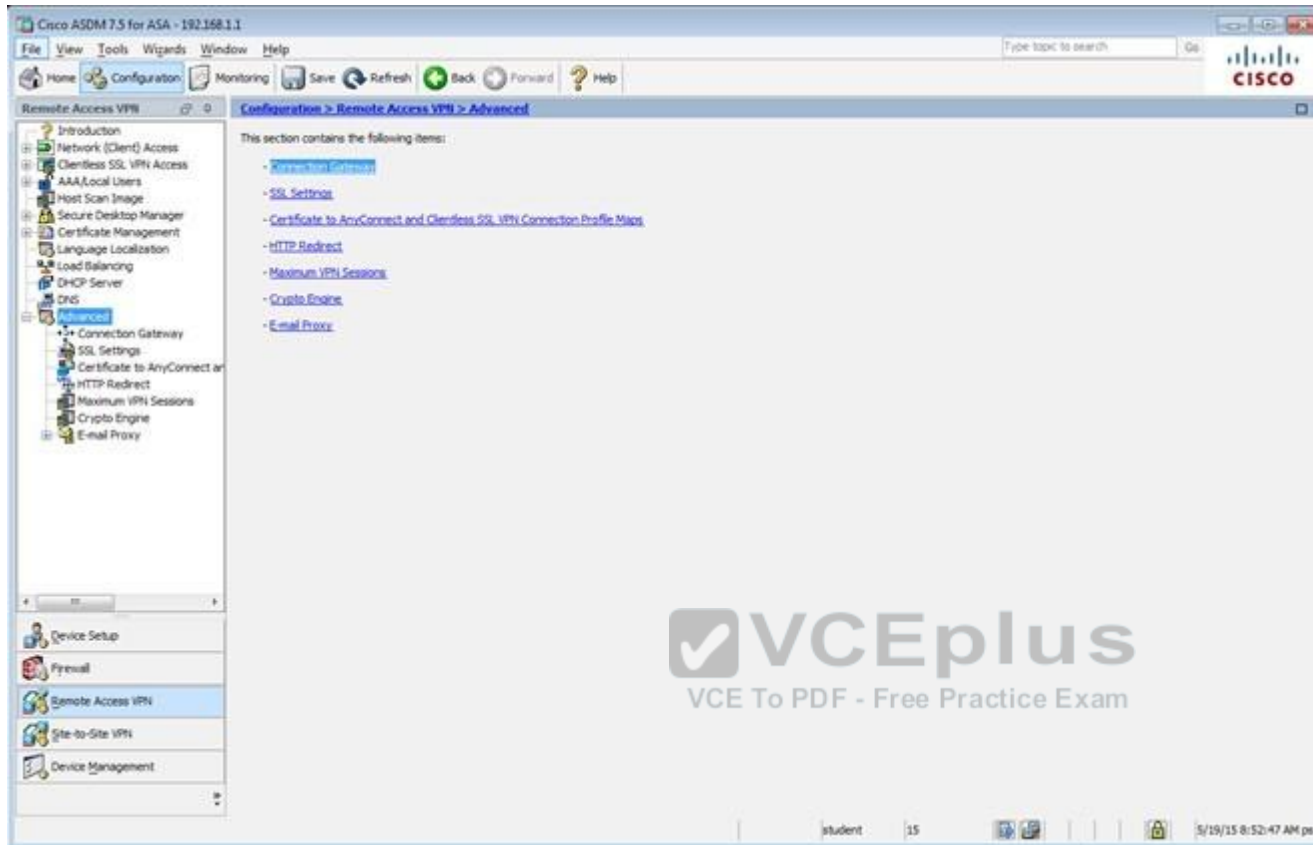


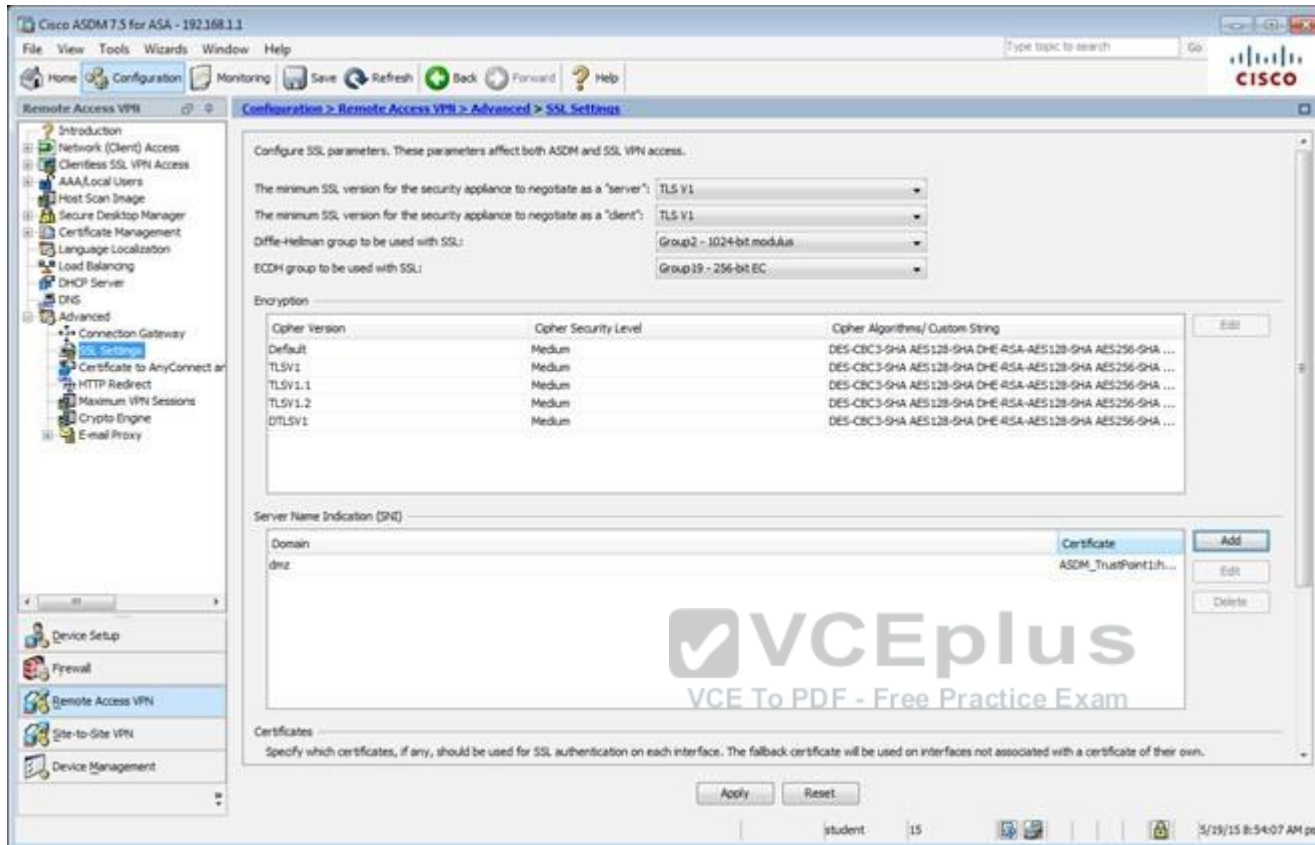


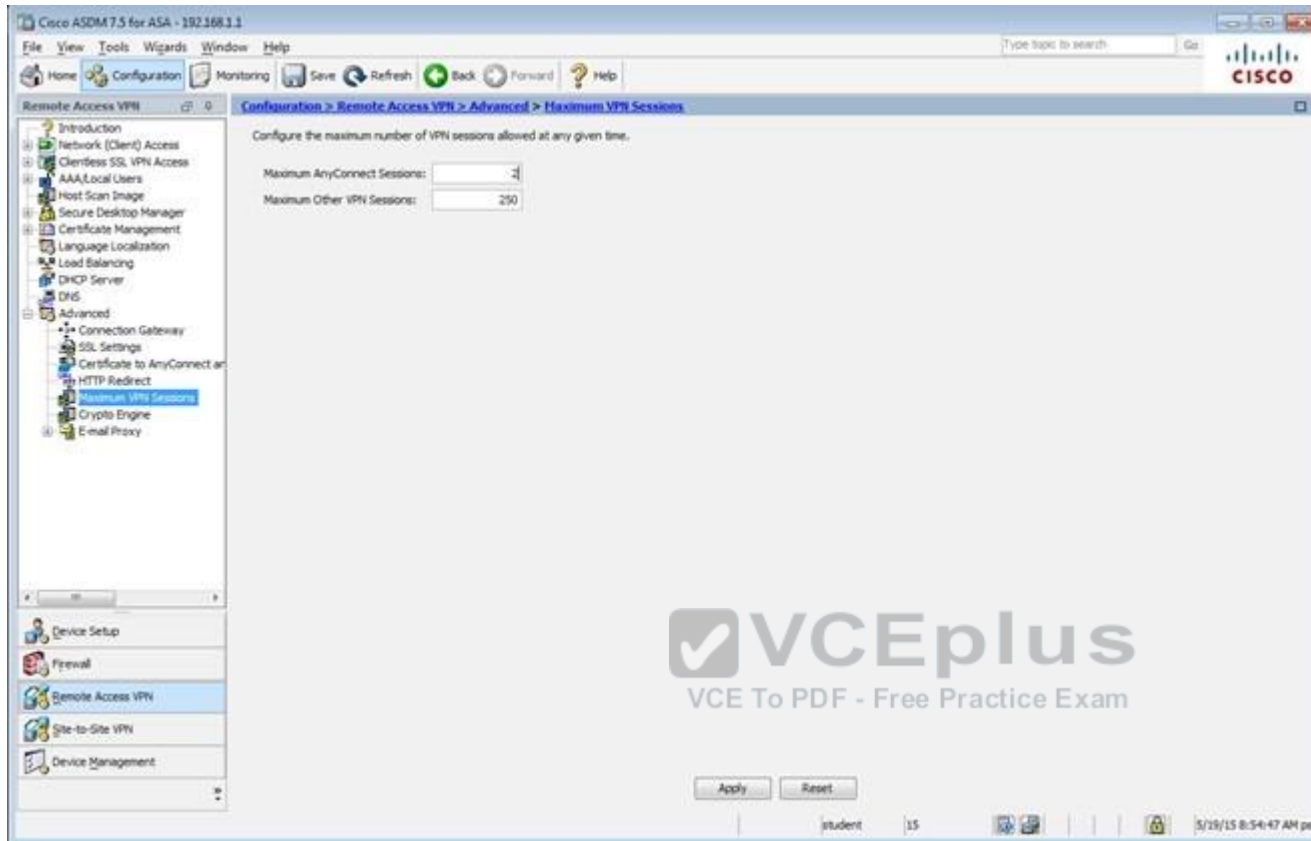


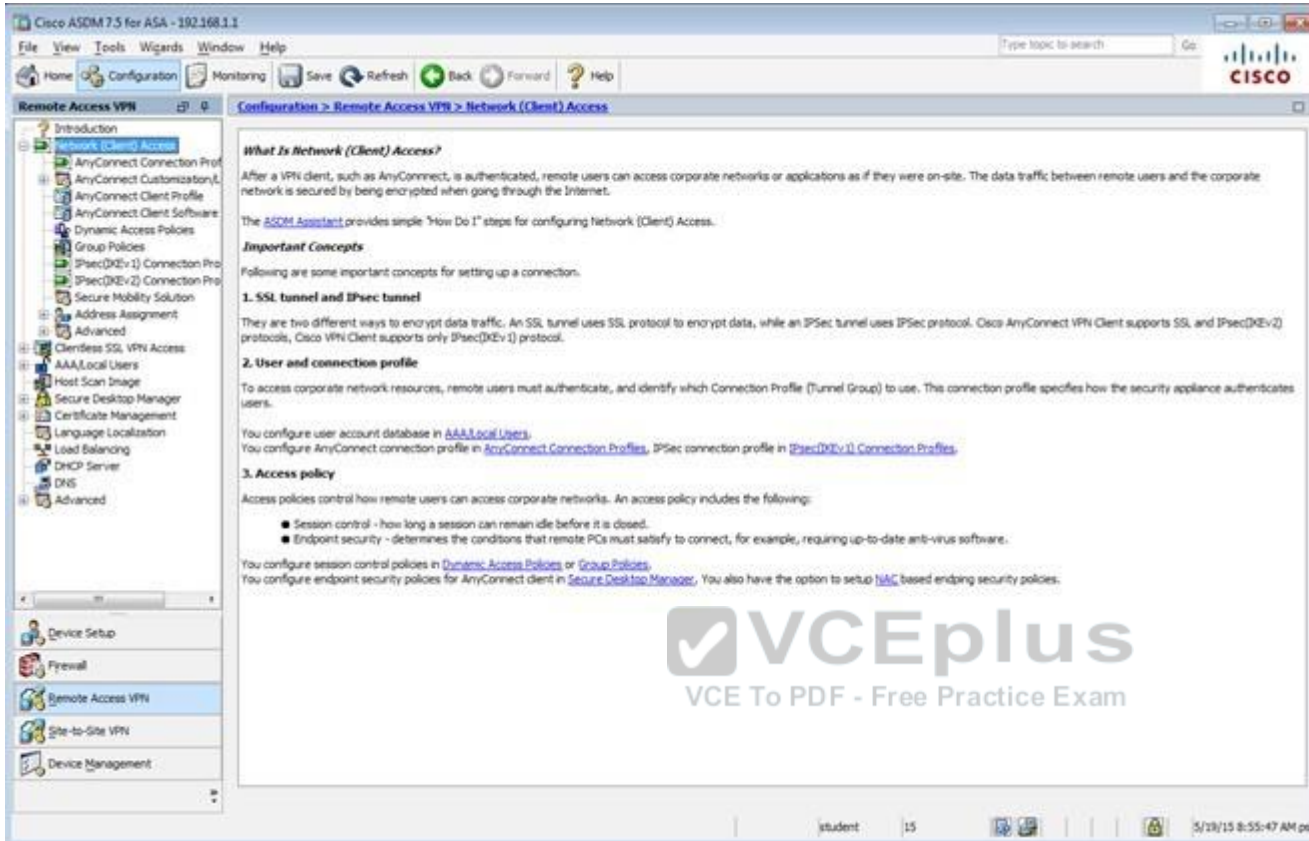
The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with the following columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. A single entry is listed with 'hostname-17-ASA.sec...' in the first two columns, an expiry date of '11:10:33 pet Dec 20 2024', and an associated trustpoint of 'ASDM\_TrustPoint1'. To the right of the table are buttons for 'Add', 'Show Details', 'Delete', 'Export', and 'Install'. Below the table is a search bar with 'Find:' and a 'Match Case' checkbox. Further down, there are sections for 'Certificate Expiration Alerts' (with input fields for 'Send the first alert before' and 'Repeat Alert Interval') and 'Public CA Enrollment' (with a paragraph of text and a link to 'enroll with Entrust'). At the bottom, there is a section for the 'ASDM Identity Certificate Wizard' with a paragraph of text and a 'Launch ASDM Identity Certificate Wizard' button. The status bar at the bottom shows 'student', '15', and the date/time '5/19/15 8:51:47 AM pet'.

| Issued To              | Issued By              | Expiry Date              | Associated Trustpoints | Usage           | Public Key Type |
|------------------------|------------------------|--------------------------|------------------------|-----------------|-----------------|
| hostname-17-ASA.sec... | hostname-17-ASA.sec... | 11:10:33 pet Dec 20 2024 | ASDM_TrustPoint1       | General Purpose | RSA (2048 bits) |









The screenshot displays the Cisco ASDM 7.5 for ASA - 102.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Network (Client) Access'. It contains the following text:

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

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

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

**1. SSL tunnel and IPsec tunnel**  
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.

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

You configure user account database in [AAA Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).

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

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

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

The bottom of the window shows a status bar with 'student', '15', and a timestamp '5/28/15 8:55:47 AM pet'.

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol               | Connection Profiles/Users Assigned To                  |
|--------------------------------|----------|----------------------------------|--|
| Sales                          | Internal | ssl-clientless                   | clientless   |
| DefaultPolicy (System Default) | Internal | (rev 1) ssl-clientless/ssl-ipsec | DefaultPolicyGroupDefaultPolicyGroupDefaultPolicyGroup |

Find: Match Case

Apply Reset

student 15 5/21/15 10:17:10 AM pst

Edit Internal Group Policy: DftrGpPolicy

**General**

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

Name: DftrGpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: -- None -- Manage...

NAC Policy: -- None -- Manage...

Access Hours: -- Unrestricted -- Manage...

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

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

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles

Introduction  
Network (Client) Access  
AnyConnect Connection Profile  
AnyConnect Customization...  
AnyConnect Client Profile  
AnyConnect Client Software  
Dynamic Access Policies  
Group Policies  
IPsec(IKv1) Connection Profile  
IPsec(IKv2) Connection Profile  
Secure Mobility Solution  
Advanced  
Clientless SSL VPN Access  
AAA/Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DHCP  
Advanced

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

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

| Name              | IPsec Enabled                       | L2TP/IPsec Enabled                  | Authentication Server Group | Group Policy  |
|-------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultVRAGroup   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| DefaultIKEV1Group | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| Clientless        | <input type="checkbox"/>            | <input type="checkbox"/>            | LOCAL                       | Sales         |

Find:  Match Case

Apply Reset

student 15 5/19/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

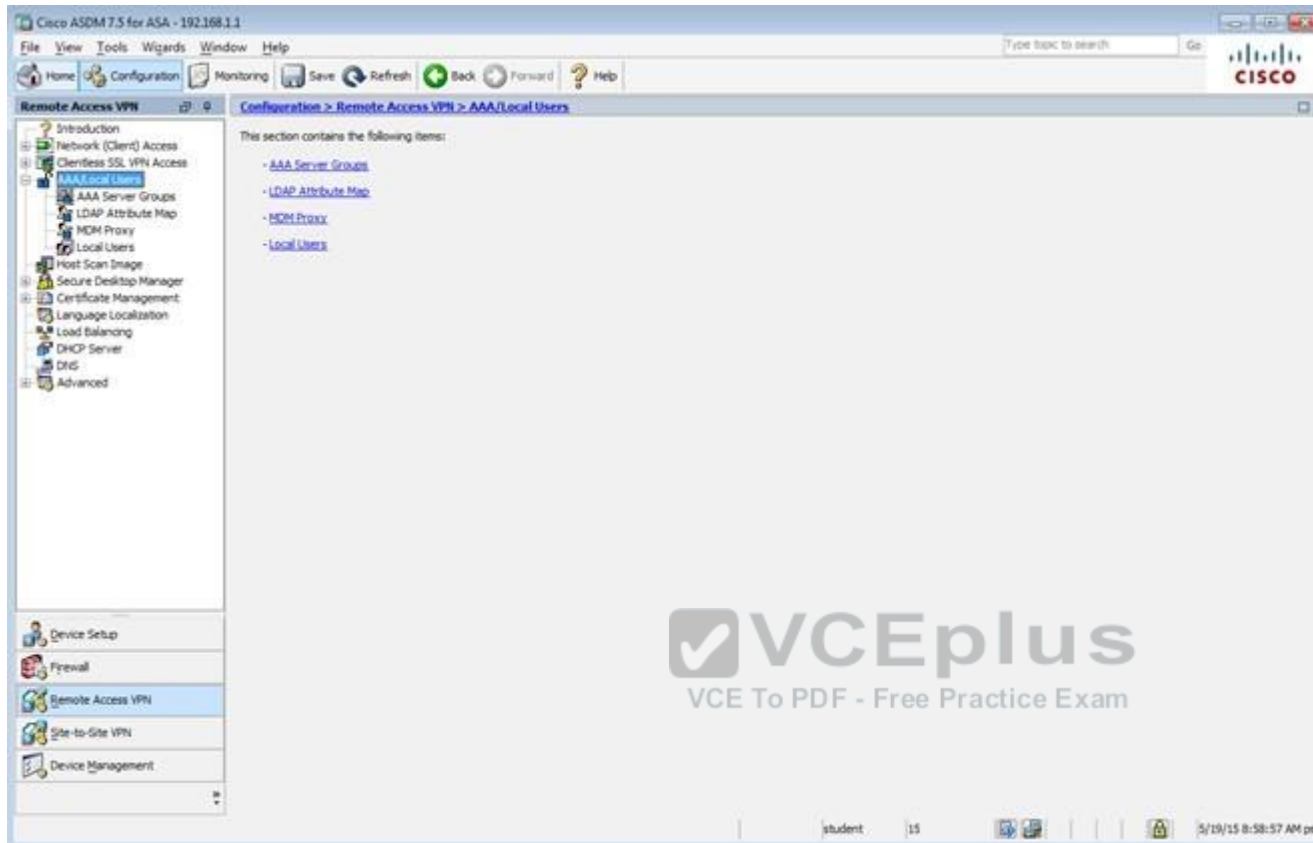
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name            | SSL Enabled                         | IPsec Enabled                       | Aliases | Authentication Method | Group Policy  |
|-----------------|-------------------------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| DefaultEAPGroup | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| Clientless      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | yes     | SSL (OCSP)            | Clientless    |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction  
Network (Client) Access  
Clientless SSL VPN Access  
AAA/Local Users  
AAA Server Groups  
LDAP Attribute Map  
MDM Proxy  
Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DNS  
Advanced

Create entries in the ASA local user database.

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

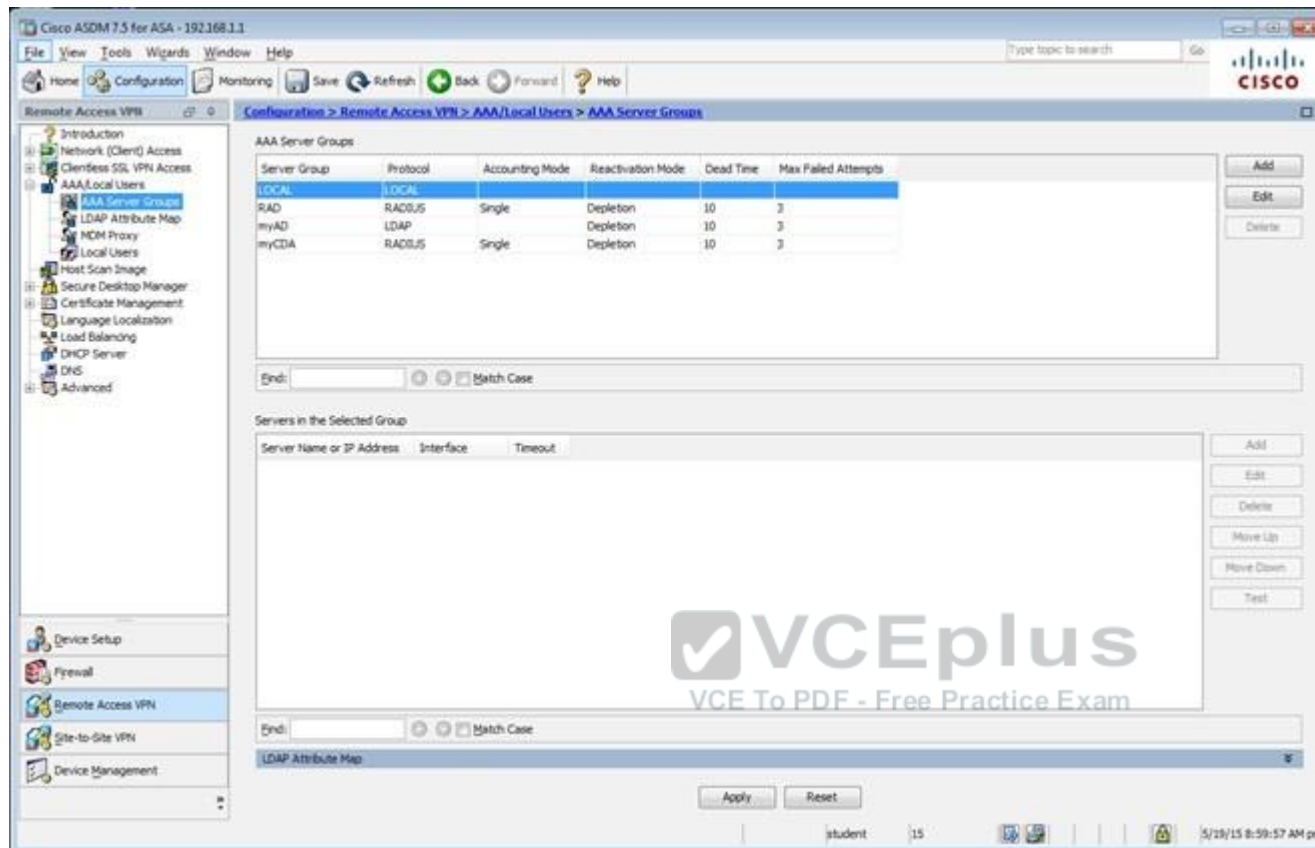
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

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

Find: [ ] [ ] [ ] Match Case

Apply Reset

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



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

- A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM\_TrustPoint1.
- B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
- C. The Inside-SRV bookmark references the https://192.168.1.2 URL
- D. Only Clientless SSL VPN access is allowed with the Sales group policy
- E. AnyConnect, IPsec IKEv1, and IPsec IKEv2 VPN access is enabled on the outside interface
- F. The Inside-SRV bookmark has not been applied to the Sales group policy

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

For B:

**Virtual Terminal**

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

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

**Login Page Setting**

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

**Connection Profiles**

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

[Add](#) [Edit](#) [Delete](#) Find:

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

For C, Navigate to the Bookmarks tab:

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign

[Add](#)
[Edit](#)
[Delete](#)
[Import](#)
[Export](#)
[Assign](#)

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


Then hit "edit" and you will see this:

 Edit Bookmark List



Bookmark List Name: Inside-SRV

| Bookmark Title | URL                |
|----------------|--------------------|
| Inside Server  | http://192.168.1.2 |

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

Add

Edit

Delete

Move Up

Move Down

Find:



Match Case

OK

Cancel

Help

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

**Virtual Terminal**

Remote Access VPN

**Configuration > Remote Access VPN > Certificate Management > Identity Certificates**

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

**Find:**    ☐ Match Case

**Certificate Expiration Alerts**

Send the first alert before :  (days)

Repeat Alert Interval :  (days)

**Public CA Enrollment**

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

**Device Setup**

Note E:

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

**Remote Access VPN**

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

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page .

Connection Profiles

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

Find:

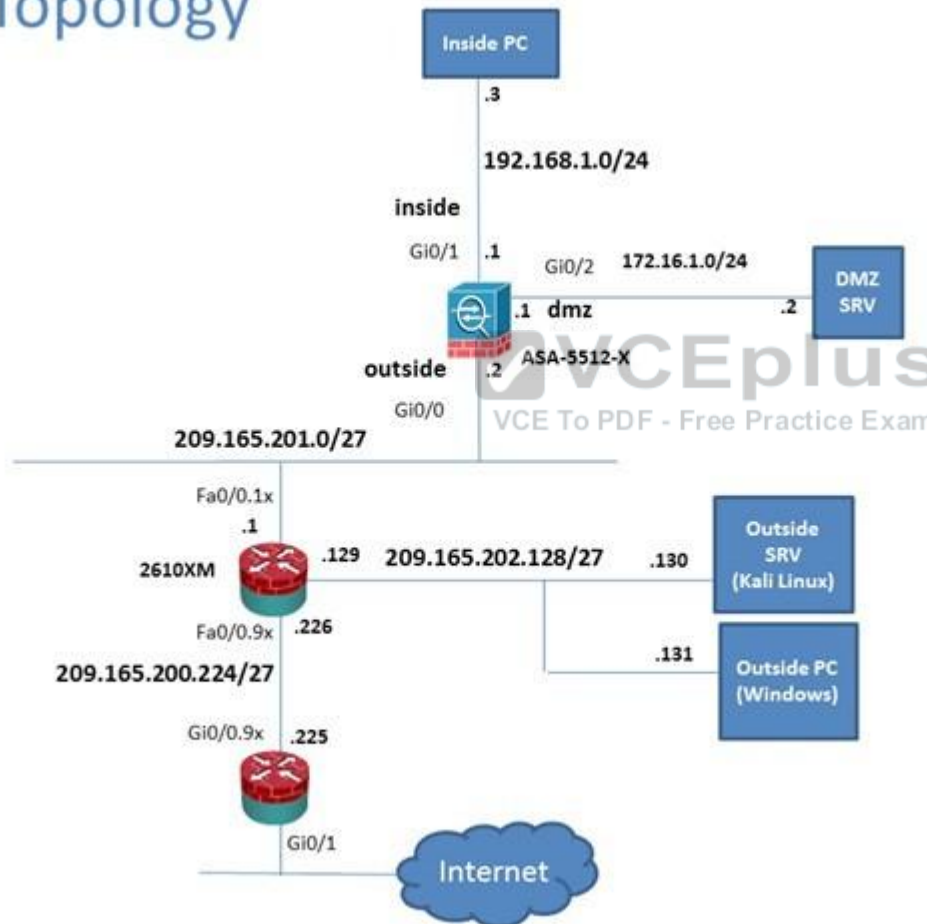
**QUESTION 67**  
Scenario

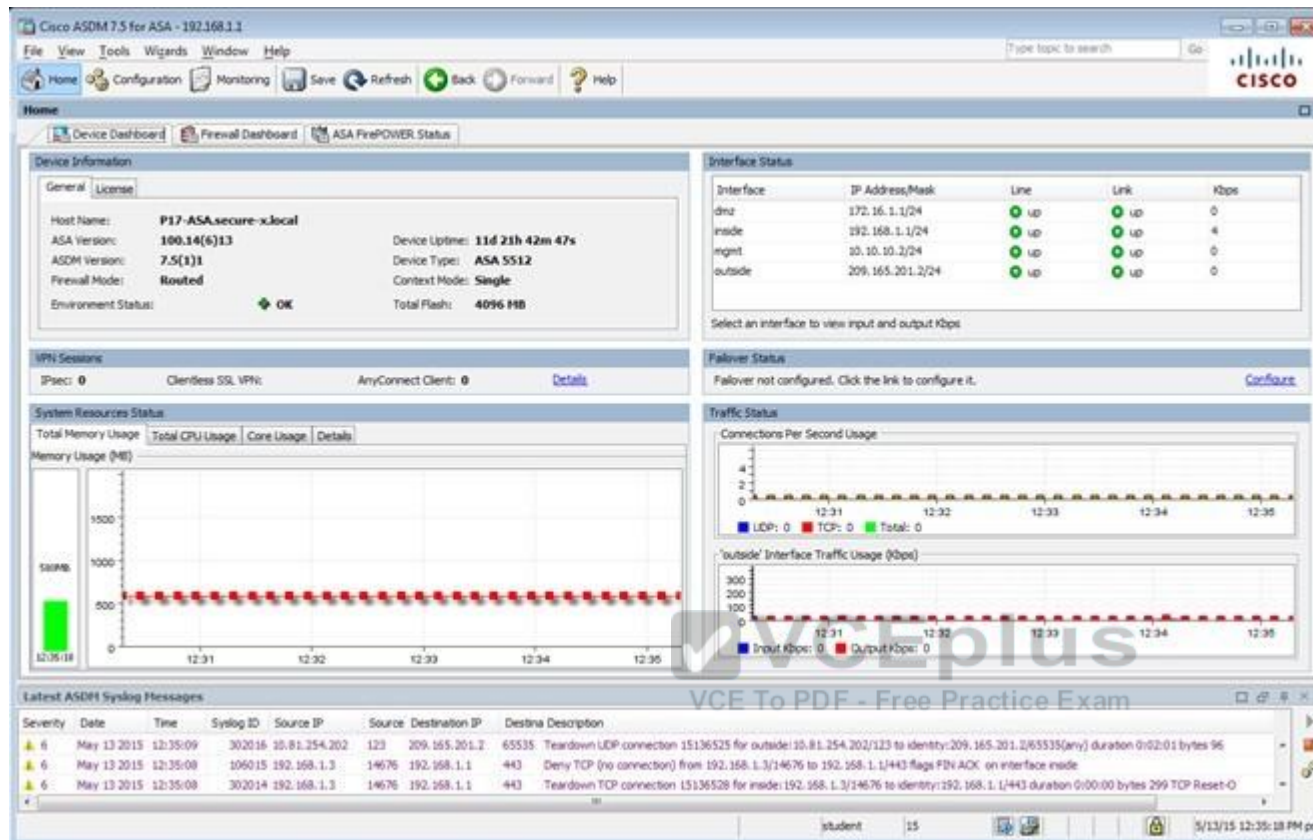
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

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

## Lab Topology





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address    | MAC Address    | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside   | 209.165.201.1 | 000c.3014.3820 | No        |
| inside    | 192.168.1.4   | 0050.5633.3333 | No        |
| inside    | 192.168.1.3   | 0050.5611.1111 | No        |
| inside    | 192.168.1.2   | 0050.5622.2222 | No        |
| inside    | 192.168.1.56  | 0050.5692.5c7b | No        |
| inside    | 192.168.1.55  | 0006.86e4.98f3 | No        |
| dmz       | 172.16.1.2    | 0050.5644.4444 | No        |
| mgmt      | 10.10.10.1    | 000c.3014.3820 | No        |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/PSec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions

Clientless SSL VPN

VPN Connection Graphs

WSA Sessions

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Monitoring > VPN > VPN Statistics > Sessions

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

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

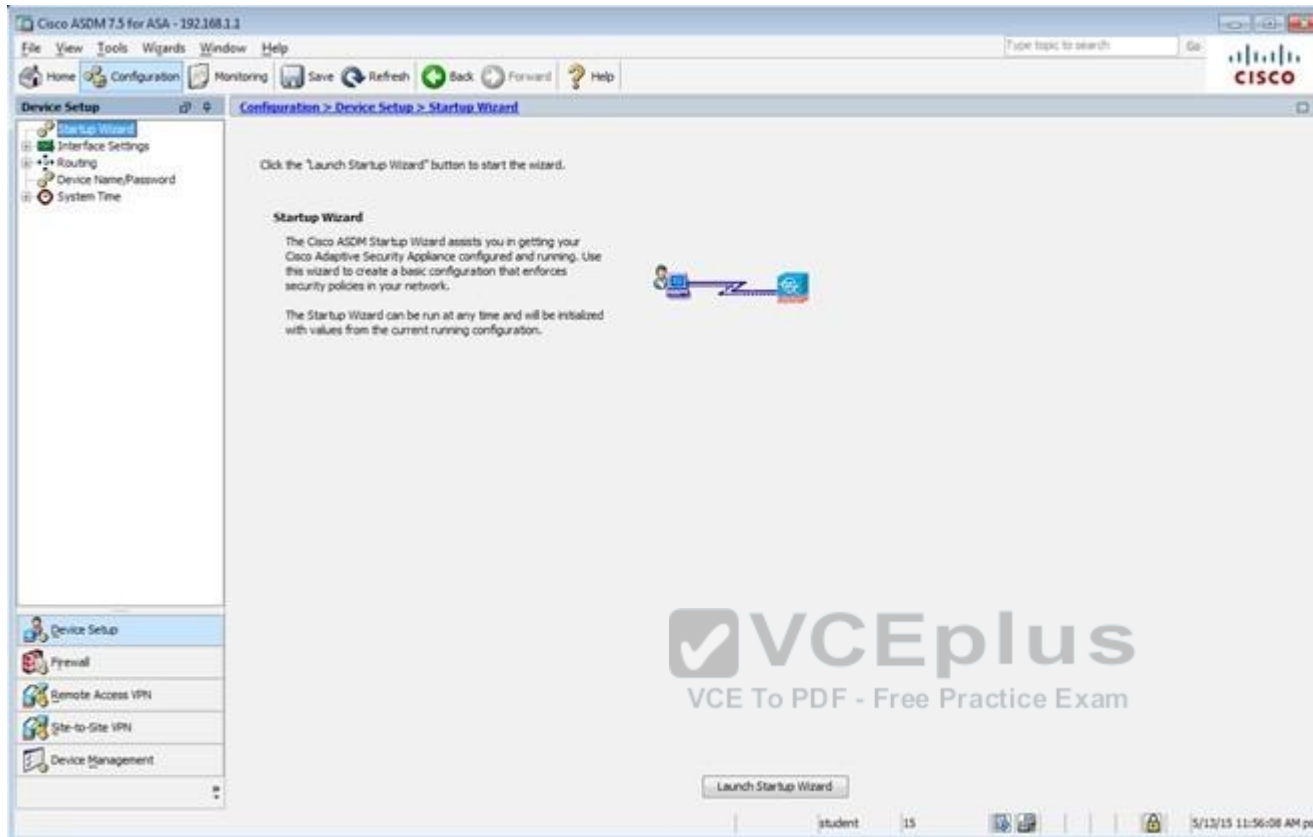
| Username | IP Address      | Group Policy | Connection Profile | Protocol   | Encryption         | Login Time                   | Duration   | Bytes Tx | Bytes Rx |
|----------|-----------------|--------------|--------------------|------------|--------------------|------------------------------|------------|----------|----------|
| student  | 209.165.202.131 | Sales        | Clientless         | Clientless | Clientless (13AC4) | 08:03:46 sat Thu May 21 2013 | 2h:09m:19s | 316774   | 41833    |

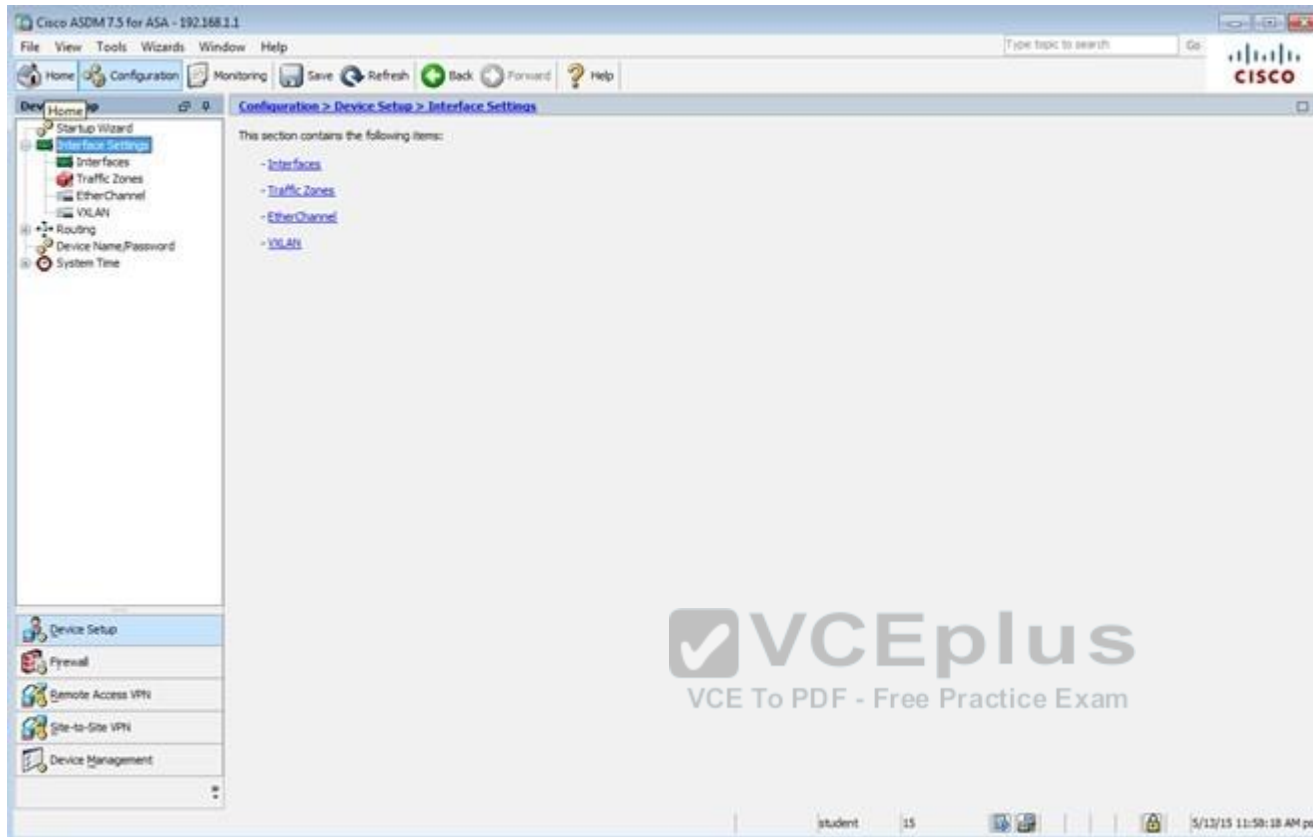
Details Logout Ping

Refresh

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

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Type topic to search Go

CISCO

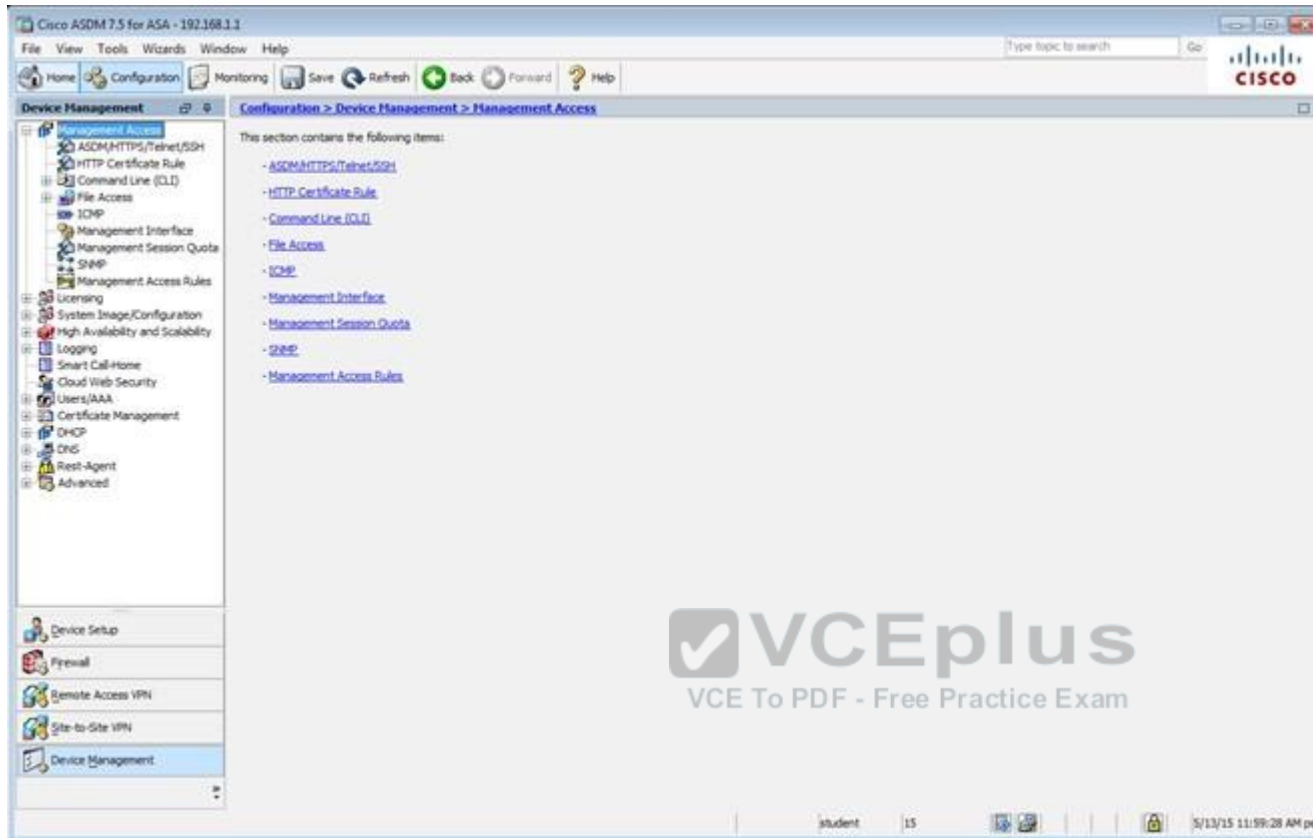
Device Setup

Configuration > Device Setup > Interface Settings > Interfaces

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

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

Student 15 5/13/15 12:42:48 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

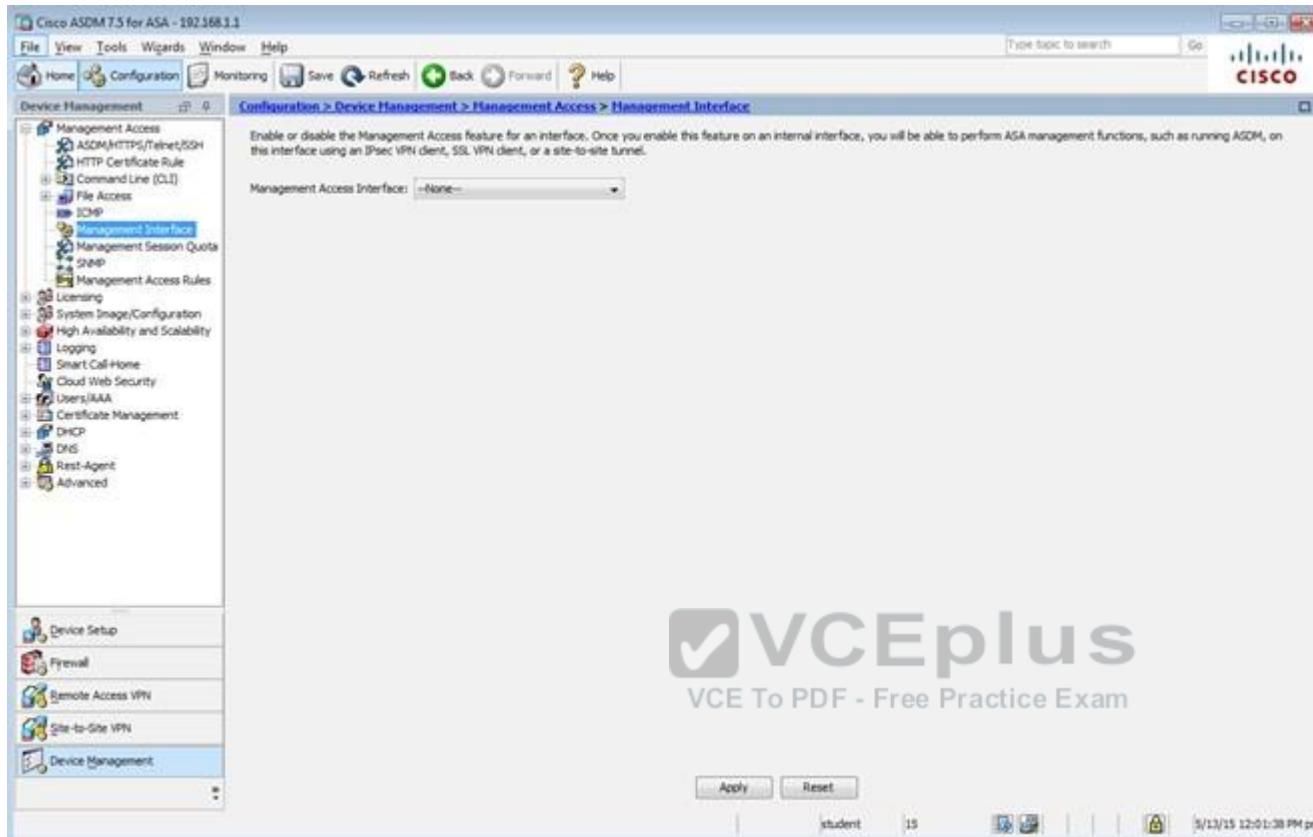
Allowed SSH Version(s): 1 & 2

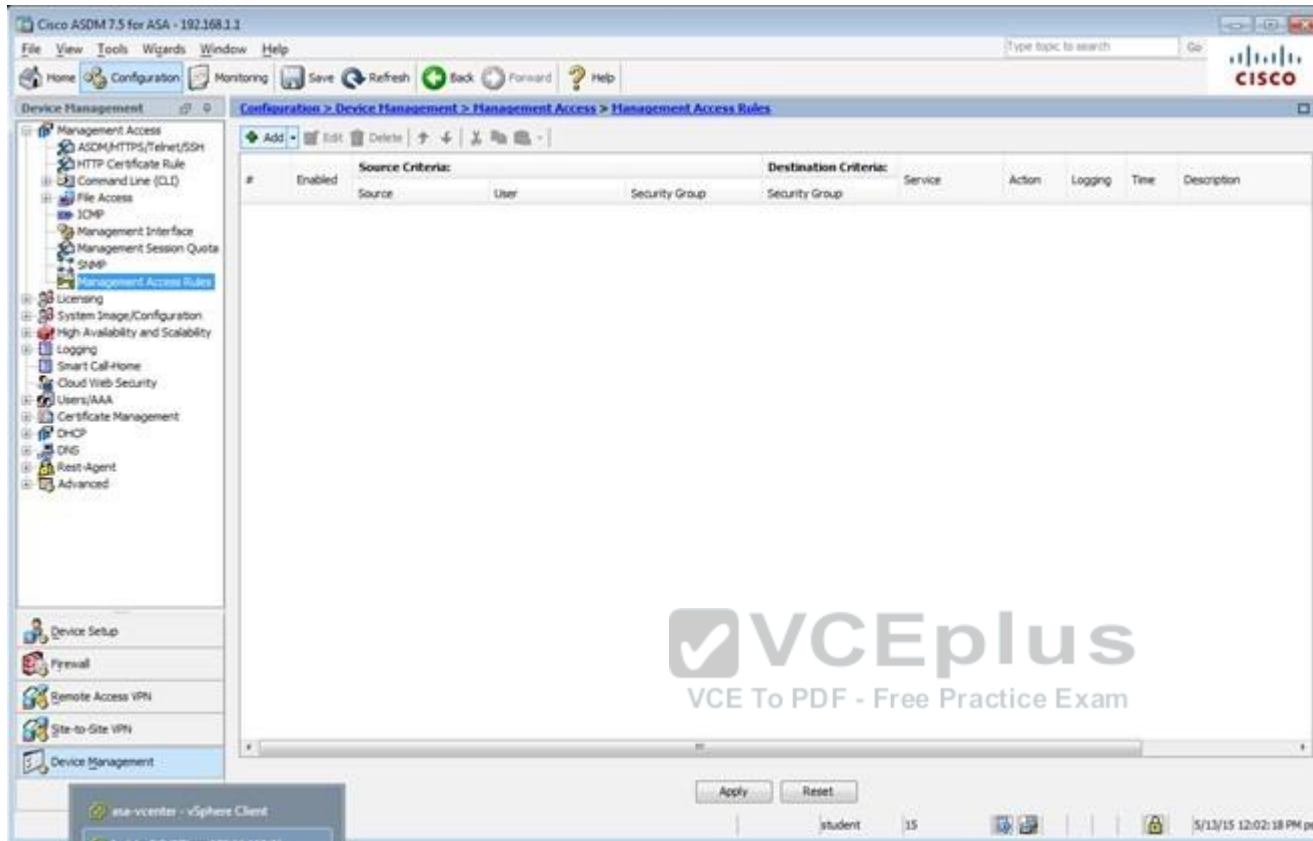
SSH Timeout: 5 minutes

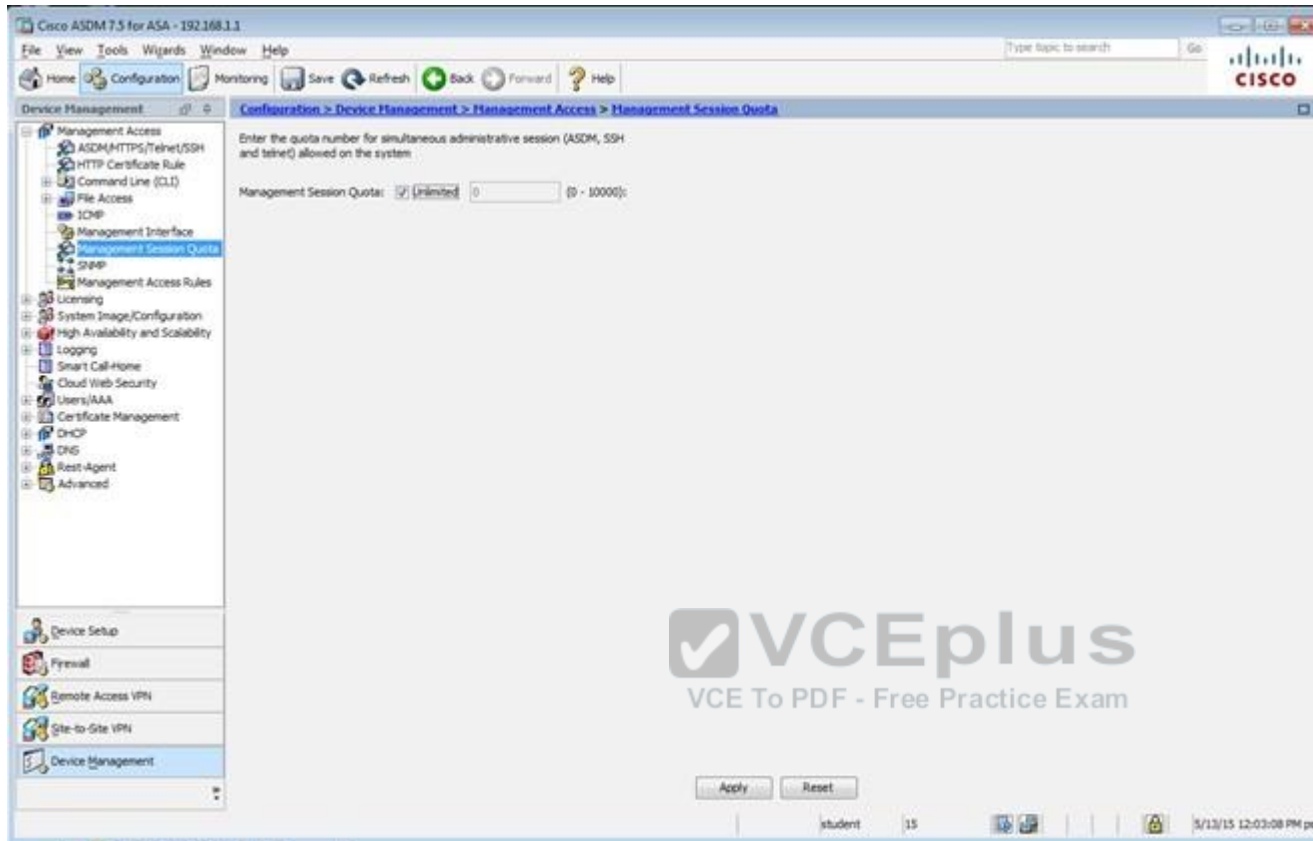
DH Key Exchange: ☒ Group 1 ☐ Group 14

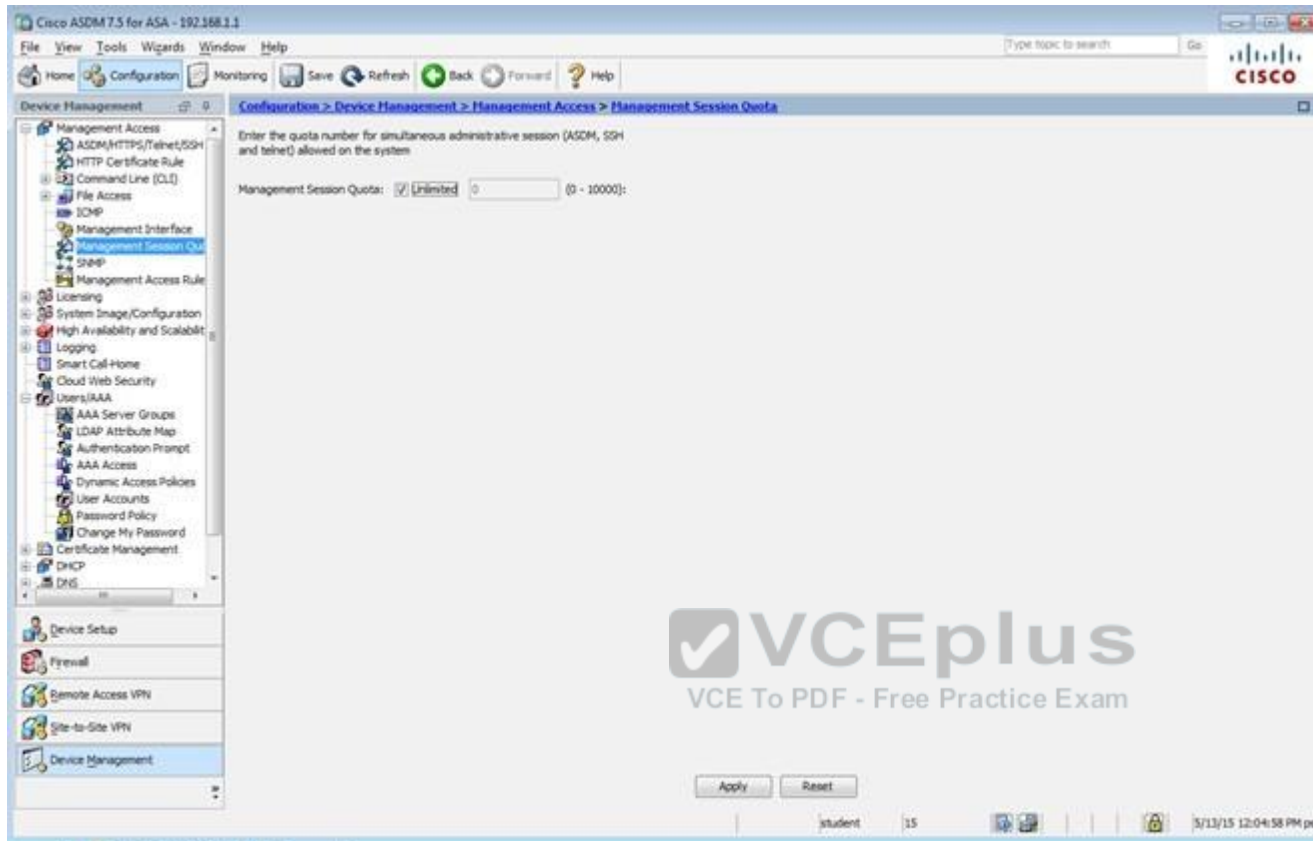
Apply Reset

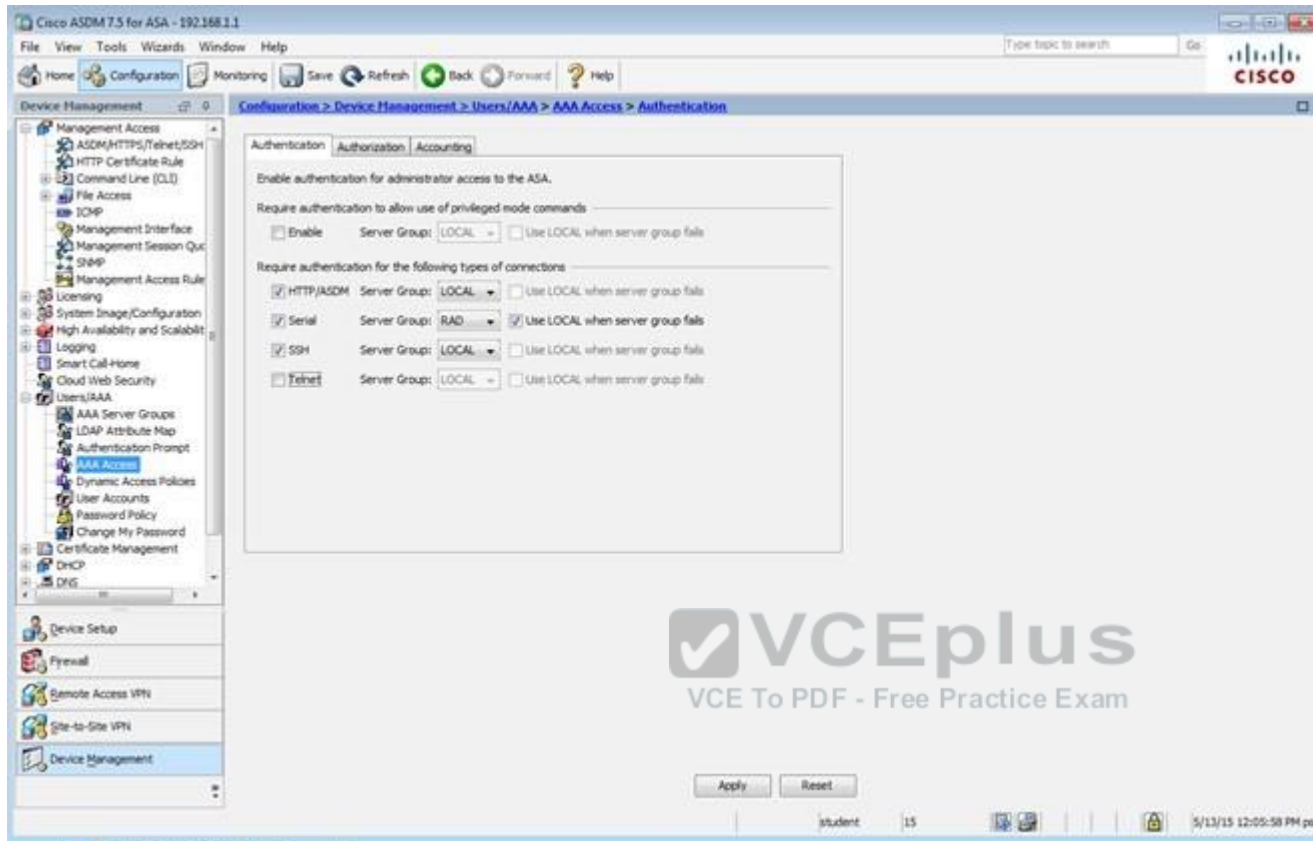
student 15 5/13/15 12:00:38 PM pet

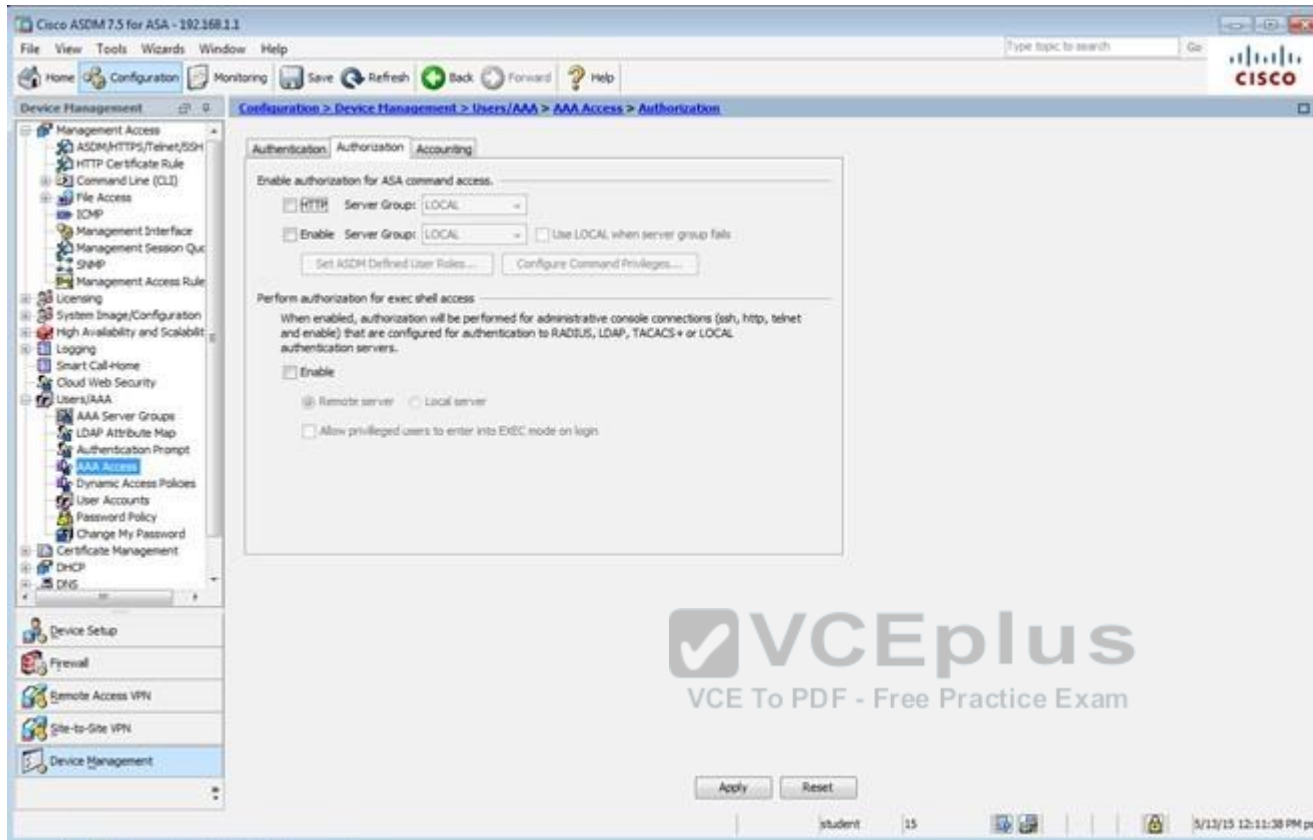


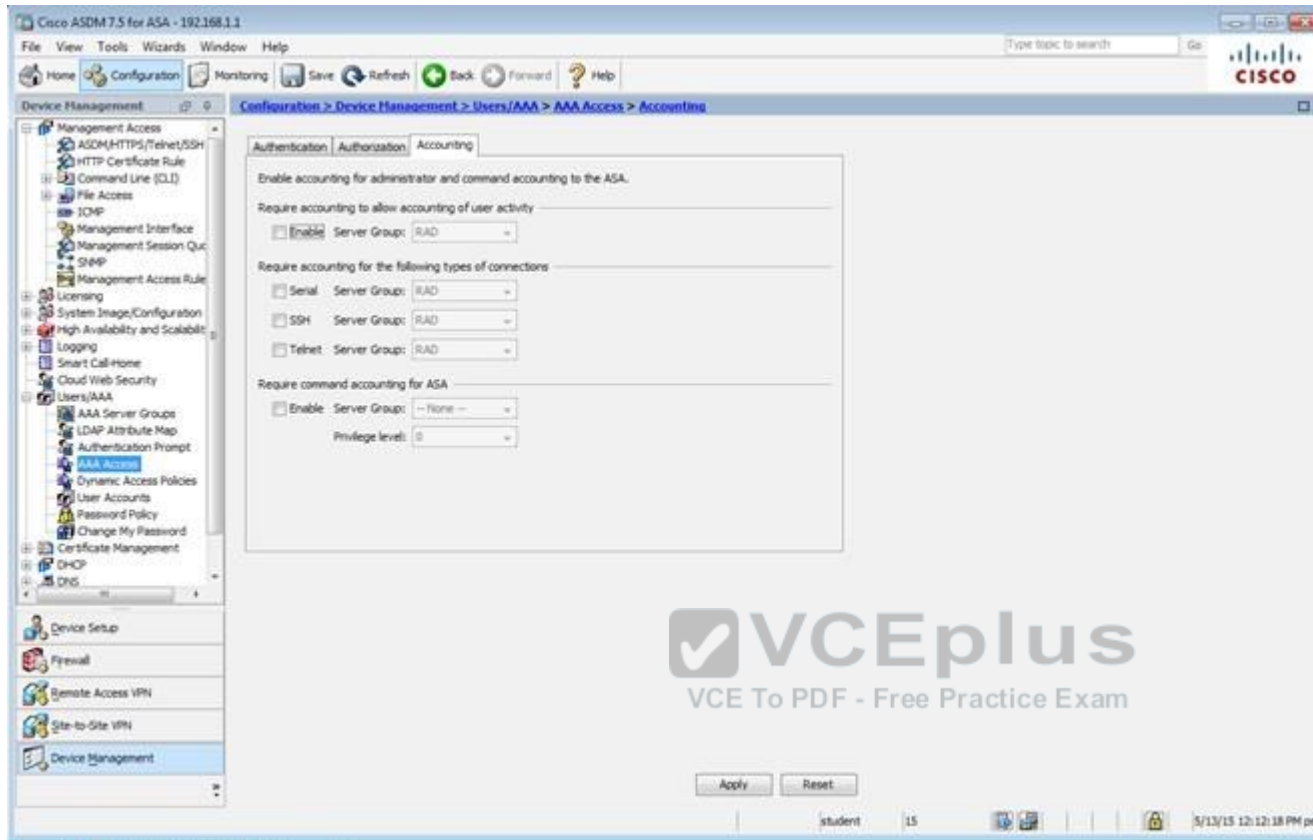


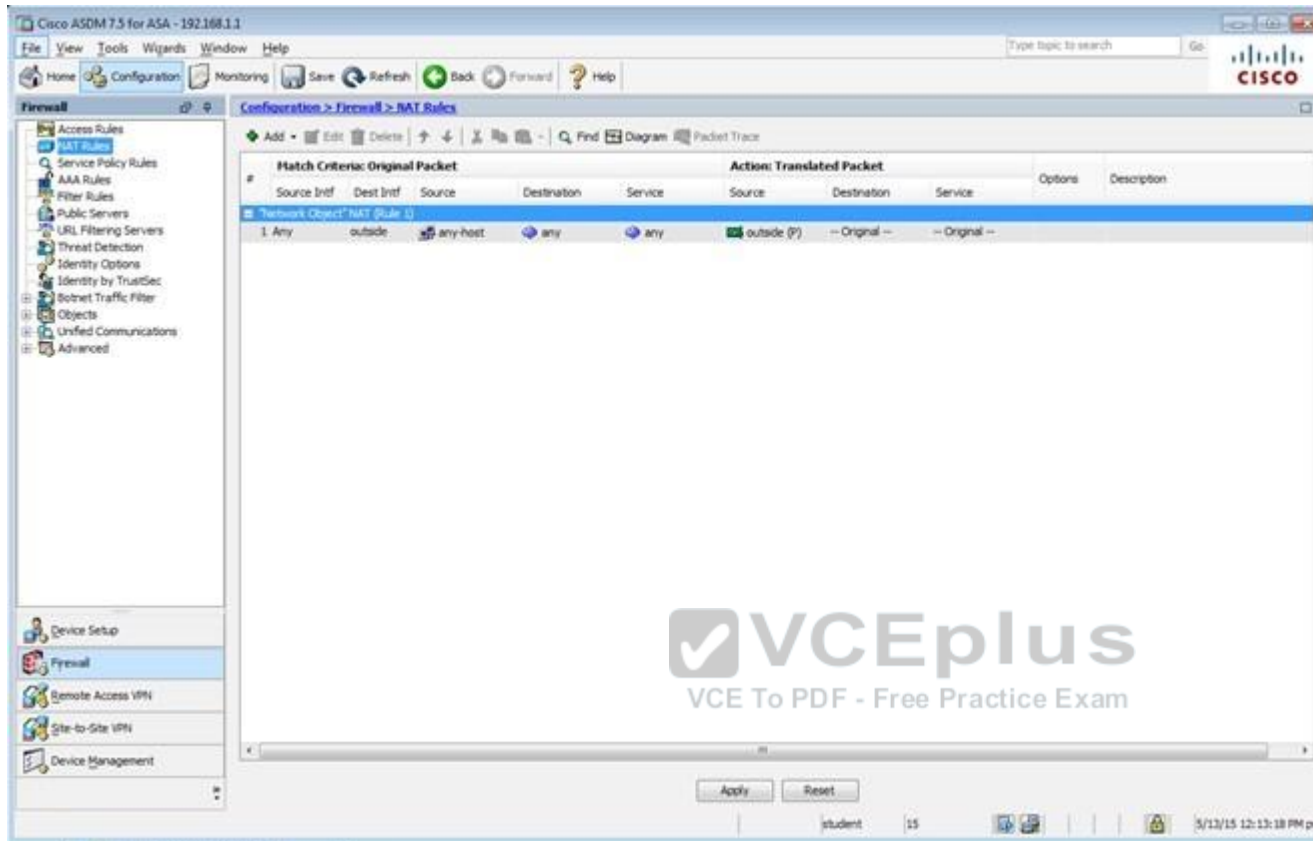


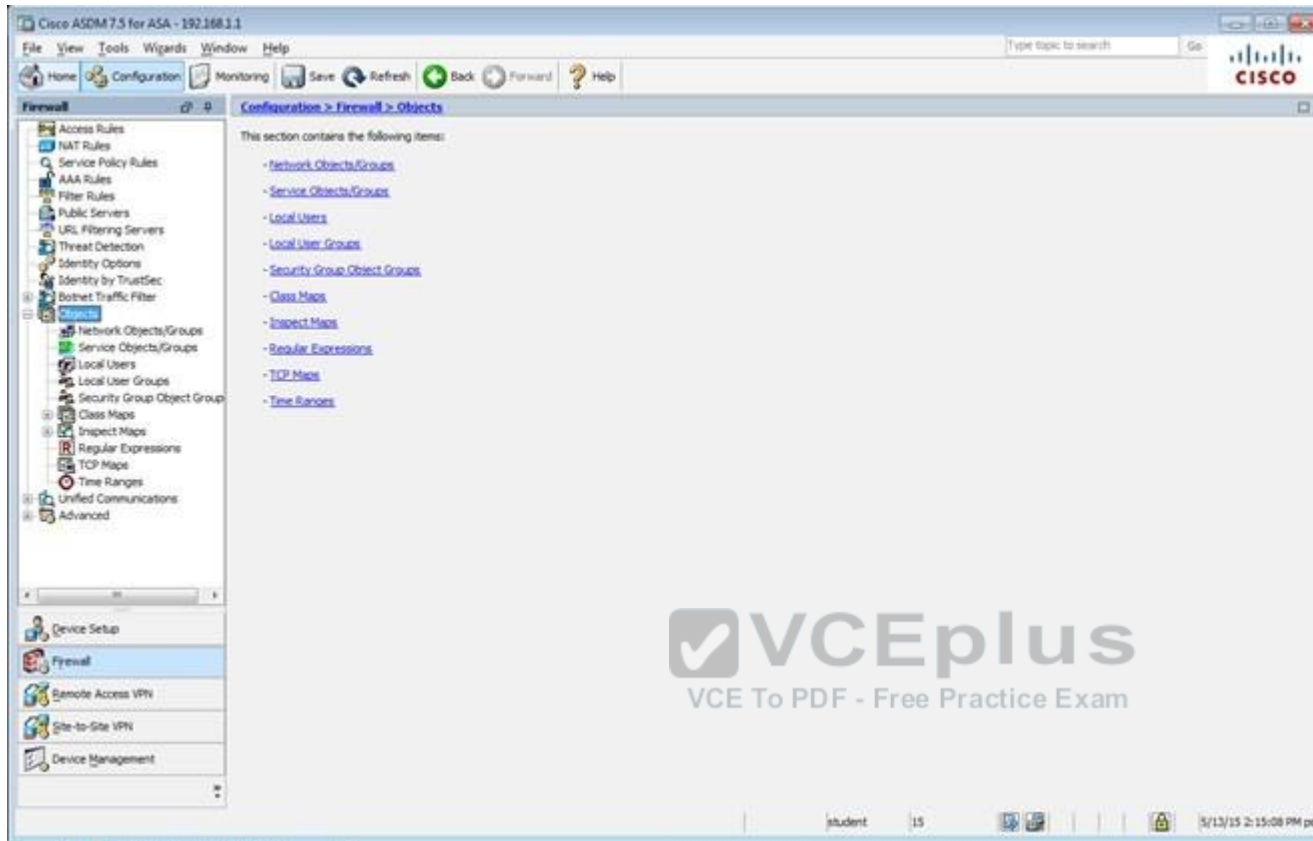












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

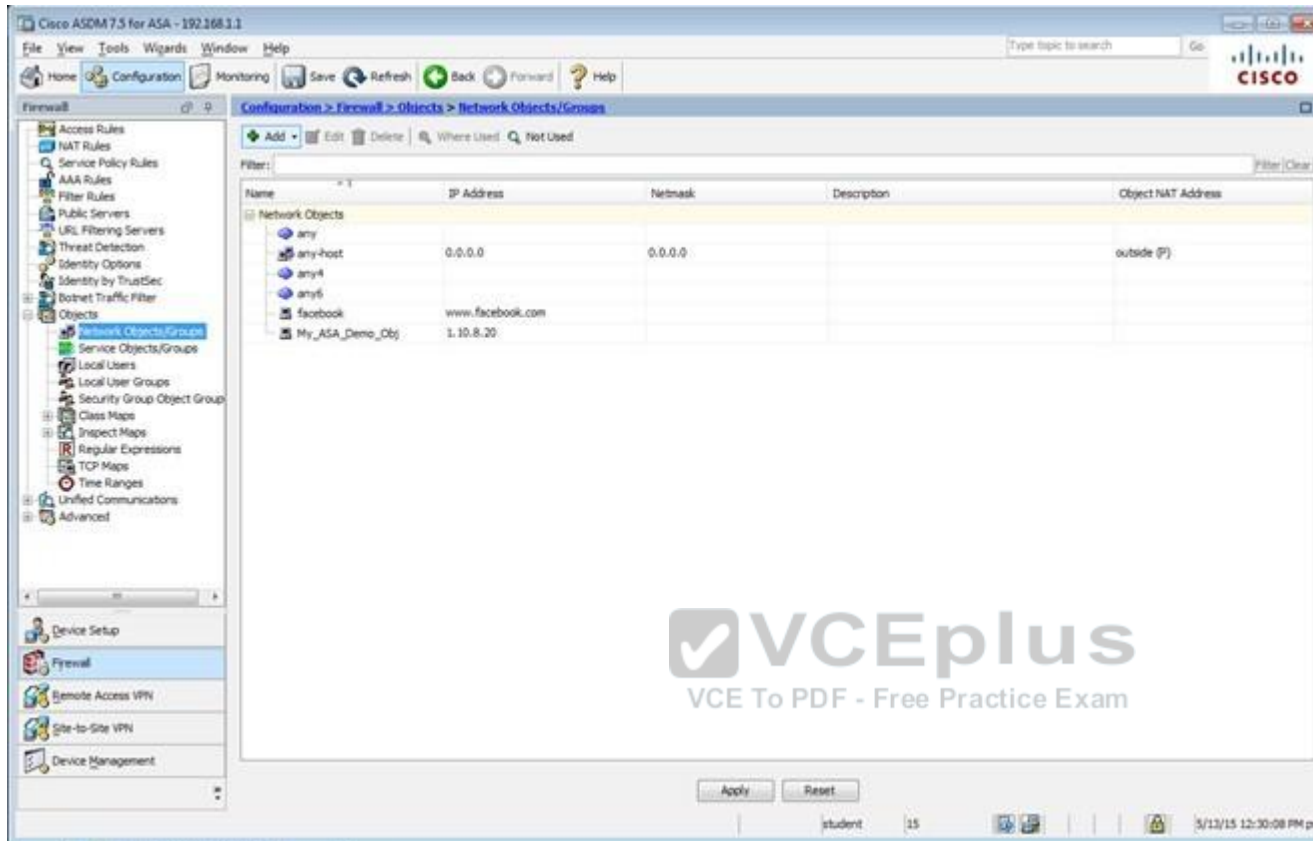
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

Add Edit Delete

End: [ ] [ ] [ ] Match Case

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Service Policy Rules

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

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

Configuration > Firewall > Service Policy Rules

Add Edit Delete Find Diagram Packet Trace

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

Apply Reset

student 15 5/13/15 12:15:48 PM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Access Rules

Access Rules

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

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

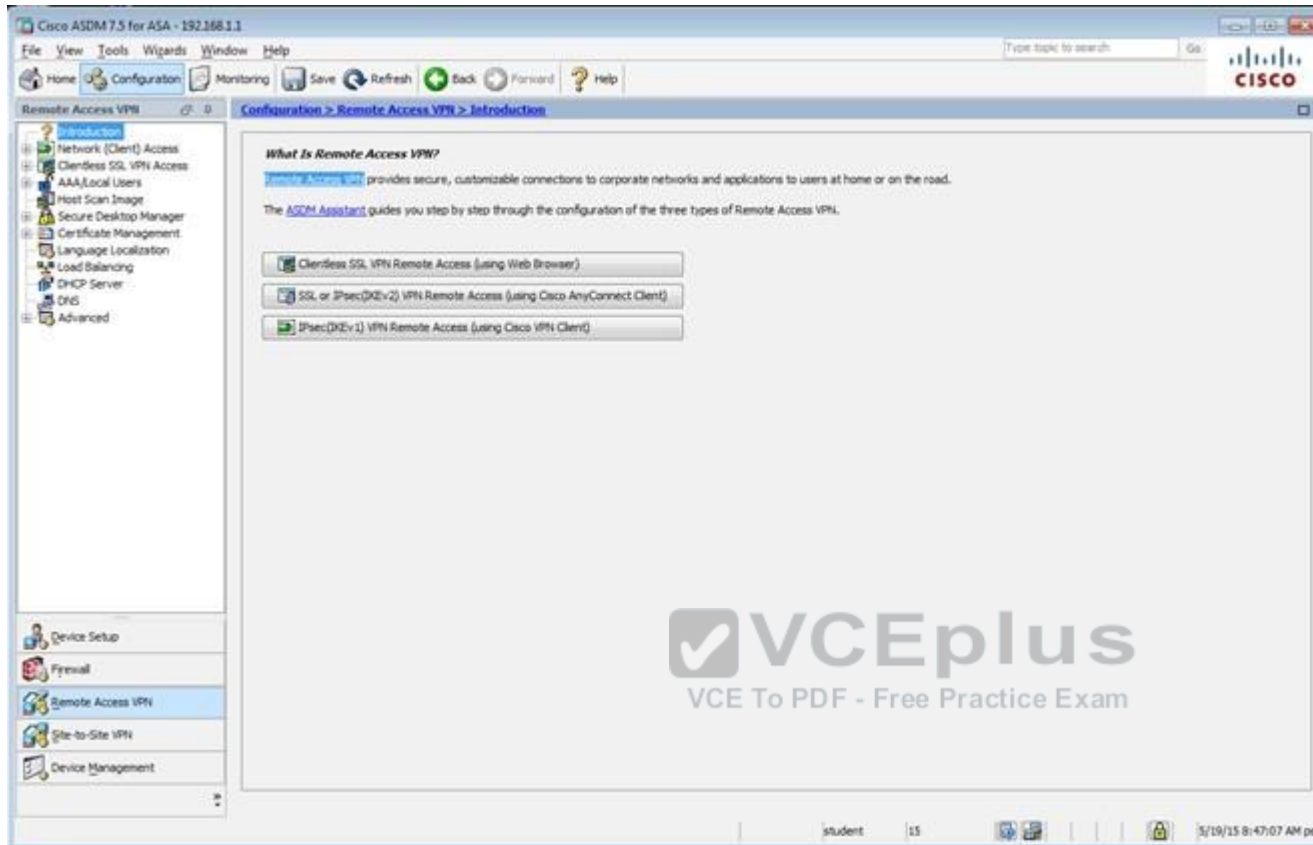
Configuration > Firewall > Access Rules

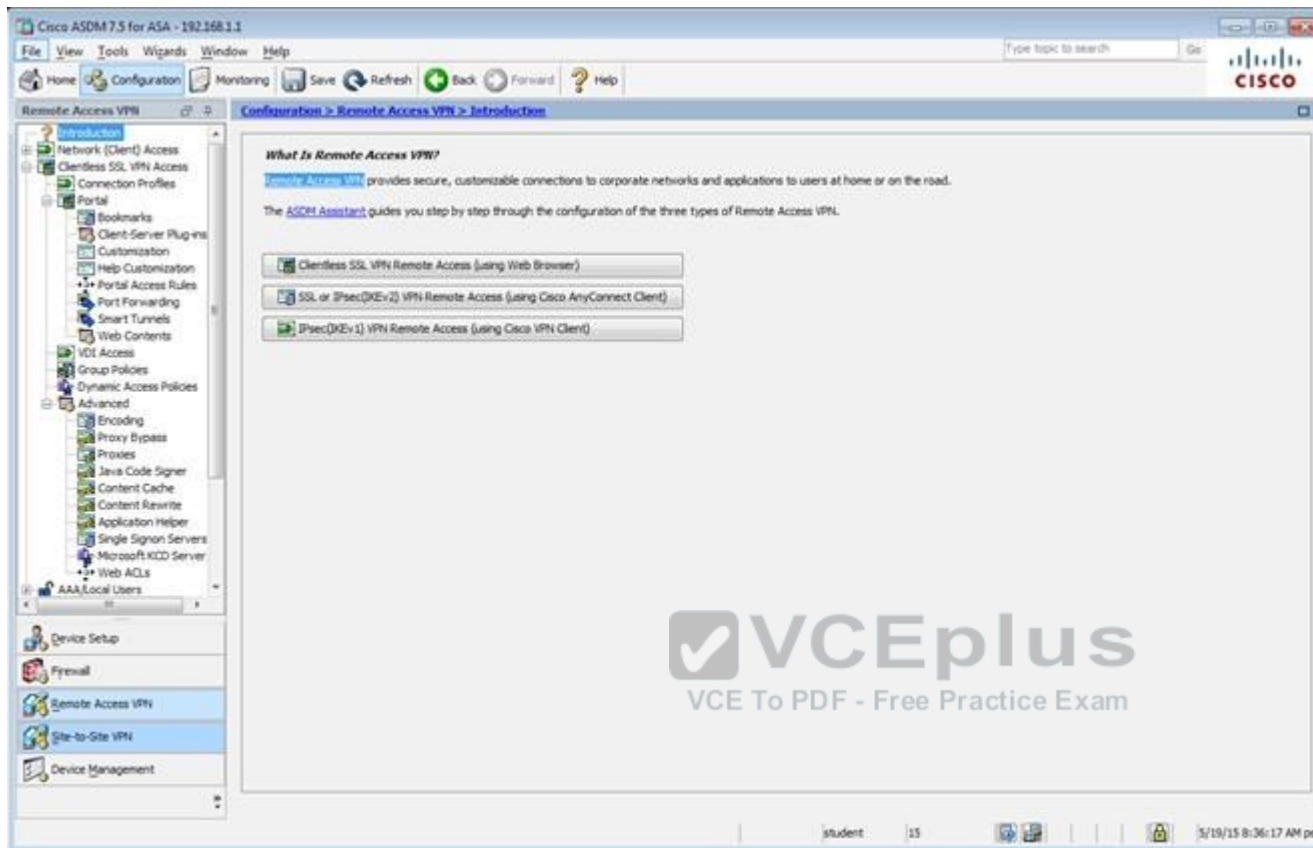
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

| # | Enabled                             | Source Criteria:                    | Destination Criteria: | Service | Action | Hits  | Logging |
|---|-------------------------------------|-------------------------------------|-----------------------|---------|--------|-------|---------|
|   |                                     | Source                              | Destination           |         |        |       |         |
| 1 | <input checked="" type="checkbox"/> | any                                 | Any less secure ne... | HTTP    | Permit |       |         |
| 2 | <input checked="" type="checkbox"/> | inside (1 implicit rule)            | any                   | HTTP    | Permit | 54... |         |
| 3 | <input checked="" type="checkbox"/> | any                                 | any                   | HTTP    | Permit |       |         |
| 4 | <input checked="" type="checkbox"/> | outside (0 implicit incoming rules) | any                   | HTTP    | Permit |       |         |
| 5 | <input checked="" type="checkbox"/> | Global (1 implicit rule)            | any                   | HTTP    | Deny   |       |         |

Apply Reset Advanced...

student 15 5/13/15 12:28:58 PM pst





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

Access Interfaces  
Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

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

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

Add Edit Delete Find: Match Case

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

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

Name: clientless  
Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

☐ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add - Delete (The table is in-line editable.)

| Alias | Enabled                             |
|-------|-------------------------------------|
| test  | <input checked="" type="checkbox"/> |

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add - Delete (The table is in-line editable.)

| URL                        | Enabled                             |
|----------------------------|-------------------------------------|
| https://209.165.201.2/test | <input checked="" type="checkbox"/> |

You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Interface-Specific Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL |
|-----------|--------------|-------------------|
|-----------|--------------|-------------------|

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Secondary Authentication Server Group

Server Group: -- None -- Manage...

☐ Use LOCAL if Server Group fails

☐ Use primary username (Hide secondary username on login page)

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

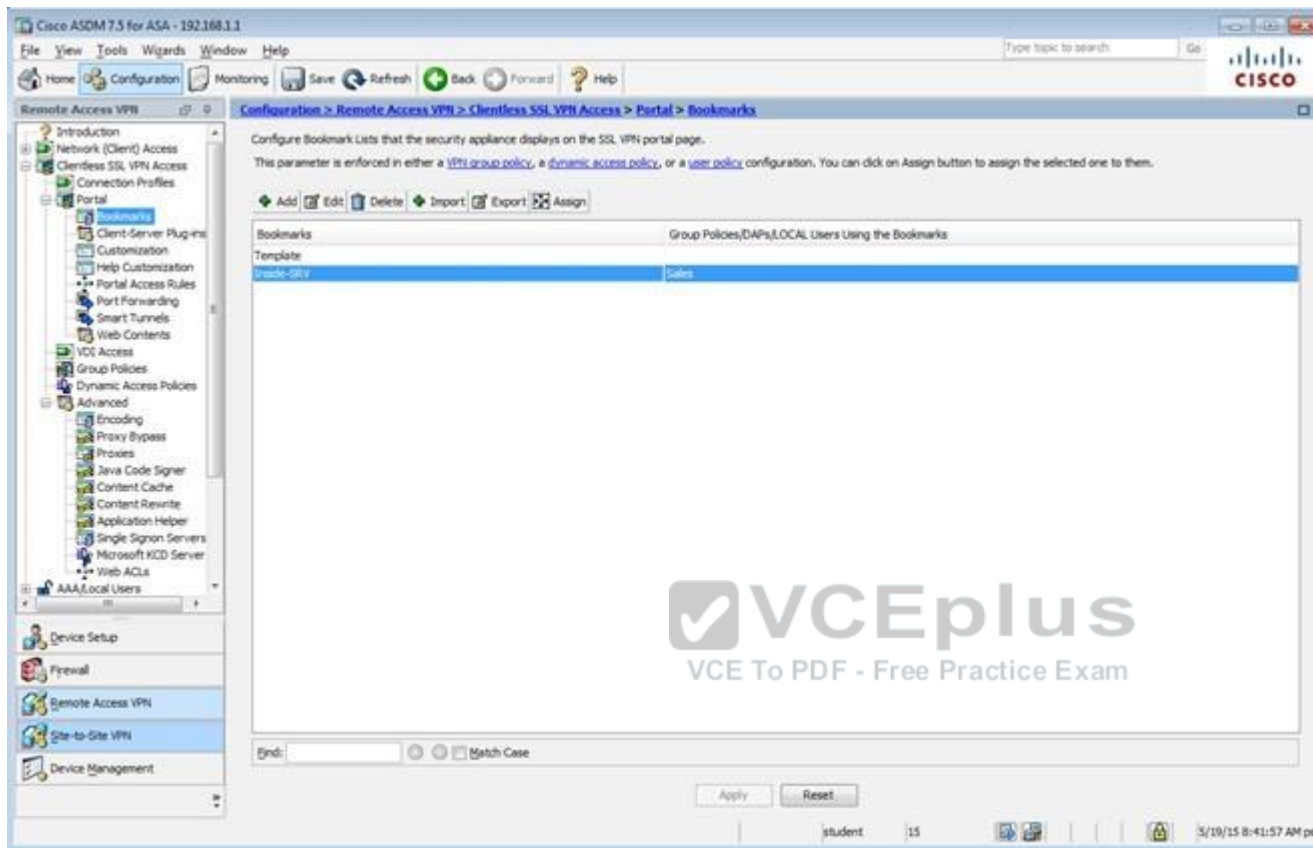
☐ Use the entire DN as the username

☐ Use script to select username

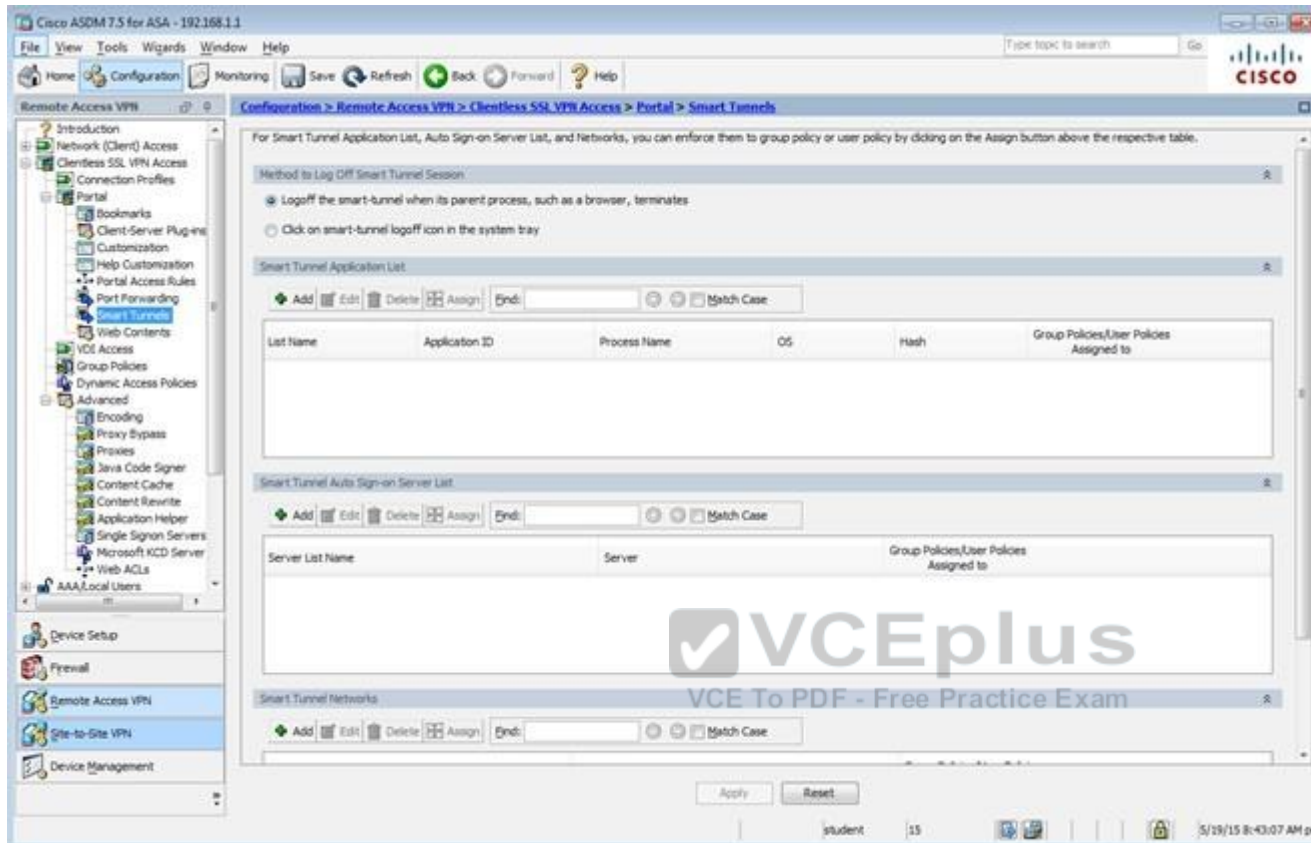
-- None -- + Add Edit Delete

Find:  Next Previous

OK Cancel Help







The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with the following items: Introduction, Network (Client) Access, Clientless SSL VPN Access, Connection Profiles, Portal, Bookmarks, Client-Server Plug-ins, Customization, Help Customization, Portal Access Rules, Port Forwarding (selected), Smart Tunnels, Web Contents, VDI Access, Group Policies, Dynamic Access Policies, Advanced, Encoding, Proxy Bypass, Proxies, Java Code Signer, Content Cache, Content Rewrite, Application Helper, Single Signon Servers, Microsoft KCD Server, Web ACLs, AAA/Local Users, Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management.

The main content area is titled "Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding". It contains the following text:

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

Below the text is a table with the following columns: List Name, Local TCP Port, Remote Server, Remote TCP Port, Description, and Group Policies/User Policies Assigned to. The table is currently empty.

At the bottom of the main content area, there is a "Find:" search bar and a "Match Case" checkbox. Below the search bar are "Apply" and "Reset" buttons.

The status bar at the bottom of the window shows "student", "15", and the date/time "5/19/15 8:43:47 AM pst".

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

◆ Add ◆ Edit ◆ Delete ◆ Assign

| Name                                | Type     | Tunneling Protocol                  | Connection Profiles/Users Assigned To                  |
|-------------------------------------|----------|-------------------------------------|--|
| Clientless                          | Internal | ssl-clientless                      | Clientless   |
| DefaultGroupPolicy (System Default) | Internal | kev1:kev2:ssl-clientless/2to-espsec | DefaultRAGroup/DefaultIL2Group/DefaultADMPGroup/Def... |

Find: [ ] [ ] [ ] Match Case

Apply Reset

student 15 5/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

Tunneling Protocols: ☐ Inherit ☒ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 ☐ IPsec IKEv2 ☐ L2TP/IPsec

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

Find:  ☐ Next ☐ Previous

OK Cancel Help

The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' expanded. The main pane shows the 'Group Policies' configuration page for 'Clientless SSL VPN Access'. The page includes a description of VPN group policies and a table listing the configured policies.

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

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

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

Buttons: Add, Edit, Delete, Assign

| Name                           | Type     | Tunneling Protocol                 | Connection Profiles/Users Assigned To |
|--------------------------------|----------|------------------------------------|---------------------------------------|
| Sales                          | Internal | l2l-clientless                     | Sales                                 |
| DfltGrpPolicy (System Default) | Internal | ikev1ikev2ssl-clientless/2ip-4psec | DfltGrpPolicy                         |

Find: [ ] Match Case [ ]

Buttons: Apply, Reset

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

Edit Internal Group Policy: Sales

General  
More Options  
Customization  
Login Setting  
Single Signon  
VDI Access  
Session Settings

Bookmark List: ☐ Inherit  Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit  Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit  Manage...

Tunnel Option:  Manage...

Smart Tunnel Application: ☒ Inherit  Manage...

☐ Smart Tunnel all Applications (This feature only works with Windows platforms)

☐ Auto Start

Auto Sign-on Server: ☒ Inherit  Manage...

Windows Domain Name (optional):

Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find:  ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DfBGrpPolicy

**General**  
Servers  
Advanced

Name: DfBGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None--

Access Hours: --Unrestricted--

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

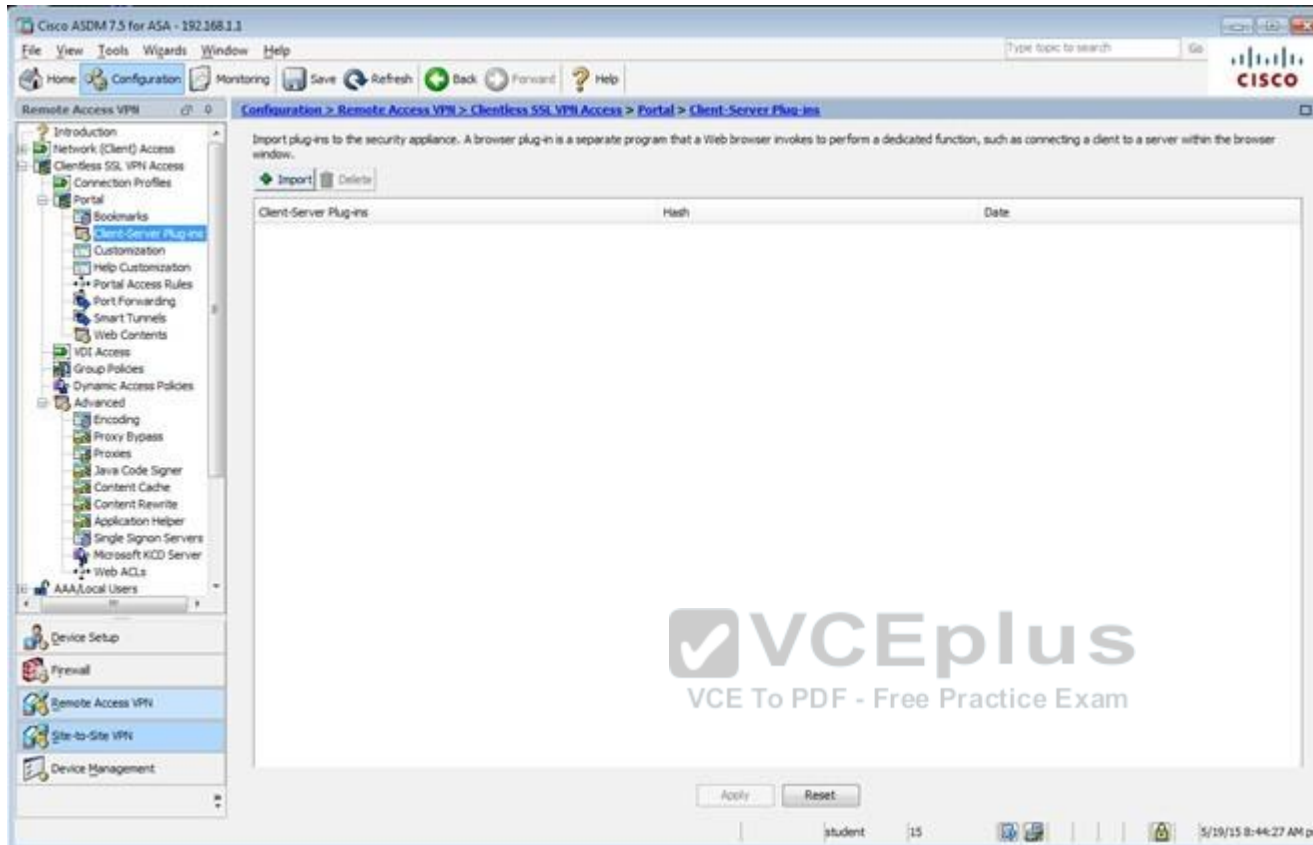
Maximum Connect Time: ☒ Unlimited  minutes

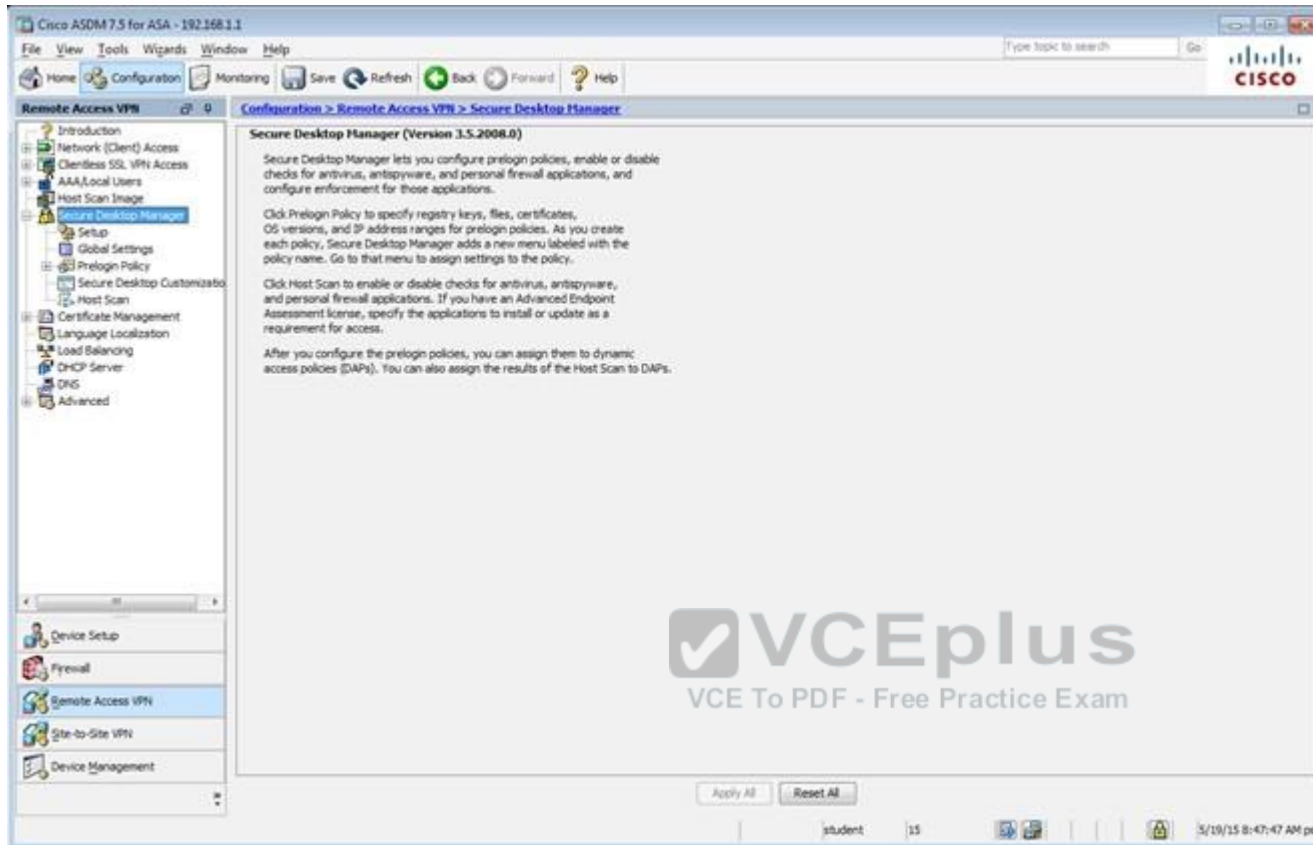
Idle Timeout: ☐ None  30 minutes

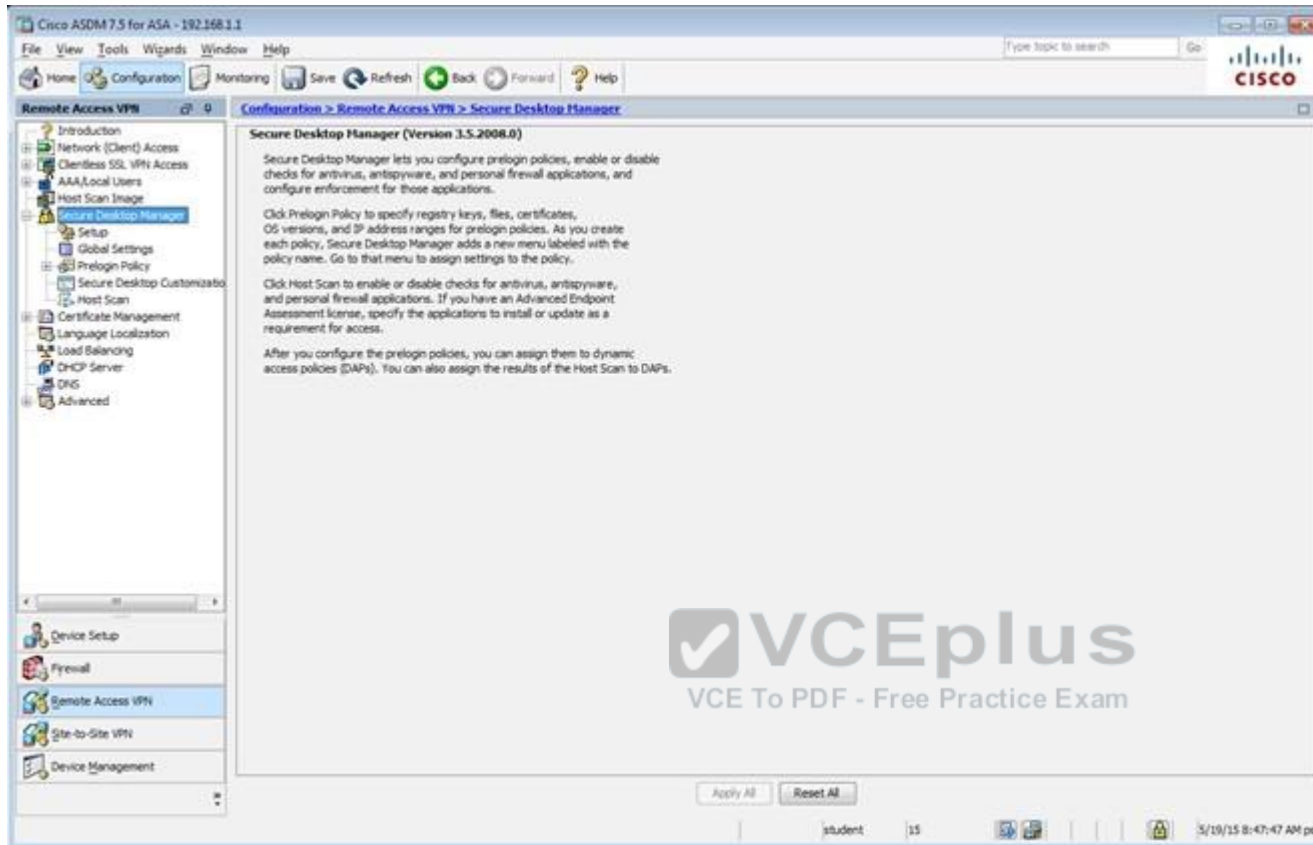
On smart card removal: ☒ Disconnect ☐ Keep the connection

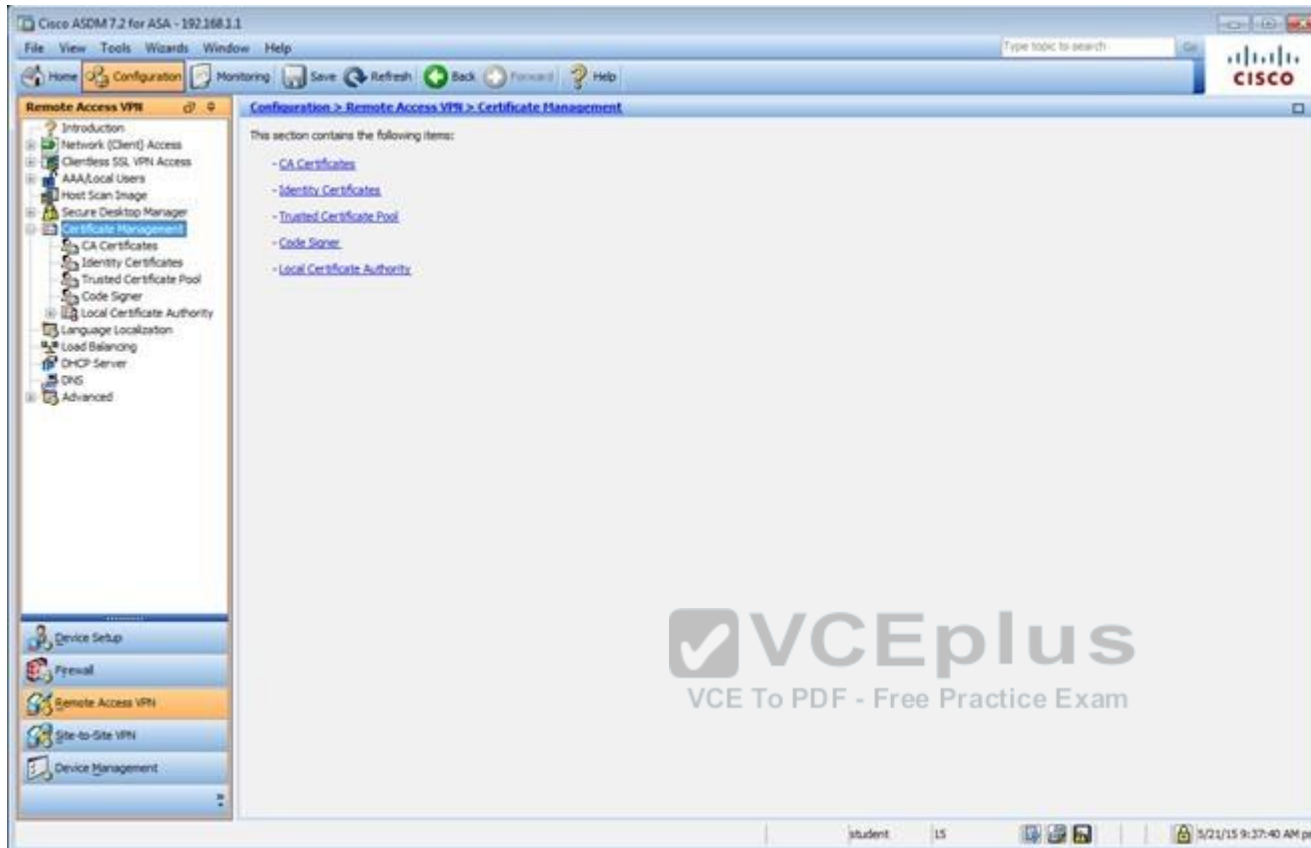
**VCEplus**  
VCE To PDF - Free Practice Exam

Find:





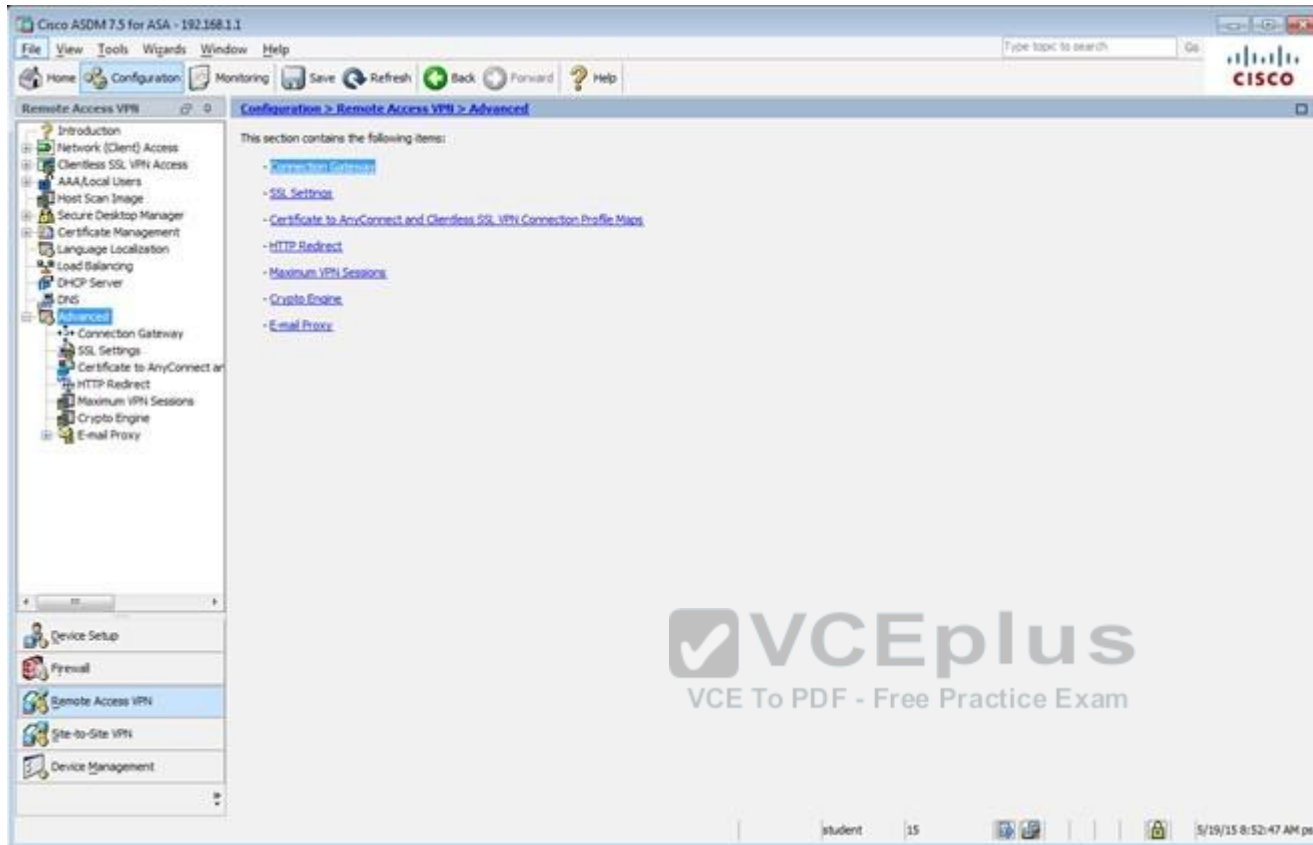


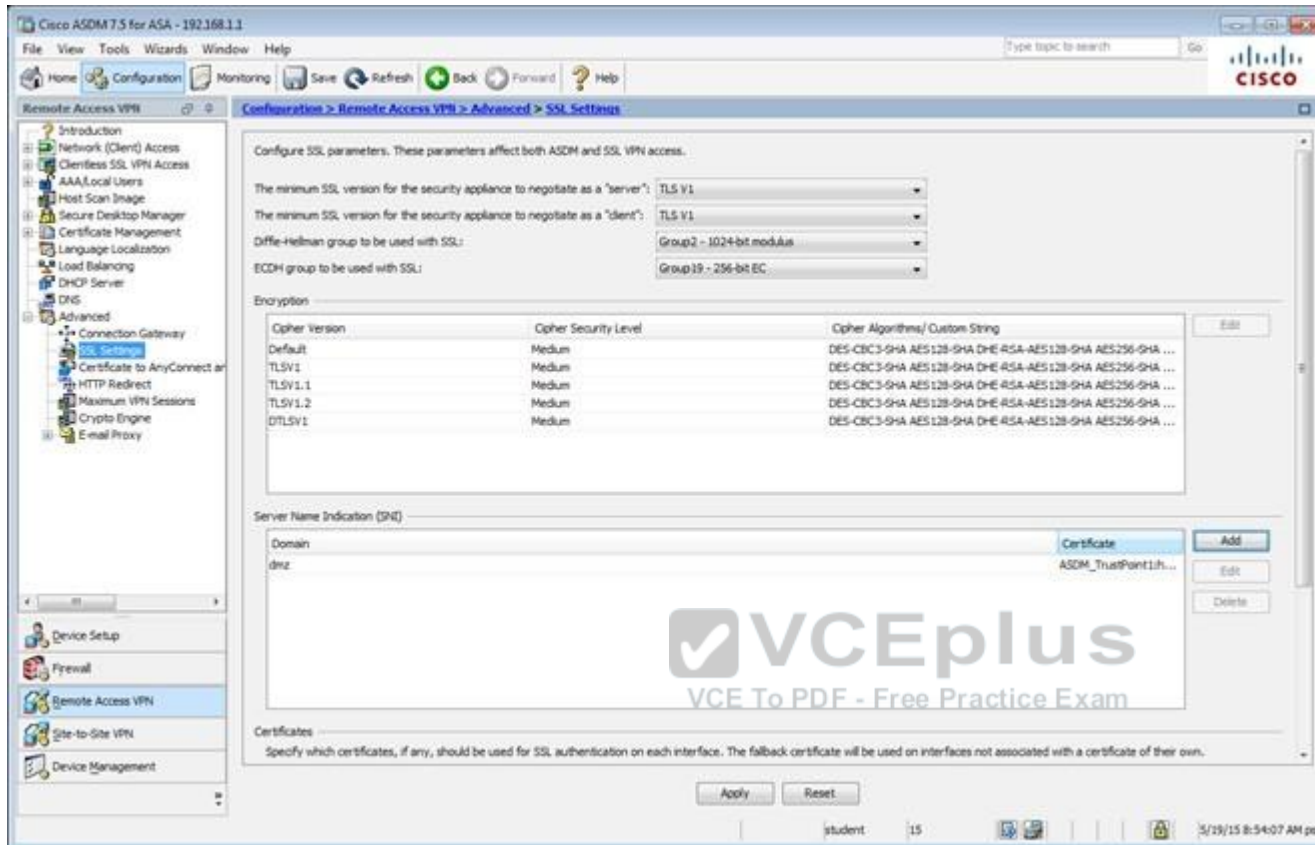


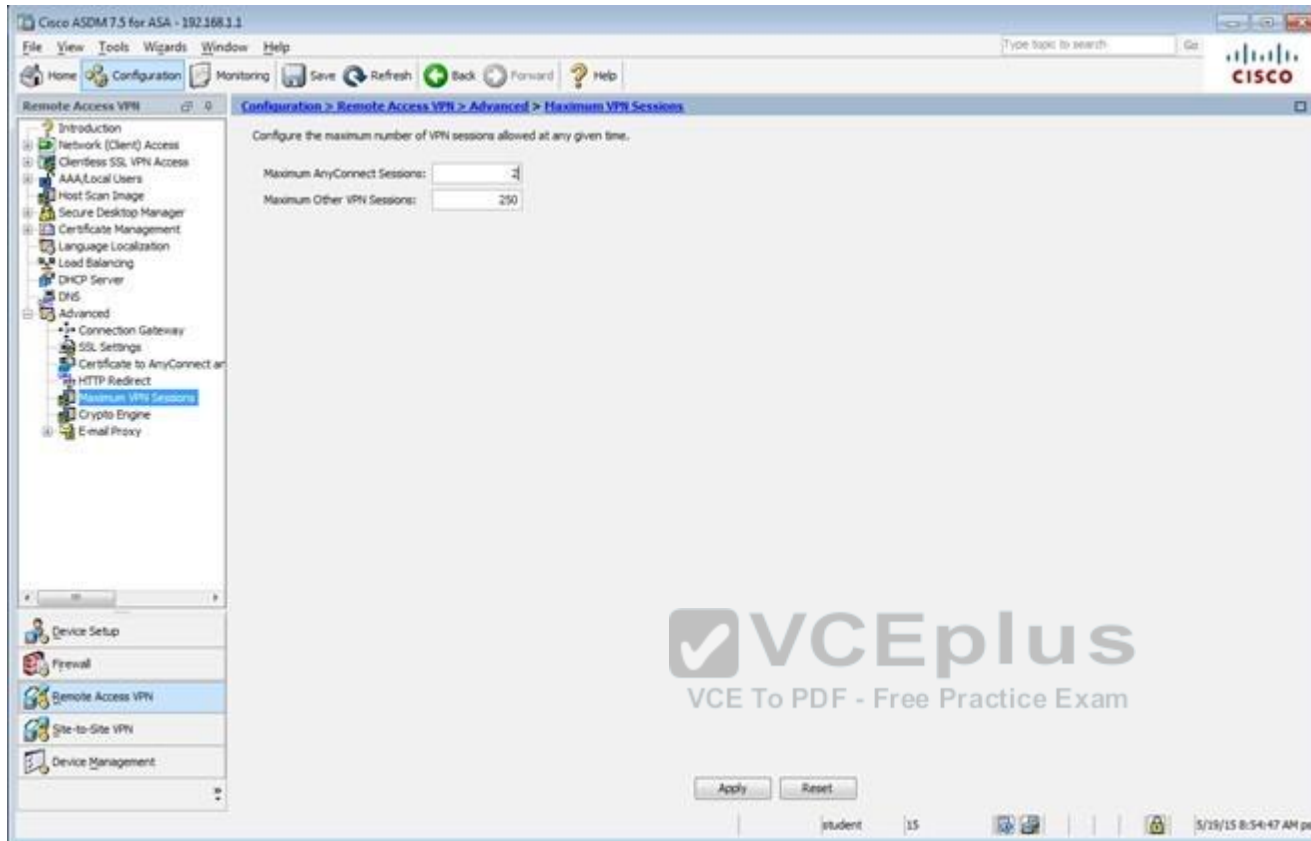
The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with the following data:

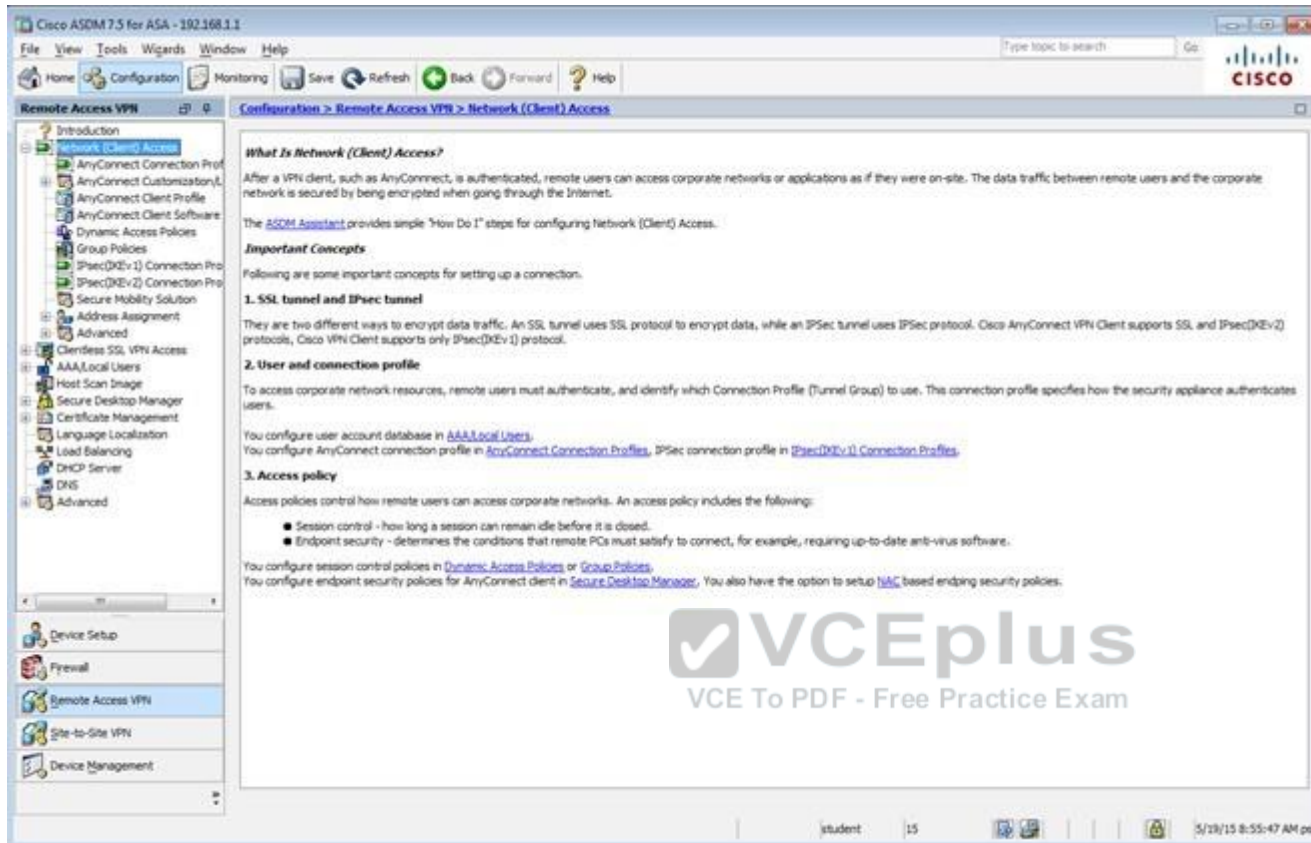
| Issued To                 | Issued By                 | Expiry Date              | Associated Trustpoints | Usage           | Public Key Type |
|---------------------------|---------------------------|--------------------------|------------------------|-----------------|-----------------|
| hostname-wp 17-ASA.sec... | hostname-wp 17-ASA.sec... | 11:10:33 pet Dec 20 2024 | ASDM_TrustPoint1       | Generic Purpose | RSA (2048 bits) |

Below the table, there are sections for 'Certificate Expiration Alerts' and 'Public CA Enrollment'. The 'Public CA Enrollment' section includes a link to 'Enroll ASA SSL certificate with Entrust'. At the bottom, there is a 'Launch ASDM Identity Certificate Wizard' button.









The screenshot displays the Cisco ASDM 7.5 for ASA - 102.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Network (Client) Access'. It contains the following text:

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

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

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

**1. SSL tunnel and IPsec tunnel**  
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.

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

You configure user account database in [AAA Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).

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

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

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

The bottom of the window shows a status bar with 'student', '15', and a timestamp '5/28/15 8:55:47 AM pet'.

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol               | Connection Profiles/Users Assigned To                  |
|--------------------------------|----------|----------------------------------|--|
| Sales                          | Internal | ssl-clientless                   | clientless   |
| DefaultPolicy (System Default) | Internal | (rev 1) ssl-clientless/ssl-ipsec | DefaultPolicyGroupDefaultPolicyGroupDefaultPolicyGroup |

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: DftrGrpPolicy

**General**

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

Name: DftrGrpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: -- None -- Manage...

NAC Policy: -- None -- Manage...

Access Hours: -- Unrestricted -- Manage...

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

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

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKv1) Connection Profiles

Introduction  
Network (Client) Access  
AnyConnect Connection Profile  
AnyConnect Customization...  
AnyConnect Client Profile  
AnyConnect Client Software  
Dynamic Access Policies  
Group Policies  
IPsec(IKv1) Connection Profile  
IPsec(IKv2) Connection Profile  
Secure Mobility Solution  
Advanced  
Clientless SSL VPN Access  
AAA/Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DHCP  
Advanced

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

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dmt       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

| Name              | IPsec Enabled                       | L2TP/IPsec Enabled                  | Authentication Server Group | Group Policy  |
|-------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultVRAGroup   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| DefaultIKEV1Group | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| Clientless        | <input type="checkbox"/>            | <input type="checkbox"/>            | LOCAL                       | Sales         |

Find:  Match Case

Apply Reset

student 15 5/19/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

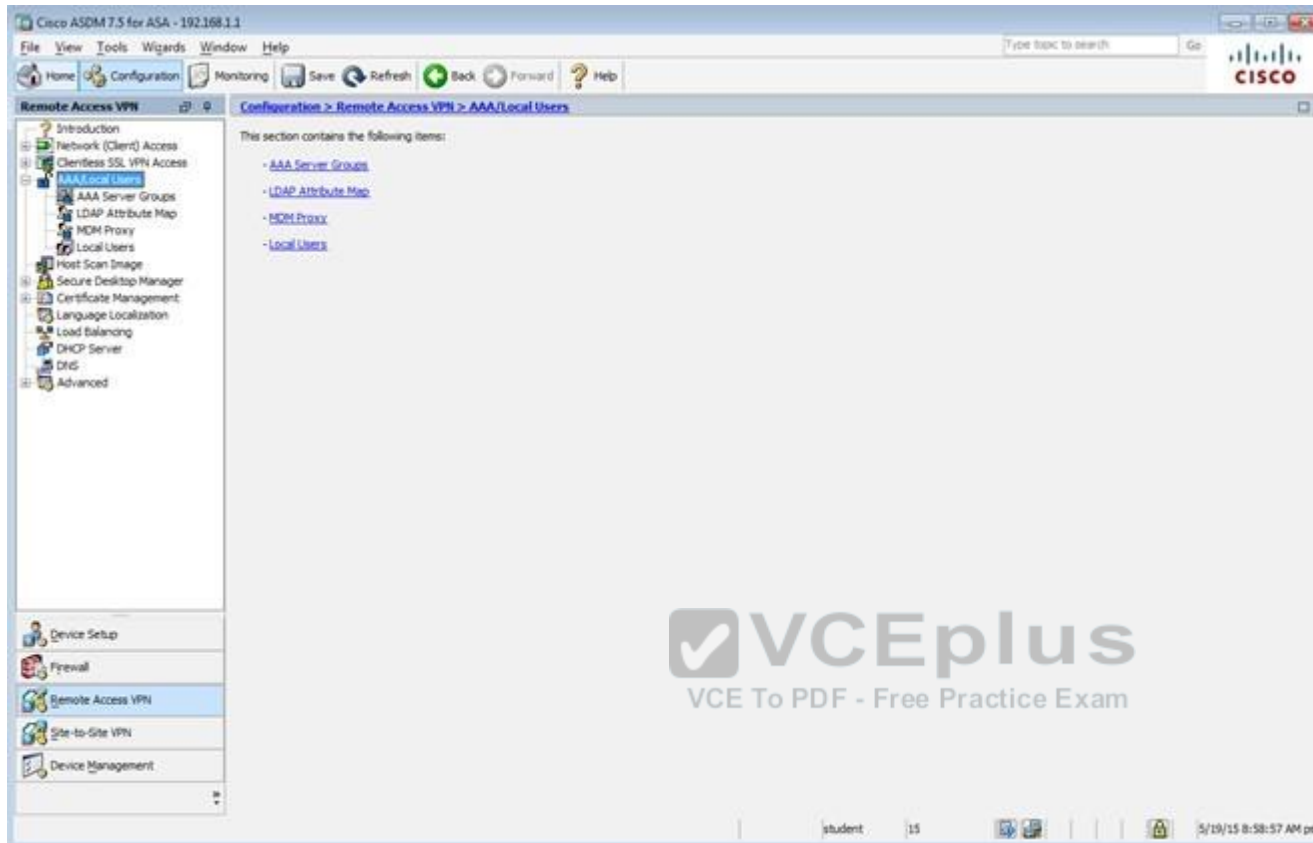
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

End:

| Name            | SSL Enabled                         | IPsec Enabled                       | Aliases | Authentication Method | Group Policy  |
|-----------------|-------------------------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| DefaultEAPGroup | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | DefaultPolicy |
| Clientless      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | yes     | SSL (OCSP)            | Clientless    |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction  
Network (Client) Access  
Clientless SSL VPN Access  
AAA/Local Users  
AAA Server Groups  
LDAP Attribute Map  
MDM Proxy  
Local Users  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DNS  
Advanced

Create entries in the ASA local user database.

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

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

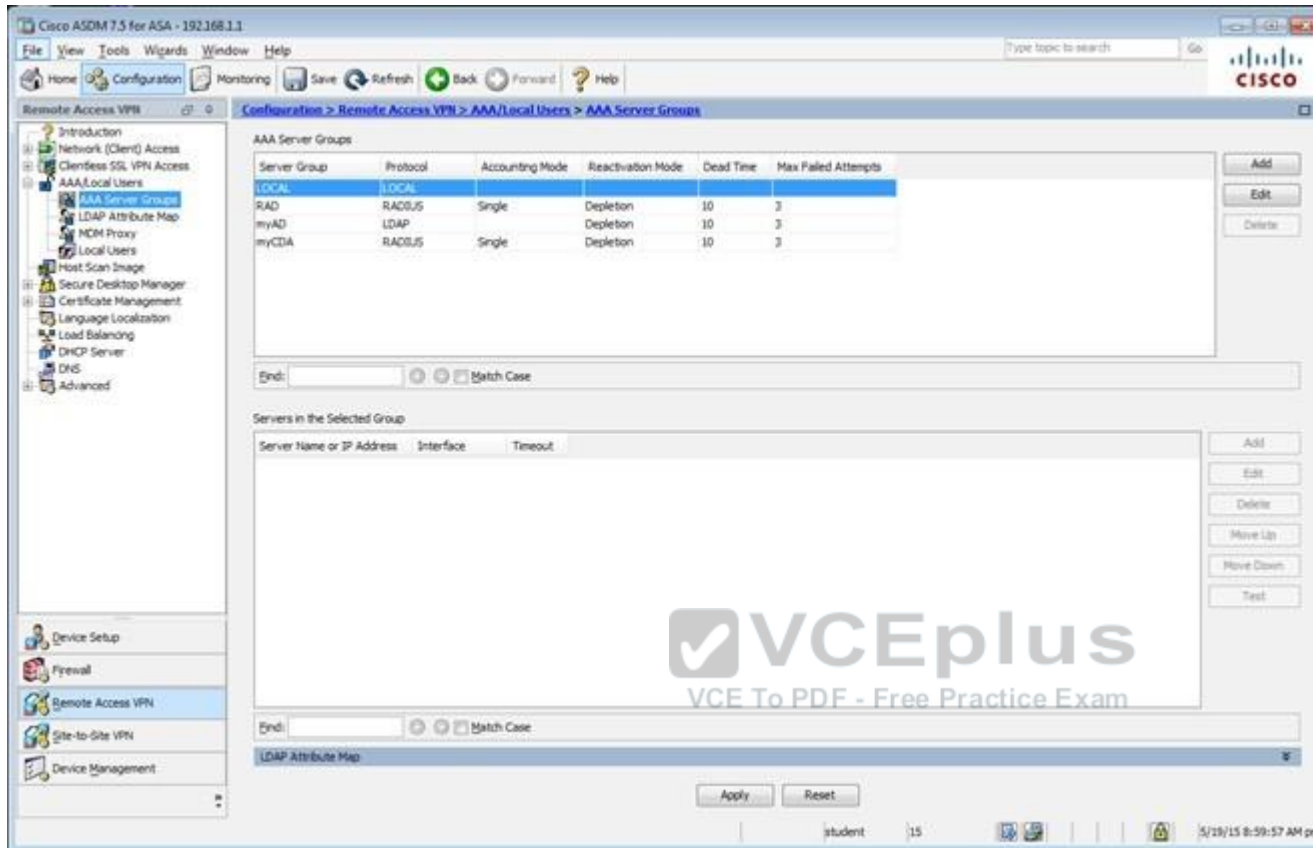
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

Add Edit Delete

Find: Match Case

Apply Reset

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



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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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

**Virtual Terminal**

Home Configuration Monitoring Save Refresh Back Forward Help

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

**Remote Access VPN**

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

**Access Interfaces**

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...

Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

**Login Page Setting**

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

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

☐ Shutdown portal login page.

**Connection Profiles**

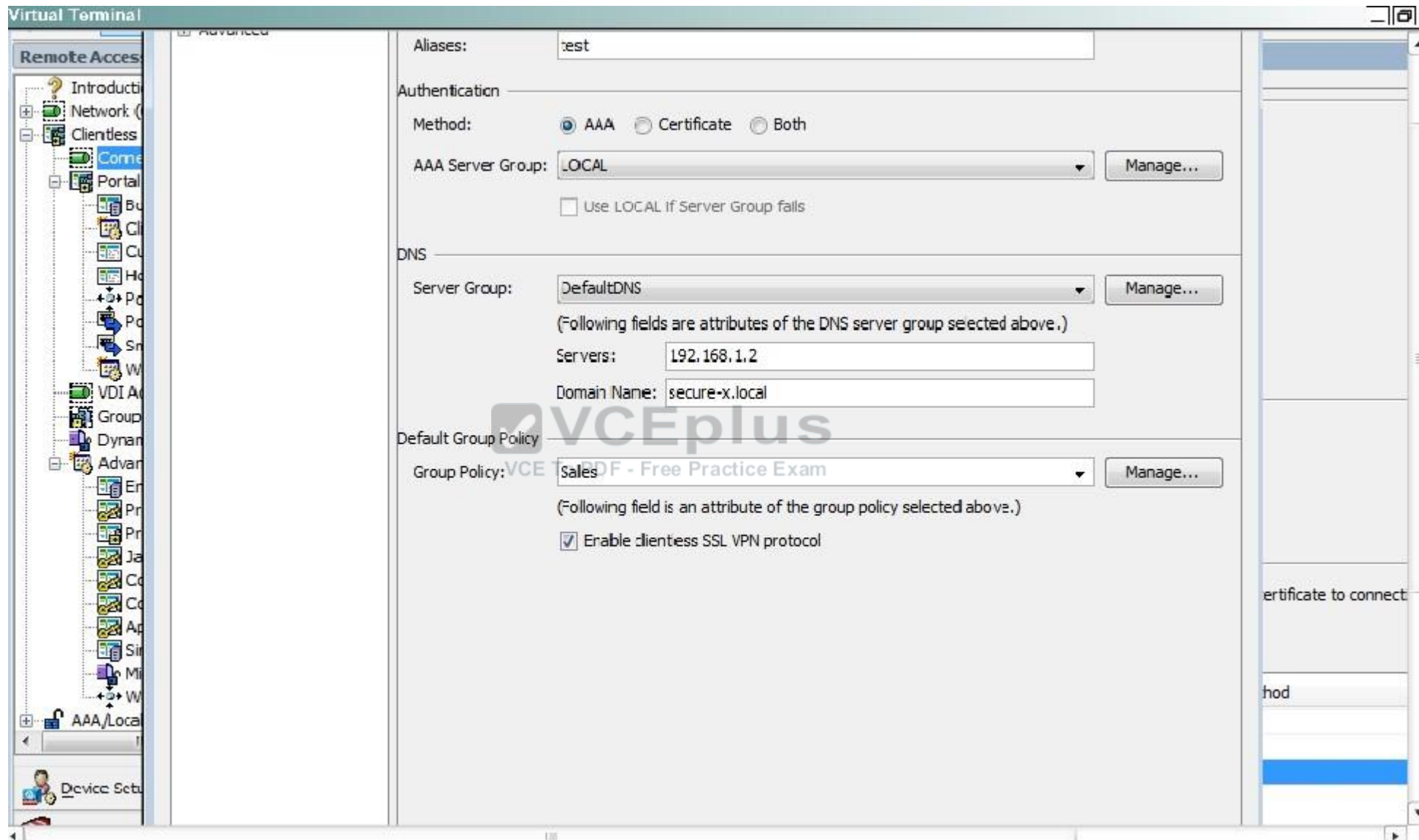
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connect

+ Add Edit Delete Find: Match Case

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

Device Setup

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](http://www.cisco.com)) by opening the inside PC command prompt window. In this simulation, only testing pings to [www.cisco.com](http://www.cisco.com) will work.

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

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

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

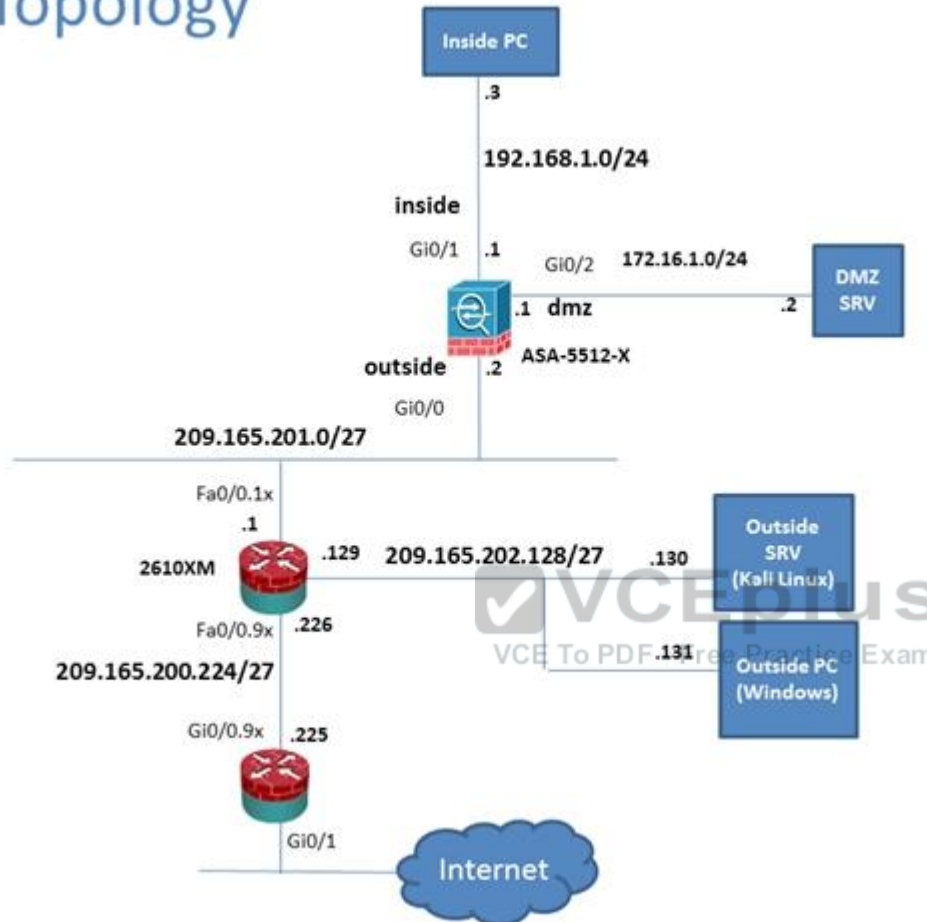
#### Note:

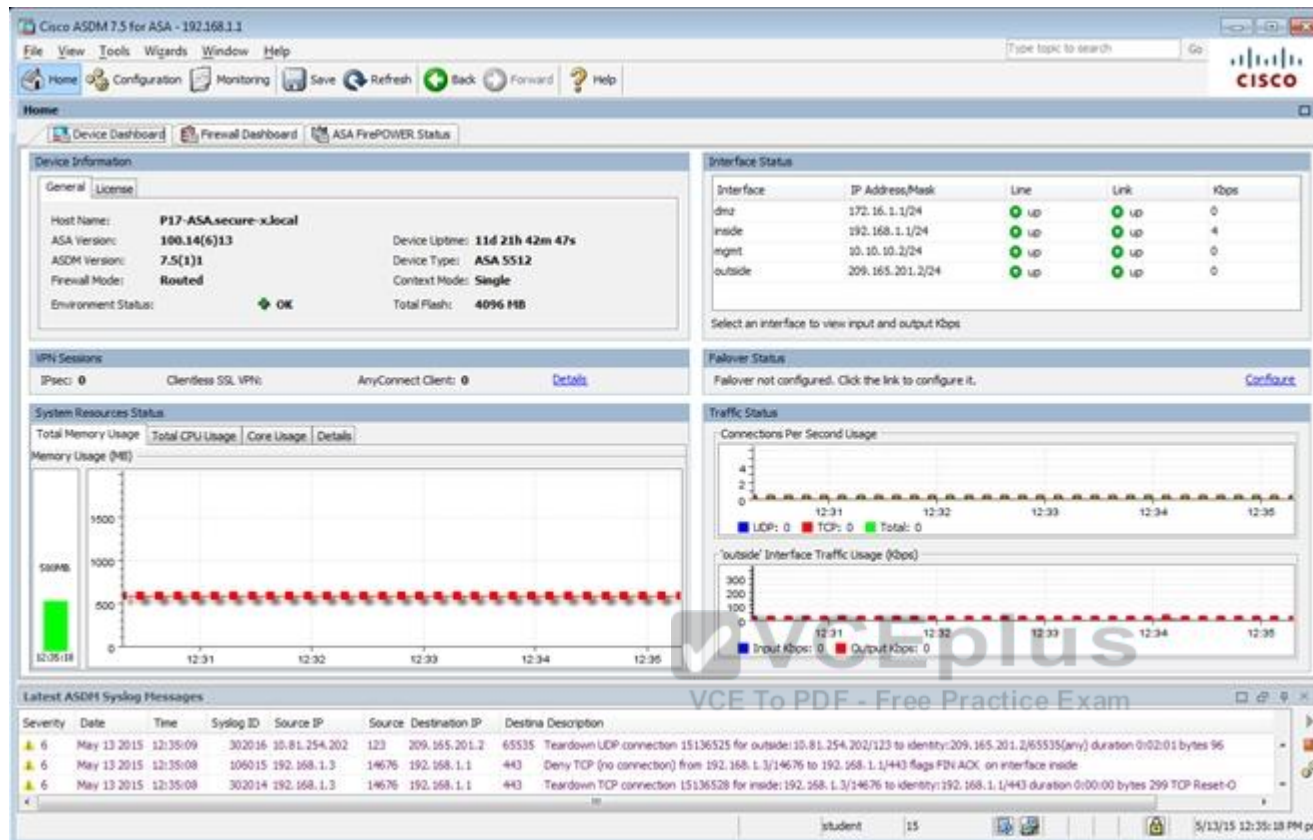
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.

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

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

## Lab Topology





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address    | MAC Address    | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside   | 209.165.201.1 | 000c.3014.3600 | No        |
| inside    | 192.168.1.4   | 0050.5633.3333 | No        |
| inside    | 192.168.1.3   | 0050.5611.1111 | No        |
| inside    | 192.168.1.2   | 0050.5622.2222 | No        |
| inside    | 192.168.1.56  | 0050.5692.5c7b | No        |
| inside    | 192.168.1.55  | 0006.85e5.98f3 | No        |
| dmz       | 172.16.1.2    | 0050.5644.4444 | No        |
| mgmt      | 10.10.10.1    | 000c.3014.3820 | No        |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

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

Interfaces

VPN

Botnet Traffic Filter

Routing

Properties

Logging

Type Active Cumulative Peak Concurrent Inactive

Clientless VPN

Browser

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

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

Details

Logout

Ping

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- Logout Sessions

Refresh

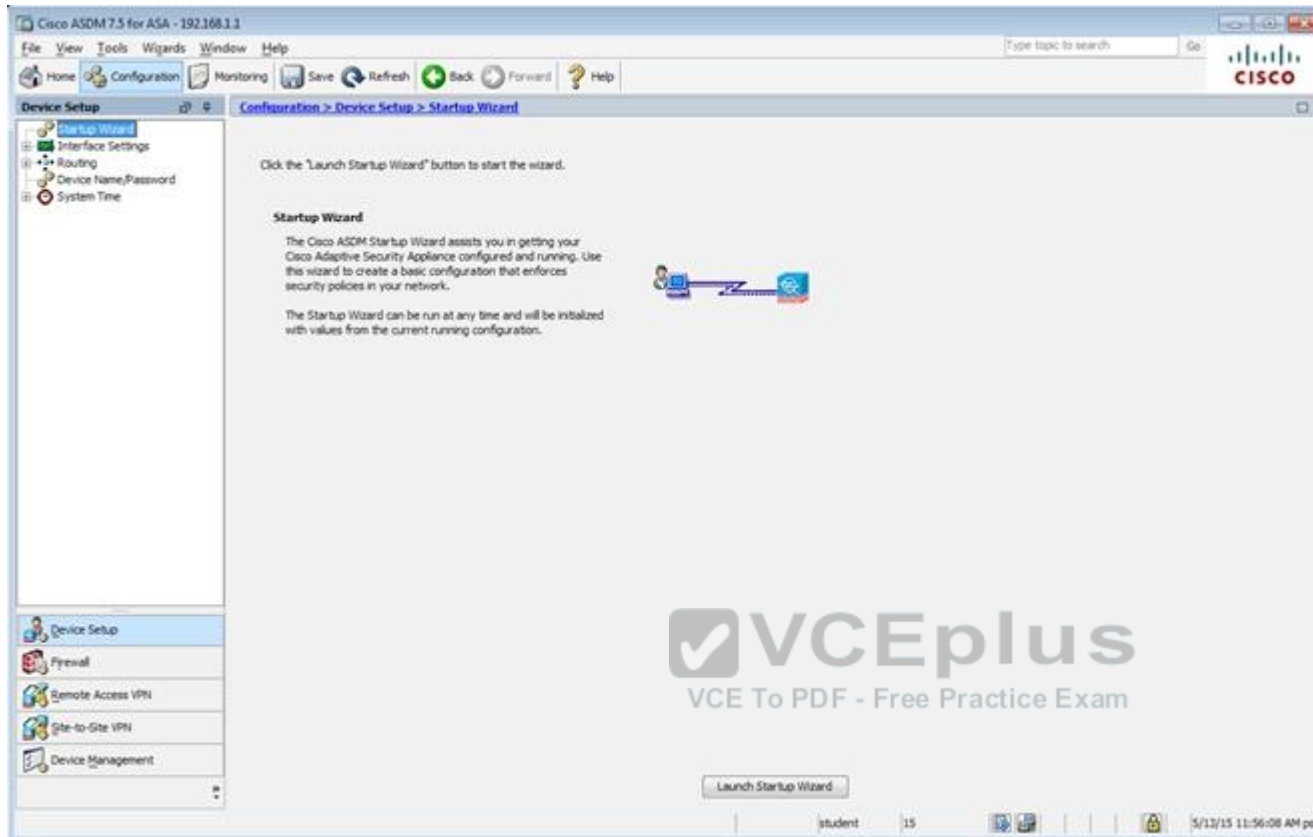
Last Updated: 5/19/15 9:33:12 AM

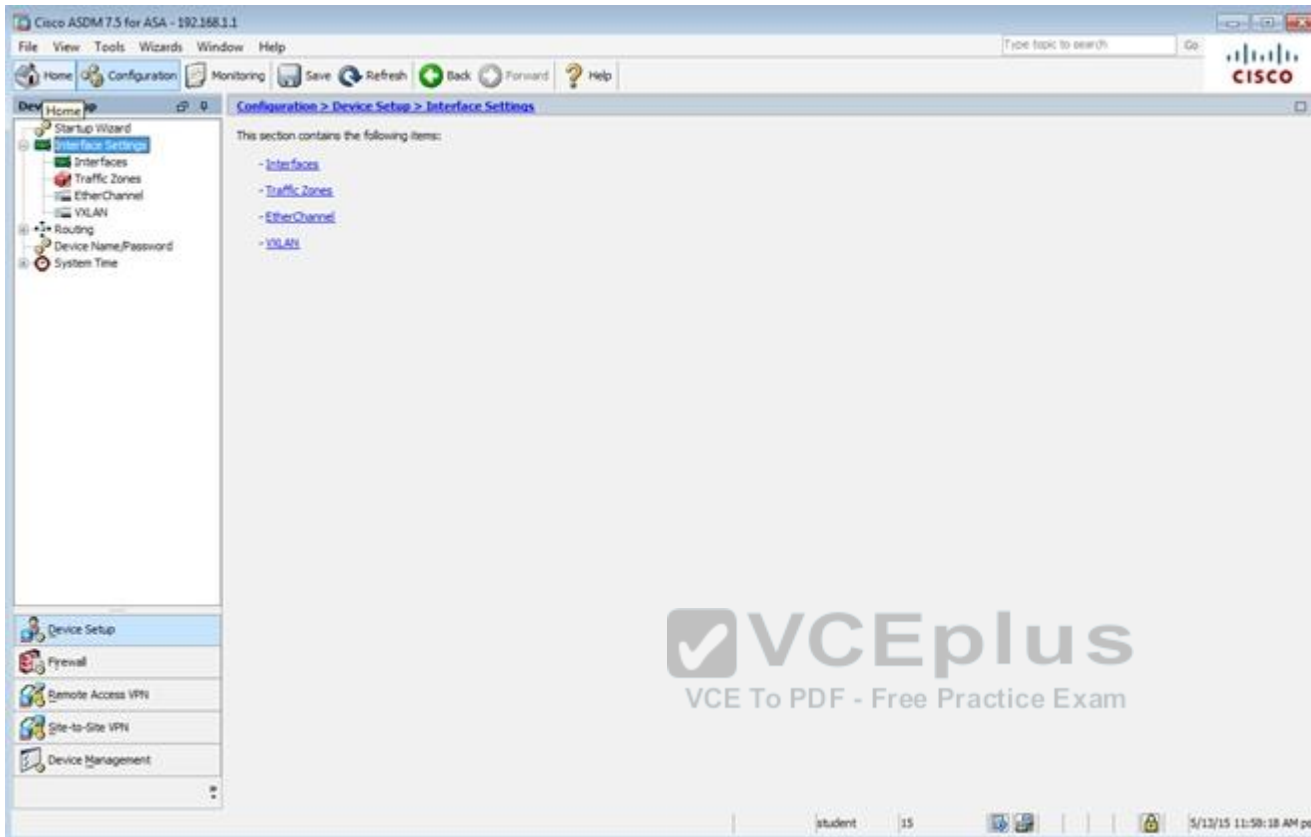
Data Refreshed Successfully.

student 15

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

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

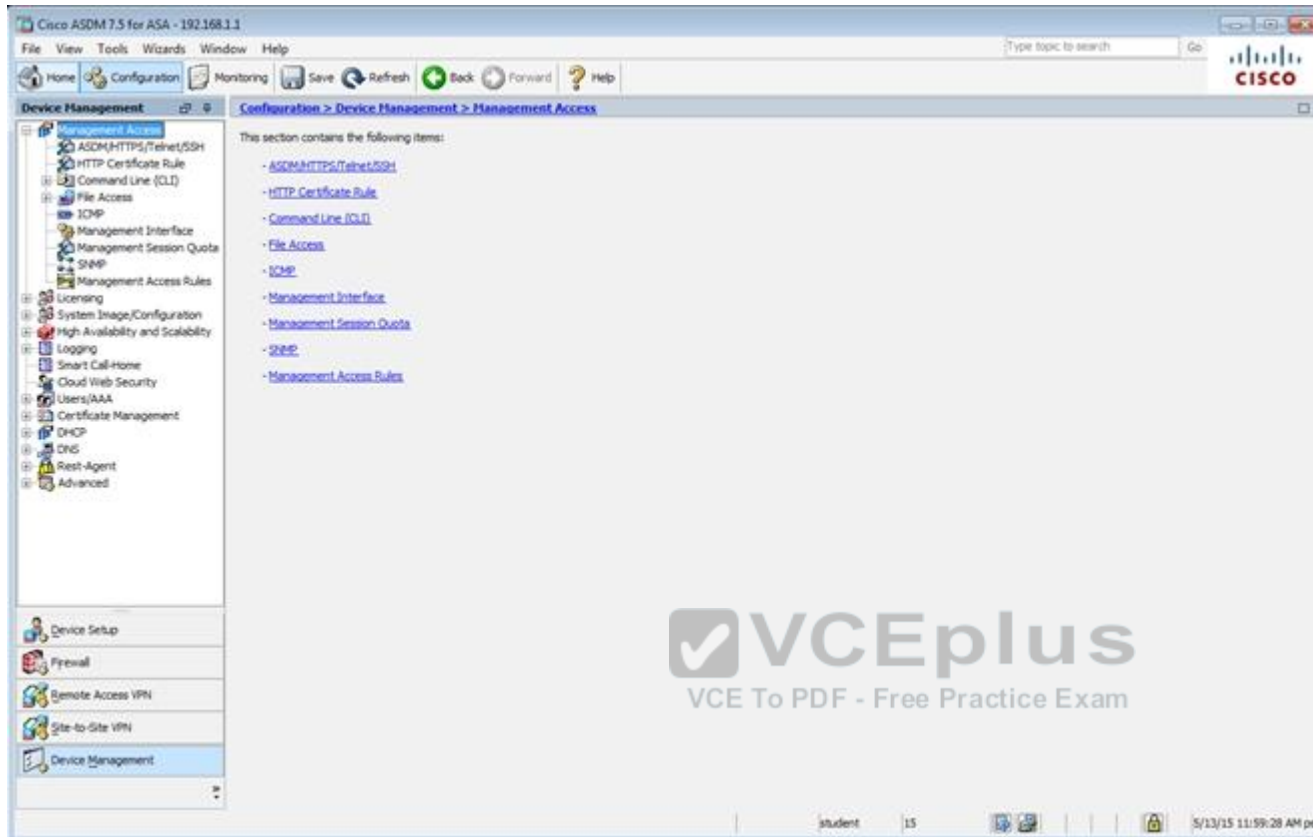
Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interface Settings > Interfaces

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

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

student 15 5/13/15 12:42:48 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

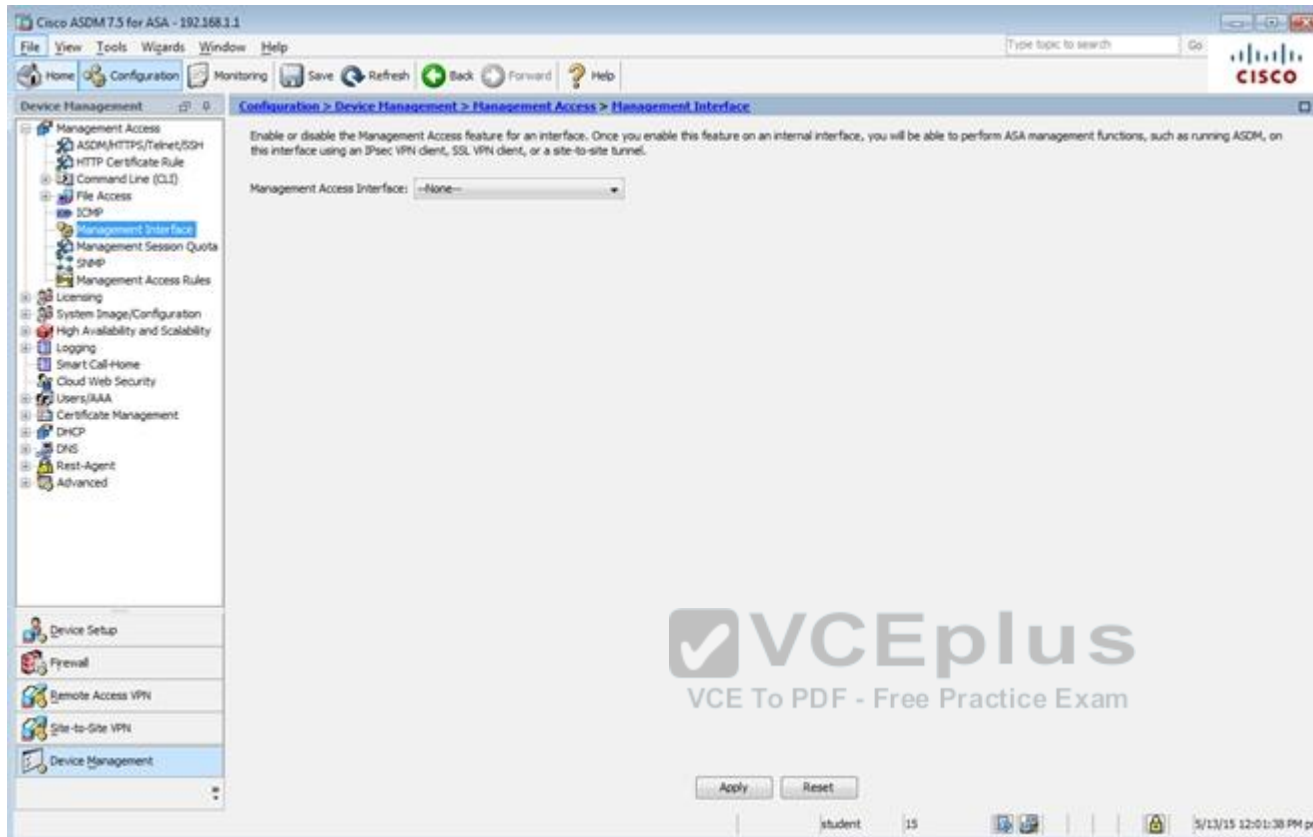
Allowed SSH Version(s): 1 & 2

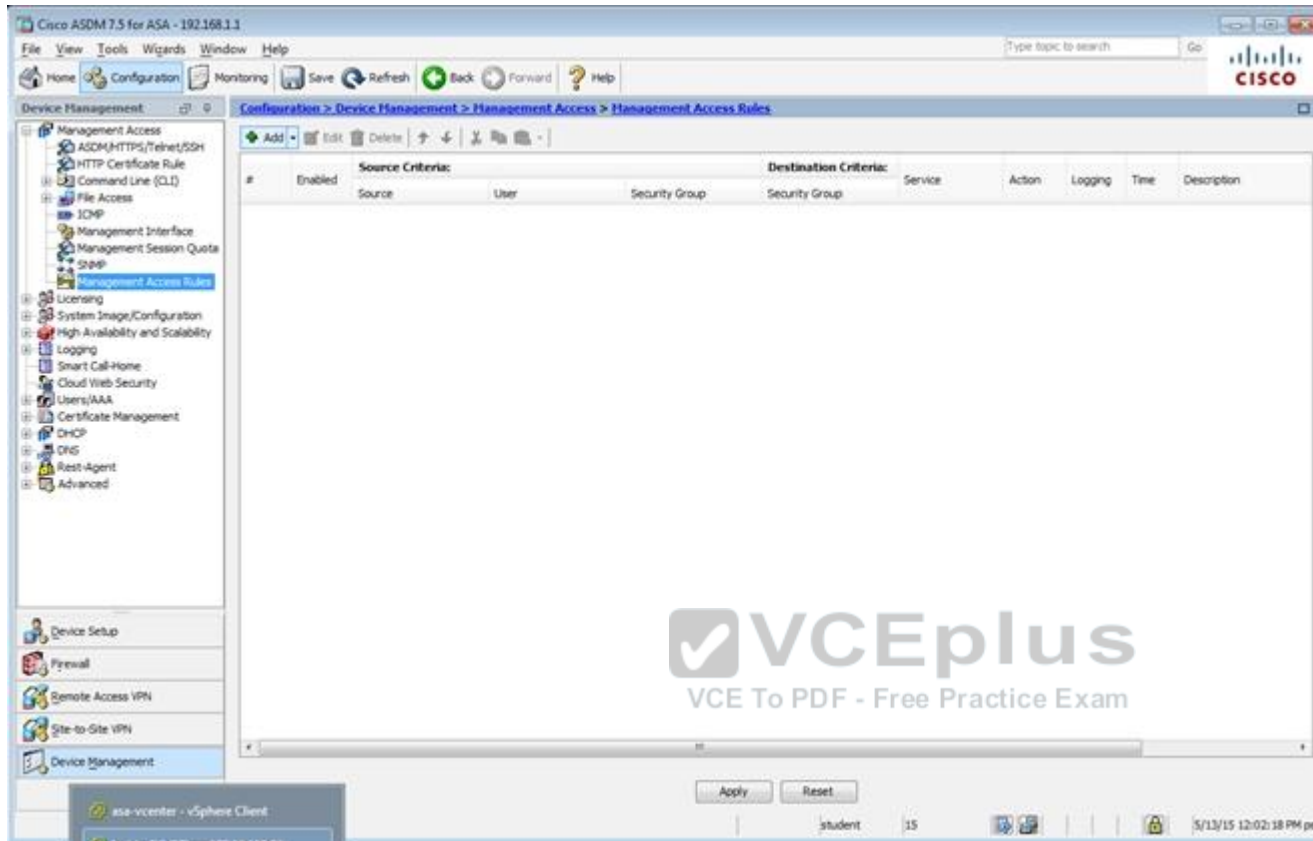
SSH Timeout: 5 minutes

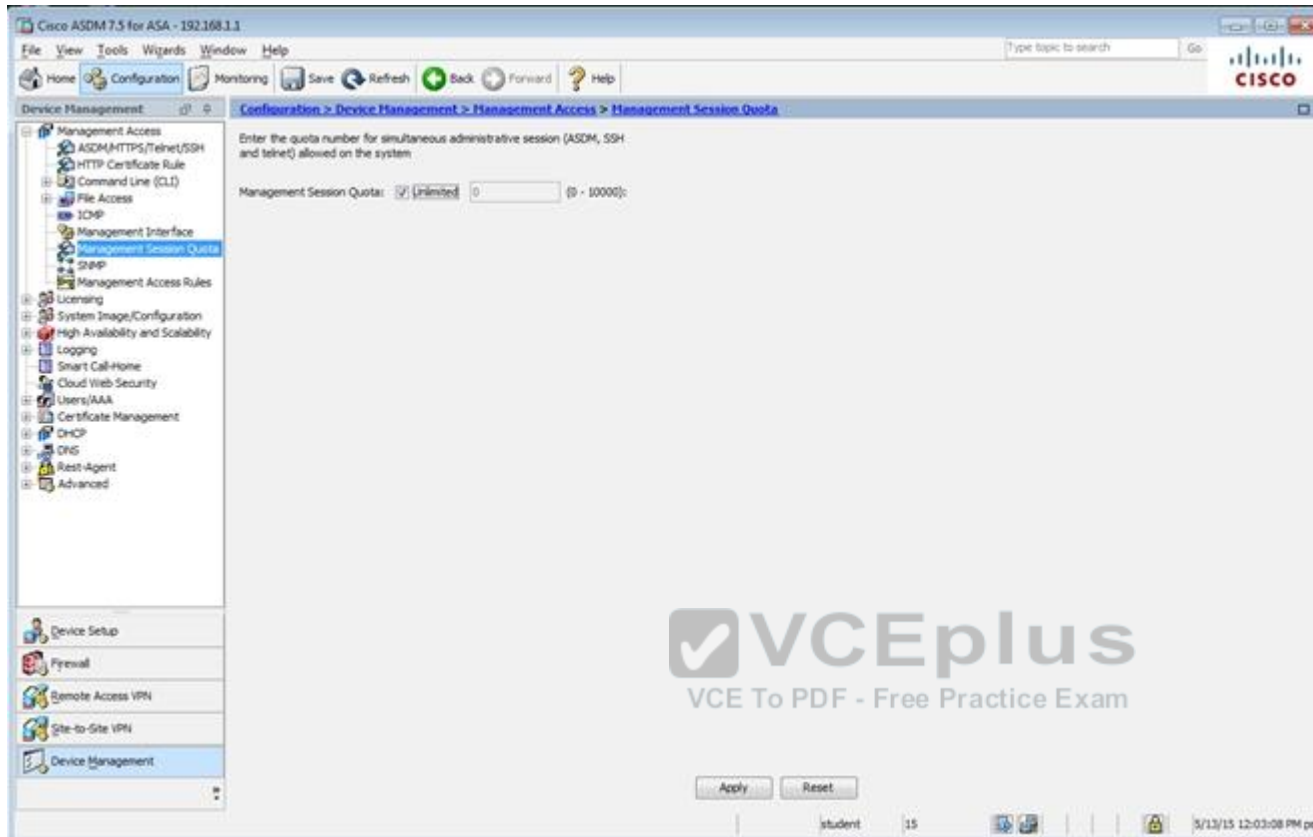
DH Key Exchange: ☒ Group 1 ☐ Group 14

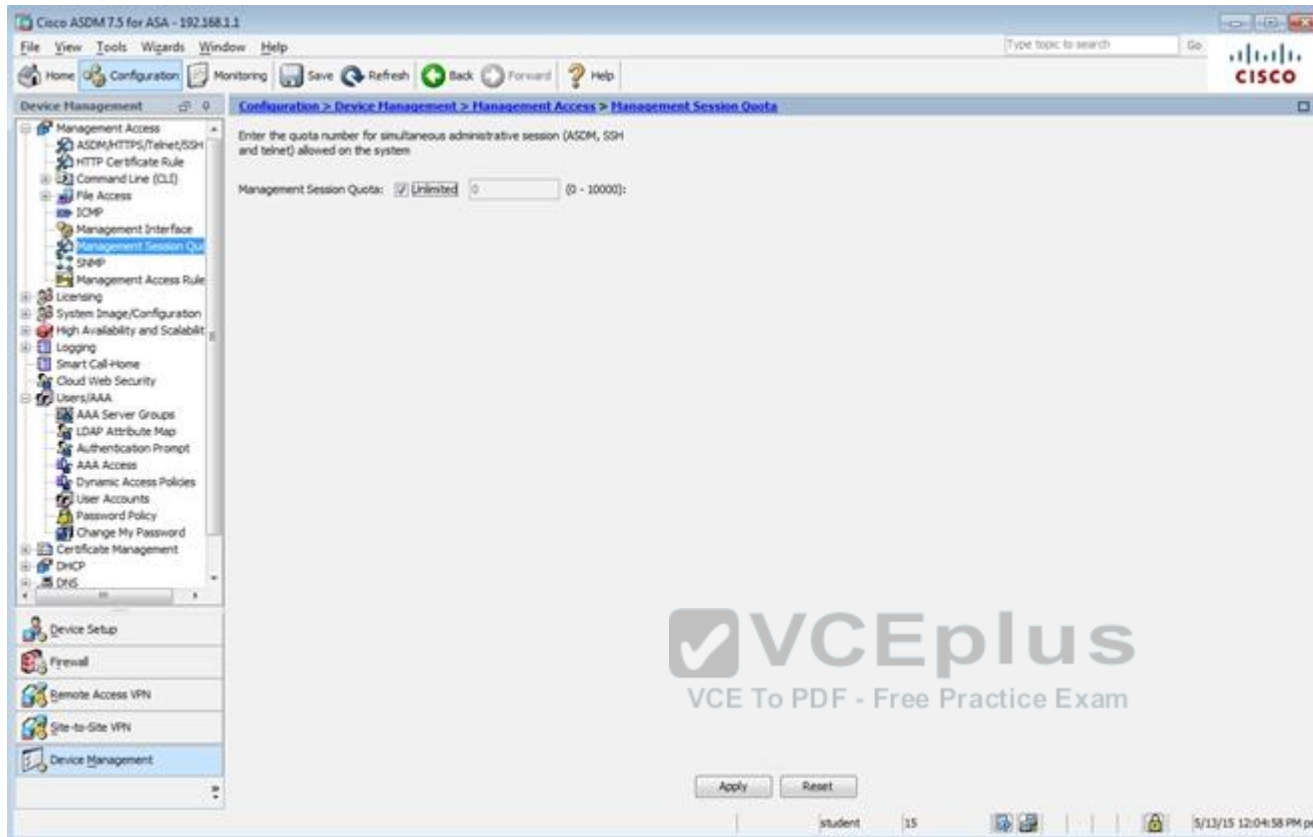
Apply Reset

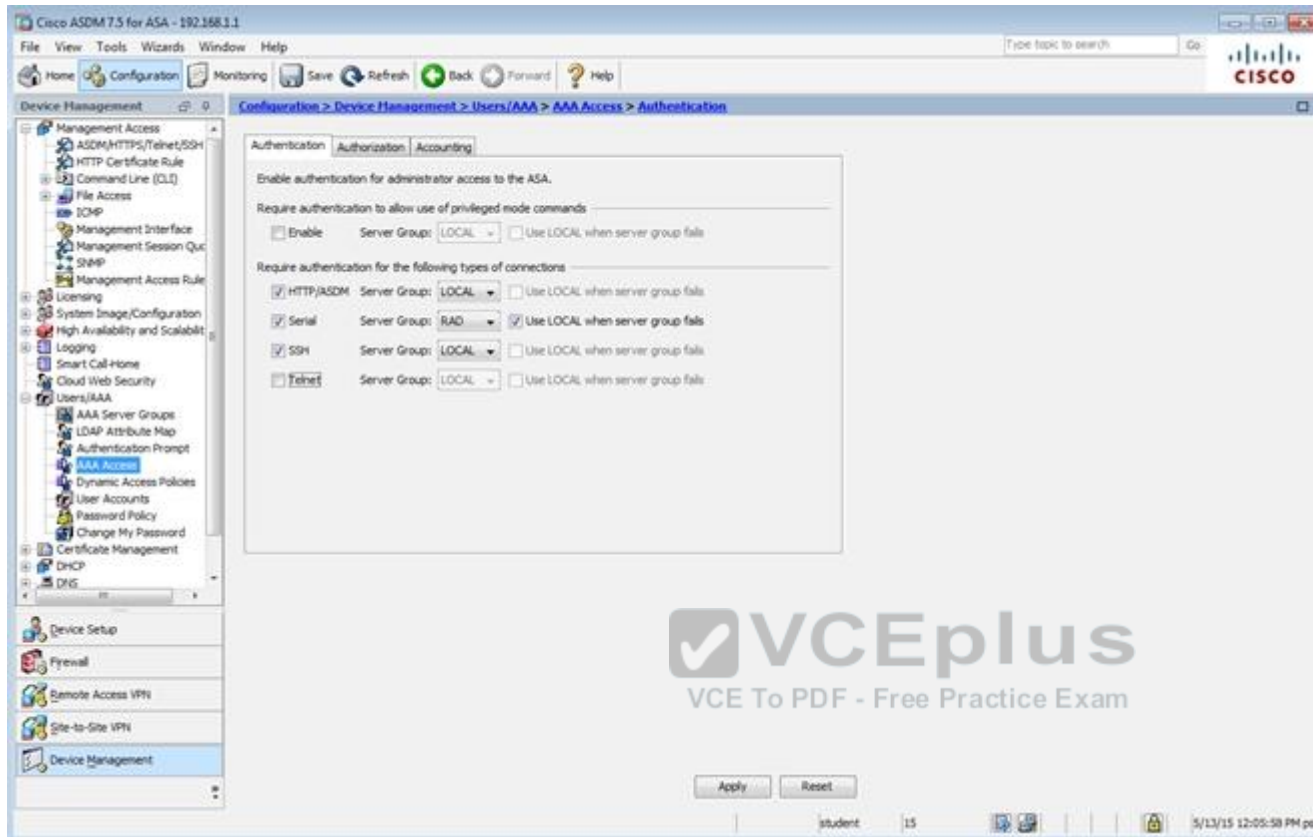
student 15 5/13/15 12:00:38 PM pst

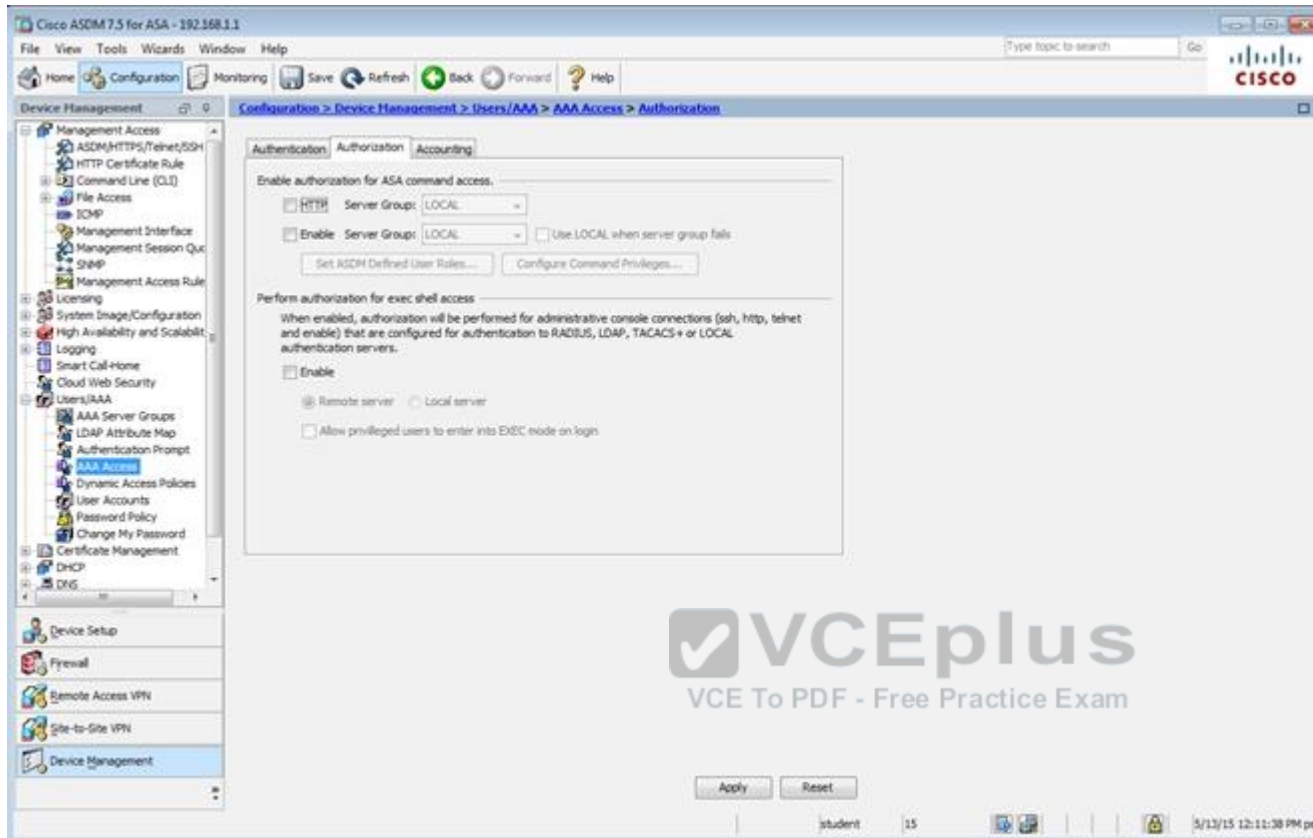


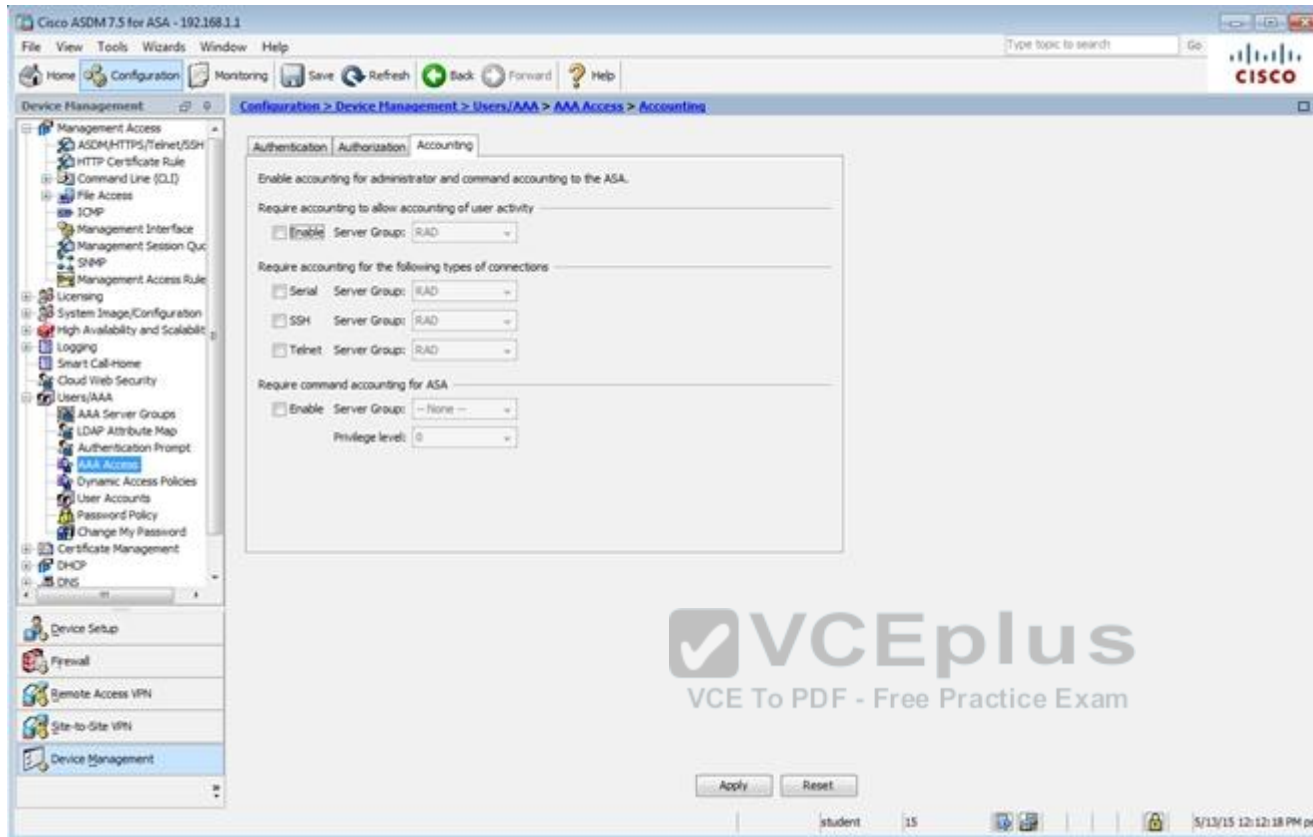












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

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

Find: Match Case

Servers in the Selected Group

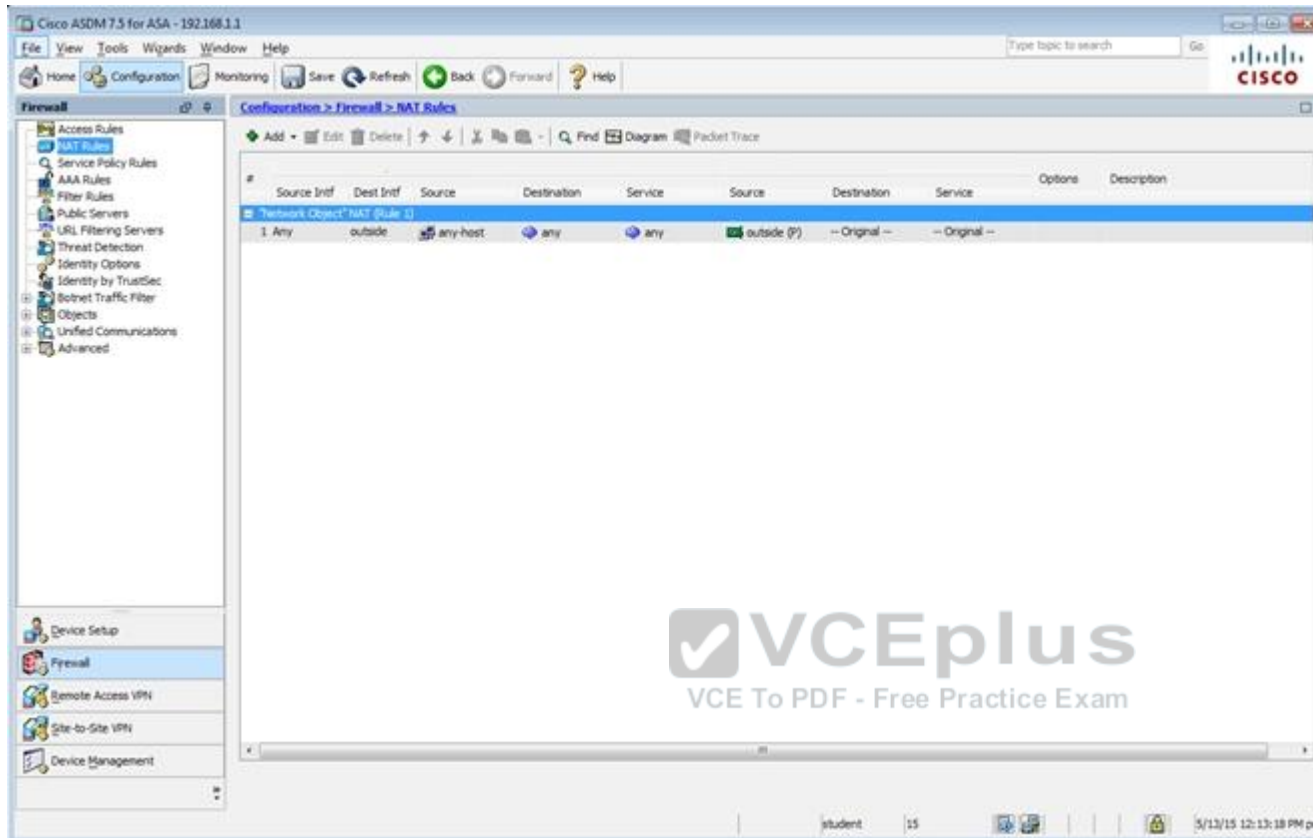
| Server Name or IP Address | Interface | Timeout |
|---------------------------|-----------|---------|
| 192.168.1.100             | inside    | 10      |

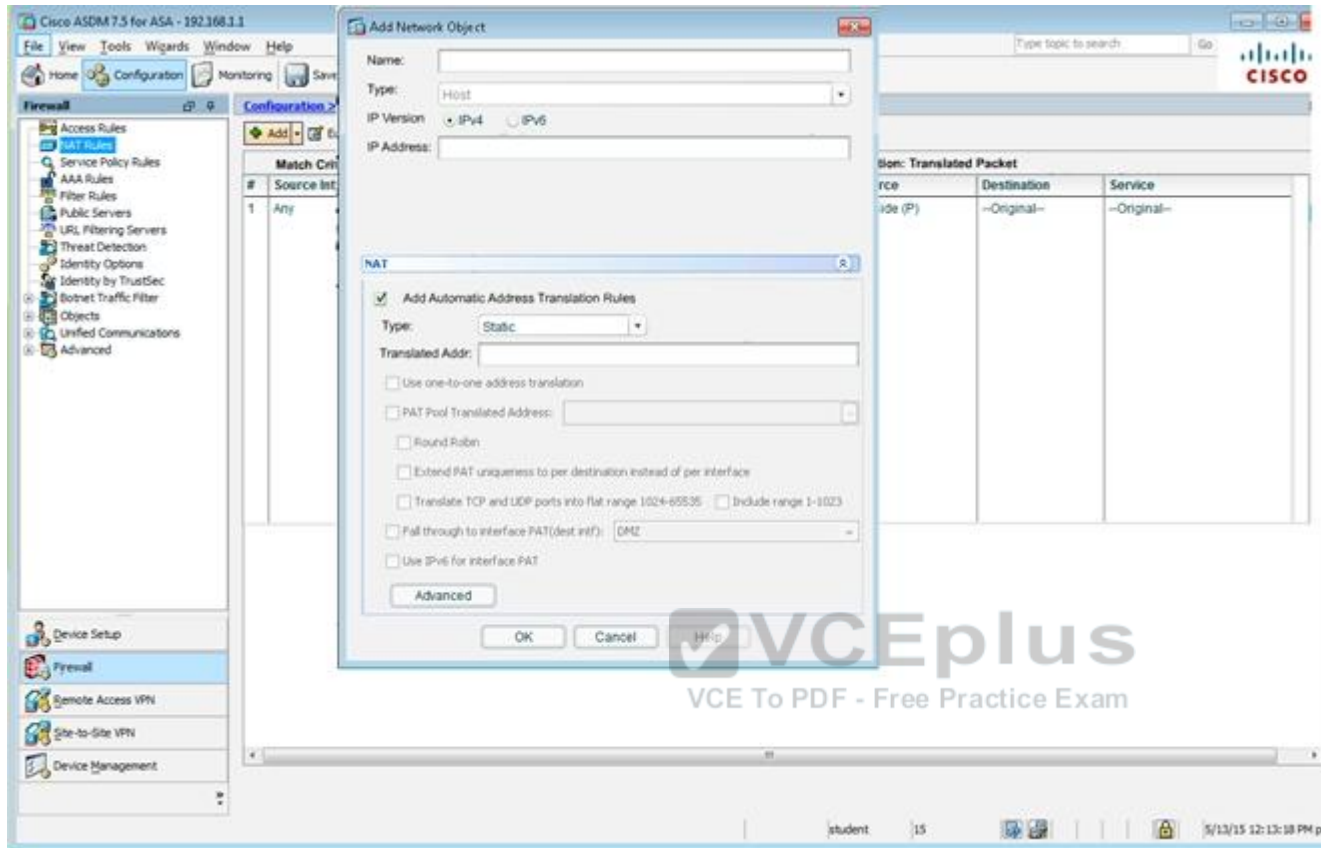
Find: Match Case

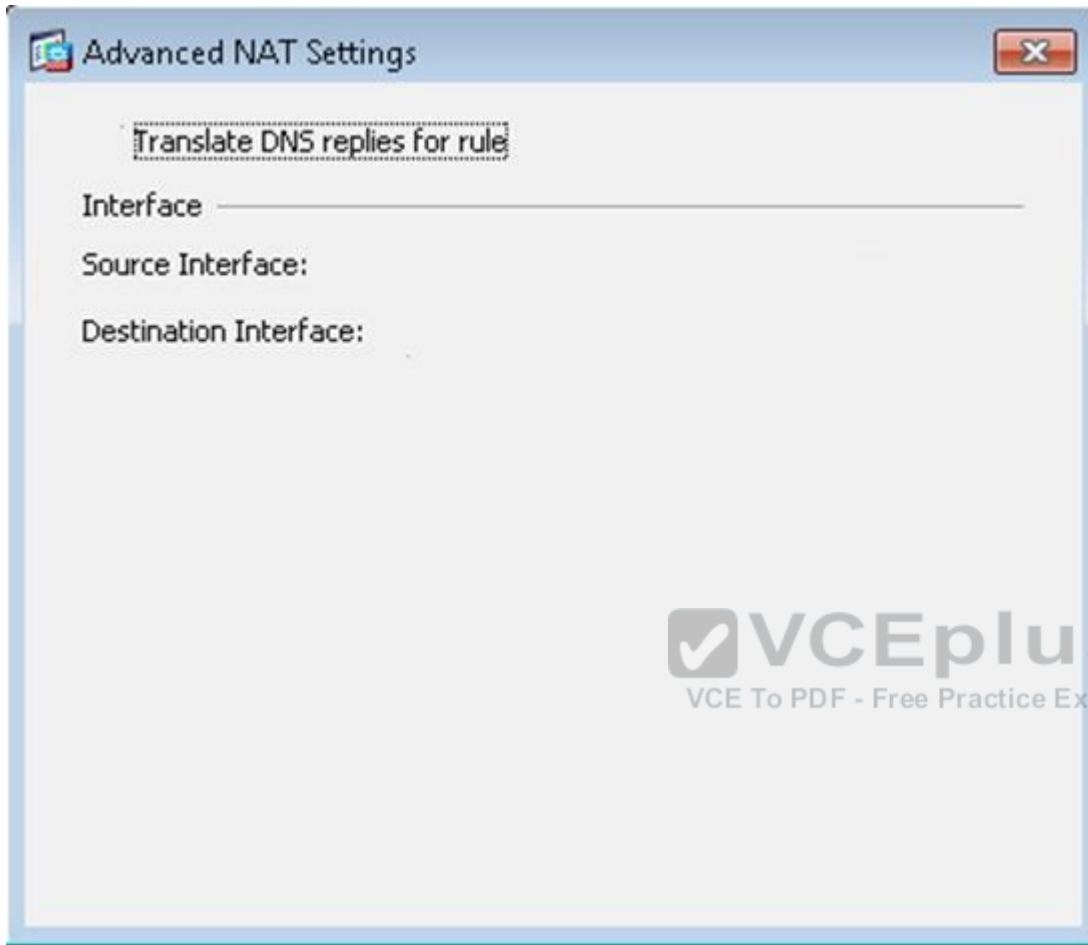
LDAP Attribute Map

Apply Reset

student 15 3/13/15 12:16:58 PM pst







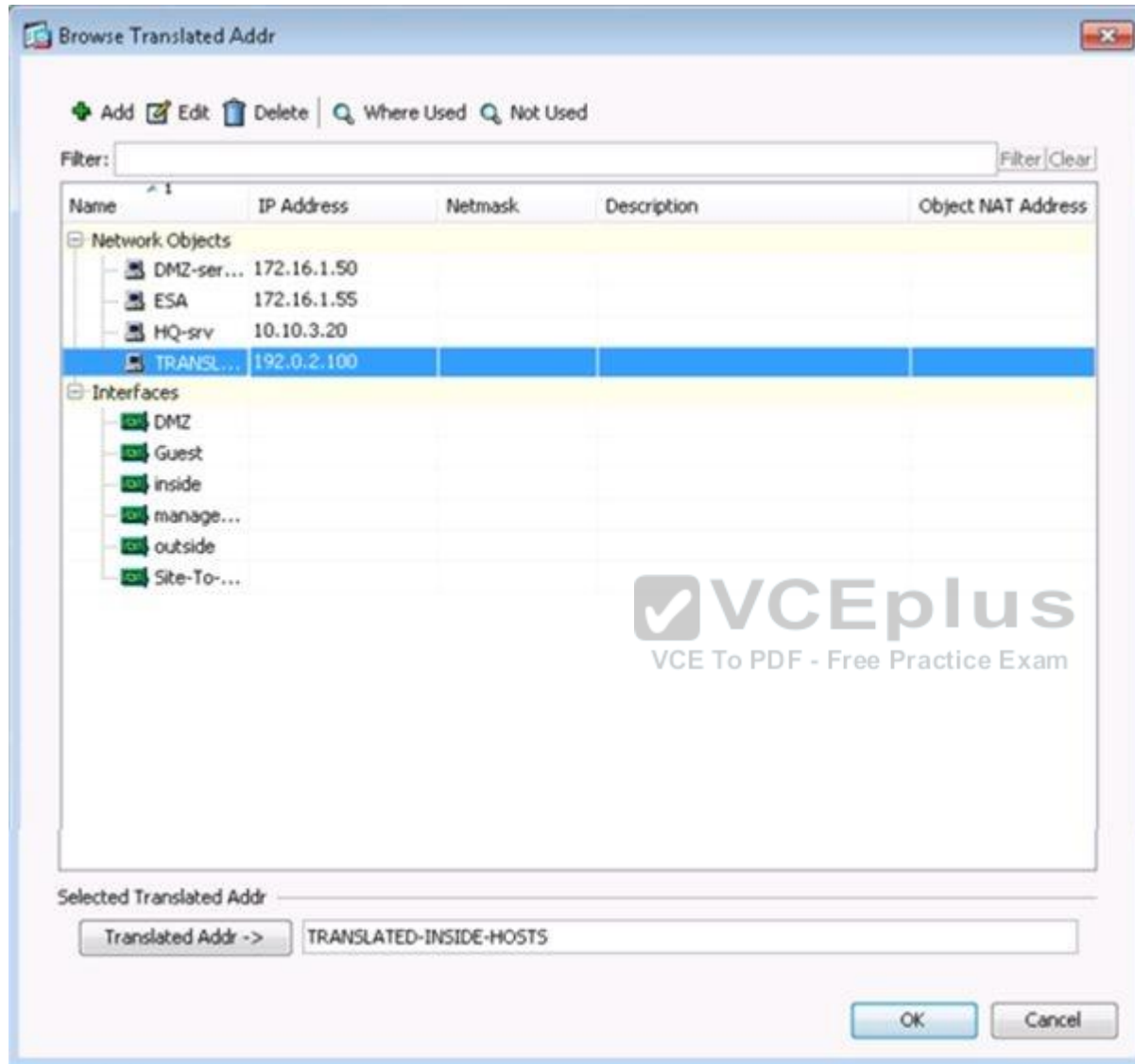
Advanced NAT Settings

☒ Translate DNS replies for rule

Interface \_\_\_\_\_

Source Interface:

Destination Interface:



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

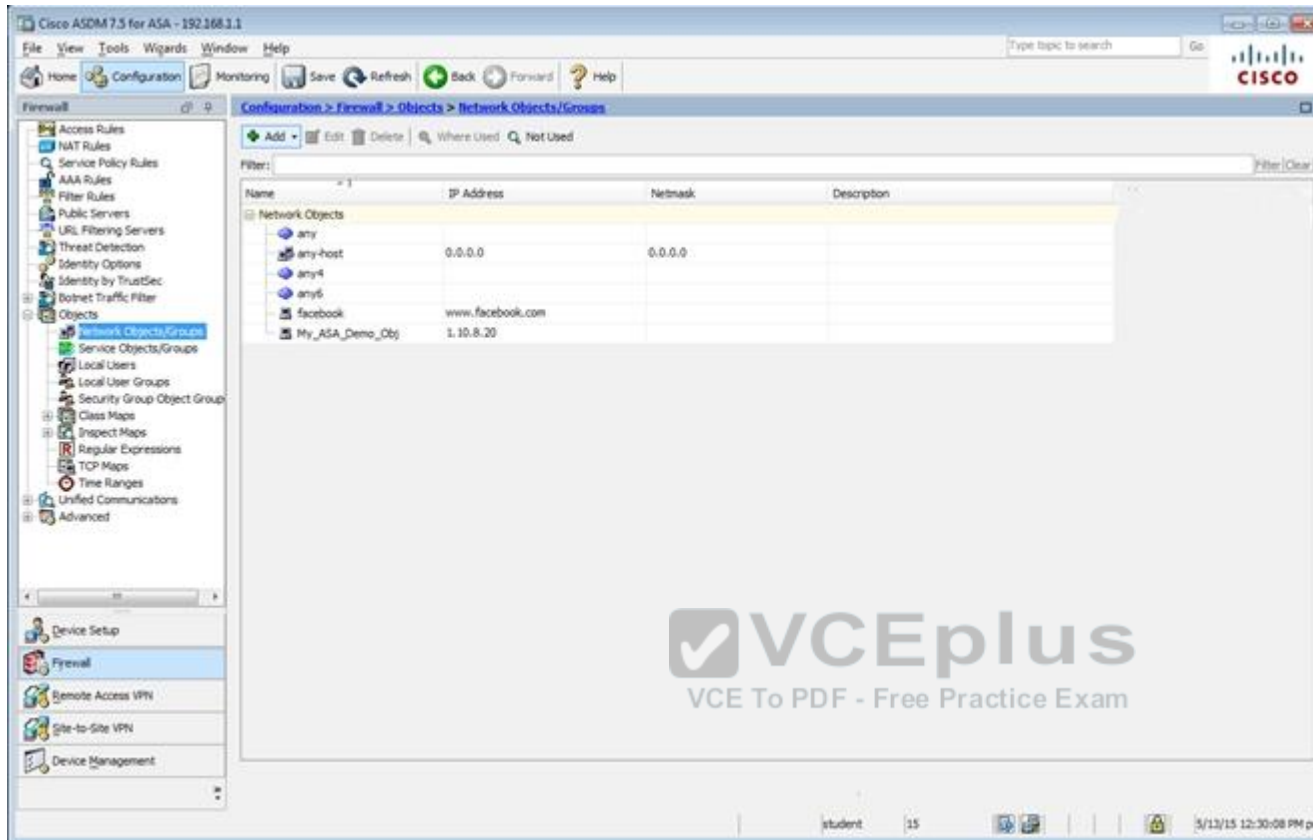
| Username  | Privilege Level (Role) | Access Restrictions | VPN Group Policy           | VPN Group Lock             |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student   | 15                     | Full                | --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

Add Edit Delete

End: [ ] [ ] [ ] Match Case

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Service Policy Rules

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

Configuration

Firewall > Service Policy Rules

Add Edit Delete Find Diagram Packet Trace

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

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

student 15 5/13/15 12:15:48 PM pet

**Edit Service Policy Rule**


Traffic Classification    Default Inspections    Rule Actions

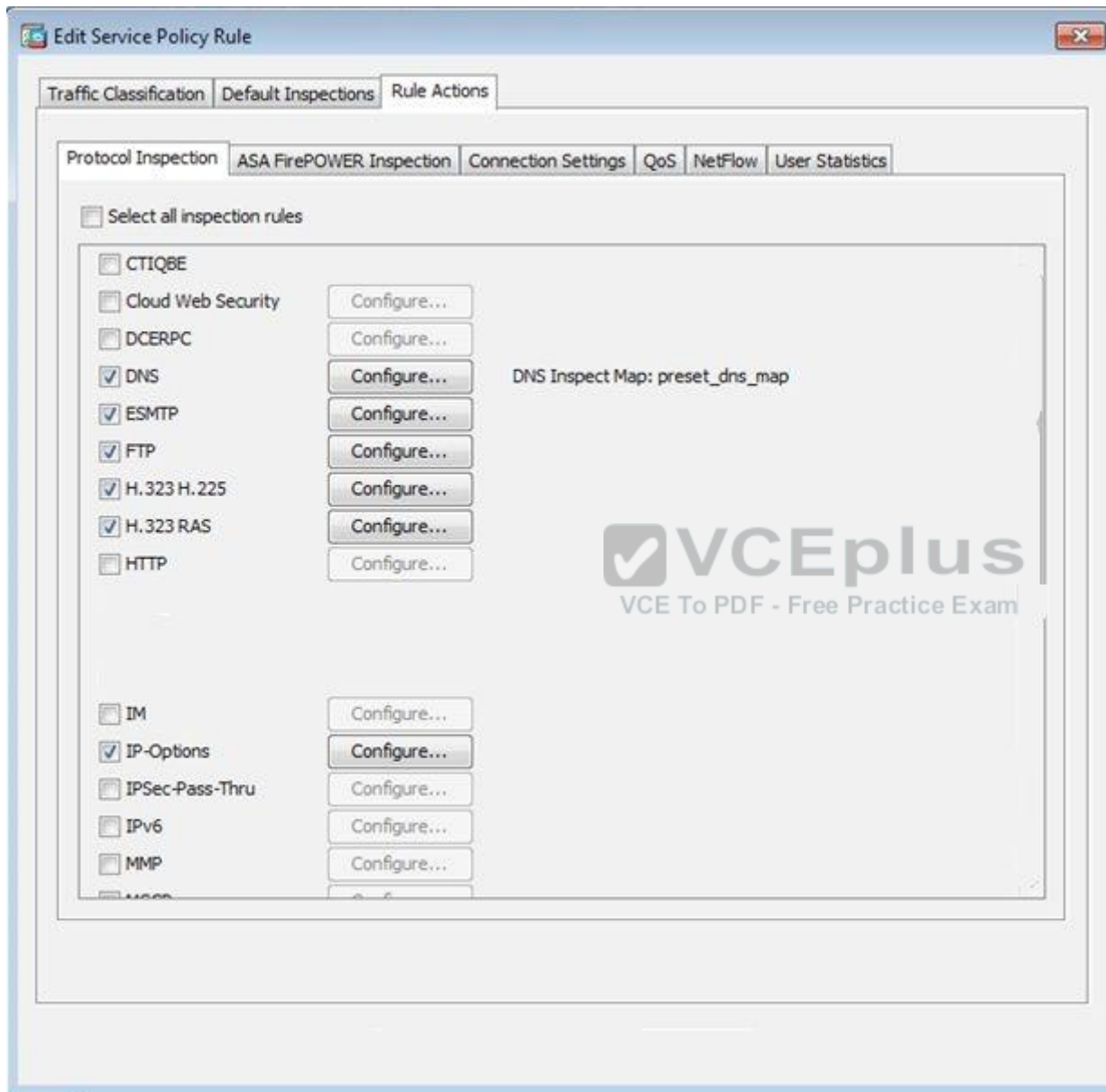
Name: inspection\_default

Description (optional):

Traffic Match Criteria

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Access Rules

Access Rules

- 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

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN



Device Management

Configuration > Firewall > Access Rules

Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace

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


student 15 5/13/15 12:28:58 PM pst


 **Add Access Rule** 


Interface:

Action:

Source Criteria

Source:  

User:  

Security Group:  

Destination Criteria


Destination:


Security Group:

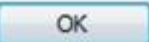
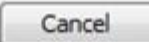
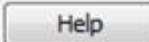
Service:

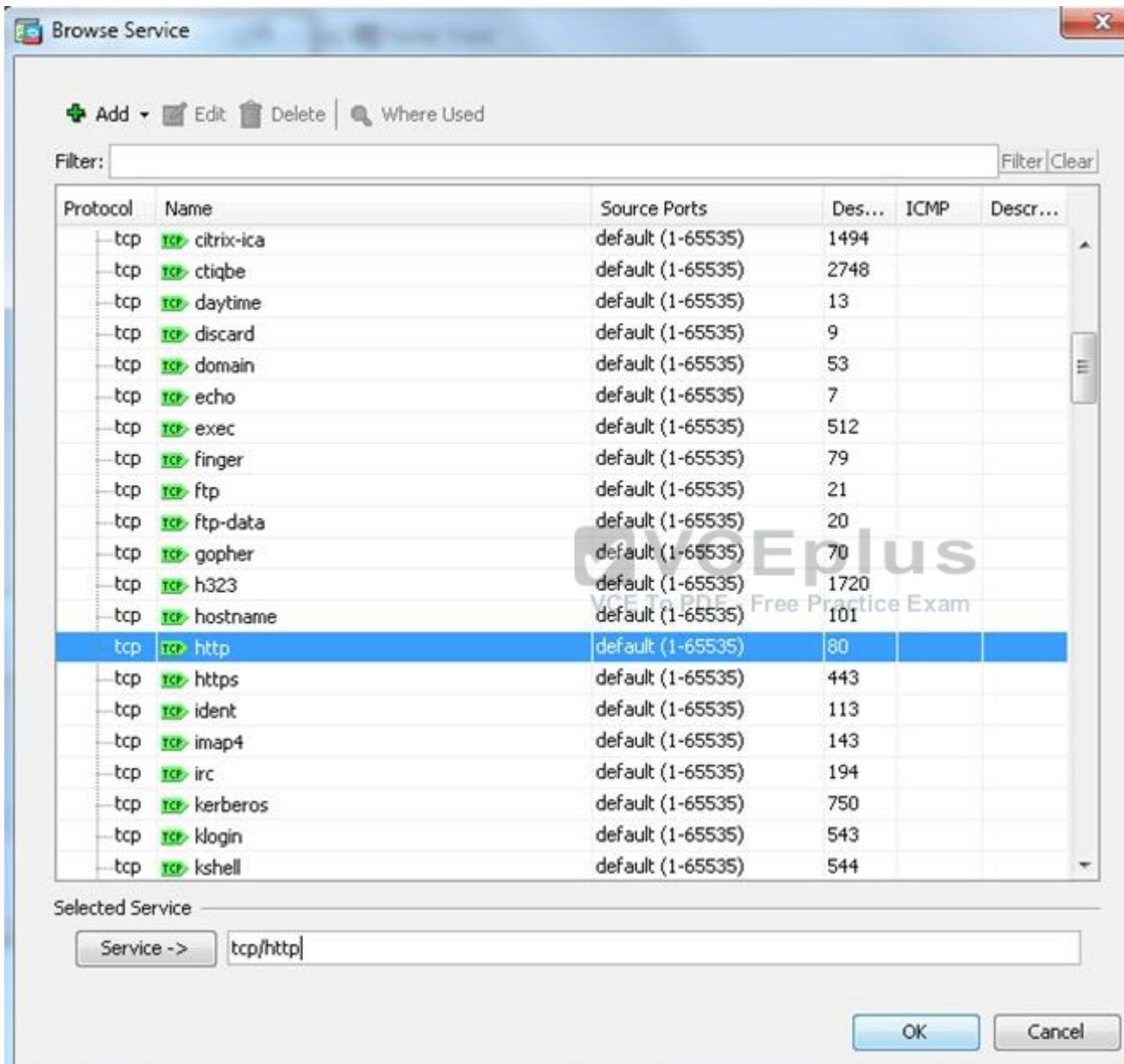
Description:

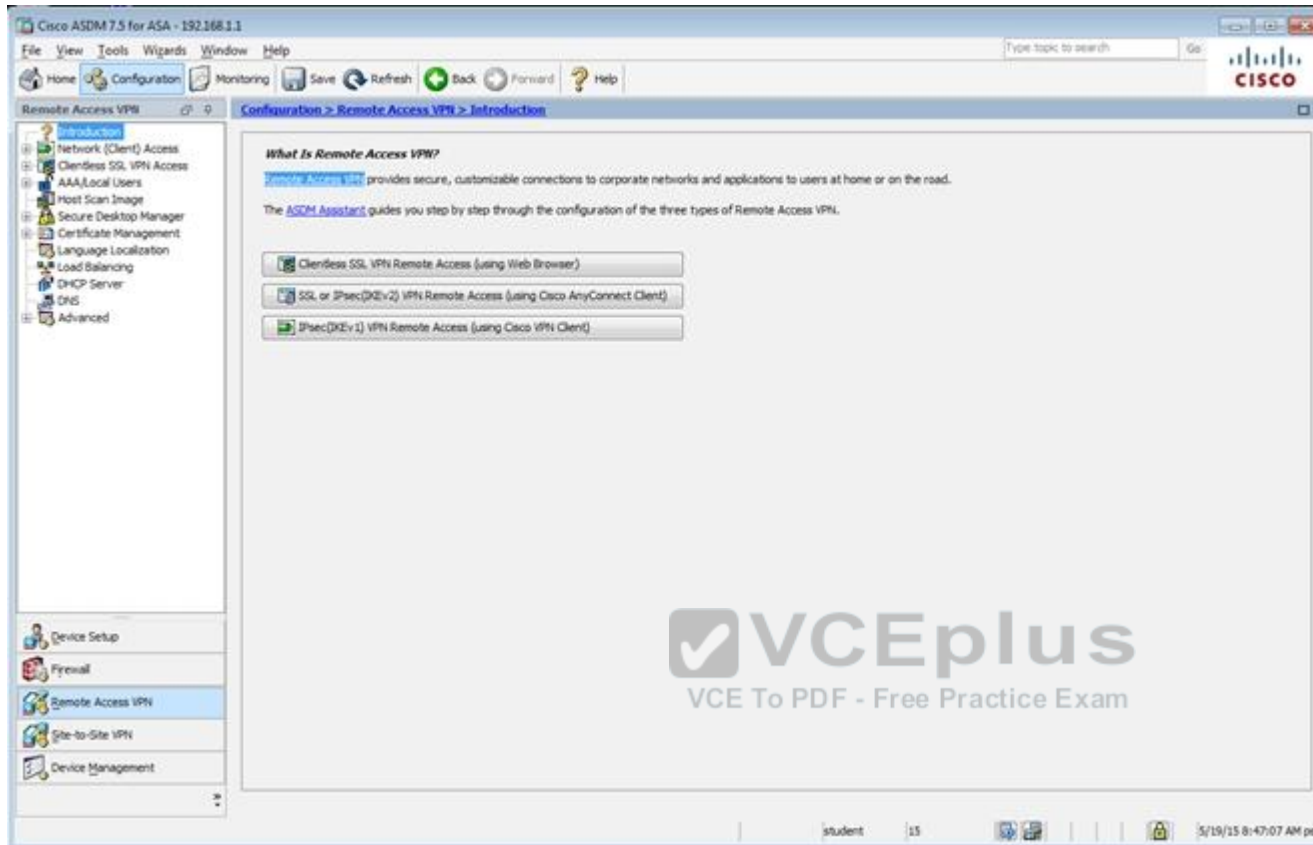
☒ Enable Logging

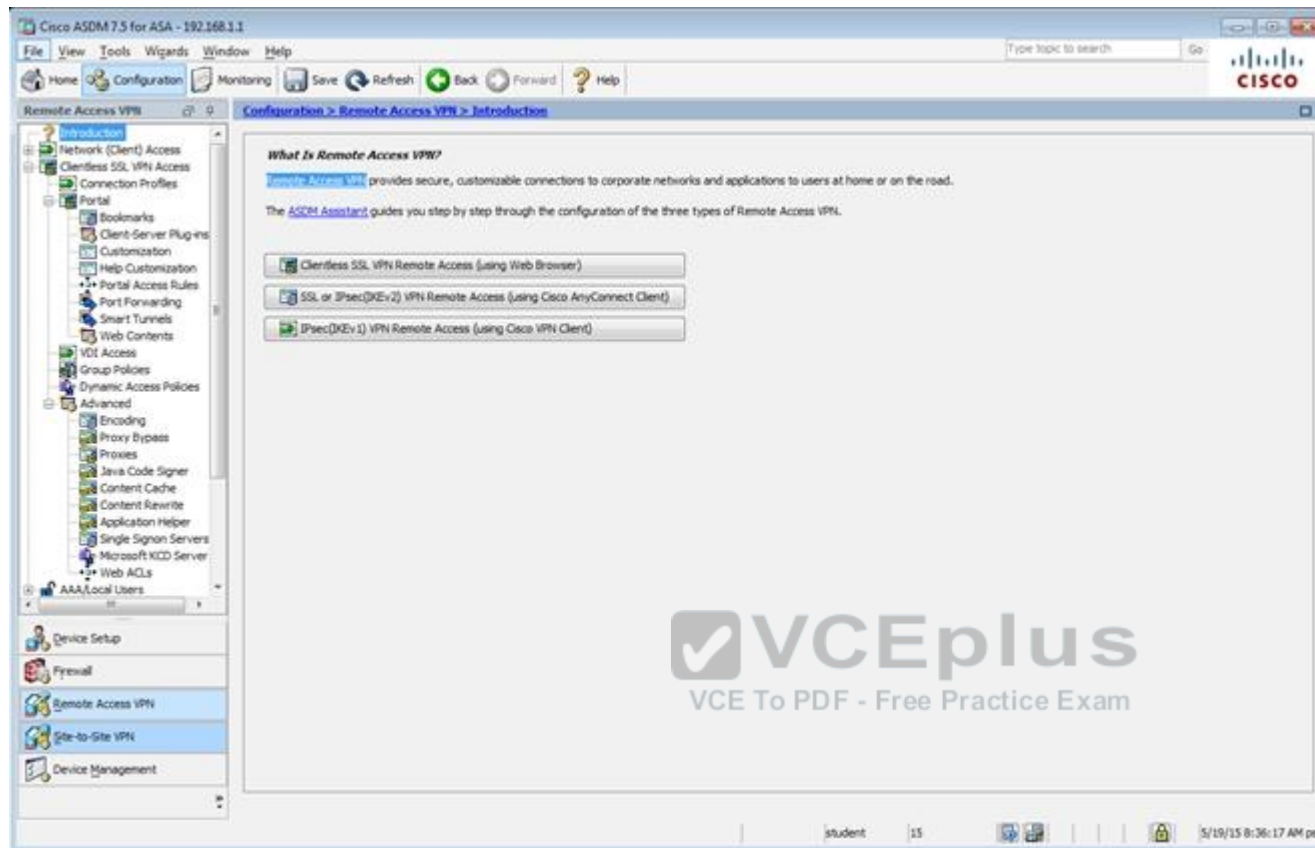
Logging Level:  

**More Options** 







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...  
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions  
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

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

Connection Profiles

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

Add Edit Delete Find: Match Case

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

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced

Name: clientless  
Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Login and Logout Page Customization: DfltCustomization Manage...

☐ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add - Delete (The table is in-line editable.)

| Alias | Enabled                             |
|-------|-------------------------------------|
| test  | <input checked="" type="checkbox"/> |

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add - Delete (The table is in-line editable.)

| URL                        | Enabled                             |
|----------------------------|-------------------------------------|
| https://209.165.201.2/test | <input checked="" type="checkbox"/> |

You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find:  ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
General  
Authentication  
Secondary Authentication  
Authorization  
Accounting  
NetBIOS Servers  
Clientless SSL VPN

Interface-Specific Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL |
|-----------|--------------|-------------------|
|-----------|--------------|-------------------|

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
Advanced  
  General  
  Authentication  
  Secondary Authentication  
  Authorization  
  Accounting  
  NetBIOS Servers  
  Clientless SSL VPN

Secondary Authentication Server Group

Server Group: -- None -- Manage...

☐ Use LOCAL if Server Group fails

☐ Use primary username (Hide secondary username on login page)

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add E Edit D Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

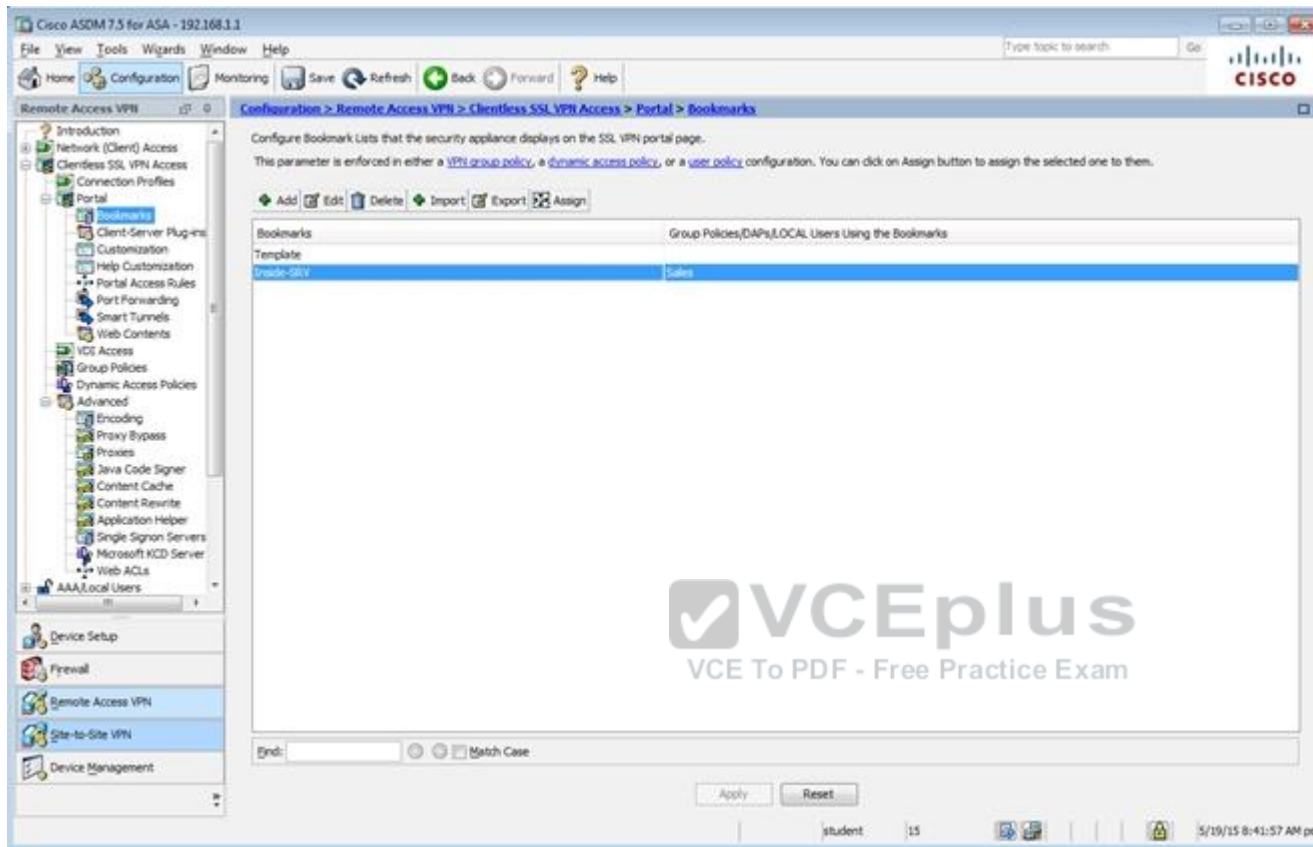
☐ Use the entire DN as the username

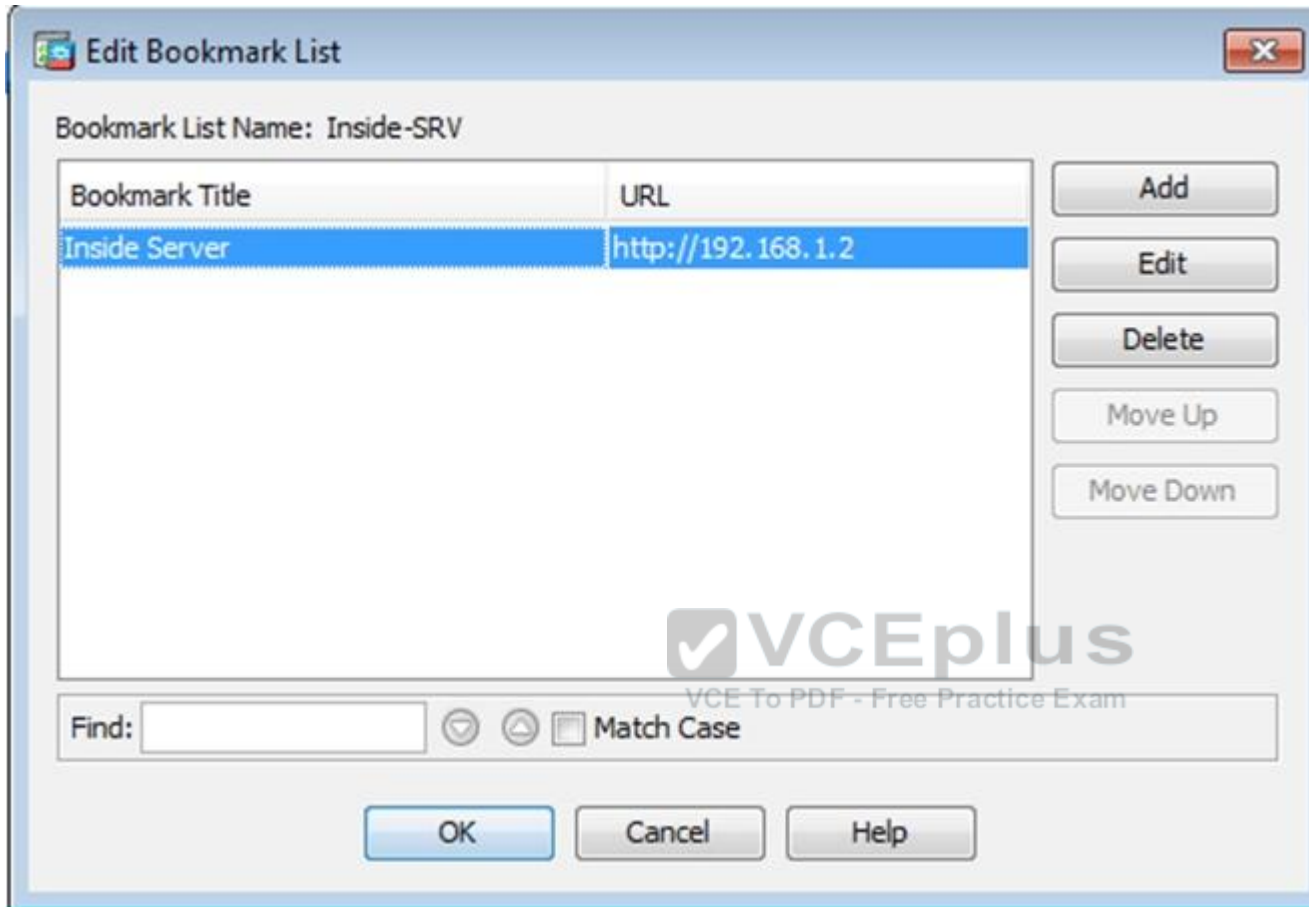
☐ Use script to select username

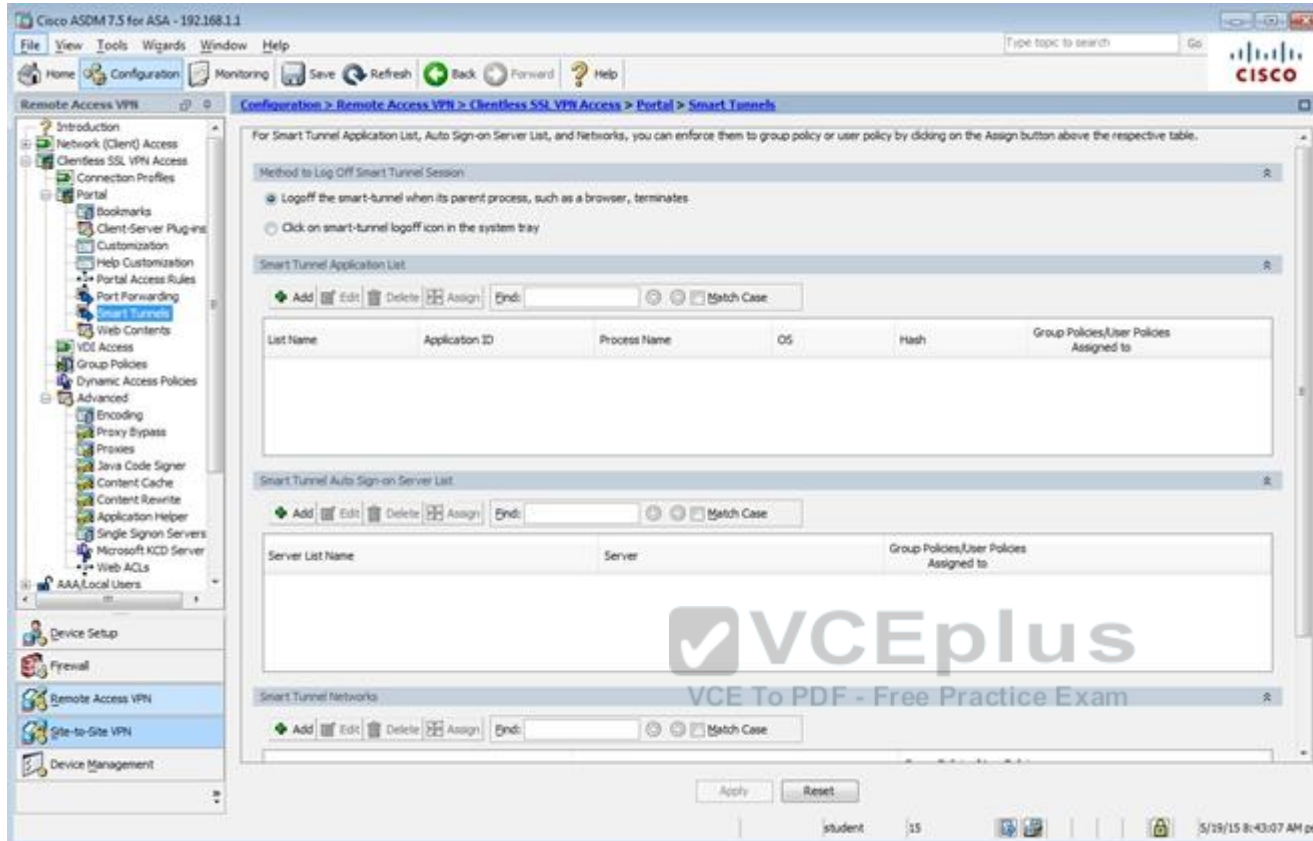
-- None -- + Add E Edit D Delete

Find:  Next Previous

OK Cancel Help







The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with the following items: Introduction, Network (Client) Access, Clientless SSL VPN Access, Connection Profiles, Portal, Bookmarks, Client-Server Plugins, Customization, Help Customization, Portal Access Rules, Smart Tunnels, Web Contents, VDI Access, Group Policies, Dynamic Access Policies, Advanced, Encoding, Proxy Bypass, Proxies, Java Code Signer, Content Cache, Content Rewrite, Application Helper, Single Signon Servers, Microsoft KCD Server, Web ACLs, AAA Local Users, Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management. The main pane displays the configuration page for Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding. The page title is "Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection." Below the title, there is a text block stating: "This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user policy](#) configuration. You can click on Assign button to assign the selected one to them." Below this text, there are buttons for Add, Edit, Delete, and Assign. A table with the following columns is displayed: List Name, Local TCP Port, Remote Server, Remote TCP Port, Description, and Group Policies/User Policies Assigned to. The table is currently empty. At the bottom of the main pane, there is a search bar with the text "Find:" and a "Match Case" checkbox. The bottom status bar shows the user "student", the page number "15", and the date and time "5/19/15 8:43:47 AM pst".

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies' page. The page includes a description of VPN group policies and a table of existing policies.

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

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

Buttons: Add, Edit, Delete, Assign

| Name                                | Type     | Tunneling Protocol                  | Connection Profiles/Users Assigned To                 |
|-------------------------------------|----------|-------------------------------------|---|
| celnet                              | Internal | ssl-clientless                      | clientless  |
| DefaultGroupPolicy (System Default) | Internal | kev1:kev2:ssl-clientless/2to-espsec | DefaultRAGroup/DefaultL2Group/DefaultADMPGroup/Def... |

Search bar: Find: [ ] Match Case

Buttons: Apply, Reset

Status bar: student 15 5/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

Tunneling Protocols: ☐ Inherit ☒ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 ☐ IPsec IKEv2 ☐ L2TP/IPsec

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

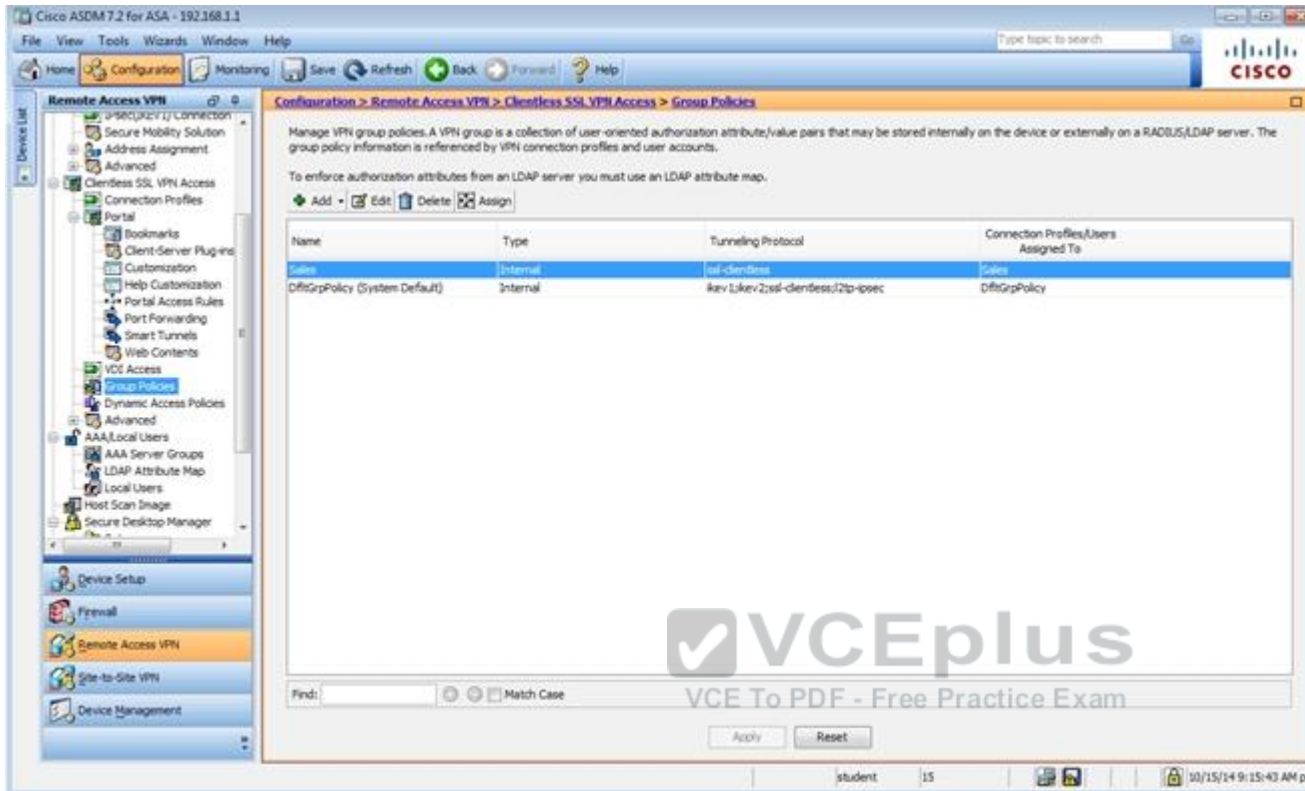
Session Alert Interval: ☒ Inherit ☐ Default:  minutes

Idle Alert Interval: ☒ Inherit ☐ Default:  minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

Find:  ☐ Next ☐ Previous

OK Cancel Help



Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

| Name                           | Type     | Tunneling Protocol                 | Connection Profiles/Users Assigned To |
|--------------------------------|----------|------------------------------------|---------------------------------------|
| Sales                          | Internal | l2l-clientless                     | Sales                                 |
| DiffGrpPolicy (System Default) | Internal | ikev1ikev2ssl-clientless/l2l-ipsec | DiffGrpPolicy                         |

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

General  
More Options  
Customization  
Login Setting  
Single Signon  
VDI Access  
Session Settings

Bookmark List: ☐ Inherit  Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit  Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit   Manage...

Smart Tunnel Application: ☒ Inherit  Manage...

☐ Smart Tunnel all Applications (This feature only works with Windows platforms)

☐ Auto Start

Auto Sign-on Server: ☒ Inherit  Manage...

Windows Domain Name (optional):

Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find:  ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

**General**  
Servers  
Advanced

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None--

Access Hours: --Unrestricted--

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

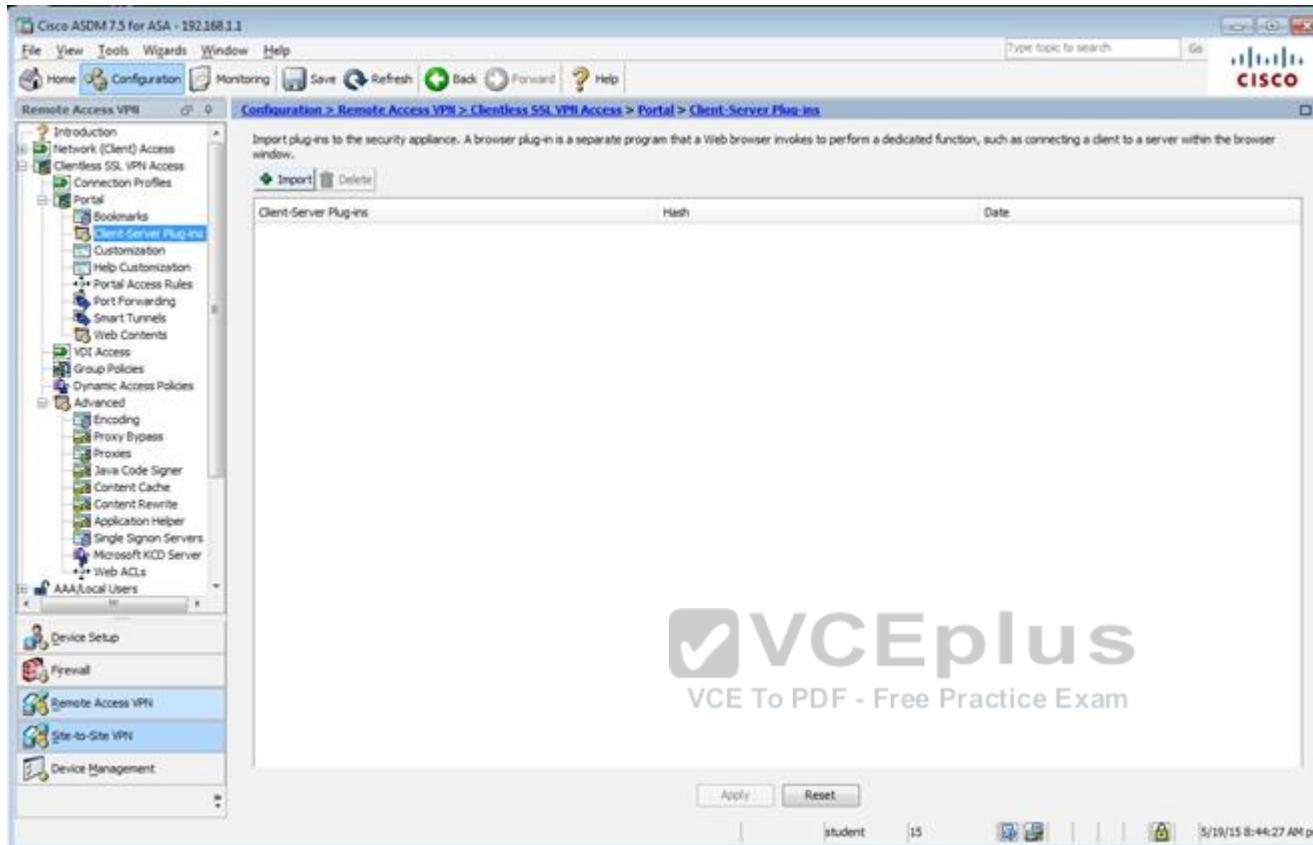
Maximum Connect Time: ☒ Unlimited  minutes

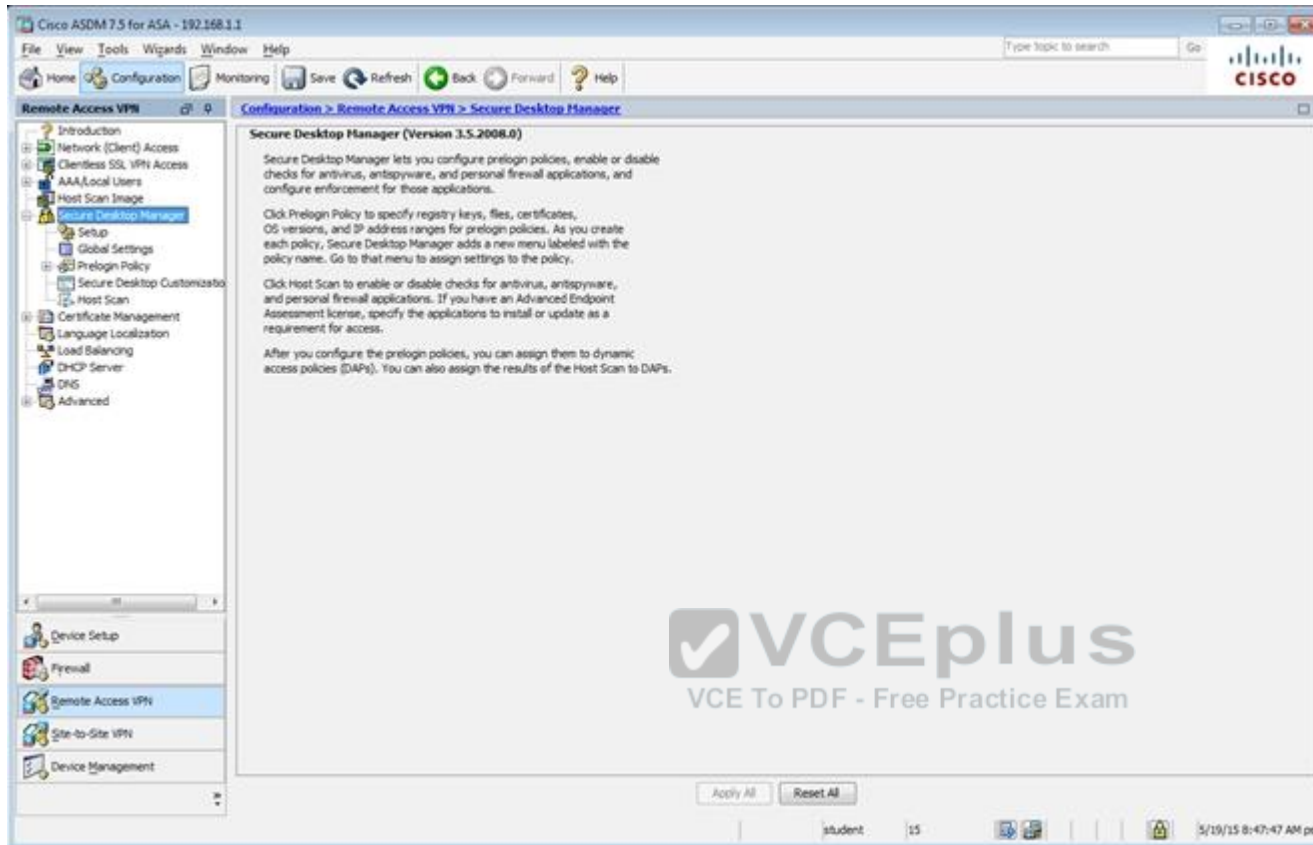
Idle Timeout: ☐ None  30 minutes

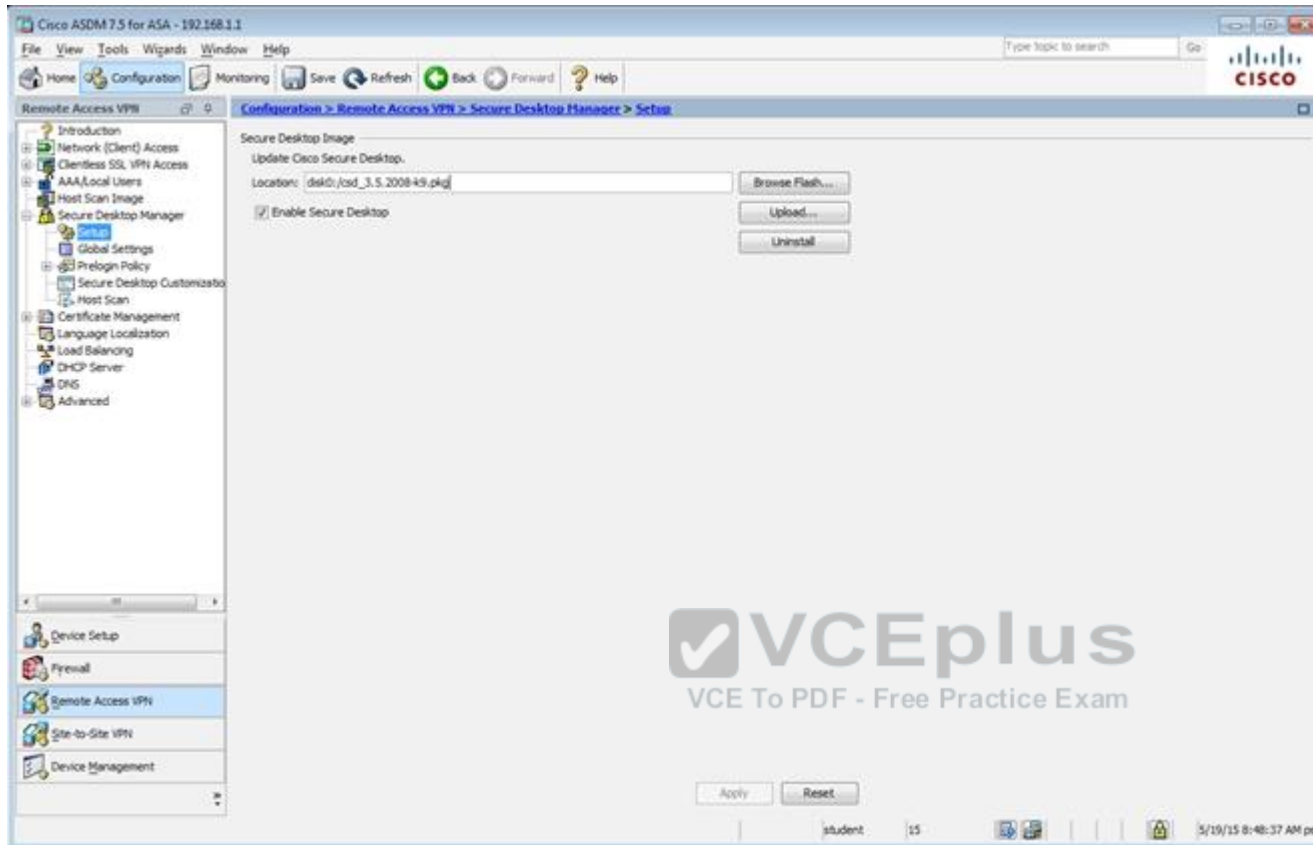
On smart card removal: ☒ Disconnect ☐ Keep the connection

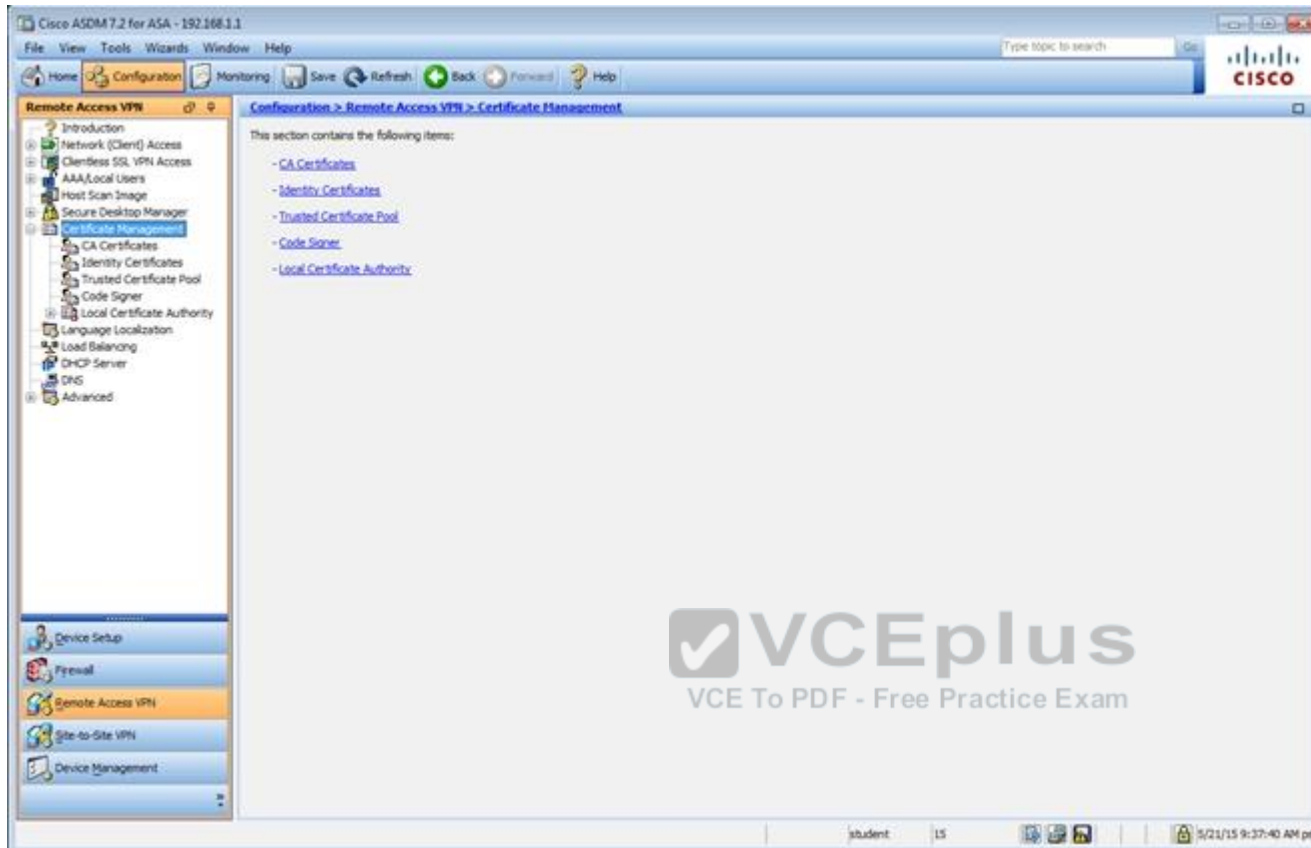
**VCEplus**  
VCE To PDF - Free Practice Exam

Find:





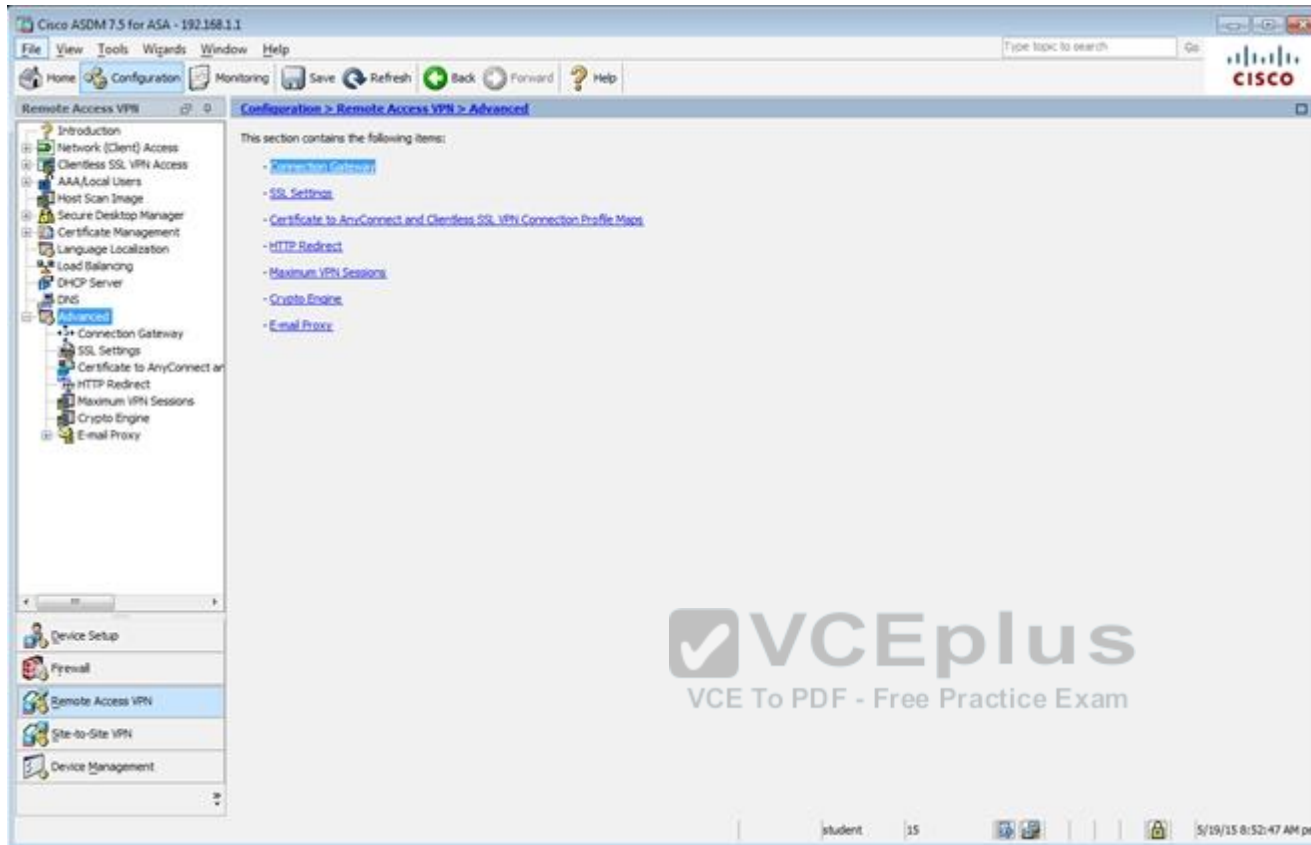




The screenshot displays the Cisco ASDM 7.5 for ASA - 392.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with the following data:

| Issued To                 | Issued By                 | Expiry Date              | Associated Trustpoints | Usage           | Public Key Type |
|---------------------------|---------------------------|--------------------------|------------------------|-----------------|-----------------|
| hostname-wf-17-ASA.sec... | hostname-wf-17-ASA.sec... | 11:10:33 pet Dec 20 2024 | ASDM_TrustPoint1       | General Purpose | RSA (2048 bits) |

Below the table, there are sections for 'Certificate Expiration Alerts' and 'Public CA Enrollment'. The 'Public CA Enrollment' section includes a link to 'Enroll ASA SSL certificate with Entrust'. At the bottom, there is a section for the 'ASDM Identity Certificate Wizard' with a 'Launch ASDM Identity Certificate Wizard...' button.



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

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

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

Encryption

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

Server Name Indication (SNI)

Domain: dmz

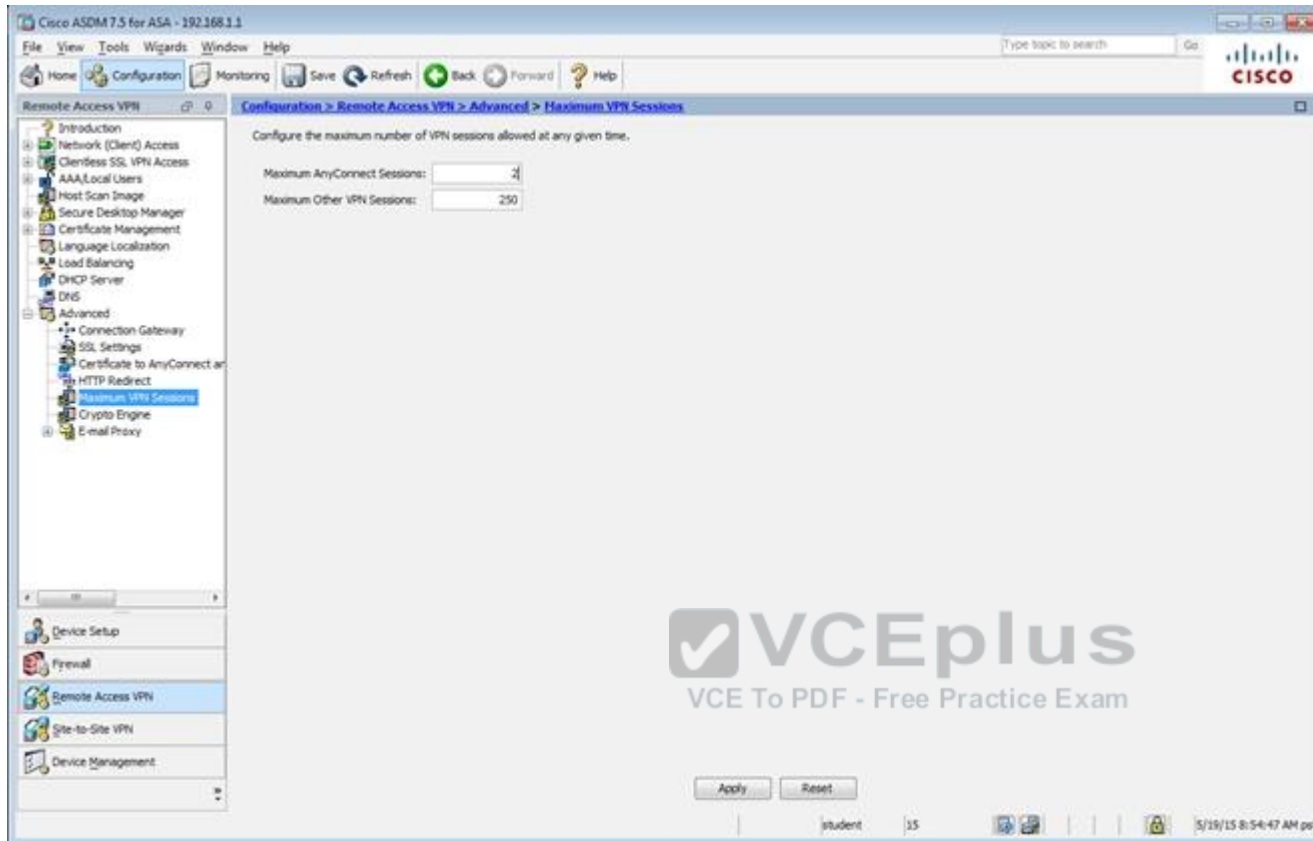
Certificate: ASDM\_TrustPoint1.h...

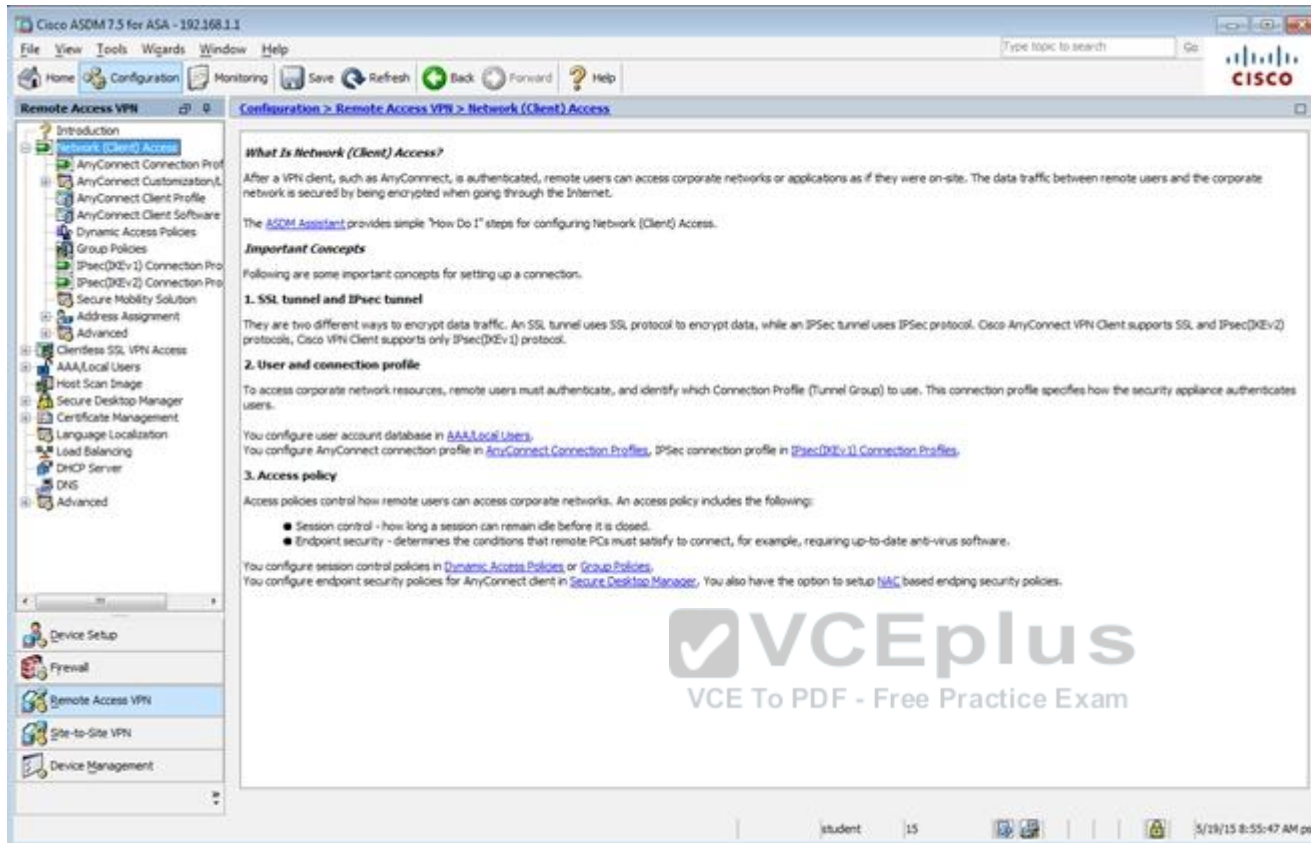
Certificates

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

Apply Reset


student 15 5/19/15 8:54:07 AM pst

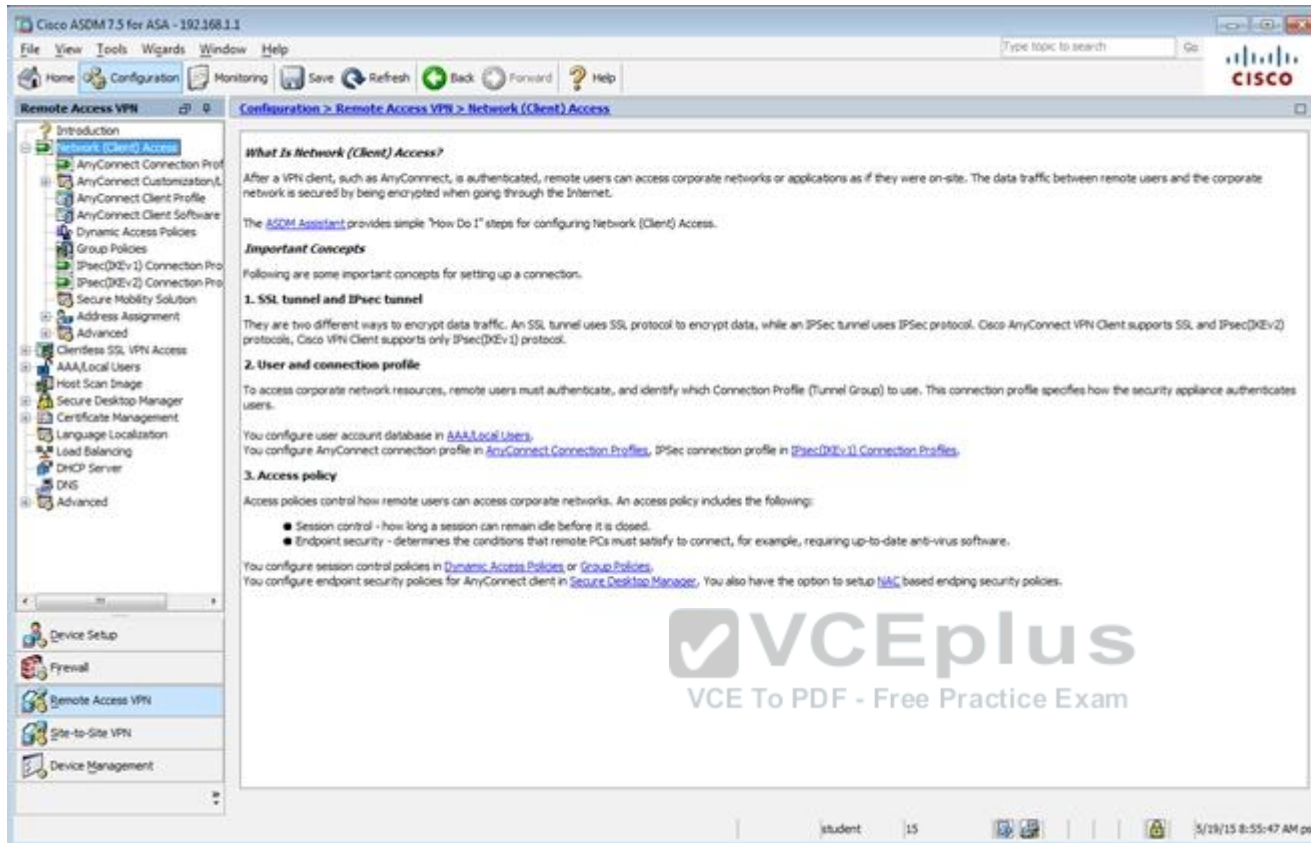




The screenshot displays the Cisco ASDM 7.5 for ASA - 102.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access' page. The page content includes:

- What Is Network (Client) Access?**  
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
- Important Concepts**  
Following are some important concepts for setting up a connection:
  - 1. SSL tunnel and IPsec tunnel**  
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.
  - 2. User and connection profile**  
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.  
You configure user account database in [AAA/Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).
  - 3. Access policy**  
Access policies control how remote users can access corporate networks. An access policy includes the following:
    - Session control - how long a session can remain idle before it is closed.
    - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

At the bottom of the page, there is a large watermark:  **VCEplus**  
VCE To PDF - Free Practice Exam



The screenshot displays the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the configuration tree with 'Remote Access VPN' expanded, and 'Network (Client) Access' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access' page. The page content includes an introduction, important concepts, and configuration steps for Network (Client) Access.

**What Is Network (Client) Access?**

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

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

**Important Concepts**

Following are some important concepts for setting up a connection.

**1. SSL tunnel and IPsec tunnel**

There are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec (IKEv2) protocols. Cisco VPN Client supports only IPsec (IKEv1) protocol.

**2. User and connection profile**

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

You configure user account database in [AAA/Local Users](#).  
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec \(IKEv1\) Connection Profiles](#).

**3. Access policy**

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

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

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

**Navigation Bar:** Home, Configuration, Monitoring, Save, Refresh, Back, Forward, Help

**Bottom Bar:** student | 15 | 3/19/15 8:55:47 AM pst

Edit Internal Group Policy: DfGrpPolicy

**Servers**  
Advanced  
Split Tunneling  
Browser Proxy  
AnyConnect Client  
IPsec(IKEv1) Client

Name: DfGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

**More Options**

Tunneling Protocols: ☒ Clientless SSL VPN ☐ SSL VPN Client ☒ IPsec IKEv1 ☒ IPsec IKEv2 ☒ L2TP/IPsec

Filter: --None--

NAC Policy: --None--

Access Hours: --Unrestricted--

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

Connection Profile (Tunnel Group) Lock: --None--

Maximum Connect Time: ☒ Unlimited  minutes

Idle Timeout: ☐ None  30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find:

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv1) Connection Profiles

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

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

Access Interfaces

Enable interfaces for IPsec access.

| Interface | Allow Access                        |
|-----------|-------------------------------------|
| outside   | <input checked="" type="checkbox"/> |
| dms       | <input type="checkbox"/>            |
| inside    | <input type="checkbox"/>            |

☒ Bypass interface access lists for inbound VPN sessions.

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

Connection Profiles

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

+ Add Edit Delete

| Name              | IPsec Enabled                       | L2TP/IPsec Enabled                  | Authentication Server Group | Group Policy  |
|-------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| DefaultIkev1Group | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD                         | DiffGrpPolicy |
| Clientless        | <input type="checkbox"/>            | <input type="checkbox"/>            | LOCAL                       | Sales         |

Find:  Match Case

Apply Reset

student 15 5/19/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

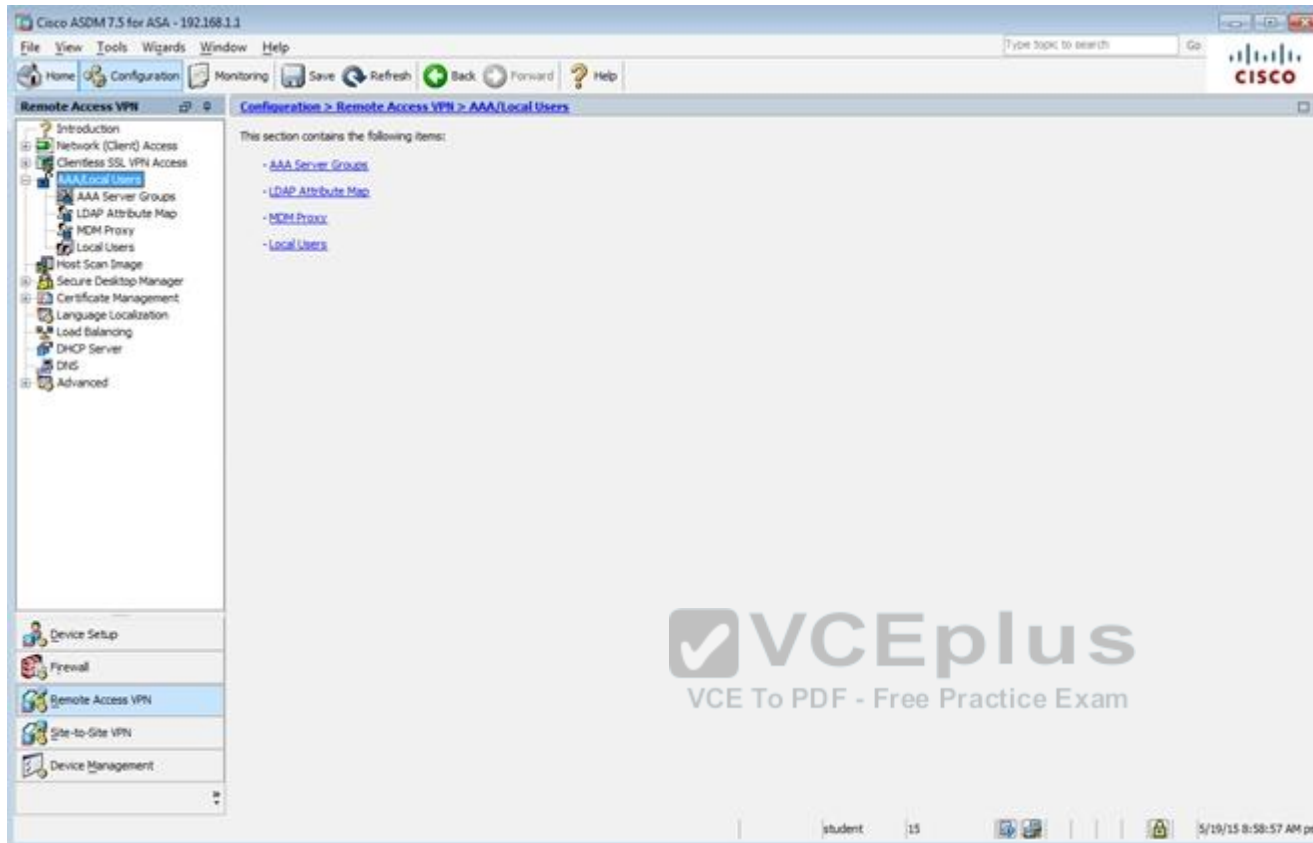
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

End:

| Name            | SSL Enabled                         | IPsec Enabled                       | Aliases | Authentication Method | Group Policy |
|-----------------|-------------------------------------|-------------------------------------|---------|-----------------------|--------------|
| DefaultRAGroup  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | GrpGrpPolicy |
| DefaultEAPGroup | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |         | AAA(RADIUS)           | GrpGrpPolicy |
| DefaultSSLGroup | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | yes     | AAA(RADIUS)           | GrpGrpPolicy |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction  
Network (Client) Access  
Clientless SSL VPN Access  
AAA/Local Users  
AAA Server Groups  
LDAP Attribute Map  
MDM Proxy  
**Local Users**  
Host Scan Image  
Secure Desktop Manager  
Certificate Management  
Language Localization  
Load Balancing  
DHCP Server  
DNS  
Advanced

Create entries in the ASA local user database.

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

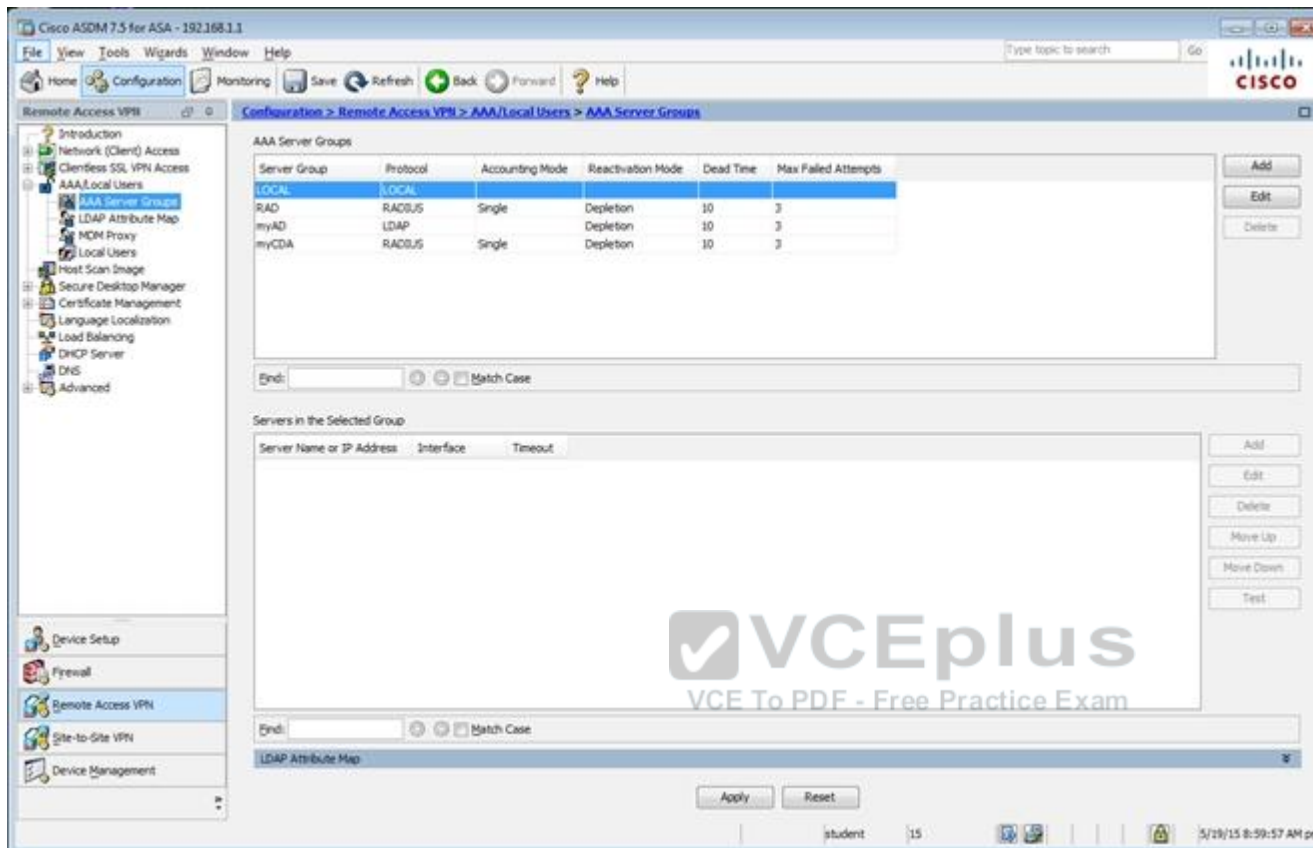
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

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

Find: Match Case

Apply Reset

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



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

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save

Firewall

- 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 >

Match Criteria

| # | Source Interface |
|---|------------------|
| 1 | Any              |

Add Network Object

Name: HTTP

Type: Host

IP Version: ☒ IPv4 ☐ IPv6

IP Address: 209.165.201.30

NAT

☒ Add Automatic Address Translation Rules

Type: Static

Translated Address: 172.16.1.2

☐ Use one-to-one address translation

☐ PAT Pool Translated Address: ..

☐ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

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

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

Add

#

dmz (1 in

1

inside (1 in

1

outside (1 in

1

Global (1 in

1

Add Access Rule

Interface: outside

Action: ☒ Permit ☐ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: 209.165.201.30

Security Group:

Service: tcp/http

Description:

☒ Enable Logging

Logging Level: Default

More Options

OK Cancel Help

Scenario TOPOLOGY

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Access Rules

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

+ Add Edit Delete Where Used Not Used

Diagram Export Clear Hits Show Log Packet Tr

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

Apply

Reset

Advanced

Scenario

TOPOLOGY

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

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



Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Service Policy Rules

+ Add Edit Delete Up Down Copy Paste Find Diagram Packet Trace

Traffic Classification

| Name                                    | # | Enabled | Match | Source | Src Security Group | Destination | Dst Security Group |
|---|---|---------|-------|--------|--------------------|-------------|--------------------|
| Interface: dmz; Policy: asacx_policy    |   |         |       |        |                    |             |                    |
| class-default                           |   |         | Match | any    |                    | any         |                    |
| Interface: inside; Policy: asacx_policy |   |         |       |        |                    |             |                    |
| class-default                           |   |         | Match | any    |                    | any         |                    |
| Global; Policy: global_policy           |   |         |       |        |                    |             |                    |
| inspection_de...                        |   |         | Match | any    |                    | any         |                    |

Apply Reset

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

Configuration

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
- ☐ DCERPC
- ☒ DNS
- ☒ ESMTP
- ☒ FTP
- ☒ H.323 H.225
- ☒ H.323 RAS
- ☐ HTTP
- ☒ ICMP
- ☐ ICMP Error
- ☐ ILS
- ☐ IM
- ☒ IP-Options
- ☐ IPSec-Pass-Thru
- ☐ IPv6
- ☐ MMP

Configure...

DNS Inspect Map: preset\_dns\_map

Scenario TOPOLOGY

After that is done, we can ping [www.cisco.com](http://www.cisco.com) again to verify:



Inside PC



cmd.exe

```
Press RETURN to get started!
C:\ping www.cisco.com
Pinging  with 32 bytes of data:Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for www.cisco.com:    Packets: Sent = 4,  Recieved = 0,  Lost = 
(100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\ping www.cisco.com
Pinging el44.dscb.akamaiedge.net [23.72.192.170] with 32 bytes of data: with 3
bytes of data:
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:\
```

