# Cisco.210-260.v2020-02-04.q100

| | |
|---|---|
| **Exam Code:** | 210-260 |
| **Exam Name:** | Implementing Cisco Network Security |
| **Certification Provider:** | Cisco |
| **Free Question Number:** | 100 |
| **Version:** | v2020-02-04 |
| **# of views:** | 823 |
| **# of Questions views:** | 26606 |
| https://www.freecram.net/torrent/Cisco.210-260.v2020-02-04.q100.html | |

**NEW QUESTION: 1**
In which two situations should you use in band management? (Choose two.)
**A.** when multiple management applications need concurrent access to the device
**B.** when you require ROMMON access
**C.** when a network device fails to forward packets
**D.** when the control plane fails to respond
**E.** when you require administrator access from multiple locations
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 2**
Which technology can block a non-malicious program that is run from a local computer that has been disconnected from the network?
**A.** firewall
**B.** network IPS
**C.** antivirus software
**D.** host IPS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 3**
What type of attack was the Stuxnet virus?
**A.** cyber warfare
**B.** hacktivism
**C.** botnet
**D.** social engineering
**Answer: (SHOW ANSWER)**
Explanation
Stuxnet is a computer worm that targets industrial control systems that are used to monitor and control large

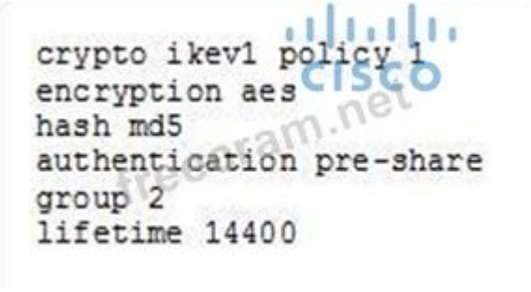
scale industrial facilities like power plants, dams, waste processing systems and similar operations. It allows the attackers to take control of these systems without the operators knowing. This is the first attack we've seen that allows hackers to manipulate real-world equipment, which makes it very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

**NEW QUESTION: 4**
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)
**A.** Port security
**B.** DHCP snooping
**C.** IP source guard
**D.** Dynamic ARP inspection
**Answer: (SHOW ANSWER)**
Explanation
+ ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received.
+ DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.
+ DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database.
Source: Cisco Official Certification Guide, Dynamic ARP Inspection, p.254

**NEW QUESTION: 5**
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: (SHOW ANSWER)**
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: 6**
Refer to the exhibit.




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

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

**A.** The ASA will apply the actions from only the first matching class map it finds for the feature type.
**B.** The ASA will apply the actions from only the most specific matching class map it finds for the feature type.
**C.** The ASA will apply the actions from all matching class maps it finds for the feature type.
**D.** The ASA will apply the actions from only the last matching class map it finds for the feature type.
**Answer: (SHOW ANSWER)**
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: 8**
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: (SHOW ANSWER)**
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: 9**
Which two features are commonly used by CoPP and CPPr to protect the control plane?

**A.** QoS
**B.** traffic classification
**C.** access lists
**D.** policy maps
**E.** class maps
**F.** Cisco Express Forwarding
**Answer: (SHOW ANSWER)**
Explanation
For example, you can specify that management traffic, such as SSH/HTTPS/SSL and so on, can be ratelimited (policed) down to a specific level or dropped completely.
Another way to think of this is as applying quality of service (QoS) to the valid management traffic and policing to the bogus management traffic.
Source: Cisco Official Certification Guide, Table 10-3 Three Ways to Secure the Control Plane, p.269

**NEW QUESTION: 10**
Which technology could be used on top of an MPLS VPN to add confidentity.
**A.** IPsec
**B.** AES
**C.** SSL
**D.** 3DES
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 11**
By which kind of threat is the victim tricked into entering username and password information at a disguised website?
**A.** Spoofing
**B.** Malware
**C.** Spam
**D.** Phishing
**Answer: (SHOW ANSWER)**
Explanation
Phishing presents a link that looks like a valid trusted resource to a user. When the user clicks it, the user is prompted to disclose confidential information such as usernames/passwords.
Source: Cisco Official Certification Guide, Table 1-5 Attack Methods, p.13

**NEW QUESTION: 12**
How can you proect CDP from reconnaissance attacks?
**A.** Disable CDP on ports connected to endpoints.
**B.** Enable dynamic ARP inspection on all untrusted ports.
**C.** Enable dot1x on all ports that are connected to other switches.
**D.** Disbale CDP on trunk ports.

**Answer: (SHOW ANSWER)**

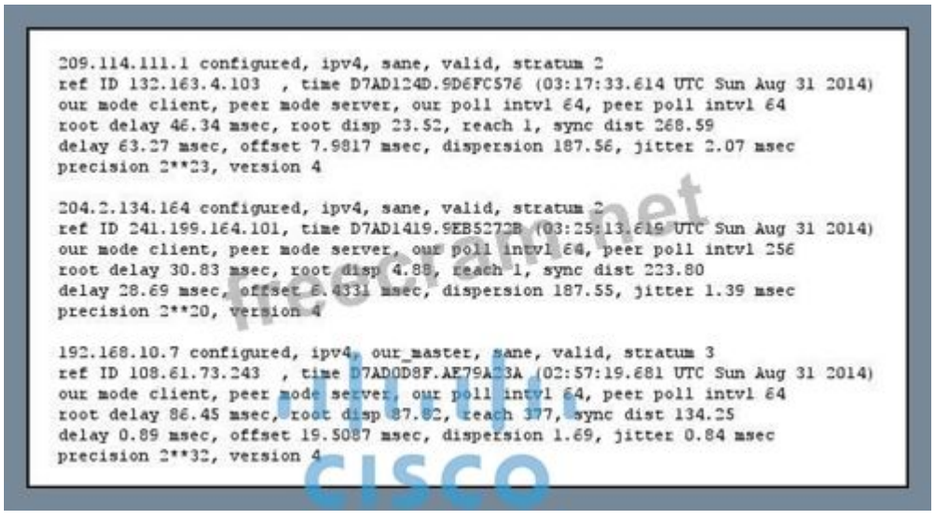
**NEW QUESTION: 13**
Which accounting notices are used to send a failed authentication attempt record to a AAA server? (Choose two.)
**A.** start-stop
**B.** stop-record
**C.** stop-only
**D.** stop
**Answer: A,C (LEAVE A REPLY)**
Explanation
aaa accounting { auth-proxy | system | network | exec | connection | 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: 14**
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: (SHOW ANSWER)**
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: 15**
Which tool can an attacker use to attempt a DDoS attack?

**A.** botnet
**B.** Trojan horse
**C.** virus
**D.** adware
**Answer: (SHOW ANSWER)**
Explanation
Denial-of-service (DoS) attack and distributed denial-of-service (DDoS) attack. An example is using a botnet to attack a target system.
Source: Cisco Official Certification Guide, Table 1-6 Additional Attack Methods, p.16

**NEW QUESTION: 16**
Refer to the exhibit.




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 (LEAVE A REPLY)**
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: 17**
Which type of PVLAN port allows communication from all port types?
**A.** isolated
**B.** community
**C.** in-line
**D.** promiscuous
**Answer: (SHOW ANSWER)**
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: 18**
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: (SHOW ANSWER)**
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: 19**
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: (SHOW ANSWER)**
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: 20**

Which statement about traffic inspection using the Cisco Modular Policy Framework on the ASA is true?

**A.** HTTP inspection is supported with Cloud Web Security inspection

**B.** Traffic can be sent to multiple modules for inspection

**C.** QoS policing and QoS pnonty queuing can be configured for the same traffic

**D.** ASA with FirePOWER supports HTTP inspection

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 21**

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.

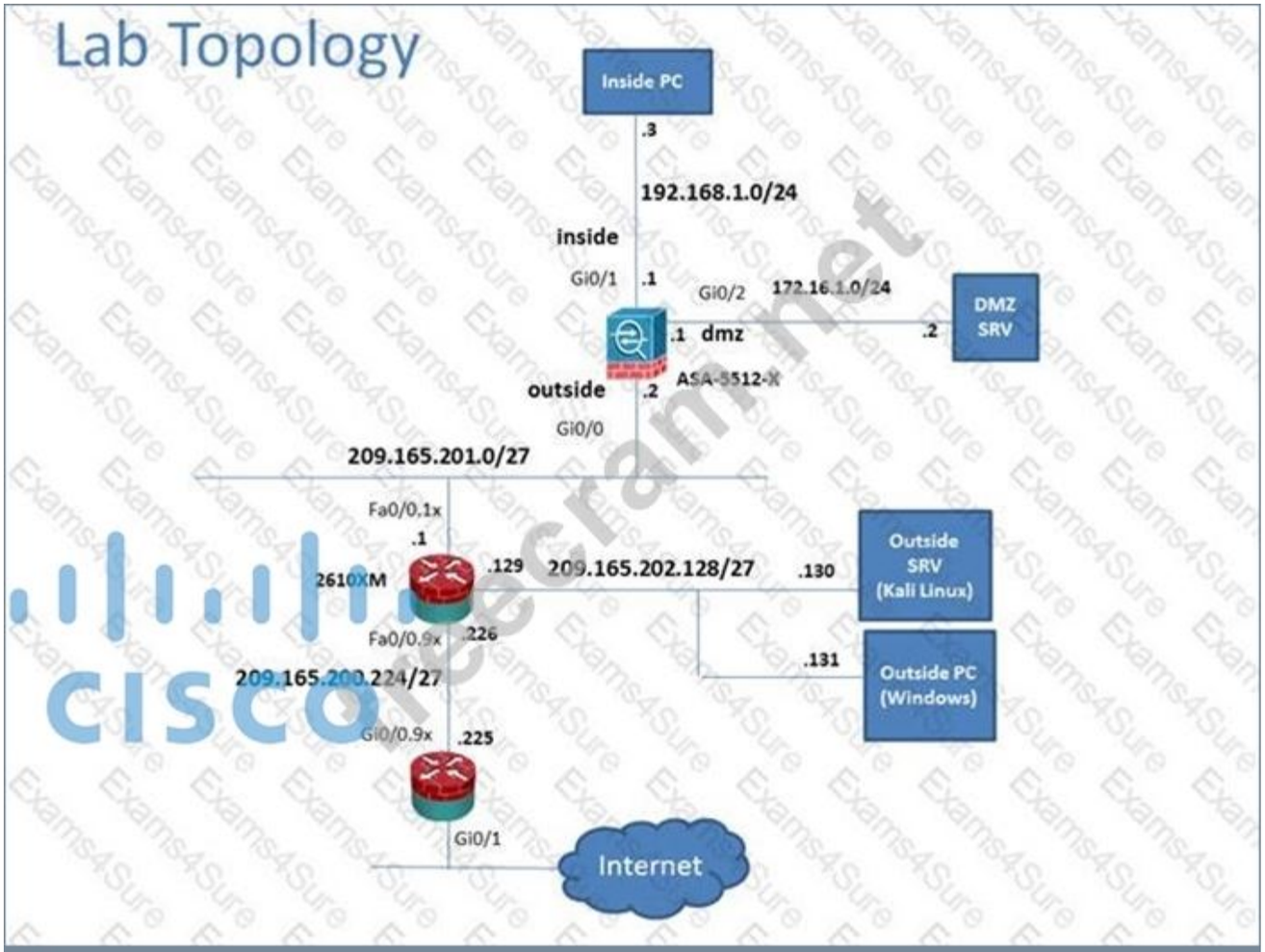
To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.

Note:

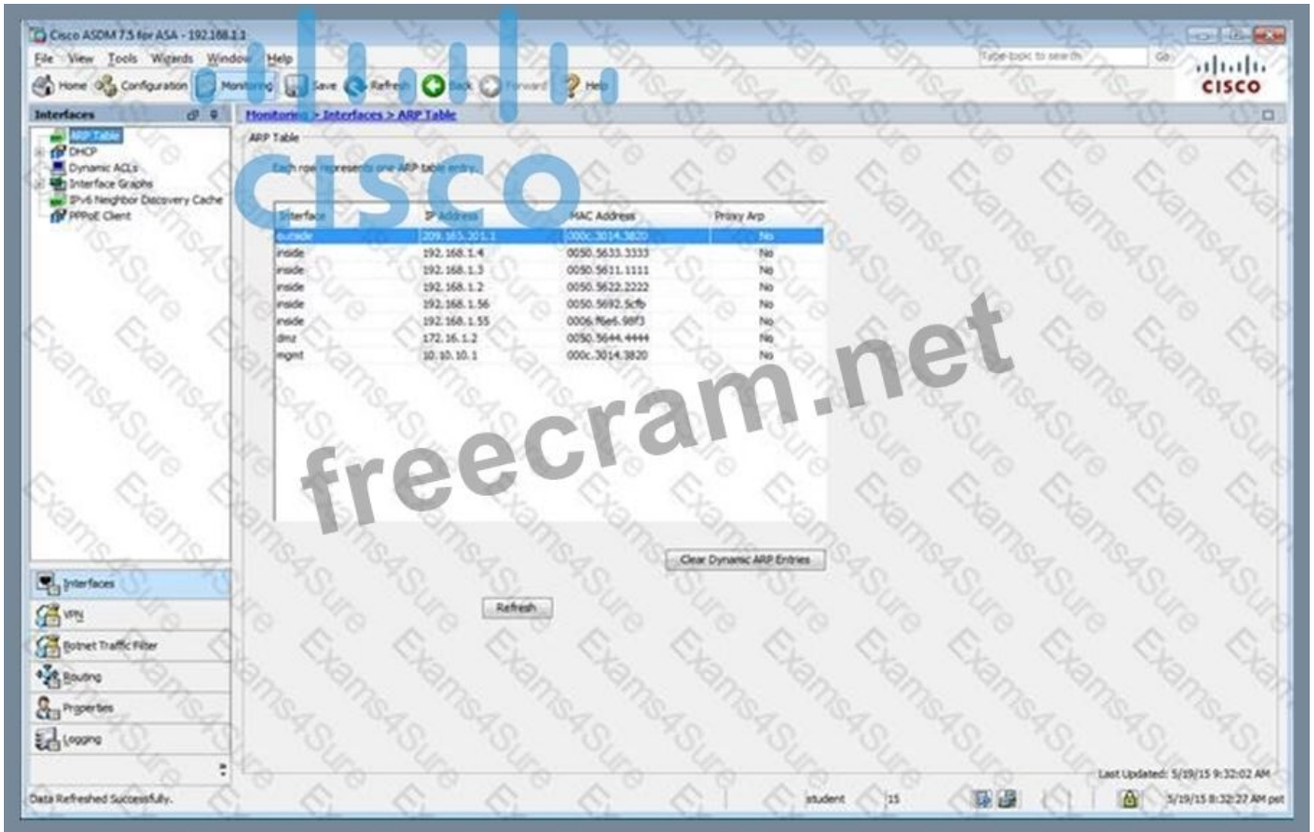
After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.

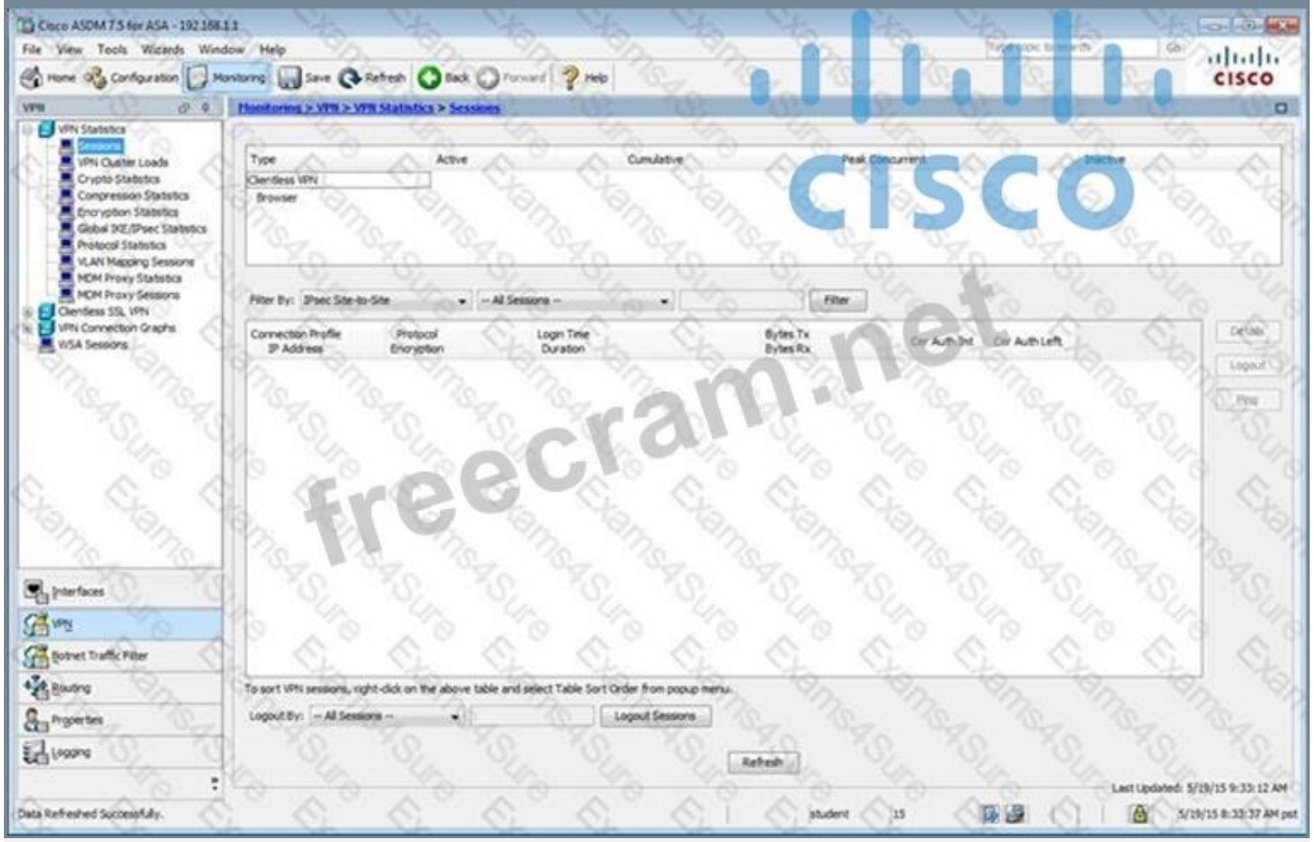
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.

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

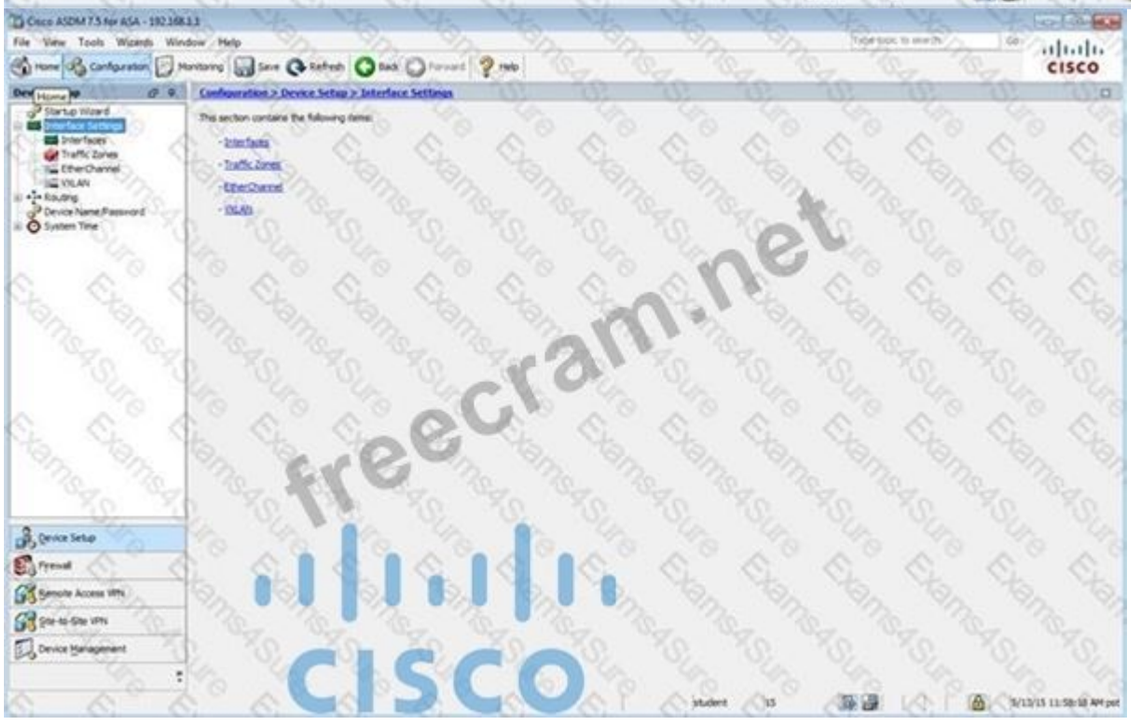

Lab Topology
Inside PC
.3
192.168.1.0/24
inside
Gi0/1
.1
Gi0/2
172.16.1.0/24
DMZ SRV
.2
.1 dmz
outside
.2
ASA-5512-X
Gi0/0
209.165.201.0/27
Fa0/0.1x
.1
2610XM
.129
209.165.202.128/27
.130
Outside SRV (Kali Linux)
Fa0/0.9x
.226
.131
Outside PC (Windows)
209.165.200.224/27
Gi0/0.9x
.225
Gi0/1
Internet

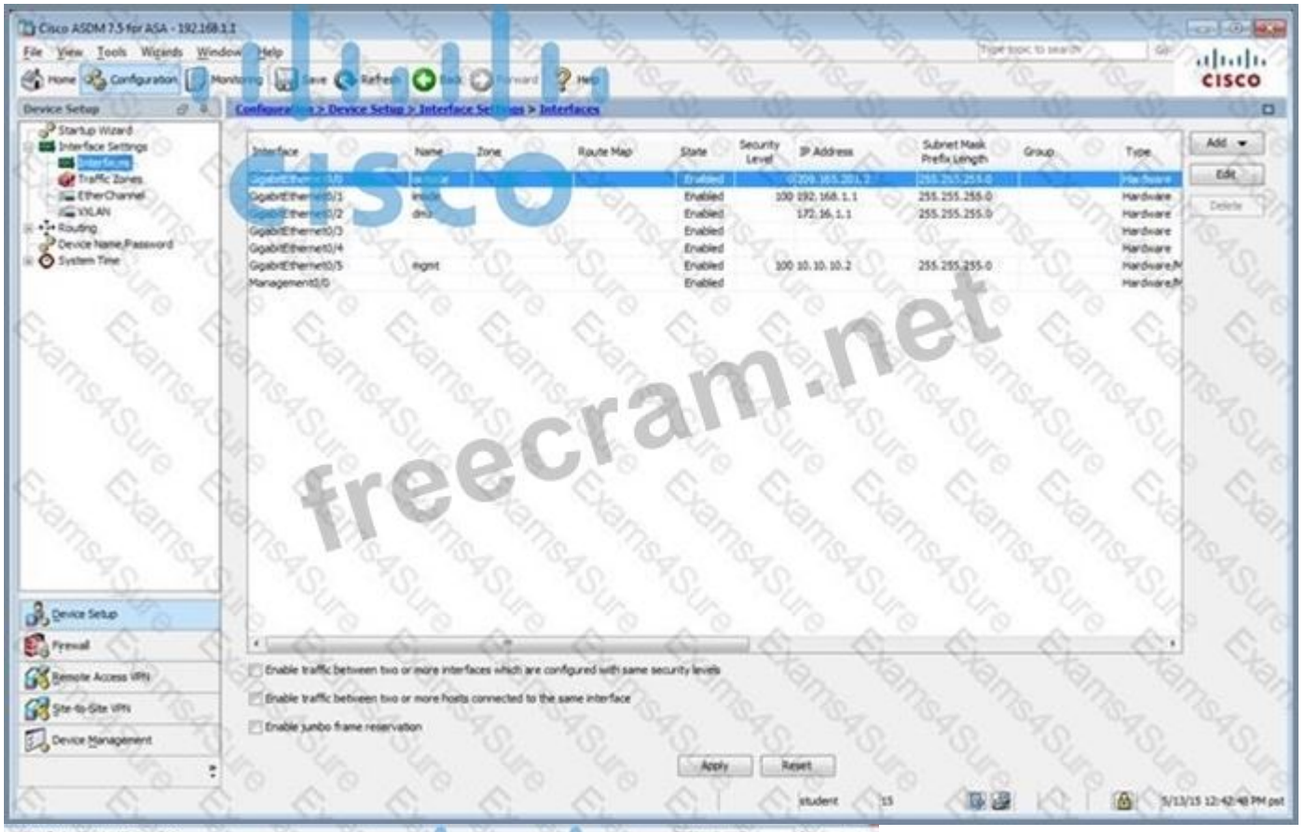

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
Interface Status
Latest ASDM Syslog Messages

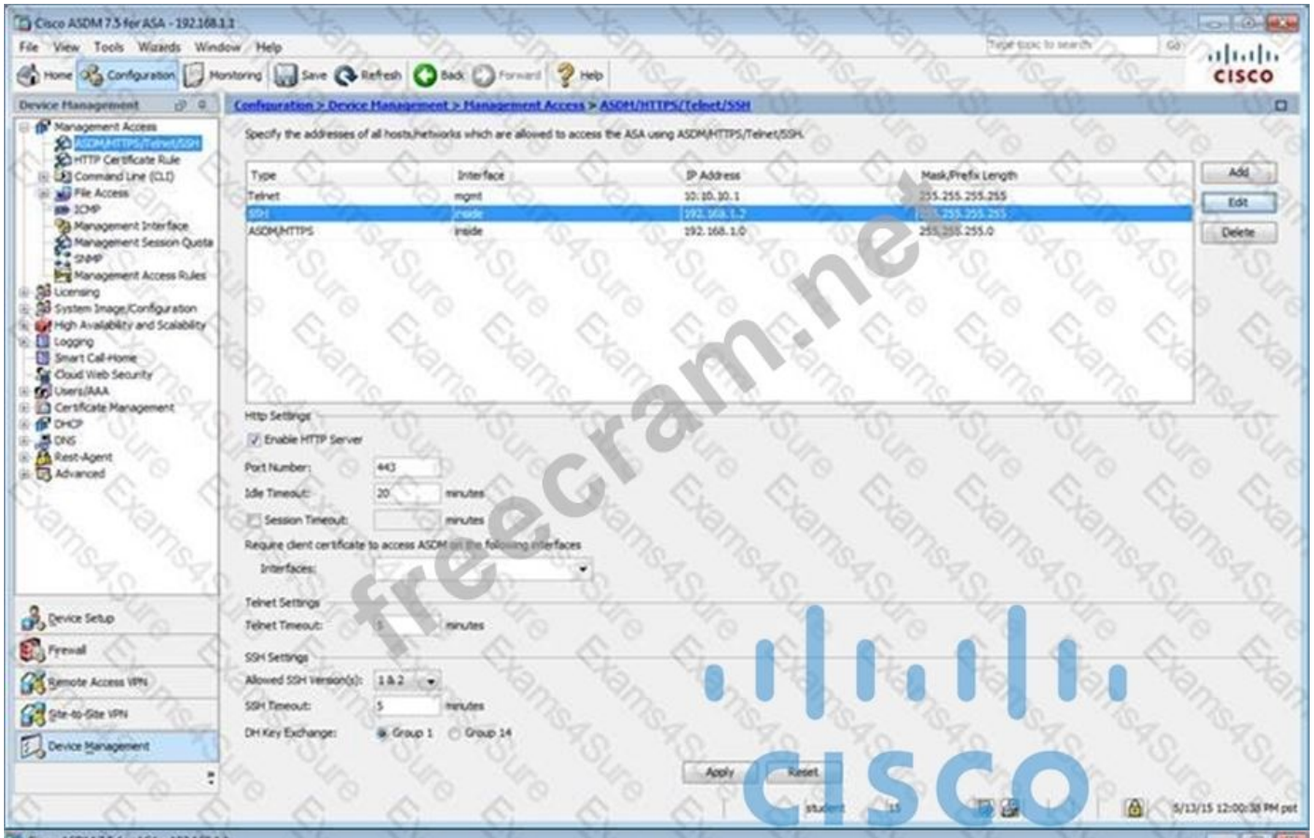


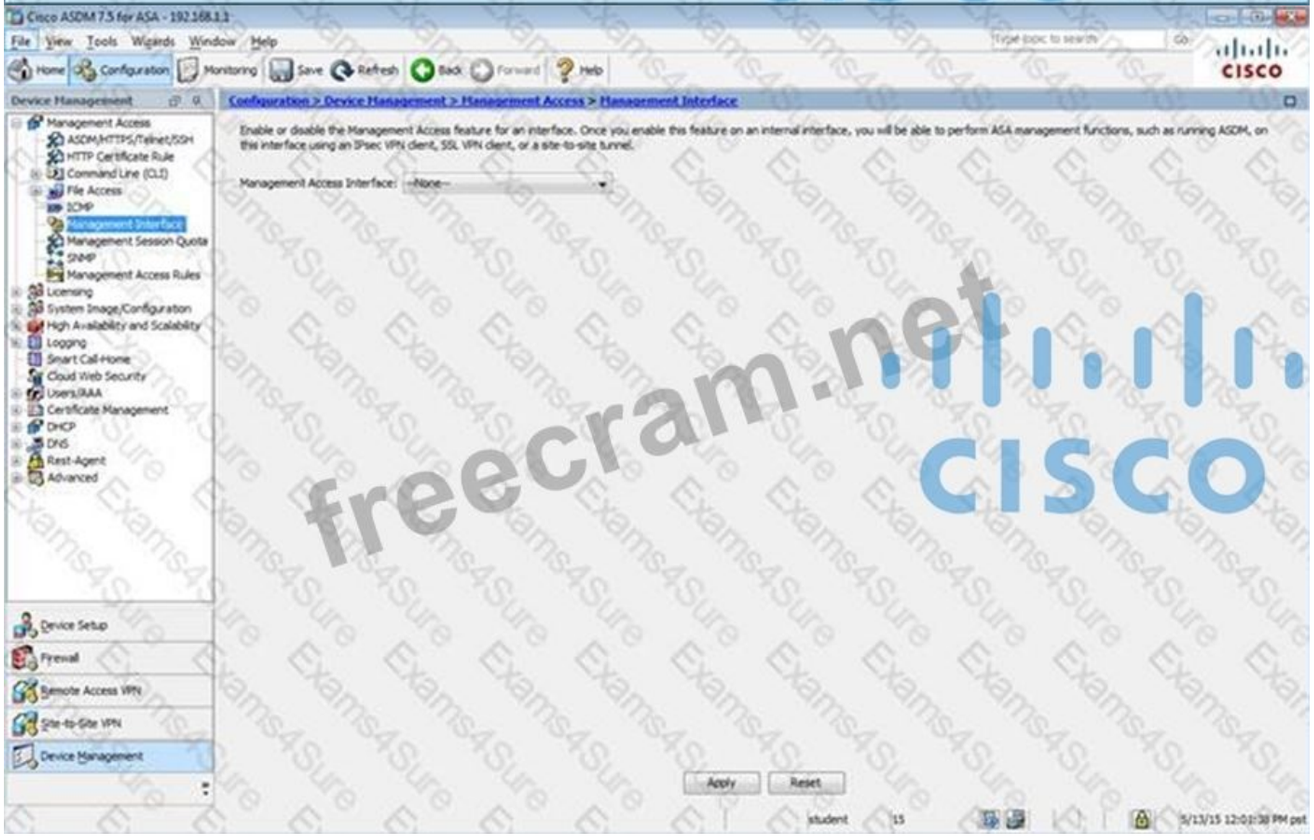



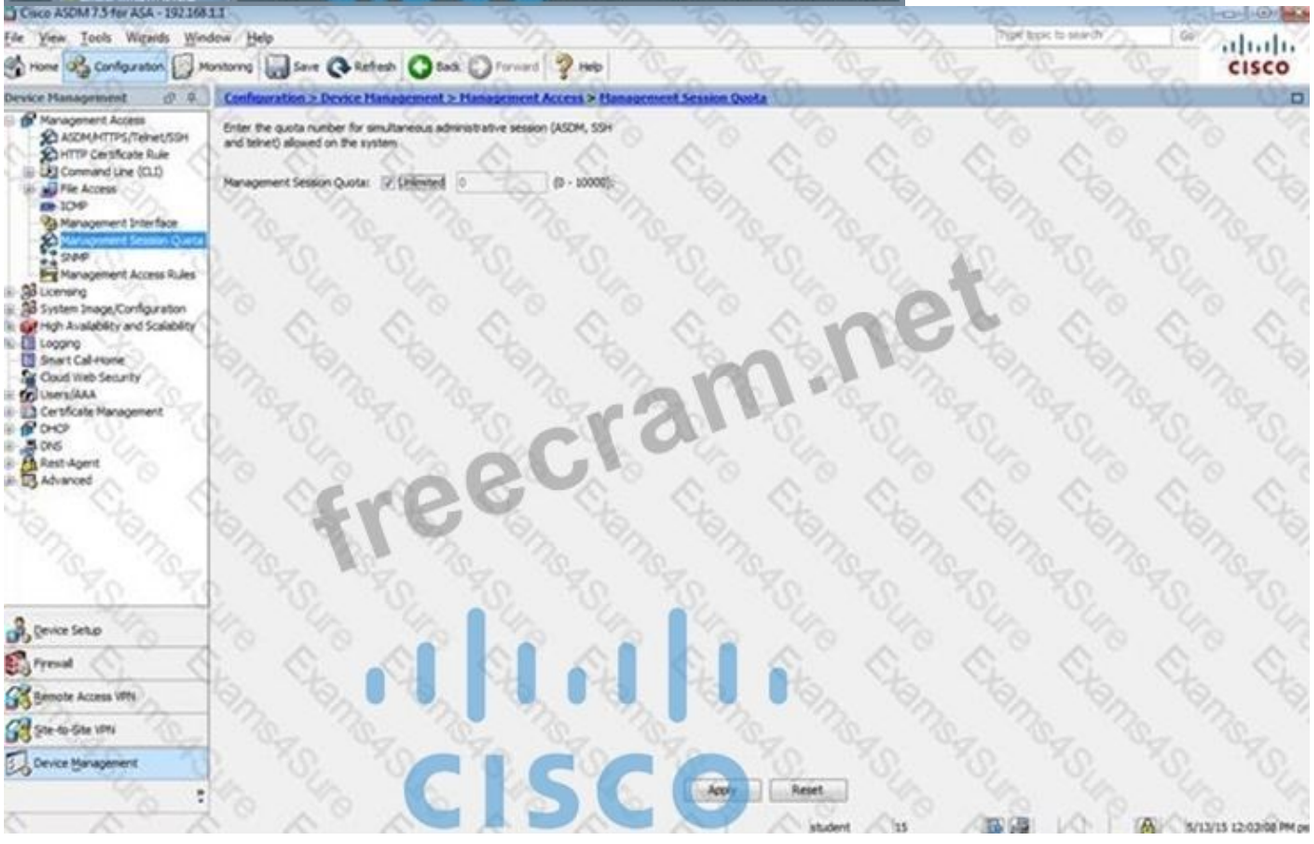

Filter By: Clientless SSL VPN -- All Sessions -- Filter

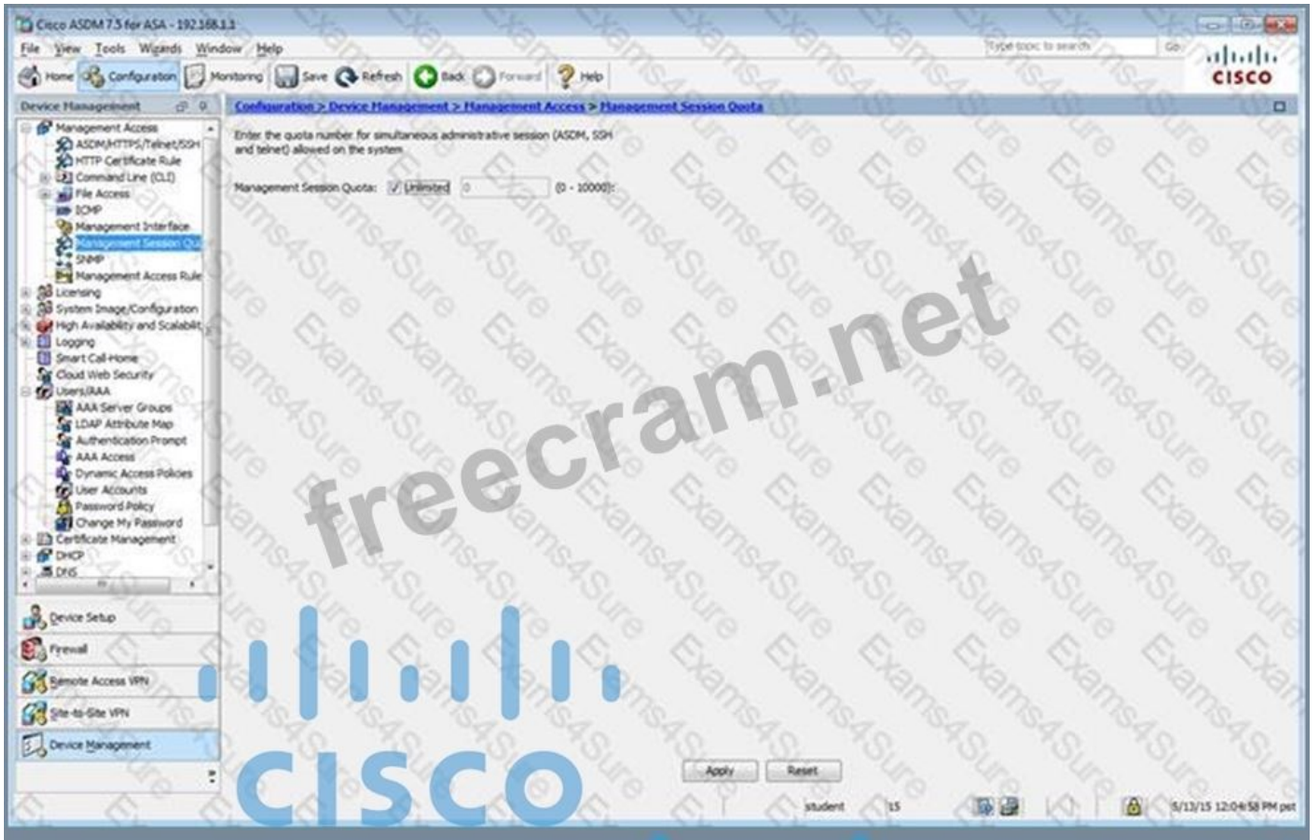



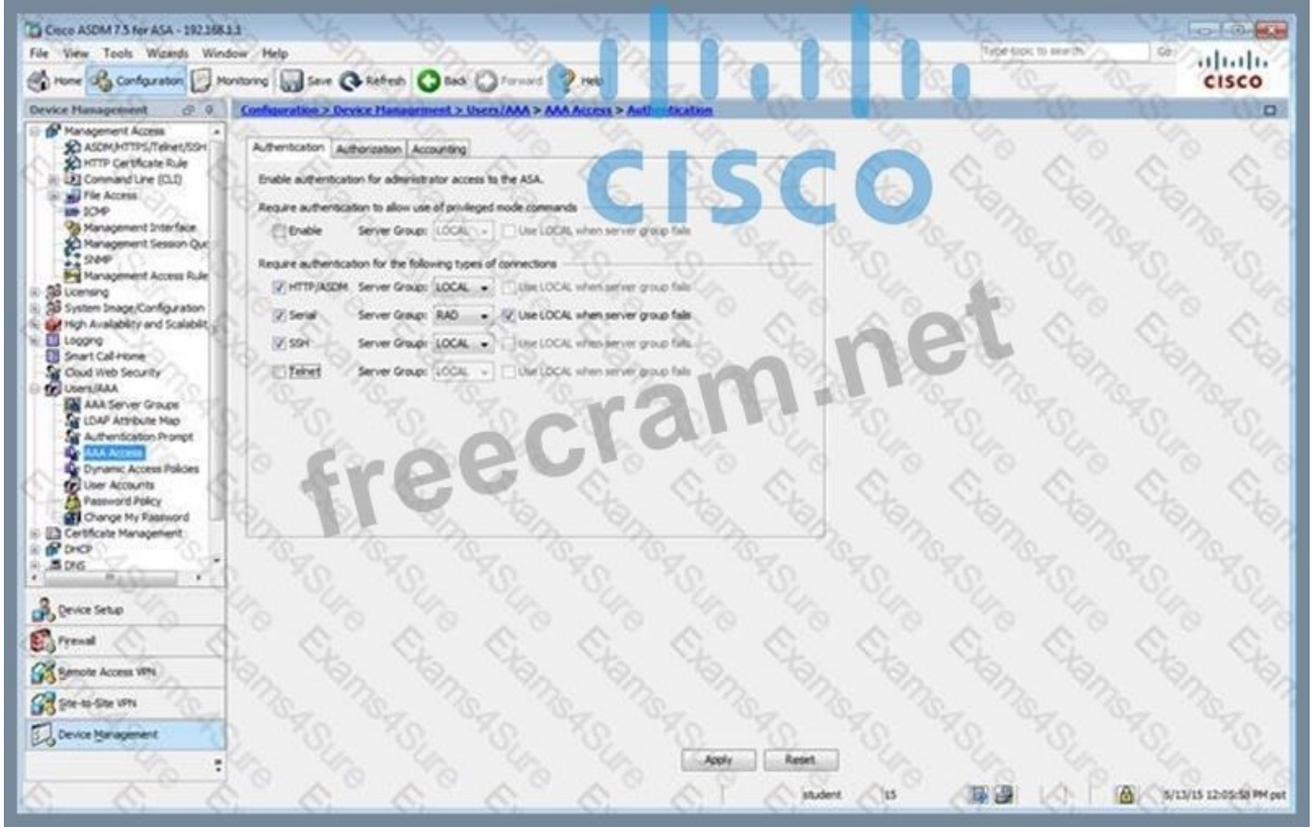


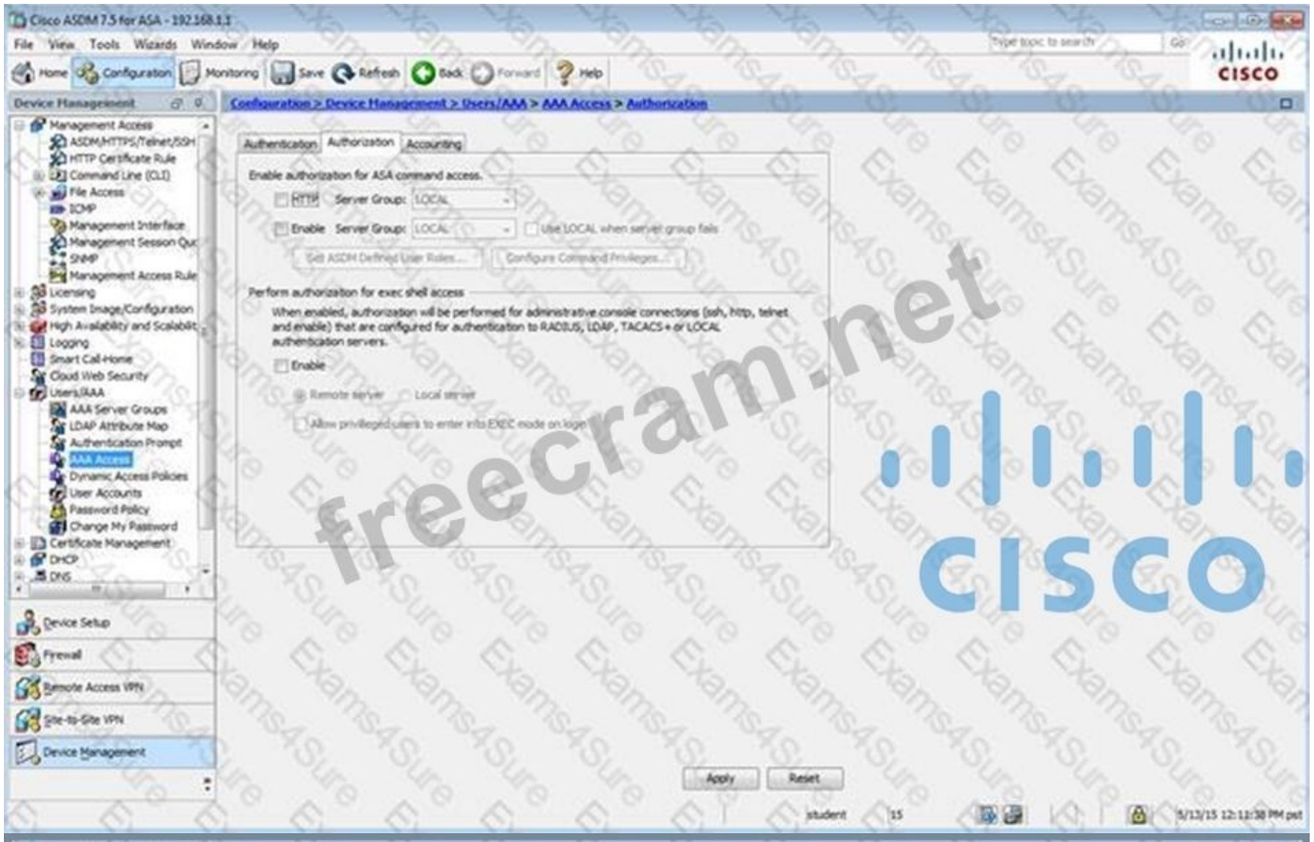



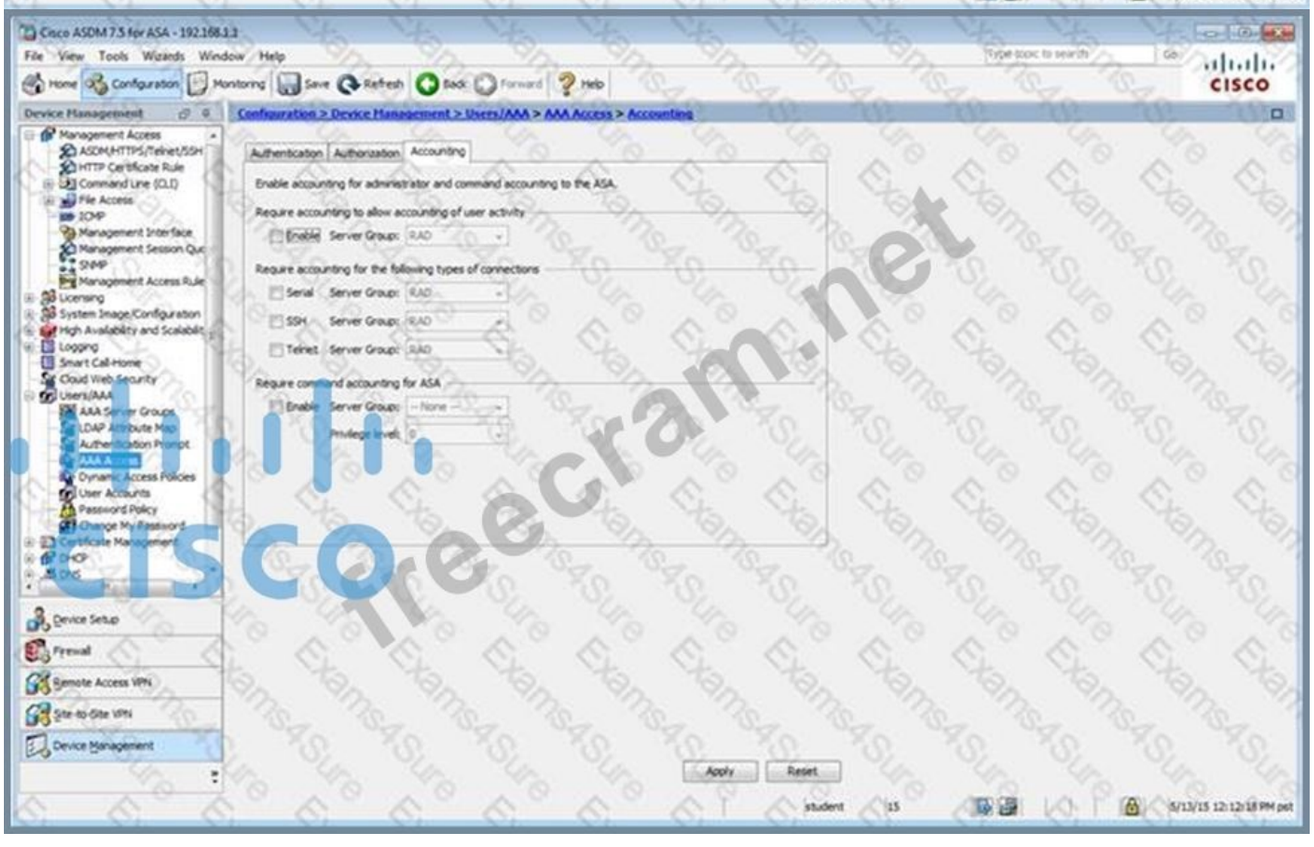



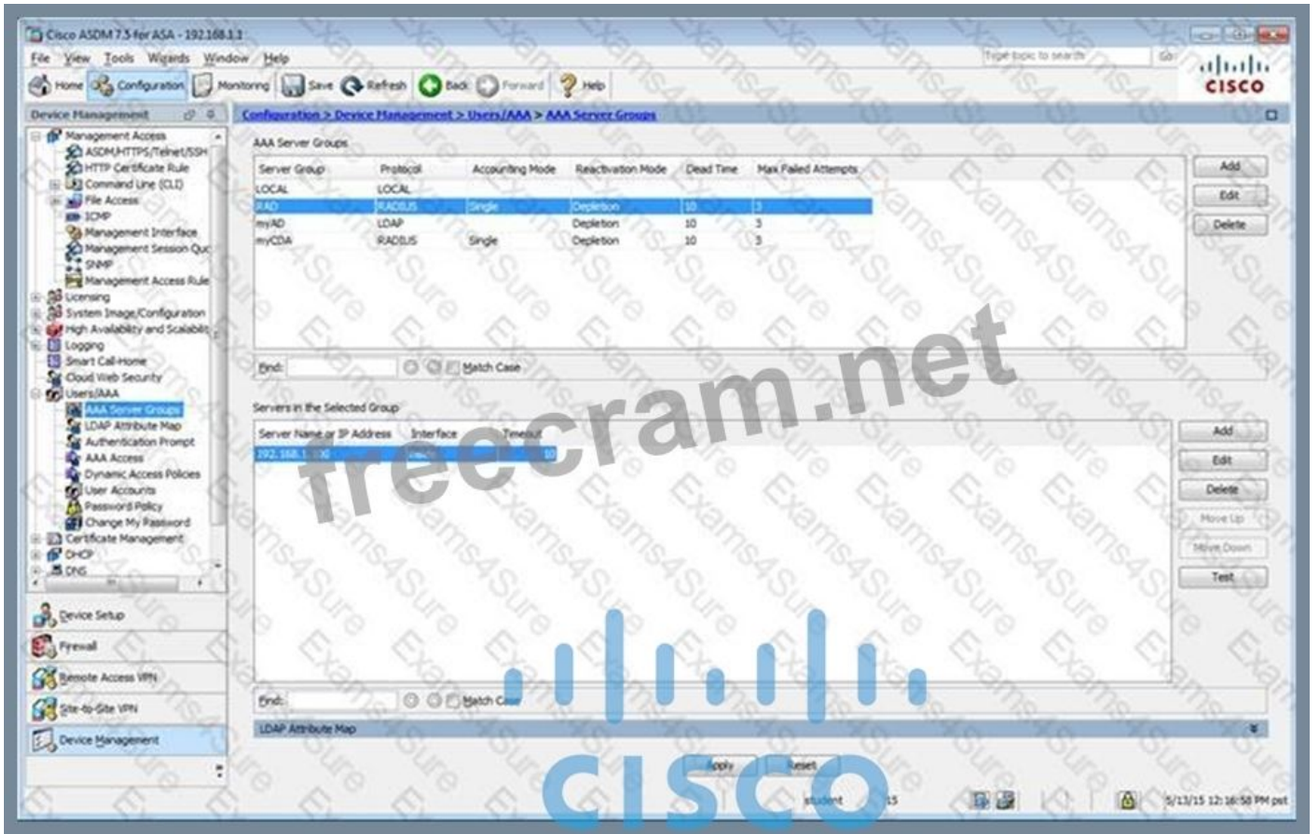


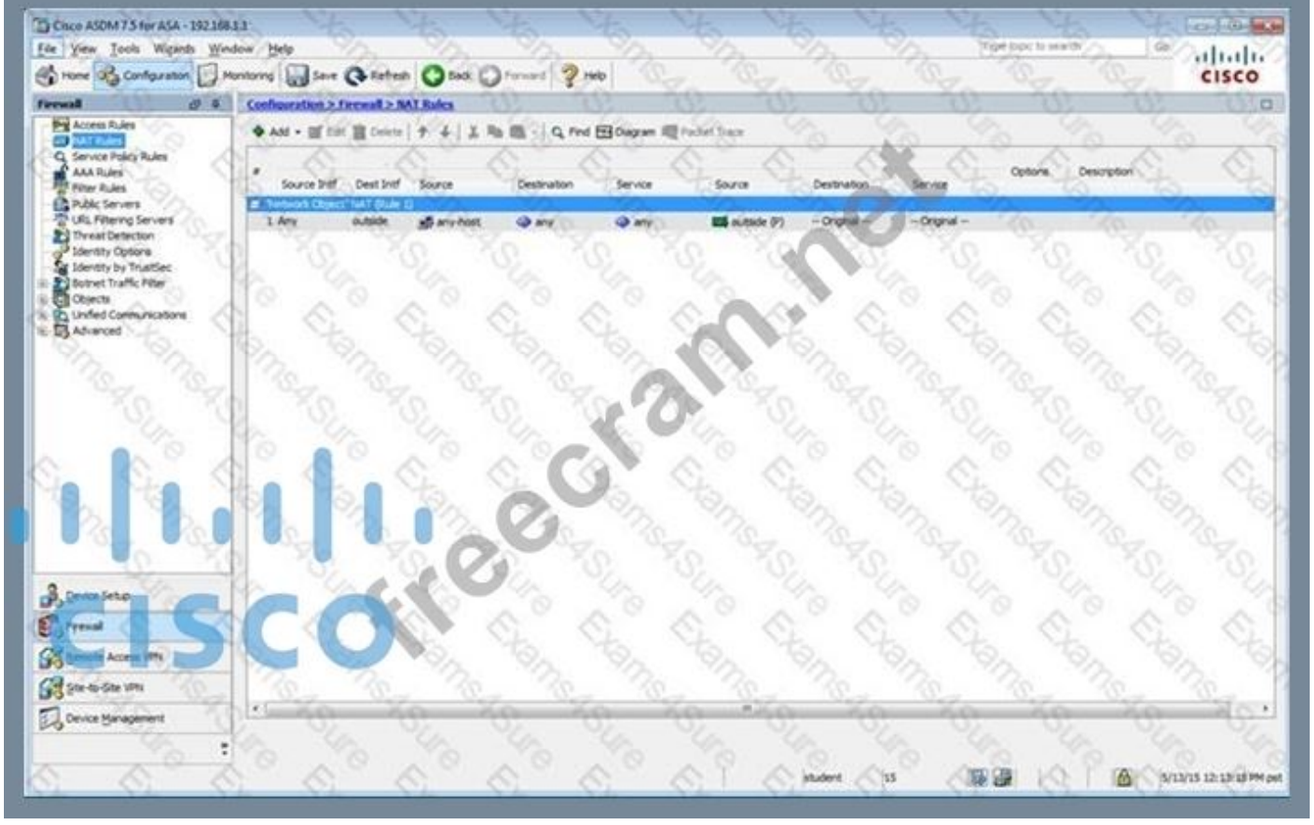


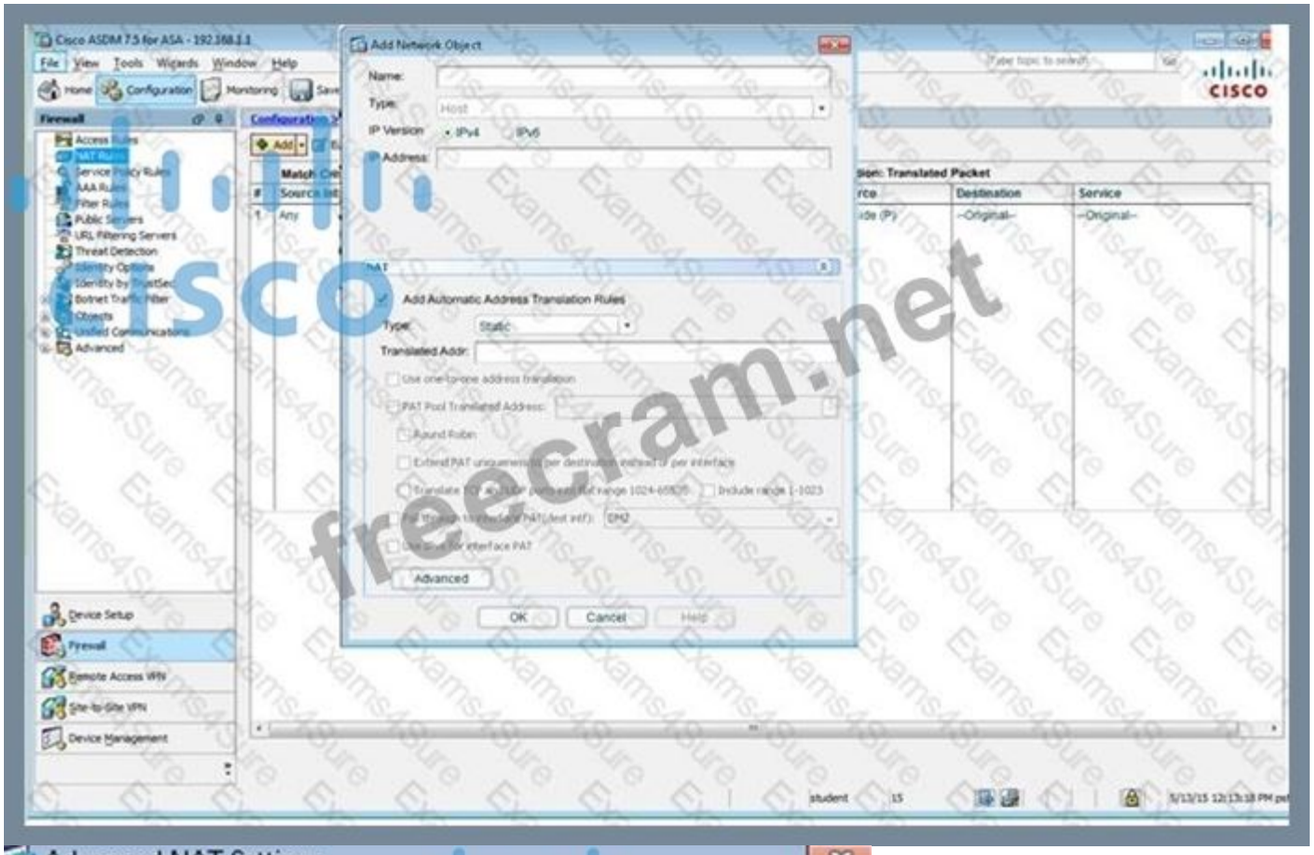



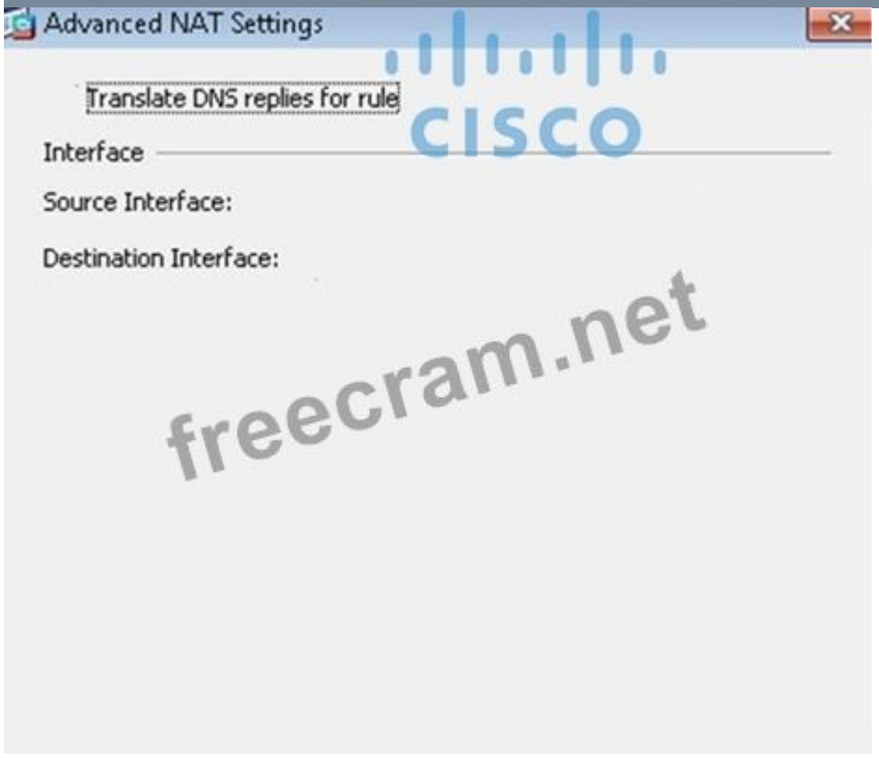


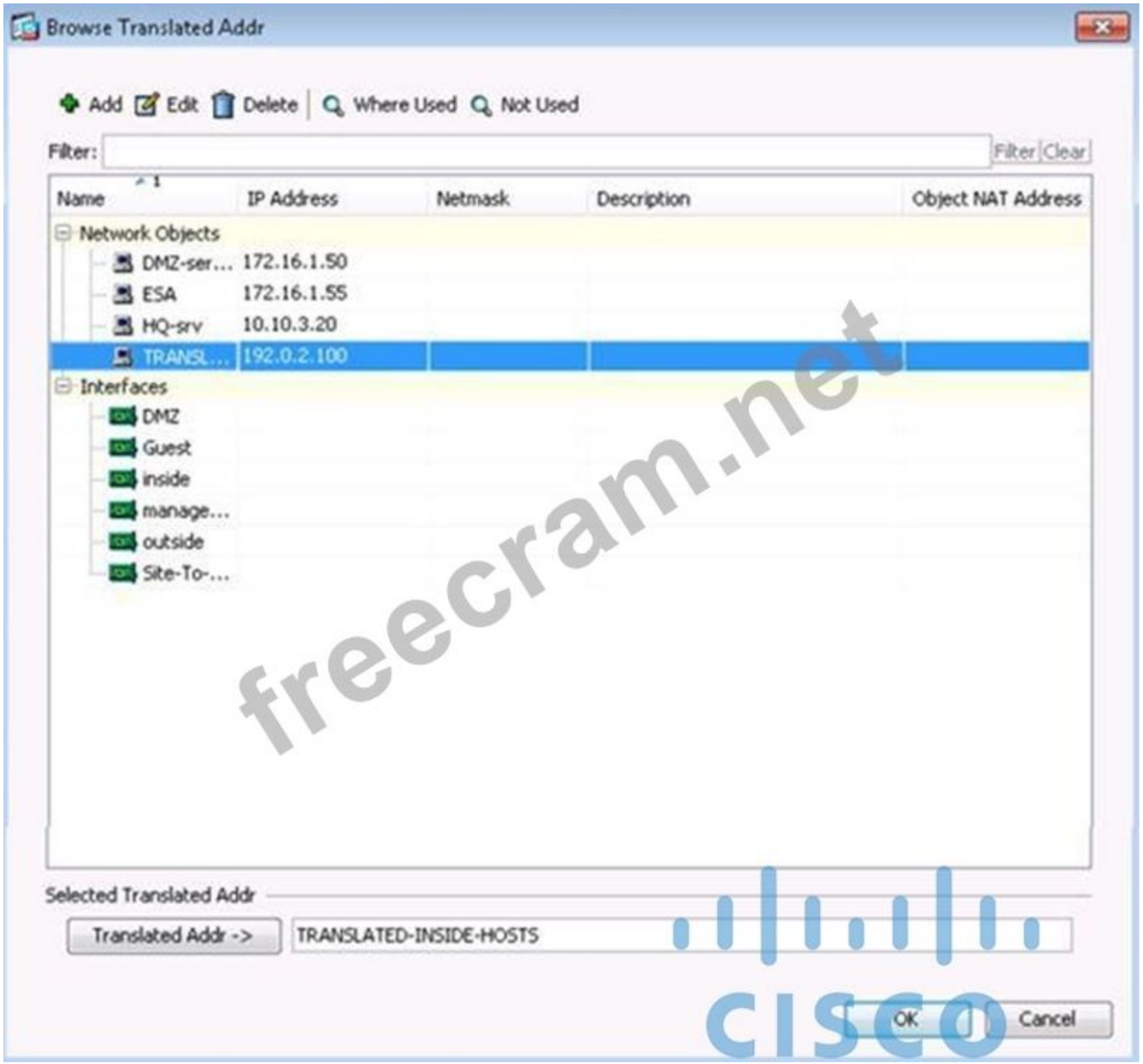



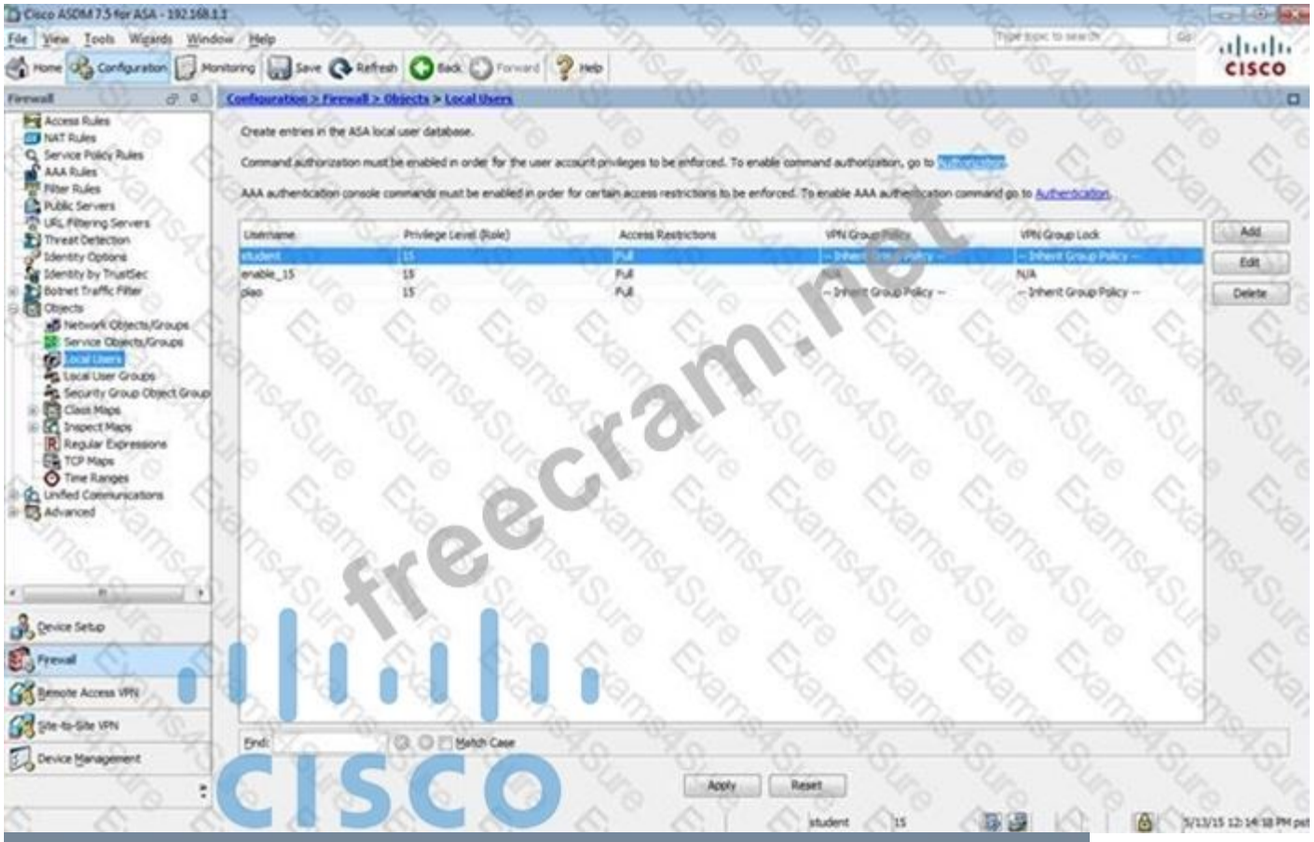


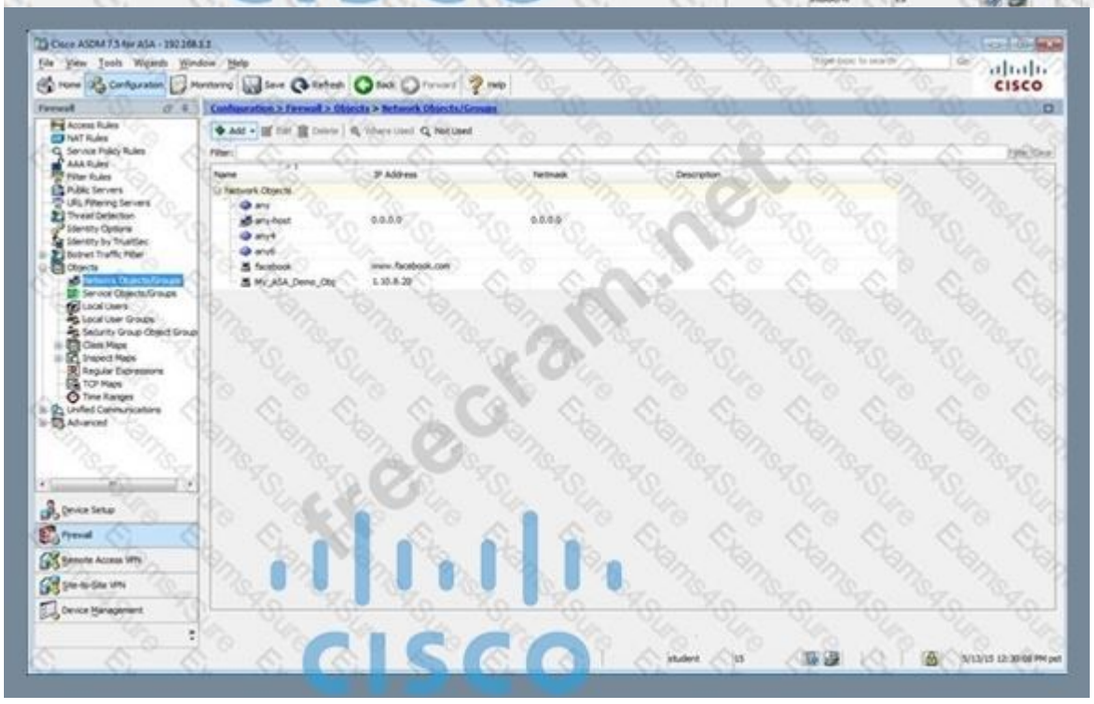



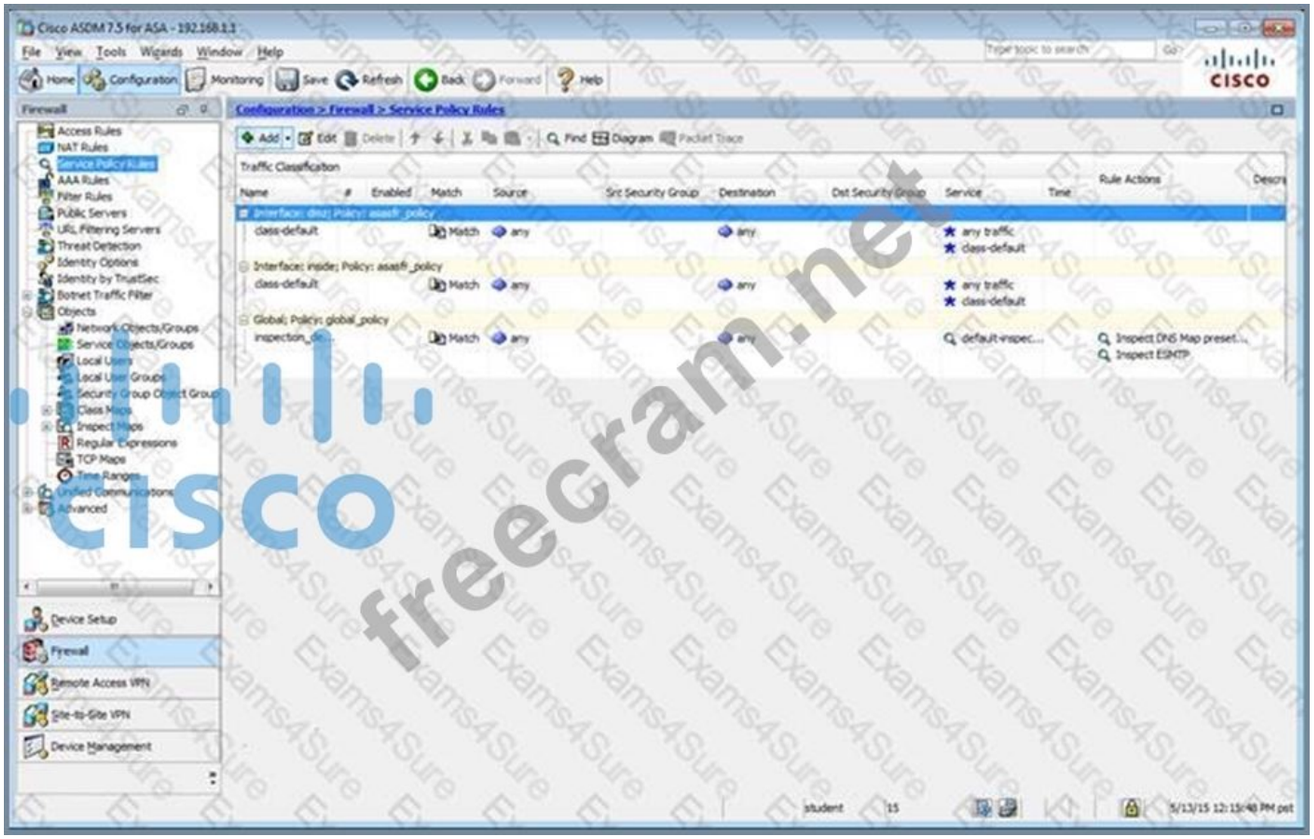


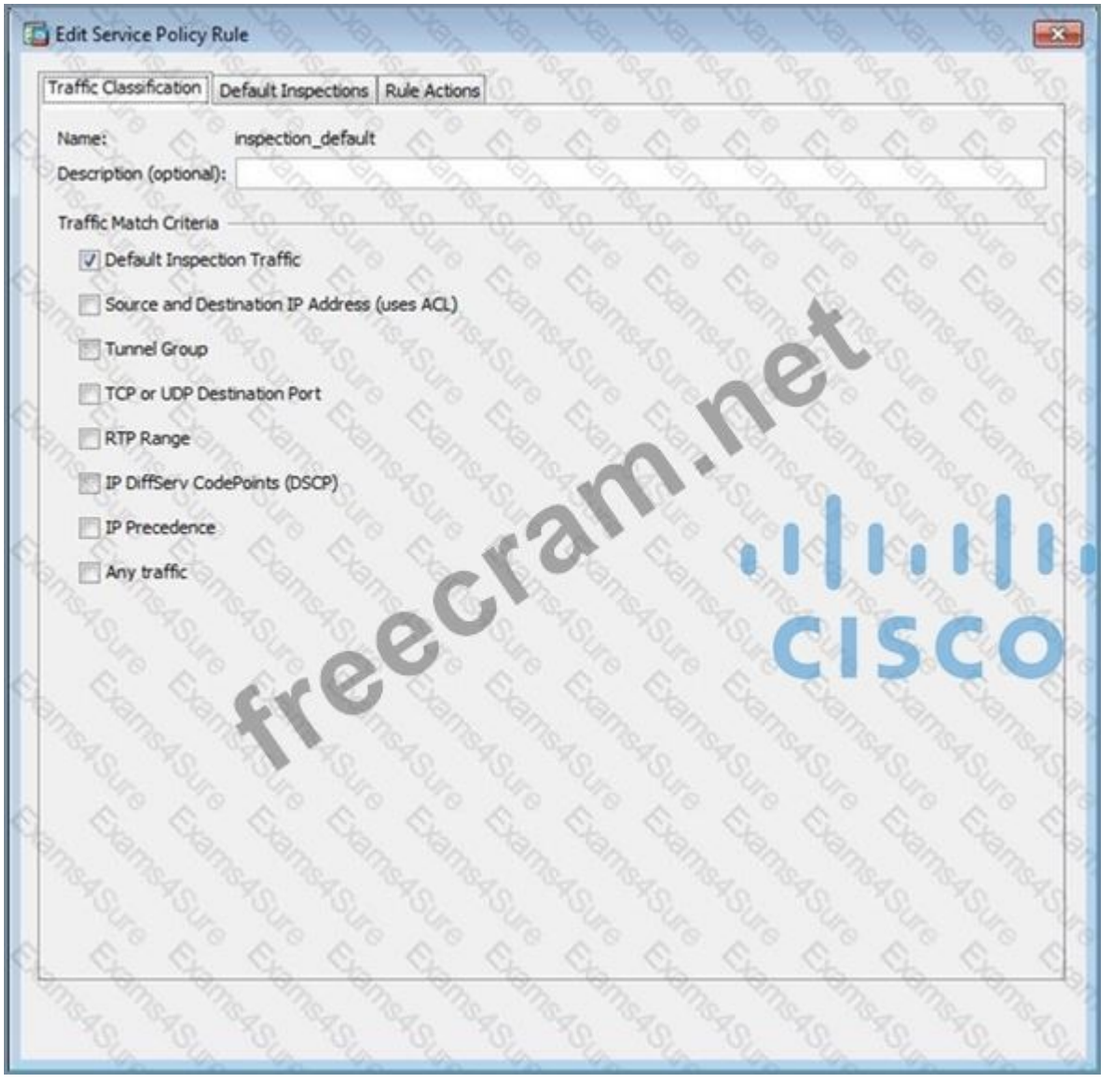



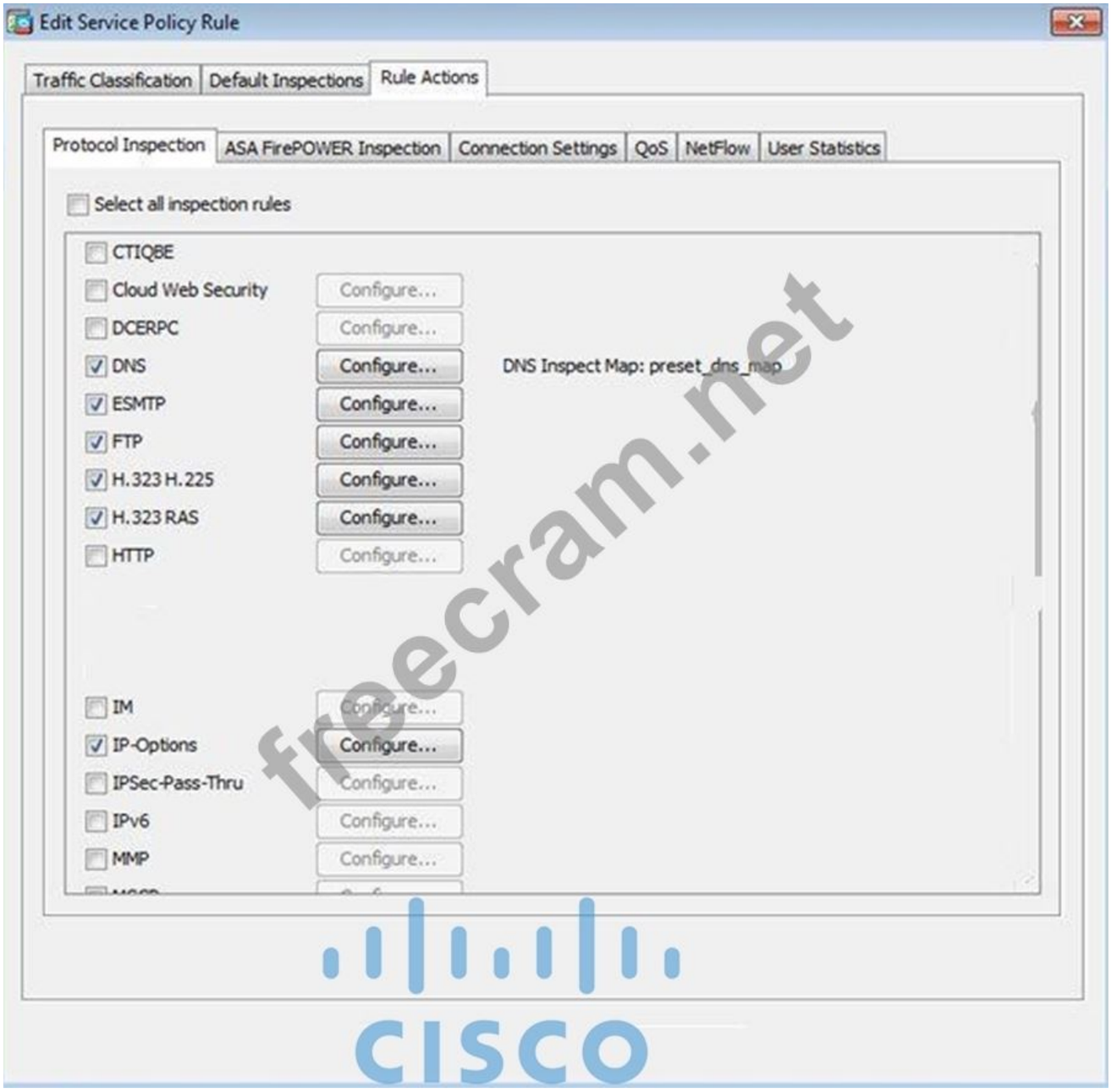


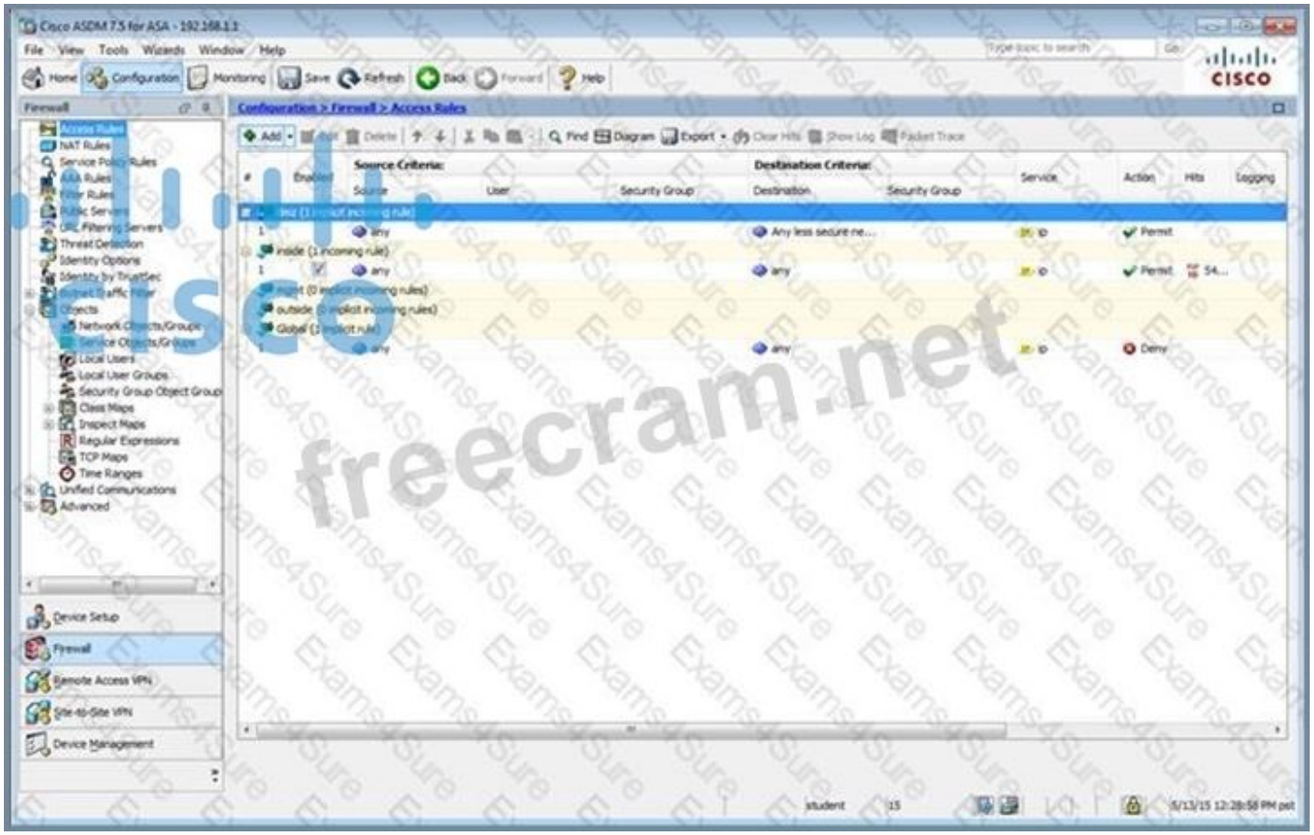

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user 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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
freecram.net
Exams4Sure

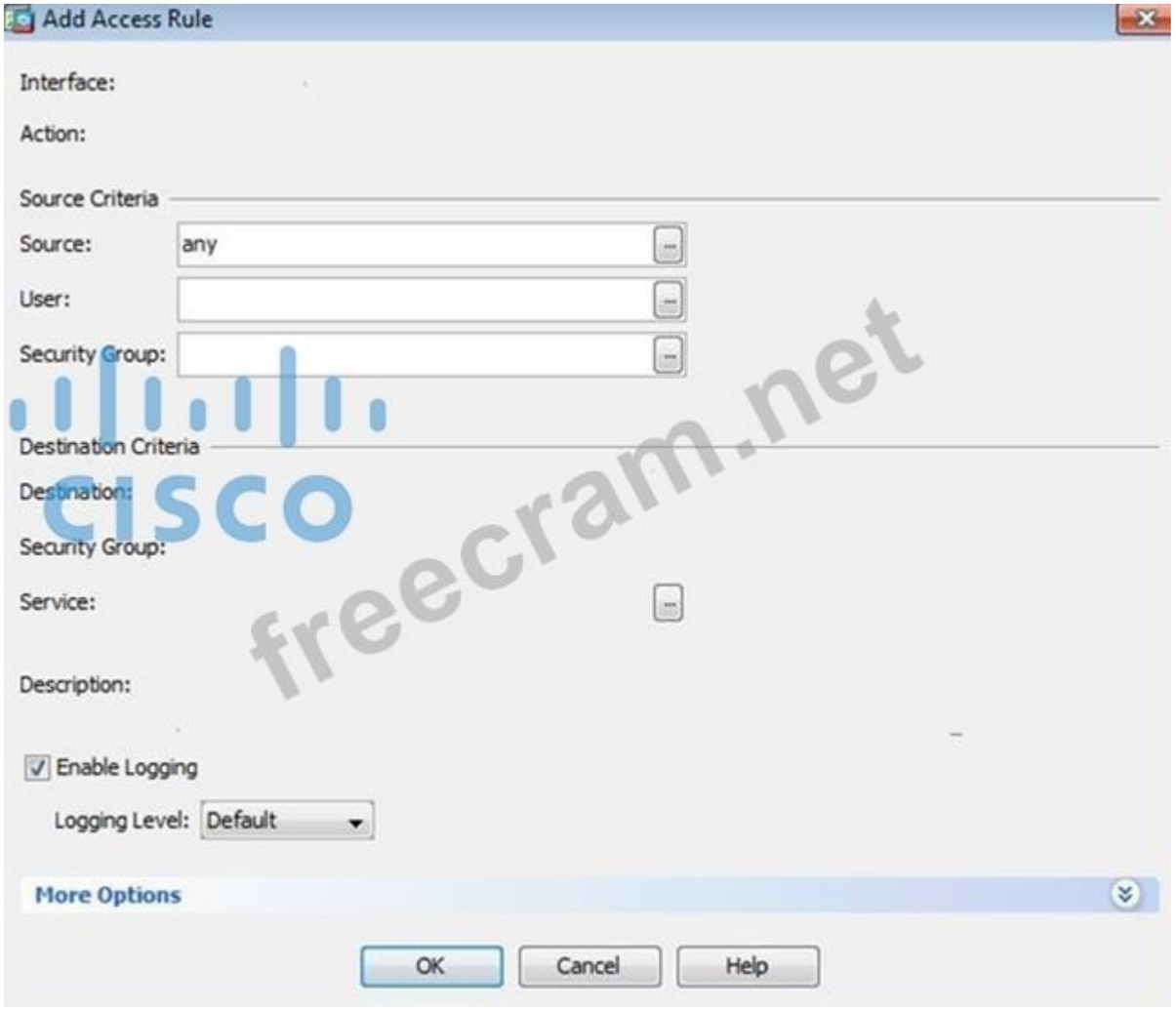

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Network Objects/Groups
Add
Edit
Delete
Where Used
Not Used
Filter:
Name
IP Address
Netmask
Description
Network Objects
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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15
freecram.net
Exams4Sure

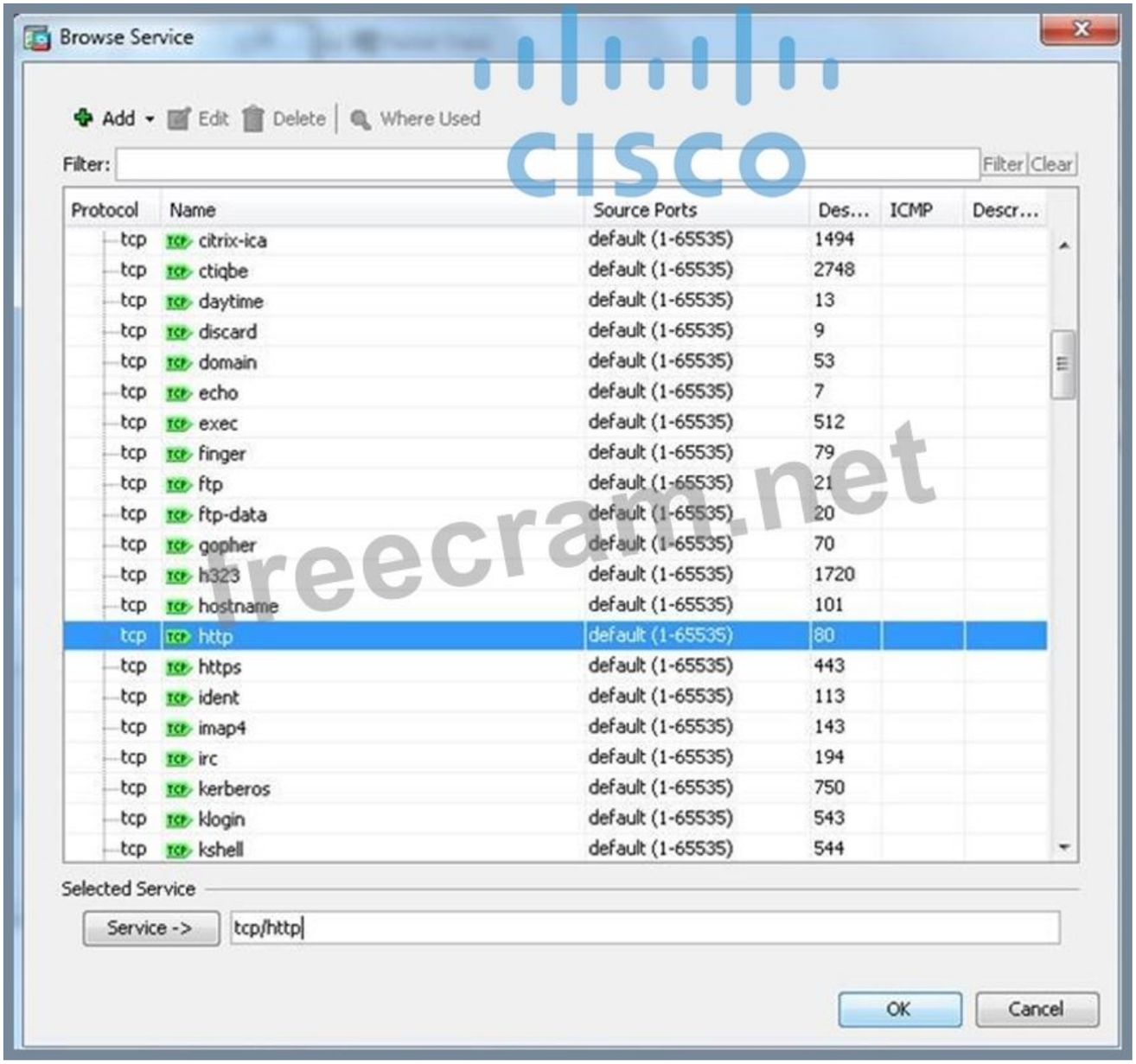

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Firewall
Configuration > Firewall > Service Policy Rules
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
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: inside; Policy: asafi_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
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student 15
5/13/15 12:15:48 PM pst

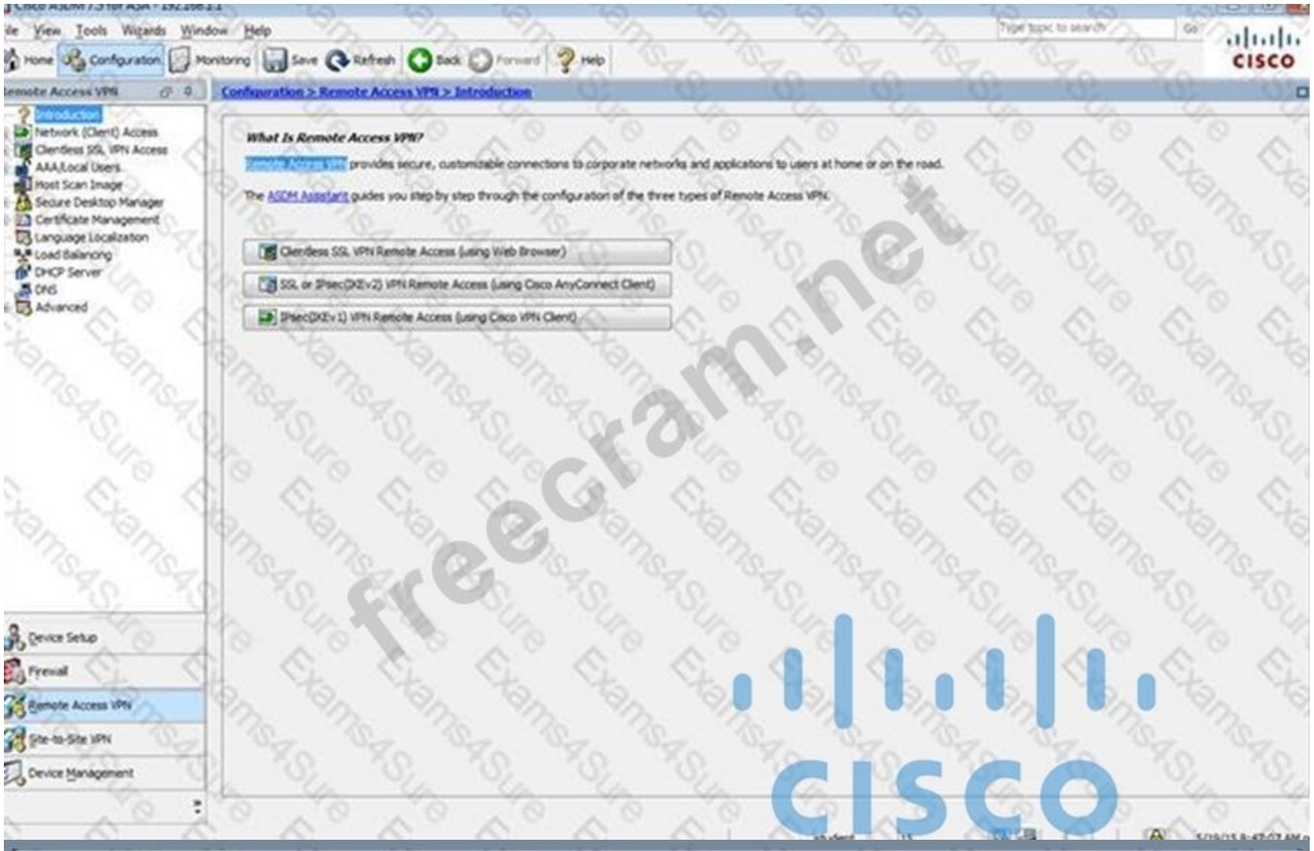

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Name:
inspection_default
Description (optional):
Traffic Match Criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
Tunnel Group
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)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

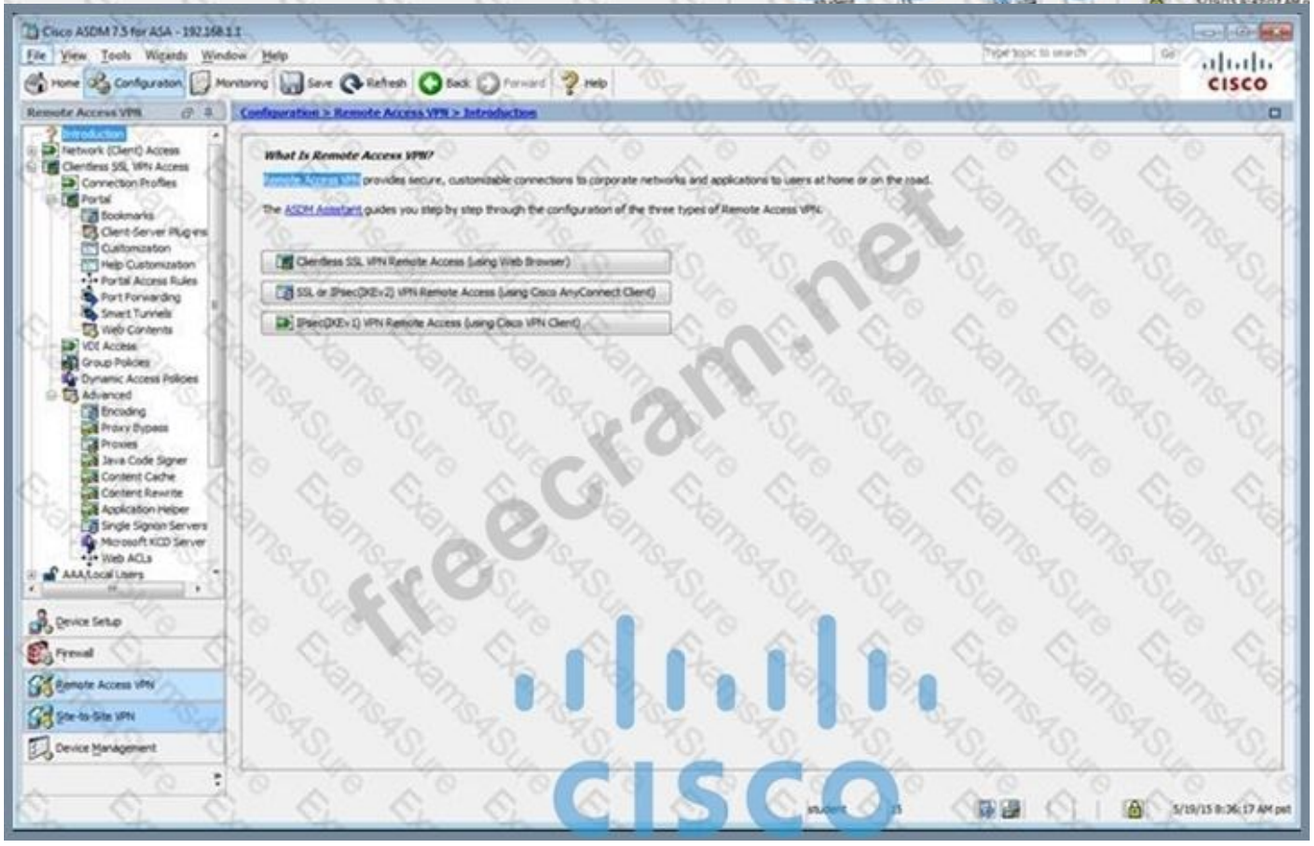

Edit Service Policy Rule
Traffic Classification
Default Inspections
Rule Actions
Protocol Inspection
ASA FirePOWER Inspection
Connection Settings
QoS
NetFlow
User Statistics
Select all inspection rules
CTIQBE
Cloud Web Security
Configure...
DCERPC
Configure...
DNS
Configure...
DNS Inspect Map: preset_dns_map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


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 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
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
any
Any less secure ne...
ip
Permit
inside (1 incoming rule)
any
any
ip
Permit
outside (1 implicit incoming rules)
Global (1 implicit rule)
any
any
ip
Deny
student
15
5/13/15 12:28:58 PM pst

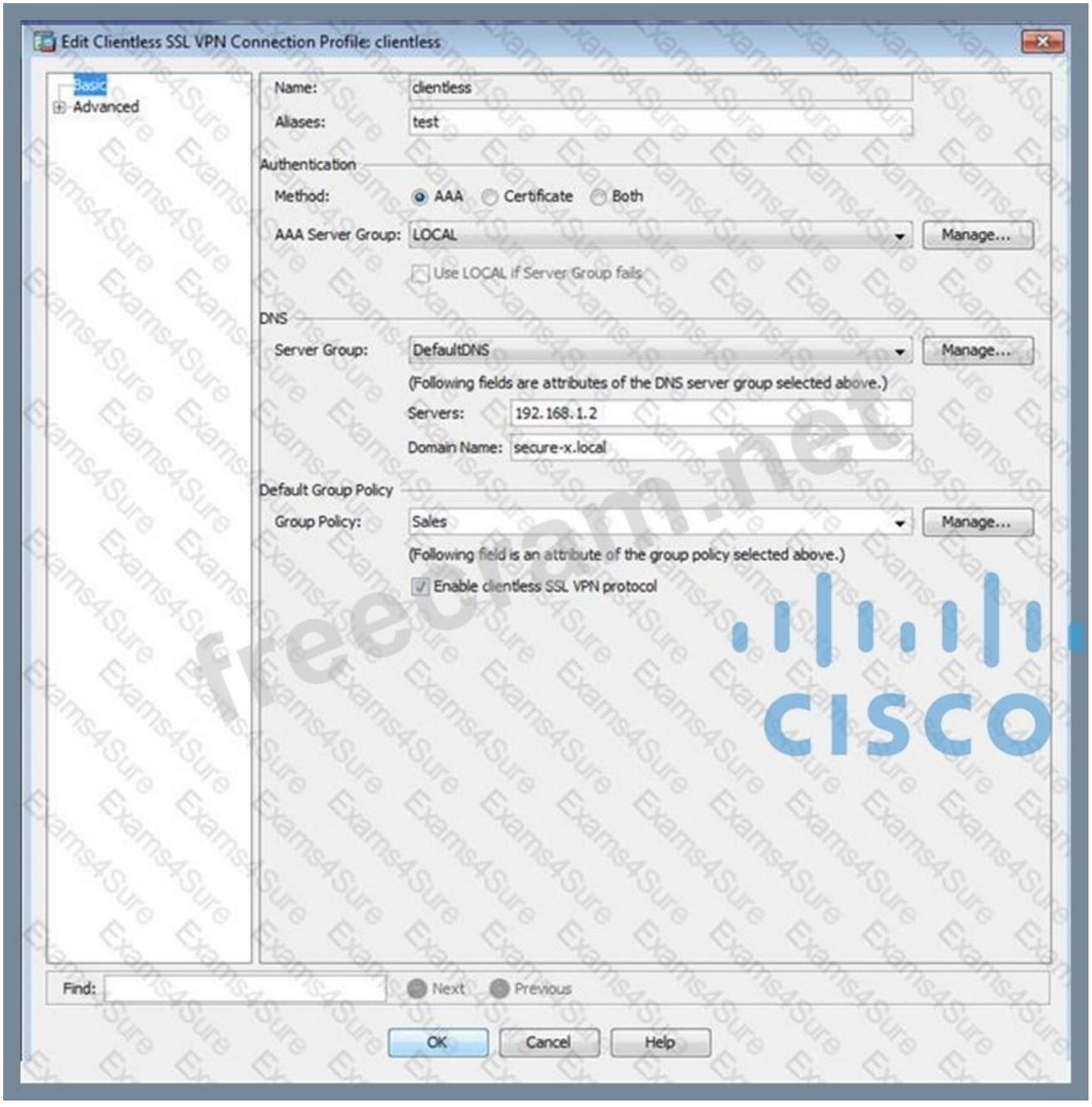


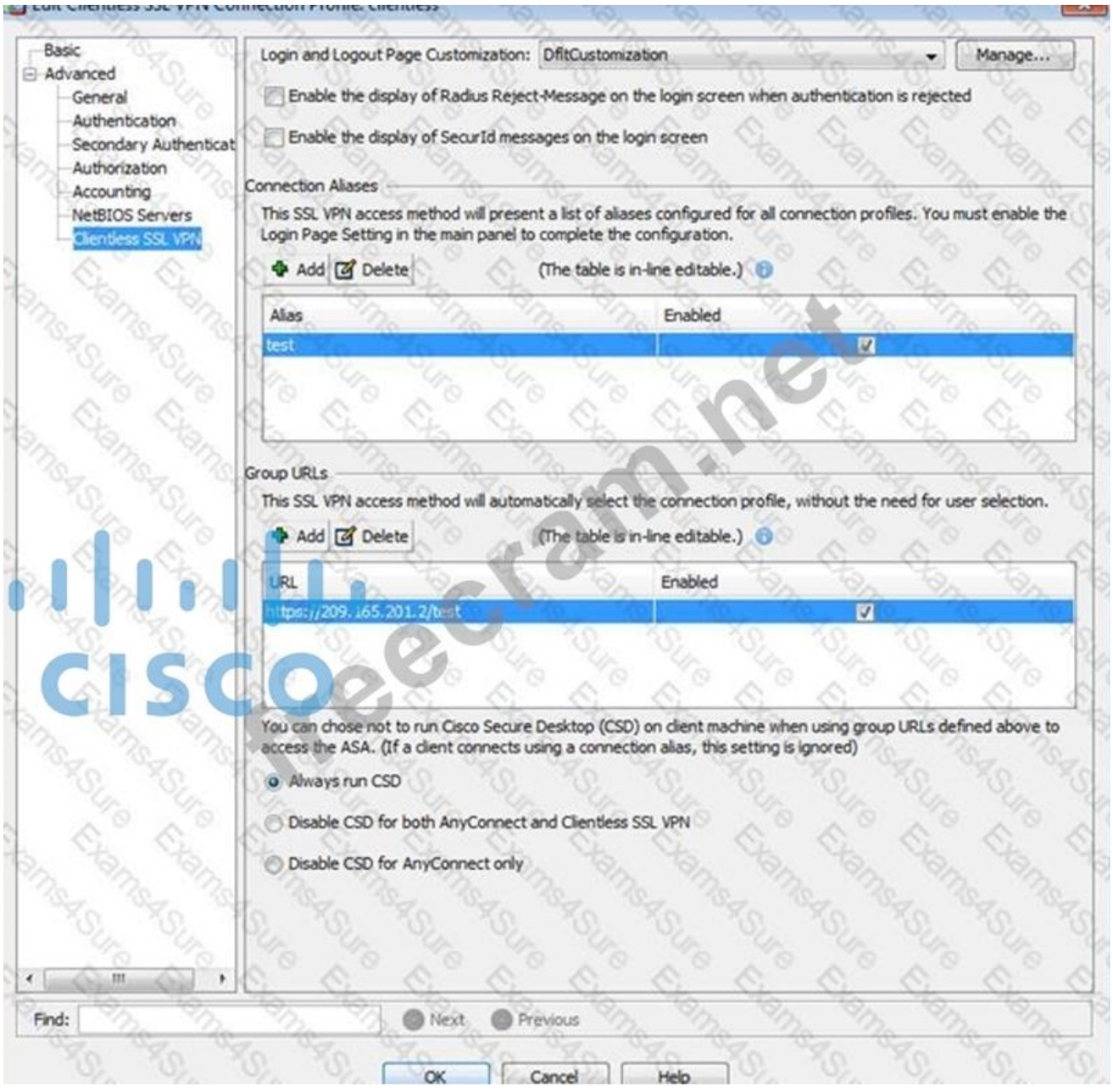


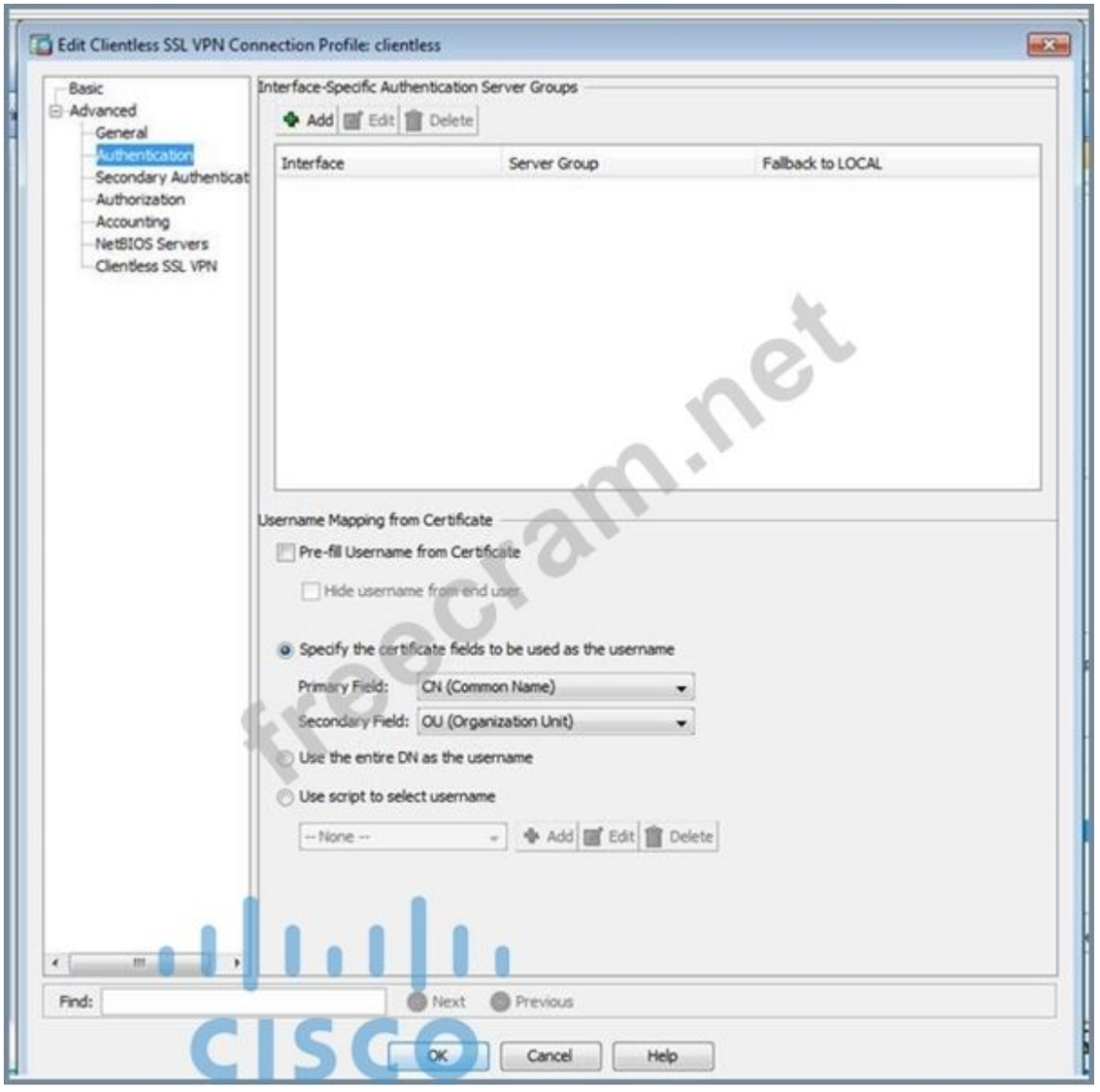

File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
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

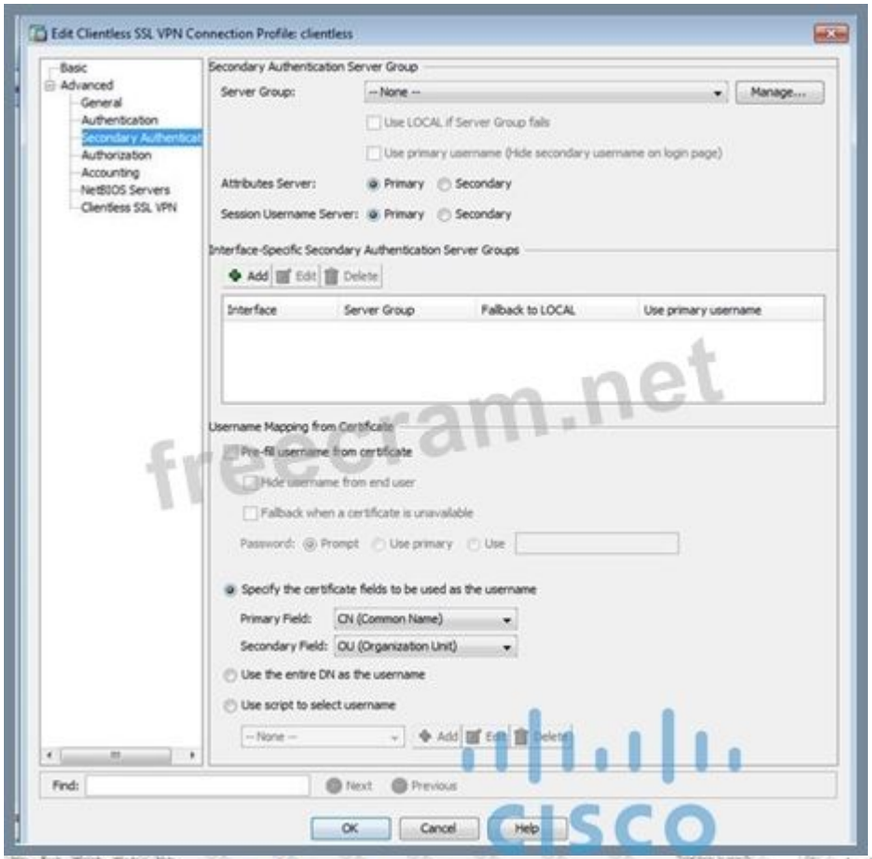

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
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
5/19/15 8:36:17 AM pst


Access Interfaces
Enable interfaces for clientless SSL VPN access.
Login Page Setting
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters.
Add
Edit
Delete
Find:
Match Case
Name
Enabled
Aliases
Authentication Method
Group Policy
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

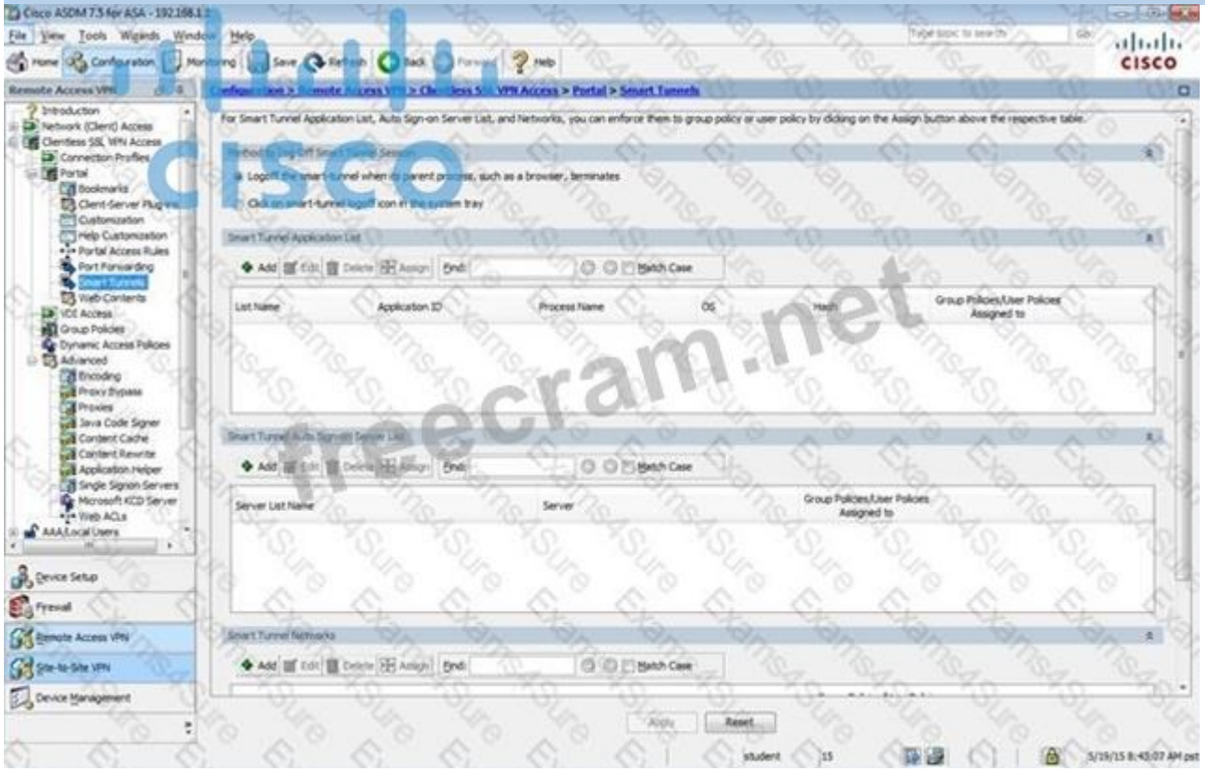

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server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

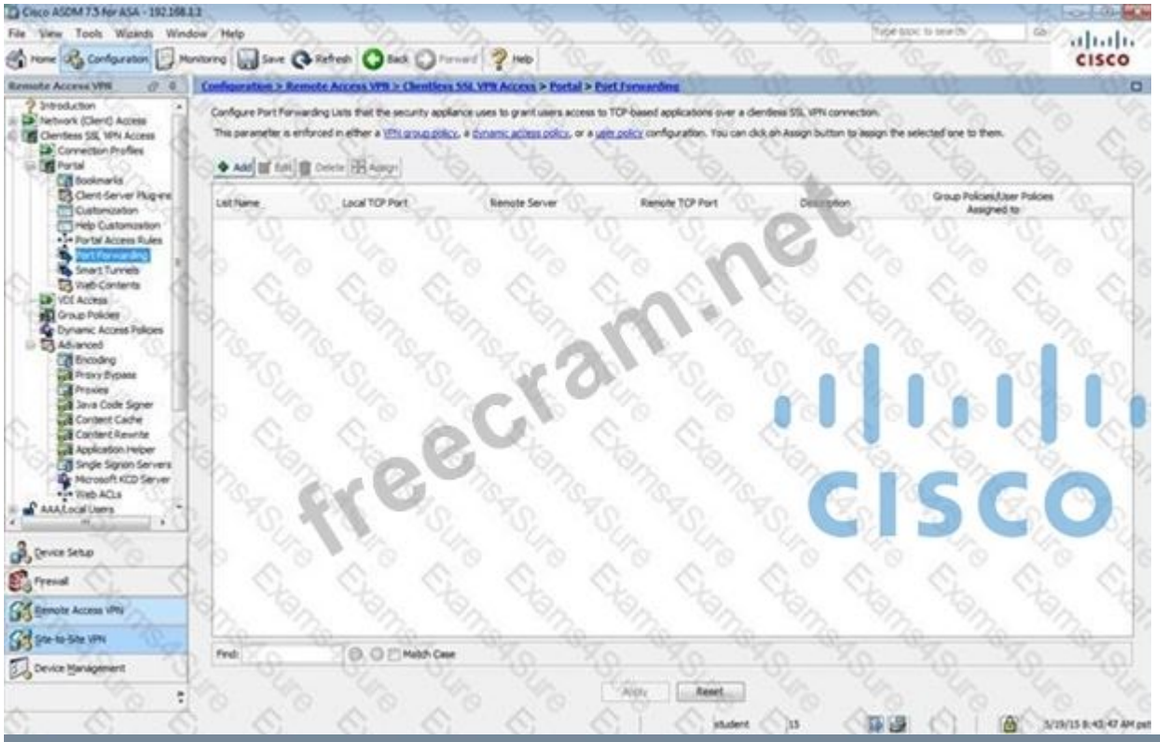

Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen when authentication is rejected
Enable the display of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

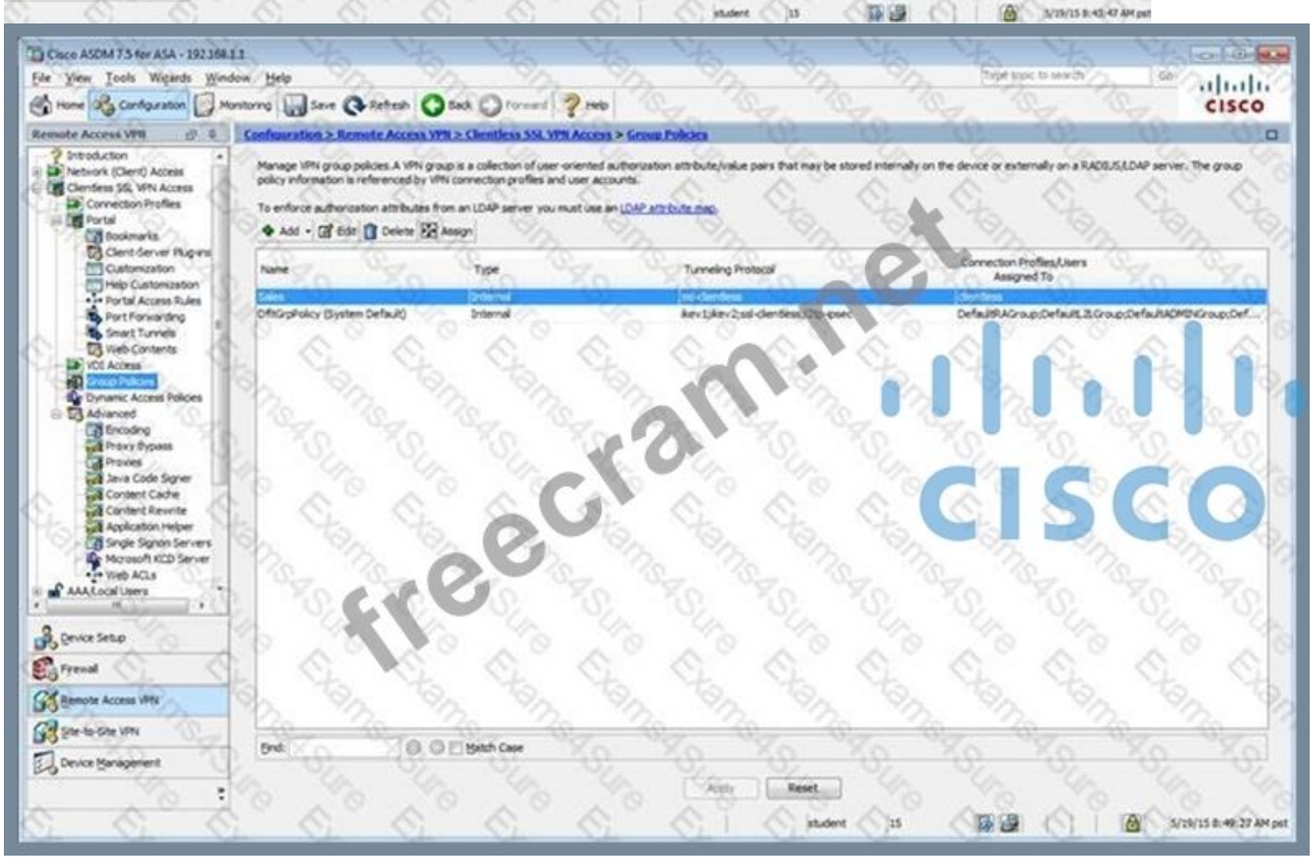


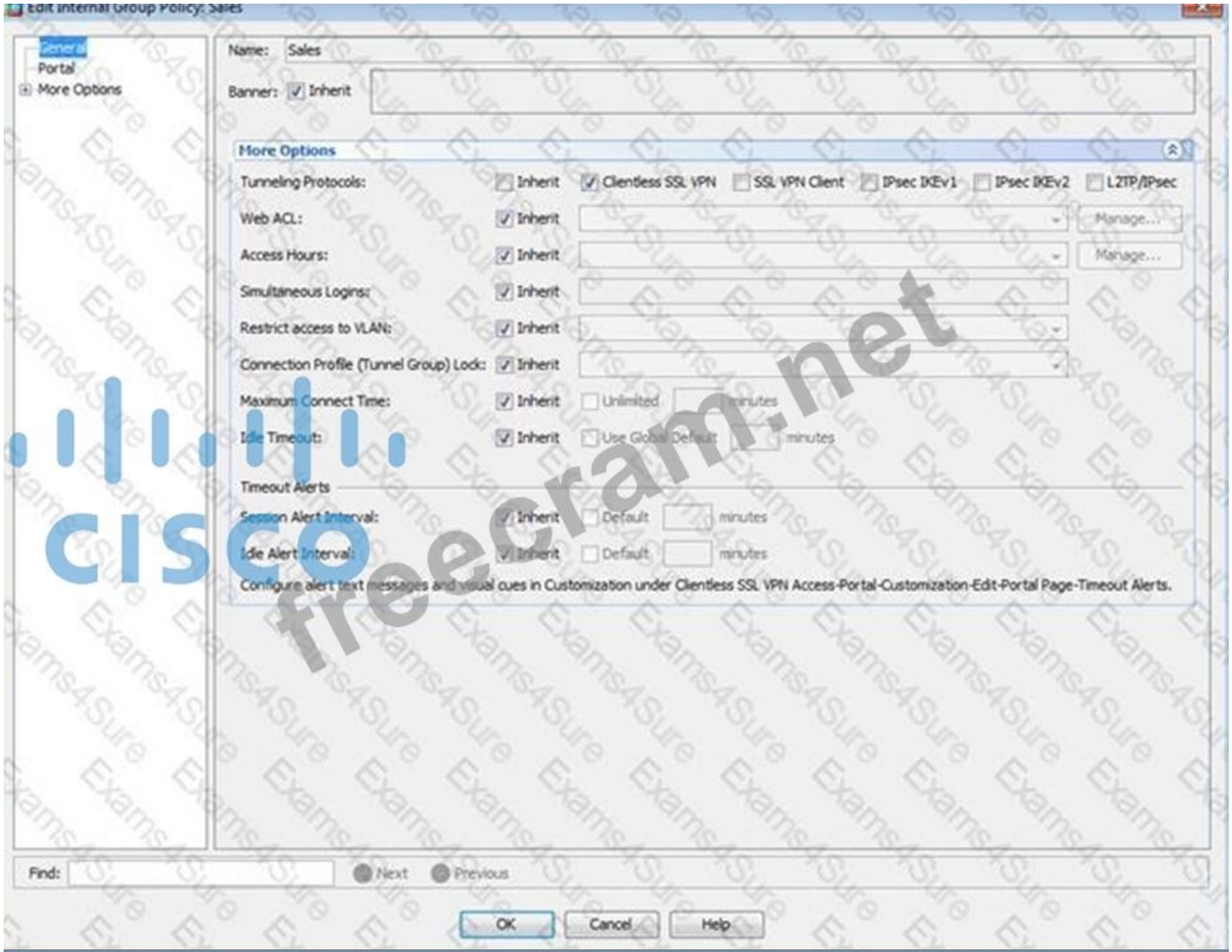


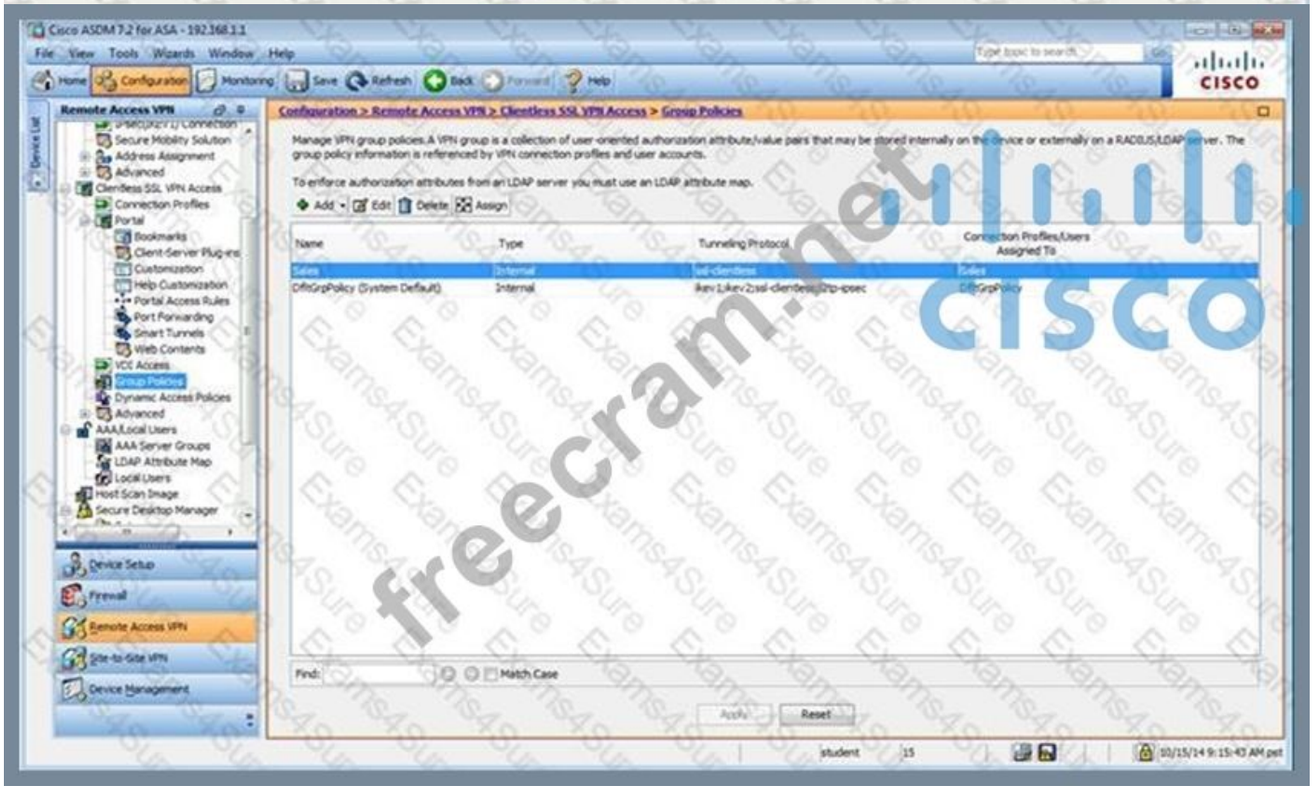


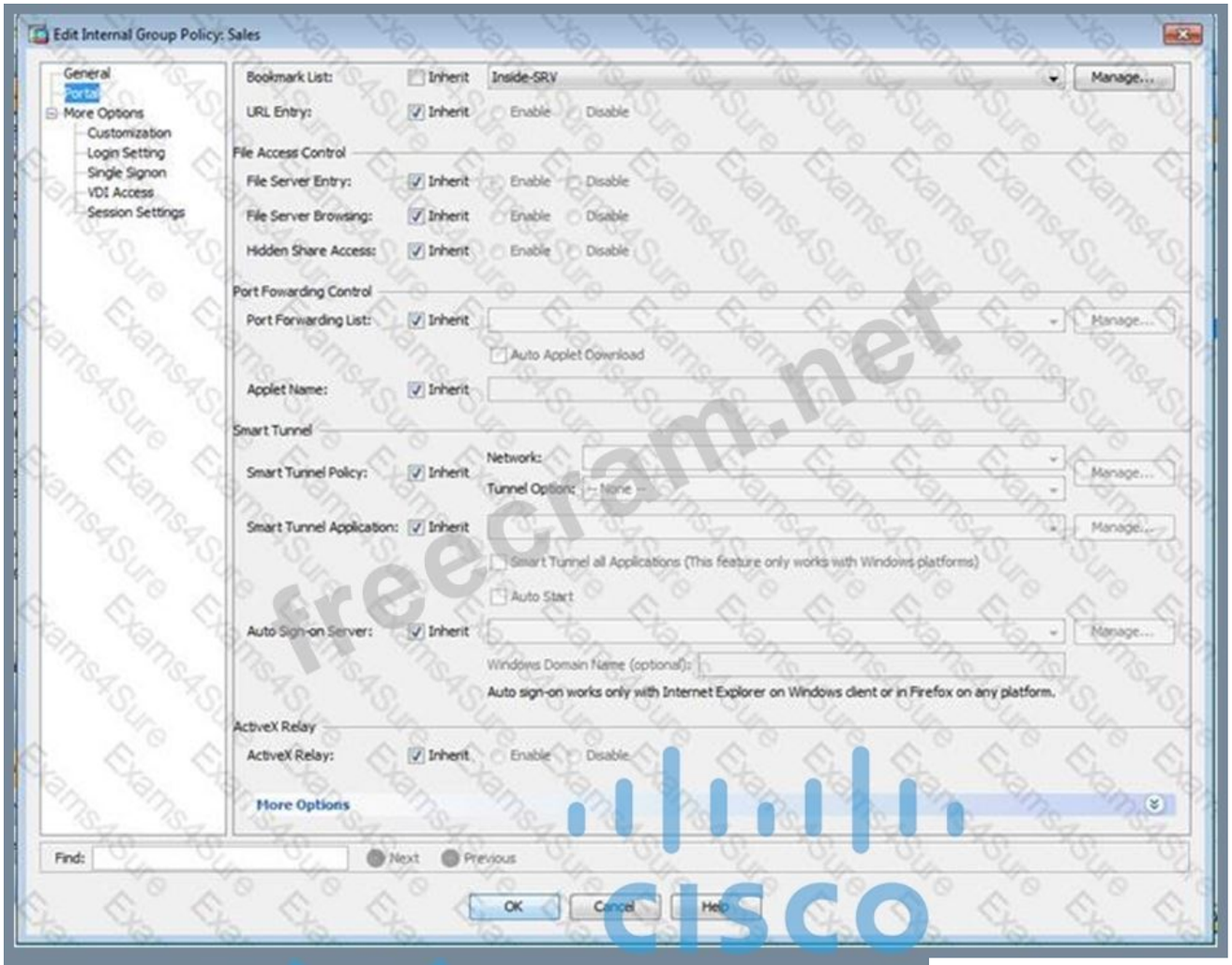


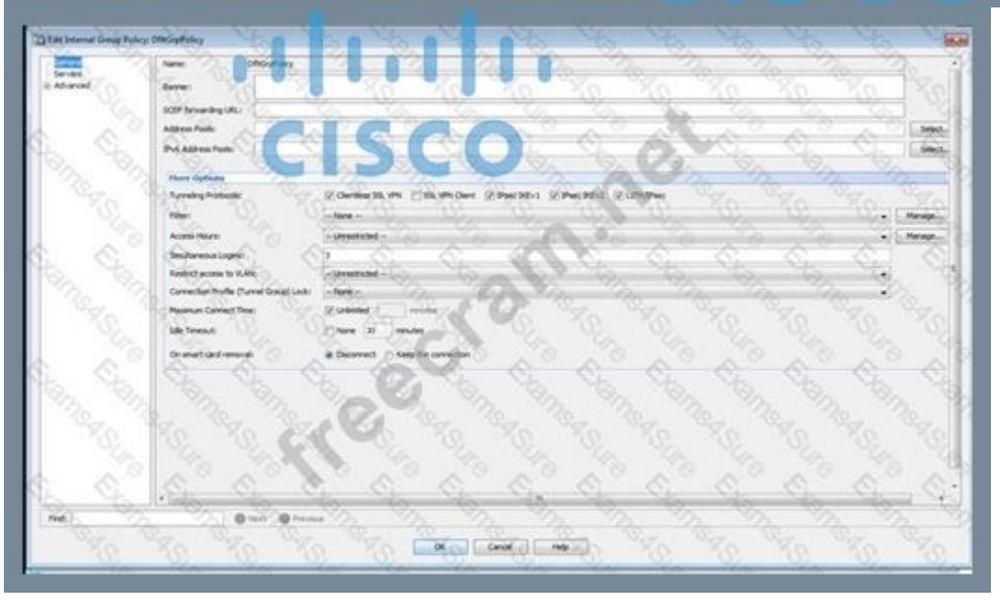

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Configure Port Forwarding Lists that the security appliance 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 8:45:47 AM pst
freecram.net

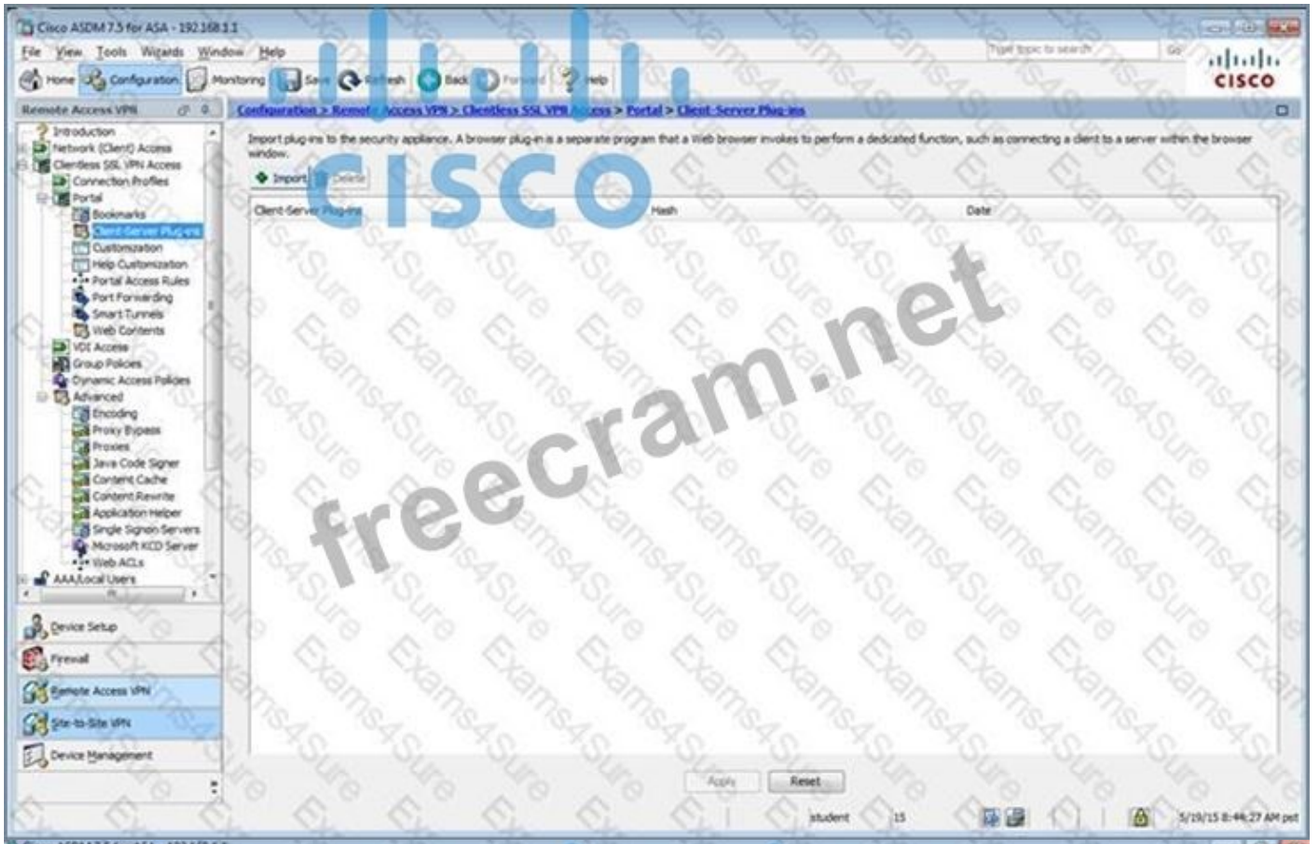

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented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

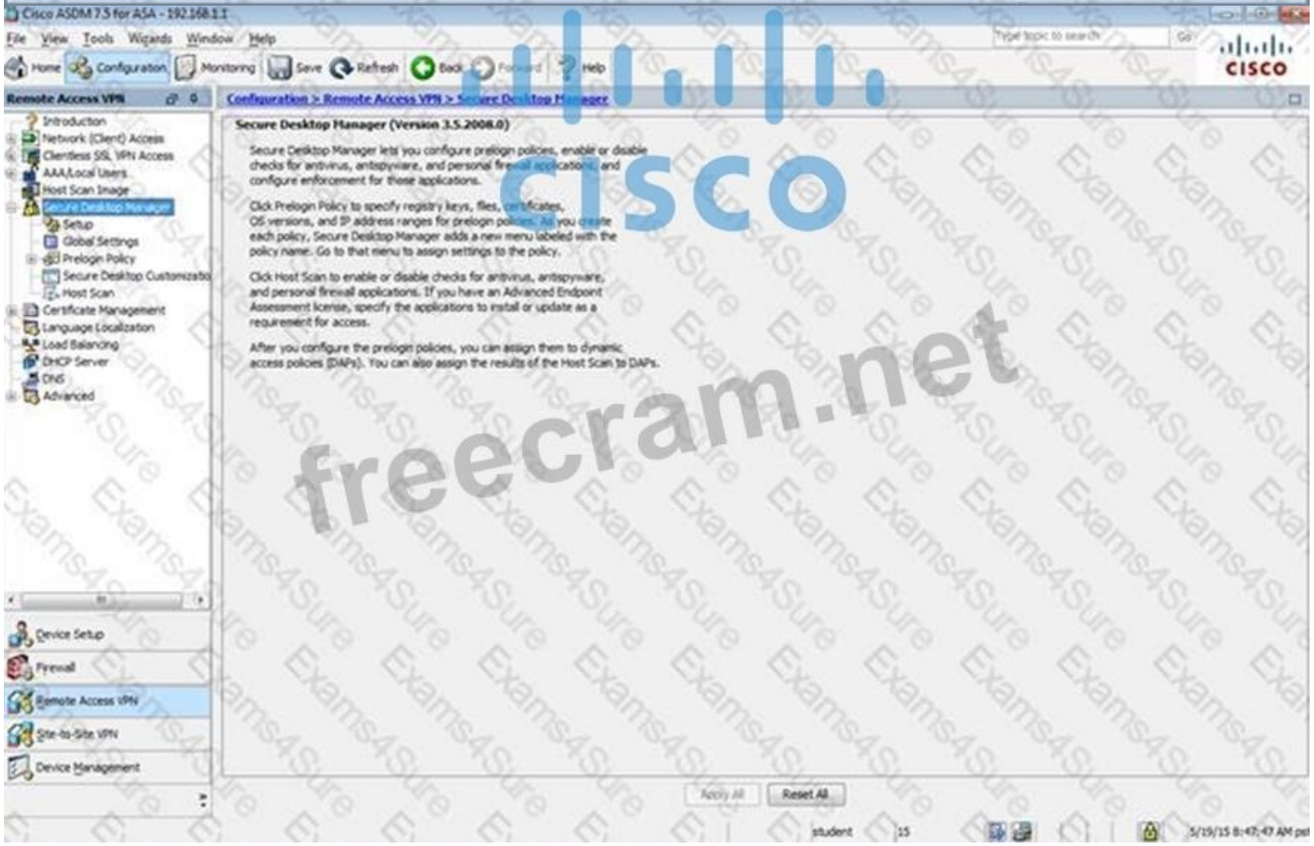


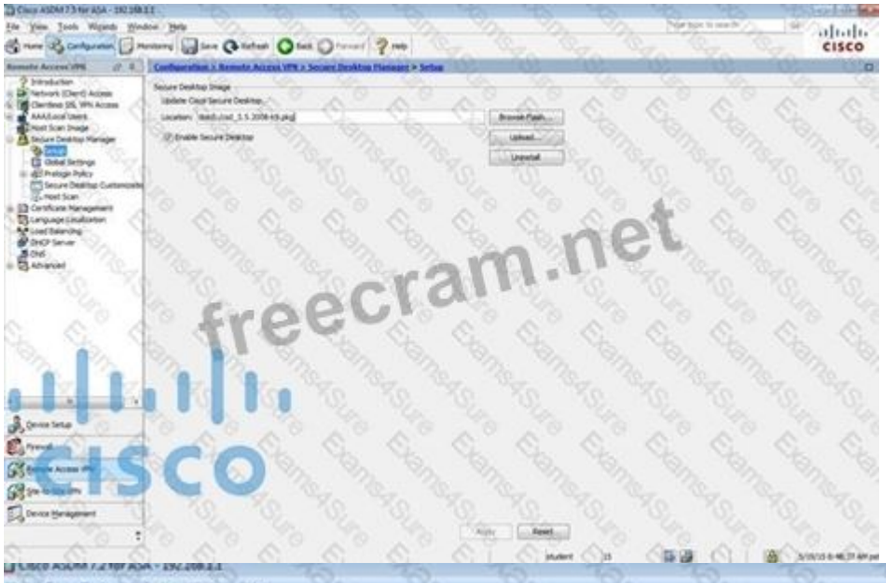



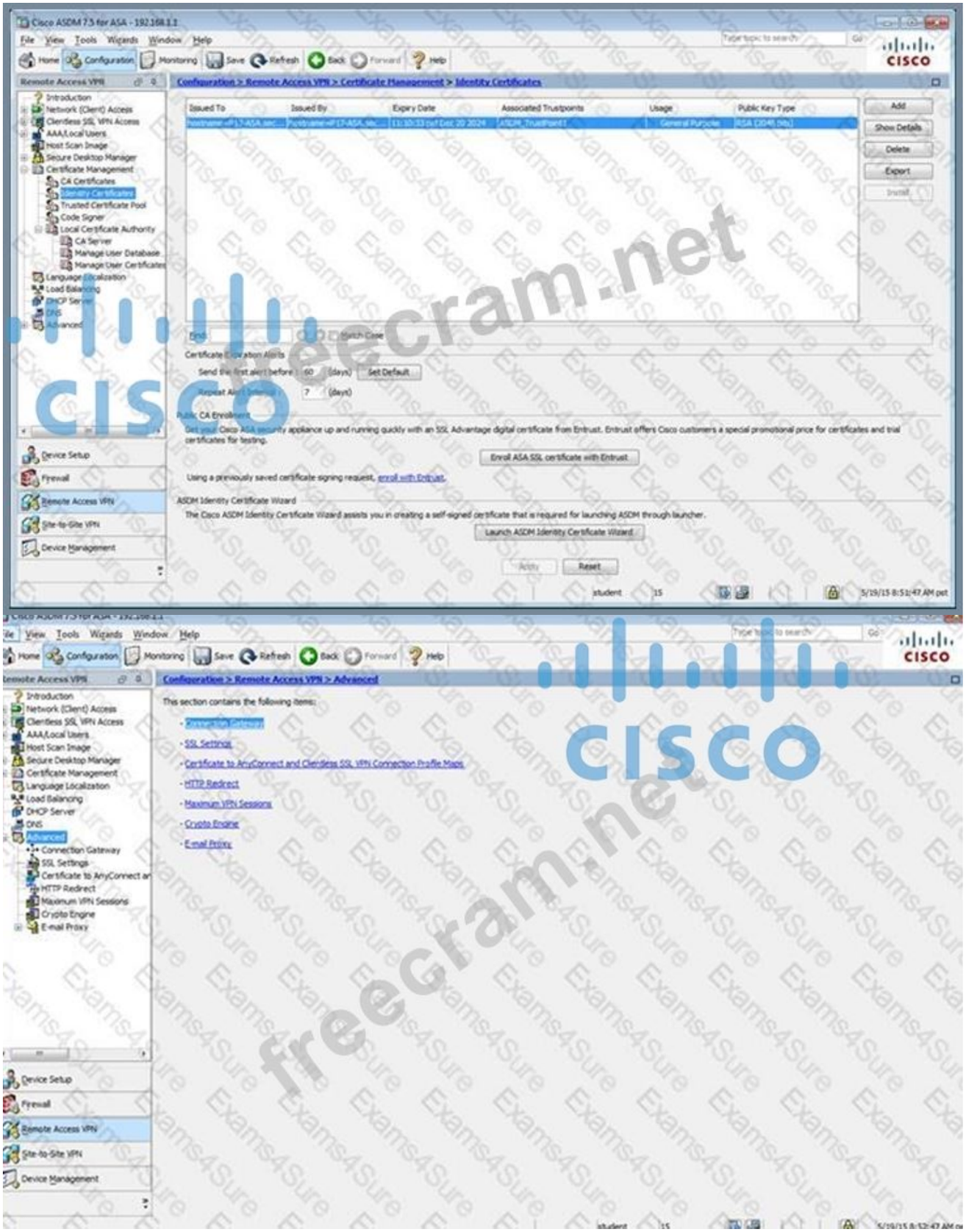

Edit Internal Group Policy: Sales
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Bookmark List:
Inherit
Inside-SRV
Manage...
URL Entry:
Inherit
Enable
Disable
File Access Control
File Server Entry:
File Server Browsing:
Hidden Share Access:
Port Fowarding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



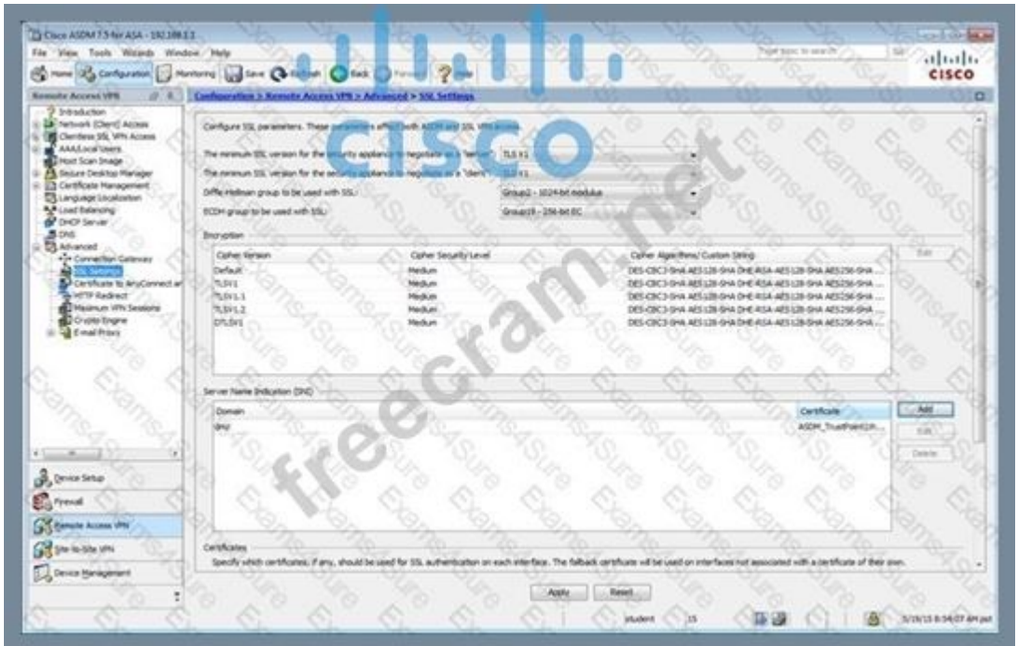

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins
Introduction
Network (Client) Access
Clientless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

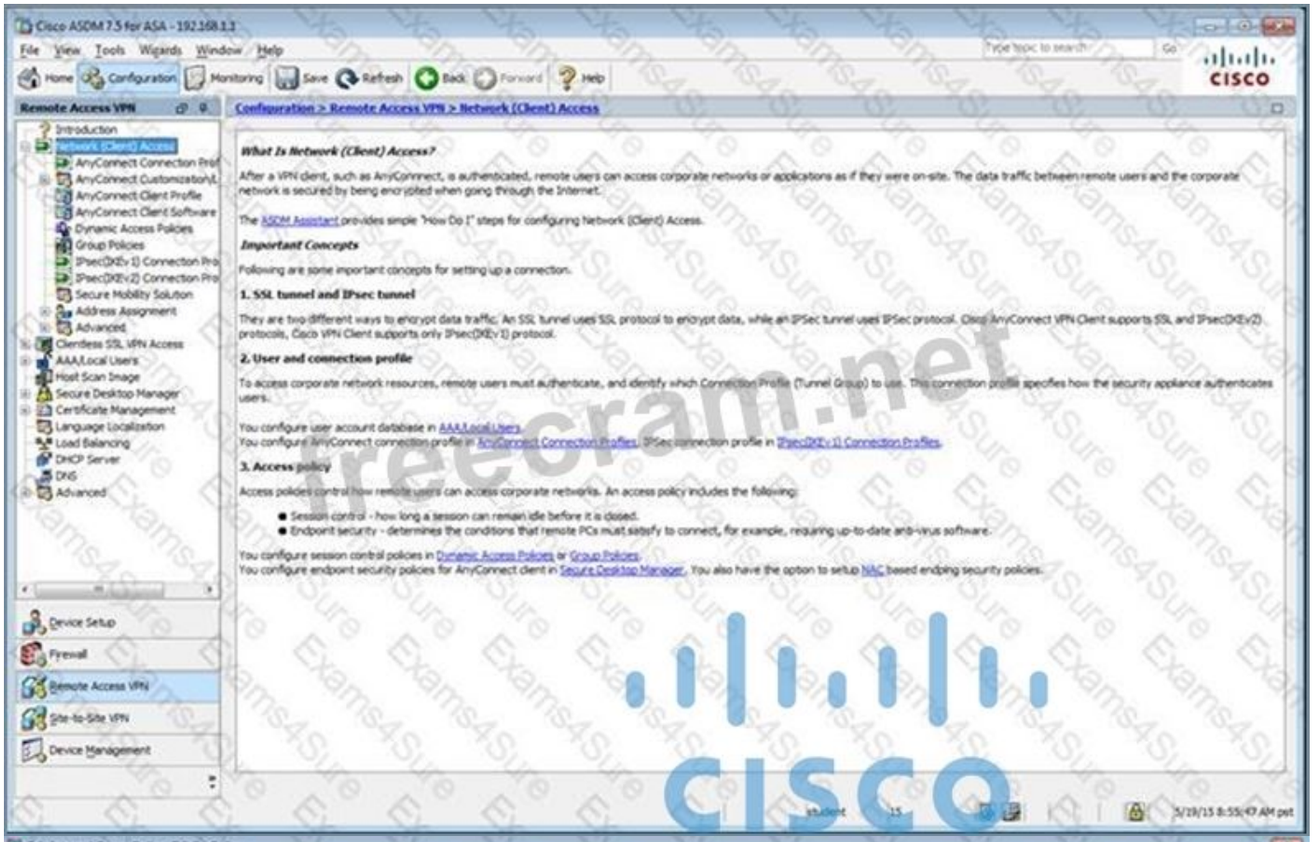

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Secure Desktop Manager
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host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

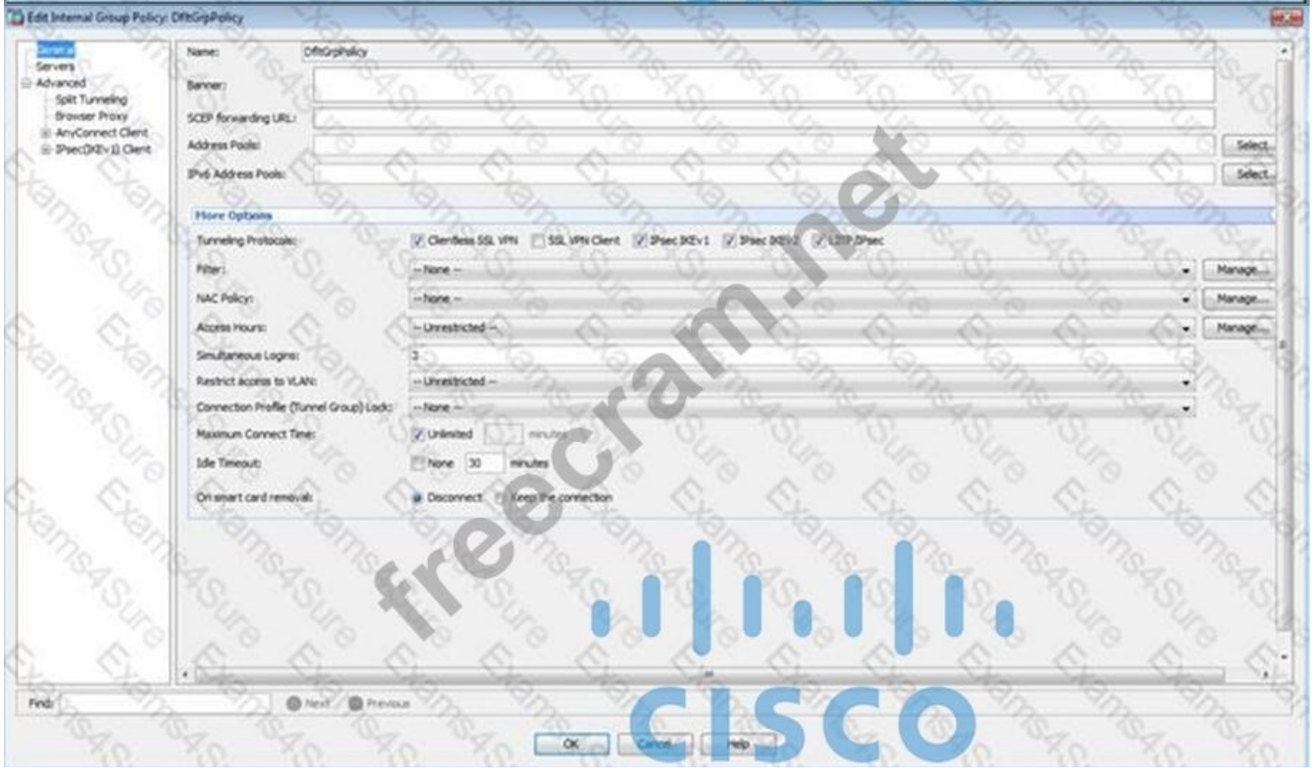


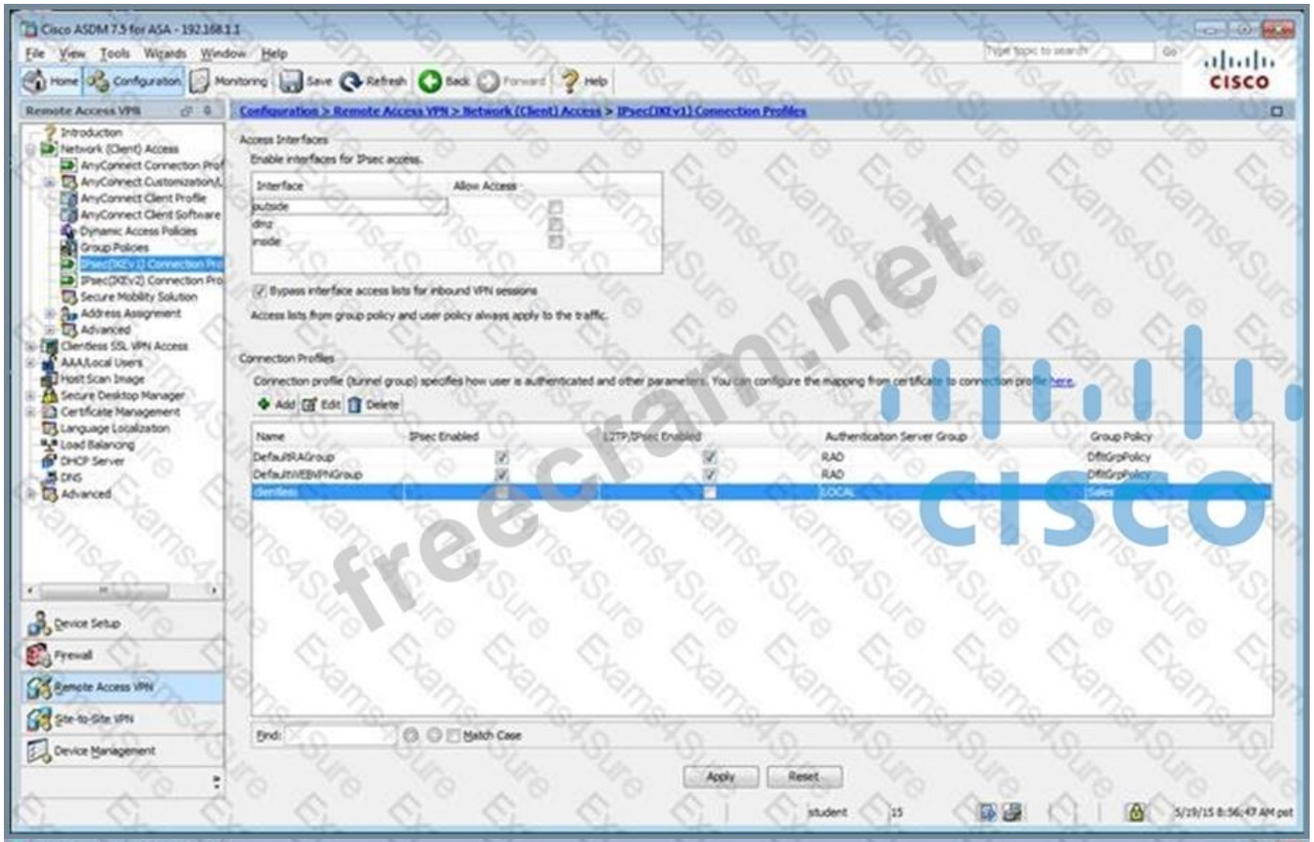

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Introduction
Network (Client) Access
Clientless SSL VPN Access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

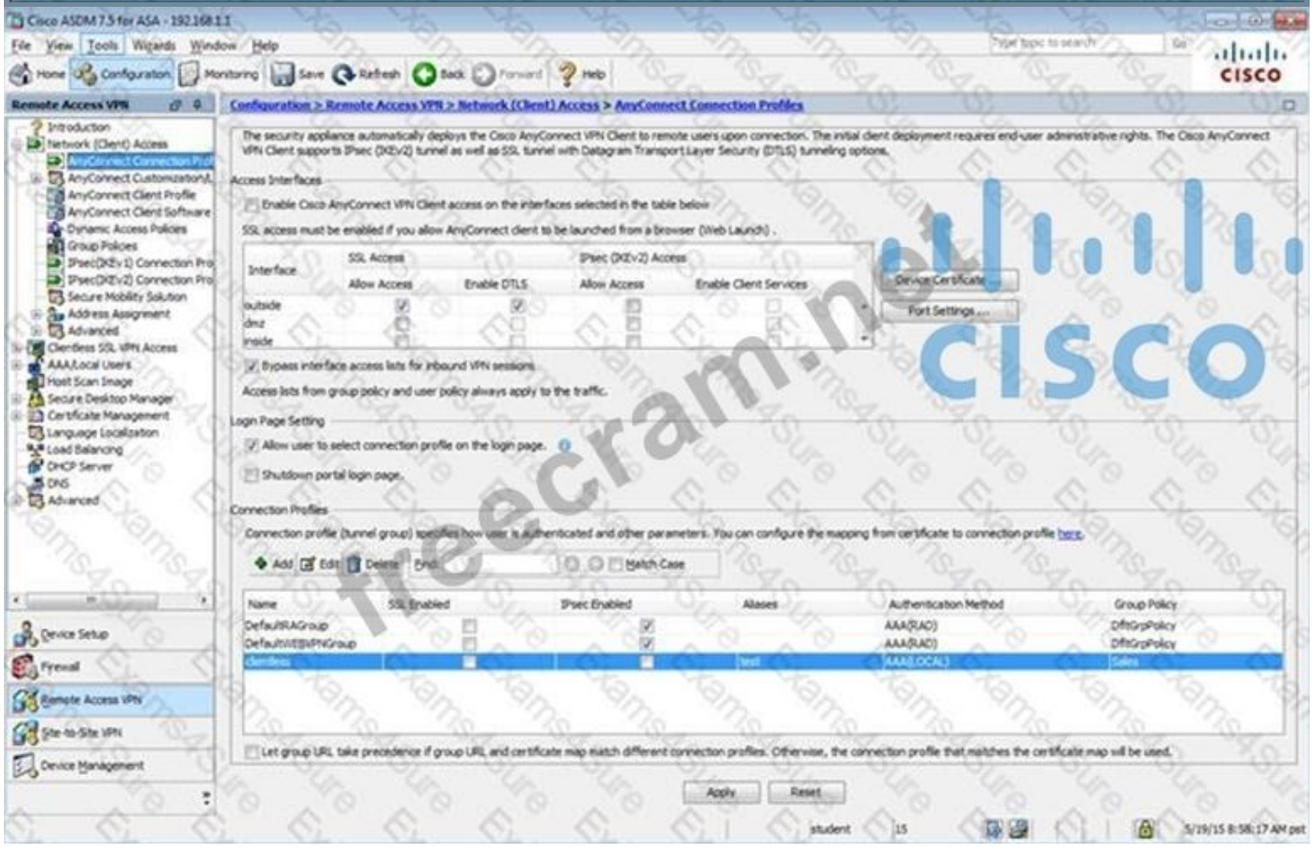

File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Remote Access VPN > Advanced
This section contains the following items:
- Connection Gateway
- SSL Settings
- Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps
- 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
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

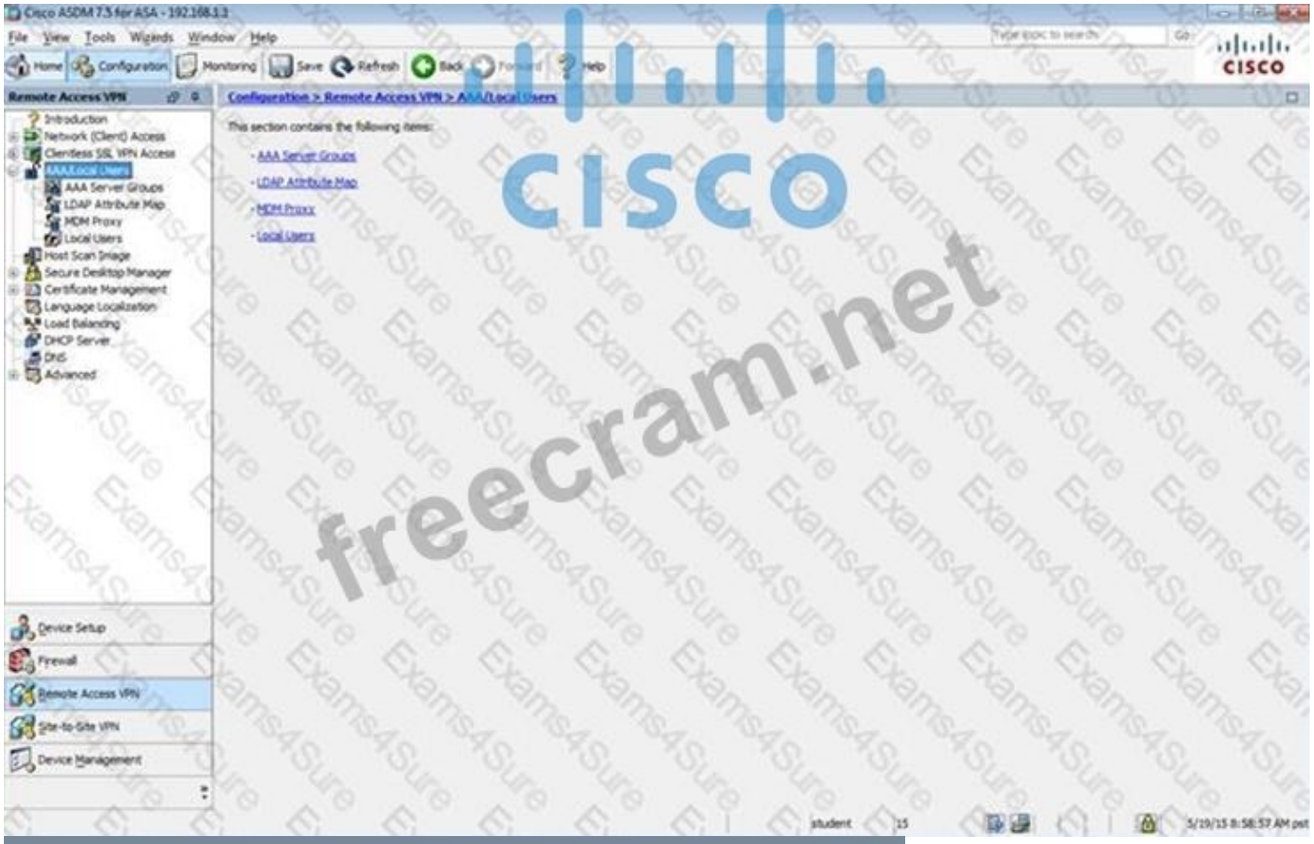


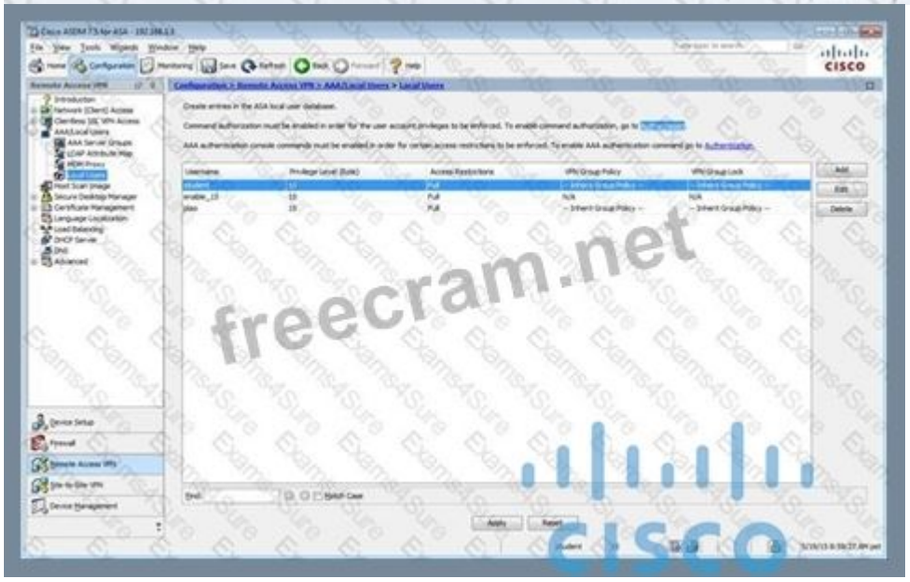







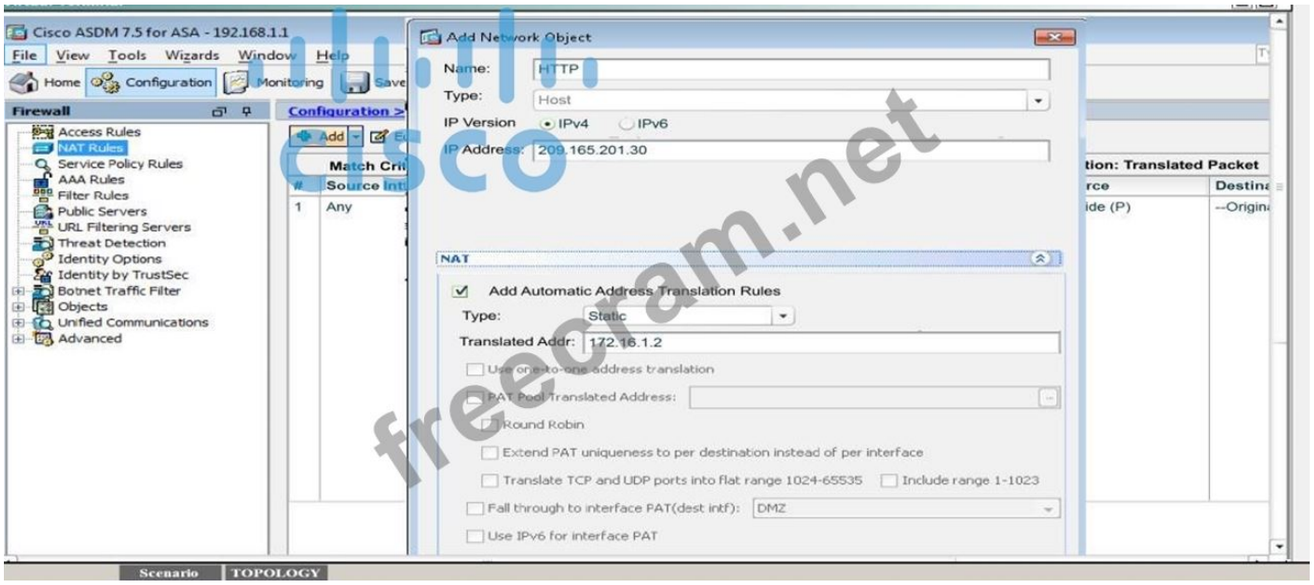




**Answer:**

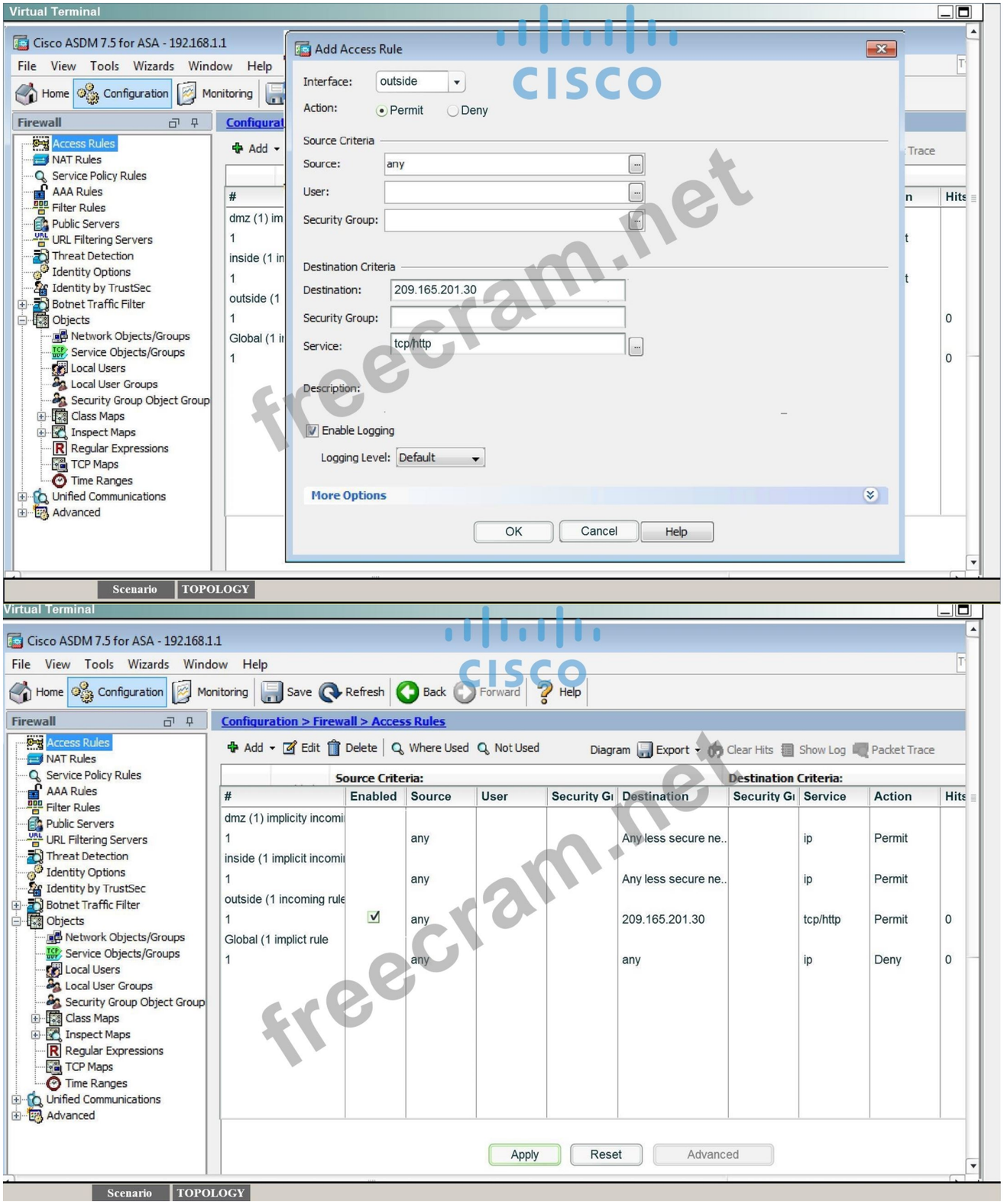
Follow the explanation part to get answer on this sim question.

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:

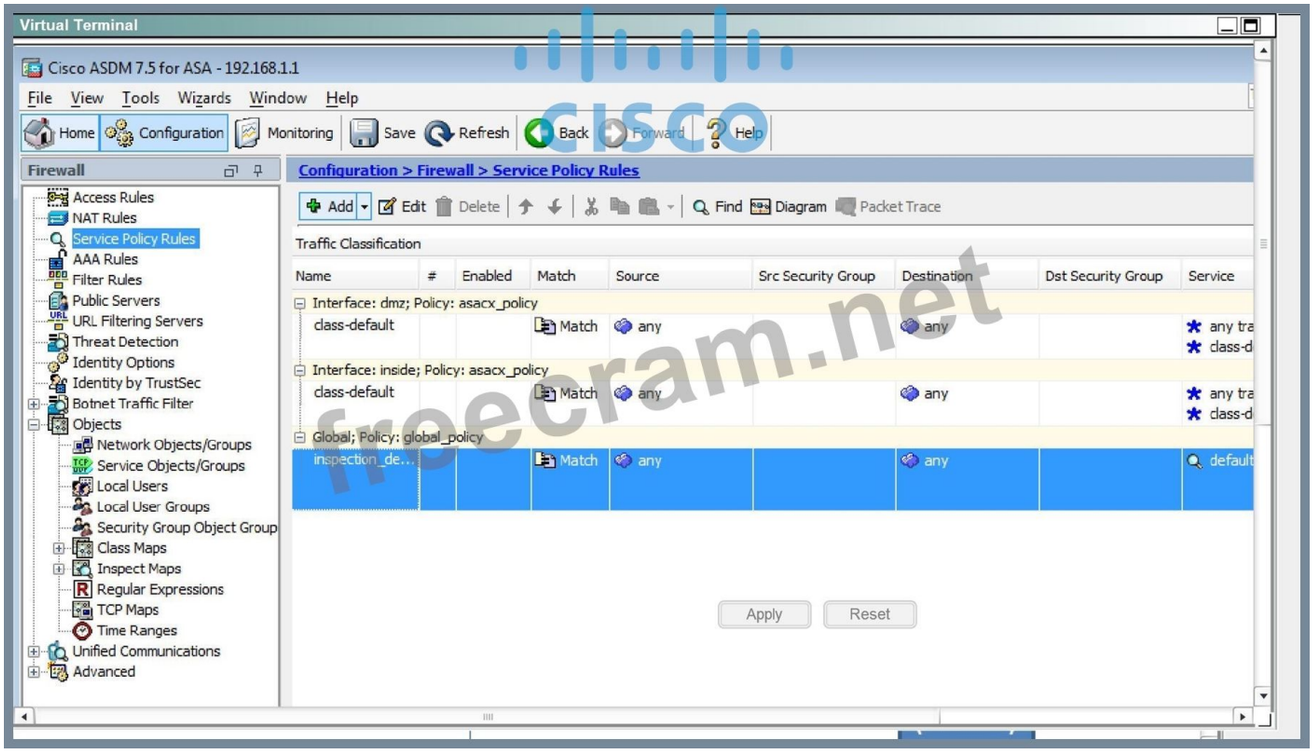




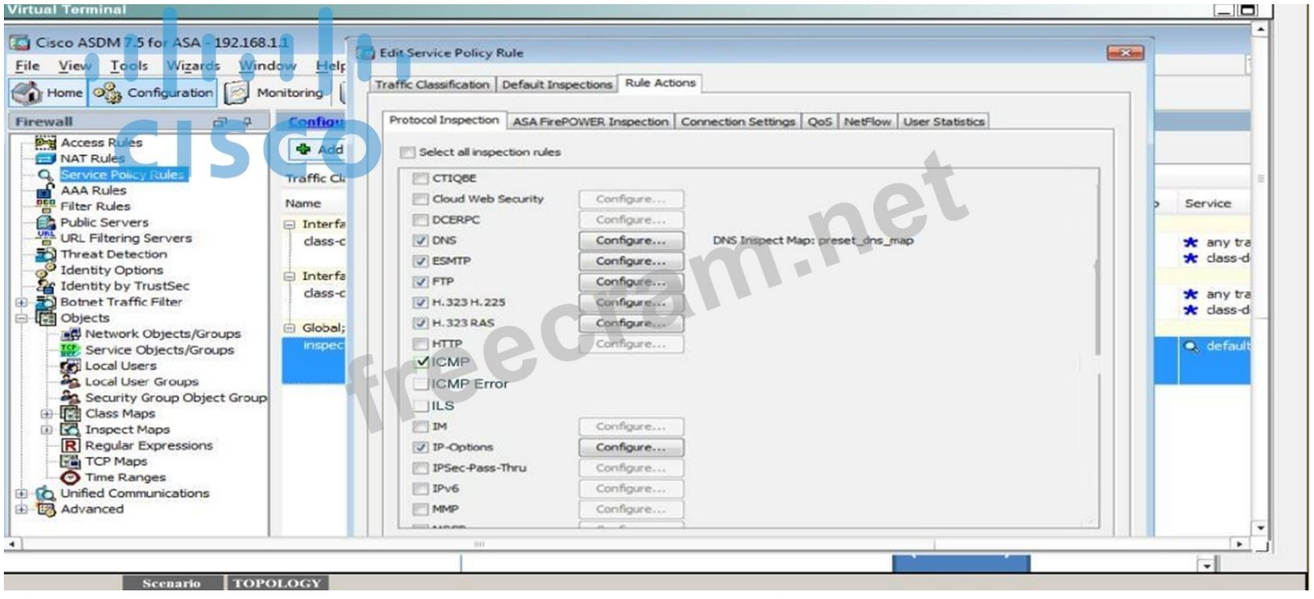


You can verify using the outside PC to HTTP into 209.165.201.30.

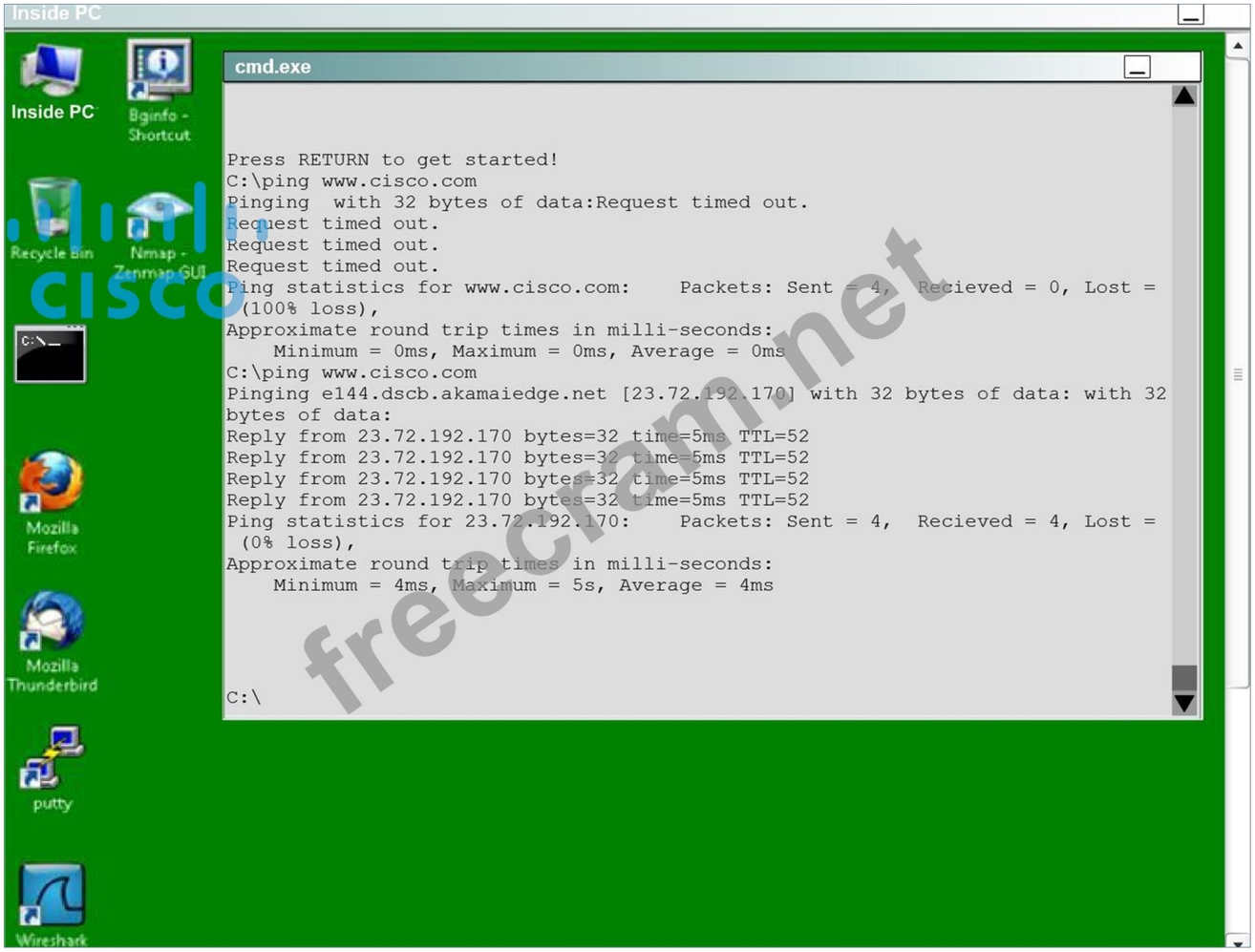
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:




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: 22**

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

**A.** Unidirectional Link Detection

**B.** Unicast Reverse Path Forwarding

**C.** TrustSec

**D.** IP Source Guard

**Answer: (SHOW ANSWER)**

Explanation

Unicast Reverse Path Forwarding (uRPF) can mitigate spoofed IP packets. When this feature is enabled on an interface, as packets enter that interface the router spends an extra moment considering the source address of the packet. It then considers its own routing table, and if the routing table does not agree that the interface that just received this packet is also the best egress interface to use for forwarding to the source address of the packet, it then denies the packet.

This is a good way to limit IP spoofing.

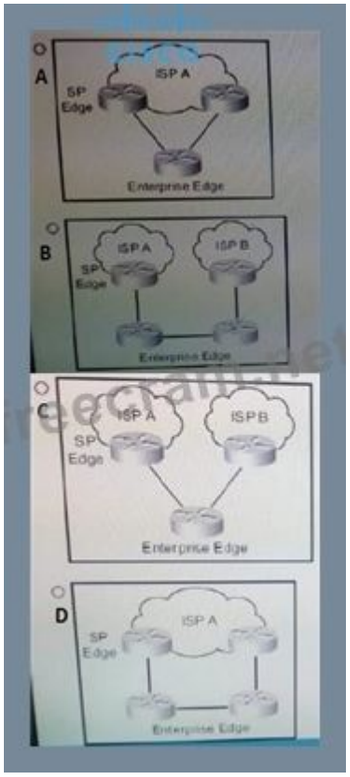
Source: Cisco Official Certification Guide, Table 10-4 Protecting the Data Plane, p.270

**NEW QUESTION: 23**

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

**A.** process ID
**B.** area ID
**C.** administrative distance value
**D.** ABR ID
**Answer: (SHOW ANSWER)**
Explanation
Enabling OSPF
SUMMARY STEPS
1. enable
2. configure terminal
3. router ospf process-id
4. network ip-address wildcard-mask area area-id
5. end
Source:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html

**NEW QUESTION: 24**
Which internet Multihoming solution is a resistant to a failure of any single component?




**A.** Option D
**B.** Option C
**C.** Option B
**D.** Option A
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 25**
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: (SHOW ANSWER)**
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: 26**
When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)
**A.** pass
**B.** police
**C.** inspect
**D.** drop
**E.** queue
**F.** shape
**Answer: (SHOW ANSWER)**
Explanation
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml
Zone-Based Policy Firewall Actions
ZFW provides three actions for traffic that traverses from one zone to another:
Drop - This is the default action for all traffic, as applied by the "class class-default" that terminates every inspect-type policy-map. Other class-maps within a policy-map can also be configured to drop unwanted traffic.
Traffic that is handled by the drop action is "silently" dropped (i.e., no notification of the drop is sent to the relevant end-host) by the ZFW, as opposed to an ACL's behavior of sending an ICMP "host unreachable" message to the host that sent the denied traffic. Currently, there is not an option to change the "silent drop" behavior. The log option can be added with drop for syslog notification that traffic was dropped by the firewall.
Pass - This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPSec ESP, IPSec AH, ISAKMP, and other inherently secure protocols with

predictable behavior. However, most application traffic is better handled in the ZFW with the inspect action.
Inspect-The inspect action offers state-based traffic control. For example, if traffic from the private zone to the Internet zone in the earlier example network is inspected, the router maintains connection or session information for TCP and User Datagram Protocol (UDP) traffic. Therefore, the router permits return traffic sent from Internet-zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic.
Audit-trail can be applied with a parameter-map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.

**NEW QUESTION: 27**
In which two models can the Cisco Web Security Appliance be deployed? (Choose two.)
**A.** as a transparent proxy using the Secure Sockets Layer protocol
**B.** as a transparent proxy using the HyperText Transfer Protocol
**C.** explicit active mode
**D.** as a transparent proxy using the Web Cache Communication Protocol
**E.** explicit proxy mode
**Answer: (SHOW ANSWER)**
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-businessarchitecture/sba_w

**NEW QUESTION: 28**
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: (SHOW ANSWER)**
Explanation
http://searchsecurity.techtarget.com/definition/secret-key-algorithm

**NEW QUESTION: 29**
How does the Cisco ASA use Active Directory to authorize VPN users?
**A.** It queries the Active Directory server for a specific attribute for the specified user.
**B.** It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.
**C.** It downloads and stores the Active Directory database to query for future authorization requests.
**D.** It redirects requests to the Active Directory server defined for the VPN group.
**Answer: A (LEAVE A REPLY)**

Explanation
When ASA needs to authenticate a user to the configured LDAP server, it first tries to login using the login DN provided. After successful login to the LDAP server, ASA sends a search query for the username provided by the VPN user. This search query is created based on the naming attribute provided in the configuration. LDAP replies to the query with the complete DN of the user. At this stage ASA sends a second login attempt to the LDAP server. In this attempt, ASA tries to login to the LDAP server using the VPN user's full DN and password provided by the user. A successful login to the LDAP server will indicate that the credentials provided by the VPN user are correct and the tunnel negotiation will move to the Phase 2.
Source:
http://www.networkworld.com/article/2228531/cisco-subnet/using-your-active-directory-for-vpn-authentication-on-asa.html

**NEW QUESTION: 30**
Which primary security attributes can be achieved by BYOD Architecture?
**A.** checking compliance with policy
**B.** public wireless network
**C.** pushing patches
**D.** Trusted enterprise network
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 31**
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: (SHOW ANSWER)**
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: 32**
In which form of fraud does an attacker try to team information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels?
**A.** Phishing
**B.** Identity Spoofing
**C.** Hacking
**D.** Smarting
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 33**
What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the computer?
**A.** always-on
**B.** proxy
**C.** transparent mode
**D.** Trusted Network Detection
**Answer: (SHOW ANSWER)**
Explanation
You can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer expires. The group policy assigned to the session specifies these timer values. If AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned to the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.
Source:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac03vpn.pdf

**NEW QUESTION: 34**
How can you protect CDP from reconnaissance attacks?
**A.** Disable CDP on ports connected to endpoints.
**B.** Disable CDP on trunk ports.
**C.** Enable dynamic ARP inspection on all untrusted ports.
**D.** Enable dot1x on all ports that are connected to other switches.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
Which FirePOWER preprocessor engine is used to prevent SYN attacks?

**A.** Rate-Based Prevention
**B.** Portscan Detection
**C.** IP Defragmentation
**D.** Inline Normalization
**Answer: (SHOW ANSWER)**
Explanation
Rate-based attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate requests. Rate-based attacks usually have one of the following characteristics:
+ any traffic containing excessive incomplete connections to hosts on the network, indicating a SYN flood attack
+ any traffic containing excessive complete connections to hosts on the network, indicating a TCP/IP connection flood attack
+ excessive rule matches in traffic going to a particular destination IP address or addresses or coming from a particular source IP address or addresses.
+ excessive matches for a particular rule across all traffic.
Preventing SYN Attacks
The SYN attack prevention option helps you protect your network hosts against SYN floods. You can protect individual hosts or whole networks based on the number of packets seen over a period of time. If your device is deployed passively, you can generate events. If your device is placed inline, you can also drop the malicious packets. After the timeout period elapses, if the rate condition has stopped, the event generation and packet dropping stops.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Threat-Detection.html

**NEW QUESTION: 36**
What is the main purpose of Control Plane Policing?
**A.** To prevent exhaustion of route-processor resources
**B.** To maintain the policy map
**C.** To define traffic classes
**D.** To organization packet queues
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
What is the effect of the ip scp server enable command?
**A.** It references an access list that allows specific SCP servers.
**B.** It adds SCP to the list of allowed copy functions.
**C.** It allows the router to become an SCP server.
**D.** It allows the router to initiate requests to an SCP server.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 38**

Refer to the exhibit.

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

What is the effect of the given command?

**A.** It merges authentication and encryption methods to protect traffic that matches an ACL.

**B.** It configures the network to use a different transform set between peers.

**C.** It configures encryption for MD5 HMAC.

**D.** It configures authentication as AES 256.

**Answer: A (LEAVE A REPLY)**

Explanation

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

Source:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command

Explanation/Reference/srfipsec.html#wp1017694 To define a transform set -- an acceptable combination of security protocols and algorithms -- use the crypto ipsec transform-set global configuration command.

ESP Encryption Transform

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

ESP Authentication Transform

+

esp-md5-hmac: ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended)

Source: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c3.html#wp2590984165

**NEW QUESTION: 39**

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

**A.** ppp authentication chap pap test

**B.** test aaa-server authentication dialergroup username <user> password.

**C.** dialer aaa suffix <suffix> password <password>

**D.** aaa authentication enable default test group tacacs+

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 40**

Which two actions can an end user take to manage a lost or stolen device in Cisco ISE? (Choose two)

**A.** Force the device to be locked with a PIN.

**B.** Add the MAC address of the device to a list of blacklisted devices.

**C.** Reinstate a device that the user previously marked as lost or stolen.

**D.** Activate Cisco ISE Endpoint protection Services to quarantine the device.

**E.** Request revocation of the digital certificate of the device.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 41**
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: (SHOW ANSWER)**
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

**NEW QUESTION: 42**
Which two options are Private-VLAN secondary VLAN types?
**A.** Isolated
**B.** Segregated
**C.** Common
**D.** Secured
**E.** Community
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 43**
Which type of social engineering attack targets top executives?
**A.** Baiting
**B.** Vishing
**C.** Whaling
**D.** Spear phishing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 44**
Which two types of malware can self-replica and spread?
**A.** Backdoors
**B.** Worms
**C.** Viruses
**D.** Trojans
**E.** bots
**Answer: (SHOW ANSWER)**

Explanation
https://tools.cisco.com/security/center/resources/virus_differences
Two of the most common types of malware are viruses and worms. These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies.

**NEW QUESTION: 45**
Which IPS detection method can you use to detect attacks that based on the attackers IP addresses?
**A.** Signature-based
**B.** Policy-based
**C.** Anomaly-based
**D.** Reputation-based
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
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: (SHOW ANSWER)**
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: 47**
Which option is a key security component of an MDM deployment?
**A.** using an application tunnel by default.
**B.** using self-signed certificates to validate the server.
**C.** using MS-CHAPv2 as the primary EAP method.
**D.** using network-specific installer packages
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 48**
In which two modes can the Cisco Web Security Appliance be deployed?
**A.** as a transparent proxy using the Secure Sockets Layer protocol
**B.** as a transparent proxy using the HyperText Transfer Protocol
**C.** explicit active mode
**D.** as a transparent proxy using the Web Cache Communication Protocol
**E.** explicit proxy mode
**Answer: (SHOW ANSWER)**
Explanation
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sba_w

**NEW QUESTION: 49**
In a Cisco Cloud Web Security environment, when can network traffic bypass the scanning proxies?
**A.** When the client is connected to a wired network
**B.** When the client is connected to a VPN service that bypass proxies
**C.** When the client is on a trusted corporate network
**D.** When the client is connected to a WPA2 Enterprise network
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 50**
Which statement about IOS privilege levels is true?
**A.** Privilege-level commands are set explicitly for each user.
**B.** Each privilege level is independent of all other privilege levels.
**C.** Each privilege level supports the commands at its own level and all levels above it.
**D.** Each privilege level supports the commands at its own level and all levels below it.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 51**
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: (SHOW ANSWER)**
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: 52**
Which two 802.1x features can you enable by running the IOS authentication priority command? (Choose two.)
**A.** Web authentication
**B.** automatic selection
**C.** forced authorized port state
**D.** MAC authentication bypass
**E.** Telnet authentication
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 53**
Which Auto NAT policies are processed first ?
**A.** Dynamic with longest prefix
**B.** Dynamic with shortest prefix
**C.** Static with longest prefix
**D.** Static with shortest prefix
**Answer: (SHOW ANSWER)**
Explanation
All packets processed by the ASA are evaluated against the NAT table. This evaluation starts at the top (Section 1) and works down until a NAT rule is matched. Once a NAT rule is matched, that NAT rule is applied to the connection and no more NAT policies are checked against the packet.
+ Section 1 - Manual NAT policies: These are processed in the order in which they appear in the

configuration.
+ Section 2 - Auto NAT policies: These are processed based on the NAT type (static or dynamic) and the prefix (subnet mask) length in the object.
+ Section 3 - After-auto manual NAT policies: These are processed in the order in which they appear in the configuration.
Source:
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116388-technote-nat-00.html

**NEW QUESTION: 54**
What is the best definition of hairpinning?
**A.** traffic that enters one interface on a device and that exits through another interface
**B.** traffic that tunnels through a device interface
**C.** traffic that enters and exits a device through the same interface
**D.** ingress traffic that traverses the outbound interface on a device
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 55**
Which effect of the secure boot-image command is true?
**A.** It archives a secure copy of the IOS image.
**B.** It configure the device to boot to the secure IOS image.
**C.** It displays the status of the bootset
**D.** It archives a secure copy of the device configuration.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 56**
When a company puts a security policy in place, what is the effect on the company's business?
**A.** Minimizing risk
**B.** Minimizing total cost of ownership
**C.** Minimizing liability
**D.** Maximizing compliance
**Answer: (SHOW ANSWER)**
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: 57**

Which command is needed to enable SSH support on a Cisco Router?
**A.** crypto key lock rsa
**B.** crypto key generate rsa
**C.** crypto key zeroize rsa
**D.** crypto key unlock rsa
**Answer: (SHOW ANSWER)**
Explanation
There are four steps required to enable SSH support on a Cisco IOS router:
+ Configure the hostname command.
+ Configure the DNS domain.
+ Generate the SSH key to be used.
+ Enable SSH transport support for the virtual type terminal (vtys).
!--- Step 1: Configure the hostname if you have not previously done so.
hostname carter
!--- The aaa new-model command causes the local username and password on the router !--- to be used in the absence of other AAA statements.
aaa new-model
username cisco password 0 cisco
!--- Step 2: Configure the DNS domain of the router.
ip domain-name rtp.cisco.com
!--- Step 3: Generate an SSH key to be used with SSH.
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
!--- Step 4: By default the vtys' transport is Telnet. In this case, !--- Telnet is disabled and only SSH is supported.
line vty 0 4
transport input SSH
Source:
http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html#settingupaniosrouterasssh

**NEW QUESTION: 58**
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 (LEAVE A REPLY)**
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: 59**
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: (SHOW ANSWER)**
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: 60**
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: (SHOW ANSWER)**
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: 61**
Refer to the exhibit.


Which statement about this output is true?
**A.** The user logged into the router with the incorrect username and password.
**B.** The login failed because there was no default enable password.
**C.** The login failed because the password entered was incorrect.
**D.** The user logged in and was given privilege level 15.
**Answer: (SHOW ANSWER)**
Explanation
http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html
debug aaa authentication
To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication, use the debug aaa authentication privileged EXEC command. To disable debugging command, use the no form of the command.
debug aaa authentication
no debug aaa authentication
The following is sample output from the debug aaa authentication command. A single EXEC login that uses the "default" method list and the first method, TACACS+, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several

are occurring concurrently.
Router# debug aaa authentication
6:50:12: AAA/AUTHEN: create_user user='' ruser='' port='tty19' rem_addr='172.31.60.15' authen_type=1 service=1 priv=1
6:50:12: AAA/AUTHEN/START (0): port='tty19' list='' action=LOGIN service=LOGIN
6:50:12: AAA/AUTHEN/START (0): using "default" list
6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+
6:50:12: TAC+ (50996740): received authen response status = GETUSER
6:50:12: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN/CONT (50996740): continue_login
6:50:15: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN (50996740): Method=TACACS+
6:50:15: TAC+: send AUTHEN/CONT packet
6:50:15: TAC+ (50996740): received authen response status = GETPASS
6:50:15: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN/CONT (50996740): continue_login
6:50:20: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
6:50:20: TAC+: send AUTHEN/CONT packet
6:50:20: TAC+ (50996740): received authen response status = PASS
6:50:20: AAA/AUTHEN (50996740): status = PASS



**NEW QUESTION: 62**
Which statement about NAT table evaluation in the ASA is true?
**A.** The ASA uses the most specific match
**B.** Manual NAT policies are applied first
**C.** Auto NAT policies are applied first
**D.** After-auto NAT polices are applied first
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 63**
Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data?

**A.** hack
**B.** mitigation
**C.** risk
**D.** vulnerability
**E.** exploit
**Answer: D (LEAVE A REPLY)**
Explanation
vulnerability A flaw or weakness in a system's design or implementation that could be exploited.

**NEW QUESTION: 64**
In a security context, which action can you take to address compliance?
**A.** Implement rules to prevent a vulnerability.
**B.** Correct or counteract a vulnerability.
**C.** Reduce the severity of a vulnerability.
**D.** Follow directions from the security appliance manufacturer to remediate a vulnerability.
**Answer: (SHOW ANSWER)**
Explanation
In general, compliance means conforming to a rule, such as a specification, policy, standard or law.
Source: https://en.wikipedia.org/wiki/Regulatory_compliance

**NEW QUESTION: 65**
If a personal Firewall specifically blocks NTP, which type of blocking is the firewall performing?
**A.** network
**B.** service
**C.** file
**D.** application
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 66**
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: (SHOW ANSWER)**
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: 67**
What are two challenges of using a network-based IPS? (Choose two.)
**A.** As the network expands, it requires you to add more sensors
**B.** It is unable to determine whether a detected attack was successful
**C.** It requires additional storage and processor capacity on syslog servers
**D.** It must support multiple operating systems
**E.** It is unable to detect attacks across the entire network
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 68**
What protocol provides CIA ?
**A.** HA
**B.** ESP
**C.** IKEV1
**D.** IKEV2
**Answer: B (LEAVE A REPLY)**
Explanation
Encapsulating Security Payload or ESP refers to the protocol which offers confidentiality on top of integrity and authentication to the IPSec data.

**NEW QUESTION: 69**
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: (SHOW ANSWER)**
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: 70**

When you edit an IPS sub signature, what is the effect on the parent signature and the family of subsignature?



**A.** The change applies to the parent signature and the entire family of subsignature.
**B.** Other signatures are unaffected, the change applies only to the subsignature that you edit.
**C.** The change applies only to sub signature that are numbered sequentially after the subsignatre that you edit.
**D.** The change applies to the parent signature and the subsignature that you edit.
**Answer: (SHOW ANSWER)**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager

**NEW QUESTION: 71**

What can cause the state table of a stateful firewall to update? (choose two)
**A.** when a connection is created
**B.** When a connection's timer has expired within state table
**C.** when packet is evaluated against the outbound access list and is denied
**D.** when outbound packets forwarded to outbound interface
**E.** when rate-limiting is applied
**Answer: (SHOW ANSWER)**
Explanation
Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection,

and stores the data in dynamic state tables. This cumulative data is evaluated, so that filtering decisions would not only be based on administrator-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection.
Entries are created only for TCP connections or UDP streams that satisfy a defined security policy.
In order to prevent the state table from filling up, sessions will time out if no traffic has passed for a certain period. These stale connections are removed from the state table.
Source: https://en.wikipedia.org/wiki/Stateful_firewall

**NEW QUESTION: 72**
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: (SHOW ANSWER)**
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: 73**
Which IPSec mode is used to encrypt traffic directly between a client and a server VPN endpoint?
**A.** tunnel mode
**B.** aggressive mode
**C.** transport mode
**D.** quick mode
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 74**
Which statement about TACACS+ is true?
**A.** TACACS_ is flexible than RADIUS because it separates all AAA into individual processes.

**B.** TACACS_ server listens UDP port 1813 for accounting
**C.** All data that is transmitted between the client and TACACS+ server is cleartext
**D.** Passwords are transmitted between the client and server using MD5 hasing.
**E.** TACACS_ is used for access to network resources more than administrator access to network devices.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 75**
(Choose Two)
**A.** Correlation between logs Which two functions can SIEM provide?and events from multiple systems.
**B.** event aggregation that allows for reduced log storage requirements.
**C.** proactive malware analysis to block malicious traffic.
**D.** dual-factor authentication.
**E.** centralized firewall management.
**Answer: (SHOW ANSWER)**
Explanation
+ 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-businessarchitecture/sbaSIEM_deployG.pdf

**NEW QUESTION: 76**
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: (SHOW ANSWER)**
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: 77**
Which component offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?
**A.** Cisco ASA 5500-X Series Next Gen. Security appliance
**B.** Cisco ASA 5500 series security appliance
**C.** Cisco IOS router
**D.** Cisco 4200 series IPS appliance
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 78**
Which command do you enter to verify the status and settings of an IKE Phase 1 tunnel?
**A.** show crypto isakmp policy
**B.** show crypto isakmp sa
**C.** show crypto Ipsec as output
**D.** show crypto ipsec transform-sat
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
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: (SHOW ANSWER)**
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:

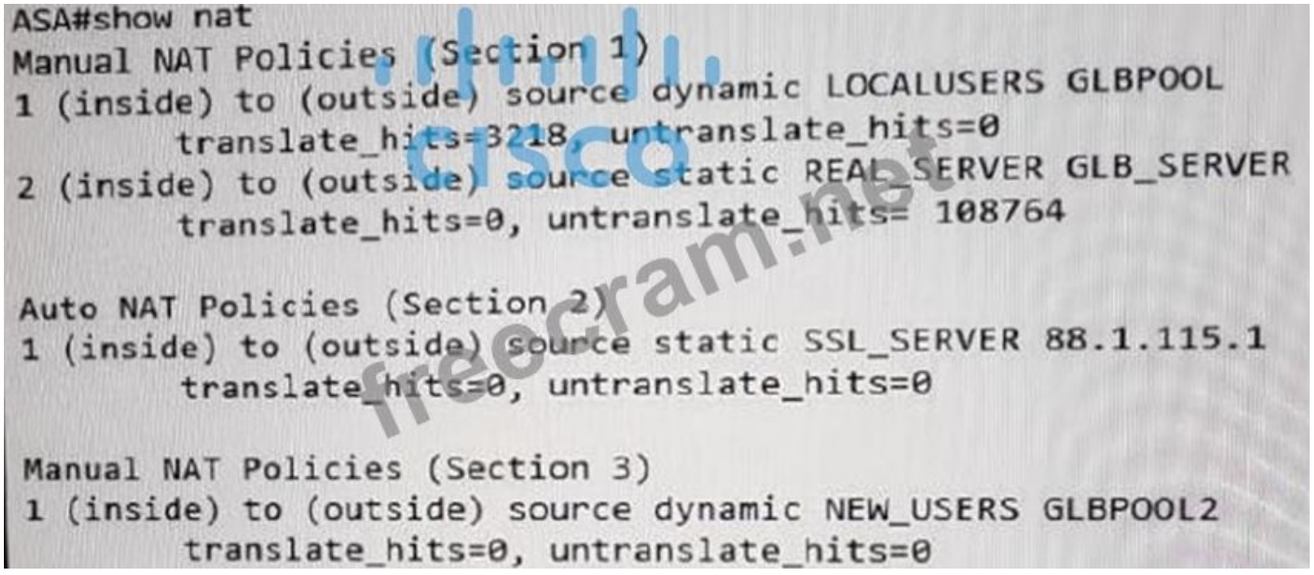
+ If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
Source:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swspan.html

**NEW QUESTION: 80**
Which technology can best protect data at rest on a user system?
**A.** router ACL
**B.** IPsec tunnel
**C.** full-disk encryption
**D.** network IPS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 81**
Which label is given to a person who uses existing computer scripts to hack into computers lacking the expertise to write their own?
**A.** phreaker
**B.** hacktivist
**C.** script kiddy
**D.** white hat hacker
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 82**
Which command can you enter to configure OSPF to use hashing to authenticate routing updates?
**A.** ip ospf priority 1
**B.** ip ospf authentication-key
**C.** neighbor 192.168.0.112 cost md5
**D.** ip ospf authentication message-digest
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 83**
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.** First policy in the Section 1 is as dynamic nat entry defined in the object configuration.

**B.** NAT policy in Section 2 is a static entry defined in the obkect configuration

**C.** Transalation in Section 3 used when a connection does not match any entries in first two sections.

**D.** There are only reverse transalation matches for the REAL_SERVER object.

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 84**

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: (SHOW ANSWER)**

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: 85**

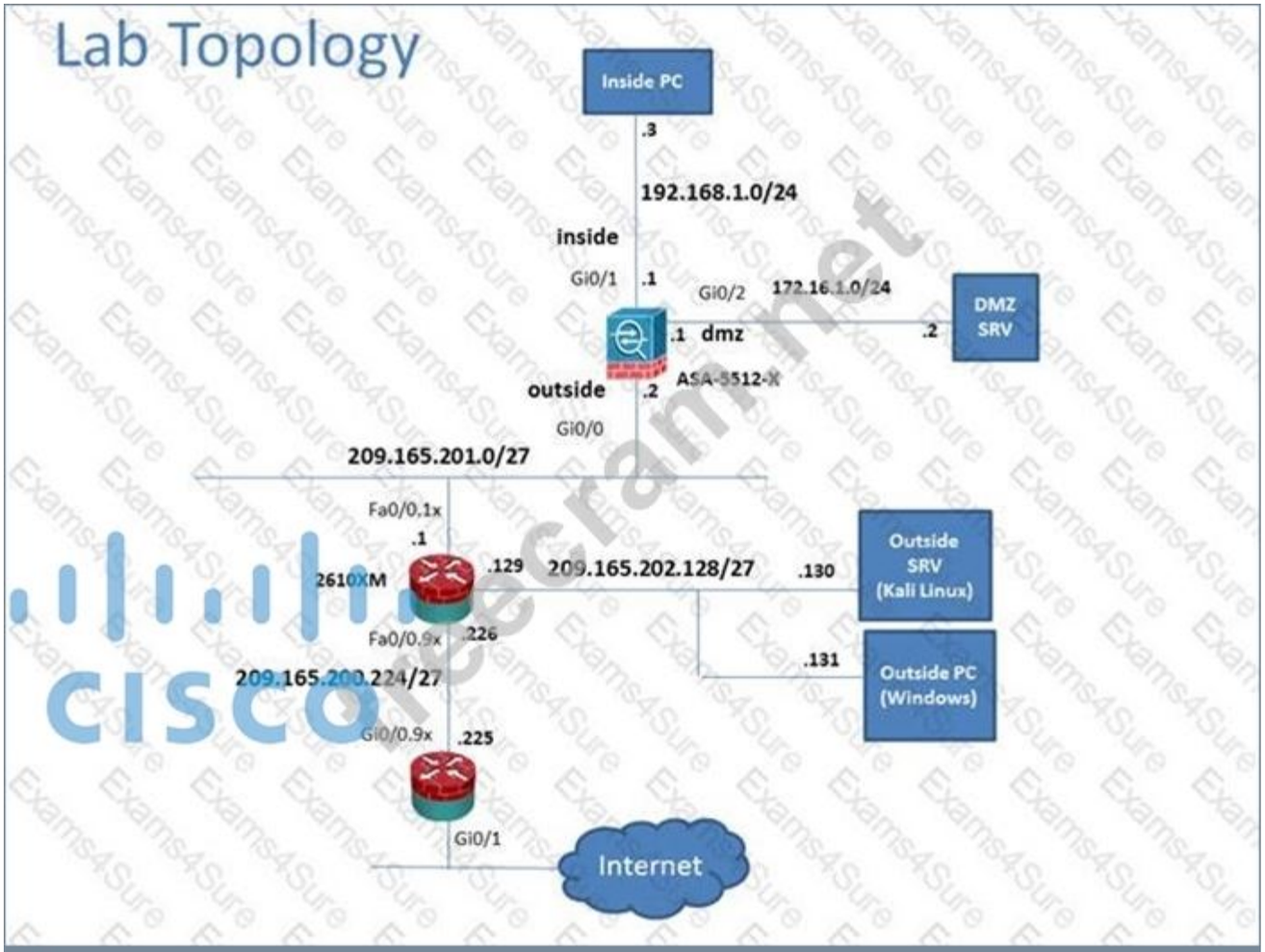
If a router configuration includes the line aaa authentication login default group tacacs+ enable, which events

will occur when the TACACS+ server returns an error? (Choose two.)
**A.** Authentication will use the router`s local database
**B.** Authentication attempts will be sent to the TACACS+ server
**C.** Authentication attempts to the router will be denied
**D.** The user will be prompted to authenticate using the enable password
**Answer: (SHOW ANSWER)**

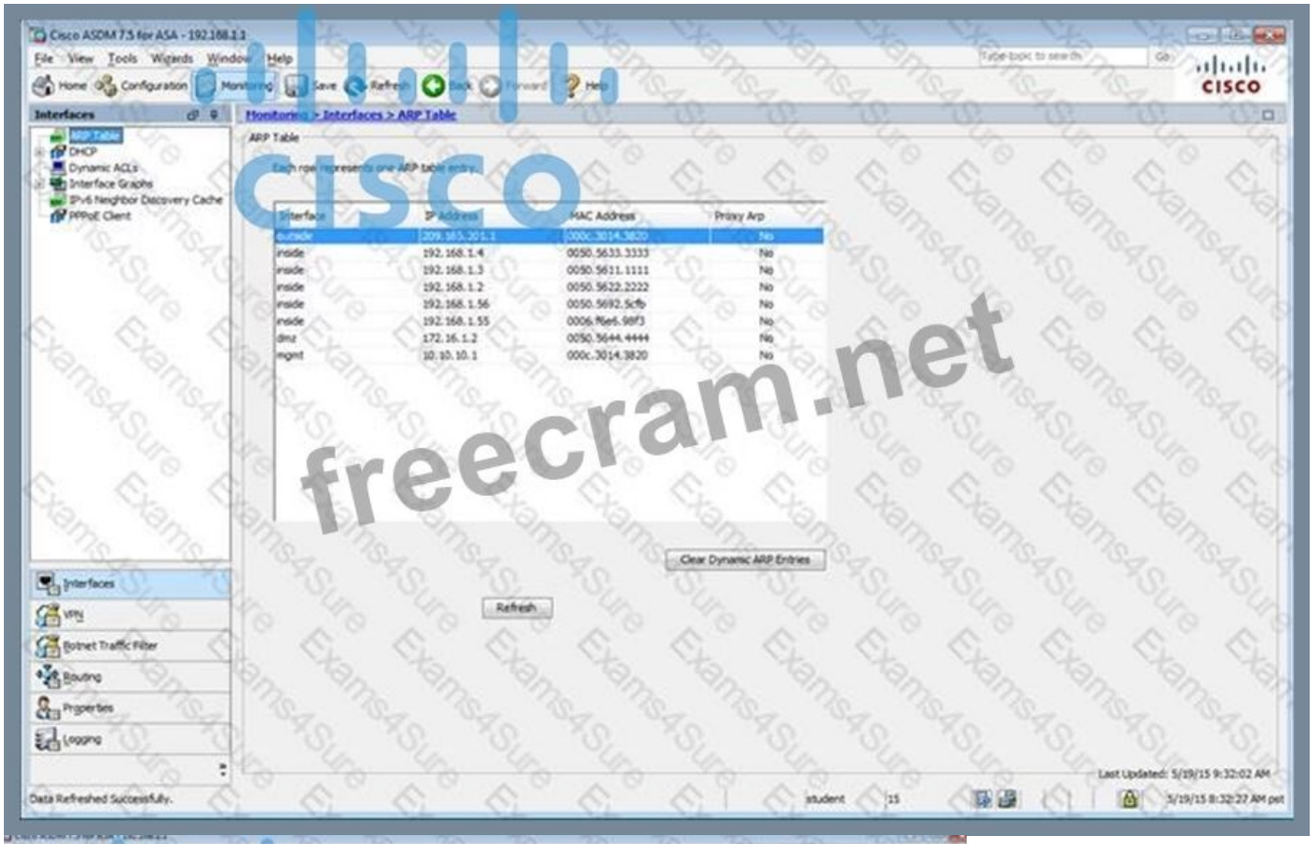
**NEW QUESTION: 86**
Which is a key security component of MDM deployment?
**A.** Using self-signed certificates to validate the server - generate self-signed certificate to connect to server (Deployed certificates ;Issued certificate to the server likely)
**B.** Using MS-CHAPv2 as primary EAP method
**C.** Using application tunnel
**D.** Using network-specific installer package
**Answer: (SHOW ANSWER)**

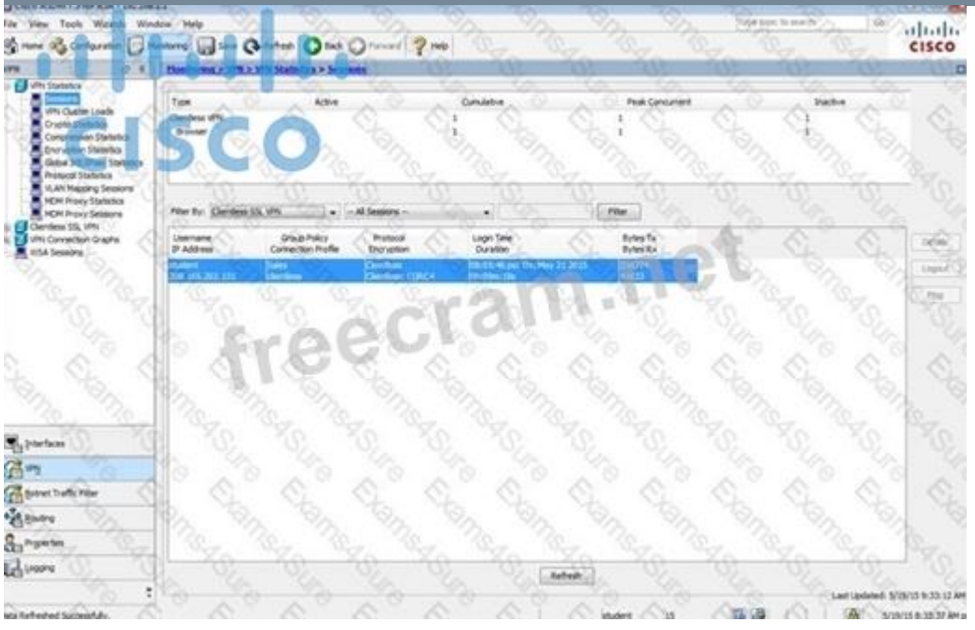
**NEW QUESTION: 87**
Which two are characteristics of RADIUS? (Choose two.)
**A.** Uses UDP port 49
**B.** Uses TCP port 49
**C.** Encrypts only the password between user and server
**D.** Uses TCP ports 1812/1813
**E.** Uses UDP ports 1812/1813
**Answer: C,E (LEAVE A REPLY)**

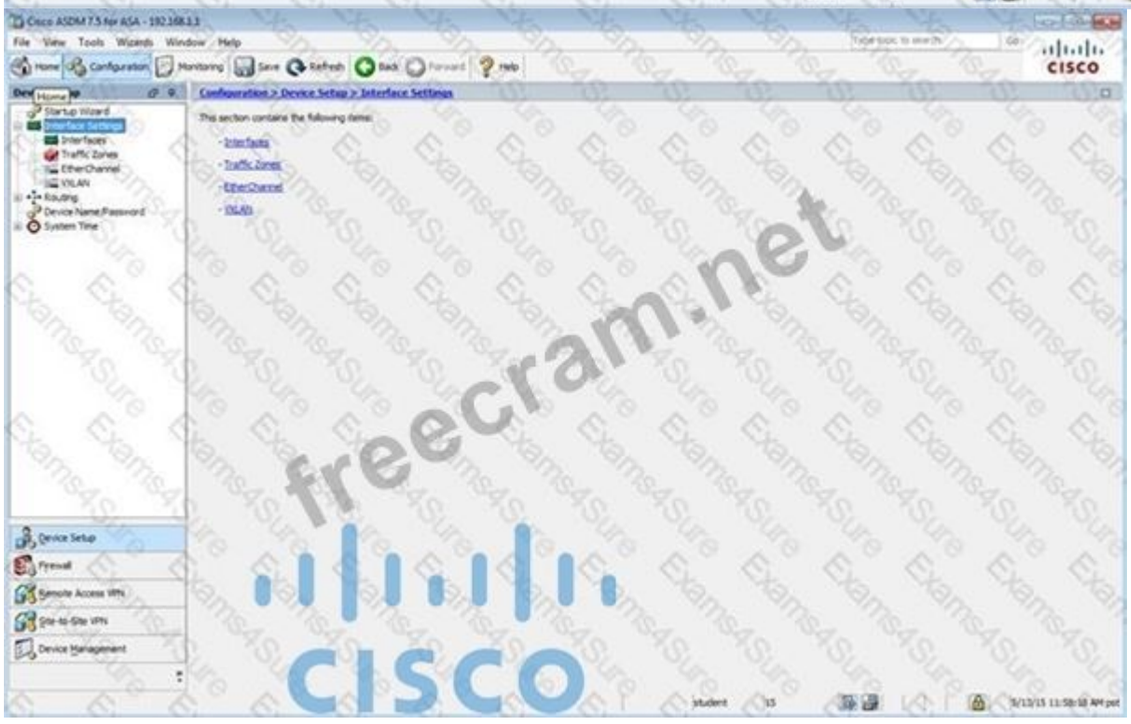
**NEW QUESTION: 88**
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

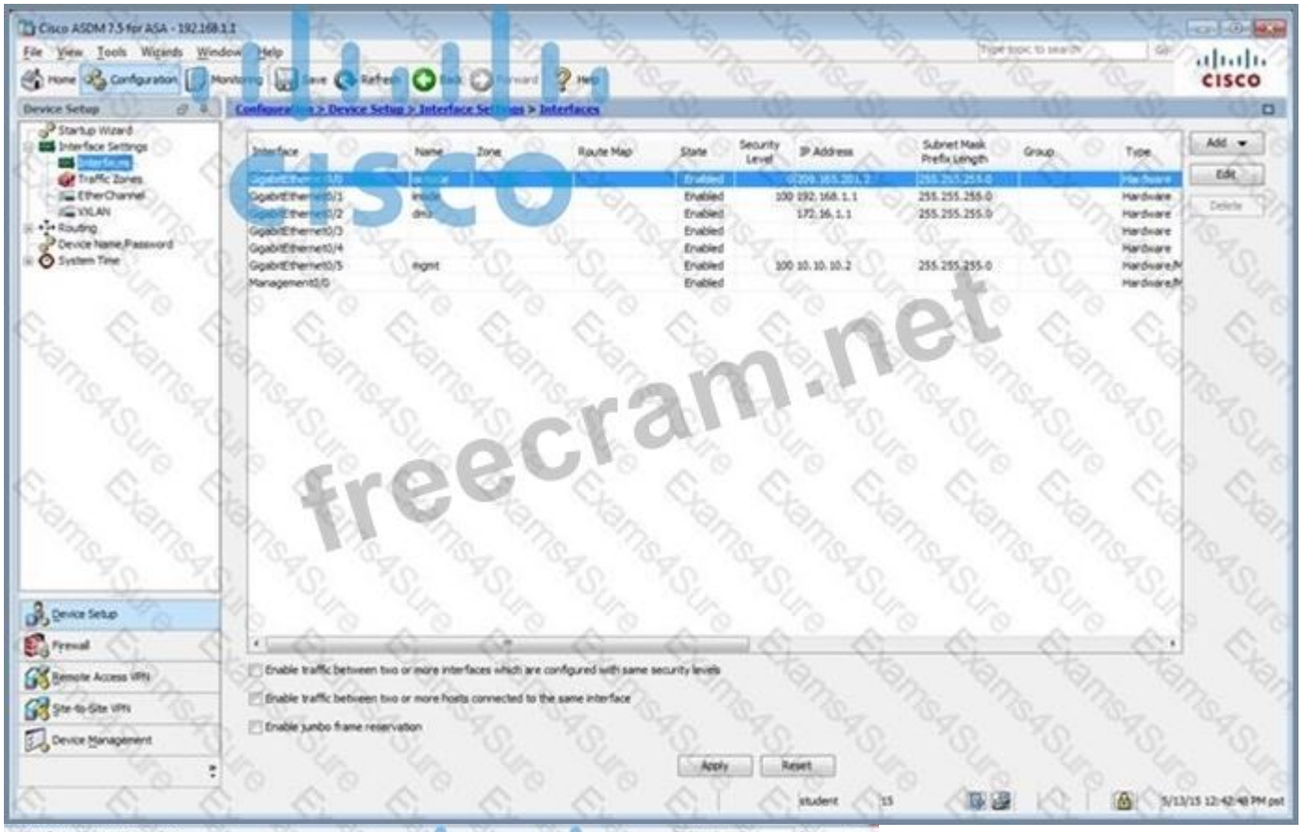

Lab Topology
Inside PC
.3
192.168.1.0/24
inside
Gi0/1
.1
Gi0/2
172.16.1.0/24
DMZ SRV
.2
.1 dmz
outside
.2
ASA-5512-X
Gi0/0
209.165.201.0/27
Fa0/0.1x
.1
2610XM
.129
209.165.202.128/27
.130
Outside SRV (Kali Linux)
Fa0/0.9x
.226
.131
Outside PC (Windows)
209.165.200.224/27
Gi0/0.9x
.225
Gi0/1
Internet

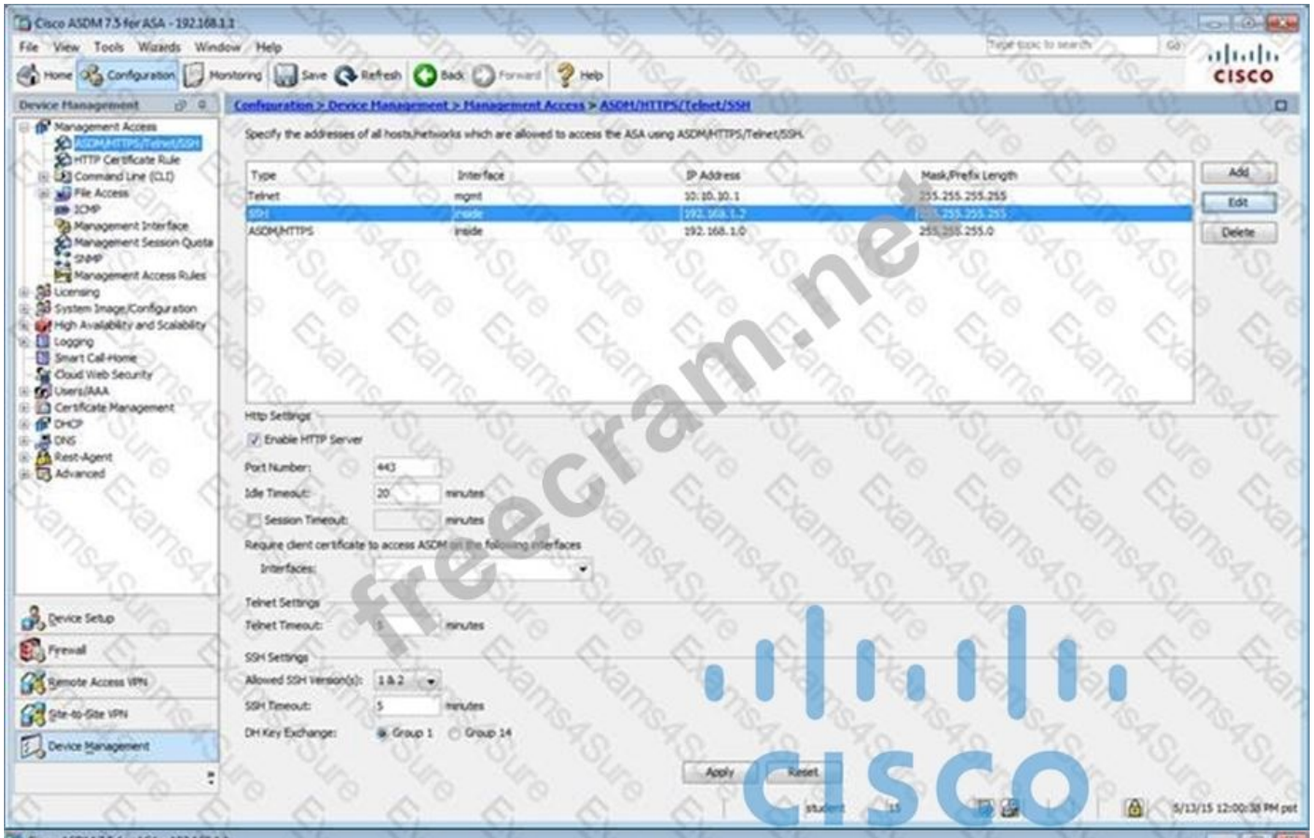

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
Interface Status
Latest ASDM Syslog Messages

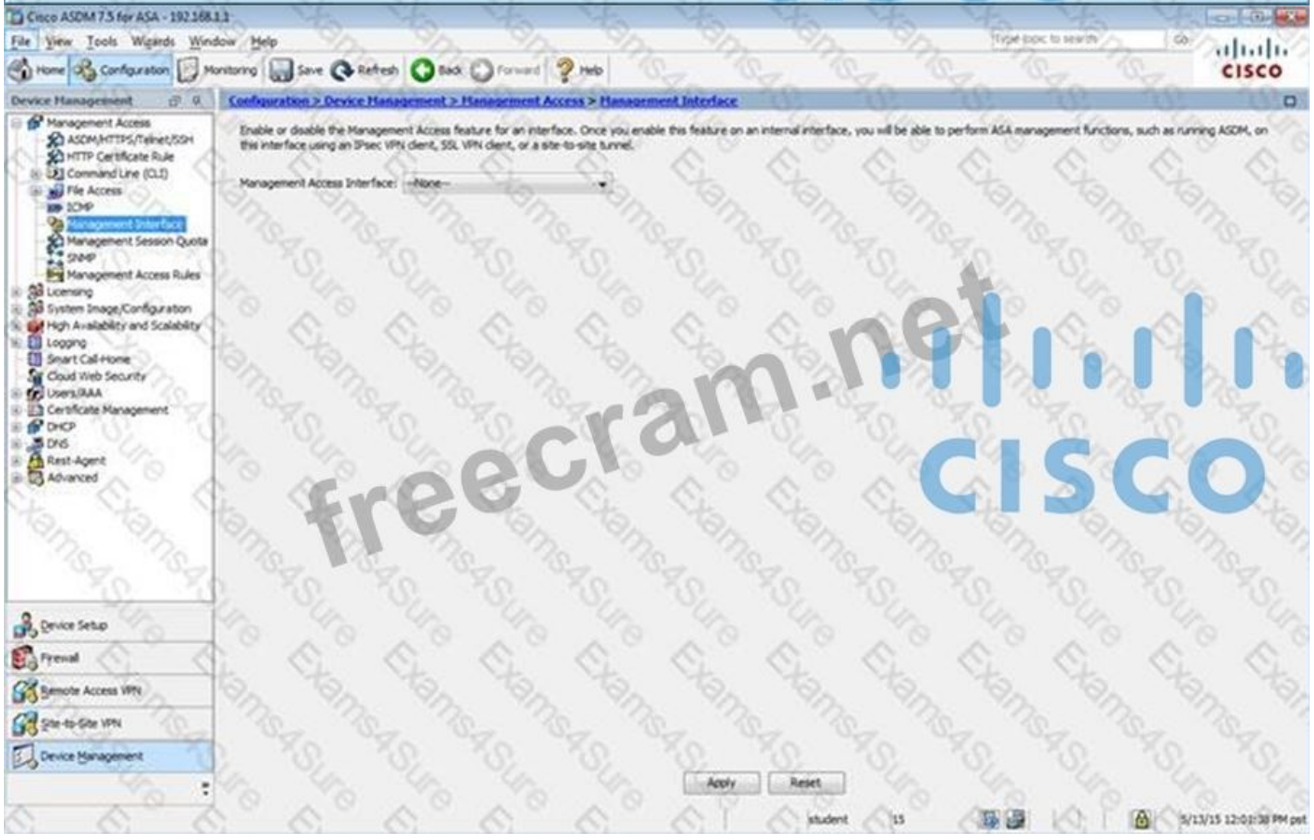


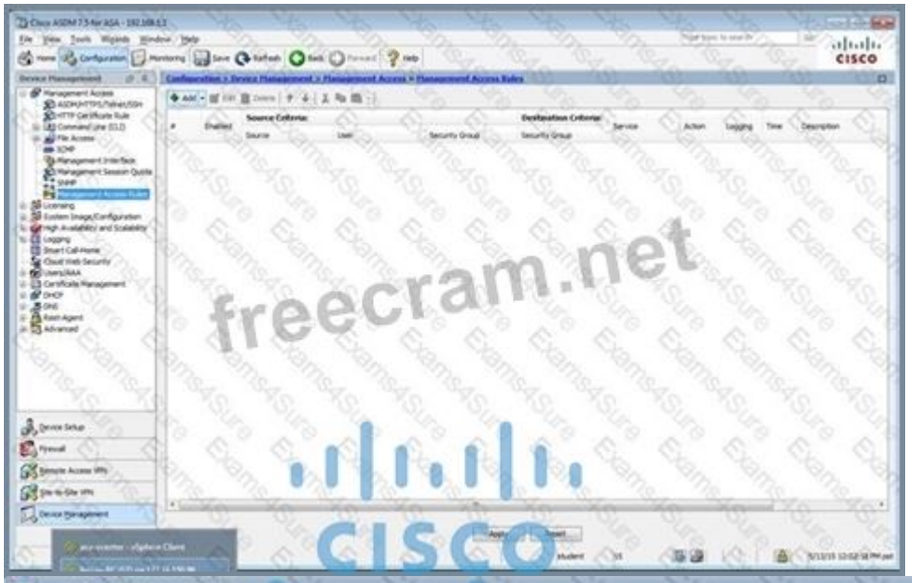



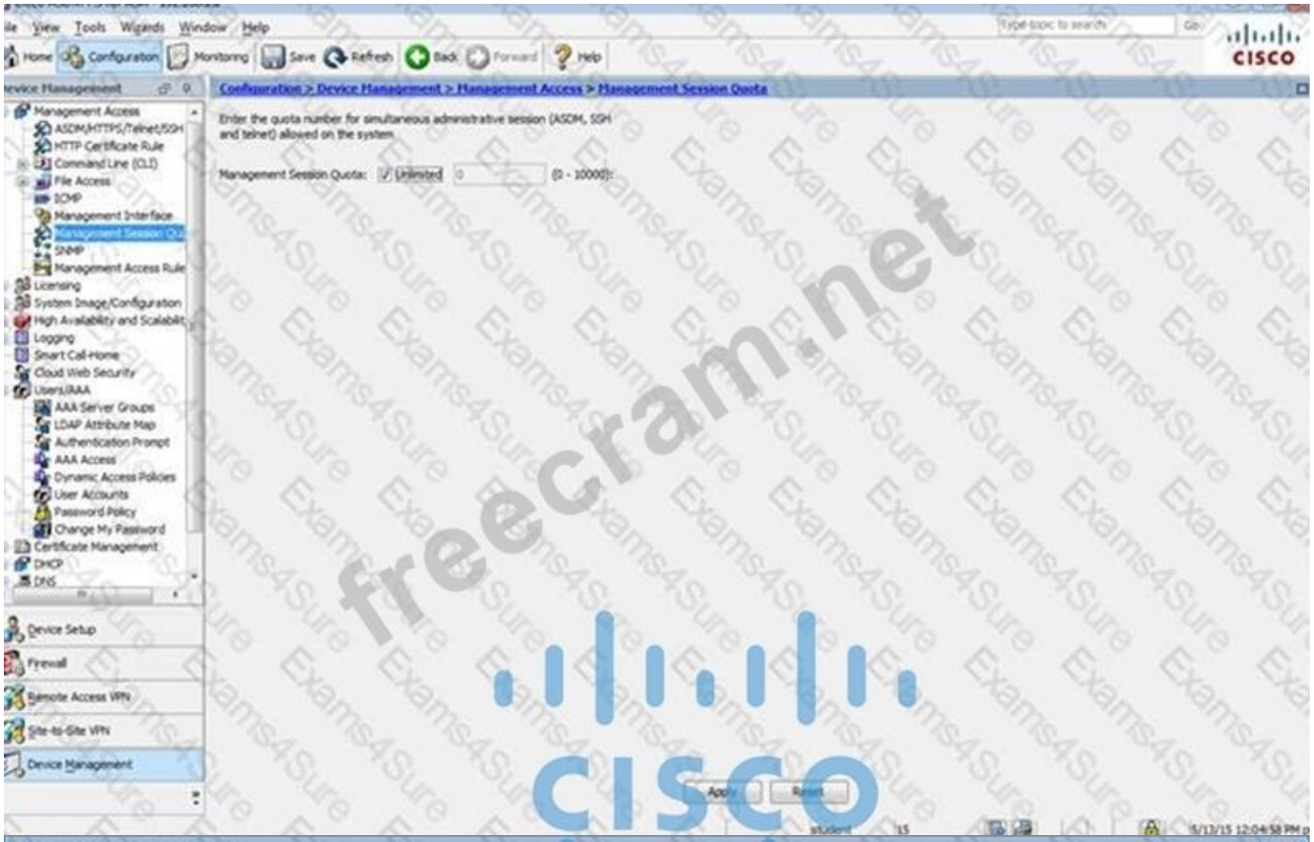



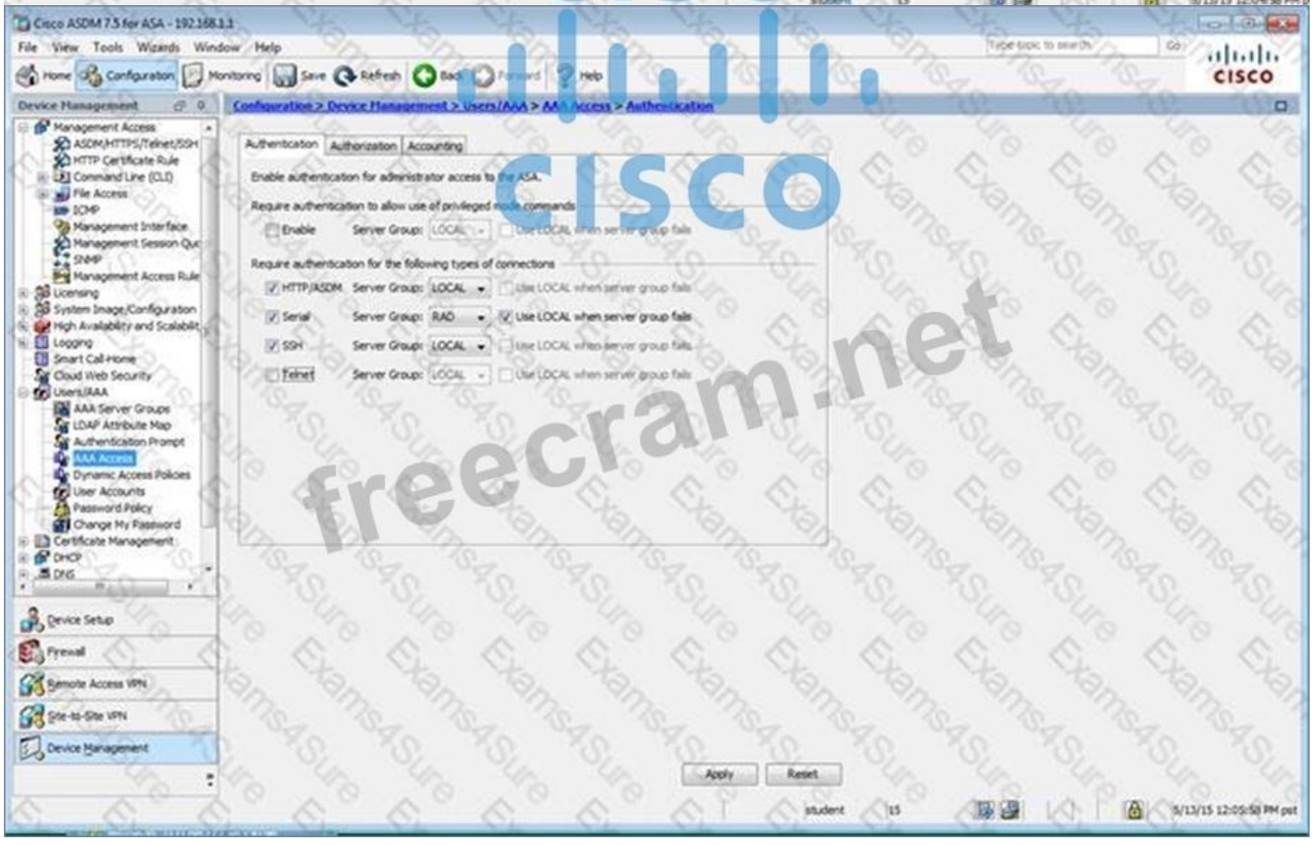


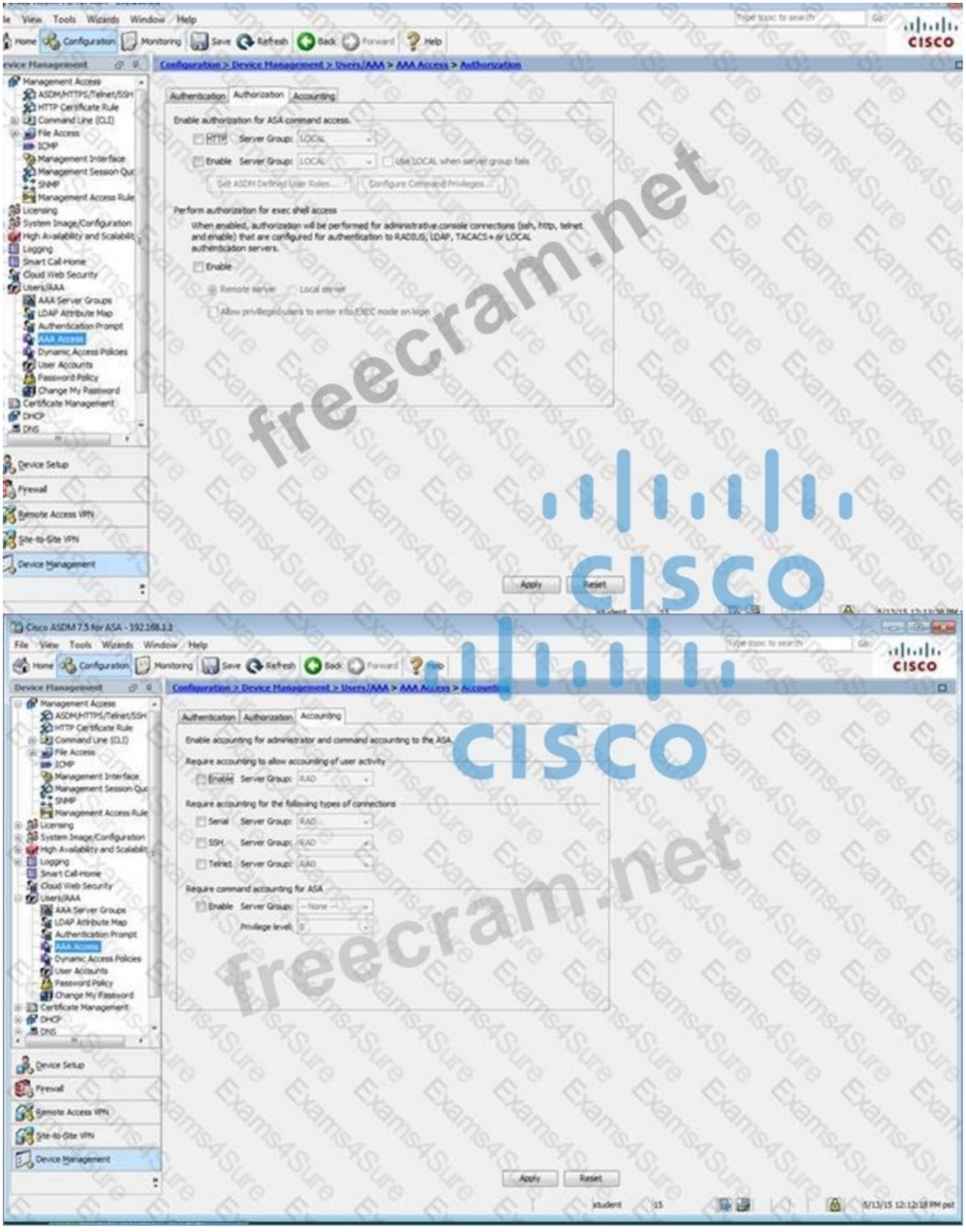



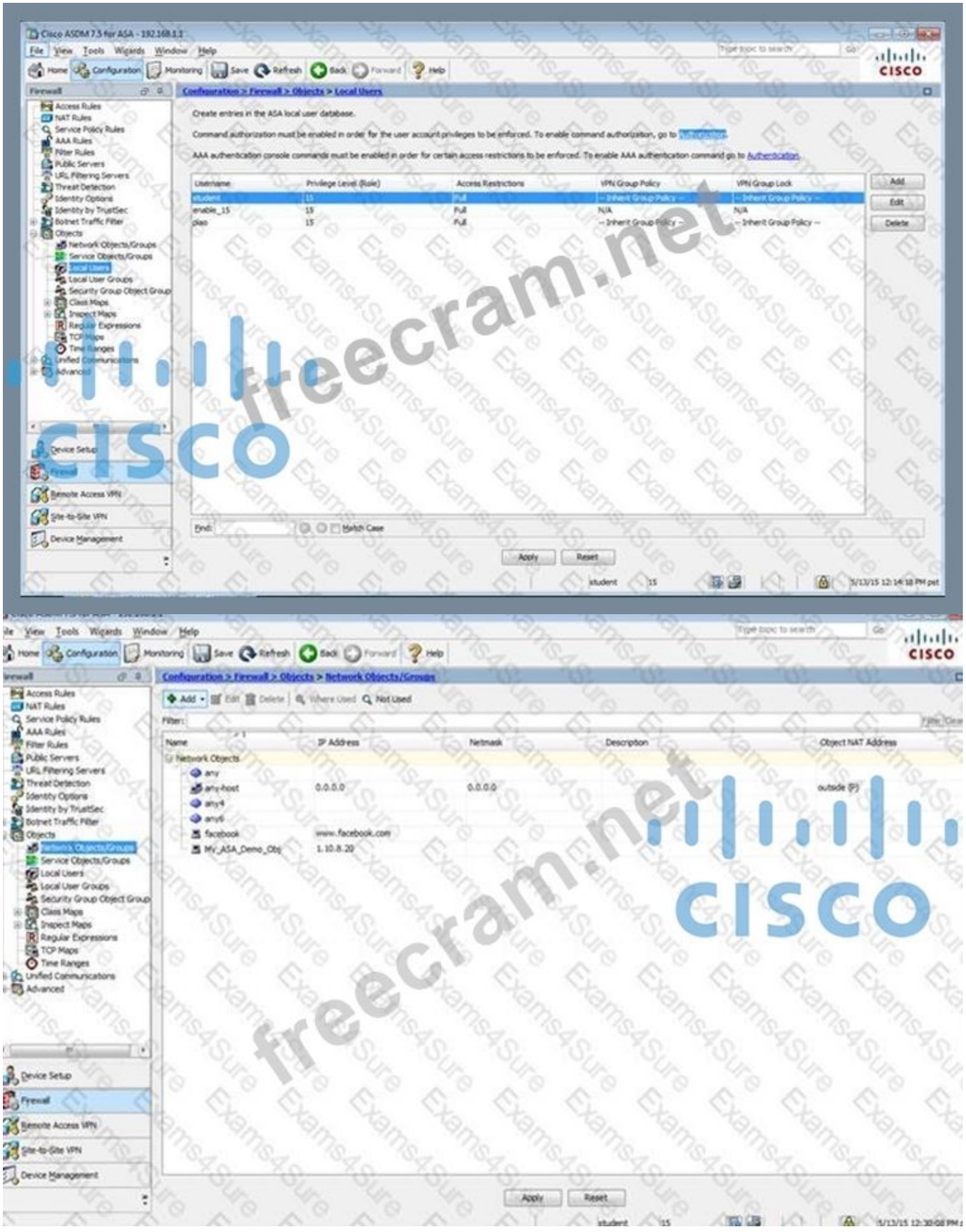



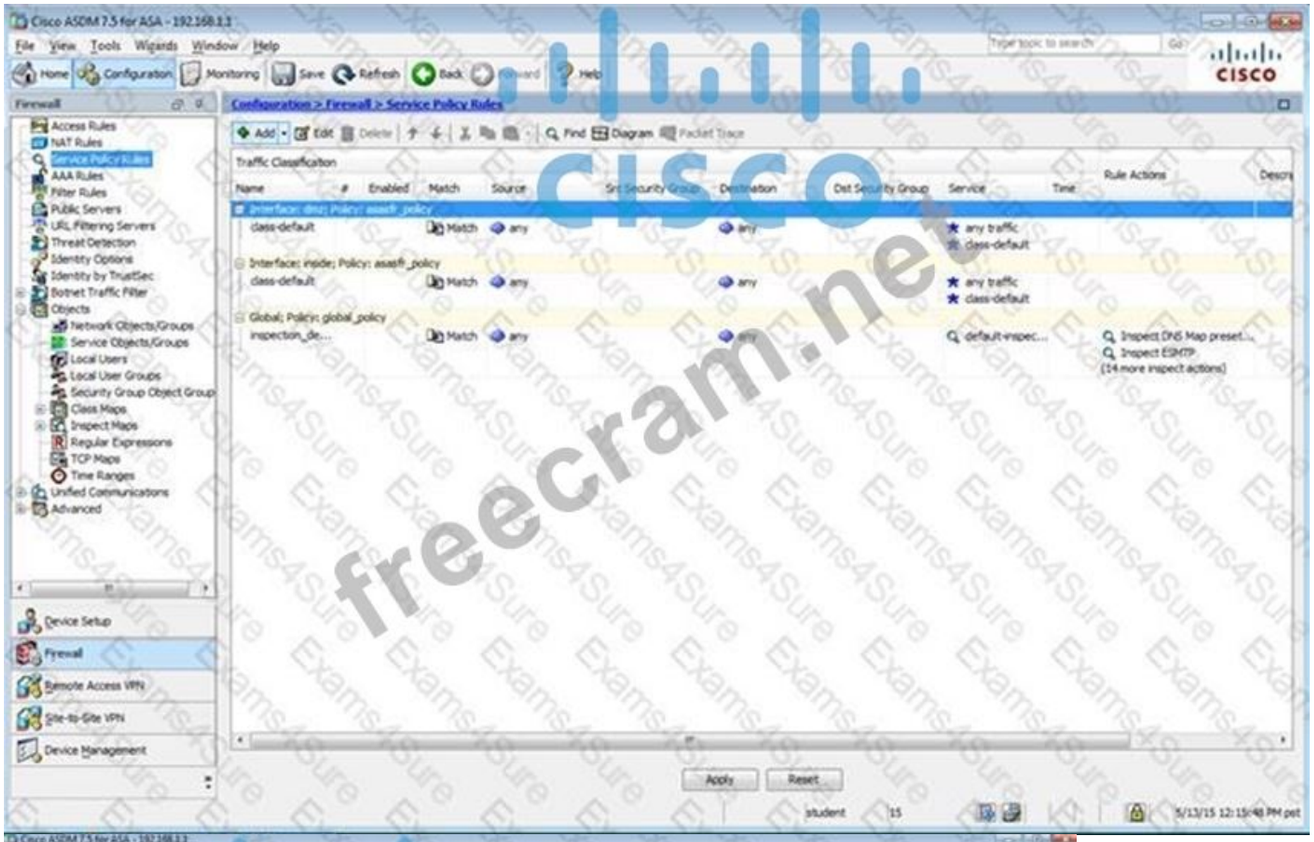


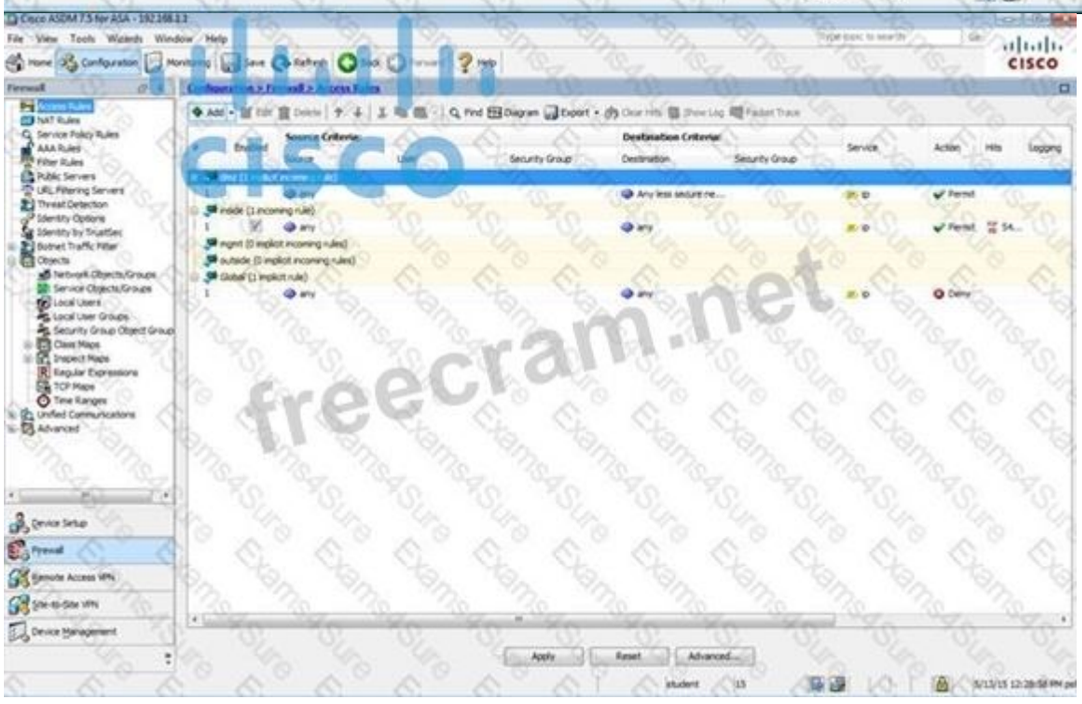


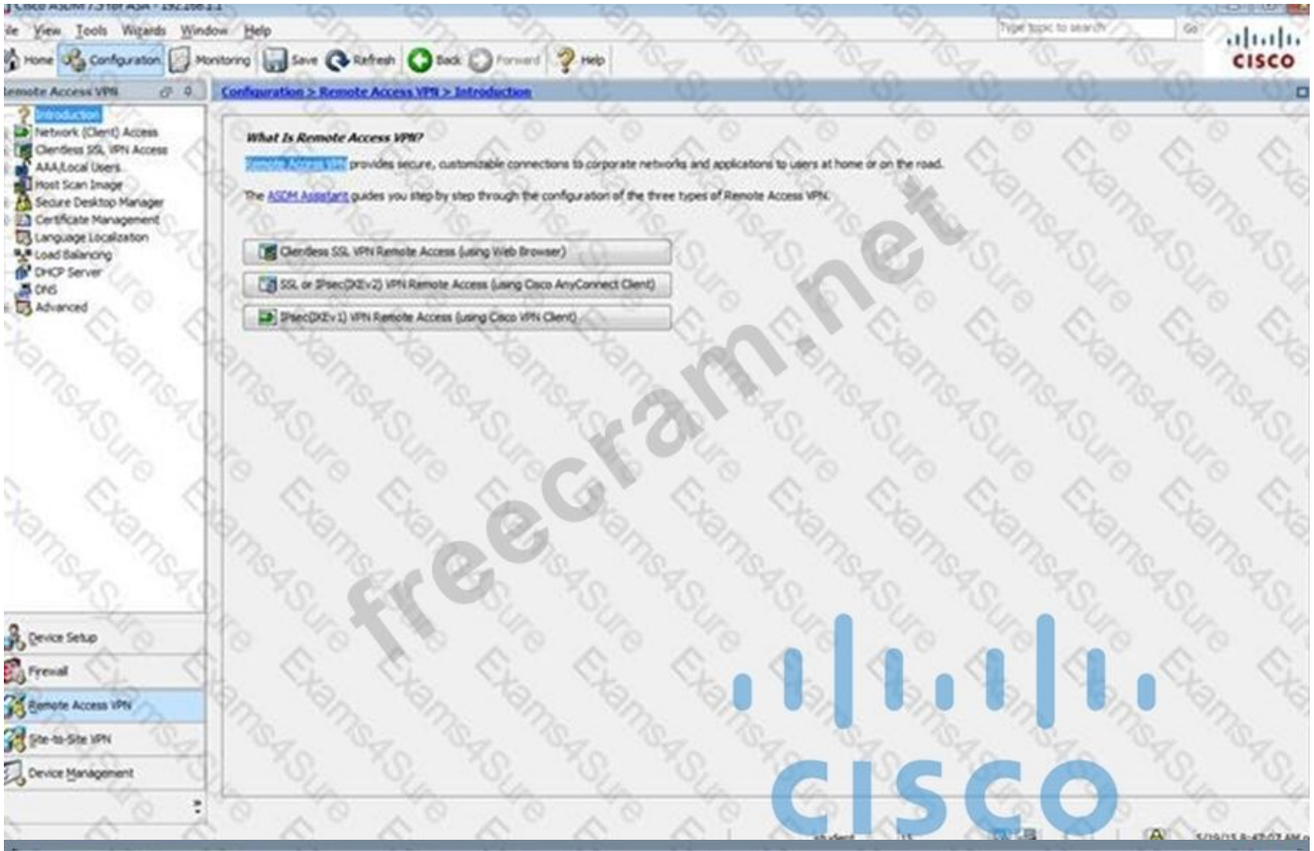



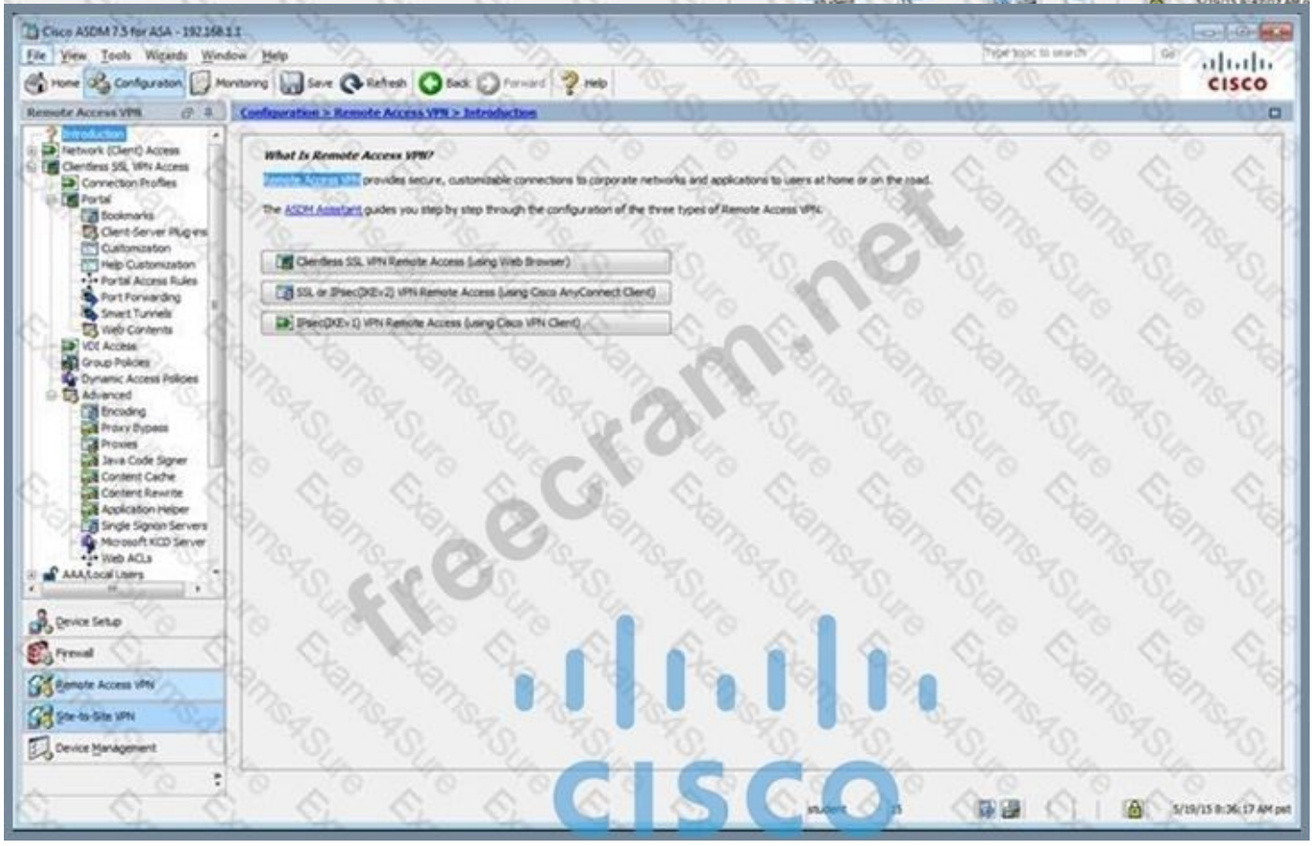

Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication
Authorization
Accounting
Enable authorization for ASA command access.
HTTP
Server Group:
LOCAL
Enable
Use LOCAL when server group fails
Perform authorization for exec shell access
When enabled, authorization will 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
Apply
Reset
Cisco ASDM 7.5 for ASA - 192.168.1.1
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Enable accounting for administrator and command accounting to the ASA.
Require accounting to allow accounting of user activity
Require accounting for the following types of connections
Serial
SSH
Telnet
Require command accounting for ASA
Privilege level:
Apply
Reset
student
15

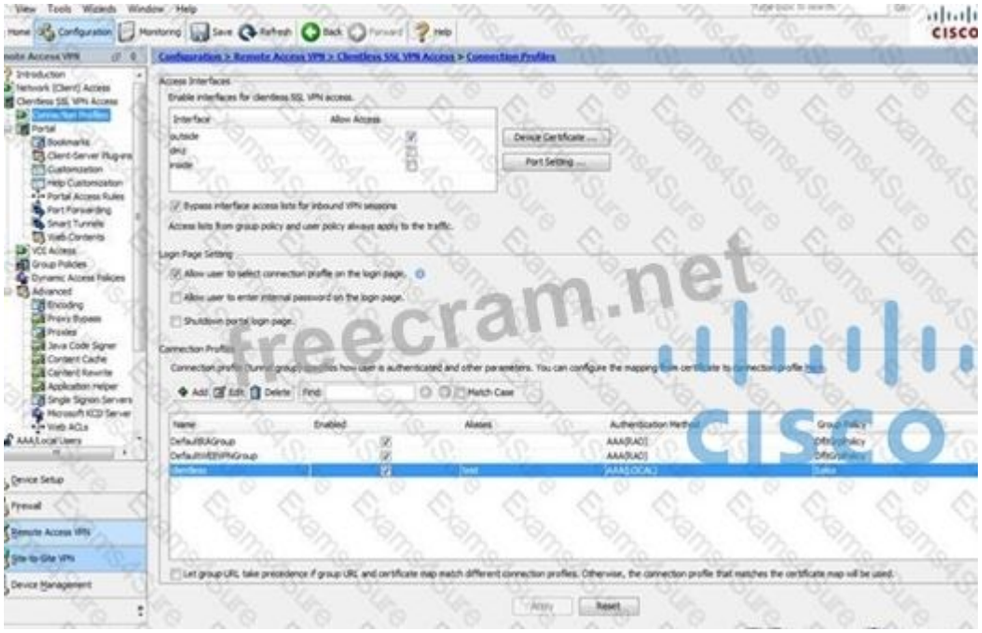

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Objects > Local Users
Create entries in the ASA local user database.
Command authorization must be enabled in order for the user 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 Group
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
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
5/13/15 12:30:08 PM

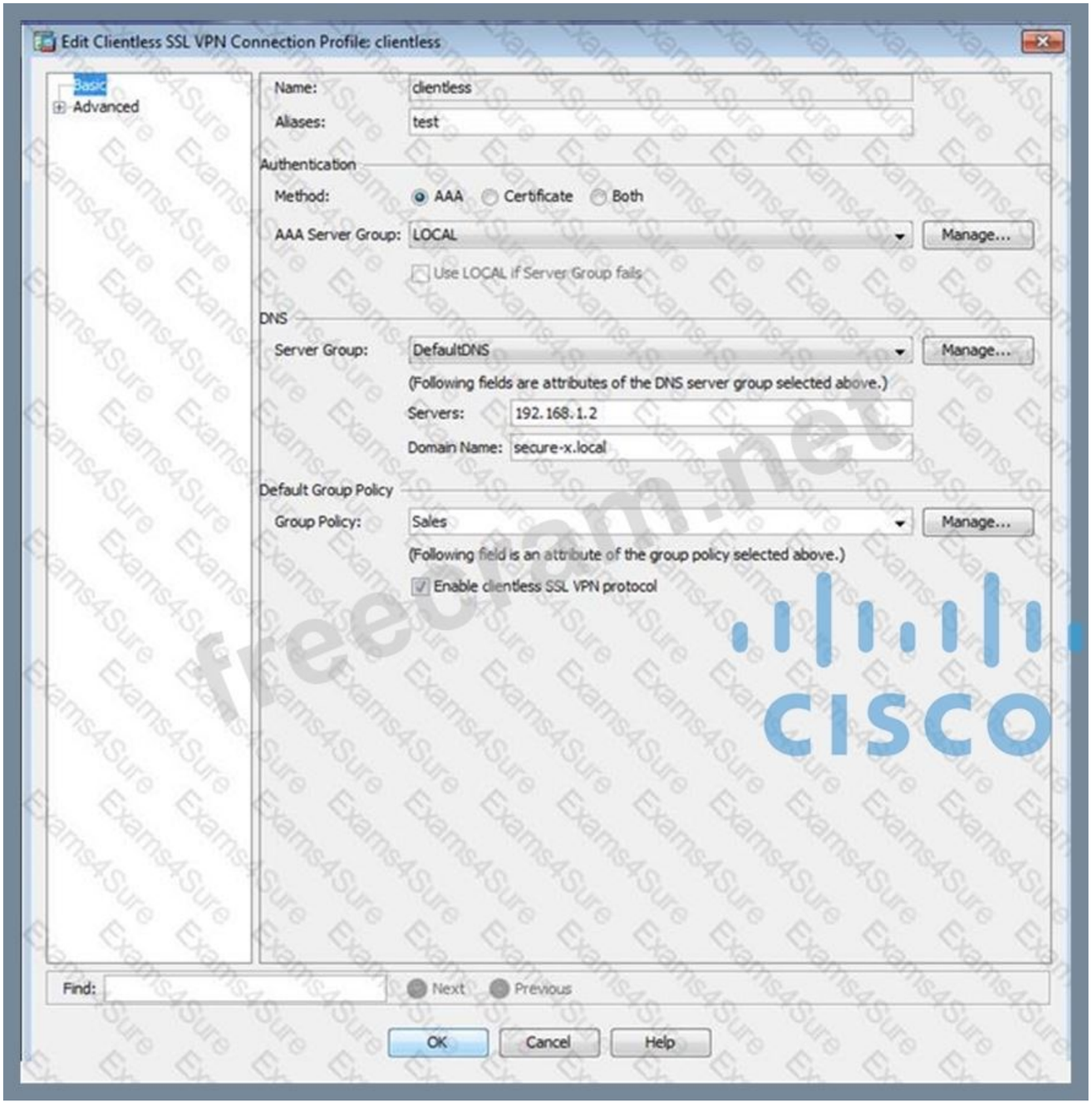

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Firewall
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security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

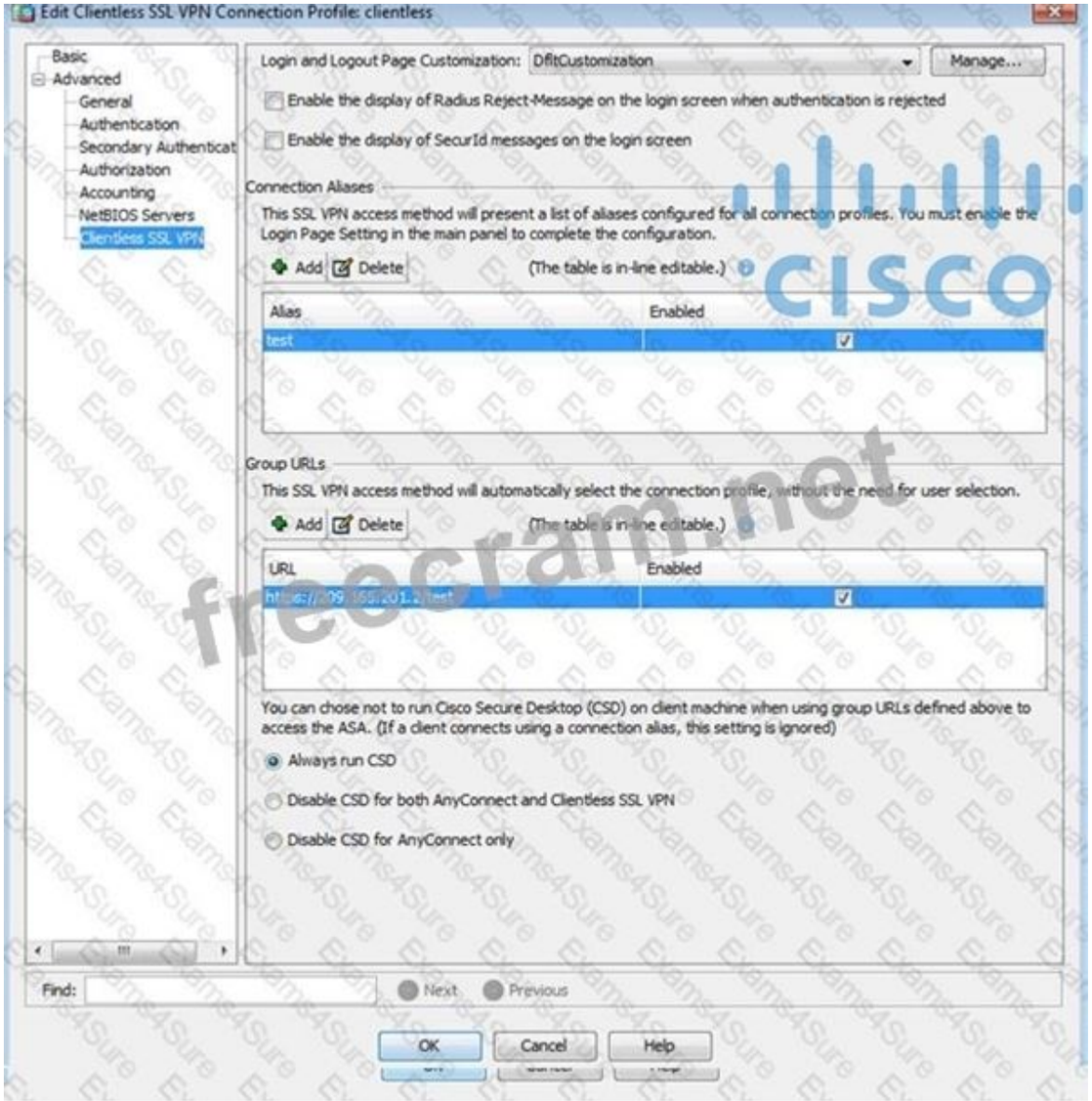

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
CISCO
Add Edit Delete Find Diagram Export Clear Hits Show Log Packet Trace
Source Criteria: Destination Criteria
Enabled Source Security Group Destination Security Group Service Action Hits Logging
inside (1 incoming rule)
mgmt (0 implicit incoming rules)
outside (0 implicit incoming rules)
Global (1 implicit rule)
Any less secure ne... ip Permit
any any ip Permit
any any ip Deny
Apply Reset Advanced...
student 15

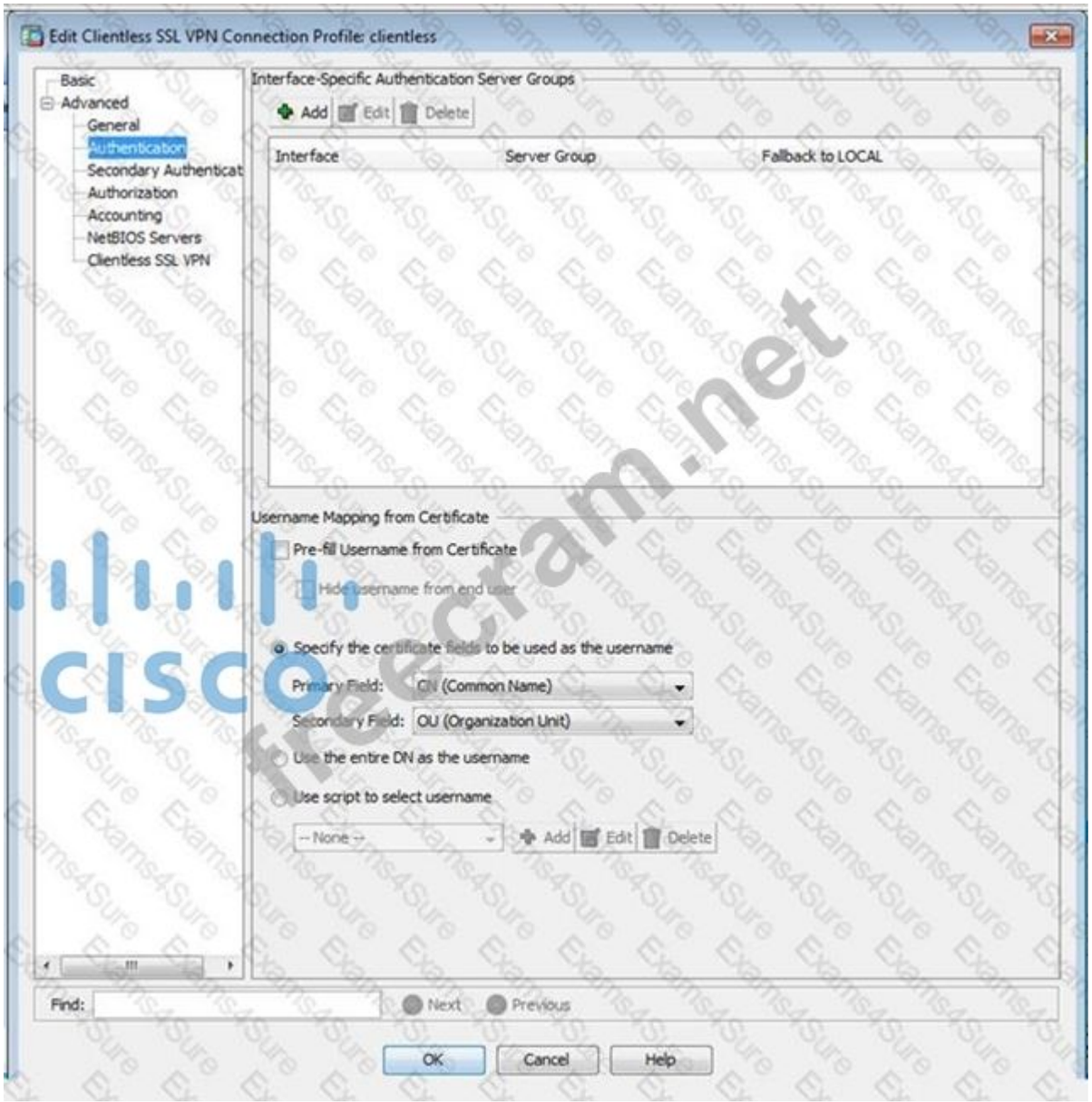

File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
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

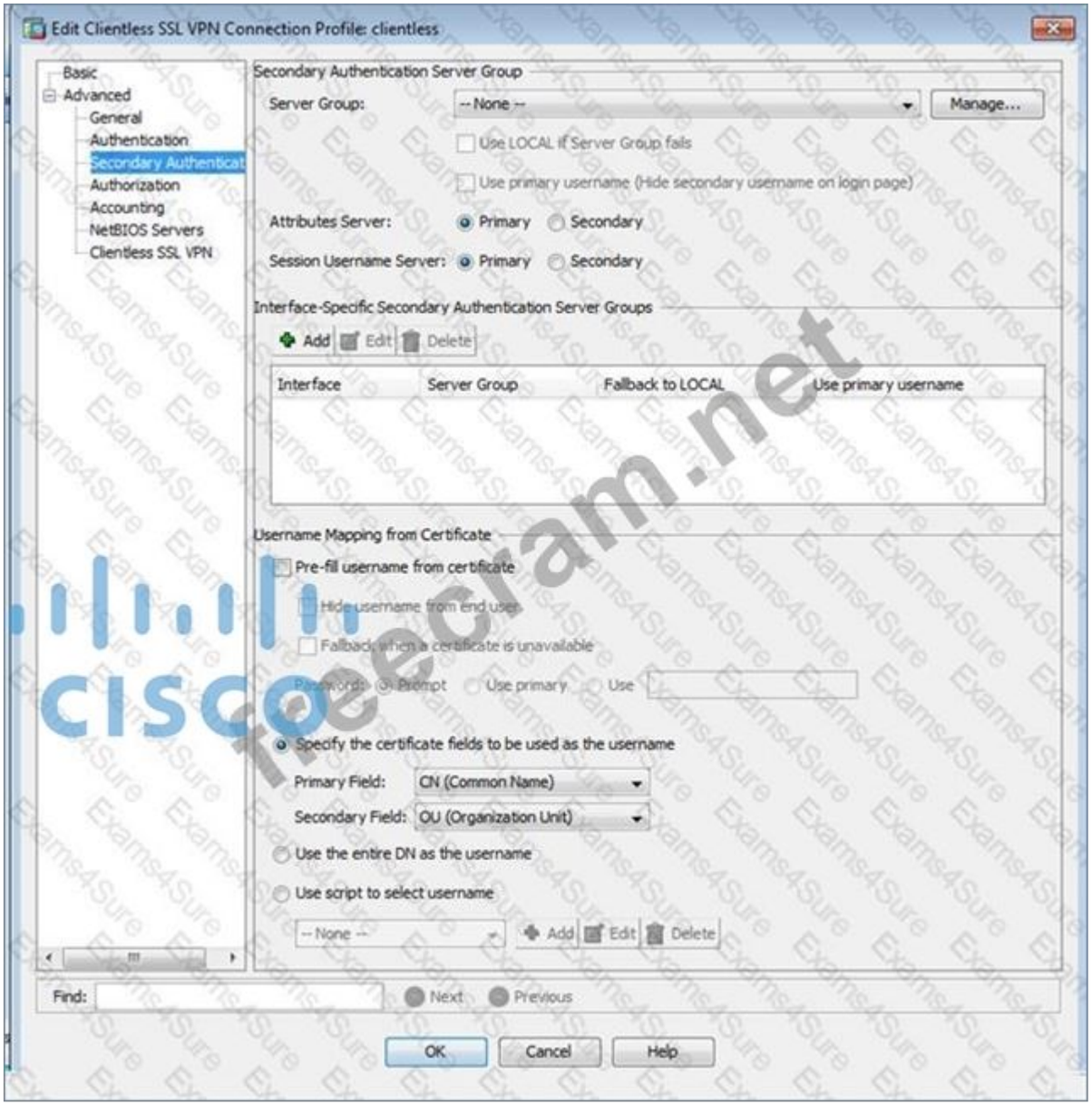

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Introduction
Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
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
5/19/15 8:36:17 AM pst

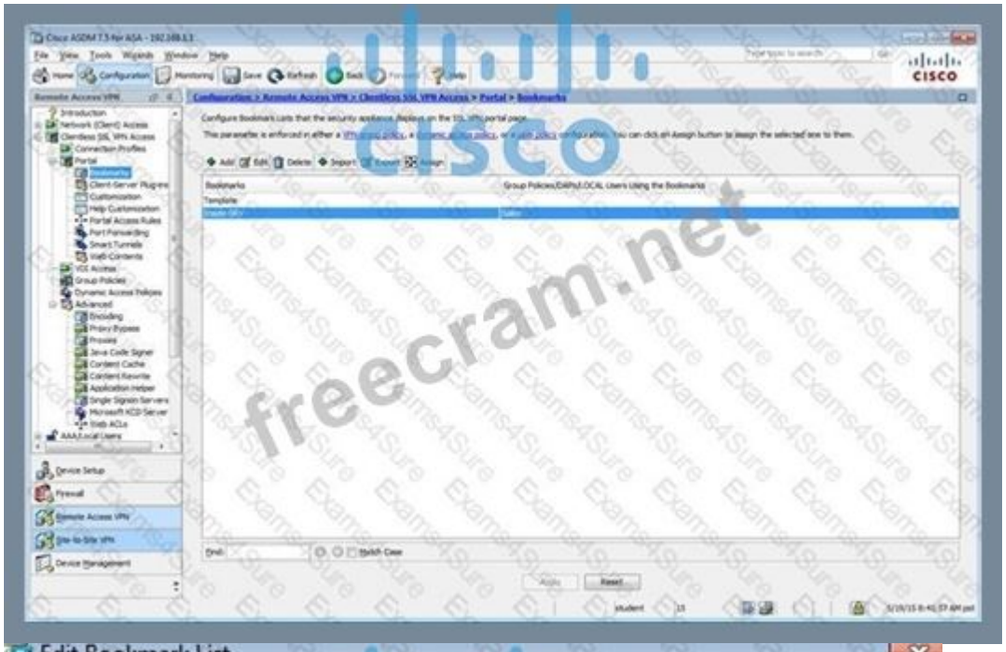


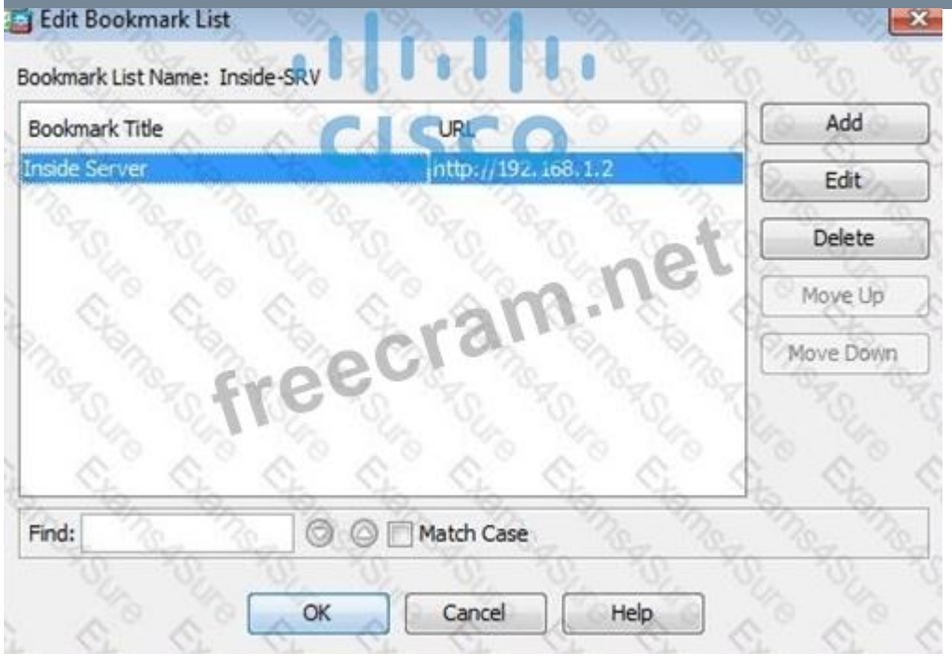

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
Name: clientless
Aliases: test
Authentication
Method: AAA Certificate Both
AAA Server Group: LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group: DefaultDNS
Manage...
(Following fields are attributes of the DNS server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

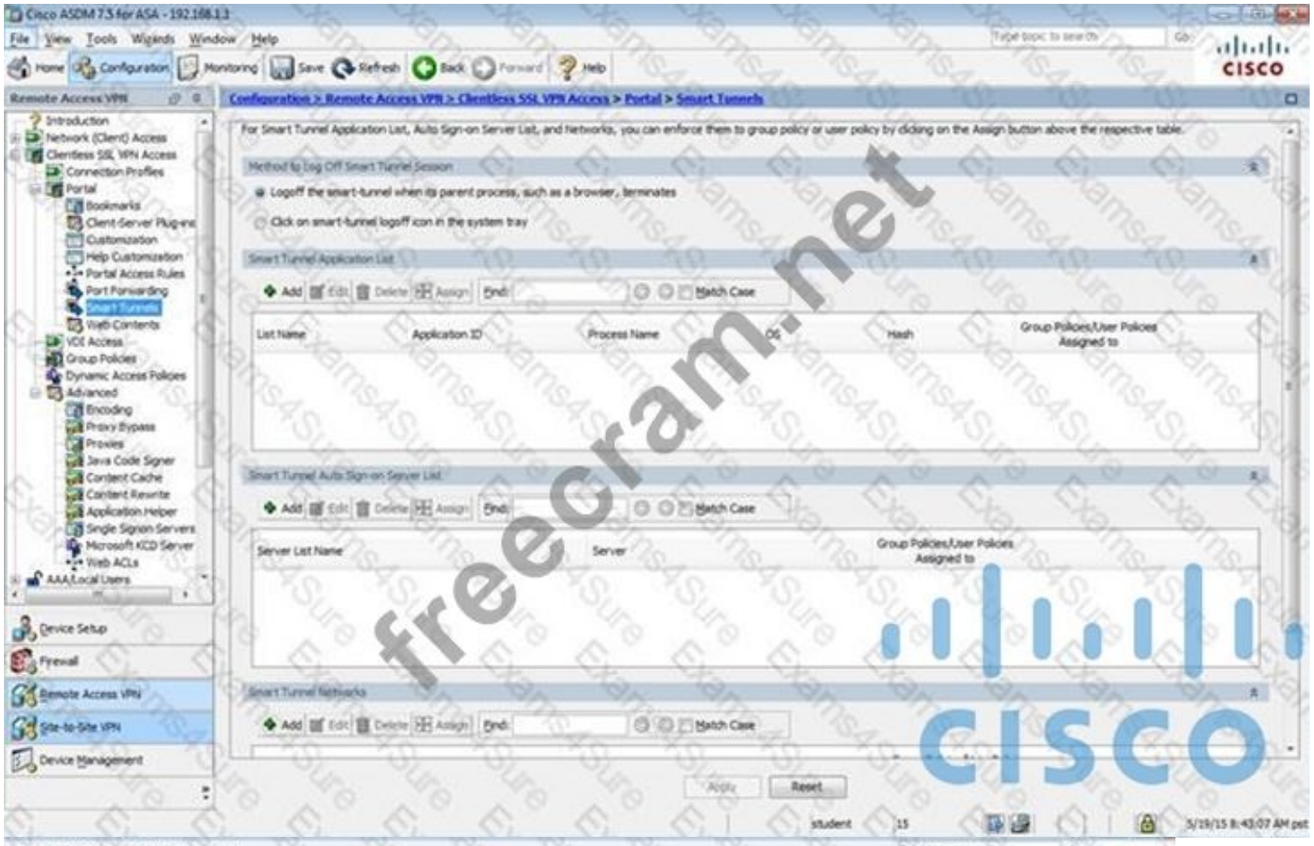

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Login and Logout Page Customization: DfltCustomization
Manage...
Enable the display of Radius Reject-Message on the login screen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

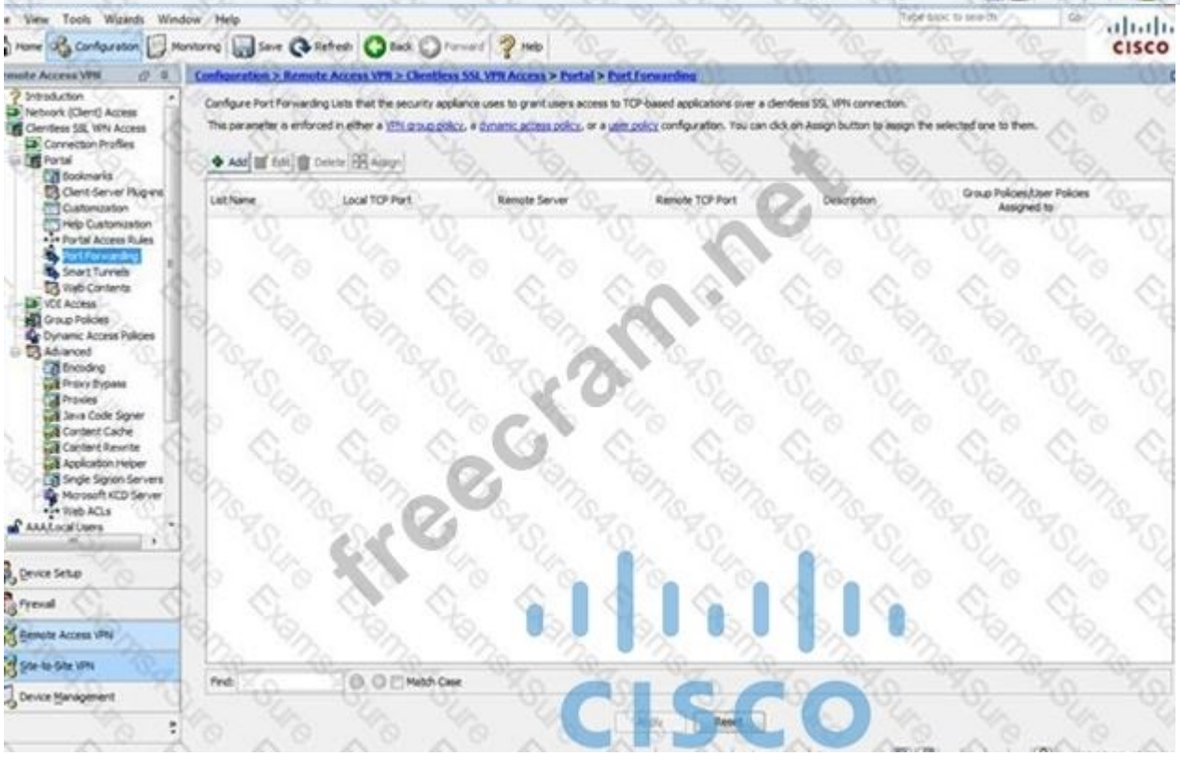

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Username Mapping from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

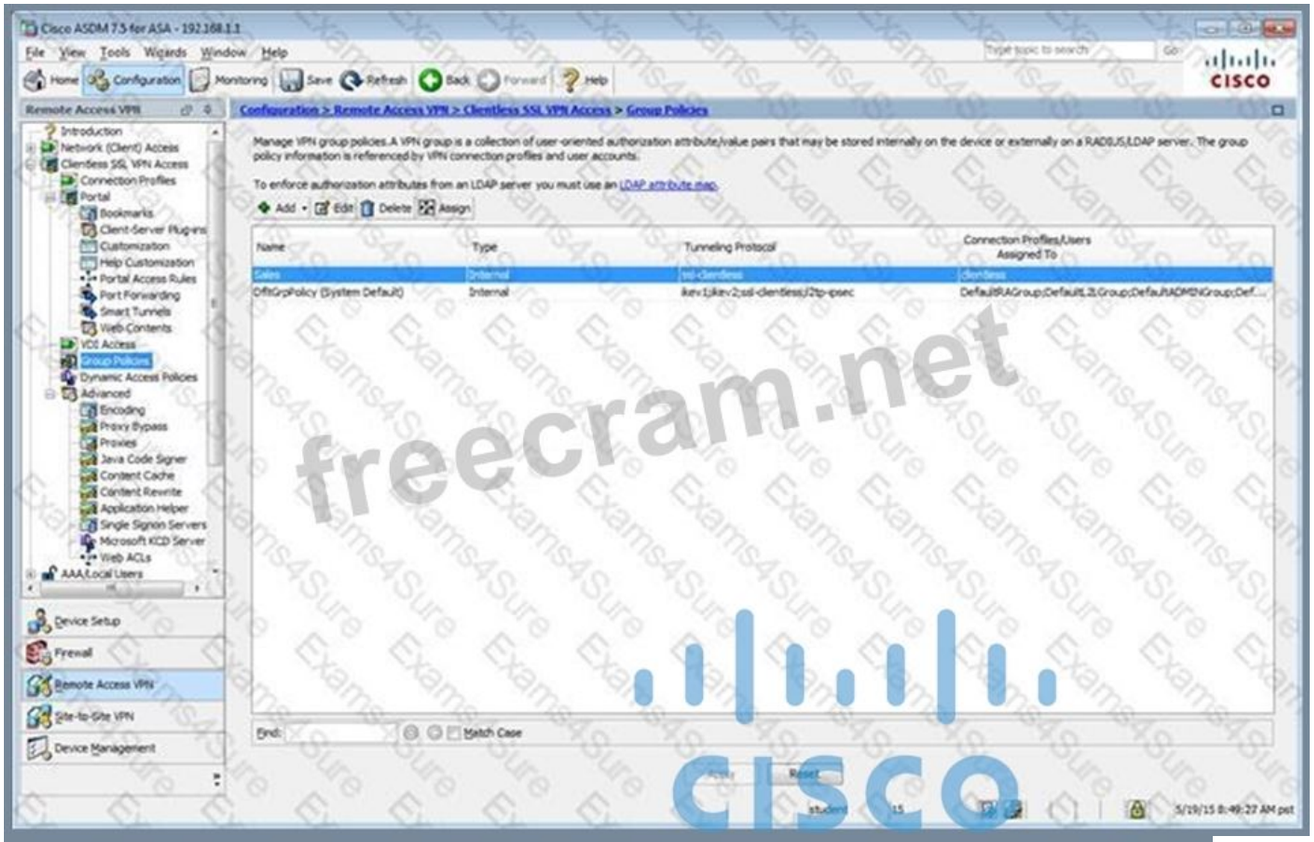

Edit Clientless SSL VPN Connection Profile: clientless
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
-- None --
Manage...
Use LOCAL if Server Group fails
Use primary username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

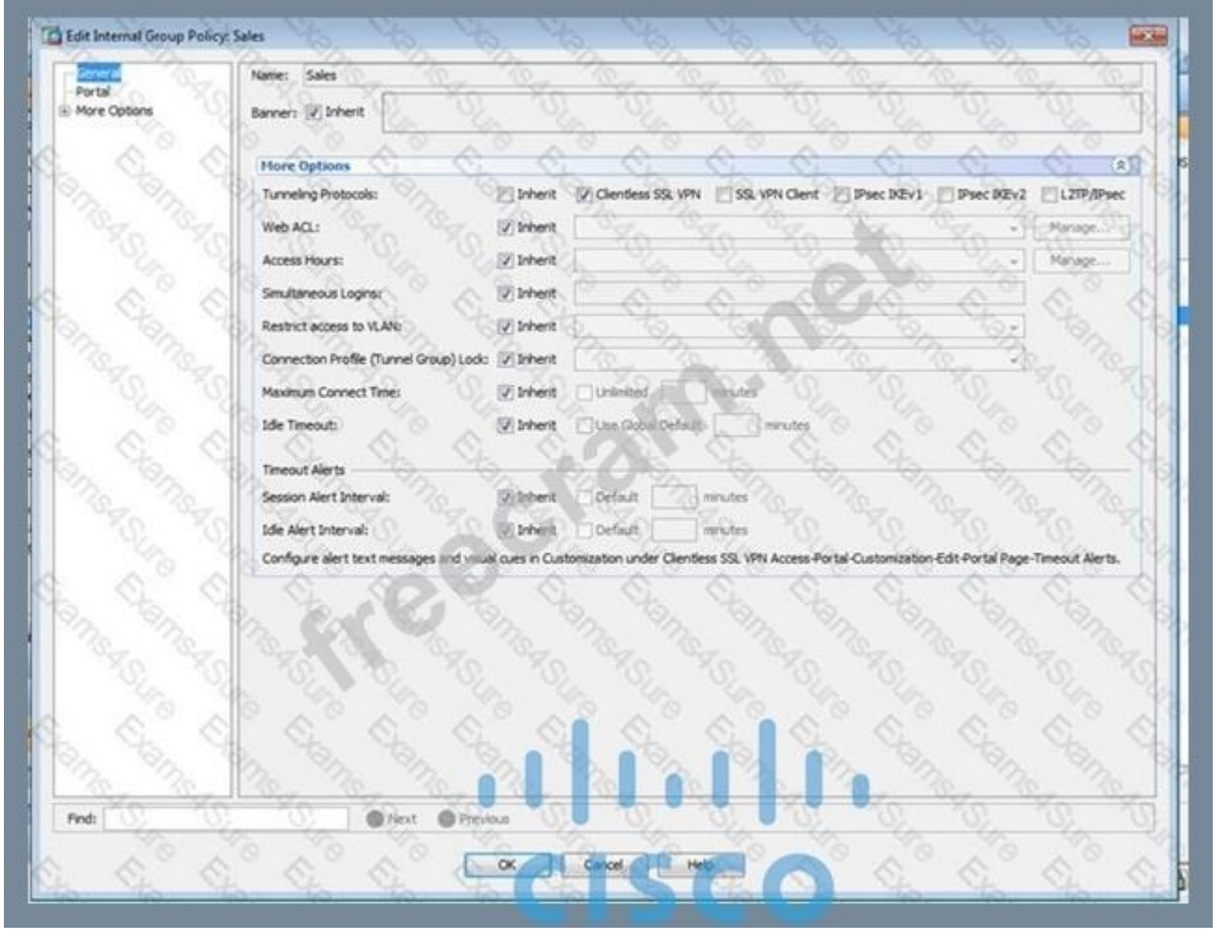


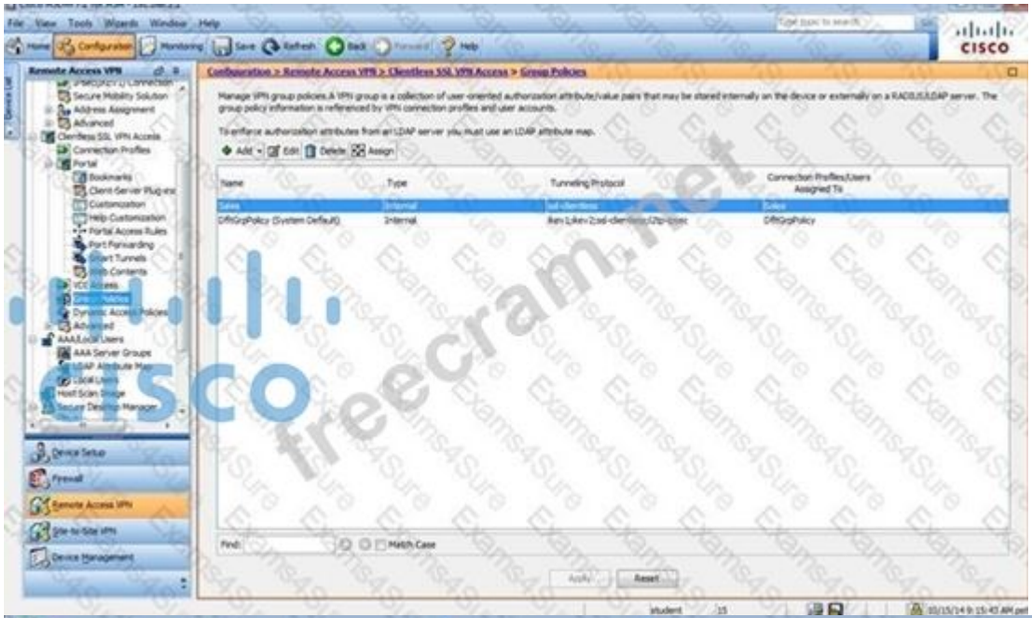

Edit Bookmark List
Bookmark List Name: Inside-SRV
Bookmark Title
URL
Inside Server
http://192.168.1.2
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help

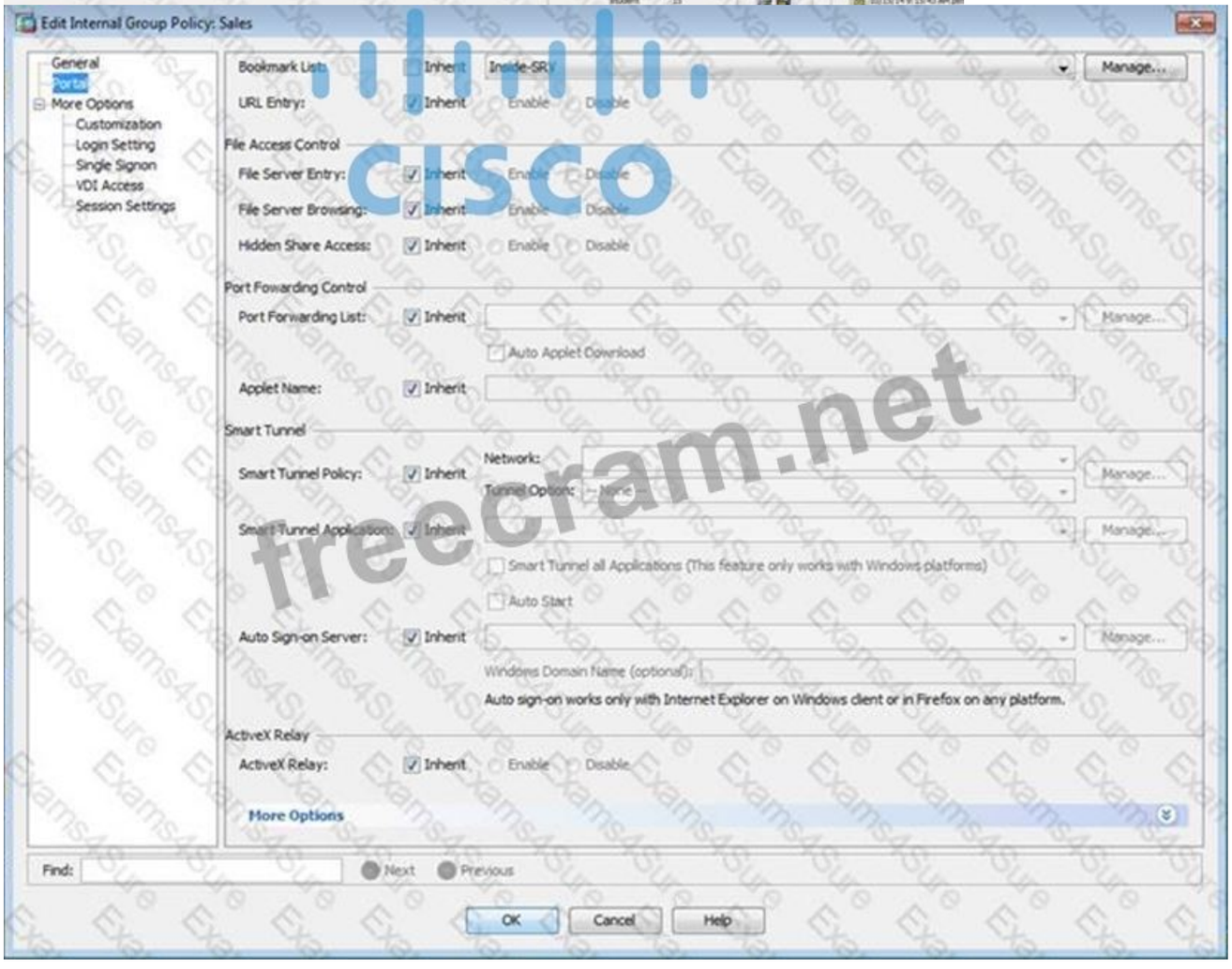


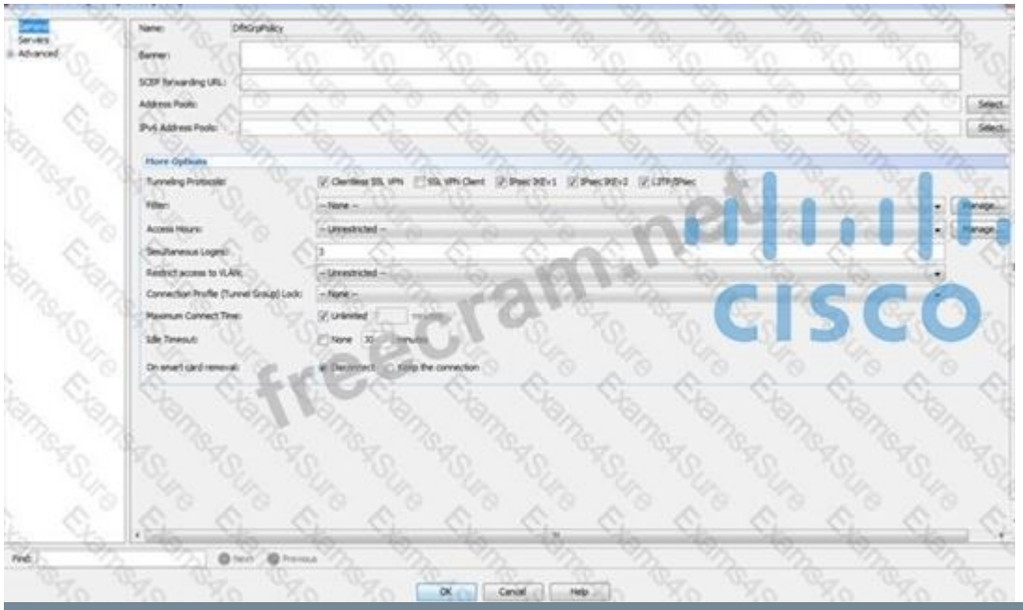



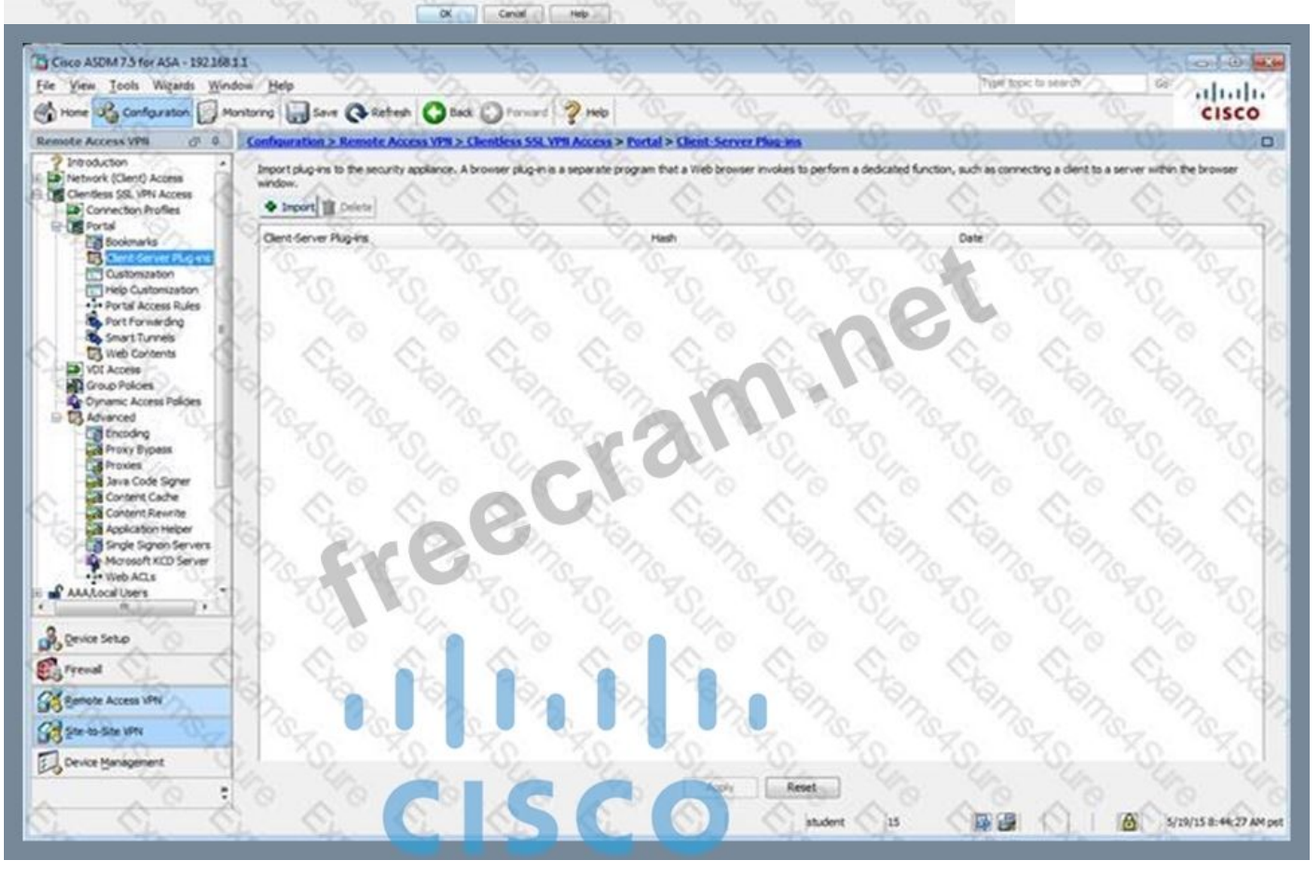

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented 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
5/19/15 8:49:27 AM pst

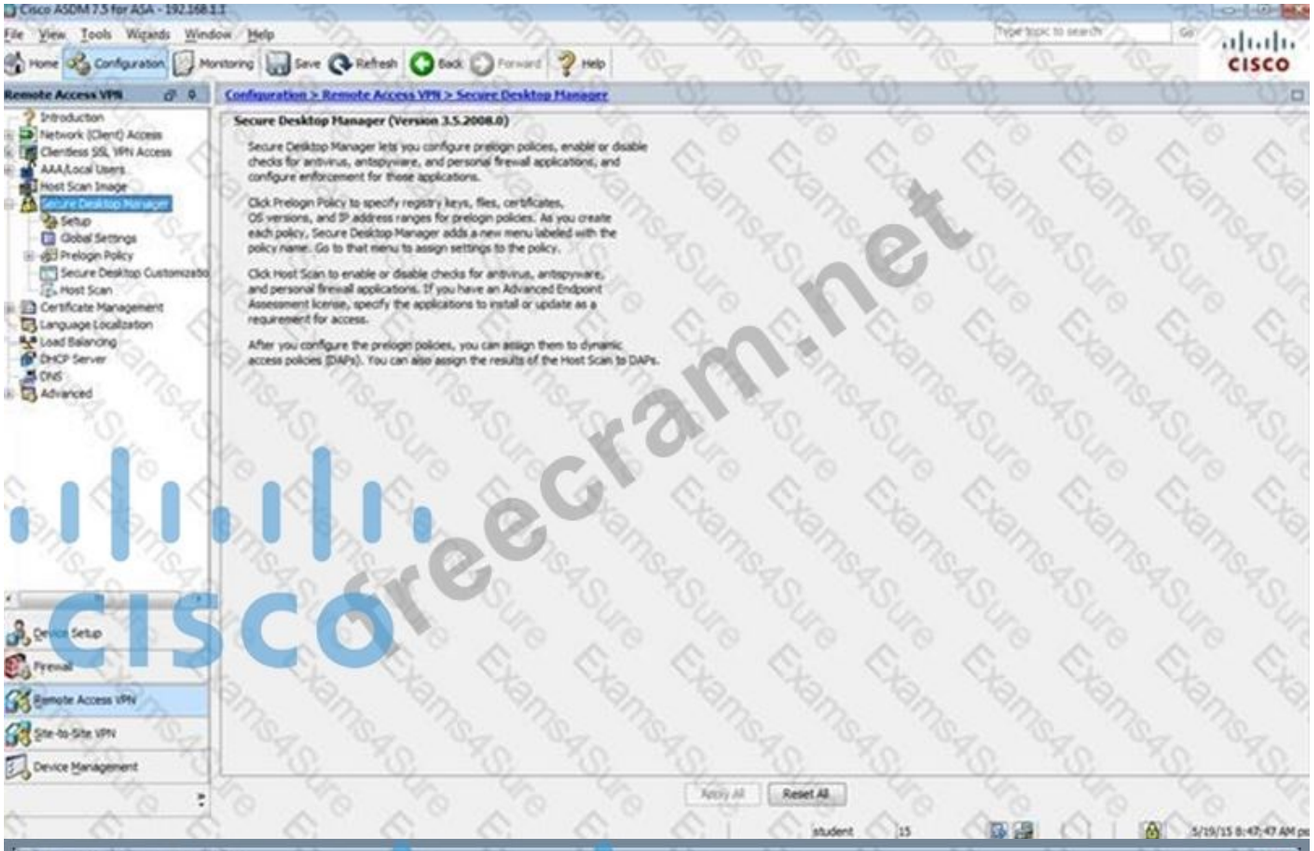

Edit Internal Group Policy: Sales
General
Portal
More Options
Name: Sales
Banner: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
Web ACL: Inherit Manage...
Access Hours: Inherit Manage...
Simultaneous Logins: Inherit
Restrict access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

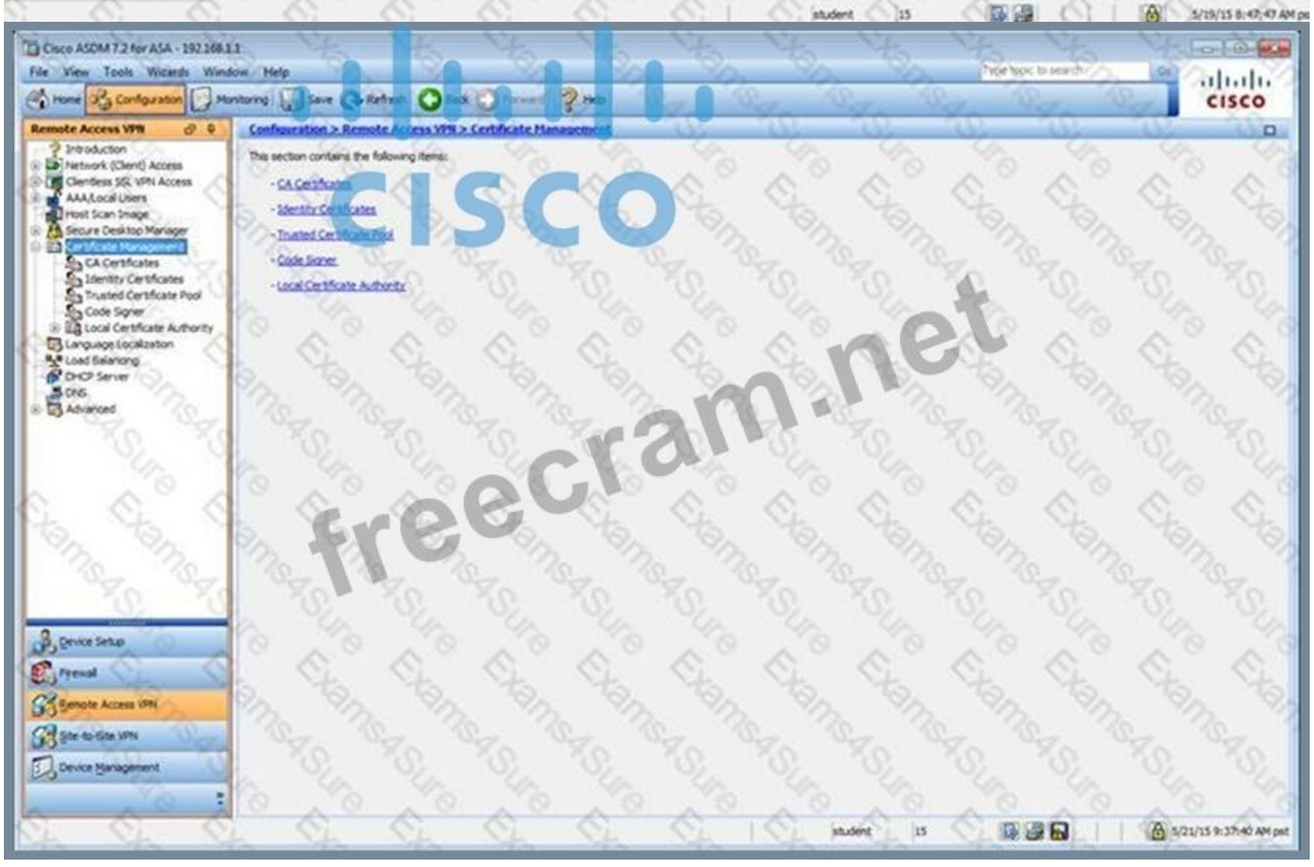


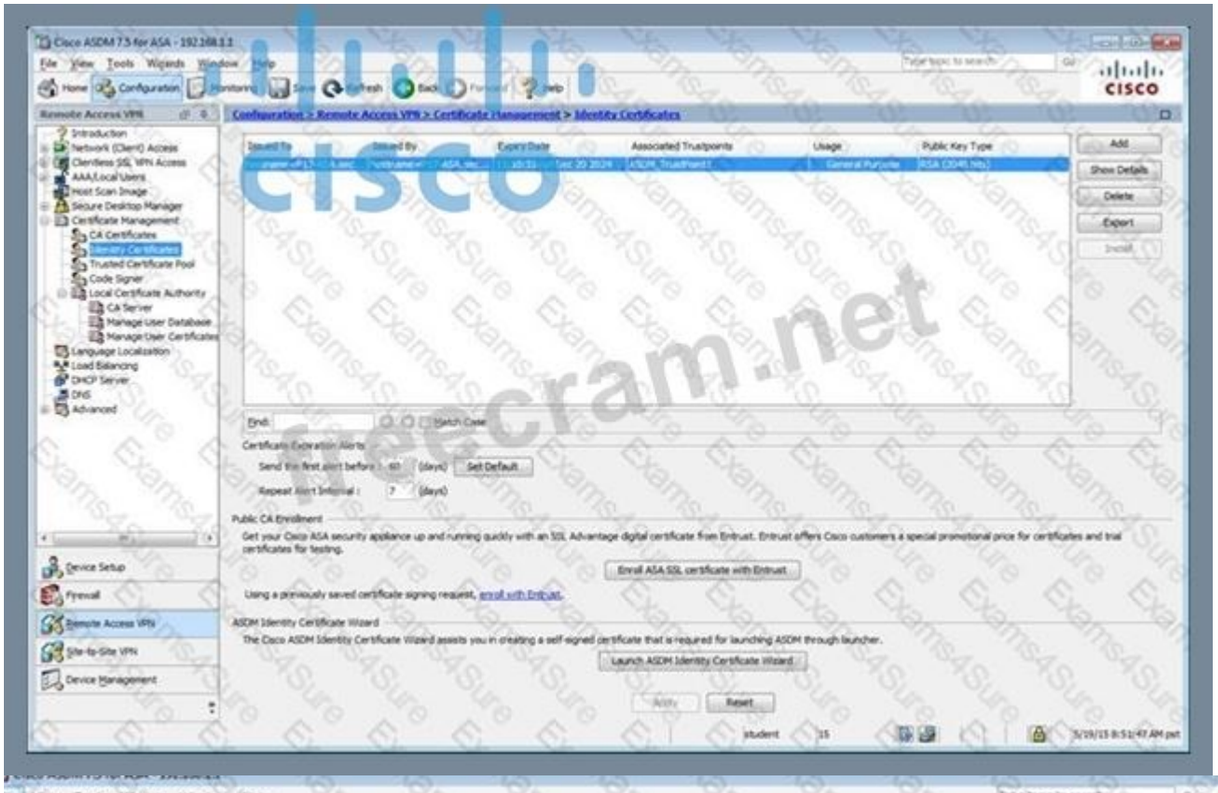



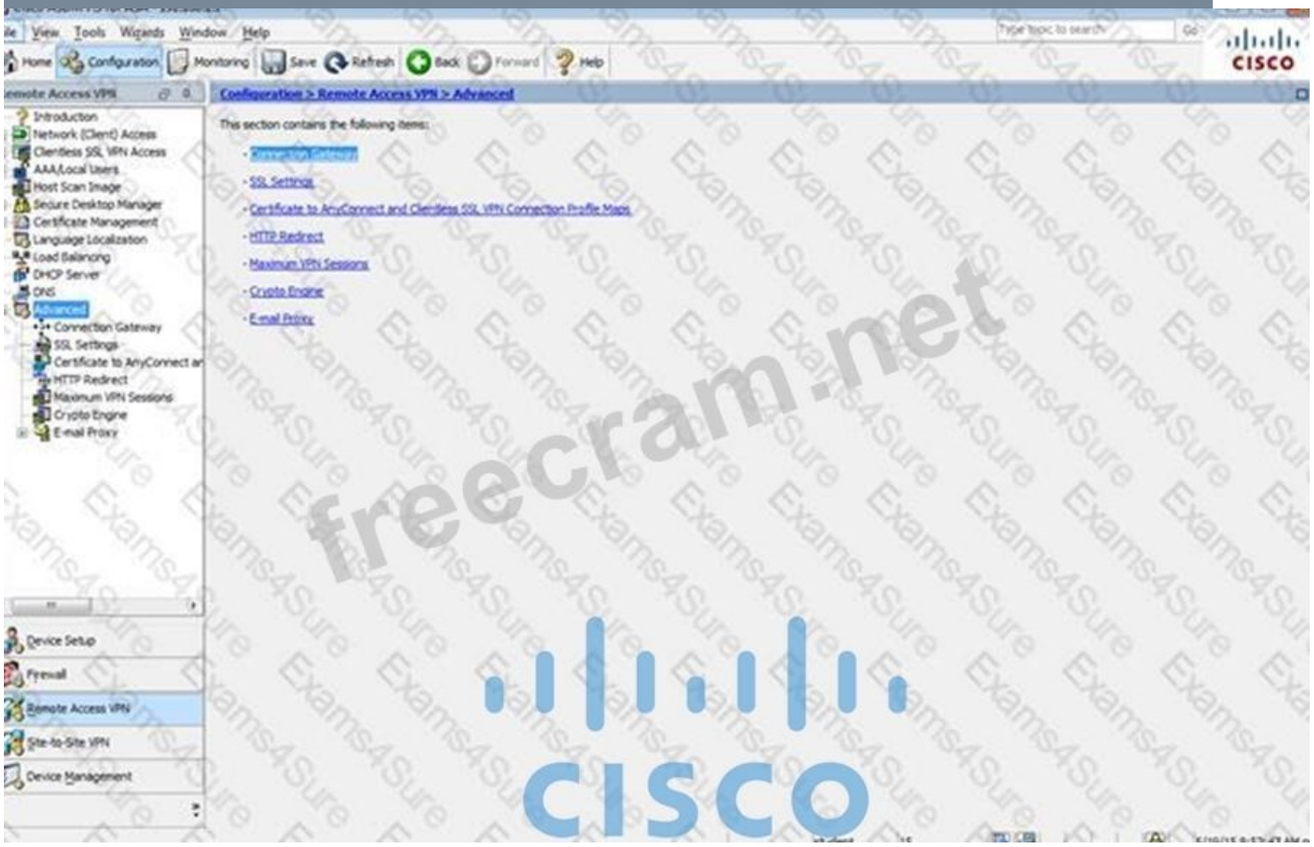


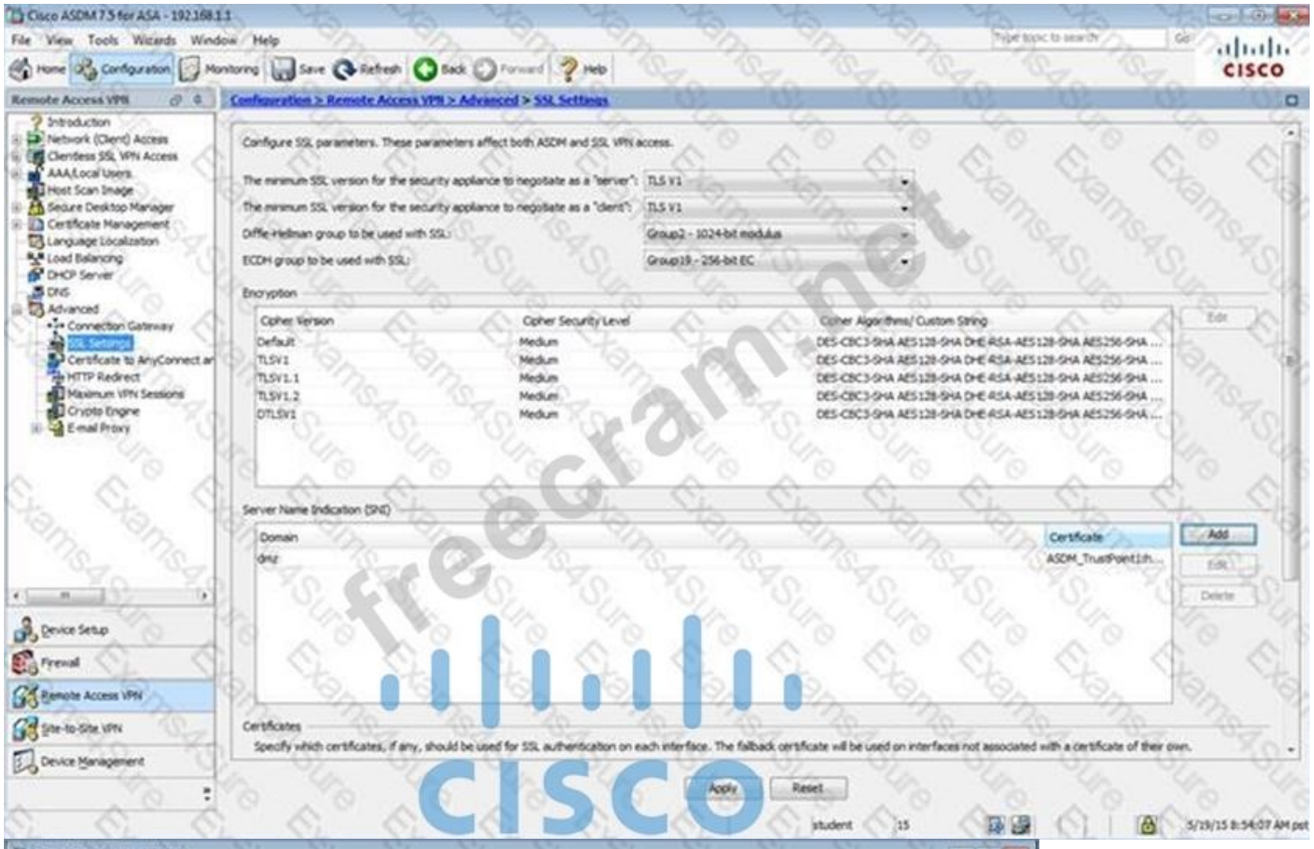



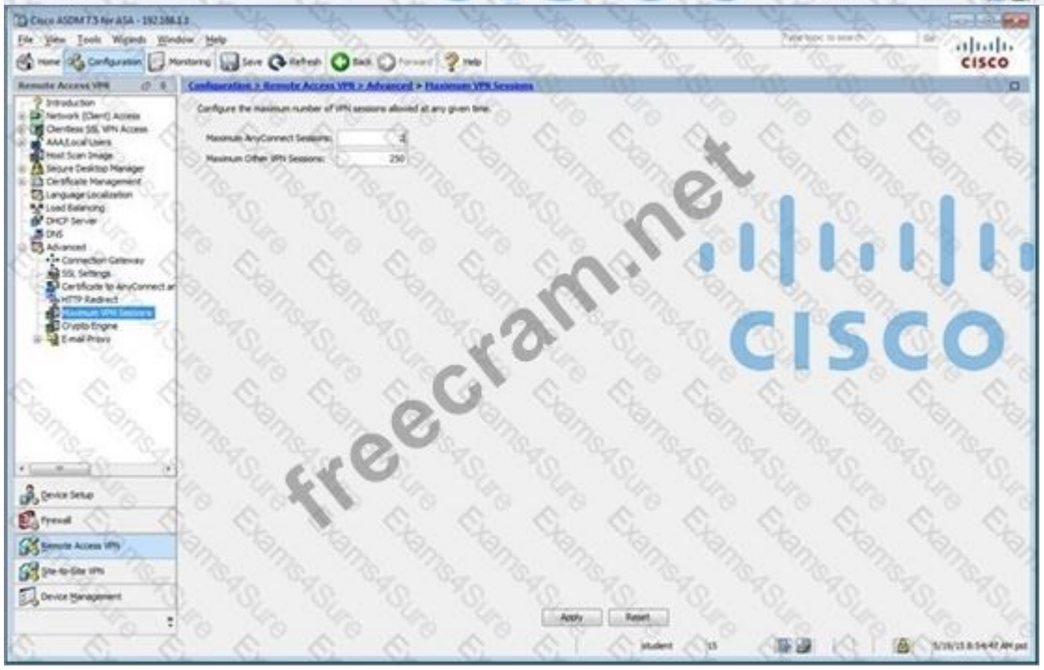


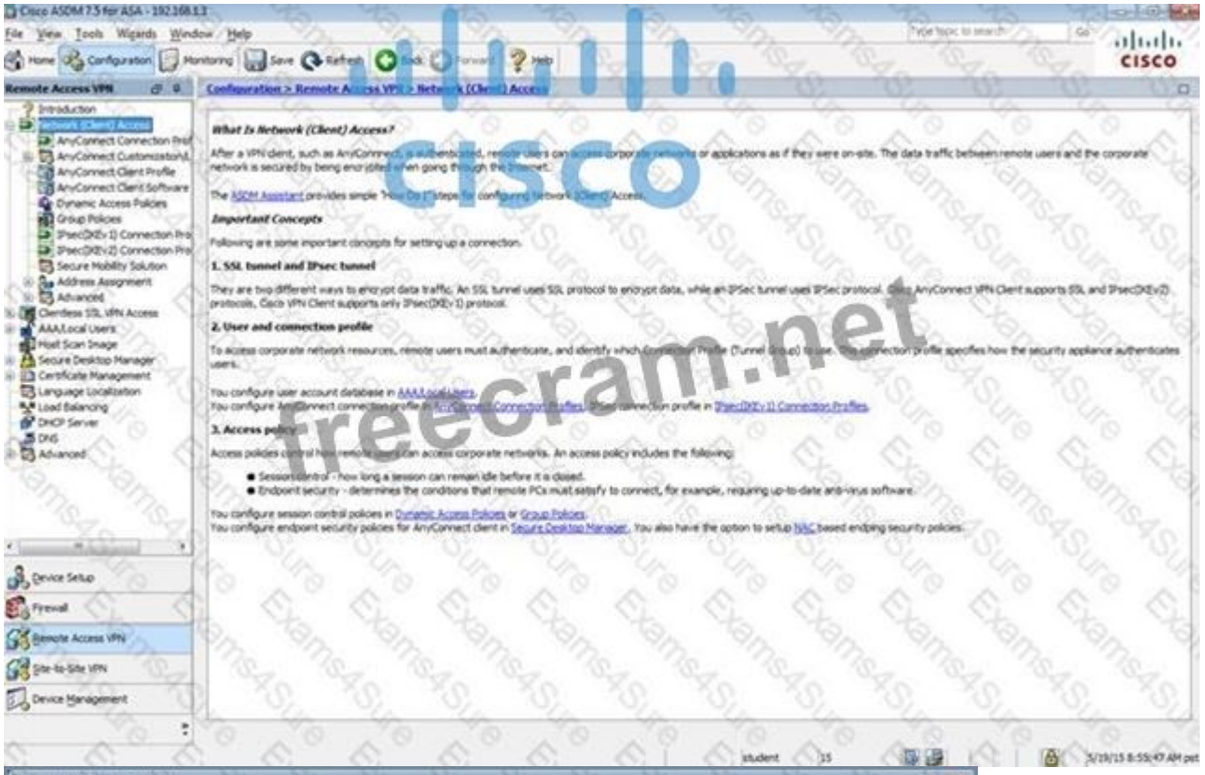



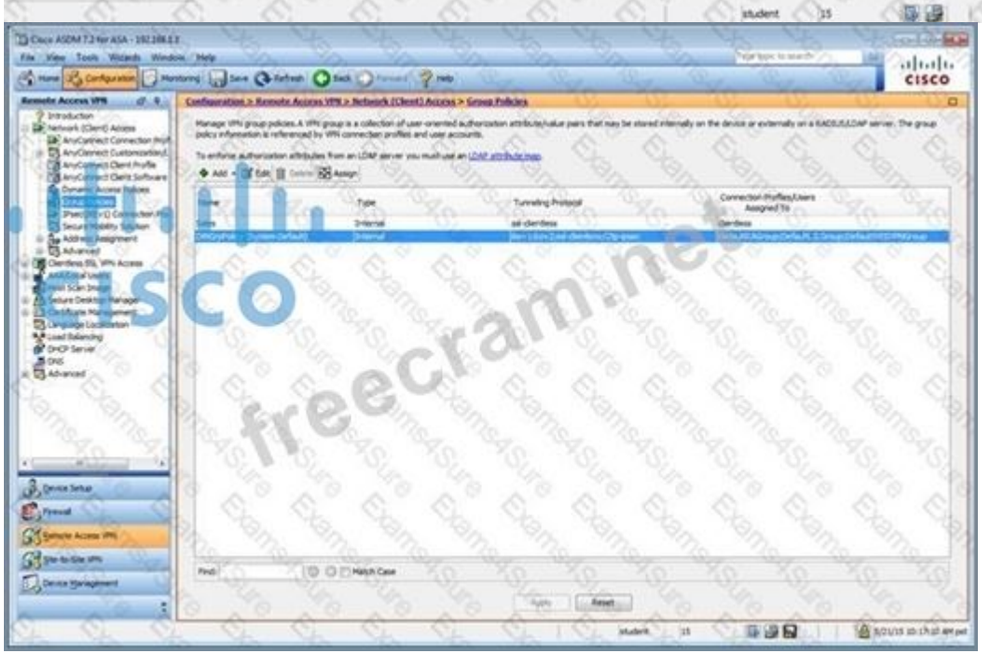


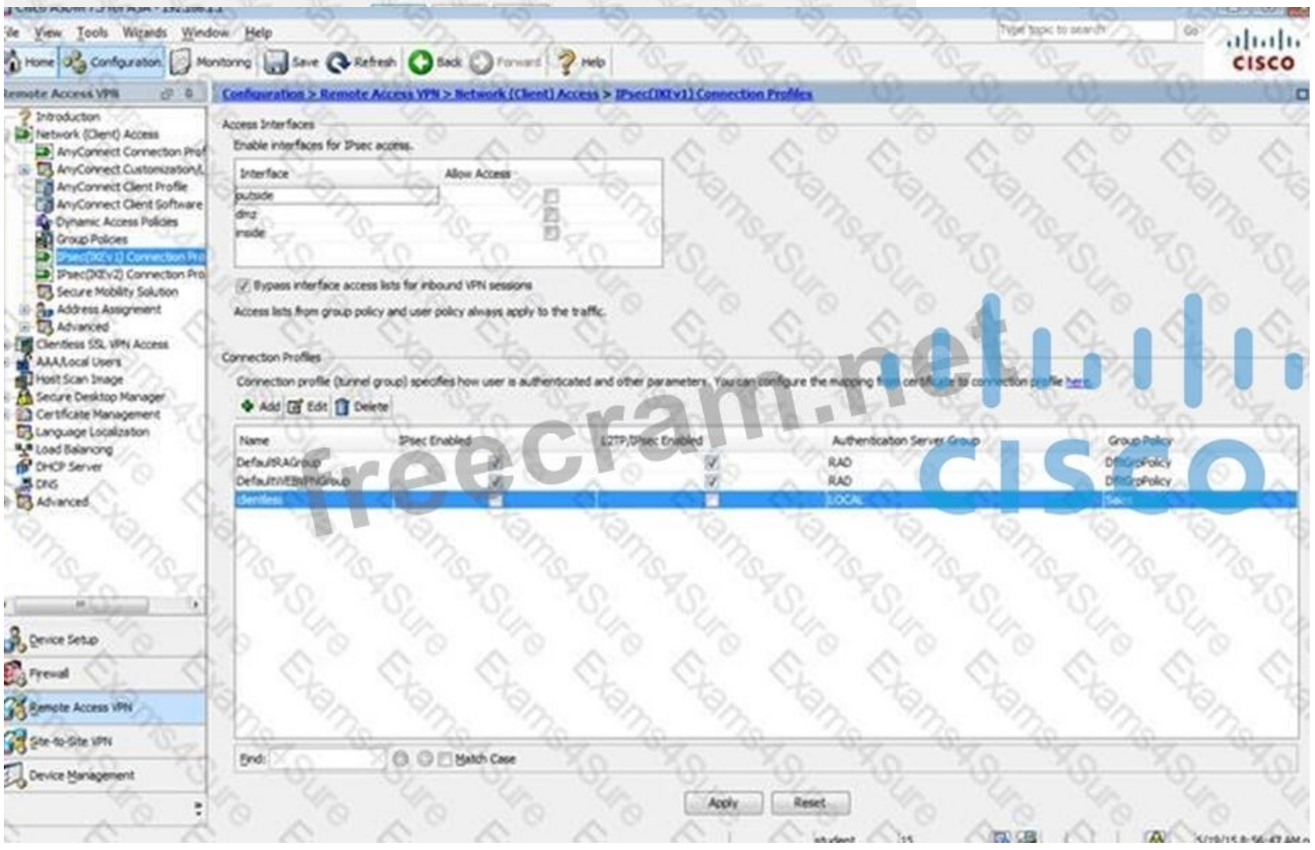



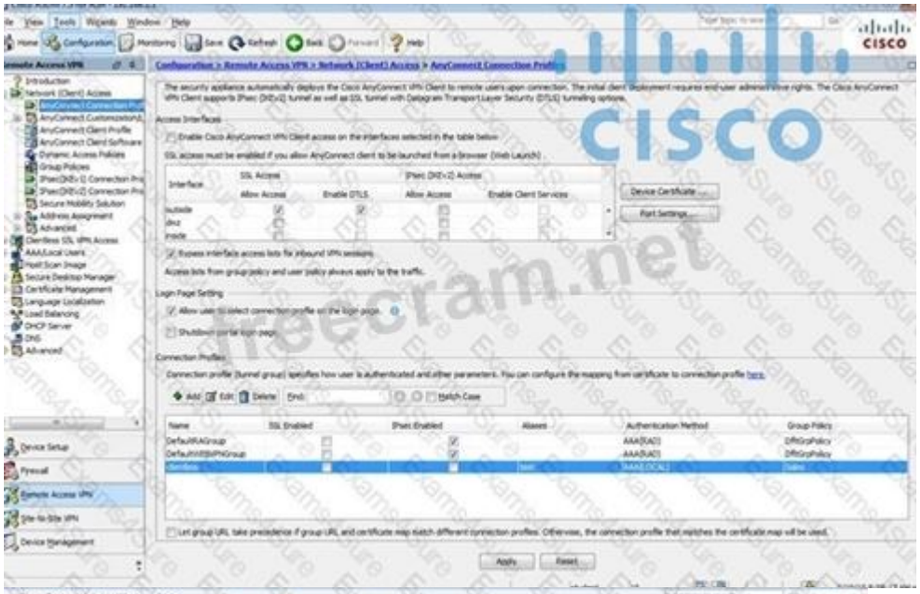

Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Advanced > SSL Settings
Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
Host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

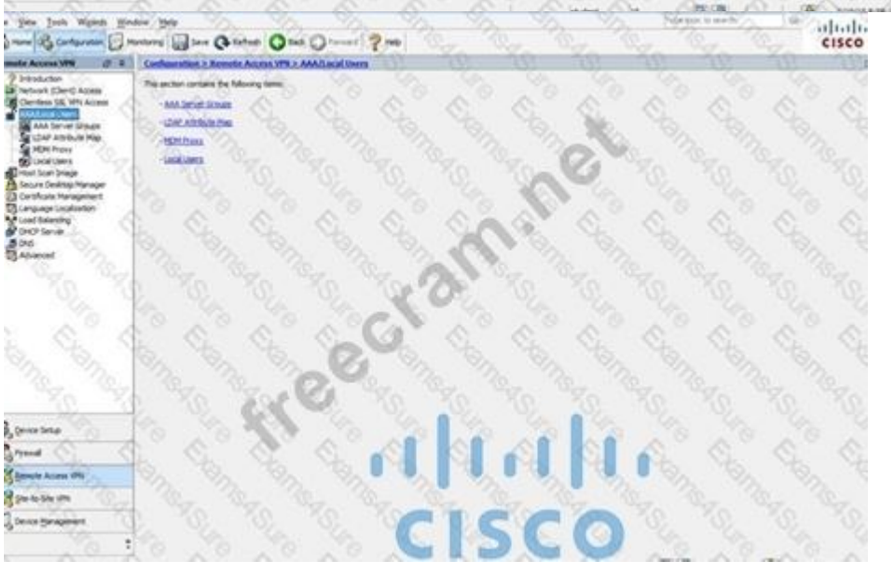

Cisco ASDM 7.5 for ASA - 192.168.1.1
CISCO
Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions
Configure the maximum number of VPN sessions allowed at any given time.
Maximum AnyConnect Sessions:
Maximum Other VPN Sessions:
250
Apply
Reset
student
15


Cisco ASDM 7.5 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
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
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. The connection profile specifies how the security appliance authenticates users.
You configure user account database in AAA/Local Users.
You configure AnyConnect connection profile in AnyConnect Connection Profiles. IPsec connection profile in IPsec(IKEv1) Connection Profiles.
3. Access policy
Access policies control how remote users can access corporate networks. An access policy includes the following:
Session control - how long a session can remain idle before it is closed.
Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.
You configure session control policies in Dynamic Access Policies or Group Policies.
You configure endpoint security policies for AnyConnect client in Secure Desktop Manager. You also have the option to setup NAC based endpoint security policies.
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15


Cisco ASDM 7.2 for ASA - 192.168.1.1
File View Tools Wizards Window 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
Internal
ssl-clientless
clientless
Find:
Match Case
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
student
15


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles
Introduction
Network (Client) Access
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
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.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Authentication Server Group
Group Policy
DefaultRAGroup
RAD
DefaultL2LGroup
RAD
clientless
LOCAL
Find:
Match Case
Apply
Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management




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

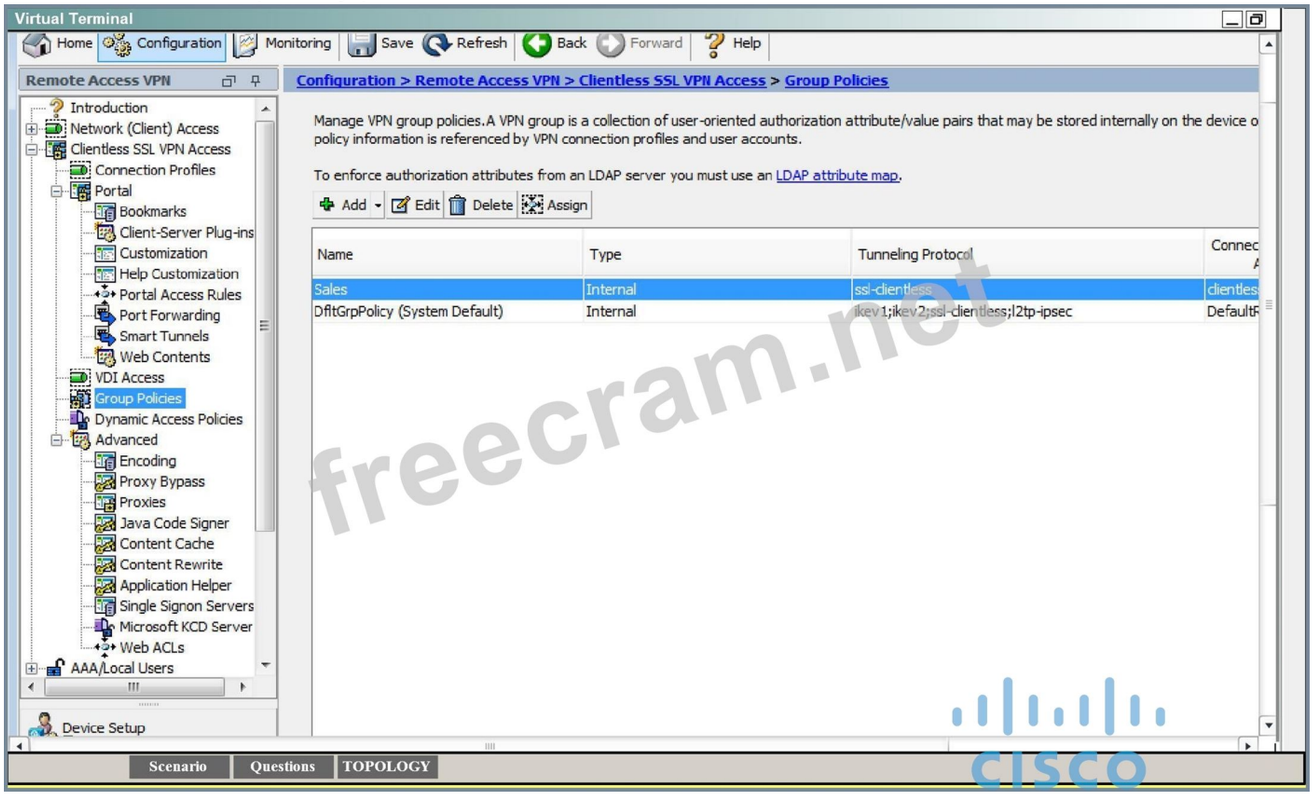
**E.** IPsec IKEv1

**F.** IPsec IKEv2

**Answer: (SHOW ANSWER)**

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: 89**

Which type of malicious software can create a back-door into a device or network?

**A.** Worm

**B.** Virus

**C.** Bot

**D.** Trojan

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 90**

**A.** username Operator privilege 1 password cisco

**B.** user name Operator privilege 15 password cisco

**C.** usemame Operator privilege 7 password Cisco

**D.** usemame Operator password cisco privilege 15

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 91**

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 (LEAVE A REPLY)**
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: 92**
With which preprocesor do you detect incomplete TCP handshakes
**A.** rate based prevention
**B.** portscan detection
**Answer: A (LEAVE A REPLY)**
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: 93**

Which options are filtering options used to display SDEE message types? (Choose two.)
**A.** stop
**B.** none
**C.** error
**D.** all
**Answer: (SHOW ANSWER)**
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: 94**
Which statement about college campus is true?
**A.** College campus has geographical position.
**B.** College campus Has very beautiful girls
**C.** College campus Hasn`t got internet access.
**D.** College campus Has multiple subdomains.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 95**
Which term refer to the electromagnetic interference that can radiate from cables?
**A.** emanations
**B.** Dopper waves
**C.** Multimode distortion
**D.** Gaussian distributions
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 96**
What is the actual IOS privilege level of User Exec mode?
**A.** 1
**B.** 0
**C.** 5
**D.** 15
**Answer: (SHOW ANSWER)**
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: 97**
What is the highest security level can be applied to an ASA interface?
**A.** 100
**B.** 200
**C.** 50
**D.** 0
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 98**
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: (SHOW ANSWER)**
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: 99**

Which description of the use of a private key is true?

**A.** The sender encrypts a message using the receiver's private key.

**B.** The sender signs a message using the receiver's private key.

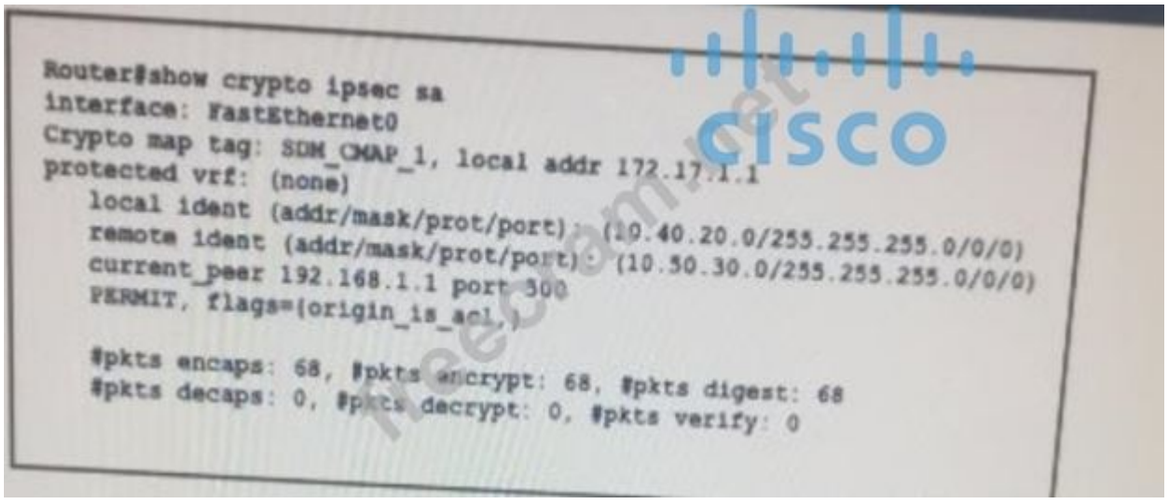
**C.** The receiver decrypts a message using the sender's private key.

**D.** The sender signs a message using their private key.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 100**

Refer to the exhibit.




For which reason is the tunnel unable to pass traffic?

**A.** UDP port 500 is blocked.

**B.** The tunnel is failing to receive traffic from the remote peer.

**C.** The IP address of the remote peer is incorrect.

**D.** The local peer is unable to encrypt the traffic.

**Answer: (SHOW ANSWER)**