Cisco

Exam Questions 210-260

Implementing Cisco Network Security

NEW QUESTION 1
What is the Cisco preferred countermeasure to mitigate CAM overflows?

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

Answer: B

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

NEW QUESTION 2
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

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

Answer: D

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

NEW QUESTION 3
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 4
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

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

Answer: B

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

NEW QUESTION 5
Refer to the exhibit.

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

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

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

Answer: A

Explanation: To check the status of Simple Network Management Protocol (SNMP) communications, use the show snmp command in user EXEC or privileged EXEC mode.
Illegal operation for community name supplied: Number of packets requesting an operation not allowed for that community
Source:
http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command

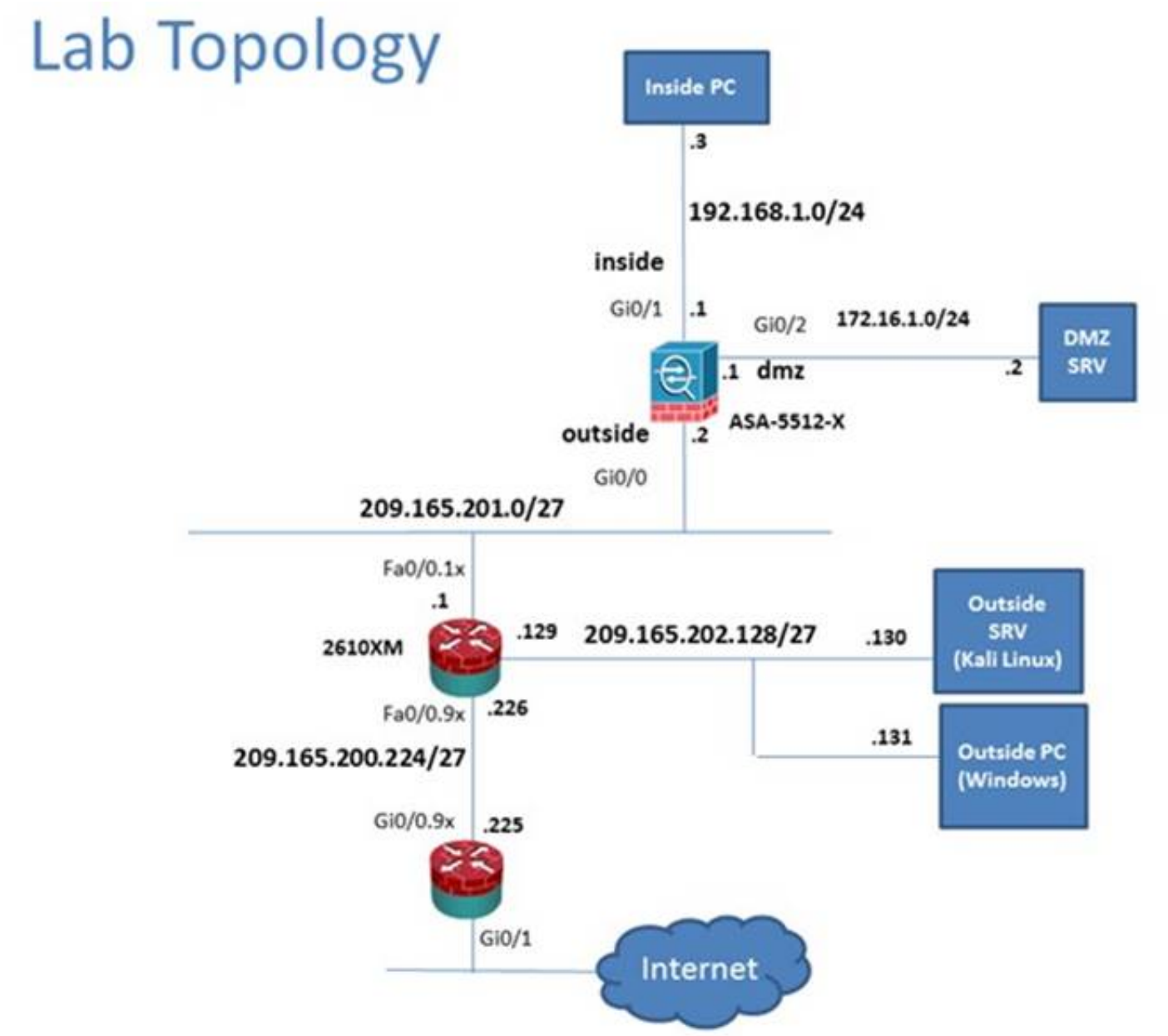
NEW QUESTION 6
What features can protect the data plane? (Choose three.)

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

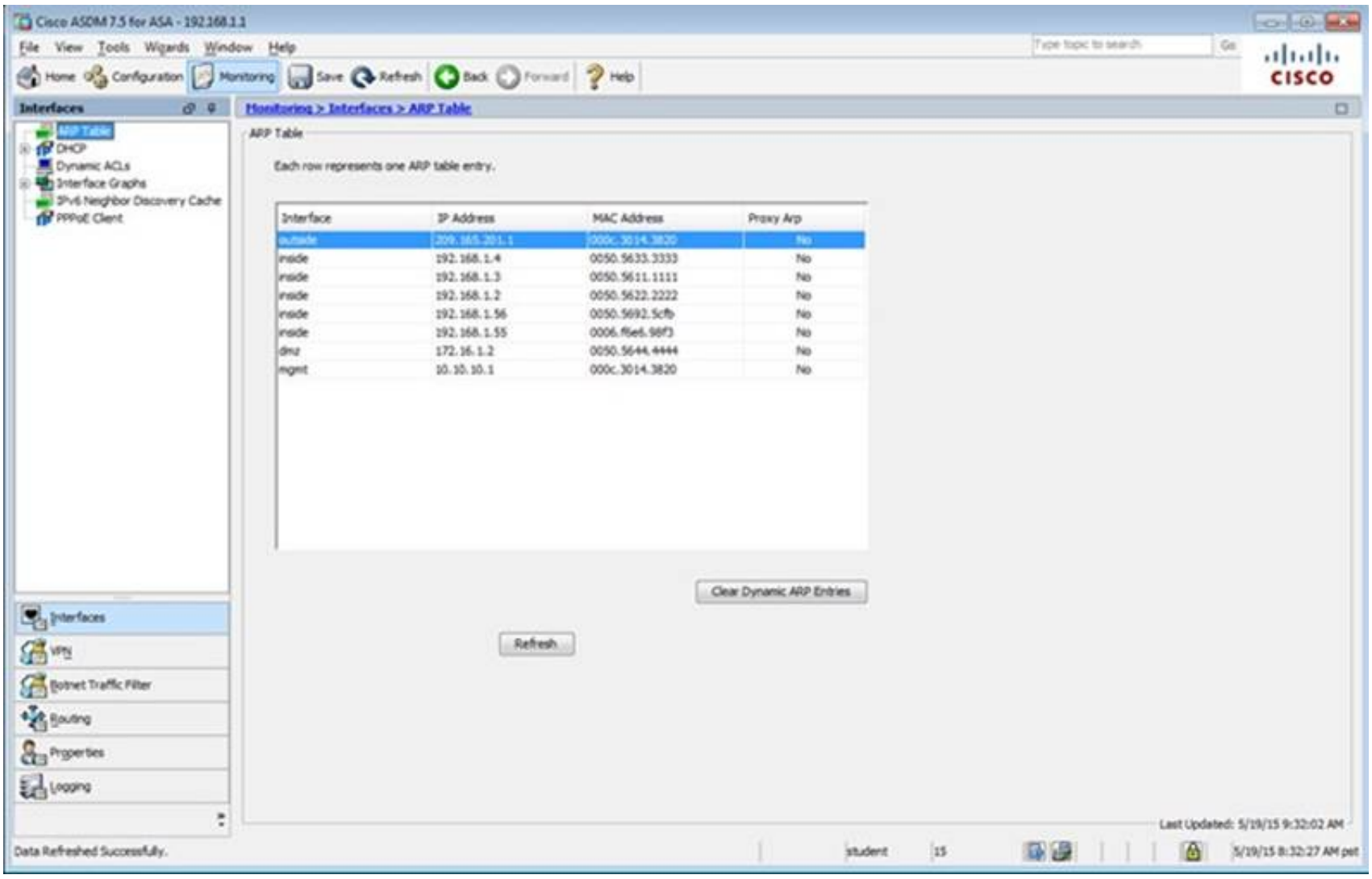
Answer: BDF

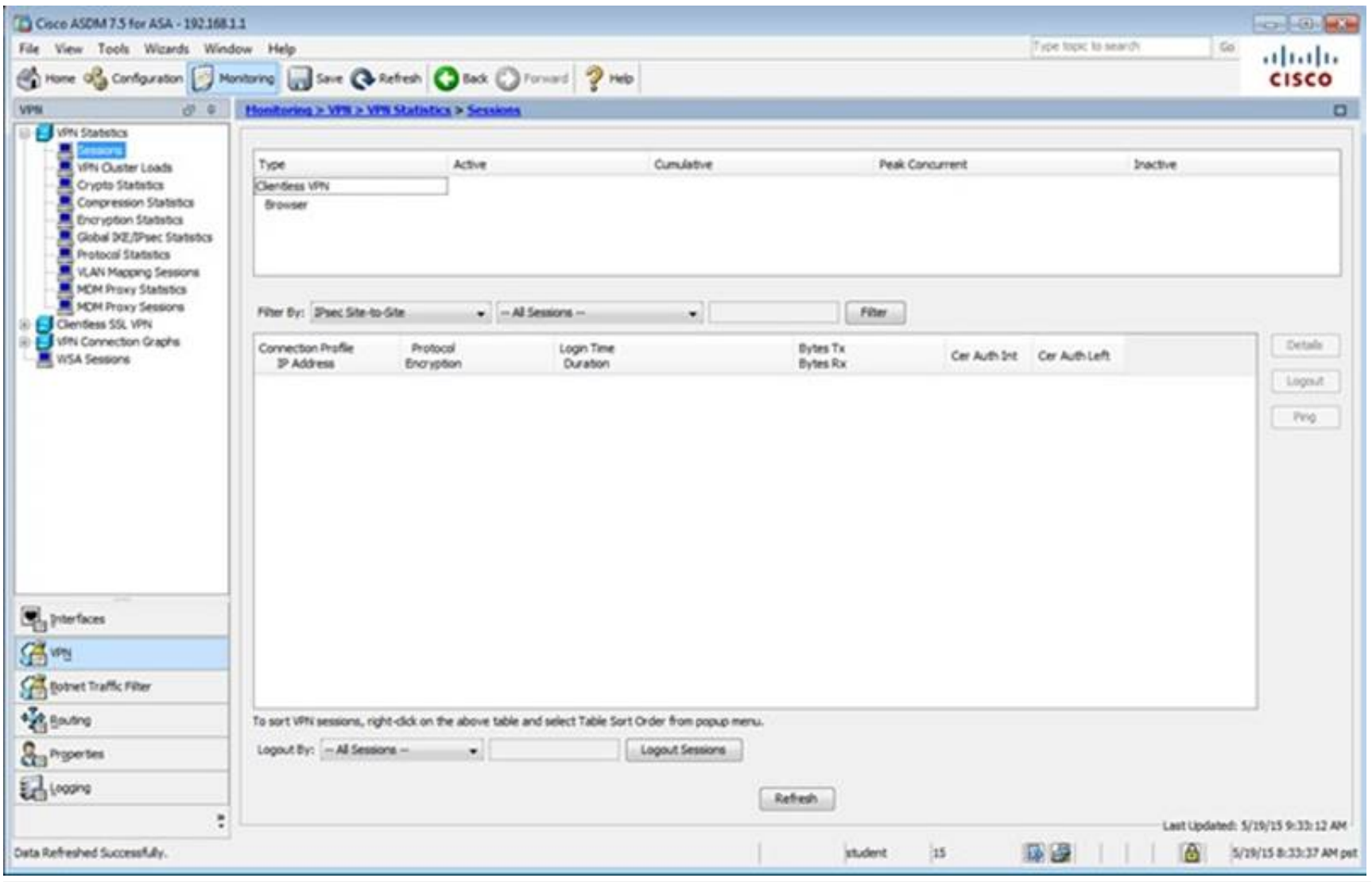
Explanation: + Block unwanted traffic at the router. If your corporate policy does not allow TFTP traffic, just implement ACLs that deny traffic that is not allowed.
+ Reduce spoofing attacks. For example, you can filter (deny) packets trying to enter your network (from the outside) that claim to have a source IP address that is from your internal network.
+ Dynamic Host Configuration Protocol (DHCP) snooping to prevent a rogue DHCP server from handing out incorrect default gateway information and to protect a DHCP server from a starvation attack Source: Cisco Official Certification Guide, Best Practices for Protecting the Data Plane , p.271

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

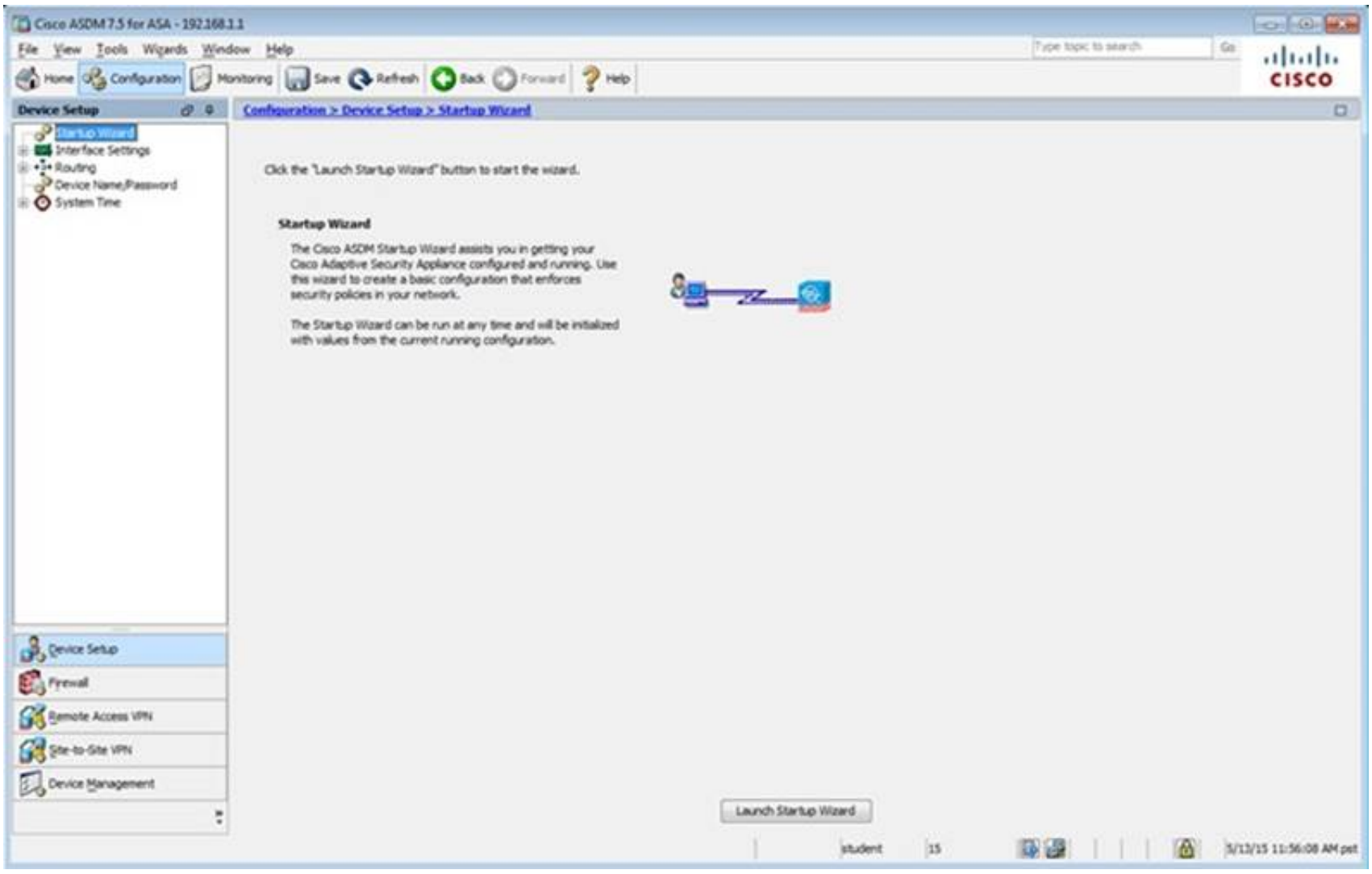

Lab Topology
Inside PC
.3
192.168.1.0/24
inside
Gi0/1
.1
Gi0/2
172.16.1.0/24
DMZ SRV
.1
dmz
.2
ASA-5512-X
outside
.2
Gi0/0
209.165.201.0/27
Fa0/0.1x
.1
2610XM
.129
209.165.202.128/27
.130
Outside SRV (Kali Linux)
Fa0/0.9x
.226
.131
Outside PC (Windows)
209.165.200.224/27
Gi0/0.9x
.225
Gi0/1
Internet

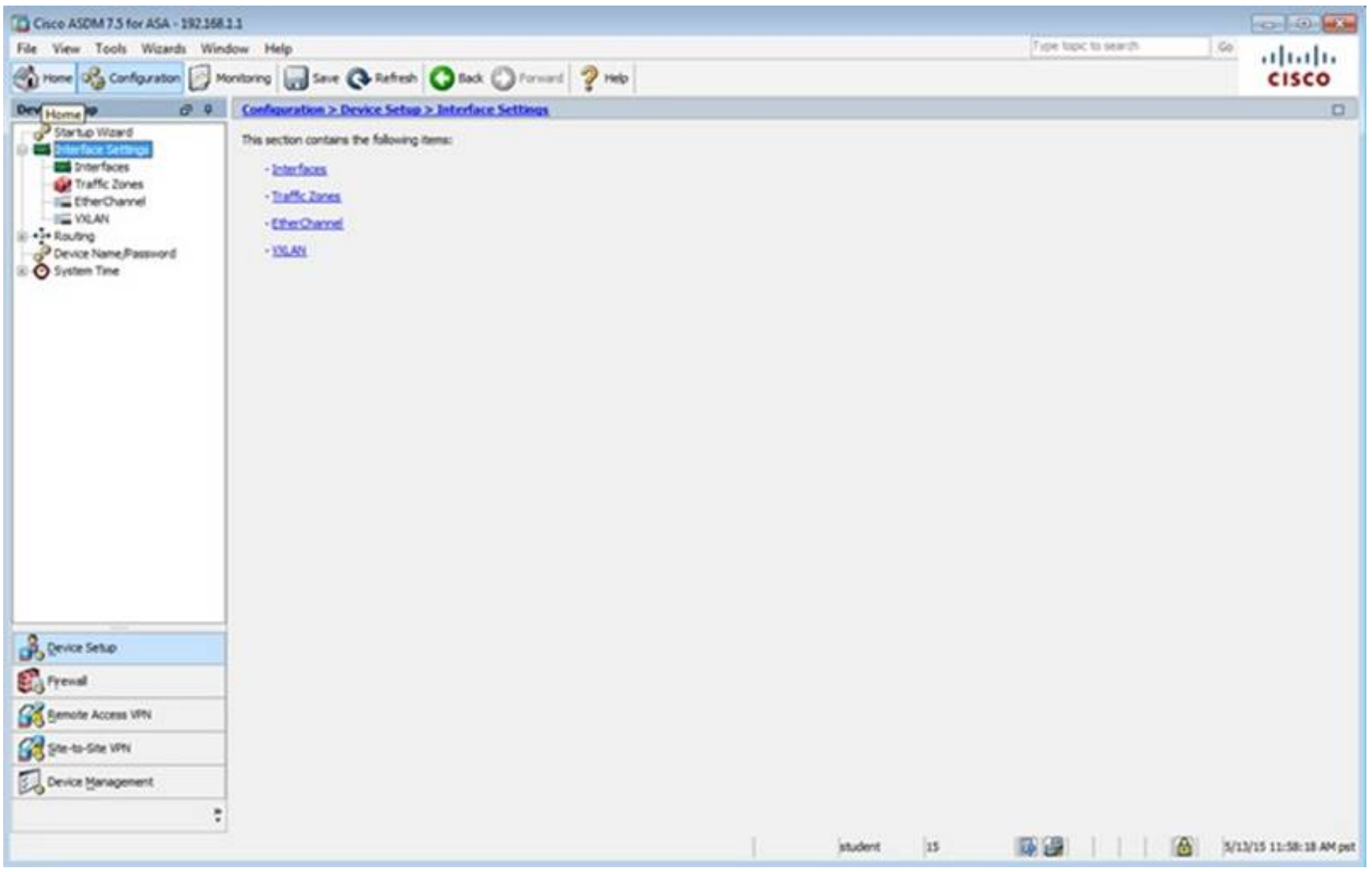

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License
Host Name: P17-ASA.secure-x.local
ASA Version: 100.14(6)13
ASDM 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

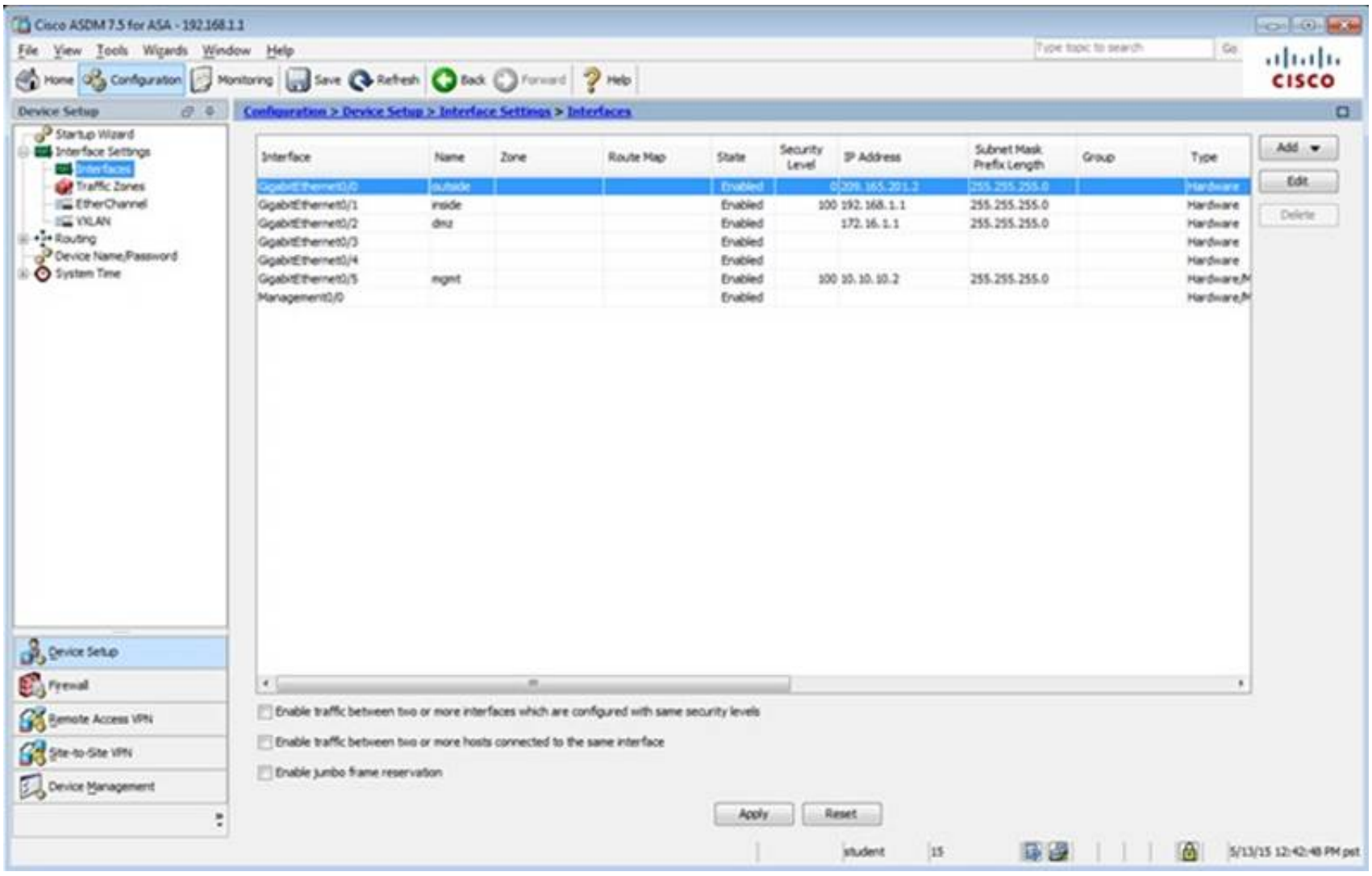

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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

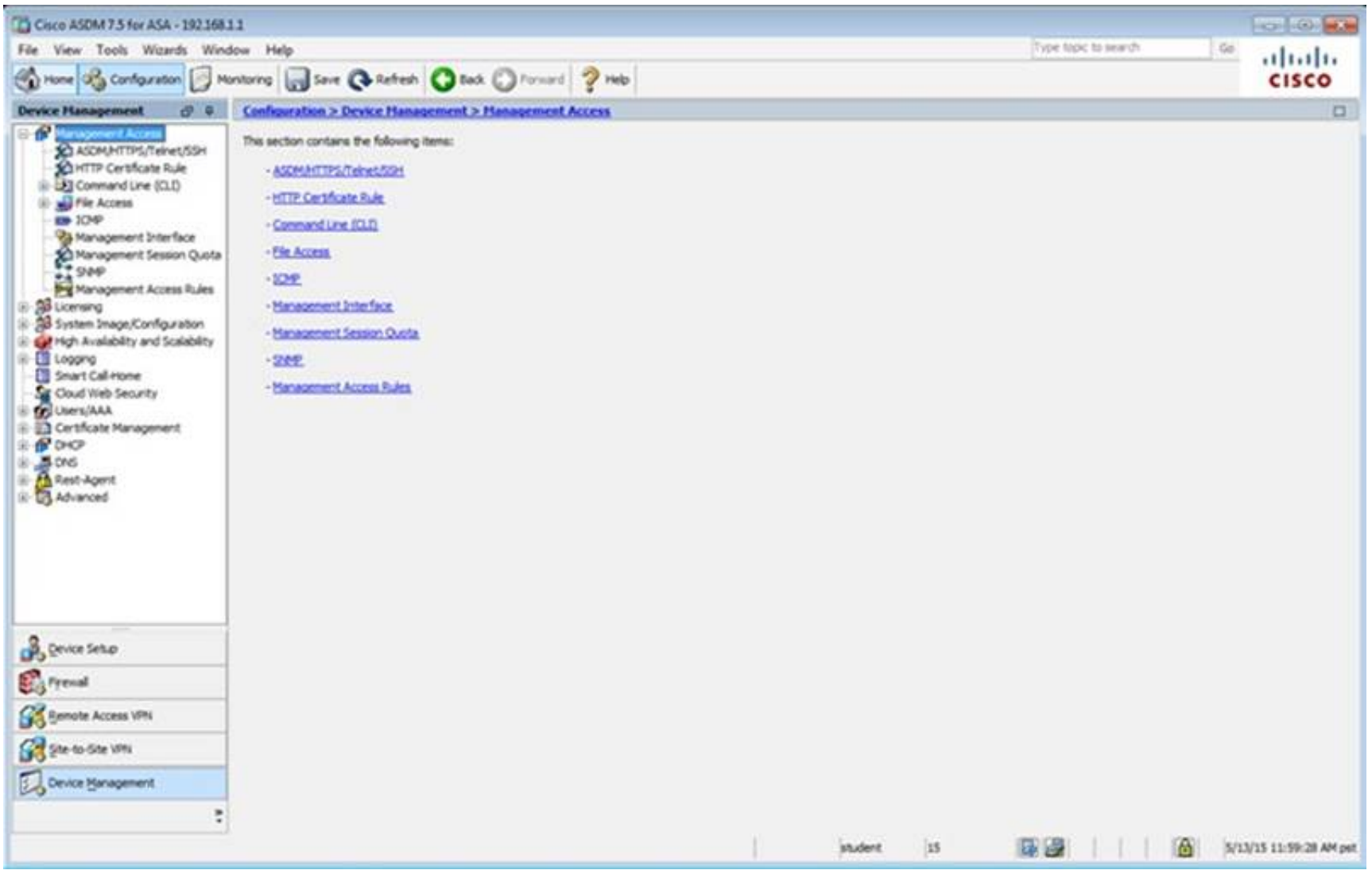

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN 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: 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

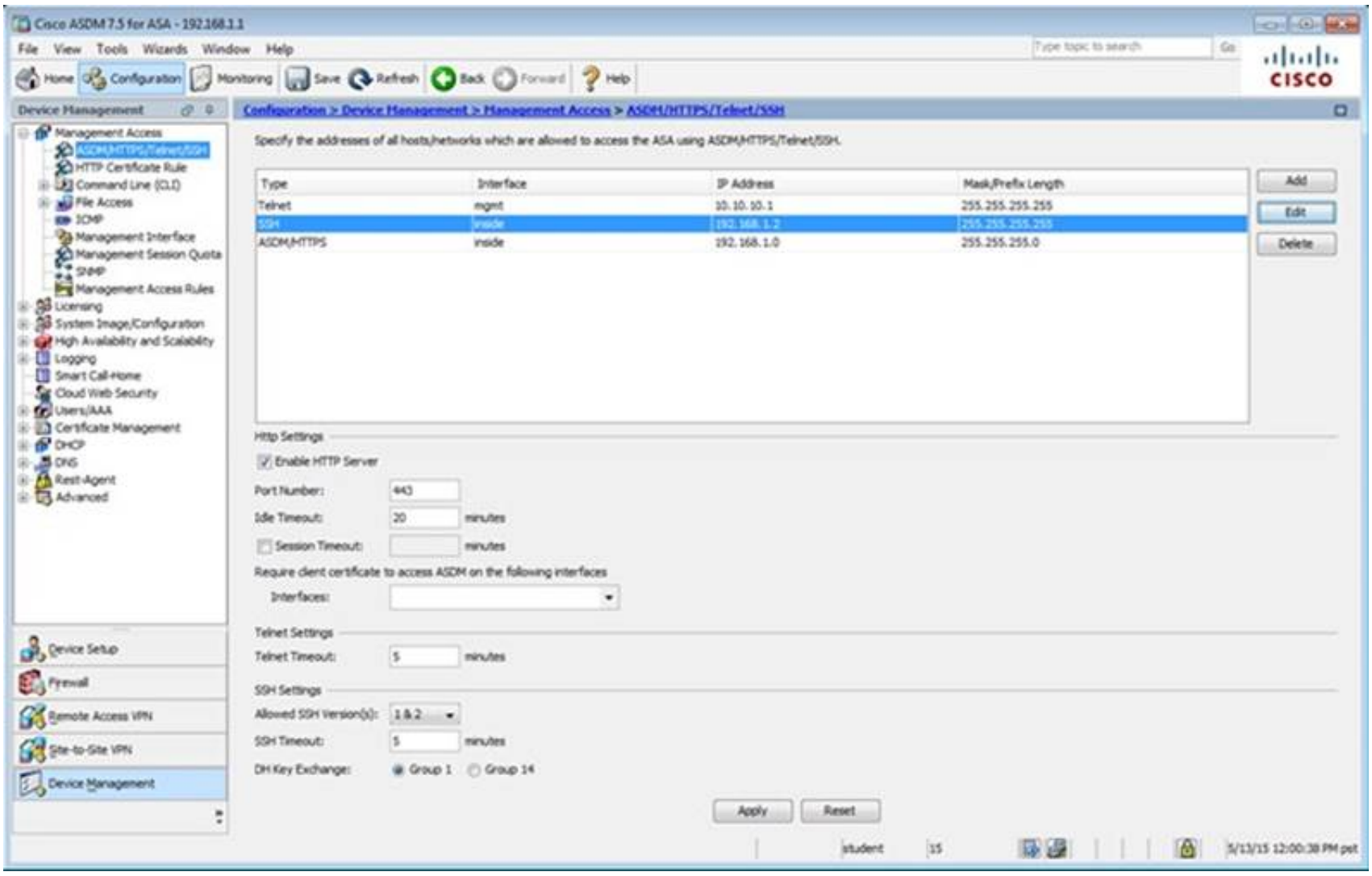

Filter By: Clientless SSL VPN -- All Sessions -- Filter

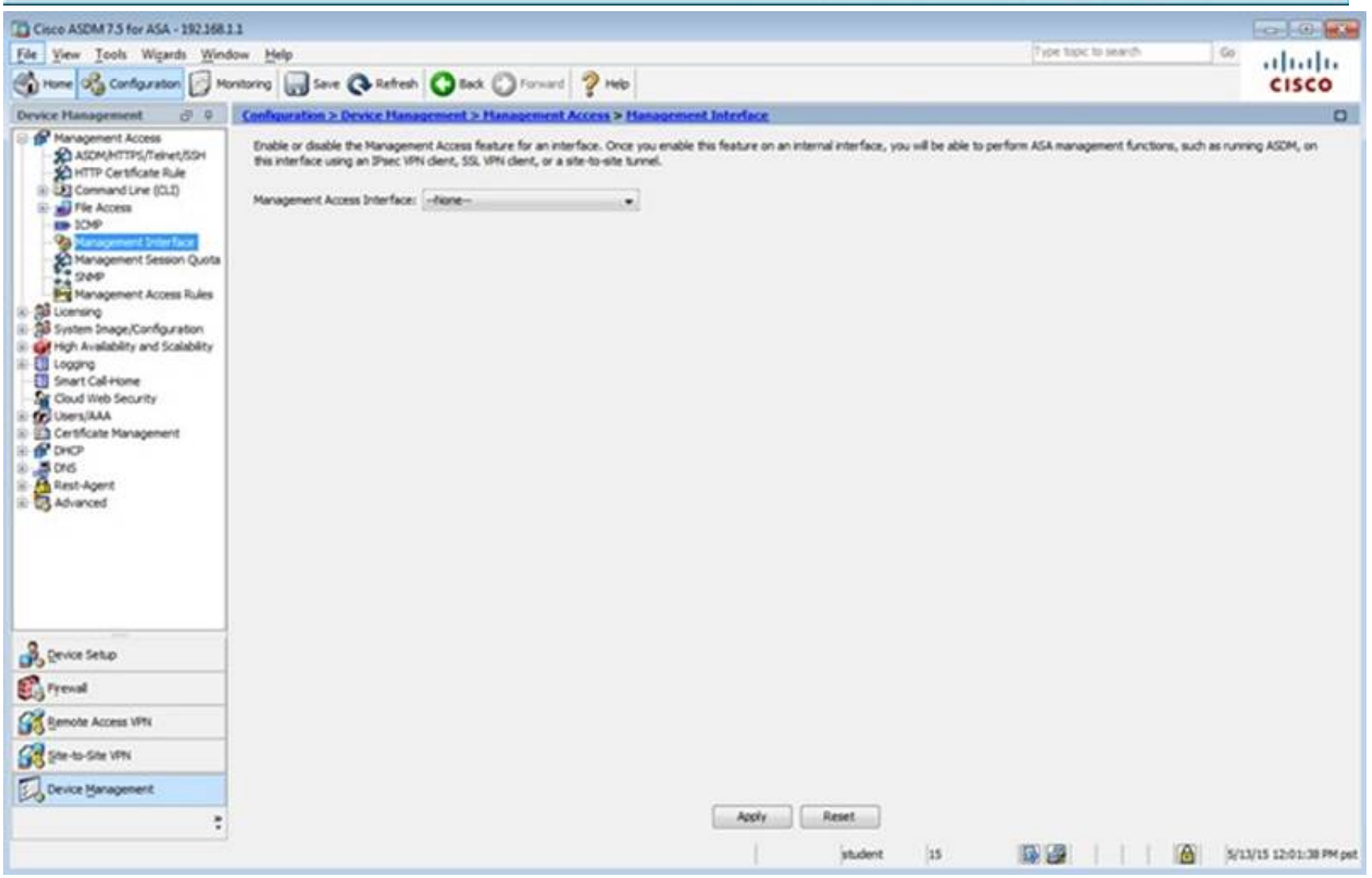

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" 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

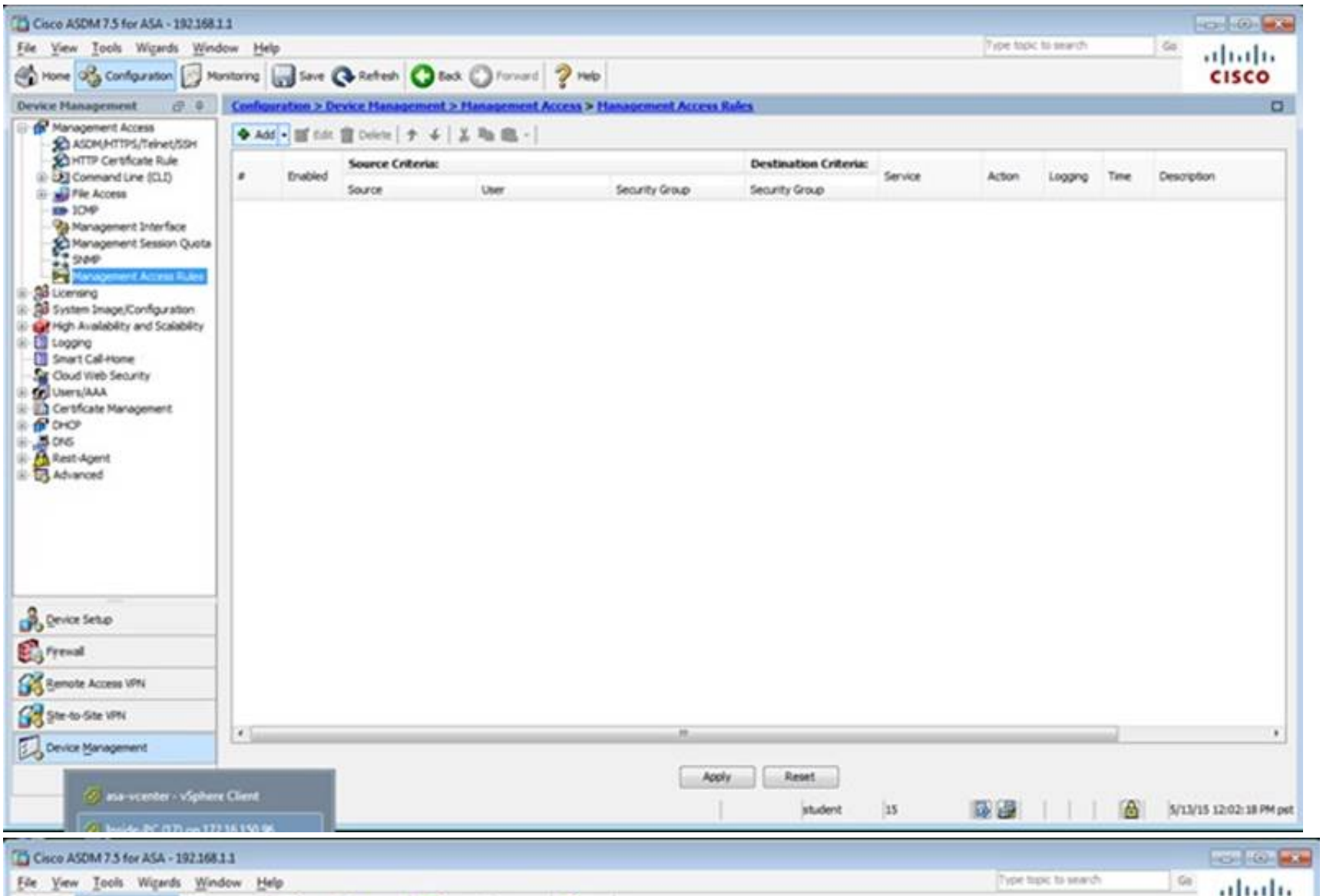

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interface 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

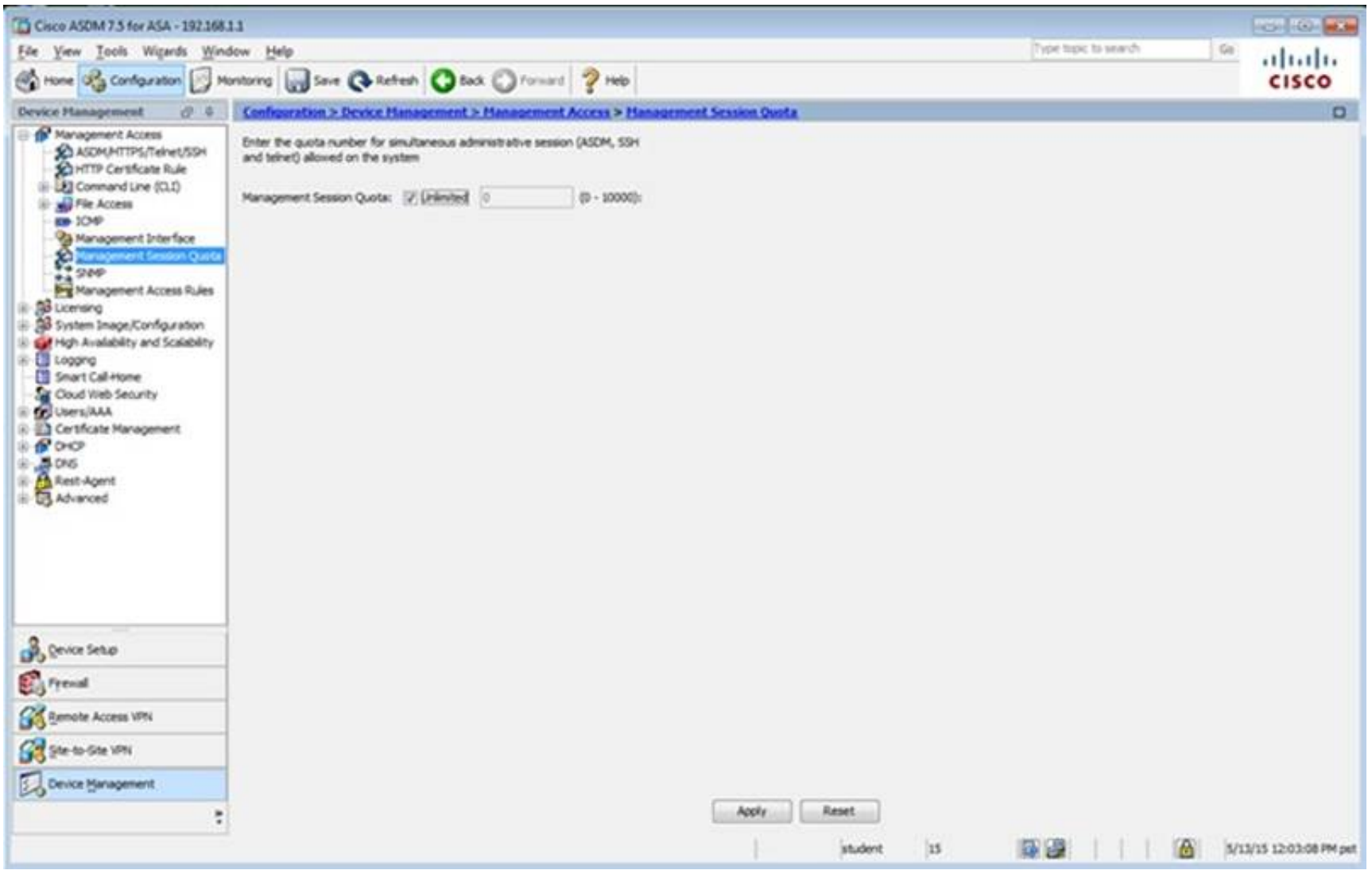

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Configuration > Device Setup > Interface Settings > Interfaces
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
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

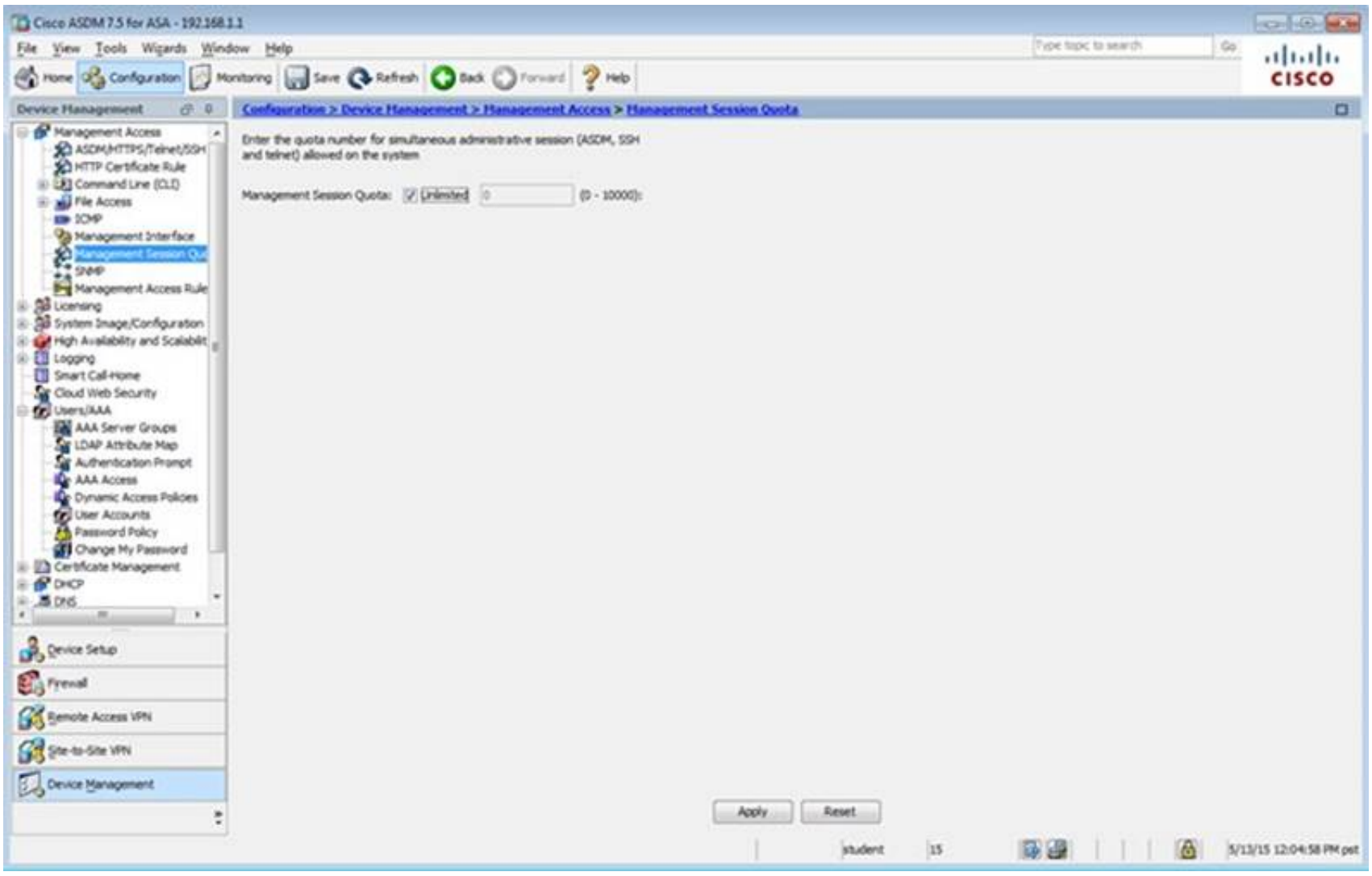

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
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

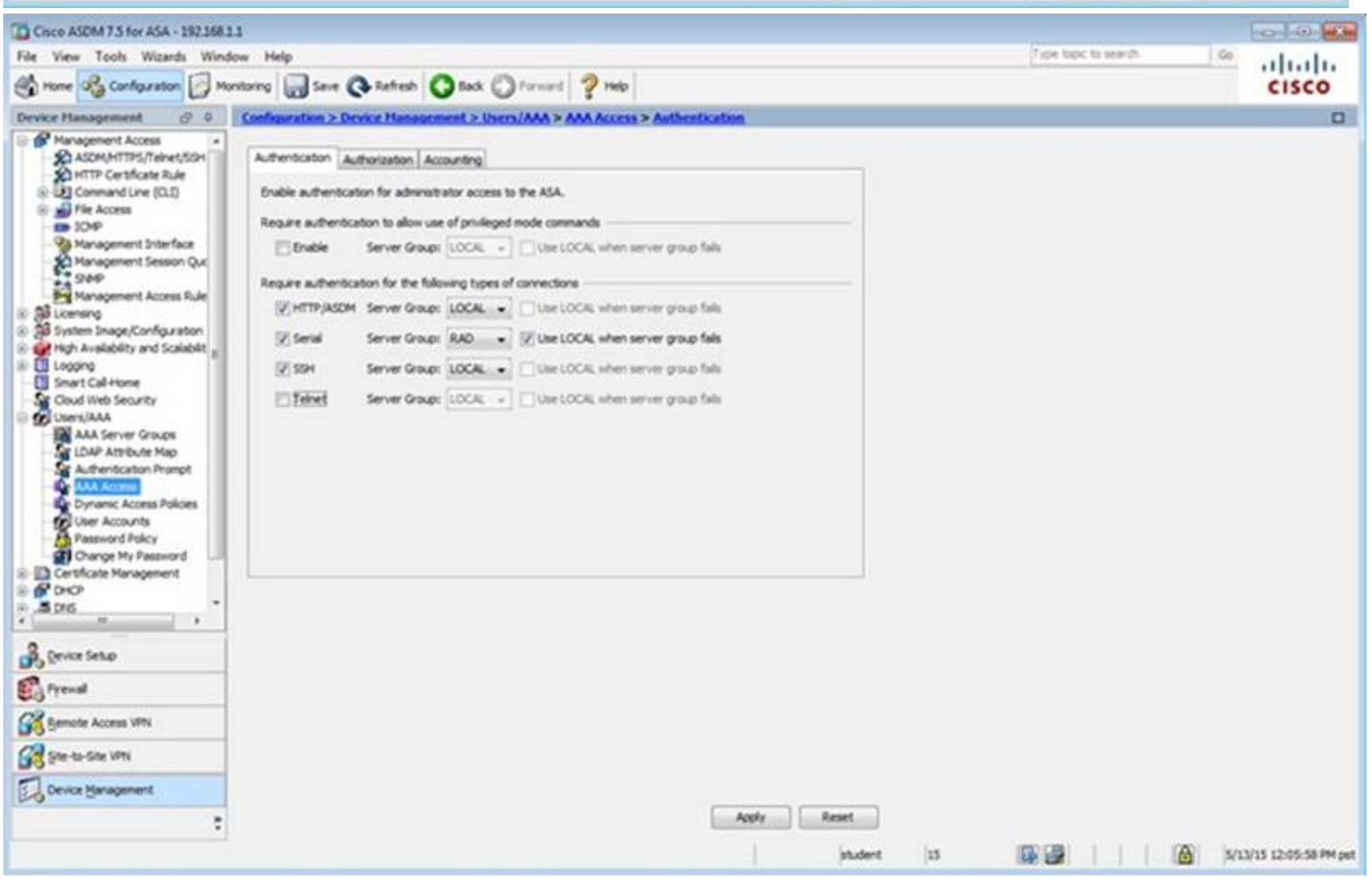

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Specify the addresses of all hosts/networks which are allowed to 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

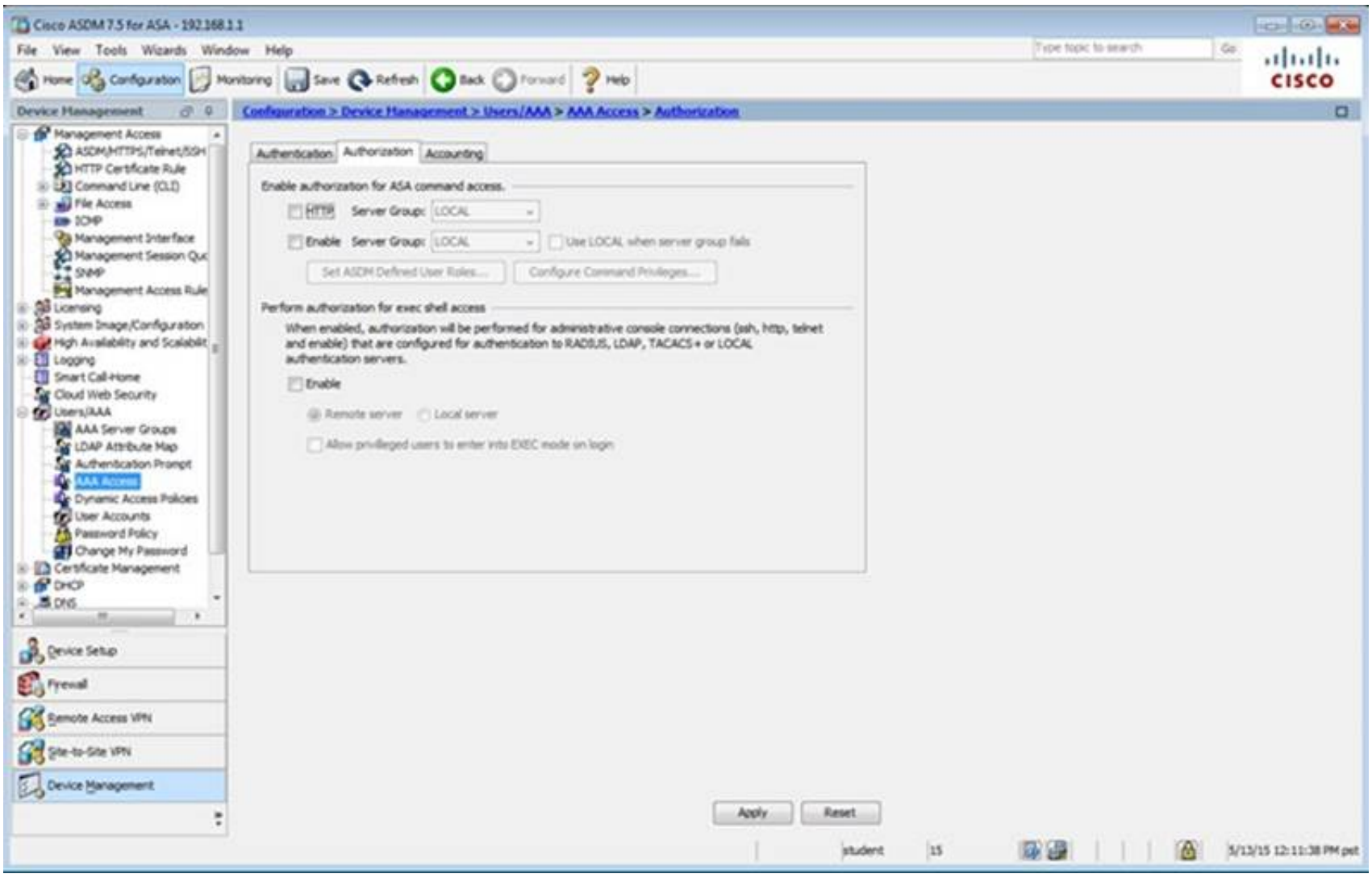

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Enable or disable the Management Access feature for an interface.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

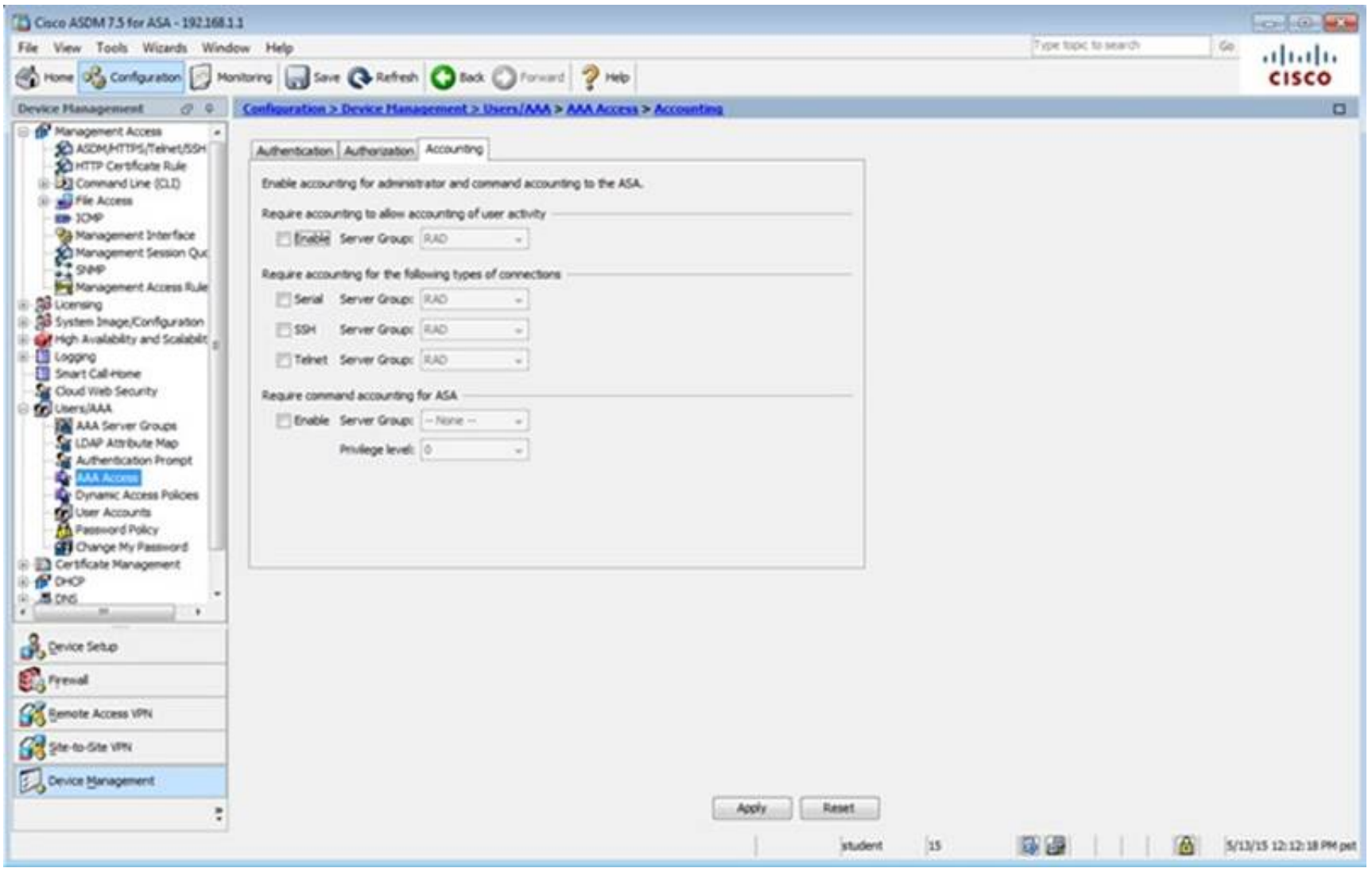

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Access Rules
Add Edit Delete
Enabled Source Criteria: Source User Security Group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

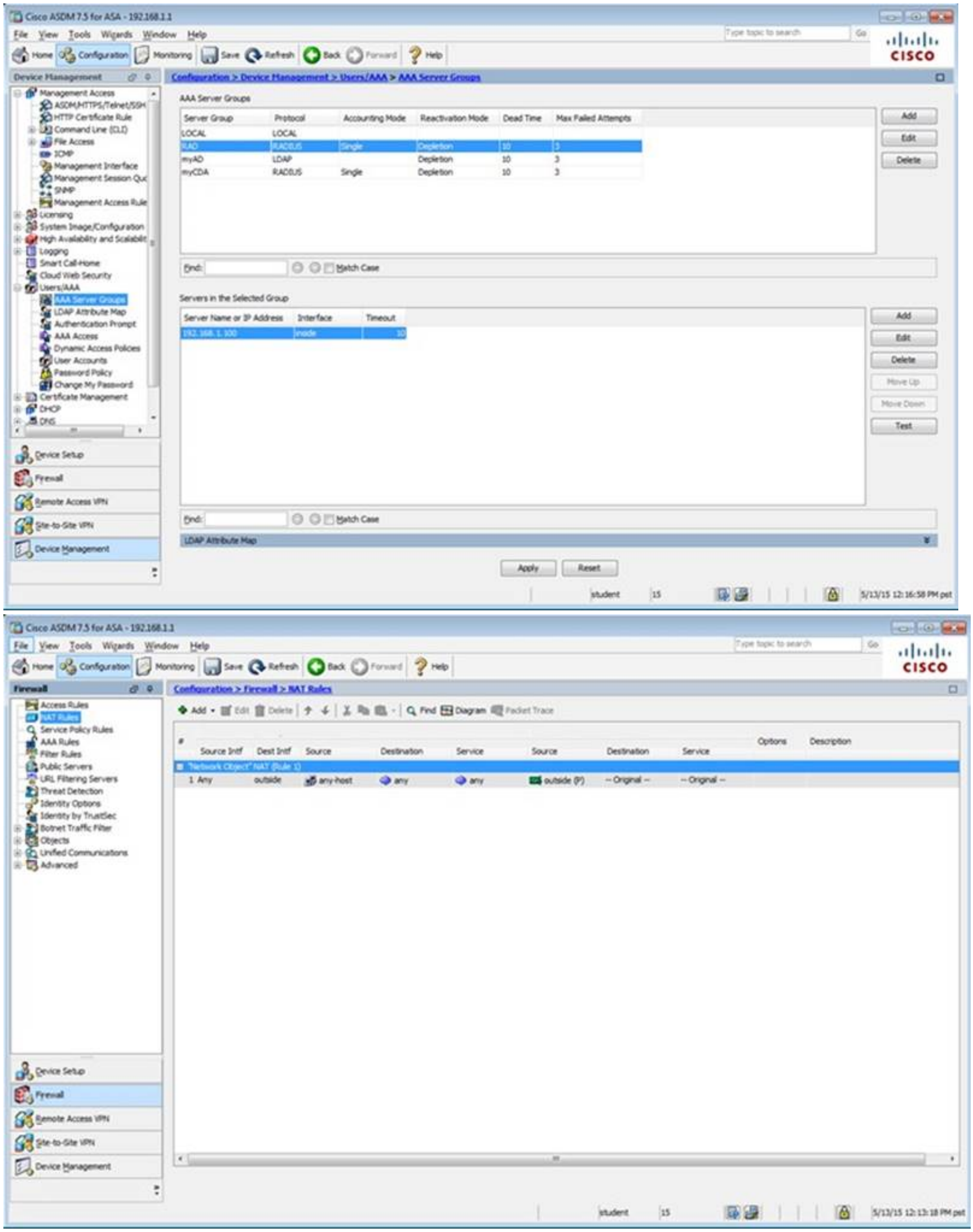

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (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 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:04:58 PM pst

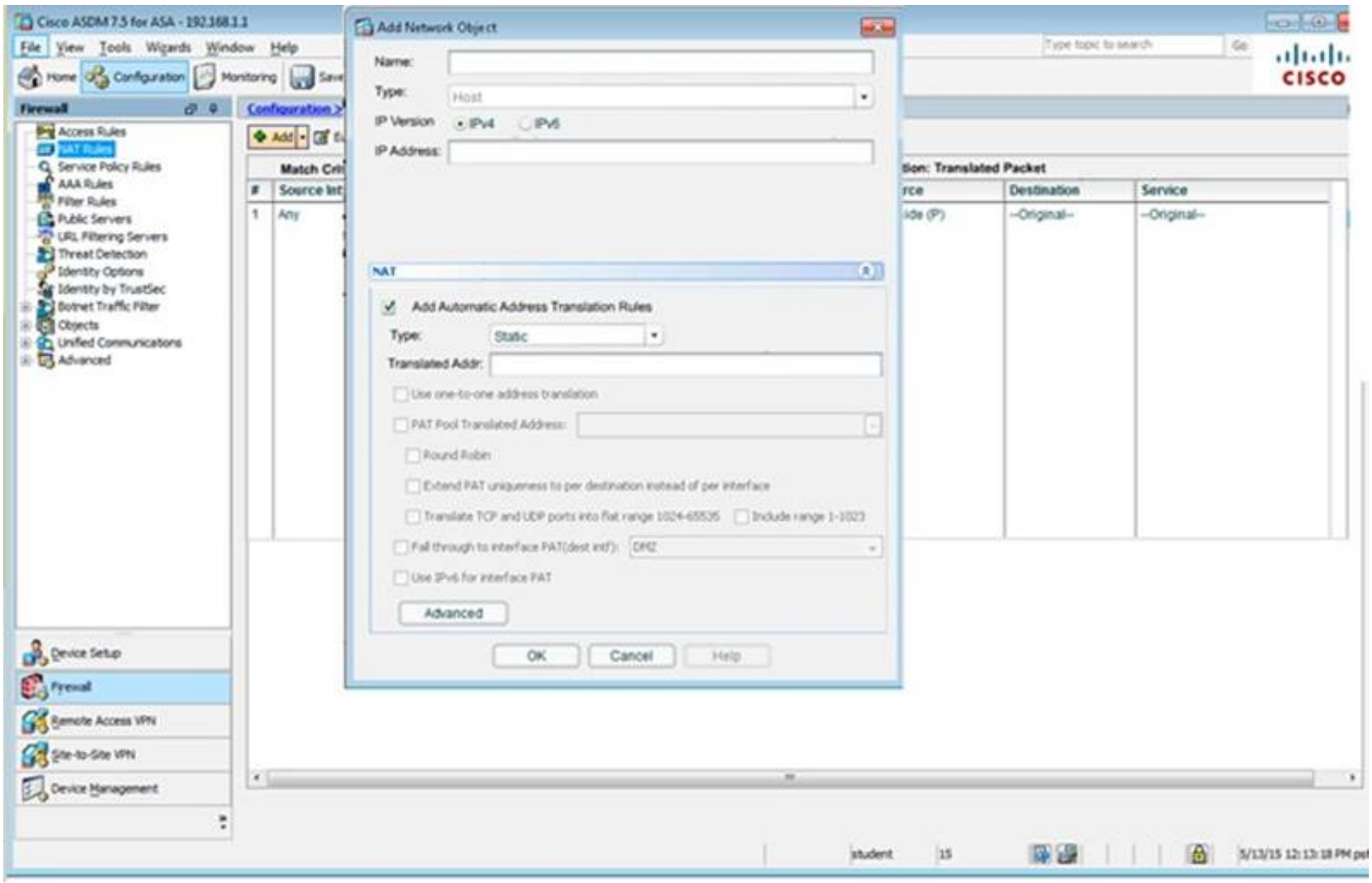

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Authorization Accounting
Enable authentication for administrator 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 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/13/15 12:05:58 PM pst

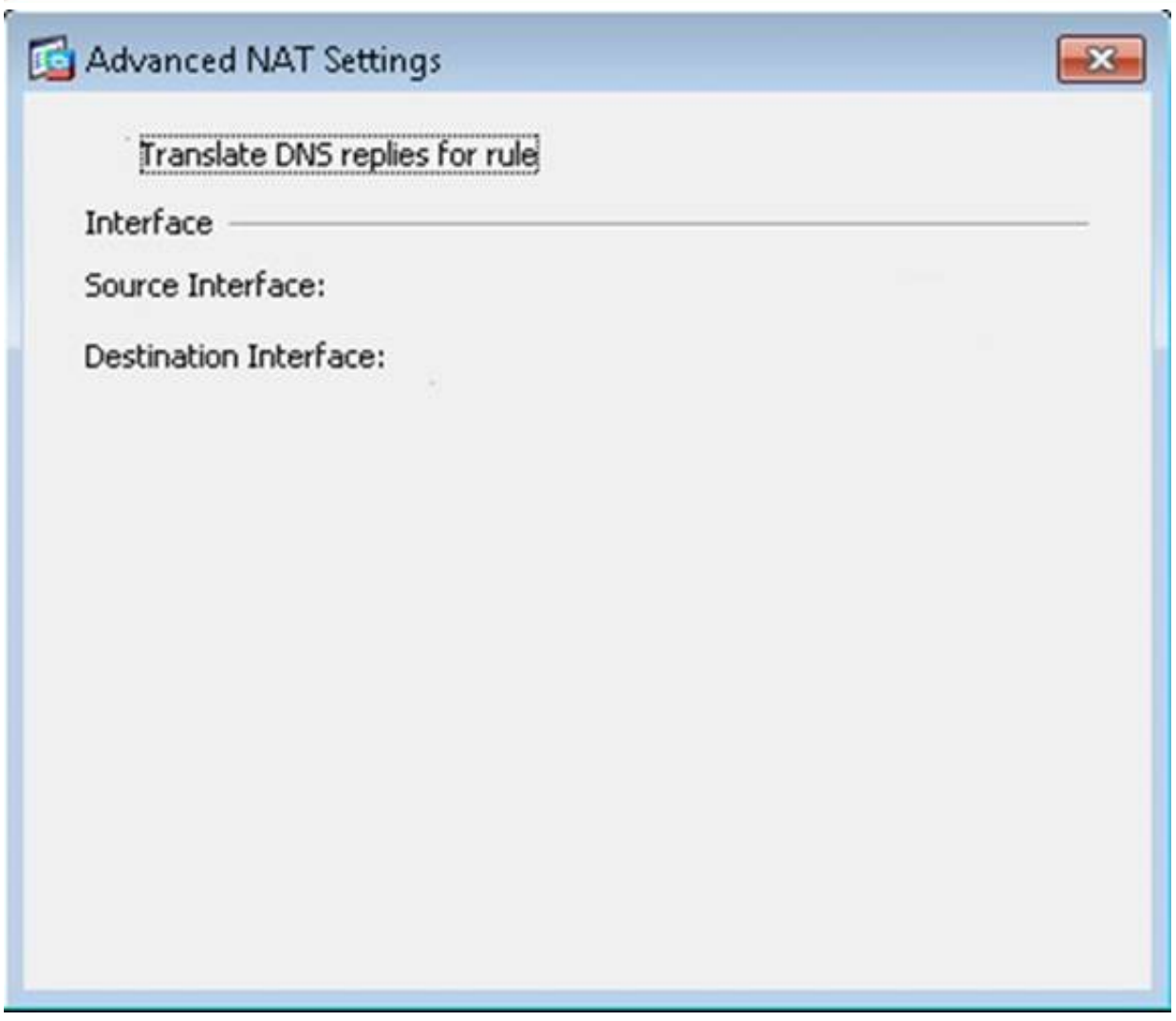

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Enable authorization for ASA 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

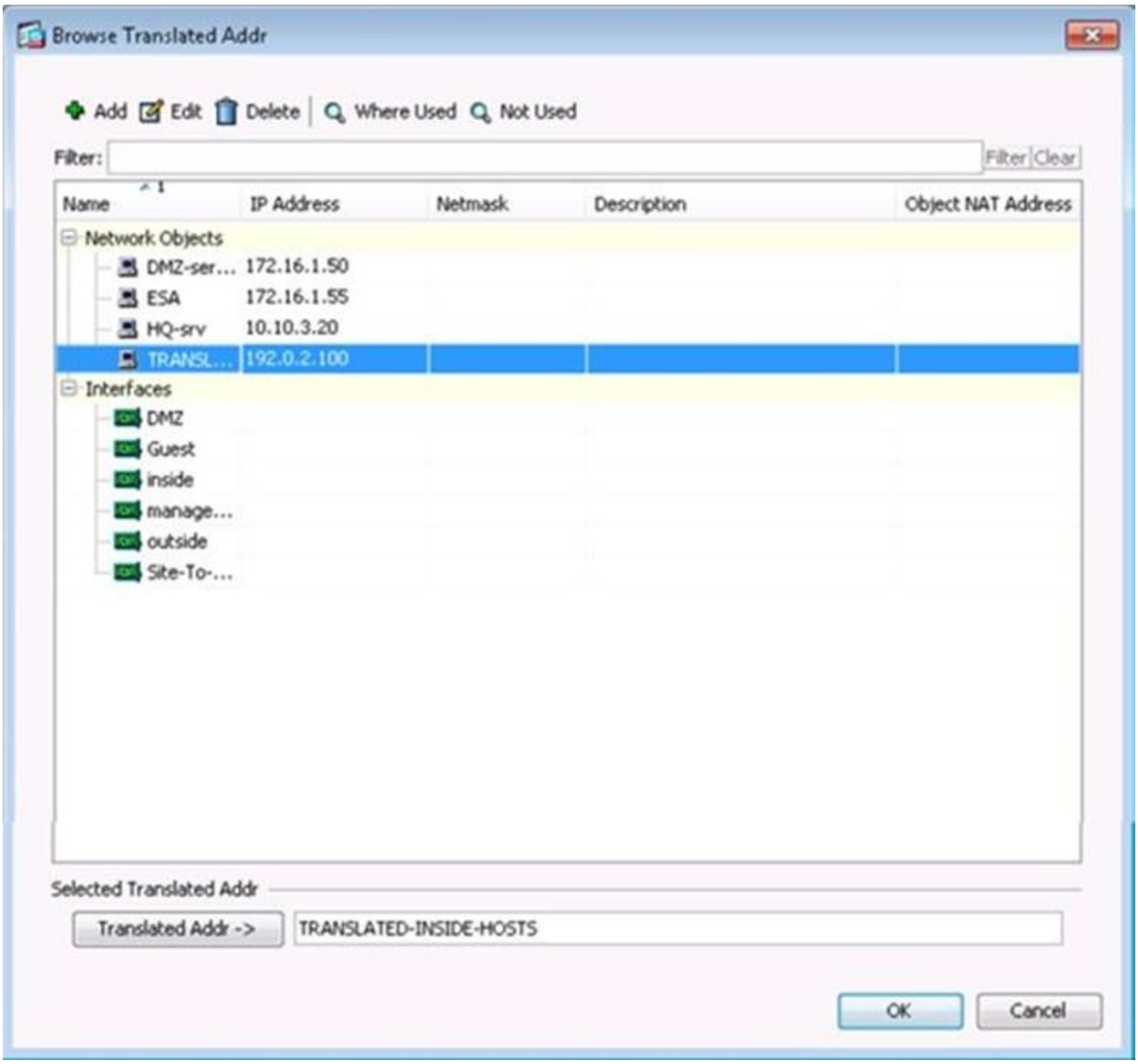

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Authentication Authorization Accounting
Enable accounting for administrator 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

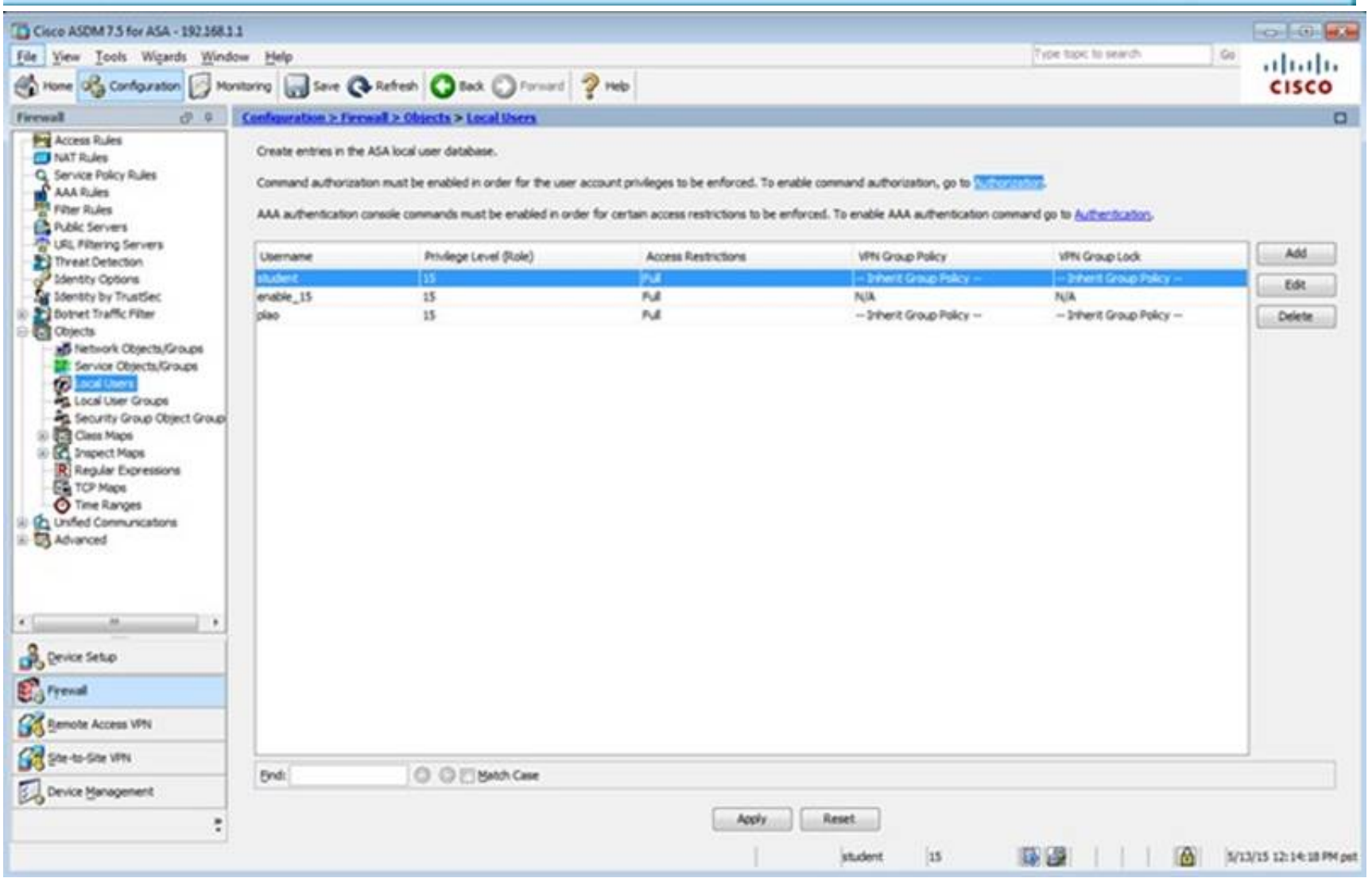

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Server Groups
AAA Server Groups
Server Group Protocol Accounting Mode Reactivation Mode Dead 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

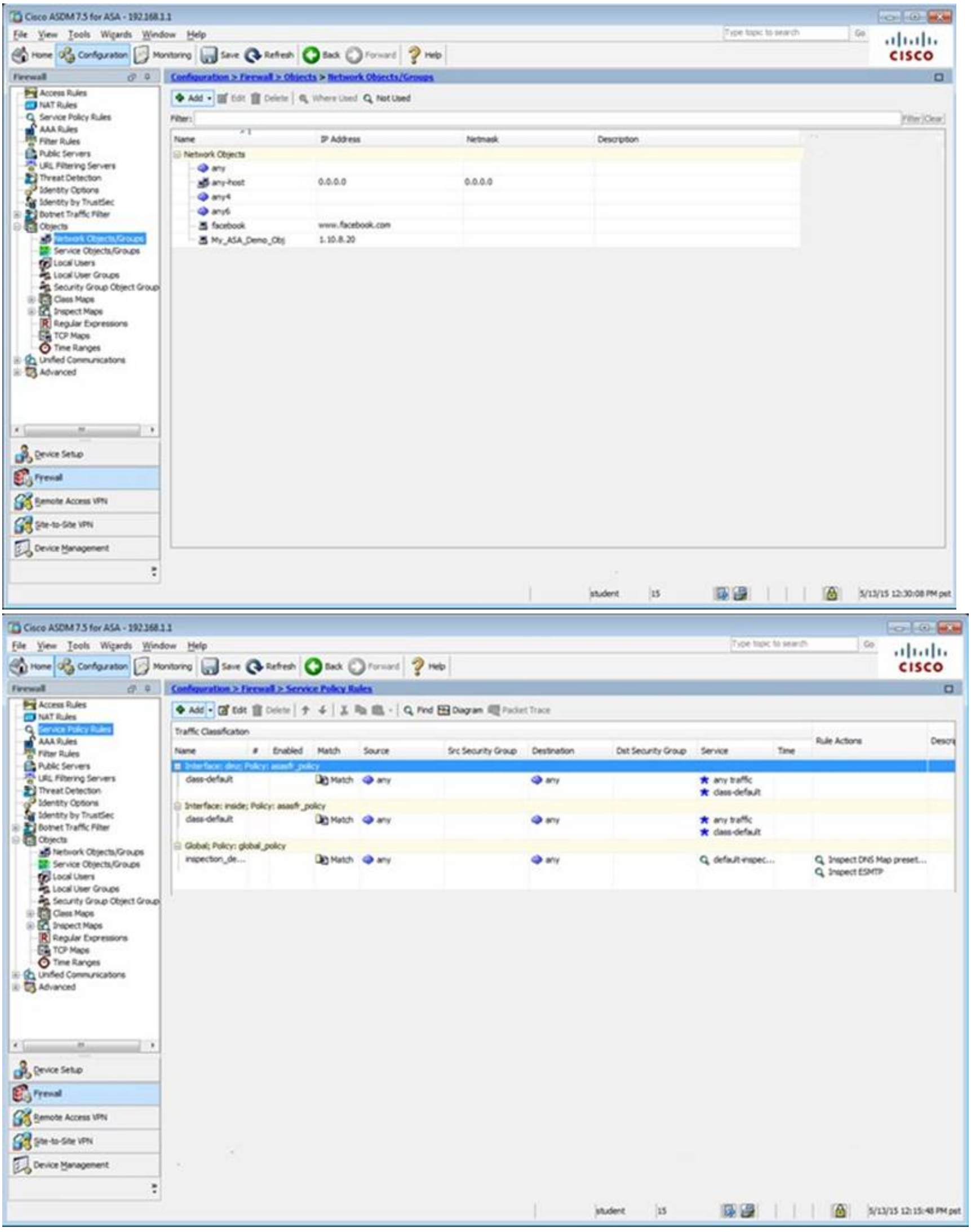
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Source Intf Dest Intf Source Destination Service Source Destination Service 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

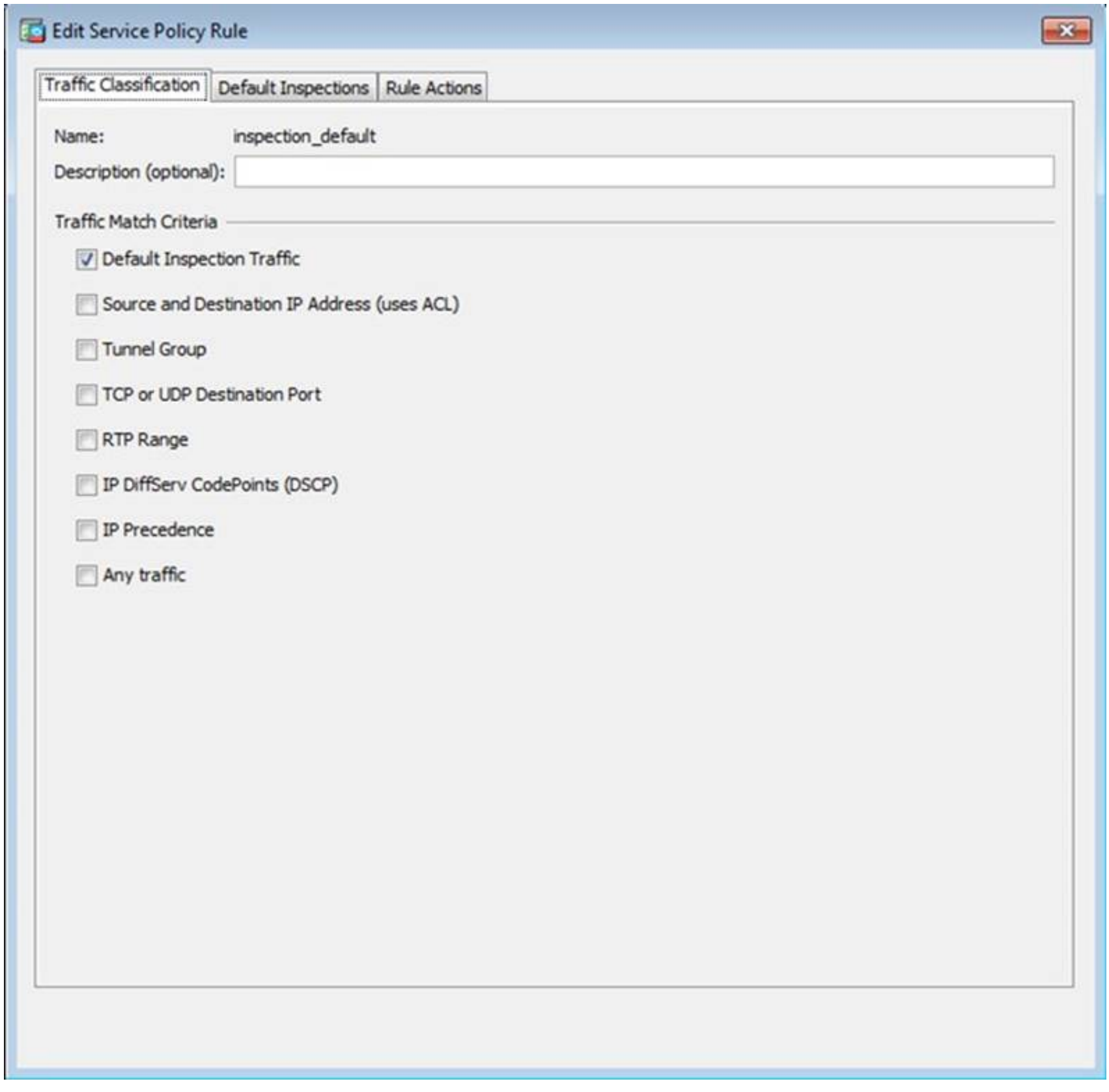

Advanced NAT Settings
Translate DNS replies for rule
Interface
Source Interface:
Destination Interface:

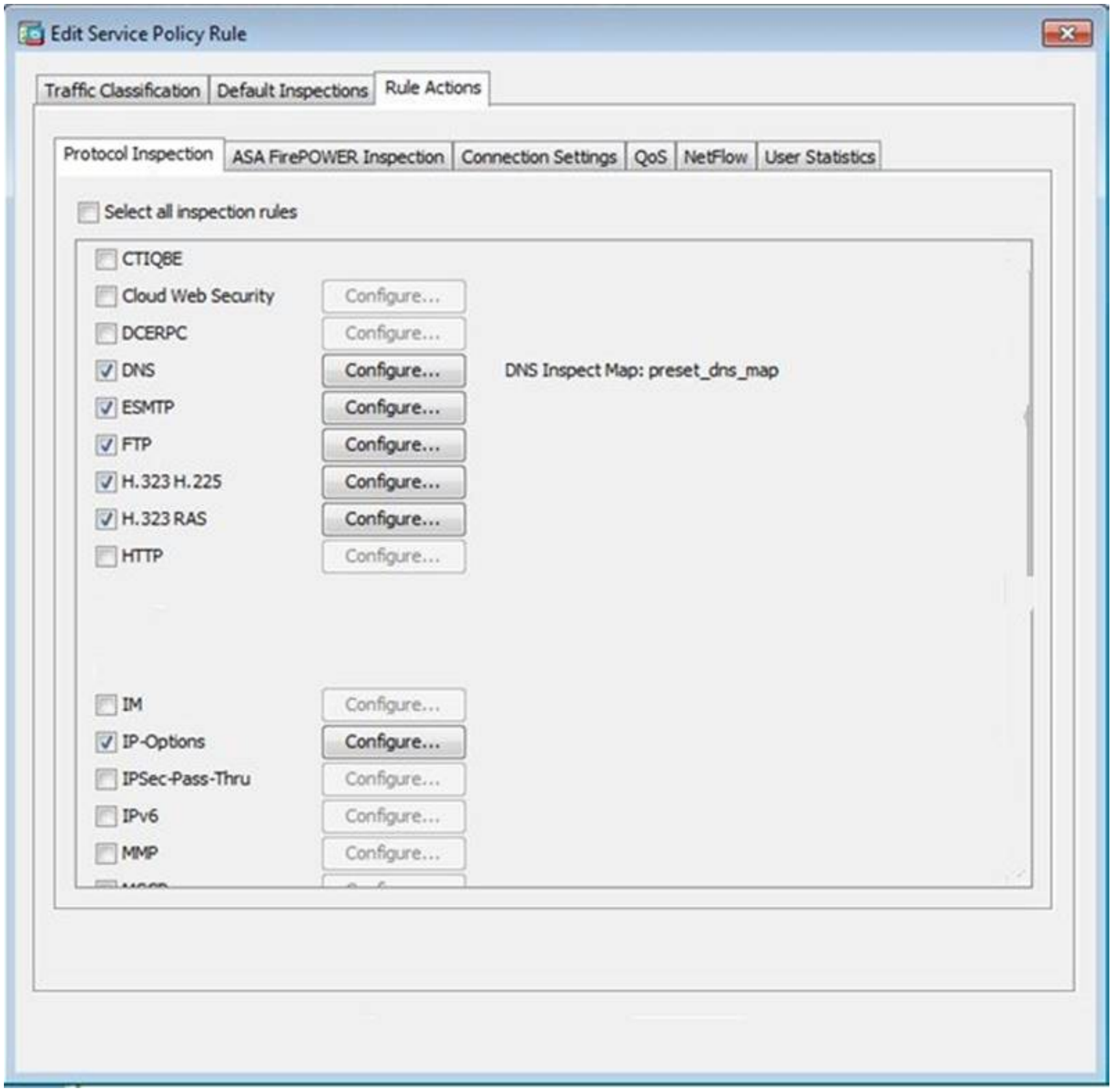

Browse Translated Addr
Add
Edit
Delete
Where Used
Not Used
Filter:
Filter
Clear
Name
IP Address
Netmask
Description
Object NAT Address
Network Objects
DMZ-ser...
172.16.1.50
ESA
172.16.1.55
HQ-srv
10.10.3.20
TRANSL...
192.0.2.100
Interfaces
DMZ
Guest
inside
manage...
outside
Site-To-...
Selected Translated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

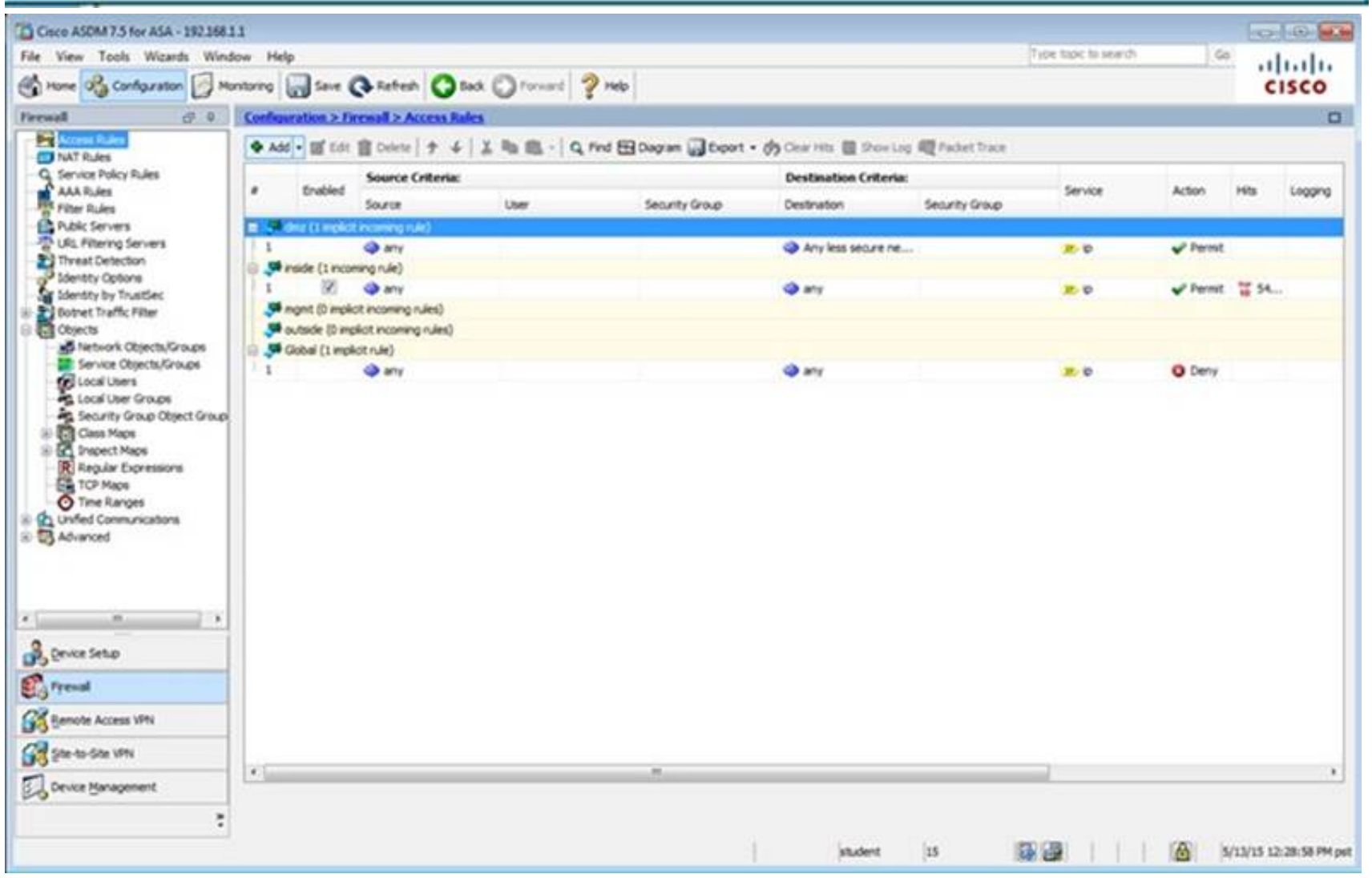

Cisco ASDM 7.5 for ASA - 192.168.1.1
File
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Network Objects/Groups
Service Objects/Groups
Local Users
Local User Groups
Security Group Object Group
Class Maps
Inspect Maps
Regular Expressions
TCP Maps
Time Ranges
Unified Communications
Advanced
Configuration > Firewall > 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
3/13/15 12:14:18 PM pst

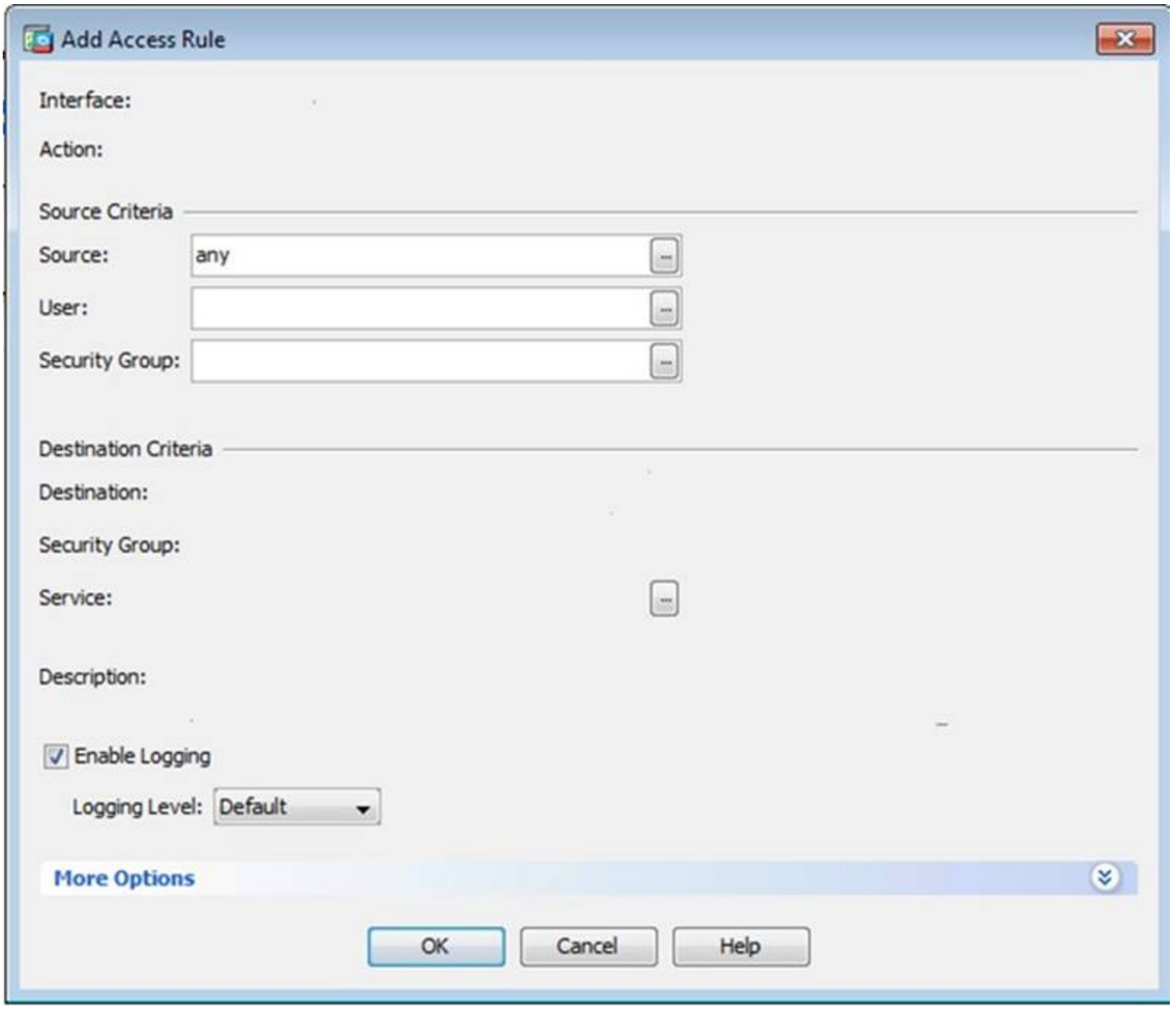

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Filter:
Name IP Address Netmask Description
Network Objects
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

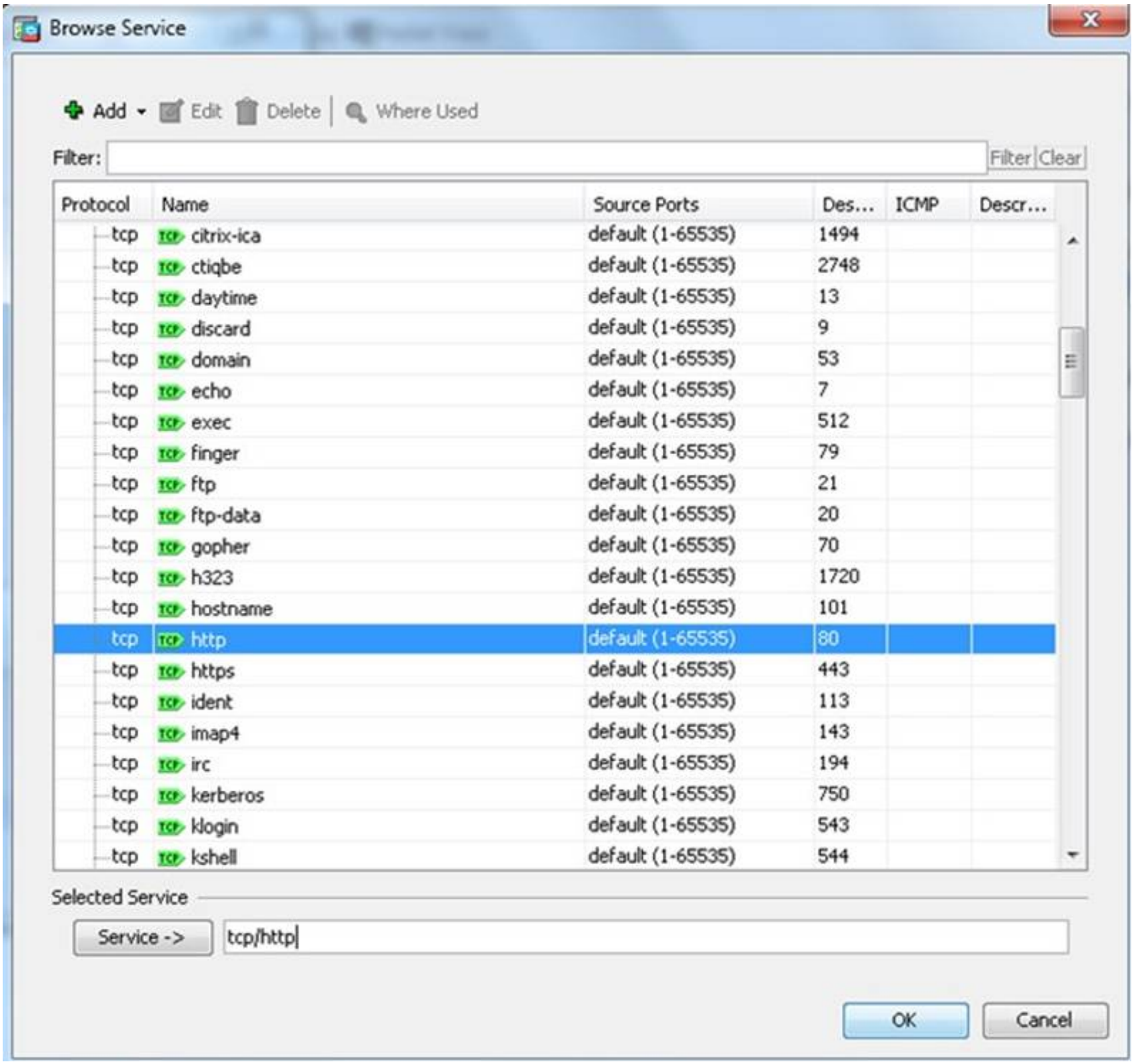
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security 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

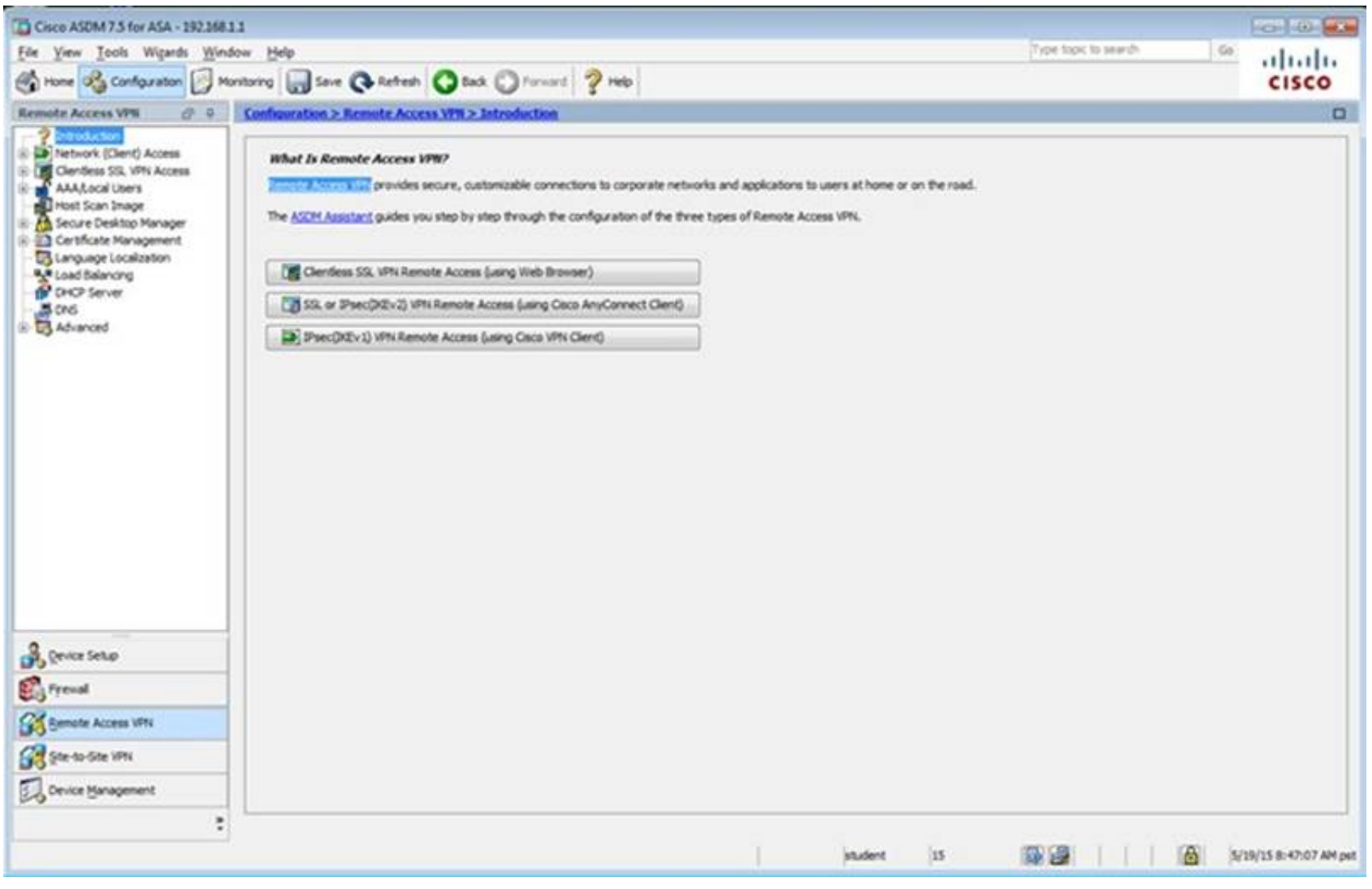

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Name:
inspection_default
Description (optional):
Traffic Match Criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
Tunnel Group
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)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

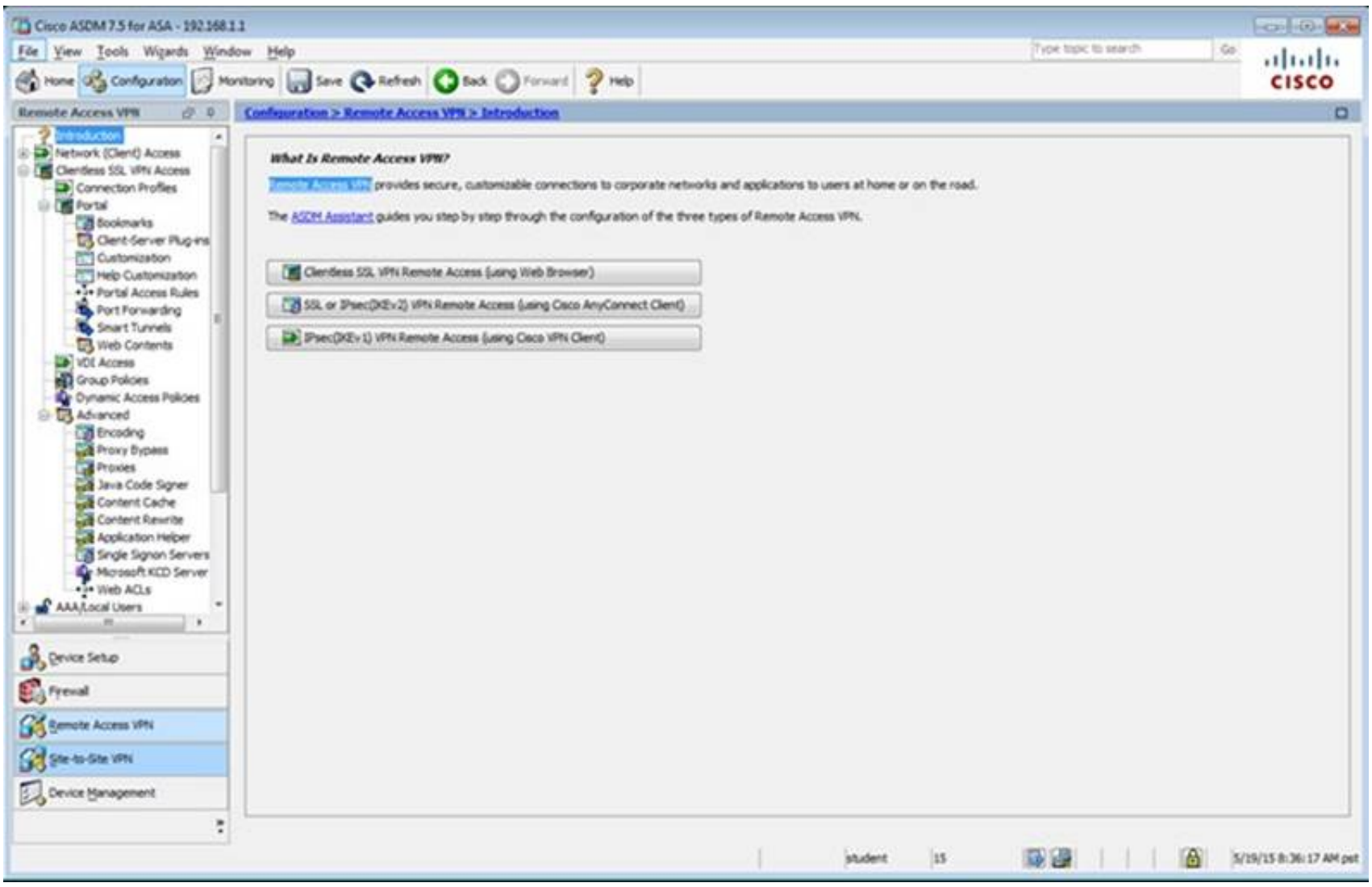

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Protocol Inspection
ASA FirePOWER Inspection
Connection Settings
QoS
NetFlow
User Statistics
Select all inspection rules
CTIQBE
Cloud Web Security
Configure...
DCERPC
Configure...
DNS
Configure...
DNS Inspect Map: preset_dns_map
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...

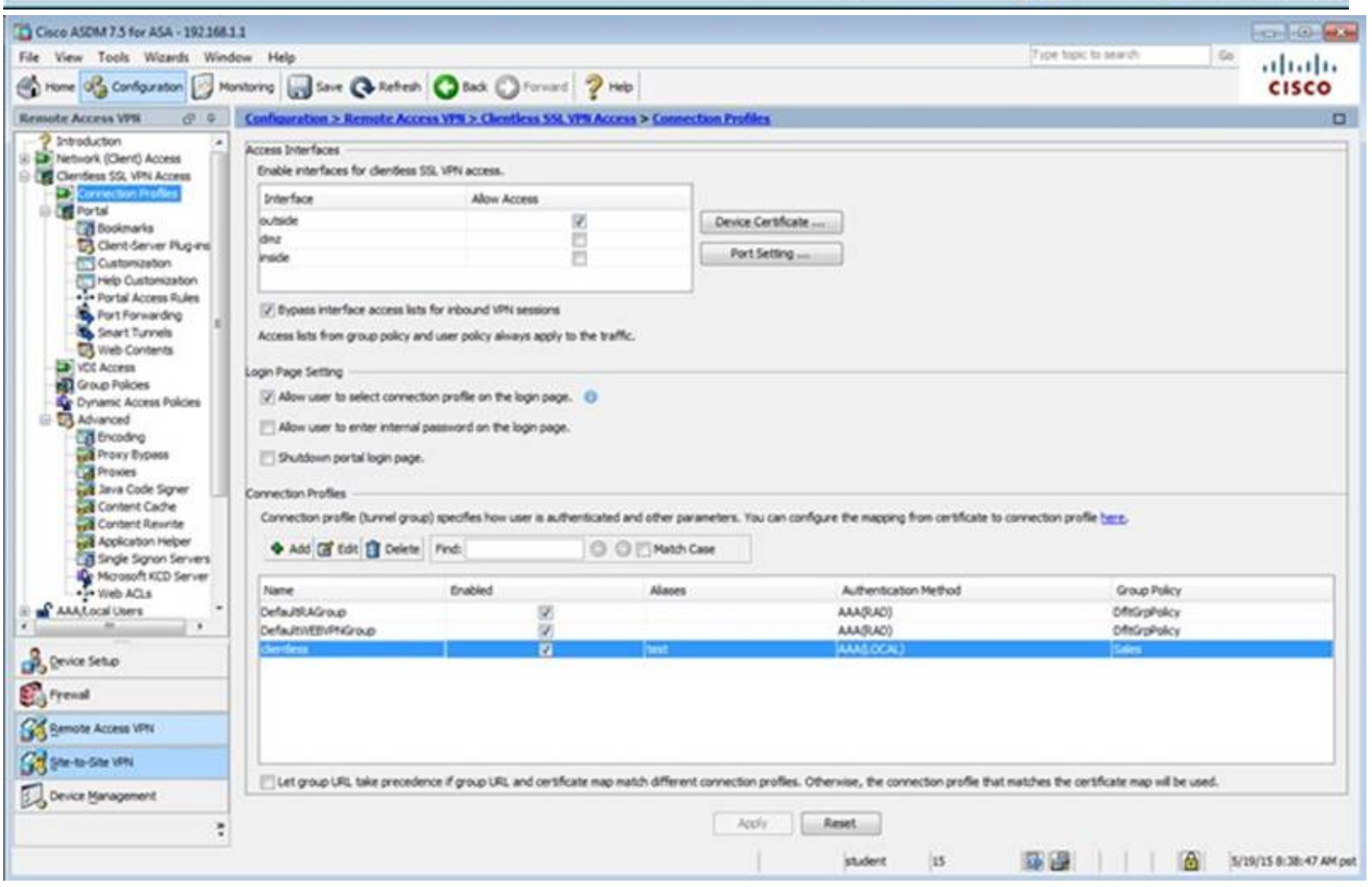

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria:
Destination Criteria:
Enabled
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

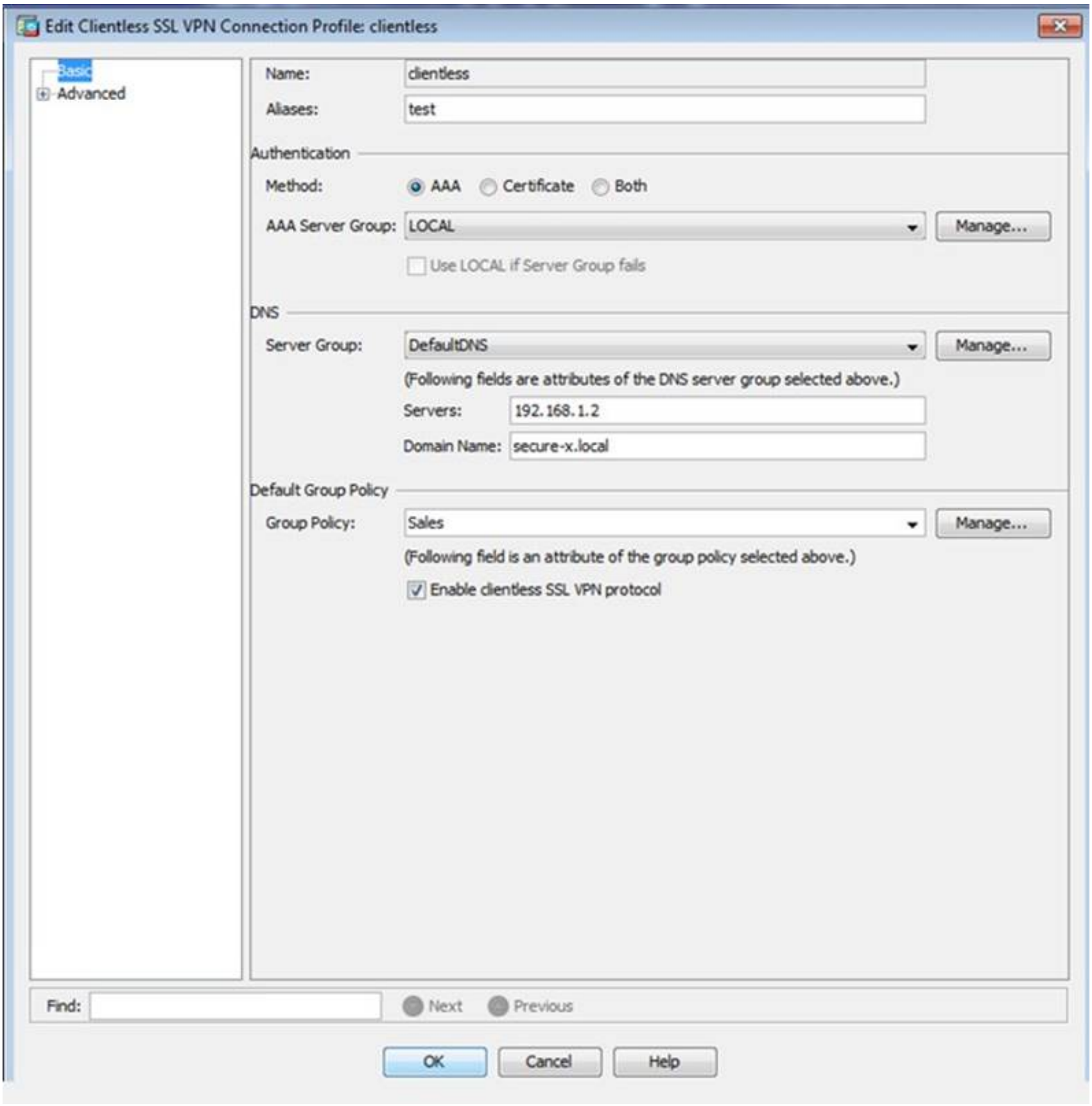

Add Access Rule
Interface:
Action:
Source Criteria
Source:
any
User:
Security Group:
Destination Criteria
Destination:
Security Group:
Service:
Description:
Enable Logging
Logging Level:
Default
More Options
OK
Cancel
Help

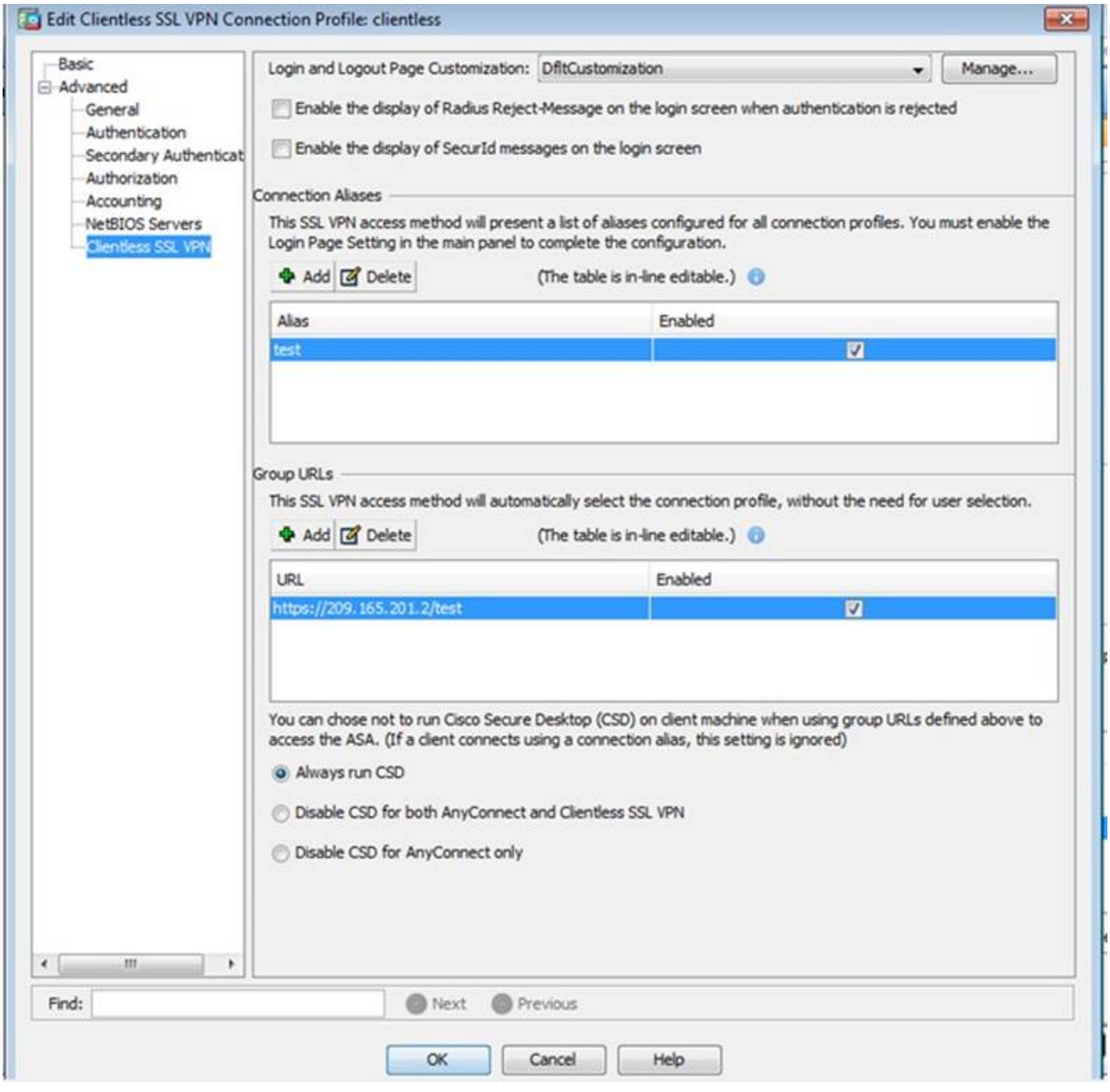

Browse Service
Add
Edit
Delete
Where Used
Filter:
Filter
Clear
Protocol
Name
Source Ports
Des...
ICMP
Descr...
tcp citrix-ica default (1-65535) 1494
tcp ctiqbe default (1-65535) 2748
tcp daytime default (1-65535) 13
tcp discard default (1-65535) 9
tcp domain default (1-65535) 53
tcp echo default (1-65535)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

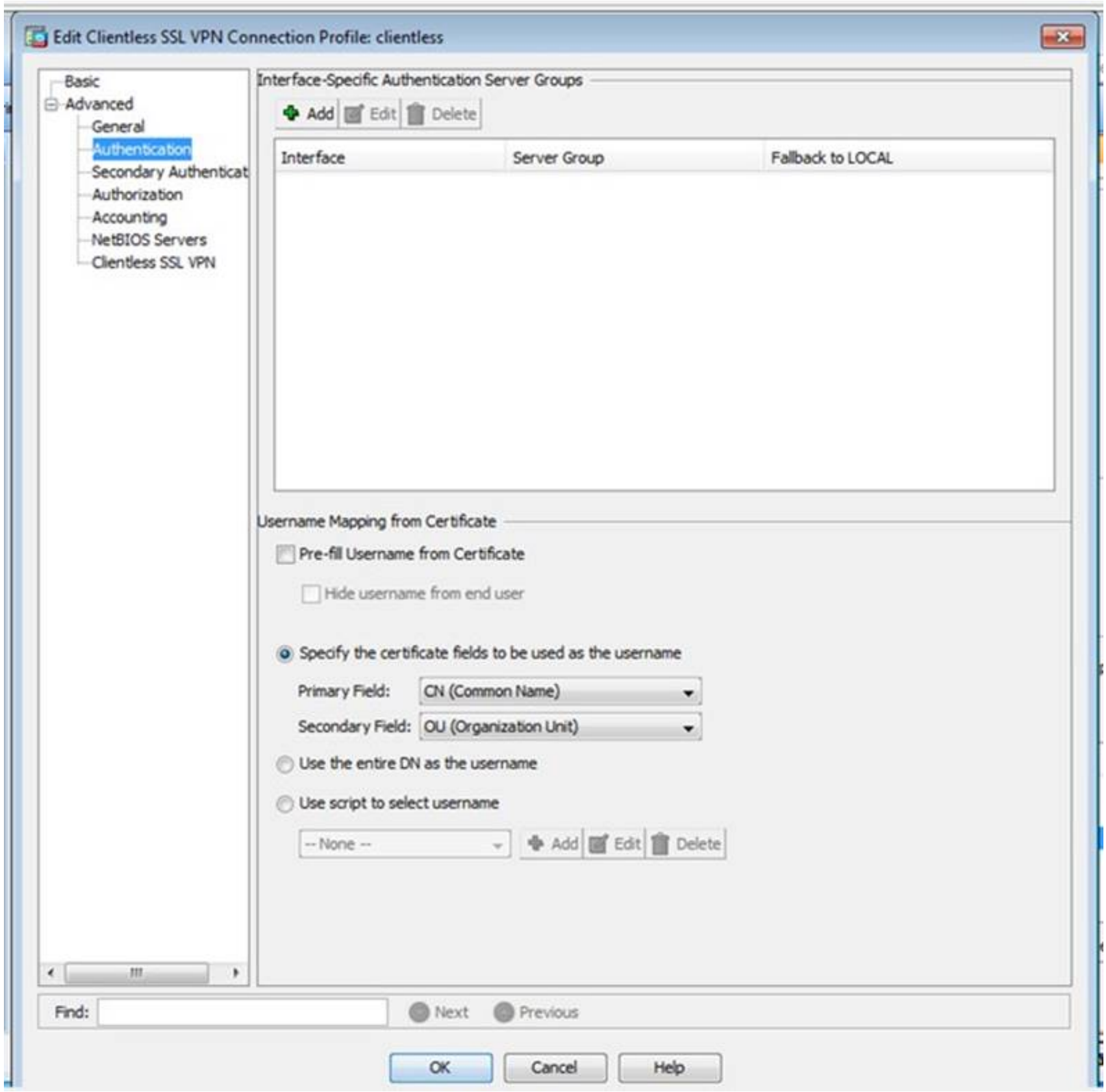

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
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

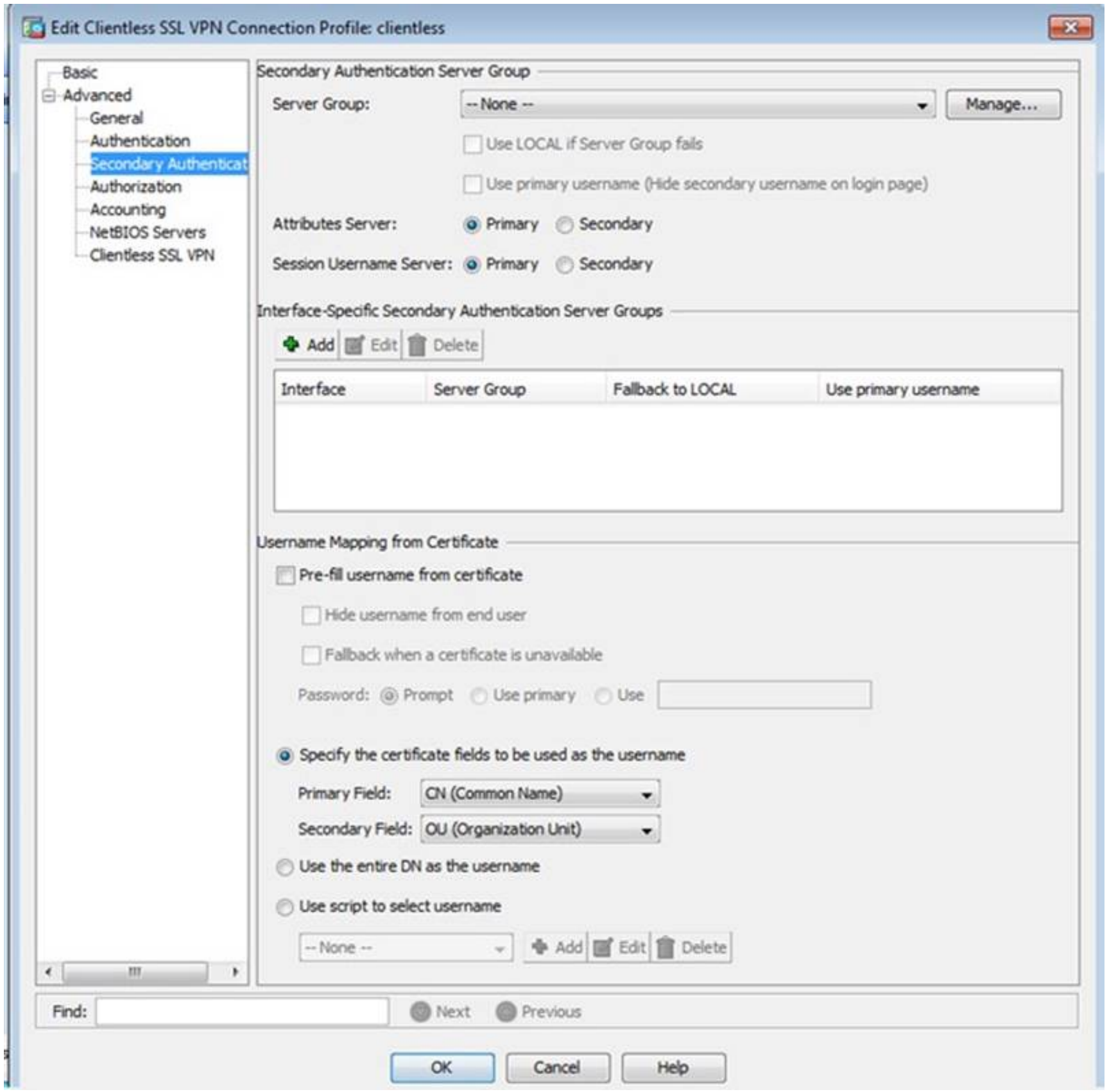

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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

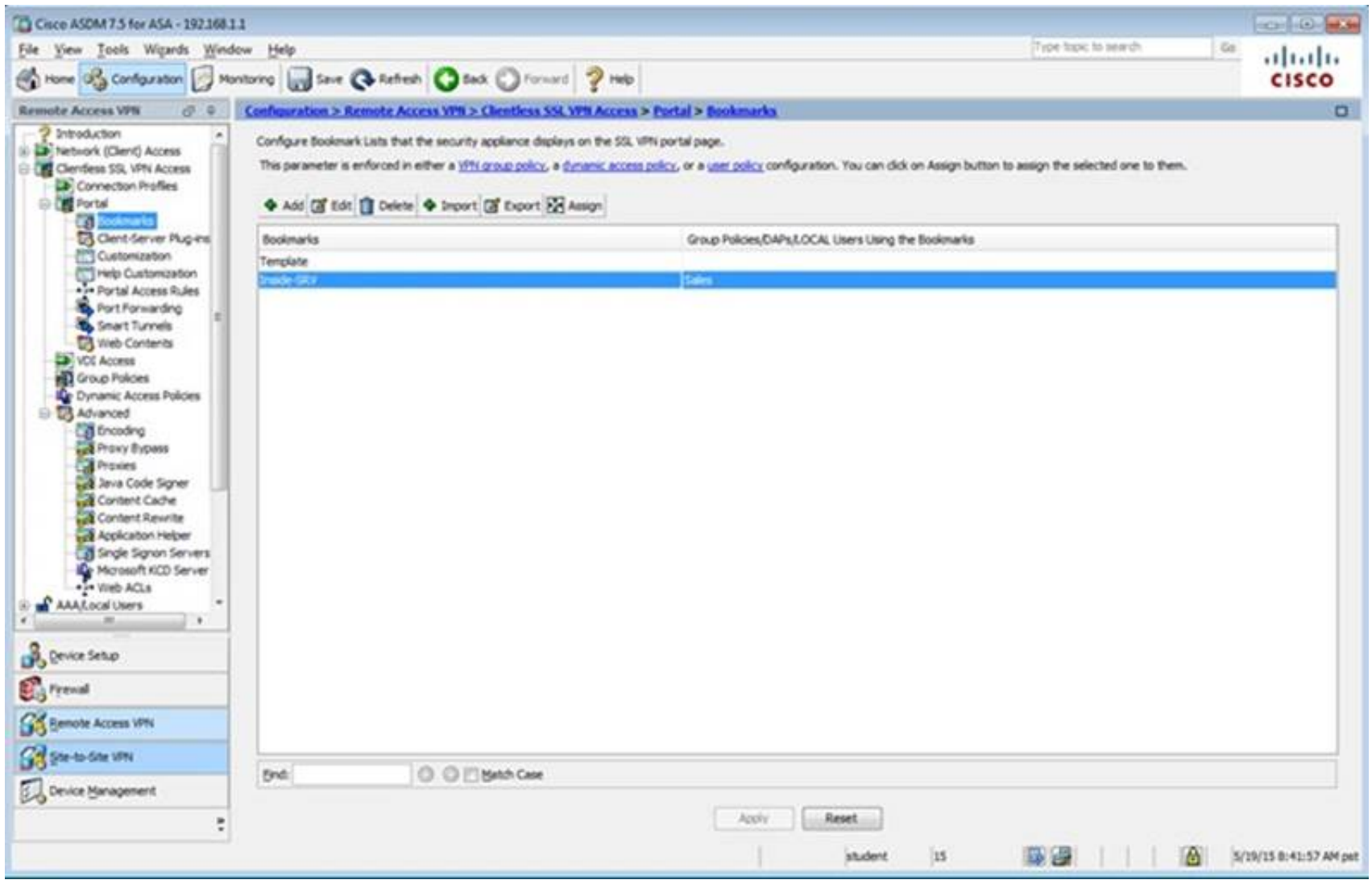

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Access Interfaces
Enable interfaces for clientless SSL VPN 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

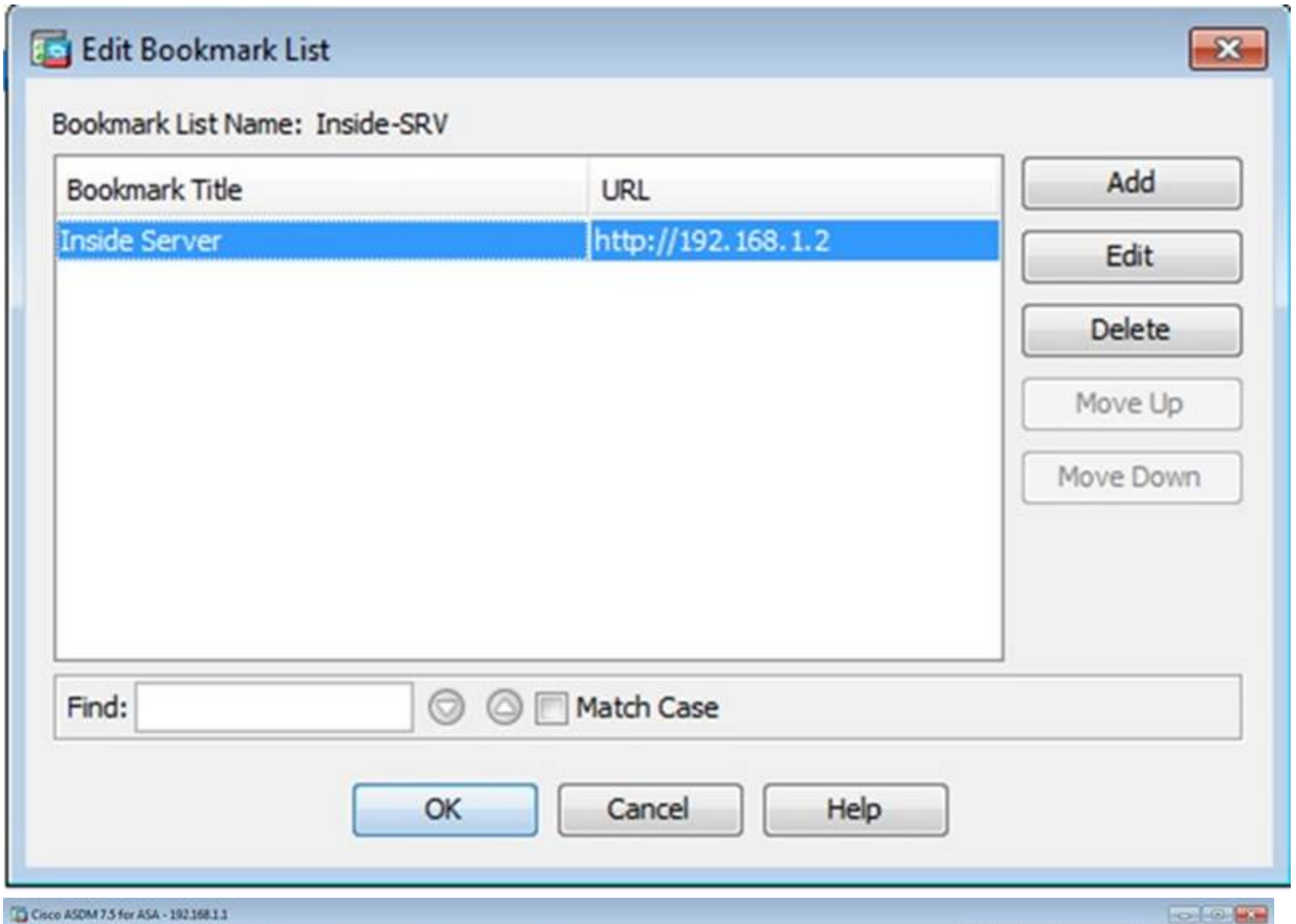

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server 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

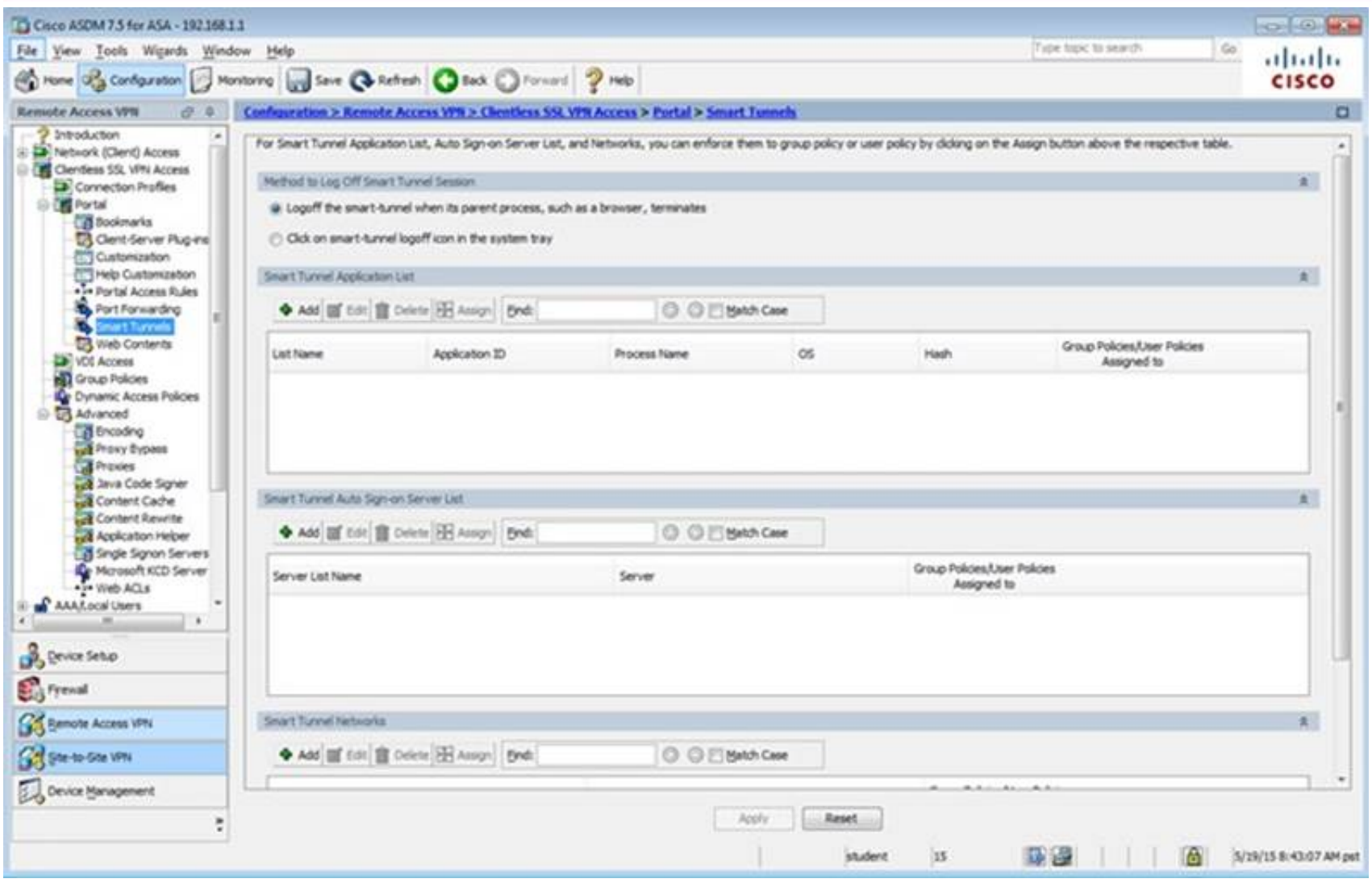

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen 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

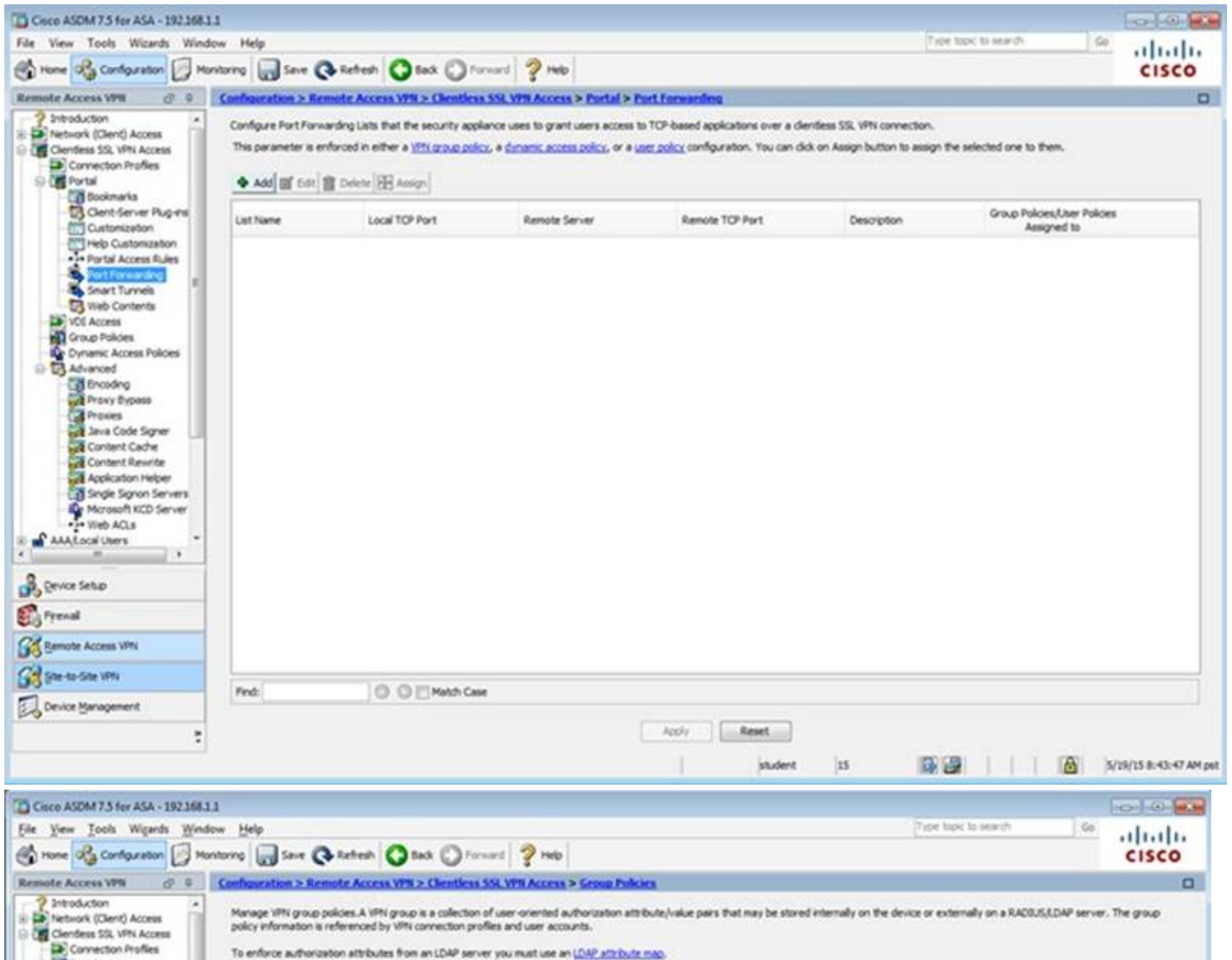

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from 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

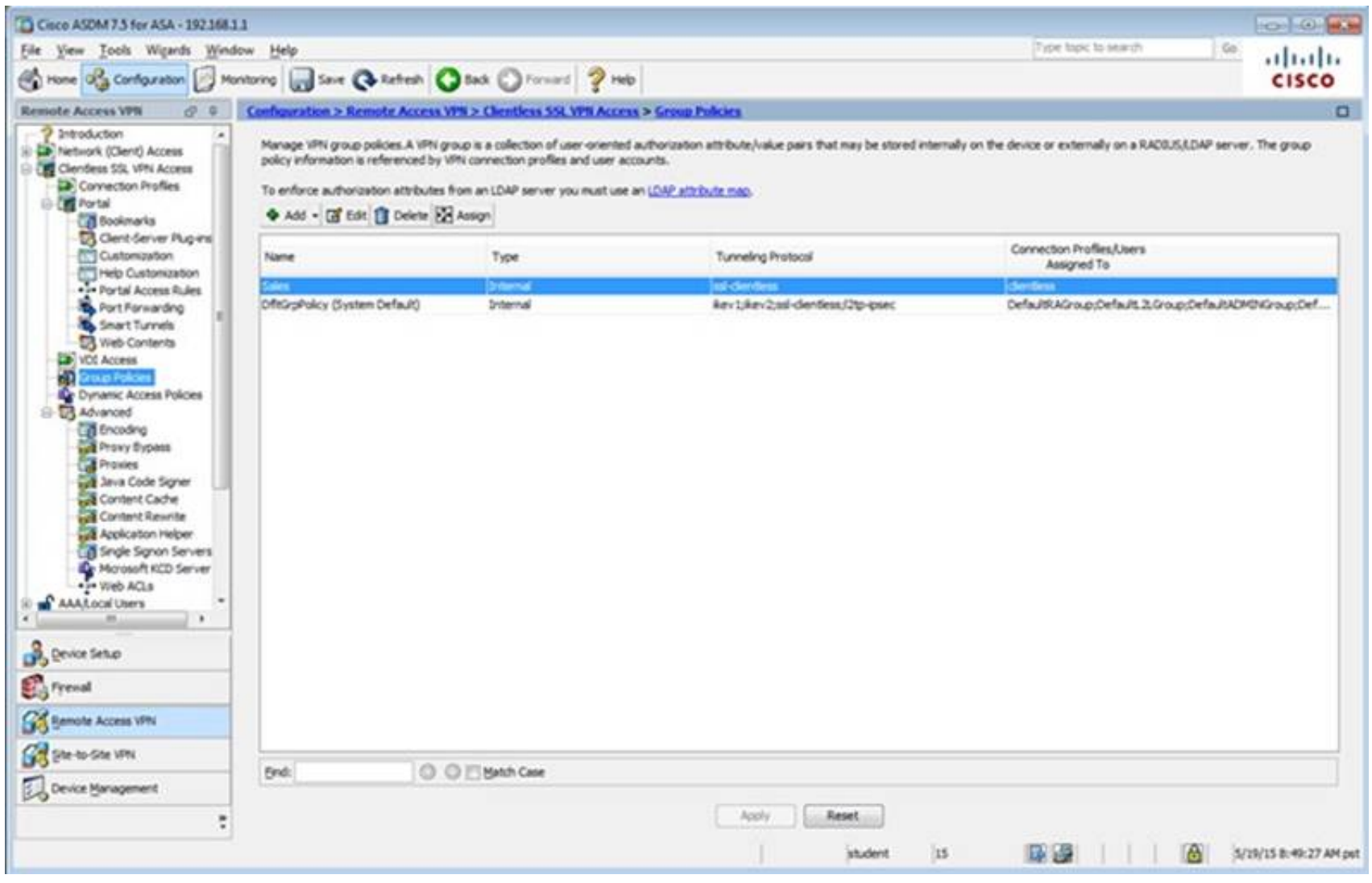

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
-- None --
Manage...
Use LOCAL if Server Group fails
Use primary username (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

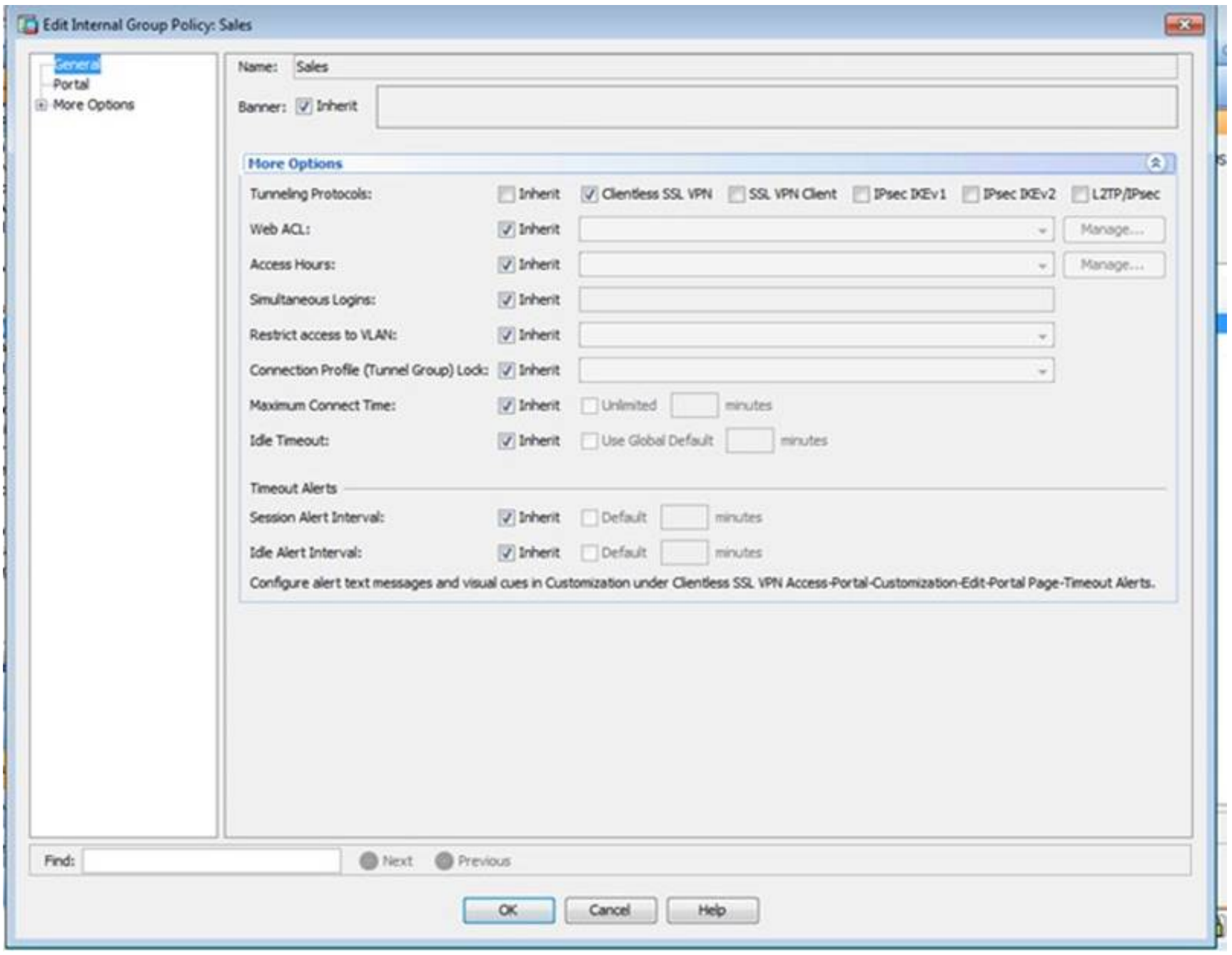

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
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

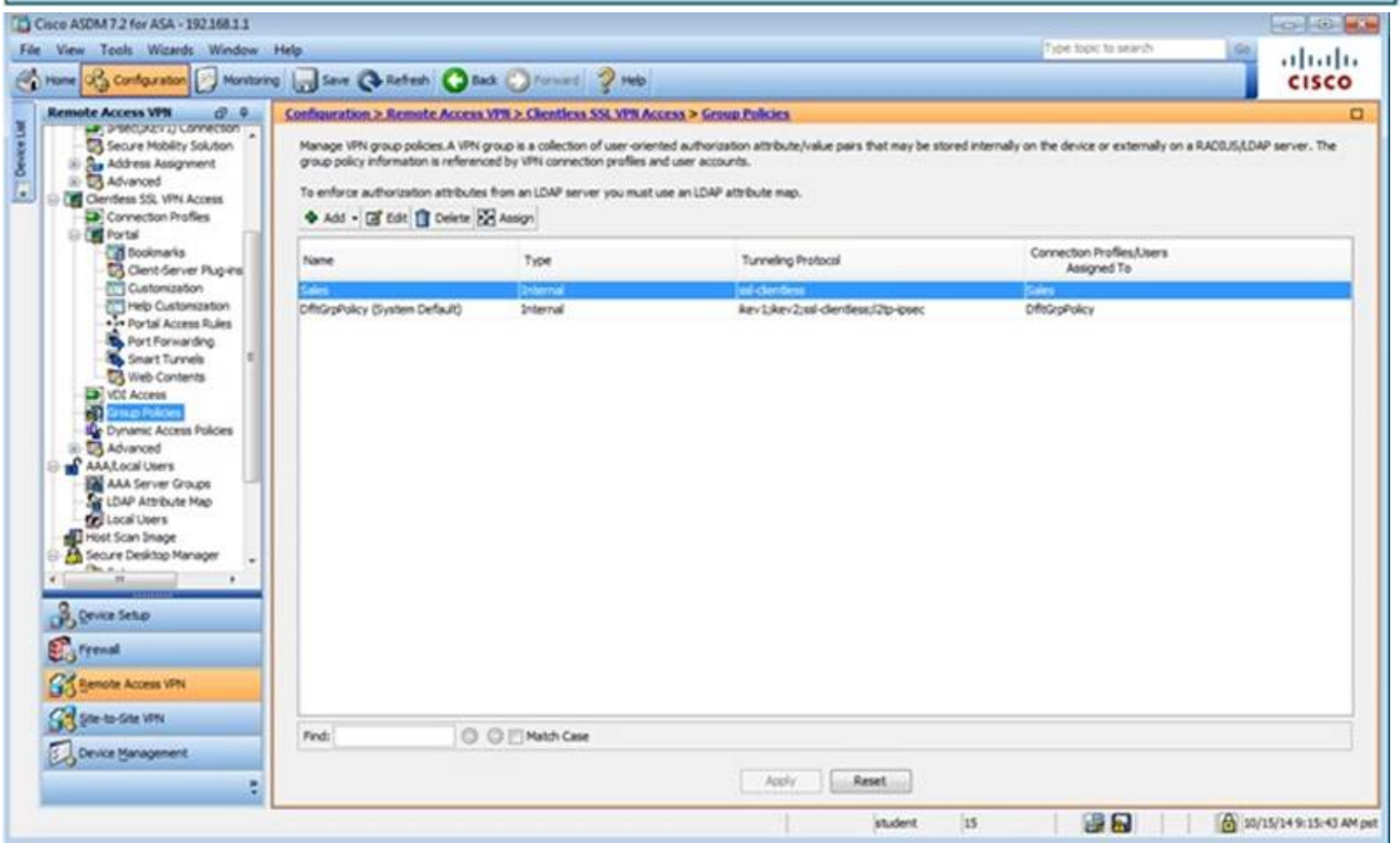

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

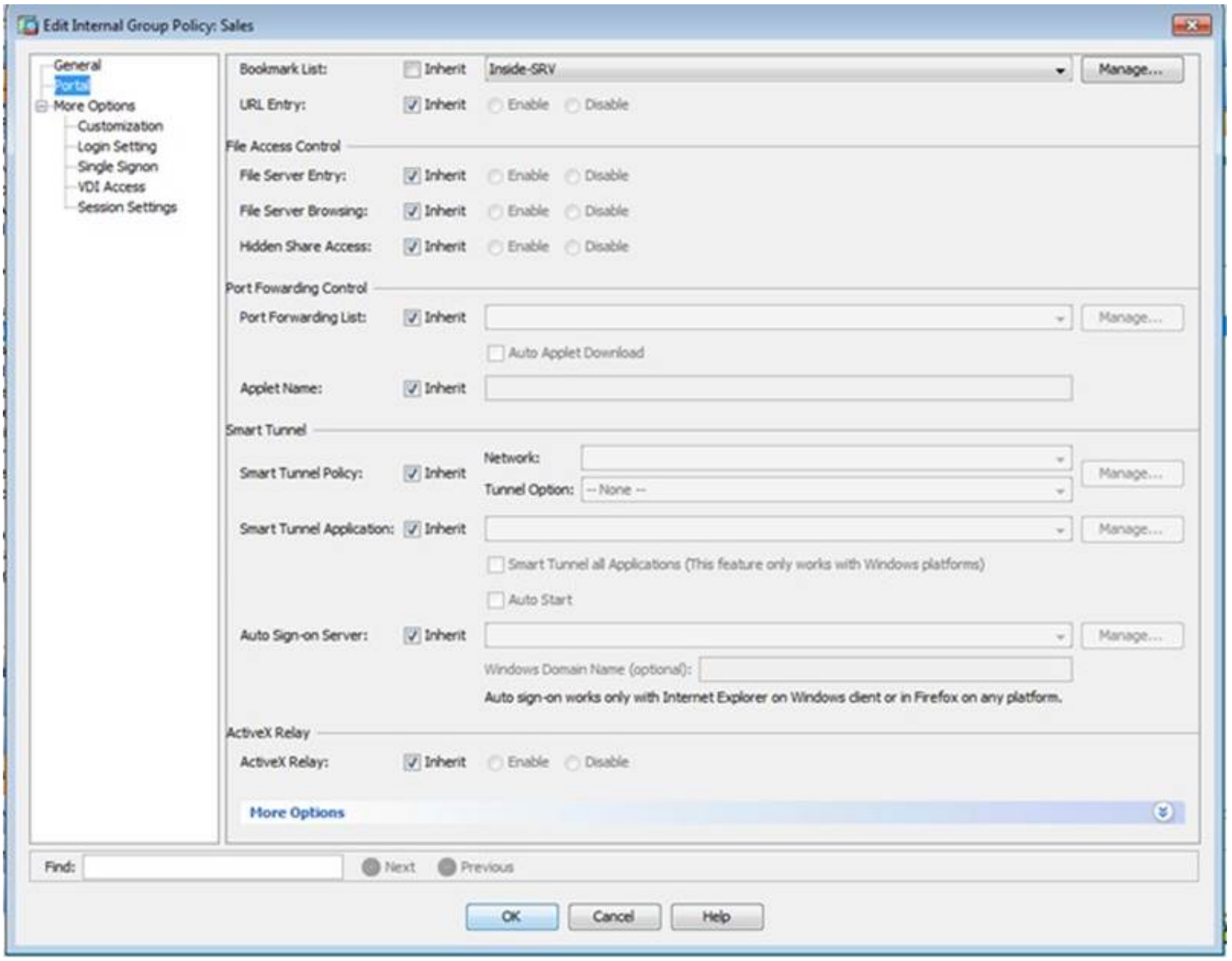

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN 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

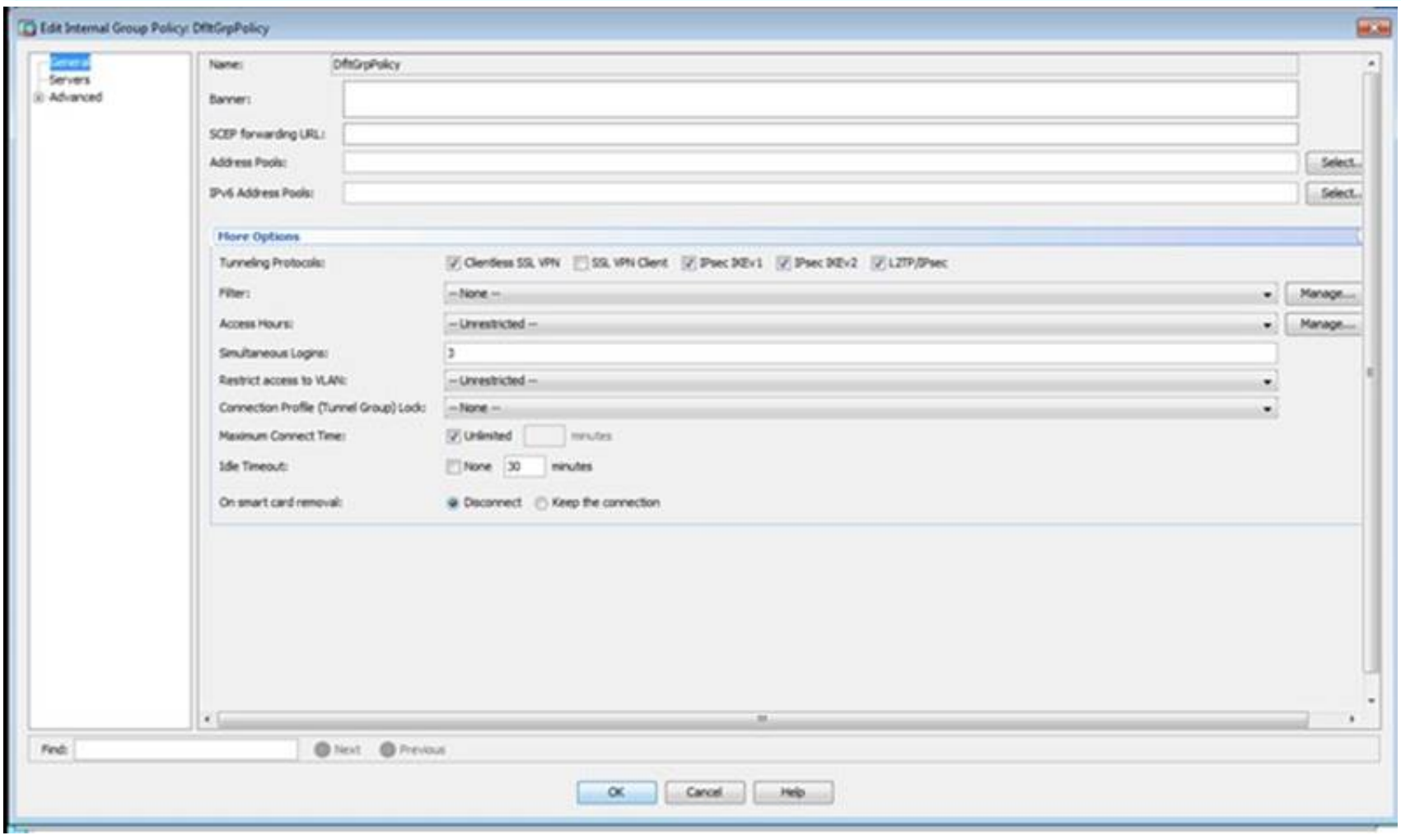

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Introduction
Network (Client) Access
Clientless SSL VPN 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

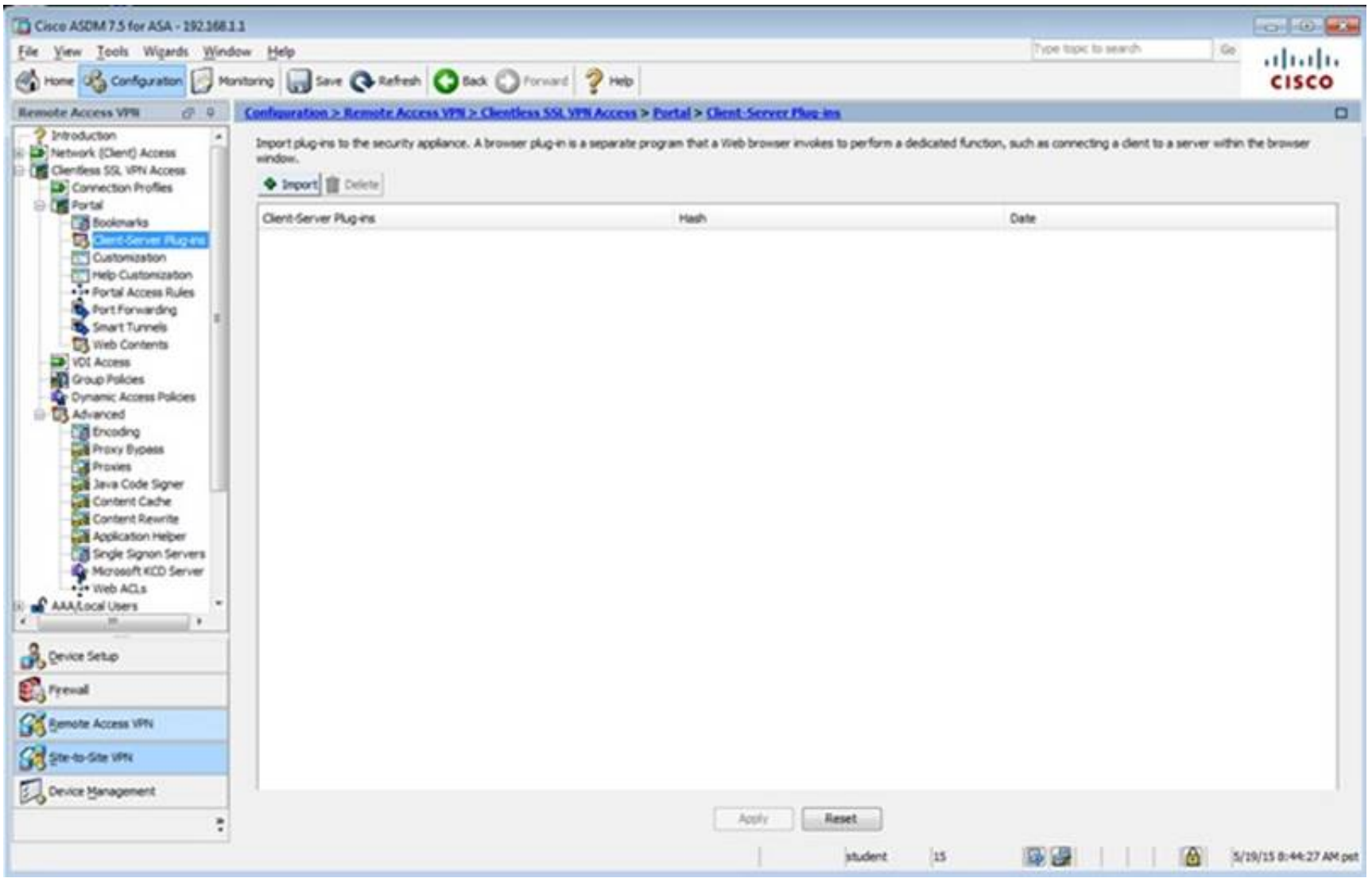

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection 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

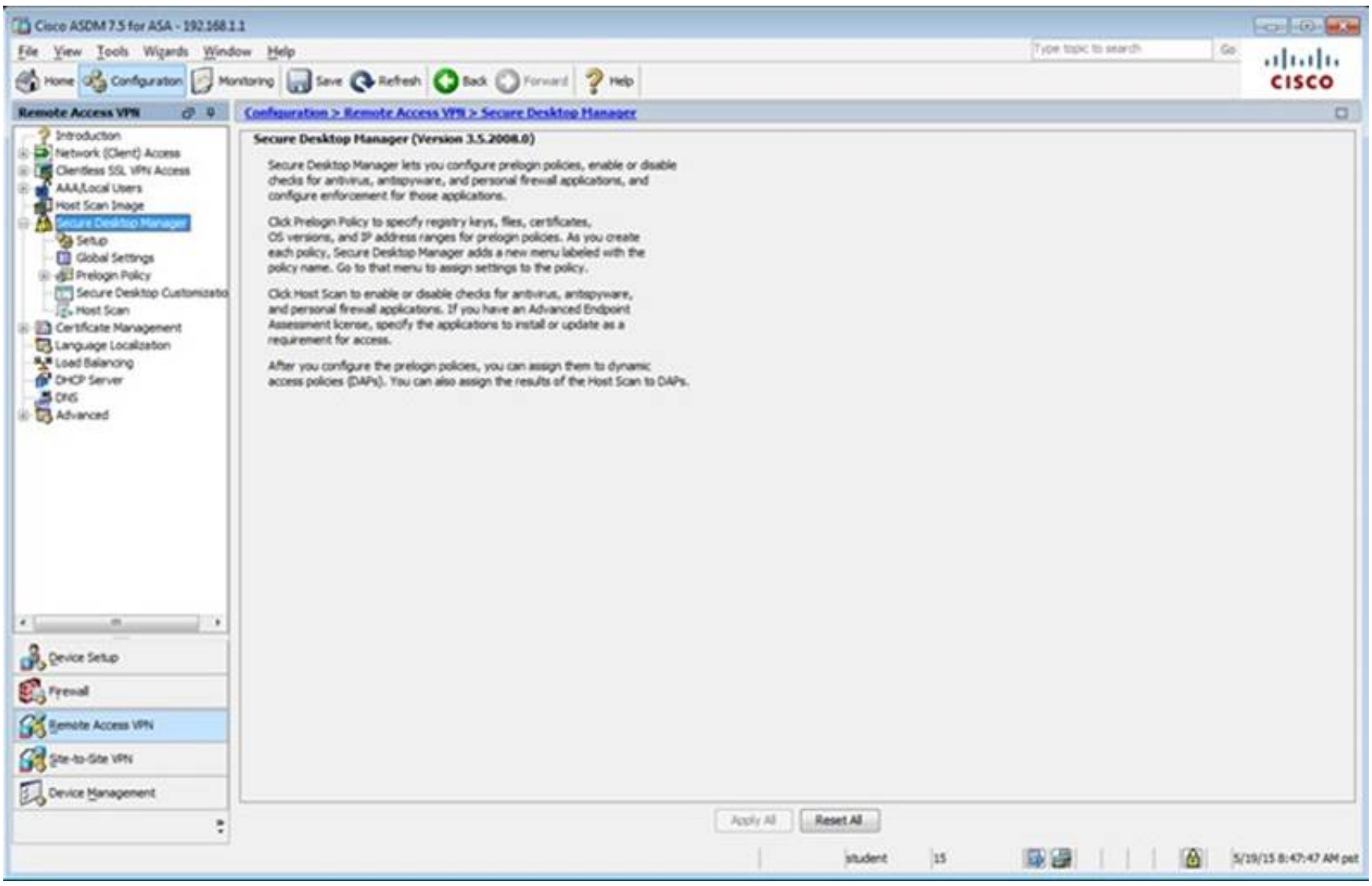

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access 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

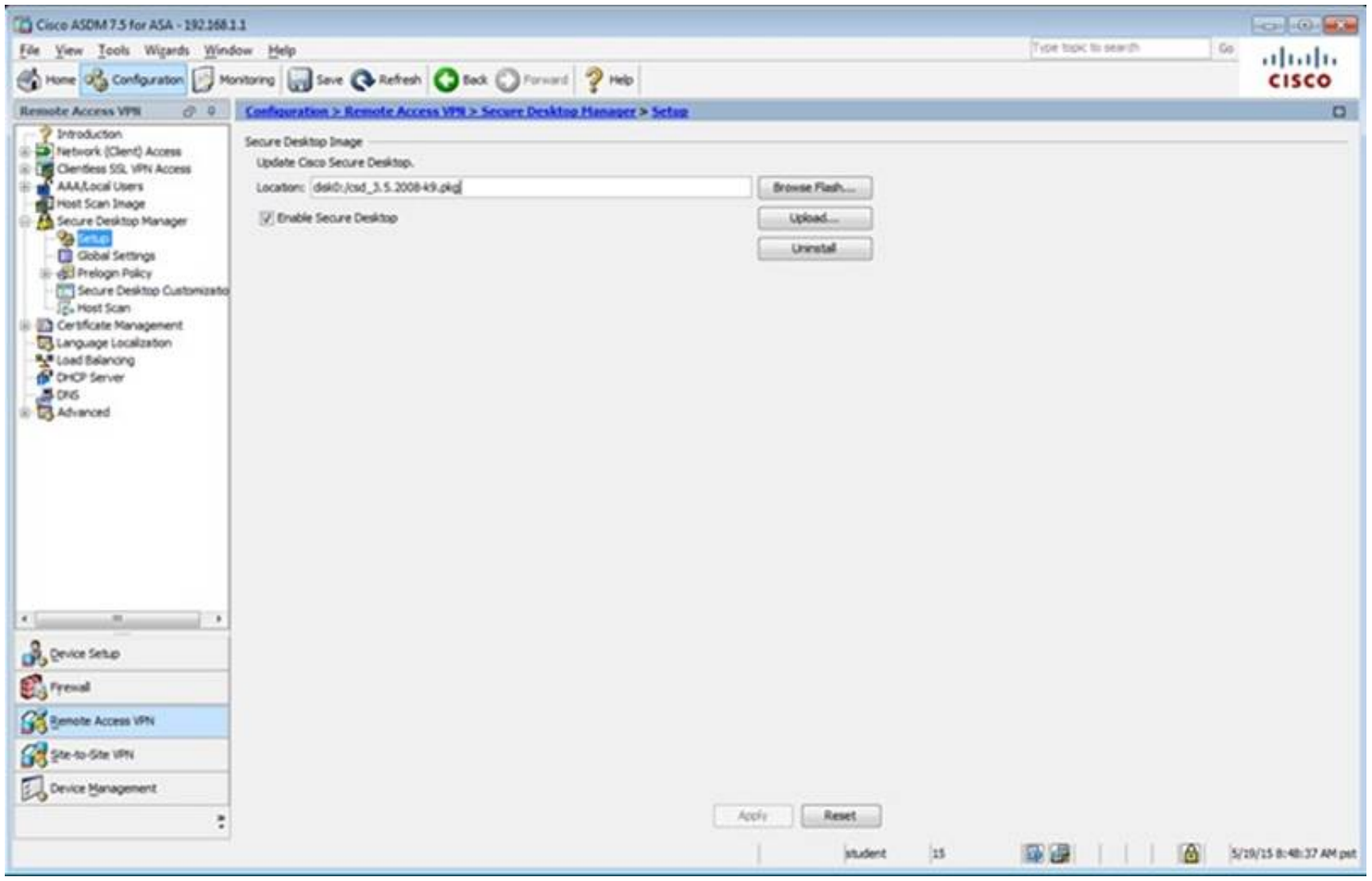

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
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

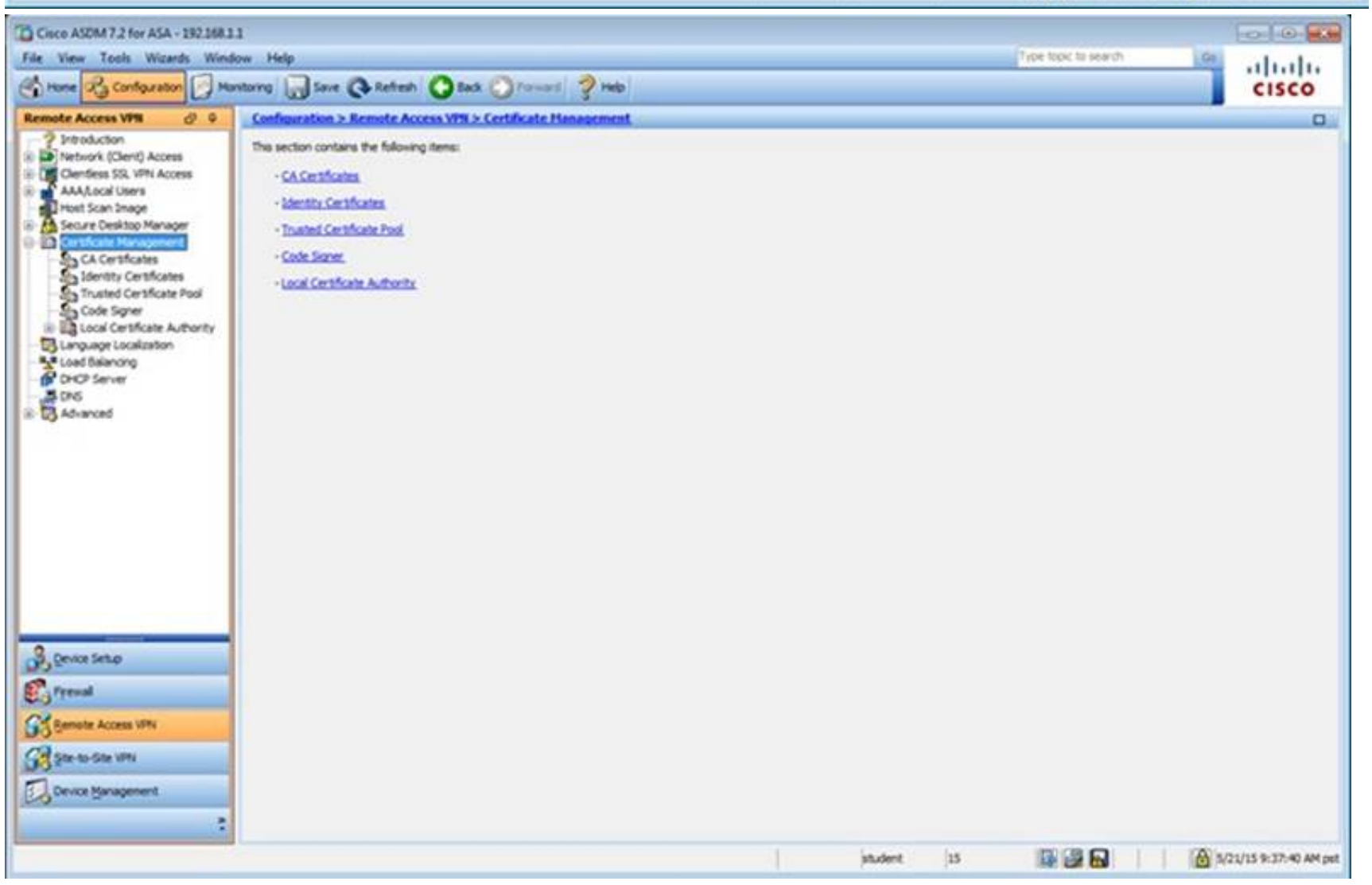

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding 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

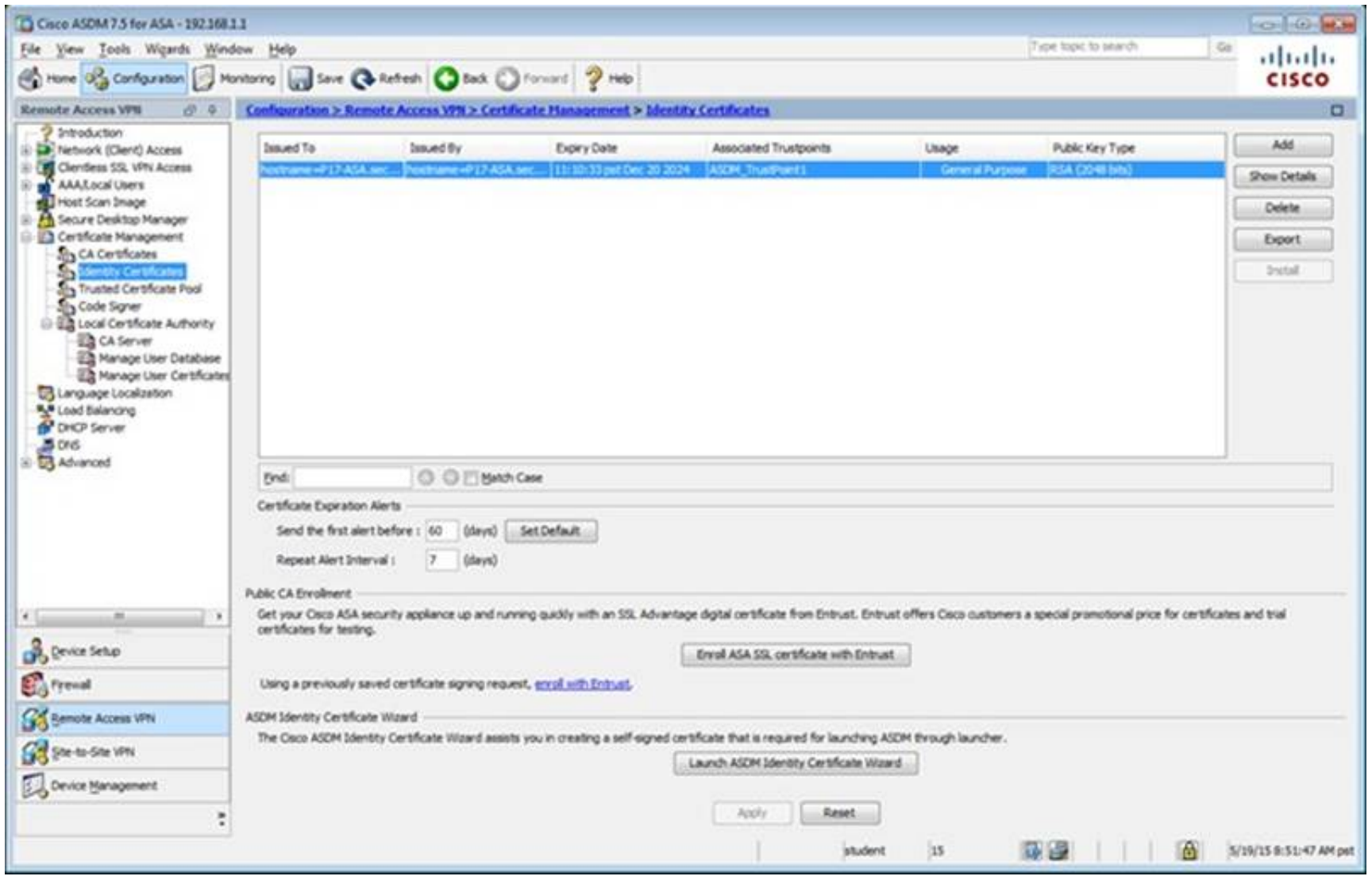

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
Select...
IPv6 Address Pools:
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- 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

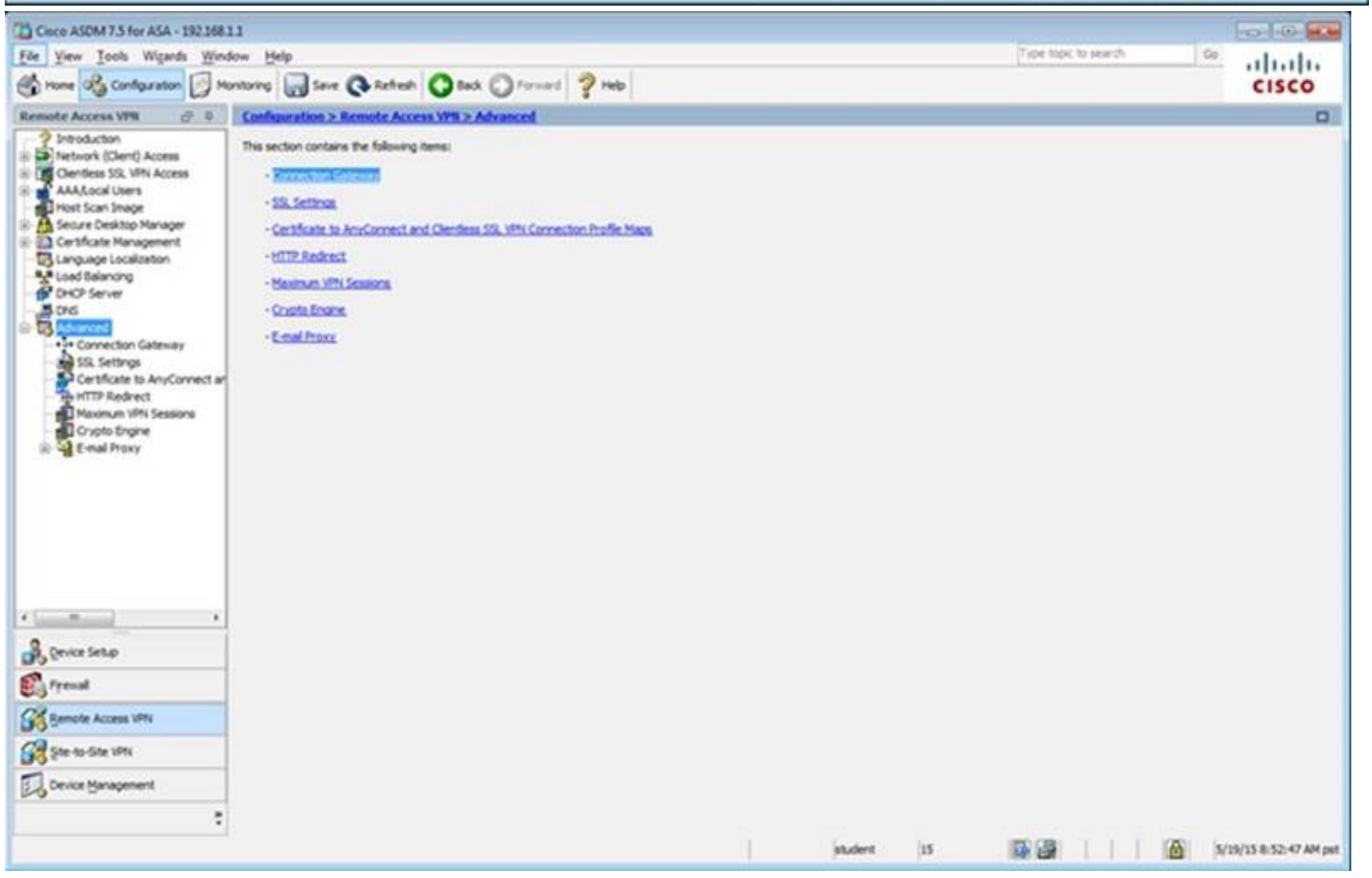

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless 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

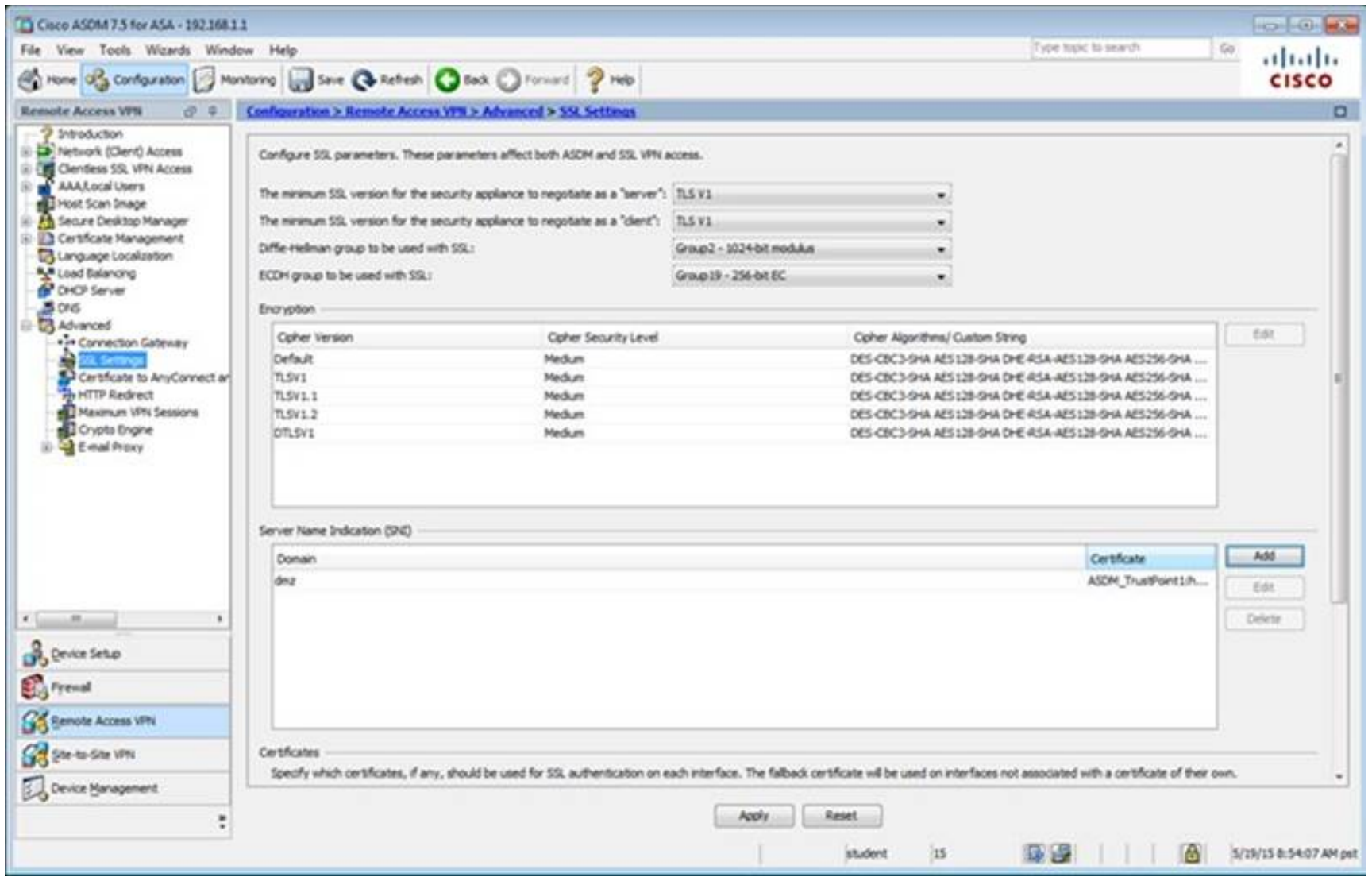

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

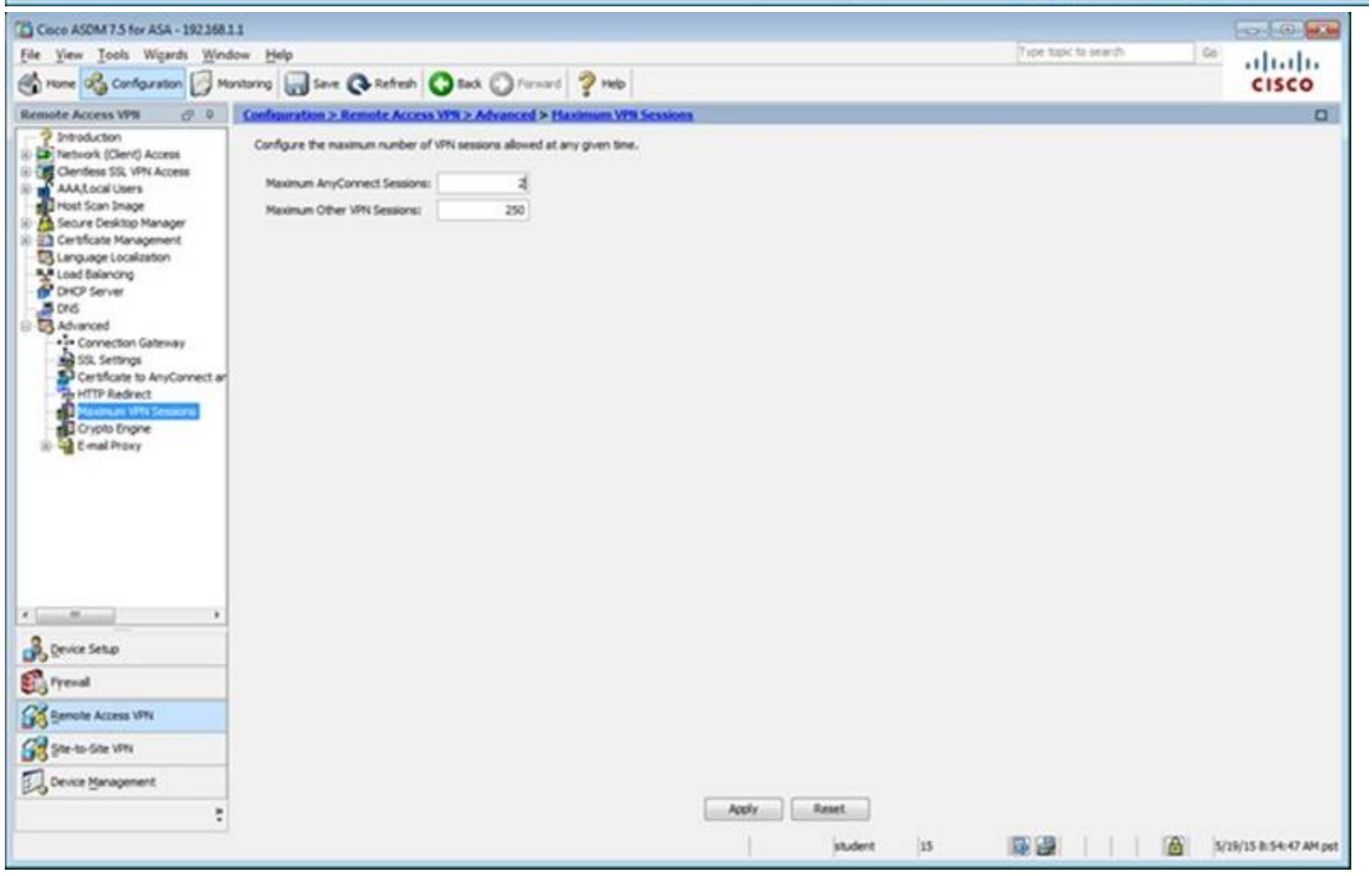

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager > Setup
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
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

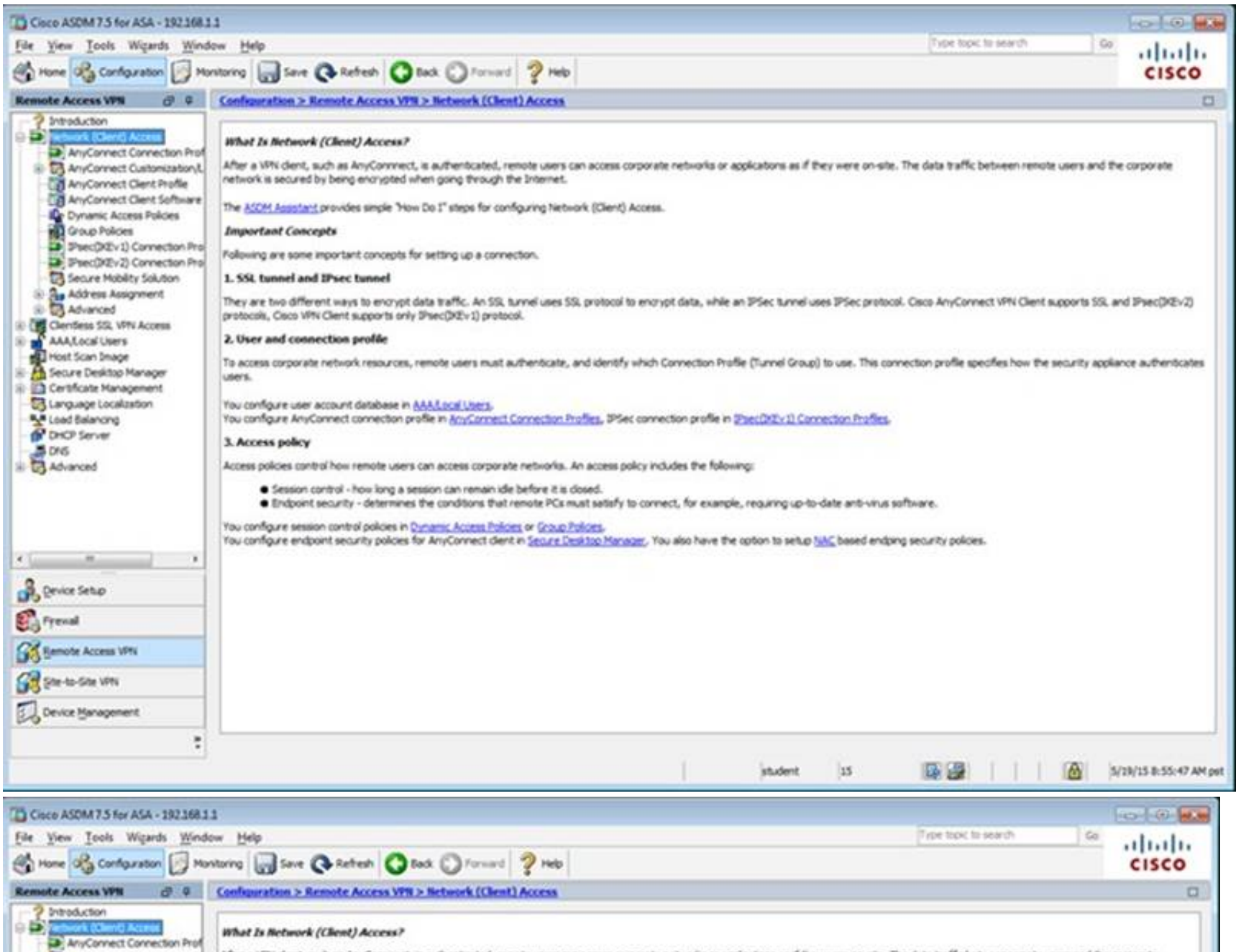

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

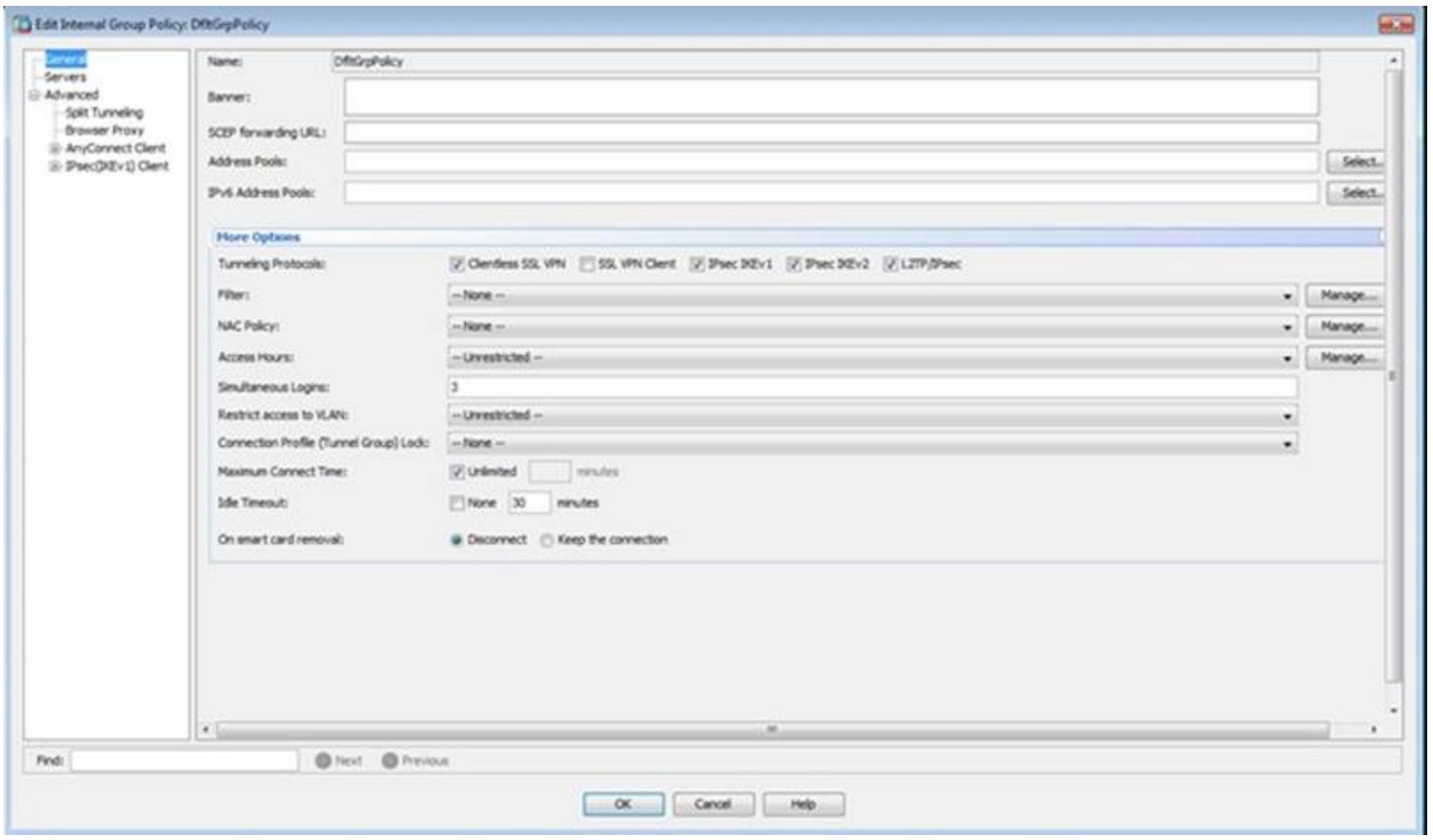

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Introduction
Network (Client) Access
Clientless SSL VPN Access
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

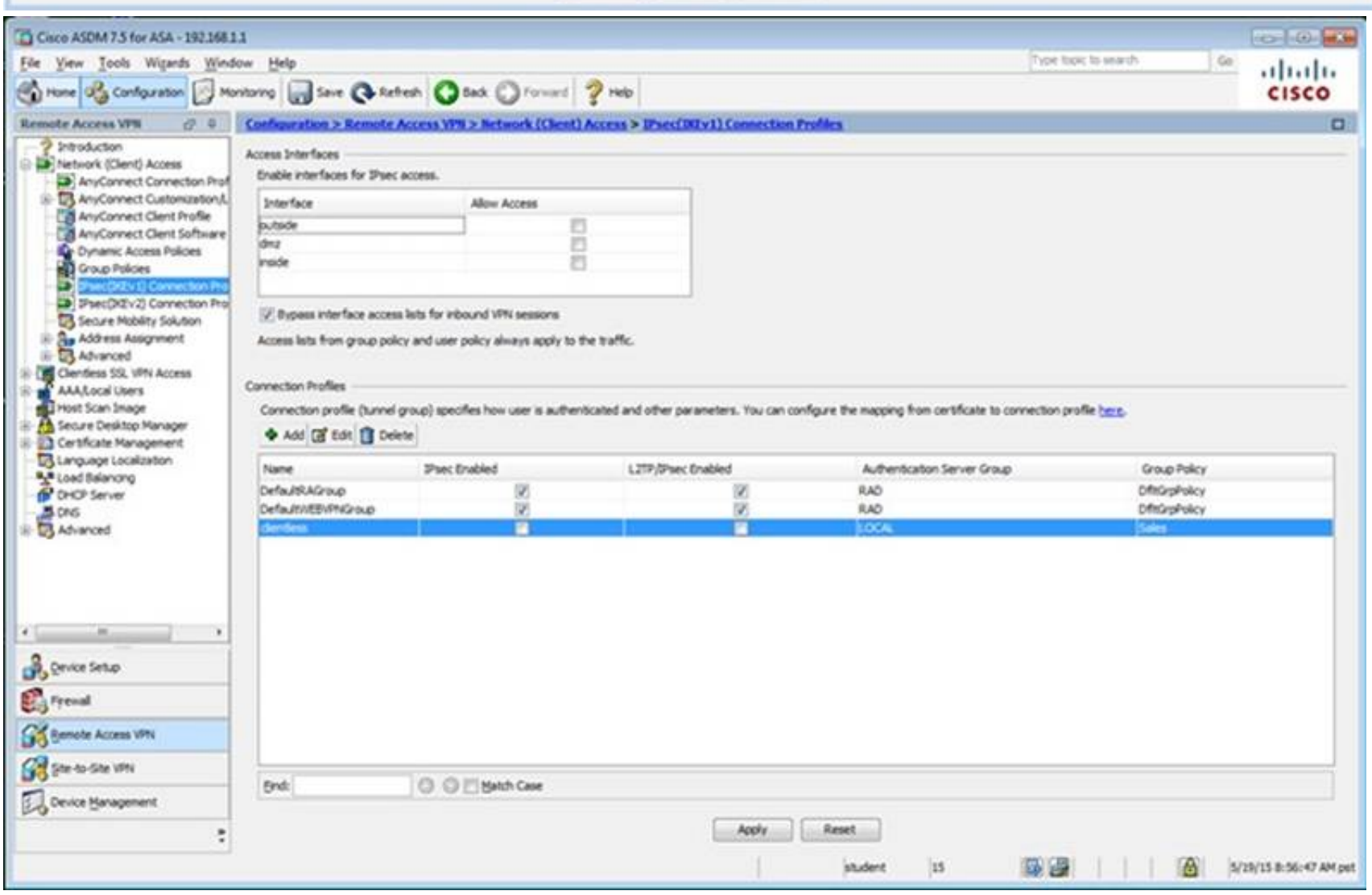

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- SSL Settings
- Certificate to AnyConnect and Clientless 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

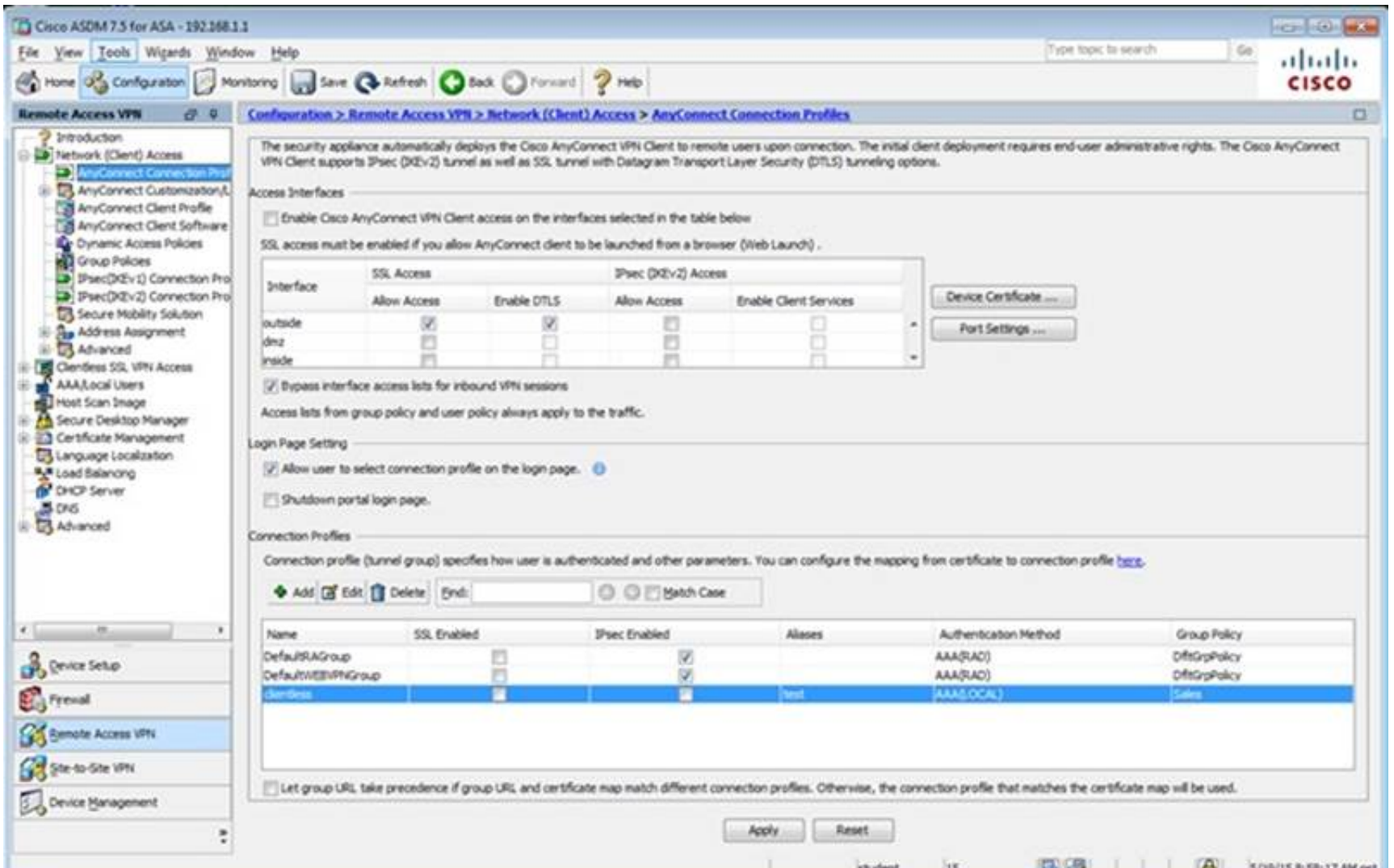

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

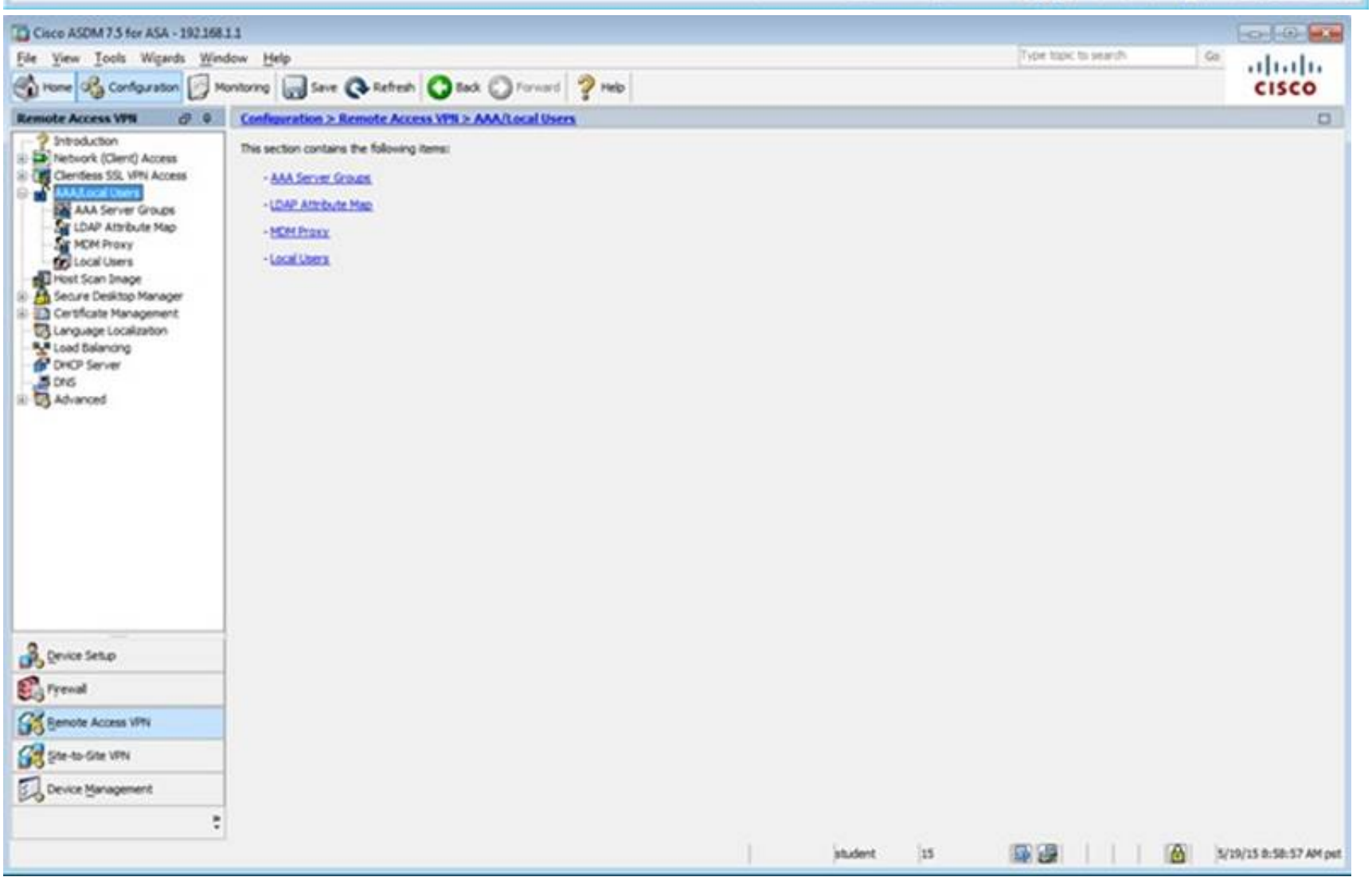

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:54:47 AM pst

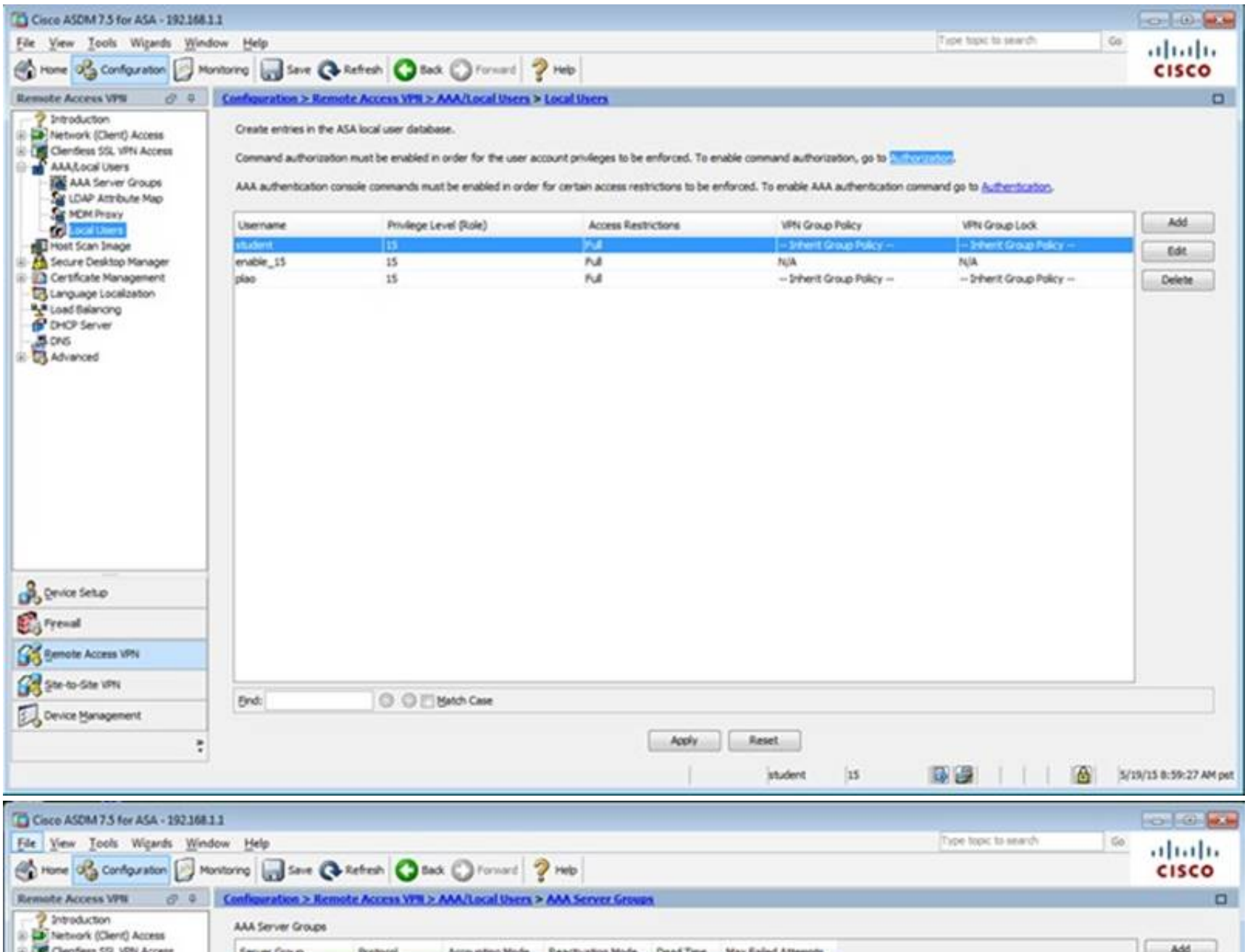

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, 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

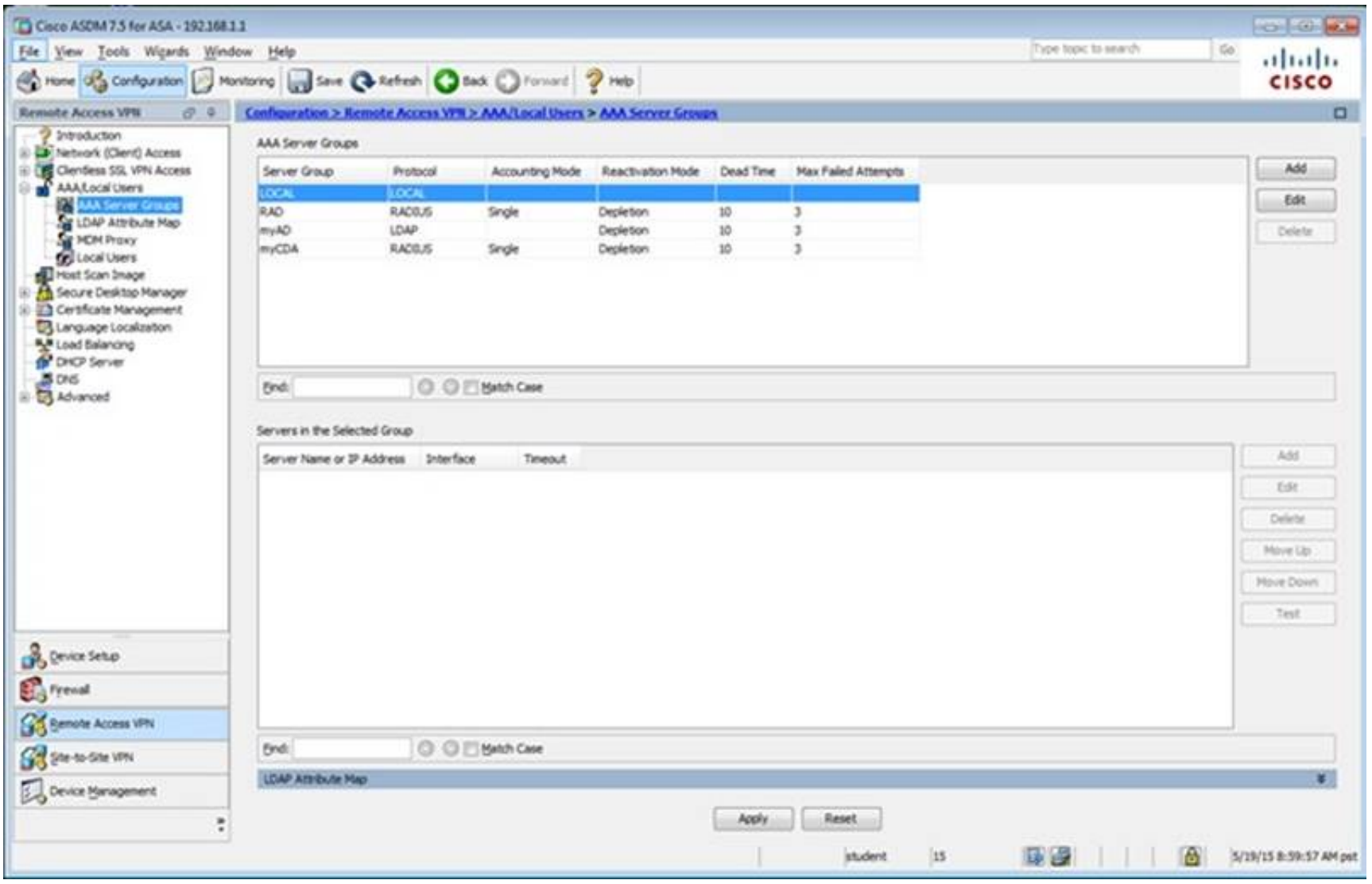

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Name: DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
IPv6 Address Pools:
Select...
More Options
Tunneling Protocols: Clientless SSL VPN, SSL VPN Client, IPsec 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
DefaultL2LGroup
test
AAA(LOCAL)
Sales
AAA(RAD)
DfltGrpPolicy
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

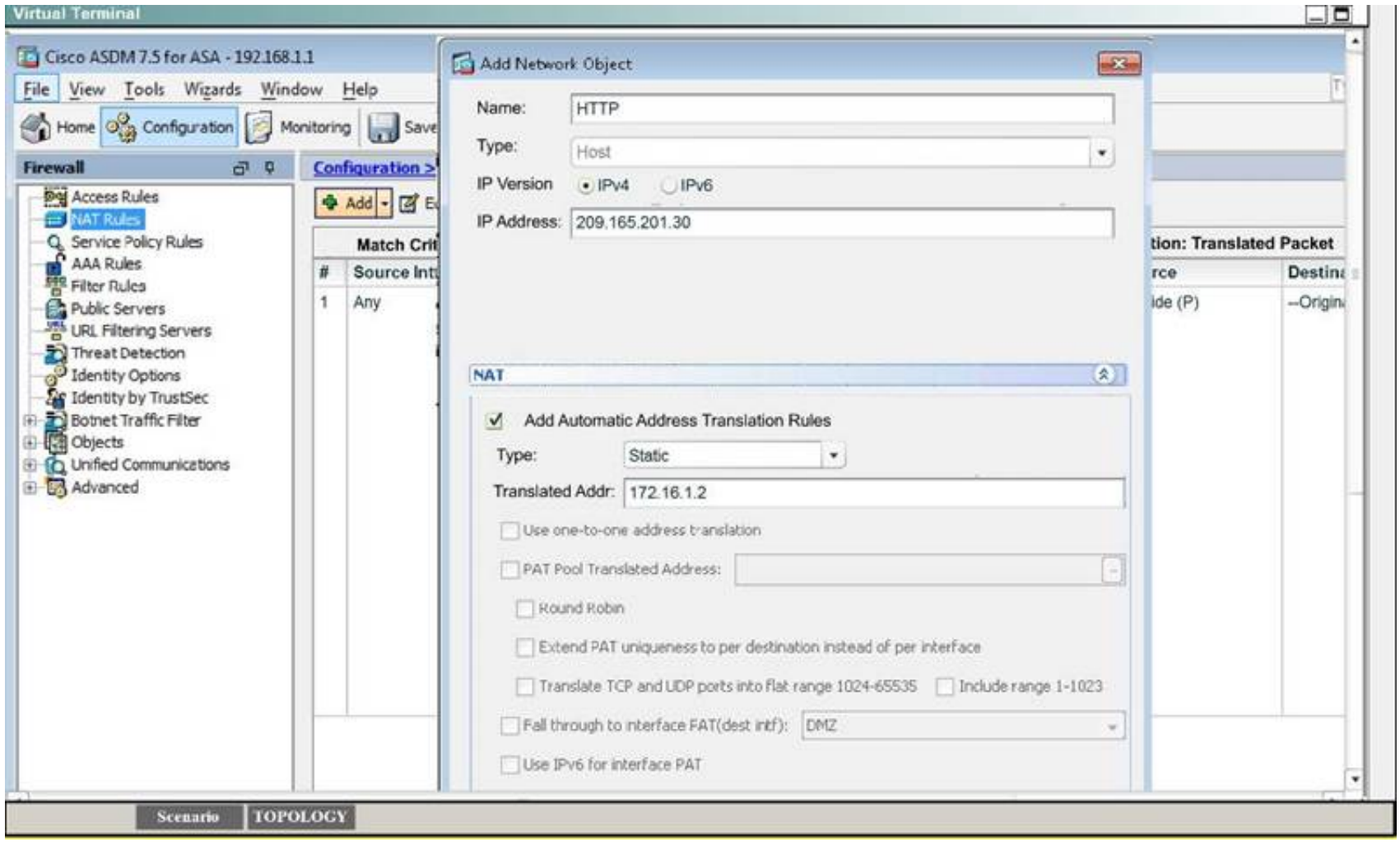

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > AAA/Local Users
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
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



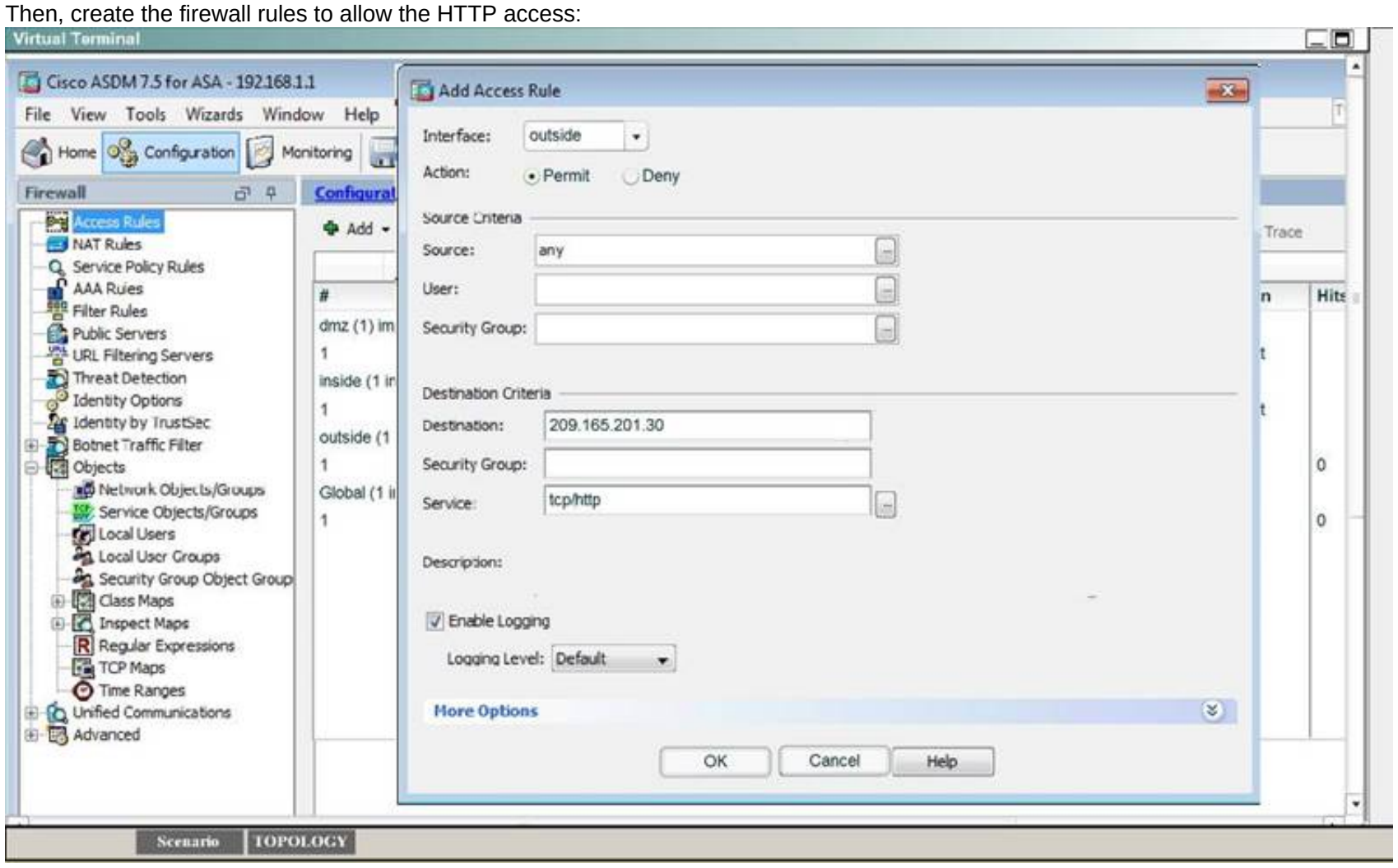


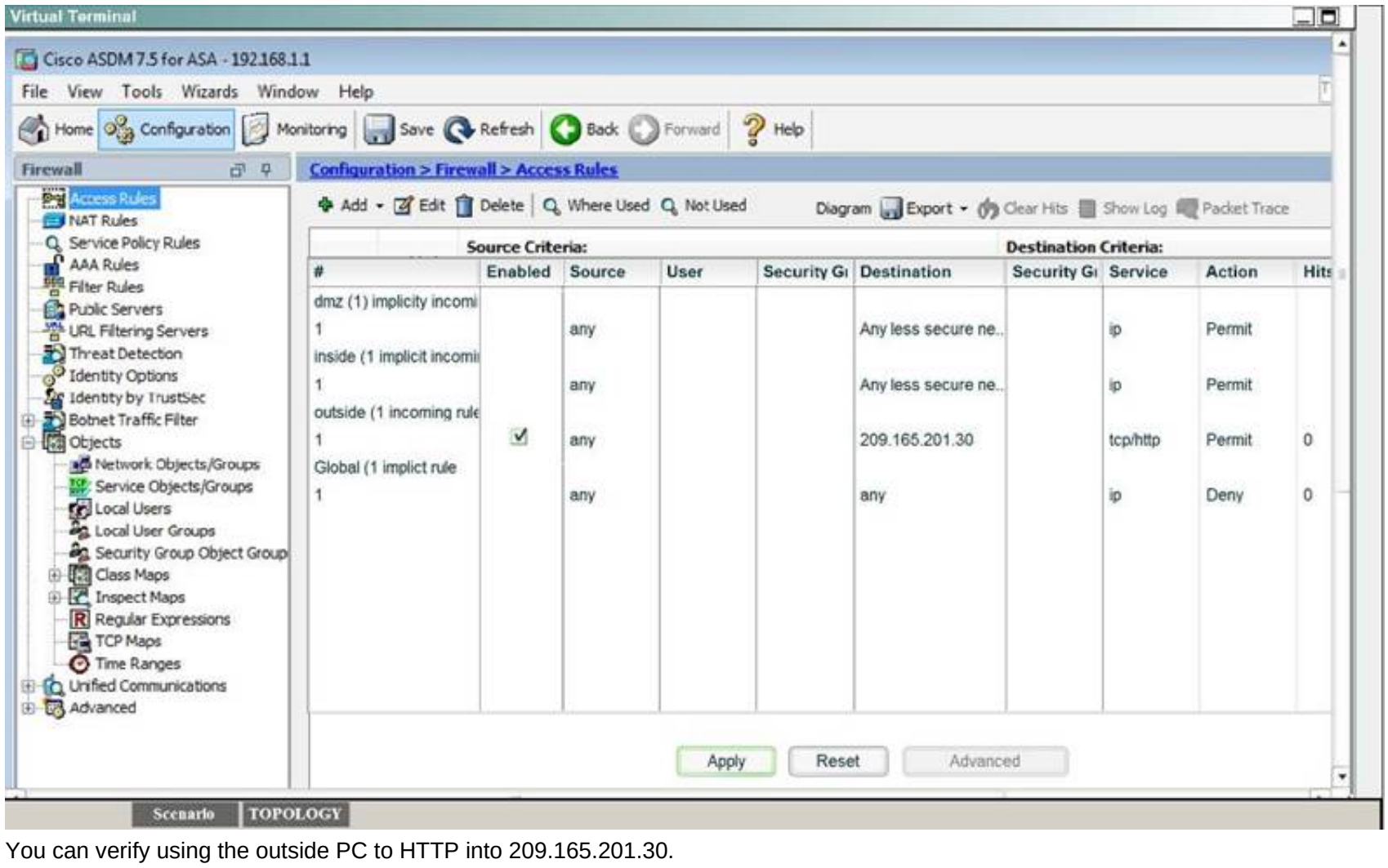
Answer:

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.

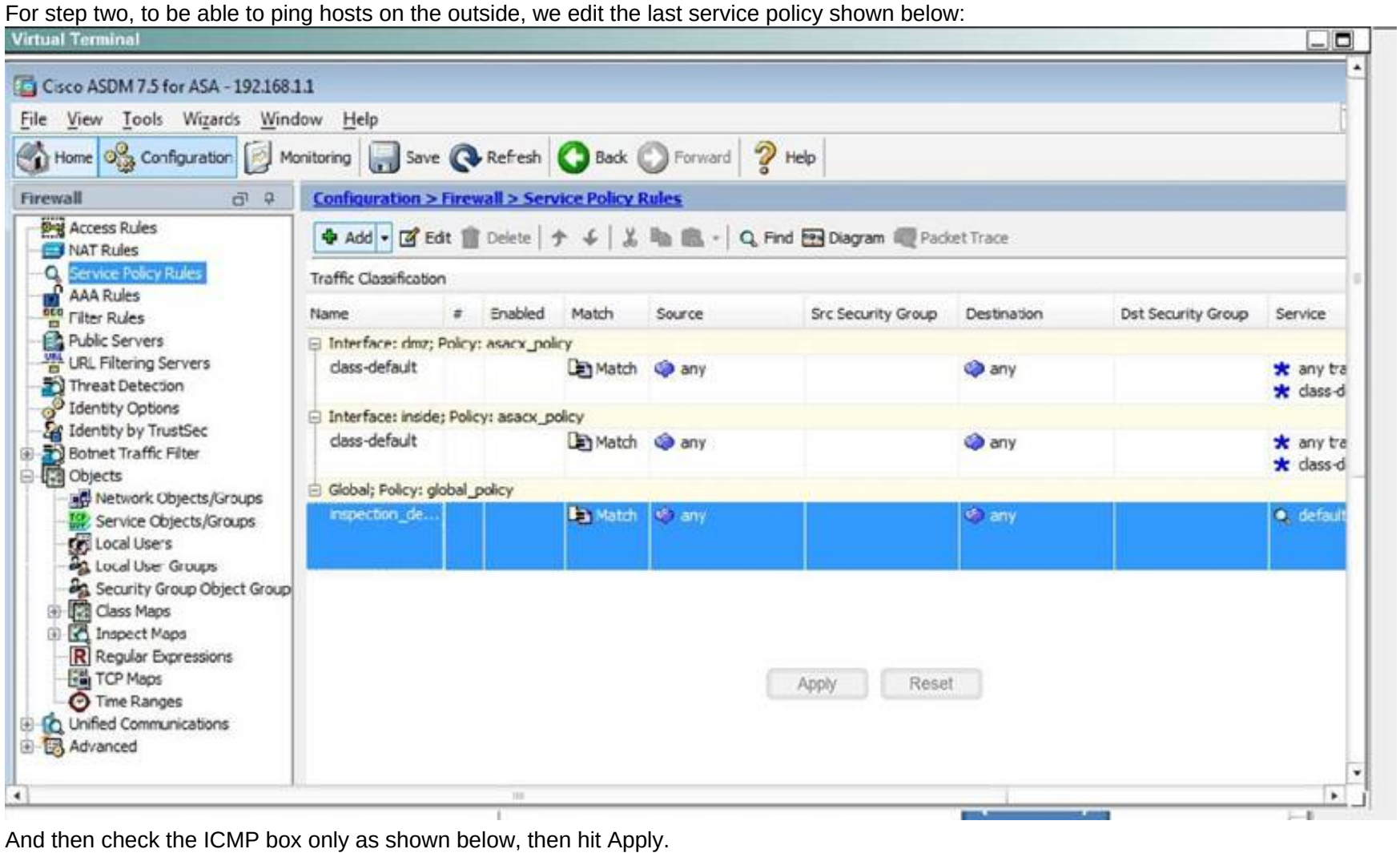


Then, create the firewall rules to allow the HTTP access:

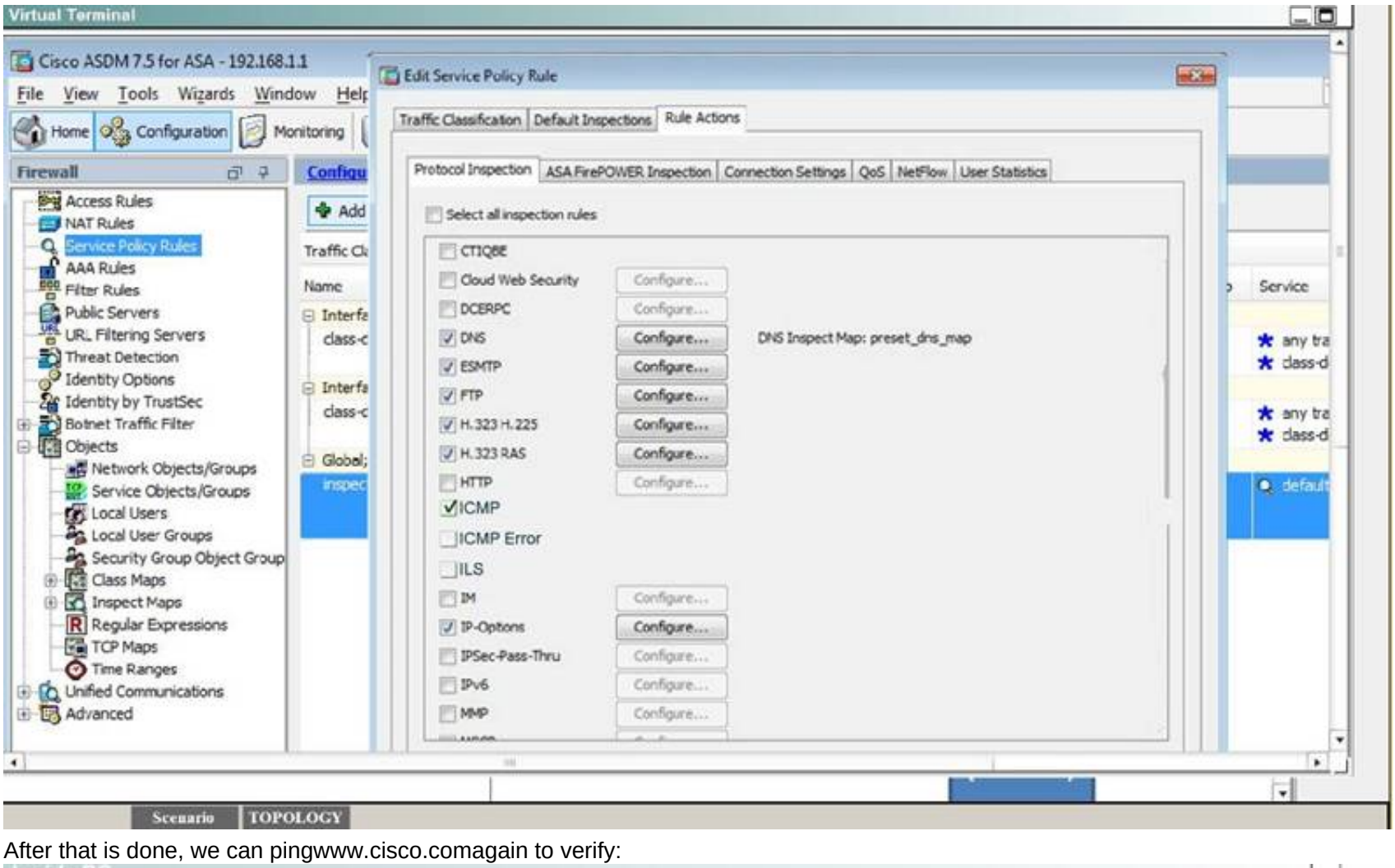




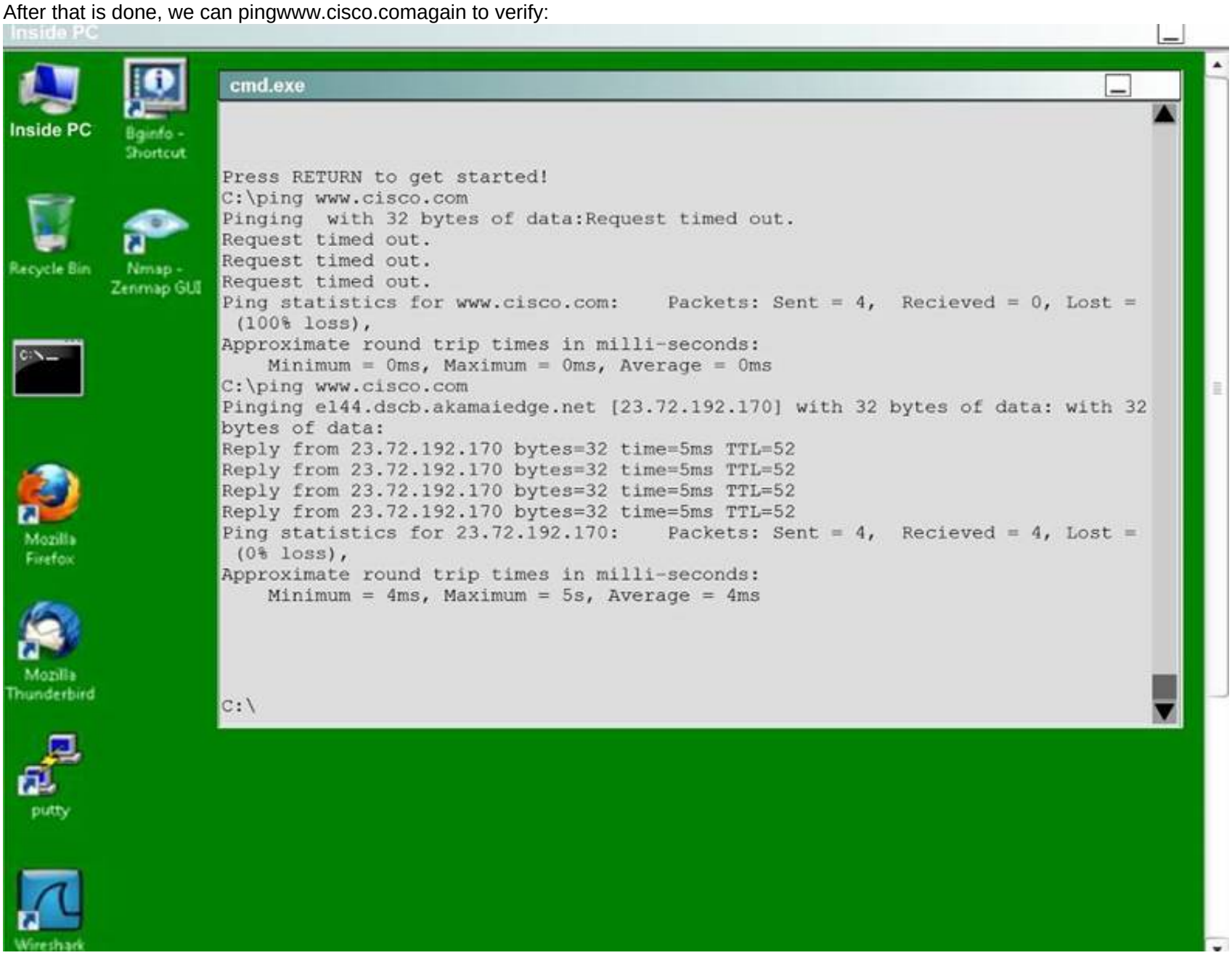
You can verify using the outside PC to HTTP into 209.165.201.30.
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



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 8
Refer to the exhibit.

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

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

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

Answer: A

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

NEW QUESTION 9
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 10
What is one requirement for locking a wired or wireless device from ISE?

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

Answer: A

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

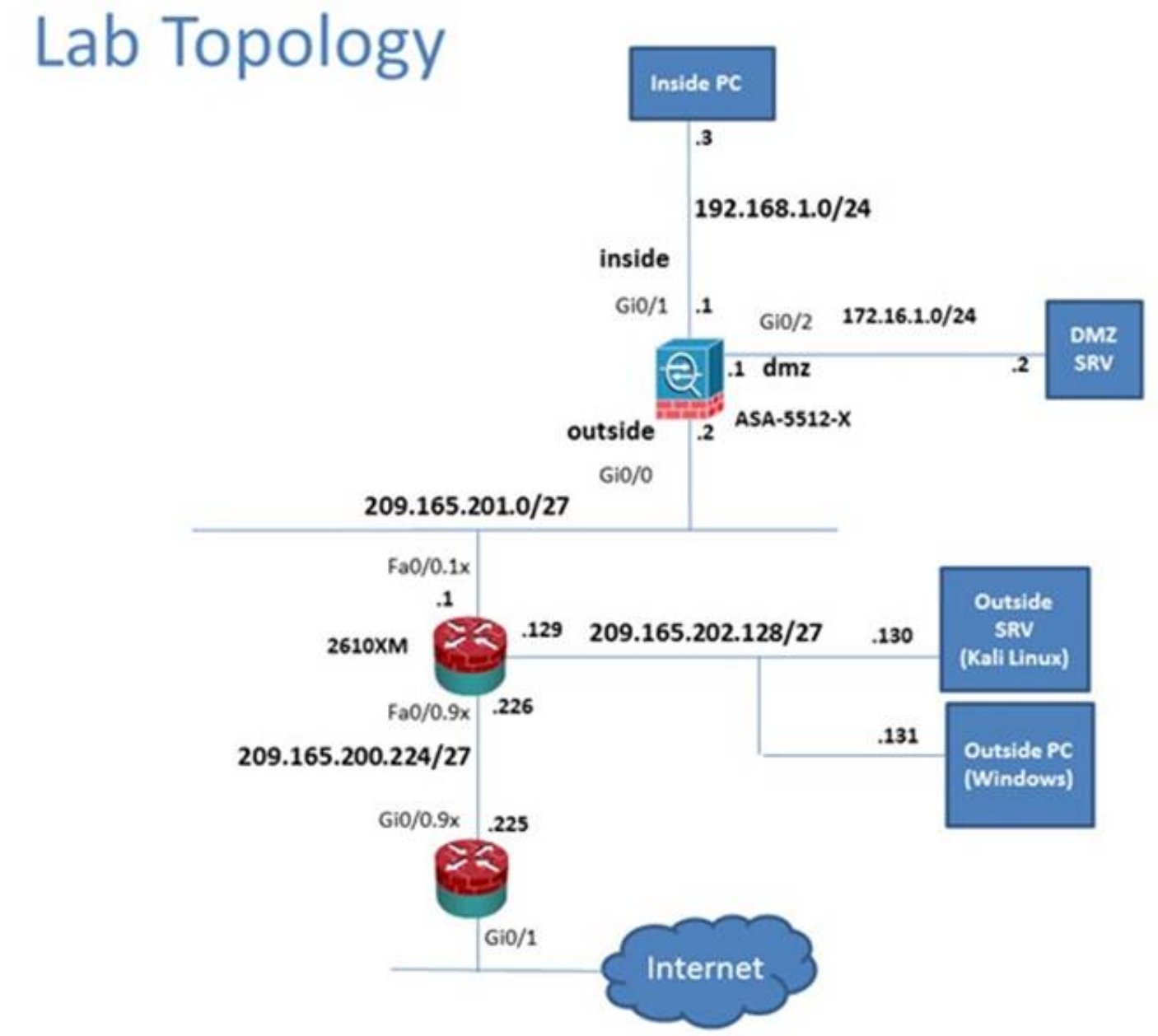
NEW QUESTION 10
Which statement about a PVLAN isolated port configured on a switch is true?

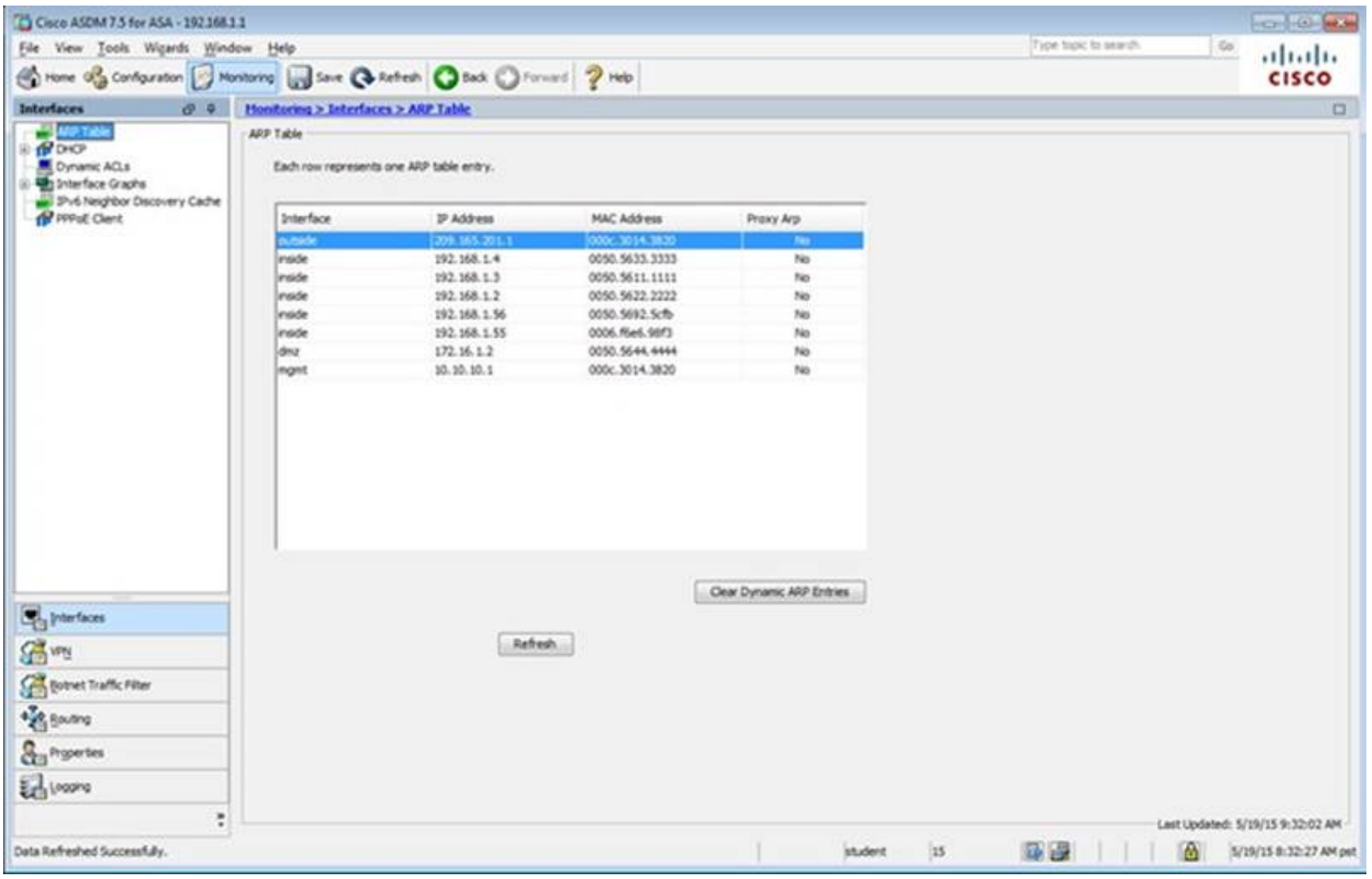
A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.
D. The isolated port can communicate only with other isolated ports.

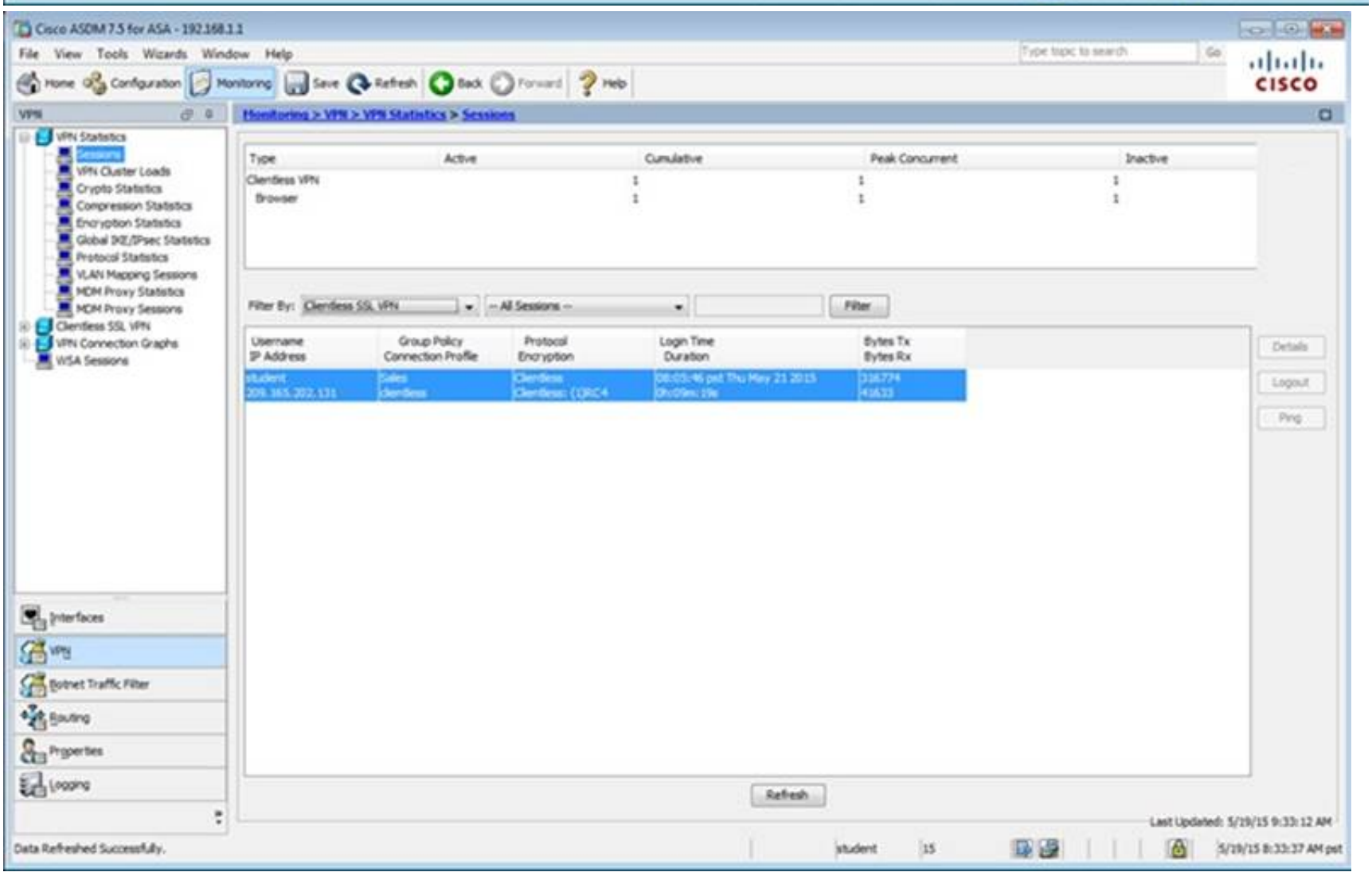
Answer: A

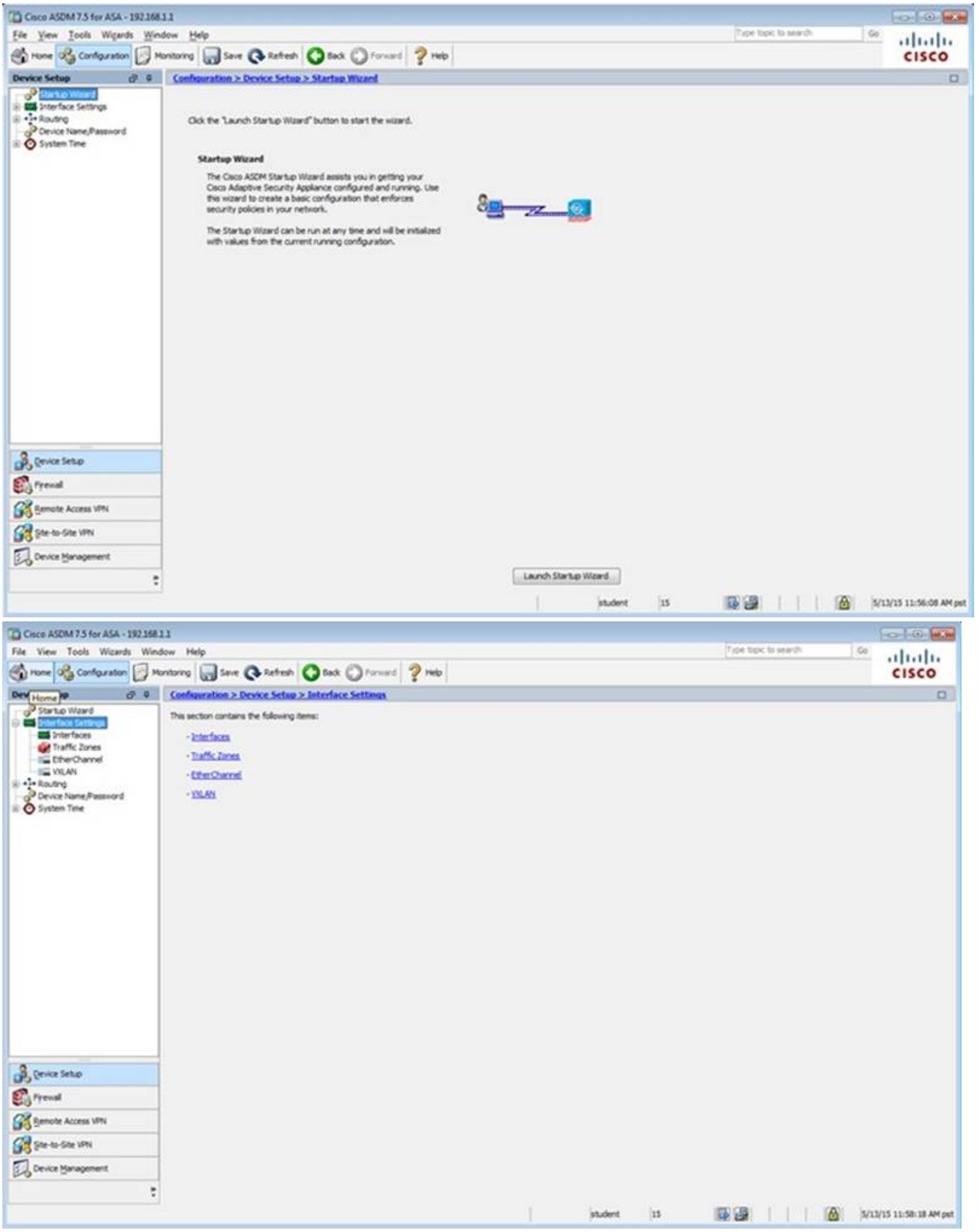
Explanation: Isolated -- An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports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

NEW QUESTION 13
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.

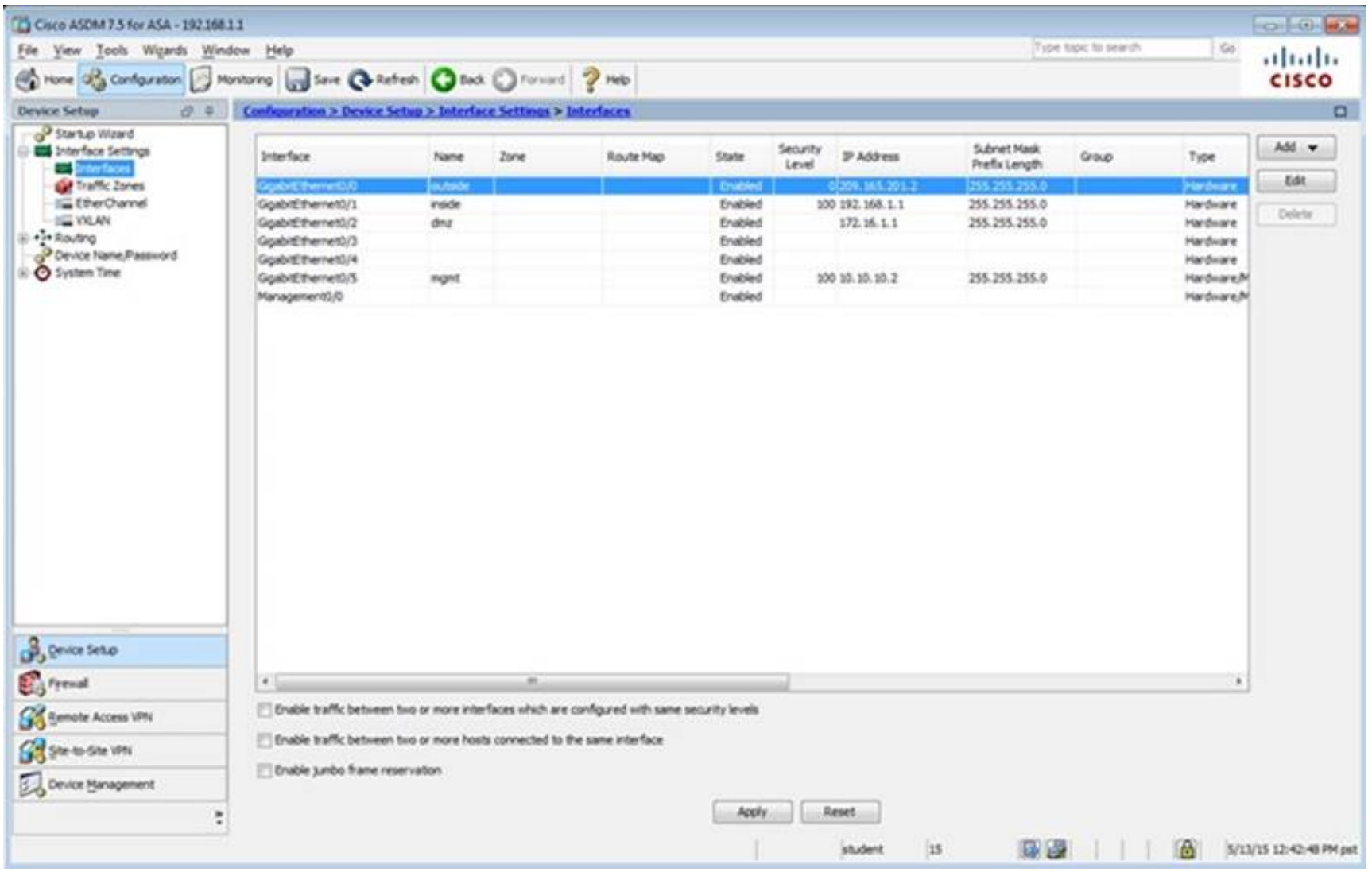


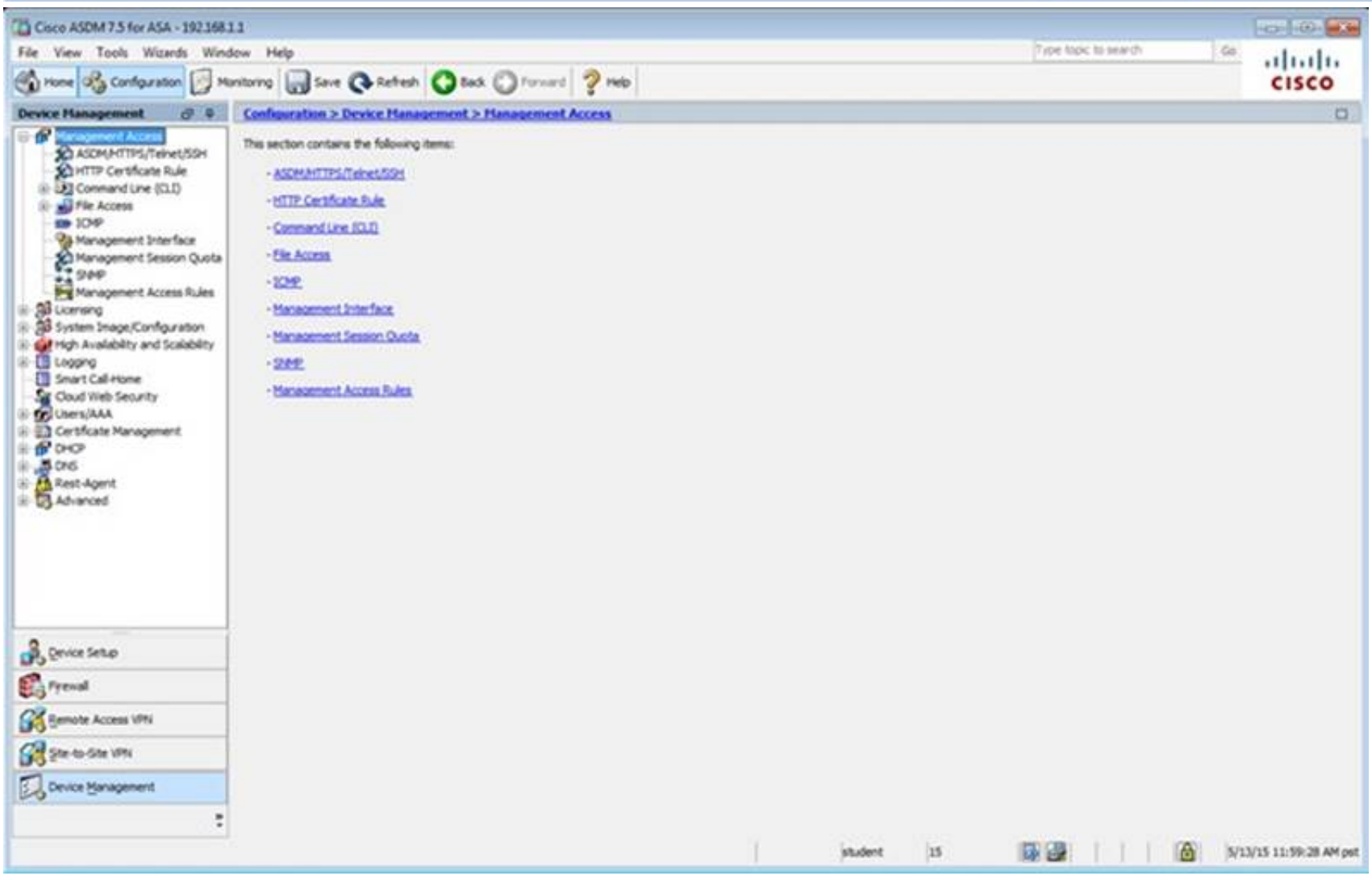

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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

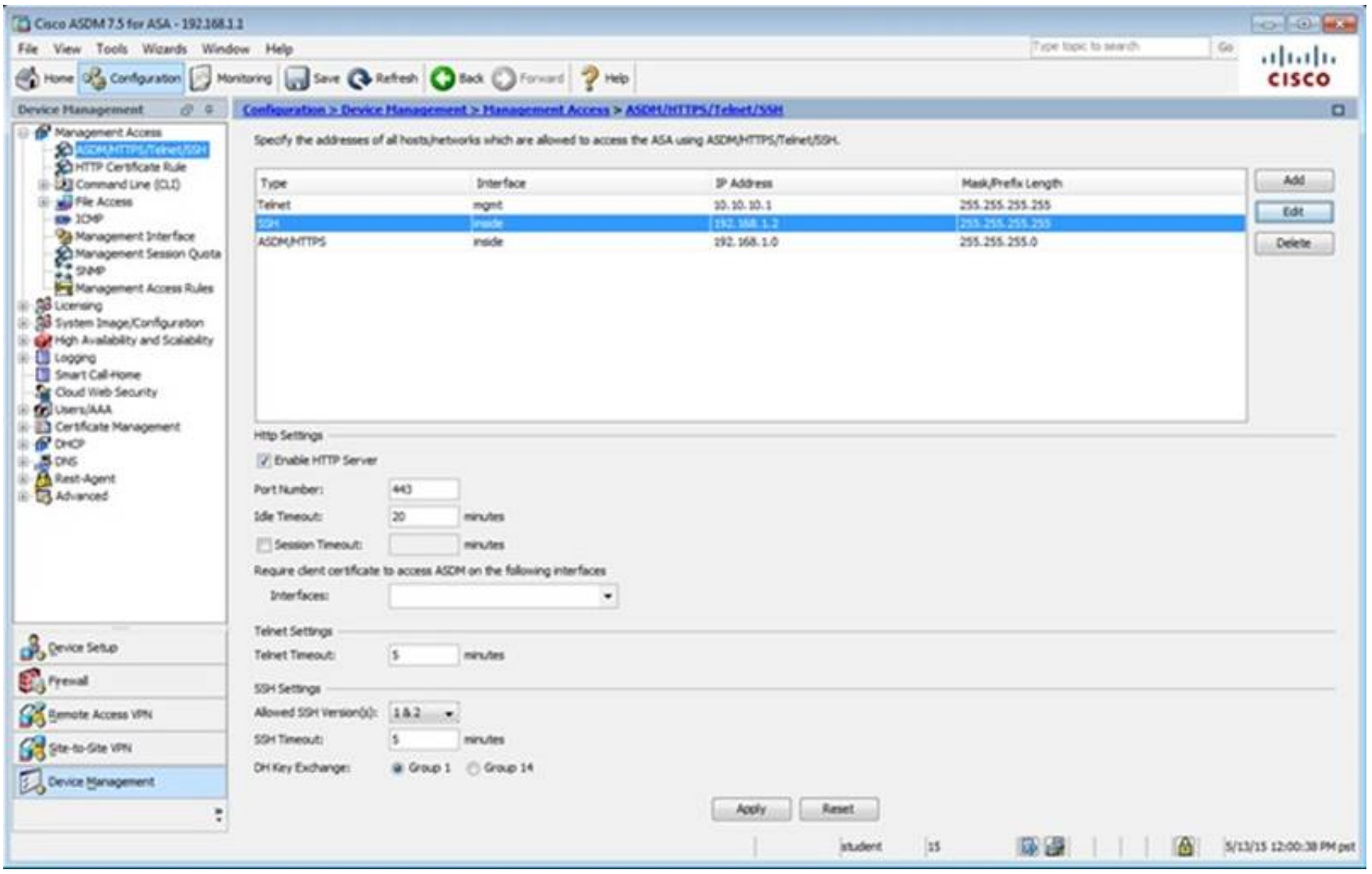

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN 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
Browser 1 1 1
Filter By: Clientless SSL VPN -- All Sessions -- Filter
Username IP Address Group Policy Connection Profile Protocol Encryption Login Time Duration Bytes Tx Bytes Rx
student 209.165.202.131 Sales clientless Clientless Clientless: (1)RC4 08:05:46 pst Thu May 21 2015 0h:09m:19s 116774 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

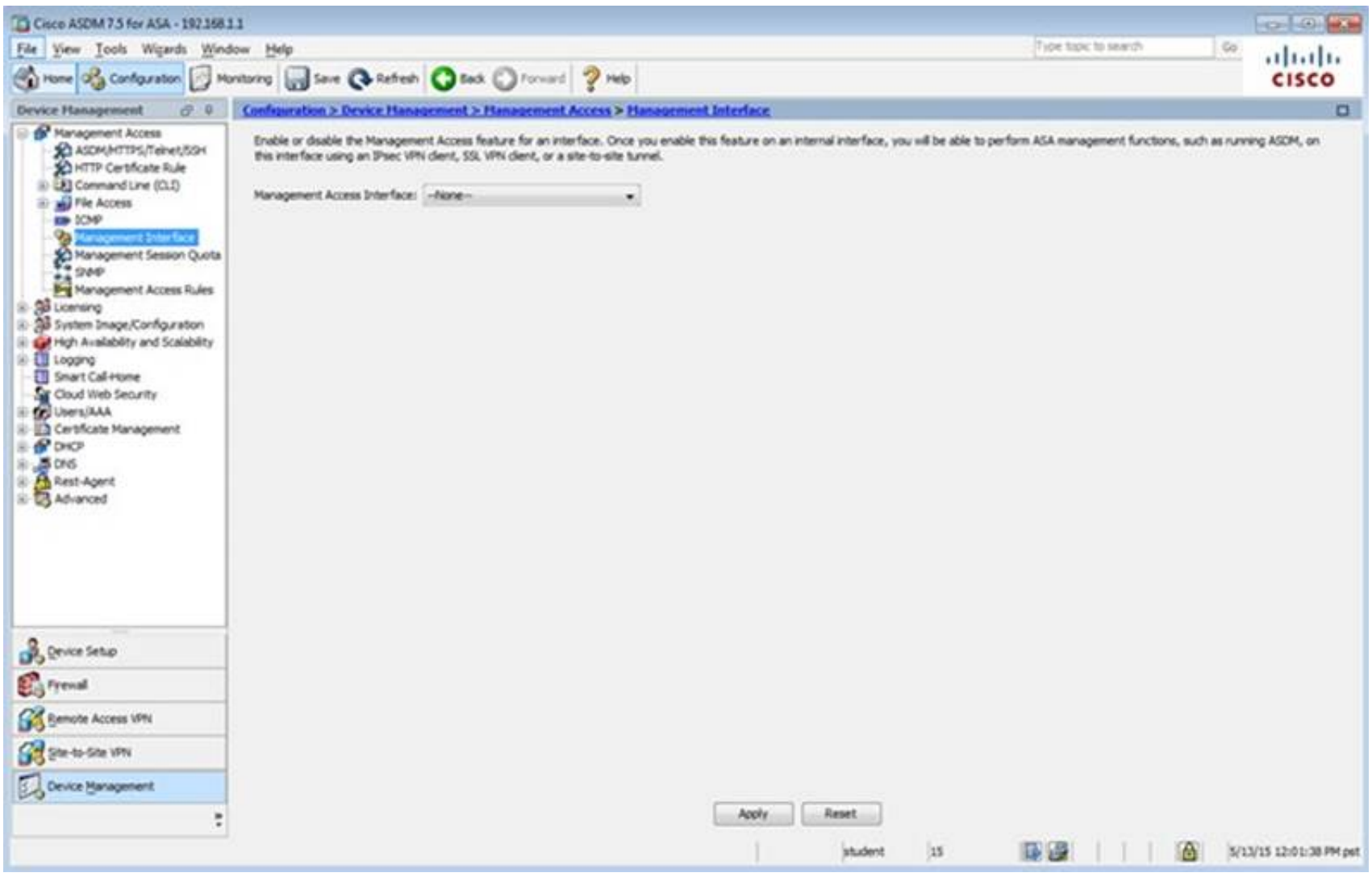

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" 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

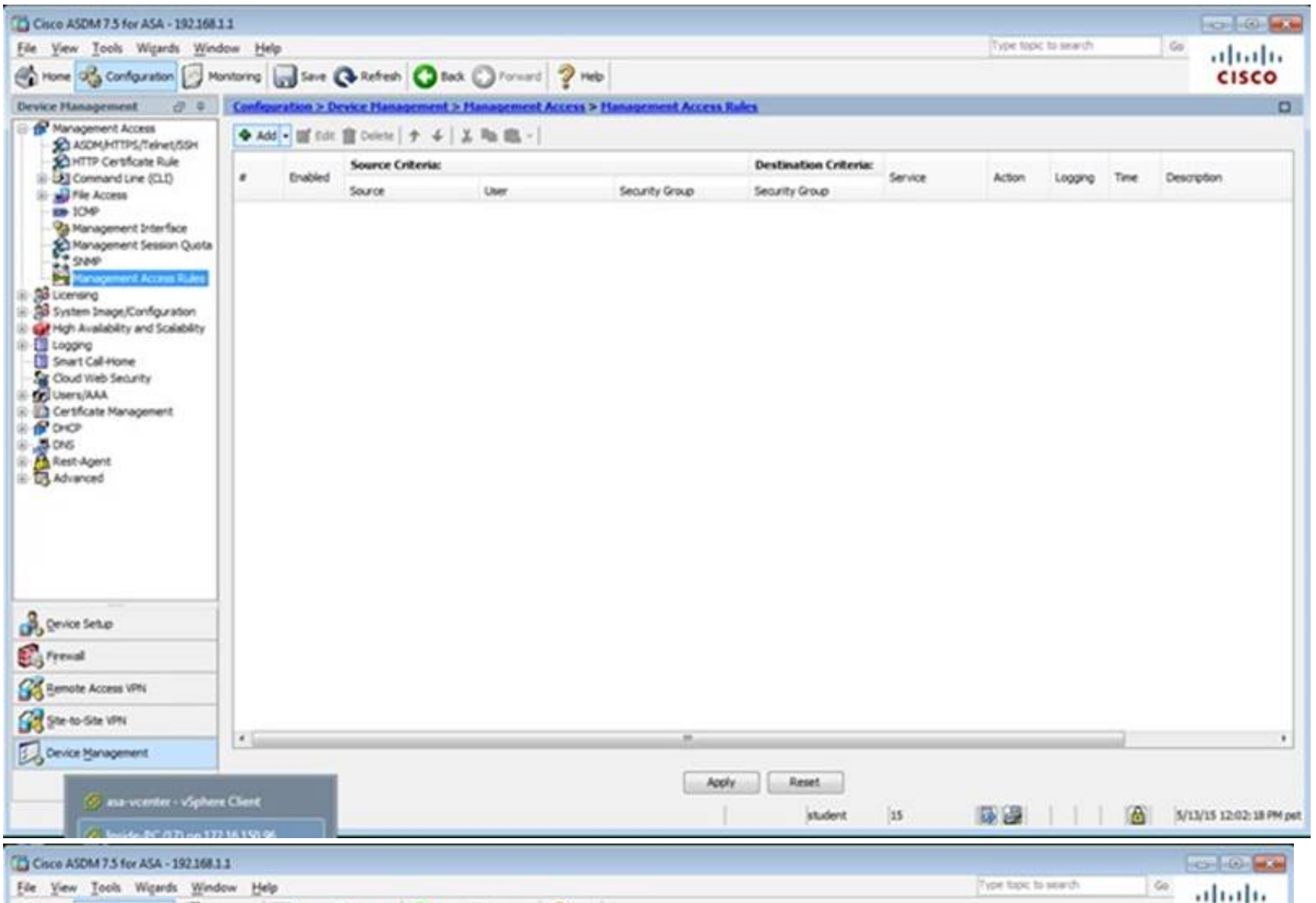
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
Device Name/Password
System Time
Configuration > Device Setup > Interface 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

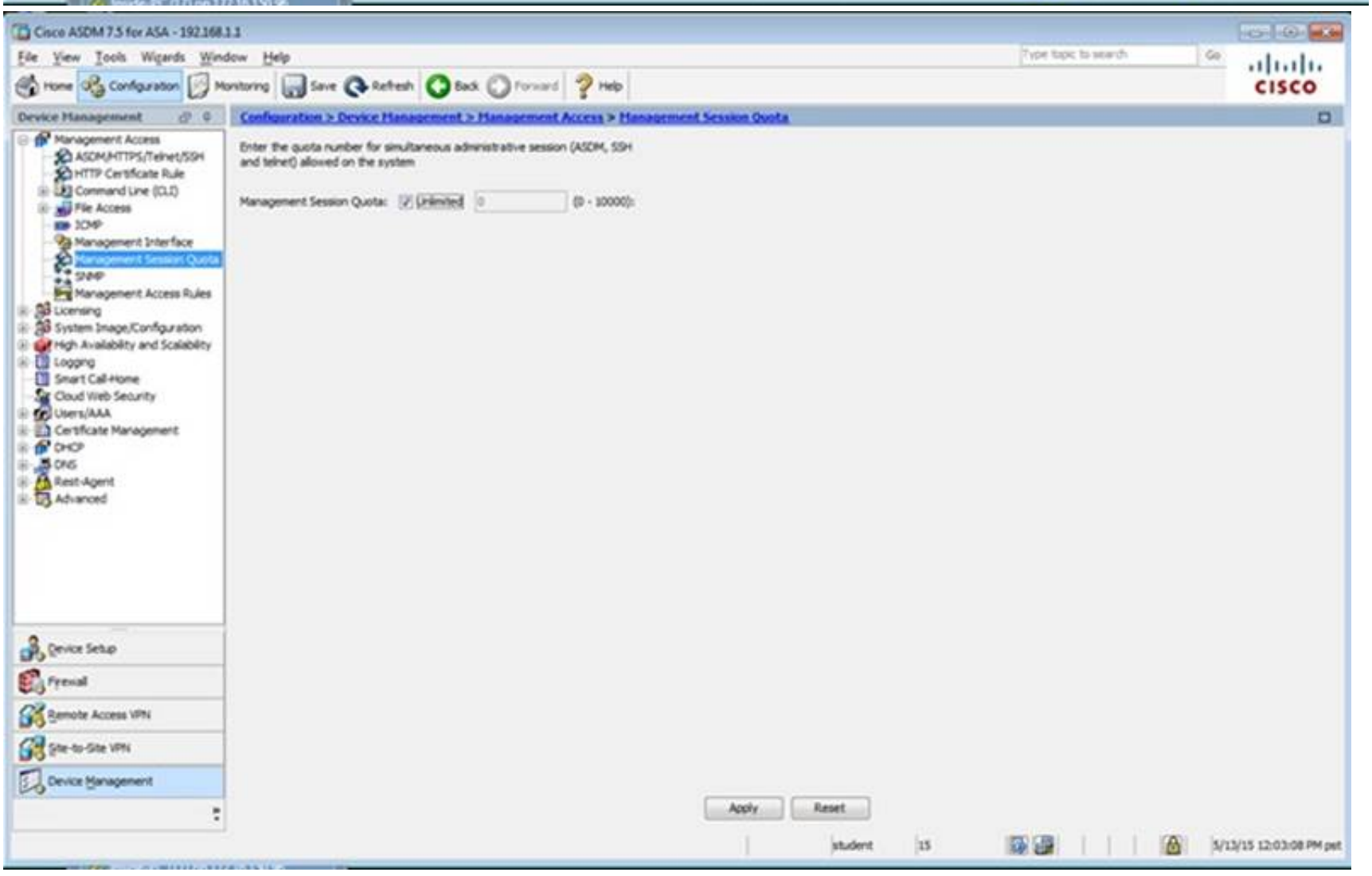

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Configuration > Device Setup > Interface Settings > Interfaces
Startup Wizard
Interface Settings
Interfaces
Traffic Zones
EtherChannel
VXLAN
Routing
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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

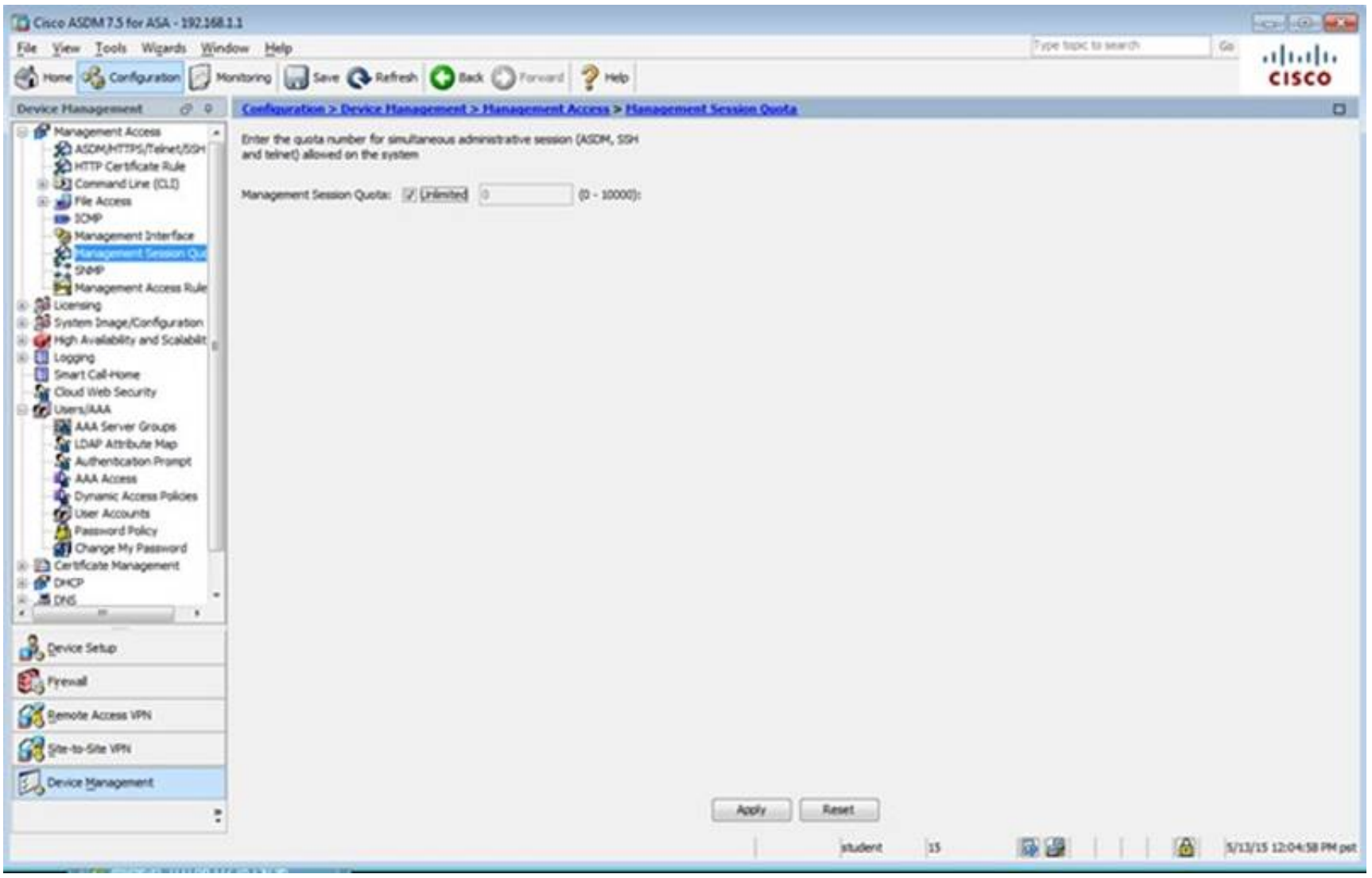

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
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

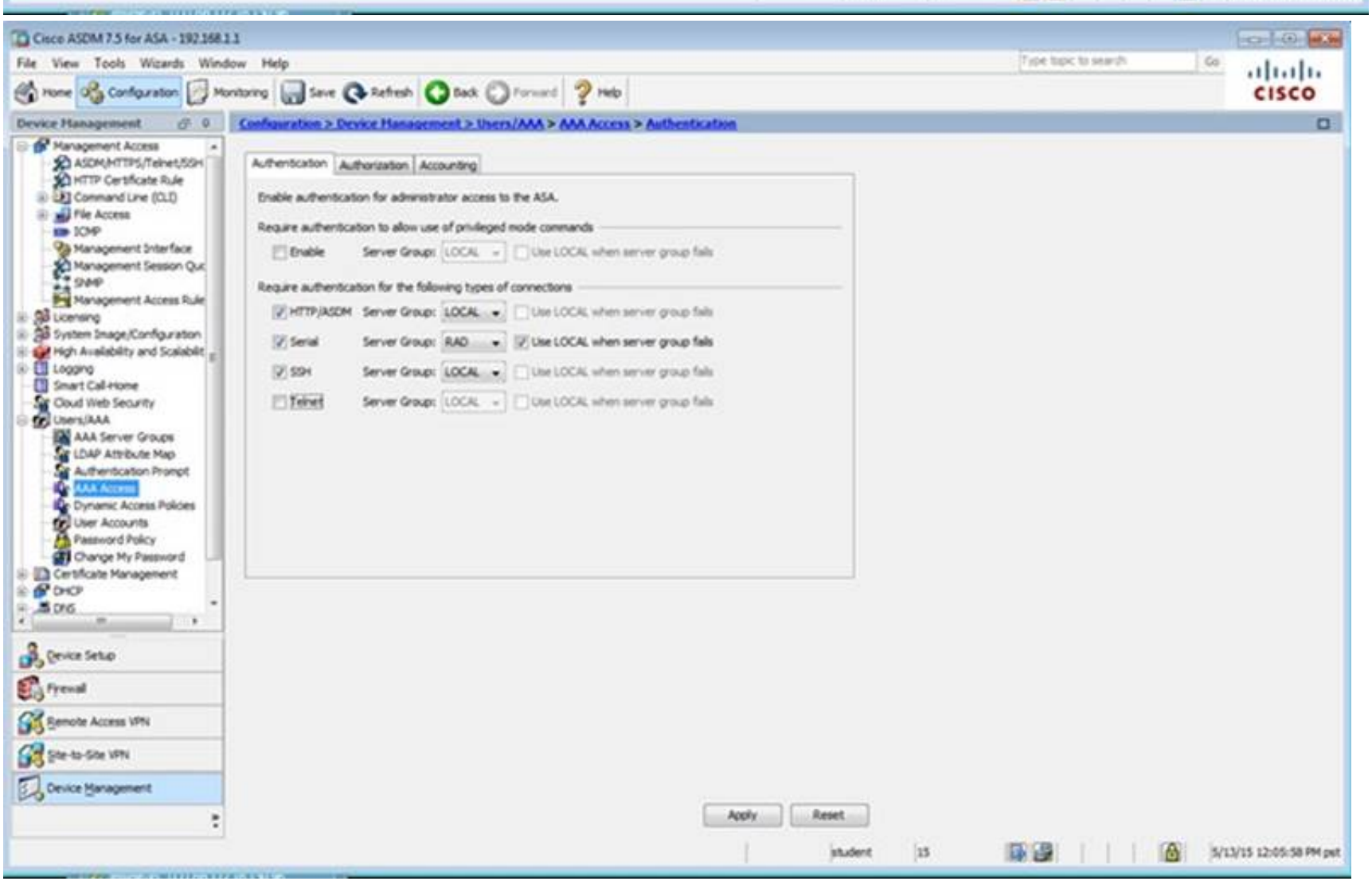

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Specify the addresses of all hosts/networks which are allowed to 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

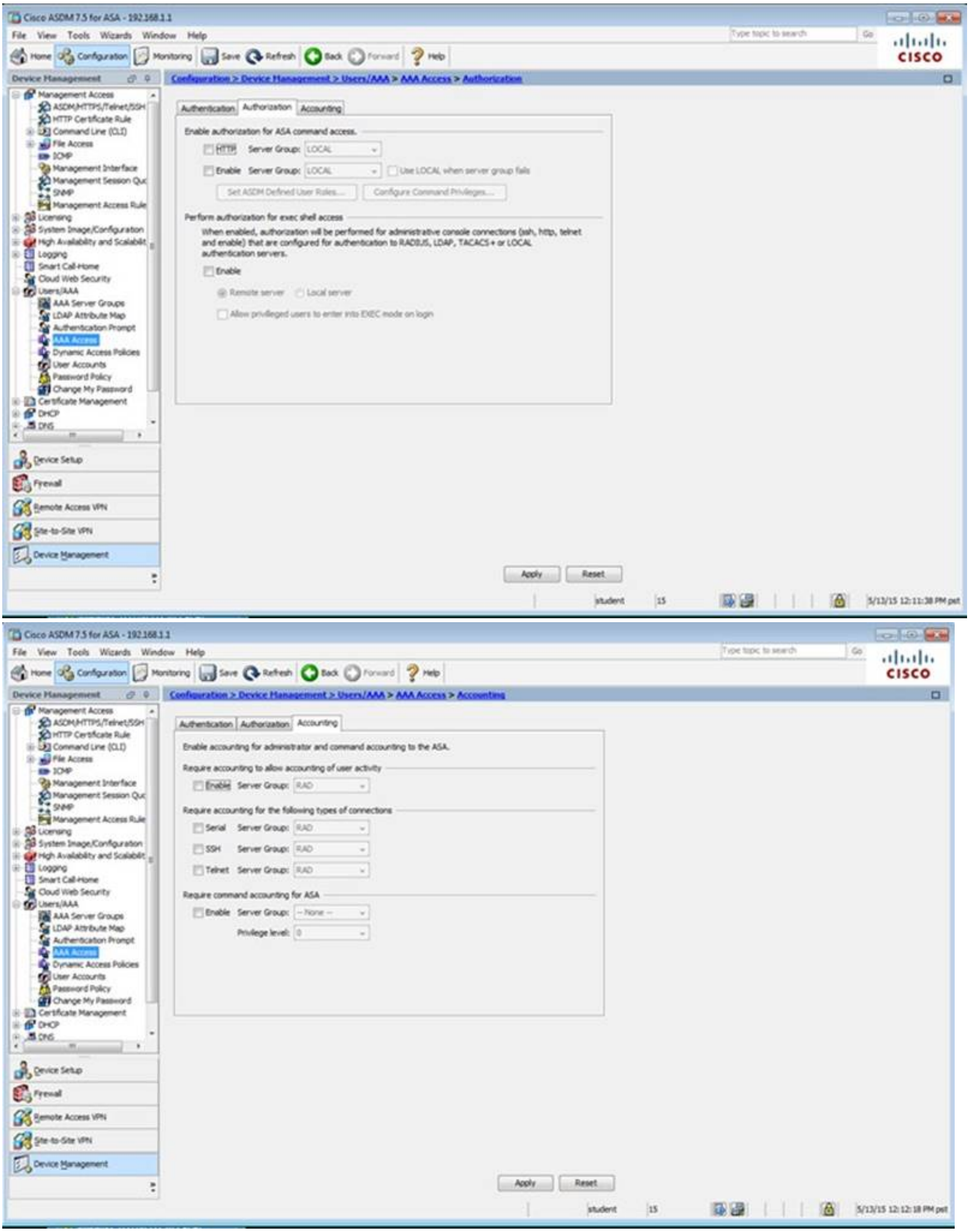

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Enable or disable the Management Access feature for an interface. 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

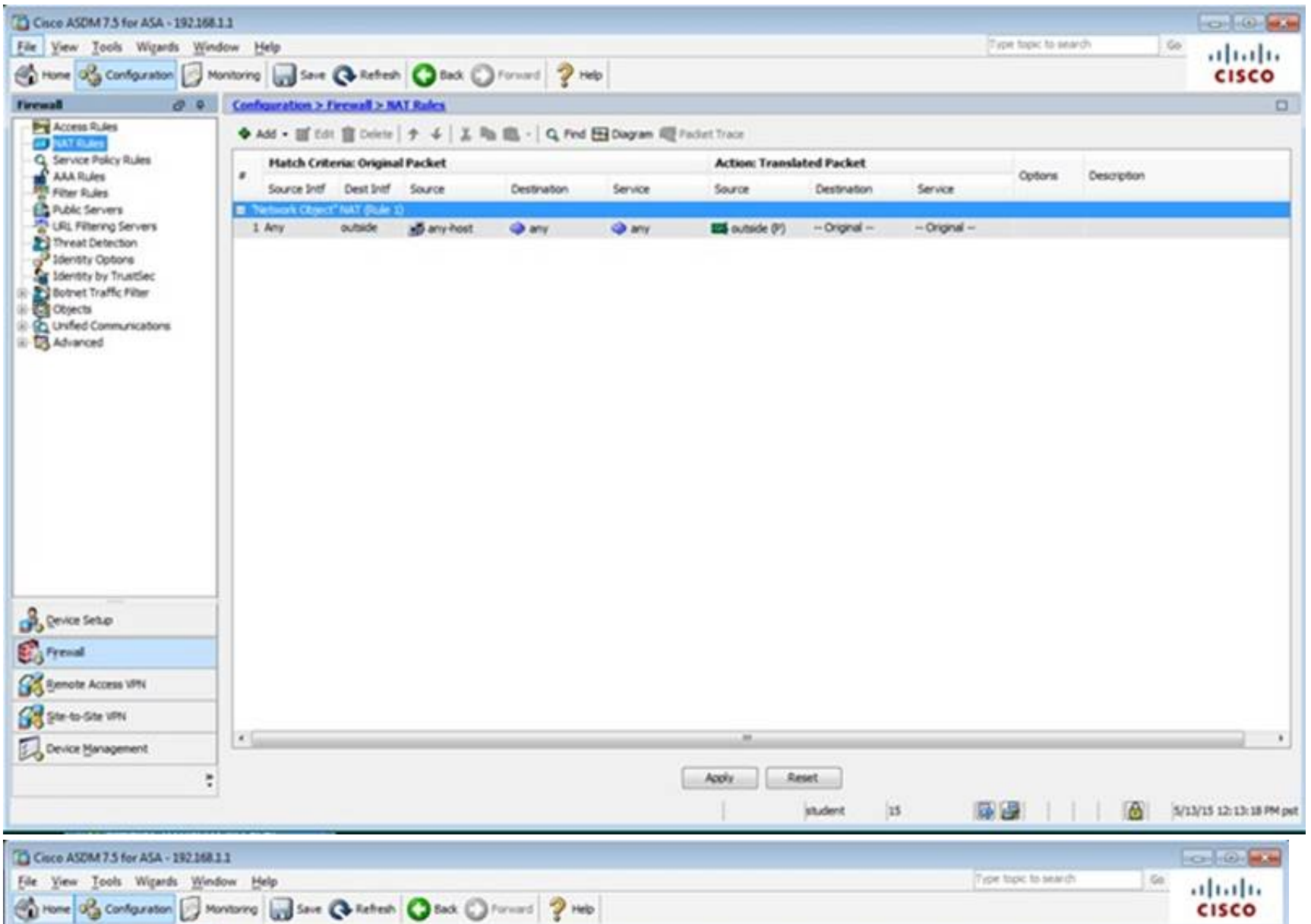

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (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

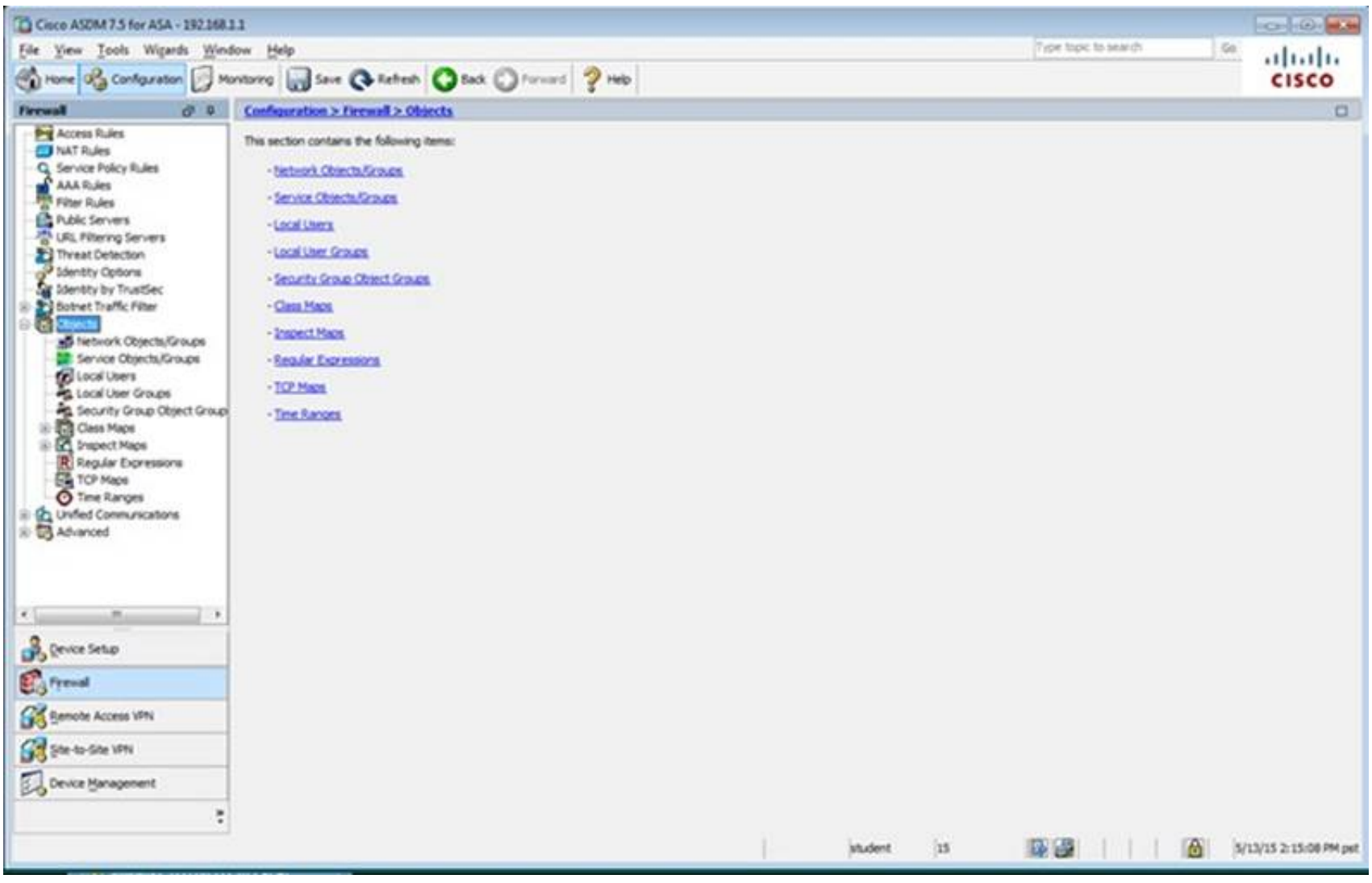

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
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

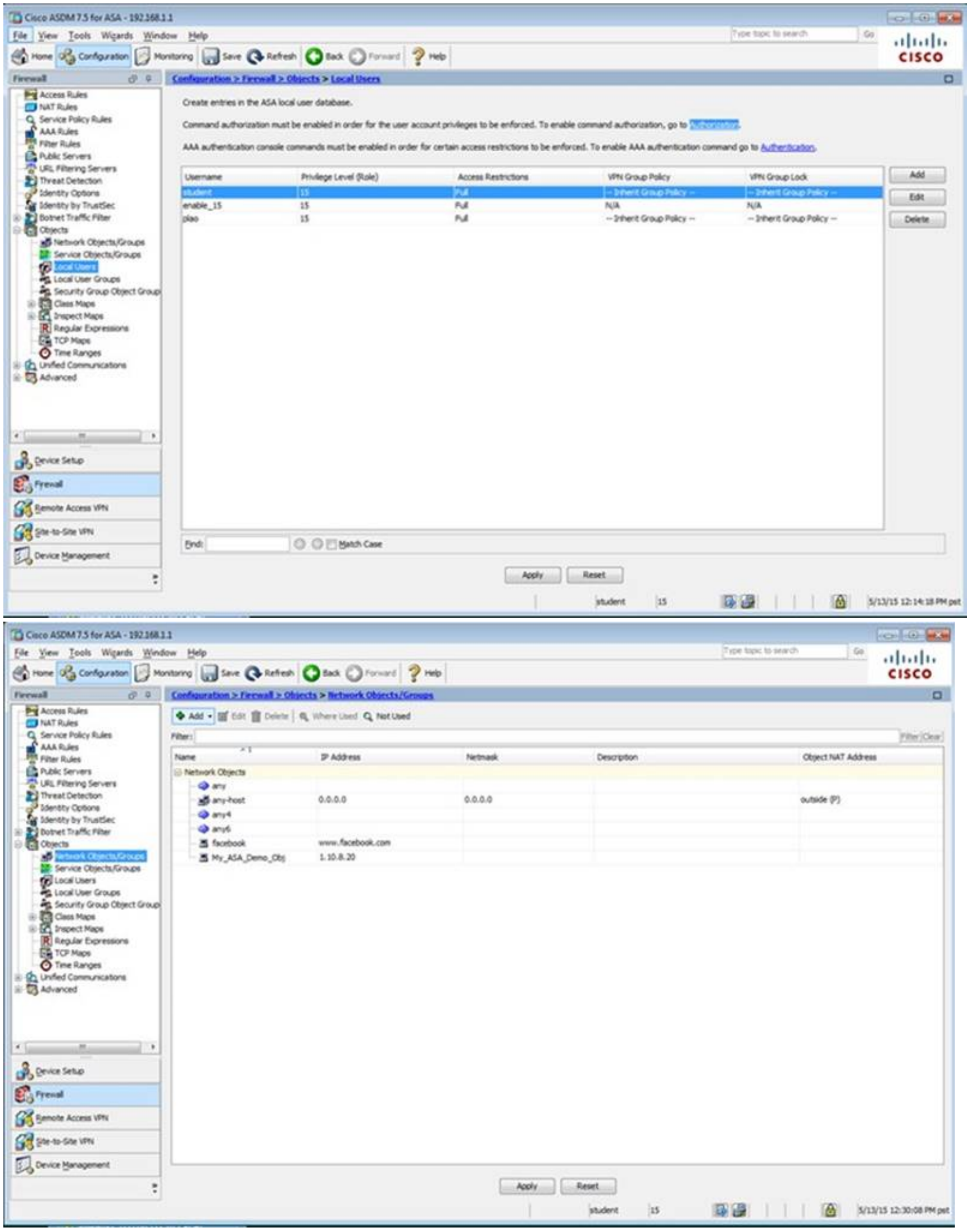

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command Line (CLI)
File Access
ICMP
Management Interface
Management Session 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
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

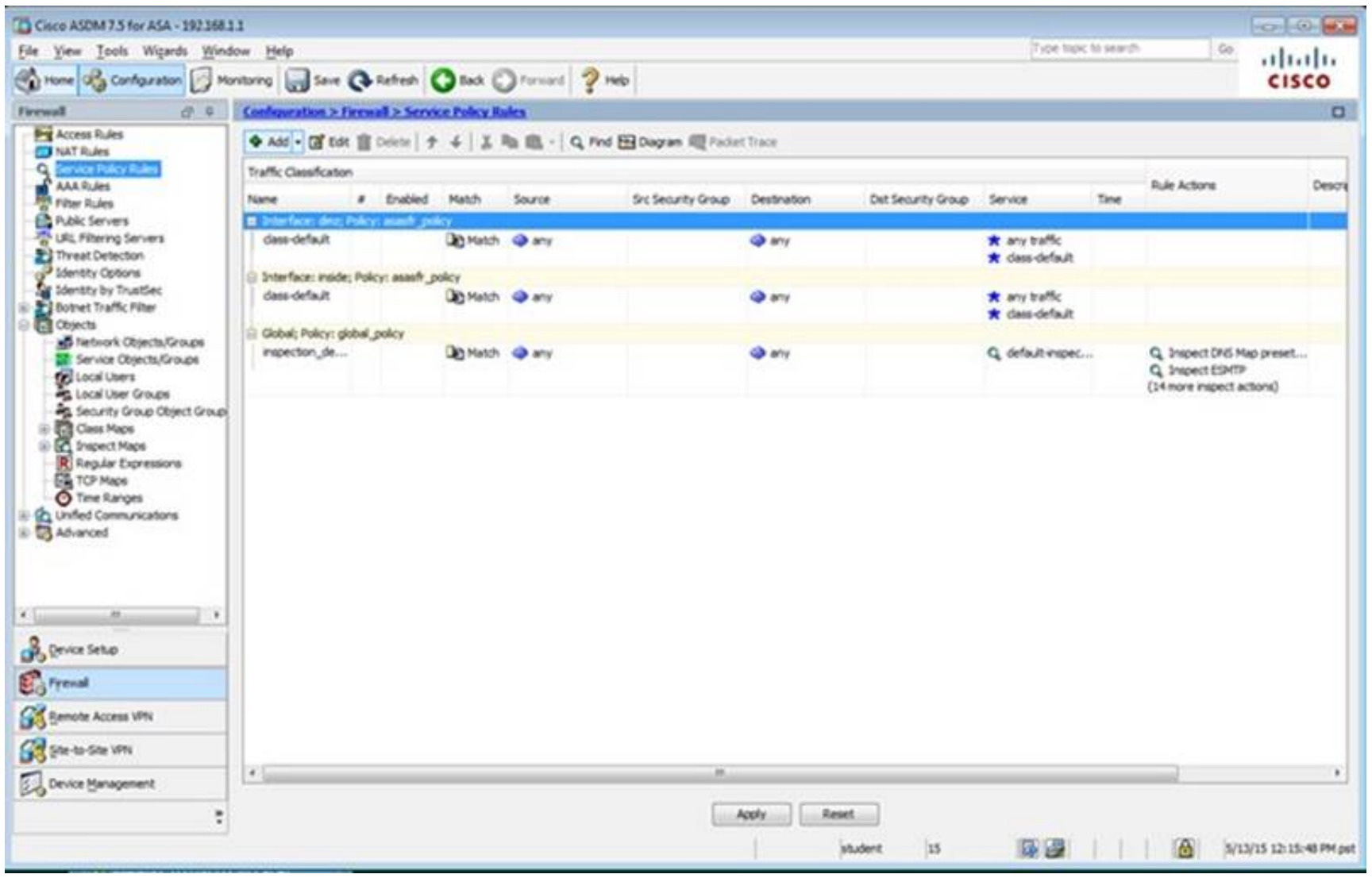
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Authentication Authorization Accounting
Enable accounting for administrator 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

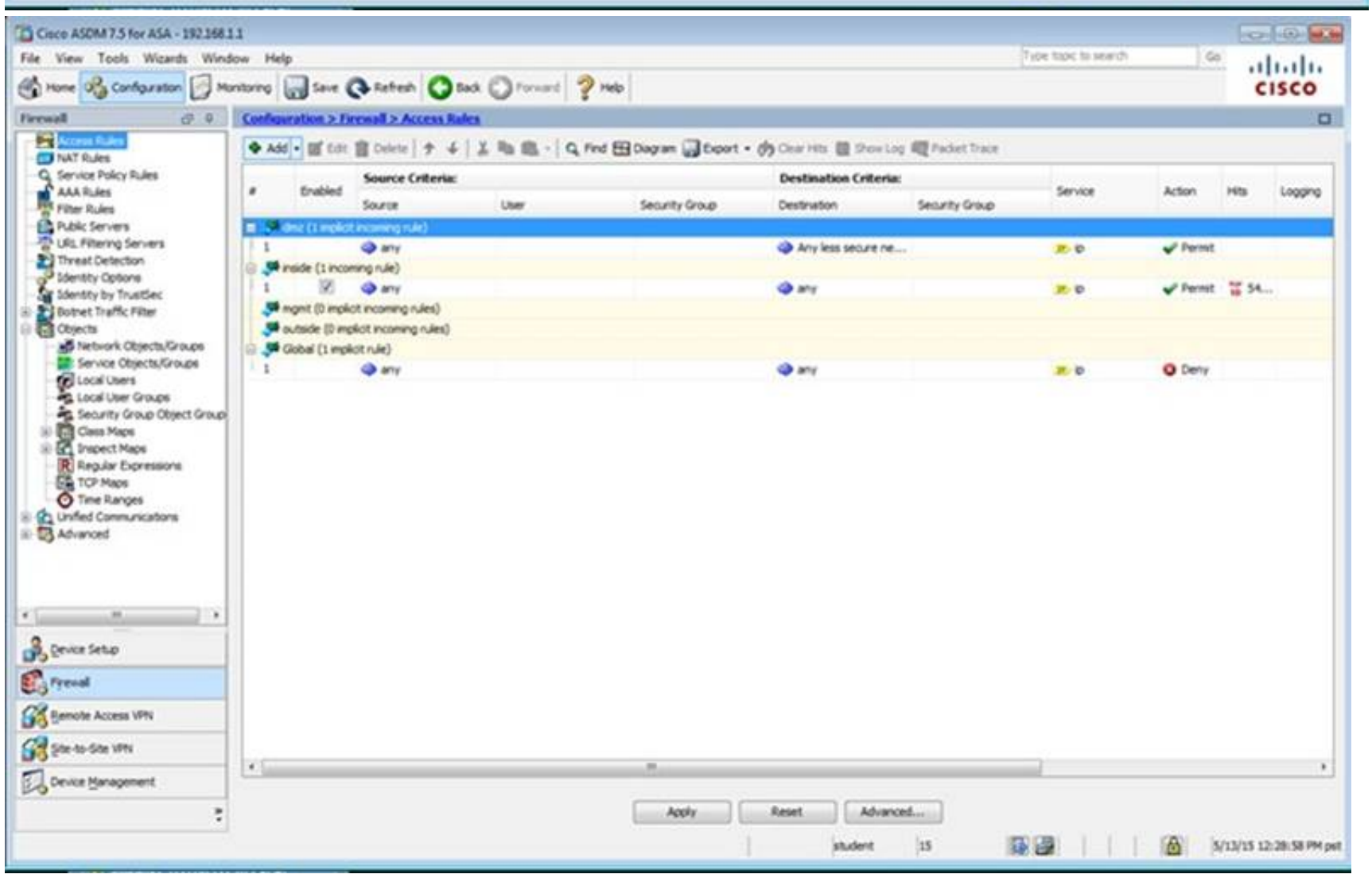

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
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

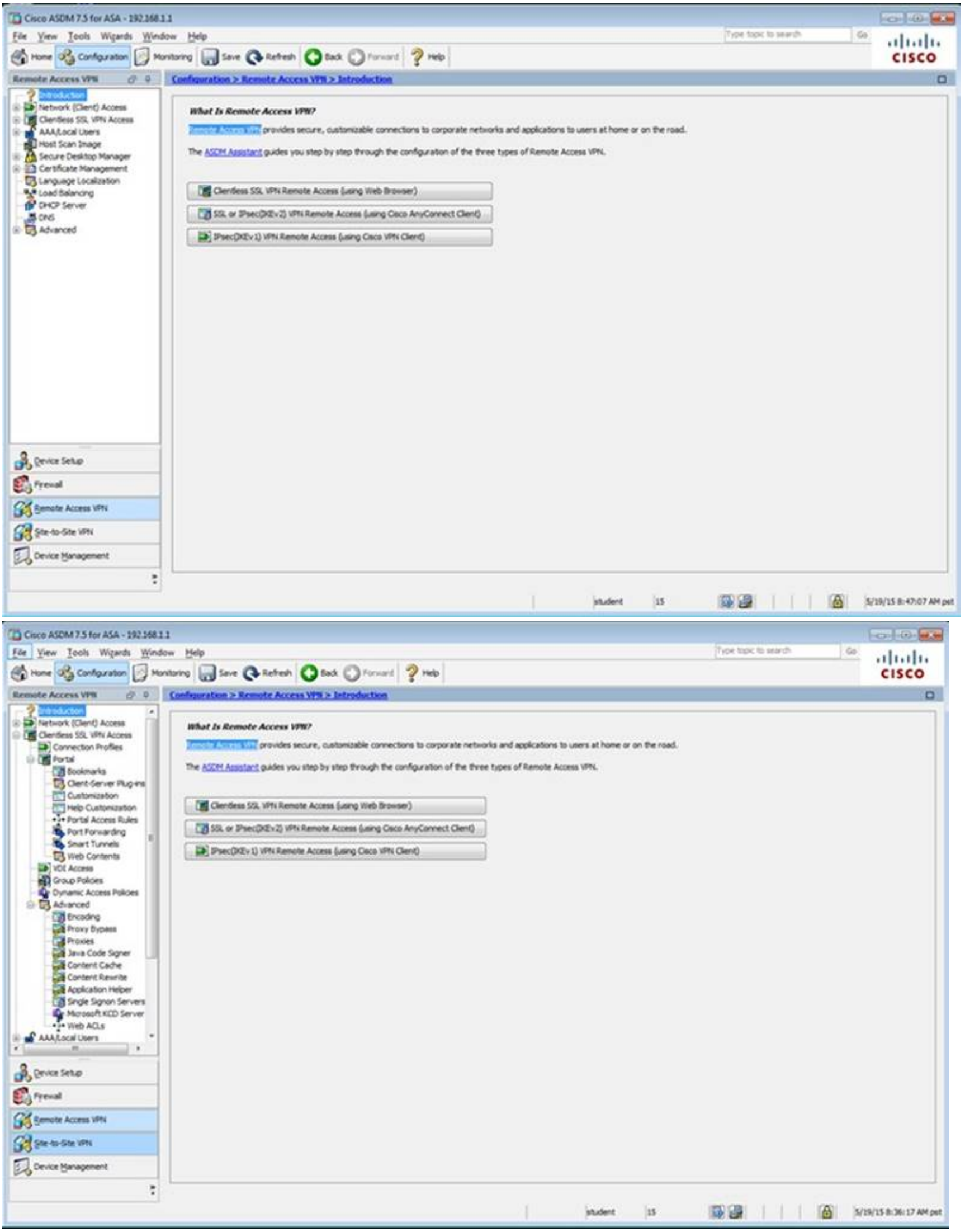

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects
This section contains the following items:
- Network Objects/Groups
- Service Objects/Groups
- Local Users
- Local User 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

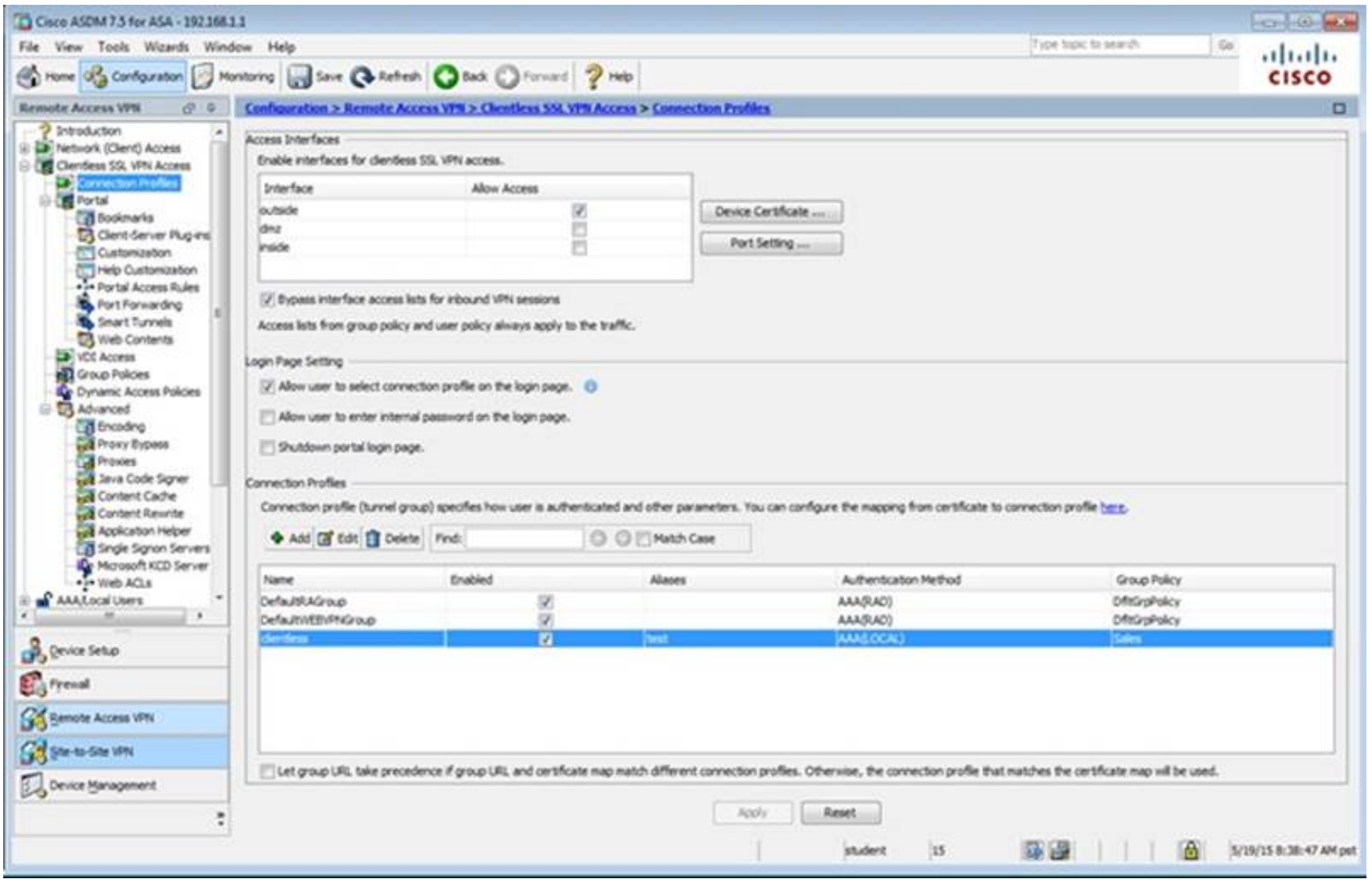

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user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

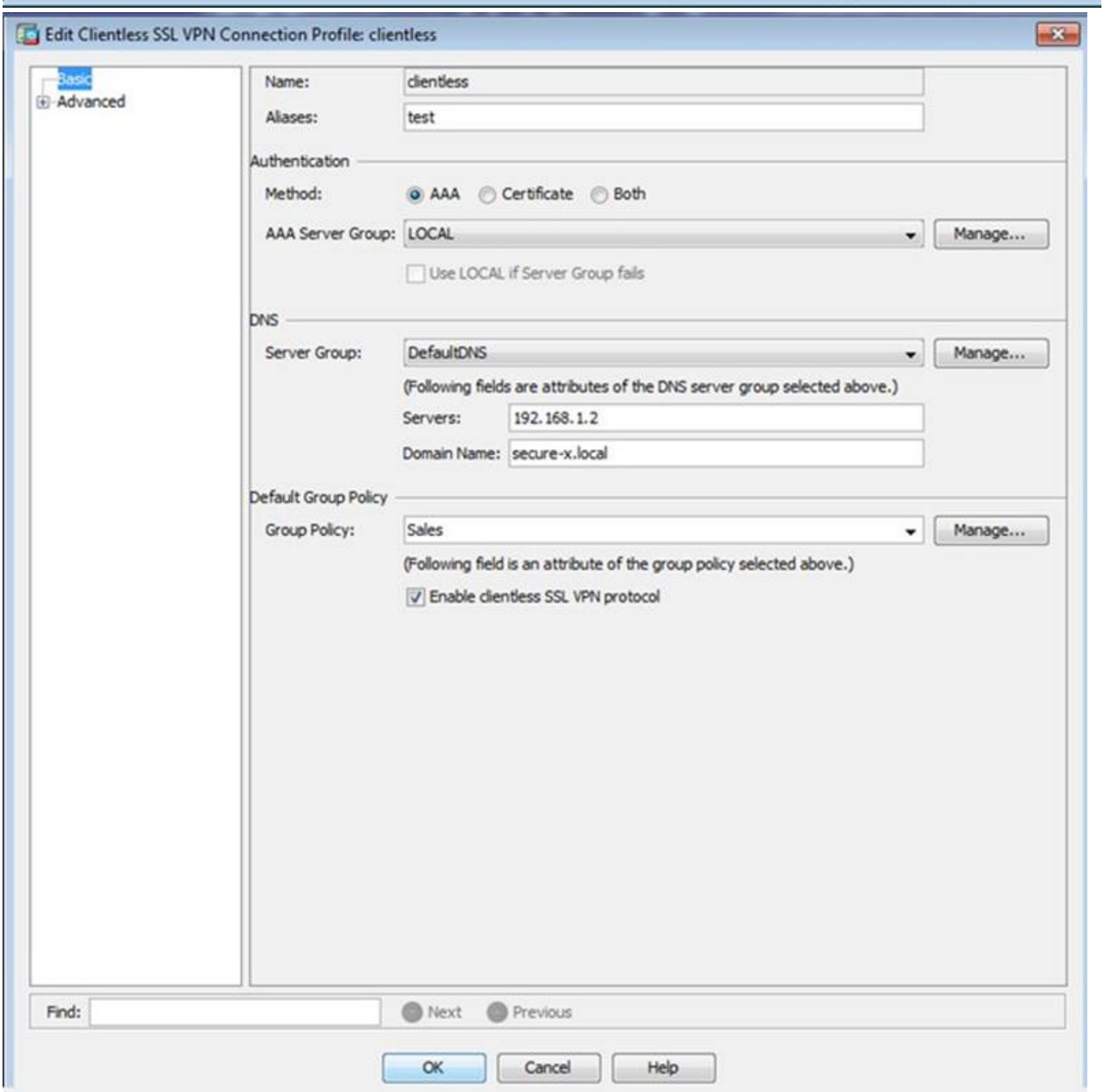
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add Edit Delete Where Used Not Used
Filter:
Name | IP Address | Netmask | Description | Object 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

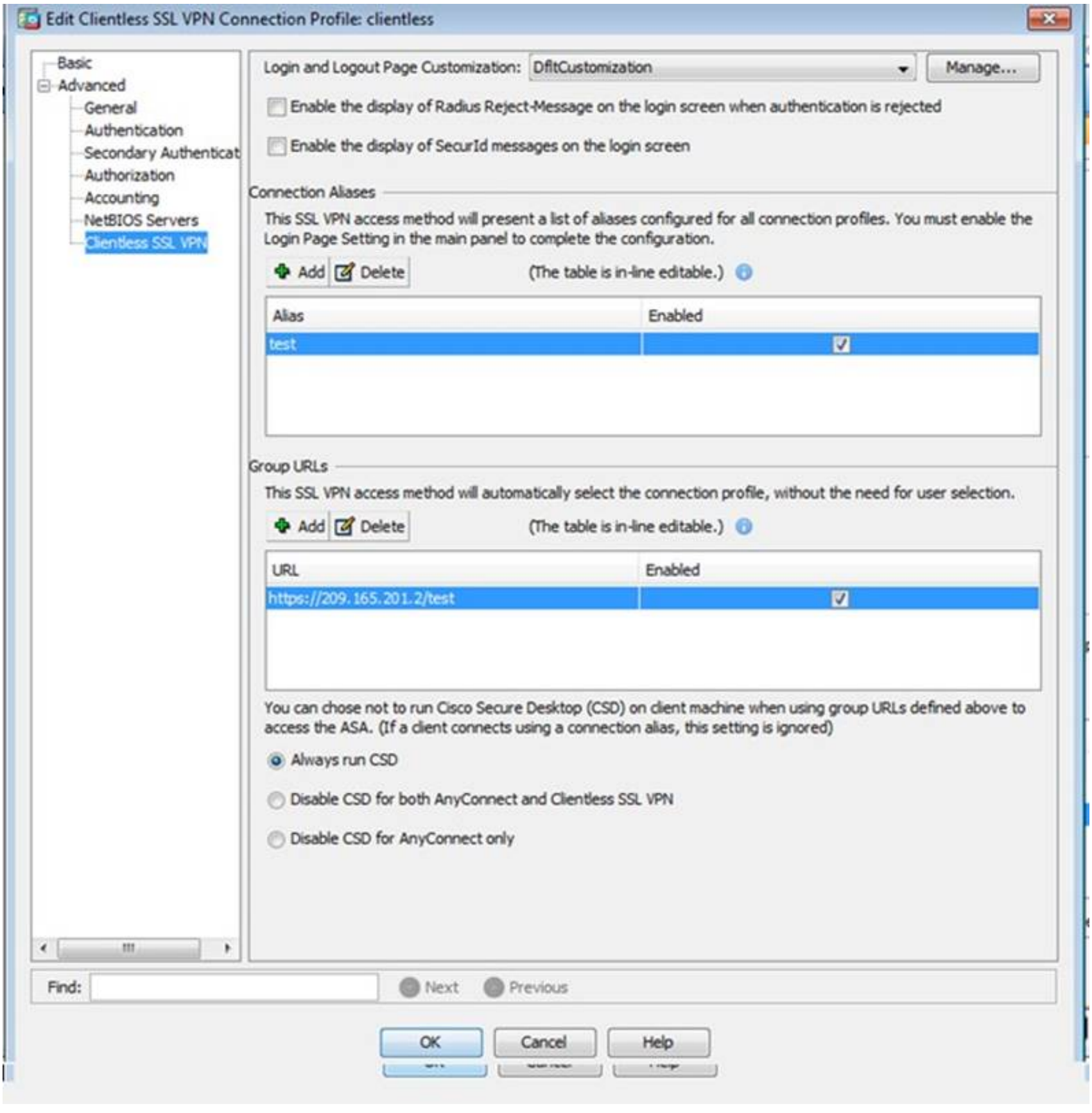

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
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

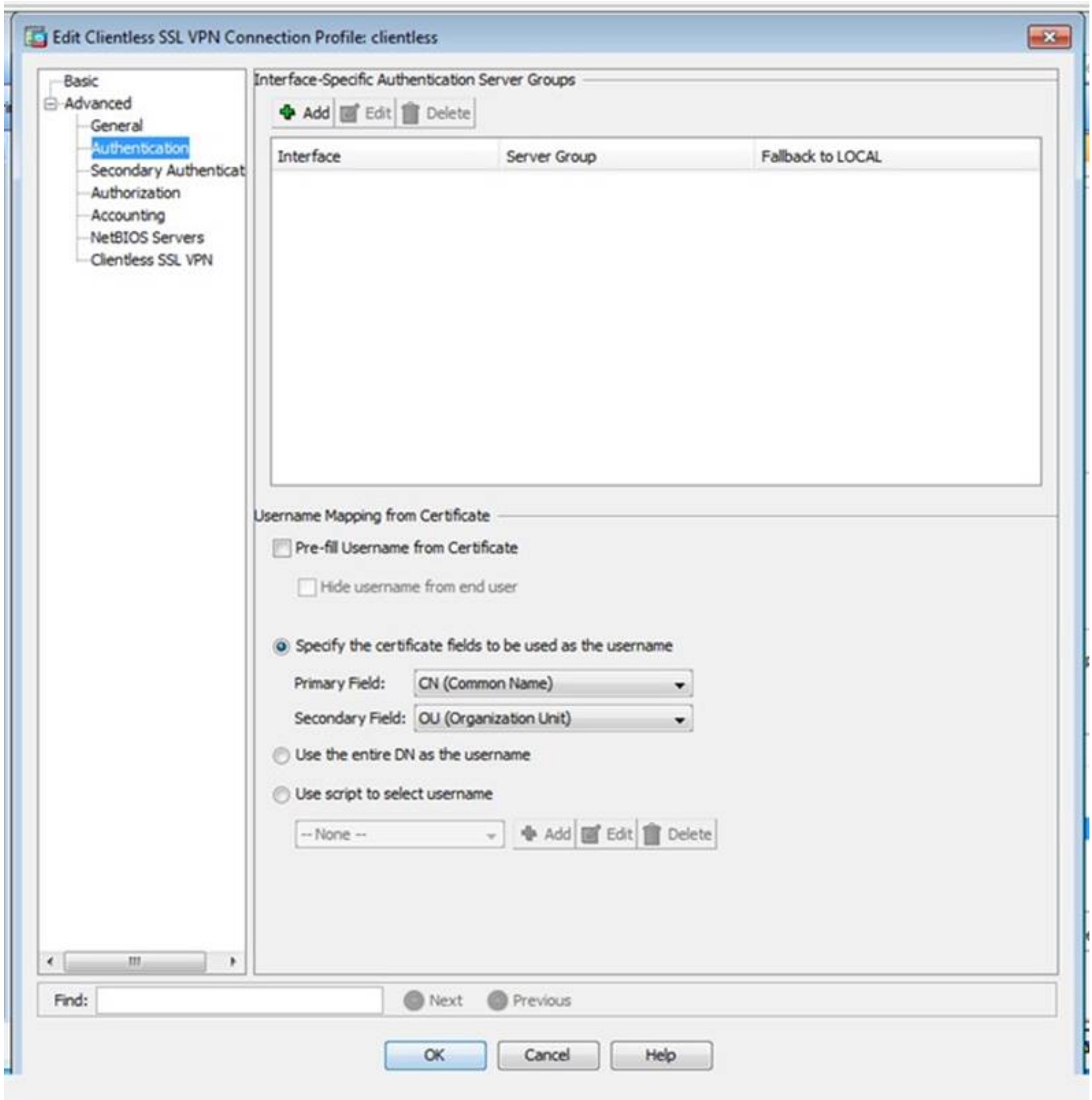

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
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

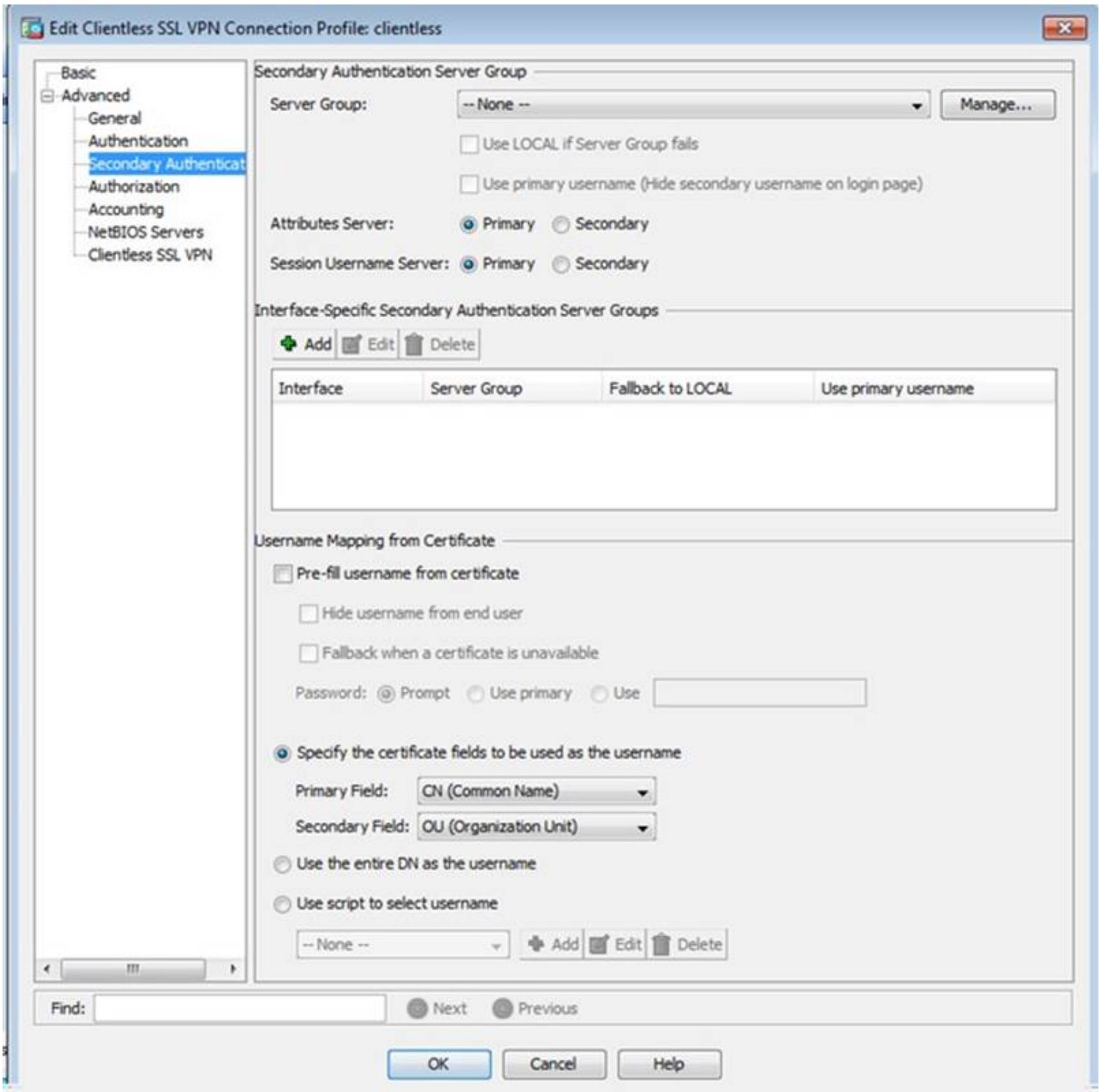

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
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

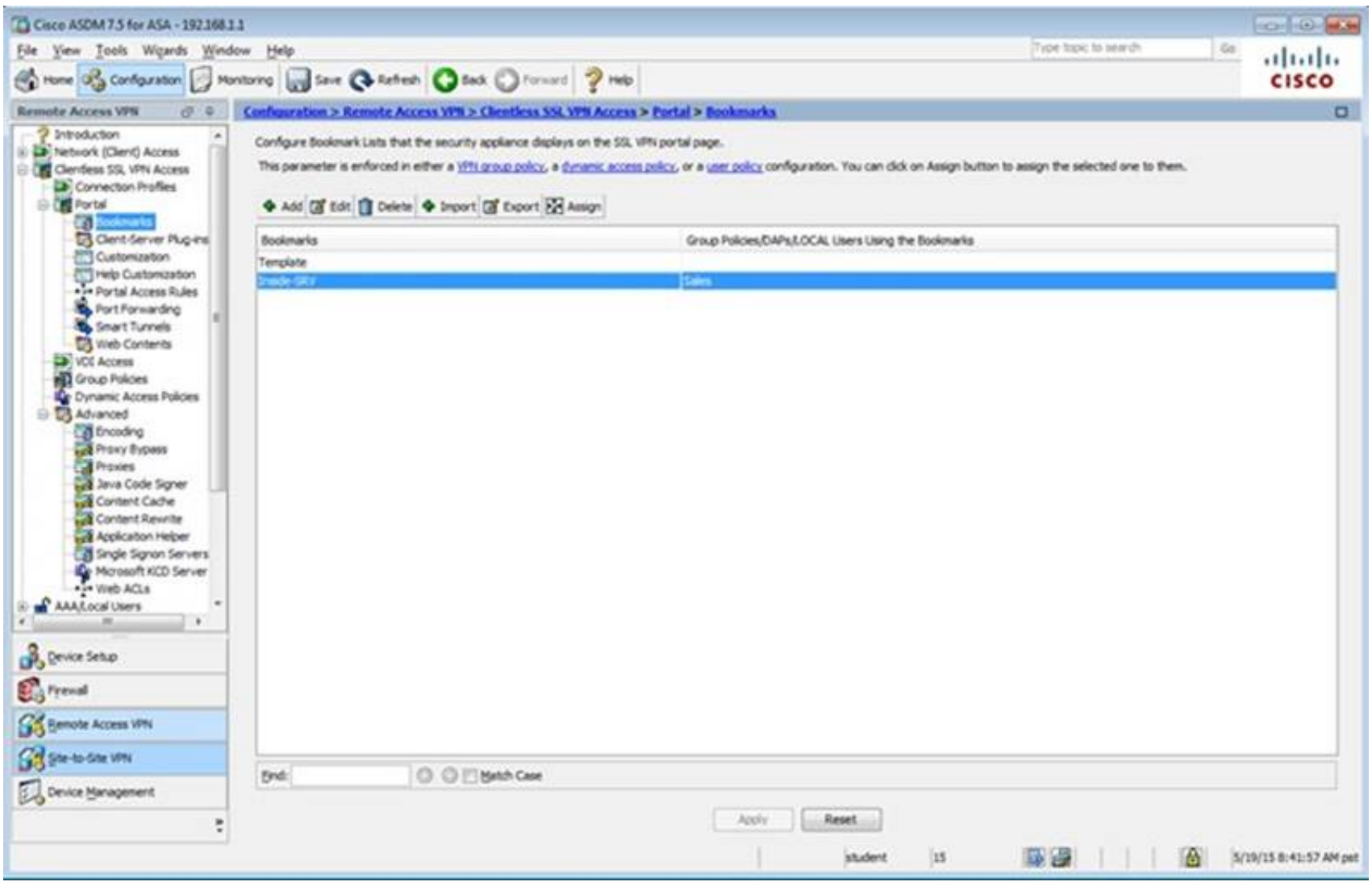

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Introduction
Network (Client) Access
Clientless SSL VPN Access
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
5/19/15 8:38:47 AM pst

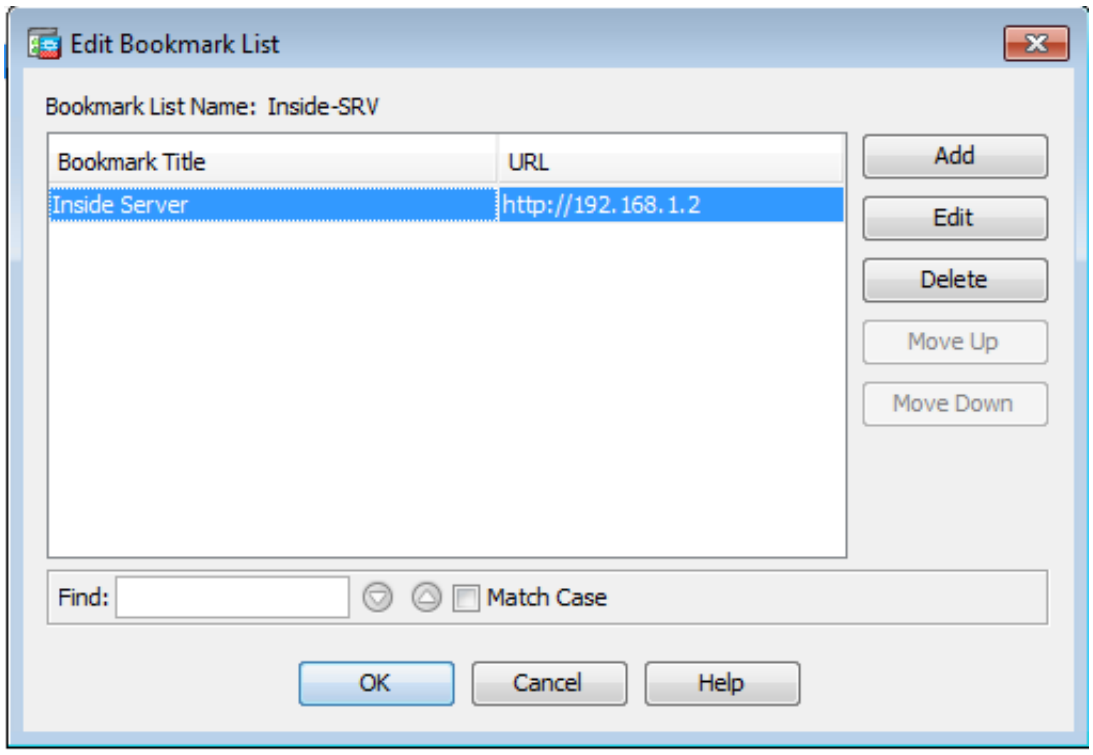

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server 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

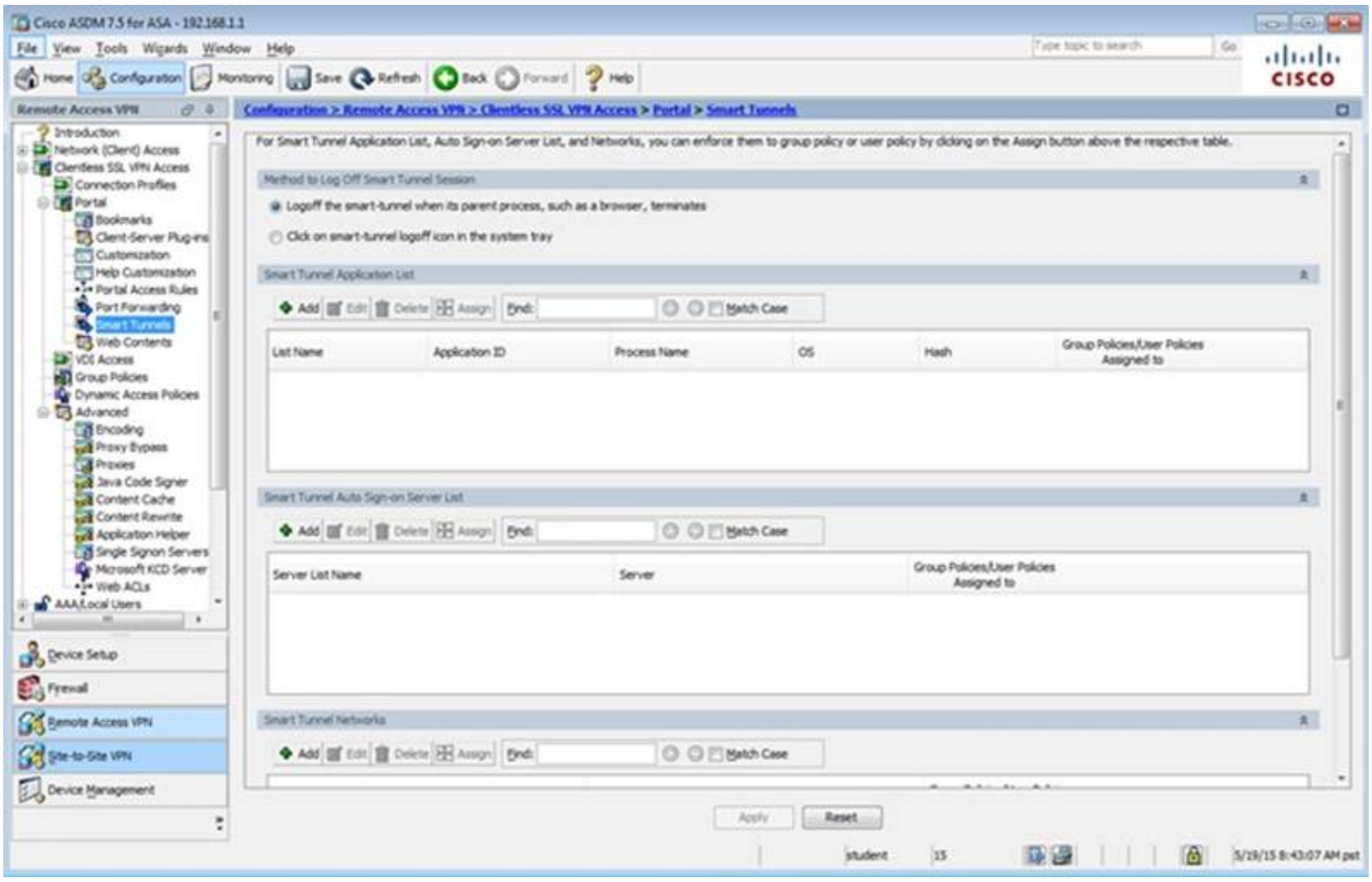

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen 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

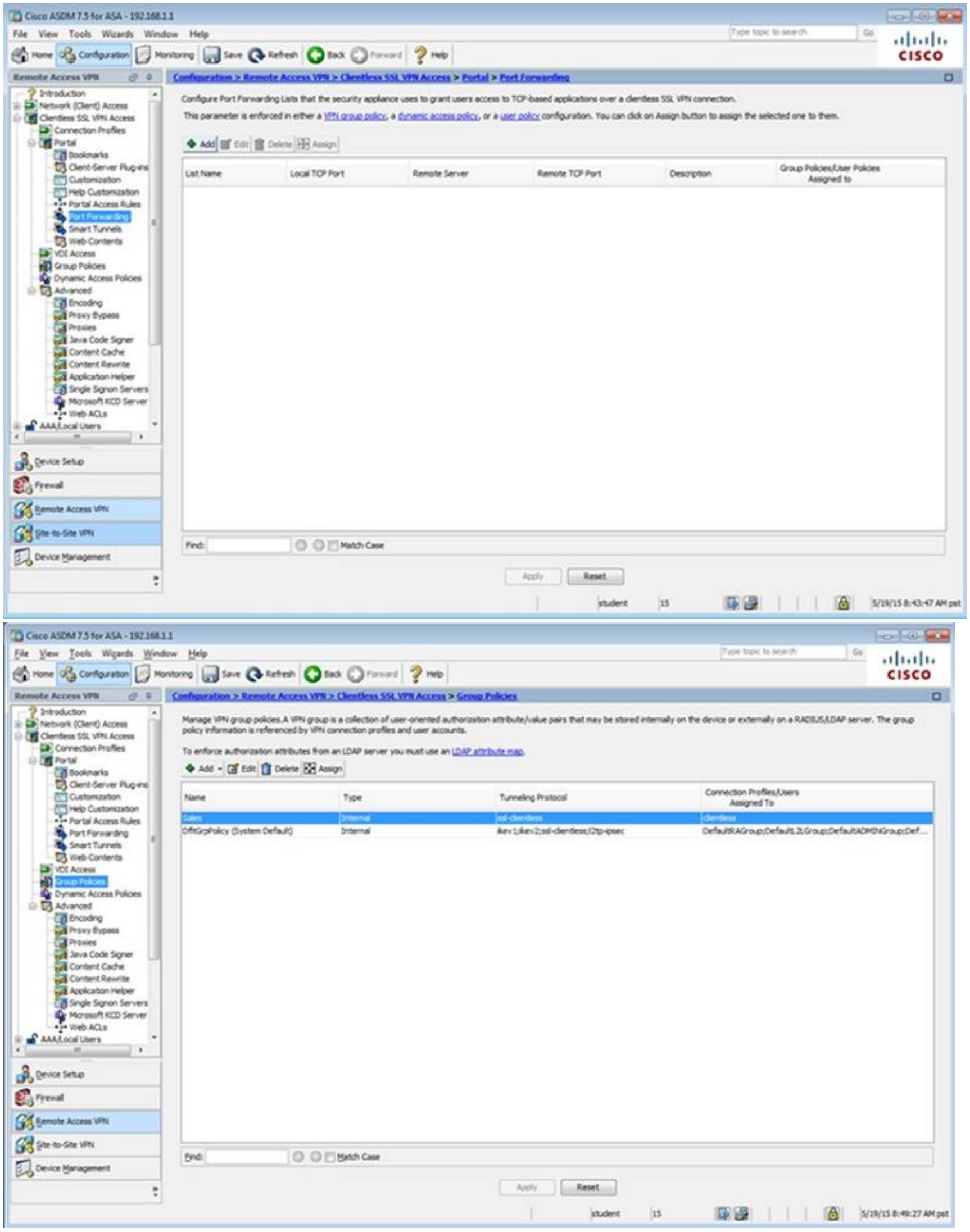

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from 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

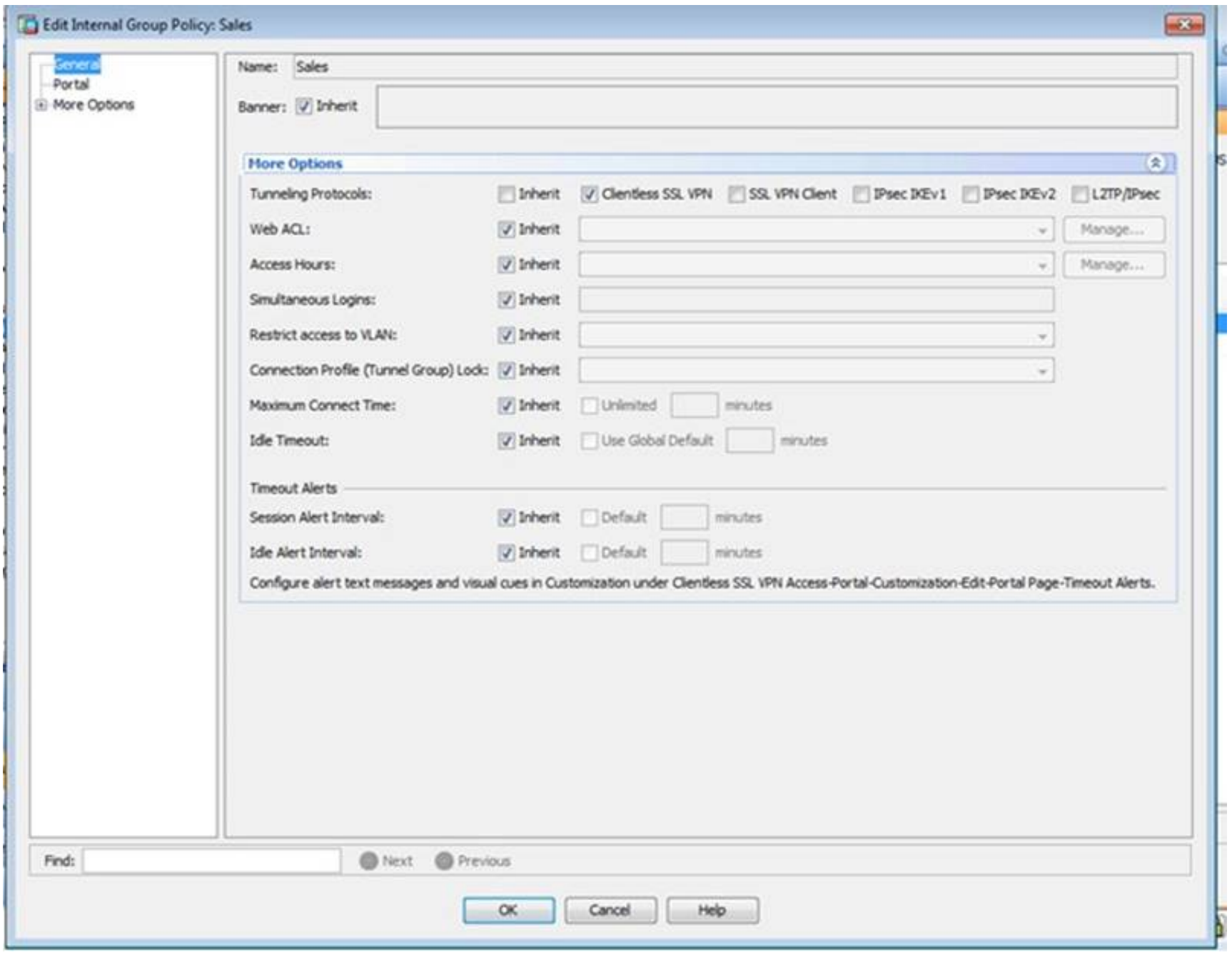

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection 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

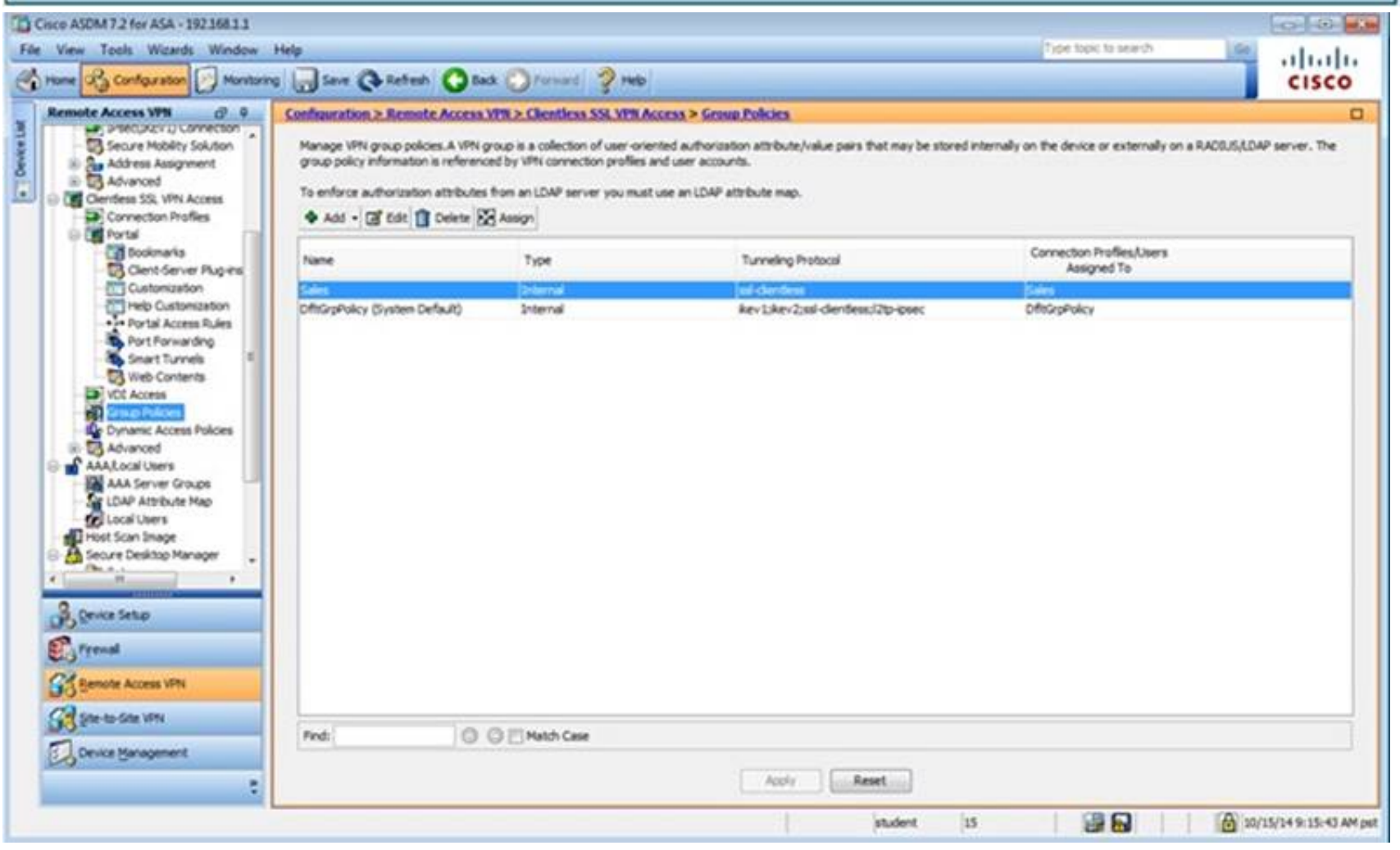

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

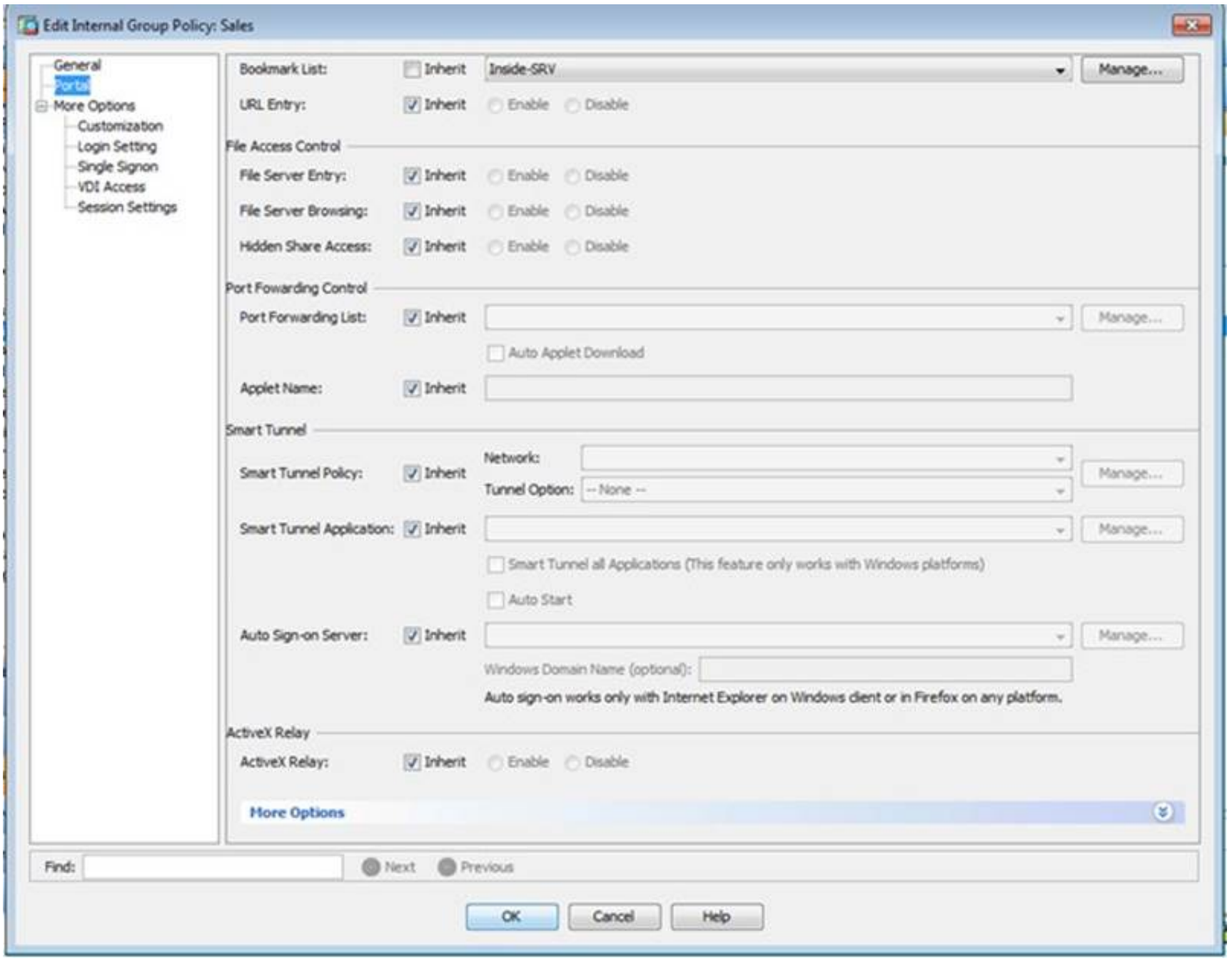

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection 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

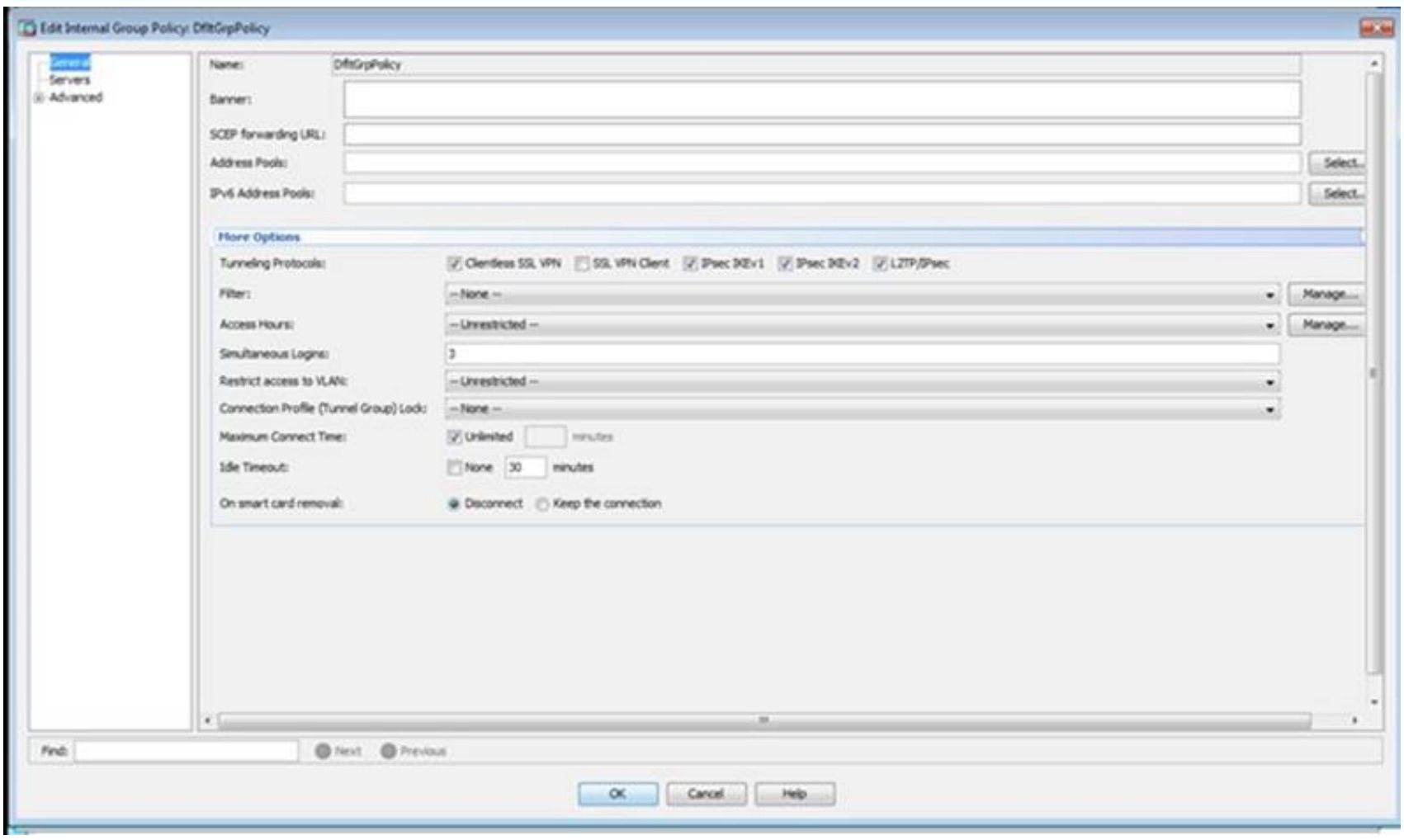

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Configure Port Forwarding Lists that the security appliance 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

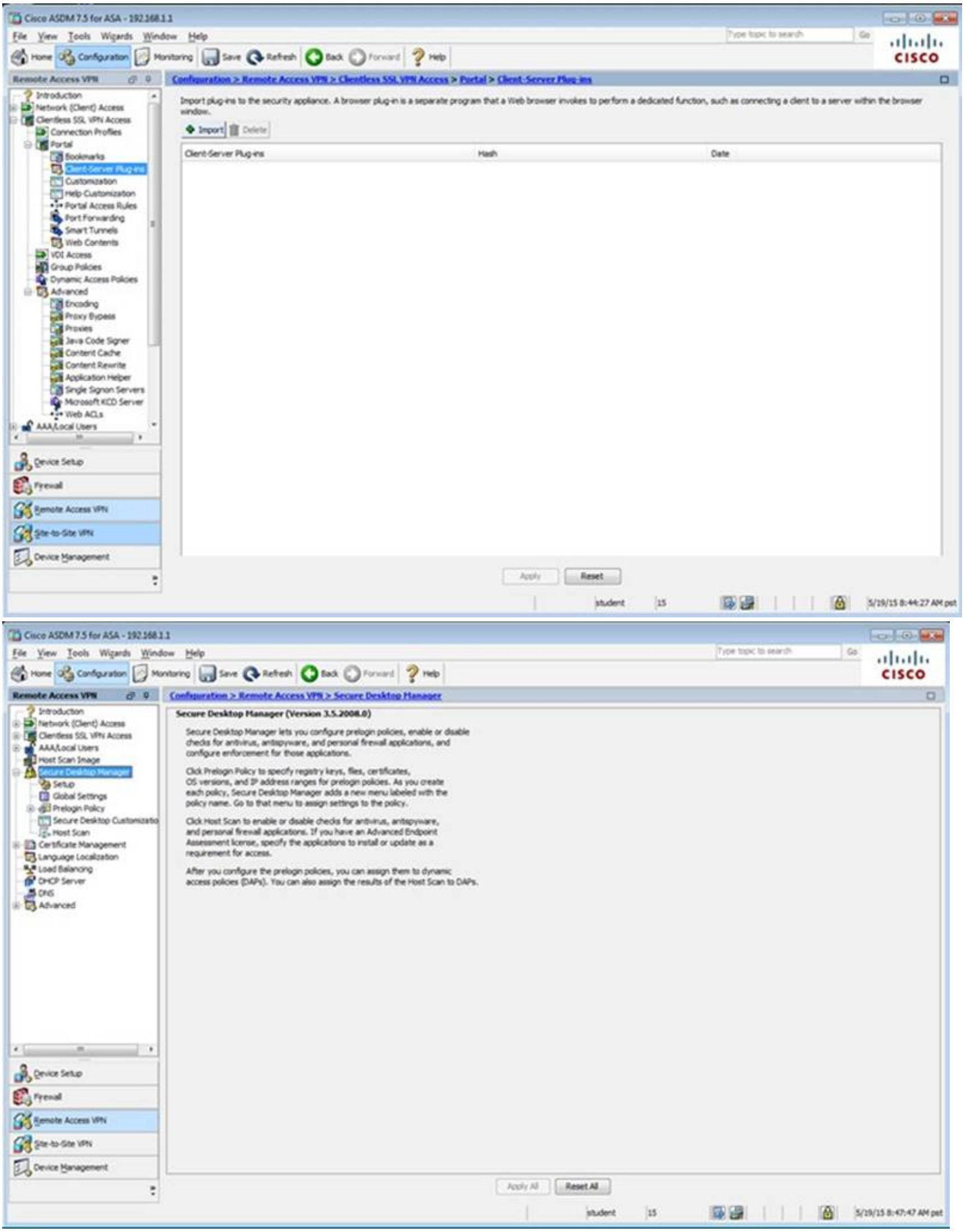
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented 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

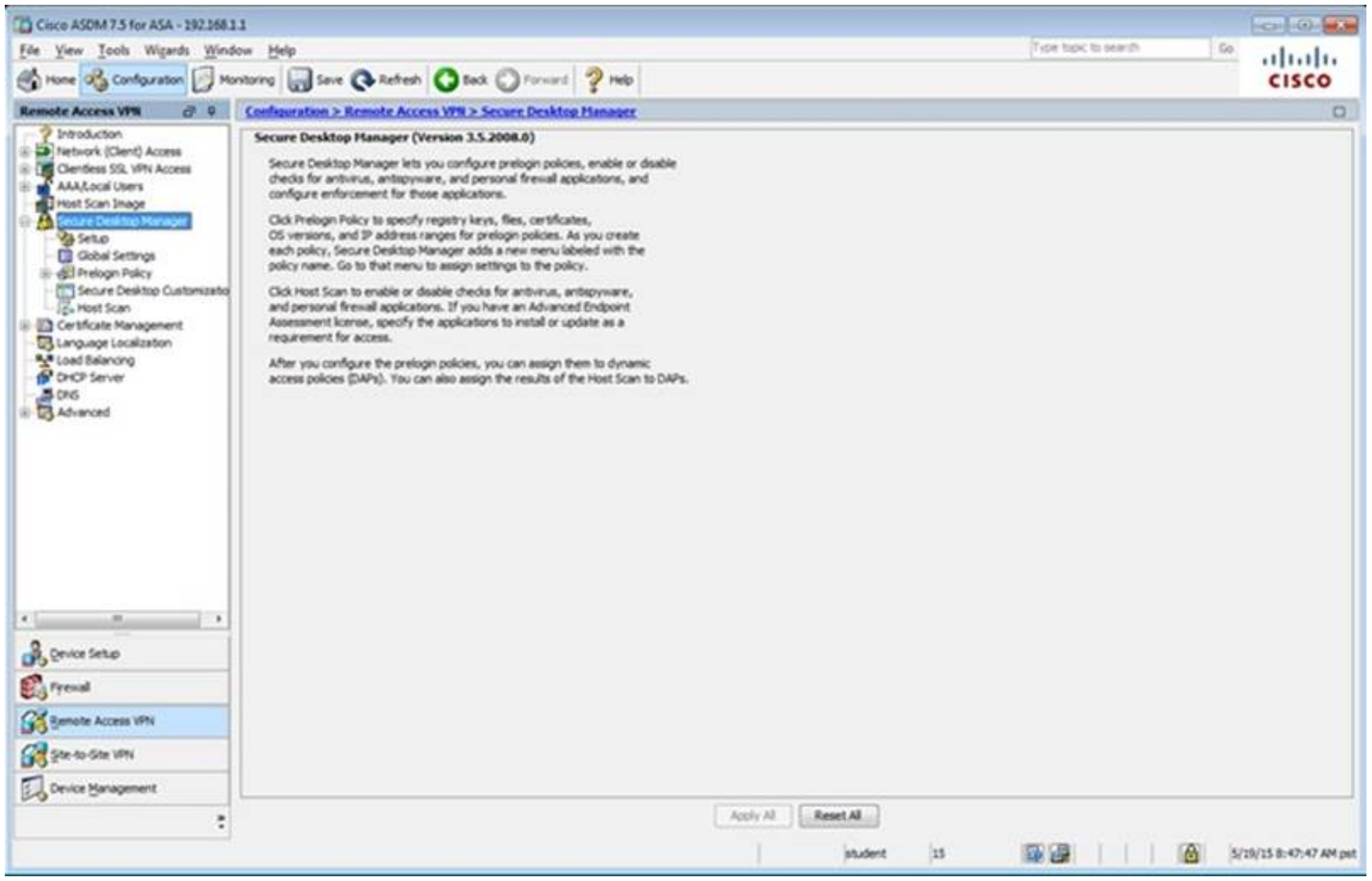

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
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

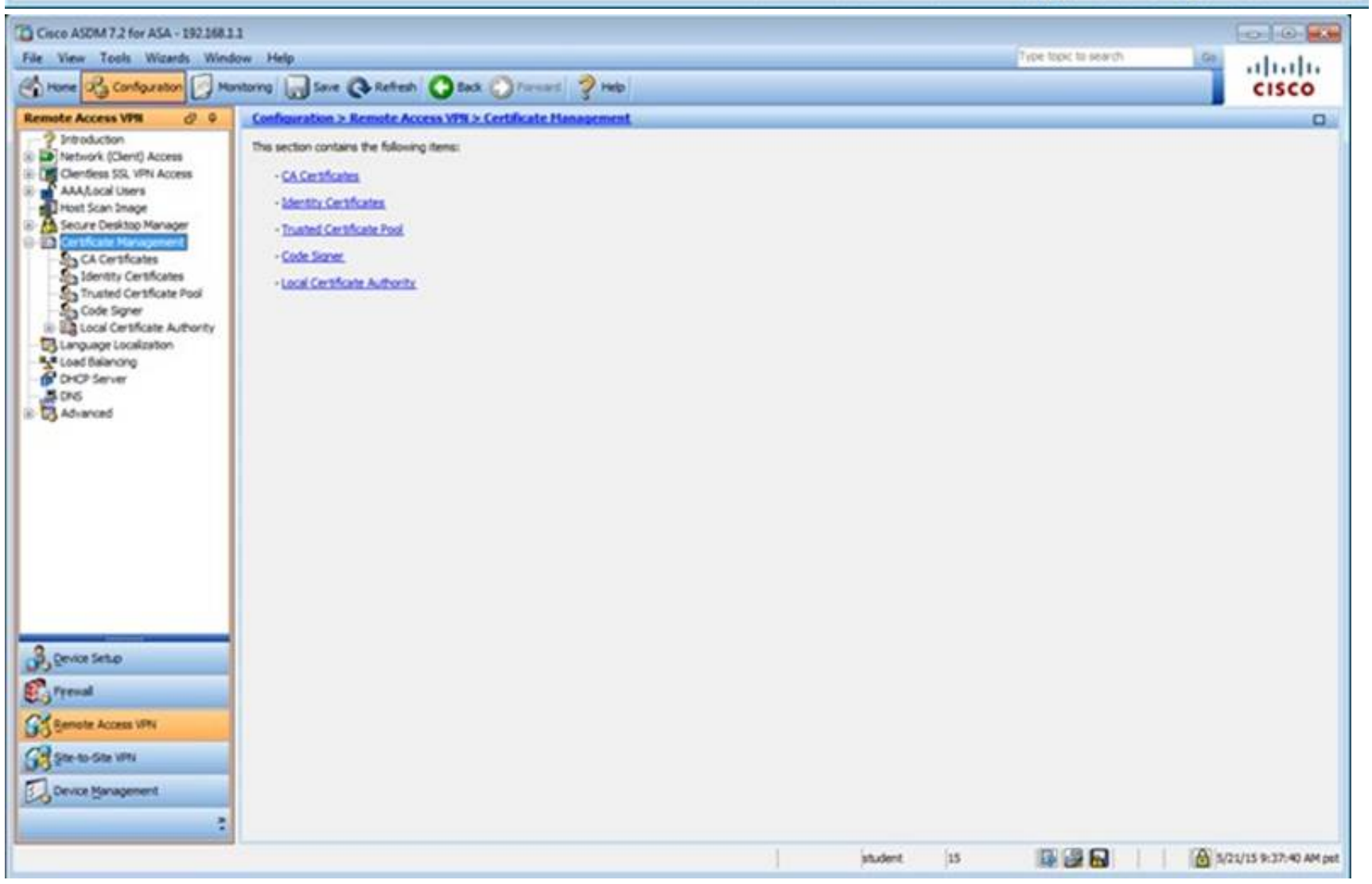

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding 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

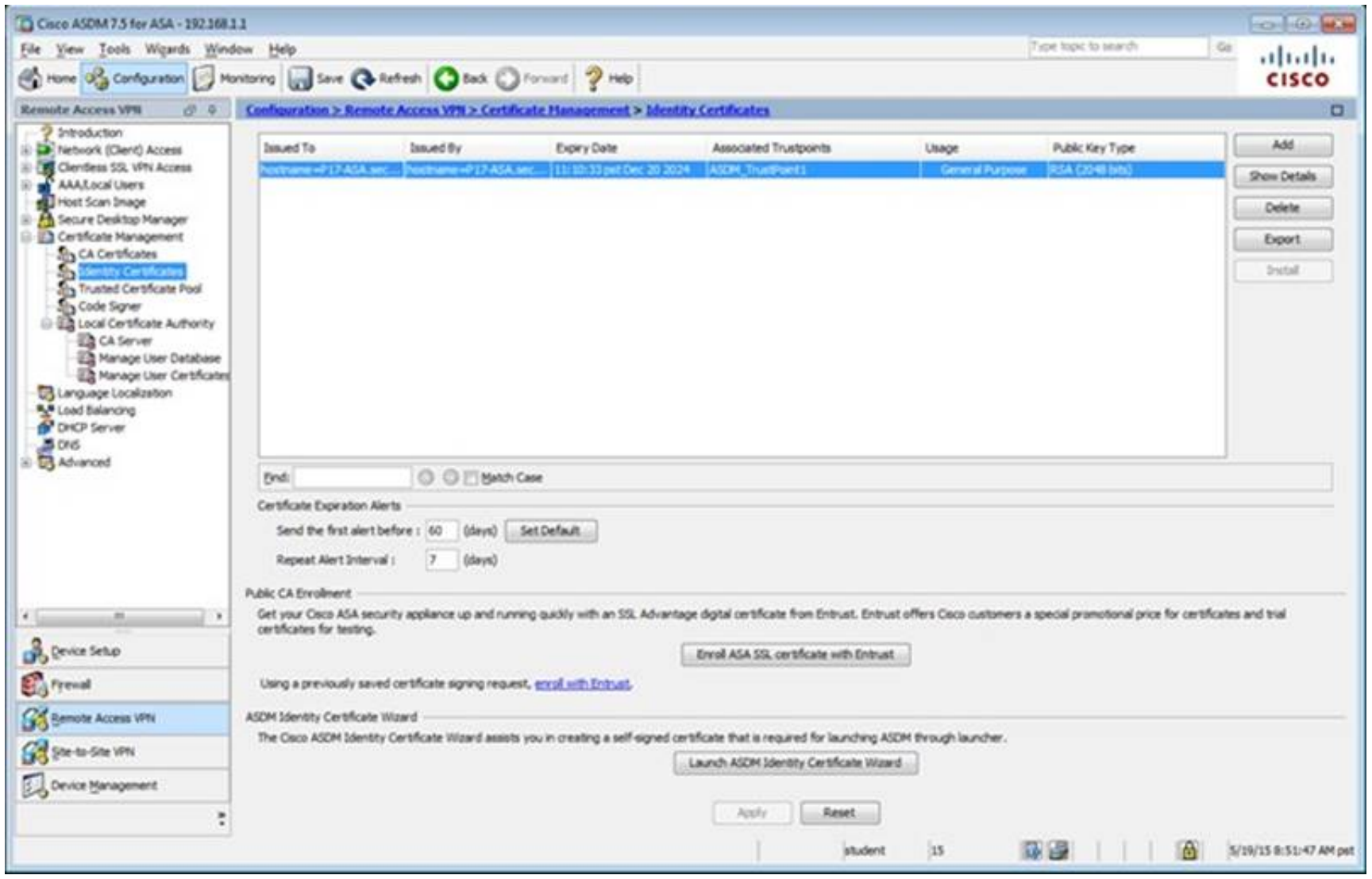

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
Select...
IPv6 Address Pools:
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- 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

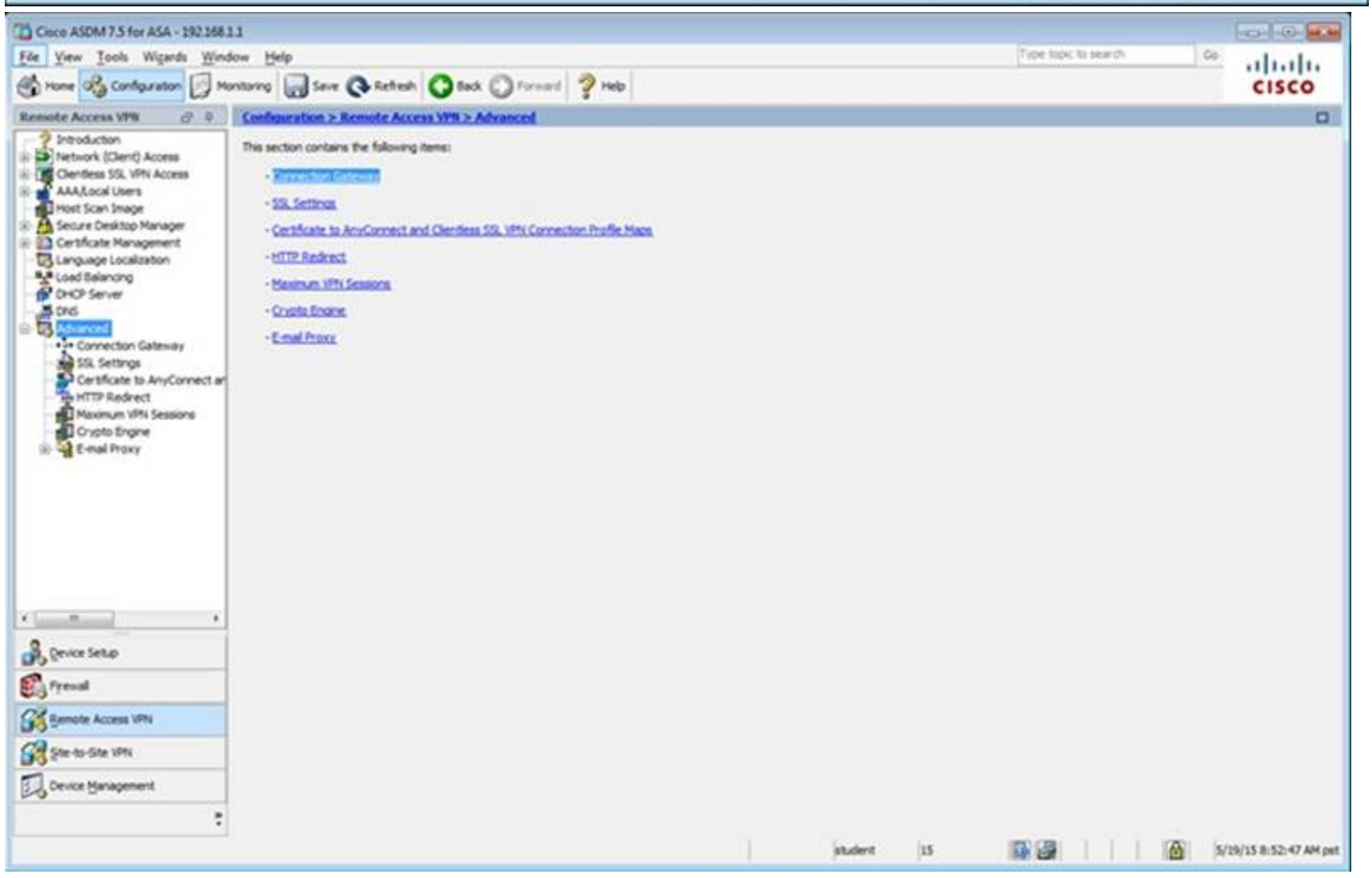

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless 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

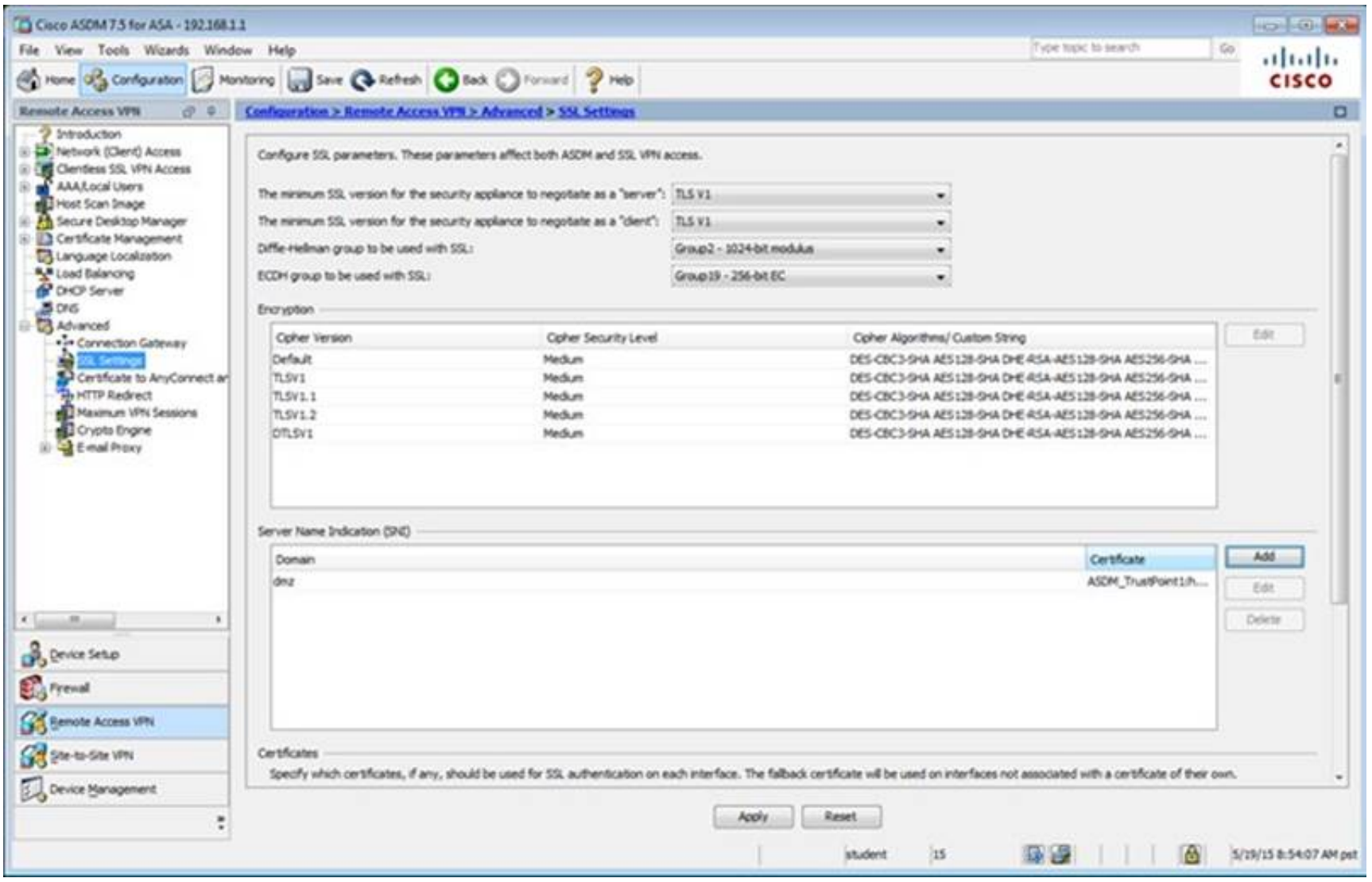
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

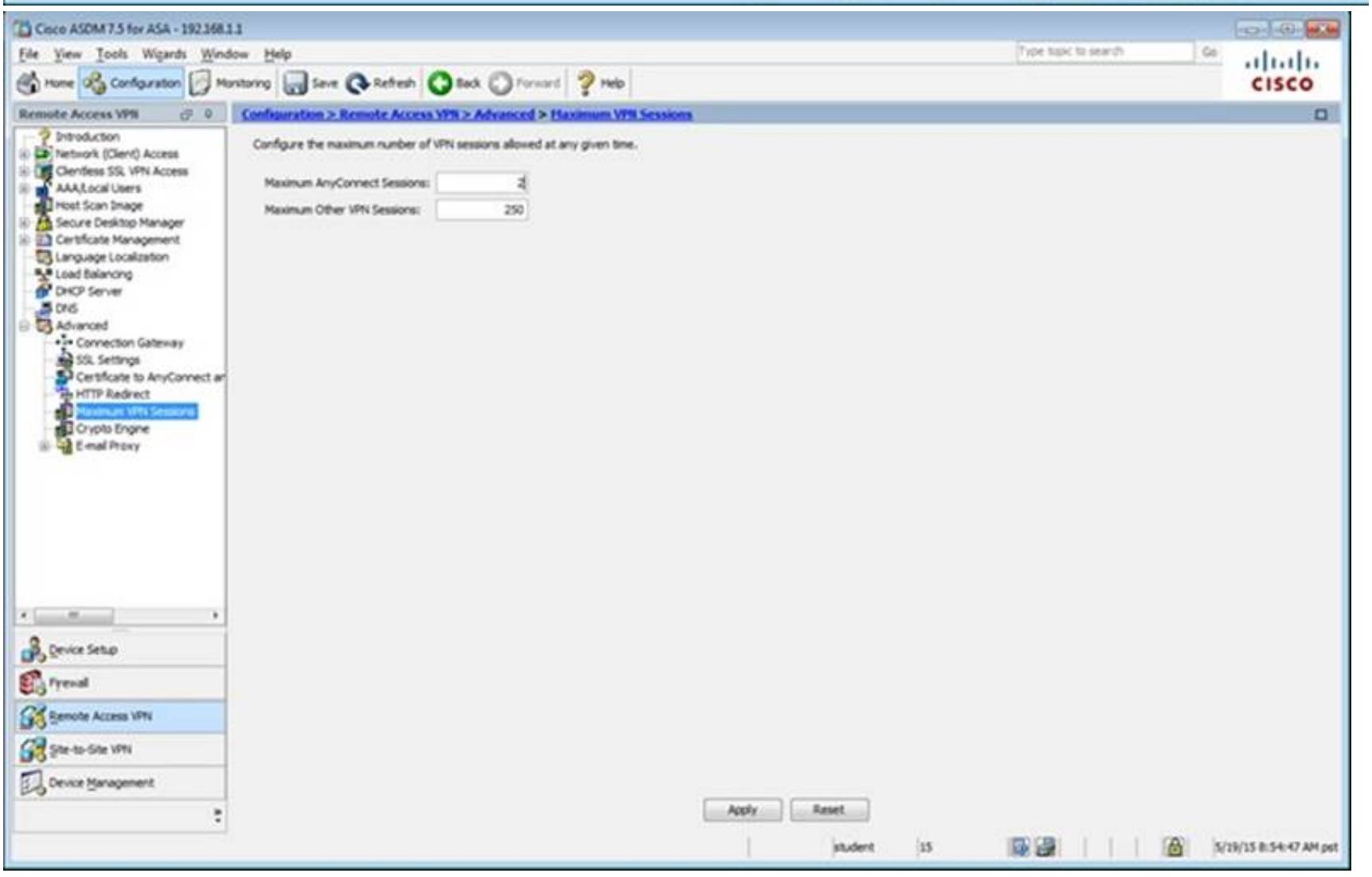

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Secure Desktop Manager (Version 3.5.2008.0)
Secure Desktop Manager lets you configure 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.
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
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

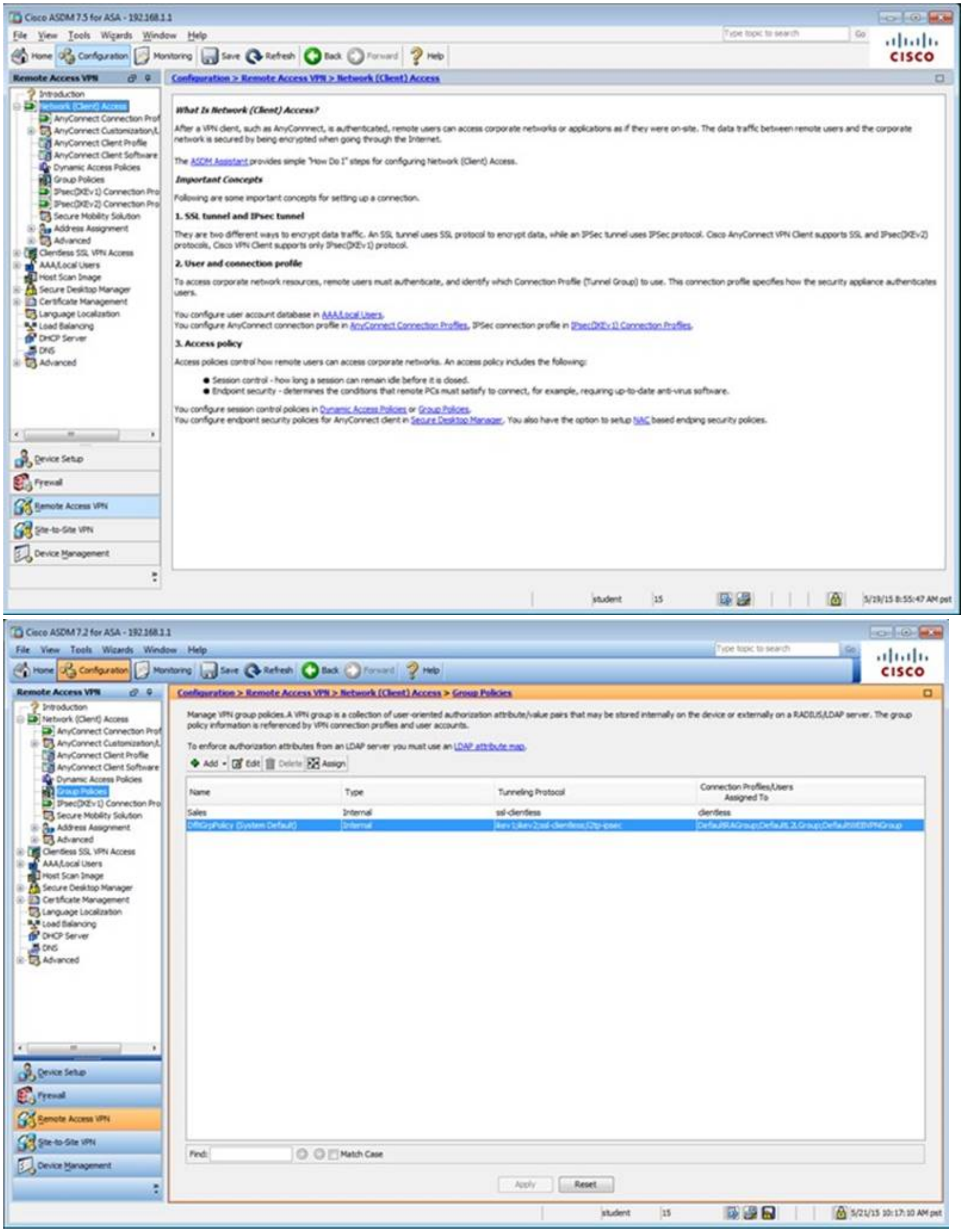

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
This section contains the following items:
- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority
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
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

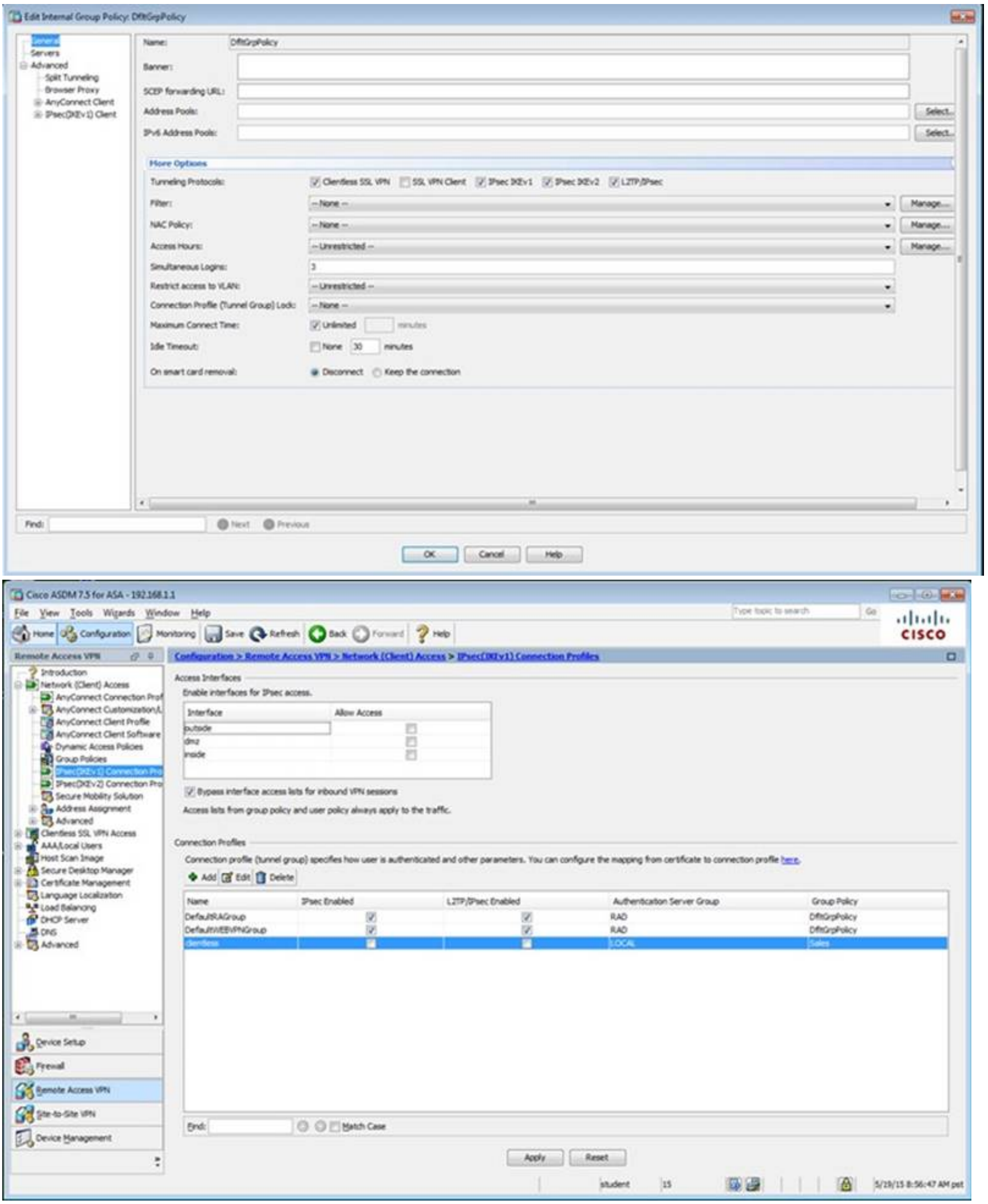

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- Connection Gateway
- SSL Settings
- Certificate to AnyConnect 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

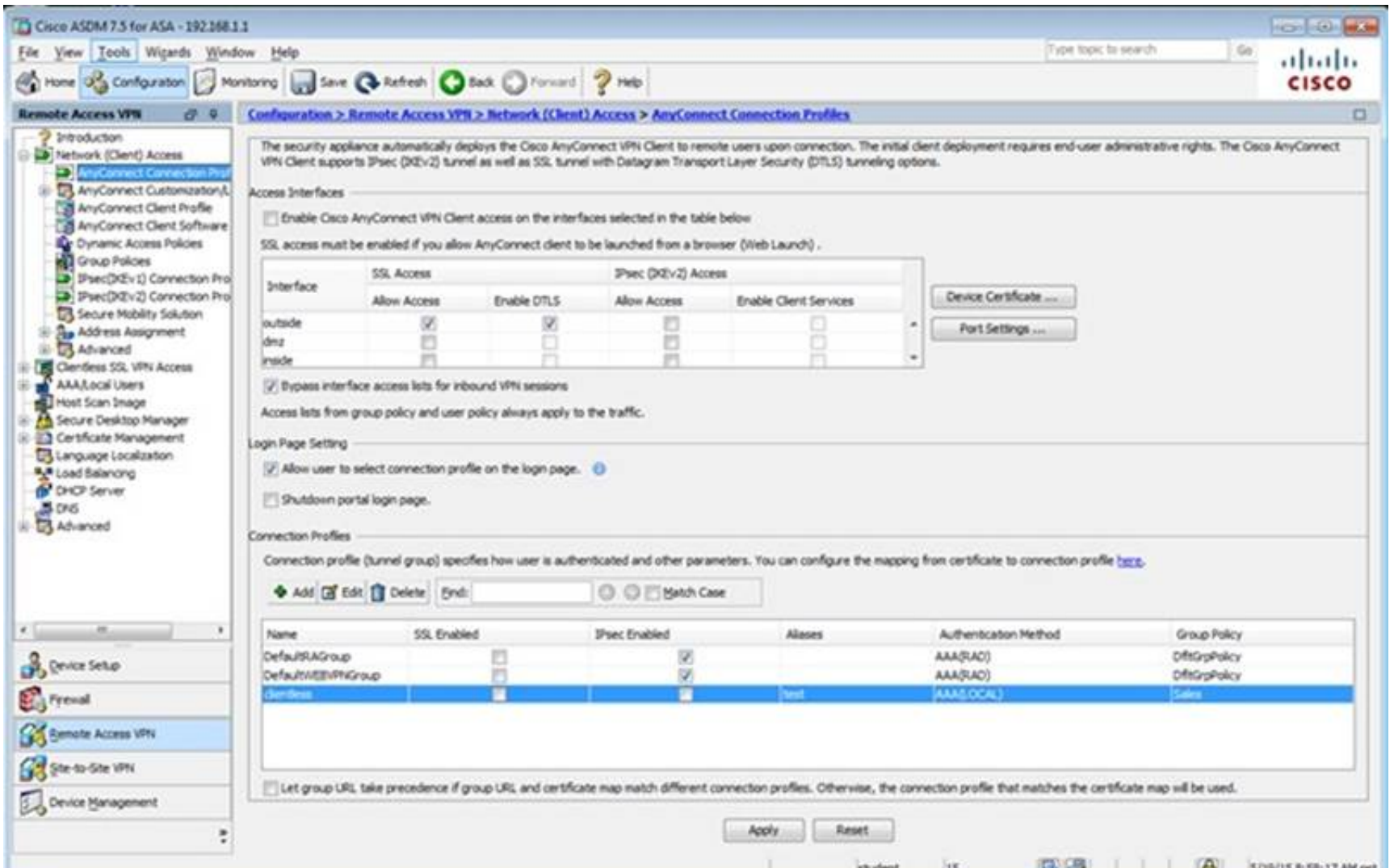

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

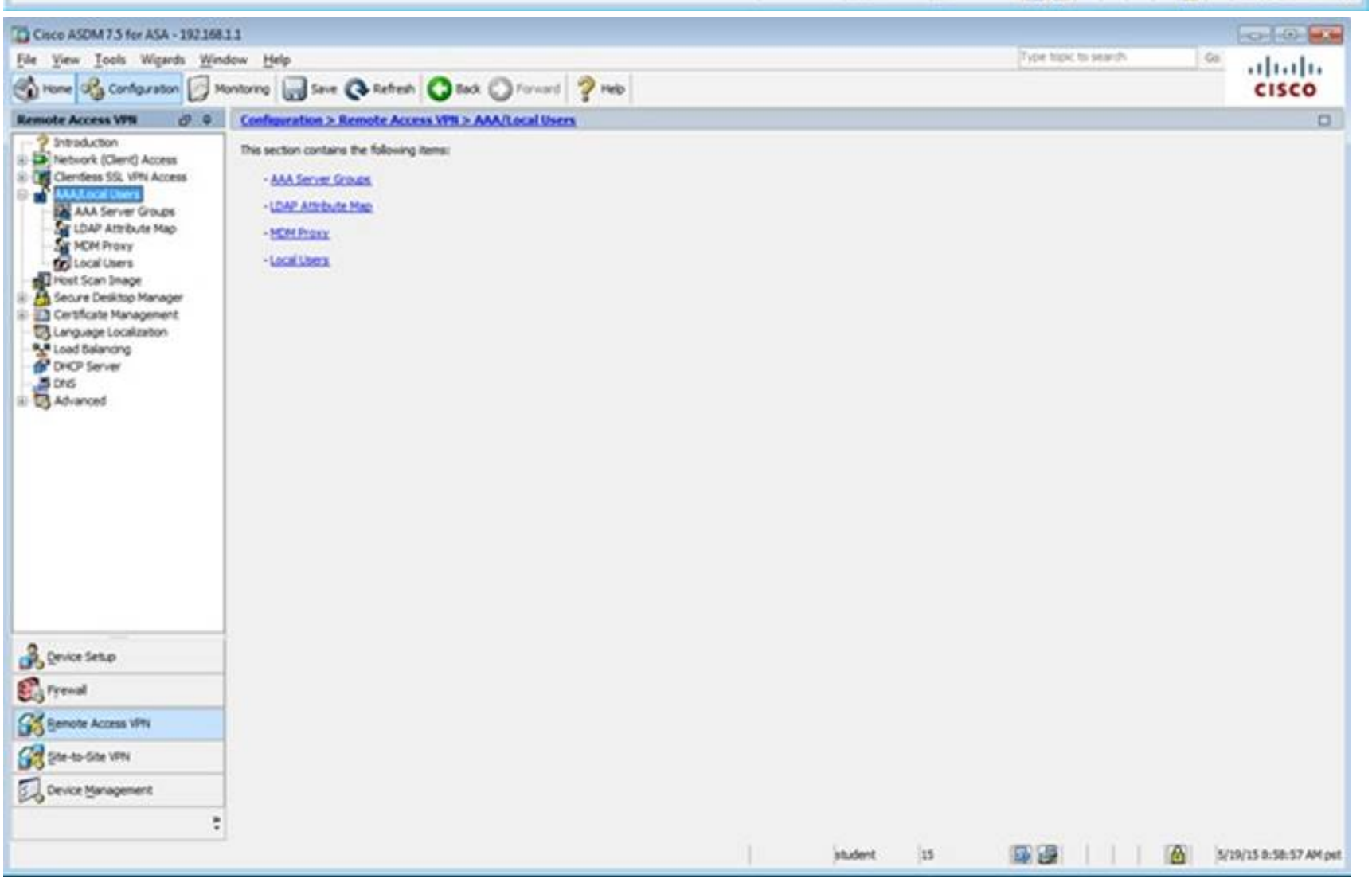

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset
student
15
5/19/15 8:54:47 AM pst

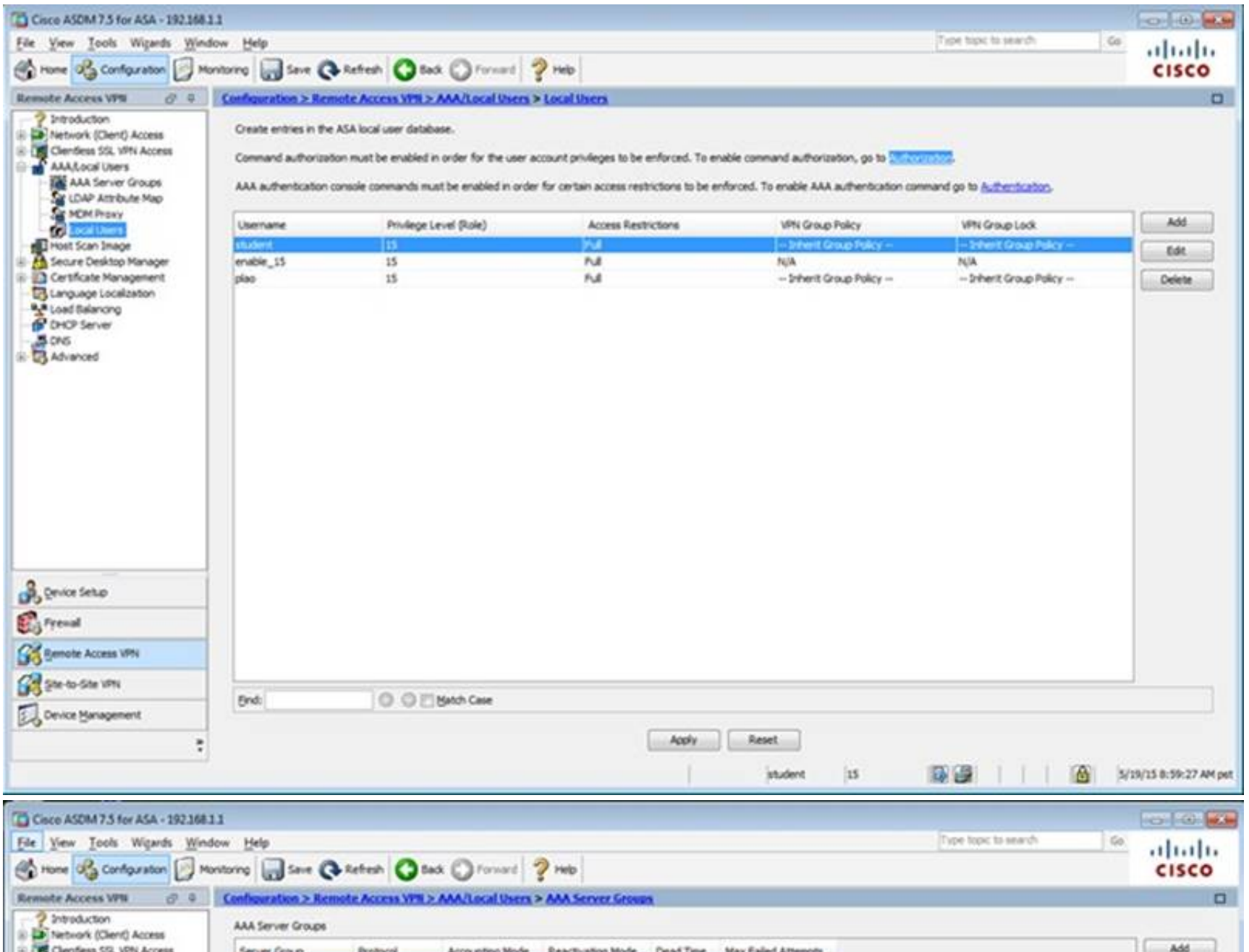

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, 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

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
Sales
Internal
ssl-clientless
clientless
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
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



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 17
Which EAP method uses Protected Access Credentials?

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

Answer: A

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

NEW QUESTION 21
Which two statements about stateless firewalls are true? (Choose two.)

A. They compare the 5-tuple of each incoming packet against configurable rules.
B. They cannot track connections.
C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
D. Cisco IOS cannot implement them because the platform is stateful by nature.
E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Answer: AB

Explanation: In stateless inspection, the firewall inspects a packet to determine the 5-tuple--source and destination IP addresses and ports, and protocol--information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.
Source:
http://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/19-0/XMART/PSF/19-PSF-Admin/19-PSF- Admin_chapter_01.html

NEW QUESTION 23
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 27
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 32
Refer to the exhibit.

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

What is the effect of the given command sequence?

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

Answer: A

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

NEW QUESTION 37
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 40
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 44
A specific URL has been identified as containing malware. What action can you take to block users from accidentally visiting the URL and becoming infected with malware.

A. Enable URL filtering on the perimeter router and add the URLs you want to block to the router's local URL list.
B. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the router's local URL list.
C. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewall's local URL list.
D. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
E. Create a whitelist that contains the URLs you want to allow and activate the whitelist on the perimeter router.

Answer: A

Explanation: URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in an URL list. You can maintain a local URL list on the router. If the Cisco IOS image on the router supports URL filtering but does not support Zone-based Policy Firewall (ZPF), you can maintain one local URL list on the router to add or edit an URLs. Enter a full domain name or a partial domain name and choose whether to Permit or Deny requests for this URL.
Source:
http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/ software/user/guide/URLftr.html#wp999509

NEW QUESTION 48
When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?

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

Answer: A

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

NEW QUESTION 51
Refer to the exhibit.

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

What is the effect of the given command sequence?

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

Answer: A

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

NEW QUESTION 55
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 57
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

A. The secure boot-image command is configured.
B. The secure boot-comfit command is configured.
C. The confreg 0x24 command is configured.
D. The reload command was issued from ROMMON.

Answer: A

Explanation: autocommand: (Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
So after successfully logs in the Admin user sees the running configuration and immediately after is disconnected by the router. So removing the command lets keeps him connected.
Source:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe- 3se-3850-cr-book_chapter_0110.html

NEW QUESTION 62
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 67
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 68
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 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 74
What is the purpose of the Integrity component of the CIA triad?

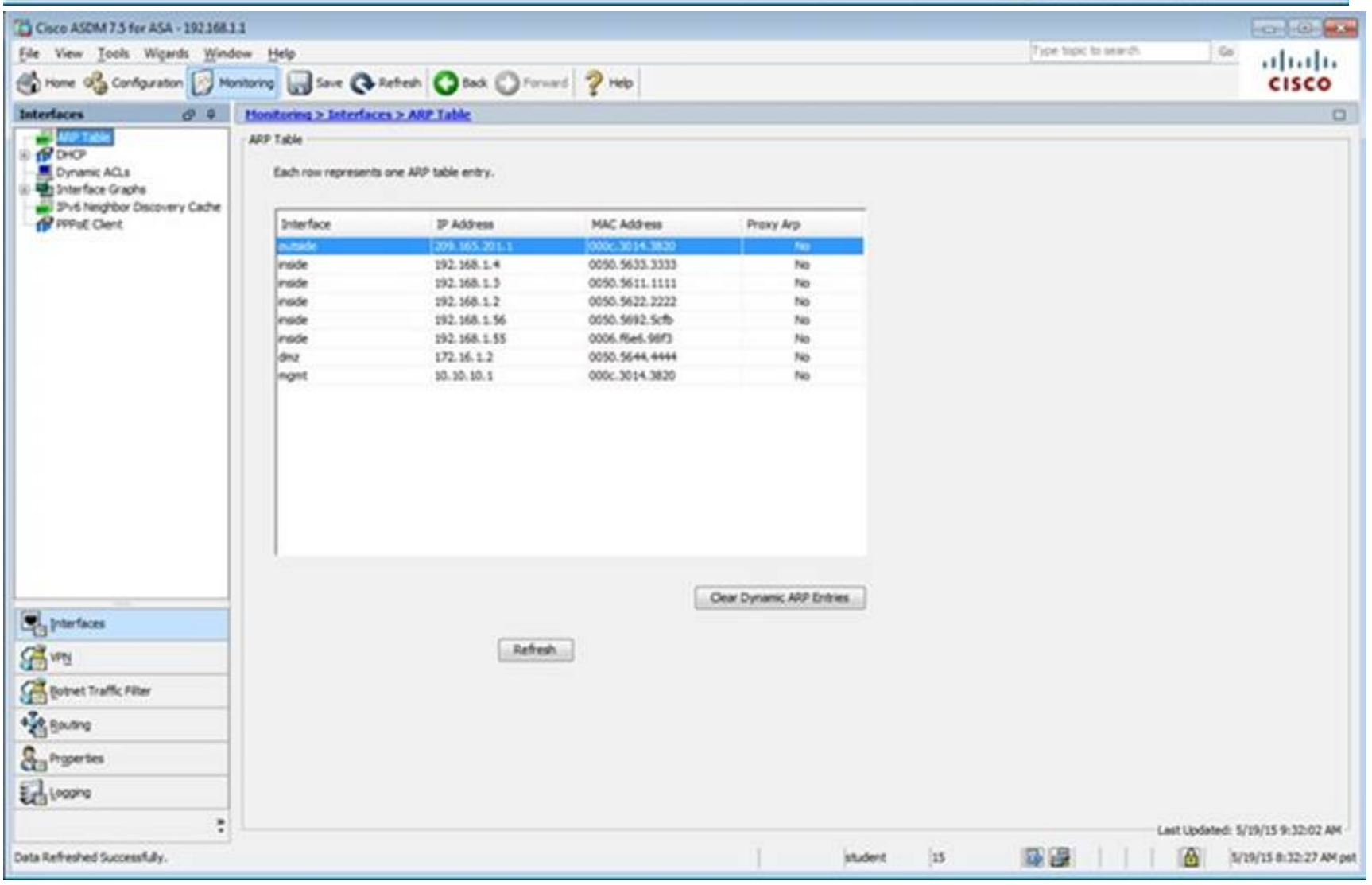
A. to ensure that only authorized parties can modify data
B. to determine whether data is relevant
C. to create a process for accessing data
D. to ensure that only authorized parties can view data

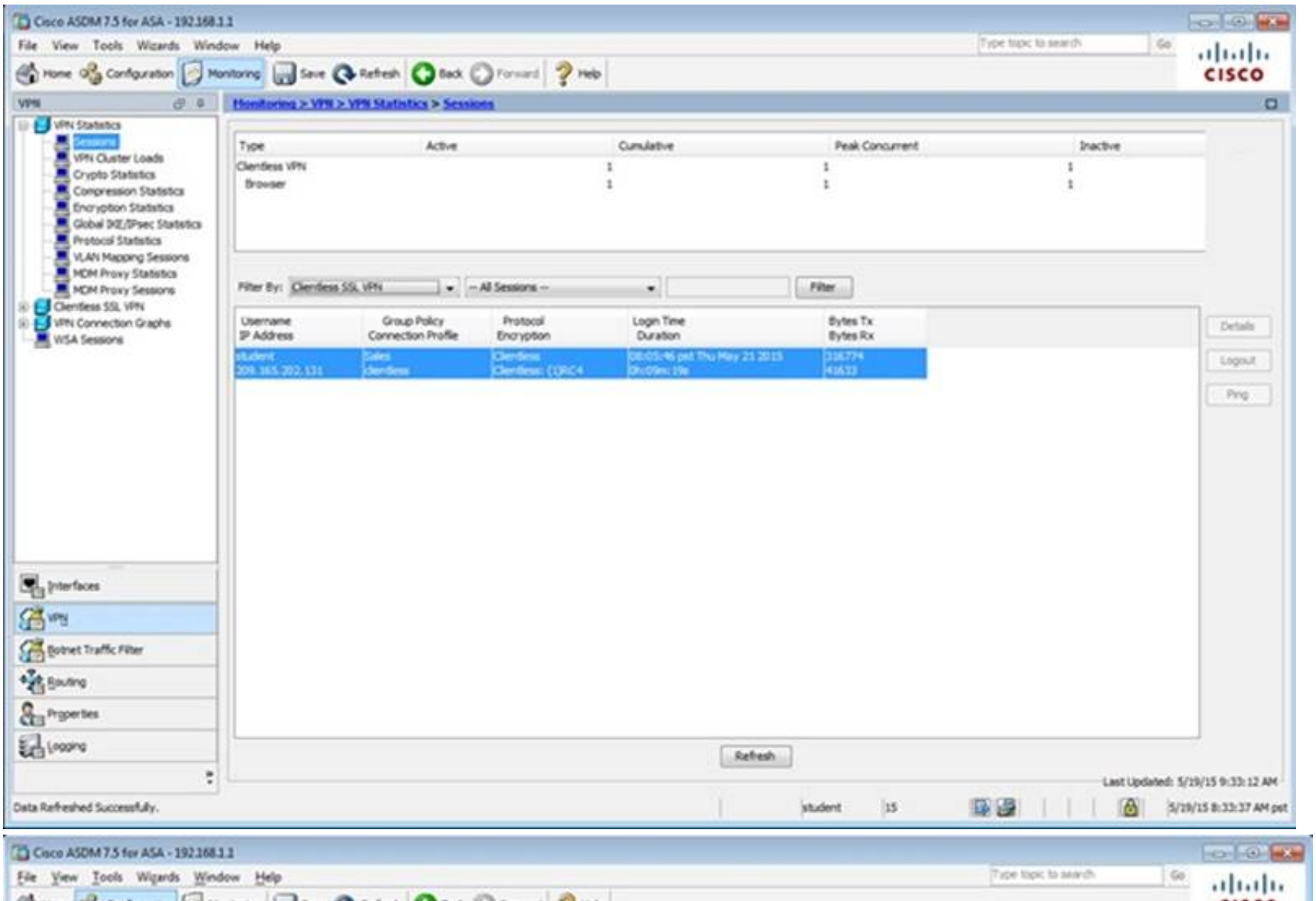
Answer: A

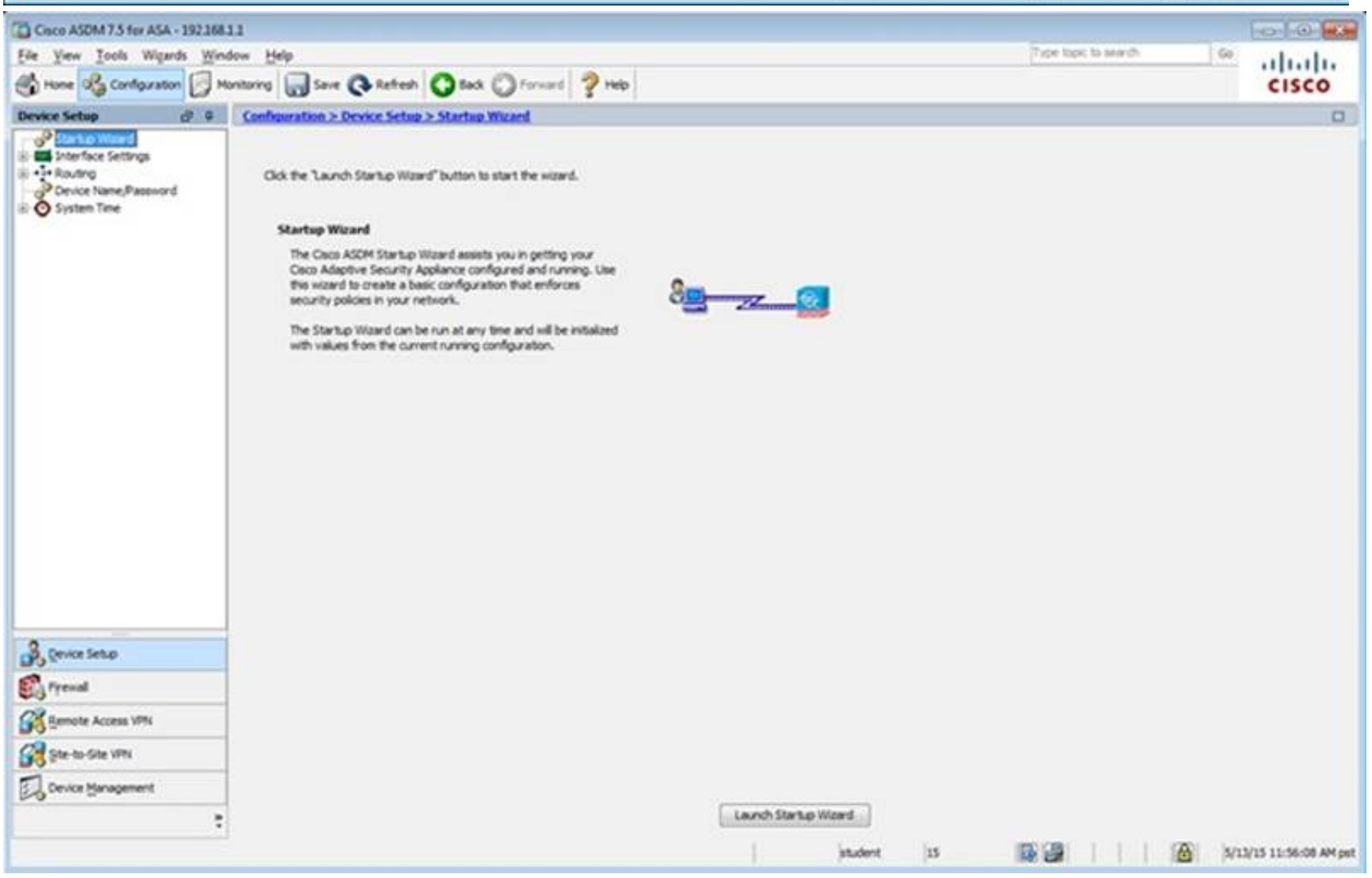
Explanation: Integrity for data means that changes made to data are done only by authorized individuals/systems. Corruption of data is a failure to maintain data integrity.
Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

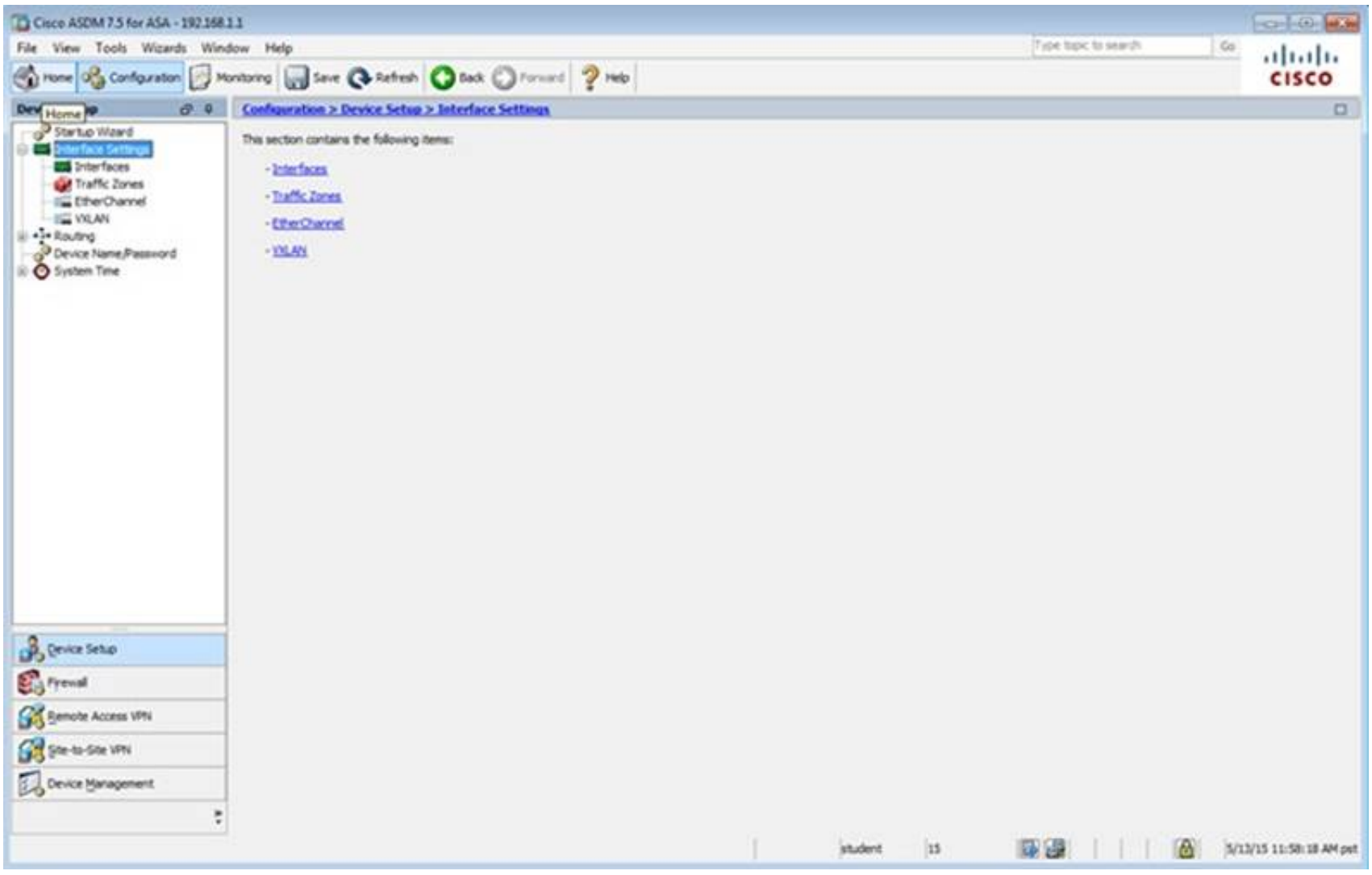
NEW QUESTION 77
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram. Note: Not all ASDM functionalities 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.

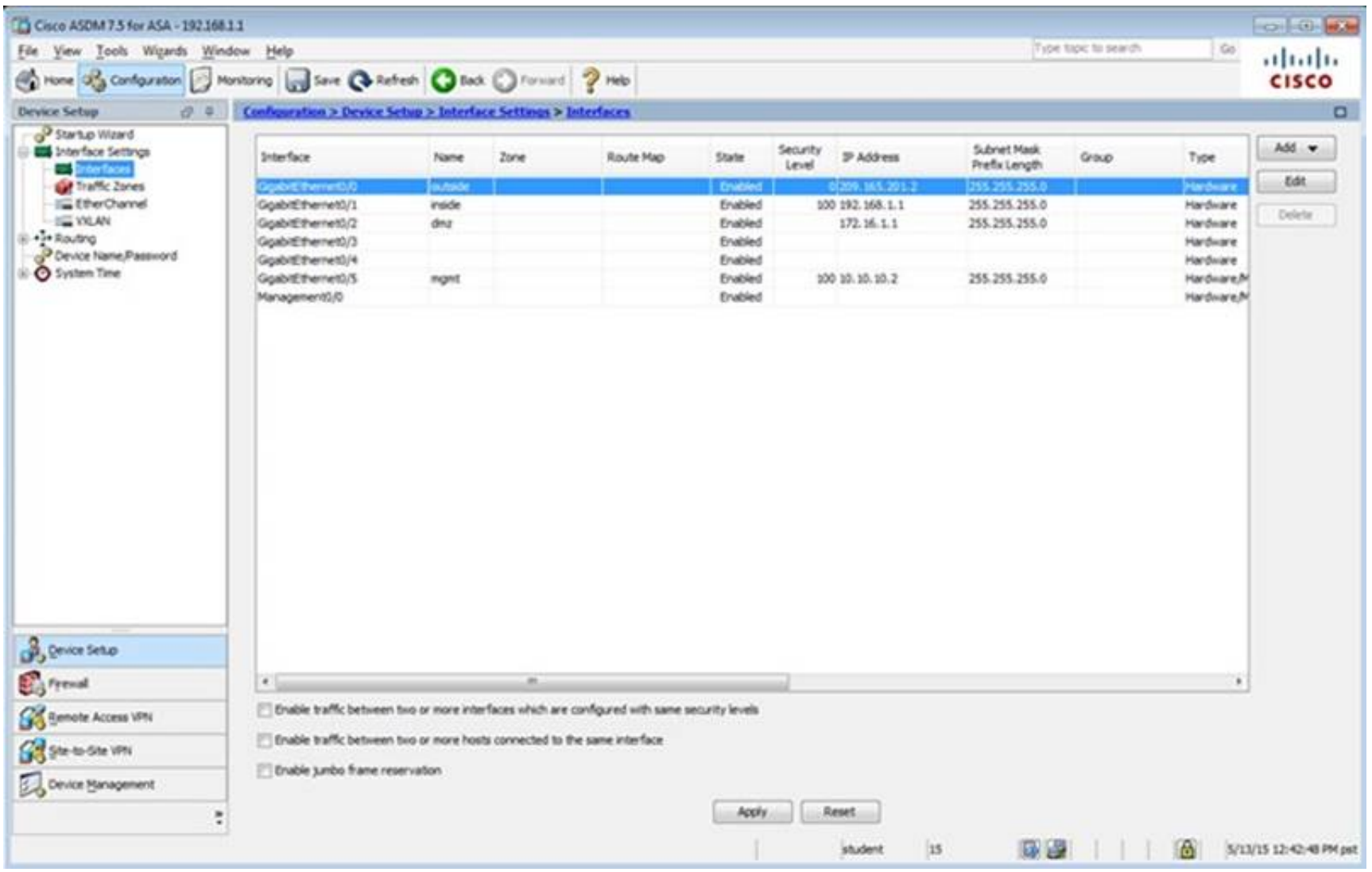

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License
Host Name: P17-ASA.secure-x.local
ASA Version: 100.14(6)13
ASDM 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

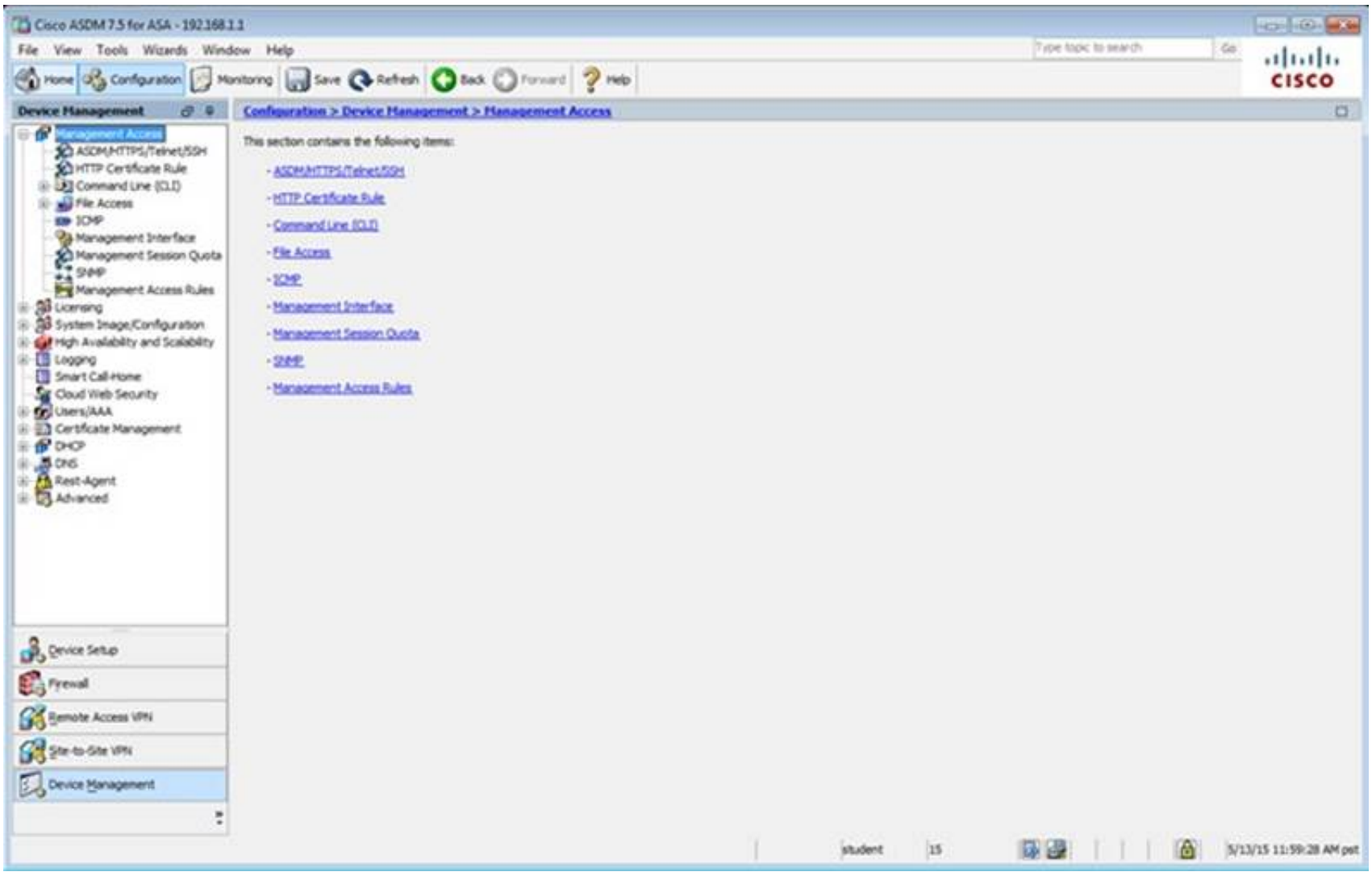

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Interfaces
ARP Table
DHCP
Dynamic ACLs
Interface Graphs
IPv6 Neighbor Discovery Cache
PPPoE Client
Monitoring > Interfaces > ARP Table
ARP Table
Each row represents 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

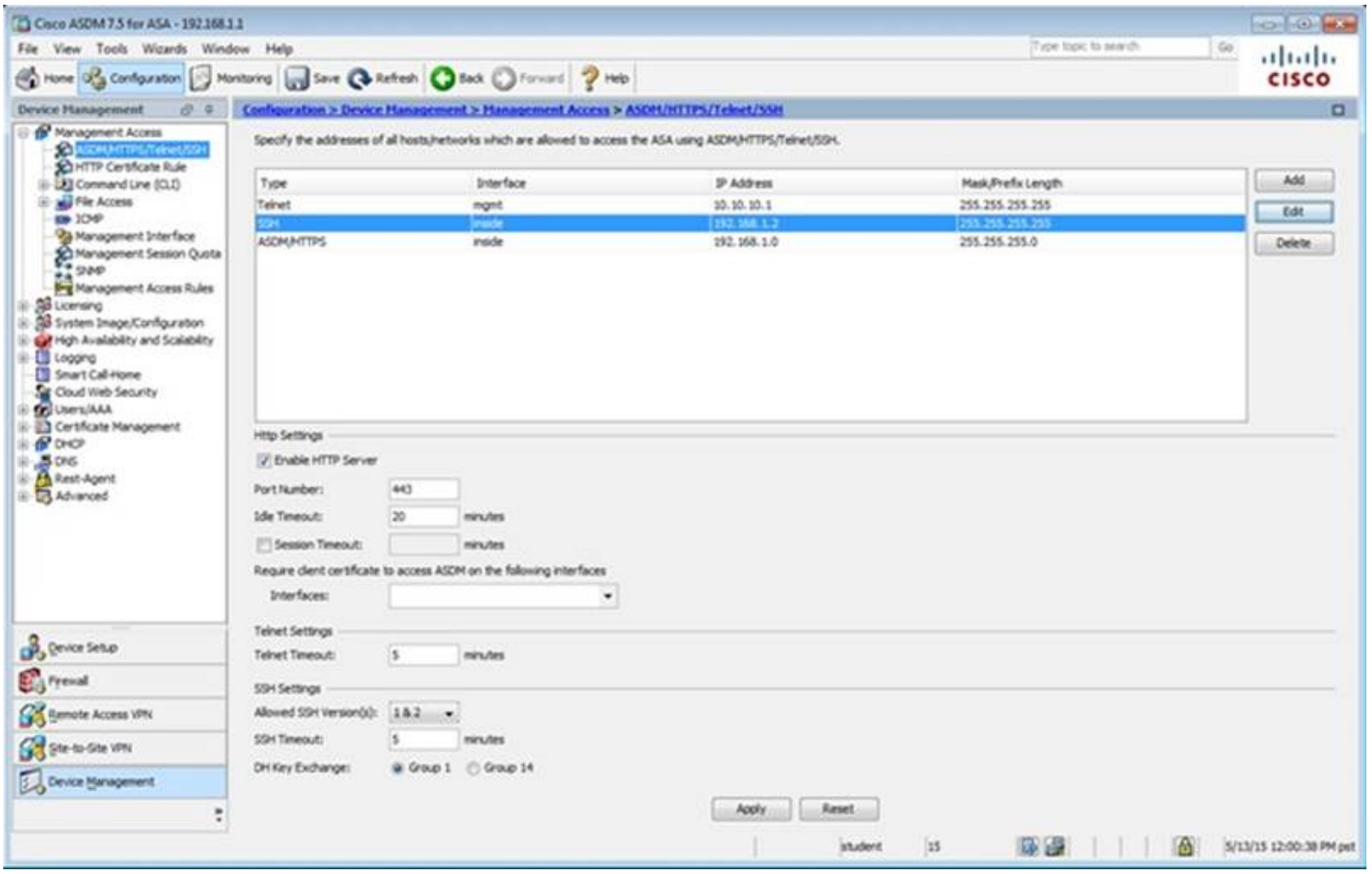

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
VPN
VPN Statistics
Sessions
VPN Cluster Loads
Crypto Statistics
Compression Statistics
Encryption Statistics
Global IKE/IPsec Statistics
Protocol Statistics
VLAN 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
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

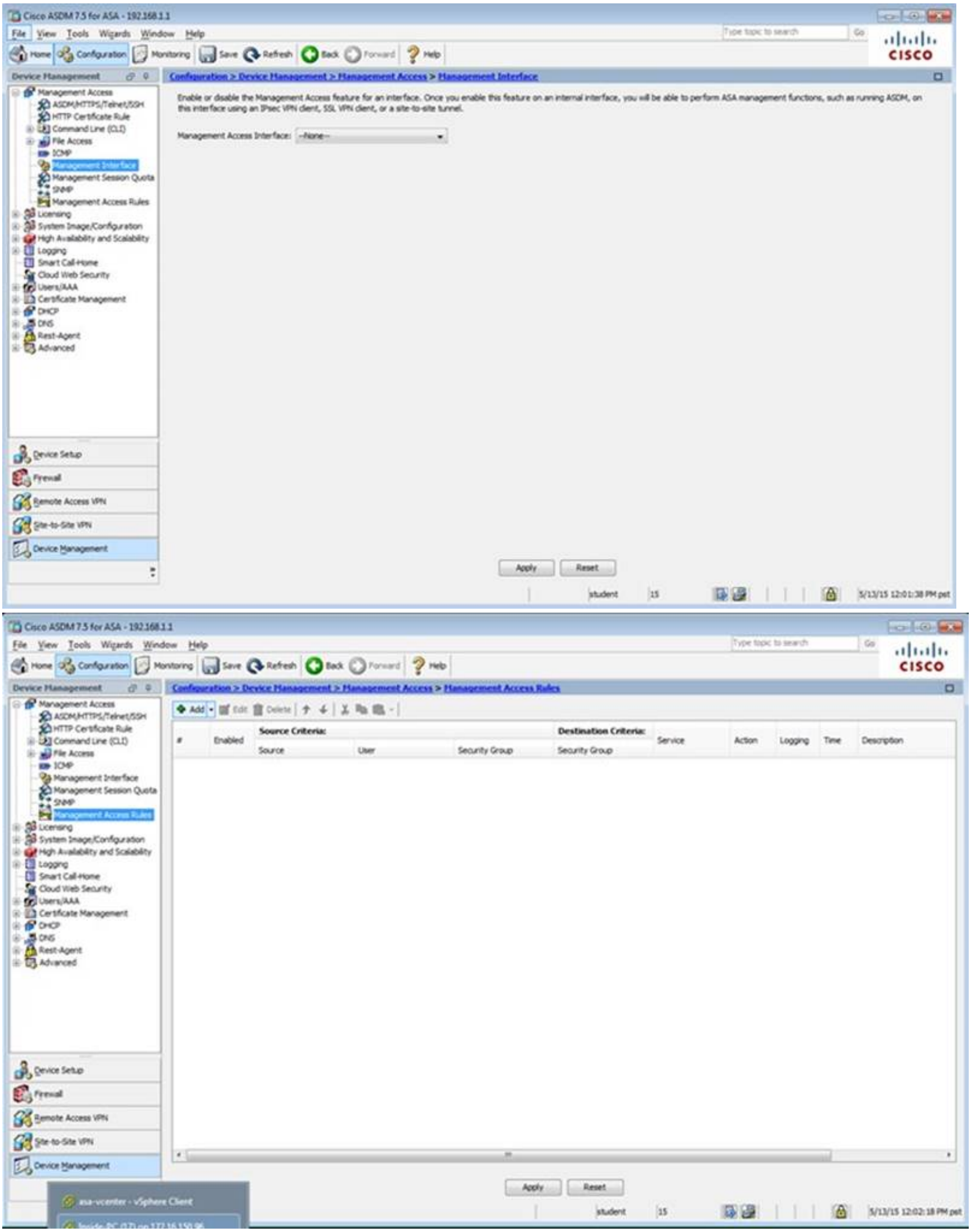

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" 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

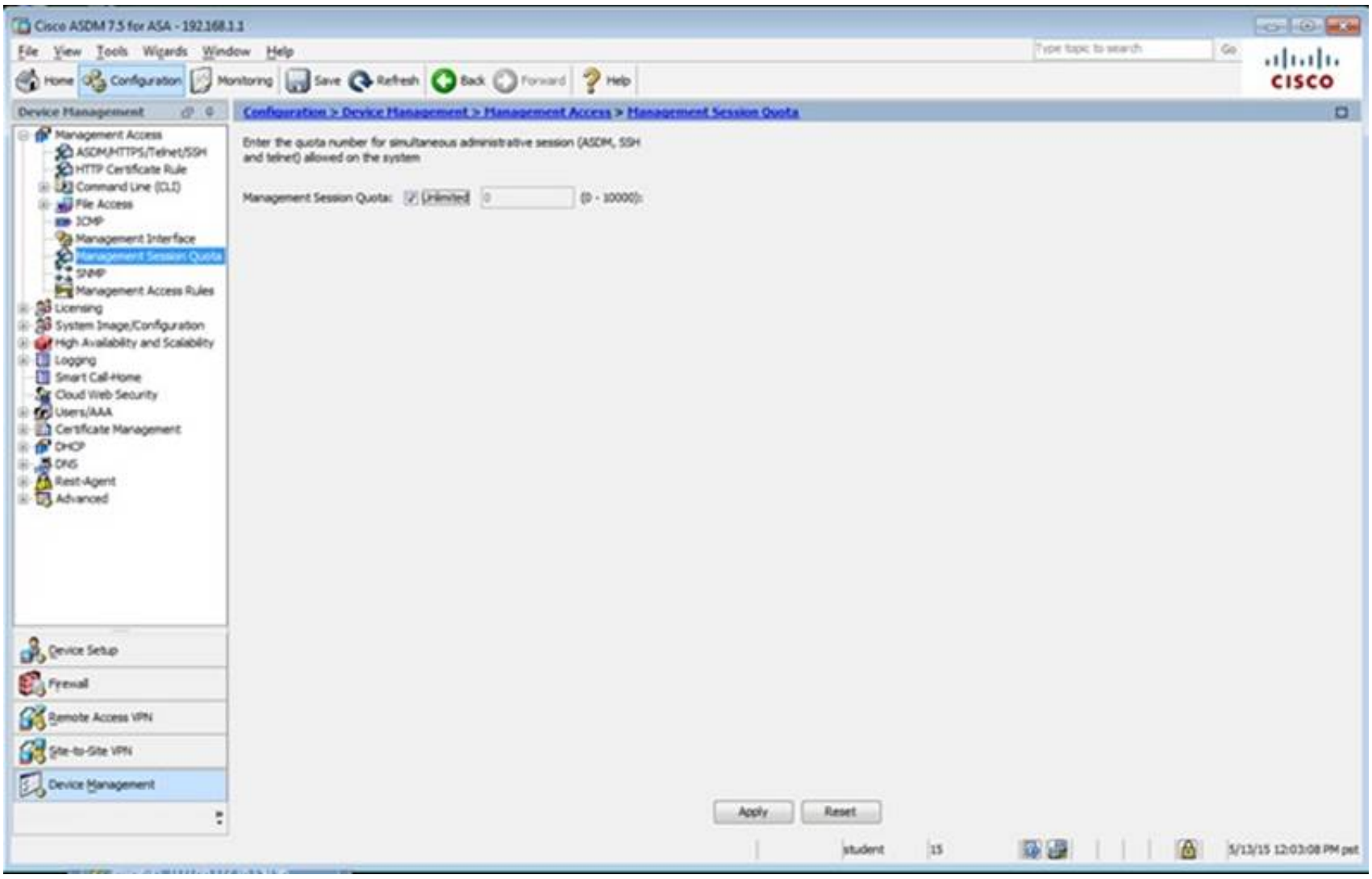

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Device Setup > Interface Settings > Interfaces
Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/13/15 12:42:48 PM pst

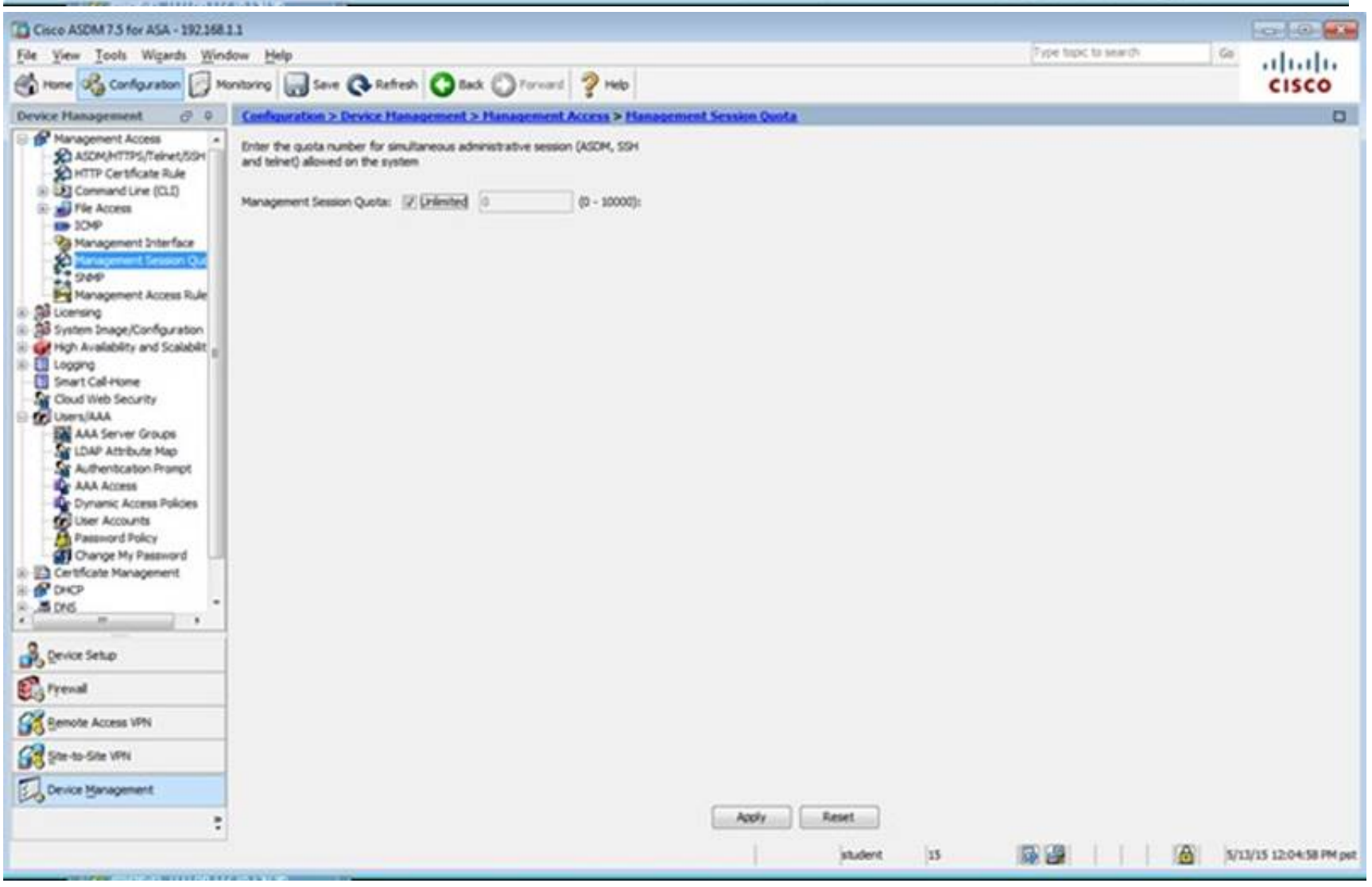

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access
This section contains the following items:
- ASDM/HTTPS/Telnet/SSH
- HTTP Certificate Rule
- 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

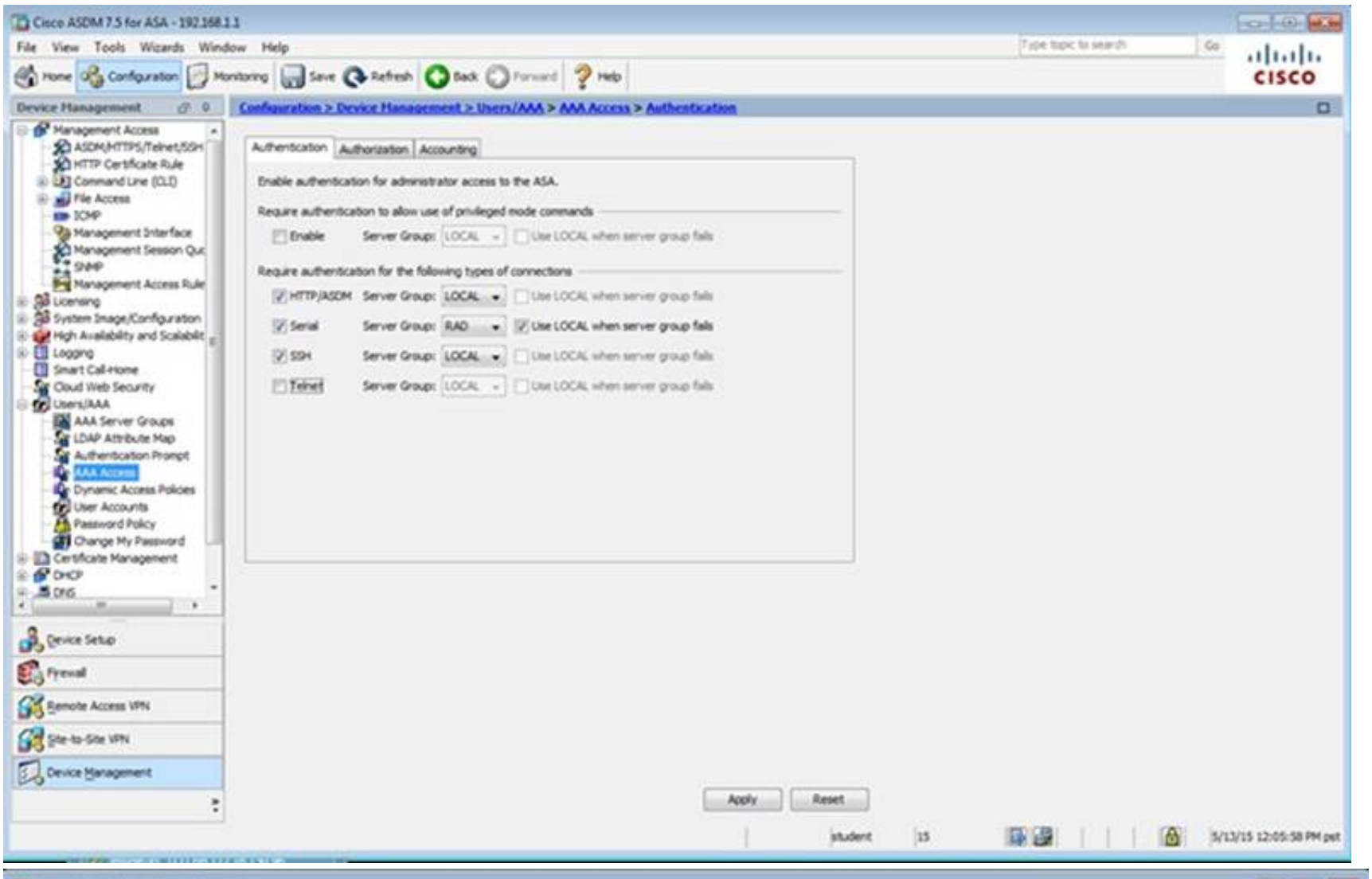

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
Specify the addresses of all hosts/networks which are allowed to 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
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

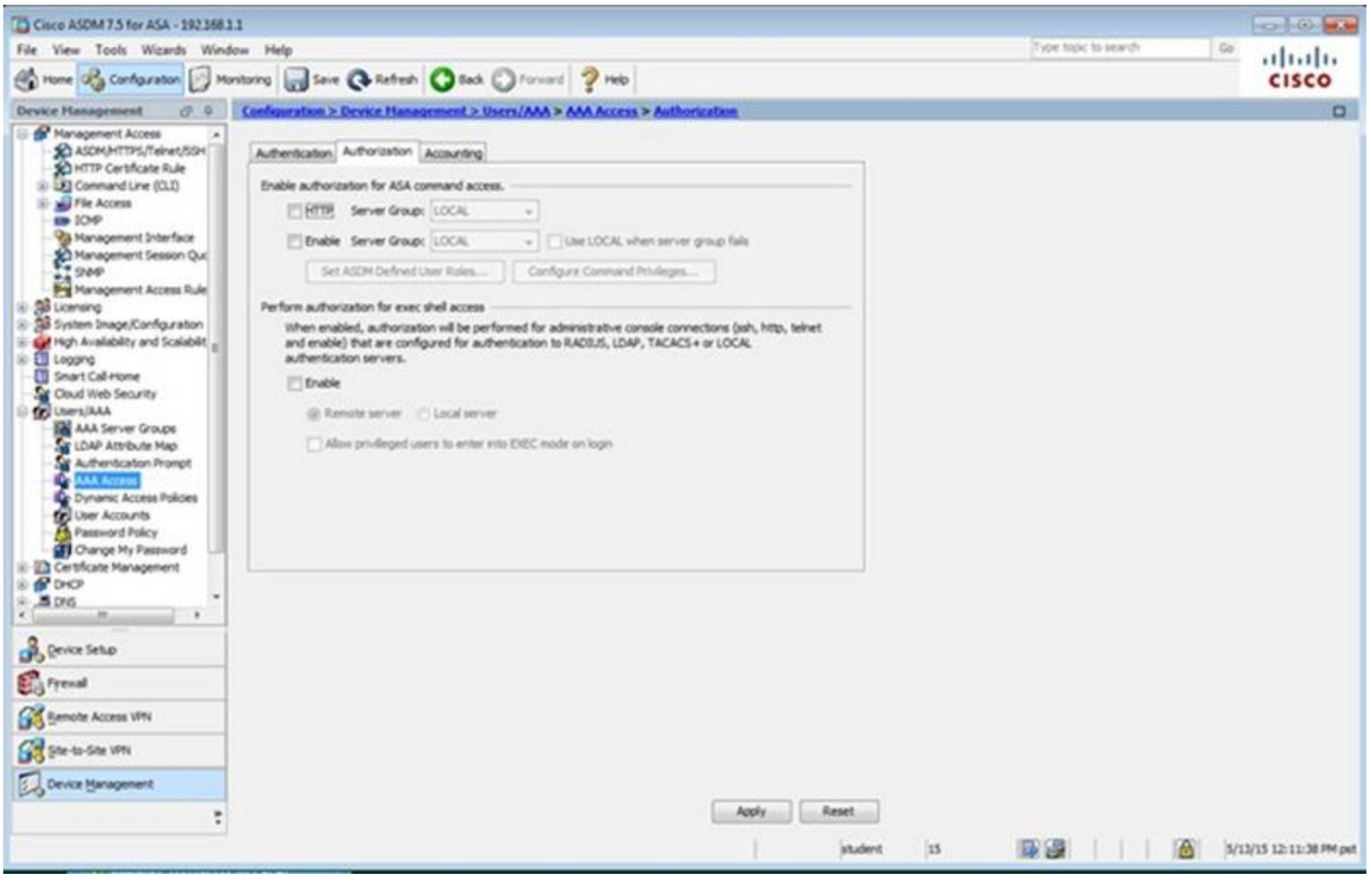

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Interface
Management Access
ASDM/HTTPS/Telnet/SSH
HTTP Certificate Rule
Command 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

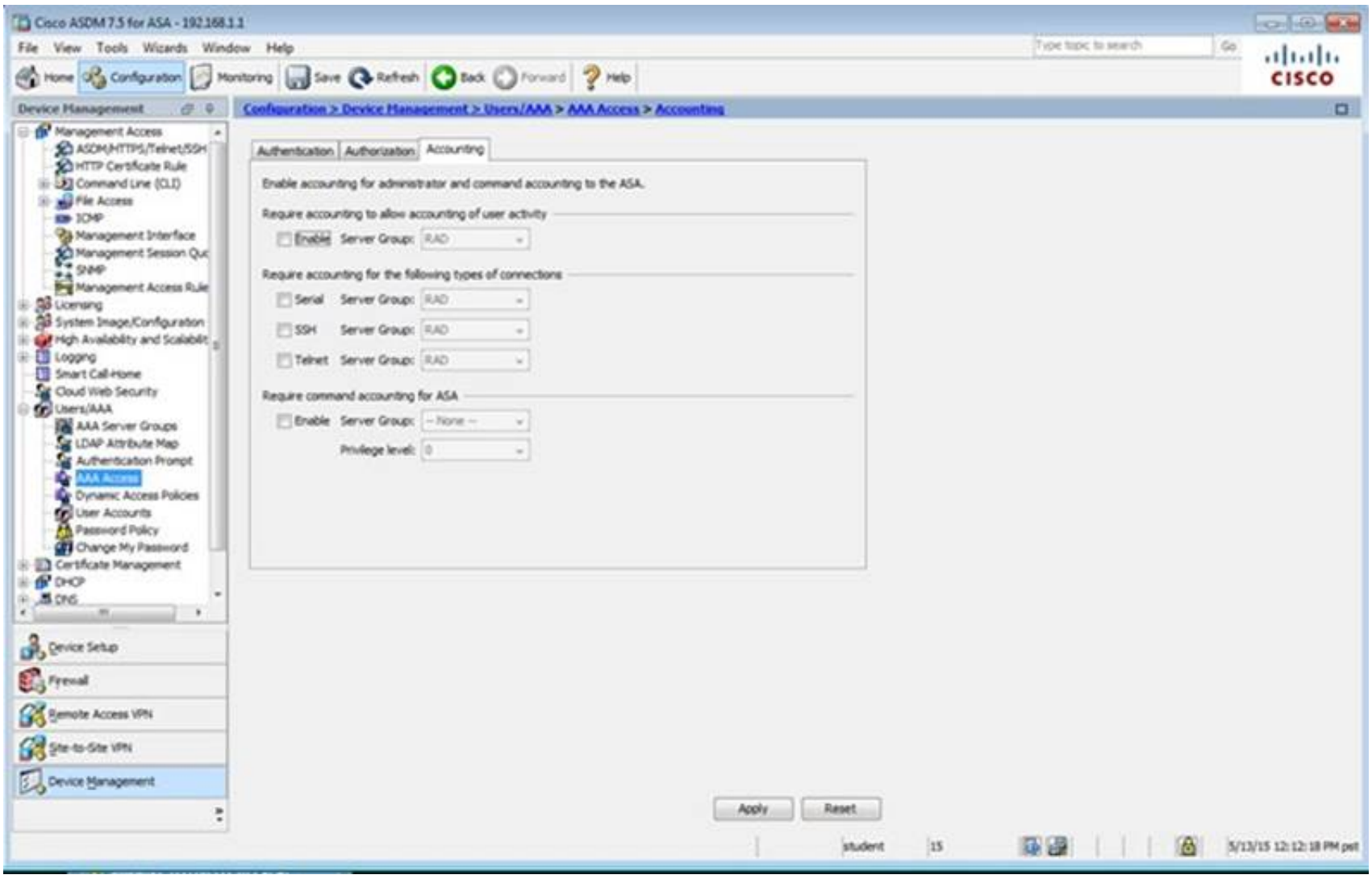
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Access Rules
Add Edit Delete
Enabled Source Criteria: Source User Security Group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

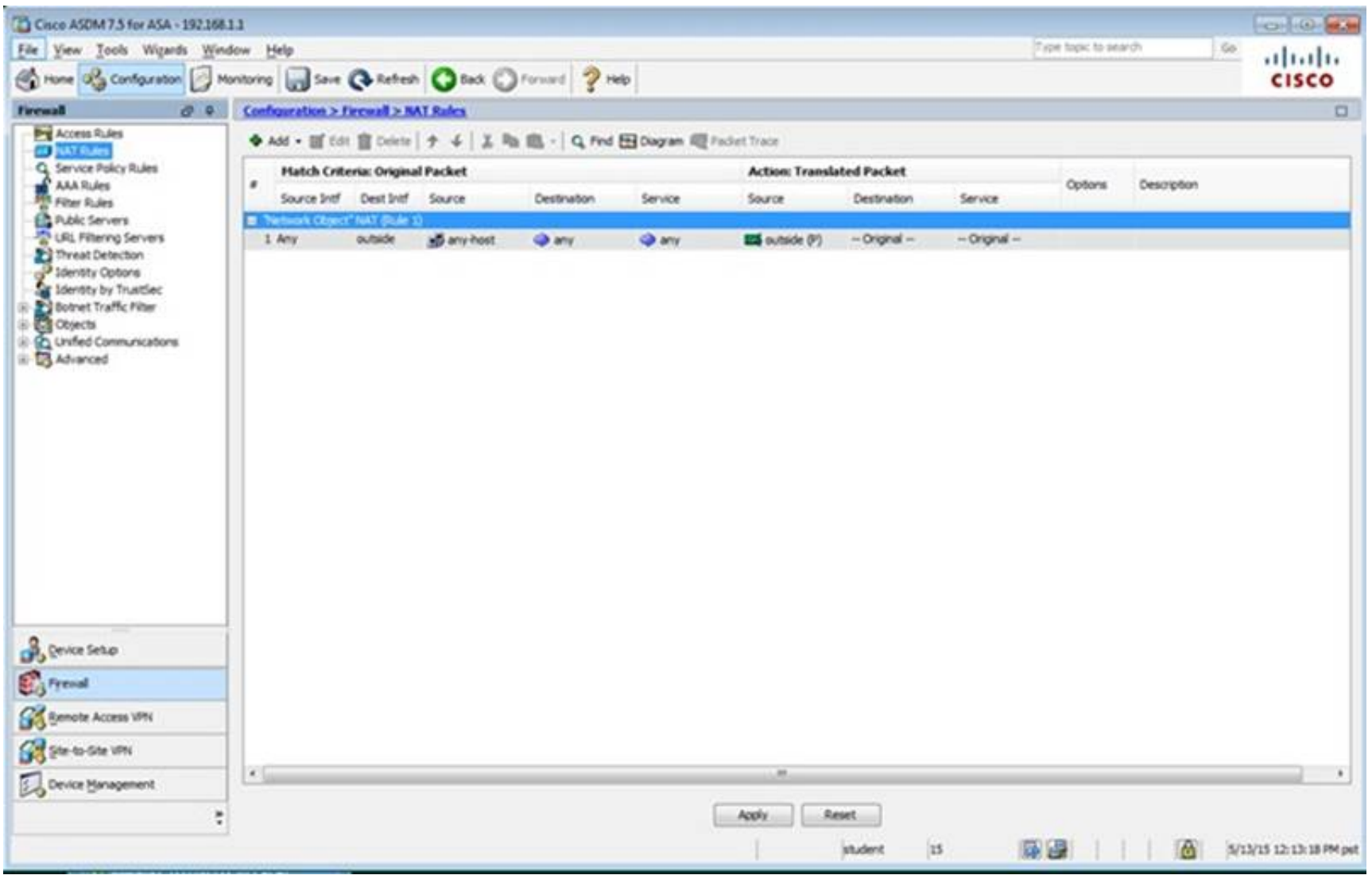

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (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

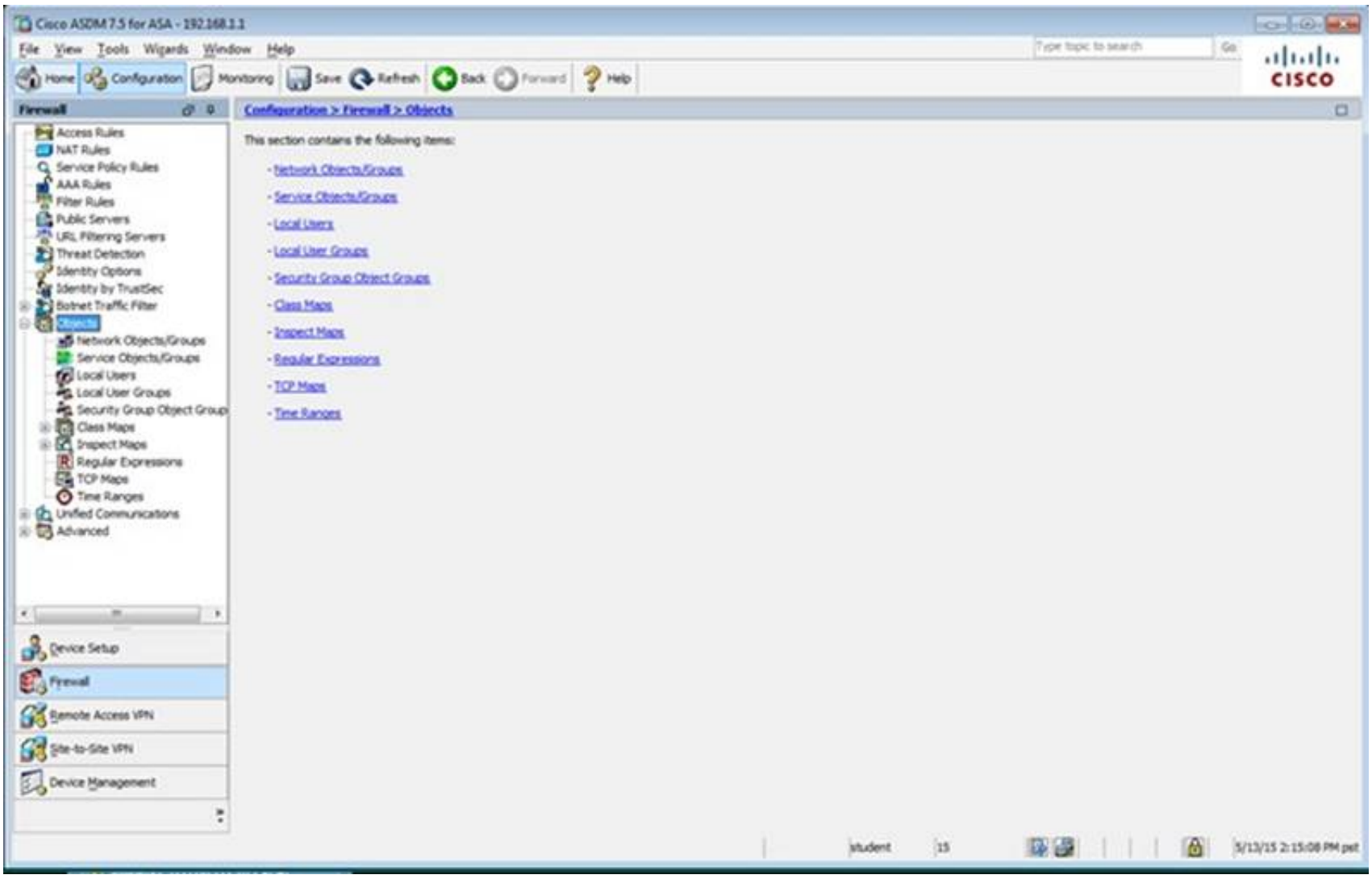

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Management Access > Management Session Quota
Enter the quota number for simultaneous administrative session (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

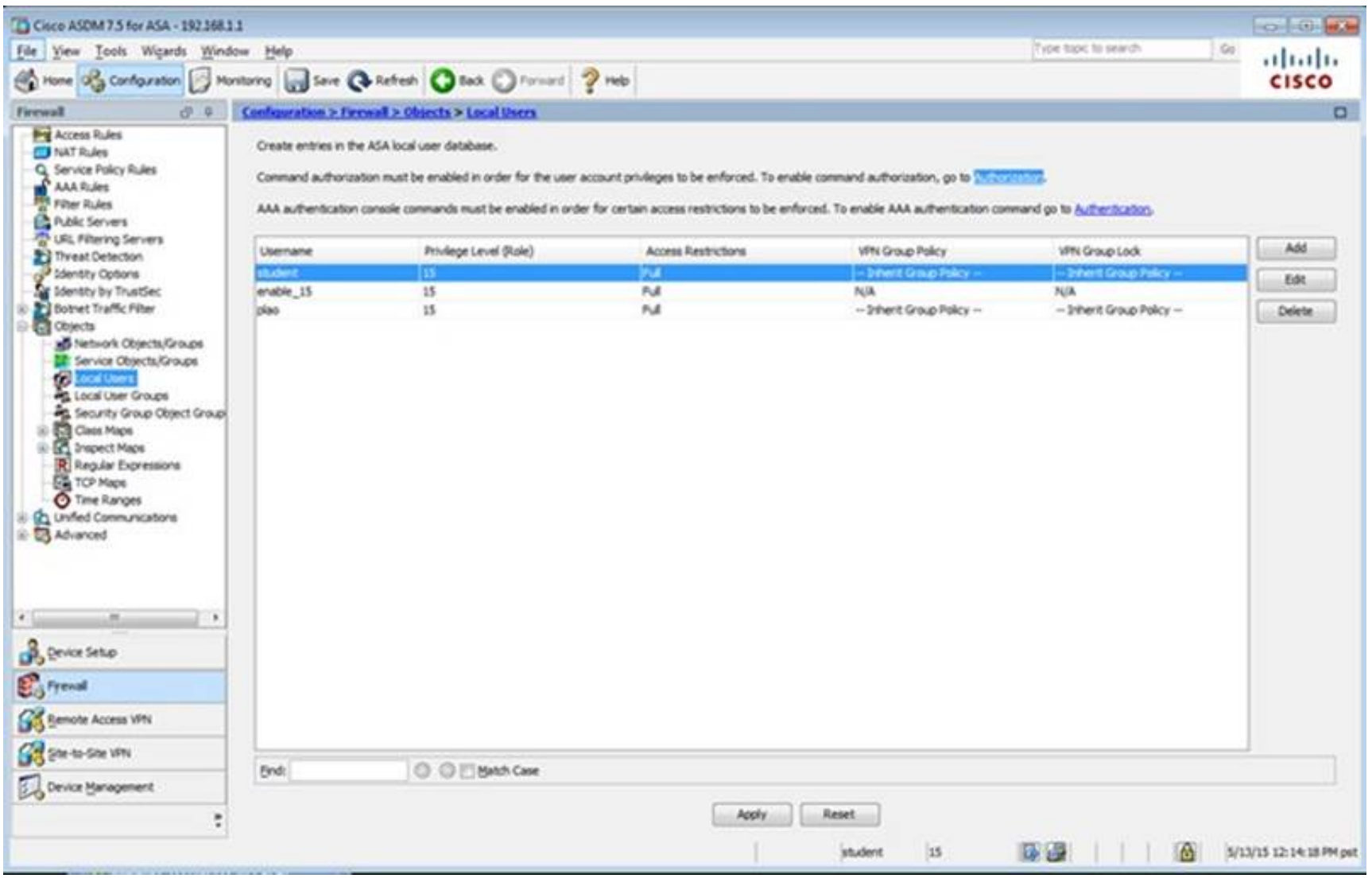

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Authorization Accounting
Enable authentication for administrator 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

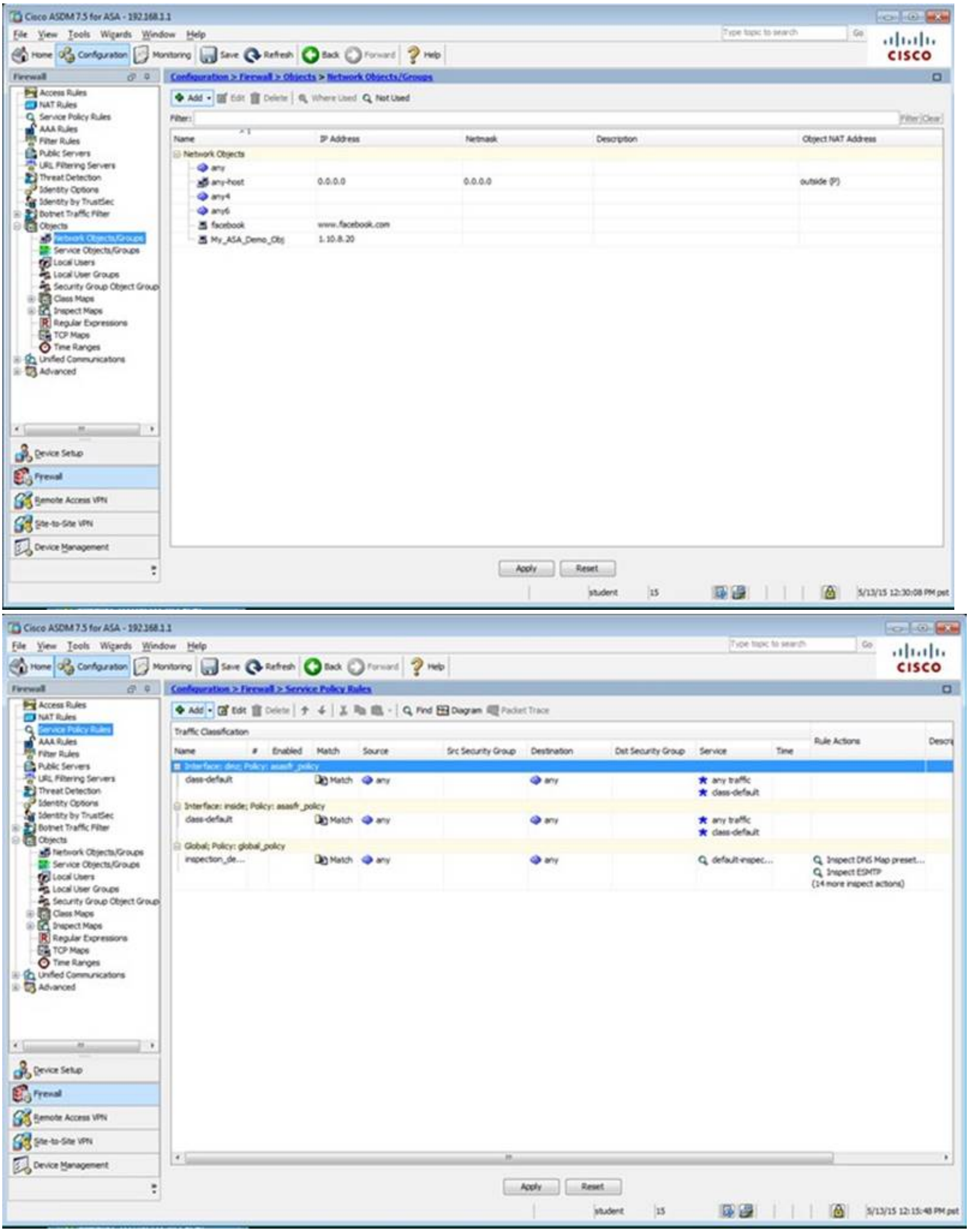

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Enable authorization for ASA 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
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
SNMP
Licensing
System Image/Configuration
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

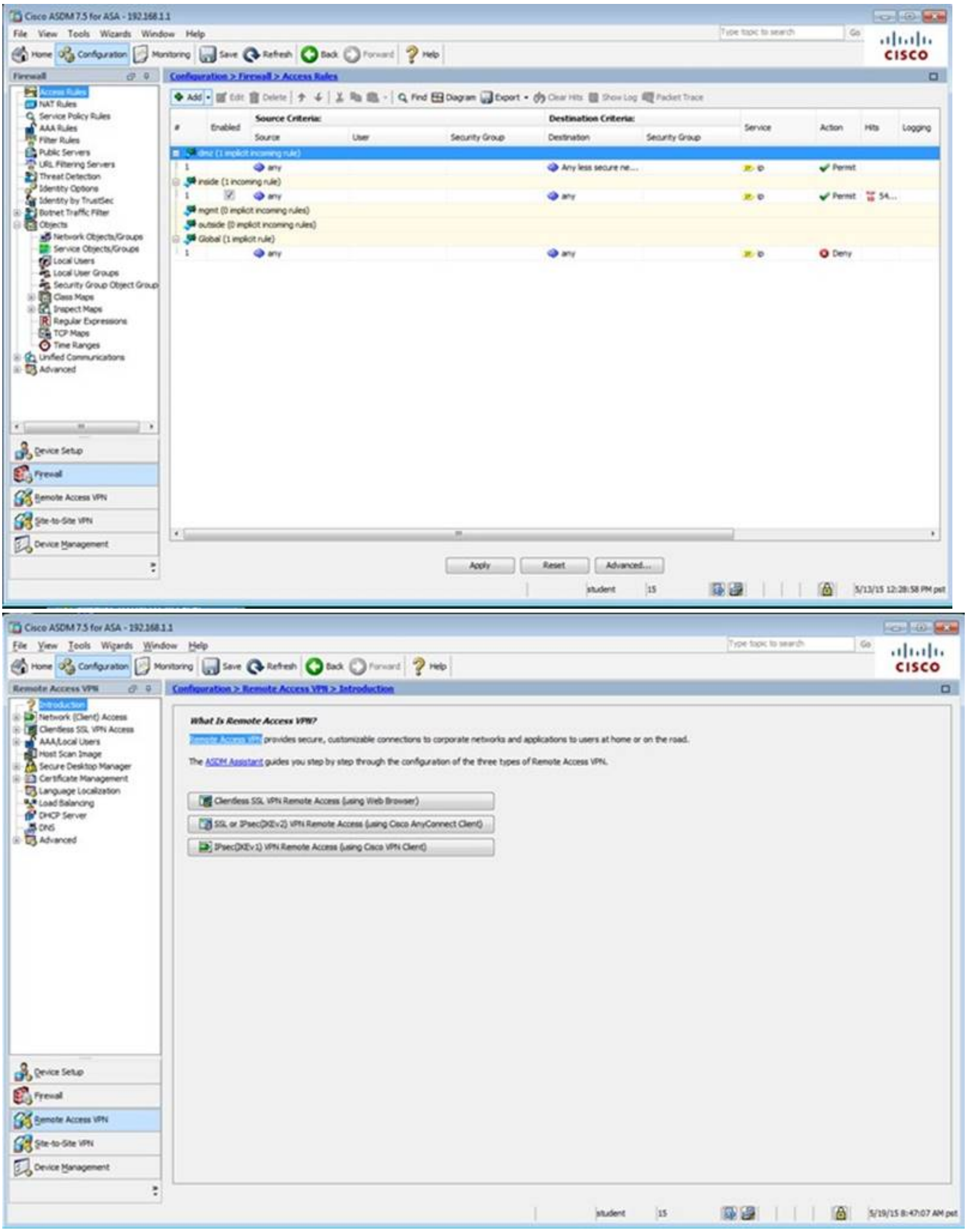

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Match Criteria: Original Packet
Action: Translated Packet
Source Intf Dest 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 --
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
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

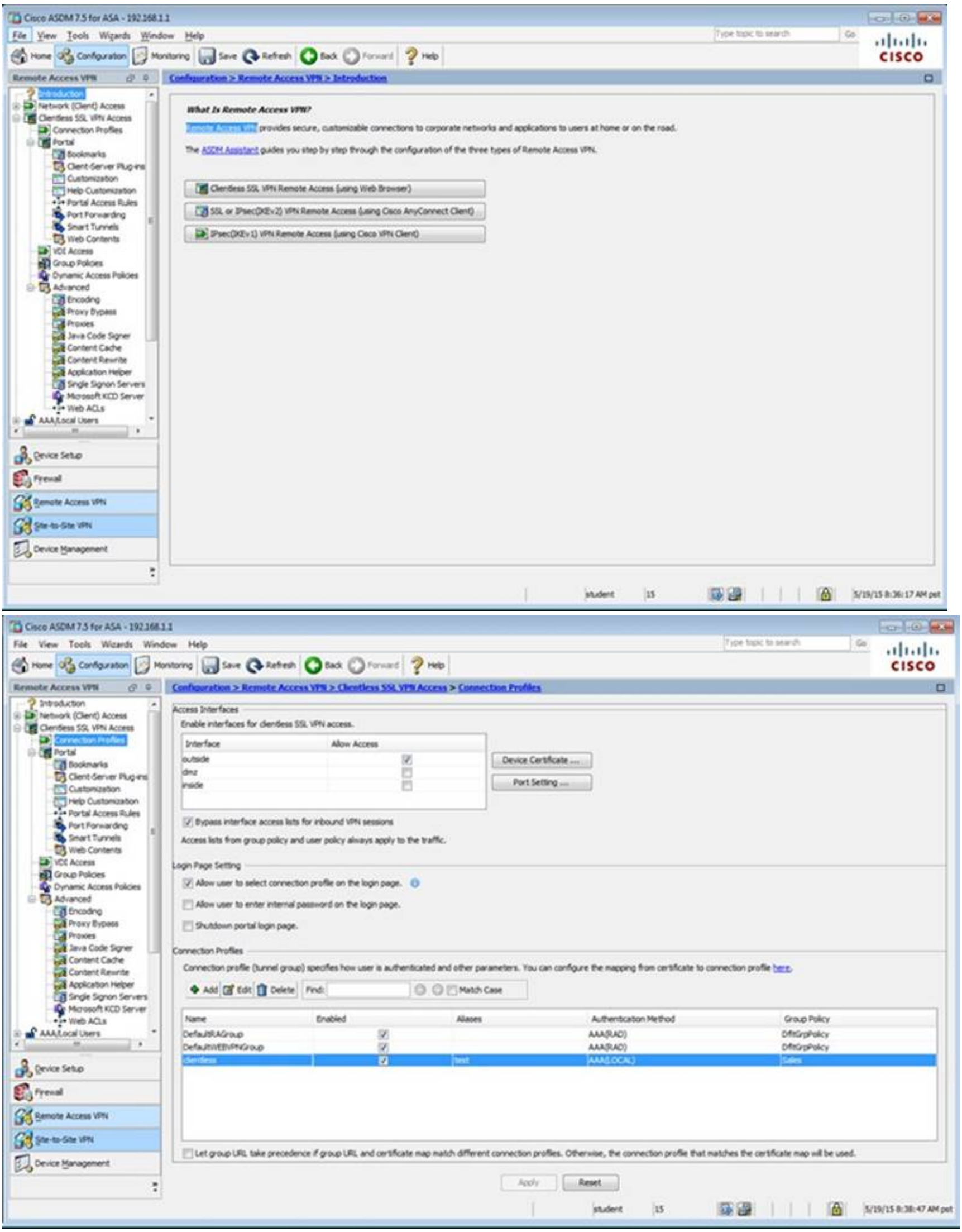

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user 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
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 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

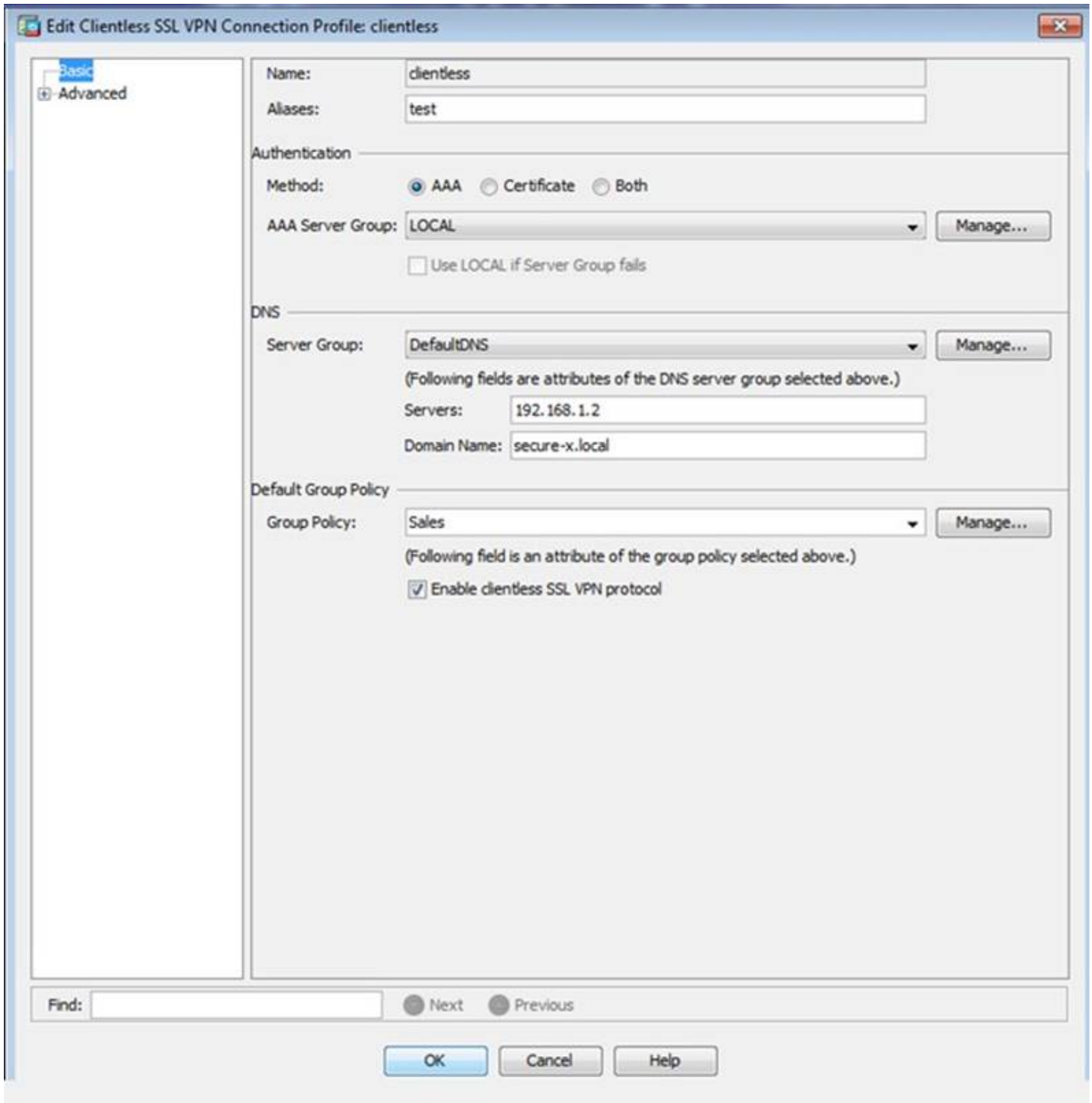
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security 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

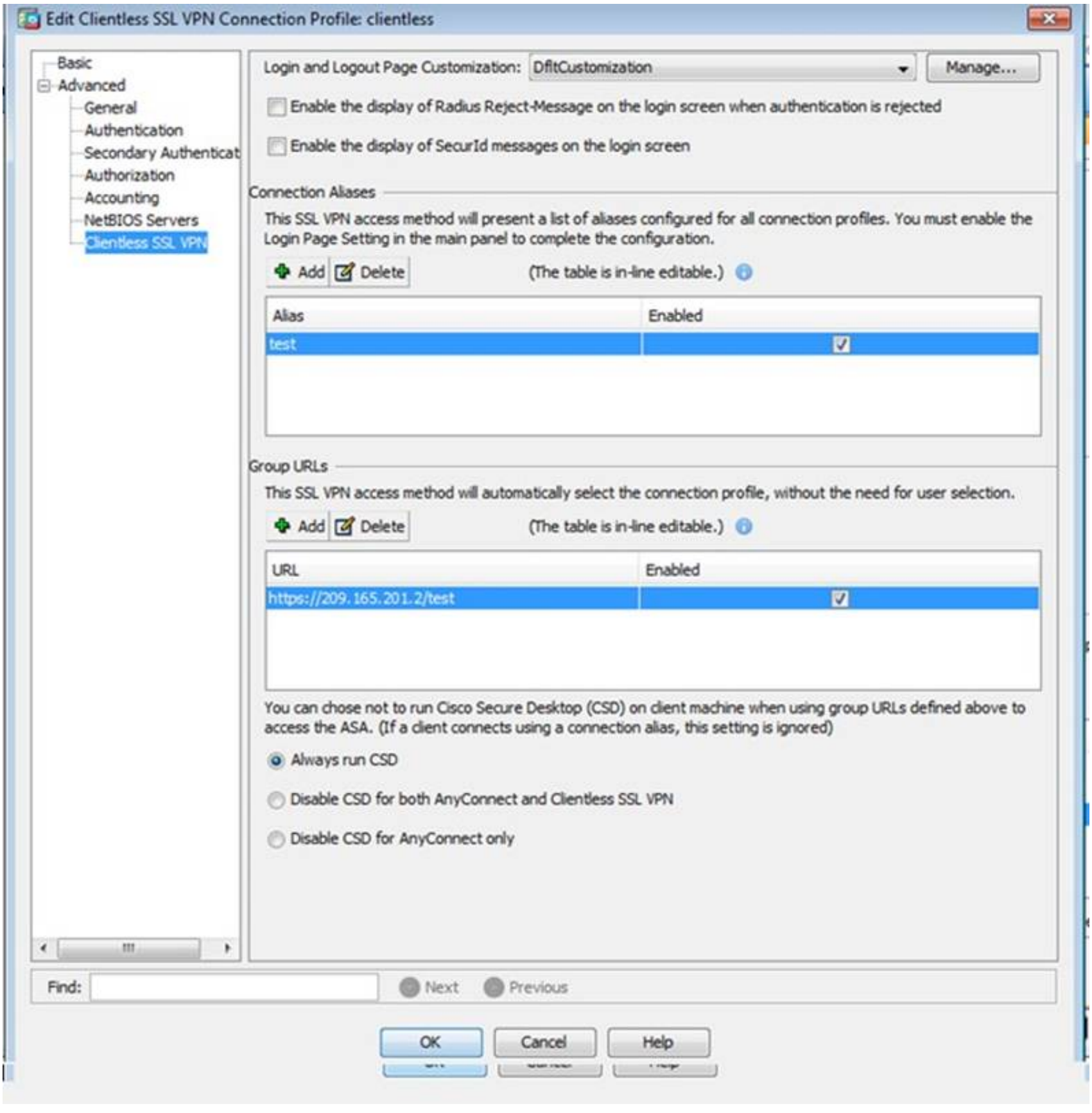

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria: Destination Criteria:
Enabled 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

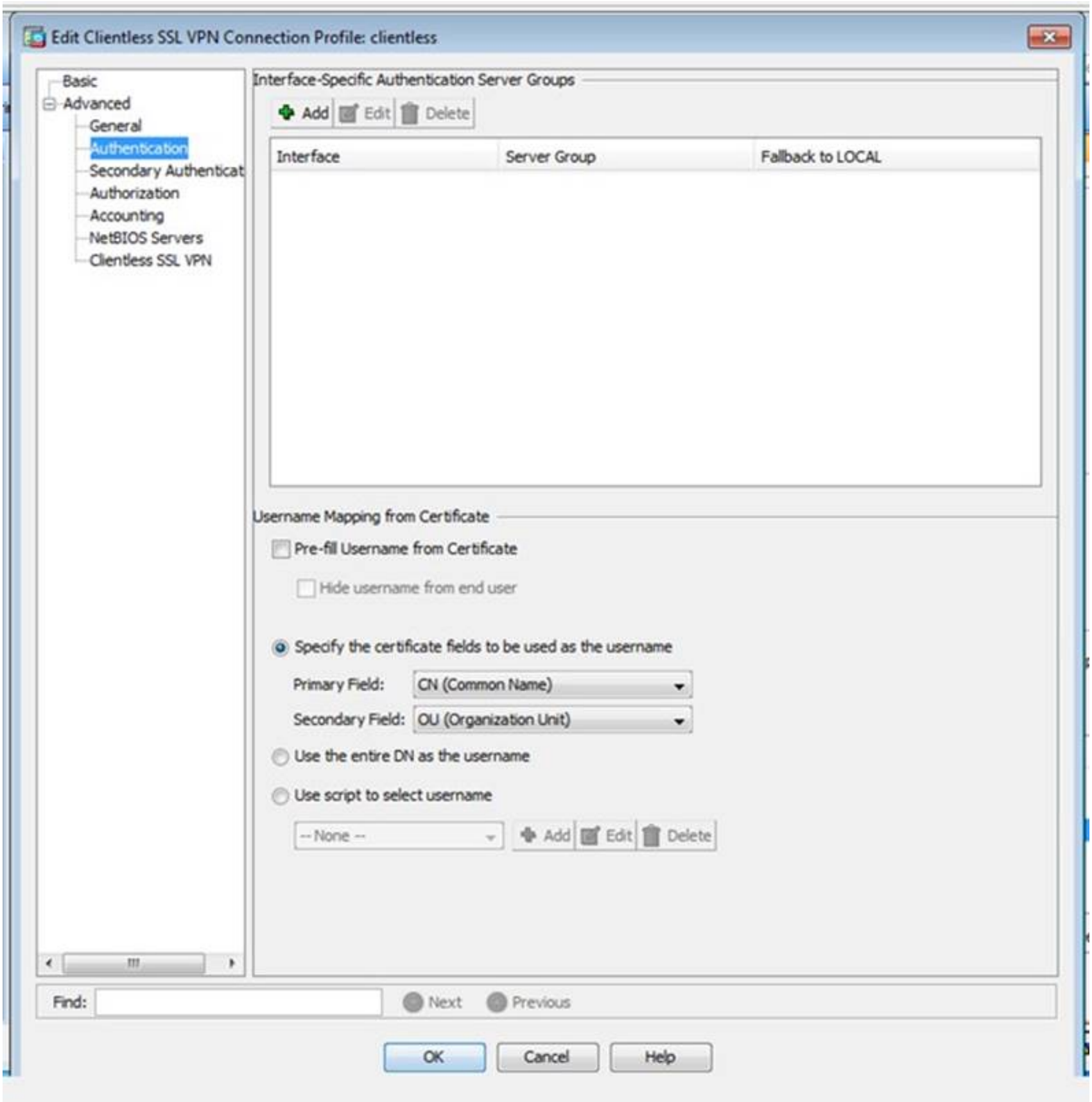
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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

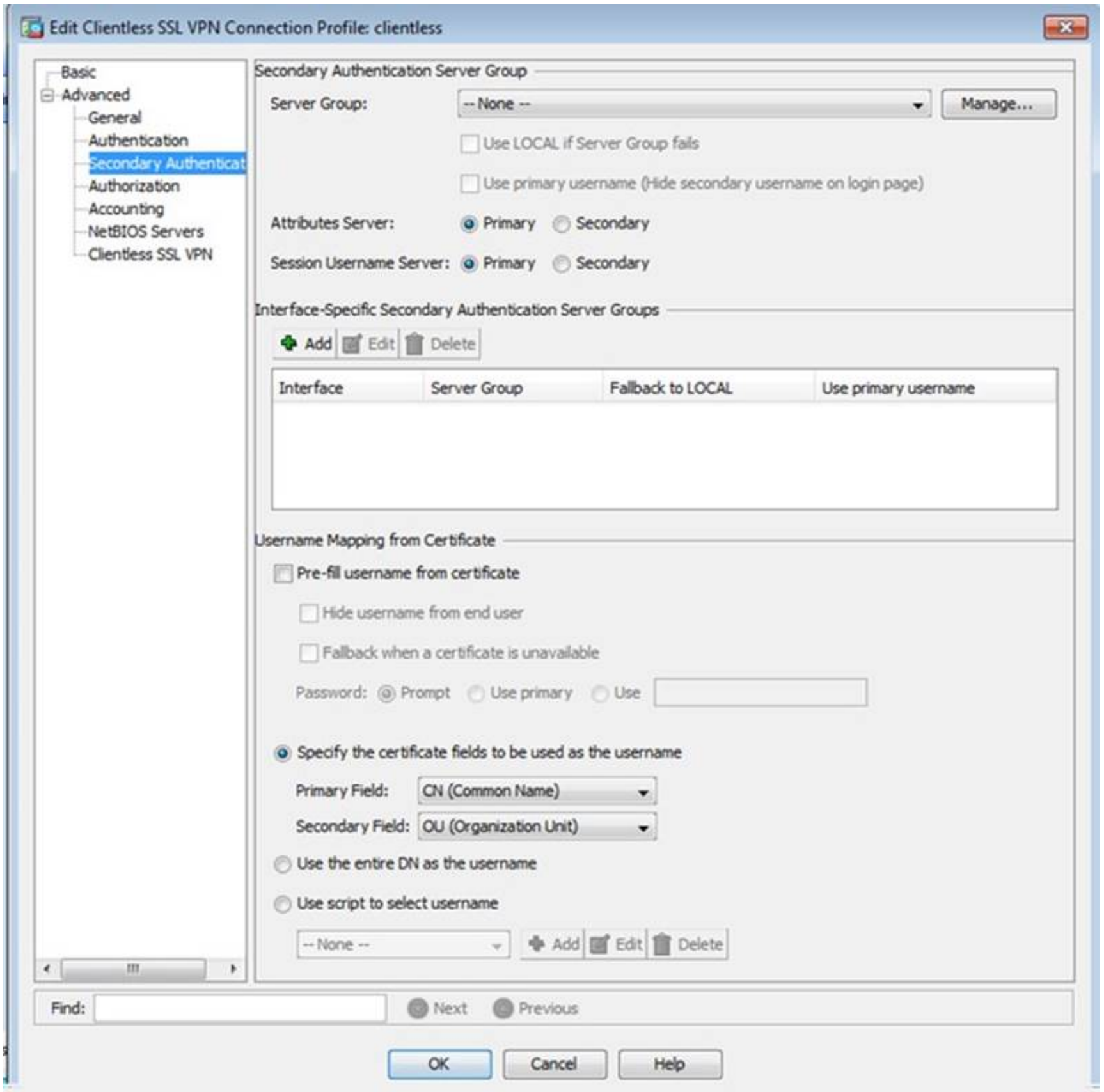

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
What Is Remote Access VPN?
Remote Access VPN provides secure, customizable connections to corporate 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

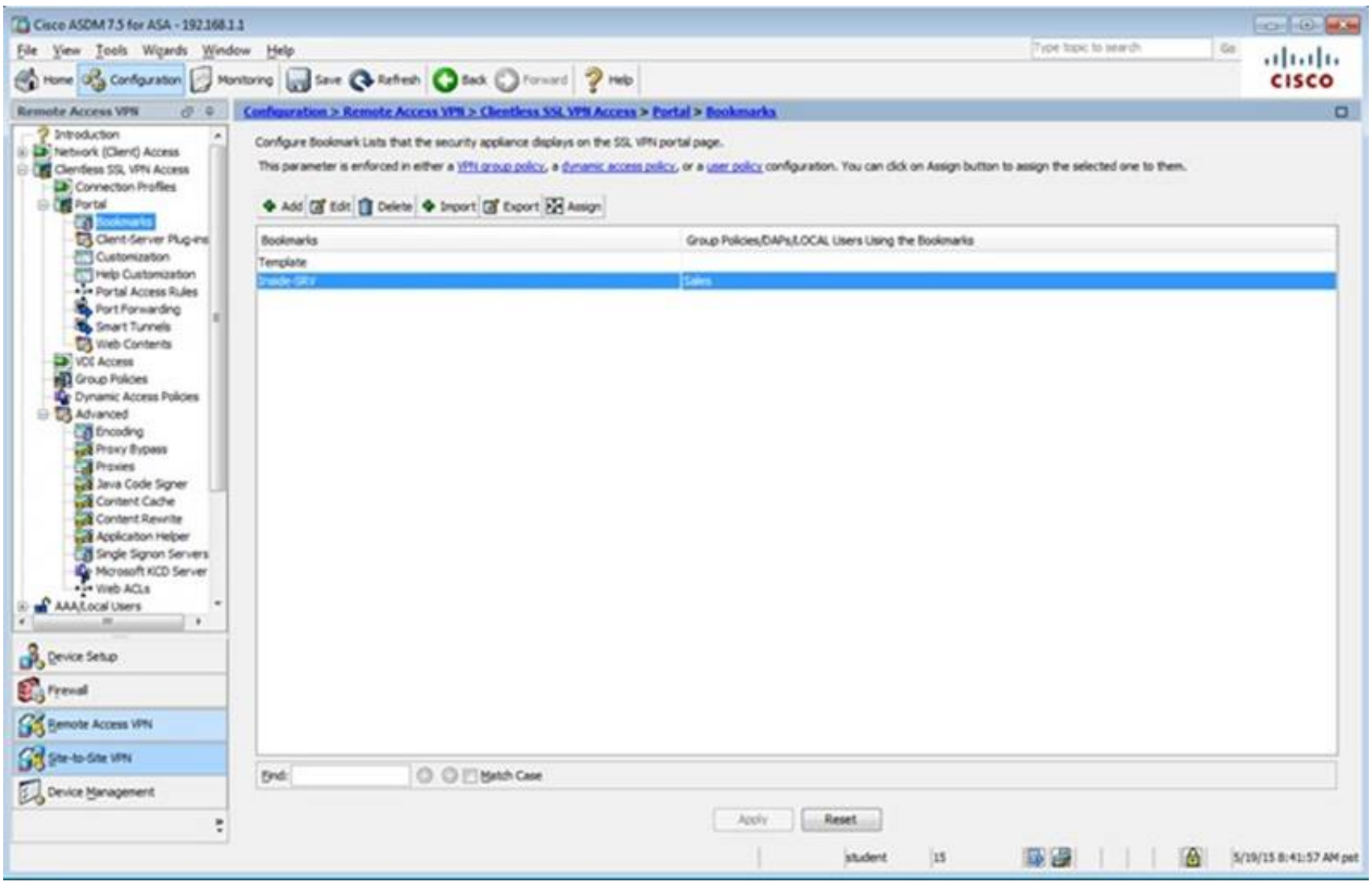
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles
Access Interfaces
Enable interfaces for clientless SSL VPN 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
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

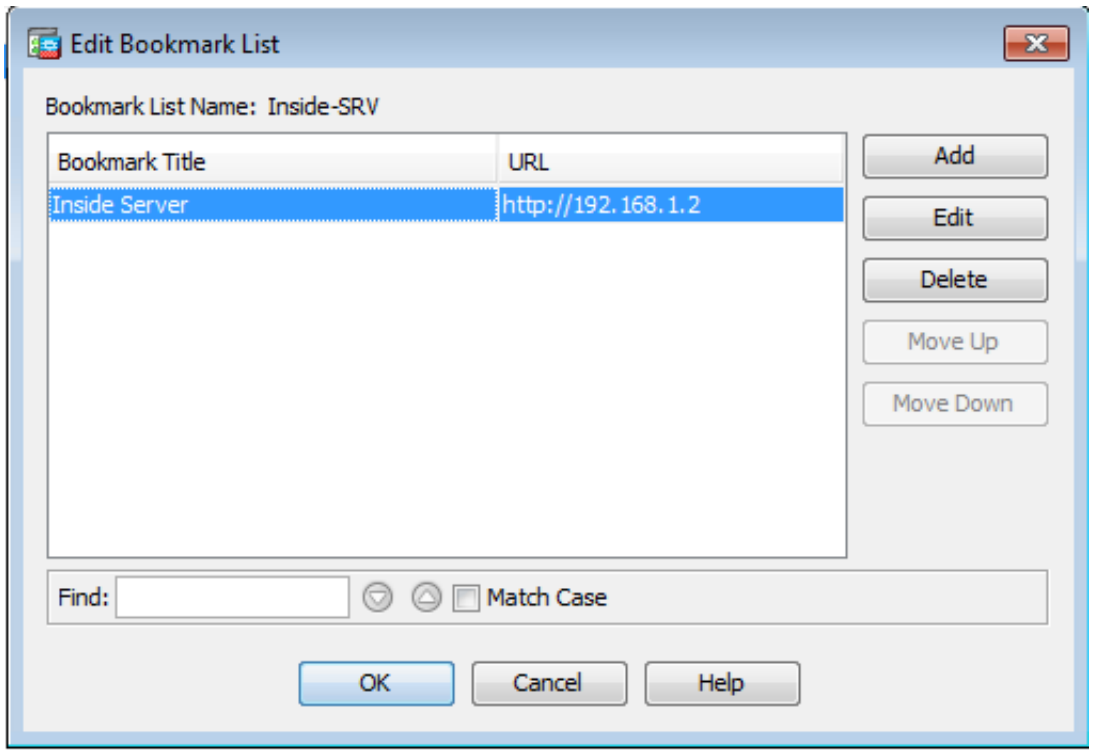

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server 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

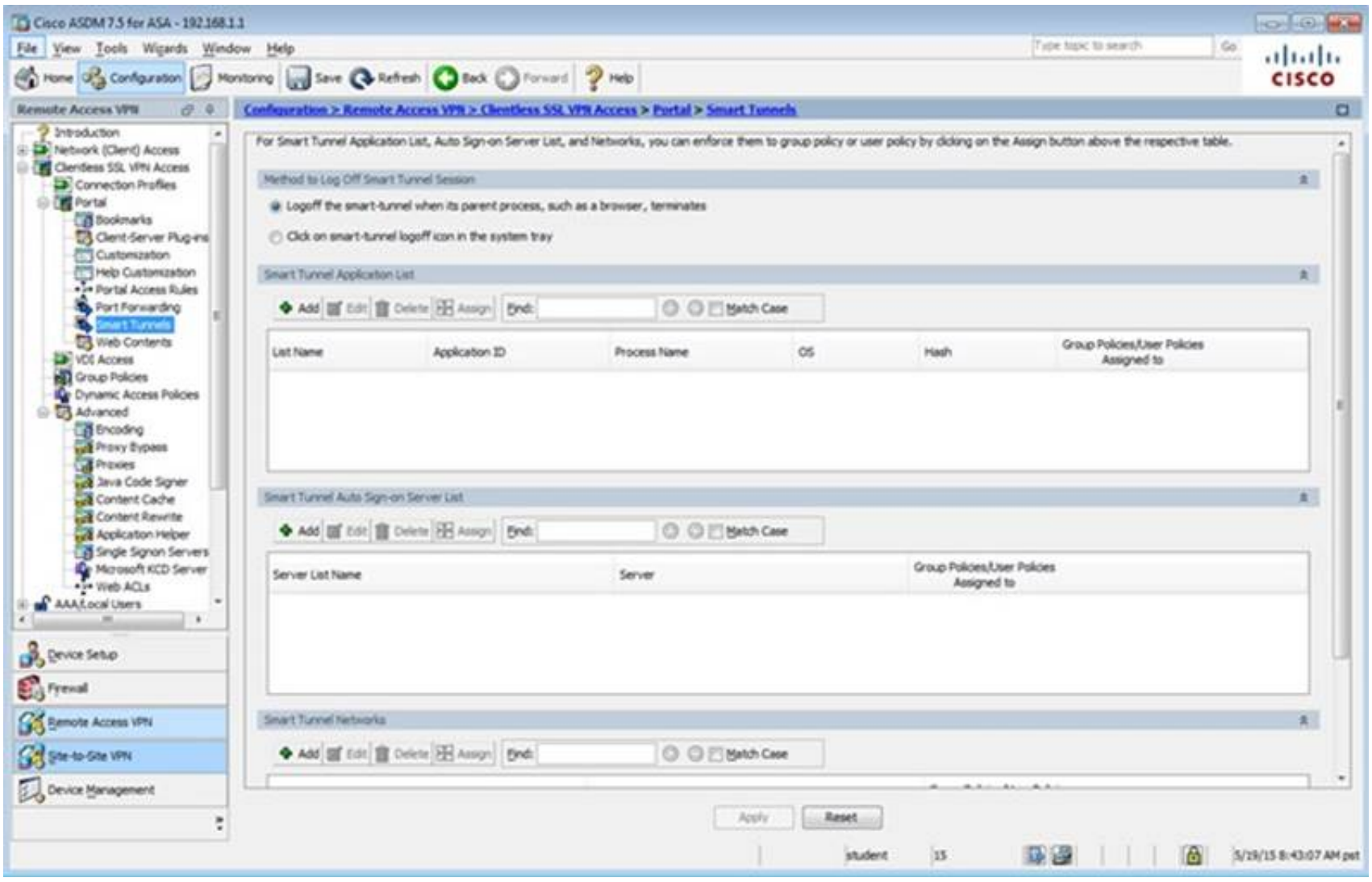

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen 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

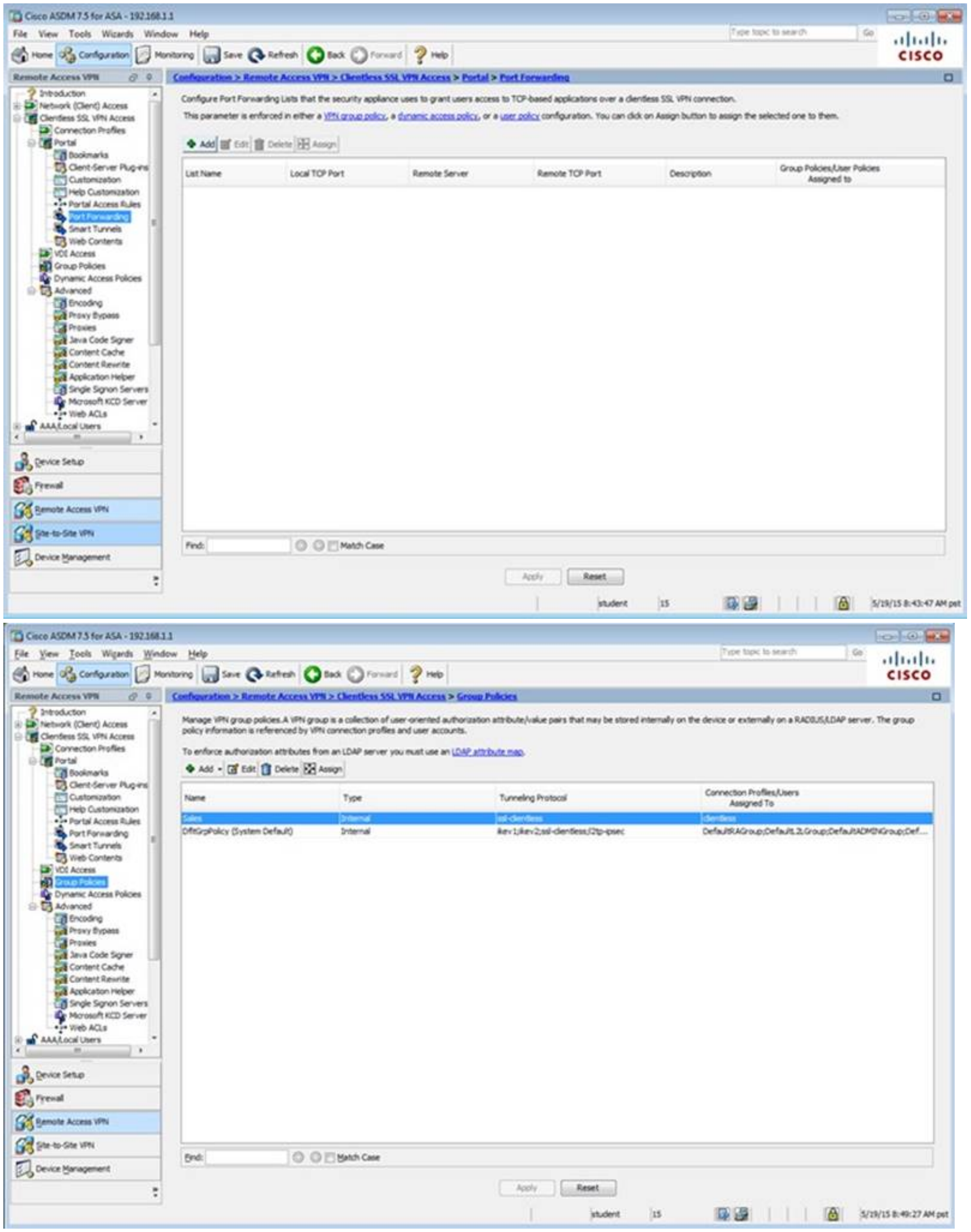

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from 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

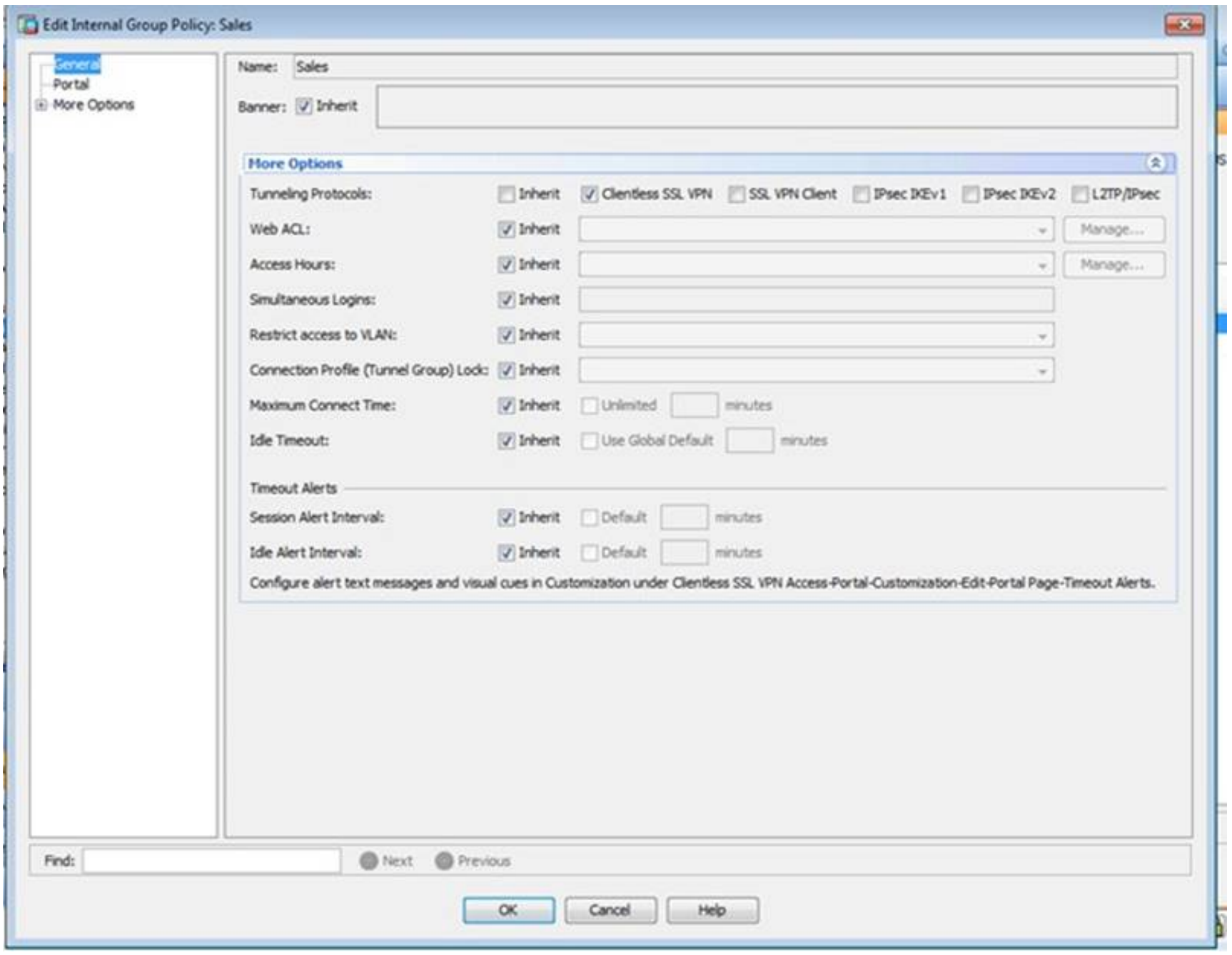

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection 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

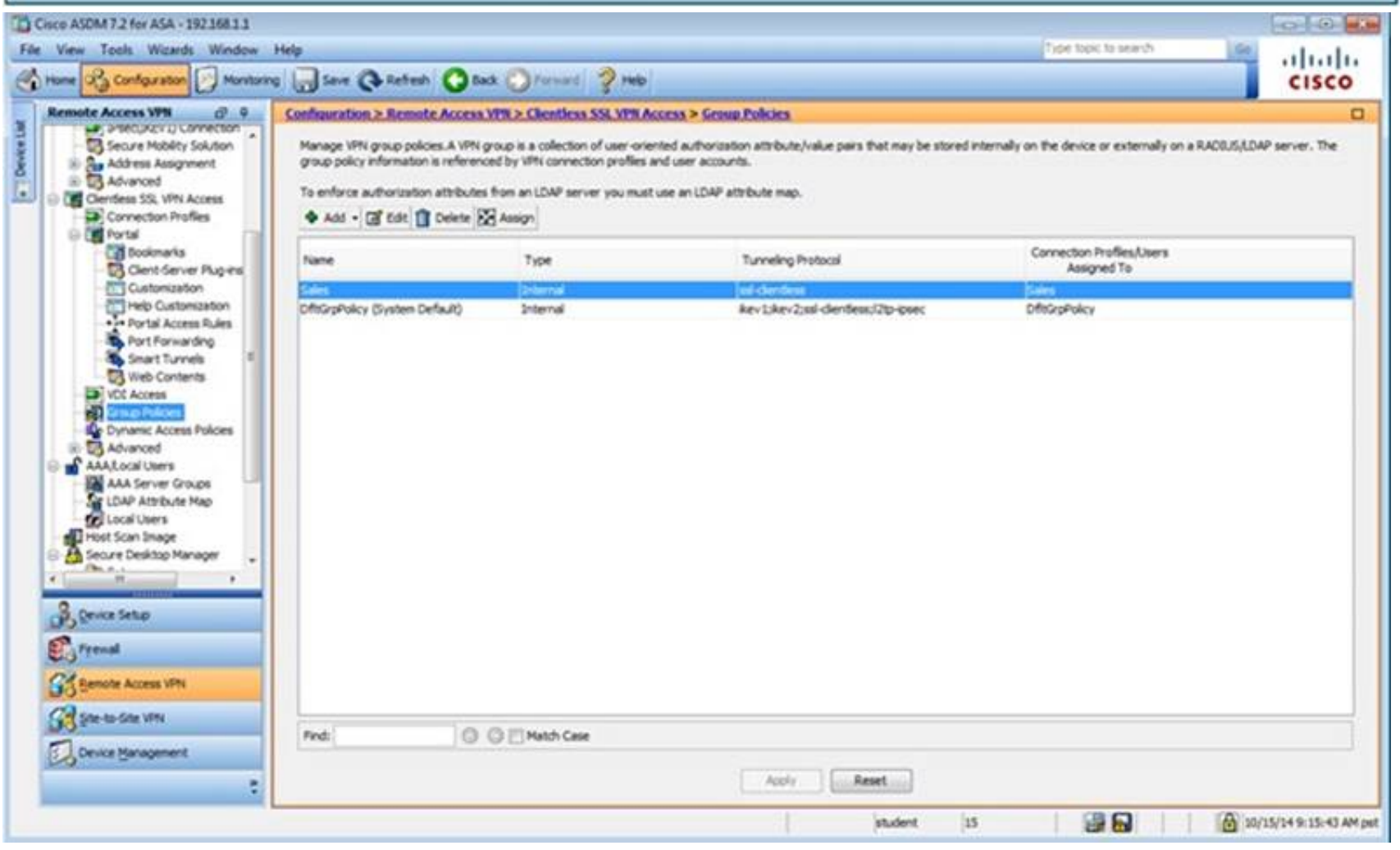

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

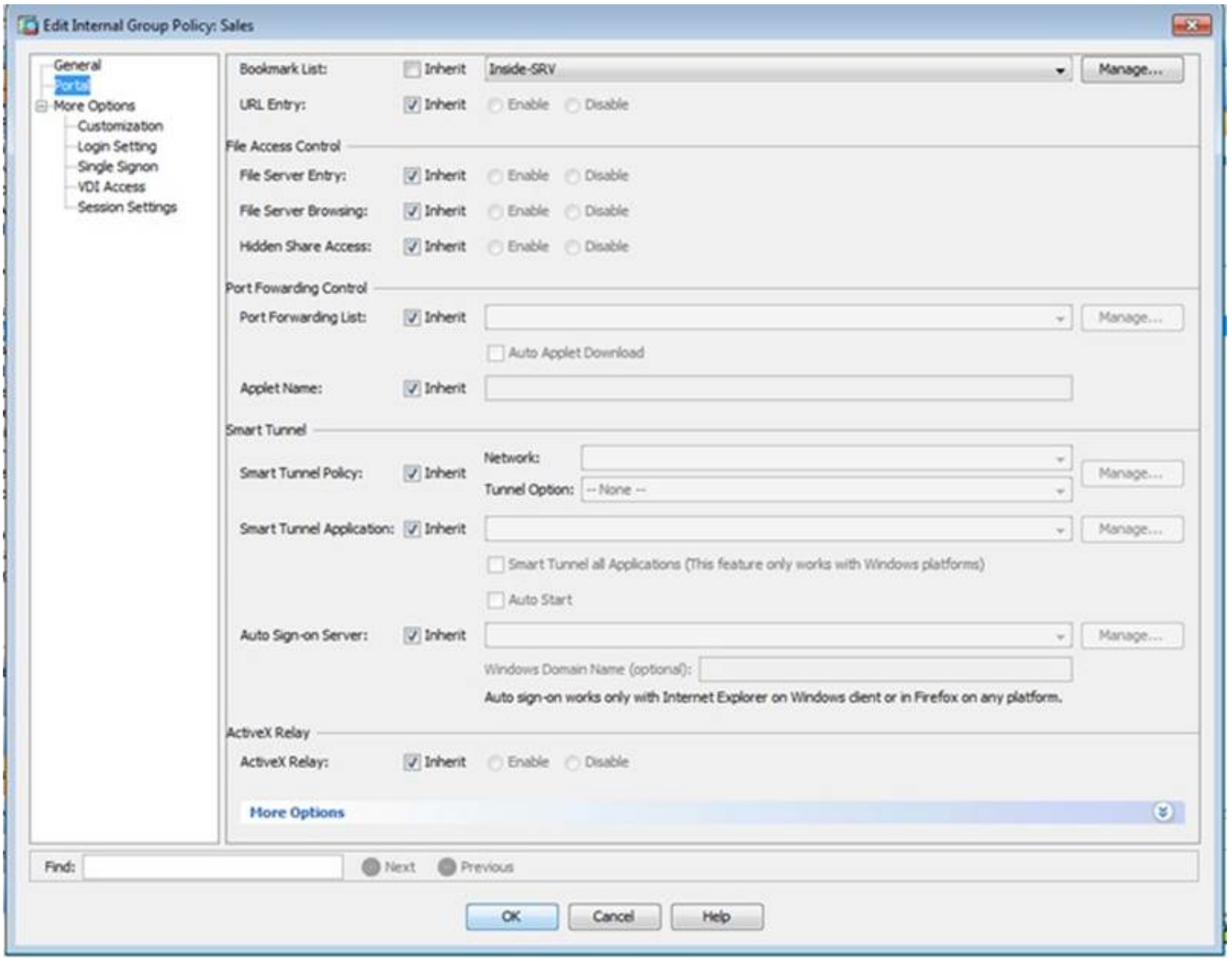

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection 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

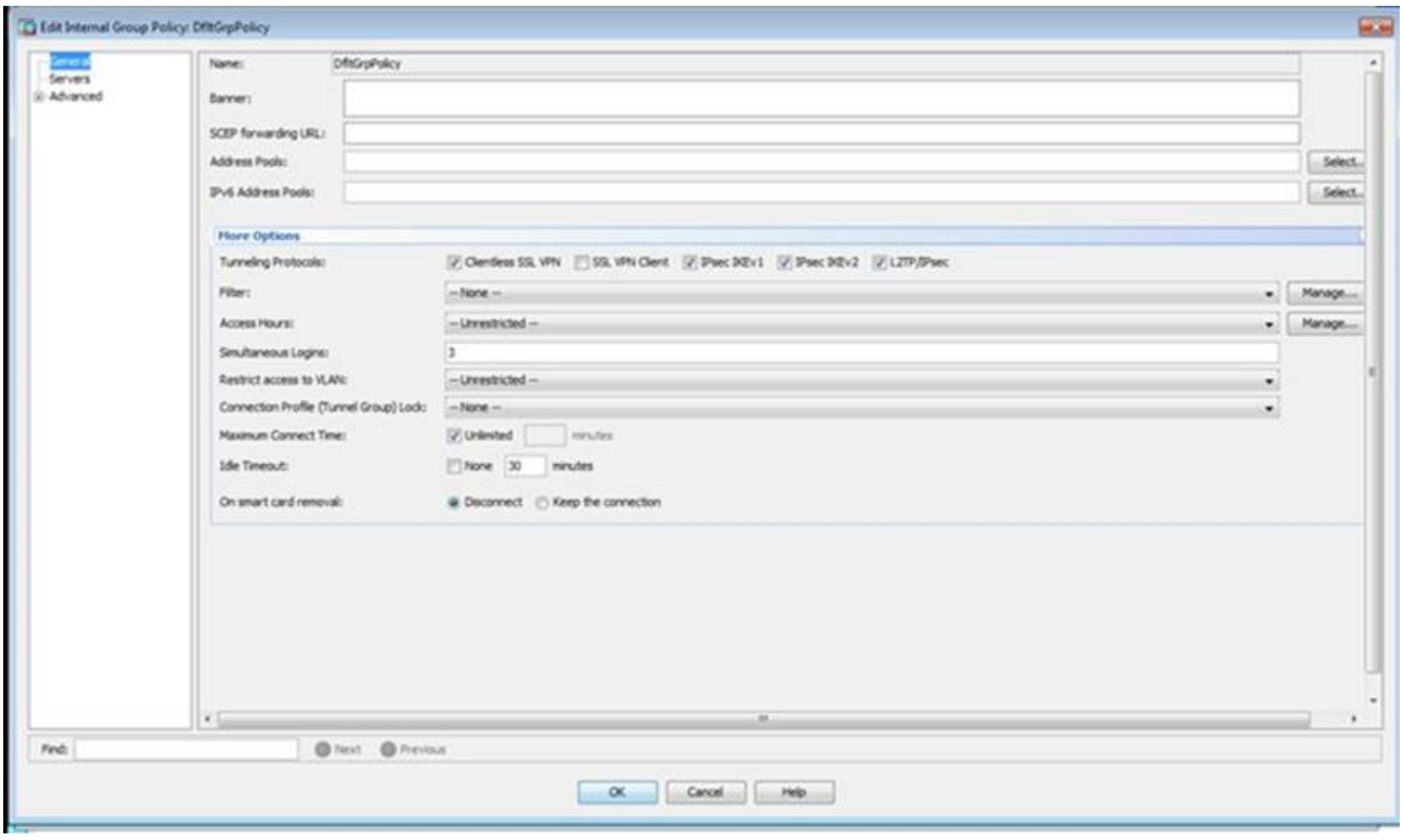

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Configure Port Forwarding Lists that the security appliance 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

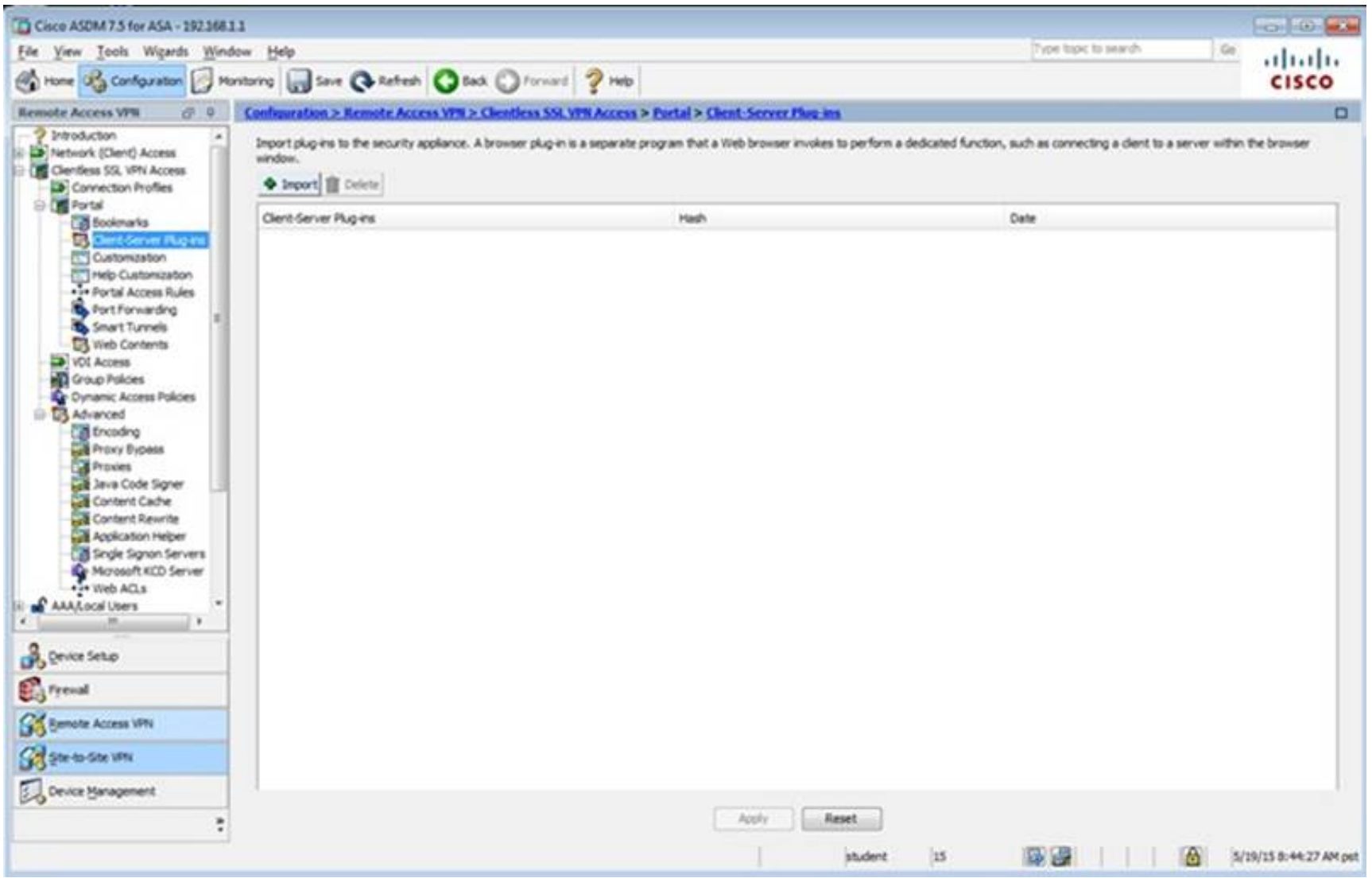
Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented 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

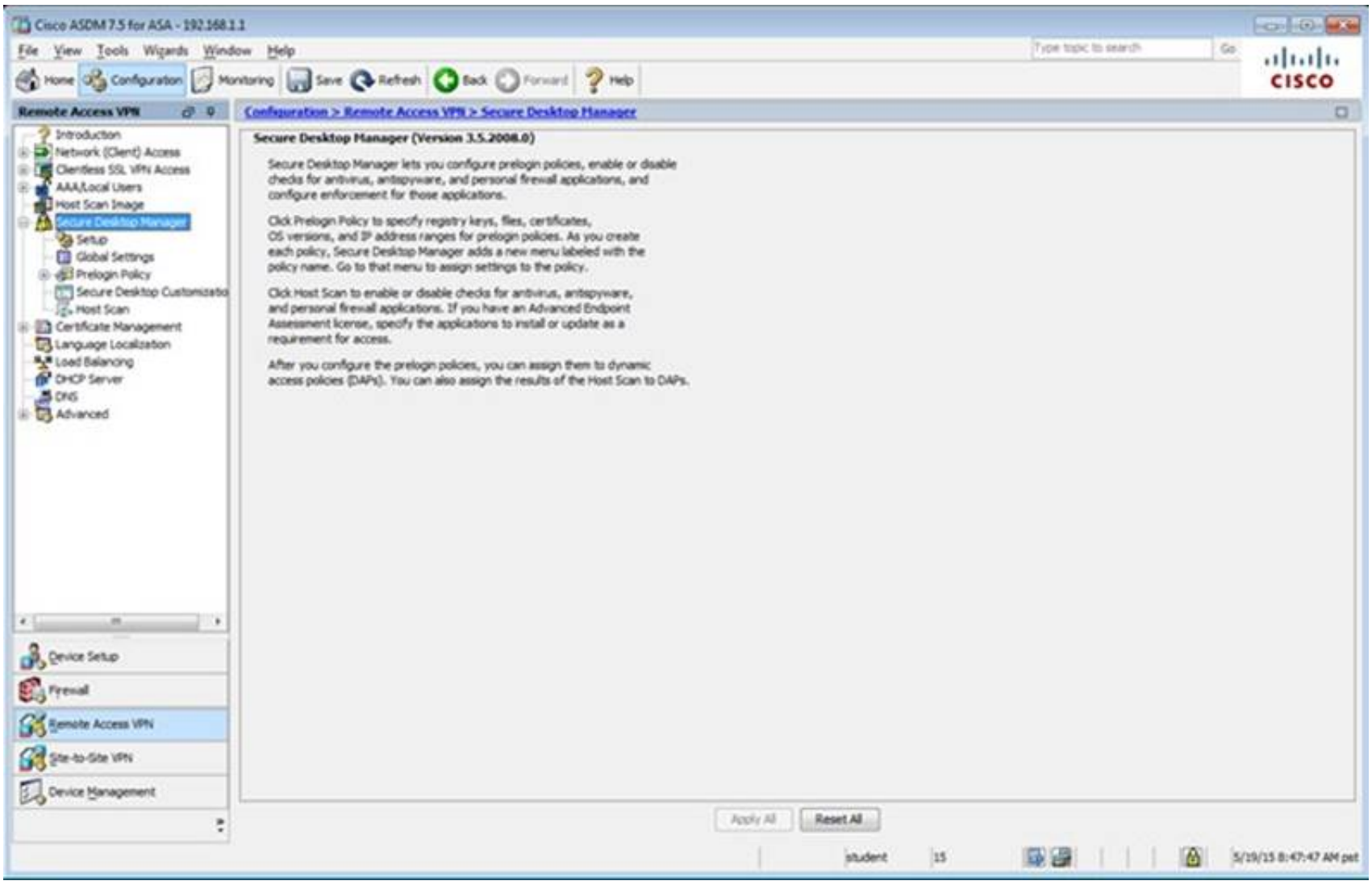

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access 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

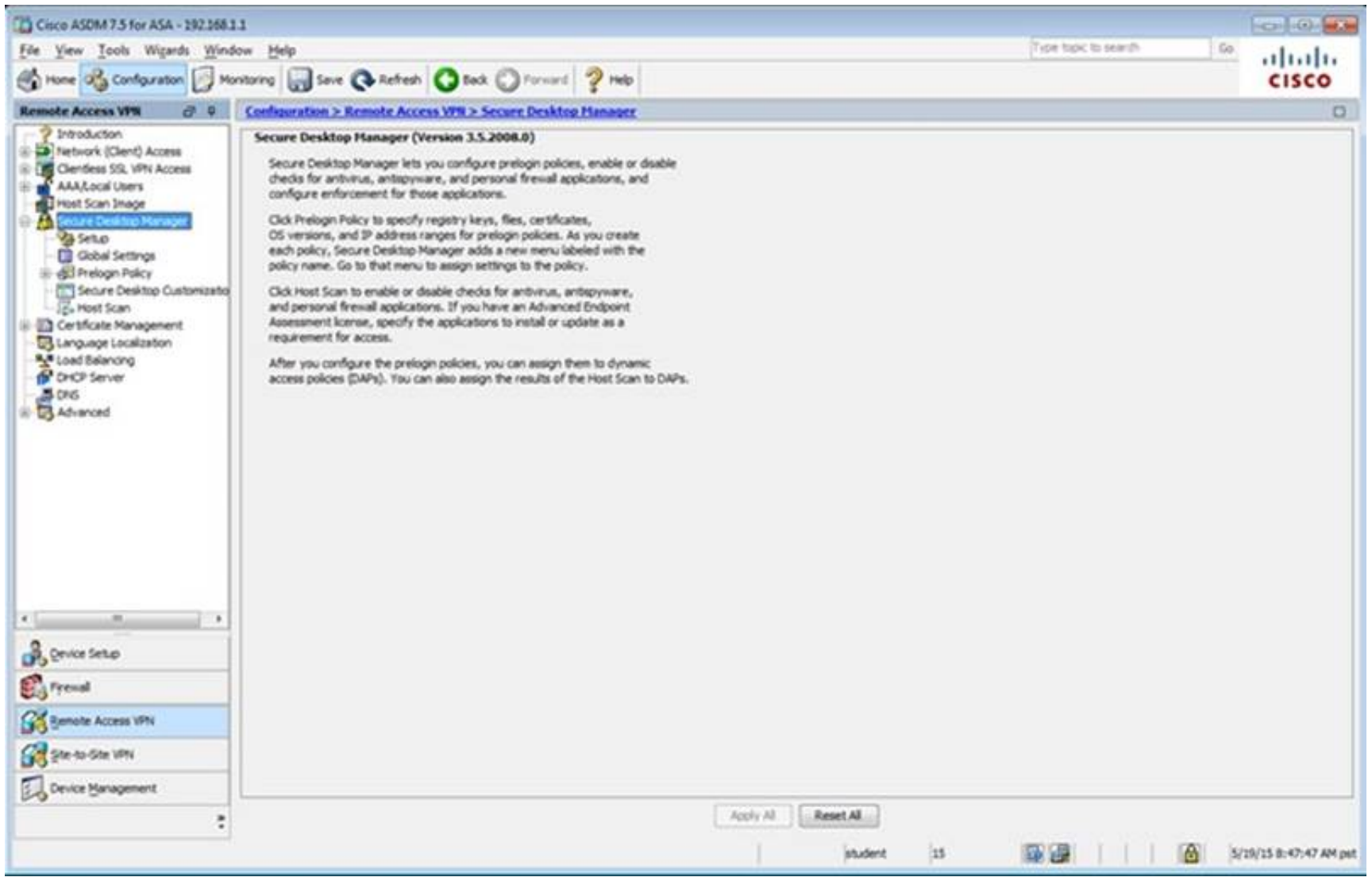

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented 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
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
Find: Match Case
Apply Reset
student 15
10/15/14 9:15:43 AM pst

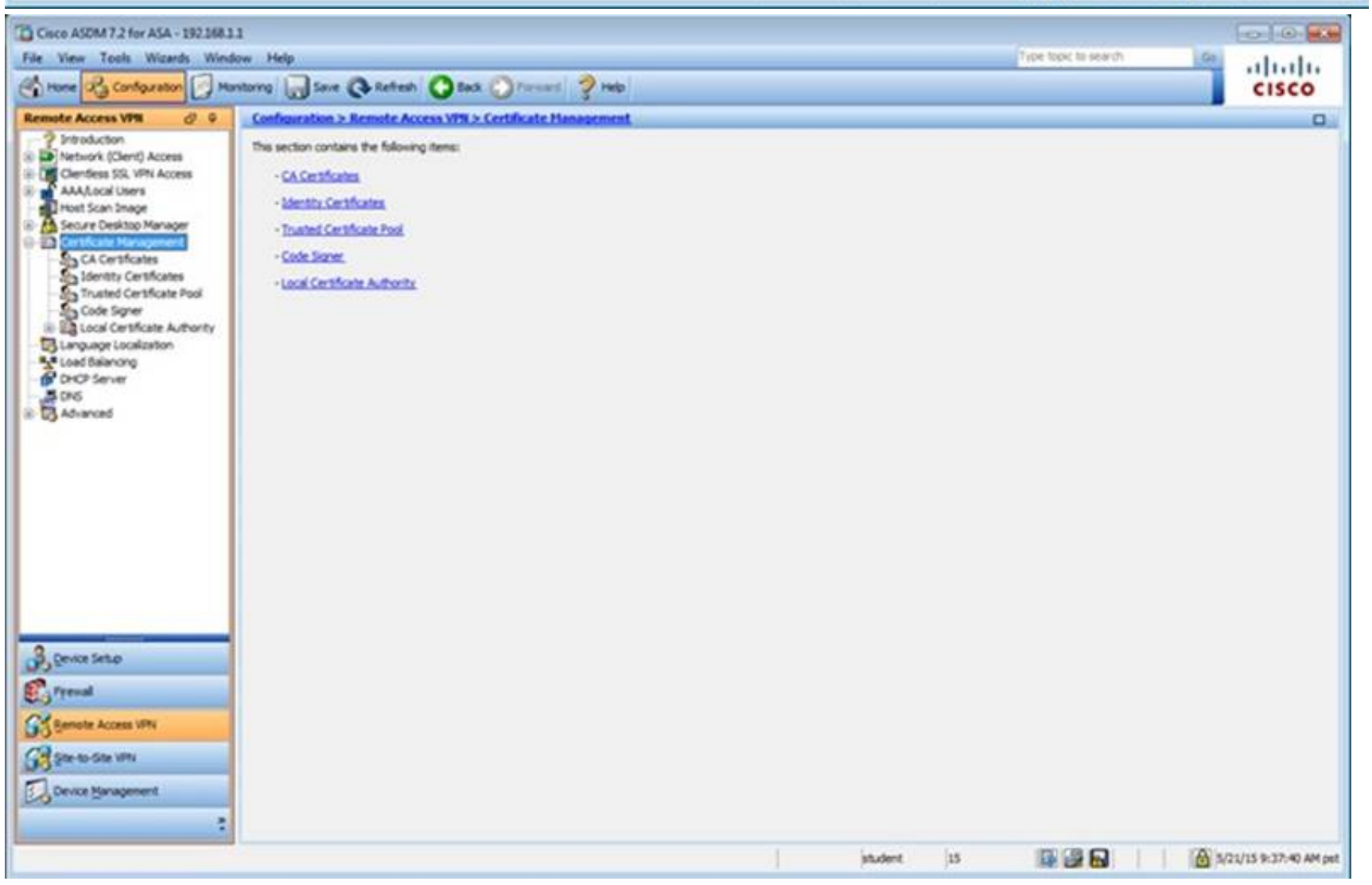

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding 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

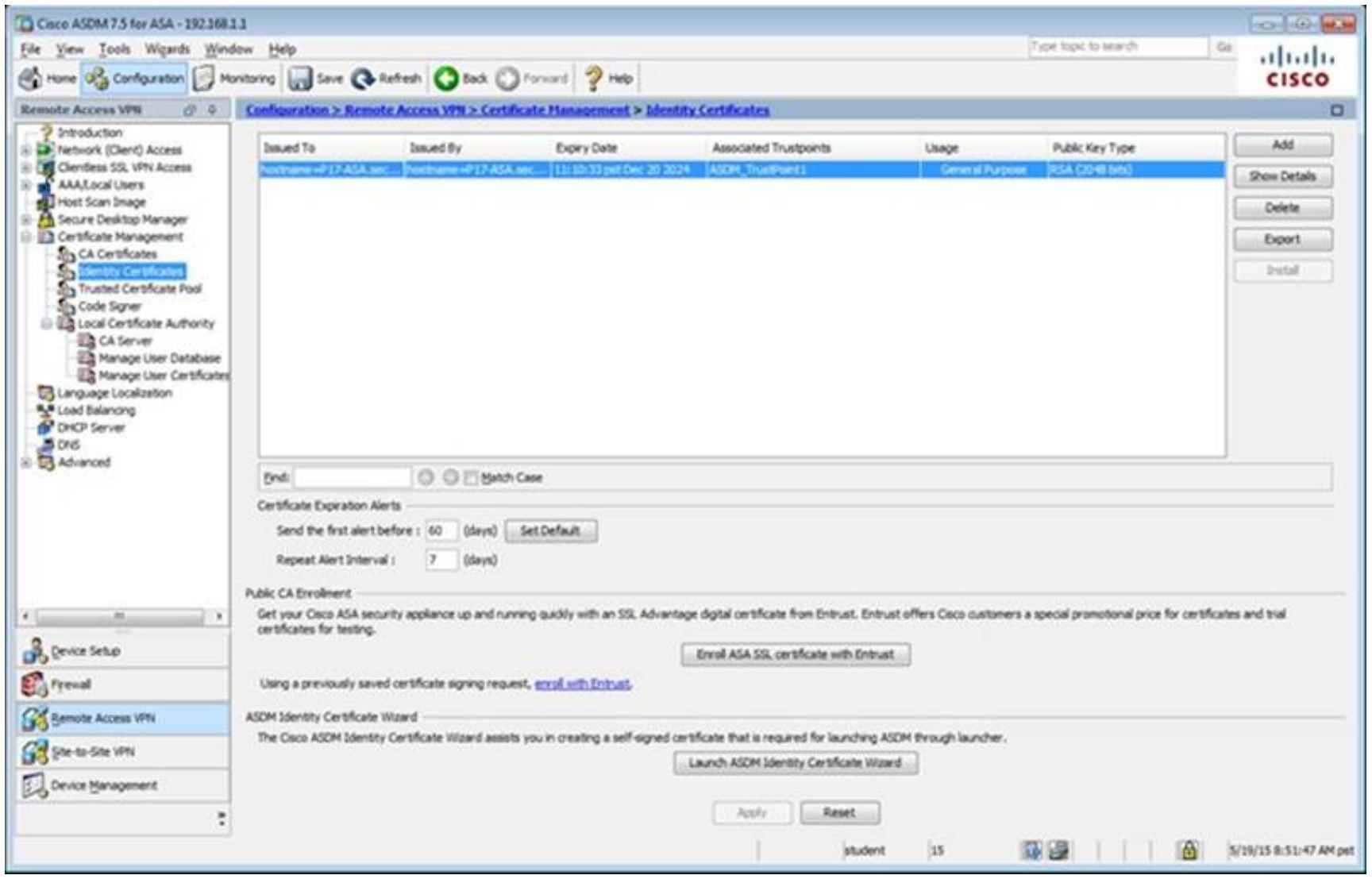

Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Name:
DfltGrpPolicy
Banner:
SCEP forwarding URL:
Address Pools:
Select...
IPv6 Address Pools:
More Options
Tunneling Protocols:
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
L2TP/IPsec
Filter:
-- None --
Manage...
Access Hours:
-- 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

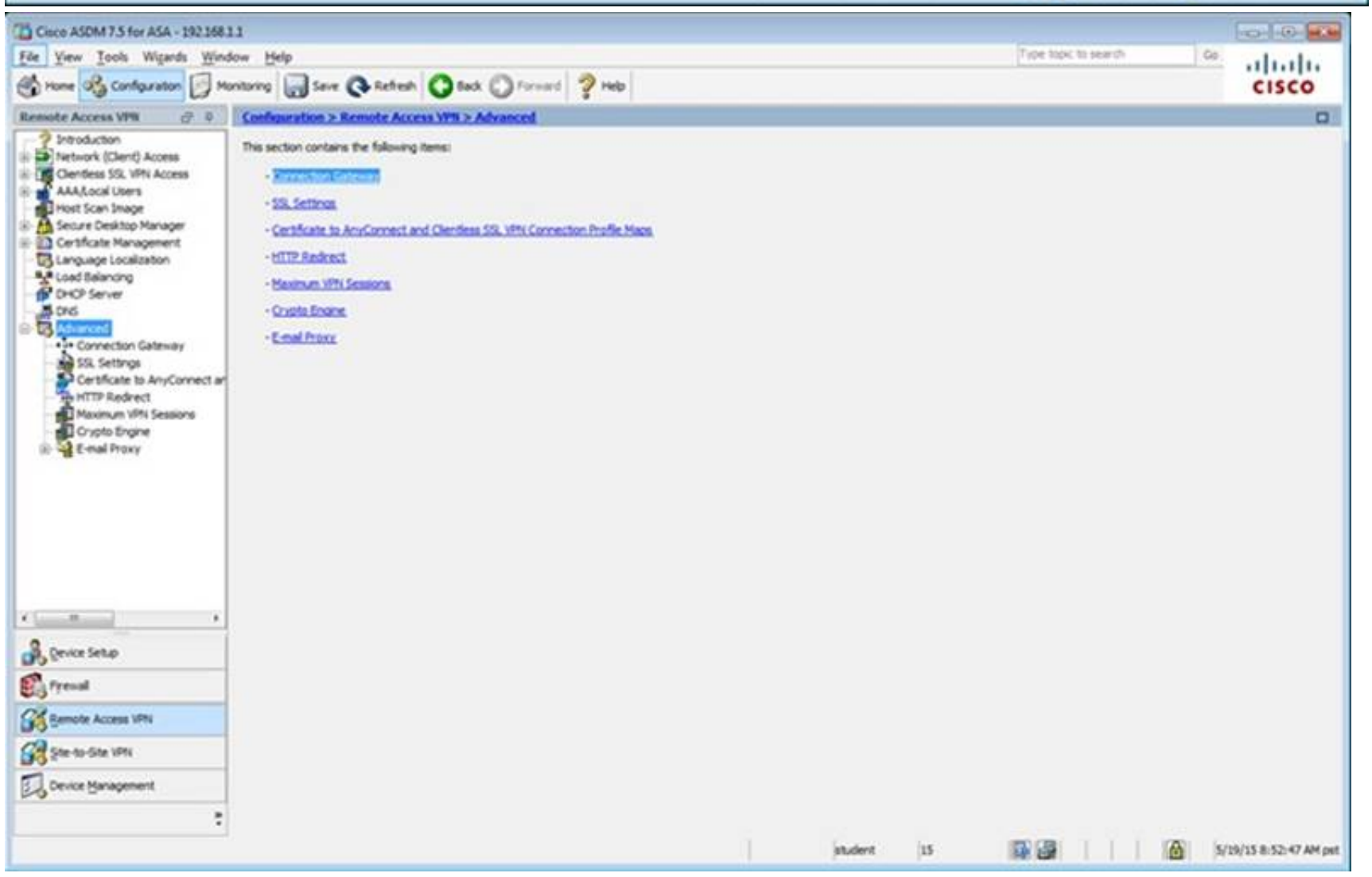

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless 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

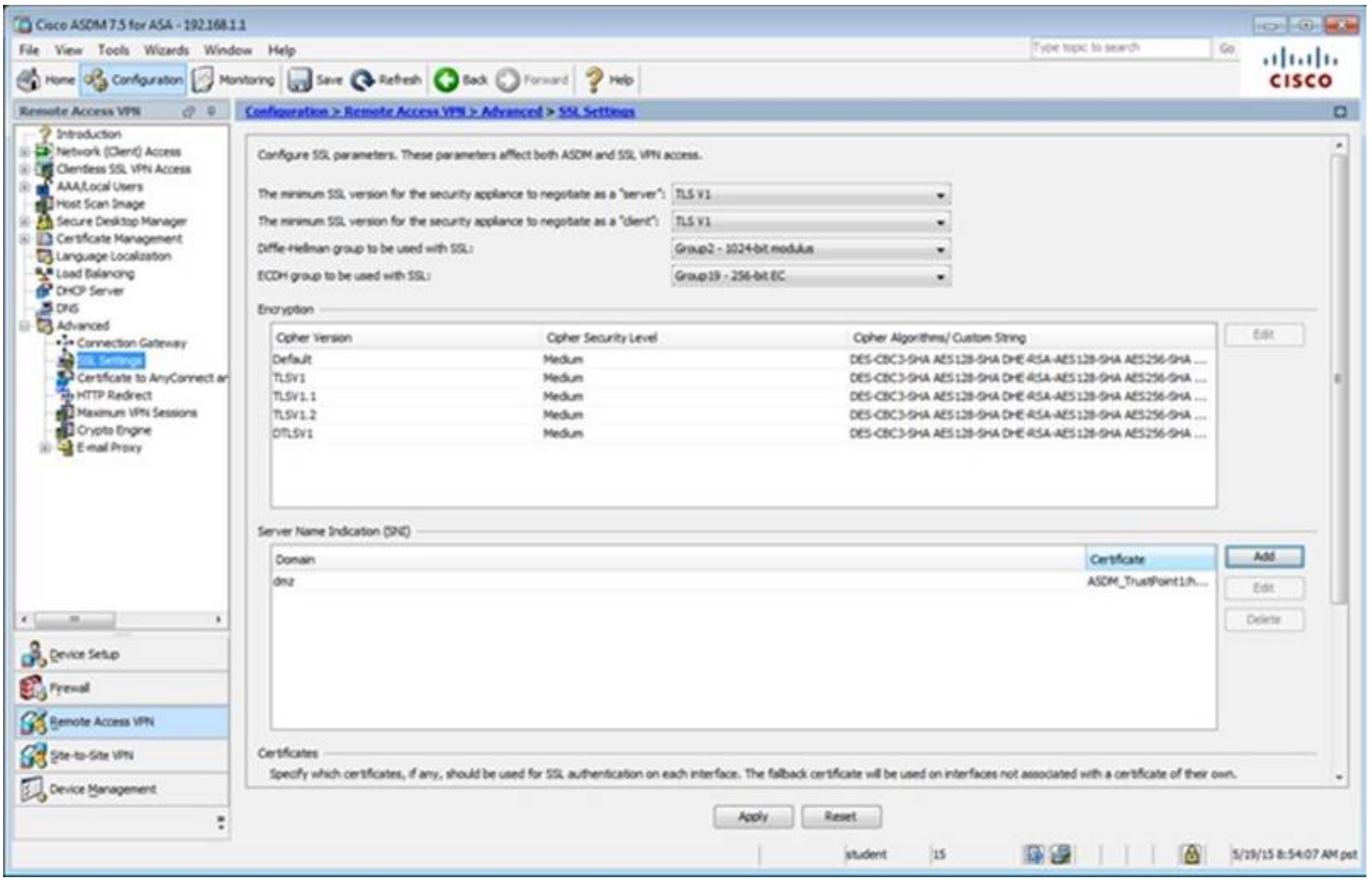

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

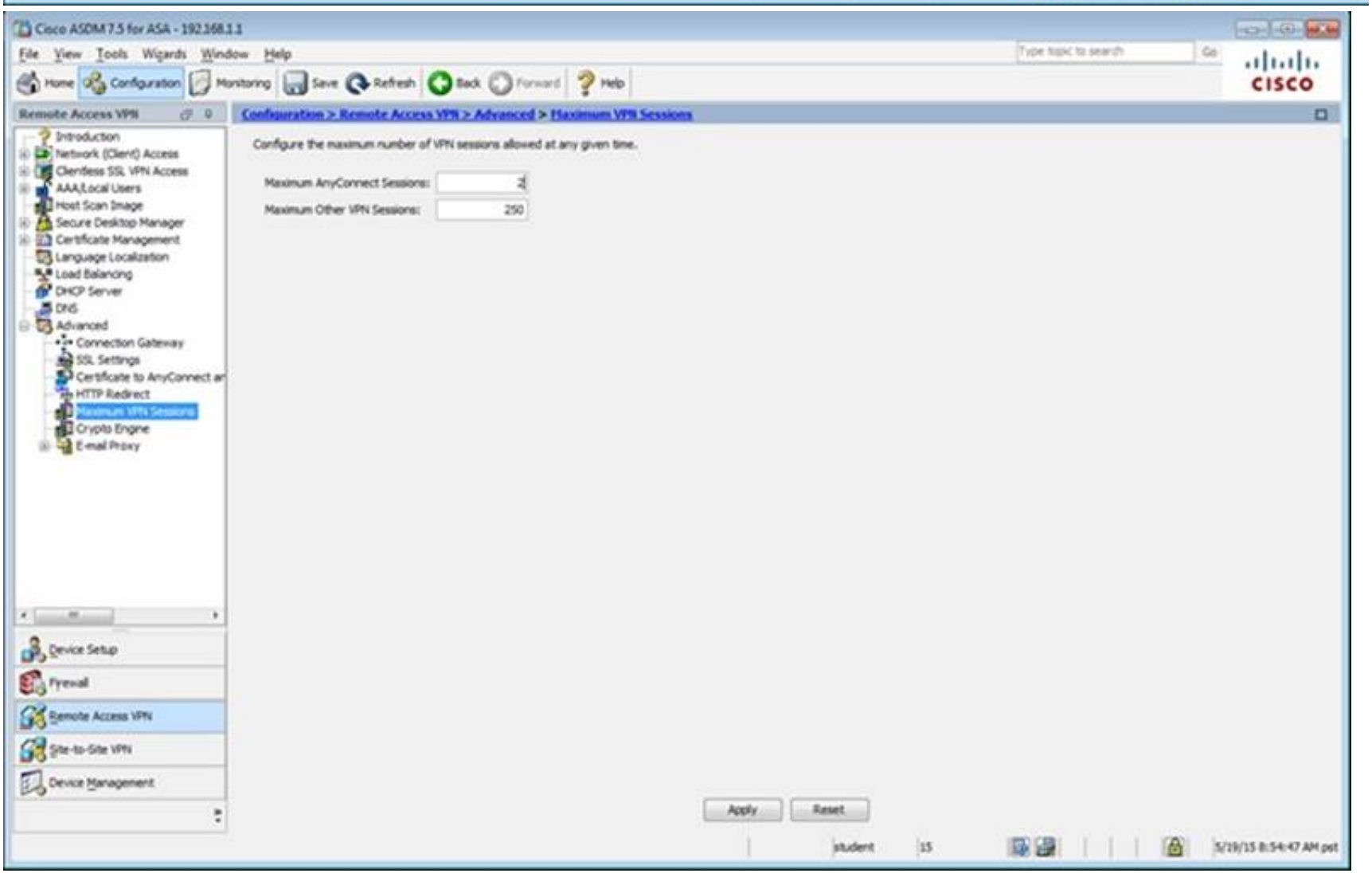

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Secure Desktop Manager (Version 3.5.2008.0)
Secure Desktop Manager lets you configure 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.
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
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

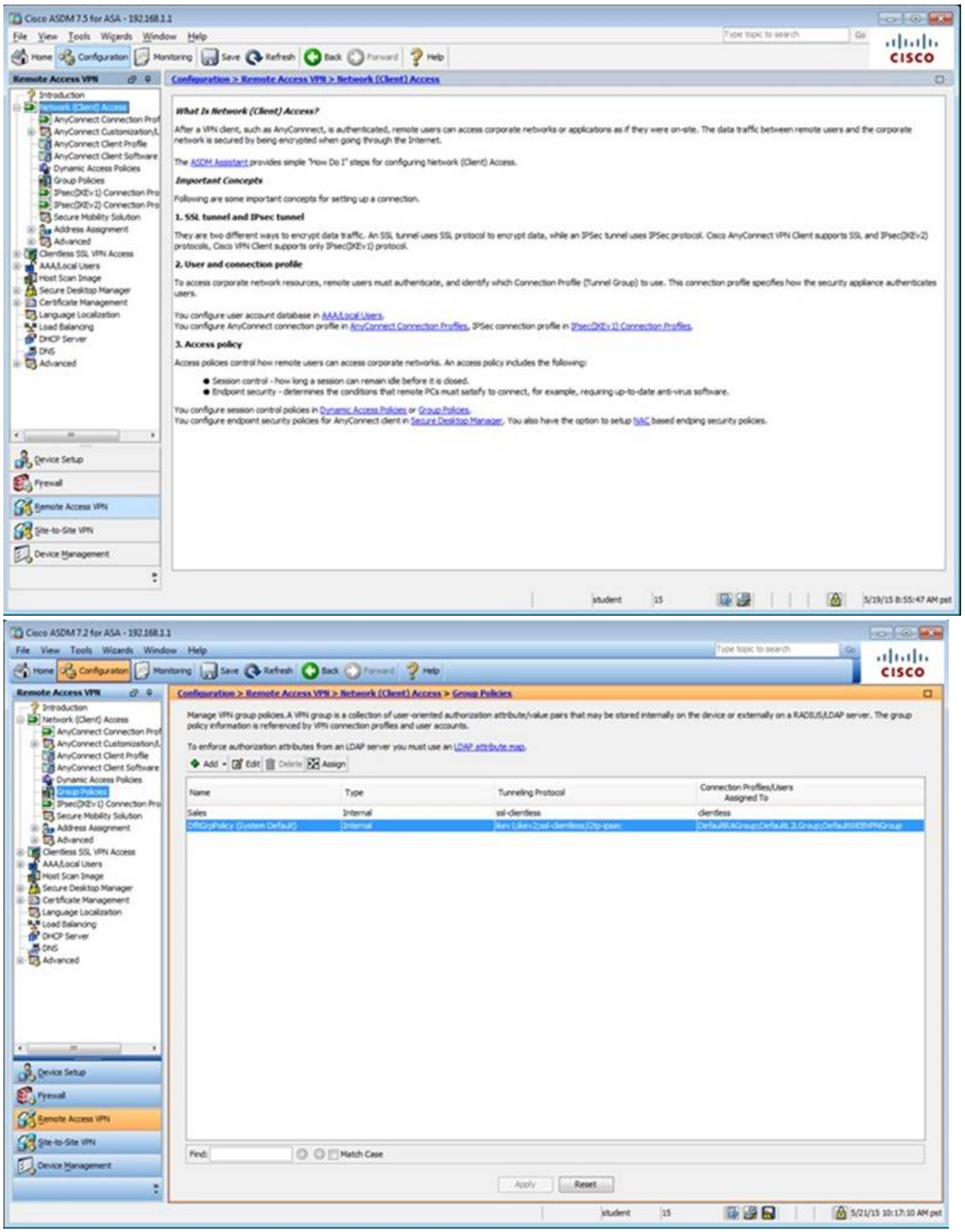

Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management
This section contains the following items:
- CA Certificates
- Identity Certificates
- Trusted Certificate Pool
- Code Signer
- Local Certificate Authority
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
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

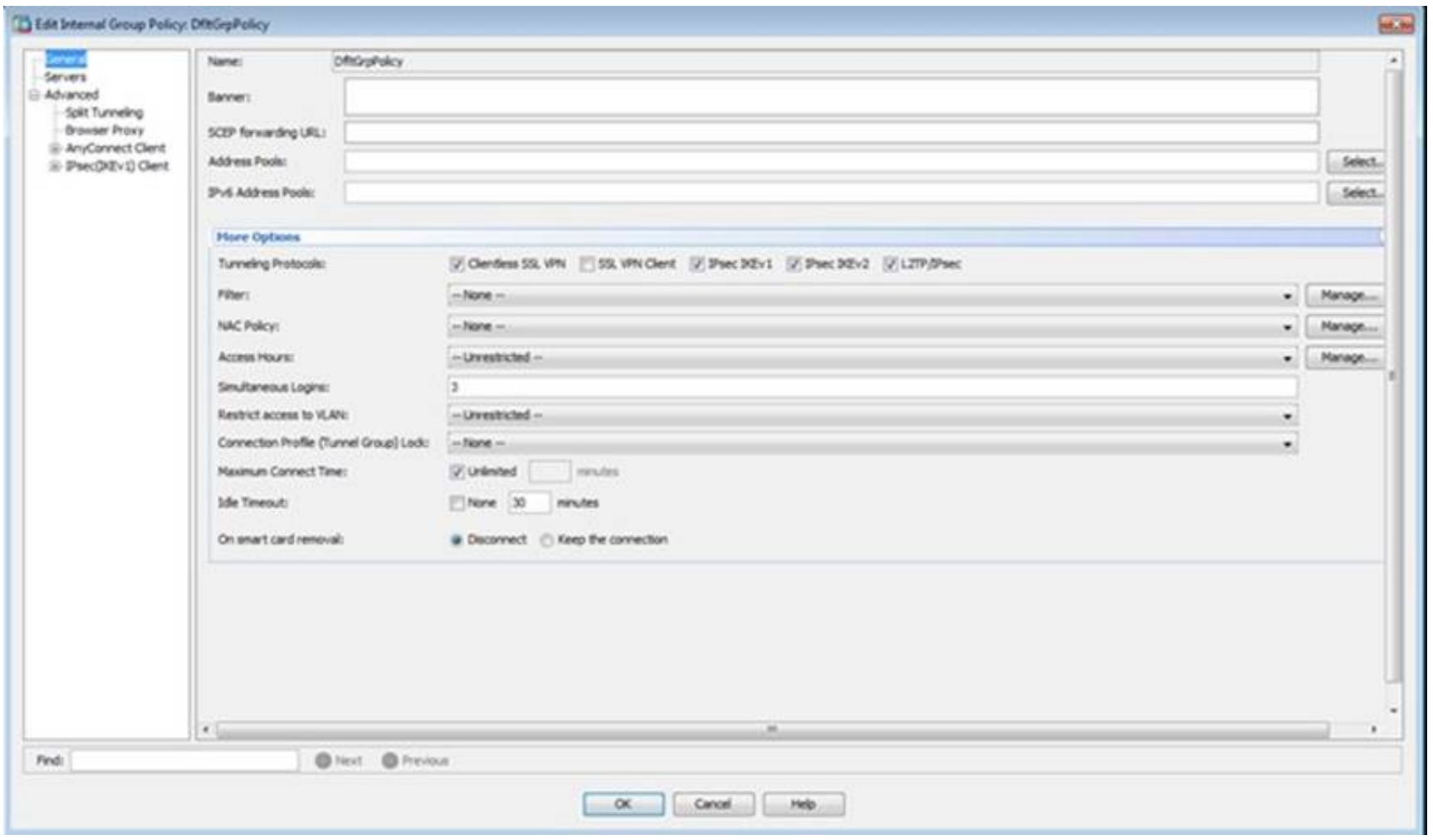

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- Connection Gateway
- SSL Settings
- Certificate to AnyConnect 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

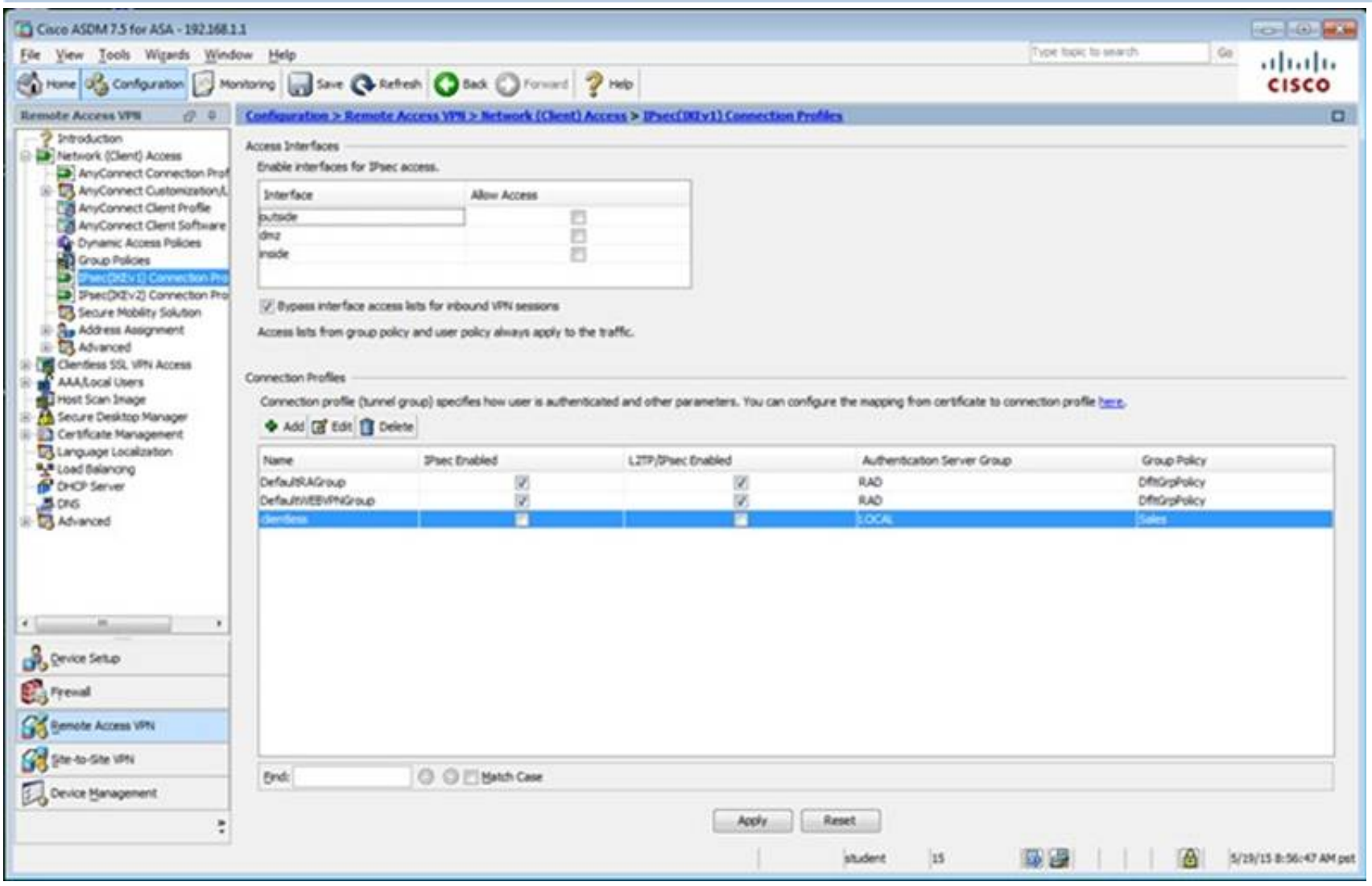

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host 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

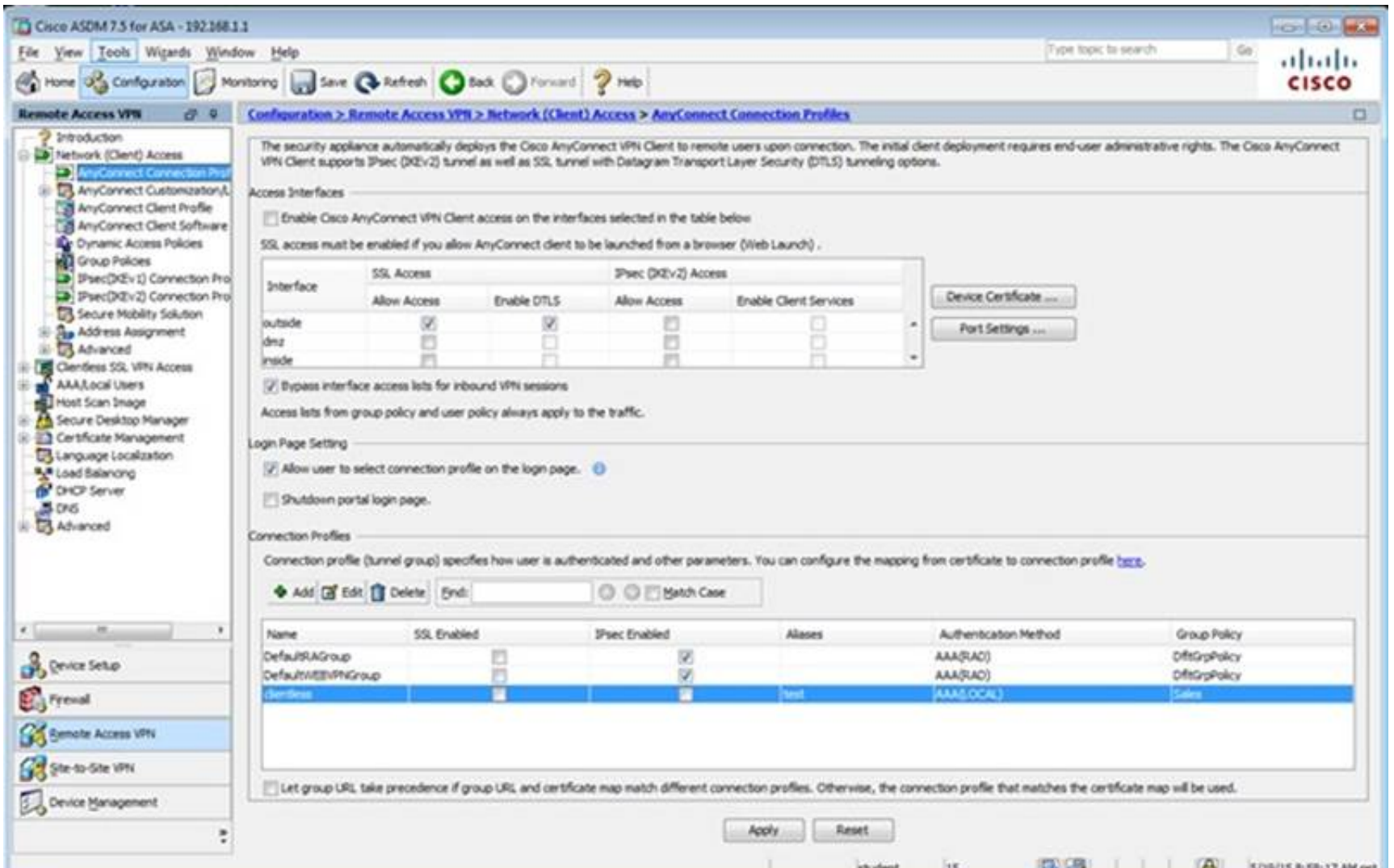

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
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: 3
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

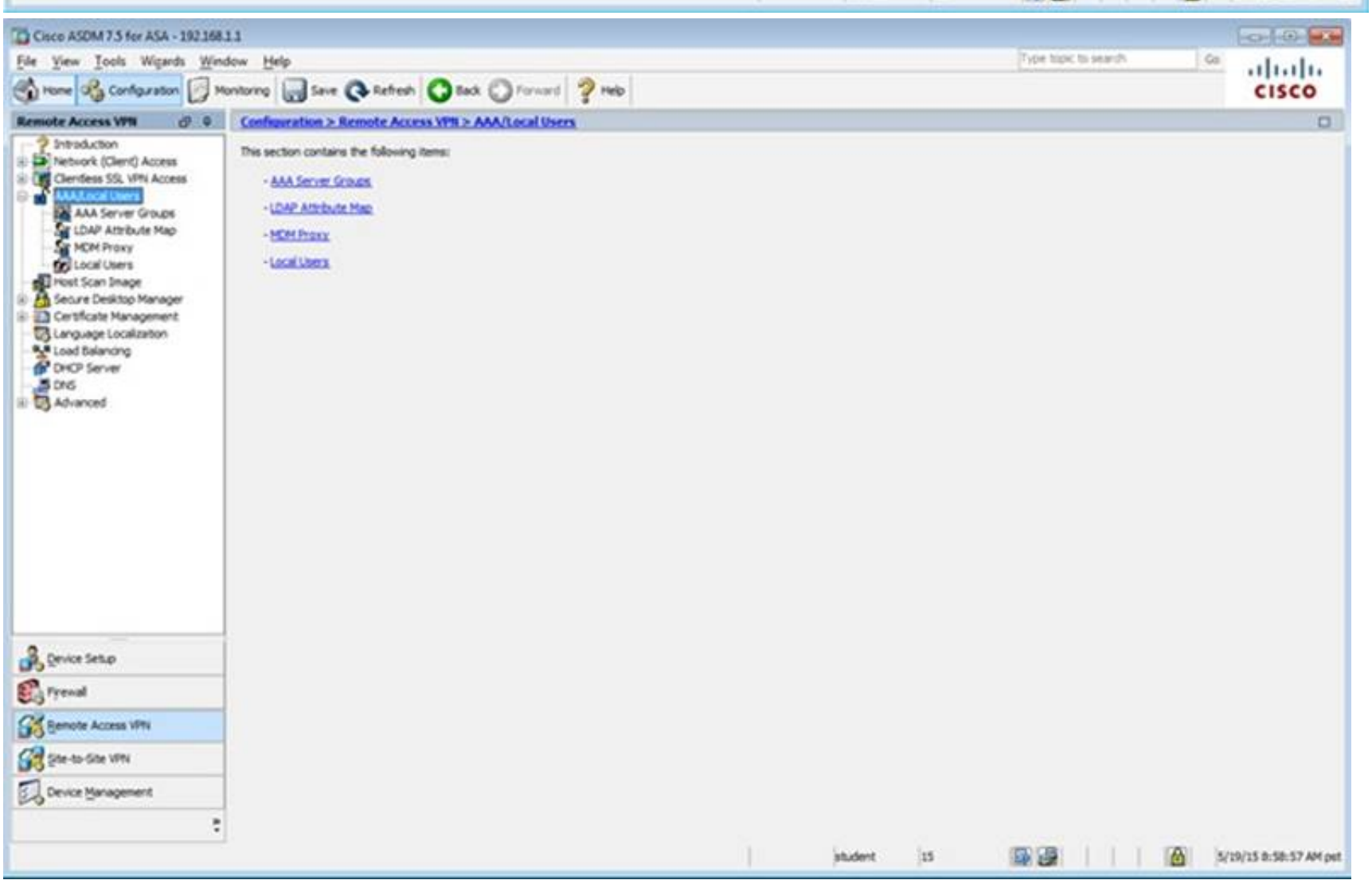

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
What Is Network (Client) Access?
After a VPN client, such as AnyConnect, is authenticated, 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 5/20/15 8:55:47 AM pst

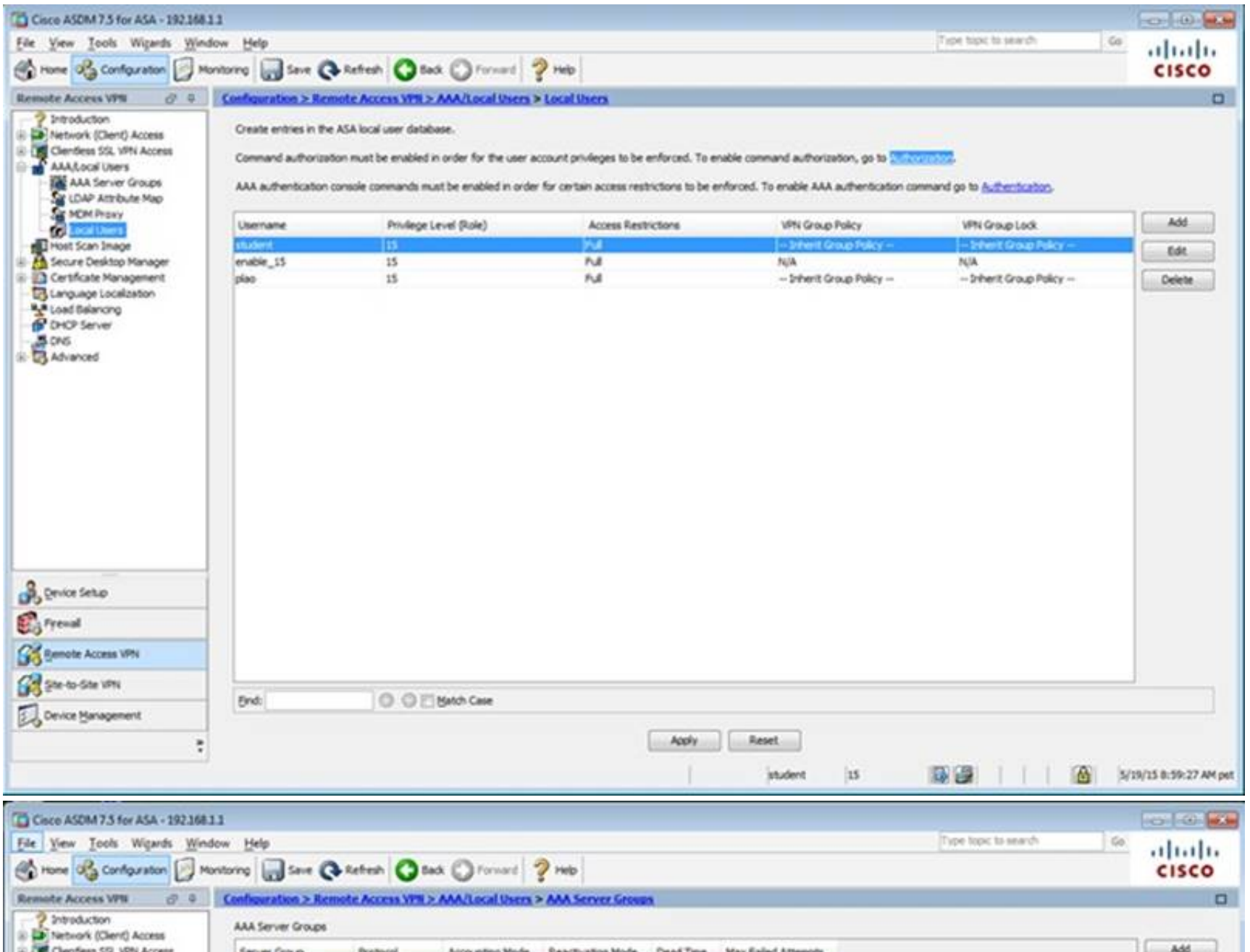
Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented 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
Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles
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
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
Access Interfaces
Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .
Interface
SSL Access
IPsec (IKEv2) Access
Allow Access
Enable DTLS
Allow Access
Enable Client Services
outside
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
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
Remote Access VPN
Configuration > Remote Access VPN > AAA/Local Users
This section contains the following items:
- AAA Server Groups
- LDAP Attribute Map
- MDM Proxy
- Local Users
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
5/19/15 8:58:57 AM pst

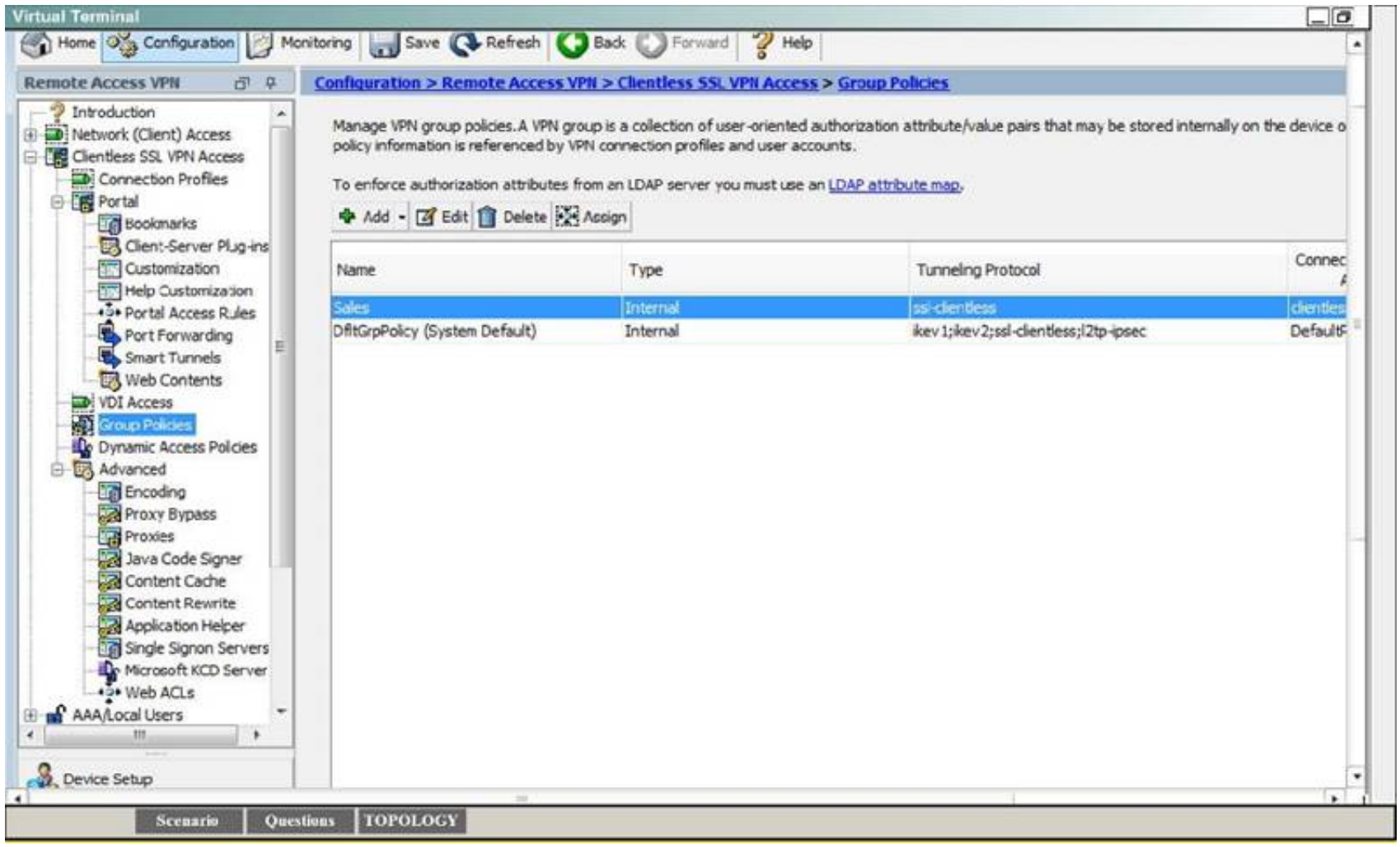


Which for tunneling protocols are enabled in the DfltGrpPolicy group policy? (Choose four)

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

Answer: ADEF

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



NEW QUESTION 81
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 tasks is the session management path responsible for? (Choose three.)

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

Answer: BDF

Explanation: The ASA has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the " session management path," and depending on the type of traffic, it might also pass through the "control plane path." The session management path is responsible for the following tasks:
+ Performing the access list checks
+ Performing route lookups
+ Allocating NAT translations (xlates)
+ Establishing sessions in the "fast path"
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/intro.html

NEW QUESTION 87
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 90
What is an advantage of implementing a Trusted Platform Module for disk encryption?

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

Answer: A

Explanation: Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
Software can use a Trusted Platform Module to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.
Source: https://en.wikipedia.org/wiki/Trusted_Platform_Module#Disk_encryption

NEW QUESTION 94
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 98
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 101
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 103
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 106
In what type of attack does an attacker virtually change a device's burned-in address in an attempt to circumvent access lists and mask the device's true identity?

A. gratuitous ARP
B. ARP poisoning
C. IP spoofing
D. MAC spoofing

Answer: D

Explanation: If a switch receives an inferior BPDU, nothing changes. Receiving a superior BPDU will kick off a reconvergence of the STP topology. So the rogue switch may become a root bridge.
Source:
http://www.networkpcworld.com/what-are-inferior-and-superior-bpdus-of-stp/

NEW QUESTION 109
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 113
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

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

Answer: ABC

Explanation: In promiscuous mode, packets do not flow through the sensor. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack.
Source:
http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/ cli_interfaces.html

NEW QUESTION 117
What is the most common Cisco Discovery Protocol version 1 attack?

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

Answer: A

Explanation: CDP contains information about the network device, such as the software version, IP address, platform, capabilities, and the native VLAN. When this information is available to an attacker computer, the attacker from that computer can use it to find exploits to attack your network, usually in the form of a Denial of Service (DoS) attack.
Source: https://howdoesinternetwork.com/2011/cdp-attack

NEW QUESTION 120
Which two statements about Telnet access to the ASA are true? (Choose two).

A. You may VPN to the lowest security interface to telnet to an inside interface.
B. You must configure an AAA server to enable Telnet.
C. You can access all interfaces on an ASA using Telnet.
D. You must use the command virtual telnet to enable Telnet.
E. Best practice is to disable Telnet and use SSH.

Answer: AE

Explanation: The ASA allows Telnet and SSH connections to the ASA for management purposes. You cannot use Telnet to the lowest security interface unless you use Telnet inside an IPSec tunnel.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/ access_management.html#wp1054101

NEW QUESTION 125
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 130
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 133
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 136
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 139
Which two services define cloud networks? (Choose two.)

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

Answer: AB

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

NEW QUESTION 144
Which address block is reserved for locally assigned unique local addresses?

A. 2002::/16
B. FD00::/8
C. 2001::/32
D. FB00::/8

Answer: B

Explanation: The address block fc00::/7 is divided into two /8 groups:
+ The block fc00::/8 has not been defined yet. It has been proposed to be managed by an allocation authority, but this has not gained acceptance in the IETF
+ The block fd00::/8 is defined for /48 prefixes, formed by setting the 40 least-significant bits of the prefix to a randomly generated bit string
Prefixes in the fd00::/8 range have similar properties as those of the IPv4 private address ranges:
+ They are not allocated by an address registry and may be used in networks by anyone without outside involvement.
+ They are not guaranteed to be globally unique.
+ Reverse Domain Name System (DNS) entries (under ip6.arpa) for fd00::/8 ULAs cannot be delegated in the global DNS.
Source: https://en.wikipedia.org/wiki/Unique_local_address

NEW QUESTION 147
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 151
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 154
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 156
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 157
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

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

Answer: AD

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

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

NEW QUESTION 160
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 161
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 162
According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 164
Which network device does NTP authenticate?

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

Answer: A

Explanation: You can configure the device to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.

Source:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/ configuration/guide/sm_nx_os_cg/sm_3ntp.html#wp1100303%0A

NEW QUESTION 166
What type of algorithm uses the same key to encrypt and decrypt data?

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

Answer: A

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

NEW QUESTION 167
Which option is the most effective placement of an IPS device within the infrastructure?

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

Answer: A

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

NEW QUESTION 169
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 173
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 175
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 179
What is a reason for an organization to deploy a personal firewall?

A. To protect endpoints such as desktops from malicious activity.
B. To protect one virtual network segment from another.
C. To determine whether a host meets minimum security posture requirements.
D. To create a separate, non-persistent virtual environment that can be destroyed after a session.
E. To protect the network from DoS and syn-flood attacks.

Answer: A

Explanation: The term personal firewall typically applies to basic software that can control Layer 3 and Layer 4 access to client machines. HIPS provides several features that offer more robust security than a traditional personal firewall, such as host intrusion prevention and protection against spyware, viruses, worms, Trojans, and other types of malware.
Source: Cisco Official Certification Guide, Personal Firewalls and Host Intrusion Prevention Systems , p.499

NEW QUESTION 182
Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

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

Answer: CEF

Explanation: The ASA supports the following authentication methods with RADIUS servers:
+ PAP -- For all connection types.
+ CHAP and MS-CHAPv1 -- For L2TP-over-IPsec connections.
+ MS-CHAPv2 - For L2TP-over-IPsec connections
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/ aaa_radius.pdf

NEW QUESTION 183
Which Cisco product can help mitigate web-based attacks within a network?

A. Adaptive Security Appliance
B. Web Security Appliance
C. Email Security Appliance
D. Identity Services Engine

Answer: B

Explanation: Web-based threats continue to rise. To protect your network you need a solution that prevents them. Cisco Advanced Malware Protection (AMP) for Web Security goes beyond the basics in threat detection, URL filtering, and application control. It provides continuous file analysis, retrospective security, and sandboxing to help your security team catch even the stealthiest threats.
Source:
http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/amp-for-web- security.html

NEW QUESTION 187
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 190
Which source port does IKE use when NAT has been detected between two VPN gateways?

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

Answer: C

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

NEW QUESTION 194
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 198
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 201
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

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

Answer: A

Explanation: Deny connection inline: This action terminates the packet that triggered the action and future packets that are part of the same TCP connection. The attacker could open up a new TCP session (using different port numbers), which could still be permitted through the inline IPS.
Available only if the sensor is configured as an IPS.
Source: Cisco Official Certification Guide, Table 17-4 Possible Sensor Responses to Detected Attacks, p.465

NEW QUESTION 202
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 204
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 208
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 209
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 210
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 213
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 215
Which feature filters CoPP packets?

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

Answer: A

NEW QUESTION 220
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 222
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 224

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 227
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 230
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 235
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 239
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 242
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 247
How does PEAP protect the EAP exchange?

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

Answer: A

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

NEW QUESTION 249
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 253

Refer to the exhibit.

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

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

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

Answer: A

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

NEW QUESTION 254
How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?

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

Answer: C

NEW QUESTION 258
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 261
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 263
Which Sourcefire event action should you choose if you want to block only malicious traffic from a particular end user?

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

Answer: A

Explanation: A file policy is a set of configurations that the system uses to perform advanced malware protection and file control, as part of your overall access control configuration.

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

NEW QUESTION 268
Which statement about the communication between interfaces on the same security level is true?

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

Answer: A

Explanation: By default, if two interfaces are both at the exact same security level, traffic is not allowed between those two interfaces.
To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the same-security-traffic command in global configuration mode.
#same-security-traffic
permit {inter-interface | intra-interface} Source: Cisco Official Certification Guide, The Default Flow of Traffic, p.422
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command

NEW QUESTION 270
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 271
Which three statements describe DHCP spoofing attacks? (Choose three.)

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

Answer: ABC

Explanation: DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
Source: https://learningnetwork.cisco.com/thread/67229 https://learningnetwork.cisco.com/docs/DOC-24355
Also when i took the exam, it asked me for only 2 options. AB is correct

NEW QUESTION 274
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 275
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 277
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 278
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 282
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 285
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 289
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 292
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 293
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 295
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 297
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 300
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 303
What improvement does EAP-FASTv2 provide over EAP-FAST?

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

Answer: A

Explanation: As an enhancement to EAP-FAST, a differentiation was made to have a User PAC and a Machine PAC. After a successful machine-authentication, ISE will issue a Machine-PAC to the client. Then, when processing a user- authentication, ISE will request the Machine-PAC to prove that the machine was successfully authenticated, too. This is the first time in 802.1X history that multiple credentials have been able to be authenticated within a single EAP transaction, and it is known as "EAP Chaining".
Source:
http://www.networkworld.com/article/2223672/access-control/which-eap-types-do-you-need-for-which- identity-projects.html

NEW QUESTION 307
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 311
In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch acts as a hub?

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

Answer: C

Explanation: MAC address flooding is an attack technique used to exploit the memory and hardware limitations in a switch's CAM table.
Source:
http://hakipedia.com/index.php/CAM_Table_Overflow

NEW QUESTION 315
What are the primary attack methods of VLAN hopping? (Choose two.)

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

Answer: BD

Explanation: VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.
+ In a switch spoofing attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host.
+ In a double tagging attack, an attacking host connected on a 802.1q interface prepends two VLAN tags to packets that it transmits.
Source: https://en.wikipedia.org/wiki/VLAN_hopping

NEW QUESTION 316
How does a device on a network using ISE receive its digital certificate during the new-device registration process?

A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server.
B. ISE issues a certificate from its internal CA server.
C. ISE issues a pre-defined certificate from a local database.
D. The device requests a new certificate directly from a central CA.

Answer: A

Explanation: SCEP Profile Configuration on ISE
Within this design, ISE is acting as a Simple Certificate Enrollment Protocol (SCEP) proxy server, thereby allowing mobile clients to obtain their digital certificates from the CA server. This important feature of ISE allows all endpoints, such as iOS, Android, Windows, and MAC, to obtain digital certificates through the ISE. This feature combined with the initial registration process greatly simplifies the provisioning of digital certificates on endpoints.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/ BYOD_Design_Guide/BYOD_ISE.html

NEW QUESTION 317
In which stage of an attack does the attacker discover devices on a target network?

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

Answer: A

Explanation: Reconnaissance: This is the discovery process used to find information about the network. It could include scans of the network to find out which IP addresses respond, and further scans to see which ports on the devices at these IP addresses are open. This is usually the first step taken, to discover what is on the network and to determine potential vulnerabilities.
Source: Cisco Official Certification Guide, Table 1-5 Attack Methods, p.13

NEW QUESTION 322
How can FirePOWER block malicious email attachments?

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

Answer: C

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

NEW QUESTION 324
Which of the following statements about access lists are true? (Choose three.)

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

Answer: BCE

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

Topic 3, Exam Pool C

NEW QUESTION 329
Which ports must be open between a AAA server and a Microsoft server to permit active directory authentication?

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

Answer: A

NEW QUESTION 330
What is the highest security level can be applied to an ASA interface?

A. 50
B. 100
C. 200

Answer: C

NEW QUESTION 335
What does the command crypto isakmp nat-traversal do?

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

Answer: A

NEW QUESTION 338

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

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

Answer: D

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

NEW QUESTION 341
Which of the following pairs of statements is true in terms of configuring MD authentication?

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

Answer: C

NEW QUESTION 344
Which line in the following OSPF configuration will not be required for MD5 authentication to work?

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

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

Answer: C

NEW QUESTION 349
Which two features of Cisco Web Reputation tracking can mitigate web-based threats? (Choose Two)

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

Answer: AD

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

NEW QUESTION 351
Which two statements about the self zone on Cisco zone based policy firewall are true ? (Choose two)

A. multiple interfaces can be assigned to the self zone .
B. traffic entering the self zone must match a rule.

C. zone pairs that include the self zone apply to traffic transiting the device.
D. it can be either the source zone or destination zone .
E. it supports statefull inspection for multicast traffic

Answer: AD

NEW QUESTION 354
When setting up a site-to-site VPN with PSK authentication on a Cisco router, which two elements must be configured under crypto map? (Choose two.)

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

Answer: BD

NEW QUESTION 357
Within an 802.1X enabled network with the Auth Fail feature configured, when does a switch port get placed into a restricted VLAN?

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

Answer: C

NEW QUESTION 360
What port option in a PVLAN that can communicate with every other port?

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

Answer: A

Explanation: + Promiscuous -- A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN.
+ Isolated -- An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports
+Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports Source: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html

NEW QUESTION 362
Referencing the CIA model, in which scenario is a hash-only function most appropriate?

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

Answer: A

NEW QUESTION 364
Which type of encryption technology has the broadcast platform support?

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

Answer: C

NEW QUESTION 369
What encryption technology has broadest platform support

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

Answer: C

NEW QUESTION 370
With which technology do apply integrity, confidentially and authenticate the source

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

Answer: A

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

NEW QUESTION 373
What is example of social engineering

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

Answer: C

NEW QUESTION 376
SSL certificates are issued by Certificate Authority(CA) are?

A. Trusted root
B. Not trusted

Answer: A

NEW QUESTION 377
Which two actions can a zone based firewall take when looking at traffic? (Choose two)

A. Filter
B. Forward
C. Drop
D. Broadcast
E. Inspect

Answer: CE

NEW QUESTION 380
If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

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

Answer: A

NEW QUESTION 385
When is the default deny all policy an exception in zone-based firewalls?

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

Answer: A

NEW QUESTION 390
What feature defines a campus area network?

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

Answer: A

NEW QUESTION 395
When is "Deny all" policy an exception in Zone Based Firewall

A. traffic traverses 2 interfaces in same zone
B. traffic sources from router via self zone
C. traffic terminates on router via self zone
D. traffic traverses 2 interfaces in different zones
E. traffic terminates on router via self zone

Answer: A

Explanation: + There is a default zone, called the self zone, which is a logical zone. For any packets directed to the router directly (the destination IP represents the packet is for the router), the router automatically considers that traffic to be entering the self zone. In addition, any traffic initiated by the router is considered as leaving the self zone.
By default, any traffic to or from the self zone is allowed, but you can change this policy.
+ For the rest of the administrator-created zones, no traffic is allowed between interfaces in different zones.
+ 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 400
Which command is used to verify a VPN connection is operational?

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

Answer: A

Explanation: #show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see
#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
which means packets are encrypted and decrypted by the IPsec peer.
Source:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ipsec_sa

NEW QUESTION 403
Which command do you enter to verify that a VPN connection is established between two endpoints and that the connection is passing traffic?

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

Answer: A

NEW QUESTION 408
Refer to the exhibit.

```
Router#show crypto ipsec sa
interface: FastEthernet0
Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
protected vrf: (none)
   local ident (addr/mask/prot/port): (10.40.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.50.30.0/255.255.255.0/0/0)
   current_peer 192.168.1.1 port 500
   PERMIT, flags={origin_is_acl,}

   #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

For which reason is the tunnel unable to pass traffic?

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

Answer: C

NEW QUESTION 411
Which type of attack is directed against the network directly:

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

Answer: A

Explanation: Denial of service refers to willful attempts to disrupt legitimate users from getting access to the resources they intend to. Although no complete solution exists, administrators can do specific things to protect the network from a DoS attack and to lessen its effects and prevent a would-be attacker from using a system as a source of an attack directed at other systems. These mitigation techniques include filtering based on bogus source IP addresses trying to come into the networks and vice versa. Unicast reverse path verification is one way to assist with this, as are access lists. Unicast reverse path verification looks at the source IP address as it comes into an interface, and then looks at the routing table. If the source address seen would not be reachable out of the same interface it is coming in on, the packet is considered bad, potentially spoofed, and is dropped.
Source: Cisco Official Certification Guide, Best Practices Common to Both IPv4 and IPv6, p.332

NEW QUESTION 413
In which configuration mode do you configure the ip ospf authentication-key 1 command?

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

Answer: A

Explanation: ip ospf authentication-key is used under interface configuration mode, so it's in interface level, under global configuration mode. If it asks about interface level then choose that.
interface Serial0
ip address 192.16.64.1 255.255.255.0
ip ospf authentication-key c1$c0

NEW QUESTION 414
Which type of layer 2 attack enables the attacker to intercept traffic that is intended for one specific recipient?

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

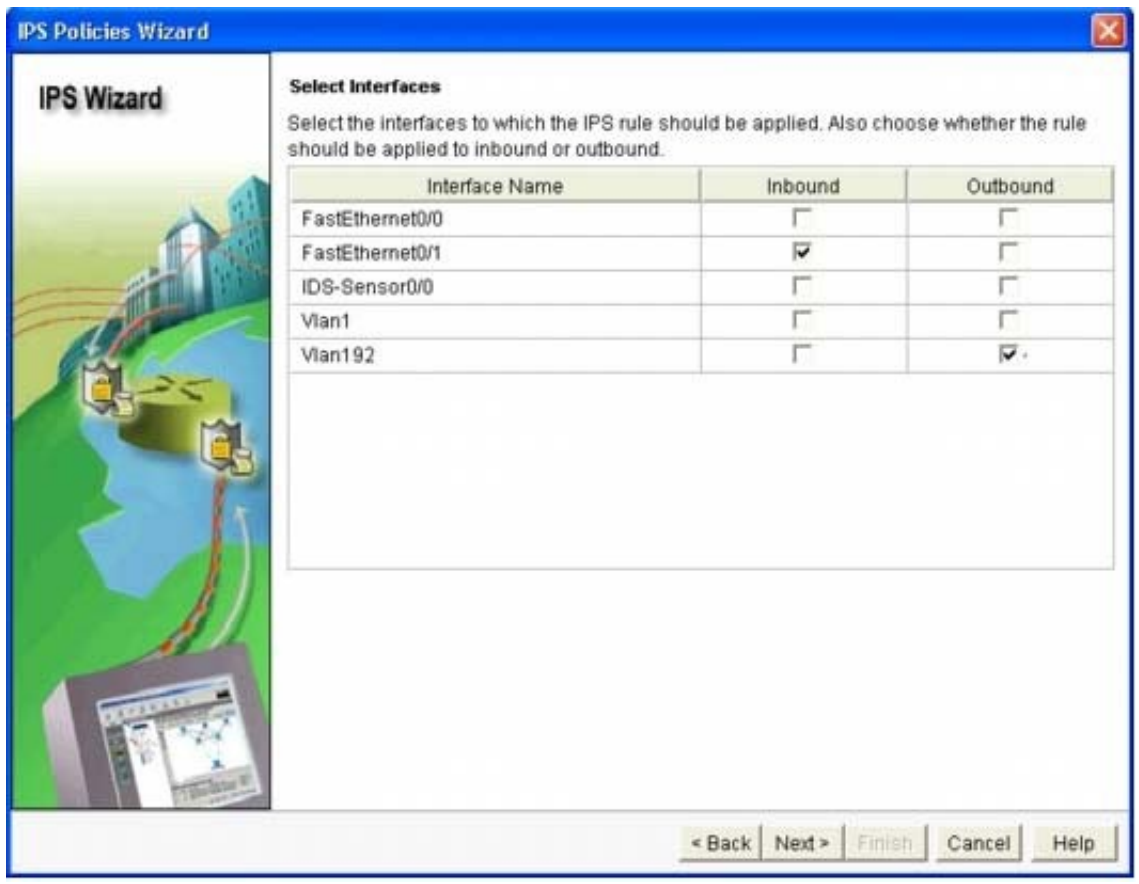
Answer: D

NEW QUESTION 418
Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

A. Select the interface(s) to apply the IPS rule.
B. Select the traffic flow direction that should be applied by the IPS rule.
C. Add or remove IPS alerts actions based on the risk rating.
D. Specify the signature file and the Cisco public key.
E. Select the IPS bypass mode (fail-open or fail-close).
F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

Answer: ABDF

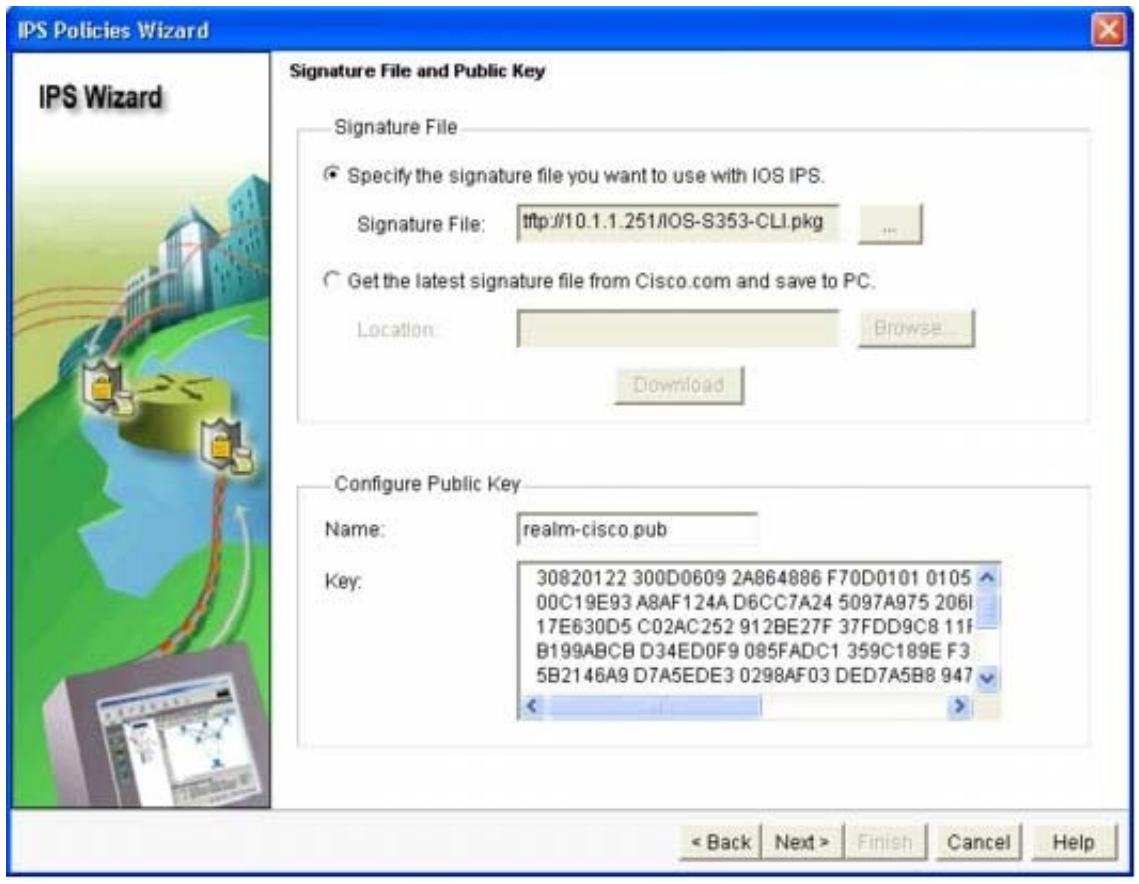
Explanation: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html
Step 11. At the `Select Interfaces' screen, select the interface and the direction that IOS IPS will be applied to, then click `Next' to continue.



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

Step 13. In the `Configure Public Key' section, enter `realm-cisco.pub' in the `Name' text field, then copy and paste the following public key's key-string in the `Key' text field. This public key can be downloaded from Cisco.com at: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. Click `Next ' to continue.

30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128 B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624
7E0764BF 3E53053E 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87 89BCB7BB 994AE74C
FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3 F3020301 0001



NEW QUESTION 422
What data is transferred during DH for making public and private key?

A. Random prime Integer
B. Encrypted data transfer
C. Prime integer
D. Random number

Answer: A

NEW QUESTION 426
Which command should be used to enable AAA authentication to determine if a user can access the privilege command level?

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

Answer: B

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

NEW QUESTION 429
Which security term refers to a person, property, or data of value to a company?

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

Answer: B

NEW QUESTION 433
Which two characteristics of symmetric encryption are true? (Choose two)

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

Answer: BE

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

NEW QUESTION 438
The purpose of the RSA SecureID server/application is to provide what?

A. Authentication, authorization, accounting (AAA) functions
B. One-time password (OTP) capabilities
C. 802.1X enforcement
D. VPN access

Answer: B

NEW QUESTION 443
SYN flood attack is a form of ?

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

Answer: A

Explanation: A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
Source: https://en.wikipedia.org/wiki/SYN_flood

NEW QUESTION 447
Refer to the exhibit.

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

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

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

Answer: BE

Explanation: 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 449
With which preprocesor do you detect incomplete TCP handshakes

A. rate based prevention
B. portscan detection

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.
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 453
What command could you implement in the firewall to conceal internal IP address?

A. no source-route
B. no cdp run
C. no broadcast…
D. no proxy-arp

Answer: D

Explanation: The Cisco IOS software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender,

and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data-link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is enabled by default.
Router(config-if)# ip proxy-arp - Enables proxy ARP on the interface.
Source:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001233

NEW QUESTION 457
Which IDS/IPS is used for monitoring system?

A. HIPS
B. WIPS
C. visibility tool

Answer: A

NEW QUESTION 459
Which cisco IOS device support firewall, antispyware, anti-phishing, protection, etc.

A. Cisco IOS router
B. Cisco 4100 IOS IPS appliance
C. Cicso 5500 series ASA
D. Cisco 5500x next generation ASA

Answer: D

NEW QUESTION 463
Which label is given to a person who uses existing computer scripts to hack into computers lacking the expertise to write their own?

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

Answer: D

NEW QUESTION 465
What are characteristics of the Radius Protocol? choose Two

A. Uses TCP port 49
B. Uses UDP Port 49
C. Uses TCP 1812/1813
D. Uses UDP 1812/1813
E. Comines authentication and authorization

Answer: DE

NEW QUESTION 468
What is true about the Cisco IOS Resilient Configuration feature?

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

Answer: C

Explanation: The following factors were considered in the design of Cisco IOS Resilient Configuration:
+ The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
+ The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
+ The feature automatically detects image or configuration version mismatch .
+ Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
+ The feature can be disabled only through a console session Source: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt- book/sec-resil-config.html

NEW QUESTION 469
What show command can see vpn tunnel establish with traffic passing through.

A. show crypto ipsec sa
B. show crypto session
C. show crypto isakmp sa
D. show crypto ipsec transform-set

Answer: A

Explanation:

#show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see
#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
which means packets are encrypted and decrypted by the IPsec peer.
Source:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec- debug-00.html#ipsec_sa

NEW QUESTION 474
Which type of attack can exploit design flaws in the implementation of an application without going noticed?

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

Answer: D

NEW QUESTION 478
The first layer of defense which provides real-time preventive solutions against malicious traffic is provided by?

A. Banyan Filters
B. Explicit Filters
C. Outbreak Filters

Answer: C

NEW QUESTION 482
Security well known terms Choose 2

A. Trojan
B. Phishing
C. Something LC
D. Ransomware

Answer: BD

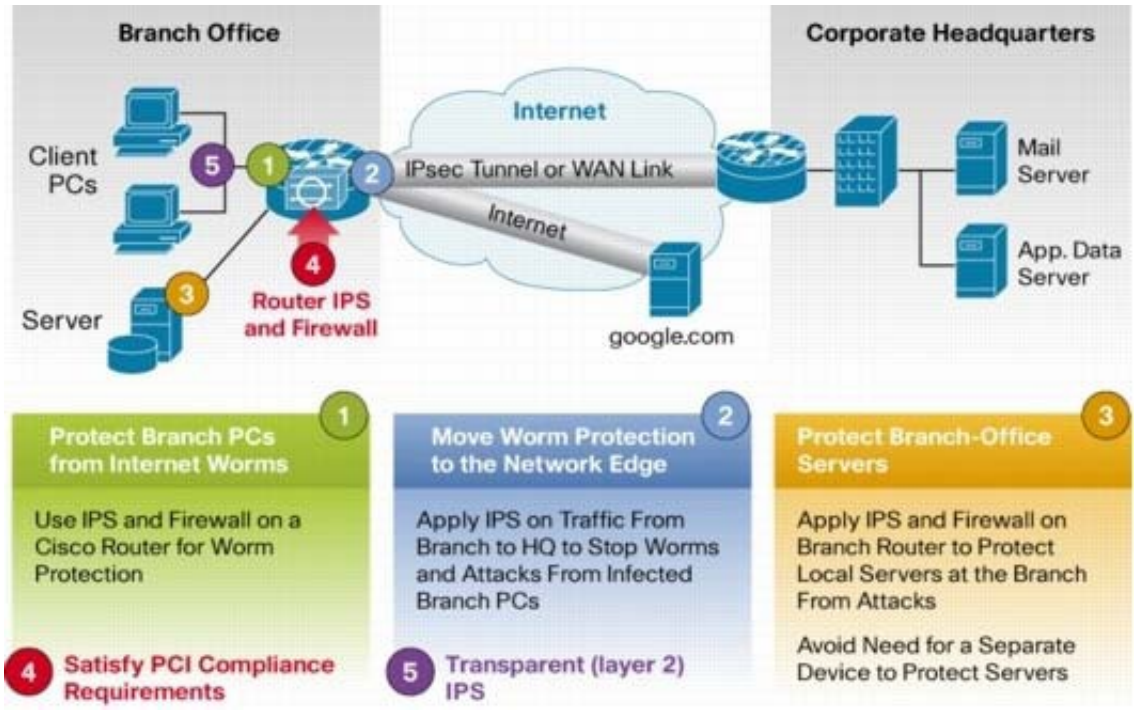
Explanation: The following are the most common types of malicious software:
+ Computer viruses
+ Worms
+ Mailers and mass-mailer worms
+ Logic bombs
+ Trojan horses
+ Back doors
+ Exploits
+ Downloaders
+ Spammers
+ Key loggers
+ Rootkits
+ Ransomware

NEW QUESTION 484
Which statement is a benefit of using Cisco IOS IPS?

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

Answer: A

Explanation: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd80313 Product Overview
In today's business environment, network intruders and attackers can come from outside or inside the network.
They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses.
Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.
Cisco IOS IPS: Major Use Cases and Key Benefits IOS IPS helps to protect your network in 5 ways:



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

NEW QUESTION 486
Which product can be used to provide application layer protection for TCP port 25 traffic?

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

Answer: A

NEW QUESTION 487
Which type of PVLAN port allows a host in the same VLAN to communicate only with promiscuous hosts?

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

Answer: B

Explanation: The types of private VLAN ports are as follows:
+ Promiscuous - The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN
+ Isolated - This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
+ Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.
Source:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/ CLIConfigurationGuide/PrivateVLANs.html#42874

NEW QUESTION 491
What IPSec mode is used to encrypt traffic between a server and VPN endpoint?

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

Answer: E

Explanation: @Tullipp on securitytut.com commented:
"the IPSEC Mode question did come up. It has been been very badly worded in the dumps and I knew It cant be right.
The question that comes in the exam is "between client and server vpn endpoints".
So the keyword here is vpn endpoints. Not the end points like its worded in the dumps. So the answer is transport mode."
+ 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 495
which are two valid TCP connection states (pick 2) is the gist of the question.

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

Answer: AB

Explanation: TCP Finite State Machine (FSM) States, Events and Transitions + CLOSED: This is the default state that each connection starts in before the process of establishing it begins.
The state is called "fictional" in the standard.
+ LISTEN
+ SYN-SENT
+ SYN-RECEIVED: The device has both received a SYN (connection request) from its partner and sent its own SYN. It is now waiting for an ACK to its SYN to finish connection setup.
+ ESTABLISHED
+ CLOSE-WAIT
+ LAST-ACK
+ FIN-WAIT-1
+ FIN-WAIT-2
+ CLOSING
+ TIME-WAIT
Source:
http://tcpipguide.com/free/t_TCPOperationalOverviewandtheTCPFiniteStateMachineF-2.htm

NEW QUESTION 496
Which is not a function of mobile device management (MDM)?

A. Enforce strong passwords on BYOD devices
B. Deploy software updates to BYOD devices
C. Remotely wipe data from BYOD devices
D. Enforce data encryption requirements on BYOD devices

Answer: B

NEW QUESTION 499
Which statement about an ASA in transparent mode is true?

A. It requires a management IP address.
B. It allows the use of dynamic NAT.
C. It supports OSPF
D. It requires an IP address for each interface.

Answer: A

NEW QUESTION 502
Diffie-Hellman key exchange question

A. IKE
B. IPSEC
C. SPAN
D. STP

Answer: A

NEW QUESTION 507
Which of the following are IKE modes? (choose all and apply)

A. Main Mode
B. Fast Mode
C. Aggressive Mode
D. Quick Mode
E. Diffie-Hellman Mode

Answer: ACD

Explanation: https://supportforums.cisco.com/t5/security-documents/main-mode-vs-aggressive-mode/ta-p/3123382
Main Mode - An IKE session begins with the initiator sending a proposal or proposals to the responder. The proposals define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced, for example. Multiple proposals can be sent in one offering. The first exchange between nodes establishes the basic security policy; the initiator proposes the encryption and authentication algorithms it is willing to use. The responder chooses the appropriate proposal (we'll assume a proposal is chosen) and sends it to the initiator. The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA. The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.
Aggressive Mode - Aggressive Mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator. The responder sends the proposal, key material and ID, and authenticates the session in the next packet. The initiator replies by authenticating the session. Negotiation is quicker, and the initiator and responder ID pass in the clear.
Quick Mode - IPSec negotiation, or Quick Mode, is similar to an Aggressive Mode IKE negotiation, except negotiation must be protected within an IKE SA. Quick Mode negotiates the SA for the data encryption and manages the key exchange for that IPSec SA.

NEW QUESTION 510
Which two characteristics apply to an Intrusion Prevention System (IPS) ? Choose two

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

Answer: BC

Explanation: + Position in the network flow: Directly inline with the flow of network traffic and every packet goes through the sensor on its way through the network.
+ Mode: Inline mode
+ The IPS can drop the packet on its own because it is inline. The IPS can also request assistance from another device to block future packets just as the IDS does.
Source: Cisco Official Certification Guide, Table 17-2 IDS Versus IPS, p.461

NEW QUESTION 511
Which IDS/IPS solution can monitor system processes and resources?

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

Answer: B

NEW QUESTION 516
Which command enable ospf authentication on an interface?

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

Answer: A

Explanation: https://supportforums.cisco.com/document/22961/ospf-authentication

NEW QUESTION 517
Which 2 NAT type allows only objects or groups to reference an IP address?

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

Answer: AC

Explanation: http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/nat_objects.htm

NEW QUESTION 522

What is the primary purpose of the Integrated Services Routers (ISR) in the BYOD solution?

A. Provide connectivity in the home office environment back to the corporate campus
B. Provide WAN and Internet access for users on the corporate campus
C. Enforce firewall-type filtering in the data center
D. Provide connectivity for the mobile phone environment back to the corporate campus

Answer: A

NEW QUESTION 526
Which type of PVLAN port allows communication from all port types?

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

Answer: D

Explanation: The types of private VLAN ports are as follows:
+ Promiscuous – The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN
+ Isolated – This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
+ Community — A community port is a host port that belongs to a community secondary VLAN.
Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.
Source: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/ CLIConfigurationGuide/PrivateVLANs.html#42874

NEW QUESTION 531
How does a zone paid handle traffic if the policy definition of the zone pair is missing?

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

Answer: B

NEW QUESTION 533
Which statement about zone-based firewall configuration is true?

A. Traffic is implicitly denied by default between interfaces the same zone.
B. Traffic that is desired to or sourced from the self-zone is denied by default.
C. The zone must be configured before a can be assigned.
D. You can assign an interface to more than one interface.

Answer: C

NEW QUESTION 538
What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global
B. privileged
C. in-line
D. Interface

Answer: D

Explanation: ip ospf authentication-key is used under interface configuration mode, so it’s in interface level, under global configuration mode. If it asks about interface level then choose that.
interface Serial0
ip address 192.16.64.1 255.255.25

NEW QUESTION 540
Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

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

Answer: C

Explanation: http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html aaa accounting
To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the aaa accounting command in global configuration mode or template configuration mode. To disable AAA accounting, use the no form of this command.
aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | list-name
| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} no aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default |
listname
| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} exec Runs accounting for the EXEC shell session.
start-stop
Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

NEW QUESTION 543
What is the command to authenticate an NTP time source?

A. #ntp authentication-key 1 md5 141411050D 7
B. #ntp authenticate
C. #ntp trusted-key 1
D. #ntp trusted-key 2

Answer: B

Explanation: ntp authentication-key,,,,Defines the authentication keys.
ntp authenticate,,,Enables or disables the NTP authentication feature.
ntp trusted-key #,,, Specifies one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it

NEW QUESTION 546
What is the highest security level that can be configured for an interface on an ASA?

A. 50
B. 100
C. 200

Answer: C

Explanation: Security level 100: This is the highest security level on our ASA and by default this is assigned to the “inside” interface. Normally we use this for our “LAN”. Since this is the highest security level, by default it can reach all the other interfaces.
https://networklessons.com/cisco/asa-firewall/cisco-asa-security-levels/

NEW QUESTION 551
The Oakley cryptography protocol is compatible with following for managing security?

A. IPSec
B. ISAKMP
C. Port security

Answer: B

Explanation: A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.
ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.
Source: https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key- exchange

NEW QUESTION 556
Which cloud-based security service from Cisco provides URL filtering, web browsing content security, and roaming user protection?

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

Answer: A

NEW QUESTION 559
What are two challenges when deploying host-level IPS? (Choose Two)

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

Answer: AC

Explanation: Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks
because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.
Limitations of HIPS: There are two major drawbacks to HIPS:
+ HIPS does not provide a complete network picture: Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network.
+ HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network.
Source:
http://www.ciscopress.com/articles/article.asp?p=1336425
&seqNum=3

NEW QUESTION 560
Which two options are the primary deployment models for mobile device management? (Choose two)

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

Answer: CD

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

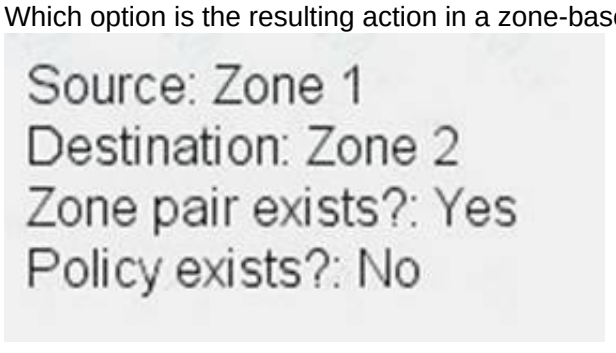
NEW QUESTION 563
Which firepower preprocessor block traffic based on IP?

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

Answer: D

Explanation: Access control rules within access control policies exert granular control over network traffic logging and handling. Reputation-based conditions in access control rules allow you to manage which traffic can traverse your network, by contextualizing your network traffic and limiting it where appropriate. Access control rules govern the following types of reputation-based control:
+ Application conditions allow you to perform application control, which controls application traffic based on not only individual applications, but also applications' basic characteristics: type, risk, business relevance, categories, and tags.
+ URL conditions allow you to perform URL filtering, which controls web traffic based on individual websites, as well as websites' system-assigned category and reputation.
The ASAFirePOWER module can perform other types of reputation-based control, but you do not configure these using access control rules. For more information, see:
+ Blacklisting Using Security Intelligence IP Address Reputation explains how to limit traffic based on the reputation of a connection's origin or destination as a first line of defense.
+ Tuning Intrusion Prevention Performance explains how to detect, track, store, analyze, and block the transmission of malware and other types of prohibited files.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-
module-user-guide-v541/AC-Rules-App-URL-Reputation.html

NEW QUESTION 566
Which option is the resulting action in a zone-based policy firewall configuration with these conditions?

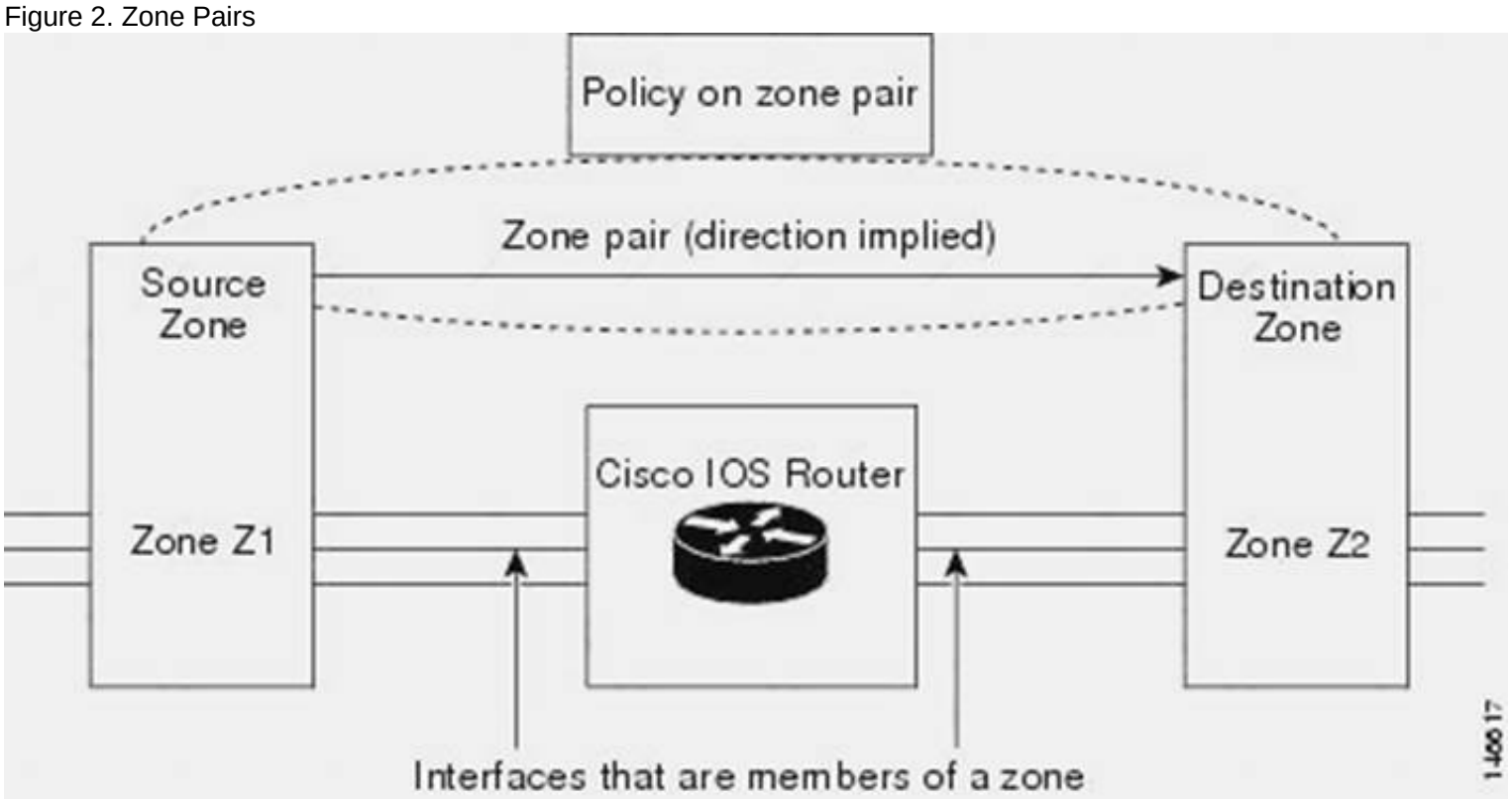


A. no impact to zoning or policy
B. no policy lookup (pass)
C. drop
D. apply default policy

Answer: C

Explanation: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-zone-pol-fw.html
Zone Pairs
A zone pair allows you to specify a unidirectional firewall policy between two security zones.

To define a zone pair, use the zone-pair security command. The direction of the traffic is specified by source and destination zones. The source and destination zones of a zone pair must be security zones.
You can select the default or self zone as either the source or the destination zone. The self zone is a systemdefined zone which does not have any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.
The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).
To permit traffic between zone member interfaces, you must configure a policy permitting (or inspecting) traffic between that zone and another zone. To attach a firewall policy map to the target zone pair, use the servicepolicy type inspect command.
The figure below shows the application of a firewall policy to traffic flowing from zone Z1 to zone Z2, which means that the ingress interface for the traffic is a member of zone Z1 and the egress interface is a member of zone Z2.
Figure 2. Zone Pairs



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

NEW QUESTION 567
The purpose of the certificate authority (CA) is to ensure what?

A. BYOD endpoints are posture checked
B. BYOD endpoints belong to the organization
C. BYOD endpoints have no malware installed
D. BYOD users exist in the corporate LDAP directory

Answer: B

NEW QUESTION 570
Which type of social-engineering attacks uses normal telephone service as the attack vector?

A. vishing
B. phising
C. smishing
D. war dialing

Answer: A

NEW QUESTION 575
Which two primary security concerns can you mitigate with a BYOD solution? (Choose two)

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

Answer: BE

NEW QUESTION 577
Which two options are Private-VLAN secondary VLAN types?

A. Isolated

B. Secured
C. Community
D. Common
E. Segregated

Answer: AC

NEW QUESTION 578
What technology can you use to provide data confidentiality, data integrity and data origin authentication on your network?

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

Answer: C

NEW QUESTION 580
nat (inside,outside) dynamic interface
Refer to the above. Which translation technique does this configuration result in?

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

Answer: C

Explanation: Configuring Dynamic NAT
nat (inside,outside) dynamic my-range-obj Configuring Dynamic PAT (Hide)
nat (inside,outside) dynamic interface
Source: http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/nat_objects.html

NEW QUESTION 585
With which type of Layer 2 attack can you intercept traffic that is destined for one host?

A. MAC spoofing
B. CAM overflow….

Answer: A

NEW QUESTION 586
Which primary security attributes can be achieved by BYOD Architecture?

A. Trusted enterprise network
B. public wireless network
C. checking compliance with policy
D. pushing patches

Answer: AC

NEW QUESTION 590
What is the actual IOS privilege level of User Exec mode?

A. 1
B. 5
C. 15

Answer: A

Explanation: By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15). However, you can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.
Source: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

NEW QUESTION 594
Which type of VLANs can communicate to PVLANs? (something like this) (choose 2)

A. promiscuous
B. isolated
C. community
D. backup
E. secondary

Answer: AB

NEW QUESTION 595
which will auto-nat process first (the focus is on auto-nat)

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

Answer: D

NEW QUESTION 600
Which command is to make sure that AAA Authentication is configured and to make sure that user can access the exec level to configure?

A. AAA authentication enable default local
B. AAA authentication enable local
C. AAA authentication enable tacacs+ default

Answer: A

NEW QUESTION 604
Which IPS detection method can you use to detect attacks that based on the attackers IP addresses?

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

Answer: D

NEW QUESTION 606
Which option is a characteristic of the RADIUS protocol?

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

Answer: C

Explanation: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Authentication and Authorization
RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to
re-authenticate. The
NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

NEW QUESTION 611
Which type of firewall can serve as the intermediary between a client and a server?

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

Answer: D

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

NEW QUESTION 615
Which of Diffie-Hellman group(s) is/are support(ed) by CISCO VPN Product (Choose all that apply?

A. Group1
B. Group2
C. Group3
D. Group5
E. Group7
F. Group8

G. Group9

Answer: ABDE

NEW QUESTION 620
By default, how does a zone-based firewall handle traffic to and from the self zone?

A. It permits all traffic without inspection.
B. It inspects all traffic to determine how it is handled.
C. it permits all traffic after inspection
D. it drops all traffic.

Answer: A

NEW QUESTION 625
Which description of the nonsecret numbers that are used to start a Diffie-Hellman exchange is true?

A. They are large pseudorandom numbers.
B. They are very small numbers chosen from a table of known values
C. They are numeric values extracted from hashed system hostnames.
D. They are preconfigured prime integers

Answer: D

NEW QUESTION 629
With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

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

Answer: BCD

Explanation: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml Rules For Applying Zone-Based Policy Firewall
Router network interfaces' membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces:
A zone must be configured before interfaces can be assigned to the zone. An interface can be assigned to only one security zone.
All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.
Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.
The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.
Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones.
Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.
If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.
From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).
The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

NEW QUESTION 631
Which two features are supported in a VRF-aware software infrastructure before VRF-lite? (Choose two)

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

Answer: BC

NEW QUESTION 634
Which NAT option is executed first during in case of multiple nat translations?

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

Answer: D

NEW QUESTION 636
How can you protect CDP from reconnaissance attacks?

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

Answer: B

NEW QUESTION 640
Which option is the default value for the Diffie–Hellman group when configuring a site-to-site VPN on an ASA device?

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

Answer: B

NEW QUESTION 644
Which type of address translation supports the initiation of communications bidirectionally?

A. multi-session PAT
B. static NAT
C. dynamic PAT
D. dynamic NAT

Answer: D

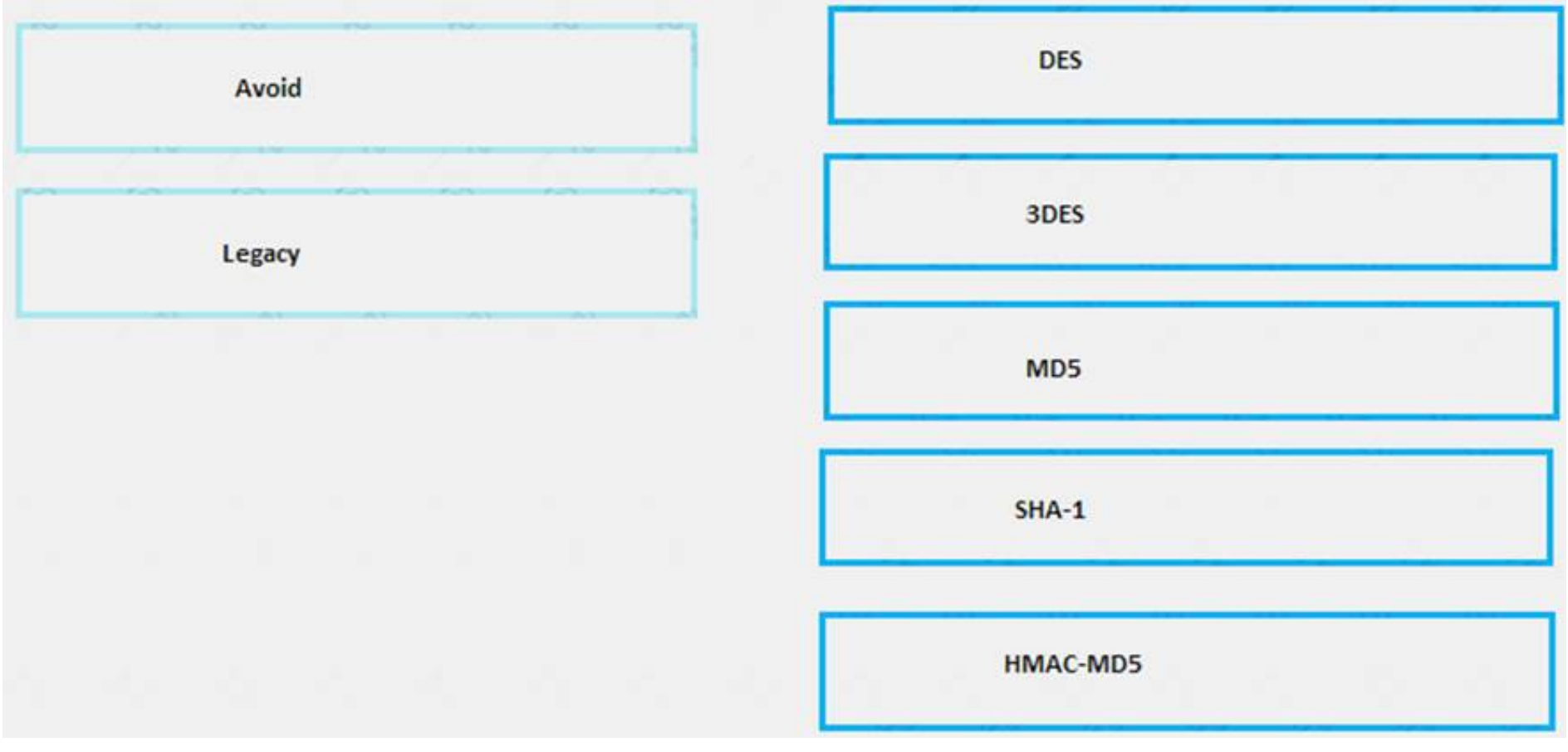
NEW QUESTION 647
Which two characteristics of the TACACS+ protocol are true? (Choose two.)

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

Answer: BC

Explanation: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Packet Encryption
RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.
TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.
Authentication and Authorization RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to
re-authenticate. The
NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

NEW QUESTION 649
Drag the recommendations on the left to the Cryptographic Algorithms on the right. Options will be used more than once.



Answer:

Explanation: DES = Avoid 3DES = Legacy MD5 = Avoid
SHA-1 = Legacy HMAC-MD5 = Legacy
https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

NEW QUESTION 653
Which two characteristics of a PVLAN are true?

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

Answer: CE

Explanation: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/pvlans.p

NEW QUESTION 658
Which statement about college campus is true?

A. College campus has geographical position.
B. College campus Hasn`t got internet access.
C. College campus Has multiple subdomains.
D. College campus Has very beautiful girls

Answer: A

NEW QUESTION 660
The command debug crypto isakmp results in ?

A. Troubleshooting ISAKMP (Phase 1) negotiation problems

Answer: A

NEW QUESTION 662
Which prevent the company data from modification even when the data is in transit?

A. Confidentiality
B. Integrity
C. Vailability

Answer: B

Explanation: Integrity: Integrity for data means that changes made to data are done only by authorized individuals/systems. Corruption of data is a failure to maintain data integrity.
Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

NEW QUESTION 666
What are the two characteristics of IPS?

A. Can drop traffic
B. Does not add delay to traffic
C. It is cabled directly inline
D. Can`t drop packets on its own

Answer: AC

Explanation: + Position in the network flow: Directly inline with the flow of network traffic and every packet goes through the sensor on its way through the network.
+ Mode: Inline mode
+ The IPS can drop the packet on its own because it is inline. The IPS can also request assistance from another device to block future packets just as the IDS does.
Source: Cisco Official Certification Guide, Table 17-2 IDS Versus IPS, p.461

NEW QUESTION 671
How to verify that TACACS+ connectivity to a device?

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

Answer: B

NEW QUESTION 676
Which Firepower Management Center feature detects and blocks exploits and hack attempts?

A. intrusion prevention
B. advanced malware protection (AMP)
C. content blocker
D. file control

Answer: B

Explanation: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-modul

NEW QUESTION 681
What type of Diffie-Hellman group would you expect to be utiliazed on a wireless device?

A. Group4
B. Group7
C. Group5
D. Group3

Answer: B

NEW QUESTION 686
Which two advantages does the on-premise model for MDM deployment have over the cloud-based model? (Choose two)

A. The on-premise model provides more control of the MDM solution than the cloud-based model
B. The on-premise model is more scalable than the cloud-based model
C. The on-premtse model is generally less expensive than the cloud-based model
D. The on-premise model is easier and faster to deploy than the cloud-based model
E. The on-premise model generally has less latency than the cloud-based model

Answer: AE

NEW QUESTION 688
Which two roles of the Cisco WSA are true? (Choose two.)

A. web proxy
B. URL filter
C. antispam
D. IPS
E. firewall

Answer: AB

NEW QUESTION 692
Which two attack types can be prevented with the implementation of a Cisco IPS solution?(Choose two.)

A. VLAN hooping
B. DDos
C. Worms
D. ARP spoofing
E. man-in-the -middle

Answer: CE

NEW QUESTION 697
Which IKE phase 1 parameter can you use to require the site-to-site VPN to us a pre-shared key?

A. group
B. hash
C. authentication
D. encryption

Answer: C

NEW QUESTION 702
On an ASA, which maps are used to identify traffic?

A. Policy maps
B. Class maps
C. Route maps
D. Service maps

Answer: B

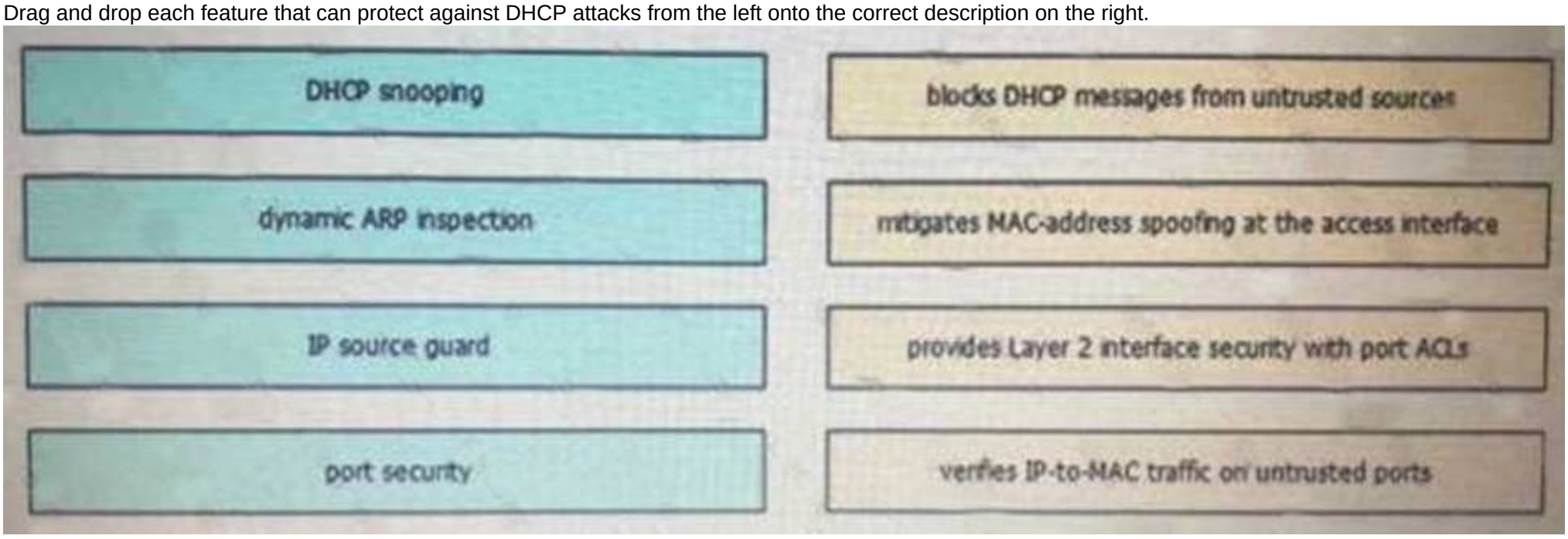
NEW QUESTION 704
Which two types of VLANs using PVLANs are valid? (Choose two.)

A. secondary
B. community
C. isolated
D. promiscuous
E. backup

Answer: CD

Explanation: Promiscuous (P) :- Usually connects to a router – a type of a port which is allowed to send and receive frames from any other port on the VLAN.
Isolated (I) : This type of port is only allowed to communicate with P ports – they are “stub”. This typ of ports usually connects to hosts.
https://learningnetwork.cisco.com/docs/DOC-16110

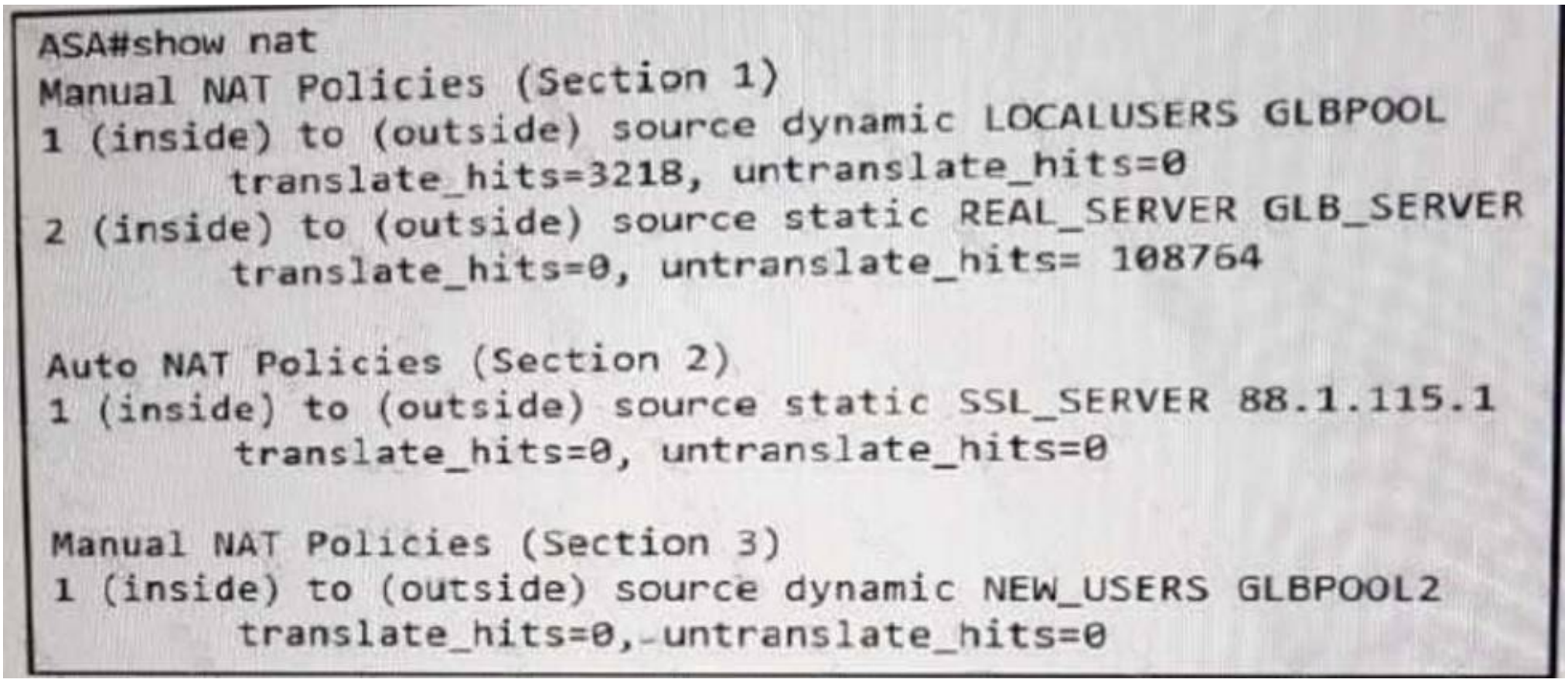
NEW QUESTION 707
Drag and drop each feature that can protect against DHCP attacks from the left onto the correct description on the right.



Answer:

Explanation: 1:1
3:2
4:3
2:4

NEW QUESTION 712
Refer to the exhibit.



A network security administrator checks the ASA firewall NAT policy table with the show nat command. Which statement is false?

A. There are only reverse transalation matches for the REAL_SERVER object.
B. First policy in the Section 1 is as dynamic nat entry defined in the object configuration.
C. NAT policy in Section 2 is a static entry defined in the obkect configuration
D. Transalation in Section 3 used when a connection does not match any entries in first two sections.

Answer: A

NEW QUESTION 715
Which two are considered basic security principles? (Choose two.)

A. Integrity
B. Confidentiality
C. Redundancy
D. Accountability
E. High Availability

Answer: AB

NEW QUESTION 717
How can you mitigate attacks in which the attacker attaches more than one VLAN tag to a packet?

A. Disable EtherChannel on the switch.
B. Assign an access VLAN to every active port on the switch.
C. Enable transparent VTP on the switch.
D. Explicitly identify each VLAN allowed across the trunk.

Answer: B

NEW QUESTION 721
Which IDS/IPS state misidentifies acceptable behavior as an attack?

A. false positive
B. false negative
C. true positive
D. true negative

Answer: A

NEW QUESTION 722
Which two options are primary deployment model for mobile device management (Choose two)

A. Cloud-based
B. Hybrid-cloud based
C. Multisite
D. On-Perimeter
E. Single site

Answer: AD

NEW QUESTION 725
Which STP feature can prevent an attacker from becoming the root bridge by immediately shutting down the interface when it receives a BPDU?

A. BPDU filtering
B. root guard
C. BPDU guard
D. portFast

Answer: C

NEW QUESTION 730
Which attack involves large numbers of ICMP packets with a spoofed source IP address?

A. Teardrop attack
B. smurf attack
C. Nuke attack
D. SYN Flood attack

Answer: B

NEW QUESTION 733
What is the effect of the ip scp server enable command?

A. It allows the router to become an SCP server.
B. It adds SCP to the list of allowed copy functions.
C. It allows the router to initiate requests to an SCP server.
D. It references an access list that allows specific SCP servers.

Answer: A

NEW QUESTION 736
What is the most common implementation of PAT in a standard networked environment?

A. configuring an any any rule to enable external hosts to communicate inside the network.
B. configuring multiple internal hosts to communicate outside of the network by using the inside interface IP address
C. configuring multiple external hosts to join the self zone and to communicate with one another
D. configuring multiple internal hosts to communicate outside of the network using the outside interface IP address

Answer: D

NEW QUESTION 740
Which action does standard antivirus software perform as part of the file-analysis process?

A. execute the file in a simulated environment to examine its behavior
B. flag the unexamined file as a potential threat
C. examine the execution instructions in the file
D. create a backup copy of the file

Answer: A

NEW QUESTION 742
A user on your network inadvertently activates a botnet program that was received as an email attachment Which type of mechanism does Cisco Firepower use to detect and block only the botnet attack?

A. network-based access control rule
B. botnet traffic filter
C. reputation-based
D. user-based access control rule

Answer: B

NEW QUESTION 744
Why does ISE require its own certificate issued by a trusted CA?

A. ISE's certificate allows guest devices to validate it as a trusted network device.
B. It generates certificates for guest devices based on its own certificate
C. ISE's certificate allows it to join the network security framework
D. It requests certificates for guest devices from the CA server based on its own certificate.

Answer: A

NEW QUESTION 745
Which two commands are used to implement Cisco IOS Resilient Configuration? (Choose two.)

A. secure boot-image
B. copy running-config startup-config
C. secure boot-config
D. copy flash:/ios.bin tftp
E. copy running-config tftp

Answer: AC

Explanation: The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).
In 12.3(8)T this feature was introduced.
The following commands were introduced or modified: secure boot-config, secure boot-image, showsecure bootset.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec

NEW QUESTION 749
What does the policy map do in CoPP?

A. defines the action to be performed
B. defines packet selection parameters
C. defines the packet filter
D. defines service parameters

Answer: C

NEW QUESTION 754
When an IPS device detects an email threat, which action can it take in response?

A. request an SNMP trace
B. request an SNMP fail
C. request an SNMP block
D. request an SNMP trap

Answer: D

NEW QUESTION 755
You are configuring a NAT rule on a Cisco ASA. Which description of a mapped interface is true?

A. It is mandatory for all fire wall modes.
B. It is mandatory for identity NAT only.
C. It is optional in transparent mode.
D. It is optional in routed mode.

Answer: D

NEW QUESTION 758
Which type of social engineering attack targets top executives?

A. baiting
B. vishing
C. whaling
D. spear phishing

Answer: A

NEW QUESTION 759
Which command successfully creates an administrative user with a password of "Cisco" on a Cisco router?

A. usemame Operator privilege 7 password Cisco
B. username Operator privilege 1 password cisco
C. user name Operator privilege 15 password cisco
D. usemame Operator password cisco privilege 15

Answer: C

NEW QUESTION 762
Which command enables authentication at the OSPFv2 routing process level?

A. area 0 authentication message-digest
B. area 0 authentication ipsec spi 500 md5 1 234567890ABCDEF1234567890ABCDEF
C. ip ospf authentication message-digest
D. ip ospf message-digest-key 1 md5 C1sc0!

Answer: A

NEW QUESTION 766
Which two parameters can you view in the Cisco ASDM Protocol Statistics window? (Choose two)

A. the number of active tunnels
B. the number of rejected connection attempts
C. the number of tunnels that have been established since the Cisco ASA was rebooted
D. the number of closed tunnels
E. the user attempting the connection

Answer: AE

NEW QUESTION 770
Which security term refers to the likelihood that a weakness will be exploited to cause damage to an asset?

A. threat
B. vulnerability
C. risk
D. countermeasure

Answer: B

NEW QUESTION 775
Which feature can help a router or switch maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch?

A. Control Plane Policing
B. Service Policy
C. Cisco Express Forwarding
D. Policy Map

Answer: A

NEW QUESTION 779
Which two types of firewalls work at Layer 4 and above? (Choose two.)

A. application-level firewall
B. static packet filter
C. stateful inspection
D. Network Address Translation
E. circuit-level gateway

Answer: BC

Explanation: Dynamic or Stateful Packet-Filtering Firewalls
Stateful inspection is a firewall architecture classified at the network layer; although, for some applications it can analyze traffic at Layers 4 and 5, too.
Unlike static packet filtering, stateful inspection tracks each connection traversing all interfaces of the firewall and confirms that they are valid. Stateful packet filtering maintains a state table and allows modification to the security rules dynamically. The state table is part of the internal structure of the firewall. It tracks all sessions and inspects all packets passing through the firewall.
Although this is the primary Cisco Firewall technology, it has some limitations:
Cannot prevent application layer attacks.
Not all protocols are stateful.
Some applications open multiple connections.
Does not support user authentication.
http://www.ciscopress.com/articles/article.asp?p=1888110

NEW QUESTION 781
Which two actions can a zone-based firewall apply to a packet as it transits a zone pair? (Choose two.)

A. drop
B. inspect
C. queue
D. quarantine
E. block

Answer: AB

NEW QUESTION 786
Which technology can you implement to centrally mitigate potential threats when users on your network download files that might be malicious?

A. Enable file-reputation services to inspect all files that traverse the company network and block files with low reputation scores.
B. Verify that the company IPS blocks all known malicious websites.
C. Verify that antivirus software is installed and up to date for all users on your network.
D. Implement URL filtering on the perimeter firewall.

Answer: D

NEW QUESTION 790

What are two advanced features of the Cisco AMP solution for endpoints? (Choose two)

A. reflection
B. foresight
C. sandboxing
D. contemplation
E. reputation

Answer: CE

NEW QUESTION 792
Which technology can best protect data at rest on a user system?

A. network IPS
B. router ACL
C. full-disk encryption
D. IPsec tunnel

Answer: C

NEW QUESTION 793
What are two limitations of the self-zone policies on a zone-based firewall? (Choose two)

A. They restnct SNMP traffic
B. They are unable to implement application inspection
C. They are unable to block HTTPS traffic
D. They are unable to support HTTPS traffic
E. They are unable to perform rate limiting.

Answer: CE

NEW QUESTION 798
Which protocol offers data integrity, encryption, authentication, and antireplay functions for IPsec VPN?

A. AH protocol
B. ESP protocol
C. IKEv2 protocol
D. IKEv1 protocol

Answer: C

Explanation: IP Security Protocol—Encapsulating Security Payload (ESP)
Encapsulating Security Payload (ESP) is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional antireplay service, and limited traffic flow confidentiality by defeating traffic flow analysis.
http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=3

NEW QUESTION 800
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

210-260 Practice Exam Features:

* 210-260 Questions and Answers Updated Frequently

* 210-260 Practice Questions Verified by Expert Senior Certified Staff

* 210-260 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 210-260 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year