

## Exam Questions 210-260

Implementing Cisco Network Security

<https://www.2passeasy.com/dumps/210-260/>



#### NEW QUESTION 1

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

**Explanation:** Split tunneling is a computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections. This connection state is usually facilitated through the simultaneous use of, a Local Area Network (LAN) Network Interface Card (NIC), radio NIC, Wireless Local Area Network (WLAN) NIC, and VPN client software application without the benefit of access control.

Source: [https://en.wikipedia.org/wiki/Split\\_tunneling](https://en.wikipedia.org/wiki/Split_tunneling)

#### NEW QUESTION 2

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

**Explanation:** <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html>

#### NEW QUESTION 3

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

**Explanation:** Health and Performance Monitor (HPM) • Monitors and displays key health, performance and VPN data for ASA and IPS devices in your network. This information includes critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. You also can categorize devices for normal or priority monitoring, and set different alert rules for the priority devices.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/security\\_management/cisco\\_security\\_manager/security\\_manager/4-4/user/guide/CSMUserGuide\\_wrapper/HPMchap.pdf](http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/HPMchap.pdf)

#### NEW QUESTION 4

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

**Explanation:** #secure boot-image

This command enables or disables the securing of the running Cisco IOS image. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk.

Source:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s1.html#wp3328121947>

#### NEW QUESTION 5

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

**Explanation:** The no switchport command makes the interface Layer 3 capable.

Source:

<http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

#### NEW QUESTION 6

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

**Explanation:** Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic. So the only choice is A.

Source: <http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

#### NEW QUESTION 7

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

**Explanation:** To check the status of Simple Network Management Protocol (SNMP) communications, use the show snmp command in user EXEC or privileged EXEC mode.

Illegal operation for community name supplied: Number of packets requesting an operation not allowed for that community

Source:

<http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command>

#### NEW QUESTION 8

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

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

**Answer:** BDF

**Explanation:** + Block unwanted traffic at the router. If your corporate policy does not allow TFTP traffic, just implement ACLs that deny traffic that is not allowed.  
+ Reduce spoofing attacks. For example, you can filter (deny) packets trying to enter your network (from the outside) that claim to have a source IP address that is from your internal network.

+ Dynamic Host Configuration Protocol (DHCP) snooping to prevent a rogue DHCP server from handing out incorrect default gateway information and to protect a

DHCP server from a starvation attack Source: Cisco Official Certification Guide, Best Practices for Protecting the Data Plane , p.271

### NEW QUESTION 9

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

**Explanation:** For interfaces that are members of the same zone, all traffic is permitted by default. Source: Cisco Official Certification Guide, Zones and Why We Need Pairs of Them, p.380

### NEW QUESTION 10

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

**Explanation:** This command shows IPsec SAs built between peers - IPsec Phase2. The encrypted tunnel is build between 10.1.1.5 and 10.1.1.1 (the router from which we issued the command).

### NEW QUESTION 10

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

**Explanation:** Remember: The [.] at the beginning of the time tells us the NTP process has last contact with its servers. We know the time is authoritative because there would be a [\*] at the beginning if not.

### NEW QUESTION 12

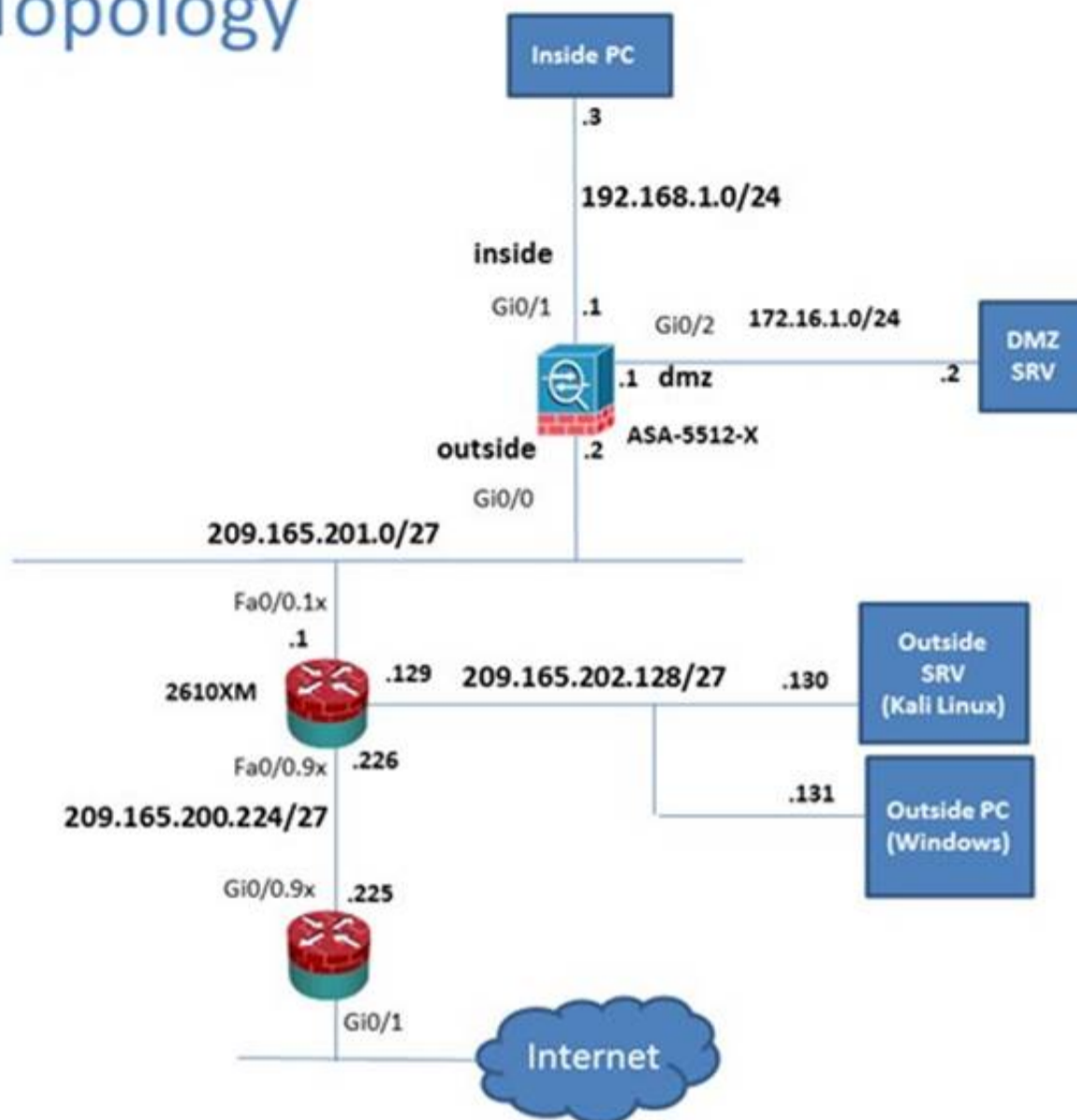
Scenario

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

To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

# Lab Topology



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA FirePOWER Status

Device Information

General License

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

ASA Version: 100.14(6)13

ASDM Version: 7.5(1)1

Firewall Model: Routed

Environment Status: OK

Device Uptime: 11d 21h 42m 47s

Device Type: ASA 5512

Context Mode: Single

Total Flash: 4096 MB

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

1500

1000

500

0

12:31 12:32 12:33 12:34 12:35

12:35:18

Traffic Status

Connections Per Second Usage

4

2

0

12:31 12:32 12:33 12:34 12:35

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

300

200

100

0

12:31 12:32 12:33 12:34 12:35

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

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.3014.3820	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.86e6.98f3	No
dmz	172.16.1.2	0050.5644.4444	No
ngint	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 pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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	sales clientless	Clientless Clientless (IPsec4)	08:05:46 pet Thu May 21 2015 0h:09m:19s	316774 41633

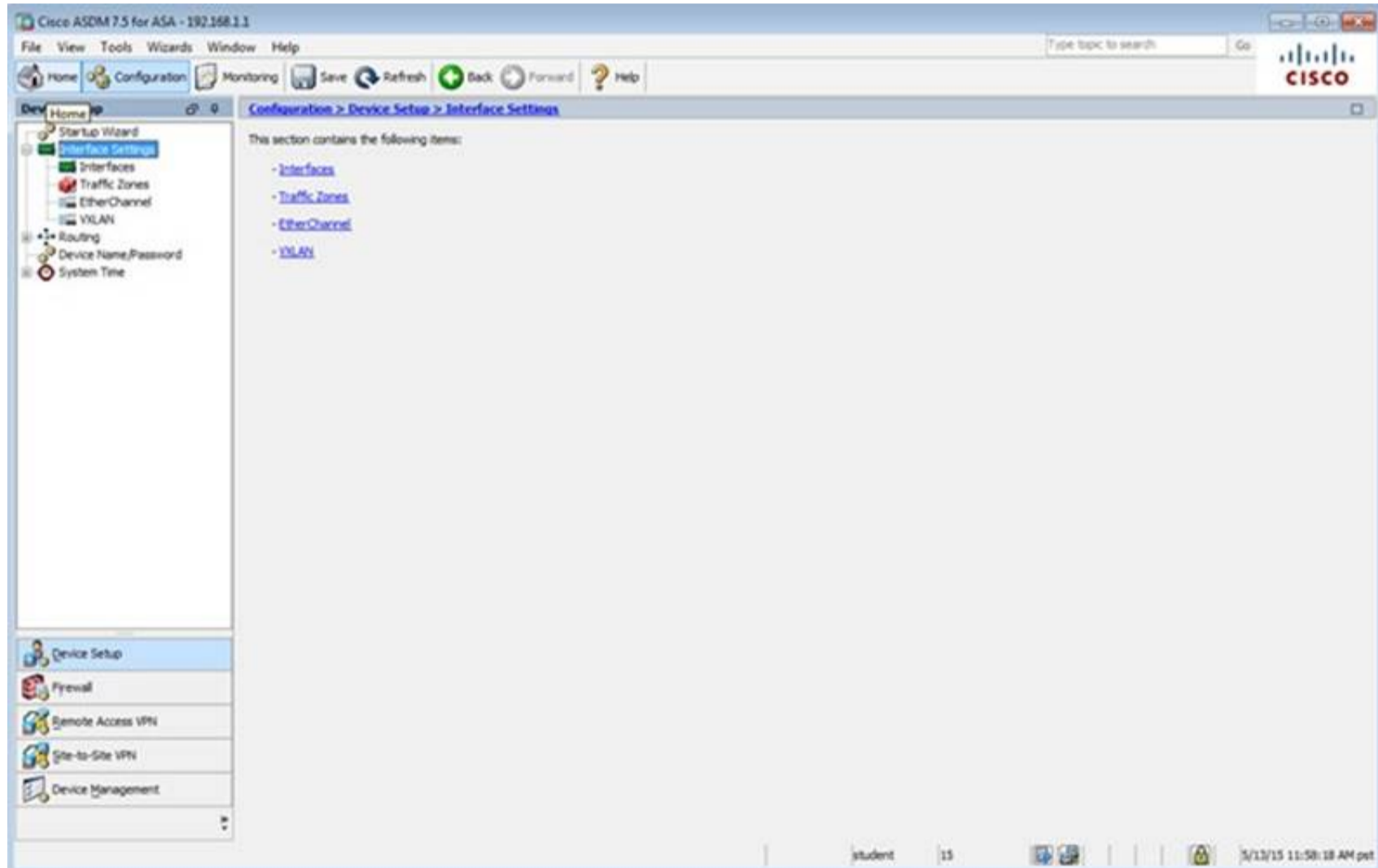
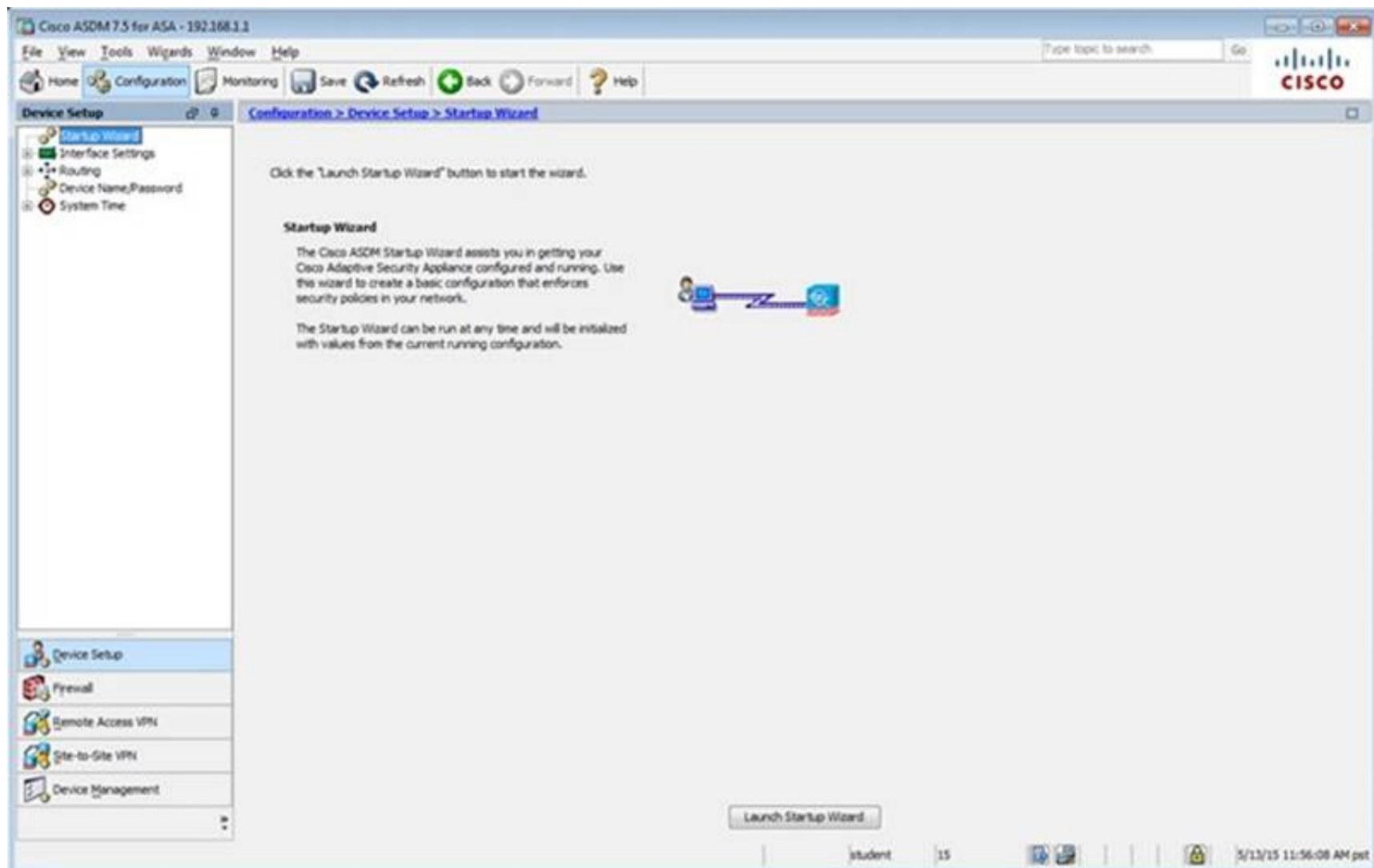
Details Logout Ping

Refresh

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

Data Refreshed Successfully.

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Configuration > Device Setup > Interface Settings > Interfaces

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask	Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled		0.0.0.0	255.255.255.0			Hardware
GigabitEthernet0/1	inside			Enabled		100 192.168.1.1	255.255.255.0			Hardware
GigabitEthernet0/2	dmz			Enabled		172.16.1.1	255.255.255.0			Hardware
GigabitEthernet0/3				Enabled						Hardware
GigabitEthernet0/4				Enabled						Hardware
GigabitEthernet0/5	mgmt			Enabled		100 10.10.10.2	255.255.255.0			Hardware
Management0/0				Enabled						Hardware

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

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Management Access

This section contains the following items:

- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Quota
- SNMP
- Management Access Rules

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

student 15 5/13/15 11:59:28 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

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

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

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

DH Key Exchange: ☒ Group 1 ☐ Group 14

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Management Access > Management Interface

Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.

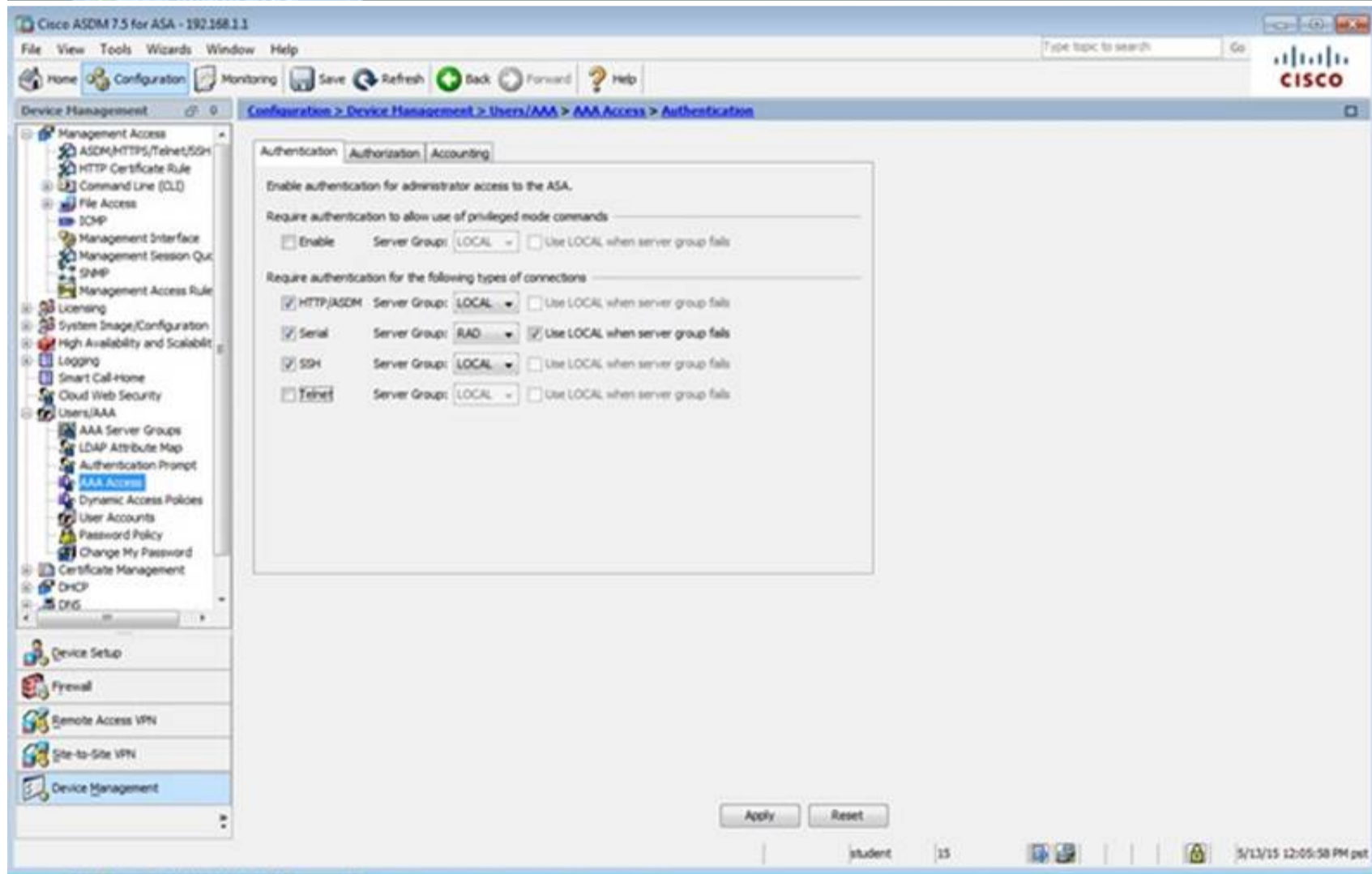
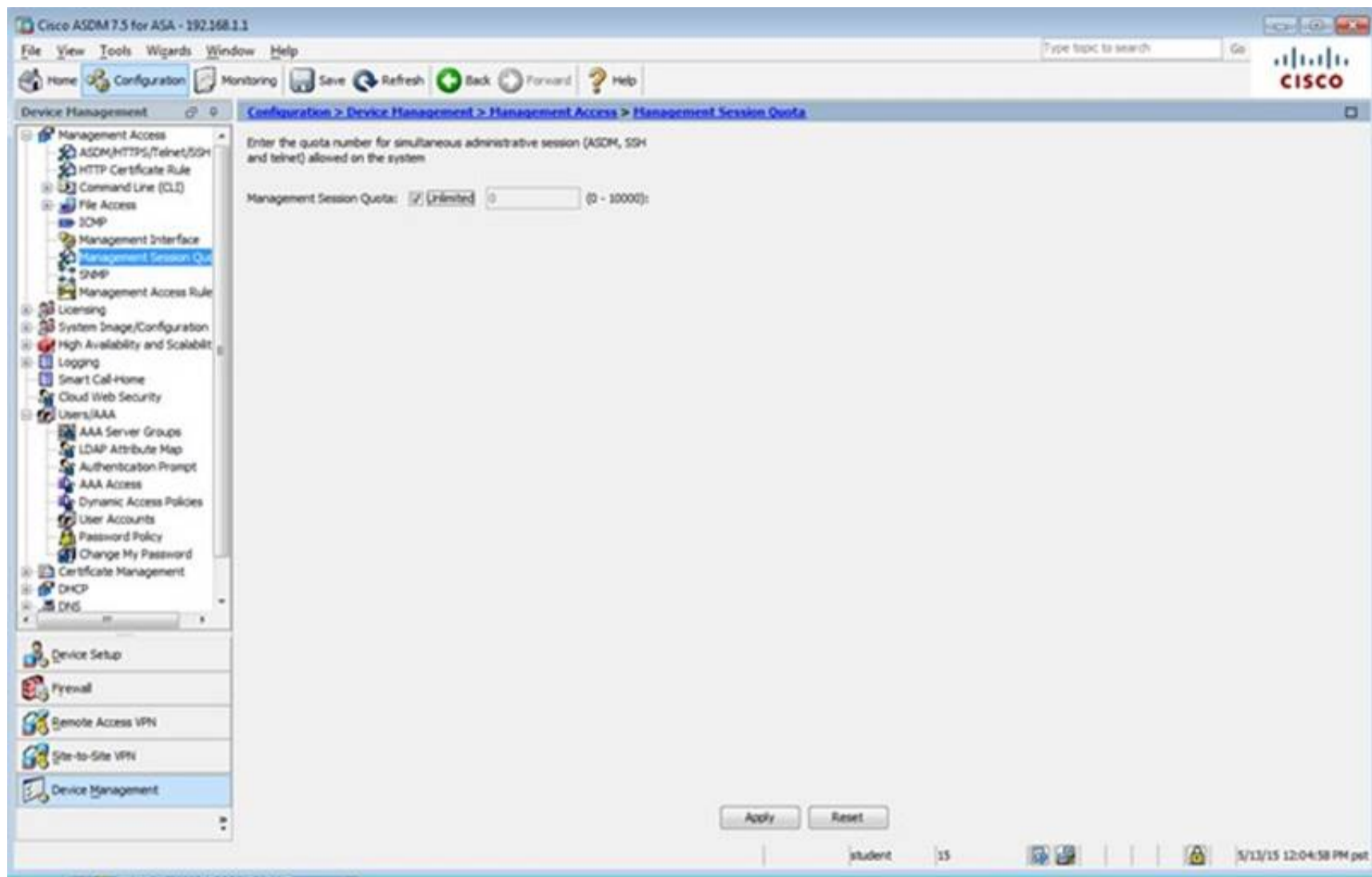
Management Access Interface: --None--

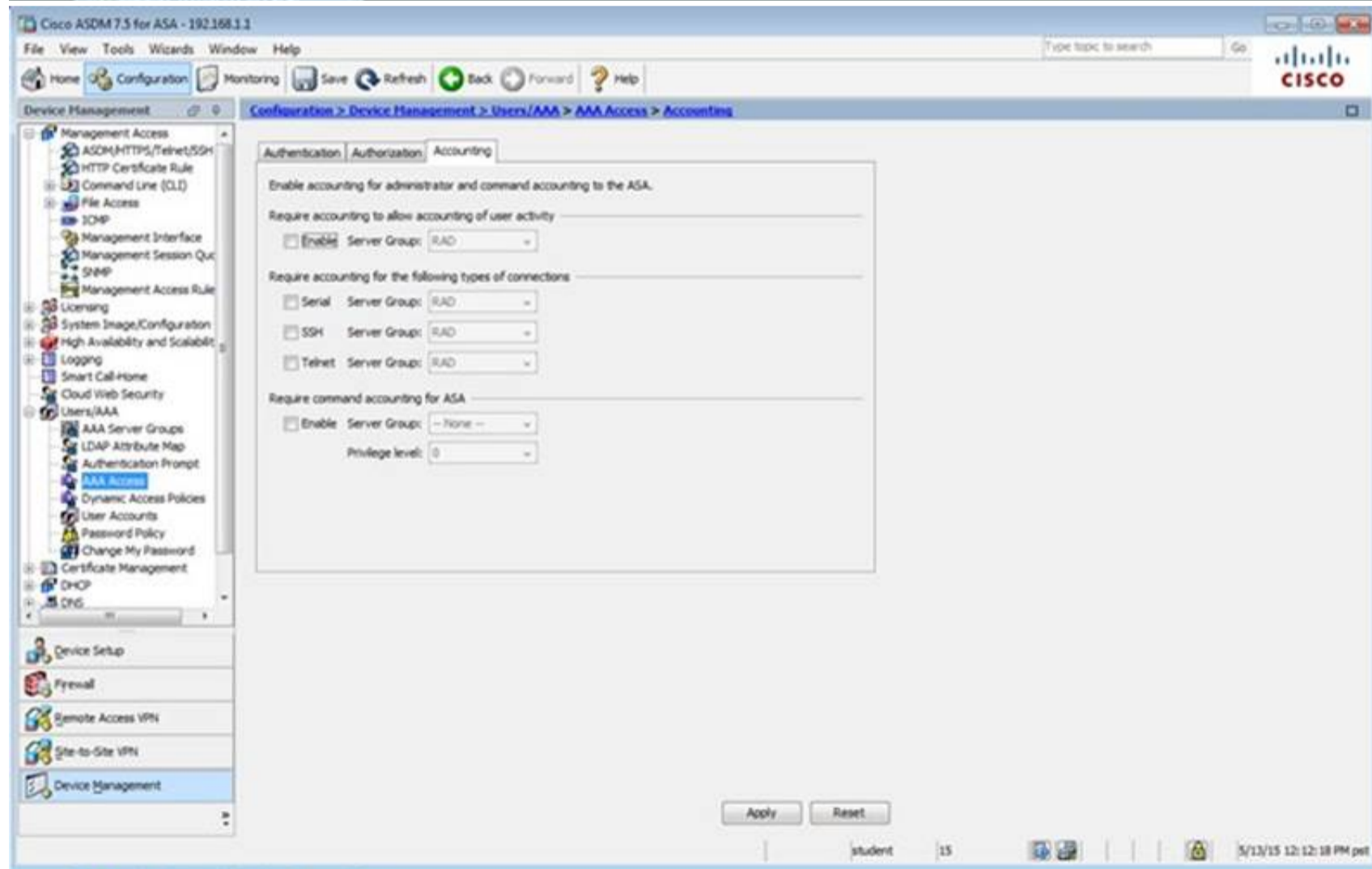
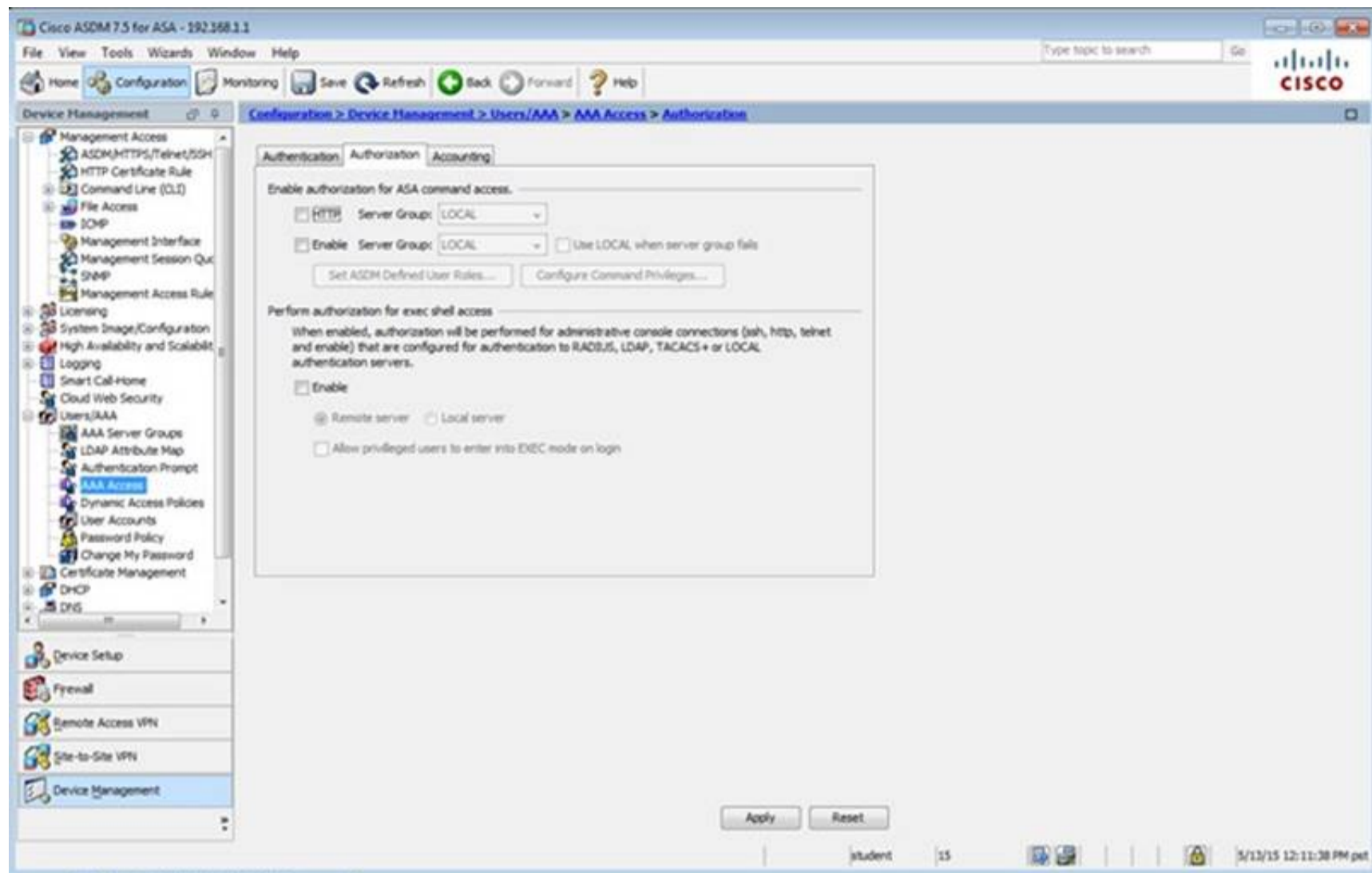
Apply Reset

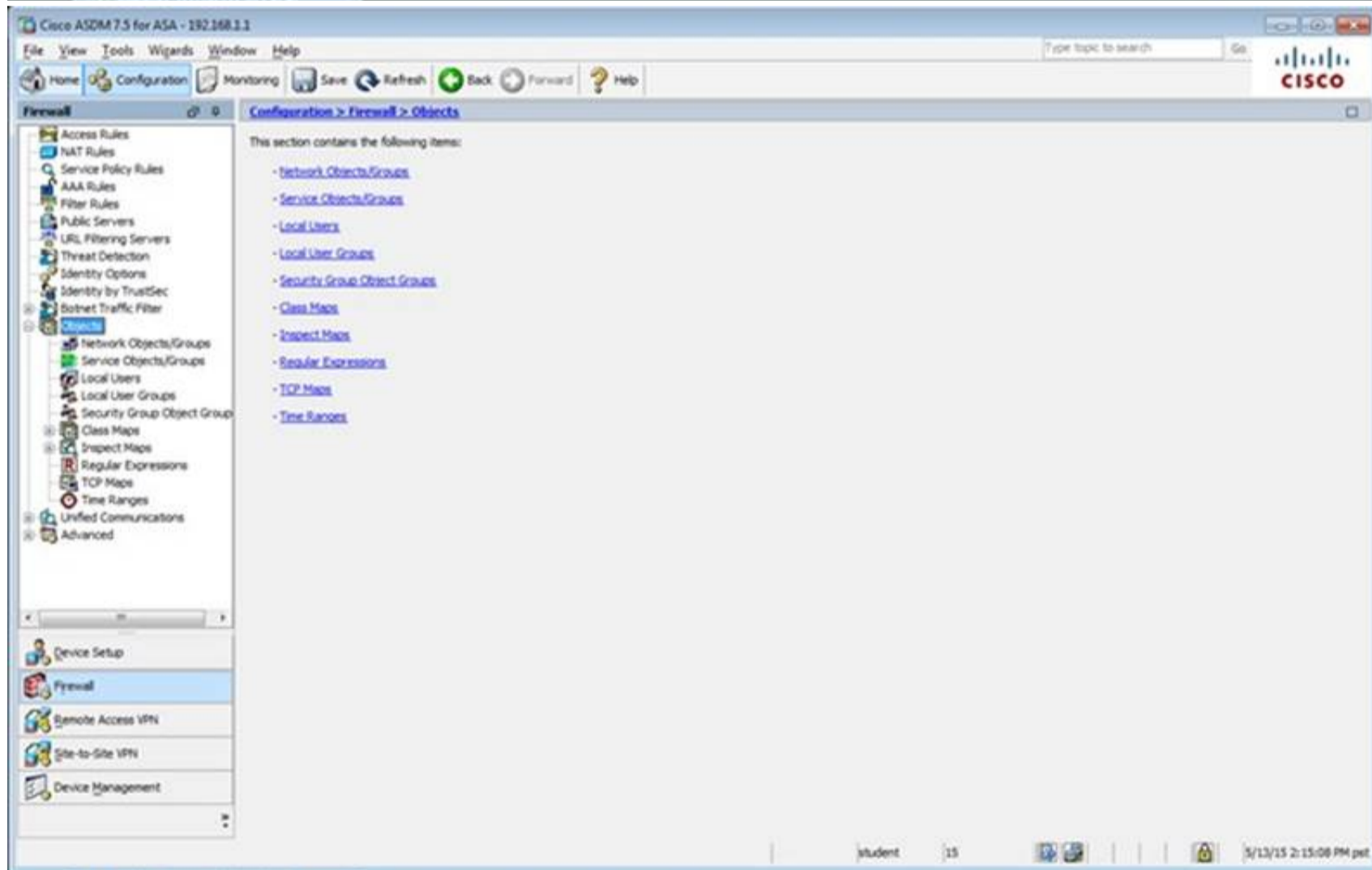
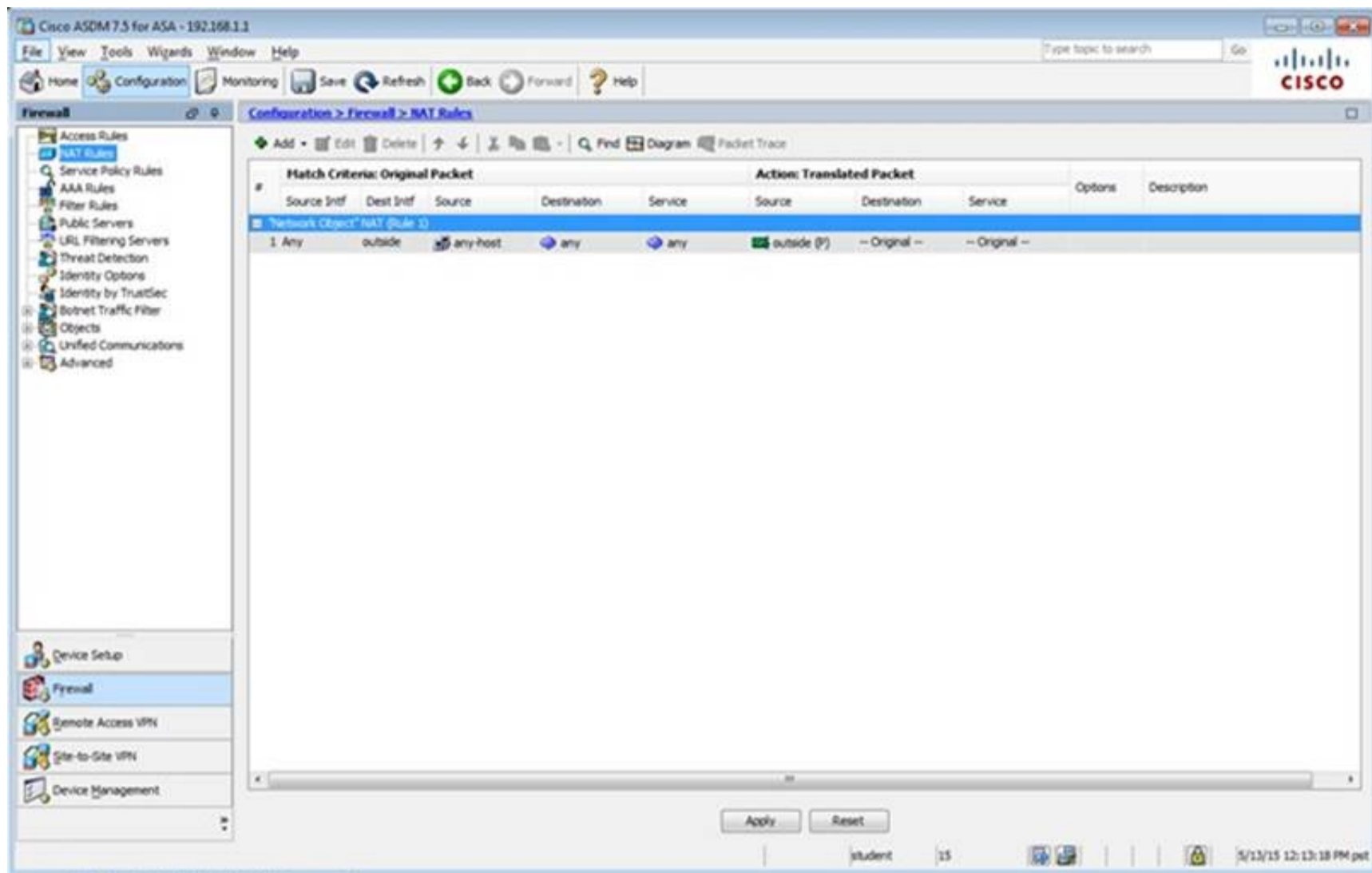
student 15 5/13/15 12:01:38 PM pet

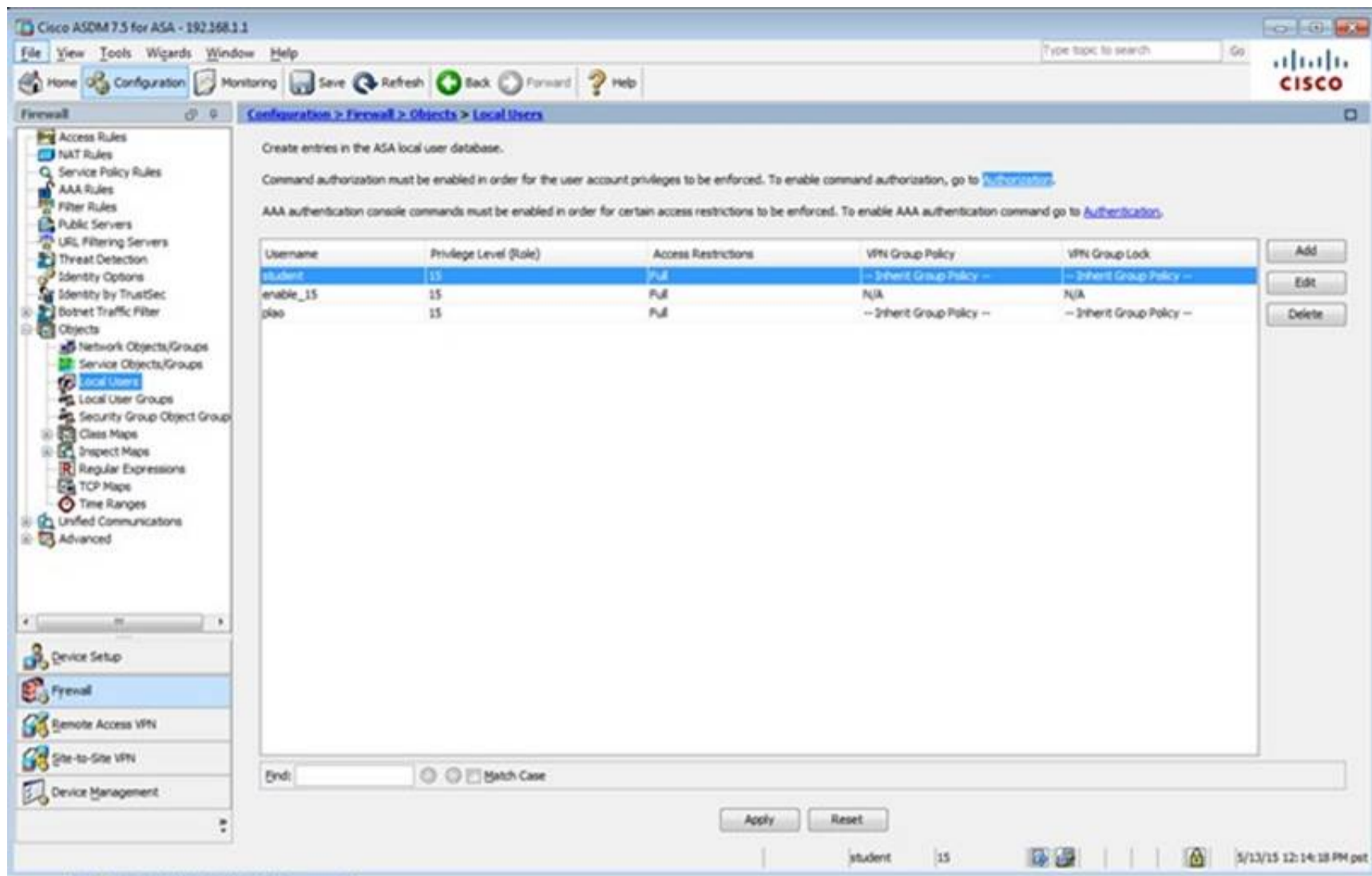
The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Device Management' tree with 'Management Access Rules' selected. The main pane shows the 'Configuration > Device Management > Management Access > Management Access Rules' configuration page. A table with columns for '#', 'Enabled', 'Source Criteria', 'Destination Criteria', 'Service', 'Action', 'Logging', 'Time', and 'Description' is visible. The 'Source Criteria' column is expanded, showing 'Source', 'User', and 'Security Group'. The 'Destination Criteria' column is also expanded, showing 'Security Group' and 'Service'. The 'Action' column is set to 'Allow'. The 'Logging' column is checked. The 'Time' column is set to 'Anytime'. The 'Description' column is empty. The 'Enabled' column is checked. The 'Add' button is visible at the top left of the table. The 'Apply' and 'Reset' buttons are at the bottom right. The status bar at the bottom shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Device Management' tree with 'Management Session Quota' selected. The main pane shows the 'Configuration > Device Management > Management Access > Management Session Quota' configuration page. The text 'Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system' is displayed. The 'Management Session Quota' is set to 'Unlimited' (0 - 30000). The 'Apply' and 'Reset' buttons are at the bottom right. The status bar at the bottom shows 'student' and '15'.









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 [Configuration > System > Command Authorization](#).

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

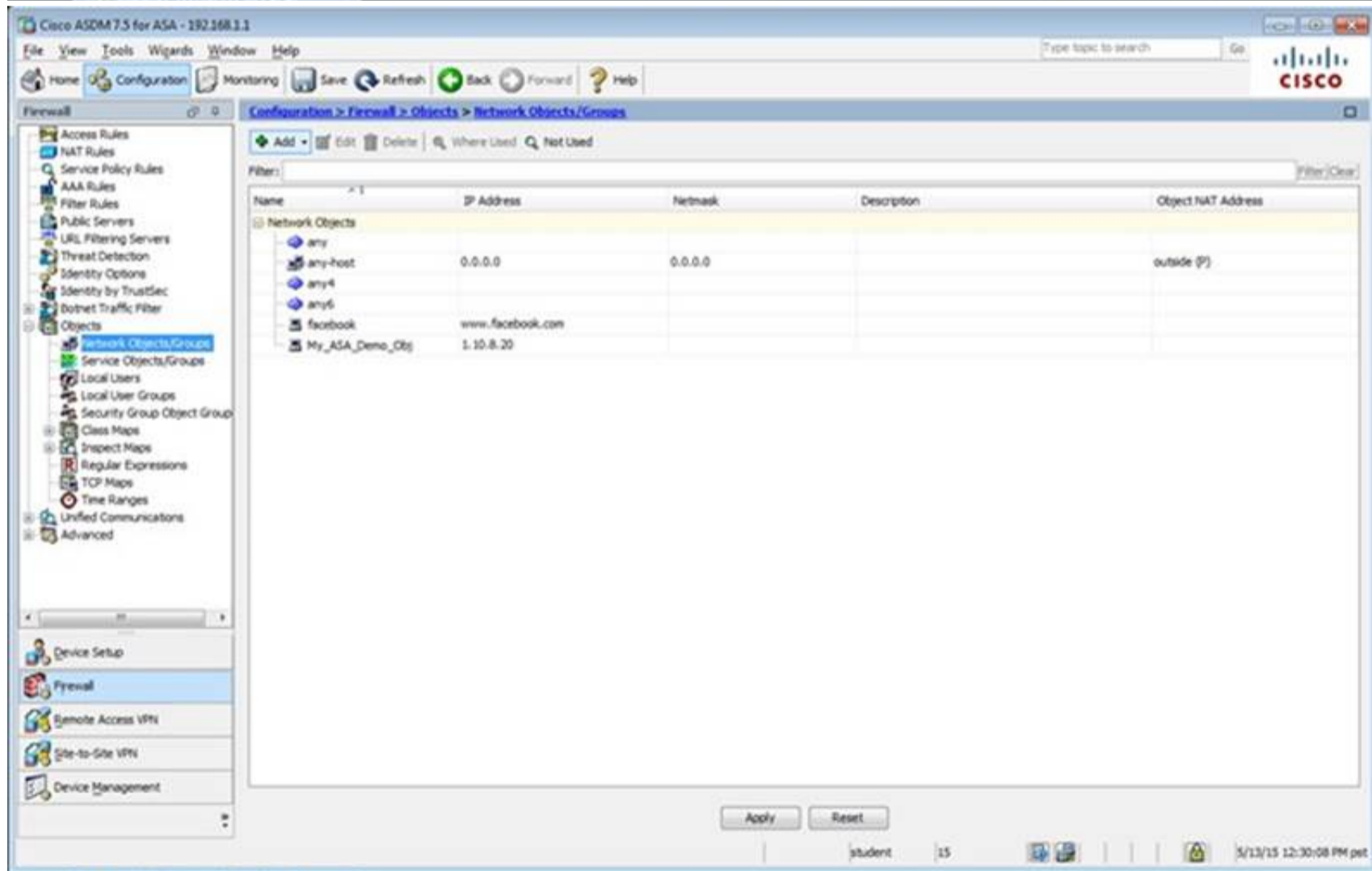
Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
student	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --
enable_15	15	Full	N/A	N/A
plao	15	Full	-- Inherit Group Policy --	-- Inherit Group Policy --

Buttons: Add, Edit, Delete

End:  Match Case

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects > Network Objects/Groups

Filters:  Filter (Clear)

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

Buttons: Add, Edit, Delete, Where Used, Not Used

Apply Reset

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

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Service Policy Rules' selected. The main pane shows the 'Configuration > Firewall > Service Policy Rules' page. A table lists the configured rules:

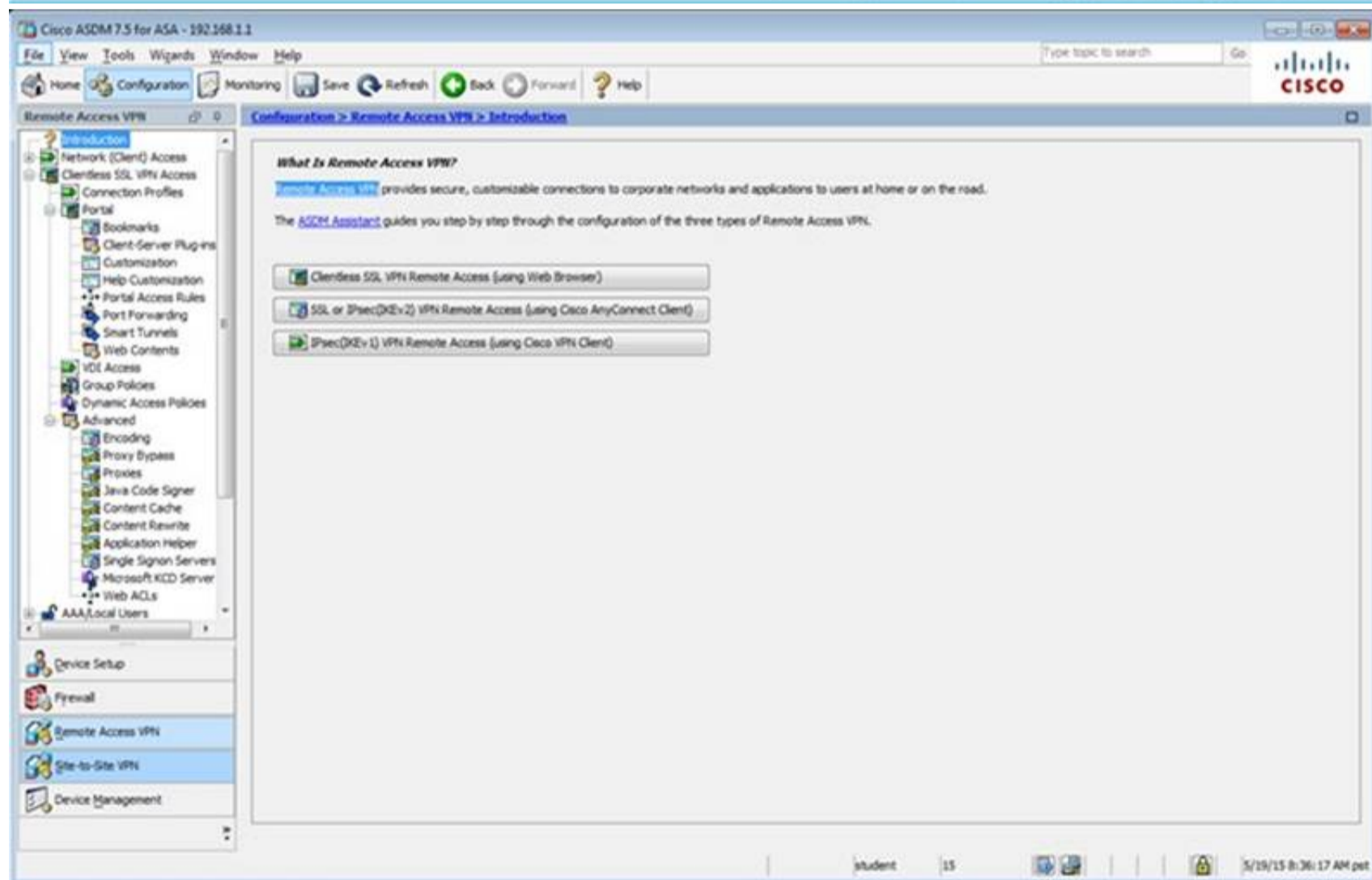
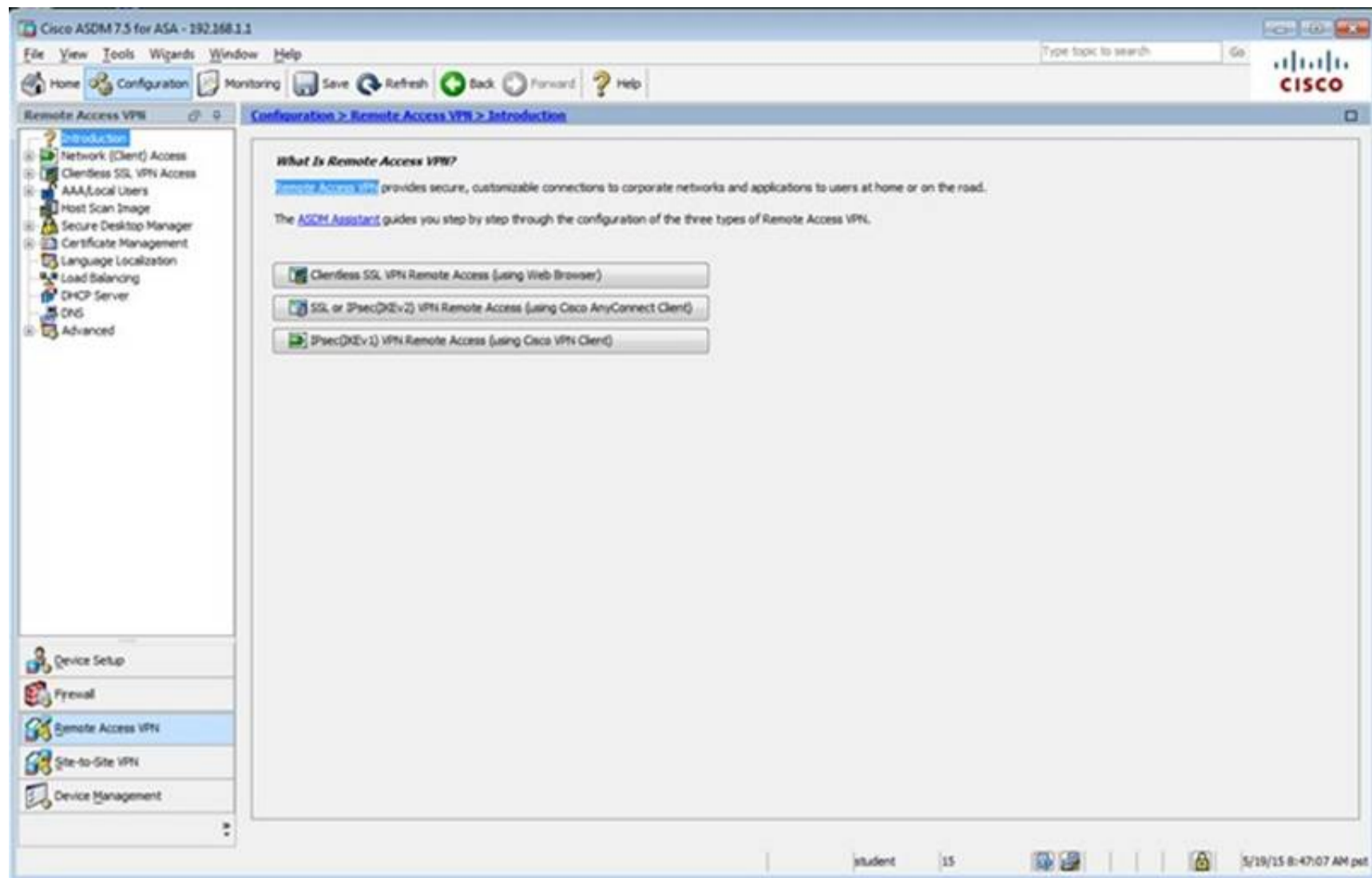
Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Descr
<b>Interface: dmz; Policy: asaifl_policy</b>											
class-default			Match	any		any		any traffic		class-default	
<b>Interface: inside; Policy: asaifl_policy</b>											
class-default		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

Buttons at the bottom include 'Apply' and 'Reset'. The status bar shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Access Rules' selected. The main pane shows the 'Configuration > Firewall > Access Rules' page. A table lists the configured rules:

#	Enabled	Source Criteria:	Destination Criteria:	Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group	
<b>dmz (1 implicit incoming rule)</b>							
1		any			Any less secure ne...		Permit
<b>inside (1 incoming rule)</b>							
1		any			any		Permit 54...
<b>mgmt (0 implicit incoming rules)</b>							
<b>outside (0 implicit incoming rules)</b>							
<b>Global (1 implicit rule)</b>							
1		any			any		Deny

Buttons at the bottom include 'Apply', 'Reset', and 'Advanced...'. The status bar shows 'student' and '15'.



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

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

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

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

[Apply](#) [Reset](#)

student 15 3/19/15 8:38:47 AM pet

Edit Clientless SSL VPN Connection Profile: clientless

Basic Advanced

Name: clientless

Aliases: test

Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

AAA Server Group: LOCAL [Manage...](#)

☐ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS [Manage...](#)

(Following fields are attributes of the DNS server group selected above.)

Servers: 192.168.1.2

Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales [Manage...](#)

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

☒ Enable clientless SSL VPN protocol

Find:

[OK](#) [Cancel](#) [Help](#)

Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Interface-Specific Authentication Server Groups

+ Add Edit Delete

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

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

Interface	Server Group	Fallback to LOCAL	Use primary username

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find:  Next Previous

OK Cancel Help

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 > Bookmarks

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

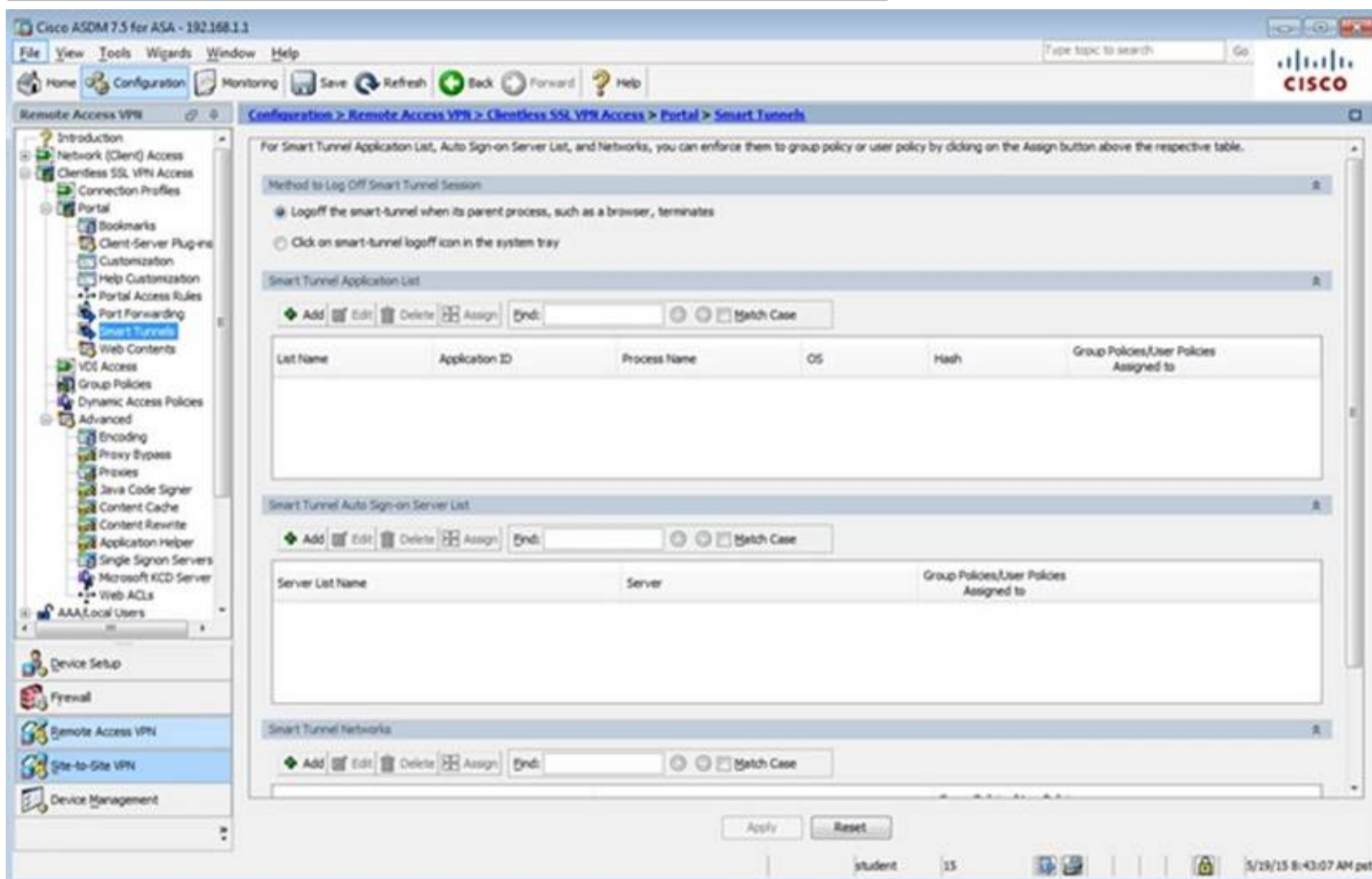
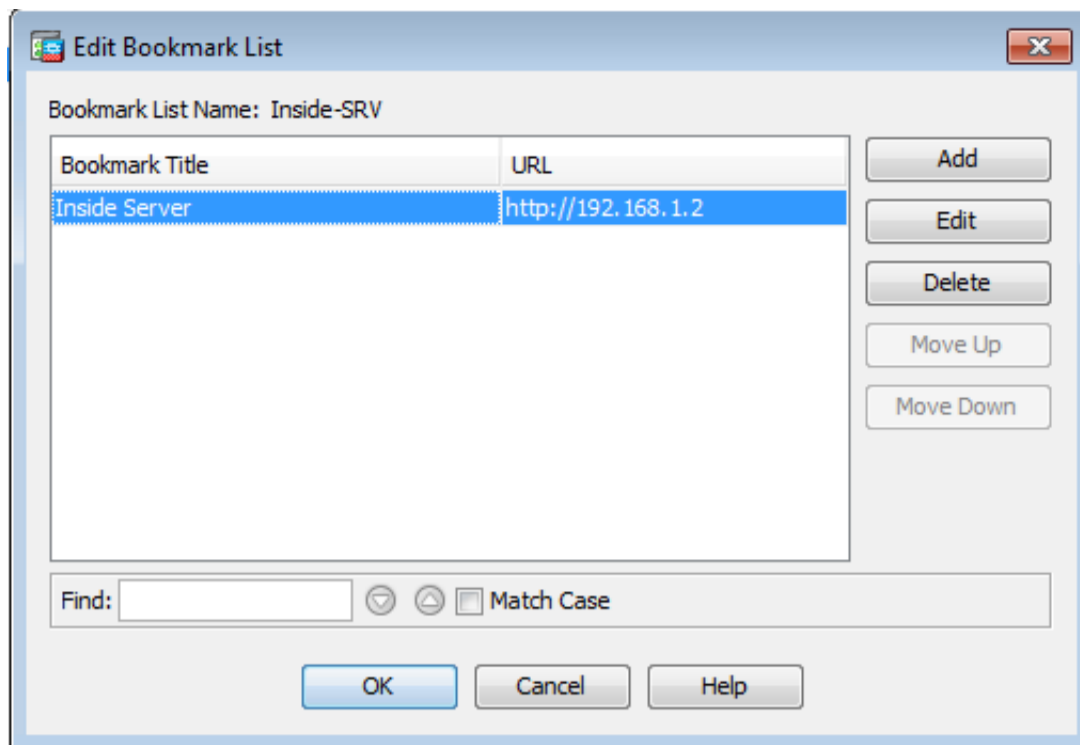
+ Add Edit Delete Import Export Assign

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Ready-001	

Find:  Match Case

Apply Reset

student 15 5/19/15 8:41:57 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 > 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 5/29/15 8:43:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
sales	Internal	ssl-clientless	clientless
DefaultGroupPolicy (System Default)	Internal	Rev 1;rev 2;ssl-clientless/2p-espsec	DefaultRAGroup;Default 2;Group;DefaultADMG;Def...

Find: Match Case

Apply Reset

student 15 5/29/15 8:49:27 AM pet

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

**More Options**

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

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

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

Find:  ☐ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	Sales
DefaultGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultGrpPolicy

Find:  ☐ Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

General

More Options

Customization

Login Setting

Single Signon

VDI Access

Session Settings

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

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Network: Manage...

Tunnel Option: -- None --

Smart Tunnel Application: ☒ Inherit Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

Advanced

Servers

Advanced

Name: DftGrpPolicy

Banner:

SOEP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

More Options

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

Filter: -- None -- Manage...

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

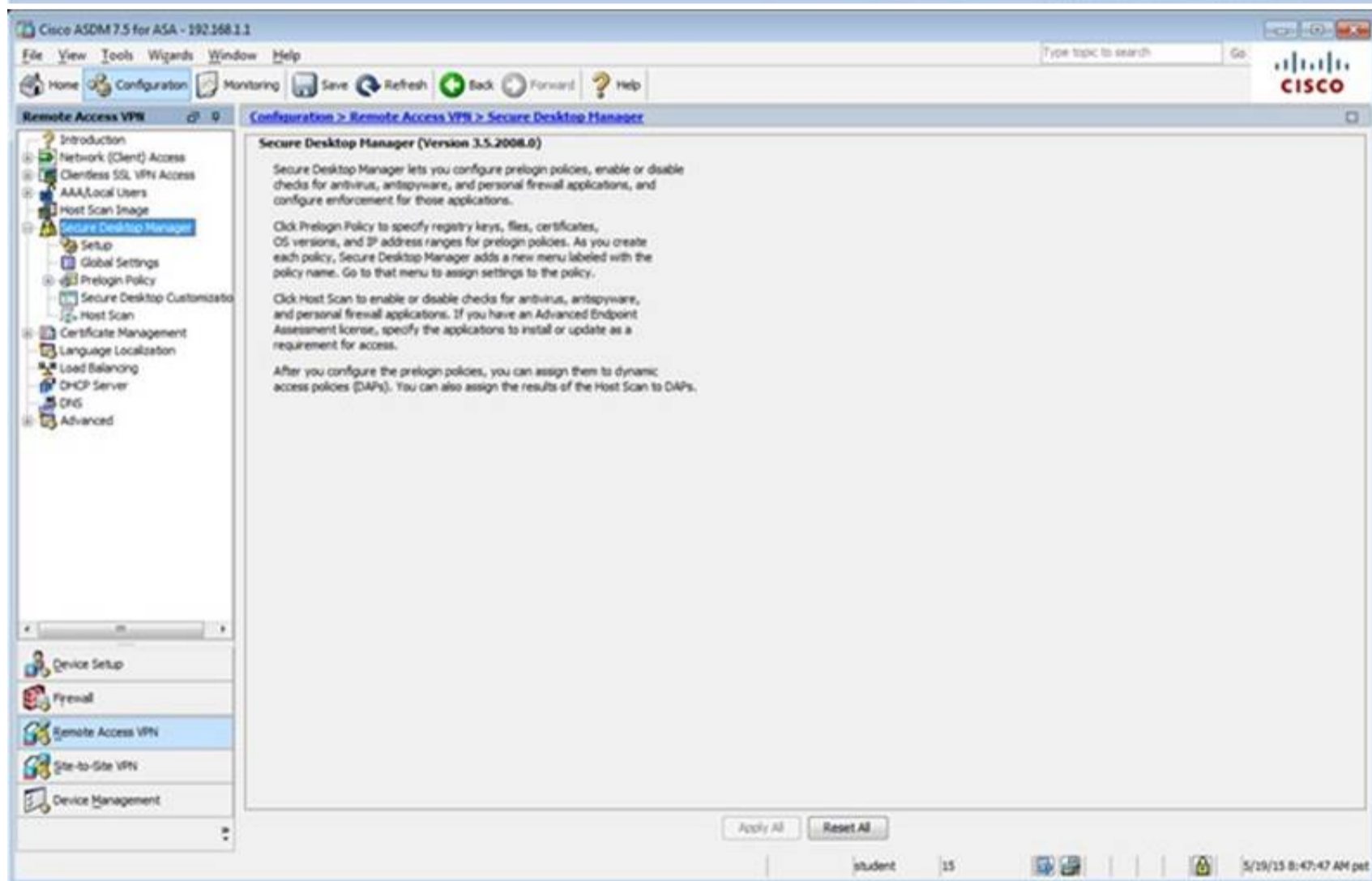
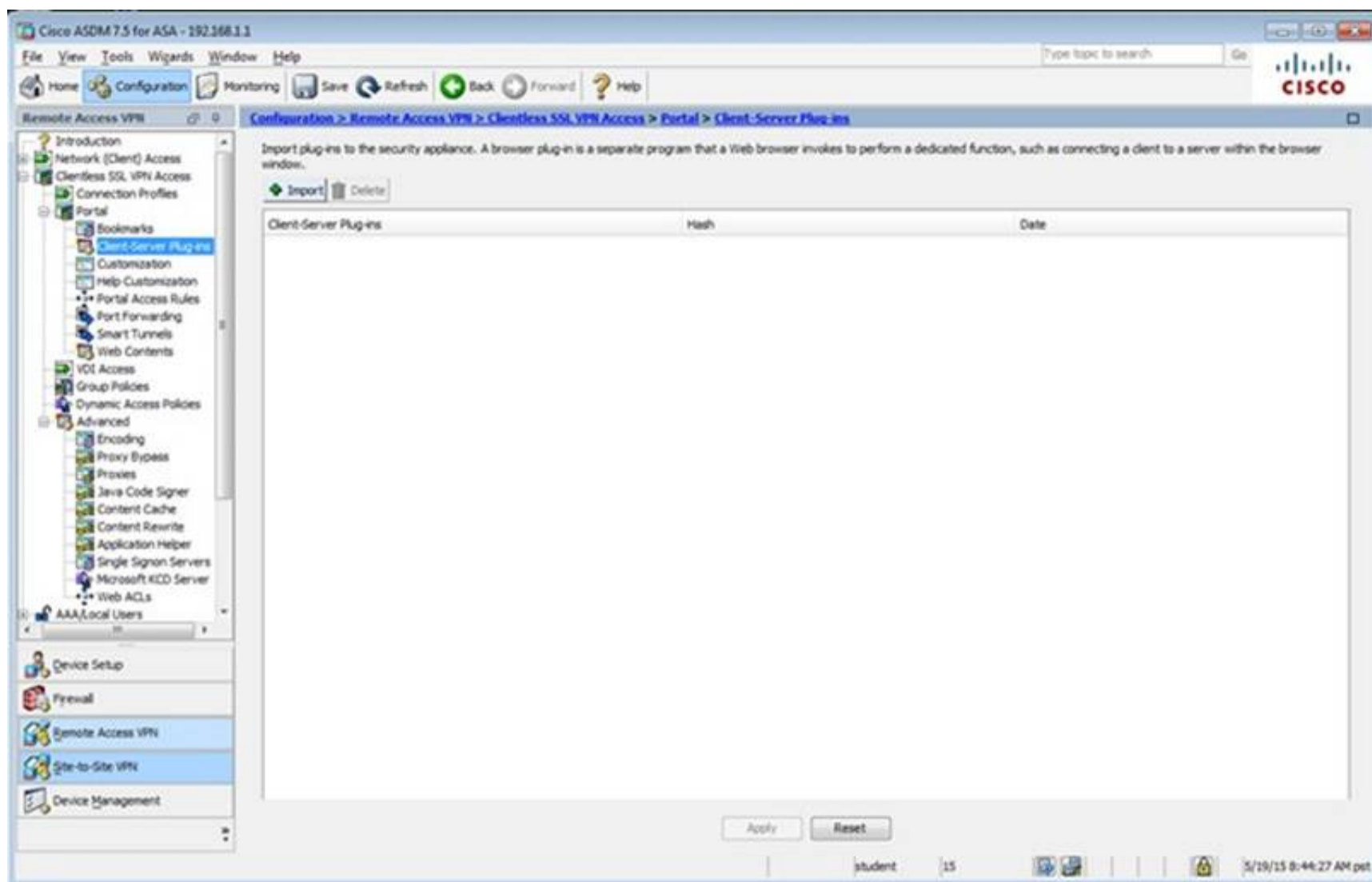
Maximum Connect Time: ☒ Unlimited ☐ minutes

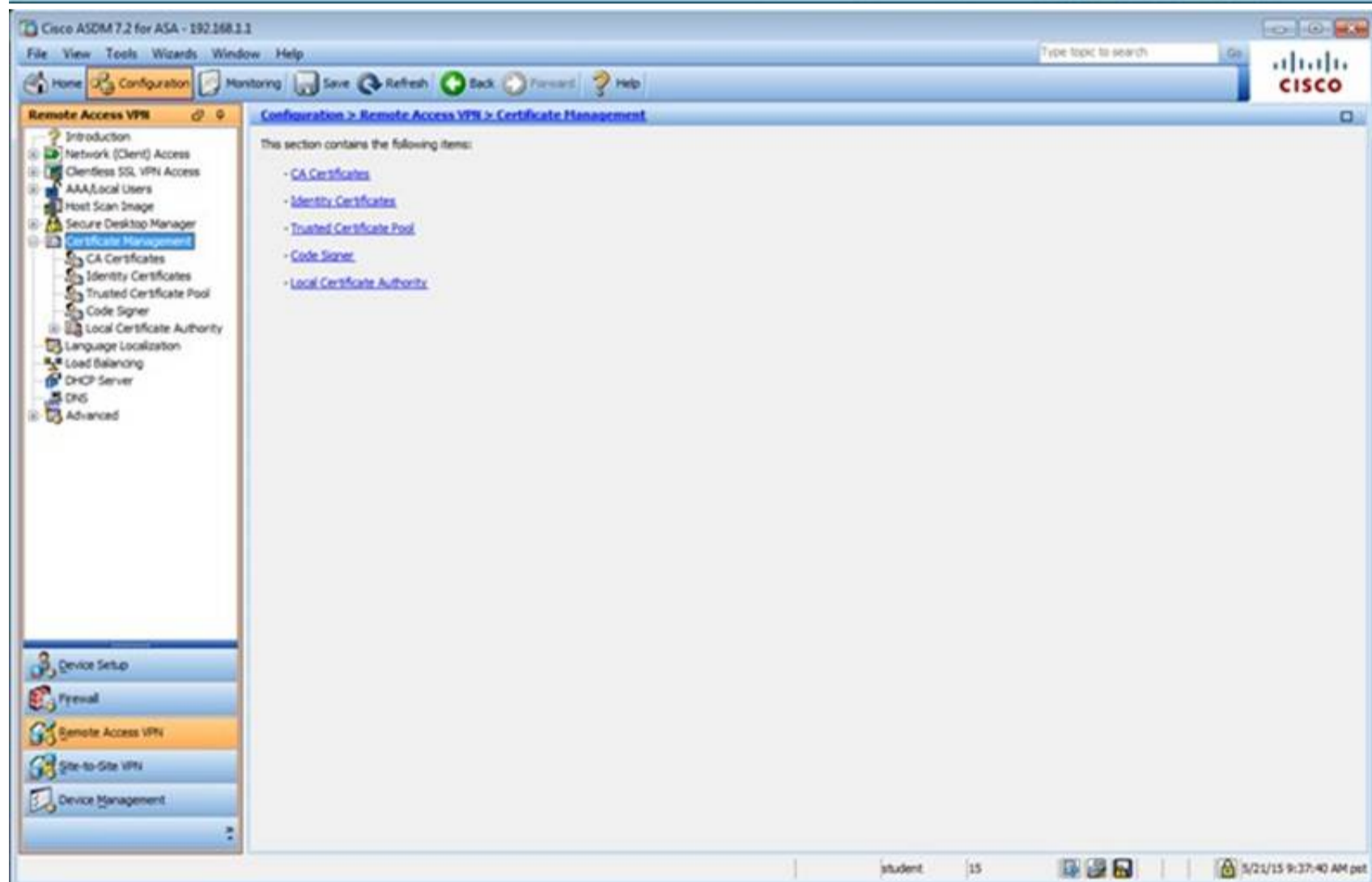
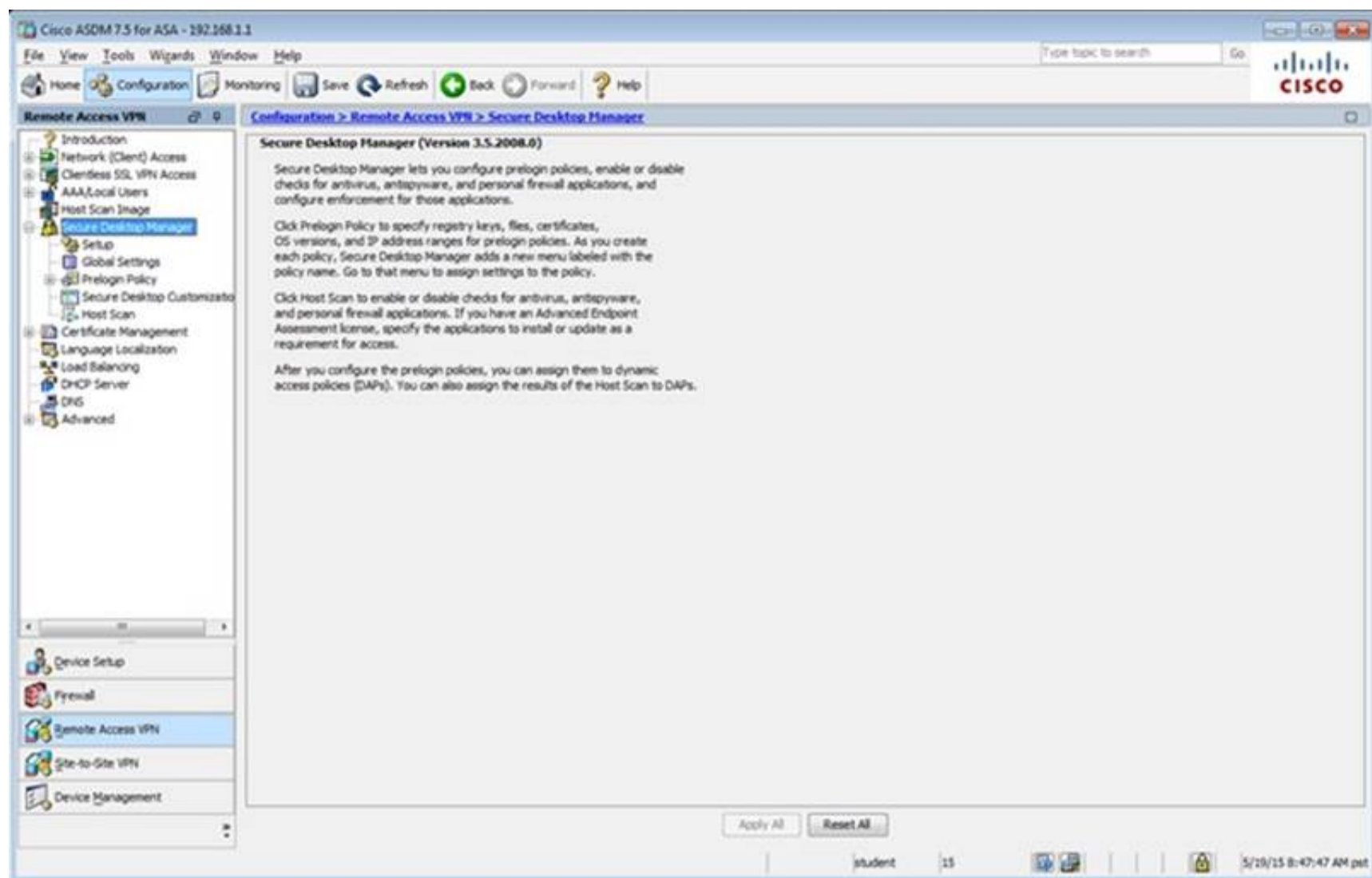
Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find: Next Previous

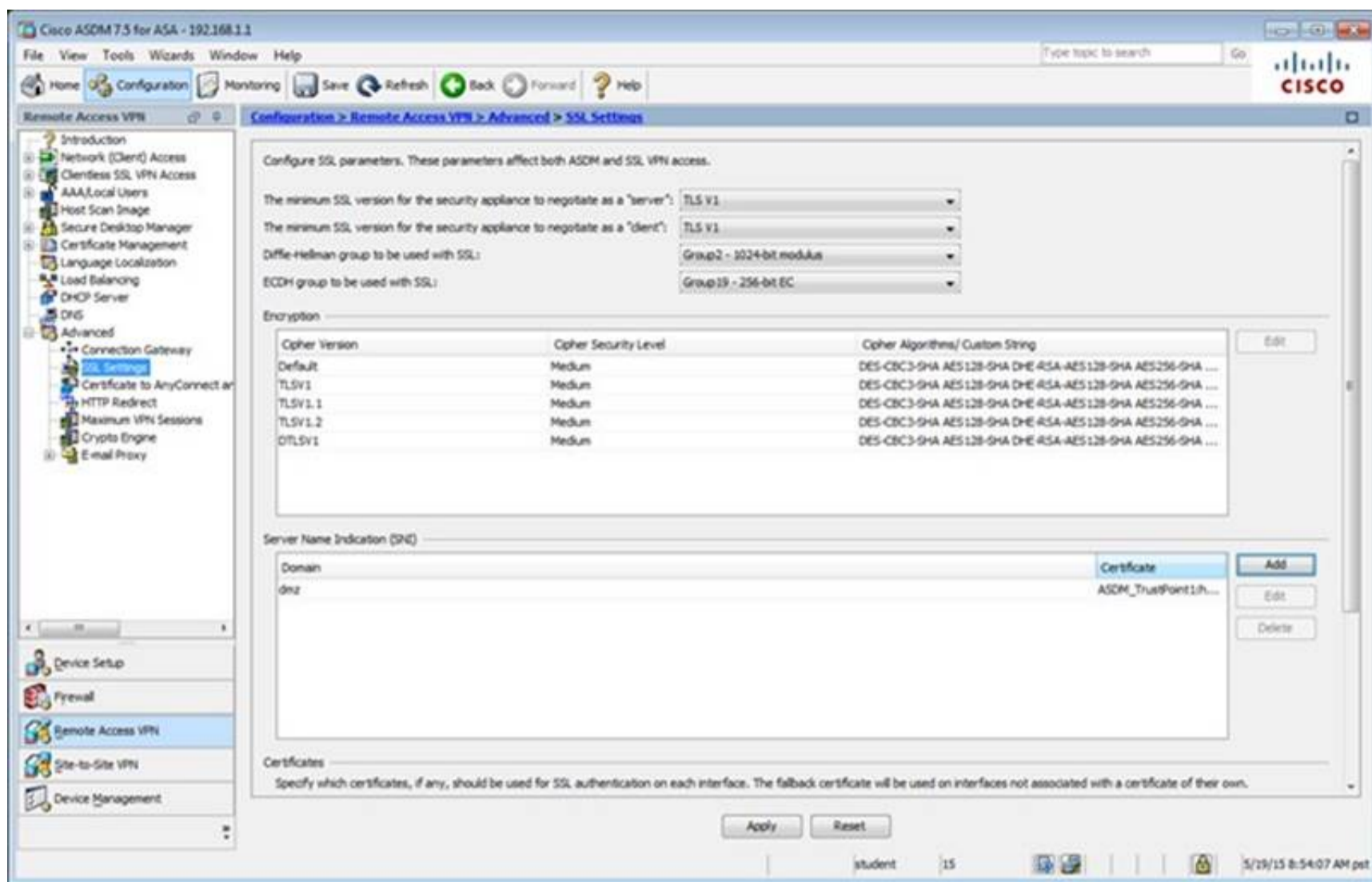
OK Cancel Help





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Identity Certificates' selected under 'Certificate Management'. The main pane displays the 'Identity Certificates' configuration page. It includes a table with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. The table contains one entry: Issued To: testname@P12-ASA.sec, Issued By: testname@P12-ASA.sec, Expiry Date: 11:10:33 pet Dec 20 2024, Associated Trustpoints: ASDM\_TrustPoint1, Usage: General Purpose, Public Key Type: RSA (2048 bits). Below the table are buttons for Add, Show Details, Delete, Export, and Install. There is also a search bar with 'Find:' and 'Match Case' options. Further down, there are sections for 'Certificate Expiration Alerts' (Send the first alert before: 60 days, Repeat Alert Interval: 7 days) and 'Public CA Enrollment' (Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust). A button 'Enroll ASA SSL certificate with Entrust' is present. Below that, a link 'enroll with Entrust' is shown. At the bottom, there is a section for 'ASDM Identity Certificate Wizard' with a button 'Launch ASDM Identity Certificate Wizard' and 'Apply' and 'Reset' buttons.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Advanced' selected under 'Remote Access VPN'. The main pane displays the 'Advanced' configuration page. It includes a list of items: Introduction, Network (Client) Access, Clientless SSL VPN Access, AAA/Local Users, Host Scan Image, Secure Desktop Manager, Certificate Management, Language Localization, Load Balancing, DHCP Server, DNS, and Advanced. The 'Advanced' section contains the following items: Connection Gateway, SSL Settings, Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps, HTTP Redirect, Maximum VPN Sessions, Crypto Engine, and E-mail Proxy. The bottom status bar shows 'student', '15', and the time '5/19/15 8:52:47 AM pet'.



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

Diffie-Hellman group to be used with SSL: Group2 - 2024-bit modulus

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

Encryption

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

Server Name Indication (SNI)

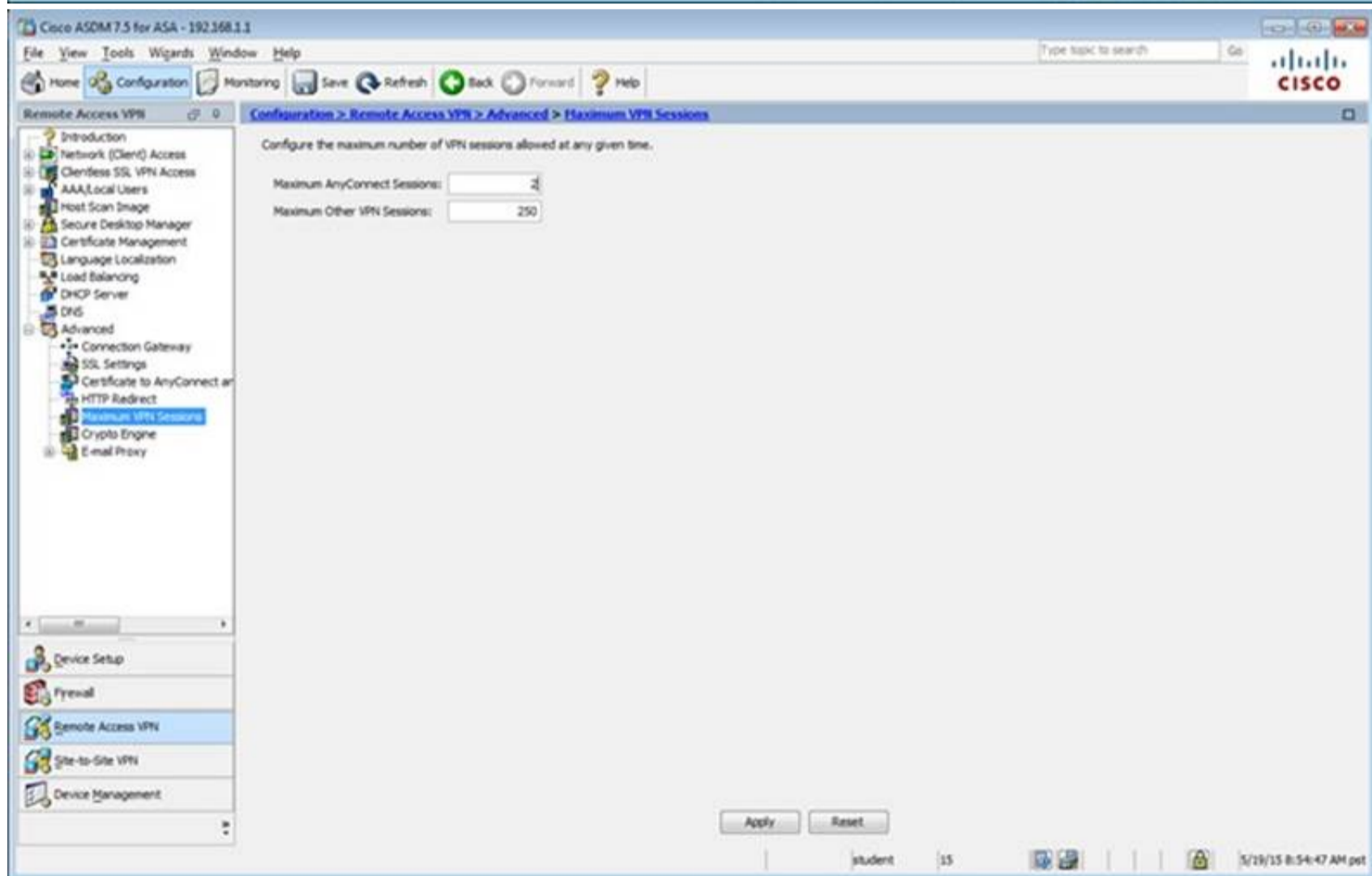
Domain	Certificate
dmz	ASDM_TrustPoint1.h...

Certificates

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

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions

Configure the maximum number of VPN sessions allowed at any given time.

Maximum AnyConnect Sessions: 2

Maximum Other VPN Sessions: 250

Apply Reset

student 15 5/19/15 8:54:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

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

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

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

**Important Concepts**

Following are some important concepts for setting up a connection.

**1. SSL tunnel and IPsec tunnel**

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

**2. User and connection profile**

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

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

**3. Access policy**

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

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

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

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

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DefaultGroup (System Default)	Internal	ikev1,ikev2,ssl-clientless,ipsec	DefaultRAGroup,Default,3,Group,DefaultVPNGroup

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: DftGrpPolicy

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for IPsec access.

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

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

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

Find: Match Case

Apply Reset

student 15 5/28/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

[Add](#) [Edit](#) [Delete](#) End:  Match Case

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

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

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > AAA/Local Users

This section contains the following items:

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

student 15 5/19/15 8:58:57 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

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

Create entries in the ASA local user database.

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

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

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

End:  Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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

AAA Server Groups

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

End:  Match Case

Servers in the Selected Group

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

End:  Match Case

LDAP Attribute Map

Apply Reset

student 15 5/19/15 8:59:57 AM pet

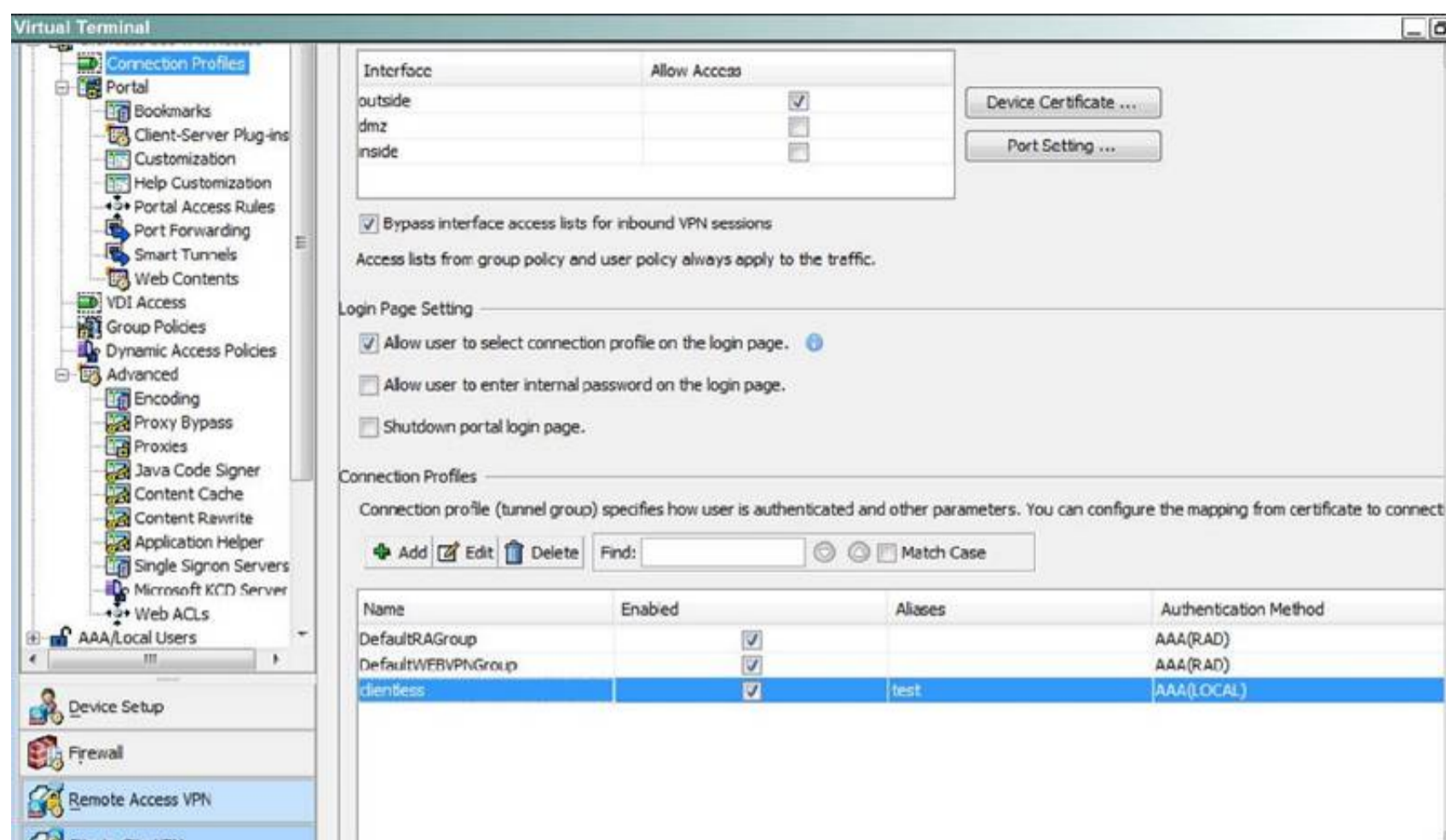
Which two statements regarding the ASA VPN configurations are correct? (Choose two)

- A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM\_TrustPoint1.
- B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
- C. The Inside-SRV bookmark references the https://192.168.1.2URL
- 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: BC

Explanation:

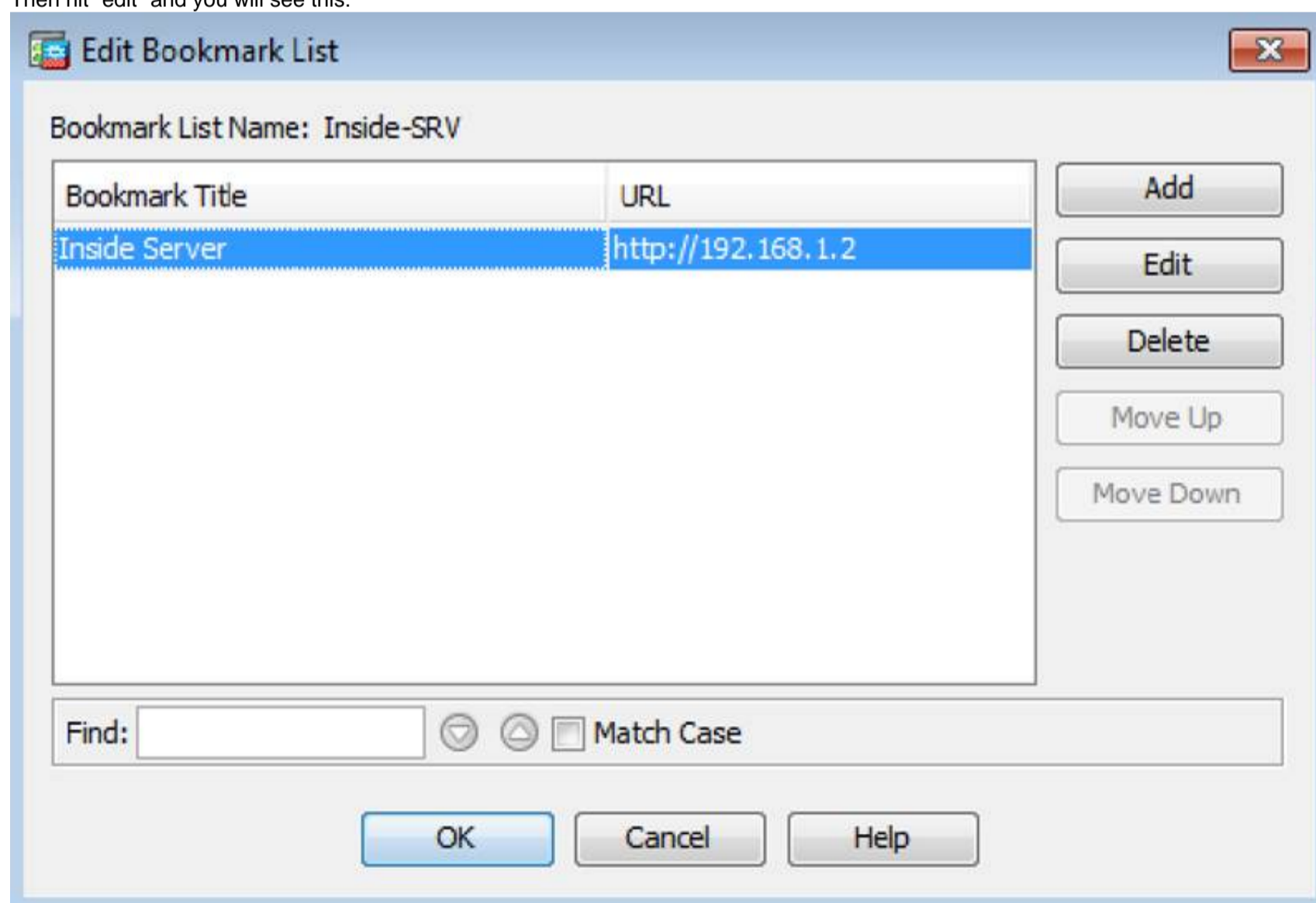
For B:



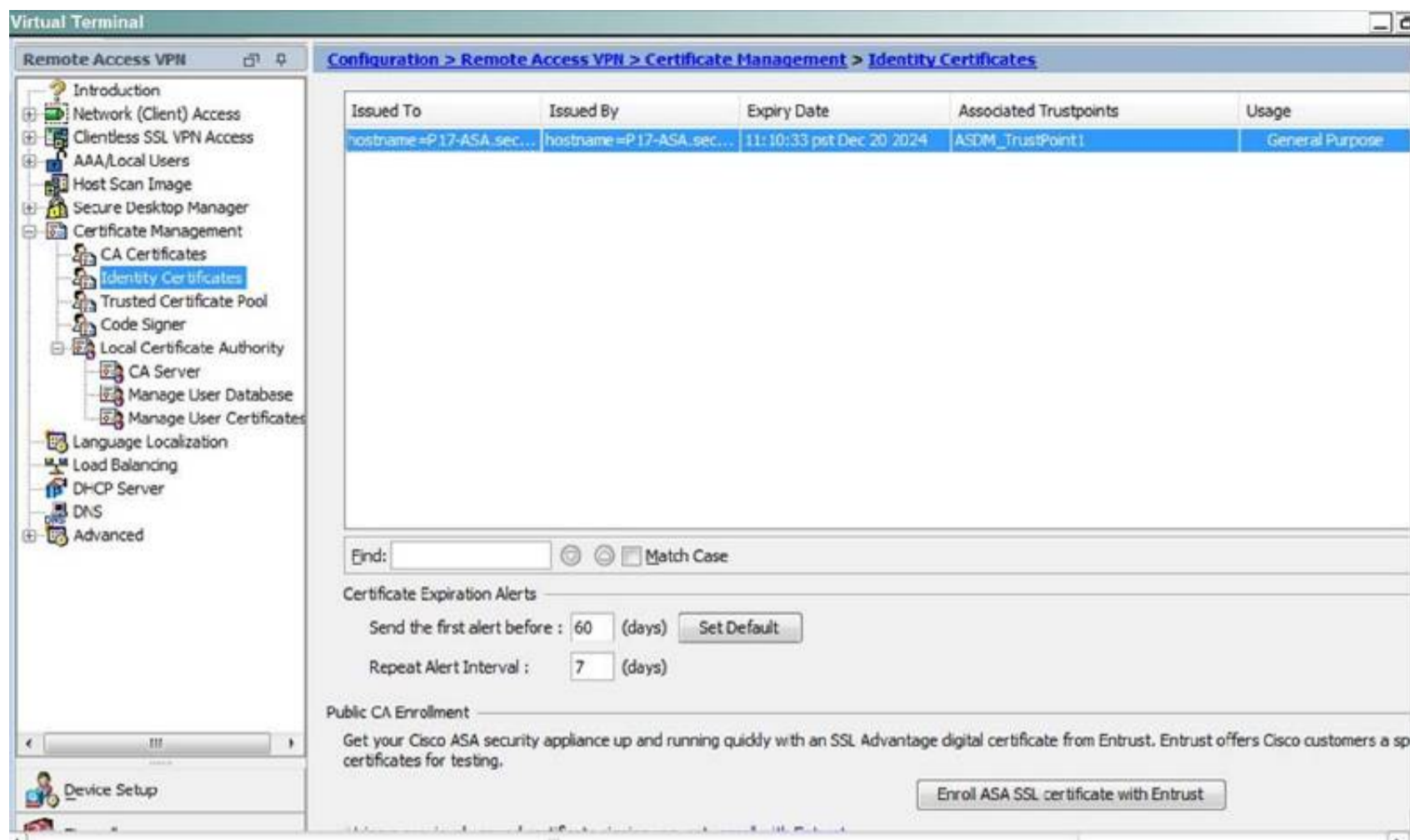
For C, Navigate to the Bookmarks tab:



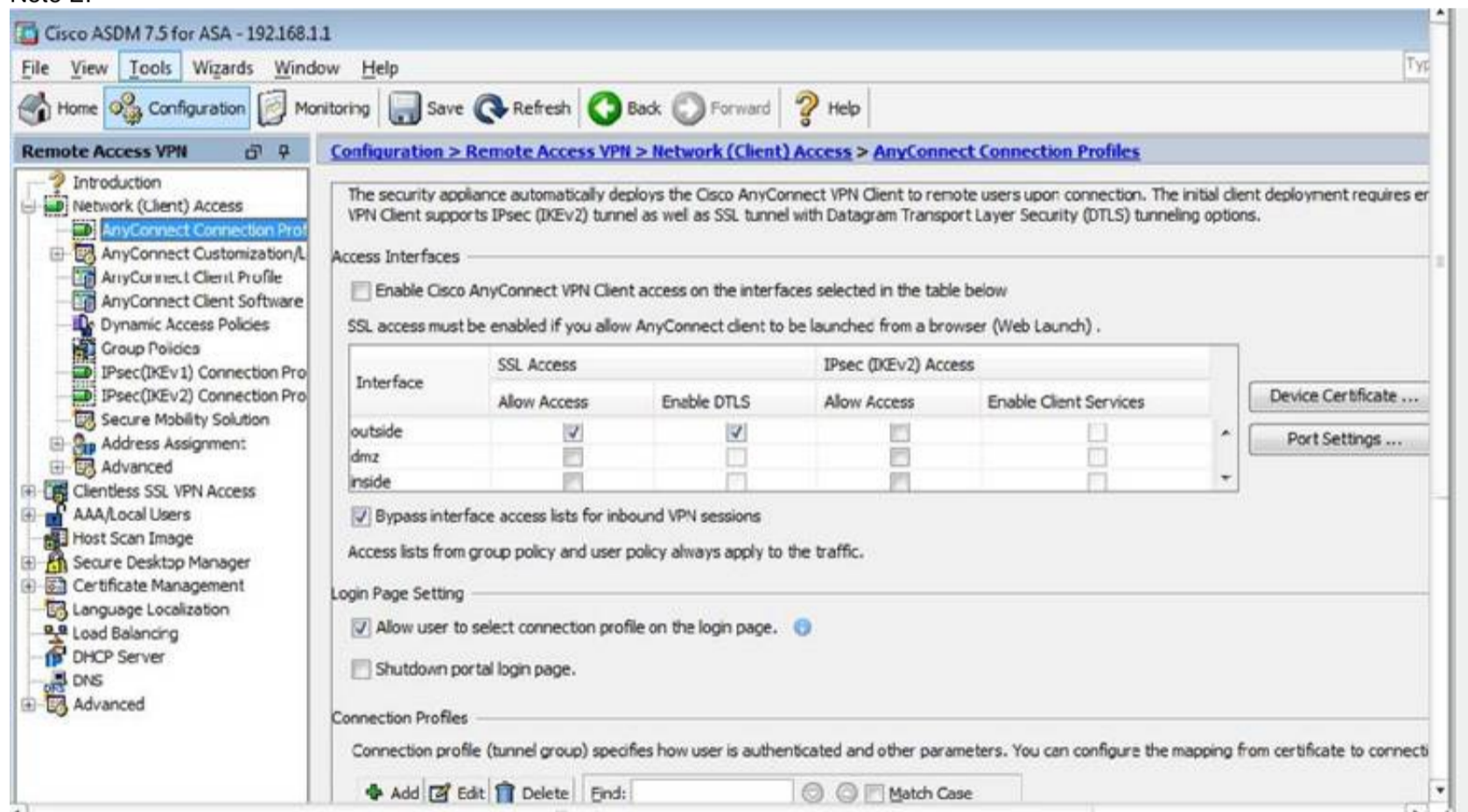
Then hit "edit" and you will see this:



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



Note E:



## NEW QUESTION 16

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: AB

**Explanation:** In stateless inspection, the firewall inspects a packet to determine the 5-tuple--source and destination IP addresses and ports, and protocol--information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

Source:

[http://www.cisco.com/c/en/us/td/docs/wireless/asr\\_5000/19-0/XMART/PSF/19-PSF-Admin/19-PSF-Admin\\_chapter\\_01.html](http://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/19-0/XMART/PSF/19-PSF-Admin/19-PSF-Admin_chapter_01.html)

## NEW QUESTION 17

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

**Explanation:** Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns.

Source:

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

#### NEW QUESTION 21

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

**Explanation:** Private VLAN divides a VLAN (Primary) into sub-VLANs (Secondary) while keeping existing IP subnet and layer 3 configuration. A regular VLAN is a single broadcast domain, while private VLAN partitions one broadcast domain into multiple smaller broadcast subdomains.

Source: [https://en.wikipedia.org/wiki/Private\\_VLAN](https://en.wikipedia.org/wiki/Private_VLAN)

#### NEW QUESTION 25

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

**Explanation:** Using Security Intelligence Whitelists

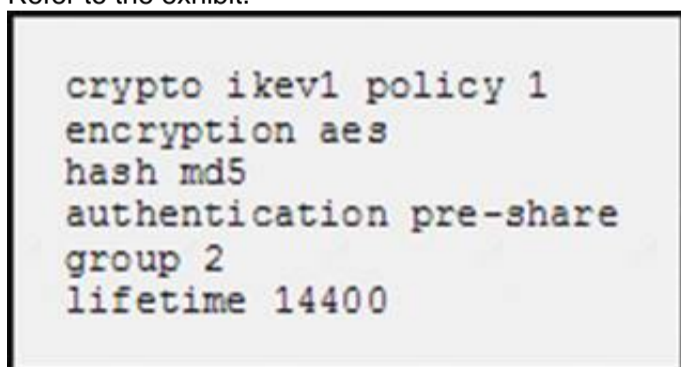
In addition to a blacklist, each access control policy has an associated whitelist, which you can also populate with Security Intelligence objects. A policy's whitelist overrides its blacklist. That is, the system evaluates traffic with a whitelisted source or destination IP address using access control rules, even if the IP address is also blacklisted. In general, use the whitelist if a blacklist is still useful, but is too broad in scope and incorrectly blocks traffic that you want to inspect.

Source:

<http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Secint-Blacklisting.pdf>

#### NEW QUESTION 28

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

**Explanation:** Configure the IPsec phase1 with the 5 parameters HAGLE (Hashing-Authentication-Group-Lifetime-Encryption)

#### NEW QUESTION 31

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

**Explanation:** URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in an URL list. You can maintain a local URL list on the router. If the Cisco IOS image on the router supports URL filtering but does not support Zone-based Policy Firewall (ZPF), you can maintain one local URL list on the router to add or edit an URLs. Enter a full domain name or a partial domain name and choose whether to Permit or Deny requests for this URL.

Source:

[http://www.cisco.com/c/en/us/td/docs/routers/access/cisco\\_router\\_and\\_security\\_device\\_manager/24/software/user/guide/URLftr.html#wp999509](http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/URLftr.html#wp999509)

#### NEW QUESTION 34

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

**Explanation:** STP switch port states:

+ Blocking - A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.

+ Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.

+ Learning - While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC address table, but does not forward frames.

+ Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

+ Disabled - Not strictly part of STP, a network administrator can manually disable a port Source: [https://en.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](https://en.wikipedia.org/wiki/Spanning_Tree_Protocol)

#### NEW QUESTION 36

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

**Explanation:** In network computing, hairpinning (or NAT loopback) describes a communication between two hosts behind the same NAT device using their mapped endpoint. Because not all NAT devices support this communication configuration, applications must be aware of it.

Hairpinning is where a machine on the LAN is able to access another machine on the LAN via the external IP address of the LAN/router (with port forwarding set up on the router to direct requests to the appropriate machine on the LAN).

Source: <https://en.wikipedia.org/wiki/Hairpinning>

#### NEW QUESTION 40

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

**Explanation:** autocommand: (Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line.

So after successfully logs in the Admin user sees the running configuration and immediately after is disconnected by the router. So removing the command lets keeps him connected.

Source:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book\\_chapter\\_0110.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_0110.html)

#### NEW QUESTION 44

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

**Explanation:** Smart Tunnel is an advanced feature of Clientless SSL VPN that provides seamless and highly secure remote access for native client-server applications. Clientless SSL VPN with Smart Tunnel is the preferred solution for allowing access from non-corporate assets as it does not require the administrative rights. Port forwarding is the legacy technology for supporting TCP based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.

Source:

<http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/tunnel.pdf>

#### NEW QUESTION 48

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

**Explanation:** An example of anomaly-based IPS/IDS is creating a baseline of how many TCP sender requests are generated on average each minute that do not get a response. This is an example of a half-opened session. If a system creates a baseline of this (and for this discussion, let's pretend the baseline is an average of 30 half-opened sessions per minute), and then notices the half-opened sessions have increased to more than 100 per minute, and then acts based on that and generates an alert or begins to deny packets, this is an example of anomaly-based IPS/IDS. The Cisco IPS/IDS appliances have this ability (called anomaly detection), and it is used to identify worms that may be propagating through the network.

Source: Cisco Official Certification Guide, Anomaly-Based IPS/IDS, p.464

#### NEW QUESTION 51

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

**Explanation:** A show crypto isakmp sa command shows the ISAKMP SA to be in MM\_NO\_STATE. This also means that main mode has failed.

Dstsrc state conn-id slot

10.1.1.2 10.1.1.1 MM\_NO\_STATE 1 0

Verify that the phase 1 policy is on both peers, and ensure that all the attributes match.

Source:

[http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#isakmp\\_sa](http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#isakmp_sa)

#### NEW QUESTION 55

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

**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

#### NEW QUESTION 57

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

**Explanation:** /Reference/ b\_syssec\_cr42crs/b\_syssec\_cr41crs\_chapter\_0100.html#wp2198915138

## NEW QUESTION 59

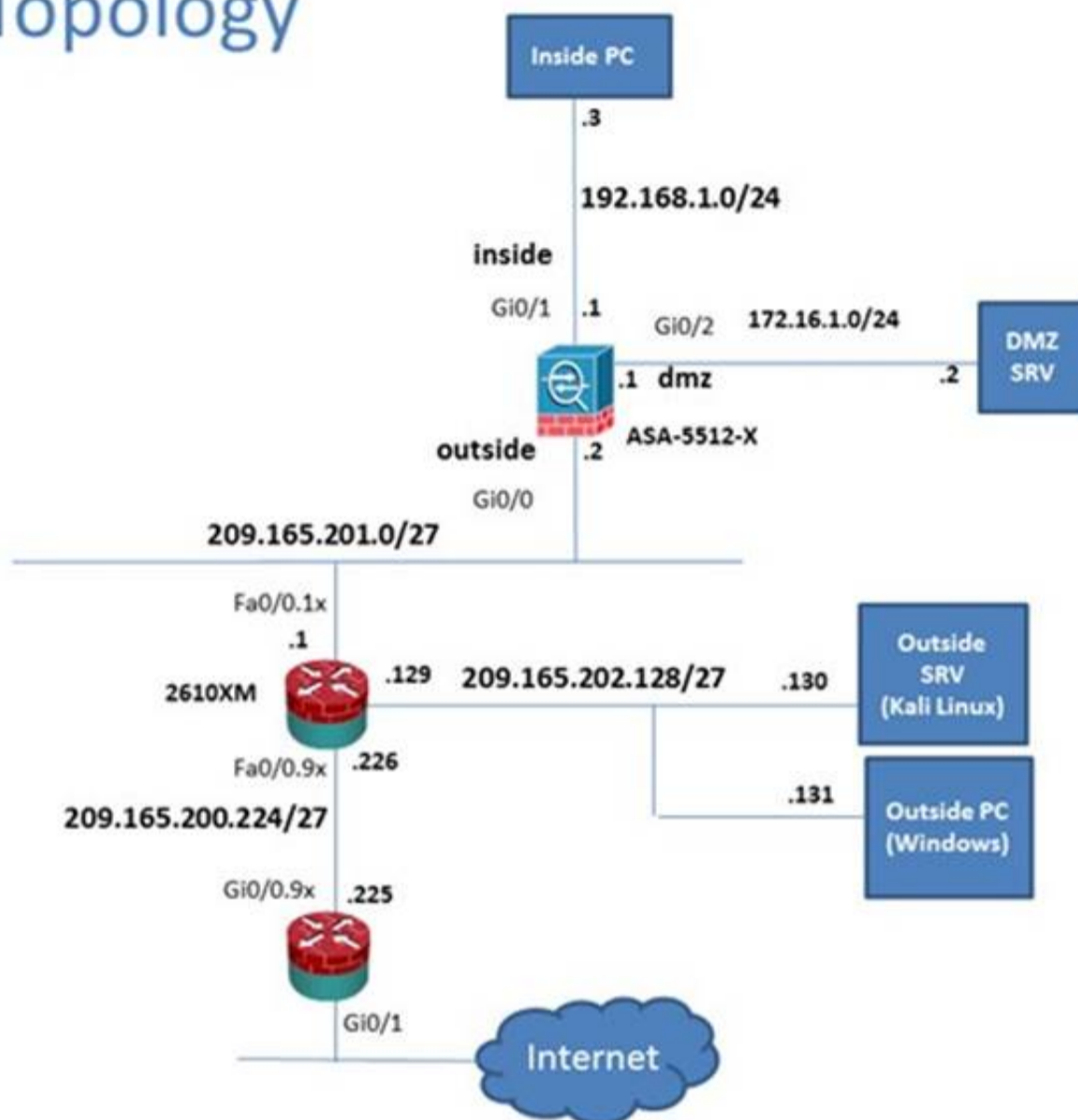
### Scenario

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

To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

## Lab Topology



The screenshot shows the Cisco ASDM 7.5 interface for ASA - 192.168.1.1. The main window displays the 'Device Information' tab, showing the host name 'P17-ASA-secure-x.local', ASA version '100.14(6)13', and device type 'ASA 5512'. The 'Interface Status' table shows the following:

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

The 'System Resources Status' section shows memory usage (100MB) and CPU usage (100%). The 'Traffic Status' section shows connections per second usage and interface traffic usage (Input Kbps: 0, Output Kbps: 0). The 'Latest ASDM Syslog Messages' section shows the following messages:

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.202.1	000c.3014.3820	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.8be6.98f3	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 pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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	Default Clientless	Clientless Clientless (IPsec4)	08:05:46 pet Thu May 21 2015 0h09m.19s	318774 41633

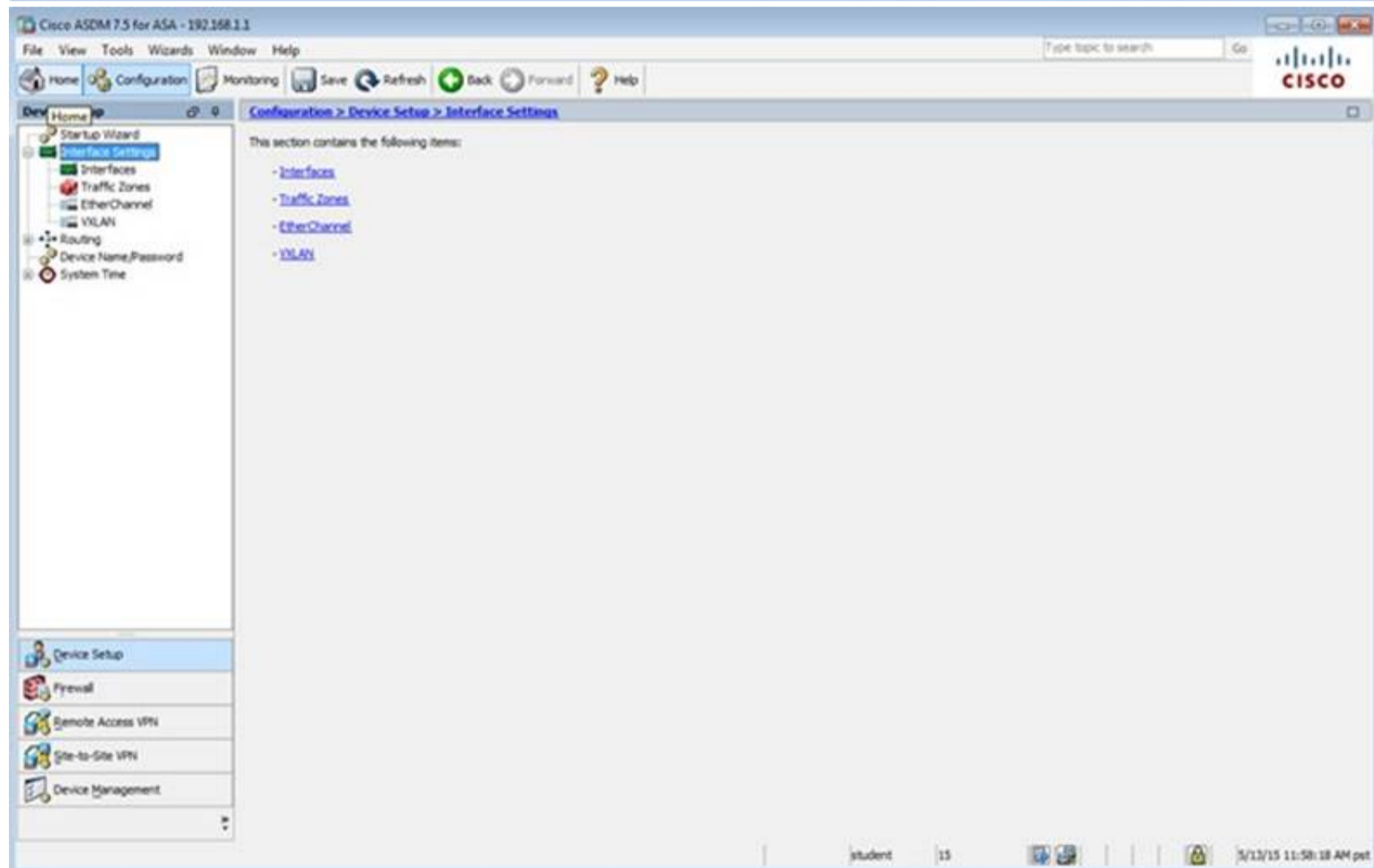
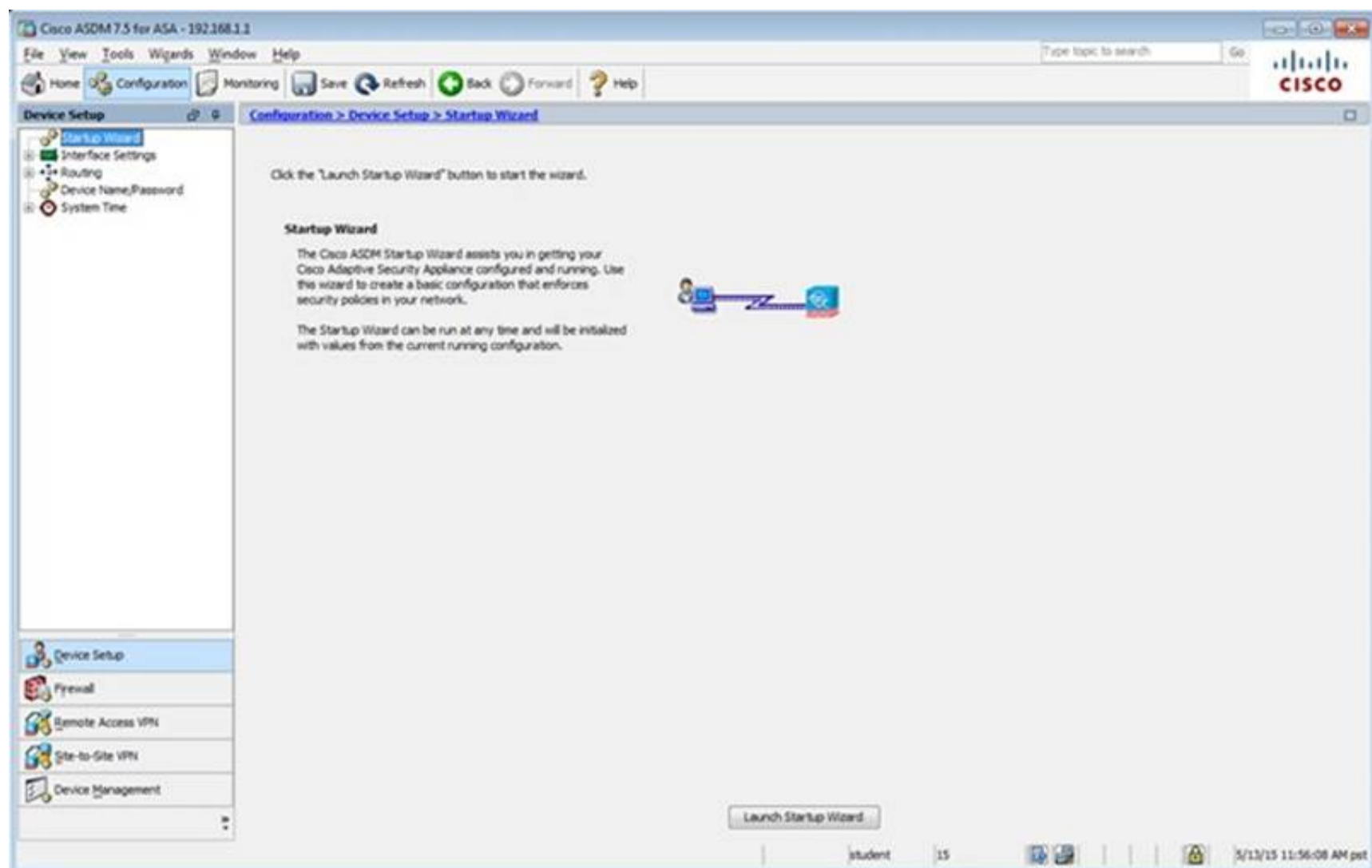
Details Logout Ping

Refresh

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

Data Refreshed Successfully.

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Configuration > Device Setup > Interface Settings > Interfaces

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask	Prefix Length	Group	Type
GigabitEthernet0/0	outside			Enabled		0.0.0.0	255.255.255.0			Hardware
GigabitEthernet0/1	inside			Enabled		100 192.168.1.1	255.255.255.0			Hardware
GigabitEthernet0/2	dmz			Enabled		172.16.1.1	255.255.255.0			Hardware
GigabitEthernet0/3				Enabled						Hardware
GigabitEthernet0/4				Enabled						Hardware
GigabitEthernet0/5	mgmt			Enabled		100 10.10.10.2	255.255.255.0			Hardware
Management0/0				Enabled						Hardware

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

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Management Access

This section contains the following items:

- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Quota
- SNMP
- Management Access Rules

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

student 15 5/13/15 11:59:28 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

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

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

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

Http Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

DH Key Exchange: ☒ Group 1 ☐ Group 14

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > Management Access > Management Interface

Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.

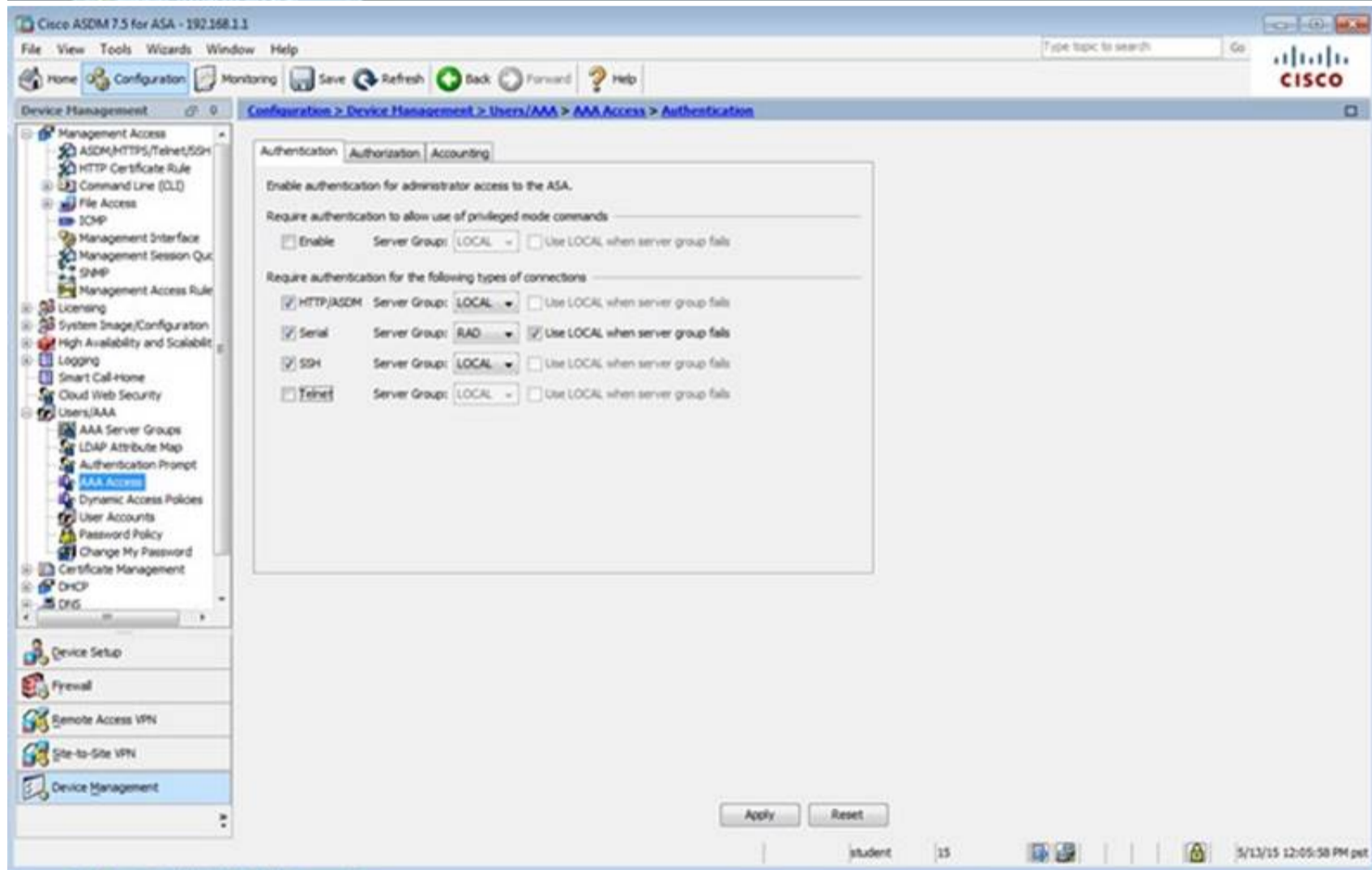
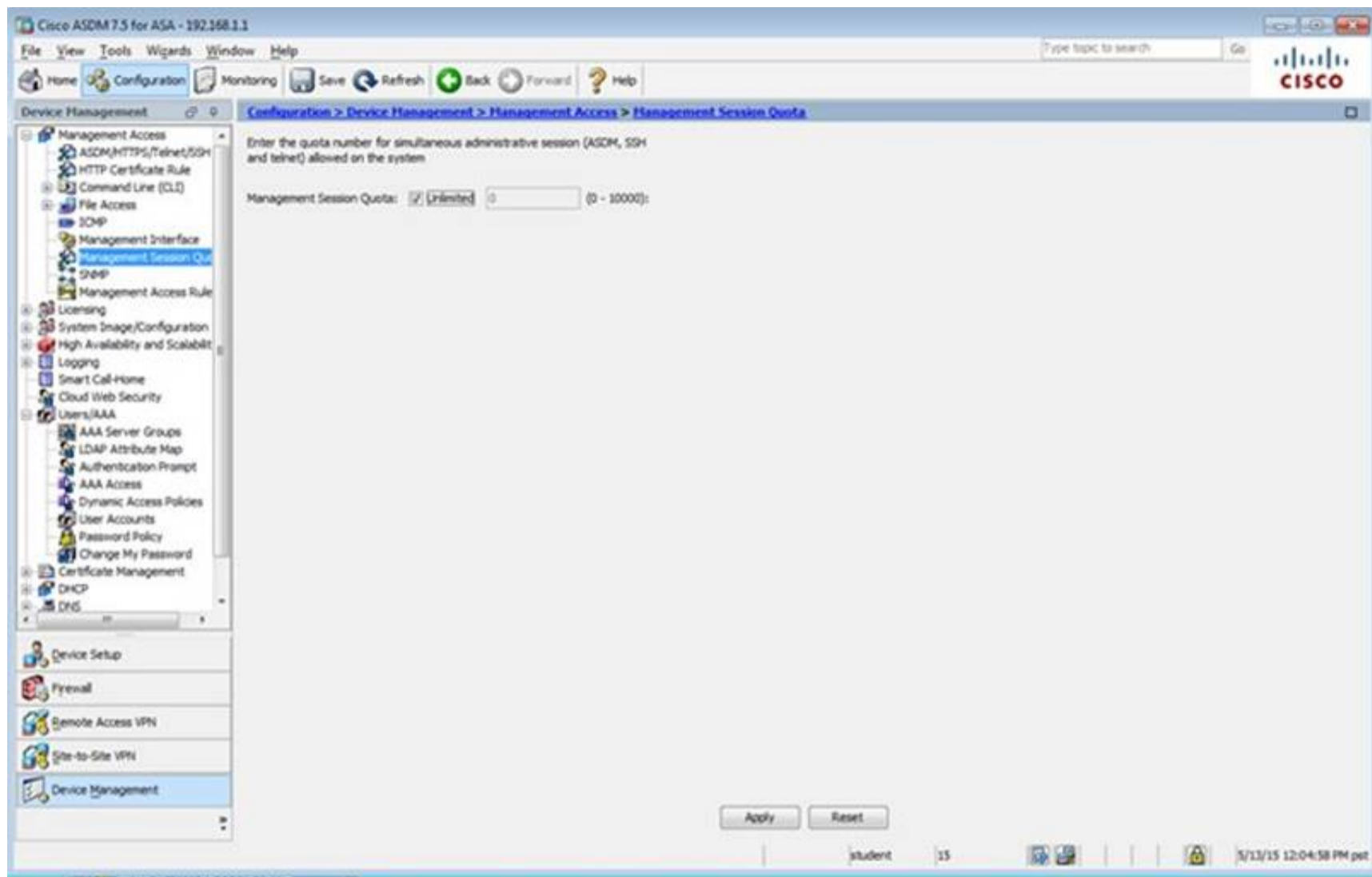
Management Access Interface: --None--

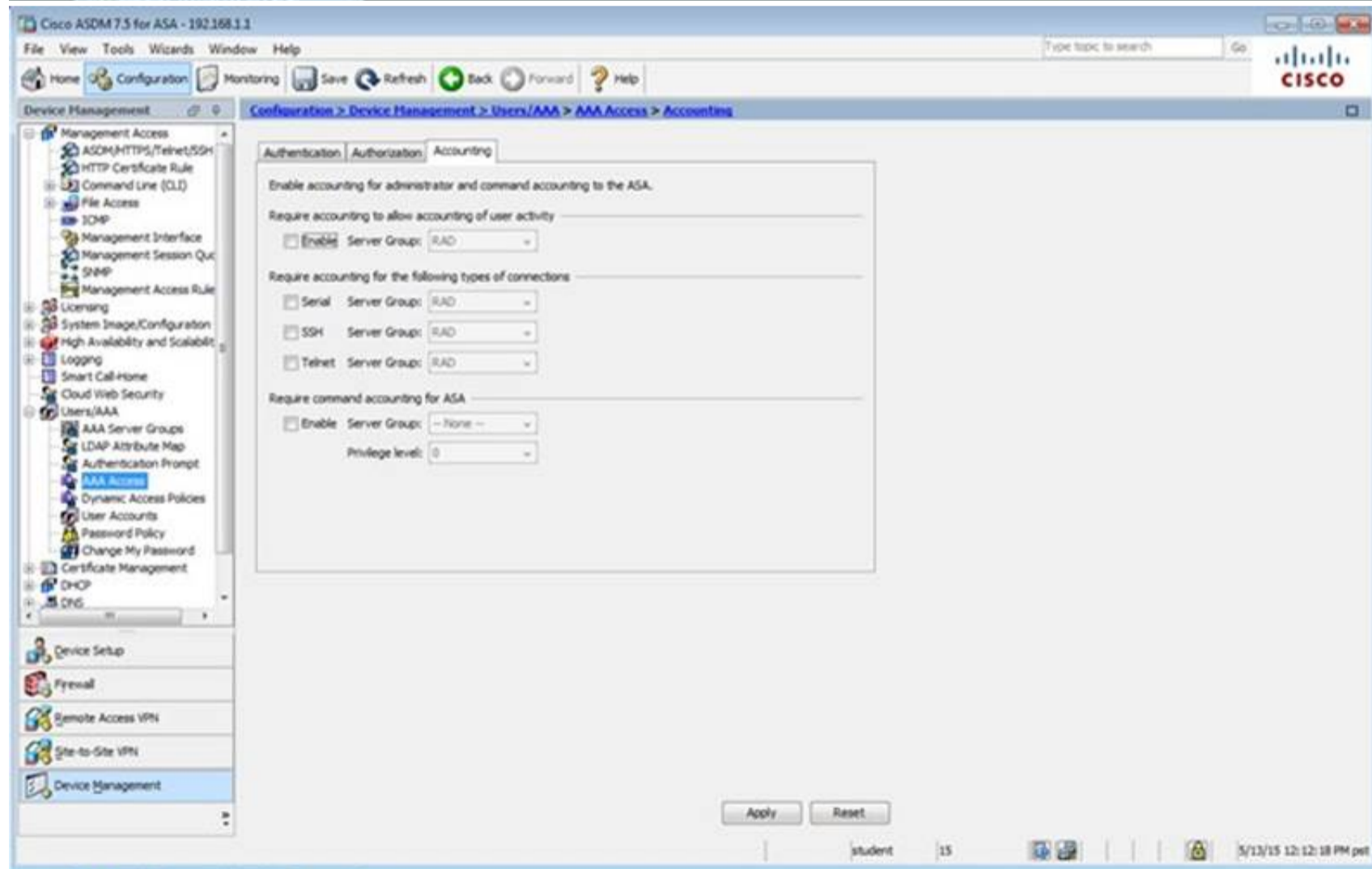
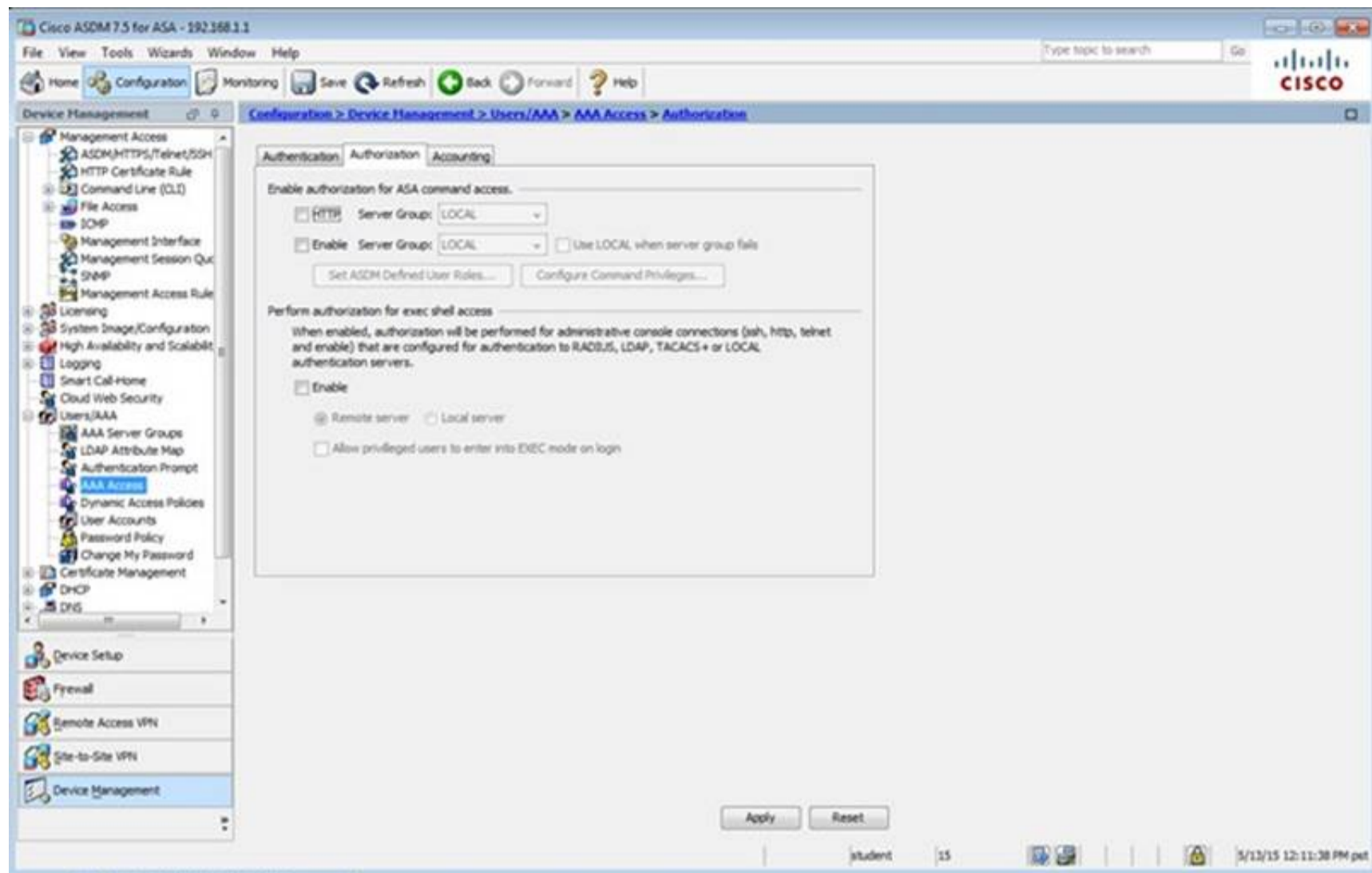
Apply Reset

student 15 5/13/15 12:01:38 PM pet

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Device Management' tree with 'Management Access Rules' selected. The main pane shows the 'Configuration > Device Management > Management Access > Management Access Rules' configuration page. A table with columns for '#', 'Enabled', 'Source Criteria', 'Destination Criteria', 'Service', 'Action', 'Logging', 'Time', and 'Description' is visible. The 'Source Criteria' column is expanded, showing 'Source', 'User', and 'Security Group'. The 'Destination Criteria' column is also expanded, showing 'Security Group' and 'Service'. The 'Action' column is set to 'Deny'. The 'Logging' column is checked. The 'Time' column is set to 'Anytime'. The 'Description' column is empty. The 'Apply' and 'Reset' buttons are at the bottom right. The status bar at the bottom shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Device Management' tree with 'Management Session Quota' selected. The main pane shows the 'Configuration > Device Management > Management Access > Management Session Quota' configuration page. The text 'Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system' is displayed. The 'Management Session Quota' is set to 'Unlimited' (0 - 30000). The 'Apply' and 'Reset' buttons are at the bottom right. The status bar at the bottom shows 'student' and '15'.





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Firewall' section with 'NAT Rules' selected. The main pane shows the 'Configuration > Firewall > NAT Rules' page. A table lists the NAT rules:

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

Buttons for 'Apply' and 'Reset' are visible at the bottom of the main pane. The status bar at the bottom indicates the user is 'student' and the time is '5/13/15 12:13:18 PM pet'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the 'Firewall' section with 'Objects' selected. The main pane shows the 'Configuration > Firewall > Objects' page. It lists the following items:

- Network Objects/Groups
- Service Objects/Groups
- Local Users
- Local User Groups
- Security Group Object Groups
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges

The status bar at the bottom indicates the user is 'student' and the time is '5/13/15 2:15:08 PM pet'.

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > 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 [Configuration > Firewall > Objects > Local Users](#).

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 pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > Objects > Network Objects/Groups

Add Edit Delete Where Used Not Used

Filters:  Filter (Clear)

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

Apply Reset

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

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Service Policy Rules' selected. The main pane shows the 'Configuration > Firewall > Service Policy Rules' page. A table lists the configured rules:

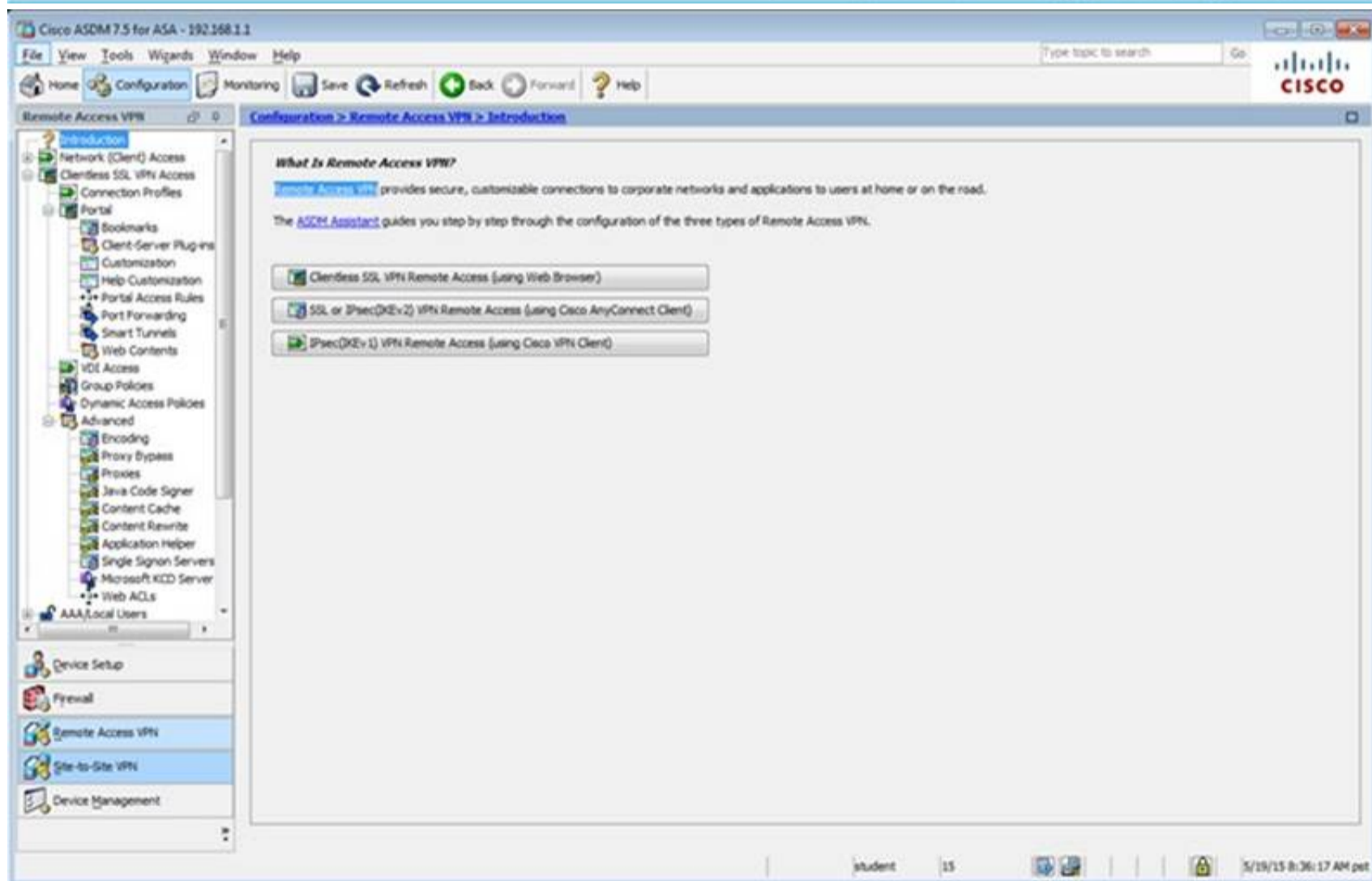
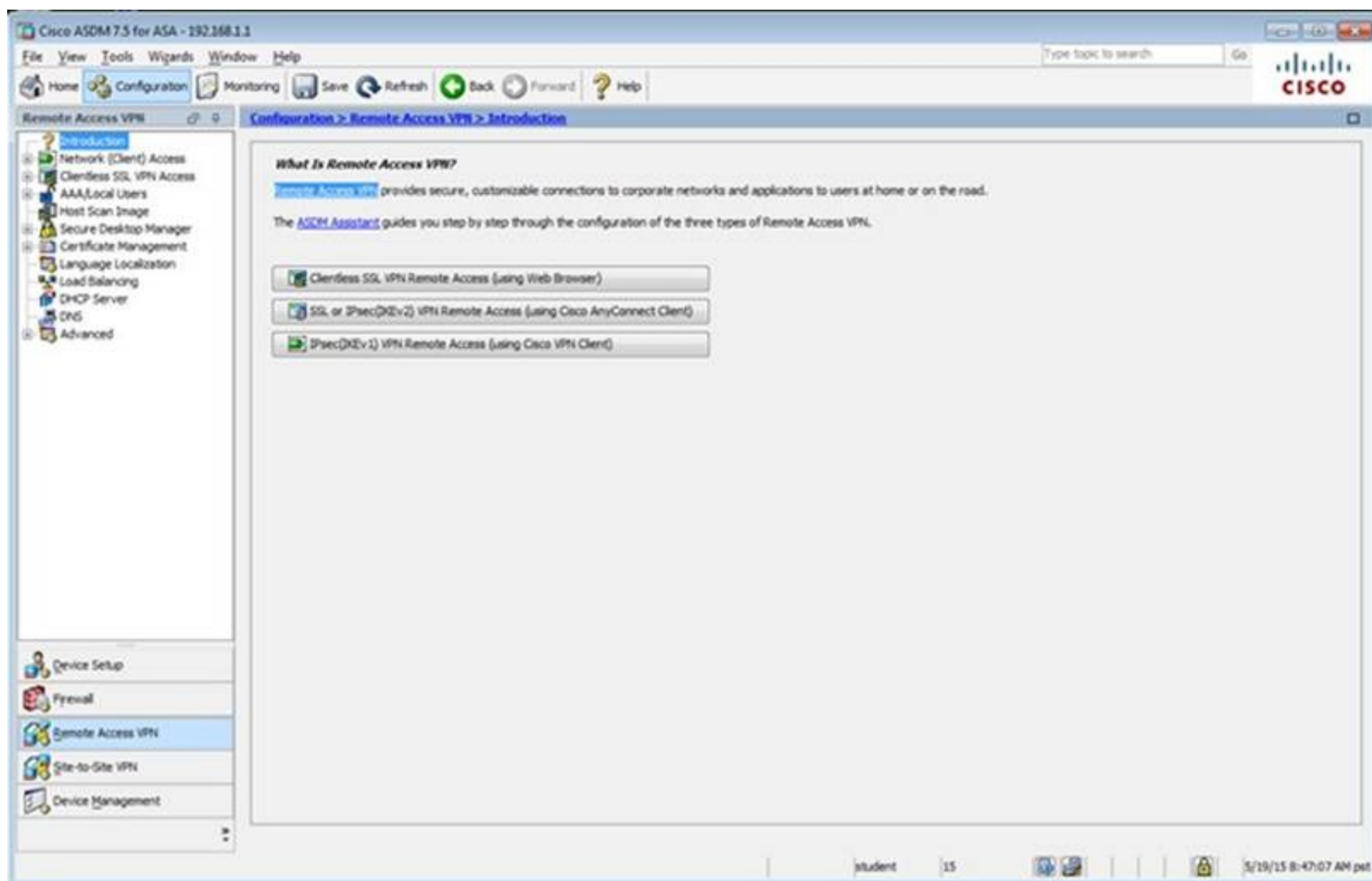
Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time	Rule Actions	Descr
<b>Interface: dmz; Policy: asaif_policy</b>											
class-default			Match	any		any		any traffic		class-default	
<b>Interface: inside; Policy: asaif_policy</b>											
class-default			Match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

Buttons at the bottom include 'Apply' and 'Reset'. The status bar shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Access Rules' selected. The main pane shows the 'Configuration > Firewall > Access Rules' page. A table lists the configured rules:

#	Enabled	Source Criteria:	Destination Criteria:	Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group	
<b>dmz (1 implicit incoming rule)</b>							
1		any			Any less secure ne...		Permit
<b>inside (1 incoming rule)</b>							
1		any			any		Permit 54...
<b>mgmt (0 implicit incoming rules)</b>							
<b>outside (0 implicit incoming rules)</b>							
<b>Global (1 implicit rule)</b>							
1		any			any		Deny

Buttons at the bottom include 'Apply', 'Reset', and 'Advanced...'. The status bar shows 'student' and '15'.



The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane displays the 'Connection Profiles' configuration page under 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles'.

**Access Interfaces**  
Enable interfaces for clientless SSL VPN access.

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

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

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

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

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

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

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

Buttons: Apply, Reset

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

The screenshot shows the 'Edit Clientless SSL VPN Connection Profile: clientless' dialog box. The 'Basic' tab is selected.

**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

Buttons: Find, Next, Previous, OK, Cancel, Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Interface-Specific Authentication Server Groups

+ Add Edit Delete

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

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

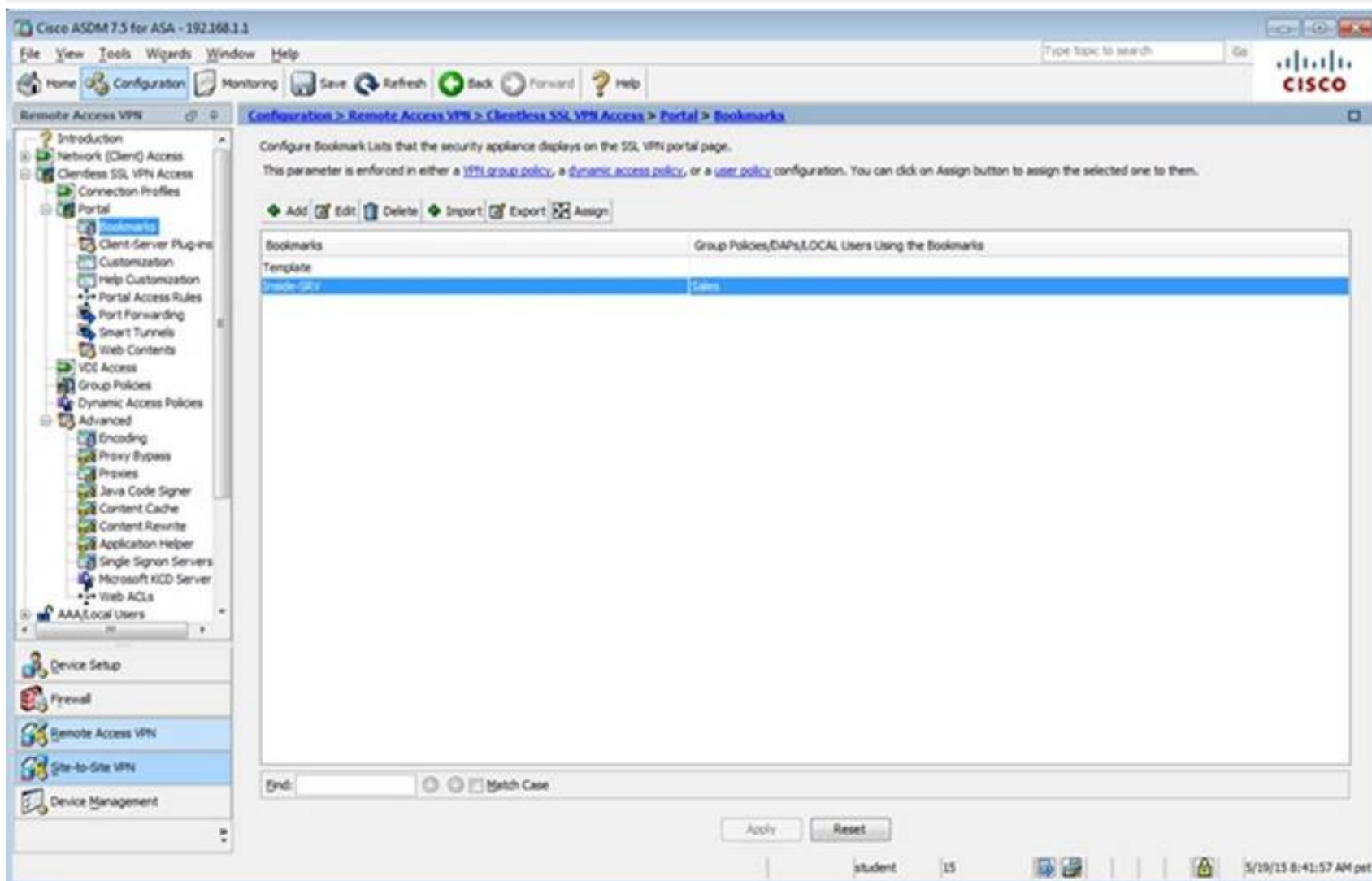
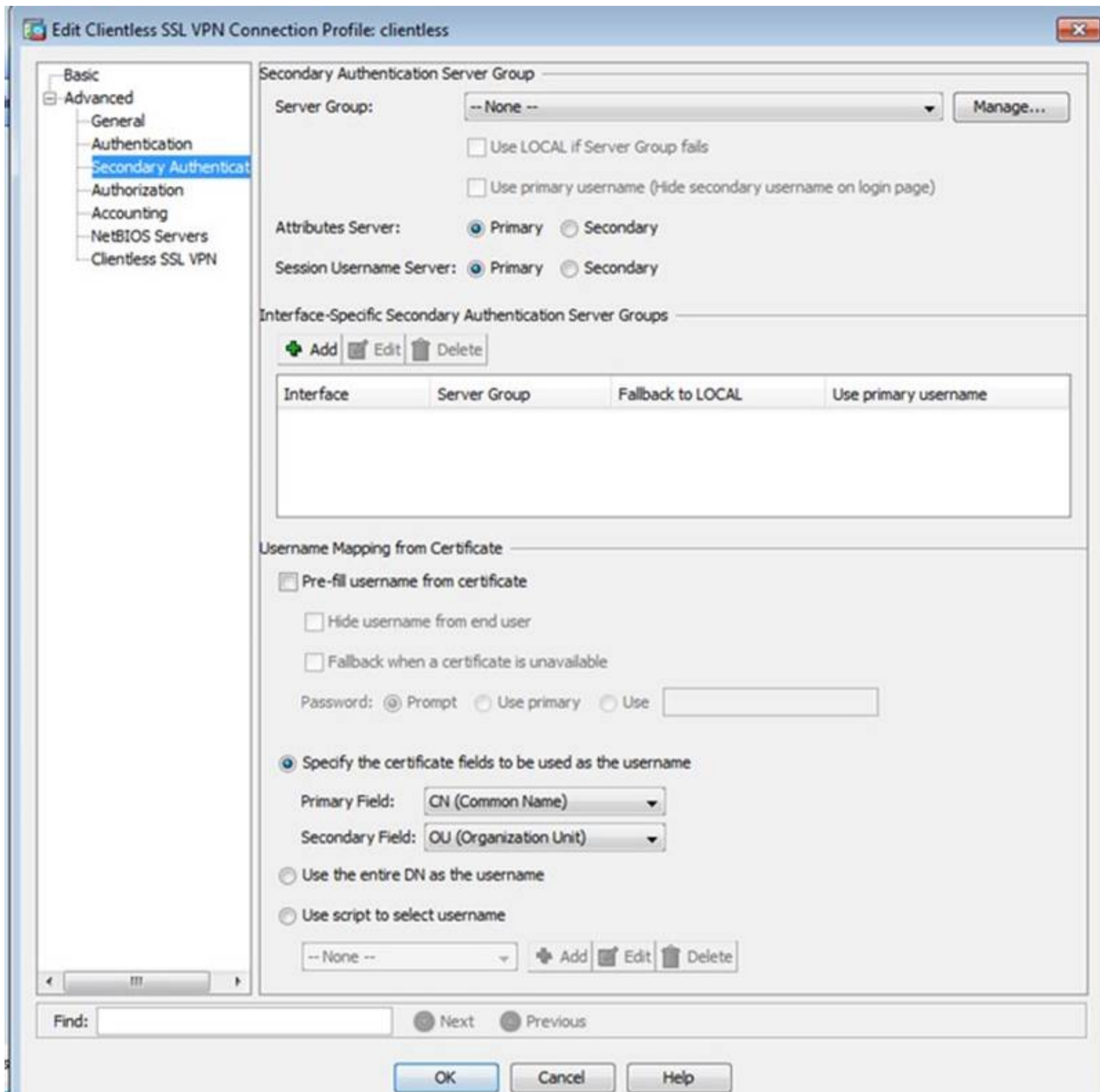
☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



**Edit Bookmark List**

Bookmark List Name: Inside-SRV

Bookmark Title	URL
Inside Server	http://192.168.1.2

Find:       ☐ Match Case

**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 > Smart Tunnels

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

Method to Log Off Smart Tunnel Session

☒ Logoff the smart-tunnel when its parent process, such as a browser, terminates

☐ Click on smart-tunnel logoff icon in the system tray

Smart Tunnel Application List

☐ Match Case

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

Smart Tunnel Auto Sign-on Server List

☐ Match Case

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

Smart Tunnel Networks

☐ Match Case

student 15 5/28/15 8:43:07 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 > 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 pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > 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	ssl-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1;rev 2;ssl-clientless/2p-quest	DefaultRAGroup;Default2;Group;DefaultADMG;Def...

Find: Match Case

Apply Reset

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

**Edit Internal Group Policy: Sales**

Name: Sales

Banner: ☒ Inherit

**More Options**

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

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

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

Find:  ☐ Next ☐ Previous

OK Cancel Help

**Cisco ASDM 7.2 for ASA - 192.168.1.1**

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	Sales
DefaultGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultGrpPolicy

Find:  ☐ Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

General

More Options

Customization

Login Setting

Single Signon

VDI Access

Session Settings

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

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Network: Manage...

Tunnel Option: -- None --

Smart Tunnel Application: ☒ Inherit Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

Advanced

Name: DftGrpPolicy

Banner:

SCEP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

More Options

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

Filter: -- None -- Manage...

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

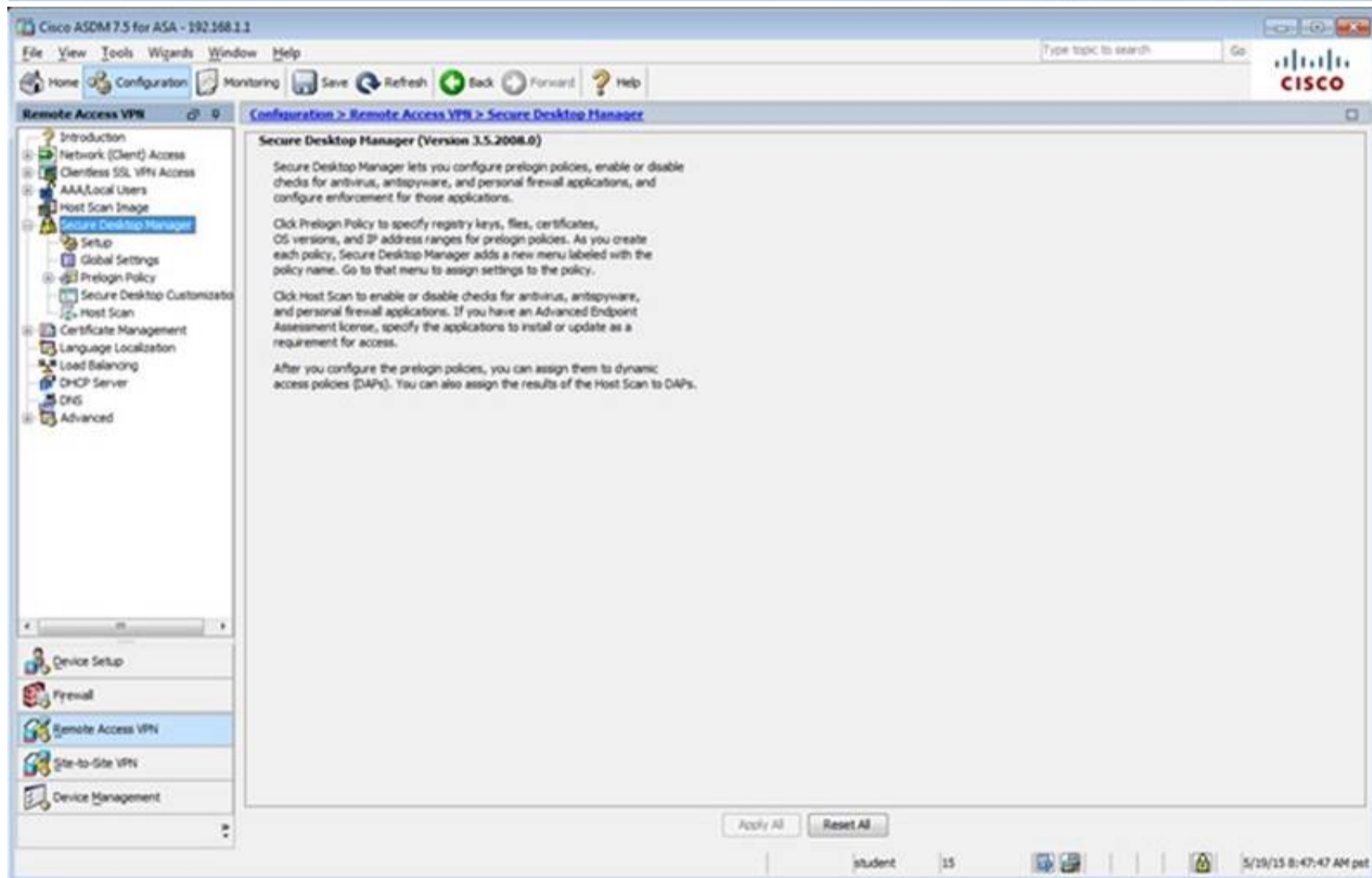
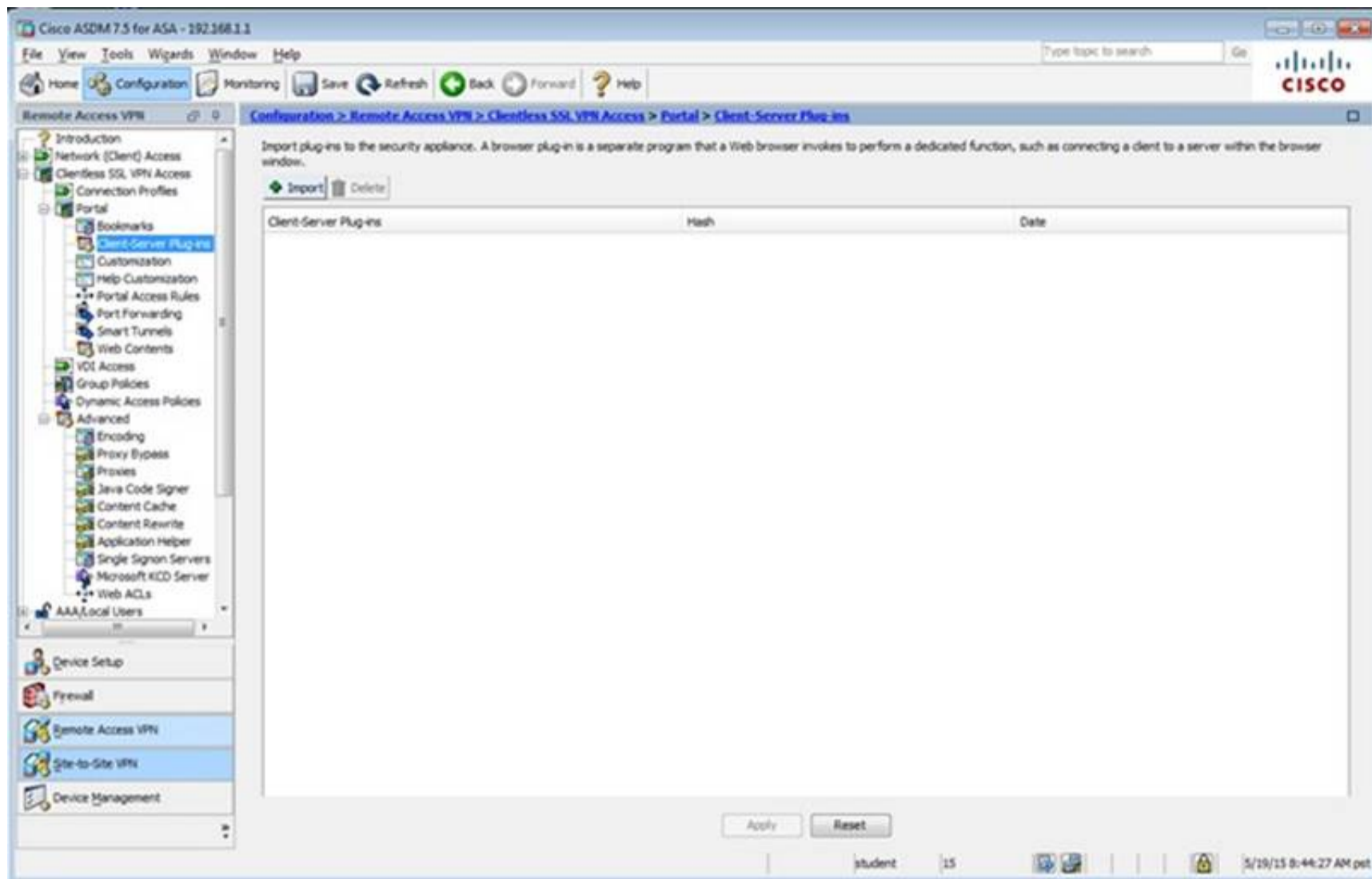
Maximum Connect Time: ☒ Unlimited ☐ minutes

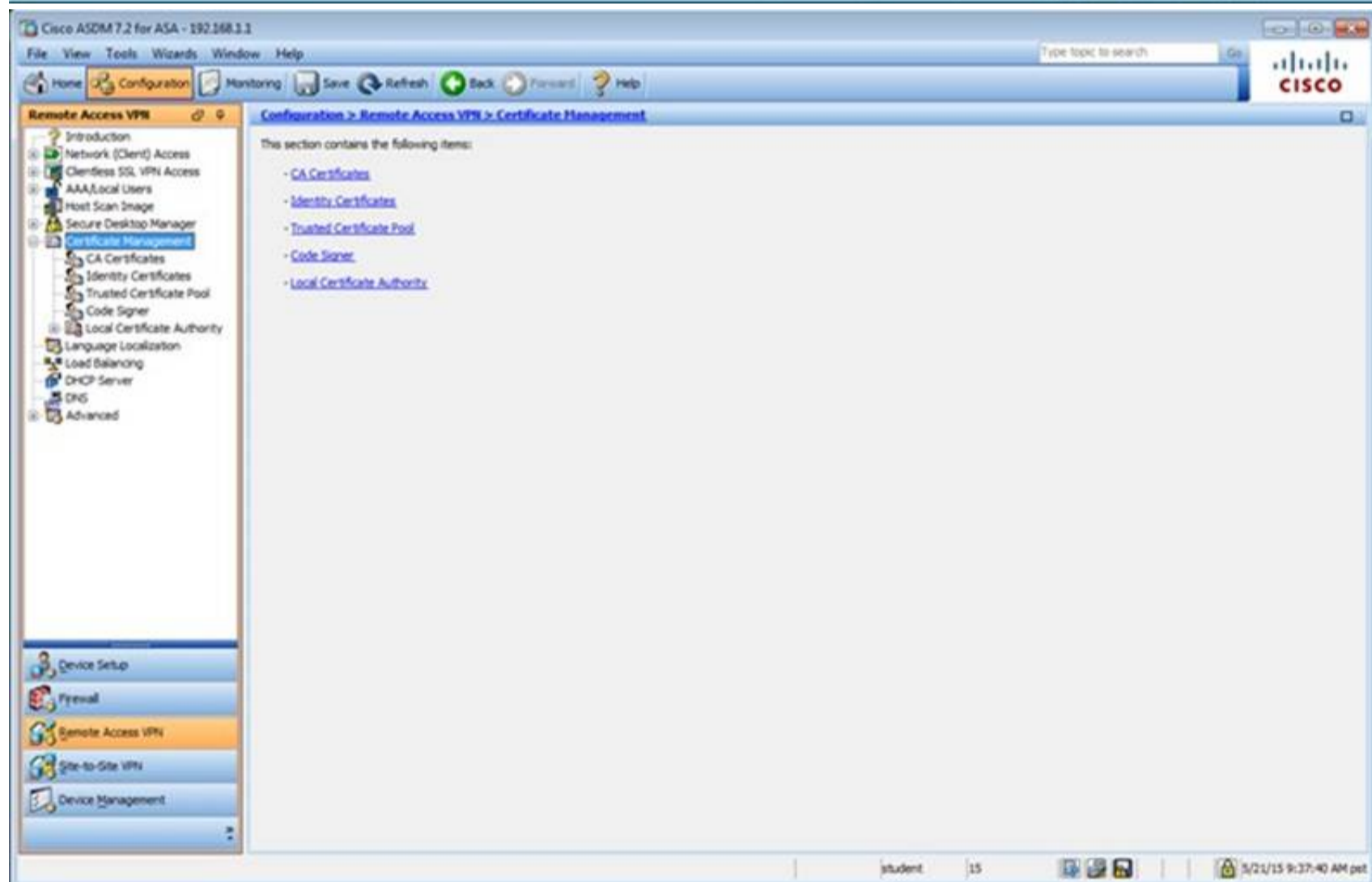
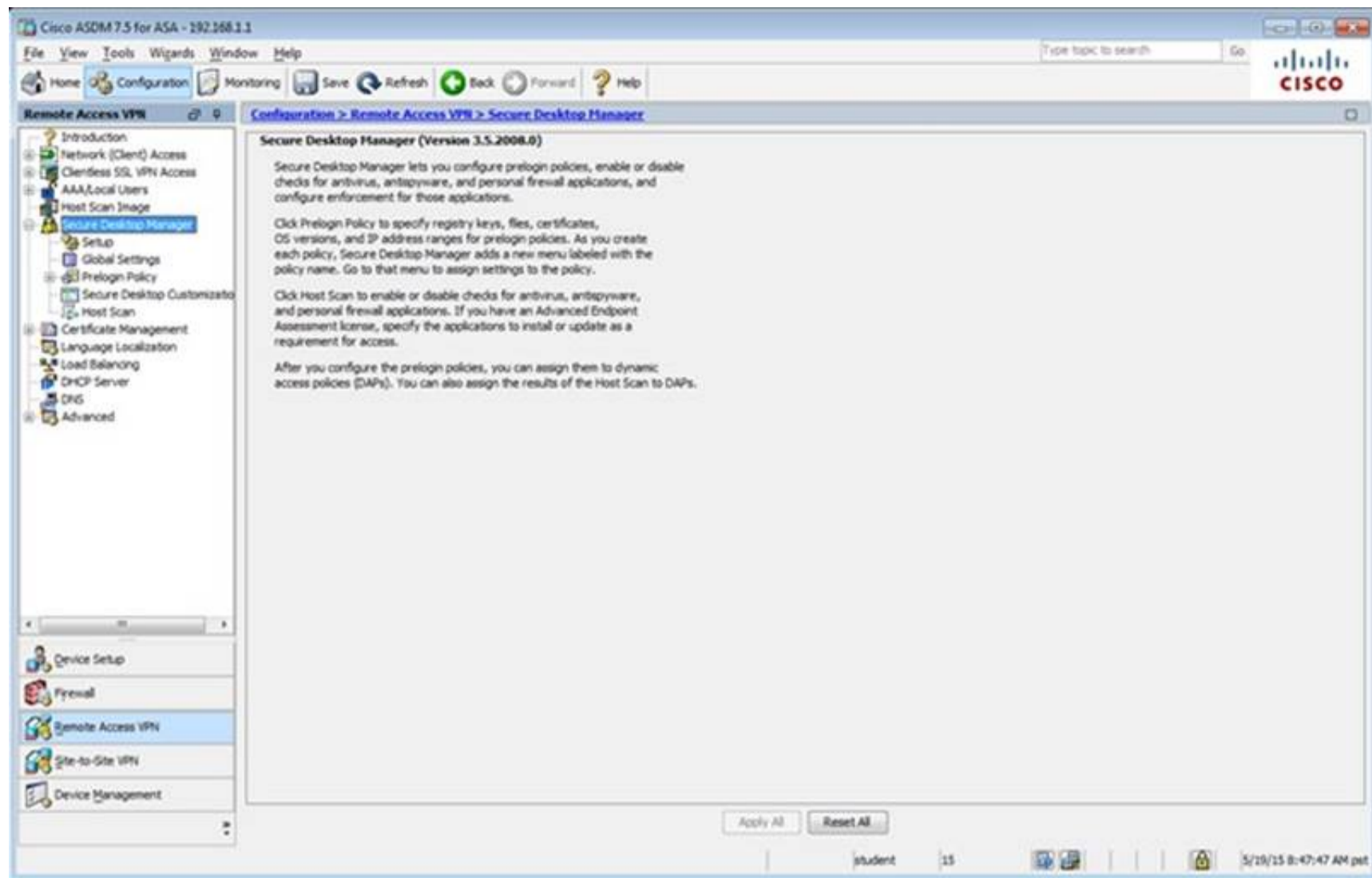
Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find: Next Previous

OK Cancel Help





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane displays the 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates' page. A table lists the following certificate:

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

Below the table, there are sections for 'Certificate Expiration Alerts' (Send the first alert before: 60 days, Repeat Alert Interval: 7 days) and 'Public CA Enrollment' (Enroll ASA SSL certificate with Entrust). At the bottom, there is a section for 'ASDM Identity Certificate Wizard' with a 'Launch ASDM Identity Certificate Wizard' button.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane displays the 'Configuration > Remote Access VPN > Advanced' page. This section contains the following items:

- [Advanced Enrollment](#)
- [SSL Settings](#)
- [Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps](#)
- [HTTP Redirect](#)
- [Maximum VPN Sessions](#)
- [Crypto Engine](#)
- [E-mail Proxy](#)

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Advanced > SSL Settings' page. The page title is 'Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.' The configuration includes dropdowns for 'The minimum SSL version for the security appliance to negotiate as a "server":' (TLS V1), 'The minimum SSL version for the security appliance to negotiate as a "client":' (TLS V1), 'Diffie-Hellman group to be used with SSL:' (Group2 - 2024-bit modulus), and 'ECDH group to be used with SSL:' (Group19 - 256-bit EC). Below these is an 'Encryption' table with columns for 'Cipher Version', 'Cipher Security Level', and 'Cipher Algorithms/ Custom String'. The table lists several cipher suites with 'Medium' security levels. At the bottom, there is a 'Server Name Indication (SNI)' section with a table for 'Domain' and 'Certificate'. The 'Domain' column contains 'dmz' and the 'Certificate' column contains 'ASDM\_TrustPoint1.h...'. There are 'Add', 'Edit', and 'Delete' buttons for this table. At the very bottom, there is a 'Certificates' section with a note: 'Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.'

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions' page. The page title is 'Configure the maximum number of VPN sessions allowed at any given time.' The configuration includes two input fields: 'Maximum AnyConnect Sessions:' (set to 2) and 'Maximum Other VPN Sessions:' (set to 250). At the bottom, there are 'Apply' and 'Reset' buttons. The status bar at the bottom right shows the date and time: '5/19/15 8:54:47 AM pst'.

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

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

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

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

**Important Concepts**

Following are some important concepts for setting up a connection.

**1. SSL tunnel and IPsec tunnel**

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

**2. User and connection profile**

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

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

**3. Access policy**

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

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

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

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

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DefaultGroup (System Default)	Internal	ikev1,ikev2,ssl-clientless,ipsec	DefaultRAGroup,Default,3,Group,DefaultWithVPNGroup

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: DftGrpPolicy

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for IPsec access.

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

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

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

Find: Match Case

Apply Reset

student 15 5/28/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

[Add](#) [Edit](#) [Delete](#) End:  Match Case

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

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

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > AAA/Local Users

This section contains the following items:

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

student 15 5/19/15 8:58:57 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

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

Create entries in the ASA local user database.

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

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

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

End:  Match Case

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

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

AAA Server Groups

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

End:  Match Case

Servers in the Selected Group

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

End:  Match Case

LDAP Attribute Map

Apply Reset

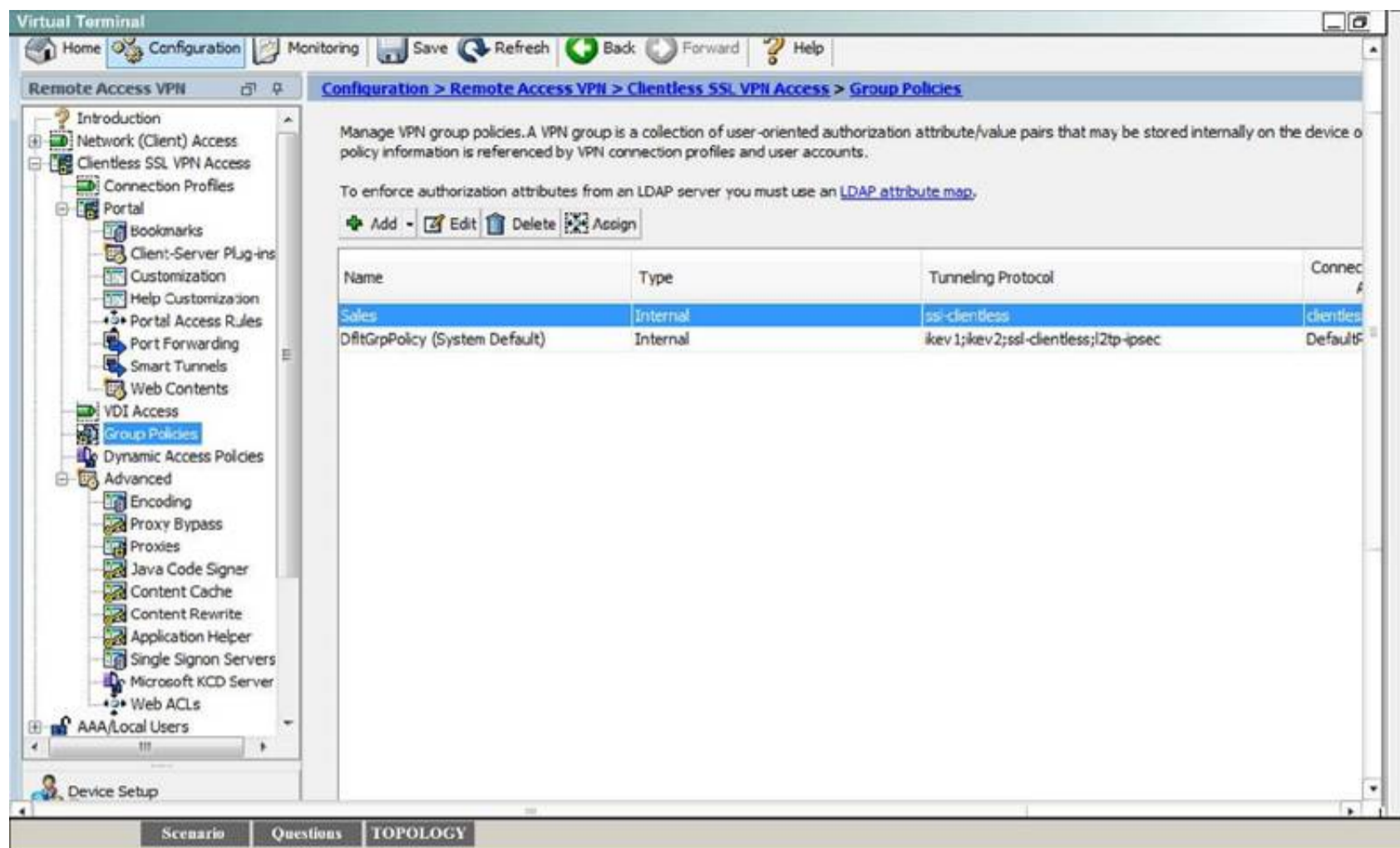
student 15 5/19/15 8:59:57 AM pet

Which for 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:** ADEF

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



#### NEW QUESTION 64

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

**Explanation:** Rate-based attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate requests. Rate-based attacks usually have one of the following characteristics:

- + any traffic containing excessive incomplete connections to hosts on the network, indicating a SYN flood attack
- + any traffic containing excessive complete connections to hosts on the network, indicating a TCP/IP connection flood attack
- + excessive rule matches in traffic going to a particular destination IP address or addresses or coming from a particular source IP address or addresses.
- + excessive matches for a particular rule across all traffic. Preventing SYN Attacks

The SYN attack prevention option helps you protect your network hosts against SYN floods. You can protect individual hosts or whole networks based on the number of packets seen over a period of time. If your device is deployed passively, you can generate events. If your device is placed inline, you can also drop the malicious packets. After the timeout period elapses, if the rate condition has stopped, the event generation and packet dropping stops.

Source:  
<http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Threat-Detection.html>

#### NEW QUESTION 65

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:** BDF

**Explanation:** The ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the "session management path," and depending on the type of traffic, it might also pass through the "control plane path." The session management path is responsible for the following tasks:

- + Performing the access list checks
- + Performing route lookups
- + Allocating NAT translations (xlates)
- + Establishing sessions in the "fast path"

Source:  
<http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/intro.html>

#### NEW QUESTION 69

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

**Explanation:** When ASA needs to authenticate a user to the configured LDAP server, it first tries to login using the login DN provided. After successful login to the LDAP server, ASA sends a search query for the username provided by the VPN user. This search query is created based on the naming attribute provided in the configuration. LDAP replies to the query with the complete DN of the user. At this stage ASA sends a second login attempt to the LDAP server. In this attempt, ASA tries to login to the LDAP server using the VPN user's full DN and password provided by the user. A successful login to the LDAP server will indicate that the credentials provided by the VPN user are correct and the tunnel negotiation will move to the Phase 2.

Source:

<http://www.networkworld.com/article/2228531/cisco-subnet/using-your-active-directory-for-vpn-authentication-on-asa.html>

### NEW QUESTION 73

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

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

**Answer:** AB

**Explanation:** These are the three different types of authentication supported by OSPF + Null Authentication--This is also called Type 0 and it means no authentication information is included in the packet header. It is the default.

+ Plain Text Authentication--This is also called Type 1 and it uses simple clear-text passwords.

+ MD5 Authentication--This is also called Type 2 and it uses MD5 cryptographic passwords.

Source:

<http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25.html>

### NEW QUESTION 74

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

**Explanation:** + Because the transparent firewall does not have any interface IP addresses, you cannot use interface PAT.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf\\_gd/cfgnat.html#wp1102744%0A](http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/cfgnat.html#wp1102744%0A)

### NEW QUESTION 77

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

**Explanation:** Flexible authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAC authentication bypass (MAB), and switch-based web authentication (local WebAuth).

Case 2: Order MABDot1x and Priority Dot1x MAB

If you change the order so that MAB comes before IEEE 802.1X authentication and change the default priority so that IEEE 802.1X authentication precedes MAB, then every device in the network will still be subject to MAB, but devices that pass MAB can subsequently go through IEEE 802.1X authentication.

Special consideration must be paid to what happens if a device fails IEEE 802.1X authentication after successful MAB. First, the device will have temporary network access between the time MAB succeeds and IEEE 802.1X authentication fails. What happens next depends on the configured event-fail behavior.

If next-method is configured and a third authentication method (such as WebAuth) is not enabled, then the switch will return to the first method (MAB) after the held period. MAB will succeed, and the device will again have temporary access until and unless the supplicant tries to authenticate again.

If next-method failure handling and local WebAuth are both configured after IEEE 802.1X authentication fails, local WebAuth ignores EAPoL-Start commands from the supplicant.

MAB -->MAB Pass--> Port Authorized by MAB --> EAPoL-Start Received --> IEEE 802.1x MAB -->MABFail--> IEEE 802.1x

(config-if)#authentication order mab dot1x (config-if)#authentication priority dot1x mab Source:

[http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application\\_note\\_c27-573287.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html)

#### NEW QUESTION 80

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

**Explanation:** Source:

<http://www.techrepublic.com/article/four-steps-to-keeping-current-with-antivirus-signature-updates/>

#### NEW QUESTION 82

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

**Explanation:** Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

Software can use a Trusted Platform Module to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.

Source: [https://en.wikipedia.org/wiki/Trusted\\_Platform\\_Module#Disk\\_encryption](https://en.wikipedia.org/wiki/Trusted_Platform_Module#Disk_encryption)

#### NEW QUESTION 85

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

**Explanation:** + Block or alert the user about all unauthorized inbound or outbound connection attempts + Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt + Hide the computer from port scans by not responding to unsolicited network traffic + Monitor applications that are listening for incoming connections + Monitor and regulate all incoming and outgoing Internet users + Prevent unwanted network traffic from locally installed applications + Provide information about the destination server with which an application is attempting to communicate + Track recent incoming events, outgoing events, and intrusion events to see who has accessed or tried to access your computer.

+ Personal Firewall blocks and prevents hacking attempt or attack from hackers Source: [https://en.wikipedia.org/wiki/Personal\\_firewall](https://en.wikipedia.org/wiki/Personal_firewall)

#### NEW QUESTION 89

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

**Explanation:** ACS can join one AD domain. If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which ACS is connected and the other domains that have user and machine information to which you need access. So B is not correct.

Source:

[http://www.cisco.com/c/en/us/td/docs/net\\_mgmt/cisco\\_secure\\_access\\_control\\_system/5-8/ACS-](http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-8/ACS-ADIntegration/guide/Active_Directory_Integration_in_ACS_5-8.pdf)

[ADIntegration/guide/Active\\_Directory\\_Integration\\_in\\_ACS\\_5-8.pdf](http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-8/ACS-ADIntegration/guide/Active_Directory_Integration_in_ACS_5-8.pdf) + You can define multiple authorization profiles as a network access policy result. In this way, you maintain a smaller number of authorization profiles, because you can use the authorization profiles in combination as rule results, rather than maintaining all the combinations themselves in individual profiles. So D. is not correct + ACS 5.1 can function both as a RADIUS and RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards the requests to the external RADIUS server. So C. is nor correct.

Source:

[http://www.cisco.com/c/en/us/td/docs/net\\_mgmt/cisco\\_secure\\_access\\_control\\_system/5-1/user/guide/acsuserguide/policy\\_mod.html](http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/acsuserguide/policy_mod.html)

#### NEW QUESTION 90

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

**Explanation:** The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions . OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide.  
Source: [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)

#### NEW QUESTION 93

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

**Explanation:** CDP contains information about the network device, such as the software version, IP address, platform, capabilities, and the native VLAN. When this information is available to an attacker computer, the attacker from that computer can use it to find exploits to attack your network, usually in the form of a Denial of Service (DoS) attack.

Source: <https://howdoesinternetwork.com/2011/cdp-attack>

#### NEW QUESTION 94

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:** AE

**Explanation:** The ASA allows Telnet and SSH connections to the ASA for management purposes. You cannot use Telnet to the lowest security interface unless you use Telnet inside an IPSec tunnel.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access\\_management.html#wp1054101](http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_management.html#wp1054101)

#### NEW QUESTION 95

Which protocol provides security to Secure Copy?

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

**Answer:** B

**Explanation:** The SCP is a network protocol, based on the BSD RCP protocol,[3] which supports file transfers between hosts on a network. SCP uses Secure Shell (SSH) for data transfer and uses the same mechanisms for authentication, thereby ensuring the authenticity and confidentiality of the data in transit.

Source: [https://en.wikipedia.org/wiki/Secure\\_copy](https://en.wikipedia.org/wiki/Secure_copy)

#### NEW QUESTION 97

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

**Explanation:** The local database must be referenced in all capital letters when AAA is in use. If lower case letters are used, the ASA will look for an AAA server group called "local".

#### NEW QUESTION 99

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

**Explanation:** Phishing presents a link that looks like a valid trusted resource to a user. When the user clicks it, the user is prompted to disclose confidential information such as usernames/passwords.

Source: Cisco Official Certification Guide, Table 1-5 Attack Methods, p.13

#### NEW QUESTION 104

Which two features are commonly used by CoPP and CPPr to protect the control plane?

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

**Answer:** AB

**Explanation:** For example, you can specify that management traffic, such as SSH/HTTPS/SSL and so on, can be ratelimited (policed) down to a specific level or dropped completely.

Another way to think of this is as applying quality of service (QoS) to the valid management traffic and policing to the bogus management traffic.

Source: Cisco Official Certification Guide, Table 10-3 Three Ways to Secure the Control Plane, p.269

#### NEW QUESTION 105

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:** AC

**Explanation:** 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 } + stop-only: Sends a stop accounting record for all cases including authentication failures

regardless of whether the aaa accounting send stop-record authentication failure command is configured. + stop-record: Generates stop records for a specified event.

For minimal accounting, include the stop-only keyword to send a "stop" accounting record for all cases including authentication failures. For more accounting, you can include the start-stop keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

Source:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html>

#### NEW QUESTION 109

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:** AF

**Explanation:** The Suite B next-generation encryption (NGE) includes algorithms for authenticated encryption, digital signatures, key establishment, and cryptographic hashing, as listed here:

+ Elliptic Curve Cryptography (ECC) replaces RSA signatures with the ECDSA algorithm + AES in the Galois/Counter Mode (GCM) of operation

+ ECCDigital Signature Algorithm

+ SHA-256, SHA-384, and SHA-512

Source: Cisco Official Certification Guide, Next-Generation Encryption Protocols, p.97

#### NEW QUESTION 112

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

**Explanation:** Slash Netmask Wildcard Mask  
/27 255.255.255.224 0.0.0.31  
Further reading  
Source: [https://en.wikipedia.org/wiki/Wildcard\\_mask](https://en.wikipedia.org/wiki/Wildcard_mask)

#### NEW QUESTION 113

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

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

**Answer:** A

**Explanation:** Denial-of-service (DoS) attack and distributed denial-of-service (DDoS) attack. An example is using a botnet to attack a target system.  
Source: Cisco Official Certification Guide, Table 1-6 Additional Attack Methods, p.16

#### NEW QUESTION 117

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

**Explanation:** A symmetric encryption algorithm, also known as a symmetrical cipher, uses the same key to encrypt the data and decrypt the data.  
Source: Cisco Official Certification Guide, p.93

#### NEW QUESTION 122

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

**Explanation:** A zone is a logical area where devices with similar trust levels reside. For example, we could define a DMZ for devices in the DMZ in an organization. A zone is created by the administrator, and then interfaces can be assigned to zones. A zone can have one or more interfaces assigned to it. Any given interface can belong to only a single zone. There is a default zone, called the self zone, which is a logical zone.  
Source: Cisco Official Certification Guide, Zones and Why We Need Pairs of Them, p.380

#### NEW QUESTION 125

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

**Explanation:** You can partition a single ASA into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices.

Common Uses for Security Contexts

- + You are a service provider and want to sell security services to many customers. By enabling multiple security contexts on the ASA, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
- + You are a large enterprise or a college campus and want to keep departments completely separate.
- + You are an enterprise that wants to provide distinct security policies to different departments.
- + You have any network that requires more than one ASA.

Source:  
[http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\\_84\\_cli\\_config/mode\\_contexts.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/mode_contexts.html)

#### NEW QUESTION 129

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:** ABC

#### NEW QUESTION 132

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:** BC

**Explanation:** In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message.  
 Source: [https://en.wikipedia.org/wiki/Hash-based\\_message\\_authentication\\_code](https://en.wikipedia.org/wiki/Hash-based_message_authentication_code)

#### NEW QUESTION 136

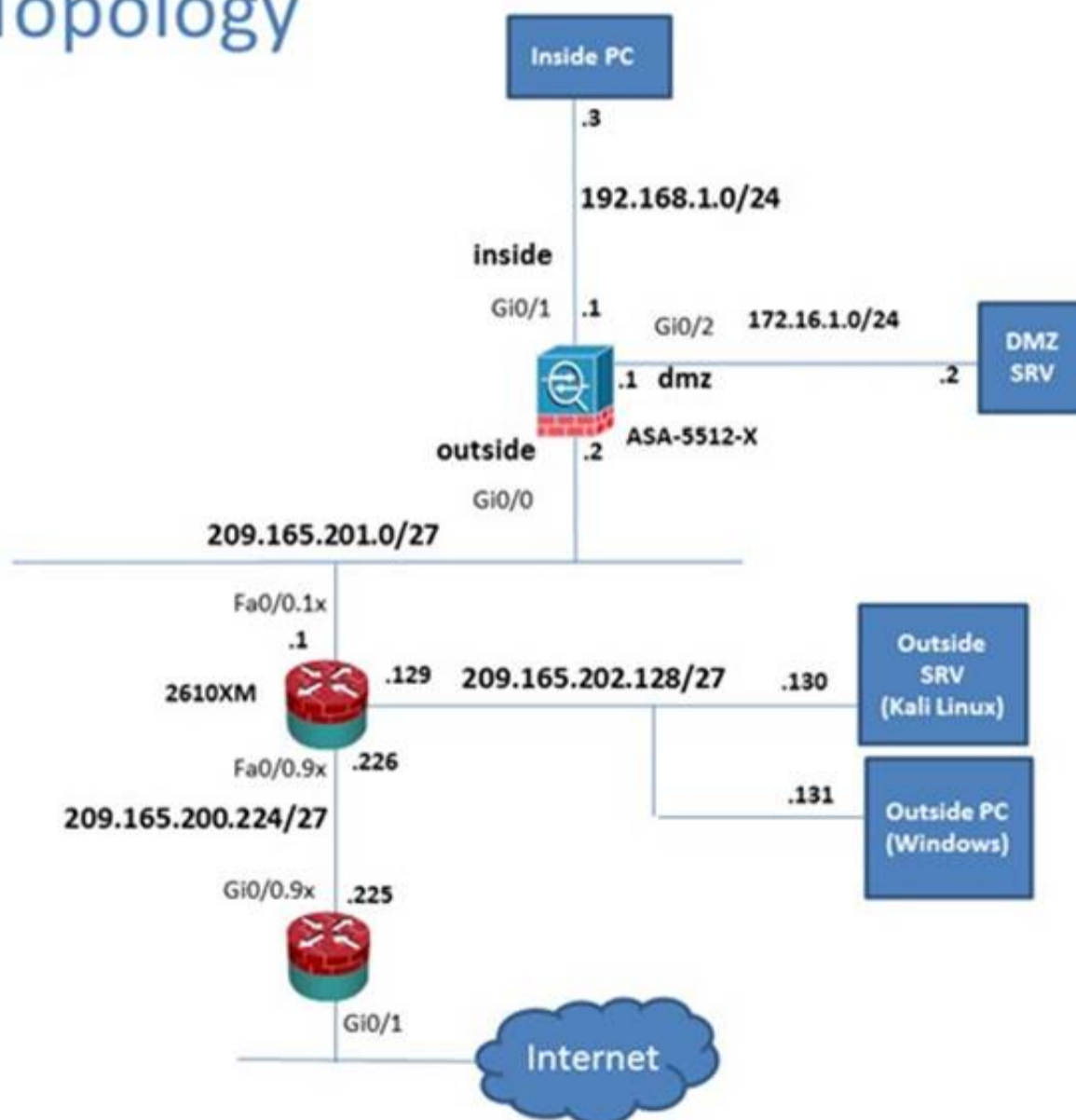
Scenario

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

To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities are enabled in this simulation.

To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

## Lab Topology



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA FirePOWER Status

Device Information

General License

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

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Clients: 0 Details

System Resources Status

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

12:05:18

12:31 12:32 12:33 12:34 12:35

1500 1000 500 0

12:31 12:32 12:33 12:34 12:35

Connections Per Second Usage

12:31 12:32 12:33 12:34 12:35

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

12:31 12:32 12:33 12:34 12:35

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Monitoring > Interfaces > ARP Table

Interfaces

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

Interfaces

- VPN
- Botnet Traffic Filter
- Routing
- Properties
- Logging

ARP Table

Each row represents one ARP table entry.

Interface	IP Address	MAC Address	Proxy Arp
outside	209.165.201.1	000c.3014.3820	No
inside	192.168.1.4	0050.5633.3333	No
inside	192.168.1.3	0050.5611.1111	No
inside	192.168.1.2	0050.5622.2222	No
inside	192.168.1.56	0050.5692.5c7b	No
inside	192.168.1.55	0006.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

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

Data Refreshed Successfully.

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

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

Interfaces  
 VPN  
 Internet Traffic Filter  
 Routing  
 Properties  
 Logging

Monitors > VPN > VPN Statistics > Sessions

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

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

Username	SP Address	Group Policy	Connection Profile	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
student	209.18.15.202.131	Sales	Clientless	Clientless	Clientless (CBC4)	06:05:46 pet Thu May 21 2015	0h:09m:19s	1187794	41633

Details  
 Logout  
 Ping

Refresh

Last Updated: 5/20/15 9:33:12 AM

Data Refreshed Successfully.

student 15 5/20/15 8:33:37 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Startup Wizard  
 Interface Settings  
 Routing  
 Device Name/Password  
 System Time

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

Configuration > Device Setup > Startup Wizard

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

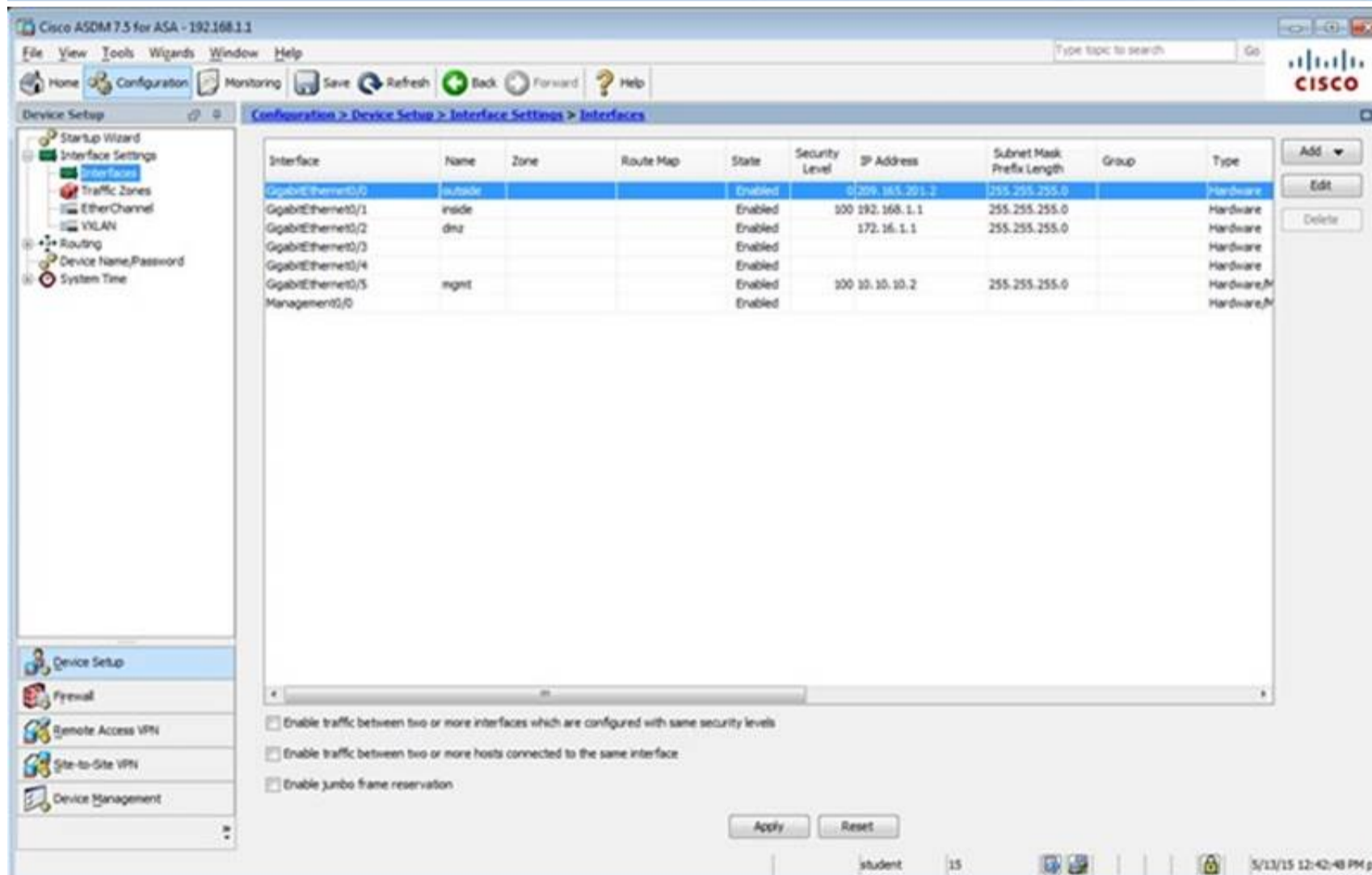
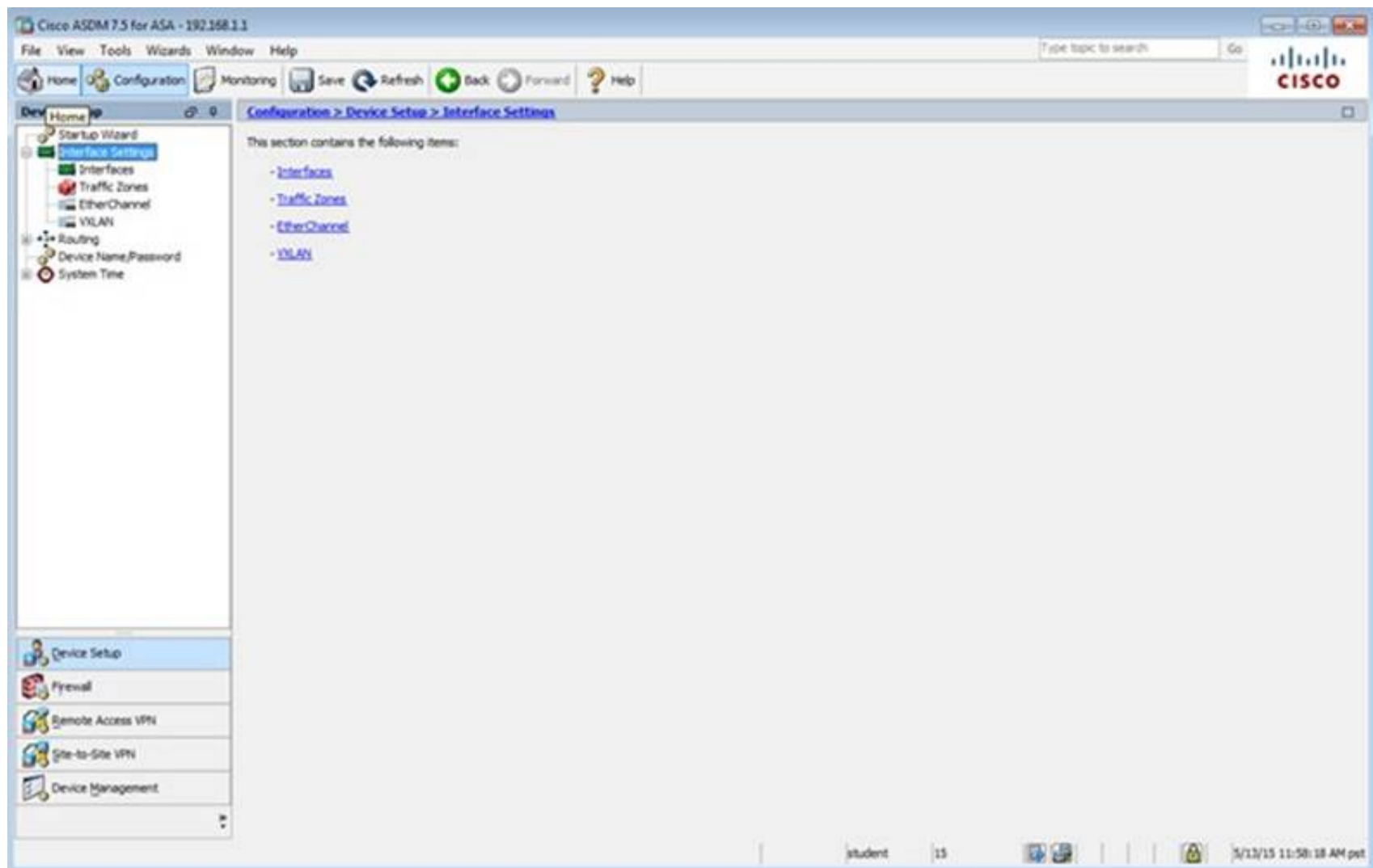
**Startup Wizard**

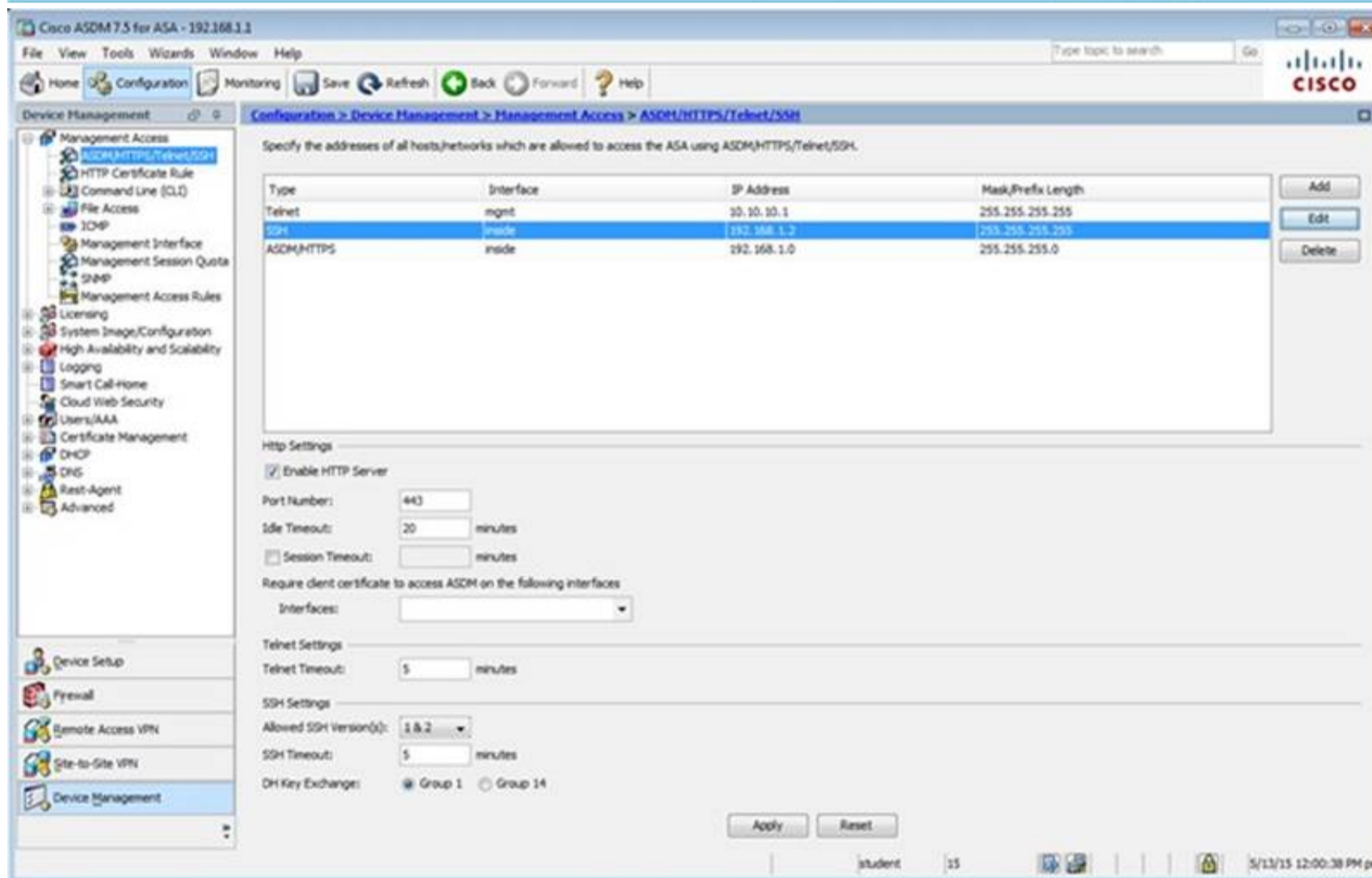
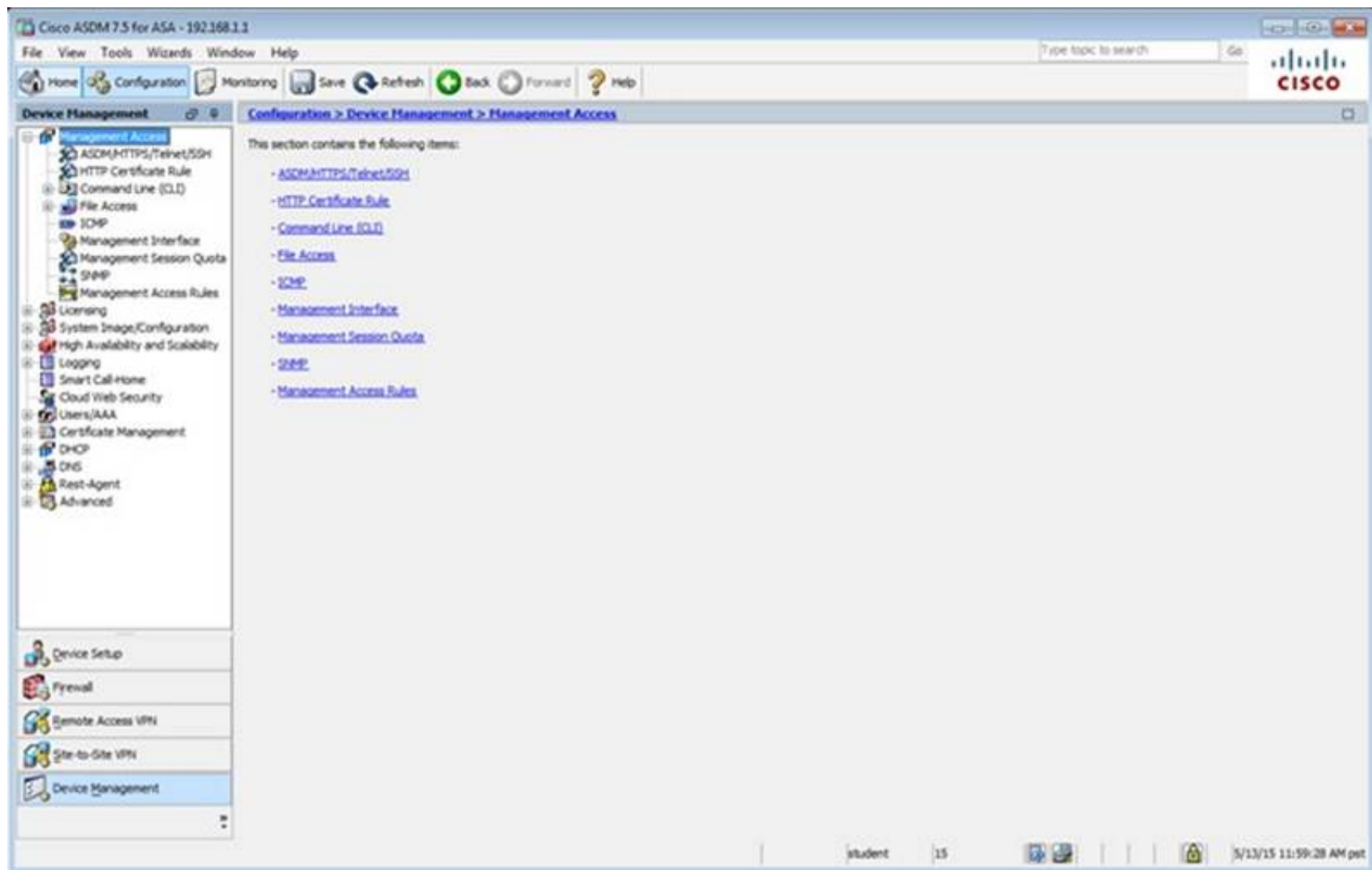
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

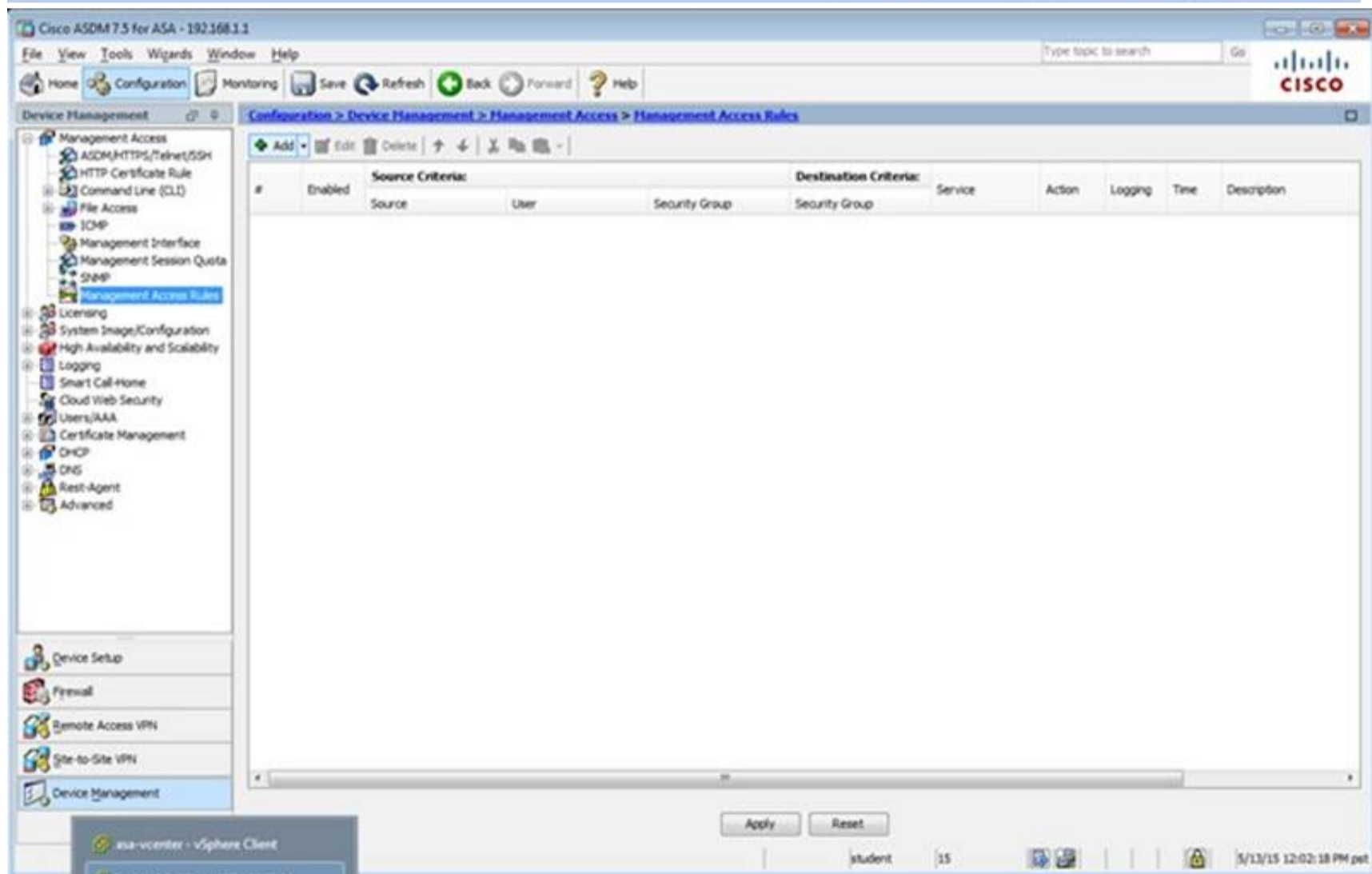
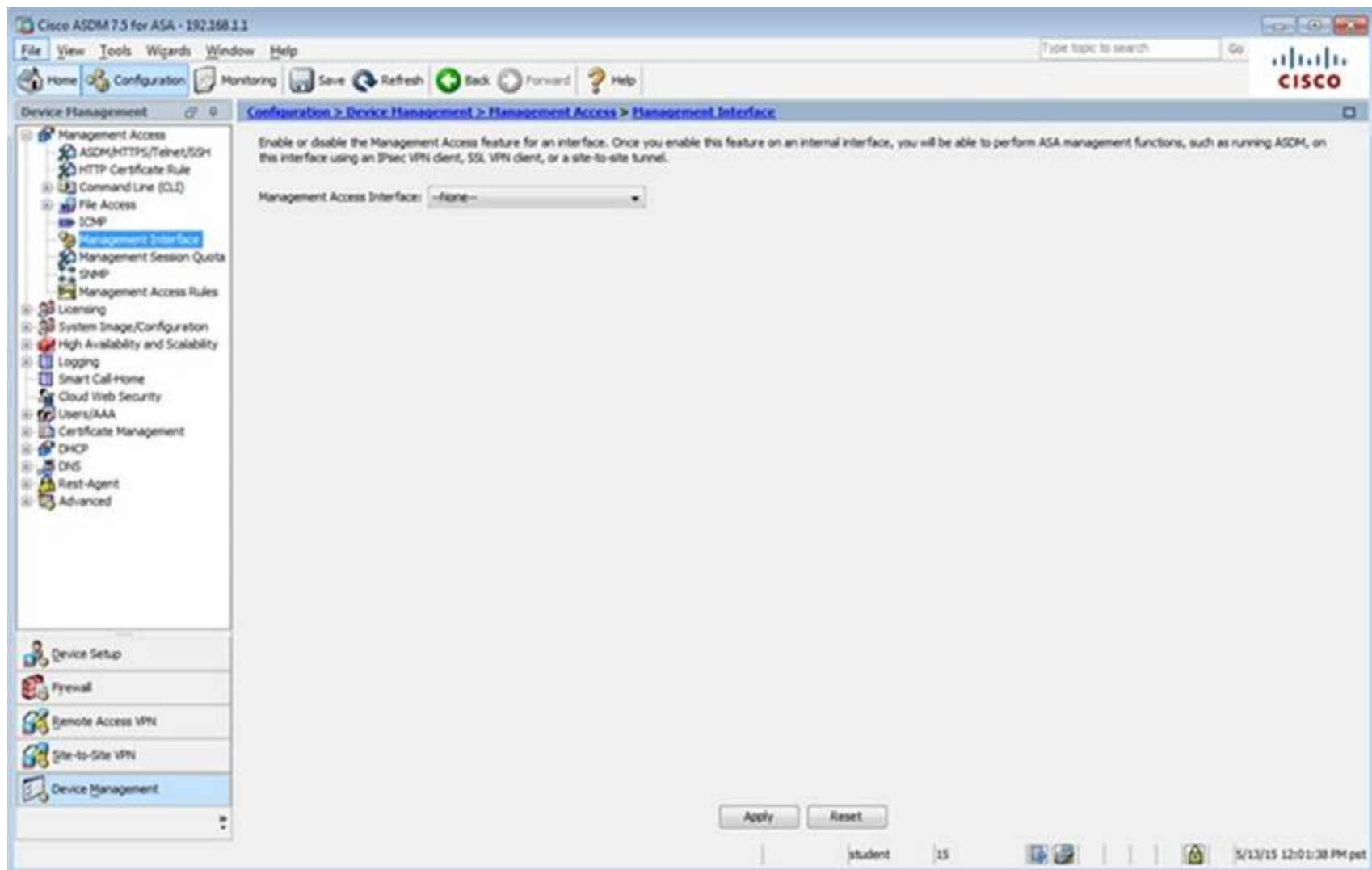
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

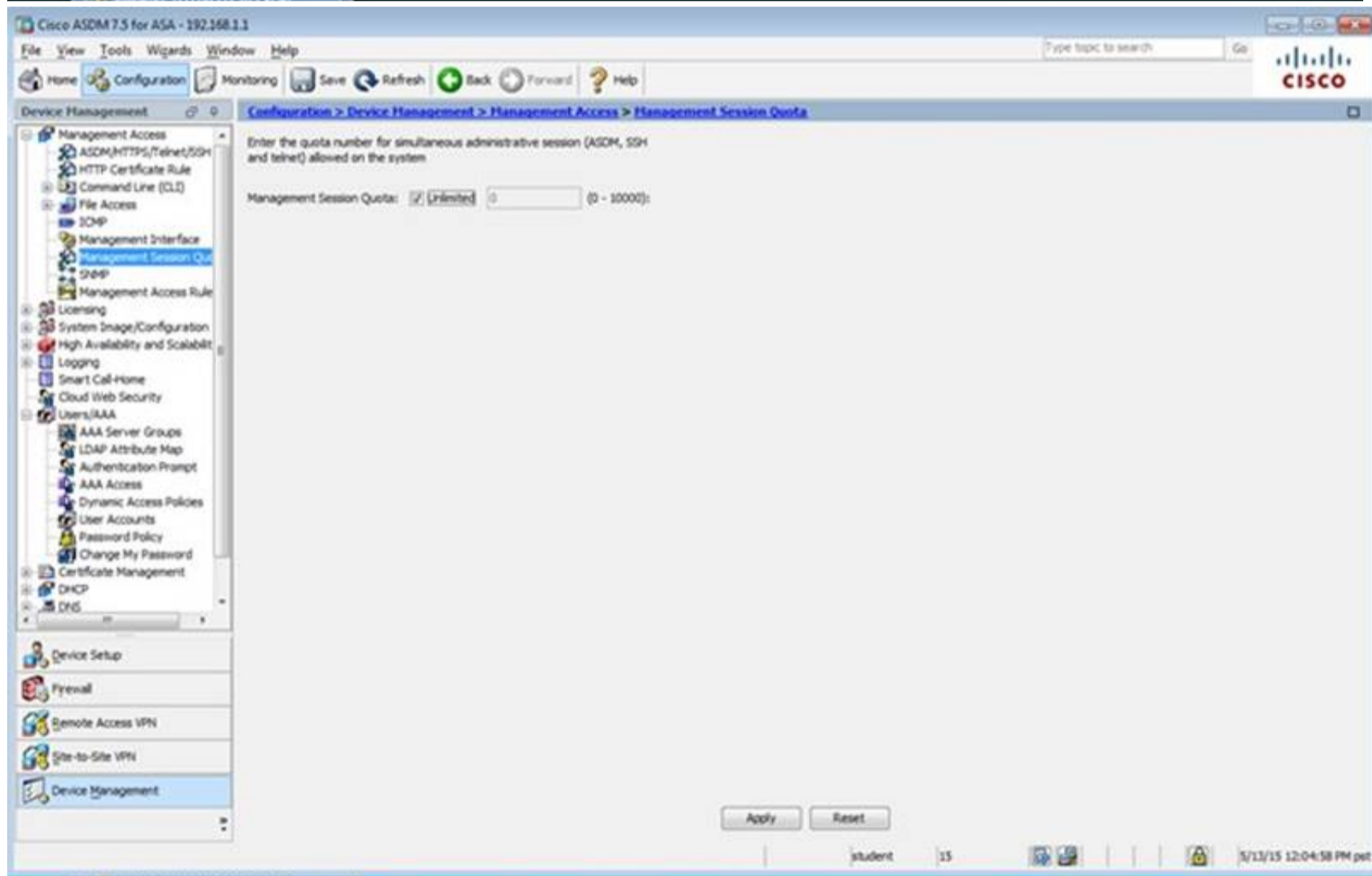
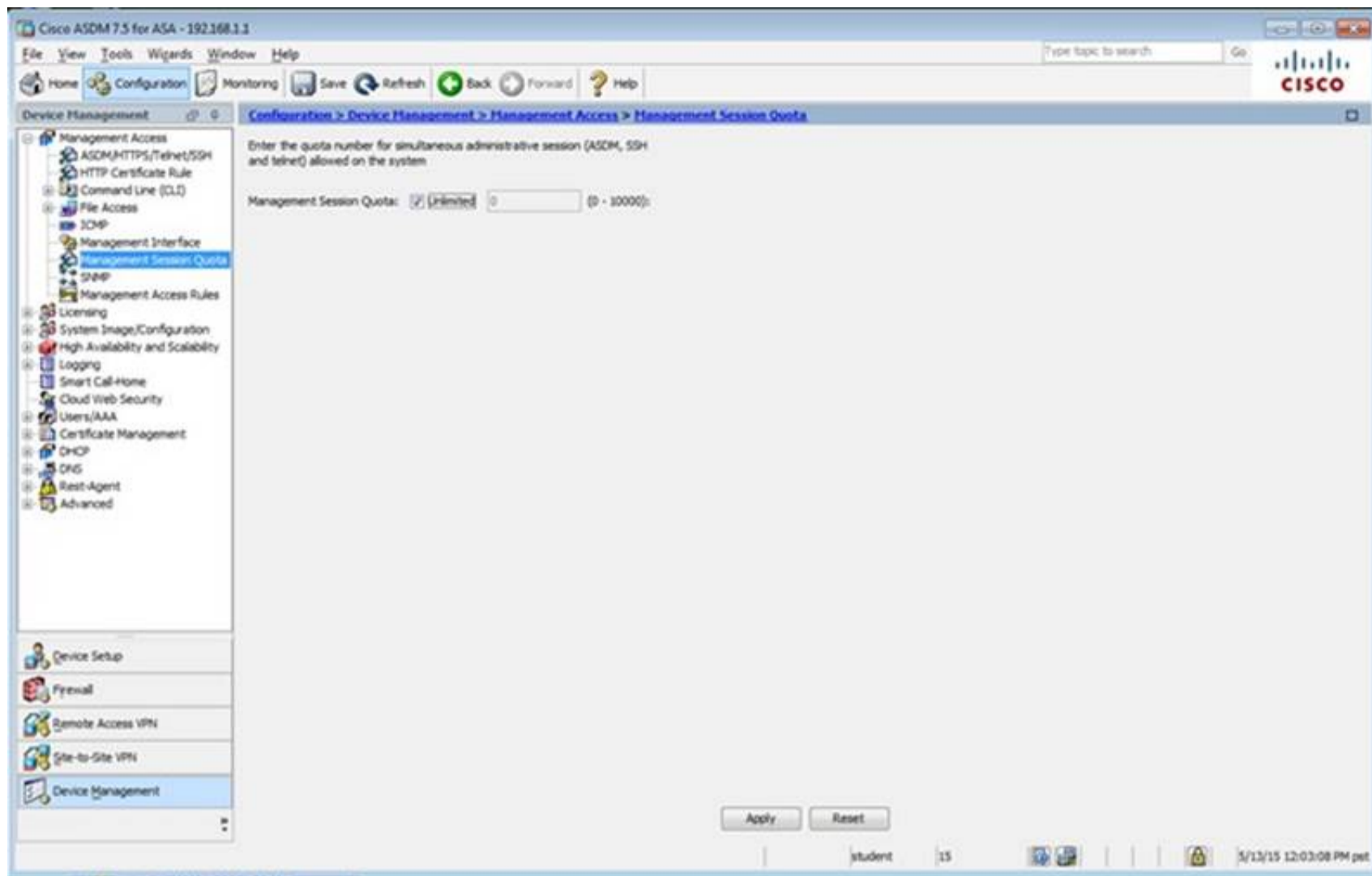
Launch Startup Wizard

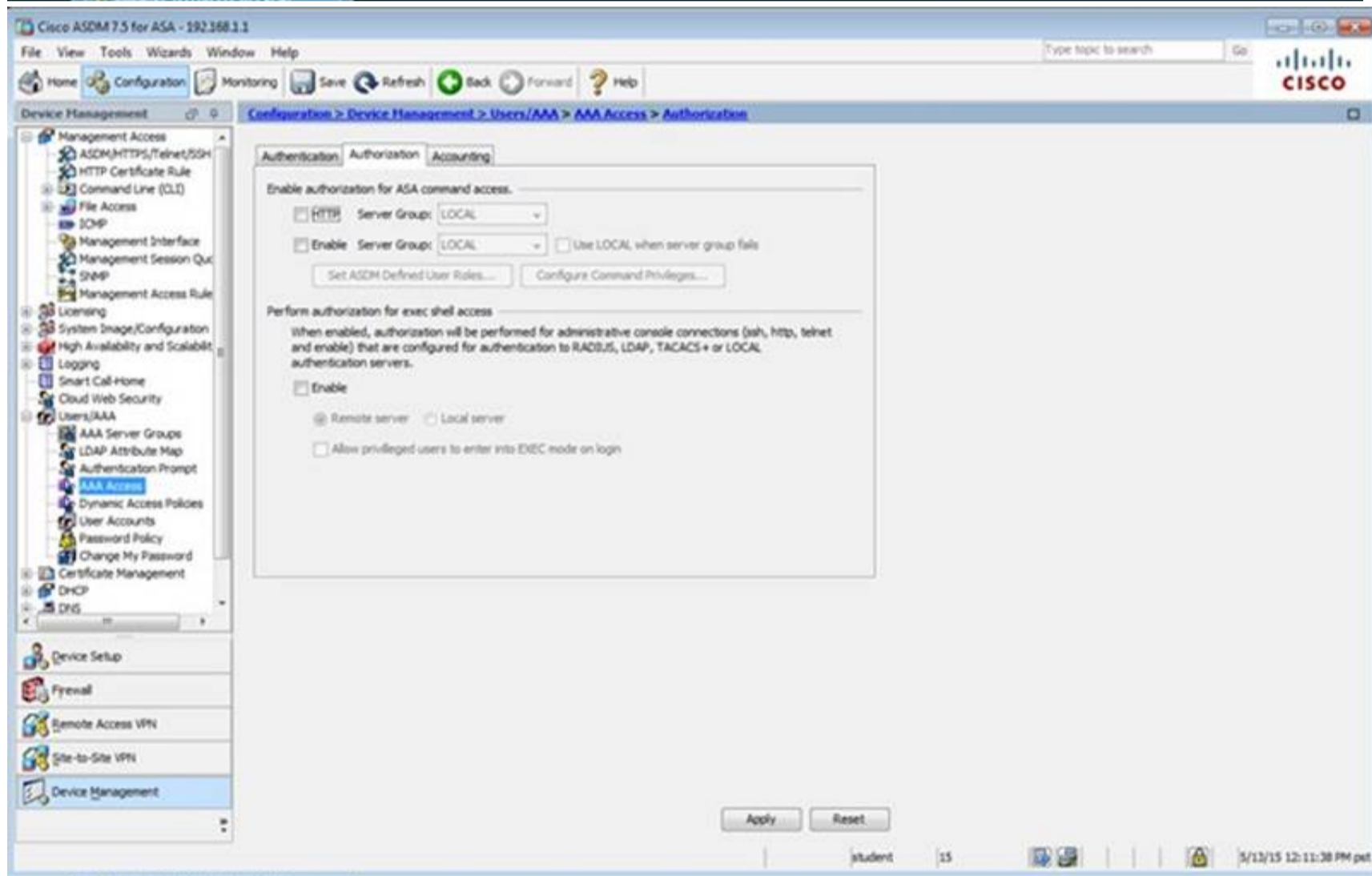
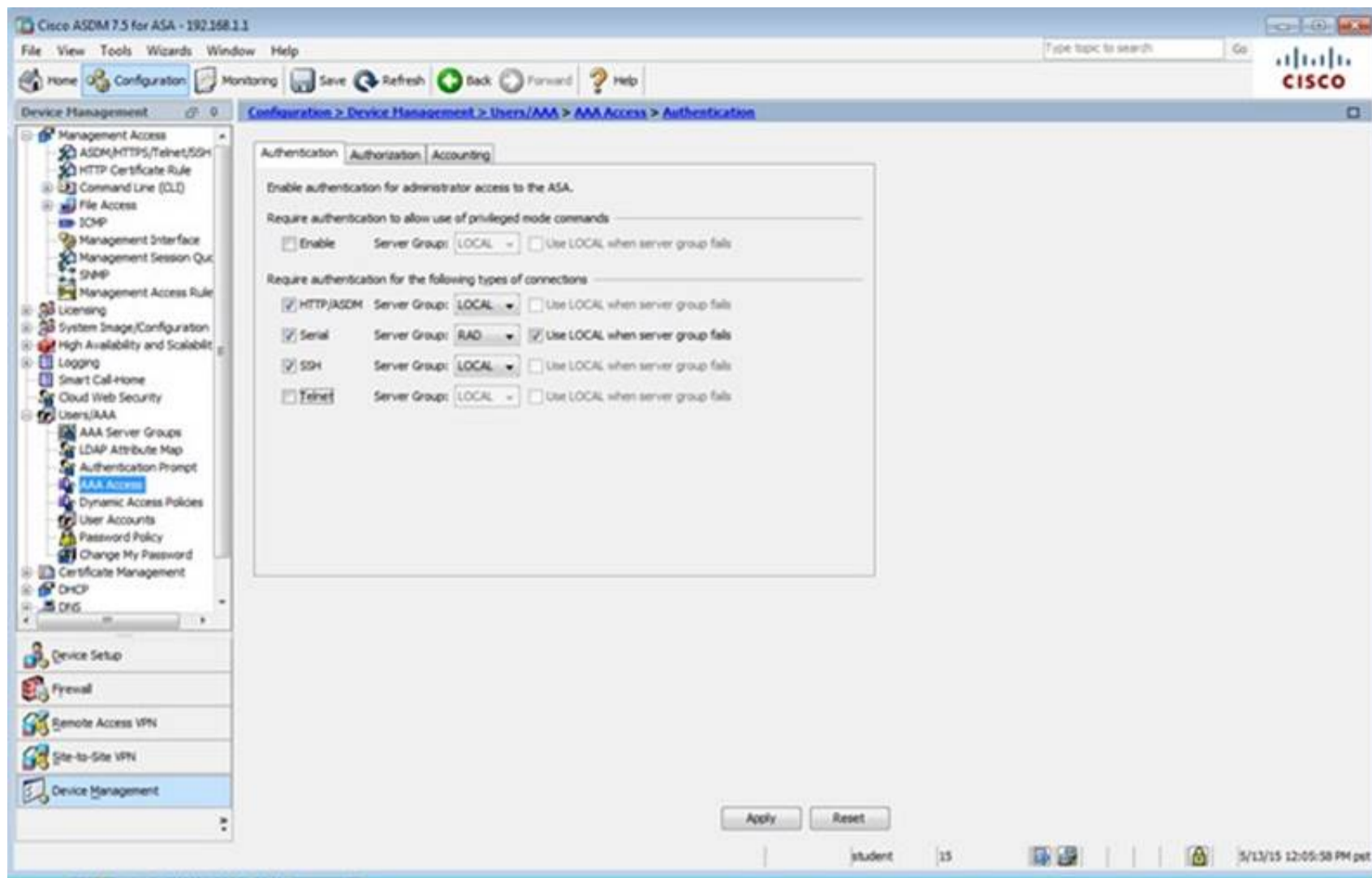
student 15 5/13/15 11:56:08 AM pet

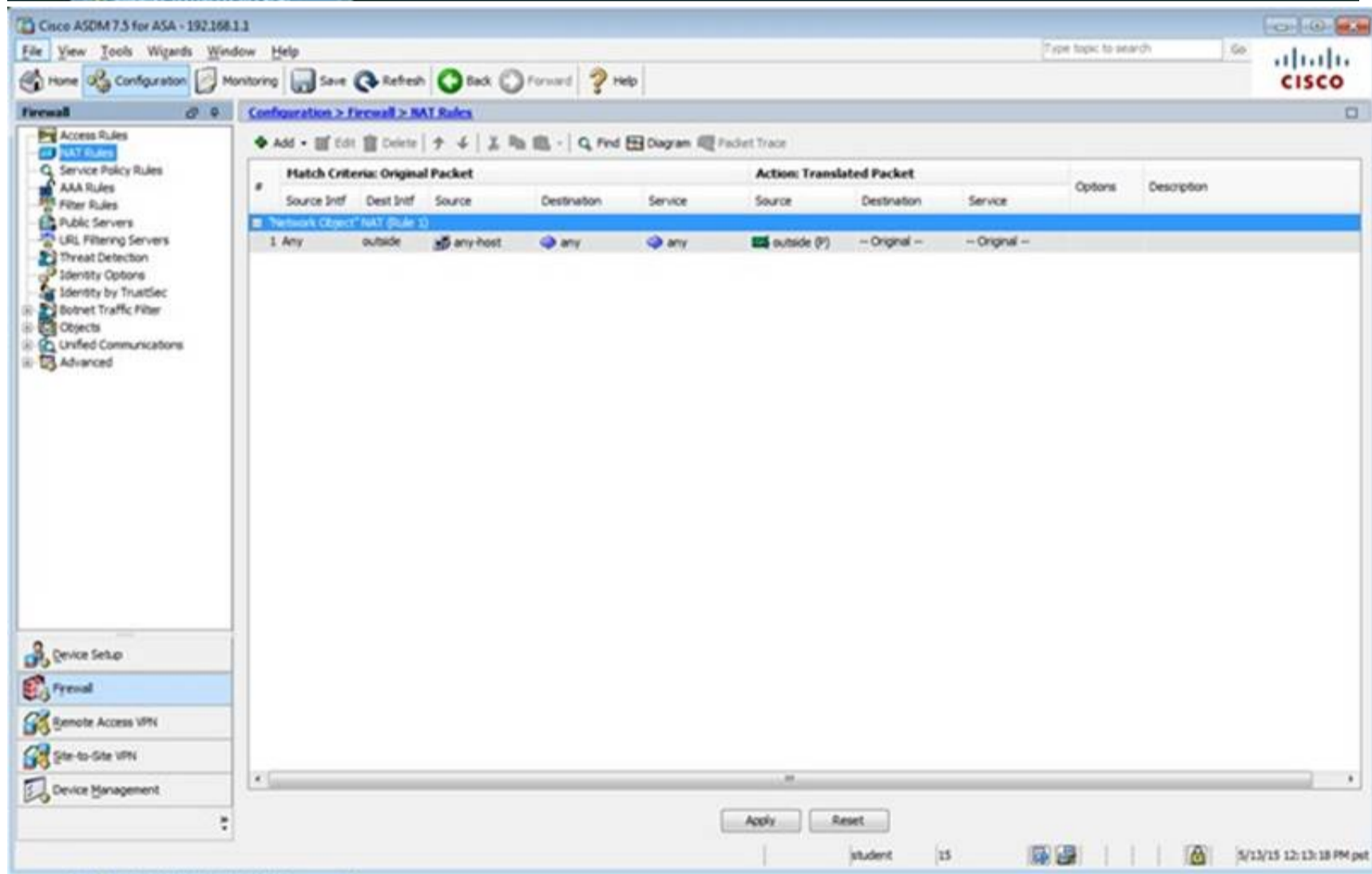
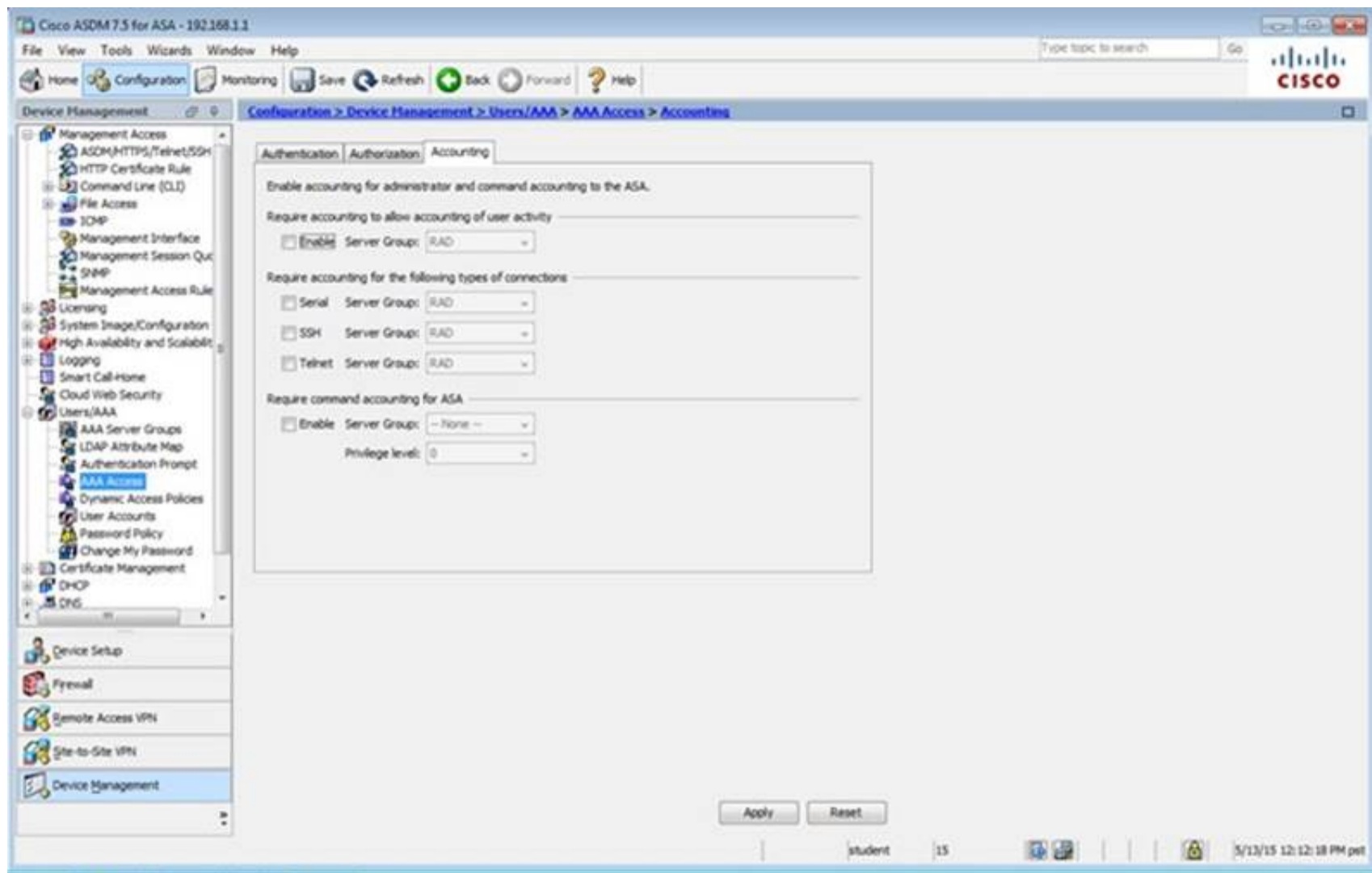


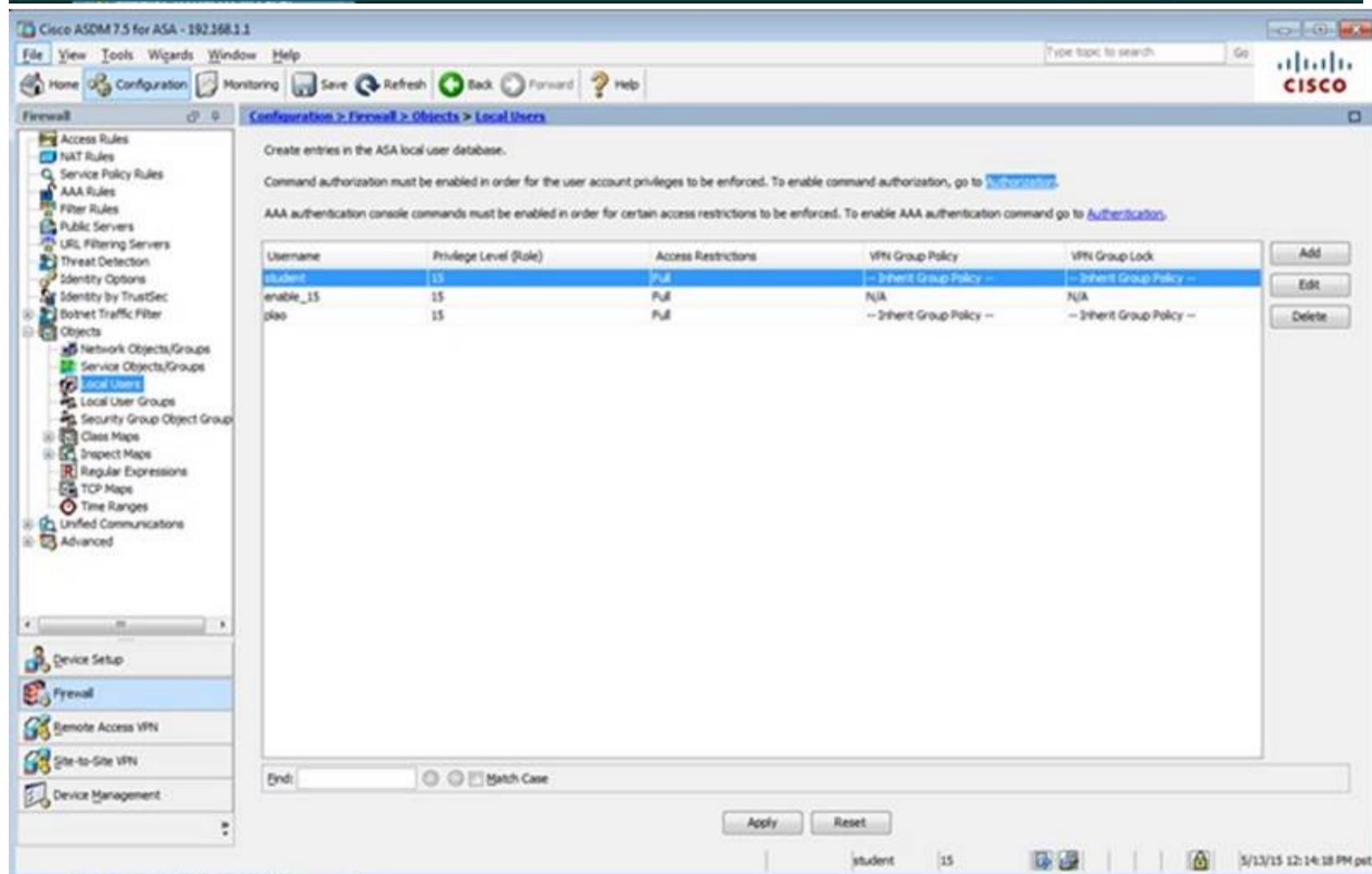
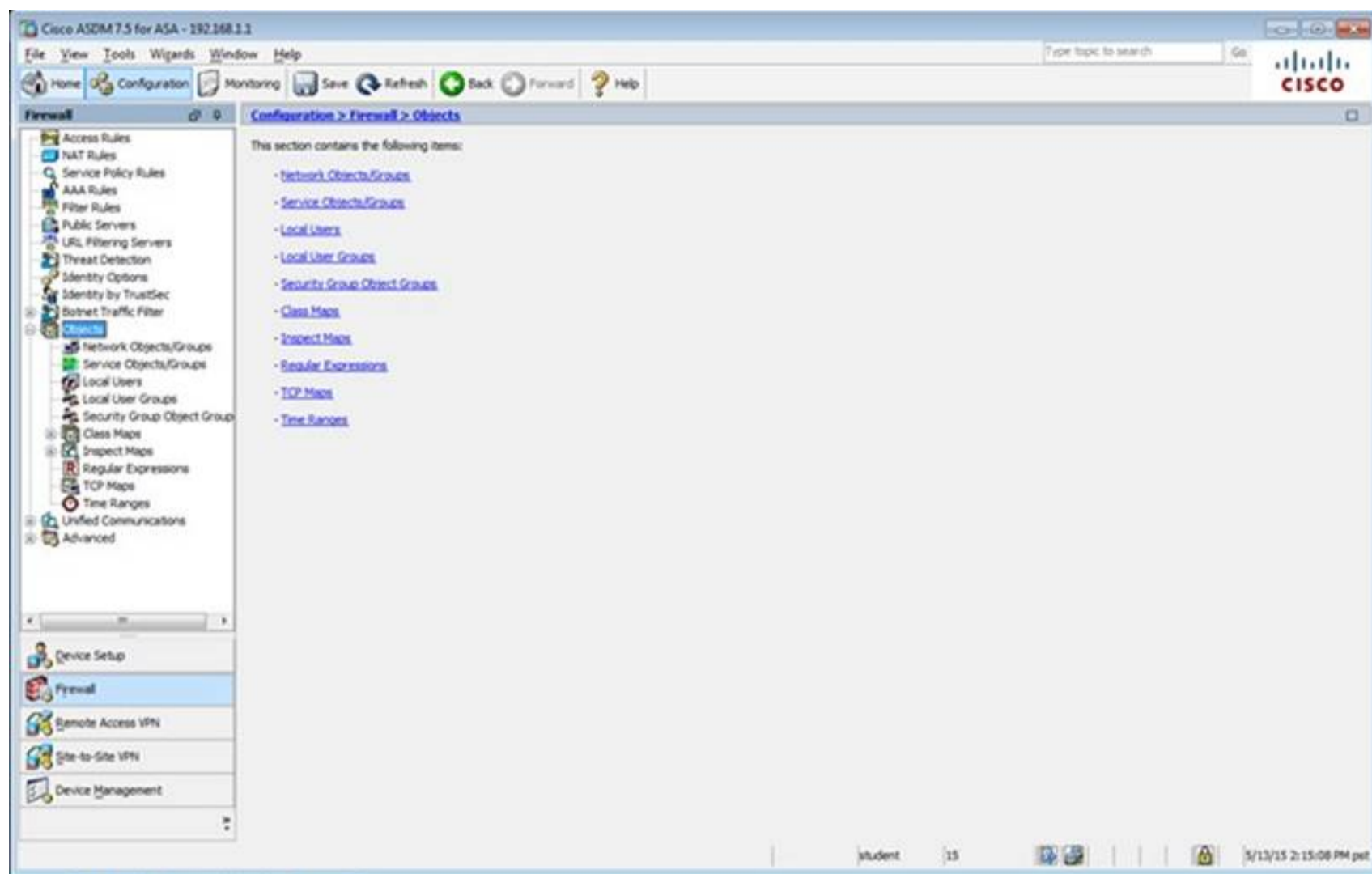












The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Network Objects/Groups' selected. The main pane shows the 'Network Objects/Groups' configuration page. The table lists the following objects:

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

Buttons at the bottom include 'Apply' and 'Reset'. The status bar shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Service Policy Rules' selected. The main pane shows the 'Service Policy Rules' configuration page. The table lists the following rules:

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

Buttons at the bottom include 'Apply' and 'Reset'. The status bar shows 'student' and '15'.

The screenshot shows the Cisco ASDM 7.5 interface for a Cisco ASA device at 192.168.1.1. The left sidebar shows the configuration tree with 'Firewall' selected. The main pane displays the 'Access Rules' configuration page. The table below represents the data shown in the interface:

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

Buttons at the bottom: Apply, Reset, Advanced...

The screenshot shows the Cisco ASDM 7.5 interface for a Cisco ASA device at 192.168.1.1. The left sidebar shows the configuration tree with 'Remote Access VPN' selected. The main pane displays the 'Introduction' page for Remote Access VPN. The text on the page reads:

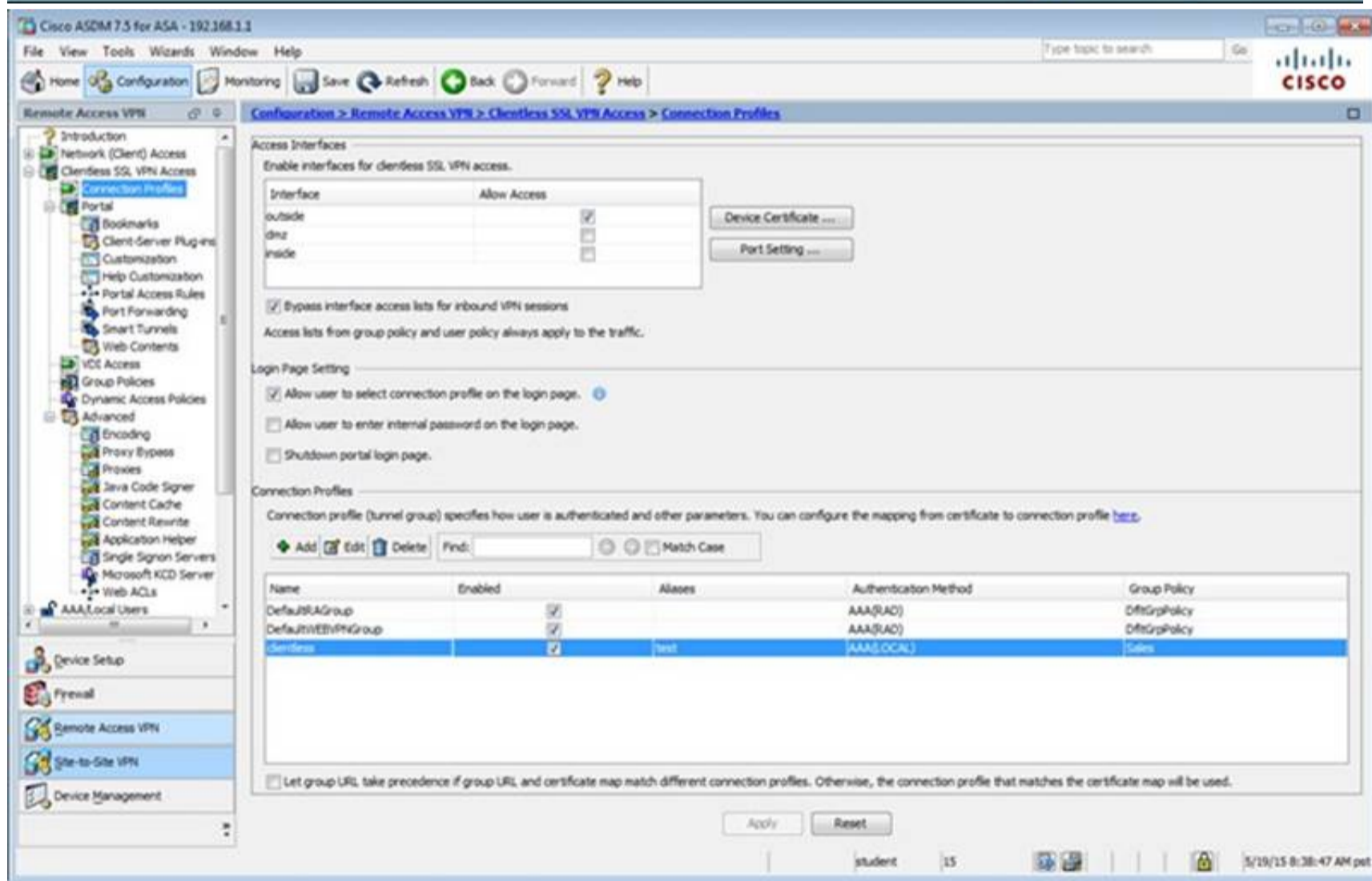
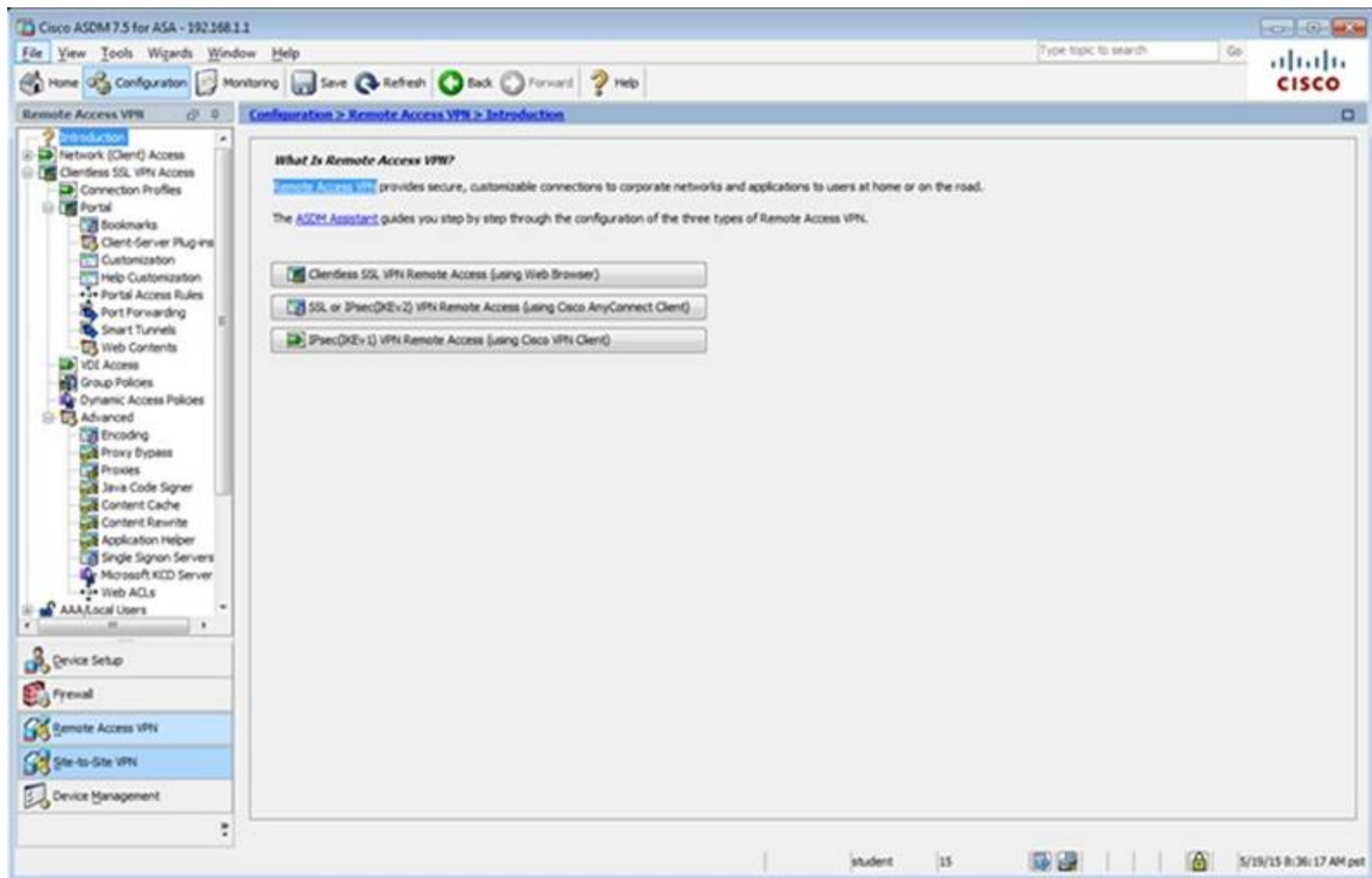
**What Is Remote Access VPN?**

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

The **ASDM Assistant** guides you step by step through the configuration of the three types of Remote Access VPN.

Buttons for configuration options:

- Clientless SSL VPN Remote Access (using Web Browser)
- SSL or IPsec (IKEv2) VPN Remote Access (using Cisco AnyConnect Client)
- IPsec (IKEv1) VPN Remote Access (using Cisco VPN Client)



Edit Clientless SSL VPN Connection Profile: clientless

Basic  
 + Advanced

Name: clientless  
 Aliases: test

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

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

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

Find:  ☐ Next ☐ Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Interface-Specific Authentication Server Groups

+ Add Edit Delete

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

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help

Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

Interface	Server Group	Fallback to LOCAL	Use primary username

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find:  Next Previous

OK Cancel Help

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 > Bookmarks

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

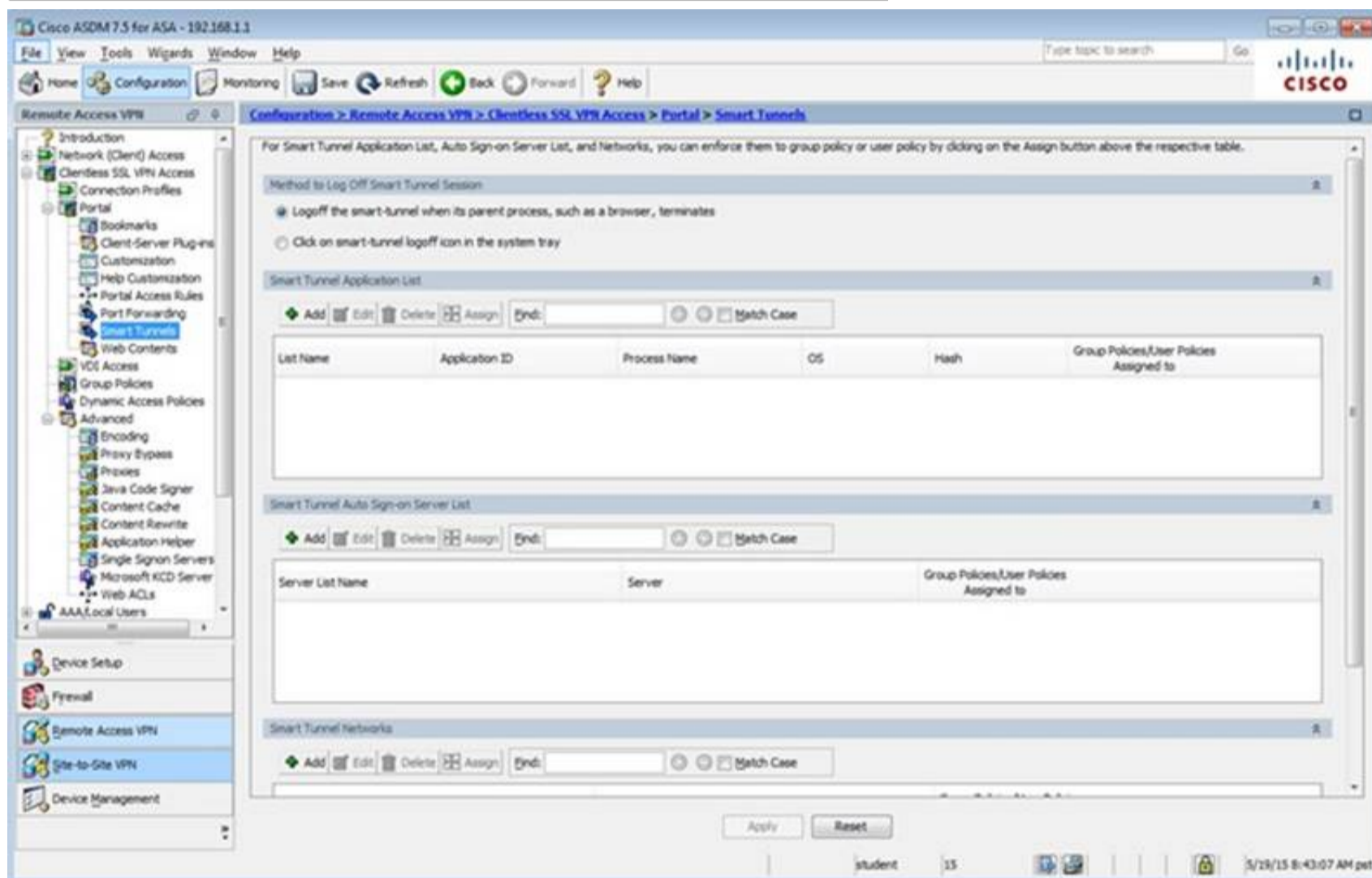
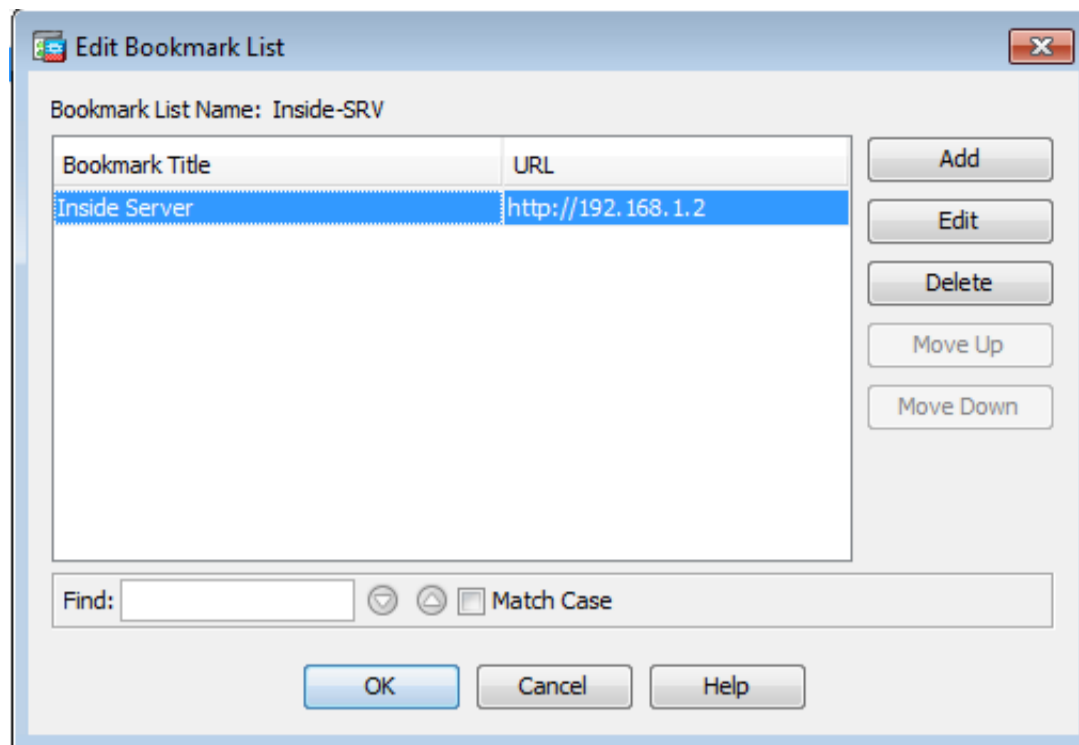
+ Add Edit Delete Import Export Assign

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	

End:  Match Case

Apply Reset

student 15 5/19/15 8:41:57 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 > 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 pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > 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	ssl-clientless	Clientless
DefaultPolicy (System Default)	Internal	Rev 1;rev 2;ssl-clientless/2p-quest	DefaultRAGroup;Default2;Group;DefaultADMG;Def...

Find: Match Case

Apply Reset

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

**Edit Internal Group Policy: Sales**

Name: Sales

Banner: ☒ Inherit

**More Options**

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

Web ACL: ☒ Inherit  Manage...

Access Hours: ☒ Inherit  Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited  minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default  minutes

**Timeout Alerts**

Session Alert Interval: ☒ Inherit ☐ Default  minutes

Idle Alert Interval: ☒ Inherit ☐ Default  minutes

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

Find:  ☐ Next ☐ Previous

**Cisco ASDM 7.2 for ASA - 192.168.1.1**

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	Sales
DefaultGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultGrpPolicy

Find:  ☐ Match Case

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

Edit Internal Group Policy: Sales

General

More Options

Customization

Login Setting

Single Signon

VDI Access

Session Settings

Bookmark List: ☐ Inherit  Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit  Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit  Network:  Manage...

Tunnel Option:

Smart Tunnel Application: ☒ Inherit  Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find:

Next Previous

OK Cancel Help

Edit Internal Group Policy: DftGrpPolicy

Advanced

Servers

Advanced

Name:

Banner:

SCEP forwarding URL:

Address Pools:  Select...

IPv6 Address Pools:  Select...

More Options

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

Filter:  Manage...

Access Hours:  Manage...

Simultaneous Logins:

Restrict access to VLAN:

Connection Profile (Tunnel Group) Lock:

Maximum Connect Time: ☒ Unlimited  minutes

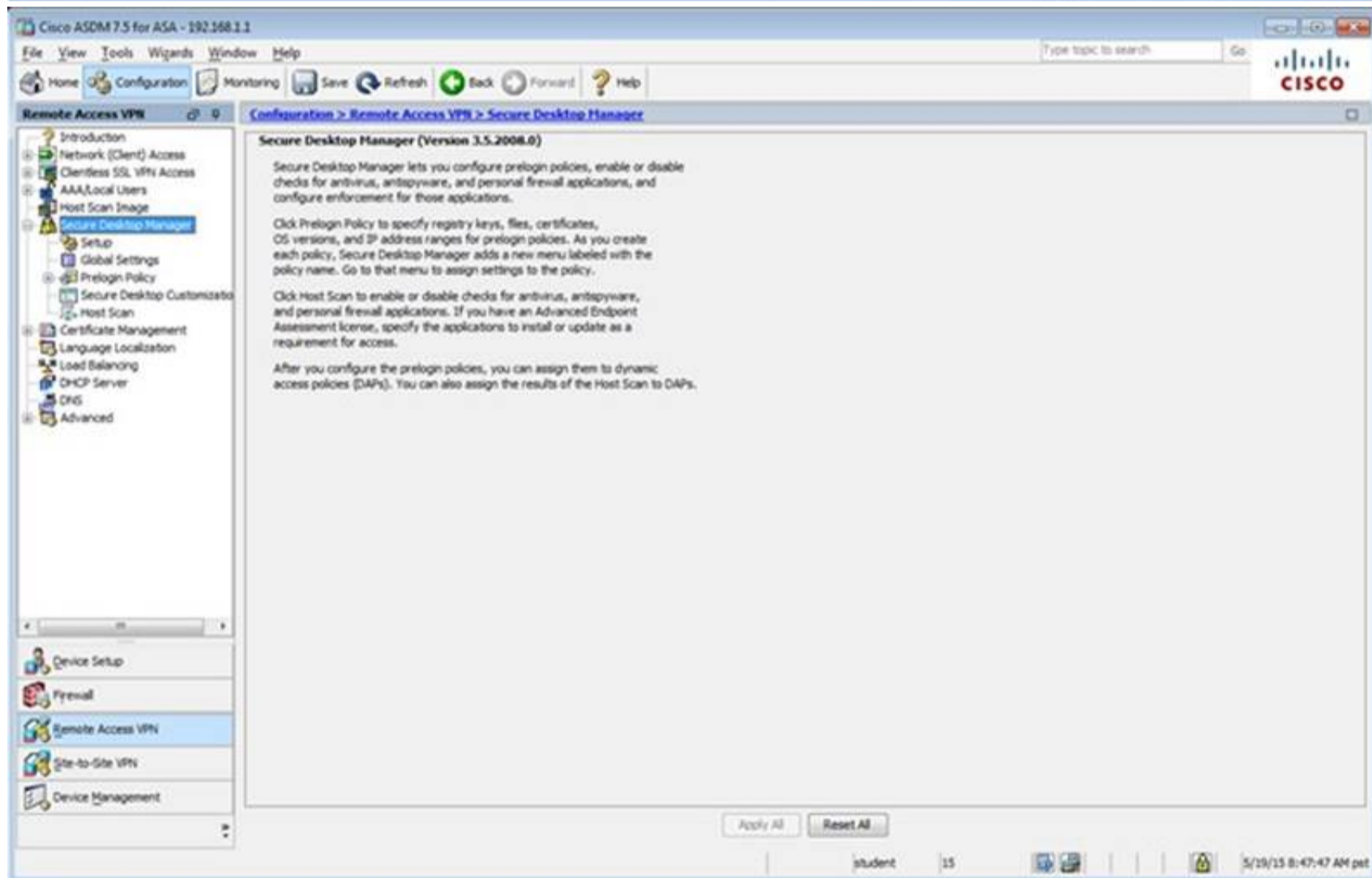
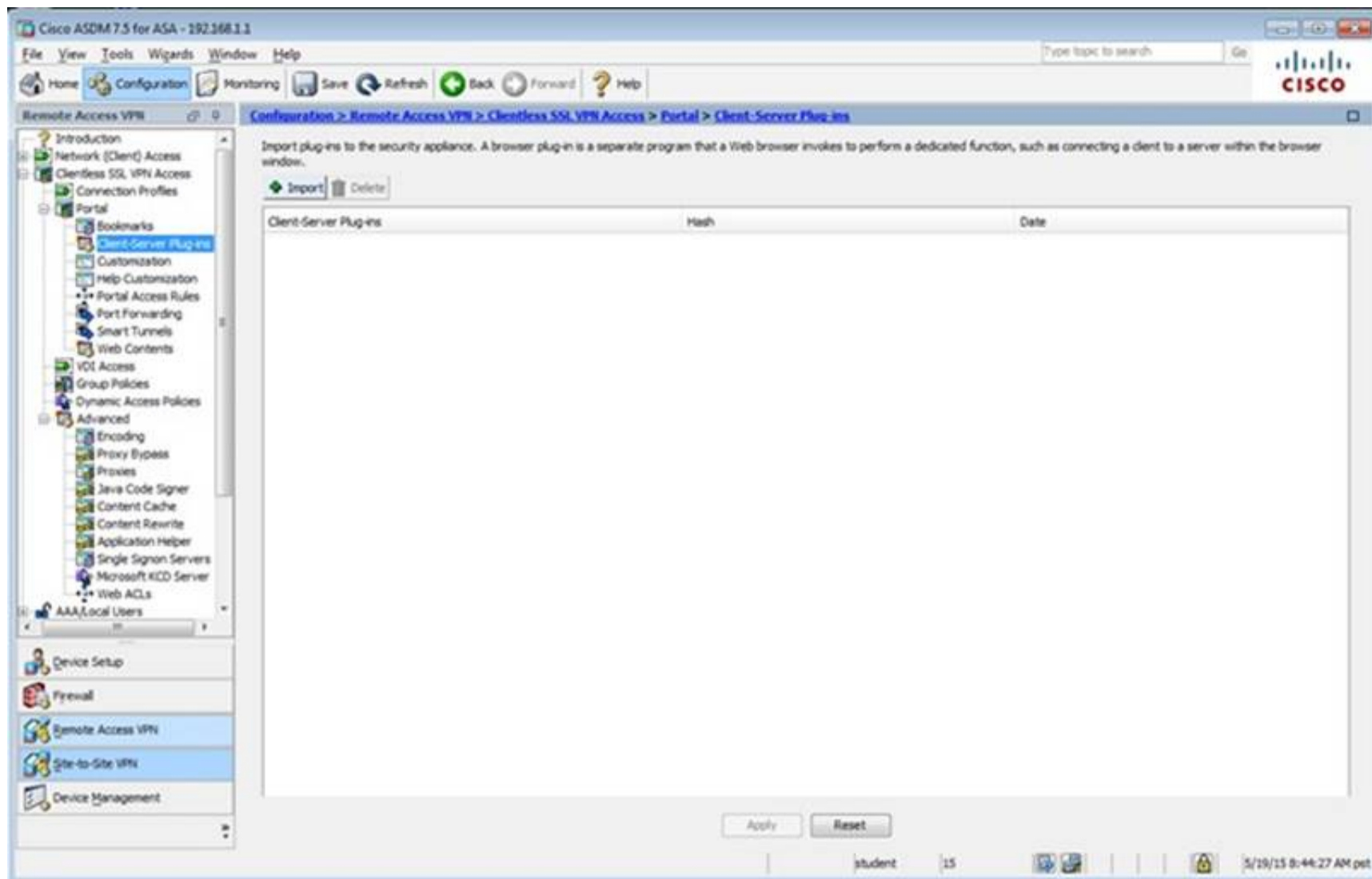
Idle Timeout: ☐ None  minutes

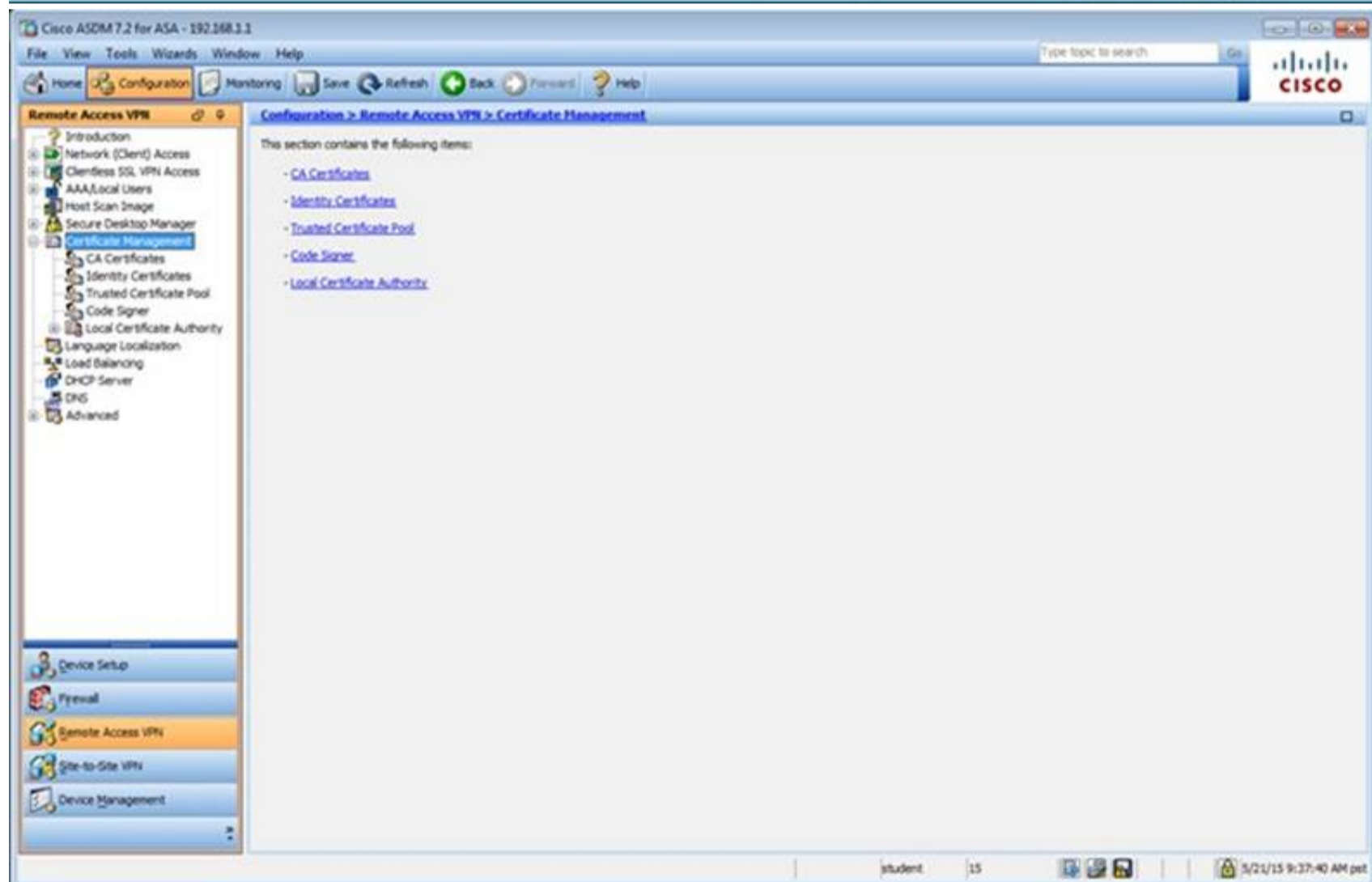
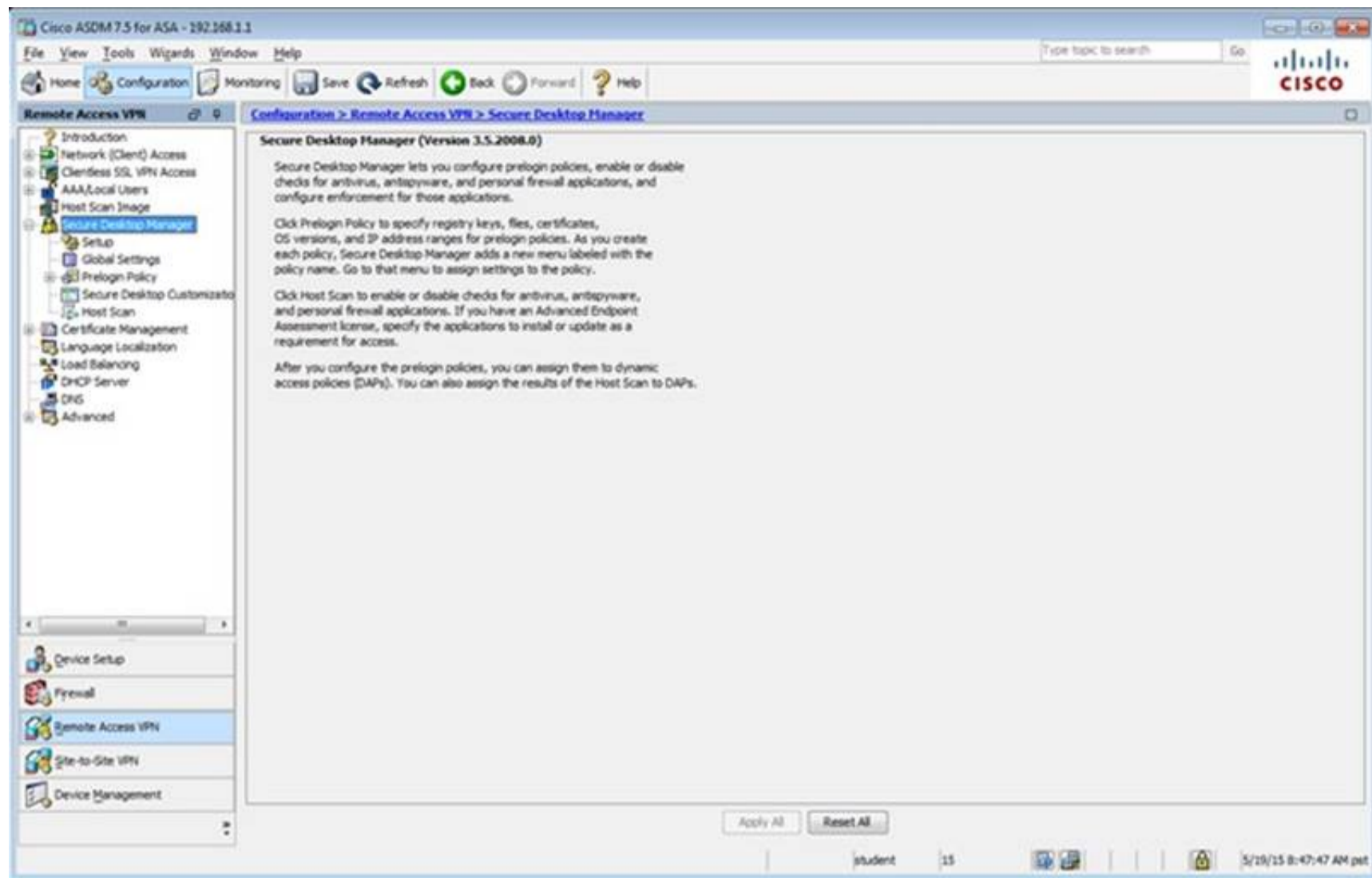
On smart card removal: ☒ Disconnect ☐ Keep the connection

Find:

Next Previous

OK Cancel Help





The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with categories like Introduction, Network (Client) Access, Clientless SSL VPN Access, AAA/Local Users, Host Scan Image, Secure Desktop Manager, Certificate Management, Language Localization, Load Balancing, DHCP Server, DNS, and Advanced. The main content area is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. A single entry is visible: Issued To: testname@P17-ASA.sec, Issued By: testname@P17-ASA.sec, Expiry Date: 11:10:33 pm Dec 20 2024, Associated Trustpoints: ASDM\_TrustPoint1, Usage: General Purpose, Public Key Type: RSA (2048 bits). To the right of the table are buttons: Add, Show Details, Delete, Export, and Install. Below the table is a search bar with 'Find:' and a 'Match Case' checkbox. Further down are sections for 'Certificate Expiration Alerts' (Send the first alert before: 60 days, Repeat Alert Interval: 7 days) and 'Public CA Enrollment' (Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust). At the bottom, there's a section for 'ASDM Identity Certificate Wizard' with a 'Launch ASDM Identity Certificate Wizard' button. The status bar at the bottom shows 'student', '15', and the time '5/19/15 8:51:47 AM pet'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Configuration > Remote Access VPN > Advanced'. It contains a list of items under the heading 'This section contains the following items:'. The items are: Introduction, SSL Settings, Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps, HTTP Redirect, Maximum VPN Sessions, Crypto Engine, and E-mail Proxy. The status bar at the bottom shows 'student', '15', and the time '5/19/15 8:52:47 AM pet'.

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the navigation tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Advanced > SSL Settings' page. The page title is 'Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.' The configuration includes dropdowns for 'The minimum SSL version for the security appliance to negotiate as a "server":' (TLS V1), 'The minimum SSL version for the security appliance to negotiate as a "client":' (TLS V1), 'Diffie-Hellman group to be used with SSL:' (Group2 - 2024-bit modulus), and 'ECDH group to be used with SSL:' (Group19 - 256-bit EC). Below these is an 'Encryption' table with columns for Cipher Version, Cipher Security Level, and Cipher Algorithms/Custom String. The table lists Default, TLSV1, TLSV1.1, TLSV1.2, and DTLSV1. At the bottom, there is a 'Server Name Indication (SNI)' section with a 'Domain' field containing 'dmz' and a 'Certificate' dropdown showing 'ASDM\_TrustPoint1.h...'. There are 'Add', 'Edit', and 'Delete' buttons for the SNI entries. At the very bottom, there is a 'Certificates' section with a note: 'Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.'

The screenshot shows the Cisco ASDM 7.5 for ASA - 192.168.1.1 interface. The left sidebar displays the navigation tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions' page. The page title is 'Configure the maximum number of VPN sessions allowed at any given time.' The configuration includes two input fields: 'Maximum AnyConnect Sessions:' (set to 2) and 'Maximum Other VPN Sessions:' (set to 250). At the bottom, there are 'Apply' and 'Reset' buttons.

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

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

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

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

**Important Concepts**

Following are some important concepts for setting up a connection.

**1. SSL tunnel and IPsec tunnel**

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

**2. User and connection profile**

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

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

**3. Access policy**

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

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

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

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

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

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

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DefaultGroup (System Default)	Internal	ikev2, ssl-clientless, ipsec	DefaultRAGroup, Default 3 Group, DefaultWithVPNGroup

Find: Match Case

Apply Reset

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

Edit Internal Group Policy: DftGrpPolicy

Name: DftGrpPolicy

Banner:

SCP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None  30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for IPsec access.

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

☒ Bypass interface access lists for inbound VPN sessions

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

Connection Profiles

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

+ Add Edit Delete

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

Find: Match Case

Apply Reset

student 15 5/28/15 8:56:47 AM pet

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

[Add](#) [Edit](#) [Delete](#) End:  Match Case

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

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

Apply Reset

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > AAA/Local Users

This section contains the following items:

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

student 15 5/19/15 8:58:57 AM pet

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

Create entries in the ASA local user database.

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

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

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

End:  Match Case

Apply Reset

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

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

AAA Server Groups

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

End:  Match Case

Servers in the Selected Group

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

End:  Match Case

LDAP Attribute Map

Apply Reset

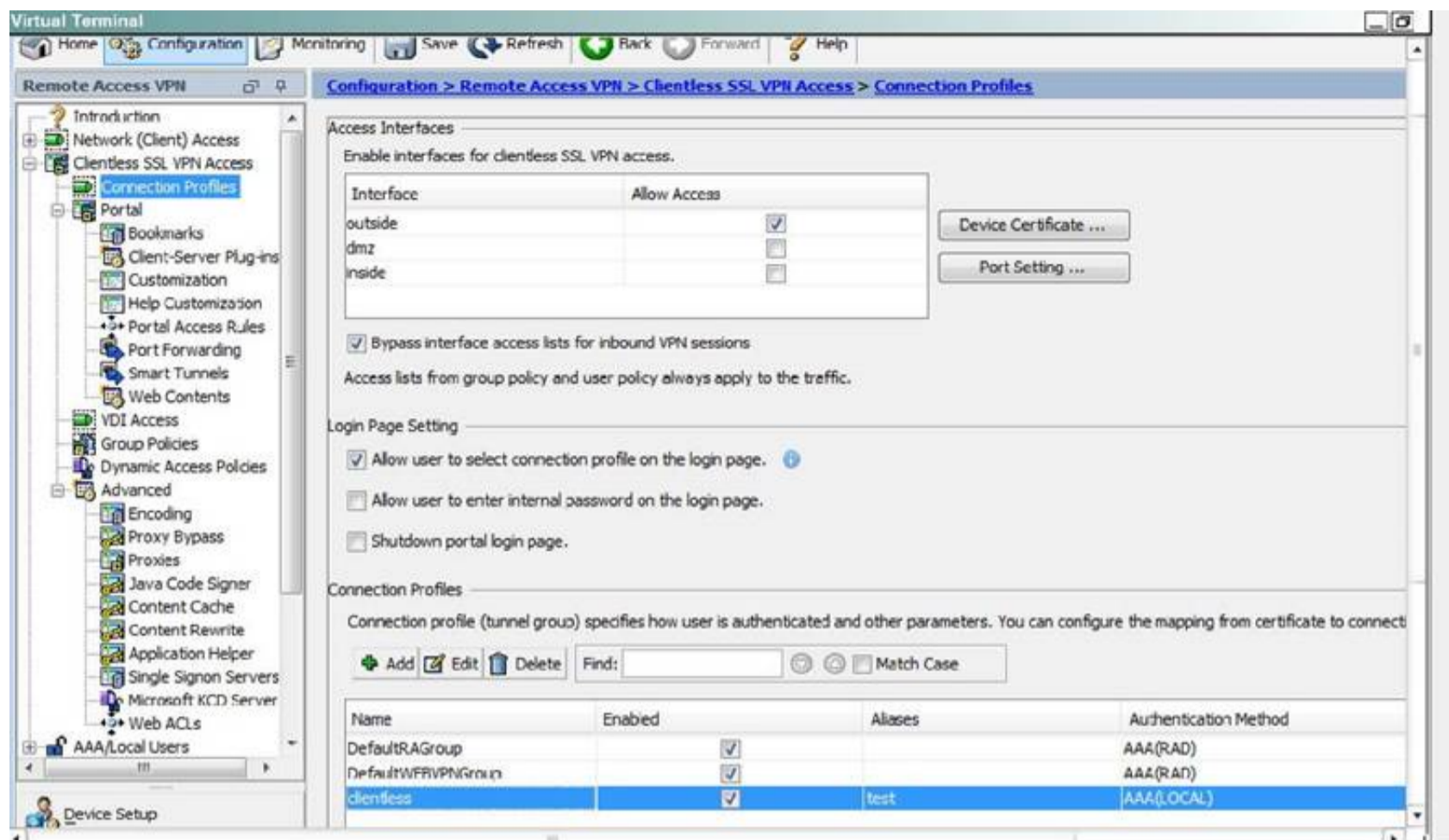
student 15 5/19/15 8:59:57 AM pet

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

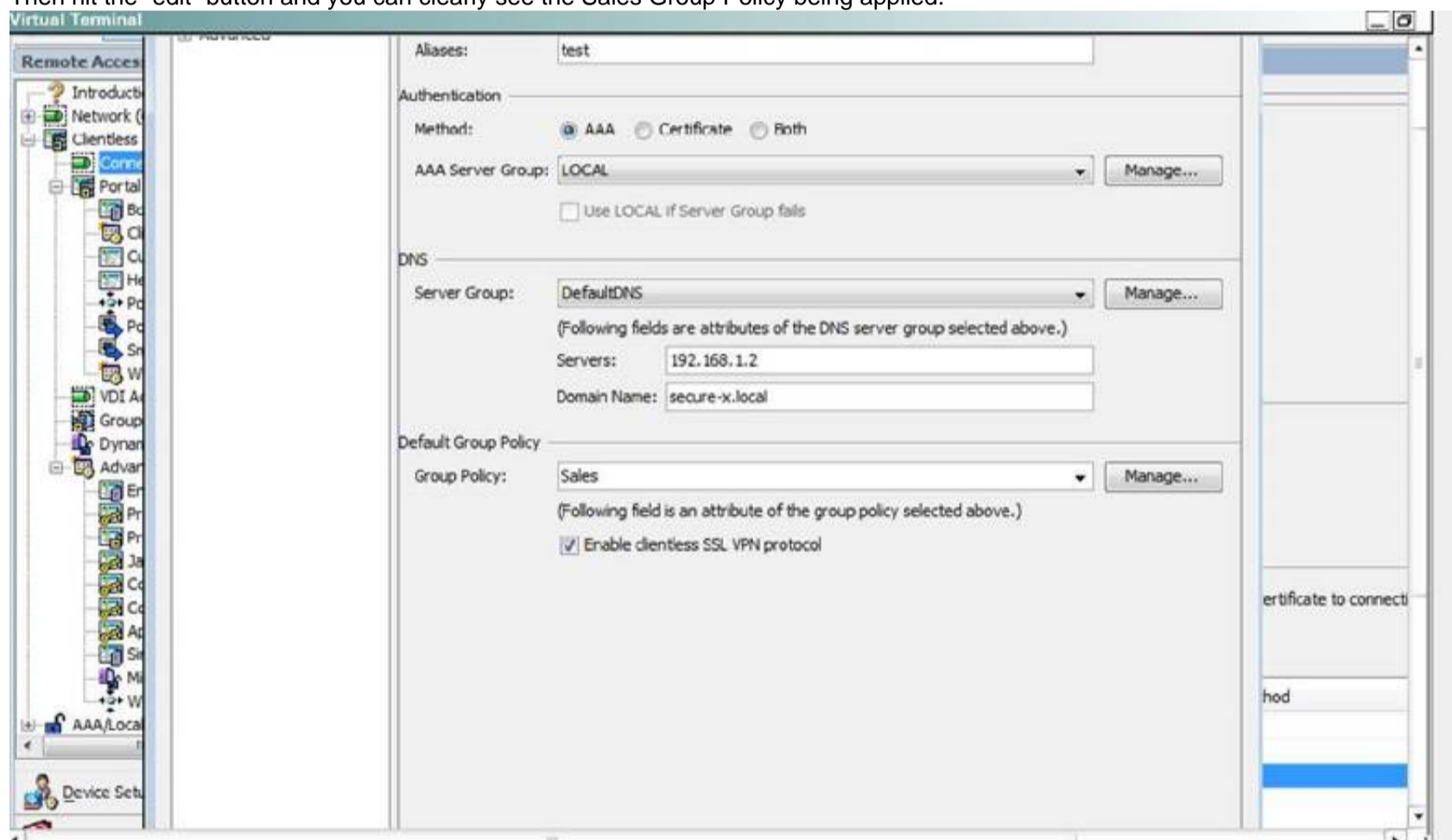
- A. test
- B. clientless
- C. Sales
- D. DfltGrpPolicy
- E. DefaultRAGroup
- F. DefaultWEBVPNGroup

**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.



### NEW QUESTION 139

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

**Explanation:** The term personal firewall typically applies to basic software that can control Layer 3 and Layer 4 access to client machines. HIPS provides several features that offer more robust security than a traditional personal firewall, such as host intrusion prevention and protection against spyware, viruses, worms, Trojans, and other types of malware.

Source: Cisco Official Certification Guide, Personal Firewalls and Host Intrusion Prevention Systems , p.499

### NEW QUESTION 141

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

**Explanation:** Web-based threats continue to rise. To protect your network you need a solution that prevents them. Cisco Advanced Malware Protection (AMP) for Web Security goes beyond the basics in threat detection, URL filtering, and application control. It provides continuous file analysis, retrospective security, and sandboxing to help your security team catch even the stealthiest threats.

Source:

<http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/amp-for-web-security.html>

#### NEW QUESTION 143

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:** DEF

**Explanation:** To define a reflexive access list, you use an entry in an extended named IP access list. This entry must use the reflect keyword.

A reflexive access list is triggered when a new IP upper-layer session (such as TCP or UDP) is initiated from inside your network, with a packet traveling to the external network.

Moreover, the previous method of using the established keyword was available only for the TCP upper-layer protocol. So, for the other upper-layer protocols (such as UDP, ICMP, and so forth), you would have to either permit all incoming traffic or define all possible permissible source/destination host/port address pairs for each protocol. (Besides being an unmanageable task, this could exhaust NVRAM space.) Source:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfreflx.html#54908](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfreflx.html#54908)

#### NEW QUESTION 146

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:** ADE

**Explanation:** + IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server. + IPsec supports two encryption modes: Transport mode and Tunnel mode. Transport mode encrypts only the data portion (payload) of each packet and leaves the packet header untouched. Transport mode is applicable to either gateway or host implementations, and provides protection for upper layer protocols as well as selected IP header fields.

Source:

<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>

[http://www.cisco.com/c/en/us/td/docs/net\\_mgmt/vpn\\_solutions\\_center/2-0/ip\\_security/provisioning/guide/IPsecPG1.html](http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html)

Generic Routing Encapsulation (GRE) is often deployed with IPsec for several reasons, including the following:

+ IPsec Direct Encapsulation supports unicast IP only. If network layer protocols other than IP are to be supported, an IP encapsulation method must be chosen so that those protocols can be transported in IP packets.

+ IPmc is not supported with IPsec Direct Encapsulation. IPsec was created to be a security protocol between two and only two devices, so a service such as multicast is problematic. An IPsec peer encrypts a packet so that only one other IPsec peer can successfully perform the de-encryption. IPmc is not compatible with this mode of operation.

Source: [https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration\\_09186a008074f26a.pdf](https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f26a.pdf)

#### NEW QUESTION 149

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:** AC

#### NEW QUESTION 151

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

**Explanation:** Impact Flag: Choose the impact level assigned to the intrusion event .

Because no operating system information is available for hosts added to the network map from NetFlow data, the system cannot assign Vulnerable (impact level 1: red) impact levels for intrusion events involving those hosts. In such cases, use the host input feature to manually set the operating system identity for the hosts.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Correlation\\_Policies.html](http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Correlation_Policies.html)

Impact

The impact level in this field indicates the correlation between intrusion data, network discovery data, and vulnerability information.

Impact Flag See Impact. Source:

<http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/ViewingEvents.html>

#### NEW QUESTION 153

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

**Explanation:** Deny connection inline: This action terminates the packet that triggered the action and future packets that are part of the same TCP connection. The attacker could open up a new TCP session (using different port numbers), which could still be permitted through the inline IPS.

Available only if the sensor is configured as an IPS.

Source: Cisco Official Certification Guide, Table 17-4 Possible Sensor Responses to Detected Attacks, p.465

#### NEW QUESTION 156

Which syslog severity level is level number 7?

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

**Answer:** D

**Explanation:** Remember: There is a mnemonic device for remembering the order of the eight syslog levels: "Every Awesome Cisco Engineer Will Need Icecream Daily"

0 - Emergency

1 - Alert

2 - Critical

3 - Error

4 - Warning

5 - Notification

6 - Informational

7 - Debugging

#### NEW QUESTION 158

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

**Explanation:** Applying an Access List to an Interface

#interface type number

#ip

access-group {access-list-number | access-list-name} { in | out} Source: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_acl/configuration/xr-3s/sec-data-acl-xr-3s-book/sec-create-ip-apply.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xr-3s/sec-data-acl-xr-3s-book/sec-create-ip-apply.html)

#### NEW QUESTION 161

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:** ABC

**Explanation:** If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form. HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls, and application firewalls in one package. Host-based IPS operates by detecting attacks that occur on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.  
Source:  
<http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3>

#### NEW QUESTION 163

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

**Explanation:** Before you can use any of the services AAA network security services provide, you must enable AAA. Source:  
[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfaaa.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfaaa.html)

#### NEW QUESTION 168

Which feature filters CoPP packets?

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

**Answer:** A

#### NEW QUESTION 169

What are two ways to prevent eavesdropping when you perform device management test? (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:** AB

**Explanation:** Both SSH and SNMPv3 provide security of the packets through encryption

#### NEW QUESTION 171

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

**Explanation:** Adding Network Objects for Mapped Addresses

For dynamic NAT, you must use an object or group for the mapped addresses. Other NAT types have the option of using inline addresses, or you can create an object or group according to this section.

\* Dynamic NAT:

+ You cannot use an inline address; you must configure a network object or group. + The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.

+ If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.

\* Dynamic PAT (Hide):

+ Instead of using an object, you can optionally configure an inline host address or specify the interface address.

+ If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.

\* Static NAT or Static NAT with port translation:

+ Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).

+ If you use an object, the object or group can contain a host, range, or subnet.

\* Identity NAT

+ Instead of using an object, you can configure an inline address. + If you use an object, the object must match the real addresses you want to translate.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa\\_90\\_cli\\_config/nat\\_objects.html#61711](http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/nat_objects.html#61711)

#### NEW QUESTION 174

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

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

**Answer:** AB

#### NEW QUESTION 175

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

#### NEW QUESTION 178

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

**Explanation:** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007.

Source: [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)

A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. A proxy firewall may also be called an application firewall or gateway firewall. Proxy firewalls are considered to be the most secure type of firewall because they prevent direct network contact with other systems.

Source:

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

#### NEW QUESTION 183

Which command initializes a lawful intercept view?

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

**Answer:** C

**Explanation:** Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information.

Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.

#li-view li-password user username password password

Source:

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t7/feature/guide/gtclivws.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html)

Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the privilege command.

#### SUMMARY STEPS

1. enable view
2. configure terminal
3. li-view li-password user username password password
4. username lawful-intercept [name] [privilege privilege-level] view view-name] password password
5. parser view view-name
6. secret 5 encrypted-password
7. name new-name

#### NEW QUESTION 185

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

**Explanation:** A Web Application Firewall (or WAF) filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, Cross-Site Scripting (XSS) and security misconfigurations.  
Source: [https://en.wikipedia.org/wiki/Web\\_application\\_firewall](https://en.wikipedia.org/wiki/Web_application_firewall)

#### NEW QUESTION 190

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

**Explanation:** PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key.  
Source: [https://en.wikipedia.org/wiki/Protected\\_Extensible\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol)

#### NEW QUESTION 191

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

**Explanation:** Each website defined in the URL filtering database is assigned one of approximately 60 different URL categories. There are two ways to make use of URL categorization on the firewall:  
Block or allow traffic based on URL category --You can create a URL Filtering profile that specifies an action for each URL category and attach the profile to a policy. Traffic that matches the policy would then be subject to the URL filtering settings in the profile. For example, to block all gaming websites you would set the block action for the URL category games in the URL profile and attach it to the security policy rule(s) that allow web access. See Configure URL Filtering for more information.  
Match traffic based on URL category for policy enforcement --If you want a specific policy rule to apply only to web traffic to sites in a specific category, you would add the category as match criteria when you create the policy rule. For example, you could use the URL category streaming-media in a QoS policy to apply bandwidth controls to all websites that are categorized as streaming media. See URL Category as Policy Match Criteria for more information.  
By grouping websites into categories, it makes it easy to define actions based on certain types of websites. Source: <https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-categories>

#### NEW QUESTION 196

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

**Explanation:** VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.  
+ In a switch spoofing attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host.  
+ In a double tagging attack, an attacking host connected on a 802.1q interface prepends two VLAN tags to packets that it transmits. Double Tagging can only be exploited when switches use "Native VLANs". Ports with a specific access VLAN (the native VLAN) don't apply a VLAN tag when sending frames, allowing the attacker's fake VLAN tag to be read by the next switch. Double Tagging can be mitigated by either one of the following actions:  
+ Simply do not put any hosts on VLAN 1 (The default VLAN). i.e., assign an access VLAN other than VLAN 1 to every access port  
+ Change the native VLAN on all trunk ports to an unused VLAN ID.  
+ Explicit tagging of the native VLAN on all trunk ports. Must be configured on all switches in network autonomy.  
Source: [https://en.wikipedia.org/wiki/VLAN\\_hopping](https://en.wikipedia.org/wiki/VLAN_hopping)

#### NEW QUESTION 198

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

**Explanation:** This is the output of the #show crypto isakmp sa command. This command shows the Internet Security Association Management Protocol (ISAKMP) security associations (SAs) built between peers - IPsec Phase1.

MM\_NO\_STATE means that main mode has failed. QM\_IDLE - this is what we want to see.

More on this

<http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html>

#### NEW QUESTION 201

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

#### NEW QUESTION 203

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

**Explanation:** Now the router itself does not have a problem with IP connectivity to the Internet because the router has a globally reachable IP address (34.0.0.3) in this example. The users are not so fortunate, however, because they are using private IP address space, and that kind of address is not allowed directly on the Internet by the service providers. So, if the users want to access a server on the Internet, they forward their packets to the default gateway, which in this case is R1, and if configured to do so, R1 modifies the IP headers in those packets and swaps out the original source IP addresses with either its own global address or a global address from a pool of global addresses (which R1 is responsible for managing, meaning that if a packet was destined to one of those addresses, the routing to those addresses on the Internet would forward the packets back to R1). These are global addresses assigned by the service provider for R1's use.

Source: Cisco Official Certification Guide, NAT Is About Hiding or Changing the Truth About Source Addresses,

#### NEW QUESTION 204

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:** ABC

#### NEW QUESTION 209

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

**Explanation:** Source:

<http://www.ciscopress.com/articles/article.asp?p=1697887> Standard ACL

- 1) Able Restrict, deny & filter packets by Host Ip or subnet only.
- 2) Best Practice is put Std. ACL restriction near from Source Host/Subnet (Interface-In-bound).
- 3) No Protocol based restriction. (Only HOST IP). Extended ACL

- 1) More flexible than Standard ACL.
- 2) You can filter packets by Host/Subnet as well as Protocol/TCP/Port/UDP/Port.
- 3) Best Practice is to put restriction near the destination Host/Subnet. (Interface-Outbound)

#### NEW QUESTION 211

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

**Explanation:** Public key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key.

Source: [https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)

#### NEW QUESTION 212

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

- A. when multiple 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:** AB

#### NEW QUESTION 216

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

**Explanation:** By default, if two interfaces are both at the exact same security level, traffic is not allowed between those two interfaces.

To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the same-security-traffic command in global configuration mode.

#same-security-traffic

permit {inter-interface | intra-interface} Source: Cisco Official Certification Guide, The Default Flow of Traffic, p.422

<http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command>

#### NEW QUESTION 221

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

**Explanation:** ARPs are allowed through the transparent firewall in both directions without an ACL. ARP traffic can be controlled by ARP inspection.

Source: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/intro-fw.html>

#### NEW QUESTION 226

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

**Explanation:** A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IP Security protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Source:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/command/Explanation:/Reference/srfipsec.html#wp1017694](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/Explanation:/Reference/srfipsec.html#wp1017694) To define a transform set -- an acceptable combination of security protocols and algorithms -- use the crypto ipsec transform-set global configuration command.

ESP Encryption Transform

+ esp-aes 256: ESP with the 256-bit AES encryption algorithm. ESP Authentication Transform

+ esp-md5-hmac: ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended) Source: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c3.html#wp2590984165>

#### NEW QUESTION 231

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:** AB

**Explanation:** Security Information Event Management SIEM

+ Log collection of event records from sources throughout the organization provides important forensic tools and helps to address compliance reporting requirements.

+ Normalization maps log messages from different systems into a common data model, enabling the organization to connect and analyze related events, even if they are initially logged in different source formats.

+ Correlation links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.

+ Aggregation reduces the volume of event data by consolidating duplicate event records. + Reporting presents the correlated, aggregated event data in real-time monitoring and long-term summaries.

Source:

[http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sbaSIEM\\_deployG.pdf](http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sbaSIEM_deployG.pdf)

#### NEW QUESTION 234

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

**Explanation:** Defense in-depth is the key to stopping most, but not all, network and computer related attacks. It's a concept of deploying several layers of defense that mitigate security threats.

Source:

<http://security2b.blogspot.ro/2006/12/what-is-defense-in-depth-and-why-is-it.html>

#### NEW QUESTION 237

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

**Explanation:** Cisco ISE allows you to wipe or turn on pin lock for a device that is lost. From the MDM Access drop-down list, choose any one of the following options:

+ Full Wipe -- Depending on the MDM vendor, this option either removes the corporate apps or resets the device to the factory settings.

+ Corporate Wipe -- Removes applications that you have configured in the MDM server policies + PIN Lock

-- Locks the device

Source:

[http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin\\_guide/b\\_ise\\_admin\\_guide\\_14/b\\_ise\\_admin\\_guide\\_14\\_chapter\\_01001.html#task\\_820C9C2A1A6647E995CA5AAB01E1CDEF](http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_01001.html#task_820C9C2A1A6647E995CA5AAB01E1CDEF)

#### NEW QUESTION 238

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:** BE

**Explanation:** + Secure Shell (SSH) provides the same functionality as Telnet, in that it gives you a CLI to a router or switch; unlike Telnet, however, SSH encrypts all the packets that are used in the session.

+ For graphical user interface (GUI) management tools such as CCP, use HTTPS rather than HTTP because, like SSH, it encrypts the session, which provides confidentiality for the packets in that session.

Source: Cisco Official Certification Guide, Encrypted Management Protocols, p.287

#### NEW QUESTION 241

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

- A. Port security
- B. DHCP snooping
- C. IP source guard
- D. Dynamic ARP inspection

**Answer:** BD

**Explanation:** + ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received.

+ DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

+ DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database.

Source: Cisco Official Certification Guide, Dynamic ARP Inspection, p.254

#### NEW QUESTION 242

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:** ABC

#### NEW QUESTION 247

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:** AB

**Explanation:** An Advanced Persistent Threat (APT) is a prolonged, aimed attack on a specific target with the intention to compromise their system and gain information from or about that target.

The target can be a person, an organization or a business. Source:

<https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/> One new malware threat has emerged as a definite concern, namely, targeted malware. Instead of blanketing the Internet with a worm, targeted attacks concentrate on a single high-value target.

Source:

[http://crissp.poly.edu/wissp08/panel\\_malware.htm](http://crissp.poly.edu/wissp08/panel_malware.htm)

#### NEW QUESTION 251

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

**Explanation:** Five basic items need to be agreed upon between the two VPN devices/gateways (in this case, the two routers) for the IKE Phase 1 tunnel to succeed, as follows:

- + Hash algorithm
- + Encryption algorithm
- + Diffie-Hellman (DH) group
- + Authentication method: used for verifying the identity of the VPN peer on the other side of the tunnel. Options include a pre-shared key (PSK) used only for the authentication or RSA signatures (which leverage the public keys contained in digital certificates).
- + Lifetime

The PSK used on the routers are different: test67890 and test12345 Source: Cisco Official Certification Guide, The Play by Play for IPsec, p.124

## NEW QUESTION 252

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

**Explanation:** The output presented is generated by the show ntp association detail command. Attributes:

+ configured: This NTP clock source has been configured to be a server. This value can also be dynamic, where the peer/server was dynamically discovered.

+ our\_master: The local client is synchronized to this peer

+ valid: The peer/server time is valid. The local client accepts this time if this peer becomes the master.

Source:

<http://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html>

#### NEW QUESTION 254

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:** AB

#### NEW QUESTION 259

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:** ABC

**Explanation:** A typical enterprise hierarchical LAN campus network design includes the following three layers:

+ Access layer: Provides workgroup/user access to the network + Distribution layer: Provides policy-based connectivity and controls the boundary between the access and core layers

+ Core layer: Provides fast transport between distribution switches within the enterprise campus Source: <http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

#### NEW QUESTION 261

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

**Explanation:** Snowshoe spamming is a strategy in which spam is propagated over several domains and IP addresses to weaken reputation metrics and avoid filters. The increasing number of IP addresses makes recognizing and capturing spam difficult, which means that a certain amount of spam reaches their destination email inboxes.

Specialized spam trapping organizations are often hard pressed to identify and trap snowshoe spamming via conventional spam filters.

The strategy of snowshoe spamming is similar to actual snowshoes that distribute the weight of an individual over a wide area to avoid sinking into the snow.

Likewise, snowshoe spamming delivers its weight over a wide area to remain clear of filters.

Source: <https://www.techopedia.com/definition/1713/snowshoe-spamming> Snowshoe spam, as mentioned above, is a growing concern as spammers distribute spam attack origination across a broad range of IP addresses in order to evade IP reputation checks. The newest AsyncOS 9 for ESA enables enhanced anti-spam scanning through contextual analysis and enhanced automation, as well as automatic classification, to provide a stronger defense against snowshoe campaigns and phishing attacks.

Source:

<http://blogs.cisco.com/security/cisco-email-security-stays-ahead-of-current-threats-by-adding-stronger-snowshoe-spam-defense-amp-enhancements-and-more>

#### NEW QUESTION 266

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

**Explanation:** You can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer expires. The group policy assigned to the session specifies these timer values. If AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned to the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

Source:

[http://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac03vpn.pdf](http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac03vpn.pdf)

#### NEW QUESTION 268

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

**Explanation:** The types of private VLAN ports are as follows:

- + Promiscuous - The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN
  - + Isolated - This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
  - + Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
- These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.

Source:

<http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html#42874>

#### NEW QUESTION 273

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

#### NEW QUESTION 277

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

#### NEW QUESTION 278

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

**Explanation:** As an enhancement to EAP-FAST, a differentiation was made to have a User PAC and a Machine PAC. After a successful machine-authentication, ISE will issue a Machine-PAC to the client. Then, when processing a user- authentication, ISE will request the Machine-PAC to prove that the machine was successfully authenticated, too. This is the first time in 802.1X history that multiple credentials have been able to be authenticated within a single EAP transaction, and it is known as "EAP Chaining".

Source:

<http://www.networkworld.com/article/2223672/access-control/which-eap-types-do-you-need-for-which-identity-projects.html>

#### NEW QUESTION 283

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

**Explanation:** Confidentiality: There are two types of data: data in motion as it moves across the network; and data at rest, when data is sitting on storage media (server, local workstation, in the cloud, and so forth). Confidentiality means that only the authorized individuals/ systems can view sensitive or classified information.

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

### NEW QUESTION 286

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

**Explanation:** tacacs-server host host-name [port integer] [timeout integer] [key string] [single-connection] [nat] The single-connection keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Source:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/command](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command)

### NEW QUESTION 291

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

**Explanation:** Command A sets the "configure terminal" command at privilege level 9, which is a higher level than HelpDesk has access to.

Also, some of the dumps say "Privilege exec level 9 show configure terminal" in the config and the answer options. This is not a different version of the question, it is a mistake. The line "show configure terminal" is not a valid command in Cisco IOS.

### NEW QUESTION 295

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

**Explanation:** Enabling OSPF SUMMARY STEPS

1. enable
2. configure terminal
3. router ospf process-id
4. network ip-address wildcard-mask area area-id
5. end

Source:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_ospf/configuration/12-4t/iro-12-4t-book/iro- cfg.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro- cfg.html)

#### NEW QUESTION 297

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

**Explanation:** MAC address flooding is an attack technique used to exploit the memory and hardware limitations in a switch's CAM table.

Source:

[http://hakipedia.com/index.php/CAM\\_Table\\_Overflow](http://hakipedia.com/index.php/CAM_Table_Overflow)

#### NEW QUESTION 302

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:** BD

**Explanation:** VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.

+ In a switch spoofing attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host.

+ In a double tagging attack, an attacking host connected on a 802.1q interface prepends two VLAN tags to packets that it transmits.

Source: [https://en.wikipedia.org/wiki/VLAN\\_hopping](https://en.wikipedia.org/wiki/VLAN_hopping)

#### NEW QUESTION 305

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

**Explanation:** SCEP Profile Configuration on ISE

Within this design, ISE is acting as a Simple Certificate Enrollment Protocol (SCEP) proxy server, thereby allowing mobile clients to obtain their digital certificates from the CA server. This important feature of ISE allows all endpoints, such as iOS, Android, Windows, and MAC, to obtain digital certificates through the ISE. This feature combined with the initial registration process greatly simplifies the provisioning of digital certificates on endpoints.

Source:

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless\\_Networks/Unified\\_Access/BYOD\\_Design\\_Guide/BYOD\\_ISE.html](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_ISE.html)

#### NEW QUESTION 310

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

**Explanation:** Reconnaissance: This is the discovery process used to find information about the network. It could include scans of the network to find out which IP addresses respond, and further scans to see which ports on the devices at these IP addresses are open. This is usually the first step taken, to discover what is on the network and to determine potential vulnerabilities.

Source: Cisco Official Certification Guide, Table 1-5 Attack Methods, p.13

#### NEW QUESTION 311

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

**Explanation:** A false negative, however, is when there is malicious traffic on the network, and for whatever reason the IPS/ IDS did not trigger an alert, so there is no visual indicator (at least from the IPS/IDS system) that anything negative is going on. In the case of a false negative, you must use some third-party or external system to alert you to the problem at hand, such as syslog messages from a network device.

Source: Cisco Official Certification Guide, Positive/Negative Terminology, p.463

#### NEW QUESTION 313

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 210-260 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 210-260 Product From:

<https://www.2passeasy.com/dumps/210-260/>

## Money Back Guarantee

### 210-260 Practice Exam Features:

- \* 210-260 Questions and Answers Updated Frequently
- \* 210-260 Practice Questions Verified by Expert Senior Certified Staff
- \* 210-260 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 210-260 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year