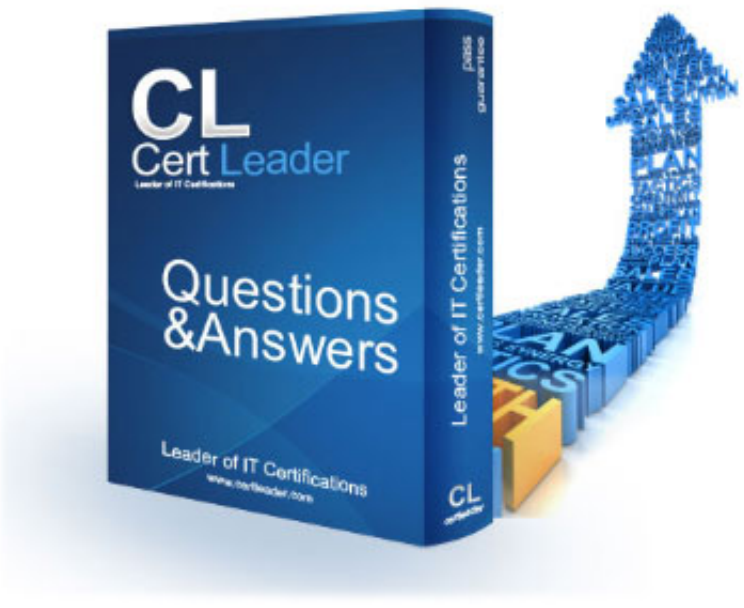
210-260 Dumps

Implementing Cisco Network Security

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



NEW QUESTION 1
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

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

Answer: A

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

NEW QUESTION 2
What is the Cisco preferred countermeasure to mitigate CAM overflows?

A. Port security
B. Dynamic port security
C. IP source guard
D. Root guard

Answer: B

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

NEW QUESTION 3
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor

Answer: D

Explanation: Health and Performance Monitor (HPM) • Monitors and displays key health, performance and VPN data for ASA and IPS devices in your network. This information includes critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. You also can categorize devices for normal or priority monitoring, and set different alert rules for the priority devices.
Source:
http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/HPMchap.pdf

NEW QUESTION 4
If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?

A. The trunk port would go into an error-disabled state.
B. A VLAN hopping attack would be successful.
C. A VLAN hopping attack would be prevented.
D. The attacked VLAN will be pruned.

Answer: C

Explanation: VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.
Double Tagging can only be exploited when switches use "Native VLANs". Double Tagging can be mitigated by either one of the following actions:
+ Simply do not put any hosts on VLAN 1 (The default VLAN)
+ Change the native VLAN on all trunk ports to an unused VLAN ID Source: https://en.wikipedia.org/wiki/VLAN_hopping

NEW QUESTION 5
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.
D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59:00 local time on December 31, 2013.
E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the

key indefinitely.
F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Answer: B

Explanation: #secure boot-image
This command enables or disables the securing of the running Cisco IOS image. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk.
Source:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s1.html#wp3328121947

NEW QUESTION 6
Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?

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

Answer: D

Explanation: The no switchport command makes the interface Layer 3 capable.
Source:
http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

NEW QUESTION 7
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Only control plane policing can protect the control plane against multicast traffic.
B. Stateful inspection of multicast traffic is supported only for the self-zone.
C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
D. Stateful inspection of multicast traffic is supported only for the internal zone.

Answer: A

Explanation: Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic. So the only choice is A.
Source: http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

NEW QUESTION 8
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

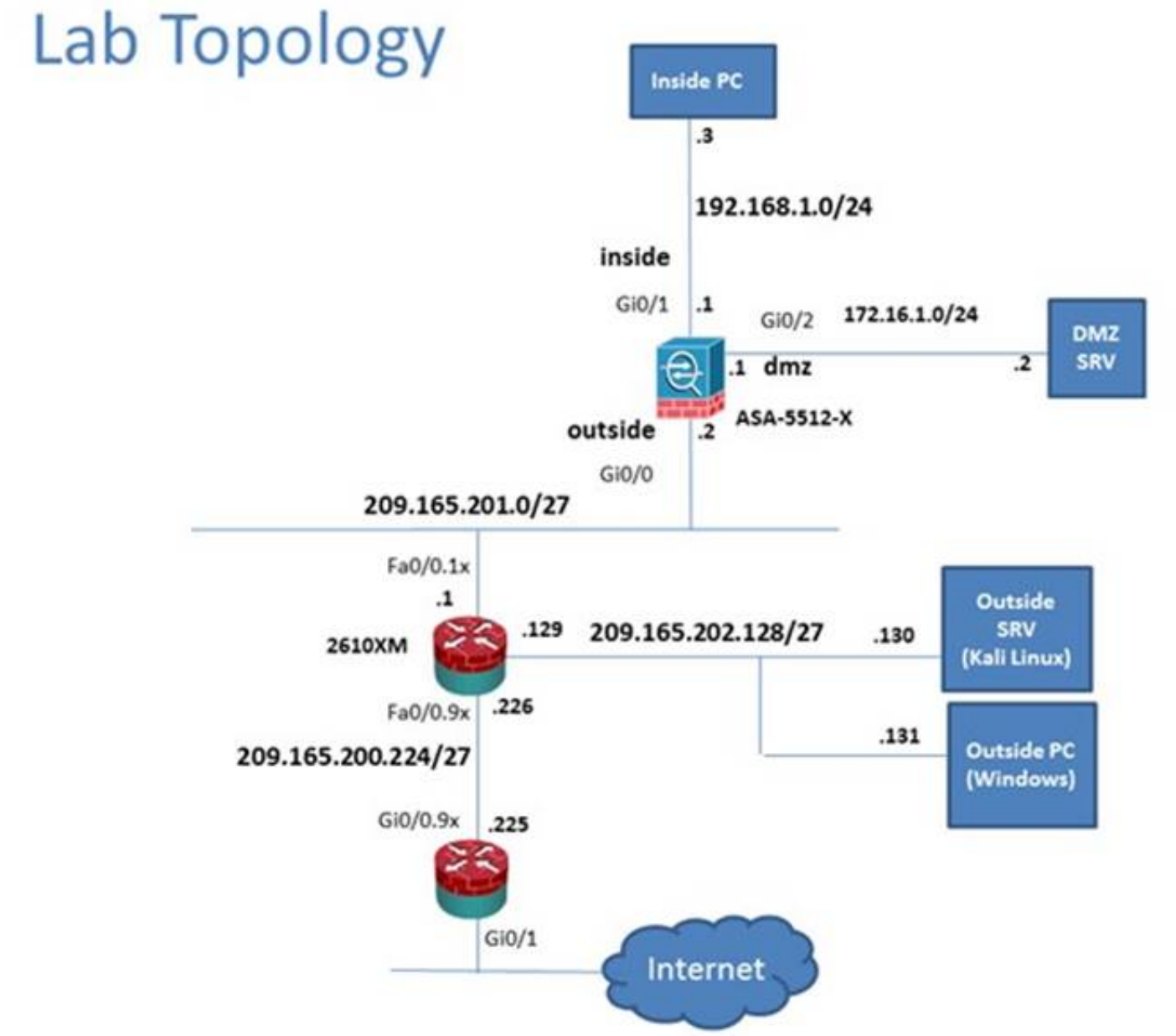
NEW QUESTION 9
What features can protect the data plane? (Choose three.)

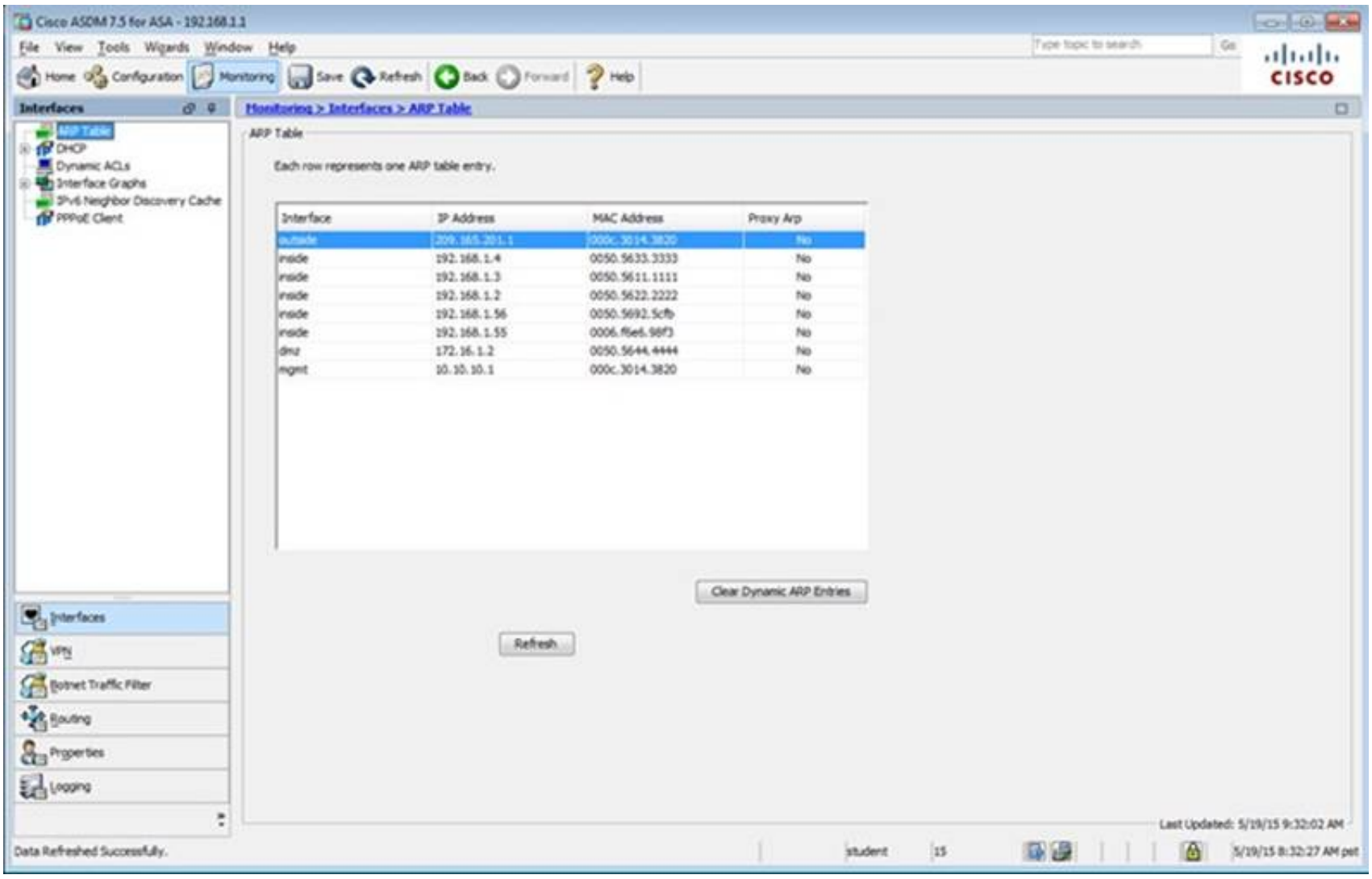
A. policing
B. ACLs
C. IPS
D. antispoofing
E. QoS
F. DHCP-snooping

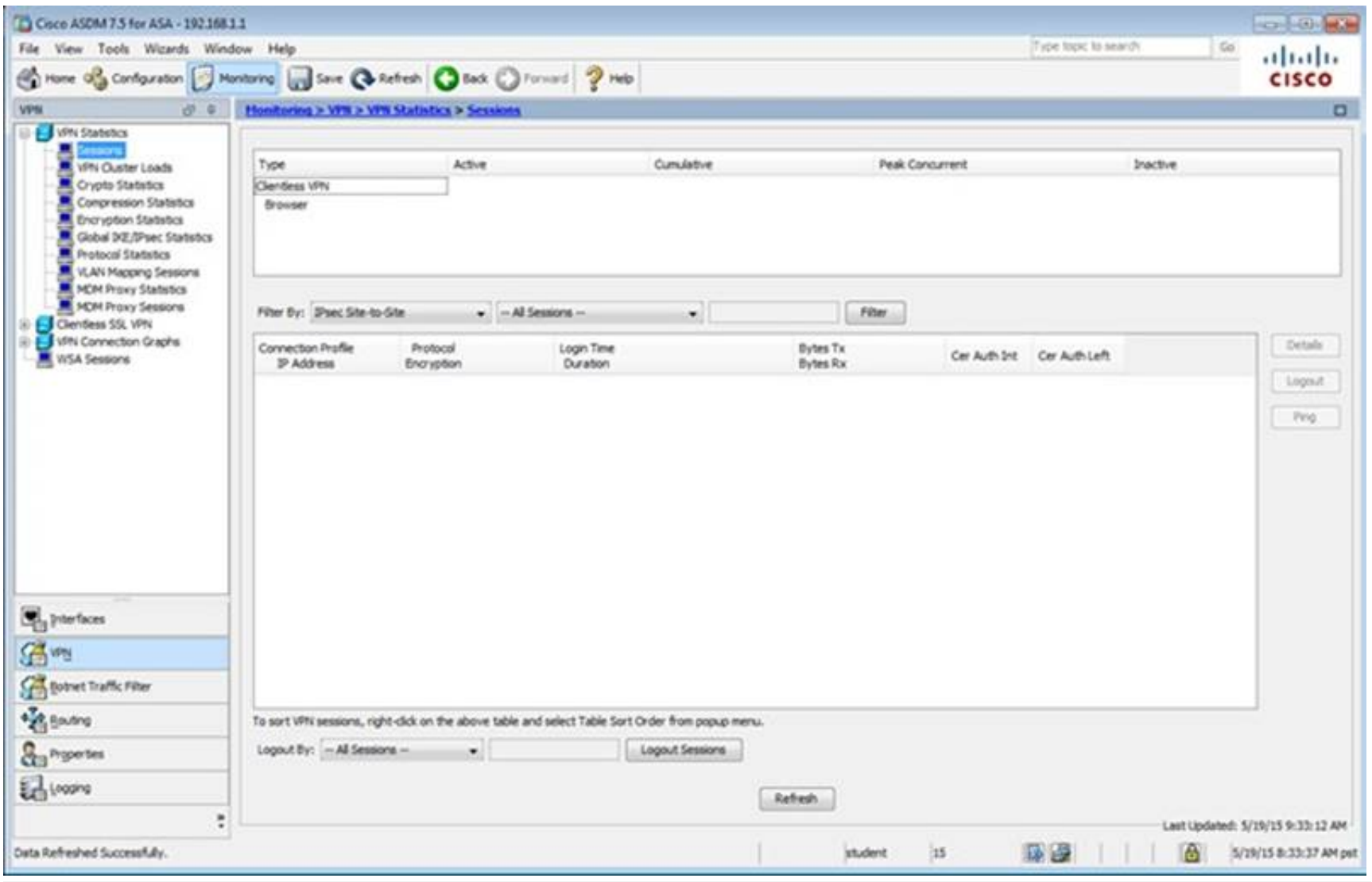
Answer: BDF

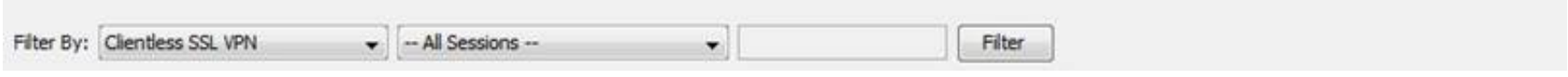
Explanation: + Block unwanted traffic at the router. If your corporate policy does not allow TFTP traffic, just implement ACLs that deny traffic that is not allowed.
+ Reduce spoofing attacks. For example, you can filter (deny) packets trying to enter your network (from the outside) that claim to have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

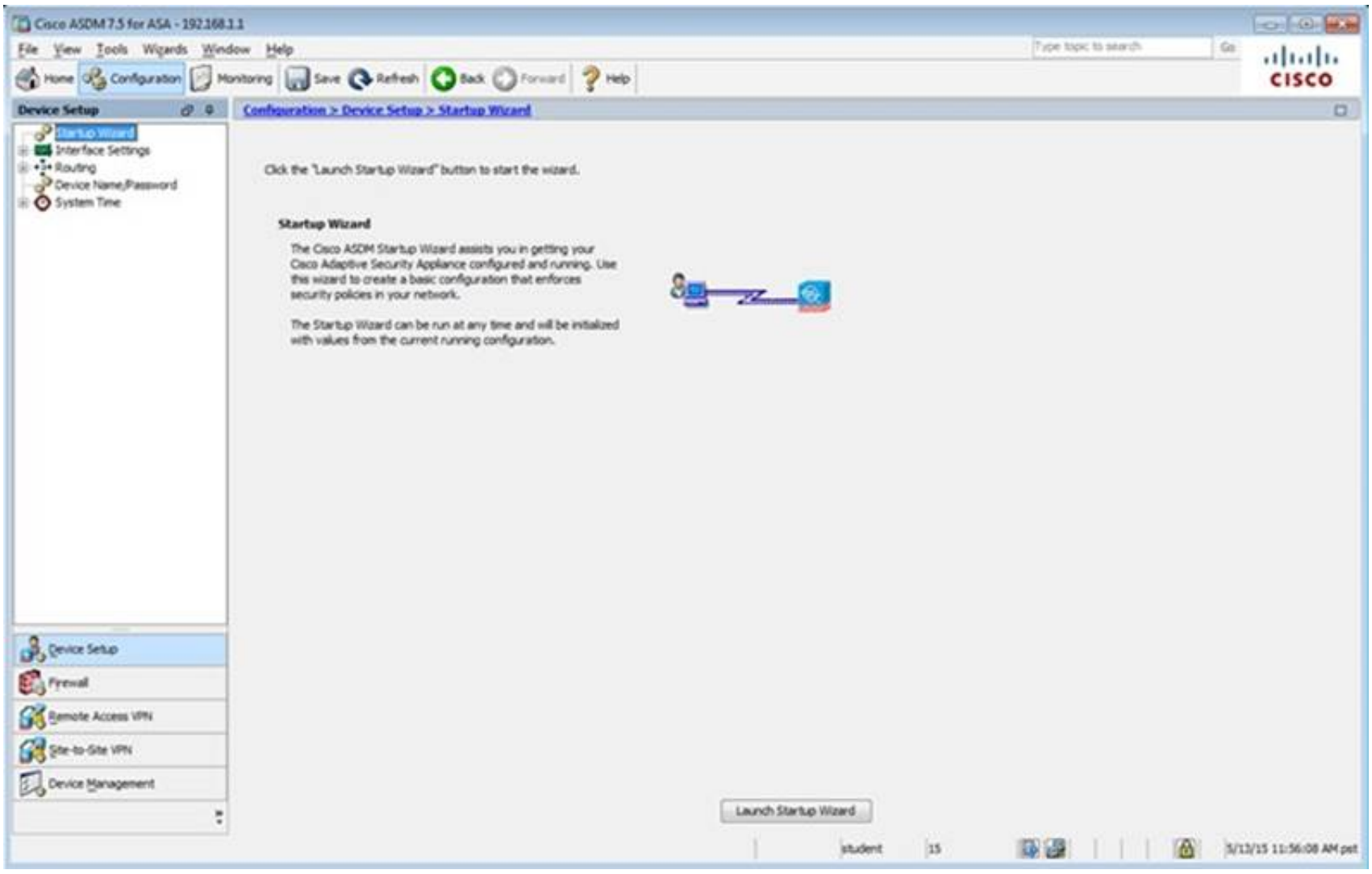
NEW QUESTION 10
Scenario
Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.
New additional connectivity requirements:
Once the correct ASA configurations have been configured: To access ASDM, click 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.

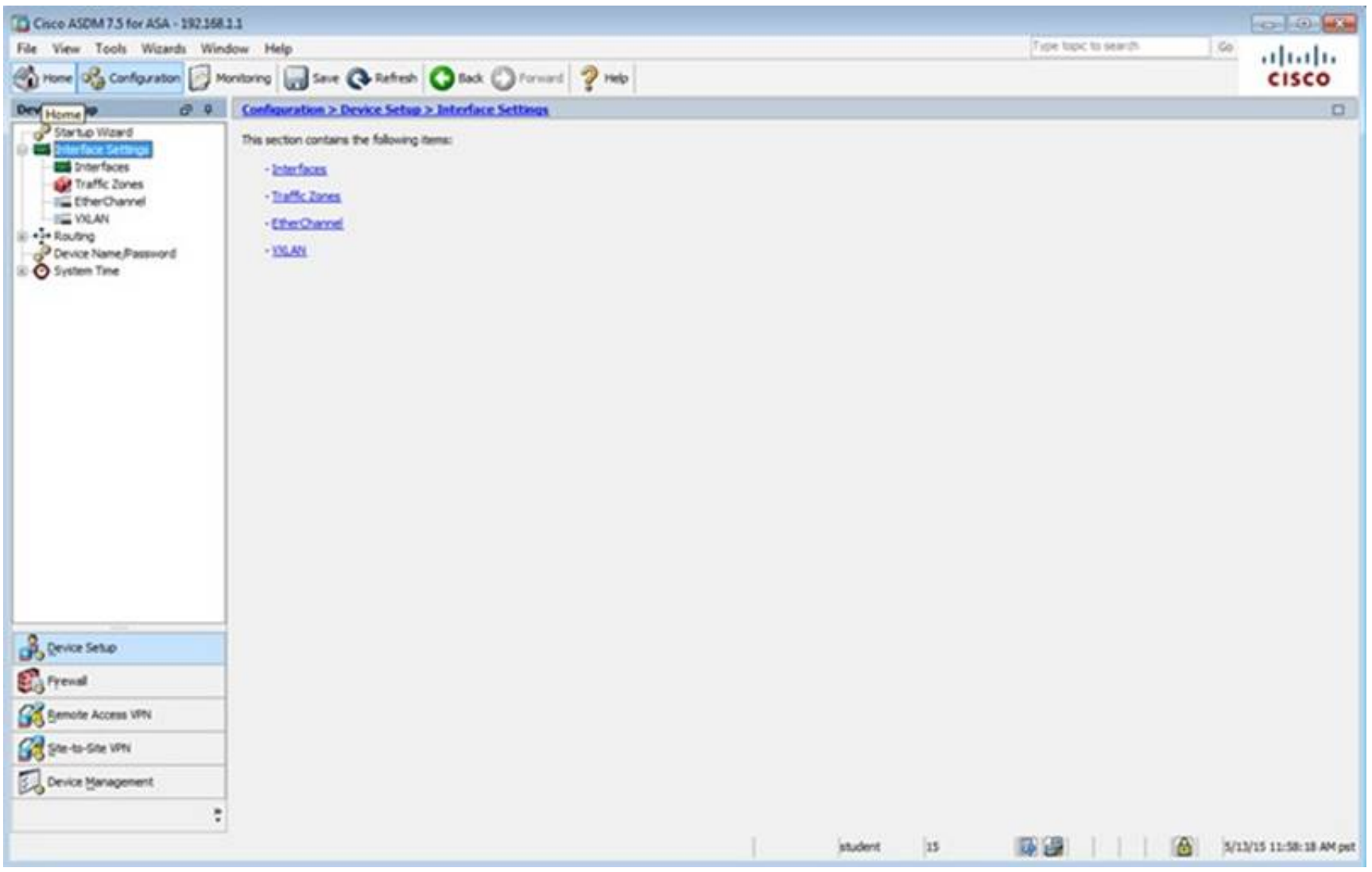


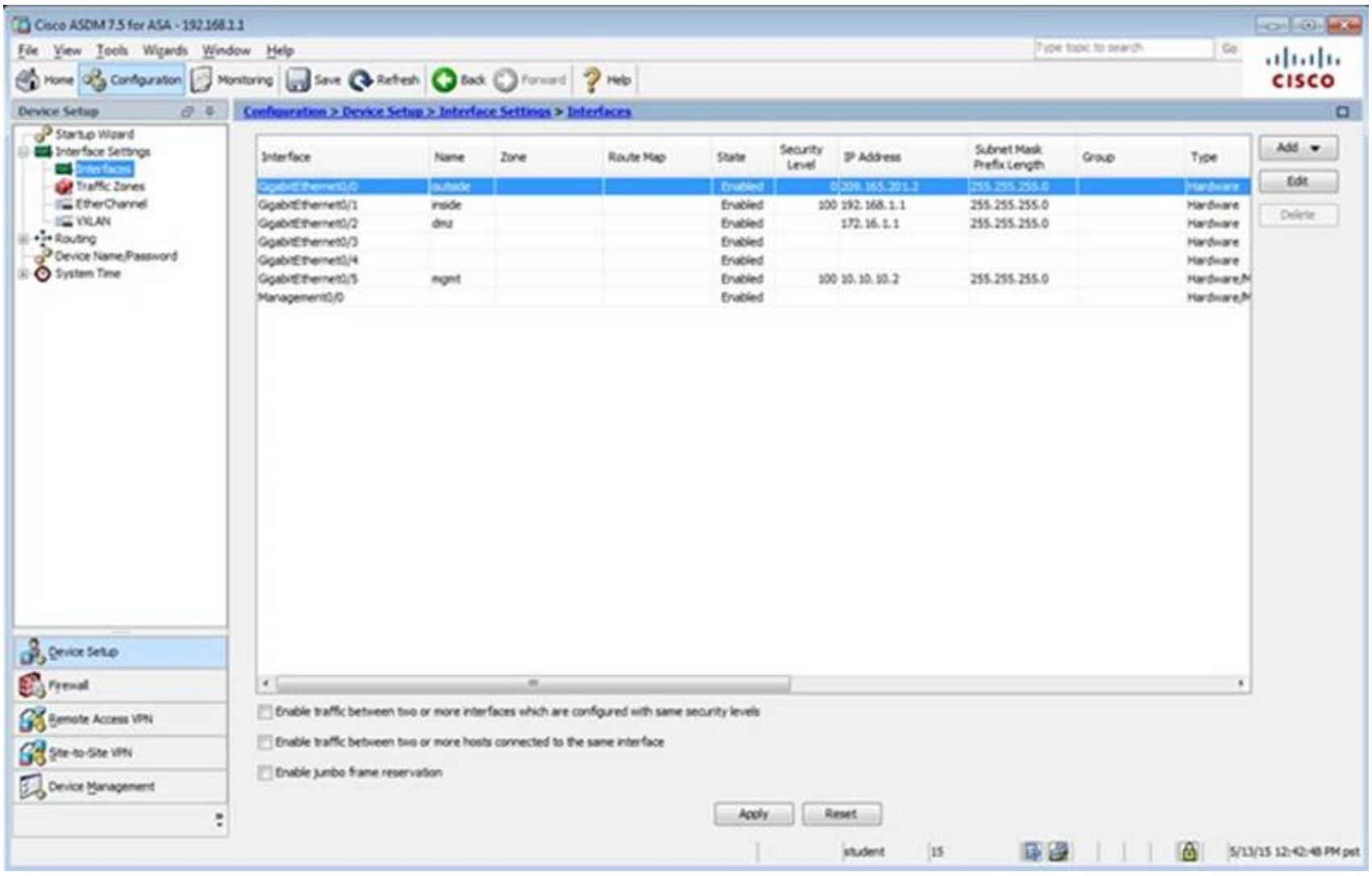

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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
Clear Dynamic ARP Entries
Refresh
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Last Updated: 5/19/15 9:32:02 AM
Data Refreshed Successfully.
student 15
5/19/15 8:32:27 AM pst

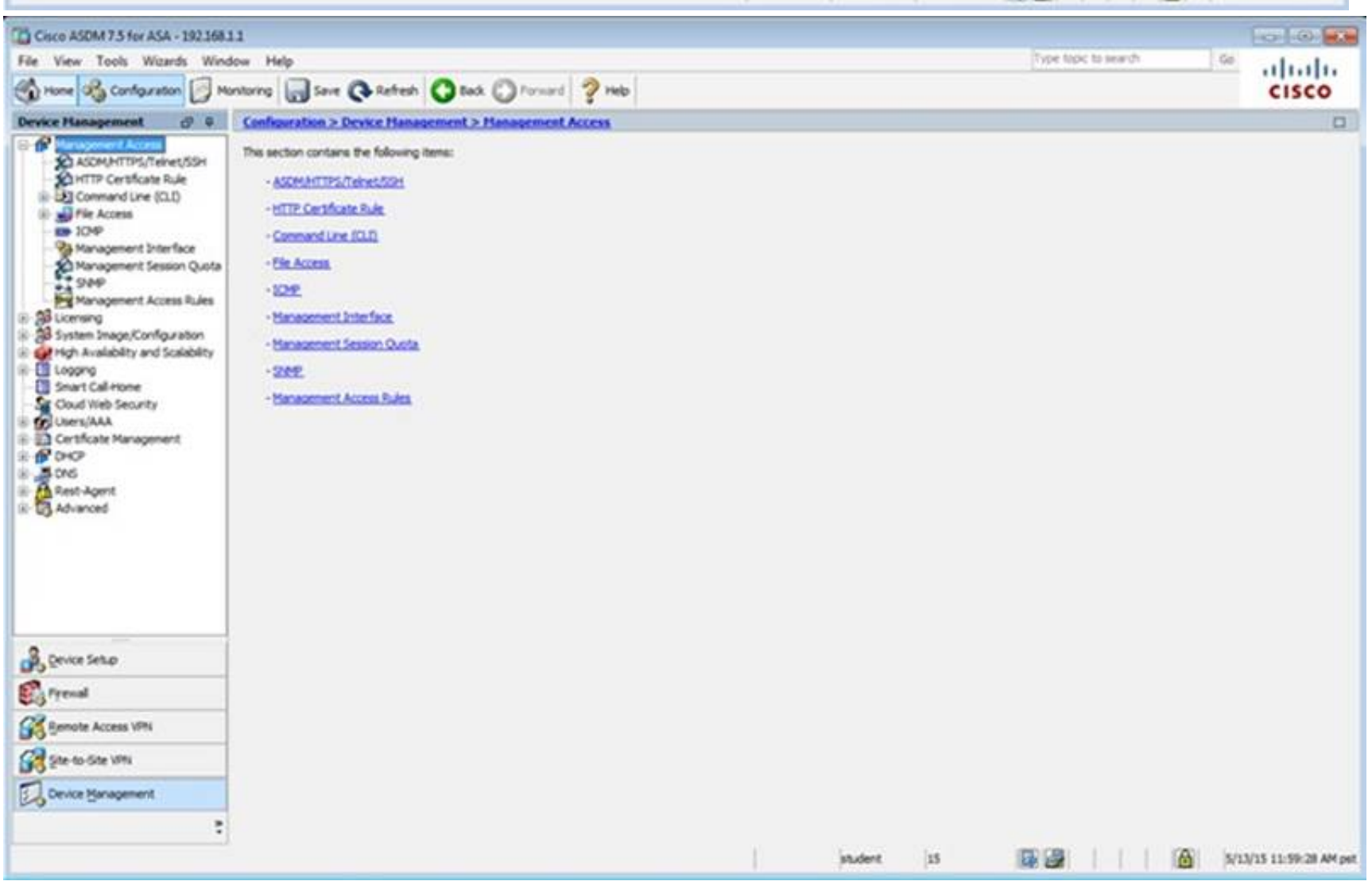

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN Mapping Sessions
MDM Proxy Statistics
MDM Proxy Sessions
Clientless SSL VPN
VPN Connection Graphs
WSA Sessions
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
Details
Logout
Ping
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.
Logout By: -- All Sessions -- Logout Sessions
Refresh
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Last Updated: 5/19/15 9:33:12 AM
Data Refreshed Successfully.
student 15
5/19/15 8:33:37 AM pst

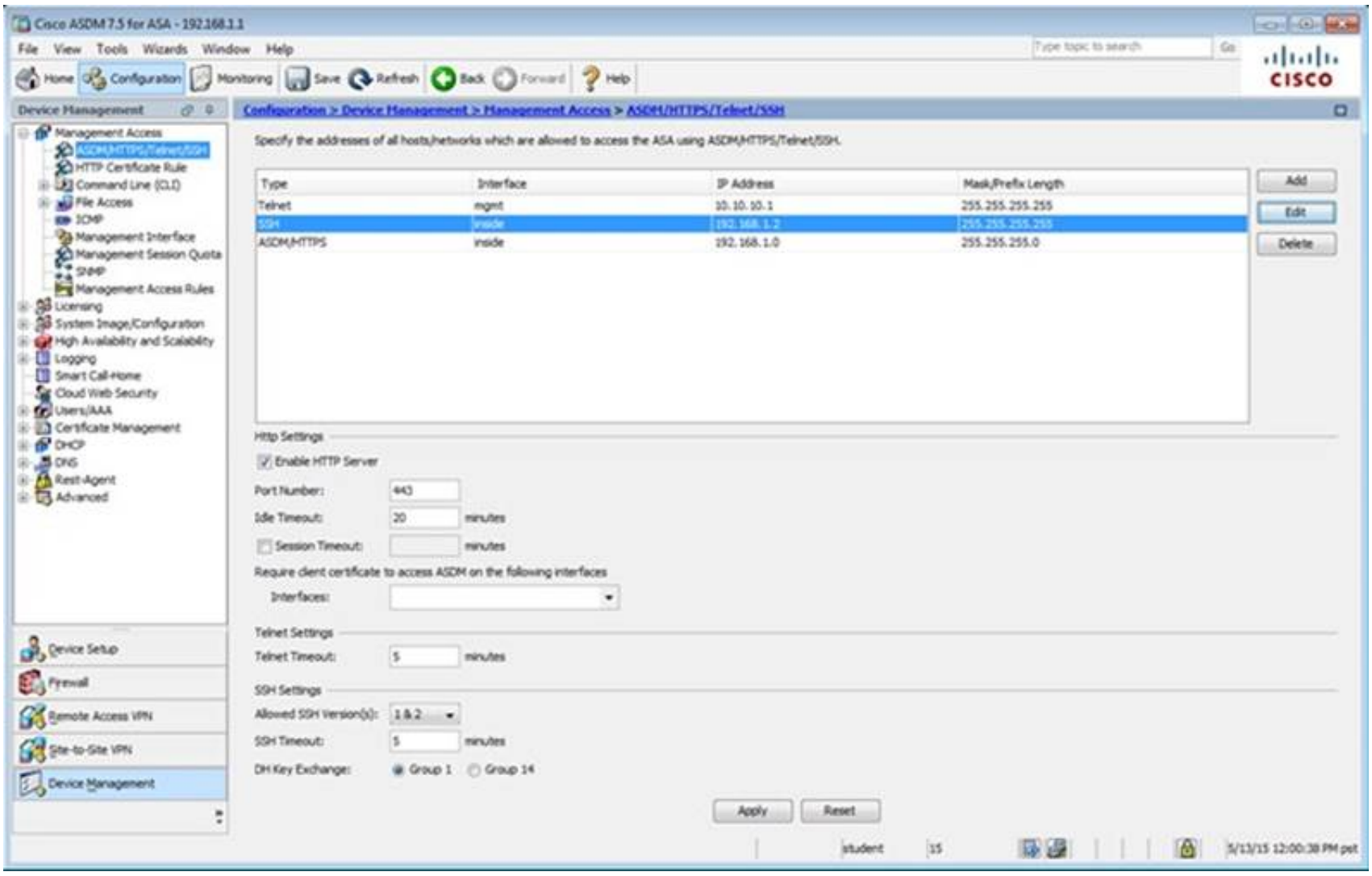

Filter By: Clientless SSL VPN -- All Sessions -- Filter

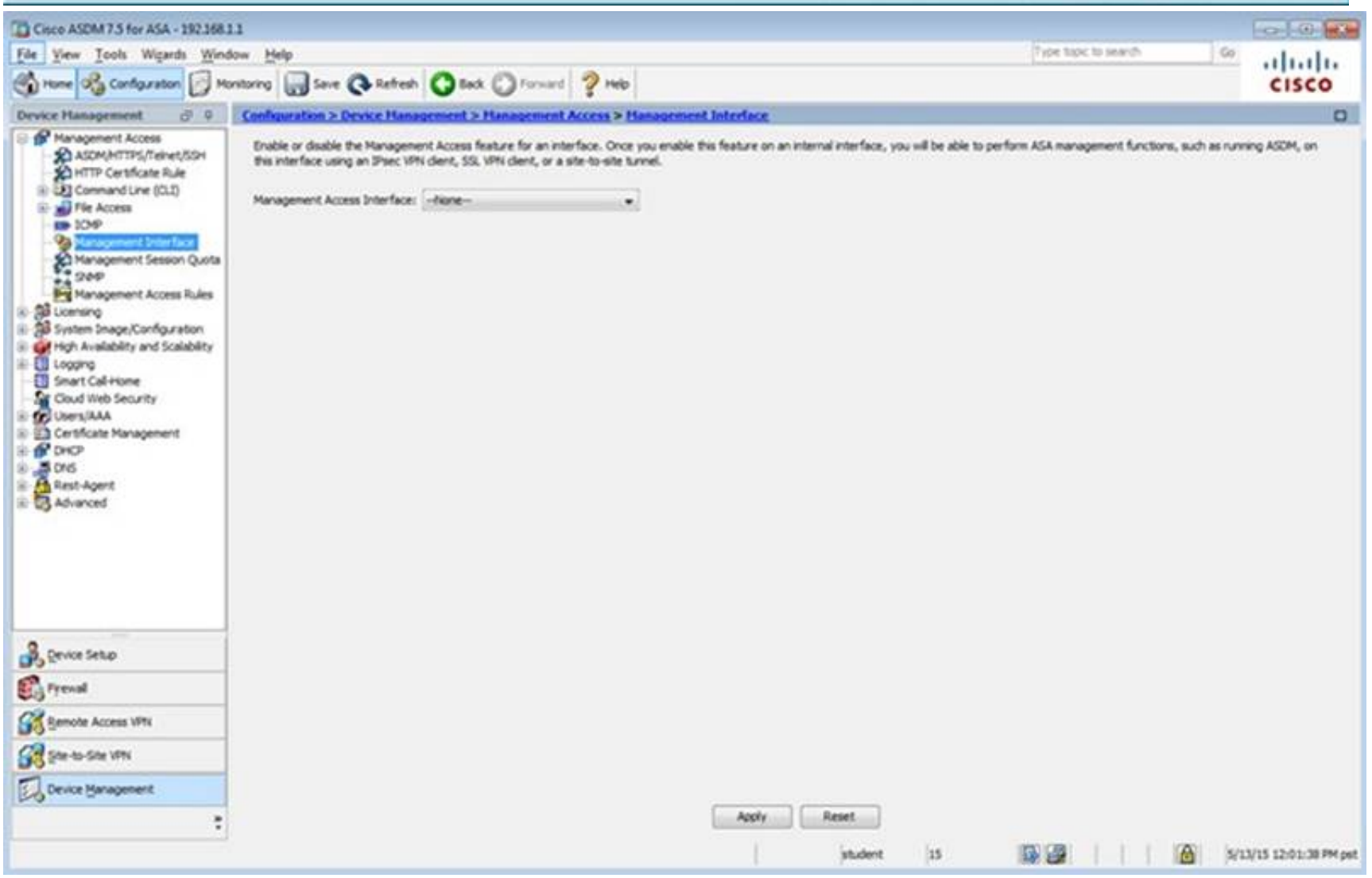

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" 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 the wizard to create a basic configuration that enforces security policies in your network.
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.
Launch Startup Wizard
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 11:56:08 AM pst

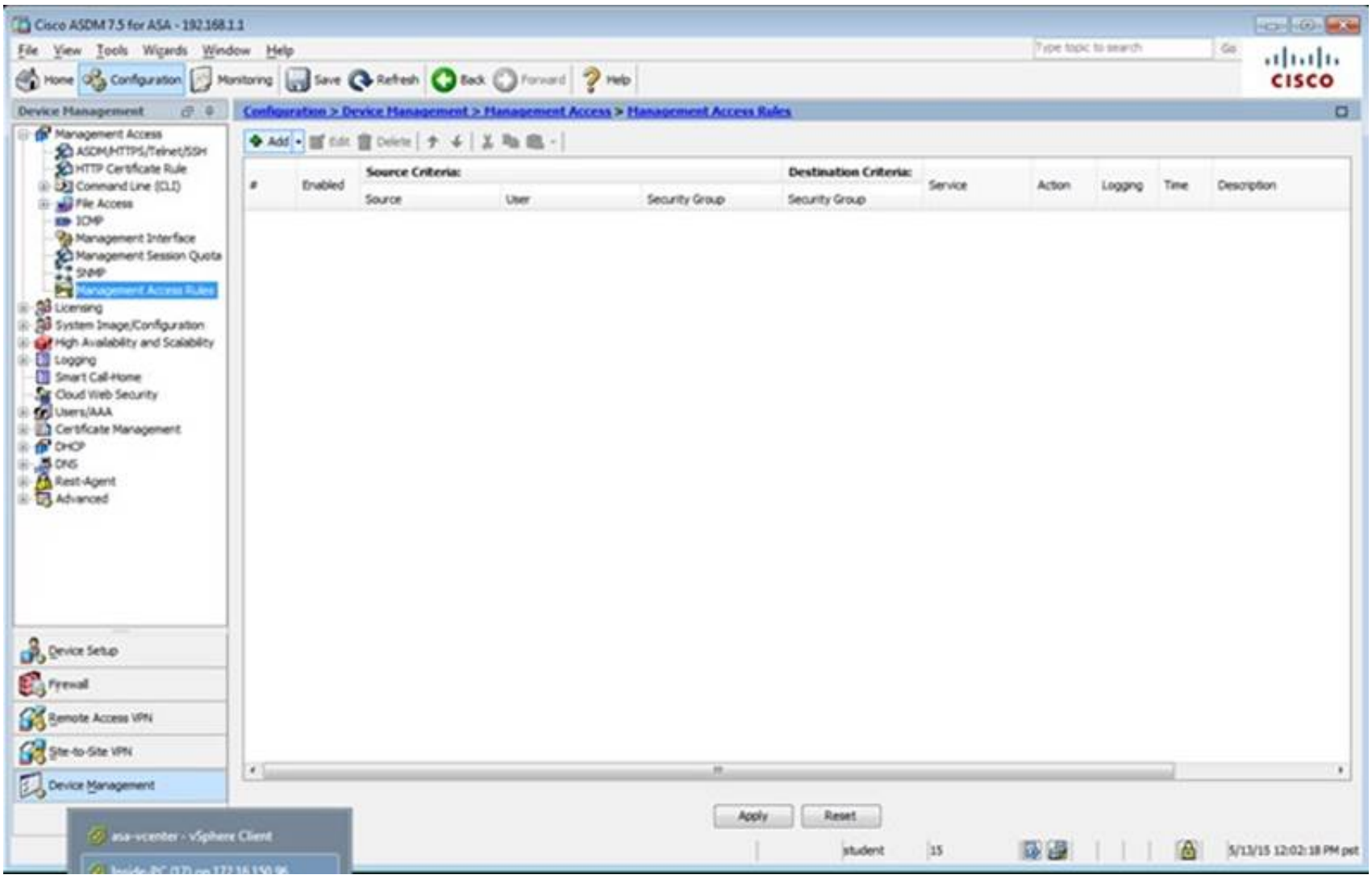

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interface Settings
This section contains the following items:
- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 11:58:18 AM pst

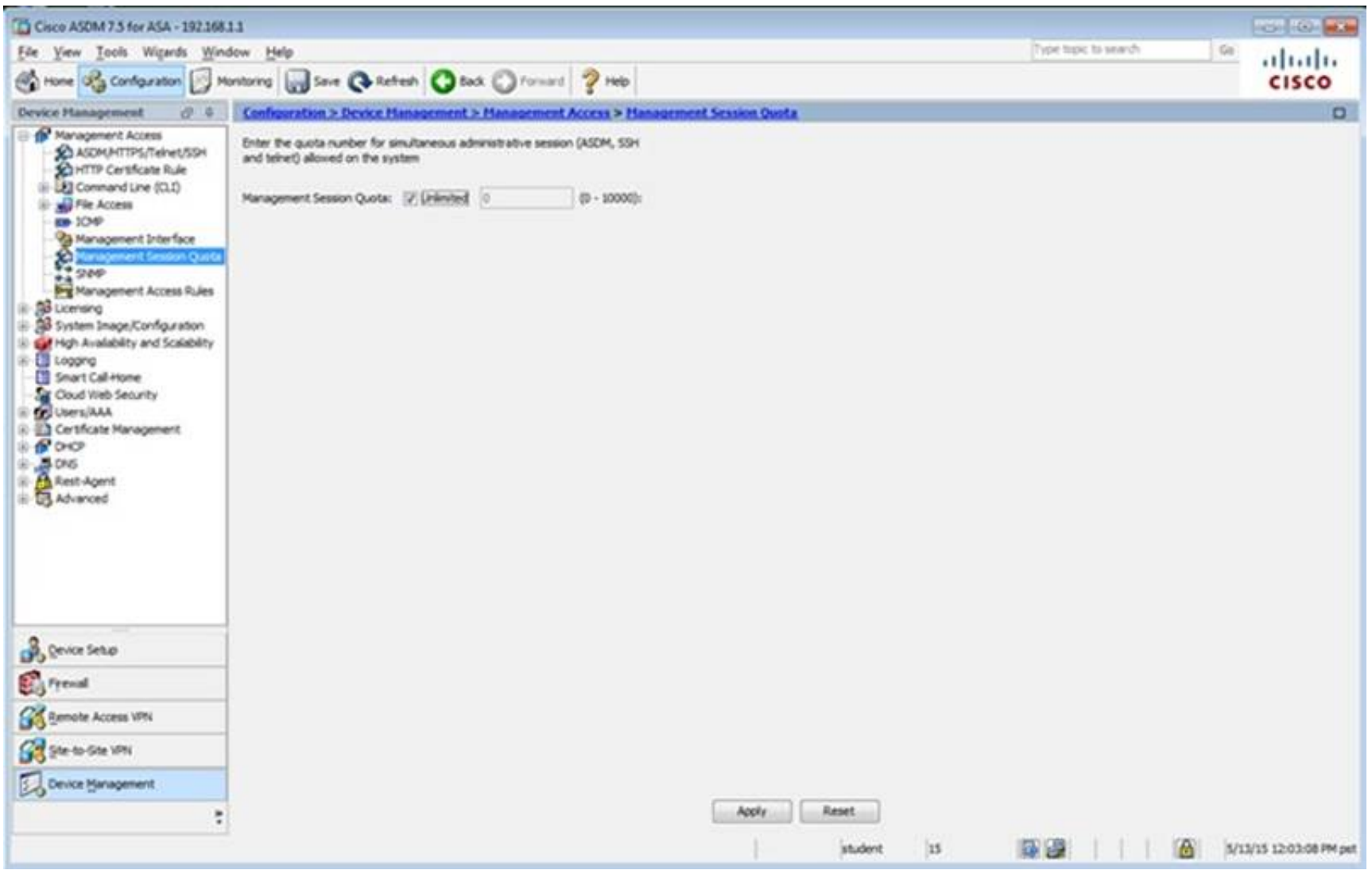

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Configuration > Device Setup > Interface Settings > Interfaces
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Interface Name Zone Route Map State Security Level IP Address Subnet Mask Prefix Length Group Type
GigabitEthernet0/0 outside Enabled 0 209.165.201.2 255.255.255.0 Hardware
GigabitEthernet0/1 inside Enabled 100 192.168.1.1 255.255.255.0 Hardware
GigabitEthernet0/2 dmz Enabled 172.16.1.1 255.255.255.0 Hardware
GigabitEthernet0/3 Enabled Hardware
GigabitEthernet0/4 Enabled Hardware
GigabitEthernet0/5 mgmt Enabled 100 10.10.10.2 255.255.255.0 Hardware
Management0/0 Enabled Hardware
Add
Edit
Delete
Enable traffic between two or more interfaces which are configured with same security levels
Enable traffic between two or more hosts connected to the same interface
Enable jumbo frame reservation
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 12:42:48 PM pst

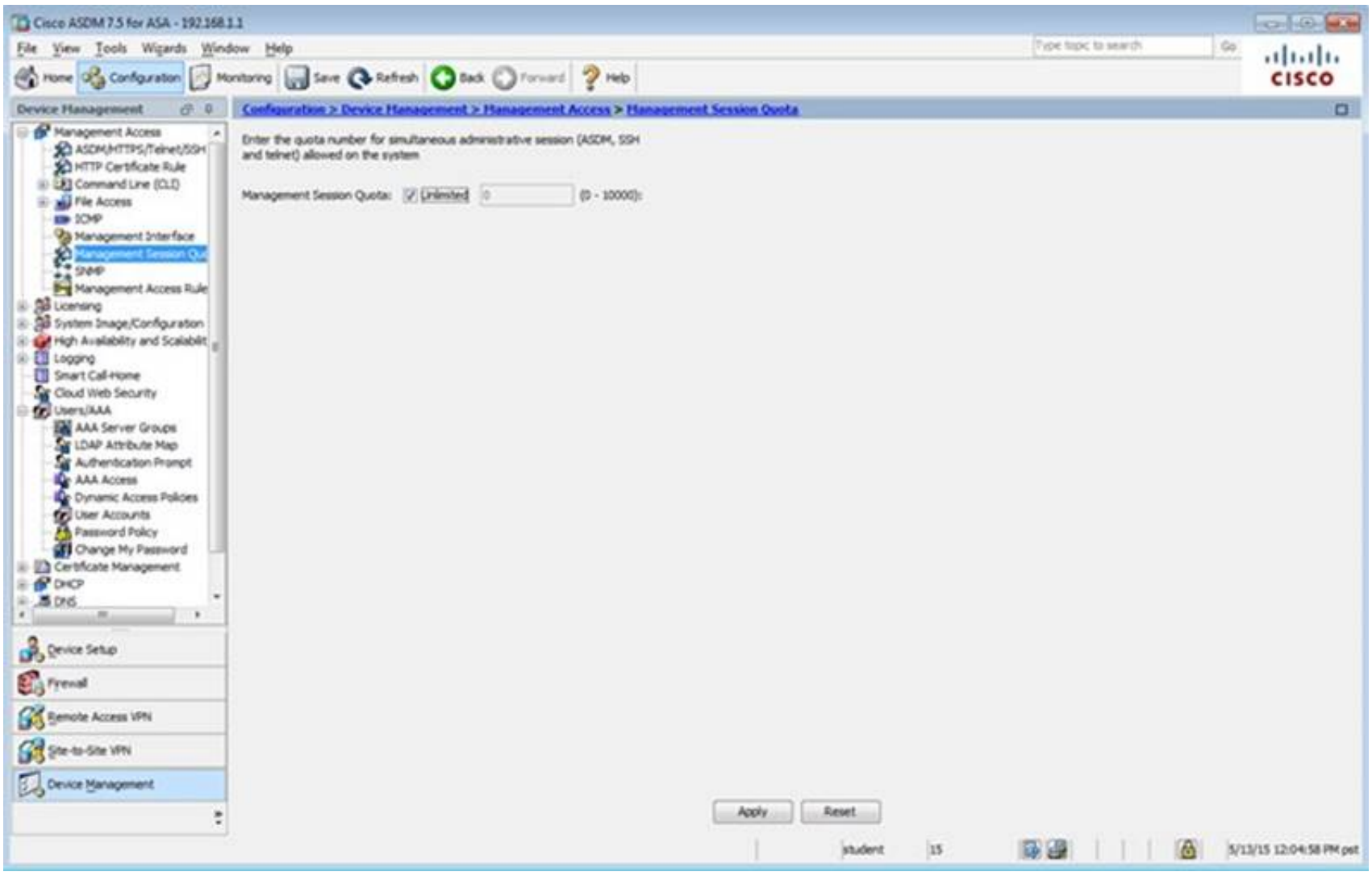

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
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
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Quota
- SNMP
- Management Access Rules
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 11:59:28 AM pst

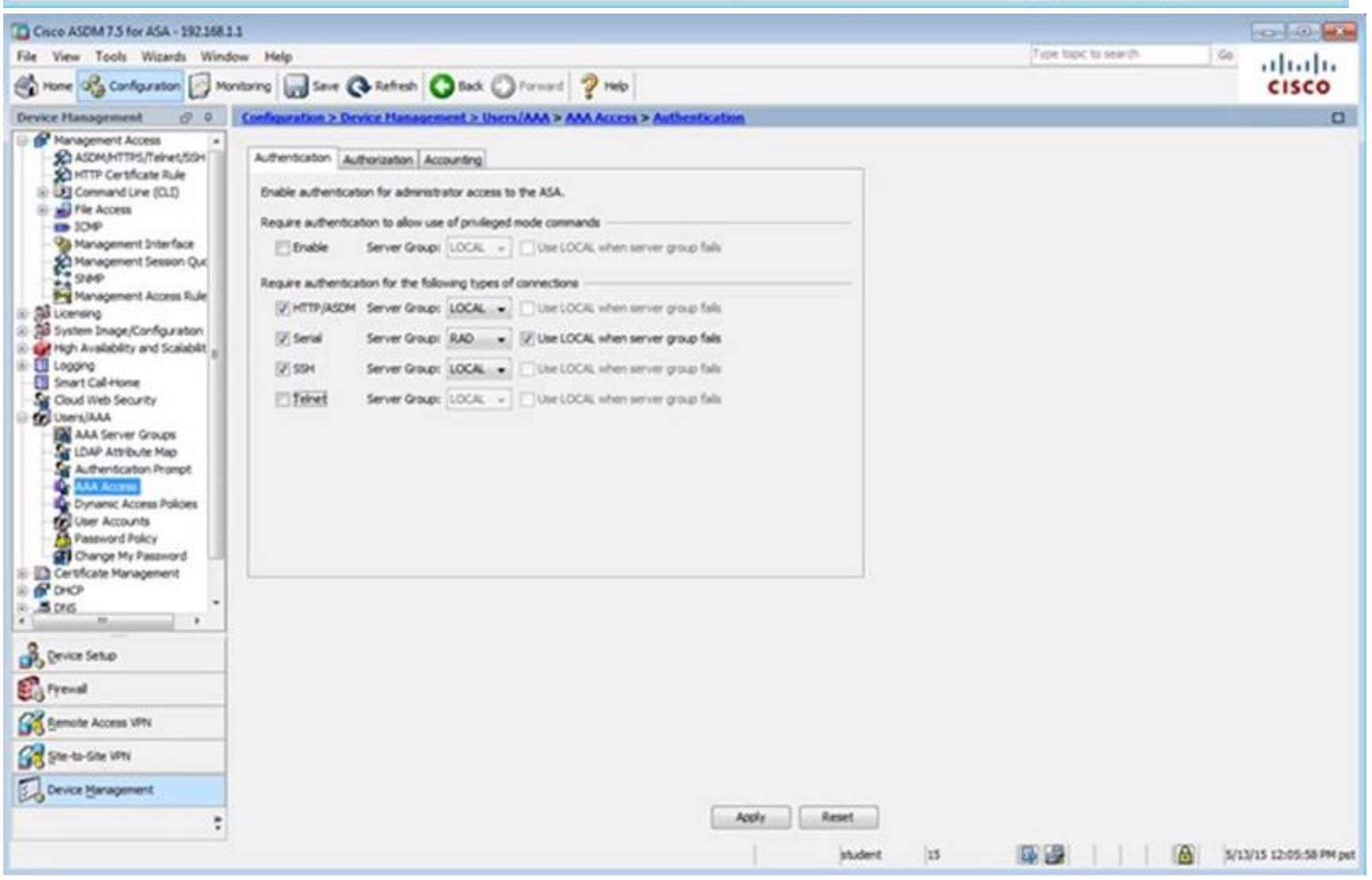

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command 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
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
Add
Edit
Delete
Http Settings
Enable HTTP Server
Port Number: 443
Idle Timeout: 20 minutes
Session Timeout: minutes
Require client certificate to access ASDM on the following interfaces
Interfaces:
Telnet Settings
Telnet Timeout: 5 minutes
SSH Settings
Allowed SSH Version(s): 1&2
SSH Timeout: 5 minutes
DH Key Exchange: Group 1 Group 14
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/13/15 12:00:38 PM pst

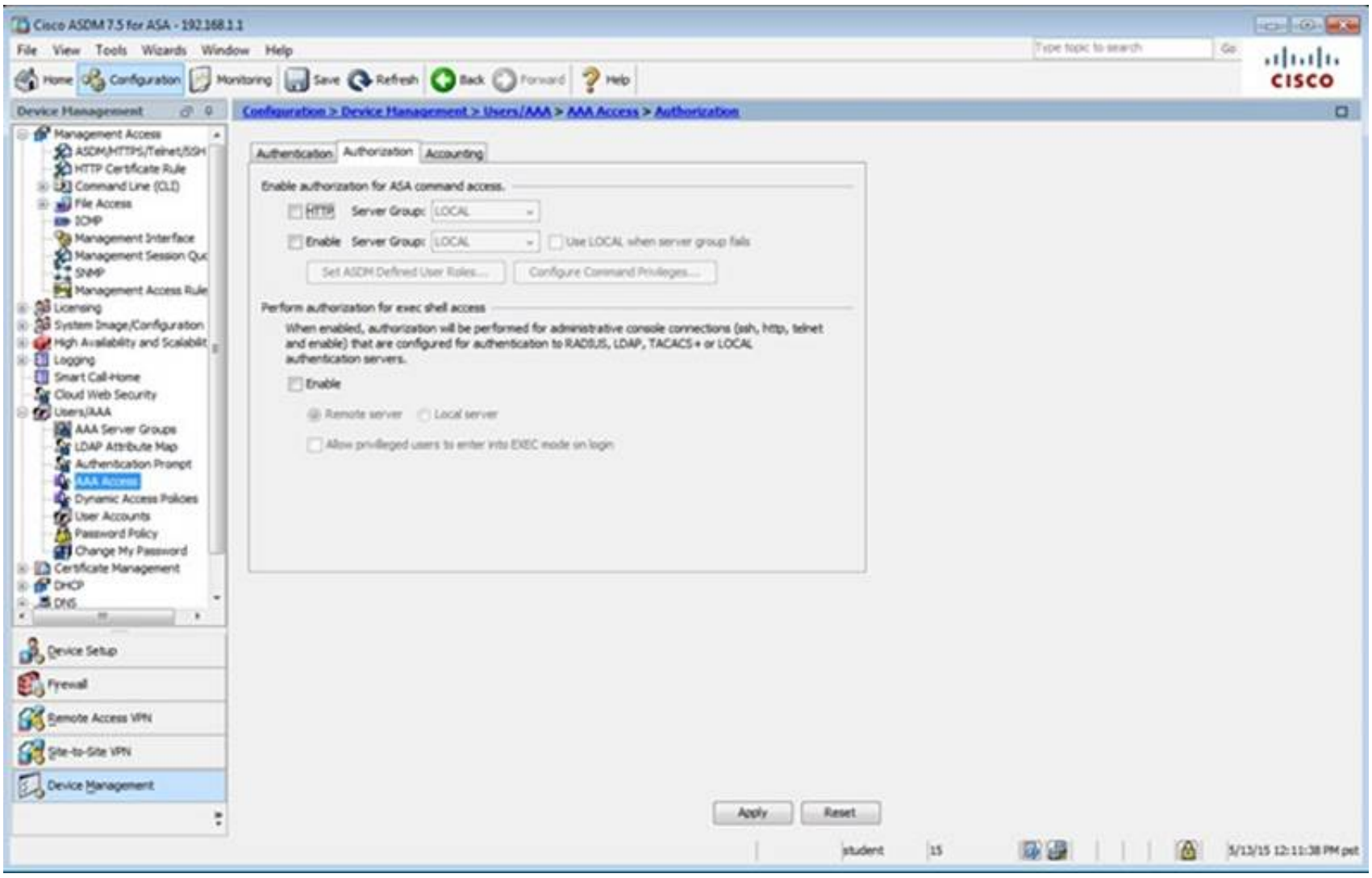

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command 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
Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.
Management Access Interface: --none--
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/13/15 12:01:38 PM pst

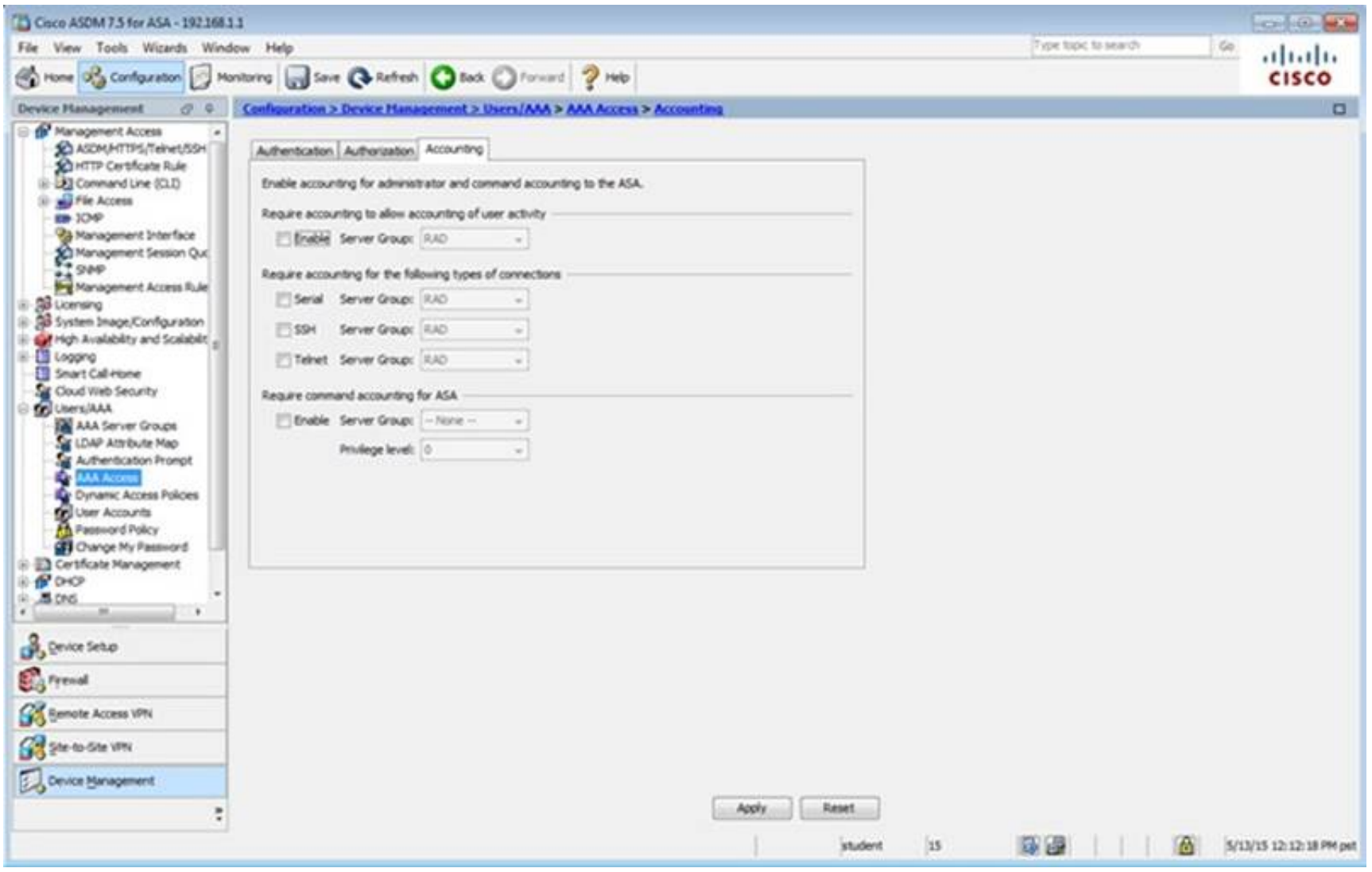

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Access Rules
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command 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
Add Edit Delete
Enabled Source Criteria: Source User Security Group Destination Criteria: Security Group Service Action Logging Time Description
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 pst

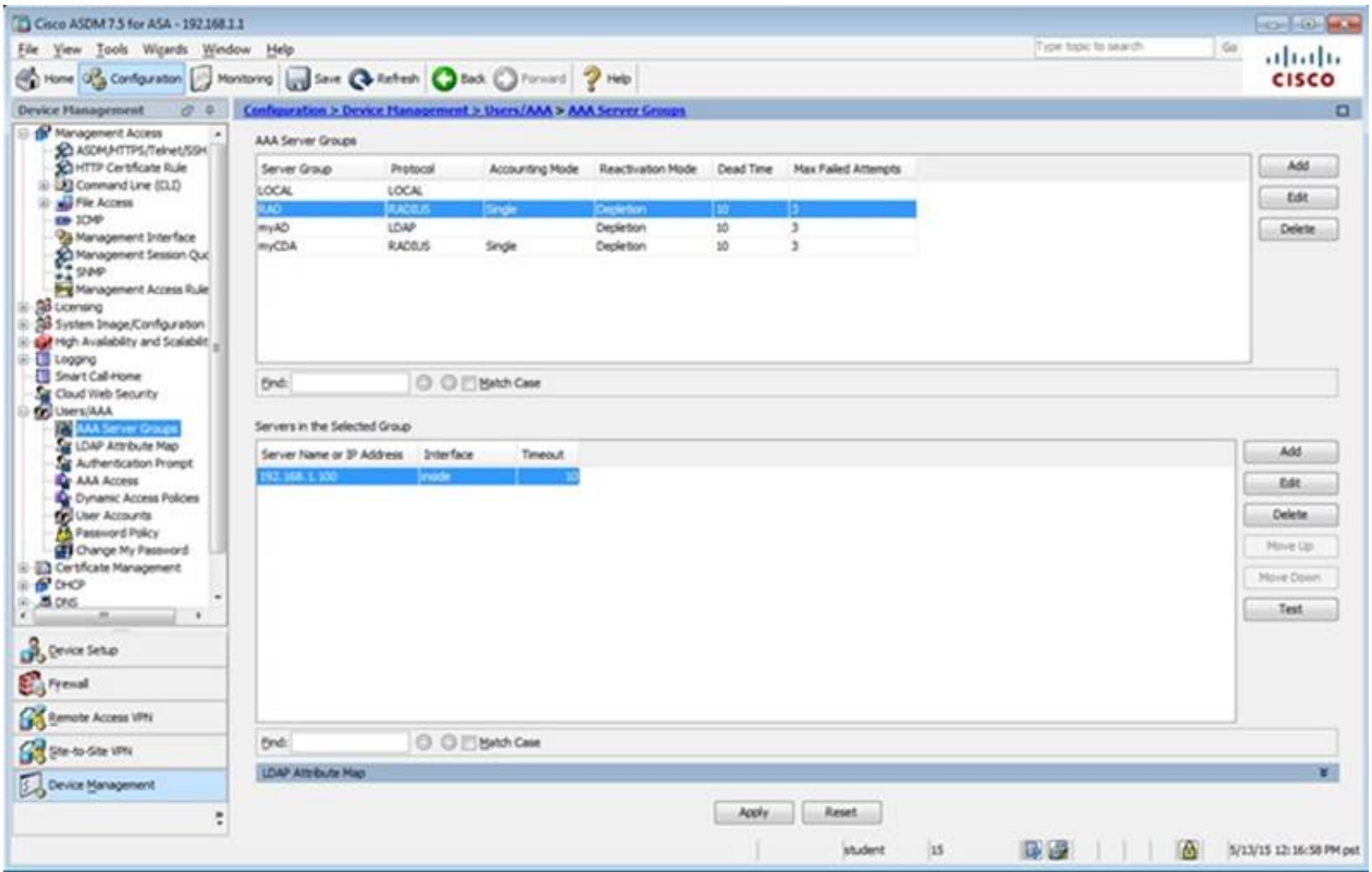

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system
Management Session Quota: Unlimited 0 (0 - 10000)
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
student 15
5/13/15 12:03:08 PM pst

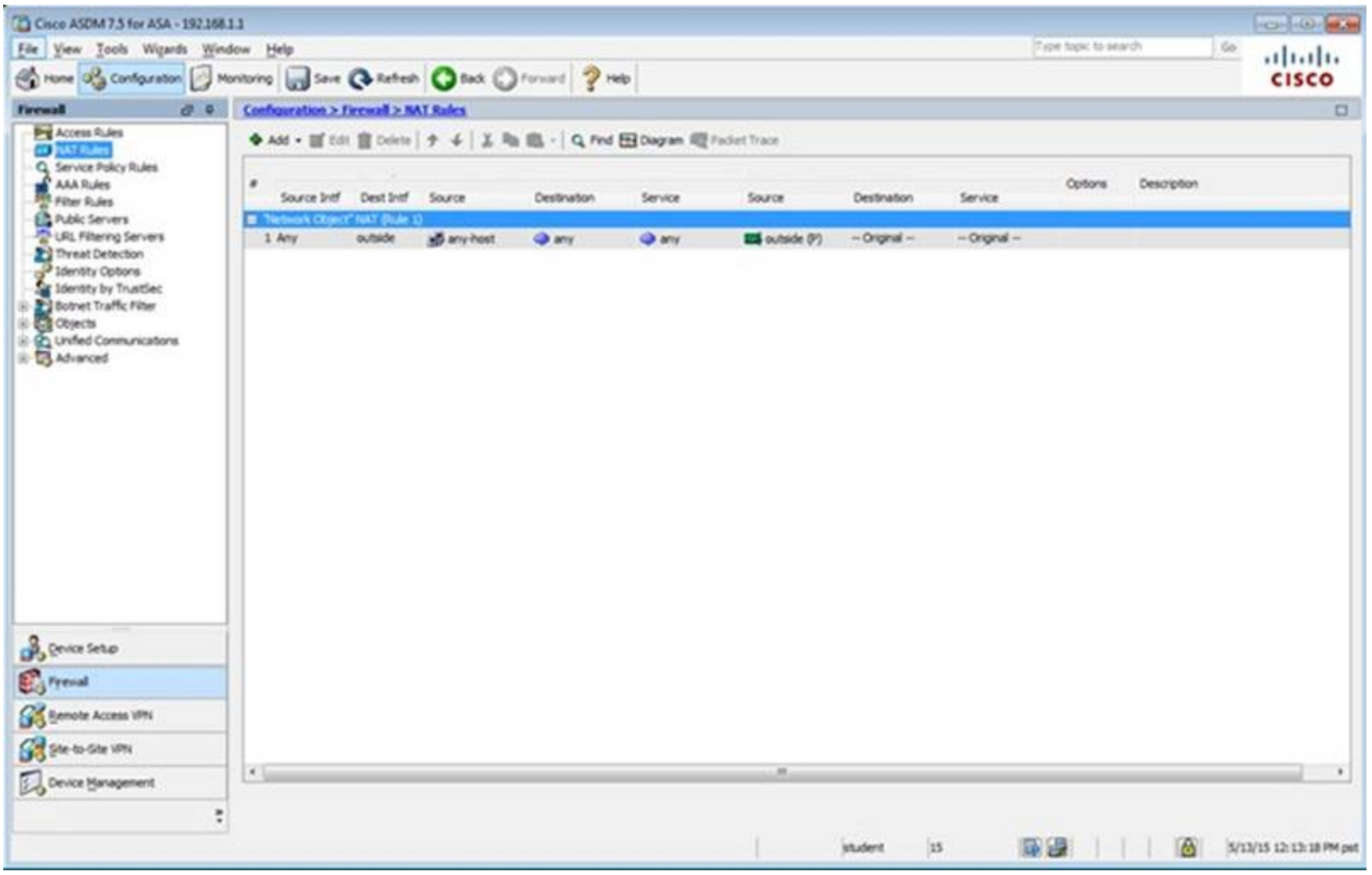

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quota
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system
Management Session Quota: Unlimited 0 (0 - 10000):
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15 5/13/15 12:04:58 PM pst

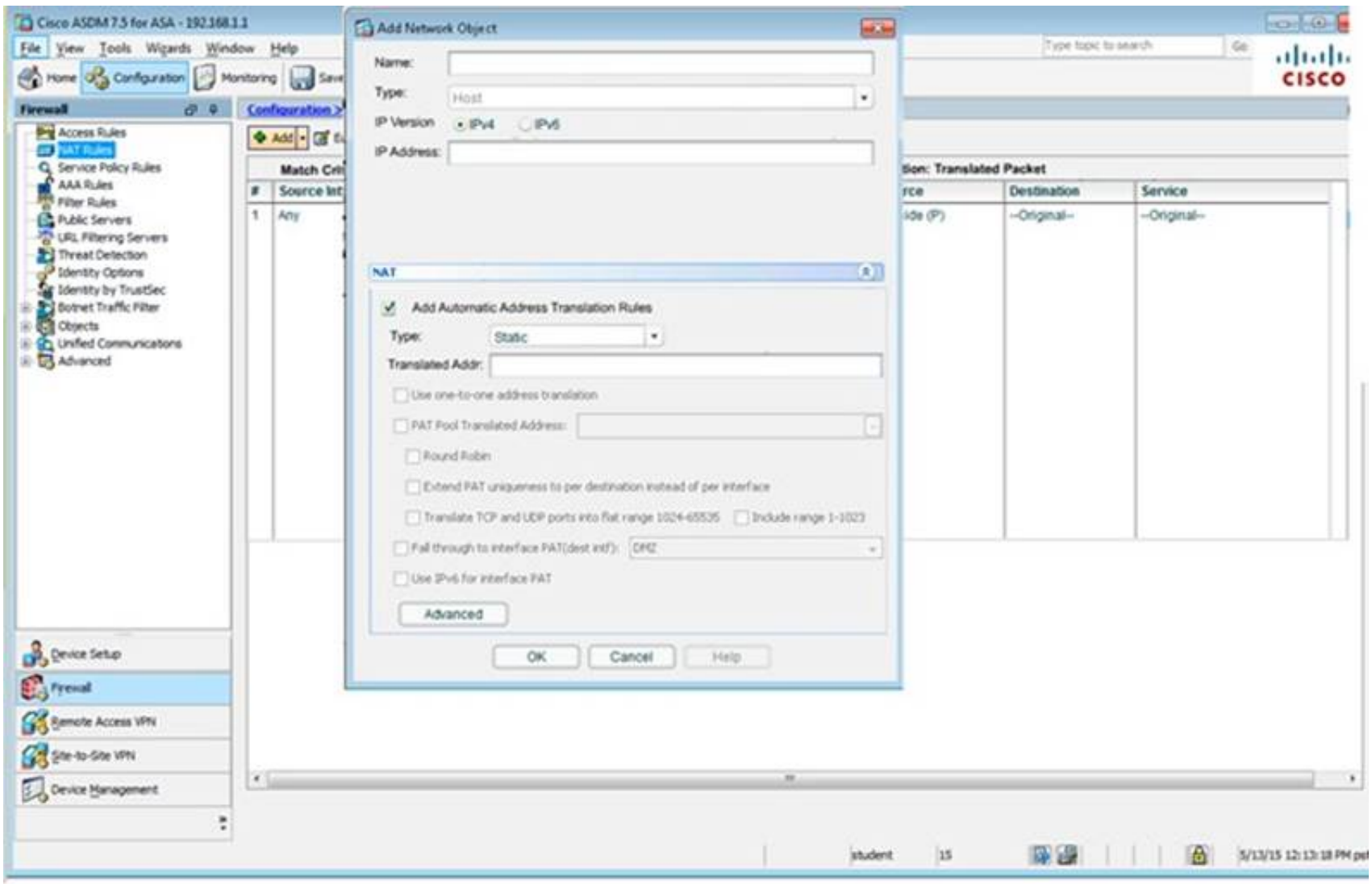

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quo
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15 5/13/15 12:05:58 PM pst

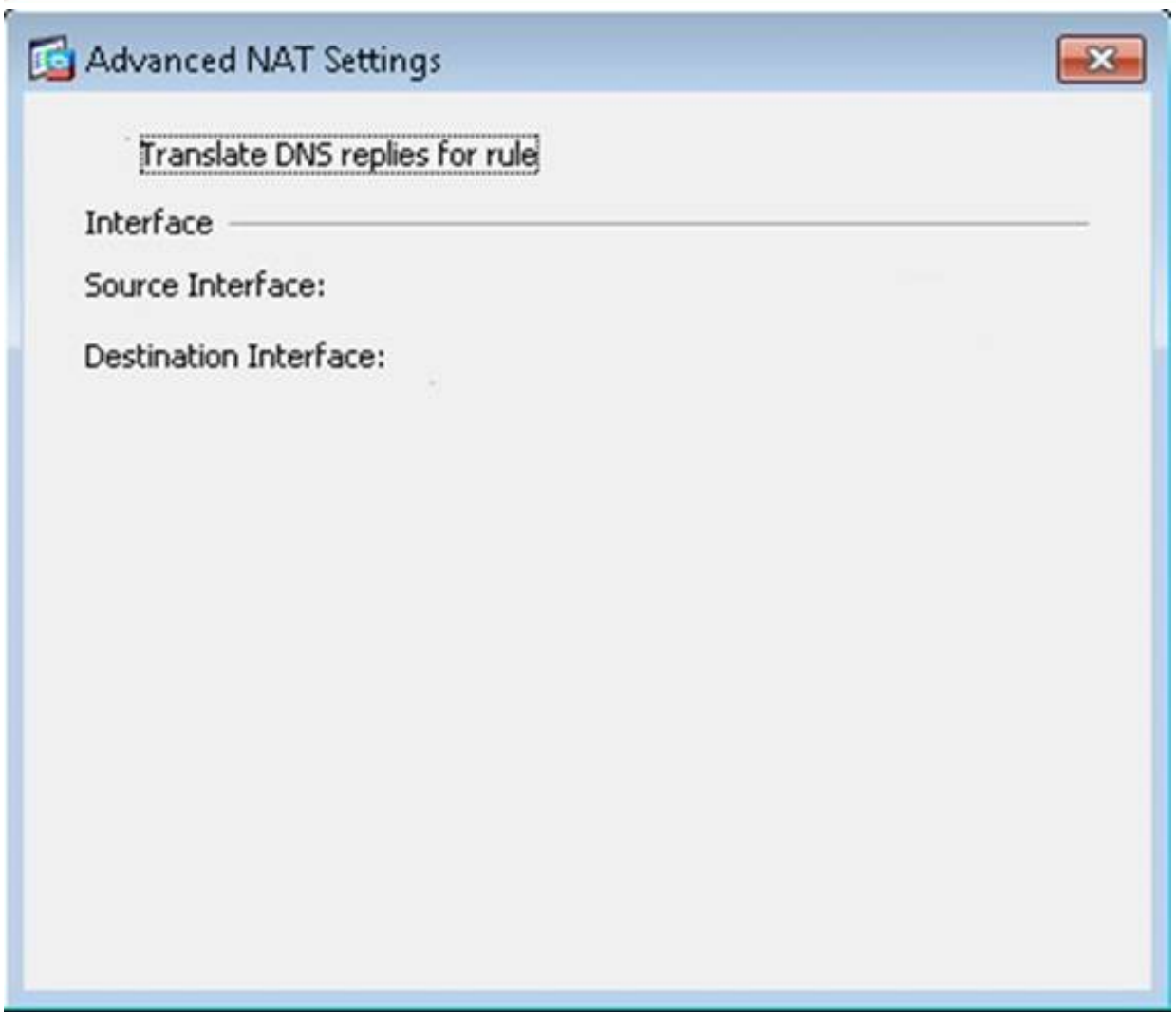

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Enable authorization for ASA 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quc
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:11:38 PM pst

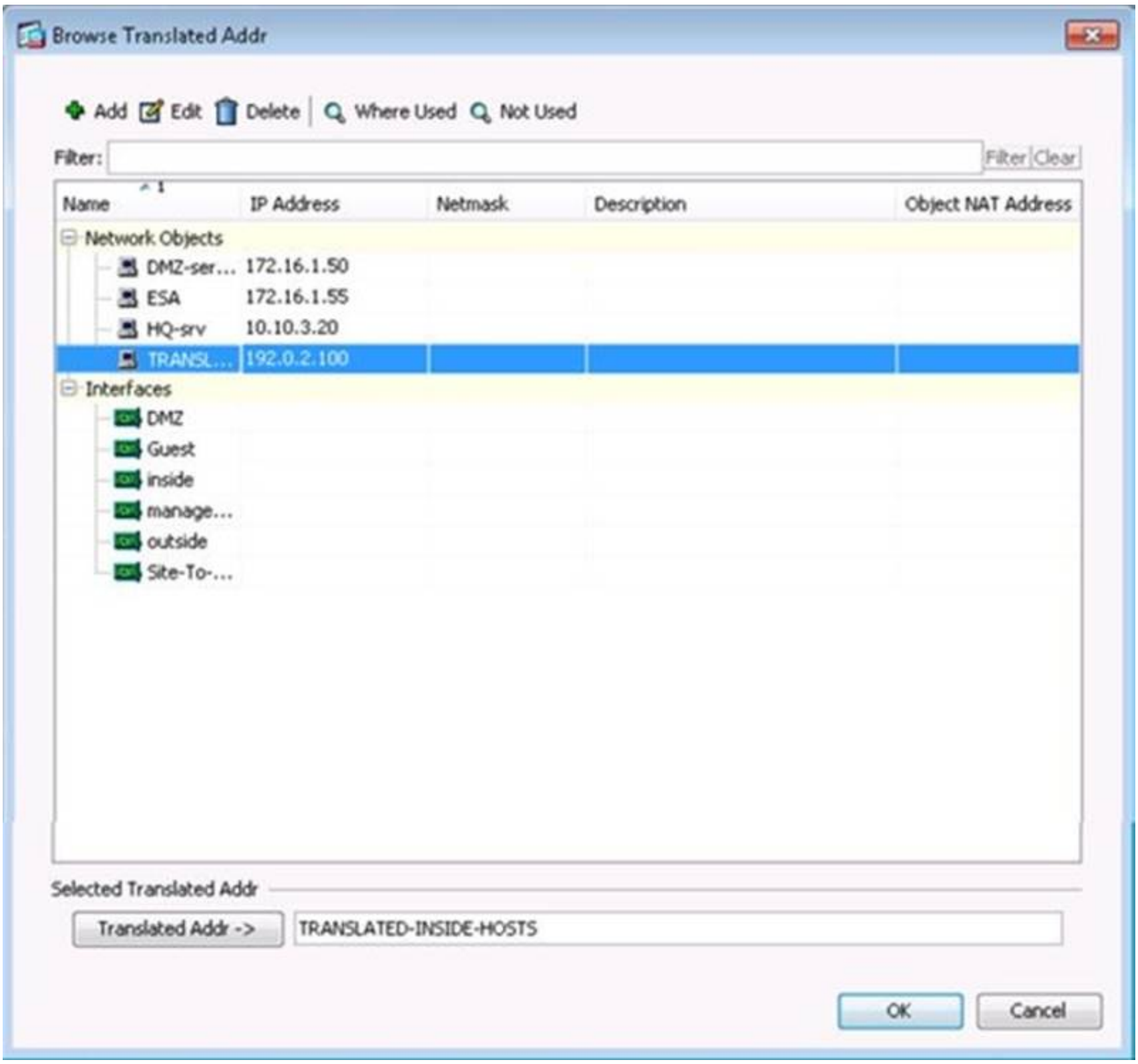

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Authentication Authorization Accounting
Enable accounting for administrator 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quc
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:12:18 PM pst

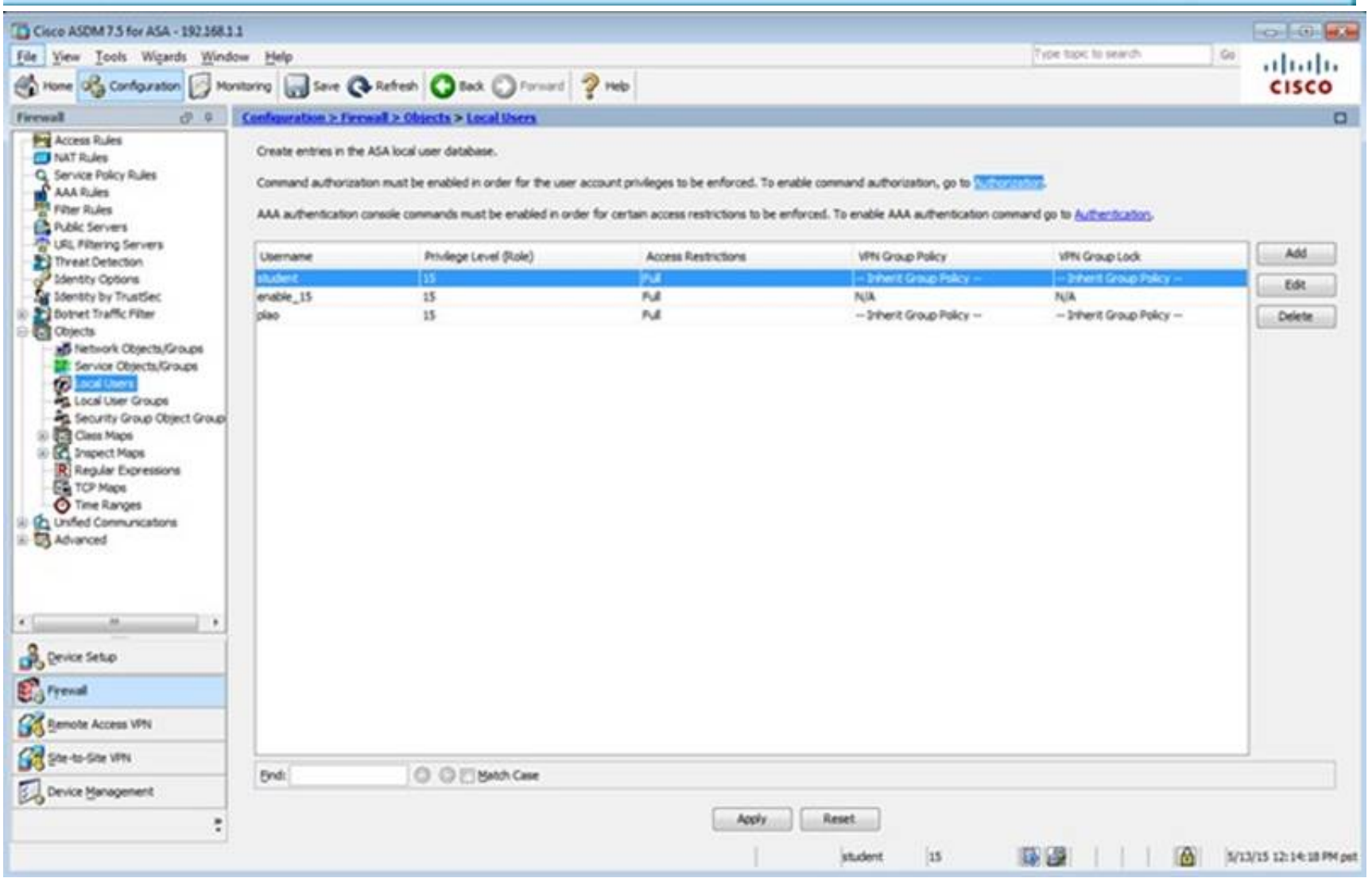

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Server Groups
AAA Server Groups
Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts
LOCAL LOCAL
RAD RADIUS Single Depletion 10 3
myAD LDAP Depletion 10 3
myCDA RADIUS Single Depletion 10 3
Add Edit Delete
Find: Match Case
Servers in the Selected Group
Server Name or IP Address Interface Timeout
192.168.1.100 inside 10
Add Edit Delete Move Up Move Down Test
LDAP Attribute Map
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/13/15 12:16:58 PM pst

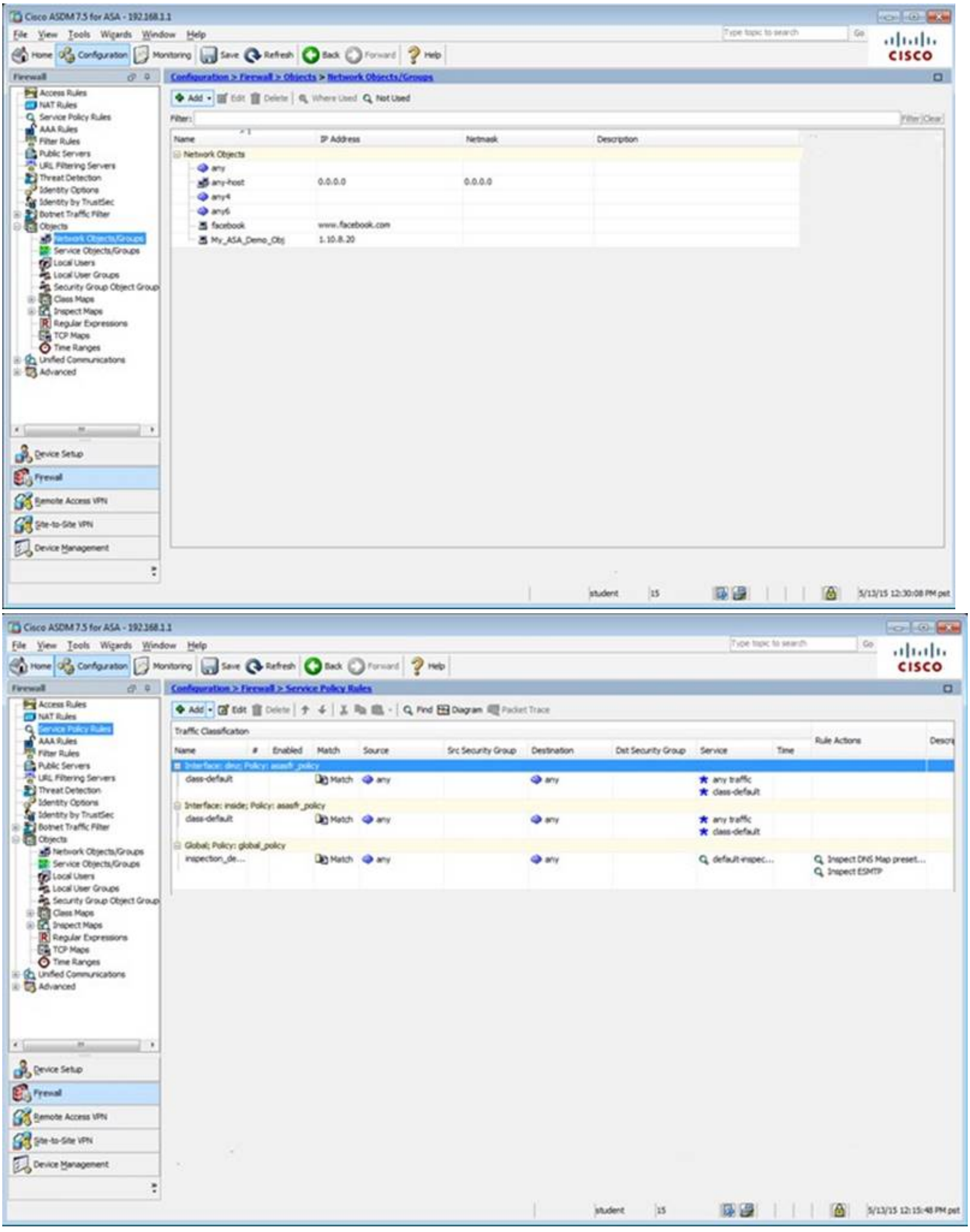

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Source Intf Dest Intf Source Destination Service Source Destination Service Options Description
"Network Object" NAT (Rule 1)
1 Any outside any-host any any outside (P) -- Original -- -- Original --
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/13/15 12:13:18 PM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
OK Cancel Help
Destination
Service
--Original--
--Original--
CISCO
student
15

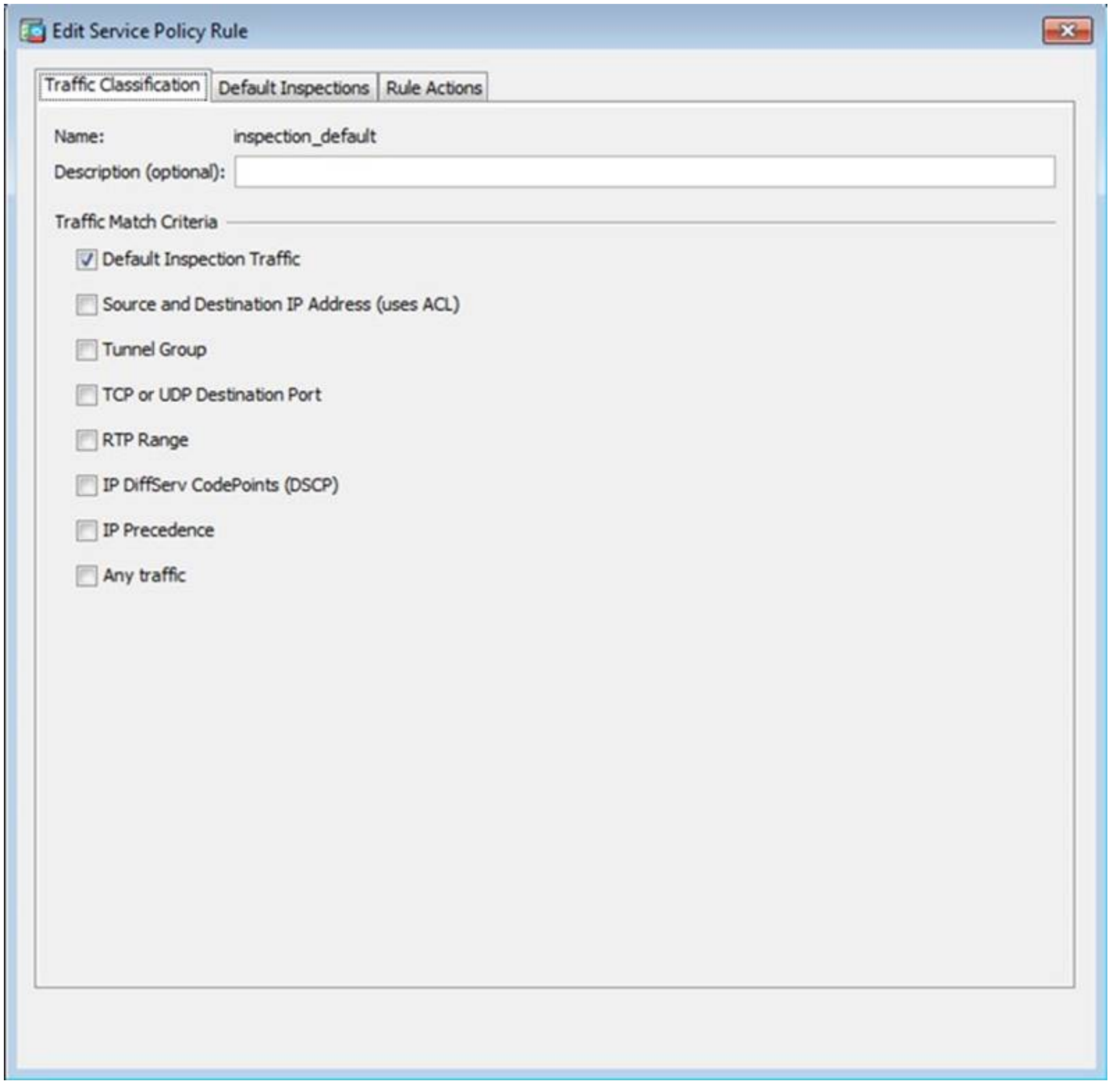

Advanced NAT Settings
Translate DNS replies for rule
Interface
Source Interface:
Destination Interface:

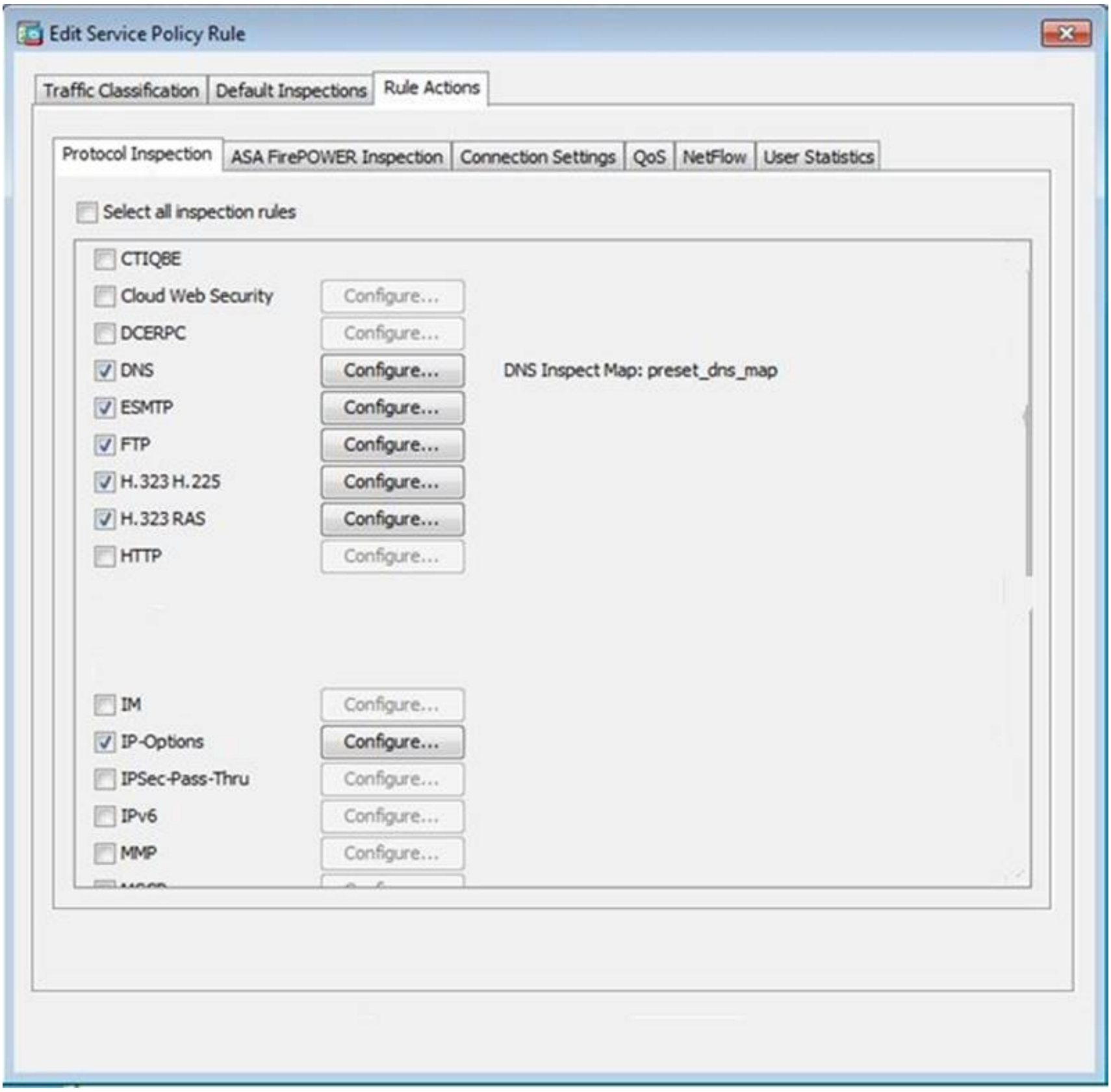

Browse Translated Addr
Add
Edit
Delete
Where Used
Not Used
Filter:
Filter
Clear
Name
IP Address
Netmask
Description
Object NAT Address
Network Objects
DMZ-ser...
172.16.1.50
ESA
172.16.1.55
HQ-srv
10.10.3.20
TRANSL...
192.0.2.100
Interfaces
DMZ
Guest
inside
manage...
outside
Site-To-...
Selected Translated Addr
Translated Addr ->
TRANSLATED-INSIDE-HOSTS
OK
Cancel

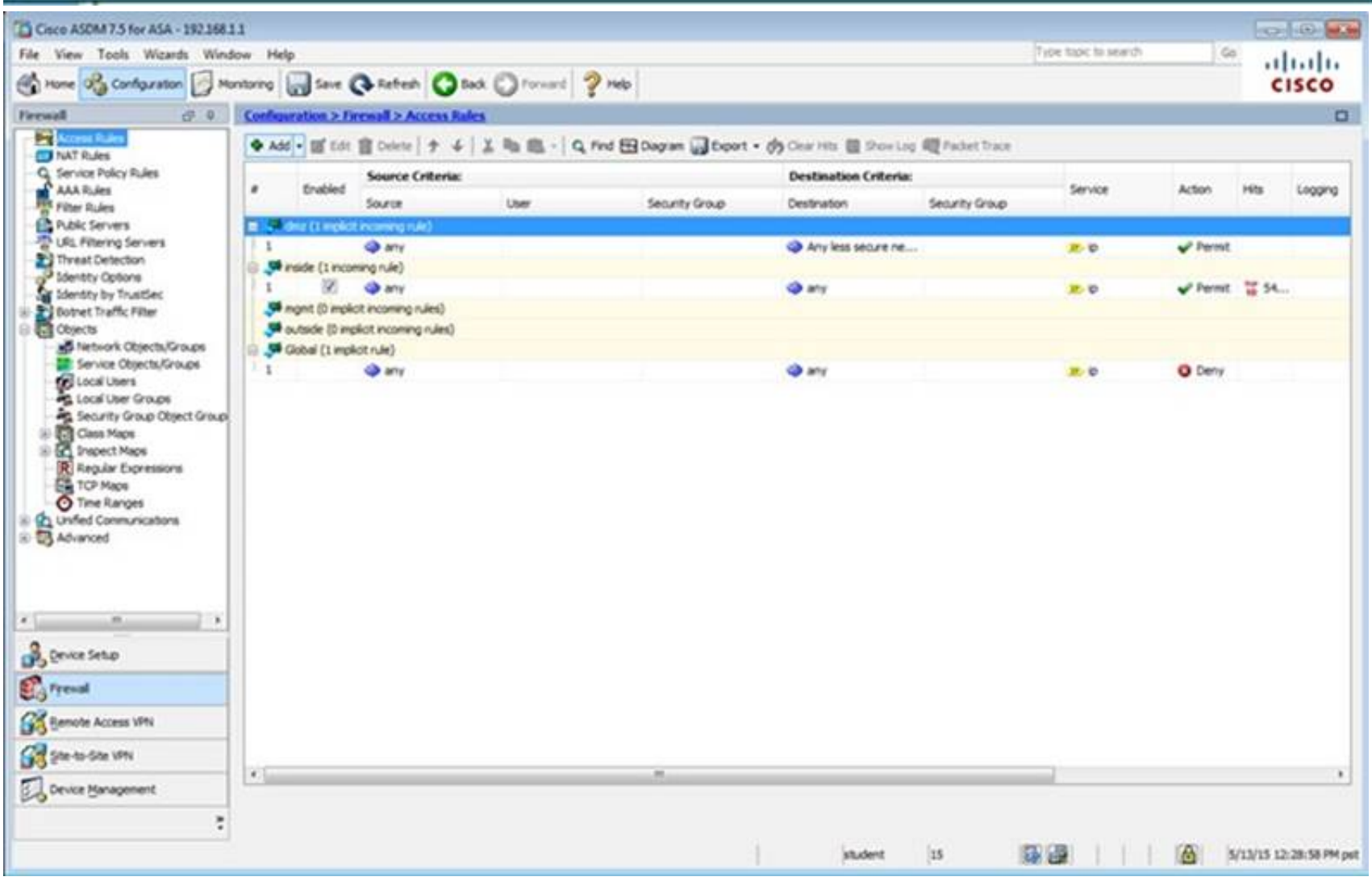

Cisco ASDM 7.5 for ASA - 192.168.1.1
File
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to 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
piao
15
Full
-- Inherit Group Policy --
-- Inherit Group Policy --
Add
Edit
Delete
Find:
Match Case
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
3/13/15 12:14:18 PM pst

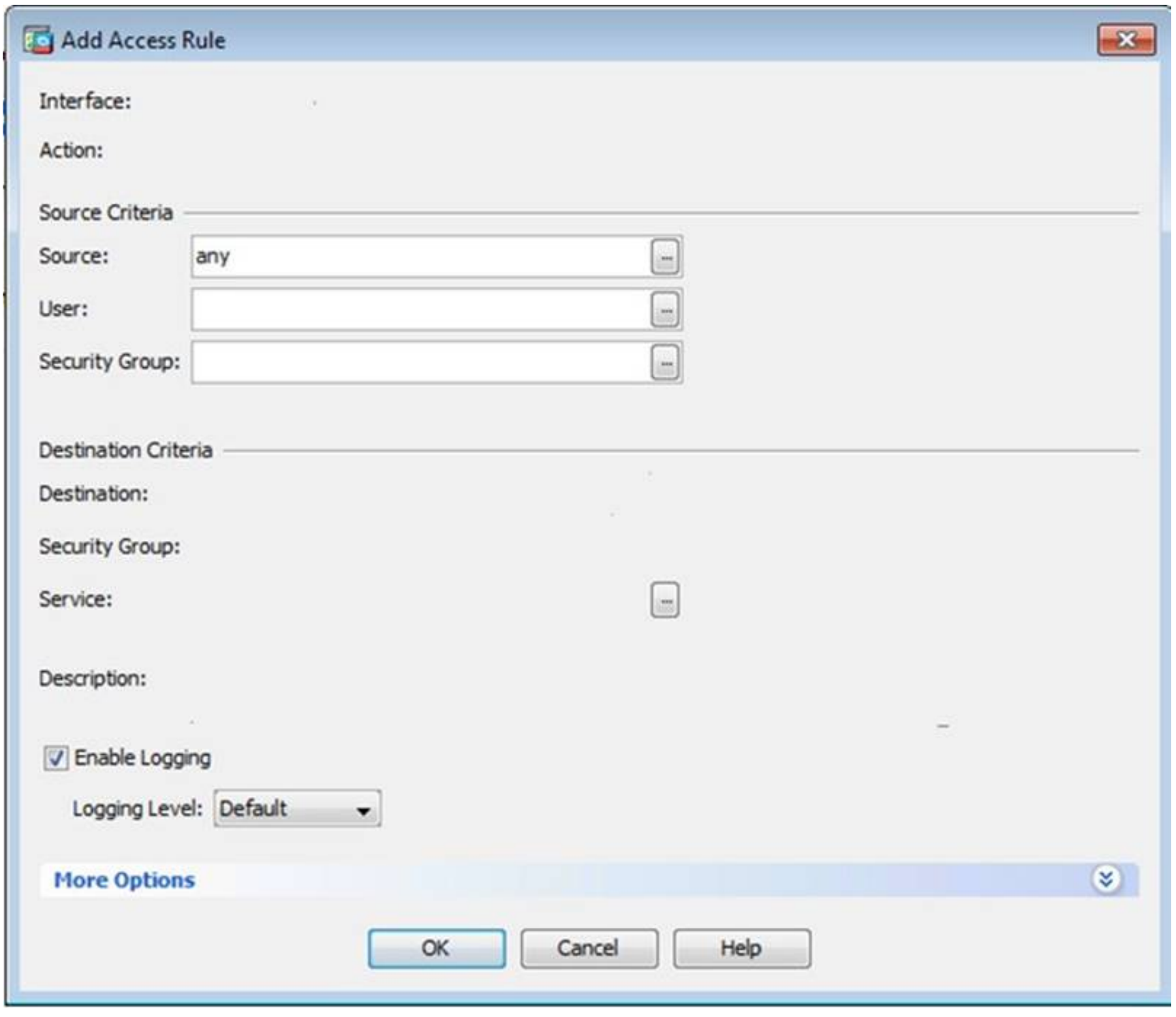

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Filter:
Name IP Address Netmask Description
Network Objects
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
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 12:30:08 PM pst

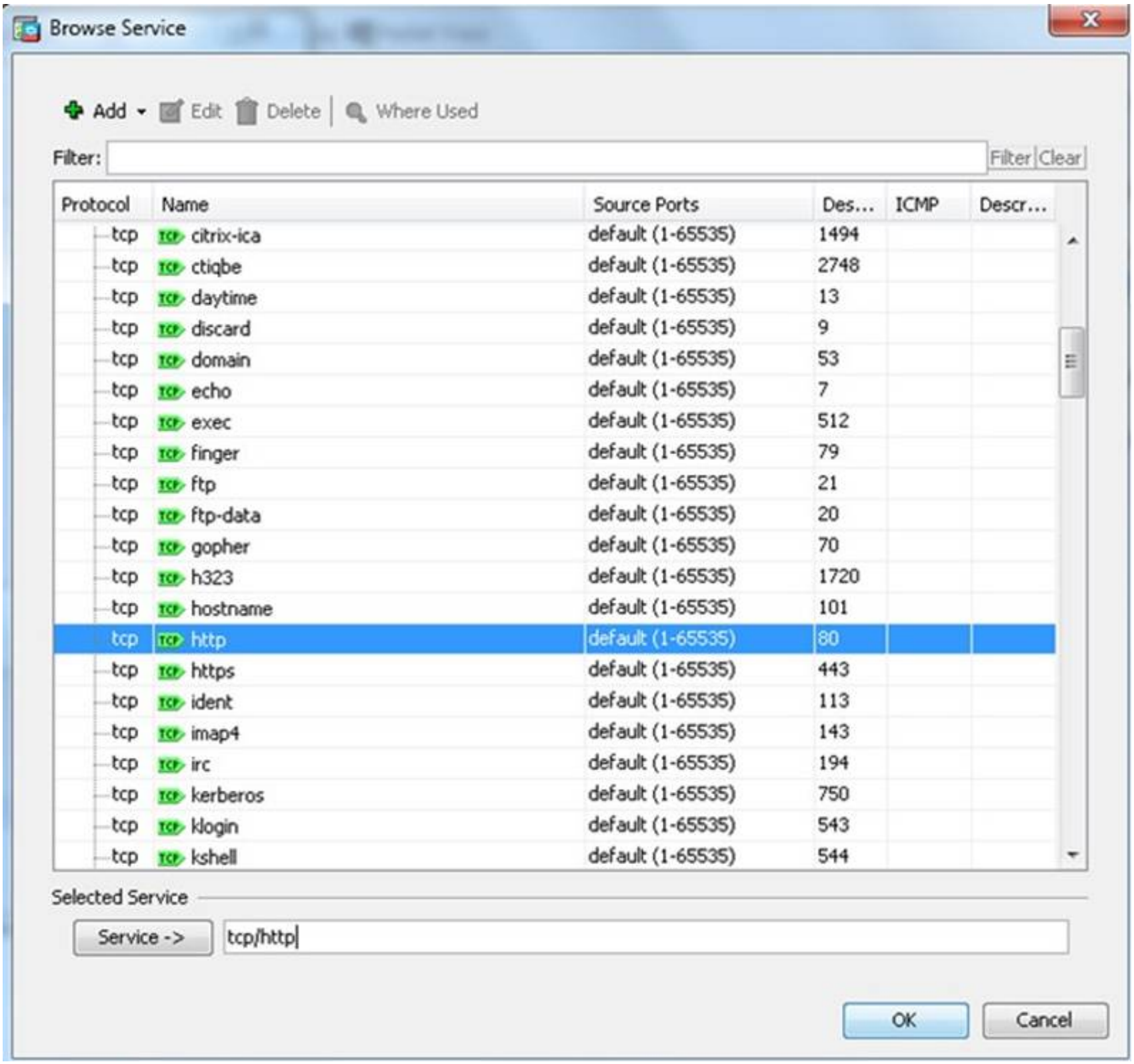
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst Security Group Service Time Rule Actions
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
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 12:15:48 PM pst

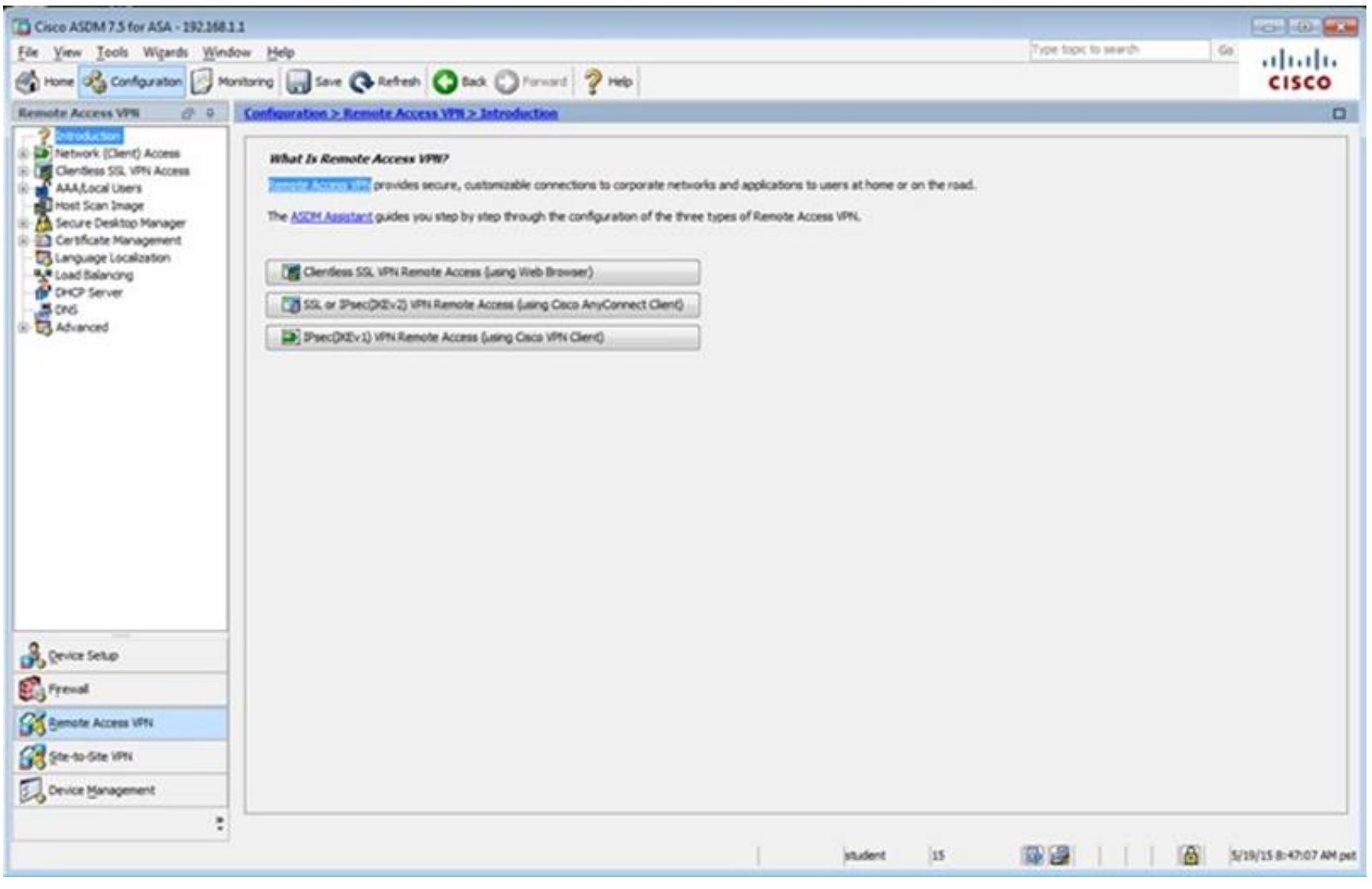

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Name:
inspection_default
Description (optional):
Traffic Match Criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
Tunnel Group
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)
IP Precedence
Any traffic

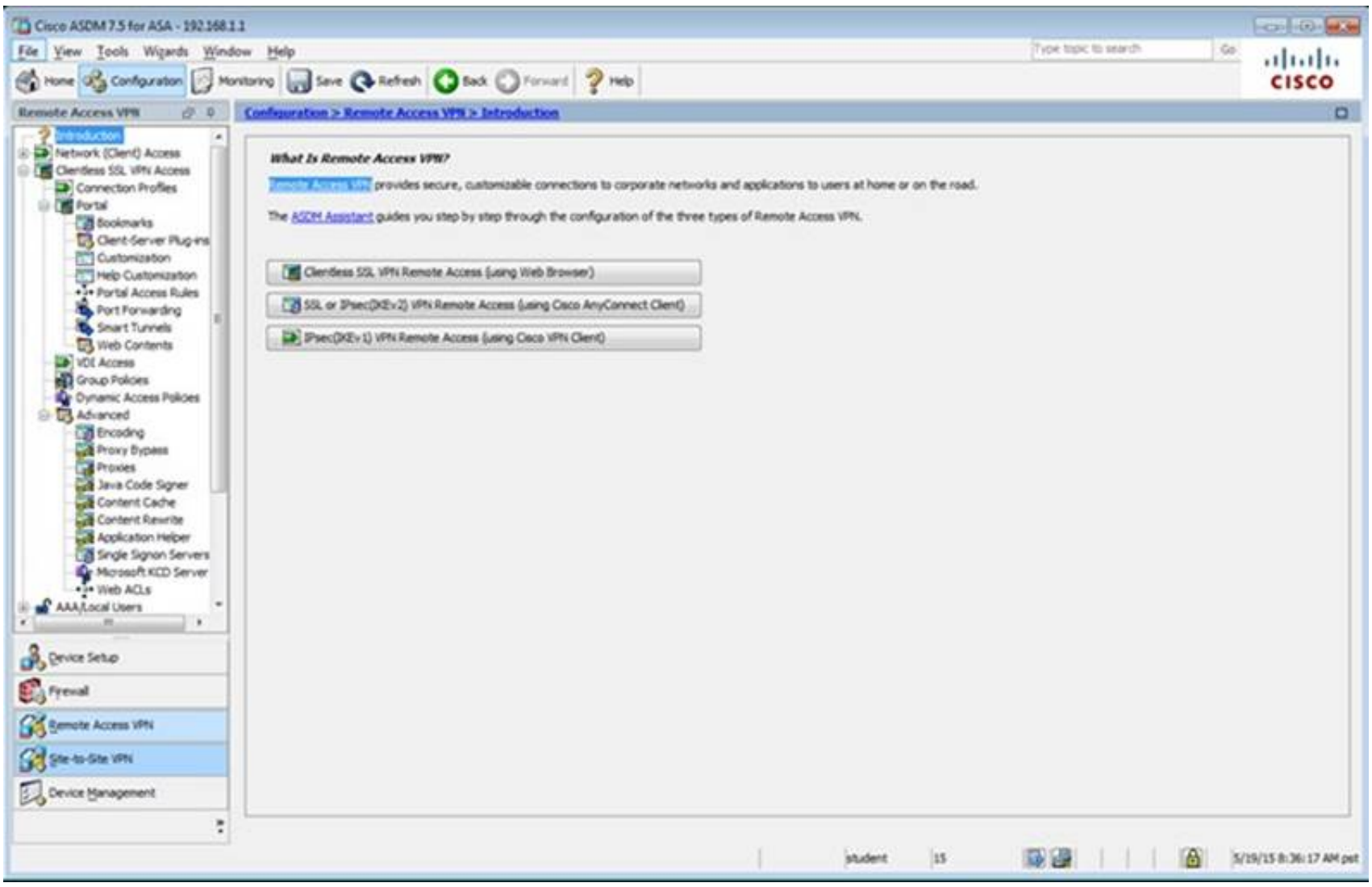

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Protocol Inspection
ASA FirePOWER Inspection
Connection Settings
QoS
NetFlow
User Statistics
Select all inspection rules
CTIQBE
Cloud Web Security
Configure...
DCERPC
Configure...
DNS
Configure...
DNS Inspect Map: preset_dns_map
ESMTP
Configure...
FTP
Configure...
H.323 H.225
Configure...
H.323 RAS
Configure...
HTTP
Configure...
IM
Configure...
IP-Options
Configure...
IPSec-Pass-Thru
Configure...
IPv6
Configure...
MMP
Configure...

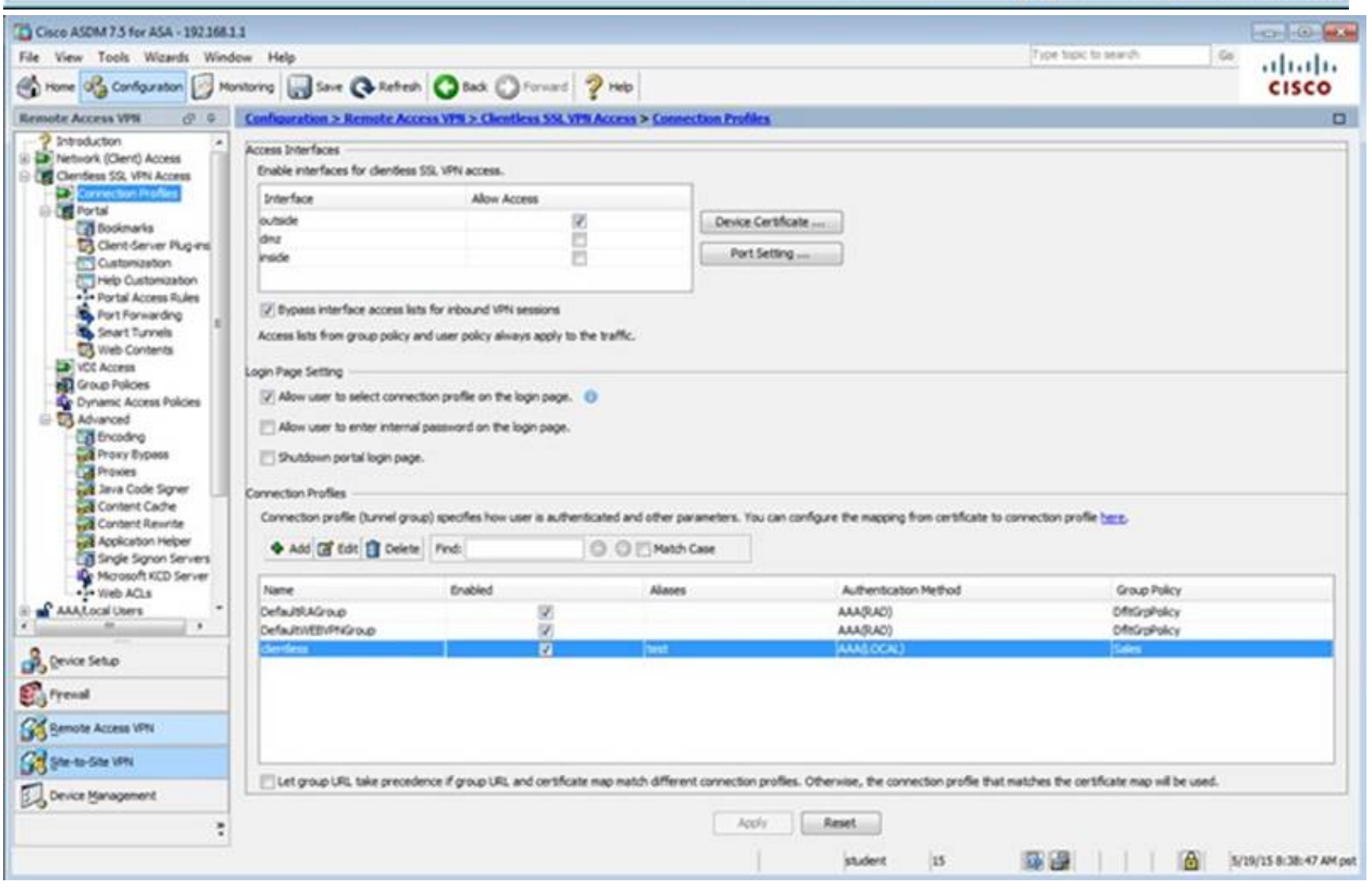

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria:
Destination Criteria:
Enabled
Source
User
Security Group
Destination
Security Group
Service
Action
Hits
Logging
dmz (1 implicit incoming rule)
any
Any less secure ne...
Permit
inside (1 incoming rule)
any
any
Permit
mgmt (0 implicit incoming rules)
outside (0 implicit incoming rules)
Global (1 implicit rule)
any
any
Deny
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 12:28:58 PM pst

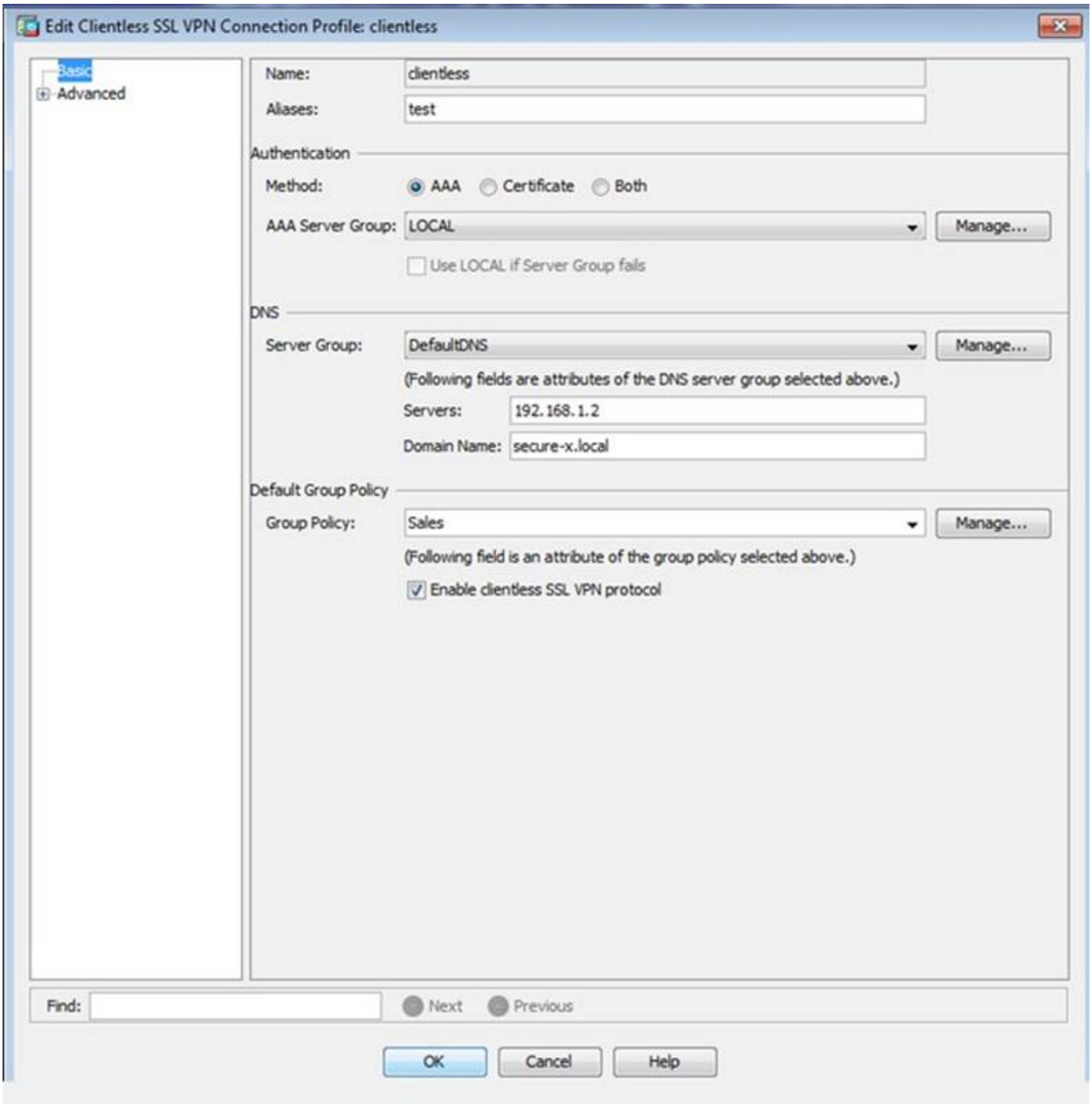

Add Access Rule
Interface:
Action:
Source Criteria
Source:
any
User:
Security Group:
Destination Criteria
Destination:
Security Group:
Service:
Description:
Enable Logging
Logging Level:
Default
More Options
OK
Cancel
Help

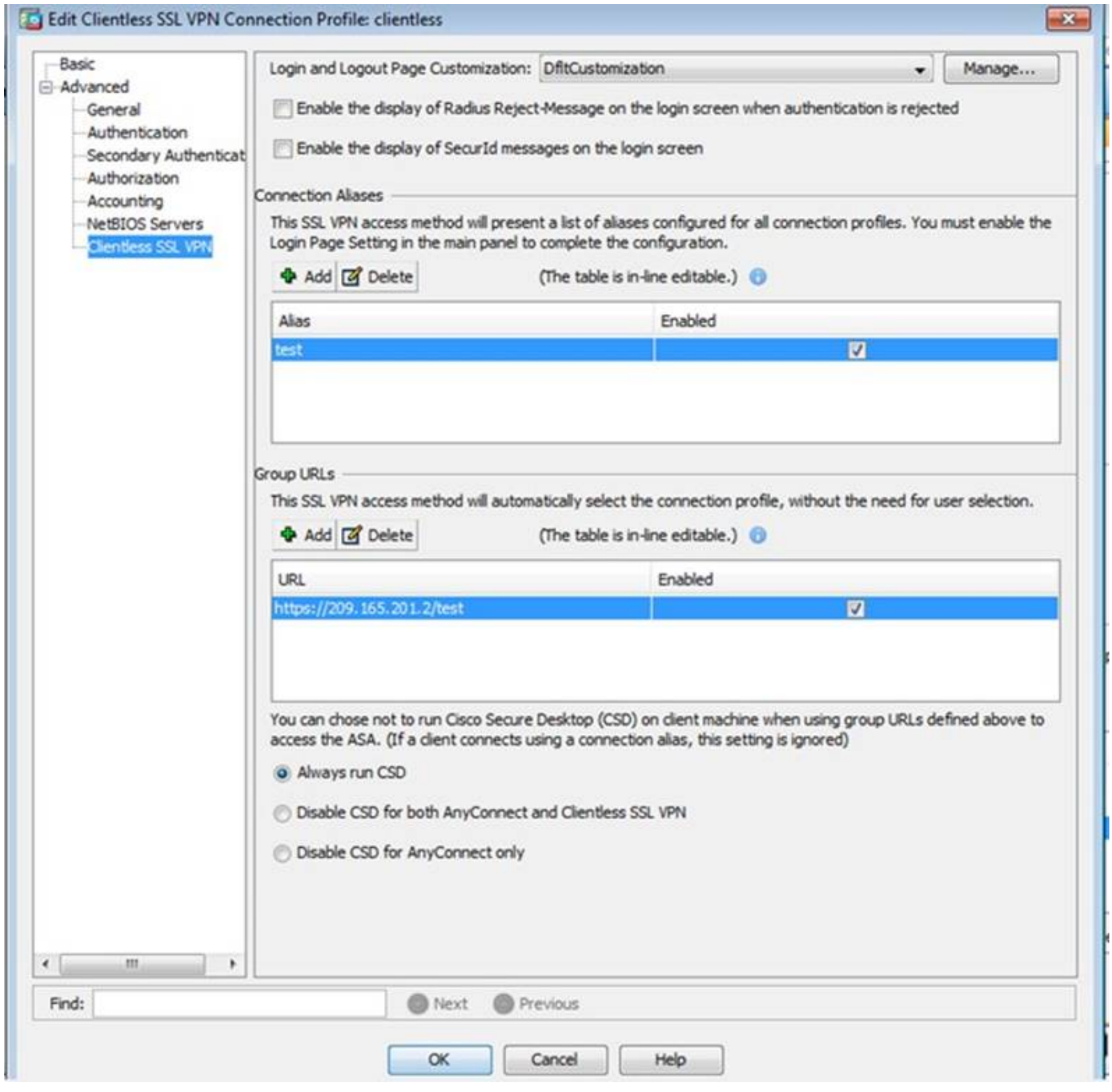

Browse Service
Add
Edit
Delete
Where Used
Filter:
Filter
Clear
Protocol
Name
Source Ports
Des...
ICMP
Descr...
tcp citrix-ica default (1-65535) 1494
tcp ctiqbe default (1-65535) 2748
tcp daytime default (1-65535) 13
tcp discard default (1-65535) 9
tcp domain default (1-65535) 53
tcp echo default (1-65535) 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
OK
Cancel

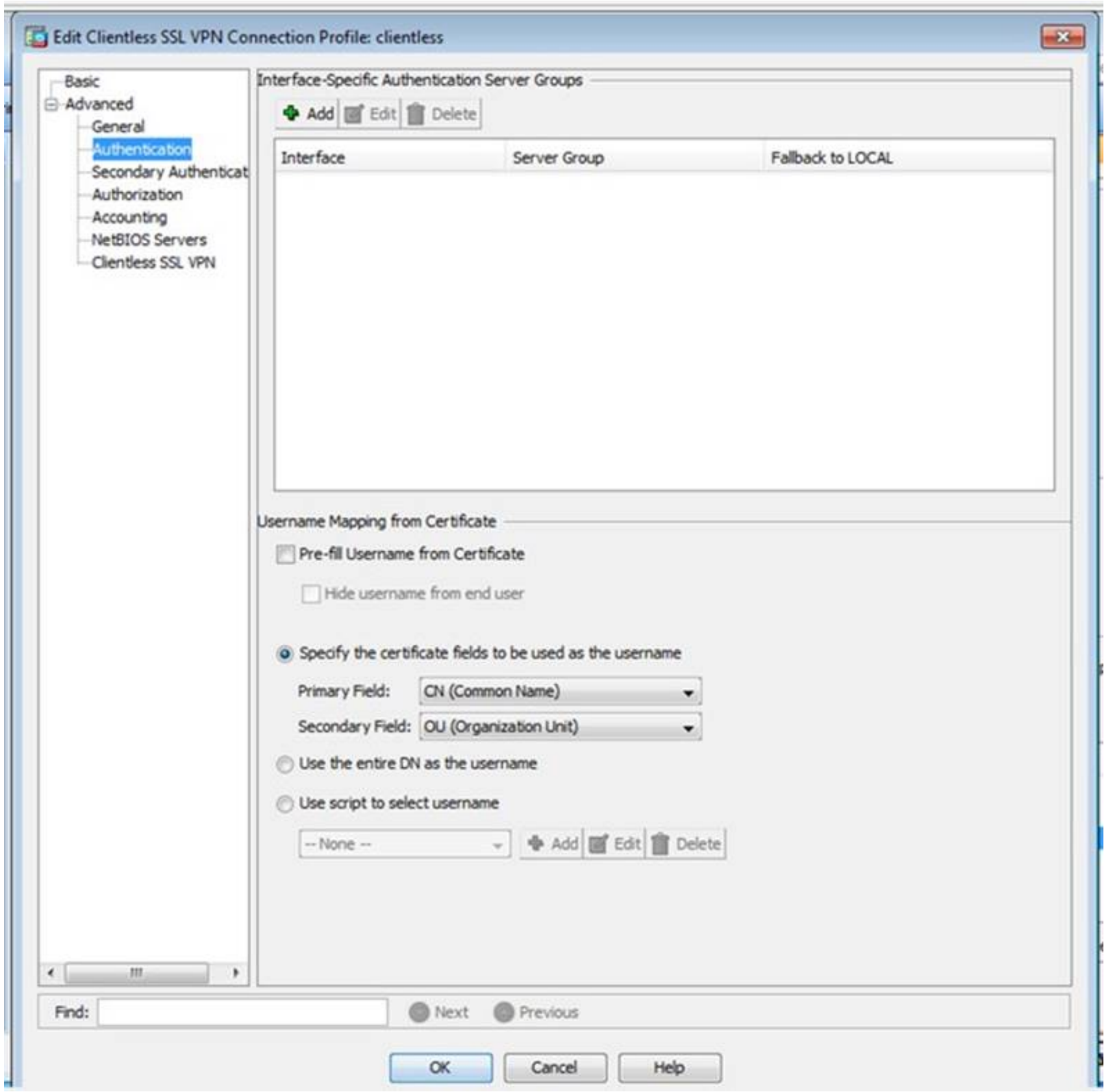

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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)
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:47:07 AM pst

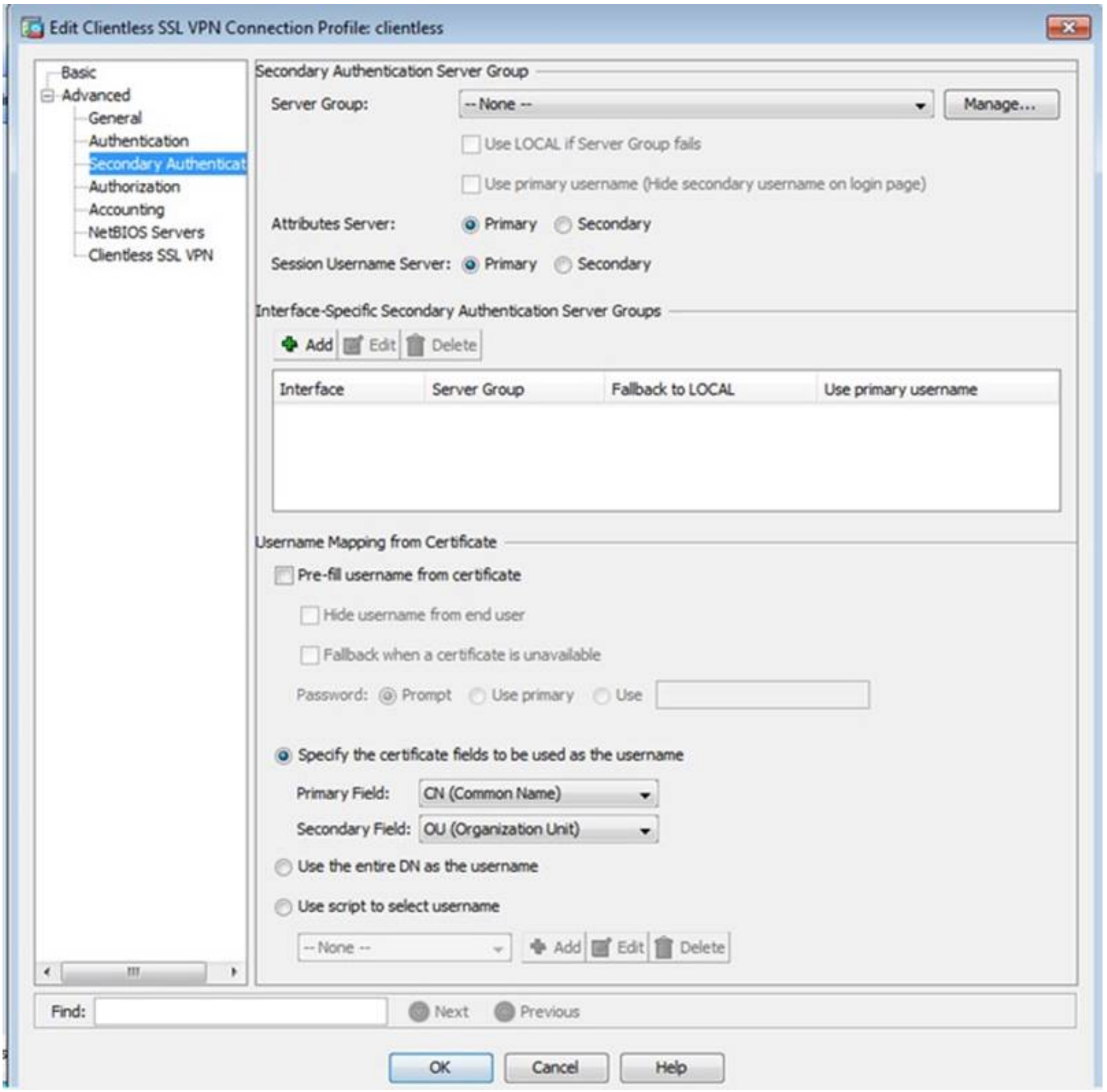

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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)
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:36:17 AM pst

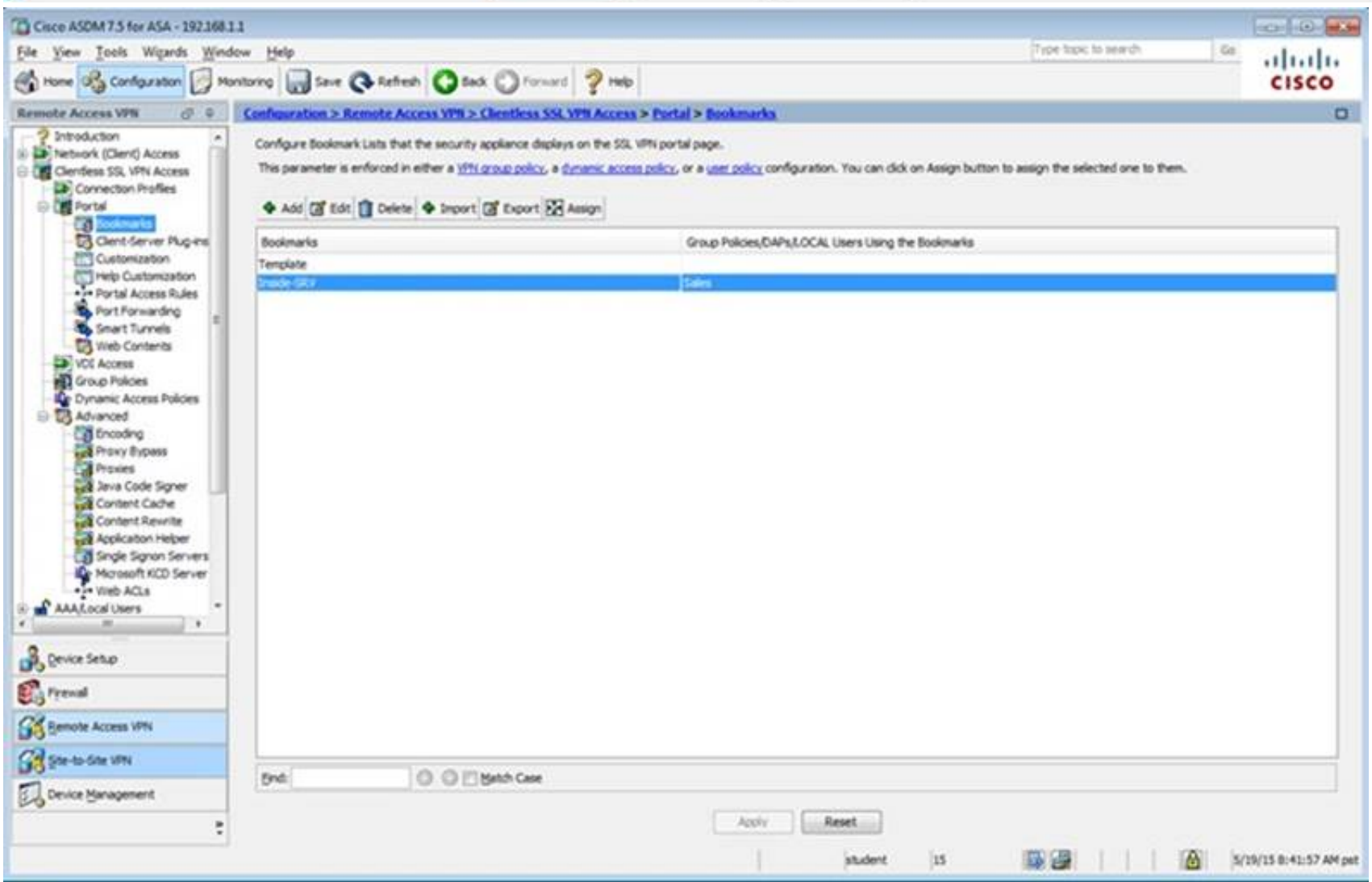

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Access Interfaces
Enable interfaces for clientless SSL VPN access.
Interface Allow Access
outside
dmz
inside
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
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:38:47 AM pst

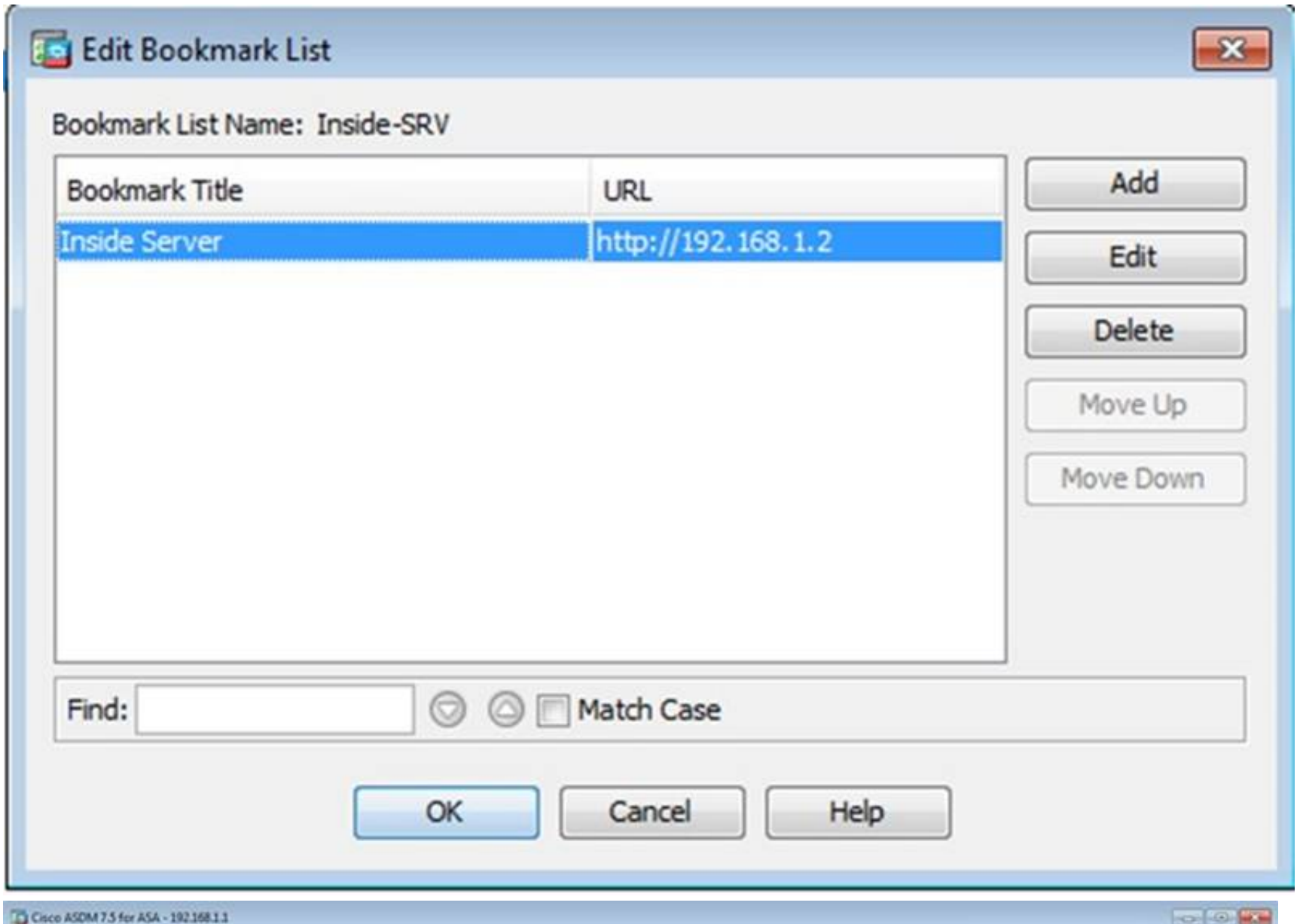

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server group selected above.)
Servers: 192.168.1.2
Domain Name: secure-x.local
Default Group Policy
Group Policy: Sales
Manage...
(Following field is an attribute of the group policy selected above.)
Enable clientless SSL VPN protocol
Find:
Next
Previous
OK
Cancel
Help

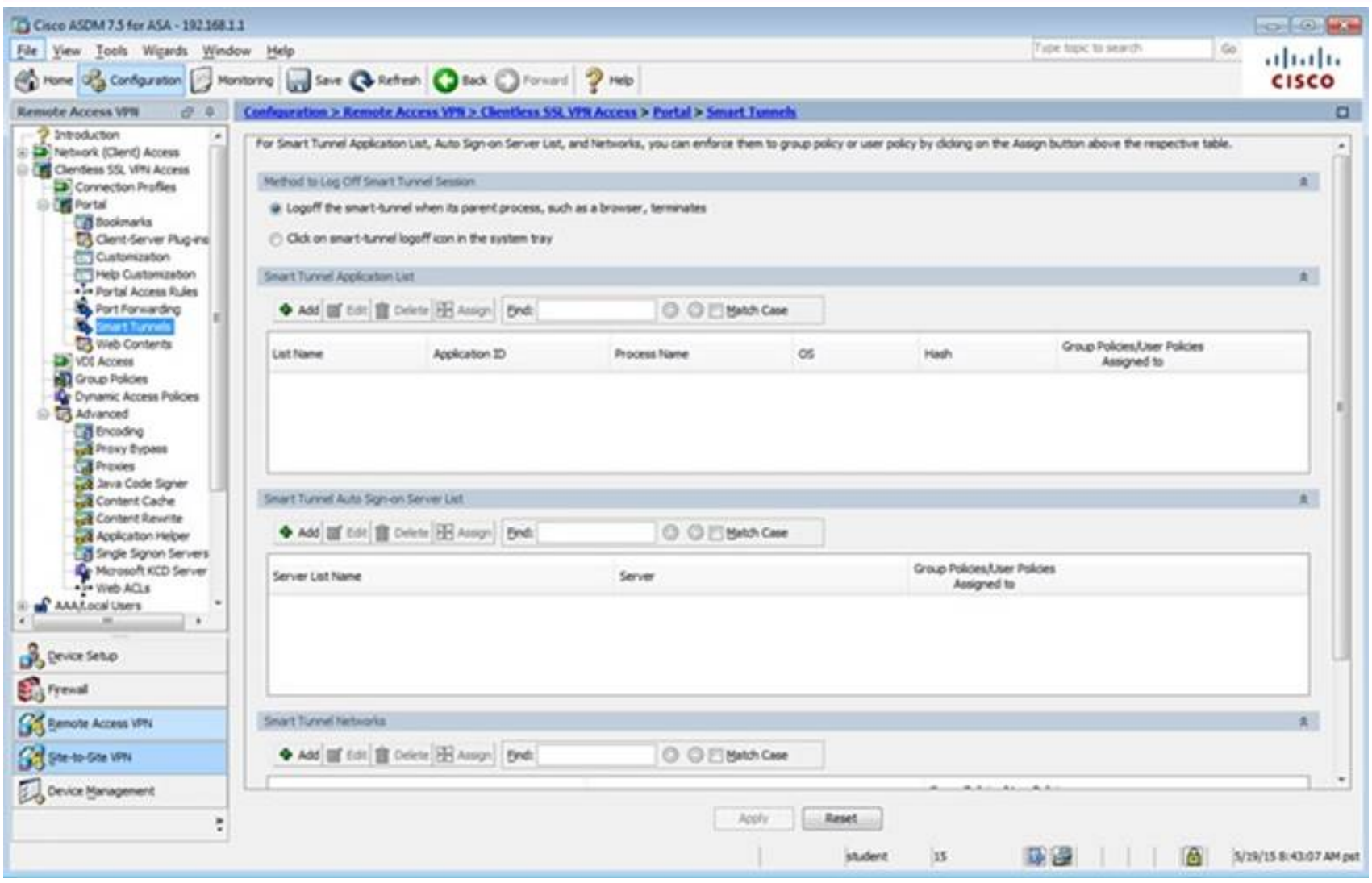

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen when authentication is rejected
Enable the display of SecurId messages on the login screen
Connection Aliases
This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.
Add
Delete
(The table is in-line editable.)
Alias
Enabled
test
Group URLs
This SSL VPN access method will automatically select the connection profile, without the need for user selection.
Add
Delete
(The table is in-line editable.)
URL
Enabled
https://209.165.201.2/test
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)
Always run CSD
Disable CSD for both AnyConnect and Clientless SSL VPN
Disable CSD for AnyConnect only
Find:
Next
Previous
OK
Cancel
Help

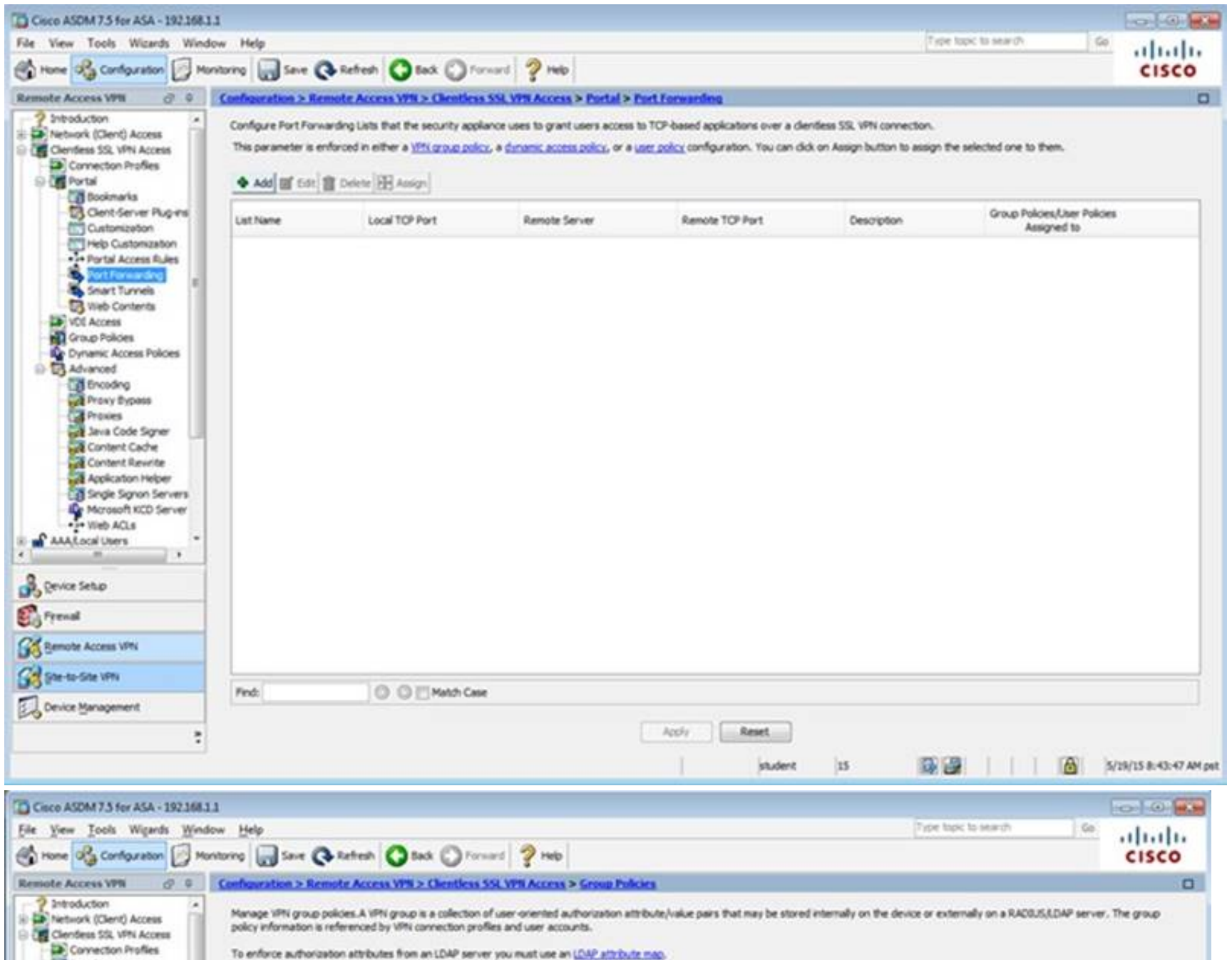

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from Certificate
Pre-fill Username from Certificate
Hide username from end user
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

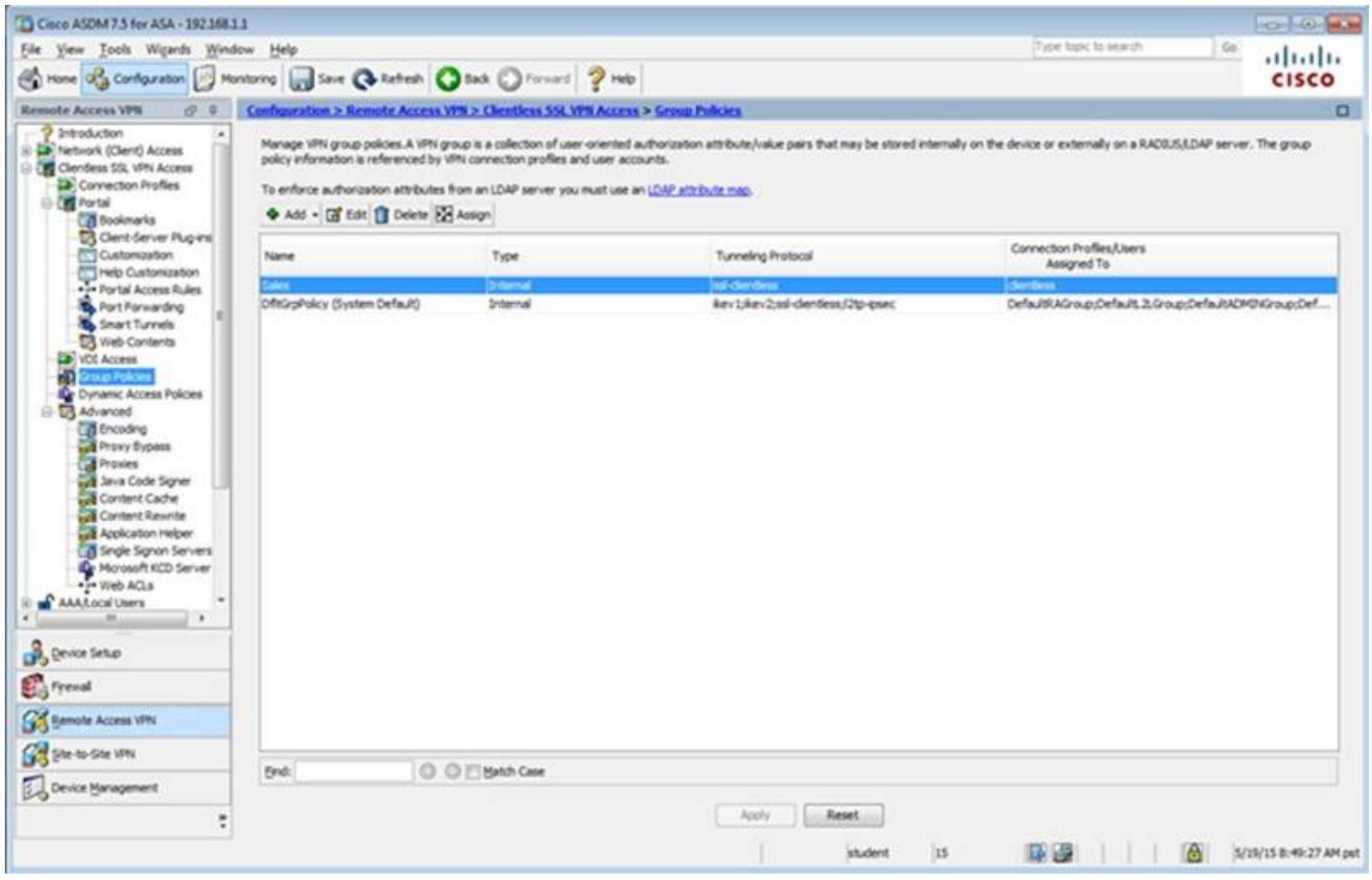

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
-- None --
Manage...
Use LOCAL if Server Group fails
Use primary username (Hide secondary username on login page)
Attributes Server:
Primary
Secondary
Session Username Server:
Primary
Secondary
Interface-Specific Secondary Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Use primary username
Username Mapping from Certificate
Pre-fill username from certificate
Hide username from end user
Fallback when a certificate is unavailable
Password:
Prompt
Use primary
Use
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

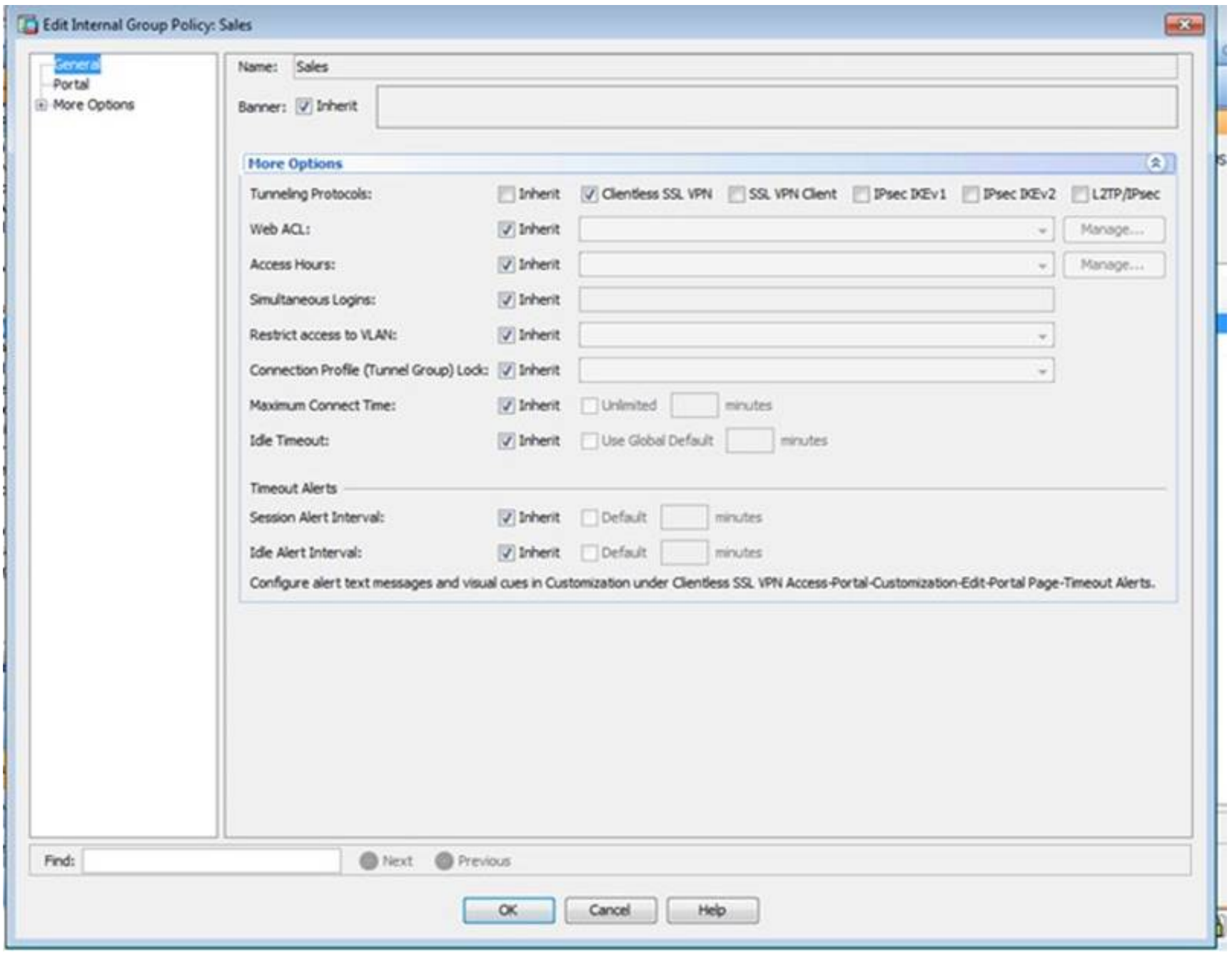

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add
Edit
Delete
Import
Export
Assign
Bookmarks
Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template
Inside-SRV
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:41:57 AM pst

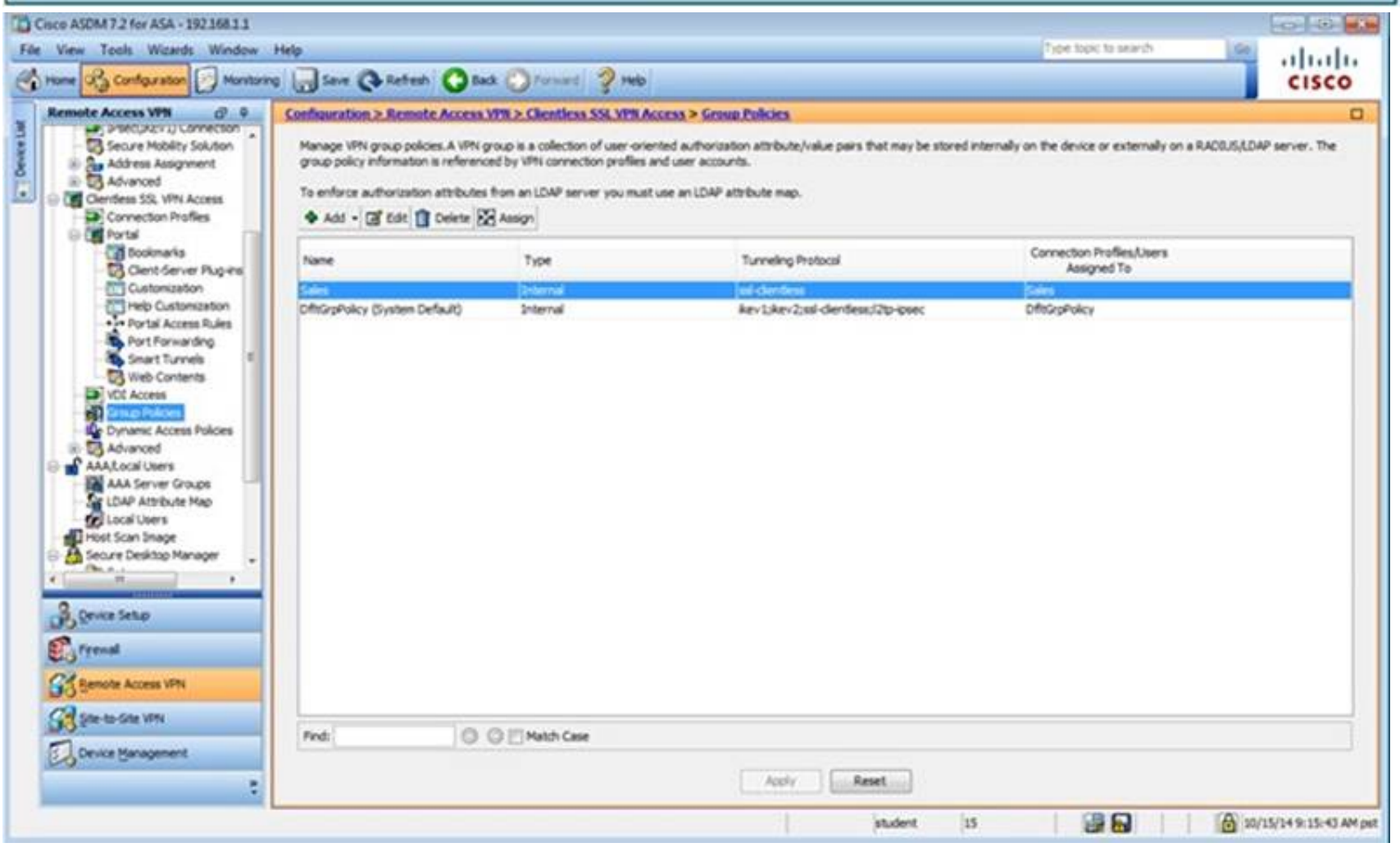

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

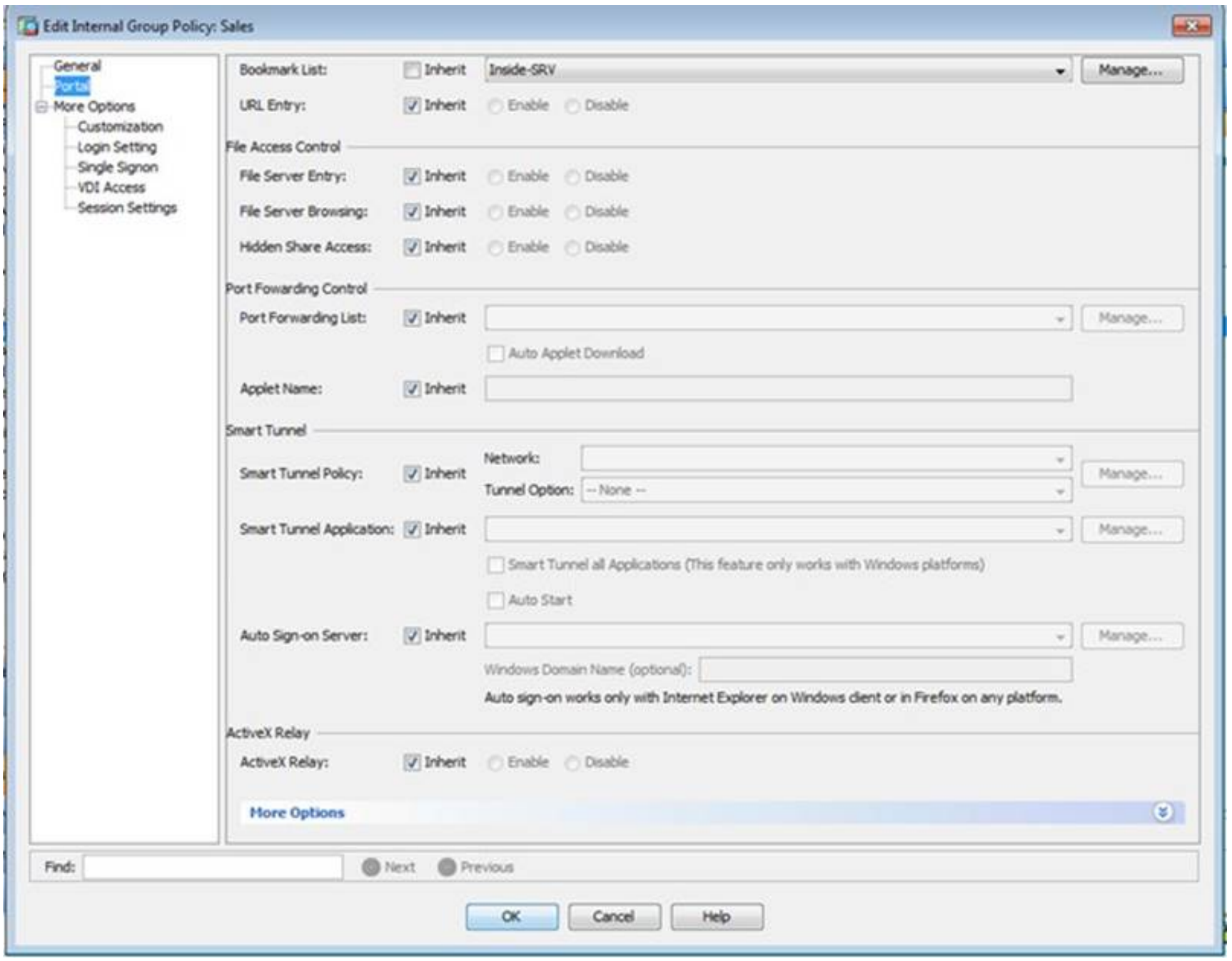

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Add Edit Delete Assign Find: Match Case
List Name
Application ID
Process Name
OS
Hash
Group Policies/User Policies Assigned to
Smart Tunnel Auto Sign-on Server List
Add Edit Delete Assign Find: Match Case
Server List Name
Server
Group Policies/User Policies Assigned to
Smart Tunnel Networks
Add Edit Delete Assign Find: Match Case
Apply
Reset
student
15
5/19/15 8:43:07 AM pst

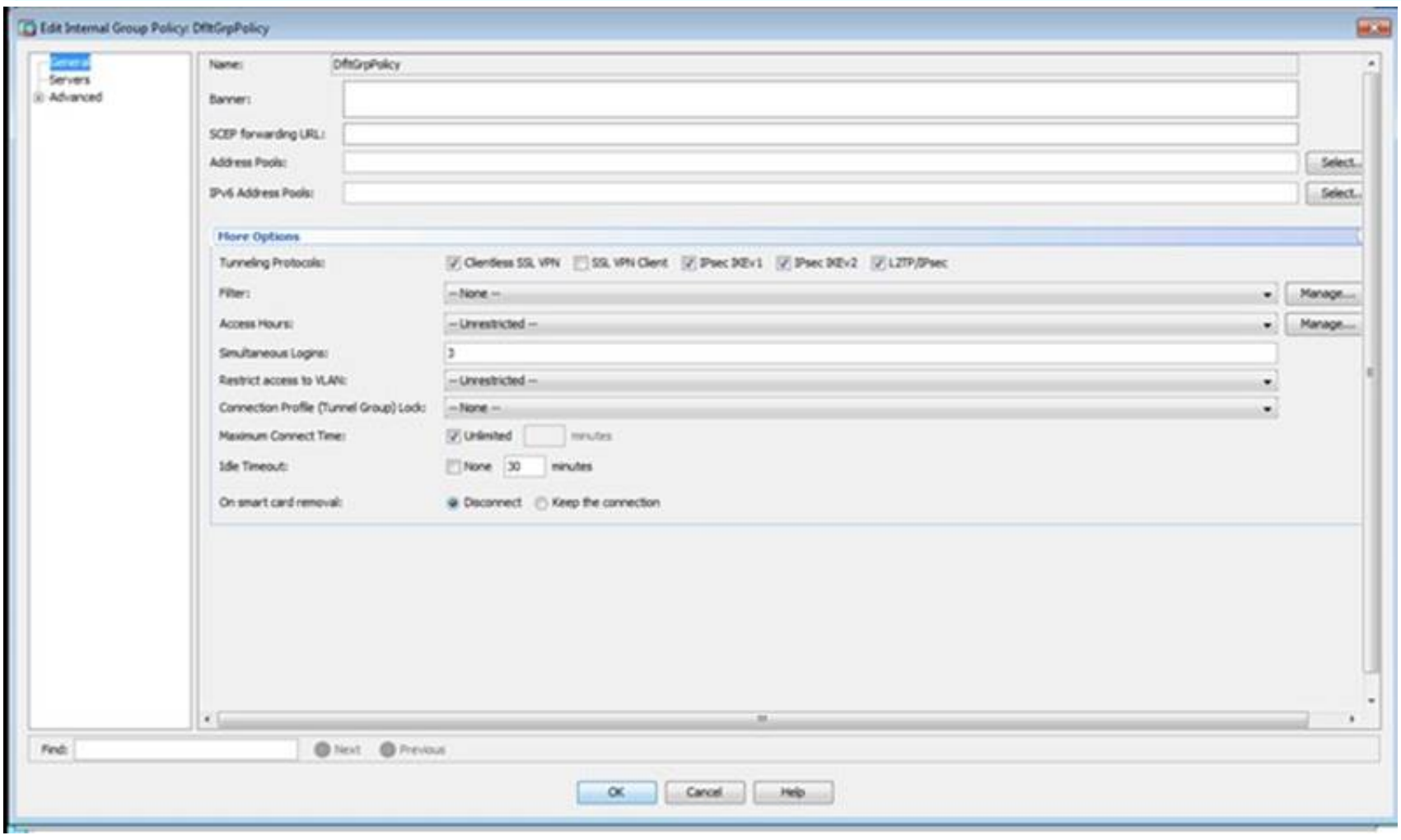

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add Edit Delete Assign
List Name
Local TCP Port
Remote Server
Remote TCP Port
Description
Group Policies/User Policies Assigned to
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:43:47 AM pst

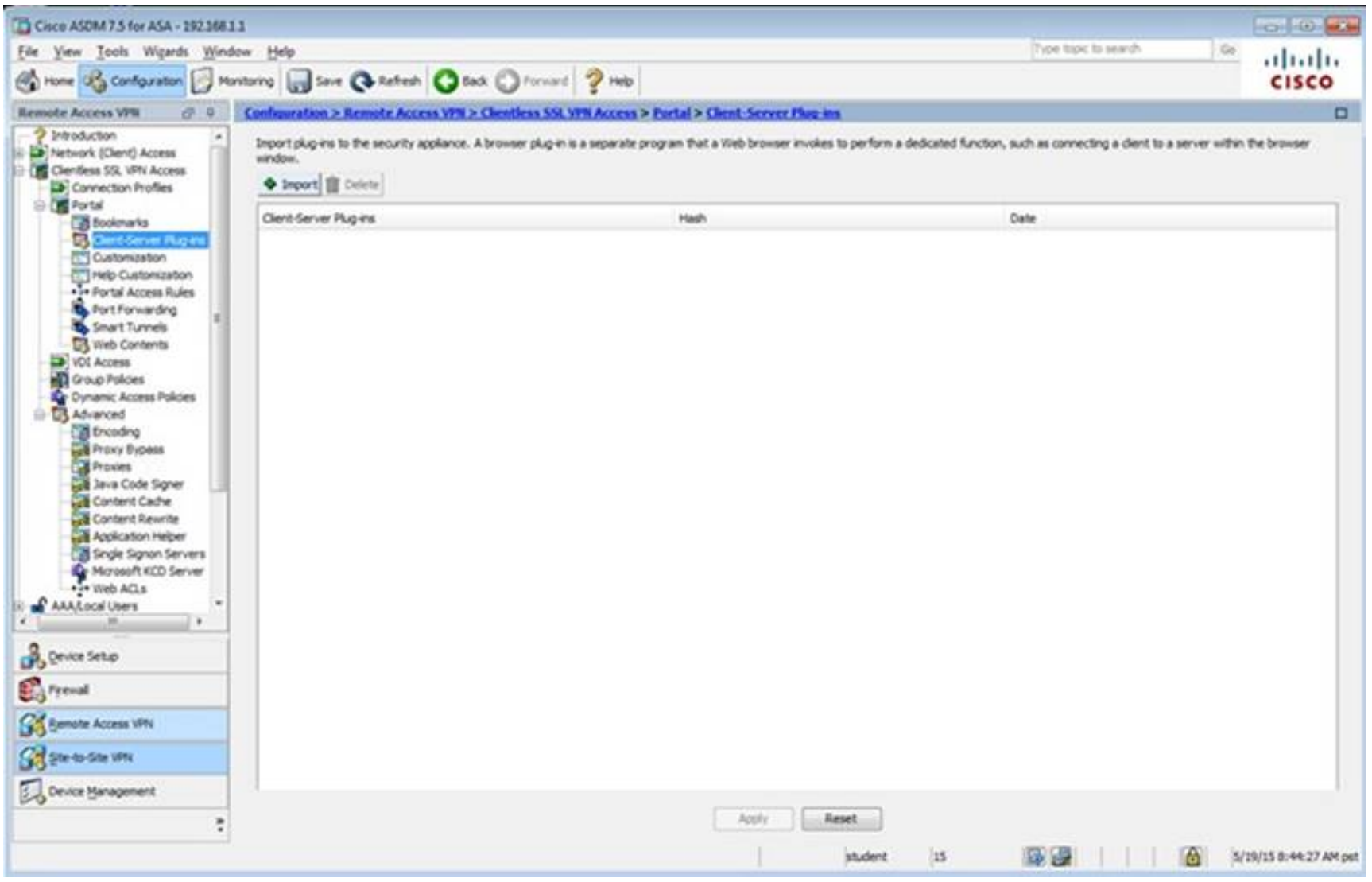

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:49:27 AM pst

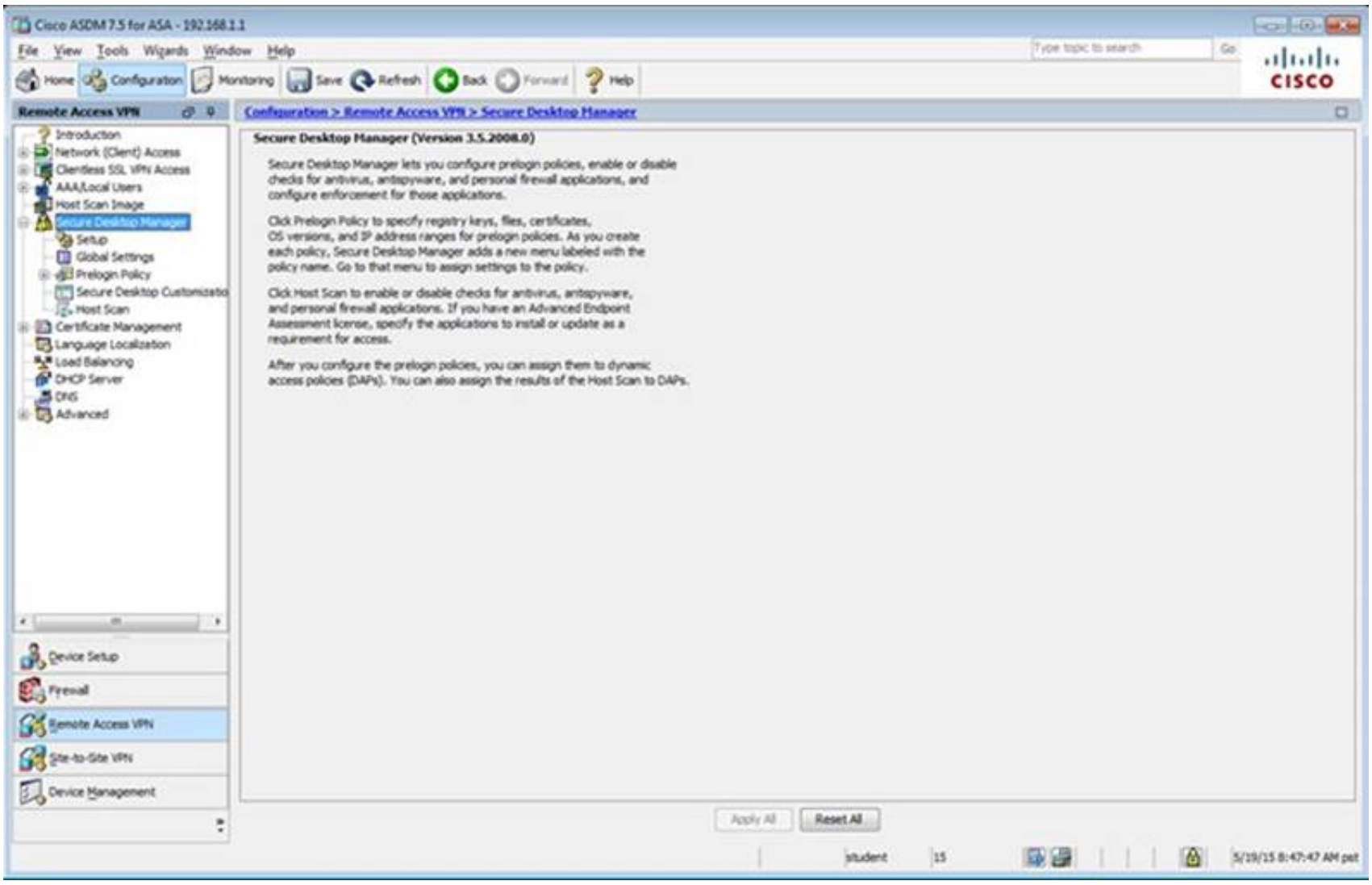

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access to VLAN: Inherit
Connection Profile (Tunnel Group) Lock: Inherit
Maximum Connect Time: Inherit Unlimited minutes
Idle Timeout: Inherit Use Global Default minutes
Timeout Alerts
Session Alert Interval: Inherit Default minutes
Idle Alert Interval: Inherit Default minutes
Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.
Find: Next Previous
OK Cancel Help

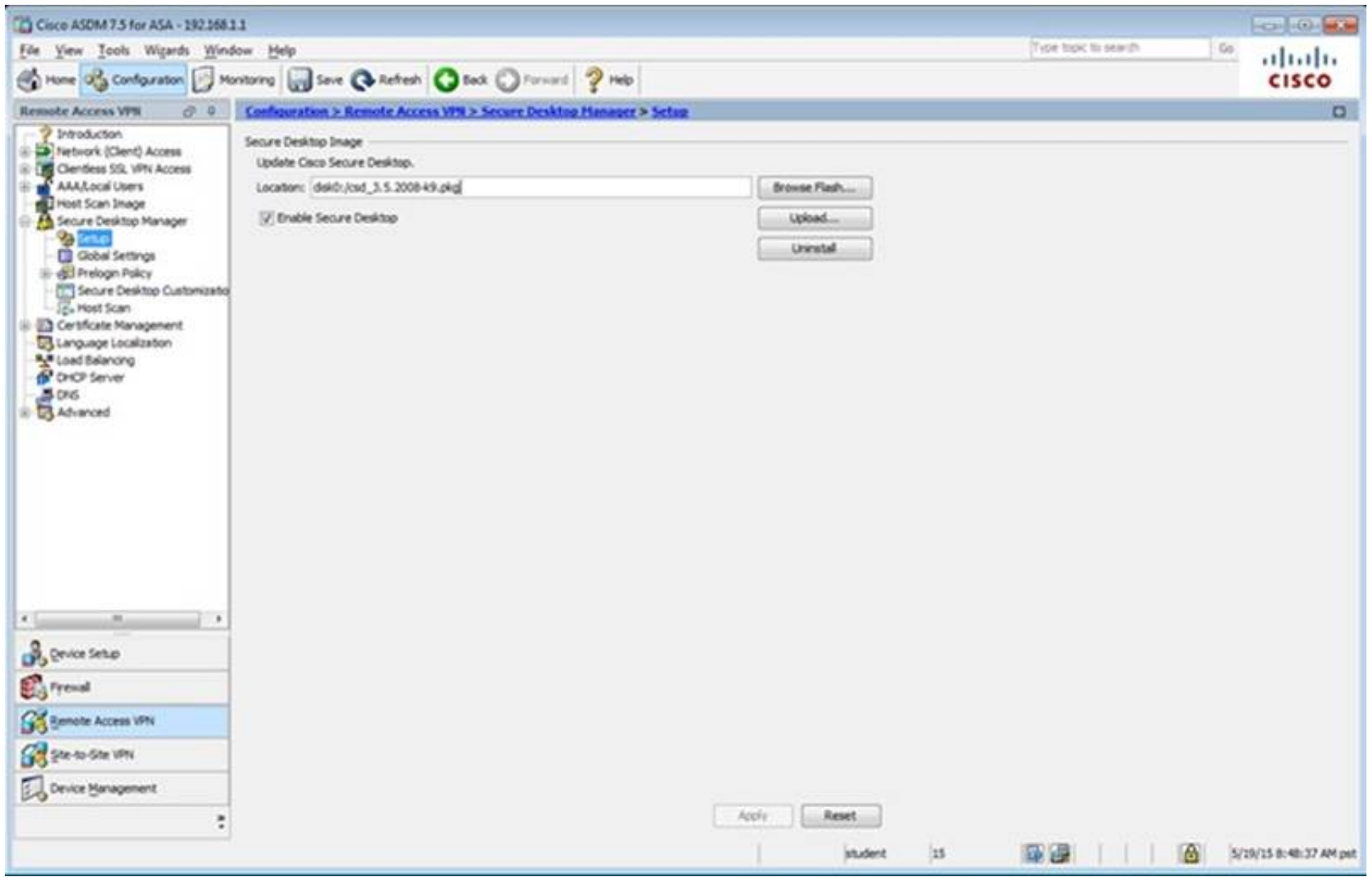

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
Sales
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DfltGrpPolicy
Find: Match Case
Apply Reset
student 15
10/15/14 9:15:43 AM pst

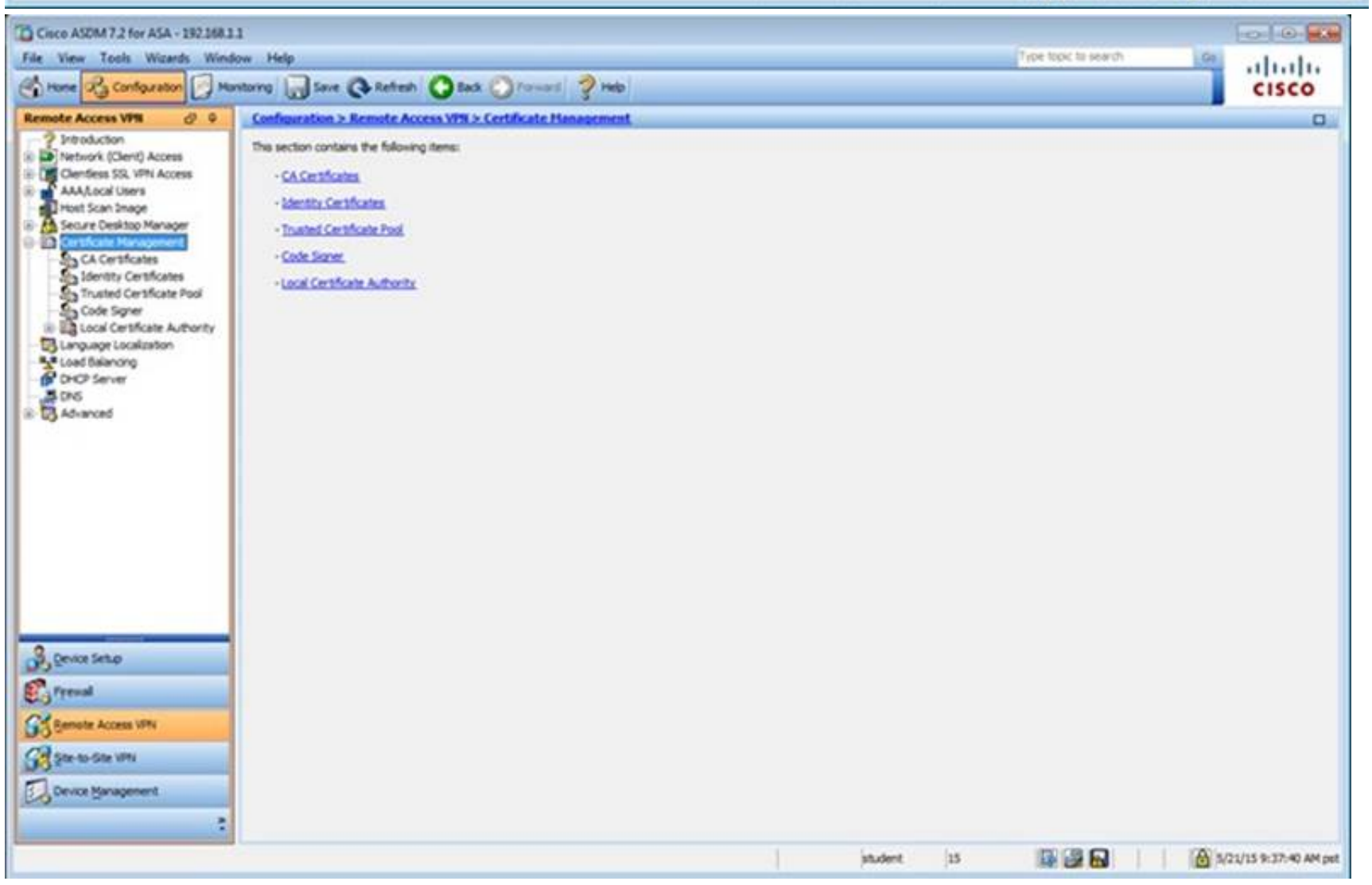

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding Control
Port Forwarding List:
Auto Applet Download
Applet Name:
Smart Tunnel
Network:
Smart Tunnel Policy:
Tunnel Option:
-- None --
Smart Tunnel Application:
Smart Tunnel all Applications (This feature only works with Windows platforms)
Auto Start
Auto Sign-on Server:
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:
More Options
Find:
Next
Previous
OK
Cancel
Help

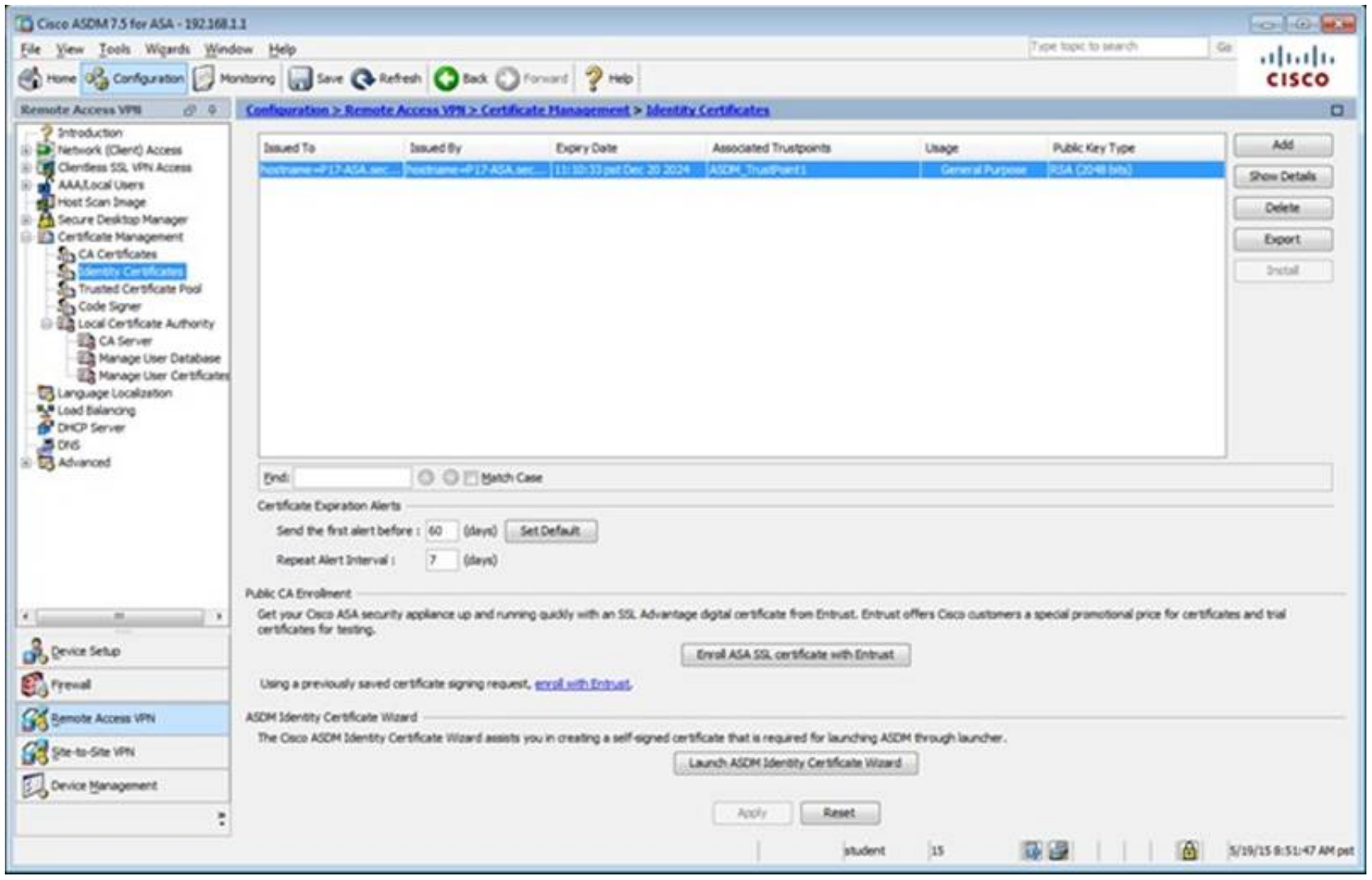

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
IPv6 Address Pools:
Select...
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- Unrestricted --
Simultaneous Logins:
3
Restrict access to VLAN:
Connection Profile (Tunnel Group) Lock:
Maximum Connect Time:
Unlimited
minutes
Idle Timeout:
None
30
minutes
On smart card removal:
Disconnect
Keep the connection
Find:
Next
Previous
OK
Cancel
Help

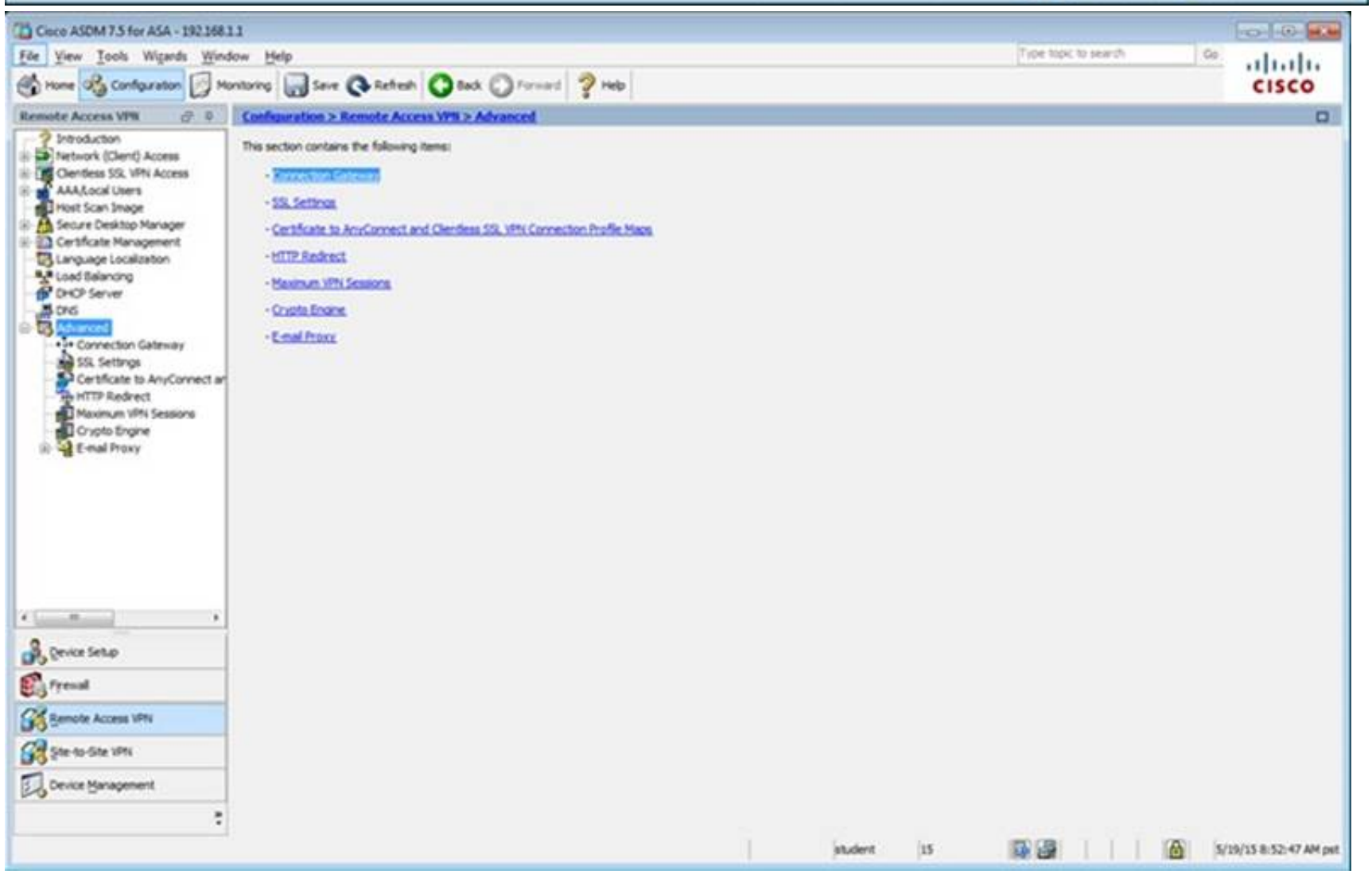

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:44:27 AM pst

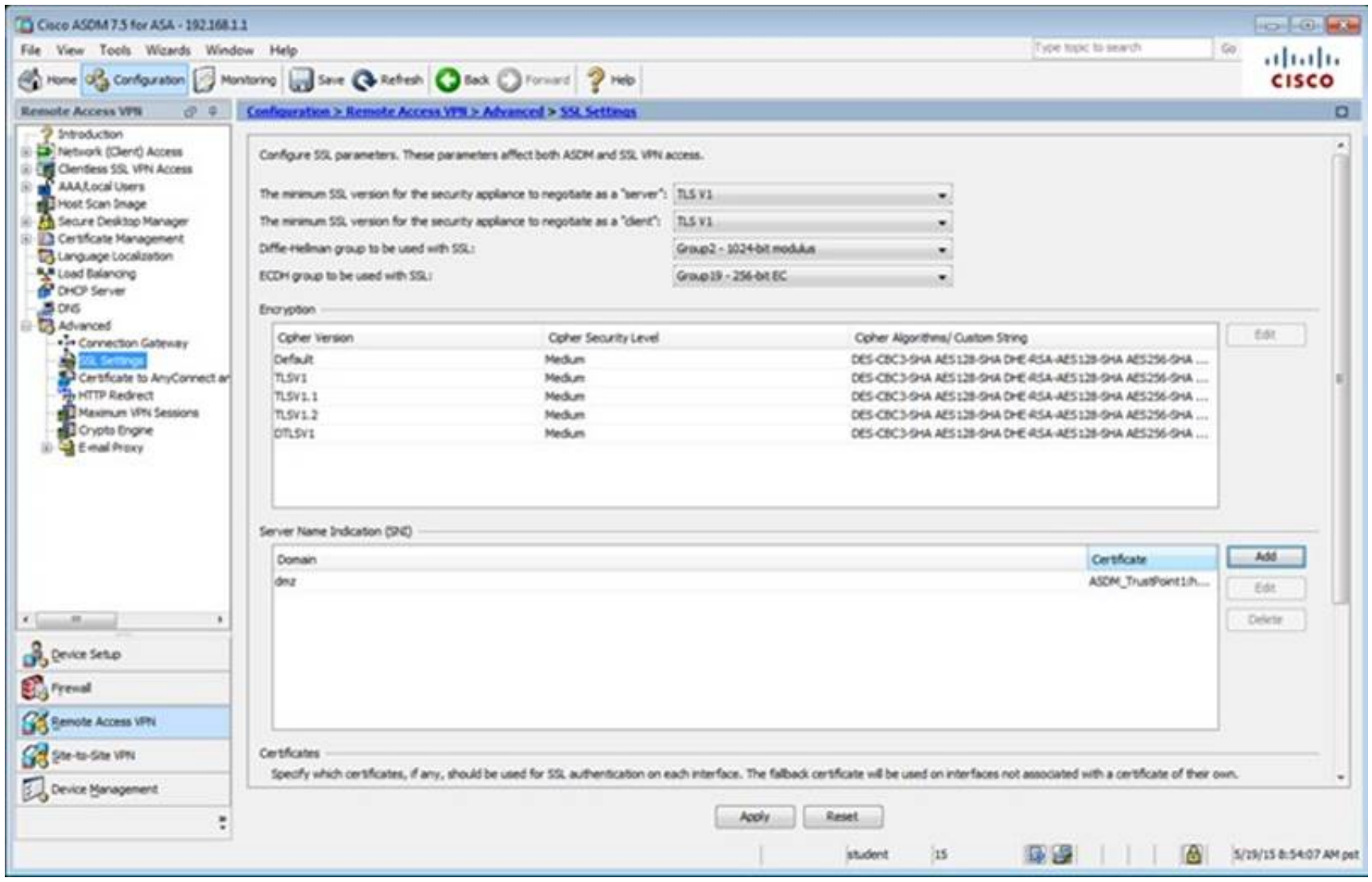

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Secure Desktop Customizatio
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply All
Reset All
student
15
5/19/15 8:47:47 AM pst

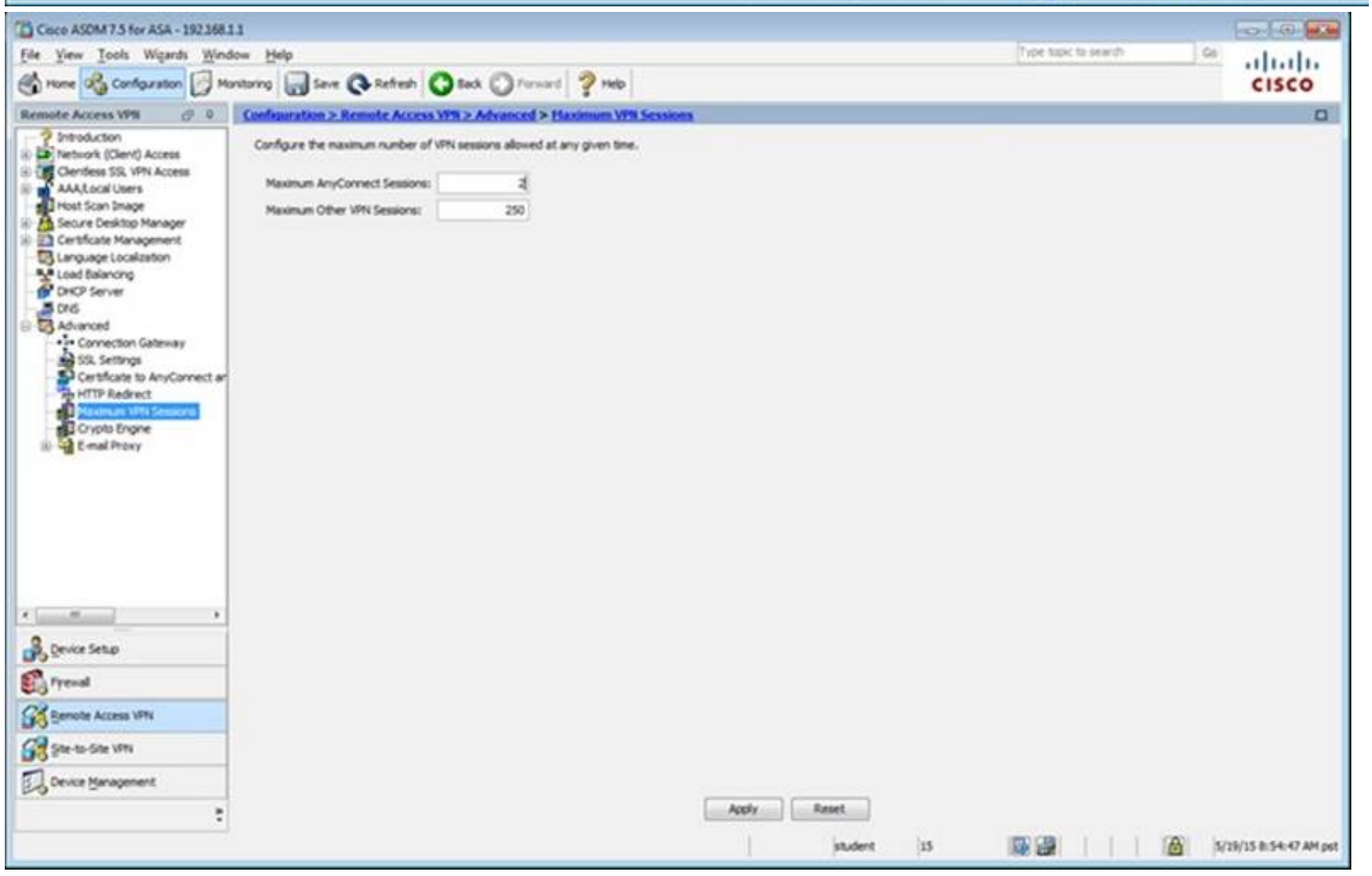

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager > Setup
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Secure Desktop Image
Update Cisco Secure Desktop.
Location: disk0:/csd_3.5.2008-49.pkg
Browse Flash...
Enable Secure Desktop
Upload...
Uninstall
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:48:37 AM pst

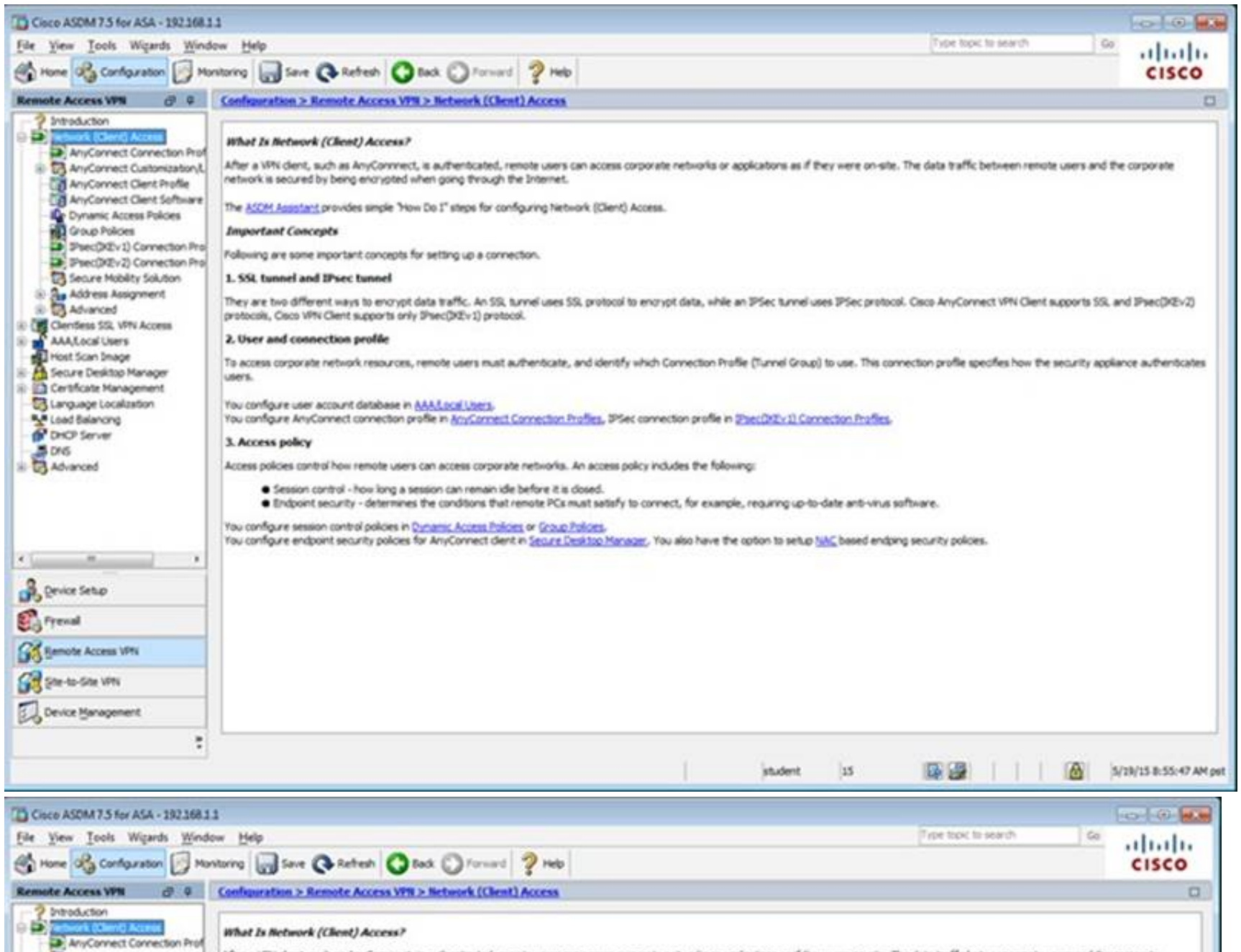

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/21/15 9:37:40 AM pst

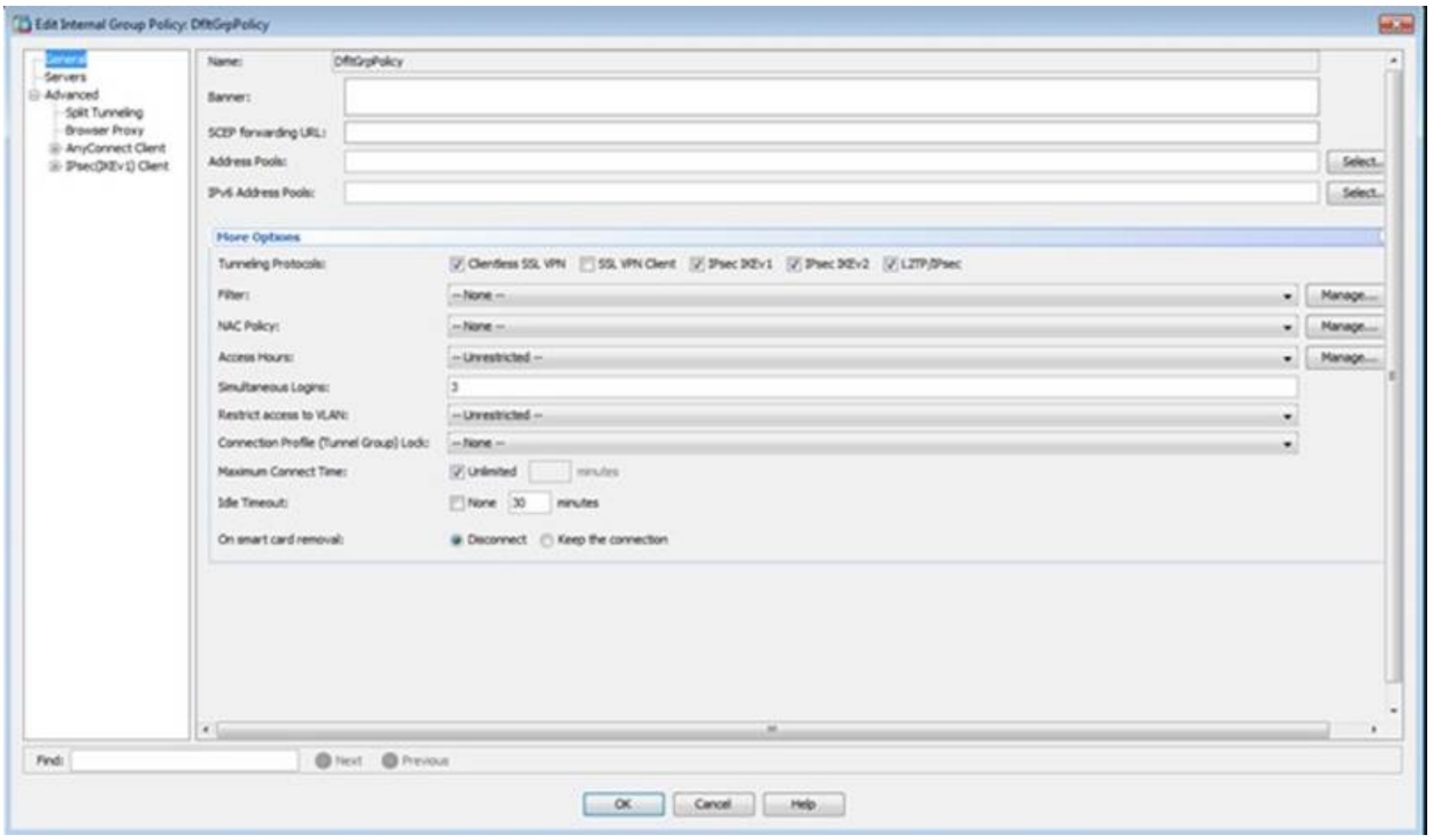

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
CA Server
Manage User Database
Manage User Certificates
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
Public Key Type
Add
Show Details
Delete
Export
Install
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:51:47 AM pst

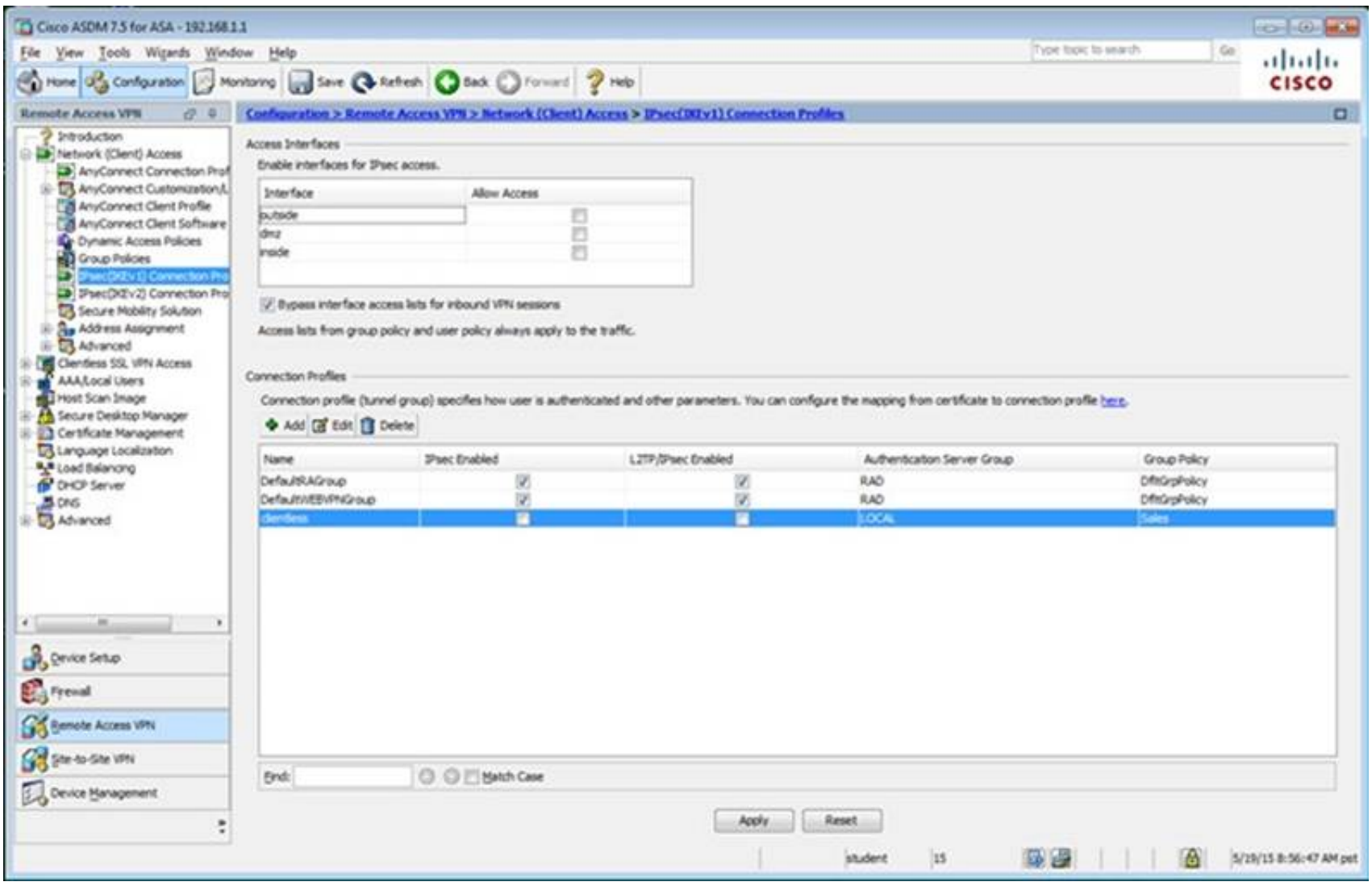

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect and
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:52:47 AM pst

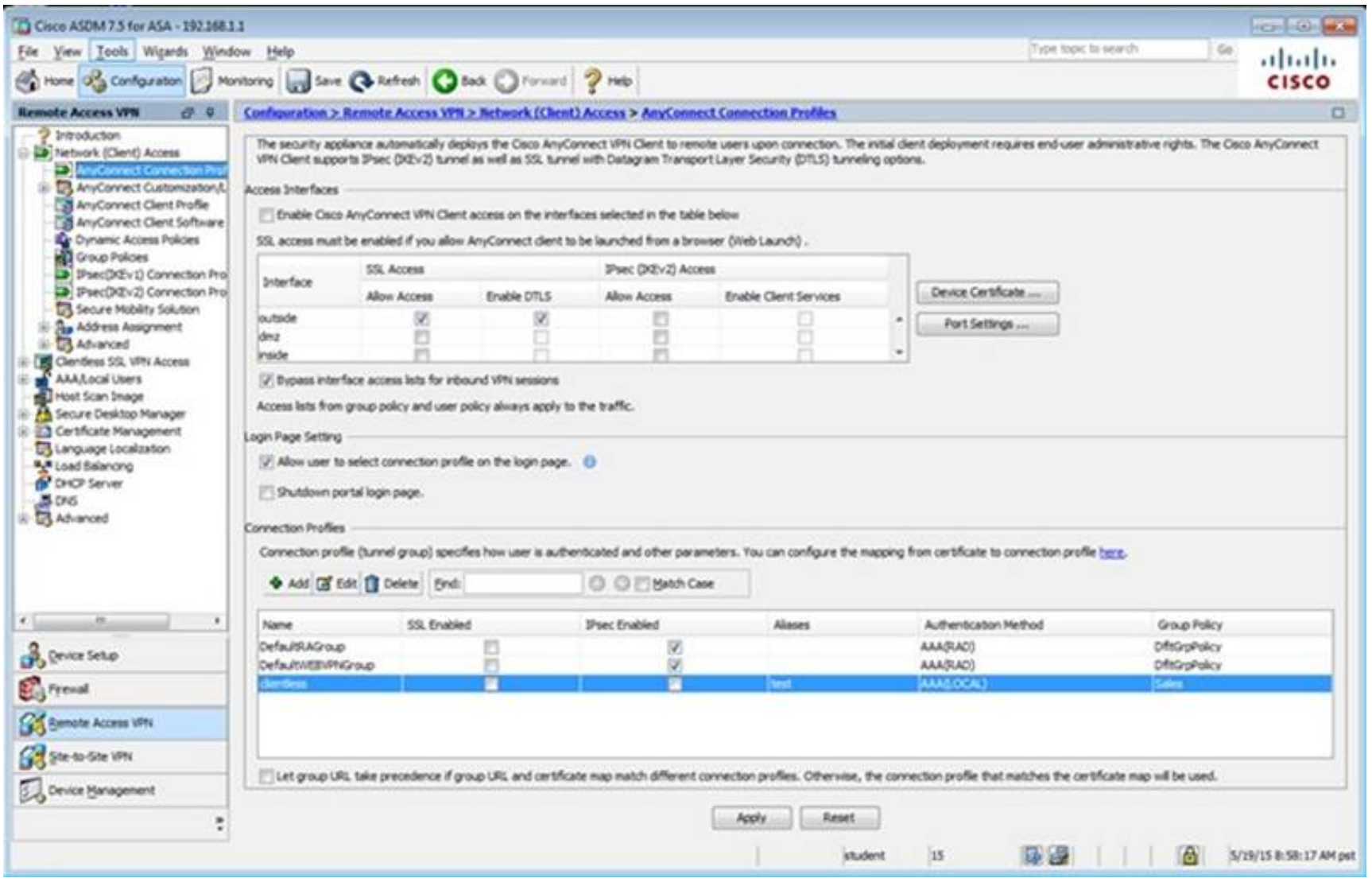

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
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
Edit
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
Add
Edit
Delete
dmz
ASDM_TrustPoint1:h...
Certificates
Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:54:07 AM pst

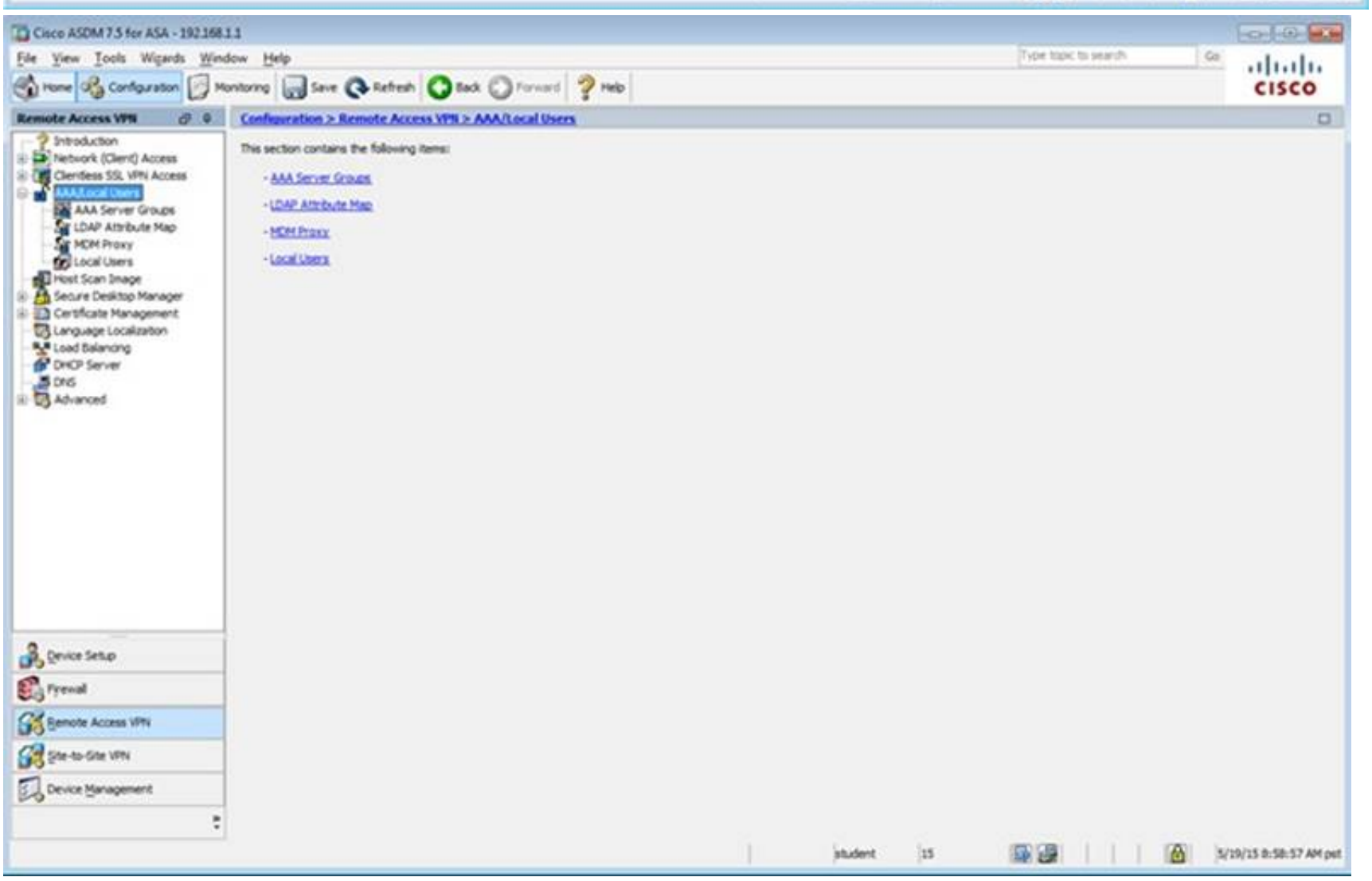

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Configure the maximum number of VPN sessions allowed at any given time.
Maximum AnyConnect Sessions: 2
Maximum Other VPN Sessions: 250
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:54:47 AM pst

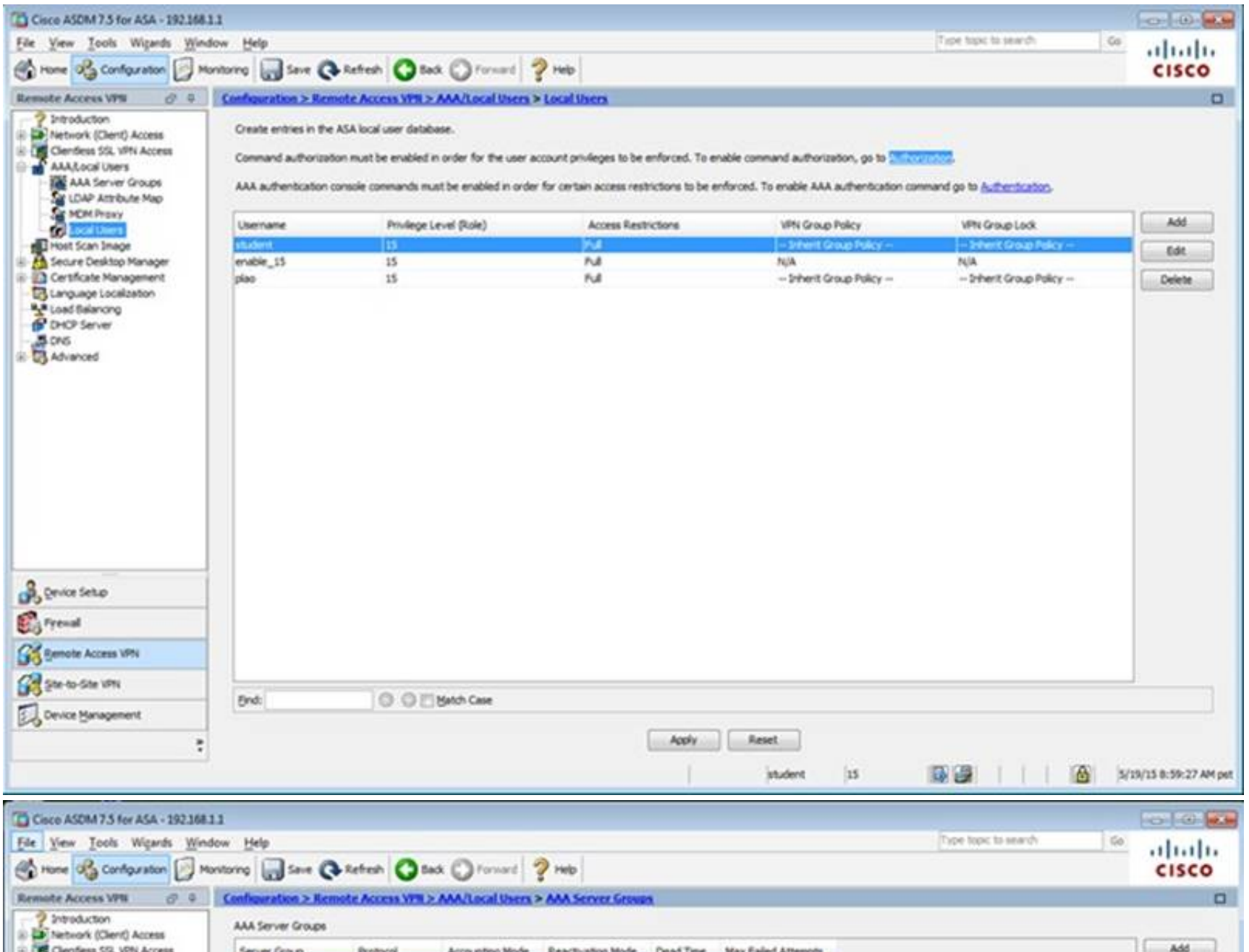

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
The ASDM Assistant provides simple "How Do I" steps for configuring Network (Client) Access.
Important Concepts
Following are some important concepts for setting up a connection.
1. SSL tunnel and IPsec tunnel
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 endpng security policies.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/19/15 8:55:47 AM pst

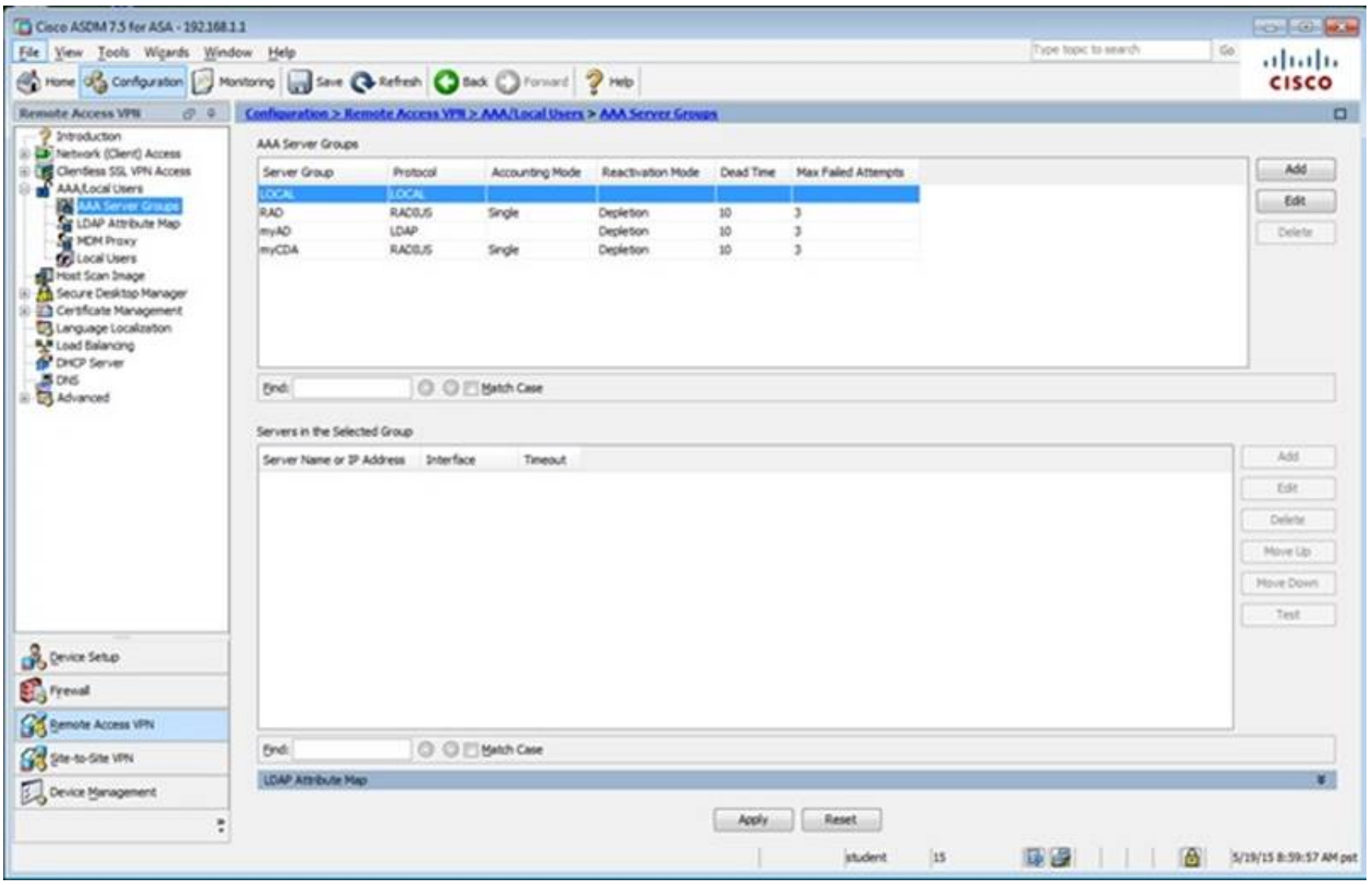

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Name: DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
IPv6 Address Pools:
Select...
More Options
Tunneling Protocols: Clientless SSL VPN, SSL VPN Client, IPsec 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
Idle Timeout: None 30 minutes
On smart card removal: Disconnect, Keep the connection
Manage...
Find:
Next
Previous
OK
Cancel
Help


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Prof
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Authentication Server Group
Group Policy
DefaultRAGroup
RAD
DfltGrpPolicy
DefaultWEBVPNGroup
RAD
DfltGrpPolicy
clientless
LOCAL
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:56:47 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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
Allow Access
Enable DTLS
IPsec (IKEv2) Access
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
DefaultWEBVPNGroup
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:17 AM pst

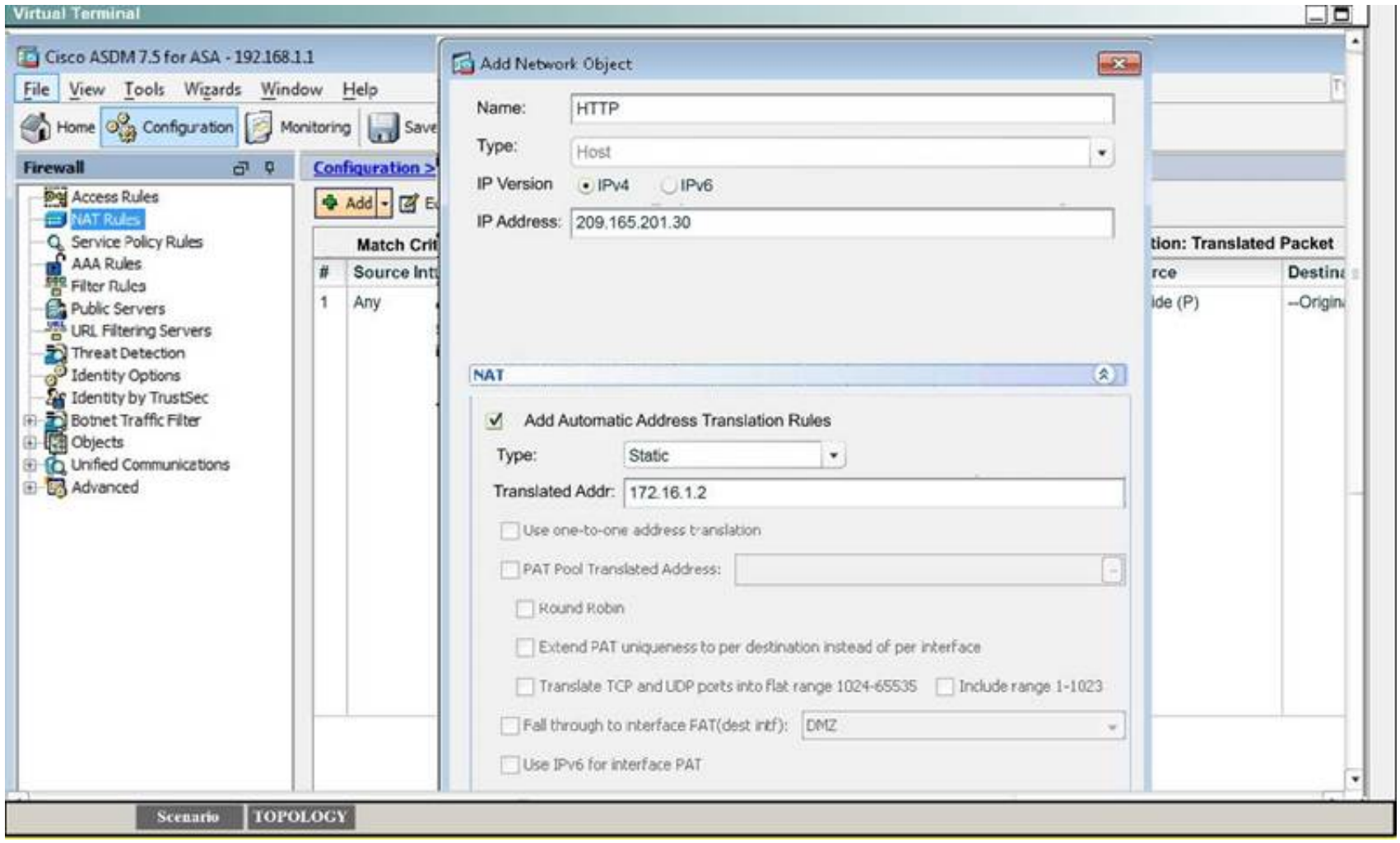

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > AAA/Local Users
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:57 AM pst



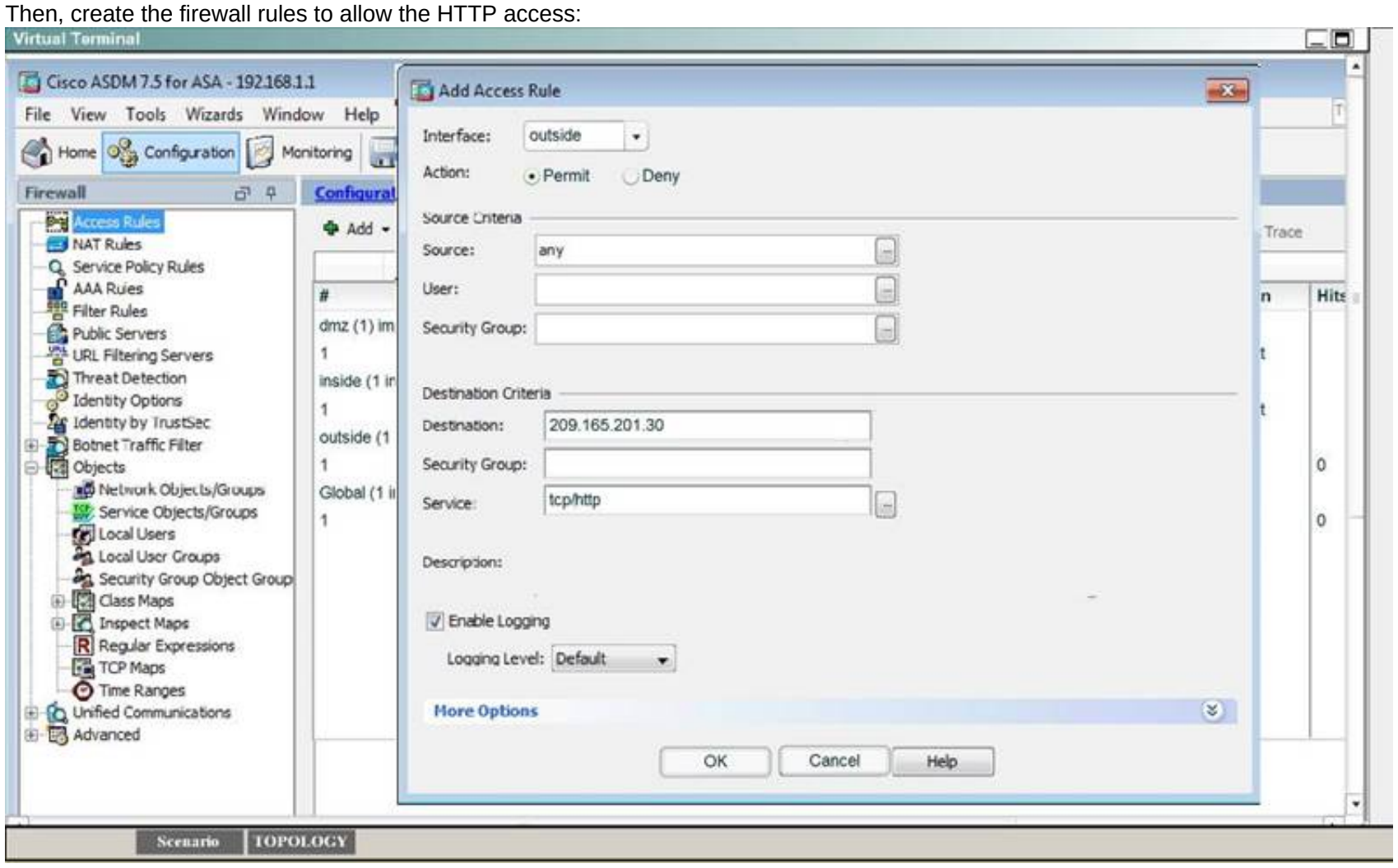


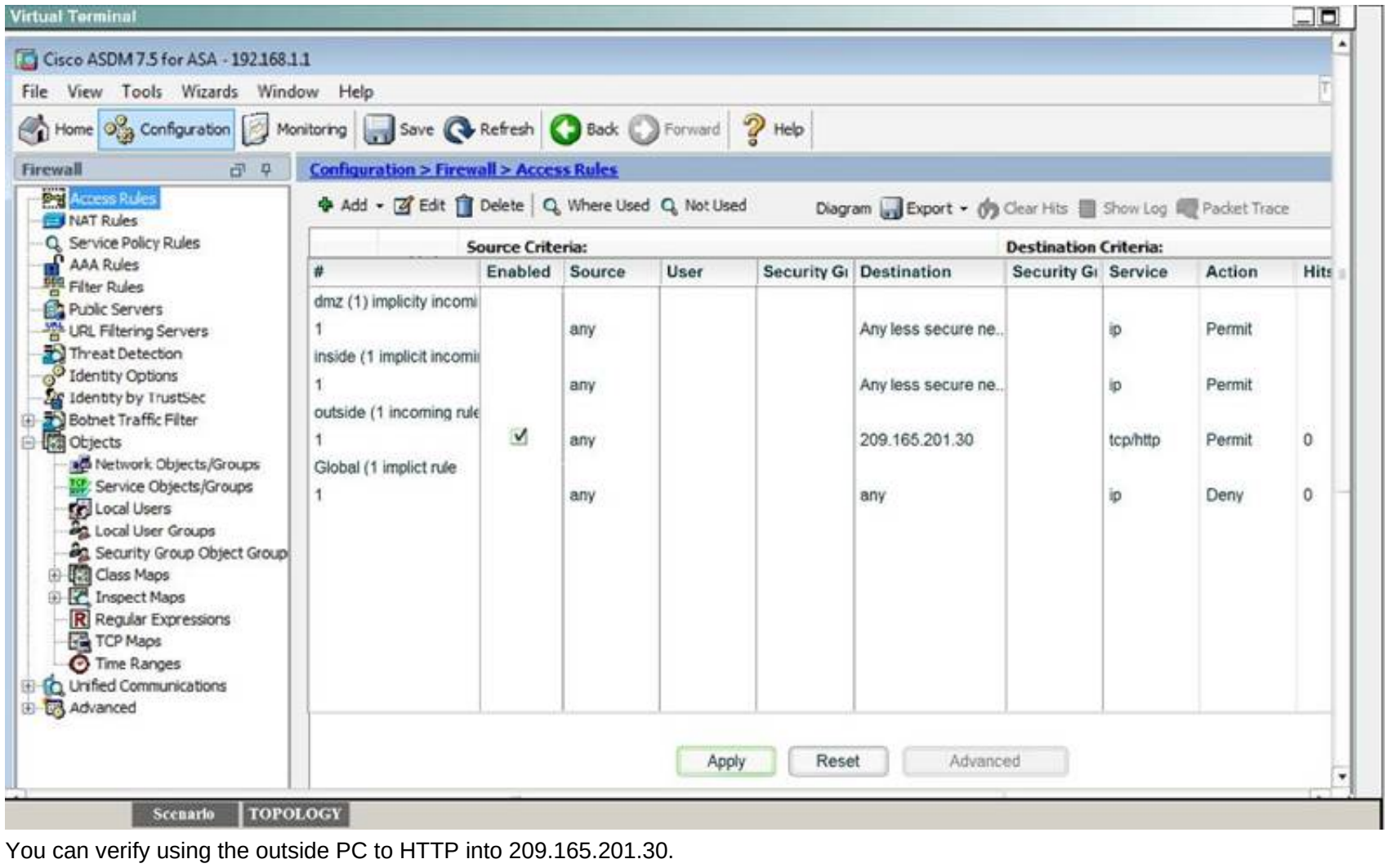
Answer:

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.



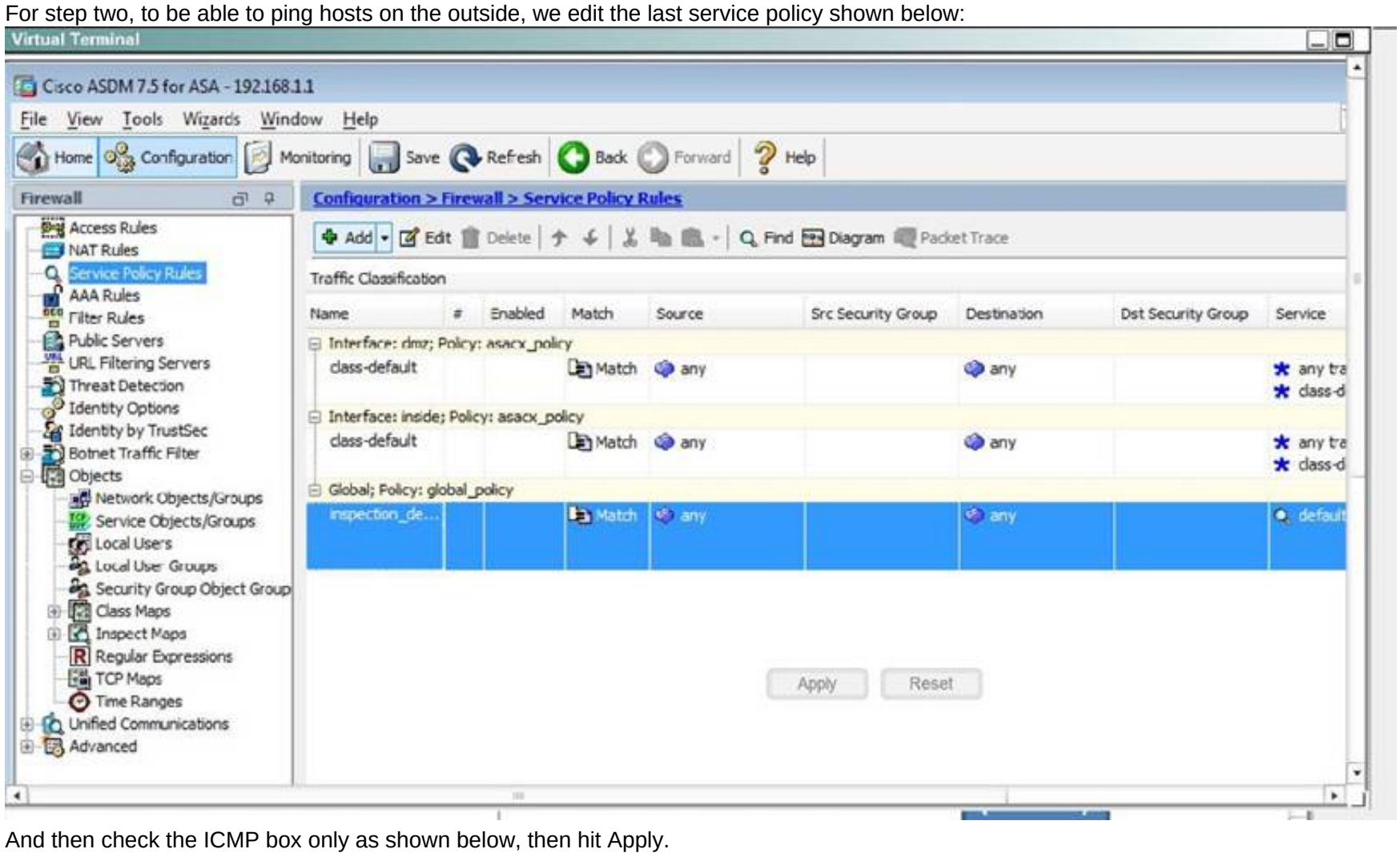
Then, create the firewall rules to allow the HTTP access:



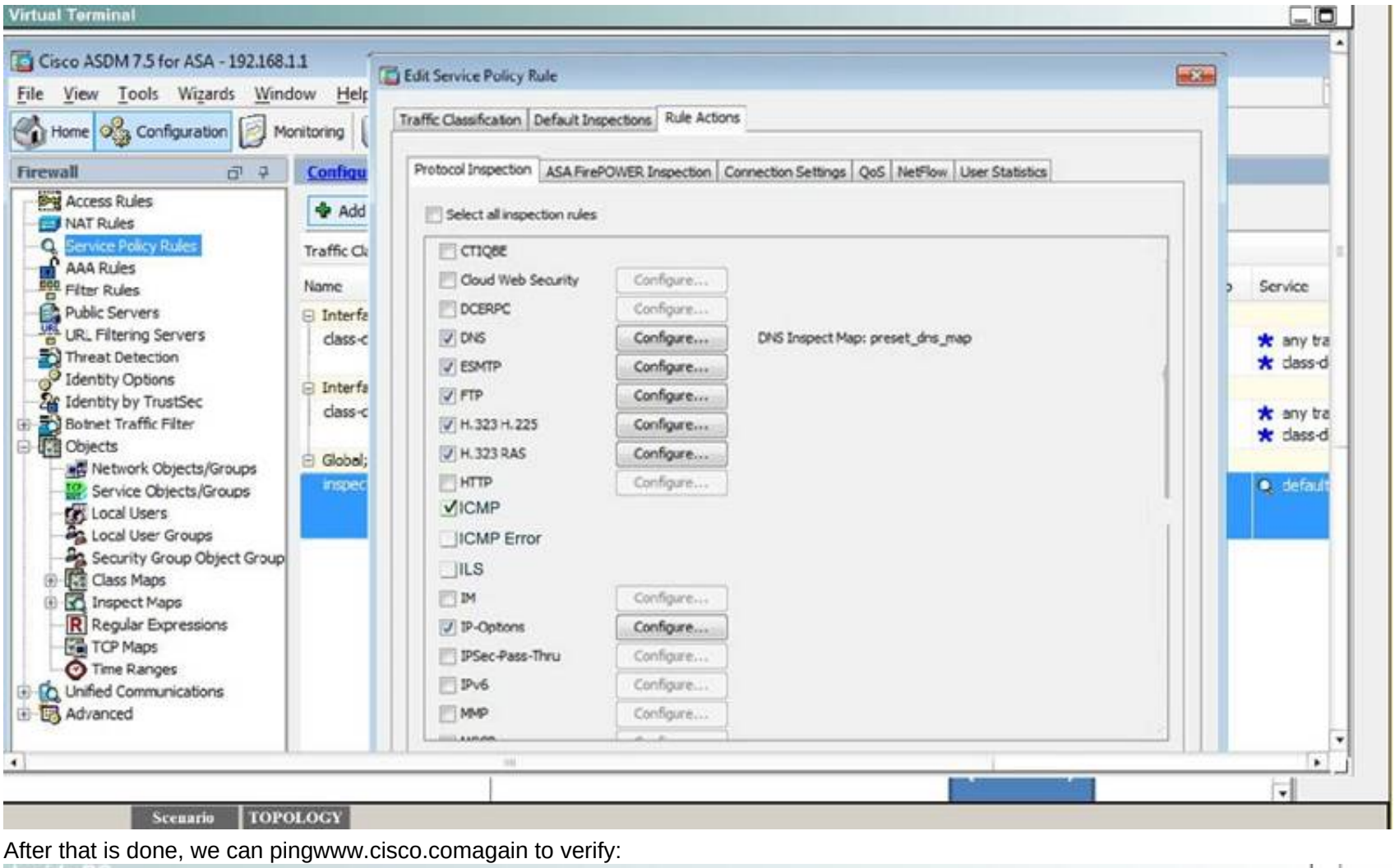


You can verify using the outside PC to HTTP into 209.165.201.30.

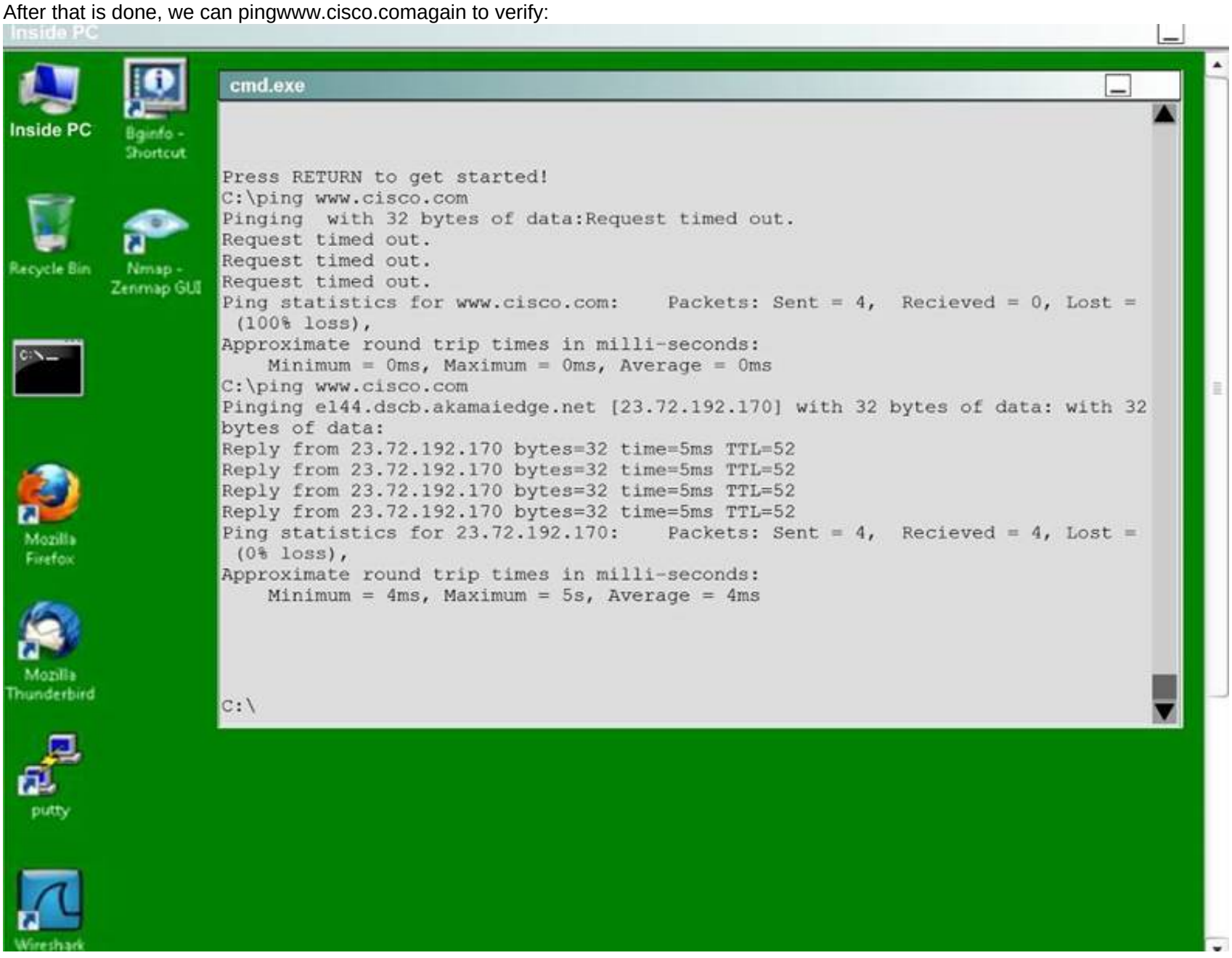
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



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



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



NEW QUESTION 10
How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

A. Traffic between two interfaces in the same zone is allowed by default.
B. Traffic between interfaces in the same zone is blocked unless you configure the same-security permit command.
C. Traffic between interfaces in the same zone is always blocked.
D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.

Answer: A

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

NEW QUESTION 15
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 16
Refer to the exhibit.

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

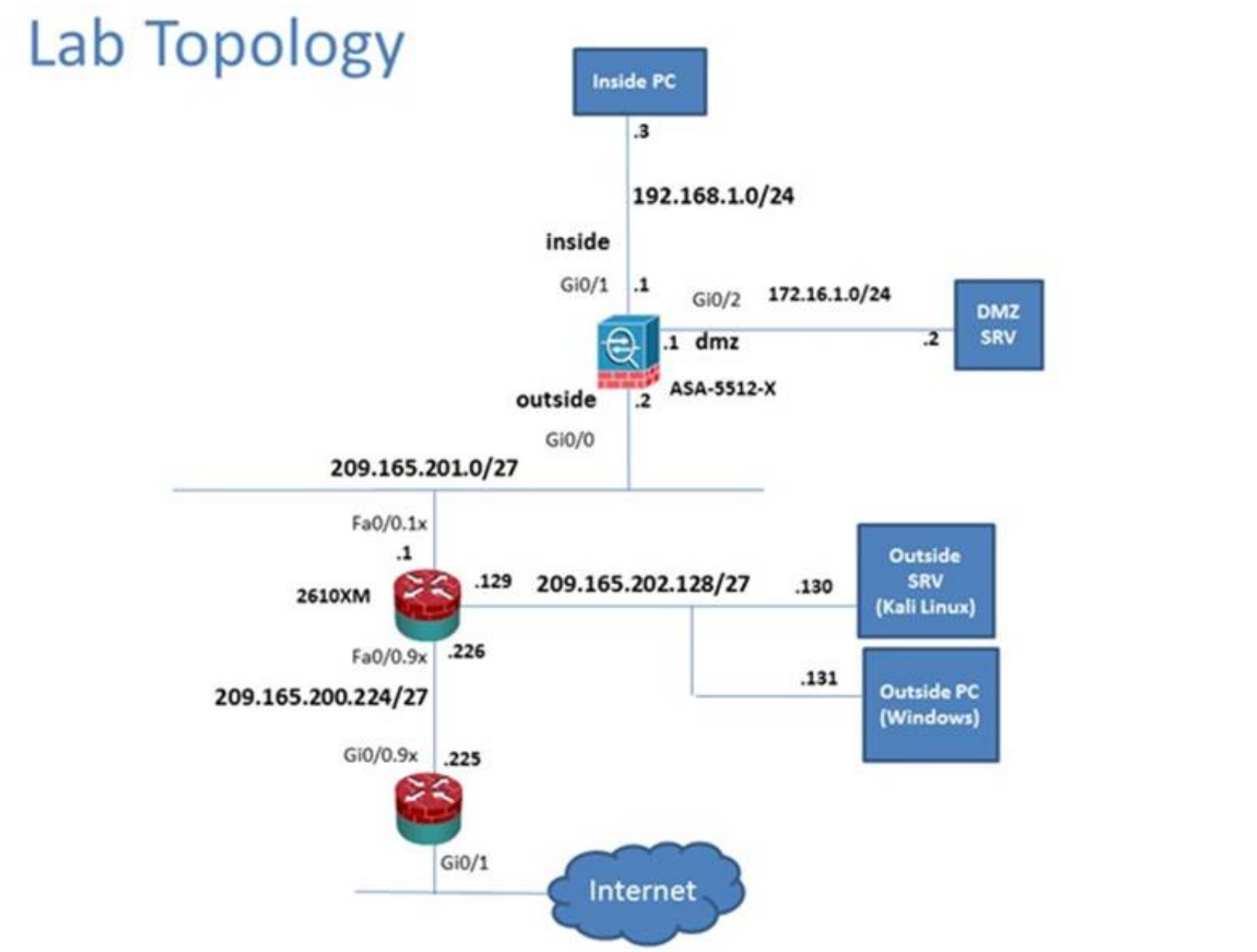
Which statement about the device time is true?

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

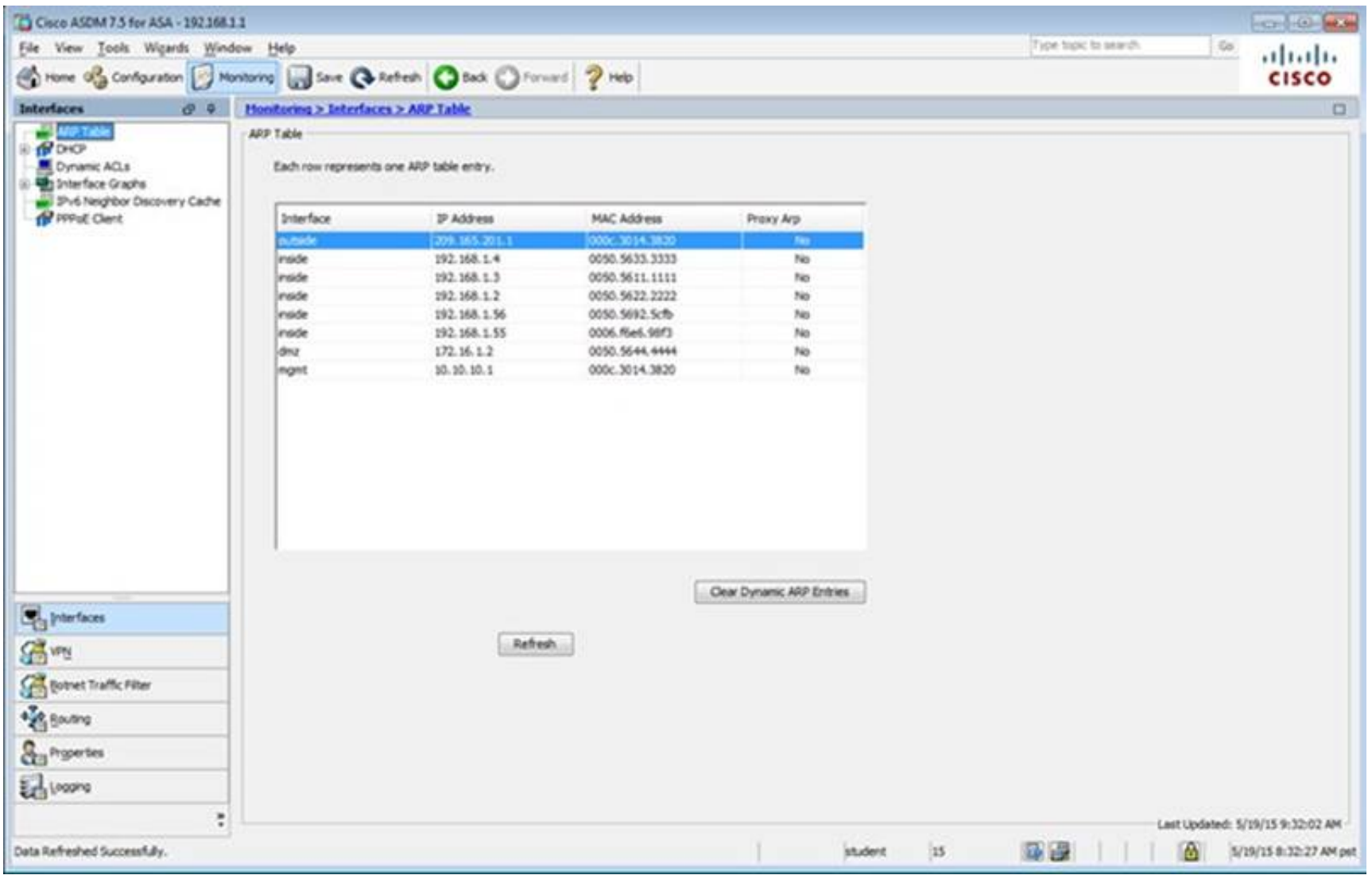
Answer: A

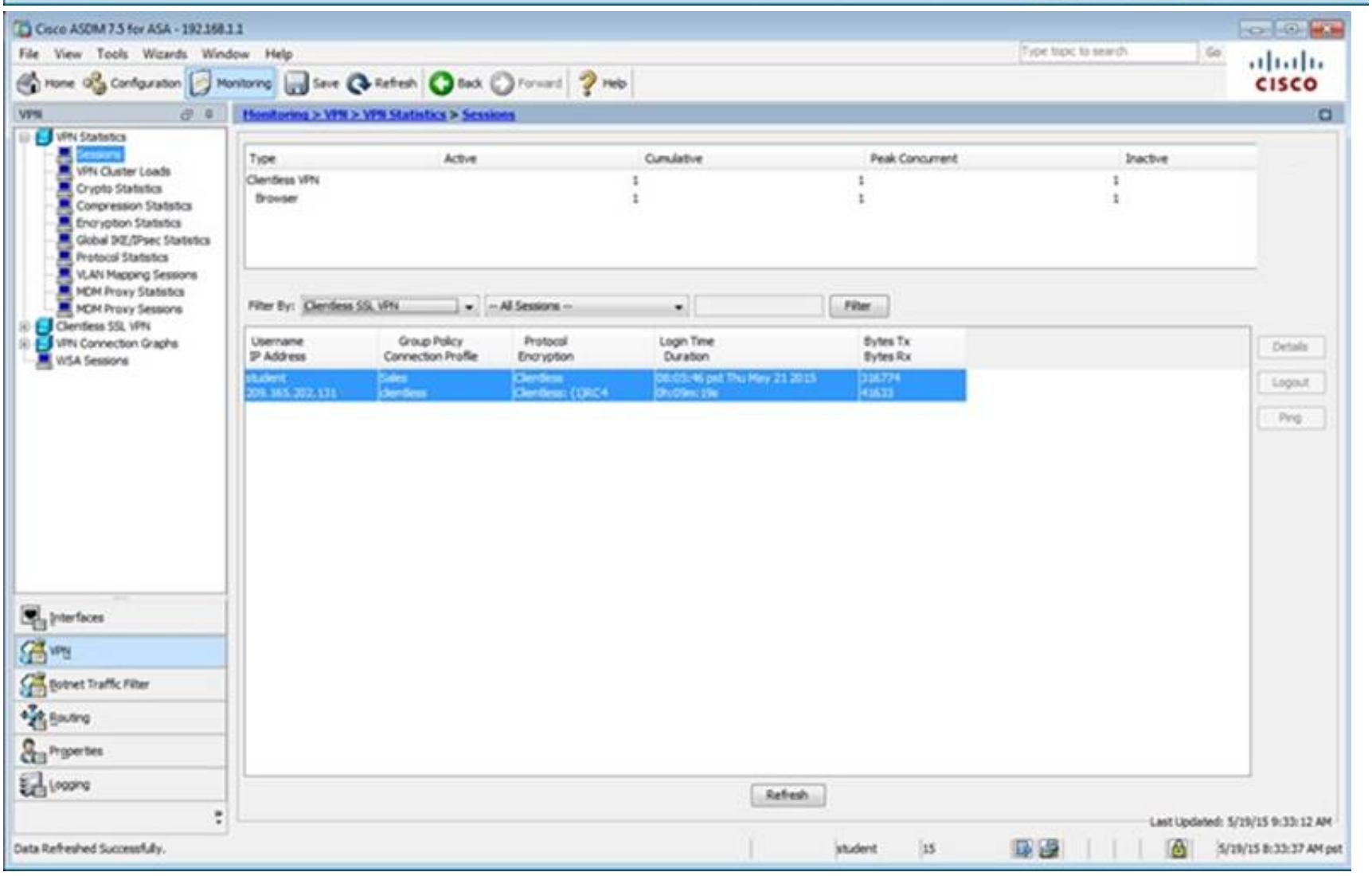
Explanation: Remember: The [.] at the beginning of the time tells us the NTP process has last contact with its servers. We know the time is authoritative because there would be a [*] at the beginning if not.

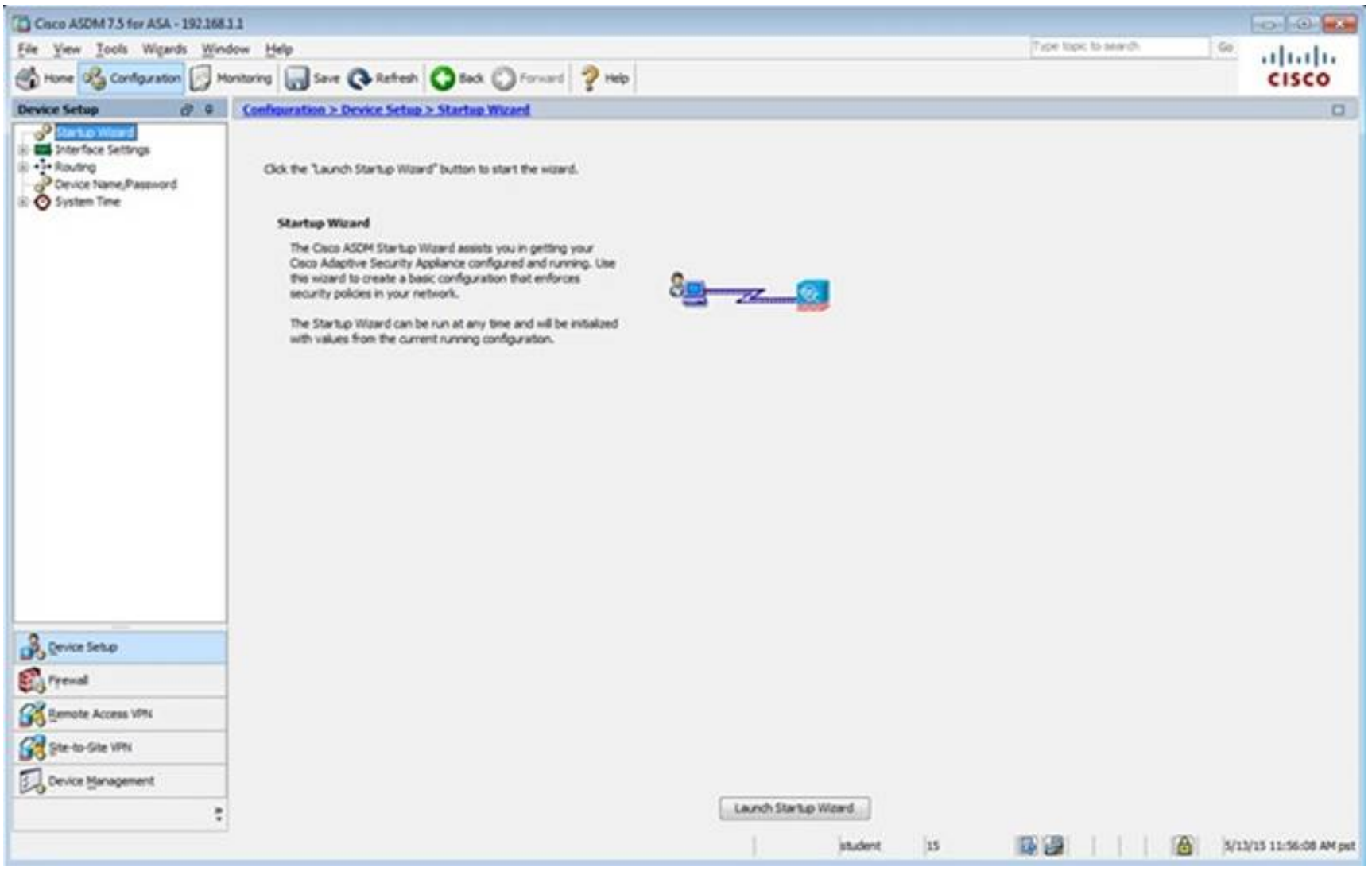
NEW QUESTION 18
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities 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.

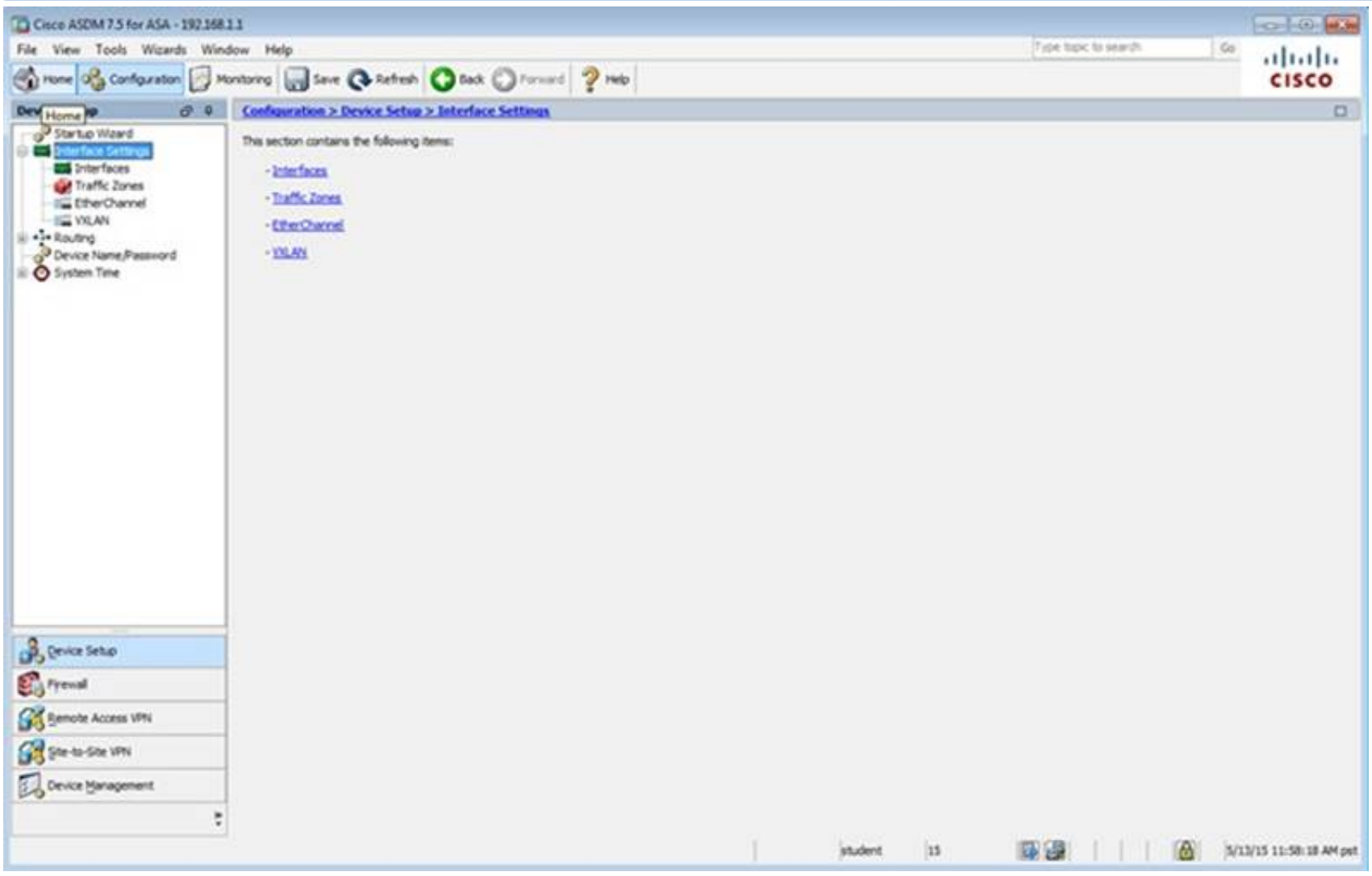

Lab Topology
Inside PC
.3
192.168.1.0/24
inside
Gi0/1
.1
Gi0/2
172.16.1.0/24
DMZ SRV
.1 dmz
.2
ASA-5512-X
outside
.2
Gi0/0
209.165.201.0/27
Fa0/0.1x
.1
2610XM
.129
209.165.202.128/27
.130
Outside SRV (Kali Linux)
Fa0/0.9x
.226
.131
Outside PC (Windows)
209.165.200.224/27
Gi0/0.9x
.225
Gi0/1
Internet

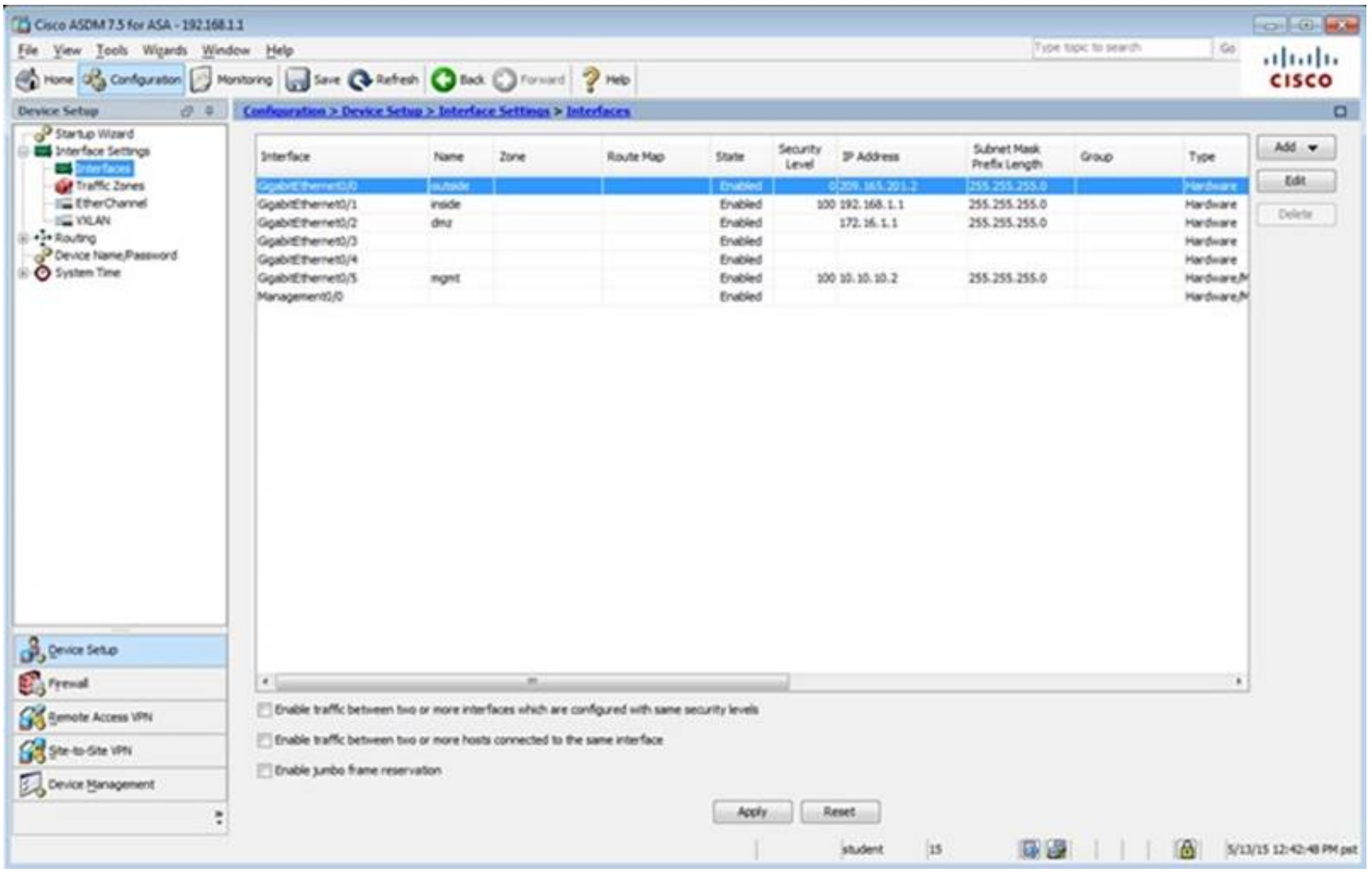

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License
Host Name: P17-ASA.secure-x.local
ASA Version: 100.14(6)13
ASDM Version: 7.5(1)1
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 11d 21h 42m 47s
Device Type: ASA 5512
Context Mode: Single
Total Flash: 4096 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
dmz 172.16.1.1/24 up up 0
inside 192.168.1.1/24 up up 4
mgmt 10.10.10.2/24 up up 0
outside 209.165.201.2/24 up up 0
Select an interface to view input and output Kbps
VPN Sessions
IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 Details
Failover Status
Failover not configured. Click the link to configure it. Configure
System Resources Status
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Latest ASDM Syslog Messages
Severity Date Time Syslog ID Source IP Source Destination IP Destina Description
6 May 13 2015 12:35:09 302016 10.81.254.202 123 209.165.201.2 65535 Teardown UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6 May 13 2015 12:35:08 106015 192.168.1.3 14676 192.168.1.1 443 Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6 May 13 2015 12:35:08 302014 192.168.1.3 14676 192.168.1.1 443 Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O
student 15
5/13/15 12:35:18 PM pst

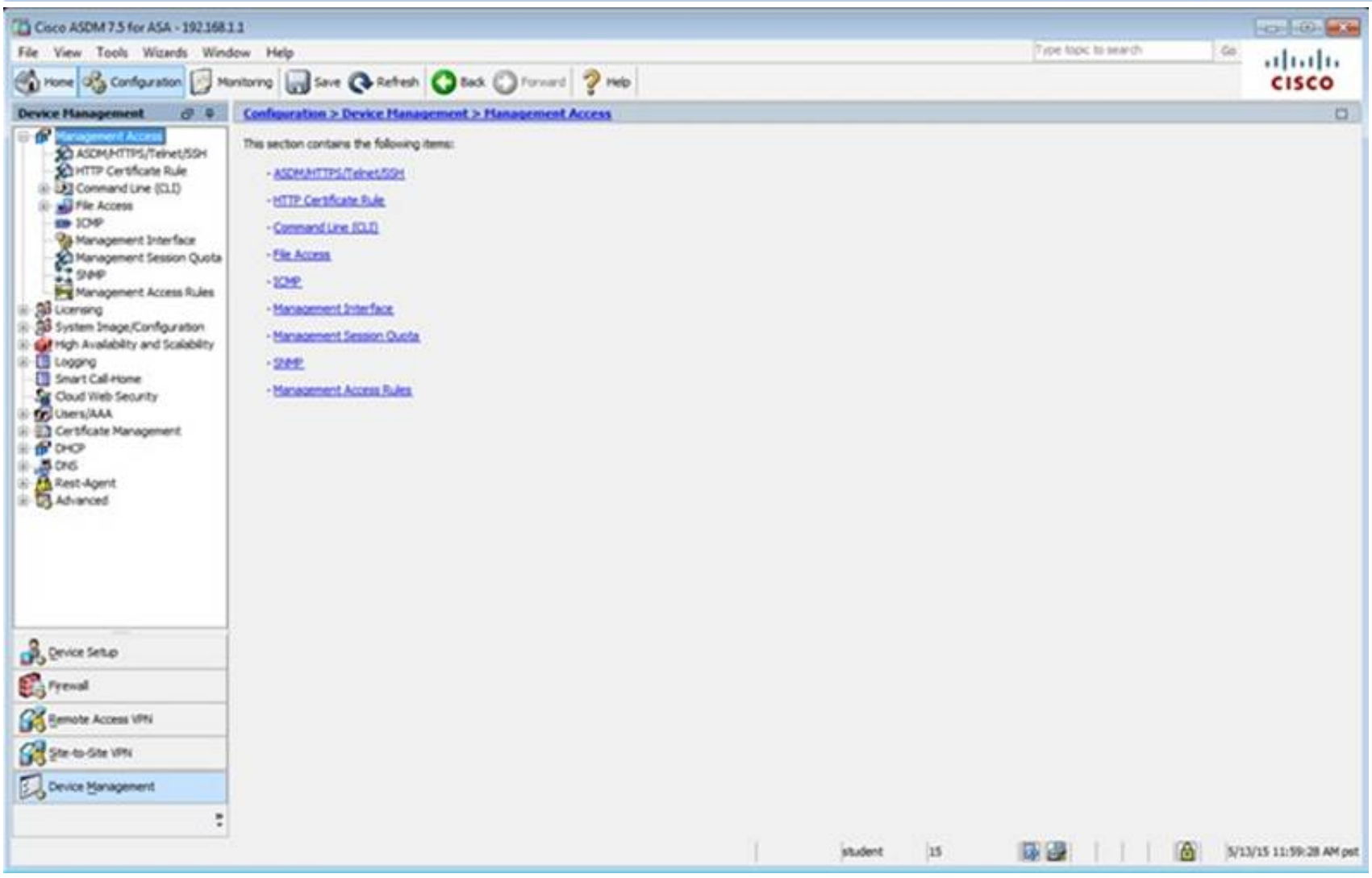

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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
Clear Dynamic ARP Entries
Refresh
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Last Updated: 5/19/15 9:32:02 AM
Data Refreshed Successfully.
student
15
5/19/15 8:32:27 AM pst

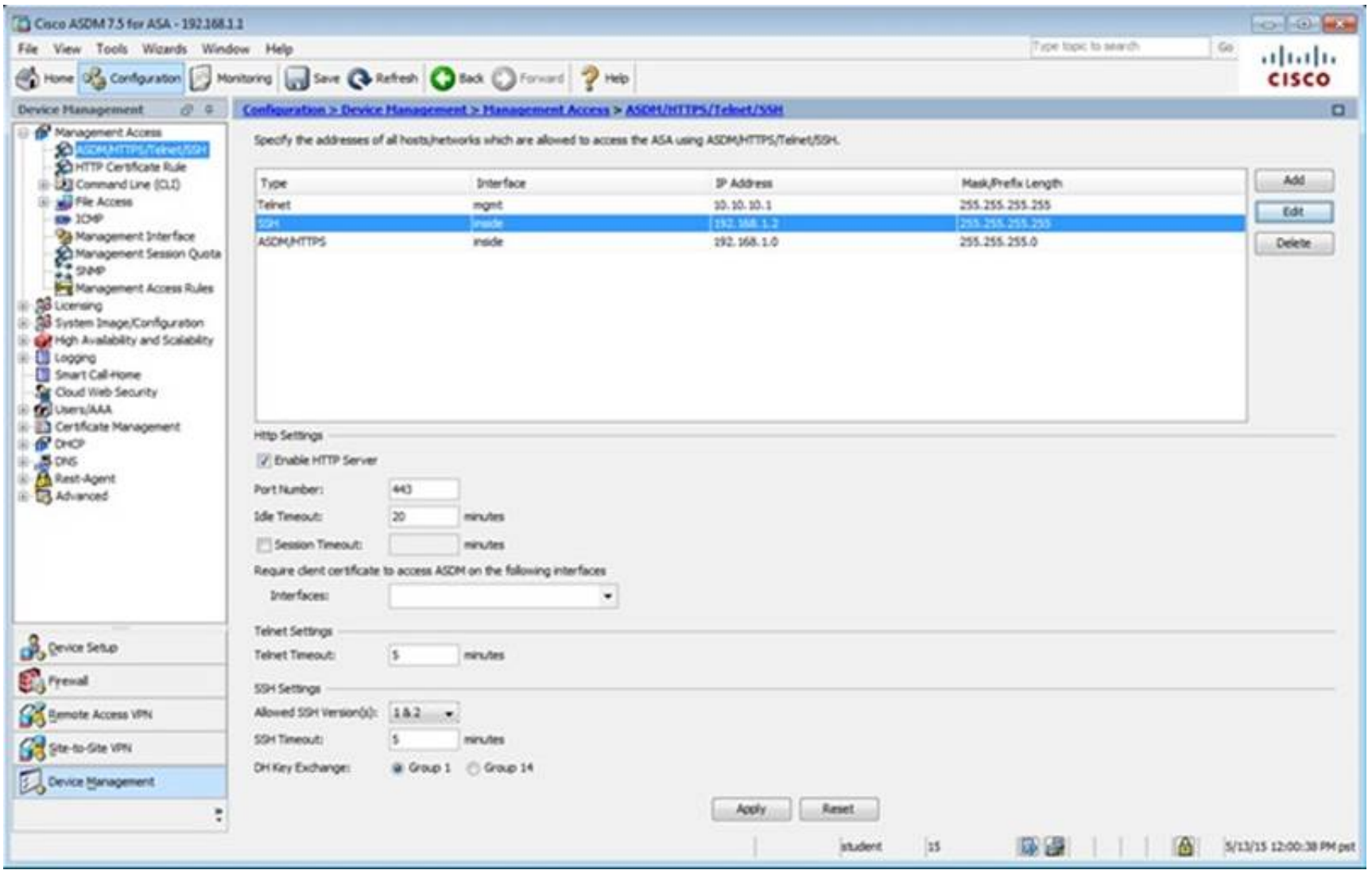

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN Mapping Sessions
MDM Proxy Statistics
MDM Proxy Sessions
Clientless SSL VPN
VPN Connection Graphs
WSA Sessions
Monitoring > VPN > VPN Statistics > Sessions
Type | Active | Cumulative | Peak Concurrent | Inactive
Clientless VPN | 1 | 1 | 1 | 1
Browser | 1 | 1 | 1 | 1
Filter By: Clientless SSL VPN -- All Sessions -- Filter
Username
IP Address
Group Policy
Connection Profile
Protocol
Encryption
Login Time
Duration
Bytes Tx
Bytes Rx
student
209.165.202.131
Sales
clientless
Clientless
Clientless: (1)RC4
08:05:46 pst Thu May 21 2015
0h:09m:19s
318774
41633
Details
Logout
Ping
Refresh
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Last Updated: 5/19/15 9:33:12 AM
Data Refreshed Successfully.
student
15
5/19/15 8:33:37 AM pst

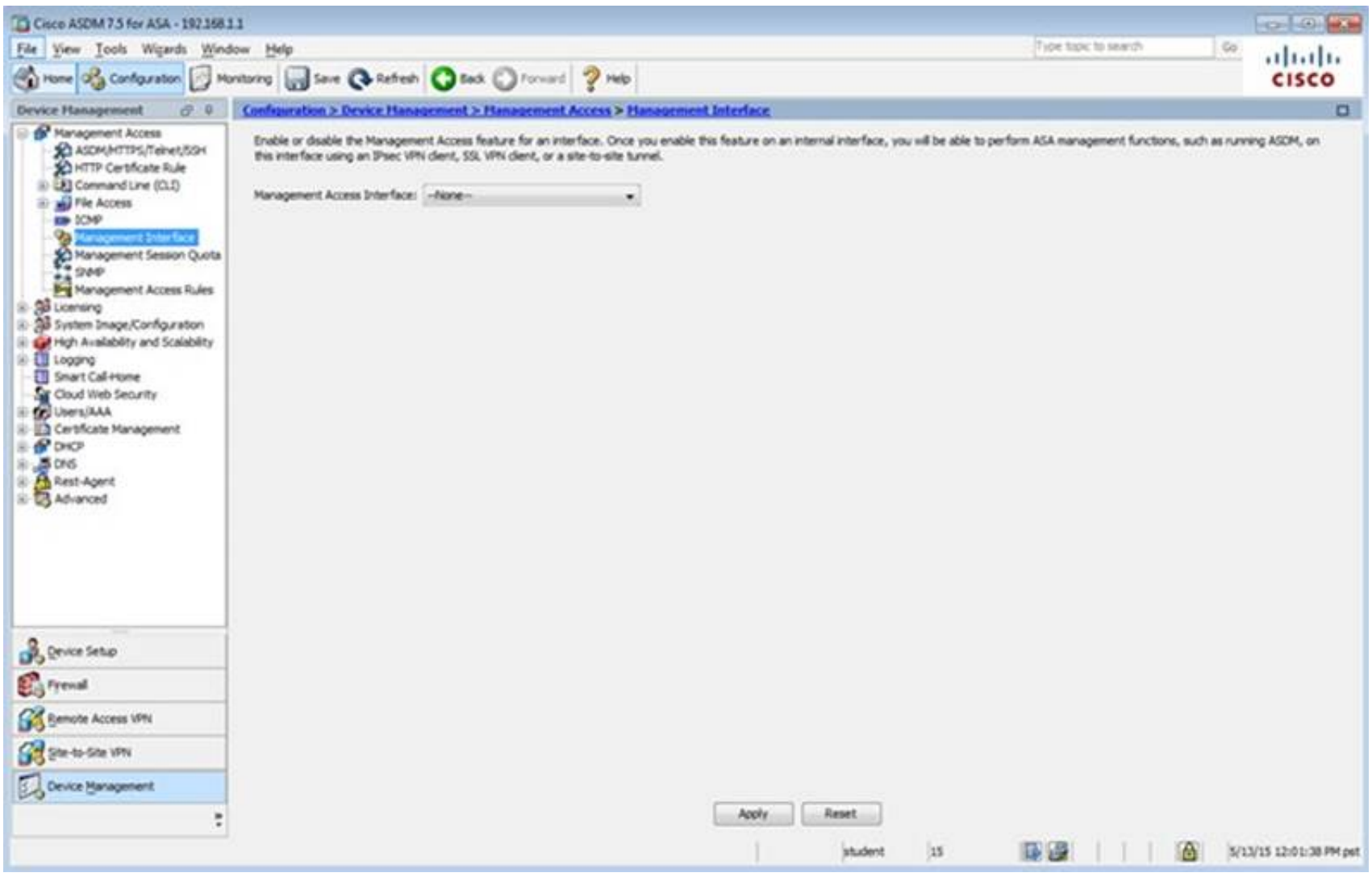

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" button to start the wizard.
Startup Wizard
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.
Launch Startup Wizard
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 11:56:08 AM pst

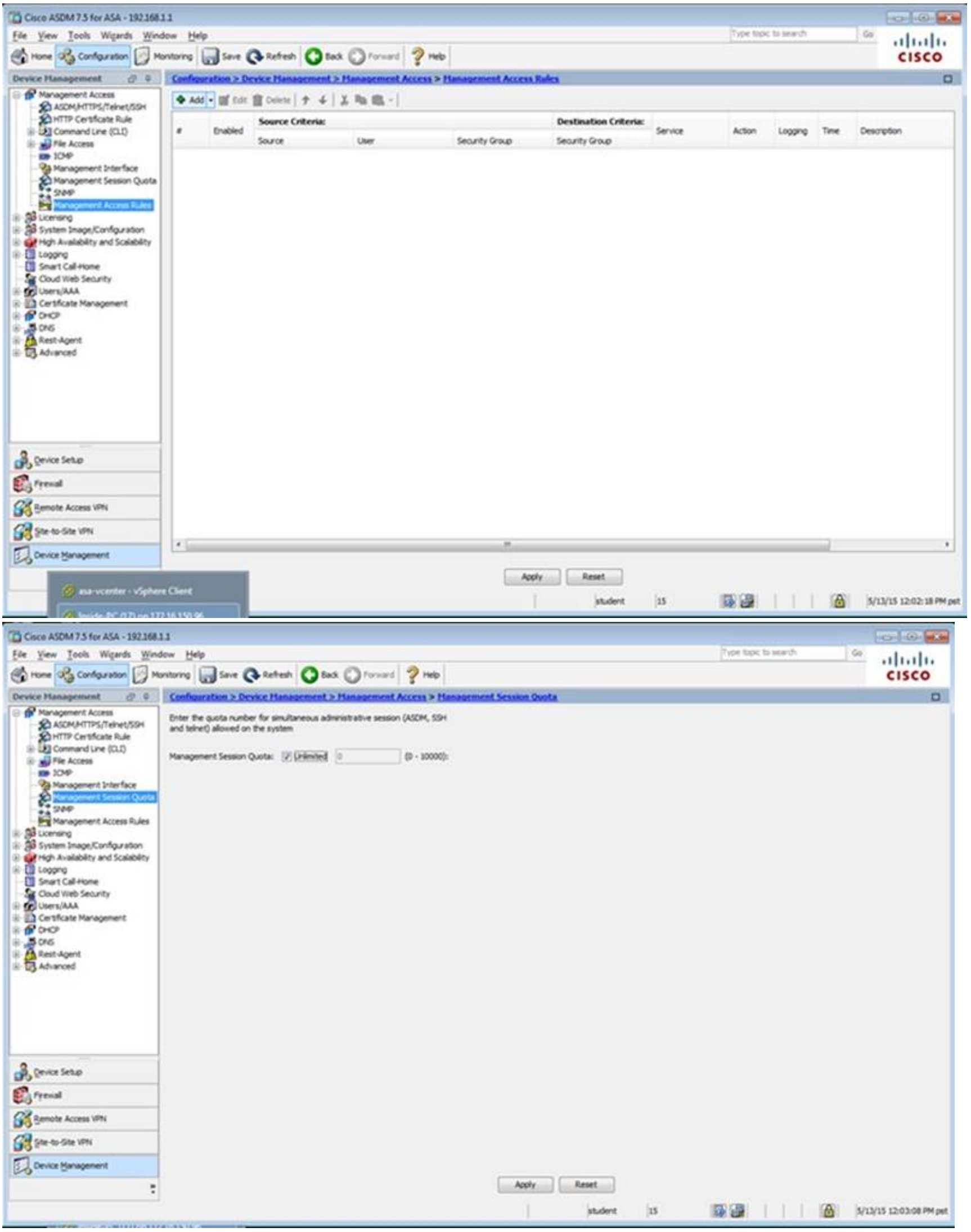

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interface Settings
This section contains the following items:
- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 11:58:18 AM pst

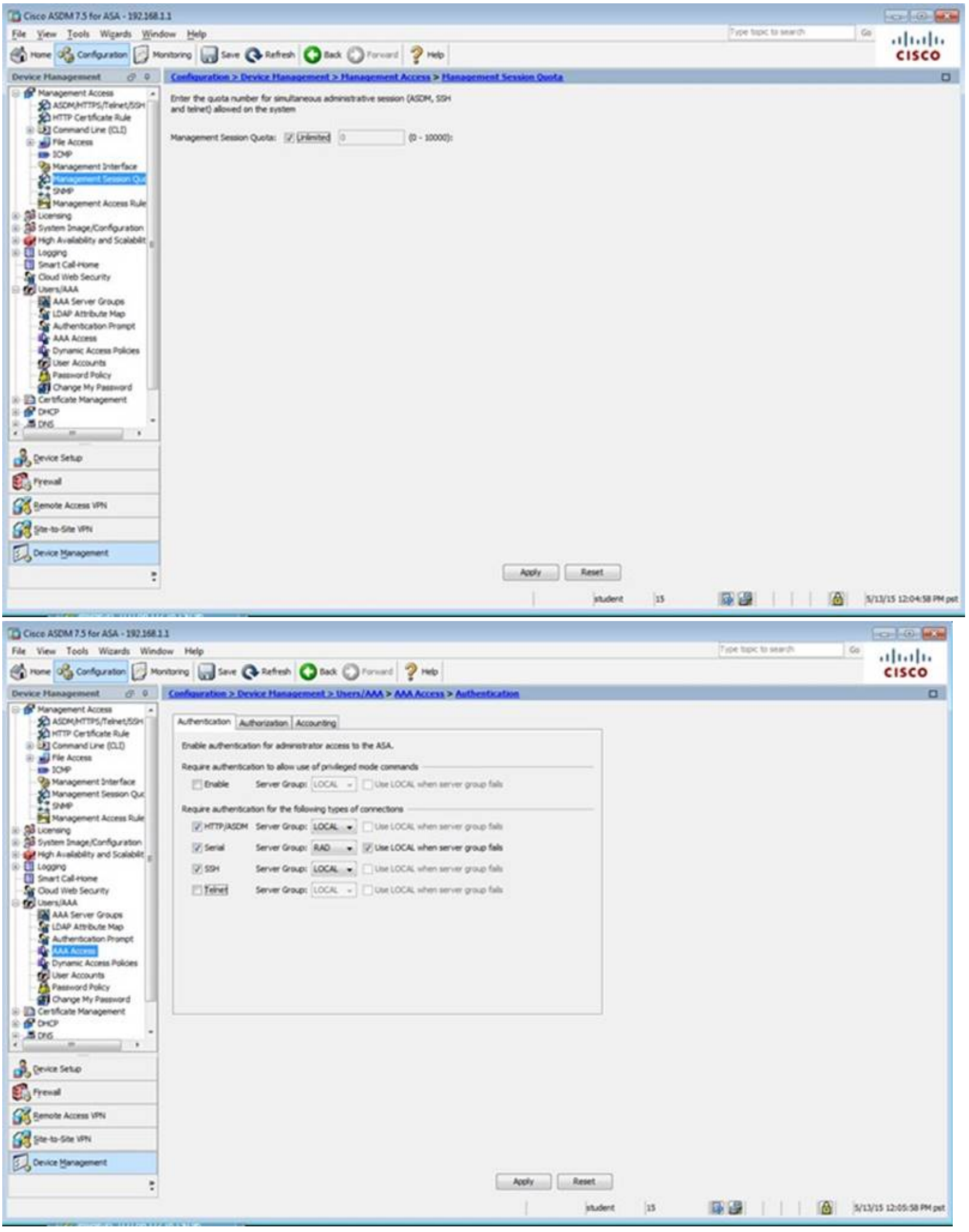

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interface Settings > Interfaces
Interface Name Zone Route Map State Security Level IP Address Subnet Mask Prefix Length Group Type
GigabitEthernet0/0 outside Enabled 0 209.165.201.2 255.255.255.0 Hardware
GigabitEthernet0/1 inside Enabled 100 192.168.1.1 255.255.255.0 Hardware
GigabitEthernet0/2 dmz Enabled 172.16.1.1 255.255.255.0 Hardware
GigabitEthernet0/3 Enabled Hardware
GigabitEthernet0/4 Enabled Hardware
GigabitEthernet0/5 mgmt Enabled 100 10.10.10.2 255.255.255.0 Hardware
Management0/0 Enabled Hardware
Add
Edit
Delete
Enable traffic between two or more interfaces which are configured with same security levels
Enable traffic between two or more hosts connected to the same interface
Enable jumbo frame reservation
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 12:42:48 PM pst

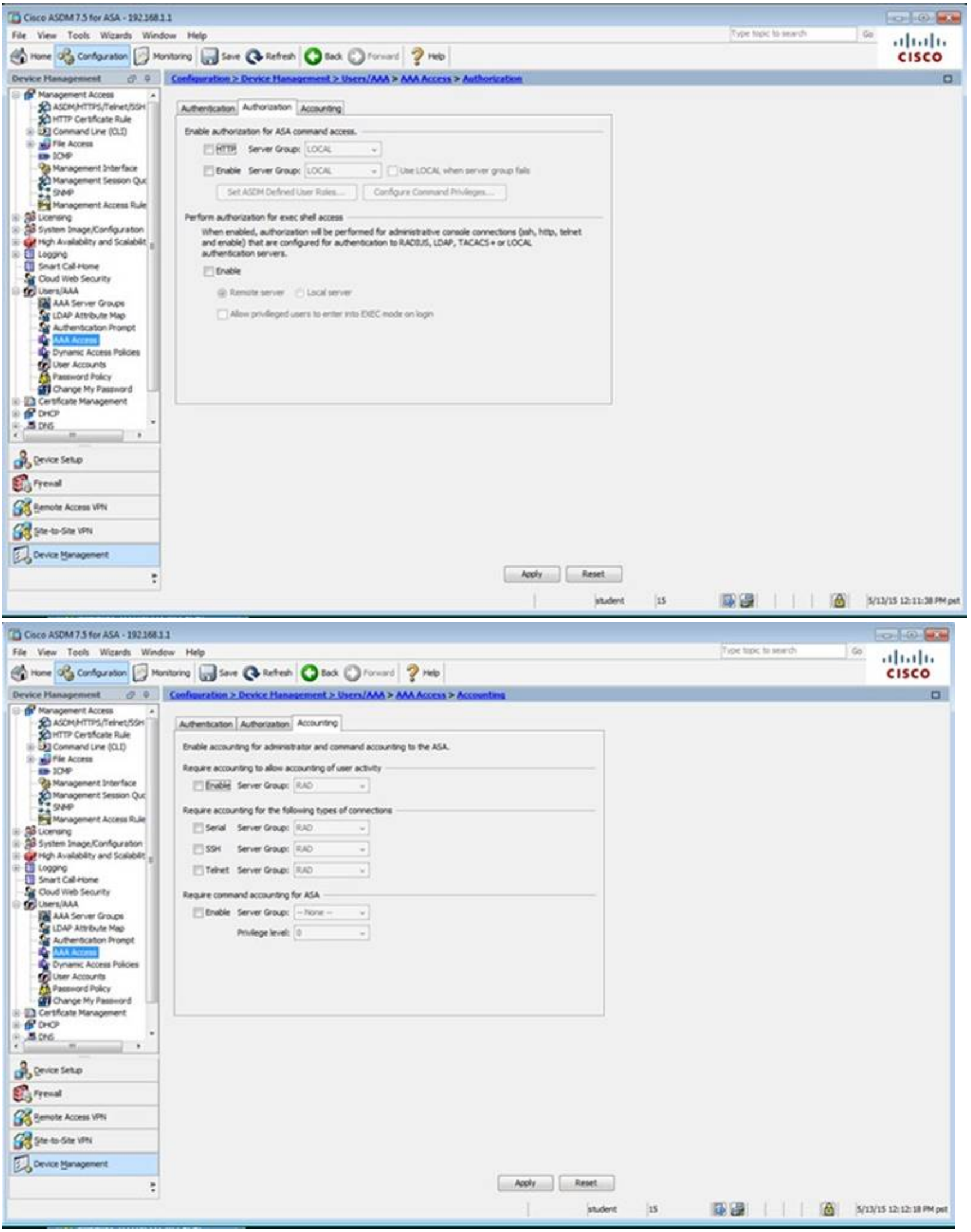

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quota
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
Configuration > Device Management > Management Access
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Quota
- SNMP
- Management Access Rules
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 11:59:28 AM 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
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.
Type Interface IP Address Mask/Prefix Length
Telnet mgmt 10.10.10.1 255.255.255.255
SSH inside 192.168.1.2 255.255.255.255
ASDM/HTTPS inside 192.168.1.0 255.255.255.0
Add Edit Delete
Http Settings
Enable HTTP Server
Port Number: 443
Idle Timeout: 20 minutes
Session Timeout: minutes
Require client certificate to access ASDM on the following interfaces
Interfaces:
Telnet Settings
Telnet Timeout: 5 minutes
SSH Settings
Allowed SSH Version(s): 1 & 2
SSH Timeout: 5 minutes
DH Key Exchange: Group 1 Group 14
Apply Reset
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
student 15
5/13/15 12:00:38 PM pst

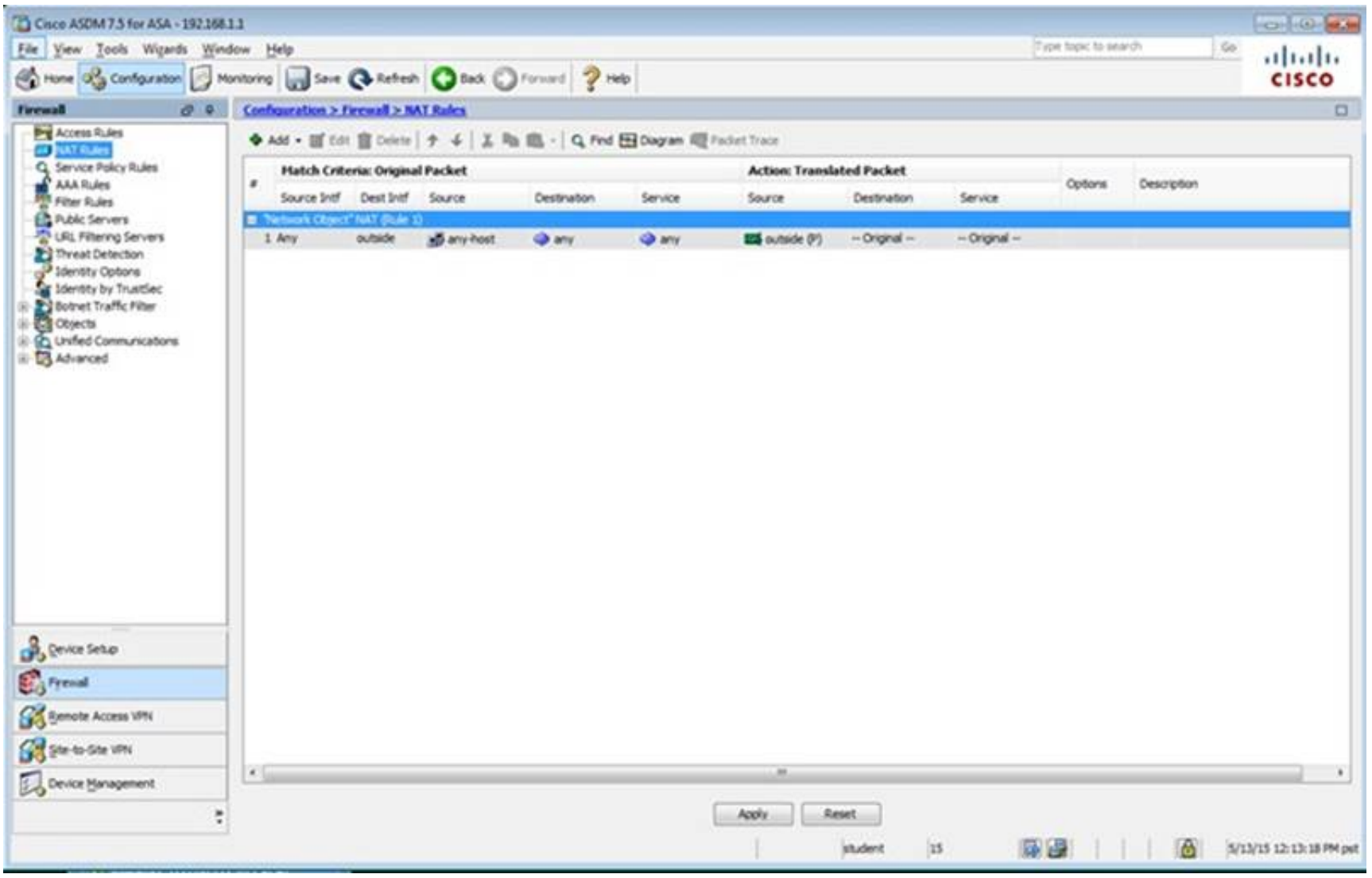

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Enable or disable the Management Access feature for an interface. Once you enable this feature on an internal interface, you will be able to perform ASA management functions, such as running ASDM, on this interface using an IPsec VPN client, SSL VPN client, or a site-to-site tunnel.
Management Access Interface: --None--
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
student 15
5/13/15 12:01:38 PM pst

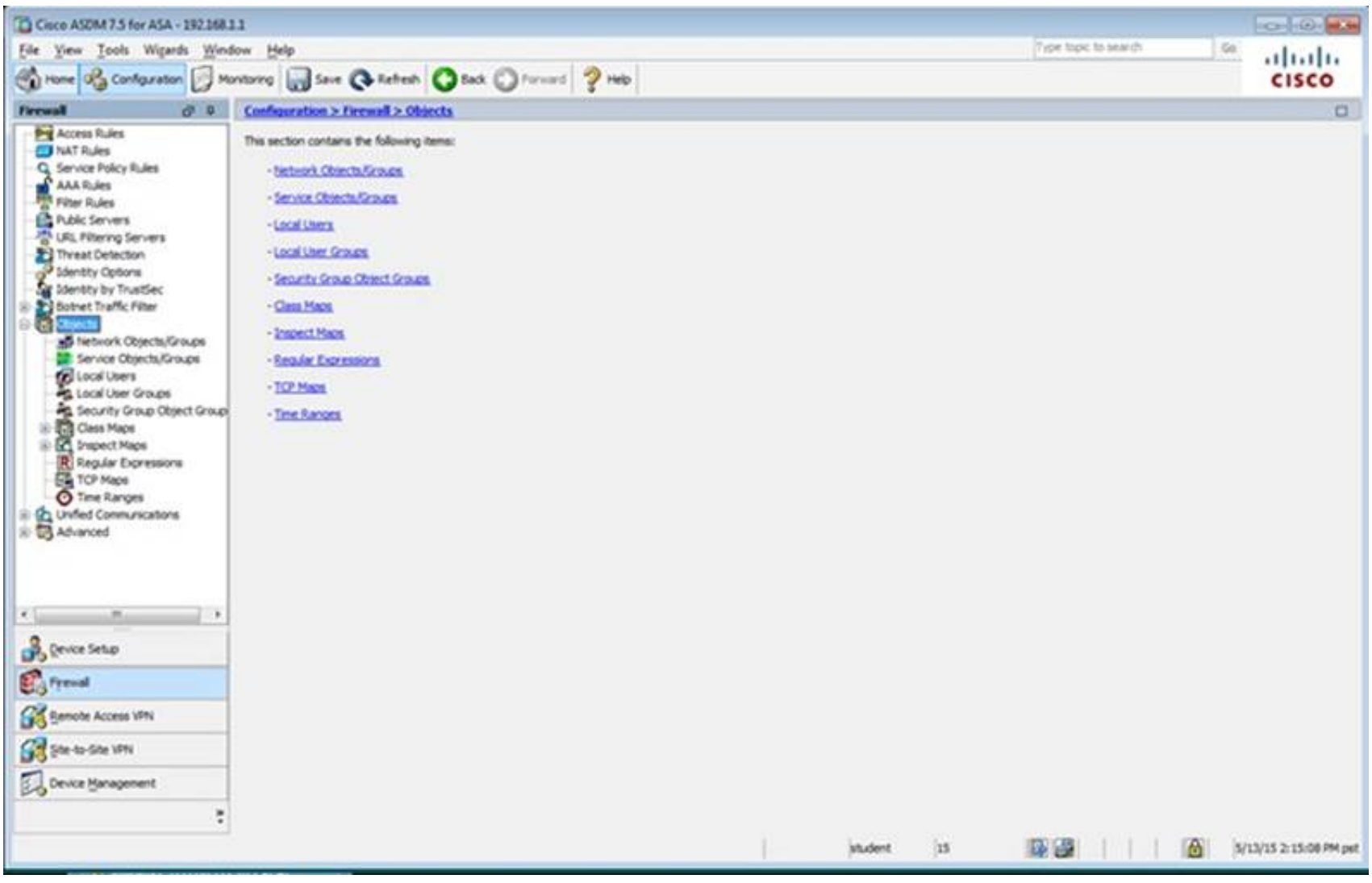

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Access Rules
Add Edit Delete
Enabled Source Criteria: Source User Security Group 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 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
CISCO
Device Management
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):
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
student 15
5/13/15 12:03:08 PM pst

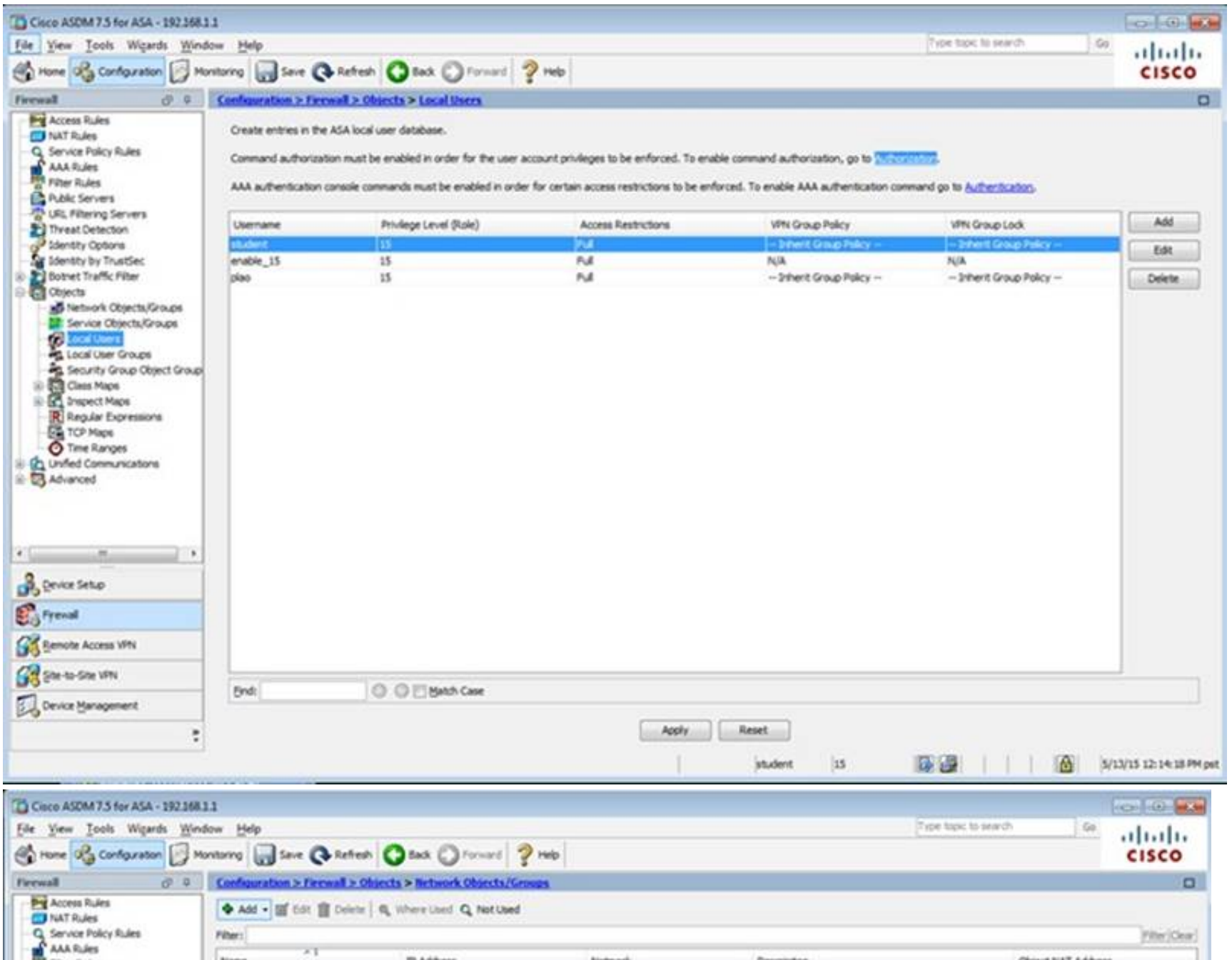

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quota
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system
Management Session Quota: Unlimited 0 (0 - 10000):
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:04:58 PM pst
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
5/13/15 12:05:58 PM pst

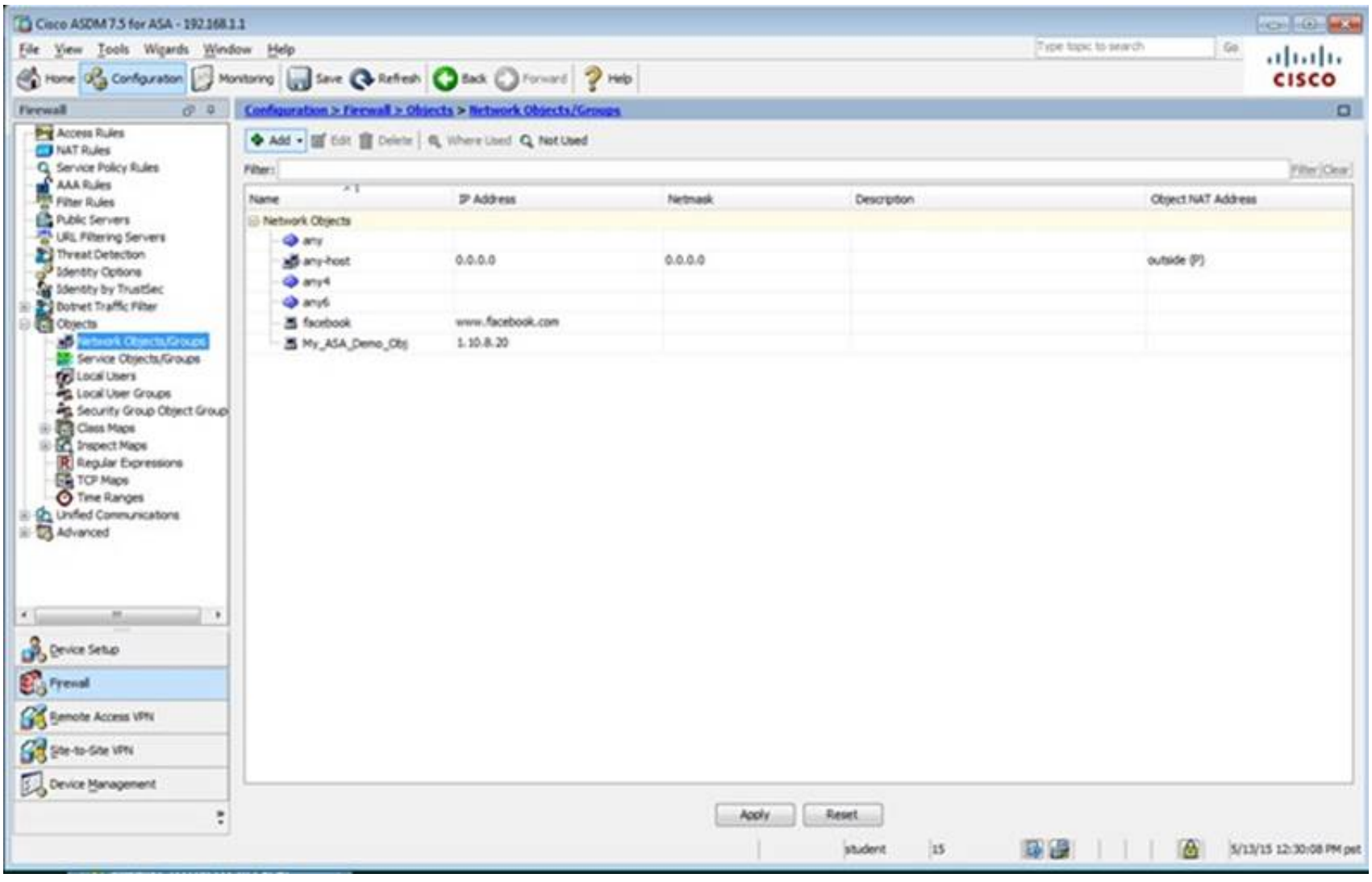

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Enable authorization for ASA 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quc
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:11:38 PM pst

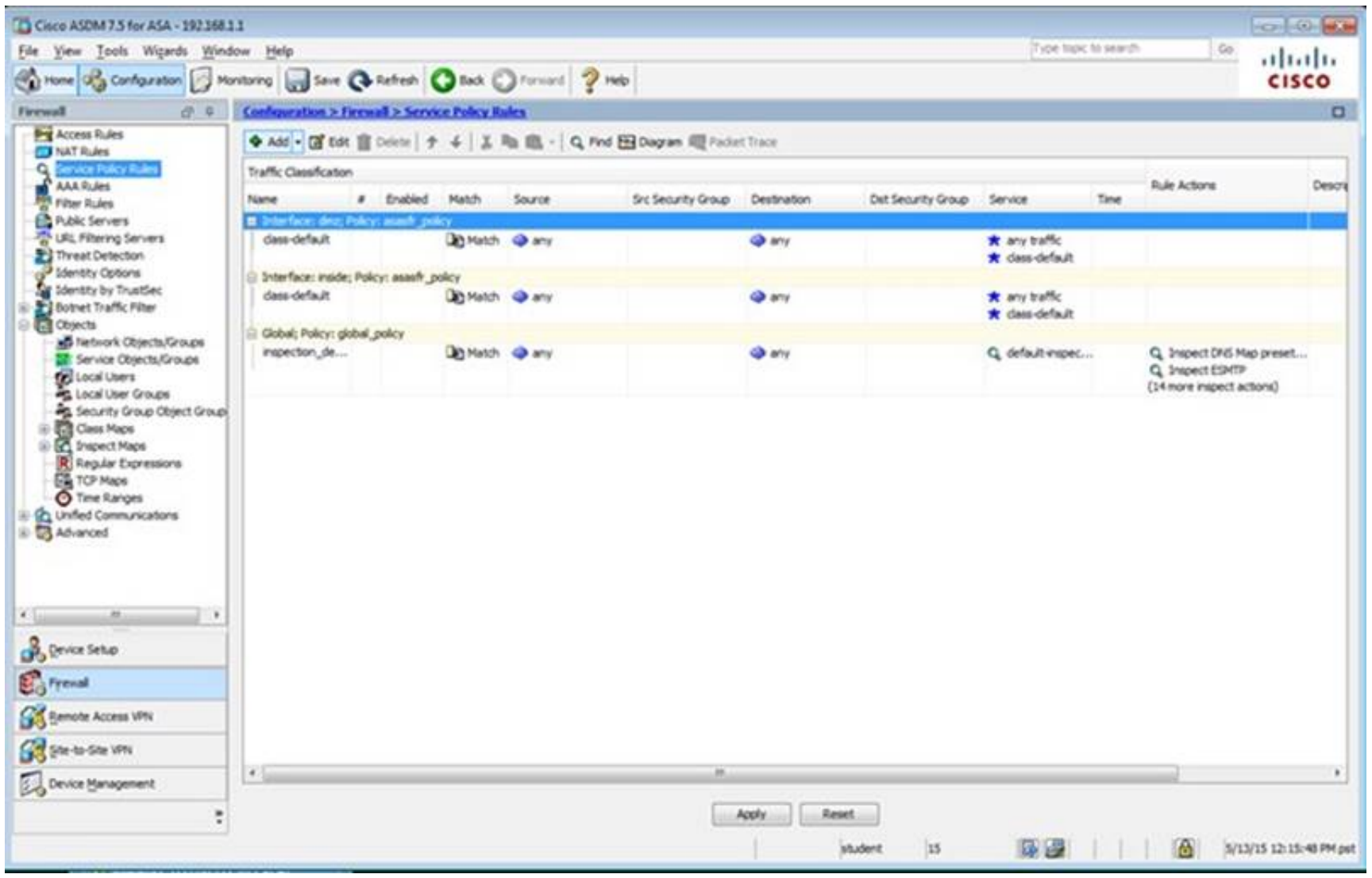
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Authentication Authorization Accounting
Enable accounting for administrator 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Quc
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:12:18 PM pst

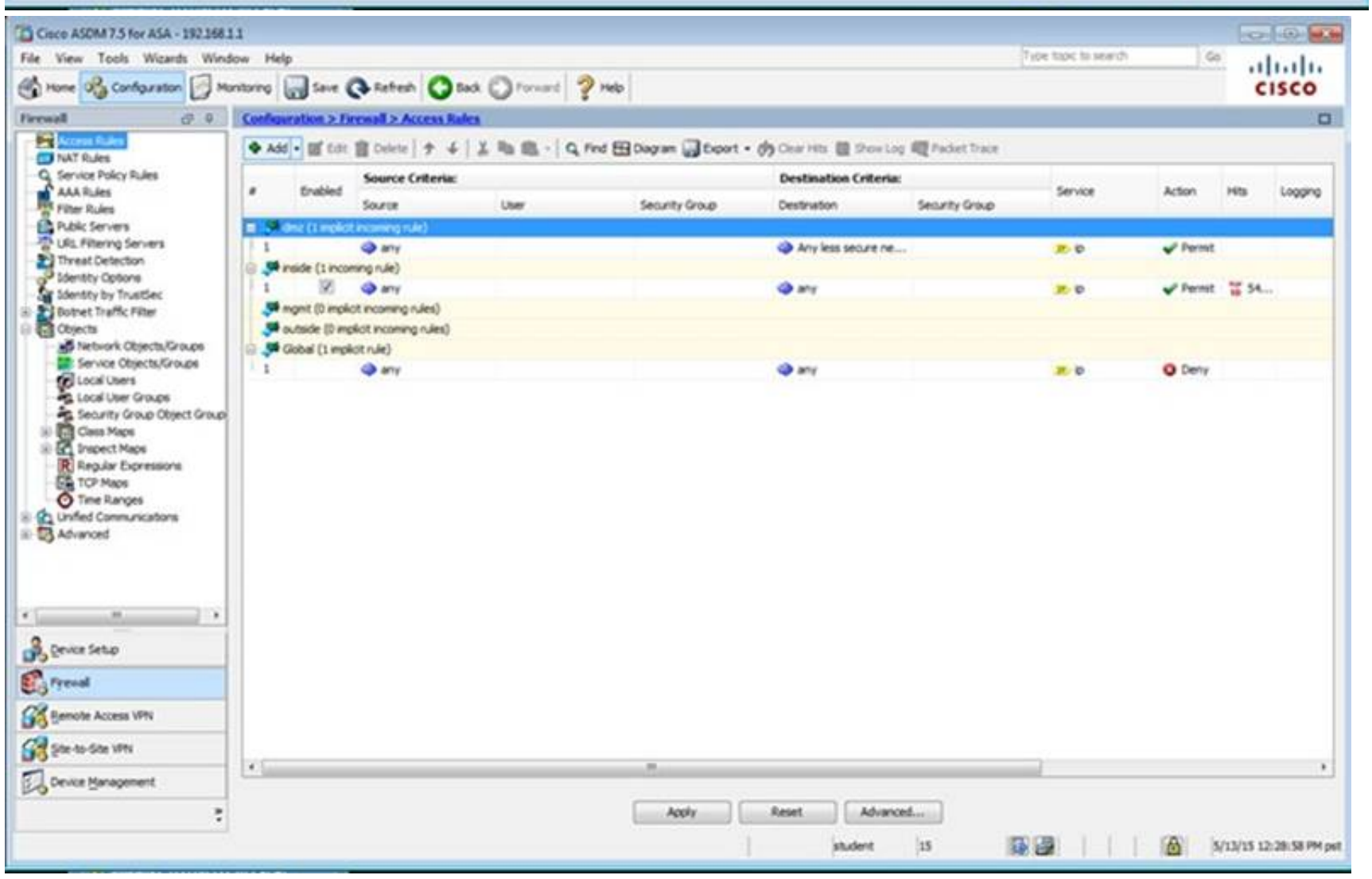

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Add Edit Delete Find Diagram Packet Trace
Match Criteria: Original Packet
Action: Translated Packet
Source Intf
Dest Intf
Source
Destination
Service
Options
Description
"Network Object" NAT (Rule 1)
1 Any outside any-host any any outside (P) -- Original -- -- Original --
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:13:18 PM pst

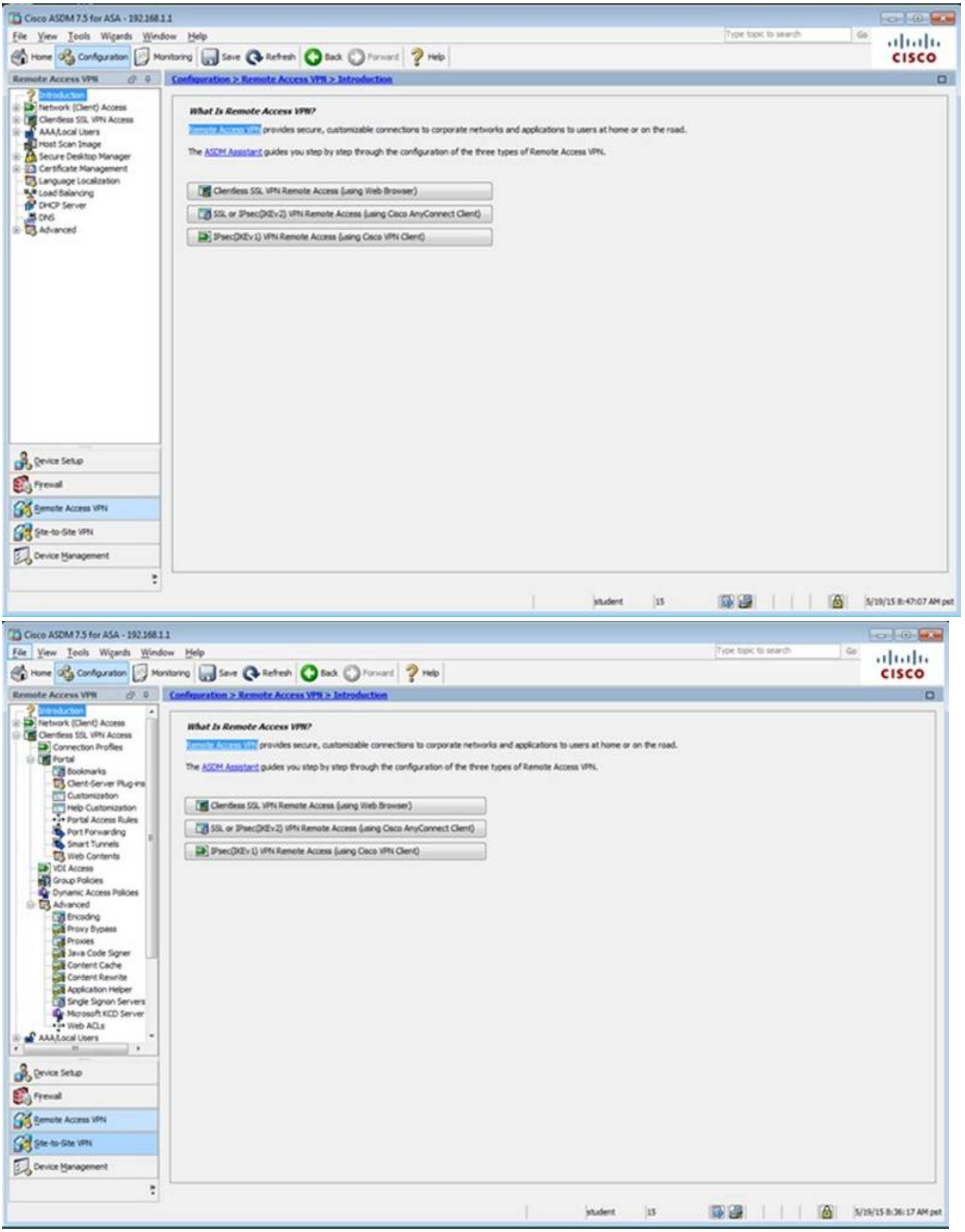

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects
This section contains the following items:
- Network Objects/Groups
- Service Objects/Groups
- Local Users
- Local User Groups
- Security Group Object Groups
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 2:15:08 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
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.
Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock
student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy --
enable_15 | 15 | Full | N/A | N/A
piao | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy --
Add
Edit
Delete
Find:
Match Case
Apply
Reset
student
15
5/13/15 12:14:18 PM pst

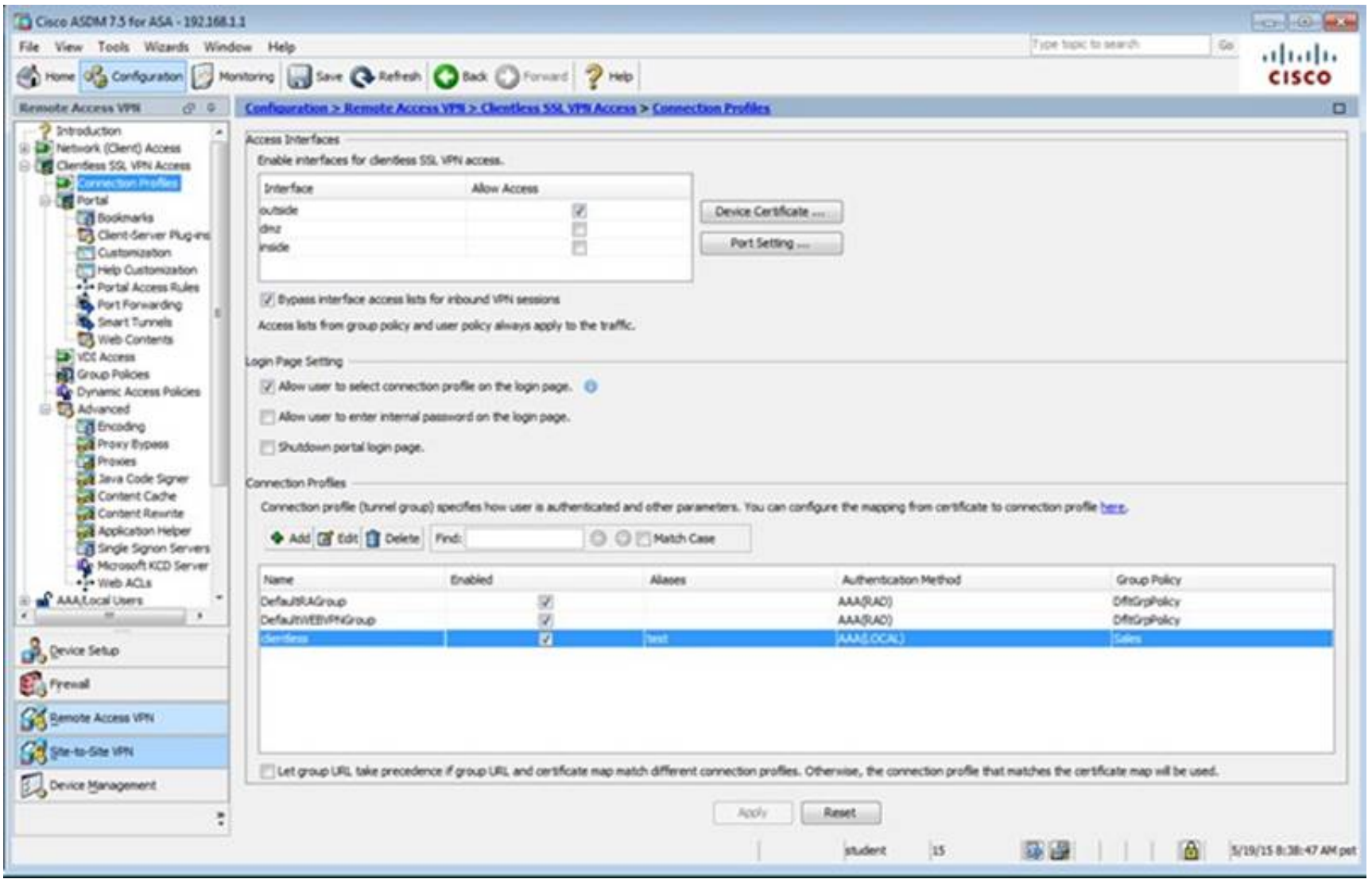

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Filter:
Name | IP Address | Netmask | Description | Object 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
Apply
Reset
student
15
5/13/15 12:30:08 PM pst

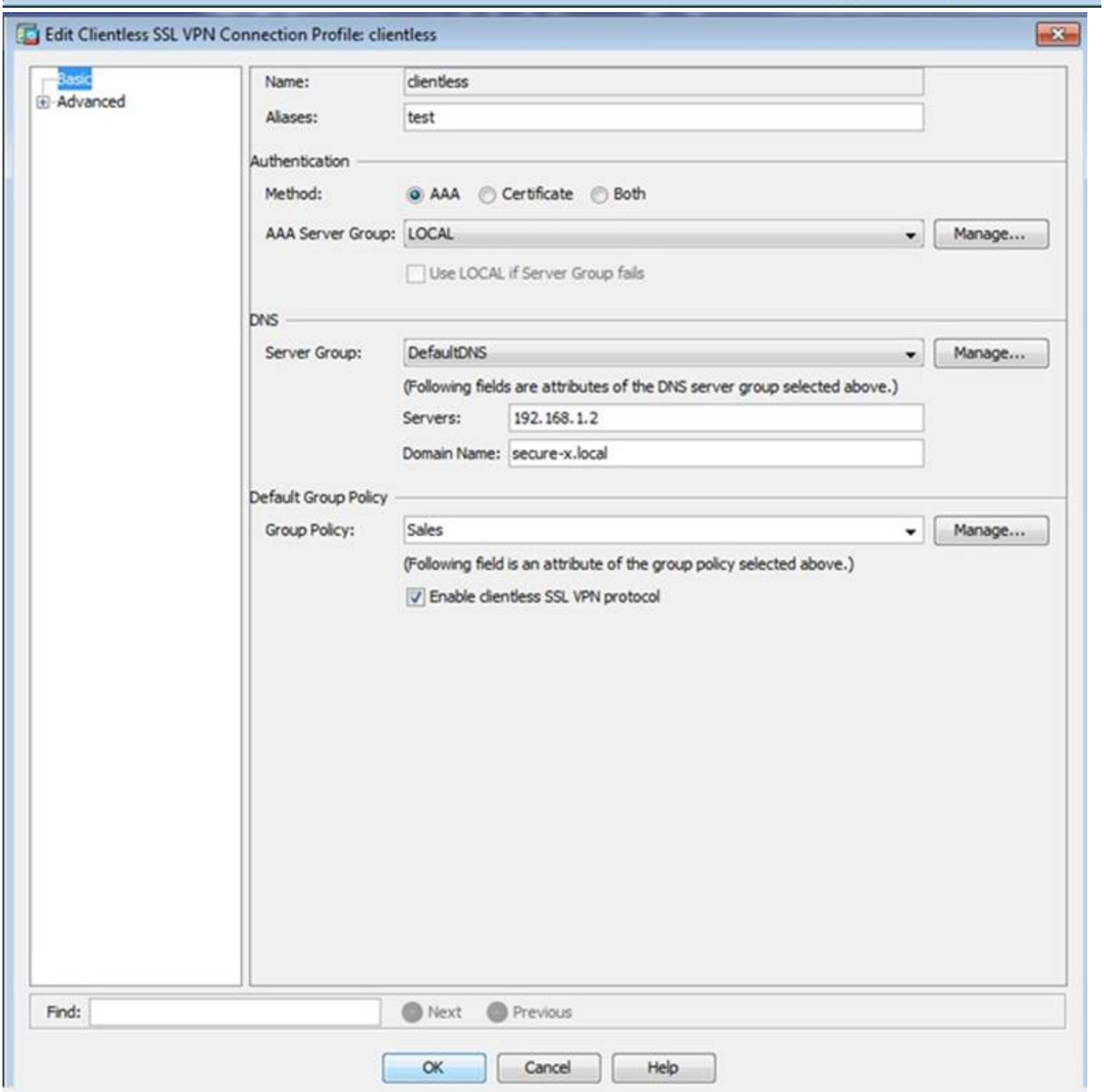

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst Security Group Service Time Rule Actions
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)
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:15:48 PM pst

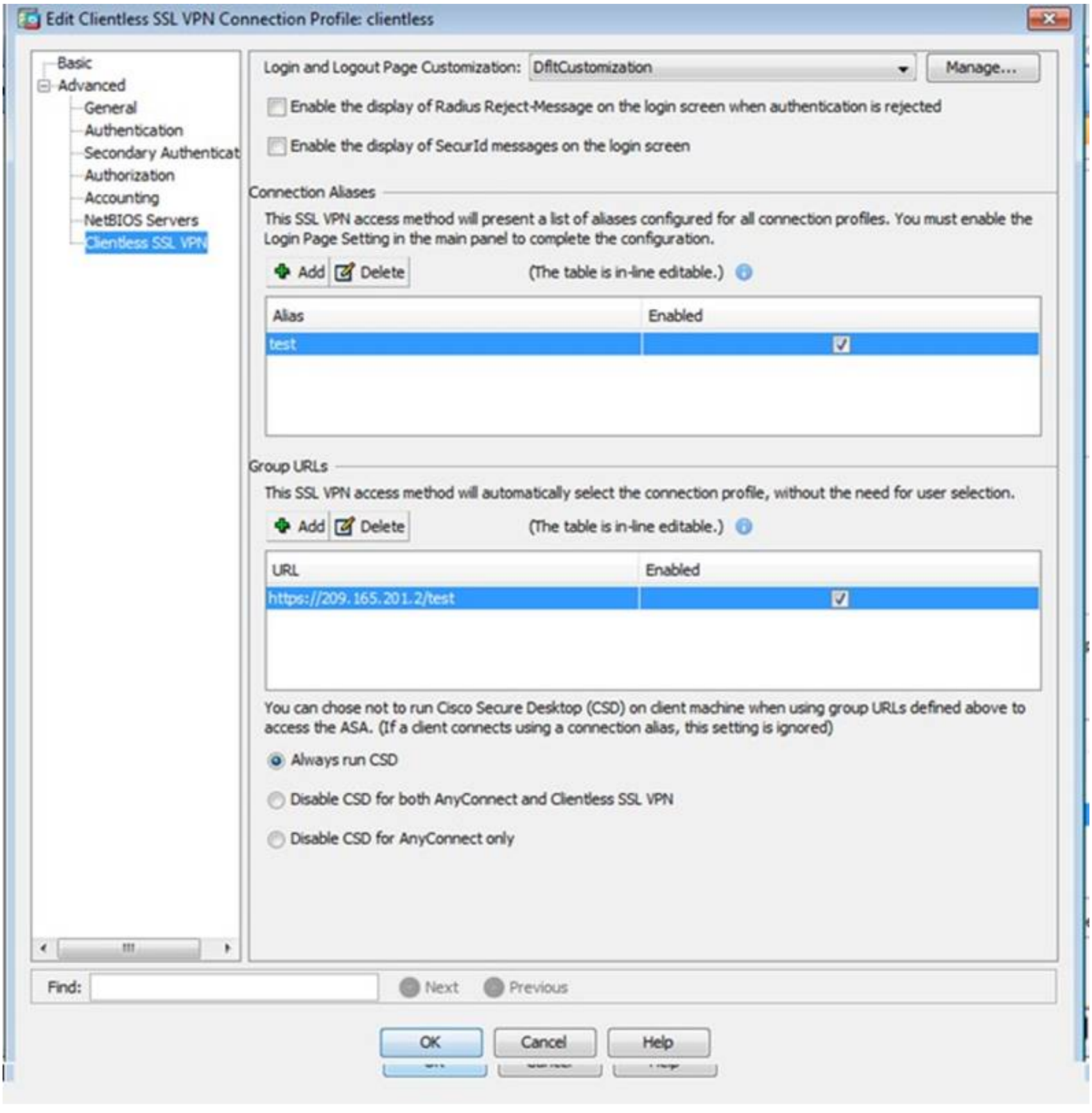

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Enabled Source Criteria: Source User Security Group Destination Criteria: Destination Security Group Service Action Hits Logging
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset Advanced...
student 15
5/13/15 12:28:58 PM pst

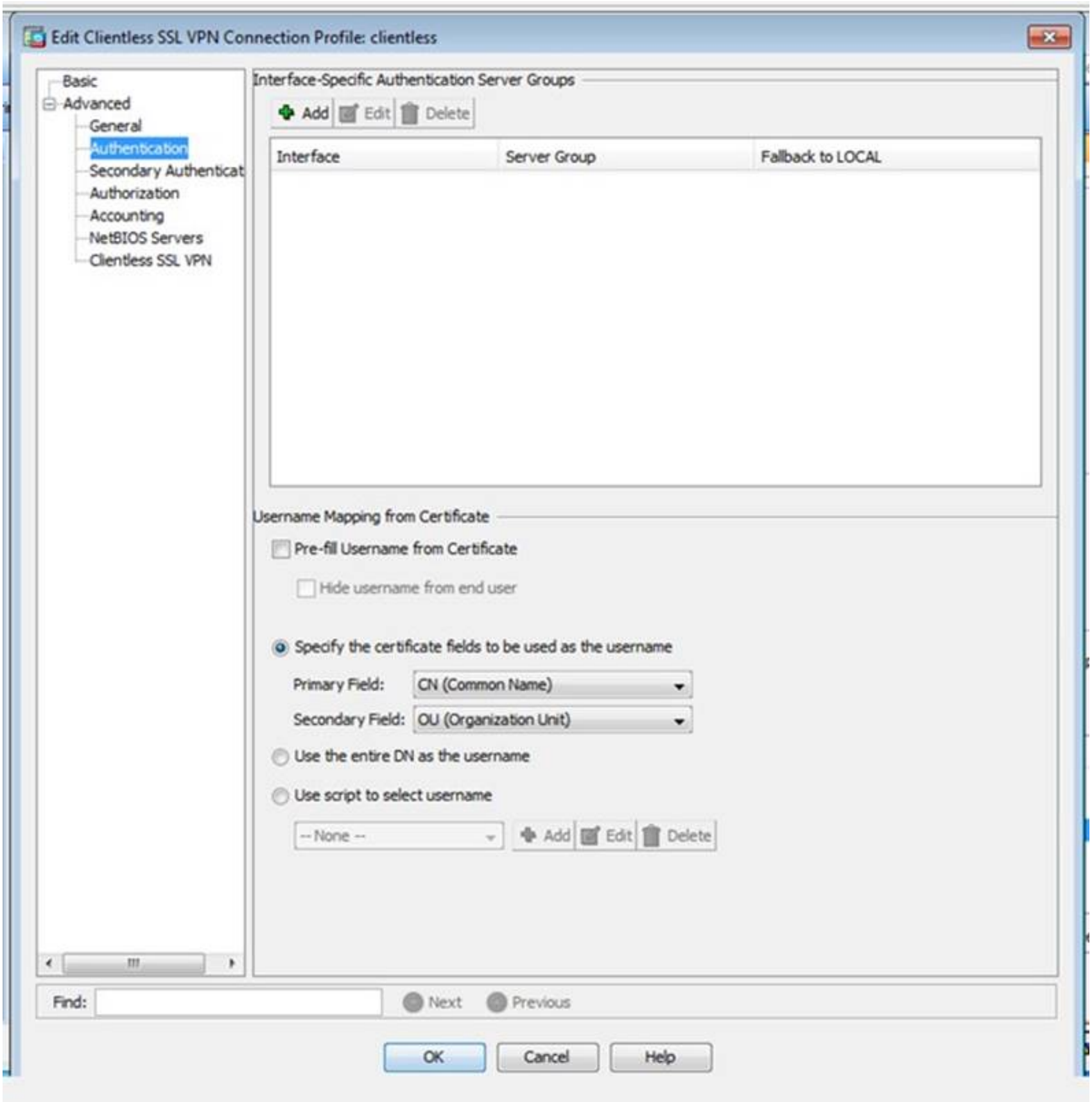

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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)
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:47:07 AM pst

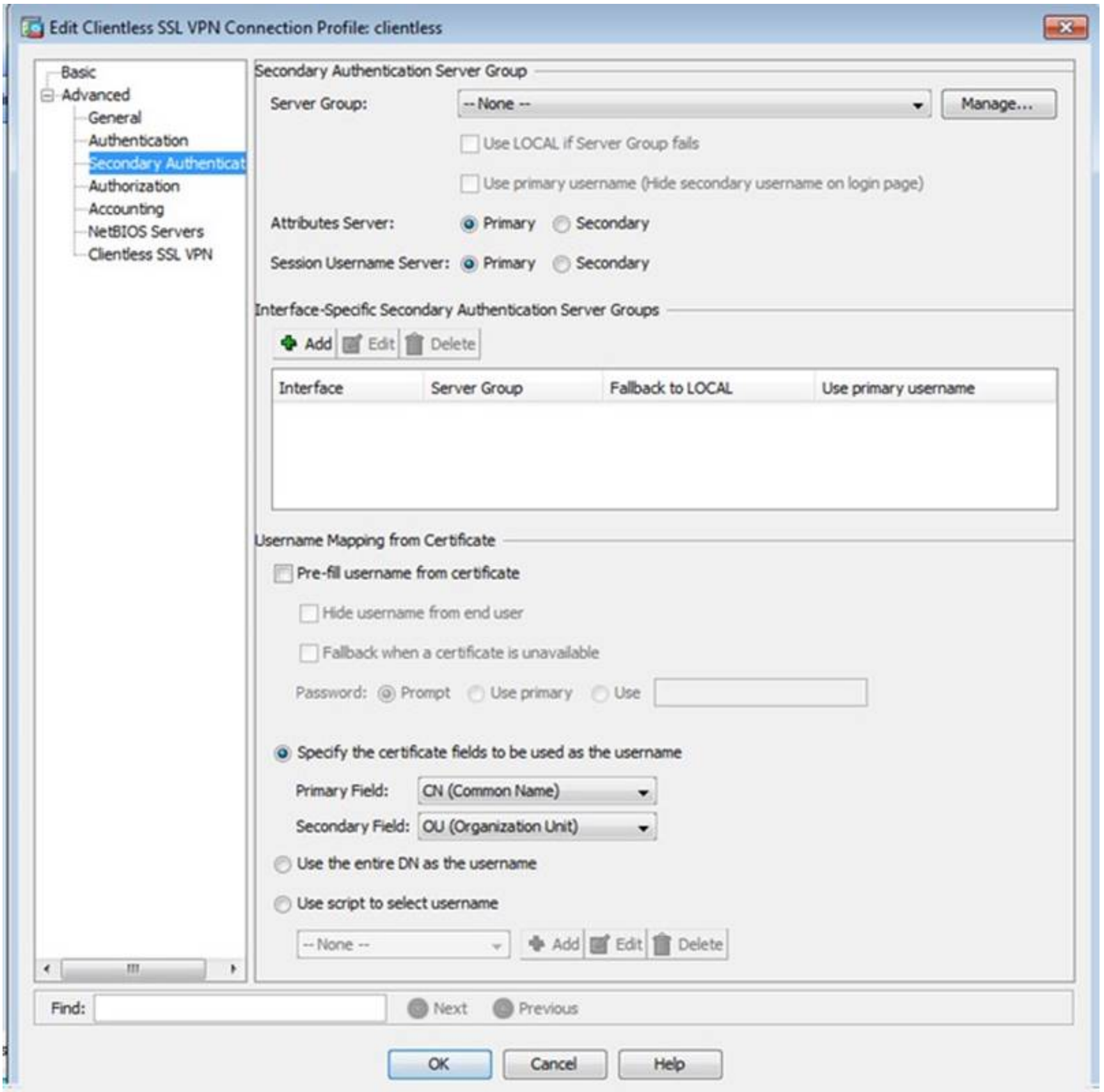
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
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)
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:36:17 AM pst

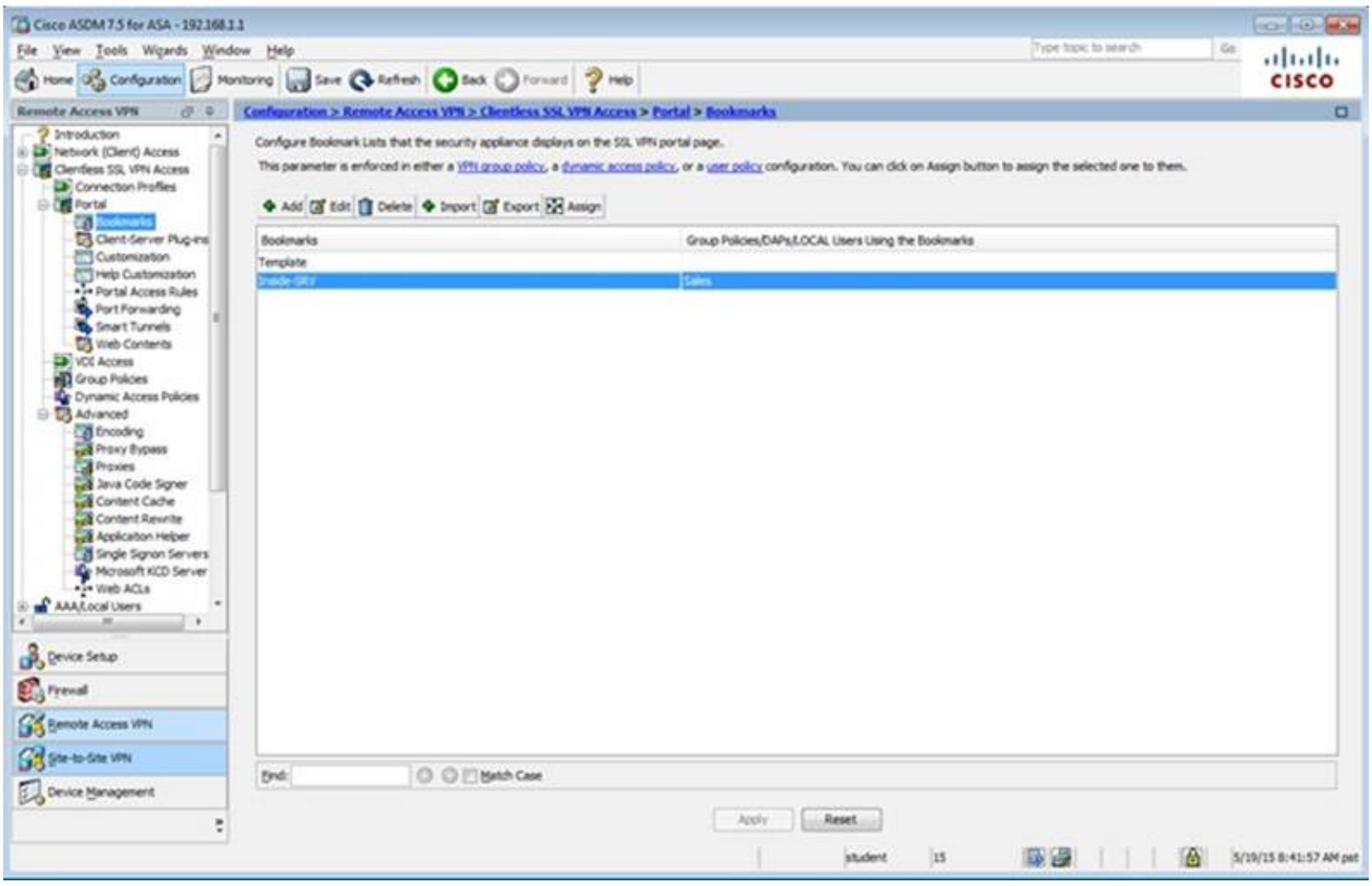

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
student
15
3/19/15 8:38:47 AM pst

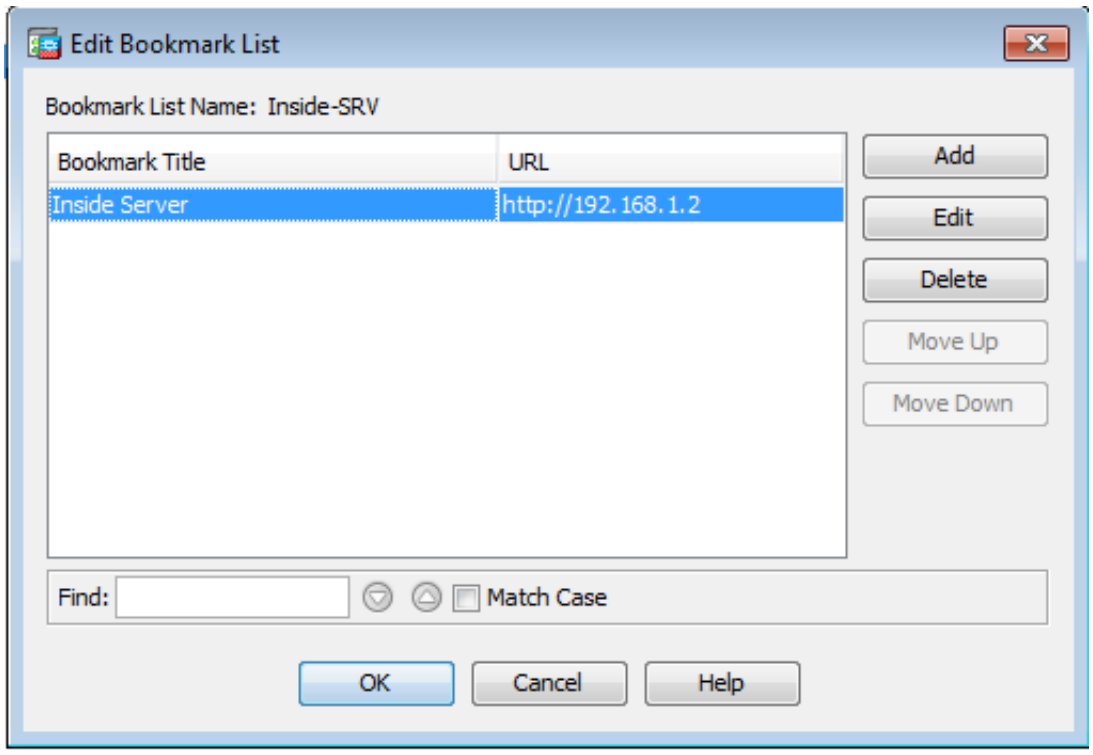

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server group selected above.)
Servers: 192.168.1.2
Domain Name: secure-x.local
Default Group Policy
Group Policy: Sales
Manage...
(Following field is an attribute of the group policy selected above.)
Enable clientless SSL VPN protocol
Find:
Next
Previous
OK
Cancel
Help

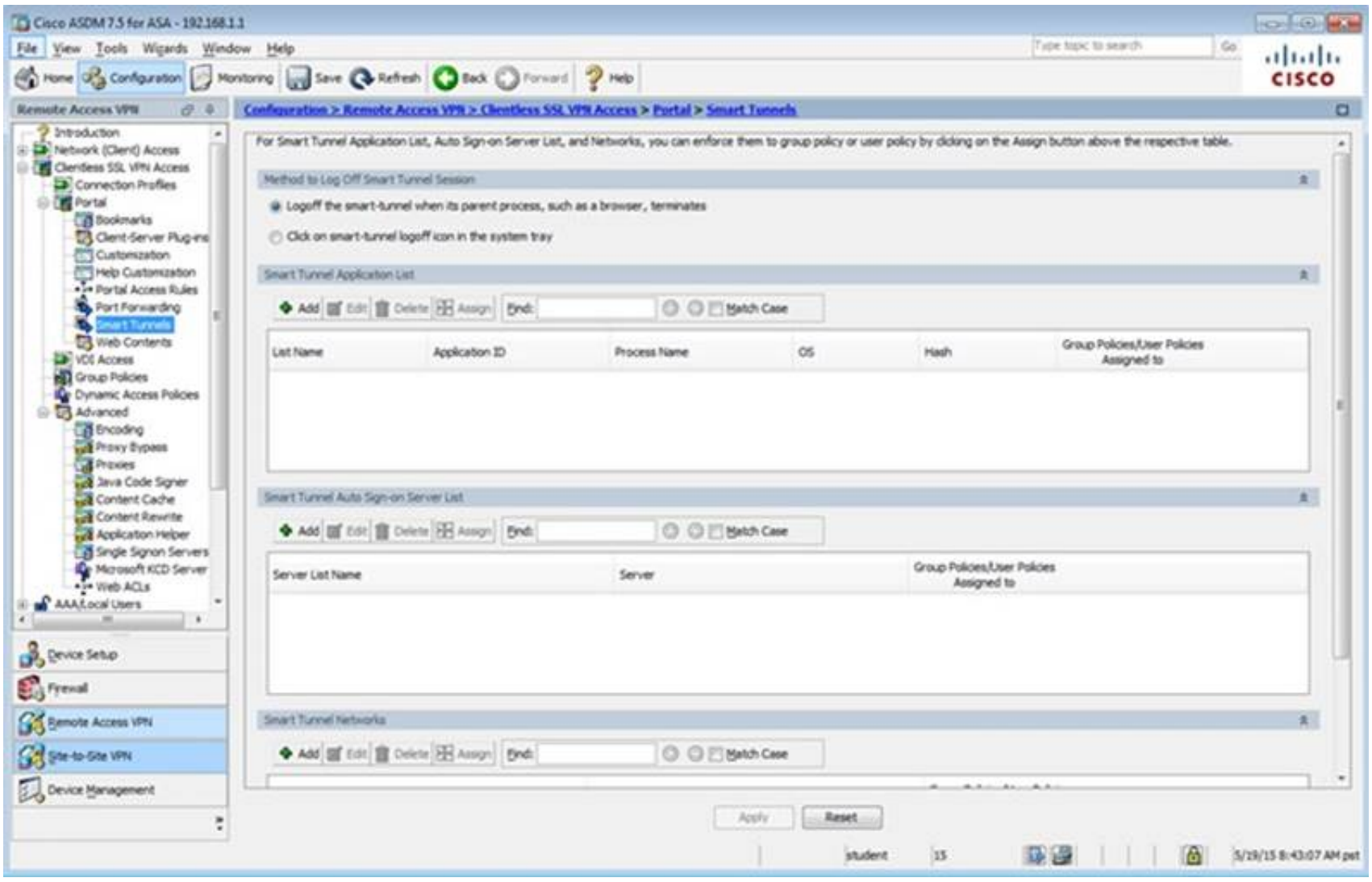

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen when authentication is rejected
Enable the display of SecurId messages on the login screen
Connection Aliases
This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.
Add
Delete
(The table is in-line editable.)
Alias
Enabled
test
Group URLs
This SSL VPN access method will automatically select the connection profile, without the need for user selection.
Add
Delete
(The table is in-line editable.)
URL
Enabled
https://209.165.201.2/test
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)
Always run CSD
Disable CSD for both AnyConnect and Clientless SSL VPN
Disable CSD for AnyConnect only
Find:
Next
Previous
OK
Cancel
Help

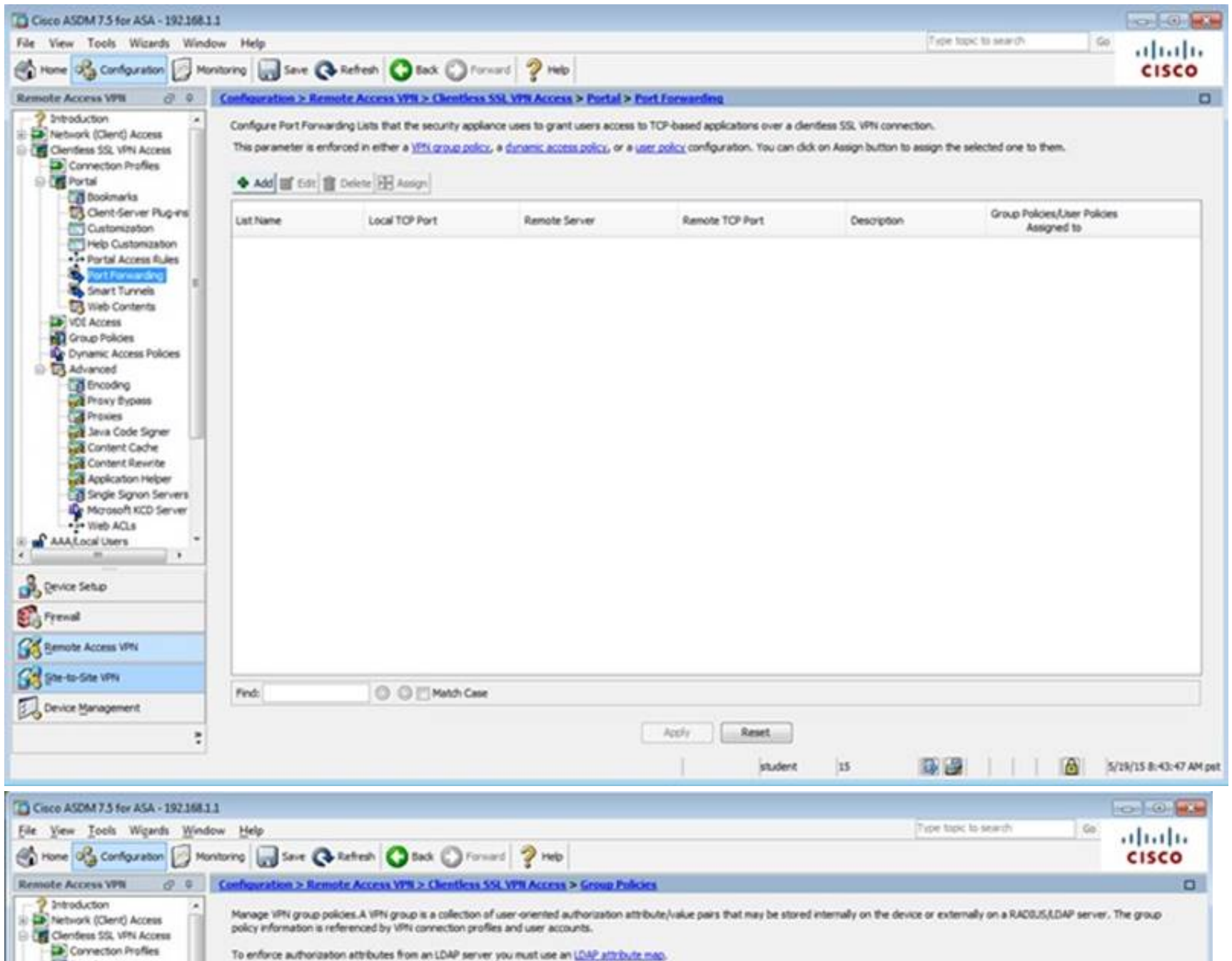

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from Certificate
Pre-fill Username from Certificate
Hide username from end user
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

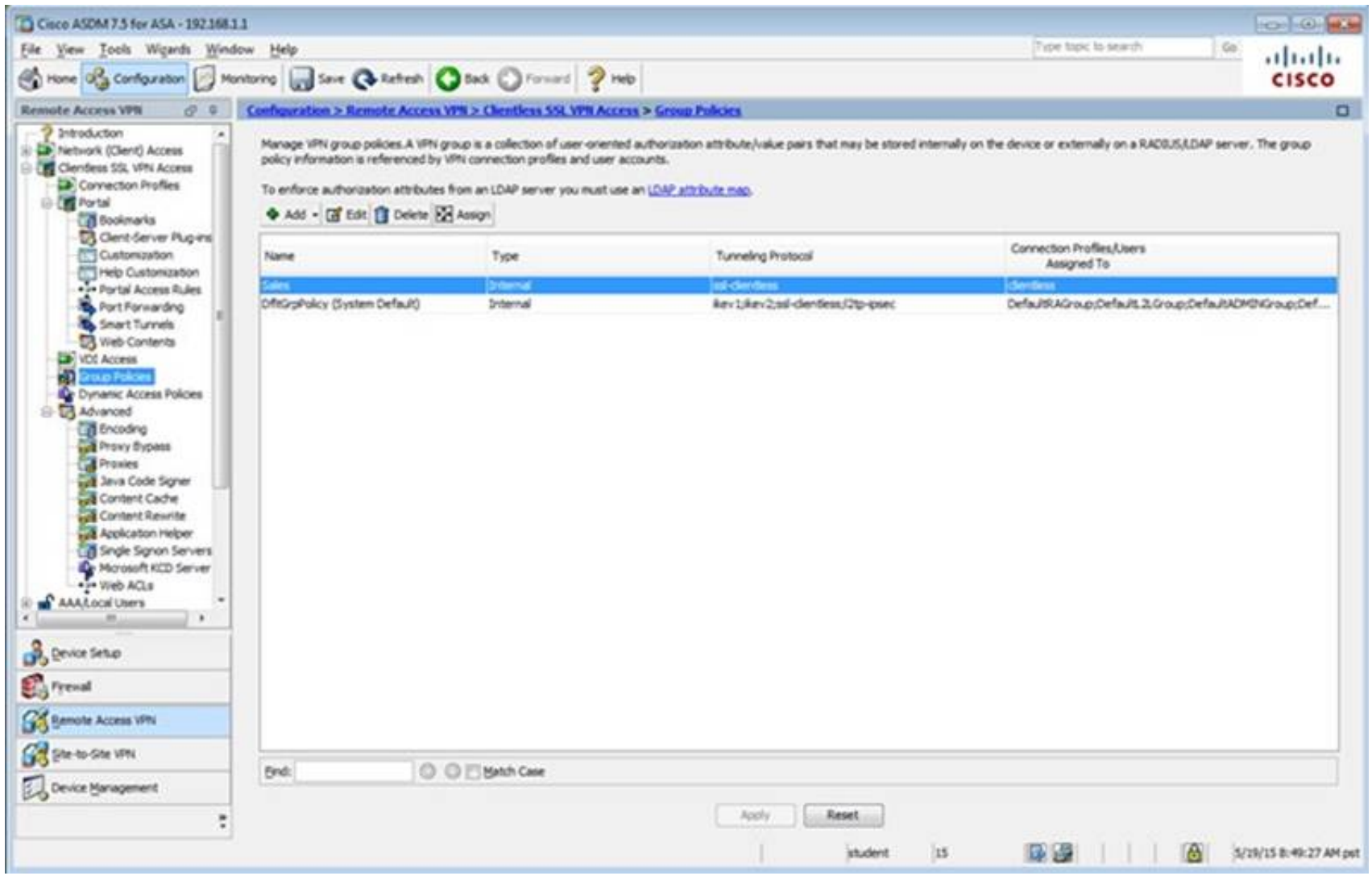

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
-- None --
Manage...
Use LOCAL if Server Group fails
Use primary username (Hide secondary username on login page)
Attributes Server:
Primary
Secondary
Session Username Server:
Primary
Secondary
Interface-Specific Secondary Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Use primary username
Username Mapping from Certificate
Pre-fill username from certificate
Hide username from end user
Fallback when a certificate is unavailable
Password:
Prompt
Use primary
Use
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

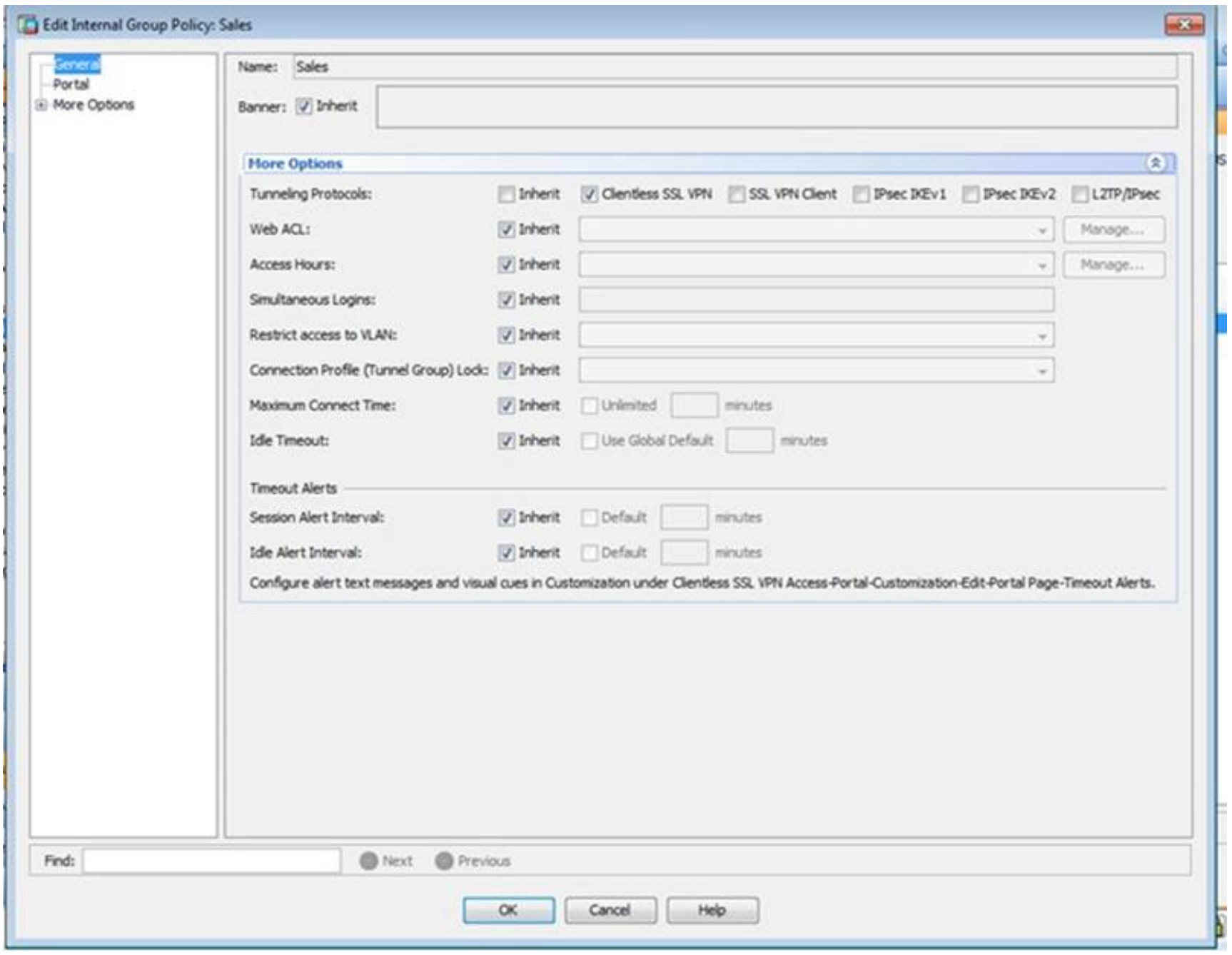

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add
Edit
Delete
Import
Export
Assign
Bookmarks
Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:41:57 AM pst

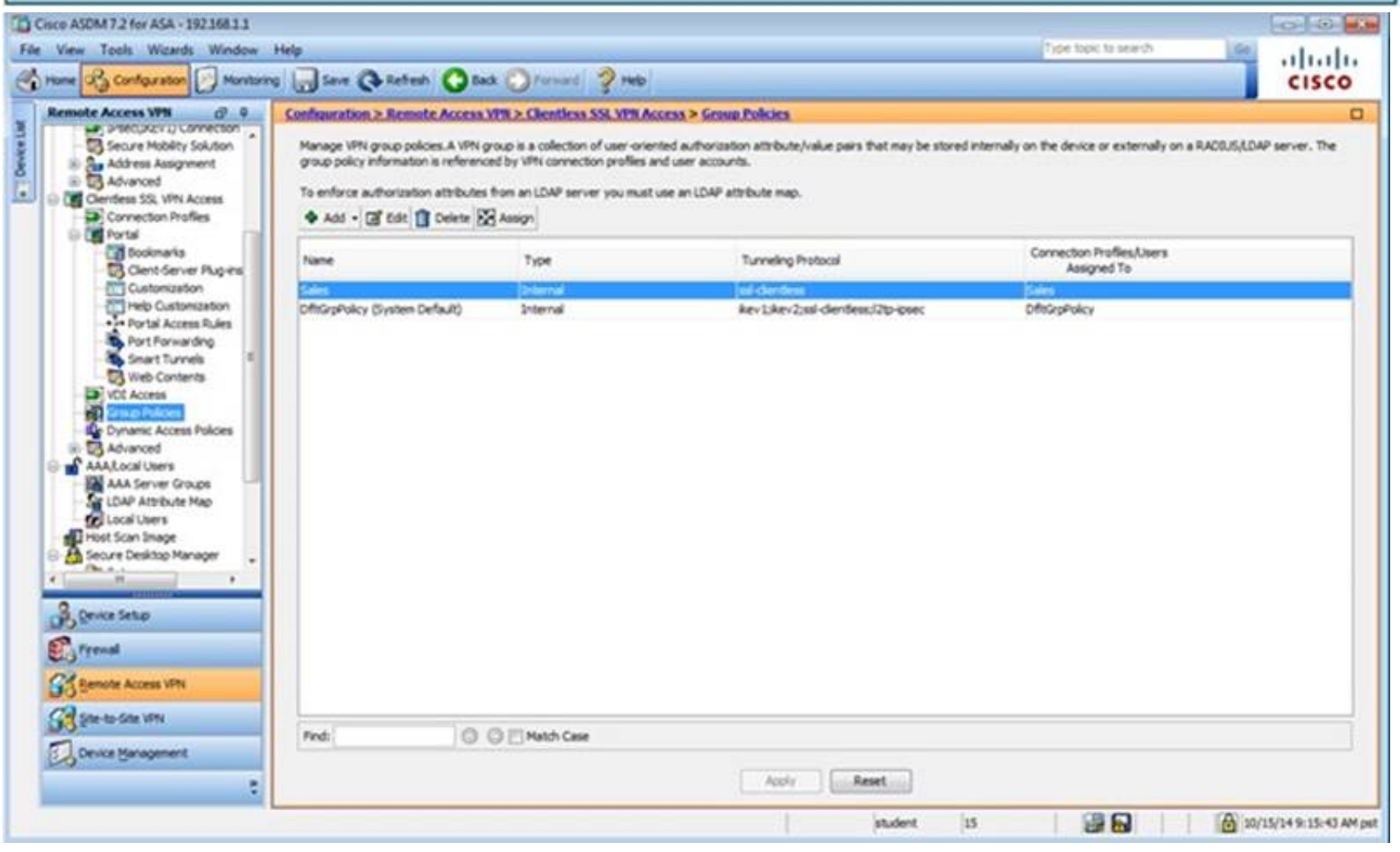

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

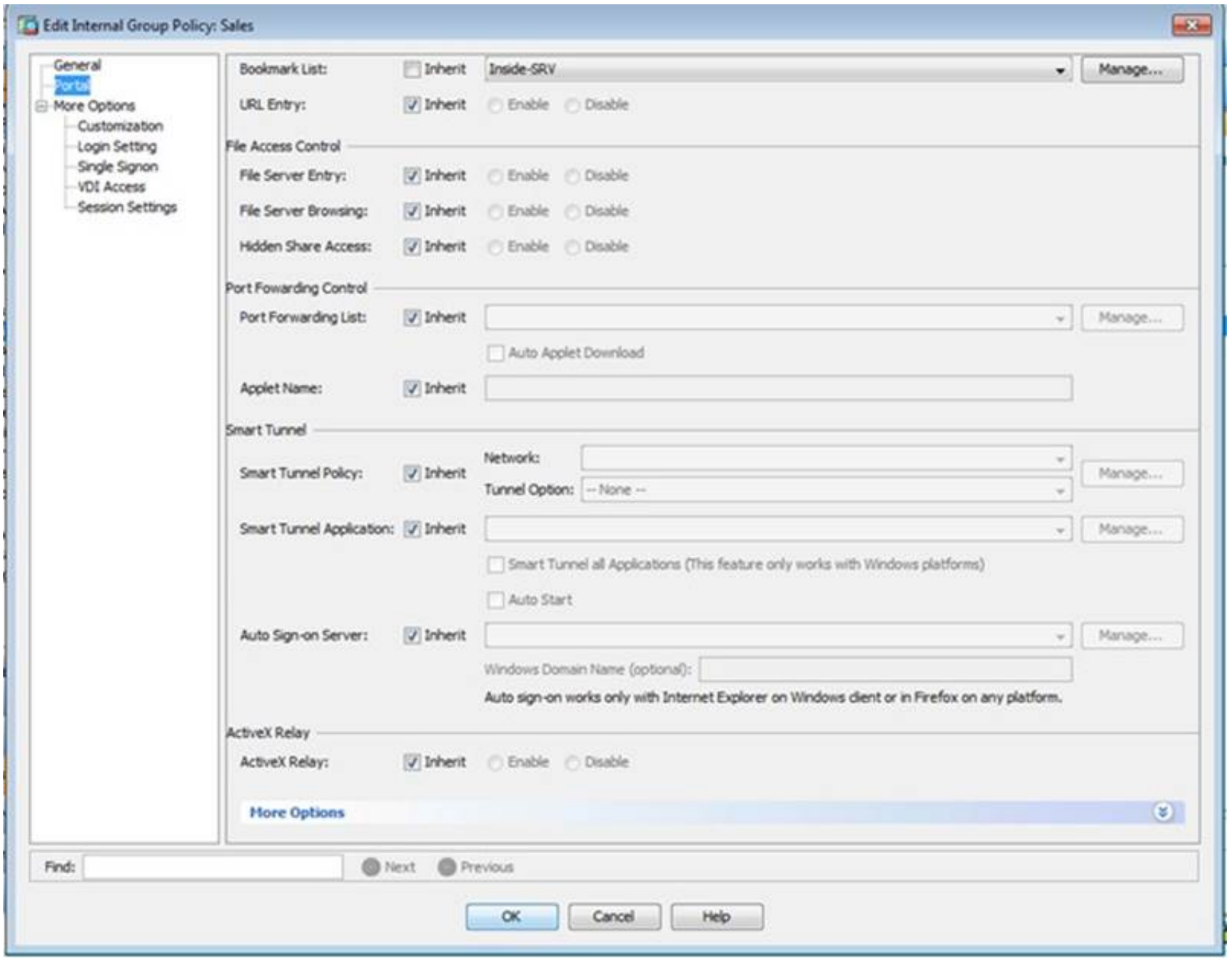

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Add Edit Delete Assign Find: Match Case
List Name
Application ID
Process Name
OS
Hash
Group Policies/User Policies Assigned to
Smart Tunnel Auto Sign-on Server List
Add Edit Delete Assign Find: Match Case
Server List Name
Server
Group Policies/User Policies Assigned to
Smart Tunnel Networks
Add Edit Delete Assign Find: Match Case
Apply
Reset
student
15
5/19/15 8:43:07 AM pst

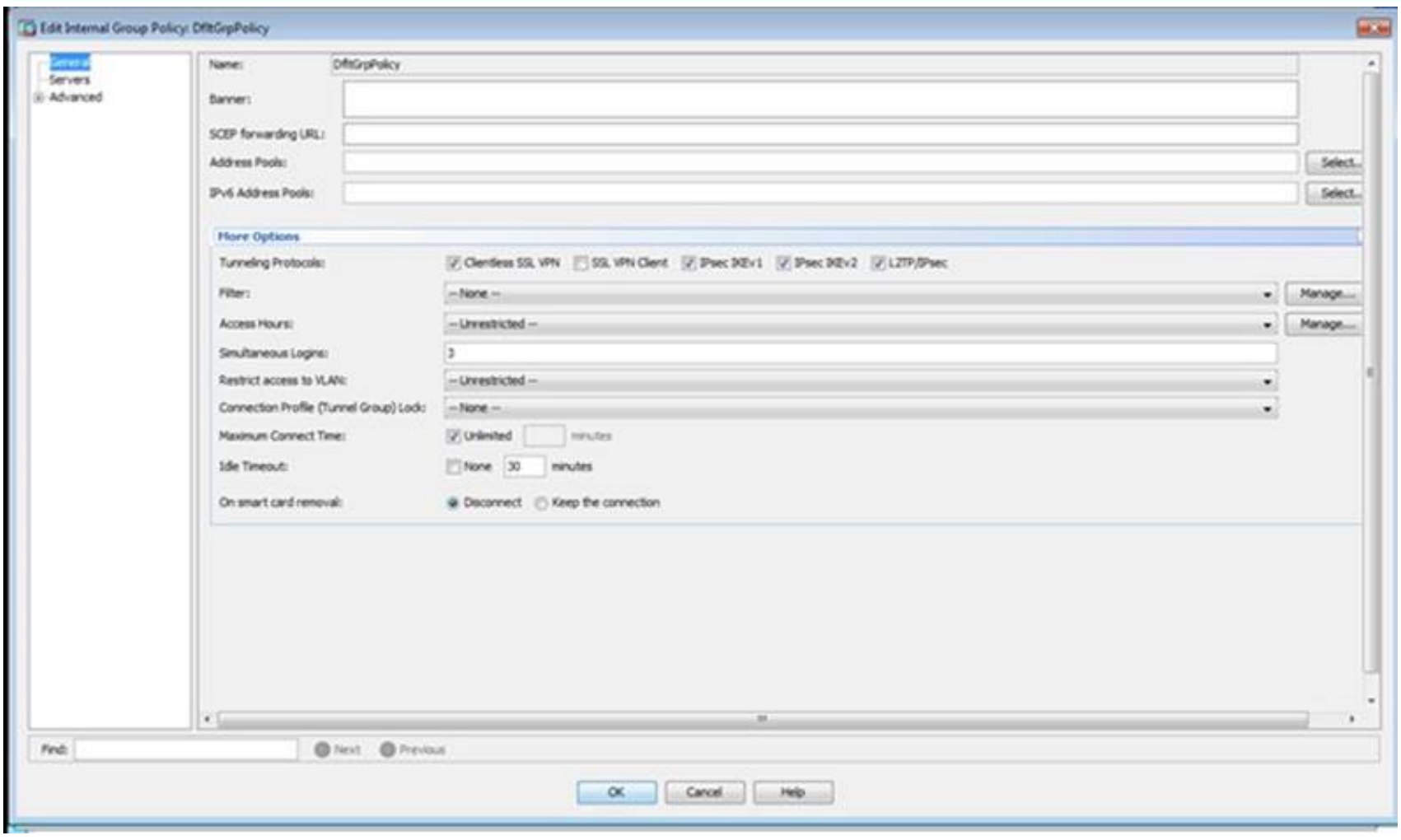

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add Edit Delete Assign
List Name
Local TCP Port
Remote Server
Remote TCP Port
Description
Group Policies/User Policies Assigned to
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:43:47 AM pst

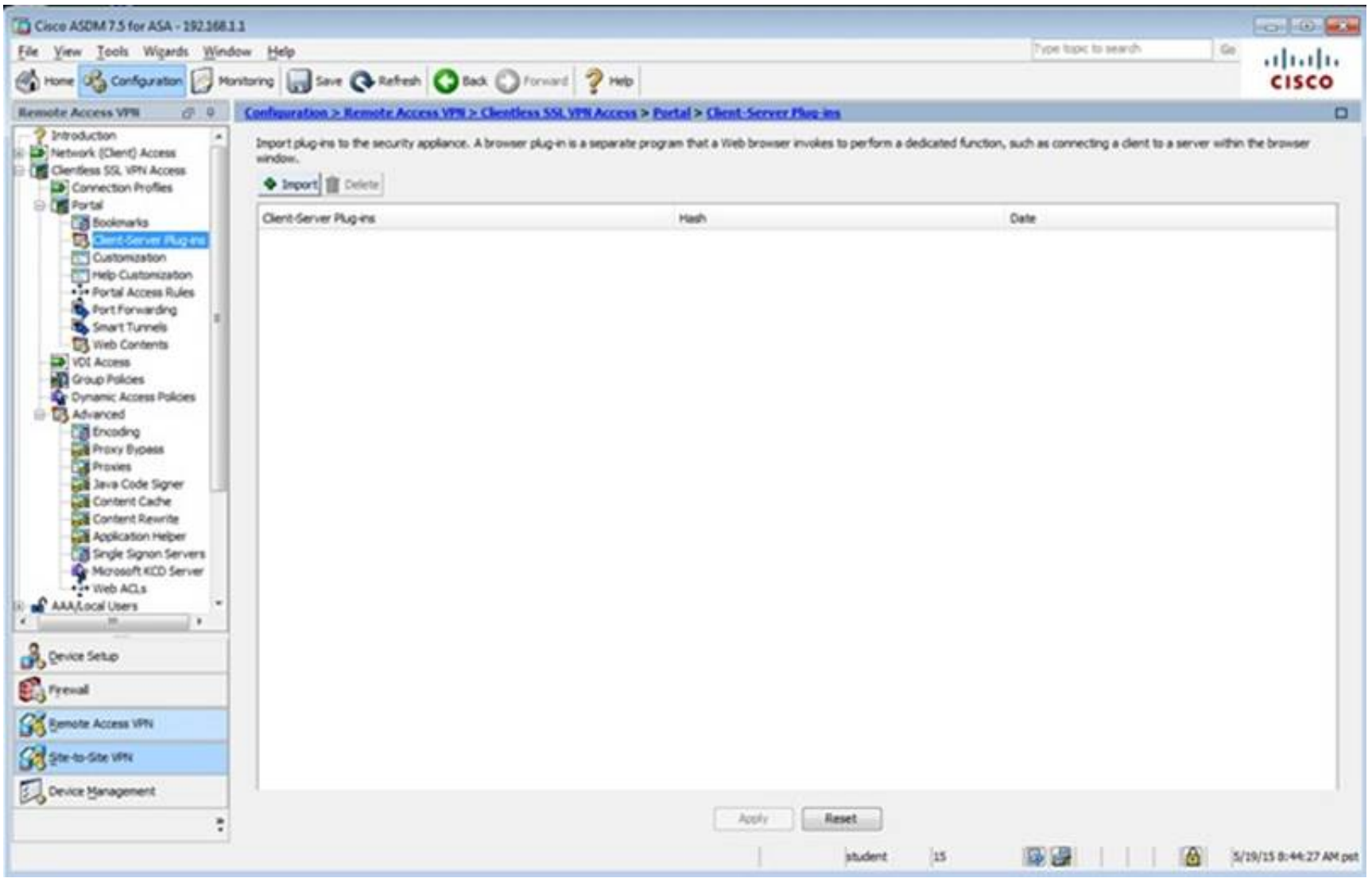

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:49:27 AM pst

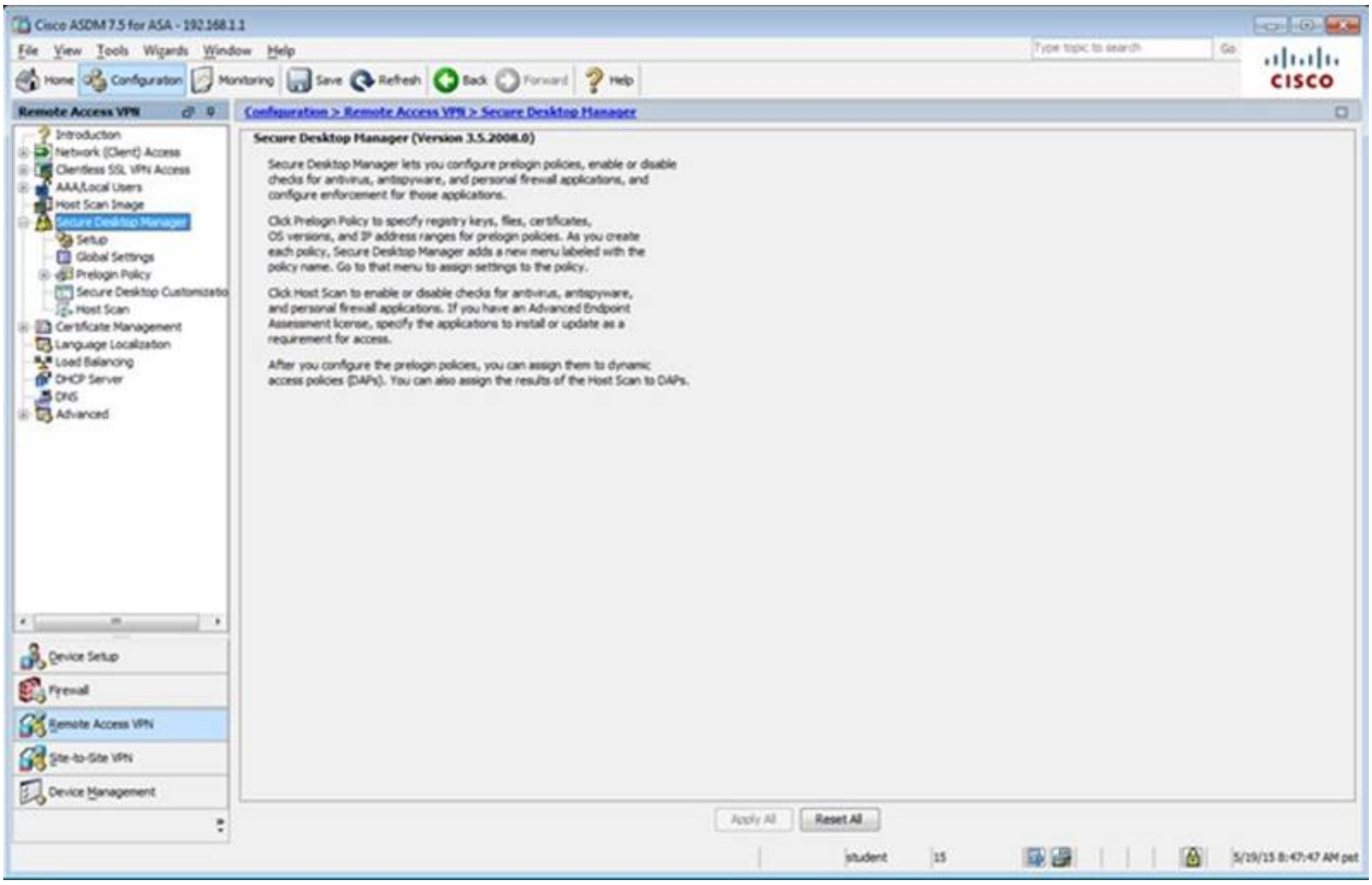

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access to VLAN: Inherit
Connection Profile (Tunnel Group) Lock: Inherit
Maximum Connect Time: Inherit Unlimited minutes
Idle Timeout: Inherit Use Global Default minutes
Timeout Alerts
Session Alert Interval: Inherit Default minutes
Idle Alert Interval: Inherit Default minutes
Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.
Find: Next Previous
OK Cancel Help

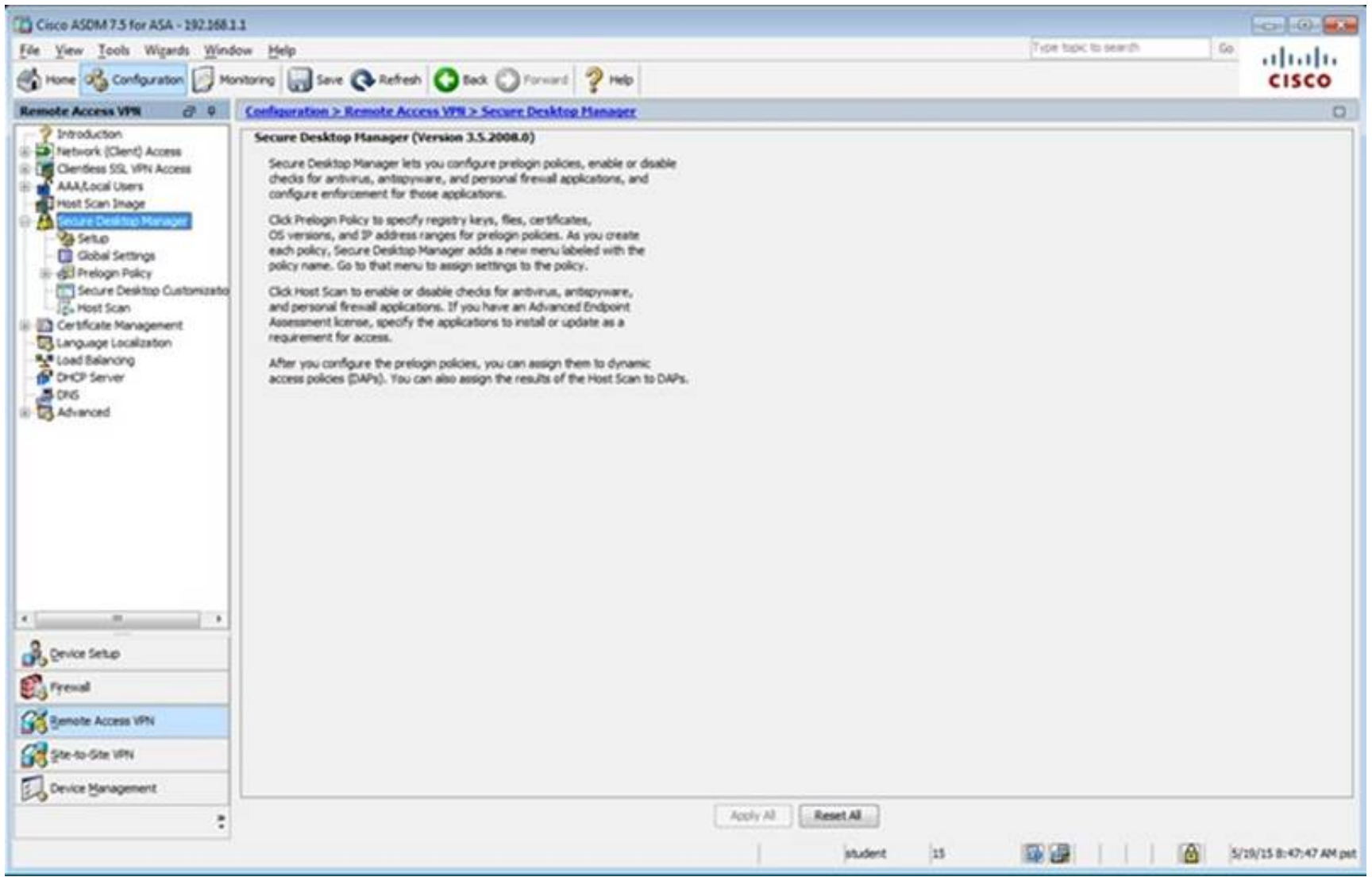

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To
Sales | Internal | ssl-clientless | Sales
DfltGrpPolicy (System Default) | Internal | ikev1;ikev2;ssl-clientless;l2tp-ipsec | DfltGrpPolicy
Find: Match Case
Apply Reset
student 15 10/15/14 9:15:43 AM pst

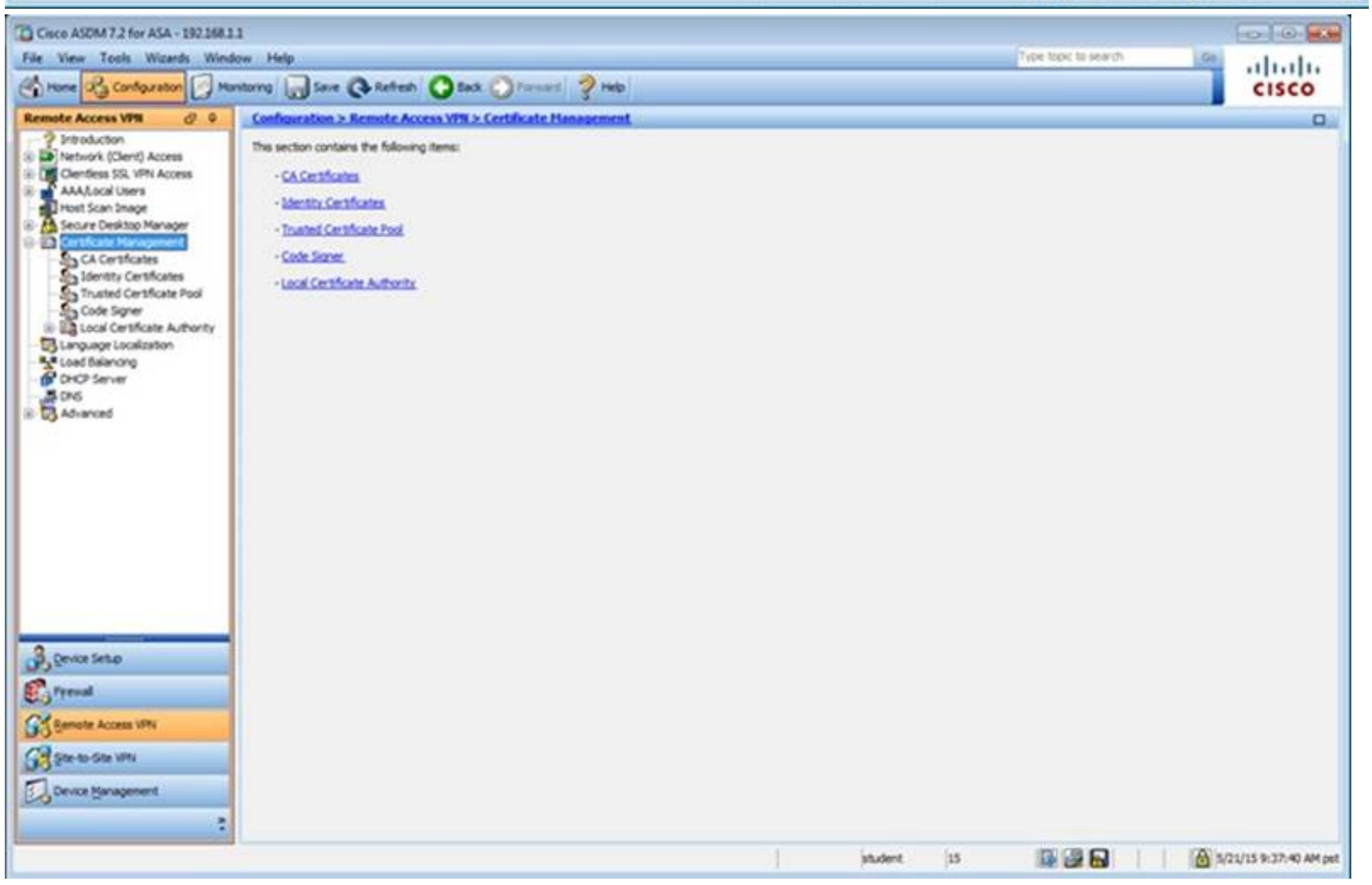

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding Control
Port Forwarding List:
Auto Applet Download
Applet Name:
Smart Tunnel
Network:
Smart Tunnel Policy:
Tunnel Option:
-- None --
Smart Tunnel Application:
Smart Tunnel all Applications (This feature only works with Windows platforms)
Auto Start
Auto Sign-on Server:
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:
More Options
Find:
Next
Previous
OK
Cancel
Help

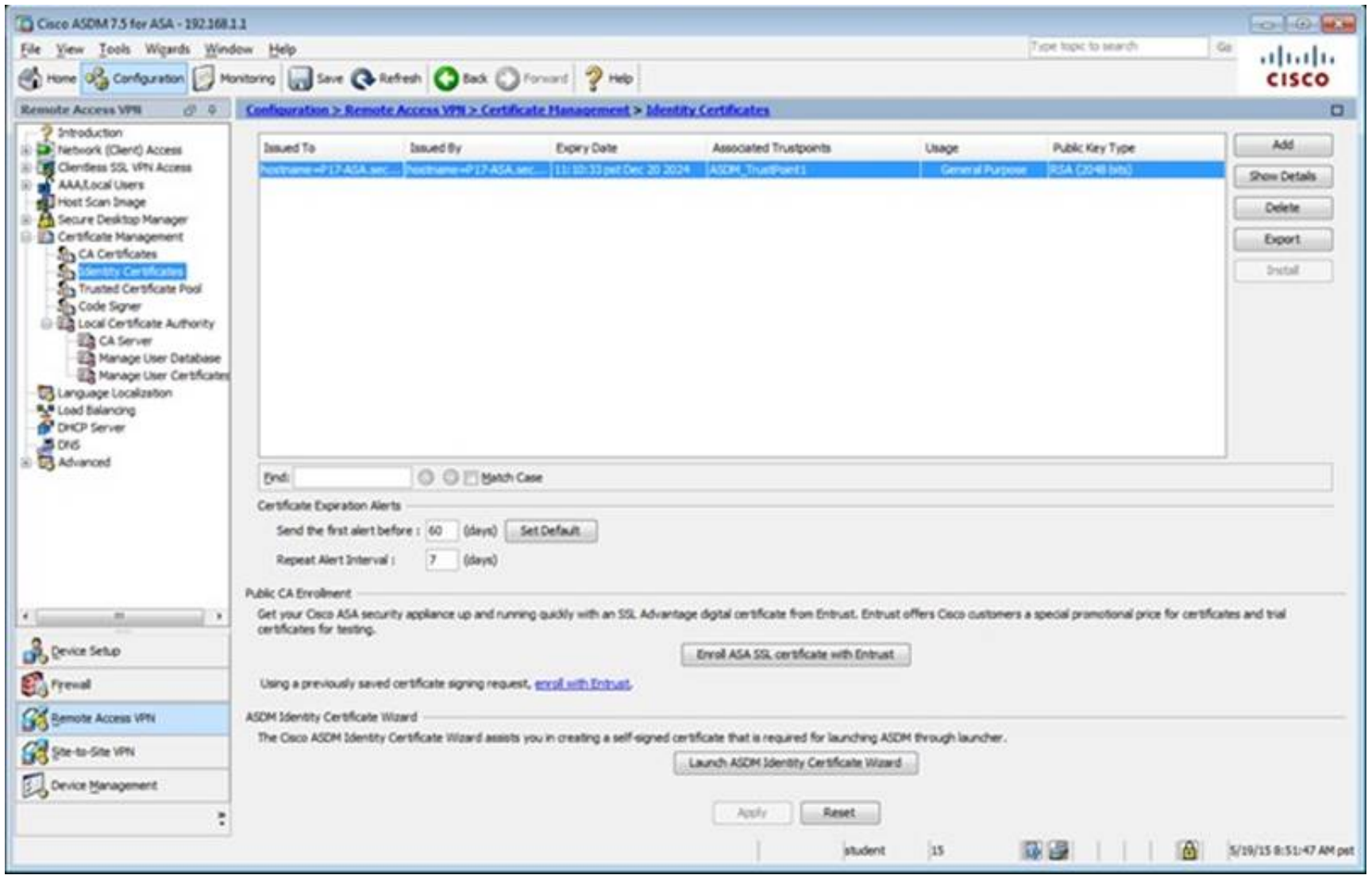

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
Select...
IPv6 Address Pools:
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- Unrestricted --
Simultaneous Logins:
3
Restrict access to VLAN:
Connection Profile (Tunnel Group) Lock:
Maximum Connect Time:
Unlimited
minutes
Idle Timeout:
None
30
minutes
On smart card removal:
Disconnect
Keep the connection
Find:
Next
Previous
OK
Cancel
Help

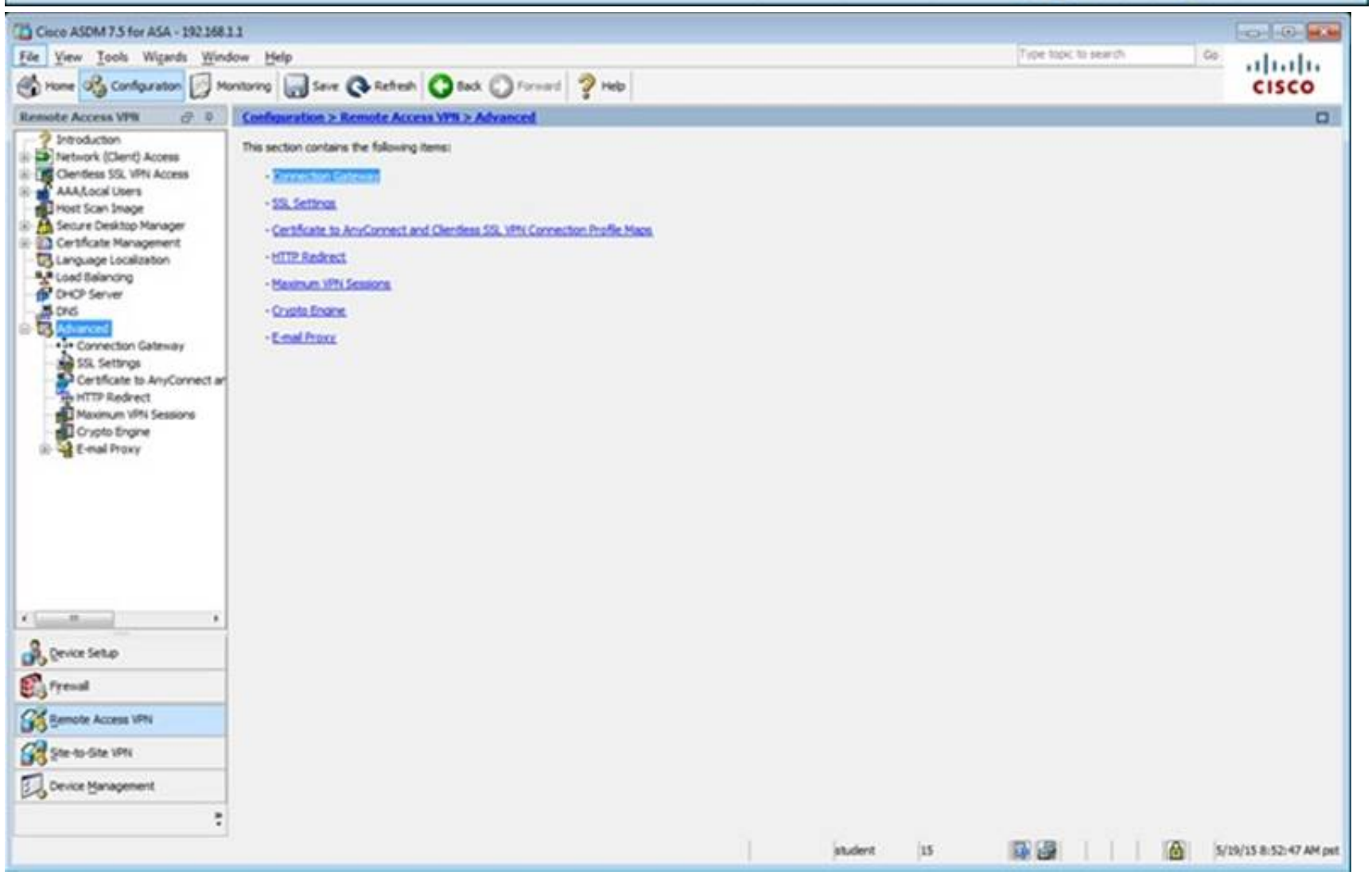

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:44:27 AM pst

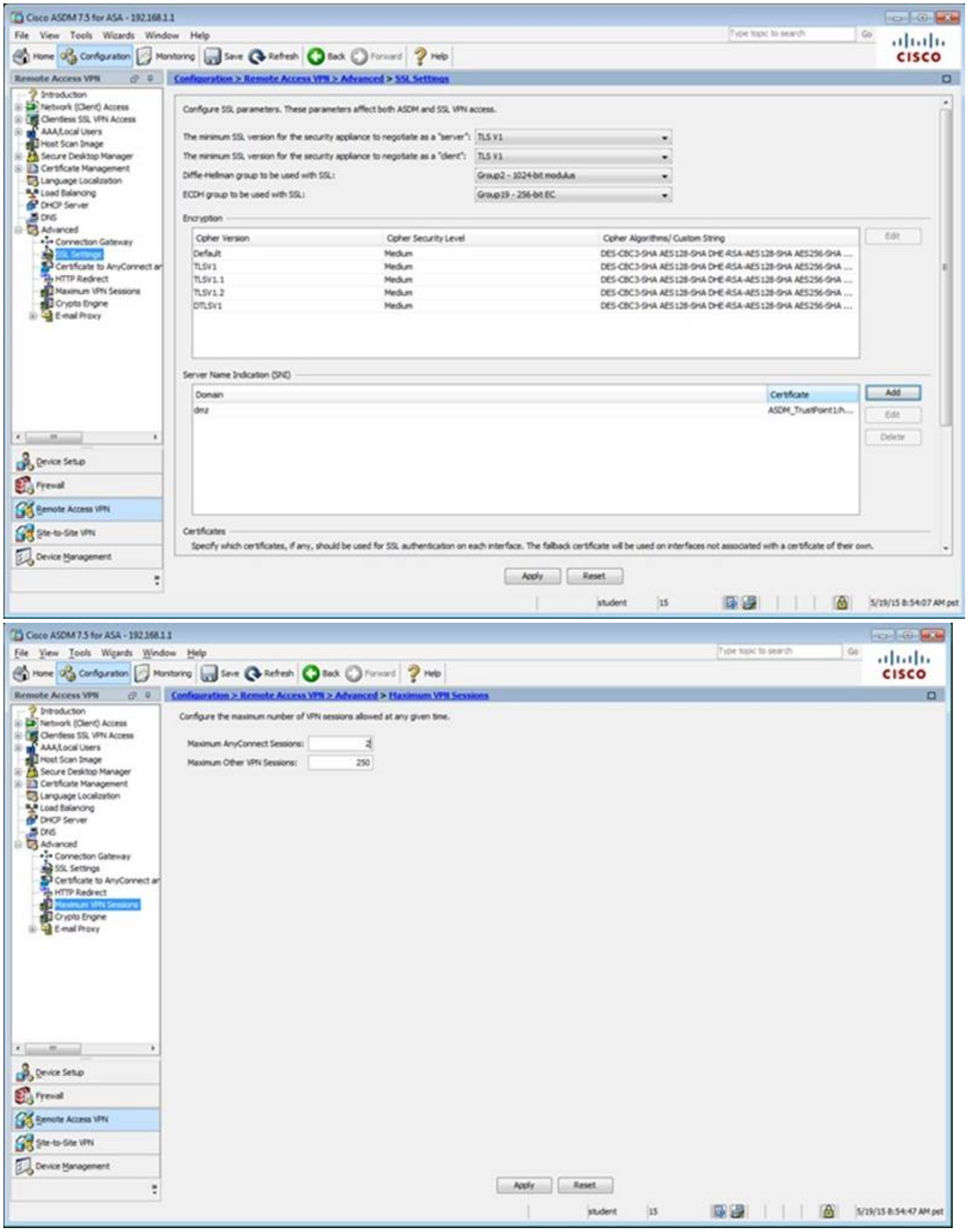

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Secure Desktop Customizatio
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply All
Reset All
student
15
5/19/15 8:47:47 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Secure Desktop Customizatio
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply All
Reset All
student
15
5/19/15 8:47:47 AM pst

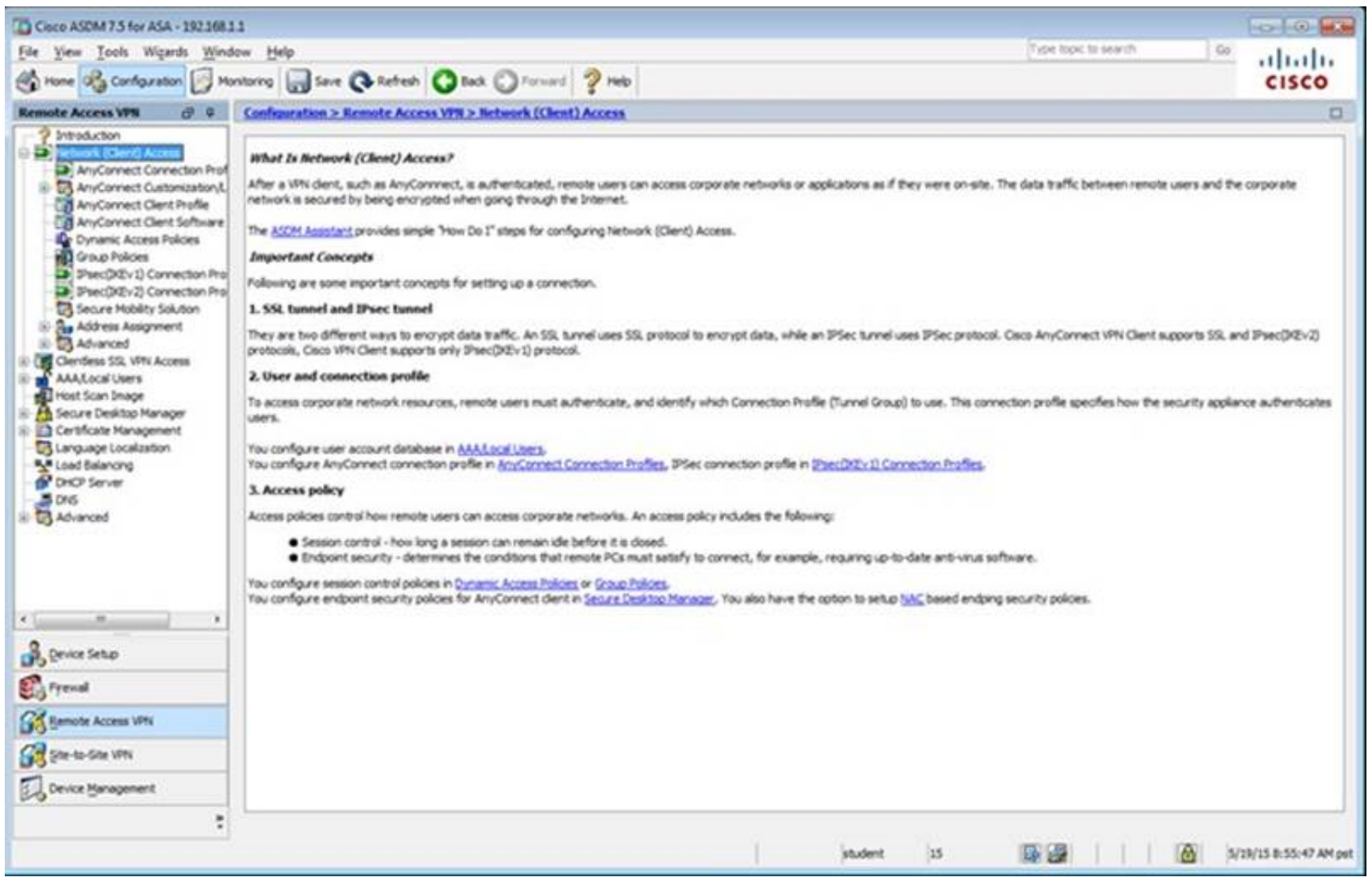

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/21/15 9:37:40 AM pst

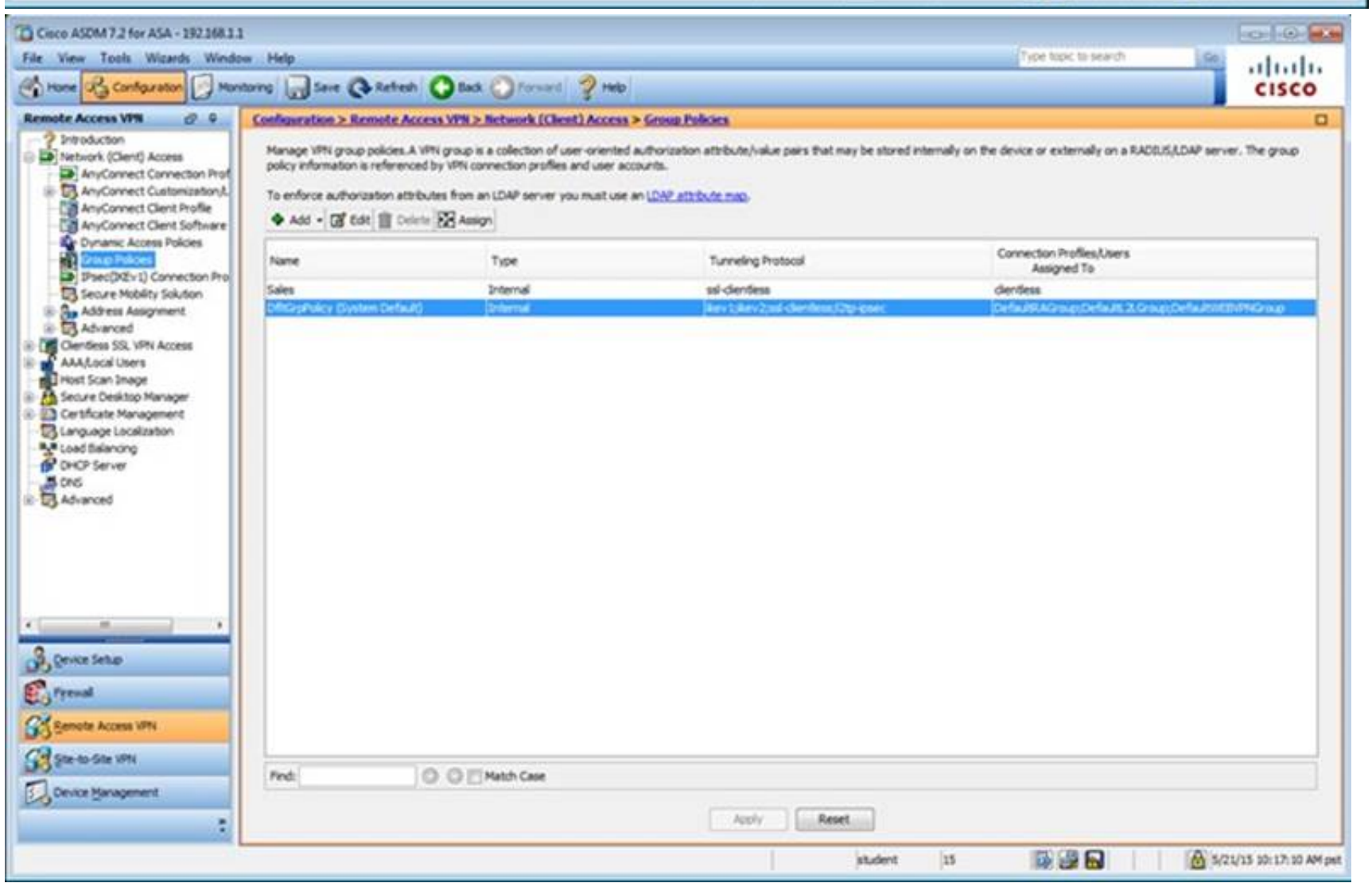

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
CA Server
Manage User Database
Manage User Certificates
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
Public Key Type
Add
Show Details
Delete
Export
Install
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:51:47 AM pst

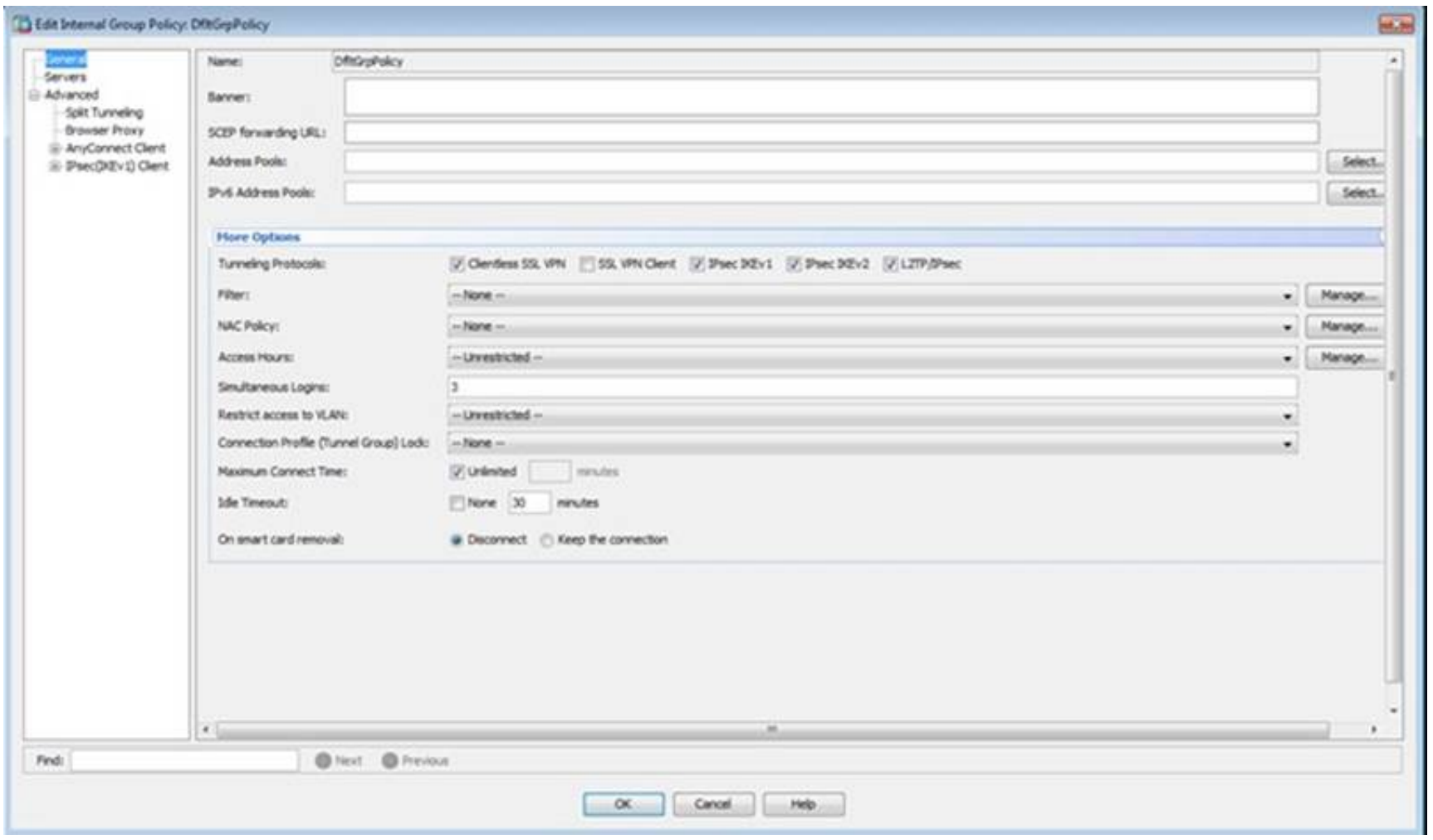

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- Connection Gateway
- SSL Settings
- Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps
- HTTP Redirect
- Maximum VPN Sessions
- Crypto Engine
- E-mail Proxy
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:52:47 AM pst

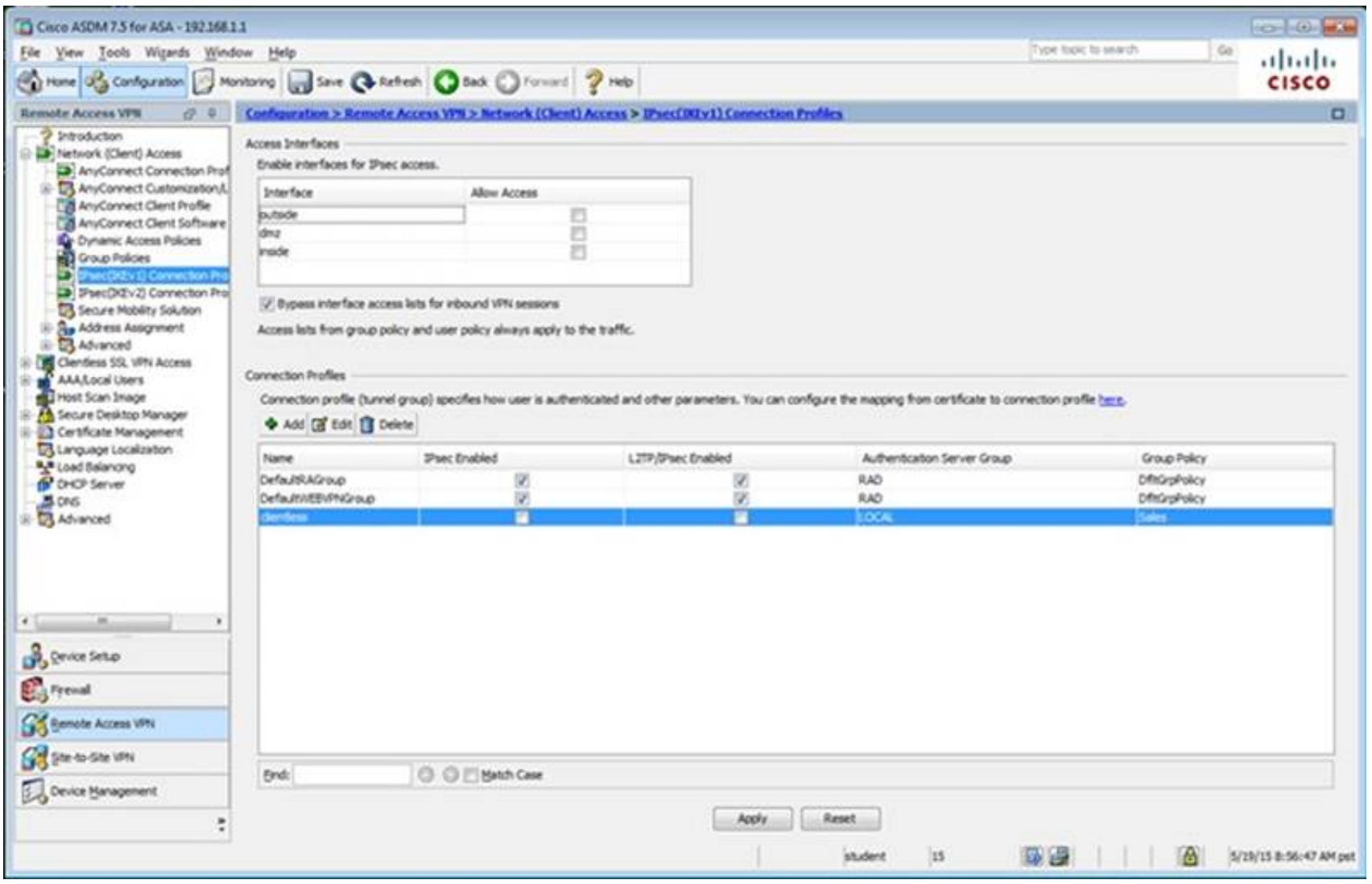

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
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
Edit
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
Add
Edit
Delete
dmz
ASDM_TrustPoint1:h...
Certificates
Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:54:07 AM pst

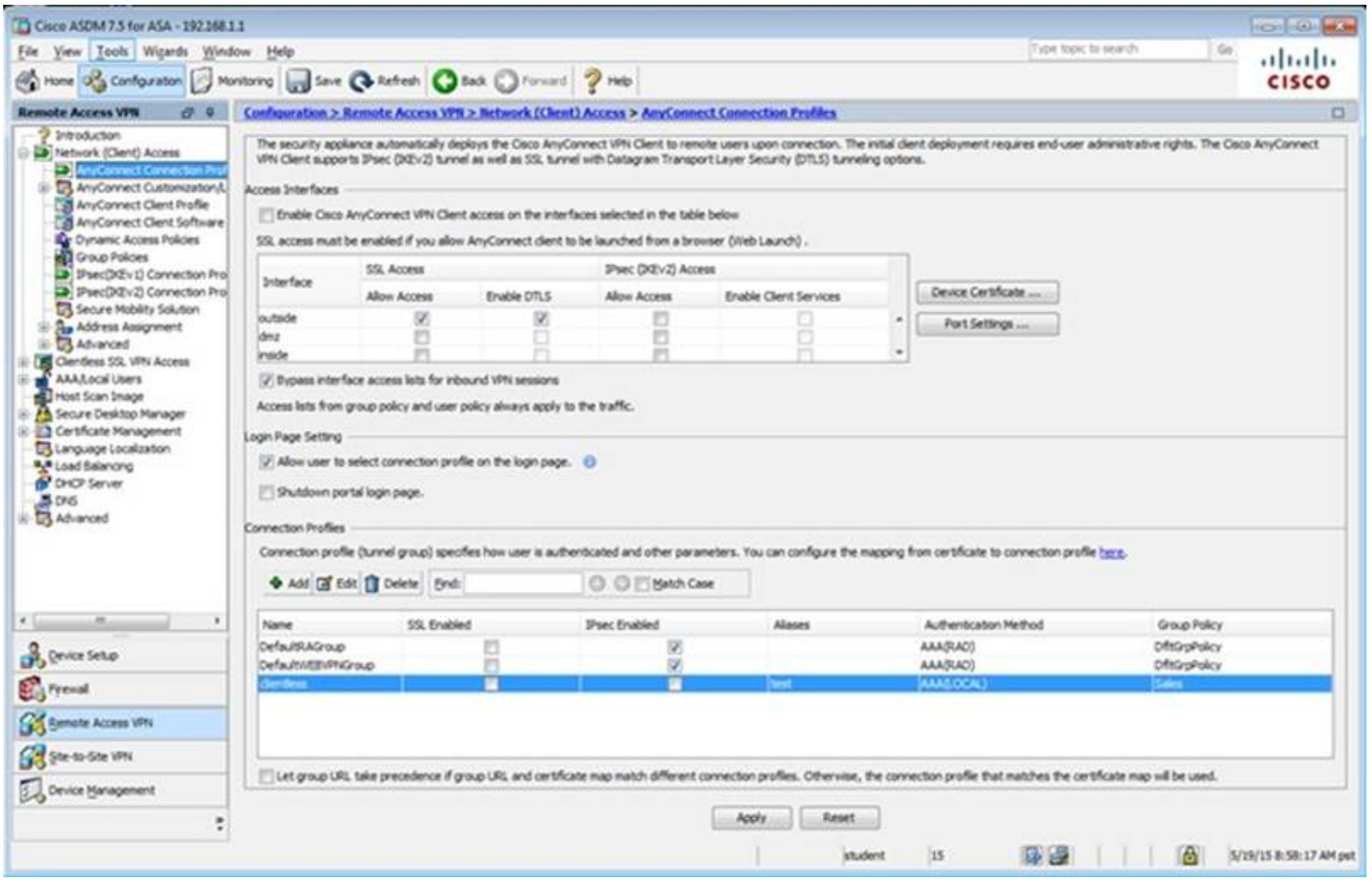
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Configure the maximum number of VPN sessions allowed at any given time.
Maximum AnyConnect Sessions: 2
Maximum Other VPN Sessions: 250
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:54:47 AM pst

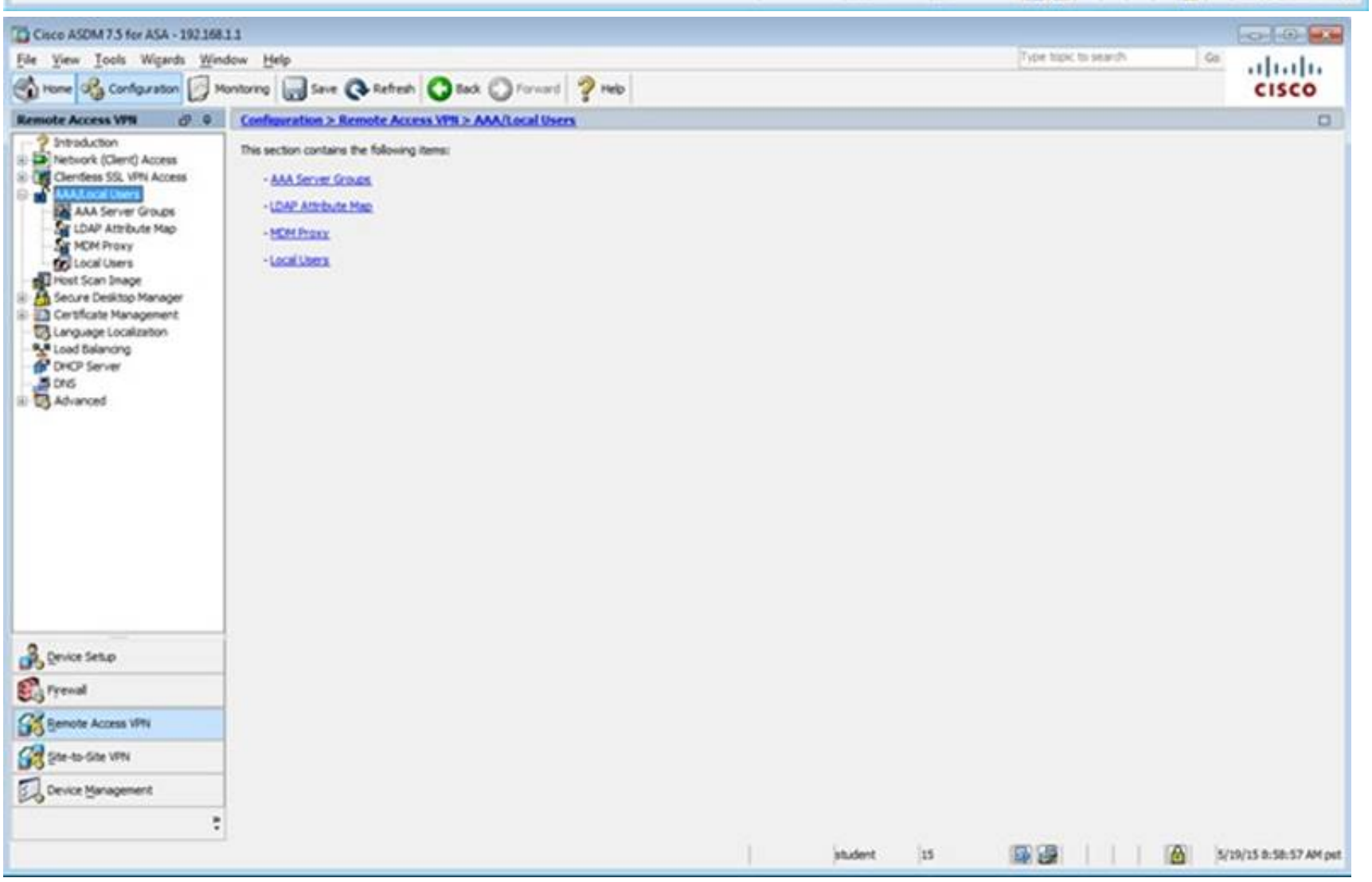

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
The ASDM Assistant provides simple "How Do I" steps for configuring Network (Client) Access.
Important Concepts
Following are some important concepts for setting up a connection.
1. SSL tunnel and IPsec tunnel
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 endpng security policies.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/20/15 8:55:47 AM pst

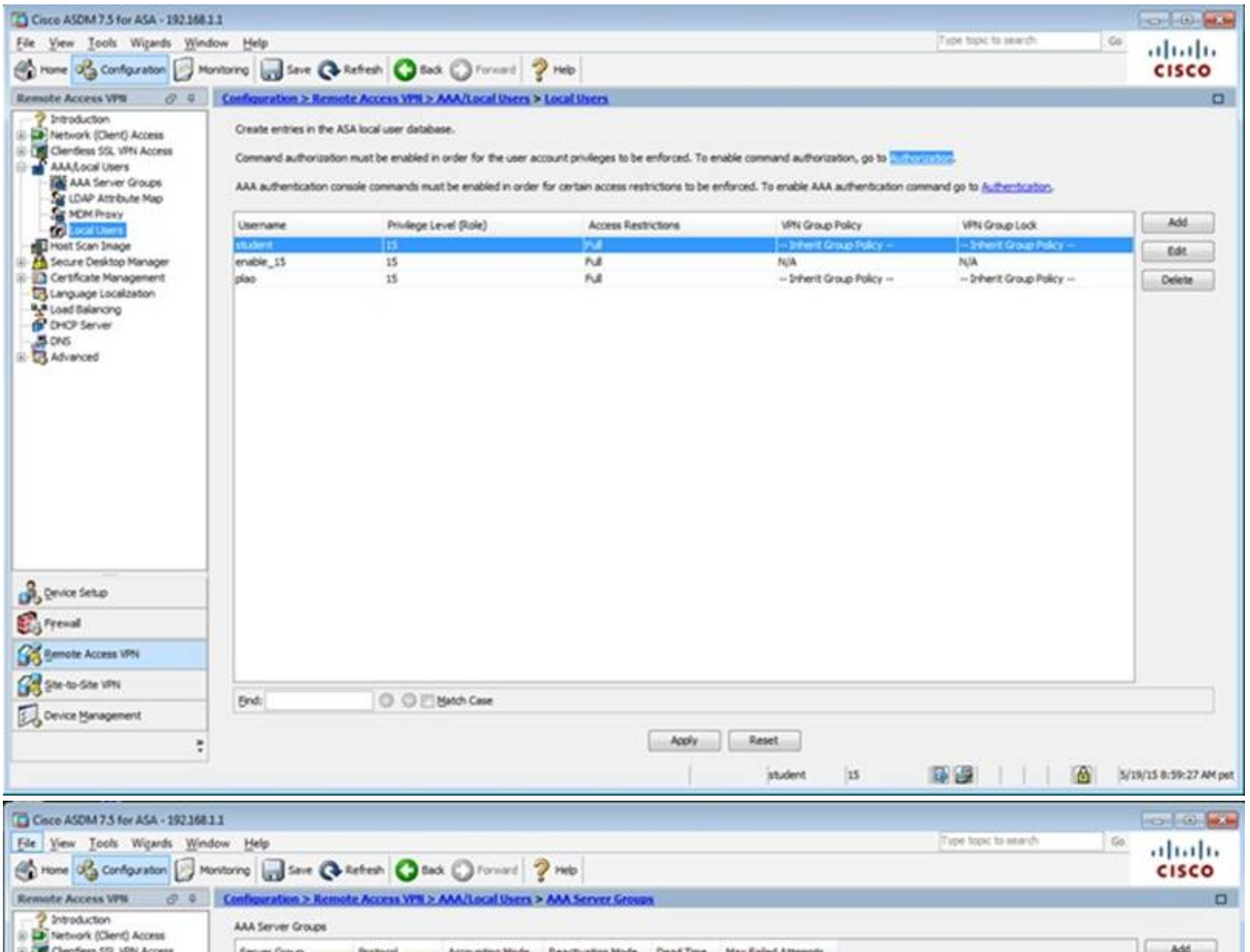

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup
Find:
Match Case
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/21/15 10:17:10 AM pst

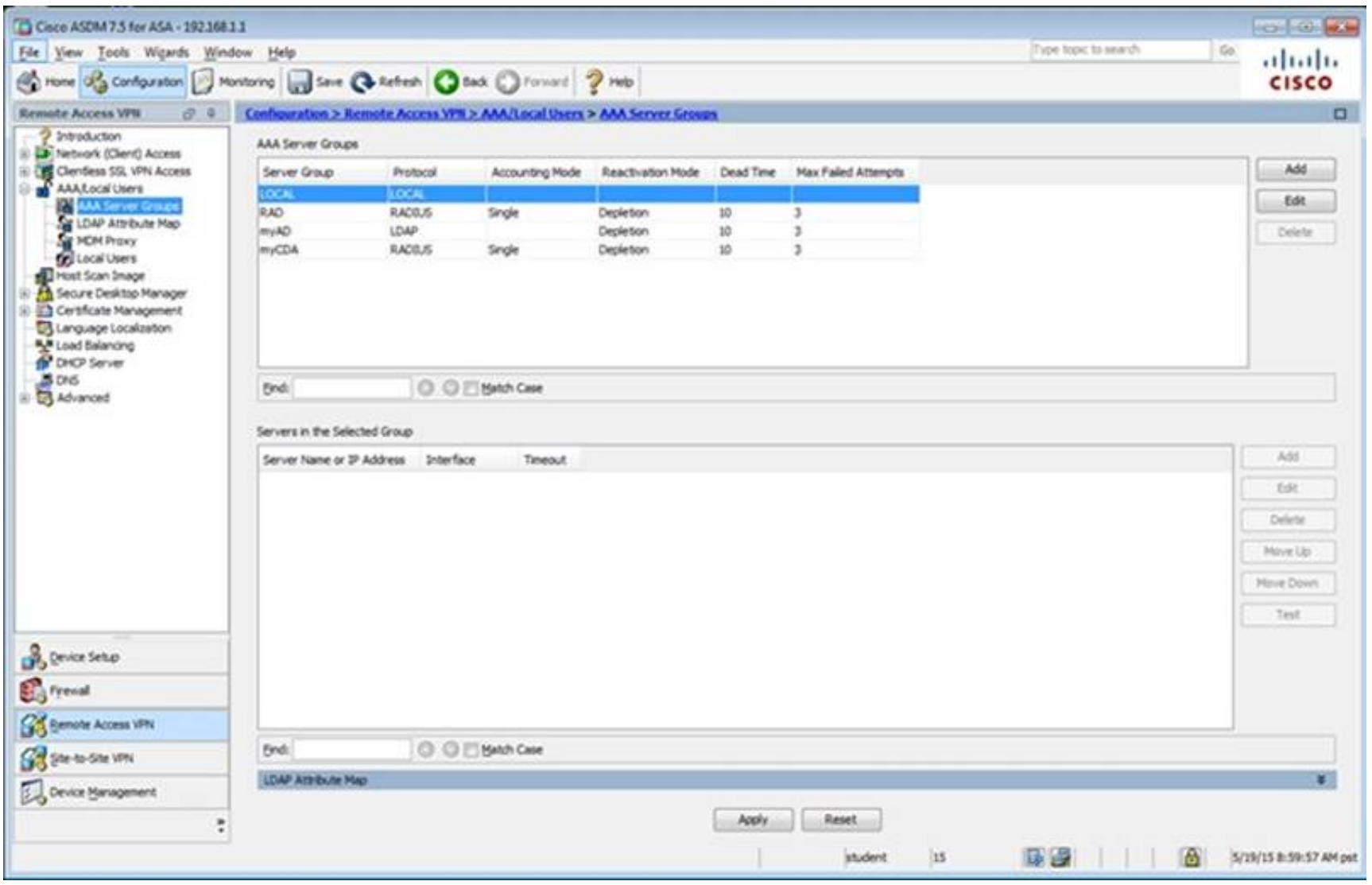

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Name: DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
IPv6 Address Pools:
Select...
More Options
Tunneling Protocols: Clientless SSL VPN, SSL VPN Client, IPsec 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
Idle Timeout: None 30 minutes
On smart card removal: Disconnect, Keep the connection
Manage...
Find:
Next
Previous
OK
Cancel
Help


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Prof
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Authentication Server Group
Group Policy
DefaultRAGroup
RAD
DfltGrpPolicy
DefaultWEBVPNGroup
RAD
DfltGrpPolicy
clientless
LOCAL
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:56:47 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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
Allow Access
Enable DTLS
IPsec (IKEv2) Access
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(RAC)
DfltGrpPolicy
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:17 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > AAA/Local Users
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:57 AM pst



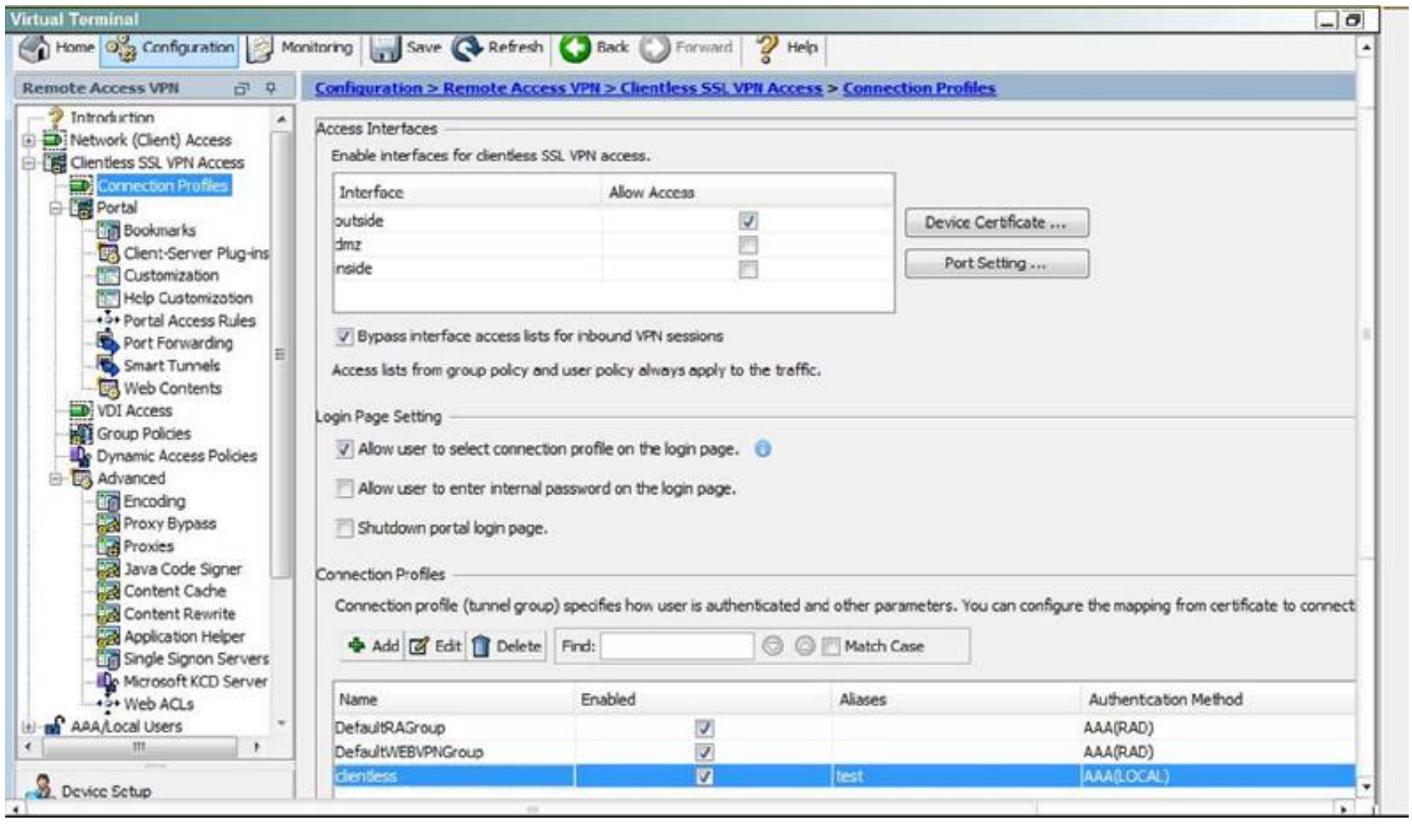


Which user authentication method is used when users login to the Clientless SSLVPN portal using https://209.165.201.2/test?

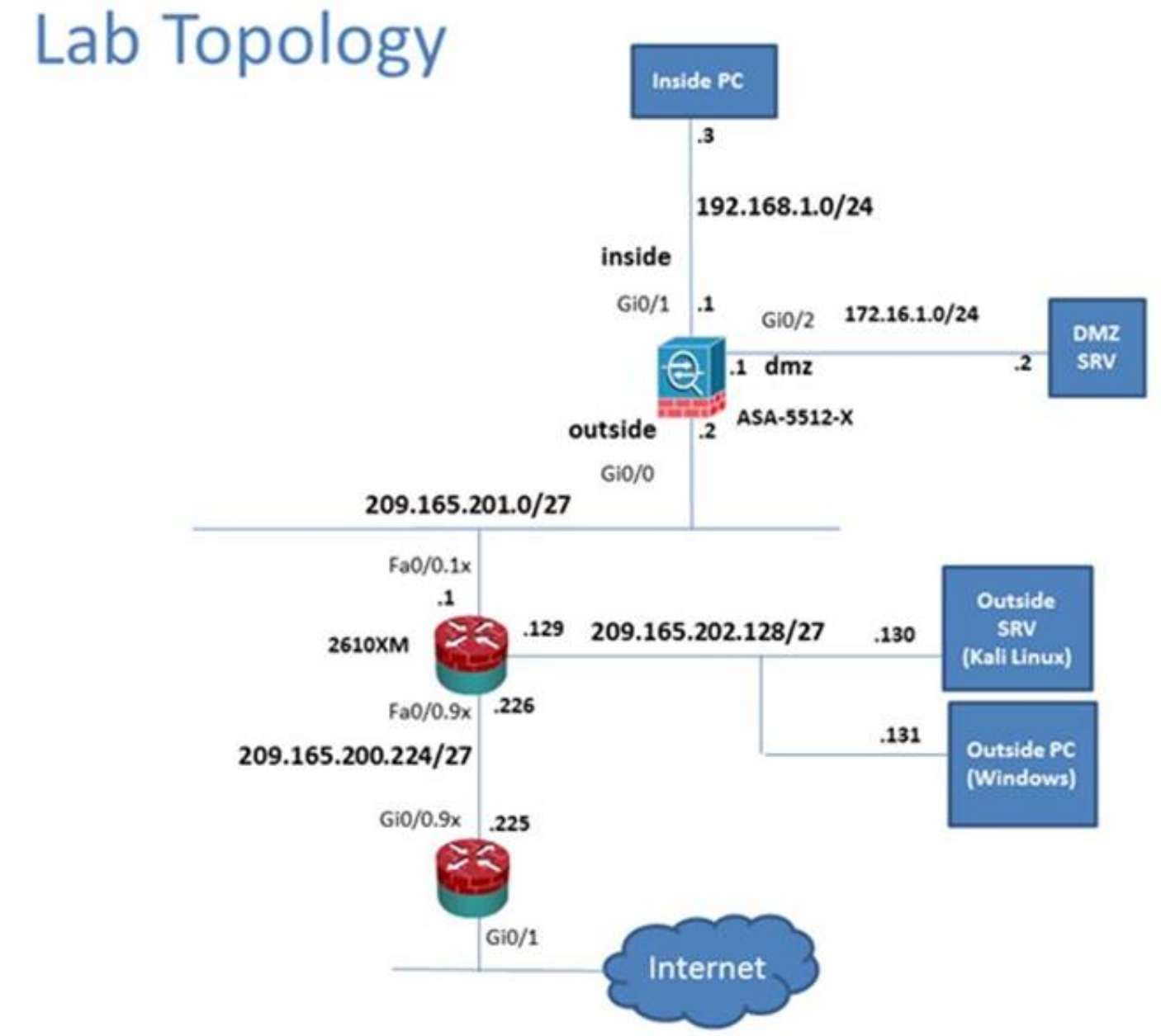
A. AAA with LOCAL database
B. AAA with RADIUS server
C. Certificate
D. Both Certificate and AAA with LOCAL database
E. Both Certificate and AAA with RADIUS server

Answer: A

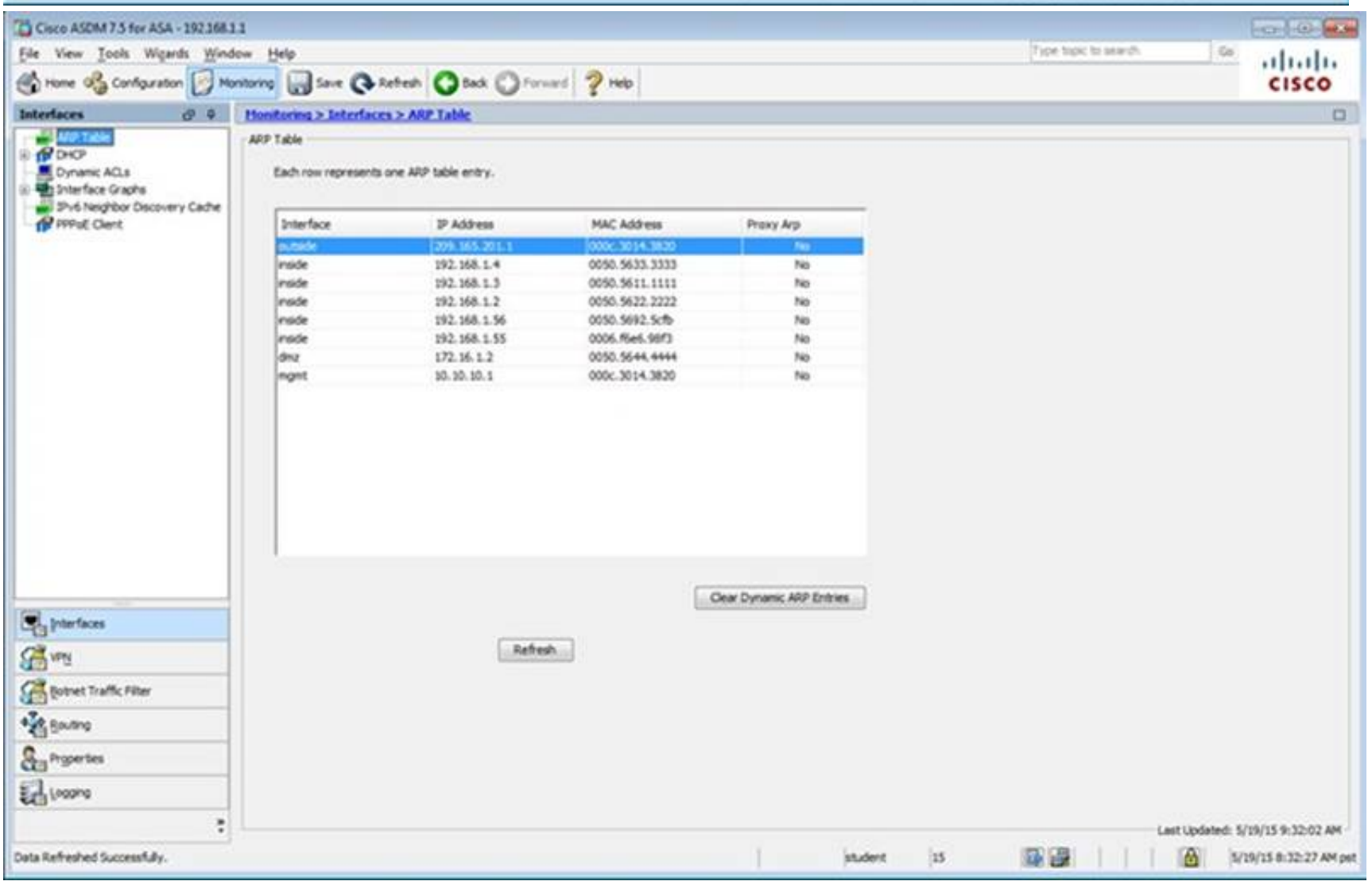
Explanation: This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used,

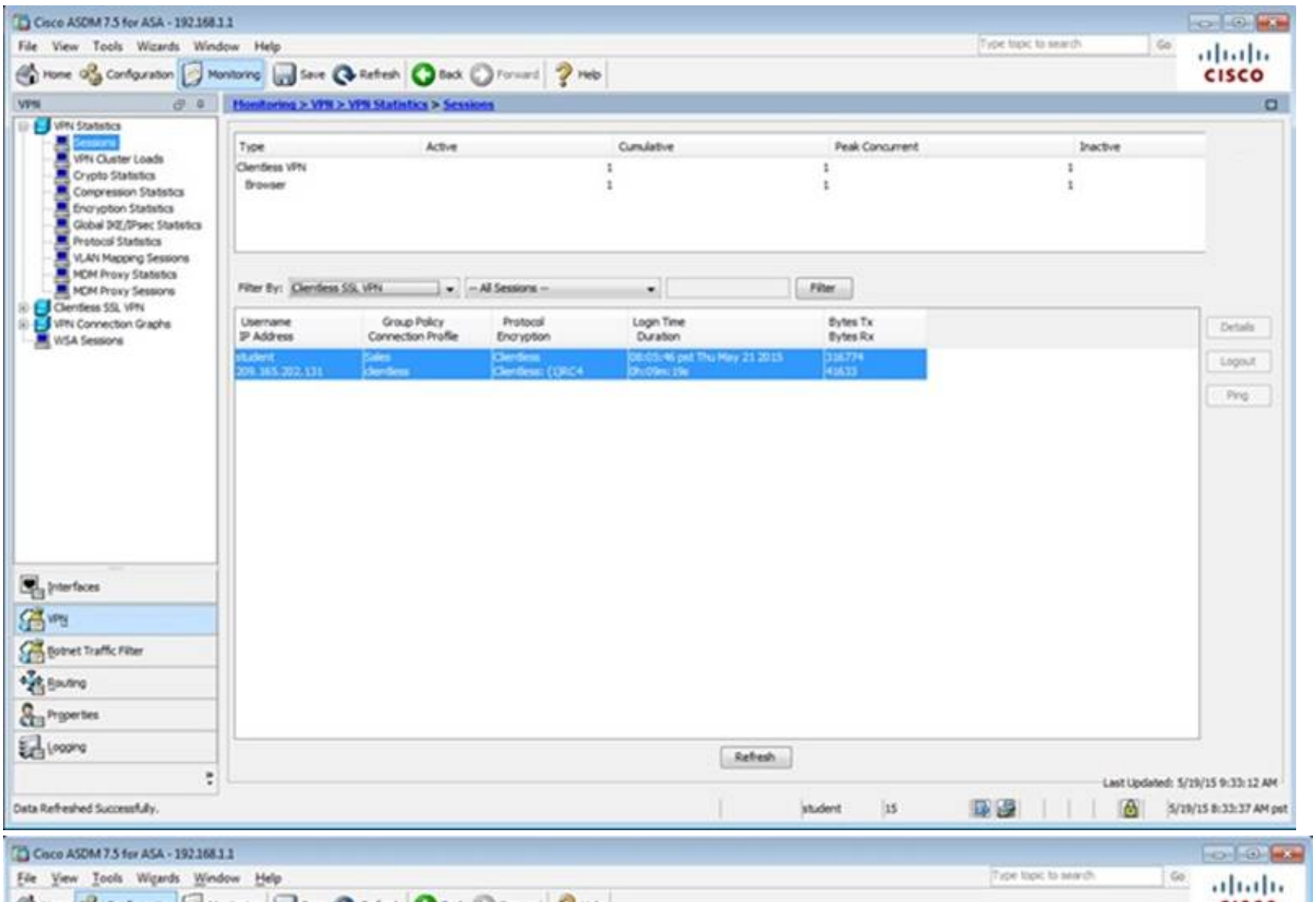


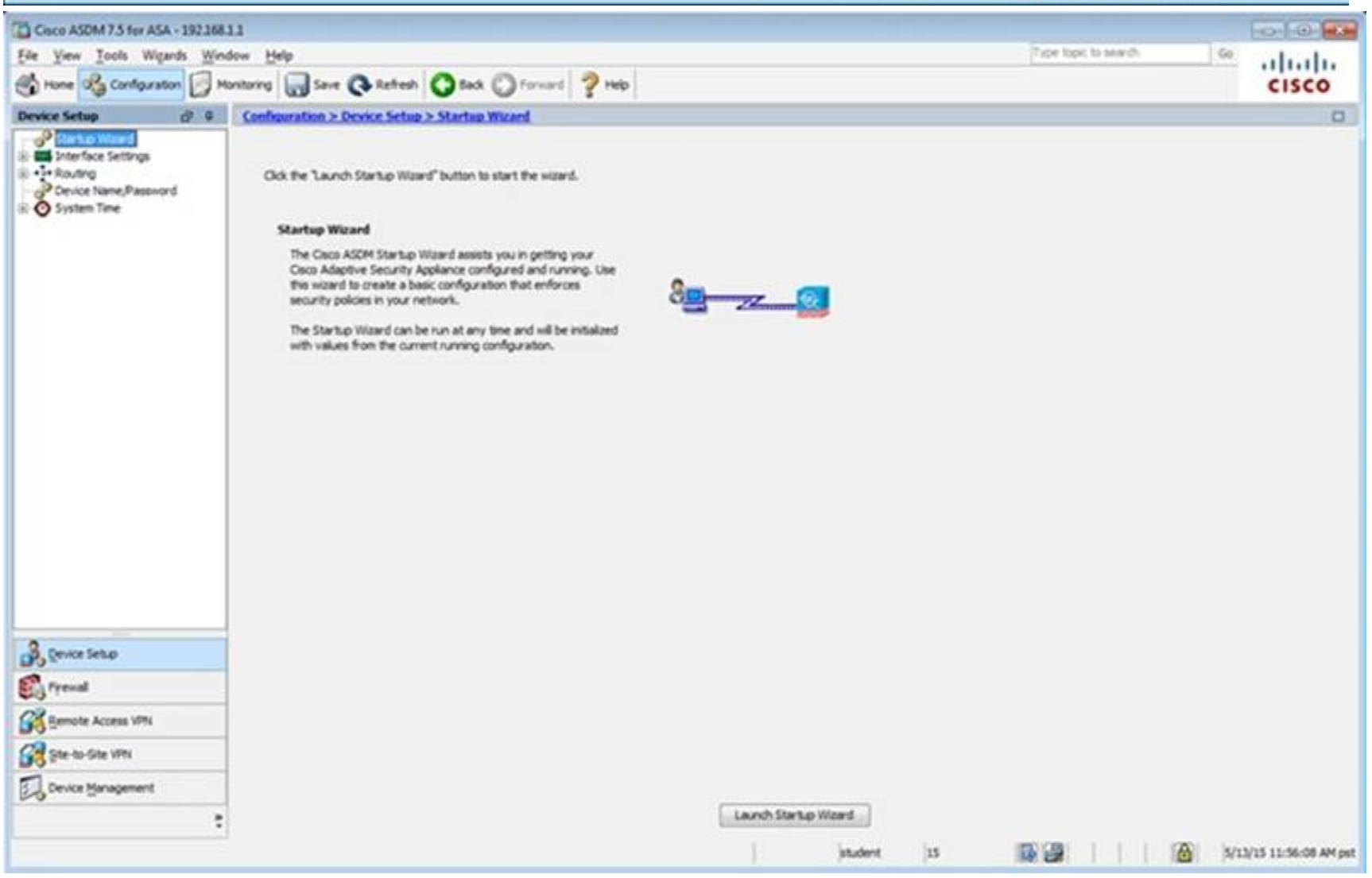
NEW QUESTION 19
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities 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.

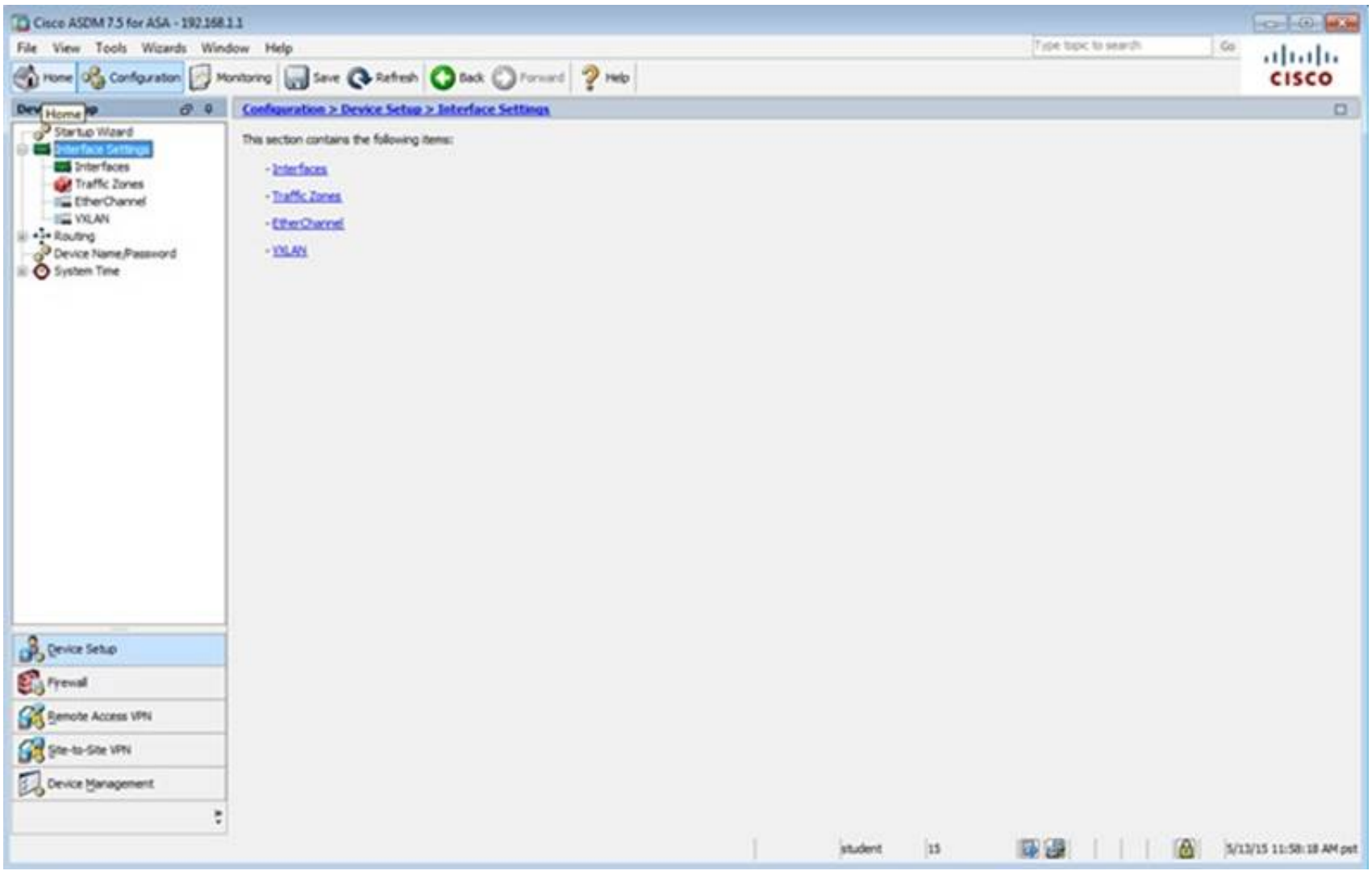


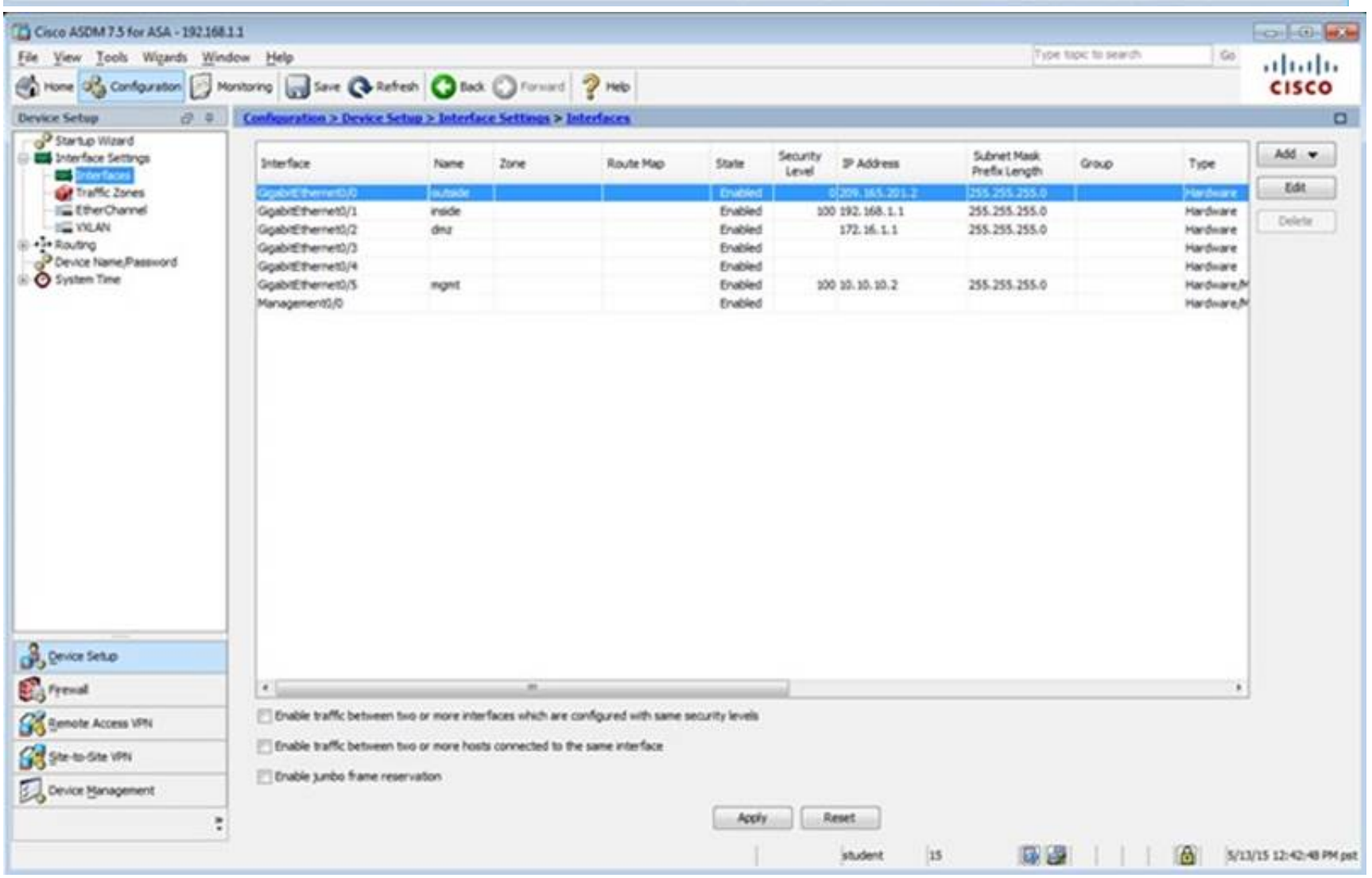

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License
Host Name: P17-ASA.secure-x.local
ASA Version: 100.14(6)13
ASDM 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
System Resources Status
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Latest ASDM Syslog Messages
Severity Date Time Syslog ID Source IP Source Destination IP Destina Description
6 May 13 2015 12:35:09 302016 10.81.254.202 123 209.165.201.2 65535 Teardown UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96
6 May 13 2015 12:35:08 106015 192.168.1.3 14676 192.168.1.1 443 Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside
6 May 13 2015 12:35:08 302014 192.168.1.3 14676 192.168.1.1 443 Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 299 TCP Reset-O
student 15
5/13/15 12:35:18 PM pst

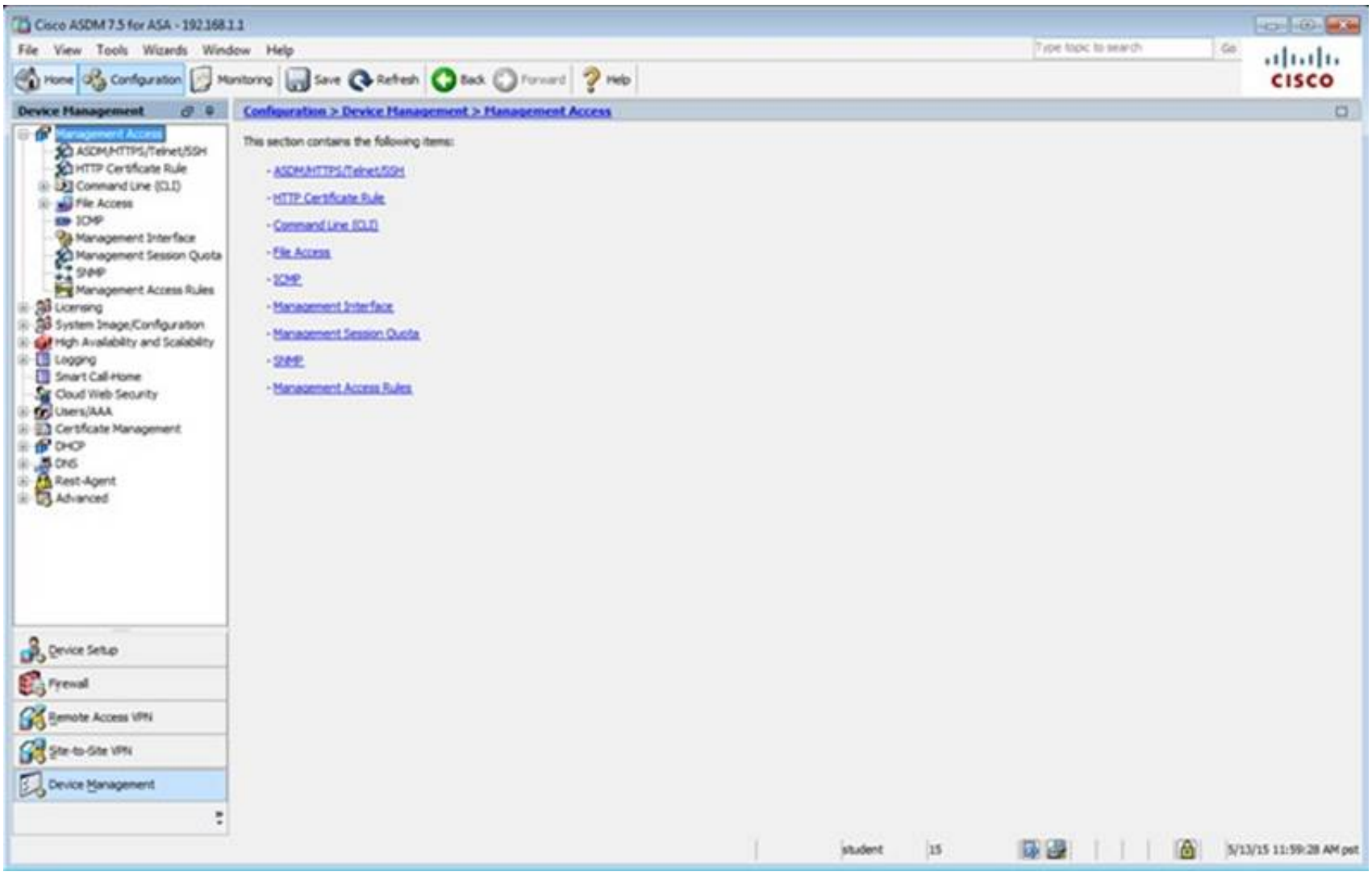

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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
Clear Dynamic ARP Entries
Refresh
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Last Updated: 5/19/15 9:32:02 AM
Data Refreshed Successfully.
student 15
5/19/15 8:32:27 AM pst

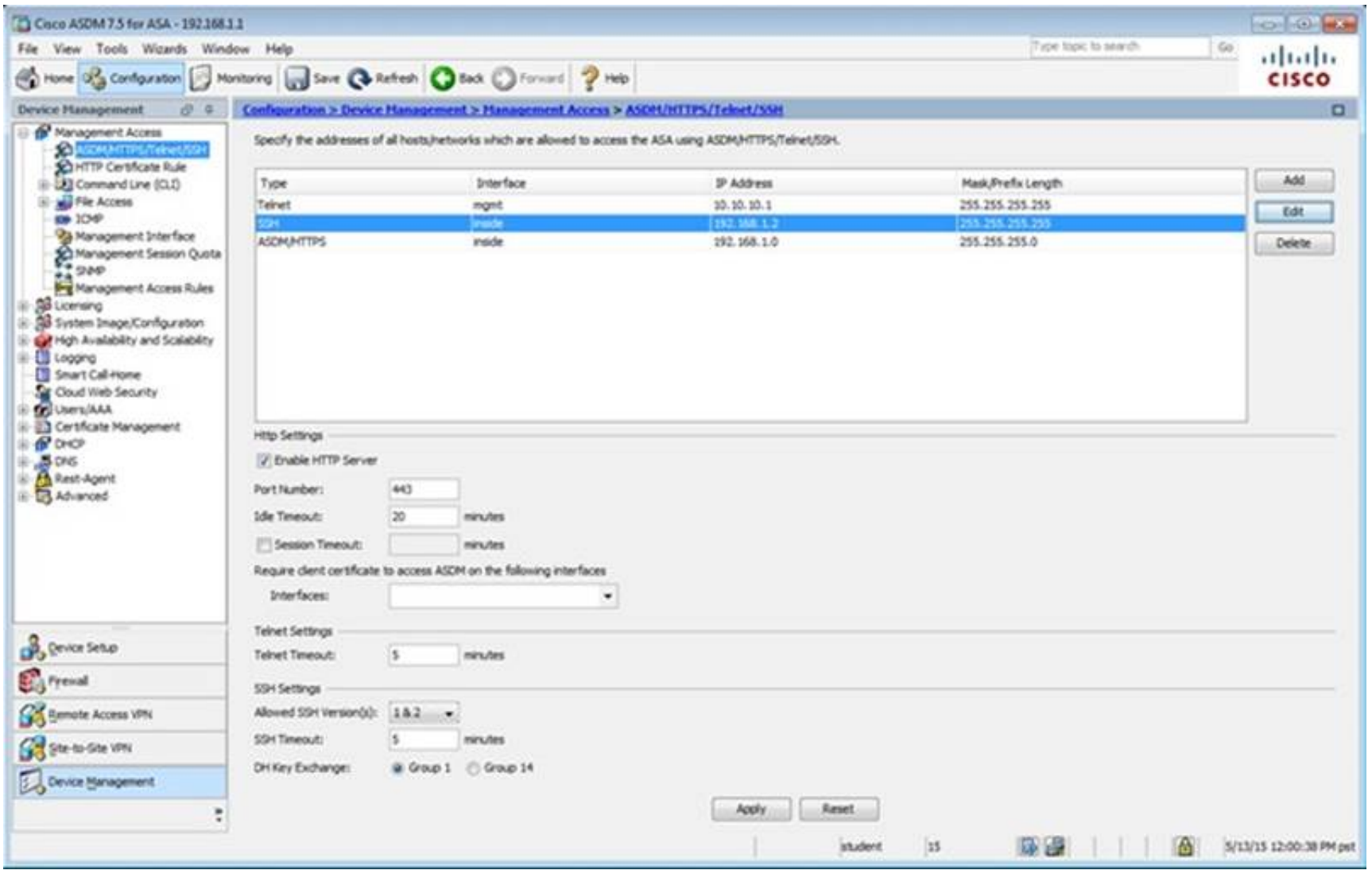

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN Mapping Sessions
MDM Proxy Statistics
MDM Proxy Sessions
Clientless SSL VPN
VPN Connection Graphs
WSA Sessions
Monitoring > VPN > VPN Statistics > Sessions
Type
Active
Cumulative
Peak Concurrent
Inactive
Clientless VPN
Browser
Filter By: Clientless SSL VPN
-- All Sessions --
Filter
Username
IP Address
Group Policy
Connection Profile
Protocol
Encryption
Login Time
Duration
Bytes Tx
Bytes Rx
student
209.165.202.131
Sales
Clientless
Clientless: (1)RC4
Details
Logout
Ping
Refresh
Last Updated: 5/19/15 9:33:12 AM
Interfaces
VPN
Botnet Traffic Filter
Routing
Properties
Logging
Data Refreshed Successfully.
student
15
5/19/15 8:33:37 AM pst

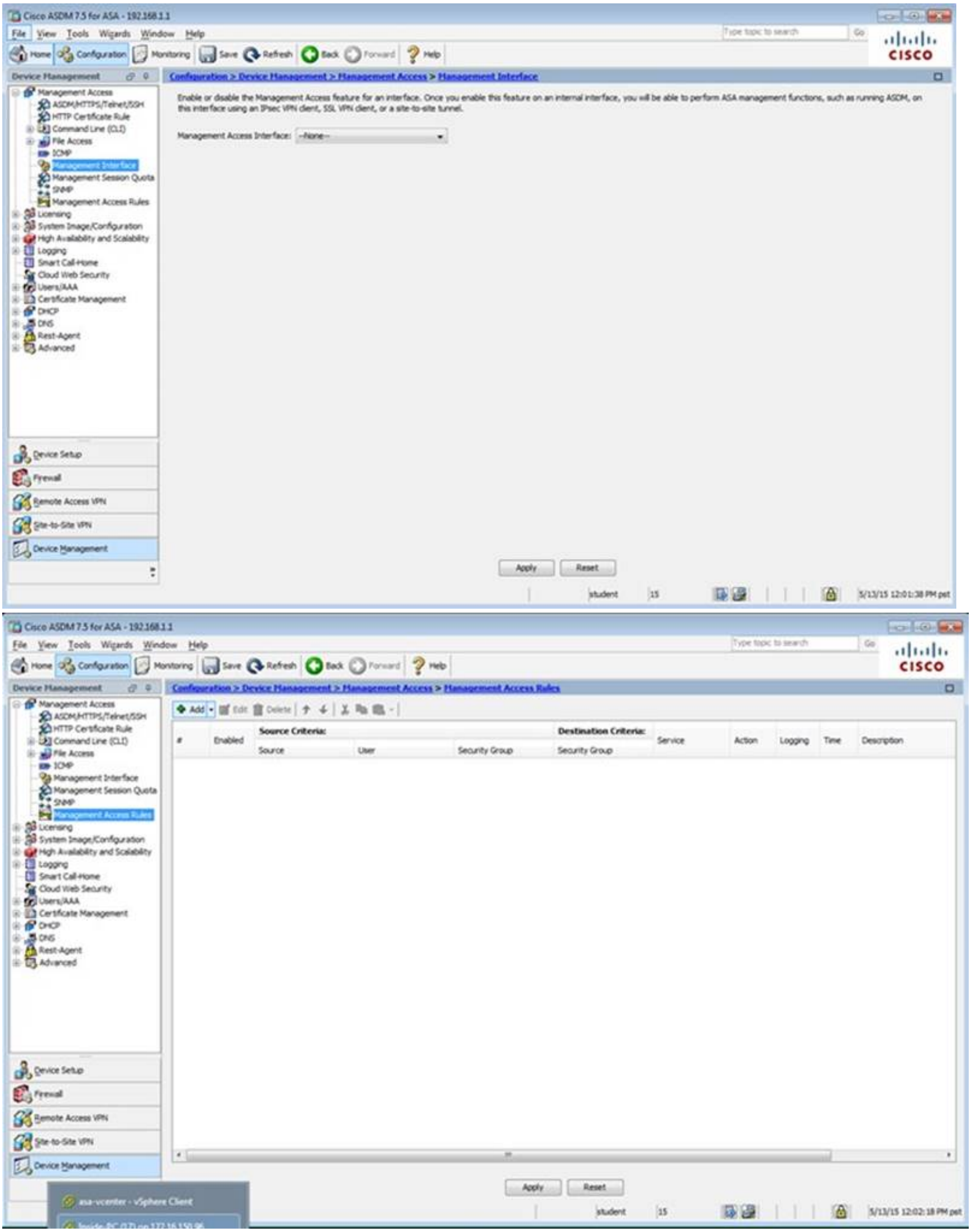

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" button to start the wizard.
Startup Wizard
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.
Launch Startup Wizard
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 11:56:08 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Device Setup > Interface Settings
This section contains the following items:
- Interfaces
- Traffic Zones
- EtherChannel
- VXLAN
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 11:58:18 AM pst

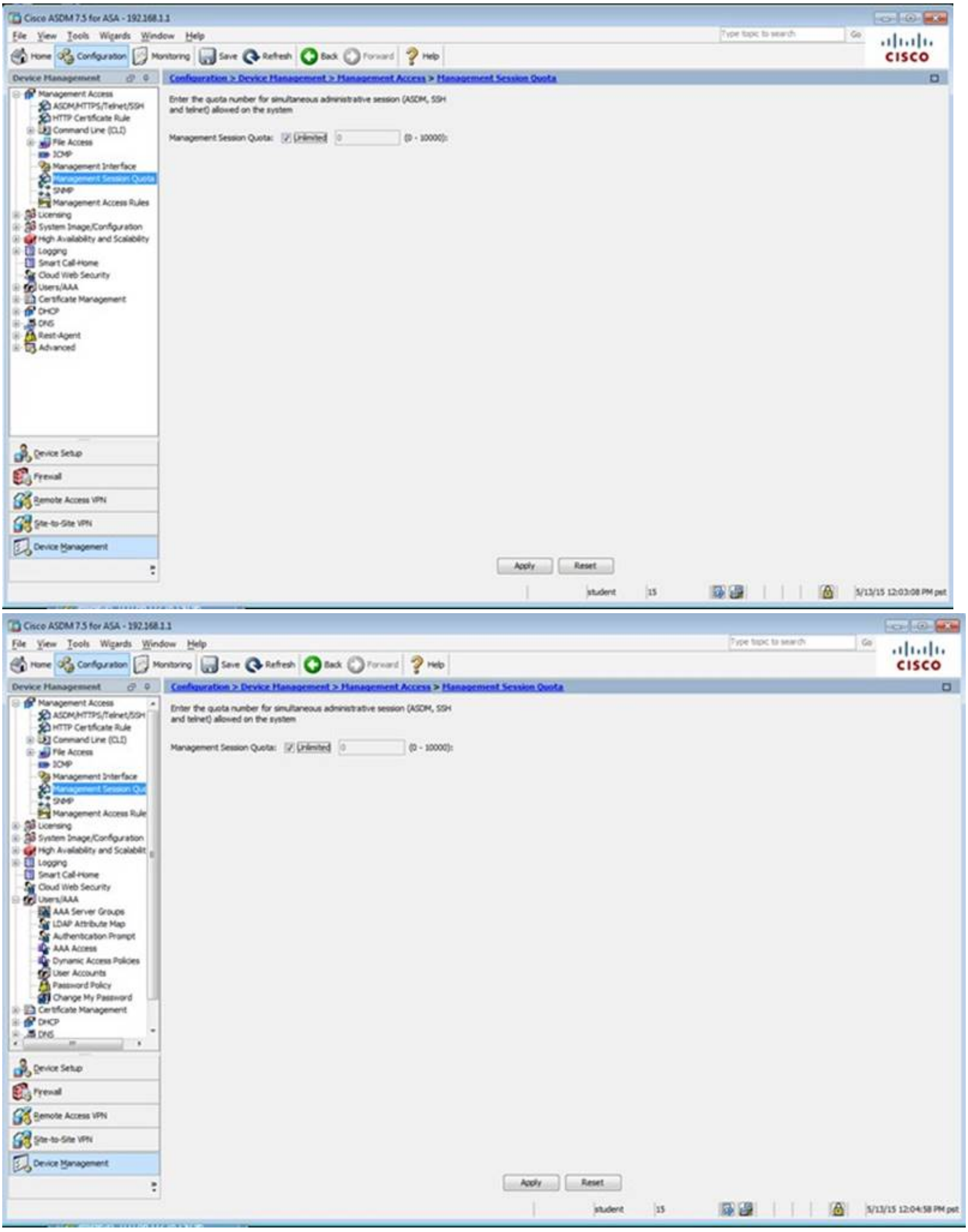

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Device Setup > Interface Settings > Interfaces
Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | 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
Add
Edit
Delete
Enable traffic between two or more interfaces which are configured with same security levels
Enable traffic between two or more hosts connected to the same interface
Enable jumbo frame reservation
Apply Reset
student 15 5/13/15 12:42:48 PM 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
CISCO
Device Management
Configuration > Device Management > Management Access
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- Management Session Quota
- SNMP
- Management Access Rules
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
student 15 5/13/15 11:59:28 AM pst

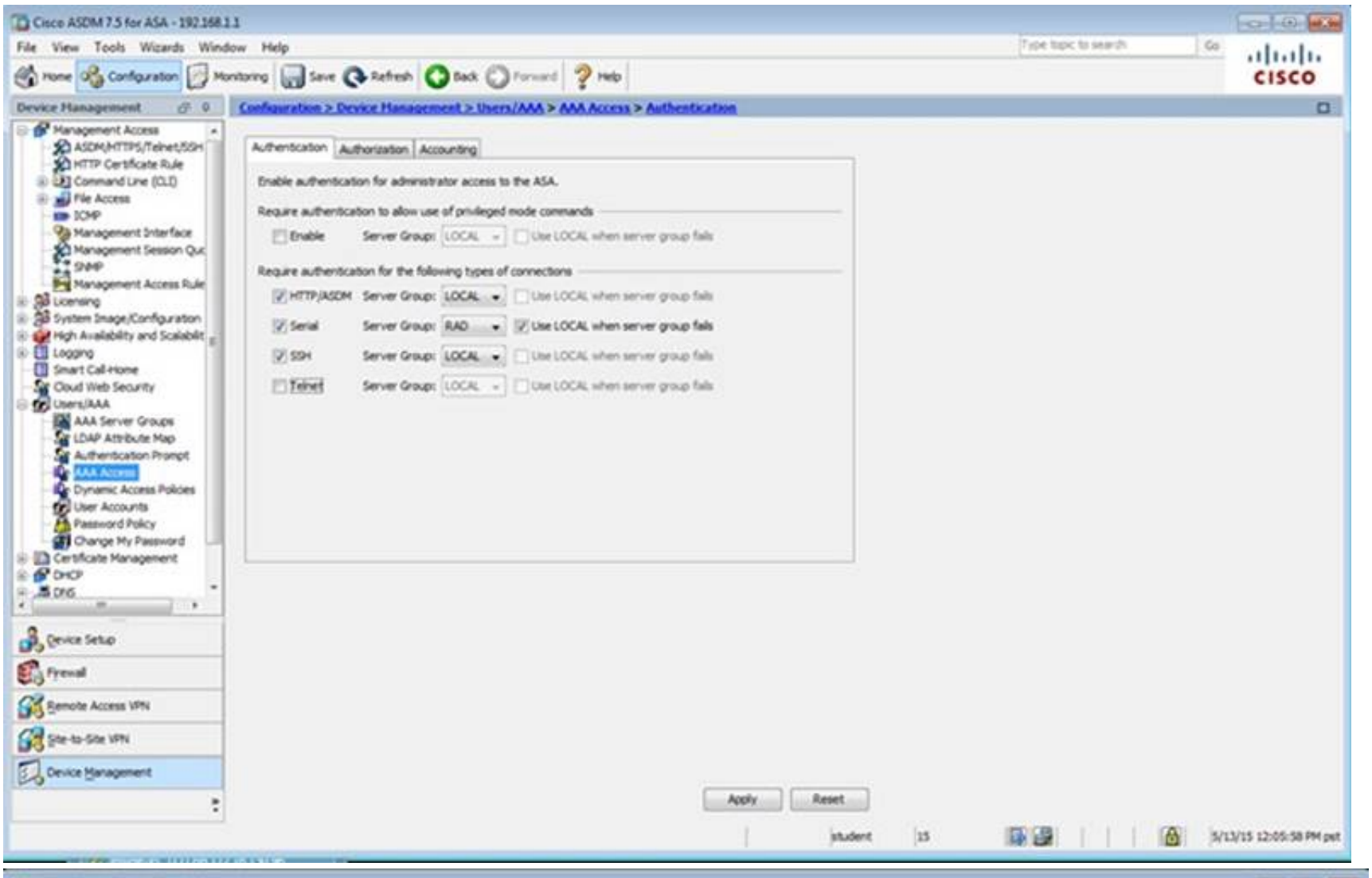

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.
Type Interface IP Address Mask/Prefix Length
Telnet mgmt 10.10.10.1 255.255.255.255
SSH inside 192.168.1.2 255.255.255.255
ASDM/HTTPS inside 192.168.1.0 255.255.255.0
Add
Edit
Delete
Http Settings
Enable HTTP Server
Port Number: 443
Idle Timeout: 20 minutes
Session Timeout: minutes
Require client certificate to access ASDM on the following interfaces
Interfaces:
Telnet Settings
Telnet Timeout: 5 minutes
SSH Settings
Allowed SSH Version(s): 1&2
SSH Timeout: 5 minutes
DH Key Exchange: Group 1 Group 14
Apply Reset
student 15 5/13/15 12:00:38 PM pst

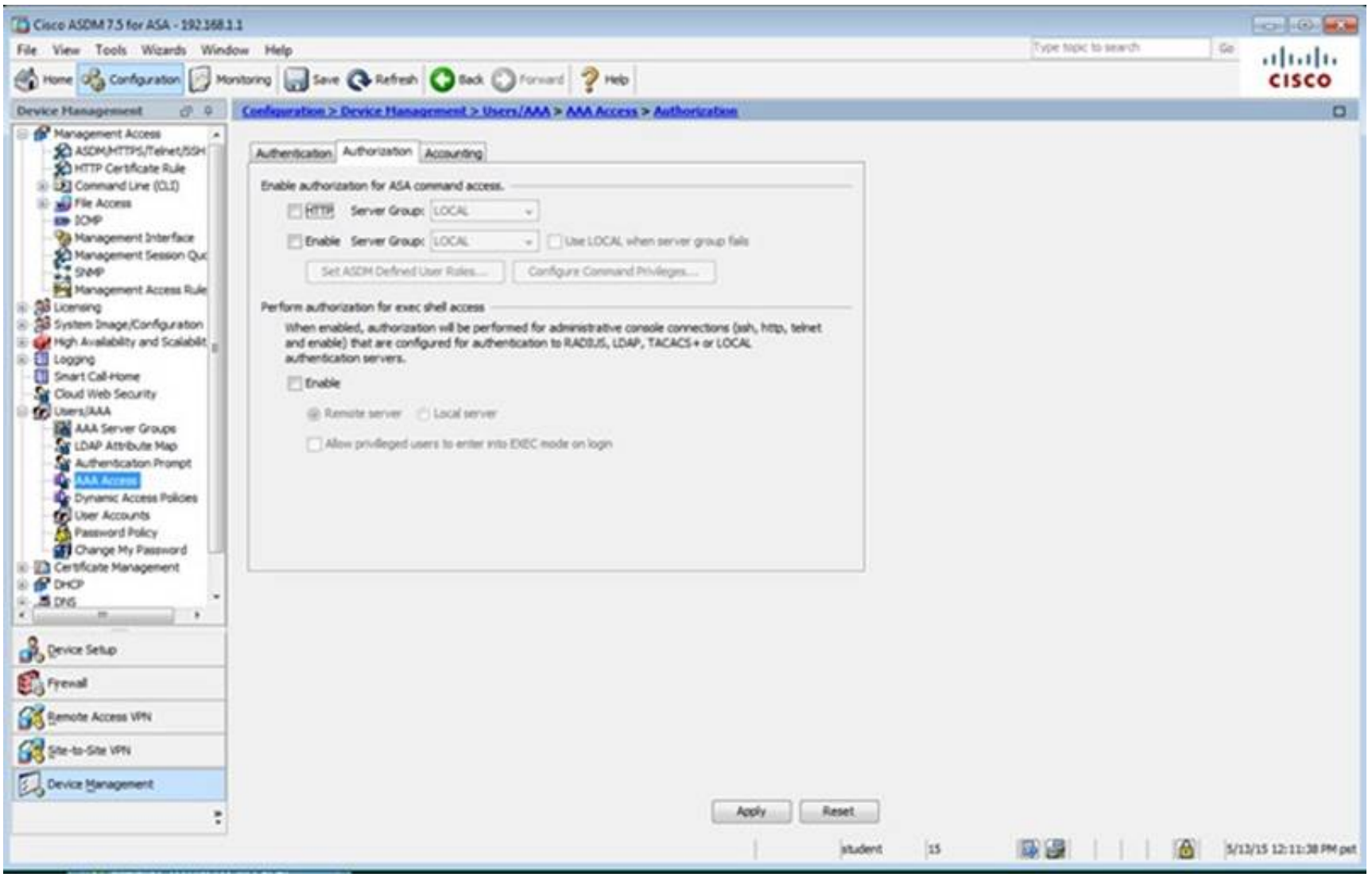

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command 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
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--
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:01:38 PM pst

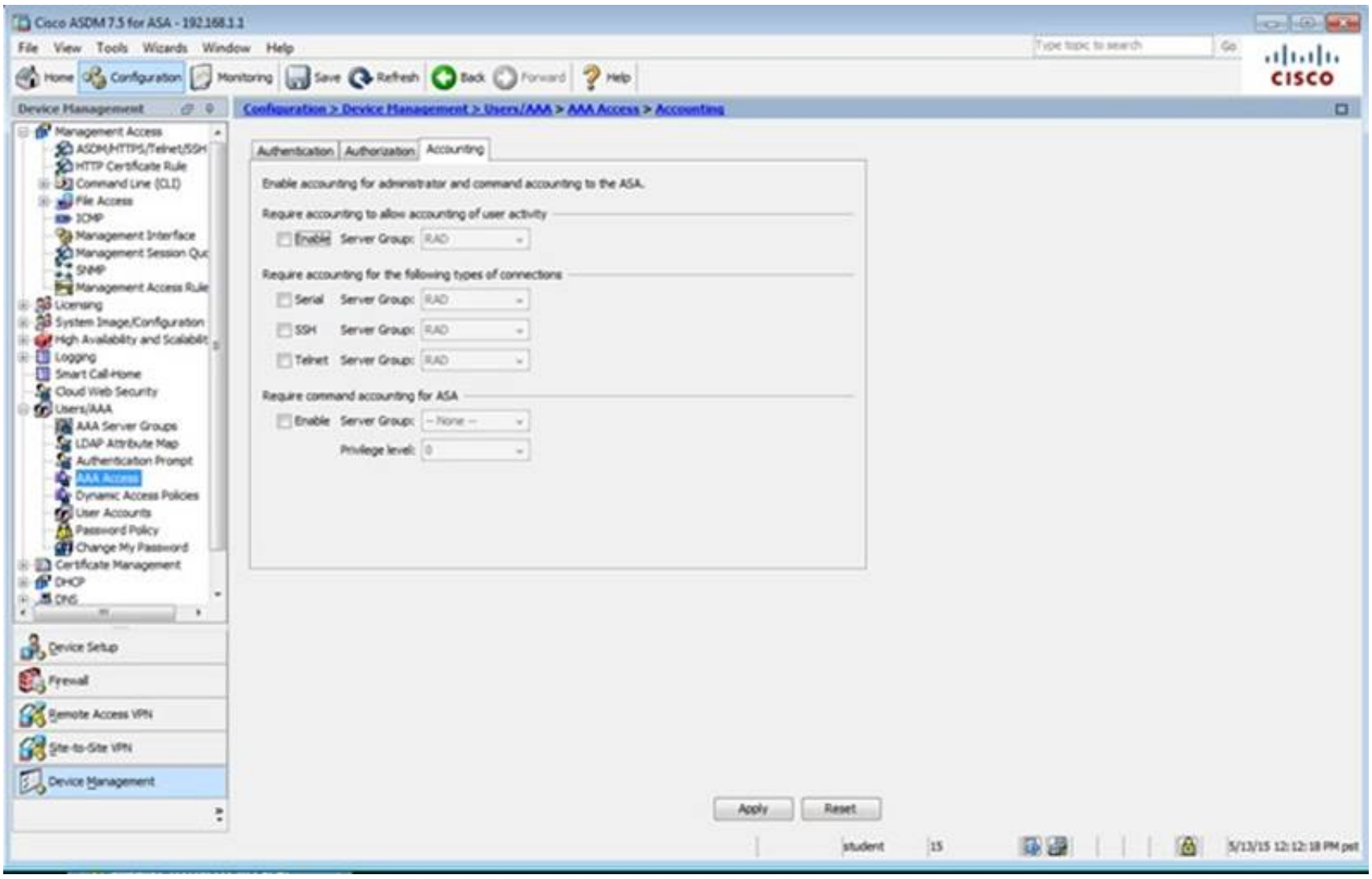
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Access Rules
Add Edit Delete
Enabled Source Criteria: Source User Security Group 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 pst

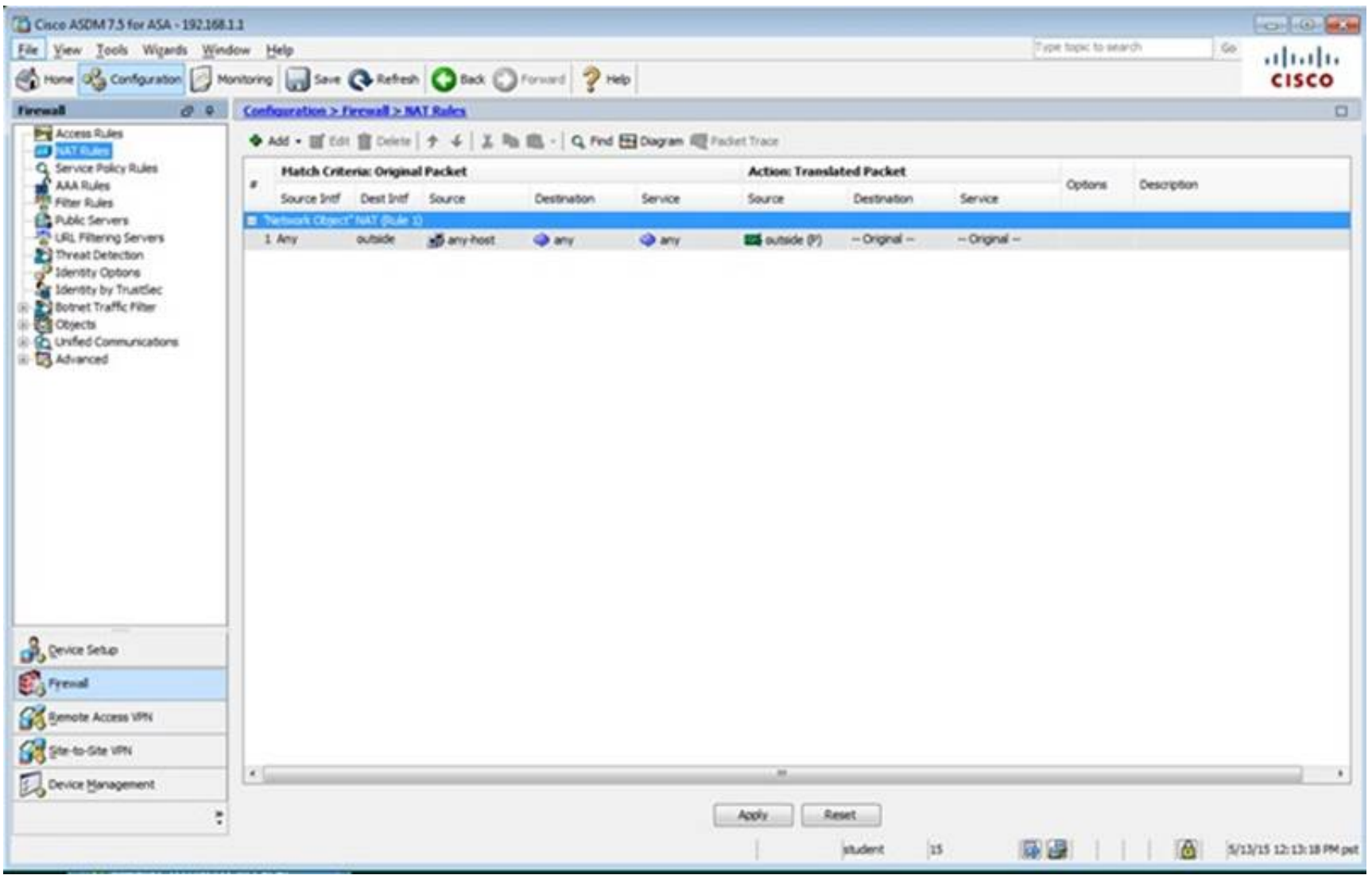

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system
Management Session Quota: Unlimited 0 (0 - 10000):
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
student 15
5/13/15 12:03:08 PM pst

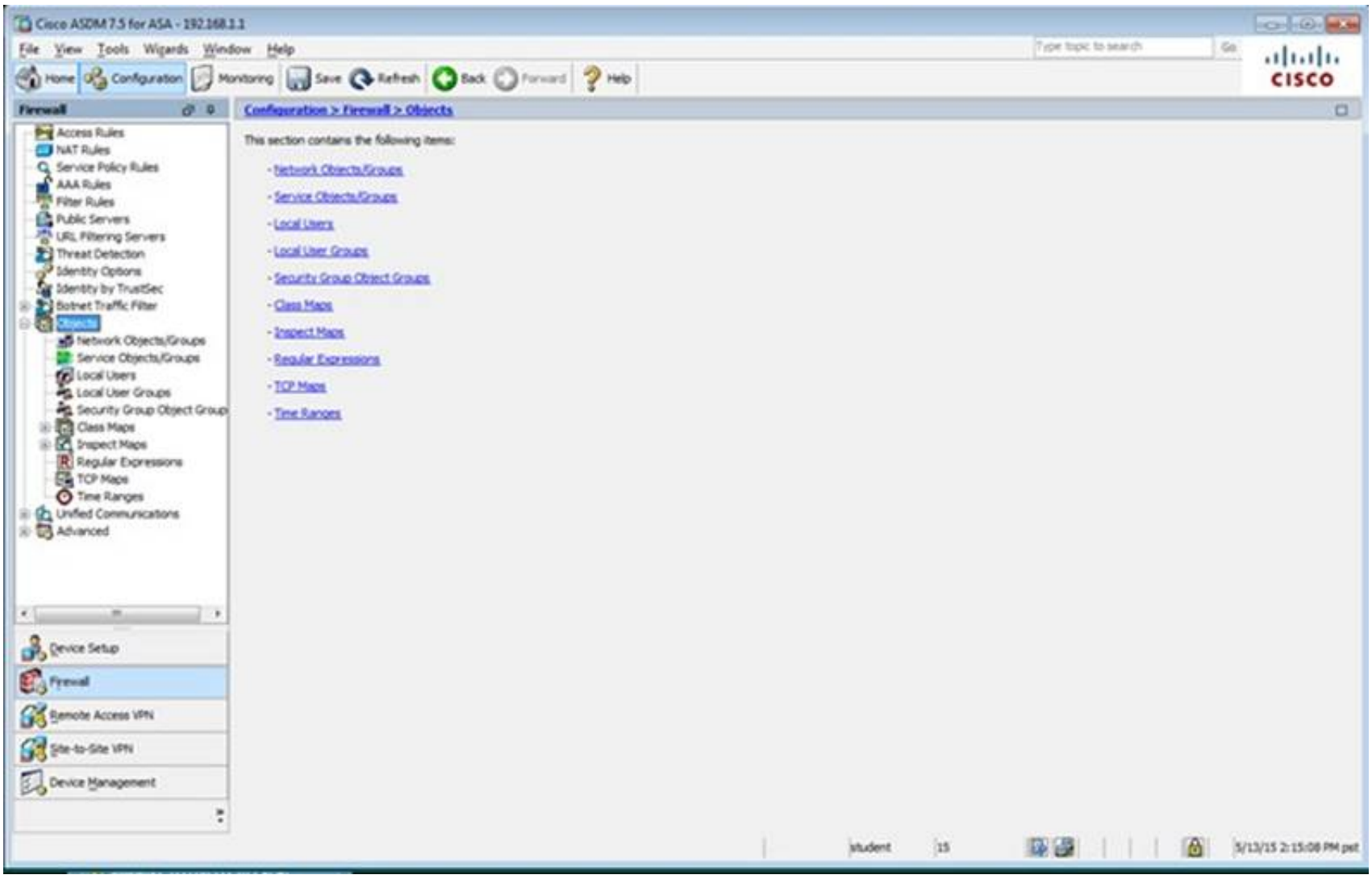
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (ASDM, SSH and telnet) allowed on the system
Management Session Quota: Unlimited 0 (0 - 10000):
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Qu
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:04:58 PM pst

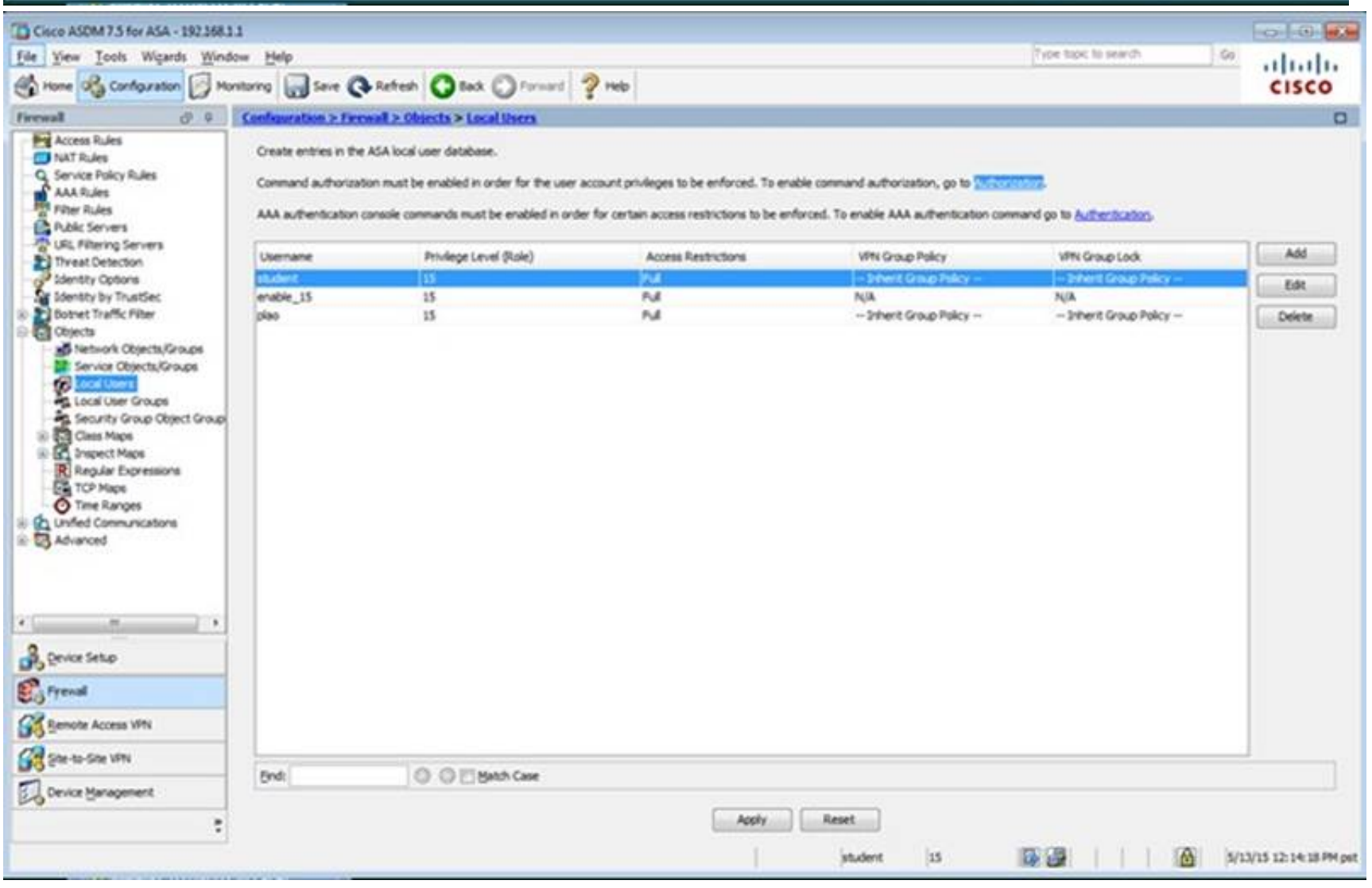

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Authorization Accounting
Enable authentication for administrator 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Qu
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabil
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:05:58 PM pst

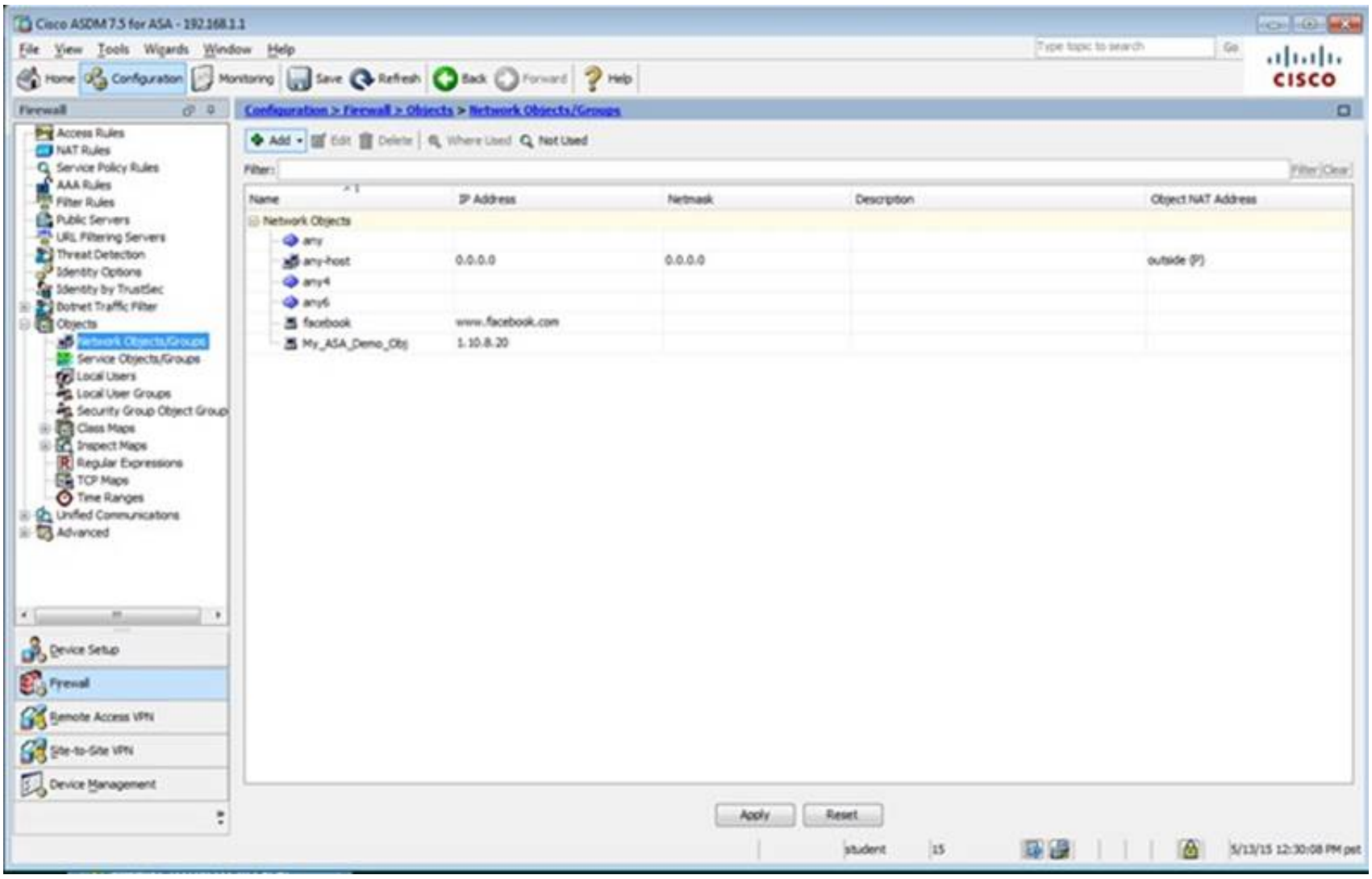

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Enable authorization for ASA 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
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Qu
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabil
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:11:38 PM pst

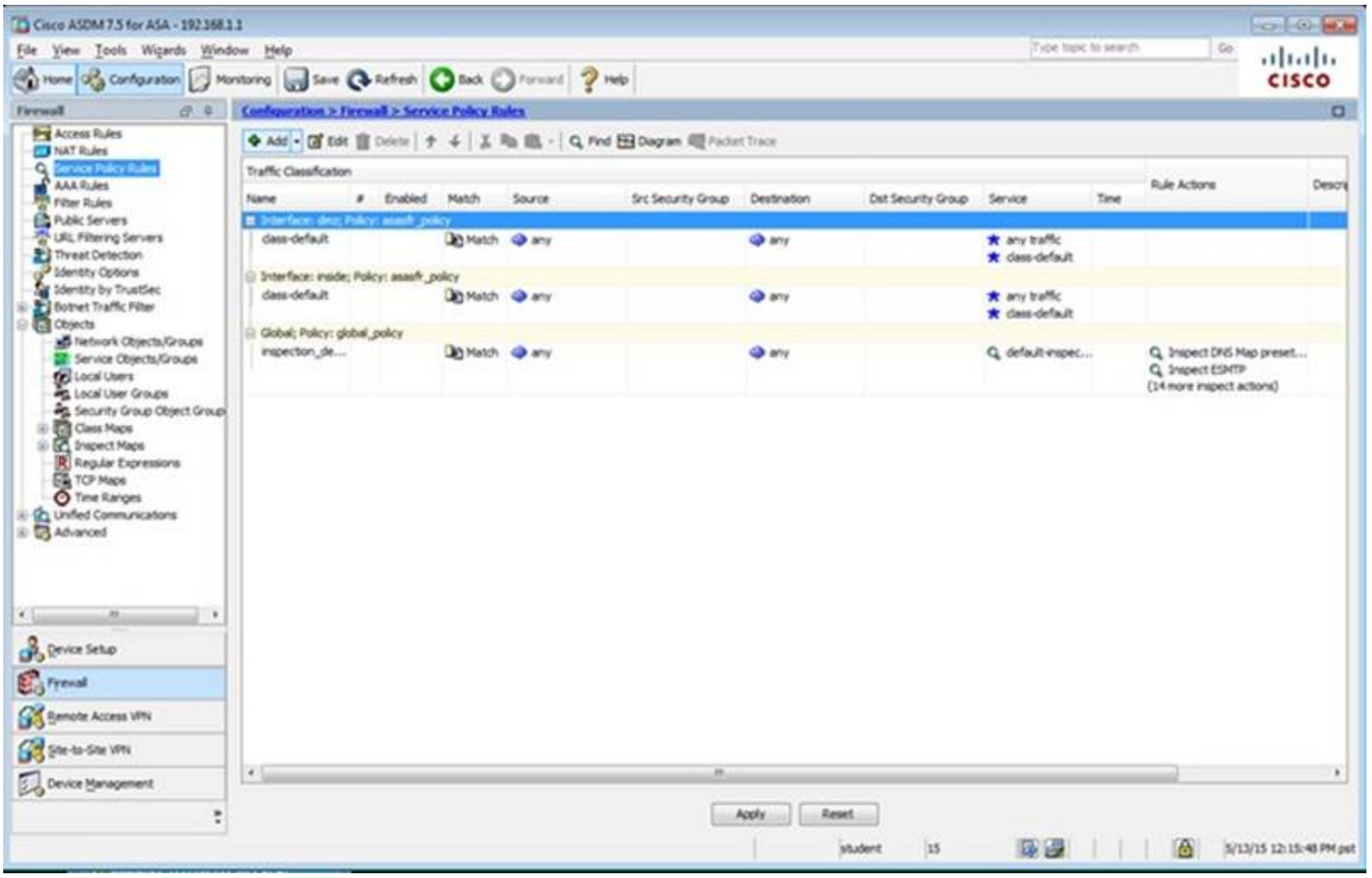

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session Qu
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Password Policy
Change My Password
Certificate Management
DHCP
DNS
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:12:18 PM pst

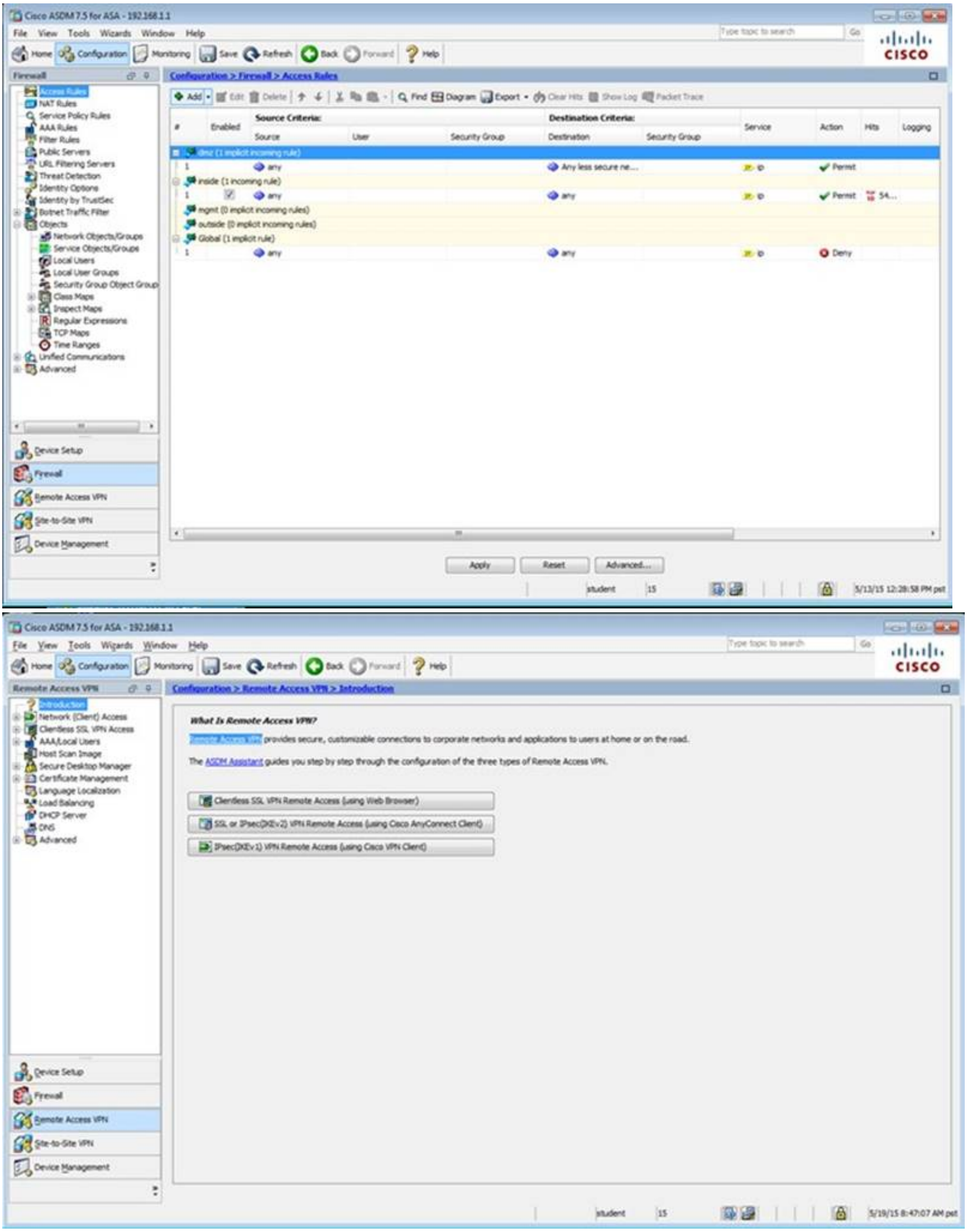

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Add Edit Delete Find Diagram Packet Trace
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 --
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:13:18 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
CISCO
Firewall
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
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/13/15 2:15:08 PM pst

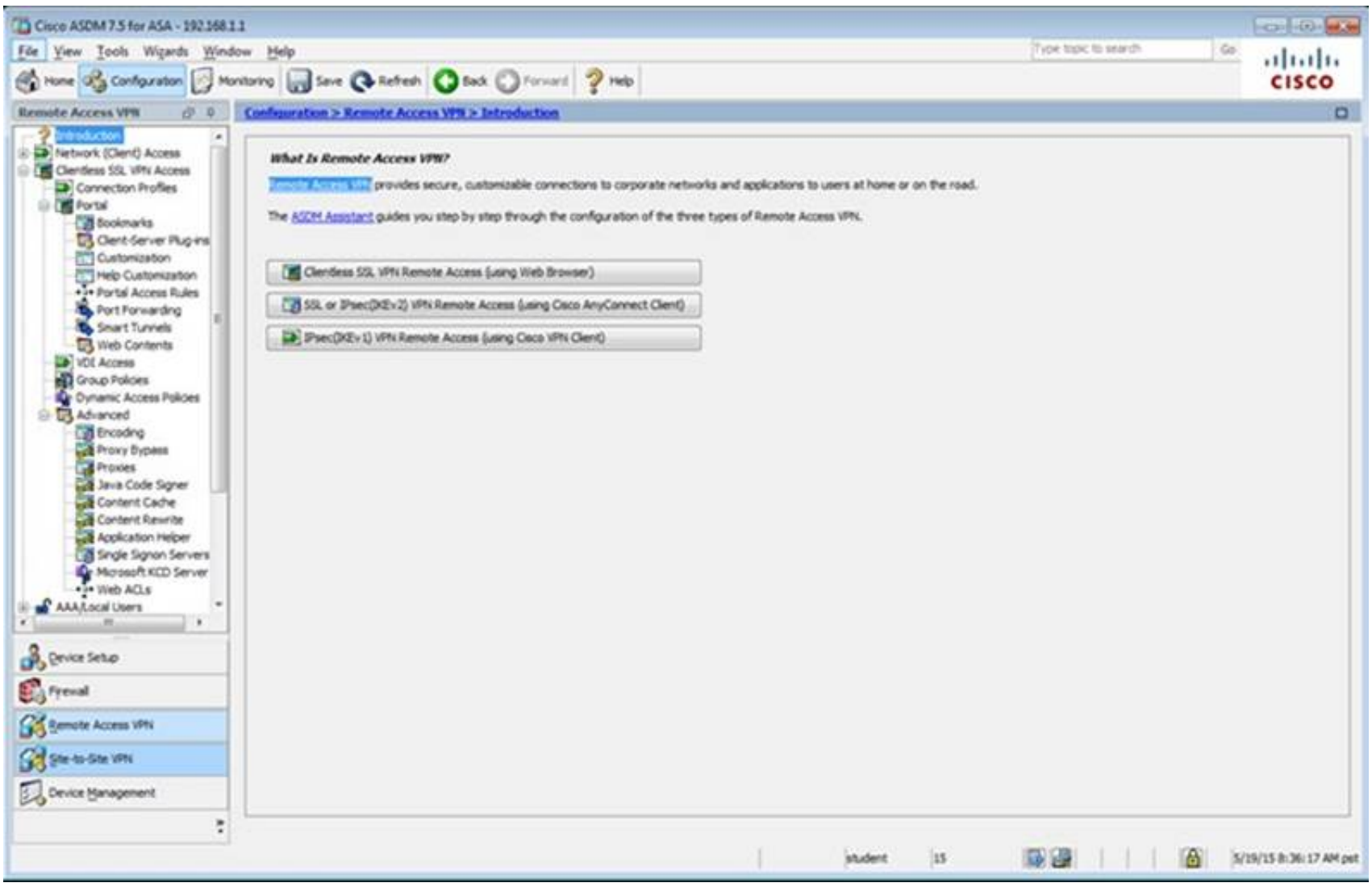

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user account 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
piao | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy --
Add
Edit
Delete
Find:
Match Case
Apply
Reset
student 15 5/13/15 12:14:18 PM pst

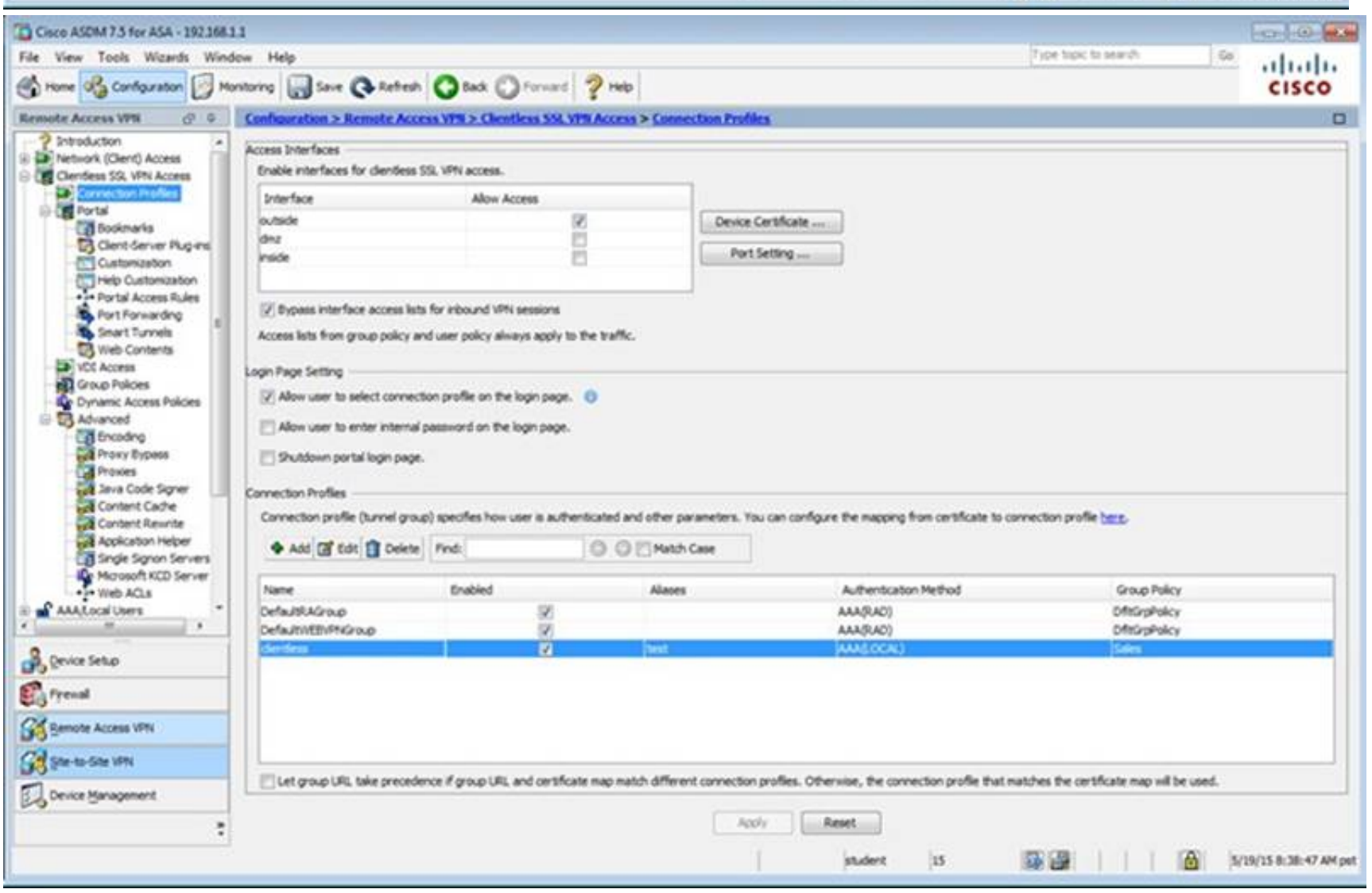

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Filter:
Name IP Address Netmask Description Object NAT Address
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
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:30:08 PM pst

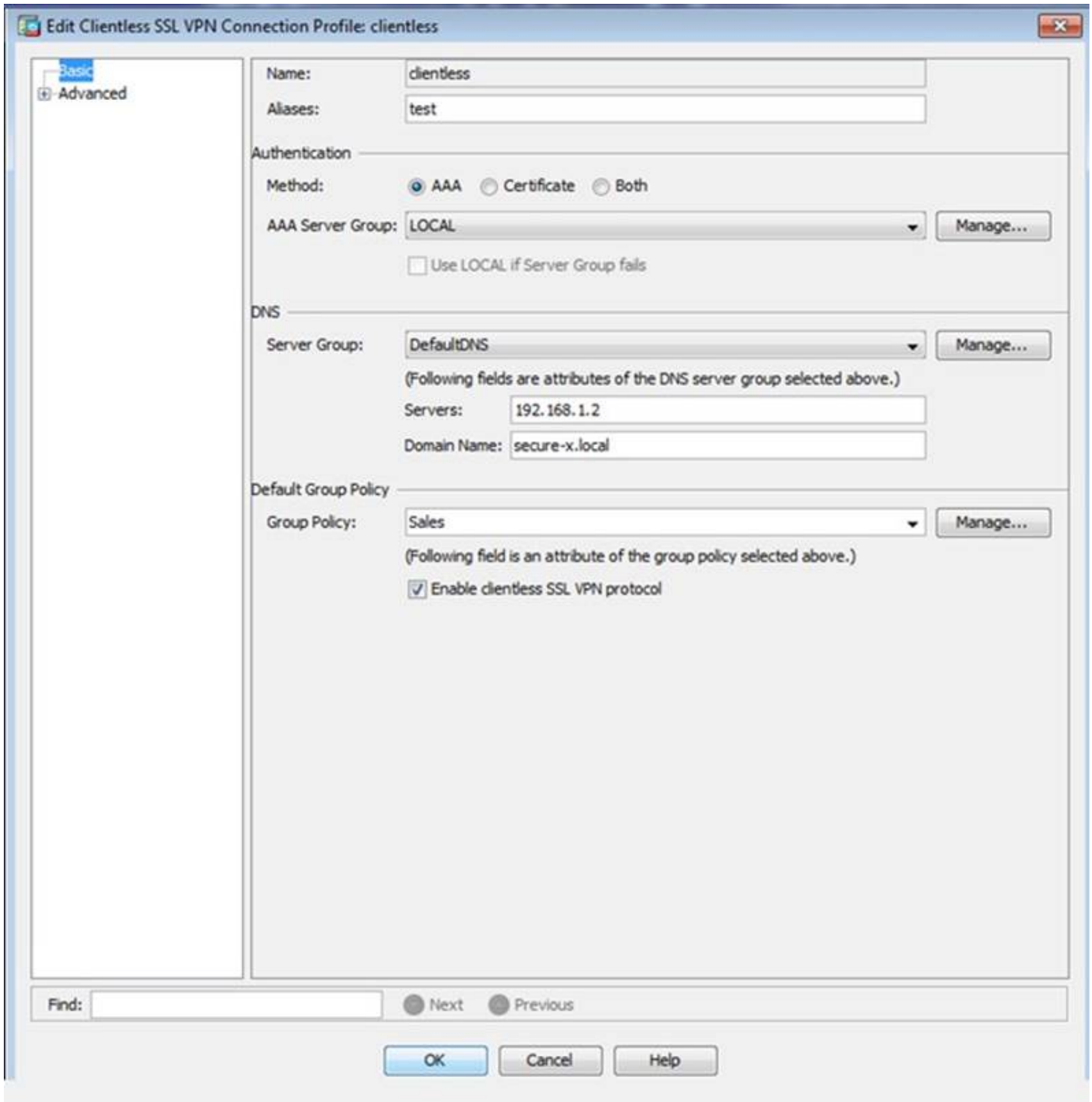

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst Security Group Service Time
Rule Actions
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)
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset
student 15
5/13/15 12:15:48 PM pst

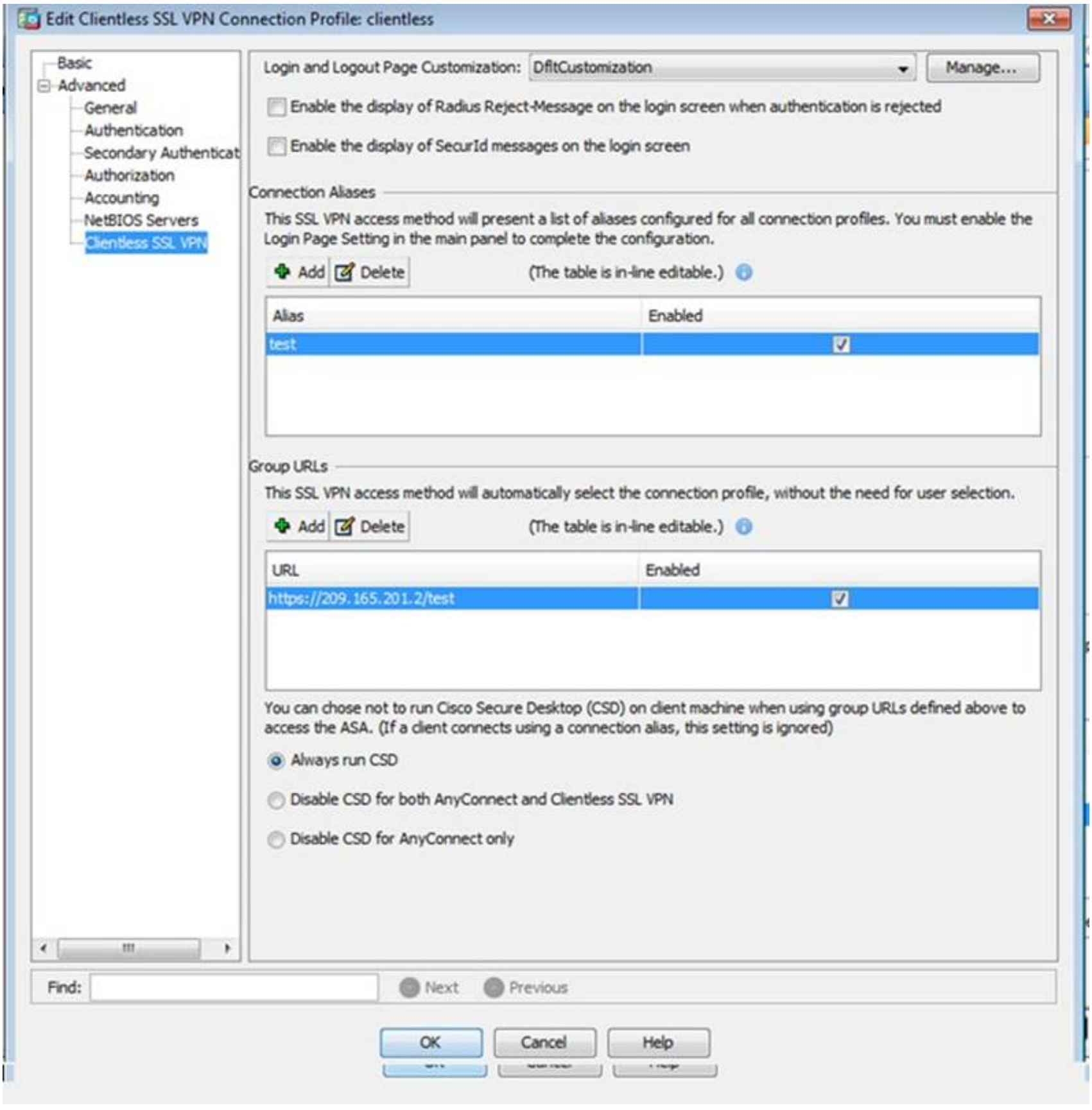

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria: Destination Criteria:
Enabled Source User Security Group Destination Security Group Service Action Hits Logging
dmz (1 implicit incoming rule)
1 any Any less secure ne... ip Permit
inside (1 incoming rule)
1 any any ip Permit
mgmt (0 implicit incoming rules)
outside (0 implicit incoming rules)
Global (1 implicit rule)
1 any any ip Deny
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Groups
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply Reset Advanced...
student 15
5/13/15 12:28:58 PM pst

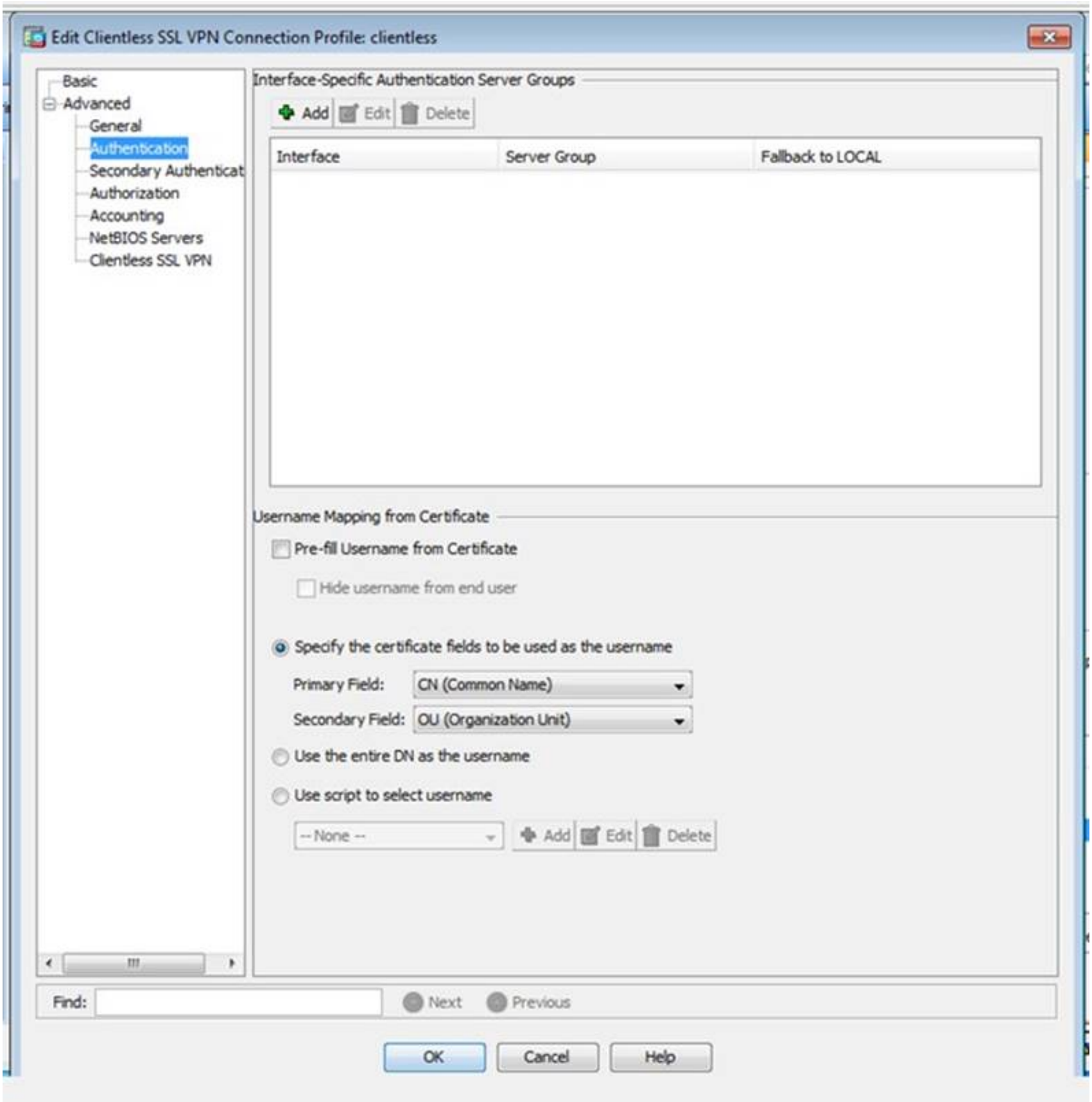
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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)
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/19/15 8:47:07 AM pst

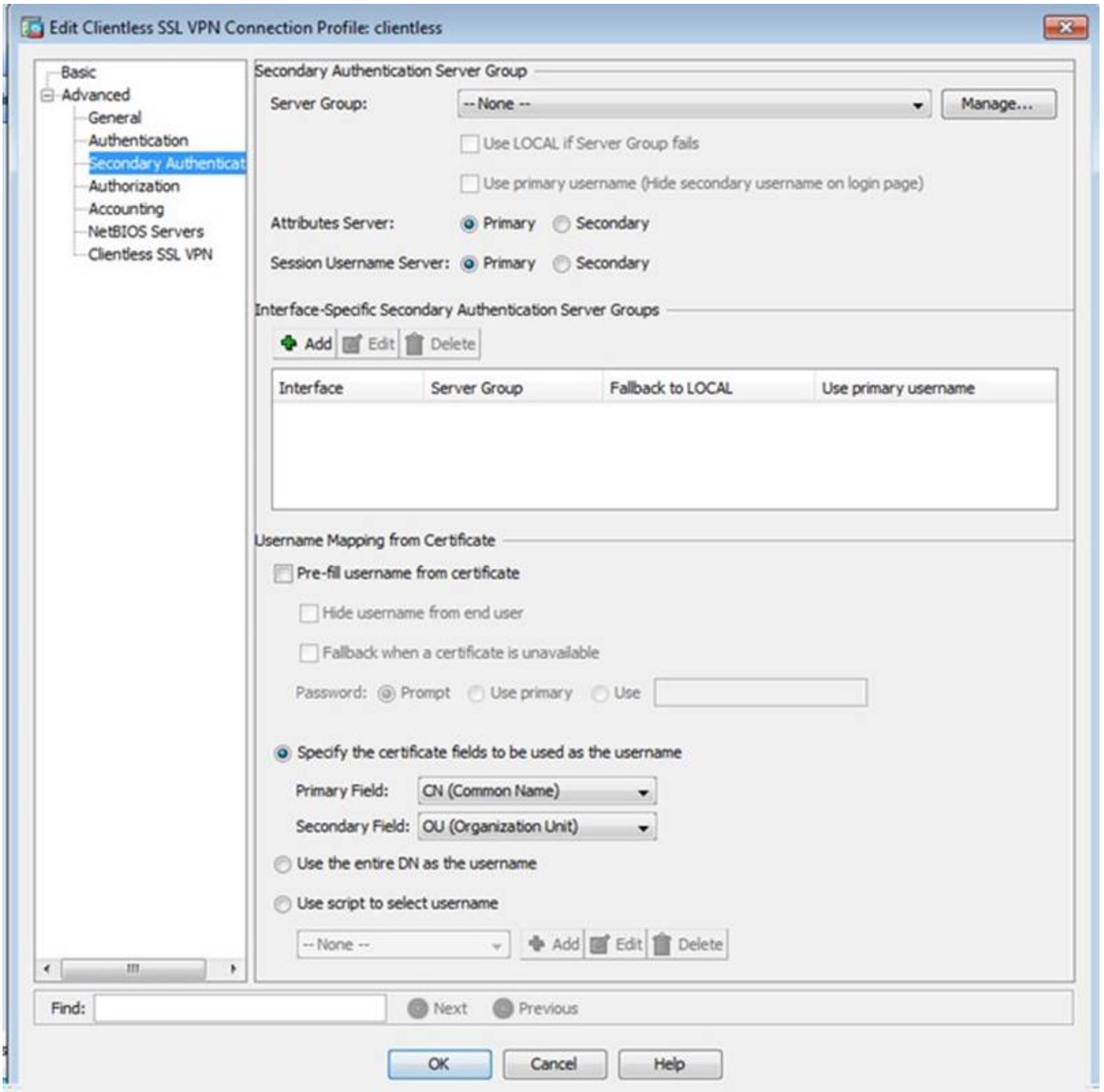

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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)
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/19/15 8:36:17 AM pst

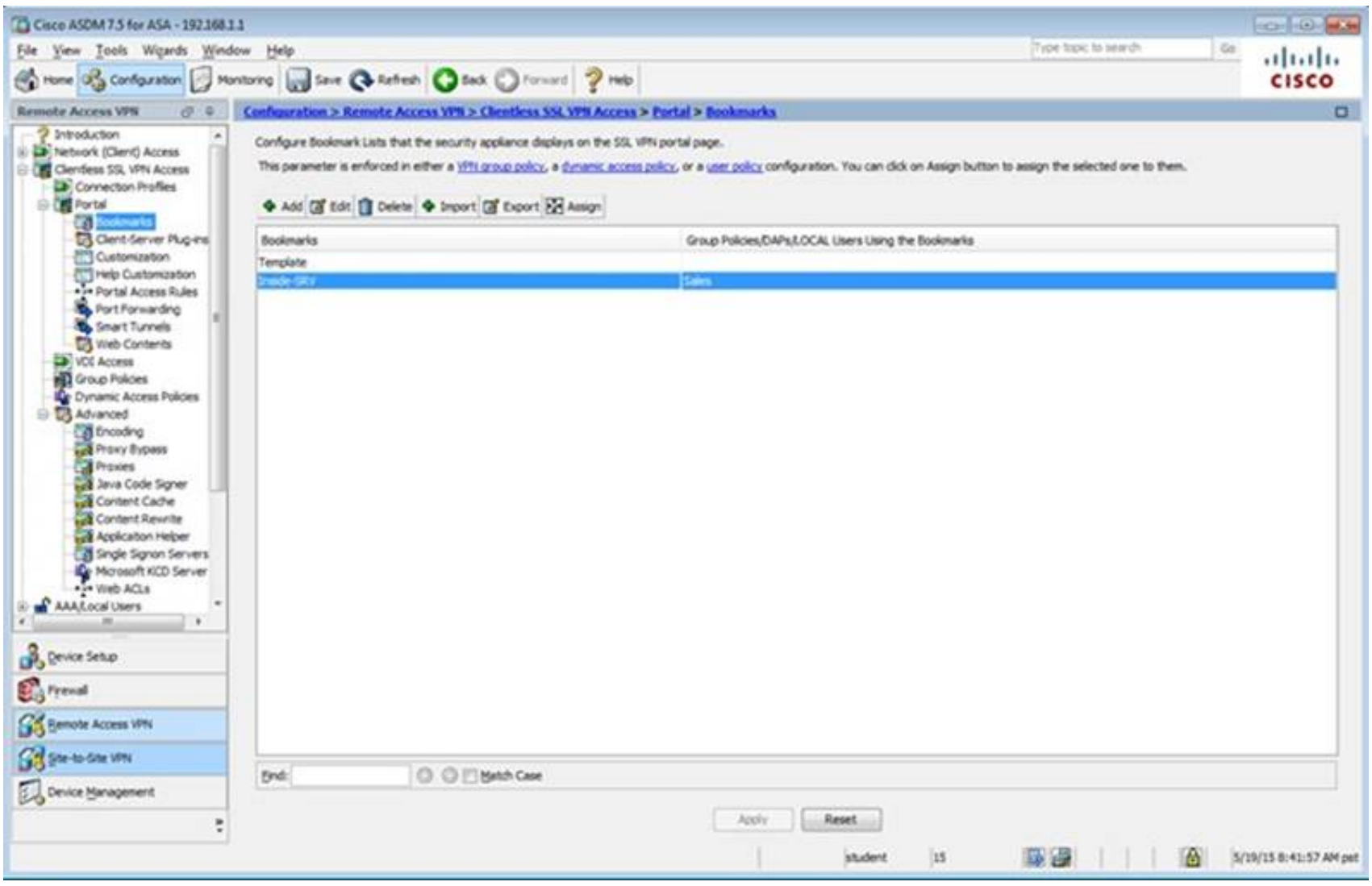

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Access Interfaces
Enable interfaces for clientless SSL VPN access.
Interface
Allow Access
outside
dmz
inside
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/19/15 8:38:47 AM pst

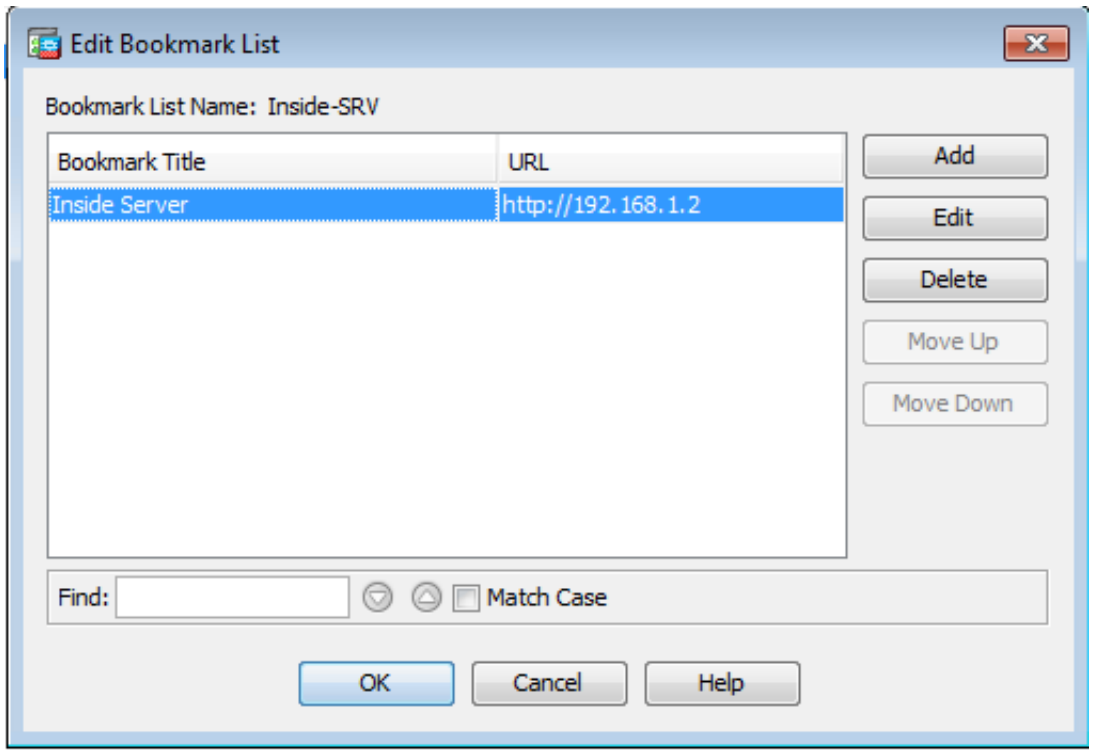

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server group selected above.)
Servers: 192.168.1.2
Domain Name: secure-x.local
Default Group Policy
Group Policy: Sales
Manage...
(Following field is an attribute of the group policy selected above.)
Enable clientless SSL VPN protocol
Find:
Next
Previous
OK
Cancel
Help

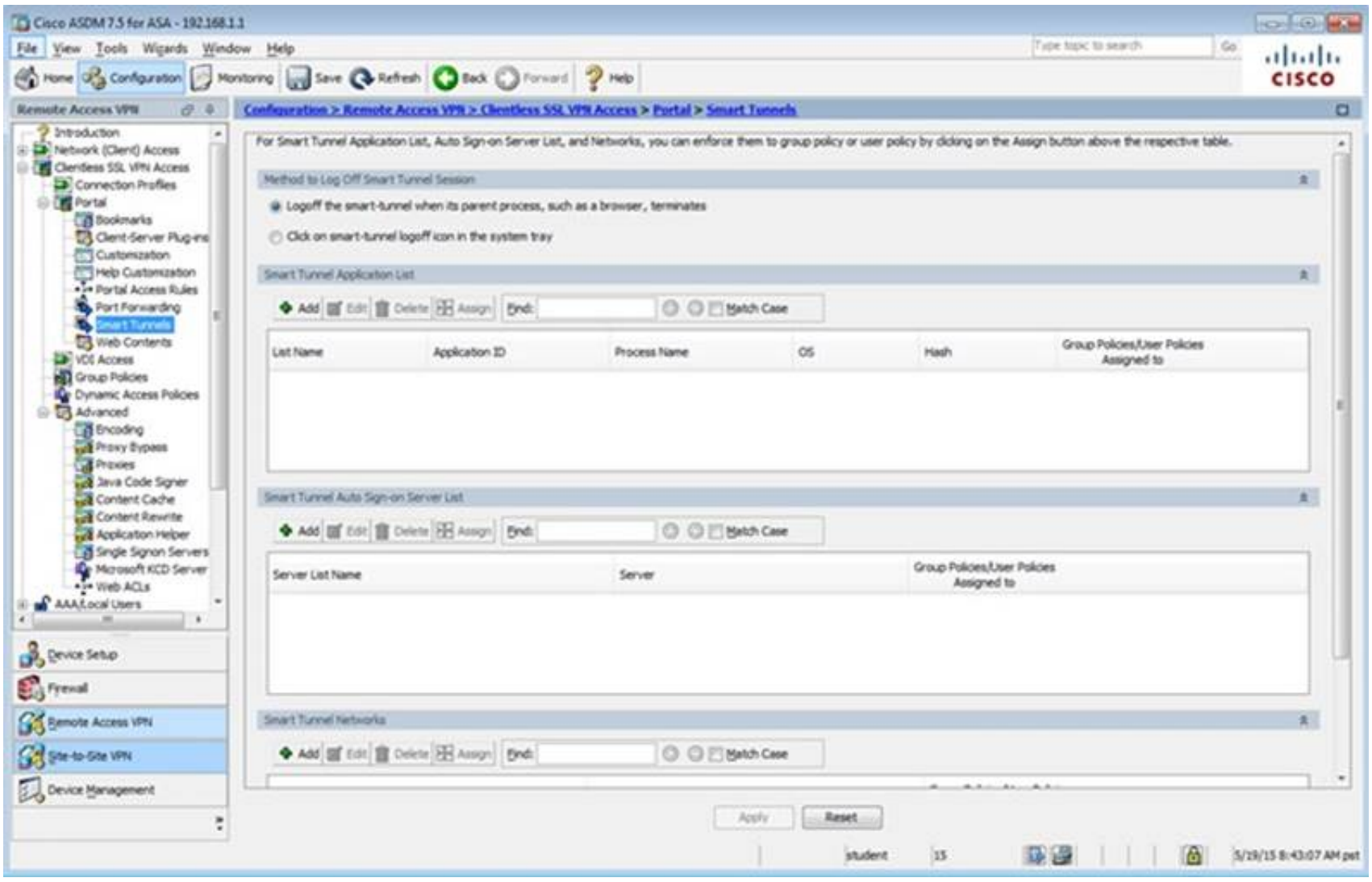

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen when authentication is rejected
Enable the display of SecurId messages on the login screen
Connection Aliases
This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.
Add
Delete
(The table is in-line editable.)
Alias
Enabled
test
Group URLs
This SSL VPN access method will automatically select the connection profile, without the need for user selection.
Add
Delete
(The table is in-line editable.)
URL
Enabled
https://209.165.201.2/test
You can chose not to run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored)
Always run CSD
Disable CSD for both AnyConnect and Clientless SSL VPN
Disable CSD for AnyConnect only
Find:
Next
Previous
OK
Cancel
Help

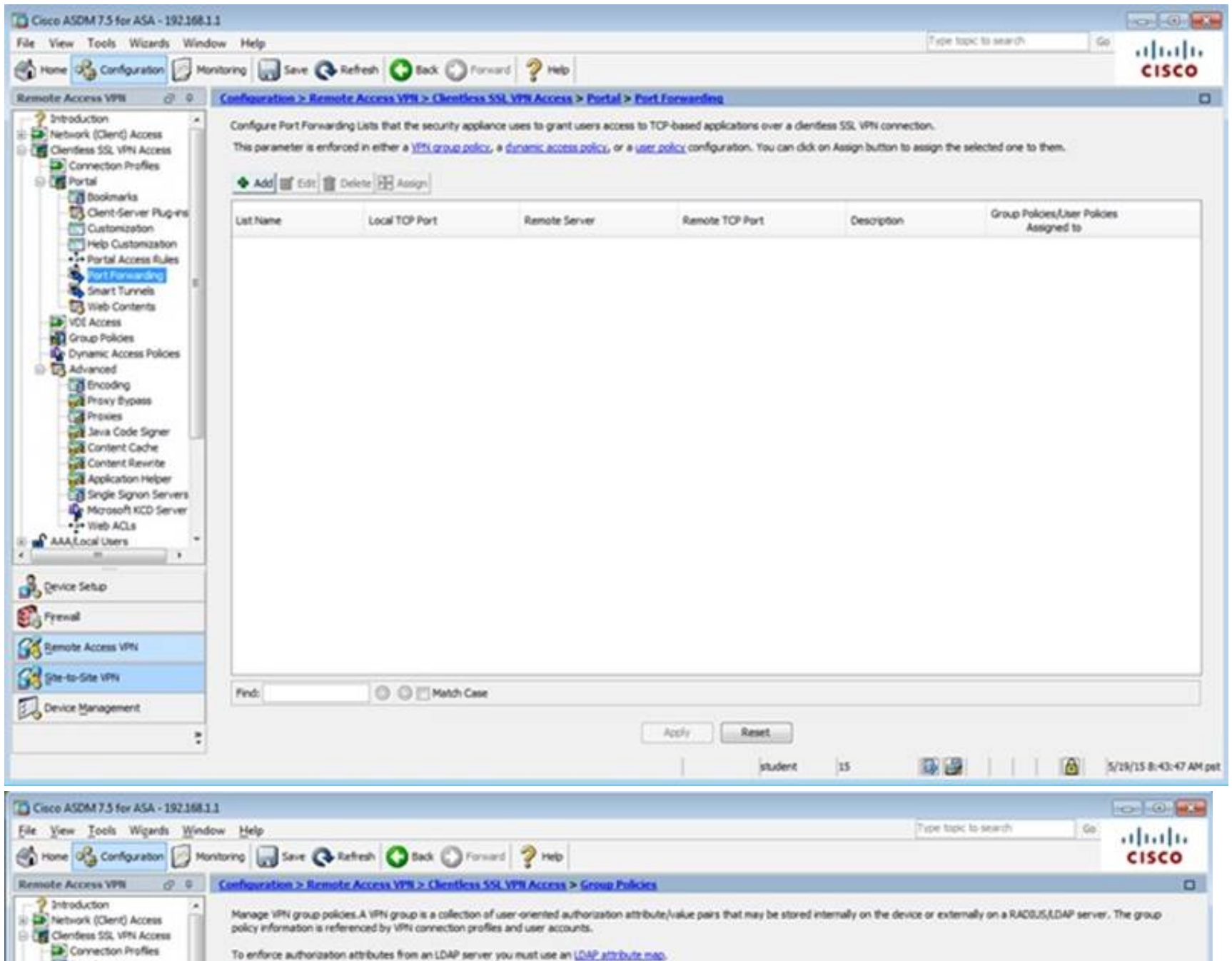

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from Certificate
Pre-fill Username from Certificate
Hide username from end user
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

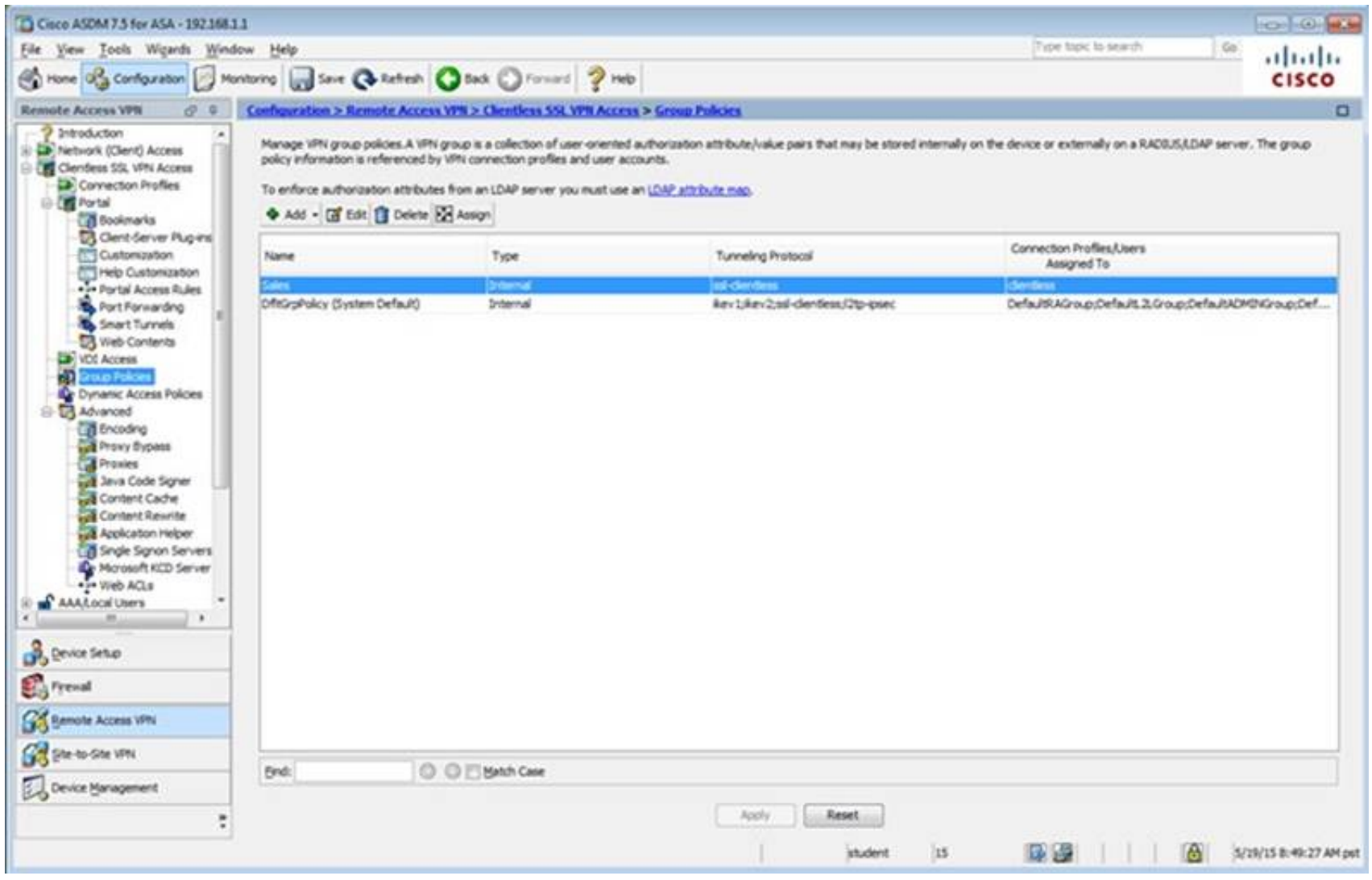

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
-- None --
Manage...
Use LOCAL if Server Group fails
Use primary username (Hide secondary username on login page)
Attributes Server:
Primary
Secondary
Session Username Server:
Primary
Secondary
Interface-Specific Secondary Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Use primary username
Username Mapping from Certificate
Pre-fill username from certificate
Hide username from end user
Fallback when a certificate is unavailable
Password:
Prompt
Use primary
Use
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username
-- None --
Add
Edit
Delete
Find:
Next
Previous
OK
Cancel
Help

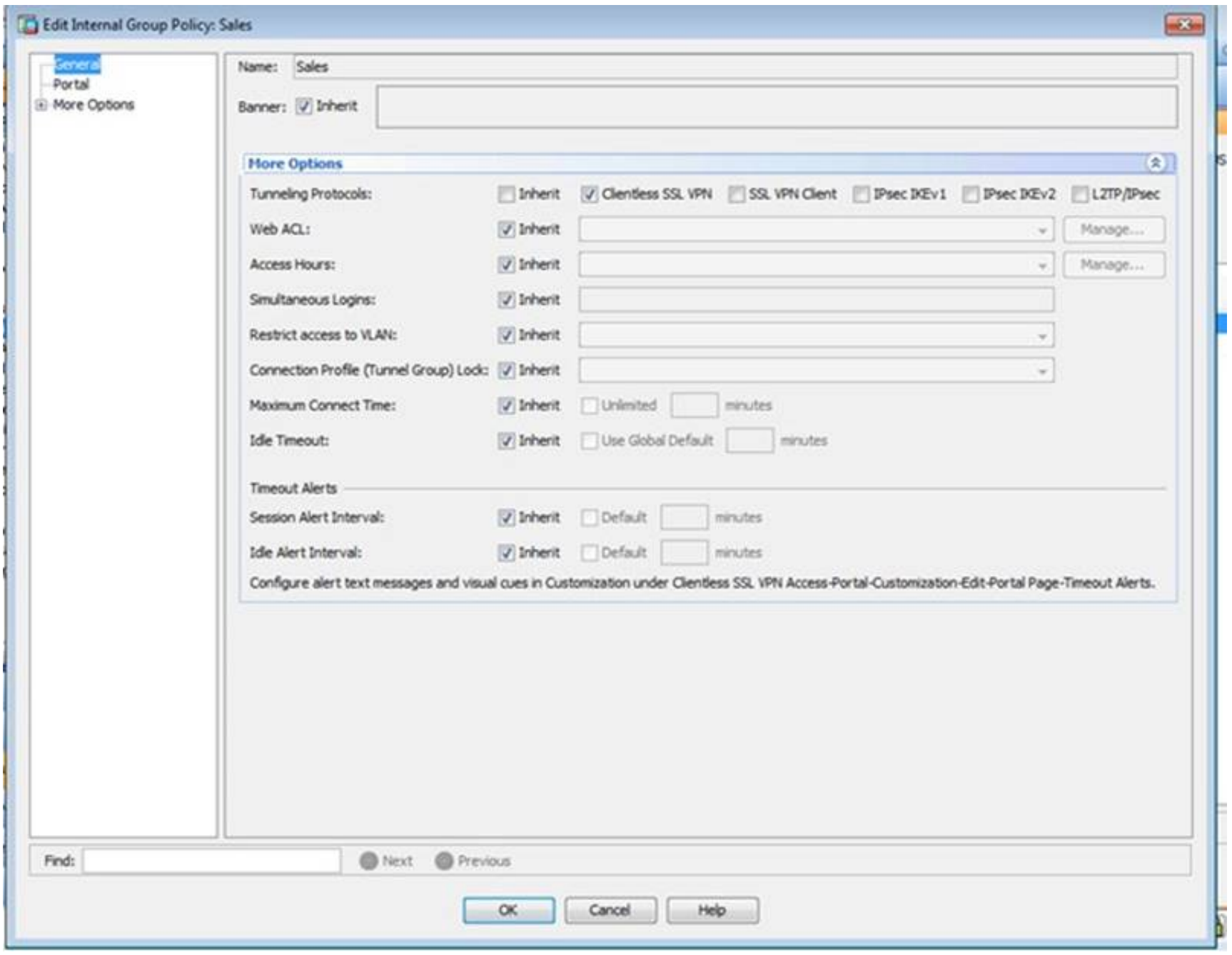

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add
Edit
Delete
Import
Export
Assign
Bookmarks
Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:41:57 AM pst

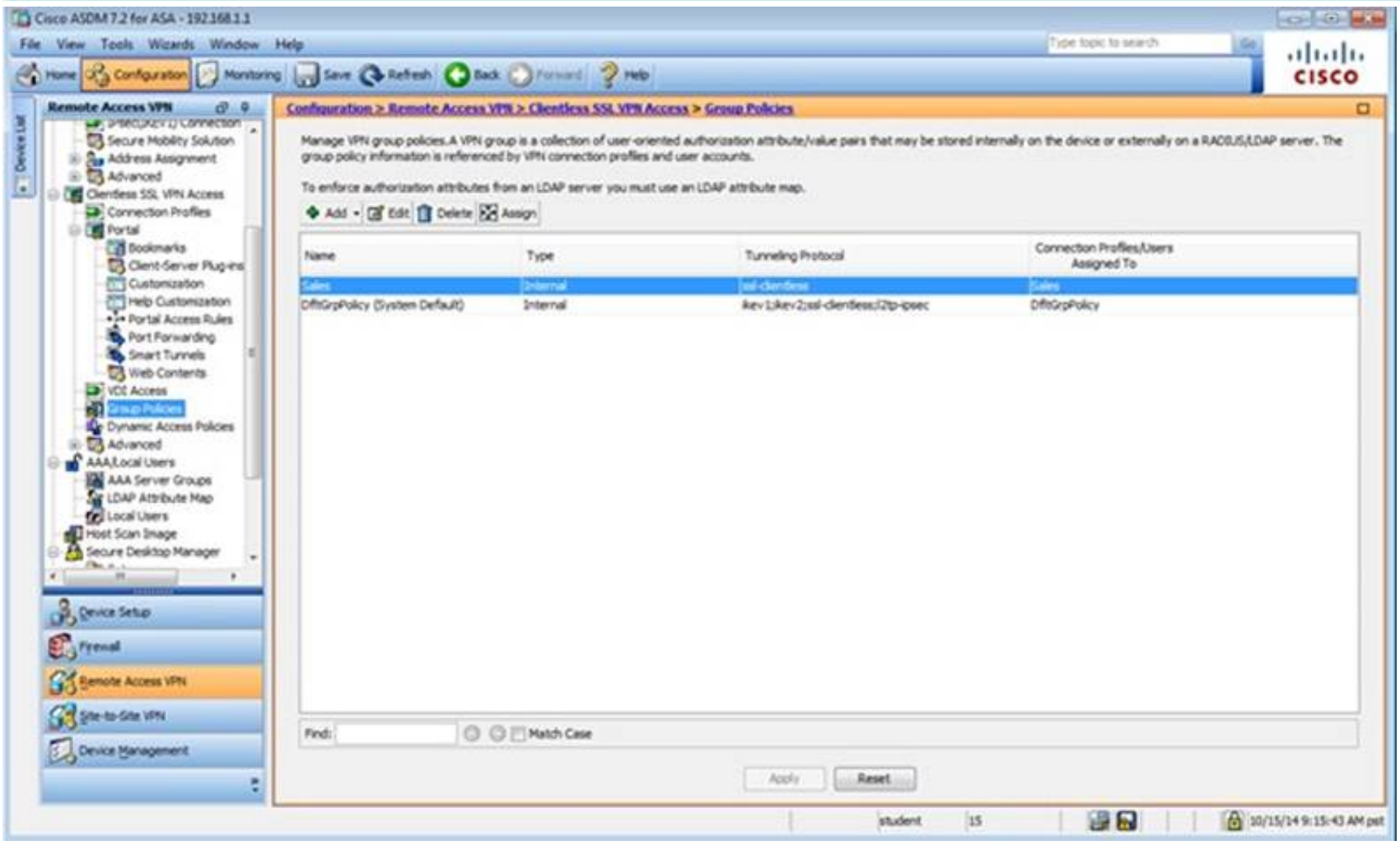

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

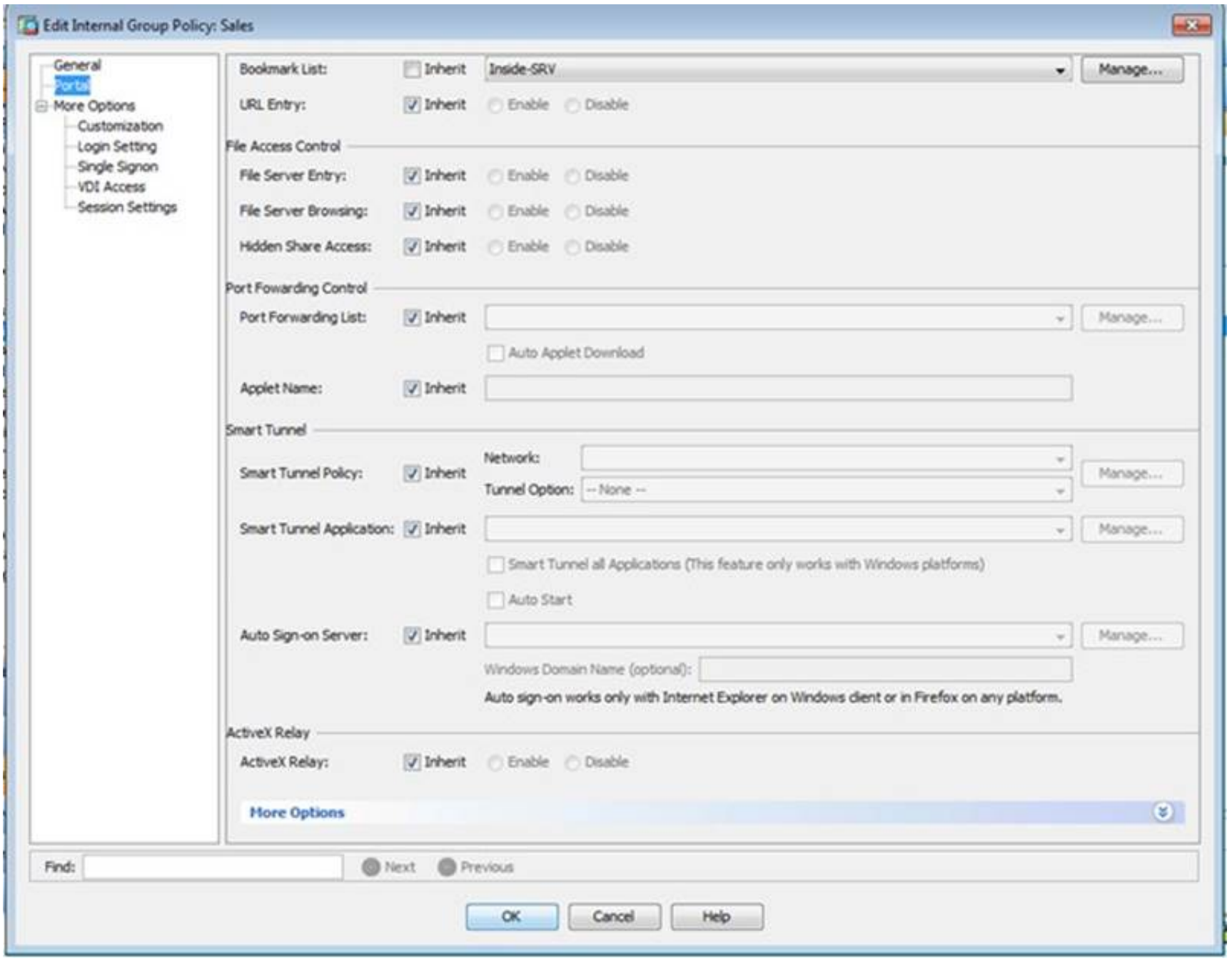

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Add Edit Delete Assign Find: Match Case
List Name
Application ID
Process Name
OS
Hash
Group Policies/User Policies Assigned to
Smart Tunnel Auto Sign-on Server List
Add Edit Delete Assign Find: Match Case
Server List Name
Server
Group Policies/User Policies Assigned to
Smart Tunnel Networks
Add Edit Delete Assign Find: Match Case
Apply
Reset
student
15
5/19/15 8:43:07 AM pst

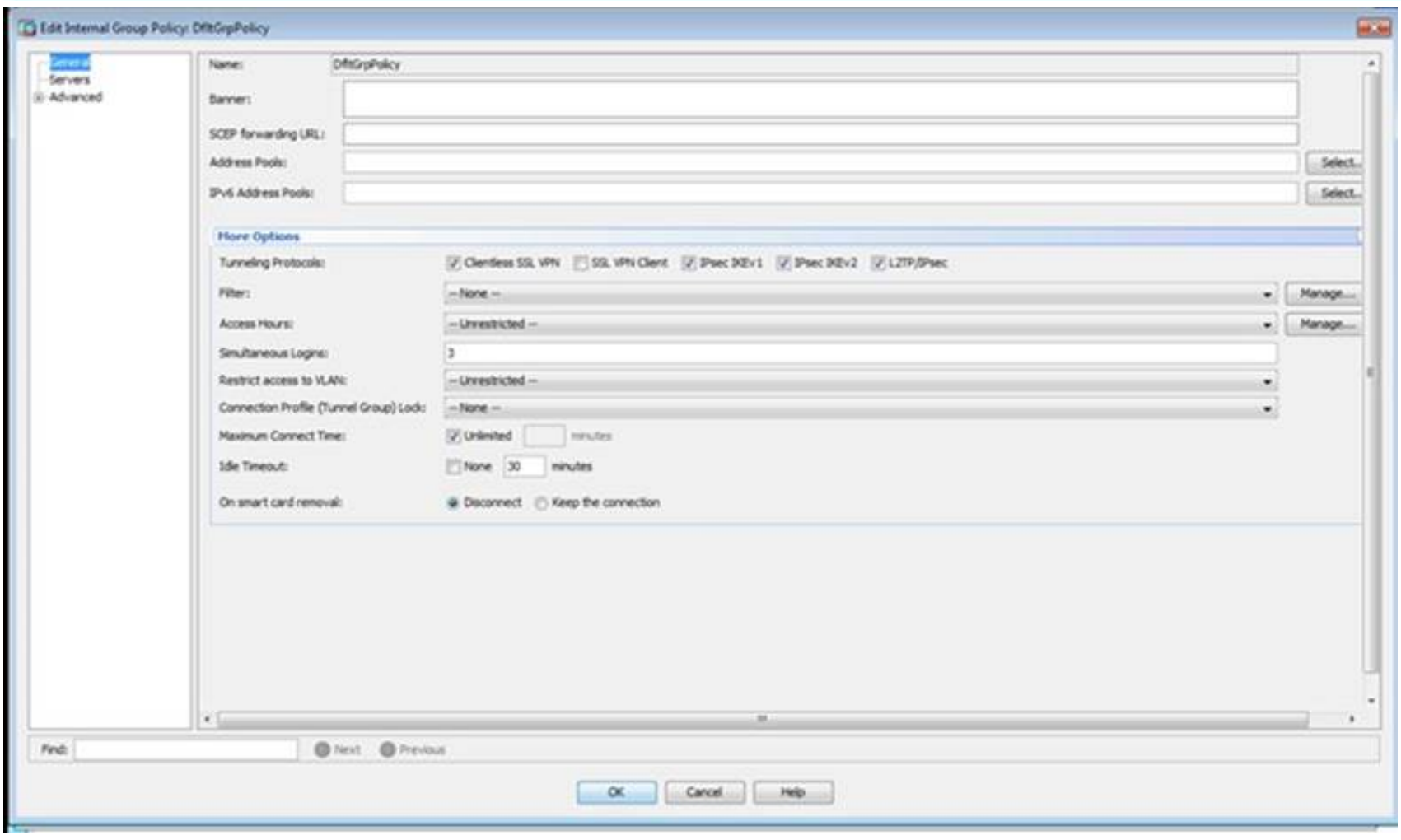

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add Edit Delete Assign
List Name
Local TCP Port
Remote Server
Remote TCP Port
Description
Group Policies/User Policies Assigned to
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:43:47 AM pst

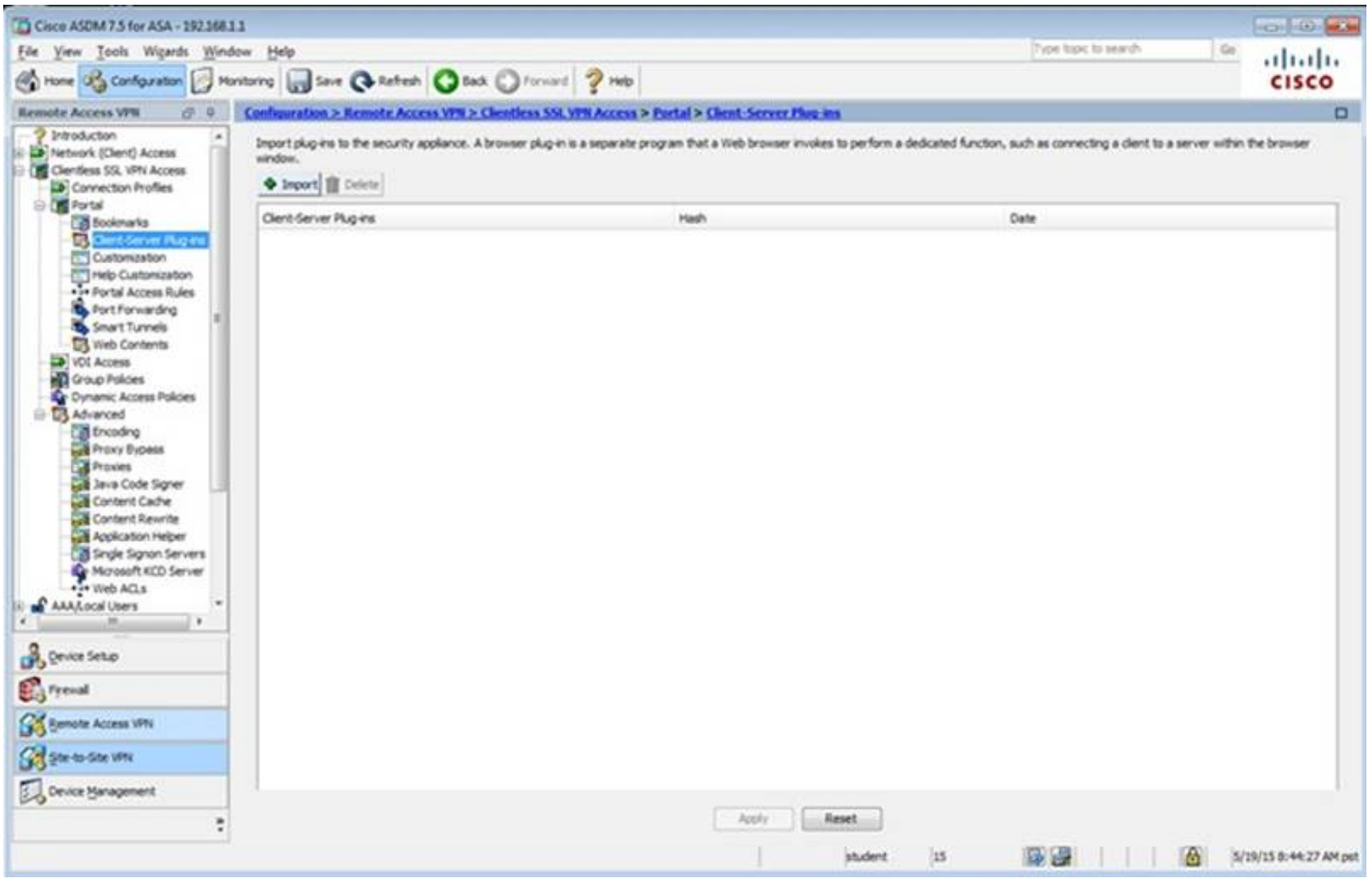

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def...
Find: Match Case
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/19/15 8:49:27 AM pst

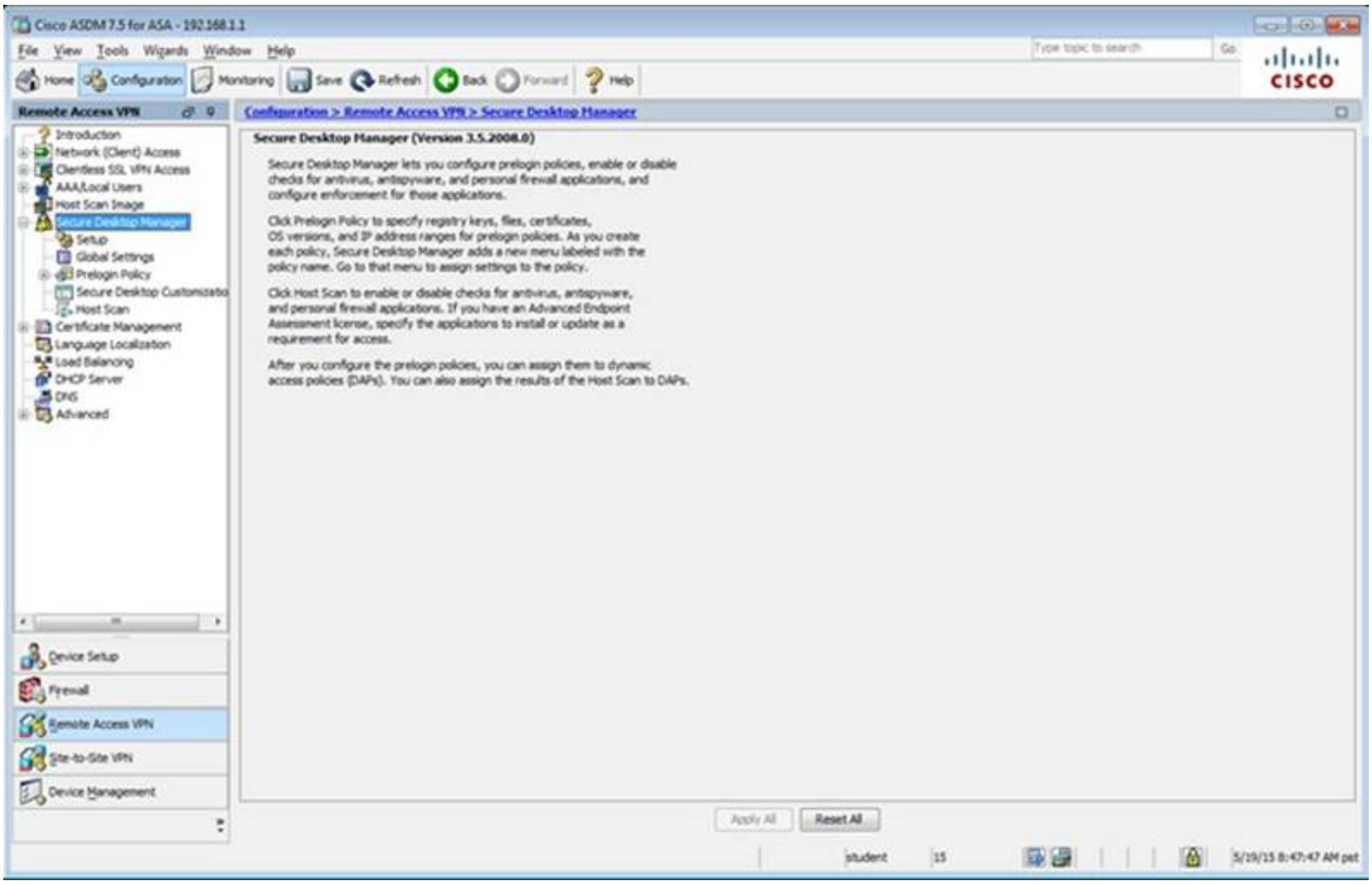

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access to VLAN: Inherit
Connection Profile (Tunnel Group) Lock: Inherit
Maximum Connect Time: Inherit Unlimited minutes
Idle Timeout: Inherit Use Global Default minutes
Timeout Alerts
Session Alert Interval: Inherit Default minutes
Idle Alert Interval: Inherit Default minutes
Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.
Find: Next Previous
OK Cancel Help

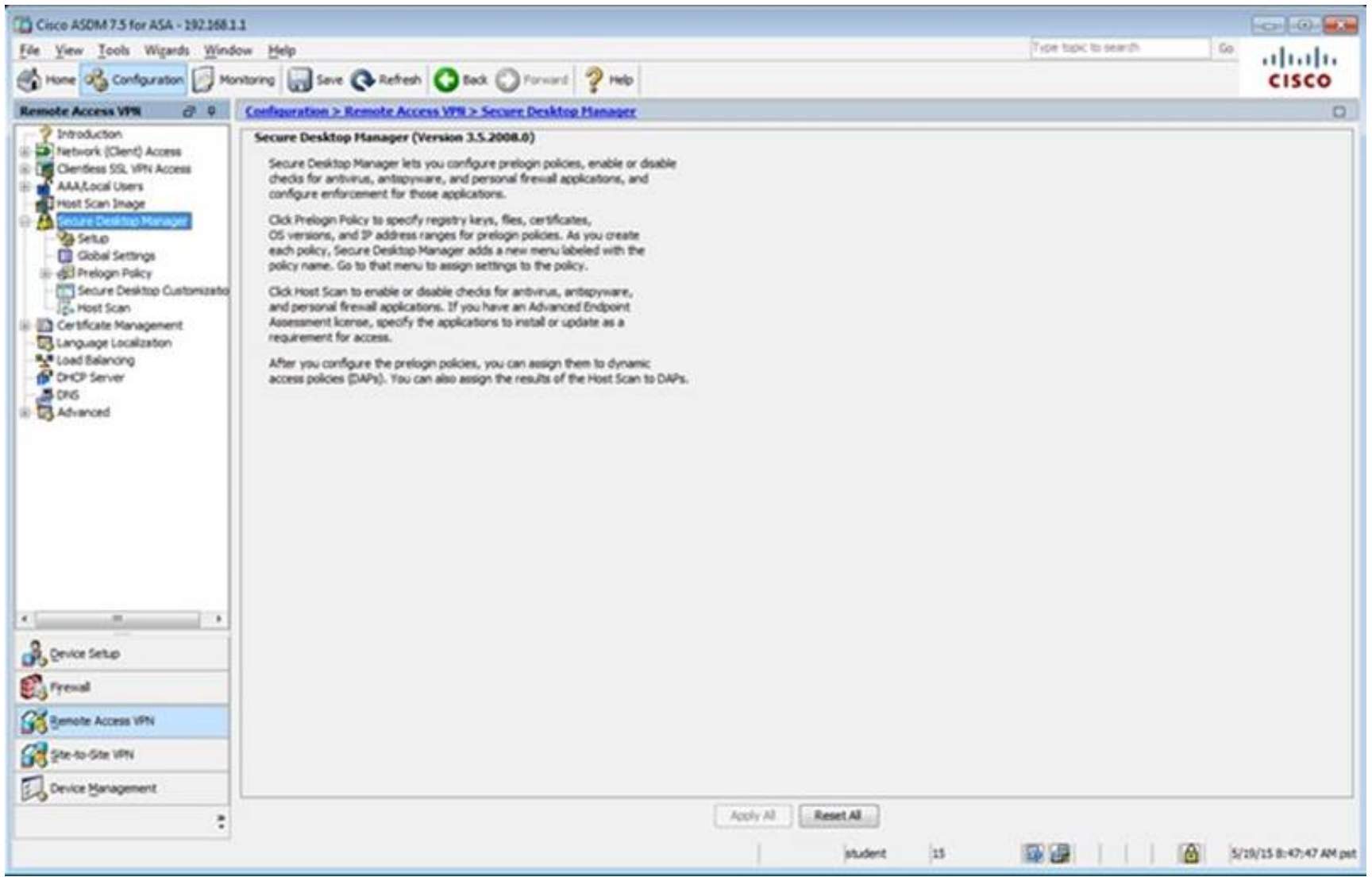

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To
Sales | Internal | ssl-clientless | Sales
DfltGrpPolicy (System Default) | Internal | ikev1;ikev2;ssl-clientless;l2tp-ipsec | DfltGrpPolicy
Find: Match Case
Apply Reset
student 15 10/15/14 9:15:43 AM pst

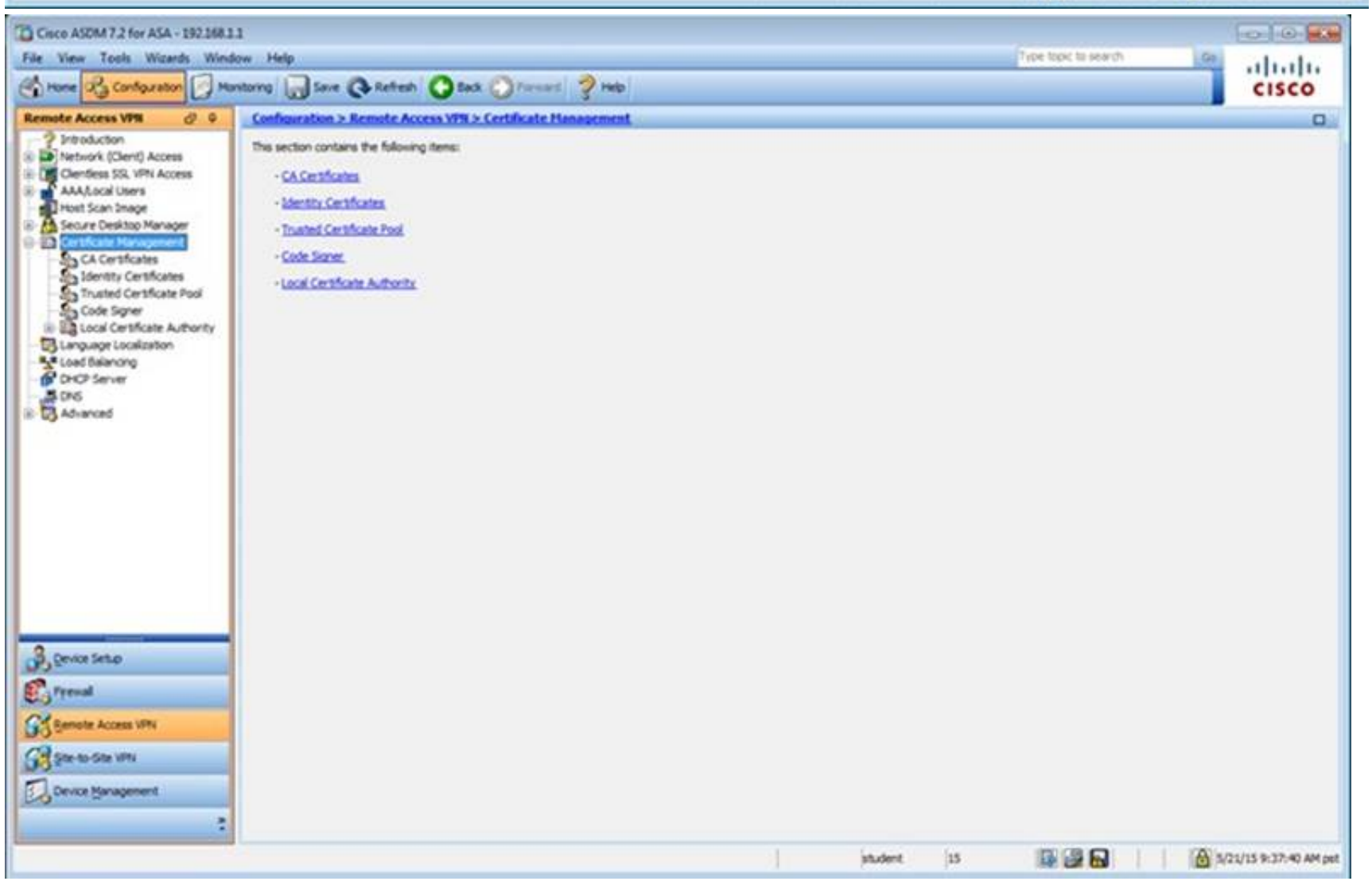

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding Control
Port Forwarding List:
Auto Applet Download
Applet Name:
Smart Tunnel
Network:
Smart Tunnel Policy:
Tunnel Option:
-- None --
Smart Tunnel Application:
Smart Tunnel all Applications (This feature only works with Windows platforms)
Auto Start
Auto Sign-on Server:
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:
More Options
Find:
Next
Previous
OK
Cancel
Help

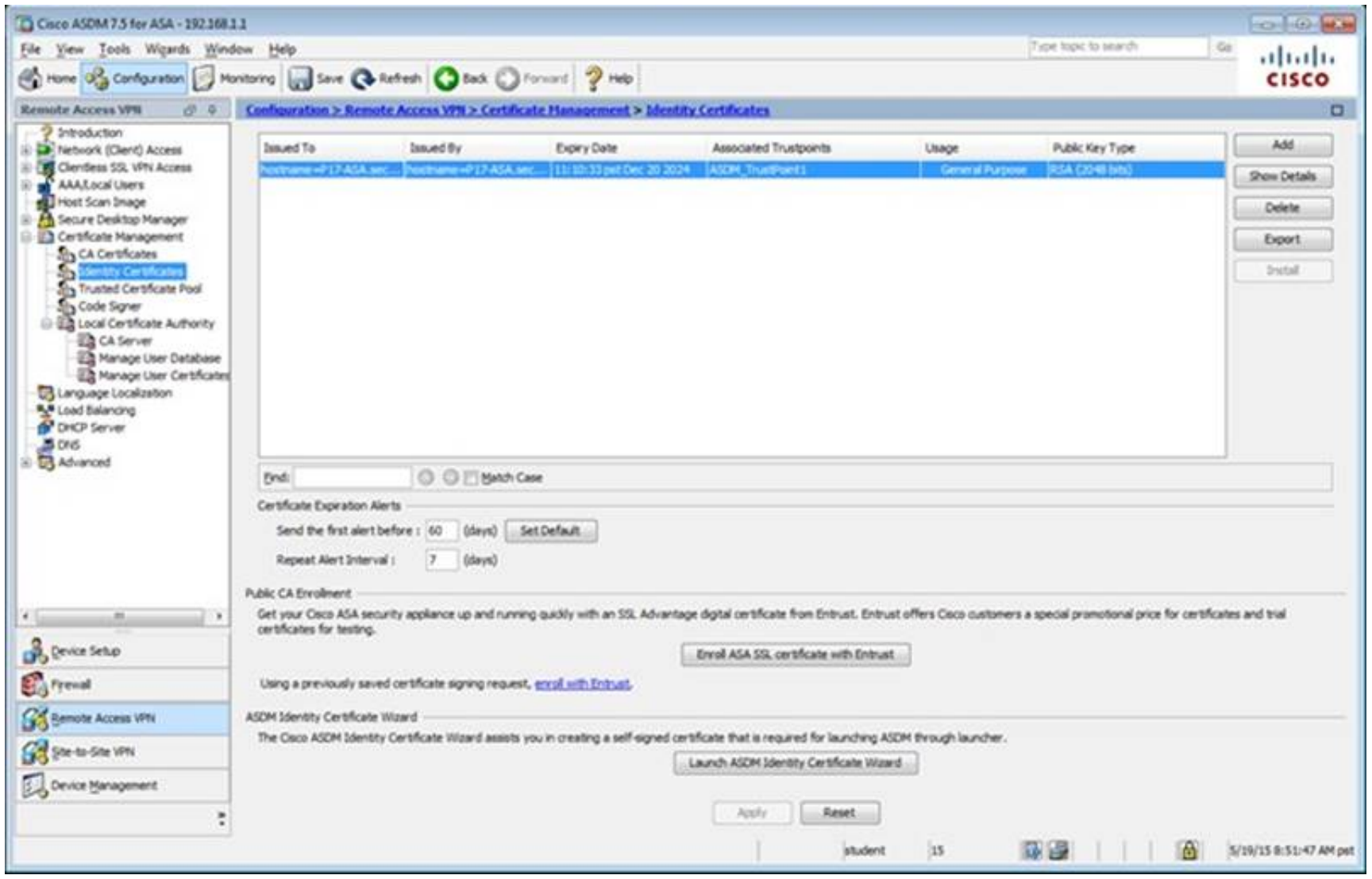

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
Select...
IPv6 Address Pools:
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- Unrestricted --
Simultaneous Logins:
3
Restrict access to VLAN:
Connection Profile (Tunnel Group) Lock:
Maximum Connect Time:
Unlimited
minutes
Idle Timeout:
None
30
minutes
On smart card removal:
Disconnect
Keep the connection
Find:
Next
Previous
OK
Cancel
Help

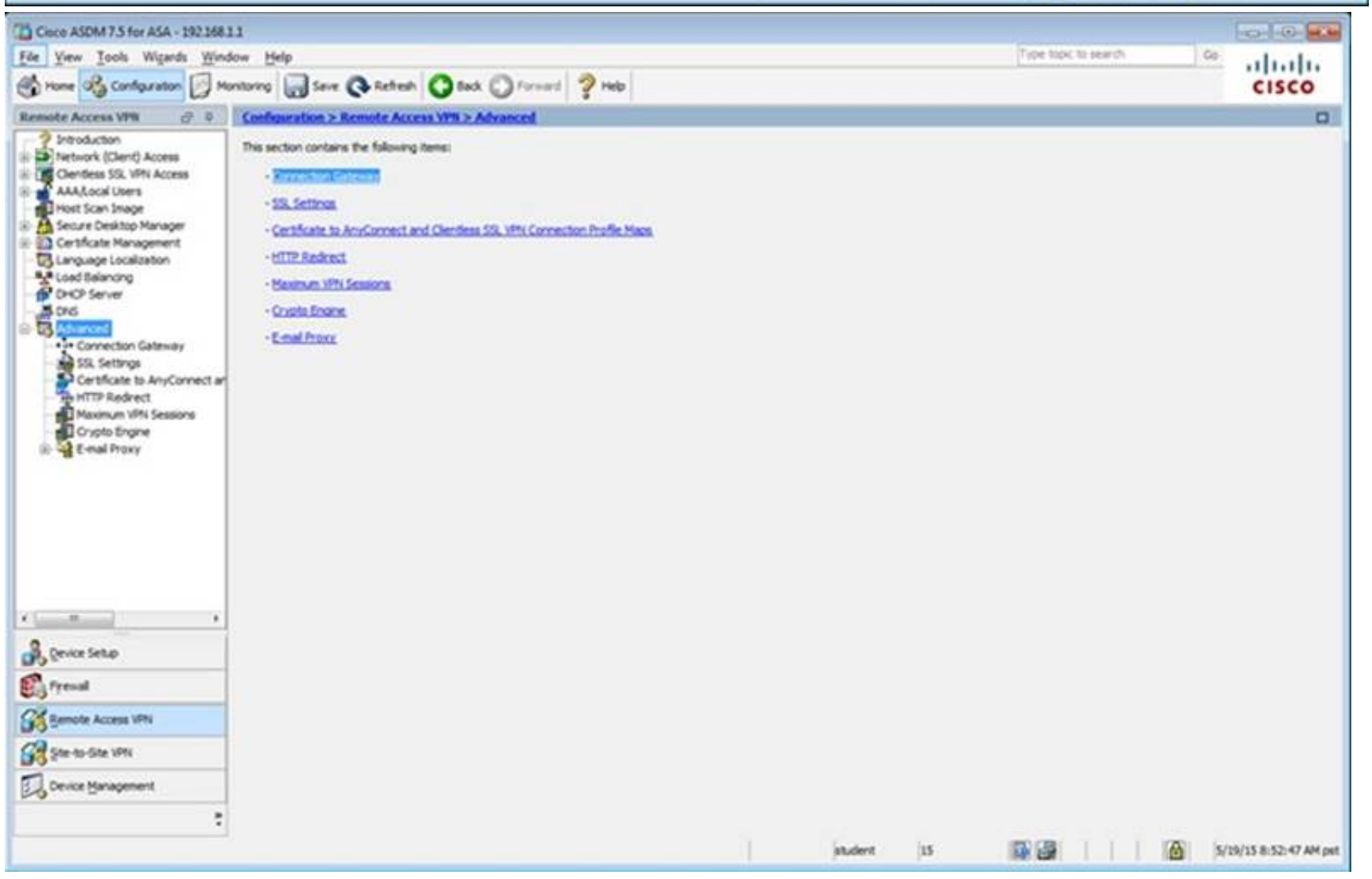

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Rewrite
Application Helper
Single Signon Servers
Microsoft KCD Server
Web ACLs
AAA/Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:44:27 AM pst

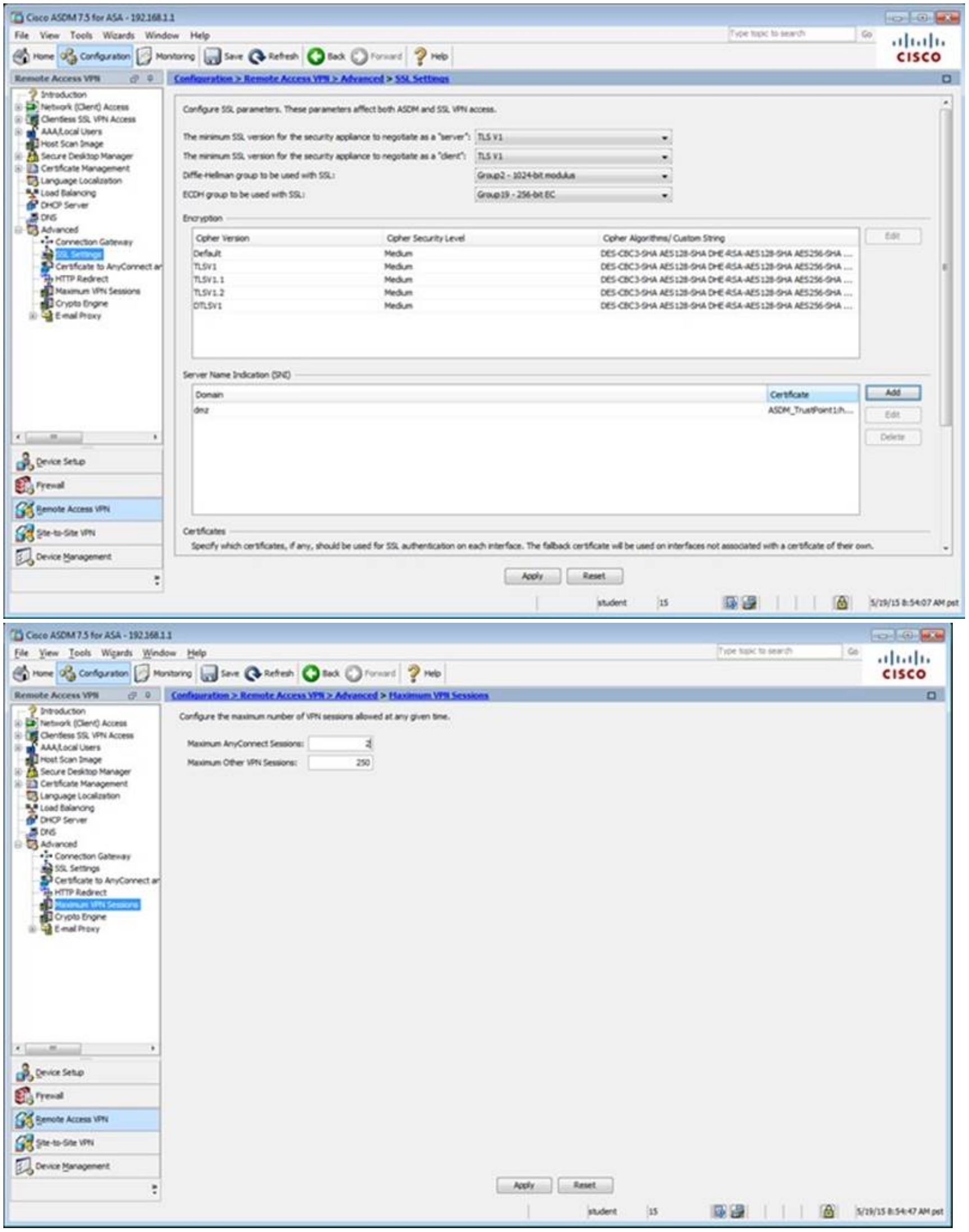

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Secure Desktop Customizatio
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply All
Reset All
student
15
5/19/15 8:47:47 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Setup
Global Settings
Prelogin Policy
Secure Desktop Customizatio
Host Scan
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply All
Reset All
student
15
5/19/15 8:47:47 AM pst

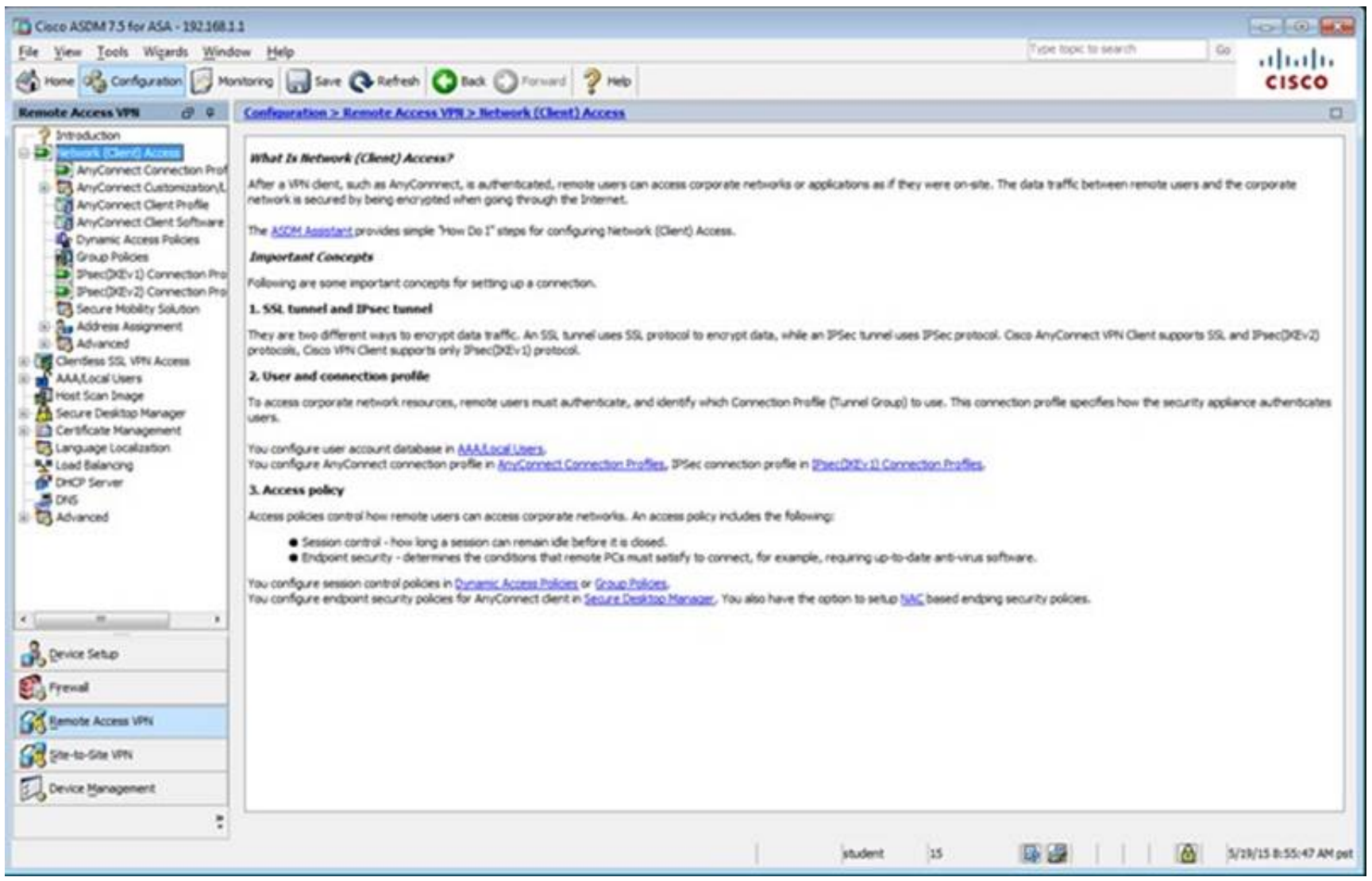

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/21/15 9:37:40 AM pst

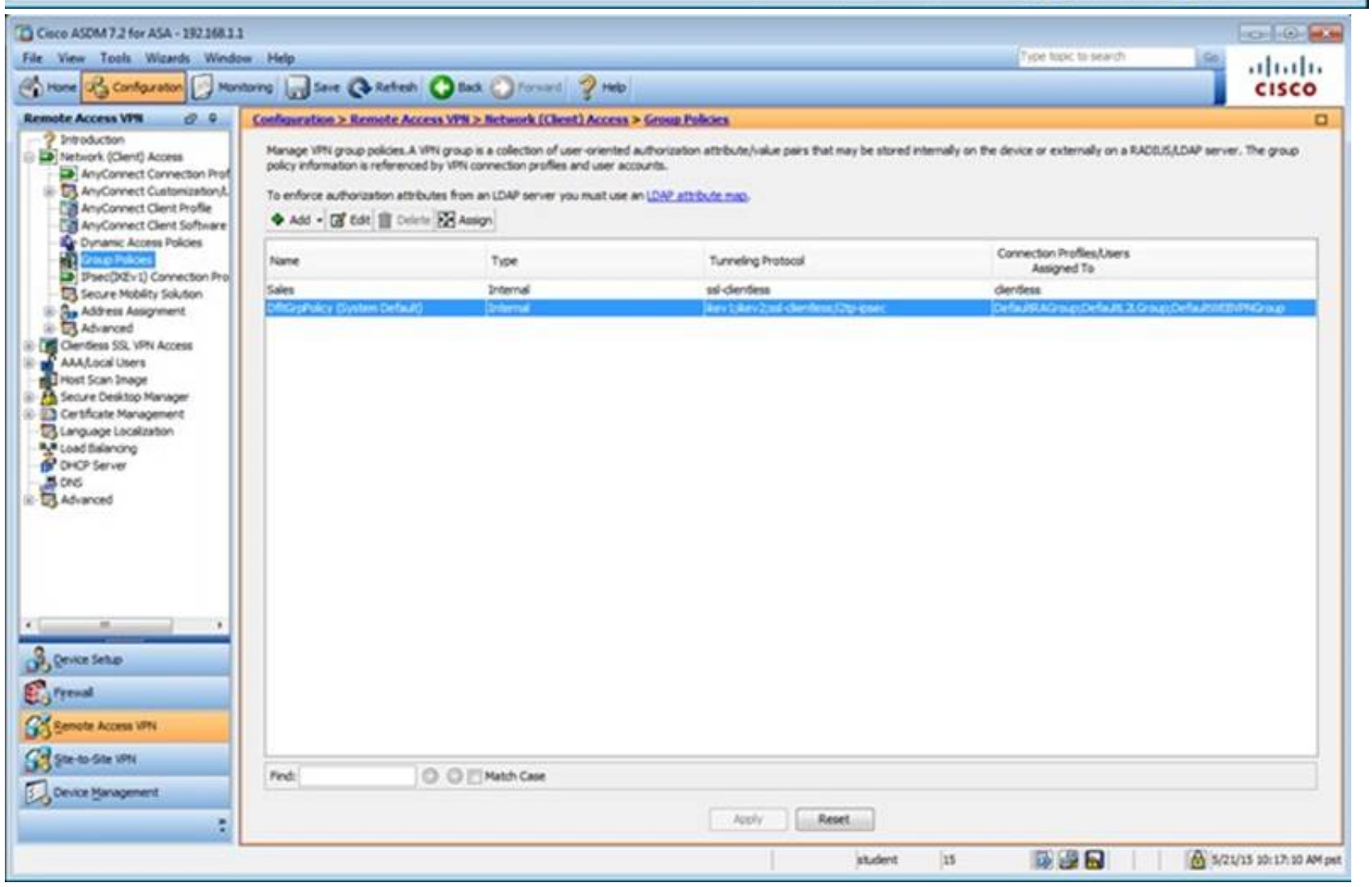

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
CA Certificates
Identity Certificates
Trusted Certificate Pool
Code Signer
Local Certificate Authority
CA Server
Manage User Database
Manage User Certificates
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
Public Key Type
Add
Show Details
Delete
Export
Install
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:51:47 AM pst

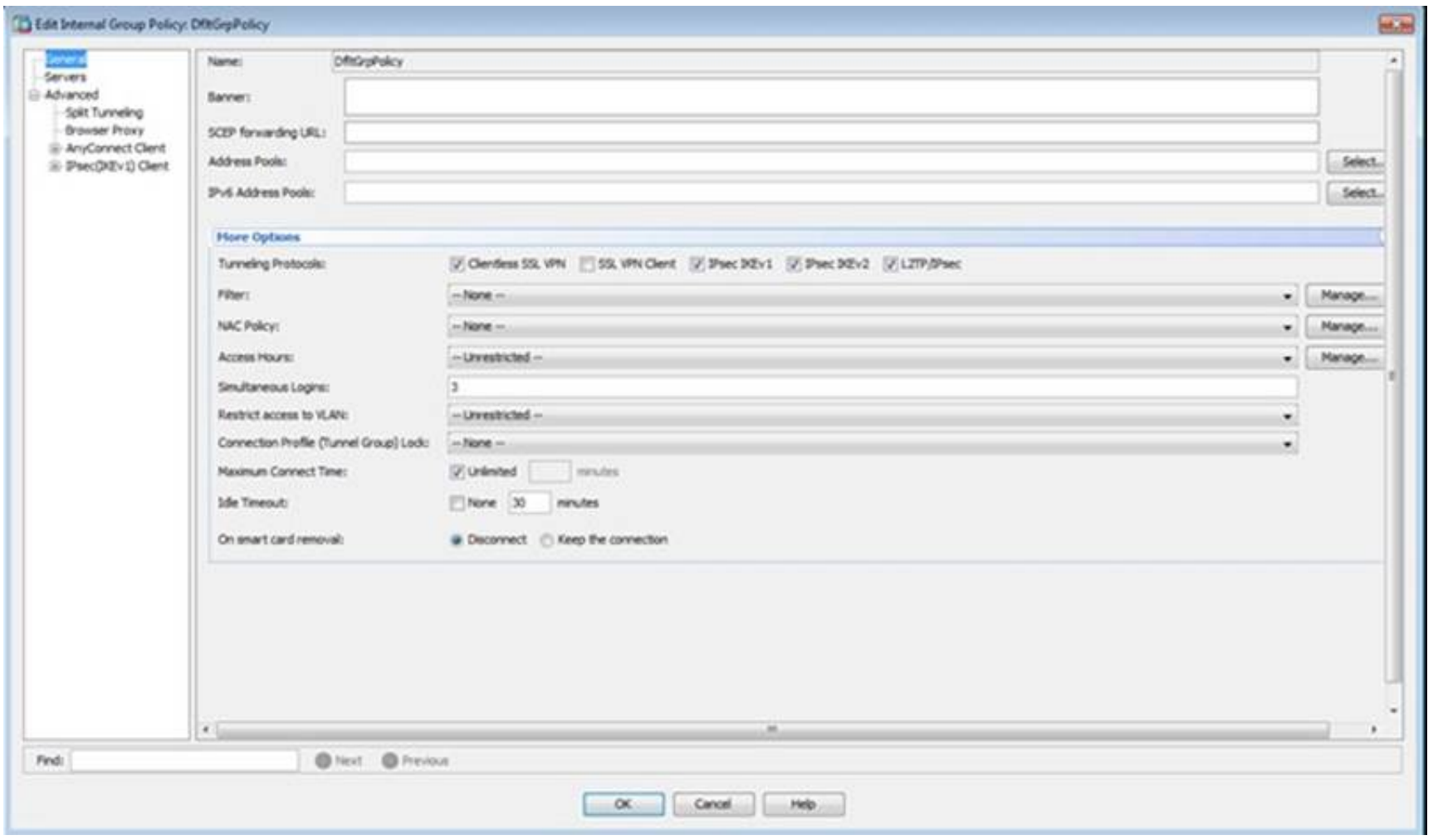

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- Connection Gateway
- SSL Settings
- Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps
- HTTP Redirect
- Maximum VPN Sessions
- Crypto Engine
- E-mail Proxy
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:52:47 AM pst

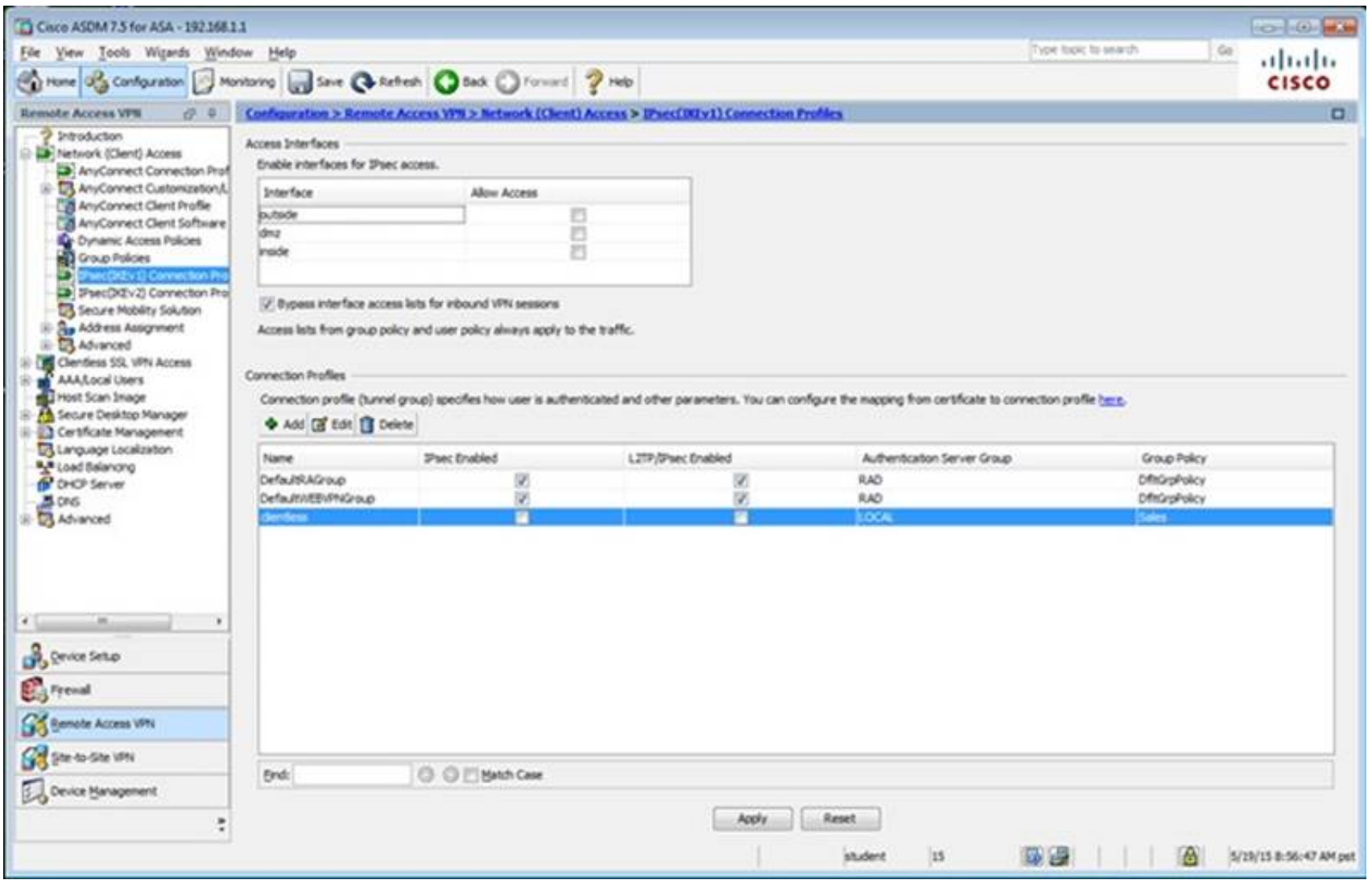

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
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
Edit
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
Add
Edit
Delete
dmz
ASDM_TrustPoint1:h...
Certificates
Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:54:07 AM pst

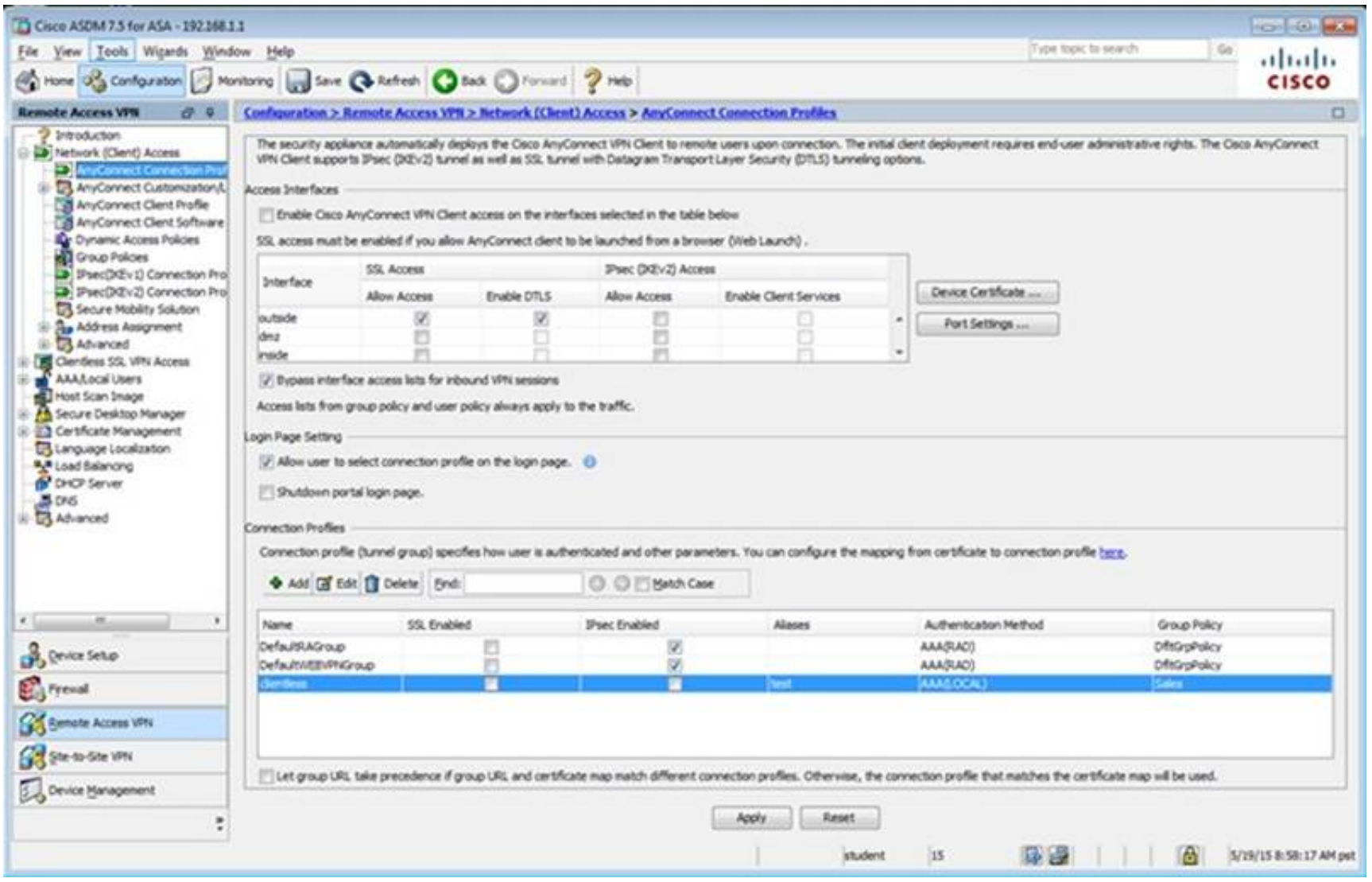
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect ar
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Configure the maximum number of VPN sessions allowed at any given time.
Maximum AnyConnect Sessions: 2
Maximum Other VPN Sessions: 250
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:54:47 AM pst

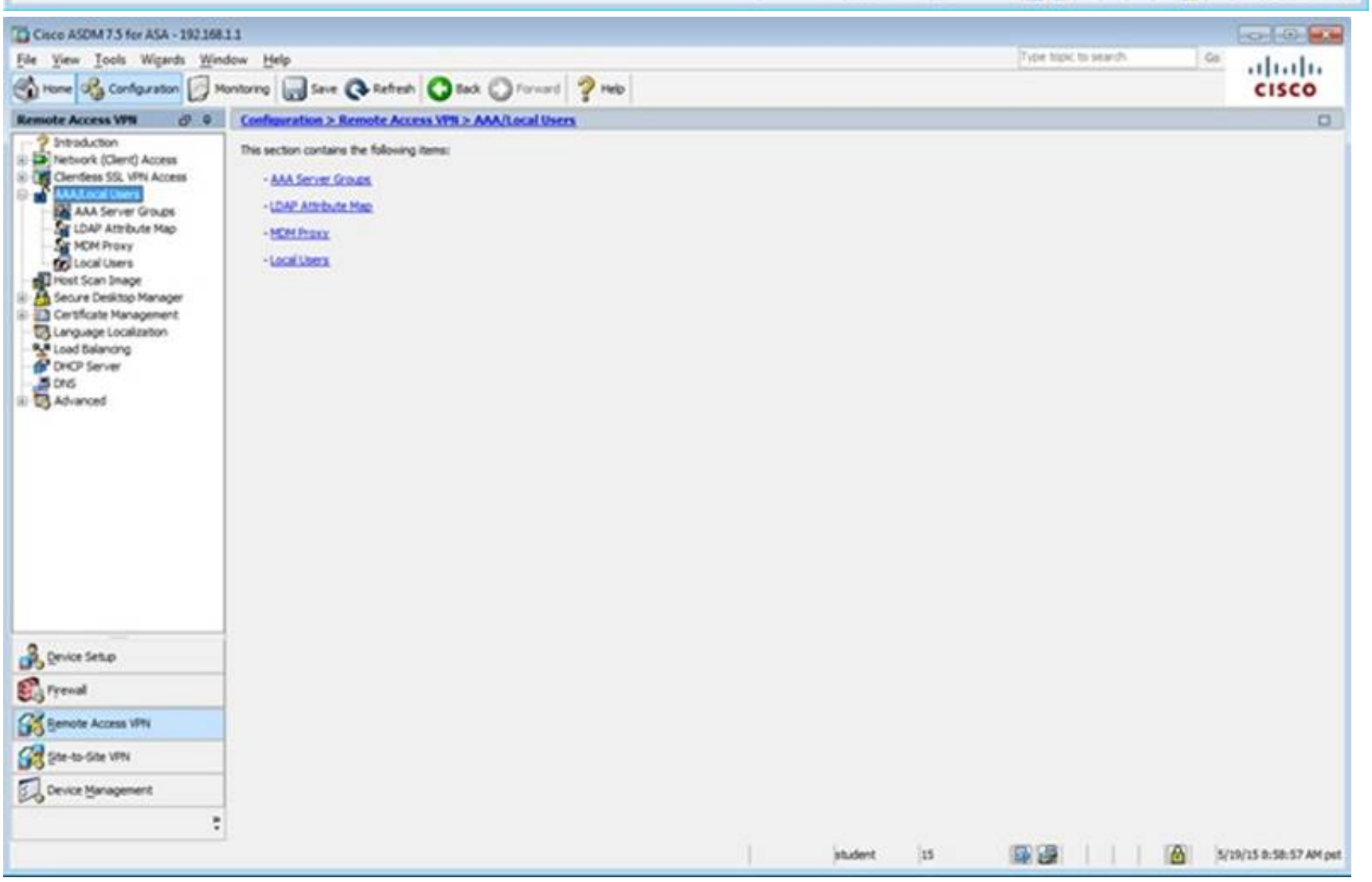

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
The ASDM Assistant provides simple "How Do I" steps for configuring Network (Client) Access.
Important Concepts
Following are some important concepts for setting up a connection.
1. SSL tunnel and IPsec tunnel
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 endpng security policies.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/20/15 8:55:47 AM pst

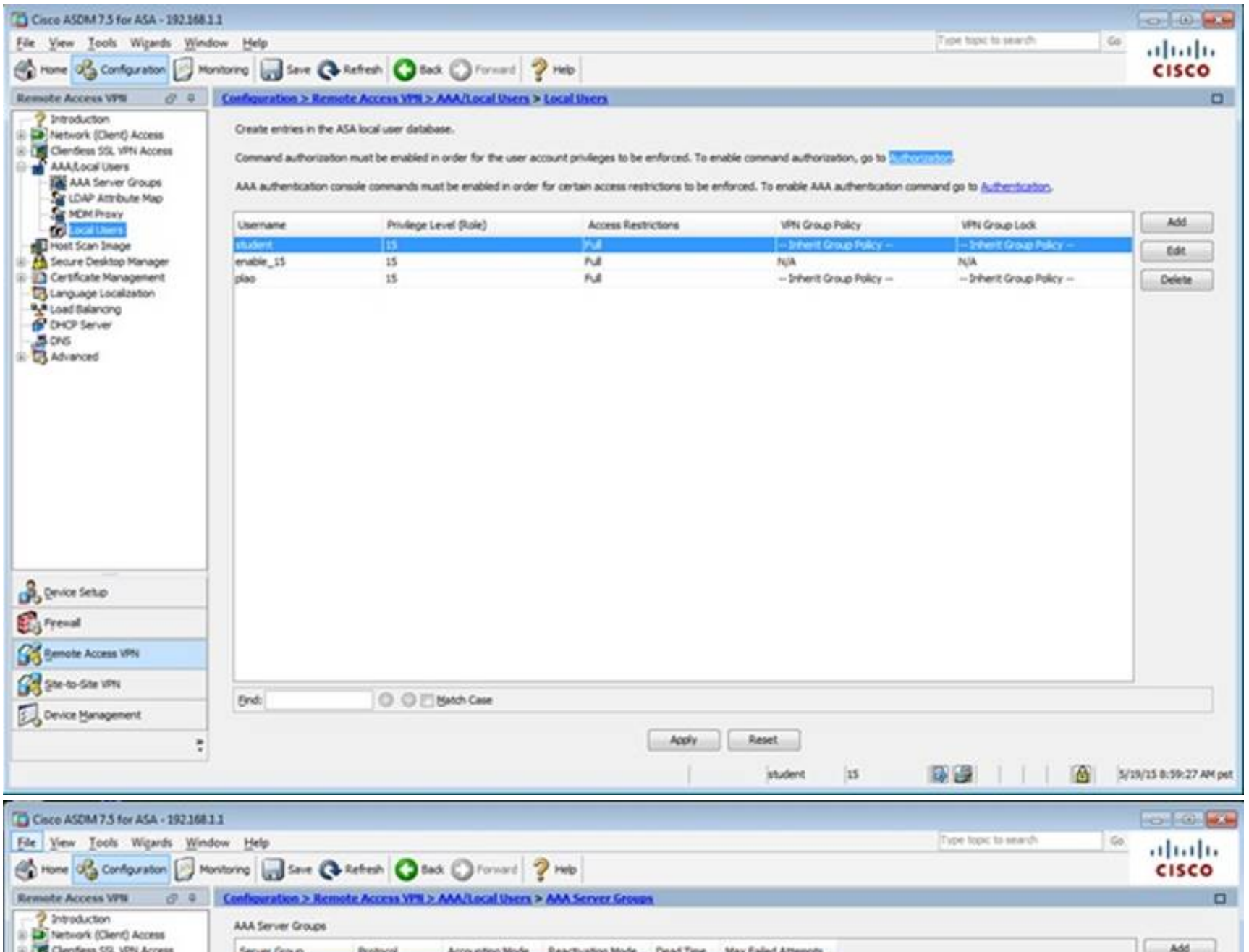

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
DfltGrpPolicy (System Default)
Internal
ikev1;ikev2;ssl-clientless;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup
Find:
Match Case
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15 5/21/15 10:17:10 AM pst


Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Name: DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
IPv6 Address Pools:
Select...
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
Idle Timeout: None 30 minutes
On smart card removal: Disconnect, Keep the connection
Manage...
Find:
Next
Previous
OK
Cancel
Help


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Prof
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Authentication Server Group
Group Policy
DefaultRAGroup
RAD
DfltGrpPolicy
DefaultWEBVPNGroup
RAD
DfltGrpPolicy
clientless
LOCAL
Sales
Find:
Match Case
Apply
Reset
student
15
5/19/15 8:56:47 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/L
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Pro
IPsec(IKEv2) Connection Pro
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
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
Allow Access
Enable DTLS
IPsec (IKEv2) Access
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(RAC)
DfltGrpPolicy
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:17 AM pst


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > AAA/Local Users
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This section contains the following items:
- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:57 AM pst

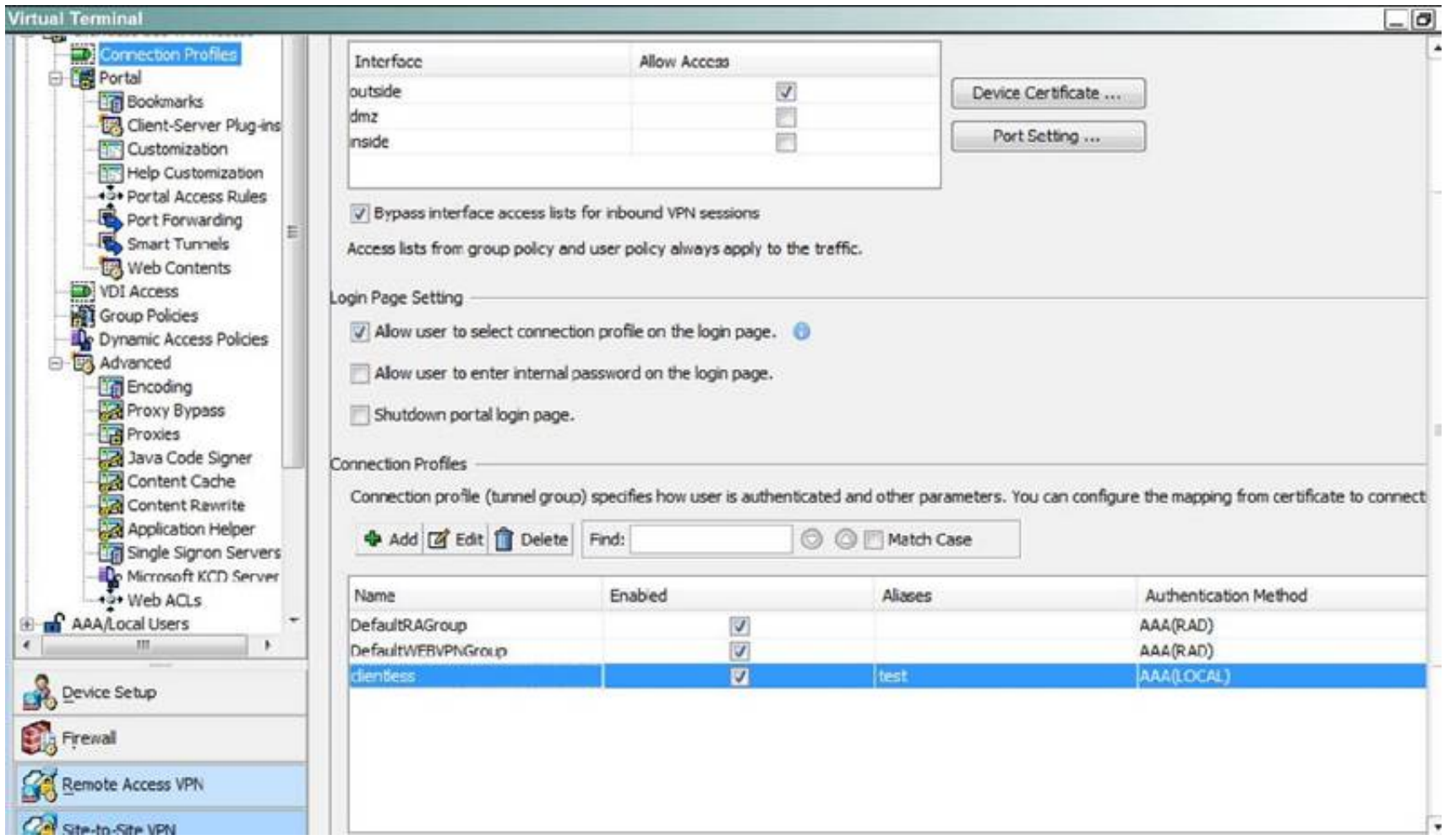


Which two statements regarding the ASA VPN configurations are correct? (Choose two)

A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1.
B. The DefaultWEBVPNGroup Connection Profile is using the AAA with RADIUS server method.
C. The Inside-SRV bookmark references thehttps://192.168.1.2URL
D. Only Clientless SSL VPN access is allowed with the Sales group policy
E. AnyConnect, IPSec IKEv1, and IPSec IKEv2 VPN access is enabled on the outside interface
F. The Inside-SRV bookmark has not been applied to the Sales group policy

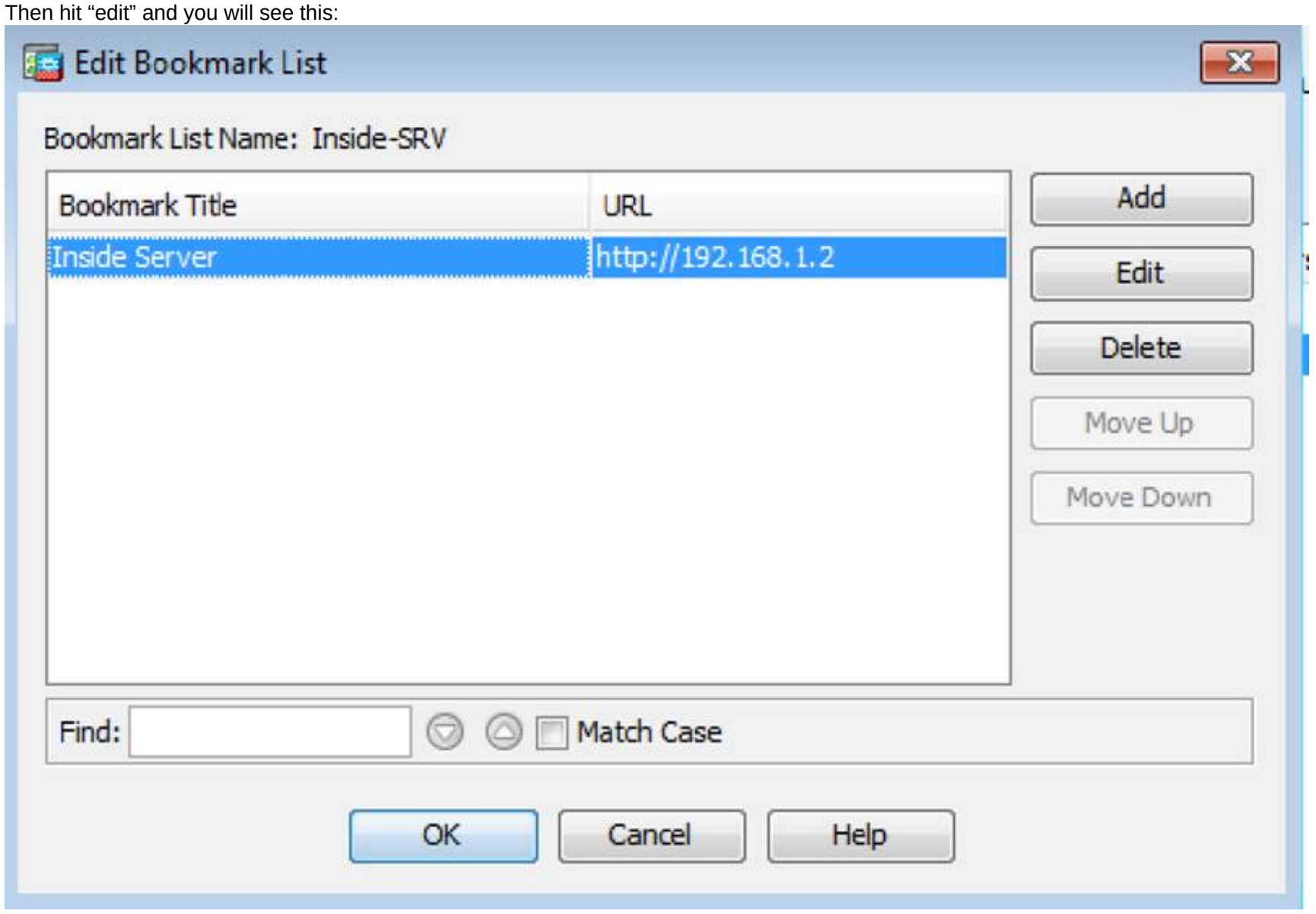
Answer: BC

Explanation:
For B:

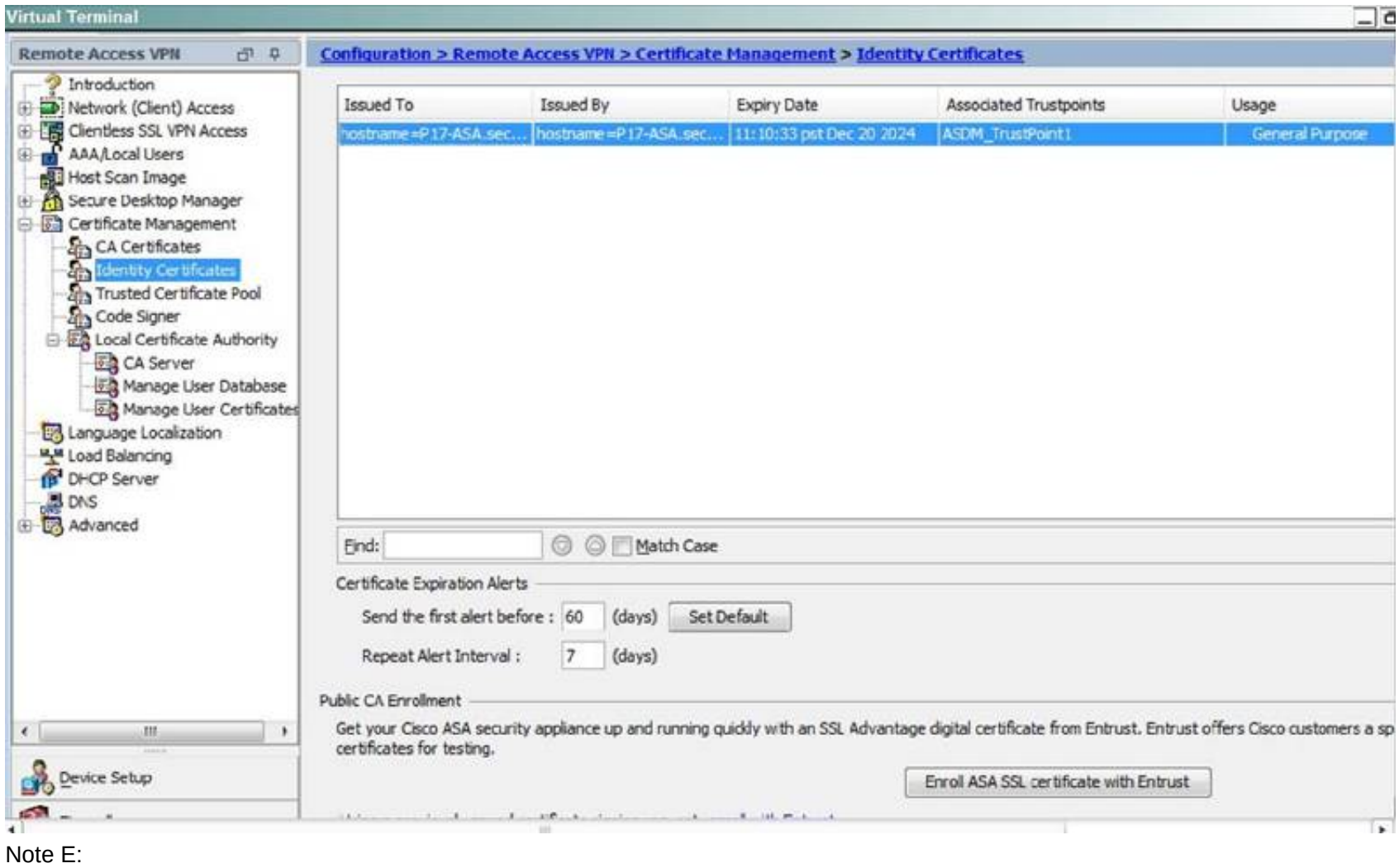


For C, Navigate to the Bookmarks tab:

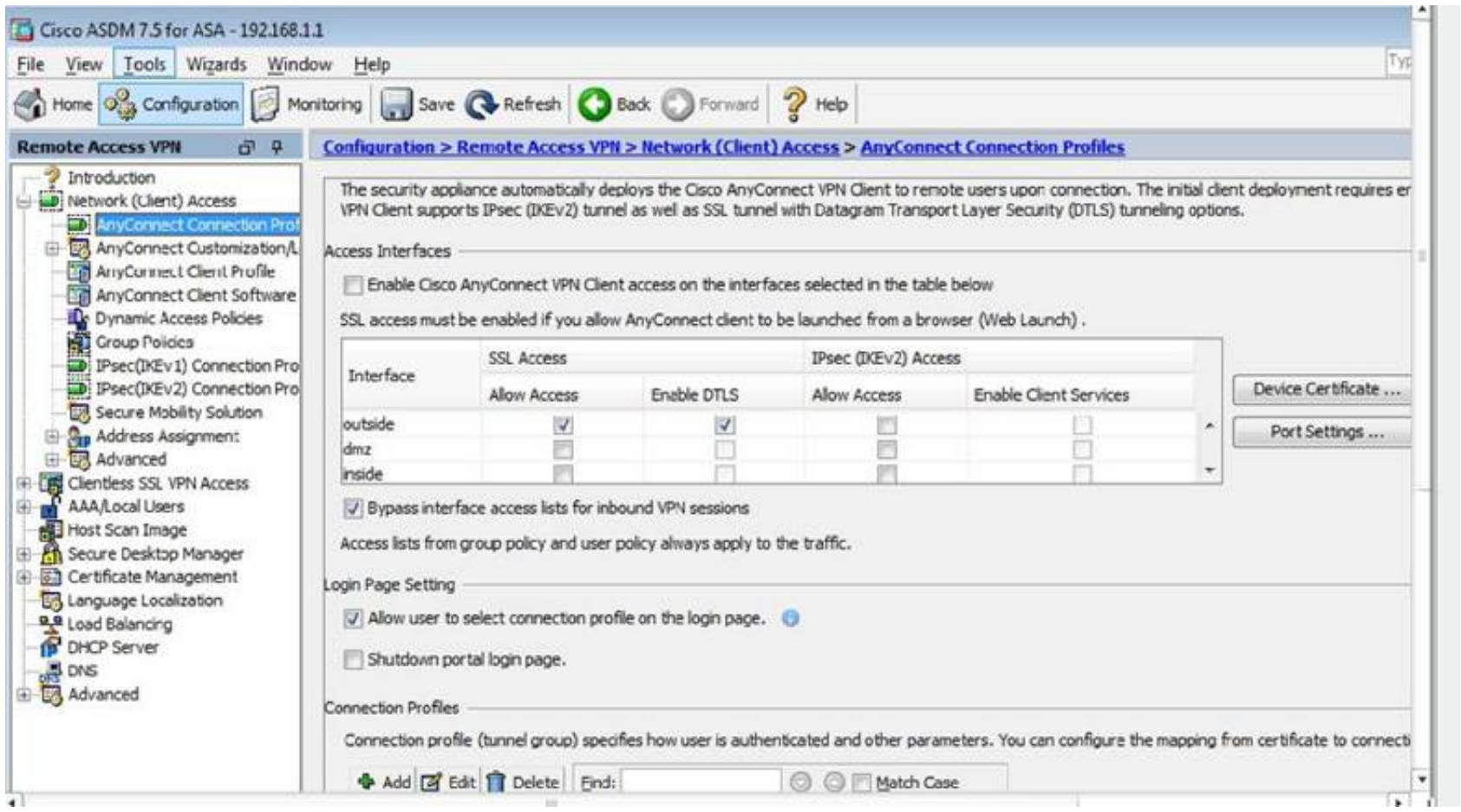
Then hit “edit” and you will see this:



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



Note E:



NEW QUESTION 22
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 27
Which statement correctly describes the function of a private VLAN?

A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains
B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains
C. A private VLAN enables the creation of multiple VLANs using one broadcast domain

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

Answer: A

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

NEW QUESTION 29
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 32
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 33
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 35
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 37
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

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

Answer: A

Explanation: In network computing, hairpinning (or NAT loopback) describes a communication between two hosts behind the same NAT device using their mapped endpoint. Because not all NAT devices support this communication configuration, applications must be aware of it.
Hairpinning is where a machine on the LAN is able to access another machine on the LAN via the external IP address of the LAN/router (with port forwarding set up on the router to direct requests to the appropriate machine on the LAN).
Source: https://en.wikipedia.org/wiki/Hairpinning

NEW QUESTION 40
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 45
Which three ESP fields can be encrypted during transmission? (Choose three.)

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

Answer: DEF

Explanation: The packet begins with two 4-byte fields (Security Parameters Index (SPI) and Sequence Number). Following these fields is the Payload Data, which has substructure that depends on the choice of encryption algorithm and mode, and on the use of TFC padding, which is examined in more detail later. Following the Payload Data are Padding and Pad Length fields, and the Next Header field. The optional Integrity Check Value (ICV) field completes the packet.
Source: https://tools.ietf.org/html/rfc4303#page-14

NEW QUESTION 48
Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

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

Answer: BDE

Explanation: Promiscuous Mode Event Actions
+ Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing.
+ Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing. + Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action.
Source:
http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html#7

NEW QUESTION 52
If the native VLAN on a trunk is different on each end of the link, what is a potential consequence?

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

Answer: B

Explanation: Smart Tunnel is an advanced feature of Clientless SSL VPN that provides seamless and highly secure remote access for native client-server applications.
Clientless SSL VPN with Smart Tunnel is the preferred solution for allowing access from non-corporate assets as it does not require the administrative rights.
Port forwarding is the legacy technology for supporting TCP based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
Source:
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/tunnel.pdf

NEW QUESTION 56
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 60
Which type of IPS can identify worms that are propagating in a network?

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

Answer: B

Explanation: An example of anomaly-based IPS/IDS is creating a baseline of how many TCP sender requests are generated on average each minute that do not get a response. This is an example of a half-opened session. If a system creates a baseline of this (and for this discussion, let's pretend the baseline is an average of 30 half- opened sessions per minute), and then notices the half-opened sessions have increased to more than 100 per minute, and then acts based on that and generates an alert or begins to deny packets, this is an example of anomaly-based IPS/IDS. The Cisco IPS/IDS appliances have this ability (called anomaly detection), and it is used to identify worms that may be propagating through the network.
Source: Cisco Official Certification Guide, Anomaly-Based IPS/IDS, p.464

NEW QUESTION 65
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 69
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 72
Which command verifies phase 1 of an IPsec VPN on a Cisco router?

A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active

Answer: C

Explanation: A show crypto isakmp sa command shows the ISAKMP SA to be in MM_NO_STATE. This also means that main mode has failed.
Dstsrc state conn-id slot
10.1.1.2 10.1.1.1 MM_NO_STATE 1 0
Verify that the phase 1 policy is on both peers, and ensure that all the attributes match.
Source:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec- debug-00.html#isakmp_sa

NEW QUESTION 73
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 78
What type of attack was the Stuxnet virus?

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

Answer: A

Explanation: Stuxnet is a computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations. It allows the attackers to take control of these systems without the operators knowing. This is the first attack we've seen that allows hackers to manipulate real-world equipment, which makes it very dangerous.
Source: https://us.norton.com/stuxnet

NEW QUESTION 83
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 87
Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

A. Unidirectional Link Detection
B. Unicast Reverse Path Forwarding
C. TrustSec
D. IP Source Guard

Answer: B

Explanation: Unicast Reverse Path Forwarding (uRPF) can mitigate spoofed IP packets. When this feature is enabled on an interface, as packets enter that interface the router spends an extra moment considering the source address of the packet. It then considers its own routing table, and if the routing table does not agree that the interface that just received this packet is also the best egress interface to use for forwarding to the source address of the packet, it then denies the packet.
This is a good way to limit IP spoofing.
Source: Cisco Official Certification Guide, Table 10-4 Protecting the Data Plane, p.270

NEW QUESTION 88
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 89
Which type of address translation should be used when a Cisco ASA is in transparent mode?

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

Answer: A

Explanation: + Because the transparent firewall does not have any interface IP addresses, you cannot use interface PAT.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/ cfgnat.html#wp1102744%0A

NEW QUESTION 93
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain.
D. The switch could become a transparent bridge.

Answer: B

Explanation: Control plane: This includes protocols and traffic that the network devices use on their own without direct interaction from an administrator. An example is a routing protocol.
Source: Cisco Official Certification Guide, The Network Foundation Protection Framework, p.264

NEW QUESTION 94
Refer to the exhibit.

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

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

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

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 98
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 99
If a router configuration includes the line aaa authentication login default group tacacs+ enable, which events will occur when the TACACS+ server returns an error? (Choose two.)

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

Answer: AB

NEW QUESTION 100
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 103

Which statement about application blocking is true?

A. It blocks access to specific programs.
B. It blocks access to files with specific extensions.
C. It blocks access to specific network addresses.
D. It blocks access to specific network services.

Answer: A

Explanation: How do you block unknown applications on Cisco Web Security Appliance If Application Visibility Controls (AVC) are enabled (Under GUI > Security Services > Web Reputation and Anti- Malware), then we can block access based on application types like Proxies, File Sharing, Internet utilities.
We can do this under Web Security Manager > Access Policies > 'Applications' column <for the required access policy>.
Source:
http://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118486-technote-wsa- 00.html

NEW QUESTION 105
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 109
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 113
Which statement about Cisco ACS authentication and authorization is true?

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

Answer: A

Explanation: ACS can join one AD domain. If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which ACS is connected and the other domains that have user and machine information to which you need access. So B is not correct.
Source:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-8/ACS-ADIntegration/guide/Active_Directory_Integration_in_ACS_5-8.pdf + You can define multiple authorization profiles as a network access policy result. In this way, you maintain a smaller number of authorization profiles, because you can use the authorization profiles in combination as rule results, rather than maintaining all the combinations themselves in individual profiles. So D. is not correct + ACS 5.1 can function both as a RADIUS and RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards the requests to the external RADIUS server. So C. is nor correct.
Source:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/ acsuserguide/policy_mod.html

NEW QUESTION 115
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 117
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 122
Which protocol provides security to Secure Copy?

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

Answer: B

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

NEW QUESTION 125
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL

Answer: D

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

NEW QUESTION 127
By which kind of threat is the victim tricked into entering username and password information at a disguised website?

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

Answer: D

Explanation: Phishing presents a link that looks like a valid trusted resource to a user. When the user clicks it, the user is prompted to disclose confidential information such as usernames/passwords.
Source: Cisco Official Certification Guide, Table 1-5 Attack Methods, p.13

NEW QUESTION 132
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 135
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 140
Which accounting notices are used to send a failed authentication attempt record to a AAA server? (Choose two.)

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

Answer: AC

Explanation: aaa accounting { auth-proxy | system | network | exec | connection | commands level | dot1x } { default | list- name | guarantee-first } [vrf vrf-name] { start-stop | stop-only | none } [broadcast] { radius | group
group-name } + stop-only: Sends a stop accounting record for all cases including authentication failures
regardless of whether the aaa accounting send stop-record authentication failure command is configured. + stop-record: Generates stop records for a specified event.
For minimal accounting, include the stop-only keyword to send a "stop" accounting record for all cases including authentication failures. For more accounting, you can include the start-stop keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.
Source:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html

NEW QUESTION 143
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 147
Which options are filtering options used to display SDEE message types? (Choose two.)

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

Answer: CD

Explanation: SDEE Messages
+ All -- SDEE error, status, and alert messages are shown.
+ Error -- Only SDEE error messages are shown.
+ Status -- Only SDEE status messages are shown.
+ Alerts -- Only SDEE alert messages are shown.
Source:
http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/ software/user/guide/IPS.html#wp1083698

NEW QUESTION 151
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 153
Which wildcard mask is associated with a subnet mask of /27?

A. 0.0.0.31
B. 0.0.027
C. 0.0.0.224
D. 0.0.0.255

Answer: A

Explanation: Slash Netmask Wildcard Mask
/27 255.255.255.224 0.0.0.31
Further reading
Source: https://en.wikipedia.org/wiki/Wildcard_mask

NEW QUESTION 156
Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

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

Answer: A

Explanation: IPS produces various types of events including intrusion alerts and status events. IPS communicates events to clients such as management applications using the proprietary RDEP2. We have also developed an IPS- industry leading protocol, SDEE, which is a product-independent standard for communicating security device events. SDEE is an enhancement to the current version of RDEP2 that adds extensibility features that are needed for communicating events generated by various types of security devices.
Source:
http://www.cisco.com/c/en/us/td/docs/security/ips/6-1/configuration/guide/ime/imeguide/ ime_system_architecture.html

NEW QUESTION 157
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 162
In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

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

Answer: ABC

NEW QUESTION 163
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 167
Which of the following are features of IPsec transport mode? (Choose three.)

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

Answer: ADE

Explanation: + IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server. + IPsec supports two encryption modes: Transport mode and Tunnel mode. Transport mode encrypts only the data portion (payload) of each packet and leaves the packet header untouched. Transport mode is applicable to either gateway or host implementations, and provides protection for upper layer protocols as well as selected IP header fields.
Source:
http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html
http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/ IPsecPG1.html
Generic Routing Encapsulation (GRE) is often deployed with IPsec for several reasons, including the following:
+ IPsec Direct Encapsulation supports unicast IP only. If network layer protocols other than IP are to be supported, an IP encapsulation method must be chosen so that those protocols can be transported in IP packets.
+ IPmc is not supported with IPsec Direct Encapsulation. IPsec was created to be a security protocol between two and only two devices, so a service such as multicast is problematic. An IPsec peer encrypts a packet so that only one other IPsec peer can successfully perform the de-encryption. IPmc is not compatible with this mode of operation.
Source: https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ ccmigration_09186a008074f26a.pdf

NEW QUESTION 168

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

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

Answer: AC

NEW QUESTION 169
What is the FirePOWER impact flag used for?

A. A value that indicates the potential severity of an attack.
B. A value that the administrator assigns to each signature.
C. A value that sets the priority of a signature.
D. A value that measures the application awareness.

Answer: A

Explanation: Impact Flag: Choose the impact level assigned to the intrusion event .
Because no operating system information is available for hosts added to the network map from NetFlow data, the system cannot assign Vulnerable (impact level 1: red) impact levels for intrusion events involving those hosts. In such cases, use the host input feature to manually set the operating system identity for the hosts.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/ Correlation_Policies.html
Impact
The impact level in this field indicates the correlation between intrusion data, network discovery data, and vulnerability information.
Impact Flag See Impact. Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower- module-user-guide-v541/ViewingEvents.html

NEW QUESTION 171
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

Explanation: This is the output of the #show crypto isakmp sa command. This command shows the Internet Security Association Management Protocol (ISAKMP) security associations (SAs) built between peers - IPsec Phase1.
The "established" clue comes from the state parameter QM_IDLE - this is what we want to see.
More on this
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

NEW QUESTION 176
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 177
Which option describes information that must be considered when you apply an access list to a physical interface?

A. Protocol used for filtering

B. Direction of the access class
C. Direction of the access group
D. Direction of the access list

Answer: C

Explanation: Applying an Access List to an Interface
#interface type number
#ip
access-group {access-list-number | access-list-name} { in | out} Source: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s- book/sec-create-ip-apply.html

NEW QUESTION 178
What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

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

Answer: A

Explanation: To set the interval for which the server waits for a server host to reply, use the tacacs-server timeout command in global configuration mode. To restore the default, use the no form of this command.
If the command is not configured, the timeout interval is 5. Source: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command

NEW QUESTION 183
Which three statements about host-based IPS are true? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 185
What command can you use to verify the binding table status?

A. show ip dhcp snooping database
B. show ip dhcp snooping binding
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping

Answer: A

Explanation: A device's burned-in address is its MAC address. So by changing it to something else may trick hosts on the network into sending packets to it.

NEW QUESTION 186
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 190
Which feature filters CoPP packets?

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

Answer: A

NEW QUESTION 192
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 195
What are two ways to prevent eavesdropping when you perform device management test? (Choose two.)

A. Use an SSH connection.
B. Use SNMPv3.
C. Use out-of-band management.
D. Use SNMPv2.
E. Use in-band management.

Answer: AB

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

NEW QUESTION 198
Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

A. file reputation
B. file analysis
C. signature updates
D. network blocking

Answer: A

NEW QUESTION 200
What do you use when you have a network object or group and want to use an IP address?

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

Answer: B

Explanation: Adding Network Objects for Mapped Addresses
For dynamic NAT, you must use an object or group for the mapped addresses. Other NAT types have the option of using inline addresses, or you can create an

object or group according to this section.
* Dynamic NAT:
+ You cannot use an inline address; you must configure a network object or group. + The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.
+ If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.
* Dynamic PAT (Hide):
+ Instead of using an object, you can optionally configure an inline host address or specify the interface address.
+ If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.
* Static NAT or Static NAT with port translation:
+ Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).
+ If you use an object, the object or group can contain a host, range, or subnet.
* Identity NAT
+ Instead of using an object, you can configure an inline address. + If you use an object, the object must match the real addresses you want to translate.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ nat_objects.html#61711

NEW QUESTION 204
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 205
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 206
A proxy firewall protects against which type of attack?

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

Answer: A

Explanation: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007.
Source: https://en.wikipedia.org/wiki/Cross-site_scripting
A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. A proxy firewall may also be called an application firewall or gateway firewall. Proxy firewalls are considered to be the most secure type of firewall because they prevent direct network contact with other systems.
Source:
http://searchsecurity.techtarget.com/definition/proxy-firewall

NEW QUESTION 211
Which command initializes a lawful intercept view?

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

Answer: C

Explanation: Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information.
Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.
#li-view li-password user username password password
Source:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html
Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the privilege command.

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

NEW QUESTION 216
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 217
You have been tasked with blocking user access to websites that violate company policy, but the sites use dynamic IP addresses. What is the best practice for URL filtering to solve the problem?

A. Enable URL filtering and use URL categorization to block the websites that violate company policy.
B. Enable URL filtering and create a blacklist to block the websites that violate company policy.
C. Enable URL filtering and create a whitelist to block the websites that violate company policy.
D. Enable URL filtering and use URL categorization to allow only the websites that company policy allows users to access.
E. Enable URL filtering and create a whitelist to allow only the websites that company policy allows users to access.

Answer: A

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

NEW QUESTION 218
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 219
Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?

A. You must configure two zone pairs, one for each direction.
B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self zone.

D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Answer: A

Explanation: If you want to allow traffic between two zones, such as between the inside zone (using interfaces facing the inside network) and the outside zone (interfaces facing the Internet or less trusted networks), you must create a policy for traffic between the two zones, and that is where a zone pair comes into play. A zone pair, which is just a configuration on the router, is created identifying traffic sourced from a device in one zone and destined for a device in the second zone. The administrator then associates a set of rules (the policy) for this unidirectional zone pair, such as to inspect the traffic, and then applies that policy to the zone pair.
Source: Cisco Official Certification Guide, Zones and Why We Need Pairs of Them, p.380

NEW QUESTION 223
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 227
What security feature allows a private IP address to access the Internet by translating it to a public address?

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

Answer: A

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

NEW QUESTION 231
Which three statements are characteristics of DHCP Spoofing? (choose three)

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

Answer: ABC

NEW QUESTION 232
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 236
Which statement about extended access lists is true?

A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination

Answer: B

Explanation: Source:
http://www.ciscopress.com/articles/article.asp?p=1697887 Standard ACL
1) Able Restrict, deny & filter packets by Host Ip or subnet only.
2) Best Practice is put Std. ACL restriction near from Source Host/Subnet (Interface-In-bound).
3) No Protocol based restriction. (Only HOST IP). Extended ACL
1) More flexible 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)

NEW QUESTION 237
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 240
In which two situations should you use in band management? (Choose two.)

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

Answer: AB

NEW QUESTION 242
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 246
What is the best way to confirm that AAA authentication is working properly?

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

Answer: A

Explanation: #test aaa group tacacs+ admin cisco123 legacy - A llow verification of the authentication function working between the AAA client (the router) and the ACS server (the AAA server).
Source: Cisco Official Certification Guide, Table 3-6 Command Reference, p.68

NEW QUESTION 247
Refer to the exhibit.

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

What is the effect of the given command?

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

Answer: A

Explanation: A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IP Security protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.
Source:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command Explanation:/Reference/srfipsec.html#wp1017694 To define a transform set -- an acceptable combination of security protocols and algorithms -- use the crypto ipsec transform-set global configuration command.
ESP Encryption Transform
+ esp-aes 256: ESP with the 256-bit AES encryption algorithm. ESP Authentication Transform
+ esp-md5-hmac: ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended) Source: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr- c3.html#wp2590984165

NEW QUESTION 252
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 254
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 257
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 260
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 261
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

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

Answer: BD

Explanation: + ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received.
+ DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the- middle attacks.
+ DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database.
Source: Cisco Official Certification Guide, Dynamic ARP Inspection, p.254

NEW QUESTION 262
Which three statements about Cisco host-based IPS solutions are true? (Choose three.)

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

Answer: ABC

NEW QUESTION 265
Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What type of attack did your team discover?

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

Answer: AB

Explanation: An Advanced Persistent Threat (APT) is a prolonged, aimed attack on a specific target with the intention to compromise their system and gain information from or about that target.
The target can be a person, an organization or a business. Source:
https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/ One new malware threat has emerged as a definite concern, namely, targeted malware. Instead of blanketing the Internet with a worm, targeted attacks concentrate on a single high-value target.
Source:
http://crissp.poly.edu/wissp08/panel_malware.htm

NEW QUESTION 266
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 269
Refer to the exhibit.

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

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

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

With which NTP server has the router synchronized?

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

Answer: A

Explanation: The output presented is generated by the show ntp association detail command. Attributes:
+ configured: This NTP clock source has been configured to be a server. This value can also be dynamic, where the peer/server was dynamically discovered.
+ our_master: The local client is synchronized to this peer
+ valid: The peer/server time is valid. The local client accepts this time if this peer becomes the master.
Source:
http://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html

NEW QUESTION 273
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 274
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 275
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

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

Answer: A

Explanation: Snowshoe spamming is a strategy in which spam is propagated over several domains and IP addresses to weaken reputation metrics and avoid filters. The increasing number of IP addresses makes recognizing and capturing spam difficult, which means that a certain amount of spam reaches their destination email inboxes.
Specialized spam trapping organizations are often hard pressed to identify and trap snowshoe spamming via conventional spam filters.
The strategy of snowshoe spamming is similar to actual snowshoes that distribute the weight of an individual over a wide area to avoid sinking into the snow. Likewise, snowshoe spamming delivers its weight over a wide area to remain clear of filters.
Source: https://www.techopedia.com/definition/1713/snowshoe-spamming Snowshoe spam, as mentioned above, is a growing concern as spammers distribute spam attack origination across a broad range of IP addresses in order to evade IP reputation checks. The newest AsyncOS 9 for ESA enables enhanced anti-spam scanning through contextual analysis and enhanced automation, as well as automatic classification, to provide a stronger defense against snowshoe campaigns and phishing attacks.
Source:
http://blogs.cisco.com/security/cisco-email-security-stays-ahead-of-current-threats-by-adding-stronger- snowshoe-spam-defense-amp-enhancements-and-more

NEW QUESTION 276
What is the primary purpose of a defined rule in an IPS?

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

Answer: A

NEW QUESTION 277
On which Cisco Configuration Professional screen do you enable AAA

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

Answer: A

NEW QUESTION 282
A data breach has occurred and your company database has been copied. Which security principle has been violated?

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

Answer: A

Explanation: Confidentiality: There are two types of data: data in motion as it moves across the network; and data at rest, when data is sitting on storage media (server, local workstation, in the cloud, and so forth). Confidentiality means that only the authorized individuals/ systems can view sensitive or classified information.
Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

NEW QUESTION 286
Refer to the exhibit.

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

tacacs server tacacs2
   address ipv4 2.2.2.2
   timeout 20
   single-connection

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

Which statement about the given configuration is true?

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

Answer: A

Explanation: tacacs-server host host-name [port integer] [timeout integer] [key string] [single-connection] [nat] The single-connection keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.
Source:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command

NEW QUESTION 291
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 210-260 Exam with Our Prep Materials Via below:

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