



Exam 210-260

Implementing Cisco Network Security

Version: 21.0

[Total Questions: 310]



1. Which FirePOWER preprocessor engine is used to prevent SYN attacks?

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

Answer: A

2. Which statement about college campus is true?

- A. College campus has geographical position.
- B. College campus Hasn't got internet access.
- C. College campus Has multiple subdomains.

Answer: A

3. 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.

Answer: B

4. 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

Answer: A



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

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

Answer: A,B,C

6. Which port should (or would) be open if VPN NAT-T was enabled

- A. port 500
- B. port 500 outside interface
- C. port 4500 outside interface
- D. port 4500 ipsec

Answer: D

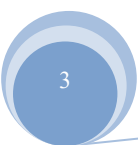
7. If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

- 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.

Answer: A

8. Which of the following pairs of statements is true in terms of configuring MD authentication?

- A. Interface statements (OSPF, EIGRP) must be configured; use of key chain in OSPF
- B. Router process (OSPF, EIGRP) must be configured; key chain in EIGRP
- C. Router process (only for OSPF) must be configured; key chain in EIGRP





D. Router process (only for OSPF) must be configured; key chain in OSPF

Answer: C

9. Which two NAT types allows only objects or groups to reference an IP address? (choose two)

- A. dynamic NAT
- B. dynamic PAT
- C. static NAT
- D. identity NAT

Answer: A,C

10. 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.

Answer: A

11. What is example of social engineering

- A. Gaining access to a building through an unlocked door.
- B. something about inserting a random flash drive.
- C. gaining access to server room by posing as IT
- D. Watching other user put in username and password (something around there)

Answer: C

12. 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

Answer: A





13. What is the effect of the ASA command `crypto isakmp nat-traversal`?

- A. It opens port 4500 only on the outside interface.
- B. It opens port 500 only on the inside interface.
- C. It opens port 500 only on the outside interface.
- D. It opens port 4500 on all interfaces that are IPsec enabled.

Answer: D

14. Which statement is a benefit of using Cisco IOS IPS?

- A. It uses the underlying routing infrastructure to provide an additional layer of security.
- B. It works in passive mode so as not to impact traffic flow.
- C. It supports the complete signature database as a Cisco IPS sensor appliance.
- D. The signature database is tied closely with the Cisco IOS image.

Answer: A

Explanation:

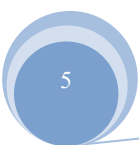
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

Product Overview

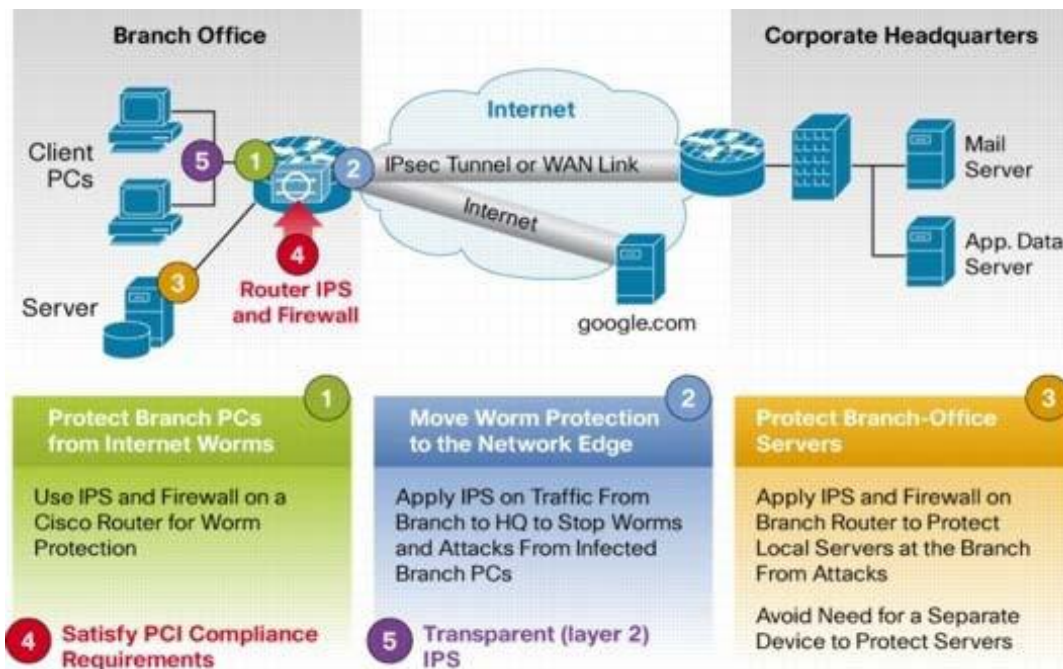
In today's business environment, network intruders and attackers can come from outside or inside the network.

They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.



Cisco IOS IPS: Major Use Cases and Key Benefits IOS IPS helps to protect your network in 5 ways:



Key Benefits:

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications.
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks.
- Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies.
- Offers field-customizable worm and attack signature set and event actions.
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions.
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router.
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances.

15. What configure mode you used for the command ip ospf authentication-key c1\$c0?

- A. global
- B. privileged



- C. in-line
- D. Interface

Answer: D

Explanation: ip ospf authentication-key is used under interface configuration mode, so it's in interface level, under global configuration mode. If it asks about interface level then choose that.

interface Serial0

ip address 192.16.64.1 255.255.25

16. 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.

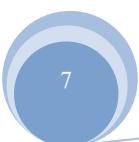
Answer: A

17. Which description of the nonsecret numbers that are used to start a Diffie-Hellman exchange is true?
- A. They are large pseudorandom numbers.
 - B. They are very small numbers chosen from a table of known values
 - C. They are numeric values extracted from hashed system hostnames.
 - D. They are preconfigured prime integers

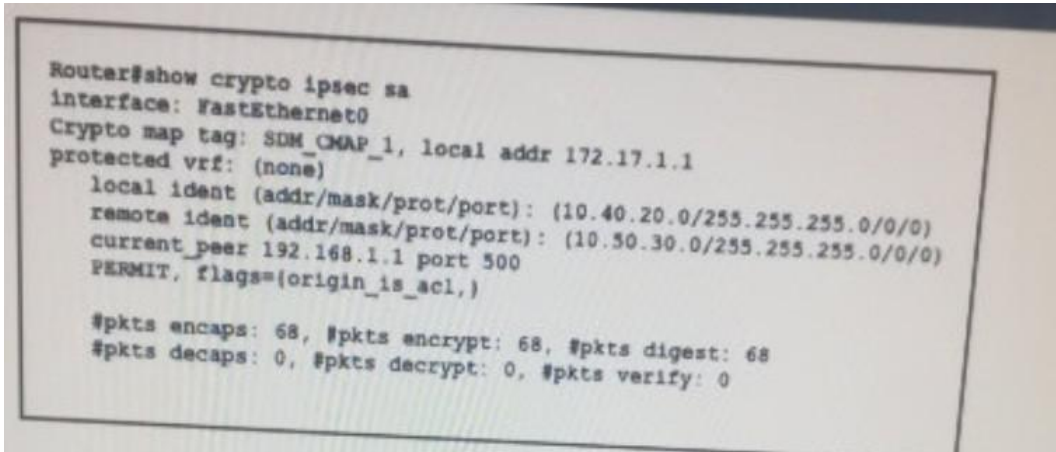
Answer: D

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

Answer: A



19. Refer to the exhibit.



For which reason is the tunnel unable to pass traffic?

- A. UDP port 500 is blocked.
- B. The IP address of the remote peer is incorrect.
- C. The tunnel is failing to receive traffic from the remote peer.
- D. The local peer is unable to encrypt the traffic.

Answer: C

20. Which two functions can SIEM provide? (Choose Two)

- A. Correlation between logs and events from multiple systems.
- B. event aggregation that allows for reduced log storage requirements.
- C. proactive malware analysis to block malicious traffic.
- D. dual-factor authentication.
- E. centralized firewall management.

Answer: A,C

21. Where OAKLEY and SKEME come to play?

- A. IKE
- B. ISAKMP
- C. DES

Answer: A

22. Which statement provides the best definition of malware?



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

Answer: A

23. 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.

Answer: A

24. What show command can see vpn tunnel establish with traffic passing through.

- A. (config)# show crypto ipsec sa
- B. #show crypto ipsec sa
- C. (config-if)#

Answer: A

25. Which command initializes a lawful intercept view?

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

Answer: C

26. With which preprocessor do you detect incomplete TCP handshakes

- A. rate based prevention
- B. portscan detection



Answer: A

27. Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

- A. nested object-class
- B. class-map
- C. extended wildcard matching
- D. object groups

Answer: D

Explanation:

Reference: <http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/objectgroups.html>

Information About Object Groups

By grouping like objects together, you can use the object group in an ACE instead of having to enter an ACE for each object separately. You can create the following types of object groups:

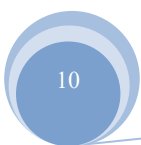
- Protocol
- Network
- Service
- ICMP type

For example, consider the following three object groups:

- MyServices — Includes the TCP and UDP port numbers of the service requests that are allowed access to the internal network.
- TrustedHosts — Includes the host and network addresses allowed access to the greatest range of services and servers.
- PublicServers — Includes the host addresses of servers to which the greatest access is provided.

After creating these groups, you could use a single ACE to allow trusted hosts to make specific service requests to a group of public servers. You can also nest object groups in other object groups.

28. 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.

Answer: A,E

29. The Oakley cryptography protocol is compatible with following for managing security?

- A. IPSec
- B. ISAKMP

Answer: B

30. 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

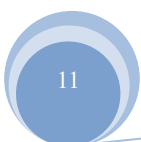
Answer: A,F

31. What can cause the the state table of a stateful firewall to update? (choose two)

- A. when a connection is created
- B. When a connection's timer has expired within state table
- C. C. when packet is evaluated against the outbound access list and is denied
- D. D. when outbound packets forwarded to outbound interface
- E. E. when rate-limiting is applied

Answer: A,B

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





- A. Sha1
- B. Sha2
- C. Md5
- D. Md1

Answer: C

33. Which security zone is automatically defined by the system?

- A. The source zone
- B. The self zone
- C. The destination zone
- D. The inside zone

Answer: B

34. With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

- A. traffic flowing between a zone member interface and any interface that is not a zone member
- B. traffic flowing to and from the router interfaces (the self zone)
- C. traffic flowing among the interfaces that are members of the same zone
- D. traffic flowing among the interfaces that are not assigned to any zone
- E. traffic flowing between a zone member interface and another interface that belongs in a different zone
- F. traffic flowing to the zone member interface that is returned traffic

Answer: B,C,D

Explanation:

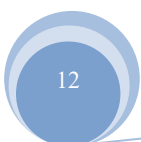
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080_8bc994.shtml

Rules For Applying Zone-Based Policy Firewall

Router network interfaces' membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces:

A zone must be configured before interfaces can be assigned to the zone. An interface can be assigned to only one security zone.

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except





traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones. Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.

If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.

From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).

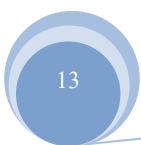
The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

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

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

Answer: A,B

36. Refer to the below.





```
Router# debug tacacs
```

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Which statement about this debug output is true?

- A. The requesting authentication request came from username GETUSER.
- B. The TACACS+ authentication request came from a valid user.
- C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.
- D. The initiating connection request was being spoofed by a different source address.

Answer: B

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfser.html debug tacacs

To display information associated with the TACACS, use the debug tacacs privileged EXEC command. The no form of this command disables debugging output.

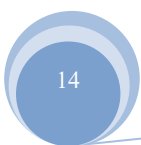
debug tacacs

no debug tacacs

The following is sample output from the debug tacacs command for a TACACS login attempt that was successful, as indicated by the status PASS:

```
Router# debug tacacs
```

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
```





(AUTHEN/START)

14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15 14:00:09: TAC+ (383258052): received authen response status = GETUSER 14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15 14:00:10: TAC+ (383258052): received authen response status = GETPASS 14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15 14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15

37. What technology can you use to provide data confidentiality, data integrity and data origin authentication on your network?

- A. Certificate Authority
- B. IKE
- C. IPSec
- D. Data Encryption Standards

Answer: C

38. Referencing the CIA model, in which scenario is a hash-only function most appropriate?

- A. securing wireless transmissions.
- B. securing data in files.
- C. securing real-time traffic
- D. securing data at rest

Answer: D

39. 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.

Answer: A

40. which are two valid TCP connection states (pick 2) is the gist of the question.

- A. SYN-RCVD
- B. Closed
- C. SYN-WAIT
- D. RCVD
- E. SENT

Answer: A,B

41. What information does the key length provide in an encryption algorithm?

- A. the packet size
- B. the number of permutations
- C. the hash block size
- D. the cipher block size

Answer: C

42. 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

Answer: A,B

43. Which line in the following OSPF configuration will not be required for MD5 authentication to work?

```
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNA
!
router ospf 65000
router-id 192.168.10.1
area 20 authentication message-digest network 10.1.1.0 0.0.0.255 area 10
network 192.168.10.0 0.0.0.255 area 0
!
```

- A. ip ospf authentication message-digest
- B. network 192.168.10.0 0.0.0.255 area 0
- C. area 20 authentication message-digest
- D. ip ospf message-digest-key 1 md5 CCNA

Answer: C

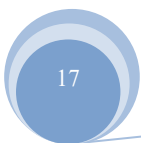
44. If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

- A. STP BPDU guard
- B. loop guard
- C. STP Root guard
- D. EtherChannel guard

Answer: A

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

- A. Adaptive Security Appliance





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

Answer: B

46. 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

Answer: A

47. Refer to the exhibit.

```
Oct 13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=""
action=LOGIN service=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): password incorrect
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct 13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

Which statement about this output is true?

- A. The user logged into the router with the incorrect username and password.
- B. The login failed because there was no default enable password.
- C. The login failed because the password entered was incorrect.
- D. The user logged in and was given privilege level 15.

Answer: C

Explanation:



http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html debug aaa authentication

To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication, use the debug aaa authentication privileged EXEC command.

To disable debugging command, use the no form of the command. debug aaa authentication
no debug aaa authentication

The following is sample output from the debug aaa authentication command. A single EXEC login that uses the "default" method list and the first method, TACACS+, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several are occurring concurrently.

Router# debug aaa authentication

6:50:12: AAA/AUTHEN: create_user user="" ruser="" port='tty19' rem_addr='172.31.60.15' authen_type=1
service=1 priv=1

6:50:12: AAA/AUTHEN/START (0): port='tty19' list="" action=LOGIN service=LOGIN 6:50:12:
AAA/AUTHEN/START (0): using "default" list

6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+

6:50:12: TAC+ (50996740): received authen response status = GETUSER 6:50:12: AAA/AUTHEN
(50996740): status = GETUSER

6:50:15: AAA/AUTHEN/CONT (50996740): continue_login

6:50:15: AAA/AUTHEN (50996740): status = GETUSER

6:50:15: AAA/AUTHEN (50996740): Method=TACACS+

6:50:15: TAC+: send AUTHEN/CONT packet

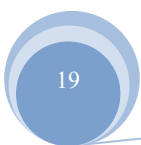
6:50:15: TAC+ (50996740): received authen response status = GETPASS 6:50:15: AAA/AUTHEN
(50996740): status = GETPASS

6:50:20: AAA/AUTHEN/CONT (50996740): continue_login

6:50:20: AAA/AUTHEN (50996740): status = GETPASS

6:50:20: AAA/AUTHEN (50996740): Method=TACACS+

6:50:20: TAC+: send AUTHEN/CONT packet



6:50:20: TAC+ (50996740): received authen response status = PASS 6:50:20: AAA/AUTHEN (50996740):
status = PASS

48. In which configuration mode do you configure the ip ospf authentication-key 1 command?

- A. Interface
- B. routing process
- C. global
- D. privileged

Answer: A

49. Which command should be used to enable AAA authentication to determine if a user can access the privilege command level?

- A. aaa authentication enable level
- B. aaa authentication enable default local
- C. aaa authentication enable method default
- D. aaa authentication enable local

Answer: B

Explanation: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfat hen.html

50. Which feature filters CoPP packets?

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

Answer: A

51. 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.

Answer: A

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

- A. access
- B. core
- C. distribution
- D. user
- E. server
- F. Internet

Answer: A,B,C

53. Which accounting notices are used to send a failed authentication attempt record to a AAA server?

(Choose two.)

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

Answer: A,C

54. Which two characteristics of an application layer firewall are true? (Choose two)

- A. provides protection for multiple applications
- B. is immune to URL manipulation
- C. provides reverse proxy services
- D. provides stateful firewall functionality
- E. has low processor usage

Answer: A,C

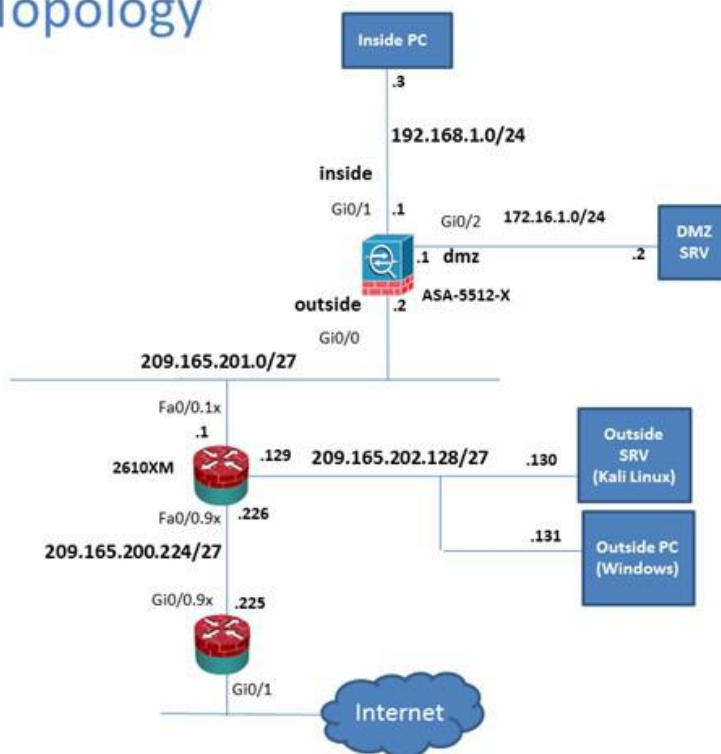
55. Scenario

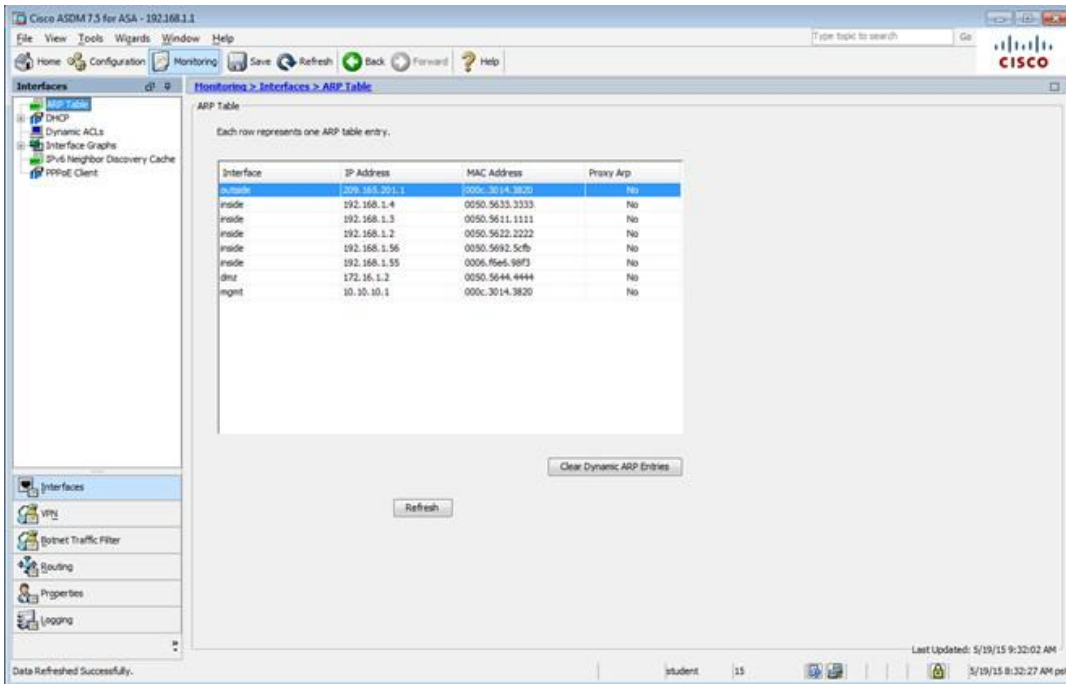
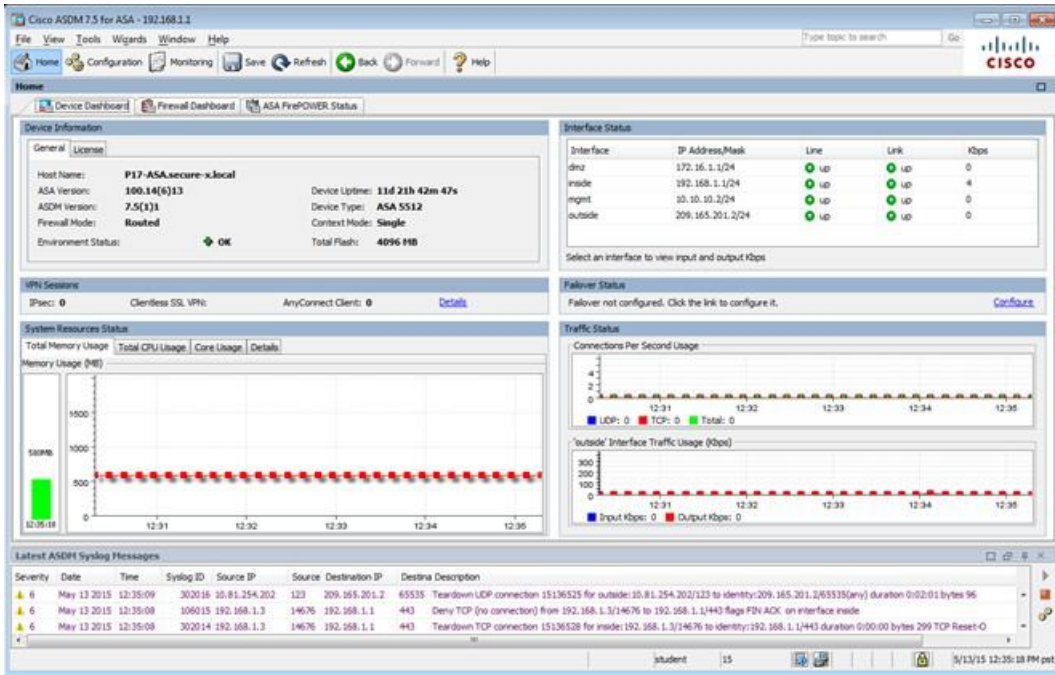
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

VPN Statistics

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IPsec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WPA Sessions

Interfaces

VPN

Internet Traffic Filter

Routing

Properties

Logging

Monitoring > VPN > VPN Statistics > Sessions

Type Active Cumulative Peak Concurrent Inactive

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	Group Policy	Protocol	Login Time	Bytes Tx	Bytes Rx
student	student	Clientless	06:05:46 pm Thu May 21 2015	316774	41633
209.165.202.131	Clientless	Clientless (IPsec)	06:05:46 pm		

Refresh

Last Updated: 5/26/15 9:33:12 AM

Data Refreshed Successfully.

student 15

5/26/15 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 > Startup Wizard

Click the "Launch Startup Wizard" button to start the wizard.

Startup Wizard

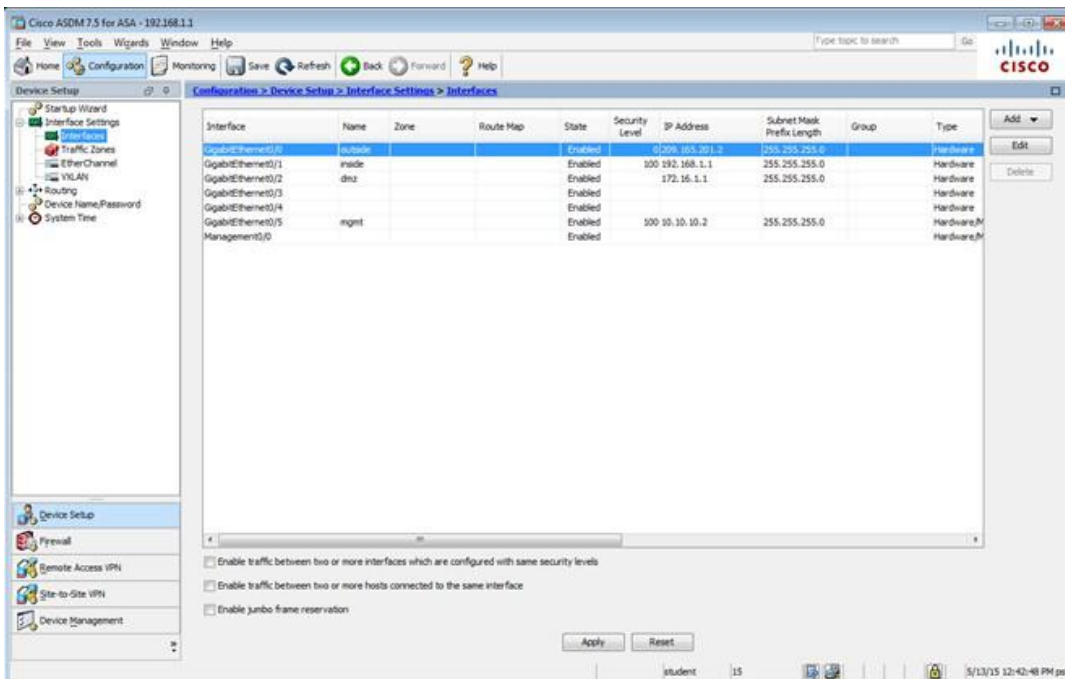
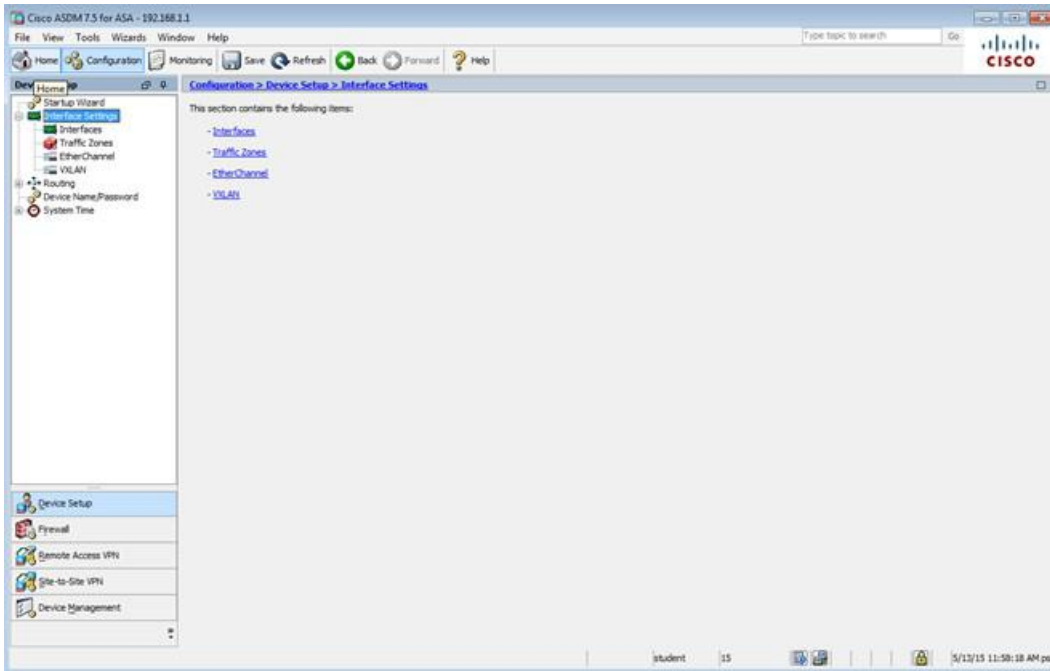
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

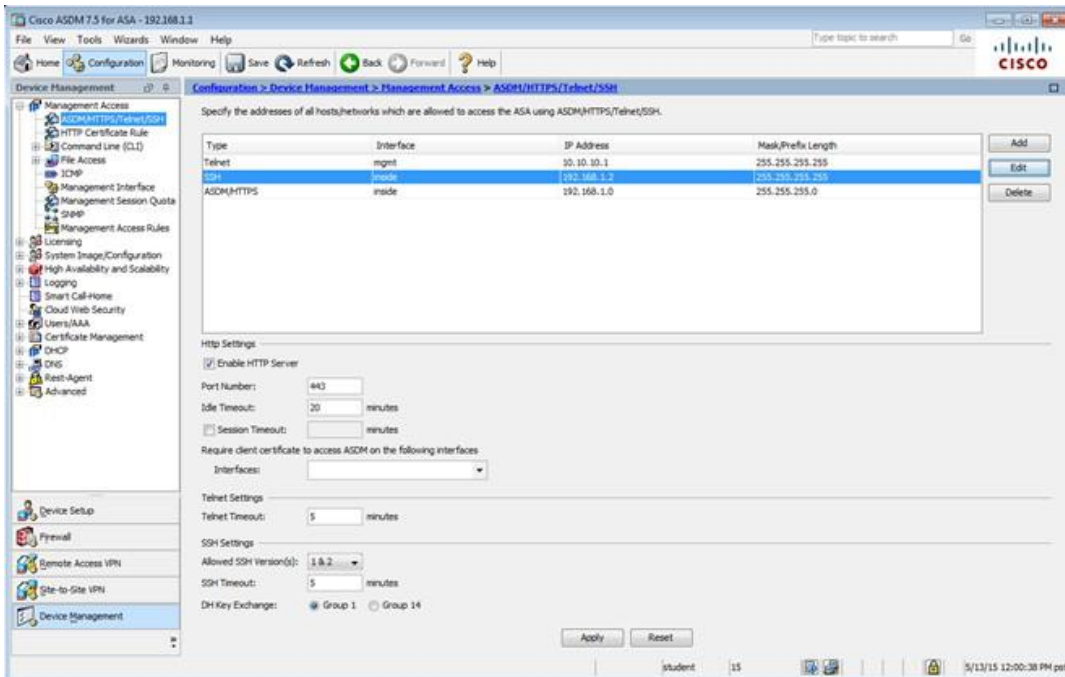
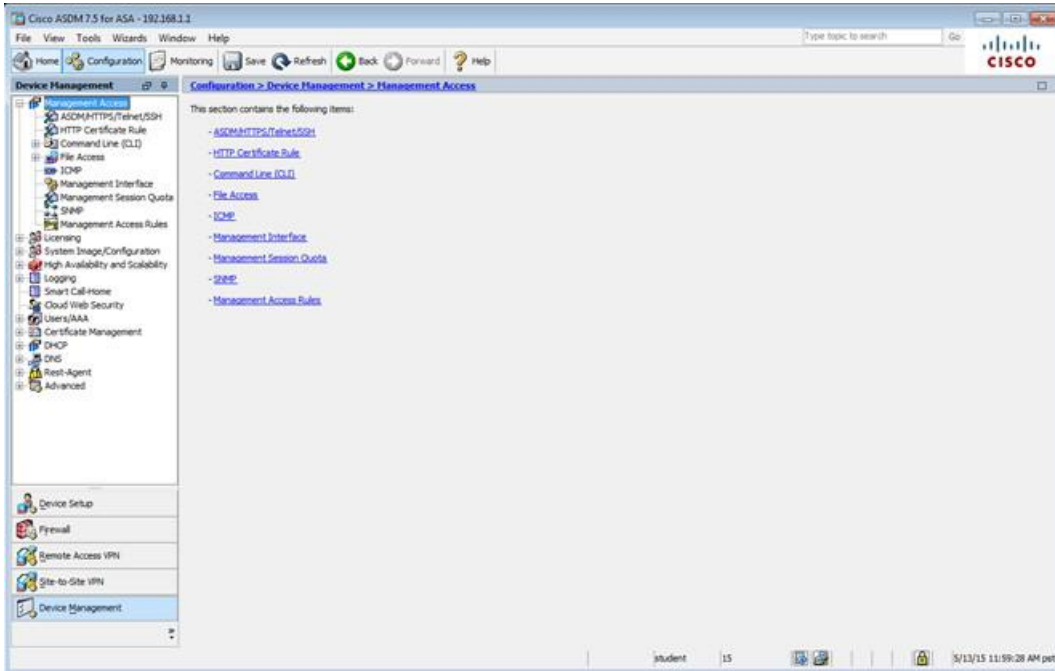
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

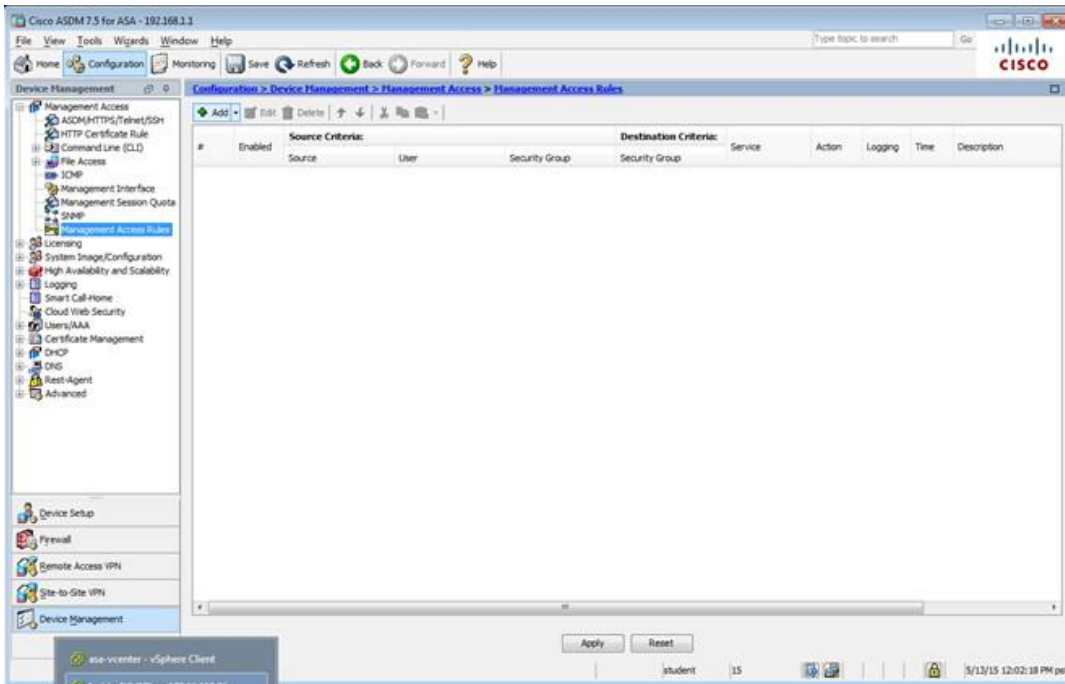
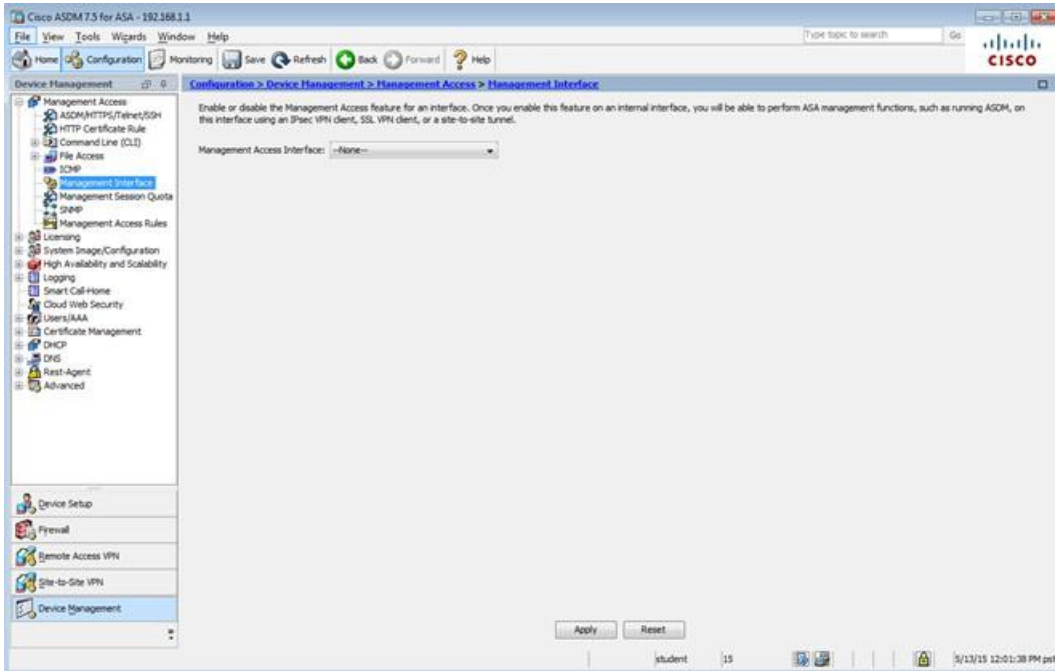
Launch Startup Wizard

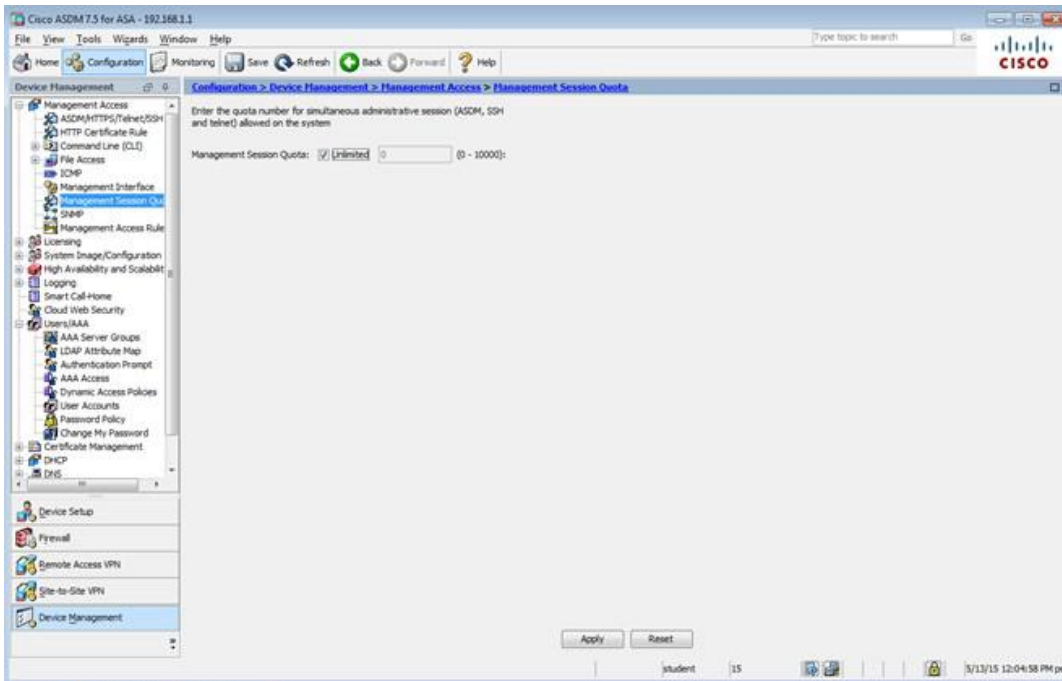
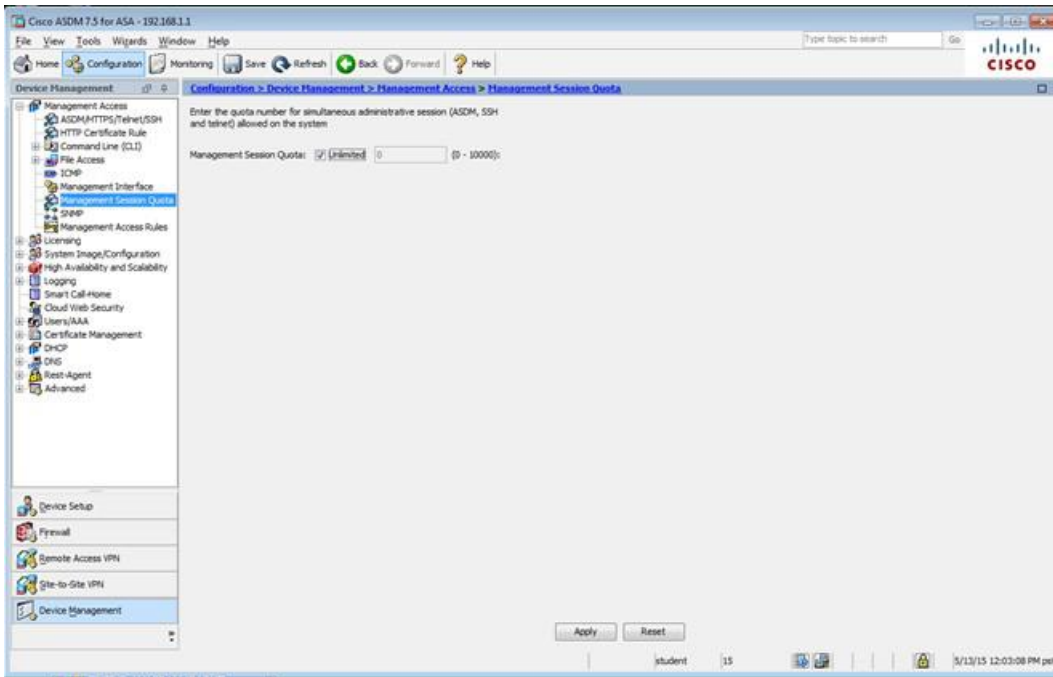
student 15

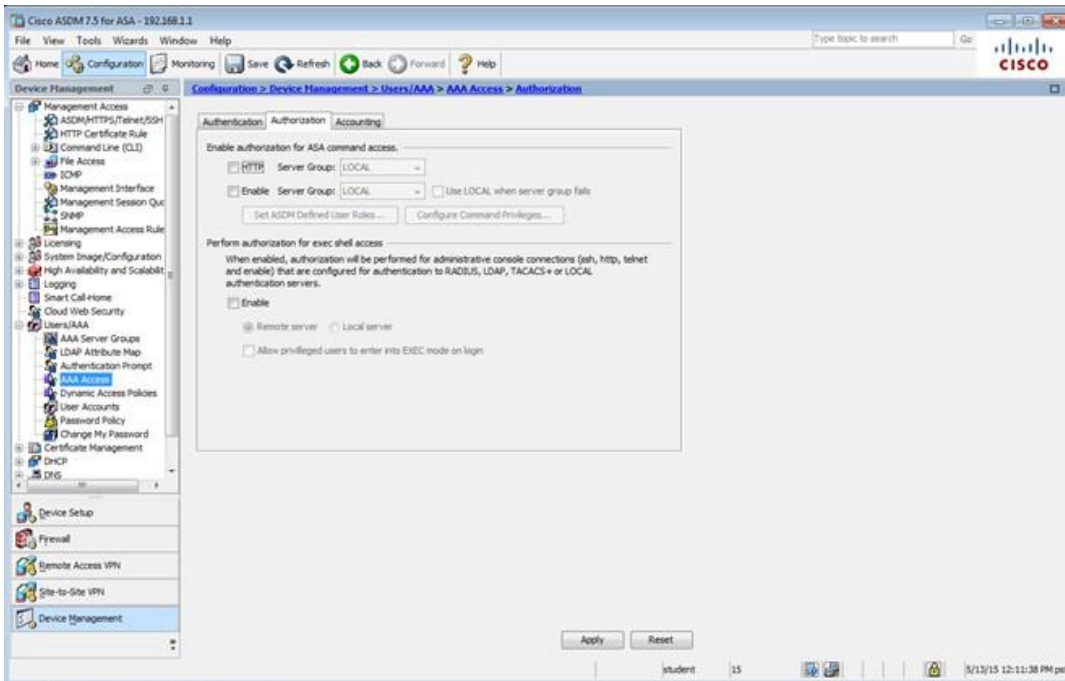
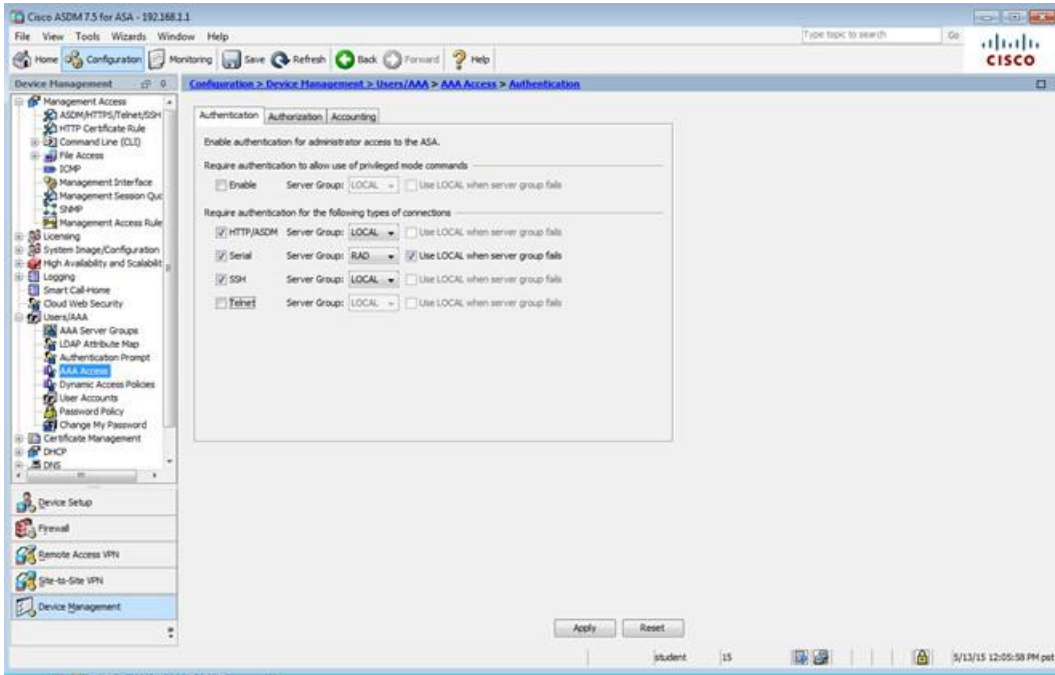
5/26/15 11:56:08 AM pst

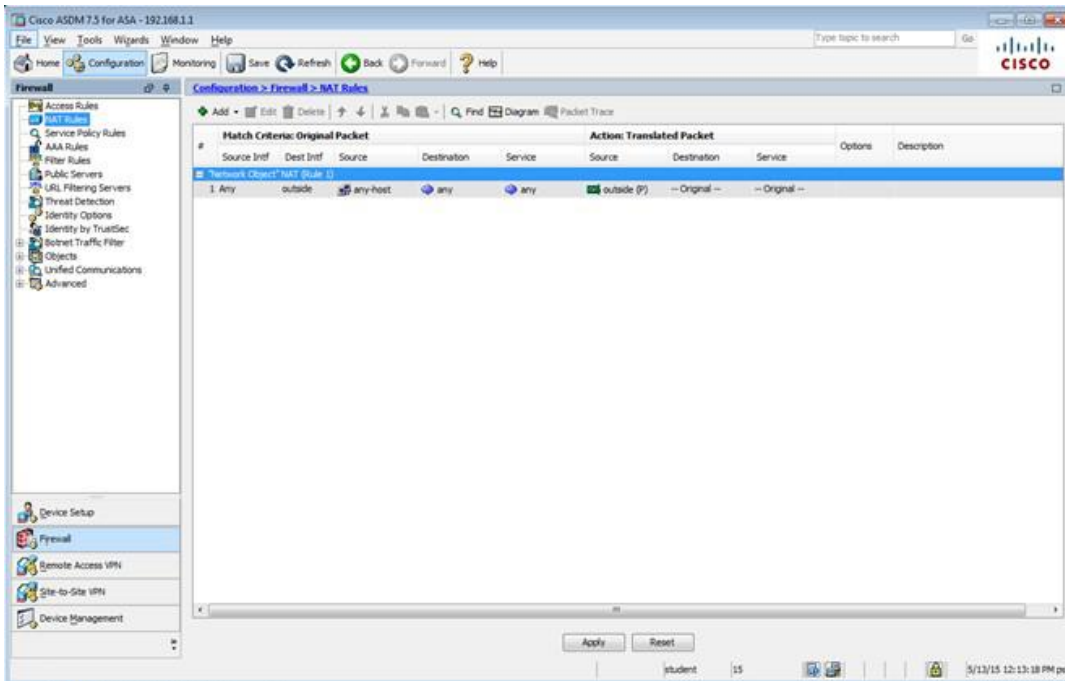
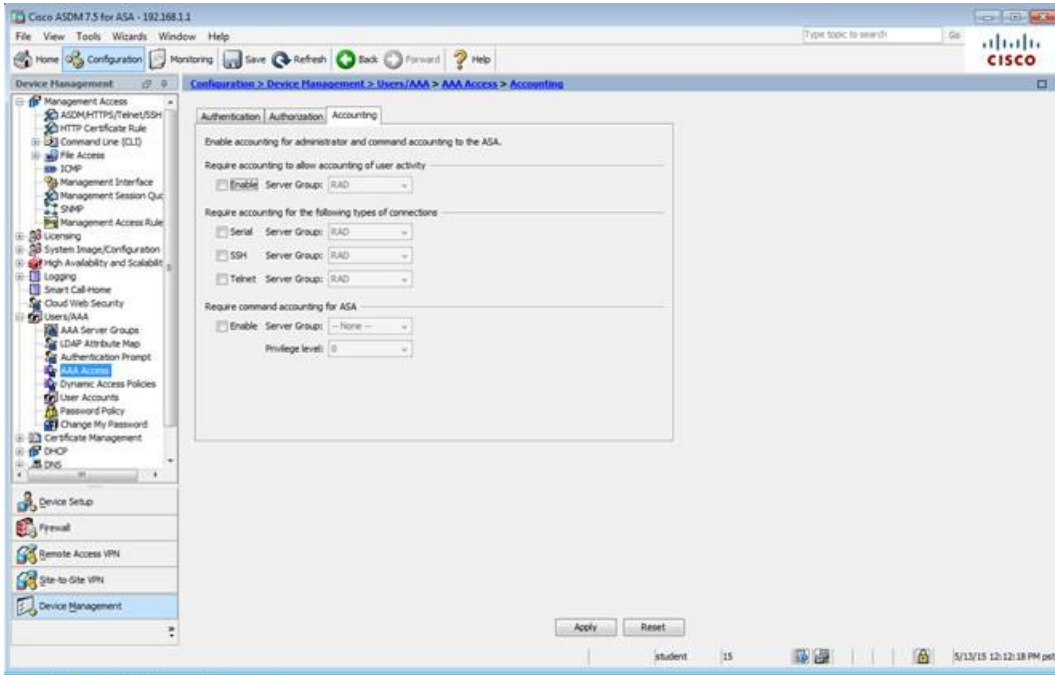


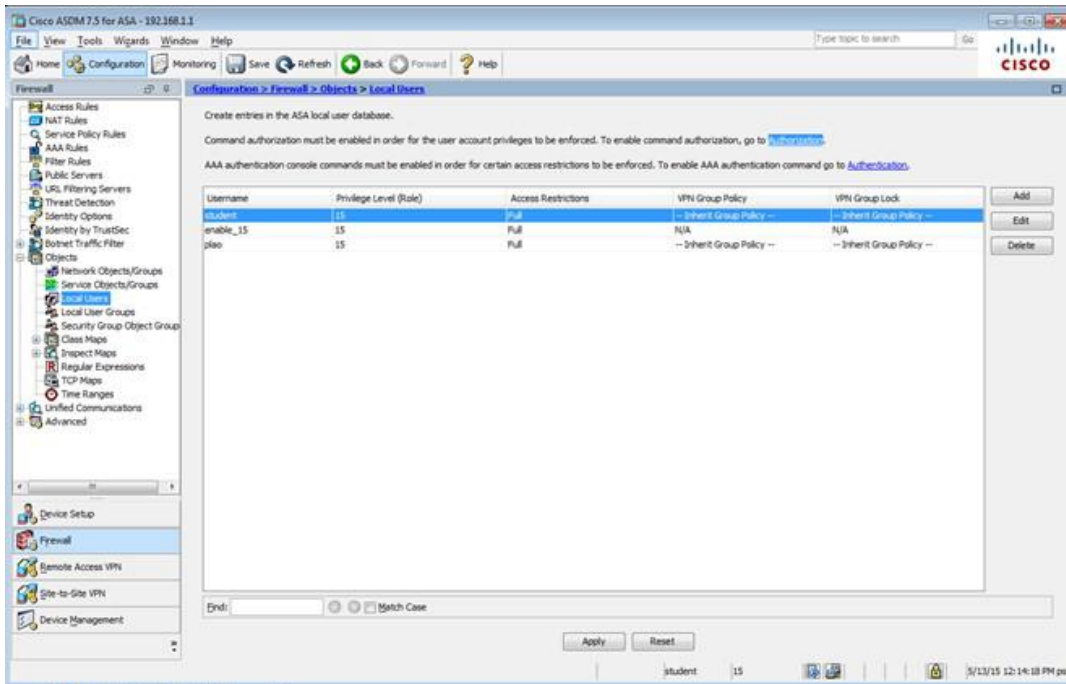
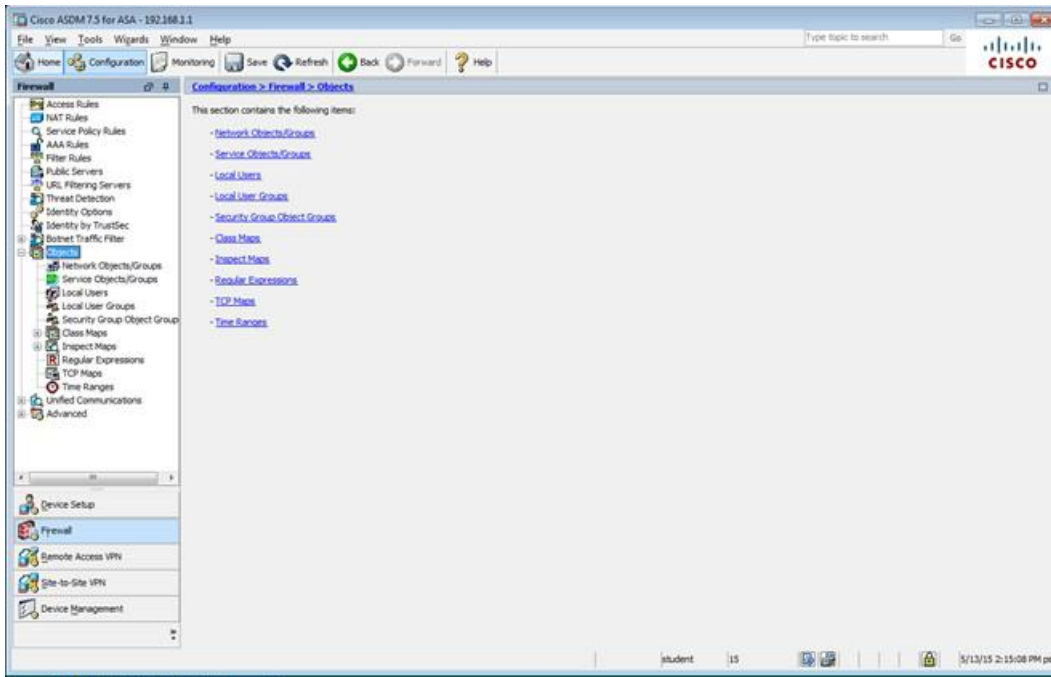


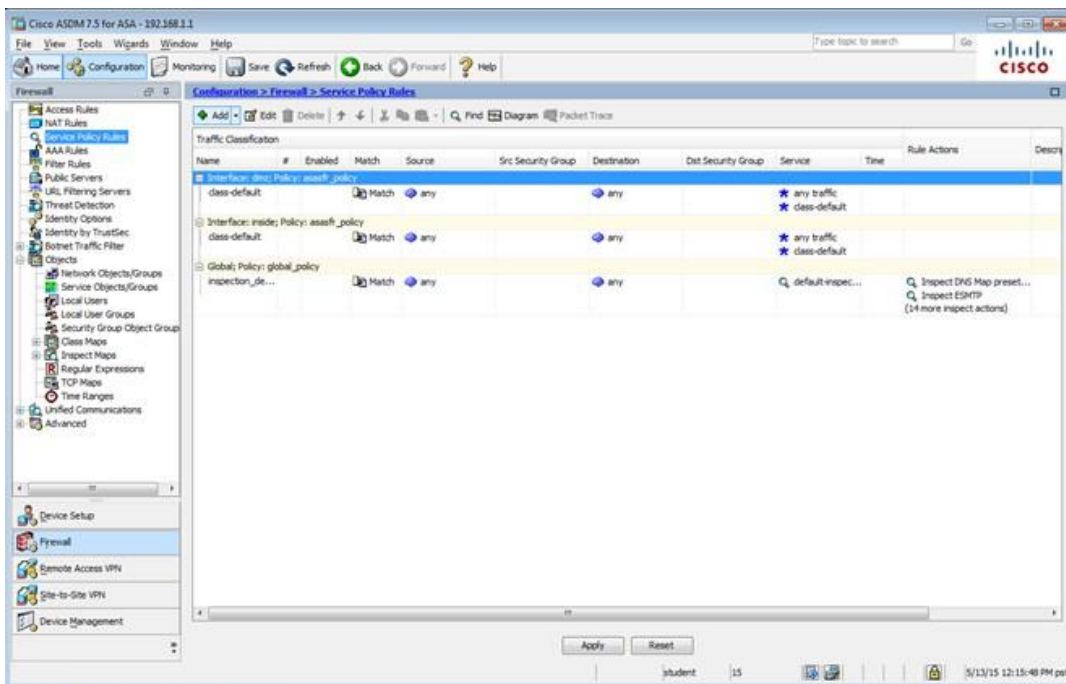
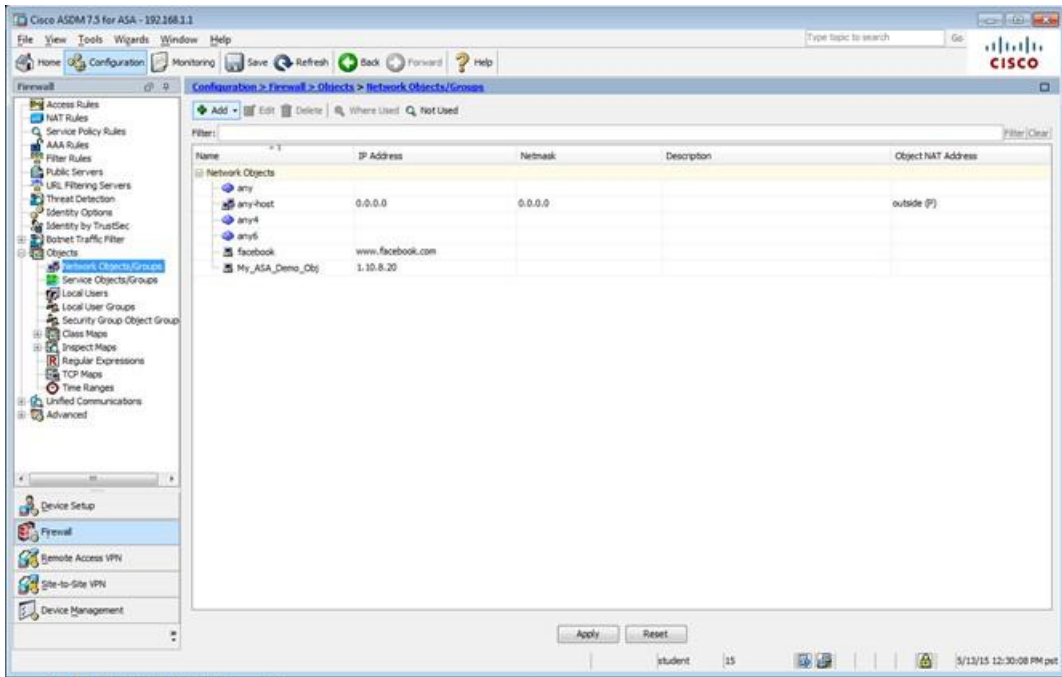


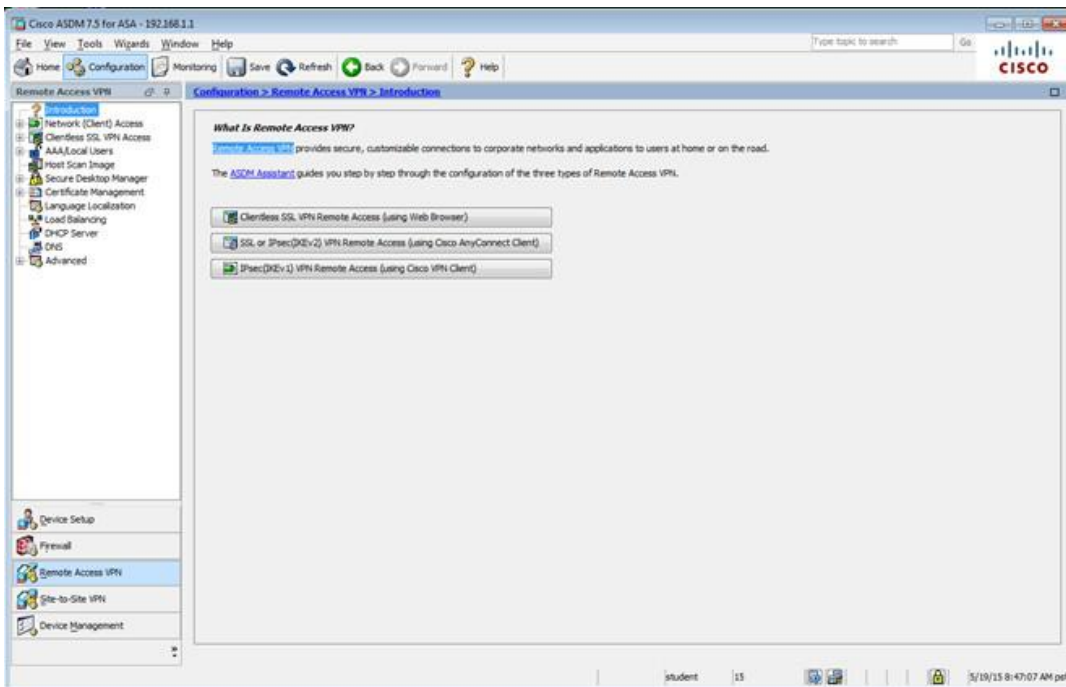
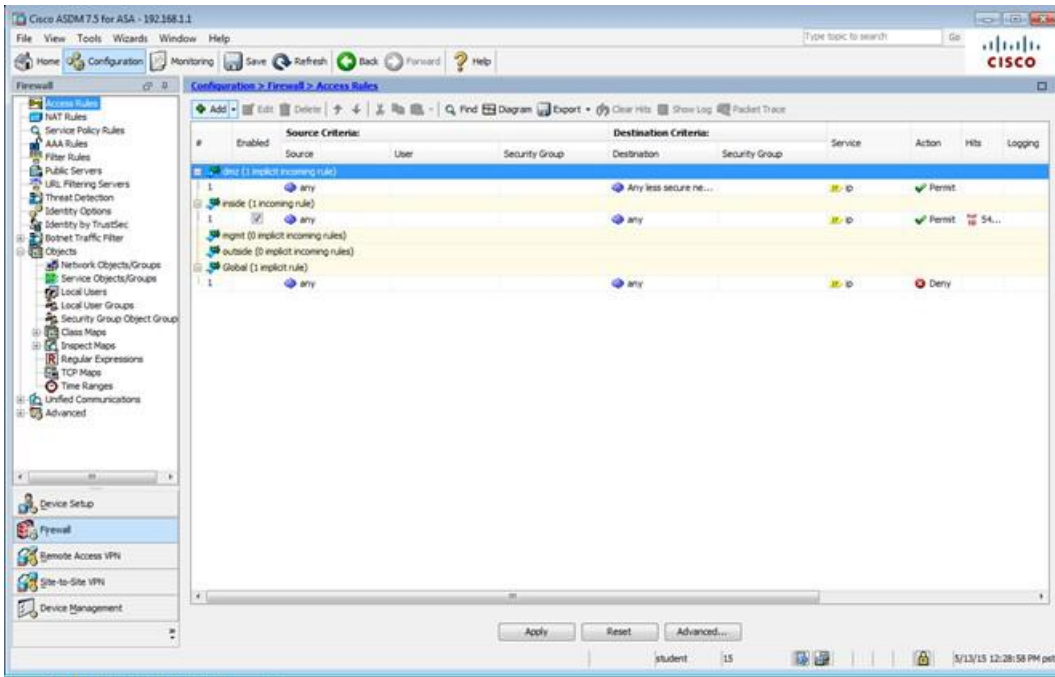


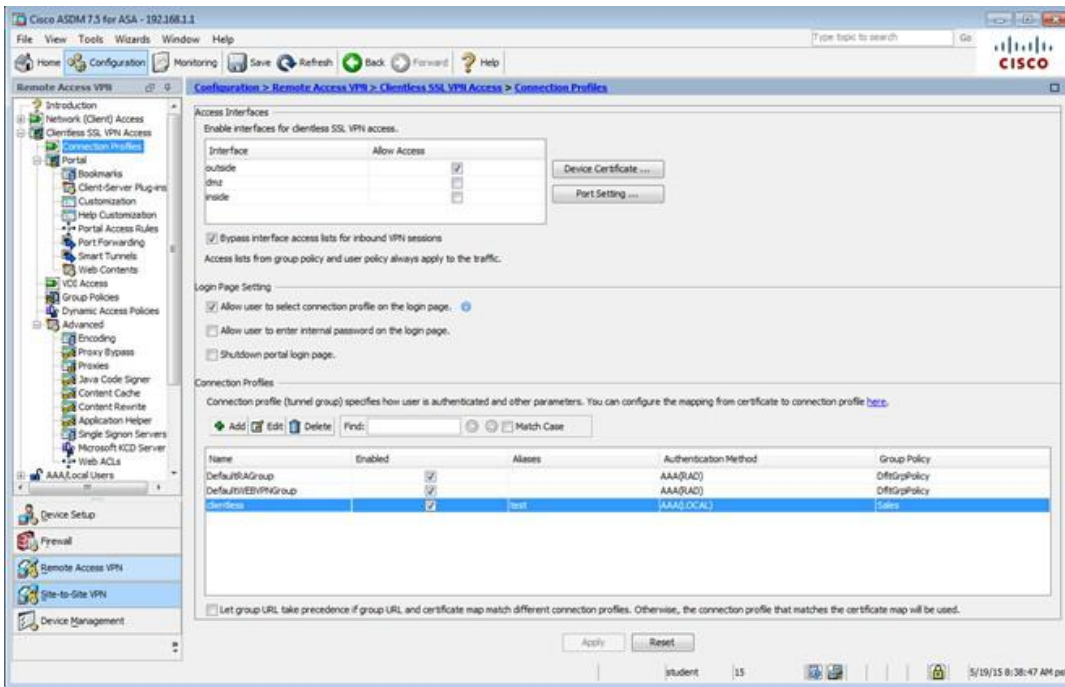
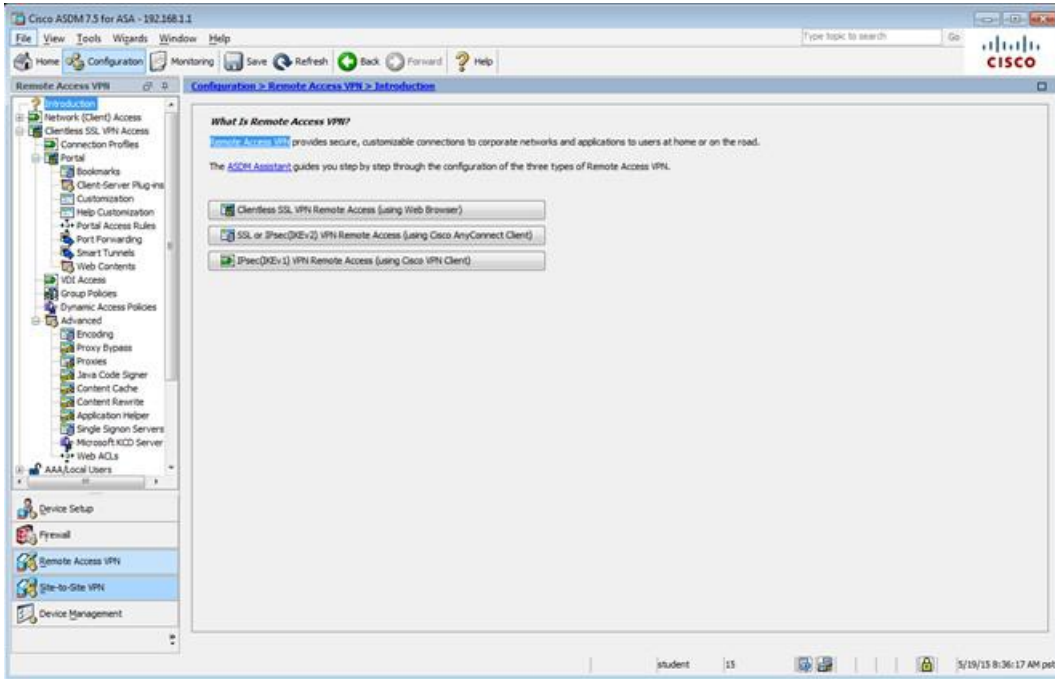












Edit Clientless SSL VPN Connection Profile: clientless

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)

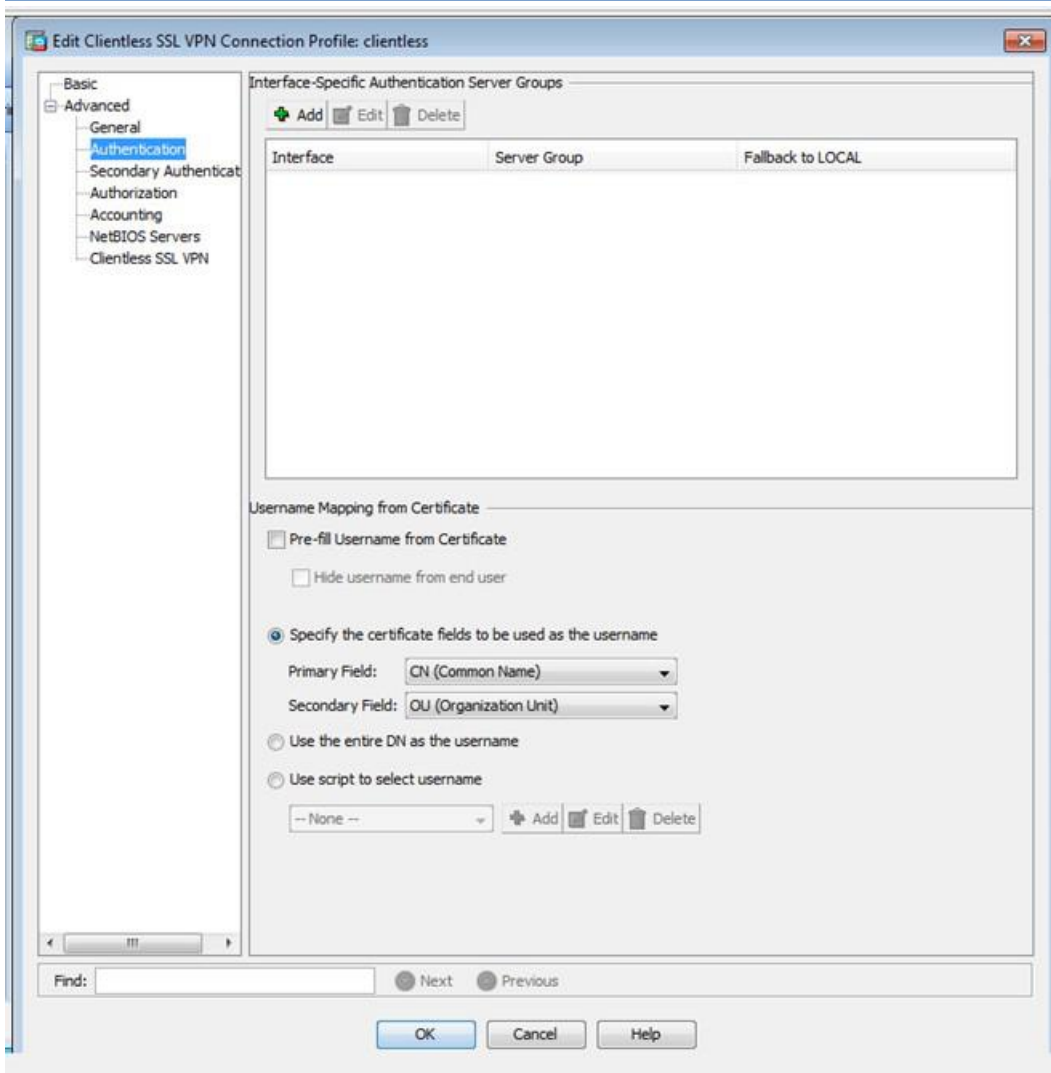
☒ Always run CSD

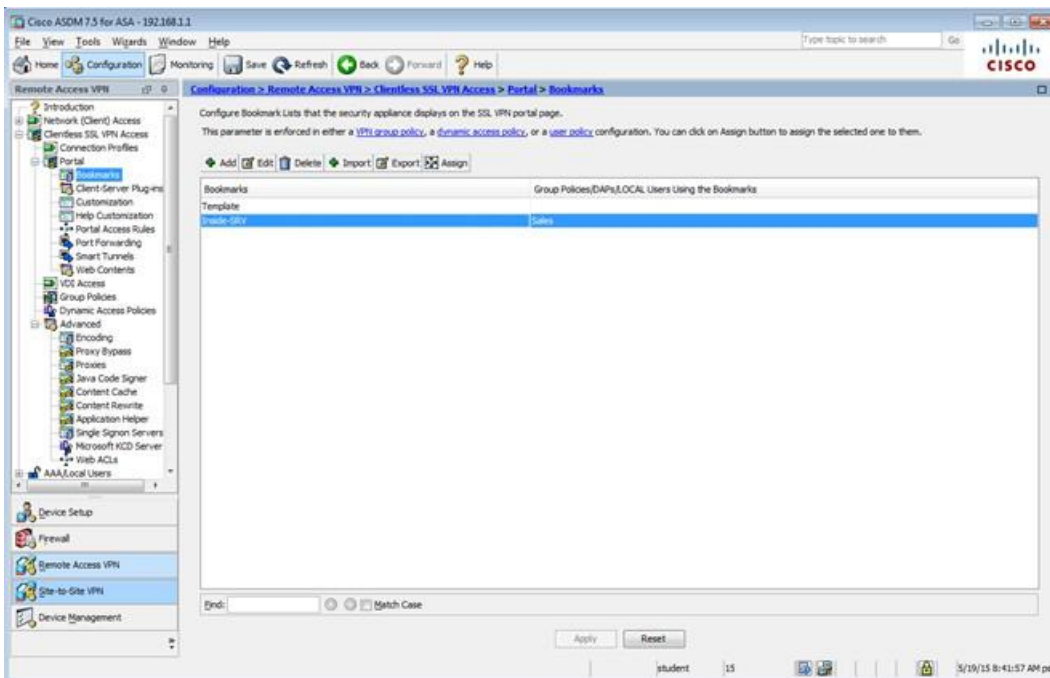
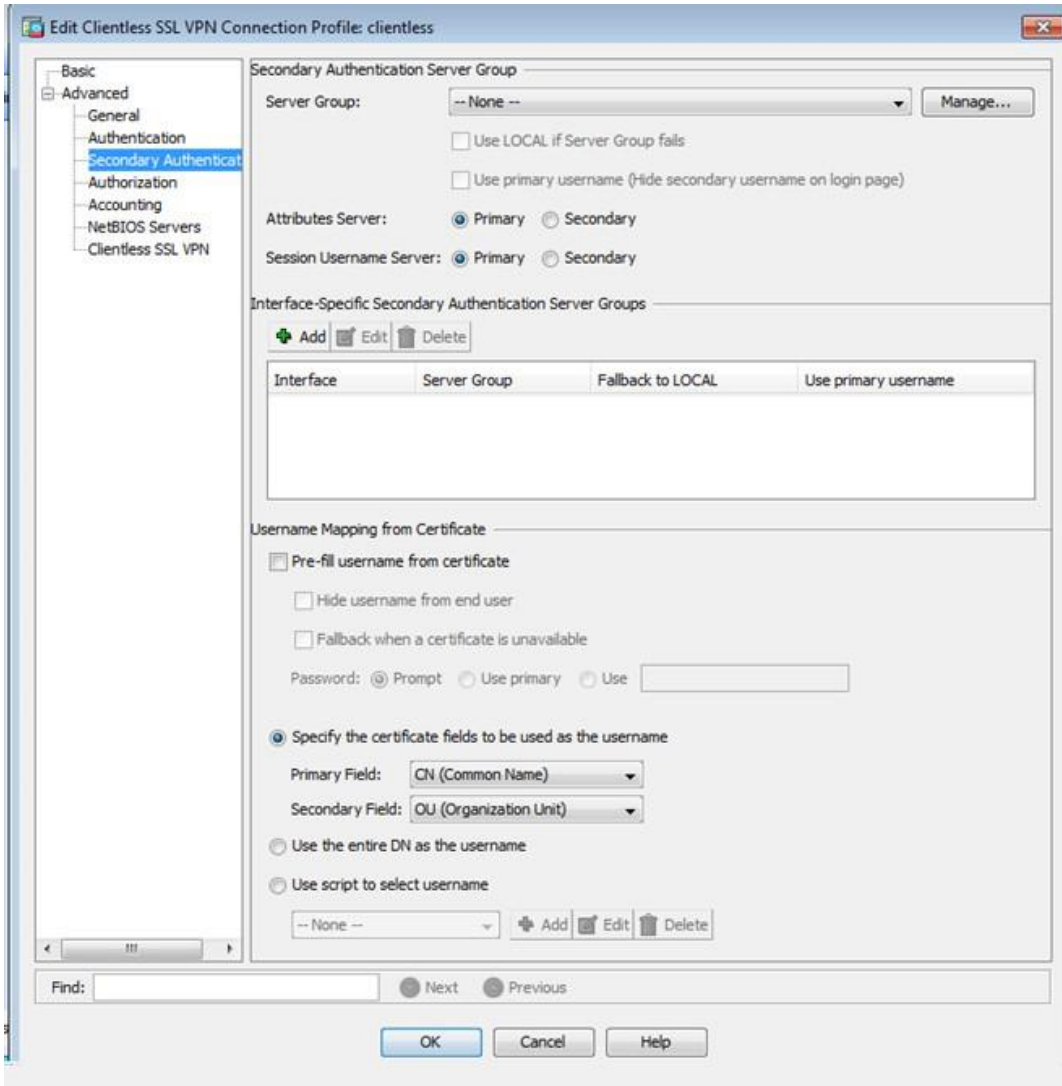
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

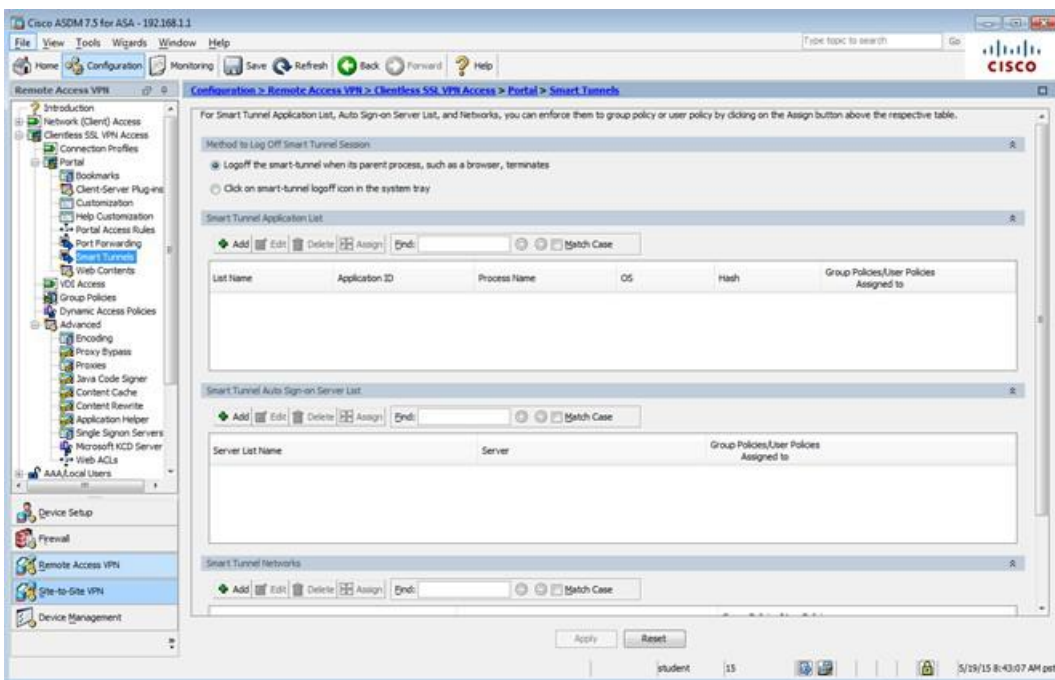
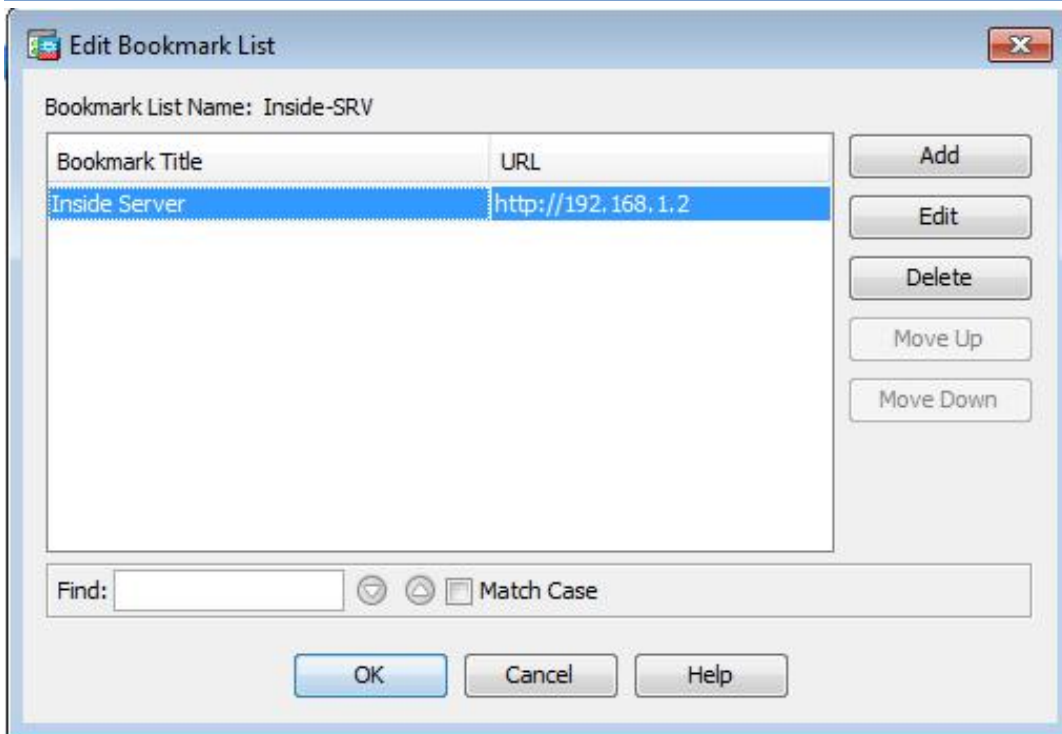
☐ Disable CSD for AnyConnect only

Find: ☐ Next ☐ Previous

OK Cancel Help







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 > Portal > Port Forwarding

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

Add Edit Delete Assign

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

Find: Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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](#).

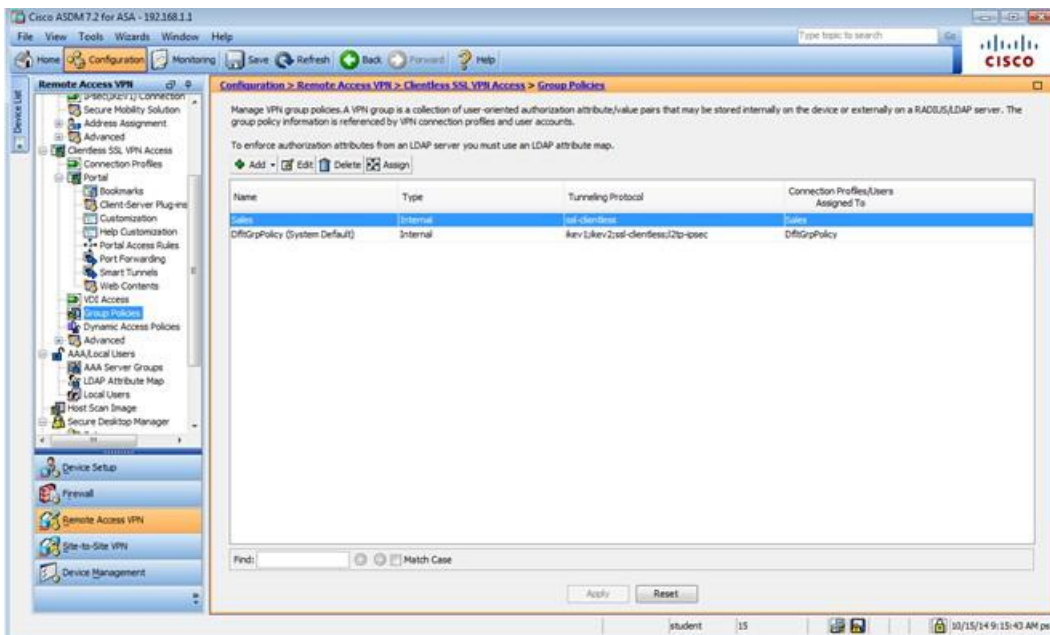
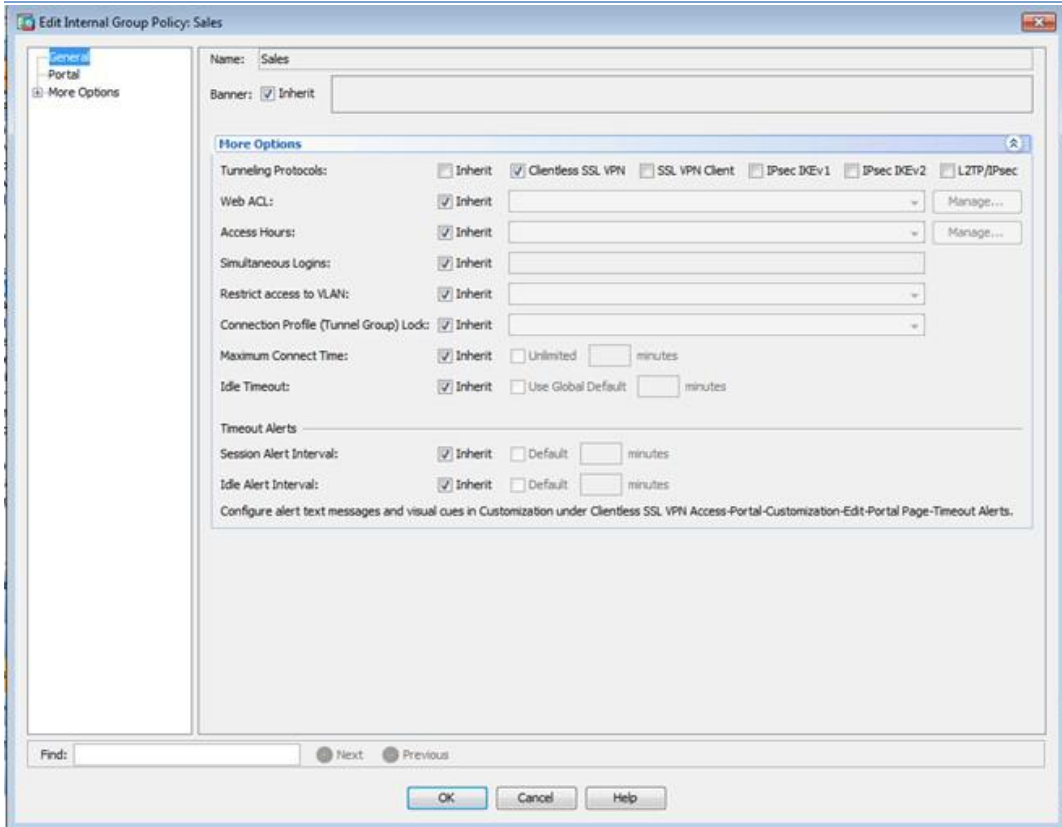
Add Edit Delete Assign

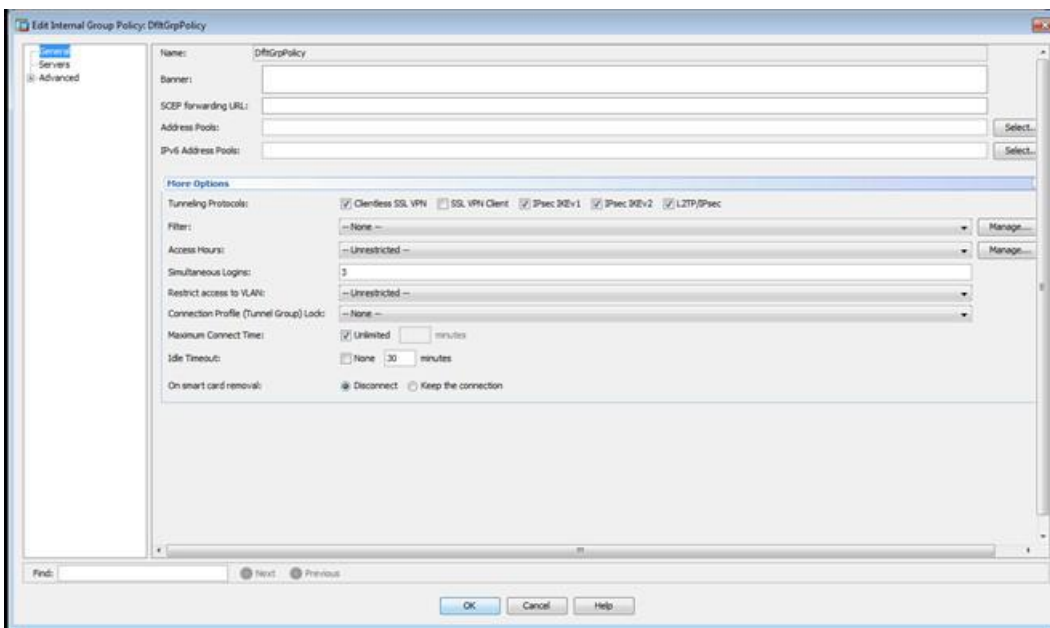
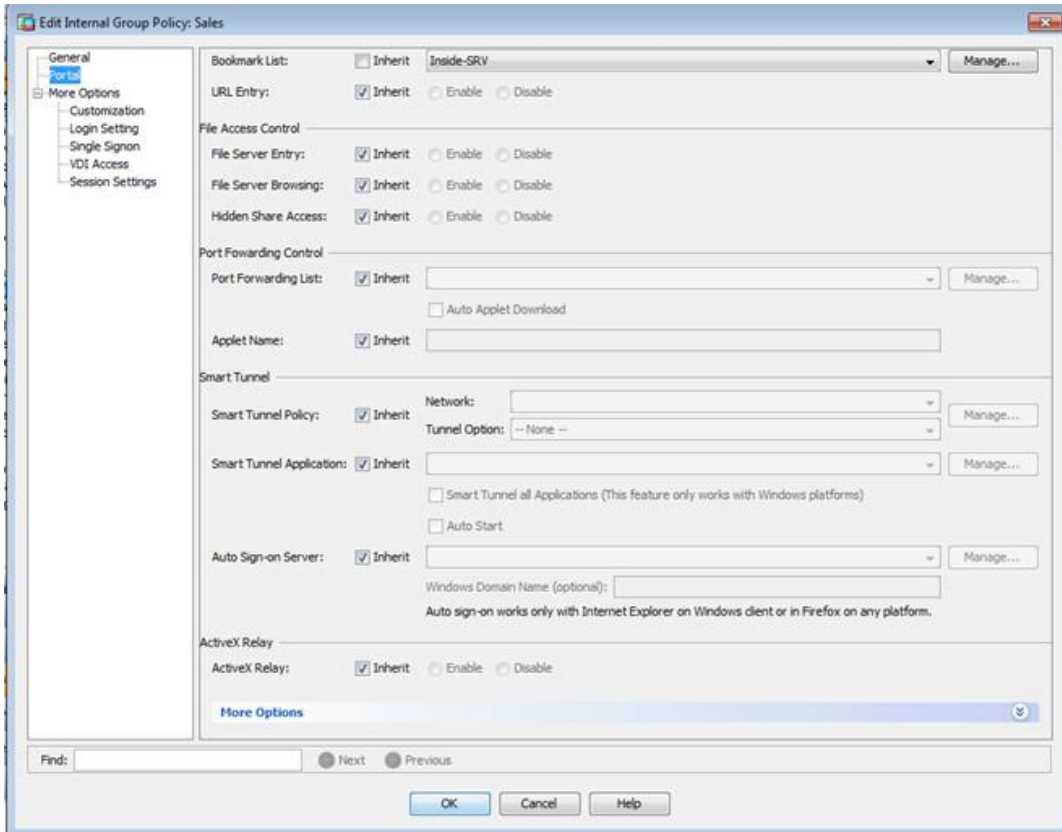
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	all-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1:rev 2:all-clientless/2to-espsec	DefaultRAGroup/DefaultIL2Group/DefaultADP2Group/Def...

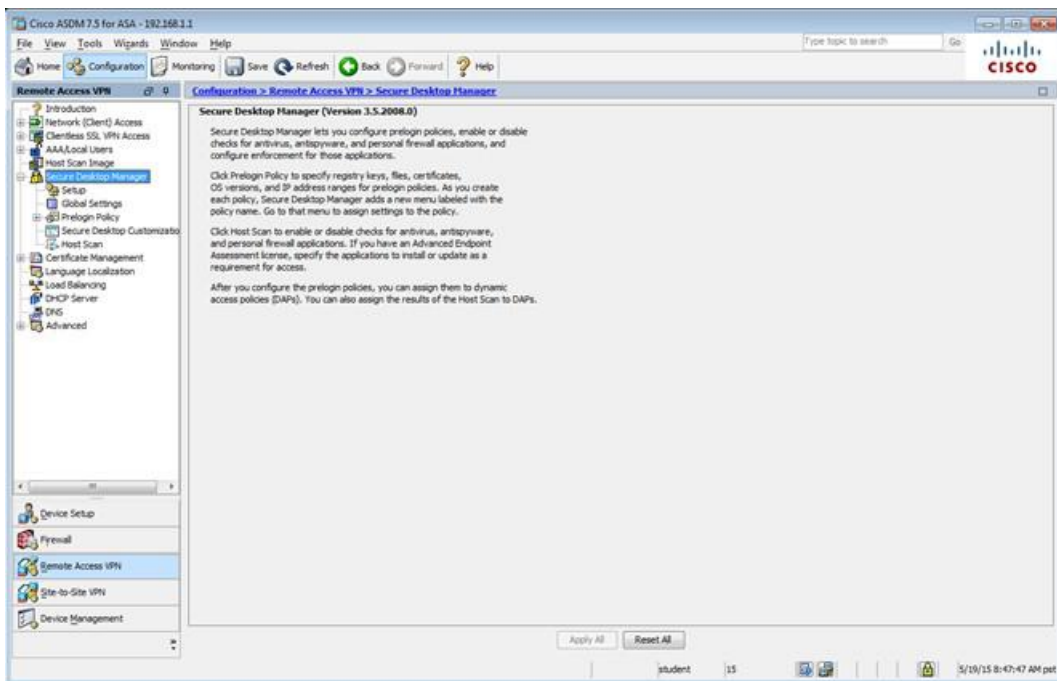
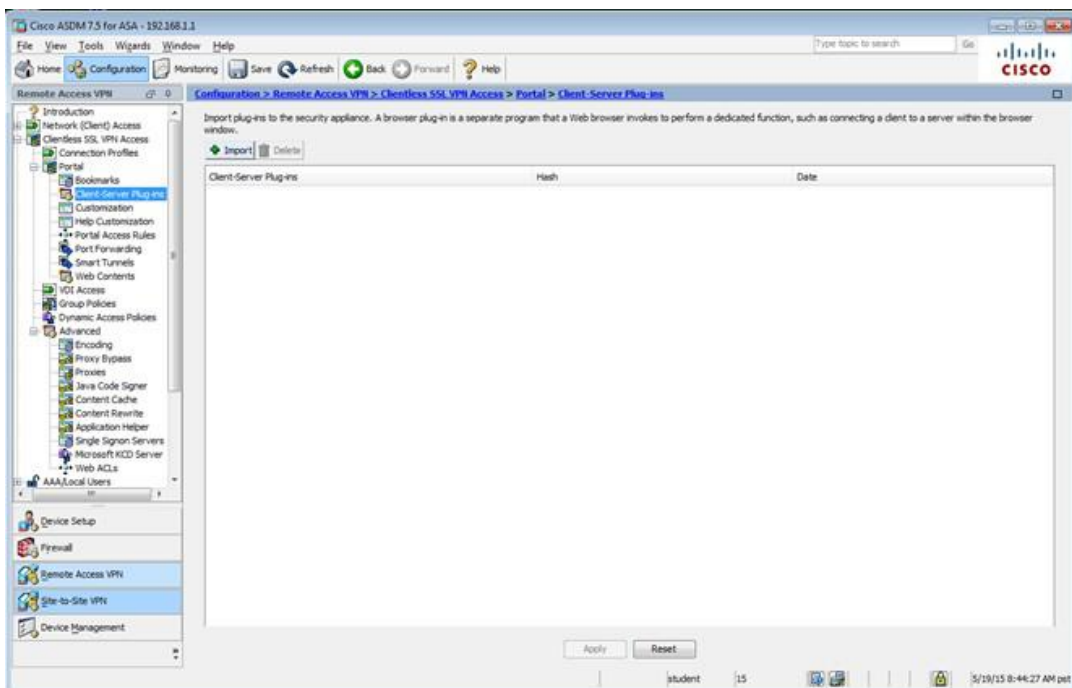
Find: Match Case

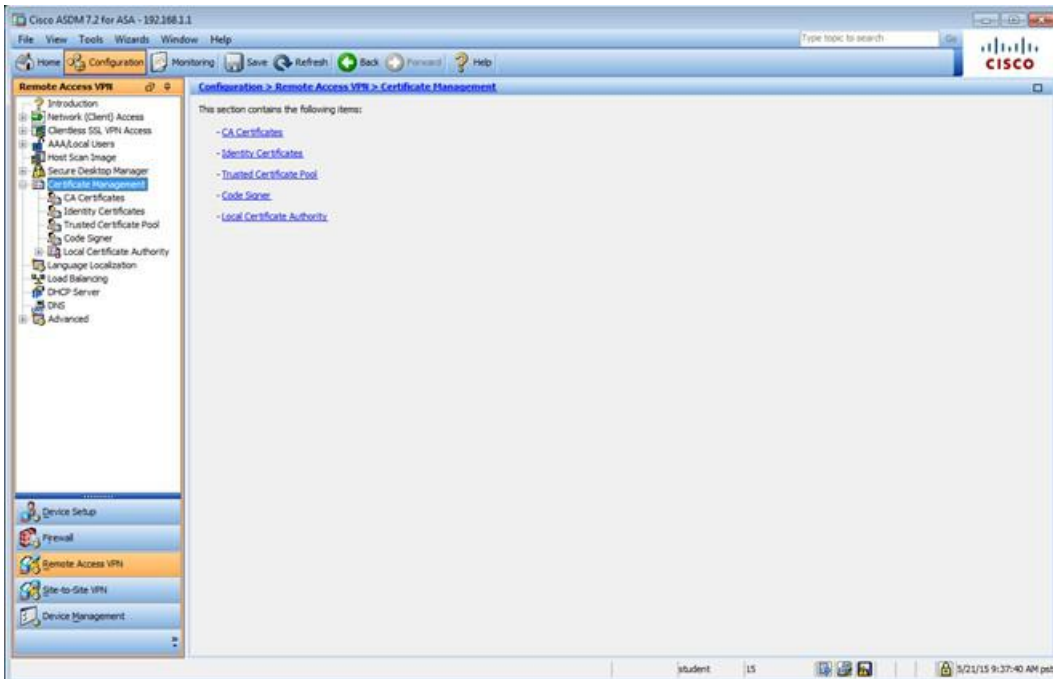
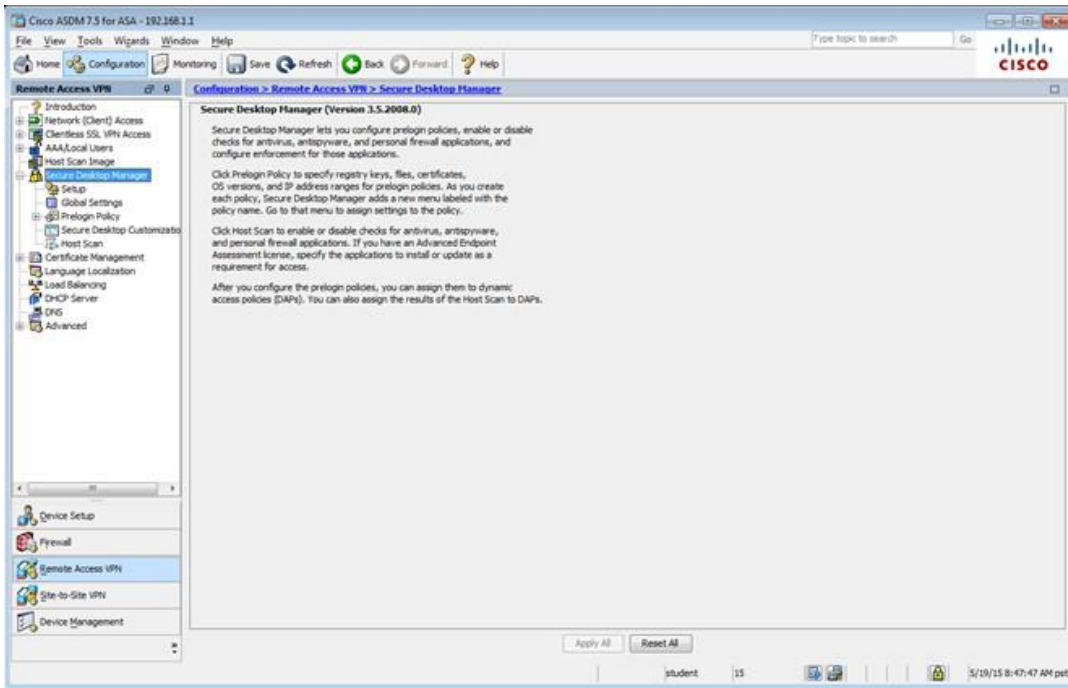
Apply Reset

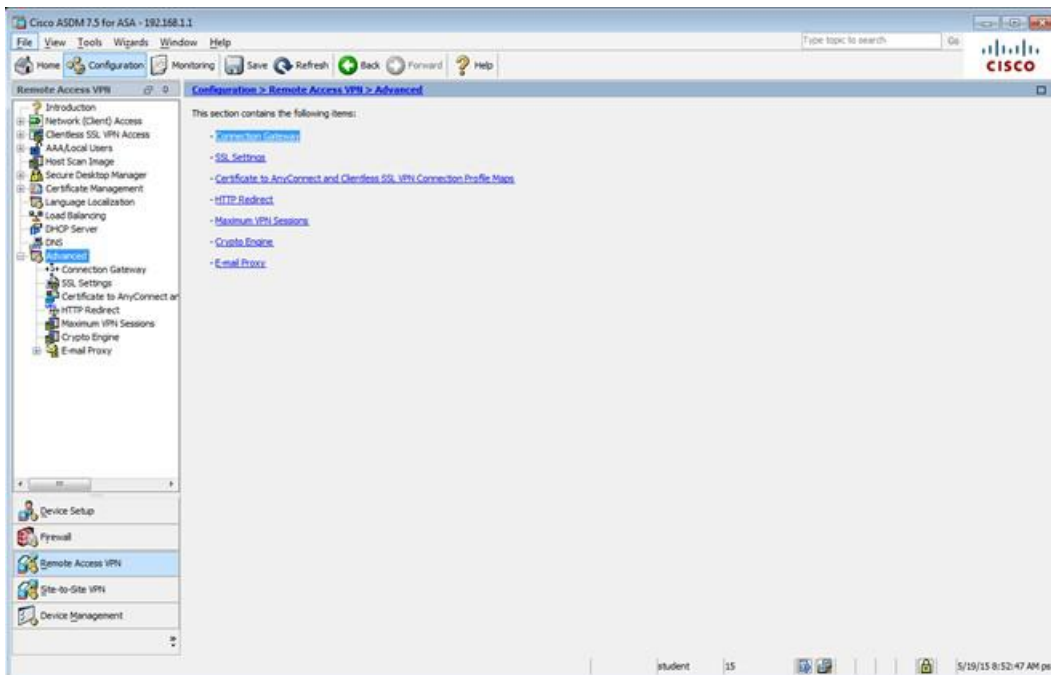
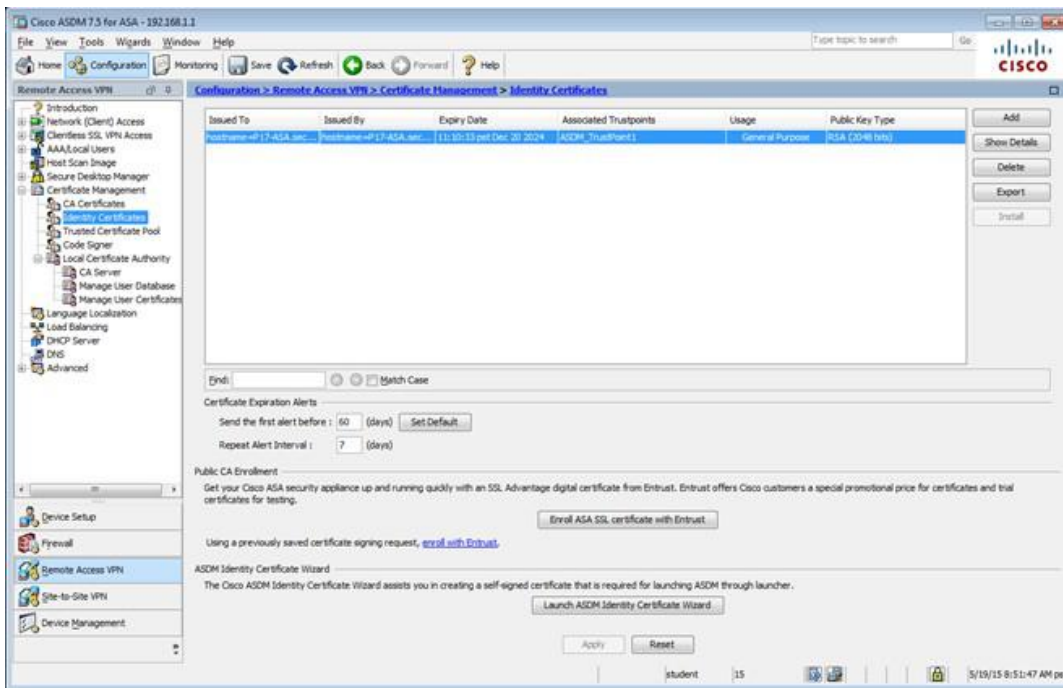
student 15 5/19/15 8:49:27 AM pst

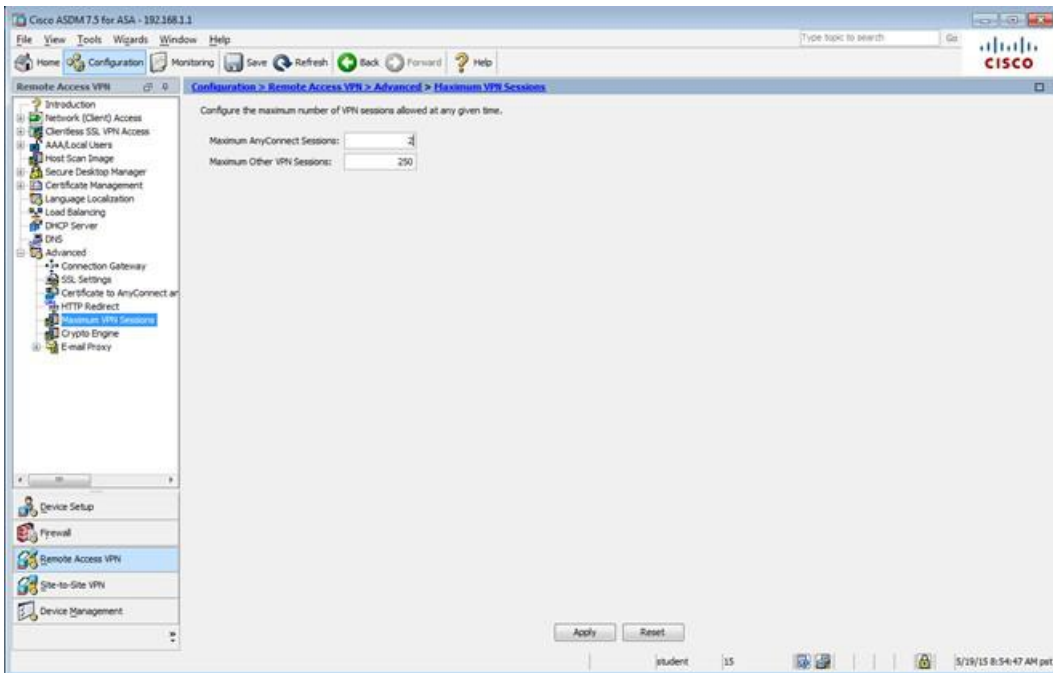
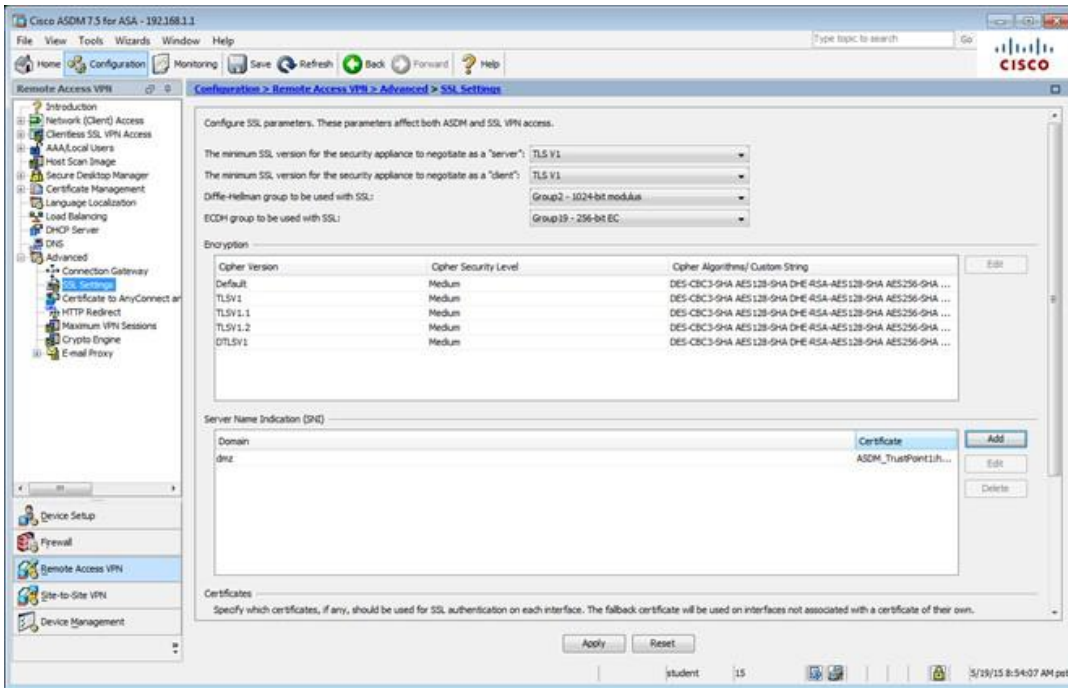












Configuration > Remote Access VPN > Network (Client) Access

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

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

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKEv2) protocols. Cisco VPN Client supports only IPsec(DKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
 You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based endpoint security policies.

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

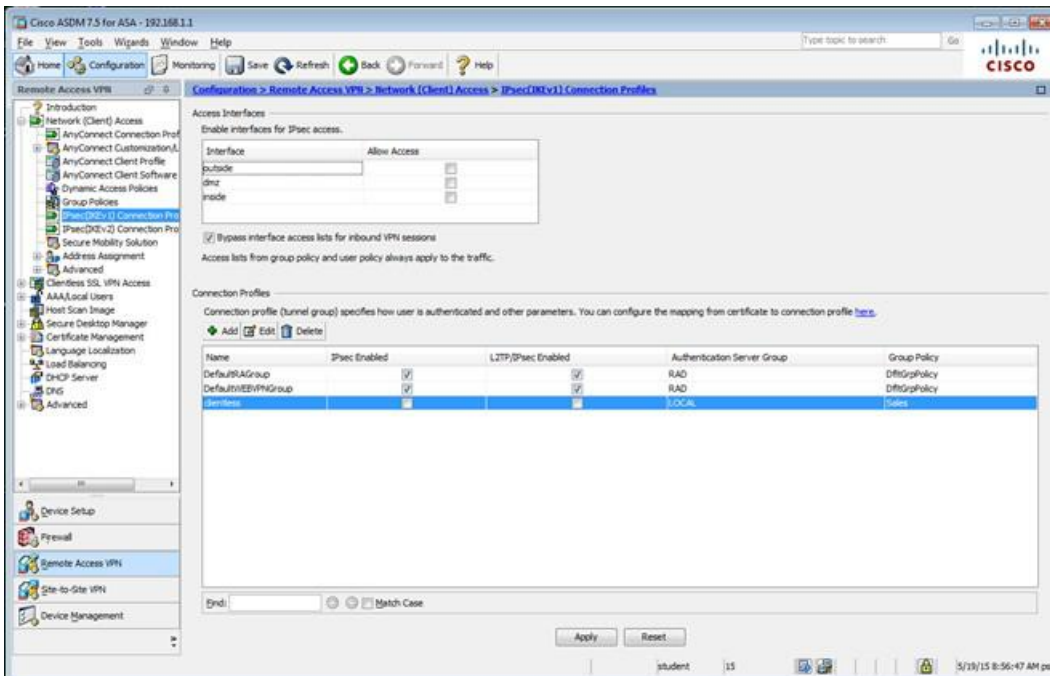
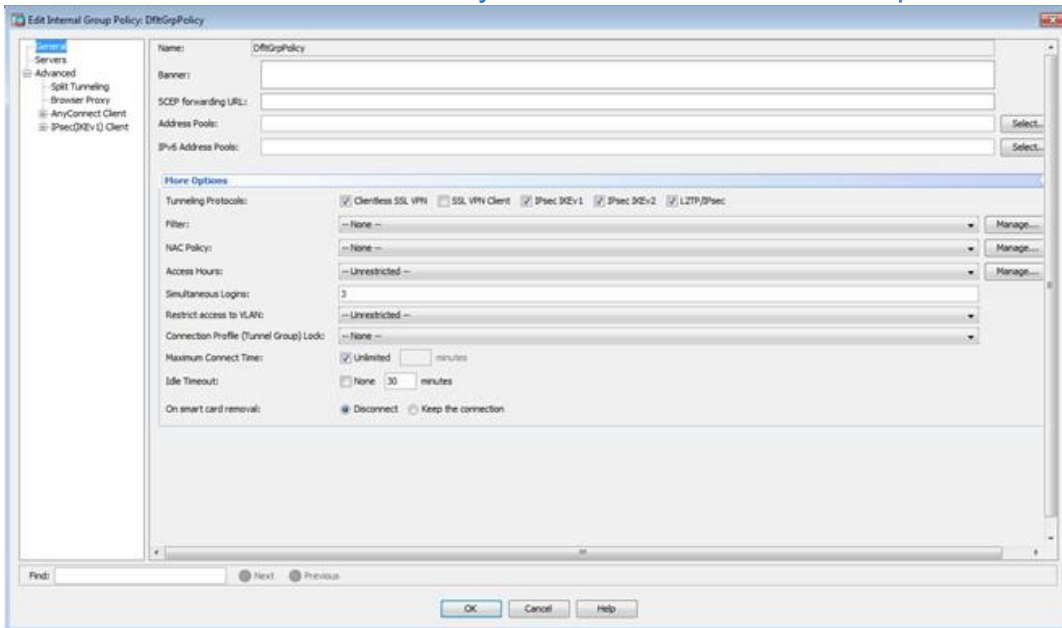
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization 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
DetrapPolicy (System Default)	Internal	ssl-clientless	DefaultGroupDefault3, GroupDefault3, PHGroup

Find: Match Case

Apply Reset



The screenshot shows the Cisco ASDM 7.5 interface for configuring AnyConnect Connection Profiles. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AnyConnect Connection Profiles' configuration page.

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

Buttons: Add, Edit, Delete, End, Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
DefaultWEBVpnGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
Clientless	<input checked="" type="checkbox"/>	<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.

Buttons: Apply, Reset

Bottom status bar: student 15 5/19/15 8:58:17 AM pst

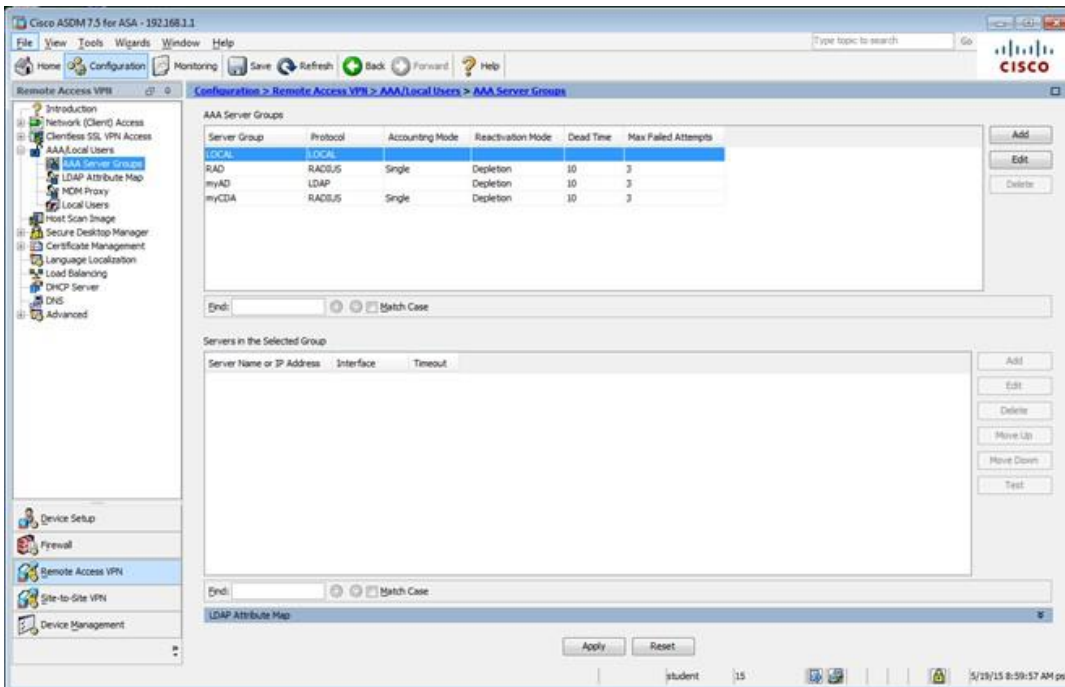
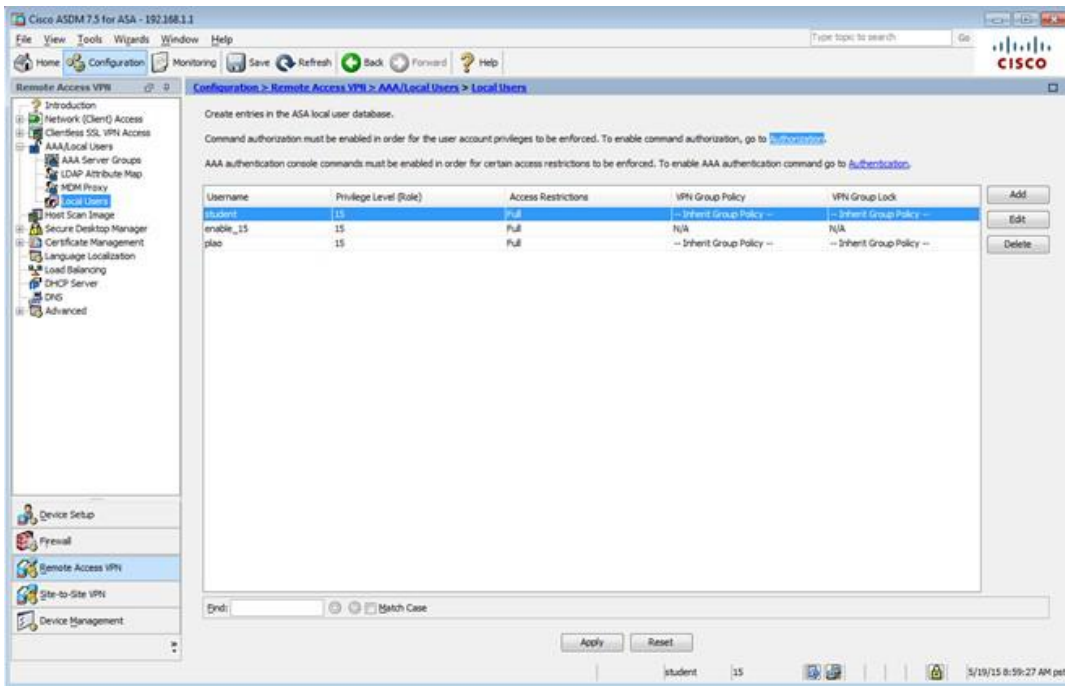
The screenshot shows the Cisco ASDM 7.5 interface for configuring AAA/Local Users. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AAA/Local Users' configuration page.

Remote Access VPN > AAA/Local Users

This section contains the following items:

- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users

Bottom status bar: student 15 5/19/15 8:58:57 AM pst



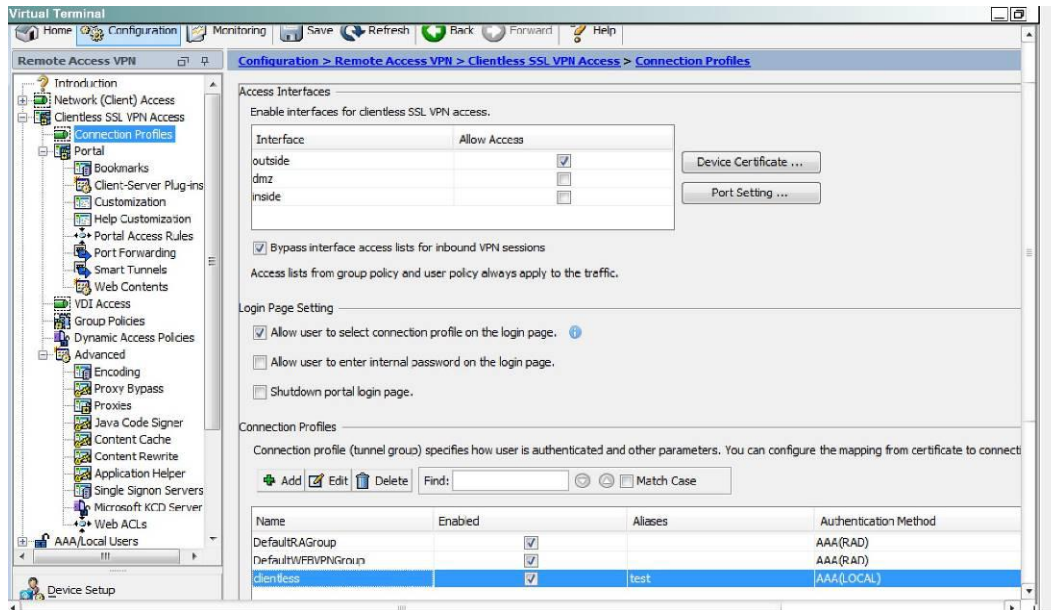
When users login to the Clientless SSLVPN using <https://209.165.201.2/test>, which group policy will be applied?

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

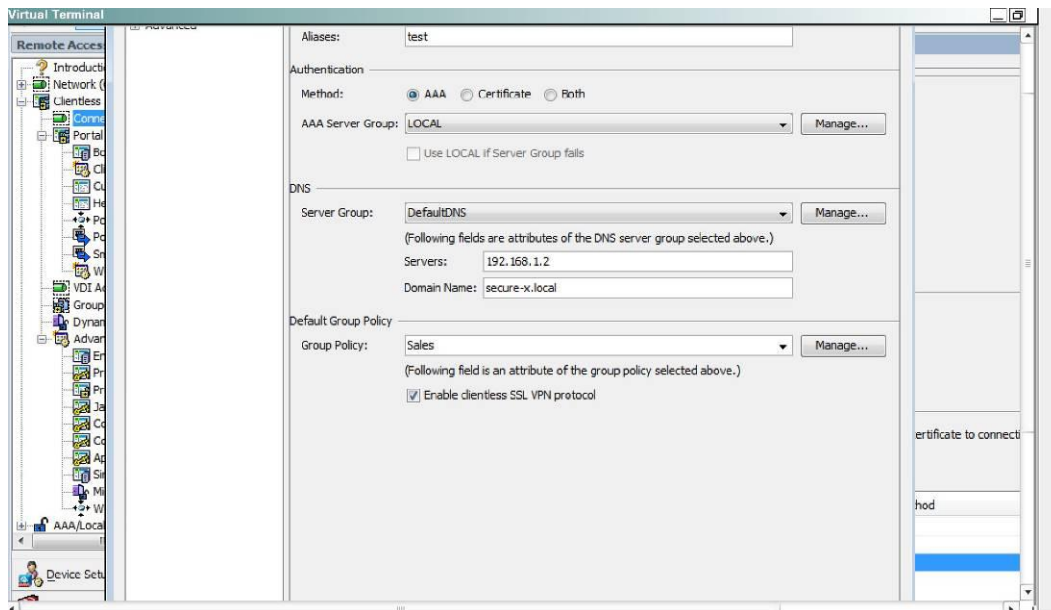
Answer: C

Explanation:

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



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



56. 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.

Answer: A

57. What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

- A. ARPs in both directions are permitted in transparent mode only.
- B. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only.
- C. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only.
- D. Only BPDUs from a higher security interface to a lower security interface are permitted in transparent mode.
- E. Only BPDUs from a higher security interface to a lower security interface are permitted in routed mode.

Answer: A

58. Which command help user1 to use enable,disable,exit&etc commands?

- A. catalyst1(config)#username user1 privilege 0 secret us1pass
- B. catalyst1(config)#username user1 privilege 1 secret us1pass
- C. catalyst1(config)#username user1 privilege 2 secret us1pass
- D. catalyst1(config)#username user1 privilege 5 secret us1pass

Answer: A



59. Which EAP method uses Protected Access Credentials?

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

Answer: A

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

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

Answer: A

61. Which IPS mode provides the maximum number of actions?

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

Answer: A

62. If a switch port goes into a blocked state only when a superior BPDU is received, what mechanism must be in use?

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

Answer: A



Explanation: Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

Source: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>

63. 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.

Answer: A

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

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

Answer: C

65. How can FirePOWER block malicious email attachments?

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

Answer: C

66. 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

Answer: A

67. Which type of PVLAN port allows a host in the same VLAN to communicate only with promiscuous hosts?

- A. Community host in the PVLAN
- B. Isolated host in the PVLAN
- C. Promiscuous host in the PVLAN
- D. Span for host in the PVLAN

Answer: B

68. 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.

Answer: A

69. 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.



Answer: A

70. Which filter uses in Web reputation to prevent from Web Based Attacks? (Choose two)

- A. outbreak filter
- B. buffer overflow filter
- C. bayesian overflow filter
- D. web reputation
- E. exploit filtering

Answer: A,D

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

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

Answer: A,C

72. Which option is a characteristic of the RADIUS protocol?

- A. uses TCP
- B. offers multiprotocol support
- C. combines authentication and authorization in one process
- D. supports bi-directional challenge

Answer: C

Explanation:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions

that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

73. On which Cisco Configuration Professional screen do you enable AAA

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

Answer: A

74. How can you protect CDP from reconnaissance attacks?

- A. Enable dot1x on all ports that are connected to other switches.
- B. Disable CP on ports connected to endpoints.
- C. Enable dynamic ARP inspection on all untrusted ports.
- D. Disable CDP on trunk ports.

Answer: B

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

- A. advanced persistent threat
- B. targeted malware
- C. drive-by spyware



D. social activism

Answer: A

76. 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.

Answer: A

77. What feature defines a campus area network?

- A. It has a single geographic location.
- B. It has limited or restricted Internet access.
- C. It has a limited number of segments.
- D. it lacks external connectivity.

Answer: A

78. What is the highest security level that can be configured for an interface on an ASA?

- A. 0
- B. 50
- C. 100
- D. 200

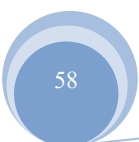
Answer: C

Explanation:

🔗 Security level 100: This is the highest security level on our ASA and by default this is assigned to the “inside” interface. Normally we use this for our “LAN”. Since this is the highest security level, by default it can reach all the other interfaces.

<https://networklessons.com/cisco/asa-firewall/cisco-asa-security-levels/>

79. What are two options for running Cisco SDM? (Choose two)





- A. Running SDM from a mobile device.
- B. Running SDM from a router's flash.
- C. Running SDM from a PC
- D. Running SDM from within CiscoWorks
- E. Running SDM from the Cisco web portal.

Answer: C,E

80. 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.

Answer: A,E

81. 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

Answer: D,E,F

82. Which label is given to a person who uses existing computer scripts to hack into computers lacking the expertise to write their own?

- A. white hat hacker
- B. hacktivist
- C. phreaker
- D. script kiddy



Answer: D

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

- A. dynamic nat with shortest prefix
- B. dynamic nat with longest prefix
- C. static nat with shortest prefix
- D. static nat with longest prefix

Answer: D

84. Which two characteristics apply to an Intrusion Prevention System (IPS) ? Choose two

- A. Does not add delay to the original traffic.
- B. Cabled directly inline with the flow of the network traffic.
- C. Can drop traffic based on a set of rules.
- D. Runs in promiscuous mode.
- E. Cannot drop the packet on its own

Answer: B,C

Explanation: + Position in the network flow: Directly inline with the flow of network traffic and every packet goes through the sensor on its way through the network.

+ Mode: Inline mode

+ The IPS can drop the packet on its own because it is inline. The IPS can also request assistance from another device to block future packets just as the IDS does.

Source: Cisco Official Certification Guide, Table 17-2 IDS Versus IPS, p.461

85. Which protocol provides security to Secure Copy?

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

Answer: B

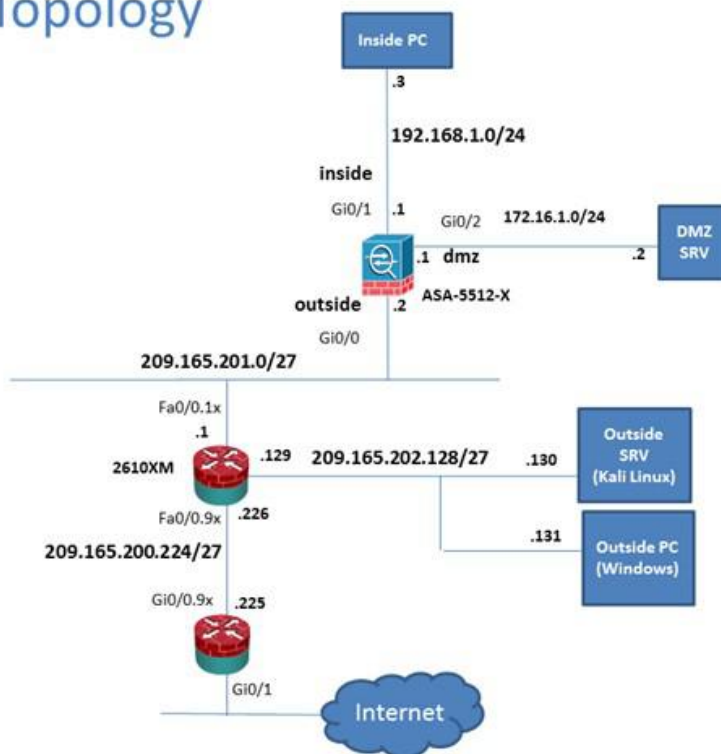
86. Scenario

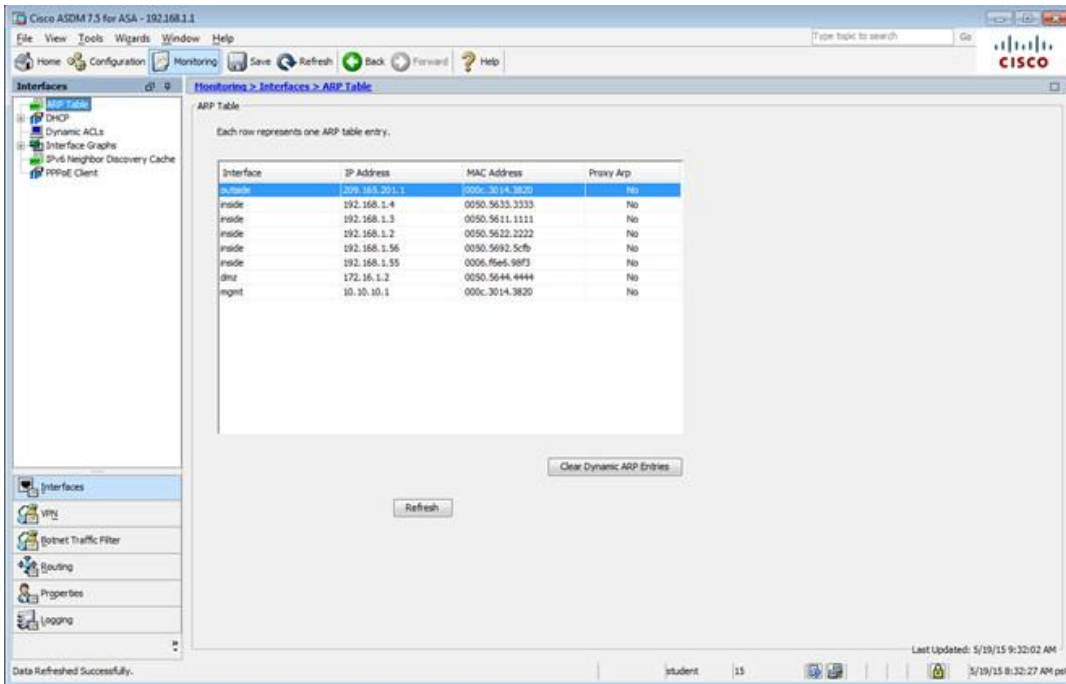
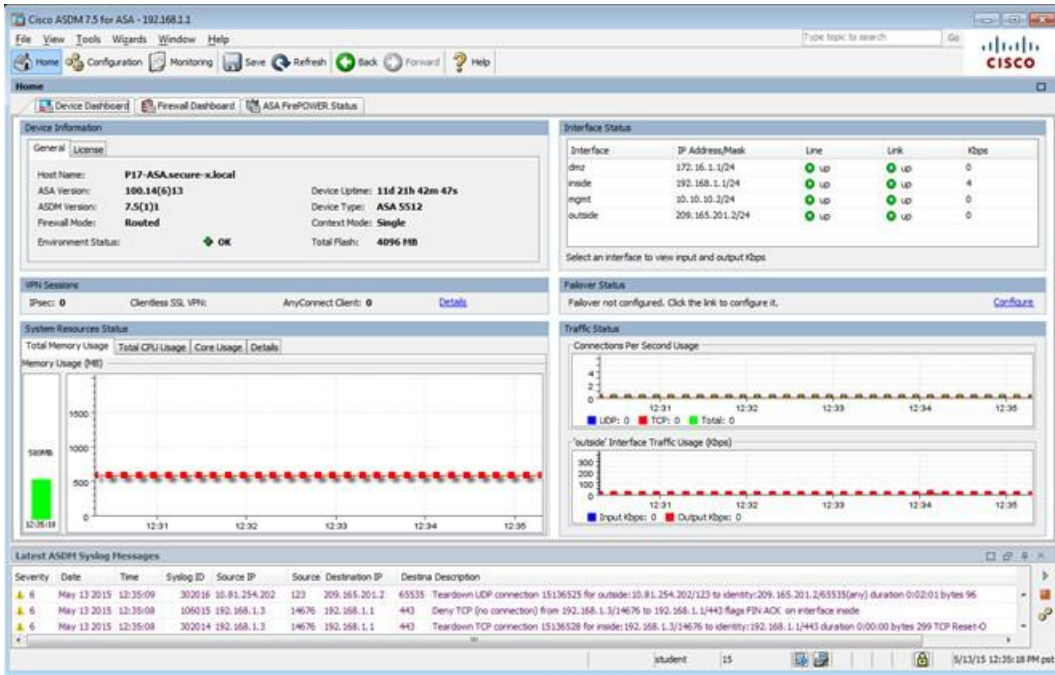
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

VPN Statistics

VPN Statistics

- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IPsec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WPA Sessions

Interfaces

VPN

Internet Traffic Filter

Routing

Properties

Logging

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	Group Policy	Protocol	Login Time	Bytes Tx	Bytes Rx
student	student	Clientless	08:05:46 pm Thu May 21 2015	316774	41633
259.165.202.131	Clientless	Clientless (IPsec)	08:05:46 pm		

Refresh

Last Updated: 5/26/15 9:33:12 AM

Data Refreshed Successfully.

student 15

5/26/15 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 > Startup Wizard

Click the "Launch Startup Wizard" button to start the wizard.

Startup Wizard

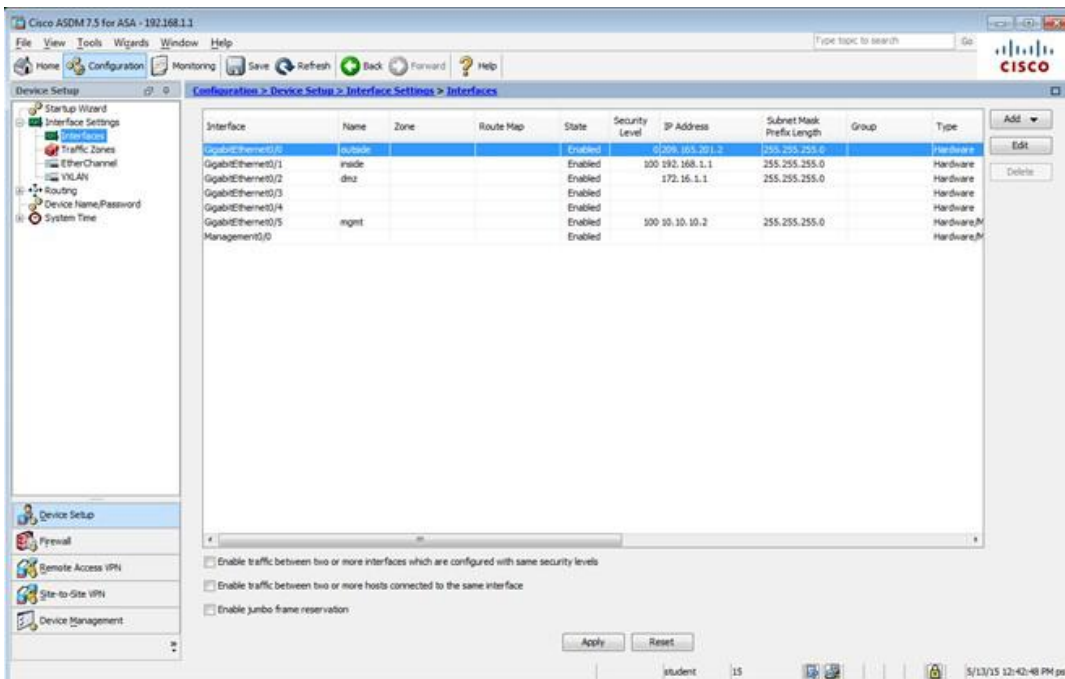
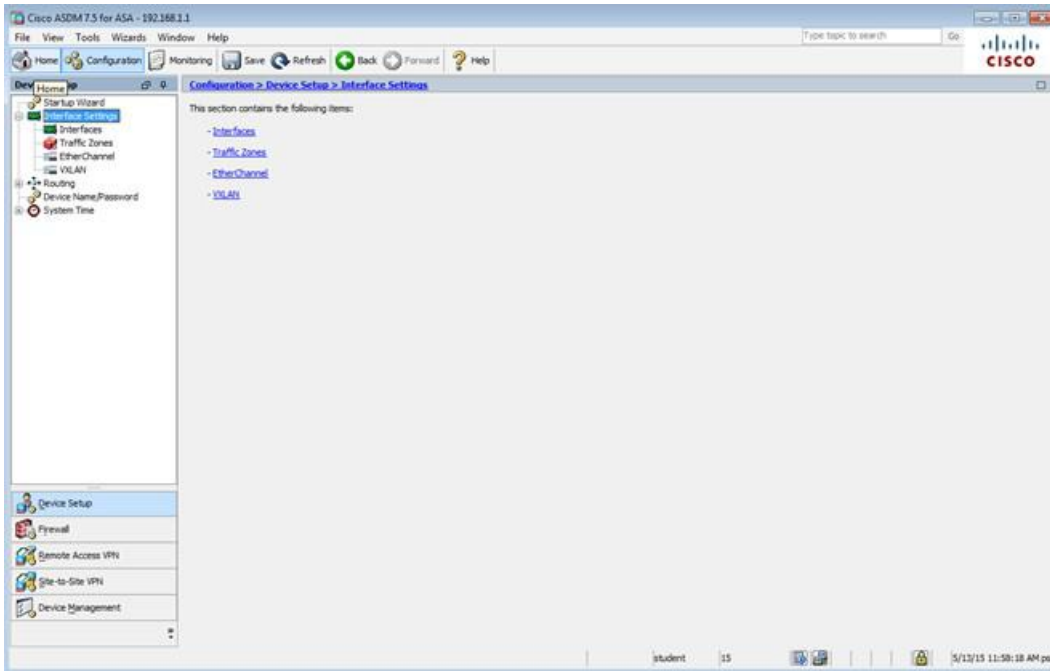
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

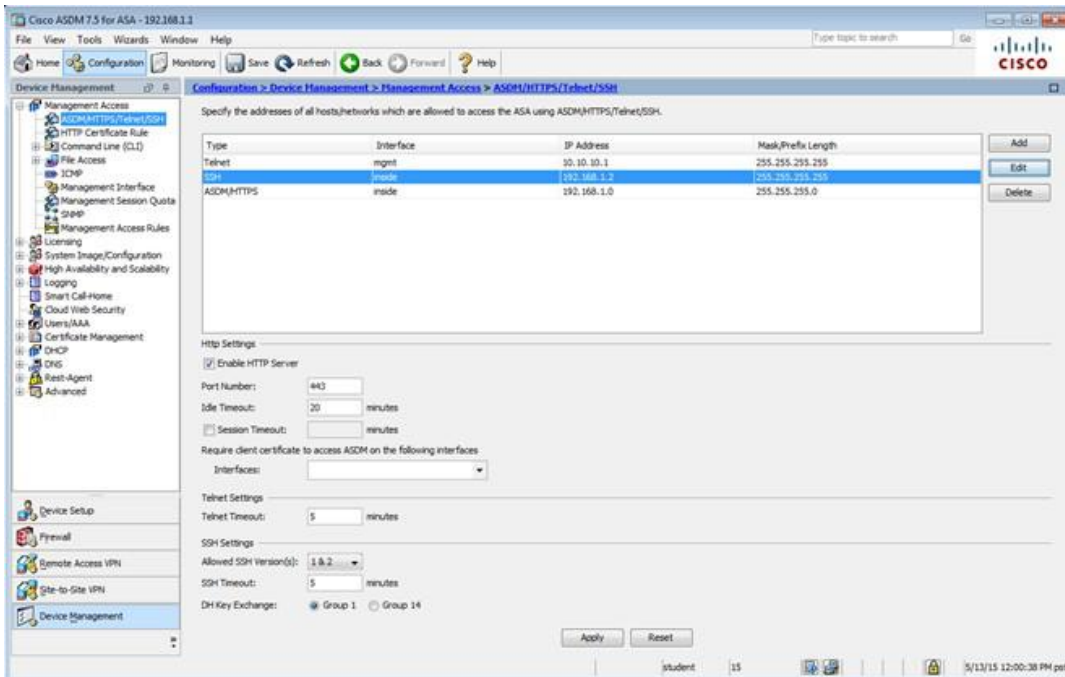
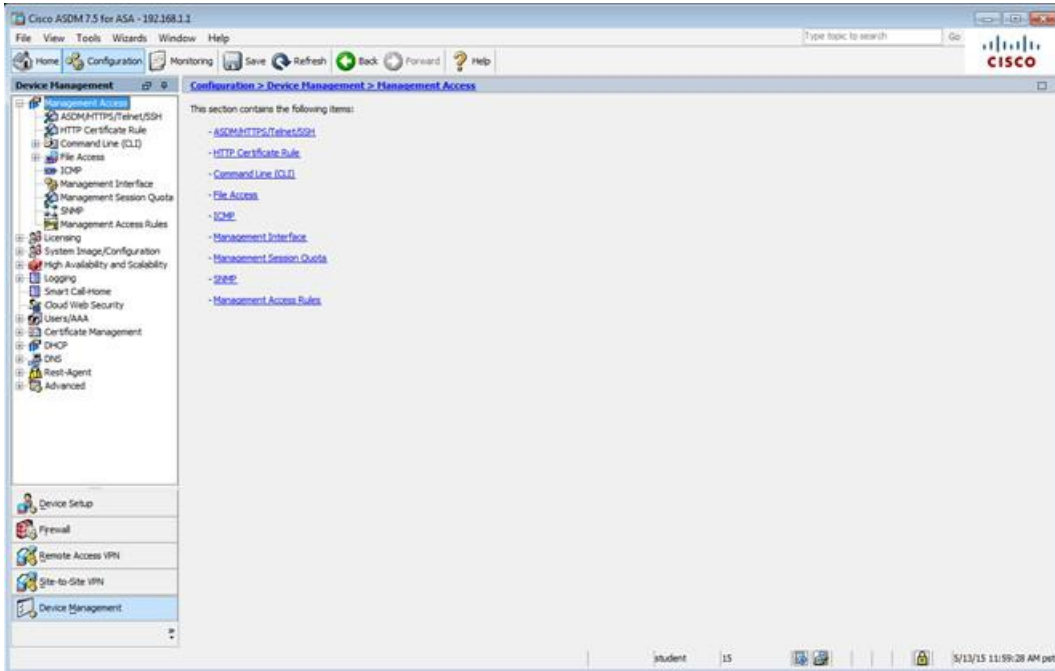
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

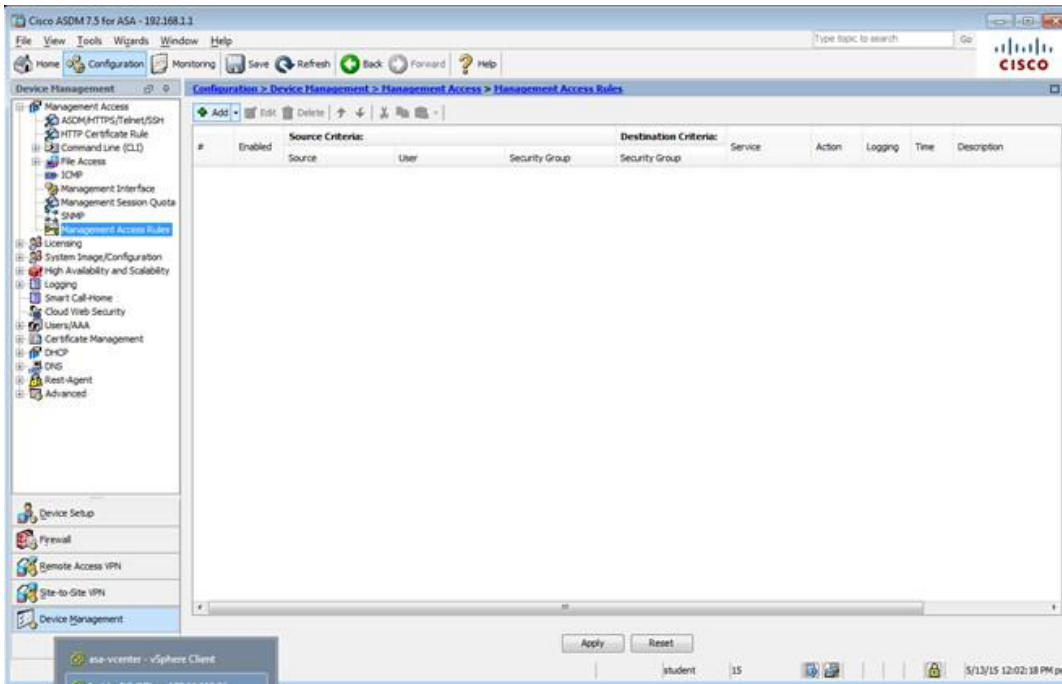
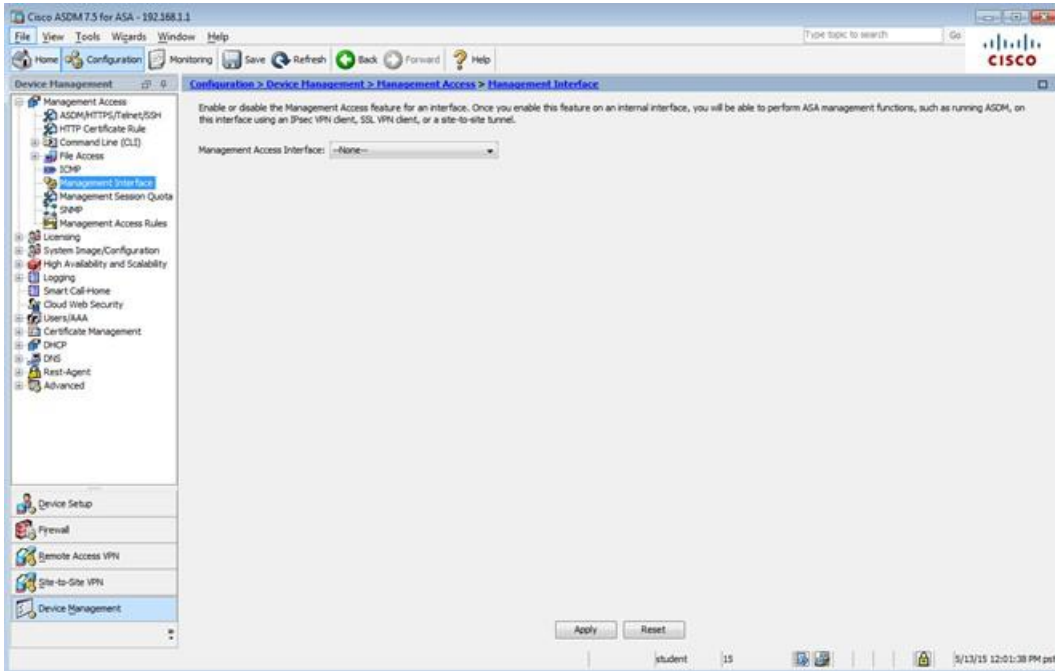
Launch Startup Wizard

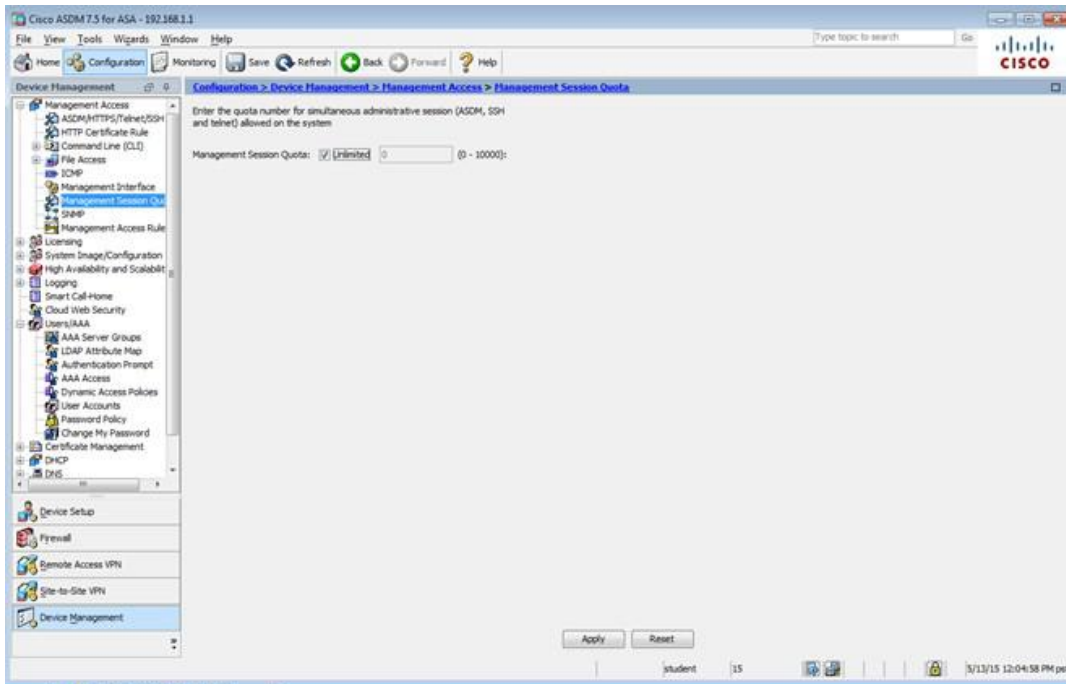
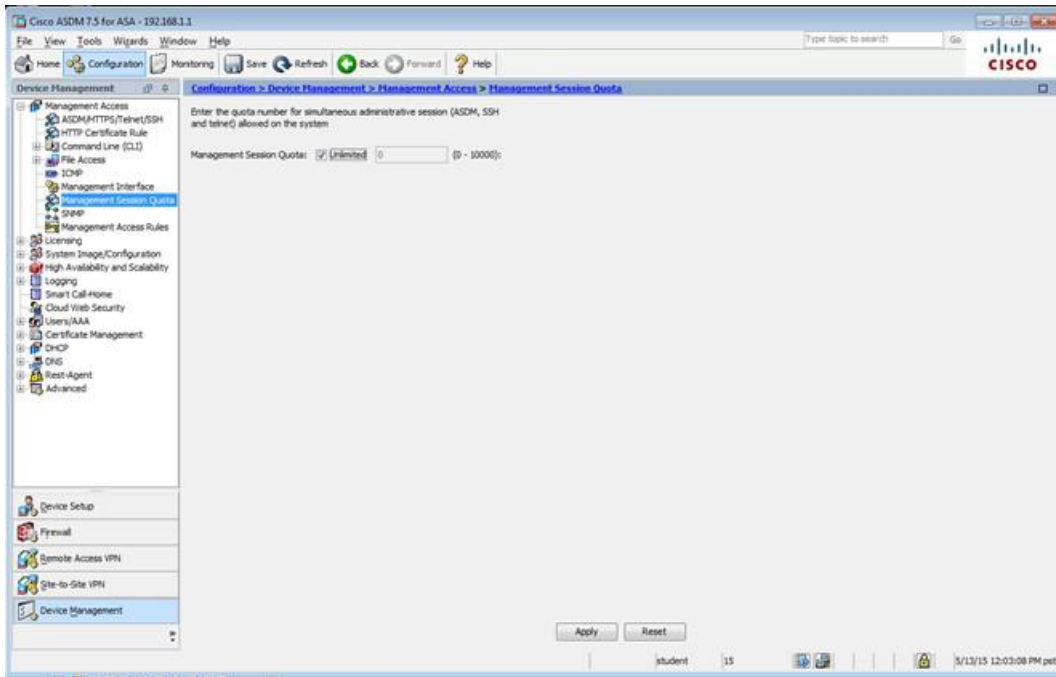
student 15

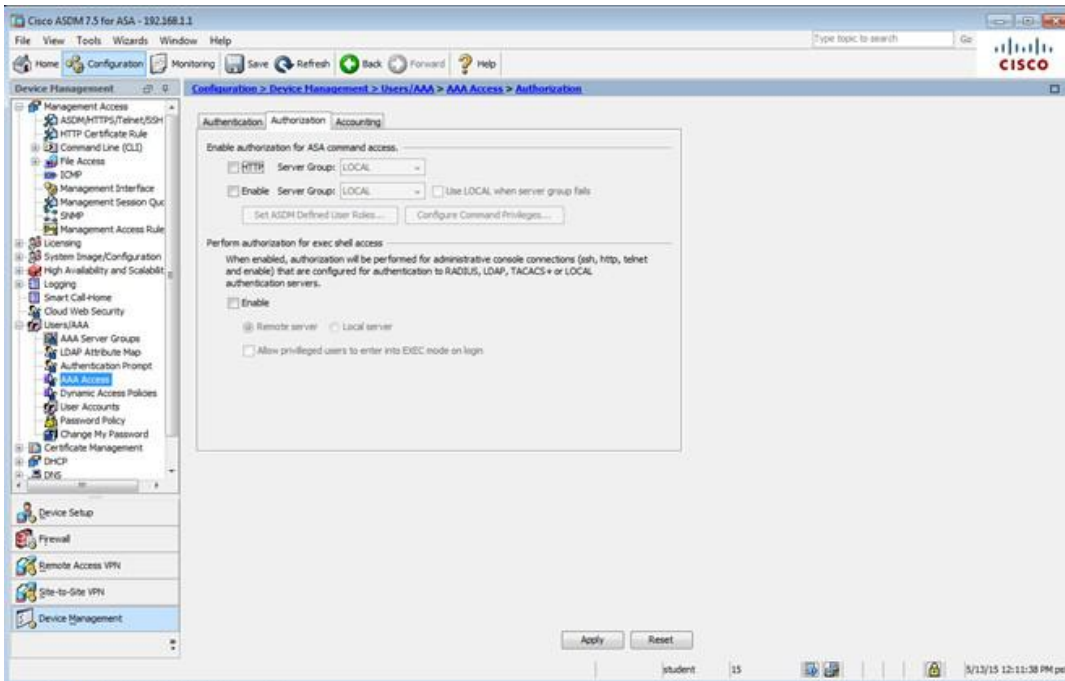
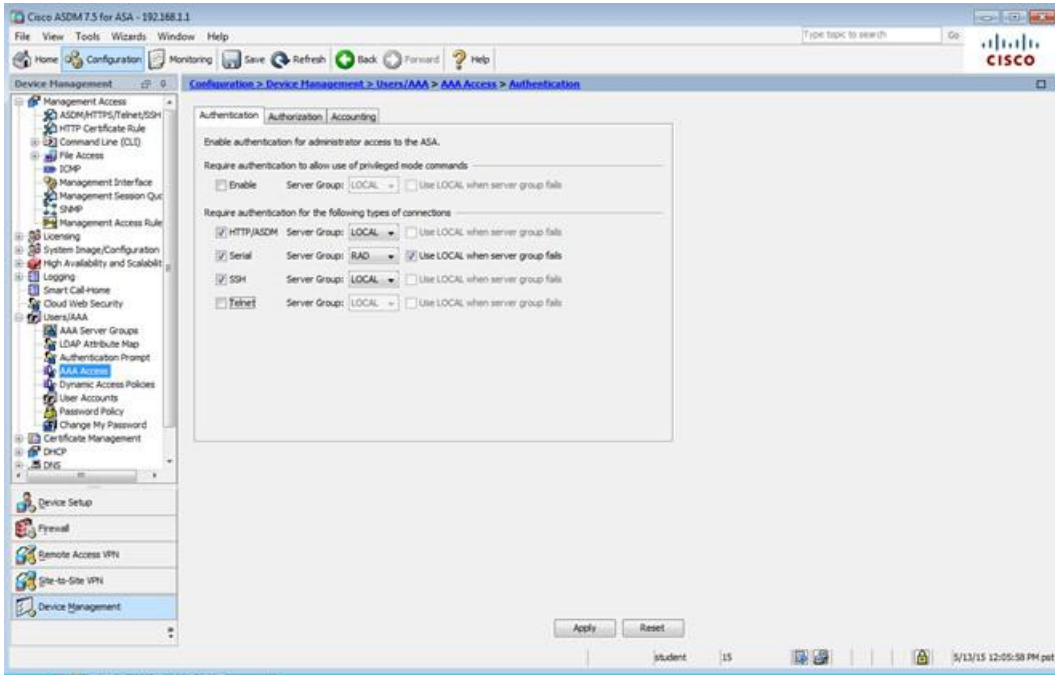
5/26/15 11:56:08 AM pst

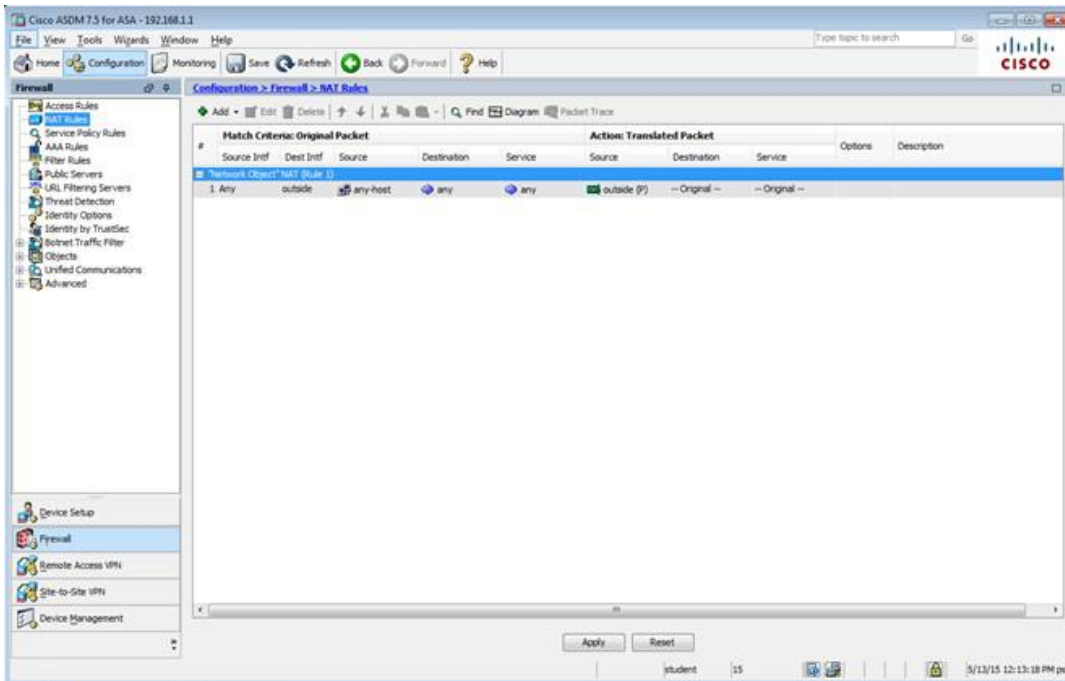
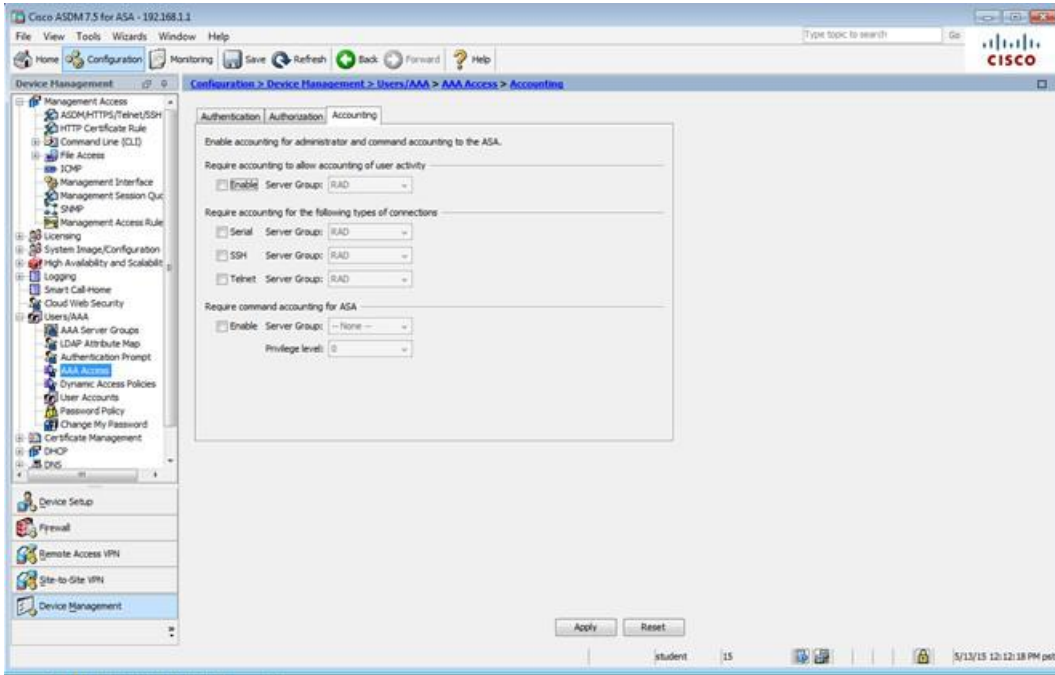


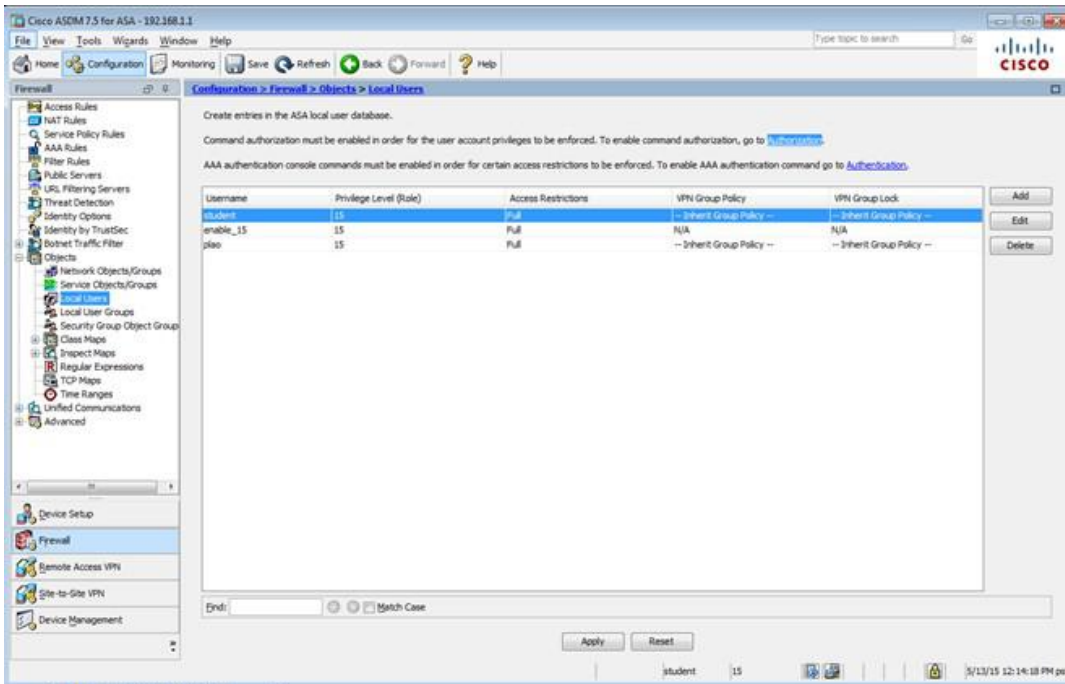
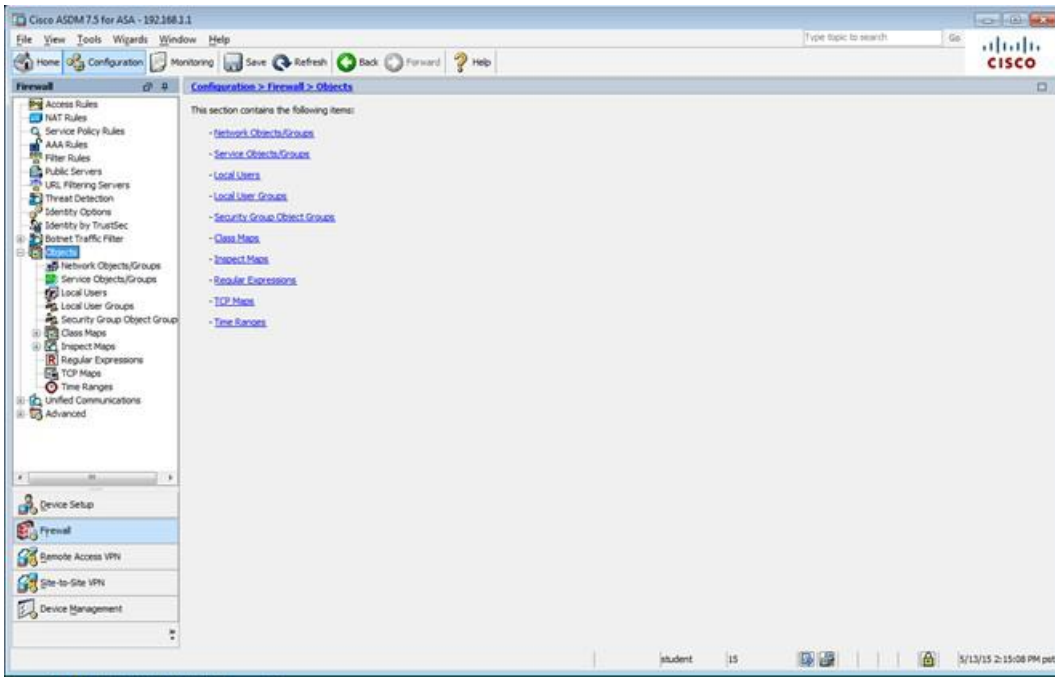


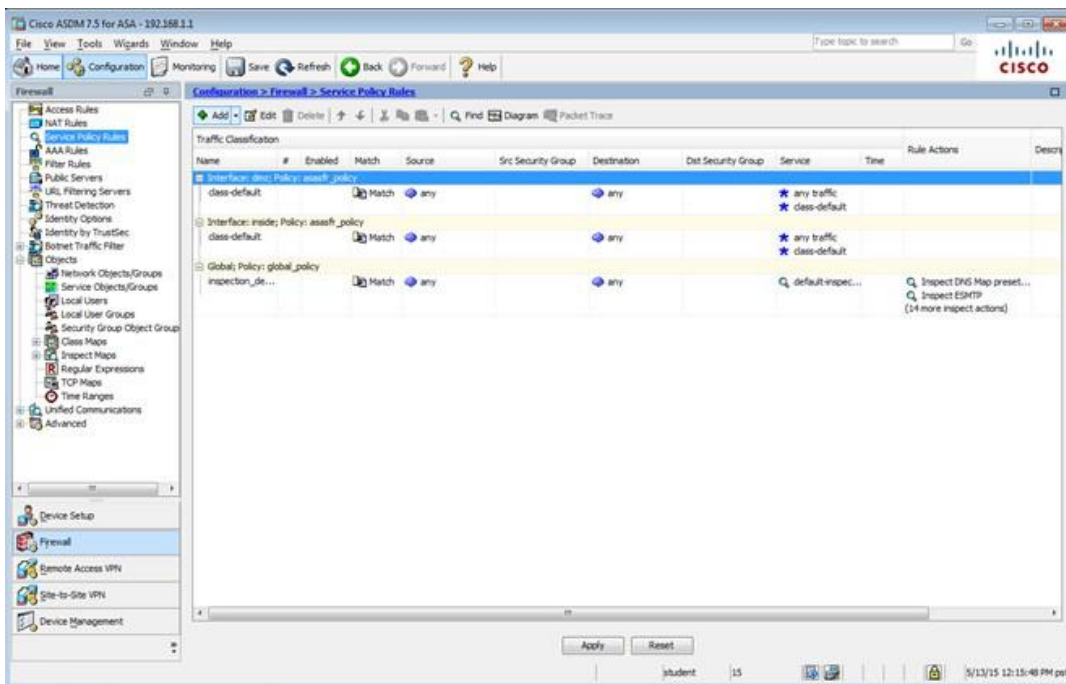
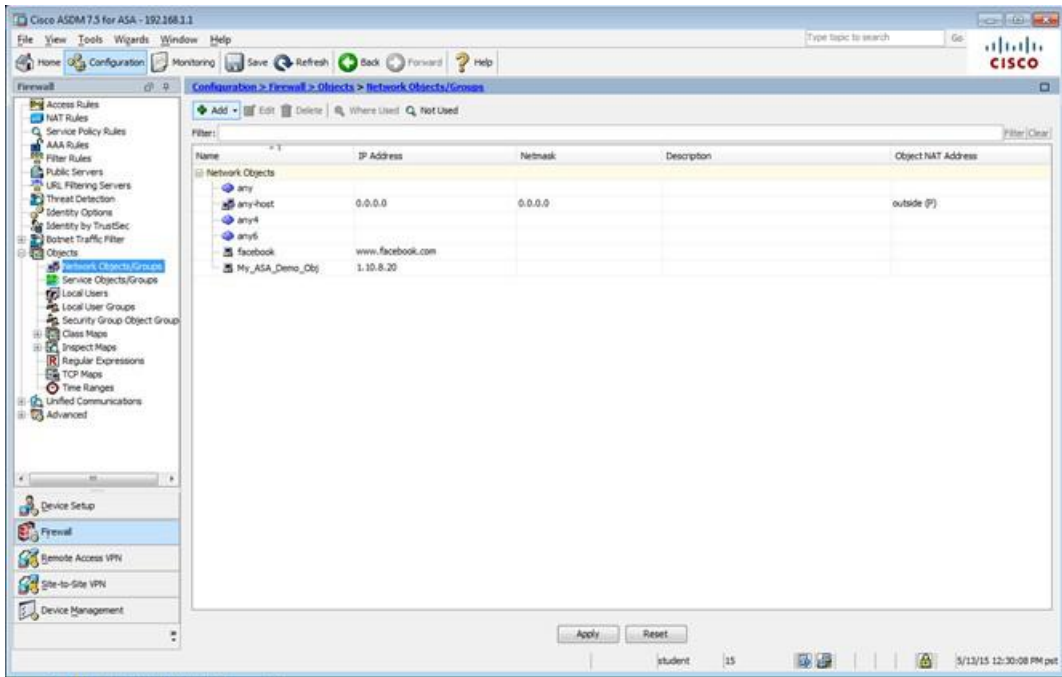


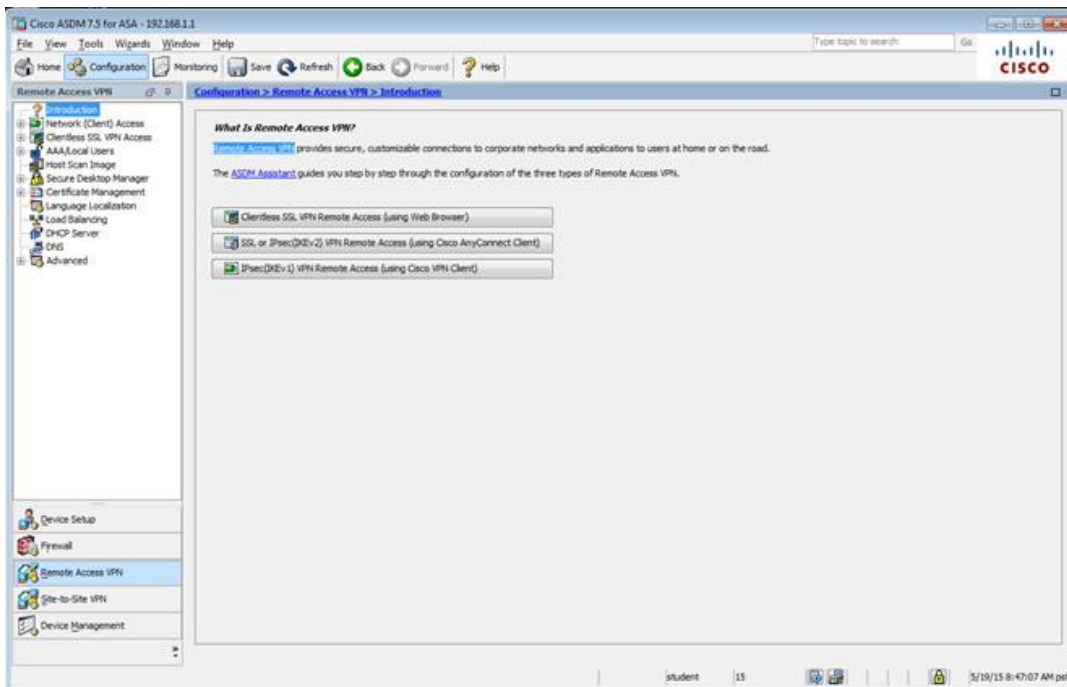
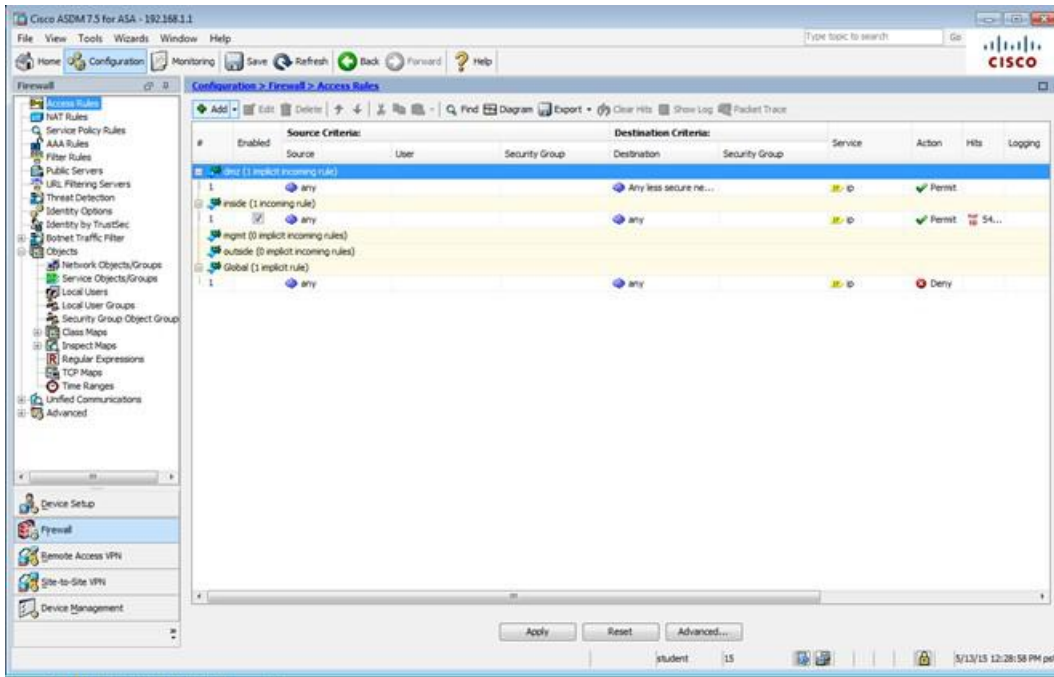


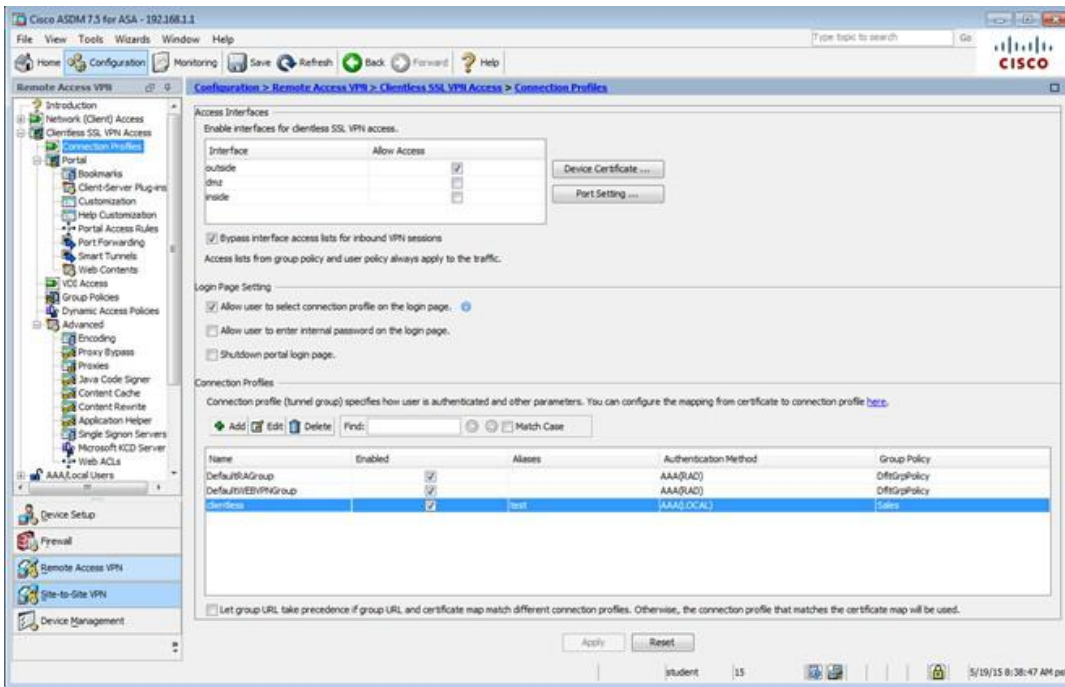
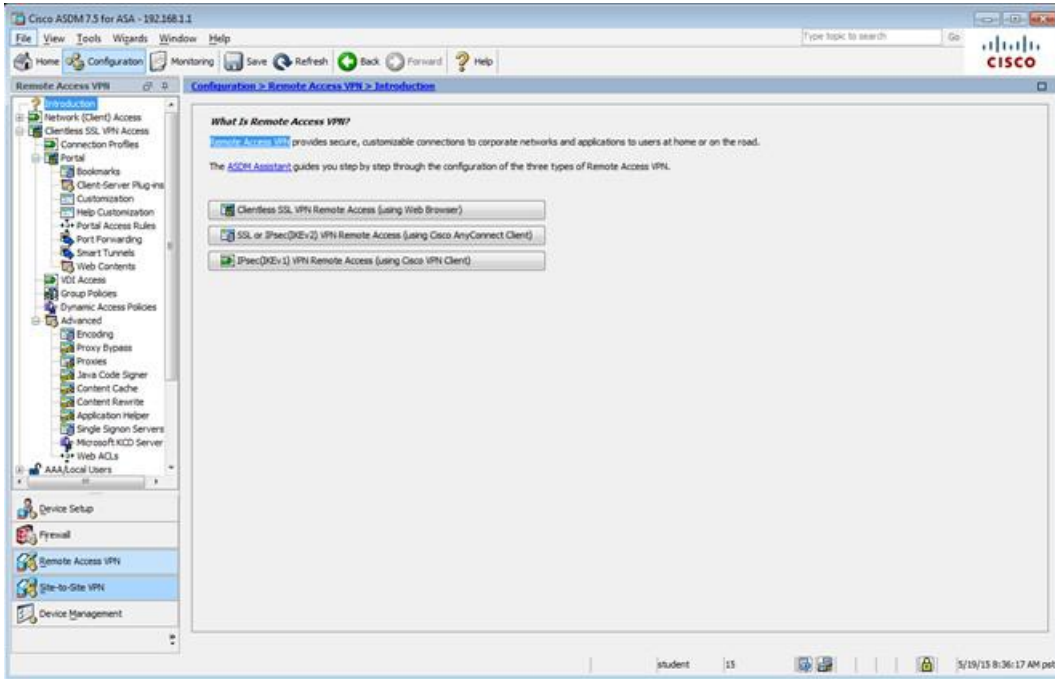












Edit Clientless SSL VPN Connection Profile: clientless

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 choose 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)

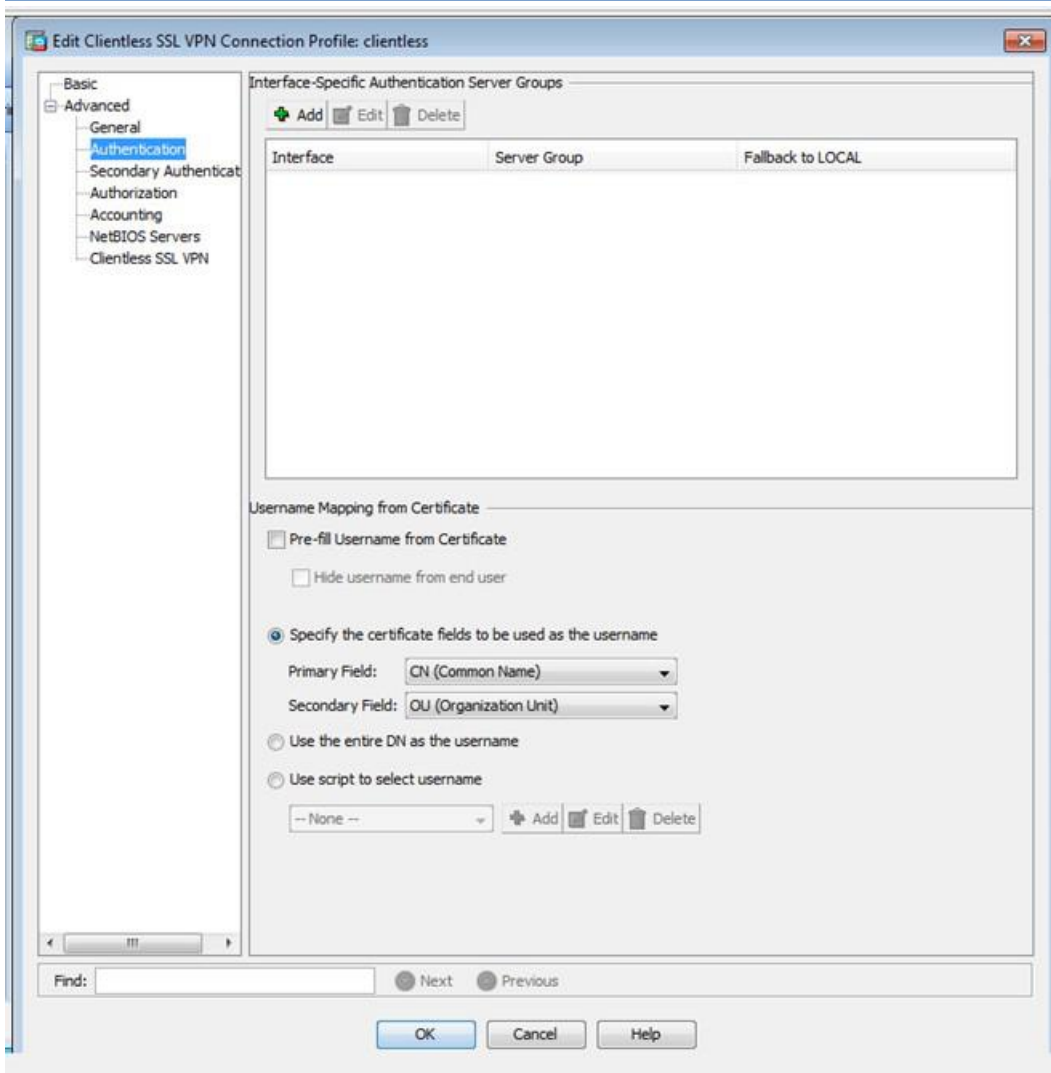
☒ Always run CSD

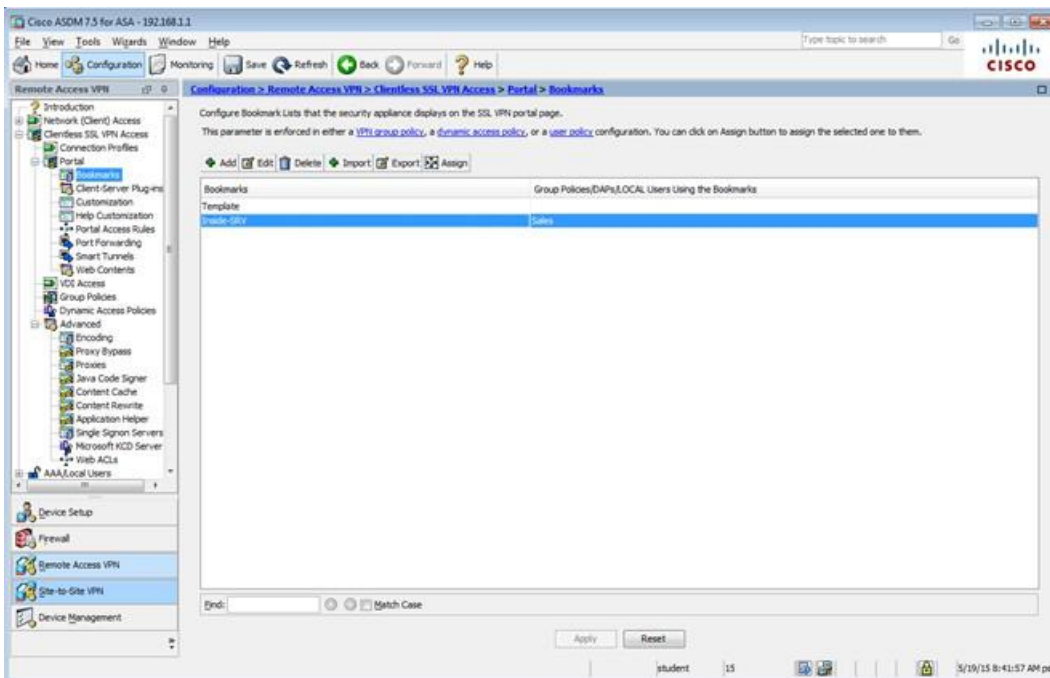
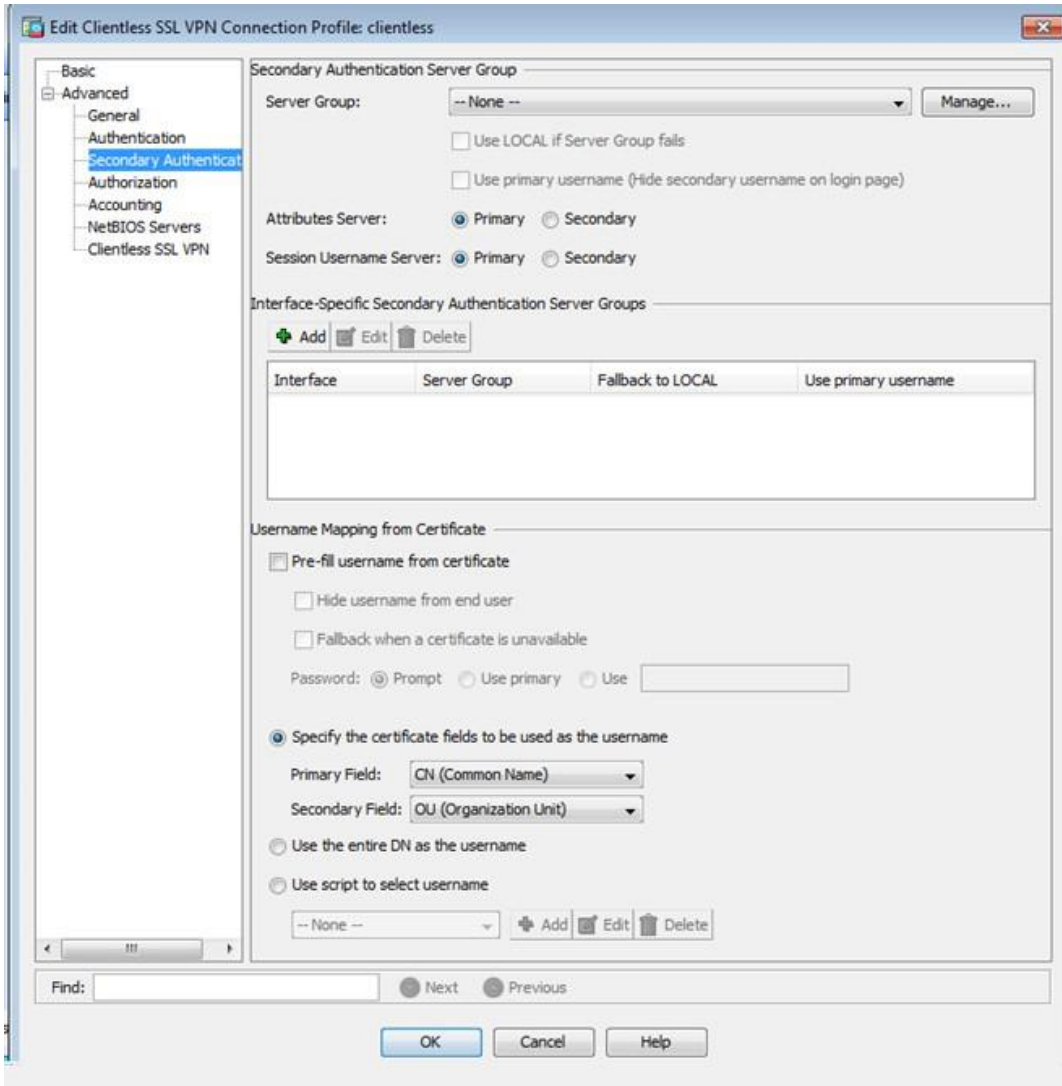
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

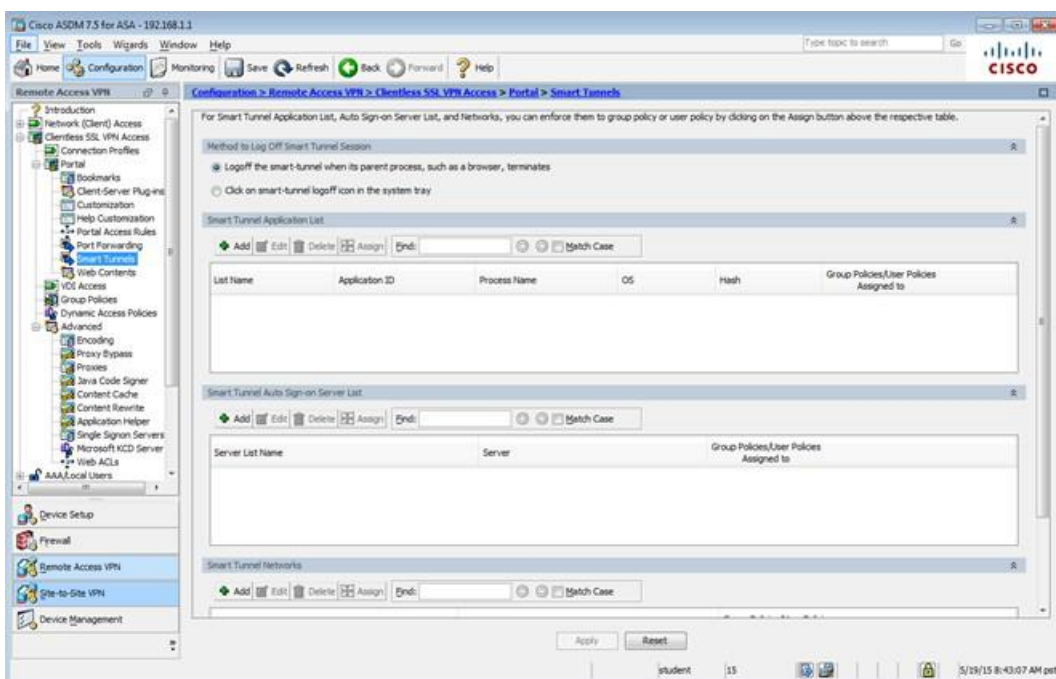
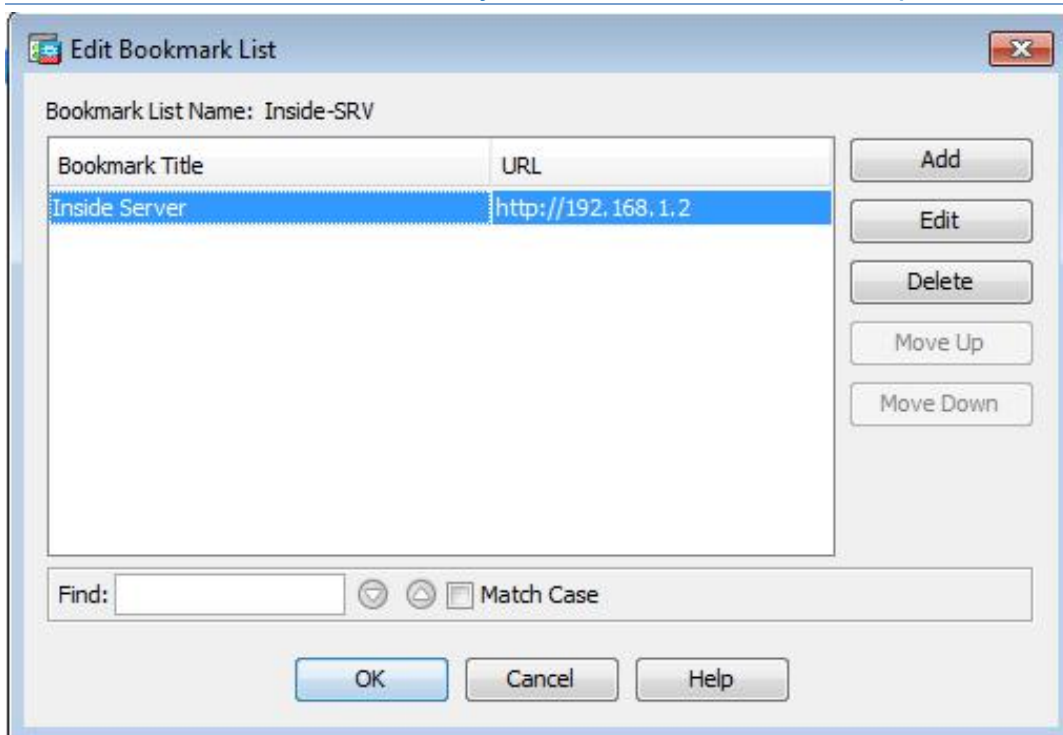
☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







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 > Portal > Port Forwarding

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

Add Edit Delete Assign

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

Find: Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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](#).

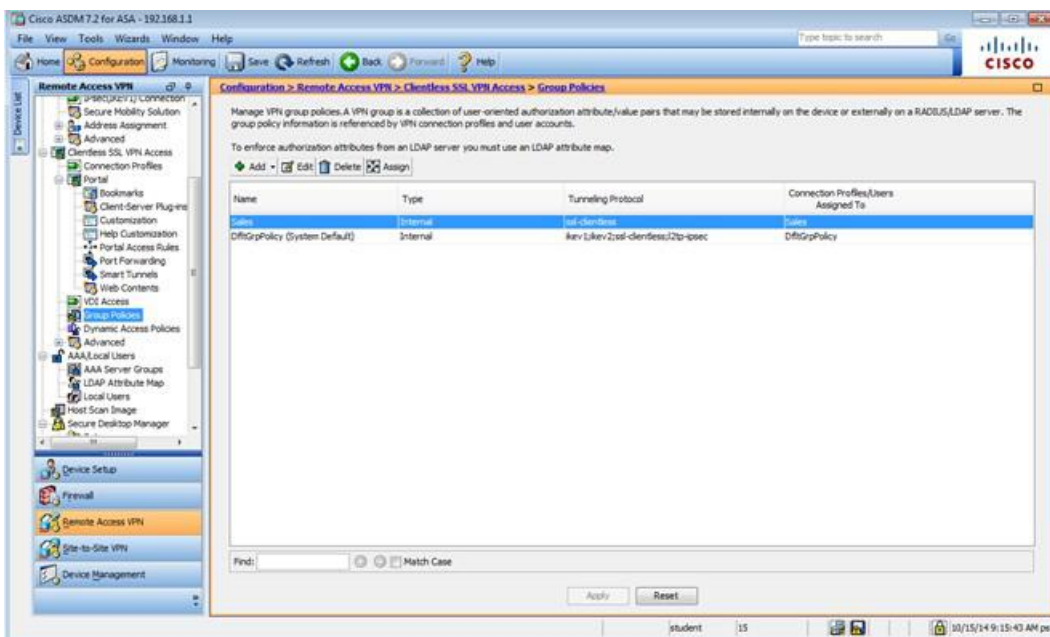
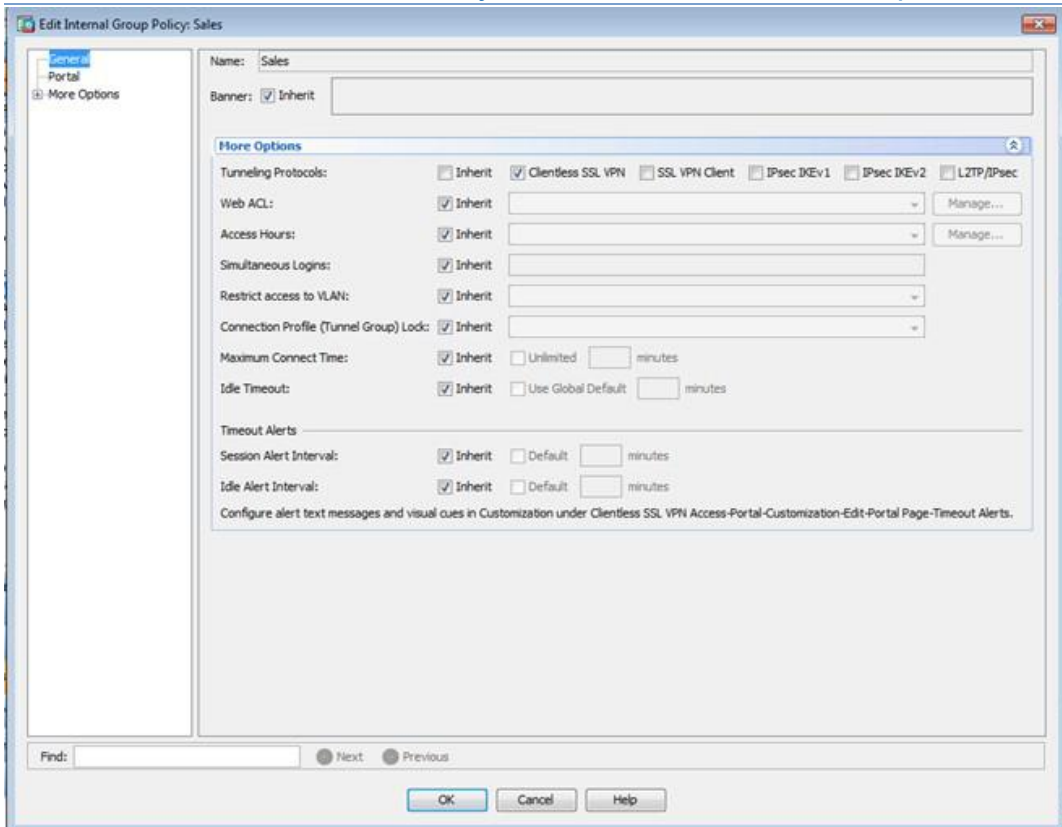
Add Edit Delete Assign

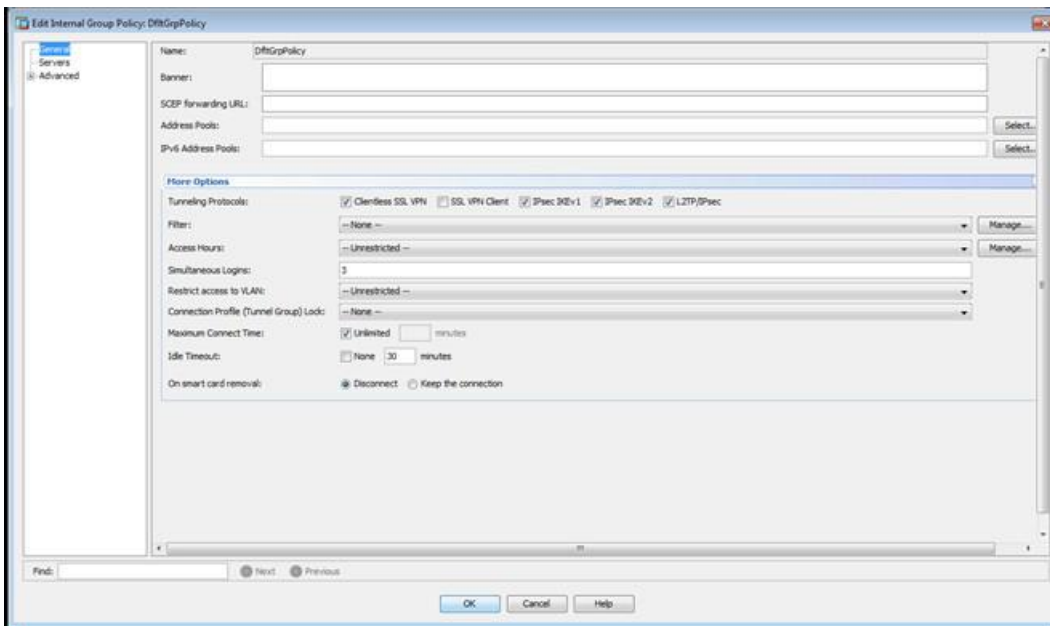
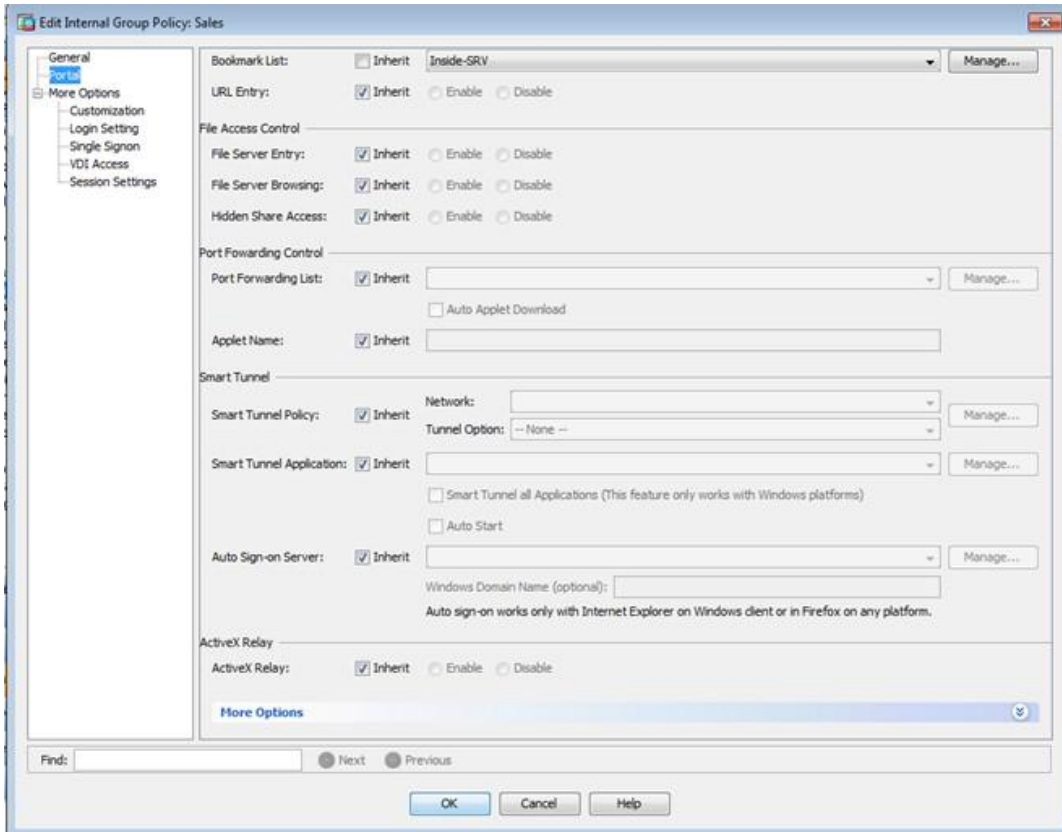
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	all-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1:rev2:ssl-clientless/2to-espsec	DefaultRAGroup/DefaultIL2Group/DefaultADP2Group/Def...

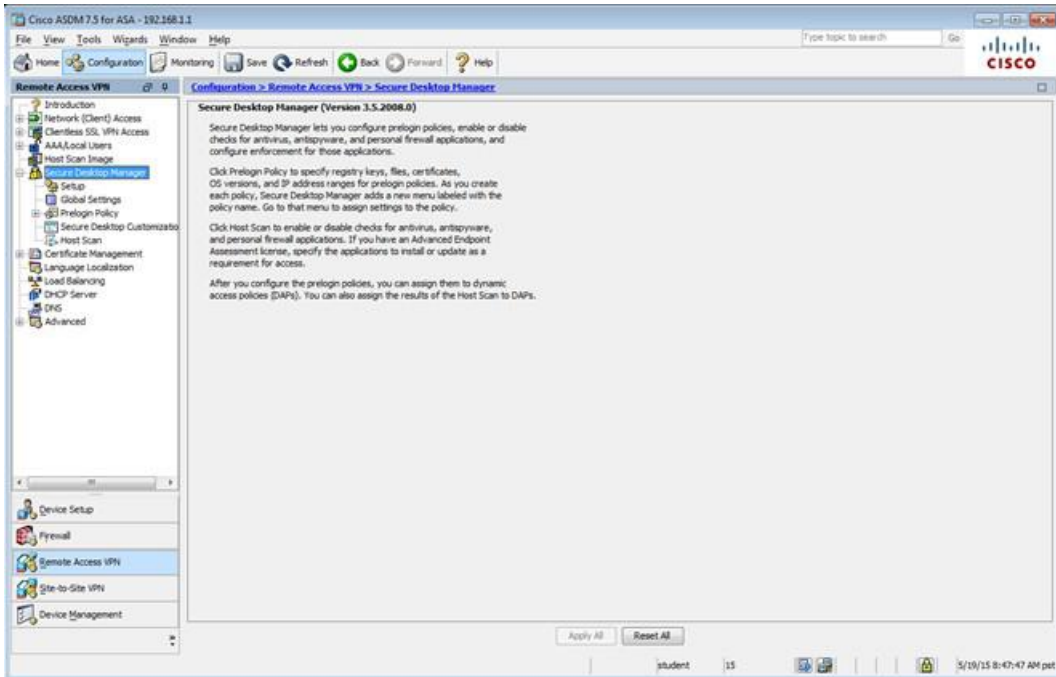
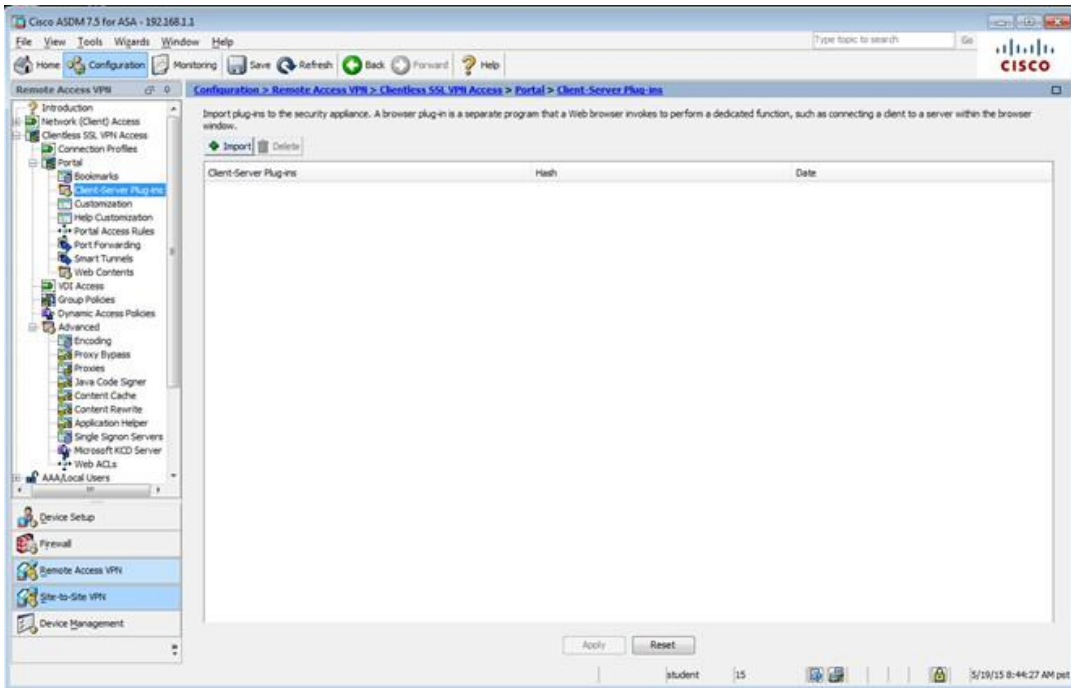
Find: Match Case

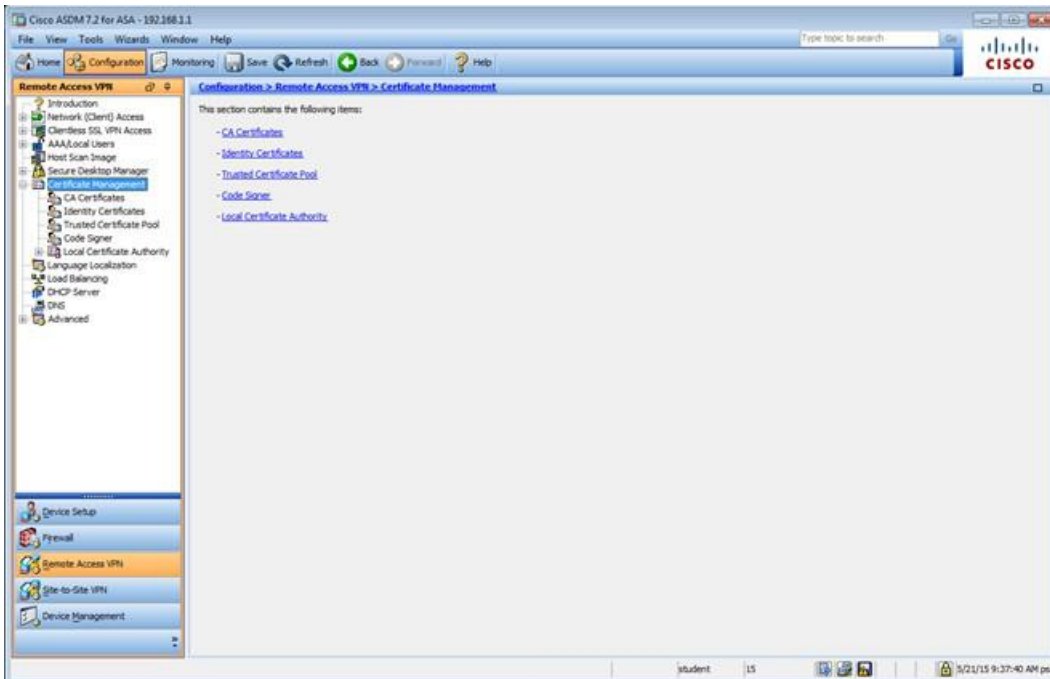
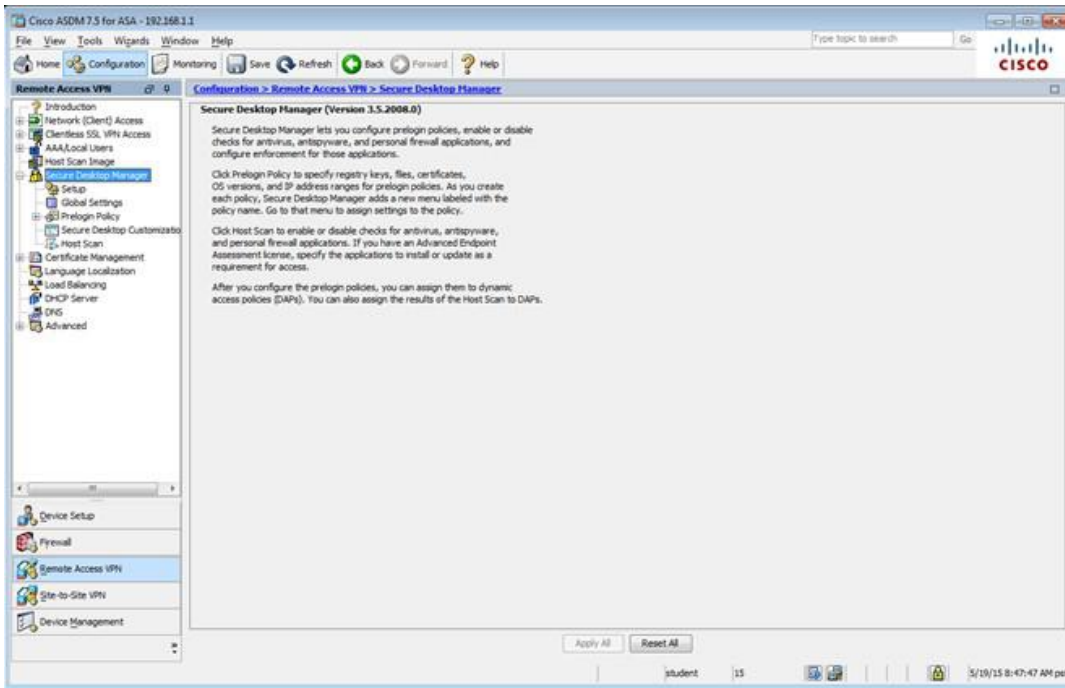
Apply Reset

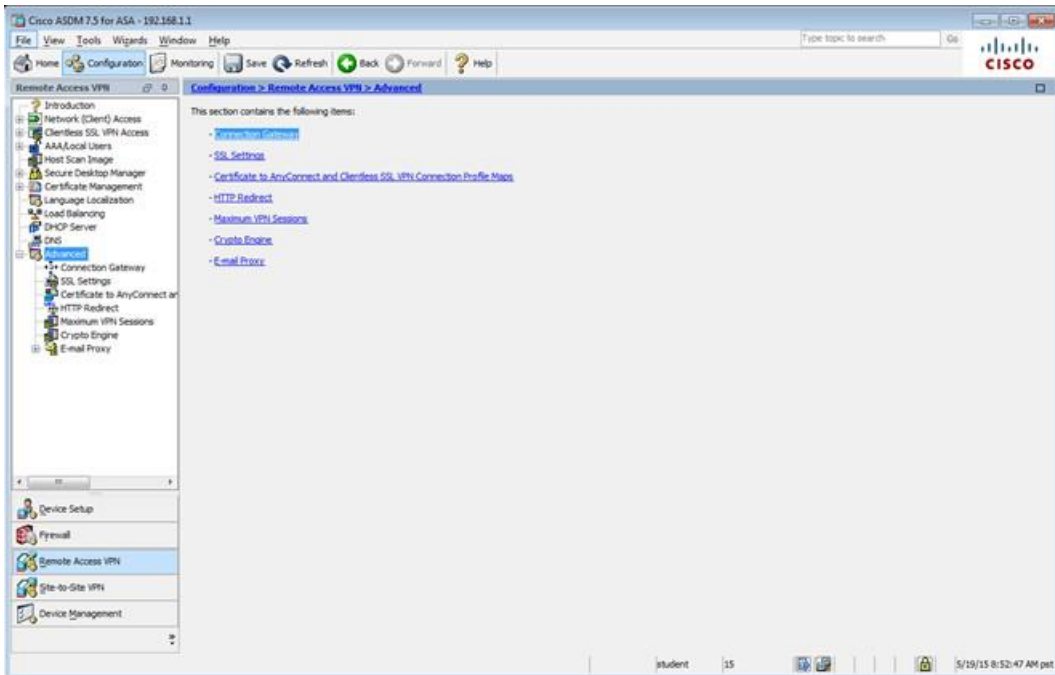
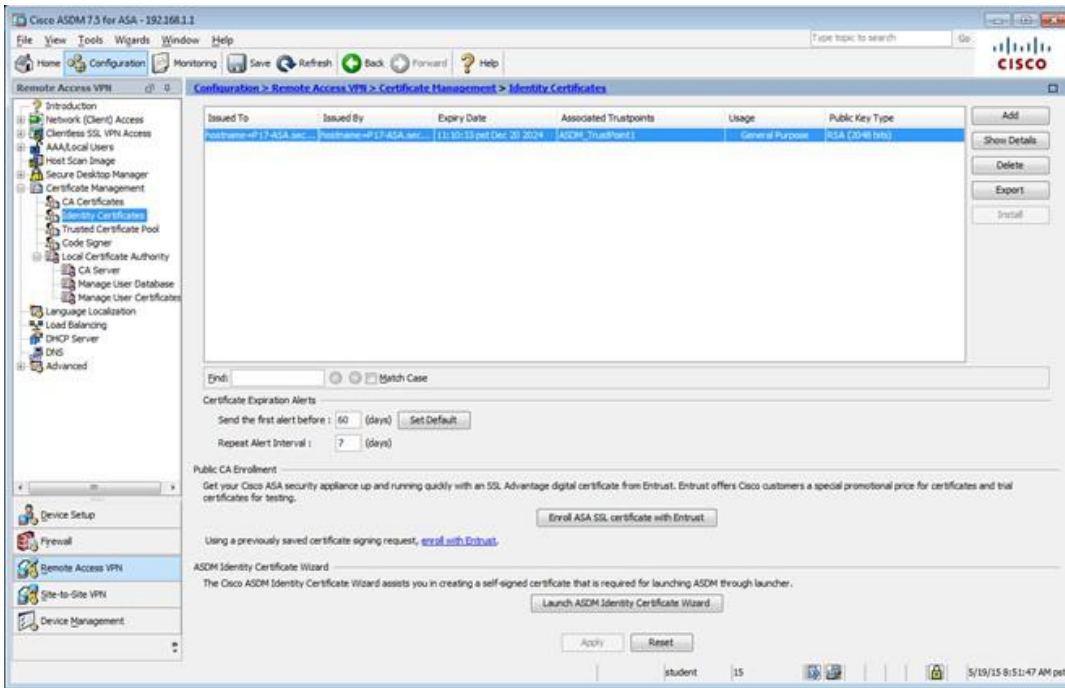
student 15 5/19/15 8:49:27 AM pst

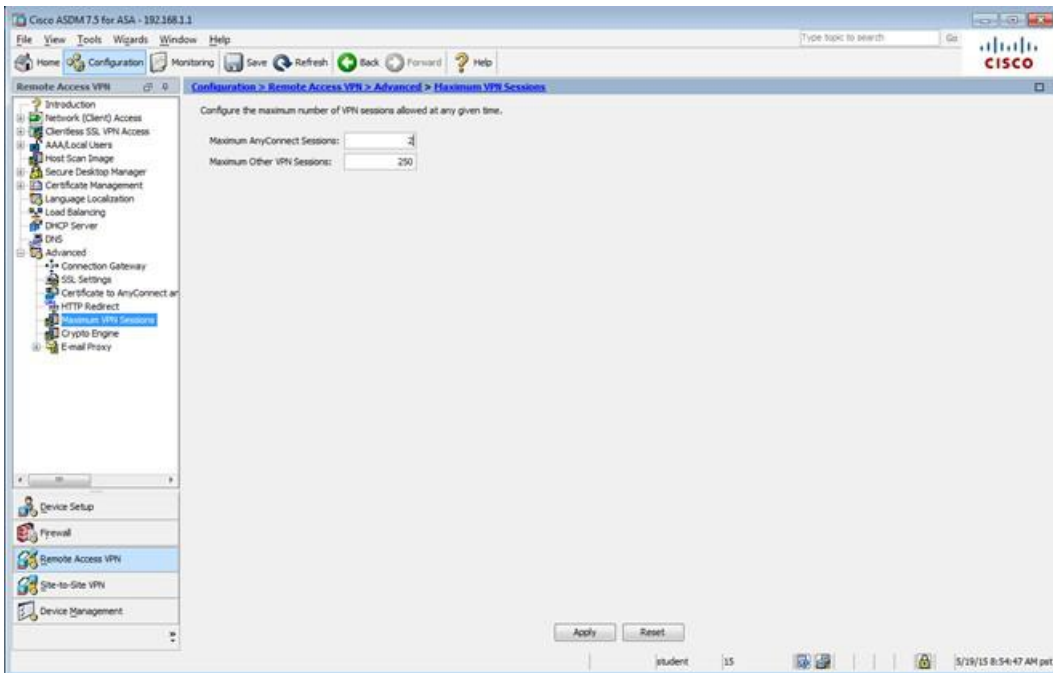
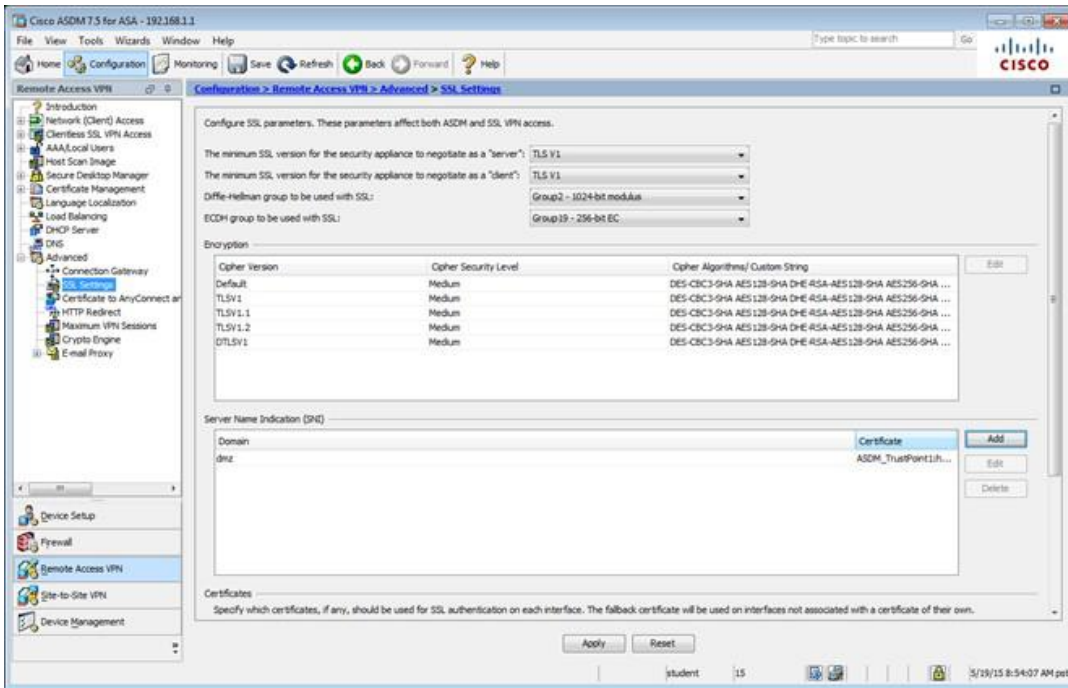












Configuration > Remote Access VPN > Network (Client) Access

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

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

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKEv2) protocols. Cisco VPN Client supports only IPsec(DKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
 You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based endpoint security policies.

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

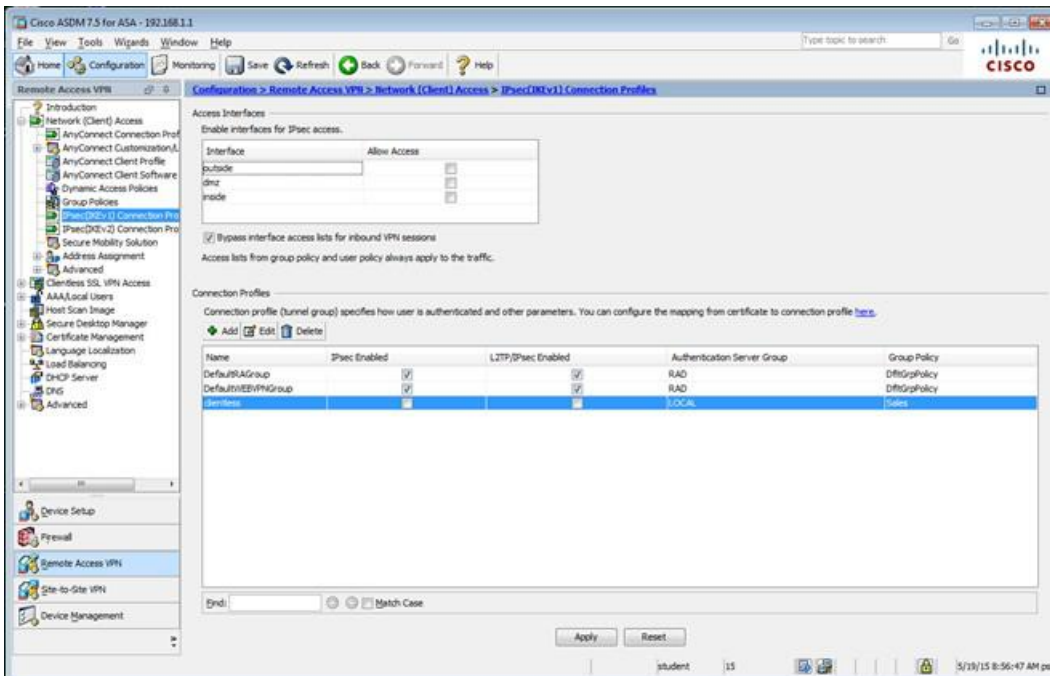
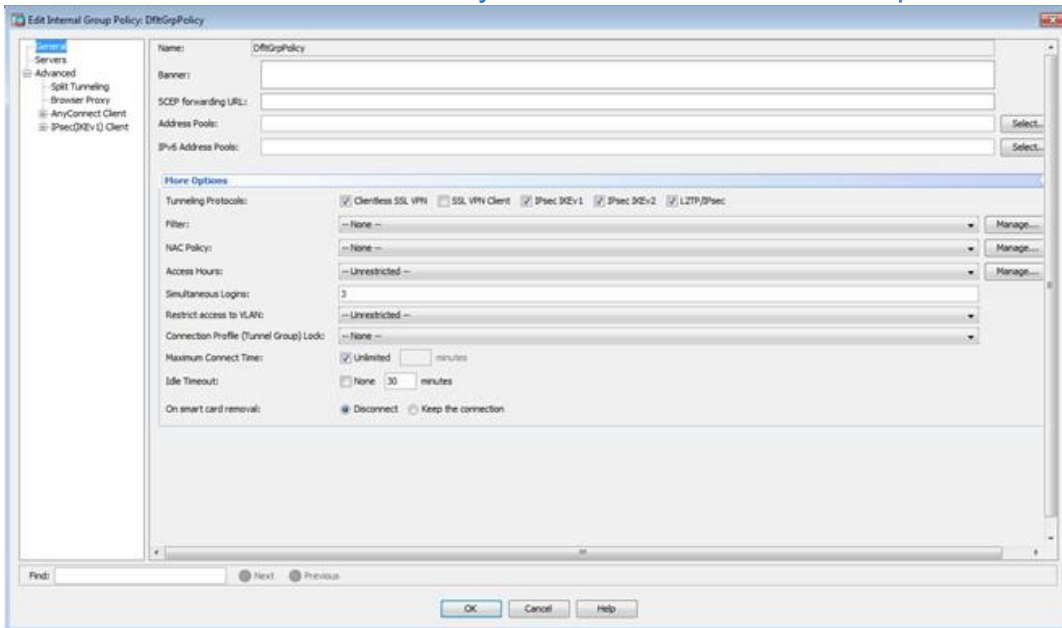
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization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

Find: Match Case

Apply Reset



The screenshot shows the Cisco ASDM 7.5 interface for configuring AnyConnect Connection Profiles. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AnyConnect Connection Profiles' configuration page.

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

Buttons: Add, Edit, Delete, End, Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
DefaultIVBGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
Clientless	<input checked="" type="checkbox"/>	<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.

Buttons: Apply, Reset

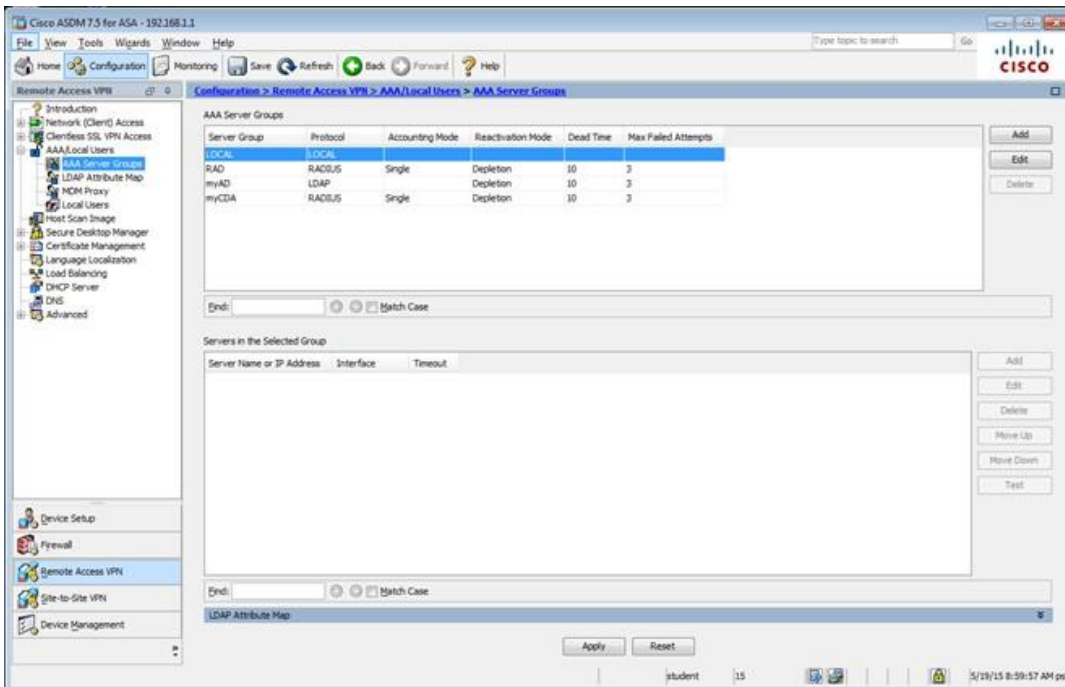
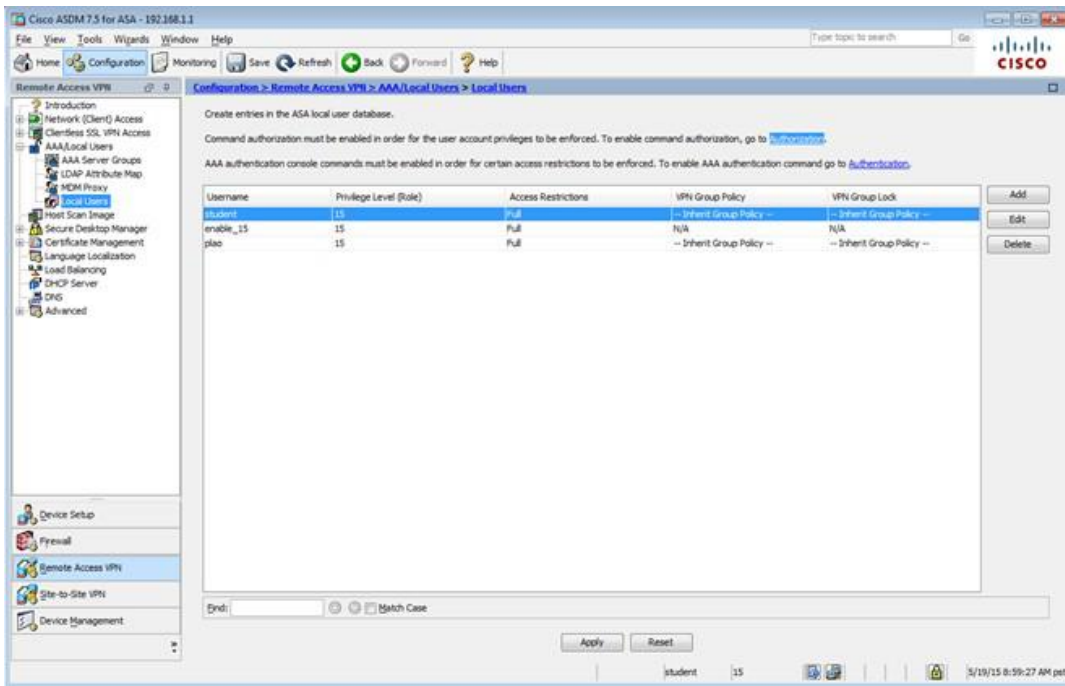
Footer: student 15 5/19/15 8:58:17 AM pst

The screenshot shows the Cisco ASDM 7.5 interface for configuring AAA/Local Users. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AAA/Local Users' configuration page.

This section contains the following items:

- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users

Footer: student 15 5/19/15 8:58:57 AM pst



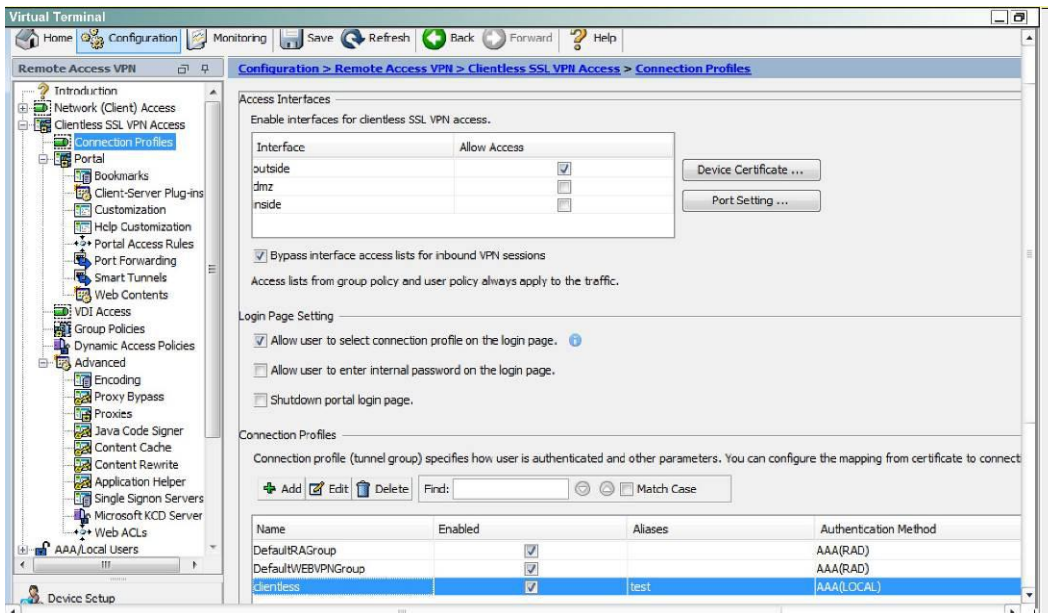
Which user authentication method is used when users login to the Clientless SSLVPN portal using <https://209.165.201.2/test?>

- 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

Answer: A

Explanation:

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



87. Which two characteristics of a PVLAN are true?

- A. isolated ports cannot communicate with other ports on the same VLAN.
- B. They require VTP to be enabled in server mode.
- C. Promiscuous ports can communicate with PVLAN ports
- D. PVLAN ports can be configured as EtherChannel ports.
- E. Community ports have to be a part of the trunk.

Answer: C,E

Explanation:

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/pvlan/ns.pdf>

88. 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

Answer: A

89. 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.

Answer: A

90. Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.)

- A. syslog
- B. SDEE
- C. FTP
- D. TFTP
- E. SSH
- F. HTTPS

Answer: B,F

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Step 4: Enabling IOS IPS

The fourth step is to configure IOS IPS using the following sequence of steps: Step 4.1: Create a rule name (This will be used on an interface to enable IPS) ip ips name <rule name> < optional ACL>





router#configure terminal router(config)# ip ips name iosips

You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

router(config)#ip ips name ips list ?

<1-199> Numbered access list WORD Named access list

Step 4.2: Configure IPS signature storage location, this is the directory 'ips' created in Step 2

ip ips config location flash:<directory name> router(config)#ip ips config location flash:ips Step 4.3: Enable IPS SDEE event notification

ip ips notify sdee router(config)#ip ips notify sdee

To use SDEE, the HTTP server must be enabled (via the 'ip http server' command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests. SDEE notification is disabled by default and must be explicitly enabled.

91. Refer to the exhibit.

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

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

R2
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

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

You have configured R1 and R2 as shown, but the routers are unable to establish a site-to-site VPN tunnel.

What action can you take to correct the problem?

- A. Edit the crypto keys on R1 and R2 to match.
- B. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.
- C. Set a valid value for the crypto key lifetime on each router.



D. Edit the crypto isakmp key command on each router with the address value of its own interface.

Answer: A

92. Which of the following statements about access lists are true? (Choose three.)

- A. Extended access lists should be placed as near as possible to the destination
- B. Extended access lists should be placed as near as possible to the source
- C. Standard access lists should be placed as near as possible to the destination
- D. Standard access lists should be placed as near as possible to the source
- E. Standard access lists filter on the source address
- F. Standard access lists filter on the destination address

Answer: B,C,E

93. Which IDS/IPS solution can monitor system processes and resources?

- A. IDS
- B. HIPS
- C. PROXY
- D. IPS

Answer: B

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

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

Answer: D

95. Protocols supported in context aware VRF over VRF lite? Choose Two

- A. EIGRP
- B. Multicast
- C. CGR



Answer: A,B

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

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

Answer: A

97. What is the best way to confirm that AAA authentication is working properly?

- A. Use the test aaa command.
- B. Ping the NAS to confirm connectivity.
- C. Use the Cisco-recommended configuration for AAA authentication.
- D. Log into and out of the router, and then check the NAS authentication log.

Answer: A

98. Which type of mirroring does SPAN technology perform?

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

Answer: C

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

- A. plaintext
- B. MD5
- C. HMAC
- D. AES 256



E. SHA-1

F. DES

Answer: A,B

100. Which IPS mode is less secure than other options but allows optimal network throughput?

A. promiscuous mode

B. inline mode

C. inline-bypass mode

D. transparent mode.

Answer: A

101. Which statement about zone-based firewall configuration is true?

A. Traffic is implicitly denied by default between interfaces the same zone

B. Traffic that is desired to or sourced from the self-zone is denied by default

C. The zone must be configured before a can be assigned

D. You can assign an interface to more than one interface

Answer: C

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

A. Ensure that the RDP2 plug-in is installed on the VPN gateway

B. Reboot the VPN gateway

C. Instruct the user to reconnect to the VPN gateway

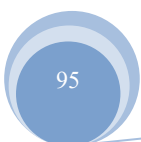
D. Ensure that the RDP plug-in is installed on the VPN gateway

Answer: D

103. 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.

Answer: A

104. What is the actual IOS privilege level of User Exec mode?

- A. 1
- B. 0
- C. 5
- D. 15

Answer: A

Explanation: By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15). However, you can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.

Source: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpas s.html

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

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

Answer: A

106. Which sensor mode can deny attackers inline?

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



Answer: A

107. What are two well-known security terms? (Choose Two)

- A. Phishing.
- B. BPDU guard
- C. LACP
- D. ransomware
- E. hair-pinning

Answer: A,D

108. 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

Answer: A,B

109. What is the primary purpose of a defined rule in an IPS?

- A. to configure an event action that takes place when a signature is triggered
- B. to define a set of actions that occur when a specific user logs in to the system
- C. to configure an event action that is pre-defined by the system administrator
- D. to detect internal attacks

Answer: A

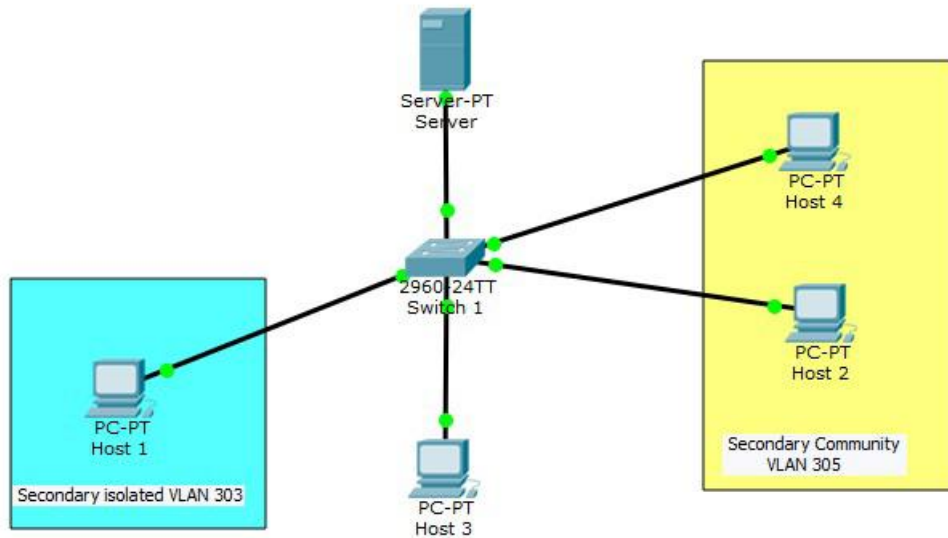
110. In which two situations should you use in-band management? (Choose two.)

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

E. when the control plane fails to respond

Answer: A,B

111. Refer to the exhibit.



All ports on switch 1 have a primary VLAN of 300. Which devices can host 1 reach?

- A. Host 2
- B. Server
- C. Host 4
- D. Other devices within VLAN 303

Answer: B

112. Which two features are supported in a VRF-aware software infrastructure before VRF-lite? (Choose two)

- A. priority queuing
- B. EIGRP
- C. multicast
- D. WCCP
- E. fair queuing

Answer: B,C



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

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

Answer: B,D,F

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

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

Answer: C,E,F

115. What is a possible reason for the error message?Router(config)#aaa server?%

Unrecognized command

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

Answer: D

116. 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.

Answer: A

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

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

Answer: C

118. Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)

- A. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- B. authenticating administrator access to the router console port, auxiliary port, and vty ports
- C. implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
- D. tracking Cisco NetFlow accounting statistics
- E. securing the router by locking down all unused services
- F. performing router commands authorization using TACACS+

Answer: A,B,F

Explanation:

http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.htm I

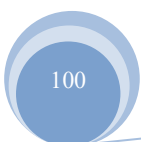
Need for AAA Services

Security for user access to the network and the ability to dynamically define a user's profile to gain access to network resources has a legacy dating back to asynchronous dial access. AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server.

Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes.

AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+.

The information can also be stored locally on the access server or router. Remote security servers, such as





RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

119. Which option is a key security component of an MDM deployment?

- A. using MS-CHAPv2 as the primary EAP method.
- B. using self-signed certificates to validate the server.
- C. using network-specific installer packages
- D. using an application tunnel by default.

Answer: B

120. 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.

Answer: A

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

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

Answer: A

122. 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.

Answer: A

123. On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

- A. used for SSH server/client authentication and encryption
- B. used to verify the digital signature of the IPS signature file
- C. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration Professional
- D. used to enable asymmetric encryption on IPsec and SSL VPNs
- E. used during the DH exchanges on IPsec VPNs

Answer: B

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Step 1: Downloading IOS IPS files

The first step is to download IOS IPS signature package files and public crypto key from Cisco.com.

Step 1.1: Download the required signature files from Cisco.com to your PC

- Location: <http://tools.cisco.com/support/downloads/go/Model.x?mdfid=281442967&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Prevention%20System%20Feature%20Software&treeMdfid=268438162>
- Files to download:

IOS-Sxxx-CLI.pkg: Signature package - download the latest signature package. realm-cisco.pub.key.txt:

Public Crypto key - this is the crypto key used by IOS IPS



124. Which IDS/IPS is used for monitoring system?

- A. HIPS
- B. WIPS
- C. visibility tool

Answer: A

125. In the router ospf 200 command, what does the value 200 stand for?

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

Answer: A

126. 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

Answer: A

127. What command could you implement in the firewall to conceal internal IP address?

- A. no source-route
- B. no broadcast....
- C. no proxy-arp

Answer: C

128. The first layer of defense which provides real-time preventive solutions against malicious traffic is provided by?

- A. Banyan Filters



- B. Explicit Filters
- C. Outbreak Filters

Answer: C

129. What is true about the Cisco IOS Resilient Configuration feature?

- A. The feature can be disabled through a remote session
- B. There is additional space required to secure the primary Cisco IOS Image file
- C. The feature automatically detects image and configuration version mismatch
- D. Remote storage is used for securing files

Answer: C

130. When is the default deny all policy an exception in zone-based firewalls?

- A. When traffic traverses two interfaces in in the same zone
- B. When traffic terminates on the router via the self zone
- C. When traffic sources from the router via the self zone
- D. When traffic traverses two interfaces in different zones

Answer: A

131. How can you detect a false negative on an IPS?

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

Answer: D

132. Whit which type of Layer 2 attack can you “do something” for one host:

- A. MAC spoofing
- B. CAM overflow....

Answer: A



133. Which prevent the company data from modification even when the data is in transit?

- A. Confidentiality
- B. Integrity
- C. Vailability

Answer: B

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

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

Answer: B

135. 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.

Answer: A

136. DRAG DROP

Drag the hash or algorithm from the left column to its appropriate category on the right.

DES	insecure
3DES	insecure
MD5	legacy
SHA-1	legacy
HMAC-MD5	legacy

Answer:

DES	MD5
3DES	DES
MD5	3DES
SHA-1	SHA-1
HMAC-MD5	HMAC-MD5

Explanation:

<https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html>

137. Which two primary security concerns can you mitigate with a BYOD solution? (Choose two)

- A. Schedule for patching the device
- B. compliance with applicable policies
- C. device lagging and inventory
- D. Connections to public Wi-Fi networks
- E. Securing access to a trusted corporate network.



Answer: B,E

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

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

Answer: C

139. 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

Answer: D,E,F

140. what causes a client to be placed in a guest or restricted VLAN on an 802.1x enabled network?

- A. client entered wrong credentials multiple times.
- B. client entered wrong credentials First time.

Answer: A

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

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



D. forwarding, listening, learning, blocking, disabled

Answer: C

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

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

Answer: A,D

143. Which command do you enter to enable authentication for OSPF on an interface?

- A. router(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
- B. router(config-router)#area 0 authentication message-digest
- C. router(config-router)#ip ospf authentication-key CISCOPASS
- D. router(config-if)#ip ospf authentication message-digest

Answer: D

144. 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

Answer: A,B,C

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

- A. when matching NAT entries are configured



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

Answer: A,B,D

146. Which two devices are components of the BYOD architectural framework?

- A. Prime Infrastructure
- B. Nexus 7010 Switch
- C. Cisco 3945 Router
- D. Wireless Access Points
- E. Identity Services Engine

Answer: A,E

147. Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

- A. aaa accounting network start-stop tacacs+
- B. aaa accounting system start-stop tacacs+
- C. aaa accounting exec start-stop tacacs+
- D. aaa accounting connection start-stop tacacs+
- E. aaa accounting commands 15 start-stop tacacs+

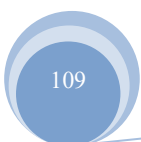
Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the aaa accounting command in global configuration mode or template configuration mode. To disable AAA accounting, use the no form of this command.

aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default |





list-name

| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name}

no aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default |

listname

| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} exec

Runs accounting for the EXEC shell session. start-stop

Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

148. 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.

Answer: B

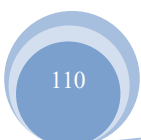
149. Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

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

Answer: B,D,E

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

- A. Unidirectional Link Detection
- B. Unicast Reverse Path Forwarding
- C. TrustSec





D. IP Source Guard

Answer: B

151. Which option is the resulting action in a zone-based policy firewall configuration with these conditions?

Source: Zone 1
Destination: Zone 2
Zone pair exists?: Yes
Policy exists?: No

A. no impact to zoning or policy

B. no policy lookup (pass)

C. drop

D. apply default policy

Answer: C

Explanation:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xr-3s/sec-zone-pol-fw.html

Zone Pairs

A zone pair allows you to specify a unidirectional firewall policy between two security zones.

To define a zone pair, use the zone-pair security command. The direction of the traffic is specified by source and destination zones. The source and destination zones of a zone pair must be security zones.

You can select the default or self zone as either the source or the destination zone. The self zone is a systemdefined zone which does not have any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.

The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).

To permit traffic between zone member interfaces, you must configure a policy permitting (or inspecting) traffic between that zone and another zone. To attach a firewall policy map to the target zone pair, use the servicepolicy type inspect command.

The figure below shows the application of a firewall policy to traffic flowing from zone Z1 to zone Z2, which means that the ingress interface for the traffic is a member of zone Z1 and the egress interface is a member of zone Z2.

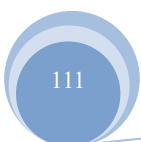
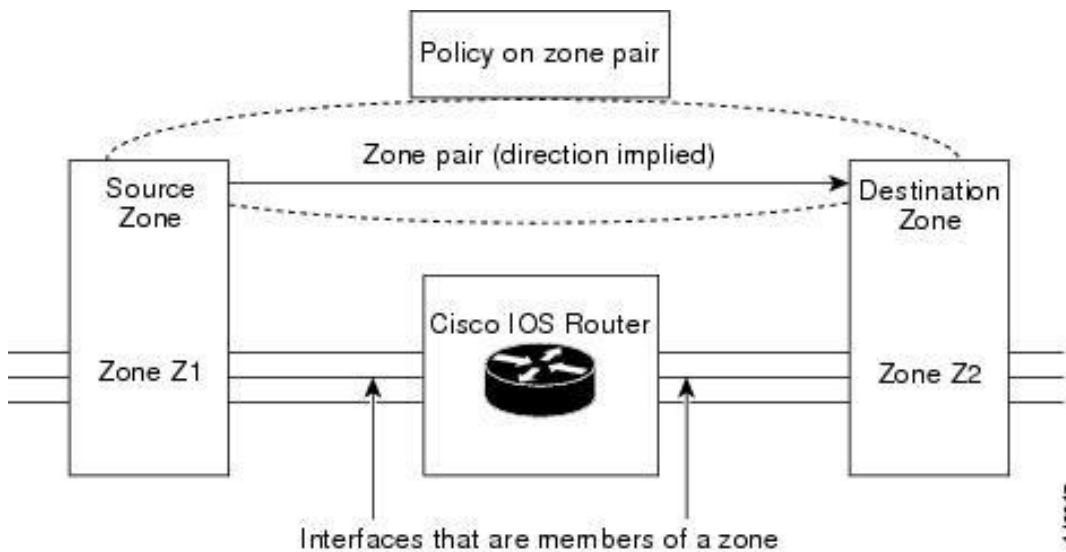


Figure 2. Zone Pairs



If there are two zones and you require policies for traffic going in both directions (from Z1 to Z2 and Z2 to Z1), you must configure two zone pairs (one for each direction).

If a policy is not configured between zone pairs, traffic is dropped. However, it is not necessary to configure a zone pair and a service policy solely for the return traffic. By default, return traffic is not allowed. If a service policy inspects the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is inspected. If a service policy passes the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is dropped. In both these cases, you need to configure a zone pair and a service policy to allow the return traffic. In the above figure, it is not mandatory that you configure a zone pair source and destination for allowing return traffic from Z2 to Z1. The service policy on Z1 to Z2 zone pair takes care of it.

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

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

Answer: A

153. Which two statements about the self zone on a Cisco zone-based policy firewall are true? (Choose Two)



- A. Multiple interfaces can be assigned to the self zone.
- B. Traffic entering the self zone must match a rule.
- C. Zone pairs that include the self zone apply to traffic transiting the device.
- D. It can be either the source zone or the destination zone.
- E. It supports stateful inspection for multicast traffic.

Answer: D,E

154. The command debug crypto isakmp results in ?

- A. Troubleshooting ISAKMP (Phase 1) negotiation problems

Answer: A

155. Which IOS command is used to define the authentication key for NTP?

- A. Switch(config)#ntp authentication-key 1 md5 C1sc0
- B. Switch(config)#ntp trusted-key 1
- C. Switch(config)#ntp source 192.168.0.1
- D. Switch(config)#ntp authenticate

Answer: A

156. What data is transferred during DH for making public and private key?

- A. Random prime Integer
- B. Encrypteddata transfer
- C. Diffie-Hellman

Answer: A

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

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



E. MS-CHAPv1

F. MS-CHAPv2

Answer: B,C,E

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

A. 2002::/16

B. FD00::/8

C. 2001::/32

D. FB00::/8

Answer: B

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

A. CCPr

B. Parser views

C. Access control lists

D. Port security

E. CoPP

Answer: A,E

160. Which statement correctly describes the function of a private VLAN?

A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains

B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains

C. A private VLAN enables the creation of multiple VLANs using one broadcast domain

D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain

Answer: A

161. Which two features of Cisco Web Reputation tracking can mitigate web-based threats? (Choose Two)

A. outbreak filter

B. buffer overflow filter



- C. bayesian filter
- D. web reputation filter
- E. exploit filtering

Answer: A,D

Explanation:

Cisco IronPort Outbreak Filters provide a critical first layer of defense against new outbreaks. With this proven preventive solution, protection begins hours before signatures used by traditional antivirus solutions are in place. Real-world results show an average 14- hour lead time over reactive antivirus solutions.

SenderBase, the world's largest email and web traffic monitoring network, provides real- time protection. The Cisco IronPort SenderBase Network captures data from over 120,000 contributing organizations around the world.

Source:

http://www.cisco.com/c/en/us/products/security/email-security-appliance/outbreak_filters_index.html

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

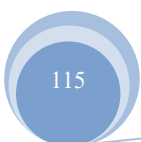
- A. deny attacker
- B. deny packet
- C. modify packet
- D. request block connection
- E. request block host
- F. reset TCP connection

Answer: A,B,C

163. Which type of encryption technology has the broadcast platform support?

- A. Middleware
- B. Hardware
- C. Software
- D. File-level

Answer: C





164. which will auto-nat process first (the focus is on auto-nat)

- A. dynamic Nat shortest prefix
- B. dynamic nat longest prefix
- C. static nat shortest prefix
- D. static nat longest prefix

Answer: D

165. 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.

Answer: A

166. 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.

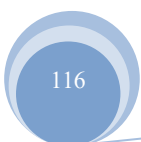
Answer: A

167. SYN flood attack is a form of ?

- A. Denial of Service attack
- B. Man in the middle attack
- C. Spoofing attack

Answer: A

168. which feature allow from dynamic NAT pool to choose next IP address and not a port on a used IP address?





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

Answer: B

169. Which two options are advantages of an application layer firewall? (Choose two.)

- A. provides high-performance filtering
- B. makes DoS attacks difficult
- C. supports a large number of applications
- D. authenticates devices
- E. authenticates individuals

Answer: B,E

Explanation:

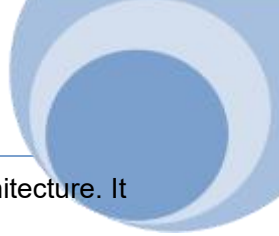
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd8058ec85.html

Adding Intrusion Prevention

Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware.

Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network.

Firewalls provide the first line of defense in any organization's network security infrastructure. They do so by matching corporate policies about users' network access rights to the connection information surrounding each access attempt. If the variables don't match, the firewall blocks the access connection. If the variables do match, the firewall allows the acceptable traffic to flow through the network.



In this way, the firewall forms the basic building block of an organization's network security architecture. It pays to use one with superior performance to maximize network uptime for business-critical operations. The reason is that the rapid addition of voice, video, and collaborative traffic to corporate networks is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, firewalls enhanced with application-level inspection examine, identify, and verify application types at Layer 7 to make sure unwanted or misbehaving application traffic doesn't join the network. With these capabilities, the firewall can enforce endpoint user registration and authentication and provide administrative control over the use of multimedia applications.

170. Which firepower preprocessor block traffic based on IP?

- A. Signature-Based
- B. Policy-Based
- C. Anomaly-Based
- D. Reputation-Based

Answer: D

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

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

Answer: D

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

- A. Port security
- B. DHCP snooping
- C. IP source guard



D. Dynamic ARP inspection

Answer: B,D

173. Which option is the cloud based security service from Cisco that provides URL filtering web browsing content security, and roaming user protection?

- A. Cloud web security
- B. Cloud web Protection
- C. Cloud web Service
- D. Cloud advanced malware protection

Answer: A

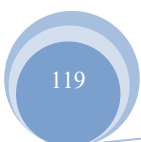
174. What improvement does EAP-FASTv2 provide over EAP-FAST?

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

Answer: A

175. 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.

Answer: B

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

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

Answer: A

177. Which ports need to be active for AAA server and a Microsoft server to permit Active Directory authentication?

- A. 445 and 389
- B. 888 and 3389
- C. 636 and 4445
- D. 363 and 983

Answer: A

178. 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.

Answer: A

179. Which term best describes the concept of preventing the modification of data in transit and in storage?

- A. Confidentiality
- B. Integrity
- C. Availability



D. fidelity

Answer: B

Explanation:

Integrity for data means that changes made to data are done only by authorized individuals/systems.

Corruption of data is a failure to maintain data integrity.

Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

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

A. always-on

B. proxy

C. transparent mode

D. Trusted Network Detection

Answer: A

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

A. Reflexive access lists create a permanent ACE

B. Reflexive access lists approximate session filtering using the established keyword

C. Reflexive access lists can be attached to standard named IP ACLs

D. Reflexive access lists support UDP sessions

E. Reflexive access lists can be attached to extended named IP ACLs

F. Reflexive access lists support TCP sessions

Answer: D,E,F

182. Refer to the exhibit.

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

The Admin user is unable to enter configuration mode on a device with the given configuration. What



change can you make to the configuration to correct the problem?

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

Answer: A

183. Which type of attack can exploit design flaws in the implementation of an application without going noticed?

- A. Volume-based DDoS attacks.
- B. application DDoS flood attacks.
- C. DHCP starvation attacks
- D. low-rate DoS attacks

Answer: D

184. Refer to the exhibit.

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

What are two effects of the given command? (Choose two.)

- A. It configures authentication to use AES 256.
- B. It configures authentication to use MD5 HMAC.
- C. It configures authorization use AES 256.
- D. It configures encryption to use MD5 HMAC.
- E. It configures encryption to use AES 256.

Answer: B,E

185. 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

Answer: A

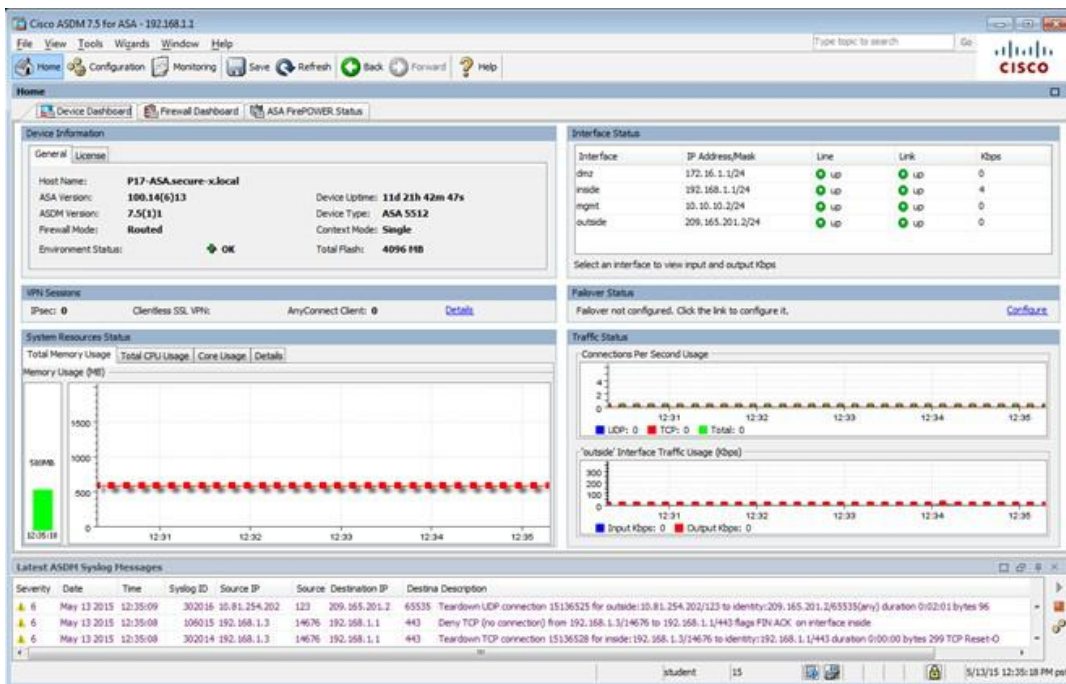
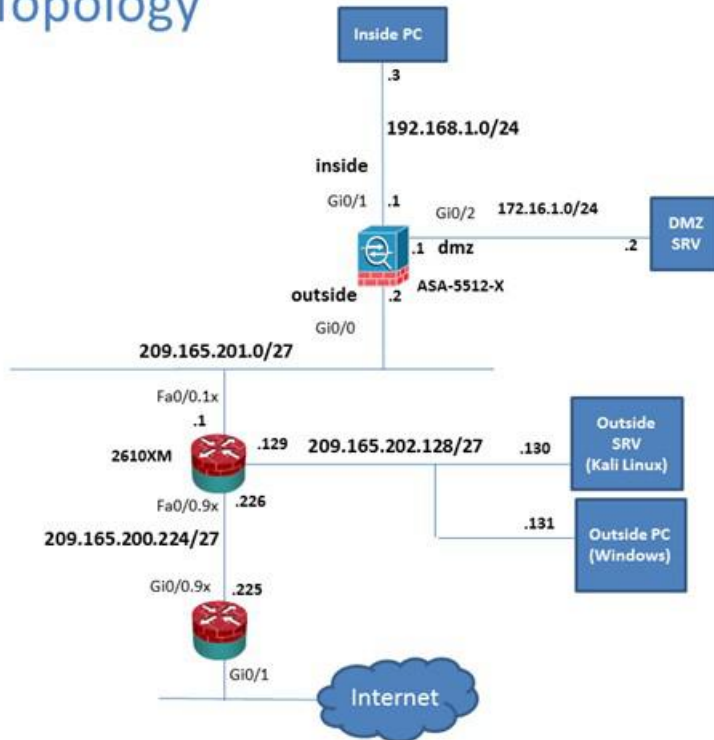
186. Scenario

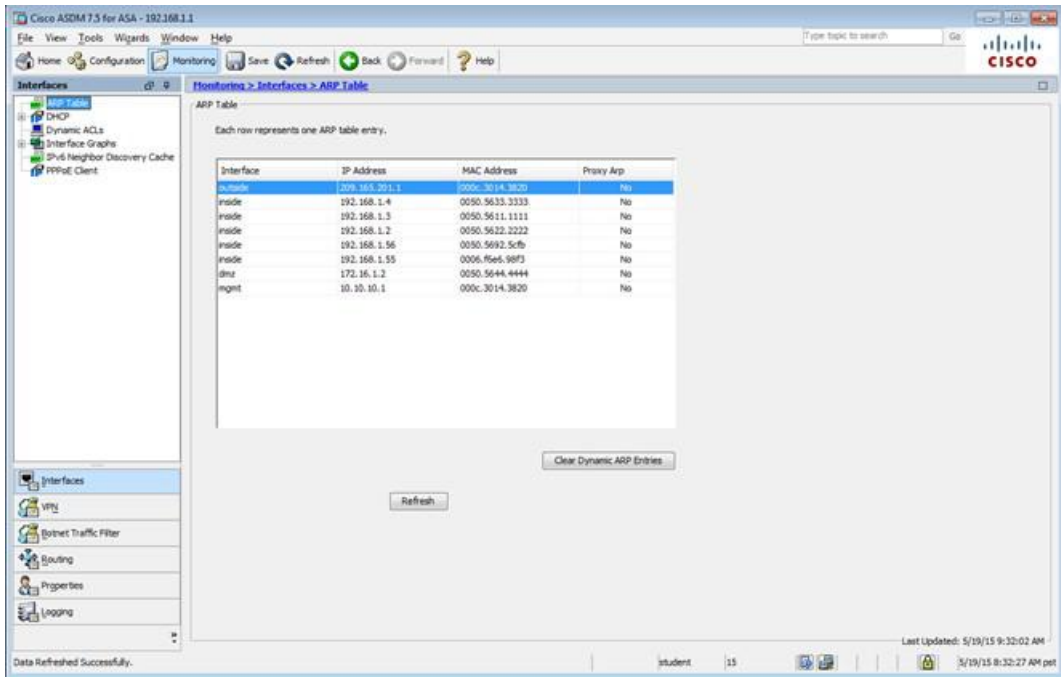
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
inside	192.168.1.1	0000.0000.0000	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	0050.5692.5cfa	No
inside	192.168.1.55	0006.86e6.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

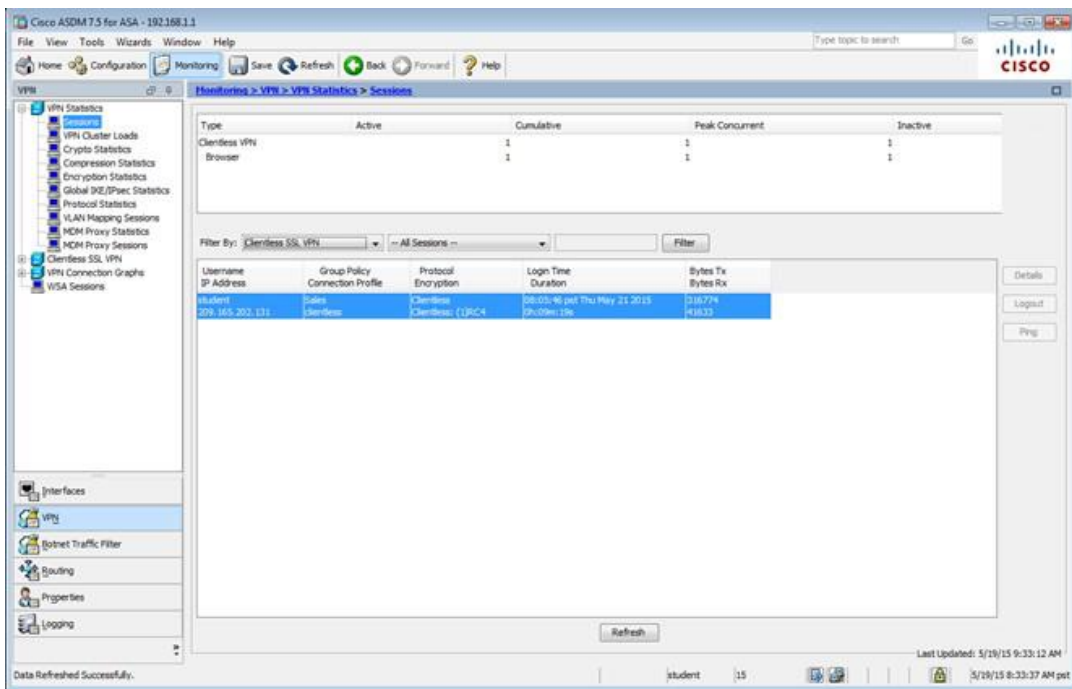
Refresh

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

Data Refreshed Successfully.

student 15

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

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	172.16.1.1	Clientless	Clientless	Clientless	(136C4)	08:05:46 pm Thu May 21 2015	0h:00m:10s	218,774	418,33

Details Logout Ping

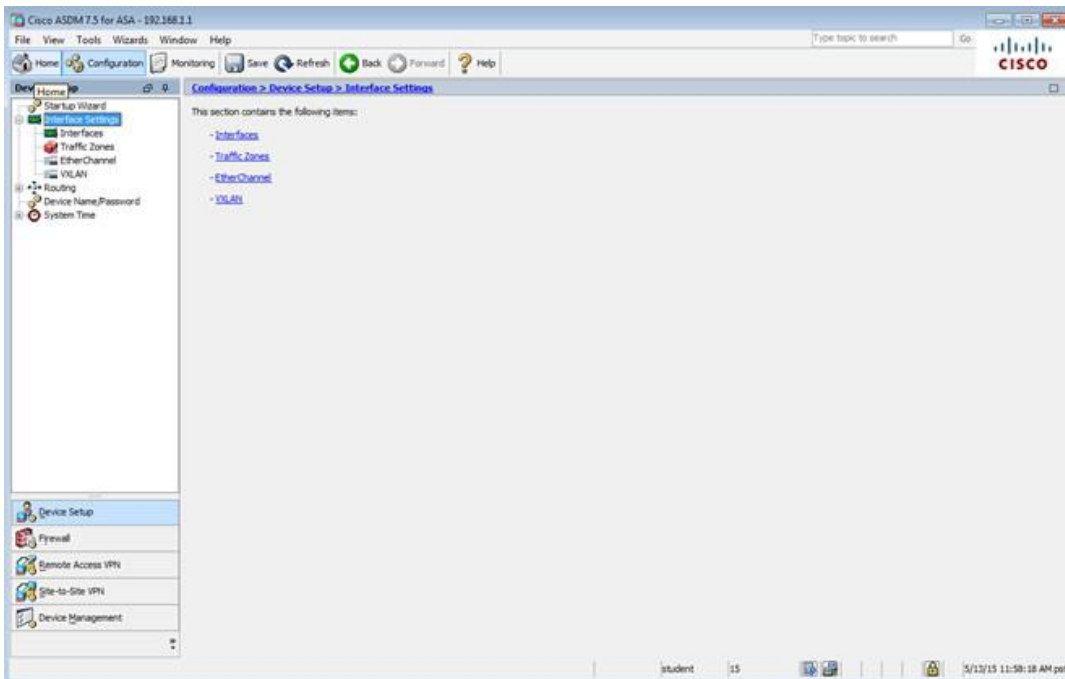
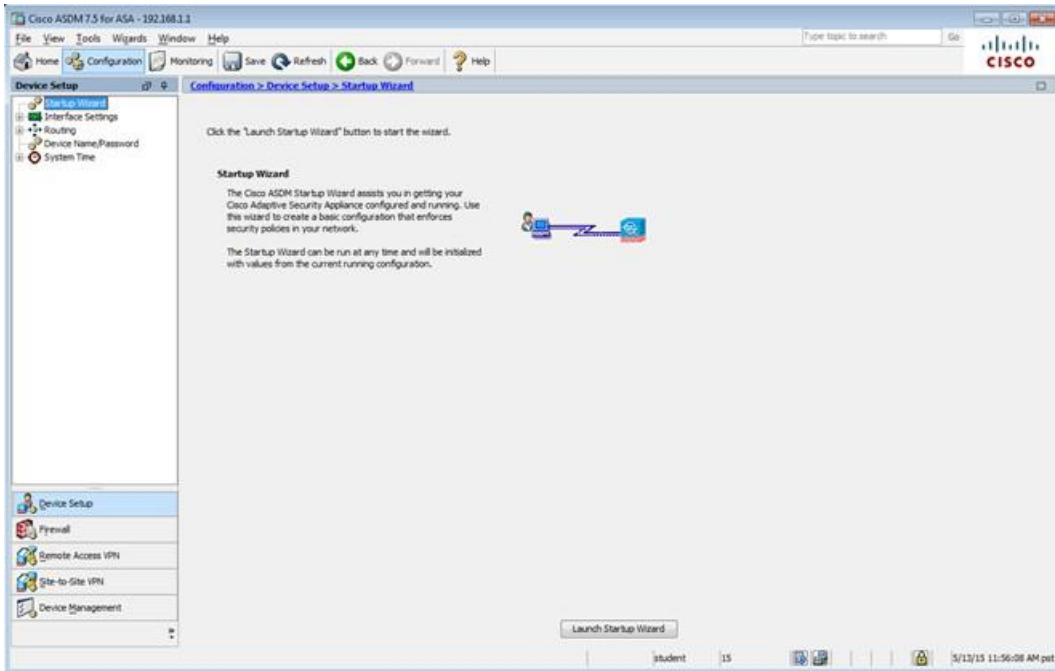
Refresh

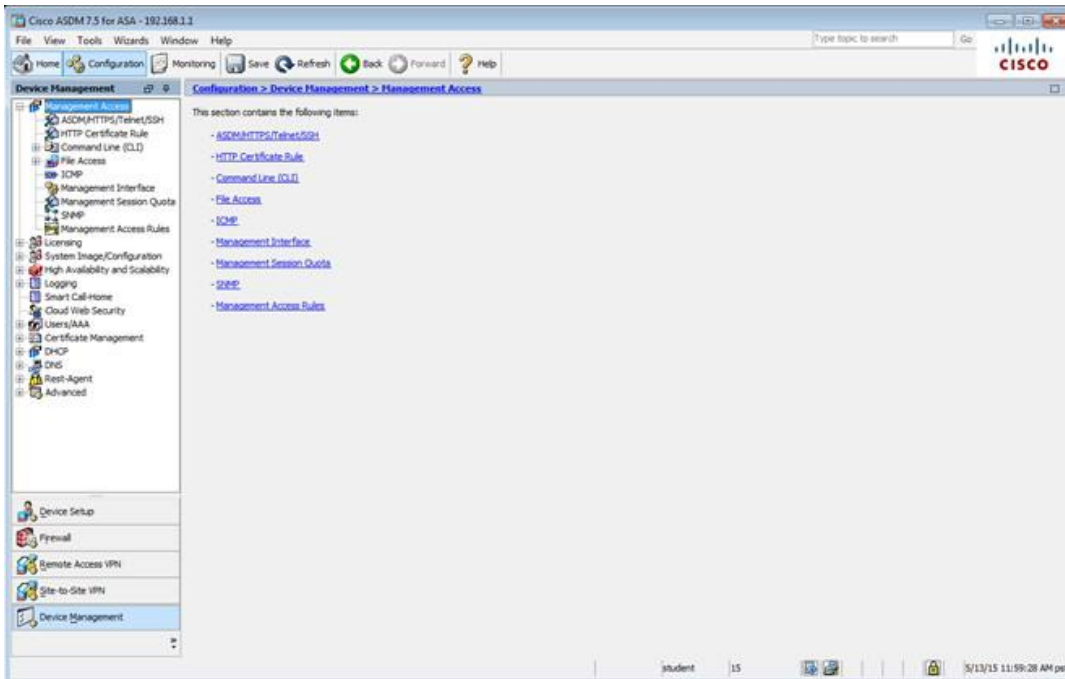
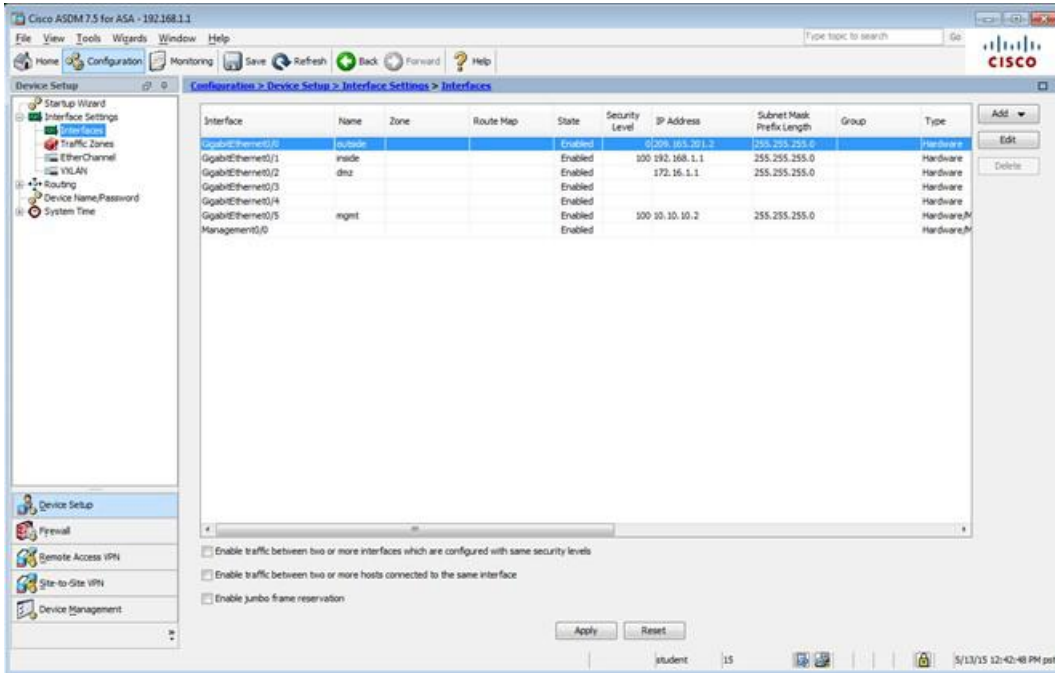
Last Updated: 5/19/15 9:33:12 AM

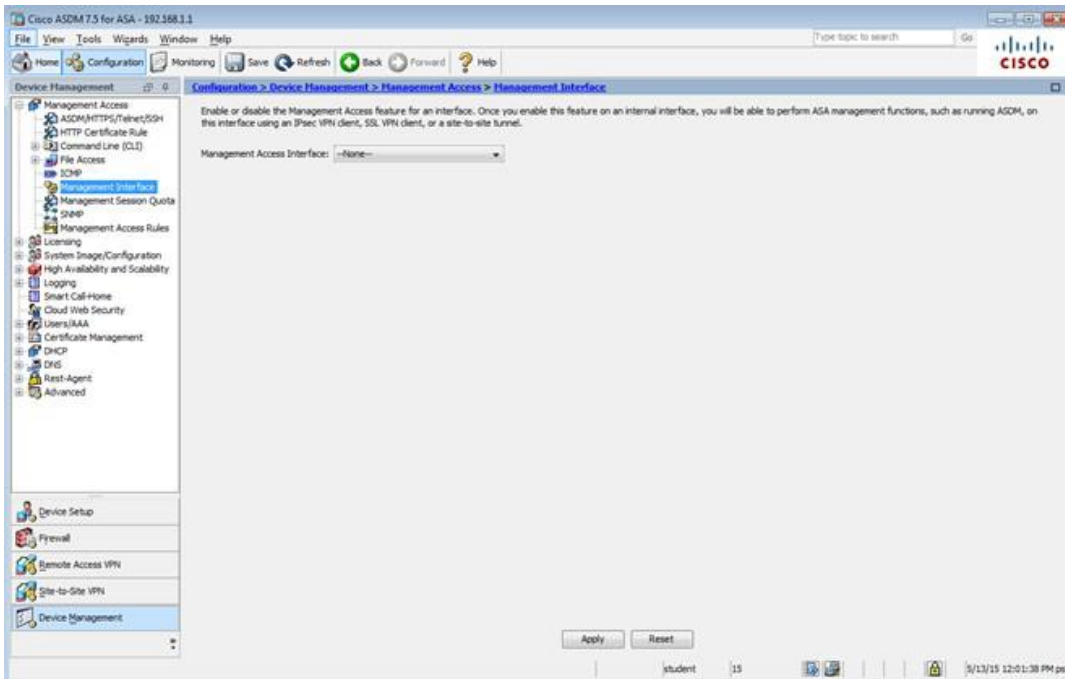
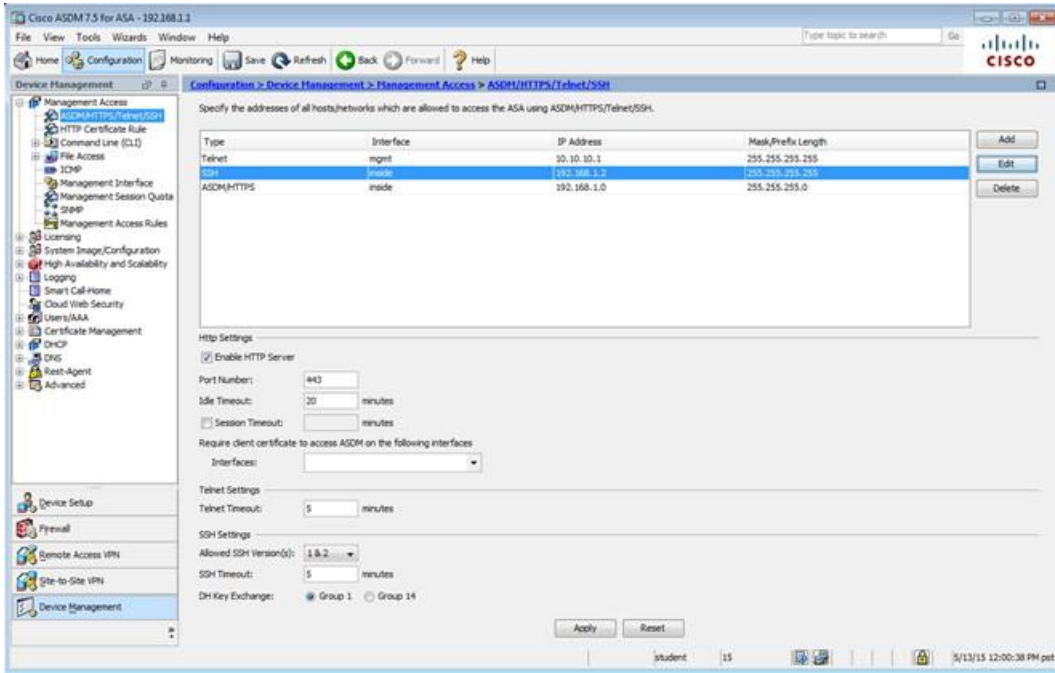
Data Refreshed Successfully.

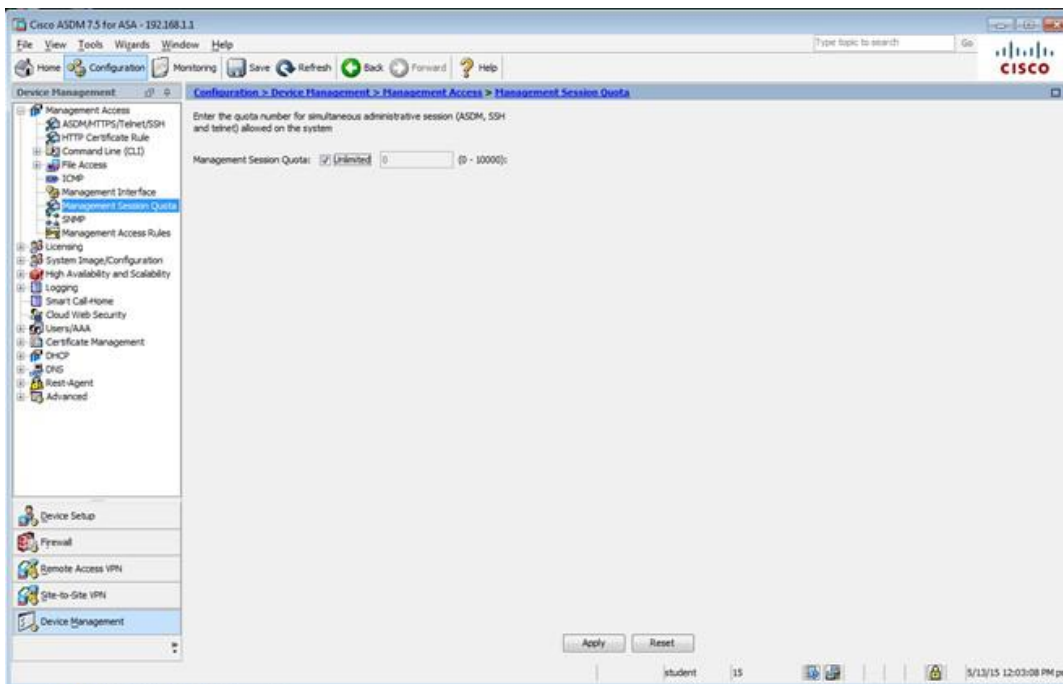
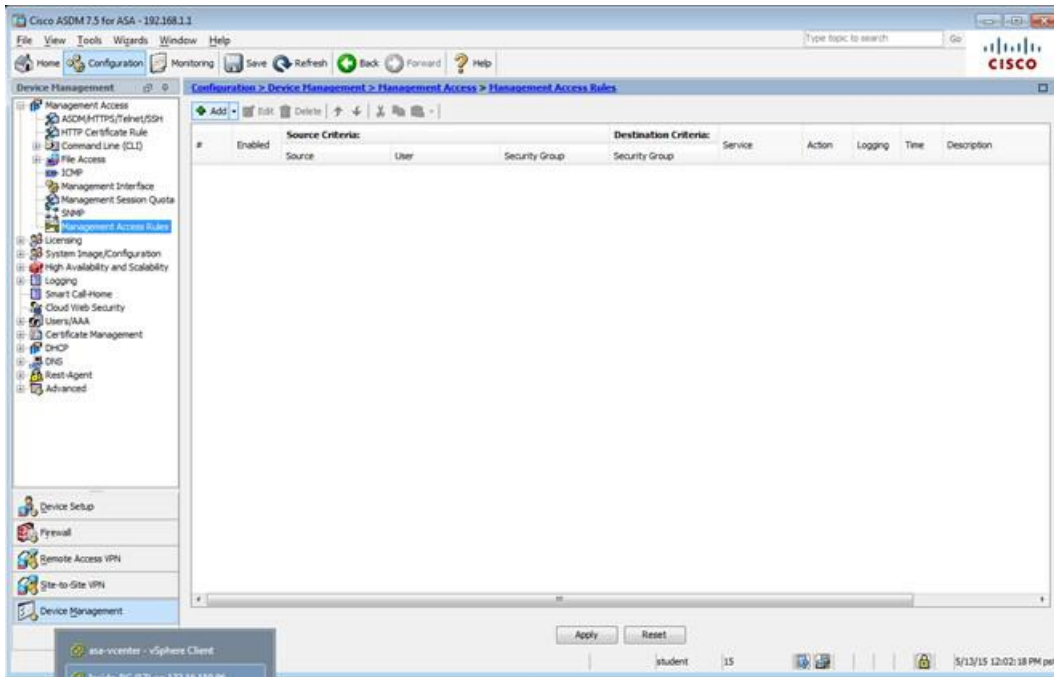
student 15

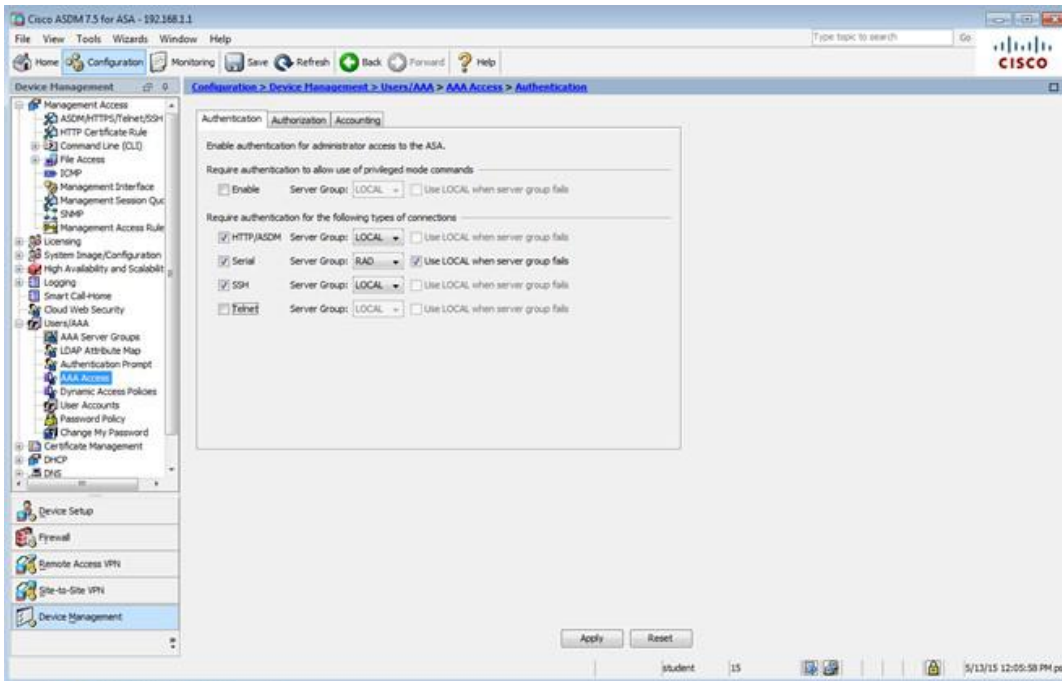
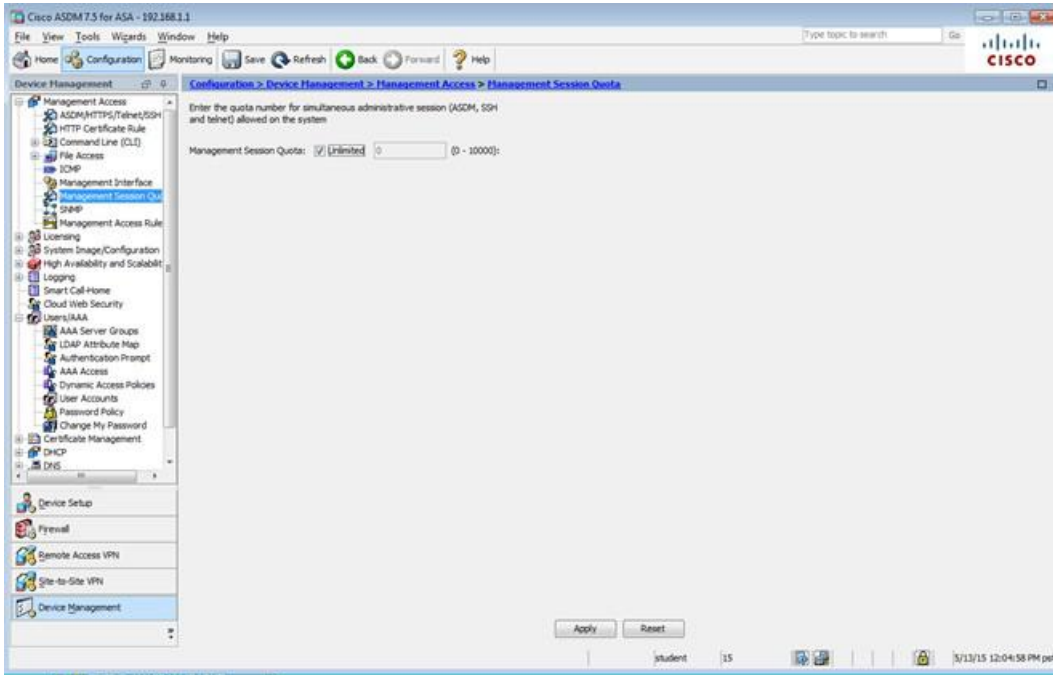
5/19/15 8:33:37 AM pst

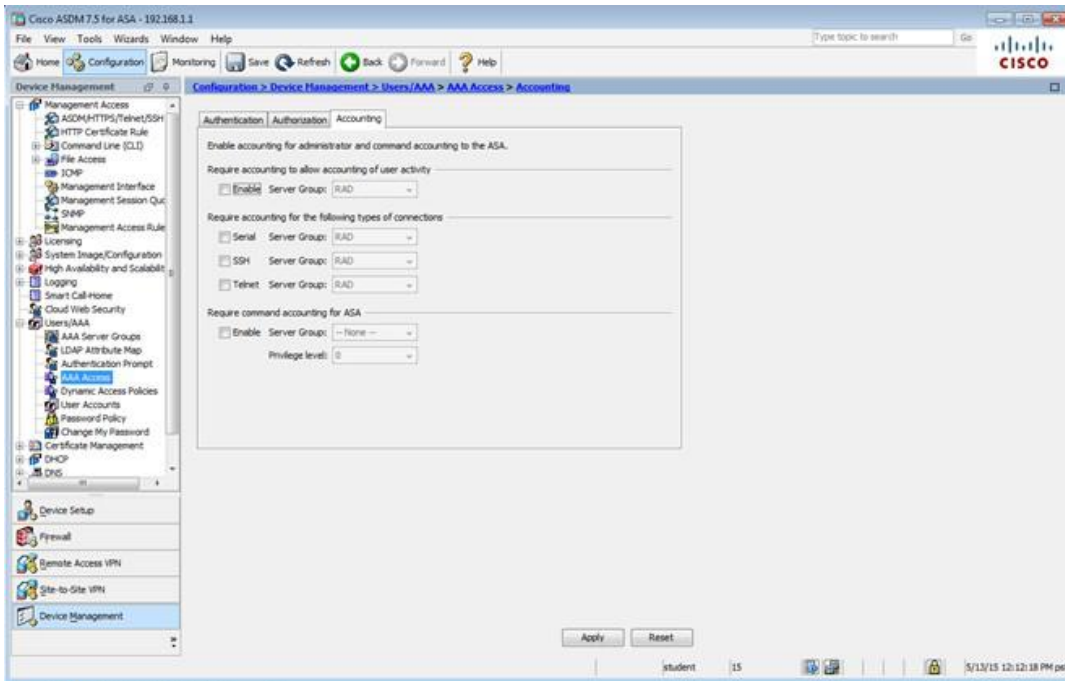
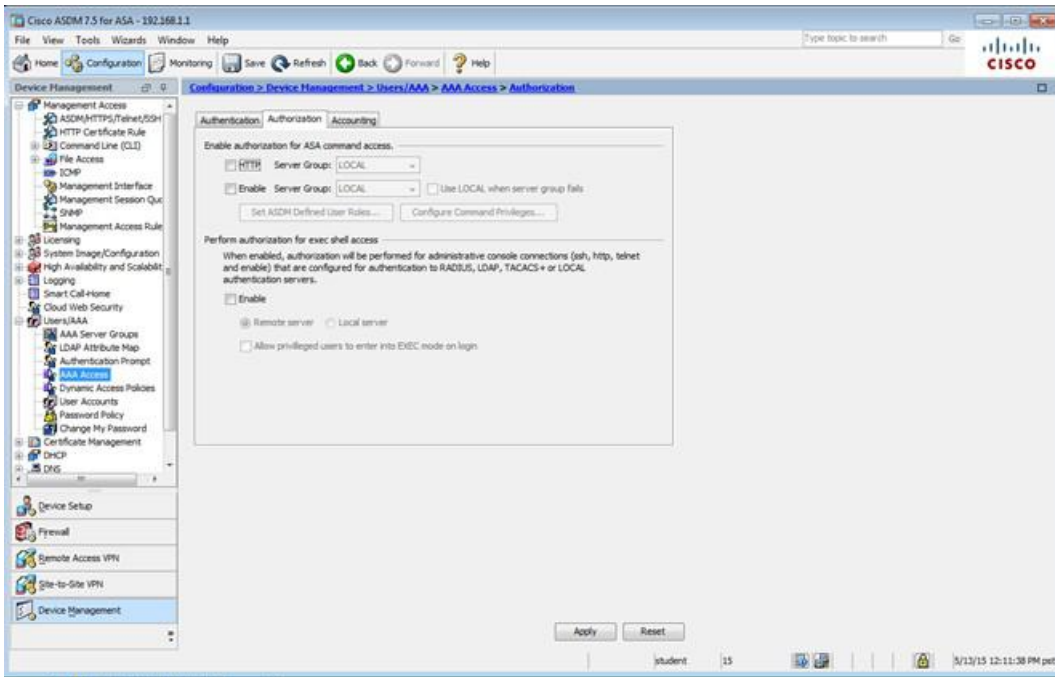


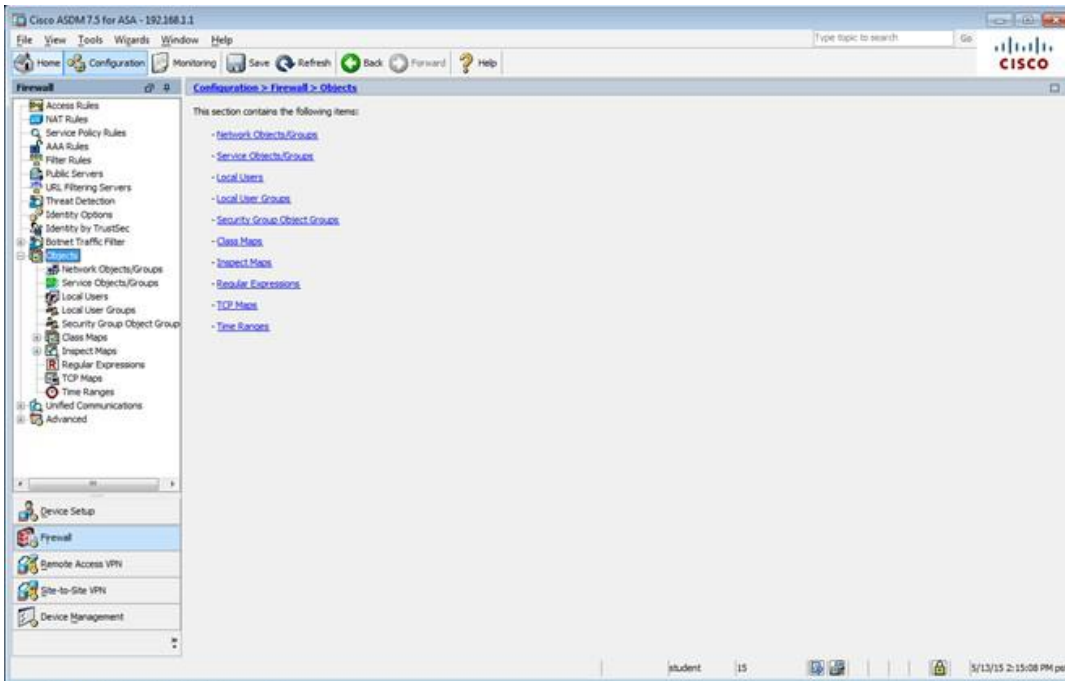


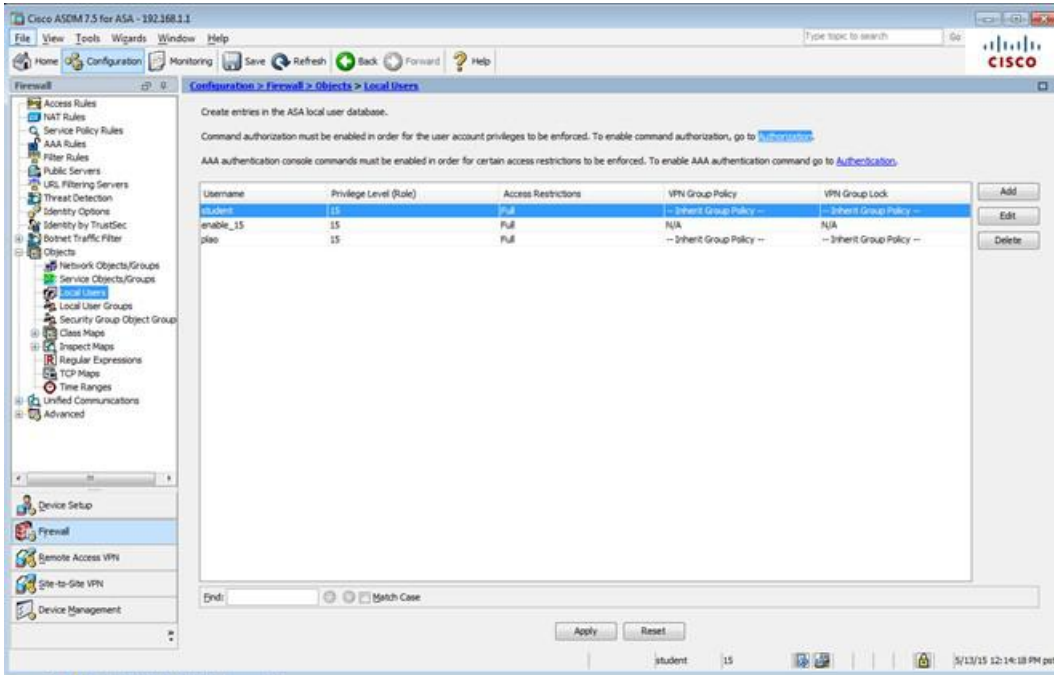












Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

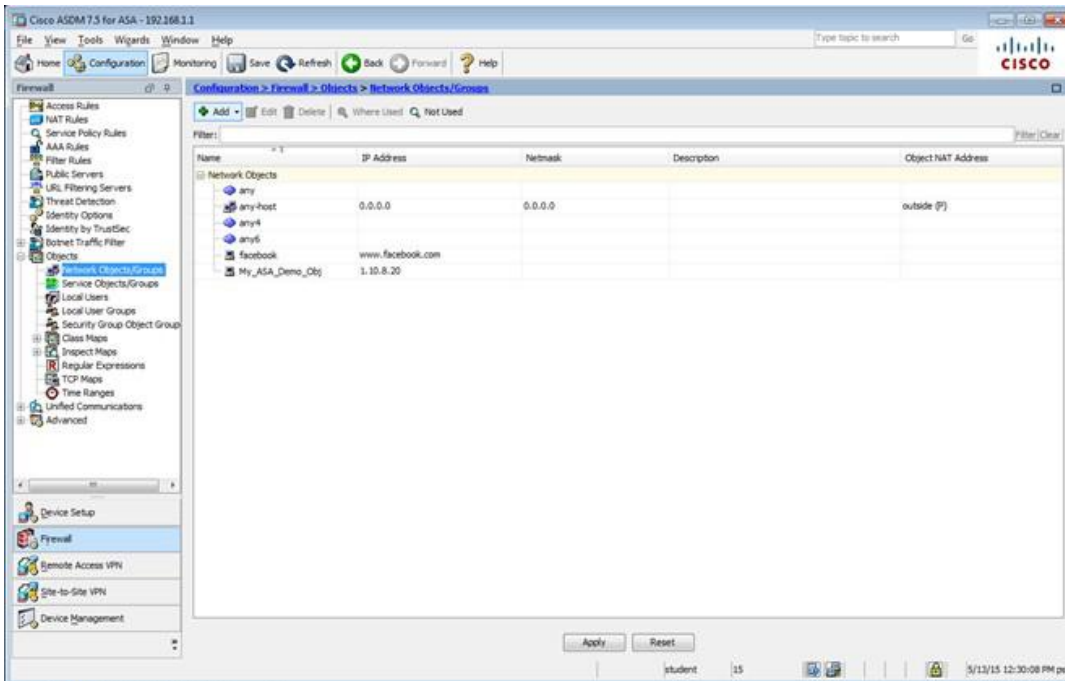
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

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 --

End: Match Case

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

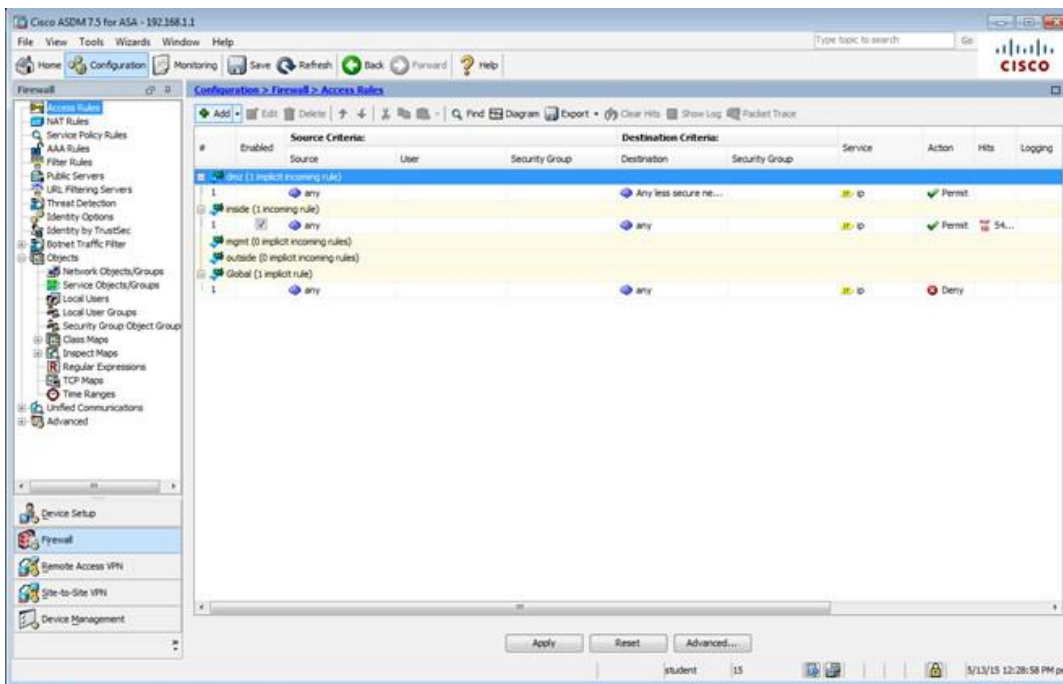
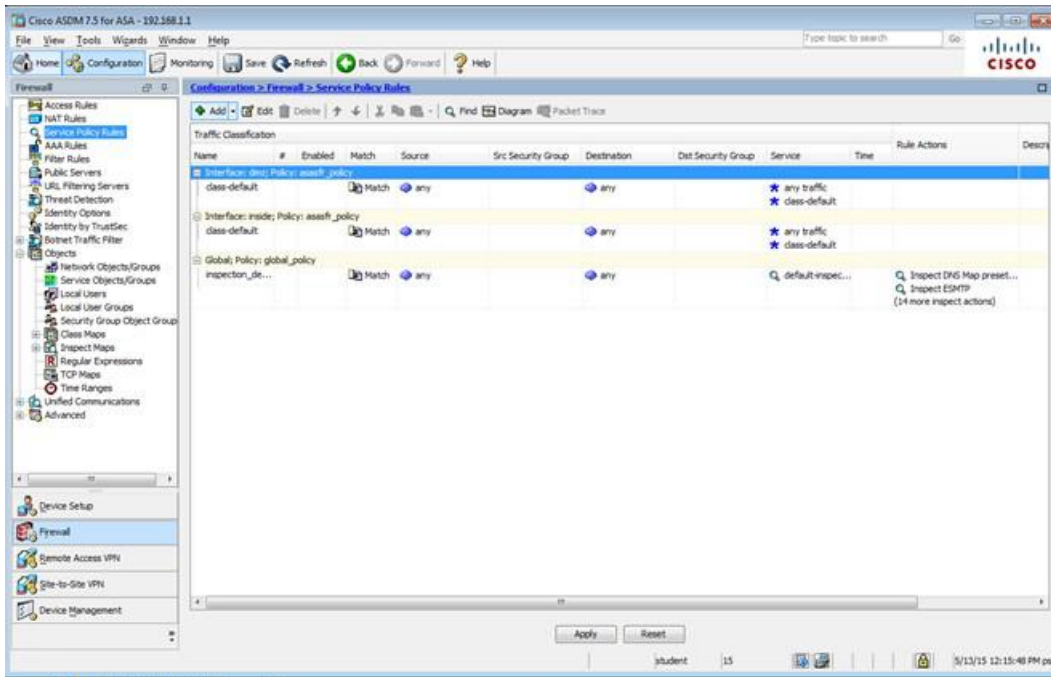
Configuration > Firewall > Objects > Network Objects/Groups

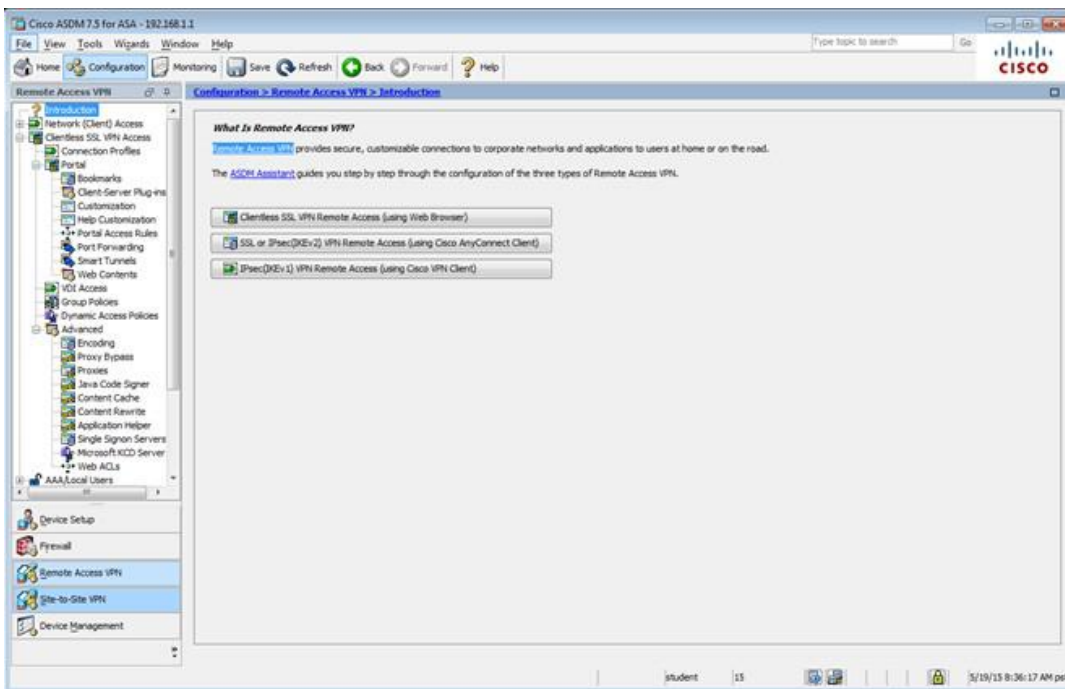
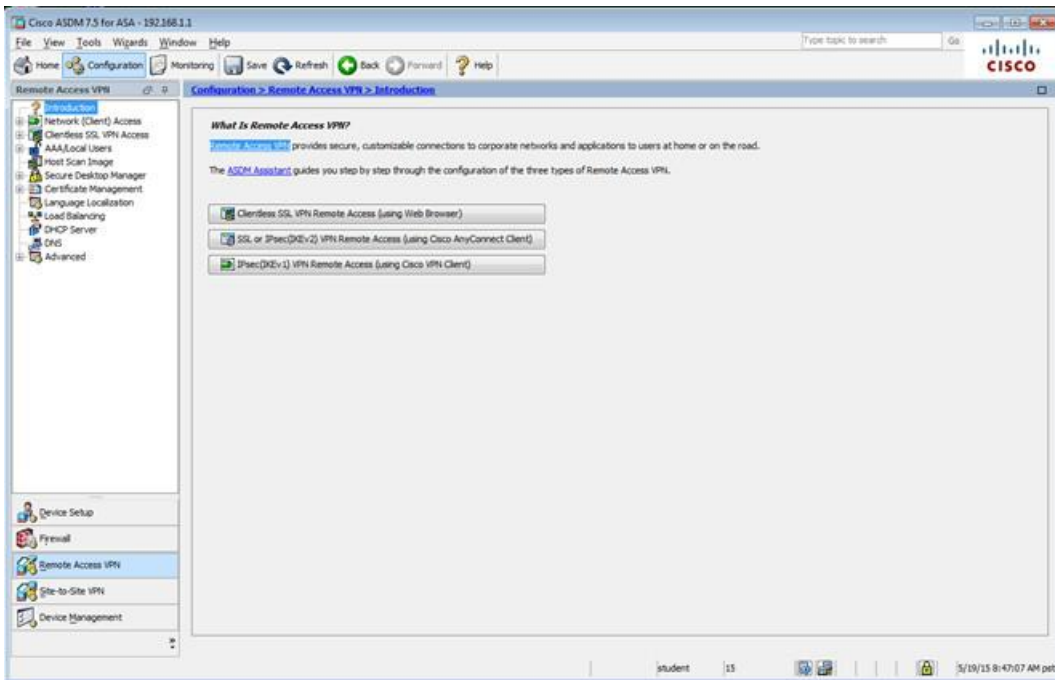
Filter: Filter/Clear

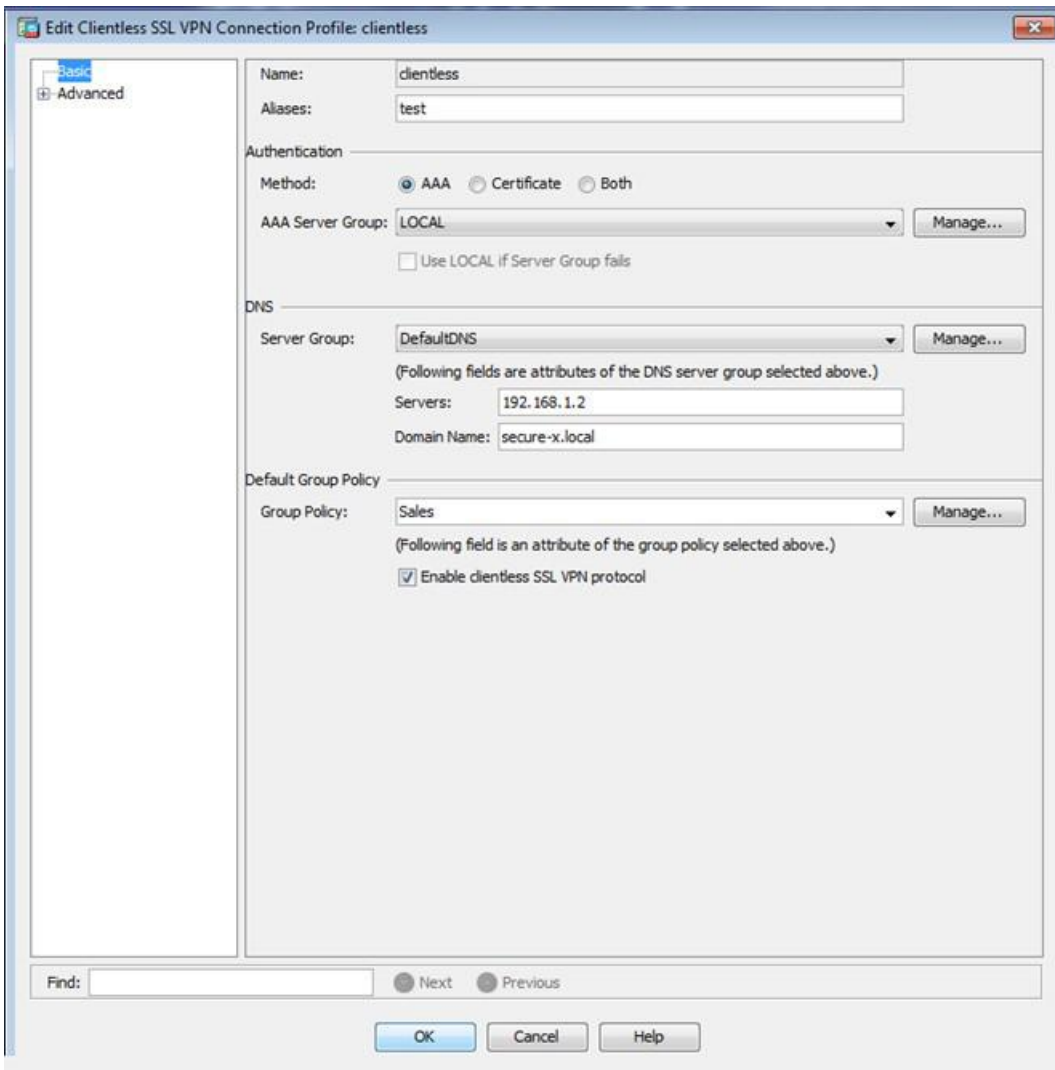
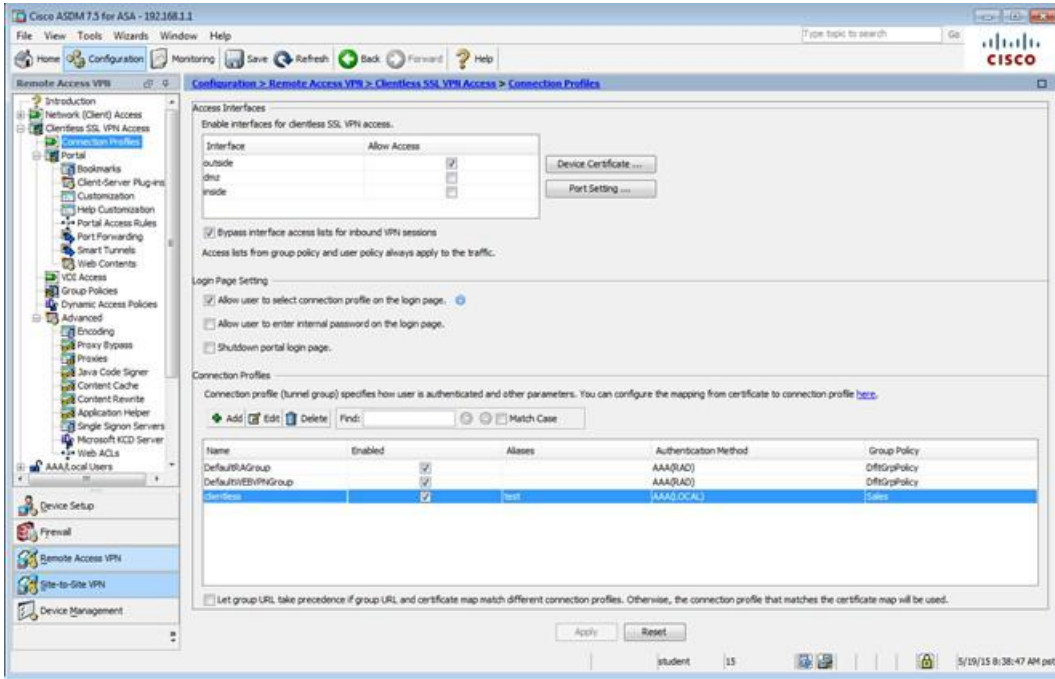
Name	IP Address	Network	Description	Object NAT Address
Network Objects				
any	0.0.0.0	0.0.0.0		outside (P)
any-host	0.0.0.0	0.0.0.0		
any4				
any6				
facebook	www.facebook.com			
My_ASA_Demo_Obj	1.10.8.20			

Apply Reset

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







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)

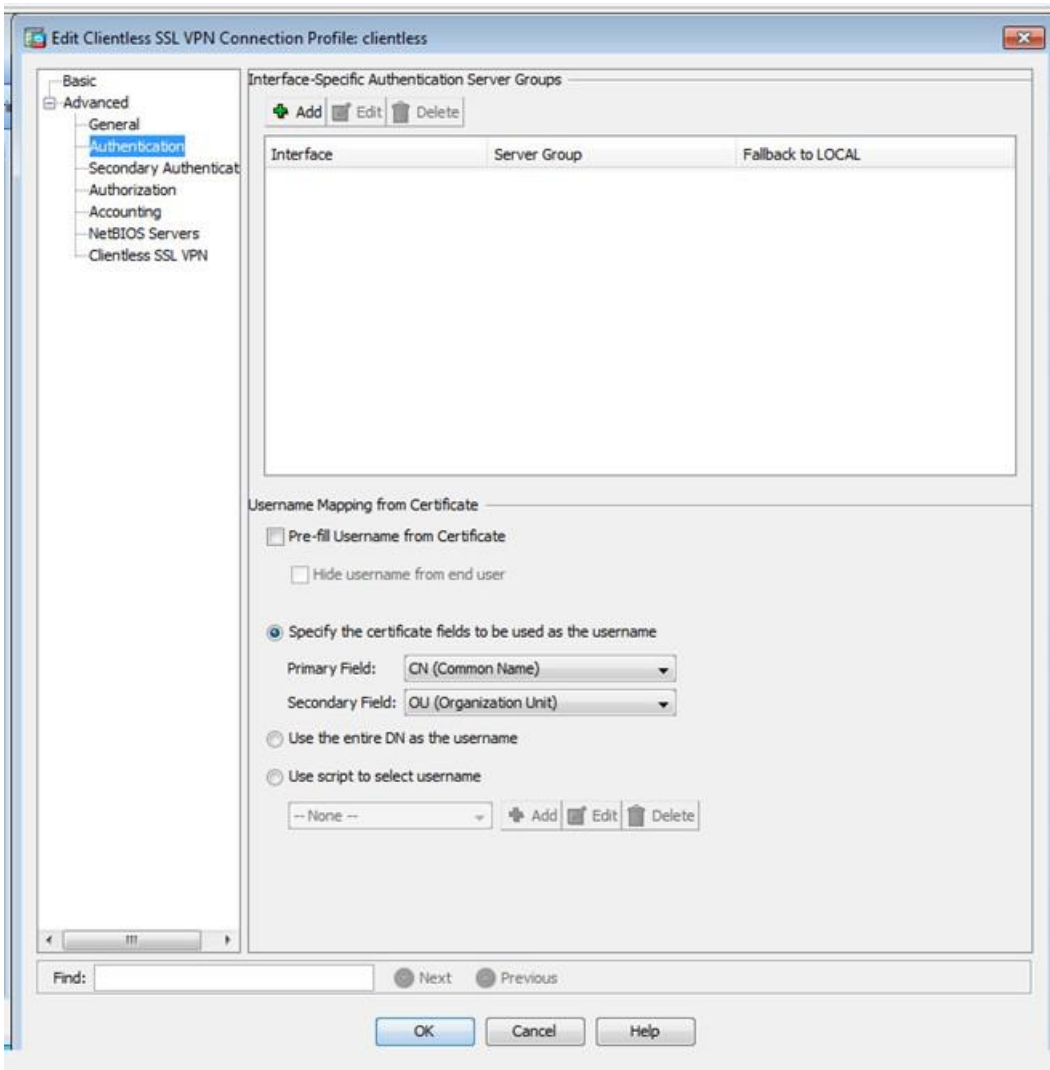
☒ Always run CSD

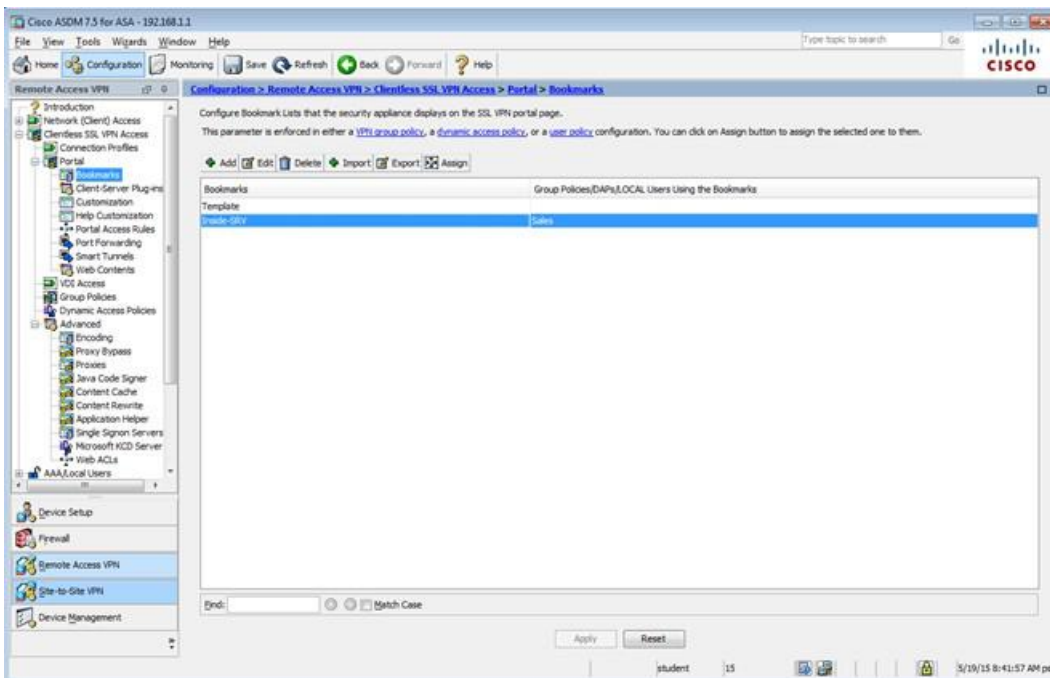
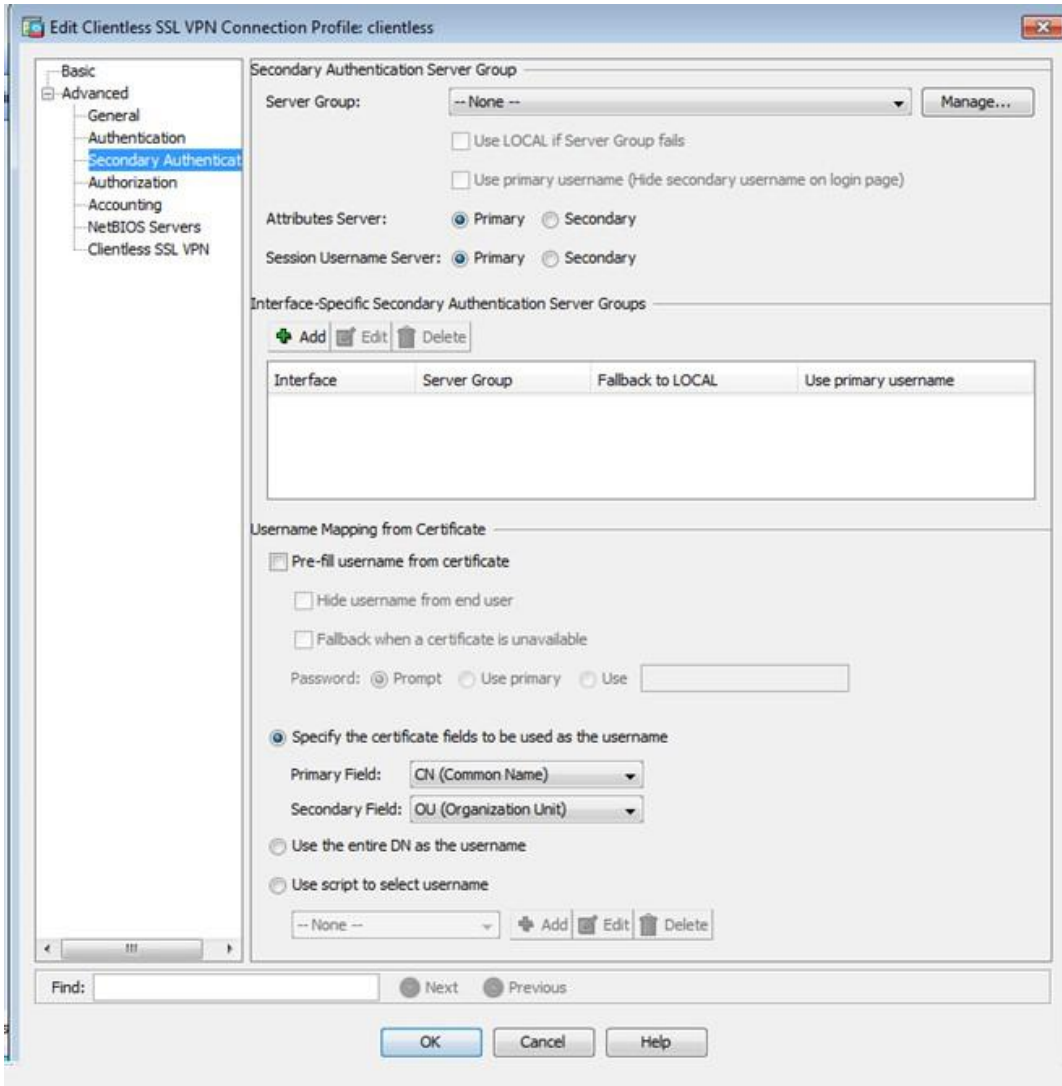
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

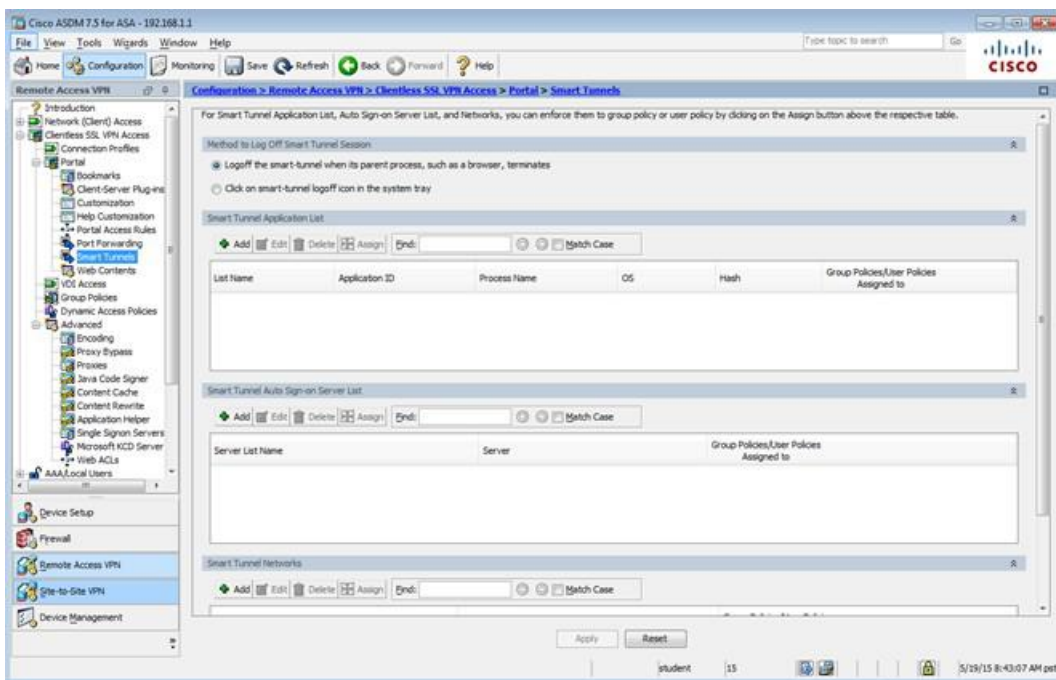
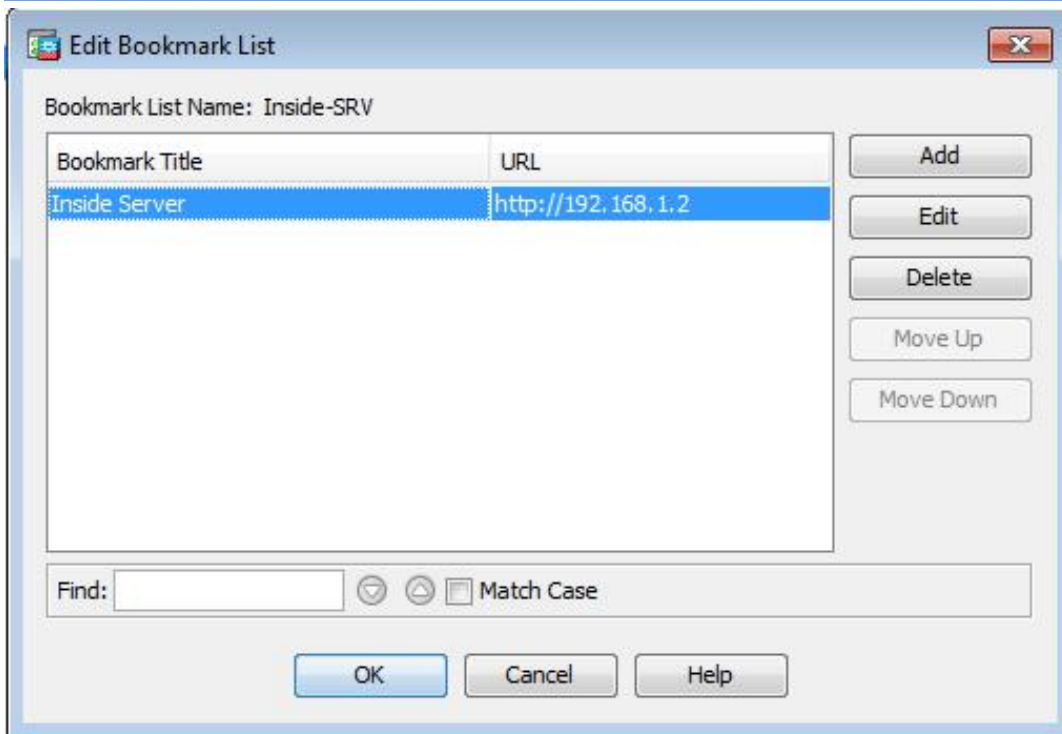
☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

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

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

Buttons: Add, Edit, Delete, Assign

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

Find: [] Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

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](#).

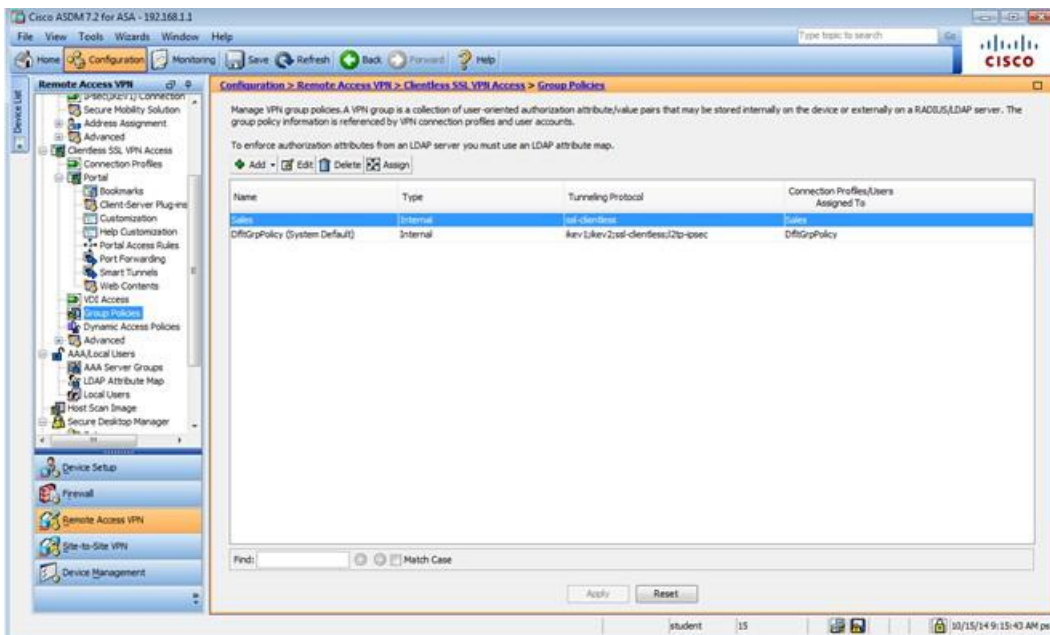
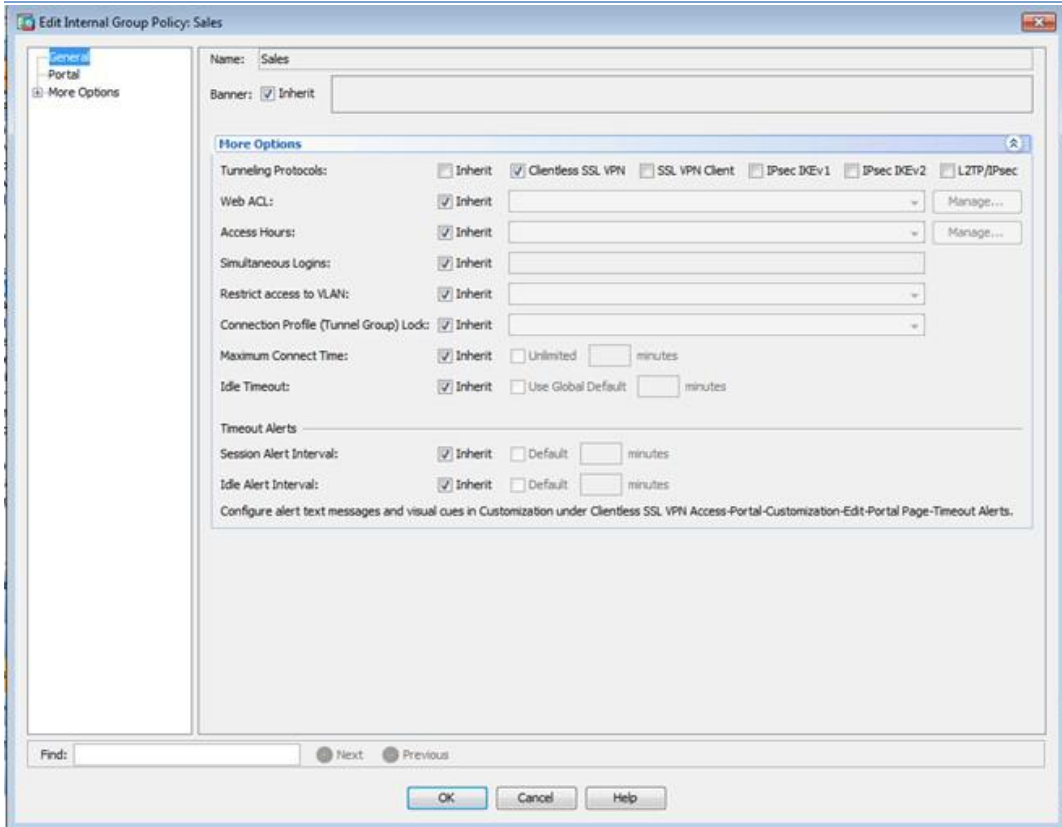
Buttons: Add, Edit, Delete, Assign

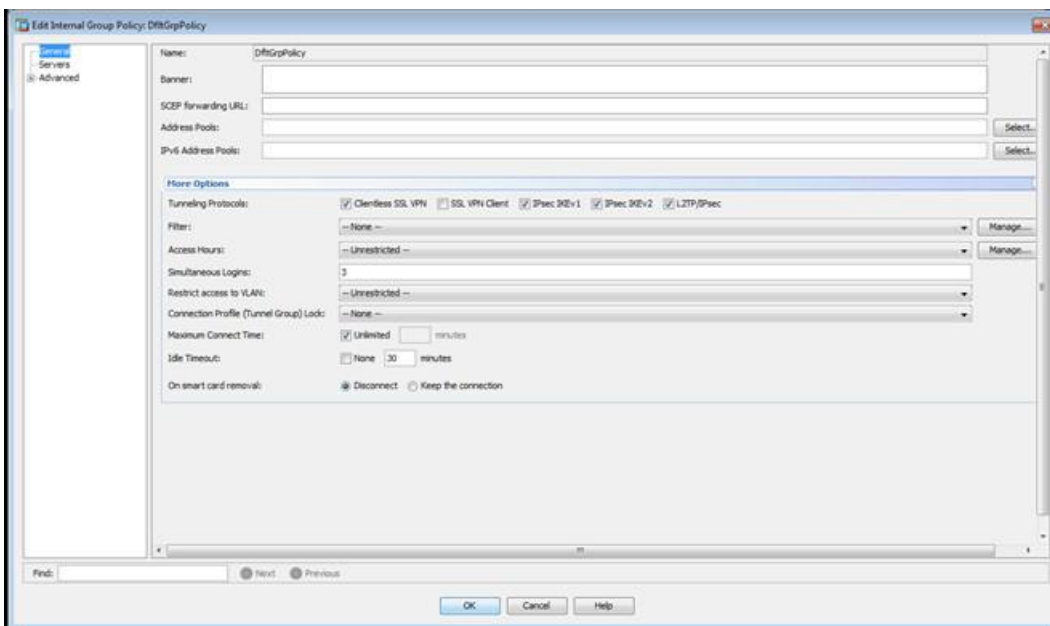
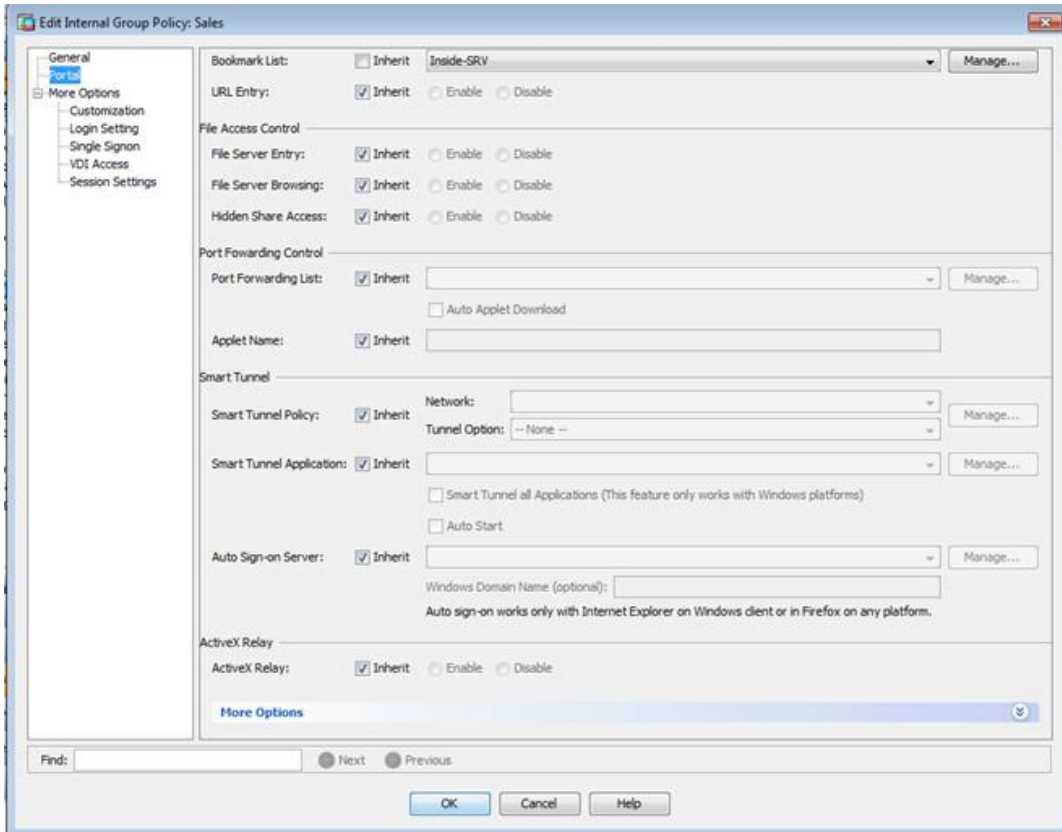
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	all-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1:rev2:ssl-clientless/2to-espsec	DefaultRAGroup/DefaultIL2LGroup/DefaultADP2NGroup/Def...

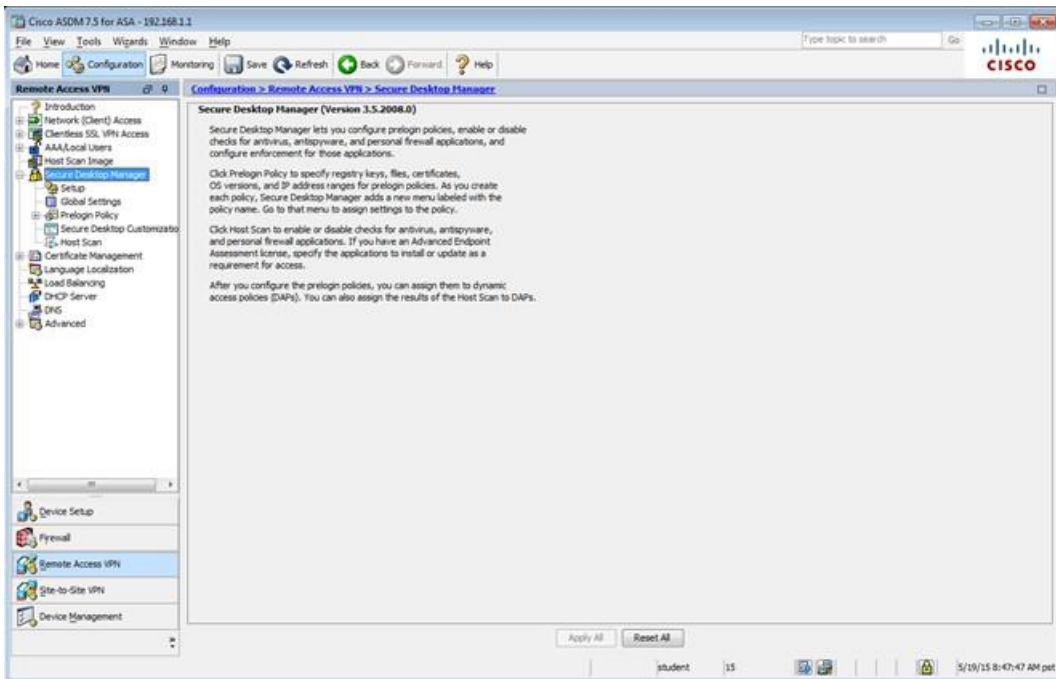
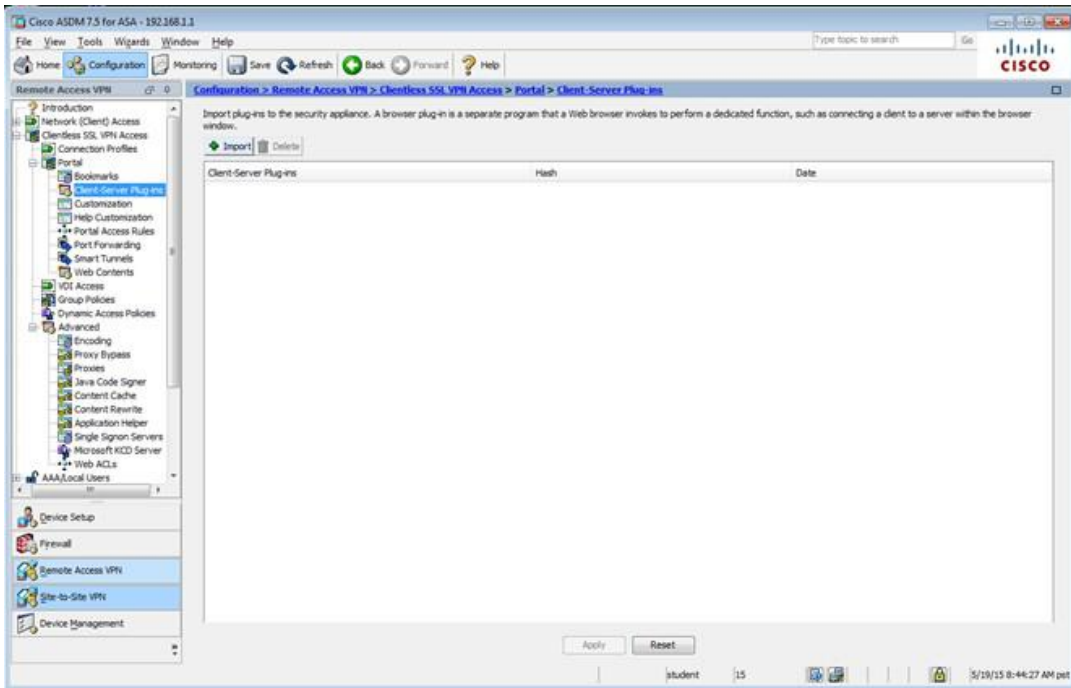
Find: [] Match Case

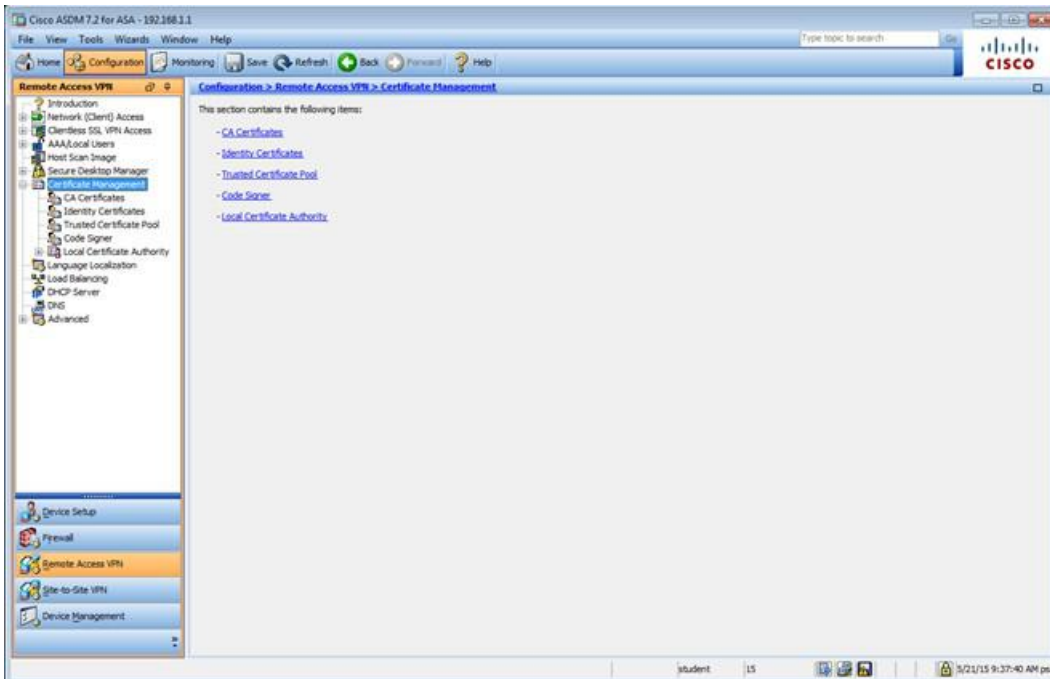
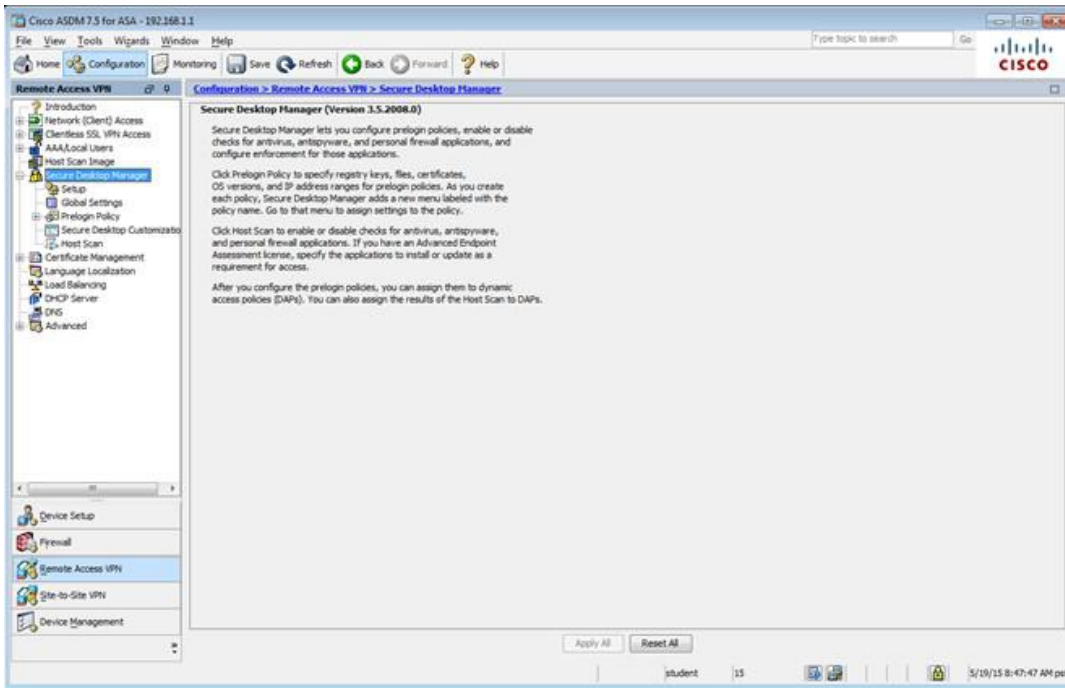
Apply Reset

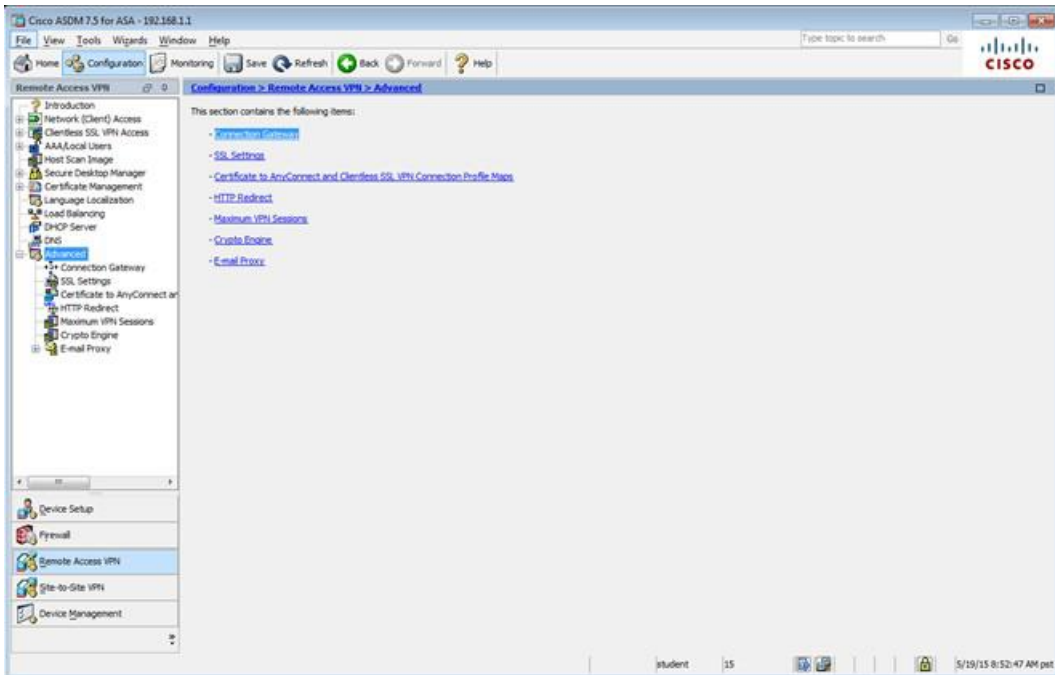
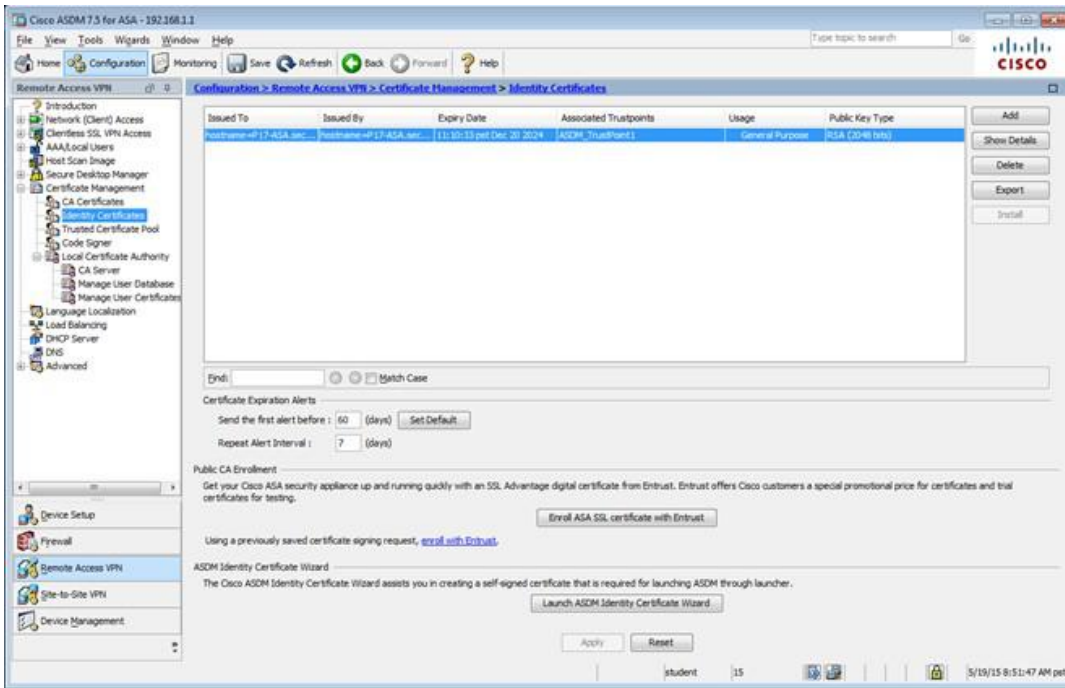
student 15 5/19/15 8:49:27 AM pst

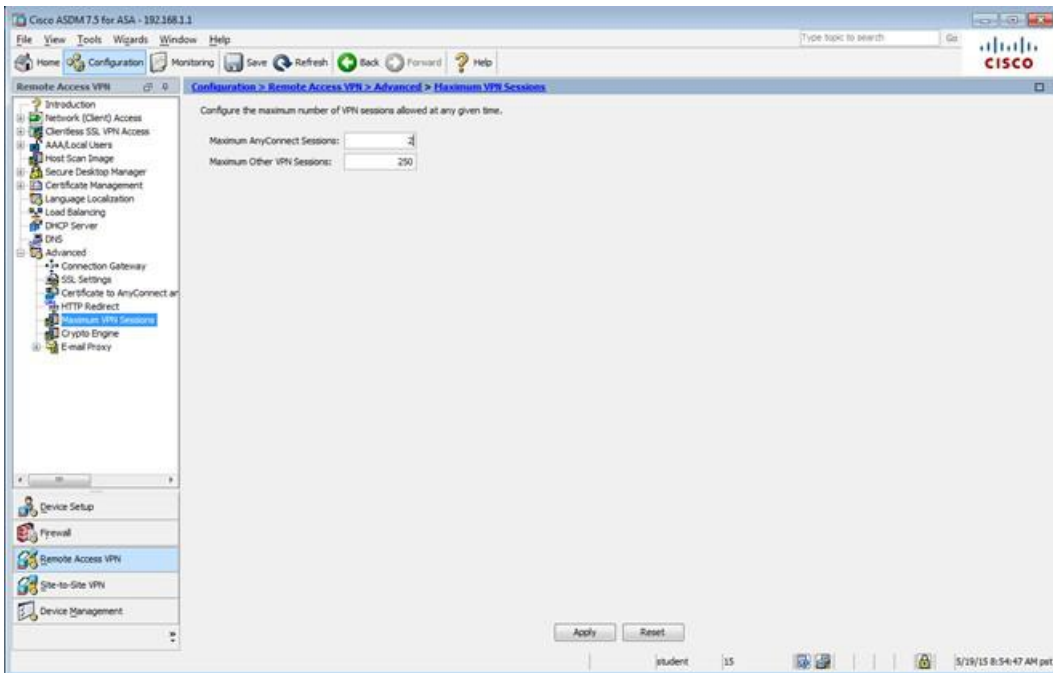
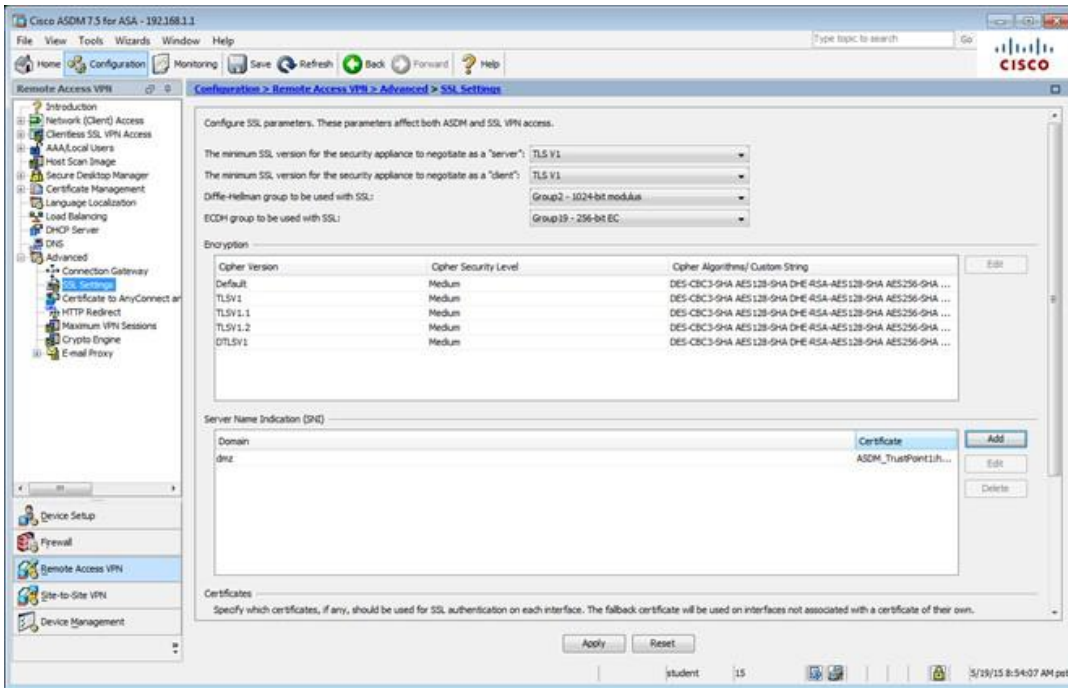












Configuration > Remote Access VPN > Network (Client) Access

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

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

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKEv2) protocols. Cisco VPN Client supports only IPsec(DKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
 You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based endpoint security policies.

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

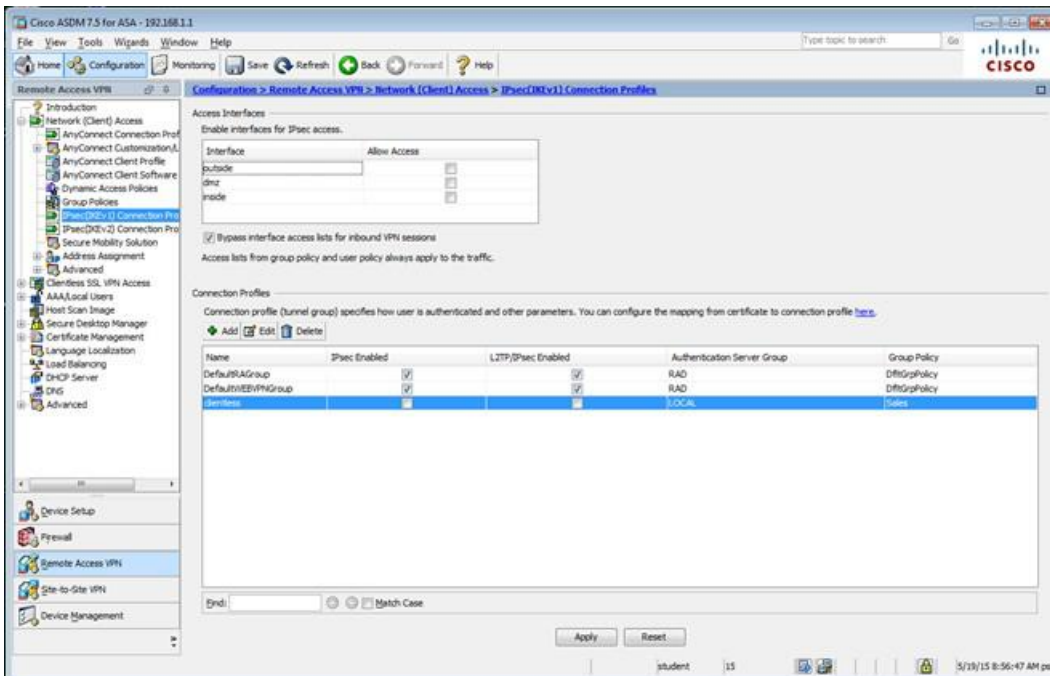
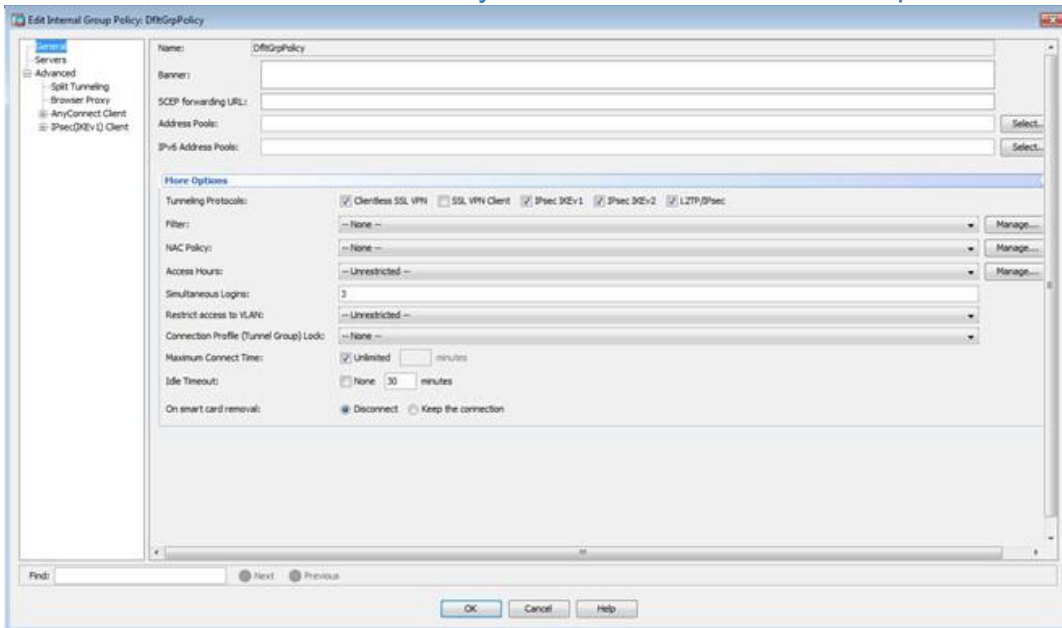
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization 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
InternetPolicy (System Default)	Internal	ssl-clientless	DefaultGroupDefault, 2, GroupDefault, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100

Find: Match Case

Apply Reset



The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AnyConnect Connection Profiles' configuration page. It includes sections for 'Access Interfaces', 'Login Page Setting', and 'Connection Profiles'.

Access Interfaces:

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below. SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

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

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
DefaultIVBGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
Clientless	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	test	AAA(LOCAL)	Sales

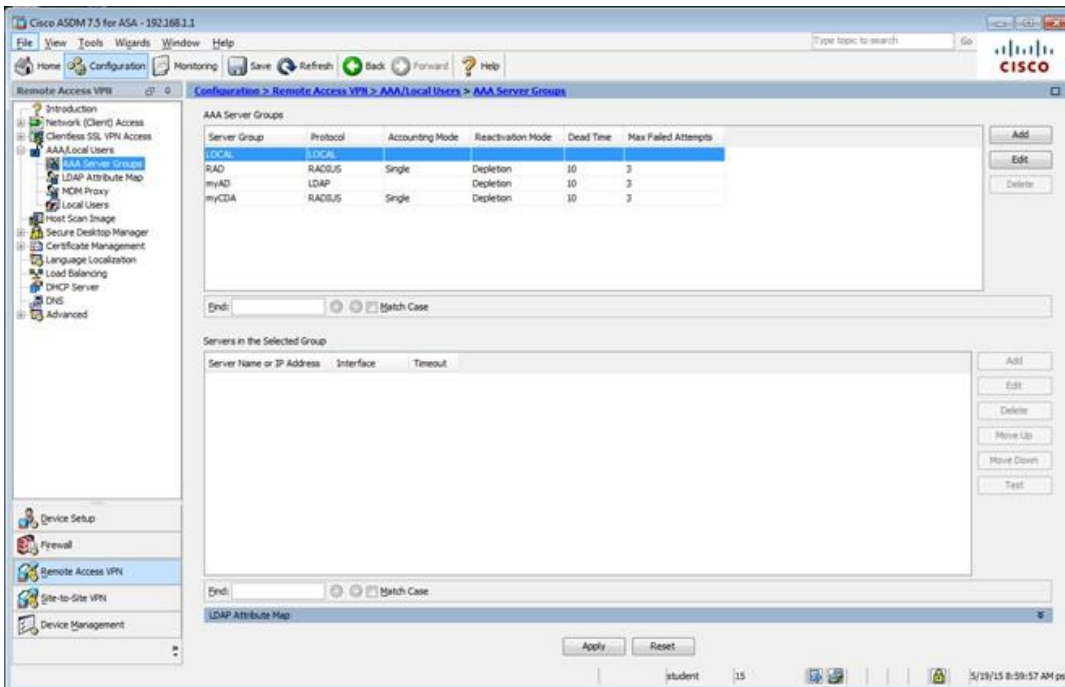
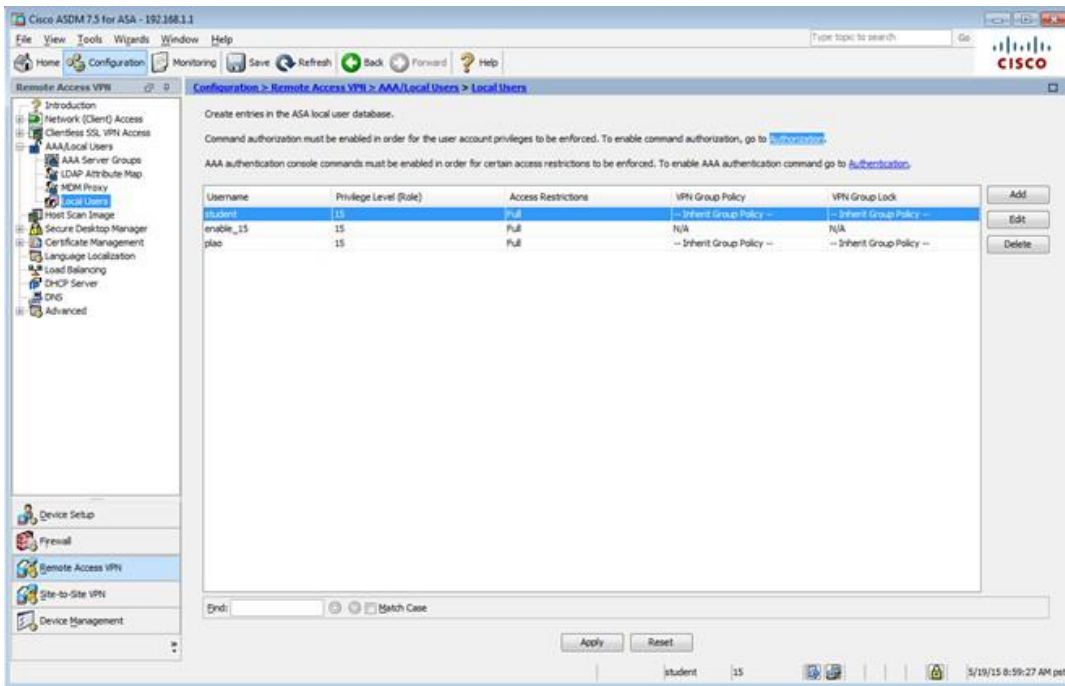
☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Buttons: Apply, Reset

The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AAA/Local Users' configuration page. It includes a list of items to be configured.

This section contains the following items:

- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users



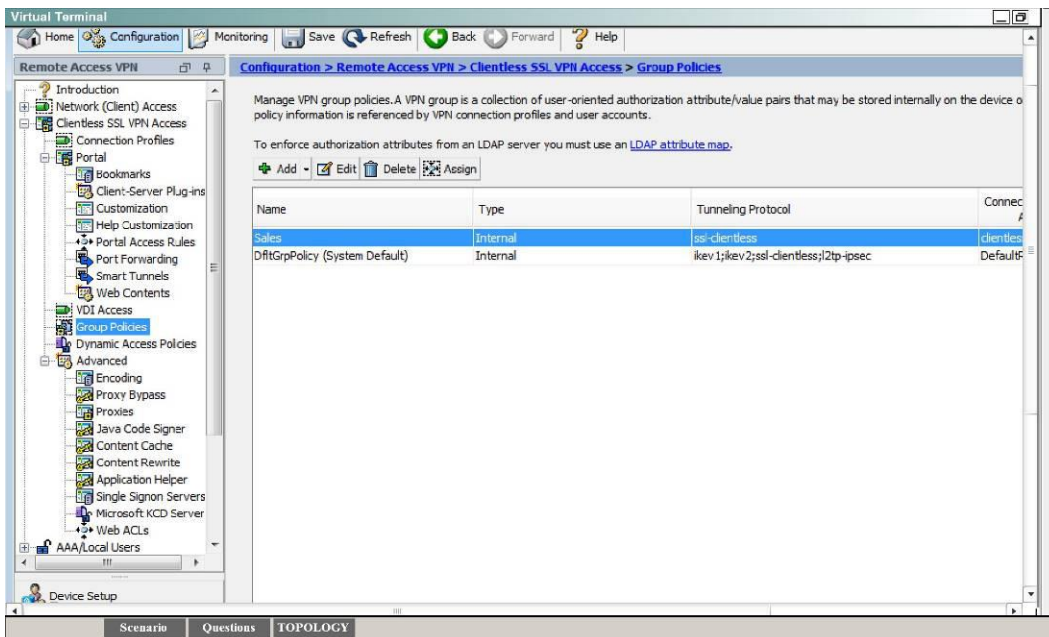
Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

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

Answer: A,D,E,F

Explanation:

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



187. What IPSec mode is used to encrypt traffic between a server and VPN endpoint?

- A. tunnel
- B. Trunk
- C. Aggregated
- D. Quick
- E. Transport

Answer: E

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

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

Answer: A



189. Which type of security control is defense in depth?

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

Answer: A

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

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

Answer: A,B

191. Which statement about IOS privilege levels is true?

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

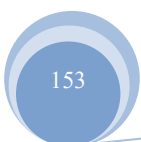
Answer: A

192. A proxy firewall protects against which type of attack?

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

Answer: A

193. Which two options are the primary deployment models for mobile device management? (Choose two)





- A. Single-site
- B. hybrid cloud-based
- C. on-premises
- D. Cloud based
- E. Multisite

Answer: C,D

Explanation: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_MDM_Int.pdf

194. DRAG DROP

Drag the recommendations on the left to the Cryptographic Algorithms on the right. Options will be used more than once.

Avoid	DES
Legacy	3DES
	MD5
	SHA-1
	HMAC-MD5

Answer:

Avoid	Avoid
Legacy	Legacy
	Avoid
	Legacy
	Legacy



Explanation: DES = Avoid 3DES = Legacy

MD5 = Avoid SHA-1 = Legacy

HMAC-MD5 = Legacy

<https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html>

195. What mechanism does asymmetric cryptography use to secure data?

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

Answer: A

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

(Choose two.)

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

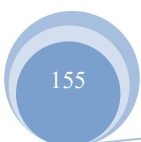
Answer: B,E

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

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

Answer: A

198. What encryption technology has broadest platform support





- A. hardware
- B. middleware
- C. Software
- D. File level

Answer: C

199. SSL certificates are issued by Certificate Authority(CA) are?

- A. Trusted root
- B. Not trusted

Answer: A

200. Which type of PVLAN port allows communication from all port types?

- A. isolated
- B. community
- C. in-line
- D. promiscuous

Answer: D

201. 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

Answer: A

202. 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.

Answer: A

203. 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

Answer: D

204. What does the command `crypto isakmp nat-traversal` do?

- A. Enables udp port 4500 on all IPsec enabled interfaces
- B. rebooting the ASA the global command

Answer: A

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

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

Answer: A

206. Which type of social-engineering attacks uses normal telephone service as the attack vector?

- A. vishing
- B. phishing
- C. smishing



D. war dialing

Answer: B

207. Which IPS mode is less secure than other options but allows optimal network throughput?

A. Promiscuous mode

B. inline mode

C. transparent mode

D. inline-bypass mode

Answer: A

Explanation: The recommended IPS deployment mode depends on the goals and policies of the enterprise.

IPS inline mode is more secure because of its ability to stop malicious traffic in real-time, however it may impact traffic throughput if not properly designed or sized. Conversely, IPS promiscuous mode has less impact on traffic throughput but is less secure because there may be a delay in reacting to the malicious traffic. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/safesmallentnetworks.html

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

A. show crypto map

B. show crypto ipsec sa

C. show crypto isakmp sa

D. show crypto engine connection active

Answer: C

209. Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

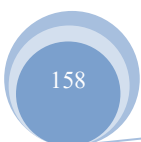
A. Select the interface(s) to apply the IPS rule.

B. Select the traffic flow direction that should be applied by the IPS rule.

C. Add or remove IPS alerts actions based on the risk rating.

D. Specify the signature file and the Cisco public key.

E. Select the IPS bypass mode (fail-open or fail-close).



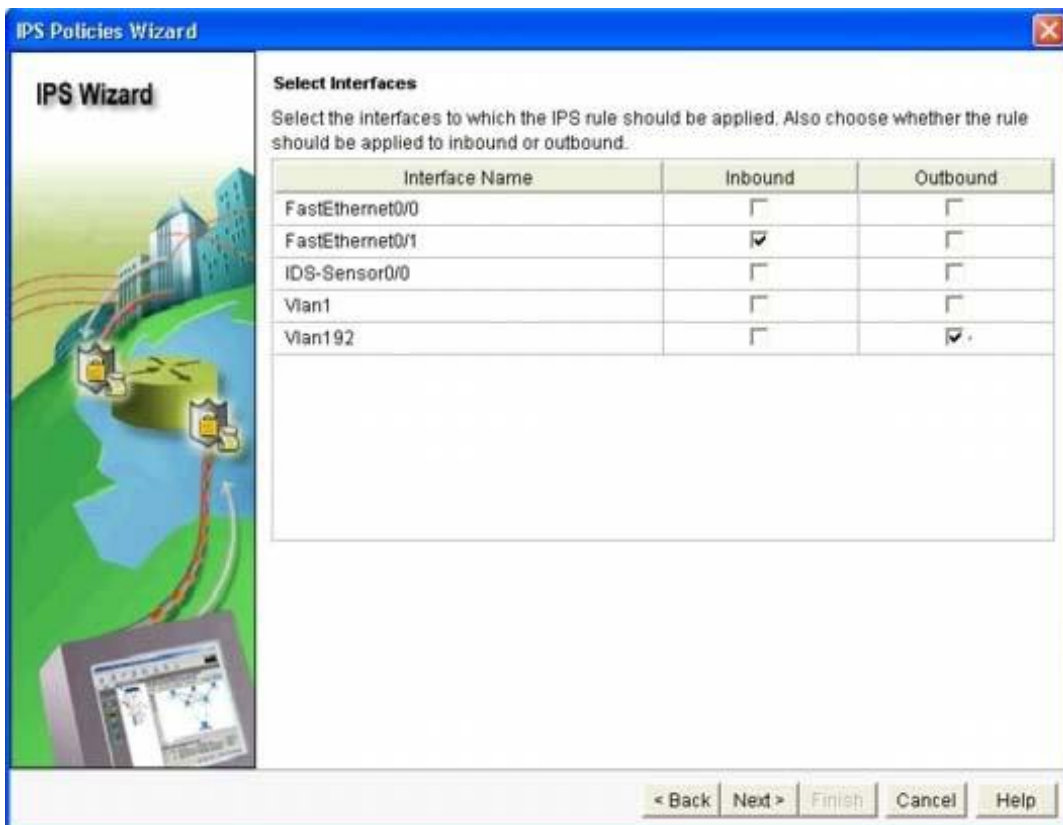
F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

Answer: A,B,D,F

Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Step 11. At the 'Select Interfaces' screen, select the interface and the direction that IOS IPS will be applied to, then click 'Next' to continue.



Step 12. At the 'IPS Policies Wizard' screen, in the 'Signature File' section, select the first radio button "Specify the signature file you want to use with IOS IPS", then click the "..." button to bring up a dialog box to specify the location of the signature package file, which will be the directory specified in Step 6. In this example, we use tftp to download the signature package to the router.



Step 13. In the 'Configure Public Key' section, enter 'realm-cisco.pub' in the 'Name' text field, then copy and paste the following public key's key-string in the 'Key' text field. This public key can be downloaded from

Cisco.com at: <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>. Click 'Next' to continue.

30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3

6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87

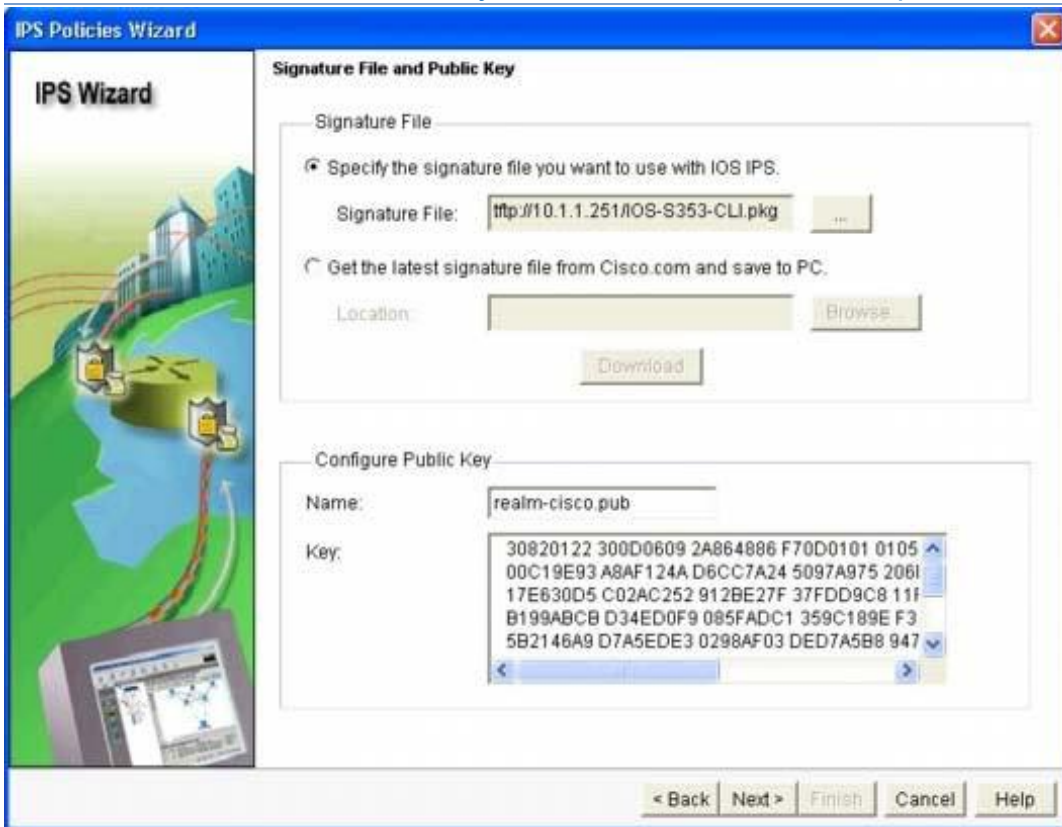
89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001



210. When AAA login authentication is configured on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can still log in to the router in case the external AAA server fails? (Choose two.)

- A. group RADIUS
- B. group TACACS+
- C. local
- D. krb5
- E. enable
- F. if-authenticated

Answer: C,E

Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html TACACS+ Authentication Examples

The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

```
aaa new-model
```

```
aaa authentication ppp test group tacacs+ local tacacs-server host 10.1.2.3
```



tacacs-server key goaway interface serial 0

ppp authentication chap pap test

The lines in the preceding sample configuration are defined as follows:

- The `aaa new-model` command enables the AAA security services.
- The `aaa authentication` command defines a method list, "test," to be used on serial interfaces running PPP.

The keyword `group tacacs+` means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword `local` indicates that authentication will be attempted using the local database on the network access server.

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml Authentication Start to configure TAC+ on the router.

Enter enable mode and type `configure terminal` before the command set. This command syntax ensures that you are not locked out of the router initially, providing the `tac_plus_executable` is not running:

!--- Turn on TAC+. `aaa new-model`

`enable password whatever`

!--- These are lists of authentication methods.

!--- "linmethod", "vtymethod", "conmethod", and

!--- so on are names of lists, and the methods

!--- listed on the same lines are the methods

!--- in the order to be tried. As used here, if

!--- authentication fails due to the

!--- `tac_plus_executable` not being started, the

!--- `enable password` is accepted because

!--- it is in each list.

!

`aaa authentication login linmethod tacacs+ enable`
`aaa authentication login vtymethod tacacs+ enable`
`aaa authentication login conmethod tacacs+ enable`

211. By default, how does a zone-based firewall handle traffic to and from the self zone?

- A. It permits all traffic without inspection.
- B. It inspects all traffic to determine how it is handled.



- C. it permits all traffic after inspection
- D. it drops all traffic.

Answer: C

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

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

Answer: D

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

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

Answer: A

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

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

Answer: A

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

- A. FlexConfig
- B. Device Manager



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

Answer: D

216. 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.

Answer: A

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

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

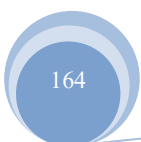
Answer: A

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

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

Answer: A,B,C

219. Which three statements about Cisco host-based IPS solutions 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.

Answer: A,B,C

220. 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.

Answer: A

221. Refer to the exhibit.

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

What is the effect of the given command?

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

Answer: A

222. Which syslog severity level is level number 7?

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



Answer: D

223. What is a benefit of a web application firewall?

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

Answer: A

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

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

Answer: C,D

225. 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.

Answer: A,B

226. 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.

Answer: A,B,C

227. Refer to the exhibit.

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

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

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

With which NTP server has the router synchronized?

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

Answer: A

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

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

Answer: A



229. 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

Answer: A

230. Which product can be used to provide application layer protection for TCP port 25 traffic?

- A. ESA
- B. CWS
- C. WSA
- D. ASA

Answer: A

231. What is the purpose of a honeypot IPS?

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

Answer: D

232. Which type of firewall can serve as the intermediary between a client and a server?

- A. Application firewall
- B. stateless firewall
- C. Personal firewall
- D. Proxy firewall

Answer: D

Explanation: <http://searchsecurity.techtarget.com/definition/proxy-firewall>



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

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

Answer: B,D

234. Which of the following commands result in a secure bootset? (Choose all that apply.)

- A. secure boot-set
- B. secure boot-config
- C. secure boot-files
- D. secure boot-image

Answer: B,D

235. Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data?

- A. hack
- B. mitigation
- C. risk
- D. vulnerability
- E. exploit

Answer: D

Explanation: vulnerability A flaw or weakness in a system's design or implementation that could be exploited.

236. How does a zone pair handle traffic if the policy definition of the zone pair is missing?

- A. It permits all traffic without logging.
- B. it drops all traffic
- C. it permits and logs all traffic
- D. it inspects all traffic



Answer: B

237. 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

Answer: A,B

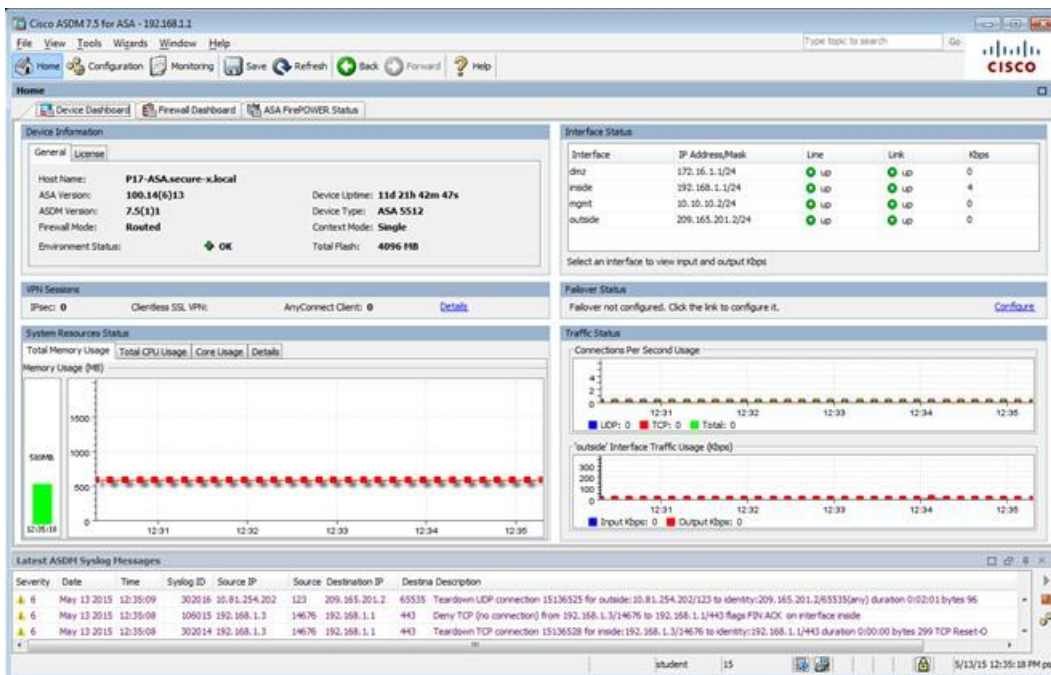
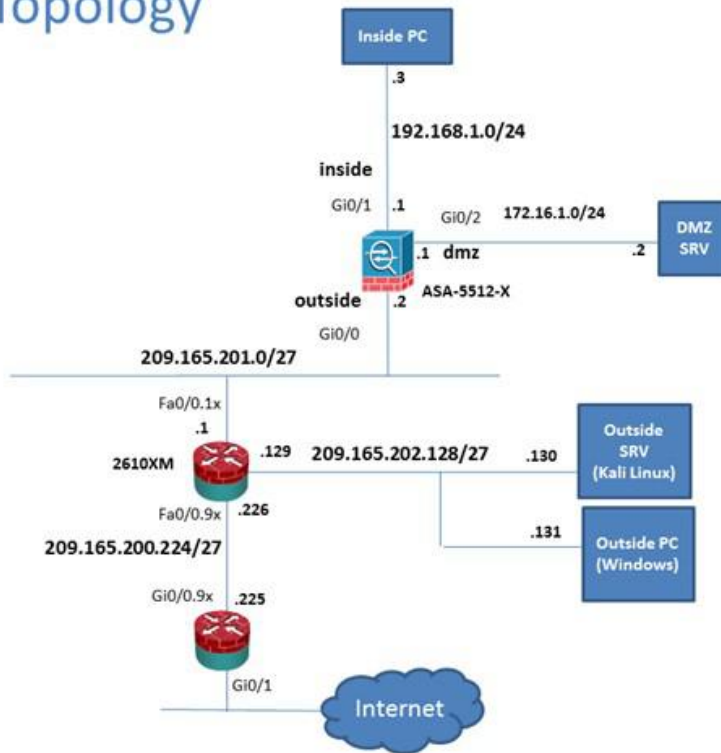
238. Scenario

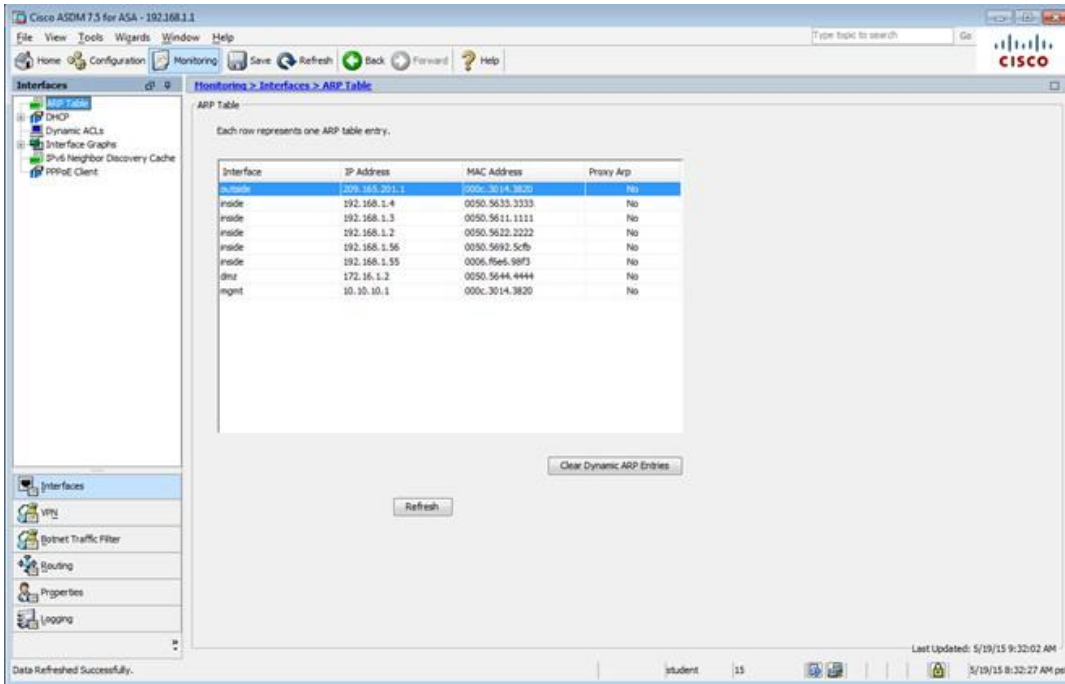
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

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	209.165.202.1	000c:29:14:3a00	No
inside	192.168.1.4	0050:5633:3333	No
inside	192.168.1.3	0050:5611:1111	No
inside	192.168.1.2	0050:5632:2222	No
inside	192.168.1.56	0050:5692:5c0b	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

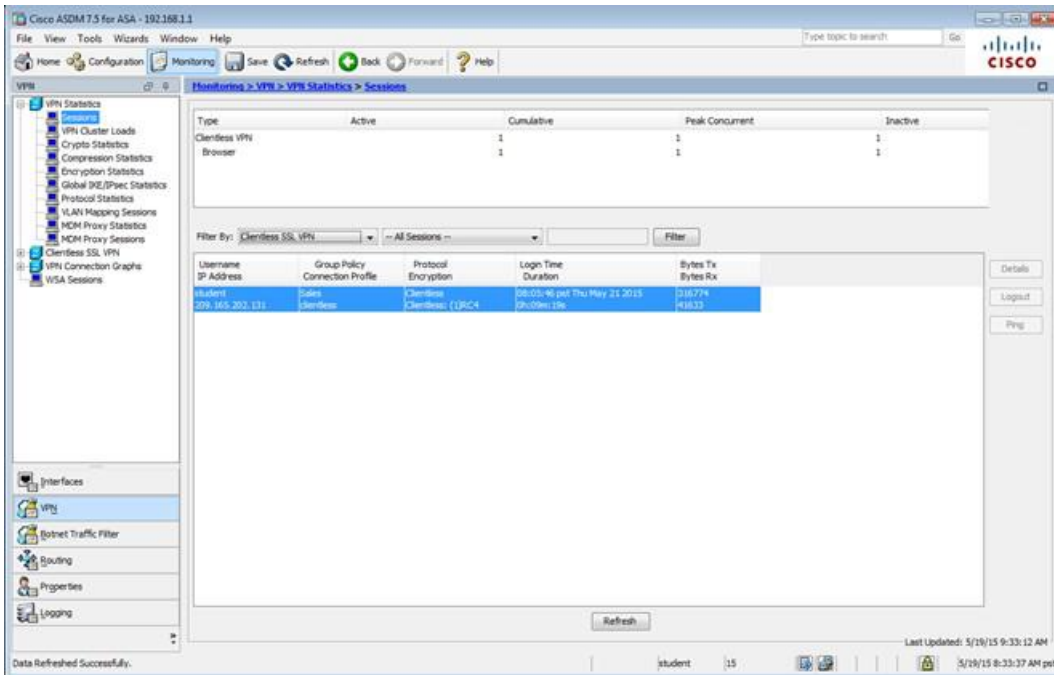
Refresh

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

Data Refreshed Successfully.

student 15

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

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	Global	Clientless	Clientless	Clientless (1)GCM4	05:05:46 pm Thu May 21 2015	0h:05m:15s	319774	41633

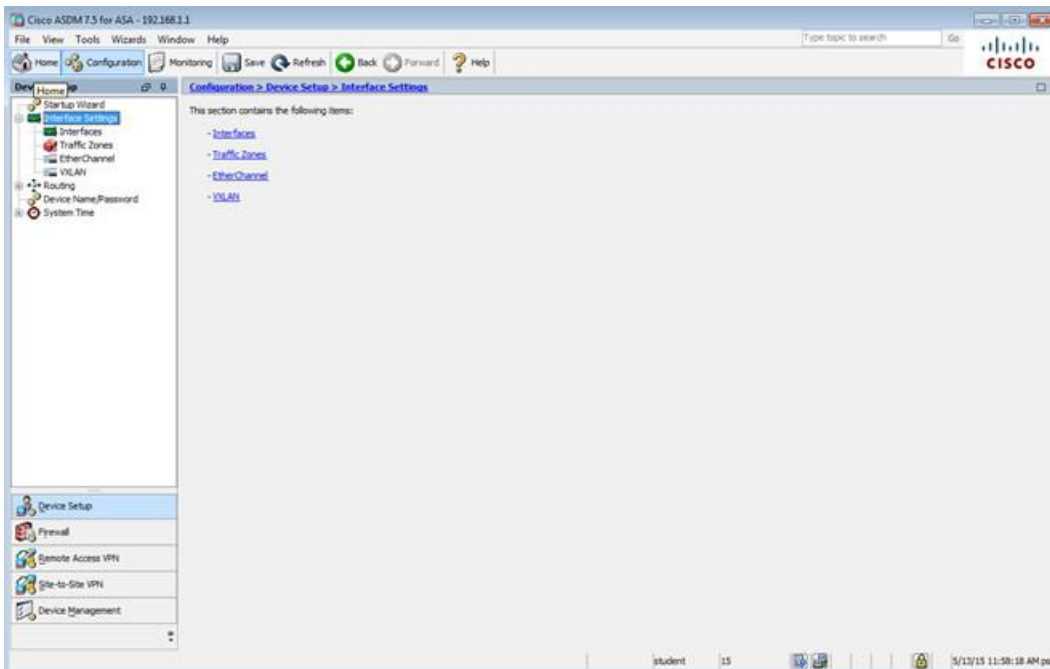
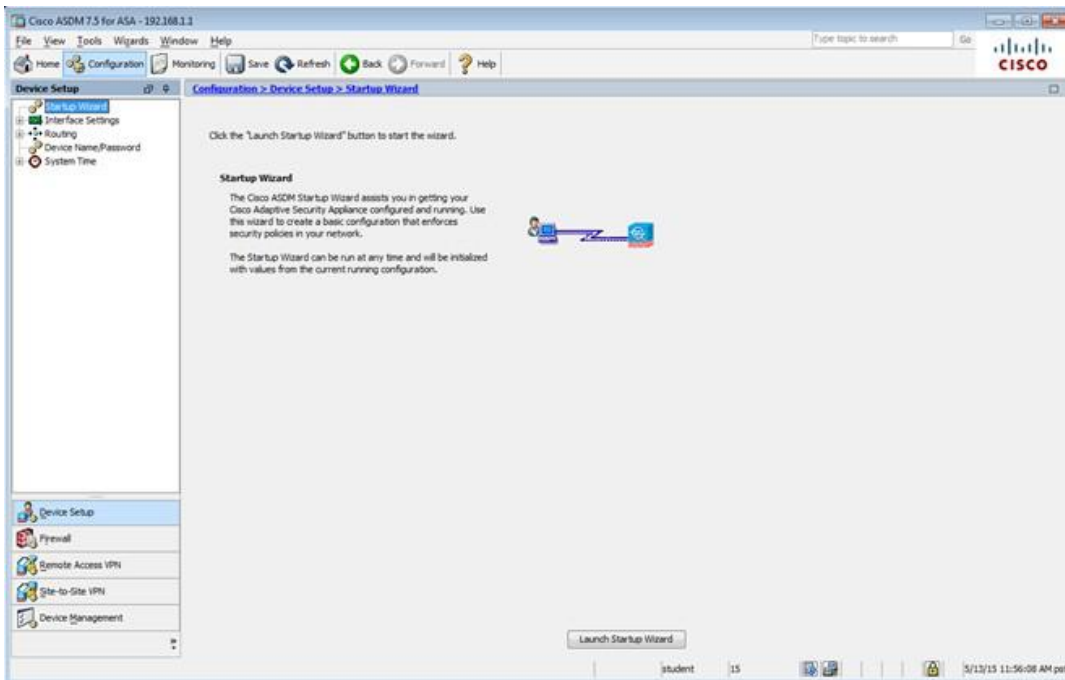
Refresh

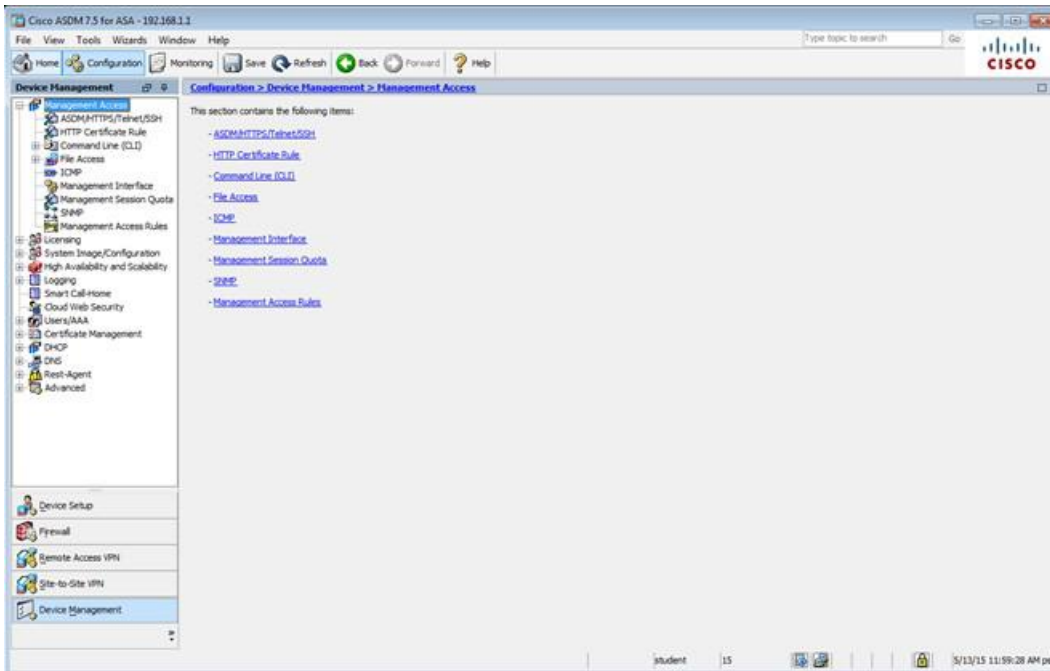
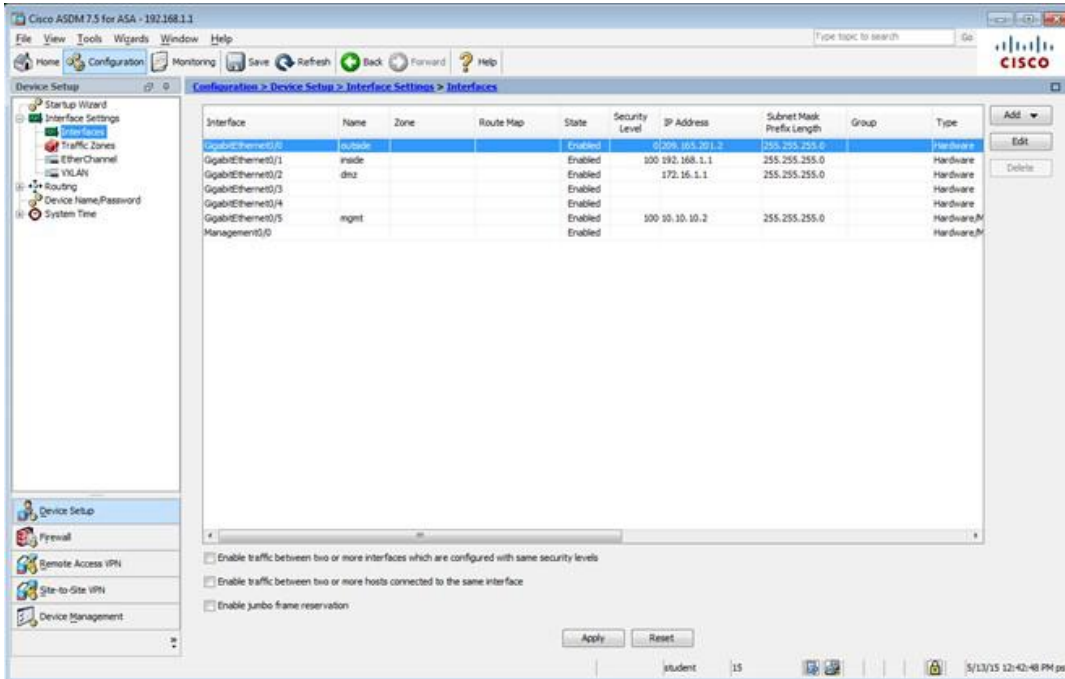
Last Updated: 5/19/15 9:33:12 AM

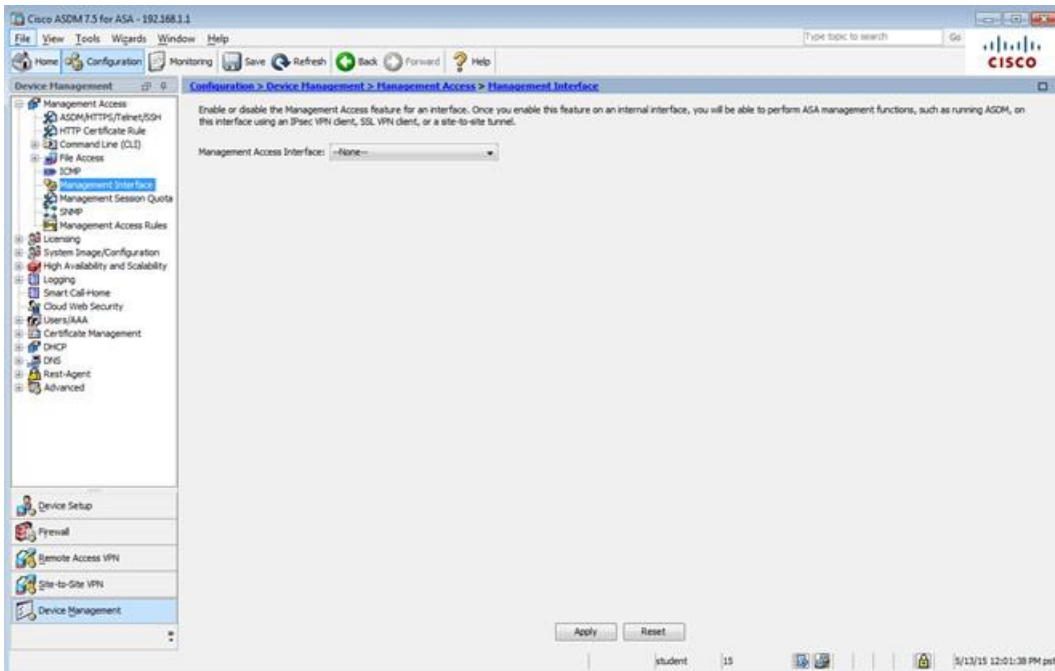
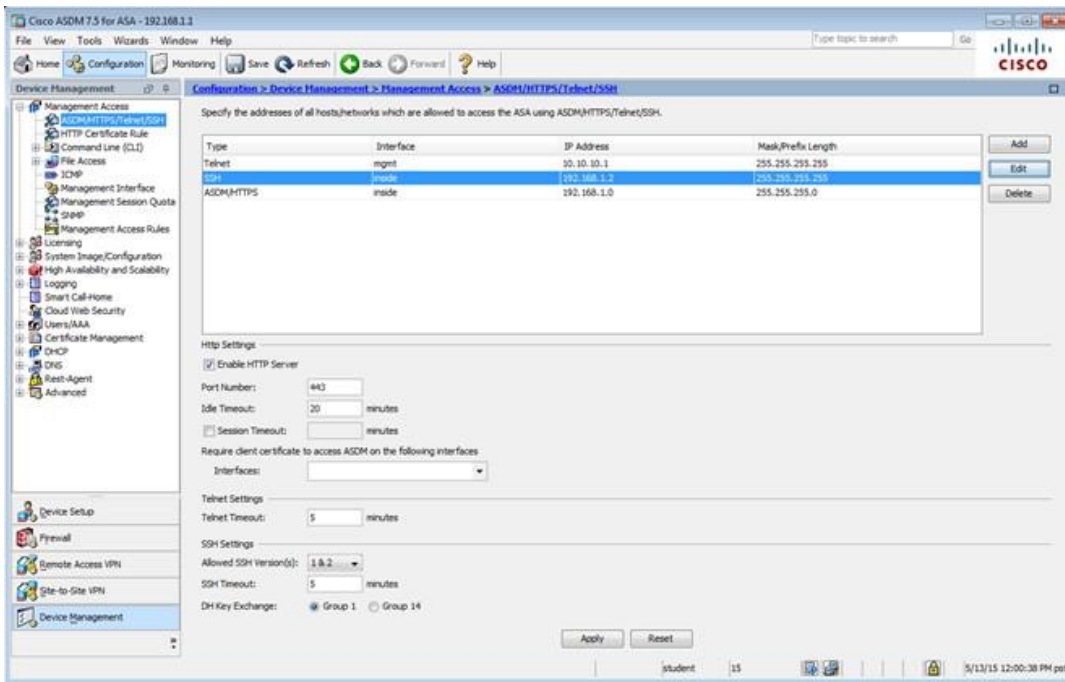
Data Refreshed Successfully.

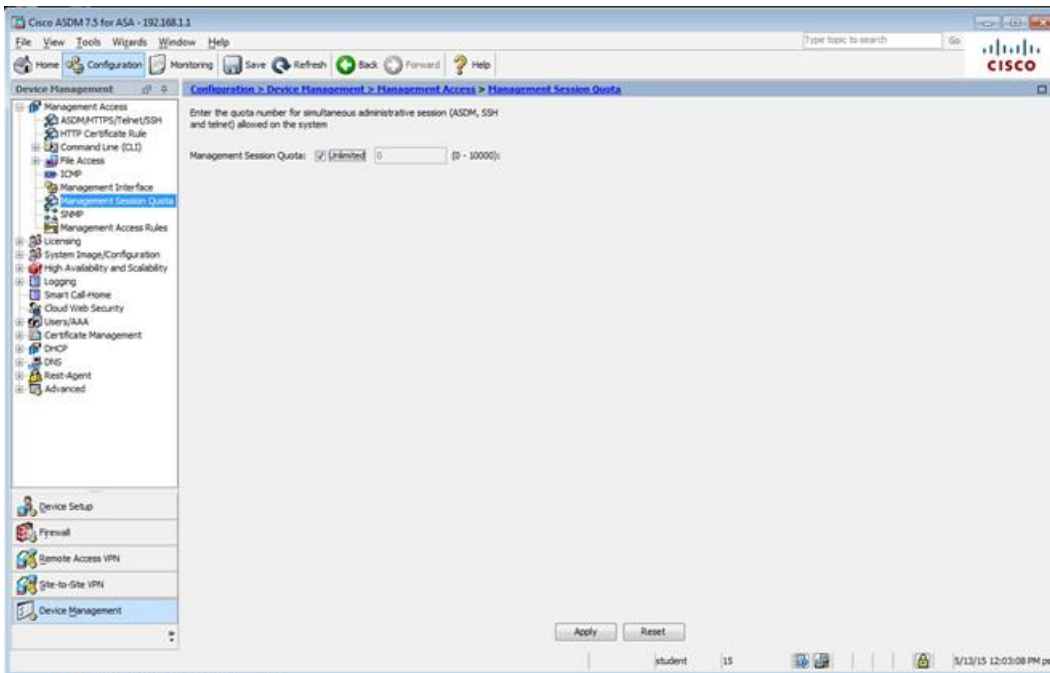
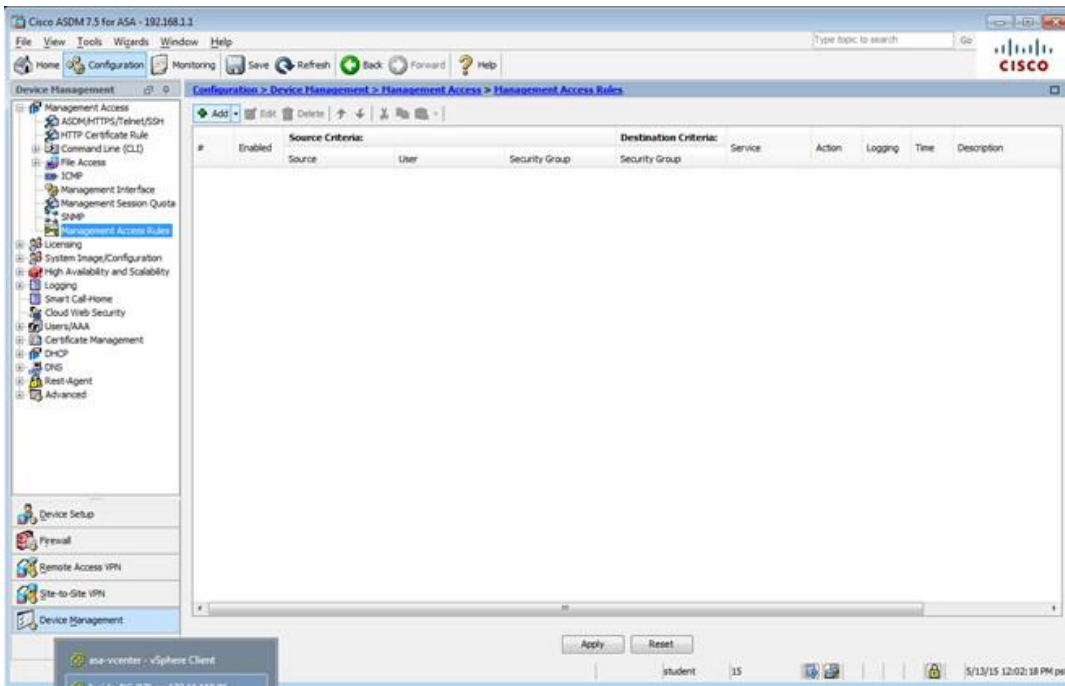
student 15

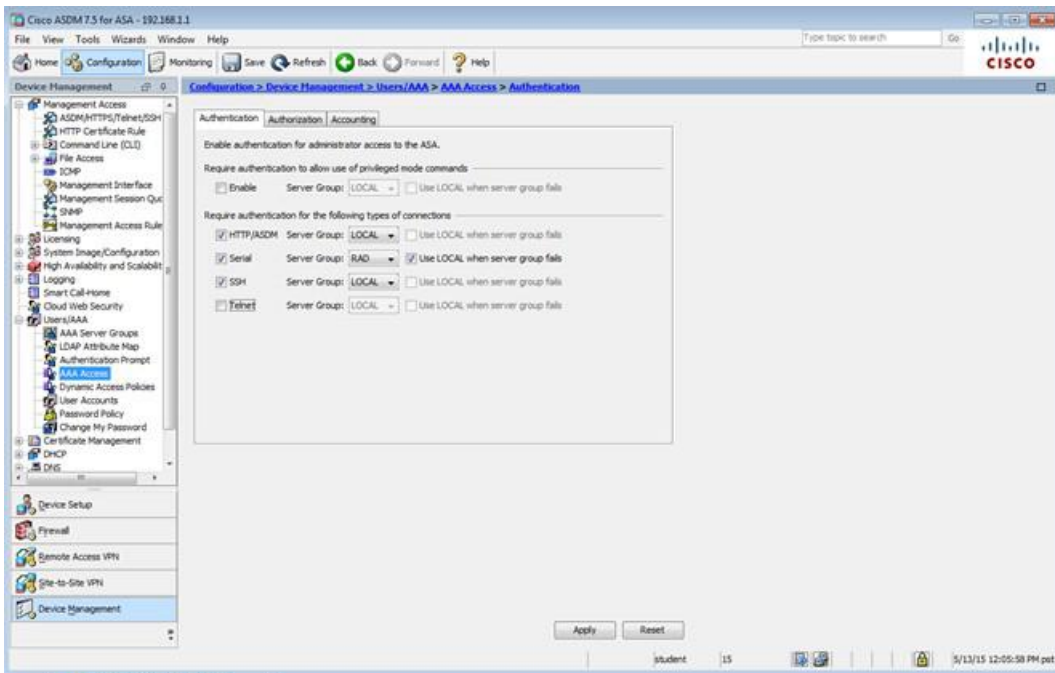
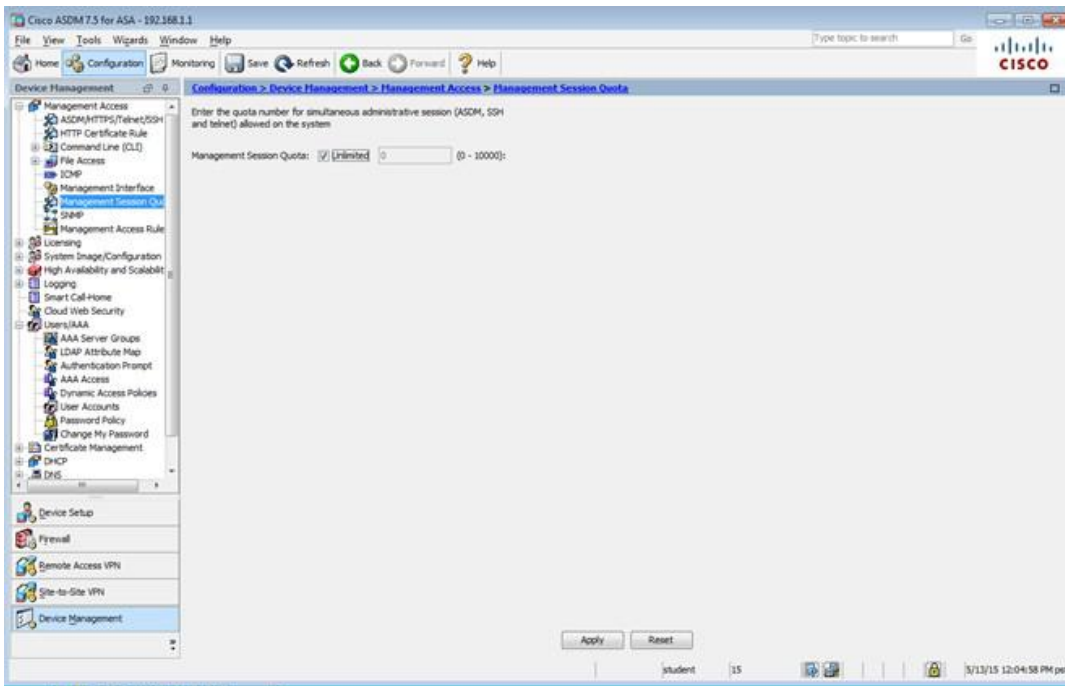
5/19/15 9:33:37 AM pst

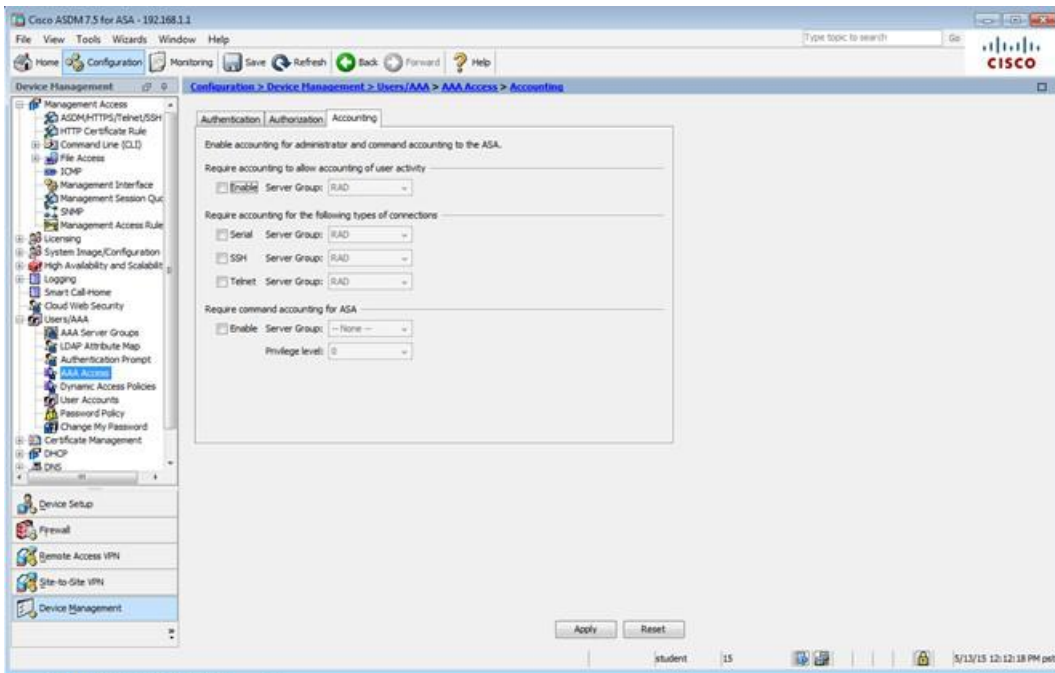
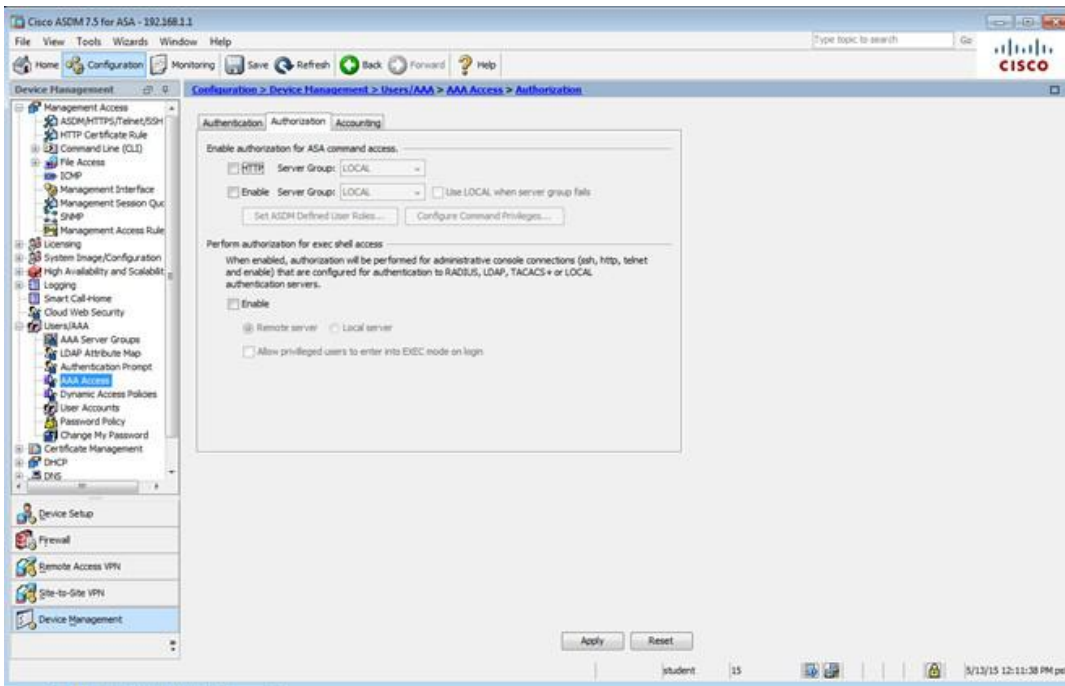


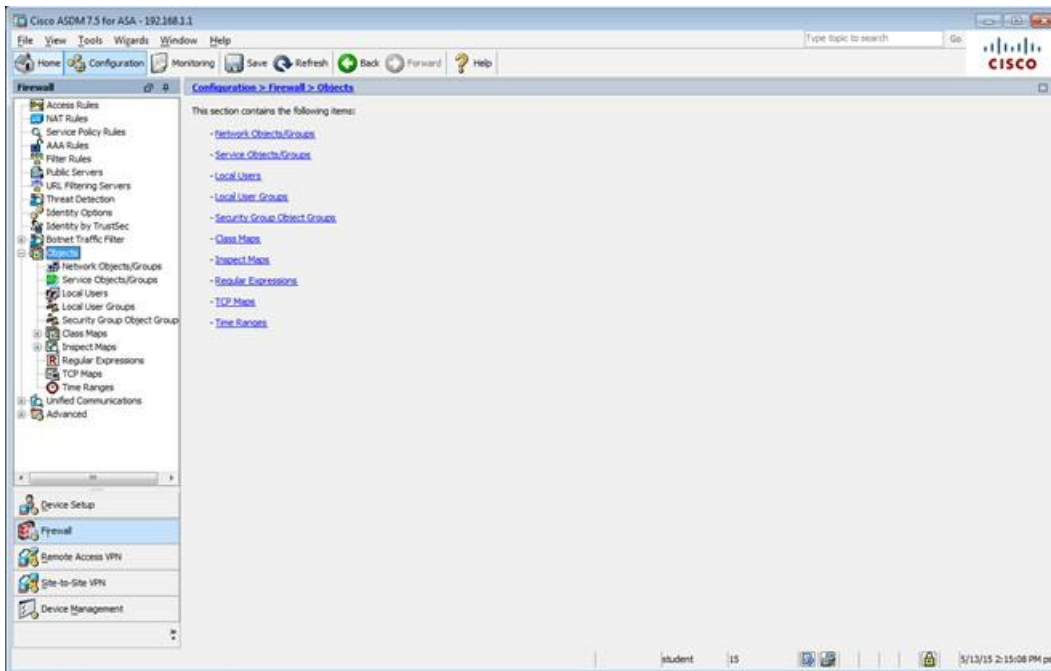
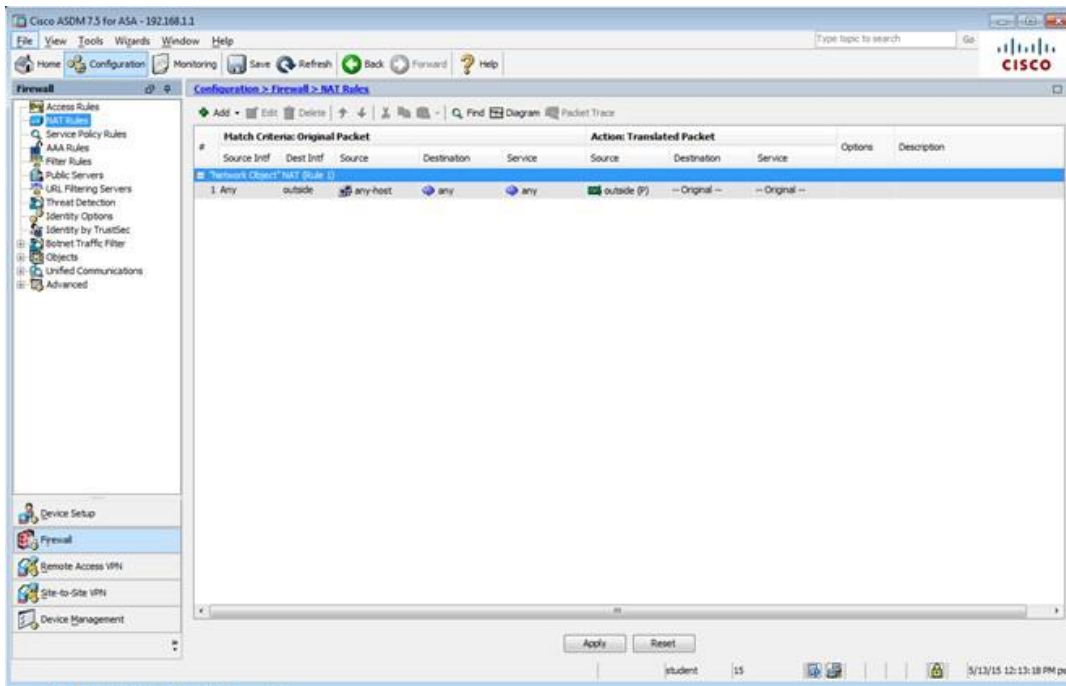


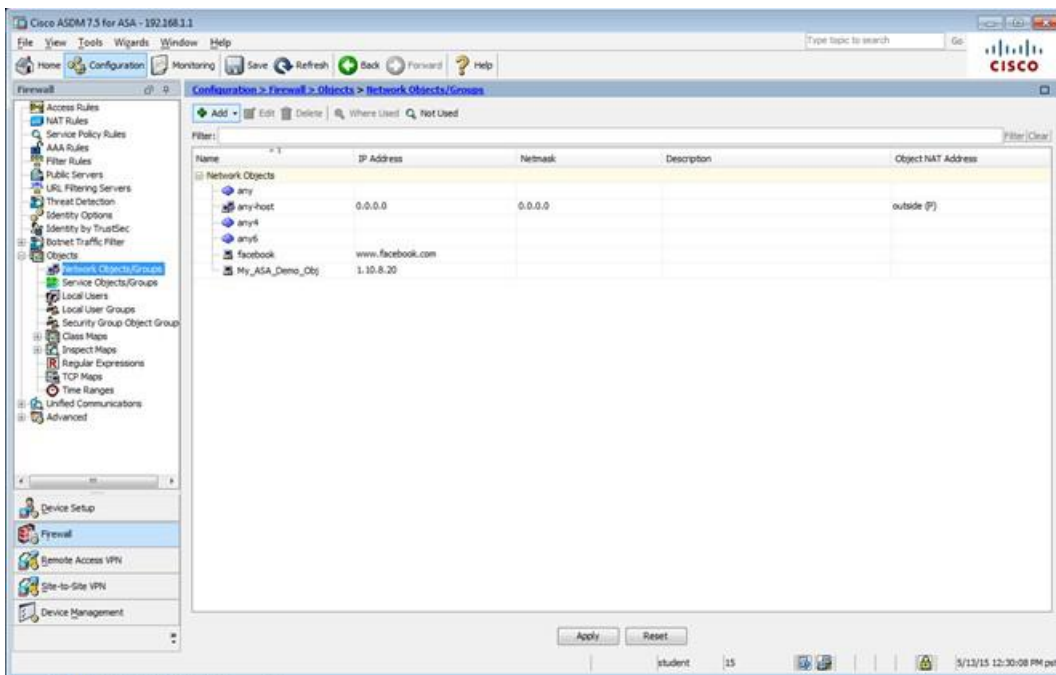
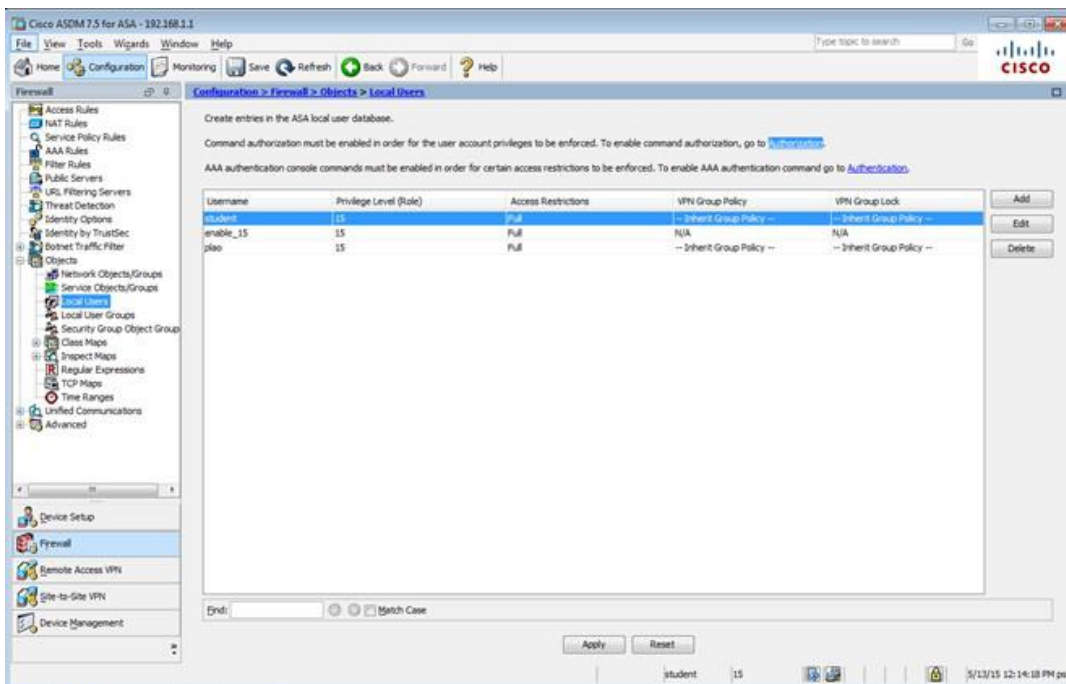


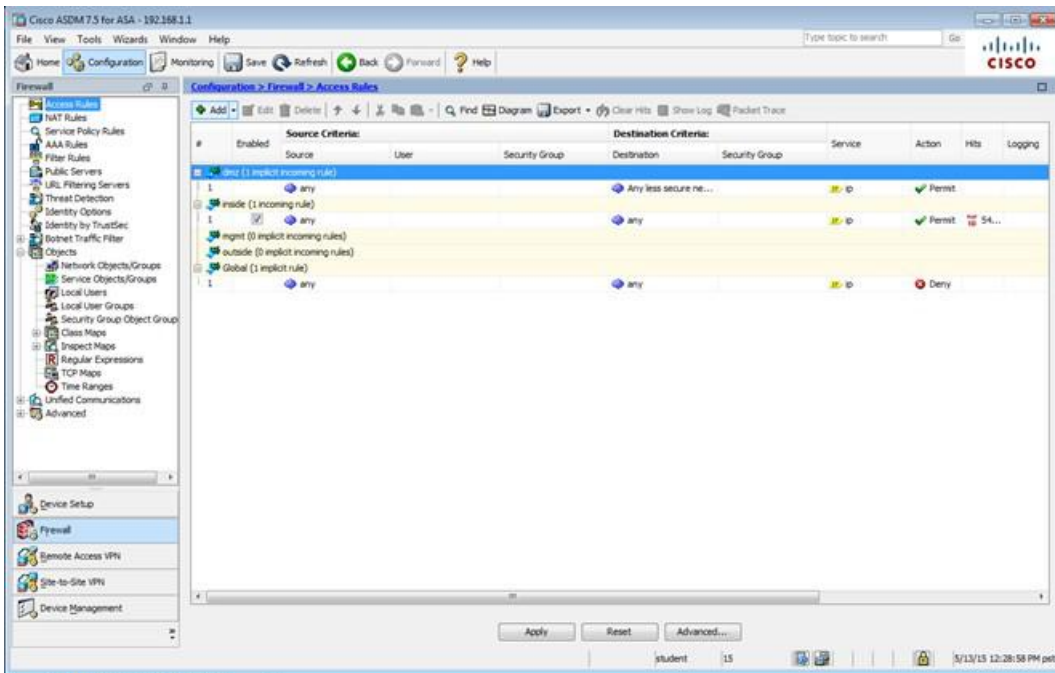
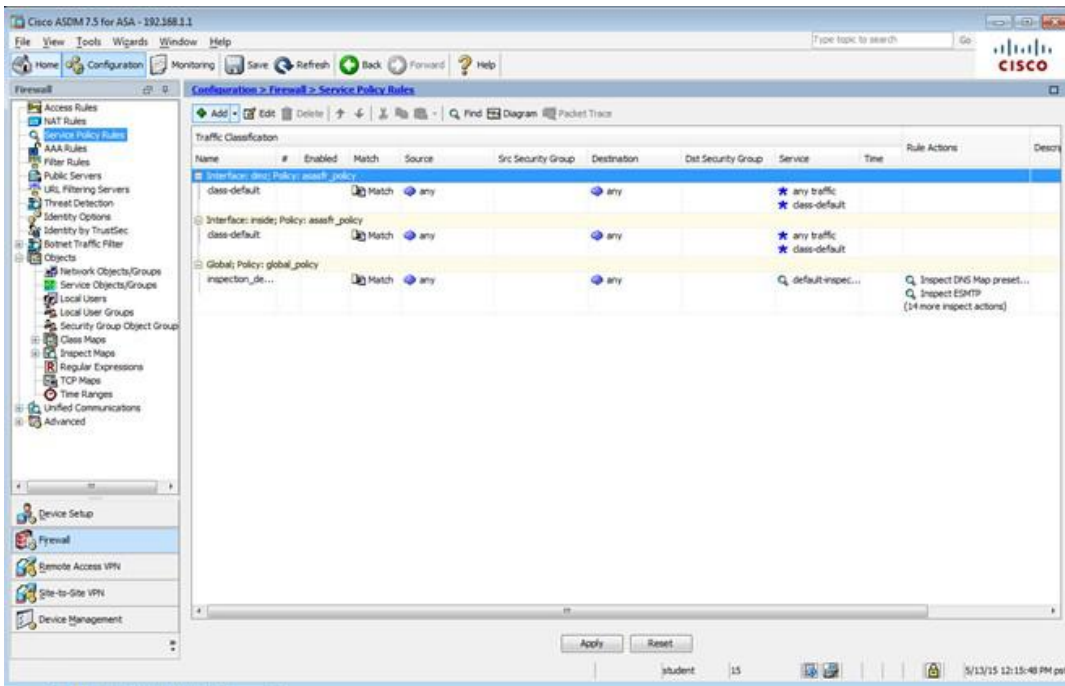


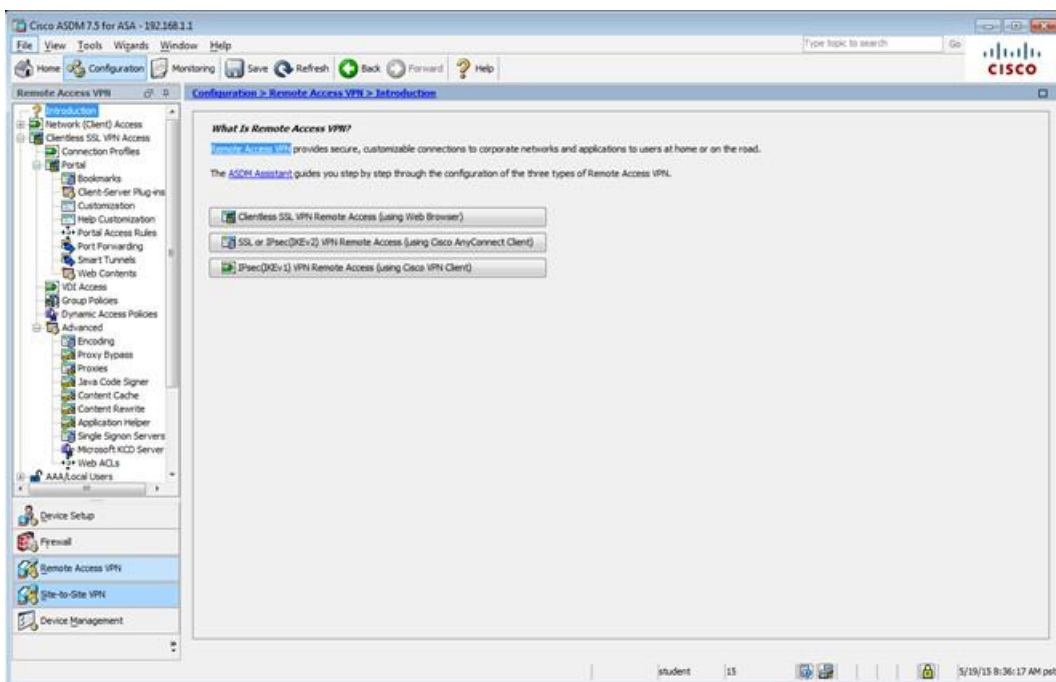
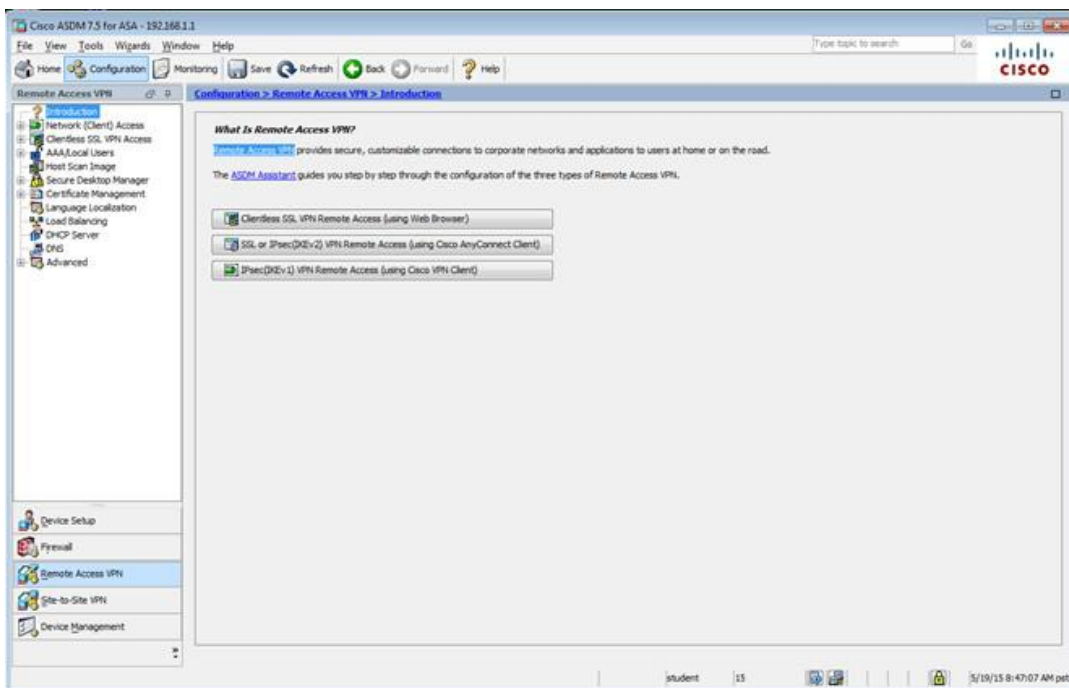


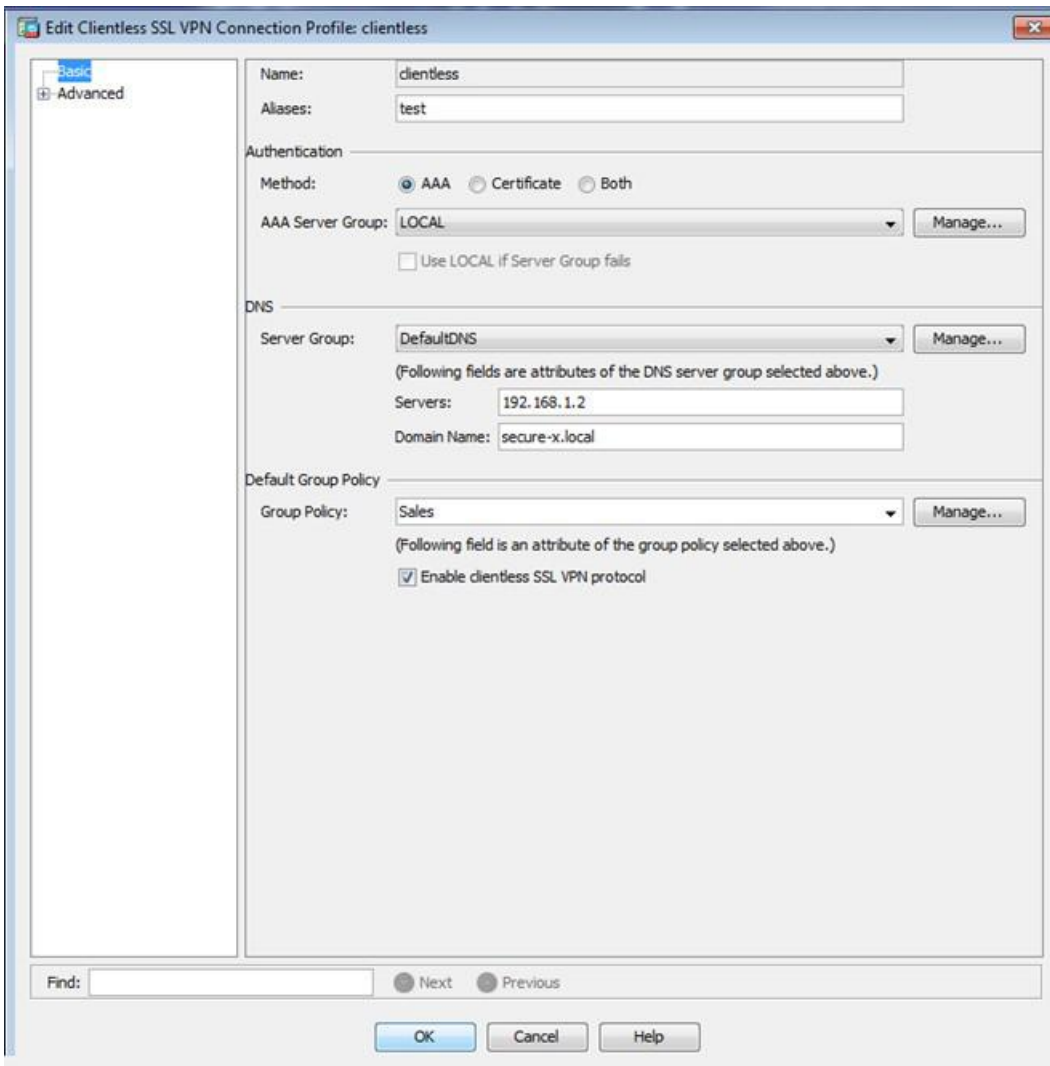
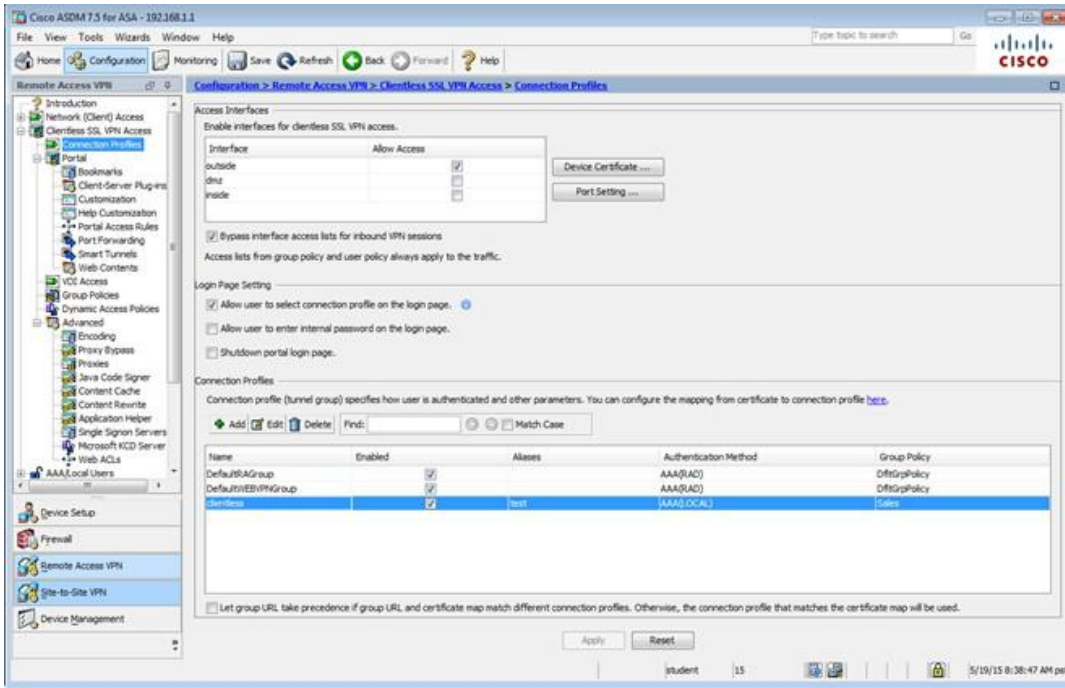












Edit Clientless SSL VPN Connection Profile: clientless

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 choose 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)

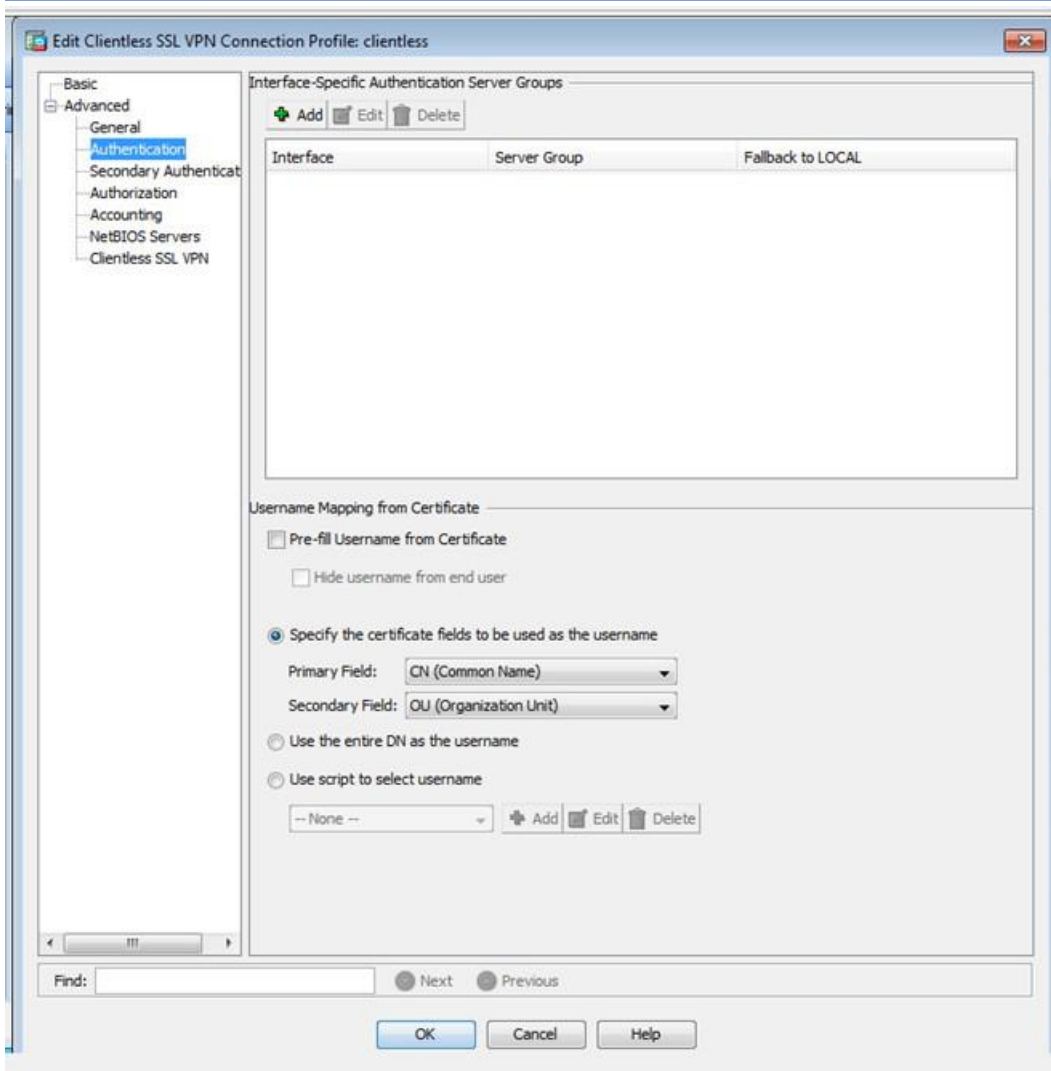
☒ Always run CSD

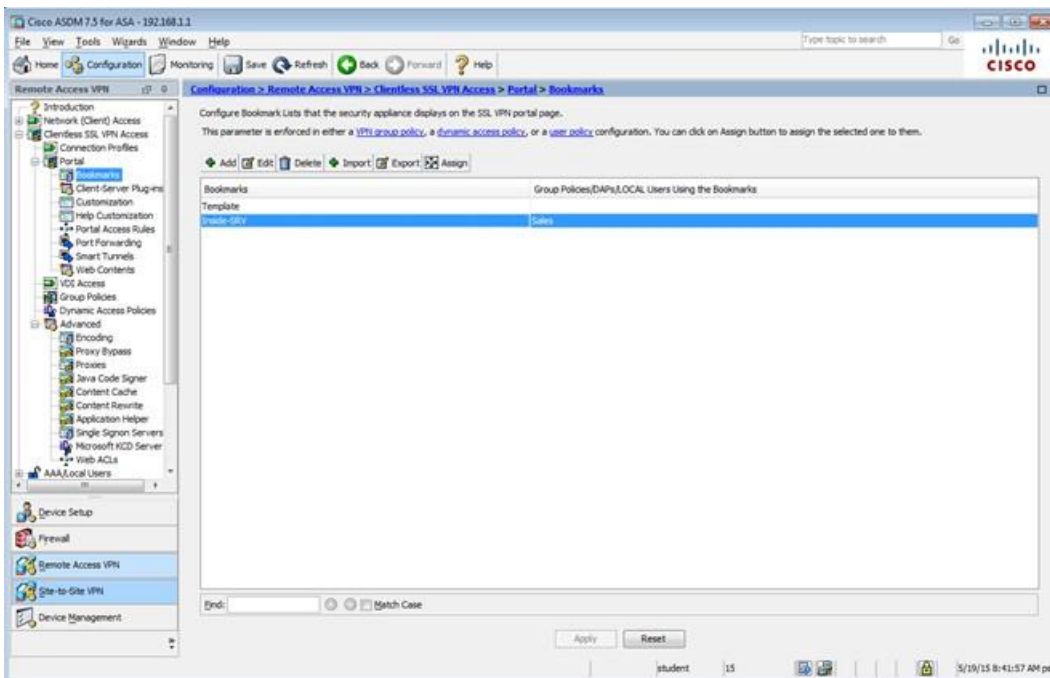
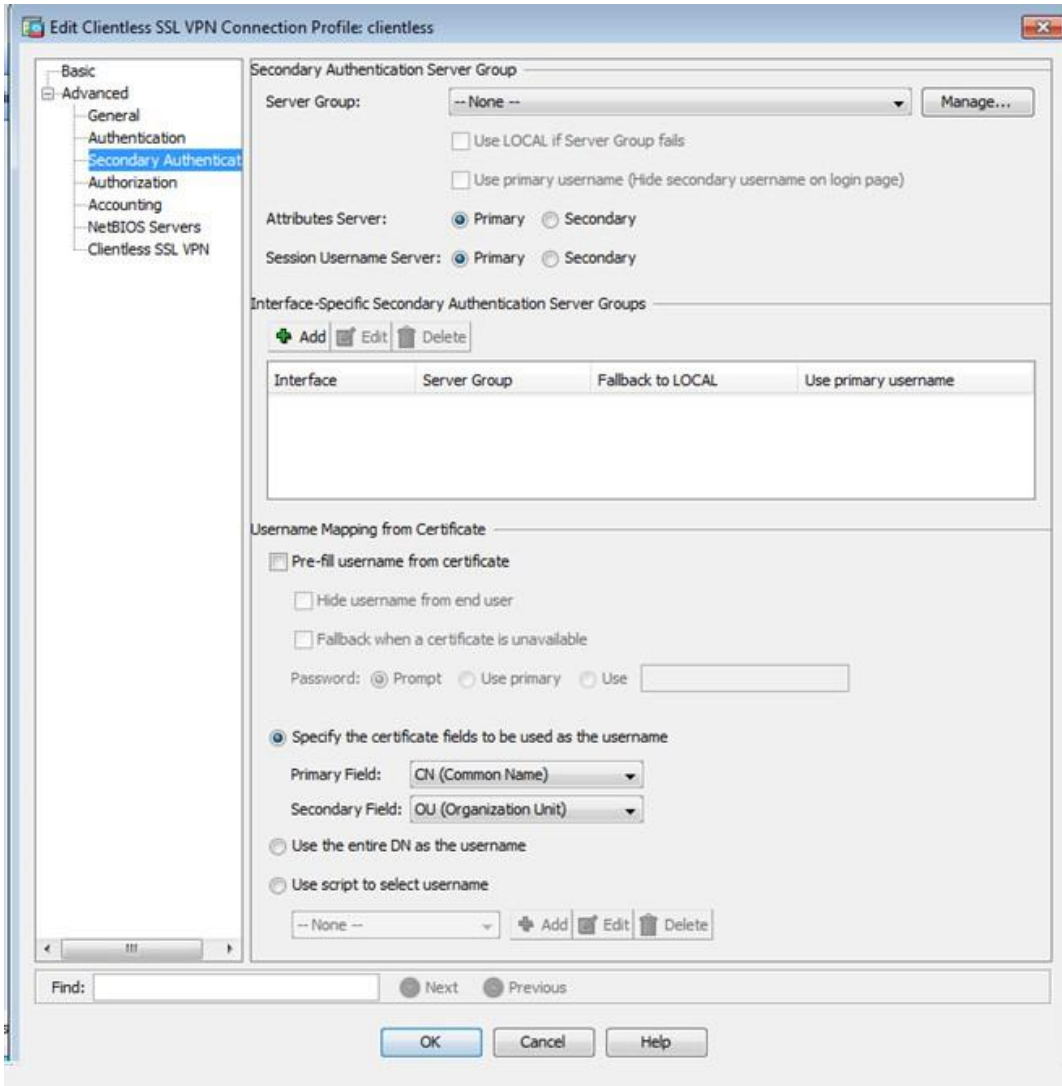
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

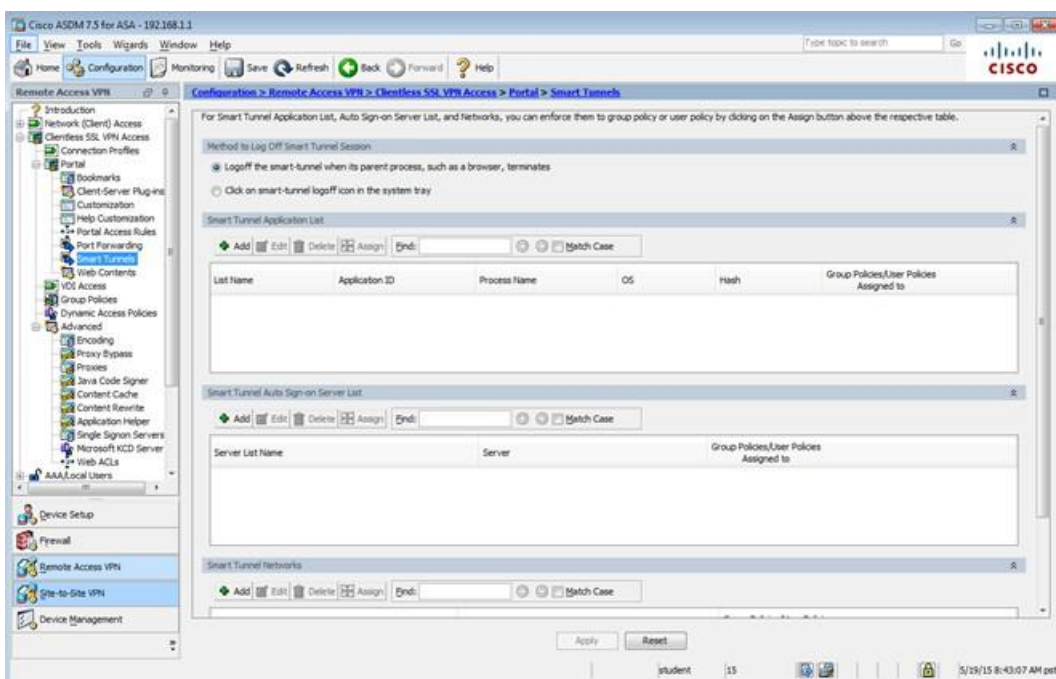
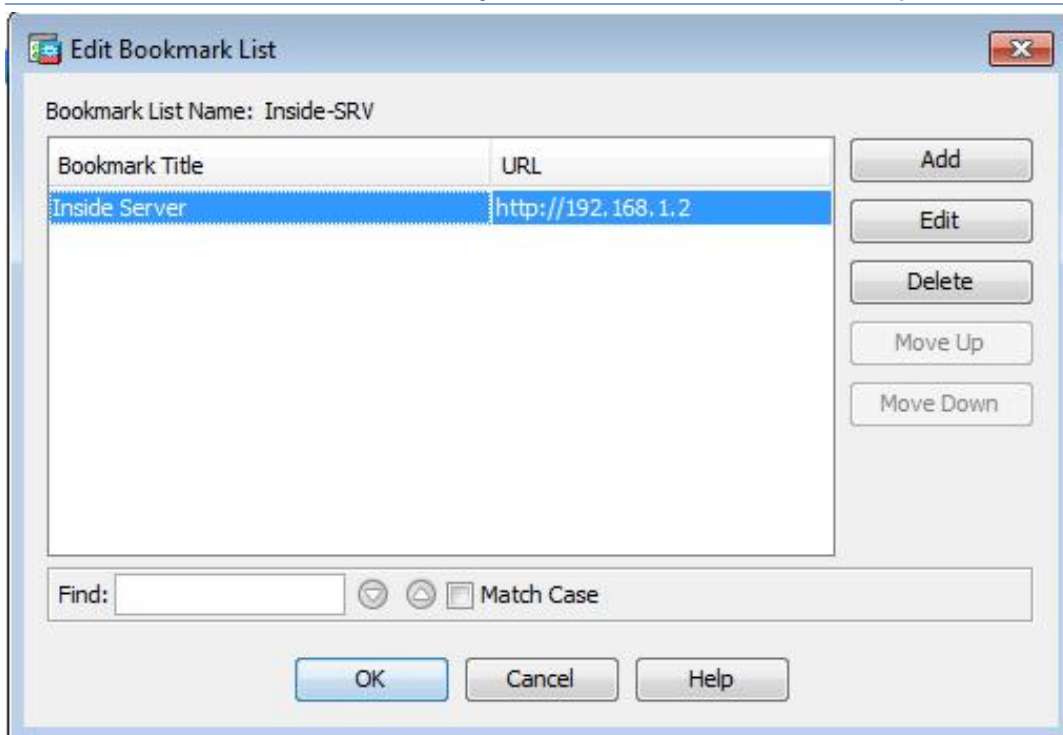
☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







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 > Portal > Port Forwarding

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

Add Edit Delete Assign

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

Find: Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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](#).

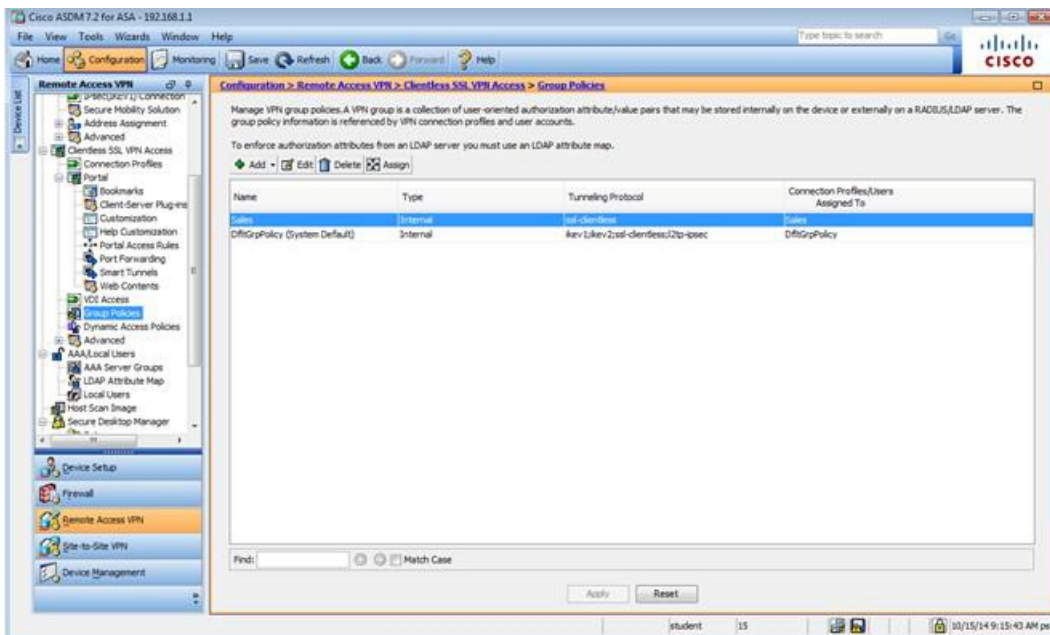
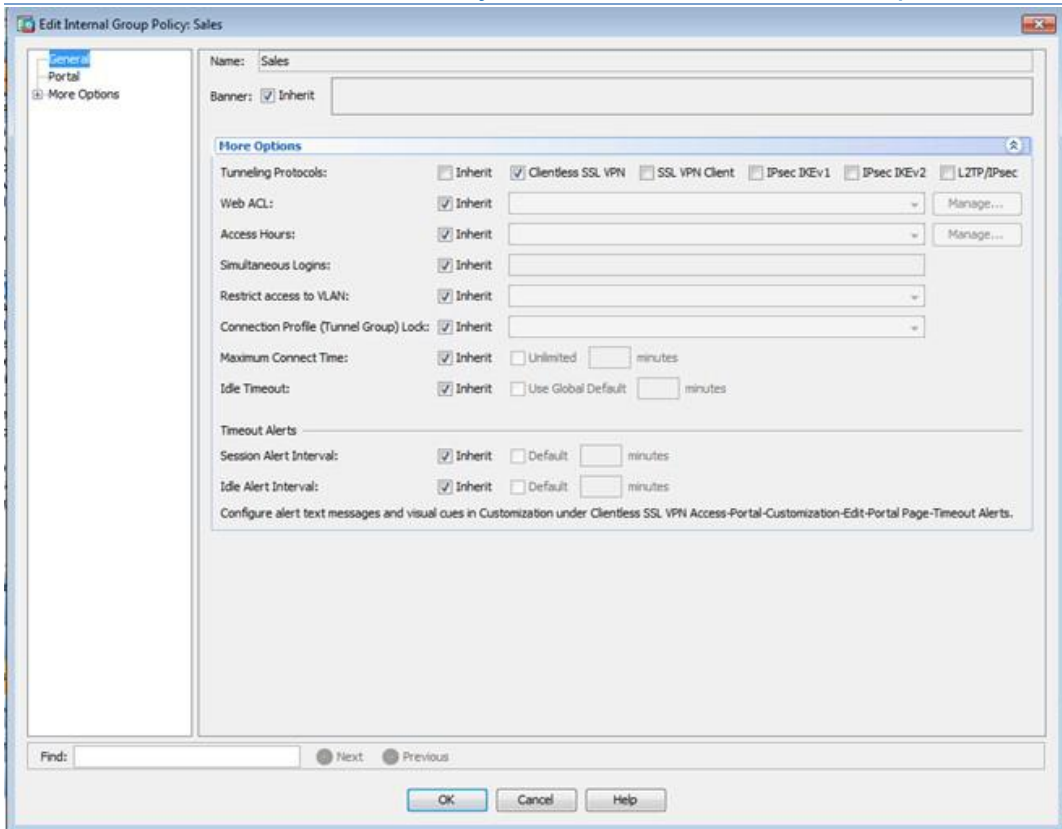
Add Edit Delete Assign

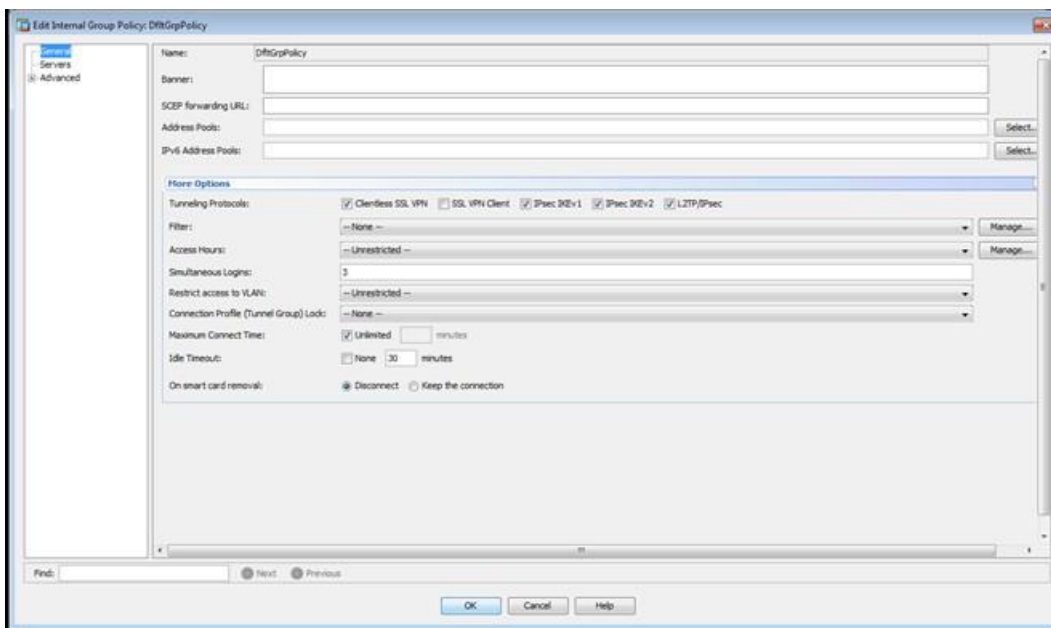
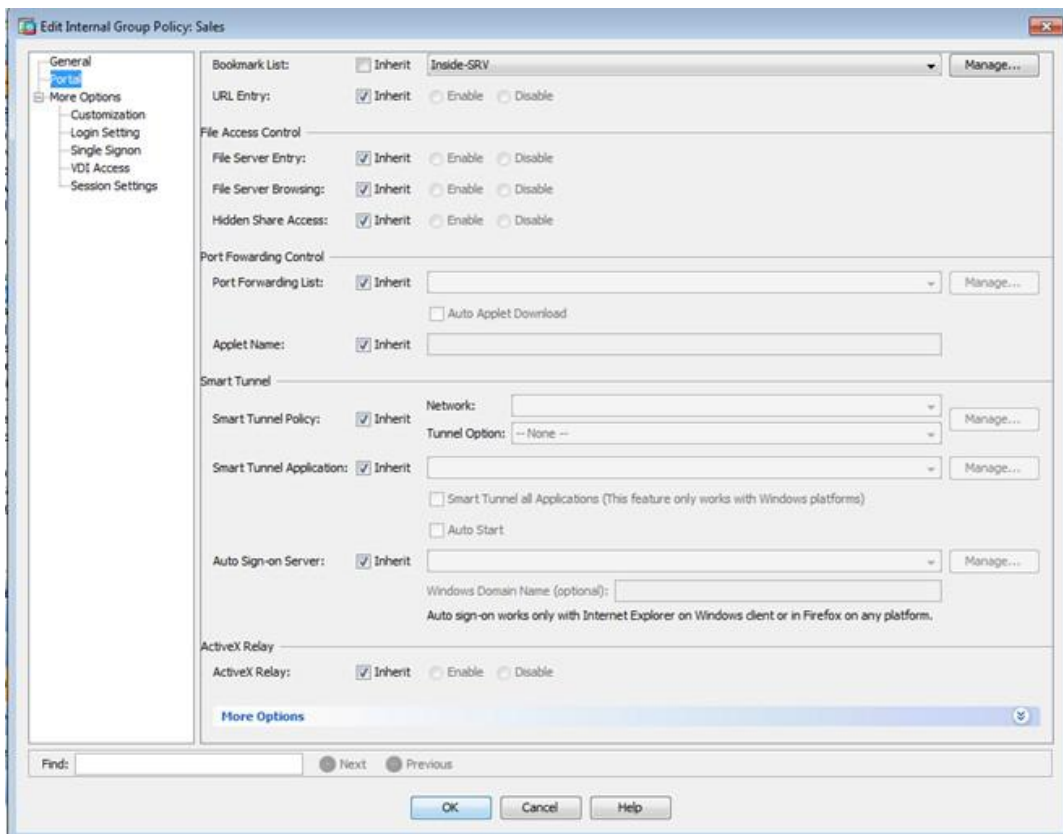
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	all-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1:rev2:ssl-clientless/2to-espsec	DefaultRAGroup/DefaultIL2Group/DefaultADP2Group/Def...

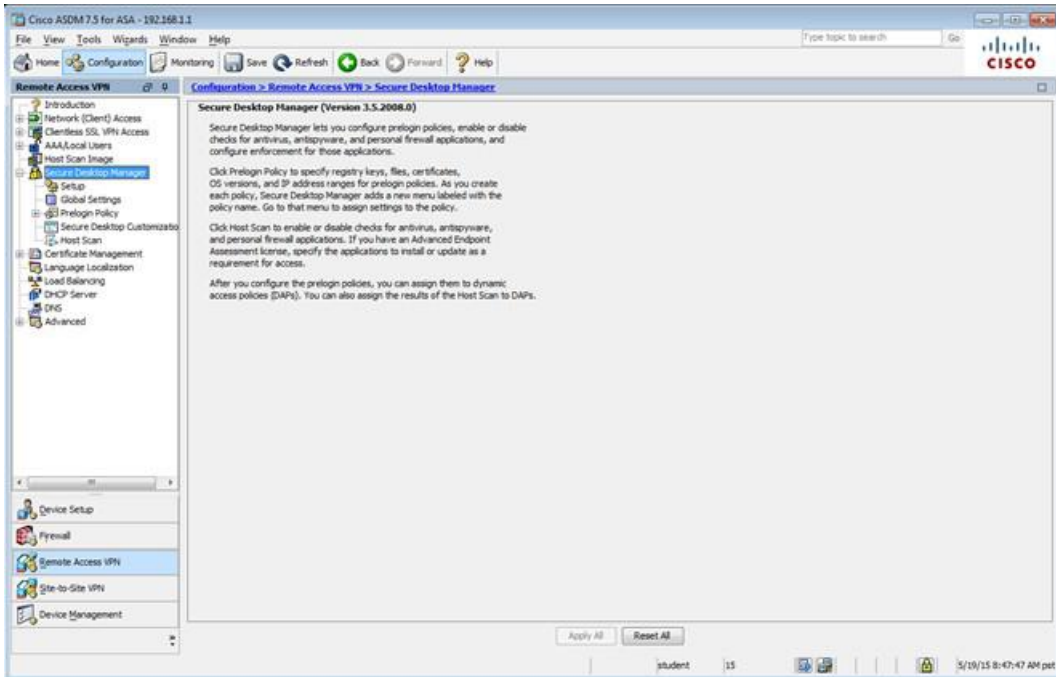
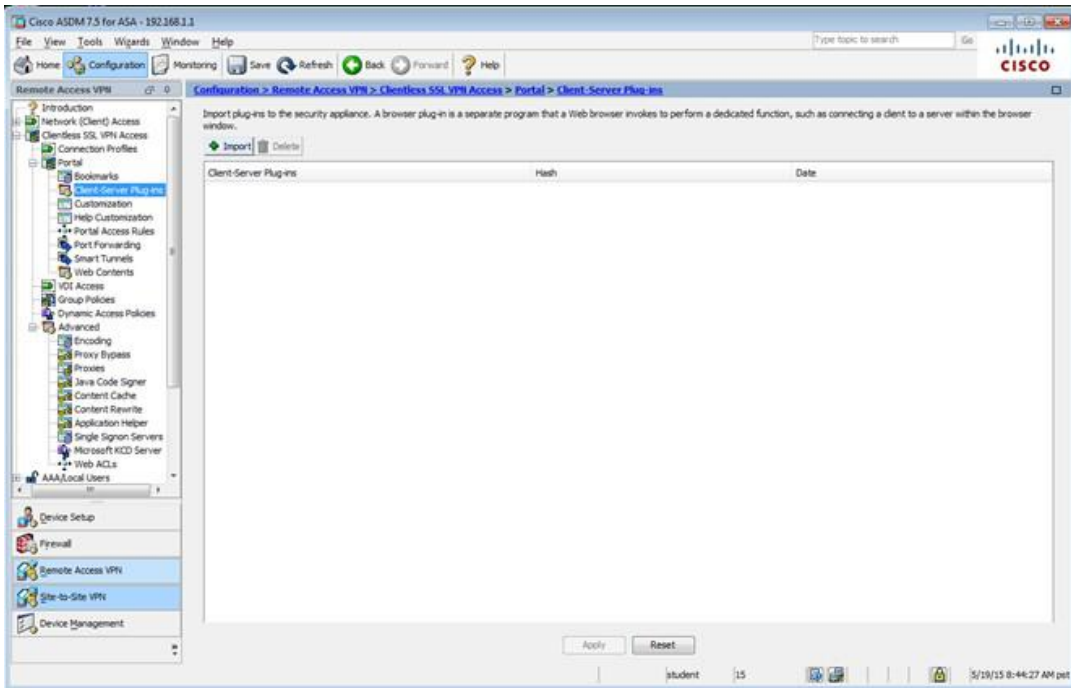
Find: Match Case

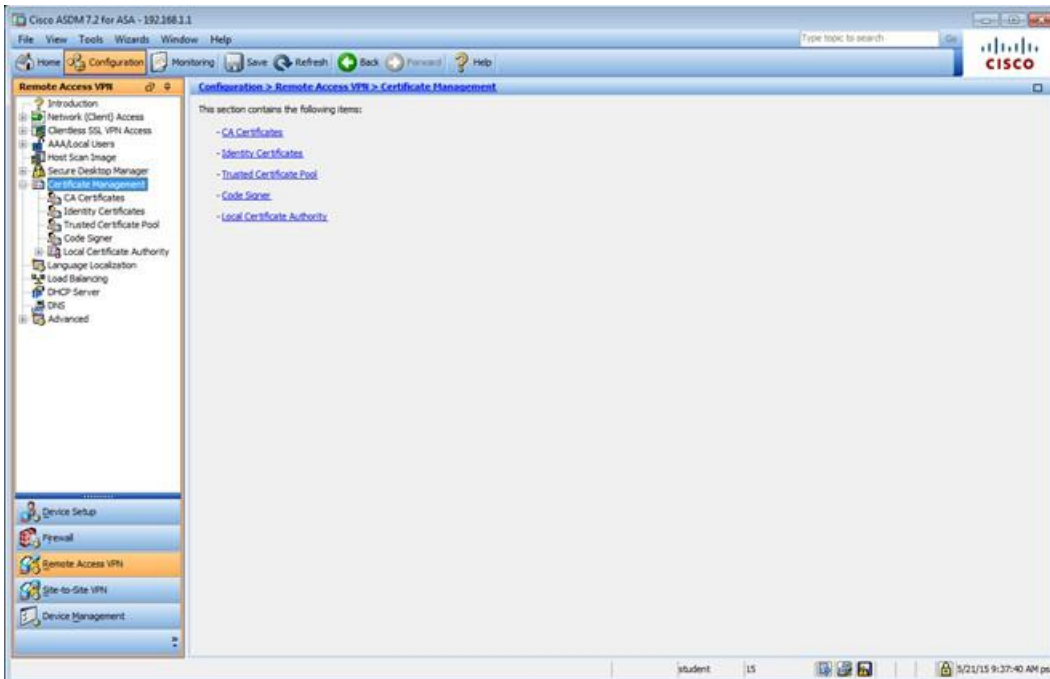
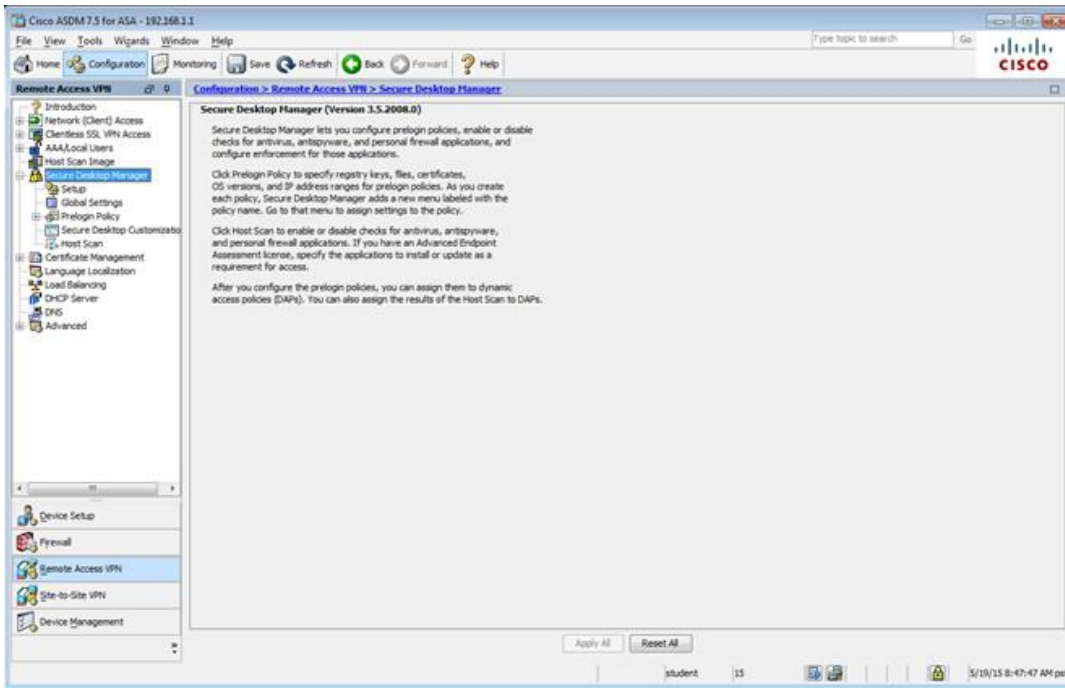
Apply Reset

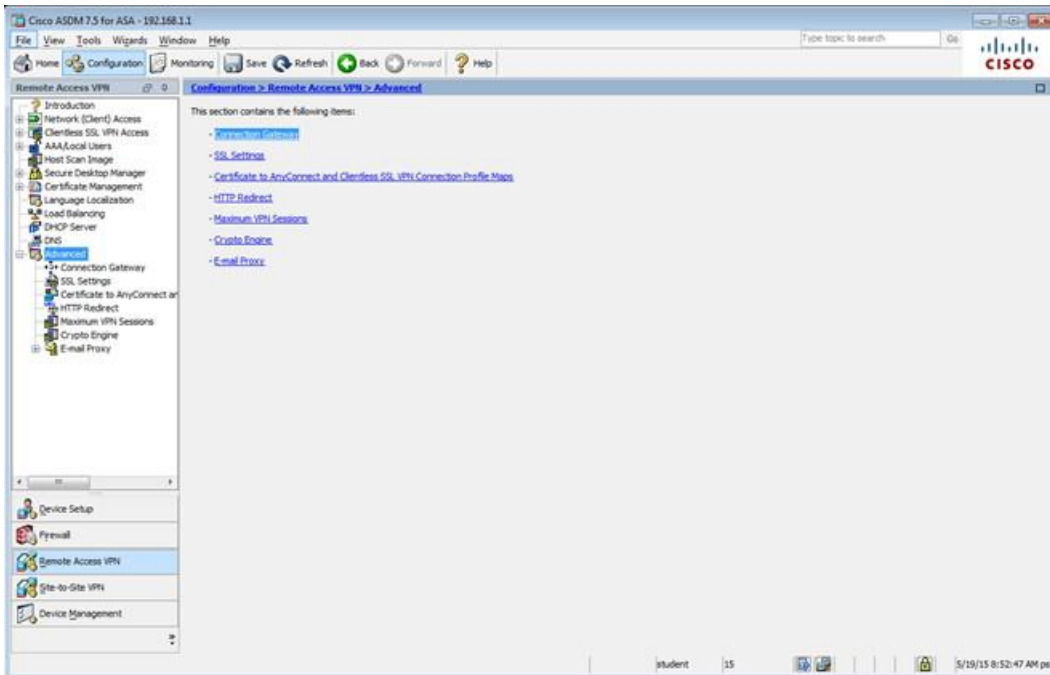
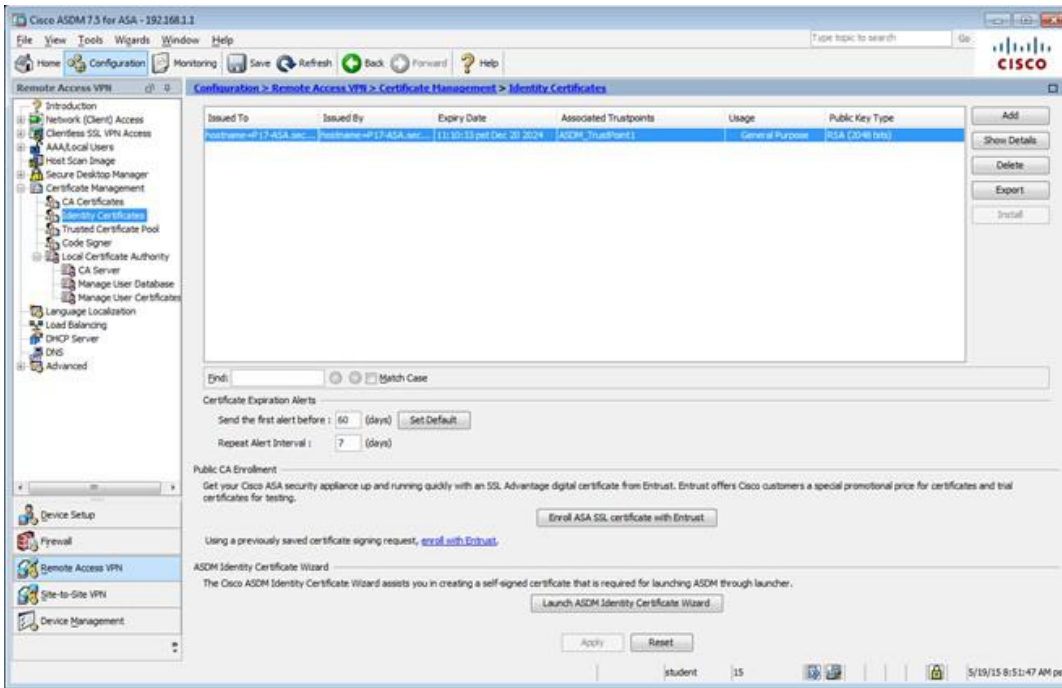
student 15 5/19/15 8:49:27 AM pst

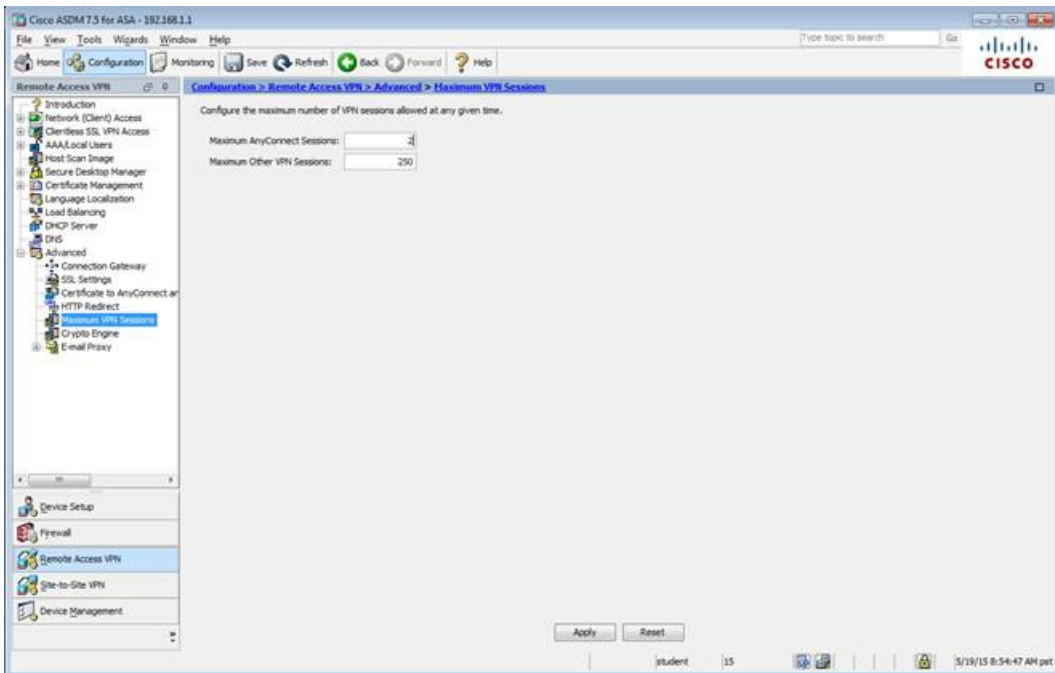
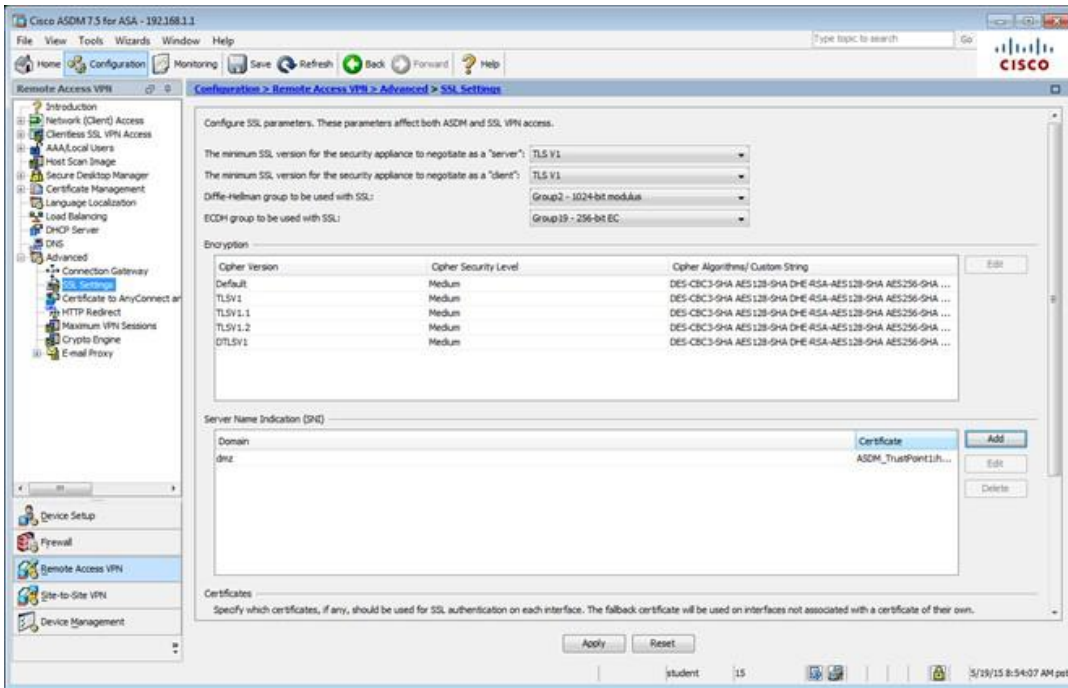












Configuration > Remote Access VPN > Network (Client) Access

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

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

- 1. SSL tunnel and IPsec tunnel**
They are two different ways to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an IPsec tunnel uses IPsec protocol. Cisco AnyConnect VPN Client supports SSL and IPsec(DKEv2) protocols. Cisco VPN Client supports only IPsec(DKEv1) protocol.
- 2. User and connection profile**
To access corporate network resources, remote users must authenticate, and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.
You configure user account database in [AAA/Local Users](#).
You configure AnyConnect connection profile in [AnyConnect Connection Profiles](#), IPsec connection profile in [IPsec\(DKEv1\) Connection Profiles](#).
- 3. Access policy**
Access policies control how remote users can access corporate networks. An access policy includes the following:
 - Session control - how long a session can remain idle before it is closed.
 - Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
 You configure session control policies in [Dynamic Access Policies](#) or [Group Policies](#).
You configure endpoint security policies for AnyConnect client in [Secure Desktop Manager](#). You also have the option to setup [NAC](#) based endpoint security policies.

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

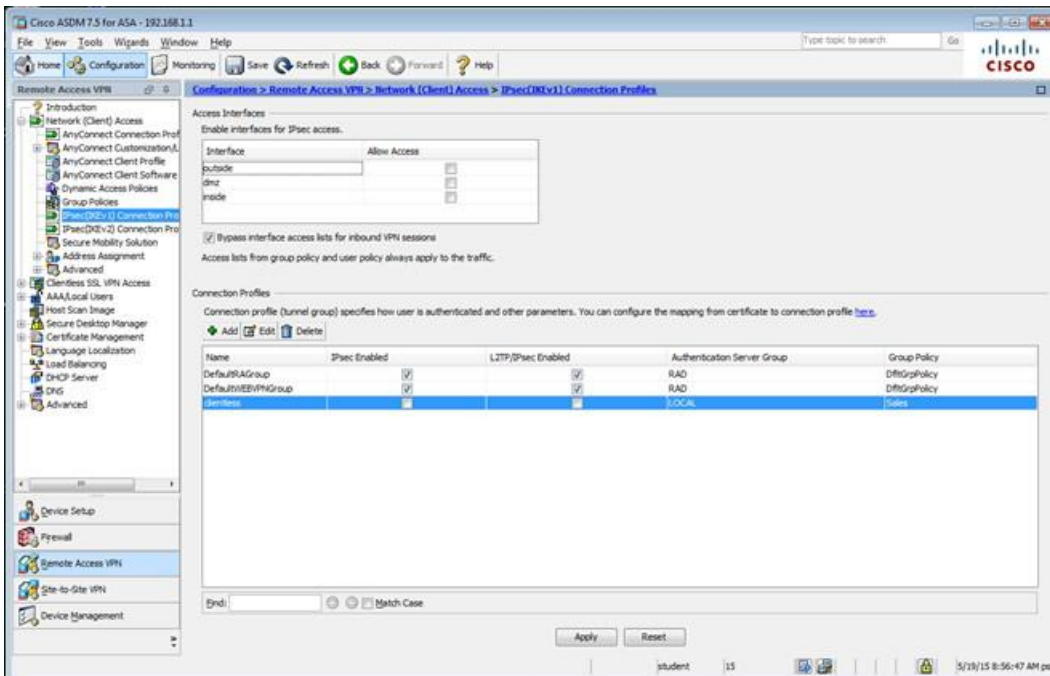
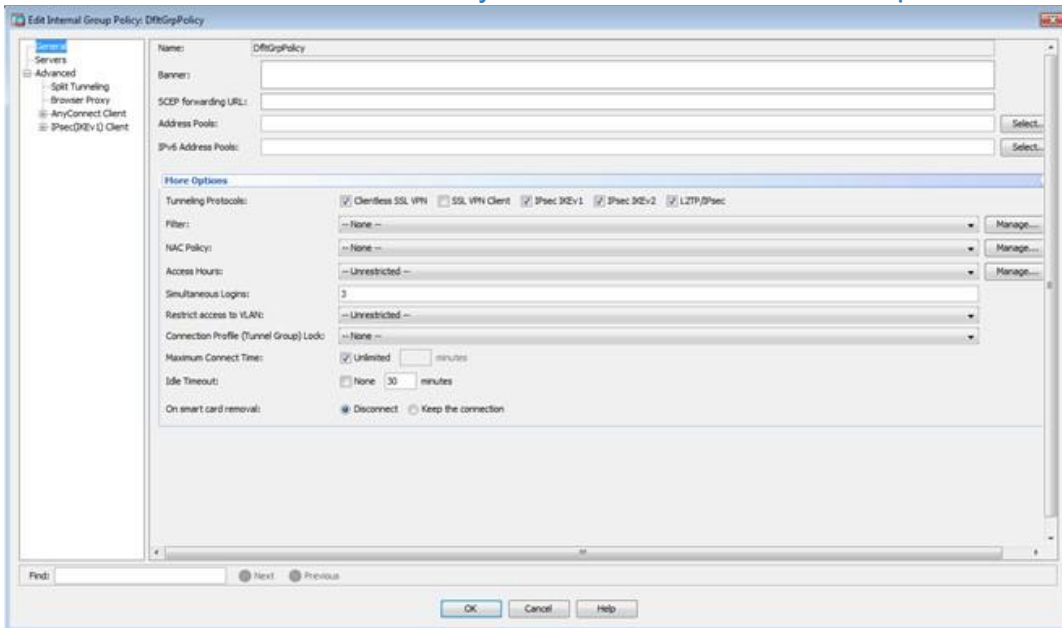
Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization 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
InternetPolicy (System Default)	Internal	ssl-clientless-clientless-ipsec	DefaultGroupDefault3, GroupDefault3, IPsecGroup

Find: Match Case

Apply Reset



The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AnyConnect Connection Profiles' configuration page. It includes sections for 'Access Interfaces', 'Login Page Setting', and 'Connection Profiles'.

Access Interfaces:

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below. SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting:

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

☐ Shutdown portal login page.

Connection Profiles:

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

Buttons: Add, Edit, Delete, End, Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
DefaultIVBGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DefaultPolicy
Default	<input checked="" type="checkbox"/>	<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.

Buttons: Apply, Reset

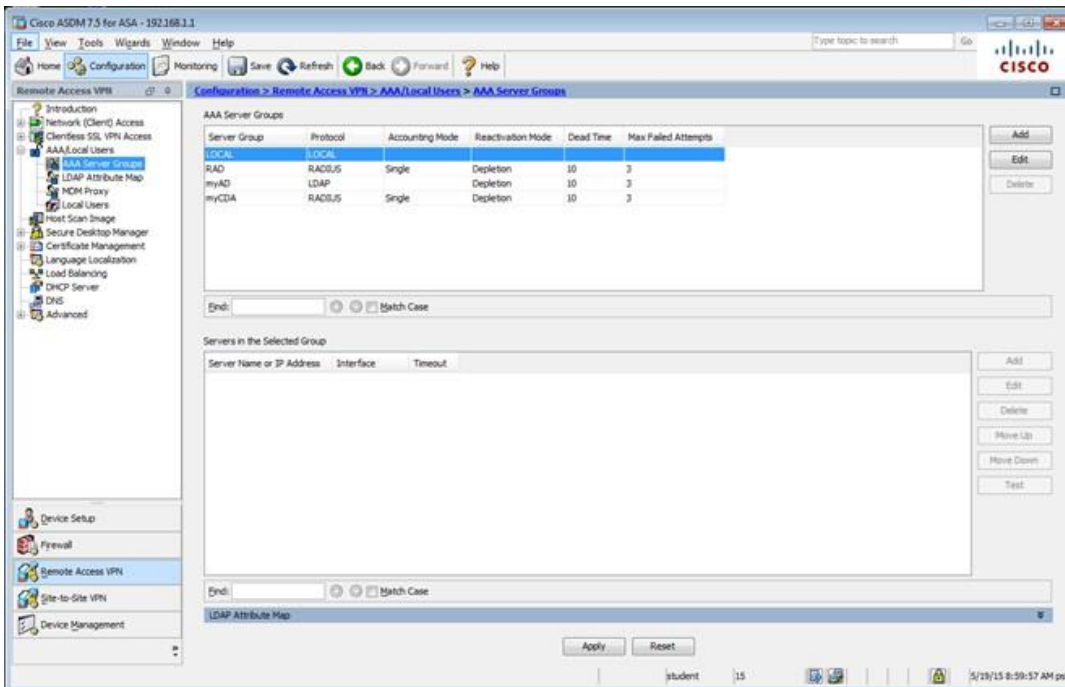
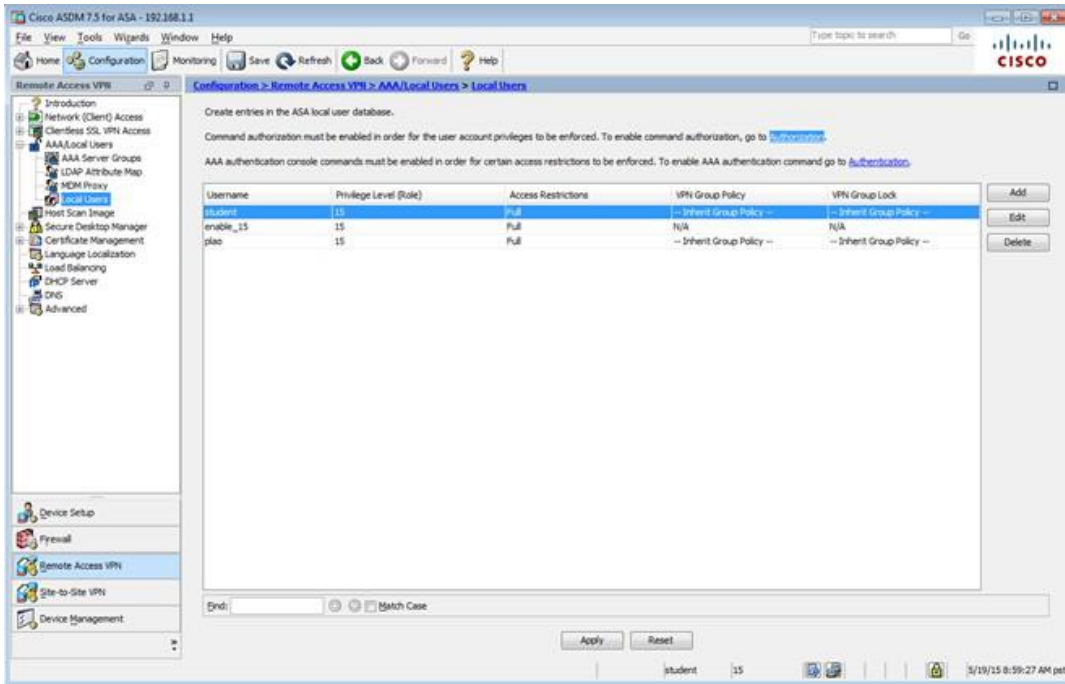
Bottom status bar: student 15 5/19/15 8:58:17 AM pst

The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AAA/Local Users' configuration page. It includes a list of items to be configured.

This section contains the following items:

- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users

Bottom status bar: student 15 5/19/15 8:58:57 AM pst



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

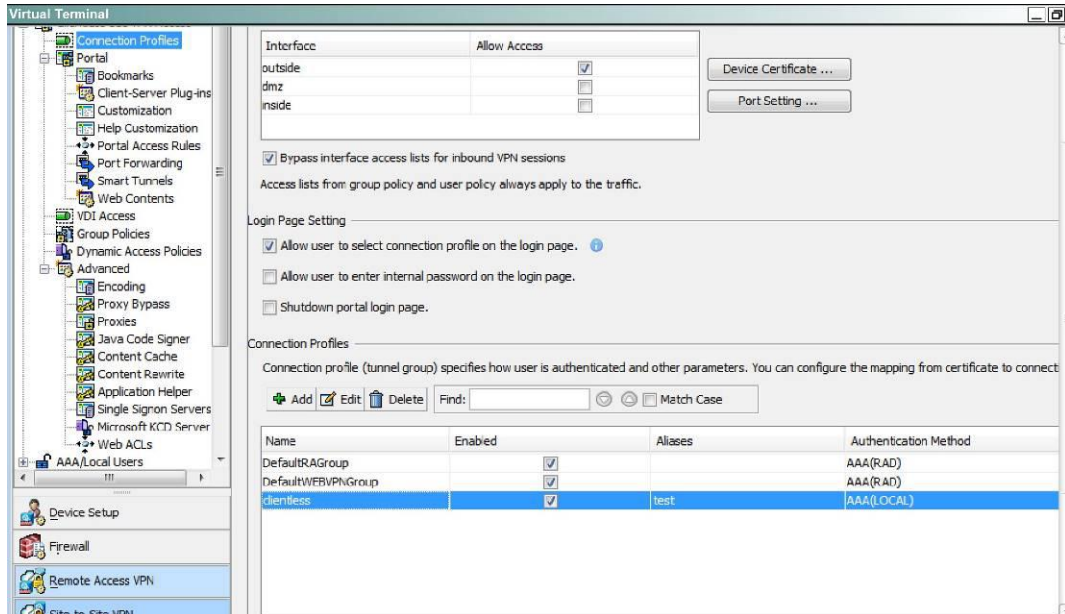
- A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
- B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
- C. The Inside-SRV bookmark references thehttps://192.168.1.2URL
- D. Only Clientless SSL VPN access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

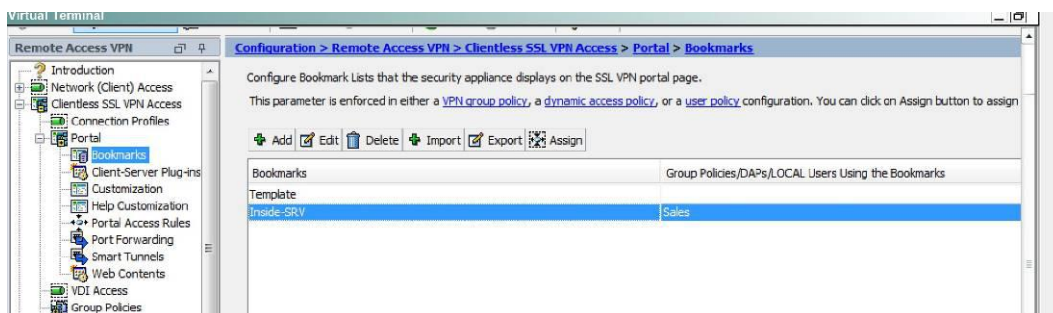
Answer: B,C

Explanation:

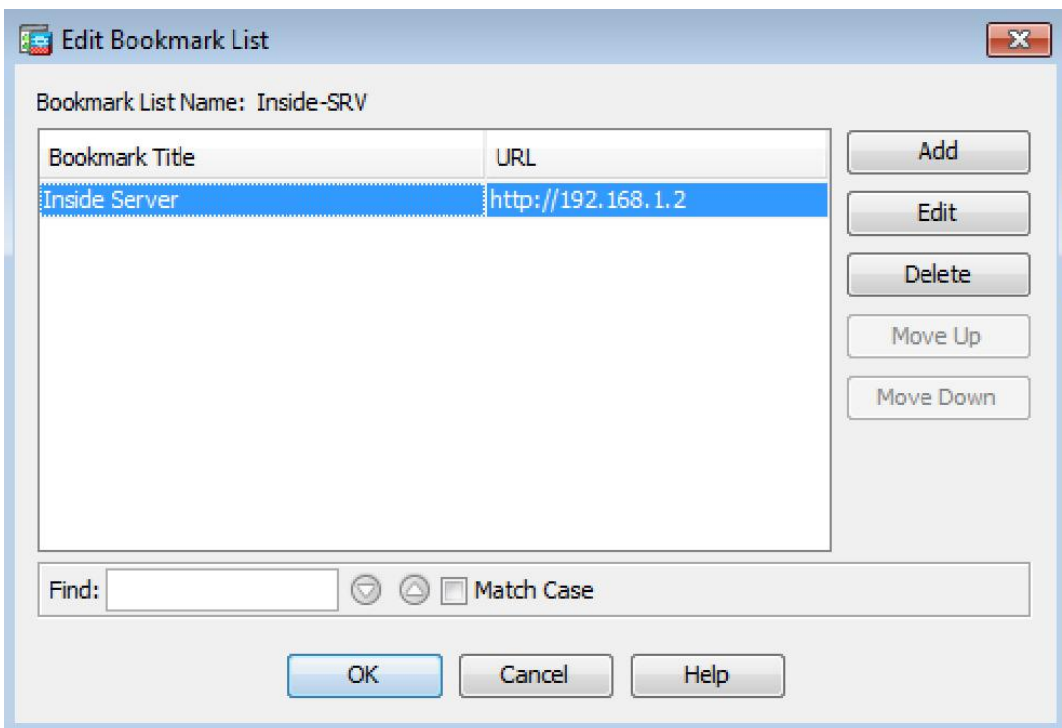
For B:



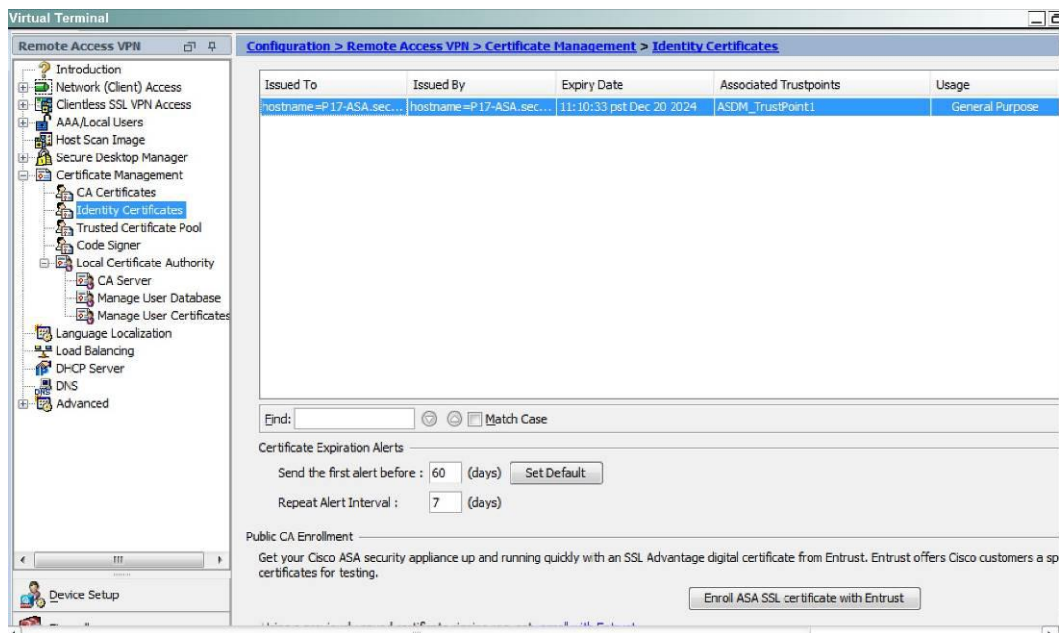
For C, Navigate to the Bookmarks tab:



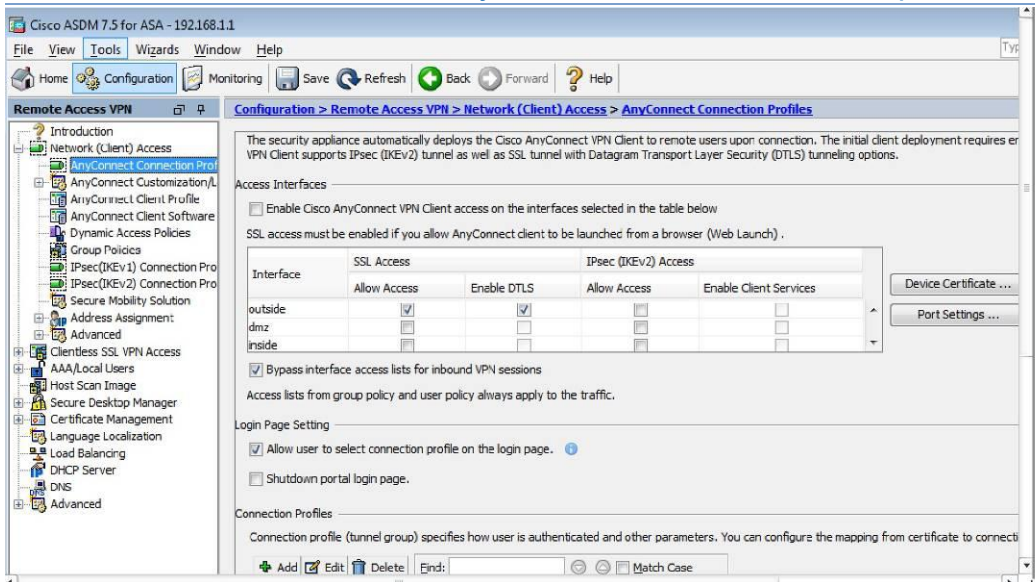
Then hit "edit" and you will see this:



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



Note E:



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

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

Answer: D

240. What port option in a PVLAN that can communicate with every other ports...

- A. promiscuous

Answer: A

241. Which type of layer 2 attack enables the attacker to intercept traffic that is intended for one specific recipient?

- A. BPDU attack
- B. DHCP Starvation
- C. CAM table overflow
- D. MAC address spoofing

Answer: D

242. Which type of attack is directed against the network directly:

- A. Denial of Service
- B. phishing
- C. trojan horse

Answer: A

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

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

Answer: A

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

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

Answer: A,B

245. Which security term refers to a person, property, or data of value to a company?

- A. Risk
- B. Asset
- C. Threat prevention
- D. Mitigation technique

Answer: B

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



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

Answer: A

247. Which quantifiable item should you consider when your organization adopts new technologies?

- A. threats
- B. vulnerability
- C. risk
- D. exploits

Answer: C

248. Which three statements are characteristics of DHCP Spoofing? (choose three)

- A. Arp Poisoning
- B. Modify Traffic in transit
- C. Used to perform man-in-the-middle attack
- D. Physically modify the network gateway
- E. Protect the identity of the attacker by masking the DHCP address
- F. can access most network devices

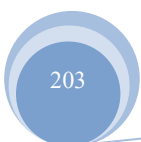
Answer: A,B,C

249. You are the security administrator for a large enterprise network with many remote locations. You have been given the assignment to deploy a Cisco IPS solution.

Where in the network would be the best place to deploy Cisco IOS IPS?

- A. Inside the firewall of the corporate headquarters Internet connection
- B. At the entry point into the data center
- C. Outside the firewall of the corporate headquarters Internet connection
- D. At remote branch offices

Answer: D





Explanation:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

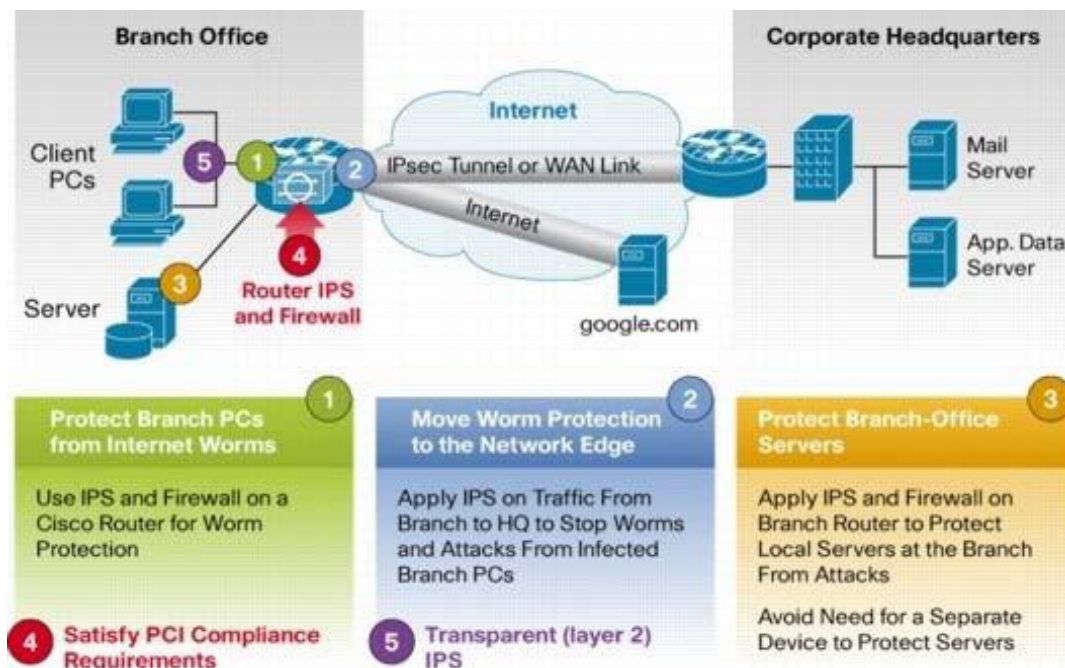
Product Overview

In today's business environment, network intruders and attackers can come from outside or inside the network.

They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical. Cisco IOS IPS: Major Use Cases and Key Benefits

IOS IPS helps to protect your network in 5 ways:



Key Benefits:

- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting



vulnerabilities in operating systems and applications.

- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks.
- Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies.
- Offers field-customizable worm and attack signature set and event actions.
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions.
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router.
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances.

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

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

Answer: B

251. When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)

- A. pass
- B. police
- C. inspect
- D. drop
- E. queue
- F. shape

Answer: A,C,D

Explanation:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080_8bc994.shtml

Zone-Based Policy Firewall Actions

ZFW provides three actions for traffic that traverses from one zone to another:

Drop — This is the default action for all traffic, as applied by the "class class-default" that terminates every inspect-type policy-map. Other class-maps within a policy-map can also be configured to drop unwanted traffic.

Traffic that is handled by the drop action is "silently" dropped (i.e., no notification of the drop is sent to the relevant end-host) by the ZFW, as opposed to an ACL's behavior of sending an ICMP "host unreachable" message to the host that sent the denied traffic. Currently, there is not an option to change the "silent drop" behavior. The log option can be added with drop for syslog notification that traffic was dropped by the firewall.

Pass — This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPSec ESP, IPSec AH, ISAKMP, and other inherently secure protocols with predictable behavior. However, most application traffic is better handled in the ZFW with the inspect action.

Inspect—The inspect action offers state-based traffic control. For example, if traffic from the private zone to the Internet zone in the earlier example network is inspected, the router maintains connection or session information for TCP and User Datagram Protocol (UDP) traffic. Therefore, the router permits return traffic sent from Internet-zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic.

Audit-trail can be applied with a parameter-map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.

252. Refer to the exhibit.

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

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



given output show?

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

Answer: A

253. 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.

Answer: A

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

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

Answer: B,F

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

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

Answer: A



256. Which two characteristics of symmetric encryption are true? (Choose two)

- A. It uses digital certificates.
- B. It uses a public key and a private key to encrypt and decrypt traffic.
- C. it requires more resources than asymmetric encryption
- D. it is faster than asymmetric encryption
- E. It uses the same key to encrypt and decrypt the traffic.

Answer: B,E

Explanation: <http://searchsecurity.techtarget.com/definition/secret-key-algorithm>

257. What's the technology that you can use to prevent non malicious program to run in the computer that is disconnected from the network?

- A. Firewall
- B. Software Antivirus
- C. Network IPS
- D. Host IPS.

Answer: D

258. Which option is the default value for the Diffie–Hellman group when configuring a site-to- site VPN on an ASA device?

- A. Group 1
- B. Group 2
- C. Group 5
- D. Group 7

Answer: B

259. Which network device does NTP authenticate?

- A. Only the time source
- B. Only the client device
- C. The firewall and the client device



D. The client device and the time source

Answer: A

260. Refer to the exhibit.

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

tacacs server tacacs2
  address ipv4 2.2.2.2
  timeout 20
  single-connection

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

Which statement about the given configuration is true?

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

Answer: A

261. Which IPS detection method can you use to detect attacks that based on the attackers IP addresses?

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

Answer: C

262. Refer to the exhibit.

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

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

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

Answer: A

263. 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.

Answer: A

264. 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.

Answer: A

265. Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

- A. next IP
- B. round robin



- C. dynamic rotation
- D. NAT address rotation

Answer: B

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

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

Answer: C

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

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

Answer: A

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

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

Answer: B,D,F

269. A Cisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0.



By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

- A. outbound traffic initiated from the inside to the DMZ
- B. outbound traffic initiated from the DMZ to the outside
- C. outbound traffic initiated from the inside to the outside
- D. inbound traffic initiated from the outside to the DMZ
- E. inbound traffic initiated from the outside to the inside
- F. inbound traffic initiated from the DMZ to the inside
- G. HTTP return traffic originating from the inside network and returning via the outside interface
- H. HTTP return traffic originating from the inside network and returning via the DMZ interface
- I. HTTP return traffic originating from the DMZ network and returning via the inside interface
- J. HTTP return traffic originating from the outside network and returning via the inside interface

Answer: A,B,C,G,H

Explanation:

<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html> Security Level

Overview

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between Interfaces on the Same Security Level" section for more information.

The level controls the following behavior:

- Network access — By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface. If you enable communication for same security interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.
- Inspection engines — Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.



–NetBIOS inspection engine—Applied only for outbound connections.

–OraServ inspection engine — If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

•Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.

•NAT control — When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

•established command — This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For same security interfaces, you can configure established commands for both directions.

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

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

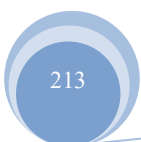
Answer: B

271. Which two characteristics of the TACACS+ protocol are true? (Choose two.)

- A. uses UDP ports 1645 or 1812
- B. separates AAA functions
- C. encrypts the body of every packet
- D. offers extensive accounting capabilities
- E. is an open RFC standard protocol

Answer: B,C

Explanation:





http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Packet

Encryption

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.

Authentication and Authorization RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

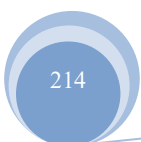
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

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

(Choose two.)

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

Answer: B,C





273. # nat (inside,outside) dynamic interface

Refer to the above. Which translation technique does this configuration result in?

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

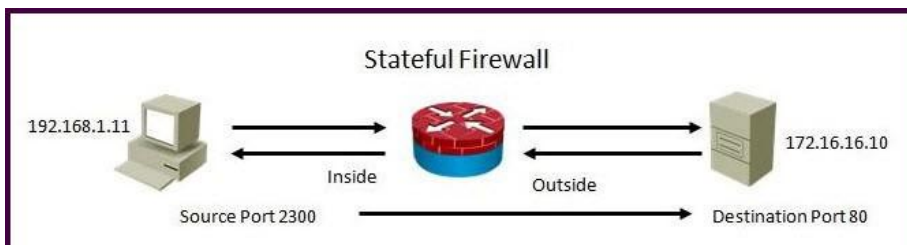
Answer: C

274. How to verify that TACACS+ connectivity to a device?

- A. You successfully log in to the device by using the local credentials.
- B. You connect to the device using SSH and receive the login prompt.
- C. You successfully log in to the device by using ACS credentials.
- D. You connect via console port and receive the login prompt.

Answer: B

275. Refer to the exhibit.



Using a stateful packet firewall and given an inside ACL entry of permit ip 192.16.1.0

0.0.0.255 any, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL?

- A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300
- B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
- C. permit tcp any eq 80 host 192.168.1.11 eq 2300
- D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Answer: A

Explanation:



http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/fwinsp.html

Understanding Inspection Rules

Inspection rules configure Context-Based Access Control (CBAC) inspection commands. CBAC inspects traffic that travels through the device to discover and manage state information for TCP and UDP sessions. The device uses this state information to create temporary openings to allow return traffic and additional data connections for permissible sessions.

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when inspected traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered inspection when exiting through the firewall.

Inspection rules are applied after your access rules, so any traffic that you deny in the access rule is not inspected. The traffic must be allowed by the access rules at both the input and output interfaces to be inspected. Whereas access rules allow you to control connections at layer 3 (network, IP) or 4 (transport, TCP or UDP protocol), you can use inspection rules to control traffic using application-layer protocol session information.

For all protocols, when you inspect the protocol, the device provides the following functions:

- Automatically opens a return path for the traffic (reversing the source and destination addresses), so that you do not need to create an access rule to allow the return traffic. Each connection is considered a session, and the device maintains session state information and allows return traffic only for valid sessions.

Protocols that use TCP contain explicit session information, whereas for UDP applications, the device models the equivalent of a session based on the source and destination addresses and the closeness in time of a sequence of UDP packets.

These temporary access lists are created dynamically and are removed at the end of a session.

- Tracks sequence numbers in all TCP packets and drops those packets with sequence numbers that are not within expected ranges.
- Uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. When a session is dropped, or reset, the device informs



both the source and destination of the session to reset the connection, freeing up resources and helping to mitigate potential Denial of Service (DoS) attacks.

276. What are two challenges faced when deploying host-level IPS? (Choose Two)

- A. The deployment must support multiple operating systems.
- B. It does not provide protection for offsite computers.
- C. It is unable to provide a complete network picture of an attack.
- D. It is unable to determine the outcome of every attack that it detects.
- E. It is unable to detect fragmentation attacks.

Answer: A,B

Explanation:

Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.

Limitations of HIPS: There are two major drawbacks to HIPS:

- + HIPS does not provide a complete network picture: Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network.
- + HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network.

Source: <http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3>

277. Which command is used to verify that a VPN connection is established between two endpoints and that the connection is passing?

- A. Firewall#sh crypto ipsec sa
- B. Firewall#sh crypto isakmp sa
- C. Firewall#debug crypto isakmp
- D. Firewall#sh crypto session



Answer: A

278. With which technology do apply integrity, confidentiality and authenticate the source

- A. IPSec
- B. IKE
- C. Certificate authority
- D. Data encryption standards

Answer: A

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

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

Answer: A,D,E

280. What do you use when you have a network object or group and want to use an IP address?

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

Answer: B

281. Which two features are commonly used CoPP and CPPr 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

Answer: A,B

282. 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.

Answer: C

283. Which Firepower Management Center feature detects and blocks exploits and hack attempts?

- A. intrusion prevention
- B. advanced malware protection
- C. content blocker
- D. file control

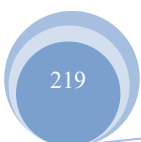
Answer: D

284. Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?

- A. You must configure two zone pairs, one for each direction.
- B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
- C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self zone.
- D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Answer: A

285. Which IOS command do you enter to test authentication against a AAA server?





- A. dialer aaa suffix <suffix> password <password>
- B. ppp authentication chap pap test
- C. aaa authentication enable default test group tacacs+
- D. test aaa-server authentication dialergroup username <user> password.

Answer: D

286. 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.

Answer: A

287. Diffie-Hellman key exchange question

- A. IKE

Answer: A

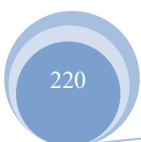
288. Within an 802.1X enabled network with the Auth Fail feature configured, when does a switch port get placed into a restricted VLAN?

- A. When 802.1X is not globally enabled on the Cisco catalyst switch
- B. When AAA new-model is enabled
- C. When a connected client fails to authenticate after a certain number of attempts
- D. If a connected client does not support 802.1X
- E. After a connected client exceeds a specific idle time

Answer: C

289. How does PEAP protect the EAP exchange?

- A. It encrypts the exchange using the server certificate.





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

Answer: A

290. 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.

Answer: A

291. CORRECT TEXT

Scenario

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

New additional connectivity requirements:

Once the correct ASA configurations have been configured: To access ASDM, click the ASA icon in the topology diagram.

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

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

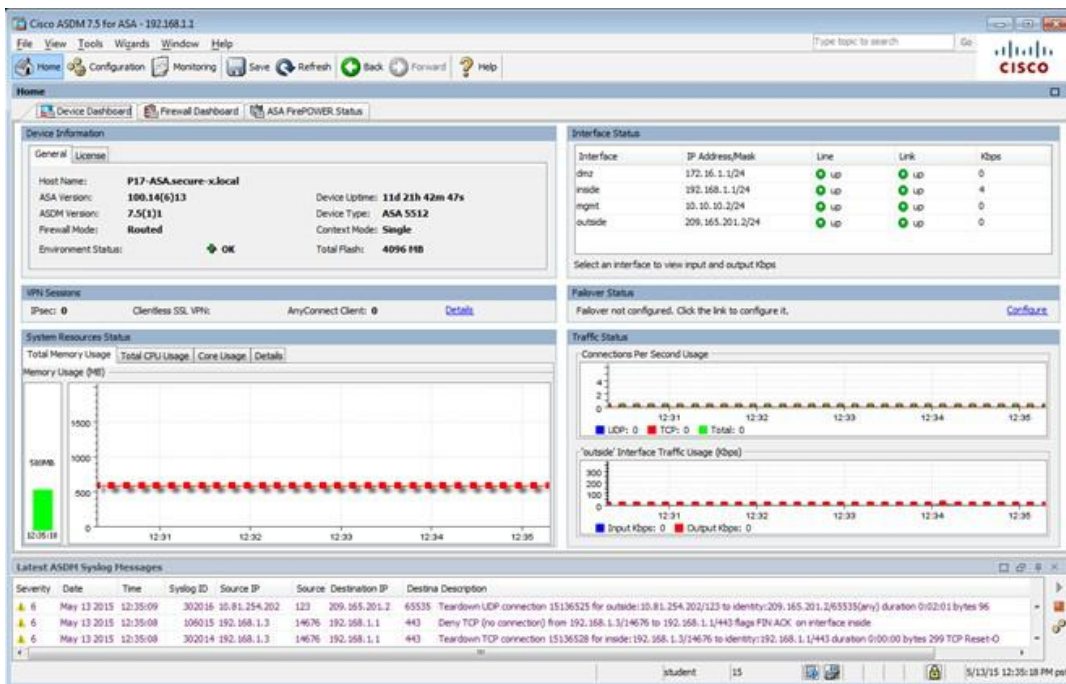
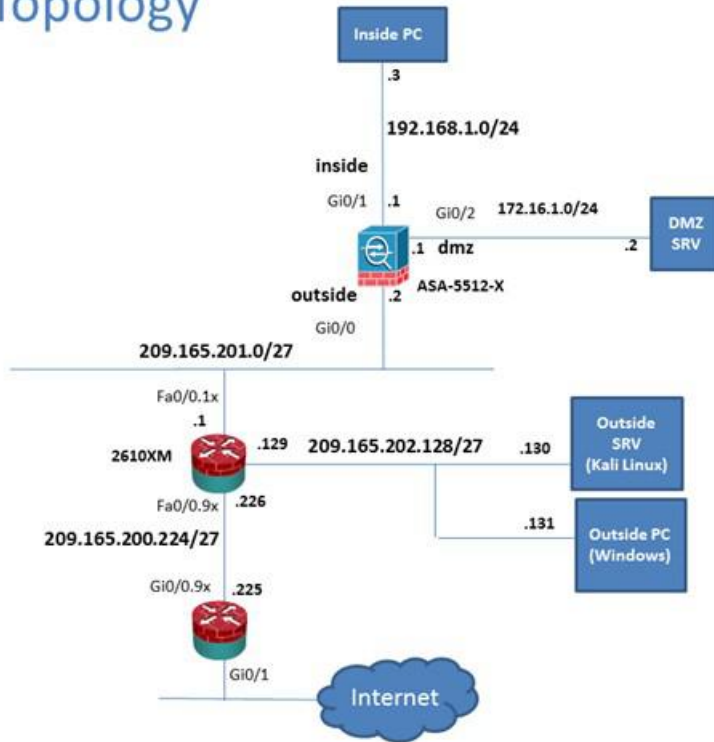
Note:

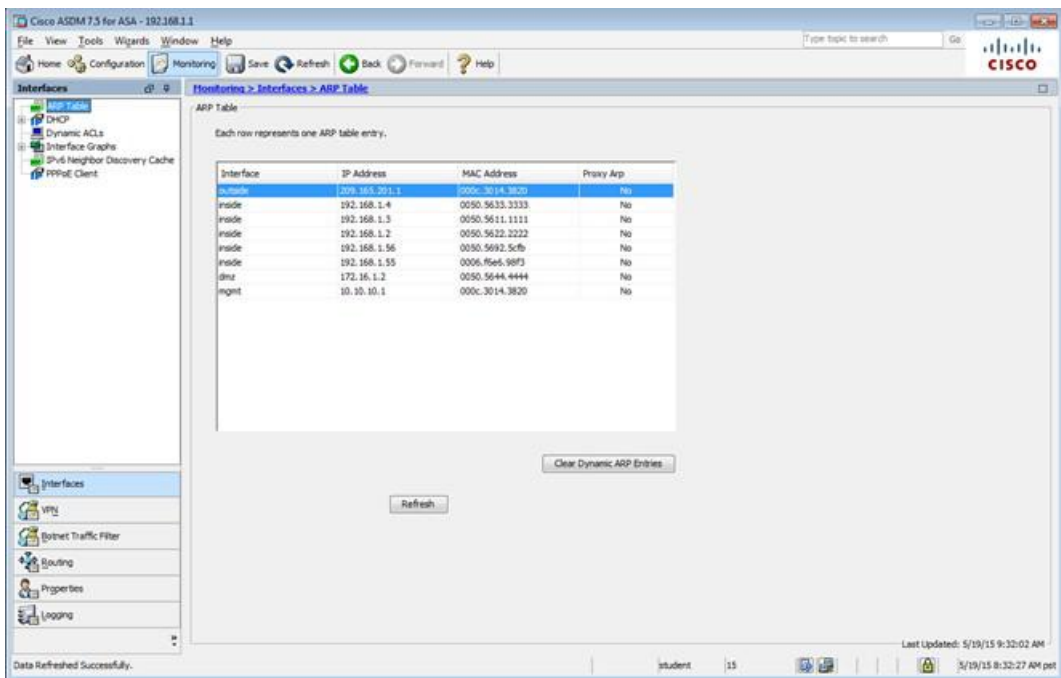
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.

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

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

Lab Topology





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

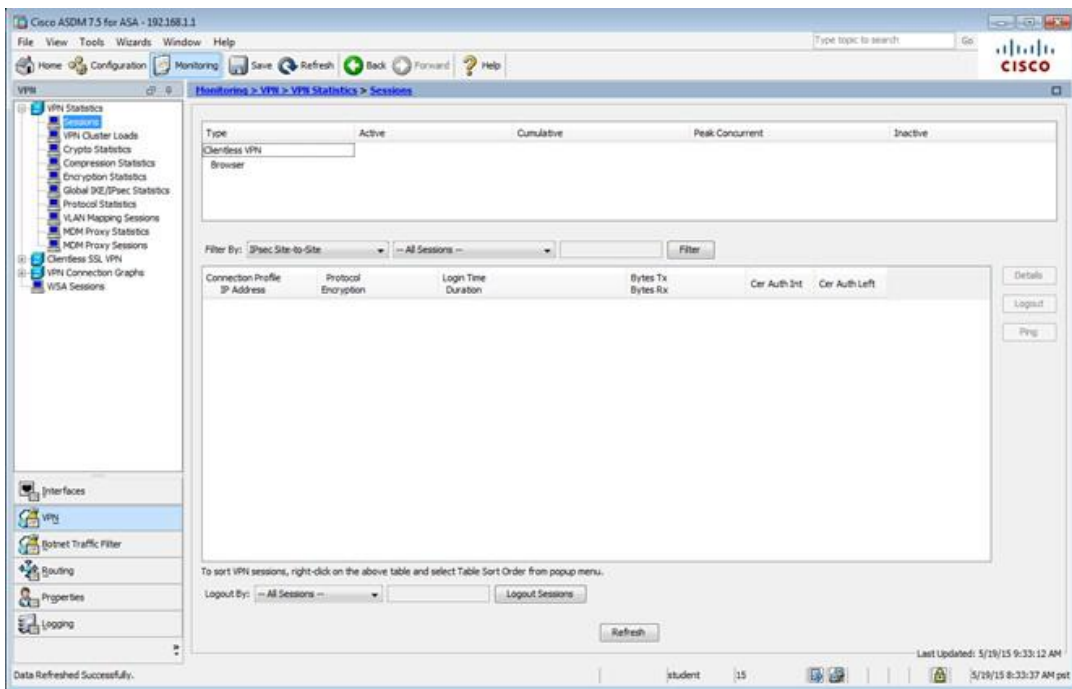
Interface	IP Address	MAC Address	Proxy Arp
inside	192.168.1.1	0050.5633.3333	No
inside	192.168.1.4	0050.5611.1111	No
inside	192.168.1.2	0050.5612.2222	No
inside	192.168.1.56	0050.5692.5cfa	No
inside	192.168.1.55	0006.f6e6.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
mgmt	10.10.10.1	000c.3014.3820	No

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

Sessions

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

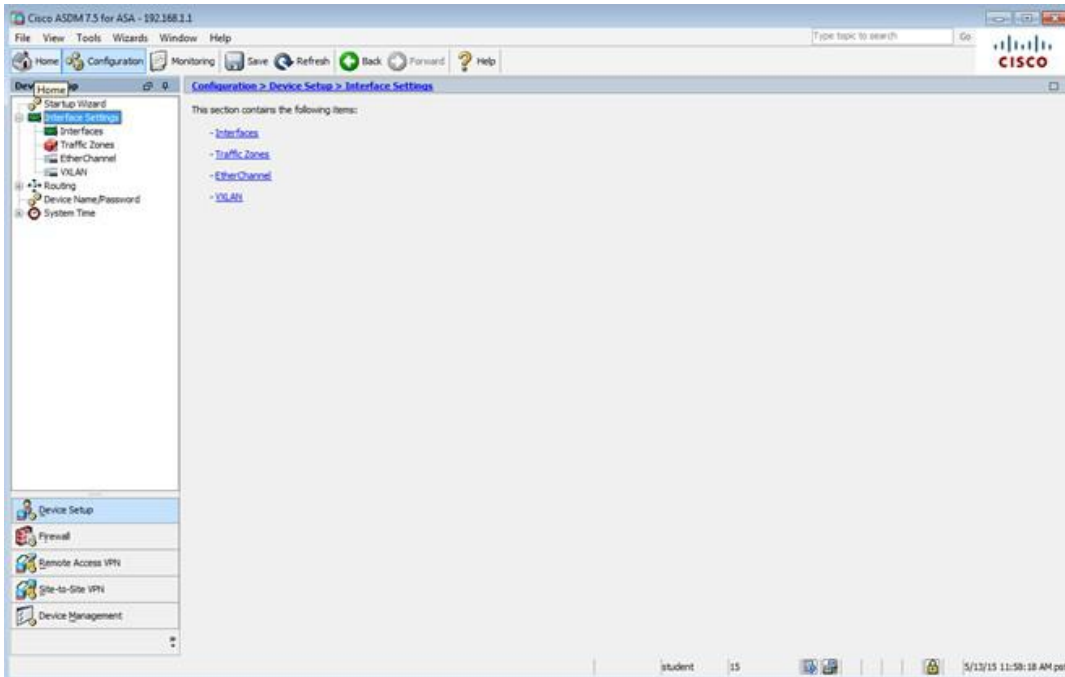
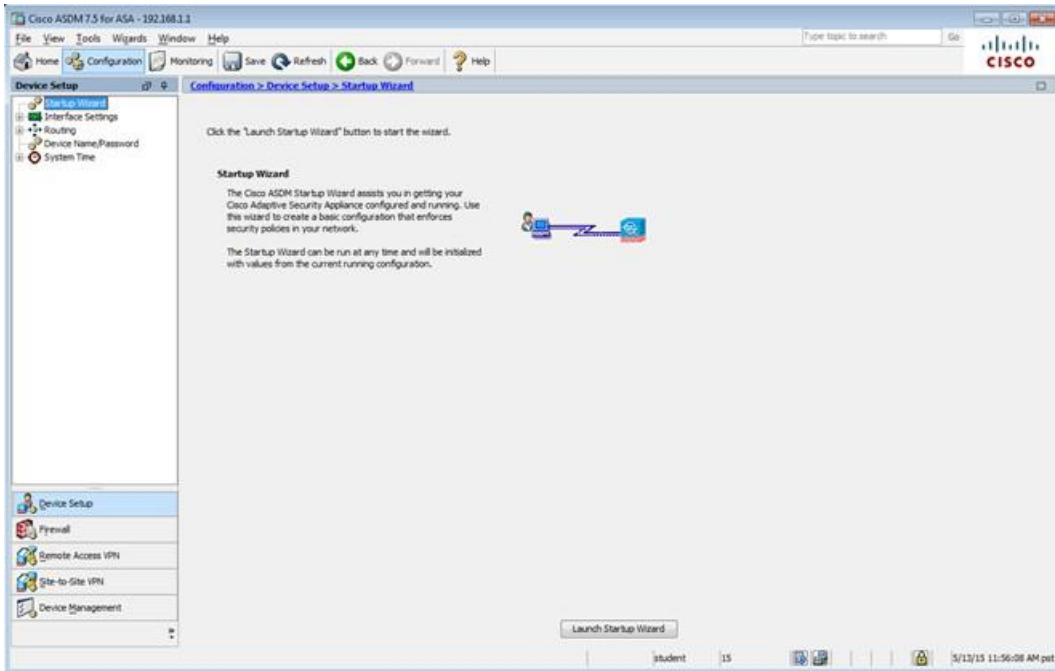
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

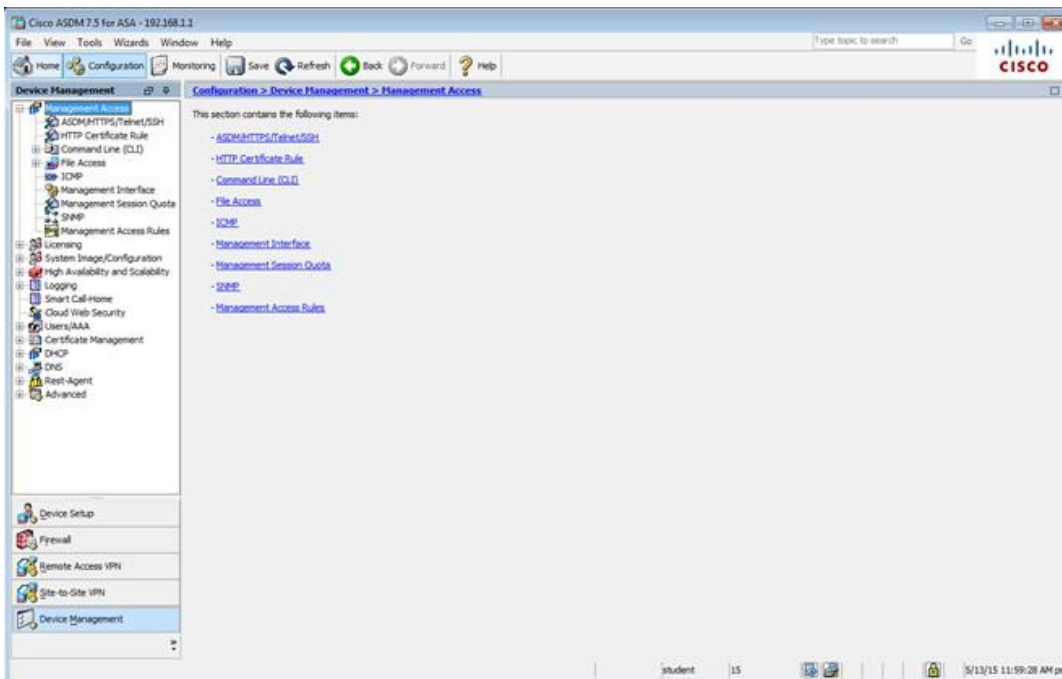
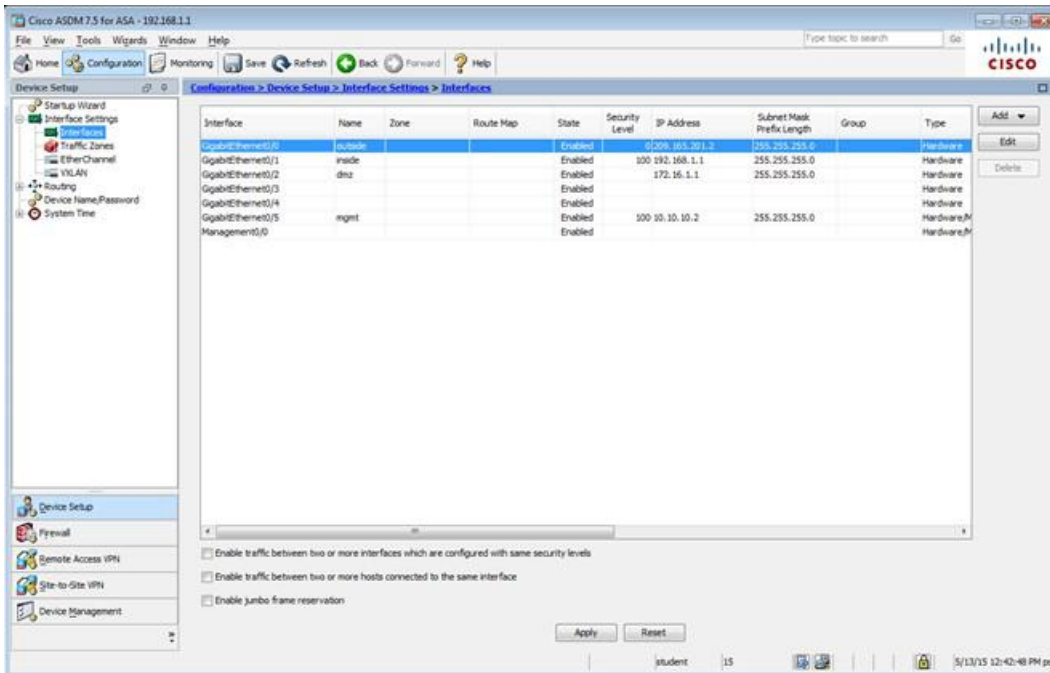
Logout By: -- All Sessions -- Logout Sessions Refresh

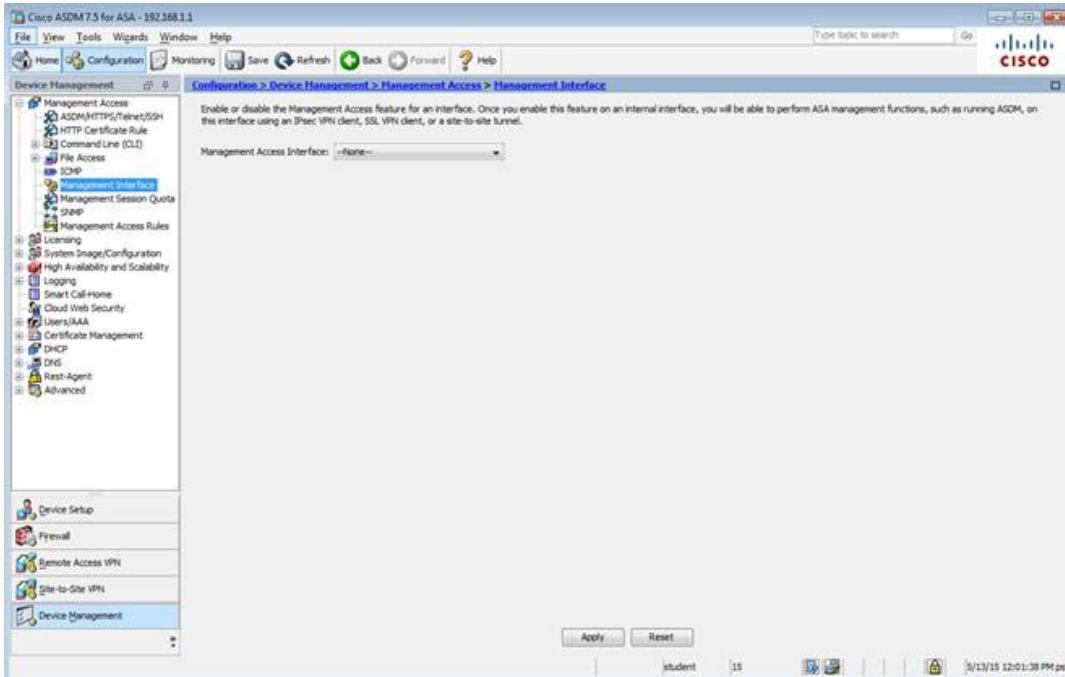
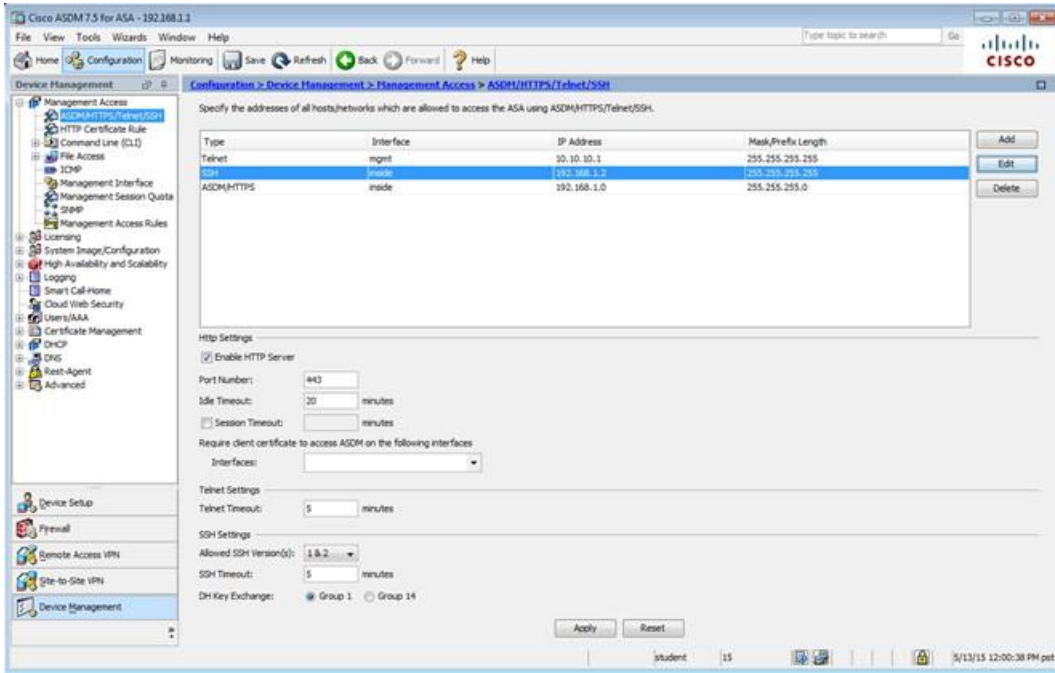
Data Refreshed Successfully.

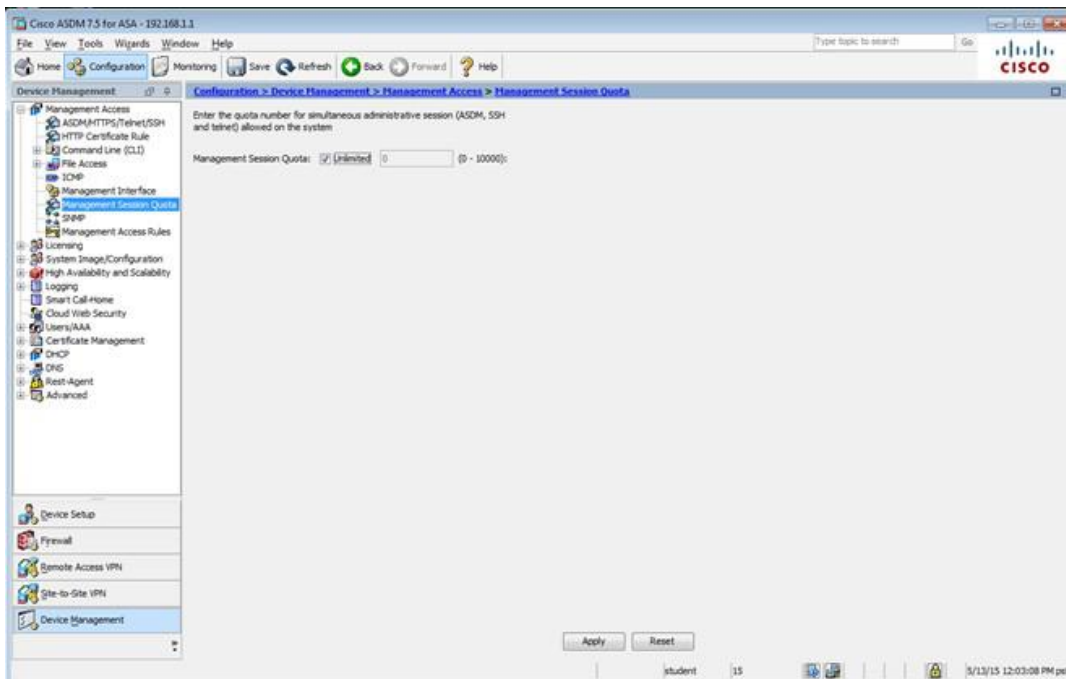
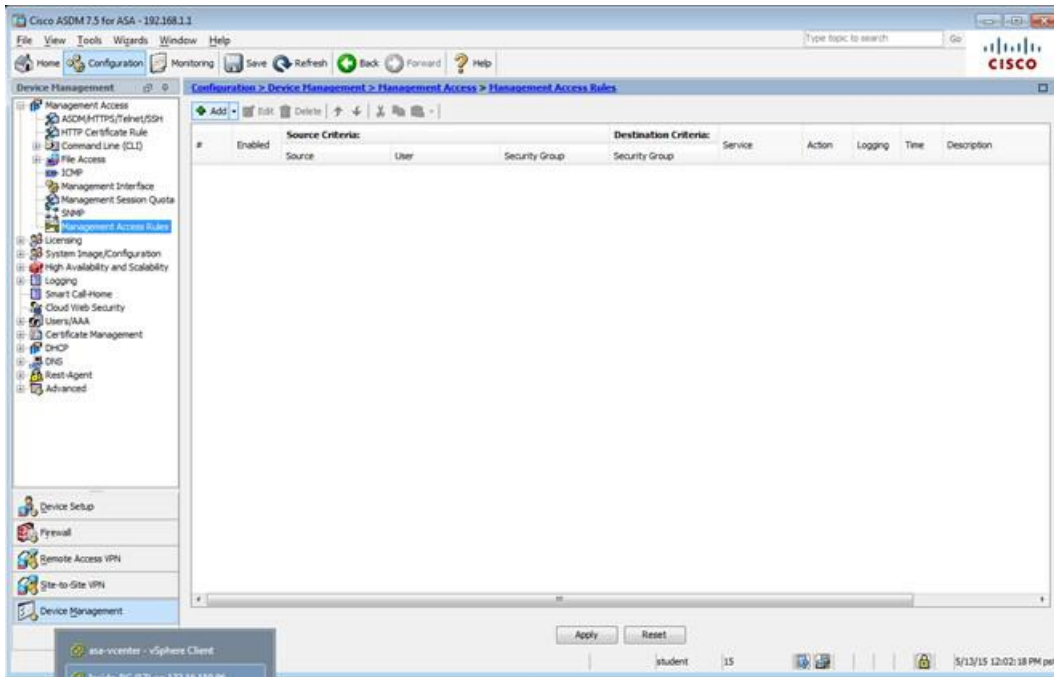
Last Updated: 5/19/15 9:33:12 AM

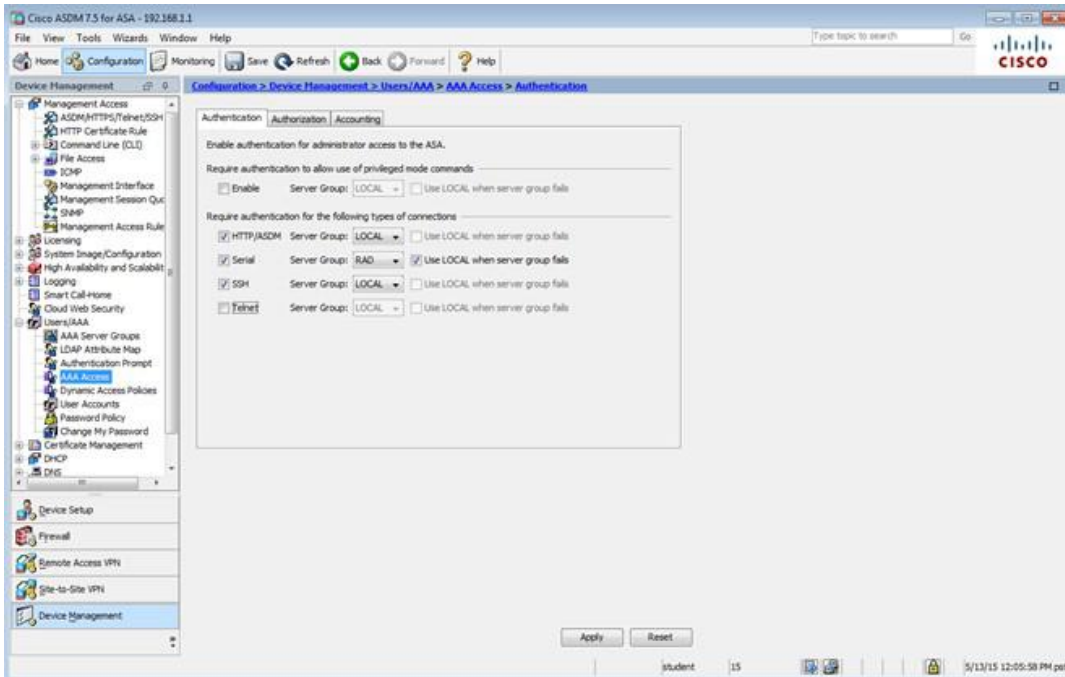
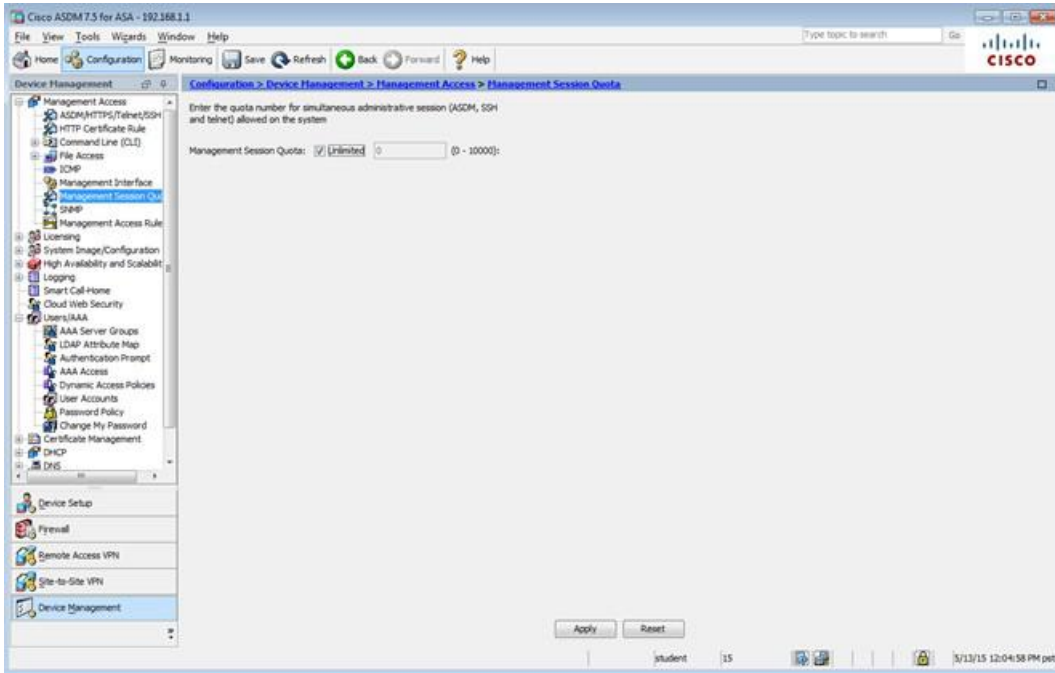
Filter By: Clientless SSL VPN -- All Sessions -- Filter

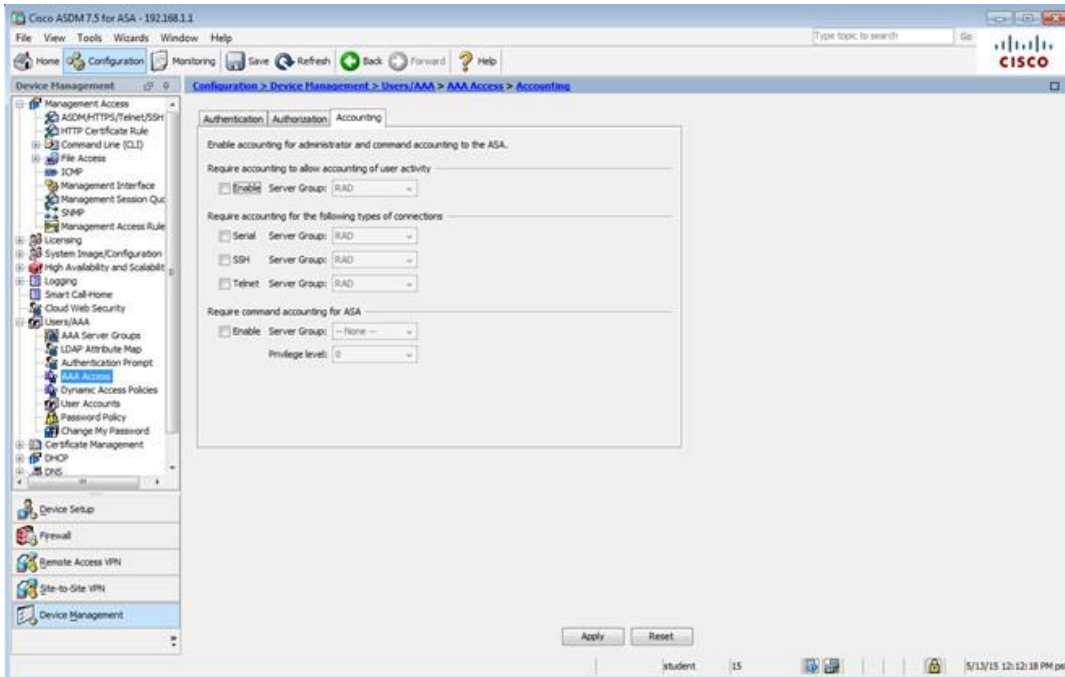
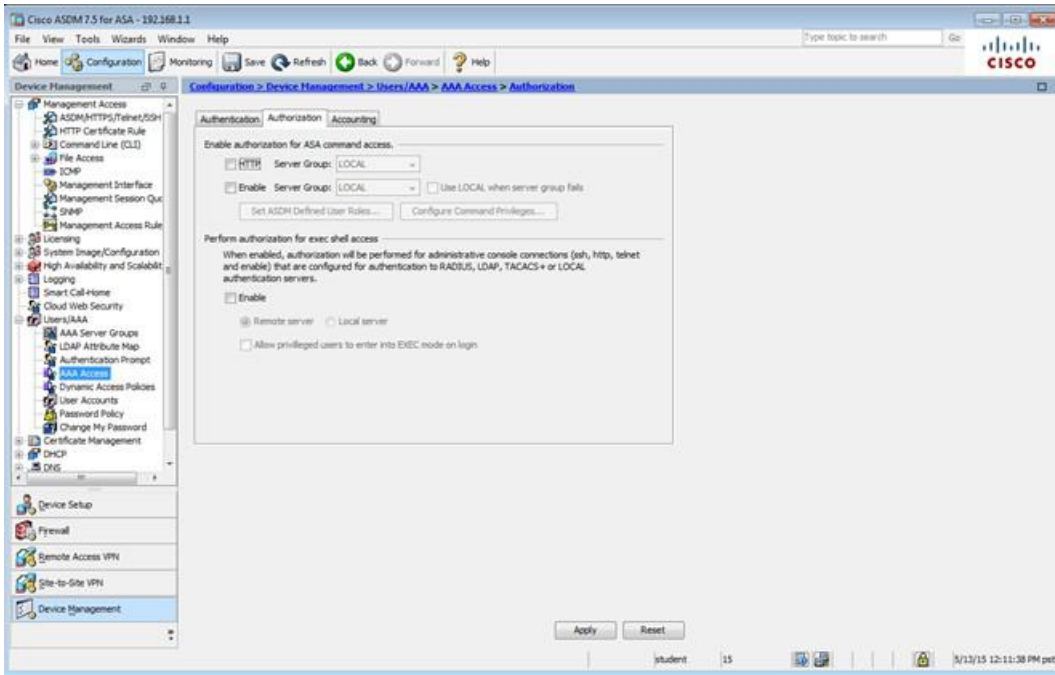


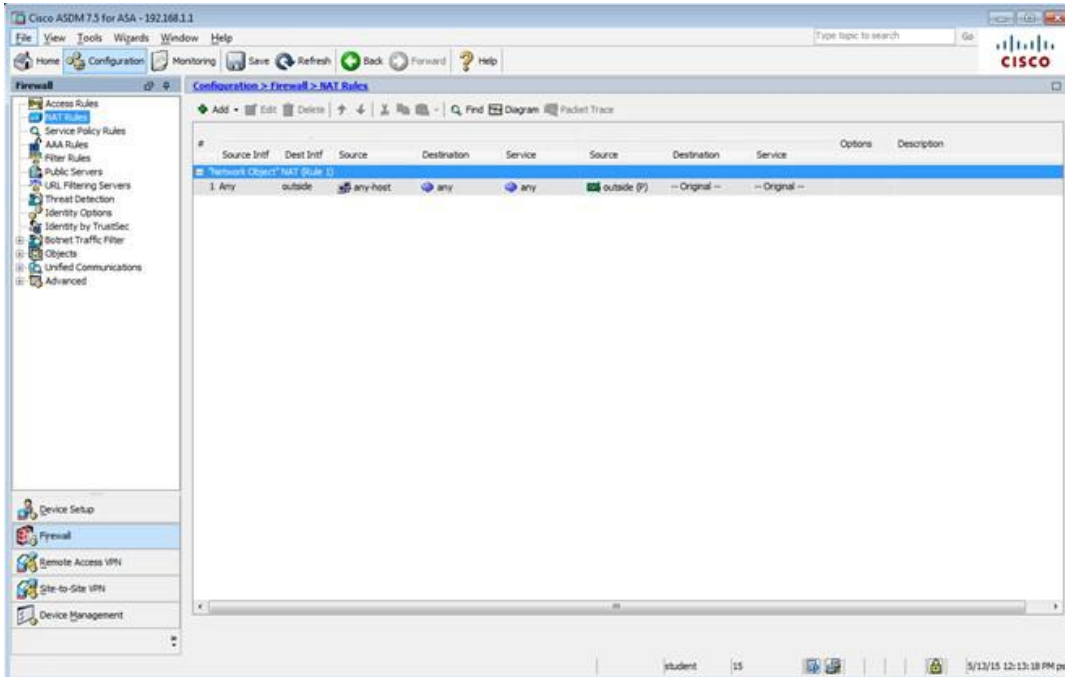
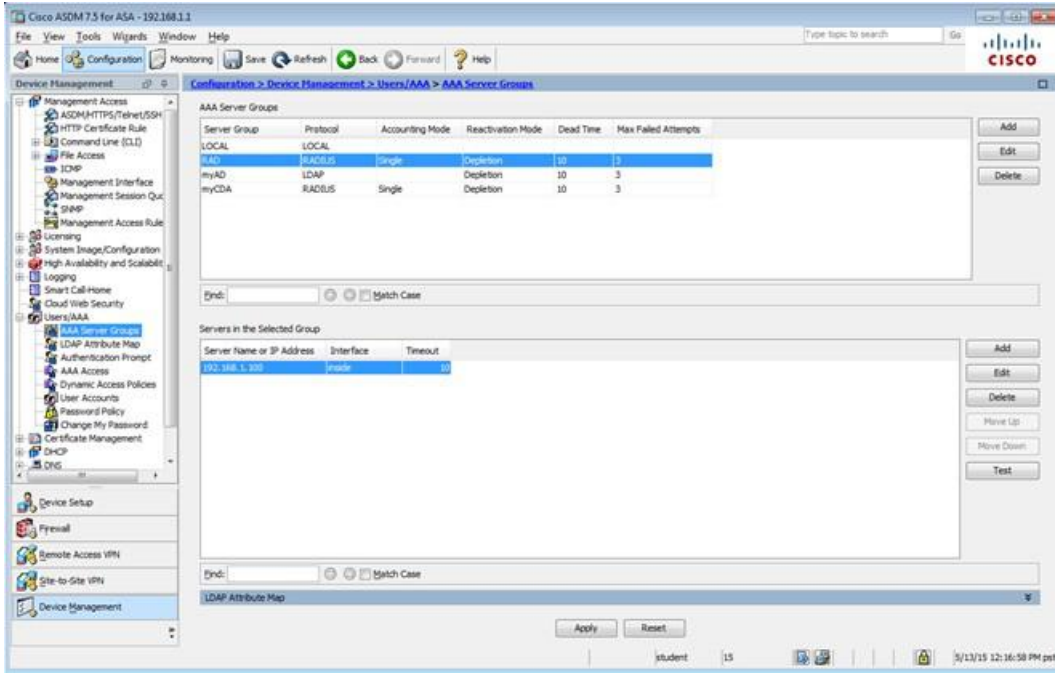


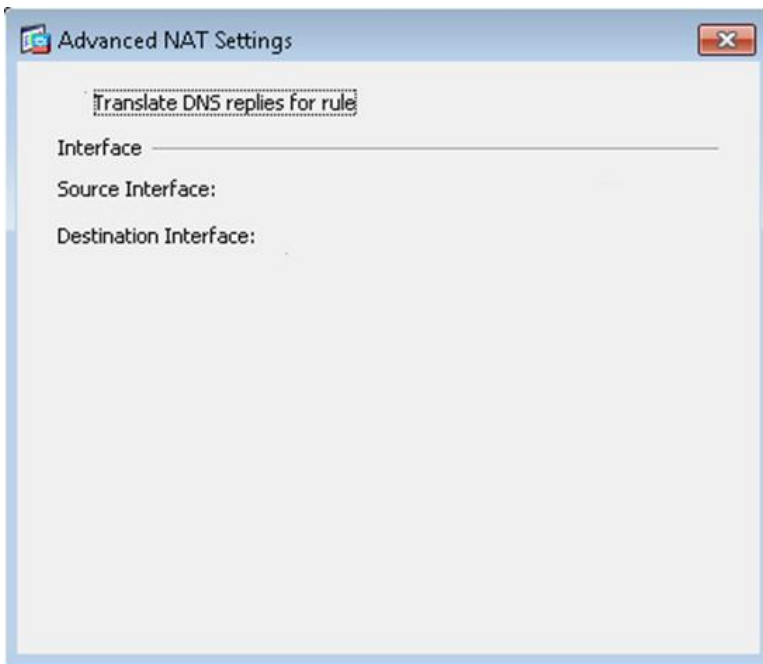
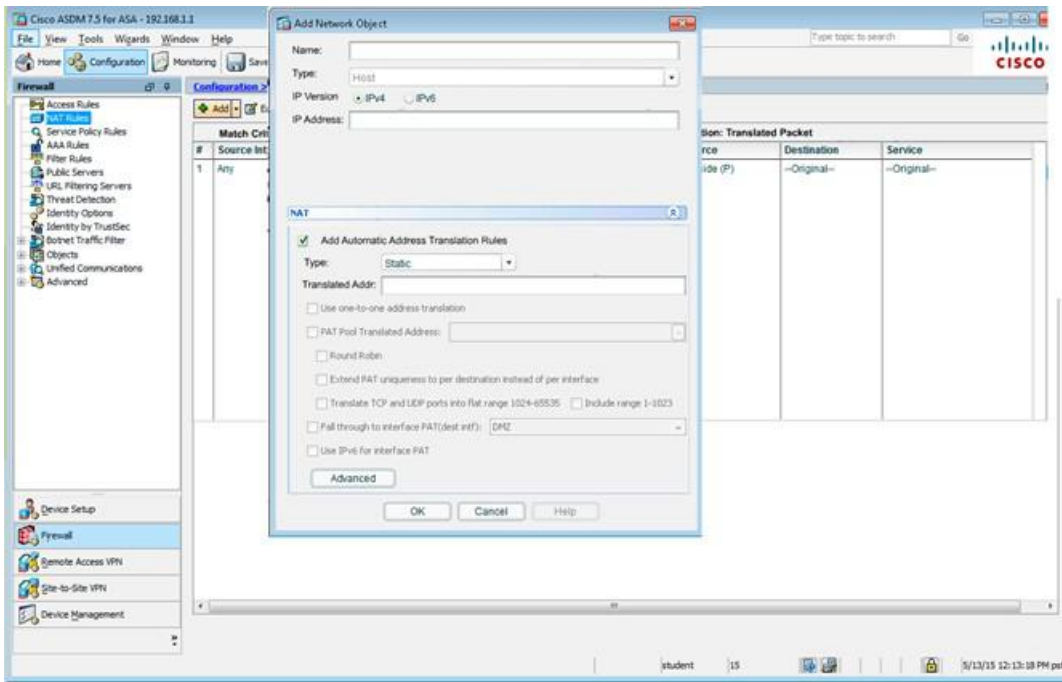


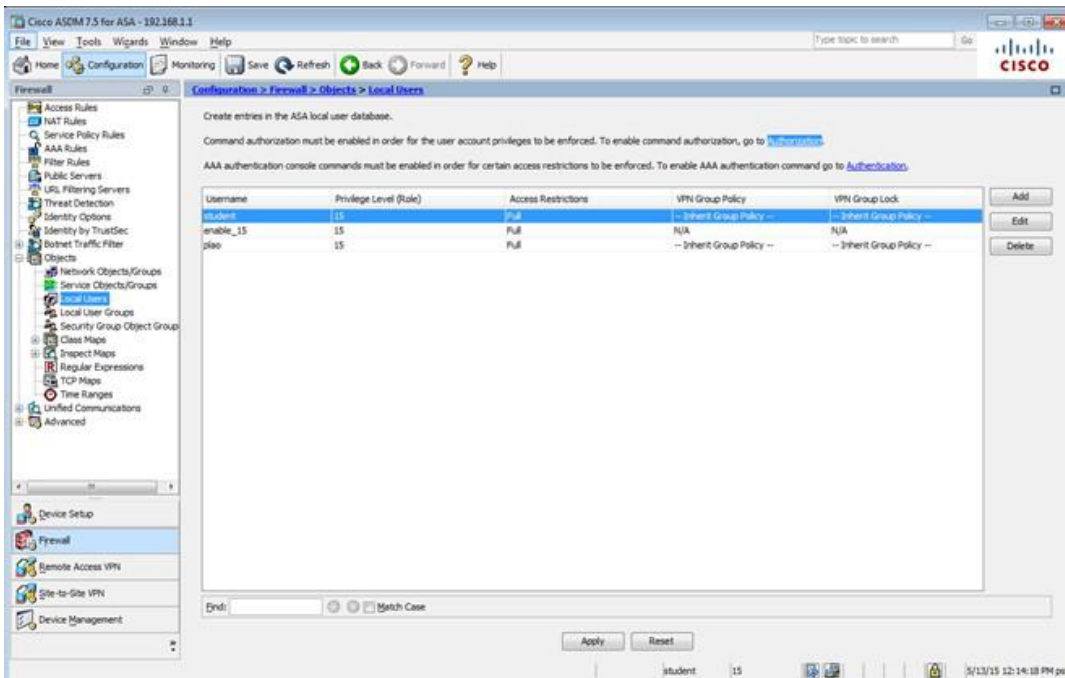
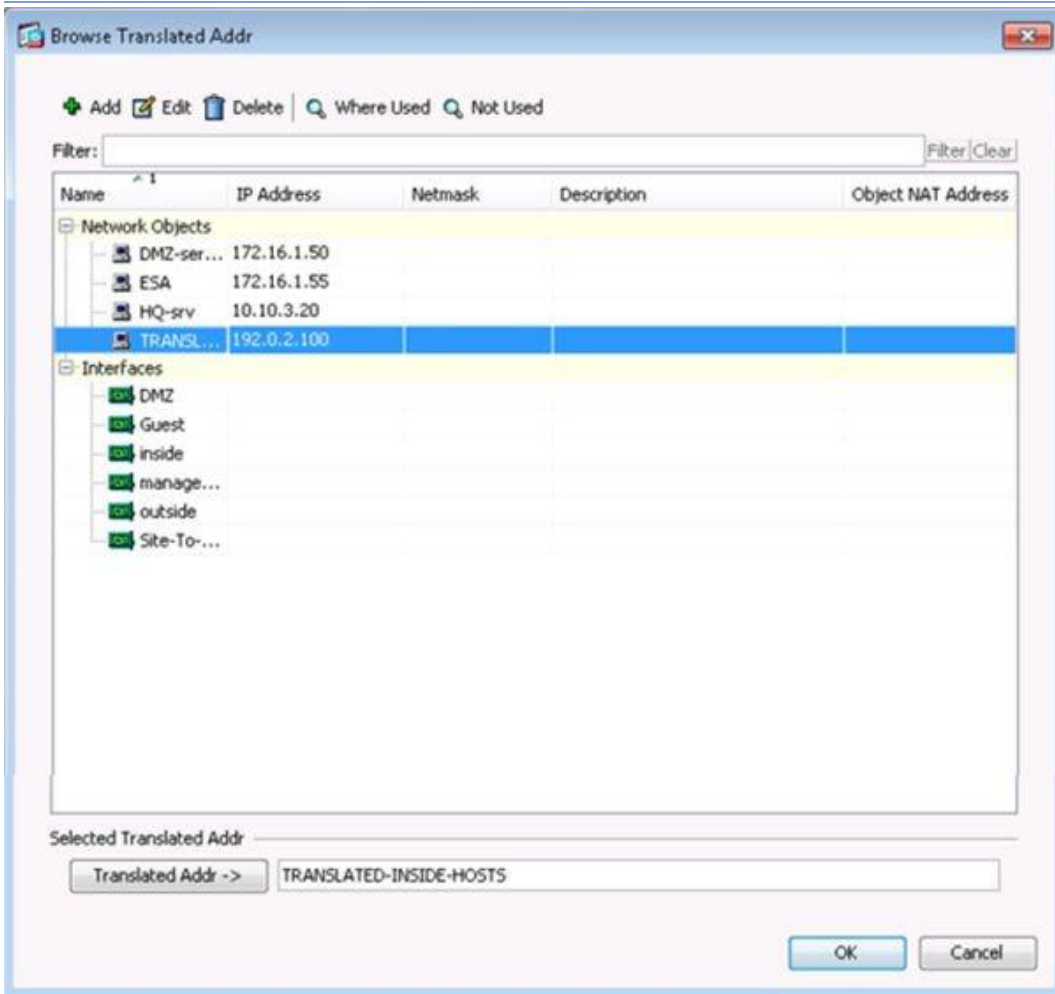


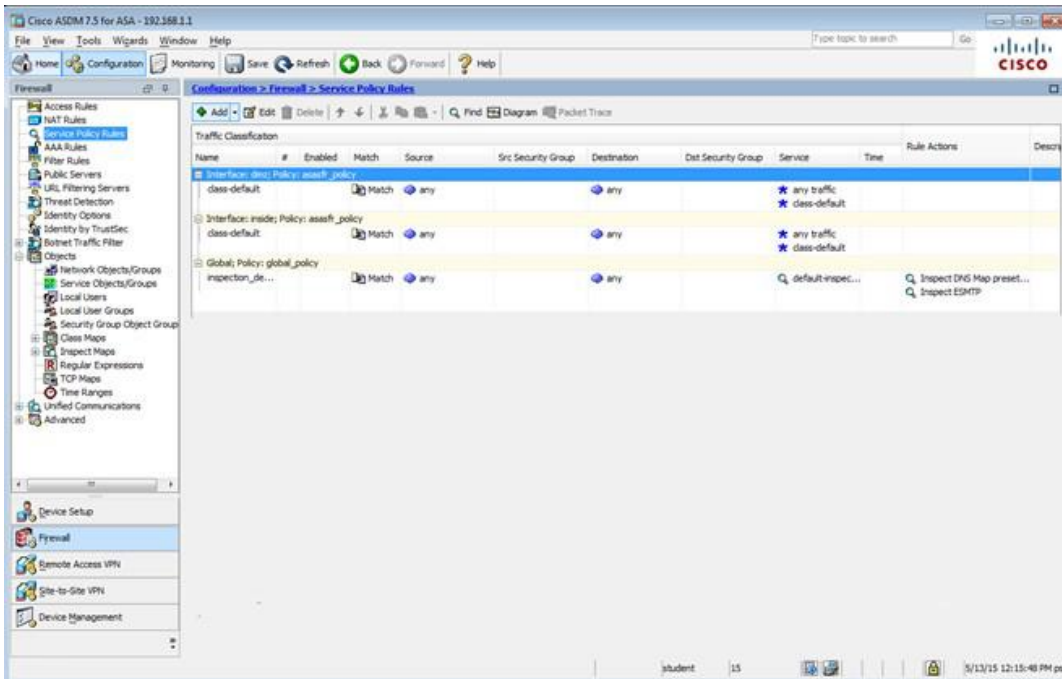
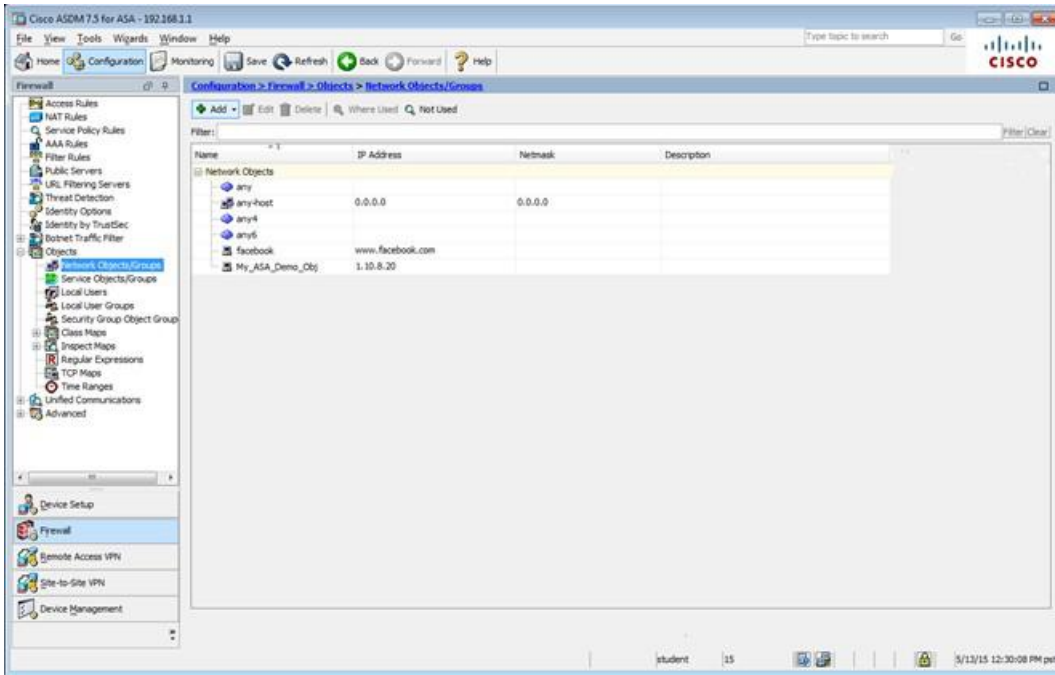












Edit Service Policy Rule

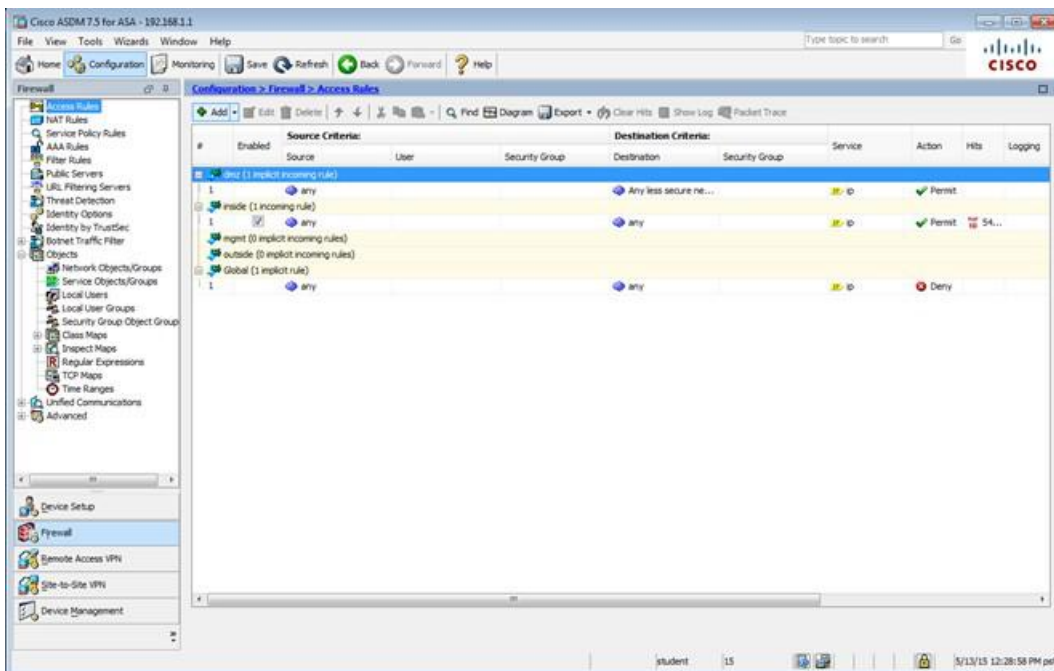
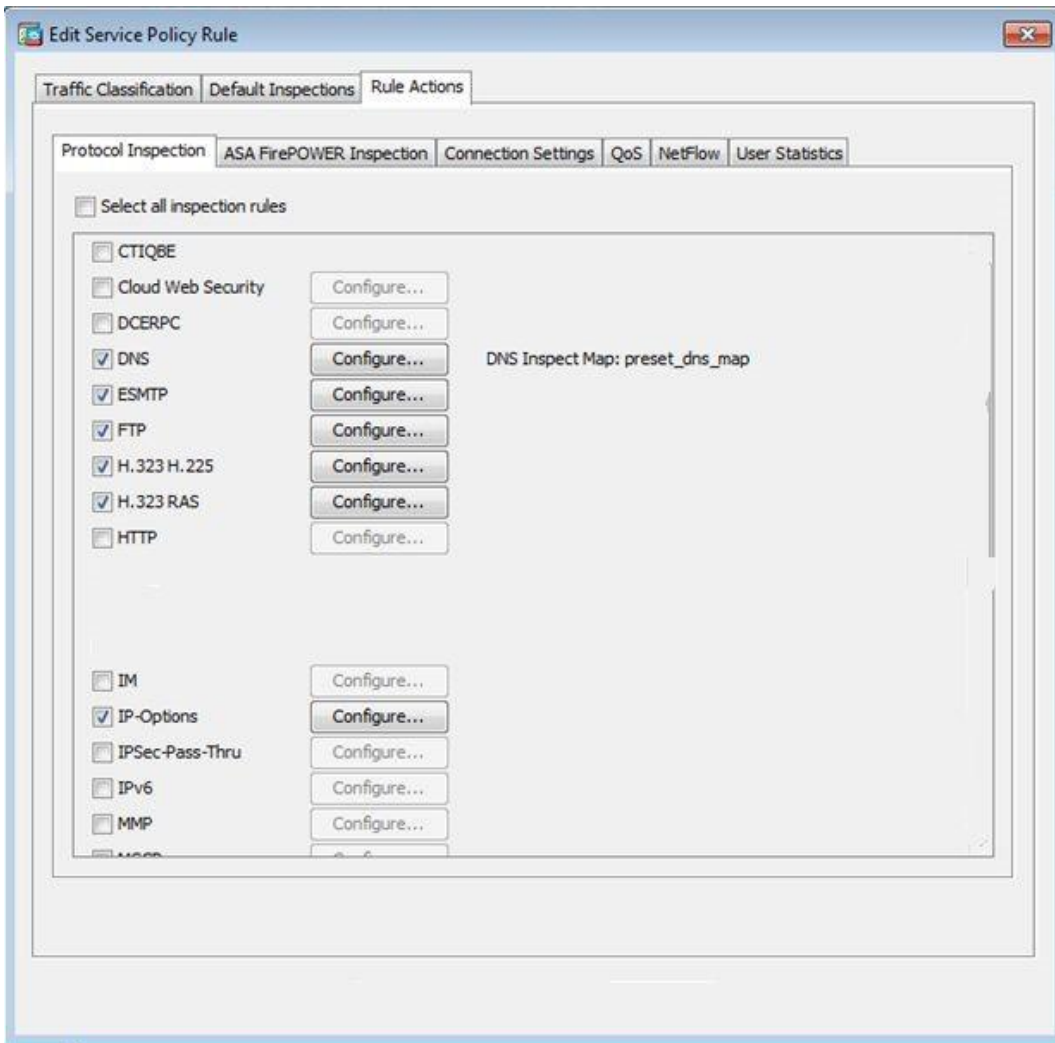
Traffic Classification | Default Inspections | Rule Actions

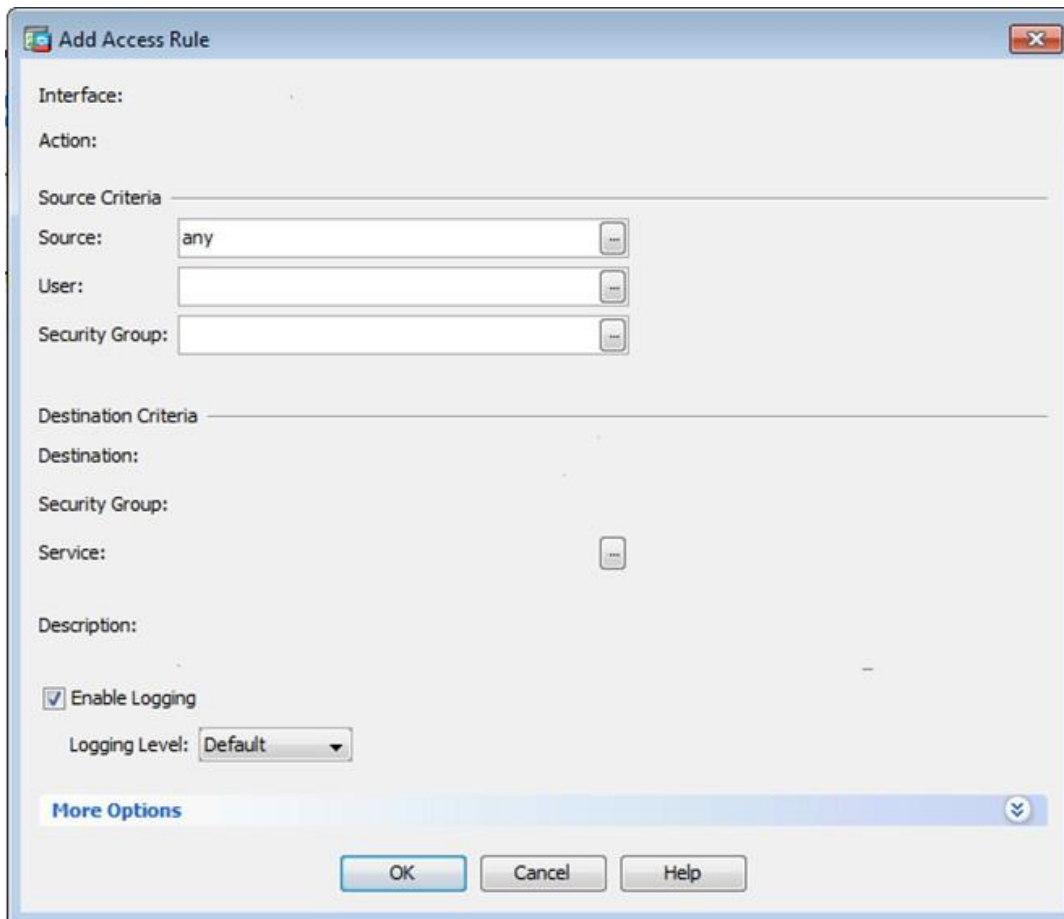
Name: inspection_default

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





The image shows a Windows-style dialog box titled "Add Access Rule". It contains several sections for configuring an access rule. The "Source Criteria" section includes fields for "Source" (set to "any"), "User", and "Security Group", each with a browse button. The "Destination Criteria" section includes fields for "Destination", "Security Group", and "Service", also with browse buttons. There is a "Description" text area. At the bottom, there is a checkbox for "Enable Logging" which is checked, and a "Logging Level" dropdown menu set to "Default". A "More Options" link with a dropdown arrow is located below the logging settings. At the very bottom are "OK", "Cancel", and "Help" buttons.

Interface:

Action:

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

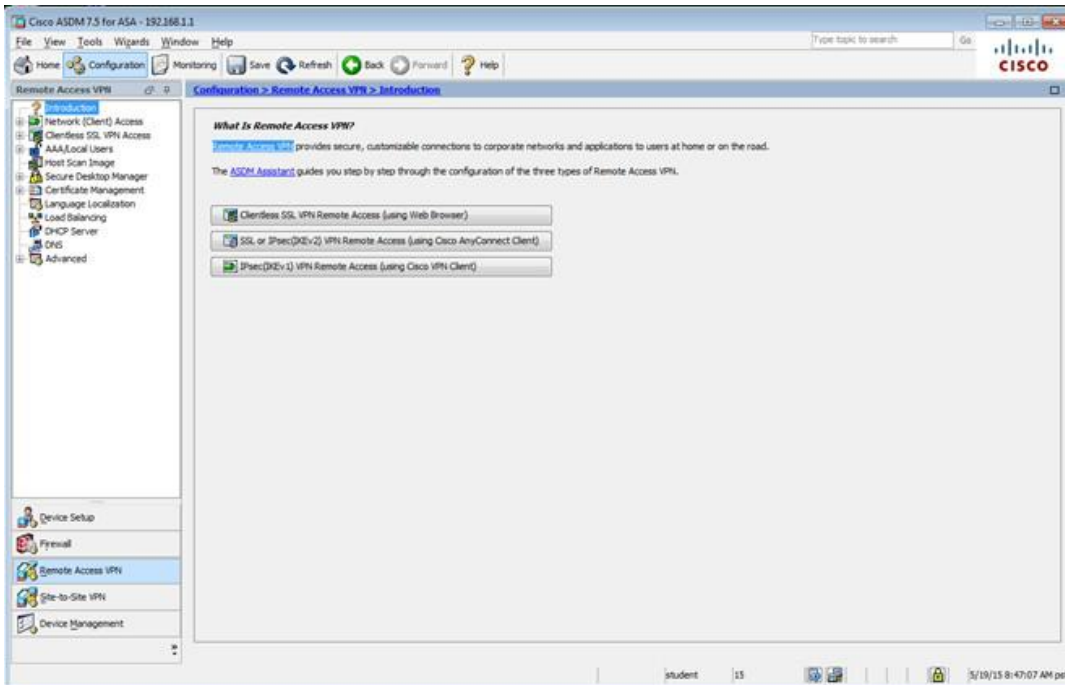
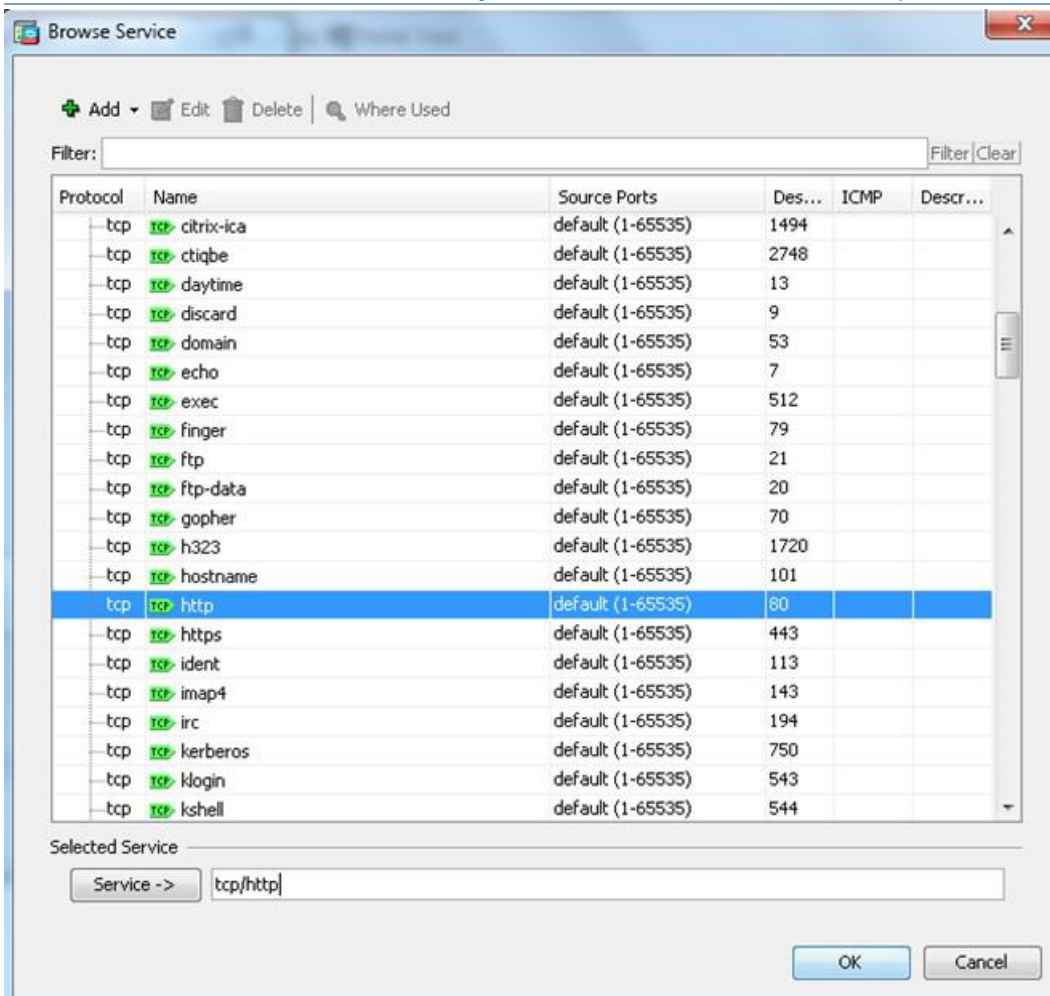
Description:

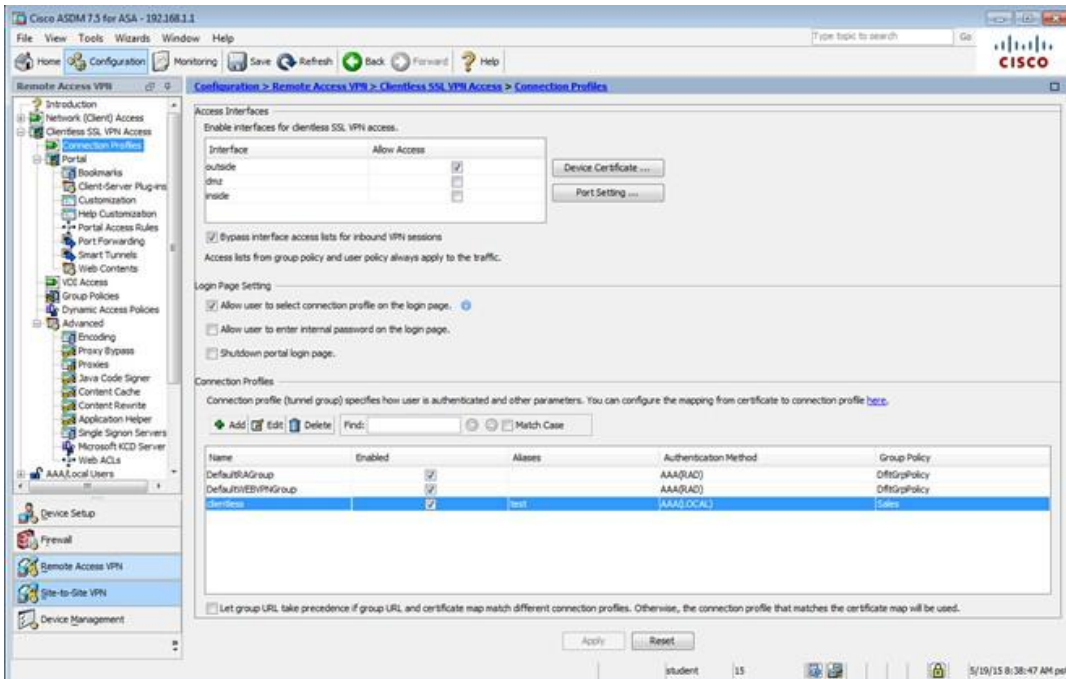
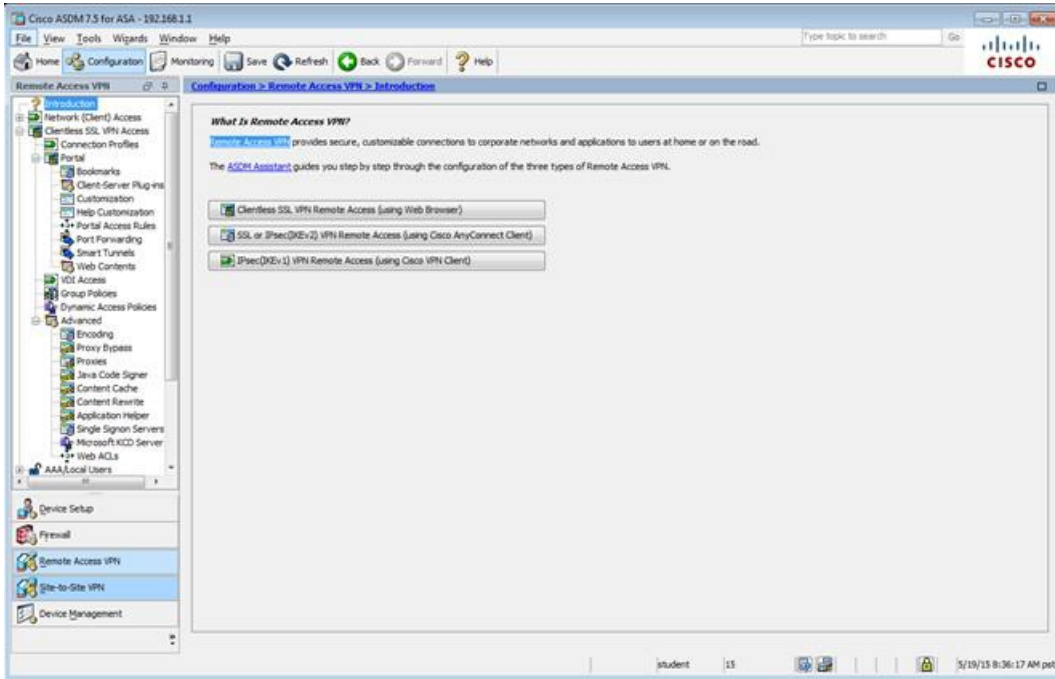
☒ Enable Logging

Logging Level: Default

More Options

OK Cancel Help





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

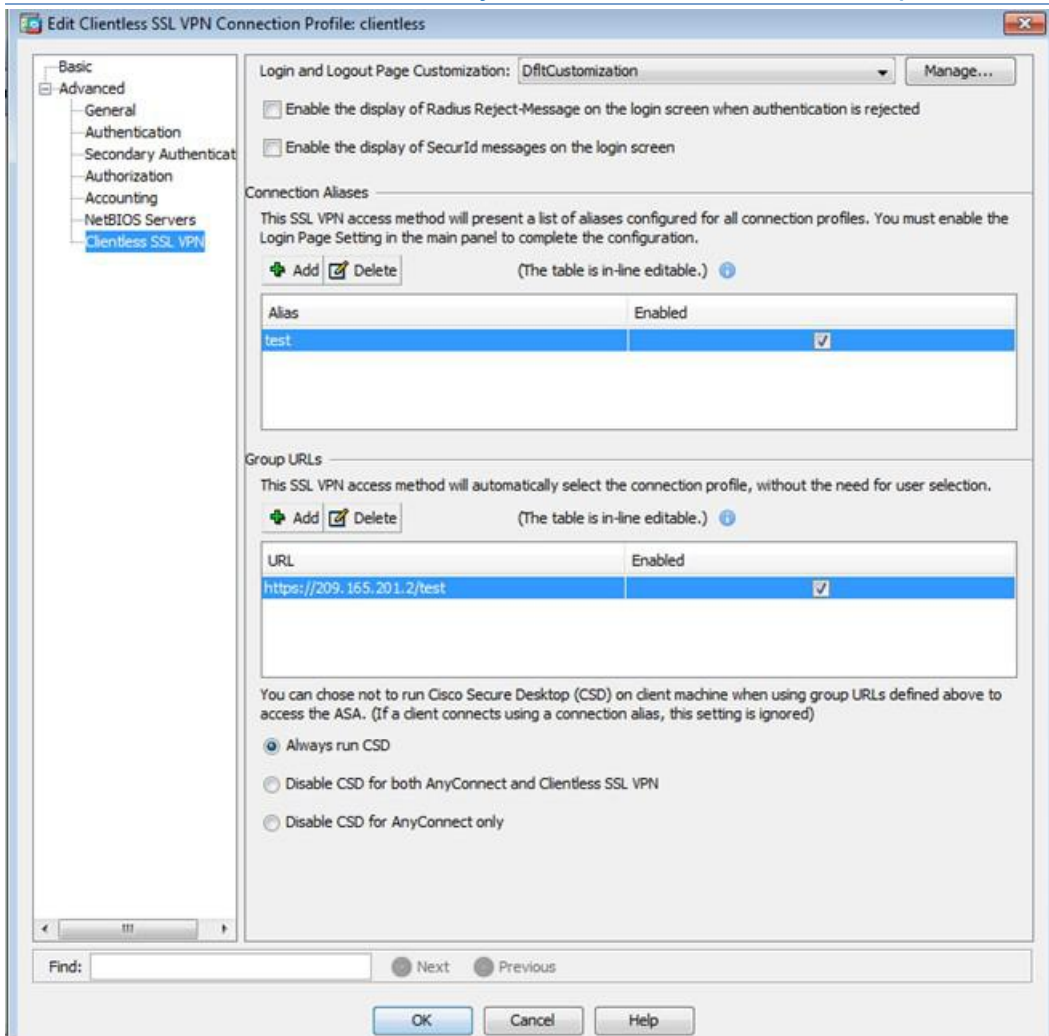
Group Policy: Sales Manage...

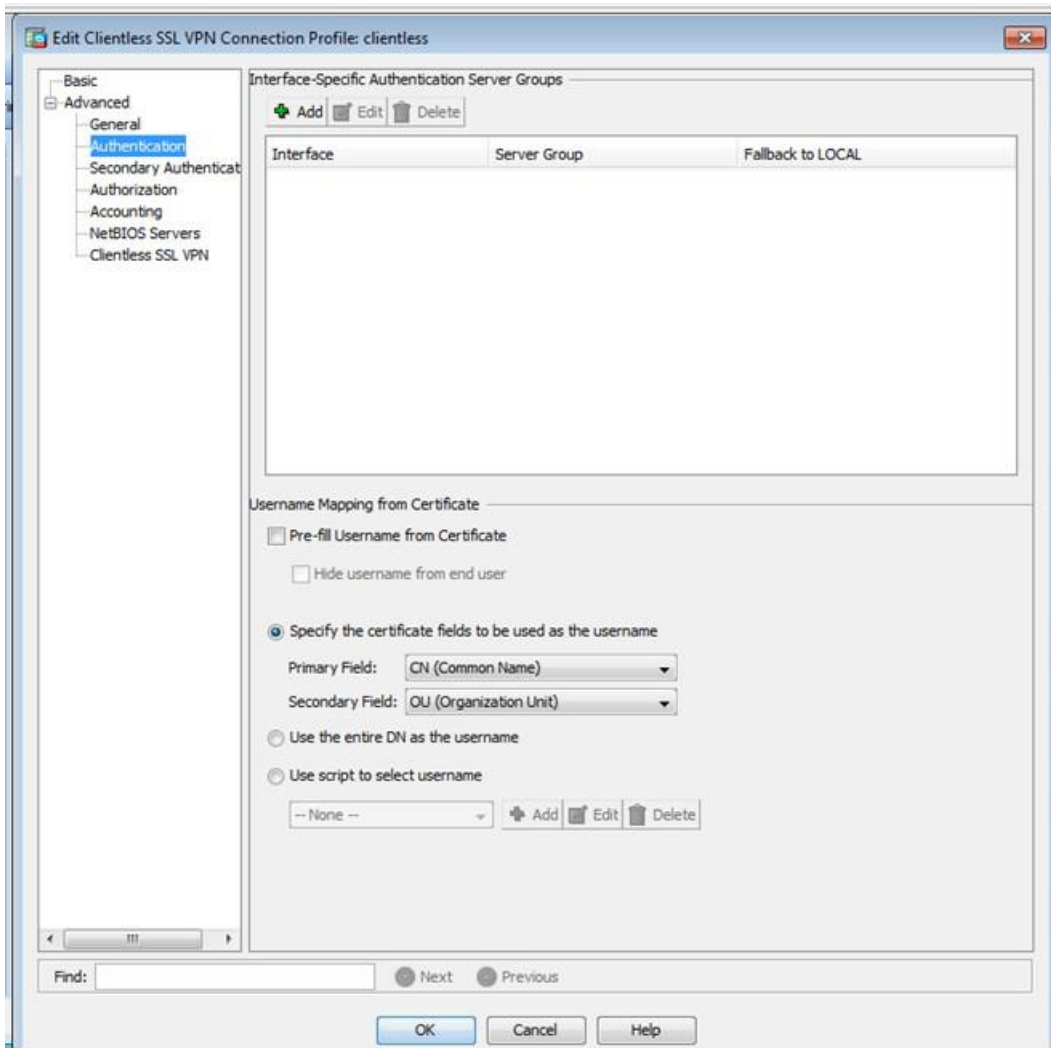
(Following field is an attribute of the group policy selected above.)

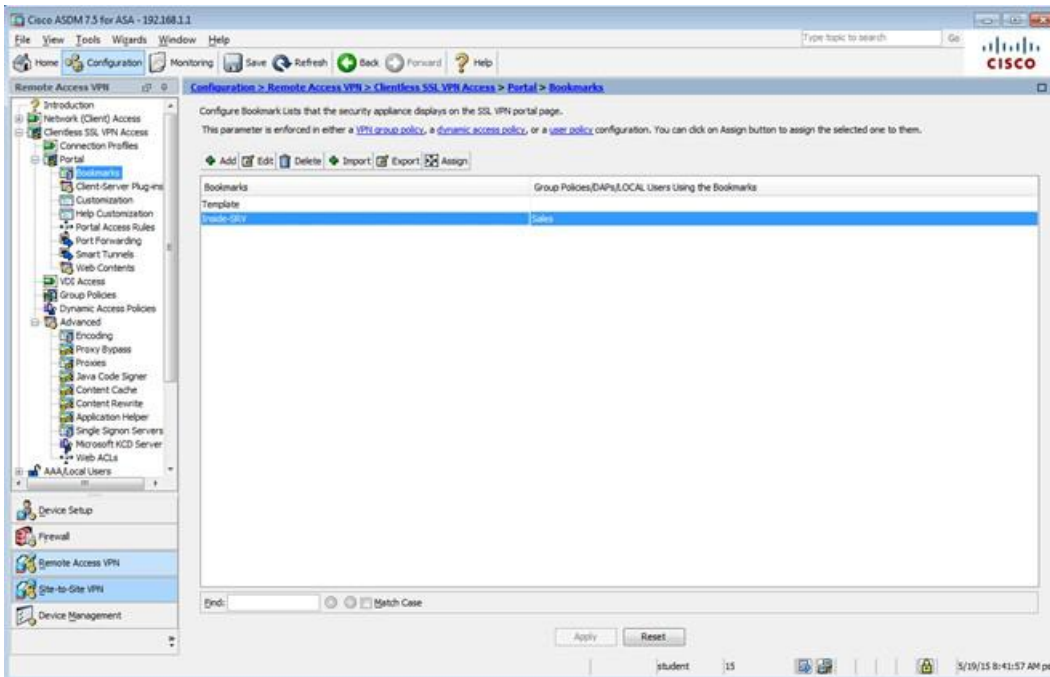
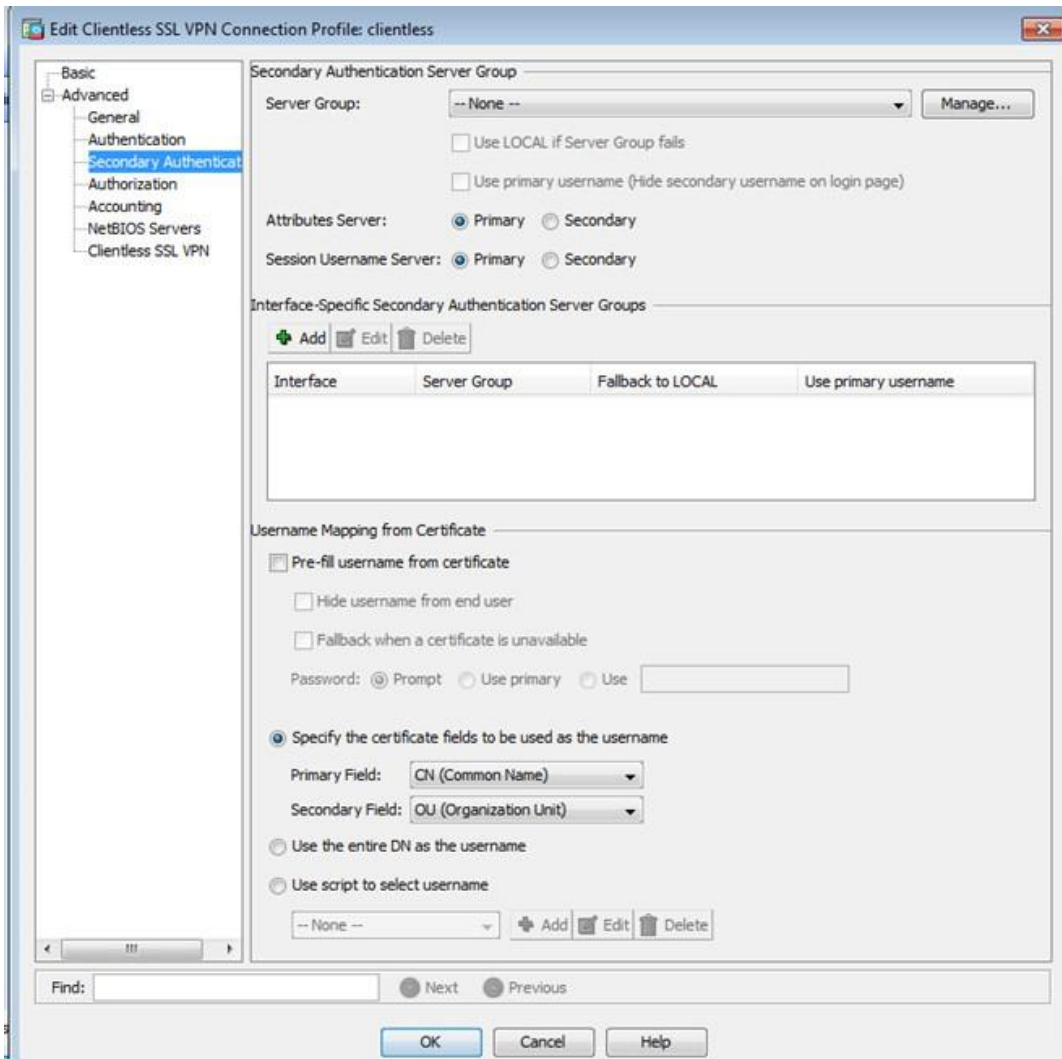
☒ Enable clientless SSL VPN protocol

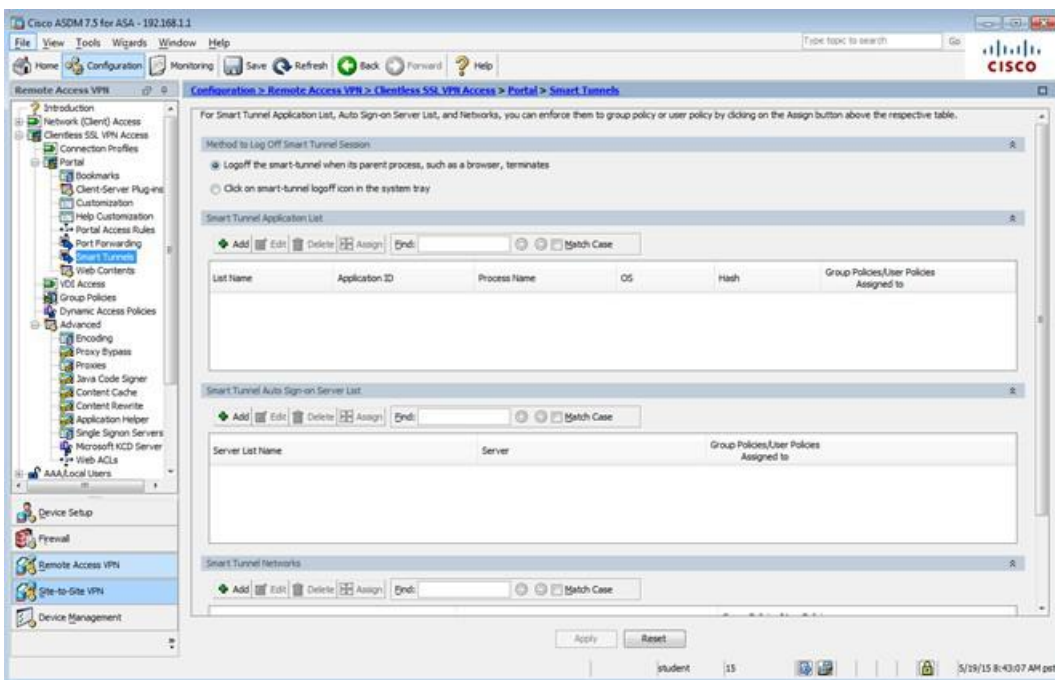
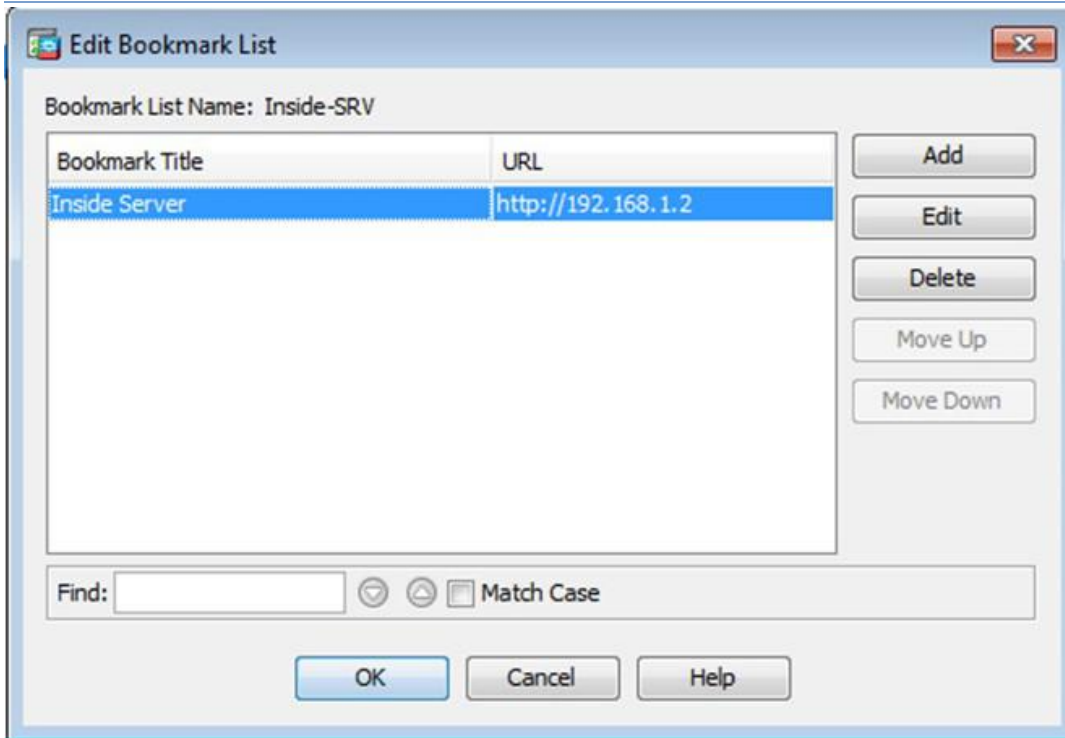
Find: Next Previous

OK Cancel Help









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 > Portal > Port Forwarding

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

Add Edit Delete Assign

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

Find: Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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](#).

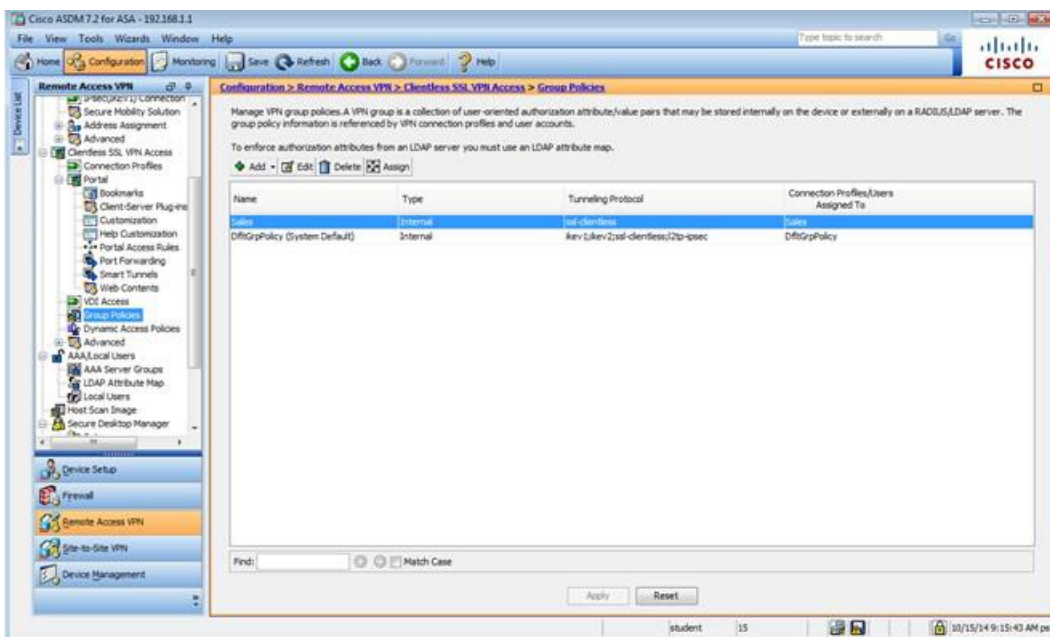
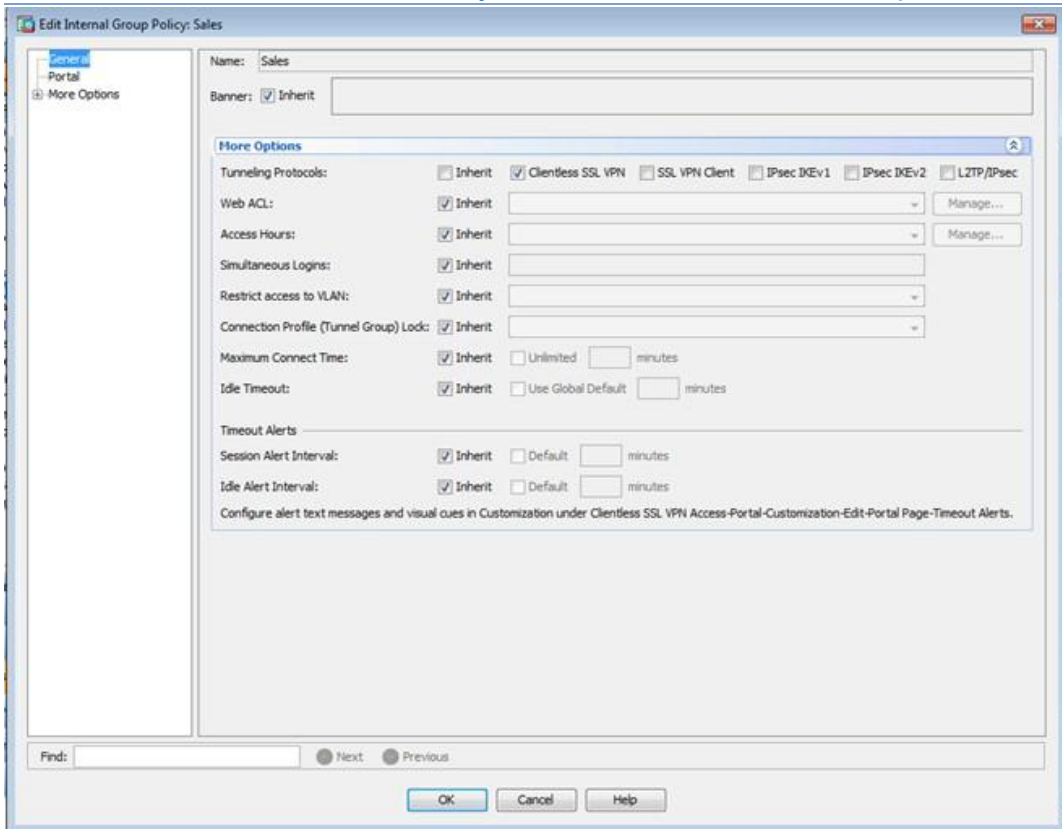
Add Edit Delete Assign

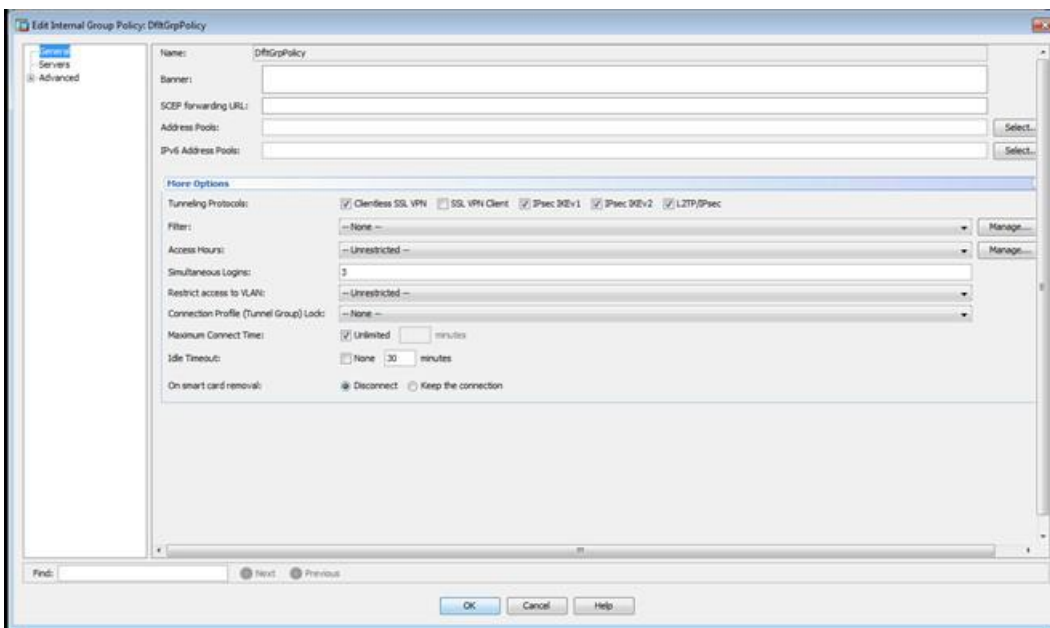
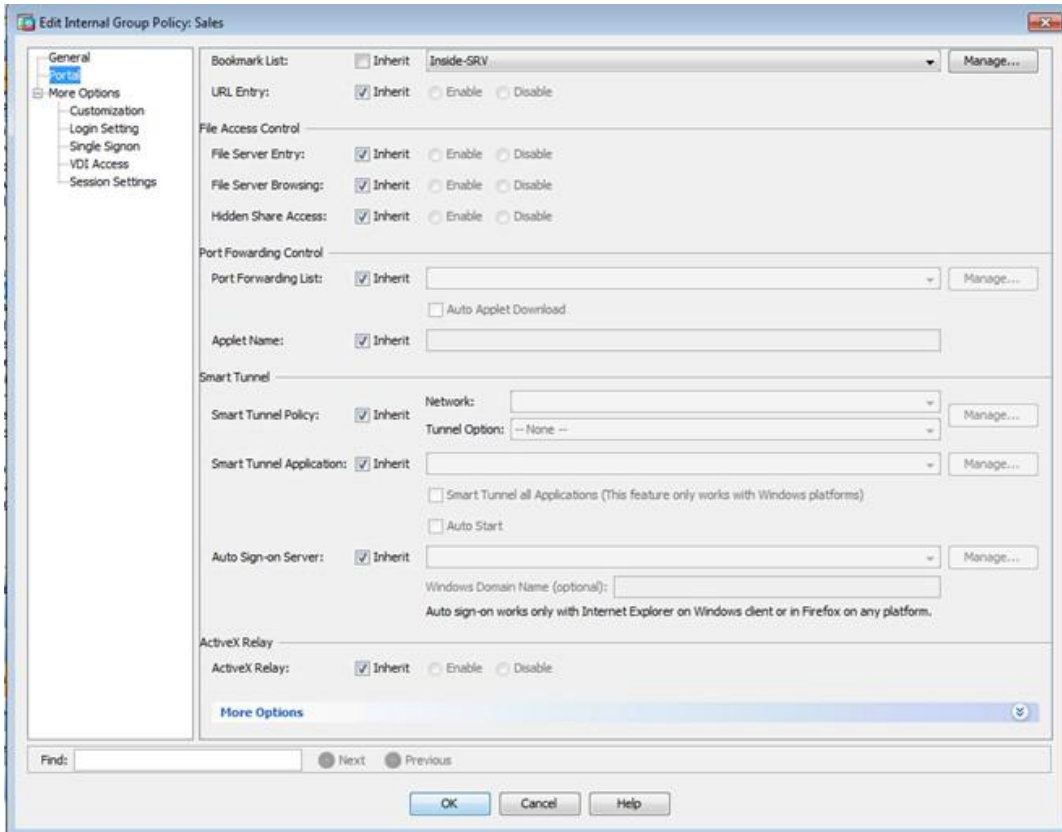
Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Default	Internal	all-clientless	Clientless
DefaultPolicy (System Default)	Internal	kev Liken/2ssl-clientless/2tp-espac	DefaultSAGroup/DefaultIL2Group/DefaultADP2Group/Def...

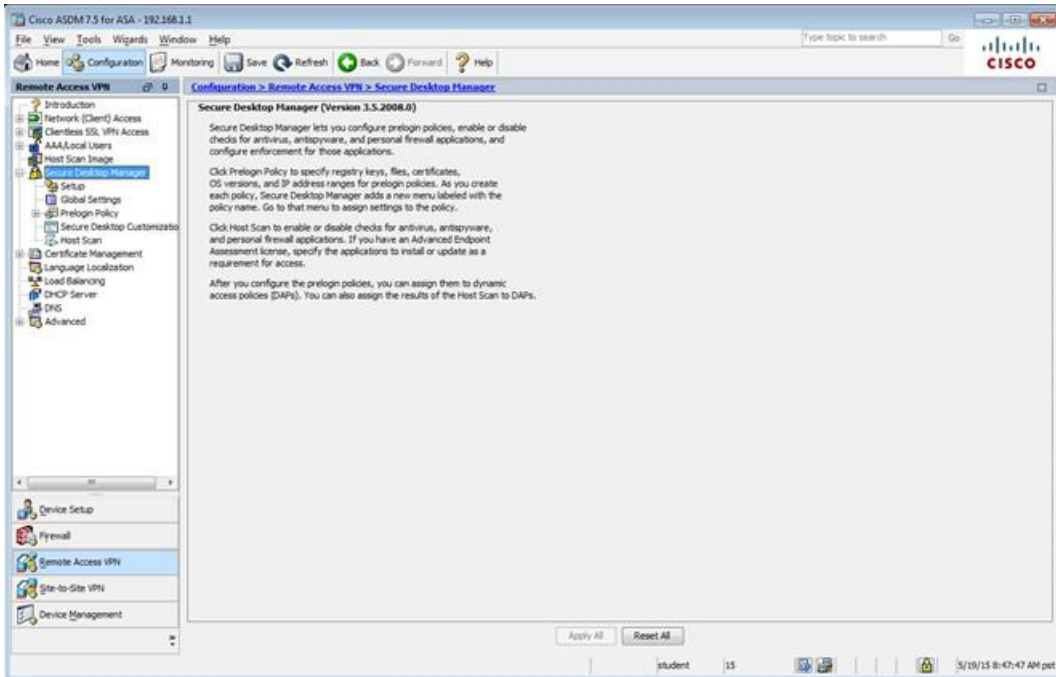
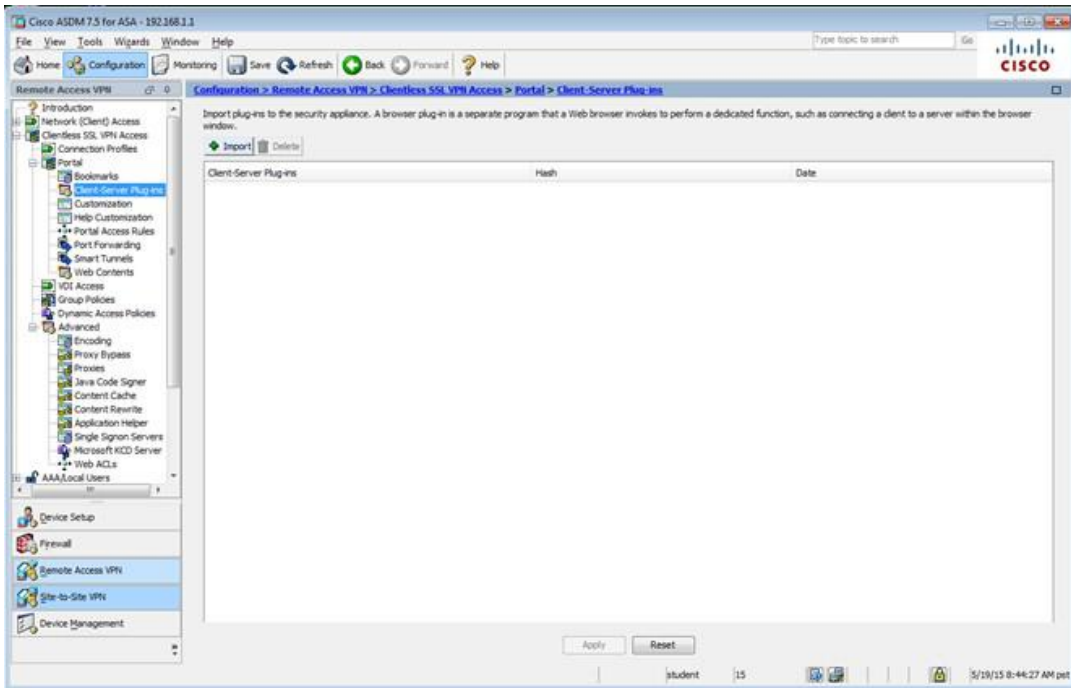
Find: Match Case

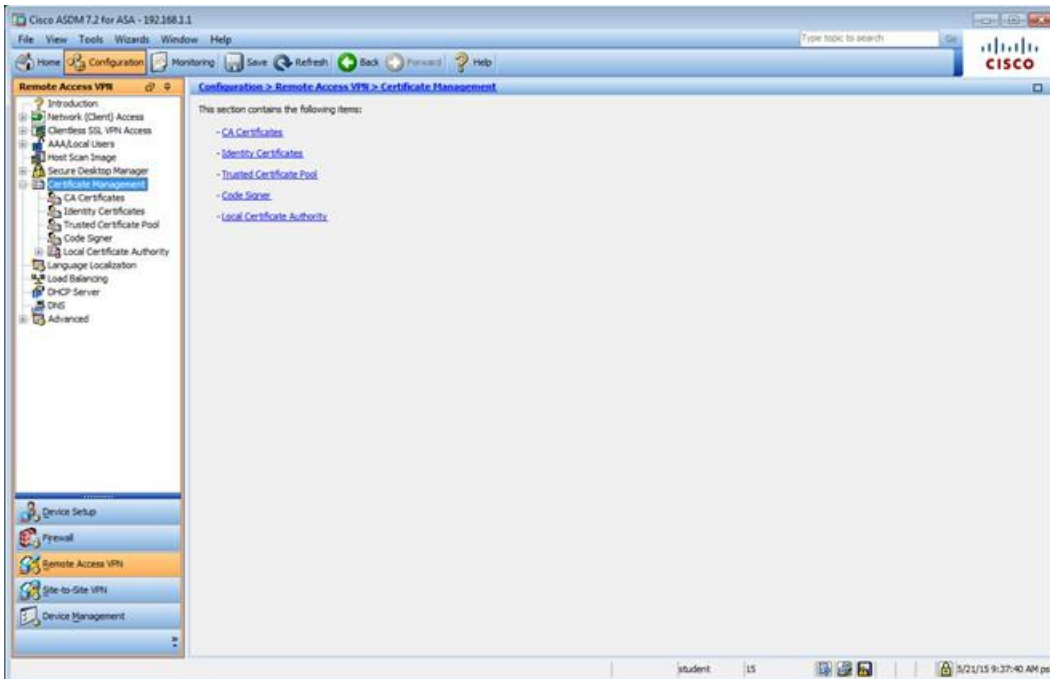
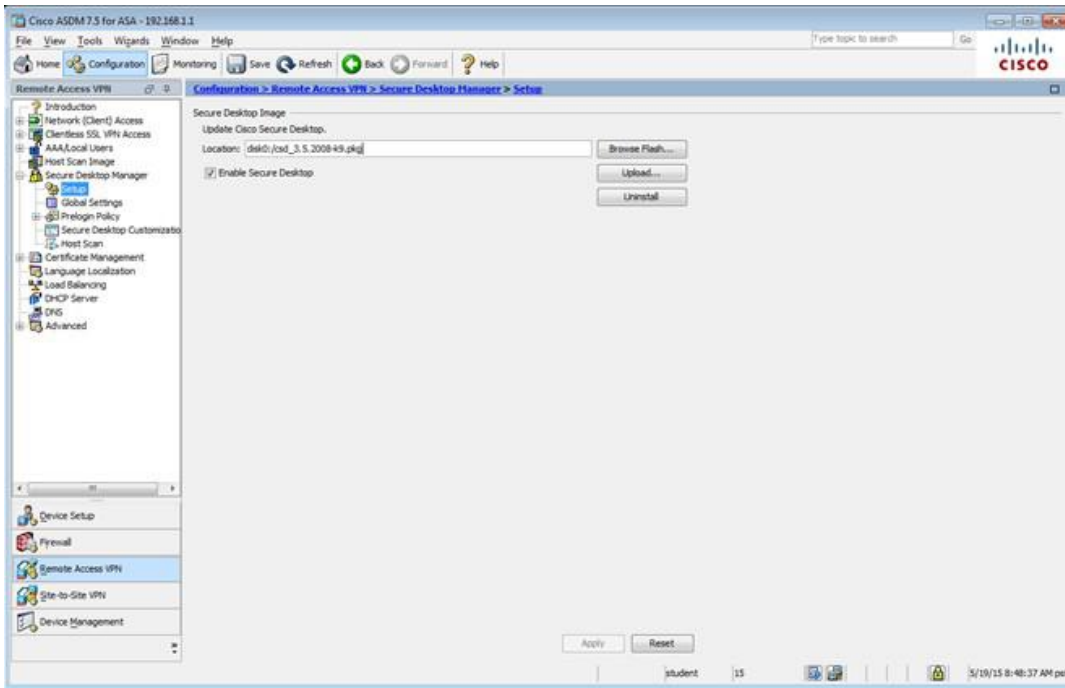
Apply Reset

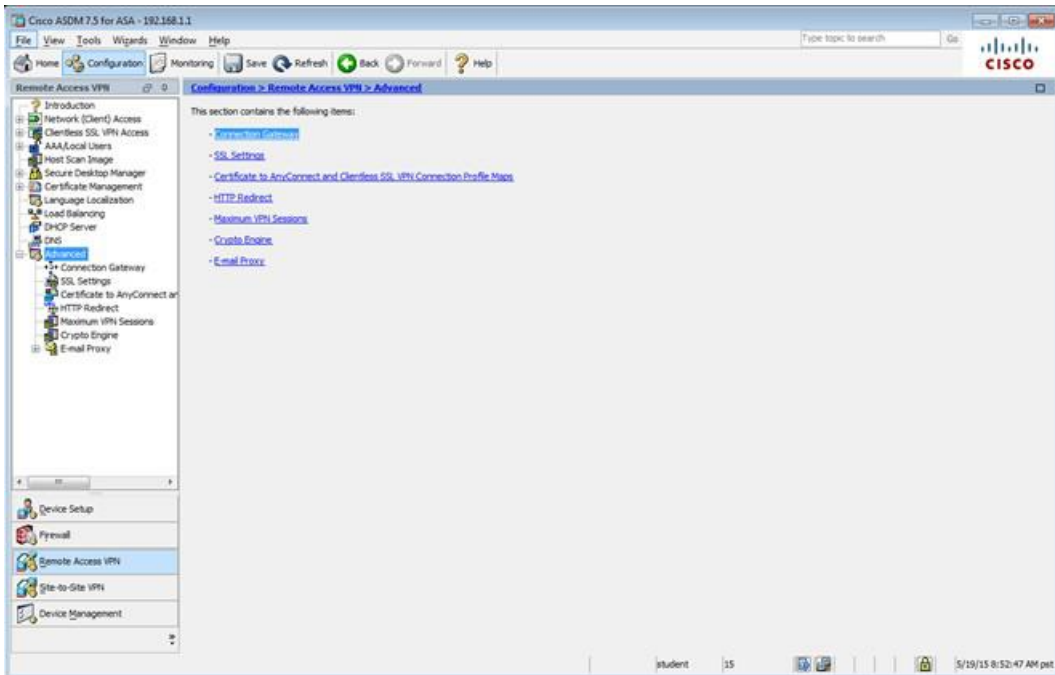
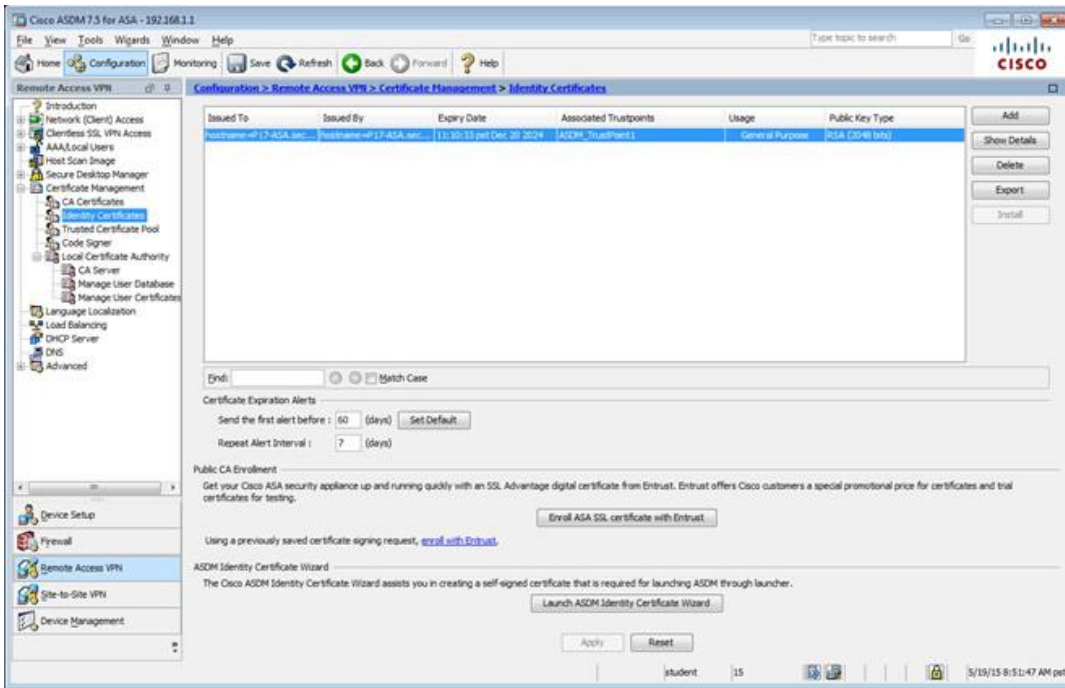
student 15 5/19/15 8:49:27 AM pst

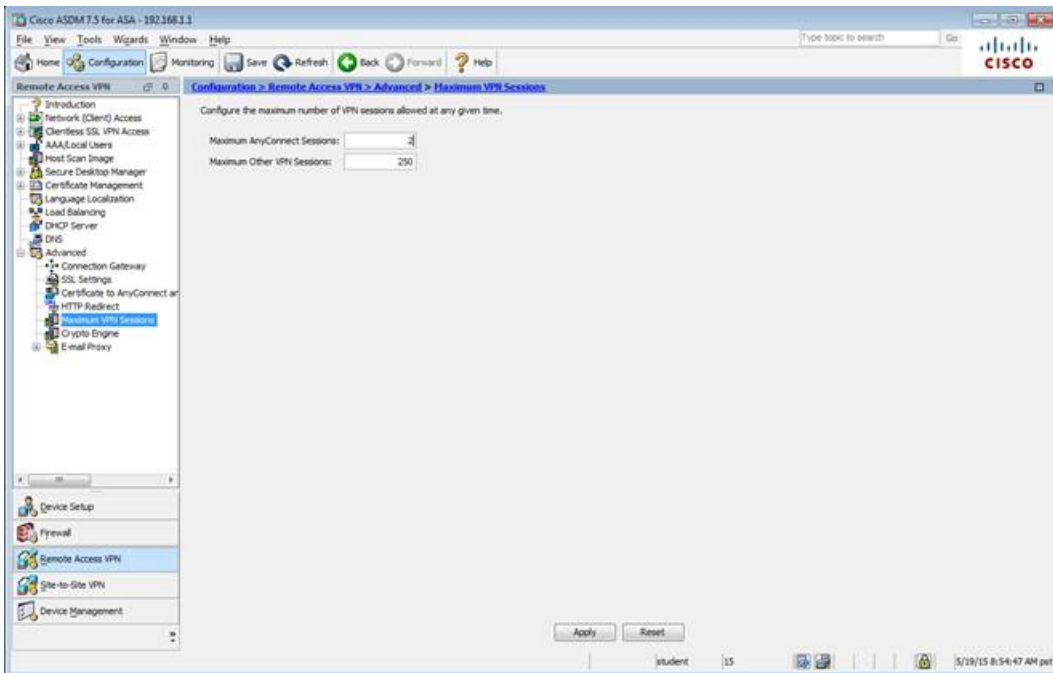
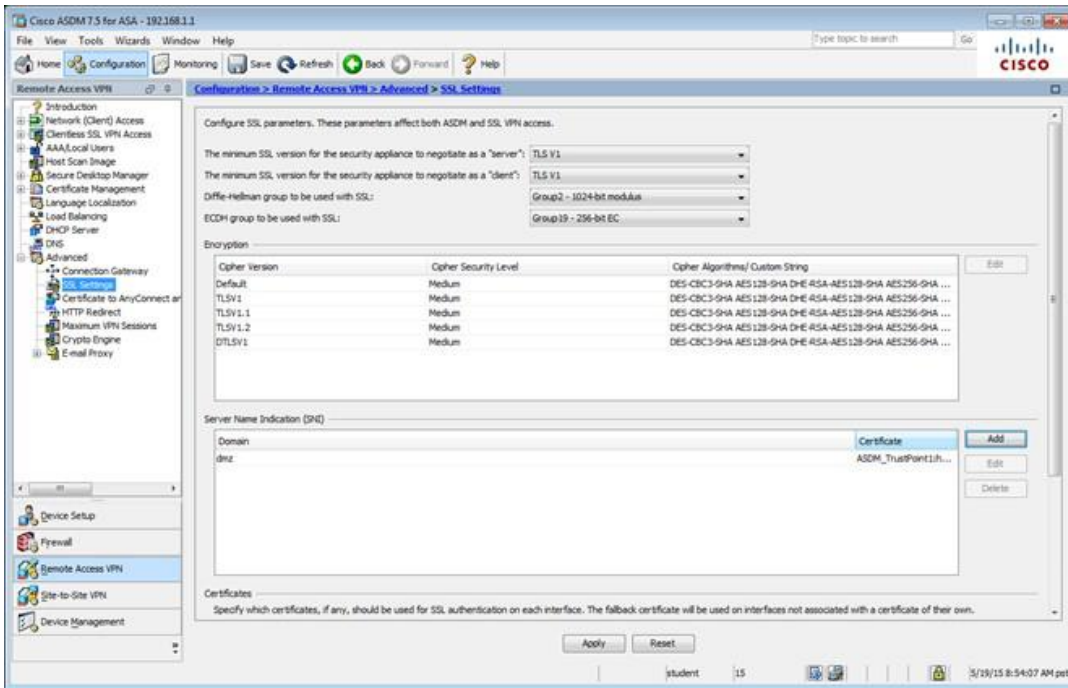


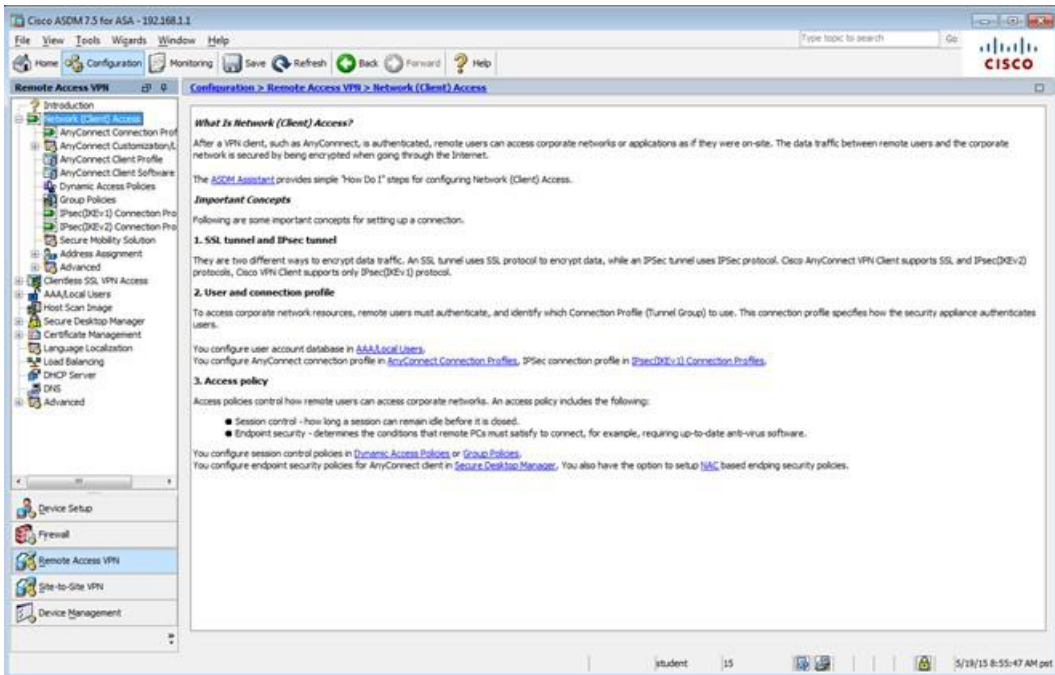
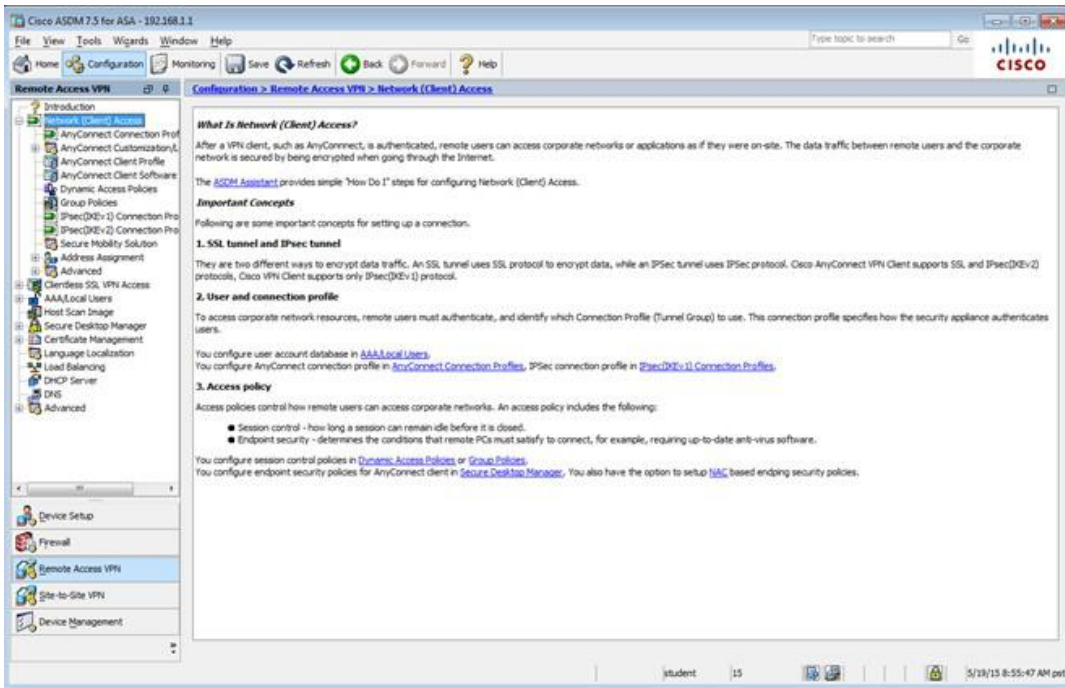


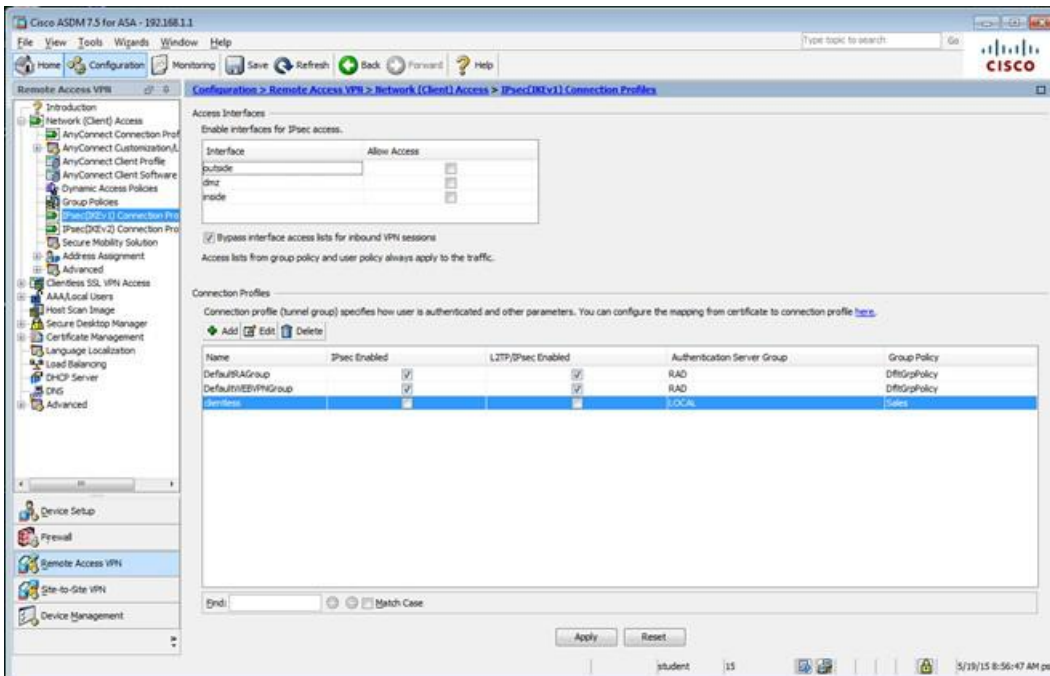
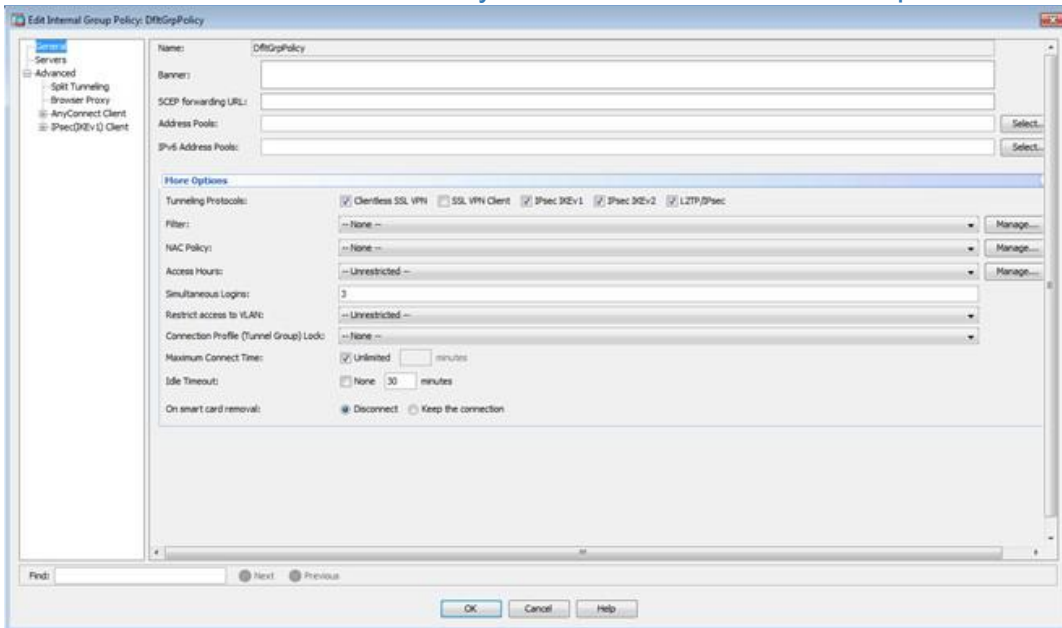












The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AnyConnect Connection Profiles' configuration page. It includes sections for 'Access Interfaces', 'Login Page Setting', and 'Connection Profiles'.

Access Interfaces:

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below. SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

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

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
DefaultIVVGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(RAD)	DfltGrpPolicy
Clientless	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	test	AAA(LOCAL)	Sales

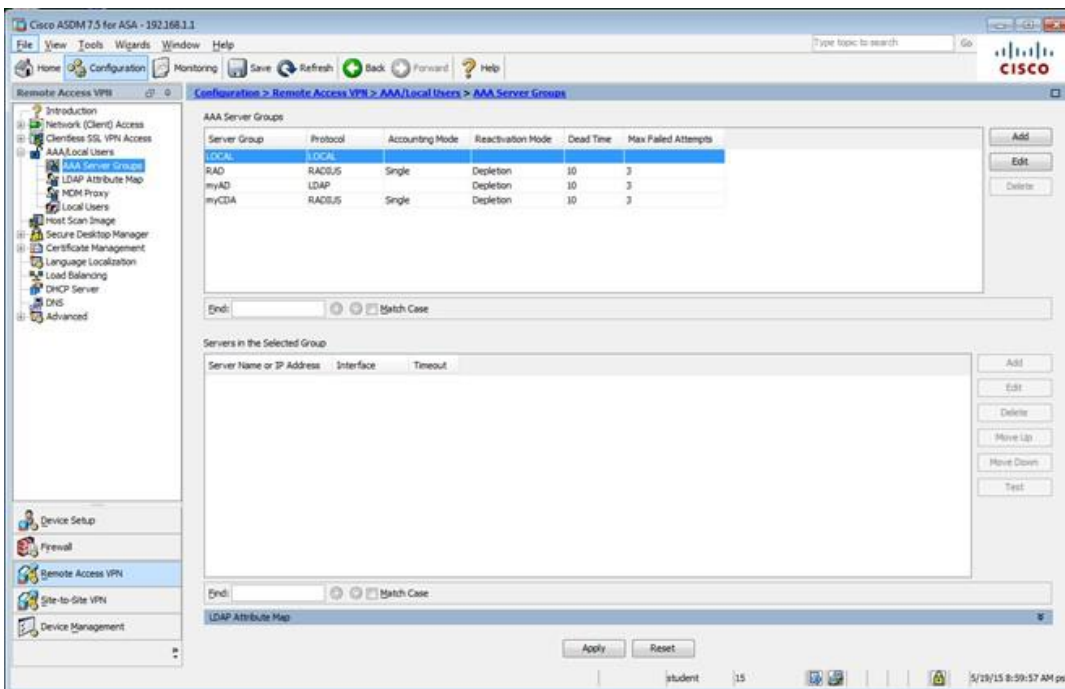
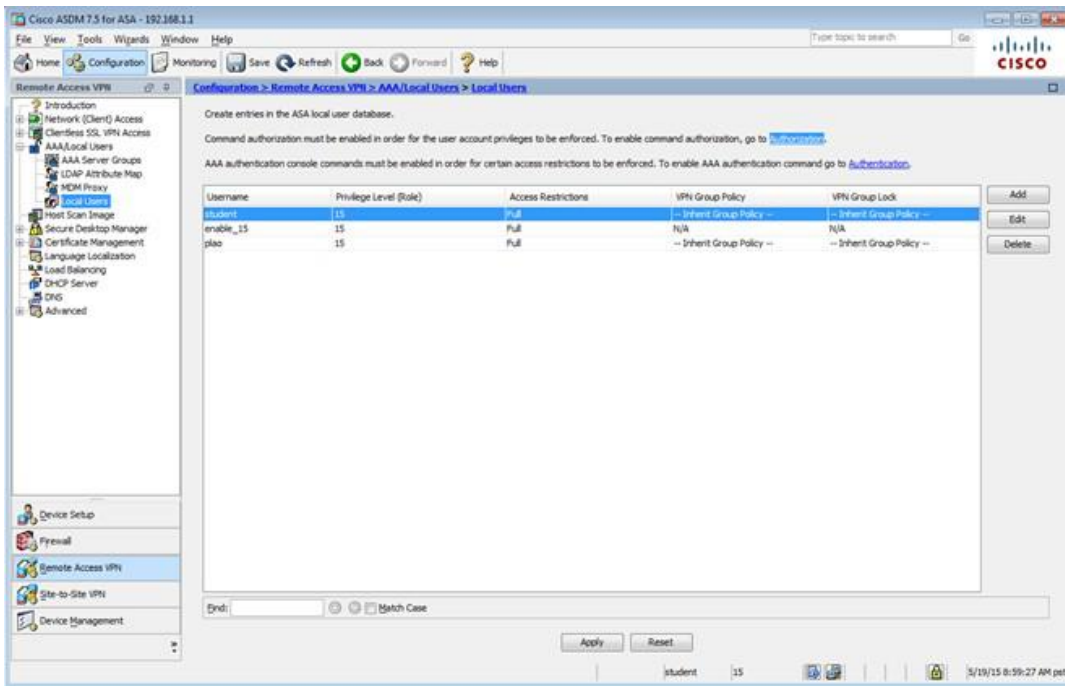
☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Buttons: Apply, Reset

The screenshot shows the Cisco ASDM 7.5 interface for configuring Remote Access VPN. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'AAA/Local Users' configuration page. It includes a section for 'This section contains the following items:' with links to 'AAA Server Groups', 'LDAP Attribute Map', 'MDM Proxy', and 'Local Users'.

This section contains the following items:

- [AAA Server Groups](#)
- [LDAP Attribute Map](#)
- [MDM Proxy](#)
- [Local Users](#)

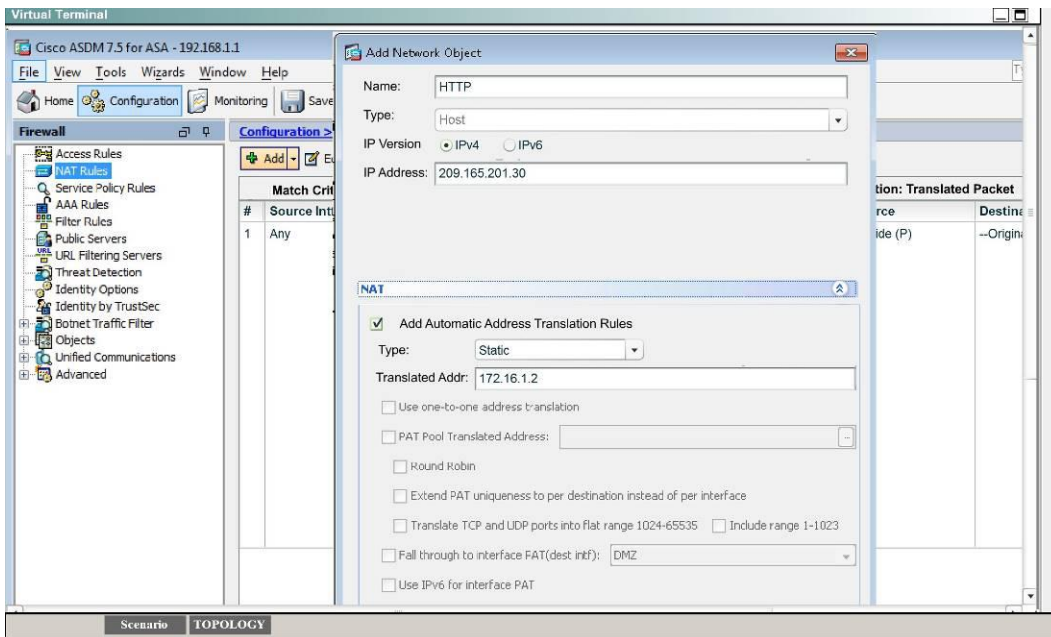


Answer:

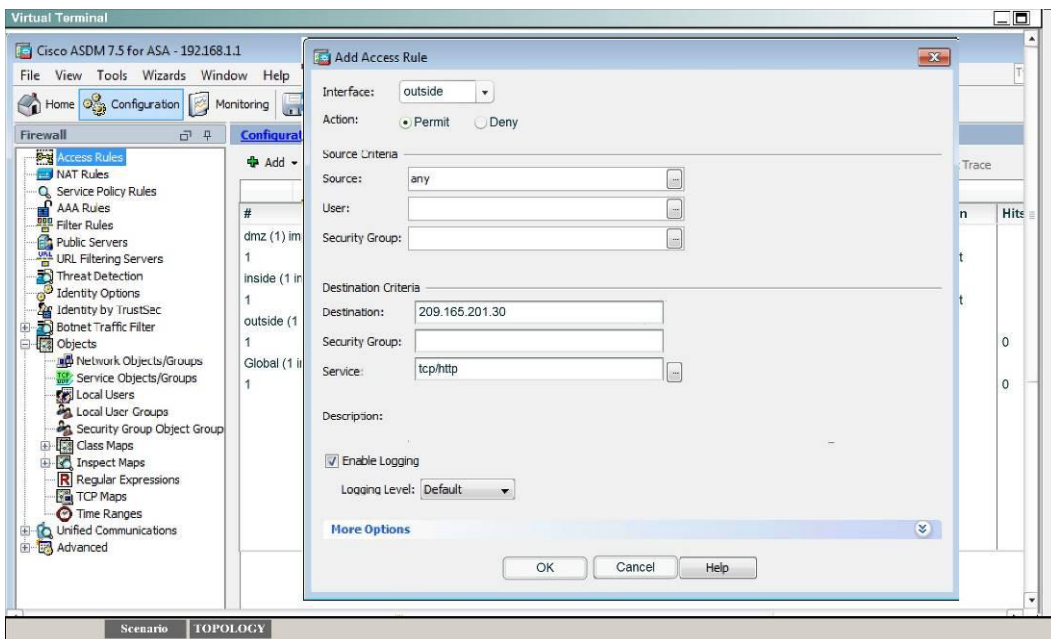
Follow the explanation part to get answer on this sim question.

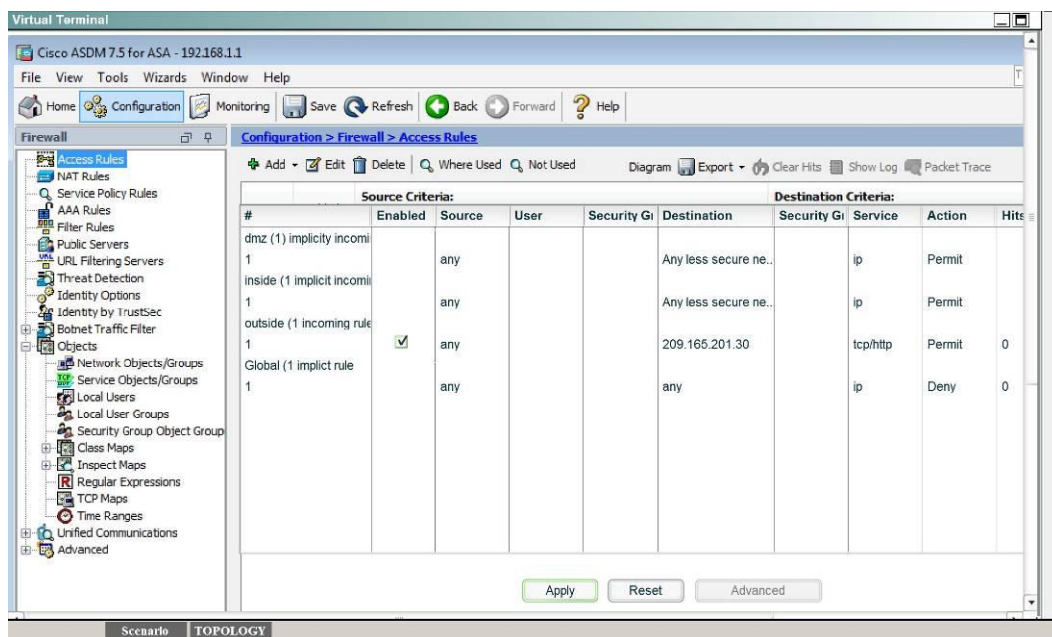
Explanation:

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



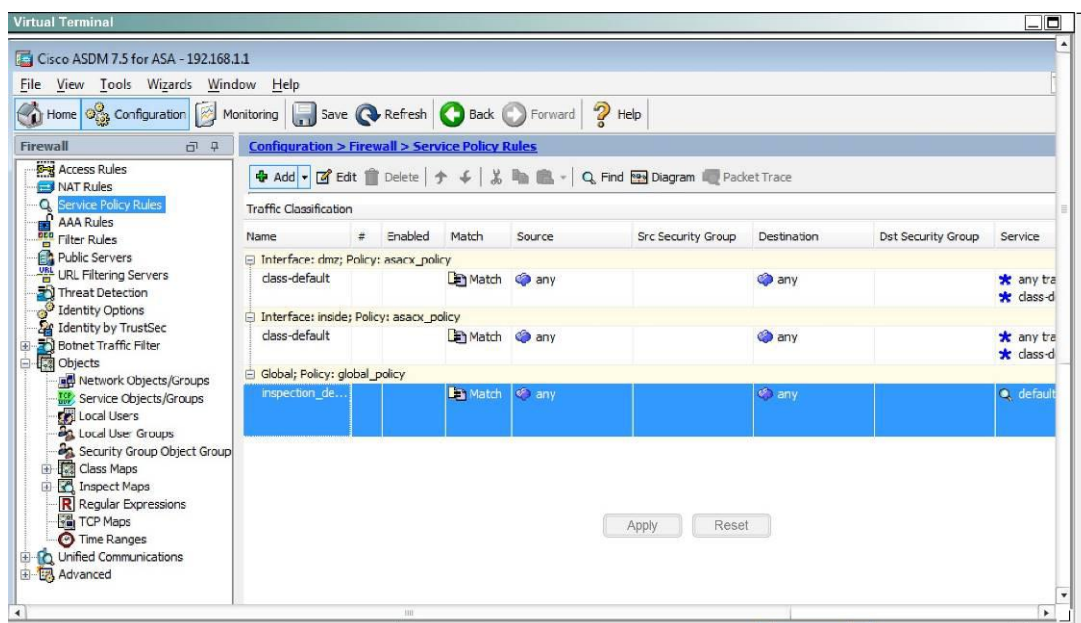
Then, create the firewall rules to allow the HTTP access:



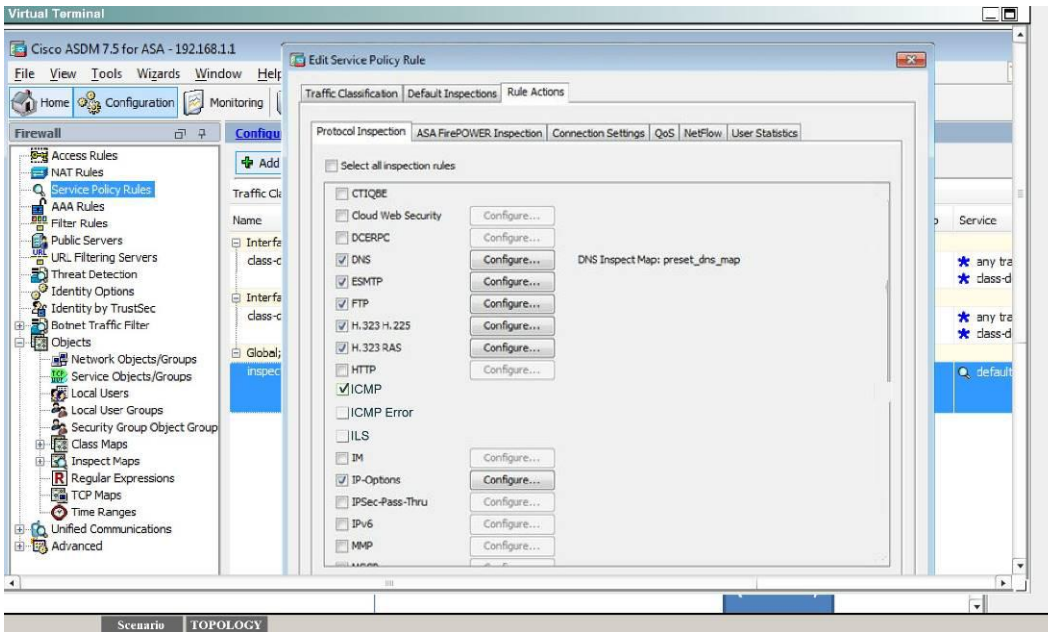


You can verify using the outside PC to HTTP into 209.165.201.30.

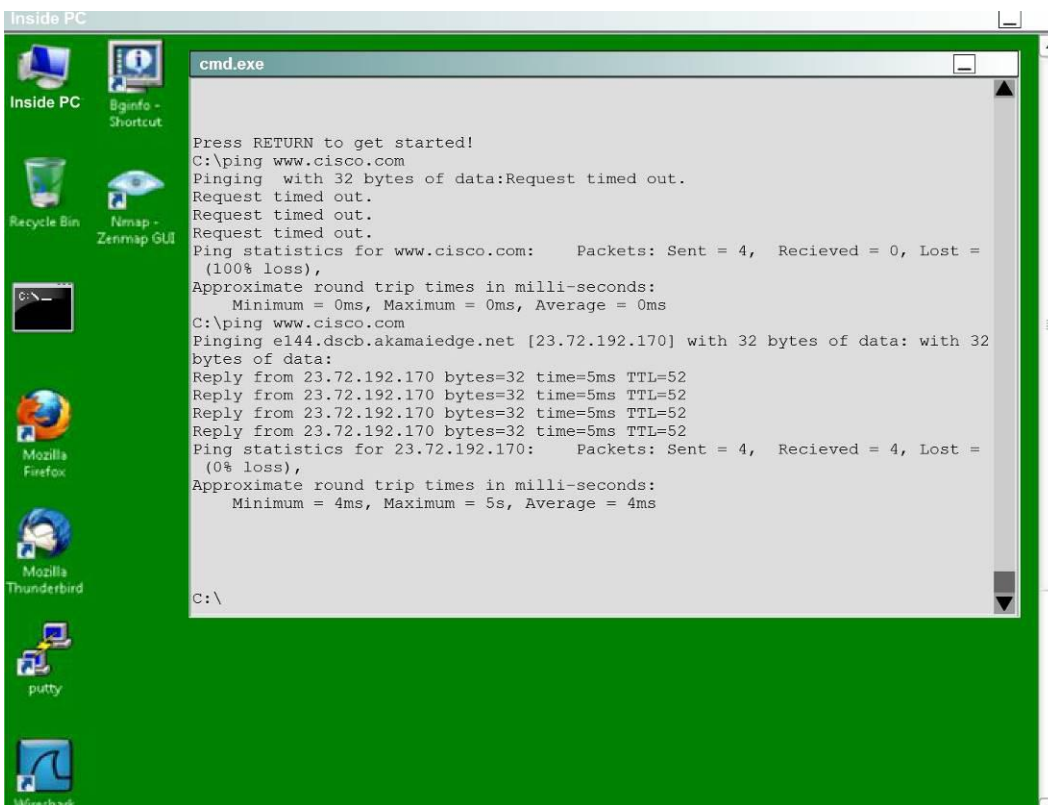
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



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



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



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

- A. aaa authentication enable console LOCAL SERVER_GROUP
- B. aaa authentication enable console SERVER_GROUP LOCAL



- C. aaa authentication enable console local
- D. aaa authentication enable console LOCAL

Answer: D

293. The stealing of confidential information of a company comes under the scope of

- A. Reconnaissance
- B. Spoofing attack
- C. Social Engineering
- D. Denial of Service

Answer: C

294. Which 2 NAT type allows only objects or groups to reference an IP address?

- A. dynamic NAT
- B. dynamic PAT
- C. static NAT
- D. identity NAT

Answer: A,C

Explanation: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_configuration/nat_objects.html#18425

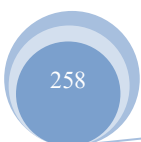
295. After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

- 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.

Answer: A

296. What is the Cisco preferred countermeasure to mitigate CAM overflows?

- A. Port security





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

Answer: B

297. Which type of address translation supports the initiation of communications bidirectionally?

- A. multi-session PAT
- B. static NAT
- C. dynamic PAT
- D. dynamic NAT

Answer: D

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

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

Answer: A,B

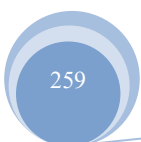
299. What type of attack was the Stuxnet virus?

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

Answer: A

300. How can you protect CDP from reconnaissance attacks?

- A. Enable dot1x on all ports that are connected to other switches.





- B. Disable CDP on ports connected to endpoints.
- C. Disbale CDP on trunk ports.
- D. Enable dynamic ARP inspection on all untrusted ports.

Answer: B

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

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

Answer: A

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

- A. file reputation
- B. file analysis
- C. signature updates
- D. network blocking

Answer: A

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

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

Answer: A

304. Security well known terms Choose 2

- A. Trojan
- B. Phishing



C. Something LC

D. Ransomware

Answer: B,D

305. Which two actions can a zone-based firewall take when looking at traffic? (Choose two)

A. Filter

B. Forward

C. Drop

D. Broadcast

E. Inspect

Answer: C,E

306. 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.

Answer: A,B,C

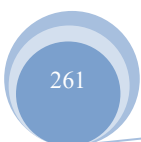
307. Which statement about extended access lists is true?

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

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

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

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





Answer: B

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

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

Answer: A

309. 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.

Answer: A

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

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

Answer: A