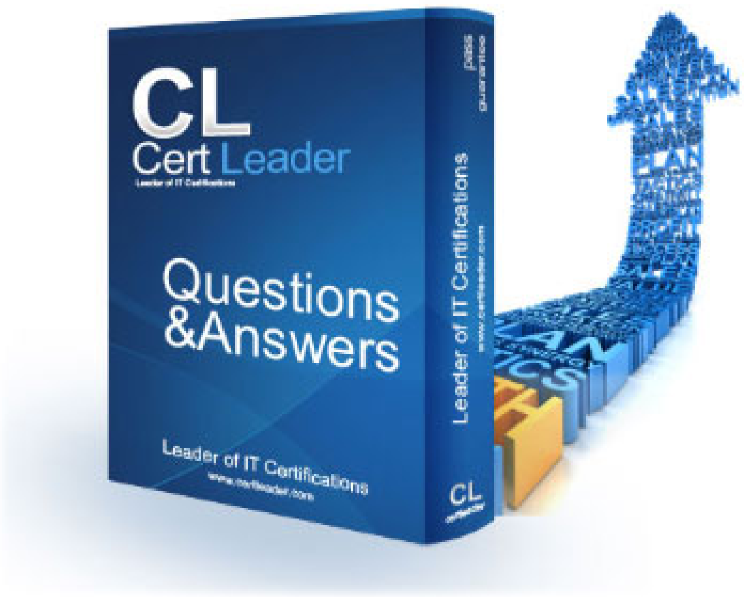
210-260 Dumps

Implementing Cisco Network Security

https://www.certleader.com/210-260-dumps.html



NEW QUESTION 1
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 2
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

NEW QUESTION 3
Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

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

Answer: BCE

Explanation: The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS- CHAPv1.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/ aaa_tacacs.pdf

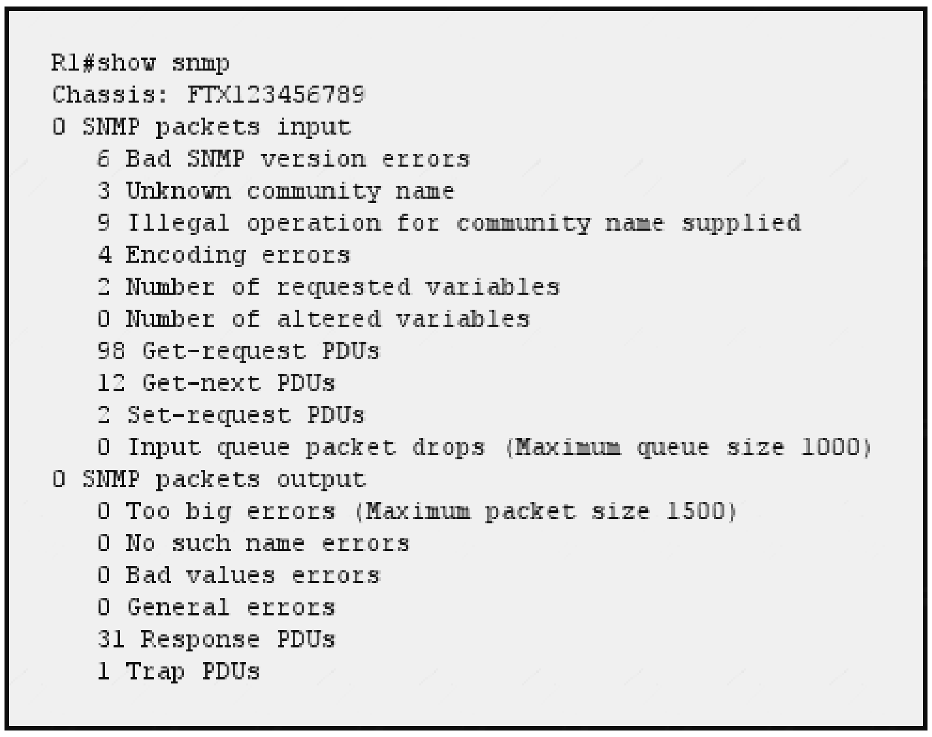
NEW QUESTION 4
What is an advantage of placing an IPS on the inside of a network?

A. It can provide higher throughput.
B. It receives traffic that has already been filtered.
C. It receives every inbound packet.
D. It can provide greater security.

Answer: B

Explanation: Firewalls are generally designed to be on the network perimeter and can handle dropping a lot of the non- legitimate traffic (attacks, scans etc.) very quickly at the ingress interface, often in hardware.
An IDS/IPS is, generally speaking, doing more deep packet inspections and that is a much more computationally expensive undertaking. For that reason, we prefer to filter what gets to it with the firewall line of defense before engaging the IDS/IPS to analyze the traffic flow.
In an even more protected environment, we would also put a first line of defense in ACLs on an edge router between the firewall and the public network(s).
Source: https://supportforums.cisco.com/discussion/12428821/correct-placement-idsips-network-architecture

NEW QUESTION 5
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

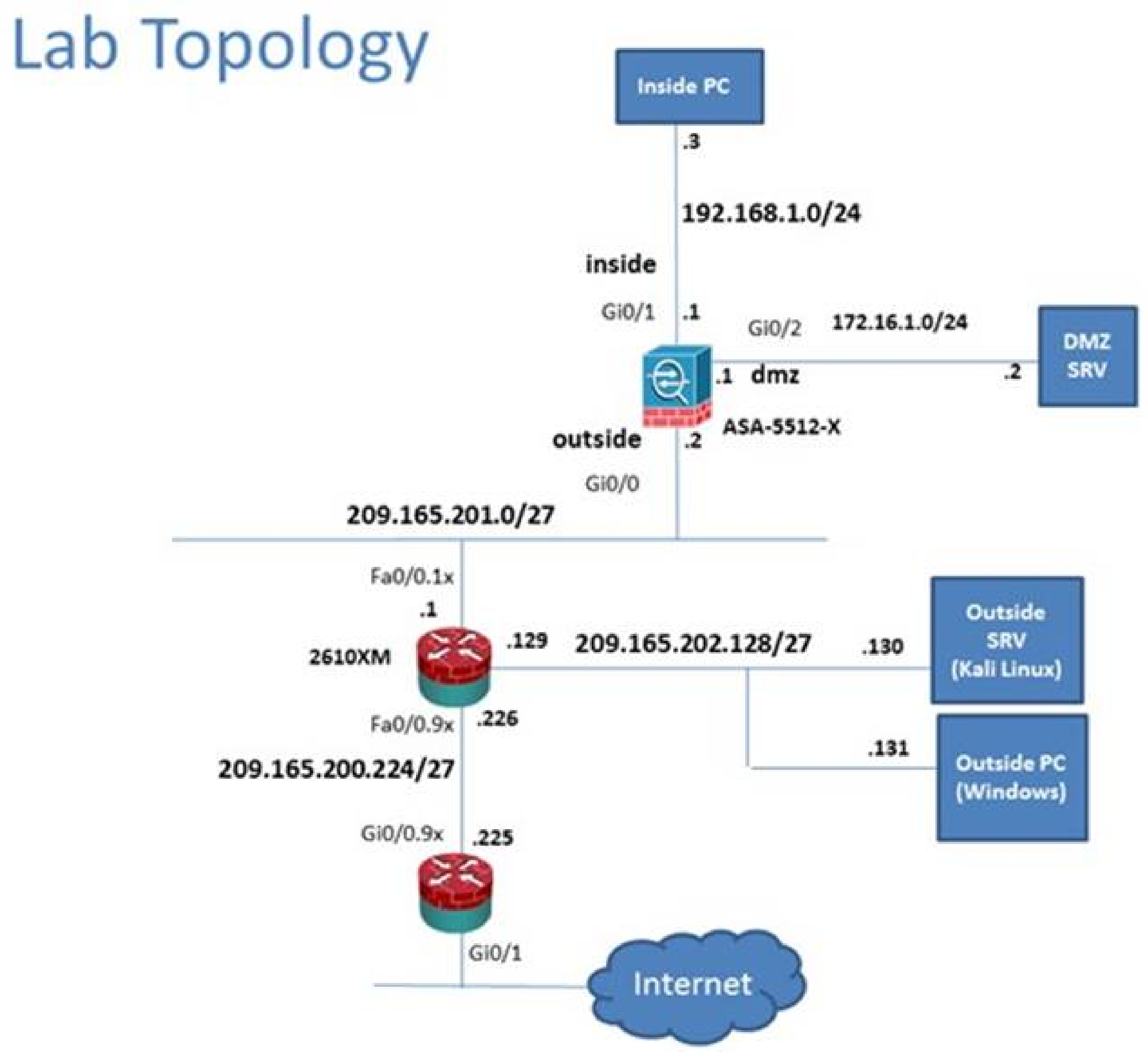
NEW QUESTION 6
What features can protect the data plane? (Choose three.)

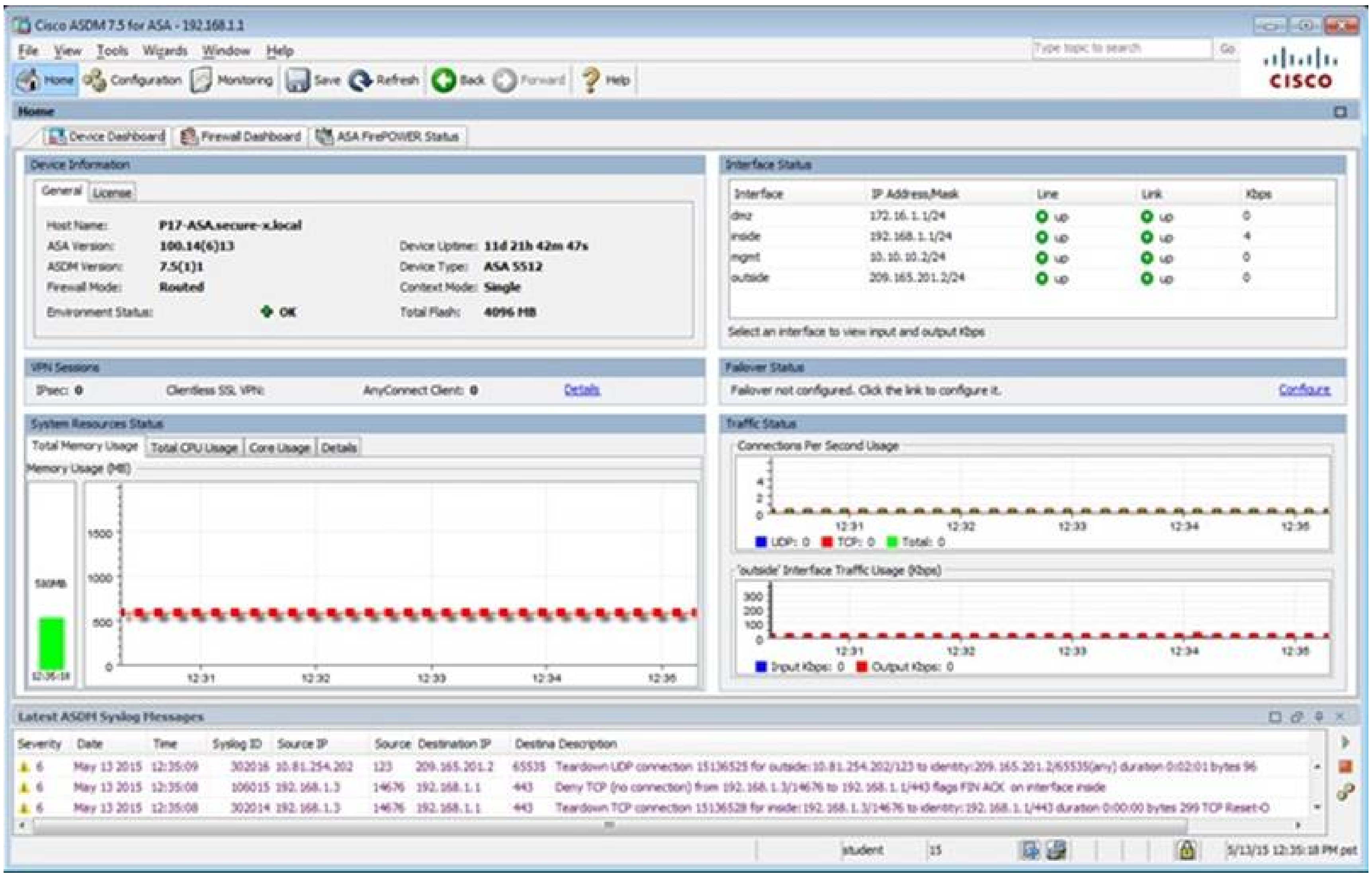
A. policing
B. ACLs
C. IPS
D. antispoofing
E. QoS
F. DHCP-snooping

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 7
Scenario
Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.
New additional connectivity requirements:
Once the correct ASA configurations have been configured: To access ASDM, click the ASA icon in the topology diagram.
To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram. To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram. Note:
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.
In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.




Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
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	Device Uptime:	11d 21h 42m 47s
ASDM Version:	7.5(1)1	Device Type:	ASA 5512
Firewall Mode:	Routed	Context Mode:	Single
Environment Status:	OK	Total Flash:	4096 MB

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

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

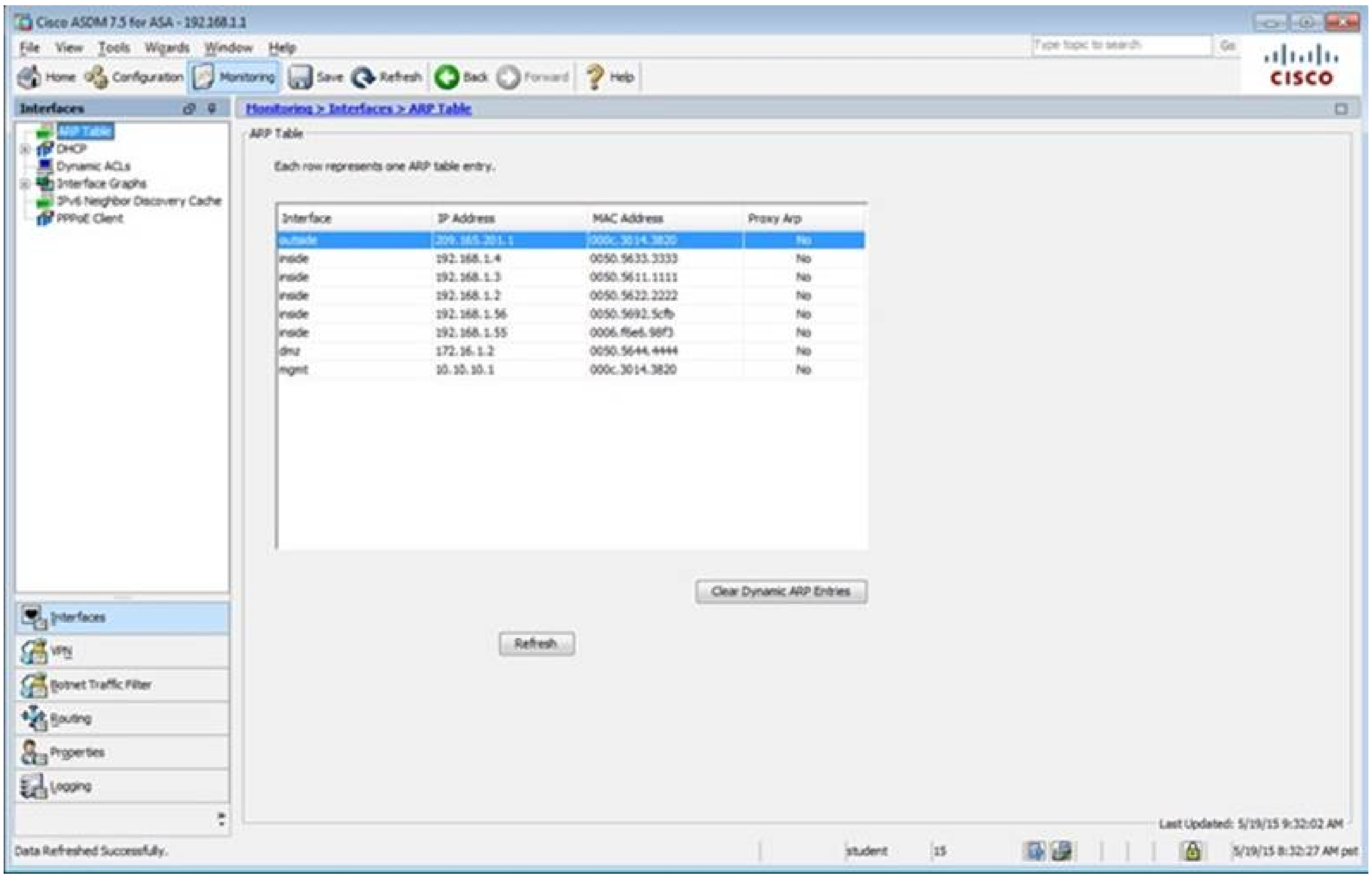
Failover Status

Failover not configured. Click the link to configure it. Configure

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 pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Clear Dynamic ARP Entries
Refresh

Monitoring > Interfaces > ARP Table

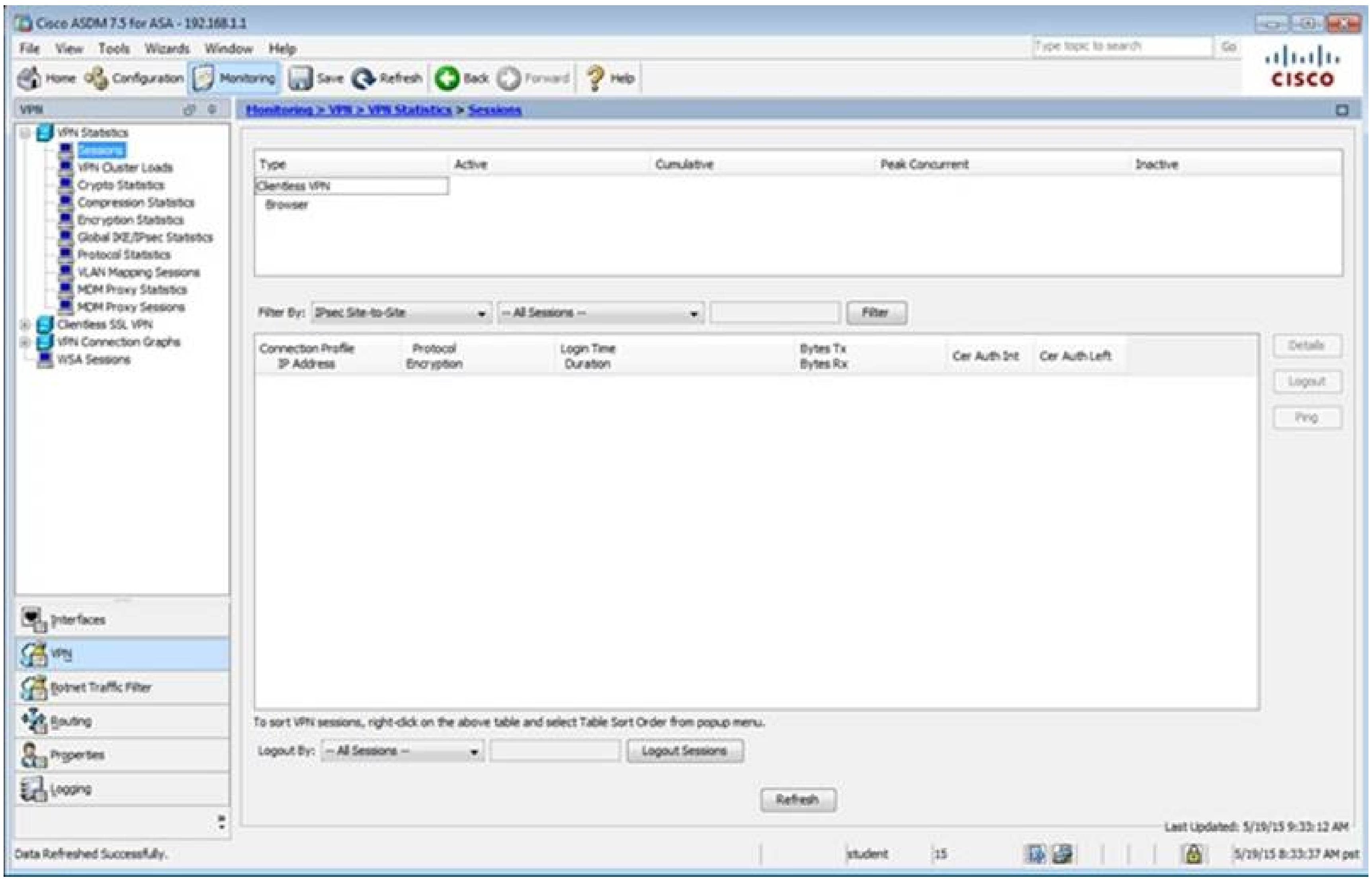
ARP Table

Each row represents one ARP table entry.

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

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

Data Refreshed Successfully. student 15 5/19/15 8:32:27 AM pst



Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN				
Browser				

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

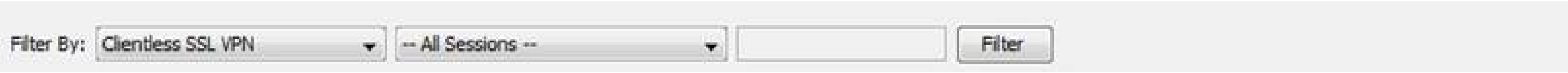
Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left

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

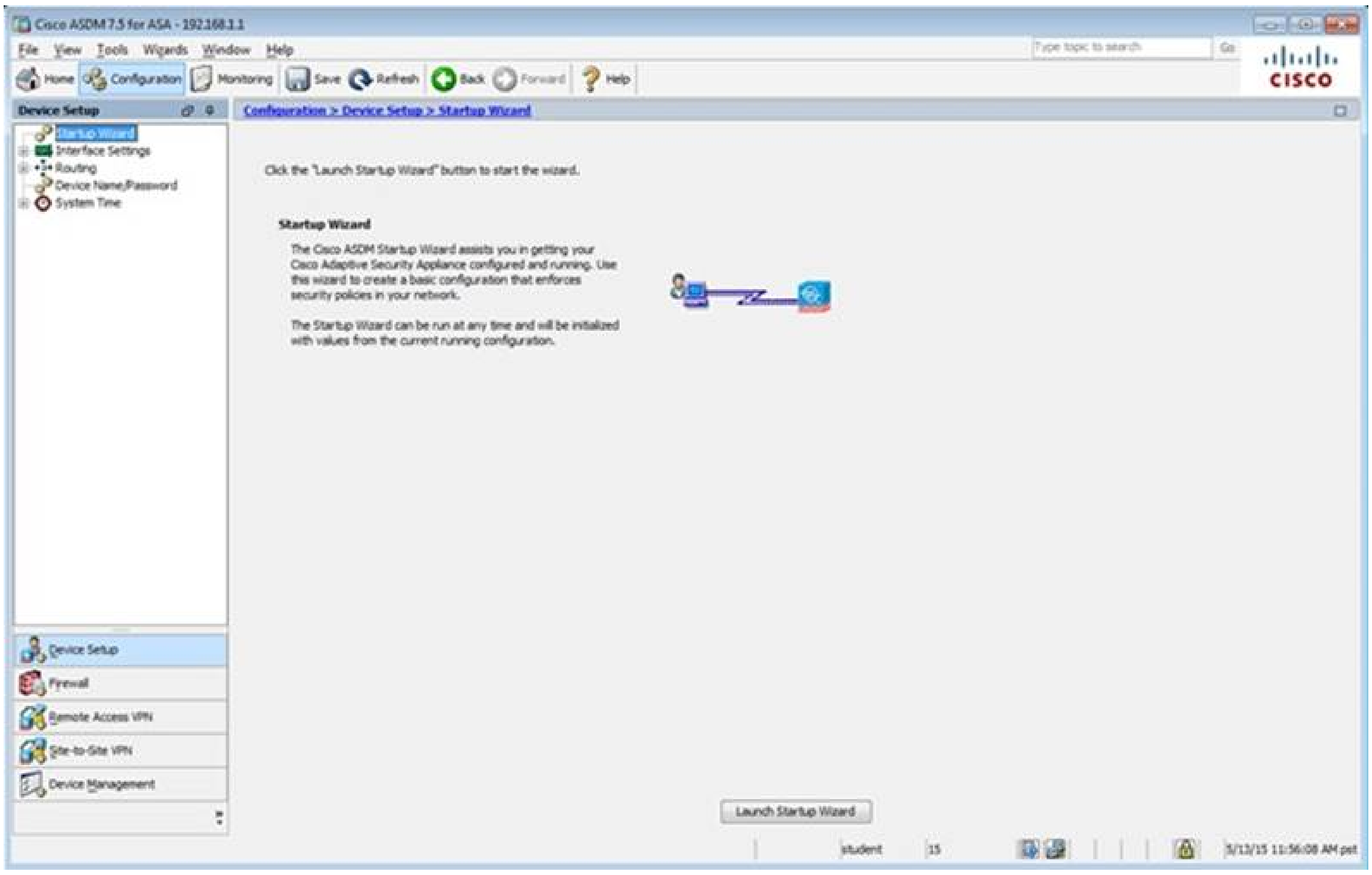
Logout By: -- All Sessions --

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

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



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



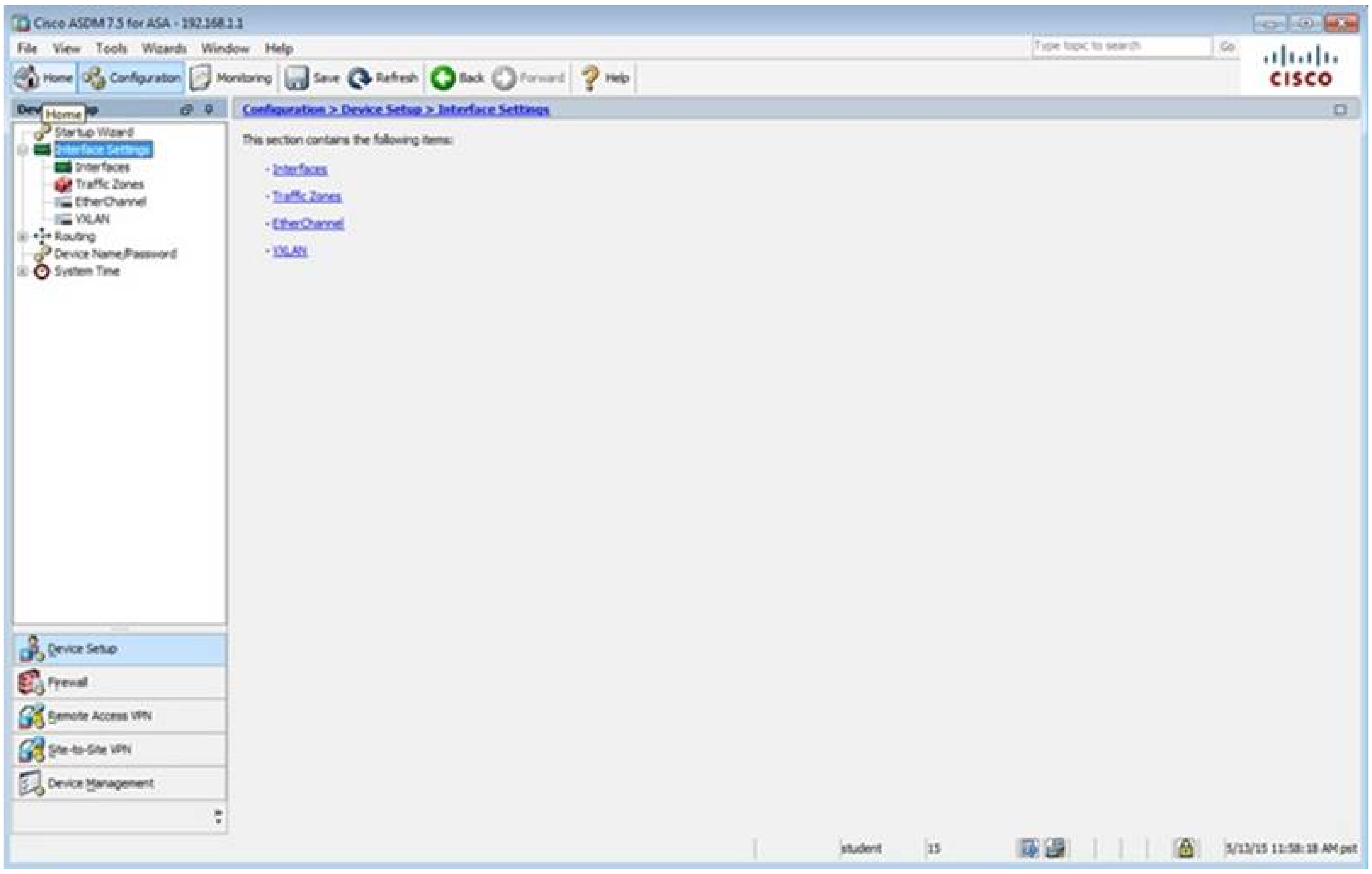
Configuration > Device Setup > Startup Wizard

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.

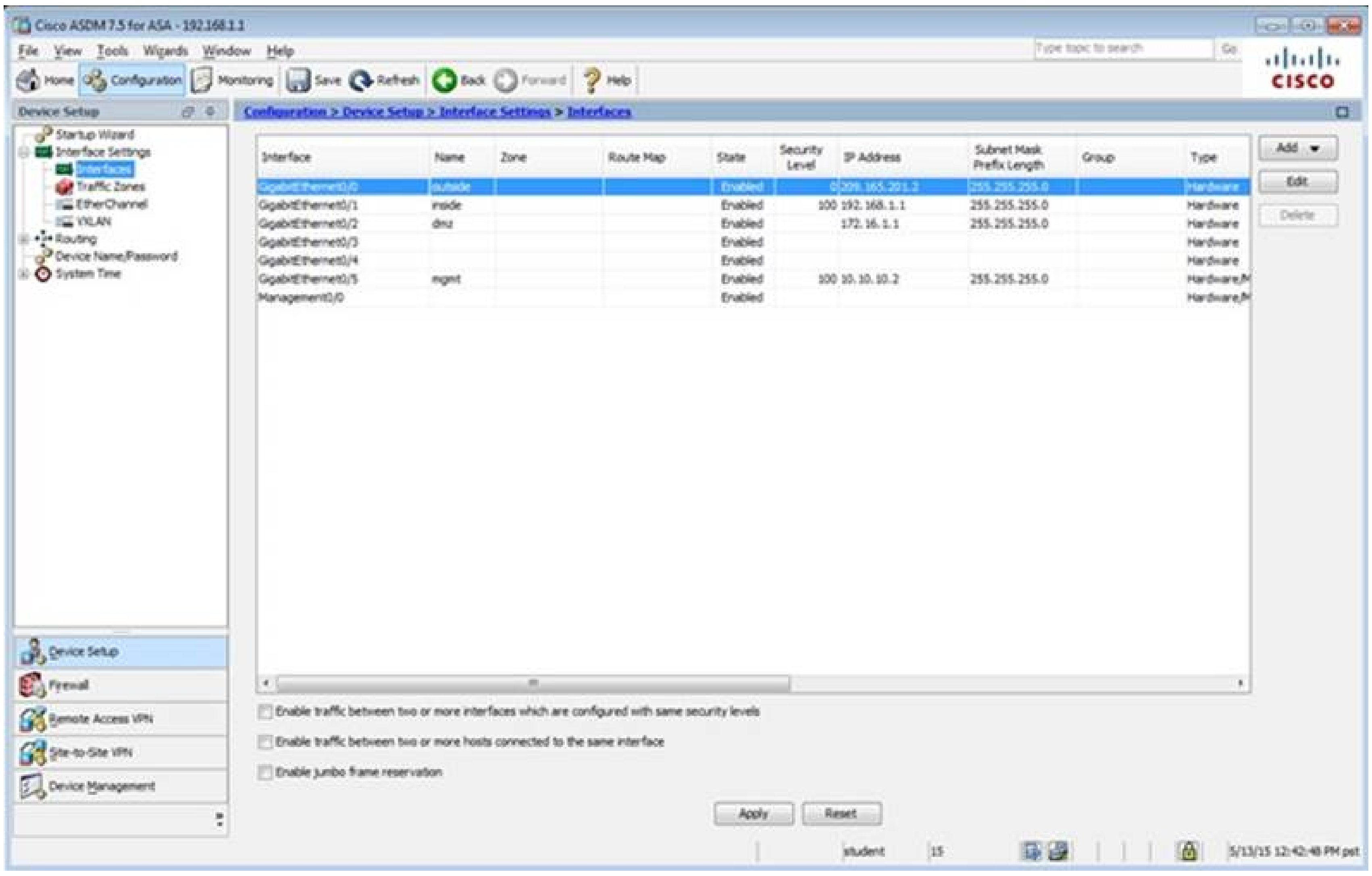
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.



Configuration > Device Setup > Interface Settings

This section contains the following items:

- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN



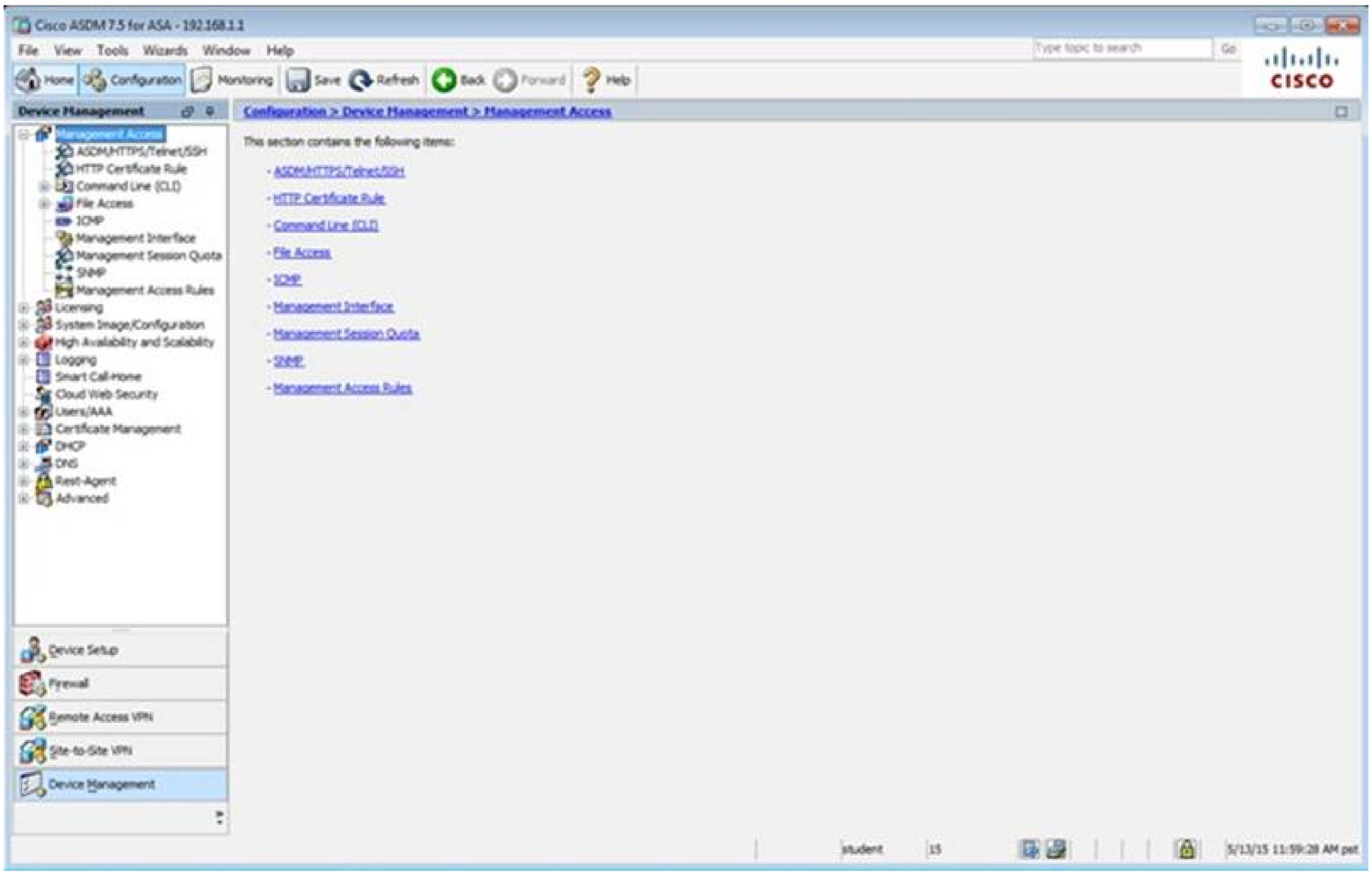
Configuration > Device Setup > Interface Settings > Interfaces

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

□ 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

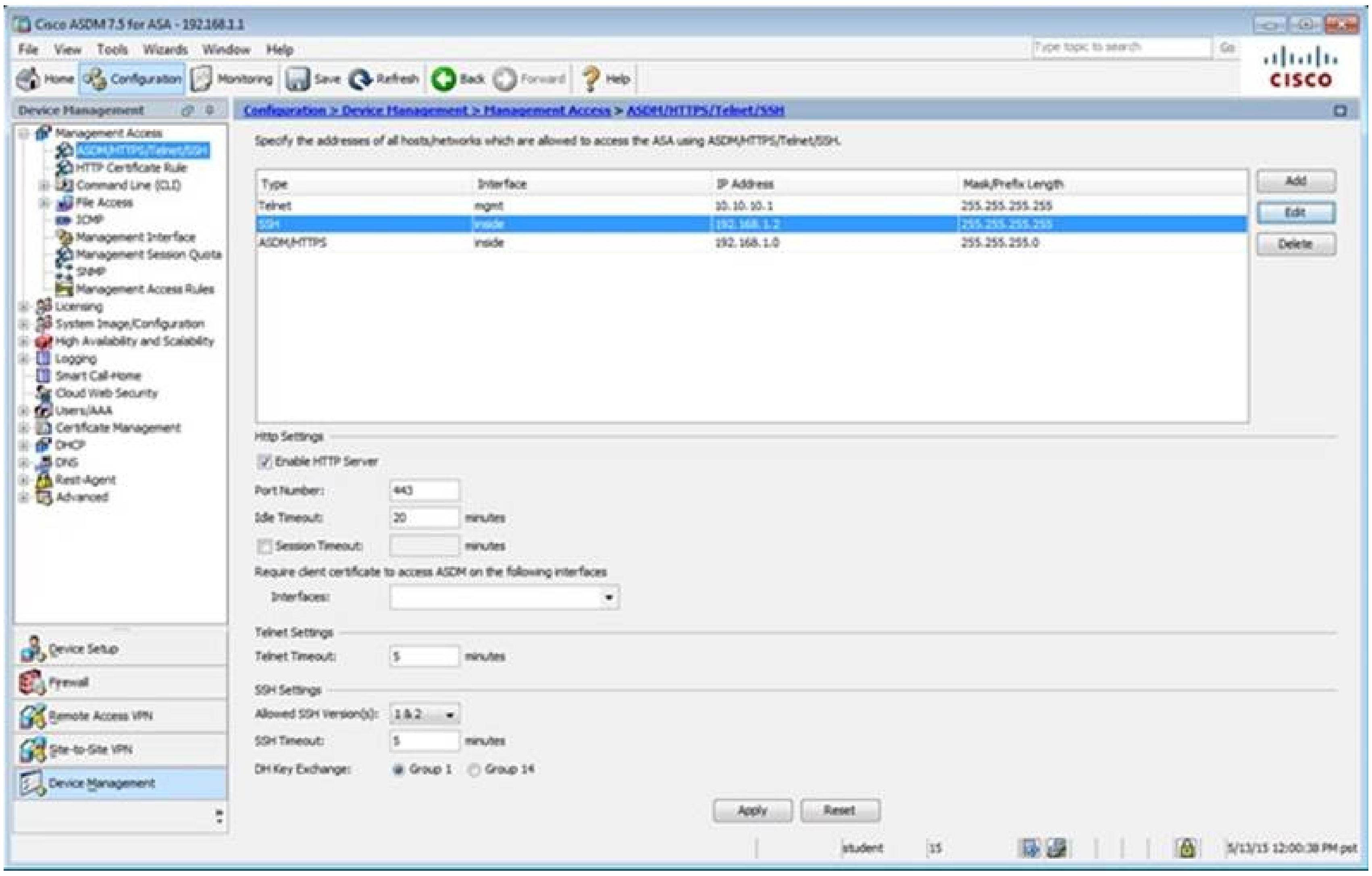
□ Enable jumbo frame reservation



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



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

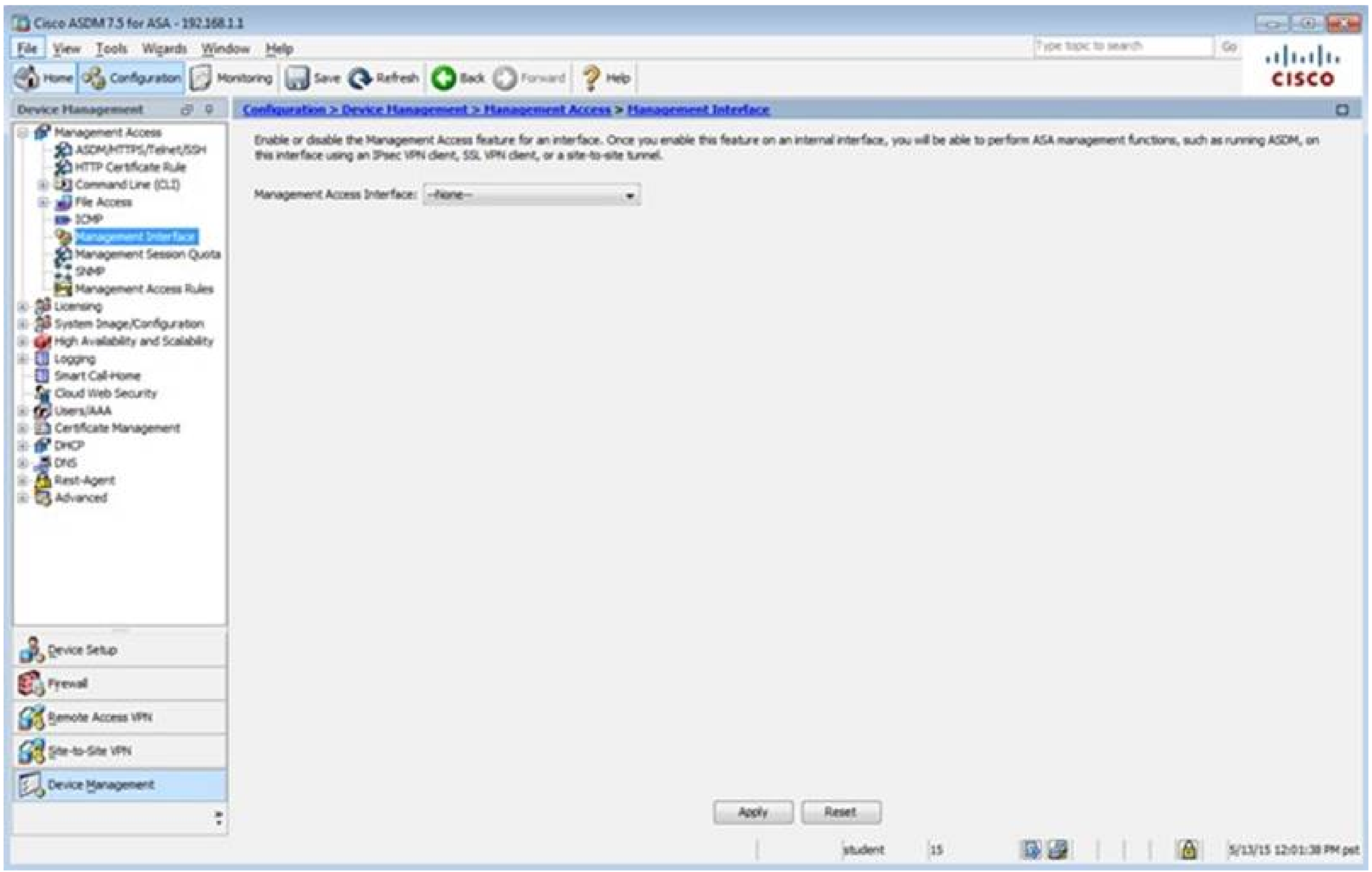
Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

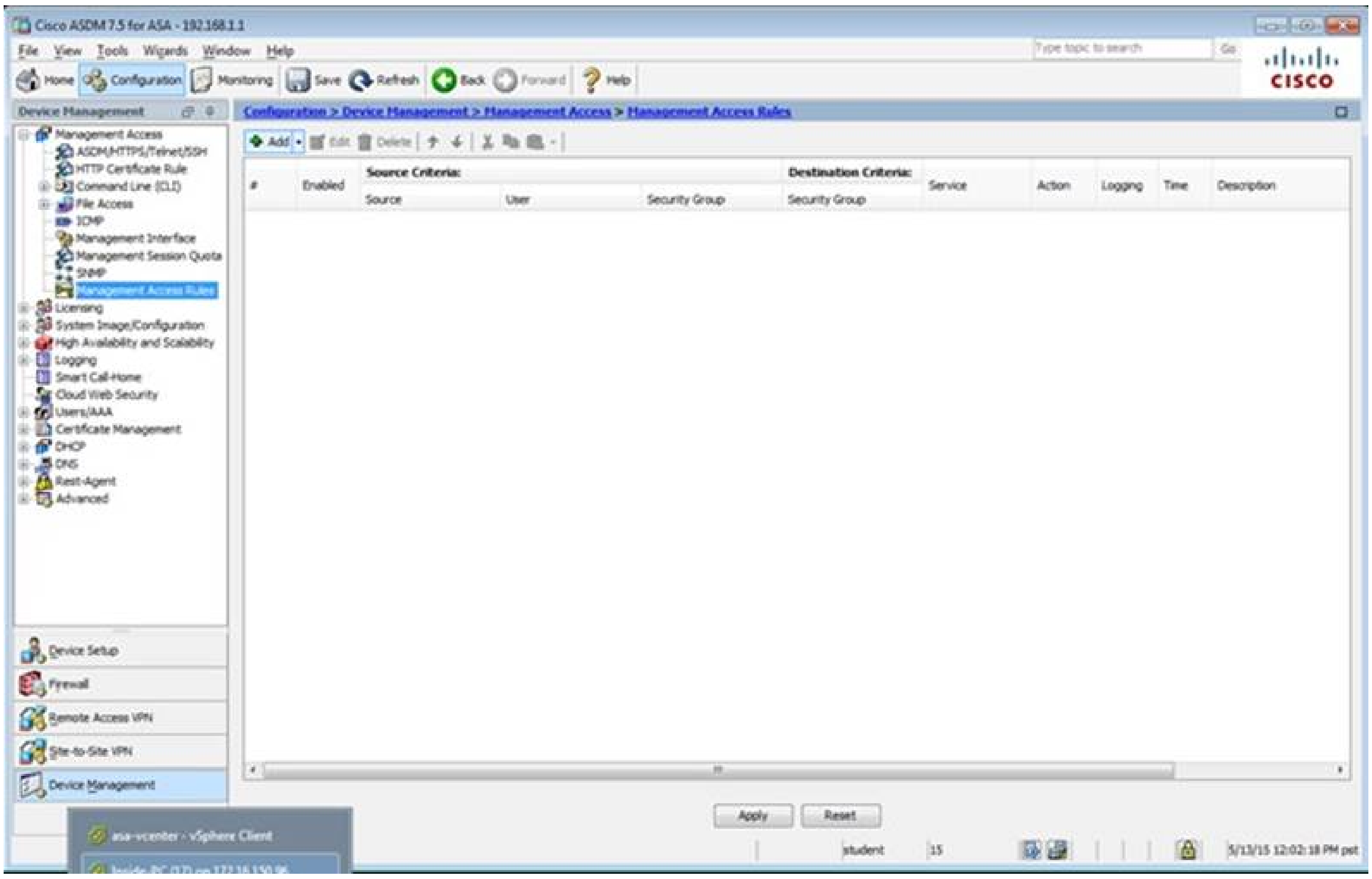
DH Key Exchange: ● Group 1 ○ Group 14

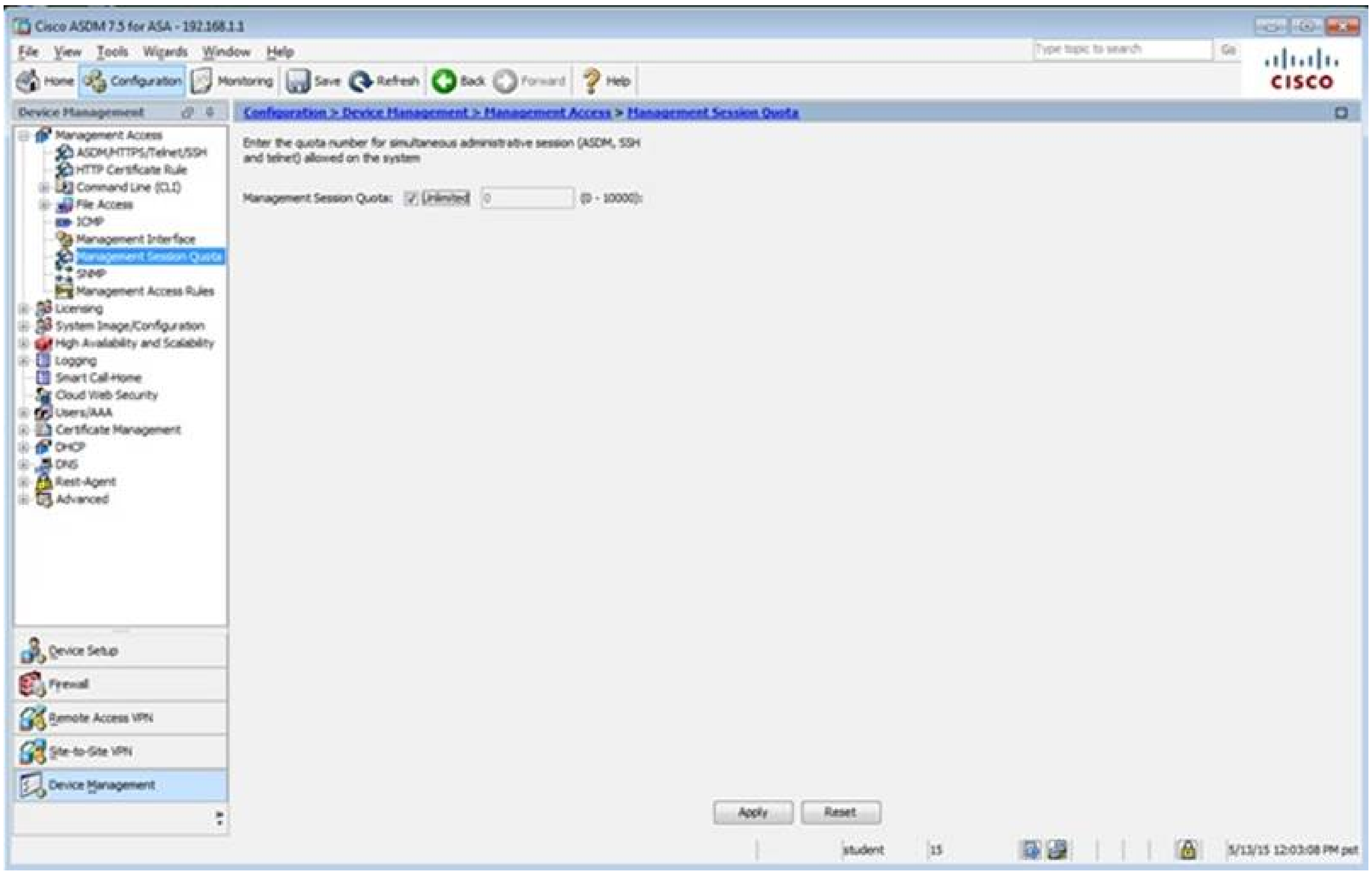


Configuration > Device Management > Management Access > Management Interface

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.

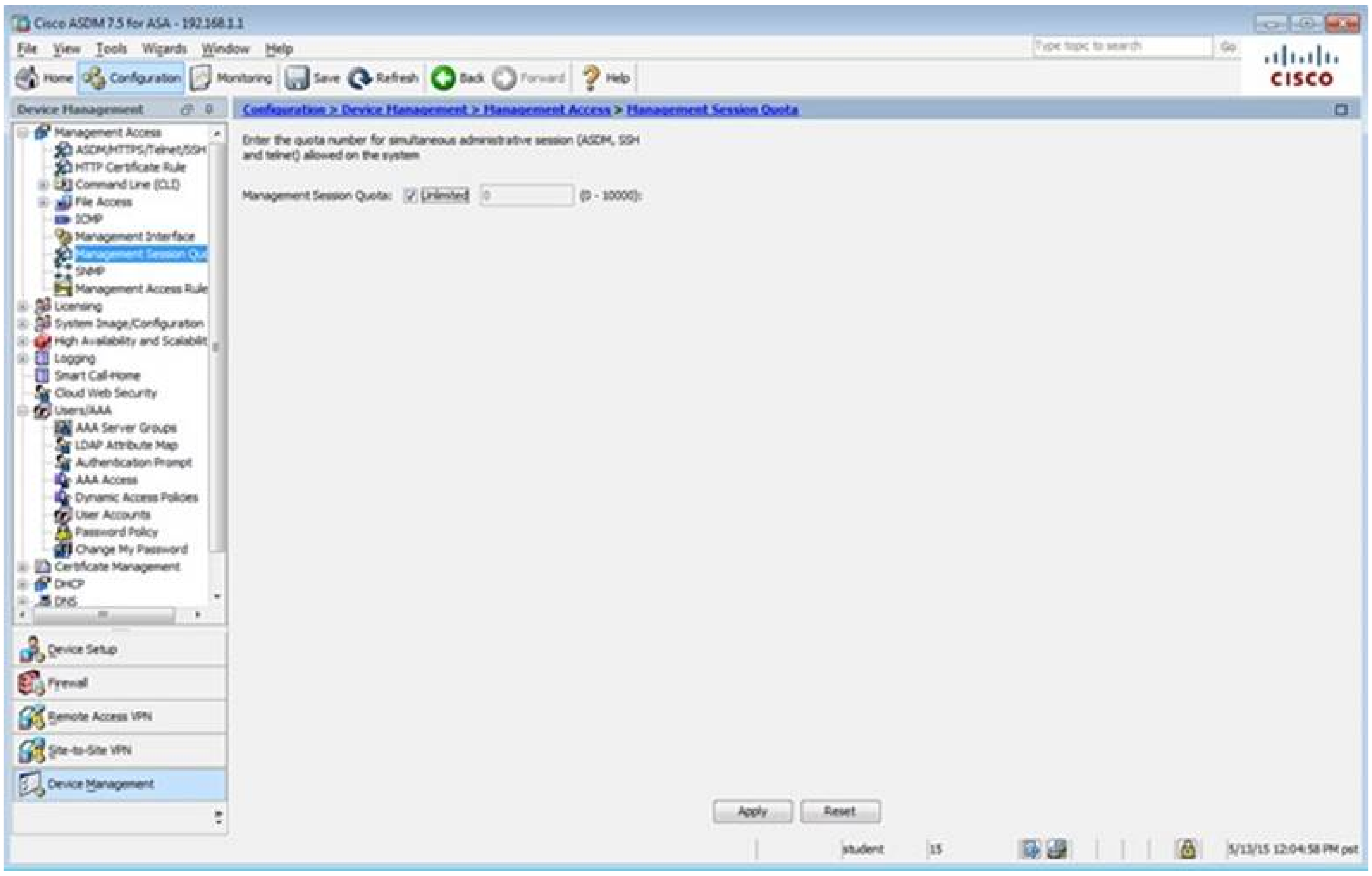
Management Access Interface: --None--


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 Access Rules
Add Edit Delete
# Enabled Source Criteria: Source User Security Group Destination Criteria: Security Group Service Action Logging Time Description
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quota
SNMP
Management Access Rules
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
DHCP
DNS
Rest-Agent
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
asa-vcenter - vSphere Client
student
15
5/13/15 12:02:18 PM pdt



Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

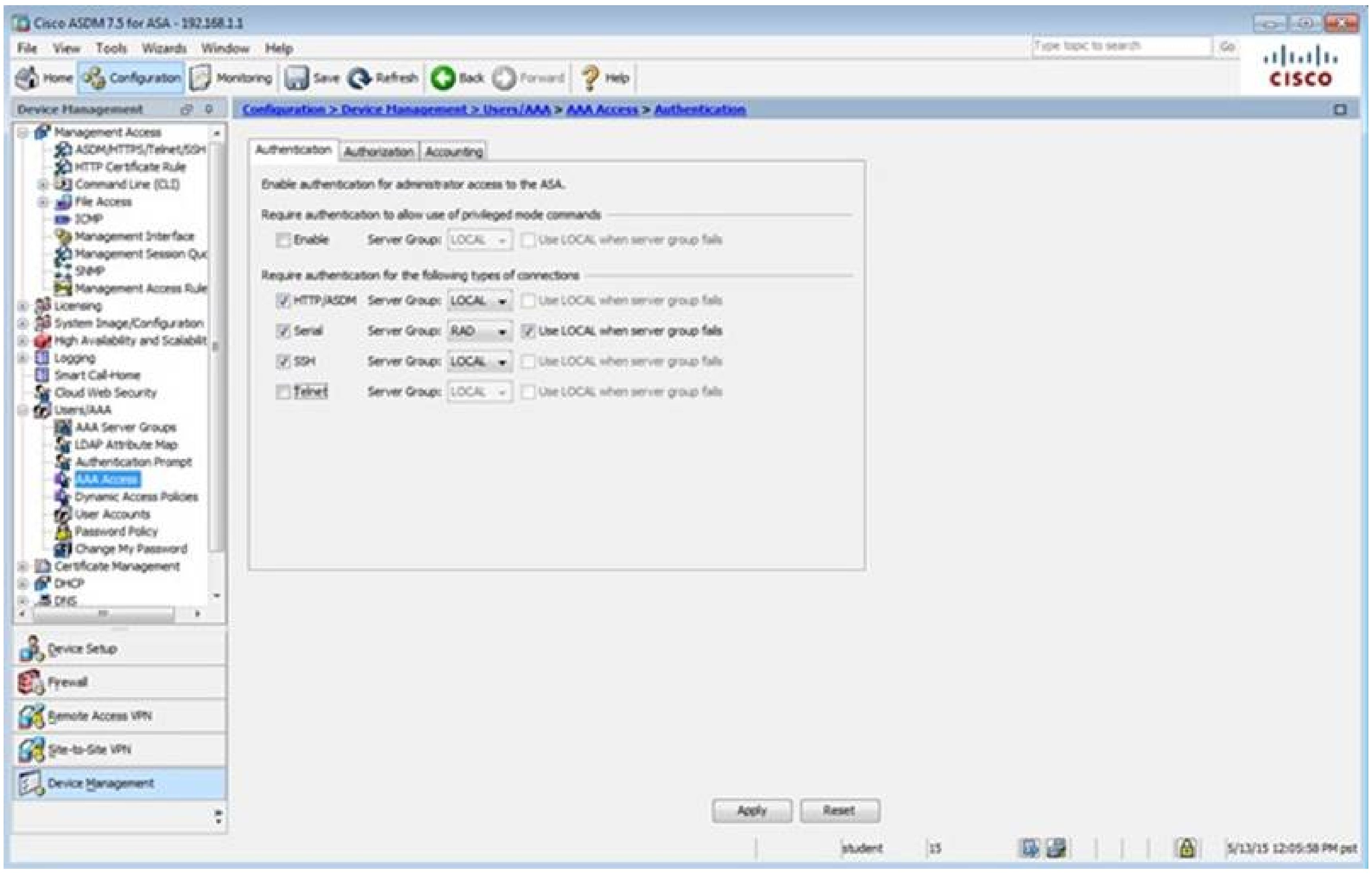
Management Session Quota: ☑ Unlimited 0 (0 - 10000):



Configuration > Device Management > Management Access > Management Session Quota

Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

Management Session Quota: ☑ Unlimited 0 (0 - 10000):



Configuration > Device Management > Users/AAA > AAA Access > Authentication

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

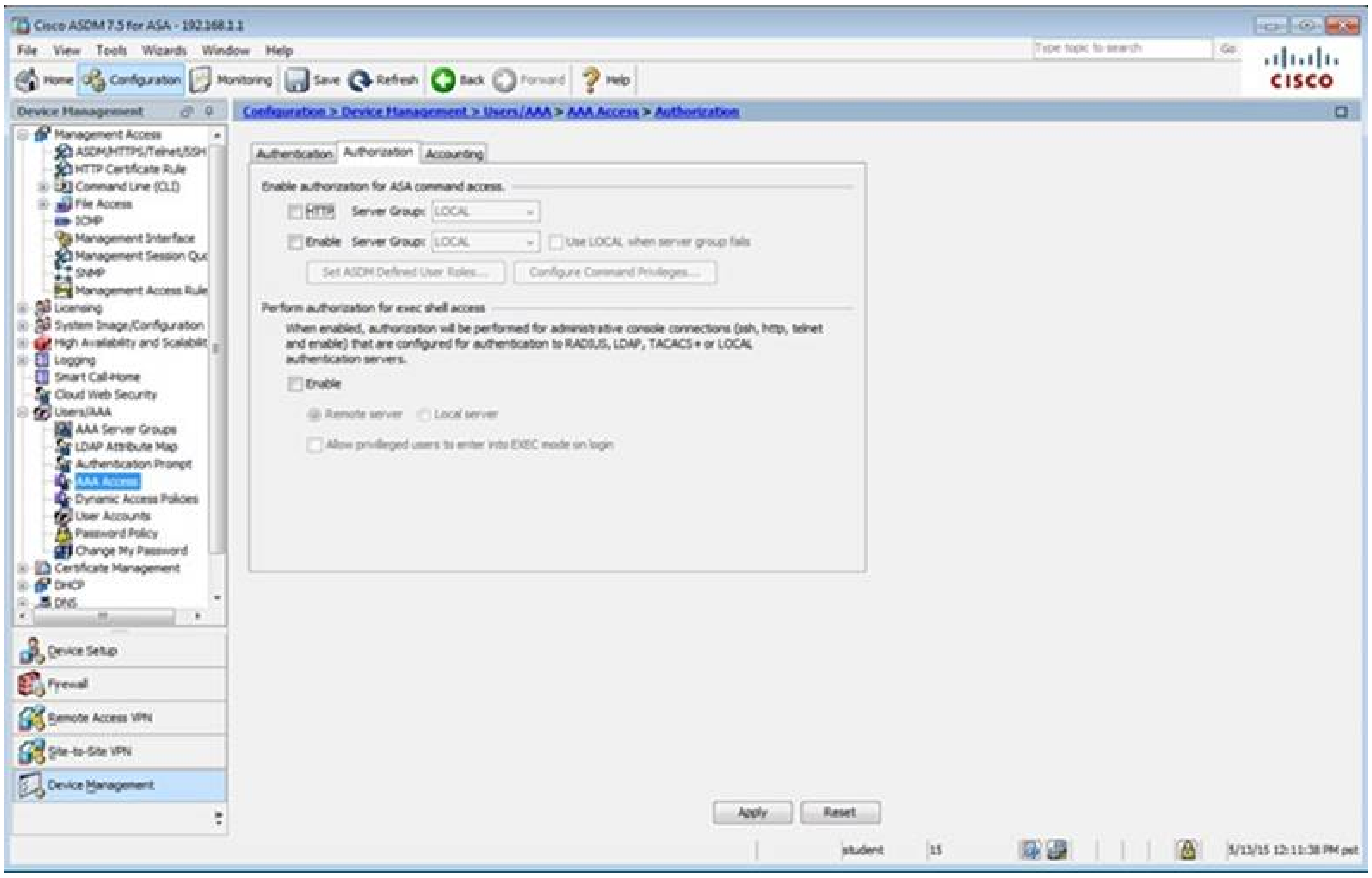
Require authentication for the following types of connections

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

☑ Serial Server Group: RAD ☑ Use LOCAL when server group fails

☑ SSH Server Group: LOCAL □ Use LOCAL when server group fails

□ Telnet Server Group: LOCAL □ Use LOCAL when server group fails



Configuration > Device Management > Users/AAA > AAA Access > Authorization

Authentication | Authorization | Accounting

Enable authorization for ASA command access.

□ HTTP Server Group: LOCAL

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Set ASDM Defined User Roles... Configure Command Privileges...

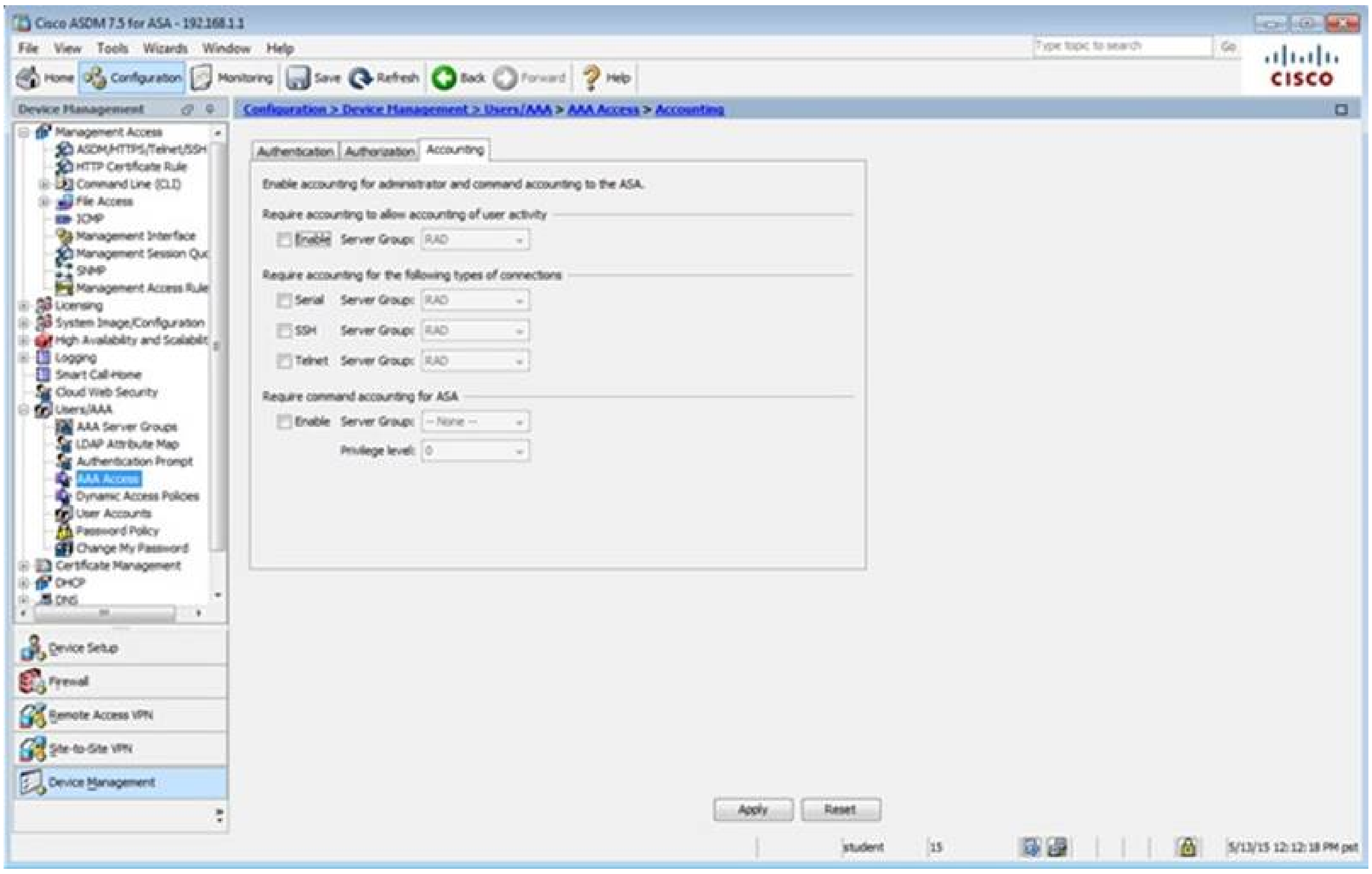
Perform authorization for exec shell access

When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.

□ Enable

● Remote server ○ Local server

□ Allow privileged users to enter into EXEC mode on login



Configuration > Device Management > Users/AAA > AAA Access > Accounting

Authentication | Authorization | Accounting

Enable accounting for administrator and command accounting to the ASA.

Require accounting to allow accounting of user activity

□ Enable Server Group: RAD

Require accounting for the following types of connections

□ Serial Server Group: RAD

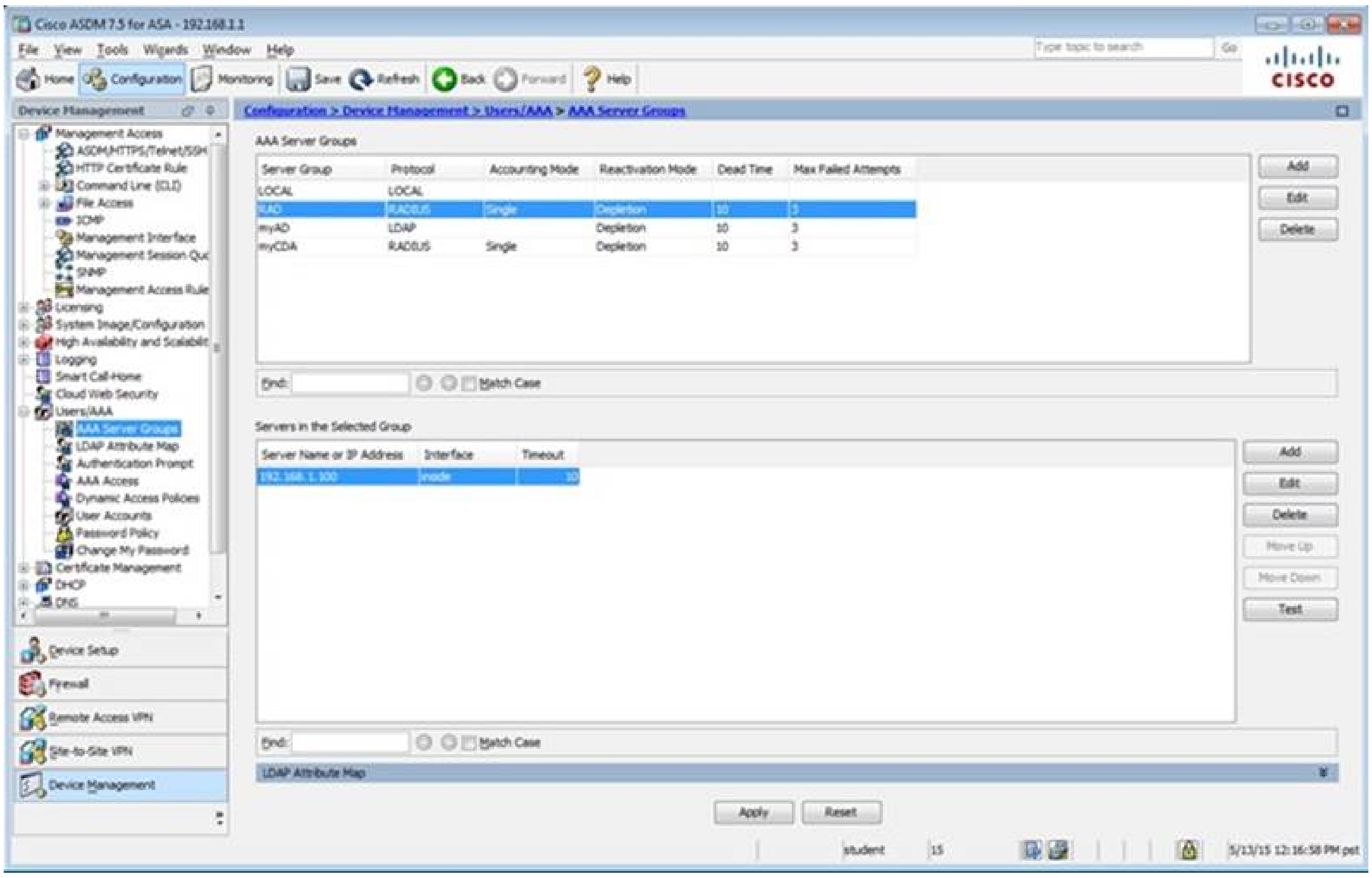
□ SSH Server Group: RAD

□ Telnet Server Group: RAD

Require command accounting for ASA

□ Enable Server Group: -- None --

Privilege level: 0



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

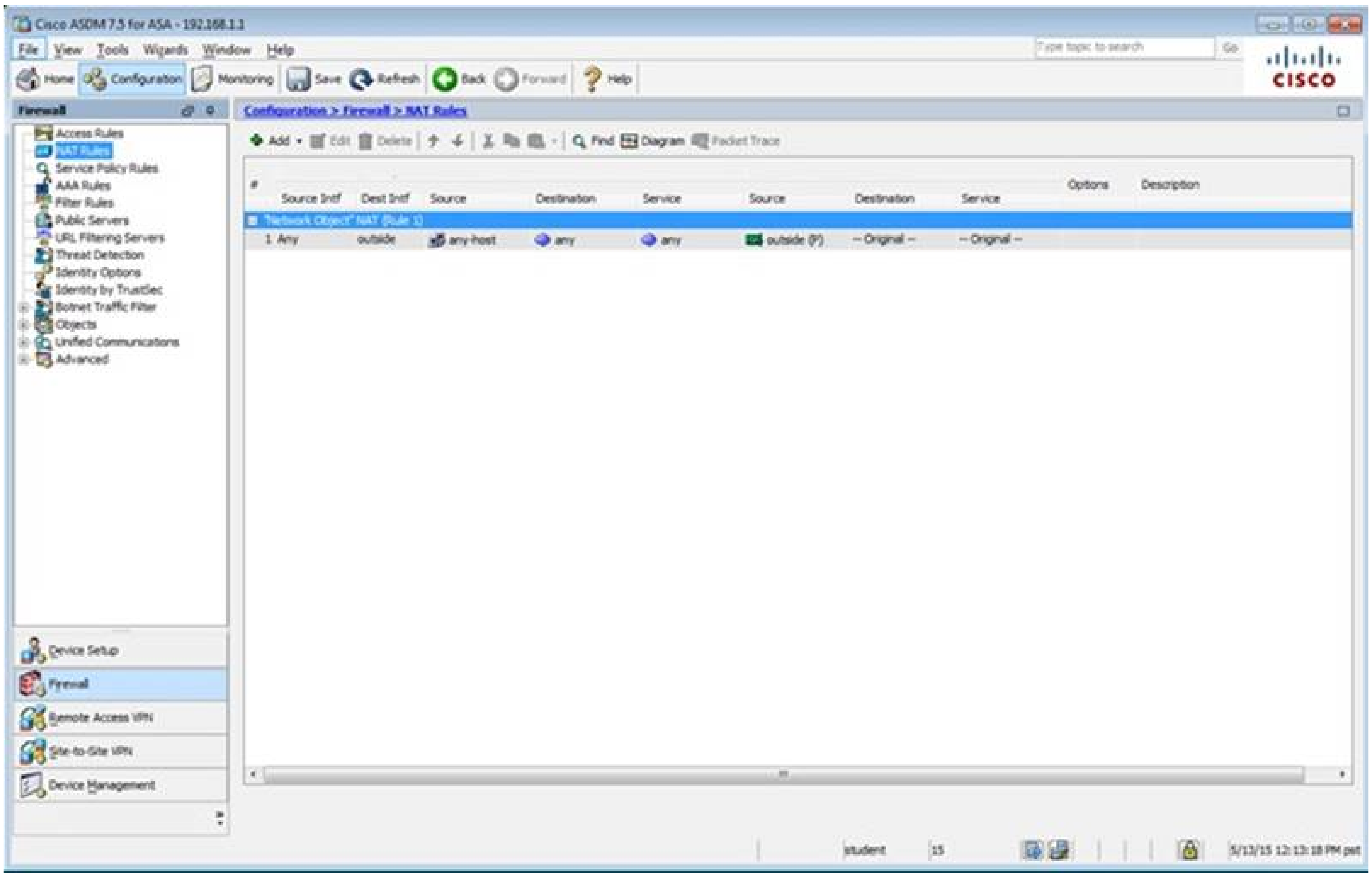
AAA Server Groups

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

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.1.100	inside	10

student 15 5/13/15 12:16:58 PM pst

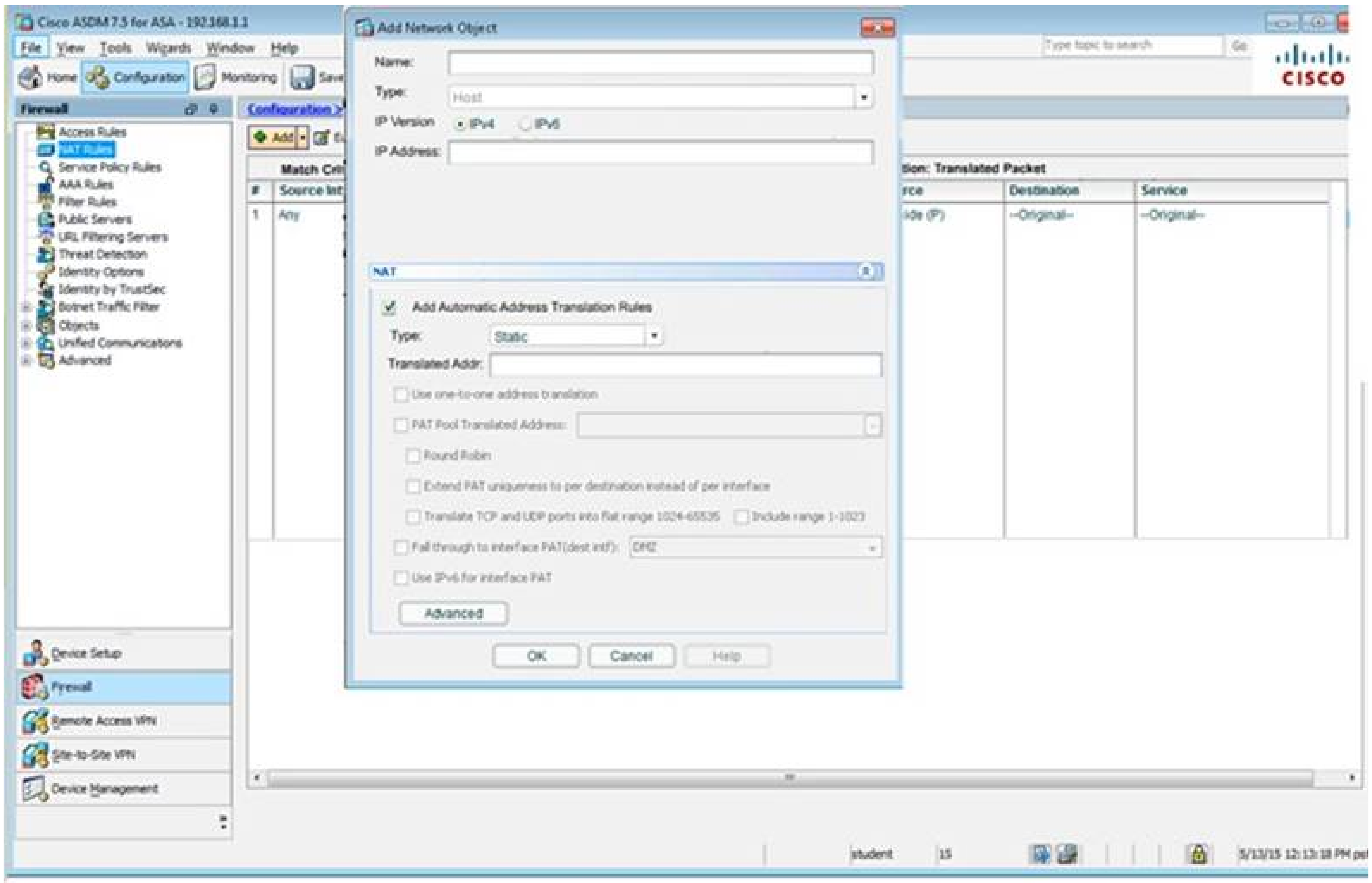


Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > NAT Rules

#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Options	Description
"Network Object" NAT (Rule 1)										
1	Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		

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



Add Network Object

Name:

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address:

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr:

□ Use one-to-one address translation

□ PAT Pool Translated Address:

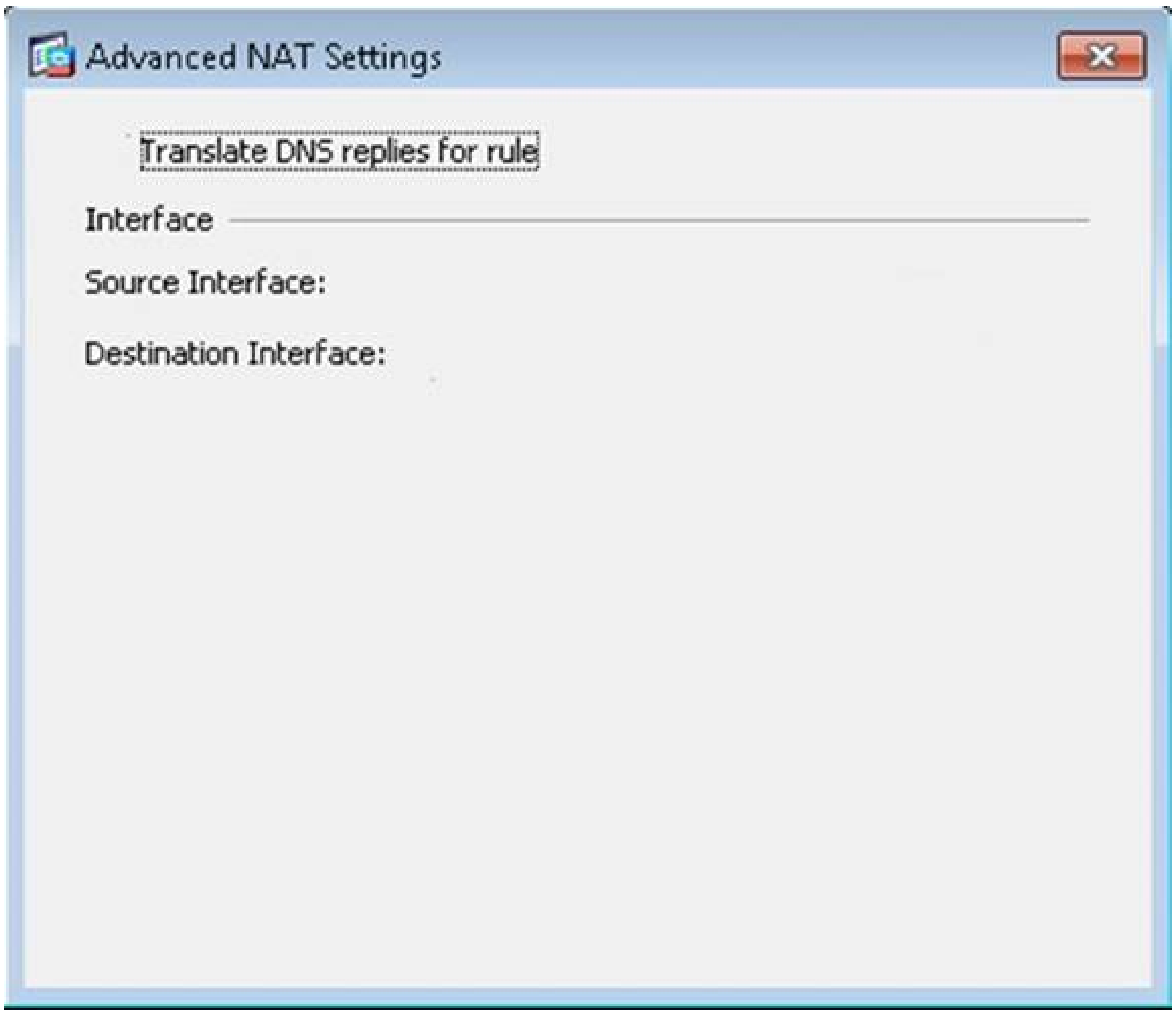
□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

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

□ Fall through to interface PAT(dest intf): DMZ

□ Use IPv6 for interface PAT

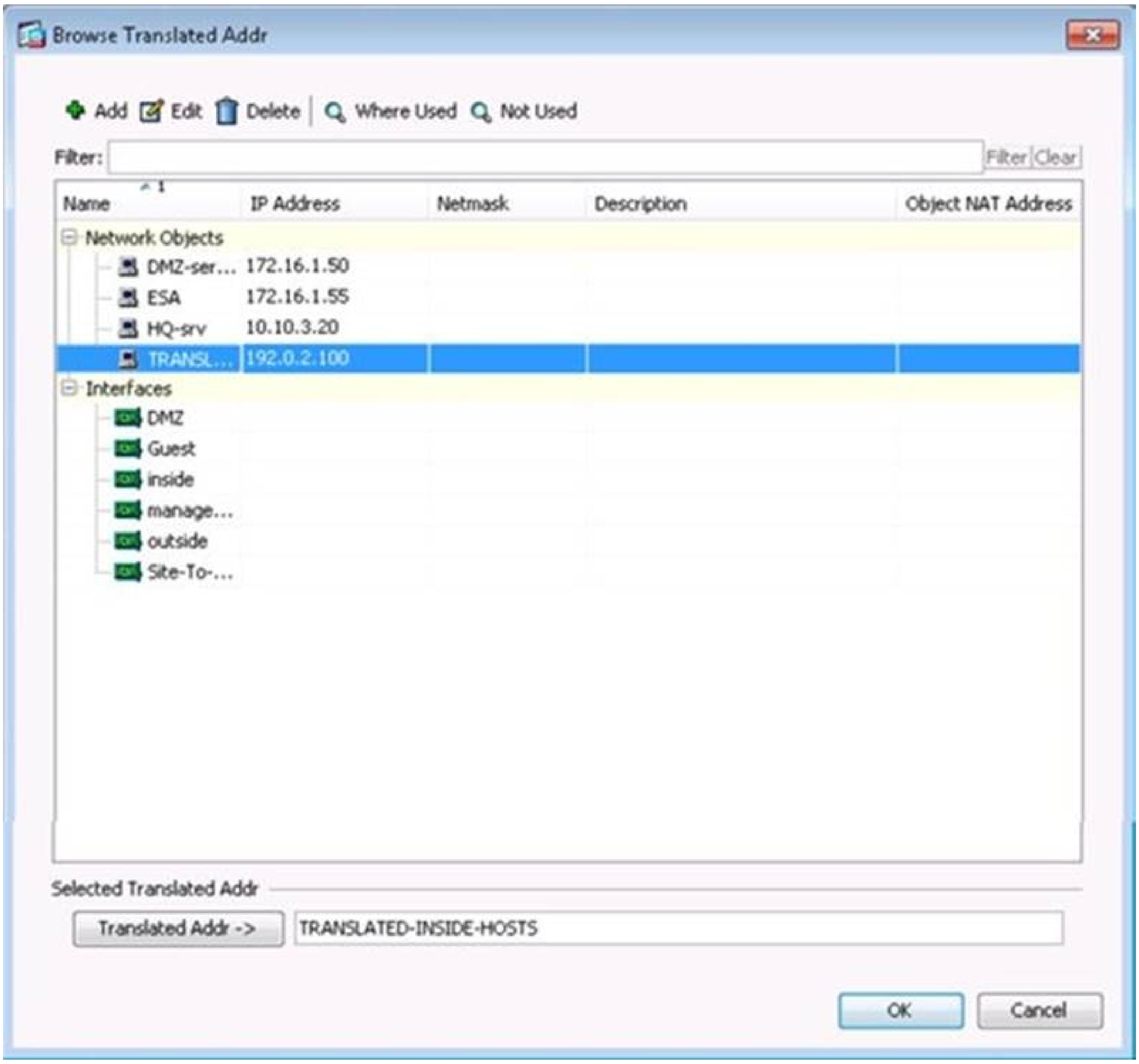

Advanced NAT Settings

Translate DNS replies for rule

Interface

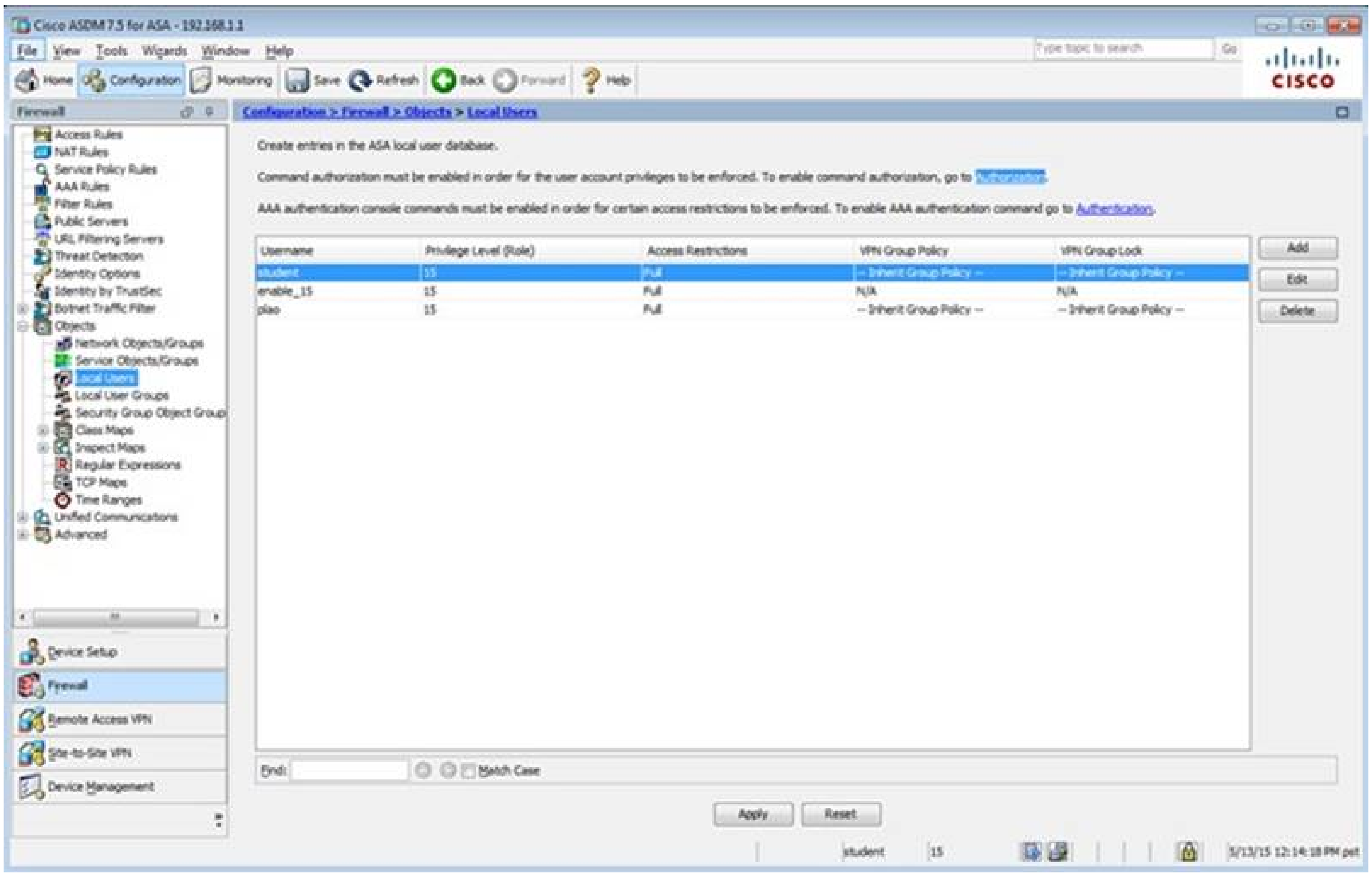
Source Interface:

Destination Interface:



Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
DMZ-ser...	172.16.1.50			
ESA	172.16.1.55			
HQ-srv	10.10.3.20			
TRANSL...	192.0.2.100			
Interfaces				
DMZ				
Guest				
inside				
manage...				
outside				
Site-To-...				

Translated Addr -> TRANSLATED-INSIDE-HOSTS



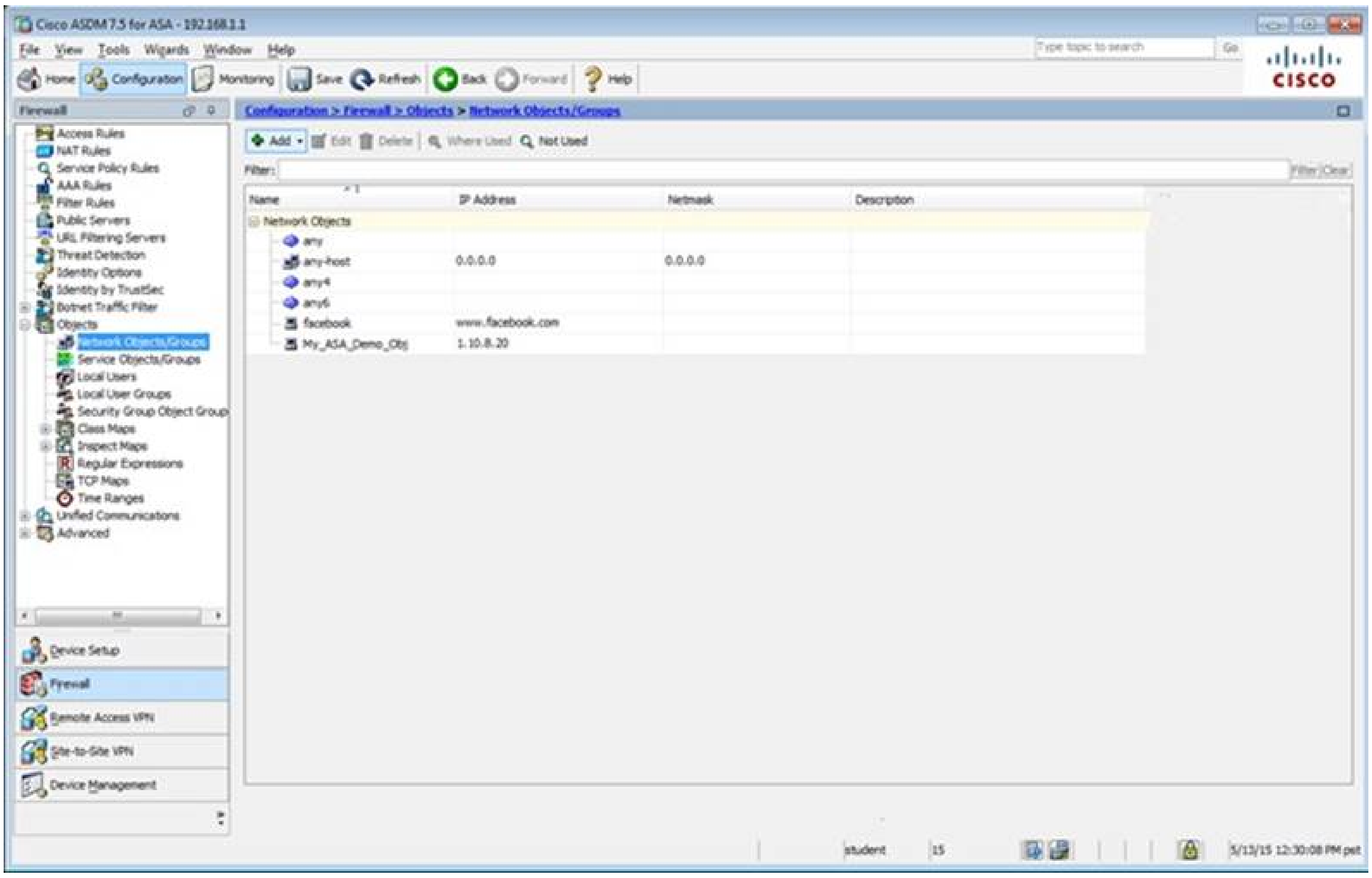
Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

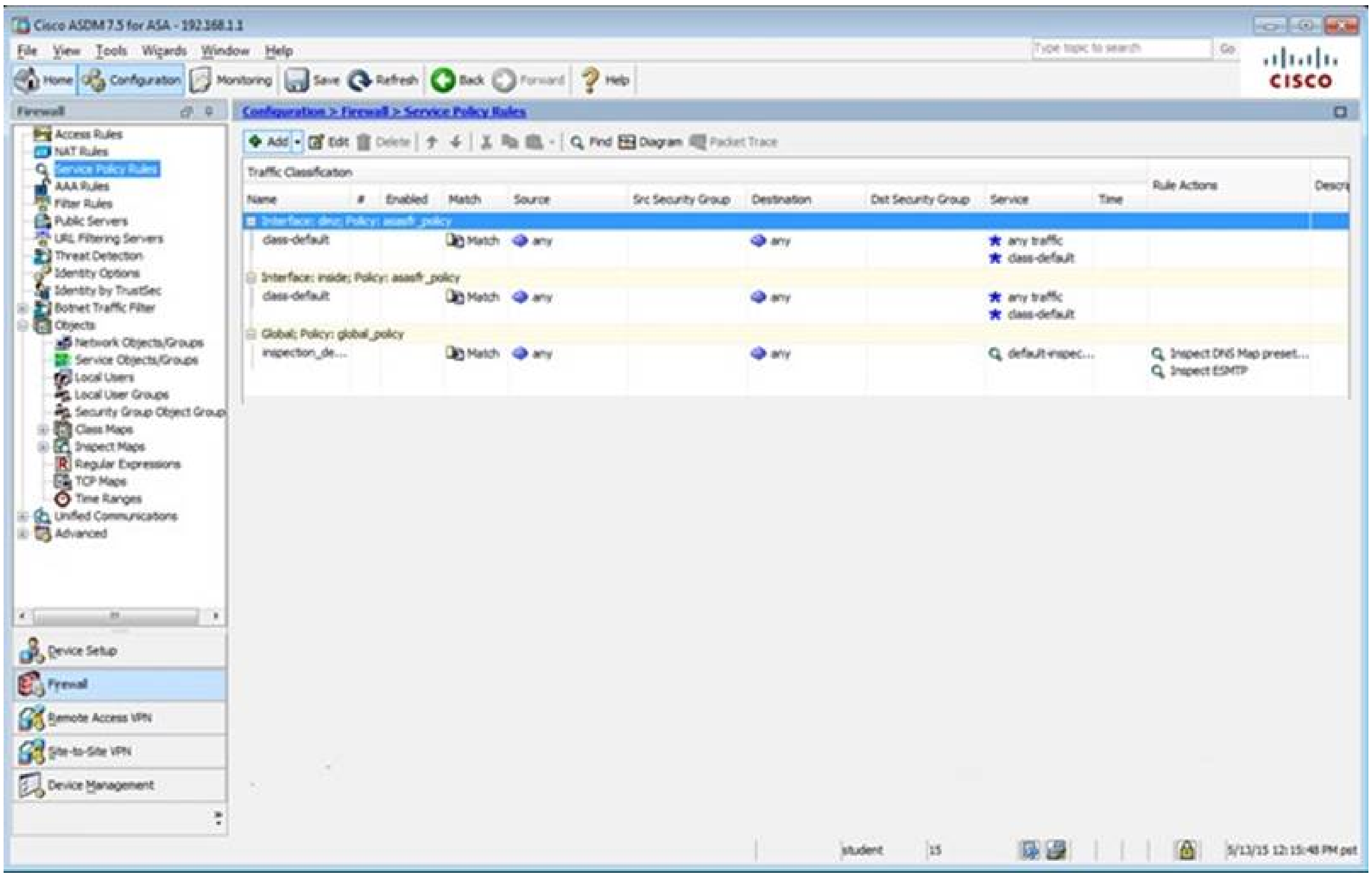
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

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



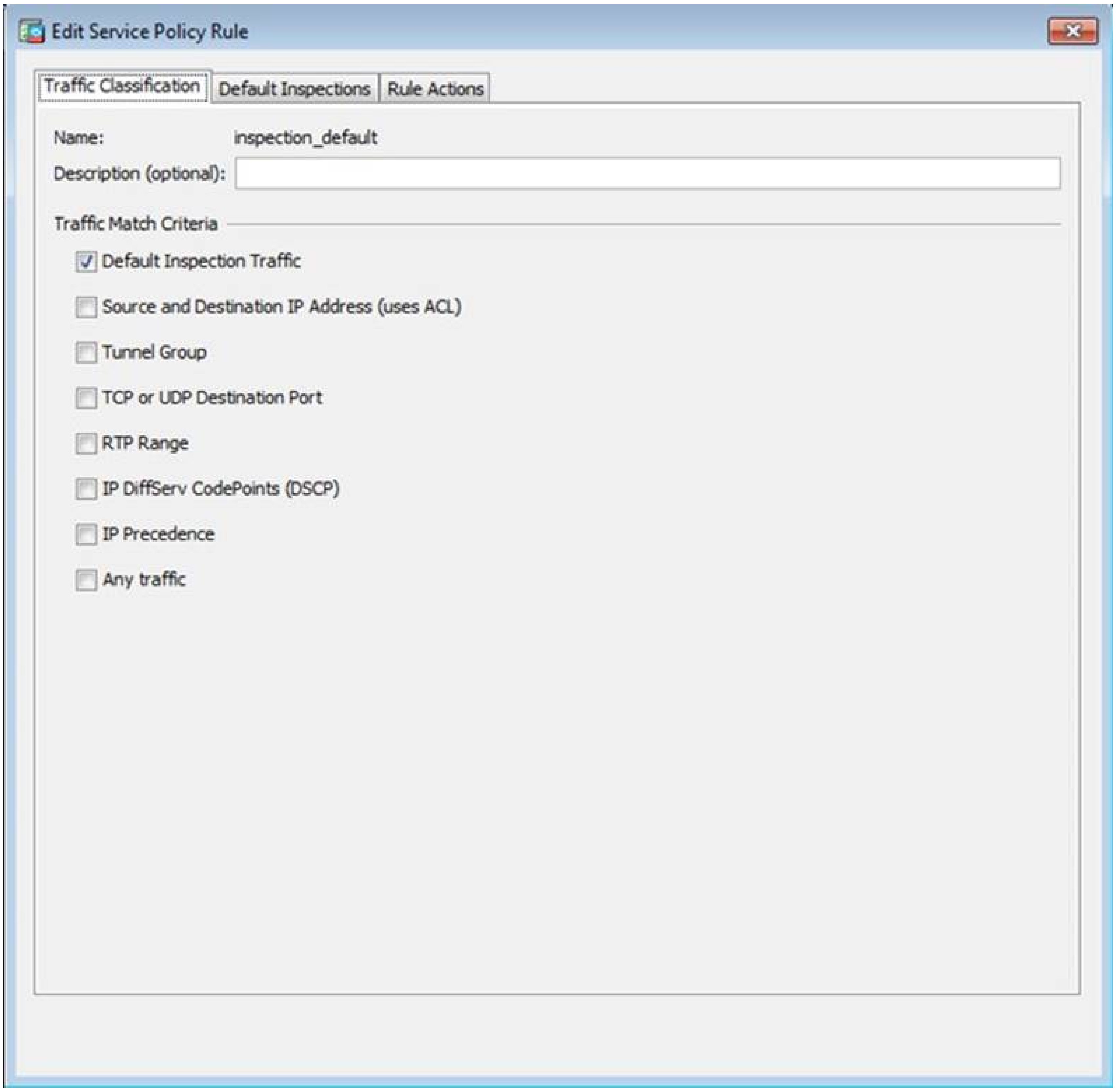
Configuration > Firewall > Objects > Network Objects/Groups

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



Configuration > Firewall > Service Policy Rules

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



Edit Service Policy Rule

Name: inspection_default

Description (optional):

Traffic Match Criteria

☑ Default Inspection Traffic

□ Source and Destination IP Address (uses ACL)

□ Tunnel Group

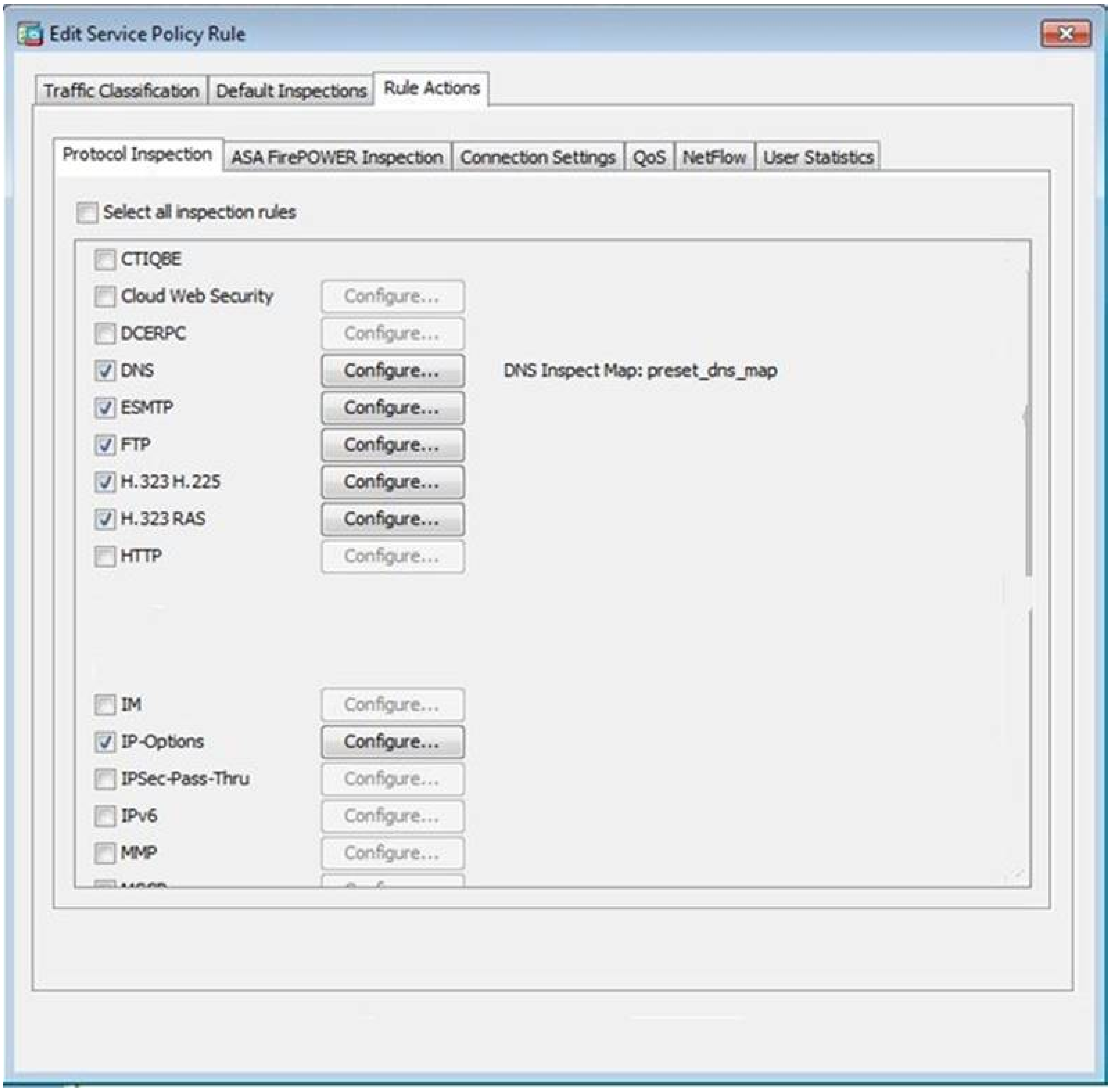
□ TCP or UDP Destination Port

□ RTP Range

□ IP DiffServ CodePoints (DSCP)

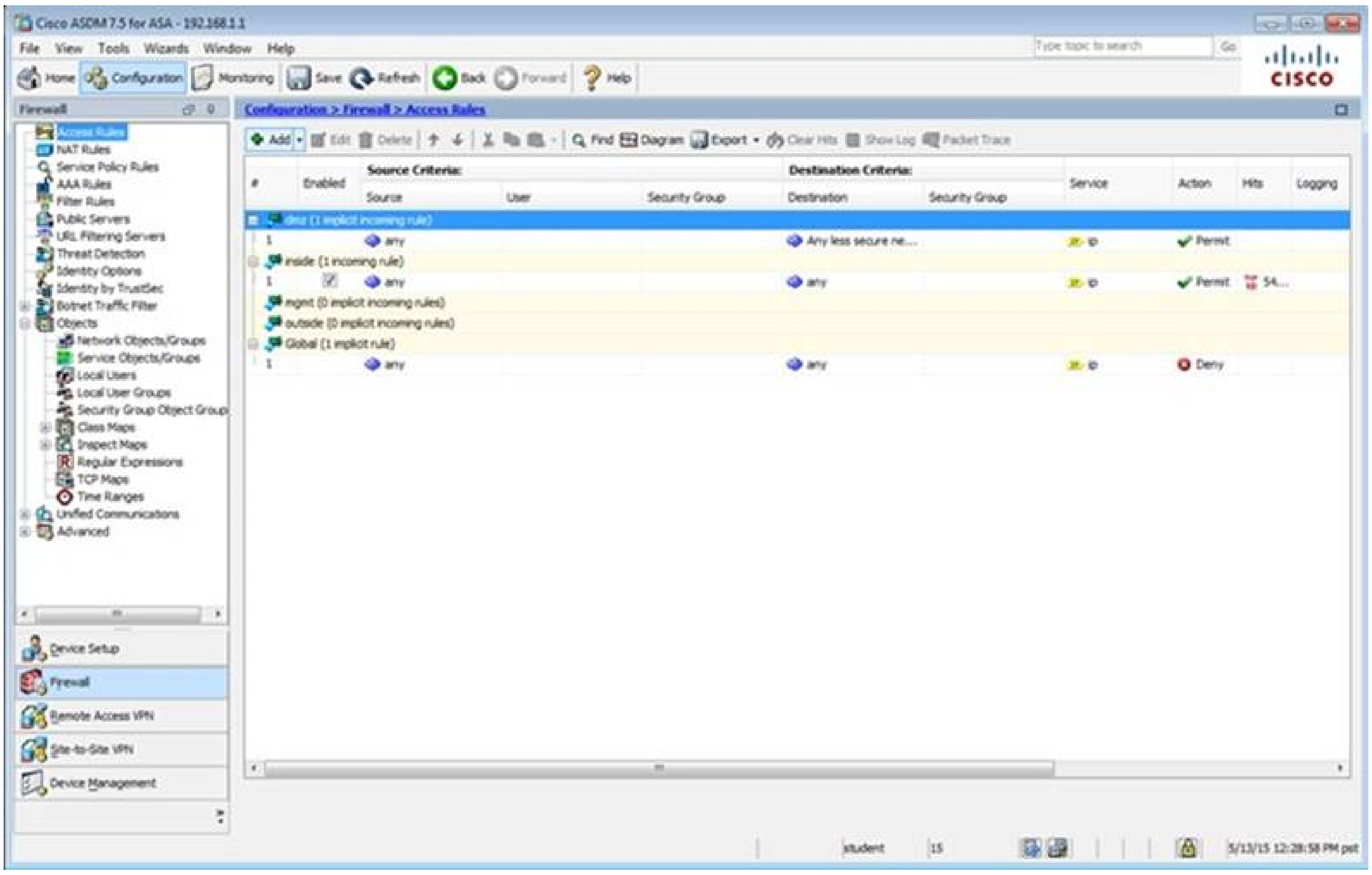
□ IP Precedence

□ Any traffic

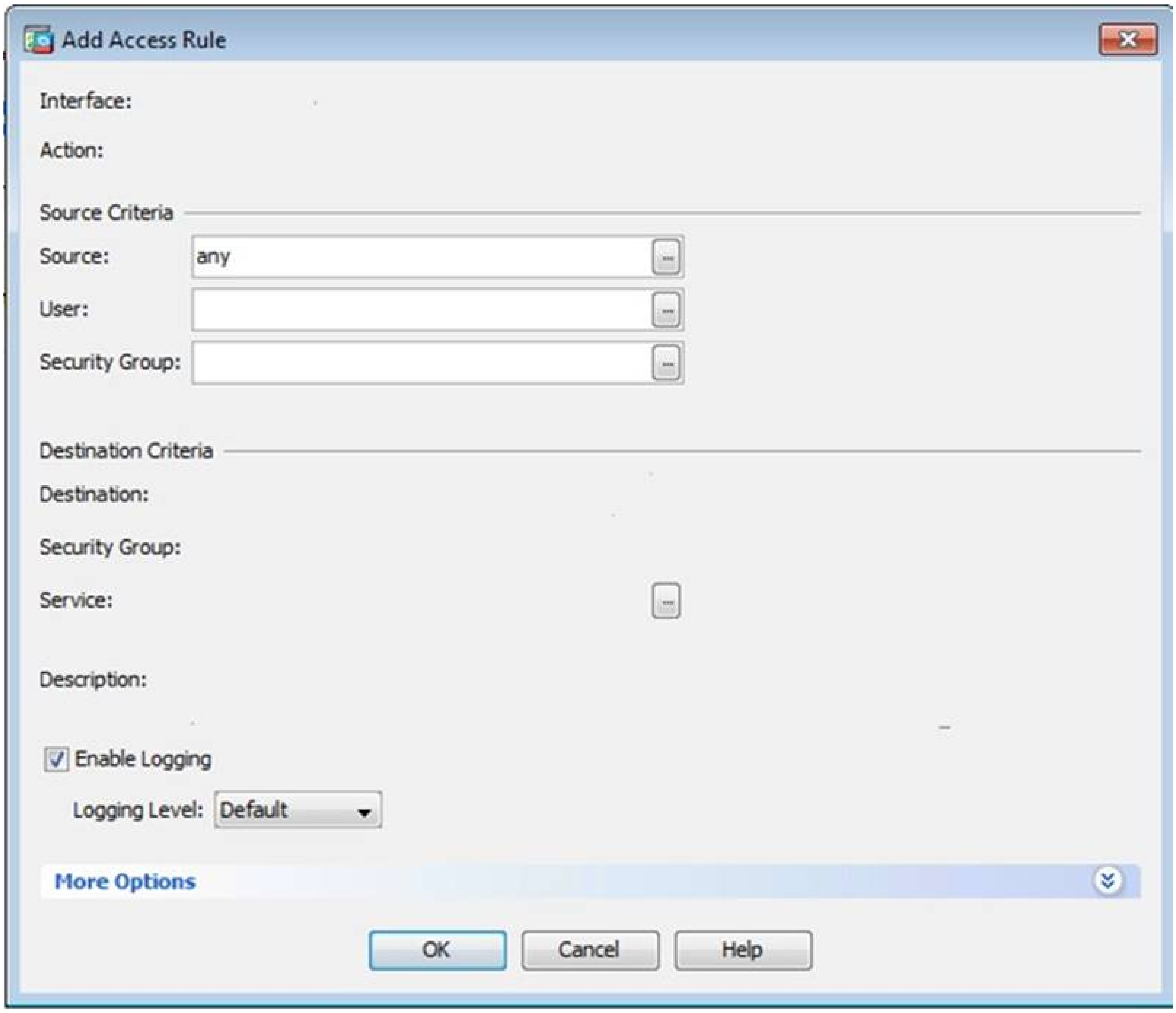


□ Select all inspection rules

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



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



Add Access Rule

Interface:

Action:

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination:

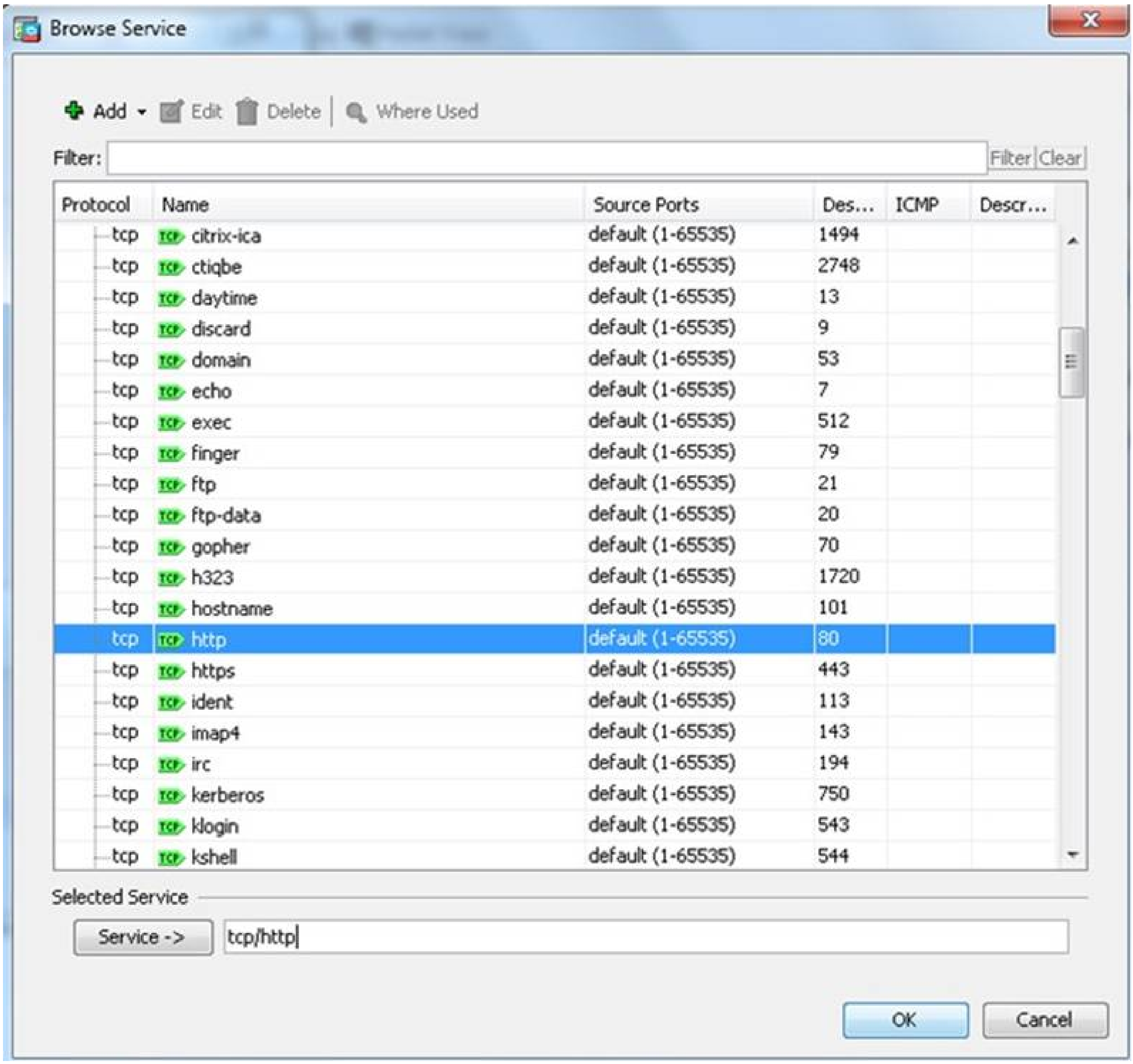
Security Group:

Service:

Description:

☑ Enable Logging

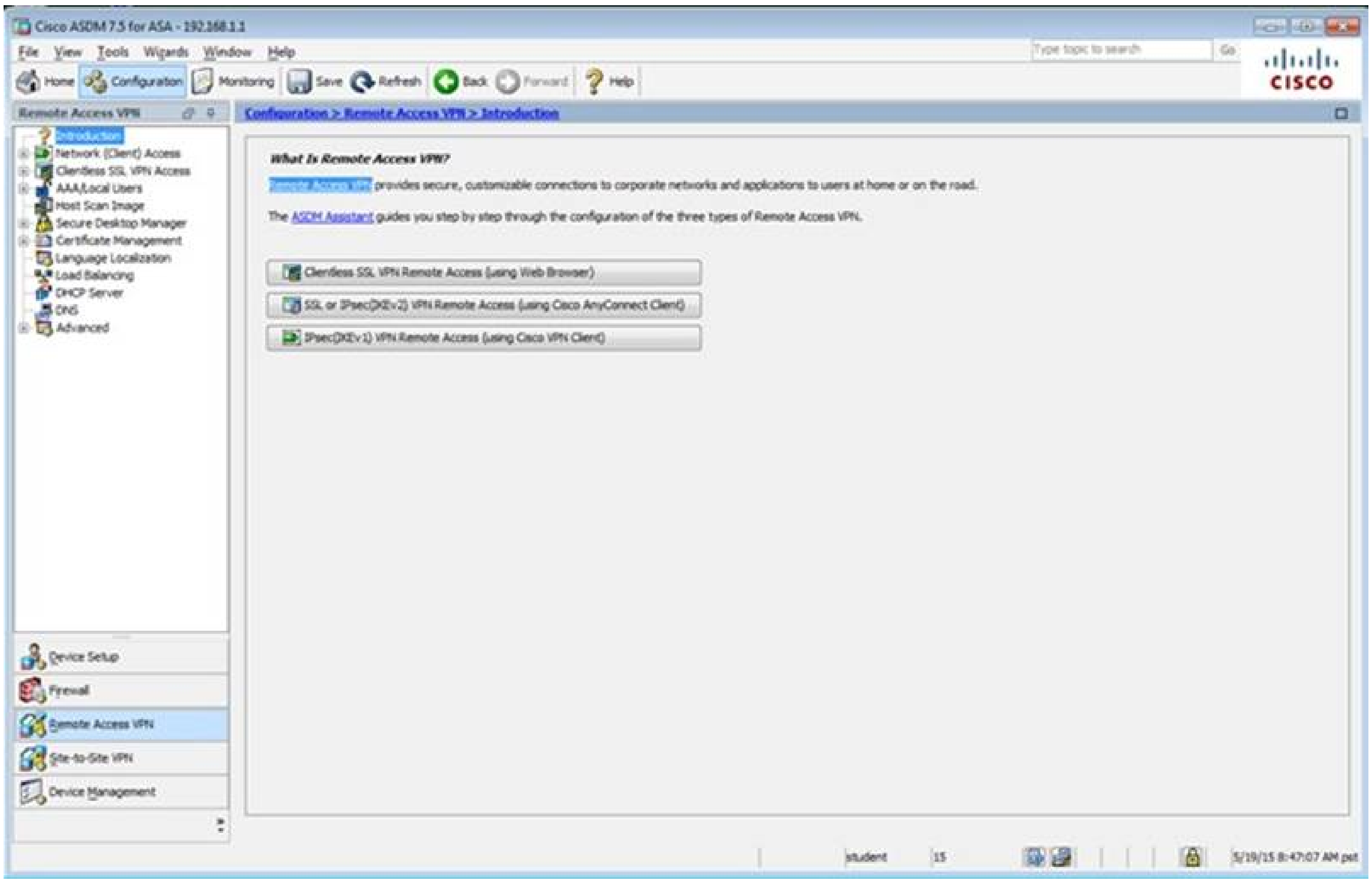
Logging Level: Default



Protocol	Name	Source Ports	Des...	ICMP	Descr...
tcp	citrix-ica	default (1-65535)	1494		
tcp	ctiqbe	default (1-65535)	2748		
tcp	daytime	default (1-65535)	13		
tcp	discard	default (1-65535)	9		
tcp	domain	default (1-65535)	53		
tcp	echo	default (1-65535)	7		
tcp	exec	default (1-65535)	512		
tcp	finger	default (1-65535)	79		
tcp	ftp	default (1-65535)	21		
tcp	ftp-data	default (1-65535)	20		
tcp	gopher	default (1-65535)	70		
tcp	h323	default (1-65535)	1720		
tcp	hostname	default (1-65535)	101		
tcp	http	default (1-65535)	80		
tcp	https	default (1-65535)	443		
tcp	ident	default (1-65535)	113		
tcp	imap4	default (1-65535)	143		
tcp	irc	default (1-65535)	194		
tcp	kerberos	default (1-65535)	750		
tcp	klogin	default (1-65535)	543		
tcp	kshell	default (1-65535)	544		

Selected Service

Service -> tcp/http



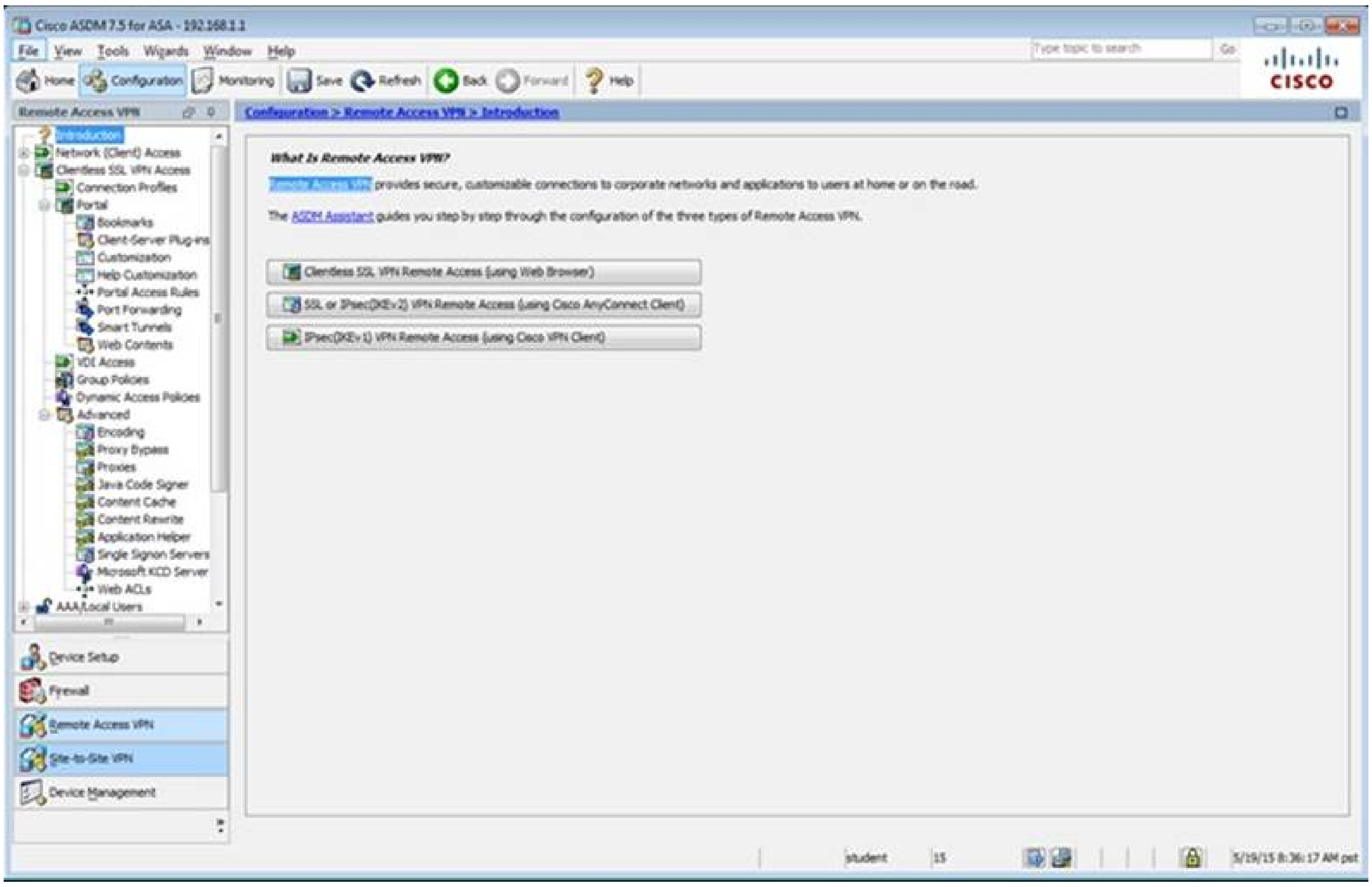
Configuration > Remote Access VPN > Introduction

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.

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)
student
15
5/19/15 8:47:07 AM pst



Configuration > Remote Access VPN > Introduction

What Is Remote Access VPN?

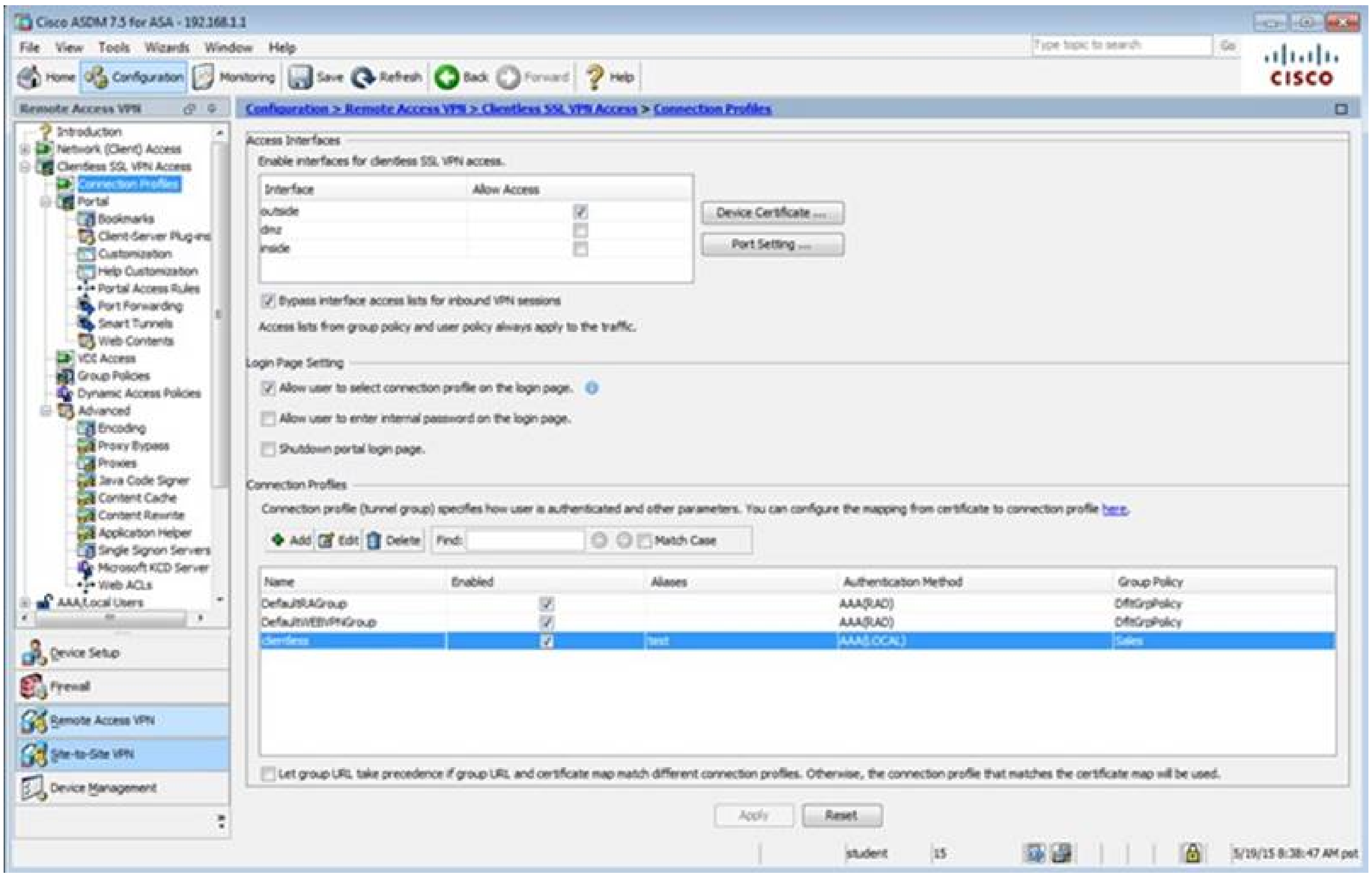
Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

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

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)



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ 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.

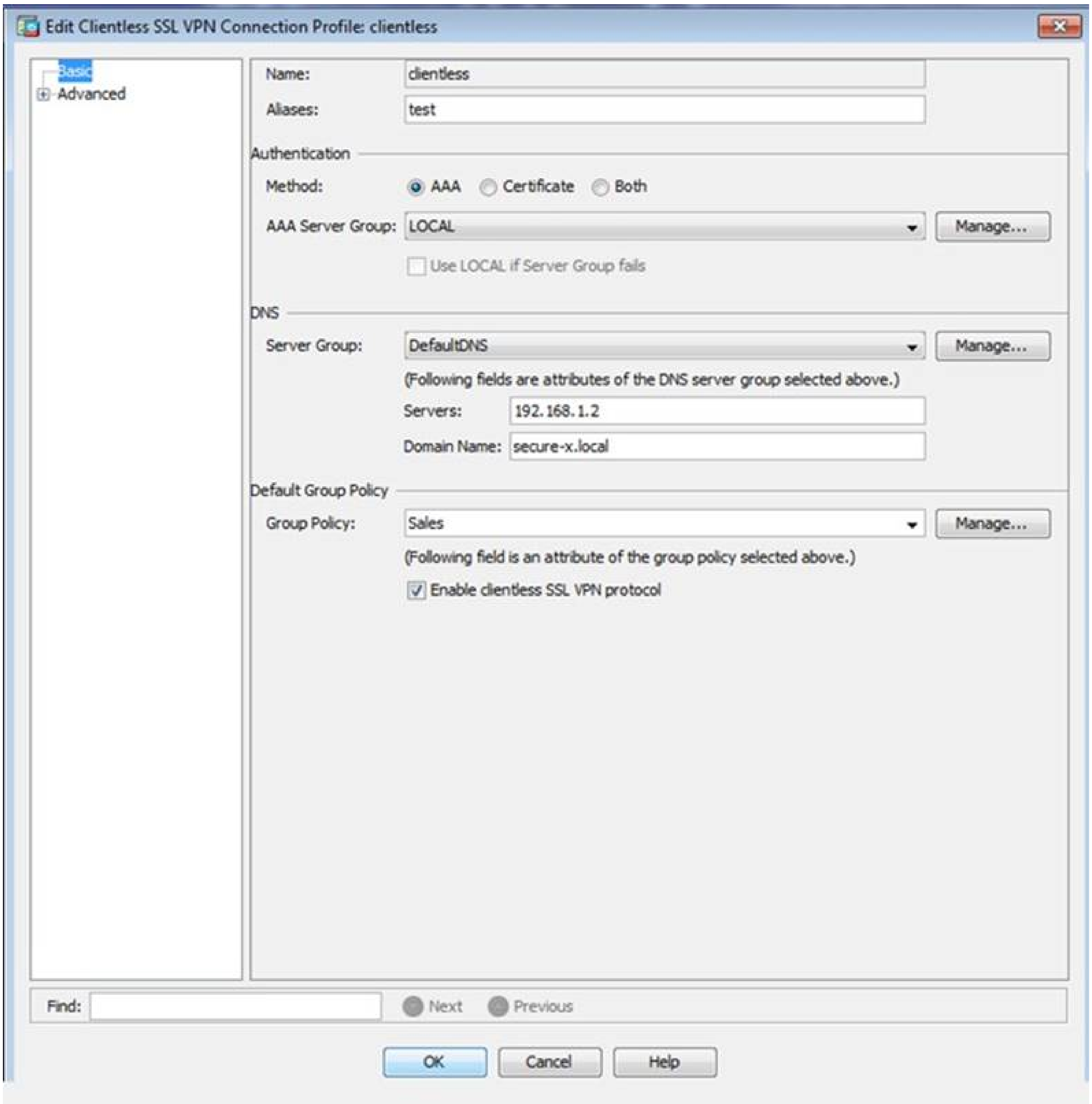
□ Shutdown portal login page.

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.

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(RAD)	DfltGrpPolicy
clientless	☑	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.



Edit Clientless SSL VPN Connection Profile: clientless

Name: clientless

Aliases: test

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

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

Servers: 192.168.1.2

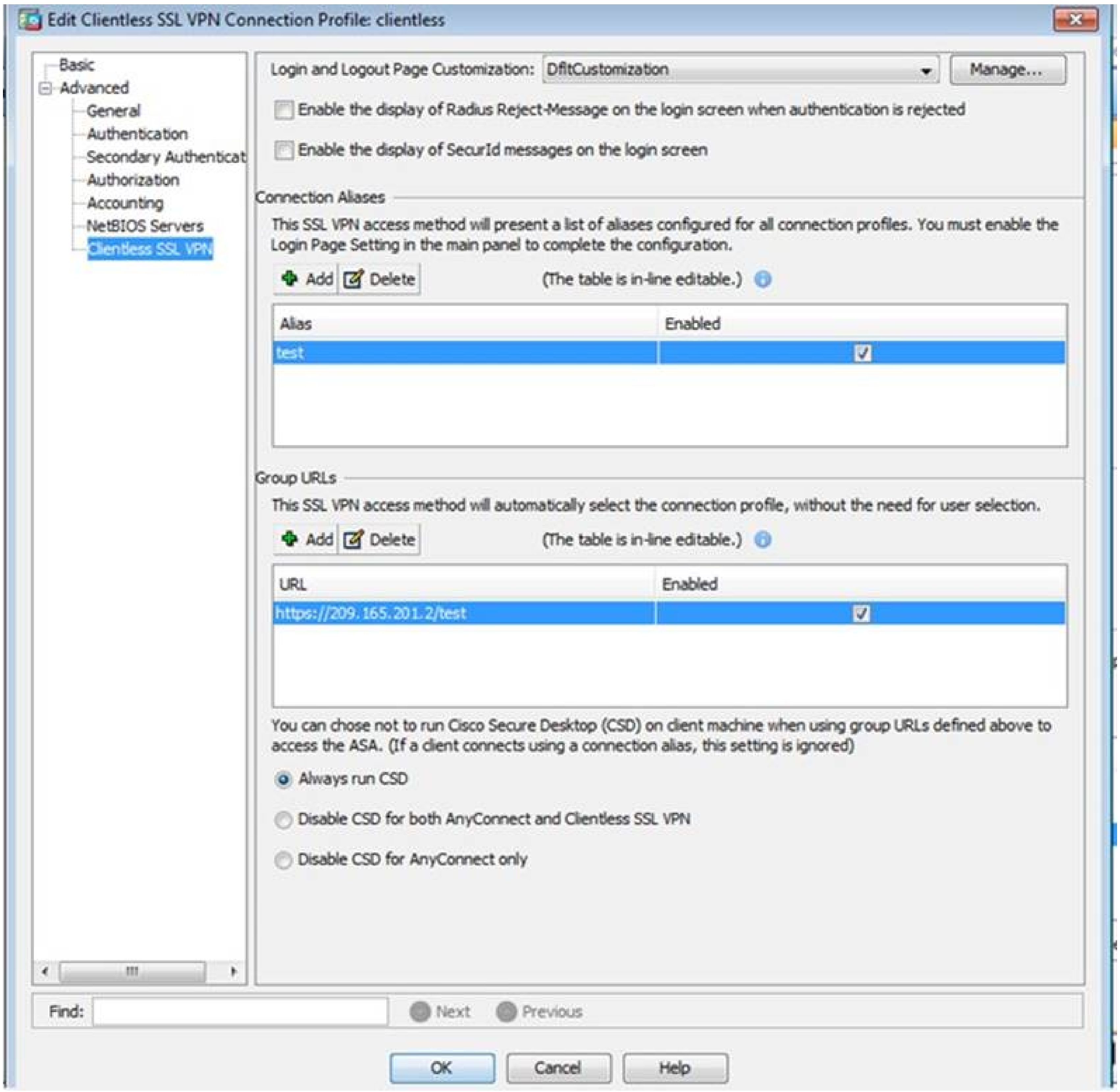
Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales

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

☑ Enable clientless SSL VPN protocol



Edit Clientless SSL VPN Connection Profile: clientless

Login and Logout Page Customization: DfltCustomization

□ 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.

(The table is in-line editable.)

Alias	Enabled
test	☑

Group URLs

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

(The table is in-line editable.)

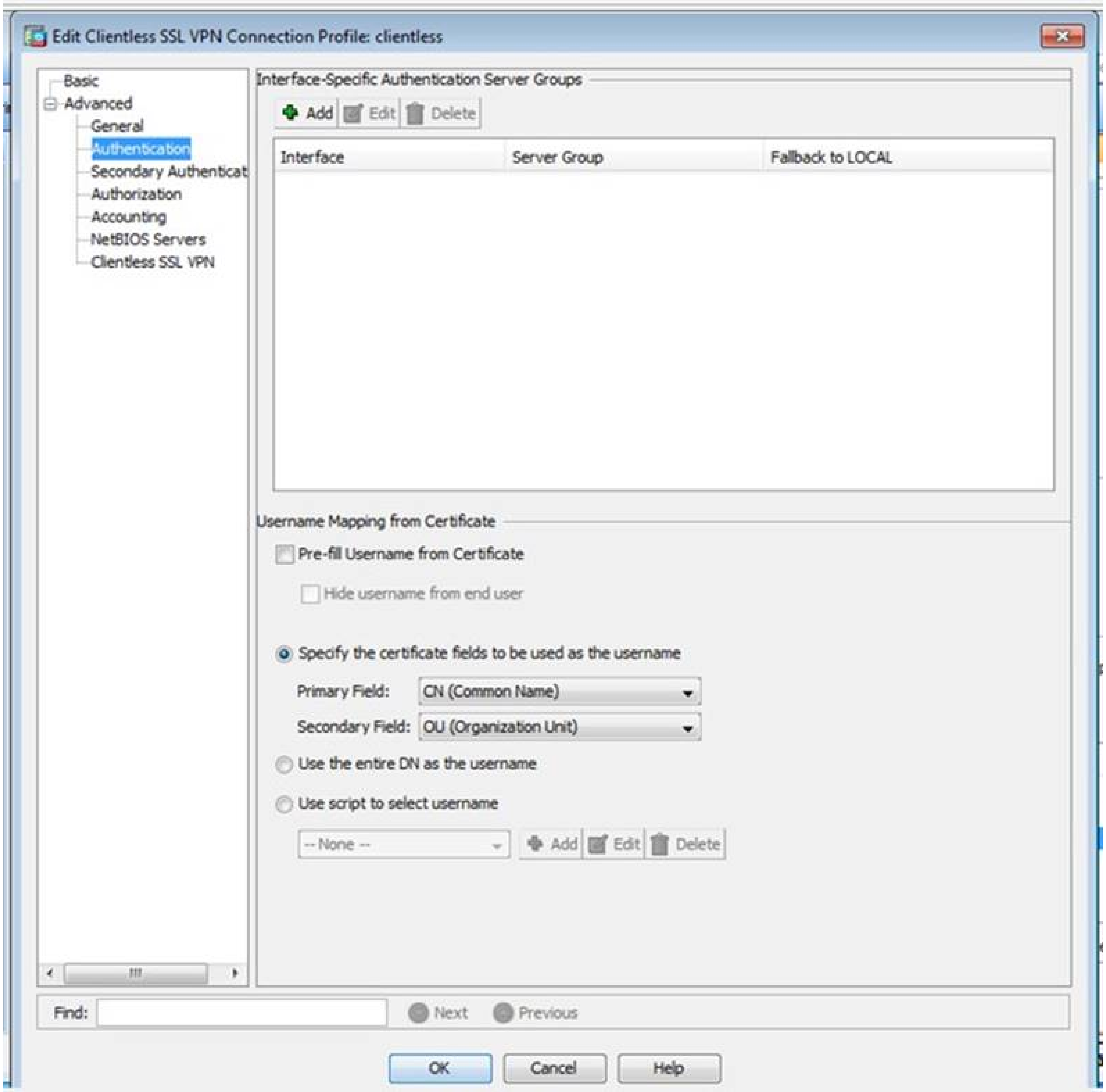
URL	Enabled
https://209.165.201.2/test	☑

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



□ Pre-fill Username from Certificate

□ Hide username from end user

● Specify the certificate fields to be used as the username

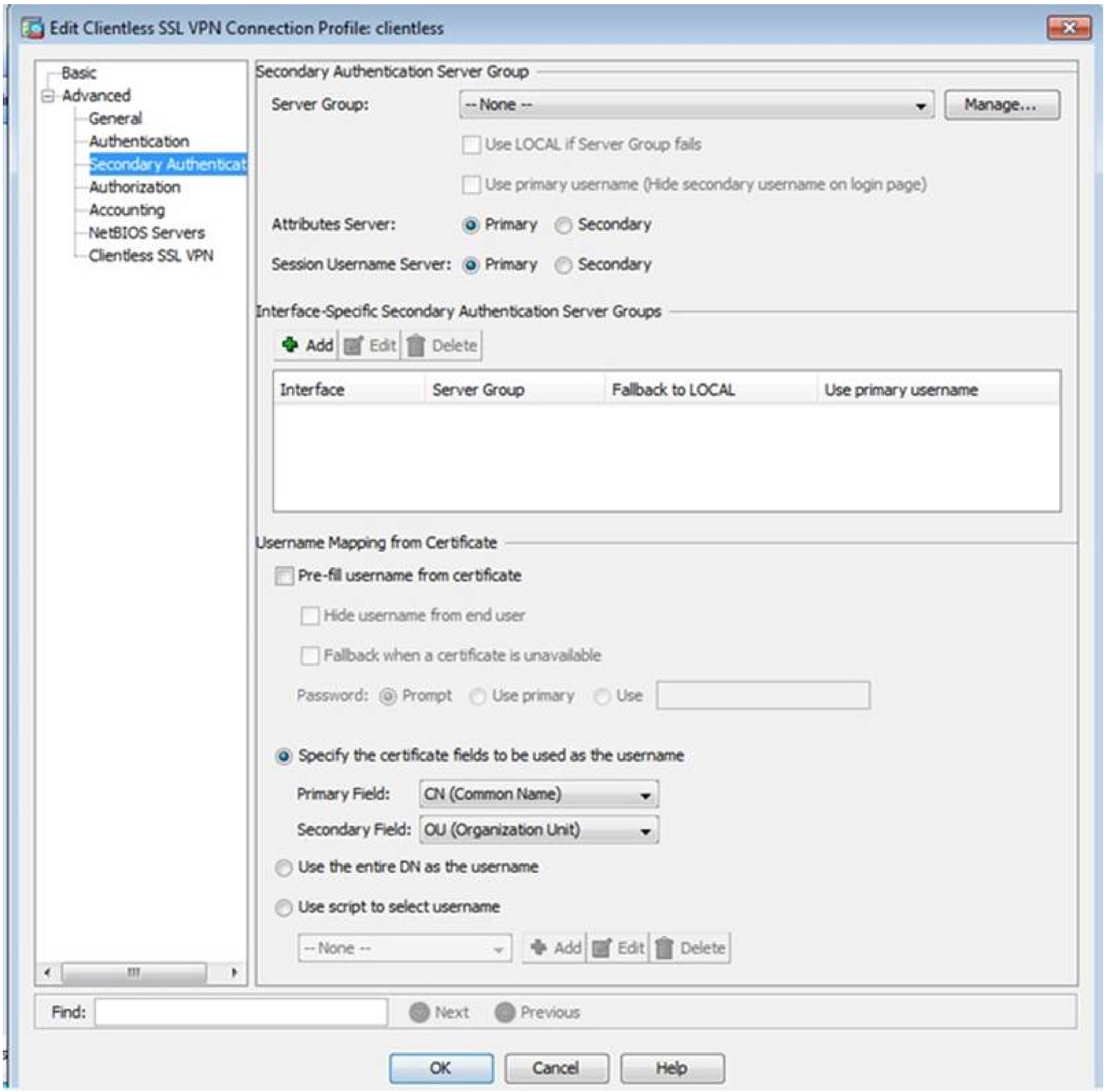
Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --



Edit Clientless SSL VPN Connection Profile: clientless

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

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

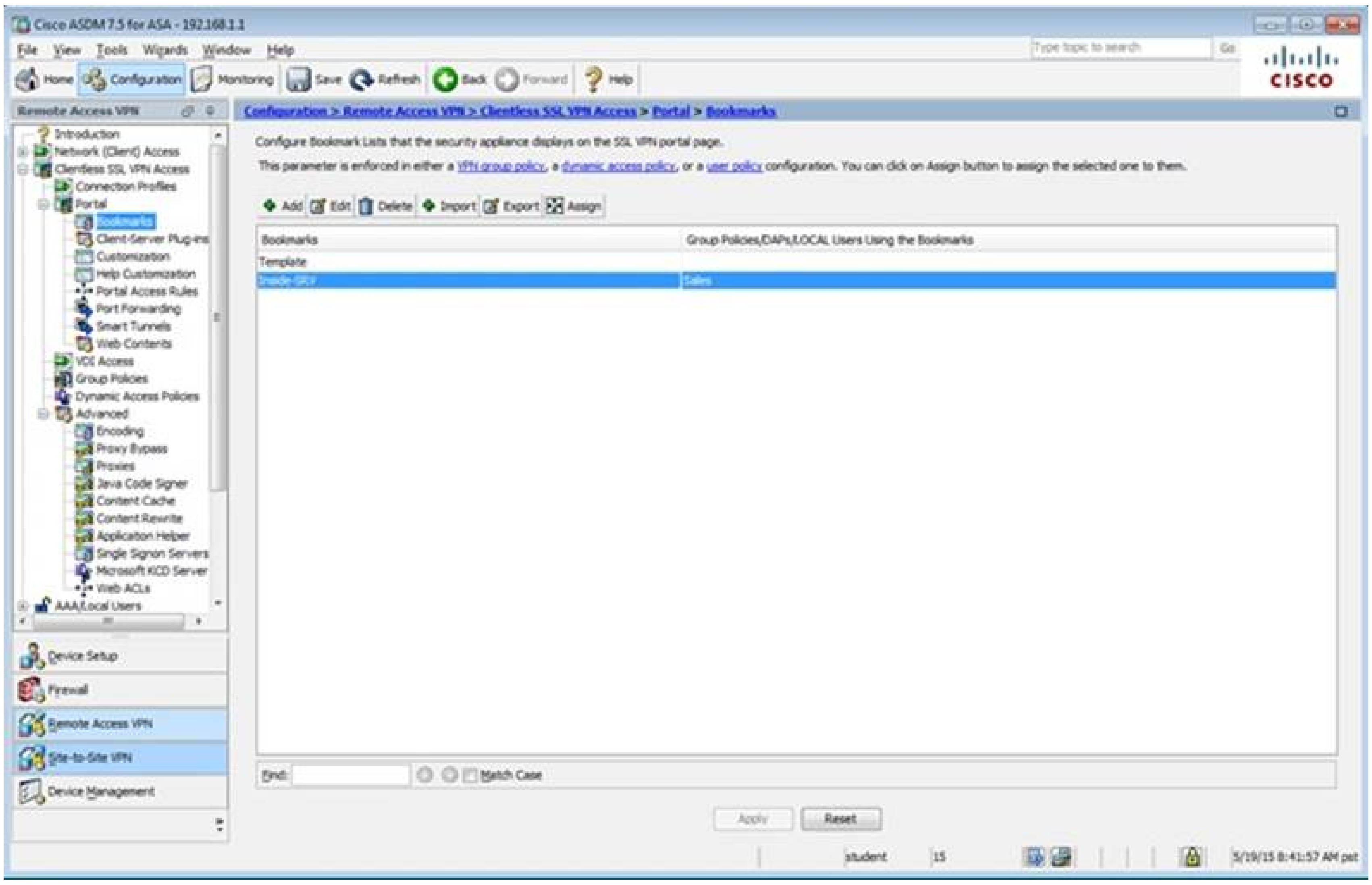
Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --



Cisco ASDM 7.5 for ASA - 192.168.1.1

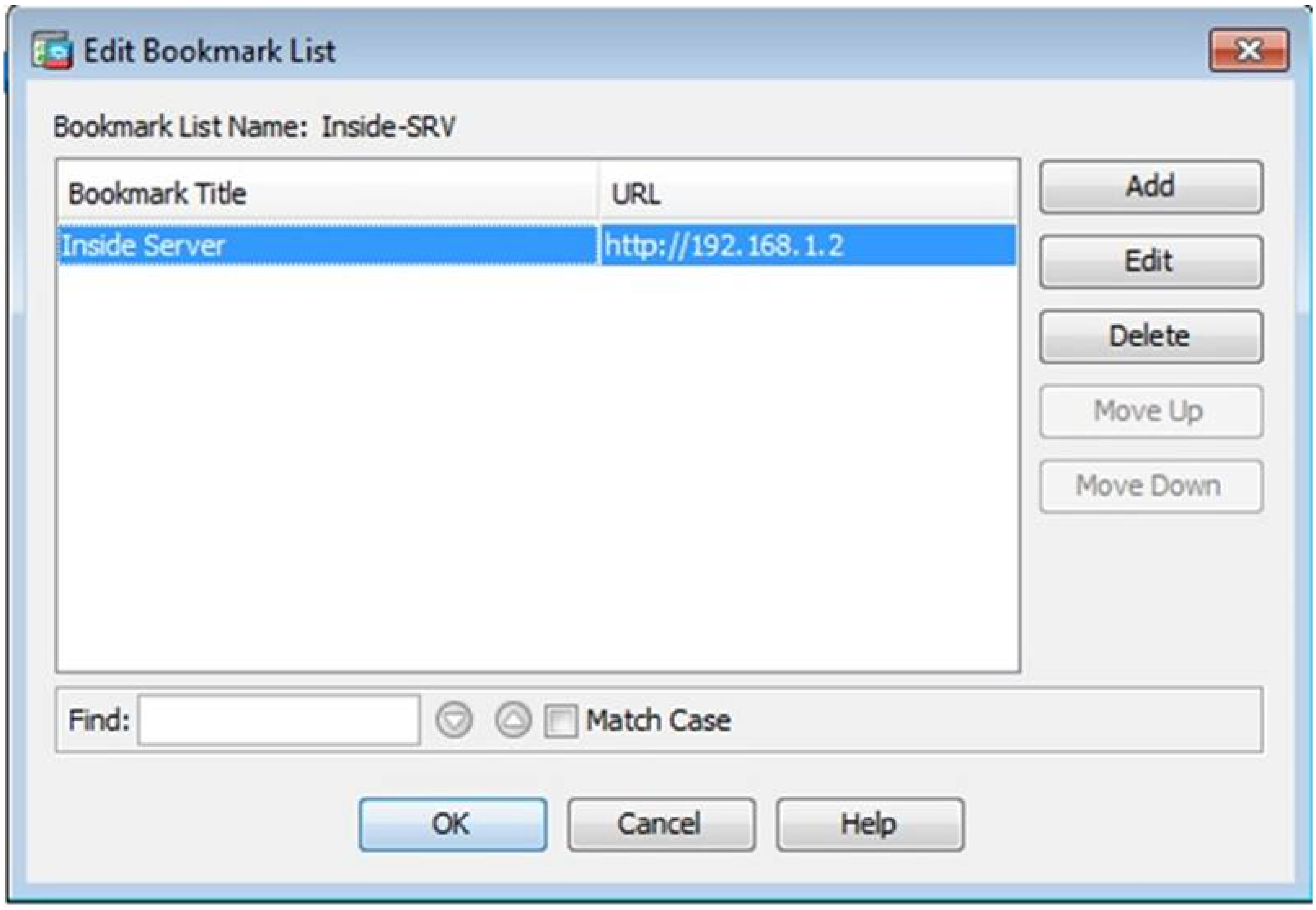
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

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.

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

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

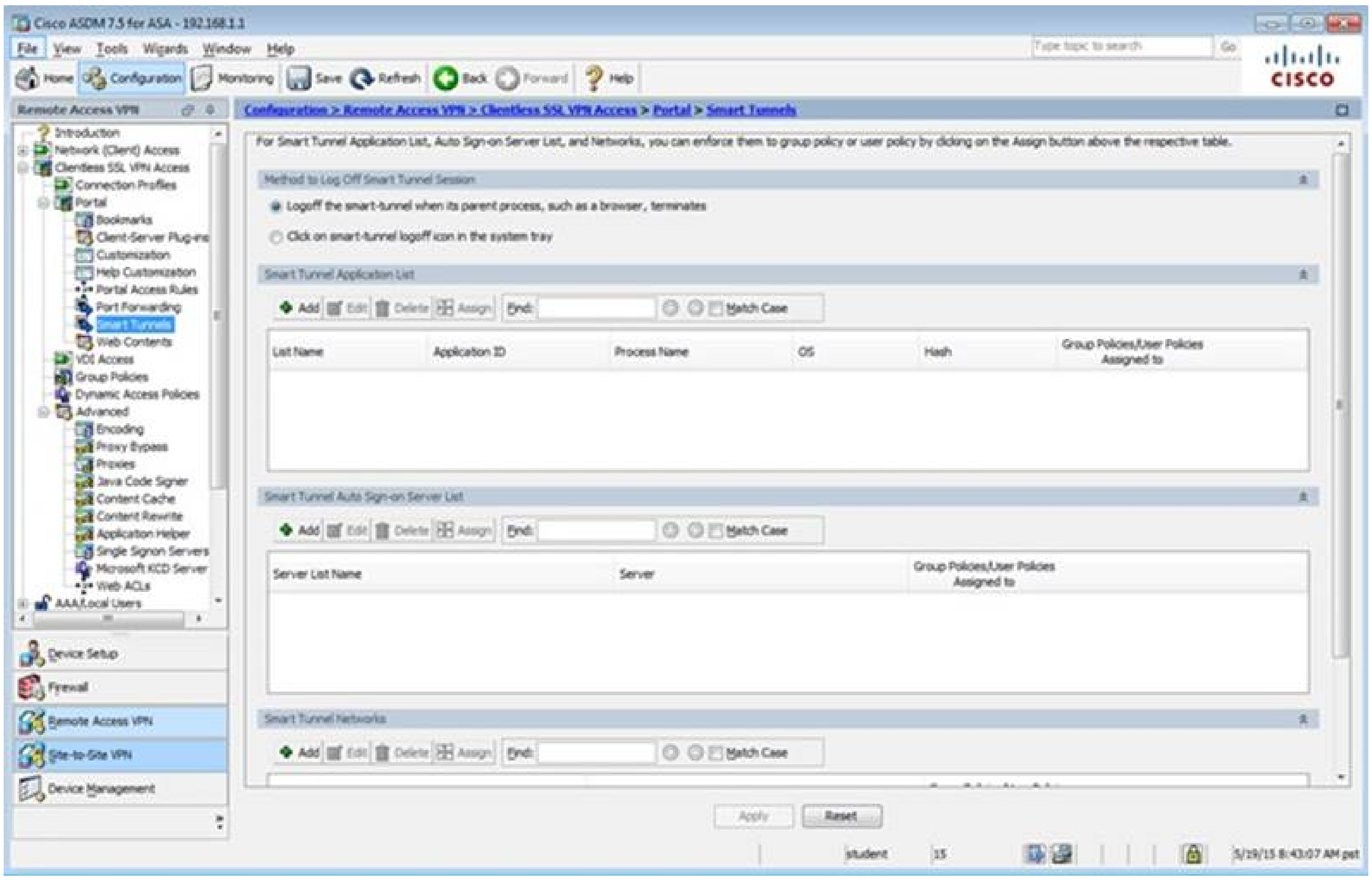


Edit Bookmark List

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

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

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

Method to Log Off Smart Tunnel Session

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

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

Smart Tunnel Application List

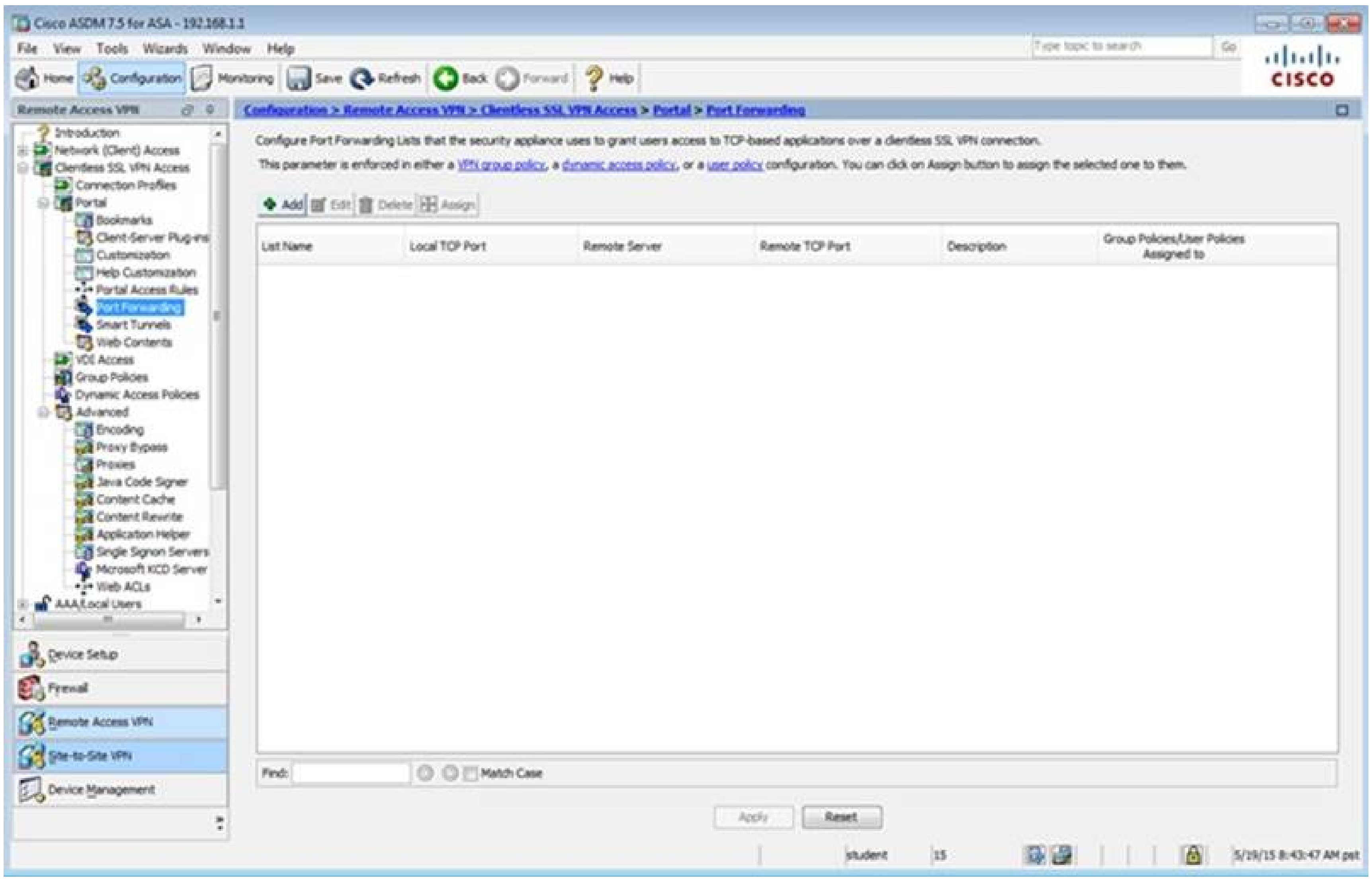
List Name	Application ID	Process Name	OS	Hash	Group Policies/User Policies Assigned to

Smart Tunnel Auto Sign-on Server List

Server List Name	Server	Group Policies/User Policies Assigned to

Smart Tunnel Networks

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

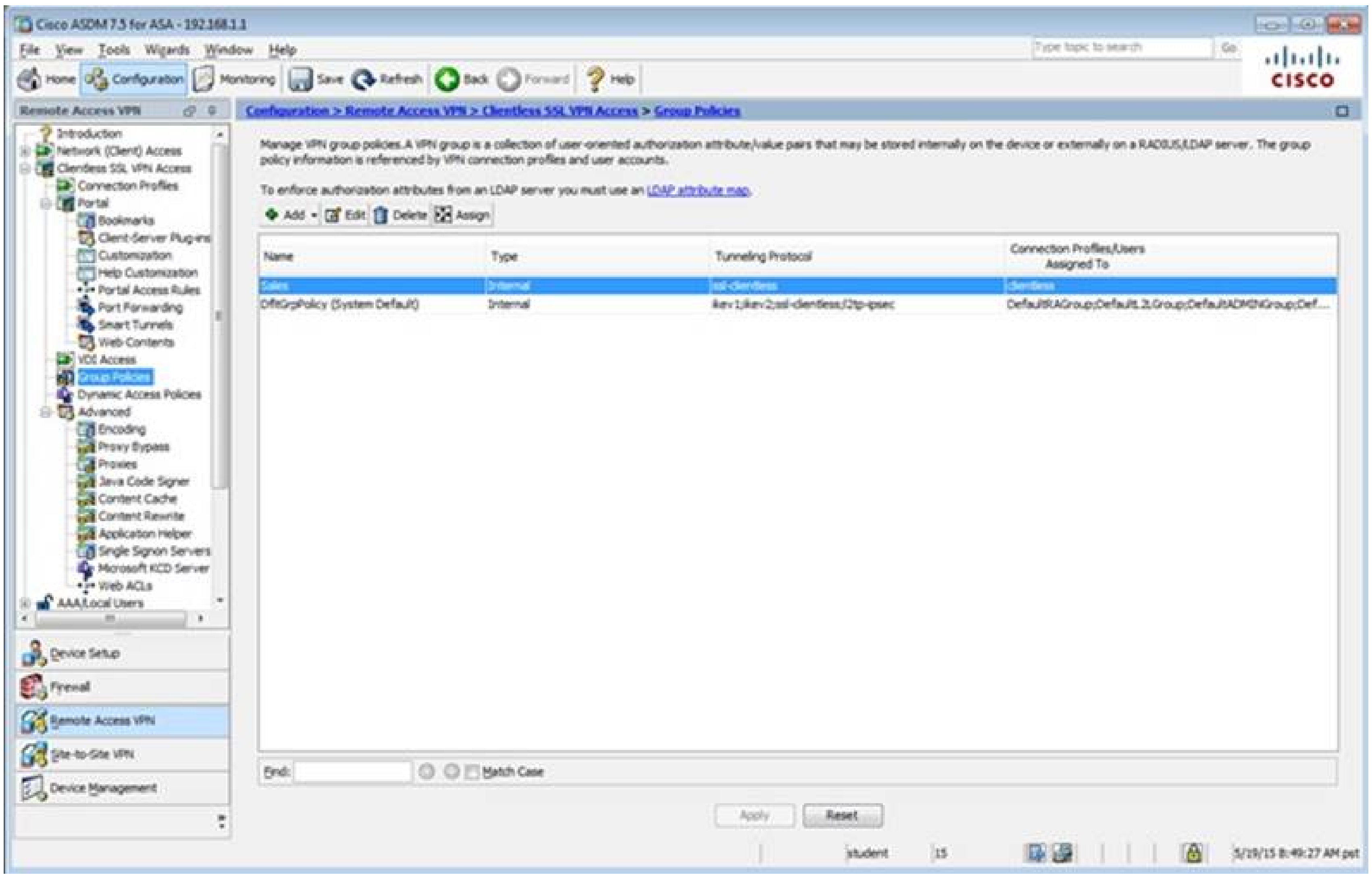


Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

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.

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

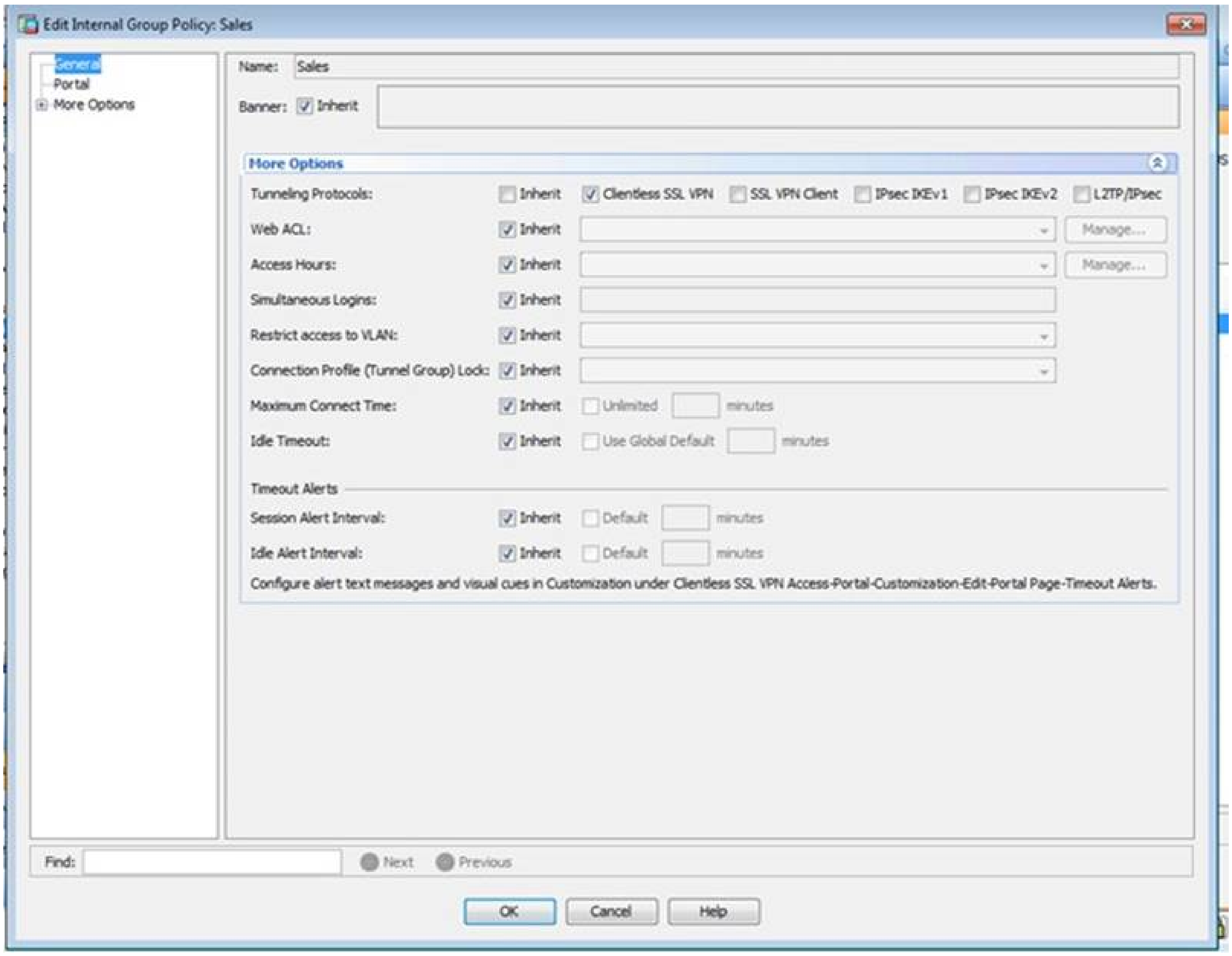


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

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	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...



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

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

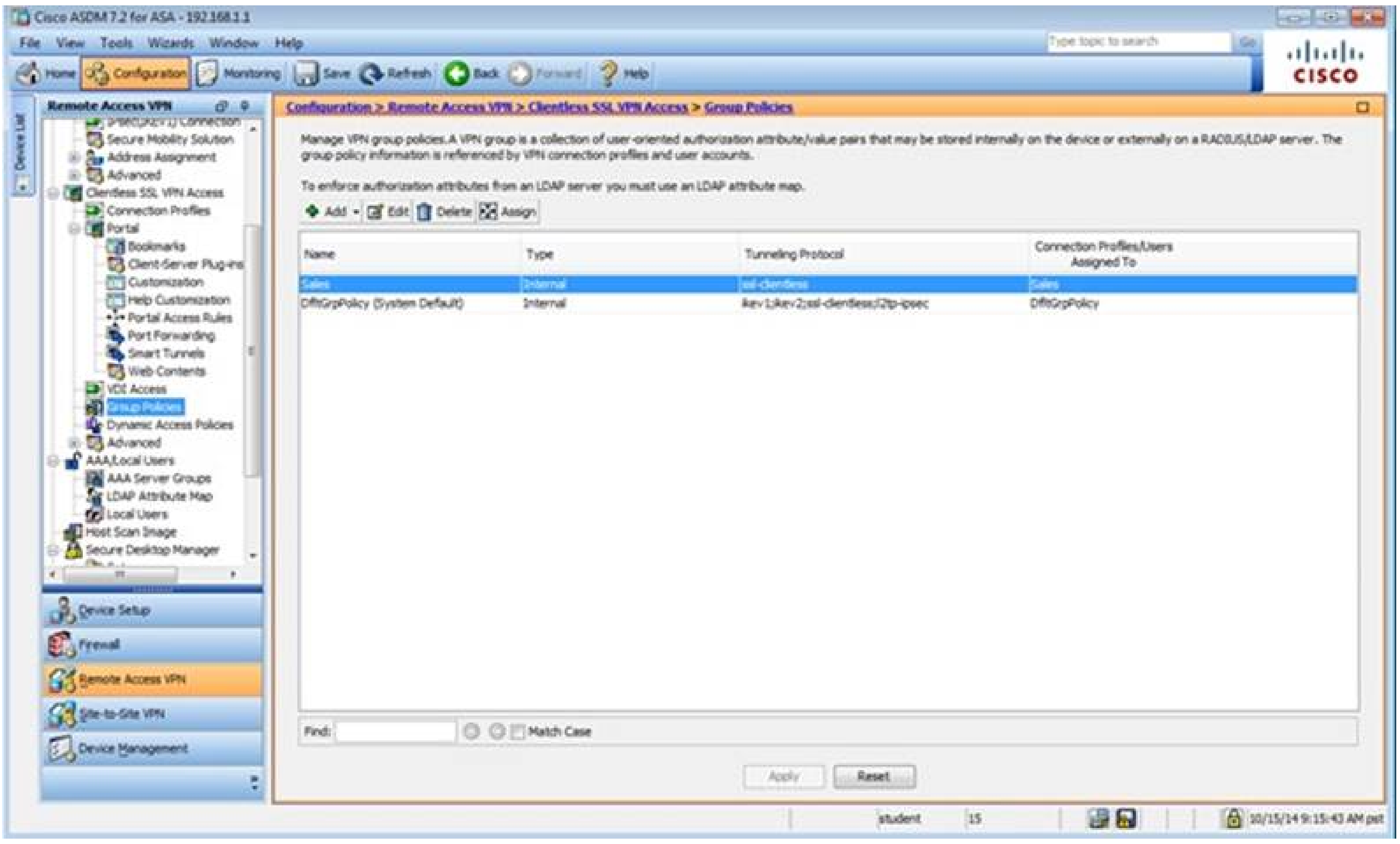
Idle Timeout: ☑ Inherit □ Use Global Default minutes

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.

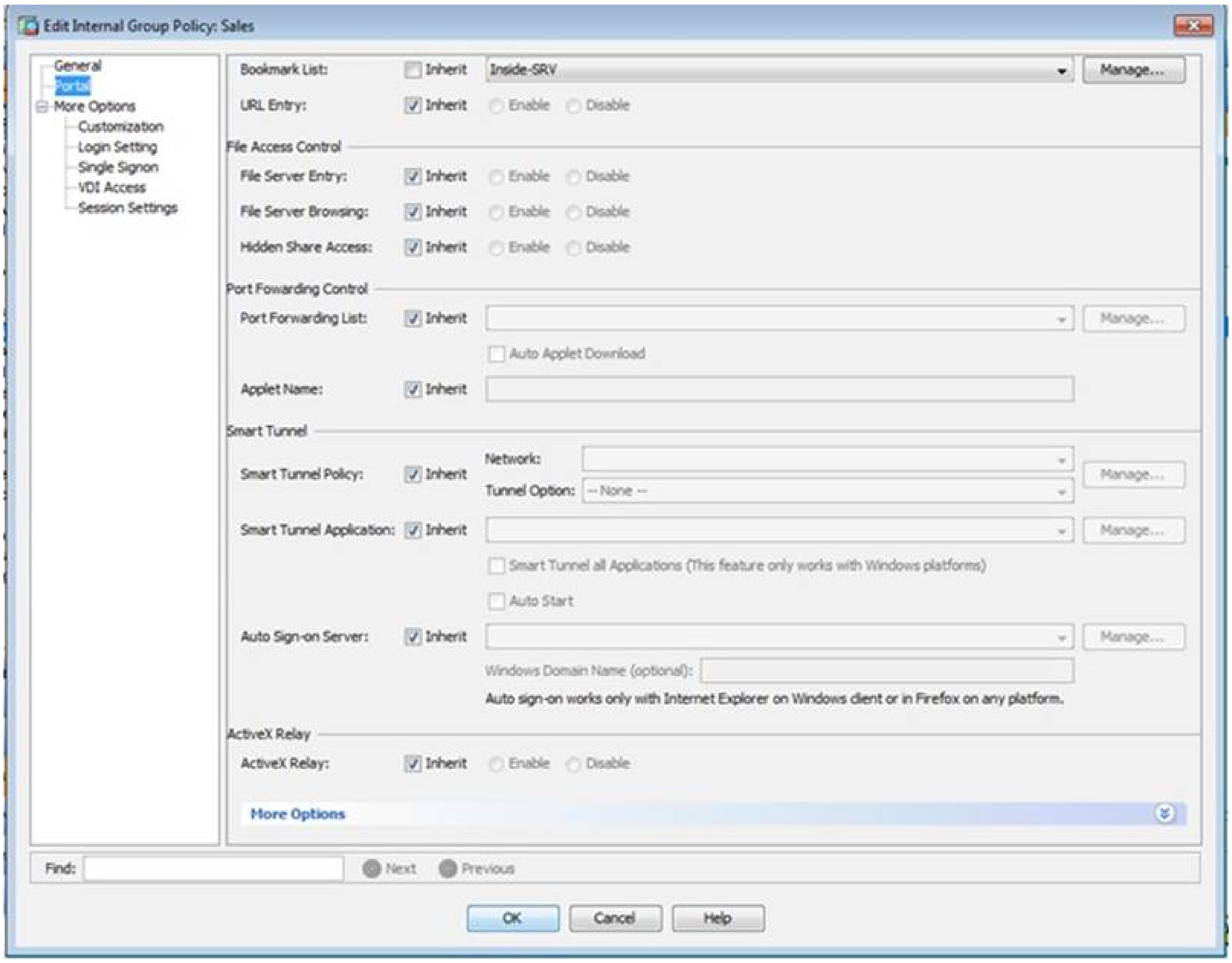


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

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
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DfltGrpPolicy



Edit Internal Group Policy: Sales

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 Fowarding Control

Port Forwarding List: ☑ Inherit Manage...

□ Auto Applet Download

Applet Name: ☑ Inherit

Smart Tunnel

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

Smart Tunnel Application: ☑ Inherit Manage...

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

□ Auto Start

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

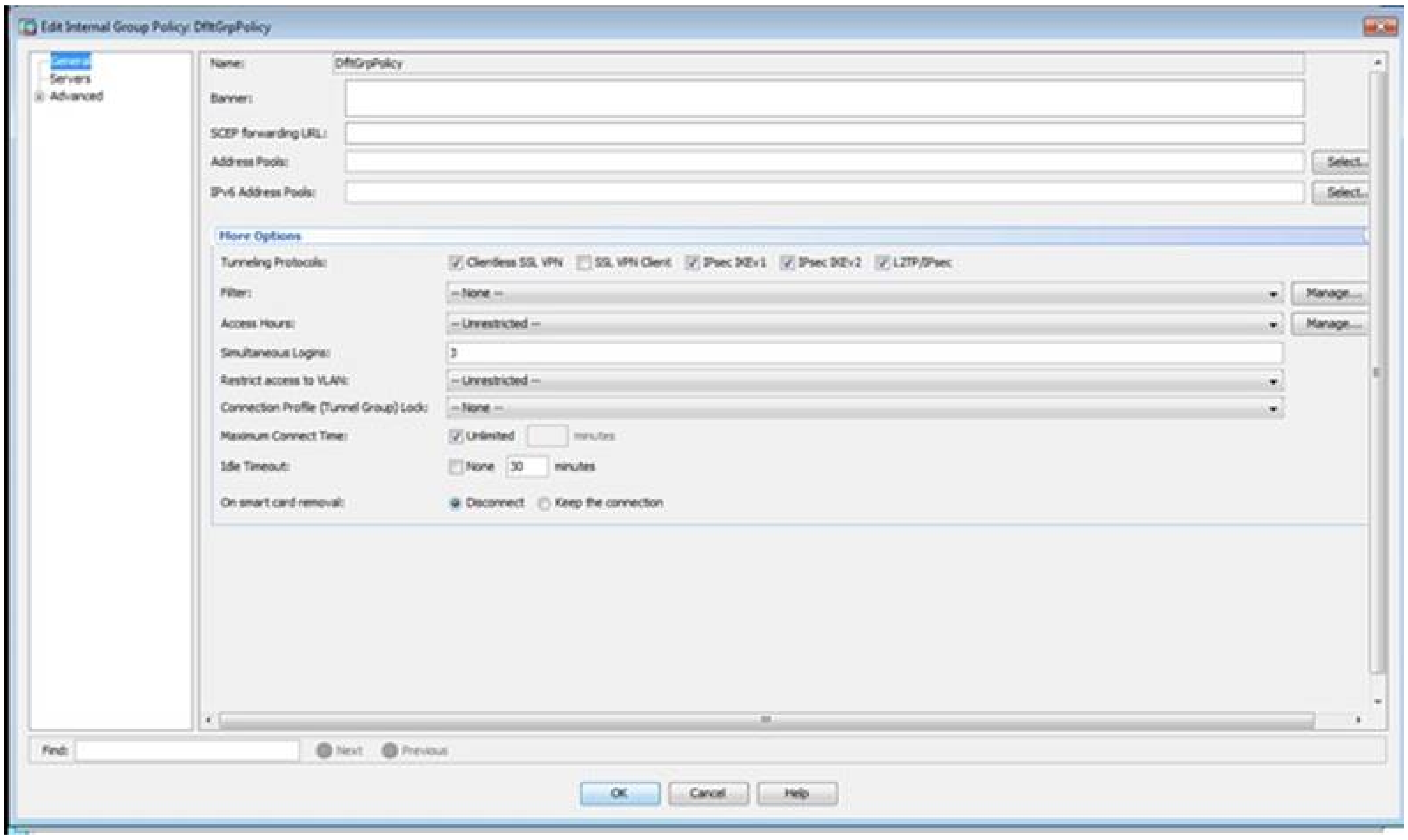
Windows Domain Name (optional):

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

ActiveX Relay

ActiveX Relay: ☑ Inherit ○ Enable ○ Disable

More Options



Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

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

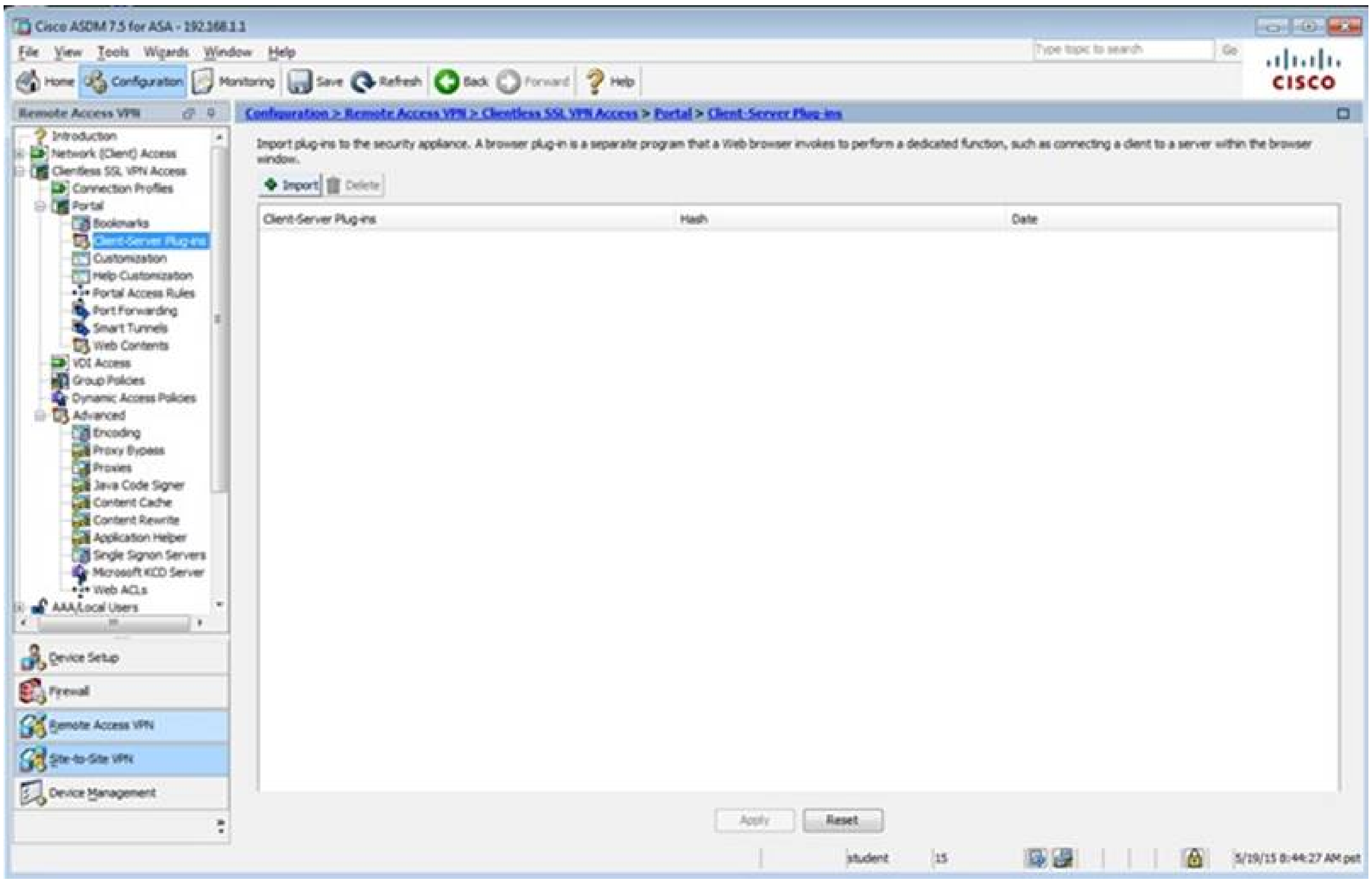
Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: □ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection



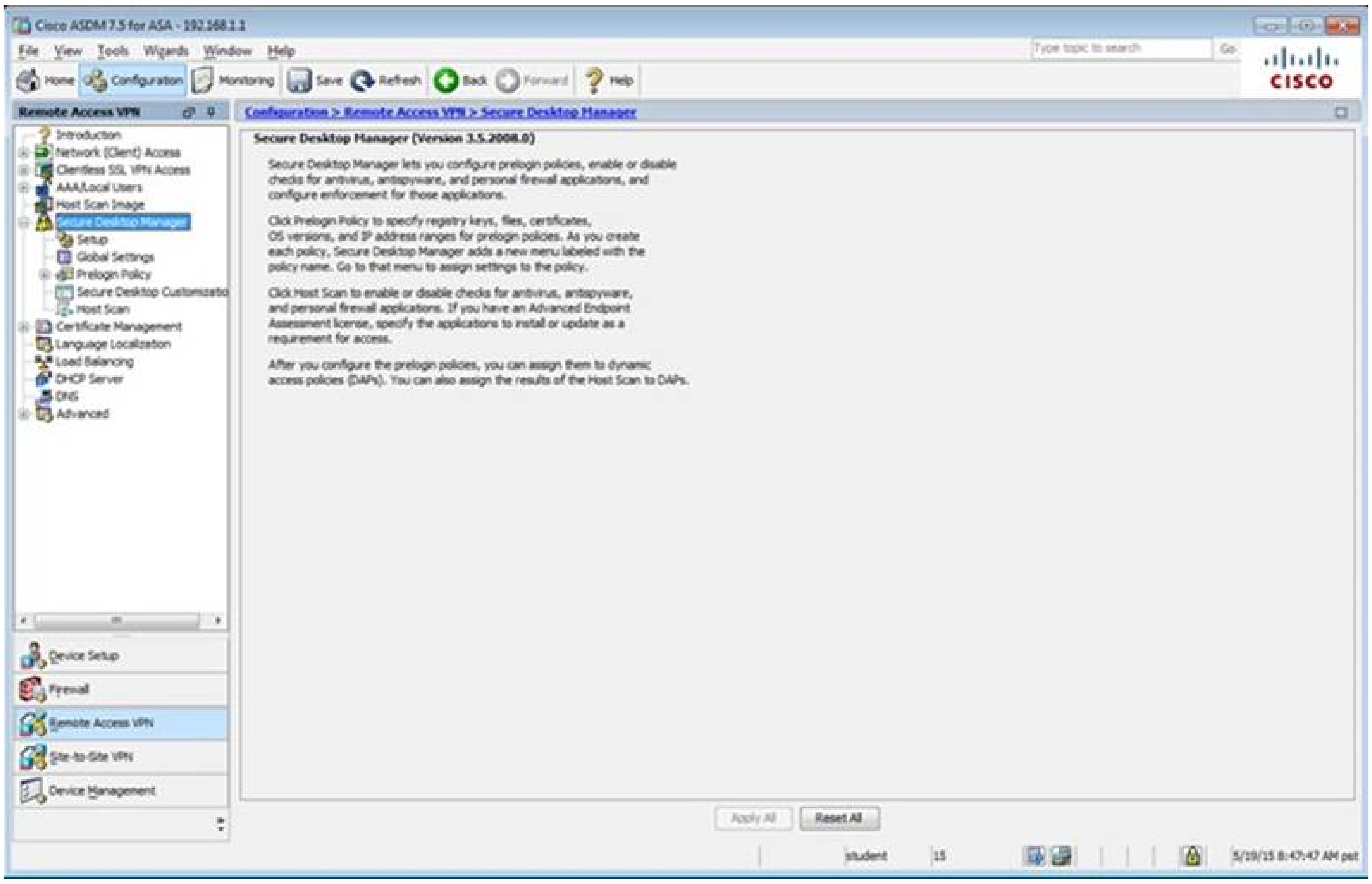
Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins

Import plug-ins to the security appliance. A browser plug-in is a separate program that a Web browser invokes to perform a dedicated function, such as connecting a client to a server within the browser window.

Client-Server Plug-ins	Hash	Date

student 15 5/19/15 8:44:27 AM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Secure Desktop Manager

Secure Desktop Manager (Version 3.5.2008.0)

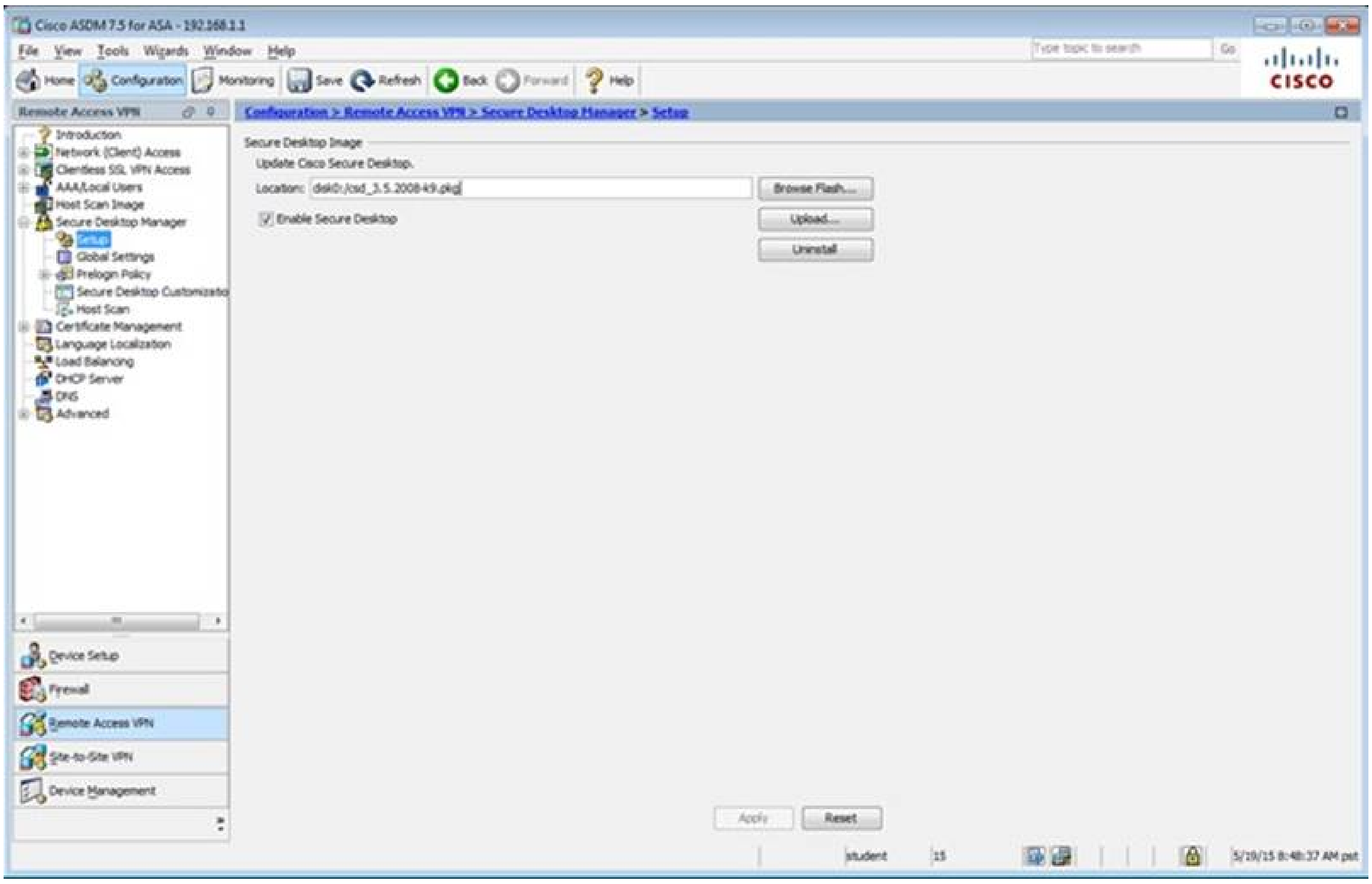
Secure Desktop Manager lets you configure prelogin policies, enable or disable checks for antivirus, antispyware, and personal firewall applications, and configure enforcement for those applications.

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

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

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

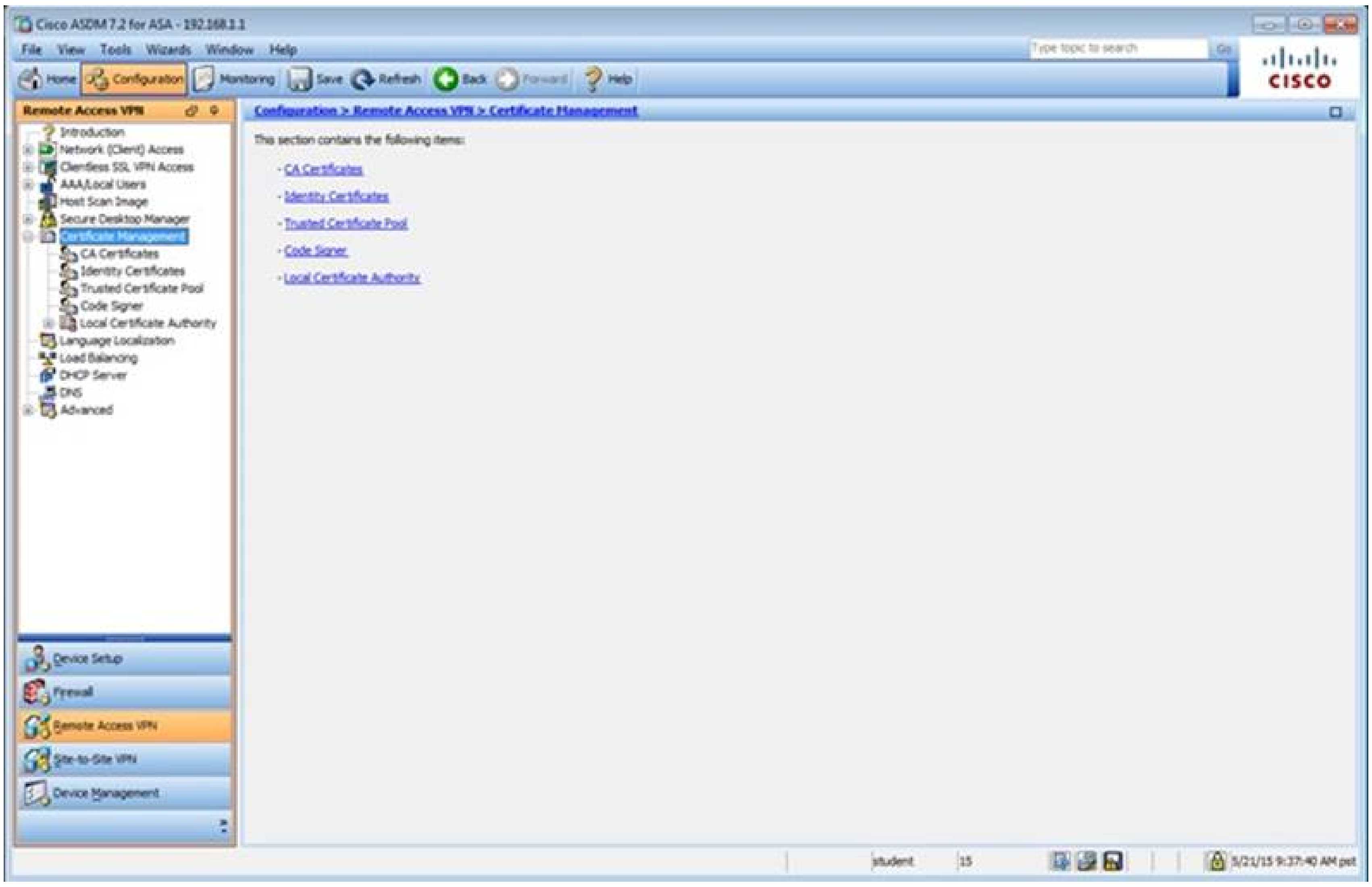
Configuration > Remote Access VPN > Secure Desktop Manager > Setup

Secure Desktop Image

Update Cisco Secure Desktop.

Location: disk0:/csd_3.5.2008-49.pkg

☑ Enable Secure Desktop

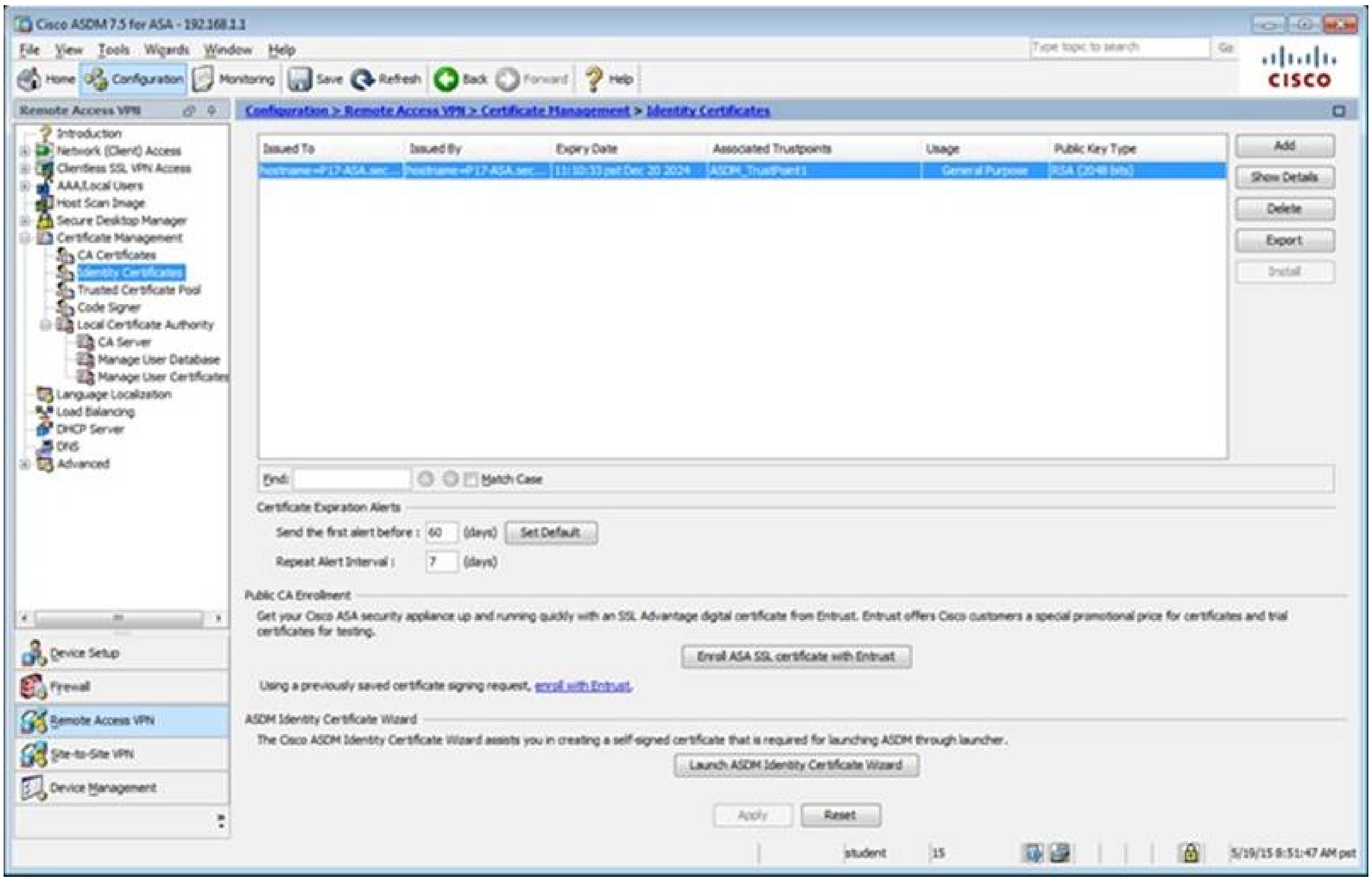


Cisco ASDM 7.2 for ASA - 192.168.1.1

Configuration > Remote Access VPN > Certificate Management

This section contains the following items:

- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM_TrustPoint1	General Purpose	RSA (2048 bits)

Find: ○ ○ □ Match Case

Certificate Expiration Alerts

Send the first alert before : 60 (days) Set Default

Repeat Alert Interval : 7 (days)

Public CA Enrollment

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

Enroll ASA SSL certificate with Entrust

Using a previously saved certificate signing request, enroll with Entrust.

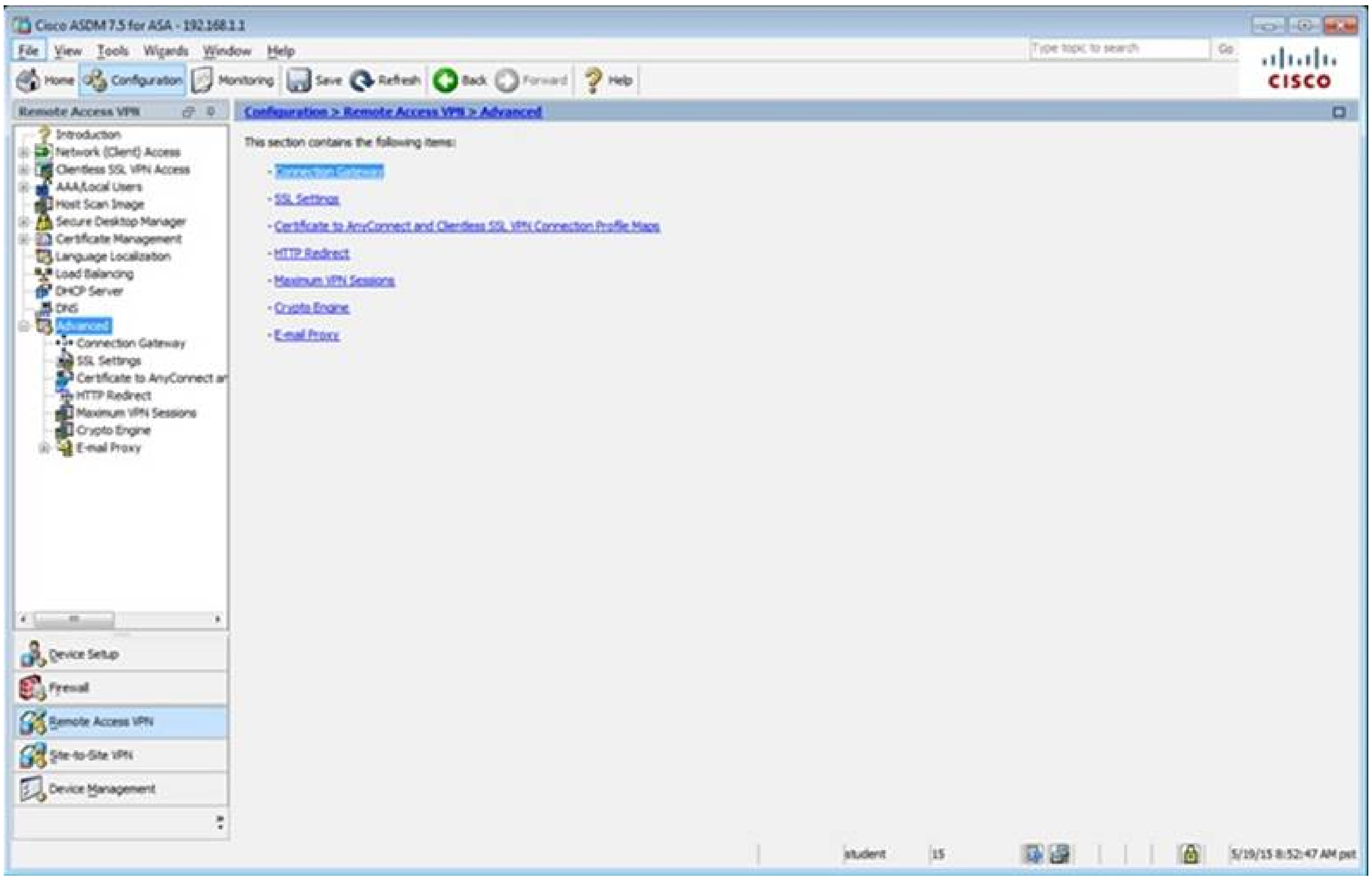
ASDM Identity Certificate Wizard

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

Launch ASDM Identity Certificate Wizard

Apply Reset

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

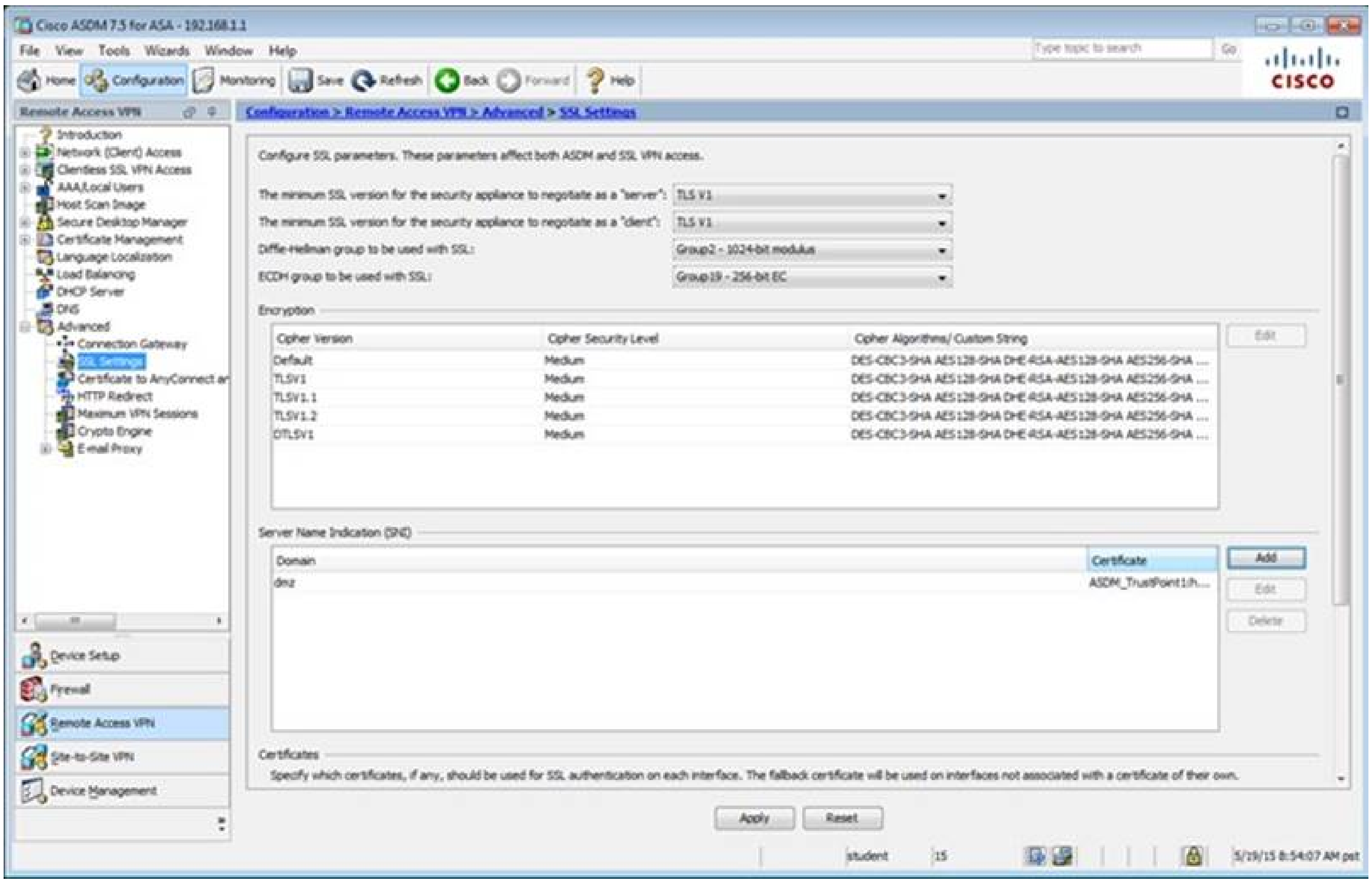


Configuration > Remote Access VPN > Advanced

This 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
- E-mail Proxy

student 15 5/19/15 8:52:47 AM pst



Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

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

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

Encryption

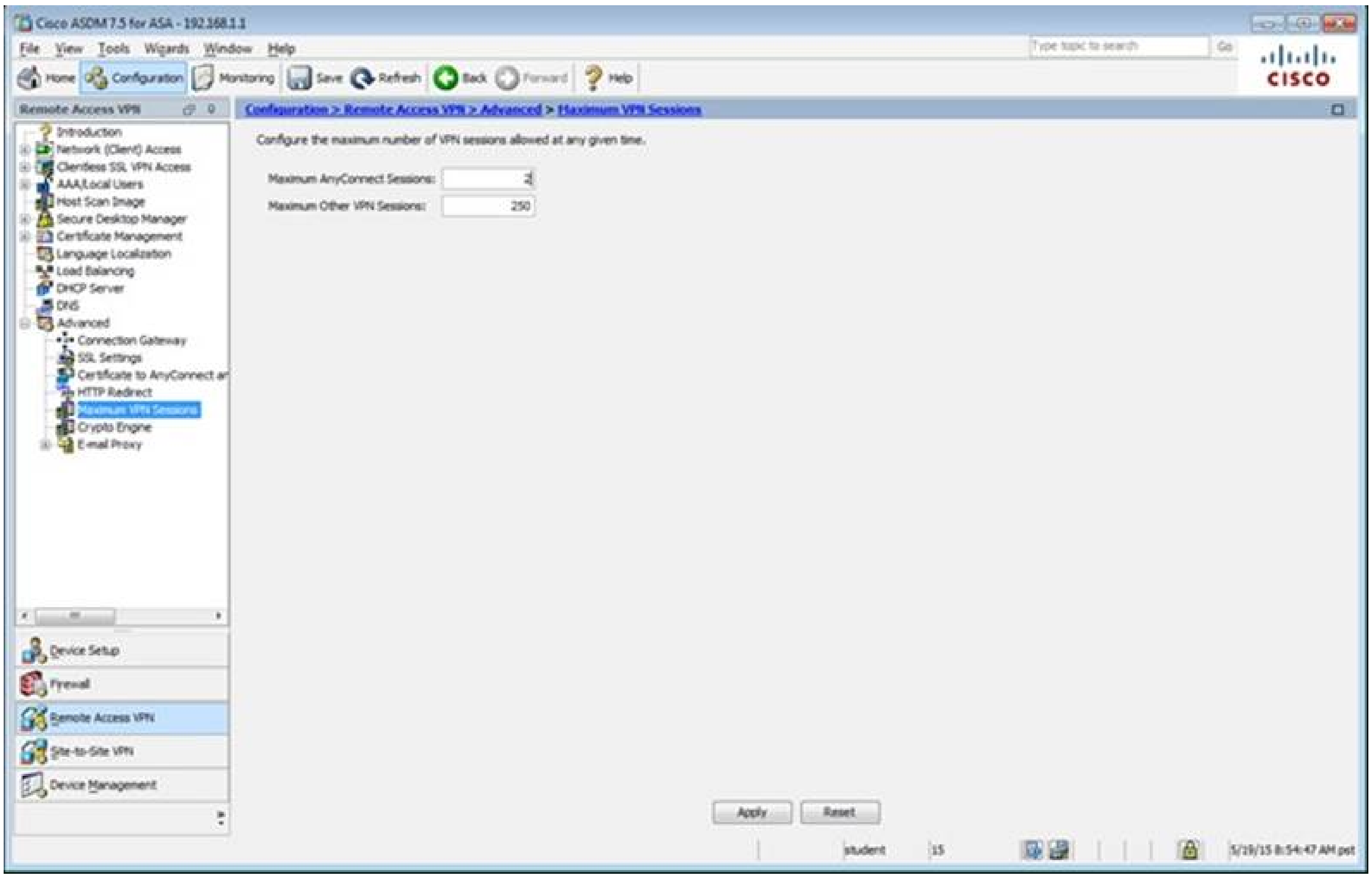
Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium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

Server Name Indication (SNI)

Domain	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.

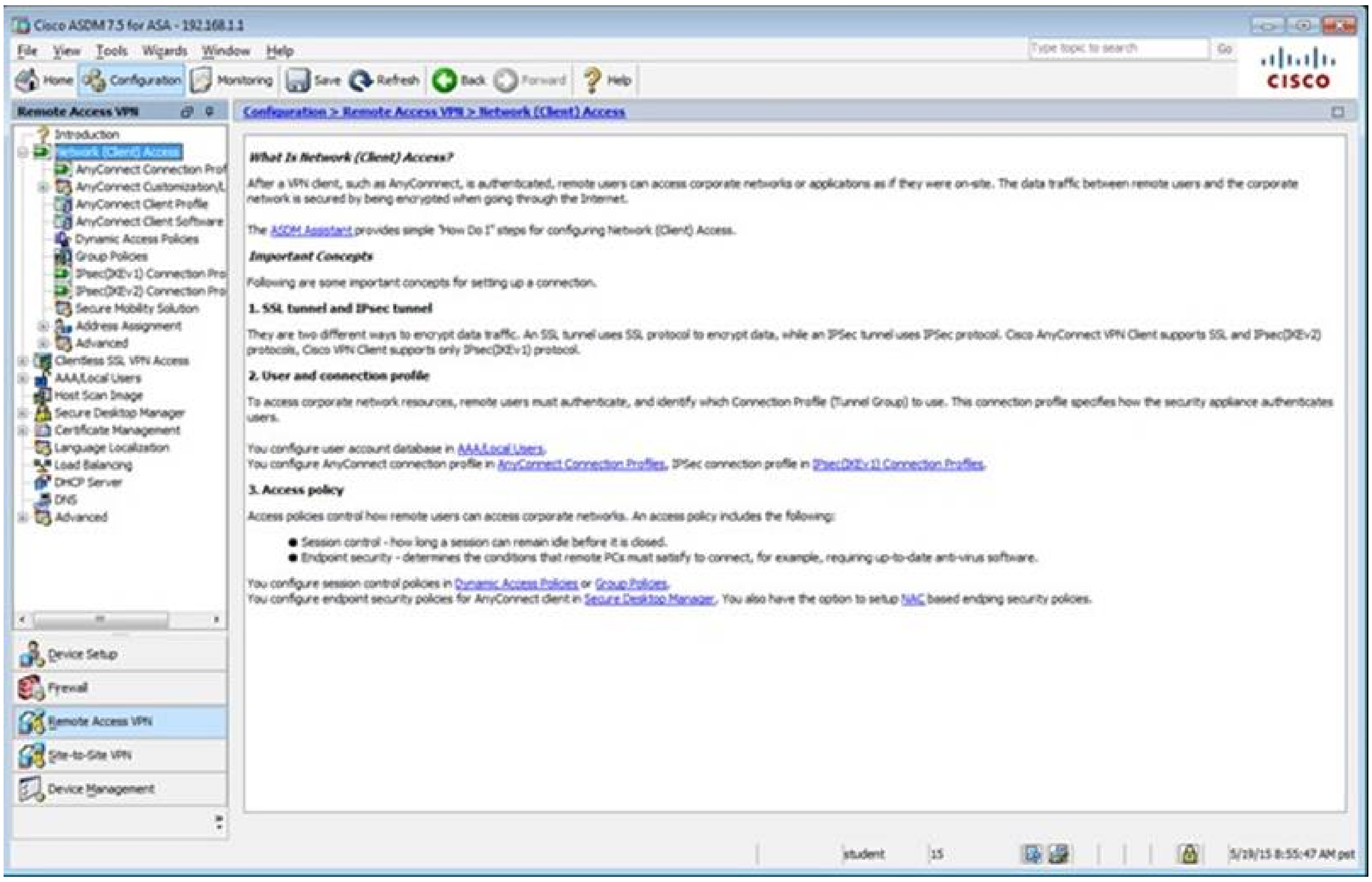


Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions

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

Maximum AnyConnect Sessions: 2

Maximum Other VPN Sessions: 250



Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

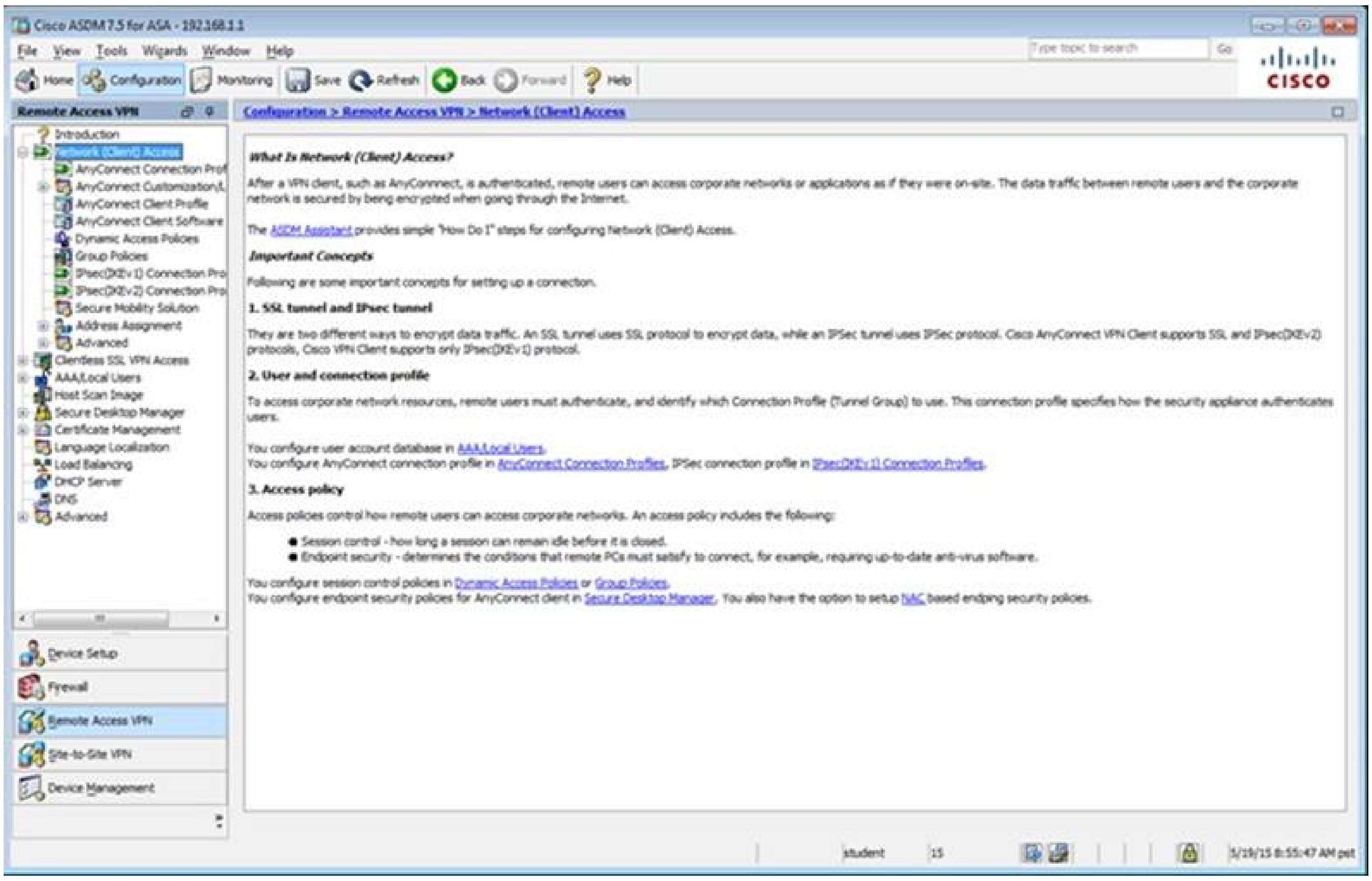
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles, IPSec connection profile in IPsec(IKEv1) Connection Profiles.

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 endping security policies.



Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

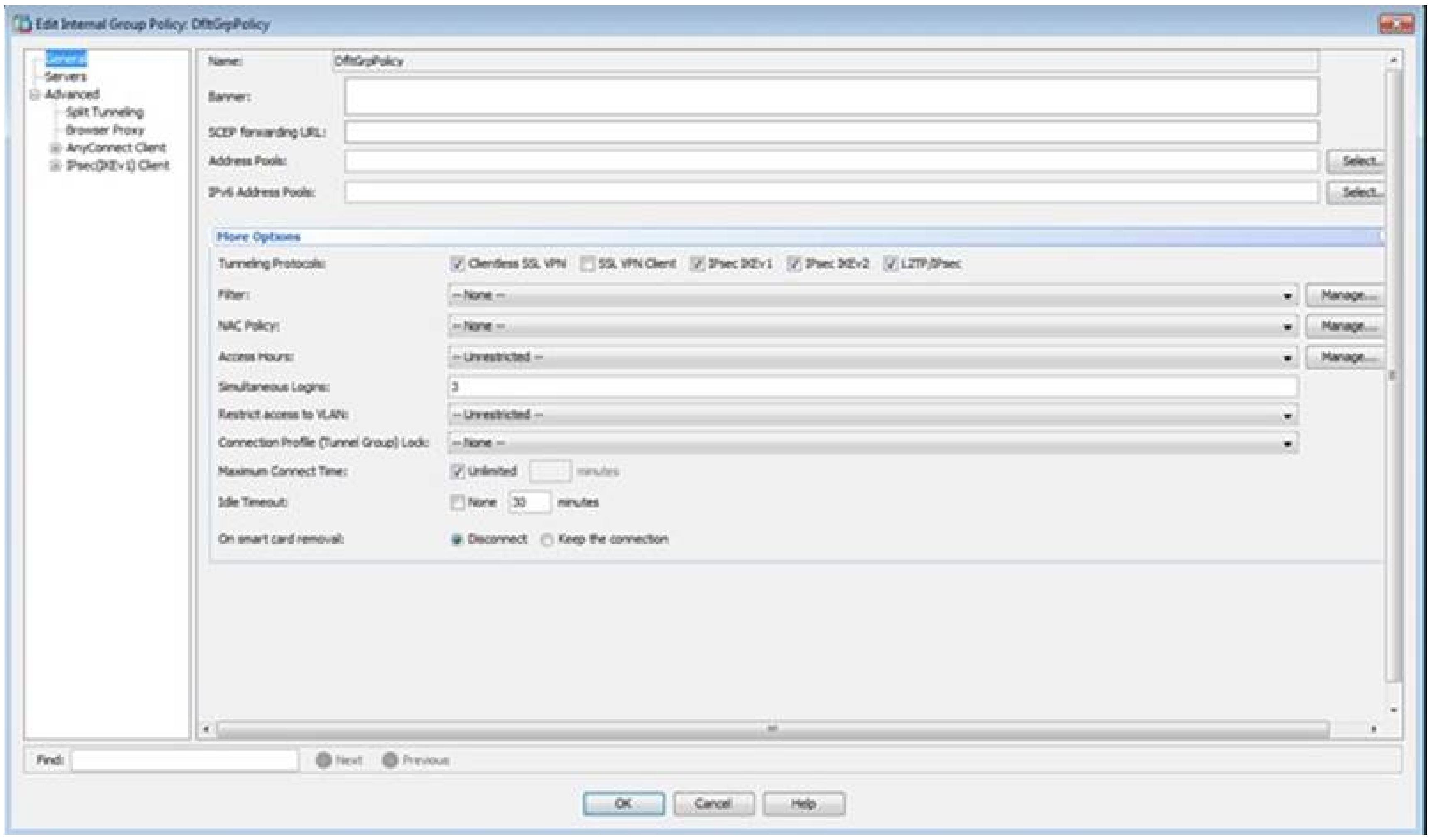
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles, IPSec connection profile in IPsec(IKEv1) Connection Profiles.

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 endping security policies.



Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Banner:

SCEP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None --

NAC Policy: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

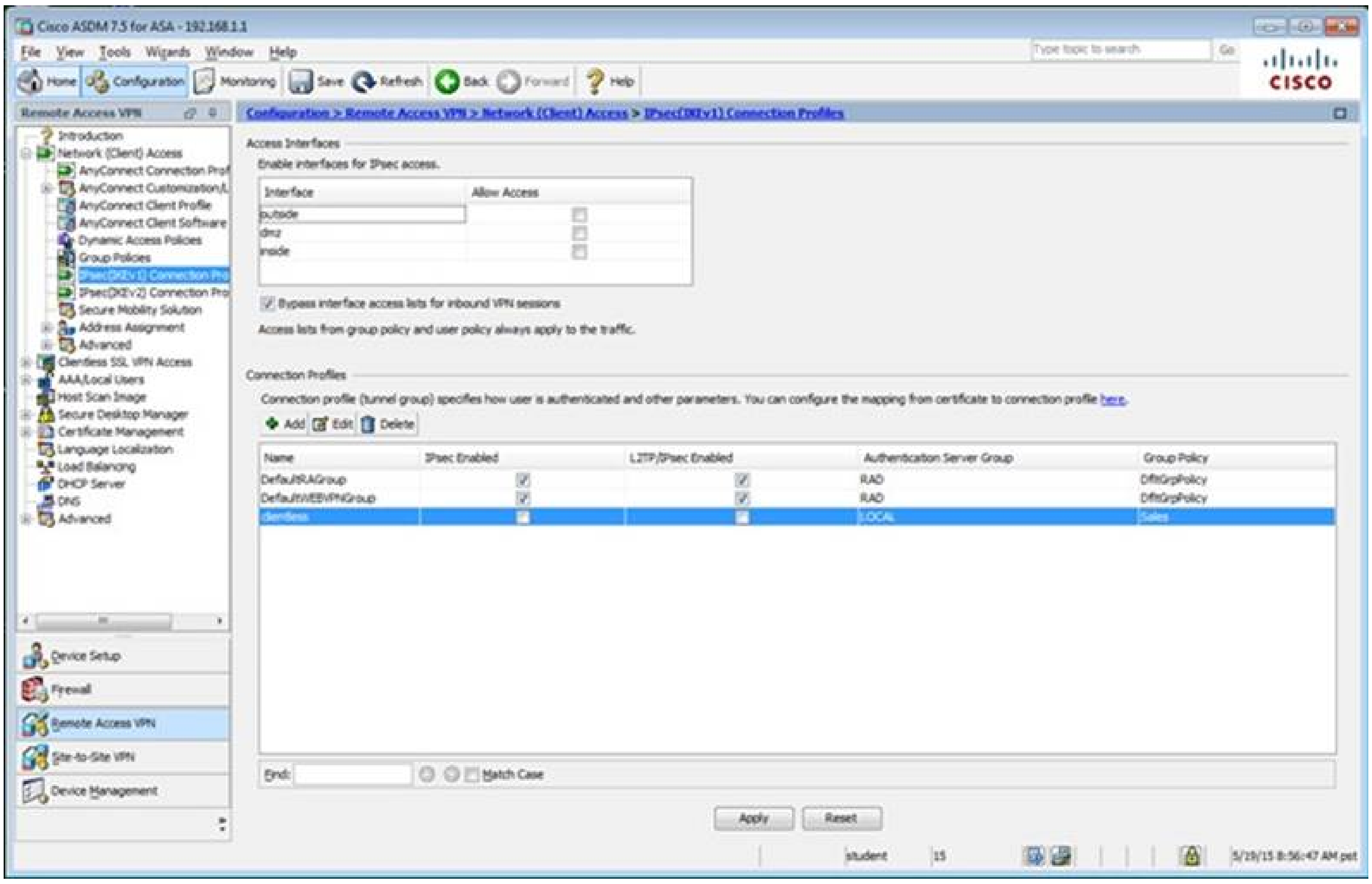
Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: ☐ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☐
dmz	☐
inside	☐

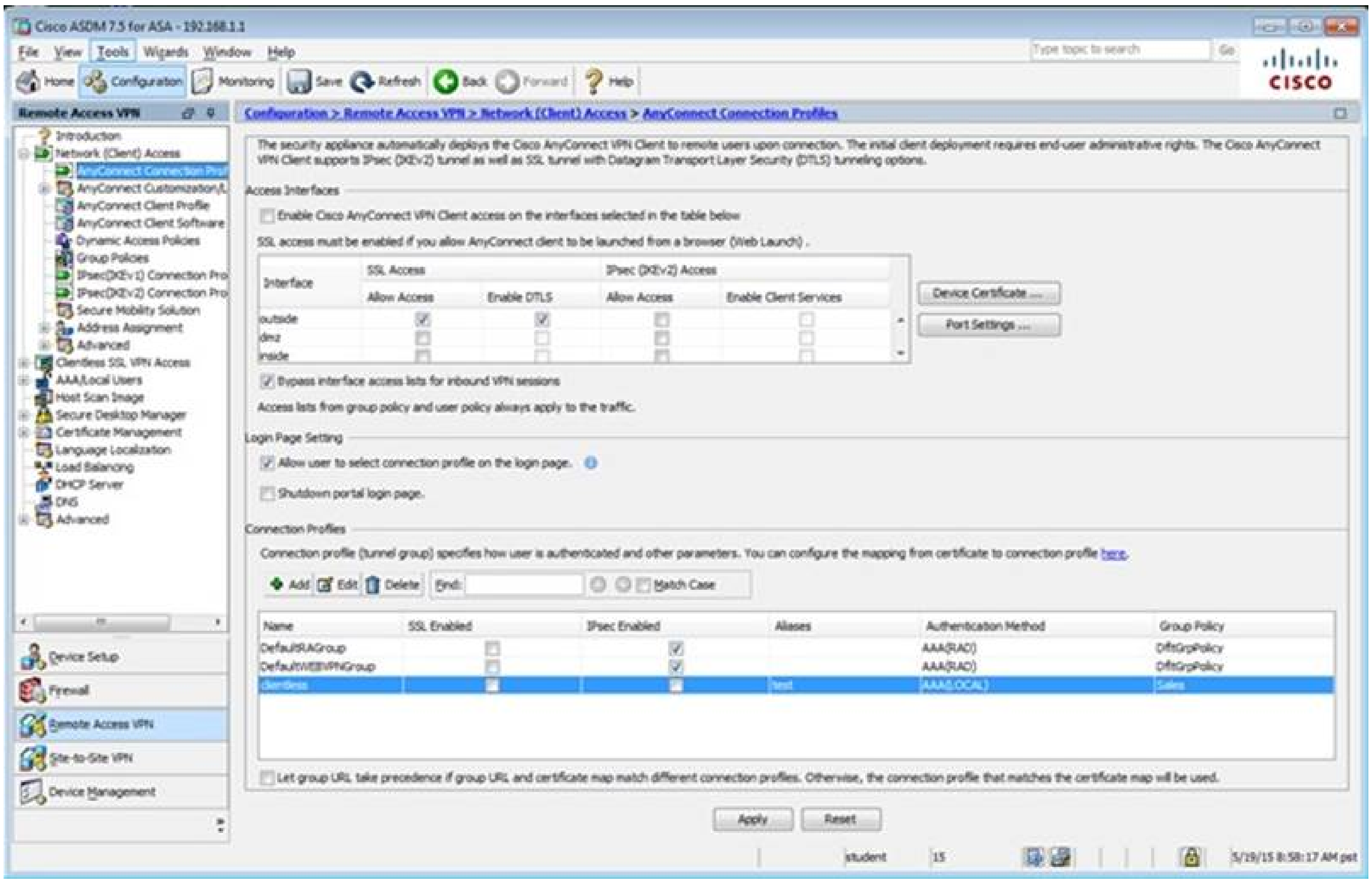
☑ Bypass interface access lists for inbound VPN sessions

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.

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	☑	☑	RAD	DfltGrpPolicy
DefaultWEBVPNGroup	☑	☑	RAD	DfltGrpPolicy
clientless	☐	☐	LOCAL	Sales



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	☑	☑	☐	☐
dmz	☐	☐	☐	☐
inside	☐	☐	☐	☐

☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

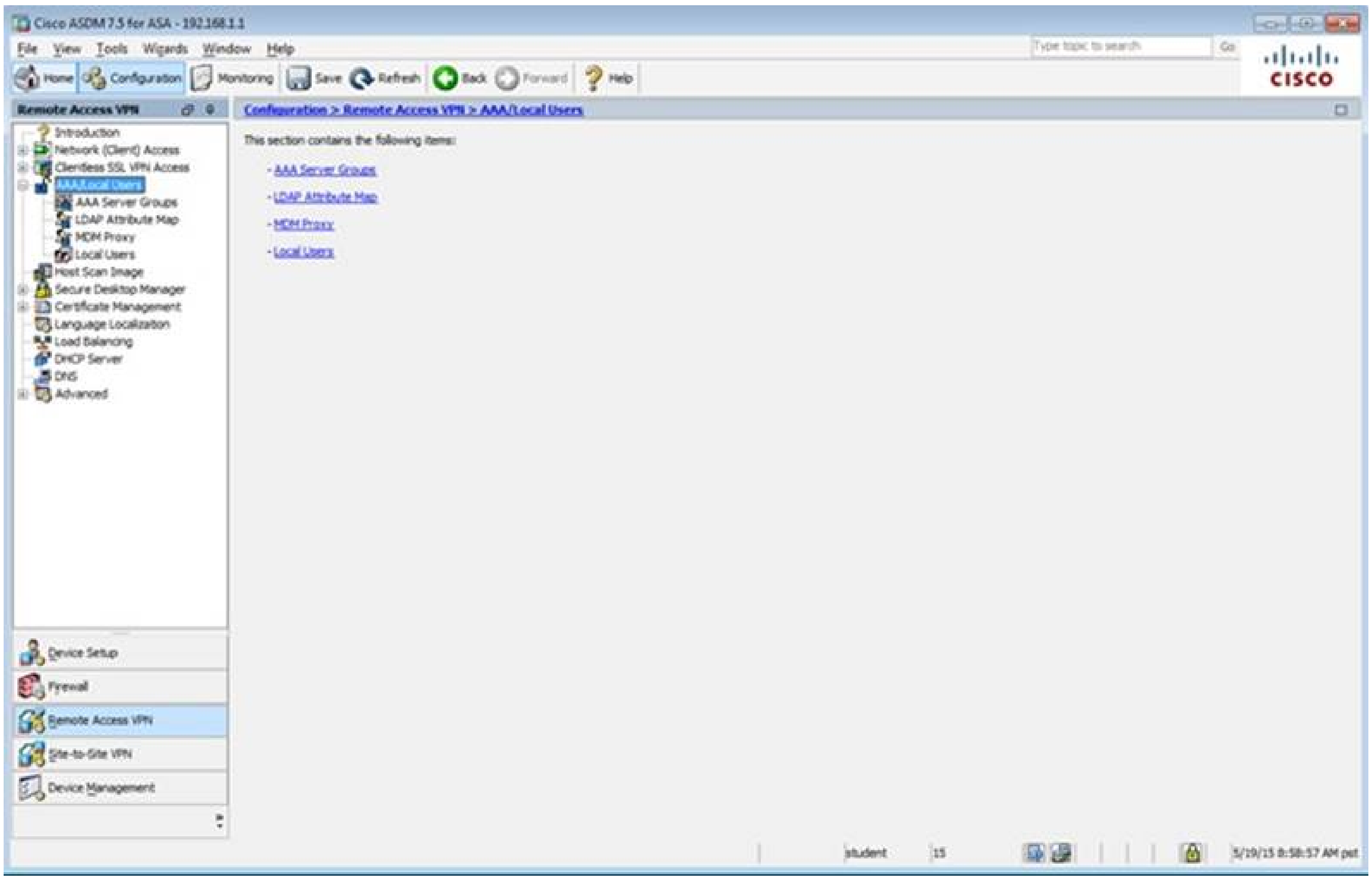
☐ Shutdown portal login page.

Connection Profiles

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

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☐	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	☐	☑		AAA(RAD)	DfltGrpPolicy
clientless	☑	☐	test	AAA(LOCAL)	Sales

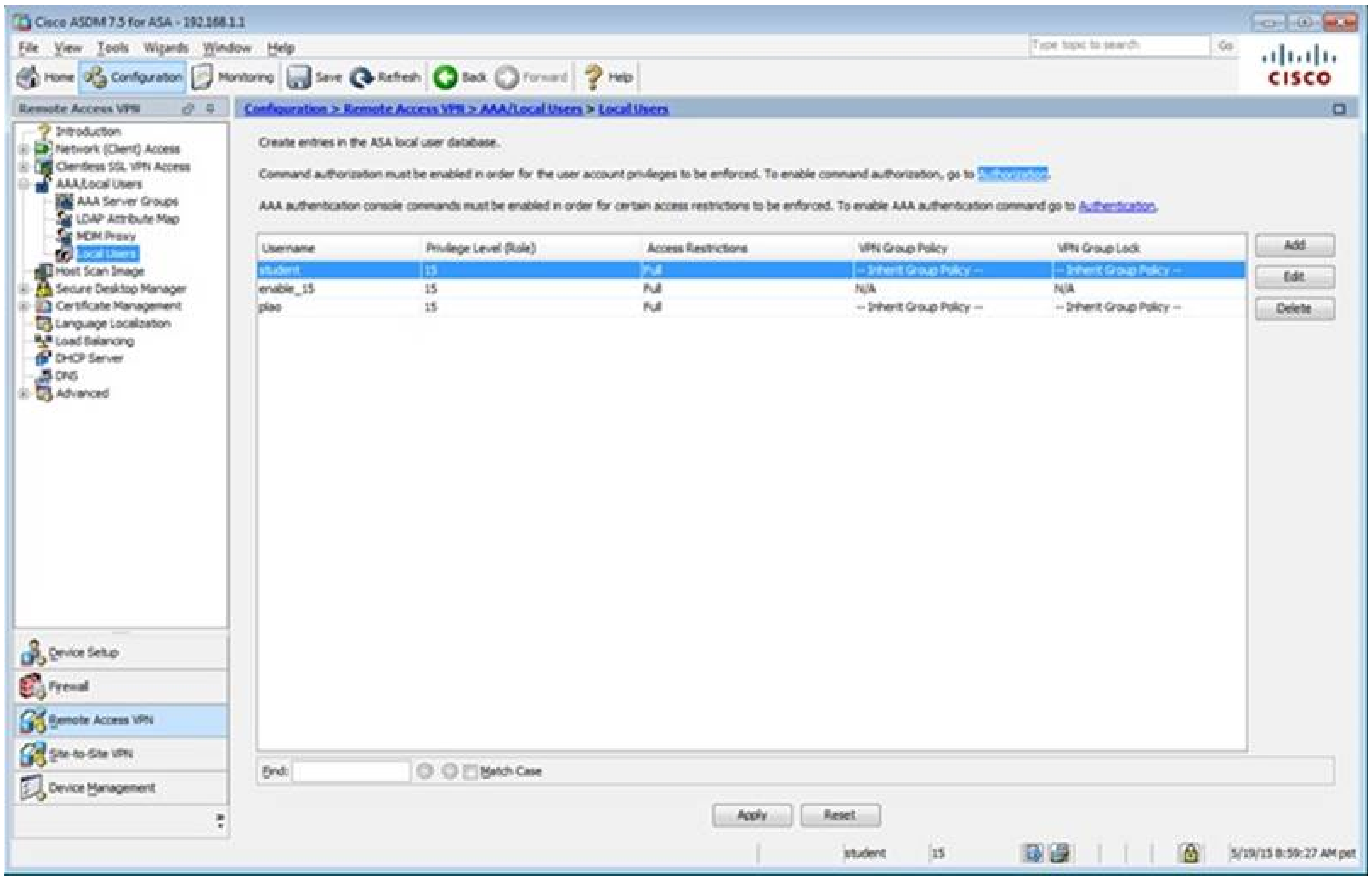
☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.



Configuration > Remote Access VPN > AAA/Local Users

This section contains the following items:

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



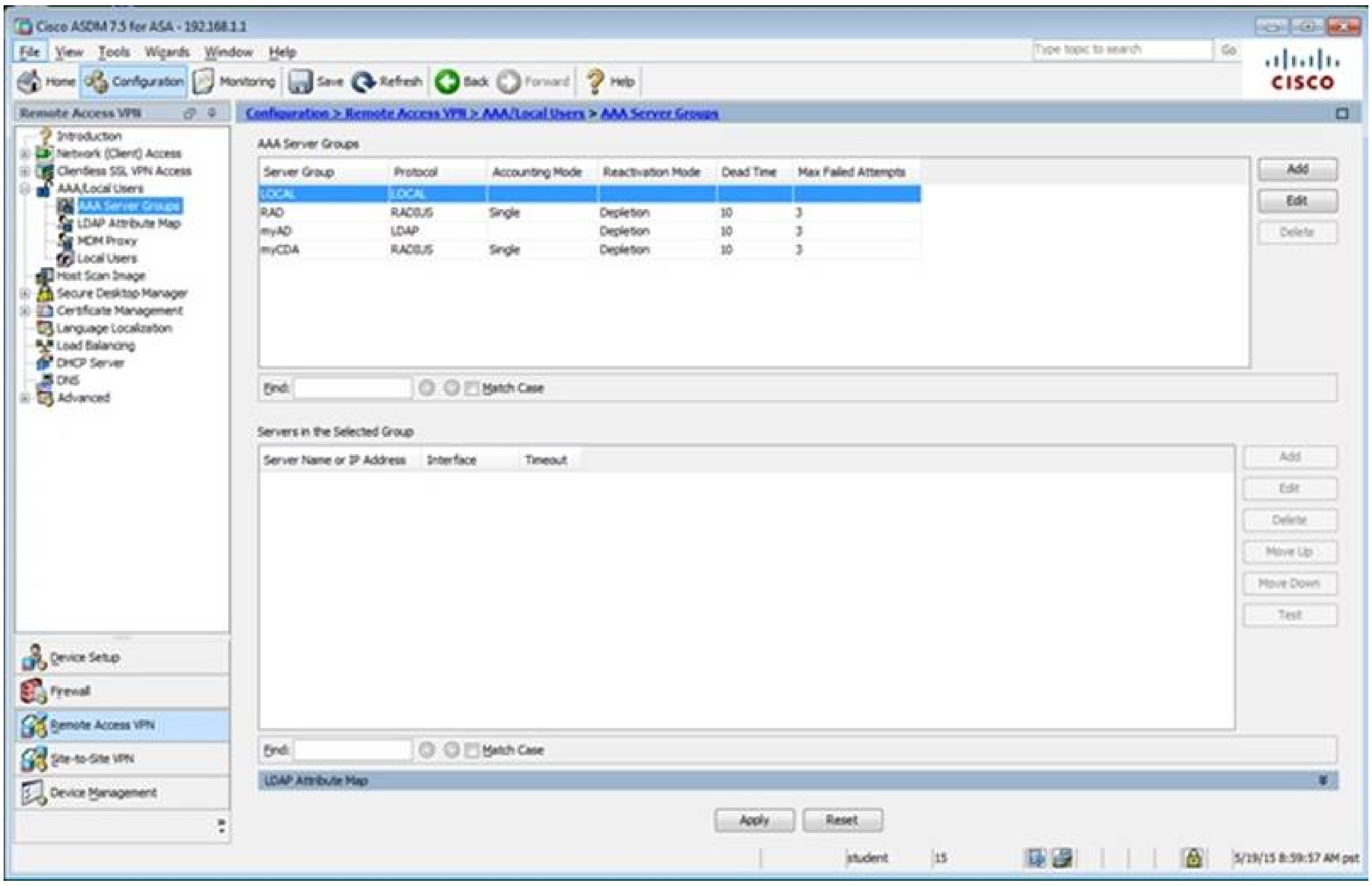
Configuration > Remote Access VPN > AAA/Local Users > Local Users

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 --



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

AAA Server Groups

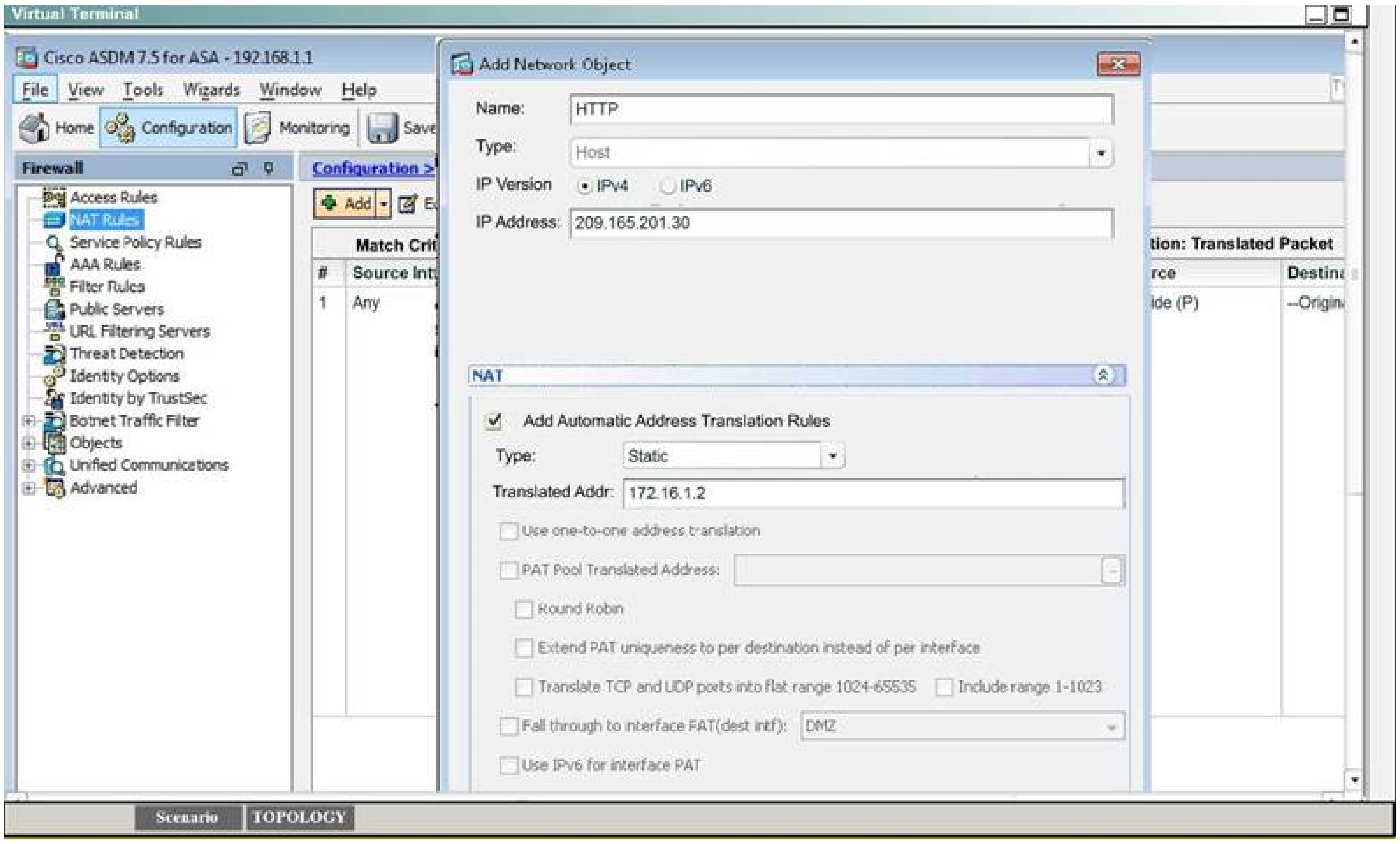
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
RAD	RADIUS	Single	Depletion	10	3
myAD	LDAP		Depletion	10	3
myCDA	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

Answer:

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



Add Network Object

Name: HTTP

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address: 209.165.201.30

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: 172.16.1.2

□ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

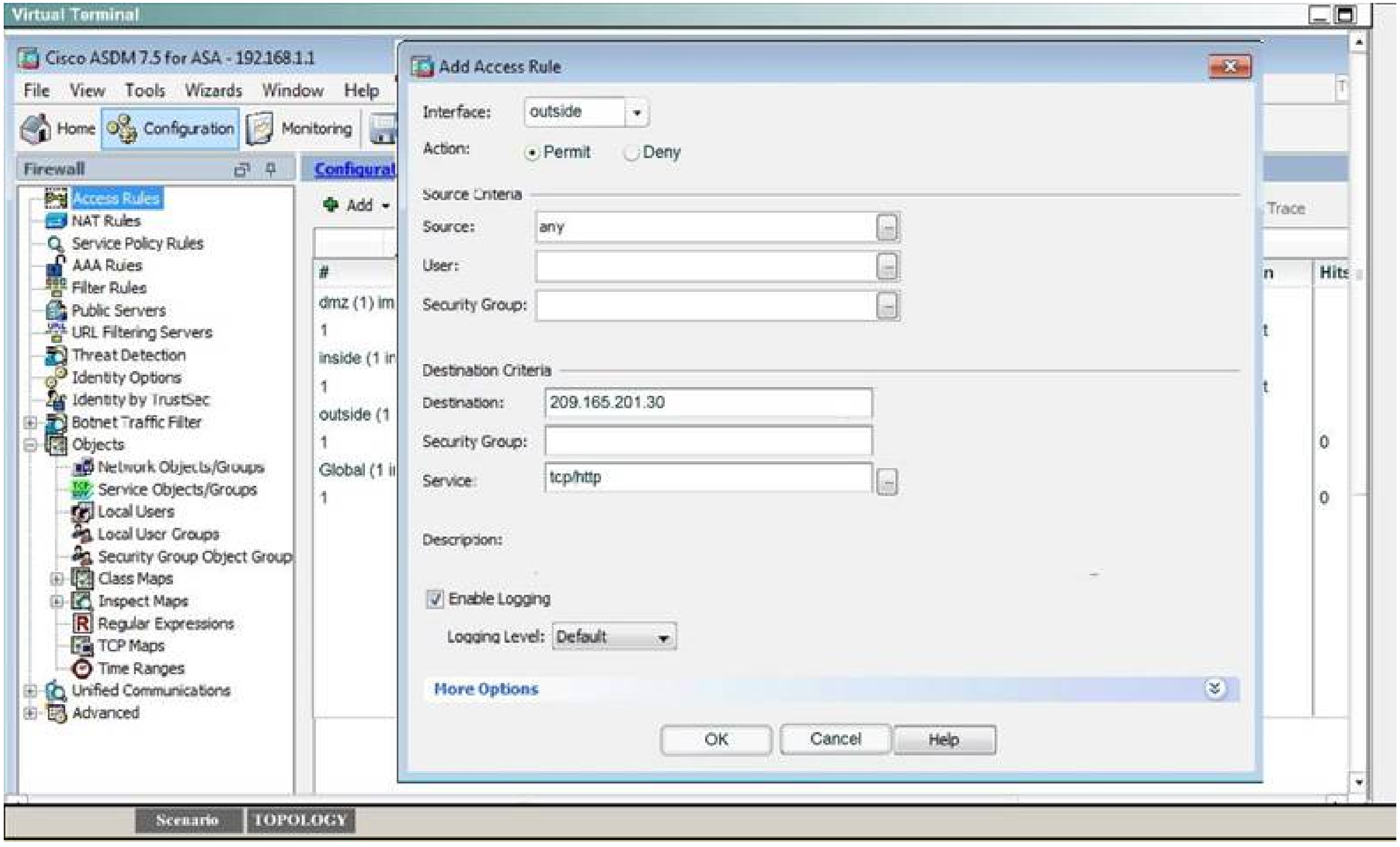
□ Extend PAT uniqueness to per destination instead of per interface

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

□ Fall through to interface PAT(dest intf): DMZ

□ Use IPv6 for interface PAT

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



Add Access Rule

Interface: outside

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: 209.165.201.30

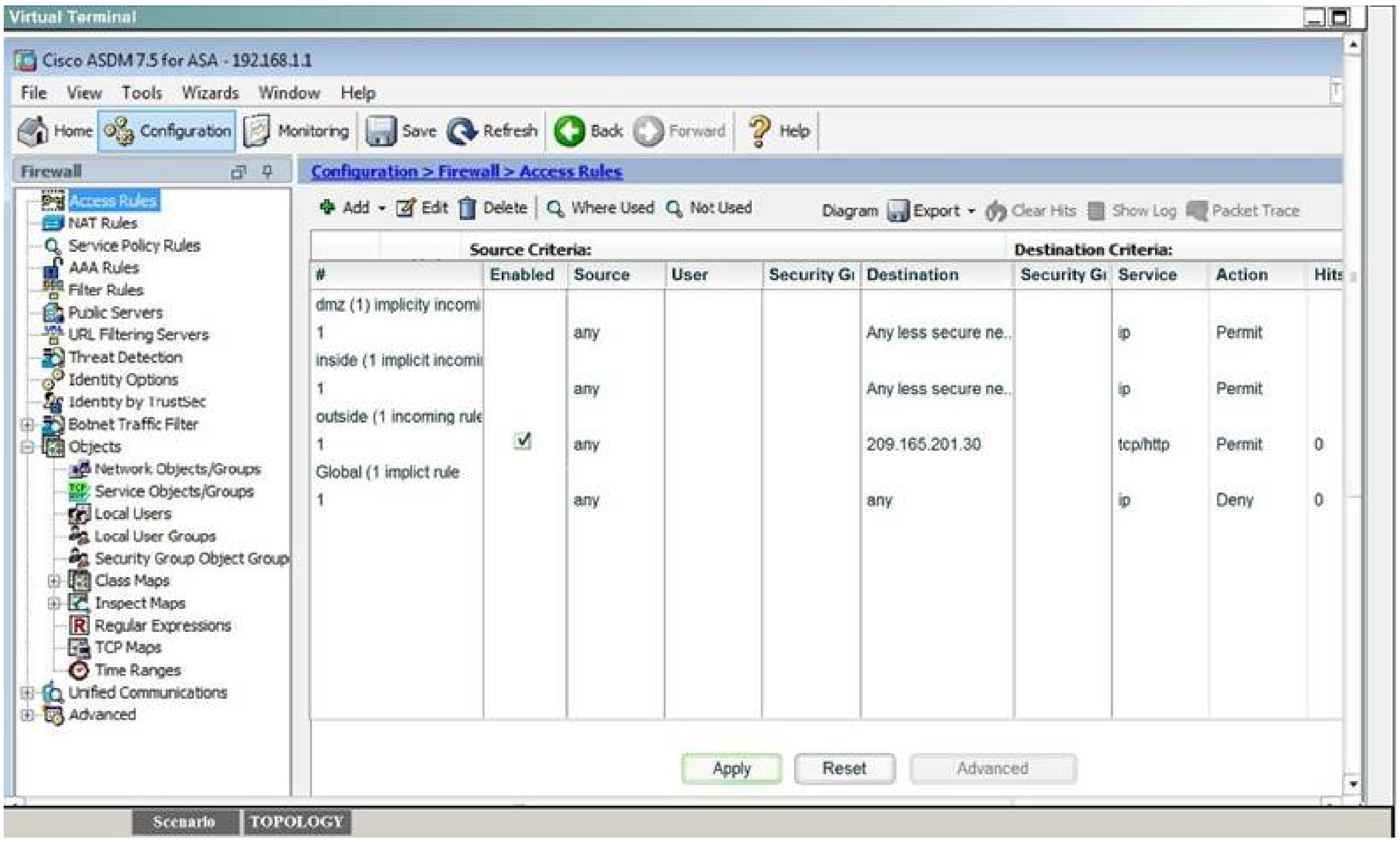
Security Group:

Service: tcp/http

Description:

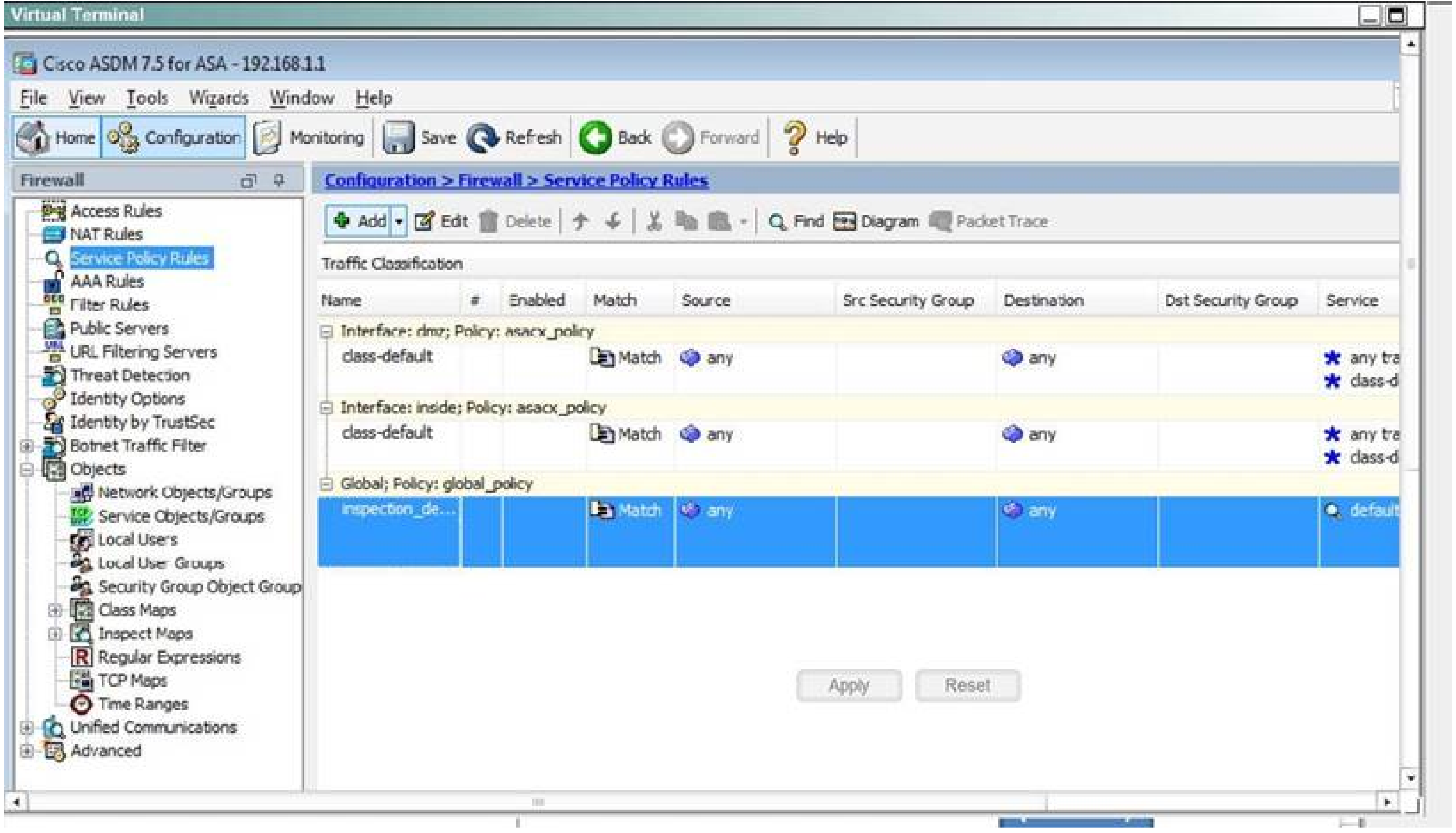
☑ Enable Logging

Logging Level: Default



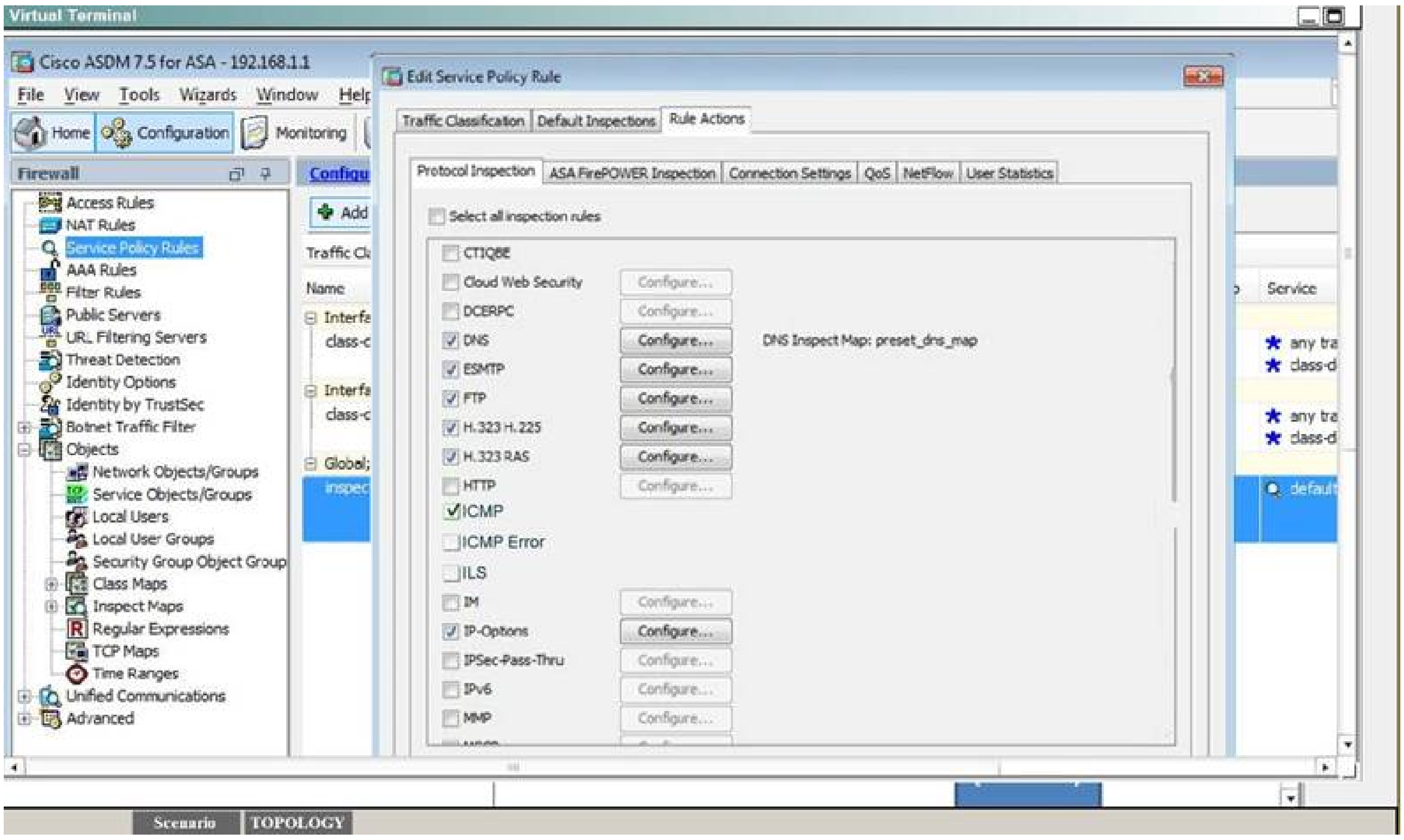
		Source Criteria:				Destination Criteria:			
#	Enabled	Source	User	Security Gi	Destination	Security Gi	Service	Action	Hits
dmz (1) implicity incomi									
1		any			Any less secure ne..		ip	Permit	
inside (1 implicit incomi									
1		any			Any less secure ne..		ip	Permit	
outside (1 incoming rule									
1	☑	any			209.165.201.30		tcp/http	Permit	0
Global (1 implict rule									
1		any			any		ip	Deny	0

You can verify using the outside PC to HTTP into 209.165.201.30.
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service
Interface: dmz; Policy: asacx_policy								
class-default			Match	any		any		any tra class-d
Interface: inside; Policy: asacx_policy								
class-default			Match	any		any		any tra class-d
Global; Policy: global_policy								
inspection_de...			Match	any		any		default

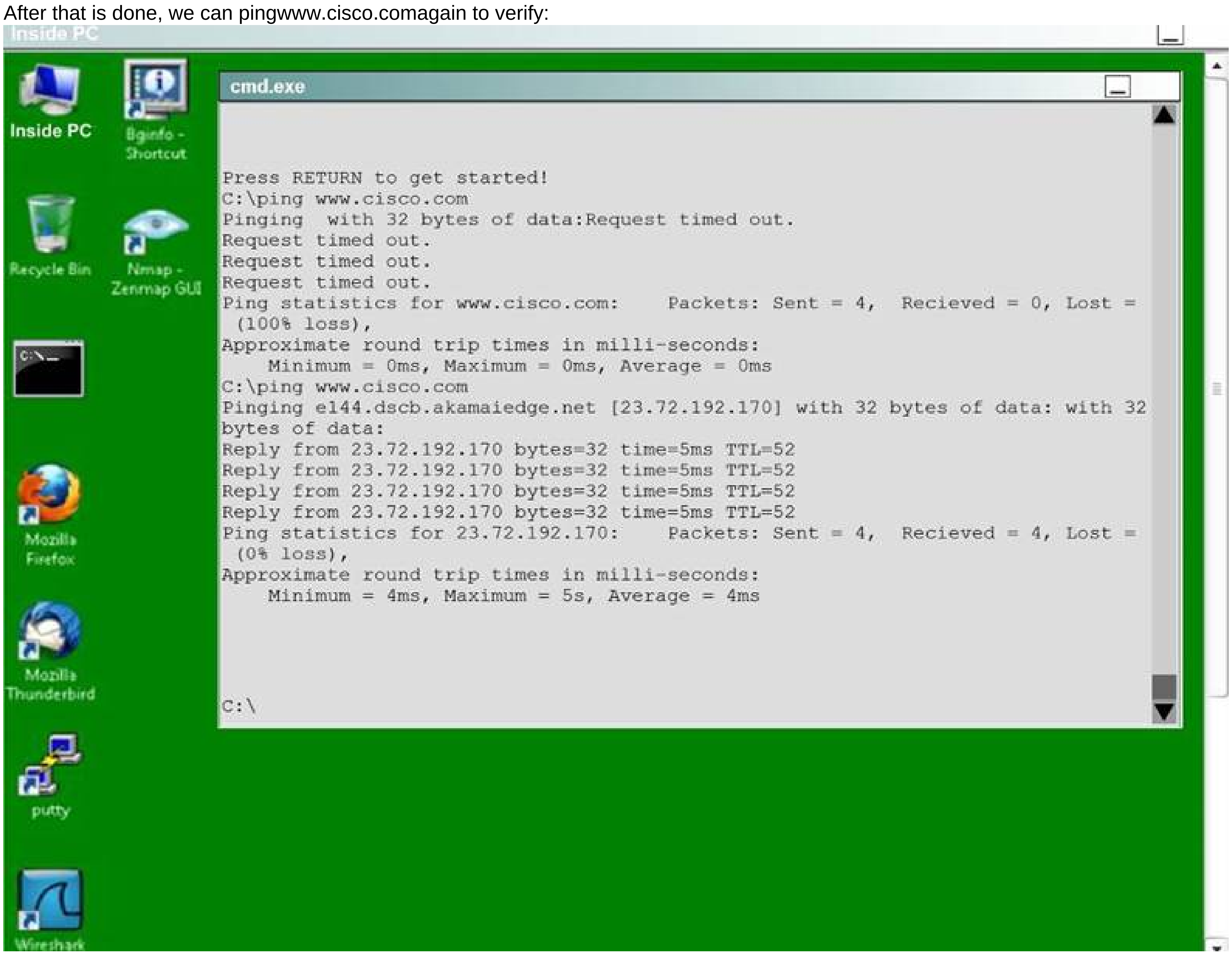
And then check the ICMP box only as shown below, then hit Apply.



□ Select all inspection rules

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

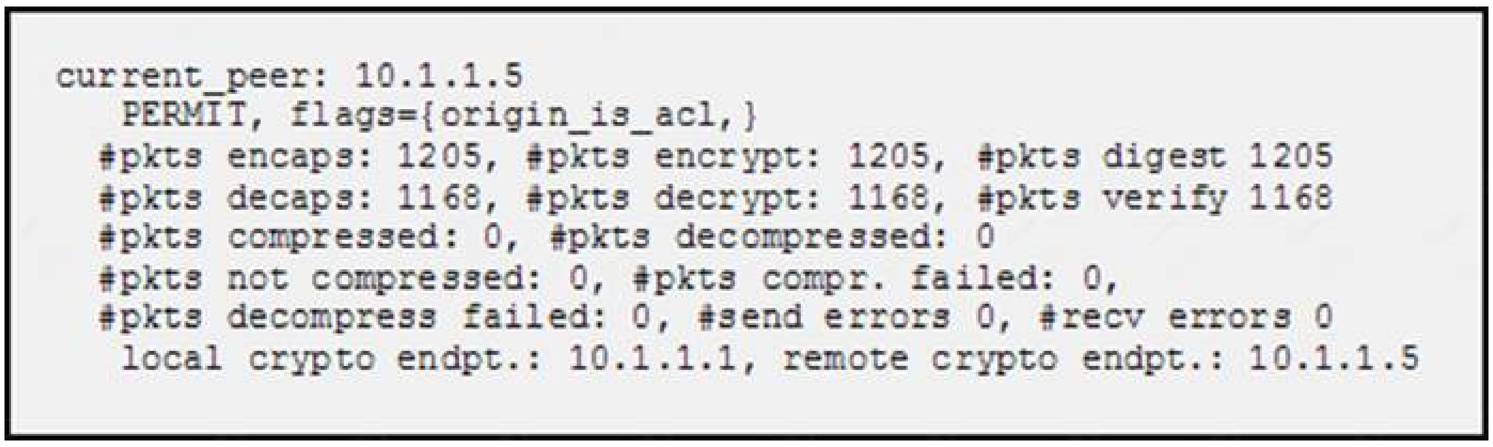
After that is done, we can pingwww.cisco.comagain to verify:



```
Press RETURN to get started!
C:\ping www.cisco.com
Pinging  with 32 bytes of data:Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for www.cisco.com:    Packets: Sent = 4,  Recieved = 0, Lost =
 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\ping www.cisco.com
Pinging e144.dscb.akamaiedge.net [23.72.192.170] with 32 bytes of data: with 32
bytes of data:
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Reply from 23.72.192.170 bytes=32 time=5ms TTL=52
Ping statistics for 23.72.192.170:    Packets: Sent = 4,  Recieved = 4, Lost =
 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5s, Average = 4ms


C:\
```

NEW QUESTION 8
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 9
What is one requirement for locking a wired or wireless device from ISE?

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

Answer: A

Explanation: Agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the AnyConnect, Cisco NAC Agent for Windows and Mac OS X) and remain on the client machine after installation, even when the client is not logged into the network. Agents can also be temporal (like the Cisco NAC Web Agent), removing themselves from the client machine after the login session has terminated.
Source:
http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010101.html

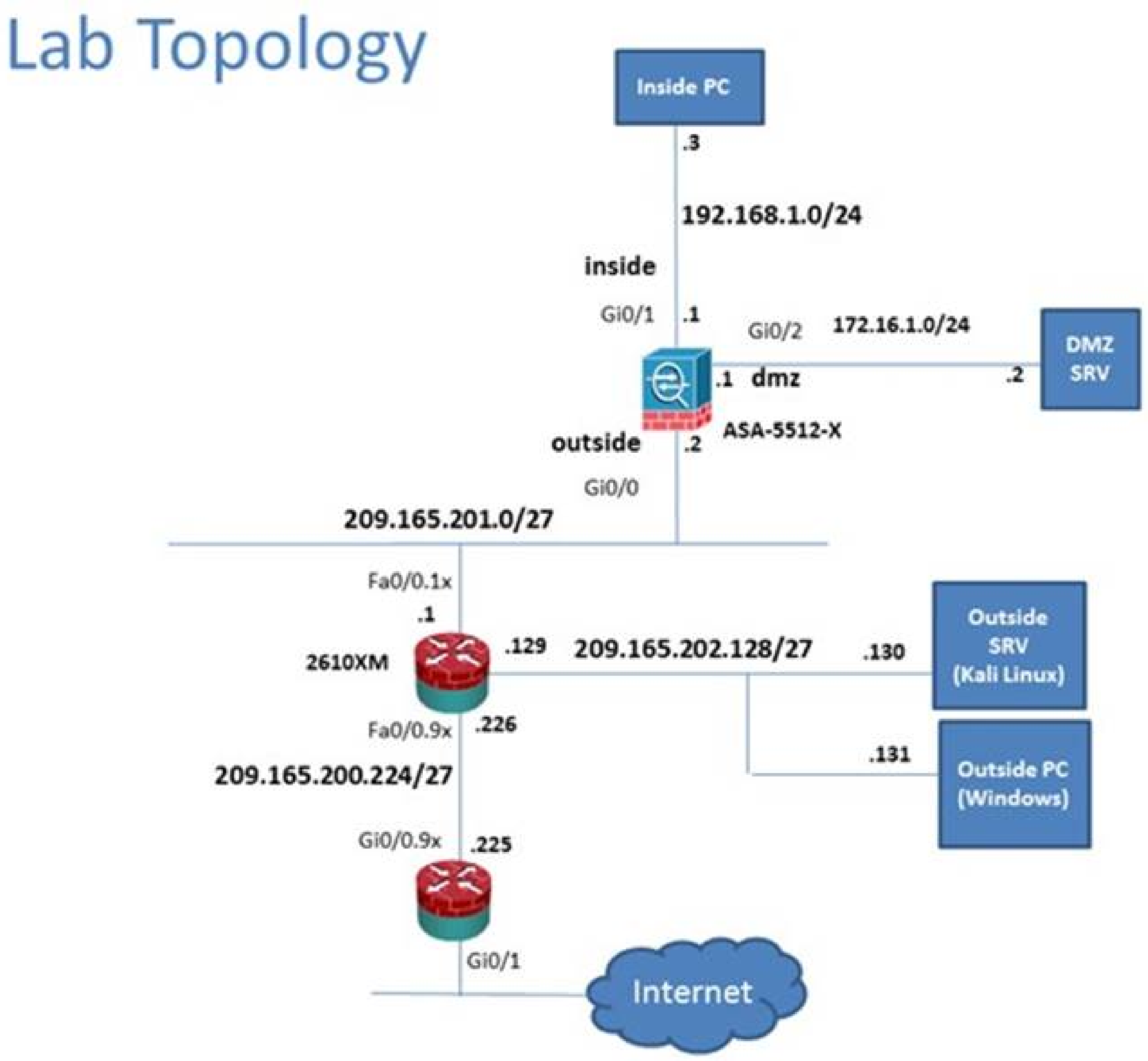
NEW QUESTION 10
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.
D. The isolated port can communicate only with other isolated ports.

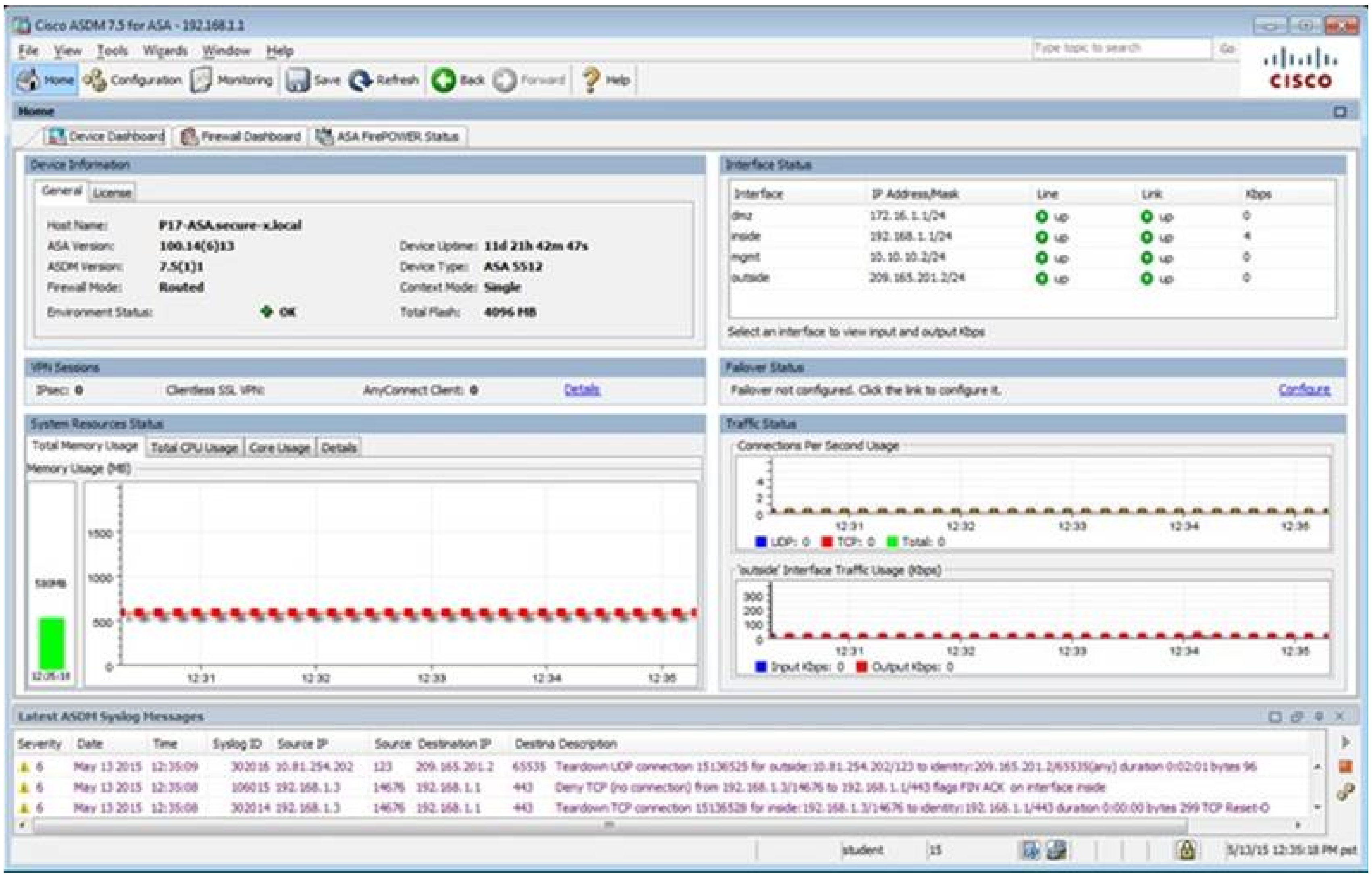
Answer: A

Explanation: Isolated -- An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.
Source:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html

NEW QUESTION 10
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



Device Information

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

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

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

Failover Status

Failover not configured. Click the link to configure it. Configure

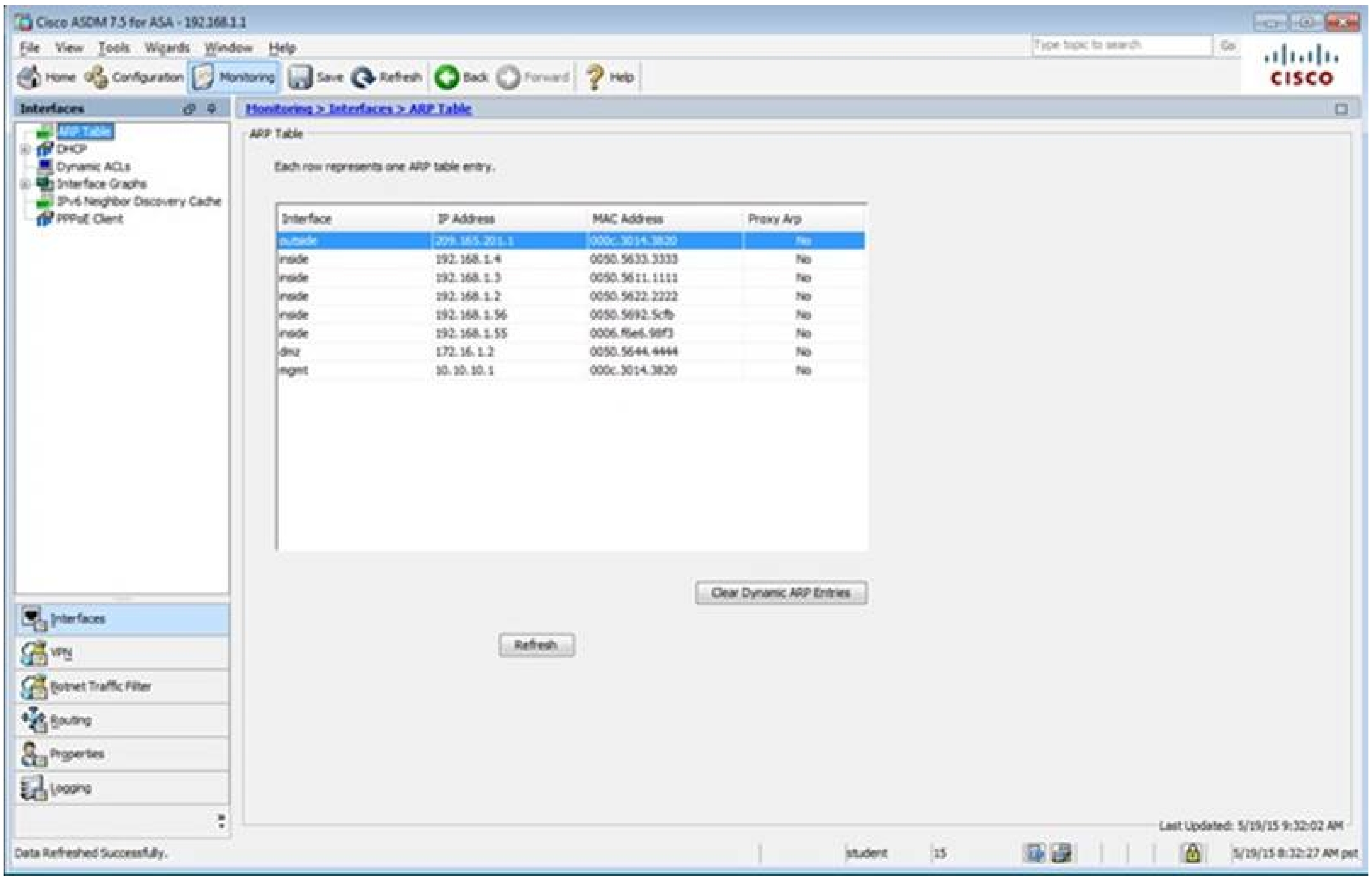
Traffic Status

UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

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 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
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Clear Dynamic ARP Entries
Refresh

Monitoring > Interfaces > ARP Table

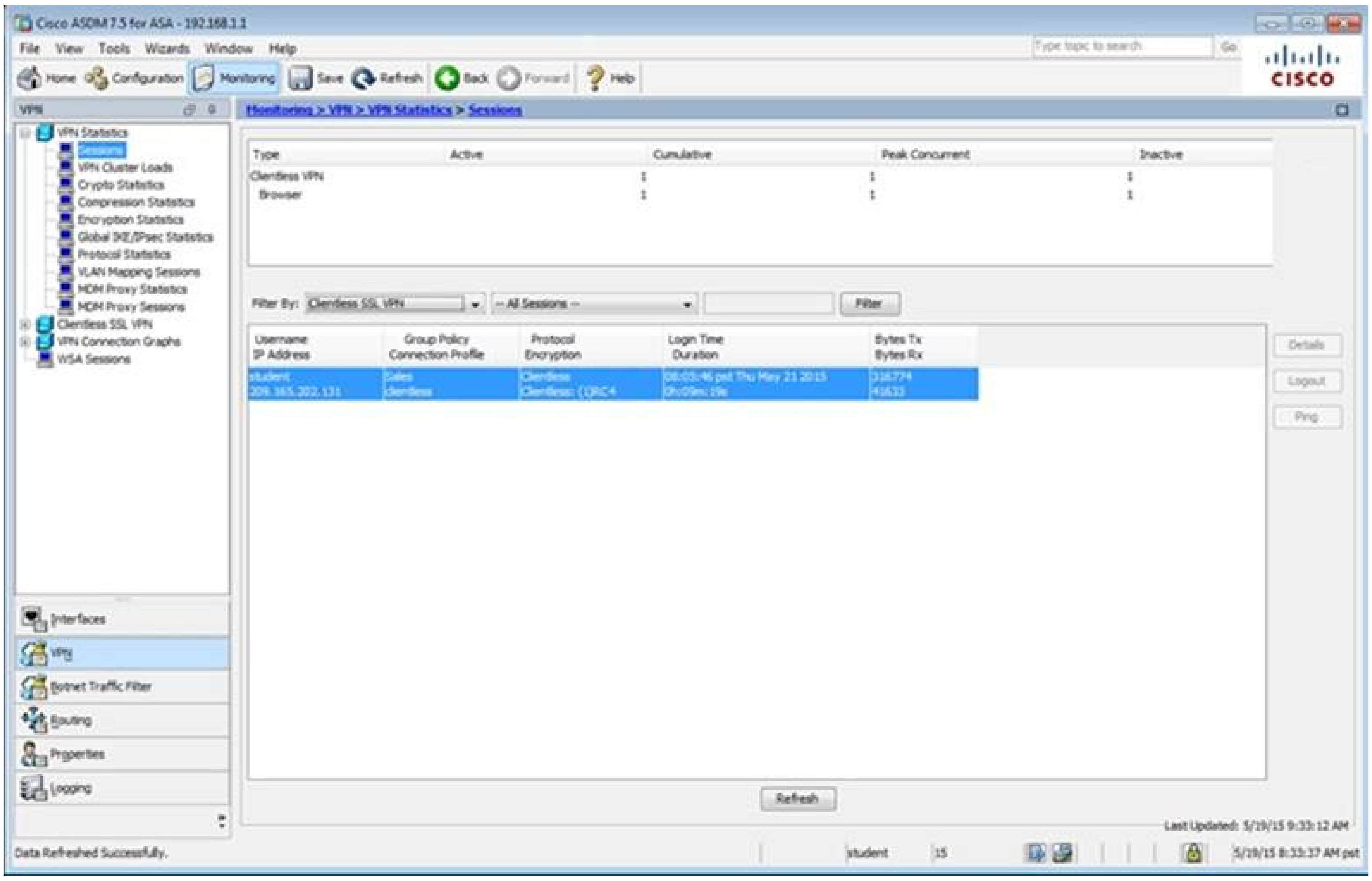
ARP Table

Each row represents one ARP table entry.

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

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

Data Refreshed Successfully. student 15 5/19/15 8:32:27 AM pst



Monitoring > VPN > VPN Statistics > Sessions

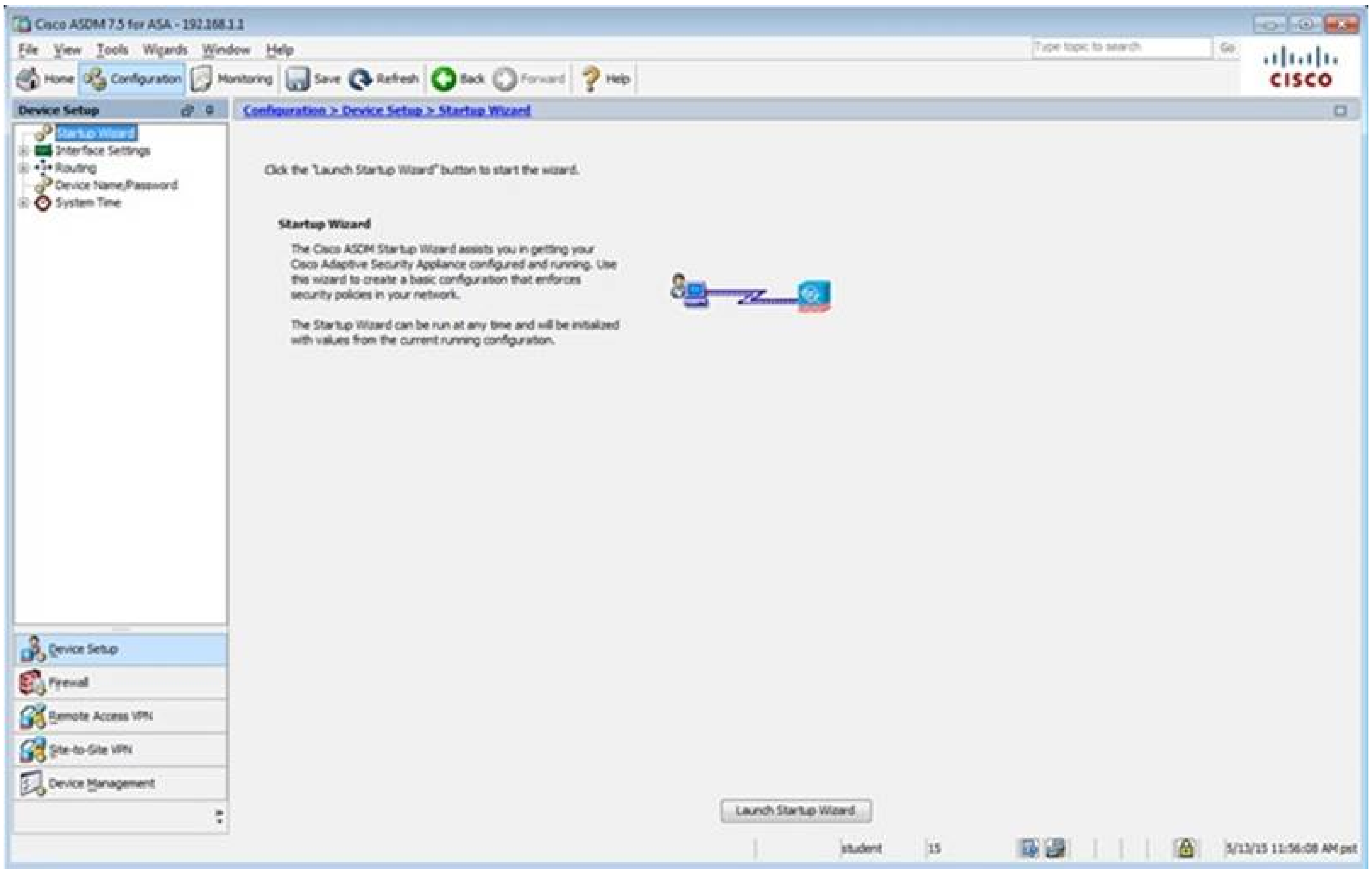
Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN	1	1	1	
Browser	1	1	1	

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

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: (1)RC4	08:05:46 pst Thu May 21 2015 0h:09m:19s	316774 41633

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

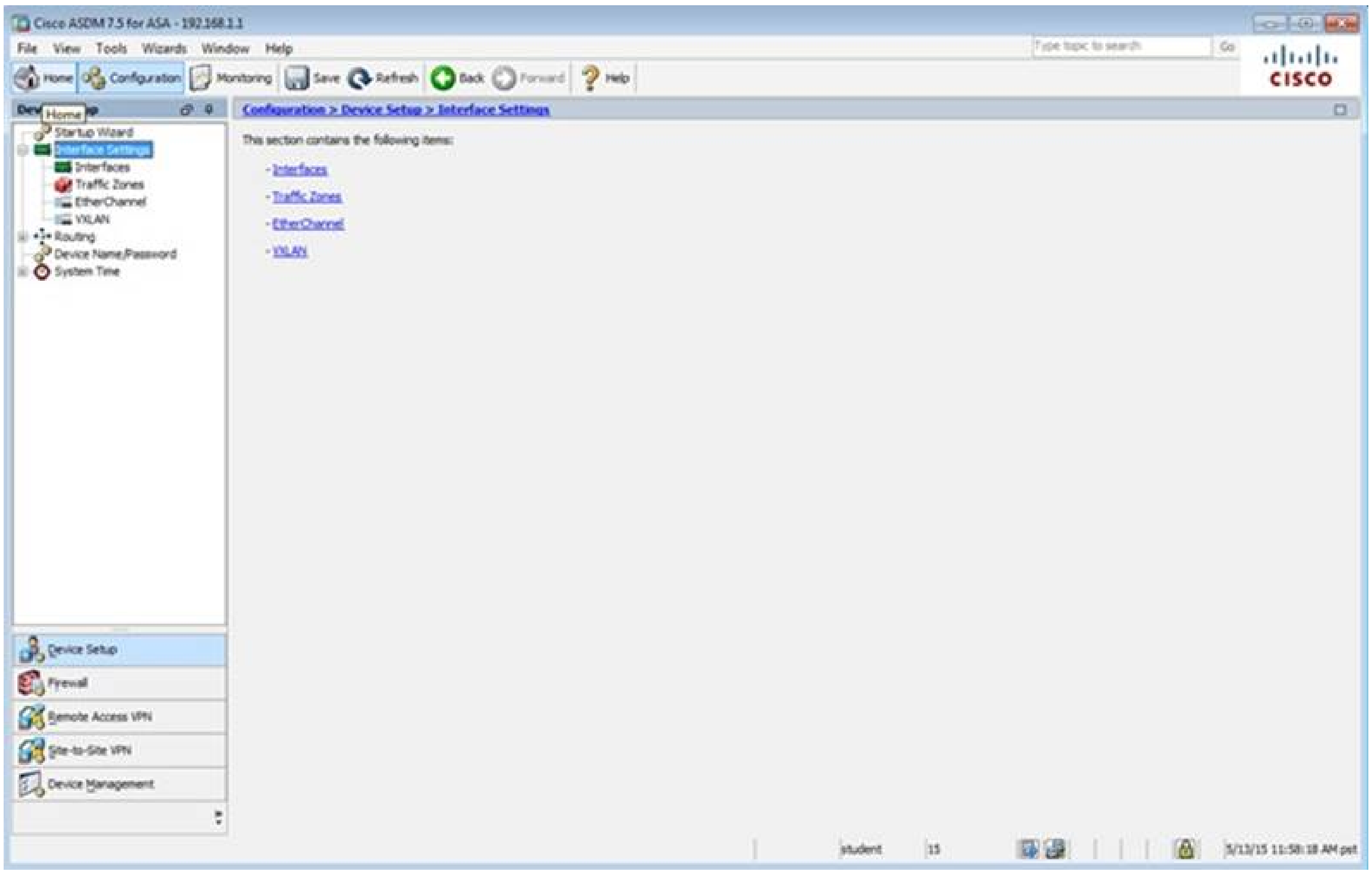
Configuration > Device Setup > Startup Wizard

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.

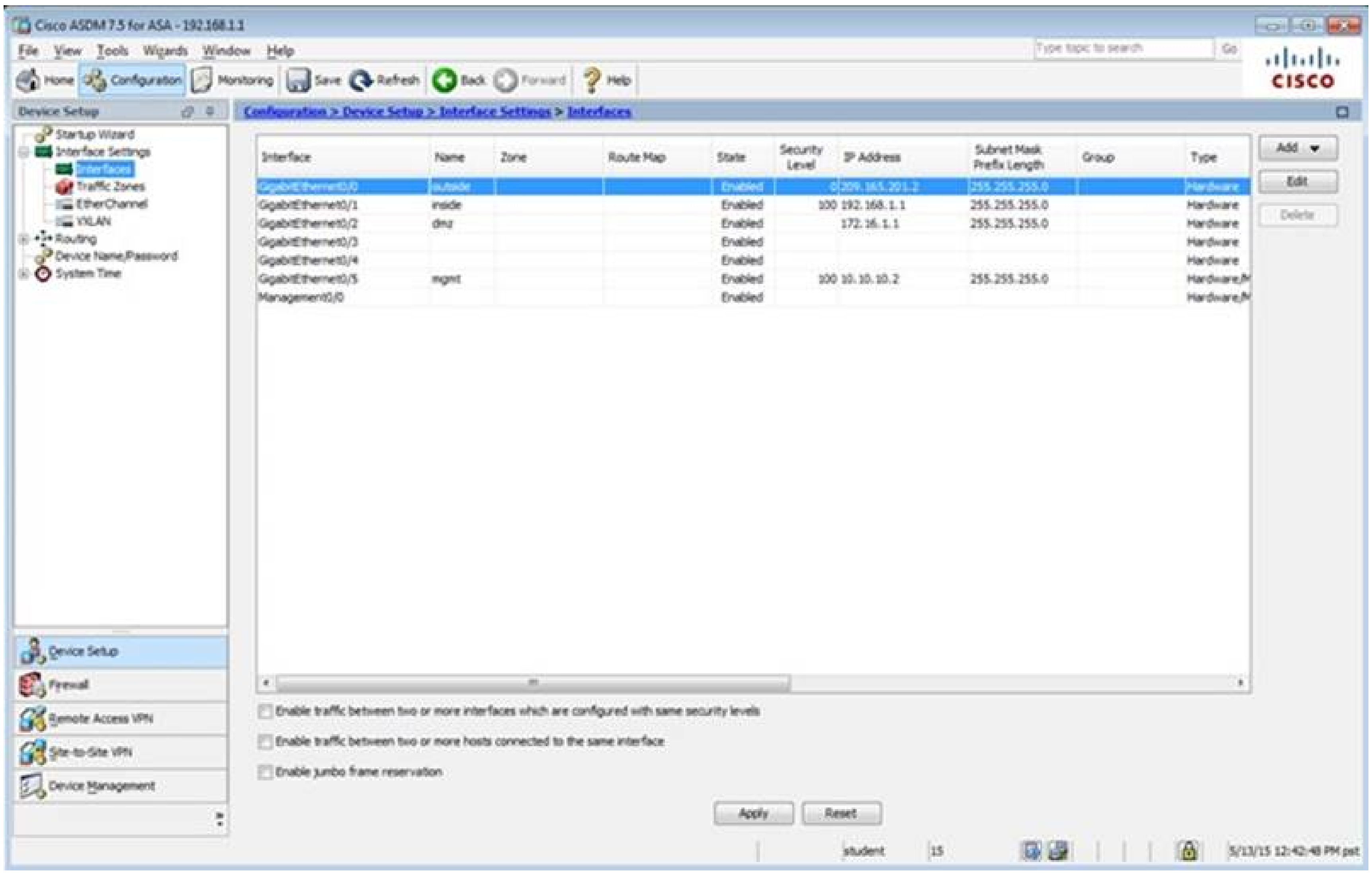


Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Device Setup > Interface Settings

This section contains the following items:

- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN



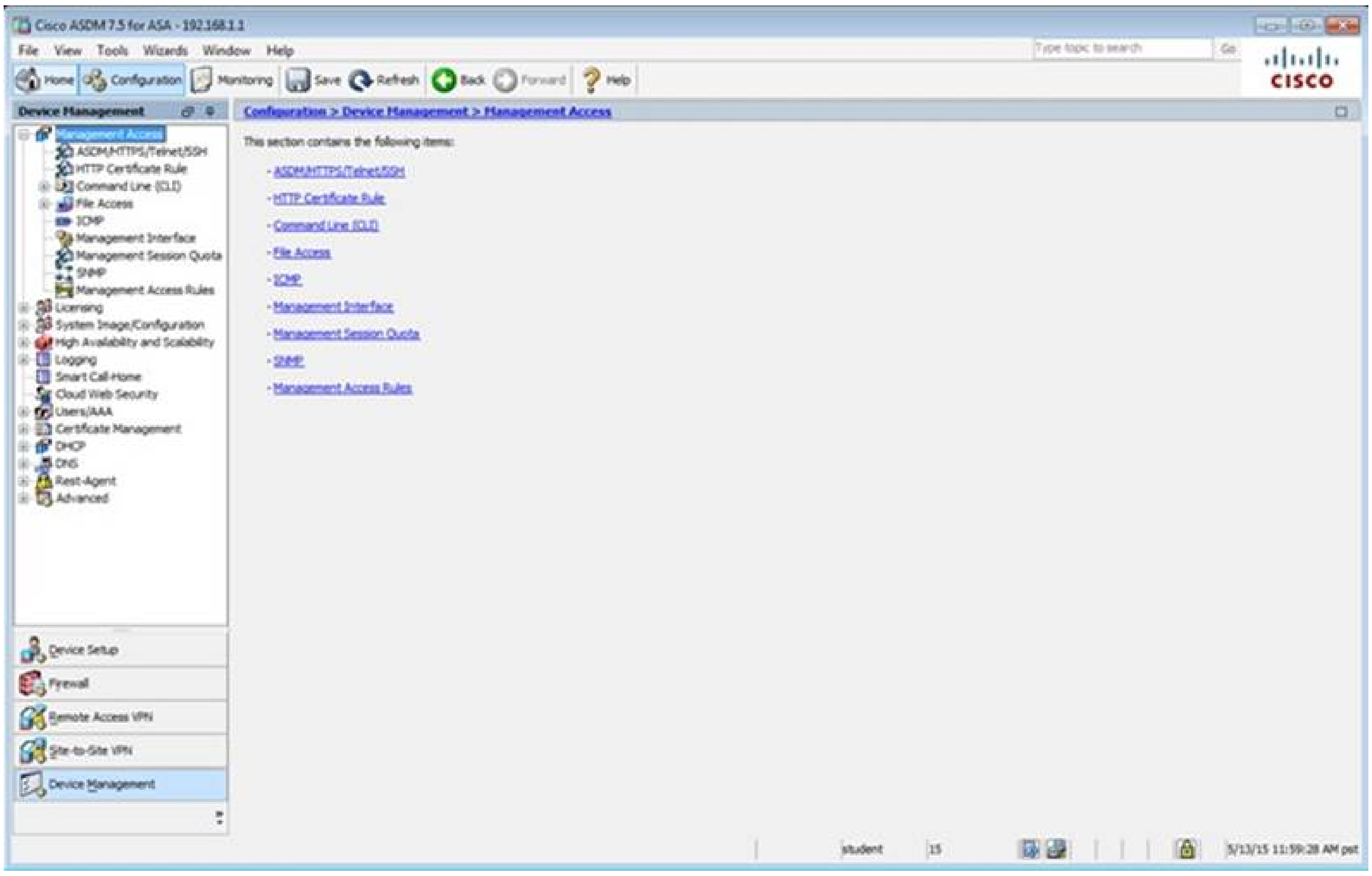
Configuration > Device Setup > Interface Settings > Interfaces

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

□ 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

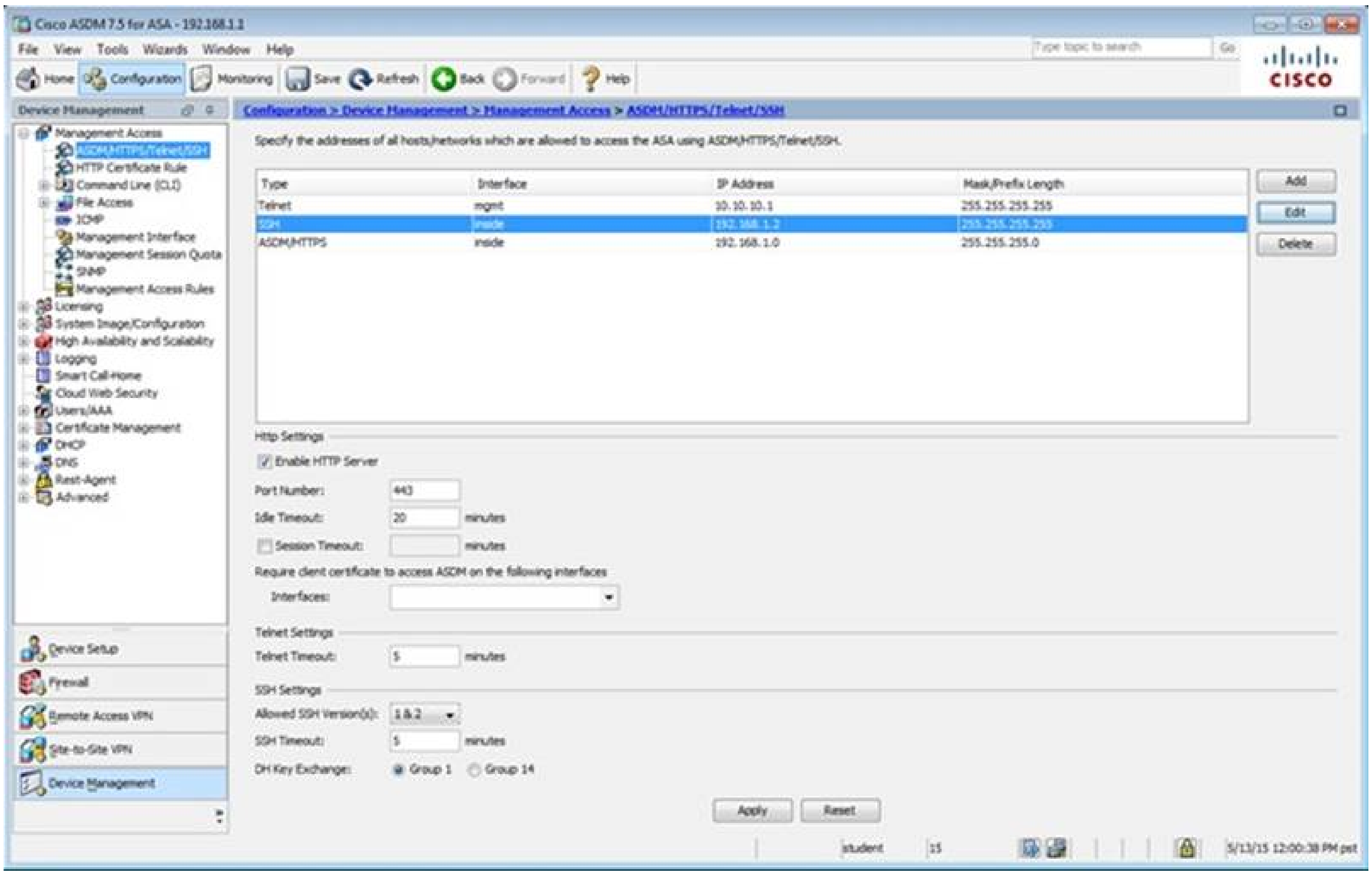
□ Enable jumbo frame reservation



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



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

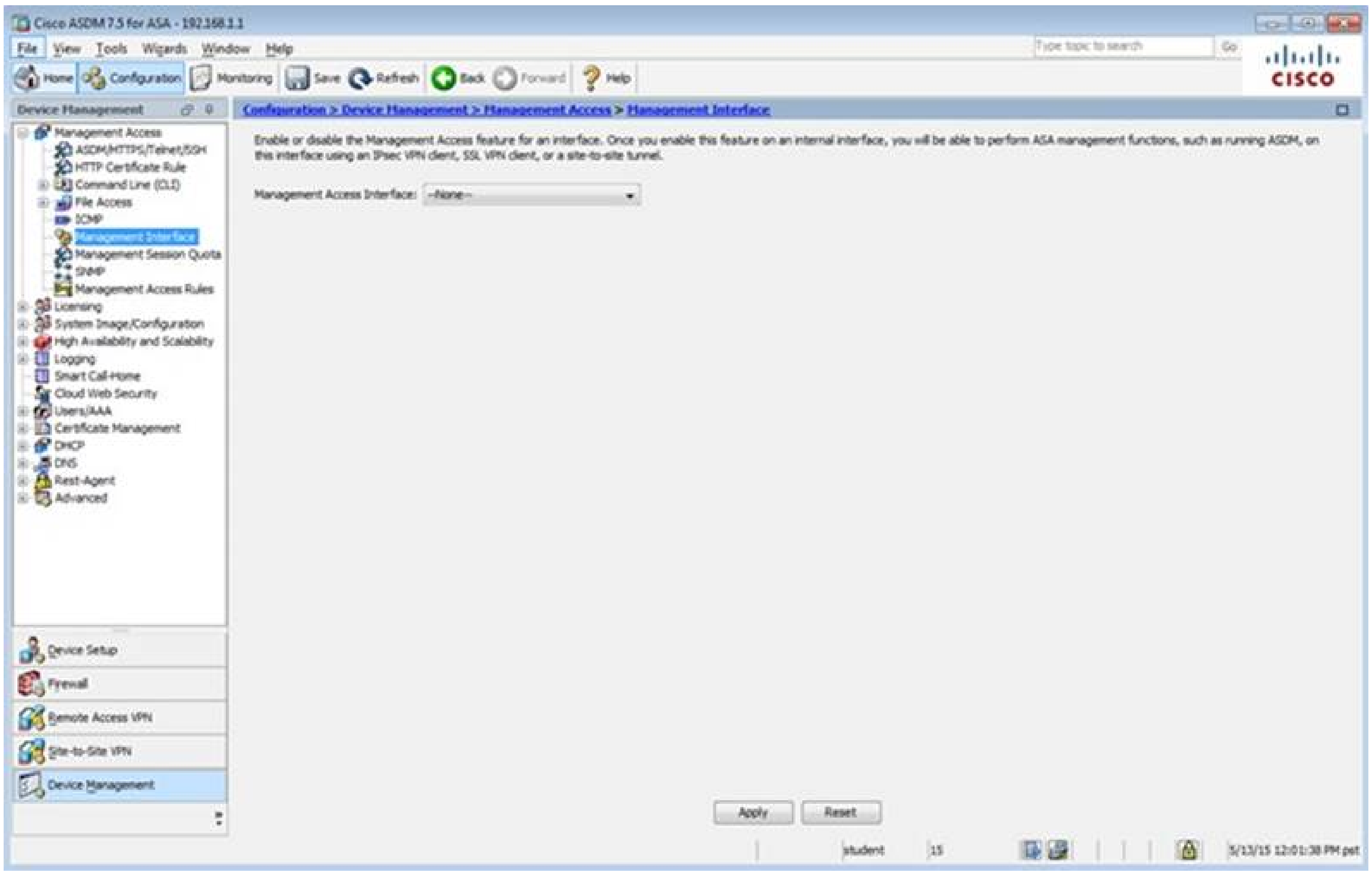
Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

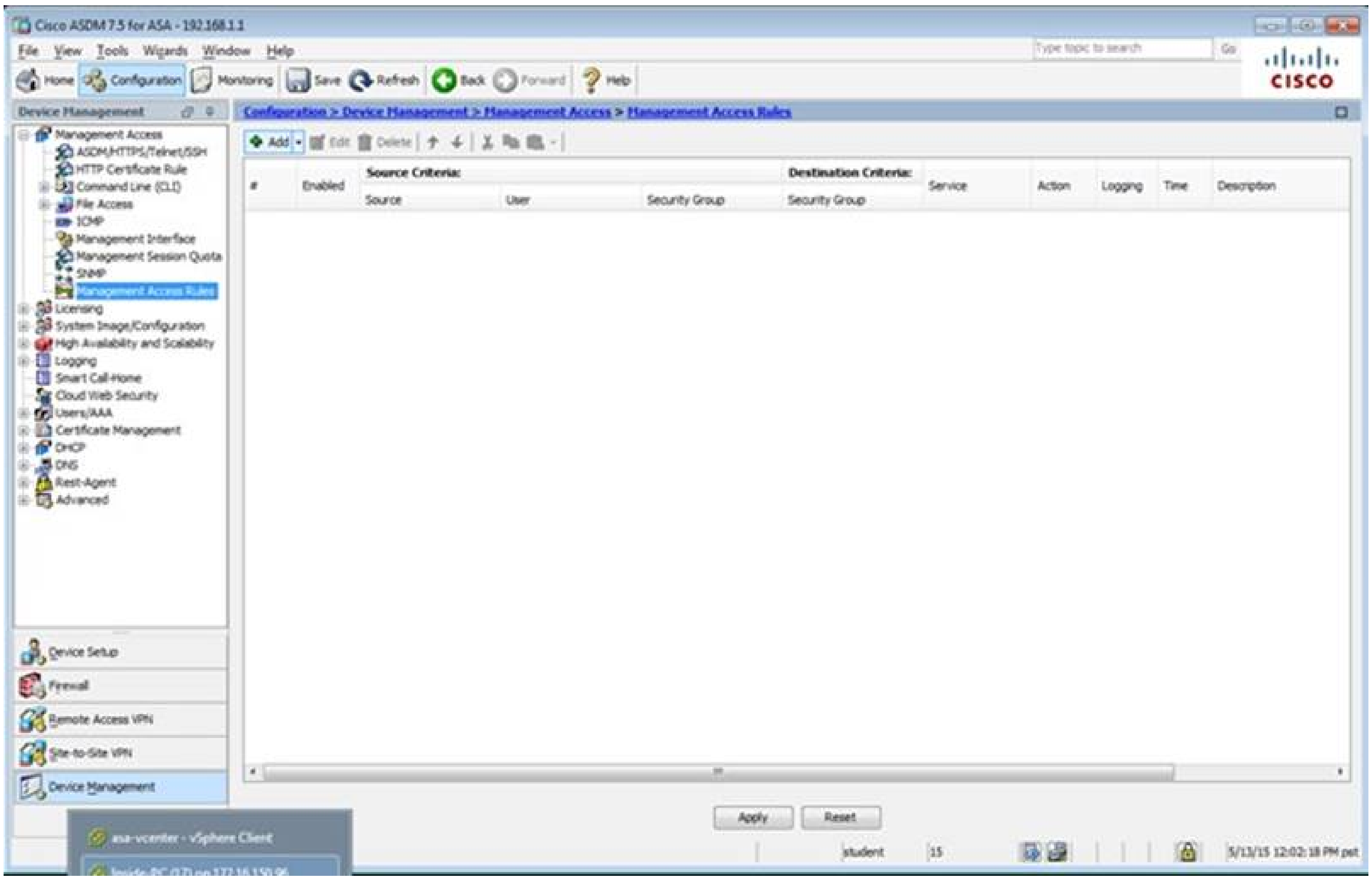
DH Key Exchange: ● Group 1 ○ Group 14



Configuration > Device Management > Management Access > Management Interface

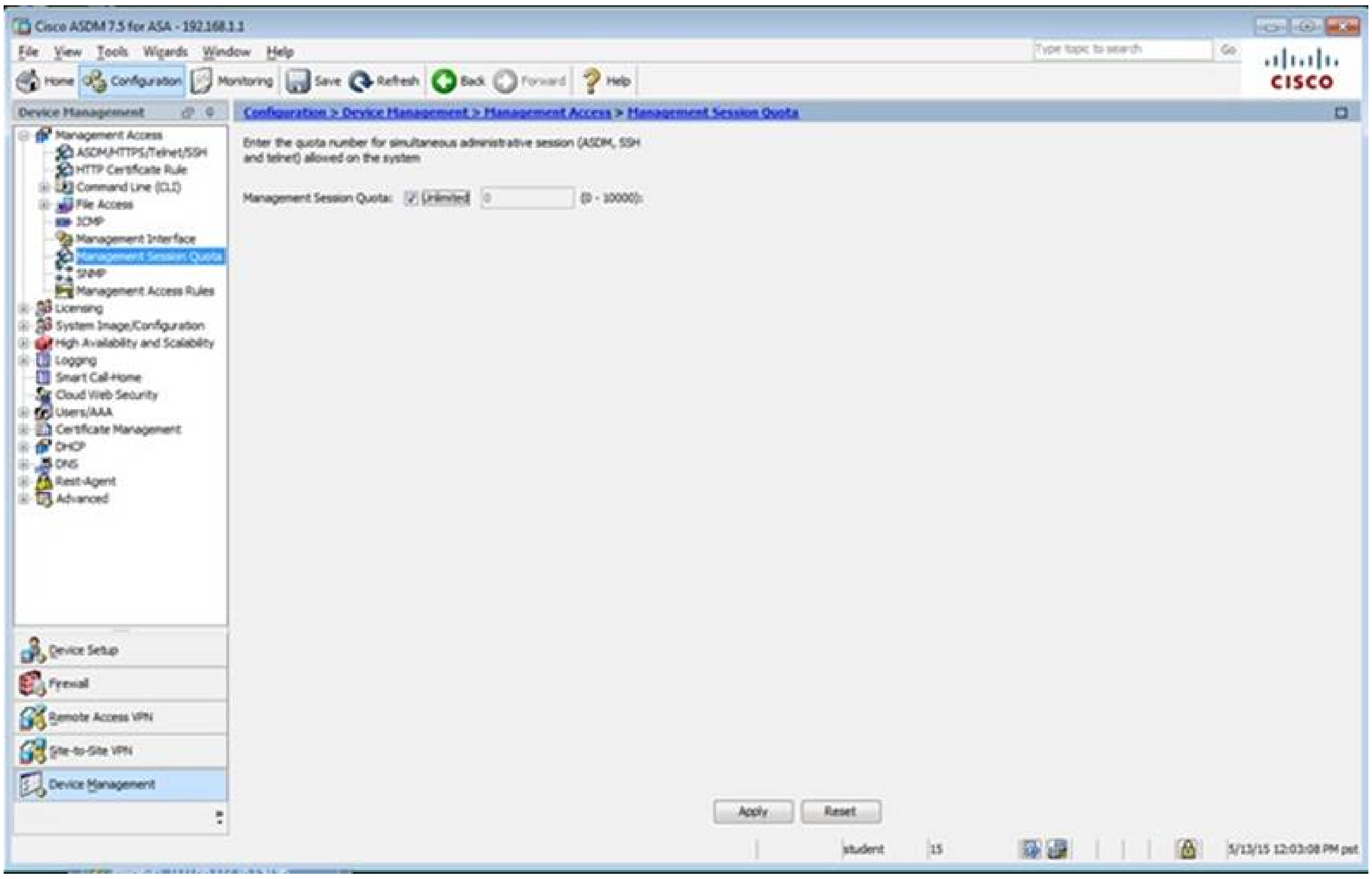
Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.

Management Access Interface: --None--



Configuration > Device Management > Management Access > Management Access Rules

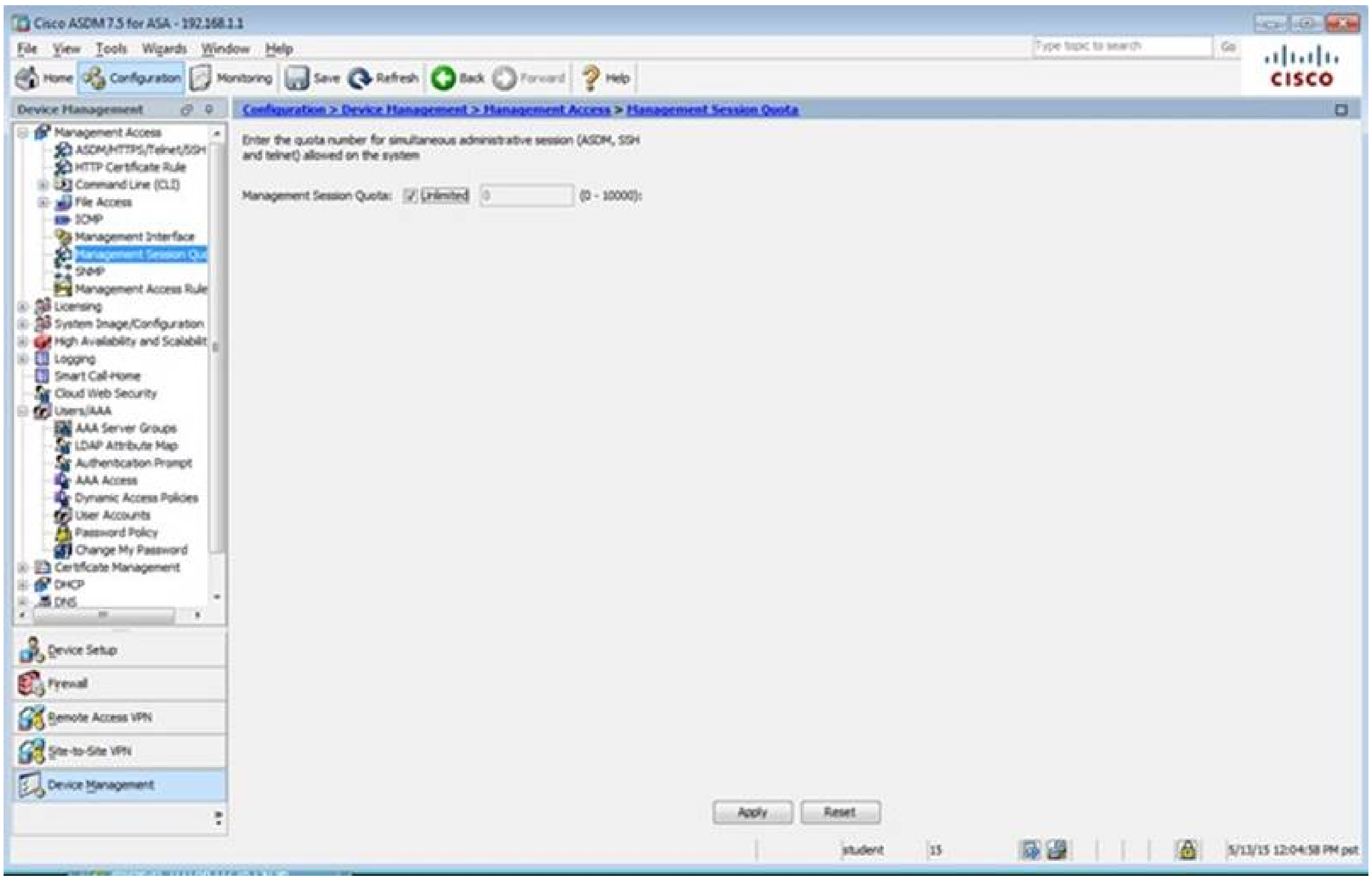
#	Enabled	Source Criteria:			Destination Criteria:	Service	Action	Logging	Time	Description
		Source	User	Security Group	Security Group					



Configuration > Device Management > Management Access > Management Session Quota

Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

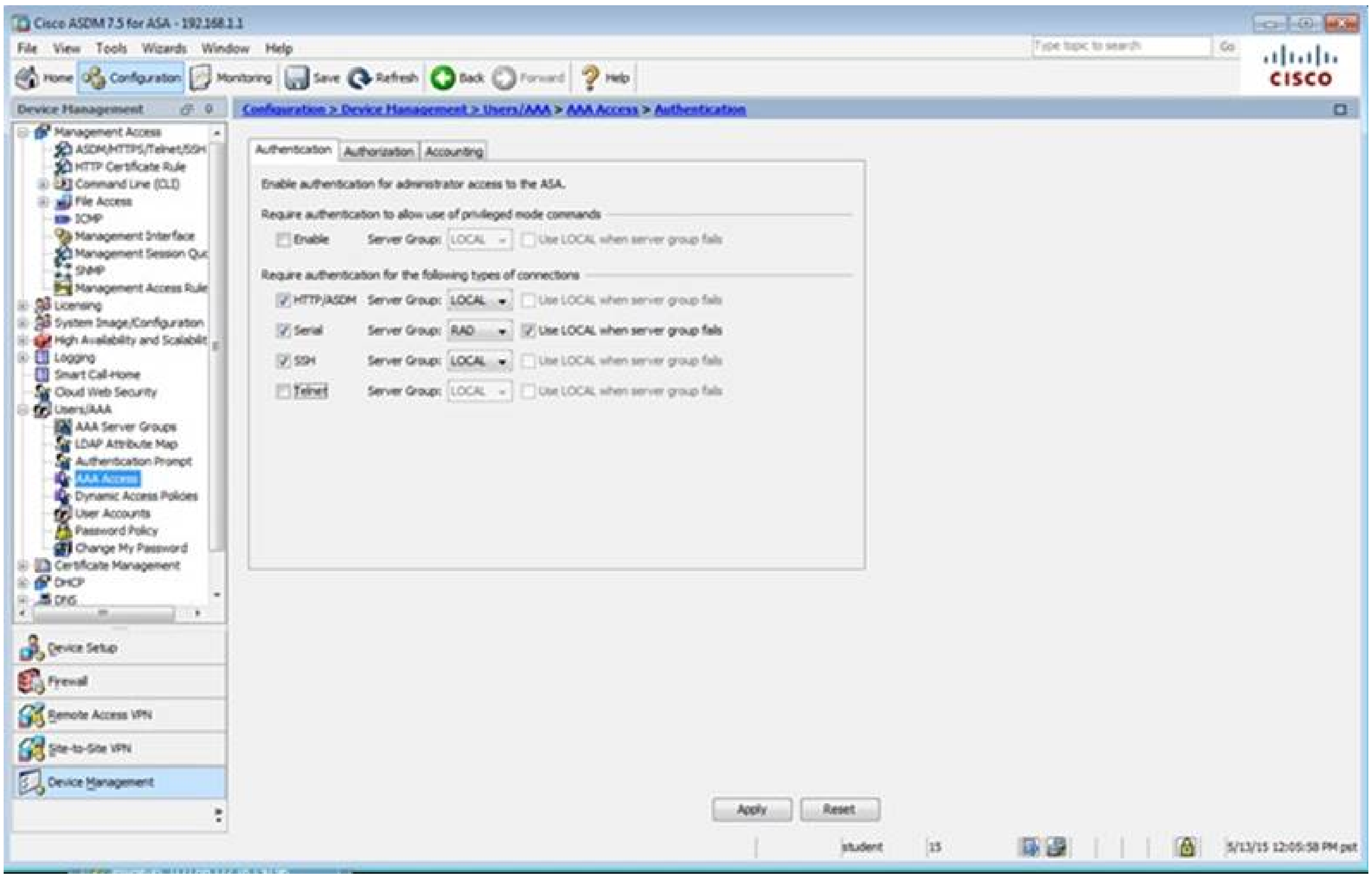
Management Session Quota: ☑ Unlimited 0 (0 - 10000):



Configuration > Device Management > Management Access > Management Session Quota

Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

Management Session Quota: ☑ Unlimited 0 (0 - 10000):



Configuration > Device Management > Users/AAA > AAA Access > Authentication

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

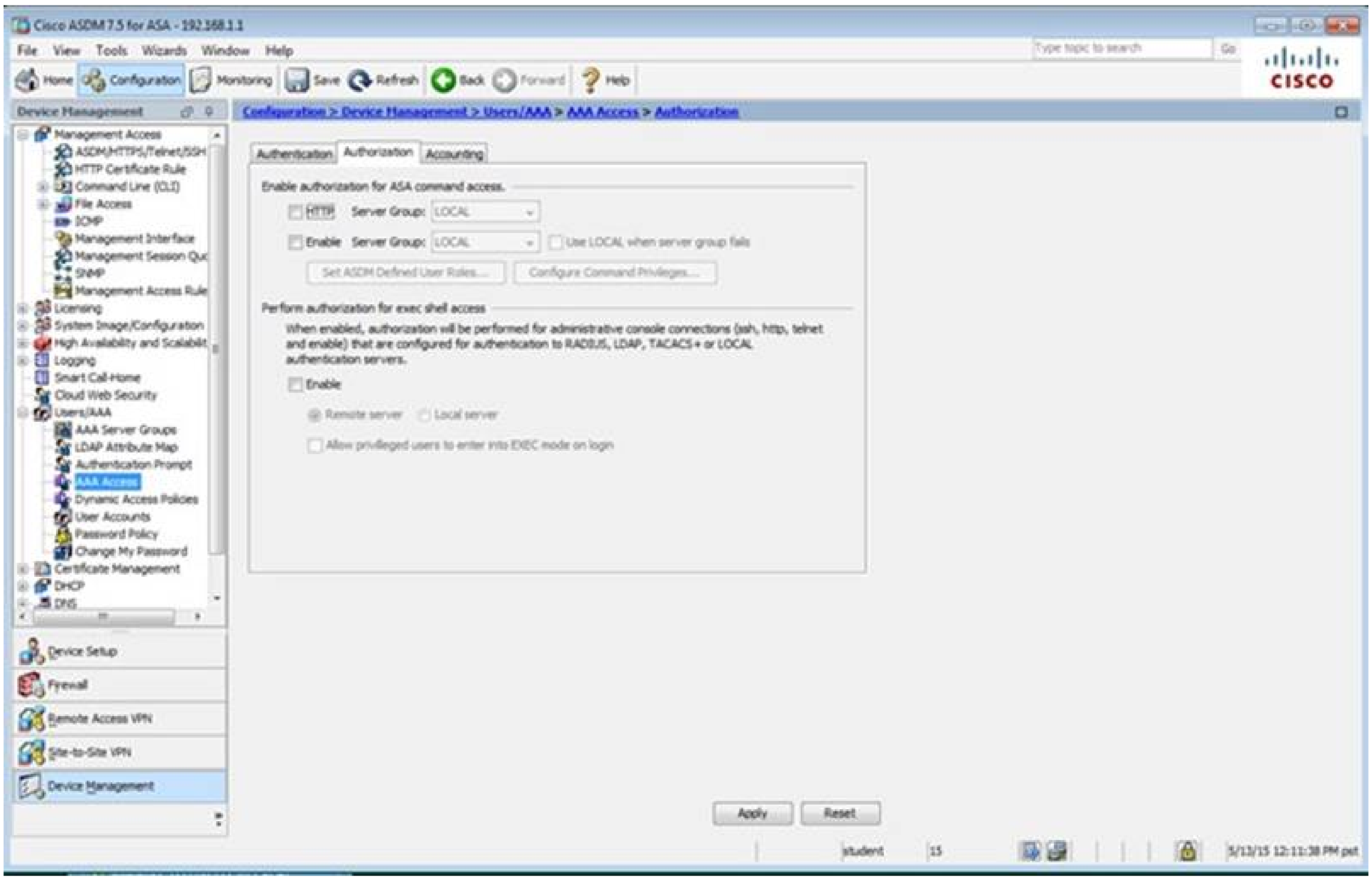
Require authentication for the following types of connections

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

☑ Serial Server Group: RAD ☑ Use LOCAL when server group fails

☑ SSH Server Group: LOCAL □ Use LOCAL when server group fails

□ Telnet Server Group: LOCAL □ Use LOCAL when server group fails



Configuration > Device Management > Users/AAA > AAA Access > Authorization

Authentication | Authorization | Accounting

Enable authorization for ASA command access.

□ HTTP Server Group: LOCAL

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Set ASDM Defined User Roles... Configure Command Privileges...

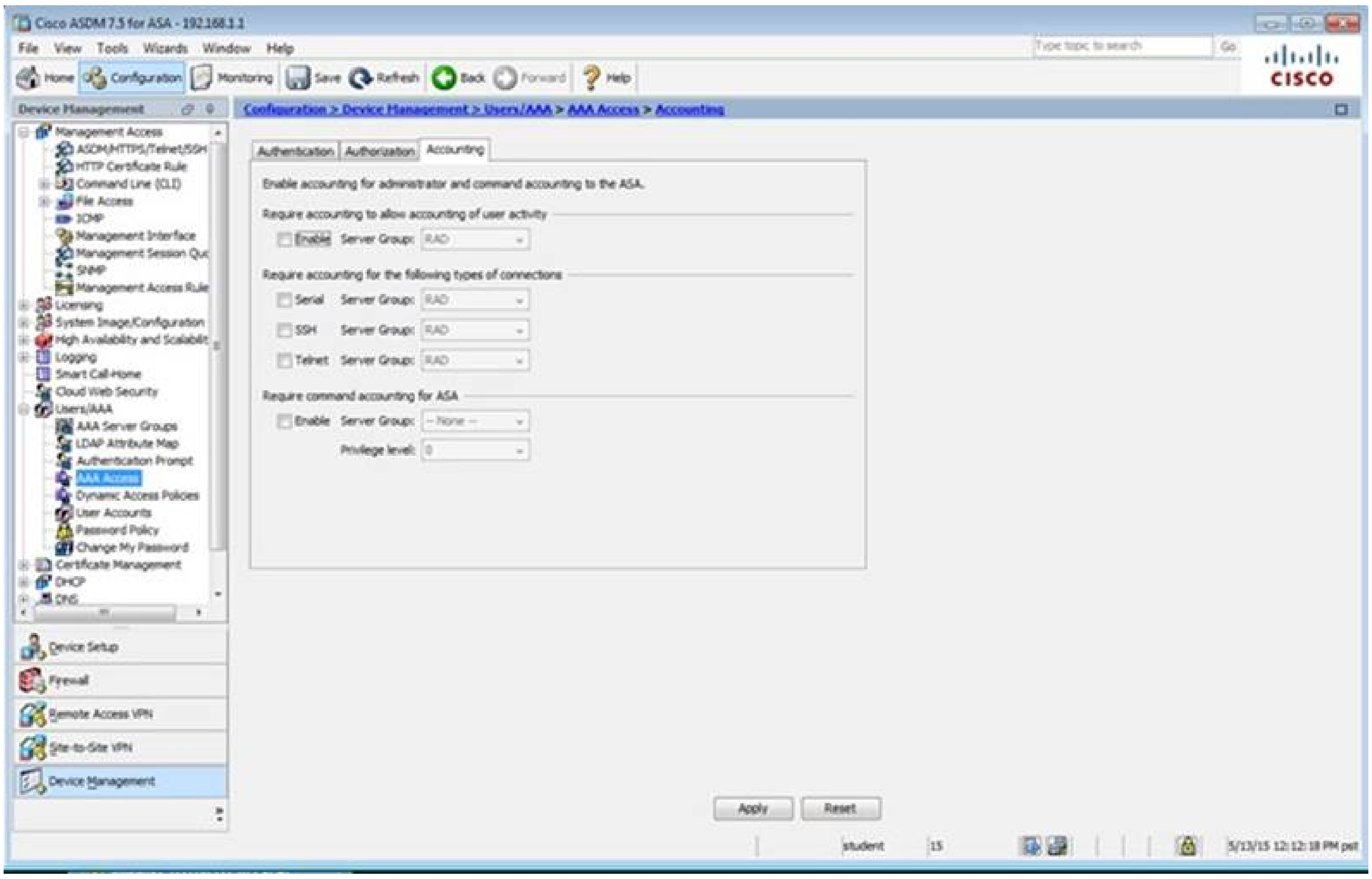
Perform authorization for exec shell access

When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.

□ Enable

● Remote server ○ Local server

□ Allow privileged users to enter into EXEC mode on login



Configuration > Device Management > Users/AAA > AAA Access > Accounting

Authentication | Authorization | Accounting

Enable accounting for administrator and command accounting to the ASA.

Require accounting to allow accounting of user activity

□ Enable Server Group: RAD

Require accounting for the following types of connections

□ Serial Server Group: RAD

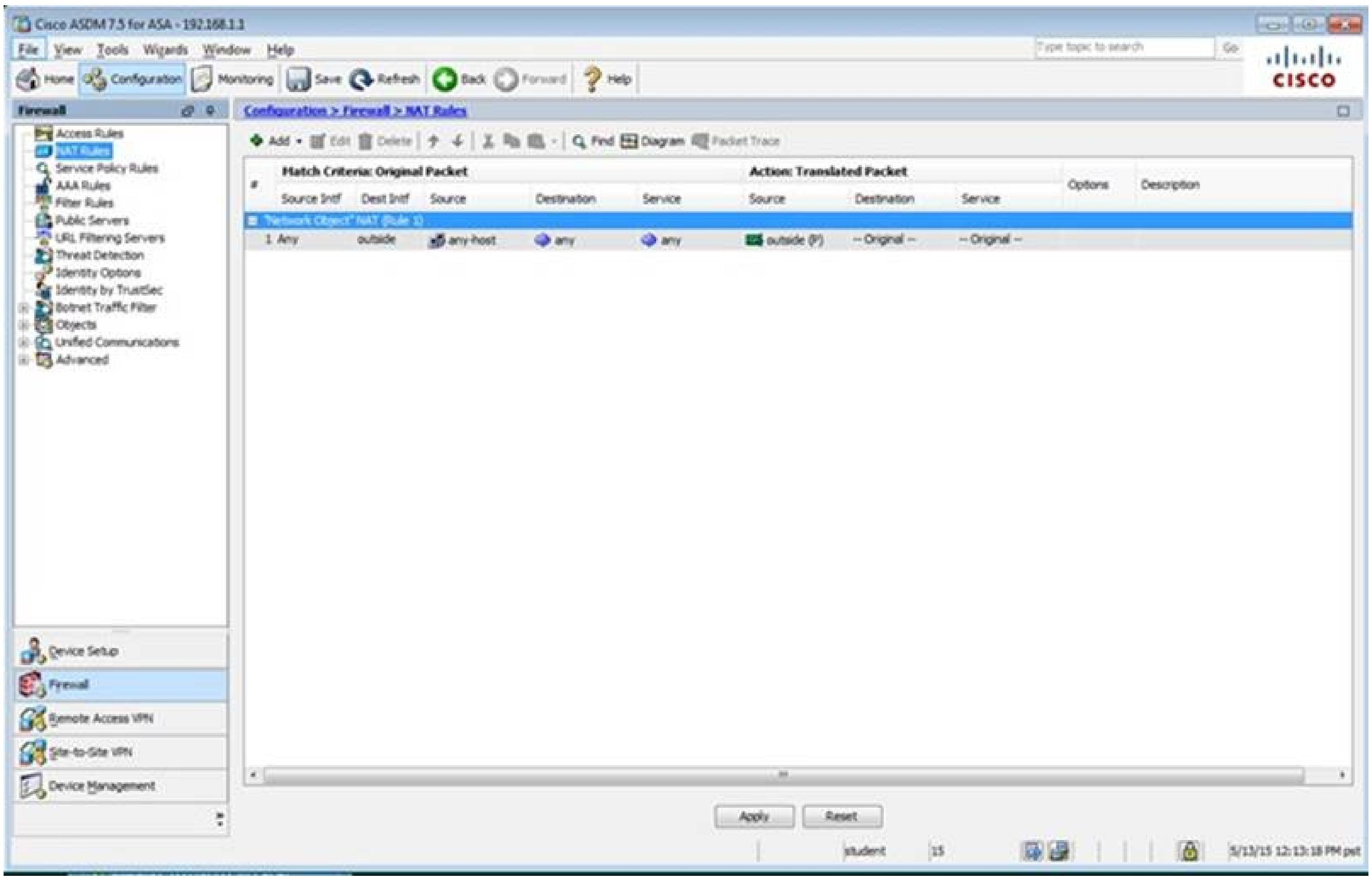
□ SSH Server Group: RAD

□ Telnet Server Group: RAD

Require command accounting for ASA

□ Enable Server Group: -- None --

Privilege level: 0

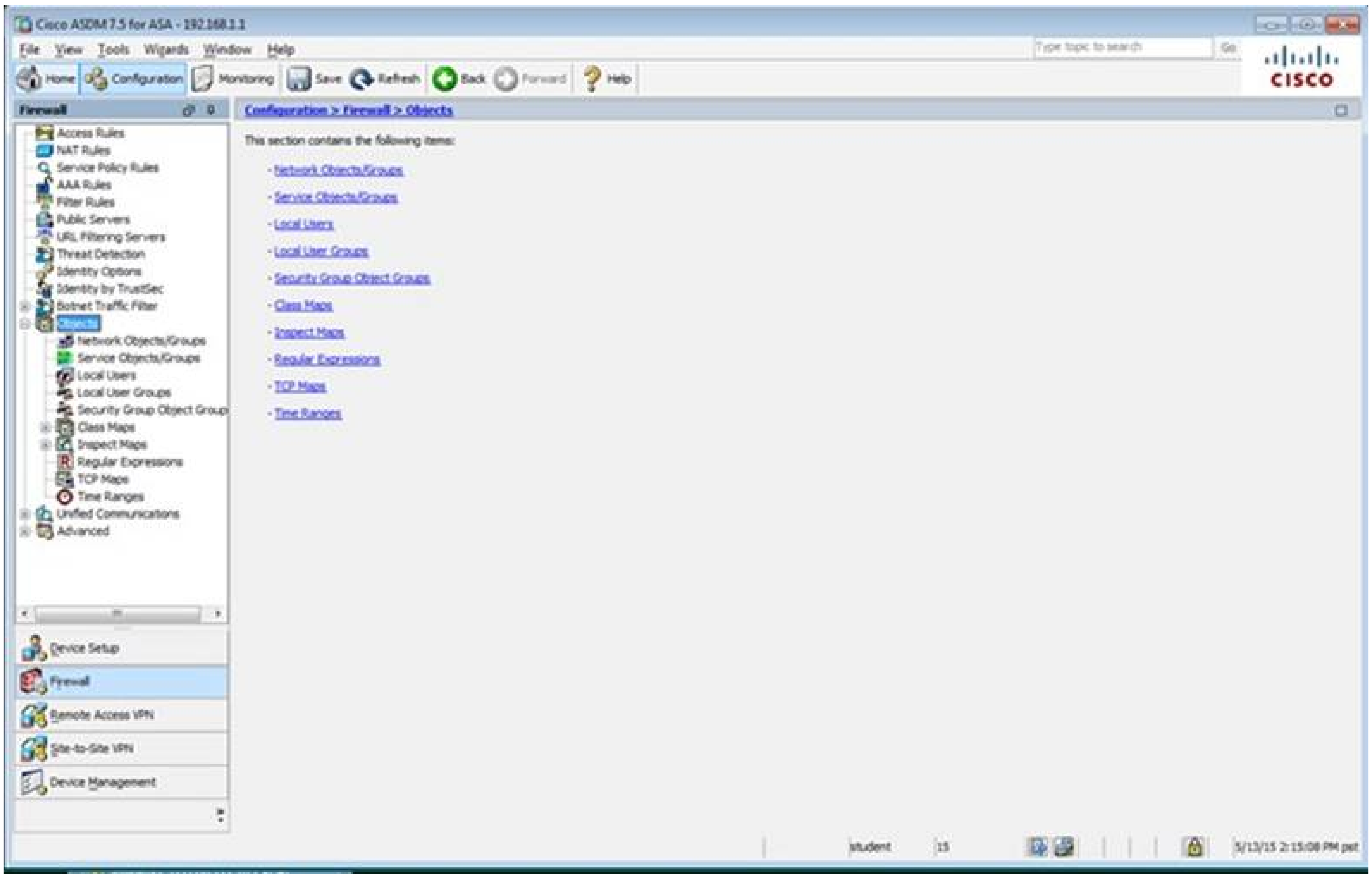


Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > NAT Rules

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

student 15 5/13/15 12:13:18 PM pdt



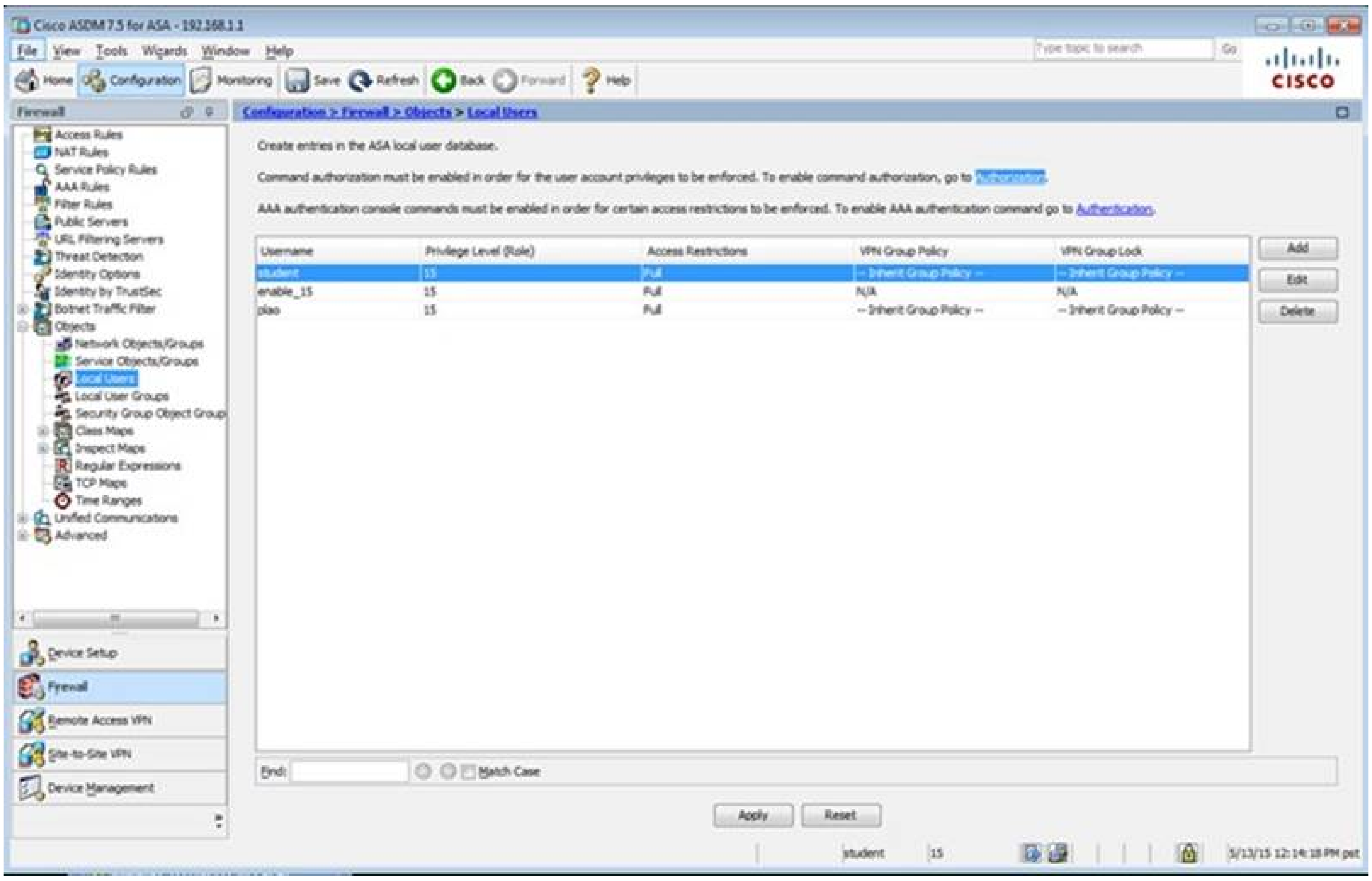
Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > Objects

This section contains 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

student 15 5/13/15 2:15:08 PM pdt



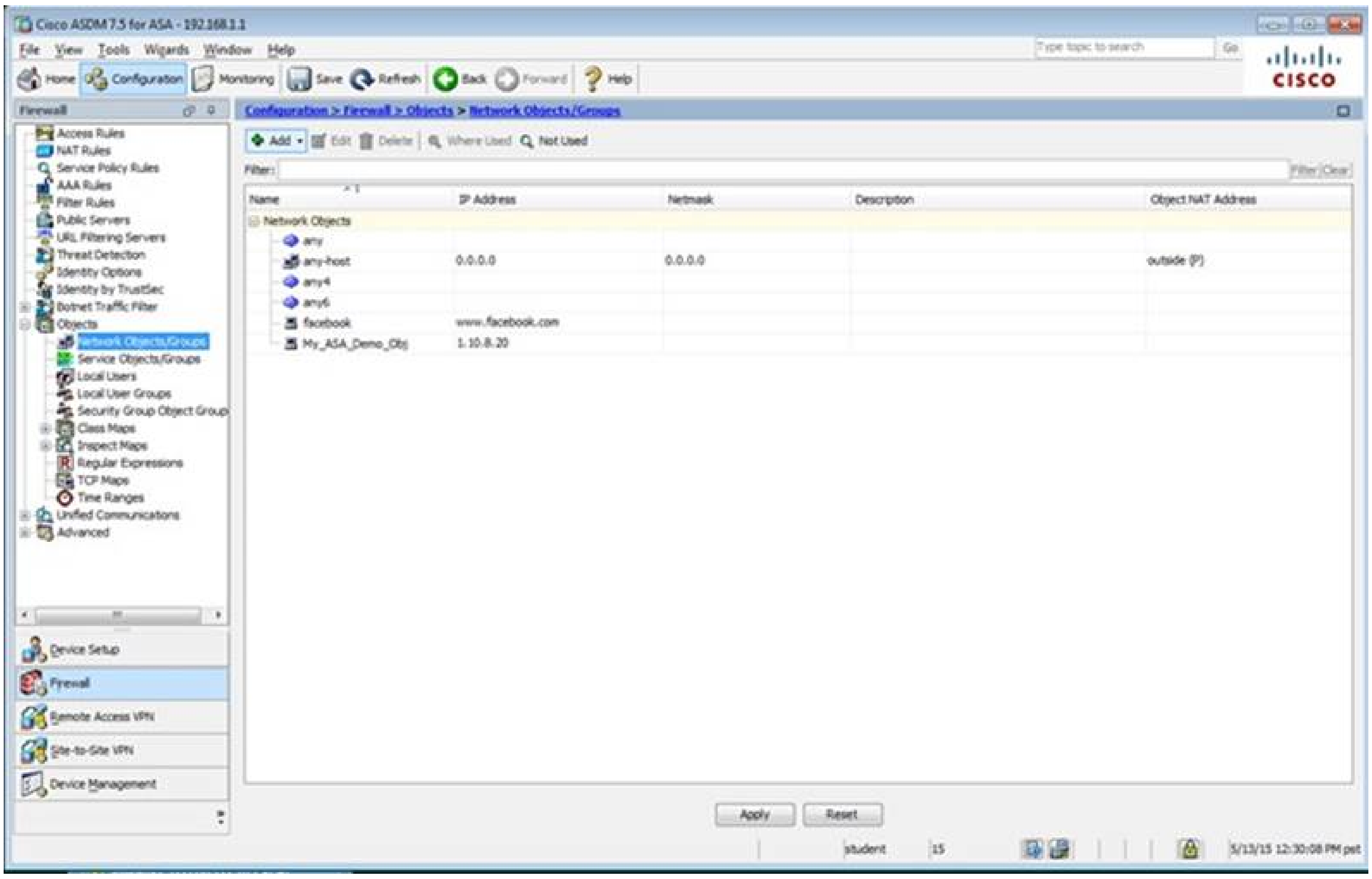
Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

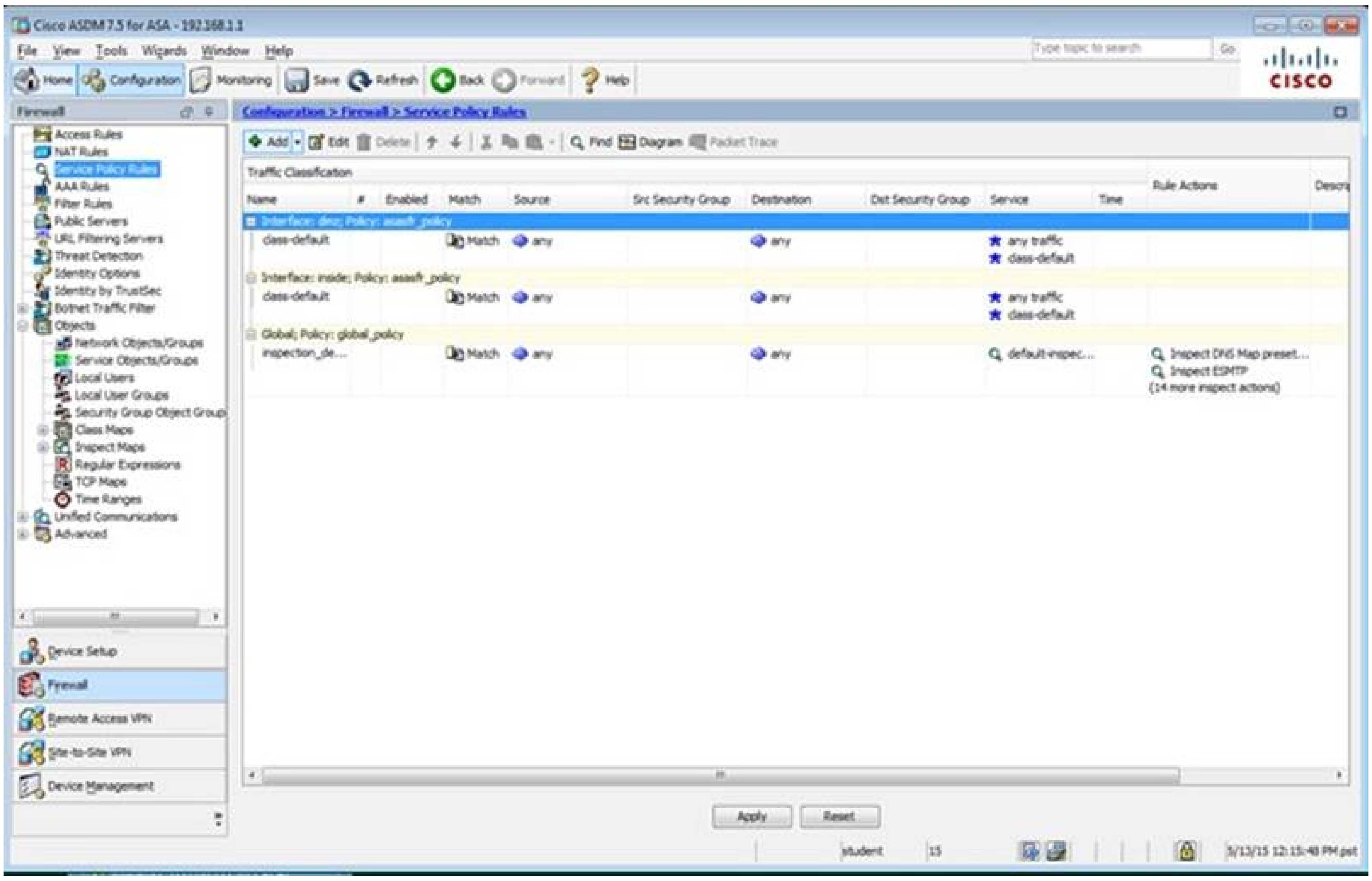
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

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



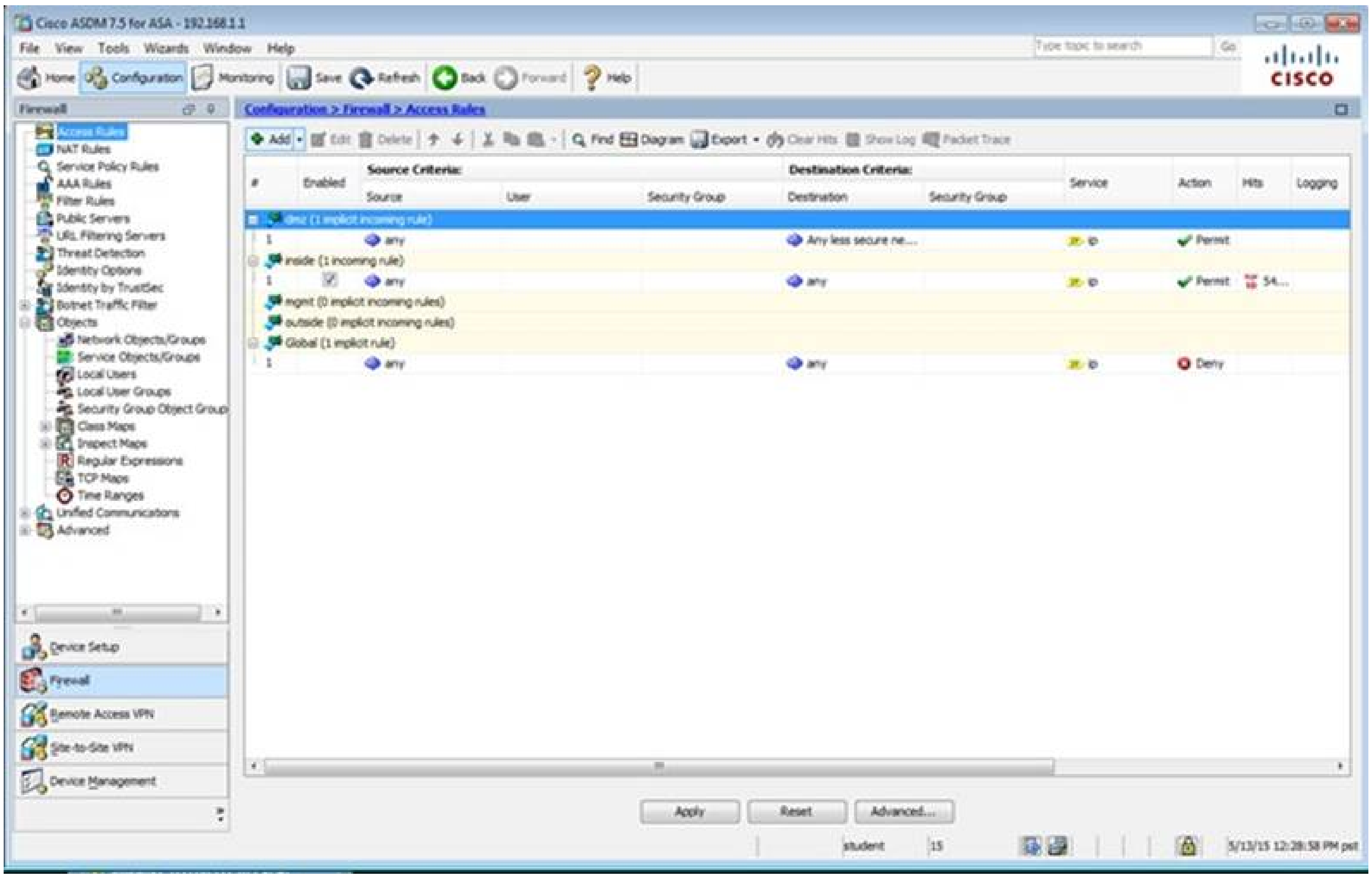
Configuration > Firewall > Objects > Network Objects/Groups

Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
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			



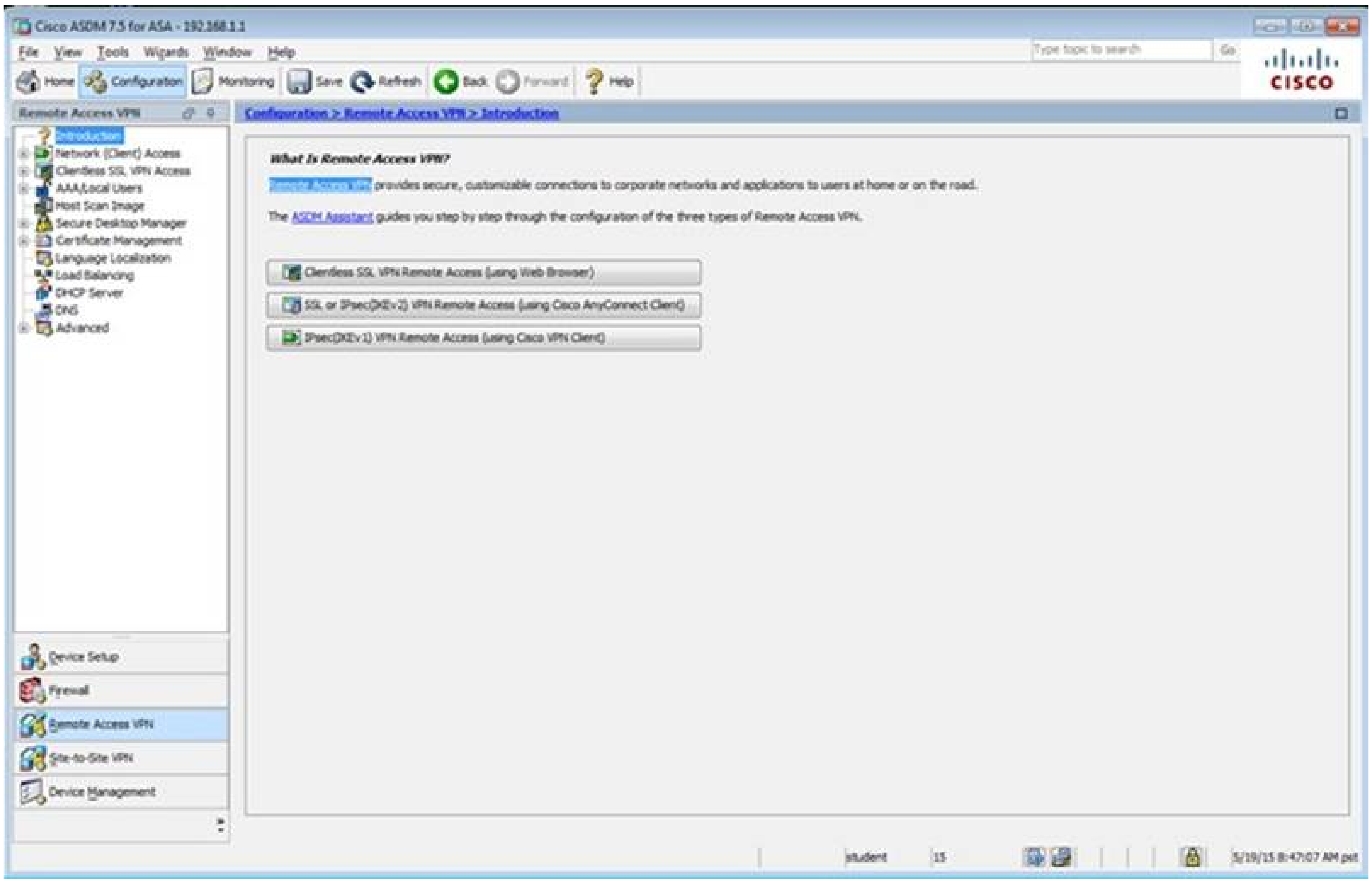
Configuration > Firewall > Service Policy Rules

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



Configuration > Firewall > Access Rules

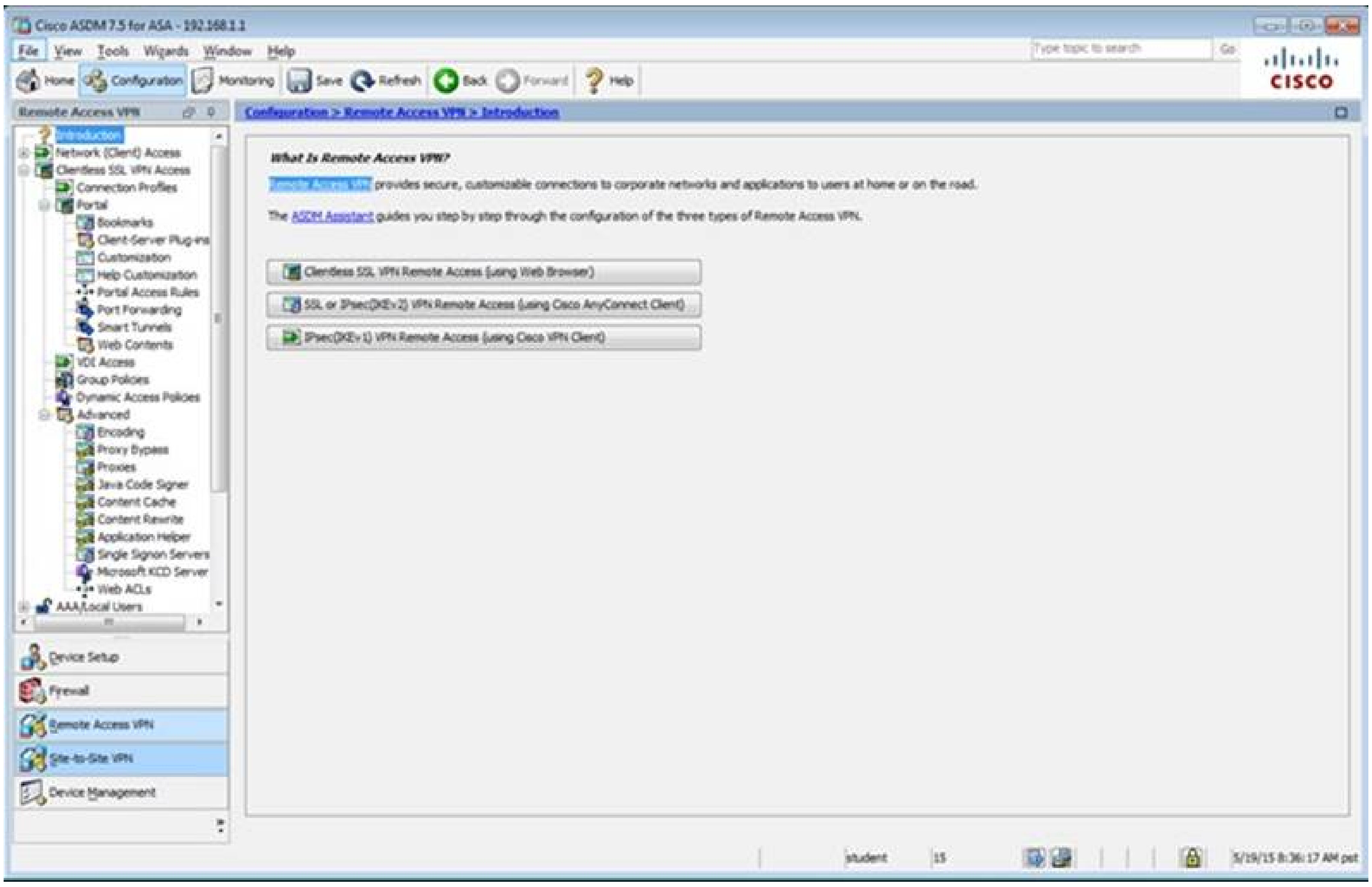
#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging
		Source	User	Security Group	Destination	Security Group				
dmz (1 implicit incoming rule)										
1		any			Any less secure ne...		ip	✓ Permit		
inside (1 incoming rule)										
1	☑	any			any		ip	✓ Permit	54...	
mgmt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



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.

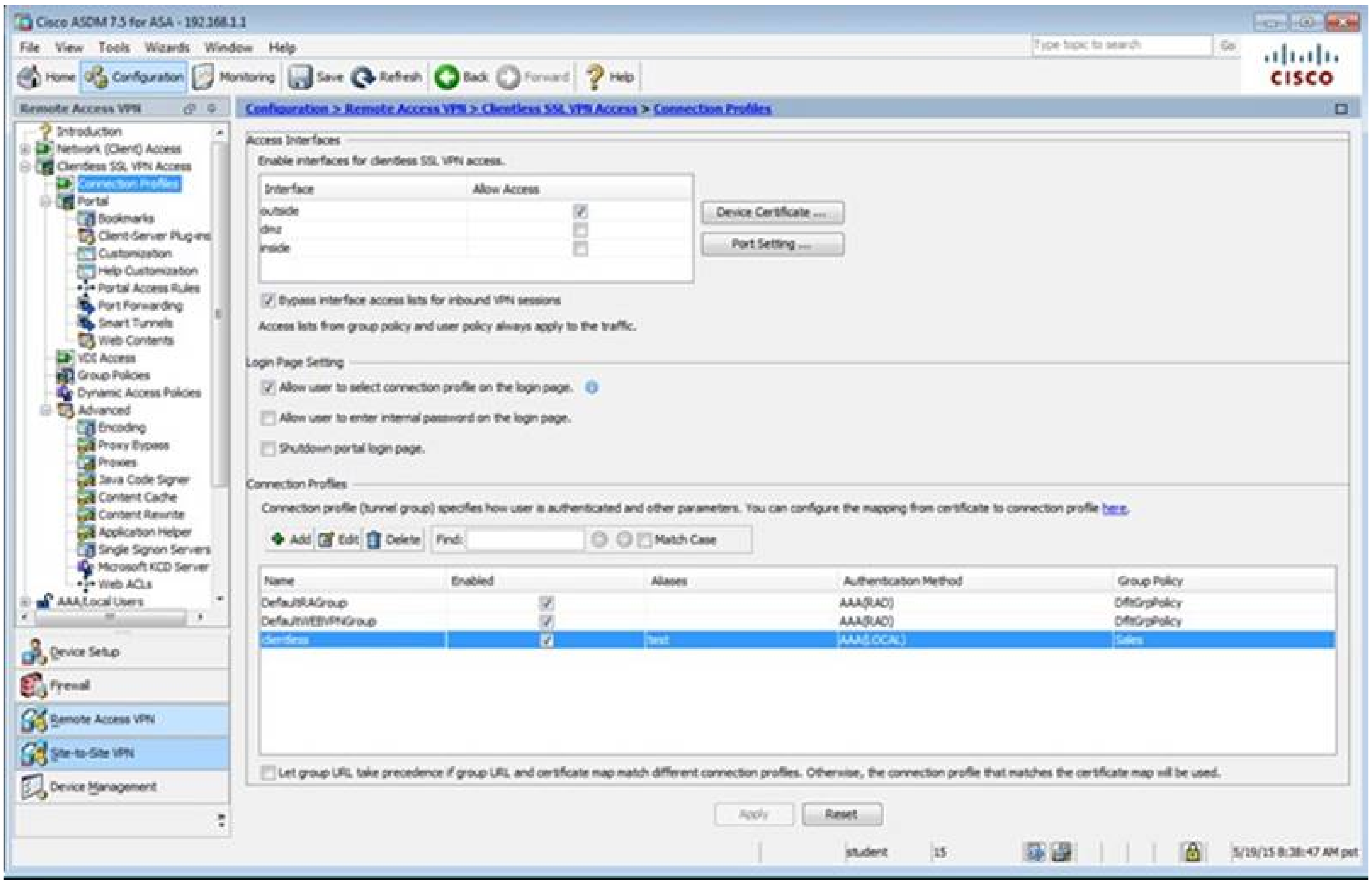
The ASDM Assistant guides you step by step through the configuration of the three types of Remote Access VPN.



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.



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ 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.

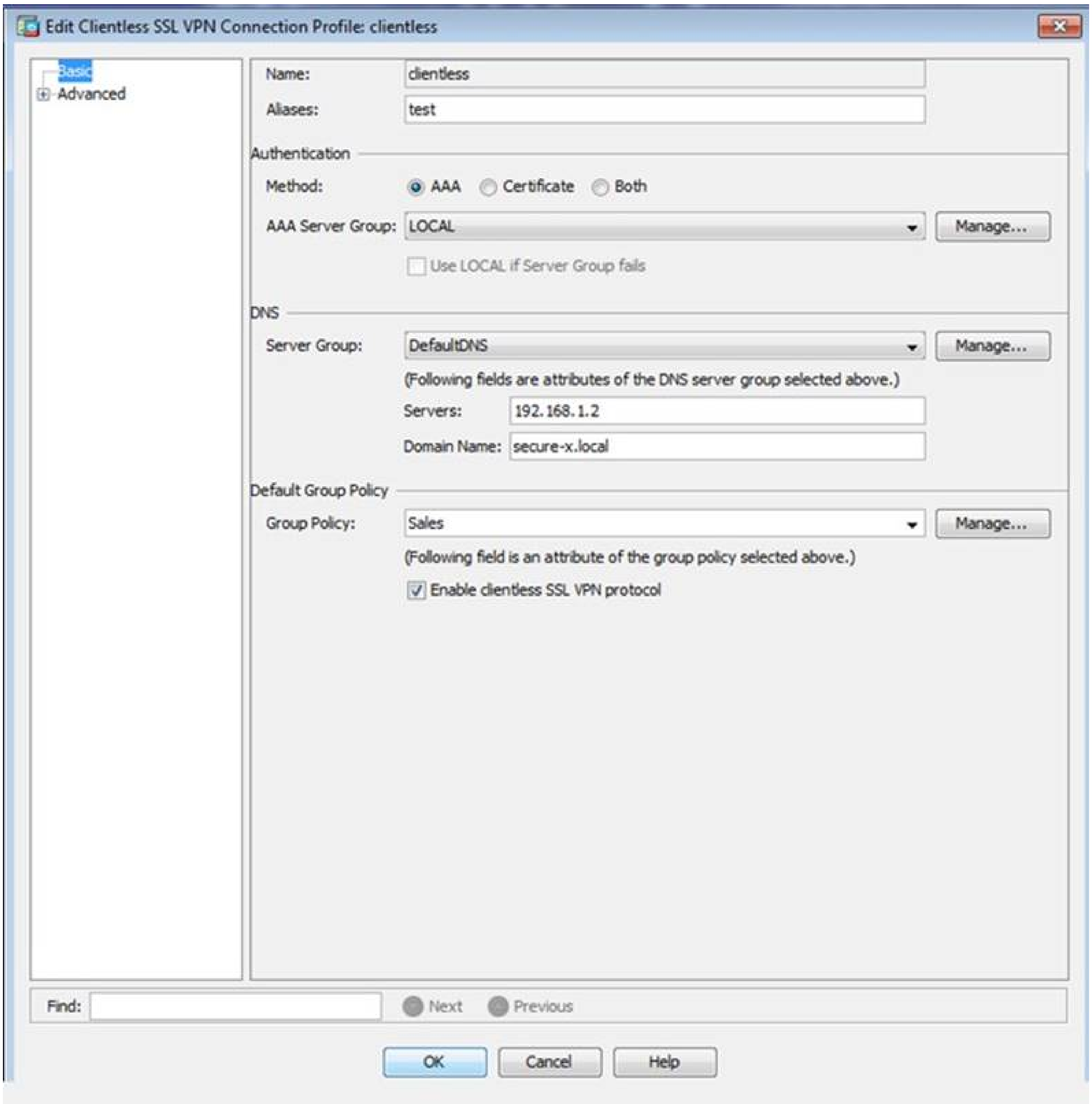
Connection Profiles

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

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(RAD)	DfltGrpPolicy
clientless	☑	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.

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



Edit Clientless SSL VPN Connection Profile: clientless

Name: clientless

Aliases: test

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

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

Servers: 192.168.1.2

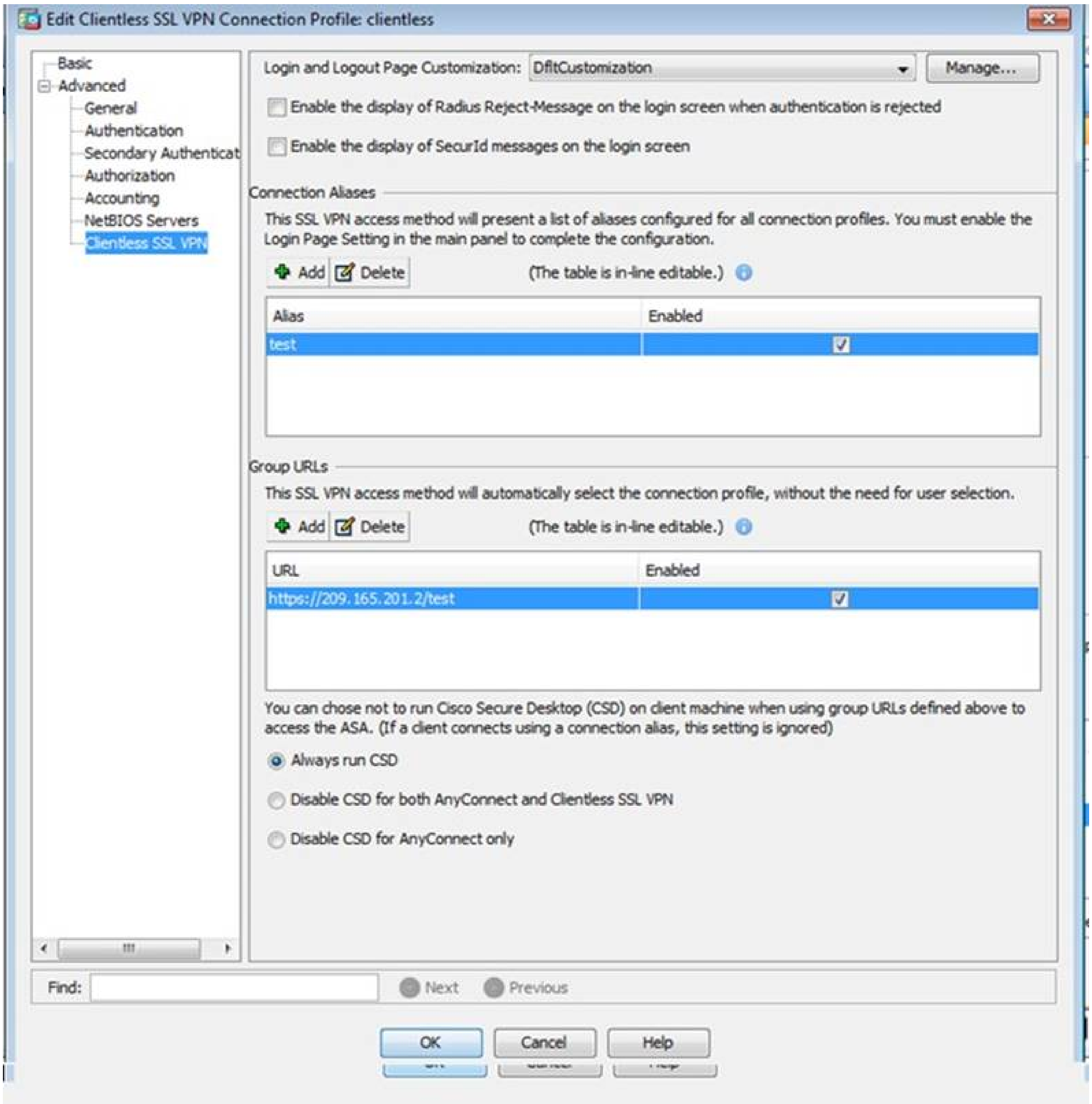
Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales

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

☑ Enable clientless SSL VPN protocol



Edit Clientless SSL VPN Connection Profile: clientless

Login and Logout Page Customization: DfltCustomization

□ 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.

(The table is in-line editable.)

Alias	Enabled
test	☑

Group URLs

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

(The table is in-line editable.)

URL	Enabled
https://209.165.201.2/test	☑

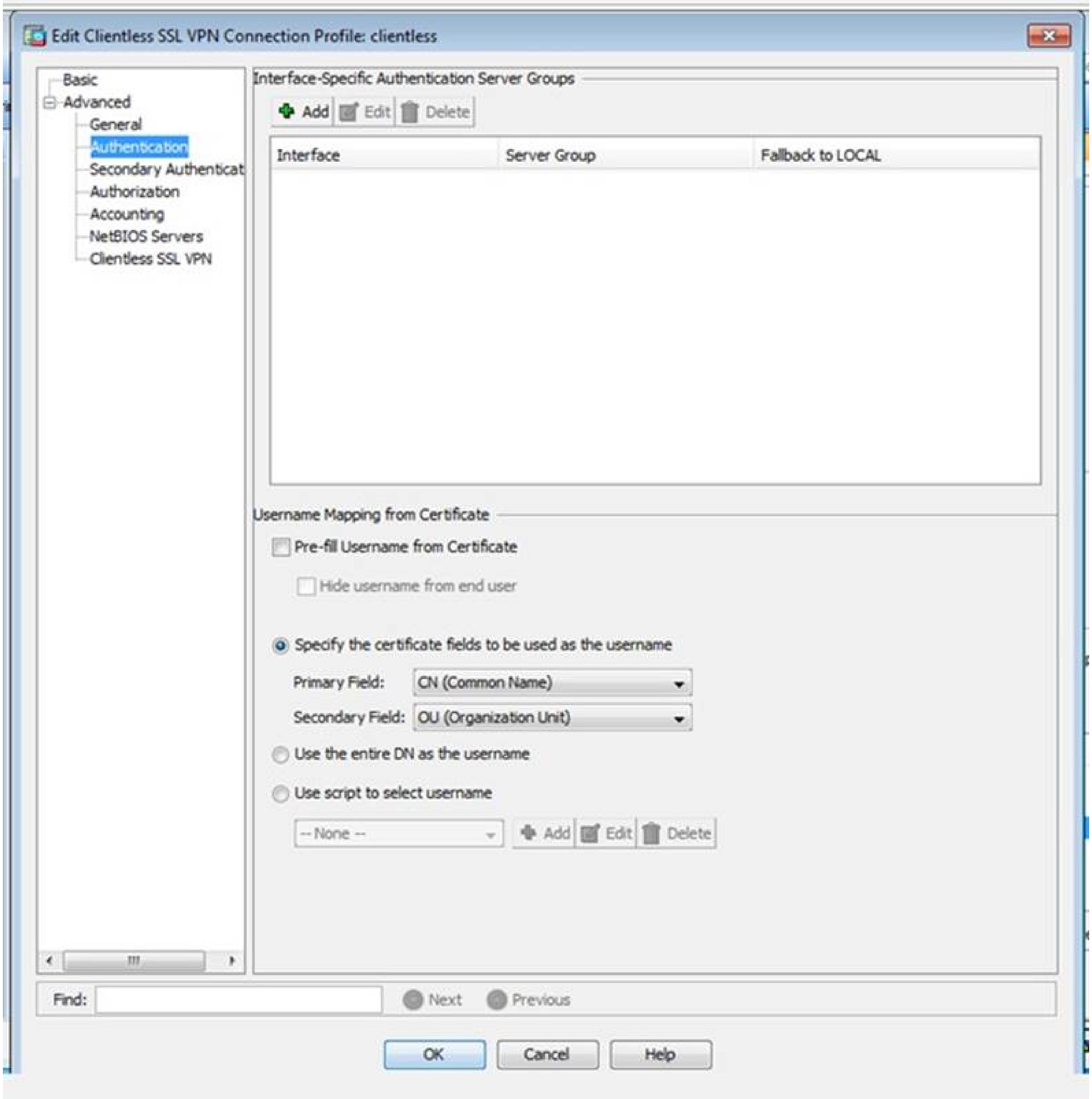
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

● Always run CSD

○ Disable CSD for both AnyConnect and Clientless SSL VPN

○ Disable CSD for AnyConnect only

Find:



Edit Clientless SSL VPN Connection Profile: clientless

Interface-Specific Authentication Server Groups

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

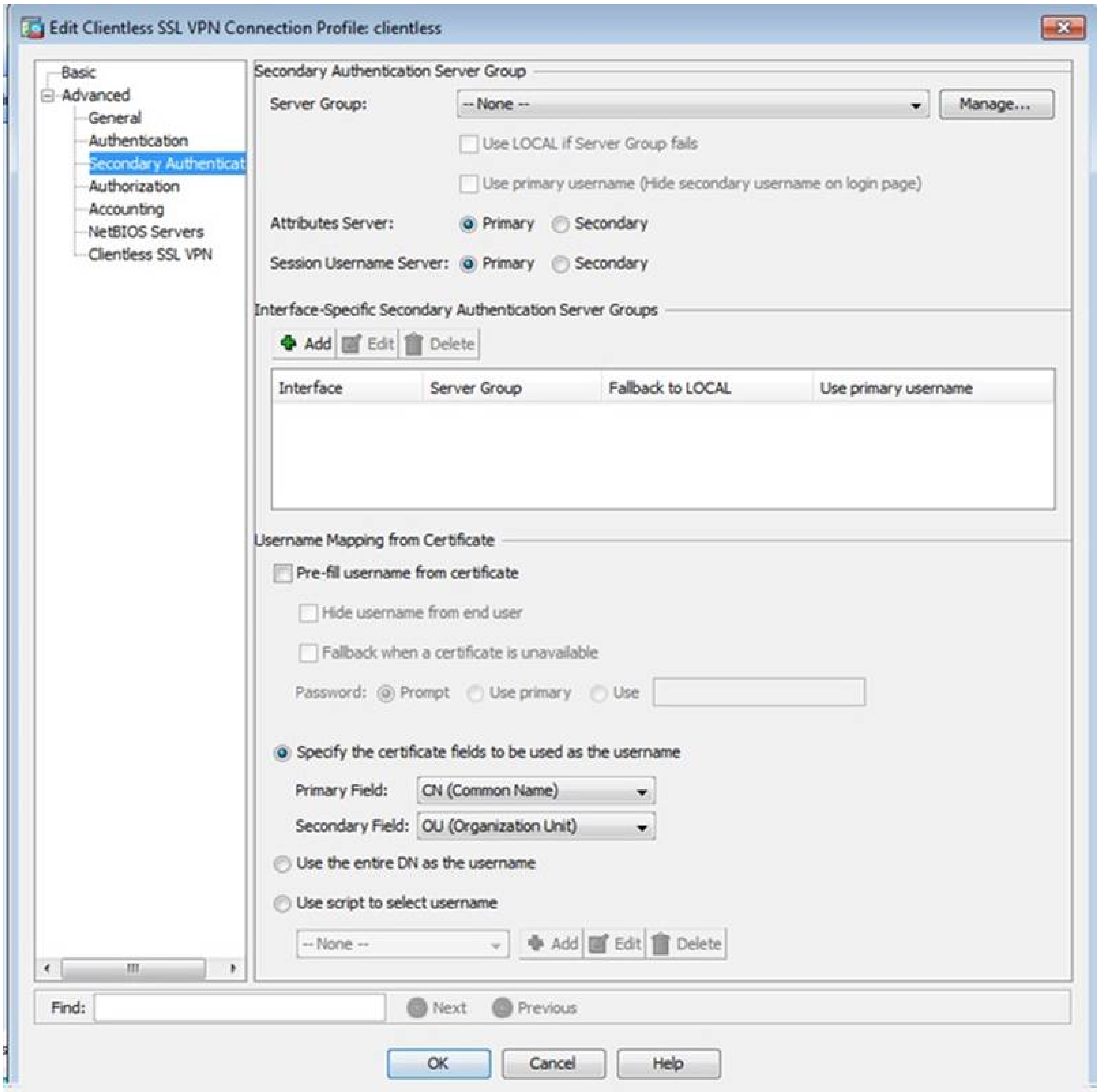
Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --



Edit Clientless SSL VPN Connection Profile: clientless

Secondary Authentication Server Group

Server Group: -- None --

□ 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

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)

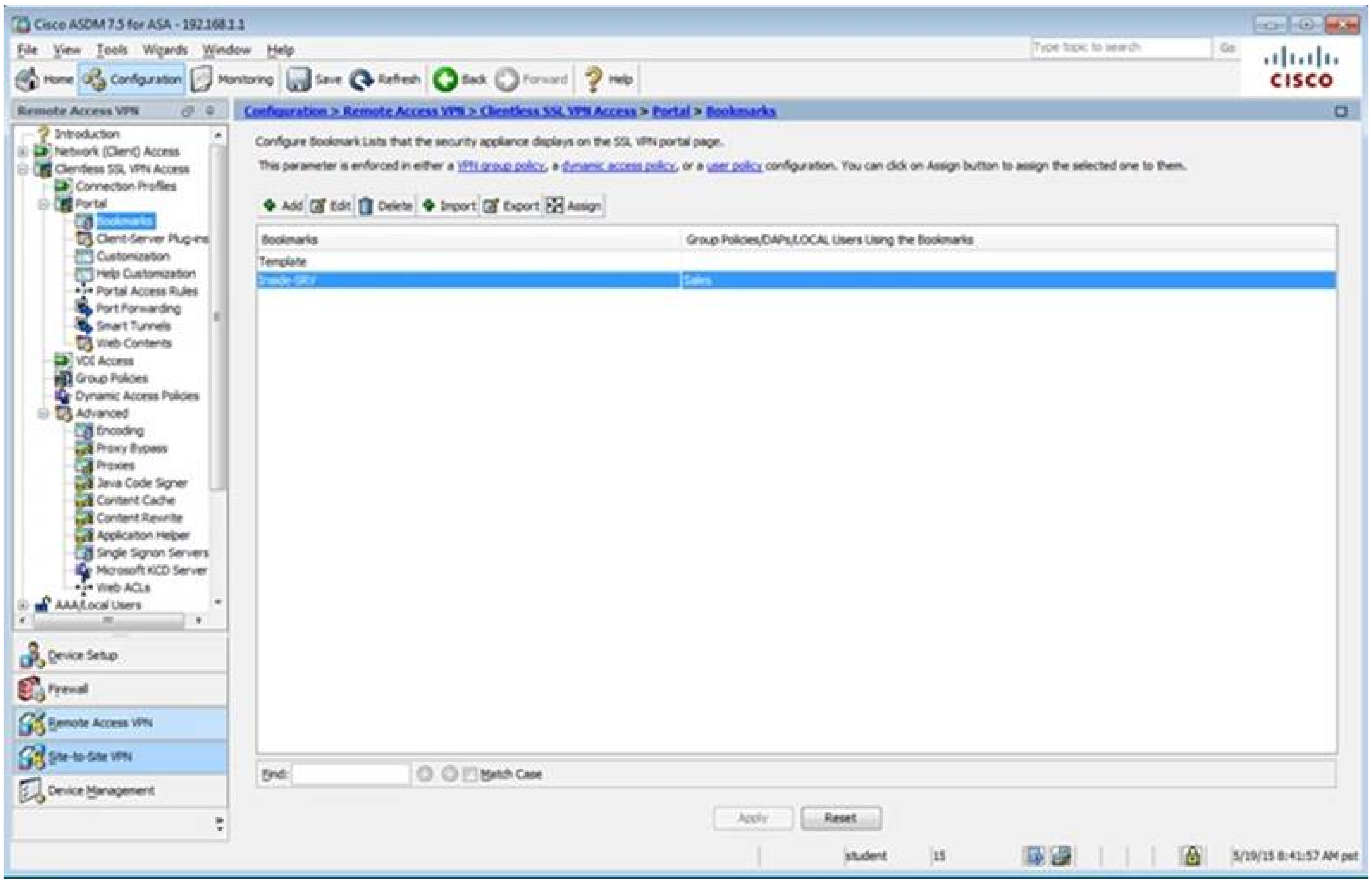
Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --

Find:



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

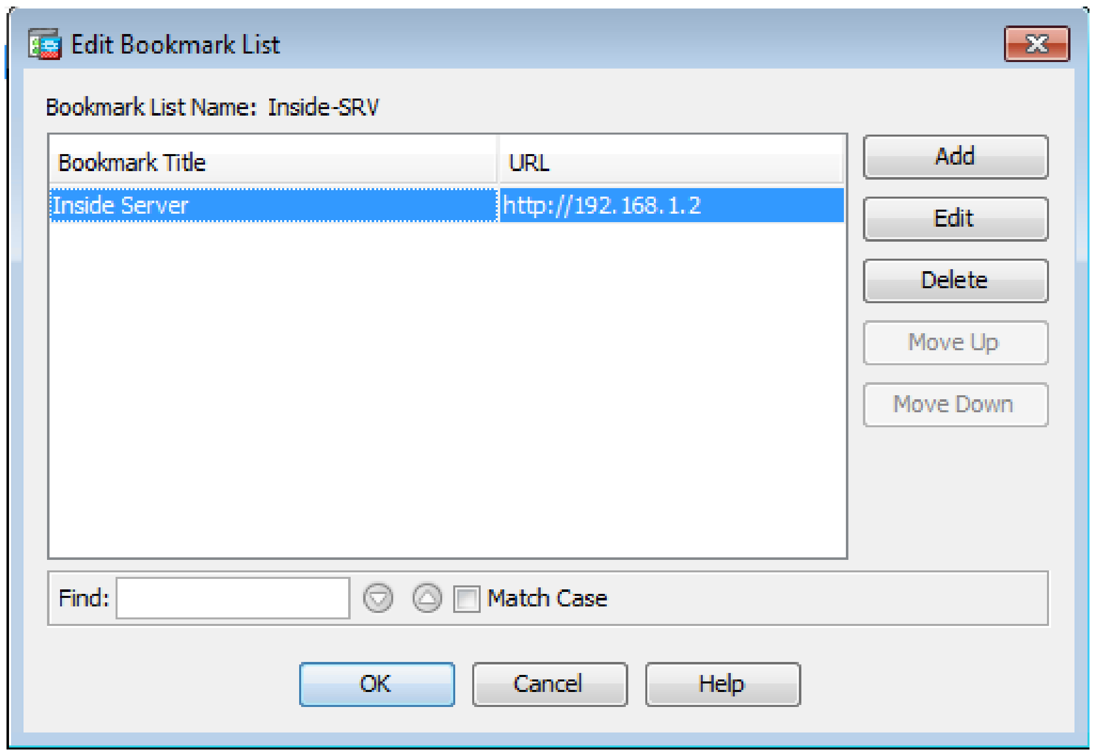
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

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.

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

Find: □ Match Case

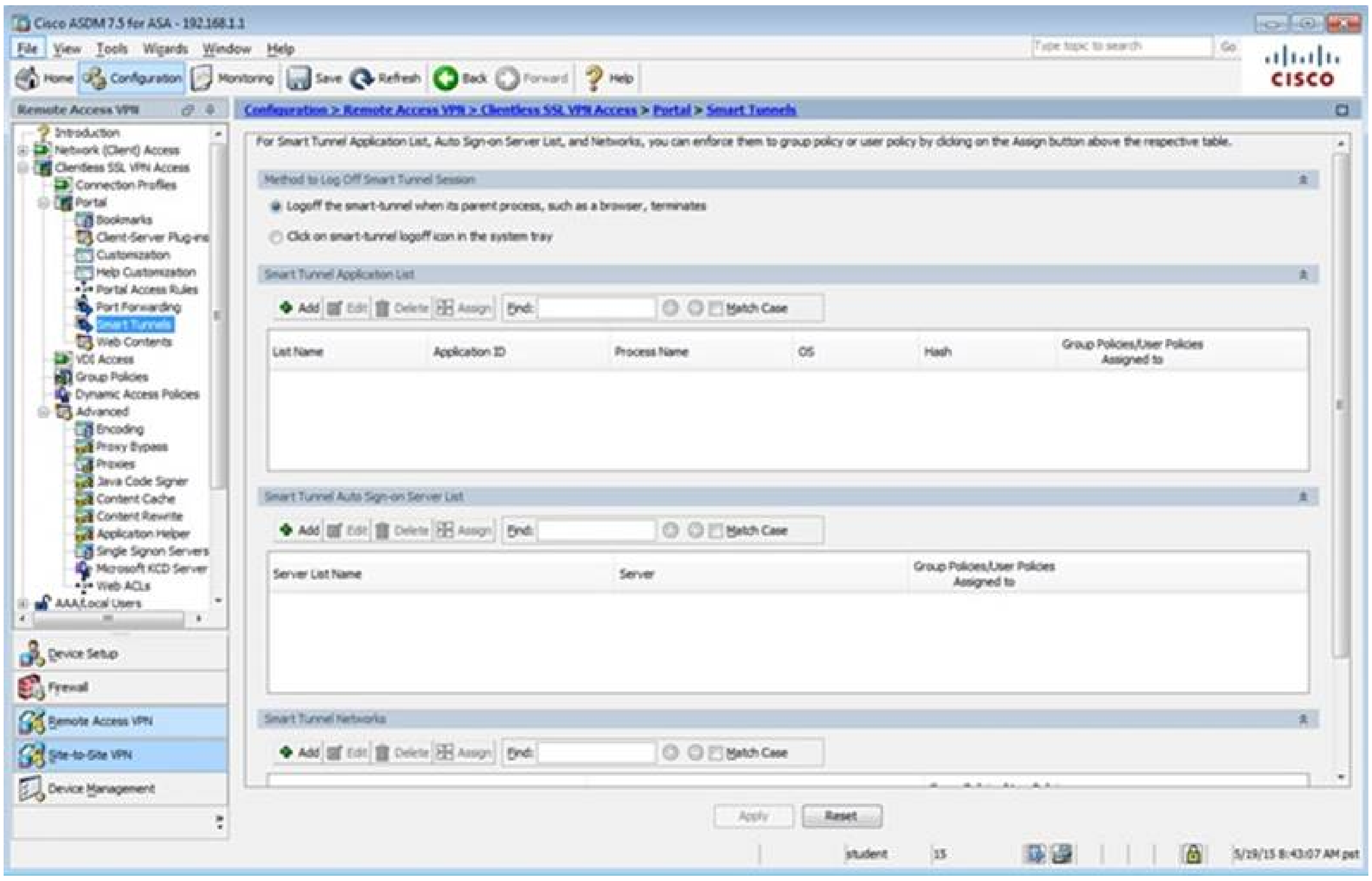
student 15 5/19/15 8:41:57 AM pst



Edit Bookmark List

Bookmark List Name: Inside-SRV

Bookmark Title	URL
Inside Server	http://192.168.1.2



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

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

Method to Log Off Smart Tunnel Session

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

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

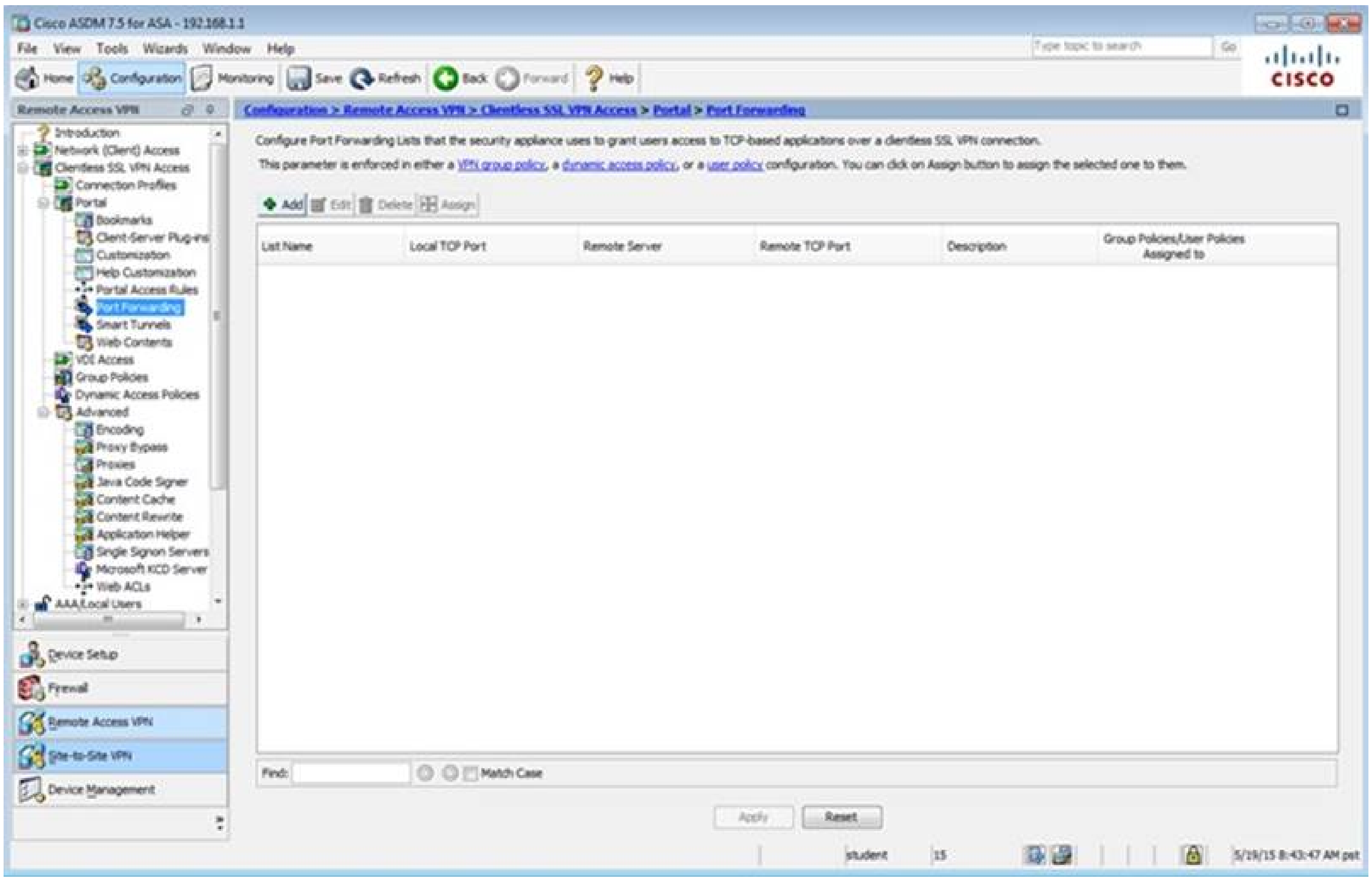
Smart Tunnel Application List

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

Smart Tunnel Auto Sign-on Server List

Server List Name	Server	Group Policies/User Policies Assigned to

Smart Tunnel Networks

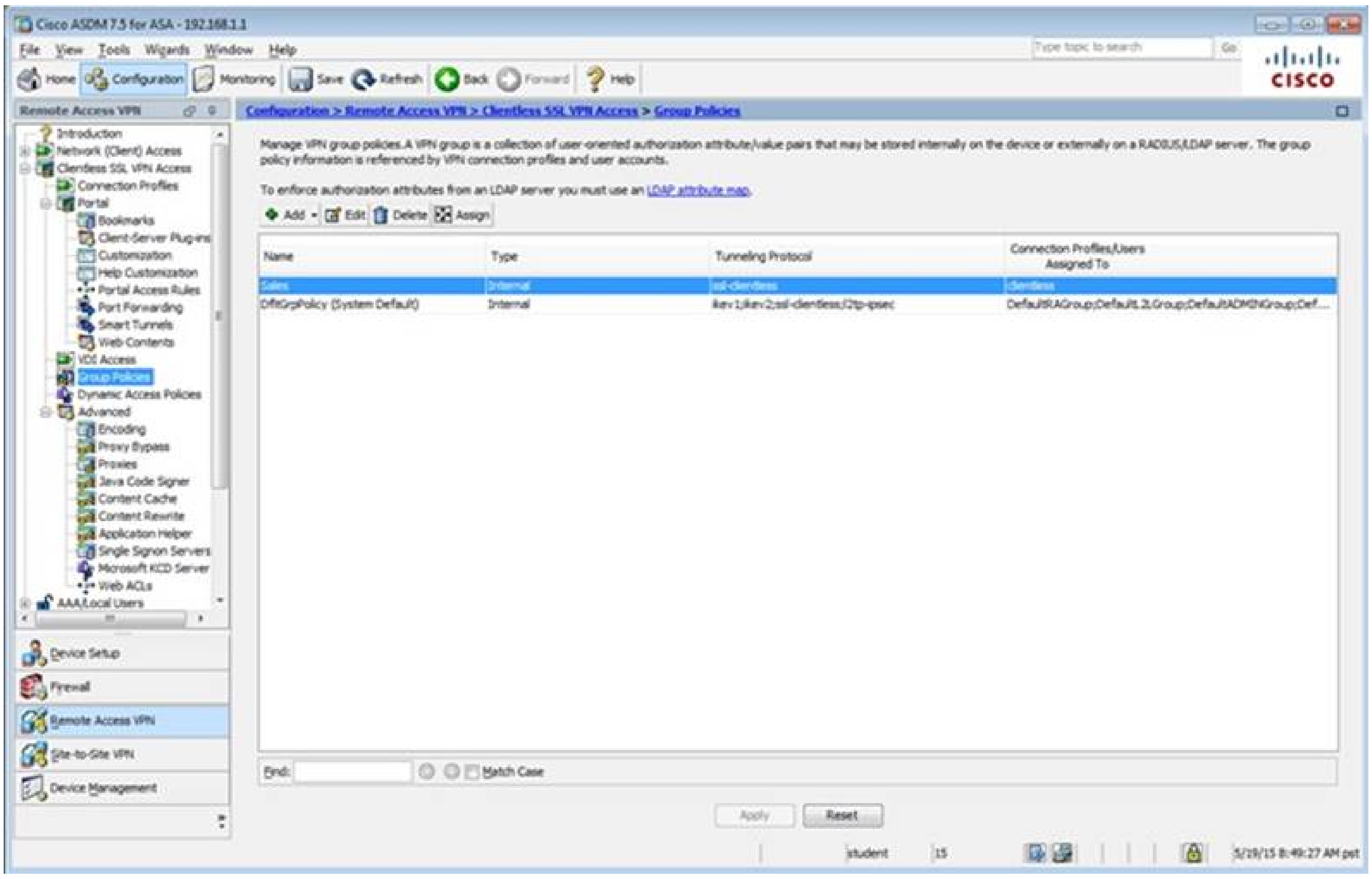


Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

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.

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

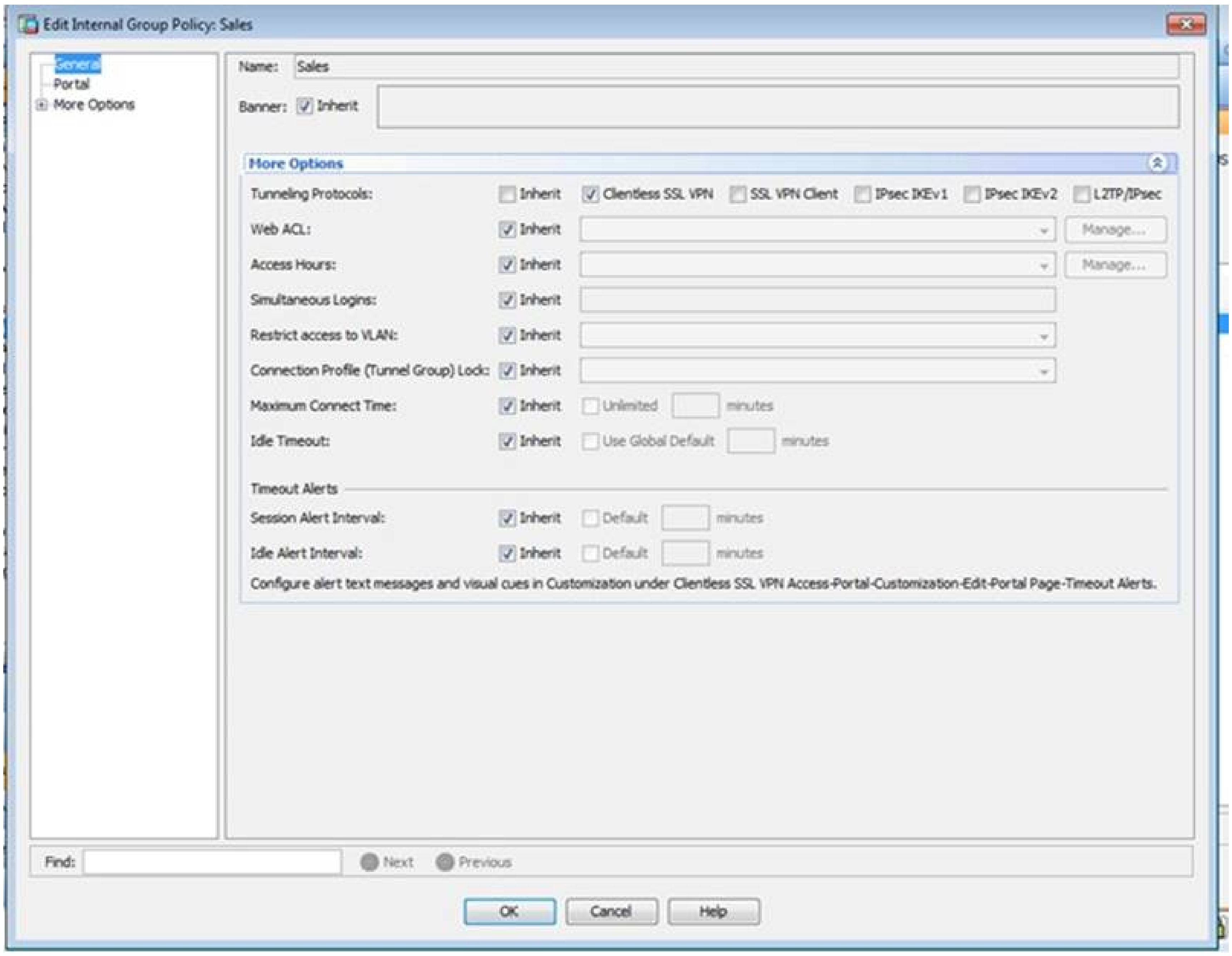


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

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	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...



Edit Internal Group Policy: Sales

Name: Sales

Banner: ☑ Inherit

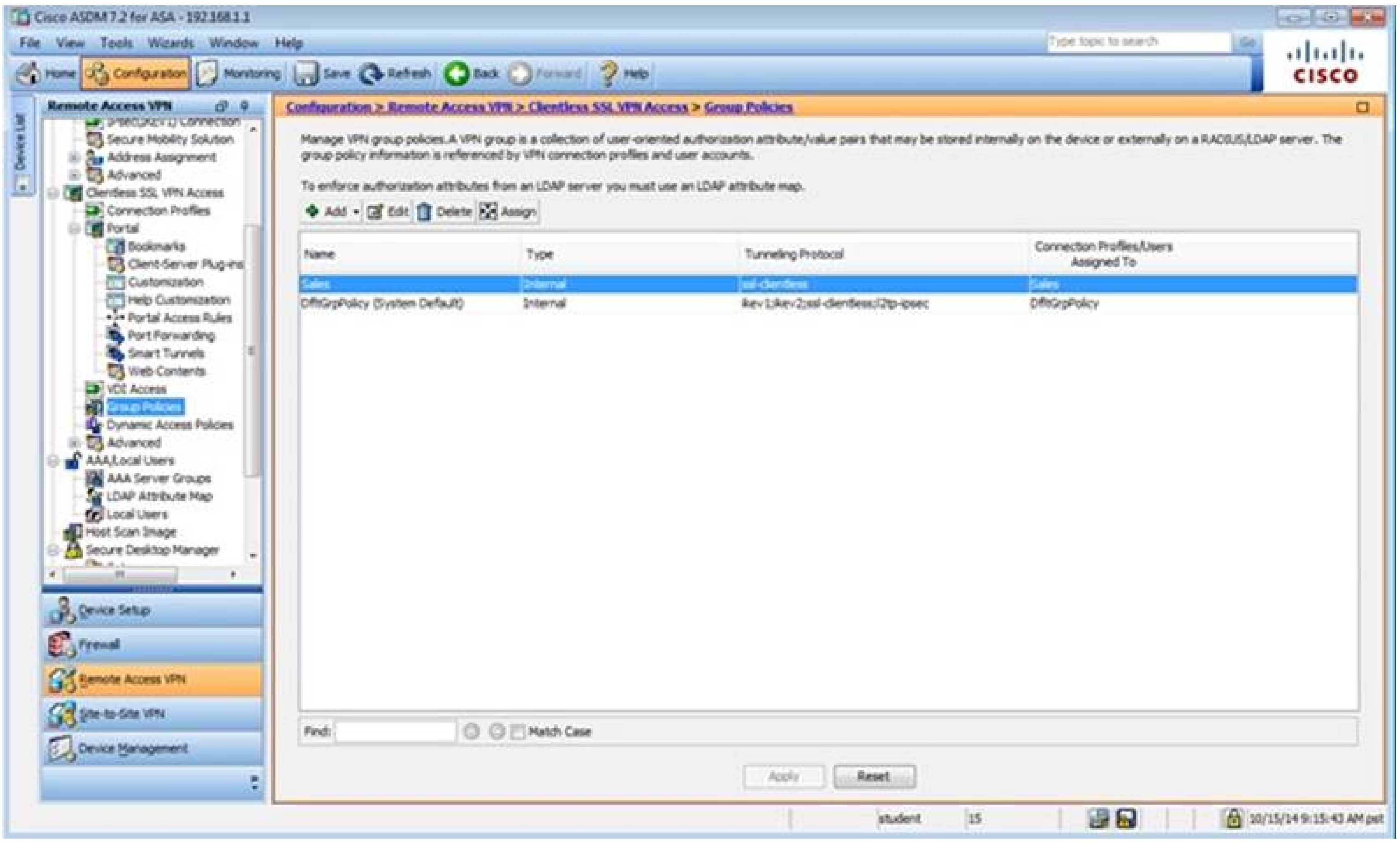
More Options

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.



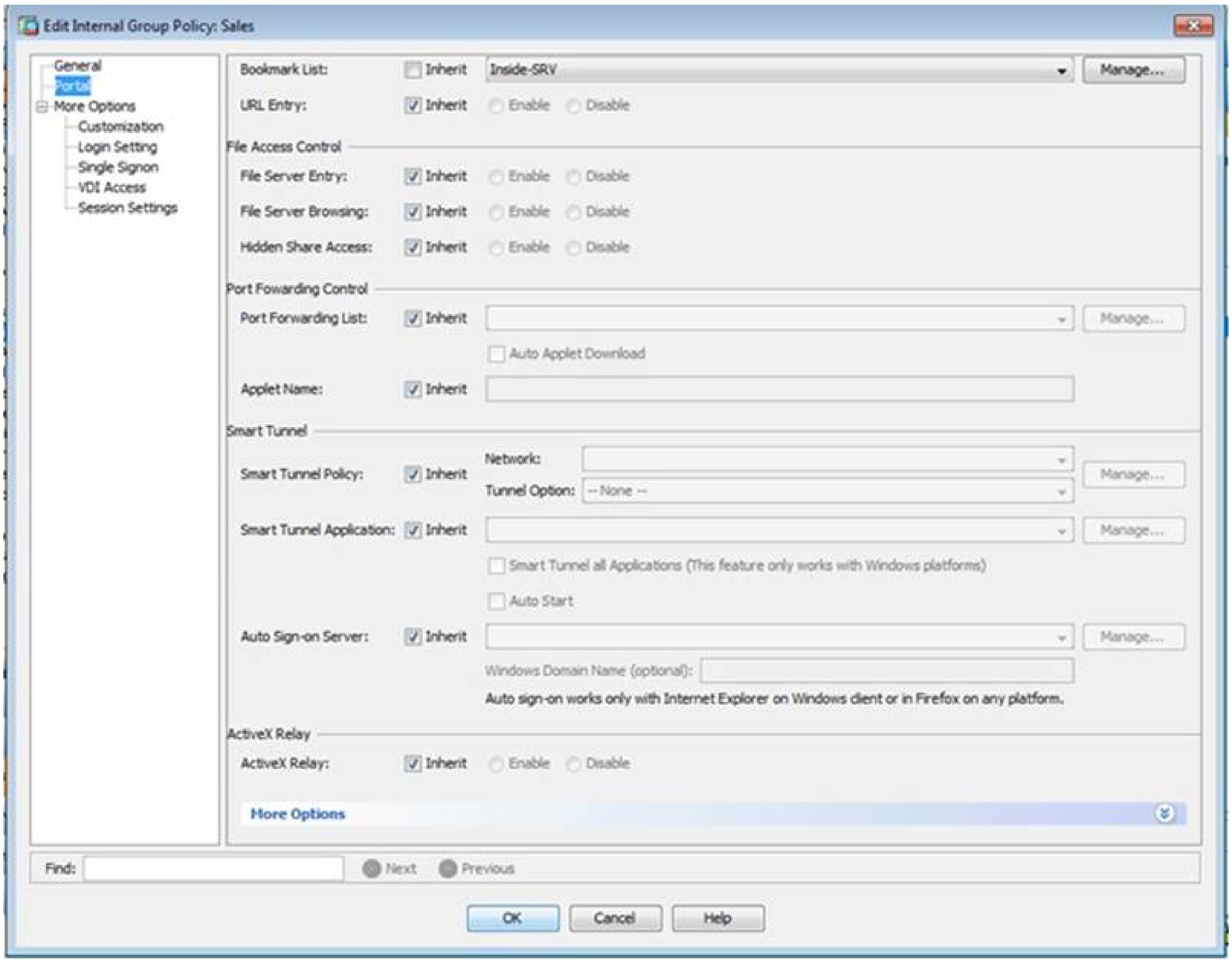
Cisco ASDM 7.2 for ASA - 192.168.1.1

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

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

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

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



Edit Internal Group Policy: Sales

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

Bookmark List: □ Inherit Inside-SRV

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 Fowarding Control

Port Forwarding List: ☑ Inherit

□ Auto Applet Download

Applet Name: ☑ Inherit

Smart Tunnel

Smart Tunnel Policy: ☑ Inherit Network: Tunnel Option: -- None --

Smart Tunnel Application: ☑ Inherit

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

□ Auto Start

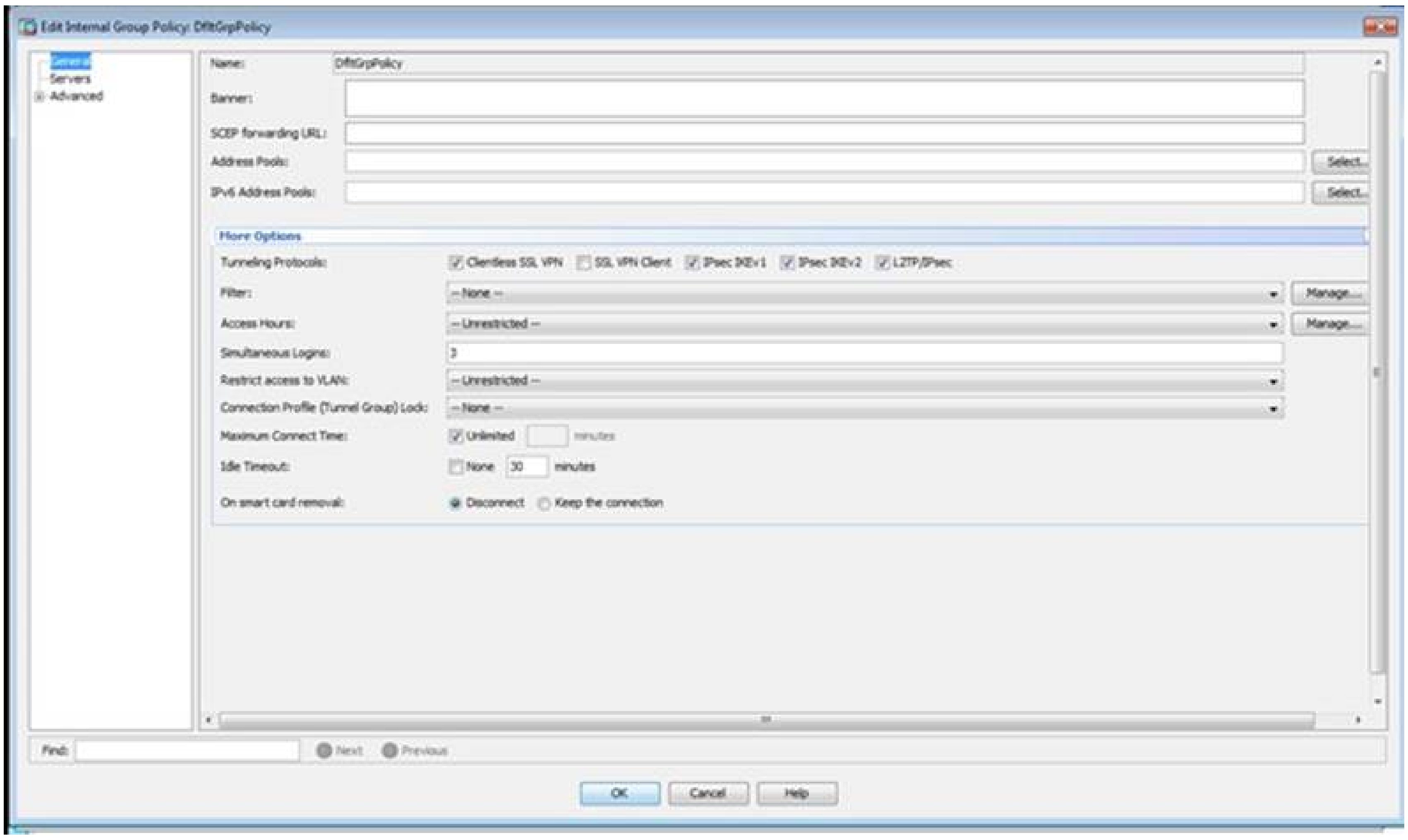
Auto Sign-on Server: ☑ Inherit

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



Edit Internal Group Policy: DfltGrpPolicy

- General
- Servers
- Advanced

Name: DfltGrpPolicy

Banner:

SCEP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

Tunneling Protocols: ☑ Clientless SSL VPN □ SSL VPN Client ☑ IPsec IKEv1 ☑ IPsec IKEv2 ☑ L2TP/IPsec

Filter: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

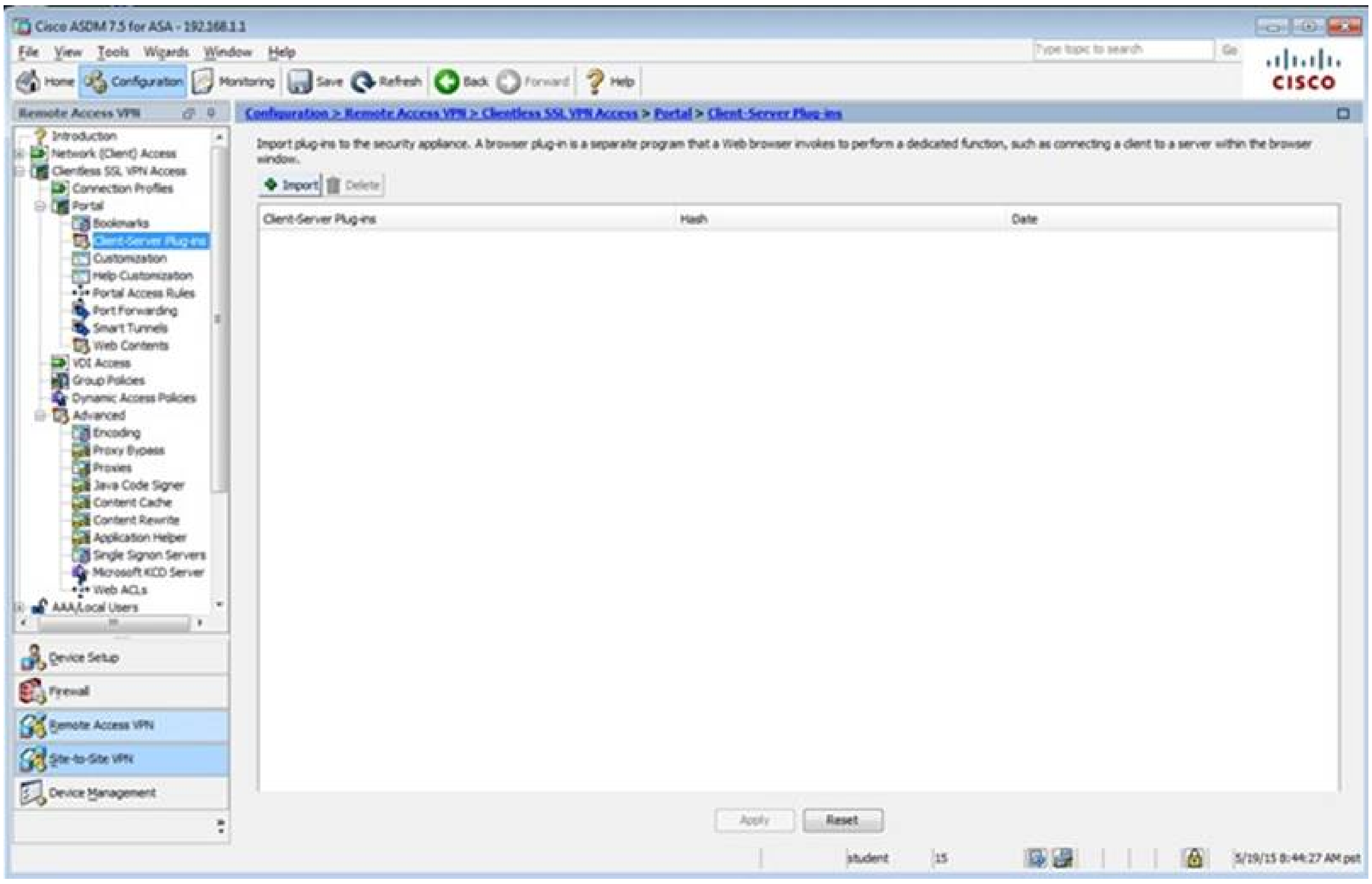
Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: □ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection

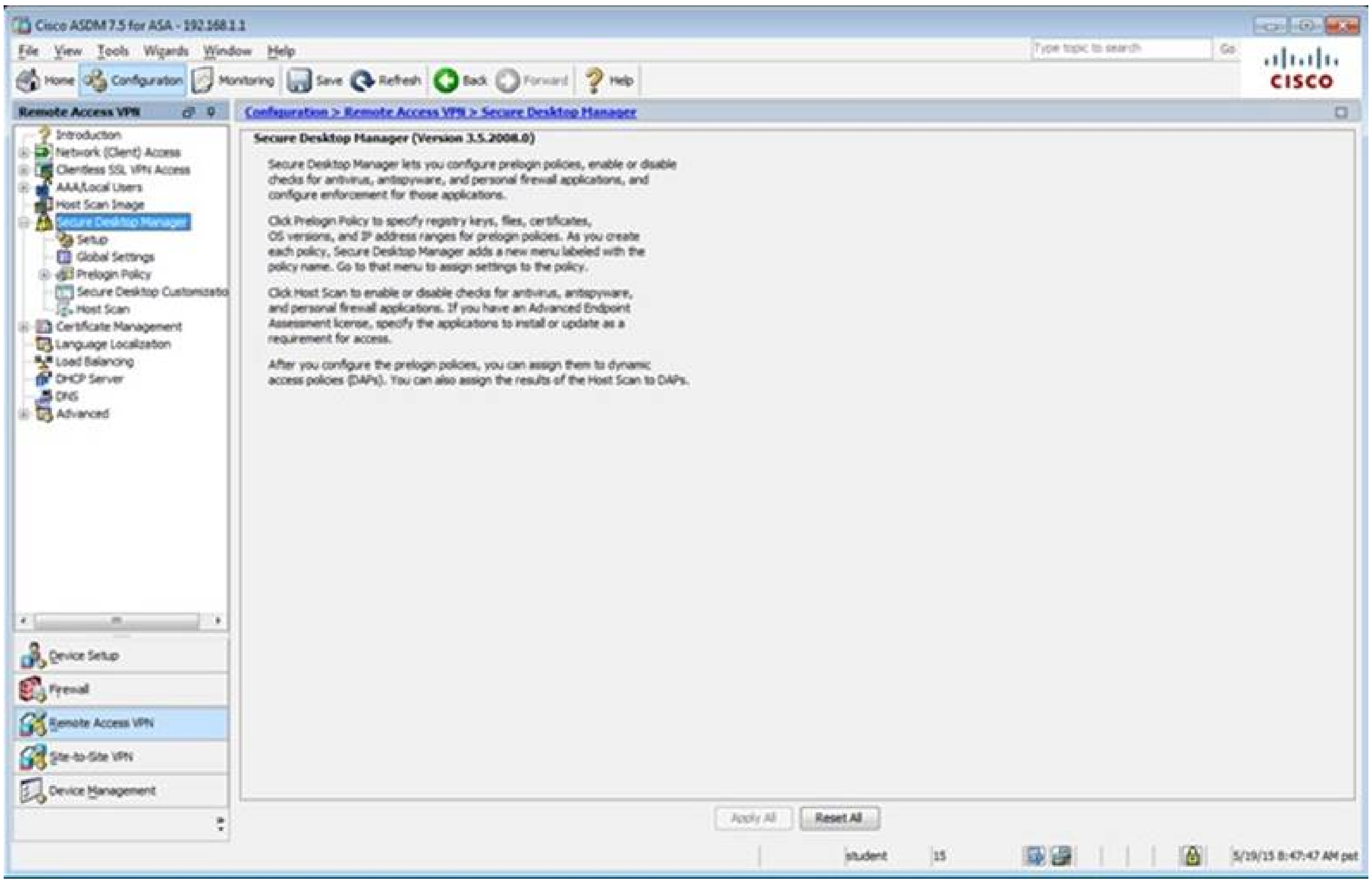


Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins

Import plug-ins to the security appliance. A browser plug-in is a separate program that a Web browser invokes to perform a dedicated function, such as connecting a client to a server within the browser window.

Import Delete

Client-Server Plug-ins	Hash	Date



Configuration > Remote Access VPN > Secure Desktop Manager

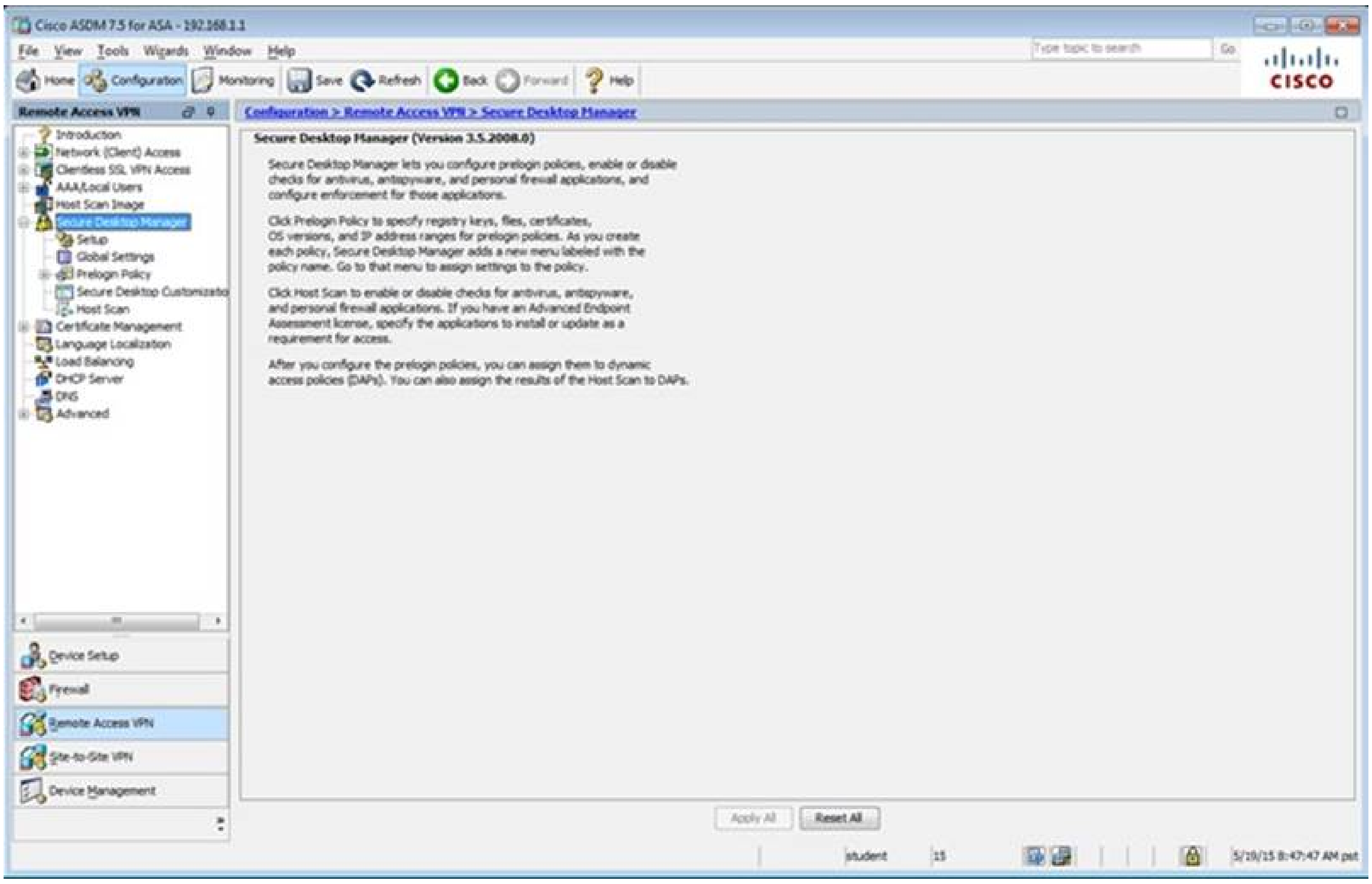
Secure Desktop Manager (Version 3.5.2008.0)

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

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

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

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



Configuration > Remote Access VPN > Secure Desktop Manager

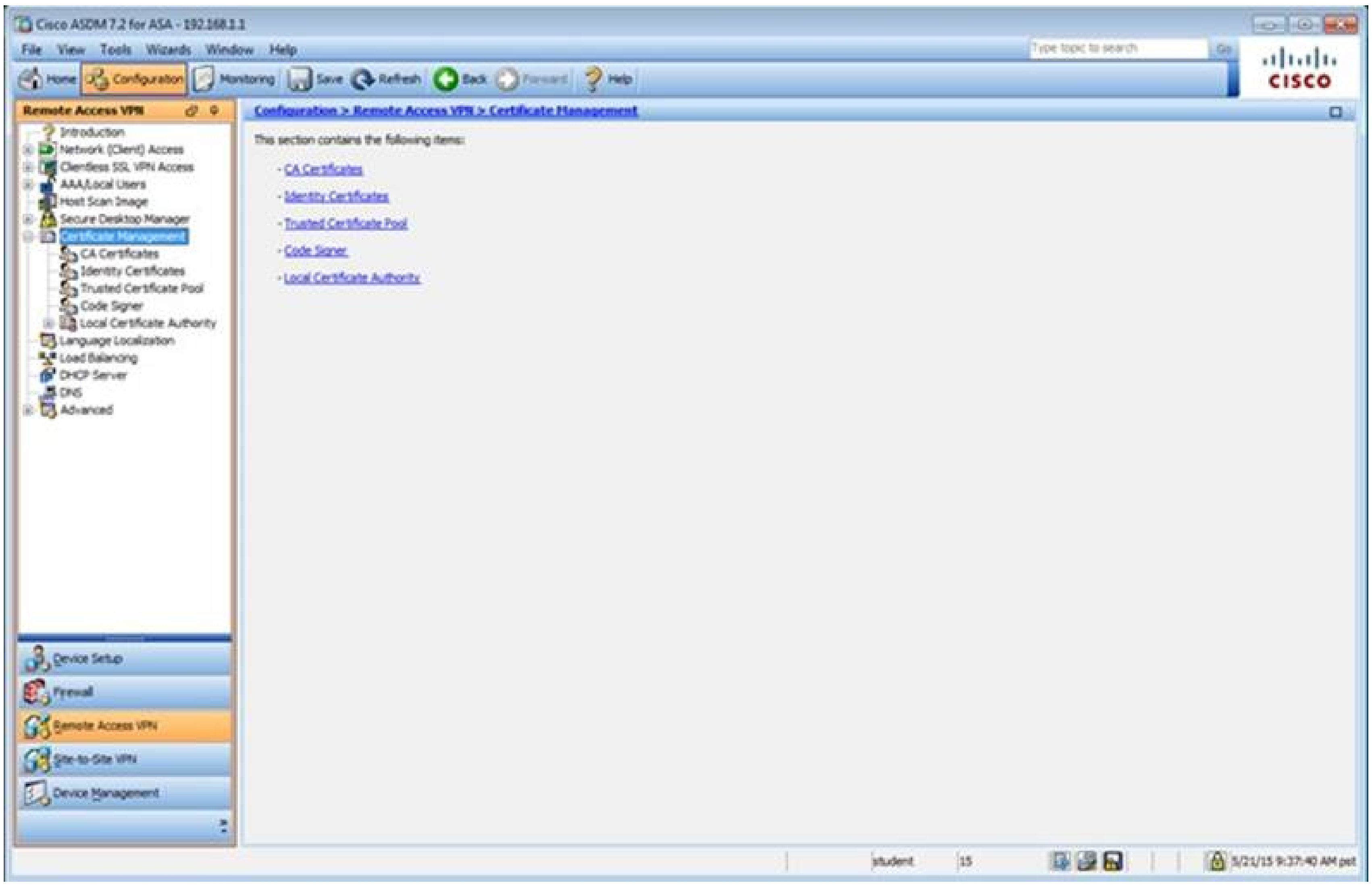
Secure Desktop Manager (Version 3.5.2008.0)

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

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

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

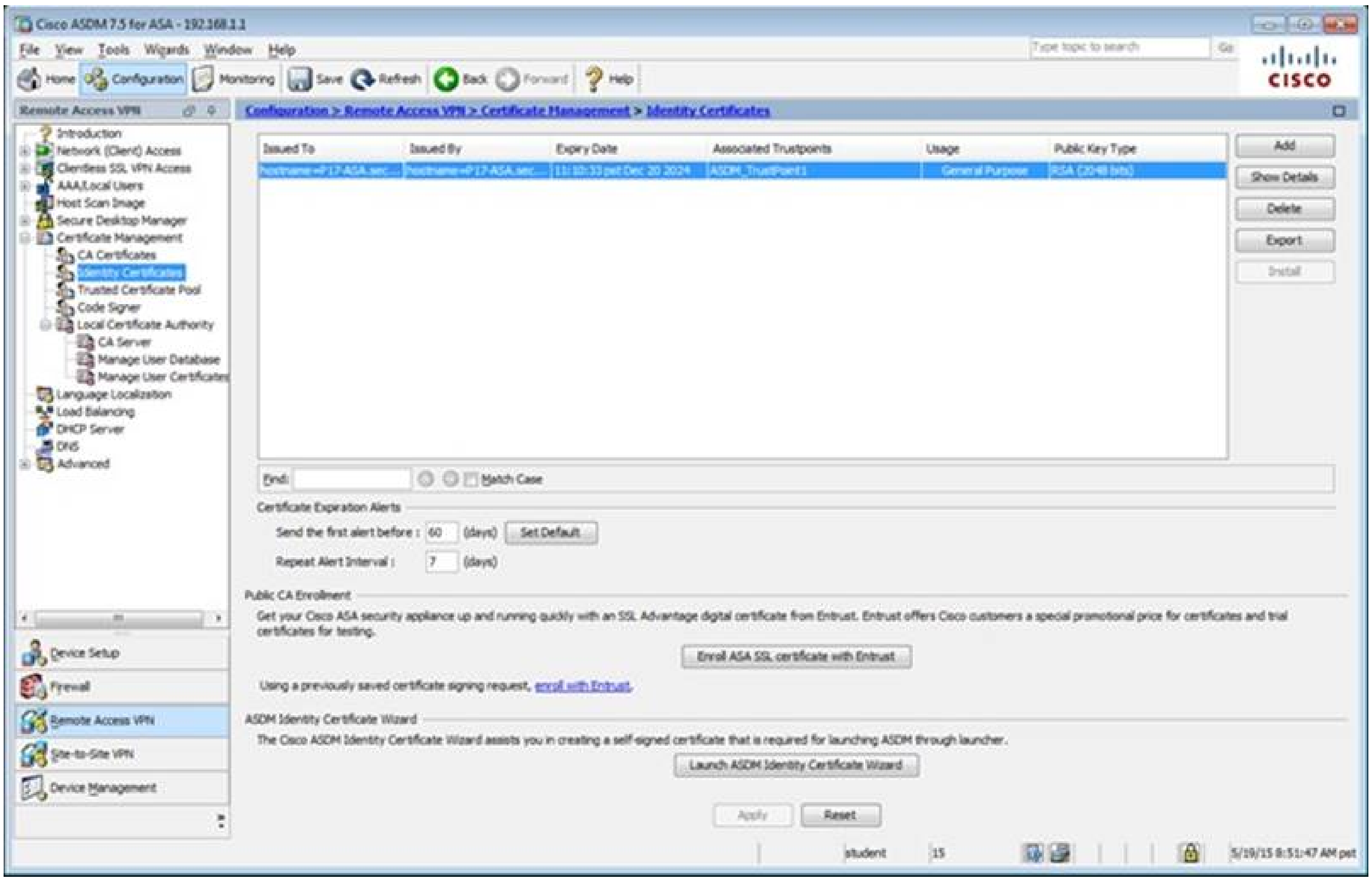
After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.



Configuration > Remote Access VPN > Certificate Management

This section contains the following items:

- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM_TrustPoint1	General Purpose	RSA (2048 bits)

Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

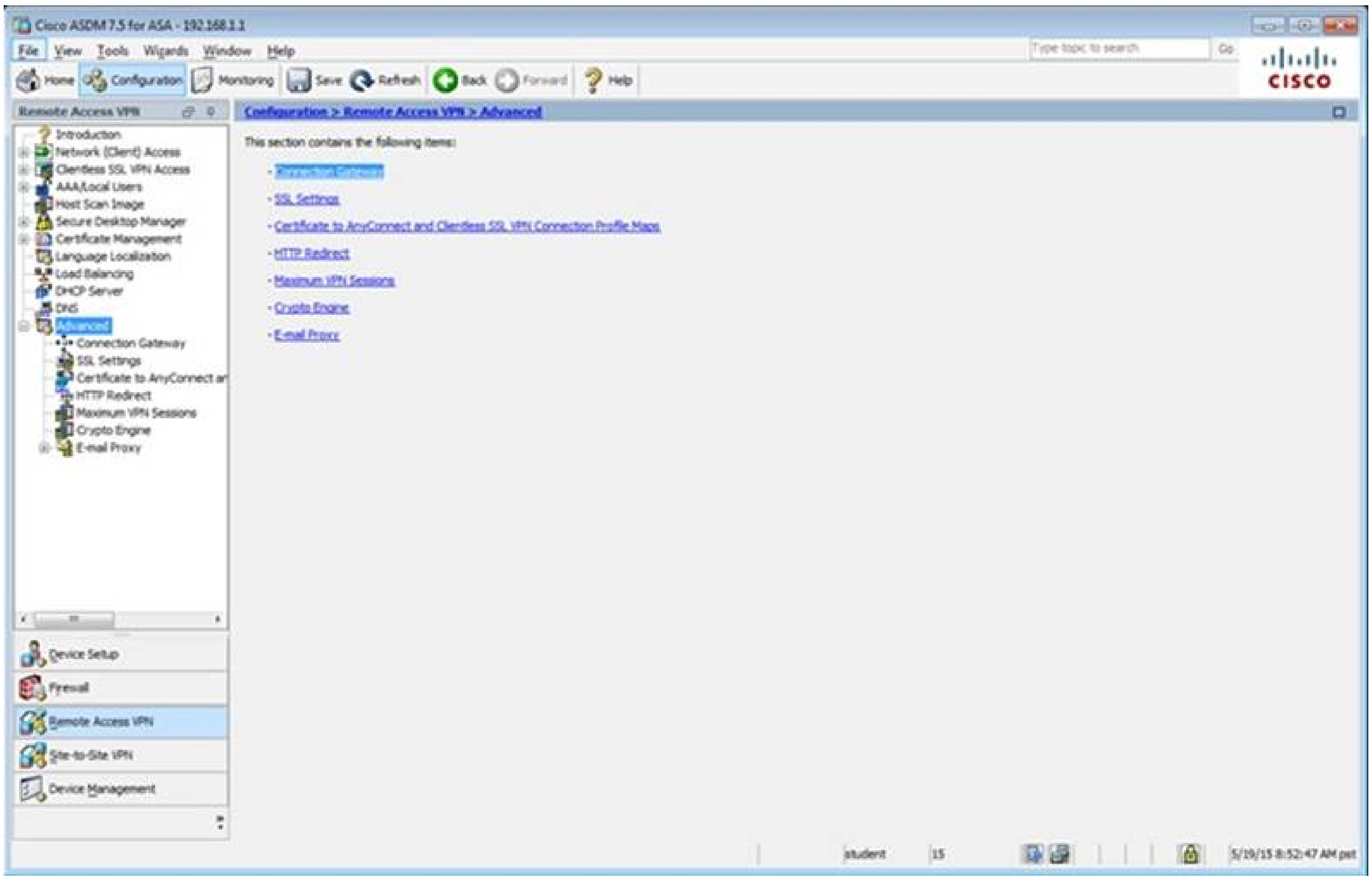
Public CA Enrollment

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

Using a previously saved certificate signing request, enroll with Entrust.

ASDM Identity Certificate Wizard

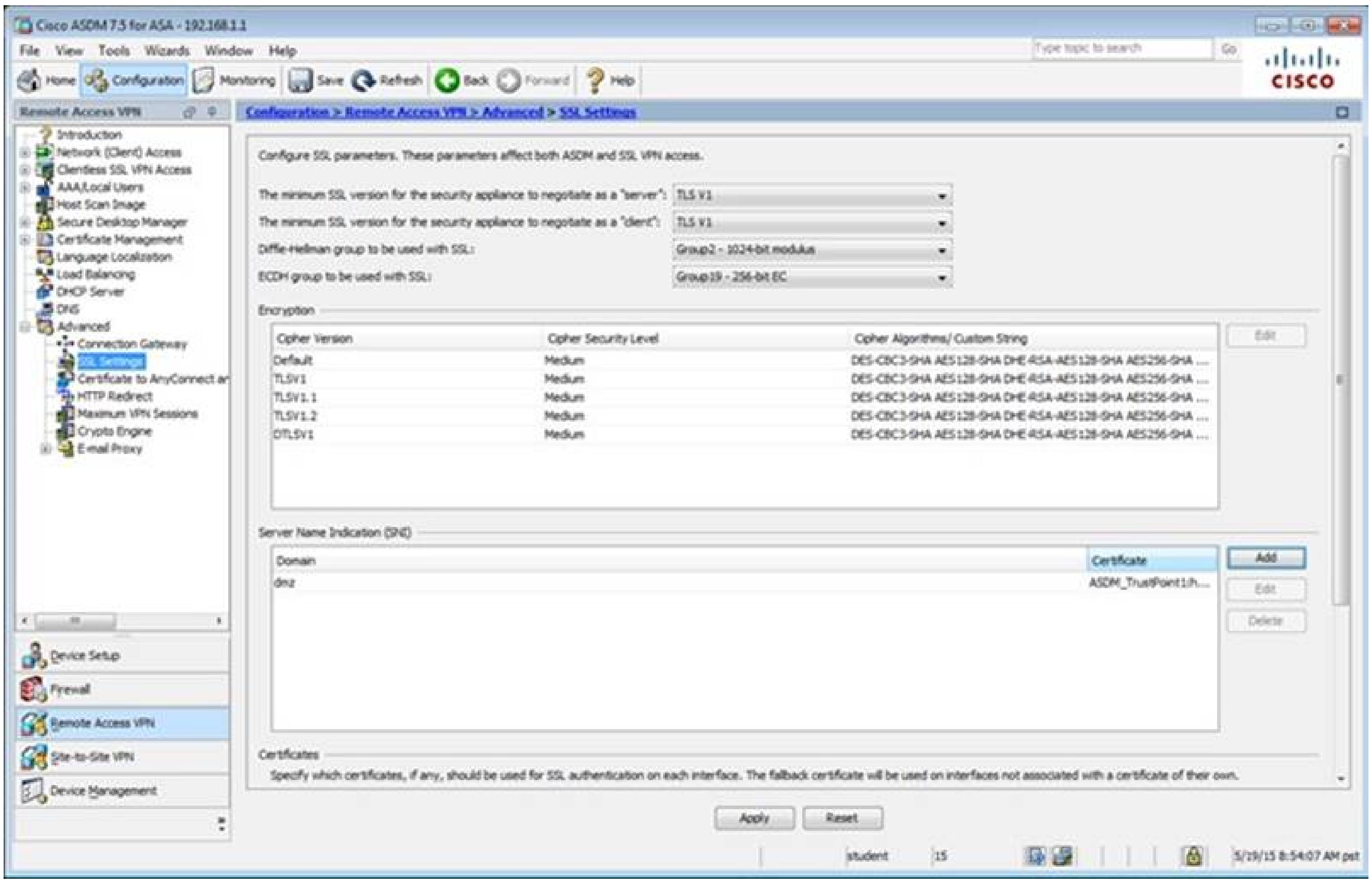
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.



Configuration > Remote Access VPN > Advanced

This 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
- E-mail Proxy



Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

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

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

Encryption

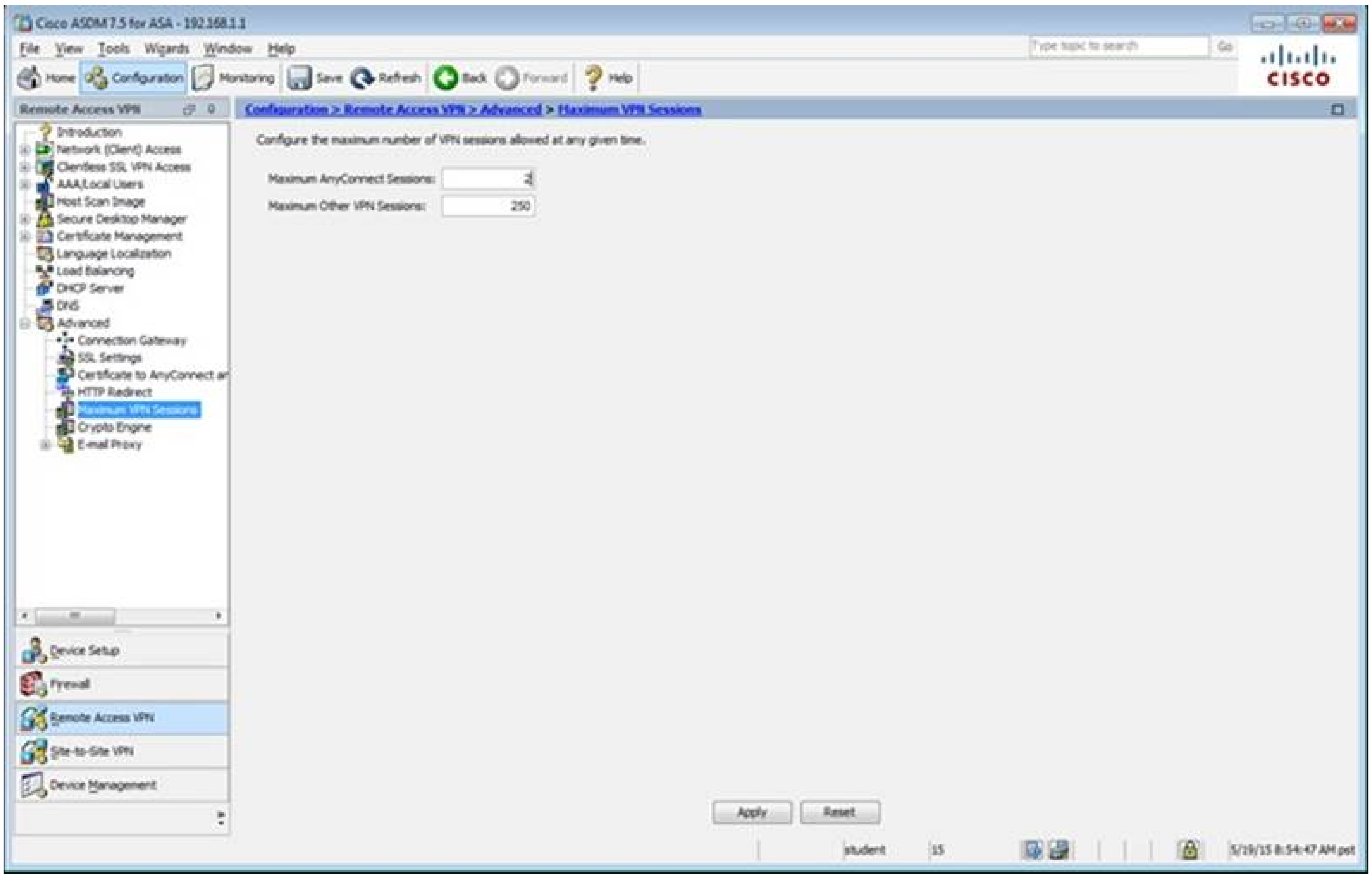
Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium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

Server Name Indication (SNI)

Domain	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.

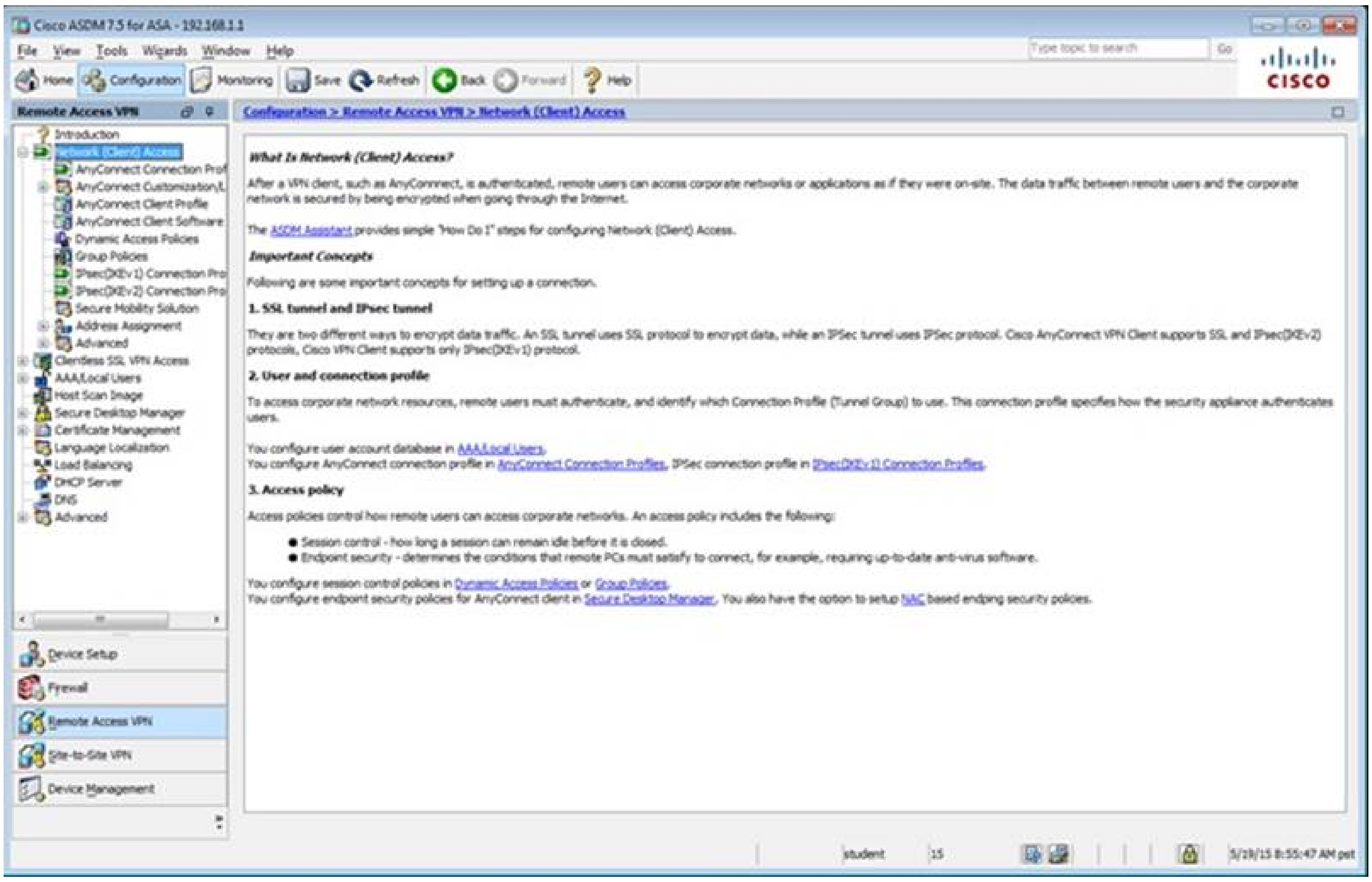


Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions

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

Maximum AnyConnect Sessions: 2

Maximum Other VPN Sessions: 250



Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

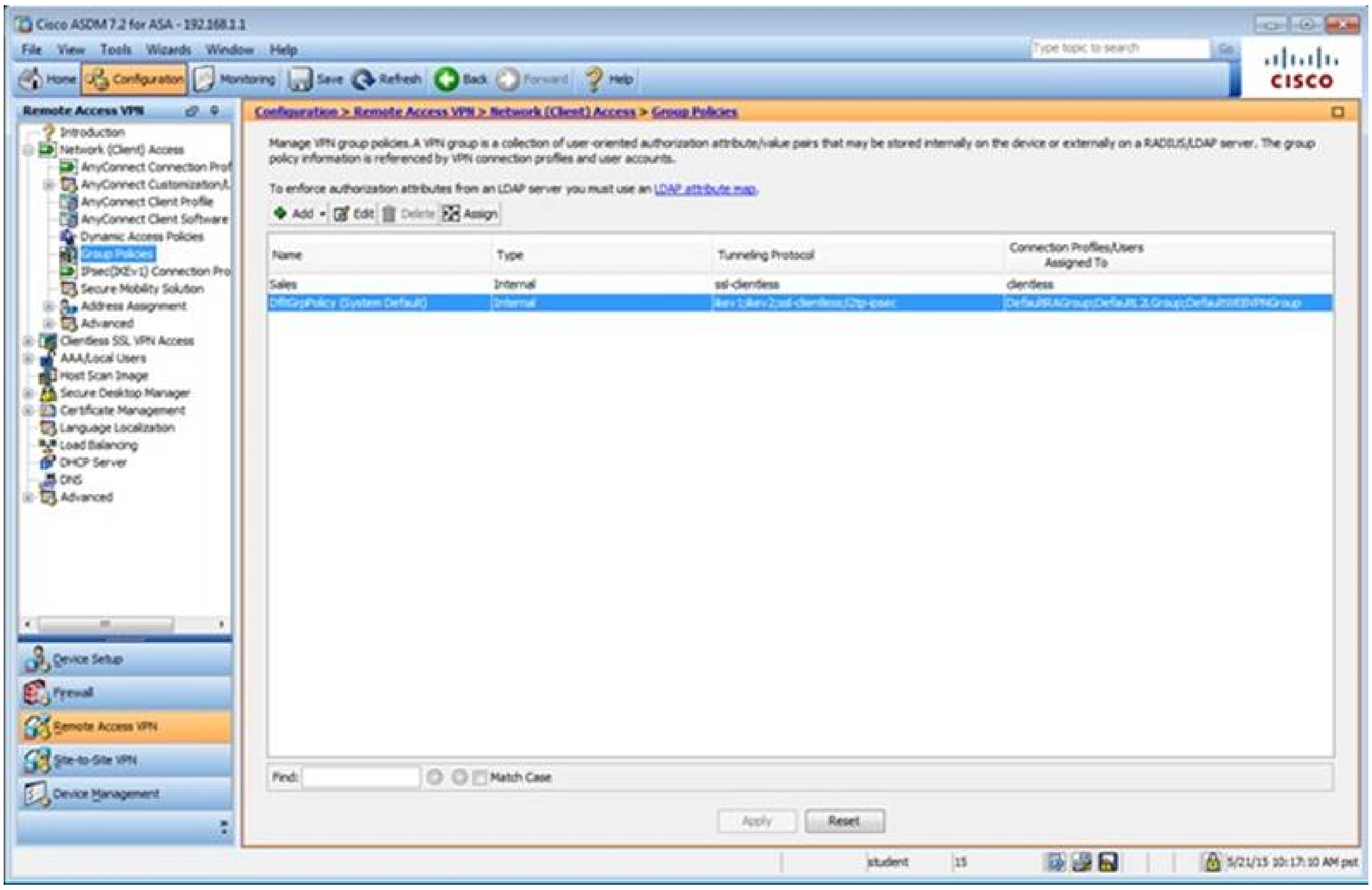
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles, IPSec connection profile in IPsec(IKEv1) Connection Profiles.

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, requring 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 endping security policies.

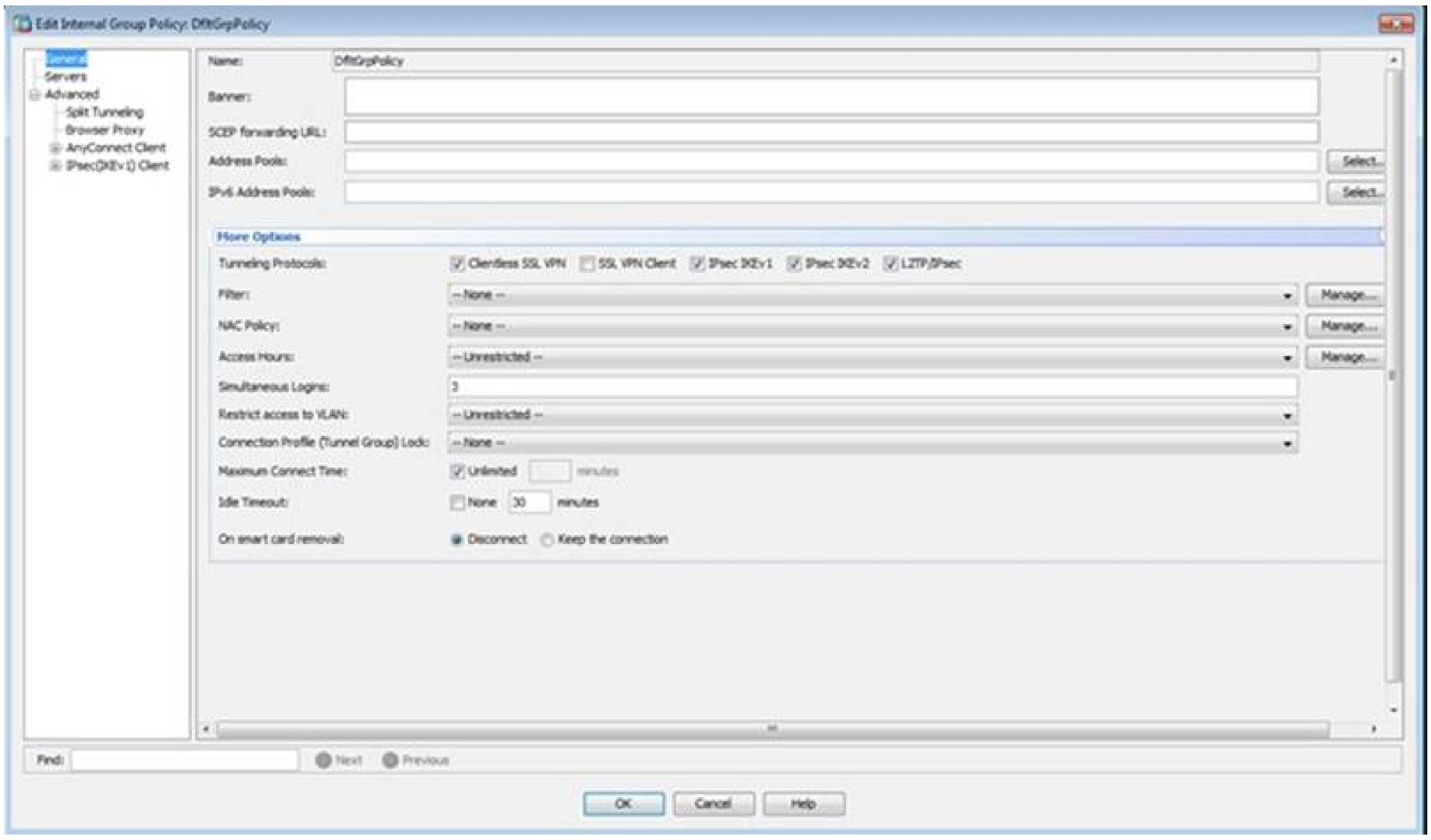


Configuration > Remote Access VPN > Network (Client) Access > Group Policies

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

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

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup



Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Banner:

SCEP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None --

NAC Policy: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

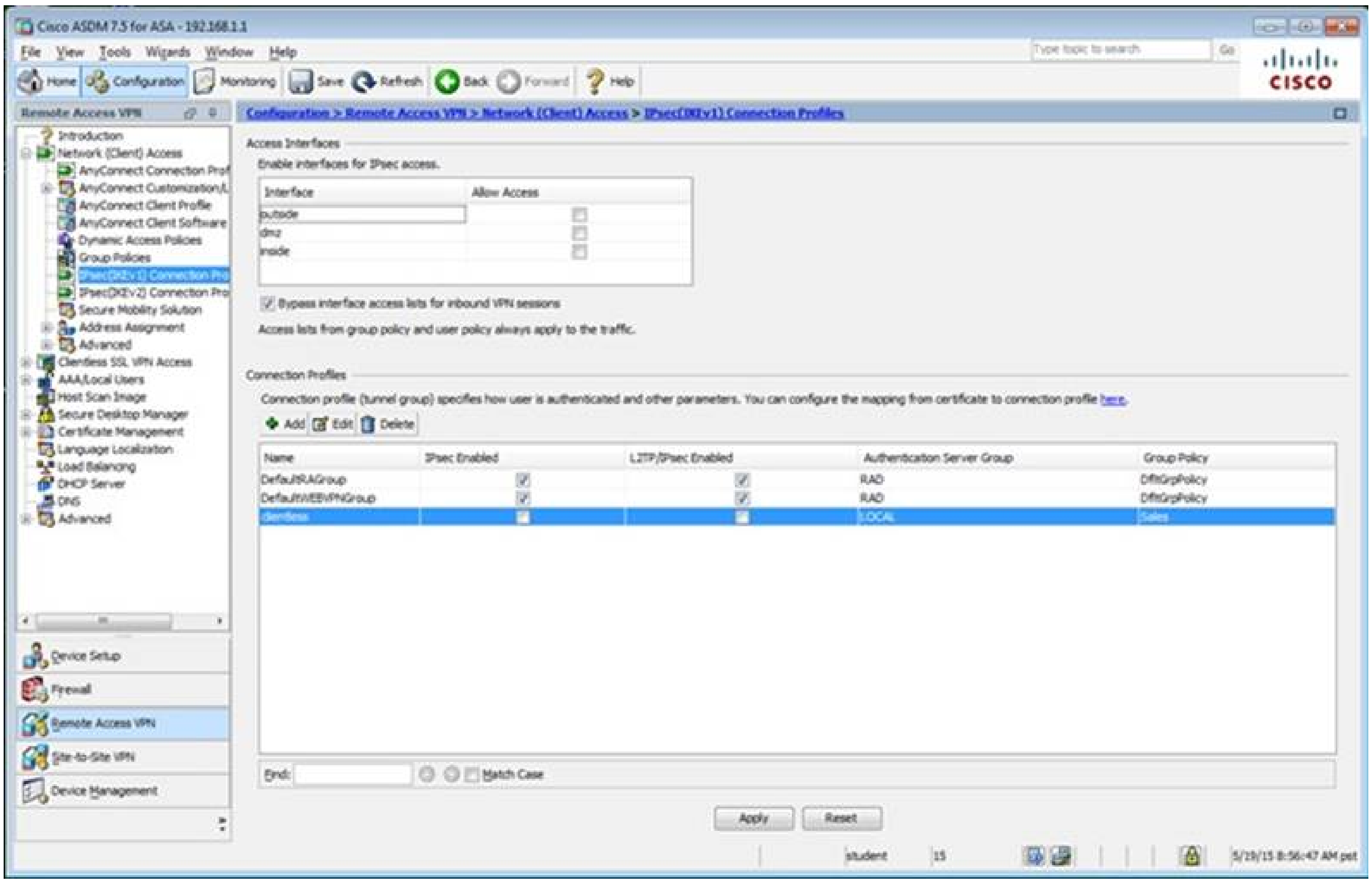
Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: ☐ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☐
dmz	☐
inside	☐

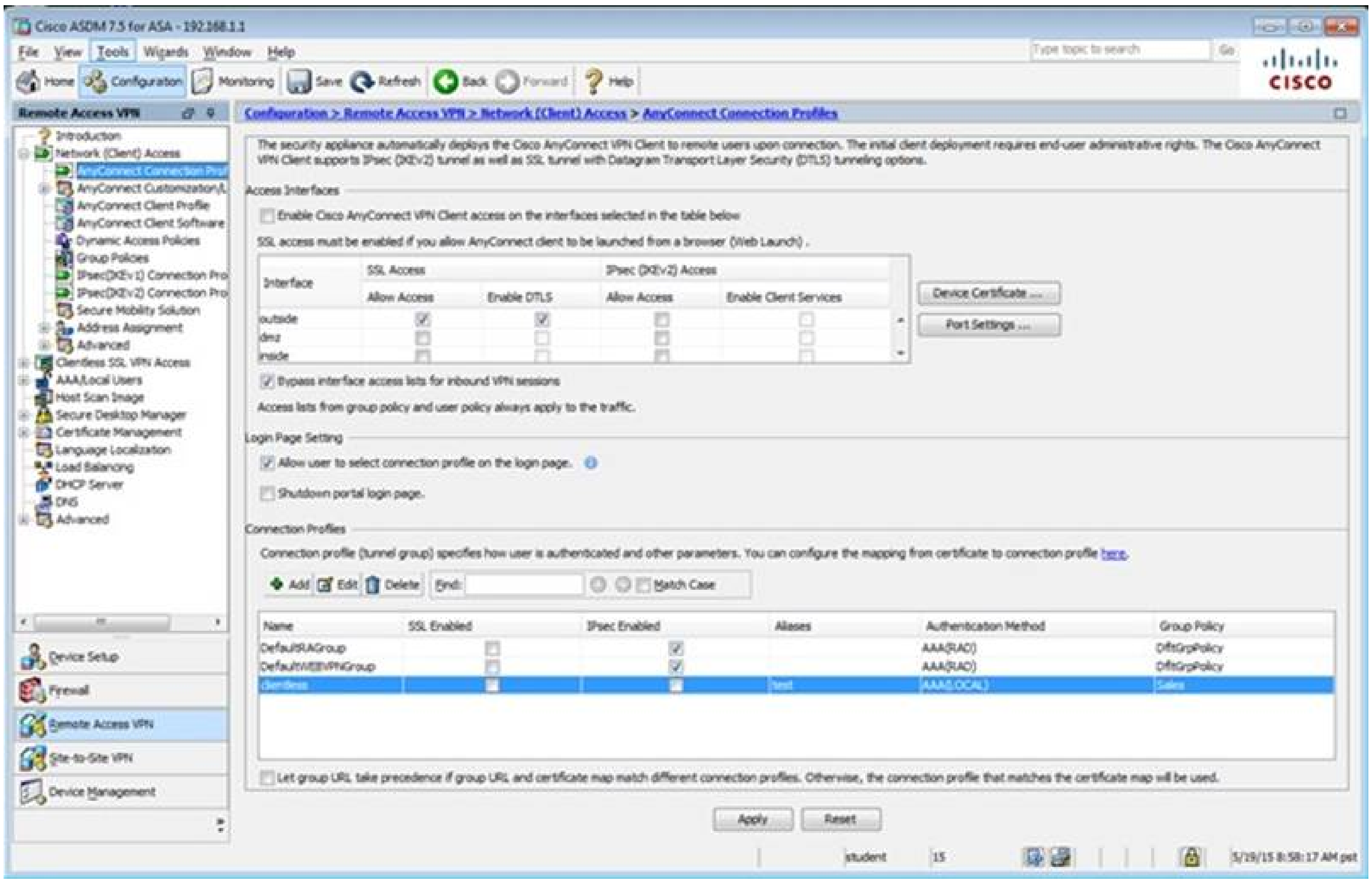
☑ Bypass interface access lists for inbound VPN sessions

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.

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	☑	☑	RAD	DfltGrpPolicy
DefaultWEBVPNGroup	☑	☑	RAD	DfltGrpPolicy
clientless	☐	☐	LOCAL	Sales



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	☑	☑	□	□
dmz	□	□	□	□
inside	□	□	□	□

Device Certificate ... Port Settings ...

☑ 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.

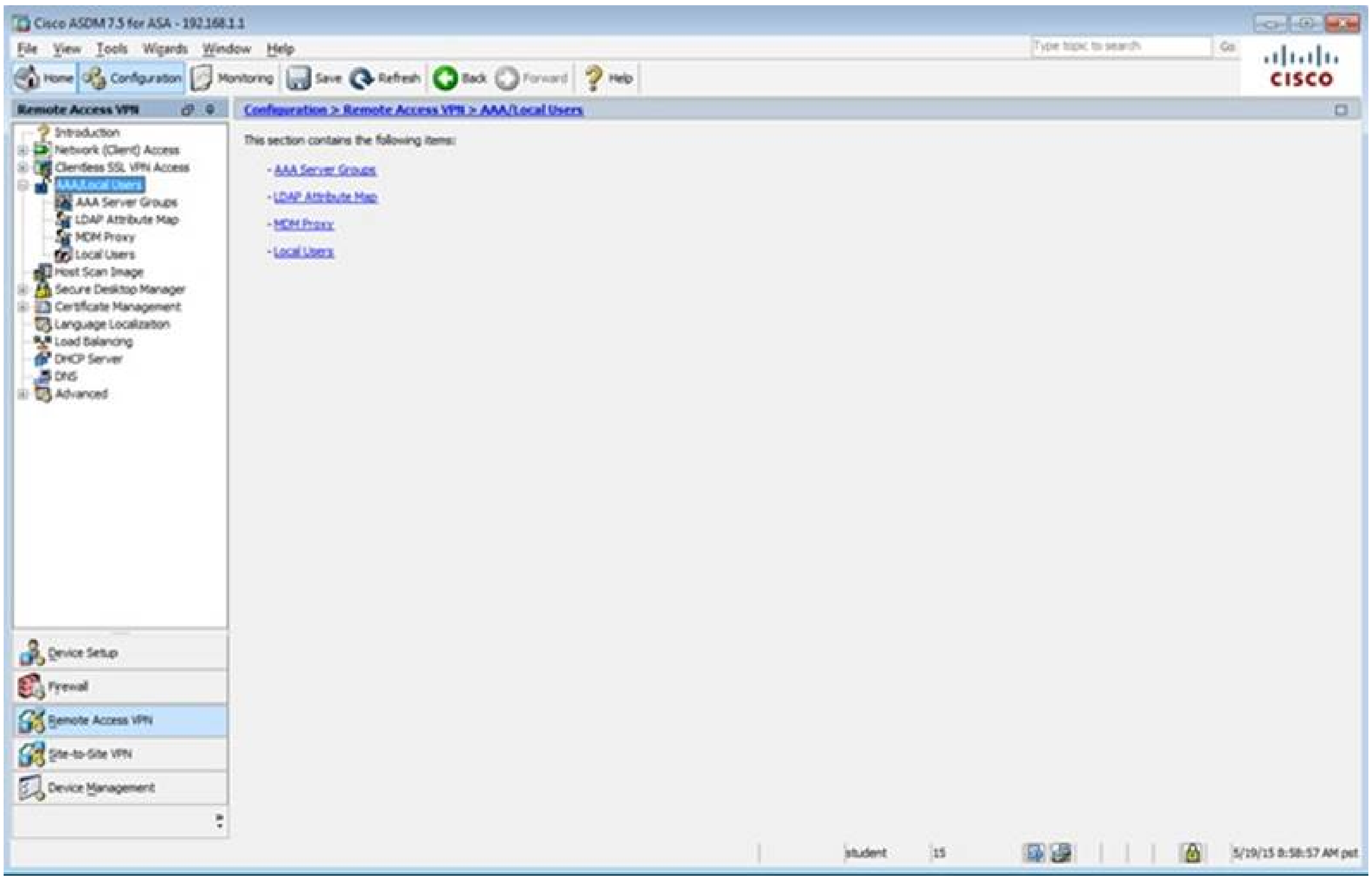
Add Edit Delete Find: □ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(RAD)	DfltGrpPolicy
clientless	□	□	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 pst

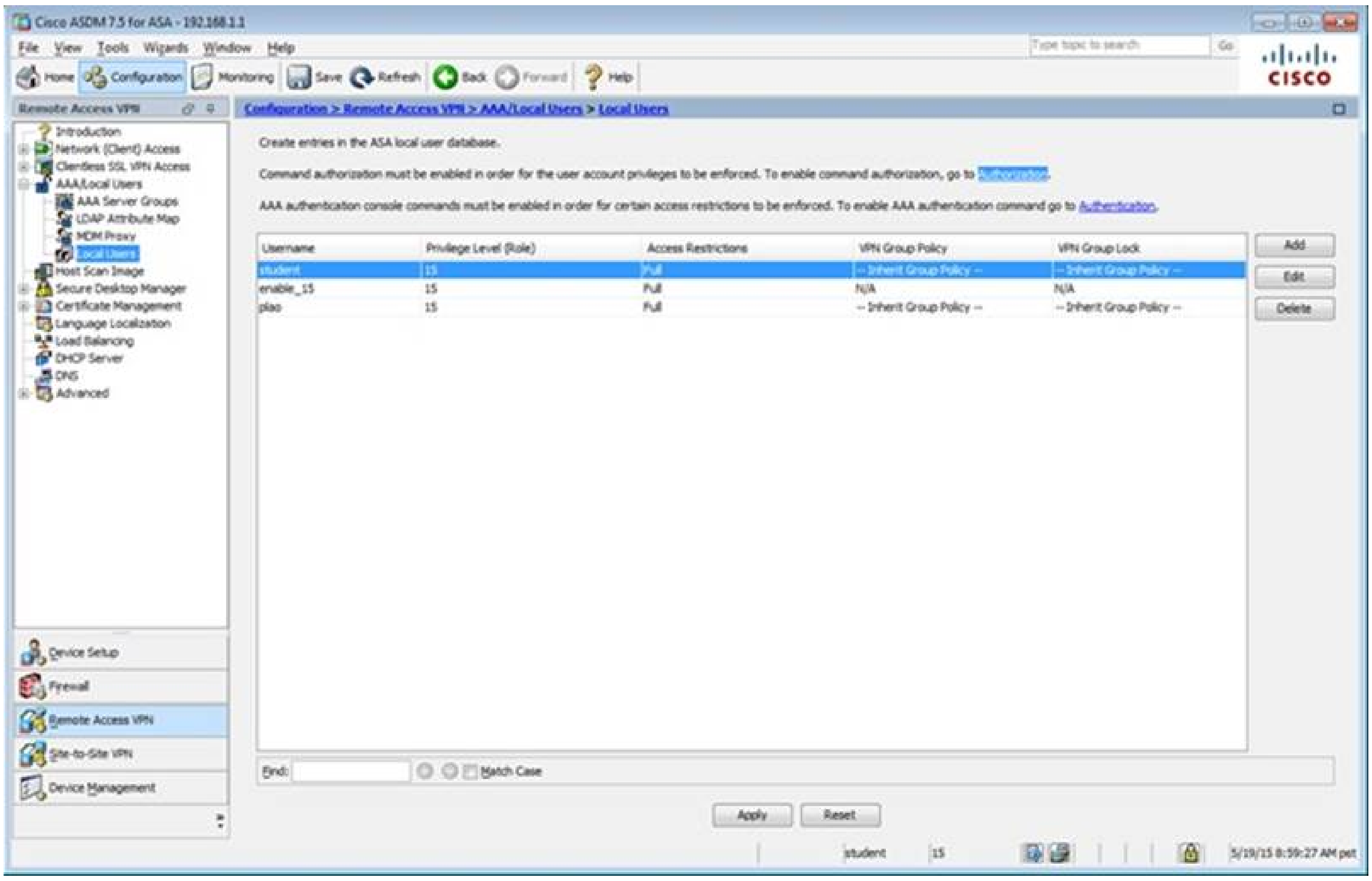


Configuration > Remote Access VPN > AAA/Local Users

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 pst



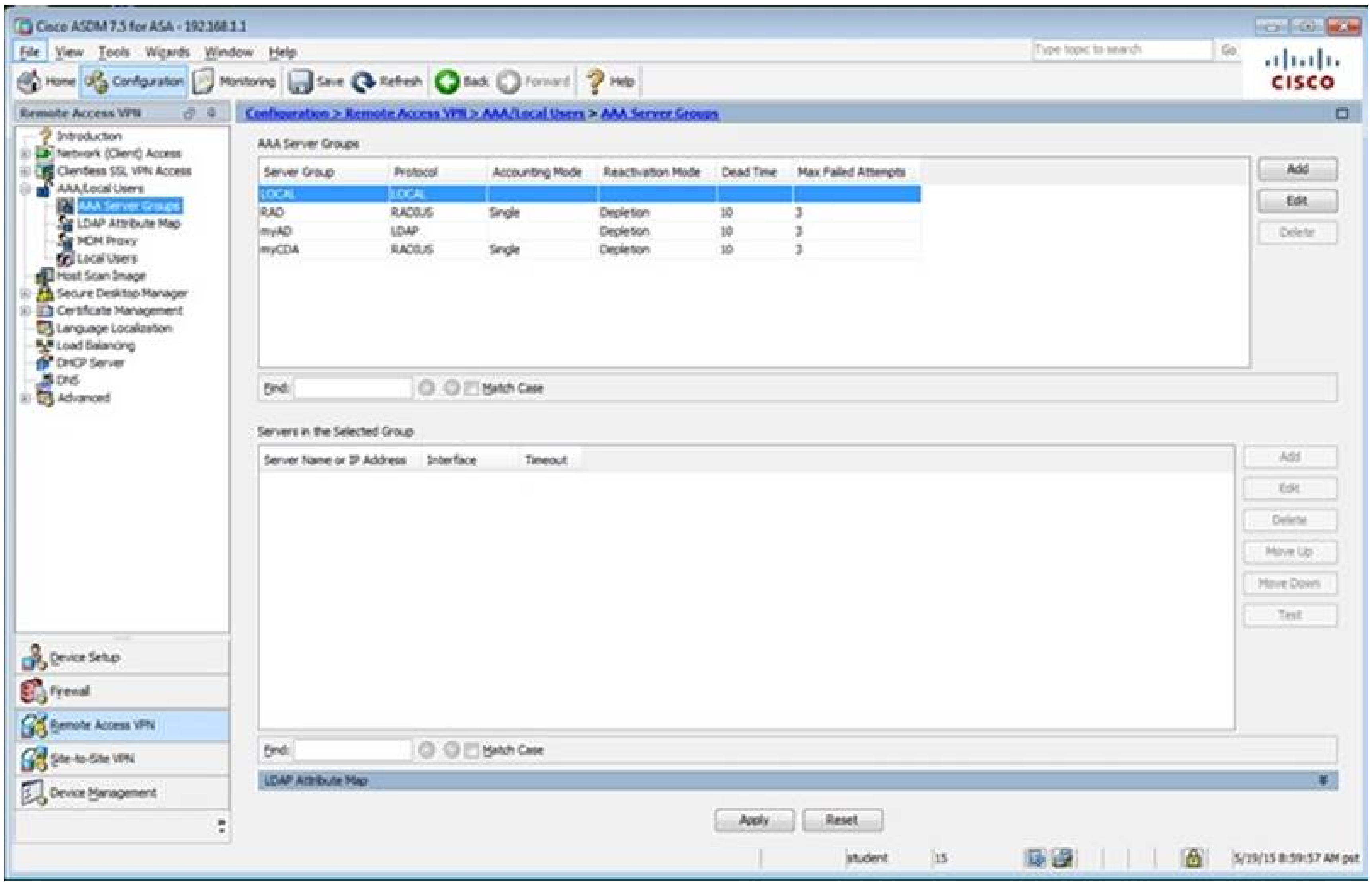
Configuration > Remote Access VPN > AAA/Local Users > Local Users

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 --



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				
RAD	RADIUS	Single	Depletion	10	3
myAD	LDAP		Depletion	10	3
myCDA	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

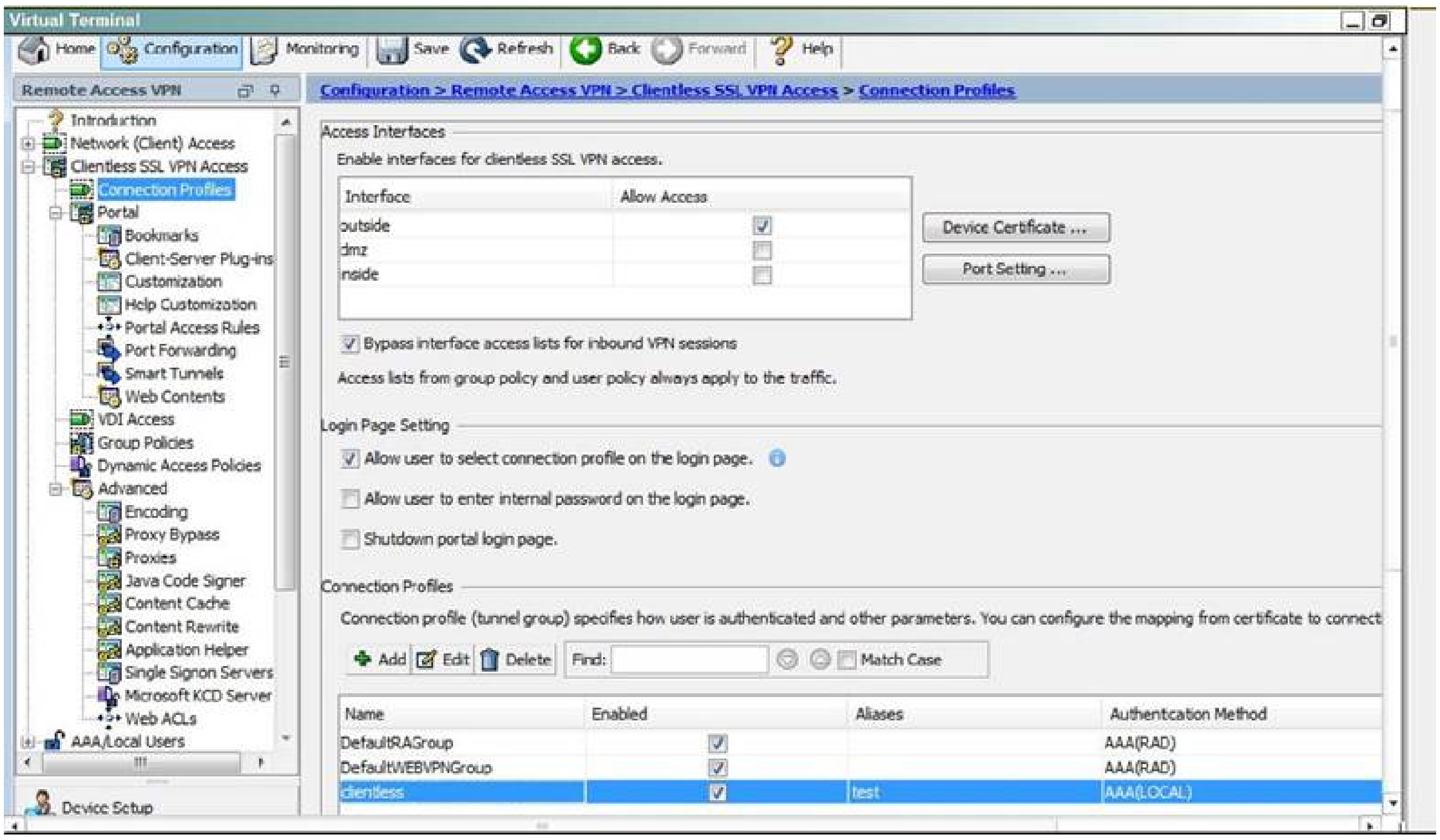
Server Name or IP Address	Interface	Timeout

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

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

Answer: A

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



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

□ Shutdown portal login page.

Connection Profiles

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

Name	Enabled	Aliases	Authentication Method
DefaultRAGroup	☑		AAA(RAD)
DefaultWEBVPNGroup	☑		AAA(RAD)
clientless	☑	test	AAA(LOCAL)

NEW QUESTION 11
Which EAP method uses Protected Access Credentials?

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

Answer: A

Explanation: Flexible Authentication via Secure Tunneling (EAP-FAST) is a protocol proposal by Cisco Systems as a replacement for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified.
Source: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

NEW QUESTION 14
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

NEW QUESTION 18
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
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

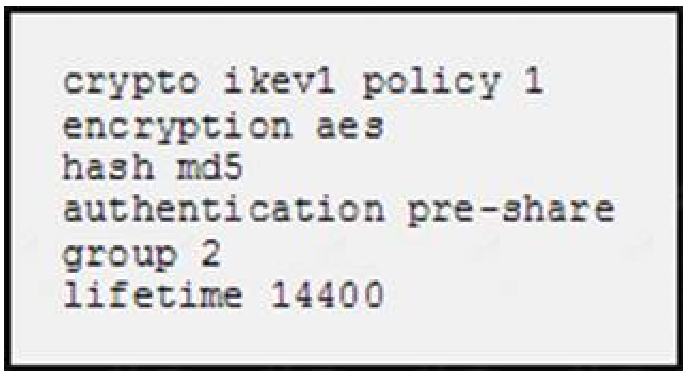
NEW QUESTION 25
Which type of secure connectivity does an extranet provide?

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

Answer: A

Explanation: What is an Extranet? In the simplest terms possible, an extranet is a type of network that crosses organizational boundaries, giving outsiders access to information and resources stored inside the organization's internal network (Loshin, p. 14).
Source: https://www.sans.org/reading-room/whitepapers/firewalls/securing-extranet-connections-816

NEW QUESTION 29
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)

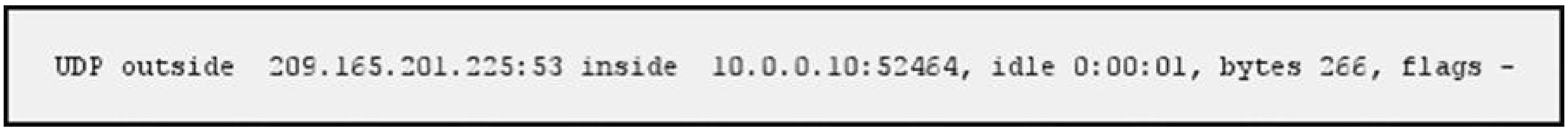
NEW QUESTION 34
What can the SMTP preprocessor in FirePOWER normalize?

A. It can extract and decode email attachments in client to server traffic.
B. It can look up the email sender.
C. It compares known threats to the email sender.
D. It can forward the SMTP traffic to an email filter server.
E. It uses the Traffic Anomaly Detector.

Answer: A

Explanation: Decoding SMTP Traffic
The SMTP preprocessor instructs the rules engine to normalize SMTP commands. The preprocessor can also extract and decode email attachments in client-to-server traffic and, depending on the software version, extract email file names, addresses, and header data to provide context when displaying intrusion events triggered by SMTP traffic.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower- module-user-guide-v541/NAP-App-Layer.html#85623

NEW QUESTION 37
Refer to the exhibit.



```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall

Answer: A

Explanation: The output is from "show conn" command on an ASA. This is another example output I've simulated ciscoasa# show conn 20 in use, 21 most used UDP OUTSIDE 172.16.0.100:53 INSIDE 10.10.10.2:59655, idle 0:00:06, bytes 39, flags -

NEW QUESTION 38
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

NEW QUESTION 39
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

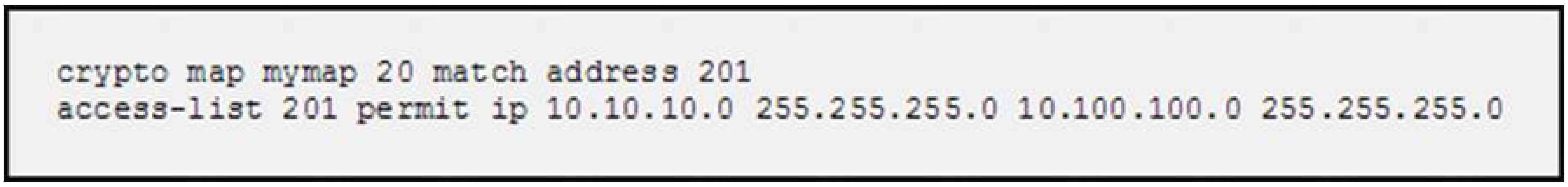
NEW QUESTION 42
When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?

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

Answer: A

Explanation: First when the switches are powered on all the ports are in Blocking state (20 sec), during this time the + Root Bridge is elected by exchanging BPDUs
+ The other switches will elect their Root ports
+ Every network segment will choosee their Designated port Source: https://learningnetwork.cisco.com/thread/7677

NEW QUESTION 47
Refer to the exhibit.



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

What is the effect of the given command sequence?

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

Answer: A

Explanation: A crypto ACL is a case for an extended ACL where we specify the source and destination address of the networks to be encrypted.

NEW QUESTION 49
In a security context, which action can you take to address compliance?

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

Answer: A

Explanation: In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Source:
https://en.wikipedia.org/wiki/Regulatory_compliance

NEW QUESTION 52
When a company puts a security policy in place, what is the effect on the company's business?

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

Answer: A

Explanation: The first step in protecting a business network is creating a security policy. A security policy is a formal, published document that defines roles, responsibilities, acceptable use, and key security practices for a
company. It is a required component of a complete security framework, and it should be used to guide investment in security defenses.
Source:
http://www.cisco.com/warp/public/cc/so/neso/sqso/secsol/setdm_wp.htm

NEW QUESTION 55
Which sensor mode can deny attackers inline?

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

Answer: A

Explanation: Deny attacker inline: This action denies packets from the source IP address of the attacker for a configurable duration of time, after which the deny action can be dynamically removed.
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 57
Which command is needed to enable SSH support on a Cisco Router?

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

Answer: B

Explanation: There are four steps required to enable SSH support on a Cisco IOS router:

+ Configure the hostname command.
+ Configure the DNS domain.
+ Generate the SSH key to be used.
+ Enable SSH transport support for the virtual type terminal (vtys).

```
!--- Step 1: Configure the hostname if you have not previously done so. hostname carter
!--- The aaa new-model command causes the local username and password on the router !--- to be used in the absence of other AAA statements.
aaa new-model
username cisco password 0 cisco
!--- Step 2: Configure the DNS domain of the router. ip domain-name rtp.cisco.com
!--- Step 3: Generate an SSH key to be used with SSH.
crypto key generate rsa ip ssh time-out 60
ip ssh authentication-retries 2
!--- Step 4: By default the vtys' transport is Telnet. In this case, !--- Telnet is disabled and only SSH is supported.
line vty 0 4 transport input SSH Source:
```

http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145- ssh.html#settingupaniosrouterasssh

NEW QUESTION 58

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

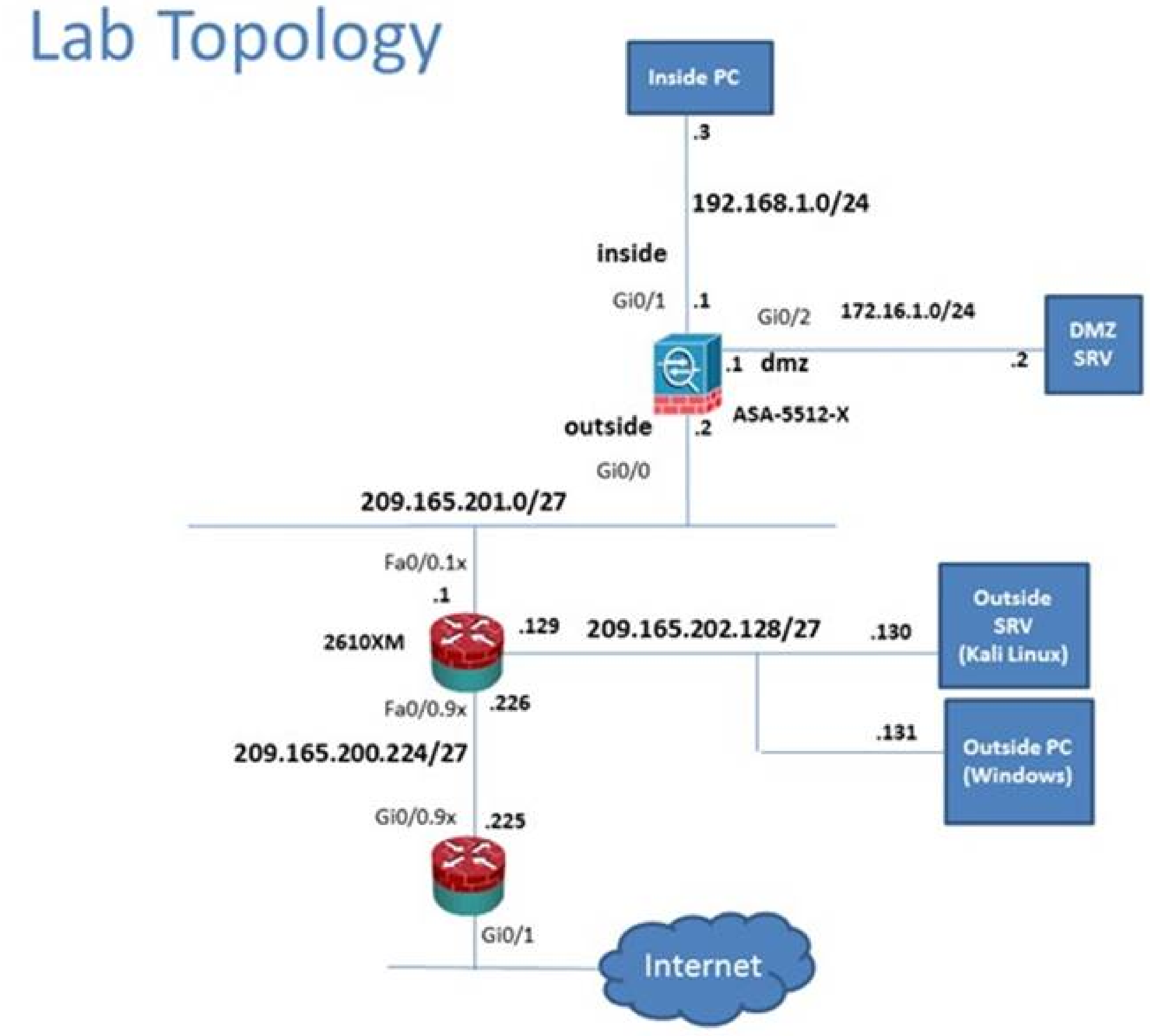
NEW QUESTION 63

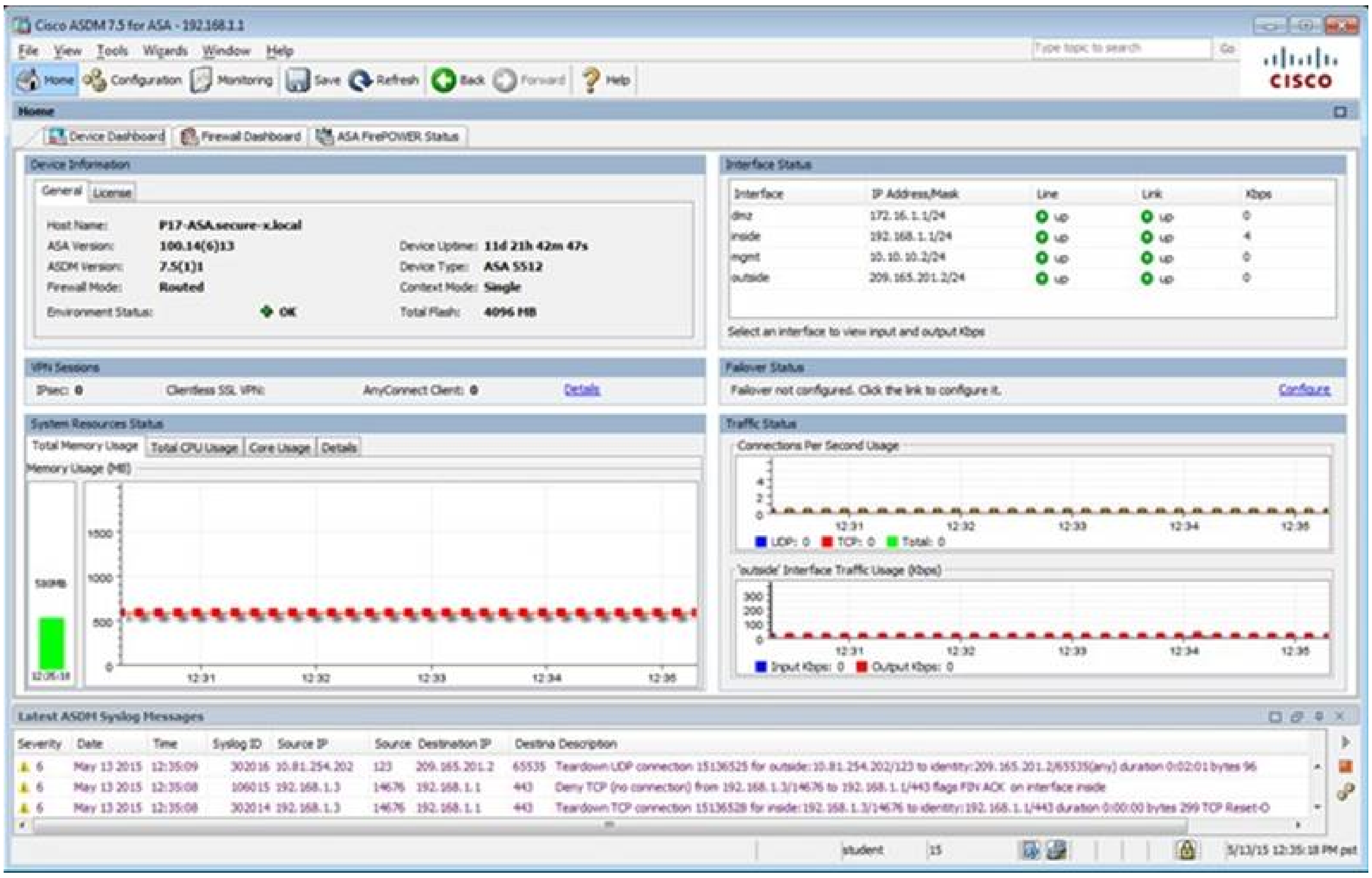
Scenario

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.





Device Information

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

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0

Failover Status

Failover not configured. Click the link to configure it.

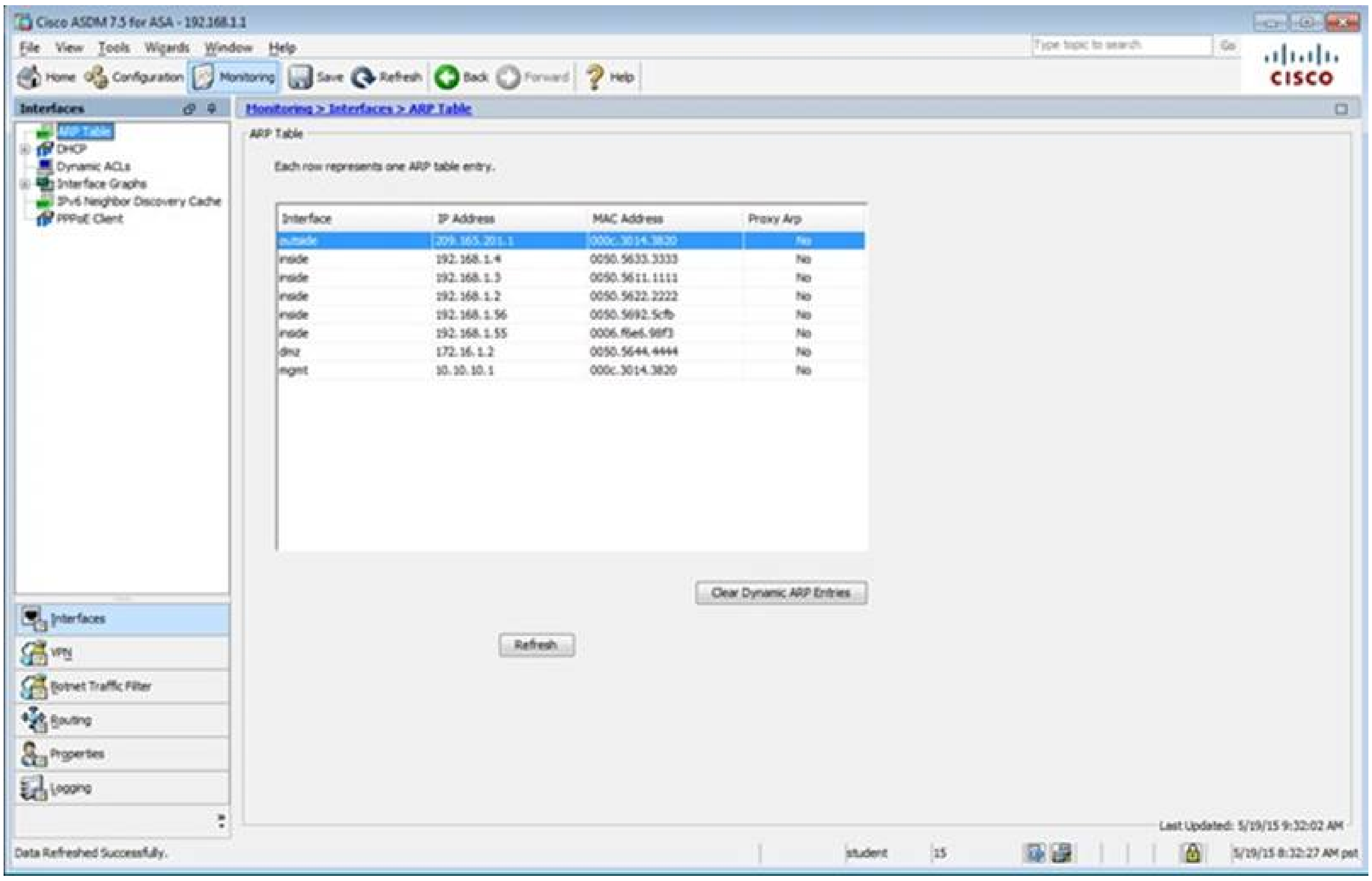
System Resources Status

Traffic Status

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 pst



Monitoring > Interfaces > ARP Table

ARP Table

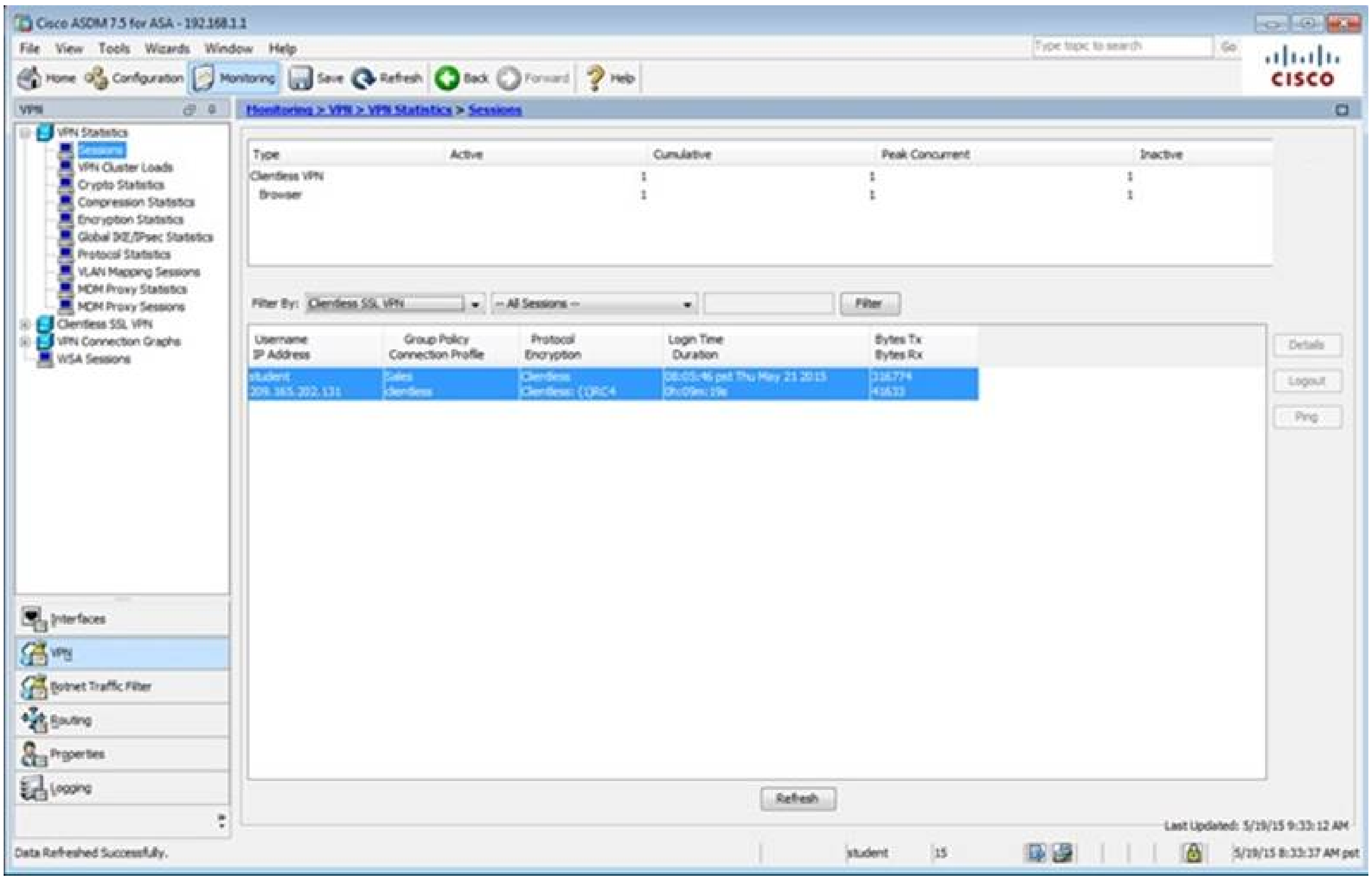
Each row represents one ARP table entry.

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

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

Data Refreshed Successfully.

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



Monitoring > VPN > VPN Statistics > Sessions

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

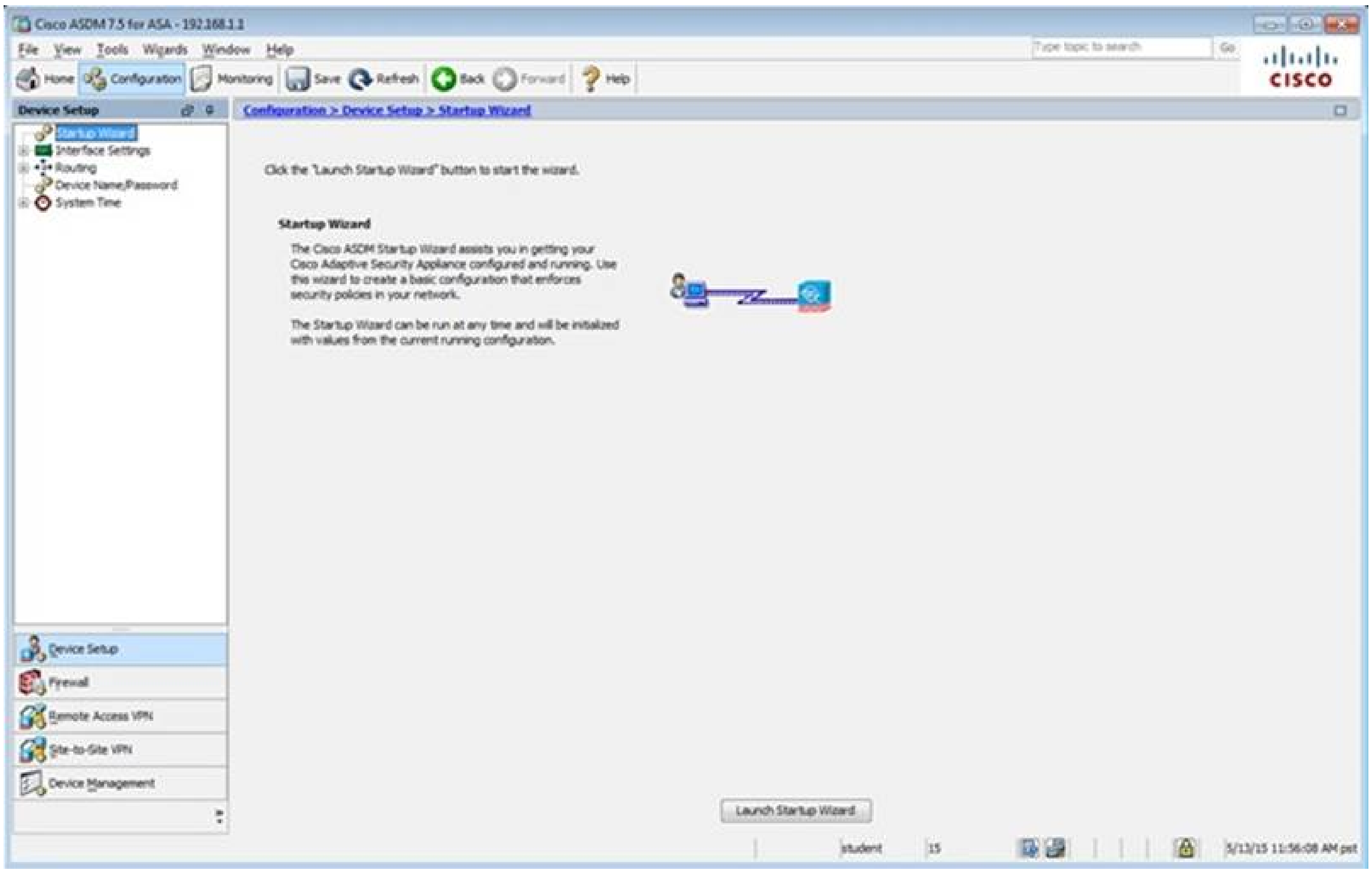
Filter By: Clientless SSL VPN | -- All Sessions -- | Filter

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

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

Data Refreshed Successfully.

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



Configuration > Device Setup > Startup Wizard

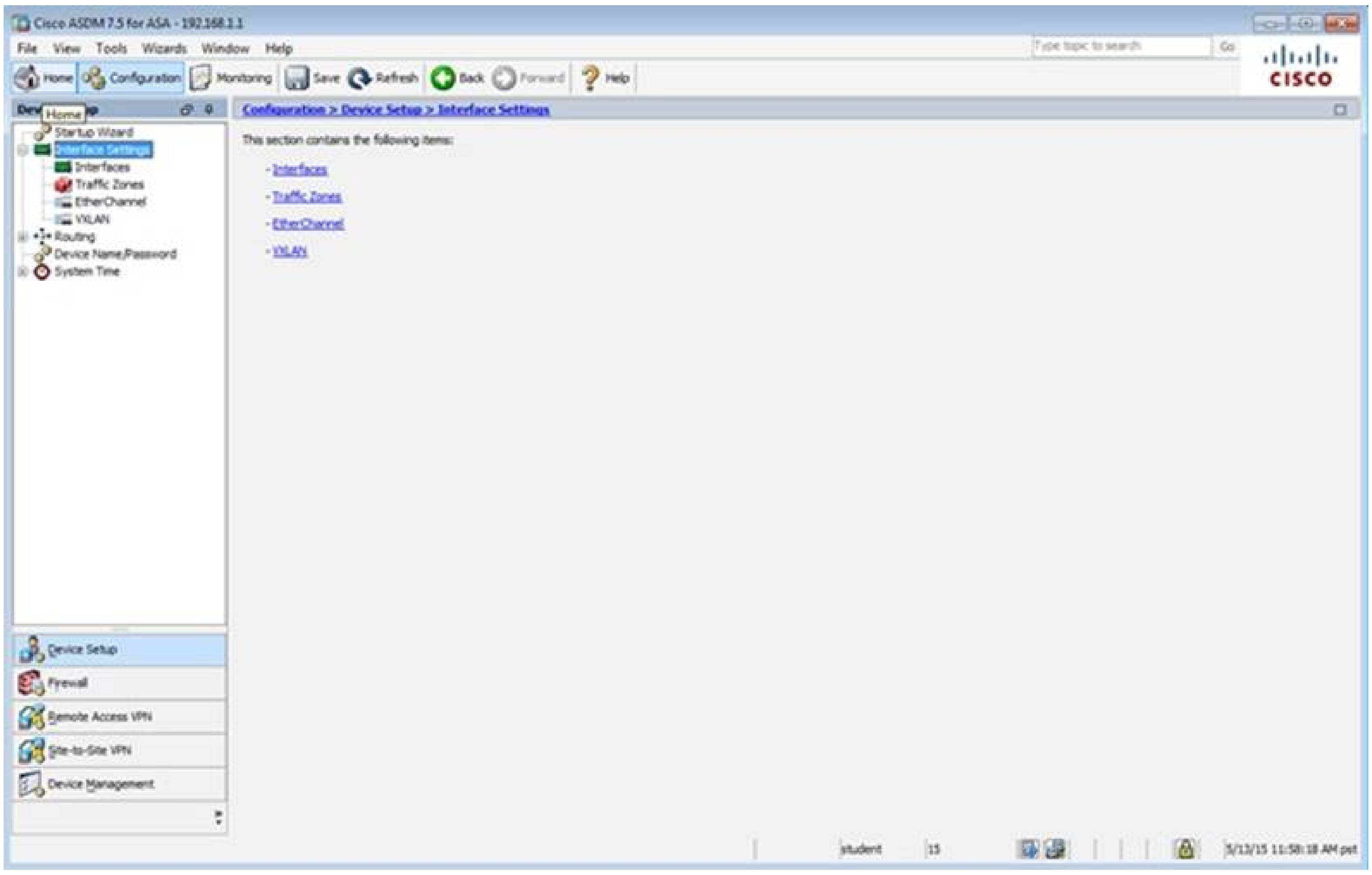
Click the "Launch Startup Wizard" button to start the wizard.

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.

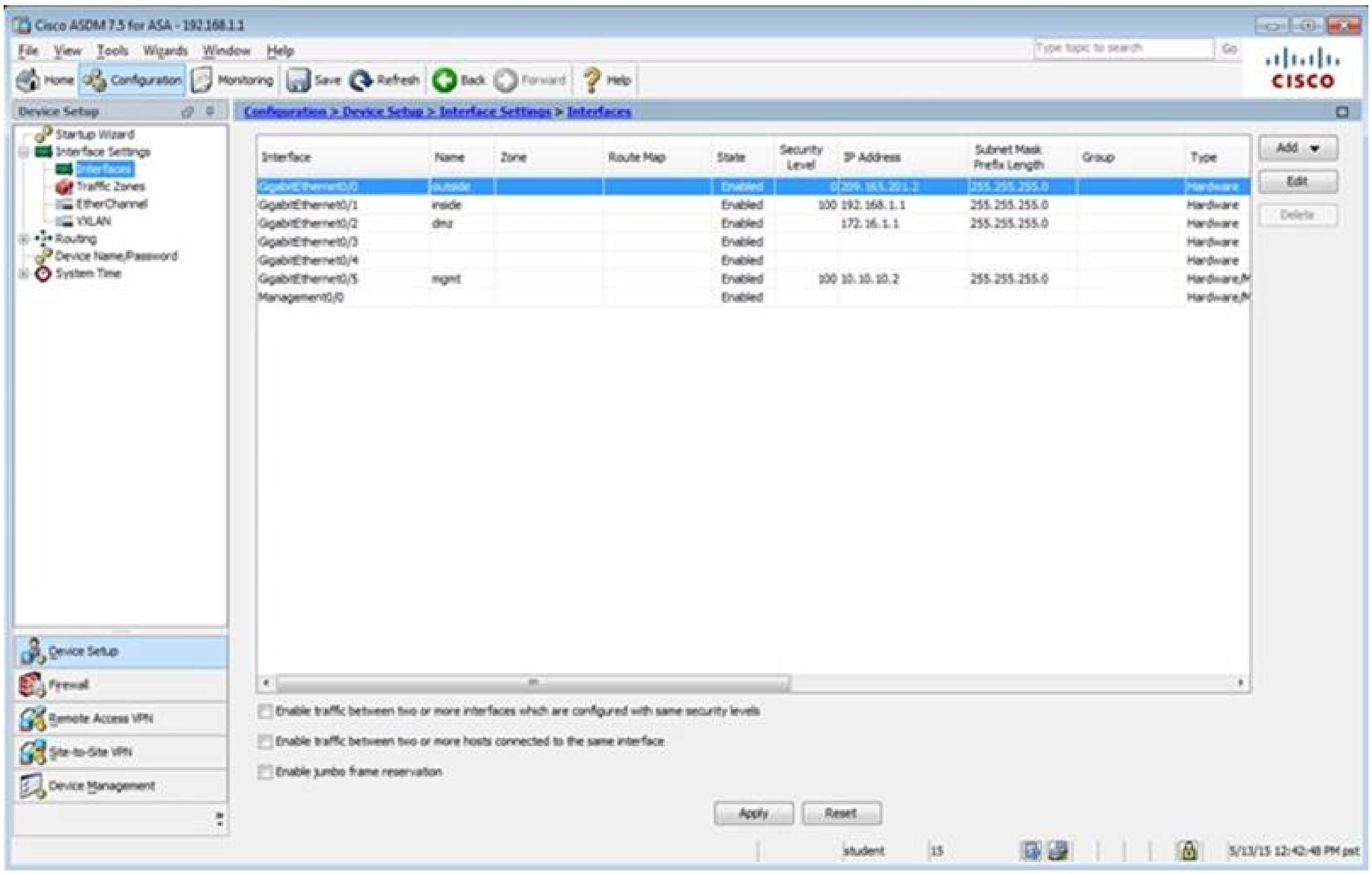
student 15 5/13/15 11:56:08 AM pdt



Configuration > Device Setup > Interface Settings

This section contains the following items:

- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN



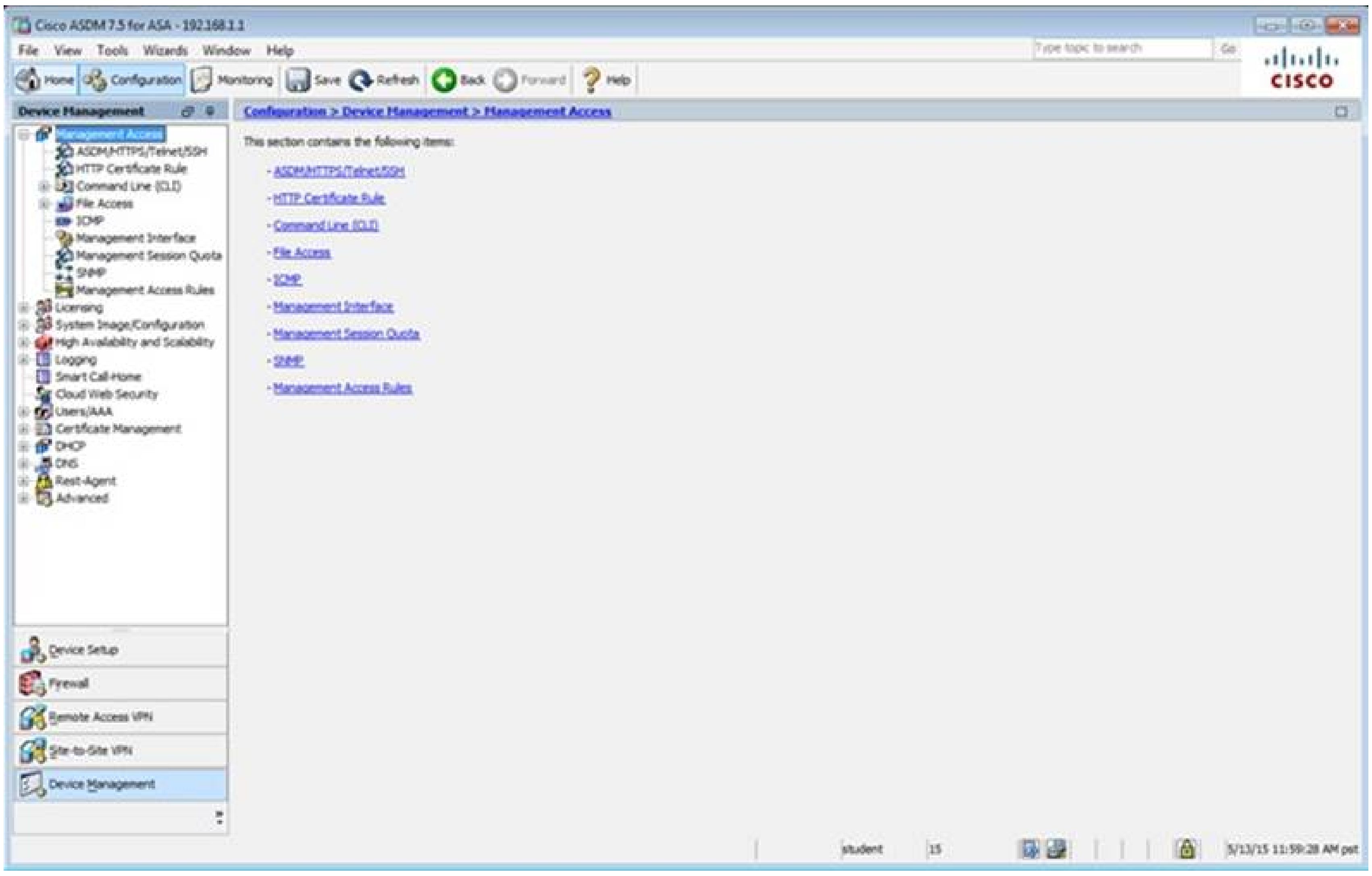
Configuration > Device Setup > Interface Settings > Interfaces

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

□ 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

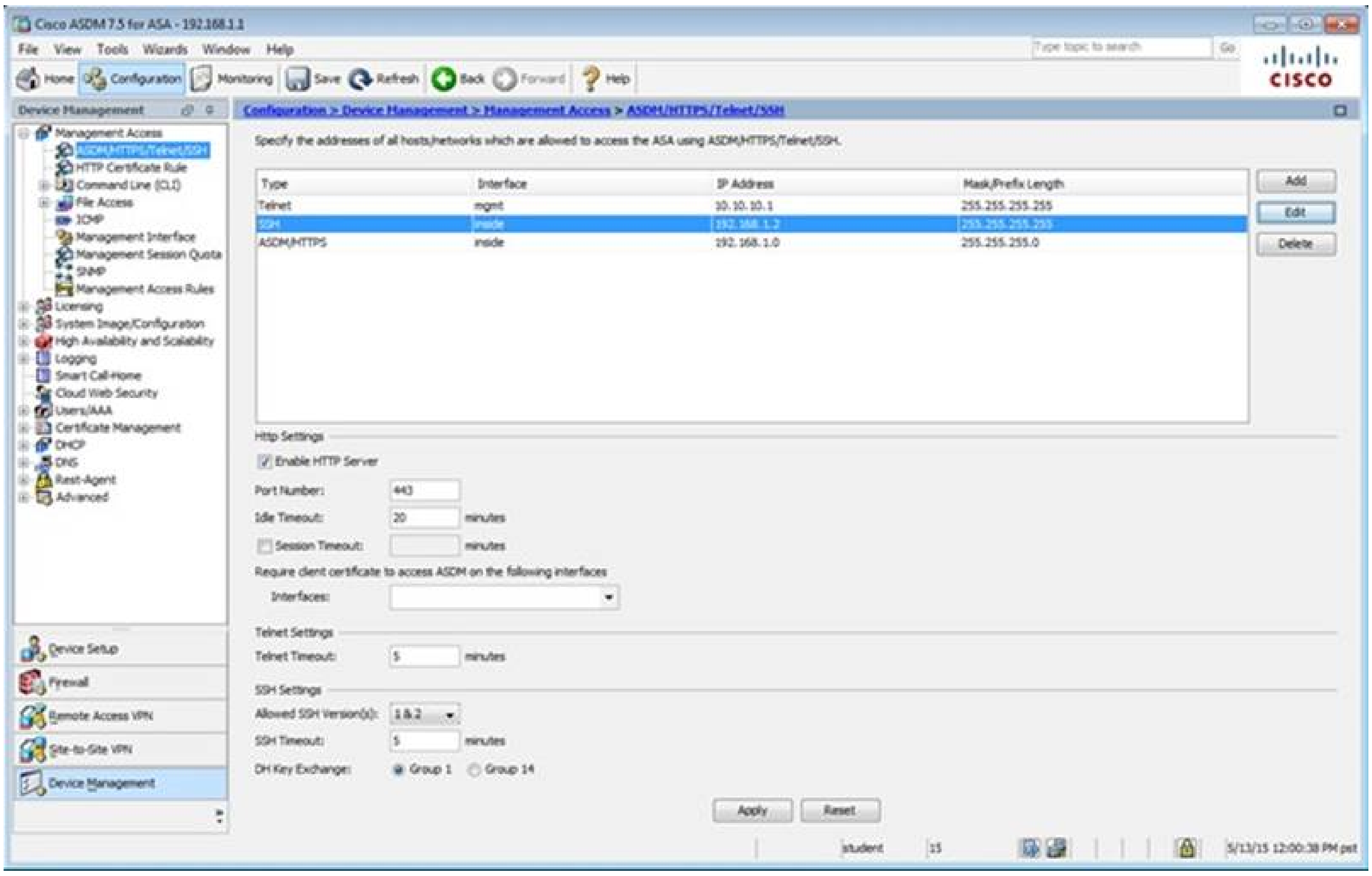
□ Enable jumbo frame reservation



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



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

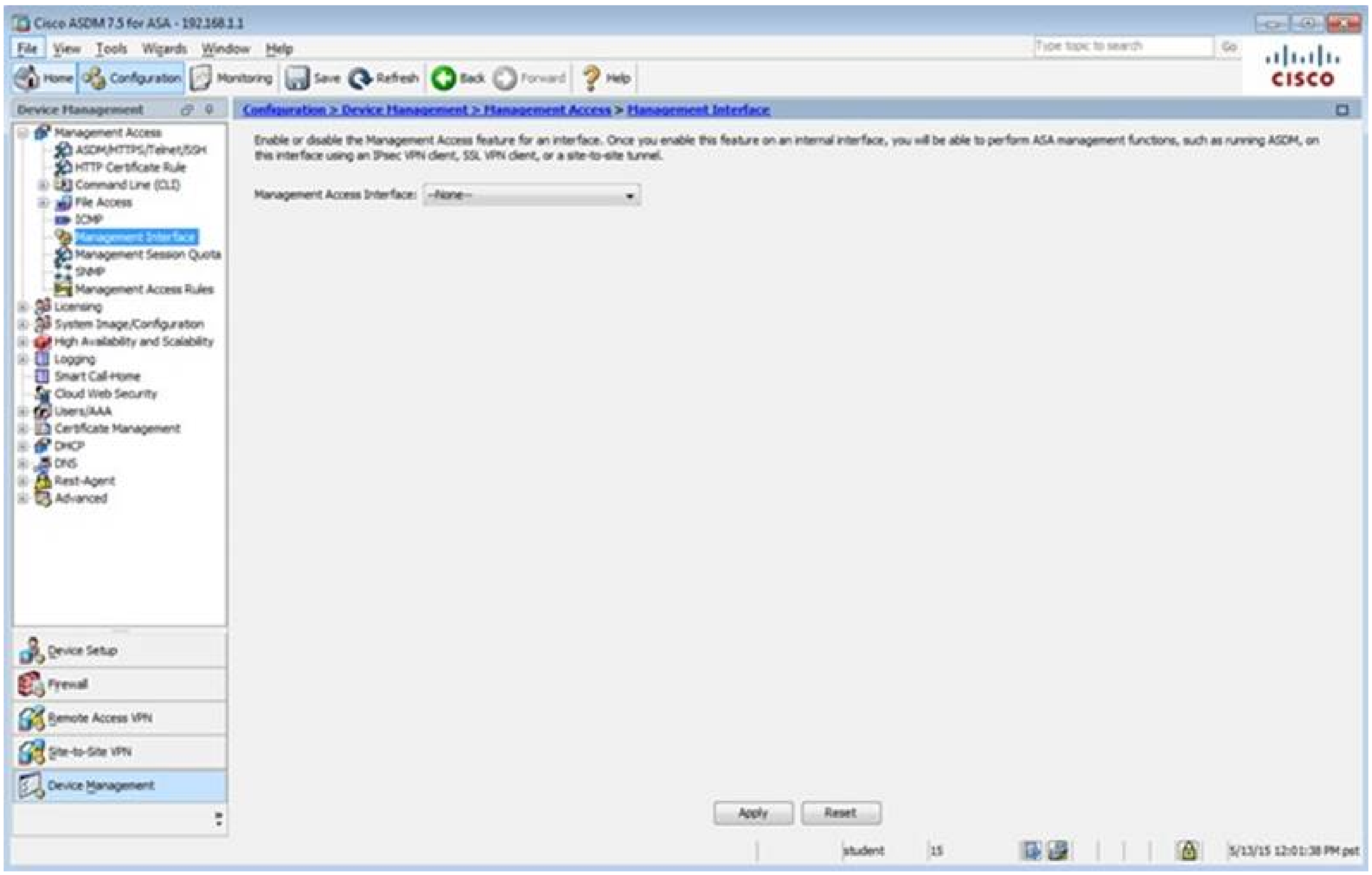
Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

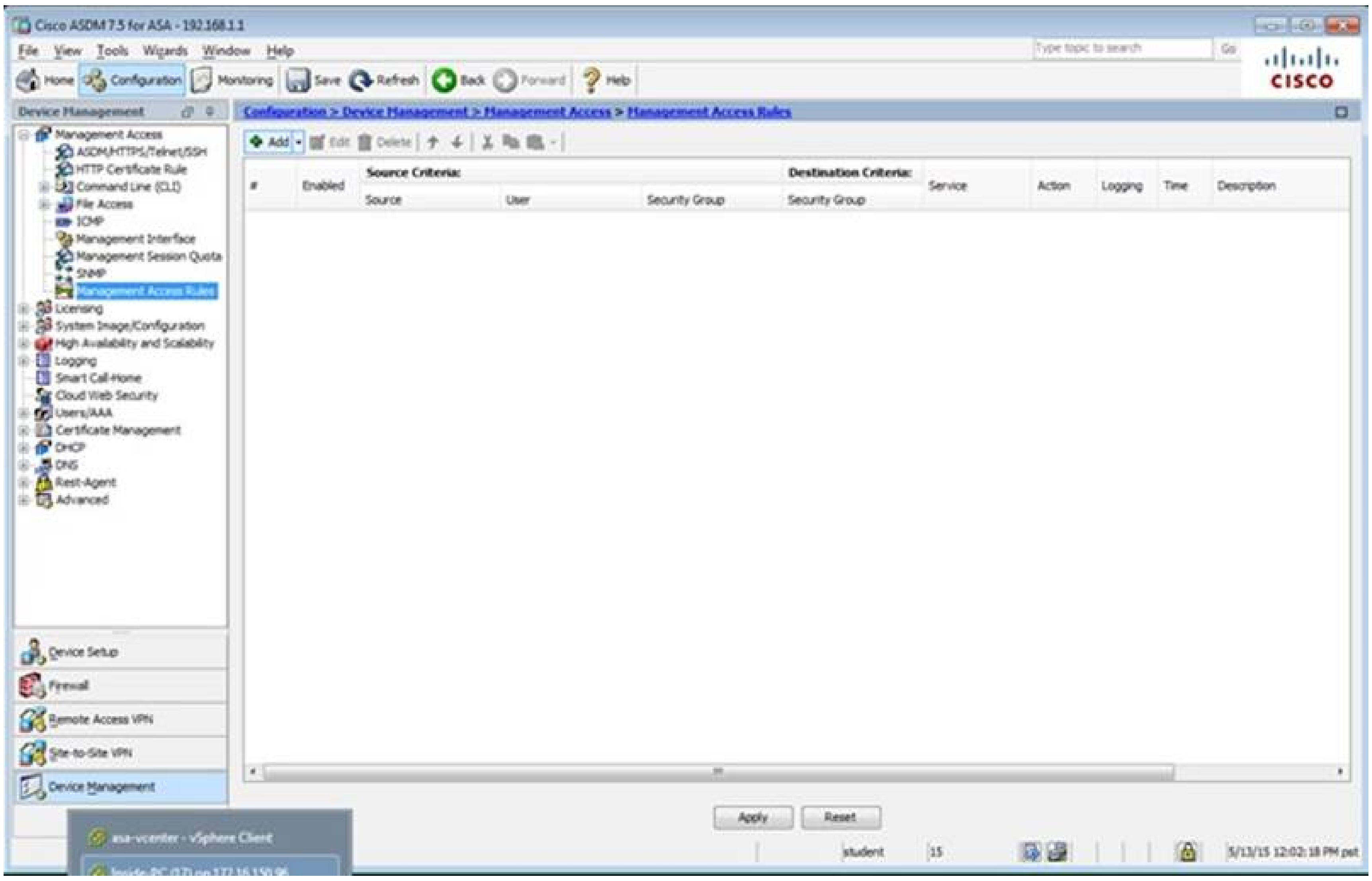
DH Key Exchange: ● Group 1 ○ Group 14



Configuration > Device Management > Management Access > Management Interface

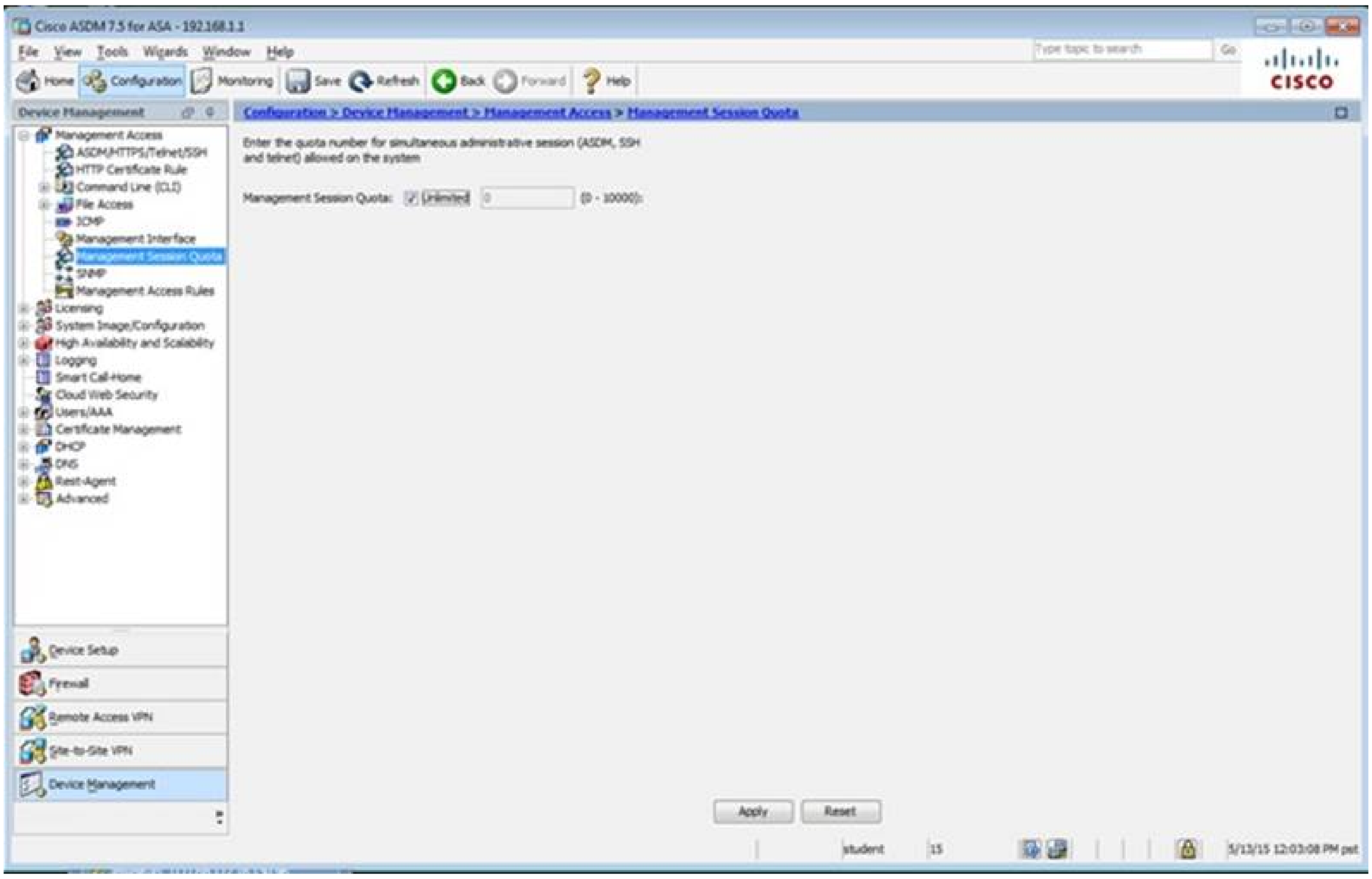
Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.

Management Access Interface: --None--



Configuration > Device Management > Management Access > Management Access Rules

#	Enabled	Source Criteria:			Destination Criteria:	Service	Action	Logging	Time	Description
		Source	User	Security Group	Security Group					

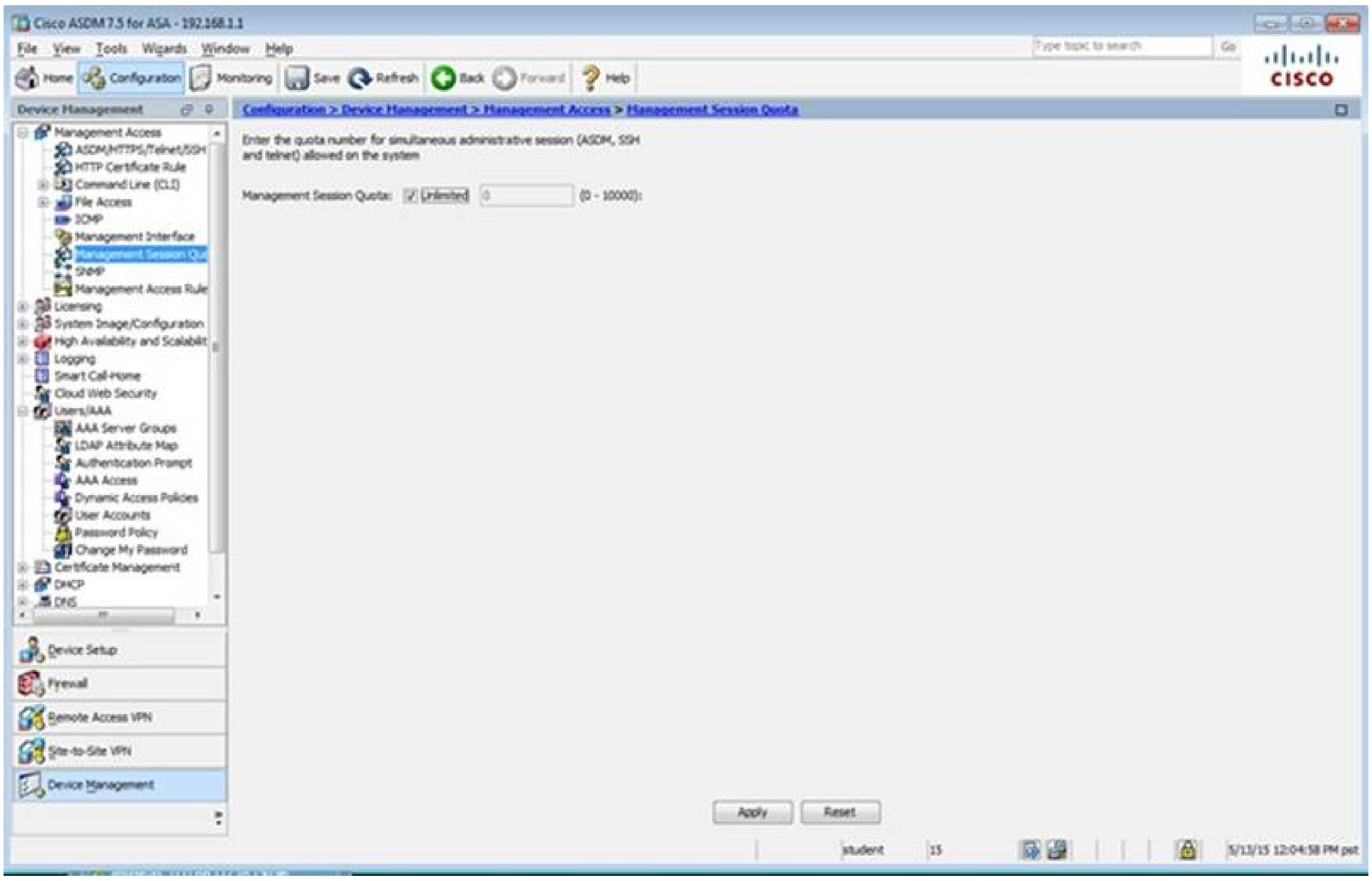


Configuration > Device Management > Management Access > Management Session Quota

Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

Management Session Quota: ☑ Unlimited 0 (0 - 10000):

student 15 5/13/15 12:03:08 PM pst

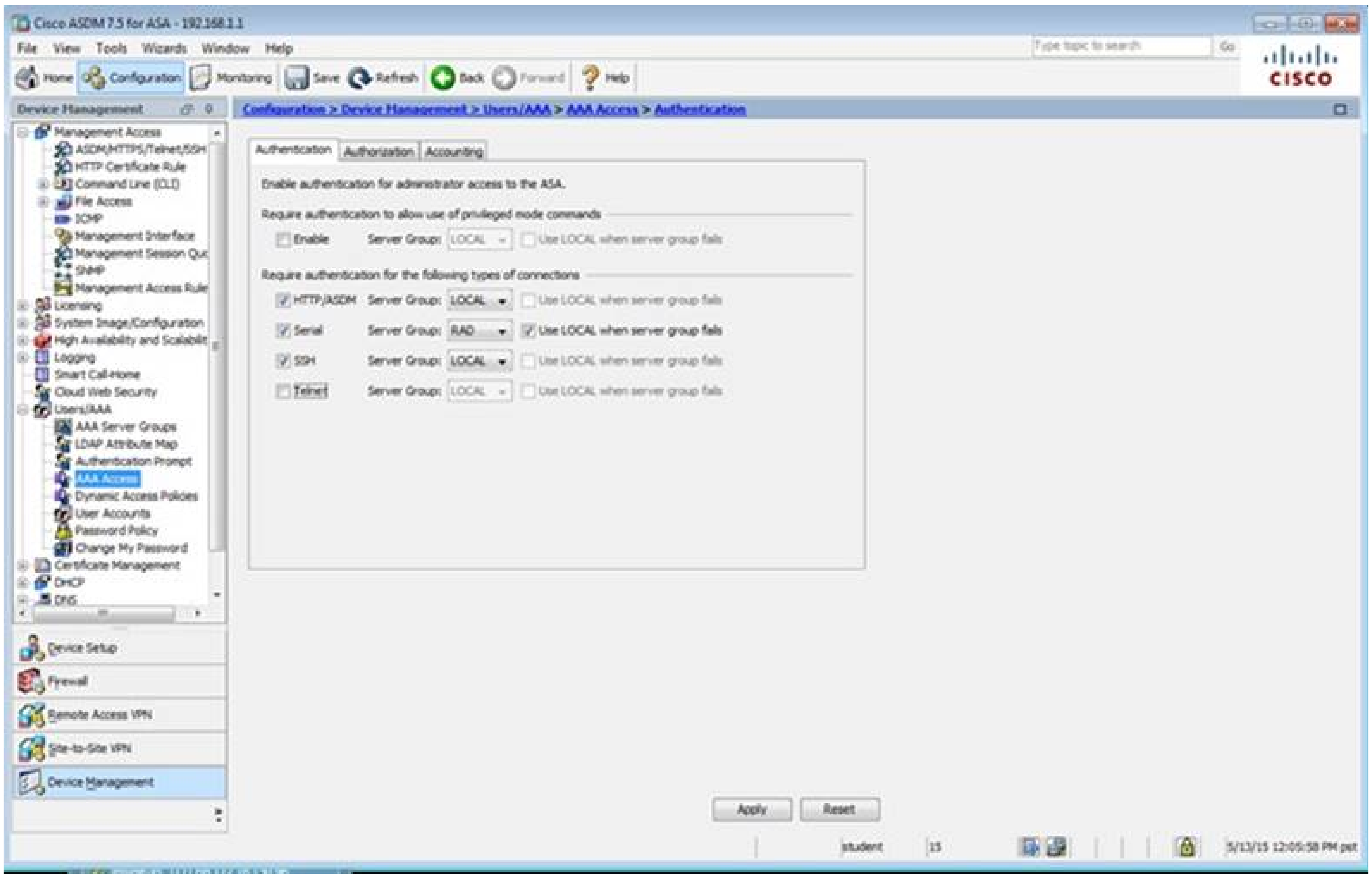


Configuration > Device Management > Management Access > Management Session Quota

Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system

Management Session Quota: ☑ Unlimited 0 (0 - 10000):

student 15 5/13/15 12:04:58 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Device Management > Users/AAA > AAA Access > Authentication

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Require authentication for the following types of connections

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

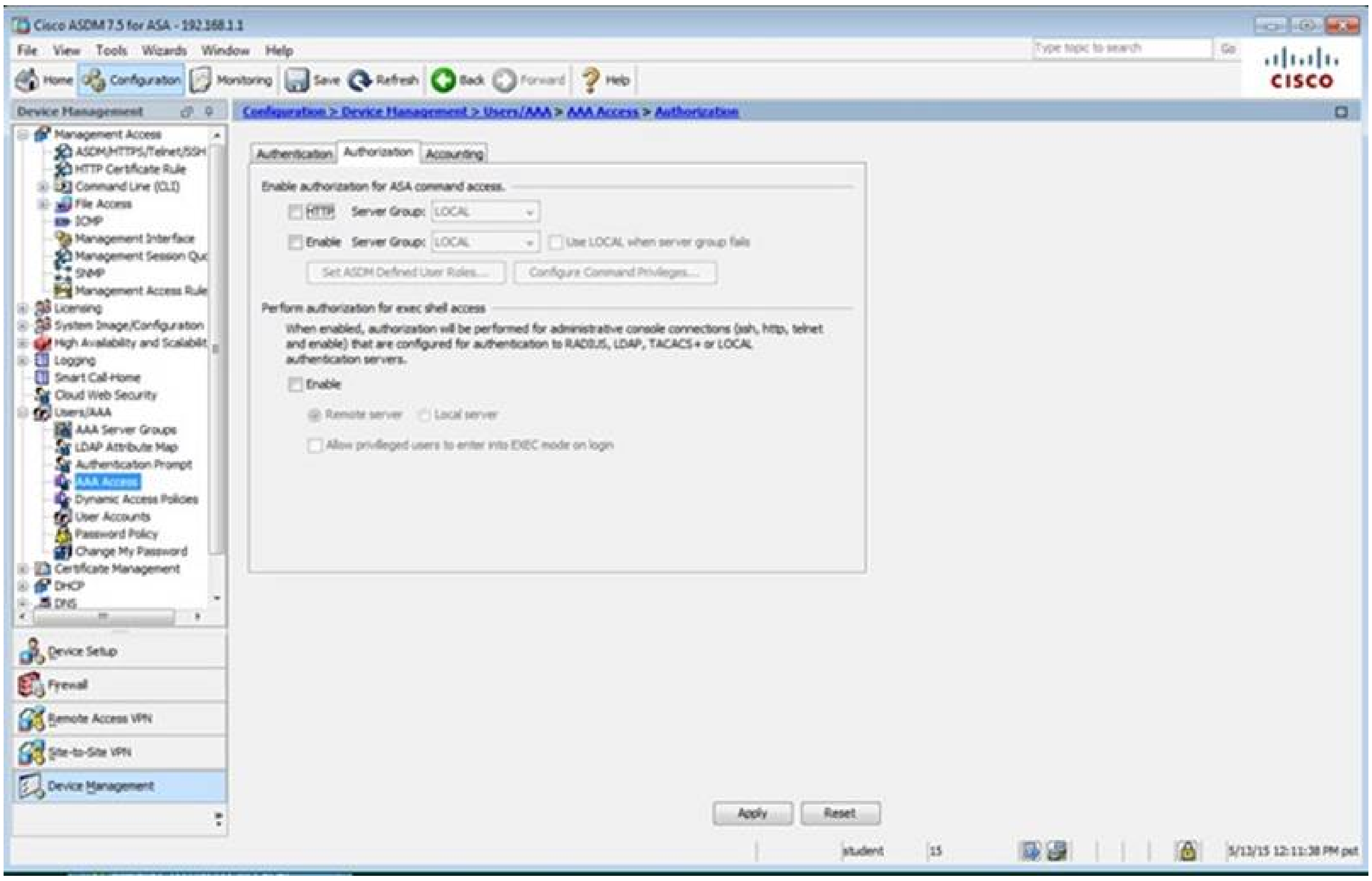
☑ Serial Server Group: RAD ☑ Use LOCAL when server group fails

☑ SSH Server Group: LOCAL □ Use LOCAL when server group fails

□ Telnet Server Group: LOCAL □ Use LOCAL when server group fails

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Device Management > Users/AAA > AAA Access > Authorization

Authentication | Authorization | Accounting

Enable authorization for ASA command access.

□ HTTP Server Group: LOCAL

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Set ASDM Defined User Roles... Configure Command Privileges...

Perform authorization for exec shell access

When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.

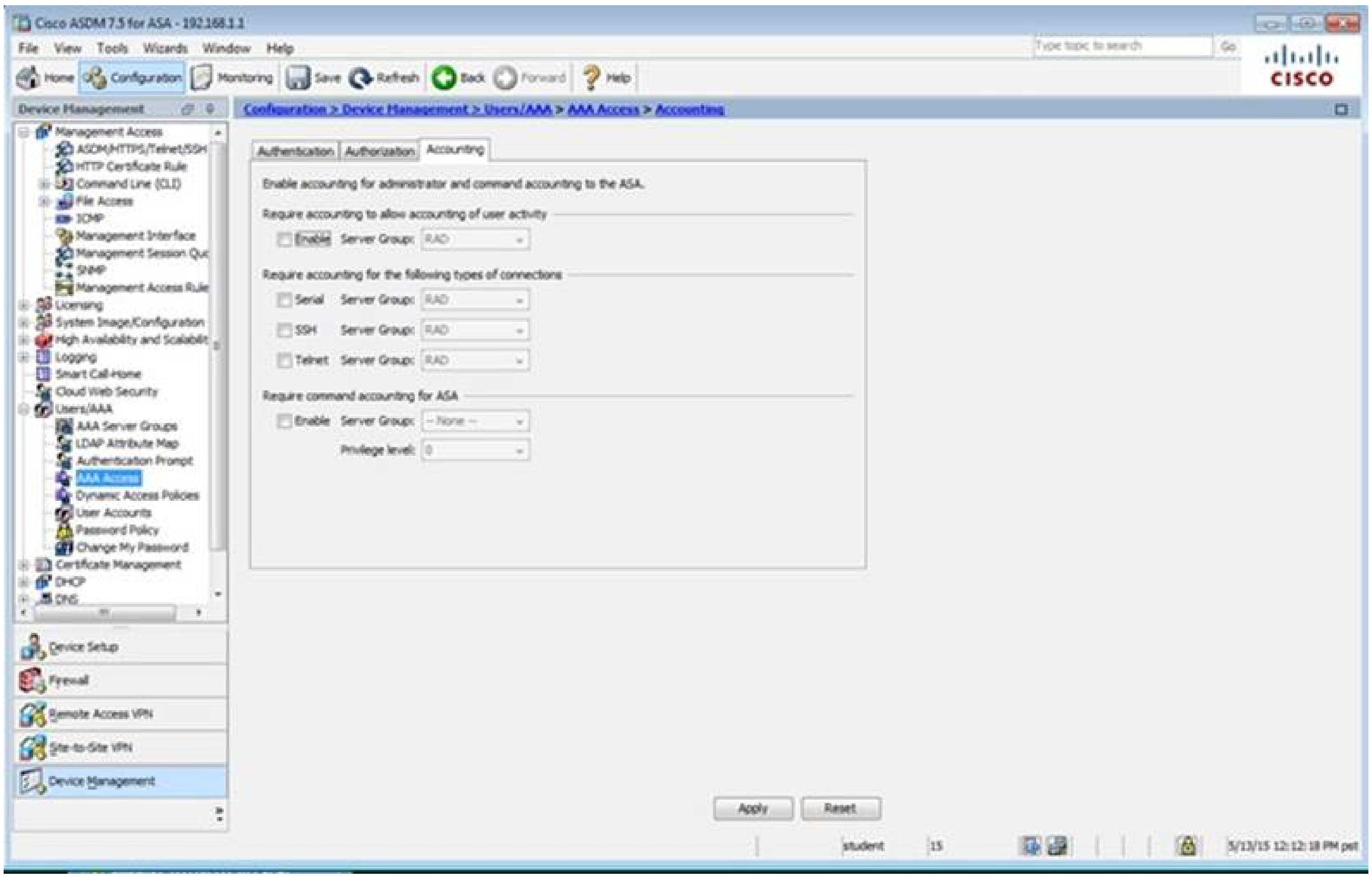
□ Enable

● Remote server ○ Local server

□ Allow privileged users to enter into EXEC mode on login

Apply Reset

student 15 5/13/15 12:11:38 PM pst



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Device Management > Users/AAA > AAA Access > Accounting

Authentication | Authorization | Accounting

Enable accounting for administrator and command accounting to the ASA.

Require accounting to allow accounting of user activity

□ Enable Server Group: RAD

Require accounting for the following types of connections

□ Serial Server Group: RAD

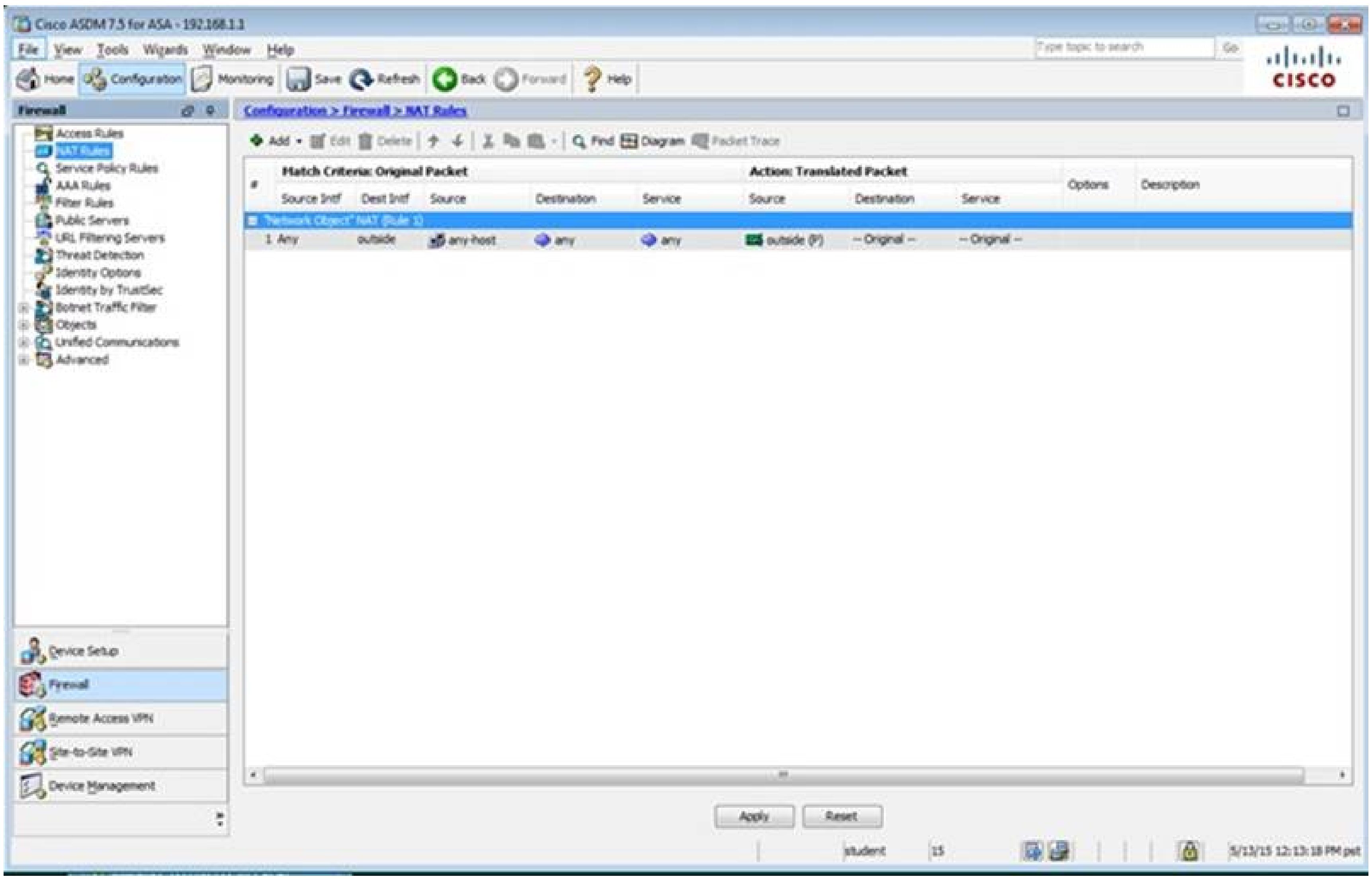
□ SSH Server Group: RAD

□ Telnet Server Group: RAD

Require command accounting for ASA

□ Enable Server Group: -- None --

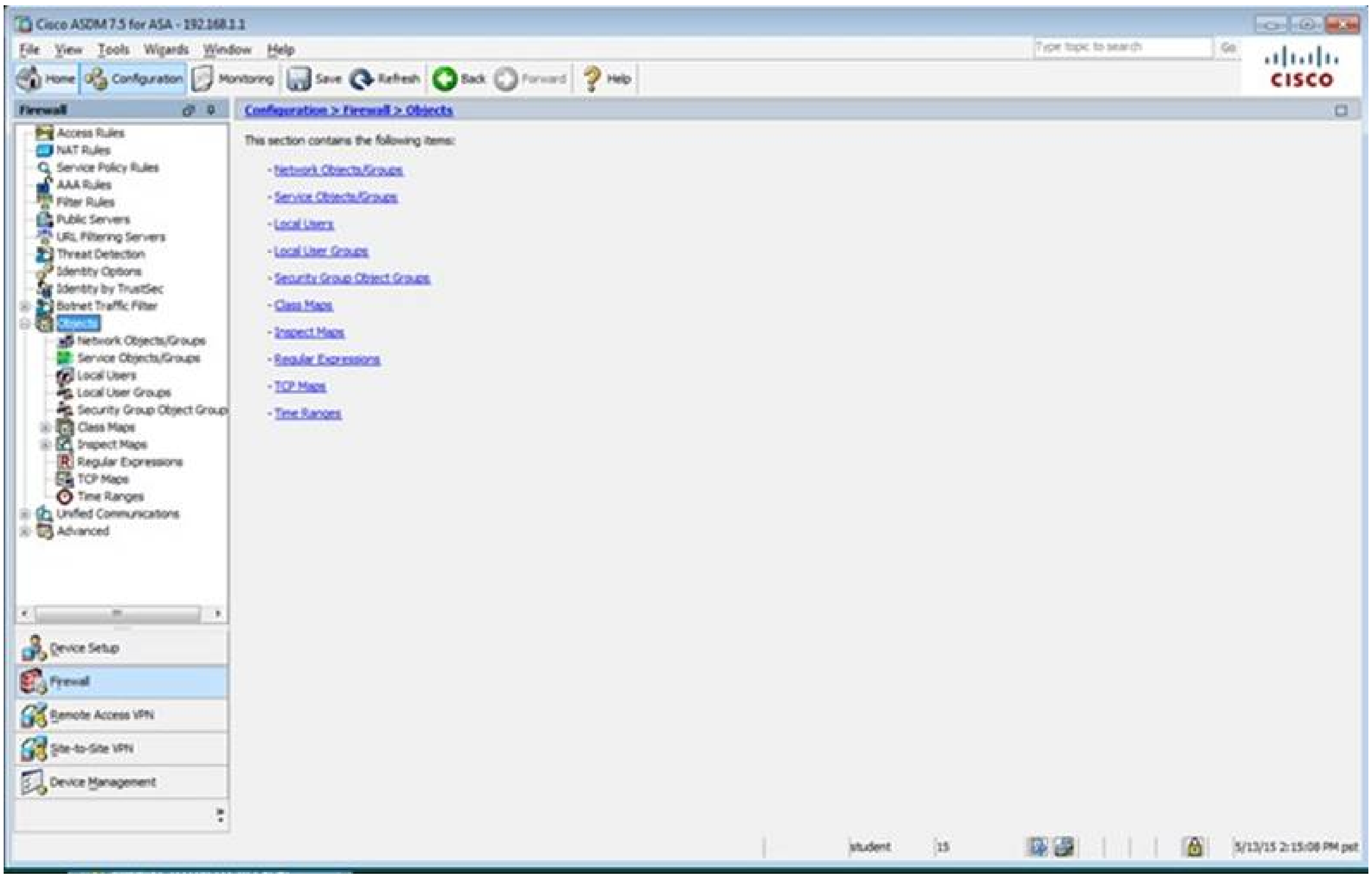
Privilege level: 0



Cisco ASDM 7.5 for ASA - 192.168.1.1

Configuration > Firewall > NAT Rules

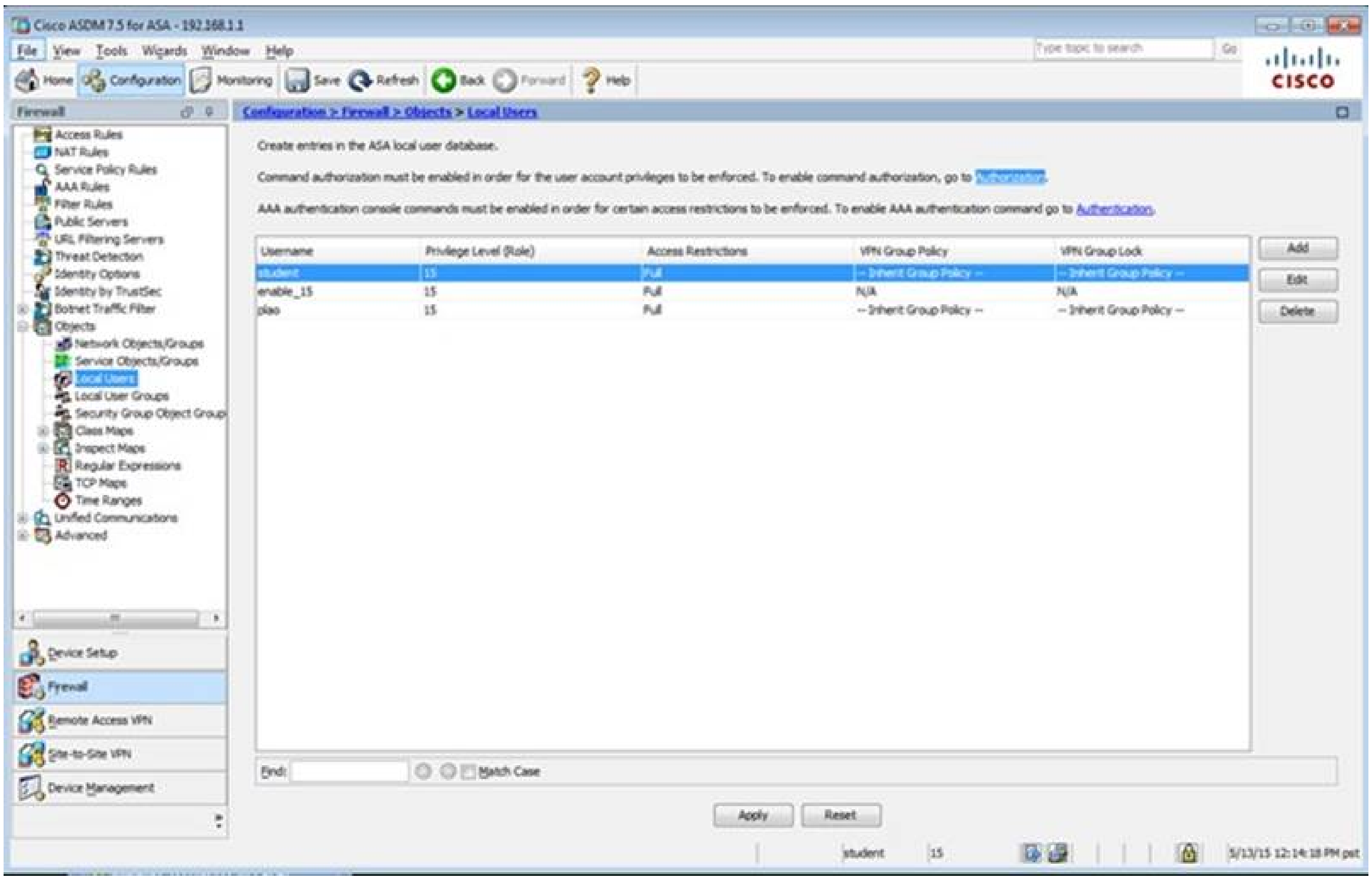
#	Match Criteria: Original Packet					Action: Translated Packet			Options	Description
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
"Network Object" NAT (Rule 1)										
1	Any	outside	any-host	any	any	outside (P)	-- Original --	-- Original --		



Configuration > Firewall > Objects

This section contains 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



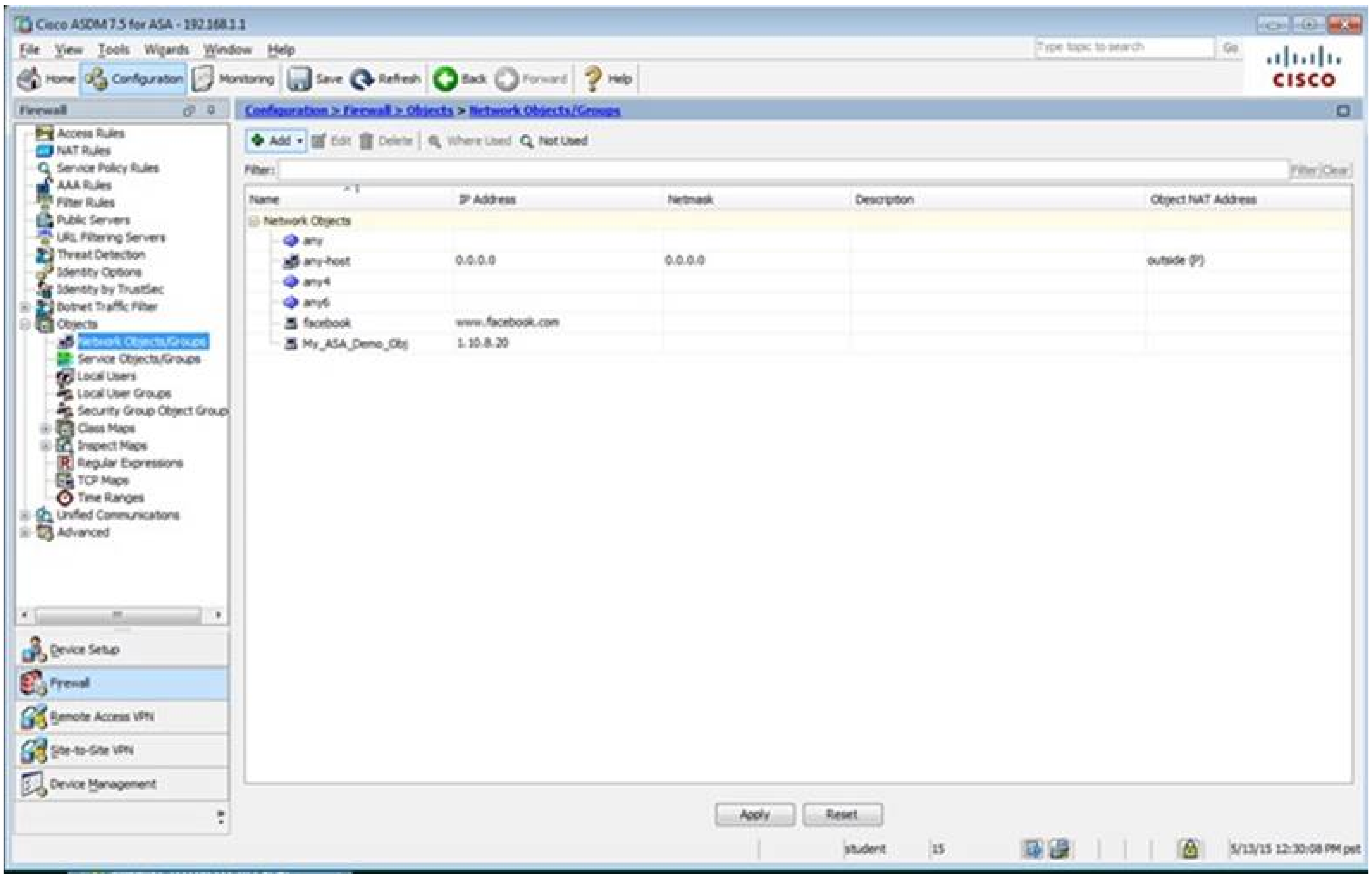
Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

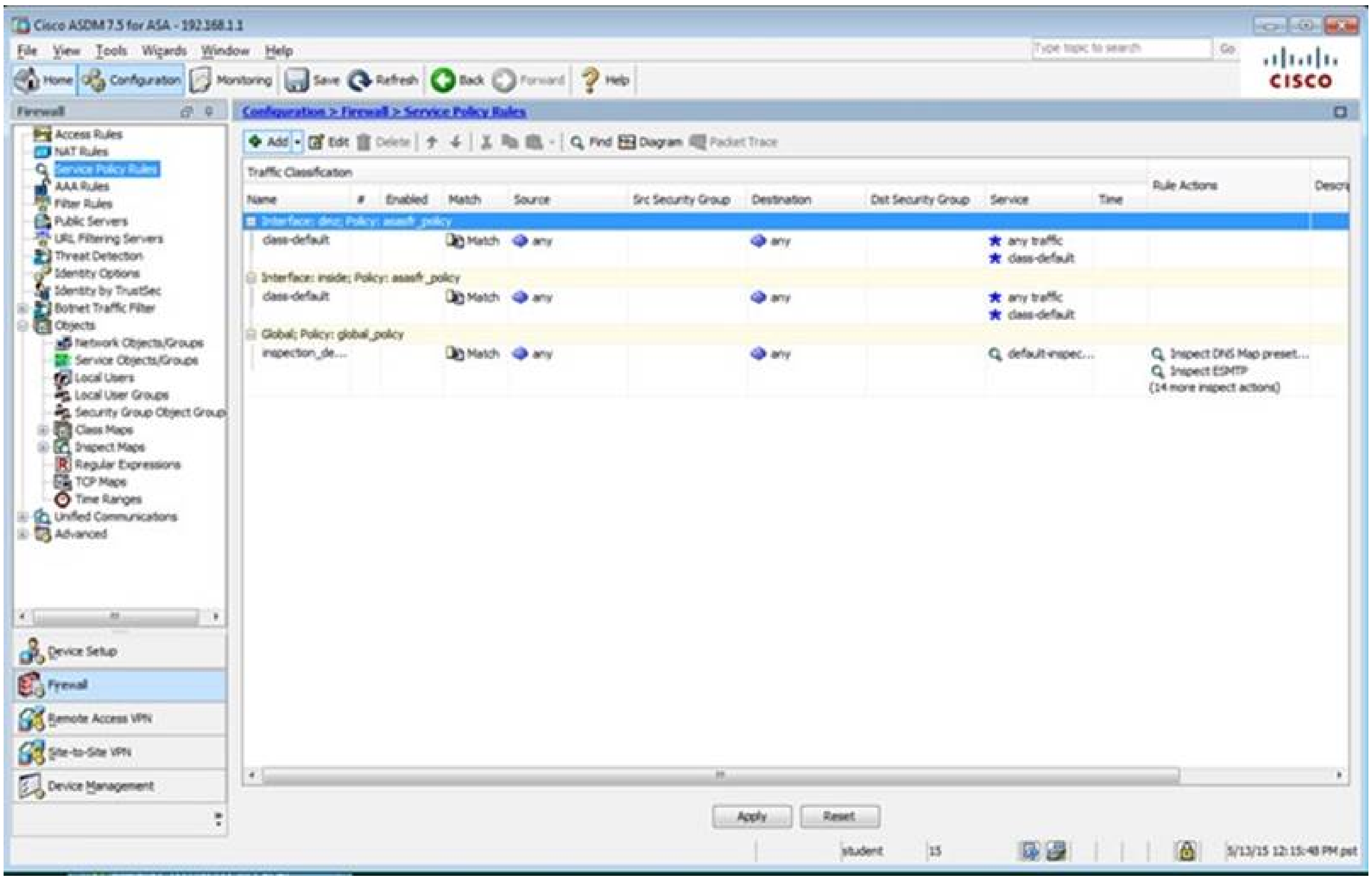
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

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



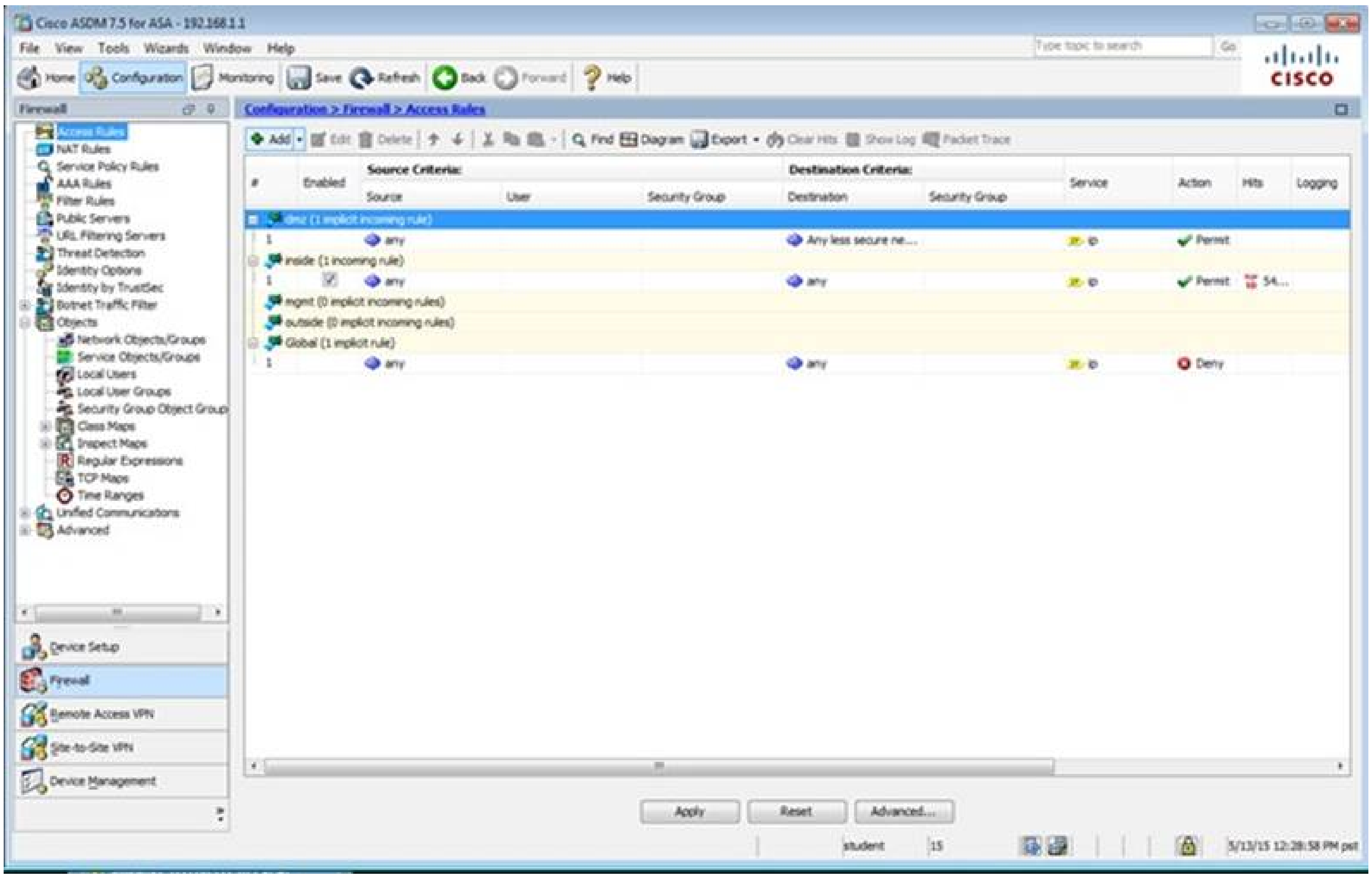
Configuration > Firewall > Objects > Network Objects/Groups

Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
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			



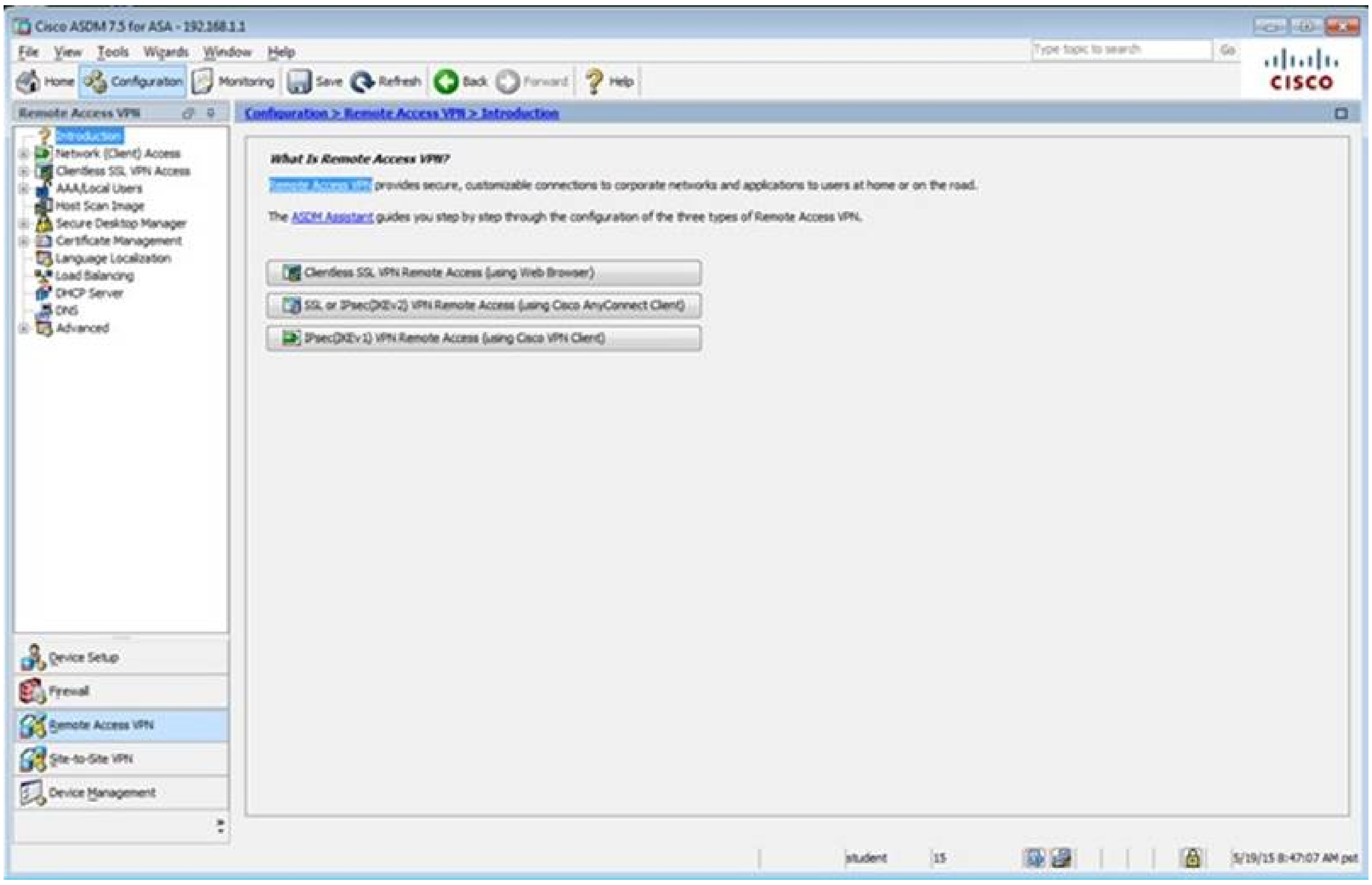
Configuration > Firewall > Service Policy Rules

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



Configuration > Firewall > Access Rules

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



Configuration > Remote Access VPN > Introduction

What Is Remote Access VPN?

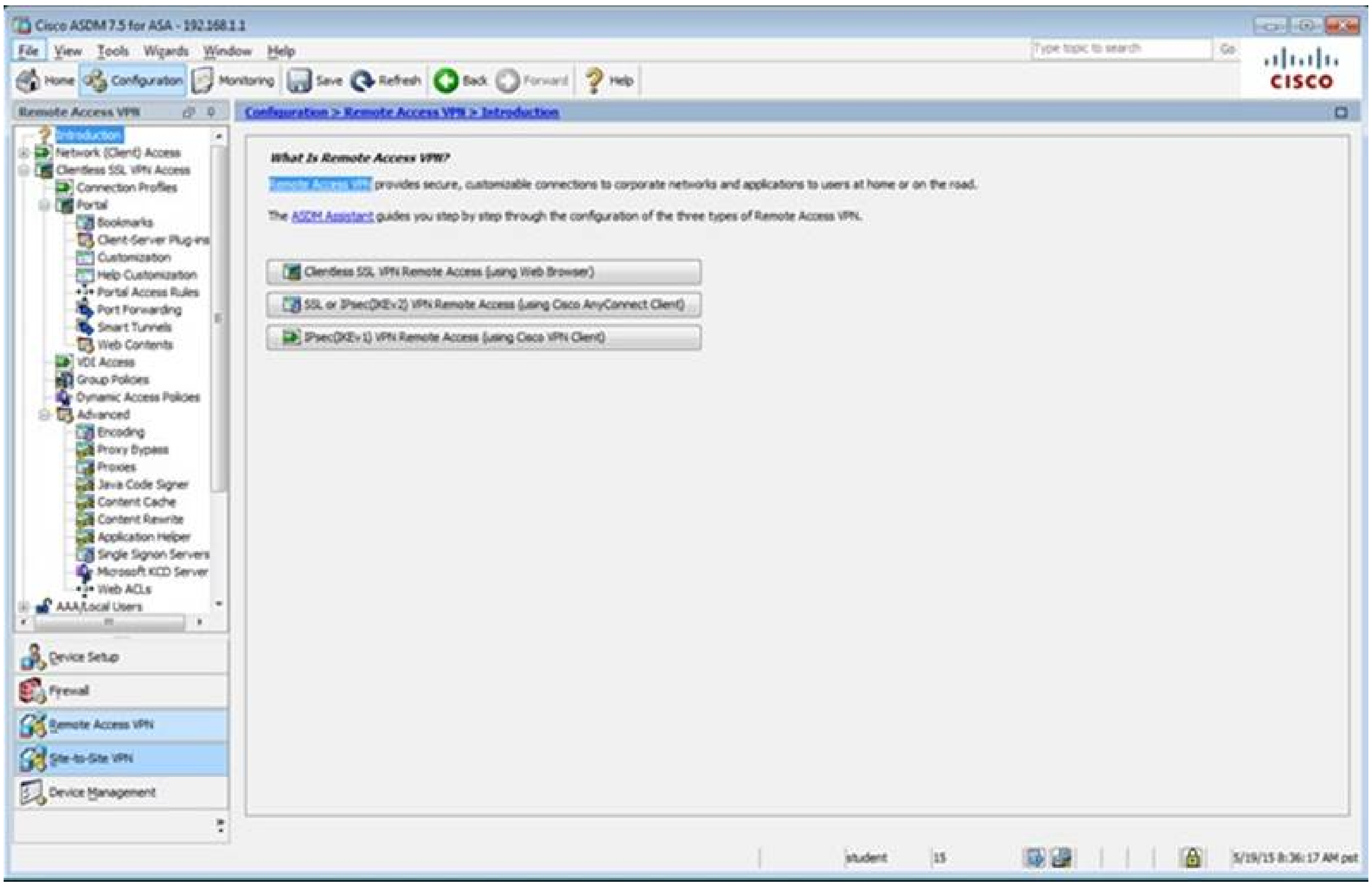
Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

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

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)



Configuration > Remote Access VPN > Introduction

What Is Remote Access VPN?

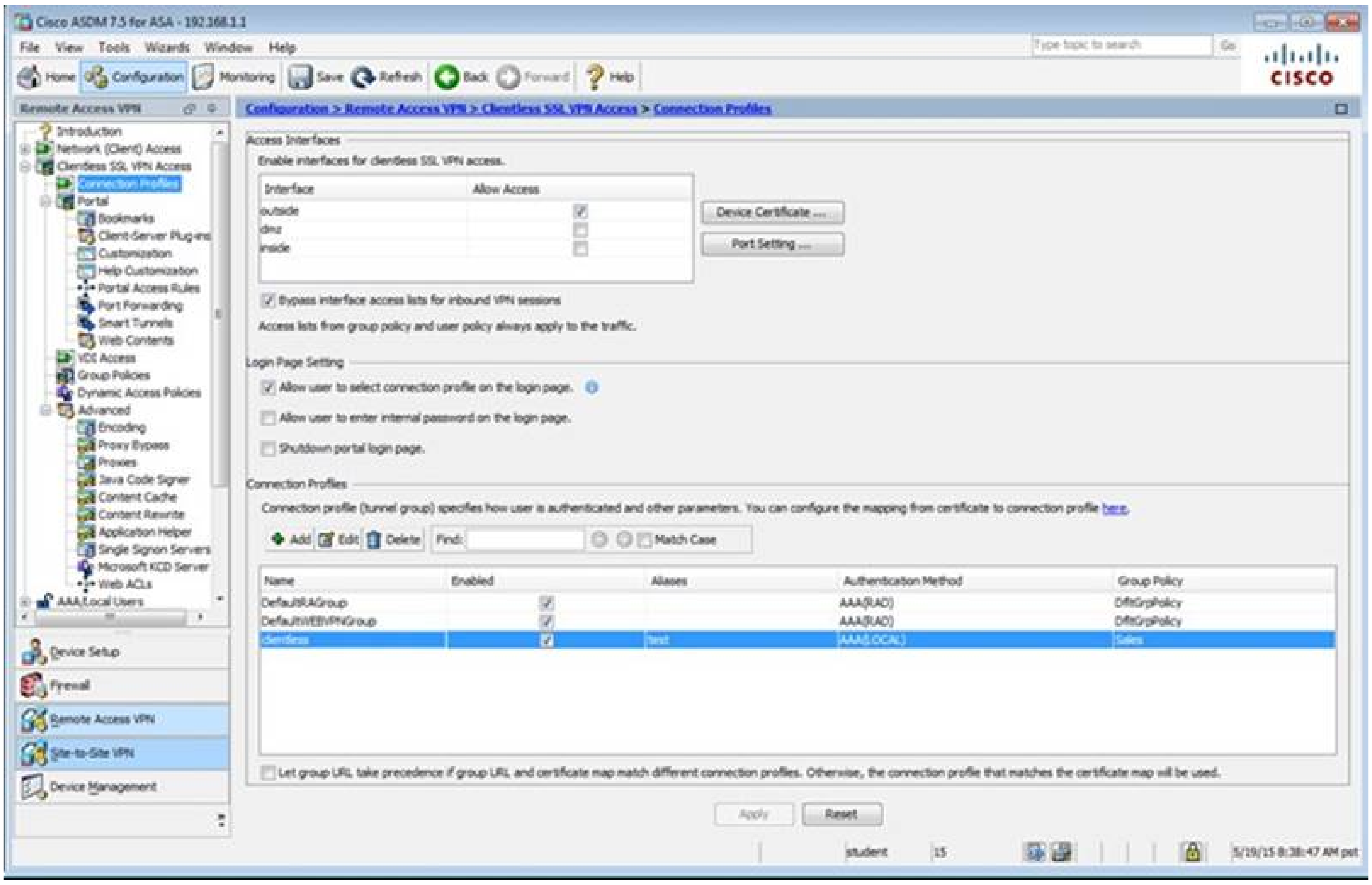
Remote Access VPN provides secure, customizable connections to corporate networks and applications to users at home or on the road.

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

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)



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	☐
inside	☐

Device Certificate ...

Port Setting ...

☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

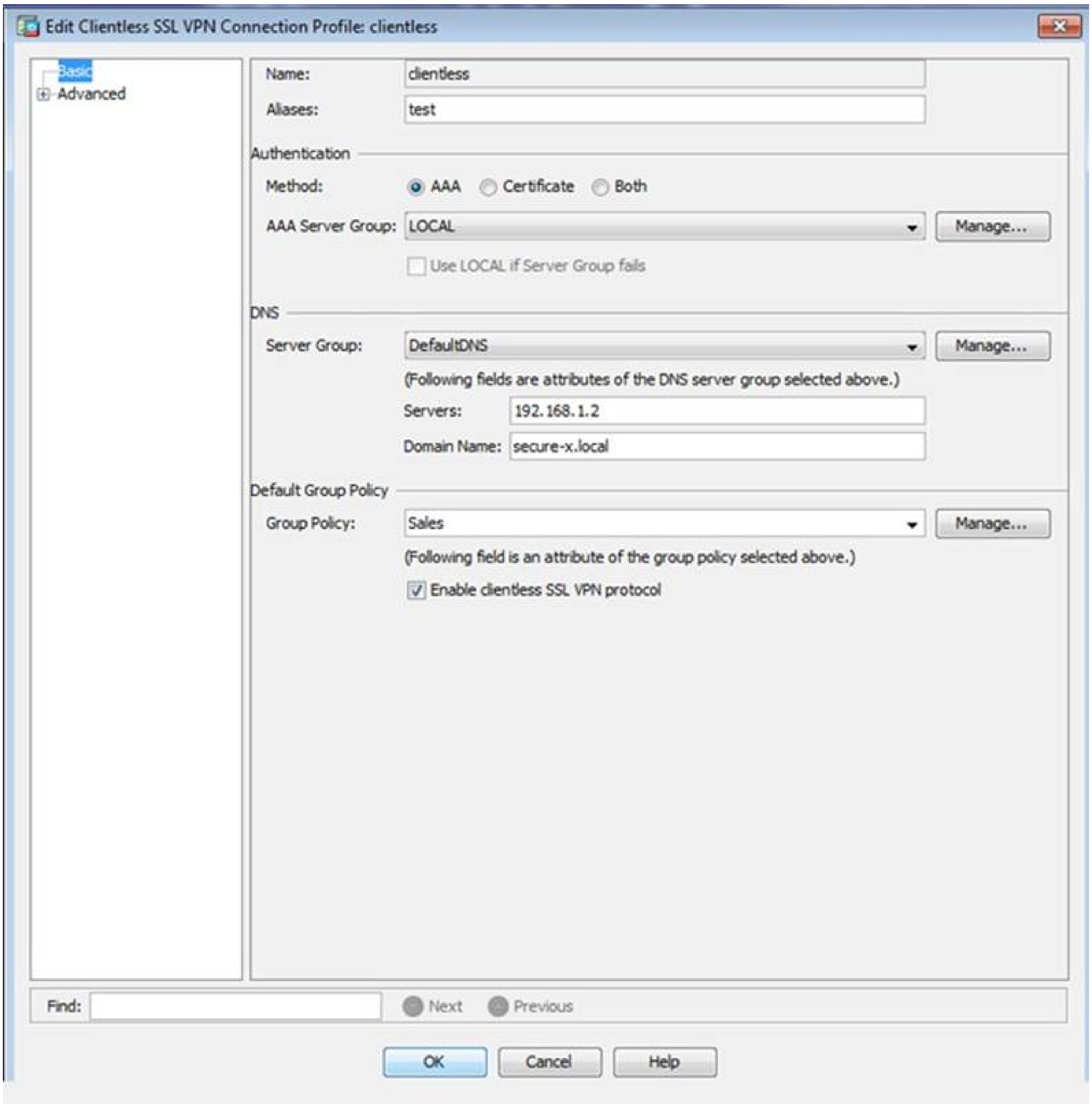
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: ☐ Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(RAD)	DfltGrpPolicy
clientless	☑	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



Edit Clientless SSL VPN Connection Profile: clientless

Name: clientless

Aliases: test

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

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

Servers: 192.168.1.2

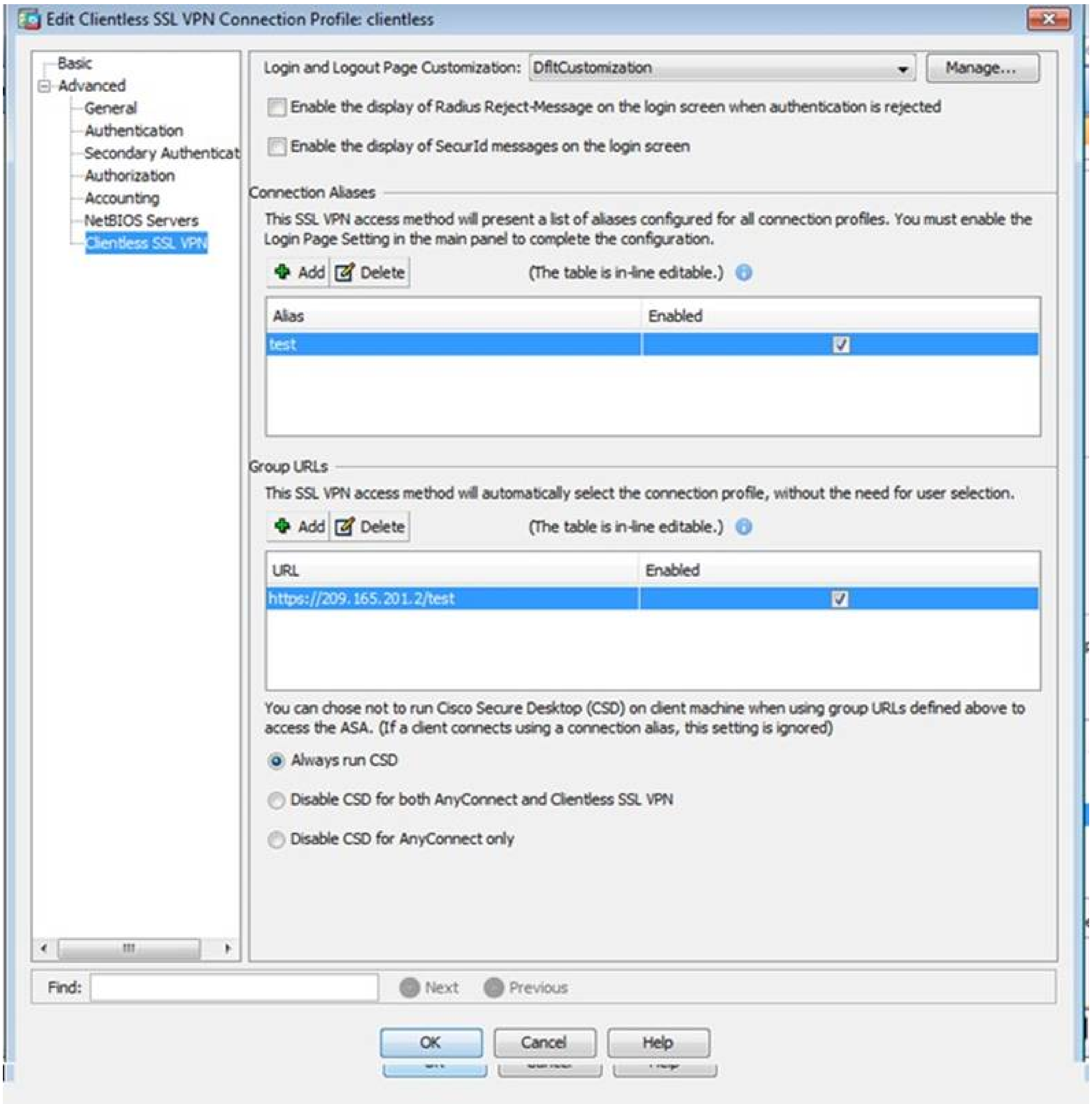
Domain Name: secure-x.local

Default Group Policy

Group Policy: Sales

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

☑ Enable clientless SSL VPN protocol



Edit Clientless SSL VPN Connection Profile: clientless

Login and Logout Page Customization: DfltCustomization

□ 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.

(The table is in-line editable.)

Alias	Enabled
test	☑

Group URLs

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

(The table is in-line editable.)

URL	Enabled
https://209.165.201.2/test	☑

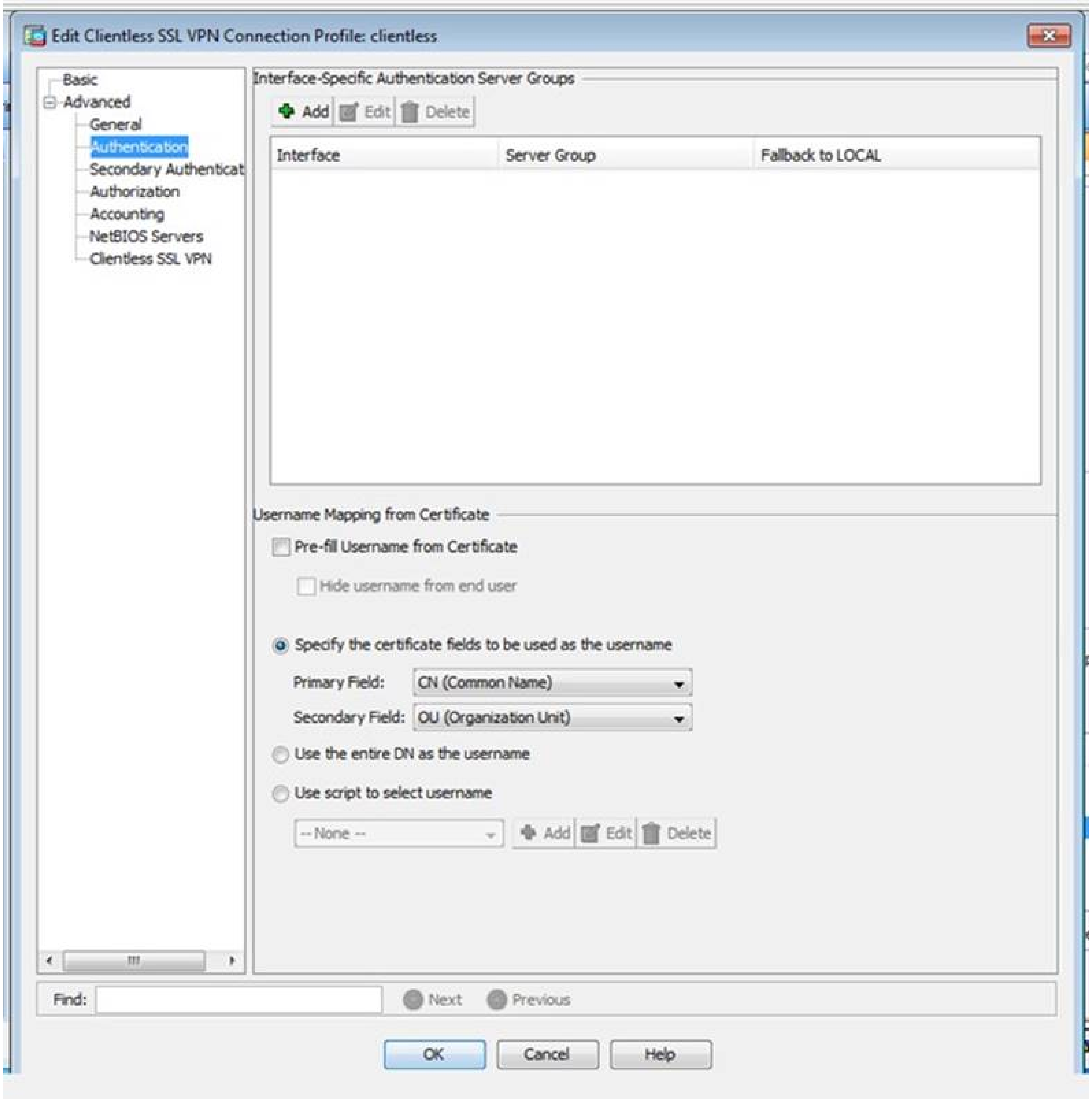
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)

● Always run CSD

○ Disable CSD for both AnyConnect and Clientless SSL VPN

○ Disable CSD for AnyConnect only

Find:



Edit Clientless SSL VPN Connection Profile: clientless

Username Mapping from Certificate

□ Pre-fill Username from Certificate

□ Hide username from end user

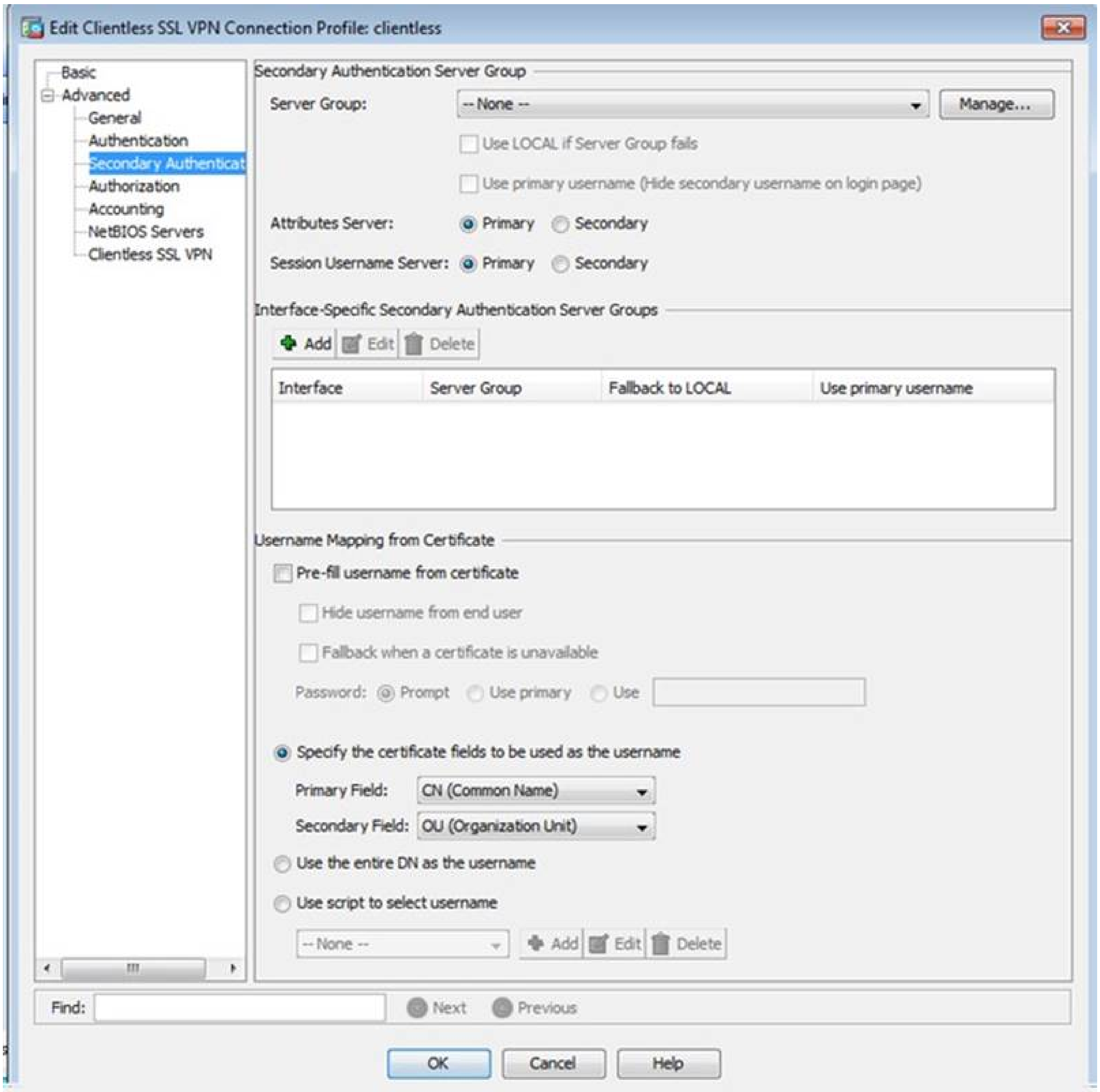
● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username



Edit Clientless SSL VPN Connection Profile: clientless

Secondary Authentication Server Group

Server Group: -- None --

□ 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

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

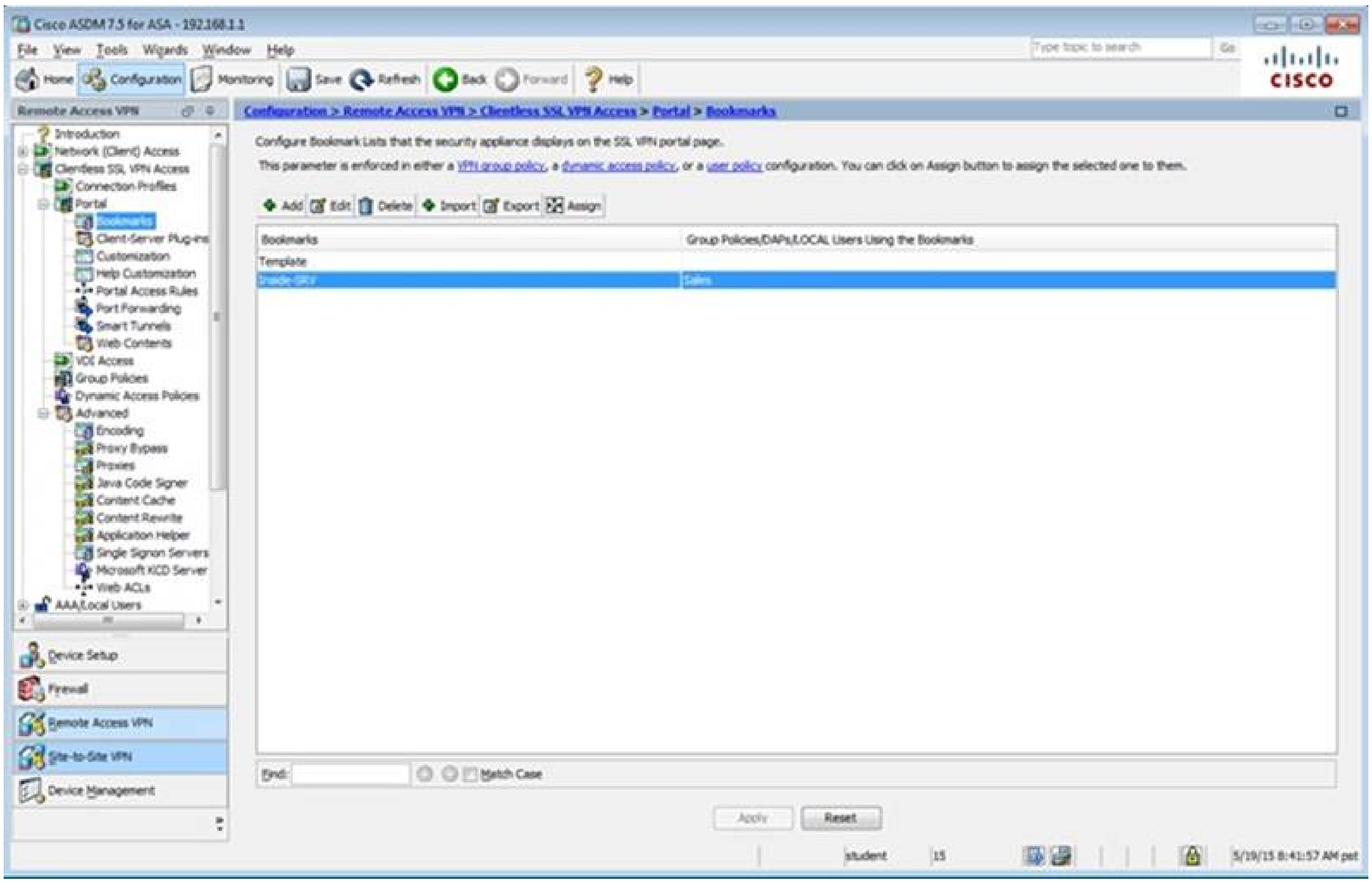
Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --



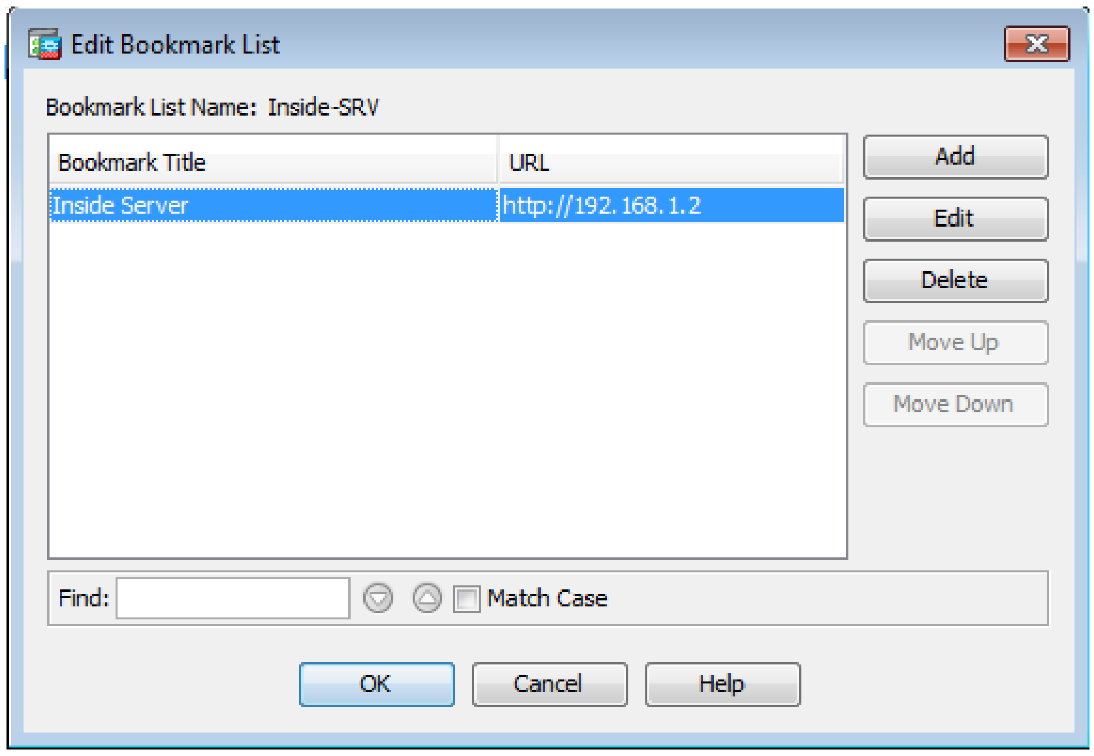
Cisco ASDM 7.5 for ASA - 192.168.1.1

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.

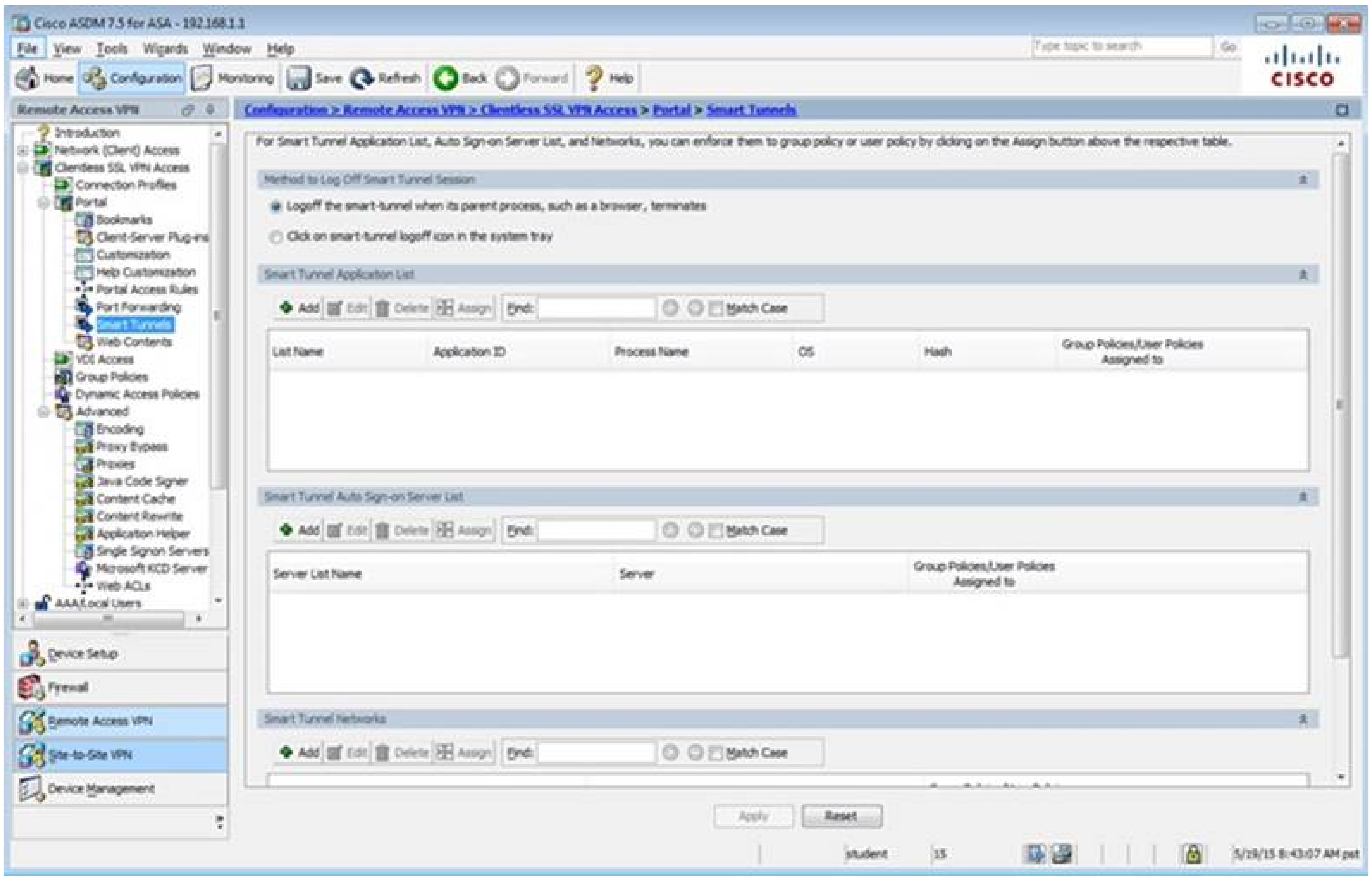
Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Inside-SRV	Sales



Edit Bookmark List

Bookmark List Name: Inside-SRV

Bookmark Title	URL
Inside Server	http://192.168.1.2



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

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

Method to Log Off Smart Tunnel Session

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

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

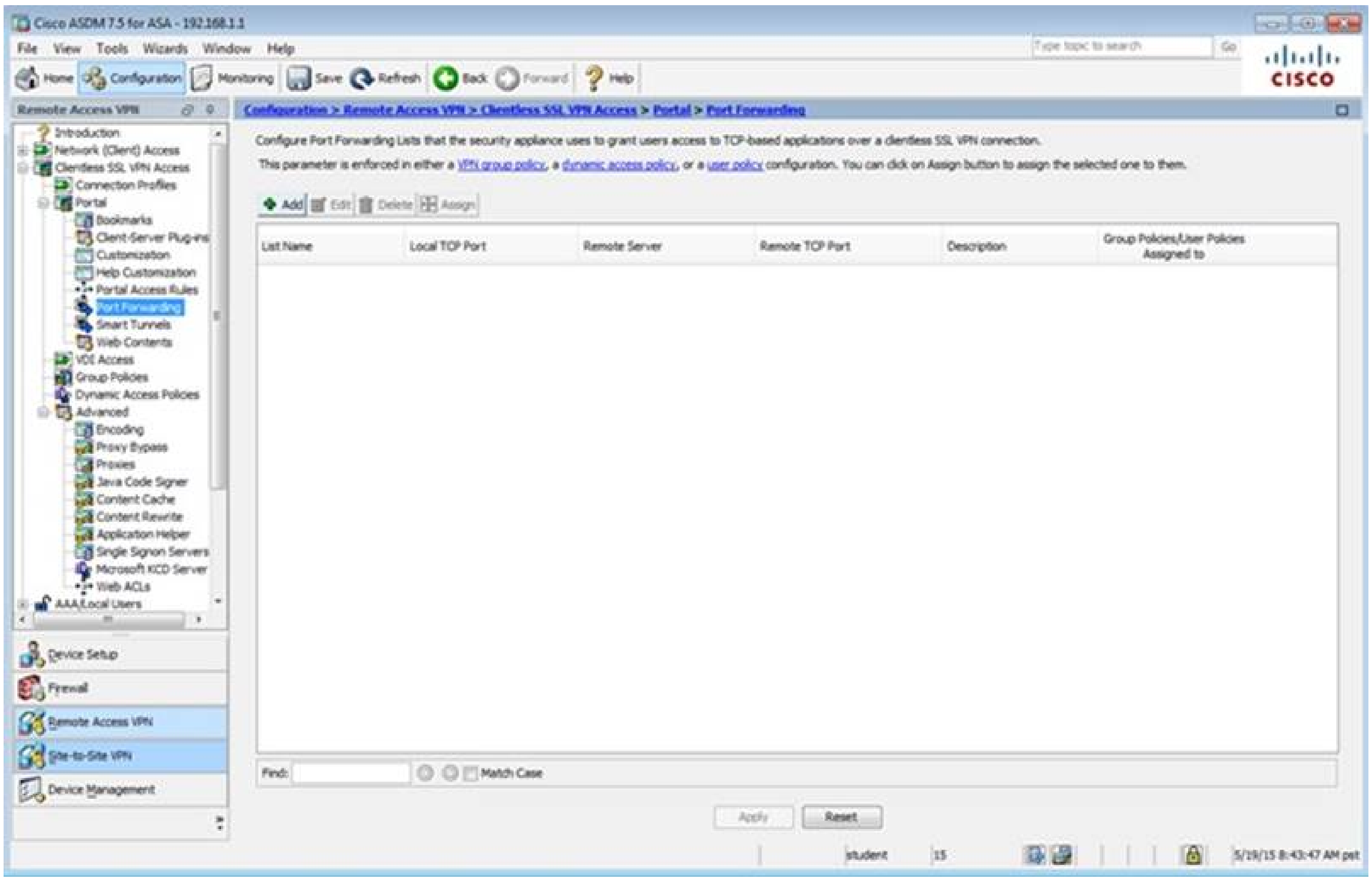
Smart Tunnel Application List

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

Smart Tunnel Auto Sign-on Server List

Server List Name	Server	Group Policies/User Policies Assigned to

Smart Tunnel Networks

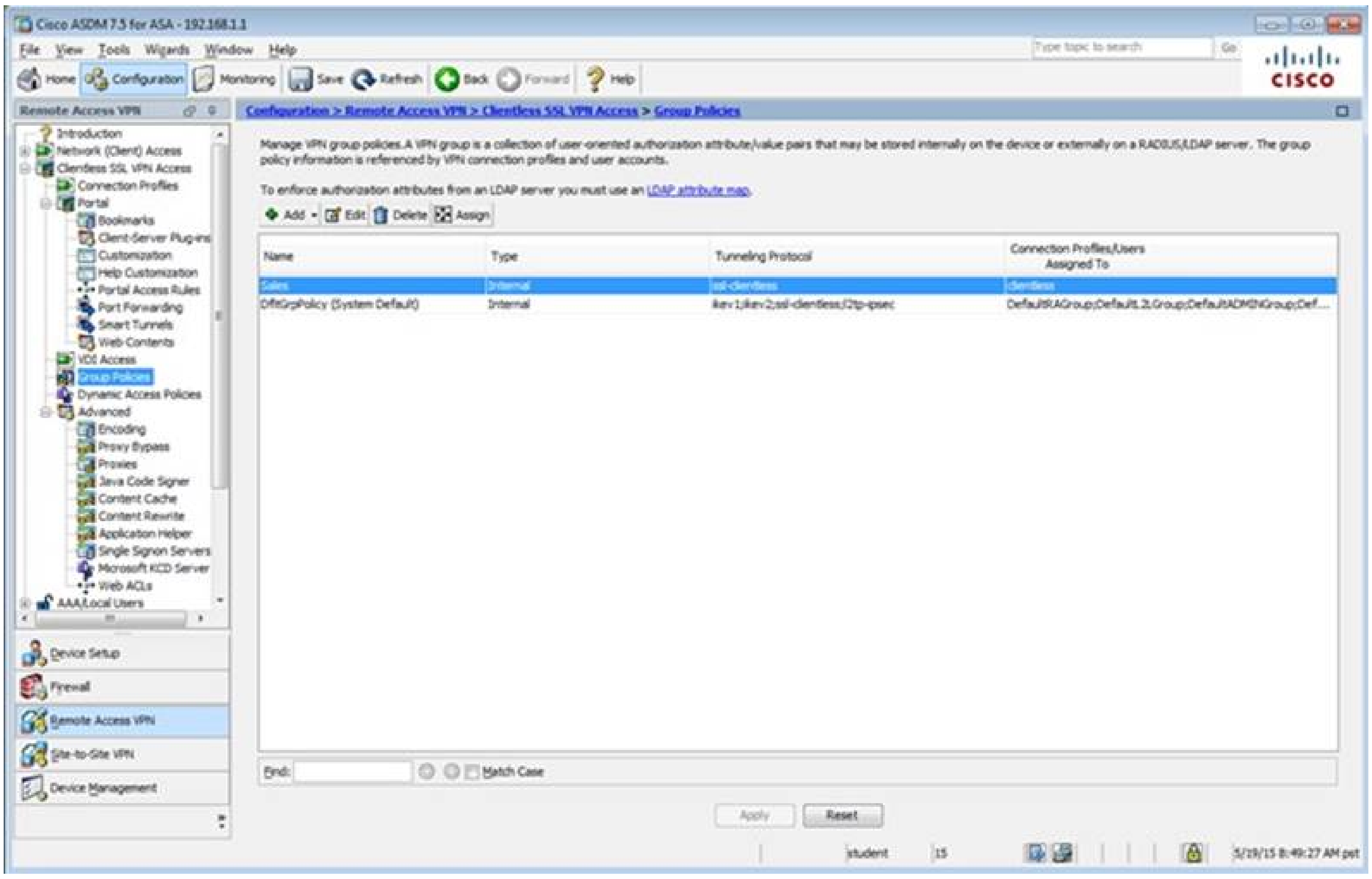


Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

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.

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

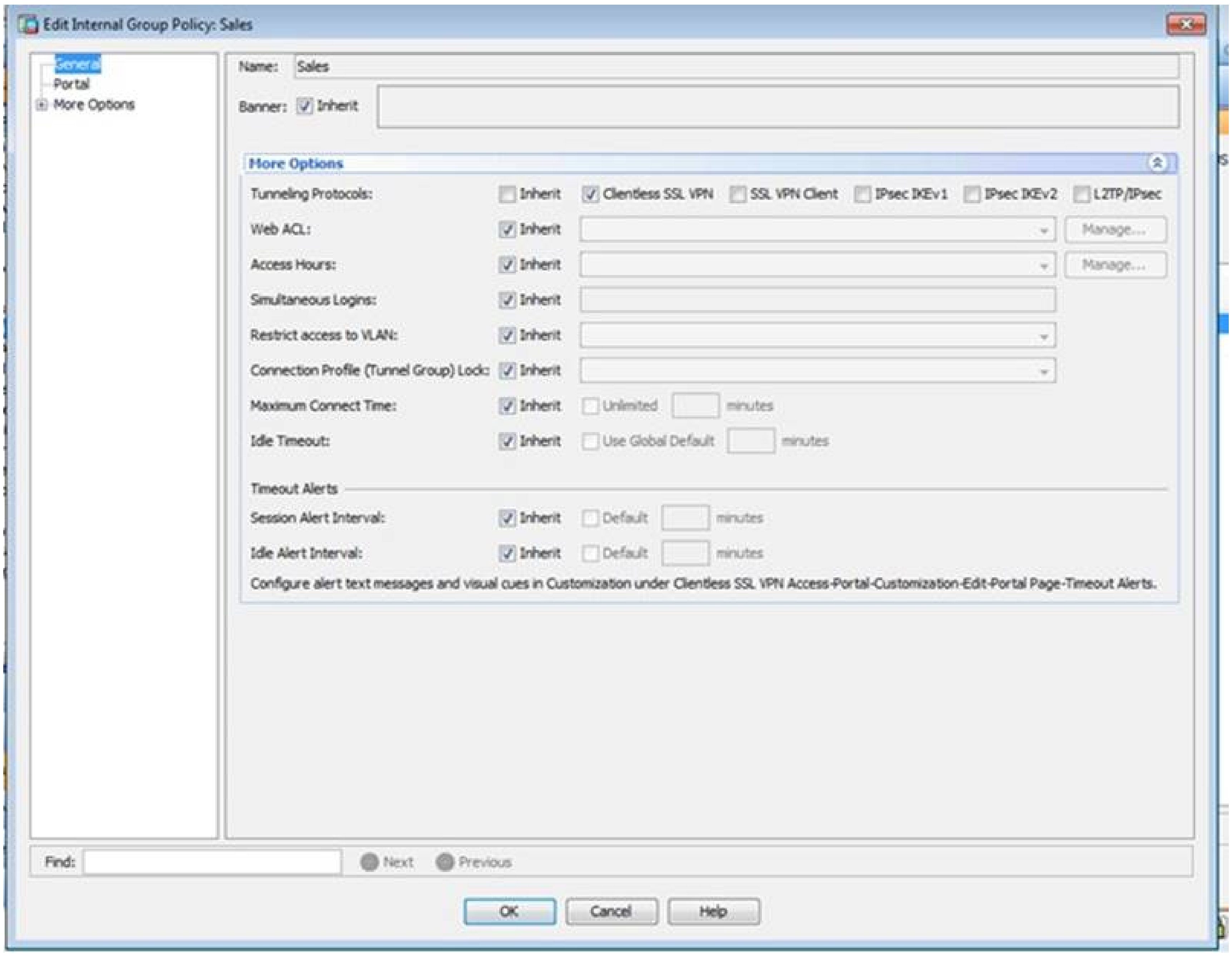


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

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	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...



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

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit ☐ Unlimited minutes

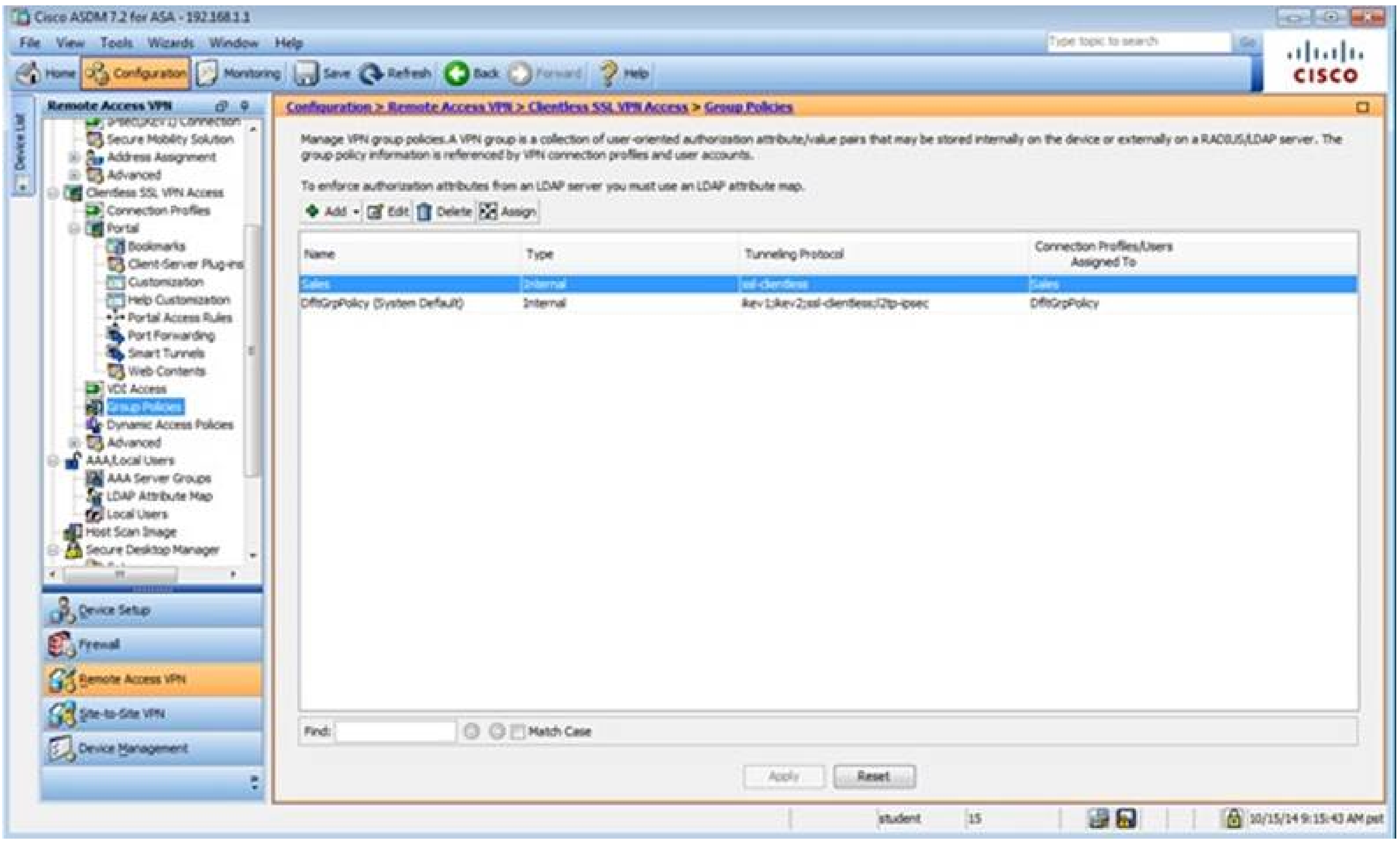
Idle Timeout: ☑ Inherit ☐ Use Global Default minutes

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.



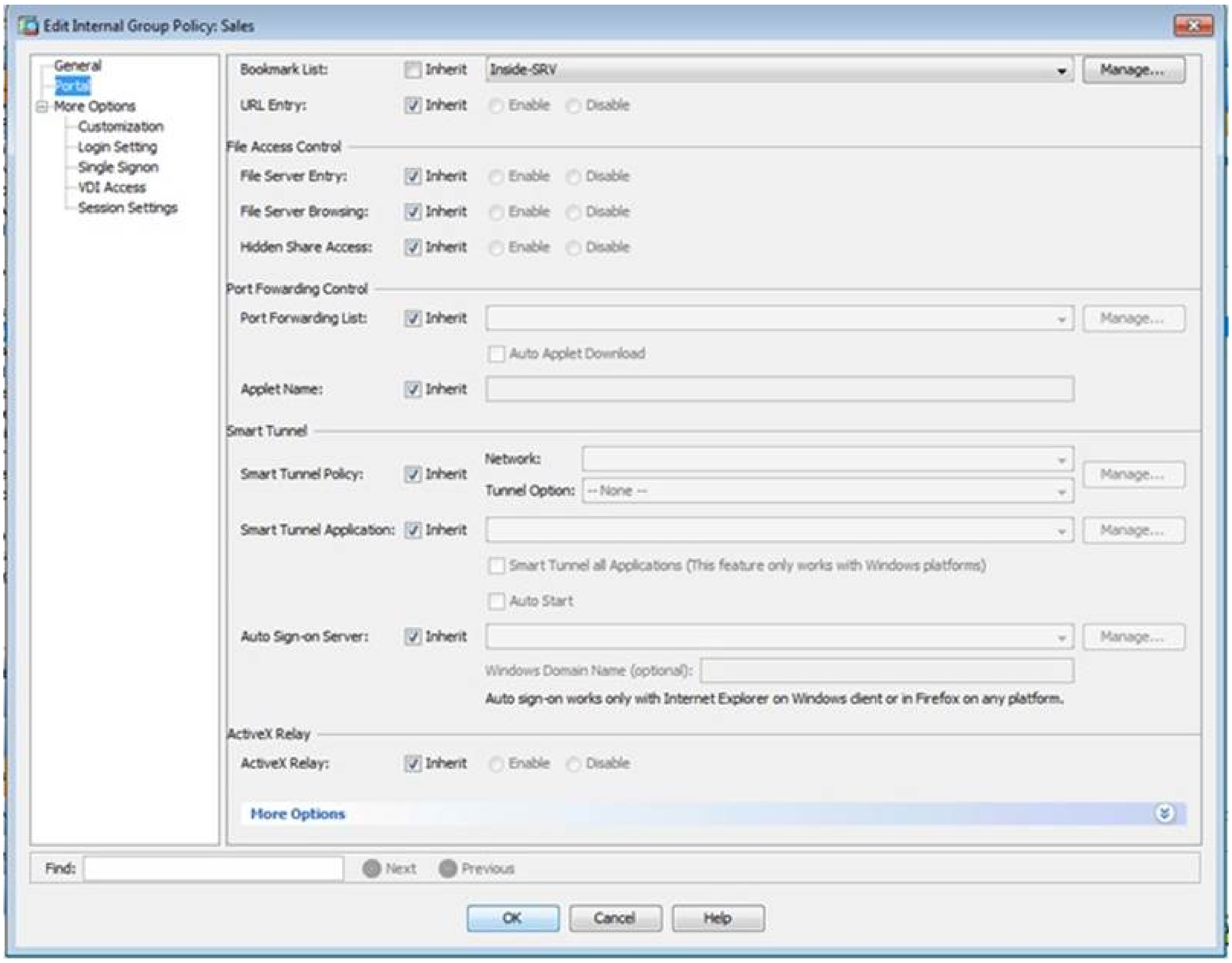
Cisco ASDM 7.2 for ASA - 192.168.1.1

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

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

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

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



Edit Internal Group Policy: Sales

General
Portal
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 Fowarding Control

Port Forwarding List: ☑ Inherit Manage...

□ Auto Applet Download

Applet Name: ☑ Inherit

Smart Tunnel

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

Smart Tunnel Application: ☑ Inherit Manage...

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

□ Auto Start

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

Windows Domain Name (optional):

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

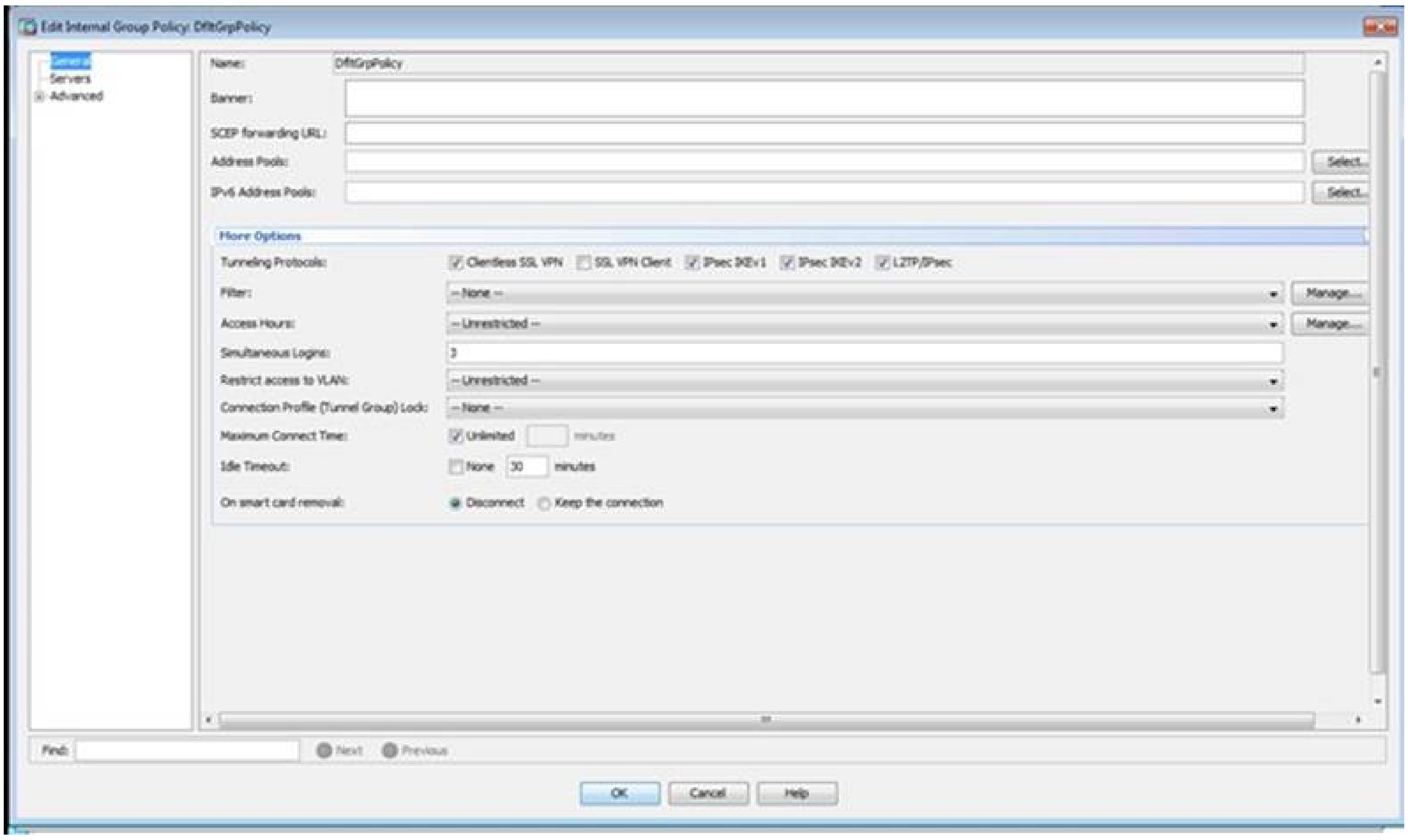
ActiveX Relay

ActiveX Relay: ☑ Inherit ○ Enable ○ Disable

More Options

Find: Next Previous

OK Cancel Help



Edit Internal Group Policy: DfltGrpPolicy

General
Servers
Advanced

Name: DfltGrpPolicy

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 --

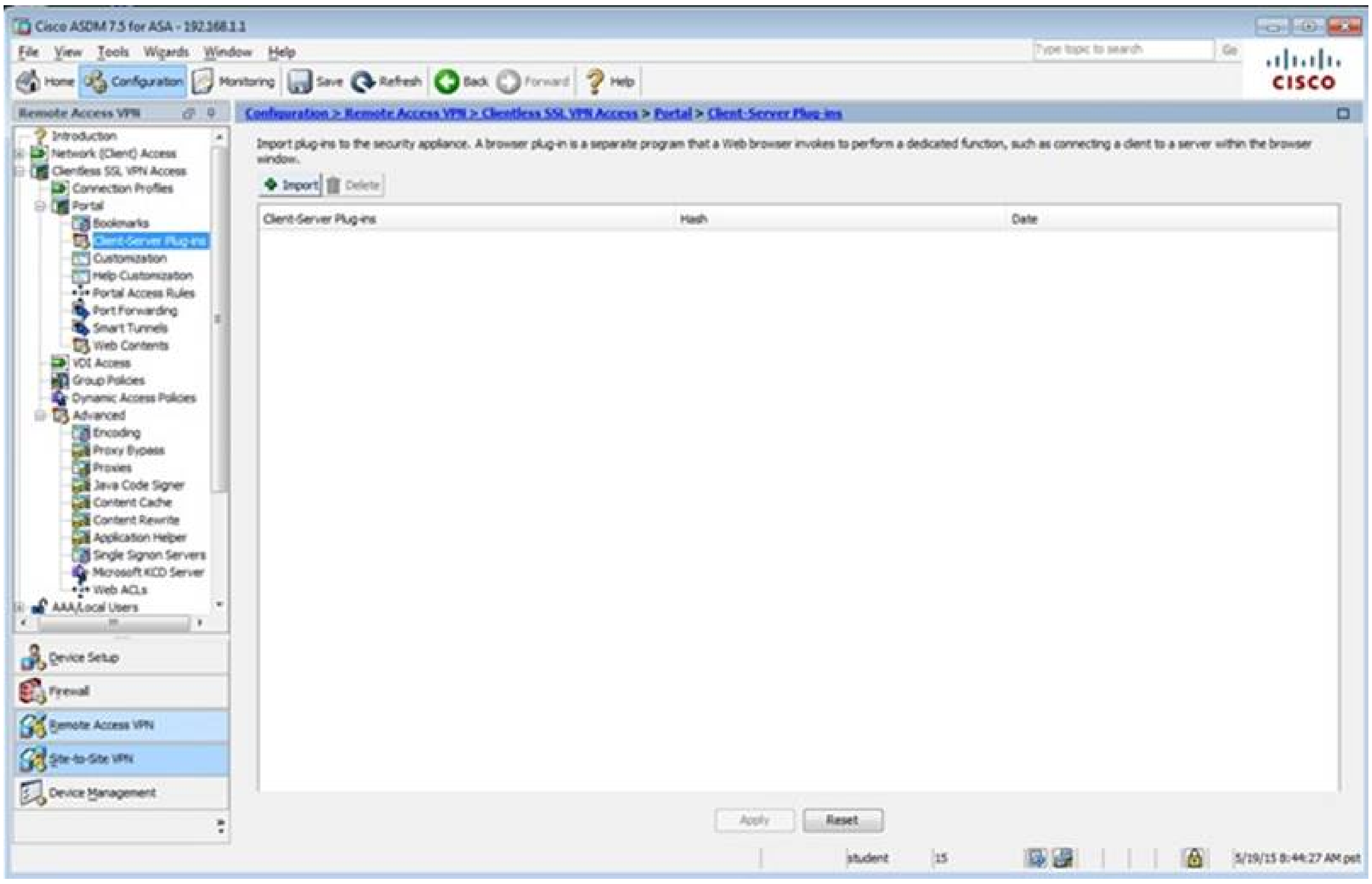
Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: □ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection

Find: Next Previous

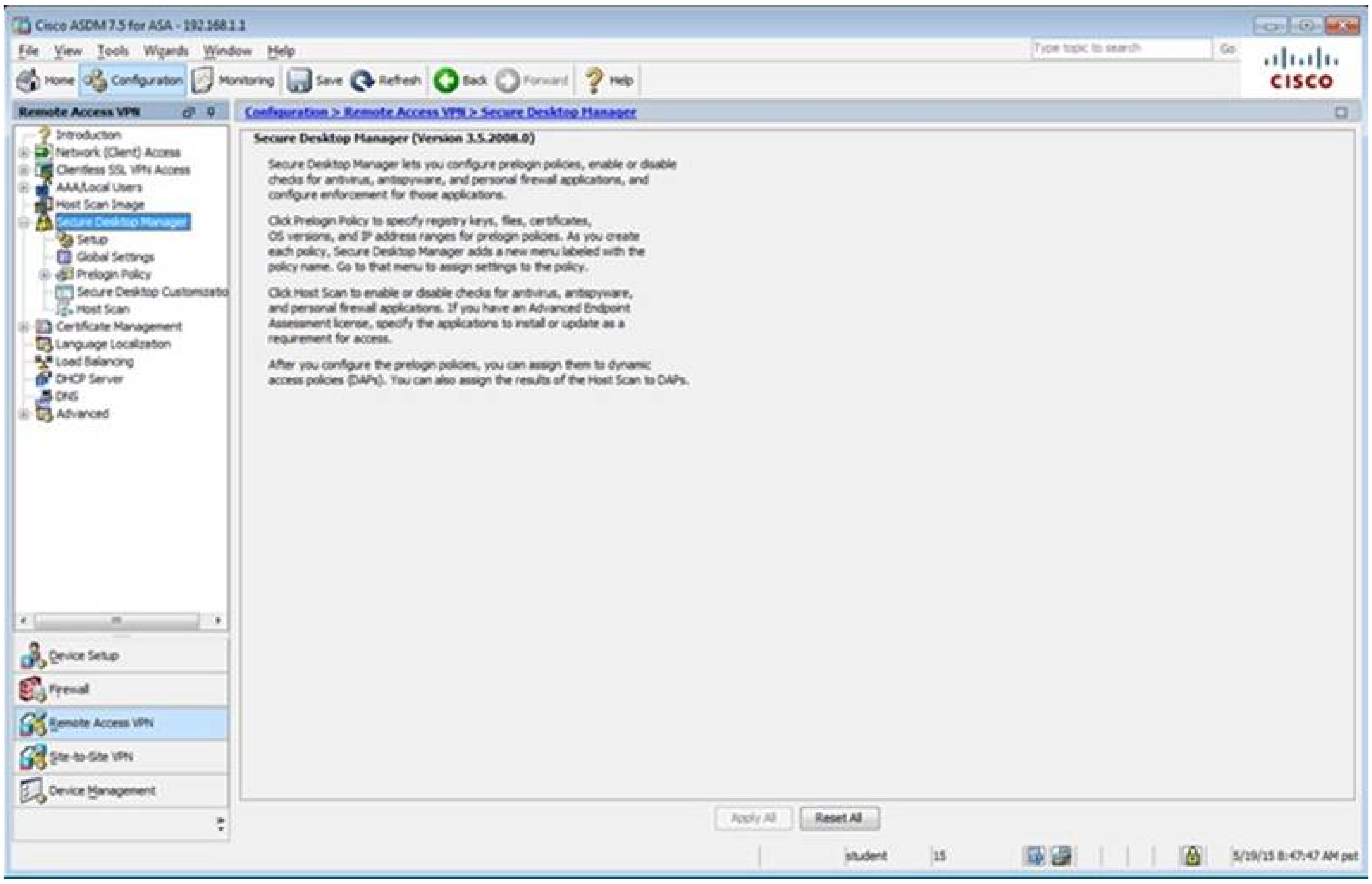
OK Cancel Help



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins

Import plug-ins to the security appliance. A browser plug-in is a separate program that a Web browser invokes to perform a dedicated function, such as connecting a client to a server within the browser window.

Client-Server Plug-ins	Hash	Date



Configuration > Remote Access VPN > Secure Desktop Manager

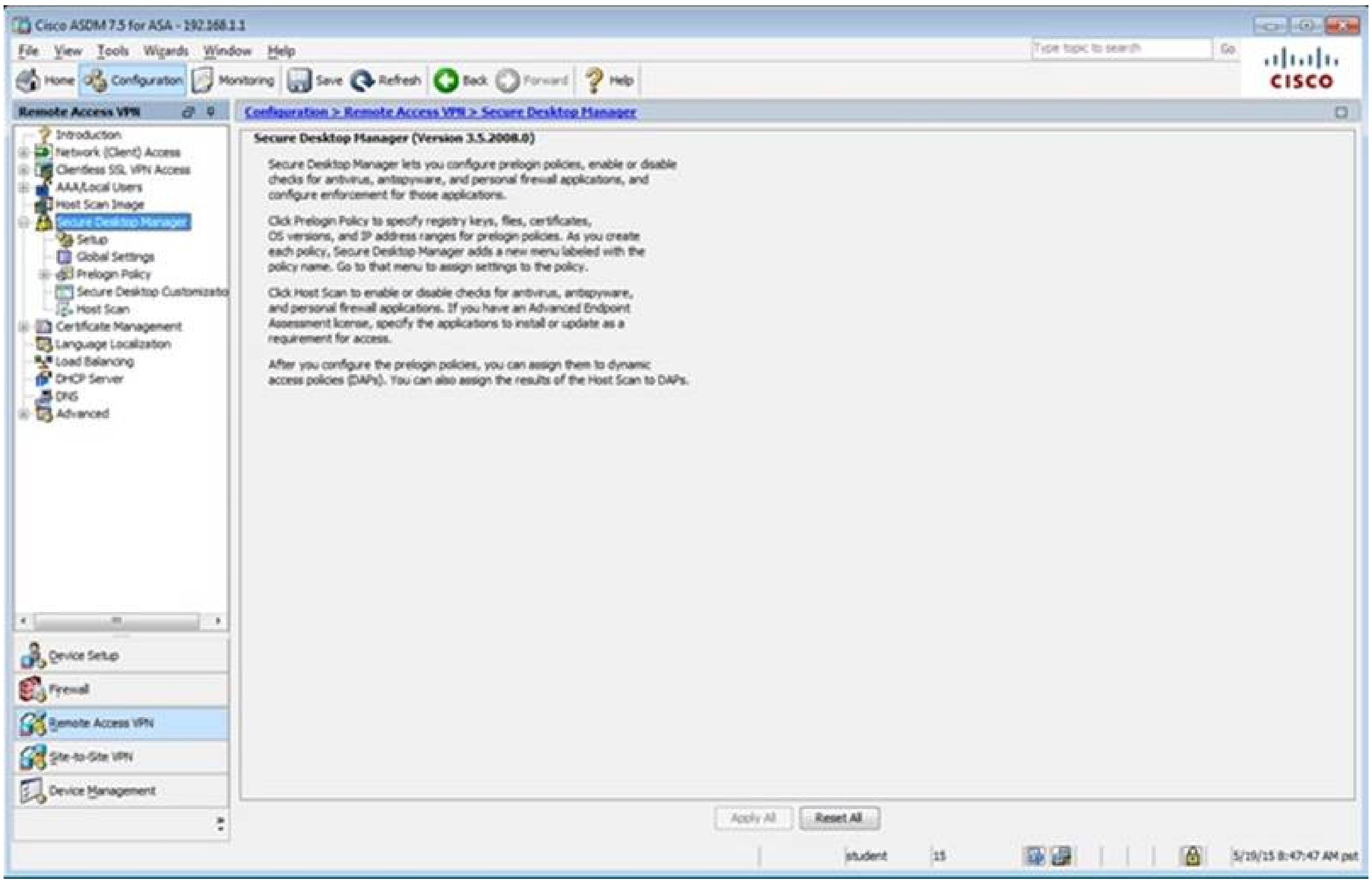
Secure Desktop Manager (Version 3.5.2008.0)

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

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

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

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



Configuration > Remote Access VPN > Secure Desktop Manager

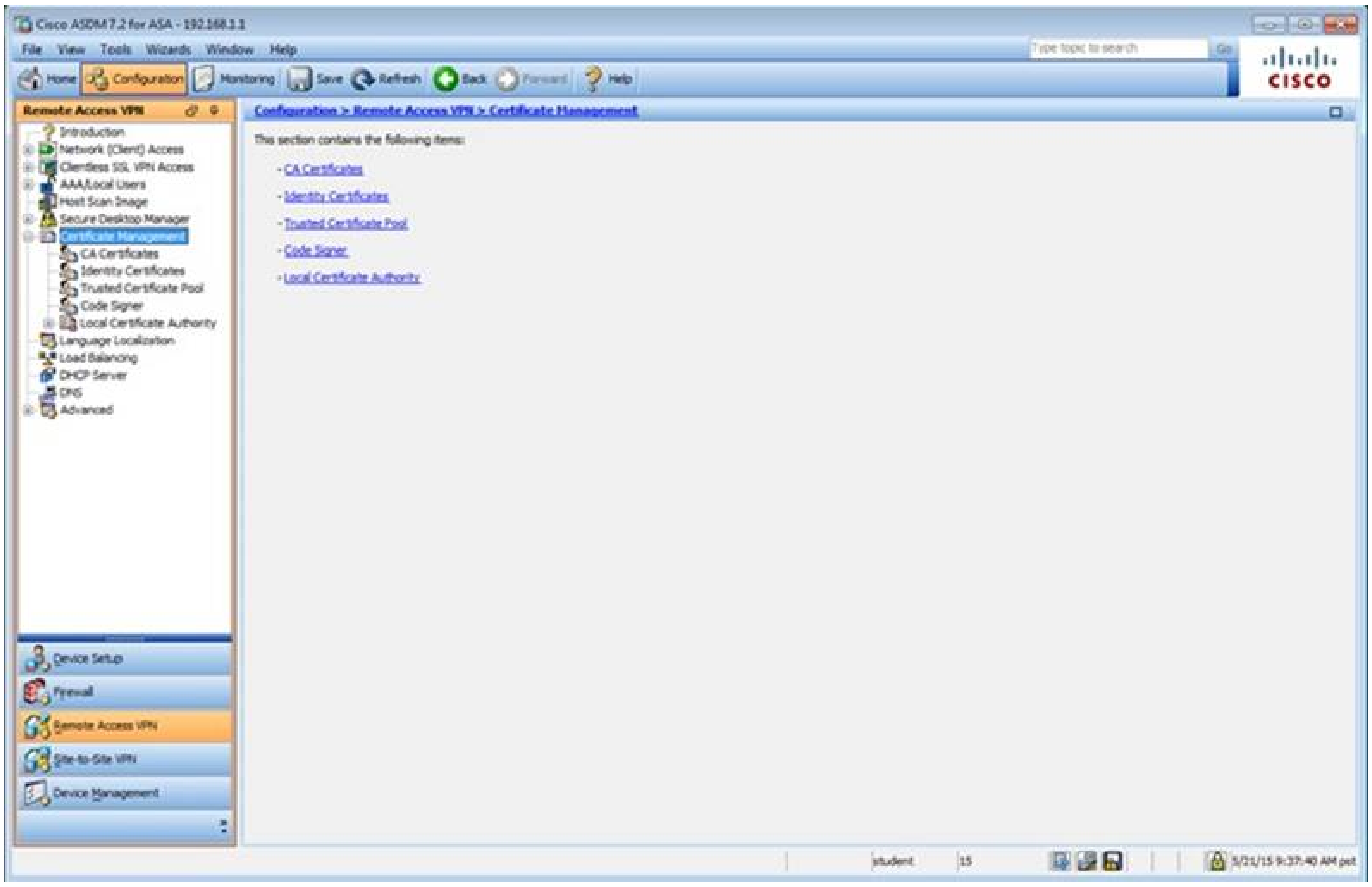
Secure Desktop Manager (Version 3.5.2008.0)

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

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

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

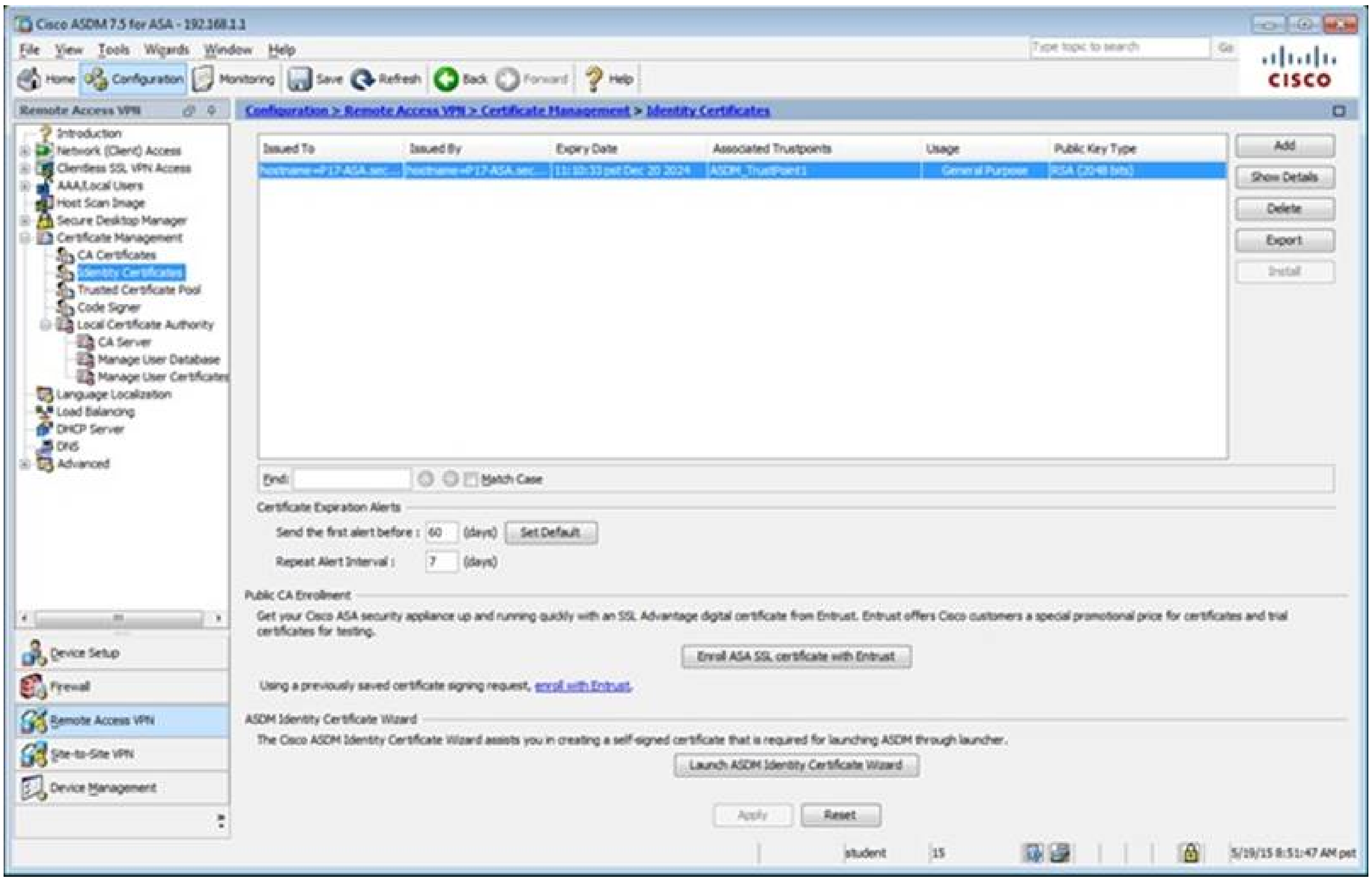
After you configure the prelogin policies, you can assign them to dynamic access policies (DAPs). You can also assign the results of the Host Scan to DAPs.



Configuration > Remote Access VPN > Certificate Management

This section contains the following items:

- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname=P17-ASA.sec...	hostname=P17-ASA.sec...	11:10:33 pst Dec 20 2024	ASDM_TrustPoint1	General Purpose	RSA (2048 bits)

Find: ○ ○ □ Match Case

Certificate Expiration Alerts

Send the first alert before : 60 (days) Set Default

Repeat Alert Interval : 7 (days)

Public CA Enrollment

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

Enroll ASA SSL certificate with Entrust

Using a previously saved certificate signing request, enroll with Entrust.

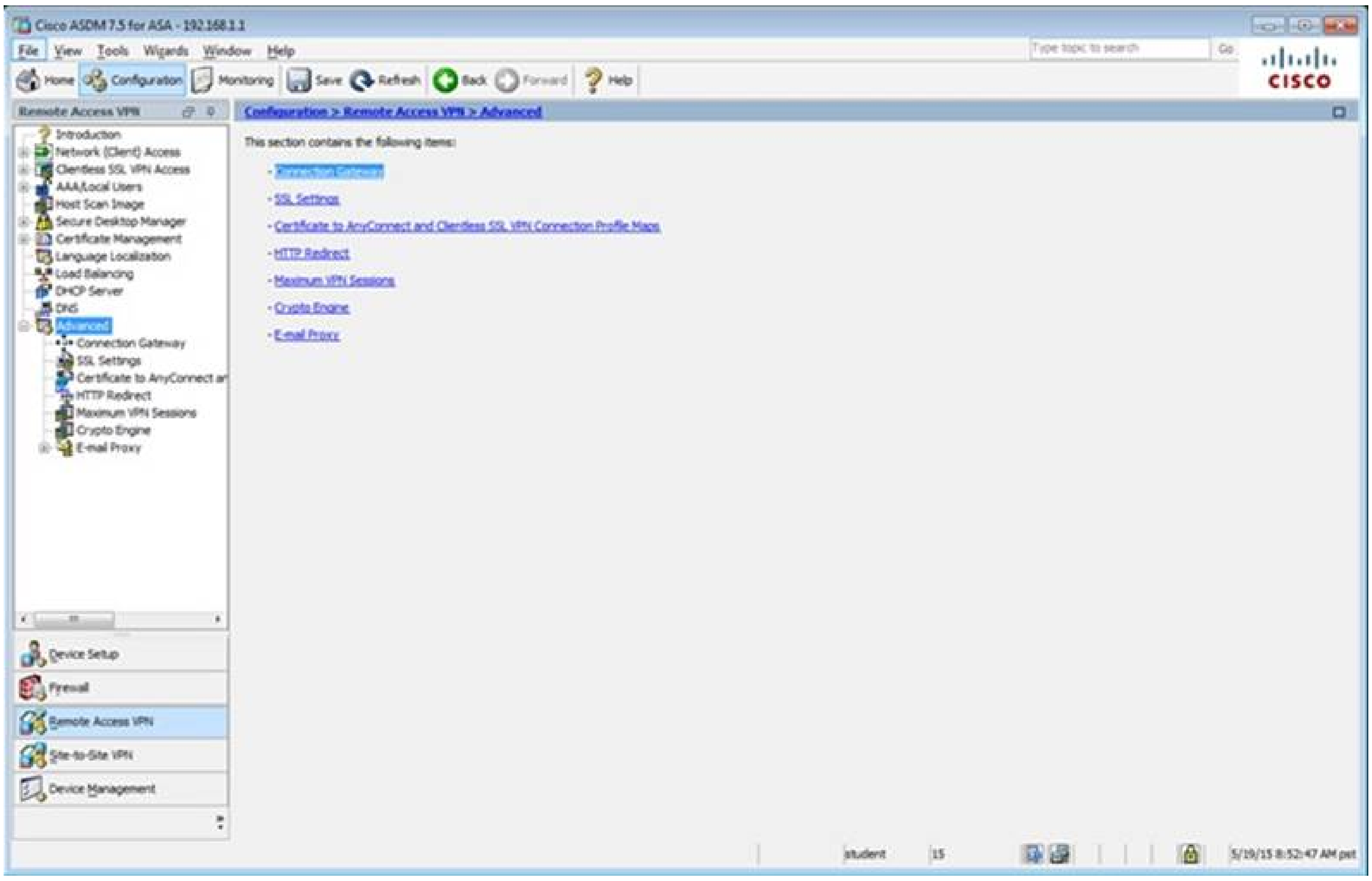
ASDM Identity Certificate Wizard

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

Launch ASDM Identity Certificate Wizard

Apply Reset

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

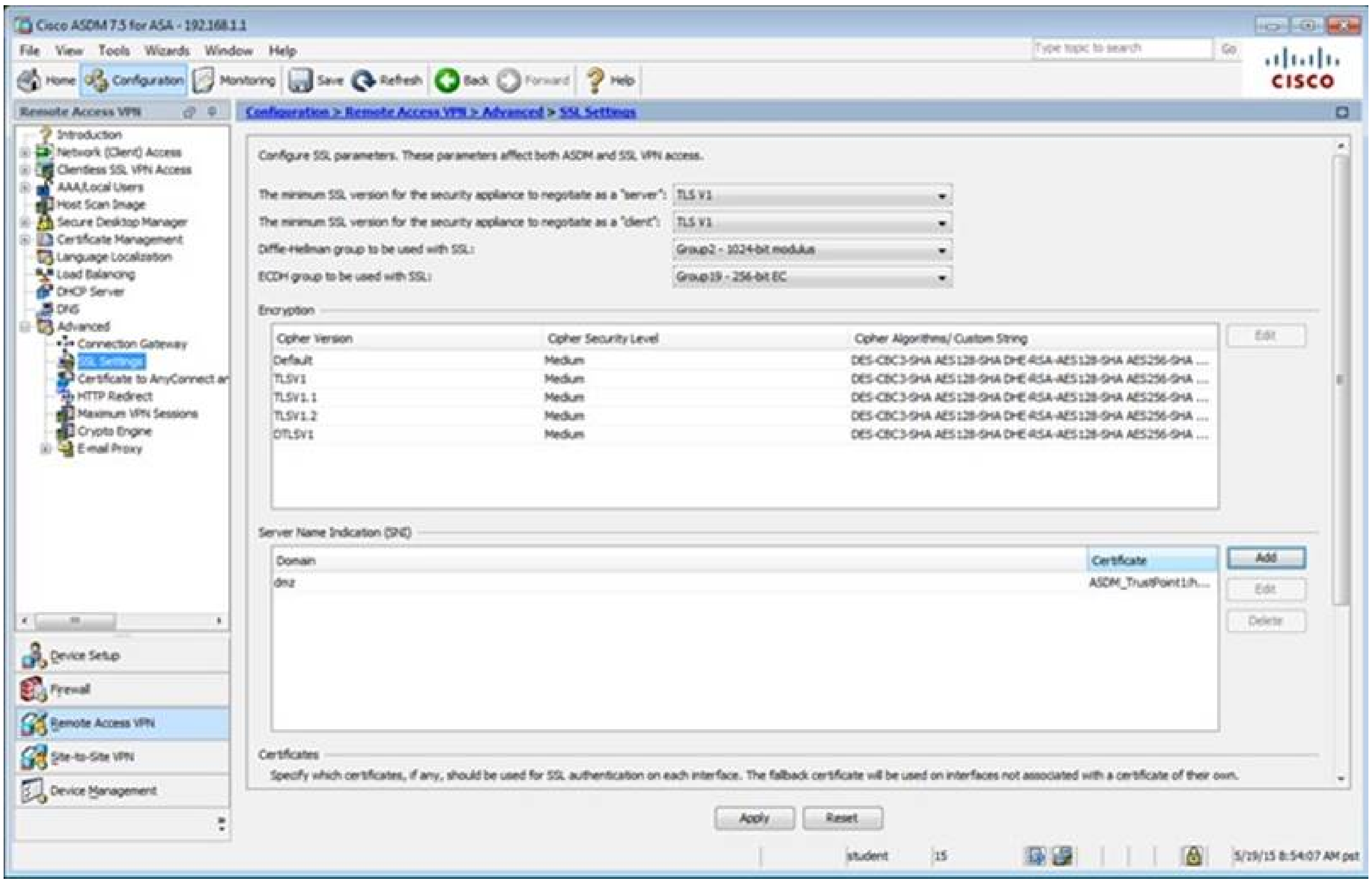


Configuration > Remote Access VPN > Advanced

This 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
- E-mail Proxy

student 15 5/19/15 8:52:47 AM pst



Configuration > Remote Access VPN > Advanced > SSL Settings

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

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

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

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

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

Encryption

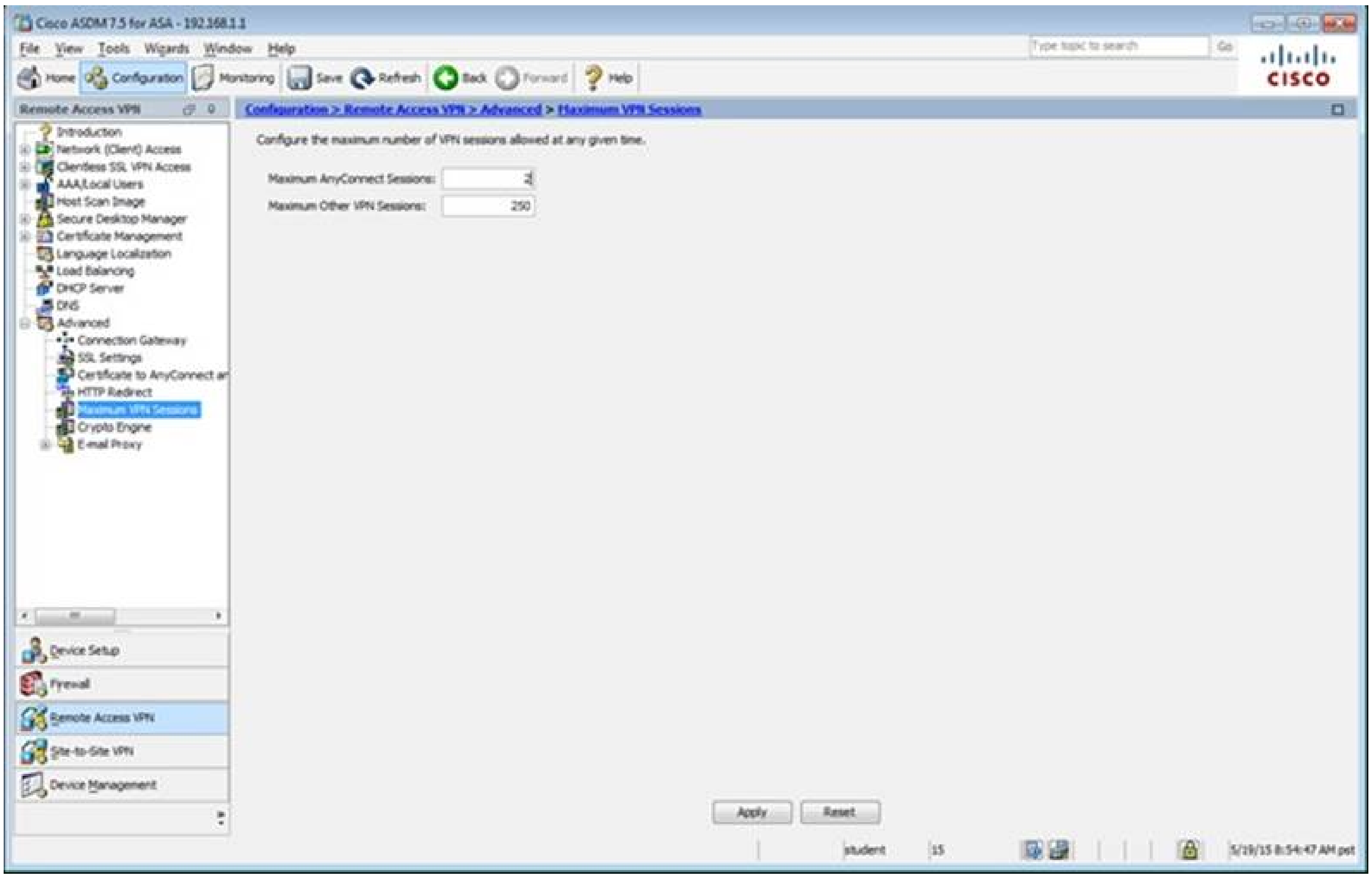
Cipher Version	Cipher Security Level	Cipher Algorithms/ Custom String
Default	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.1	Medium	DES-CBC3-SHA AES128-SHA DHE-RSA-AES128-SHA AES256-SHA ...
TLSV1.2	Medium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

Server Name Indication (SNI)

Domain	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.

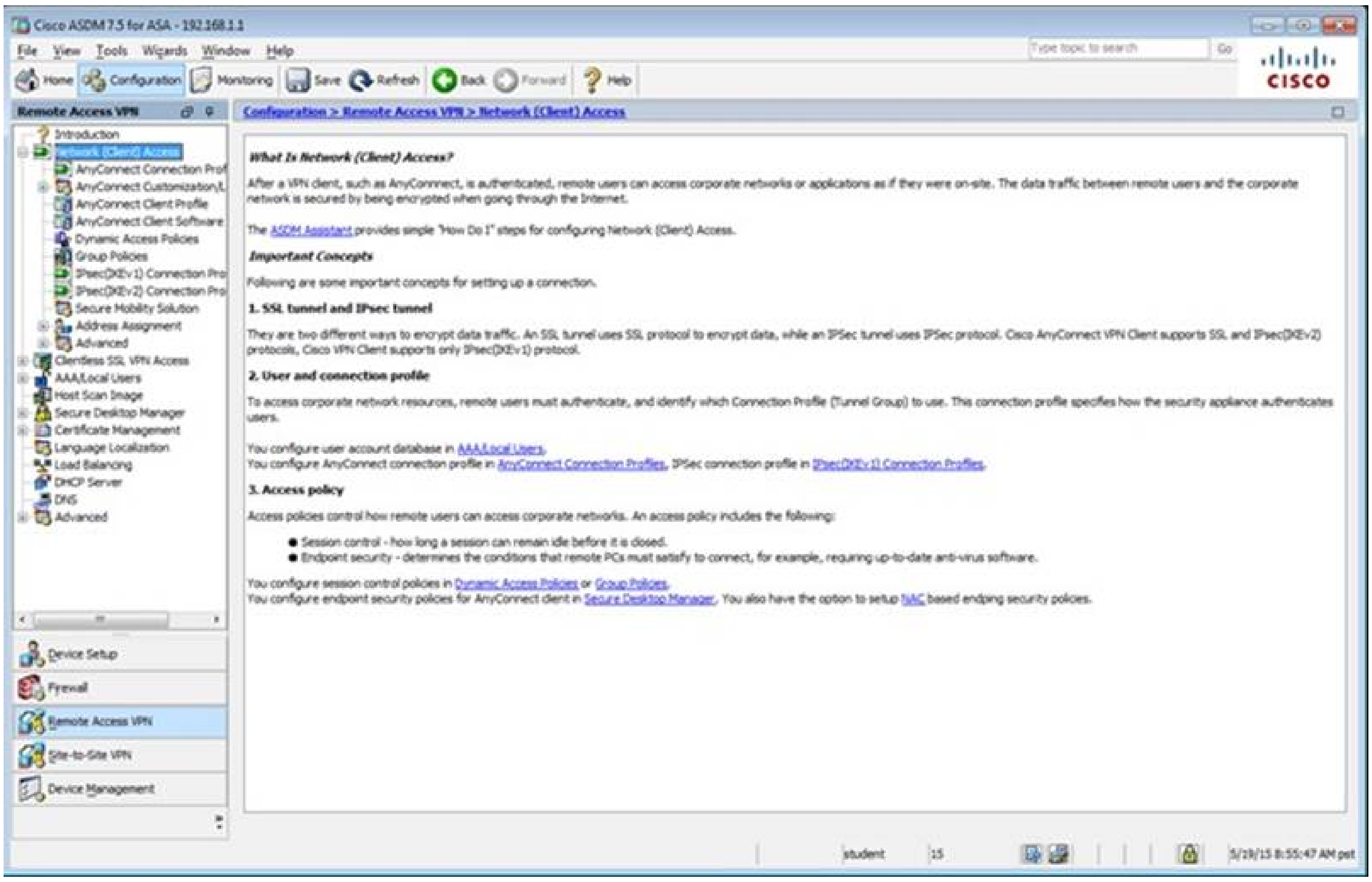


Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions

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

Maximum AnyConnect Sessions: 2

Maximum Other VPN Sessions: 250



Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

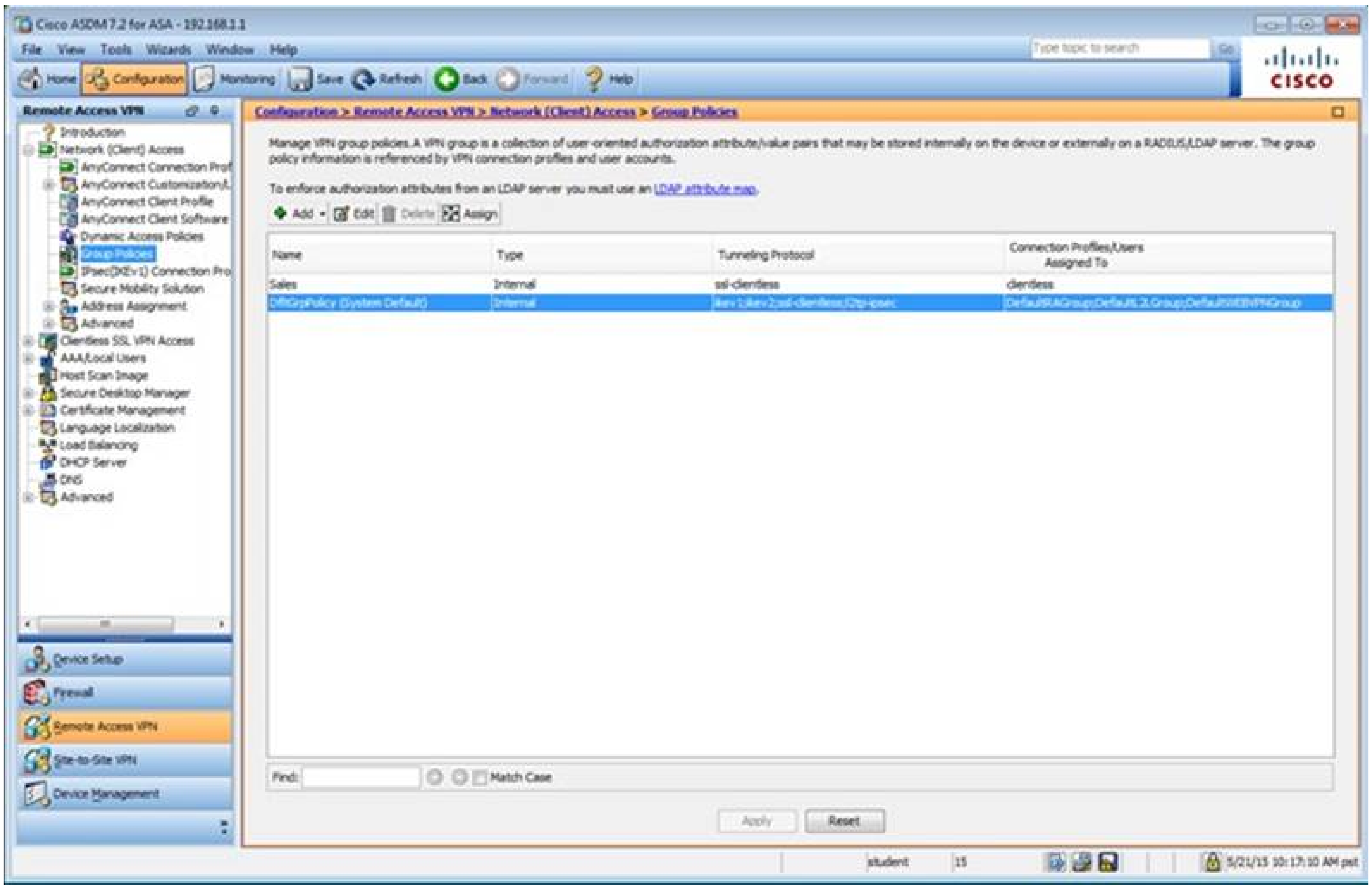
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles, IPSec connection profile in IPsec(IKEv1) Connection Profiles.

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, requring 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 endping security policies.

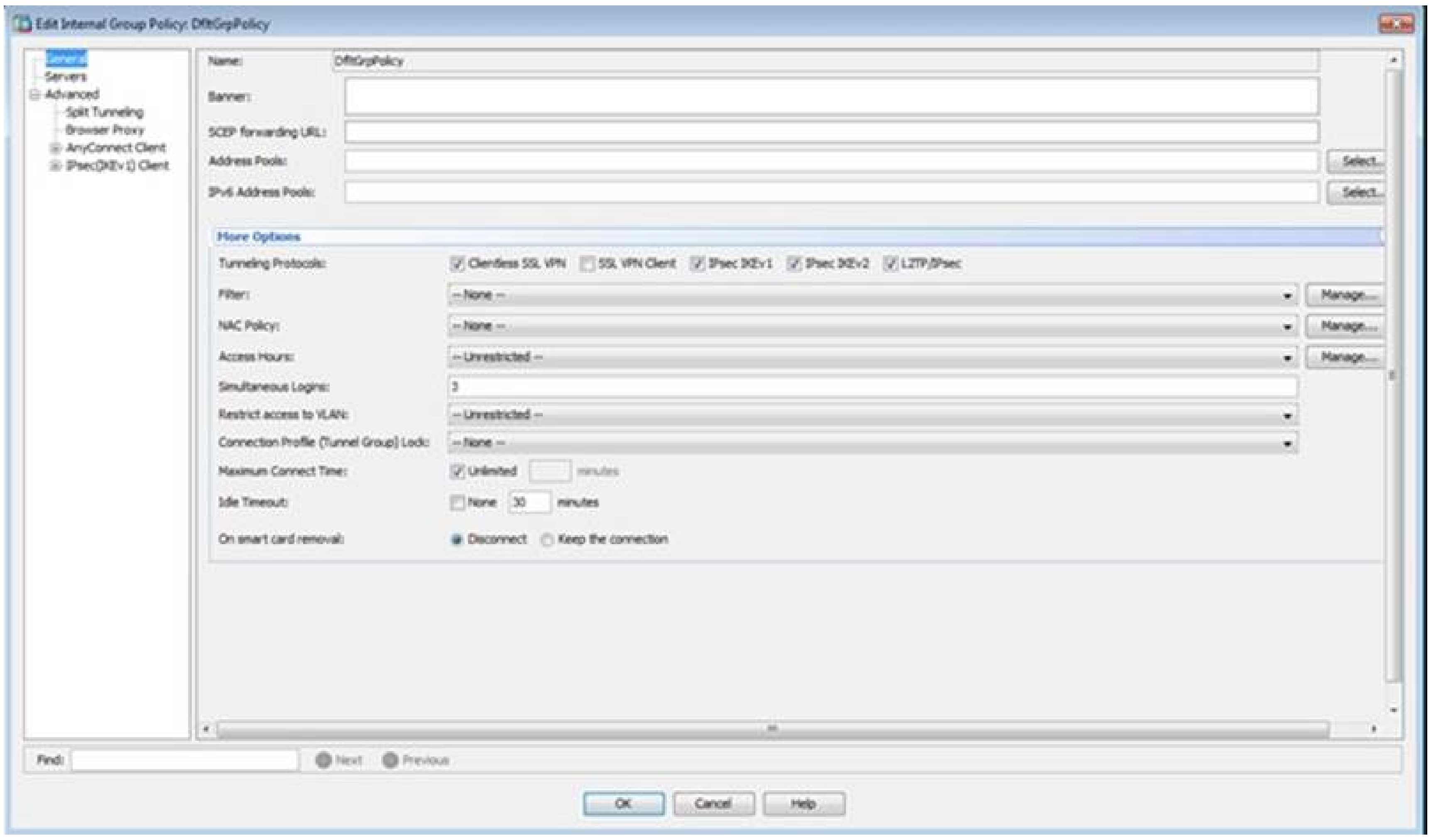


Configuration > Remote Access VPN > Network (Client) Access > Group Policies

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

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

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
Sales	Internal	ssl-clientless	clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup



Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Banner:

SCEP forwarding URL:

Address Pools:

IPv6 Address Pools:

More Options

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

Filter: -- None --

NAC Policy: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

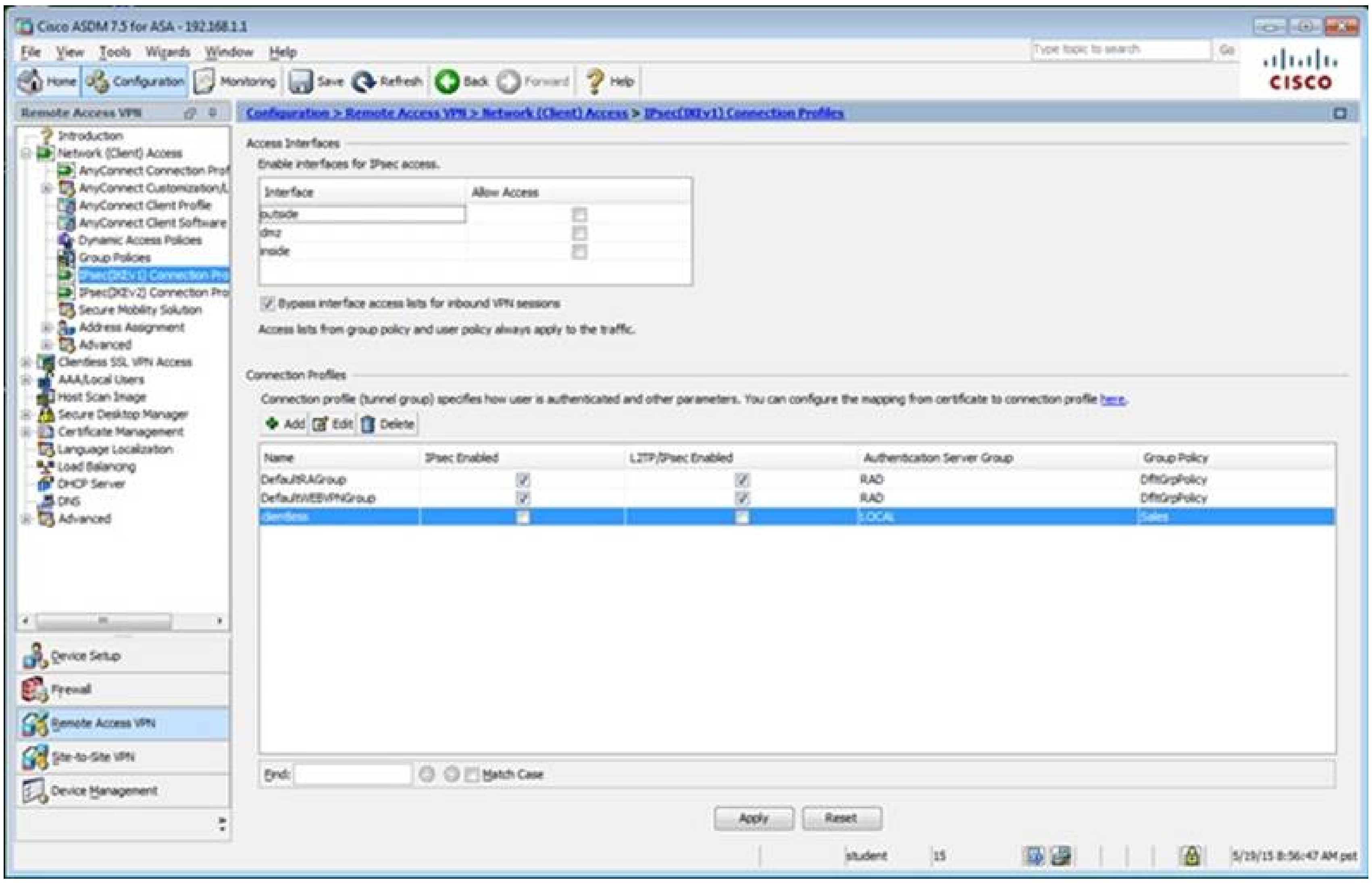
Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: ☐ None 30 minutes

On smart card removal: ● Disconnect ○ Keep the connection



Cisco ASDM 7.5 for ASA - 192.168.1.1

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

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	☐
dmz	☐
inside	☐

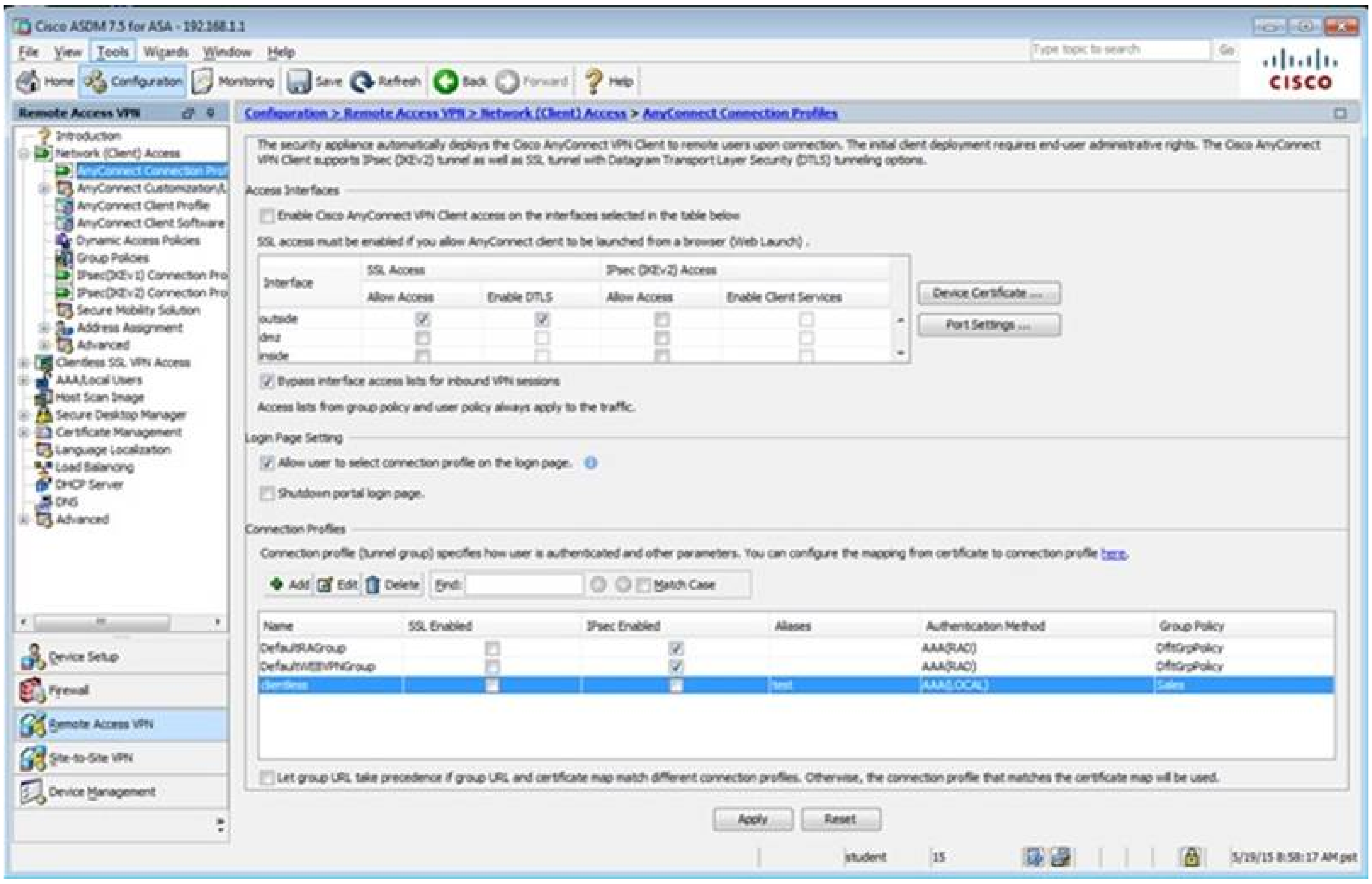
☑ Bypass interface access lists for inbound VPN sessions

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.

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group	Group Policy
DefaultRAGroup	☑	☑	RAD	DfltGrpPolicy
DefaultWEBVPNGroup	☑	☑	RAD	DfltGrpPolicy
clientless	☐	☐	LOCAL	Sales



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	☑	☑	□	□
dmz	□	□	□	□
inside	□	□	□	□

☑ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

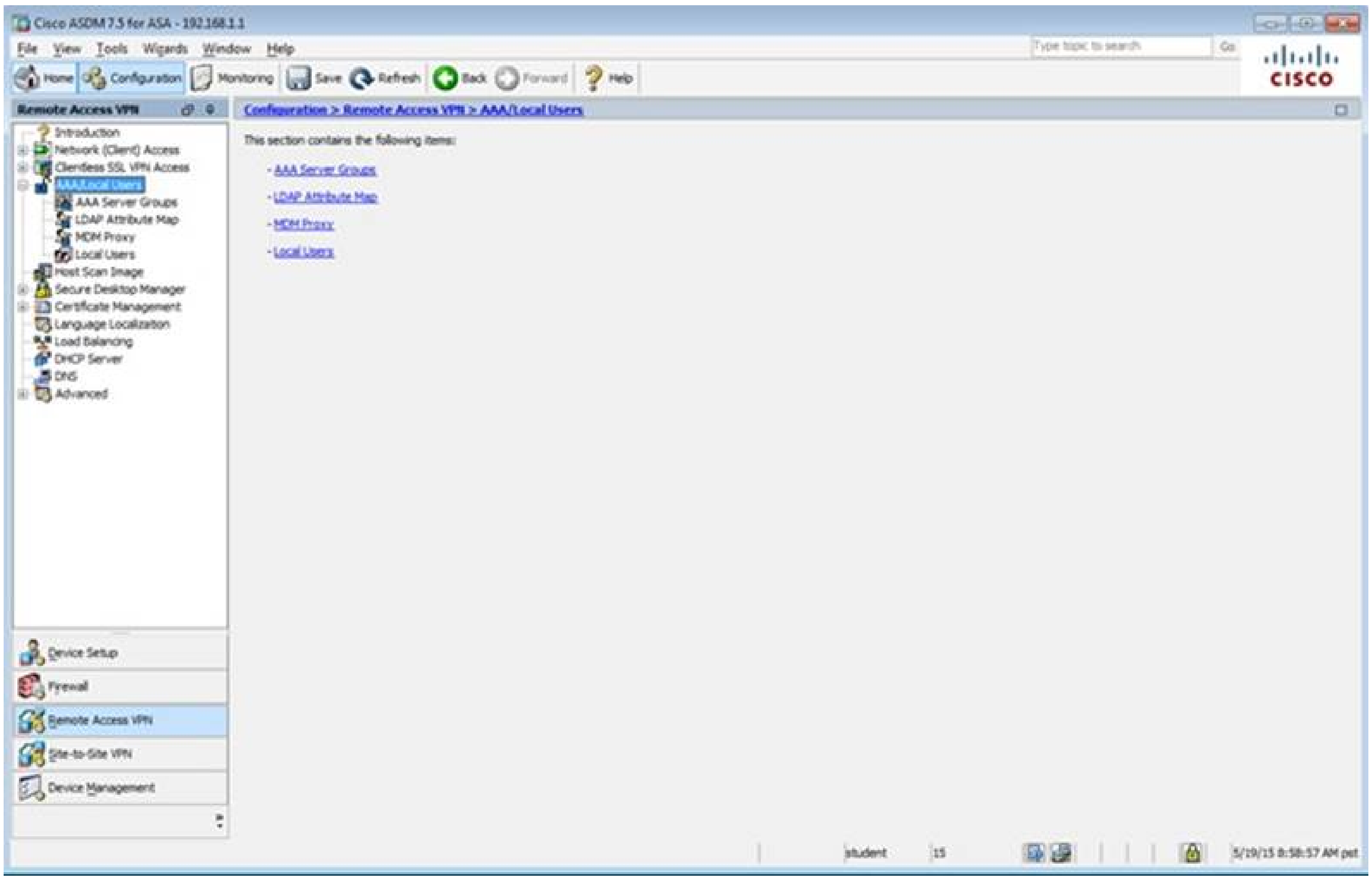
□ Shutdown portal login page.

Connection Profiles

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

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(RAD)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(RAD)	DfltGrpPolicy
clientless	☑	□	test	AAA(LOCAL)	Sales

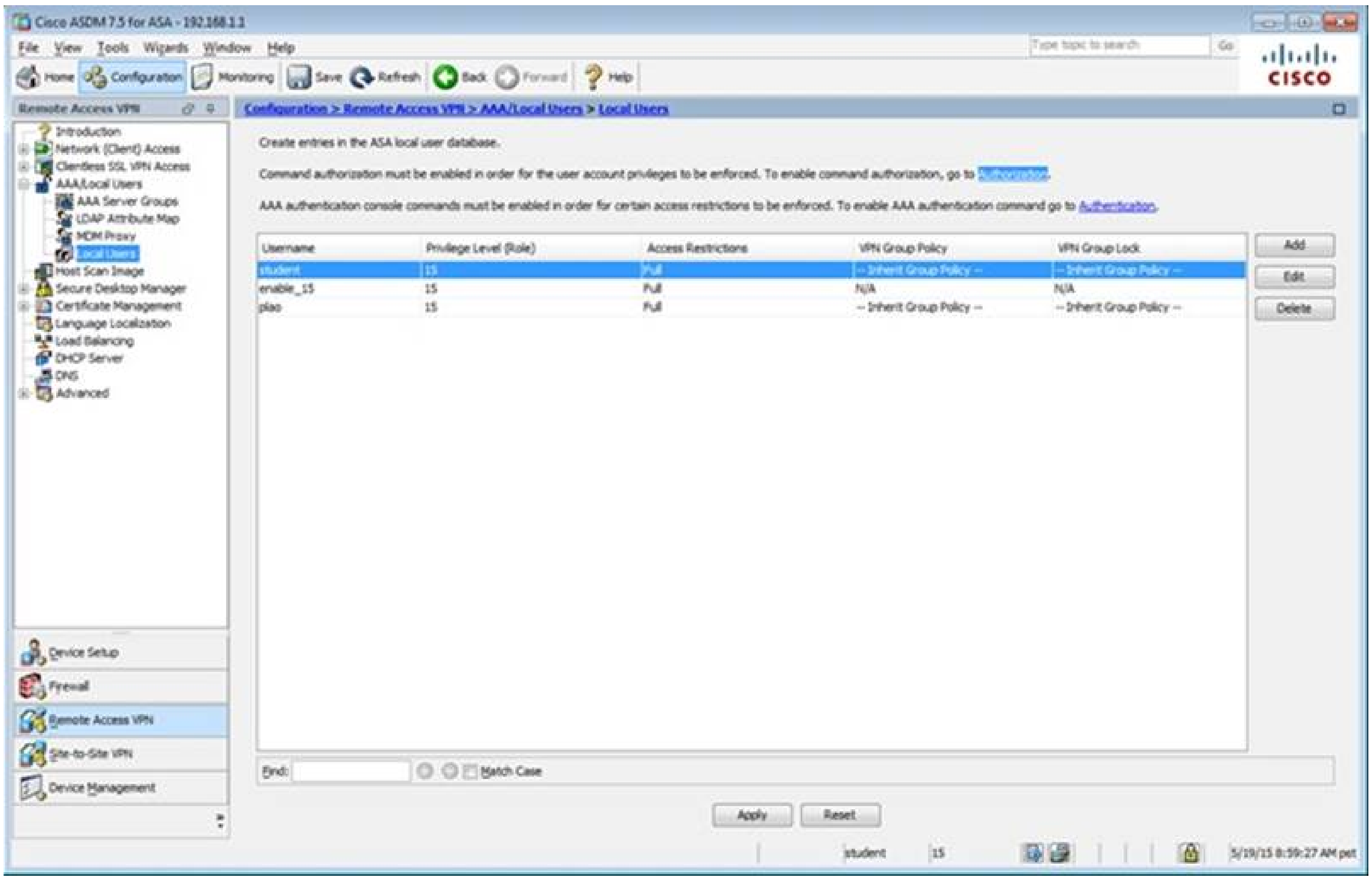
□ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.



Configuration > Remote Access VPN > AAA/Local Users

This section contains the following items:

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



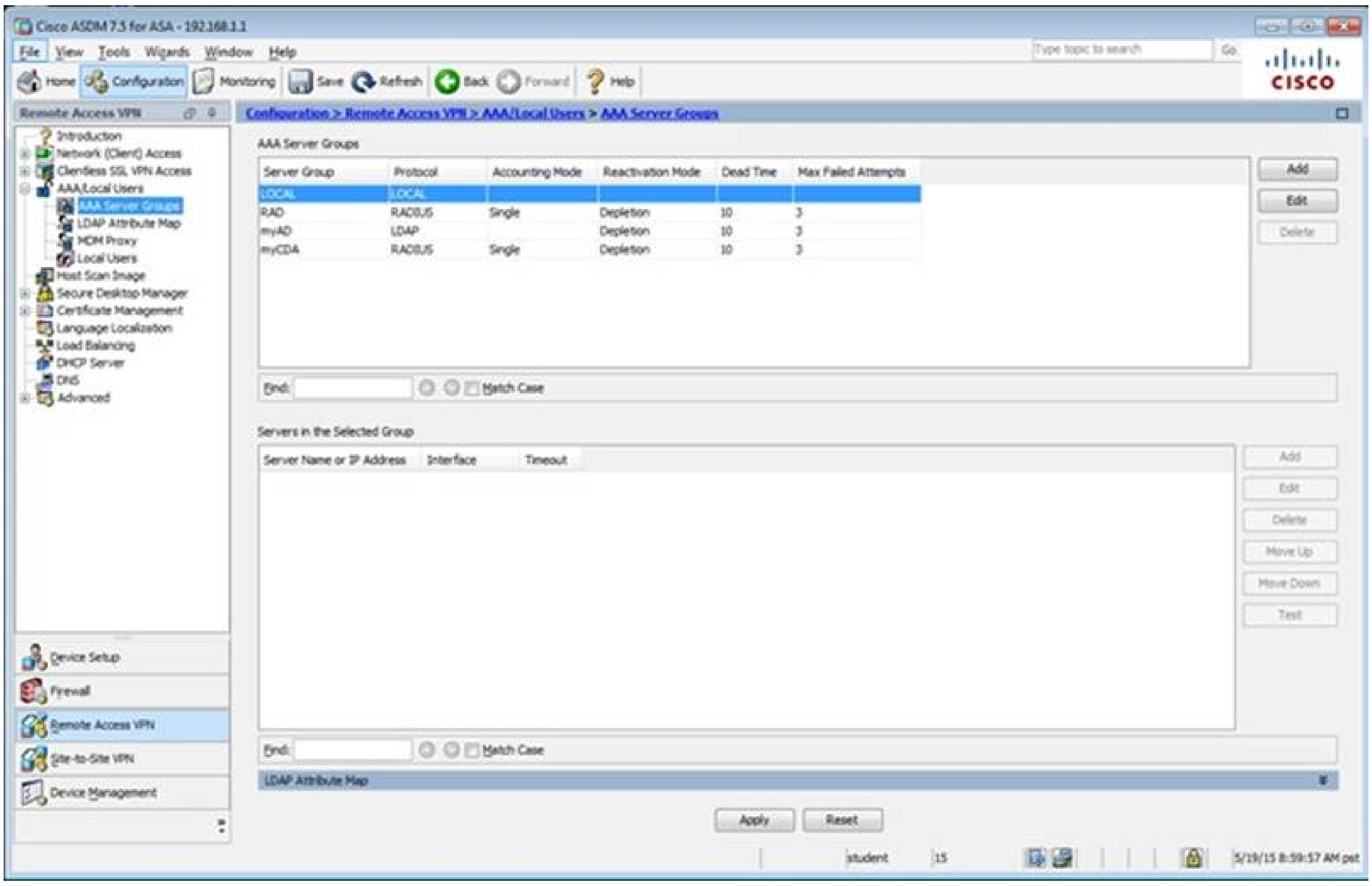
Configuration > Remote Access VPN > AAA/Local Users > Local Users

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 --



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				
RAD	RADIUS	Single	Depletion	10	3
myAD	LDAP		Depletion	10	3
myCDA	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

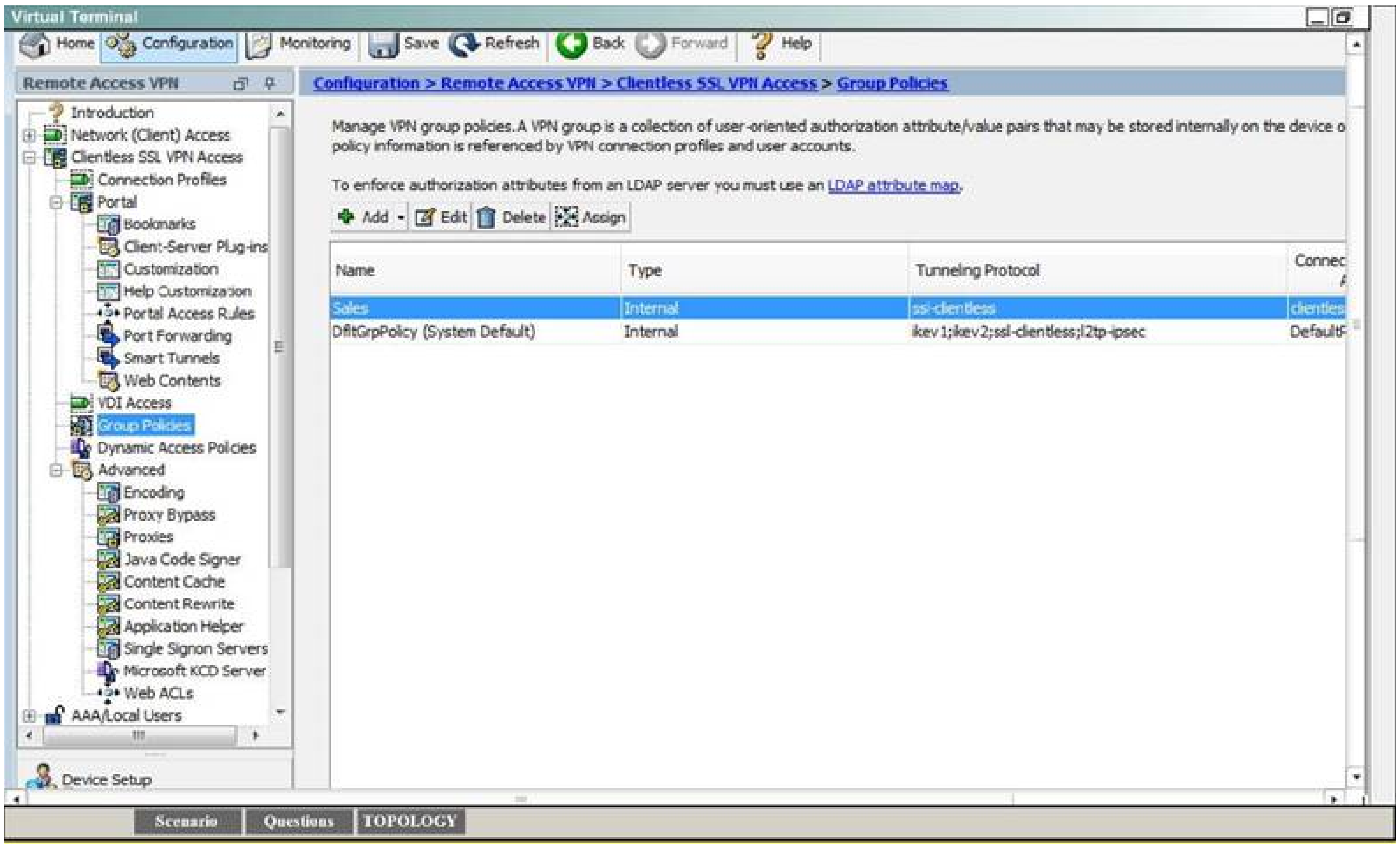
Server Name or IP Address	Interface	Timeout

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:



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 o 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	Connec
Sales	Internal	ssl-clientless	clientles
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultR

NEW QUESTION 66
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 70
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 73
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 75
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

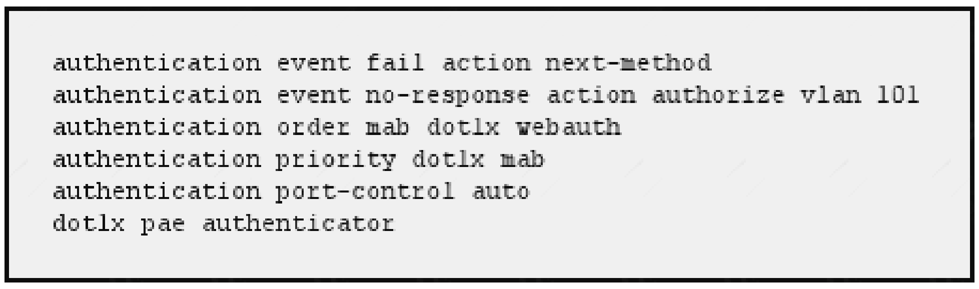
NEW QUESTION 79
If a switch port goes into a blocked state only when a superior BPDU is received, what mechanism must be in use?

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

Answer: A

Explanation: Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.
Source:
http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

NEW QUESTION 80
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

NEW QUESTION 84
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 88
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

NEW QUESTION 90
You want to allow all of your company's users to access the Internet without allowing other Web servers to collect the IP addresses of individual users. What two solutions can you use? (Choose two).

A. Configure a proxy server to hide users' local IP addresses.
B. Assign unique IP addresses to all users.
C. Assign the same IP address to all users.
D. Install a Web content filter to hide users' local IP addresses.
E. Configure a firewall to use Port Address Translation.

Answer: AE

Explanation: In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.[1] A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
Proxies were invented to add structure and encapsulation to distributed systems.[2] Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.
Source: https://en.wikipedia.org/wiki/Proxy_server
Port Address Translation (PAT) is a subset of NAT, and it is still swapping out the source IP address as traffic goes through the NAT/PAT device, except with PAT everyone does not get their own unique translated address. Instead, the PAT device keeps track of individual sessions based on port numbers and other unique identifiers, and then forwards all packets using a single source IP address, which is shared. This is often referred to as NAT with overload; we are hiding multiple IP addresses on a single global address.
Source: Cisco Official Certification Guide, Port Address Translation, p.368

NEW QUESTION 95
A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page. Which action should you take to begin troubleshooting?

A. Ensure that the RDP2 plug-in is installed on the VPN gateway
B. Reboot the VPN gateway
C. Instruct the user to reconnect to the VPN gateway
D. Ensure that the RDP plug-in is installed on the VPN gateway

Answer: D

Explanation: + RDP plug-in: This is the original plug-in created that contains both the Java and ActiveX Client. + RDP2 plug-in: Due to changes within the RDP protocol, the Proper Java RDP Client was updated in order to support Microsoft Windows 2003 Terminal Servers and Windows Vista Terminal Servers.

Source:
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation- firewalls/113600-technote-product-00.html

NEW QUESTION 99
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

NEW QUESTION 103
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

NEW QUESTION 108
In which two situations should you use out-of-band management? (Choose two.)

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

Answer: AB

Explanation: OOB management is used for devices at the headquarters and is accomplished by connecting dedicated management ports or spare Ethernet ports on devices directly to the dedicated OOB management network hosting the management and monitoring applications and services. The OOB management network can be either implemented as a collection of dedicated hardware or based on VLAN isolation.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html

NEW QUESTION 109
Which type of mirroring does SPAN technology perform?

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

Answer: C

Explanation: You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device.
Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch or switch stack. Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer:
+ If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
Source:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/ configuration/guide/scg_2960/swspan.html

NEW QUESTION 113
Which two services define cloud networks? (Choose two.)

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

Answer: AB

Explanation: The NIST's definition of cloud computing defines the service models as follows:[2] + Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
+ Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
+ Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Source: https://en.wikipedia.org/wiki/Cloud_computing#Service_models

NEW QUESTION 114
If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

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

Answer: A

Explanation: I suppose this could be an Explanation:. Not 100% confident about this. The Explanation: refers to an interface, but the question doesn't specify that.
See the following information for how a packet matches class maps in a policy map for a given interface:
1. A packet can match only one class map in the policy map for each feature type.
2. When the packet matches a class map for a feature type, the ASA does not attempt to match it to any subsequent class maps for that feature type.
3. If the packet matches a subsequent class map for a different feature type, however, then the ASA also applies the actions for the subsequent class map, if supported. See the "Incompatibility of Certain Feature Actions" section for more information about unsupported combinations.
If a packet matches a class map for connection limits, and also matches a class map for an application inspection, then both actions are applied.
If a packet matches a class map for HTTP inspection, but also matches another class map that includes HTTP inspection, then the second class map actions are not applied.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ mpf_service_policy.html

NEW QUESTION 119
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 123
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

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

Answer: AD

Explanation: IPsec uses the Internet Key Exchange (IKE) protocol to negotiate and establish secured site-to-site or remote access virtual private network (VPN) tunnels. IKE is a framework provided by the Internet Security Association and Key Management Protocol (ISAKMP) and parts of two other key management protocols, namely Oakley and Secure Key Exchange Mechanism (SKEME).

In IKE Phase 1 IPsec peers negotiate and authenticate each other. In Phase 2 they negotiate keying materials and algorithms for the encryption of the data being transferred over the IPsec tunnel.
Source: Cisco Official Certification Guide, The Internet Key Exchange (IKE) Protocol, p.123

NEW QUESTION 124
Which type of firewall can act on the behalf of the end device?

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

Answer: D

Explanation: Application firewalls, as indicated by the name, work at Layer 7, or the application layer of the OSI model. These devices act on behalf of a client (aka proxy) for requested services.
Because application/proxy firewalls act on behalf of a client, they provide an additional "buffer" from port scans, application attacks, and so on. For example, if an attacker found a vulnerability in an application, the attacker would have to compromise the application/proxy firewall before attacking devices behind the firewall. The application/proxy firewall can also be patched quickly in the event that a vulnerability is discovered. The same may not hold true for patching all the internal devices.
Source:
http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html

NEW QUESTION 129
According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

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

Answer: ABC

Explanation: ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the campus.
ACL-DEFAULT--This ACL is configured on the access layer switch and used as a default ACL on the port. Its purpose is to prevent un-authorized access.
An example of a default ACL on a campus access layer switch is shown below: Extended IP access list ACL-DEFAULT
10 permit udp any eq bootpc any eq bootps log (2604 matches) 20 permit udp any host 10.230.1.45 eq domain 30 permit icmp any any
40 permit udp any any eq tftp
50 deny ip any any log (40 matches)
As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/ BYOD_Design_Guide/BYOD_Wired.html
MAB is an access control technique that Cisco provides and it is called MAC Authentication Bypass.

NEW QUESTION 131
Which network device does NTP authenticate?

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

Answer: A

Explanation: You can configure the device to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.
Source:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/ configuration/guide/sm_nx_os_cg/sm_3ntp.html#wp1100303%0A

NEW QUESTION 136
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 140
Which option is the most effective placement of an IPS device within the infrastructure?

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

Answer: A

Explanation: Firewalls are generally designed to be on the network perimeter and can handle dropping a lot of the non- legitimate traffic (attacks, scans etc.) very quickly at the ingress interface, often in hardware.
An IDS/IPS is, generally speaking, doing more deep packet inspections and that is a much more computationally expensive undertaking. For that reason, we prefer to filter what gets to it with the firewall line of defense before engaging the IDS/IPS to analyze the traffic flow.
Source: https://supportforums.cisco.com/discussion/12428821/correct-placement-idsips-network-architecture

NEW QUESTION 141
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

NEW QUESTION 142
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

NEW QUESTION 144
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

NEW QUESTION 148

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

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

Answer: C

Explanation: The IKE protocol uses UDP packets, usually on port 500
NAT traversal: The encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing NAT
Source: https://en.wikipedia.org/wiki/Internet_Key_Exchange

NEW QUESTION 151
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 153
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 154
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

NEW QUESTION 158
Which Sourcefire logging action should you choose to record the most detail about a connection?

A. Enable logging at the end of the session.
B. Enable logging at the beginning of the session.
C. Enable alerts via SNMP to log events off-box.
D. Enable eStreamer to log events off-box.

Answer: A

Explanation: FirePOWER (former Sourcefire)
Logging the Beginning And End of Connections

When the system detects a connection, in most cases you can log it at its beginning and its end.
For a single non-blocked connection, the end-of-connection event contains all of the information in the beginning-of-connection event, as well as information gathered over the duration of the session.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower- module-user-guide-v541/AC-Connection-Logging.html#15726

Topic 2, Exam Pool B

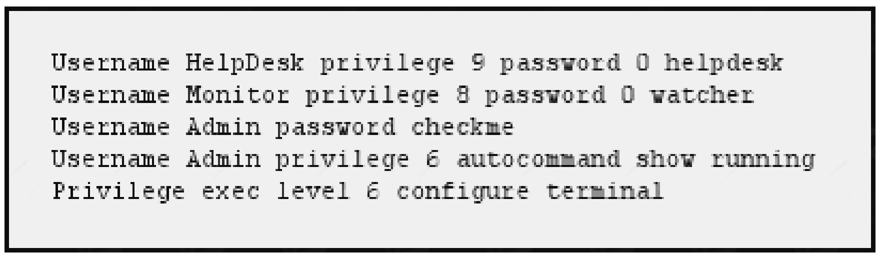
NEW QUESTION 162
Which security measures can protect the control plane of a Cisco router? (Choose two.)

A. CCPr
B. Parser views
C. Access control lists
D. Port security
E. CoPP

Answer: AE

Explanation: Three Ways to Secure the Control Plane
+ Control plane policing (CoPP): You can configure this as a filter for any traffic destined to an IP address on the router itself.
+ Control plane protection (CPPr): This allows for a more detailed classification of traffic (more than CoPP) that is going to use the CPU for handling.
+ Routing protocol authentication
For example, you could decide and configure the router to believe that SSH is acceptable at 100 packets per second, syslog is acceptable at 200 packets per second, and so on. Traffic that exceeds the thresholds can be safely dropped if it is not from one of your specific management stations.
You can specify all those details in the policy.
You learn more about control plane security in Chapter 13, “Securing Routing Protocols and the Control Plane.”
Selective Packet Discard (SPD) provides the ability to Although not necessarily a security feature, prioritize certain types of packets (for example, routing protocol packets and Layer 2 keepalive messages, route processor [RP]). SPD provides priority of critical control plane traffic which are received by the over traffic that is less important or, worse yet, is being sent maliciously to starve the CPU of resources required for the RP.
Source: Cisco Official Certification Guide, Table 10-3 Three Ways to Secure the Control Plane , p.269

NEW QUESTION 167
Refer to the exhibit.



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

The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

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

Answer: A

NEW QUESTION 171
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 174
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
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)

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

Answer: ABC

Explanation: Cisco Official Certification Guide, Table 3-2 TACACS+ Versus RADIUS, p.40

NEW QUESTION 183
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

NEW QUESTION 188
Which IPS mode provides the maximum number of actions?

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

Answer: A

Explanation: The first option is to put a sensor inline with the traffic, which just means that any traffic going through your network is forced to go in one physical or logical port on the sensor.
Because the sensor is inline with the network, and because it can drop a packet and deny that packet from ever reaching its final destination (because it might cause harm to that destination), the sensor has in fact just prevented that attack from being carried out. That is the concept behind intrusion prevention systems (IPS).
Whenever you hear IPS mentioned, you immediately know that the sensor is inline with the traffic, which makes it possible to prevent the attack from making it further into the network.
Source: Cisco Official Certification Guide, Difference Between IPS and IDS, p.460

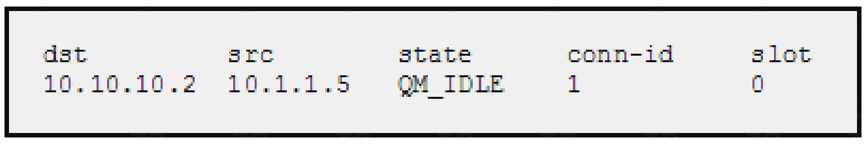
NEW QUESTION 189
Which type of encryption technology has the broadest platform support to protect operating systems?

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

Answer: A

Explanation: Much commercial and free software enables you to encrypt files in an end-user workstation or mobile device. The following are a few examples of free solutions:
+ GPG: GPG also enables you to encrypt files and folders on a Windows, Mac, or Linux system. GPG is free.
+ The built-in MAC OS X Disk Utility: D isk Utility enables you to create secure disk images by encrypting files with AES 128-bit or AES 256-bit encryption.
+ TrueCrypt: A free encryption tool for Windows, Mac, and Linux systems.
+ AxCrypt: A f ree Windows-only file encryption tool.
+ BitLocker: Full disk encryption feature included in several Windows operating systems.
+ Many Linux distributions such as Ubuntu: A llow you to encrypt the home directory of a user with built-in utilities.
+ MAC OS X FileVault: Supports full disk encryption on Mac OS X systems. The following are a few examples of commercial file encryption software:
+ Symantec Endpoint Encryption
+ PGP Whole Disk Encryption
+ McAfee Endpoint Encryption (SafeBoot)
+ Trend Micro Endpoint Encryption
Source: Cisco Official Certification Guide, Encrypting Endpoint Data at Rest, p.501

NEW QUESTION 194
Refer to the exhibit.



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

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

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

Answer: A

NEW QUESTION 195
What mechanism does asymmetric cryptography use to secure data?

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

Answer: A

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

NEW QUESTION 200
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 205
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 206
Which three statements describe DHCP spoofing attacks? (Choose three.)

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

Answer: ABC

Explanation: DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
Source: https://learningnetwork.cisco.com/thread/67229 https://learningnetwork.cisco.com/docs/DOC-24355

Also when i took the exam, it asked me for only 2 options. AB is correct

NEW QUESTION 209
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

NEW QUESTION 214
Which statement provides the best definition of malware?

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

Answer: A

Explanation: Malware, short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.[1] Before the term malware was coined by Yisrael Radai in 1990, malicious software was referred to as computer viruses.
Source: https://en.wikipedia.org/wiki/Malware

NEW QUESTION 219
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 222
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

NEW QUESTION 223
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 225
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

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

Answer: ABD

Explanation: https://supportforums.cisco.com/discussion/11809846/asa-5505-using-nat-allowing-incoming-traffic-https
https://supportforums.cisco.com/discussion/12473551/asa-what-allowing-return-http-traffic

NEW QUESTION 226
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 227
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 228
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

NEW QUESTION 233
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 236
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 238
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 242
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 245
A data breach has occurred and your company database has been copied. Which security principle has been violated?

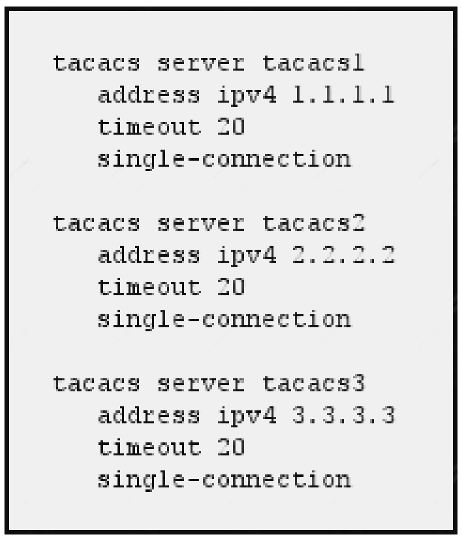
A. confidentiality
B. availability
C. access
D. control

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 246
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
```

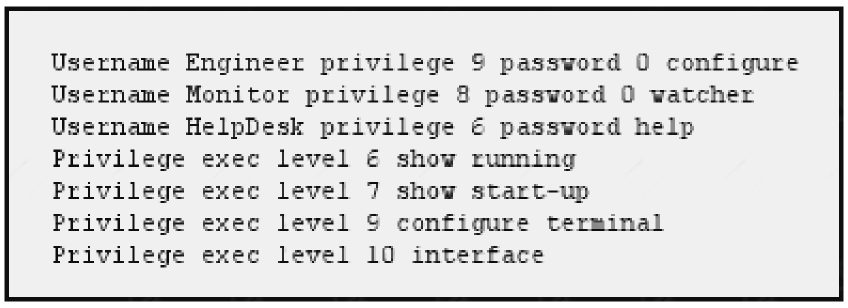
Which statement about the given configuration is true?

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

NEW QUESTION 248
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 251
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

NEW QUESTION 255
How can FirePOWER block malicious email attachments?

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

Answer: C

Explanation: A file policy is a set of configurations that the system uses to perform advanced malware protection and file control, as part of your overall access control configuration.
A file policy, like its parent access control policy, contains rules that determine how the system handles files that match the conditions of each rule. You can configure separate file rules to take different actions for different file types, application protocols, or directions of transfer.
You can associate a single file policy with an access control rule whose action is Allow, Interactive Block, or Interactive Block with reset. The system then uses that file policy to inspect network traffic that meets the conditions of the access control rule.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower- module-user-guide-v541/AMP-Config.html

NEW QUESTION 256
Which of the following statements about access lists are true? (Choose three.)

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

Answer: BCE

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 then Standard ACL.
2) You can filter packets by Host/Subnet as well as Protocol/TCPPort/UDPPort.
3) Best Practice is put restriction near form Destination Host/Subnet. (Interface-Outbound)

Topic 3, Exam Pool C

NEW QUESTION 260
ACisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0.
By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

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

Answer: ABCGH

Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html
Security Level
Overview
Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between Interfaces on the Same Security Level" section for more information.
The level controls the following behavior:
•Network access — By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface. If you enable communication for same security interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.
•Inspection engines — Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
–NetBIOS inspection engine—Applied only for outbound connections.
–OraServ inspection engine — If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
•Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).
For same security interfaces, you can filter traffic in either direction.

•NAT control — When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).
Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.
•established command — This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.
For same security interfaces, you can configure established commands for both directions.

NEW QUESTION 262
Which ports must be open between a AAA server and a Microsoft server to permit active directory authentication?

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

Answer: A

NEW QUESTION 265
Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

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

Answer: D

Explanation: :
Reference: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/objectgroups.html
Information About Object Groups
By grouping like objects together, you can use the object group in an ACE instead of having to enter an ACE for each object separately. You can create the following types of object groups:
•Protocol
•Network
•Service
•ICMP type
For example, consider the following three object groups:
•MyServices — Includes the TCP and UDP port numbers of the service requests that are allowed access to the internal network.
•TrustedHosts — Includes the host and network addresses allowed access to the greatest range of services and servers.
•PublicServers — Includes the host addresses of servers to which the greatest access is provided.
After creating these groups, you could use a single ACE to allow trusted hosts to make specific service requests to a group of public servers.
You can also nest object groups in other object groups.

NEW QUESTION 267
Command ip ospf authentication key 1 is implemented in which level.

A. Interface
B. process
C. global
D. enable

Answer: A

Explanation: Use the ip ospf authentication-key interface command to specify this password. If you enable MD5 authentication with the message-digest keyword, you must configure a password with the ip ospf message- digest-key interface command.
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNA
Source: Cisco Official Certification Guide, Implement Routing Update Authentication on OSPF, p.348 The OSPFv2 Cryptographic Authentication feature allows you to configure a key chain on the OSPF interface to authenticate OSPFv2 packets by using HMAC-SHA algorithms. You can use an existing key chain that is being used by another protocol, or you can create a key chain specifically for OSPFv2.
If OSPFv2 is configured to use a key chain, all MD5 keys that were previously configured using the ip ospf message-digest-key command are ignored.
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/0
Device (config-if)# ip ospf authentication key-chain sample1 Device (config-if)# end
Source:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro- ospfv2-crypto-authen-xe.html
In both cases OSPF and OSPFv1 the ip ospf authentication is inserted at interface level

NEW QUESTION 270
Which two features of Cisco Web Reputation tracking can mitigate web-based threats? (Choose Two)

A. outbreak filter

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

Answer: AD

Explanation: Cisco IronPort Outbreak Filters provide a critical first layer of defense against new outbreaks. With this proven preventive solution, protection begins hours before signatures used by traditional antivirus solutions are in place. Real-world results show an average 14-hour lead time over reactive antivirus solutions. SenderBase, the world's largest email and web traffic monitoring network, provides real-time protection. The Cisco IronPort SenderBase Network captures data from over 120,000 contributing organizations around the world.
Source: http://www.cisco.com/c/en/us/products/security/email-security-appliance/outbreak_filters_index.html

NEW QUESTION 275
Which two statements about the self zone on Cisco zone based policy firewall are true ? (Choose two)

A. multiple interfaces can be assigned to the self zone .
B. traffic entering the self zone must match a rule.
C. zone pairs that include the self zone apply to traffic transiting the device.
D. it can be either the source zone or destination zone .
E. it supports statefull inspection for multicast traffic

Answer: AD

NEW QUESTION 278
When setting up a site-to-site VPN with PSK authentication on a Cisco router, which two elements must be configured under crypto map? (Choose two.)

A. nat
B. transform-set
C. reverse-route
D. peer
E. pfs

Answer: BD

NEW QUESTION 281
Within an 802.1X enabled network with the Auth Fail feature configured, when does a switch port get placed into a restricted VLAN?

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

Answer: C

NEW QUESTION 282
On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

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

Answer: B

Explanation: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4e Step 1: Downloading IOS IPS files The first step is to download IOS IPS signature package files and public crypto key from Cisco.com. Step 1.1: Download the required signature files from Cisco.com to your PC
• Location: http://tools.cisco.com/support/downloads/go/Model.x?mdfid=281442967
&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Preventio
• Files to download:
IOS-Sxxx-CLI.pkg: Signature package - download the latest signature package.
realm-cisco.pub.key.txt: Public Crypto key - this is the crypto key used by IOS IPS

NEW QUESTION 287
What port option in a PVLAN that can communicate with every other port?

A. Promiscuous ports
B. Community ports
C. Ethernet ports
D. Isolate ports

Answer: A

Explanation: + Promiscuous -- A promiscuous port belongs to the primary VLAN. 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 -- An isolated port is a host port that belongs to an isolated secondary VLAN. 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 Source: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html

NEW QUESTION 291

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

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

Answer: A

NEW QUESTION 294

Which type of encryption technology has the broadcast platform support?

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

Answer: C

NEW QUESTION 299

What encryption technology has broadest platform support

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

Answer: C

NEW QUESTION 300

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

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

Answer: CE

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

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

```
aaa authentication ppp test group tacacs+ local tacacs-server host 10.1.2.3
tacacs-server key goaway interface serial 0
ppp authentication chap pap test
```

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

•The aaa new-model command enables the AAA security services.

•The aaa authentication command defines a method list, "test," to be used on serial interfaces running PPP. The keyword group tacacs+ means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword local indicates that authentication will be attempted using the local database on the network access server.

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml

Authentication Start to configure TAC+ on the router.

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

```
!--- Turn on TAC+. aaa new-model
enable password whatever
!--- These are lists of authentication methods.
!--- "linmethod", "vtymethod", "conmethod", and
!--- so on are names of lists, and the methods
!--- listed on the same lines are the methods
!--- in the order to be tried. As used here, if
!--- authentication fails due to the
!--- tac_plus_executable not being started, the
!--- enable password is accepted because
!--- it is in each list.
!
```

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

NEW QUESTION 302
With which technology do apply integrity, confidentially and authenticate the source

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

Answer: A

Explanation: IPsec is a collection of protocols and algorithms used to protect IP packets at Layer 3 (hence the name of IP Security [IPsec]). IPsec provides the core benefits of confidentiality through encryption, data integrity through hashing and HMAC, and authentication using digital signatures or using a pre-shared key (PSK) that is just for the authentication, similar to a password.
Source: Cisco Official Certification Guide, IPsec and SSL, p.97

NEW QUESTION 307
What is example of social engineering

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

Answer: C

NEW QUESTION 308
......